1. **List out the layers in OSI reference model? And explain layers in detail?**

The OSI (Open Systems Interconnection) reference model is a conceptual framework used to understand network interactions in a seven-layer structure, each with specific roles. Here's an overview of the OSI model layers, from top to bottom:

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

Let's break down each layer and its functions.

---

1. Application Layer (Layer 7)

- **Purpose**: The Application layer is closest to the end user. It enables network access to applications, providing services such as file transfer, email, and network software services.
- **Functions**:
  - Offers network services directly to user applications (e.g., browsers, email clients).
  - Provides interfaces and protocols such as HTTP, FTP, SMTP, and DNS.
- **Examples**: Web browsers using HTTP for web access, email clients using SMTP for email exchange.

2. Presentation Layer (Layer 6)

- **Purpose**: The Presentation layer ensures that data is in a usable format for applications by translating, compressing, and encrypting it.
- **Functions**:
  - Data translation, encryption, and compression.
  - Handles data format translation, such as converting from EBCDIC to ASCII.
- **Examples**: Encryption algorithms (SSL/TLS), character encoding (ASCII, Unicode).

3. Session Layer (Layer 5)

- **Purpose**: The Session layer establishes, manages, and terminates communication sessions between applications.
- **Functions**:
  - Establishes, maintains, and closes sessions between two systems.
  - Manages dialog control (e.g., full duplex or half duplex communication).
- **Examples**: RPC (Remote Procedure Call), protocols for managing session state in web applications.

4. Transport Layer (Layer 4)

- **Purpose**: The Transport layer provides reliable data transfer across a network, ensuring that data arrives error-free and in sequence.
- **Functions**:
    - Segmentation and reassembly of data, flow control, error correction.
    - Uses protocols such as TCP for reliable communication and UDP for fast, unreliable communication.
- **Examples**: TCP (Transmission Control Protocol) for reliable data transfer, UDP (User Datagram Protocol) for faster, connectionless service.

5. Network Layer (Layer 3)

- **Purpose**: The Network layer is responsible for logical addressing and routing, determining the best path for data transmission.
- **Functions**:
    - Logical addressing (IP addressing), packet forwarding, and routing.
    - Manages packet forwarding based on IP addresses.
- **Examples**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), routers that direct traffic across networks.

6. Data Link Layer (Layer 2)

- **Purpose**: The Data Link layer provides node-to-node data transfer and error detection and correction in frames.
- **Functions**:
    - Divides data into frames and ensures frames are transferred without errors.
    - Error detection, flow control, MAC (Media Access Control) addressing for device identification within a local network.
- **Examples**: Ethernet, MAC (Media Access Control) addresses, protocols like ARP (Address Resolution Protocol).

7. Physical Layer (Layer 1)

- **Purpose**: The Physical layer transmits raw bits over a physical medium, managing the hardware and connections.
- **Functions**:
    - Defines electrical and physical specifications for devices.
    - Manages data encoding, signalling, and bit synchronization for data transmission over cables or wireless media.
- **Examples**: Ethernet cables, fibre optics, radio frequencies, network interface cards (NICs).

2. Explain TCP/IP reference model with a neat labeled diagram.

The **TCP/IP reference model** is a simplified, four-layer networking model that guides data exchange across networks. Unlike the OSI model, TCP/IP is specifically designed for internetworking (connecting different

networks). It provides end-to-end data communication, specifying how data should be packaged, transmitted, routed, and received.

Layers of the TCP/IP Model

The TCP/IP model consists of four layers, each of which corresponds loosely to layers of the OSI model:

1. **Application Layer**
2. **Transport Layer**
3. **Internet Layer**
4. **Network Access Layer**

---

1. Application Layer

- **Purpose**: Provides protocols for data communication directly to applications.
- **Functions**:
    - Provides high-level protocols for specific applications like HTTP (web browsing), FTP (file transfer), SMTP (email), and DNS (domain name resolution).
    - Handles application services, data encoding, and user authentication.
- **Corresponds to**: OSI Layers 5, 6, and 7 (Session, Presentation, Application)

2. Transport Layer

- **Purpose**: Ensures reliable data transfer between devices.
- **Functions**:
    - Manages communication reliability and data integrity through two main protocols:
        - **TCP (Transmission Control Protocol)** for reliable, connection-oriented communication.
        - **UDP (User Datagram Protocol)** for faster, connectionless communication.
    - Handles segmentation, reassembly, and flow control, enabling efficient and accurate data transfer.
- **Corresponds to**: OSI Layer 4 (Transport)

3. Internet Layer

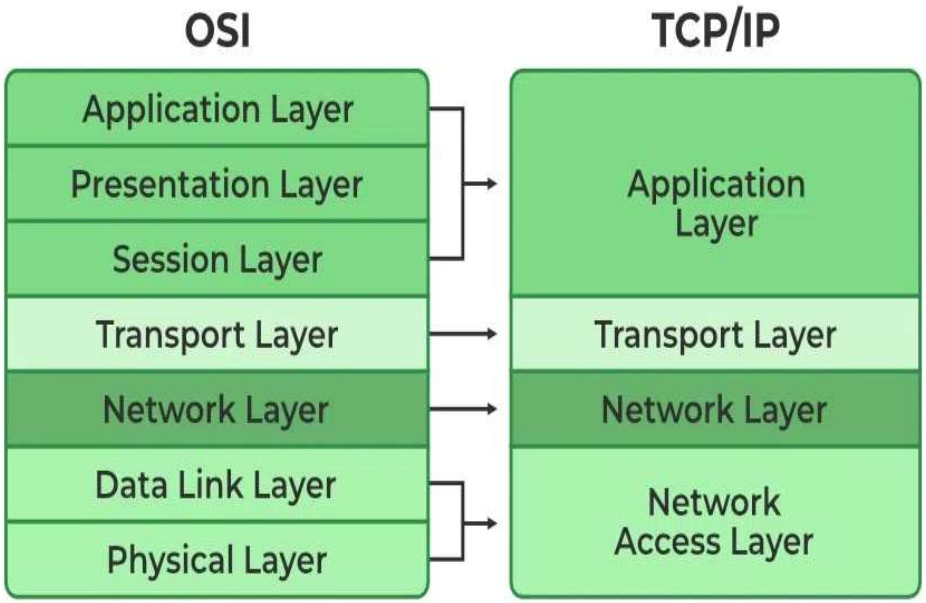
- **Purpose**: Provides logical addressing and routing.
- **Functions**:
    - Defines packet structures, addressing, and routing to send data across networks, primarily using the **IP (Internet Protocol)**.
    - Performs IP addressing and routing, allowing data to reach the correct destination.
- **Protocols**: IP, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol)
- **Corresponds to**: OSI Layer 3 (Network)

4. Network Access Layer (or Link Layer)

- **Purpose**: Manages the physical transmission of data and network interface.
- **Functions**:

- Deals with hardware addressing (MAC addresses), error detection, and data framing for direct data link communication between nodes.
- Supports specific physical media and network protocols for local transmission.

- **Examples**: Ethernet, Wi-Fi, PPP (Point-to-Point Protocol)
- **Corresponds to**: OSI Layers 1 and 2 (Physical, Data Link)



3. **Generate the CRC codeword for data-word =1001 and divisor 1011.**

Steps for CRC Calculation

1. Data word: 1001
2. Divisor (Generator Polynomial): 1011
3. Append zeros to the data word: Since the divisor has 4 bits, we append 3 zeros to the data word, making it 1001000.

Step-by-Step Binary Division (Modulo-2)

We'll divide 1001000 by 1011 using XOR operations.

1. Initial Bits: Take the first 4 bits 1001.

$$1001 \text{ XOR } 1011 = 0010$$

After this, bring down the next bit from 1001000, making it 00100.

2. Since 0010 (leftmost 4 bits) is smaller than 1011, we bring down another bit, resulting in 001000.
3. Perform XOR on the new 4 bits 1000:

$$1000 \text{ XOR } 1011 = 0011$$

Now, bring down the next bit, making it 00110.

4. Perform XOR on 0110:

Since 0110 is smaller than 1011, we bring down the final bit, making it 01100.

5. Final XOR with 1100:

$$1100 \text{ XOR } 1011 = 0111$$

The remainder after this division is 111.

Construct the CRC Codeword

The CRC codeword is the original data word appended with the remainder:

- Data word: 1001
- Remainder: 111
- CRC Codeword: 1001111

Final Answer

The CRC codeword generated for the data word 1001 with divisor 1011 is **1001111**.

4. Explain the importance of framing and Piggybacking techniques?

Framing

Definition:

Framing is the technique of encapsulating data packets into frames for transmission over a network. Each frame contains not only the payload (the actual data) but also control information, such as headers and trailers.

Importance:

a) **Data Integrity**: Framing ensures that the data is transmitted without corruption. The control information allows for error detection and correction, ensuring the integrity of the transmitted data.

b) **Synchronization**: Frames provide a clear boundary between packets of data. This synchronization helps the receiving device to identify the beginning and end of each frame, facilitating accurate data interpretation.

c) **Efficient Use of Bandwidth**: By grouping bits into frames, framing minimizes overhead, enabling efficient use of the communication channel. It helps reduce the chances of data loss during transmission.

d) **Protocol Differentiation**: Different protocols can use different framing methods (like Ethernet, PPP, etc.), allowing for protocol-specific data handling and providing flexibility in communication.

e) **Flow Control and Congestion Management**: Frames can contain information that helps in managing flow control and congestion, ensuring that the sender does not overwhelm the receiver.

Piggybacking

Definition:

Piggybacking is a technique used in two-way communication where an acknowledgment (ACK) for a received frame is sent along with the next data frame. Instead of sending a separate ACK frame, the sender combines the acknowledgment with the next outgoing data frame.

Importance:

a) **Reduced Overhead**: By combining an acknowledgment with data transmission, piggybacking minimizes the number of frames sent over the network. This reduces the overhead associated with separate acknowledgment frames, making data transmission more efficient.

b) **Increased Throughput**: Piggybacking allows for higher throughput in the network by optimizing the use of bandwidth. It leads to fewer packets being sent, which can enhance the overall efficiency of the communication process.

c) **Improved Utilization of the Network**: It makes better use of the available network capacity by allowing data frames and acknowledgments to be sent together. This technique helps in preventing the network from being idle while waiting for an acknowledgment.

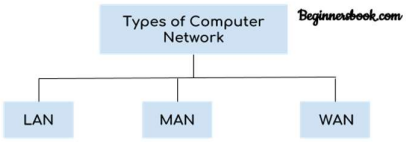
d) **Better Flow Control**: By providing feedback to the sender while simultaneously sending data, piggybacking helps maintain a smooth flow of data, preventing congestion and ensuring that the sender can adapt to the receiver's processing capabilities.

e) **Latency Reduction**: It can significantly reduce the latency in communication since the acknowledgment does not require a separate round trip. This results in quicker response times in interactive applications.

5. Define computer networks? Explain LAN, WAN, MAN in detail with a neat diagram?

Types of Computer Network: LAN, MAN and WAN

A computer network is a group of computers connected with each other through a transmission medium such as cable, wire etc.



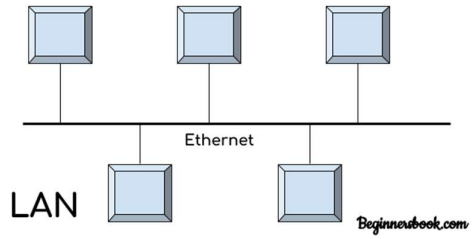
There are mainly three types of computer networks based on their size:

1. Local Area Network (LAN)

2. Metropolitan Area Network (MAN)

3. Wide area network (WAN)

1. Local Area Network (LAN)



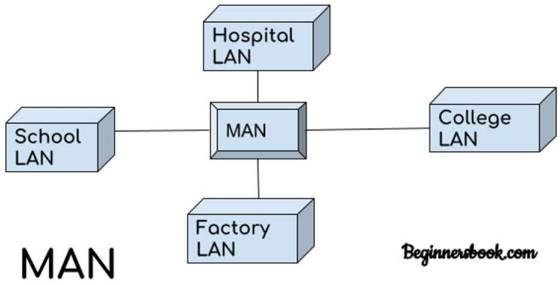
1. Local area network is a group of computers connected with each other in a small place such as school, hospital, apartment etc.

2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.

3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.

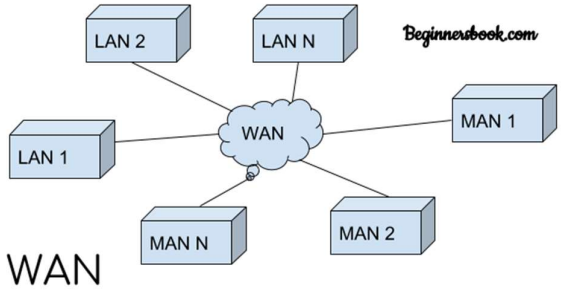
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

2. Metropolitan Area Network (MAN)



MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs (wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



WAN

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

Centralized infrastructure: One of the main advantages of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.

Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.

Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.

Expensive: Cost of installation is very high.

Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

6. **What is data communication? What are the fundamental characteristics? List and explain five components of data communication with examples?**

Data Communication

Data communication refers to the exchange of digital data between devices over a communication medium. It involves the transmission of data from a sender to a receiver, using a set of protocols that ensure the integrity and delivery of that data. Data communication can occur over various media, including wired connections (like coaxial cables and fibre optics) and wireless connections (like radio waves and infrared).

Fundamental Characteristics of Data Communication

a) **Delivery:** The data must be delivered accurately and completely to the intended recipient.
b) **Accuracy:** The data received must be the same as the data sent, ensuring no errors during transmission.
c) **Timeliness:** Data communication should occur within a reasonable time frame, providing timely delivery.
d) **Effectiveness:** The communication system must be efficient, utilizing the available bandwidth optimally without unnecessary delays.
e) **Security:** Measures should be in place to protect data from unauthorized access or tampering during transmission.

Components of Data Communication

The data communication process involves several key components, each playing a vital role in the transmission and reception of data. Here are five fundamental components:

a) **Message**
   - **Definition:** The actual data or information that is being transmitted. It can be in various forms, such as text, audio, video, or any other digital format.
   - **Example:** An email message, a file transfer (like a PDF document), or a video stream (like a YouTube video).

b) **Sender**
   - **Definition:** The device or entity that initiates the data transmission. The sender converts the message into a suitable format for transmission.
   - **Example:** A computer, smartphone, or server that sends an email or uploads a file to the internet.

c) **Receiver**
   - **Definition:** The device or entity that receives the transmitted data. The receiver converts the received signals back into a format that can be understood.
   - **Example:** A computer, smartphone, or server that receives the email or downloaded file.

d) **Transmission Medium**
   - **Definition:** The physical path through which the data travels from sender to receiver. It can be wired (copper cables, fibre optics) or wireless (radio waves, infrared).
   - **Example:**
     - Wired: Ethernet cables, fibre optic cables.
     - Wireless: Wi-Fi, Bluetooth, cellular networks.

e) **Protocol**
   - **Definition:** A set of rules and conventions that determine how data is transmitted over the network. Protocols ensure that devices can communicate effectively and understand each other.
   - **Example:**
     - TCP/IP (Transmission Control Protocol/Internet Protocol) is used for data transmission on the internet.
     - HTTP (Hypertext Transfer Protocol) is used for transferring web pages.

- FTP (File Transfer Protocol) is used for transfer

7. **Define Checksum and list the steps involved in both sender and receiver side?**

Checksum

A **checksum** is an error-detection mechanism used in data transmission to ensure the integrity of data. It involves calculating a numerical value based on the data being transmitted, which is then sent along with the data. The receiver can calculate the checksum of the received data and compare it to the transmitted checksum to determine if any errors occurred during transmission.

Steps Involved in Checksum Calculation

Sender Side

a) **Data Preparation:**
   - The sender prepares the data to be transmitted. This data could be a file, a message, or any digital information.

b) **Segmentation:**
   - The data is divided into equal-sized segments or blocks (typically, 16-bit blocks). If the last block is smaller than the specified size, it may be padded with zeros.

c) **Checksum Calculation:**
   - For each segment of data, the sender performs the following:
     - Sum all the segments together.
     - If the sum exceeds the maximum value that can be represented (e.g., 65535 for a 16-bit segment), wrap around and add the overflow back to the sum.
     - Take the one's complement of the final sum to obtain the checksum.

d) **Sending Data:**
   - The sender transmits both the original data and the calculated checksum to the receiver.
   -

Receiver Side

a) **Receiving Data:**
   - The receiver obtains the data and the accompanying checksum from the sender.

b) **Segmentation:**
   - The receiver divides the received data into the same segment sizes as the sender did.

c) **Checksum Calculation:**
   - The receiver calculates the checksum of the received data in the same manner as the sender:
     - Sum all received segments together, handling overflow as before.
     - Take the one's complement of the final sum to obtain the receiver's checksum.

d) **Checksum Comparison:**

- The receiver adds the calculated checksum to the received checksum. If the result equals the maximum value that can be represented (e.g., 65535 for a 16-bit checksum), it indicates that the data is likely error-free. If not, it indicates an error in transmission.

8. **Briefly Explain static channel and dynamic channel allocation problem.**

In computer networking and telecommunications, **channel allocation** refers to how communication channels are assigned to users or devices to enable data transmission. There are two primary types of channel allocation strategies: **static** and **dynamic**. Here's a brief explanation of both:

Static Channel Allocation

Definition: In static channel allocation, the communication channels are allocated to users or devices in a fixed manner, regardless of their demand for bandwidth. The allocation remains constant for the duration of the communication session or for a specified period.

Characteristics:

- **Fixed Assignment:** Each user is assigned a specific channel (or bandwidth) that remains unchanged during the communication session.
- **Simplicity:** The implementation of static allocation schemes is relatively straightforward since channels are pre-assigned.
- **Inefficiency:** This method can lead to inefficient use of resources. If a user does not utilize the allocated channel, the channel remains idle and is unavailable for other users.
- **Examples:** Frequency division multiplexing (FDM) where each frequency band is assigned to a specific user or time division multiplexing (TDM) where users are assigned specific time slots.

Advantages:

- Predictable performance since each user knows the channel available for their use.
- Simplified resource management as the allocation does not change.

Disadvantages:

- Inefficient utilization of channels, especially if the demand fluctuates.
- Limited flexibility to accommodate varying traffic loads.

Dynamic Channel Allocation

Definition: In dynamic channel allocation, the communication channels are allocated to users or devices based on current demand and availability. Channels can be assigned, released, or reallocated dynamically as users connect or disconnect.

Characteristics:

- **Flexible Assignment:** Users can request and release channels as needed, allowing for more efficient use of resources.
- **Scalability:** This method can accommodate varying numbers of users and fluctuating bandwidth demands more effectively.

- **Examples:** Code division multiple access (CDMA) where multiple users can share the same frequency band using unique codes, and dynamic frequency selection (DFS) that allows access points to select available channels based on current usage.

Advantages:

- More efficient use of available channels since they are allocated based on real-time demand.
- Better scalability to handle varying traffic loads and user demands.

Disadvantages:

- Increased complexity in managing channel allocation due to the dynamic nature of the assignment.
- Potential delays in channel allocation as users may have to wait for available channels.

9. **How would you compare between guided media and unguided media with examples.**

Guided Media

Definition: Guided media, also known as wired or bounded media, refers to physical transmission paths where data signals are transmitted along a specific, defined route. This type of media relies on physical cables or fibres to guide the signals from the sender to the receiver.

Characteristics:

- **Physical Connections:** Signals are transmitted through physical cables or optical fibres.
- **Less Interference:** Guided media is less susceptible to external interference compared to unguided media.
- **Higher Security:** The physical nature of the connections provides better security, as unauthorized access is more difficult.
- **Limited Mobility:** Users are typically stationary, as devices must be physically connected to the medium.

Examples:

- **Twisted Pair Cable:** Commonly used in telephone and local area networks (LANs). It consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference.
- **Coaxial Cable:** Often used for cable television and internet connections, coaxial cable consists of a central conductor surrounded by insulation, a metallic shield, and an outer cover.
- **Fiber Optic Cable:** Uses light to transmit data over long distances at high speeds. It consists of thin strands of glass or plastic that carry light signals.

Unguided Media

Definition: Unguided media, also known as wireless or unbounded media, refers to transmission methods where data signals are sent through the air or space without a defined physical path. Signals are transmitted through electromagnetic waves, and they can be received by any device within range.

Characteristics:

- **No Physical Connections:** Signals are transmitted through the air or space, allowing for greater mobility.

- **Susceptible to Interference:** Unguided media can be affected by environmental factors, such as obstacles, weather, and other electronic signals, leading to potential data loss or degradation.
- **Lower Security:** Since signals can be received by any device within range, unguided media is more vulnerable to unauthorized access and eavesdropping.
- **Greater Flexibility:** Users can connect and communicate from various locations without being physically tethered to a network.

Examples:

- **Radio Waves:** Used for broadcasting audio and video signals, such as FM/AM radio and television.
- **Microwave Transmission:** Often used for point-to-point communication systems, such as satellite communication and cellular networks.
- **Infrared Transmission:** Used for short-range communication, such as remote controls and certain wireless networking protocols (e.g., IrDA).

10. With a neat diagram, explain describe CRC encoder and decoder C (7,4).

Cyclic Redundancy Check (CRC) is an error-detection technique used in digital networks and storage devices to detect accidental changes to raw data. A CRC encoder and decoder ensure that the data sent over a network is free from errors by appending a CRC value to the data. Let's describe a CRC encoder and decoder for a specific code, C(7, 4), which means it encodes 4 bits of data into a 7-bit code word.

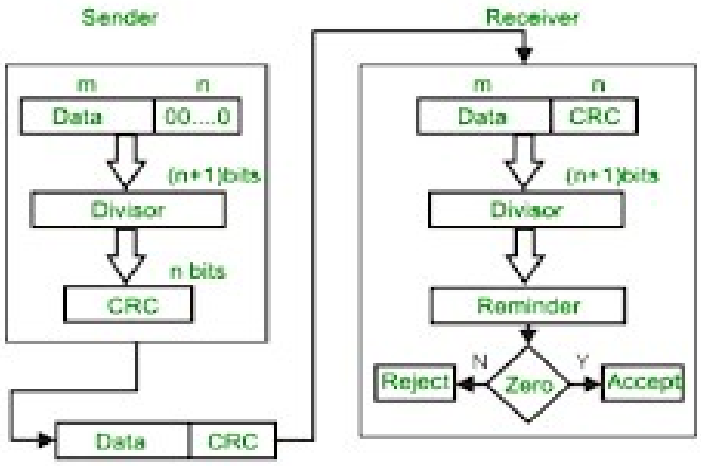
Overview of C (7, 4) Code

In C (7, 4):

- **7 bits** is the total length of the code word (including data and CRC bits).
- **4 bits** is the length of the actual data.

The remaining bits (7 - 4 = 3 bits) are used for error detection, specifically the CRC bits.

1. **CRC Encoder:**
   - **Message Polynomial:** Represent the 4-bit message as a polynomial.
   - **Generator Polynomial:** Choose a generator polynomial (usually denoted as G(x)).
   - **Shift Register:** Perform the division of the message polynomial by the generator polynomial using a s hift register.
   - **Codeword:** The 7-bit codeword is formed by appending the remainder to the original message.
2. **CRC Decoder:**
   - **Received Polynomial:** Represent the received 7-bit codeword as a polynomial.
   - **Shift Register:** Divide the received polynomial by the same generator polynomial used in encoding.
   - **Error Detection:** If the remainder is zero, the message is considered error-free; otherwise, an error is detected.



11. How would you describe the working of Go-Back-N protocol and how it is different from selective repeat ARQ?

- **Go-Back-N** is simpler but can lead to inefficiencies due to its requirement to retransmit all frames after a lost frame. It is suitable for environments where the network is reliable and has low latency.
- **Selective Repeat ARQ** is more efficient in terms of bandwidth usage as it only retransmits specific frames that are lost or erroneous, allowing for better utilization of the network. However, it requires more complex mechanisms for buffering and managing frame acknowledgments.

I. Go-Back-N Protocol

Working of Go-Back-N:

a) **Sliding Window Mechanism:**
   - The sender can send multiple frames (up to a window size, NNN) without waiting for an acknowledgment for the first frame.

b) **Frame Transmission:**
   - Frames are sent consecutively, each with a sequence number starting from 0.

c) **Receiving Acknowledgments:**
   - The receiver sends an ACK for the last correctly received frame. If a frame is lost or erroneous, the receiver discards that frame and all subsequent ones, only sending an ACK for the last correct one.

d) **Retransmission:**
   - If a frame is not acknowledged, the sender retransmits that frame and all subsequent frames in the window.

Illustration:

- **Sender:** Sends frames 0, 1, 2, 3, 4.
- **Receiver:** Receives frames 0, 1, 2, but frame 3 is lost, sending an ACK for frame 2.
- **Sender:** Retransmits frames 3, 4 after a timeout.

II. Selective Repeat ARQ Protocol

Working of Selective Repeat ARQ:

a) **Sliding Window Mechanism:**

- Similar to Go-Back-N, but the sender can also send multiple frames without waiting for ACKs.

b) **Frame Transmission:**

- The sender transmits up to NNN frames.

c) **Receiving Acknowledgments:**

- The receiver acknowledges frames individually. If a frame is received out of order, it is buffered instead of discarded.

d) **Retransmission:**

- Only the specific lost frames are retransmitted, not the subsequent frames.

Illustration:

- **Sender:** Sends frames 0, 1, 2, 3, 4.
- **Receiver:** Receives frames 0, 1, 2, but frame 3 is lost, sending an ACK for frame 2.
- **Sender:** Only retransmits frame 3.

12. Explain how the differences between IPv4 and IPv6 impact internet-connectivity and address management in practical scenarios?

The transition from IPv4 to IPv6 represents a significant evolution in internet connectivity and address management, primarily driven by the limitations of IPv4. Here's an explanation of how the differences between IPv4 and IPv6 impact these areas in practical scenarios:

1. Address Space

IPv4:

- **Format:** Uses 32-bit addresses, allowing for about 4.3 billion unique addresses.
- **Limitation:** As the internet grew, the available IPv4 addresses became exhausted, leading to address scarcity and challenges in assigning addresses to new devices.

IPv6:

- **Format:** Uses 128-bit addresses, which allows for approximately 3.4×10383.4 \times 10^{38}3.4×1038 unique addresses.
- **Impact:** The vast address space of IPv6 alleviates address exhaustion issues, enabling every device to have a unique address. This is particularly important for the growing number of Internet of Things (IoT) devices.

2. Address Management

IPv4:

- **Network Address Translation (NAT):** Due to limited addresses, NAT is often used to allow multiple devices on a local network to share a single public IP address. This complicates network configuration and management.
- **Subnetting:** Subnetting is necessary to manage address allocation efficiently, leading to complex routing and management overhead.

IPv6:

- **No NAT Required:** The abundance of IPv6 addresses reduces the need for NAT, simplifying network architecture. Each device can have a globally unique address, enhancing end-to-end connectivity.
- **Simplified Addressing:** IPv6 allows for hierarchical addressing and routing, making it easier to manage large networks and allocate addresses in a more structured manner.

3. Connectivity

IPv4:

- **Limited Mobility:** IPv4 can struggle with mobile devices due to NAT and its reliance on fixed IP addresses, making it challenging for devices to maintain connectivity when changing networks.
- **Routing Table Size:** As networks grow, IPv4 routing tables can become large and unwieldy, impacting routing efficiency and performance.

IPv6:

- **Improved Mobility:** IPv6 supports better mobility features, allowing devices to move between networks while maintaining their IP addresses, thus ensuring consistent connectivity.
- **Efficient Routing:** The hierarchical nature of IPv6 addresses leads to more efficient routing, reducing the size of routing tables and improving overall network performance.

4. Security Features

IPv4:

- **Optional Security:** Security features like IPsec are optional in IPv4, meaning that not all implementations utilize them, potentially exposing data to security risks.

IPv6:

- **Built-in Security:** IPv6 was designed with security in mind, incorporating IPsec as a fundamental component. This enhances the security of communications over the internet, making it more robust against attacks.

5. Practical Scenarios

- **IoT Expansion:** As the IoT ecosystem expands, the need for a vast number of IP addresses becomes critical. IPv6's address space allows for unique addressing for millions of devices, facilitating their integration into the internet.
- **Cloud Computing:** Organizations leveraging cloud services benefit from IPv6's ability to provide a unique address for each virtual machine, enhancing scalability and simplifying management.
- **Home Networks:** With more devices connecting to home networks (smart TVs, smartphones, smart appliances), IPv6 allows each device to connect with its own address without the complexities of NAT.
- **Network Performance:** For service providers, the efficient routing enabled by IPv6 can lead to reduced latency and improved service quality, benefiting end-users.

13. **A pure aloha network transmits 200-bit frames on a shared channel of 200kbps. Where the throughput if the system (all station together) produces a 1000 frames per second B. 500 framesper seconds C. 250 Frames per second**

To calculate the throughput of a pure Aloha network, we need to understand the basic principles of the Aloha protocol. In a pure Aloha system, the maximum throughput can be determined using the formula:

$$S = G \cdot e^{-2G}$$

Where:

- S is the throughput (in frames per second).
- G is the traffic load (the average number of frames generated by the system in one frame time).

Step 1: Calculate Frame Time

The frame size is given as 200 bits, and the channel capacity is 200 kbps (kilobits per second). First, we calculate the time taken to send one frame (frame time):

$$\text{Frame time} = \frac{\text{Frame size}}{\text{Channel capacity}} = \frac{200 \text{ bits}}{200,000 \text{ bits per second}} = 0.001 \text{ seconds} = 1 \text{ ms}$$

Step 2: Calculate the Traffic Load (G)

The traffic load G can be calculated based on the total number of frames generated by the system per second and the frame time.

Given scenarios:

- A. 1000 frames per second
- B. 500 frames per second
- C. 250 frames per second

Let's calculate G for each scenario:

$$G = \text{frames per second} \times \text{frame time}$$

- For 1000 frames per second:

$$G = 1000 \text{ frames/sec} \times 0.001 \text{ sec} = 1$$

- For 500 frames per second:

$$G = 500 \text{ frames/sec} \times 0.001 \text{ sec} = 0.5$$

- For 250 frames per second:

$$G = 250 \text{ frames/sec} \times 0.001 \text{ sec} = 0.25$$

Step 3: Calculate Throughput (S)

Now, we can calculate the throughput for each scenario using the $S = G \cdot e^{-2G}$ formula.

1. For $G = 1$:

$$S = 1 \cdot e^{-2 \cdot 1} = 1 \cdot e^{-2} \approx 1 \cdot 0.1353 \approx 0.1353 \text{ frames per second}$$

2. For $G = 0.5$:

$$S = 0.5 \cdot e^{-2 \cdot 0.5} = 0.5 \cdot e^{-1} \approx 0.5 \cdot 0.3679 \approx 0.1839 \text{ frames per second}$$

3. For $G = 0.25$:

$$S = 0.25 \cdot e^{-2 \cdot 0.25} = 0.25 \cdot e^{-0.5} \approx 0.25 \cdot 0.6065 \approx 0.1516 \text{ frames per second}$$

14. Differentiate between packet switching and circuit switching.

Circuit Switching

Circuit switching is a method where a dedicated communication path or circuit is established between two endpoints for the duration of a communication session. This approach is traditionally used in voice communication systems, like the Public Switched Telephone Network (PSTN).

- **Connection Setup**: A dedicated path must be established before data transmission can start. This setup time can introduce initial delays.
- **Dedicated Path**: Once the path is established, it remains dedicated to that session, meaning no other data can use the path until the session ends.
- **Continuous Data Flow**: Data flows in a continuous, predictable manner since the path is reserved exclusively for that connection.
- **Fixed Bandwidth**: Circuit switching provides fixed bandwidth for each connection, ensuring consistent quality of service (QoS).
- **Examples**: Traditional telephone networks, Integrated Services Digital Network (ISDN).

Advantages:

- Reliable and predictable performance due to dedicated paths.
- Ideal for real-time, continuous data transfer (e.g., voice and video).

Disadvantages:

- Inefficient use of resources, as the dedicated path remains idle if no data is being sent.
- Connection setup time can introduce delays.
- Poor scalability for networks with high traffic, as each connection requires a separate path.

Packet Switching

Packet switching is a method where data is divided into packets before being transmitted. Each packet is sent independently, potentially taking different routes to reach the destination. Packet switching is widely used in digital networks, including the internet.

- **No Dedicated Path**: Packets are routed individually based on the destination address in each packet, with no dedicated path required.
- **Dynamic Routing**: Each packet can take a different path to reach the destination, allowing for efficient use of network resources.
- **Burst Transmission**: Data is sent in bursts, with packets sent as they become available.
- **Variable Bandwidth**: The network dynamically allocates bandwidth, adjusting based on traffic and congestion.
- **Examples**: Internet Protocol (IP) networks, Ethernet, Voice over IP (VoIP).

Advantages:

- Efficient use of network resources as bandwidth is shared among multiple users.
- High scalability due to flexible routing and resource allocation.
- Suitable for data that can tolerate slight delays, like emails or web browsing.

Disadvantages:

- Potential for variable delays and packet loss due to network congestion.
- Not ideal for real-time applications without additional QoS measures.
- Packets may arrive out of order and need reassembly, requiring extra processing.

15. What is the process of error detection and error correction in block coding?

Error detection and correction in **block coding** is crucial for maintaining data integrity, especially in digital communication systems where errors can occur due to noise, signal degradation, or interference. Block coding achieves this by encoding the original data bits into longer sequences called "codewords," which include additional, carefully calculated bits known as redundant or parity bits. These extra bits enable the receiving system to detect errors, and in certain cases, correct them without needing to request a retransmission, thereby enhancing data reliability and transmission efficiency.

Parity Checking

Parity checking is one of the simplest methods of error detection. It works by adding a single extra bit, known as a parity bit, to each block of data. This parity bit is set in a way that the total number of 1's in the block becomes either even or odd. In even parity, the parity bit is chosen so that the sum of all 1's in the codeword is even, whereas in odd parity, it is set to make the sum odd. If the data arrives at the destination with an incorrect parity, it indicates that an error has occurred during transmission. While parity checking is straightforward and useful for detecting single-bit errors, it has limitations. It cannot detect multiple errors that balance each other out (i.e., an even number of errors), nor can it pinpoint the exact location of the error, making it unsuitable for error correction.

Cyclic Redundancy Checks (CRC)

Cyclic Redundancy Check (CRC) is a more advanced method commonly used for error detection in network communications, such as LANs and WANs. CRC works by treating the data as a long binary number and performing polynomial division to generate a unique remainder called the *frame check sequence*. This sequence is appended to the data before transmission. Upon receiving the data, the receiver performs the same polynomial division. If the calculated remainder (or frame check sequence) matches the appended sequence, the data is considered error-free; otherwise, an error is detected. CRC is particularly effective at detecting burst errors (a series of consecutive errors) and is widely used due to its robustness. However, CRC alone does not provide error correction; it's often used in systems that can request data retransmission if an error is detected.

Hamming Codes

Hamming codes offer both error detection and correction by adding multiple parity bits to each block of data. These parity bits are placed at specific positions in the codeword, creating a pattern that allows the receiver to identify the location of any single-bit error. For example, a (7,4) Hamming code encodes four data bits with three parity bits, creating a 7-bit codeword that can detect and correct any single-bit error. If an error is detected, the system calculates a value known as the "syndrome," which indicates the position of the error, enabling the receiver to flip the incorrect bit back to its original state. Hamming codes are particularly useful in scenarios

where single-bit errors are expected, and retransmission is not feasible, such as in computer memory systems or satellite communications.

Checksum Method

The checksum method is widely used for detecting errors in data transmissions, particularly in packet-based systems. In this technique, data is divided into segments, and a mathematical sum (known as the checksum) is calculated by adding up the segments using 1's complement arithmetic. This checksum is then transmitted alongside the data. Upon receiving the data, the receiver performs the same calculation and compares the checksum to the received checksum. If there's a mismatch, an error is detected. The checksum method is relatively simple and effective for detecting errors caused by random noise. However, it may be less capable of detecting complex or systematic error patterns, like certain types of burst errors, so it is often used in systems where error patterns are relatively random.

16. Briefly explain the problems in layered architecture.

The layered architecture is essential for organizing the different aspects of network communication.

However there are some common design issues that arises within this layered approach.

1) Layer dependencies & overhead:

Layers are designed to function independently with a specific set of responsibilities. However, this can create dependencies b/w layers where on layer needs information from another, resulting in overhead.

2) Layered complexity & performance:

Each layer adds its own processing, which can impact overall performance due to the extra processing time & memory usage

3) Data Duplication and fragmentation:

Data may need to be duplicated or split across layers. For examples, headers added at each layer can increase size, reducing transmission efficiency. This fragmentation and reassembly can lead to resource wastage and performance issues.

4) Cross-Layer Optimization challenges:

Optimizing the performance of one layer can sometimes negatively affect other layers.

For instance, if the transport layer tries to handle congestion control, it may conflict with similar mechanisms at network layer, causing in efficiencies.

5) Inter layer communication:

Layers are designed to communicate only with their adjacent layers. This constraint can make it challenging to pass necessary information directly b/w non-adjacent layers, potentially limiting performance optimizations.

17. What is VPN

Virtual Private Network (VPN):

It is a technology that allows users to create a secure and encrypted connections over a less secure network, typically the internet.

VPNs are widely used for enhancing privacy, securing communications, and enabling remote access to private networks.

VPNs work by creating an encrypted tunnel between the user's device and a VPN server, often located in a different geographic location.

This tunnel masks the user's IP address and encrypts data, making it difficult for 3rd parties, such as hackers, Internet service providers (ISPs), or even government agencies to monitor users online activities

→ When a user connects to a VPN:

1. Data is encrypted on user's device & sent to the VPN server.
2. The VPN server decrypts the data and sends it to the intended destination (e.g., a website or service).

3. The response from the destination is encrypted again by the VPN server and sent back to the user.

Advantages:

1. Enhanced security:

VPNs use strong encryption protocols to protect data, making it harder for unauthorized users or intercepts or access sensitive information.

2. Anonymity and Privacy:

By mistaking the user's IP address, VPNs can provide greater privacy and help prevent tracking by websites, ISPs or advertisers.

3. Remote Access to Resources

VPNs allow employees to securely access company resources from any location with an internet connection.

Disadvantages:

1. Slower speeds:

encryption & rerouting of traffic can lead to slower speeds.

2. Potential for VPN Blocking:

some services block VPN traffic, making it harder for certain users to access certain con while connected to a VPN

18. Explain about composite signals and their uses in data communication

Composite Signals

A composite signal is a combination of multiple sinusoidal signal signals, each with a different frequency, amplitude, and phase, combined to form a more complex waveform.

These composite signals can represent different types of data and are commonly used in digital communication to transmit information efficiently over a communication channel.

1) Carrying multiple frequencies (Frequency Spectrum):

- Composite signals have multiple frequency components which allows them to carry more information than a single frequency signal.

This is important in digital communication because digital data is often represented by high-frequency signals.

Ex: A digital signal which consists of binary values, can be represented by a series of different frequencies, with each frequency corresponding to a particular bit pattern.

2) Modulation and multiplexing:

Composite signals allow for modulation techniques where digital data modulates (alters) a carrier wave (sinusoidal signal) to create a composite waveform. Modulation methods like Amplitude modulation, frequency modulation and phase modulation use composite signals to encode information, making it easier to transmit data over long distances.

- In multiplexing, composite signals help combine multiple channels or data streams into a single signal allowing simultaneous transmission over a shared medium (eg Frequency Division multiplexing.

3) Bandwidth Efficiency:

- The frequency range, or bandwidth of a composite signal determines the amount of information it can carry.
By using composite signals with higher frequencies, digital communication systems can achieve higher bandwidths, enabling faster data transmission

4) Transmission of complex waves:

In digital communication, signals are often converted to complex waveforms to transmit bits over a channel. A composite signal which contains various frequencies, can represent these forms more accurately, thus improving the quality and reliability of data transmis

5) Reducing Interference:

Composite signals can help reduce interference from By carefully choosing the frequencies within a comp signals communication systems can minimize overlap with common sources of interference, such as other communication channels or envi noise

19.

a) What is the propagation time if the distance between the 2 points is 12000 km ? Assume the propagation speed in the cable is 2.4×10^8 m/s ?

A) Propagation time is the time it takes for a signal to travel from one point to another over a certain distance.

Given that

D = distance = 12000 km = 12000×10^3 m
$= 12 \times 10^6$ m

S = propagation speed = 2.4×10^8 m/s

T = Propagation time = $\frac{D}{S}$

$T = \frac{12 \times 10^6}{2.4 \times 10^8} = 0.05$ seconds

T = 50 milliseconds

20. Explain bit length, bit rate, baud rate

Bit Rate:

Bit rate is the number of bits transmitted per second in a communication channel. It is a measure of data transmission speed and is typically expressed in bits per second (bps).

Bit rate reflects the amount of data transferred over a network within a specific period of time.

$$\text{Bit Rate} = \frac{\text{No of. Bits}}{\text{Time}}$$

Bit length:

- Bit length refers to the physical length of one bit in a transmission medium. It is the distance a single bit occupies on a medium (such as cable) while it is being transmitted.
- Bit length depends on both the propagation speed in the medium and the bit rate of transmission.

$$\text{Bit Length} = \text{Propagation Speed} \times \frac{1}{\text{Bit Rate}}$$

Baud Rate:

It is the number of signal changes (or symbol changes) per second in a communication channel. It measures the rate at which the signal or carrier changes, and its often expressed in symbols per second.

$$\text{Baud Rate} = \frac{\text{Bit Rate}}{\text{No of Bits per symbol}}$$

21. Explain the different frame types in HDLC?

Different Frame Types in HDLC

High-Level Data Link Control (HDLC) is a protocol used for data transmission across a network. It operates on the data link layer of the OSI model and provides reliable communication by managing frames, ensuring error detection, and supporting flow control. HDLC defines three distinct frame types: **Information (I) frames**, **Supervisory (S) frames**, and **Unnumbered (U) frames**. Each frame type serves a specific purpose to facilitate effective data communication.

Information (I) frames are the most commonly used frames in HDLC and carry the actual user data from one network device to another. These frames are used for transmitting sequential data and carry sequence numbers that help ensure that the frames are received in order, enabling the protocol to detect and request retransmission of any missing frames. They also provide acknowledgment capabilities within the frame itself, allowing for efficient two-way communication.

Supervisory (S) frames are used for flow control and error control, without carrying any actual user data. They support functions like acknowledgment (ACK), negative acknowledgment (NACK), and request for retransmission of frames. S frames help manage the status of the link by indicating if the receiver is ready to accept more data, has encountered an error, or if it is temporarily not ready to receive data.

Unnumbered (U) frames serve a variety of control purposes and are used primarily for link management. Unlike I and S frames, U frames are not sequenced, making them ideal for initializing and managing the connection state. They are used to establish, terminate, and reset connections and can also convey commands such as "Set Asynchronous Balanced Mode" (SABM) to initiate the connection and "Disconnect" (DISC) to terminate it. U frames provide flexibility in controlling the link status and handling various control functions required for network management.

Each frame type in HDLC plays a vital role in ensuring smooth data communication, allowing HDLC to offer reliable, orderly, and error-free data transfer across networks.

22. Explain stop and wait automatic repeat request protocol?

Stop-and-Wait Automatic Repeat Request (ARQ) Protocol

The Stop-and-Wait Automatic Repeat Request (ARQ) protocol is a simple and widely used error-control mechanism in data communication. It ensures reliable data transfer by allowing only one data frame to be transmitted at a time, and requiring the sender to wait for an acknowledgment (ACK) from the receiver before sending the next frame. If the acknowledgment is not received within a specified timeout period, the sender assumes the frame was lost or corrupted and retransmits it.

In this protocol, the process begins when the sender transmits a single data frame to the receiver. Once the receiver successfully receives and verifies the frame, it sends an acknowledgment back to the sender. Upon receiving the ACK, the sender is allowed to send the next frame in the sequence. This approach is straightforward but introduces a

significant delay in cases where the round-trip time (RTT) is high, as the sender must wait for an acknowledgment after each frame. This waiting time can lead to inefficiencies, particularly in high-latency networks.

Stop-and-Wait ARQ also employs a simple error-detection mechanism. If a frame is found to be corrupted on the receiver's end (often detected using checksums), the receiver discards it and does not send an acknowledgment. This lack of acknowledgment prompts the sender to retransmit the frame once the timeout period elapses, ensuring that corrupted or lost frames are re-sent. However, if the acknowledgment itself is lost, the sender will retransmit the frame, potentially causing the receiver to receive the same frame twice. To prevent duplicate frames, sequence numbers (typically 0 and 1) are added to the frames, allowing the receiver to recognize and discard duplicates if necessary.

The Stop-and-Wait ARQ protocol is simple and effective for error detection and control, but it is not optimal for high-speed or long-distance networks, as it can lead to idle waiting times. Nonetheless, it forms the basis for more complex and efficient ARQ protocols used in modern data communication.

23. With the suitable example explain the working of CDMA?

Working of CDMA (Code Division Multiple Access)

Code Division Multiple Access (CDMA) is a multiple-access method used in communication systems, enabling multiple users to share the same frequency spectrum simultaneously. Unlike other techniques like Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), where users are separated by frequency or time, CDMA assigns each user a unique code sequence. These unique codes allow multiple users to transmit simultaneously over the same frequency band, with each user's signal distinguished by its code.

In CDMA, each user is assigned a unique spreading code, also known as a pseudo-random noise (PN) code or spreading sequence. The data signal from each user is multiplied (spread) by this code, which increases the bandwidth of the original signal, spreading it across a wide frequency range. At the receiver's end, the signal is multiplied by the same code to retrieve the original data. Because each user's code is orthogonal (i.e., has low cross-correlation) to others, the receiver can differentiate between signals even if multiple users transmit on the same frequency at the same time. This approach is highly resistant to interference and allows efficient use of available bandwidth.

Example of CDMA Working

Consider three users, **User A**, **User B**, and **User C**, all transmitting on the same frequency. Each user has a unique code sequence:

- **User A**: Code sequence `[+1, -1, +1, -1]`
- **User B**: Code sequence `[+1, +1, -1, -1]`
- **User C**: Code sequence `[+1, -1, -1, +1]`

Each user's data signal is multiplied by its code sequence, which spreads the signal across the frequency spectrum. Let's say **User A** wants to transmit a binary bit '1' and **User B** and **User C** want to transmit '0'. In CDMA, a binary '1' is represented by the original code sequence, while a '0' is represented by the inverted code sequence.

- **User A** transmits: `[+1, -1, +1, -1]`
- **User B** transmits: `[-1, -1, +1, +1]`
- **User C** transmits: `[-1, +1, +1, -1]`

The combined signal on the channel is the sum of these signals: `[(-1), (-1), (+3), (-1)]`.

When the signal reaches the receiver, each user's receiver multiplies the combined signal by their unique code sequence to retrieve the original bit. For **User A**, the receiver will multiply the combined signal by **User A**'s code sequence `[+1, -1, +1, -1]`. After decoding, if the output is a positive sum, the bit is interpreted as '1', and if it's negative, it is interpreted as '0'. This process allows each user to retrieve their original data bit without interference from others.

24. With the flow diagram explain the working of CSMA/CD?

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

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol used in wired local area networks (LANs) to manage data transmission and prevent data collisions on a shared communication channel. This protocol is especially crucial in Ethernet networks, where multiple devices may attempt to transmit data simultaneously. CSMA/CD helps ensure that devices take turns in accessing the network and, if a collision occurs, efficiently handles retransmission.

Steps in CSMA/CD Process with Flow Diagram Explanation

In CSMA/CD, a device listens to the channel to determine if it's free before transmitting data. If the channel is busy, the device waits until it becomes free. After detecting no active transmissions, it proceeds to transmit data. If two devices attempt to transmit at the same time, a collision occurs, which is detected by the devices, prompting them to stop transmitting and wait for a random time before attempting to retransmit. Below is an explanation of each step along with a flow diagram representation.

Step 1: Carrier Sensing

1. **Listen to Channel**: Before transmitting, each device listens to the network to check if the channel is idle.
2. **Channel Status Check**: If the channel is busy (occupied by another device), the device waits until it becomes free.

Step 2: Data Transmission

1. **Transmit Data**: Once the device detects an idle channel, it begins transmitting data.

Step 3: Collision Detection

1. **Detect Collision**: If two devices transmit simultaneously, a collision occurs. Each device can detect this by monitoring the voltage or signal strength on the network.
2. **Stop Transmission**: Upon detecting a collision, both devices immediately stop transmitting to avoid further interference.

Step 4: Backoff Mechanism

1. **Random Wait**: After detecting a collision, each device waits for a random period before retrying. This random delay helps reduce the likelihood of another collision when they attempt to retransmit.
2. **Retransmission**: Once the random waiting time has elapsed, each device reattempts the transmission, starting with the channel sensing phase again.

Step 5: Successful Transmission

1. **Transmission Success**: If there is no collision during the transmission, the data is successfully transmitted to the destination.

Flow Diagram for CSMA/CD

Below is a simplified flow of how CSMA/CD operates:

1. **Start**: The device checks if the channel is idle.
2. **Channel Free?**:
    - If the channel is busy, the device waits and rechecks.
    - If the channel is free, it starts transmitting data.
3. **Collision Occurred?**
    - If no collision occurs, the transmission is completed successfully.
    - If a collision occurs, both devices stop transmitting and enter the backoff phase.
4. **Backoff and Retransmit**: After a random waiting period, the devices sense the channel again and attempt to retransmit.

CSMA/CD efficiently controls access to the shared medium, minimizing collision impacts and maintaining smooth data flow in wired networks, making it a foundational protocol in Ethernet technology.

. Explain the working of virtual circuit in computer networks?**(Feb/Mar 2022)**

25. A pure ALOHA network transmits 200 bit frames on a shared channel of 200kbps. What is the through put if the system produces i) 1000 frames/sec ii) 500 frames/sec. **(04 Marks)**

Working of Virtual Circuit in Computer Networks

A virtual circuit is a method used in computer networks, especially in packet-switched networks, to create a logical connection between a source and a destination before data transmission. This logical path allows data packets to follow the same route across the network, which provides a more predictable and organized

transmission process. Virtual circuits are often used in connection-oriented networks, such as Frame Relay, ATM (Asynchronous Transfer Mode), and MPLS (Multiprotocol Label Switching).

The working of a virtual circuit involves three main stages:

1. **Connection Establishment**: Before data transmission, a connection is established between the sender and receiver. The network assigns a unique virtual circuit identifier (VCI) for this connection, which remains consistent throughout the session. Routers along the path set up routing tables to recognize this VCI, ensuring that packets will follow the predetermined path.
2. **Data Transfer**: Once the connection is established, data is transmitted in packets. Each packet includes the VCI, allowing routers to quickly forward the packets along the predefined path without needing to inspect the full IP address. This process reduces processing time and enhances data transfer speed. Since the packets follow the same path, they arrive in order, reducing the need for reassembly at the destination.
3. **Connection Termination**: After data transmission is complete, the connection is terminated. The sender and receiver send messages to release the reserved resources and clear the routing tables. This step ensures that resources are freed up for other transmissions, maintaining network efficiency.

Virtual circuits provide advantages such as predictable routing and ordered packet delivery. However, they can be less flexible than datagram (connectionless) networks, as they require initial setup time and resource reservation.

To calculate the throughput for a Pure ALOHA network, we can use the throughput formula for Pure ALOHA:

$$S = G \cdot e^{-2G}$$

where:

- S is the throughput (in frames per second),
- G is the average number of frames generated by the system per second.

Given Data

- **Frame size** = 200 bits
- **Channel bandwidth** = 200 kbps (kilobits per second)
- **Throughput formula** for Pure ALOHA: $S = G \cdot e^{-2G}$

Since the channel bandwidth is 200 kbps, we can transmit up to:

$$\text{Max frames per second} = \frac{\text{Channel bandwidth}}{\text{Frame size}} = \frac{200,000 \text{ bits per second}}{200 \text{ bits per frame}} = 1000 \text{ frames per second}$$

Now, we will calculate the throughput for the given values of G.

i) $G = 1000$ frames per second

Substitute $G = 1000$ into the throughput formula:

$$S = 1000 \cdot e^{-2 \cdot 1000}$$

Calculating e^{-2000} results in a very small number, effectively zero for practical purposes. This indicates that, at such a high frame generation rate, collisions dominate, leading to a throughput close to zero.

ii) $G = 500$ frames per second

Substitute $G = 500$ into the throughput formula:

$$S = 500 \cdot e^{-2 \cdot 500}$$

Similarly, calculating e^{-1000} will yield an extremely small number, leading to a throughput near zero for practical purposes due to excessive collisions.

26. Explain in detail the three controlled access methods?

Controlled access methods are networking protocols that regulate how multiple devices share a communication channel, minimizing collisions by coordinating access. The three main controlled access methods are **Reservation**, **Polling**, and **Token Passing**.

1. Reservation Access Method

In the reservation method, devices make reservations for a time slot before they can transmit data. The channel is divided into fixed time slots, and each device reserves a slot in advance, which helps prevent collisions by ensuring only one device transmits in a given slot. This method is widely used in centralized systems, like satellite communication networks.

Pros: Reduces collision risk; efficient for time-sensitive applications.
Cons: Can be inefficient if slots are unused; doesn't scale well for large networks due to high reservation overhead.

2. Polling Access Method

In polling, a central controller (like a server or primary device) polls each device in a sequence, giving each one a chance to transmit. Devices can only send data when they are specifically polled. This approach ensures orderly access to the channel, often used in systems where a central controller can manage communication, such as point-of-sale (POS) systems.

Pros: Ensures collision-free access; orderly communication.
Cons: Adds overhead with polling messages; central controller failure disrupts network operation.

3. Token Passing Access Method

In token passing, a special packet known as a token circulates around the network. Only the device that holds the token is allowed to transmit data. After transmitting, the device passes the token to the next device

in the sequence, creating a controlled access loop. This method is effective in networks with ring or bus topologies, like Token Ring and Fiber Distributed Data Interface (FDDI) networks.

Pros: Eliminates collisions, provides fair access to the channel.
Cons: Token loss or duplication can disrupt the network; slower in larger networks due to token passing delay.

27. What is the frame format of PPP? In detail?

The **Point-to-Point Protocol (PPP)** is used to establish direct connections between two network nodes, allowing for the transport of multi-protocol datagrams over a link. It is commonly employed in Internet connections like dial-up and VPNs. The PPP frame format consists of several fields, each serving a specific purpose to ensure efficient data transmission.

The **Flag** field, 1 byte in length, marks the beginning and end of the PPP frame. The value for the Flag is `0x7E` (in hexadecimal), represented as `01111110` in binary. It helps delimit the frame boundaries and prevent confusion with other bit sequences in the data, achieved through **bit stuffing**. If the sequence `11111` appears in the data, a `0` bit is inserted, ensuring the frame's integrity.

The **Address** field is also 1 byte, typically set to `0xFF`, indicating a broadcast address in PPP. This is because PPP is a point-to-point protocol, and there is no need to assign specific addresses for individual nodes.

The **Control** field, 1 byte in length, is usually set to `0x03`, indicating an **Unnumbered Information (UI)** frame type. This field controls the flow of information within the PPP frame. Since PPP is primarily used for simple, direct connections, it does not require sophisticated sequencing or flow control mechanisms.

The **Protocol** field, 2 bytes, specifies the protocol used to interpret the data portion of the frame. Common values include `0x0021` for Internet Protocol (IP), `0x8021` for AppleTalk, and `0x0057` for IPX. This field identifies the network layer protocol being transmitted, allowing the receiver to process the data appropriately.

The **Data** field, which can vary in length, carries the actual data being transmitted. The data format depends on the protocol specified in the Protocol field. For instance, if the protocol is `0x0021` (IP), the data would contain an IP packet. The maximum size of the Data field is constrained by the Maximum Transmission Unit (MTU) of the physical link, typically 1500 bytes.

The **Frame Check Sequence (FCS)** field, which can be either 2 bytes or 4 bytes, is used for error detection. It contains a **Cyclic Redundancy Check (CRC)** value calculated over the Address, Control, Protocol, and Data fields. The FCS ensures that any errors introduced during transmission are detected. If the FCS does not match the expected value at the receiver, the frame is discarded.

In summary, the PPP frame consists of the Flag, Address, Control, Protocol, Data, and FCS fields, which work together to enable reliable data communication over point-to-point links. Each field serves a specific function, from marking frame boundaries to ensuring error-free data transfer.

28. Explain 802.3 MAC frame format?

The **802.3 MAC (Media Access Control) frame format** is used in Ethernet networks to define how data is transmitted between devices on the network. It specifies the structure of the frame that encapsulates the data to be transmitted over the physical medium. Here's a breakdown of the 802.3 MAC frame format:

1. Preamble (7 bytes)

- **Purpose:** The preamble helps devices synchronize with the start of the frame. It is a series of 7 bytes, each containing the bit pattern `10101010`.
- **Function:** It helps in bit synchronization so the receiving device can detect the incoming frame correctly.

2. Start Frame Delimiter (SFD) (1 byte)

- **Purpose:** The SFD marks the actual start of the frame.
- **Bit Pattern:** `10101011`
- **Function:** It signals to the receiving device that the frame is starting and is followed by the destination address.

3. Destination MAC Address (6 bytes)

- **Purpose:** This field contains the MAC address of the device to which the frame is being sent.
- **Format:** 6 bytes (48 bits).
- **Example:** `00:11:22:33:44:55`.

4. Source MAC Address (6 bytes)

- **Purpose:** This field contains the MAC address of the device that is sending the frame.
- **Format:** 6 bytes (48 bits).
- **Example:** `66:77:88:99:AA:BB`.

5. Length / Type (2 bytes)

- **Purpose:** This field has two possible meanings:
  - **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 or equal to 1536, it indicates the type of the higher-layer protocol (such as IP, ARP, etc.).
- **Example:** `0x0800` for IPv4.

6. Data and Padding (46-1500 bytes)

- **Purpose:** This is the actual payload of the frame. It contains the data being transmitted.
- **Size:** The minimum size is 46 bytes, and the maximum size is 1500 bytes. If the data is less than 46 bytes, padding is added to meet the minimum size.
- **Function:** Carries the upper-layer data (such as IP packets).

7. Frame Check Sequence (FCS) (4 bytes)

- **Purpose:** The FCS is used for error detection. It contains a cyclic redundancy check (CRC) value to ensure data integrity.
- **Function:** The receiver calculates the CRC and compares it with the FCS value. If they don't match, the frame is discarded.