USN No. | | | | | | | | | | |

Internal Assessment Test 1 – Nov 2024

Sub:	Computer Networks					Sub Code:	BCS502	Branch:	ISE	
Date:	06/11/2024	Duration:	90 min's	Max Marks:	50	Sec	V/A, B, C			OBE

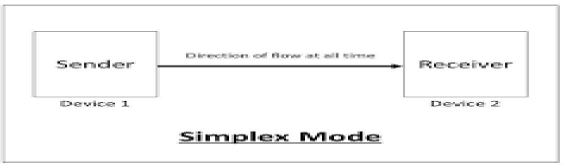
	Answer any FIVE FULL QUESTIONS	MARKS	CO	RBT
1 (a)	Describe the three modes of data flow and provide real-world examples where each mode is used.	[5]	CO1	L1

Explanation: -2 Marks
Diagram: - 2 Marks
Example: -1 Marks

The three modes of data flow are *simplex*, *half-duplex*, and *full-duplex*. Each mode defines the direction in which data can travel between devices. Here's a breakdown of each mode, with real-world examples:

1. Simplex Mode

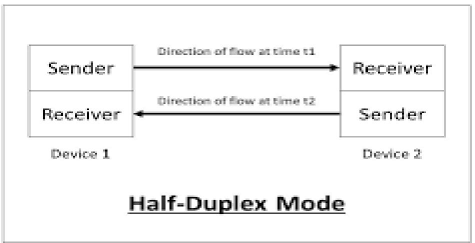
In *simplex* mode, data flows in only one direction. One device is the transmitter, and the other is the receiver, with no role reversal possible.



- **Example:**
  - Keyboard to Computer: The keyboard sends data (key presses) to the computer, but data does not flow back to the keyboard.
  - Radio Broadcasting: A radio station transmits signals to radios, but the radios cannot send any data back to the station.

2. Half-Duplex Mode

In *half-duplex* mode, data can flow in both directions, but not simultaneously. Devices take turns to send and receive data.

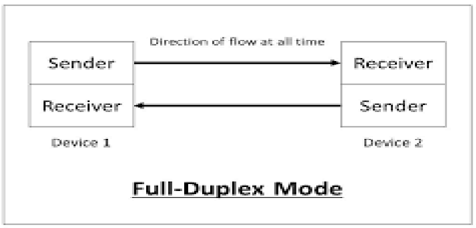


- **Example:**
  - Walkie-Talkies: In walkie-talkies, only one person can speak at a time. When one user speaks, the other listens, and vice versa, but they cannot both speak at once.

- Two-Way Radio Systems: Many police and emergency radios use half-duplex communication, allowing officers to communicate in turns.

3. Full-Duplex Mode

In *full-duplex* mode, data can flow in both directions simultaneously, allowing both devices to send and receive data at the same time.



- **Example:**
  - Telephone Calls: In a phone conversation, both parties can speak and listen simultaneously.
  - Internet Browsing: When you browse the web, your device can send requests to the server and receive responses at the same time, enabling smooth, real-time data exchange.

Each mode of data flow has specific use cases based on the communication needs, with *simplex* suited for one-way communication, *half-duplex* for controlled two-way communication, and *full-duplex* for continuous two-way communication.

		Marks	CO	Level
(b)	Define framing and give the reason it is needed.	[5]	CO1	L2

Definition: - 1 Marks
Diagram & Explanation: - 2 Marks
Reason: - 2 Marks

Framing is a technique used in data communication and networking to structure and organize data for transmission over a network. It involves dividing the stream of data into manageable, distinct units called **frames**. Each frame typically contains not only the actual data being transmitted but also additional information such as headers and trailers that help manage the transmission process.

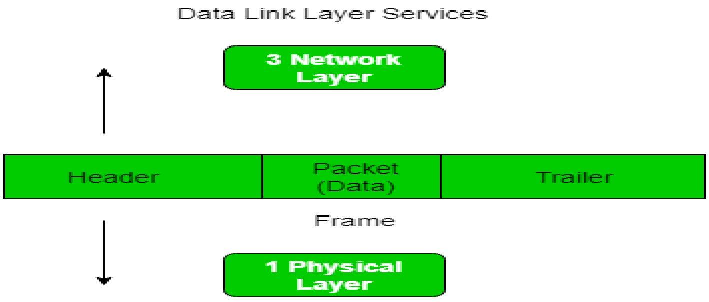
Key Components of a Frame

1. **Header**: This section usually contains control information, such as source and destination addresses, frame type, sequence number, and error-checking data.
2. **Payload**: This is the actual data being transmitted in the frame. It is the content that the sender wants to communicate to the receiver.
3. **Trailer**: This part often contains error detection codes (like CRC) to verify the integrity of the data and may also include other control information.

Reasons for Framing

1. **Data Organization**: Framing helps organize data into manageable pieces, making it easier to handle during transmission and processing. By structuring data into frames, the communication system can keep track of which segments belong to which messages.

2. **Error Detection**: Each frame can include error detection and correction information. This allows the receiving end to identify and correct errors that may have occurred during transmission, enhancing data integrity.
3. **Synchronization**: Framing provides a means to synchronize the sender and receiver. Frames indicate the beginning and end of each data packet, allowing the receiver to know when to start and stop reading the incoming data stream.
4. **Flow Control**: Framing can facilitate flow control mechanisms. By segmenting data into frames, systems can regulate the pace at which data is sent and processed, preventing overload and ensuring that the receiver can handle the incoming data efficiently.
5. **Multiplexing**: In networks with multiple data streams, framing helps in identifying and separating these streams. This allows different types of data to be sent over the same channel without confusion.
6. **Facilitating Protocols**: Different protocols (like TCP/IP, Ethernet) define specific framing methods that allow interoperability among various network devices and ensure proper communication.



Q. No.	Question	Marks	CO	Level
2 (a)	Given the dataword 101001111 and the divisor 10111, Generate the CRC codeword at the sender site (using binary division).	[5]	CO2	L3

Appending Zeros: - 1 Marks
Division operation: - 2 Marks
Check Sum: -1 Marks
Result: - 1 Marks

To generate the CRC codeword, we'll perform binary division on the dataword using the divisor. The steps are as follows:

Step 1: Append Zeros to the Dataword

The divisor has 5 bits, so we append 4 zeros (5 - 1 = 4) to the dataword. This gives us:

1010011110000101001111000010100111110000

Step 2: Perform Binary Division

We divide the modified dataword by the divisor using XOR for each step. The process continues until we reach the last bit of the dataword + zeros.

1. **Initial Step**: Take the first 5 bits, 101001010010100, which is less than the divisor, so we move to the first 6 bits: 101001101001101001.

2. **Binary Division**:

- 101001÷10111101001 ₩div 10111101001÷10111: XOR 101001 with 10111
  101001⊕10111=01110101001 ₩oplus 10111 = 01110101001⊕10111=01110
  Bring down the next bit from the dataword, forming 111001110011100.
- 11100÷1011111100 ₩div 1011111100÷10111: XOR 11100 with 10111
  11100⊕10111=0101111100 ₩oplus 10111 = 0101111100⊕10111=01011
  Bring down the next bit, forming 101101011010110.
- 10110÷1011110110 ₩div 1011110110÷10111: XOR 10110 with 10111
  10110⊕10111=0000110110 ₩oplus 10111 = 0000110110⊕10111=00001
  Bring down the next bit, forming 000110001100011.
- 00011÷1011100011 \div 1011100011÷10111: Since 000110001100011 is smaller than 101111011110111, bring down the next bit to make it 001110011100111.
- 00111÷1011100111 \div 1011100111÷10111: Still smaller, so bring down the next bit, forming 011100111001110.
- 01110÷1011101110 ₩div 1011101110÷10111: XOR 01110 with 10111
  01110⊕10111=1100101110 ₩oplus 10111 = 1100101110⊕10111=11001
  Bring down the last bit, forming 100101001010010.
- 10010÷1011110010 ₩div 1011110010÷10111: XOR 10010 with 10111
  10010⊕10111=0010110010 ₩oplus 10111 = 0010110010⊕10111=00101

Step 3: Result (Remainder)

The final remainder after all divisions is 010101010101.

Step 4: Generate the Codeword

Append the remainder to the original dataword (before appending zeros):

Dataword: 101001111\text {Dataword: } 101001111Dataword: 101001111 Remainder: 0101\text{Remainder: } 0101Remainder: 0101 CRC Codeword: 1010011110101\text{CRC Codeword: } 1010011110101CRC Codeword: 1010011110101

Final Answer

The CRC codeword generated at the sender site is:

1010011110101

(b)	Explain the layered architecture of the TCP/IP protocol suite. How does each layer contribute to overall network communication?	[5]	CO2	L2

Explanation & Diagram: - 3 Marks
Approaches: - 2 Marks

The TCP/IP protocol suite is a layered architecture that organizes network communication into a stack of four layers: **Application**, **Transport**, **Internet**, and **Network Access**. Each layer has specific functions and protocols, contributing to reliable and efficient communication across networks. Here's an overview of each layer and its role:

1. Application Layer

The **Application Layer** is the topmost layer in the TCP/IP model, providing protocols that enable applications to communicate over the network. This layer is responsible for user-facing functions like data formatting, message creation, and process-to-process communication.

- **Key Protocols**:
  - **HTTP/HTTPS**: For web browsing.
  - **SMTP**: For email exchange.
  - **FTP**: For file transfer.
  - **DNS**: For resolving domain names to IP addresses.
- **Contribution**: This layer enables applications to access network services and defines communication rules for end-user processes. It supports direct interaction with users, handling their data requests and presenting responses.

2. Transport Layer

The **Transport Layer** provides reliable, end-to-end communication between devices. It manages data segmentation, flow control, and error correction, ensuring data integrity and proper sequencing during transmission.

- **Key Protocols**:
  - **TCP (Transmission Control Protocol)**: A connection-oriented protocol that provides reliable, ordered delivery of data with mechanisms for error checking and recovery.
  - **UDP (User Datagram Protocol)**: A connectionless protocol that offers faster data delivery without reliability guarantees, suitable for real-time applications.
- **Contribution**: This layer ensures that data is delivered accurately and in the correct order, either with guaranteed delivery (TCP) or with minimal delay (UDP), depending on application requirements.

3. Internet Layer

The **Internet Layer** is responsible for logical addressing, routing, and path determination across network boundaries. It packages data into packets and determines the best path to the destination across interconnected networks.

- **Key Protocols**:
  - **IP (Internet Protocol)**: Provides addressing and routing, ensuring that packets reach the correct destination.

- ICMP (Internet Control Message Protocol): Used for error reporting and network diagnostics (e.g., ping).
    - **ARP (Address Resolution Protocol)**: Maps IP addresses to physical MAC addresses within a local network.
- **Contribution**: This layer facilitates data movement across diverse networks, enabling inter-network communication through IP addresses and routing mechanisms.

4. Network Access Layer (or Link Layer)

The **Network Access Layer** defines the protocols for physically transmitting data over network hardware, including how data is formatted for transmission on specific media (e.g., Ethernet, Wi-Fi) and how frames are transmitted and received on the local link.

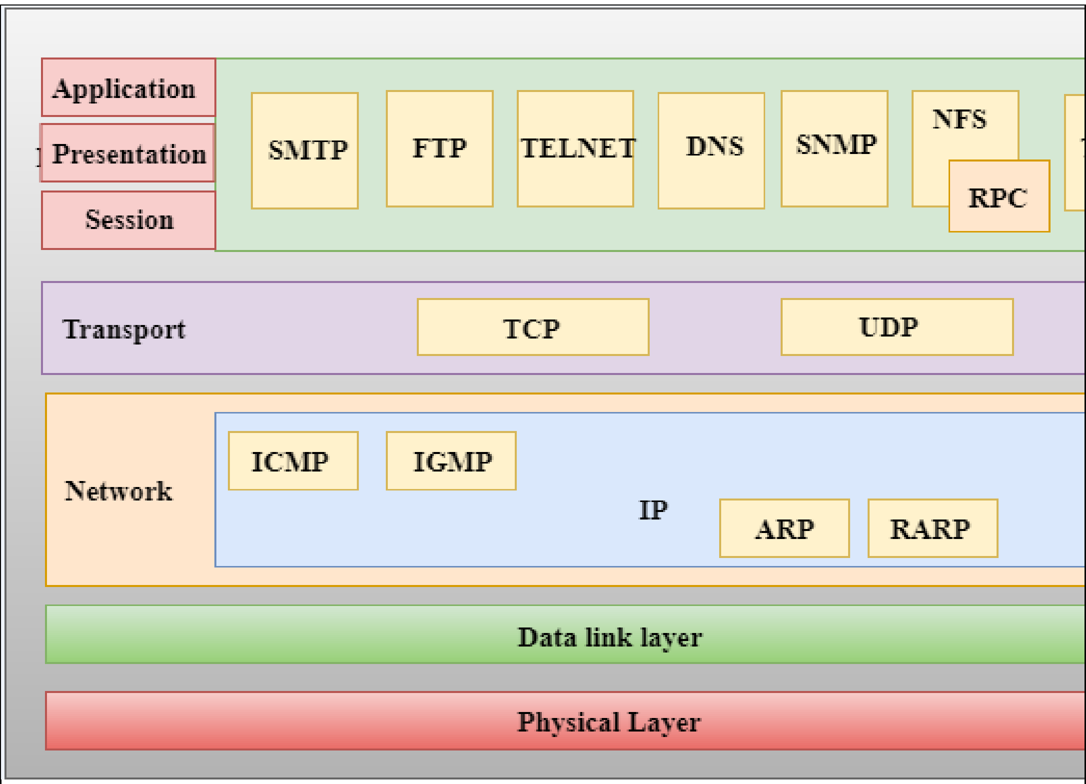
- **Key Protocols**:
    - **Ethernet**: A widely-used protocol for local area network (LAN) communication.
    - **Wi-Fi**: A wireless protocol for local area networks.
    - **PPP (Point-to-Point Protocol)**: Often used for direct communication between two devices (e.g., over a modem).
- **Contribution**: This layer provides the means to physically send and receive data frames over the local network, translating data into signals that can travel through various media like cables or radio waves.

How Each Layer Contributes to Overall Network Communication

Each layer in the TCP/IP model has a specific role in end-to-end communication:

- **Application Layer**: Directly interfaces with users and applications, translating user requests into data for network transport.
- **Transport Layer**: Manages reliable (or fast, best-effort) data transfer between devices, ensuring error recovery and proper sequencing.
- **Internet Layer**: Facilitates logical addressing and routing, allowing data to be routed across networks toward its destination.
- **Network Access Layer**: Handles the physical transmission of data on the local network, allowing data packets to travel between devices.

By separating communication tasks into these layers, the TCP/IP model achieves modularity, enabling flexibility and interoperability across different networks and devices, making global networking scalable and efficient.



3 (a)	Discuss the advantages and disadvantages of virtual-circuit networks compared to datagram networks. Include aspects such as connection setup, resource allocation, and data transfer efficiency.	[5]	CO2	L2

Advantages: - 2.5 Marks
Disadvantages: - 2.5 Marks

Virtual-circuit networks and datagram networks are two fundamental approaches to packet-switched networking, each with distinct advantages and disadvantages. Let's compare them in terms of **connection setup**, **resource allocation**, **data transfer efficiency**, and other aspects.

1. Connection Setup

- **Virtual-Circuit Networks**:
    - **Advantage**: Virtual-circuit networks require a connection setup phase before data transfer begins. This setup reserves a path through the network, ensuring that all packets for a connection follow the same route. This consistent path can simplify error recovery and ensure a predictable route, benefiting applications that need stable connections (e.g., voice calls, video conferencing).
    - **Disadvantage**: The connection setup phase introduces an initial delay, which may be inefficient for short data transfers where the setup time is significant compared to the transmission time.
- **Datagram Networks**:
    - **Advantage**: Datagram networks do not require a setup phase; each packet (or datagram) is sent independently, allowing for immediate data transfer.

This setup-free approach benefits applications that require fast, ad-hoc communication, like DNS queries or bursty data transfers.
    - **Disadvantage**: Since there is no pre-established route, each packet may take a different path to the destination, leading to possible reordering of packets. Applications sensitive to packet order might need additional mechanisms to reorder packets upon arrival.

2. Resource Allocation

- **Virtual-Circuit Networks**:
    - **Advantage**: Resources (e.g., bandwidth, buffers) are often reserved along the path during connection setup. This reservation provides a level of guaranteed quality of service (QoS), making it suitable for real-time applications requiring steady throughput and minimal delay.
    - **Disadvantage**: Resource reservation can lead to inefficient use of network capacity, especially if a connection remains idle or underutilized, as resources are dedicated exclusively to each virtual circuit.
- **Datagram Networks**:
    - **Advantage**: Datagram networks do not reserve resources in advance, which allows for more flexible and dynamic use of network resources. This approach can improve efficiency as network capacity is shared among all users, especially in bursty traffic scenarios where full resource reservation isn't needed.
    - **Disadvantage**: The lack of resource reservation can lead to congestion and variability in network performance. Without dedicated resources, packets may experience delays, especially under heavy traffic, which can be problematic for time-sensitive applications.

3. Data Transfer Efficiency

- **Virtual-Circuit Networks**:
    - **Advantage**: Once the connection is established, data transfer in virtual-circuit networks can be more efficient, as packets follow a predictable, optimized path. Intermediate routers don't need to make routing decisions for each packet, reducing overhead and increasing transfer efficiency.
    - **Disadvantage**: The initial setup time and dedicated resources can reduce overall efficiency, especially for applications with minimal data to send. Virtual circuits can also be less adaptive to changing network conditions, as they rely on a predetermined path.
- **Datagram Networks**:
    - **Advantage**: Datagram networks allow each packet to be routed individually, which can adapt to changes in network conditions (e.g., rerouting packets around a failure or congestion point). This flexibility can optimize data transfer efficiency, especially in complex or dynamic networks.
    - **Disadvantage**: Efficiency may decrease if packets arrive out of order or are lost, requiring additional processing (e.g., reordering or retransmitting packets) at the receiving end. This overhead can affect overall transfer efficiency, particularly for large data transfers that rely on packet ordering.

4. Reliability and Error Handling

- **Virtual-Circuit Networks**:
  - **Advantage**: Because all packets follow the same path, virtual-circuit networks can provide consistent service and simplify error handling. Any network issues can be isolated to a particular path, making it easier to detect and address errors.
  - **Disadvantage**: If a failure occurs along the pre-established path, the entire virtual circuit may be disrupted, requiring a new connection setup. This dependency on a fixed path can reduce resilience in some cases.
- **Datagram Networks**:
  - **Advantage**: Datagram networks are more resilient to failures, as each packet is routed independently. If a network failure occurs, packets can be dynamically rerouted to avoid the problem, improving network robustness.
  - **Disadvantage**: Error handling can be more complex because each packet may take a different path, and packet loss, duplication, or reordering may occur more frequently. Applications may need additional protocols (like TCP) for error recovery and reliable communication.

Summary Table

Aspect	Virtual-Circuit Networks	Datagram Netw
Connection Setup	Requires initial setup, good for long sessions	No setup, suitable for imr short-lived transfers
Resource Allocation	Dedicated resources per connection, supports QoS	Shared resources, more fl less predictable QoS
Data Transfer Efficiency	Efficient for established connections, predictable path	Flexible and adaptive to r conditions
Reliability	Consistent path, easier error handling	Dynamic routing, resilien but may need reordering
Typical Use Cases	Voice, video, and other real-time applications	Web browsing, DNS, em bursty applications

Choosing Between Virtual-Circuit and Datagram Networks

The choice between virtual-circuit and datagram networks depends on the specific needs of an application or network. Virtual-circuit networks are well-suited for applications

	requiring high reliability, consistent paths, and QoS guarantees, while datagram networks offer flexibility, adaptability, and efficiency for diverse, non-sequential, or short-lived communications.			
(b)	Compare HDLC with PPP.	[5]	CO2	L2

Explanation: -1*5=5 Marks

High-Level Data Link Control (HDLC) and **Point-to-Point Protocol (PPP)** are both widely used data link layer protocols for encapsulating and transmitting data over point-to-point connections. However, they have distinct features, making them suitable for different use cases. Let's compare and contrast HDLC and PPP across various aspects.

1. Protocol Type and Standardization

- **HDLC**:
  - **Type**: HDLC is a bit-oriented protocol standardized by the International Organization for Standardization (ISO).
  - **Usage**: It's a generic link layer protocol and serves as the basis for many other protocols, including proprietary versions by manufacturers (e.g., Cisco HDLC).
  - **Standardization**: HDLC is ISO standardized (ISO 3309 and ISO 4335) and was originally designed for synchronous communication.
- **PPP**:
  - **Type**: PPP is a byte-oriented protocol developed specifically for point-to-point connections and standardized by the Internet Engineering Task Force (IETF).
  - **Usage**: Primarily used for serial point-to-point connections (e.g., dial-up, DSL) and is highly suitable for IP data transmission over different physical media.
  - **Standardization**: PPP is standardized by IETF in RFC 1661

2. Frame Structure

- **HDLC**:
  - **Frame Format**: HDLC uses a consistent frame structure that includes **Flag, Address, Control, Payload, and Frame Check Sequence (FCS)** fields.
  - **Flag Field**: The frame begins and ends with a unique flag sequence (`01111110`) to delimit frames and detect frame boundaries.
  - **Address and Control Fields**: The Address field specifies the destination address (useful in multi-point configurations), while the Control field manages flow and error control.
- **PPP**:
  - **Frame Format**: PPP also has a frame structure, but it includes **Flag, Address, Control, Protocol, Payload, and FCS** fields.
  - **Flag Field**: Similar to HDLC, PPP frames are also delimited with a flag (`01111110`).
  - **Protocol Field**: The Protocol field is unique to PPP and identifies the payload type (e.g., IP, IPv6, etc.), allowing PPP to support multiple protocols over the same connection.

3. Error Detection and Correction

- **HDLC**:
  - **Error Detection**: HDLC uses a Frame Check Sequence (FCS) for error detection. Errors detected are usually handled by retransmission or by higher-level protocols.
  - **Error Correction**: HDLC does not inherently handle error correction; it relies on retransmission if errors are detected.
- **PPP**:
  - **Error Detection**: PPP also uses an FCS field to check for errors within each frame.
  - **Error Correction**: Similar to HDLC, PPP does not perform error correction directly but can request retransmission if errors are found. Additionally, PPP's multi-protocol support allows it to work with higher-layer protocols that handle error correction.

4. Link Establishment and Configuration

- **HDLC**:
  - **Configuration**: HDLC does not have any built-in mechanisms for link setup, authentication, or configuration. It's purely a data encapsulation protocol and requires additional support for session establishment and maintenance.
  - **Authentication**: Authentication is not supported directly in standard HDLC.
- **PPP**:
  - **Link Control Protocol (LCP)**: PPP includes an LCP, which enables link establishment, maintenance, and termination. LCP also negotiates configuration options and establishes parameters (e.g., frame size, compression).
  - **Authentication**: PPP supports authentication through optional protocols such as **PAP (Password Authentication Protocol)** and **CHAP (Challenge Handshake Authentication Protocol)**, making it suitable for secure connections over public networks.

5. Multiprotocol Support

- **HDLC**:
  - **Protocol Multiplexing**: Standard HDLC does not include support for multiple protocols within a single connection. Each connection is typically dedicated to one protocol, which limits flexibility.
  - **Vendor-Specific Extensions**: Some proprietary versions of HDLC (e.g., Cisco HDLC) add a protocol field for multiplexing, but this is not part of the standard HDLC protocol.
- **PPP**:
  - **Protocol Multiplexing**: PPP's Protocol field allows for the multiplexing of multiple protocols over a single point-to-point link, supporting protocols like IP, IPv6, AppleTalk, and IPX simultaneously.
  - **Flexibility**: PPP's built-in support for multiple network layer protocols makes it highly versatile and well-suited for modern, multi-protocol environments.

6. Applications and Use Cases

- **HDLC**:
  - **Use Cases**: HDLC is commonly used in leased-line point-to-point connections, typically in private networks and for synchronous data links in telecommunications.
  - **Limitations**: The lack of authentication and protocol multiplexing in standard HDLC limits its application for secure or public internet connections.
- **PPP**:
  - **Use Cases**: PPP is widely used for Internet access over dial-up, DSL, and broadband connections. It's also used in VPNs and WANs due to its flexibility, authentication support, and multi-protocol capability.
  - **Popularity**: PPP's robust feature set for link configuration, authentication, and multi-protocol support makes it highly popular for connecting to the internet over various media.

Summary Table

Feature	HDLC	PPP
Type	Bit-oriented, ISO standard	Byte-oriented, IETF st
Frame Structure	Flag, Address, Control, Payload, FCS	Flag, Address, Contro Payload, FCS
Error Detection	FCS-based detection, no error correction	FCS-based detection correction
Link Establishment	No built-in link setup or maintenance	LCP for link setup, m and termination
Authentication	Not supported in standard HDLC	PAP and CHAP au options
Multiprotocol Support	Limited (only with vendor-specific extensions)	Supports multiple pr IPv6, etc.)
Common Use Cases	Private point-to-point leased lines, synchronous links	Internet connections DSL), VPNs, WANs

4 (a)	Compare a Local Area Network (LAN) and a Wide Area Network (WAN) in terms of characteristics, speed, and geographical coverage.	[5]	CO1	L2

Explanation: - 1*5=5 Marks

Local Area Networks (LANs) and Wide Area Networks (WANs) are two types of networks that connect devices, but they differ significantly in terms of **characteristics**, **speed**, and **geographical coverage**. Here's a detailed comparison:

1. Characteristics

- **LAN**:
  - **Definition**: A LAN is a network that connects devices within a limited area, such as a home, school, or office building. It is typically owned and managed by a single organization or individual.
  - **Architecture**: LANs are often built using Ethernet or Wi-Fi and involve devices like routers, switches, and access points.
  - **Control and Management**: LANs are typically managed by an organization's IT staff, giving them full control over network resources, security, and bandwidth allocation.
- **WAN**:
  - **Definition**: A WAN covers a much larger geographical area, connecting multiple LANs and other networks over a long distance (e.g., cities, countries, or even continents). WANs can be either private or public networks, often using telecommunication infrastructure.
  - **Architecture**: WANs utilize various technologies, including leased lines, satellite links, MPLS, and the public internet. They may also involve WAN-specific routers and high-capacity backbone networks.
  - **Control and Management**: WANs are often managed by Internet Service Providers (ISPs) or telecom companies. Organizations typically lease WAN connections and rely on the service provider for network management and maintenance.

2. Speed

- **LAN**:
  - **Speed Range**: LANs typically offer high speeds, ranging from 100 Mbps to 10 Gbps or more, due to the use of fast, local transmission mediums like Ethernet and modern fiber optics.
  - **Latency**: LANs generally have very low latency due to their limited size and direct connections, making them suitable for real-time applications such as video conferencing, gaming, and VoIP.
- **WAN**:

- **Speed Range**: WAN speeds are generally lower than LANs, often ranging from 1 Mbps to several hundred Mbps, depending on the technology used (e.g., DSL, fiber, satellite). However, advanced WAN technologies (like fiber backbones) can provide speeds comparable to LANs in certain areas.
- **Latency**: WANs usually experience higher latency due to the greater distances and more complex routing involved. Factors like routing hops, network congestion, and transmission mediums (e.g., satellite) can further increase delay.

3. Geographical Coverage

- **LAN**:
  - **Coverage Area**: LANs have a limited geographical range, usually covering a single building, campus, or a small group of buildings within a localized area. The maximum range is often within a few kilometers at most.
  - **Scalability**: LANs are generally easier to expand within the existing infrastructure, although they are not designed to connect widely dispersed locations.
- **WAN**:
  - **Coverage Area**: WANs cover a broad geographical area, ranging from cities and regions to entire countries and continents. They are designed to connect LANs or other networks across large distances.
  - **Scalability**: WANs are highly scalable, allowing organizations to connect multiple locations worldwide, although expansion usually requires additional costs and coordination with service providers.

4. Cost

- **LAN**:
  - **Cost**: LANs are relatively cost-effective to establish and maintain within a confined area. The primary costs involve purchasing equipment (like routers, switches, and cables) and handling maintenance internally.
  - **Expense Level**: LAN expenses are generally lower due to the limited range and control over internal resources.
- **WAN**:
  - **Cost**: WANs are more expensive to set up and maintain, especially when using leased lines or dedicated connections over long distances. Costs often include monthly fees to ISPs, equipment, and sometimes additional security measures.
  - **Expense Level**: WANs typically require substantial investment, as they rely on third-party providers for infrastructure, which is billed on a subscription or lease basis.

5. Security

- **LAN**:
  - **Security Level**: LANs are usually more secure due to physical control and management by the organization’s IT department. Administrators can set access restrictions and configure firewalls within a controlled environment.
  - **Common Threats**: LAN security is primarily threatened by internal attacks or unauthorized access within the local network. Encryption and strict access controls can mitigate these risks.
- **WAN**:
  - **Security Level**: WANs require more robust security measures due to exposure to external networks (like the internet) and reliance on third-party providers. Encryption, VPNs, and firewalls are commonly used to protect WAN communications.
  - **Common Threats**: WANs are vulnerable to a wider range of threats, including cyber-attacks, eavesdropping, and data breaches, especially over public networks. Organizations must work closely with providers to implement comprehensive security.

Summary Table

Feature	LAN (Local Area Network)	WAN (Wide Are
Characteristics	Limited to a single organization, local area	Connects multiple L cities, countries, or c
Speed	High speeds (100 Mbps to 10 Gbps), low latency	Lower speeds (1 Mb hundreds of Mbps),
Geographical Coverage	Covers a small area (e.g., building, campus)	Covers large areas (c countries, globally)
Cost	Low setup and maintenance costs, within organization control	High costs, requires or ISP services
Security	Easier to secure internally, less exposure to external threats	Higher security risks encryption and VPN

Typical Use Cases	Office or home networks, schools, small businesses	Multi-site organizati global corporations

(b) Distinguish between a point-to-point link and a broadcast link. [5] CO1 L2

Explanation: - 1*5=5 Marks

Point-to-point links and **broadcast links** are two types of data link layer connections used in networking, differing primarily in how they connect devices and how data is transmitted between them. Here's a comparison of these two link types:

1. Definition and Structure

- **Point-to-Point Link**:
  - A point-to-point link directly connects two devices, such as two computers or a computer and a router.
  - This link type is usually represented by a single, dedicated physical or logical connection between the two devices.
  - Examples include wired connections like DSL, fiber optic links, and direct Ethernet connections.
- **Broadcast Link**:
  - A broadcast link connects multiple devices in a shared network medium, allowing data sent by one device to be received by all other devices on the same network.
  - It enables one-to-many communication by "broadcasting" messages across the entire network segment.
  - Examples include traditional Ethernet LANs (using a hub or a switch in broadcast mode) and wireless networks, where multiple devices share the same communication channel.

2. Communication Scope

- **Point-to-Point Link**:
  - Communication occurs only between the two connected devices. No other devices can directly access or intercept the communication unless they are on the same link.
  - There is no need for an addressing scheme to identify multiple recipients, as each frame has a single sender and a single receiver.
- **Broadcast Link**:
  - Communication can reach multiple devices simultaneously. Any device on the broadcast link can send data that all other devices on the same network segment can receive.
  - A **MAC (Media Access Control) address** is typically used in broadcast networks to help devices identify which frames are intended for them, either by direct addressing or broadcast addressing (e.g., Ethernet's broadcast address `FF:FF:FF:FF:FF:FF`).

3. Transmission and Efficiency

- **Point-to-Point Link**:
  - The dedicated nature of a point-to-point link allows for efficient use of the medium, as there is no sharing with other devices. This leads to minimal congestion and low latency.
  - There is typically no risk of collisions (data frames interfering with each other), as only two devices share the connection.
- **Broadcast Link**:
  - In a broadcast link, devices share the same medium, which can lead to congestion or collisions when multiple devices attempt to transmit simultaneously.
  - To avoid collisions, broadcast networks often use protocols like **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** in Ethernet networks or **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** in Wi-Fi networks.

4. Scalability and Use Cases

- **Point-to-Point Link**:
  - Point-to-point links are relatively simple and easy to set up but are limited in scalability since each connection serves only two devices.
  - They are suitable for dedicated connections, such as those between network routers or devices requiring a stable, uninterrupted link (e.g., leased lines, serial links).
- **Broadcast Link**:
  - Broadcast links are inherently more scalable, allowing multiple devices to be added to the same network segment without creating additional connections.
  - Common in Local Area Networks (LANs), especially for environments like office networks or wireless networks where multiple devices need to communicate and share resources.

5. Security

- **Point-to-Point Link**:
  - Generally more secure since data only flows between two devices, making it less susceptible to interception from other network devices.
  - Security measures are simpler, as there is no need to protect against unauthorized devices on the same link.
- **Broadcast Link**:
  - More vulnerable to security risks because all devices on the broadcast link can receive transmissions intended for others, making eavesdropping a concern.
  - Security measures, such as encryption and access control, are necessary to prevent unauthorized access and ensure that sensitive data is not intercepted

Summary Table

Feature	Point-to-Point Link	Broadcast
Connection Type	Direct link between two devices	Shared link among m devices
Communication Scope	One-to-one communication	One-to-many commu
Transmission Efficiency	Efficient, low latency, no collisions	Potential for congesti collision avoidance
Scalability	Limited to two devices	Scalable, multiple de the same link
Security	High, as only two devices communicate	Lower, requires addi measures to secure d
Common Examples	DSL, fiber optic links, leased lines, serial links	Ethernet LANs, Wi-F hub-based networks

5(a) What is a datagram network? Describe its key characteristics and how it handles packet routing and delivery. [5] CO2 L1

Definition: - 1 Marks
Characteristics: -2 Marks
Explanation: -2 Marks

A **datagram network** is a type of packet-switched network in which data is transmitted in independent units called **datagrams**. Each datagram is treated as a separate, self-contained packet with its own addressing information, allowing it to traverse the network independently of other packets. Datagram networks are used extensively in networks like the **Internet**, where the Internet Protocol (IP) routes data across interconnected networks.

Key Characteristics of Datagram Networks

1. **Connectionless Communication**:

- A datagram network is **connectionless**, meaning that there is no need to establish a dedicated connection or path before sending data. Each packet is sent independently and is routed based solely on the destination address.
    - This lack of a connection setup phase allows for fast and flexible communication, suitable for applications like web browsing, email, and streaming.
2. **Independent Packet Routing**:
    - Each datagram contains all the information needed for routing, such as the source and destination addresses, and is routed individually.
    - Since each packet is independent, different packets from the same message may take different routes to reach the destination, depending on network conditions.
3. **No Guaranteed Delivery**:
    - Datagram networks do not inherently guarantee that all packets will arrive at the destination or that they will arrive in the correct order.
    - Packets may be lost, duplicated, or arrive out of order due to dynamic routing and varying network conditions.
    - Reliability and sequencing must be managed by higher-level protocols, such as TCP, if needed by the application.
4. **Scalability and Efficiency**:
    - The connectionless nature of datagram networks allows for efficient use of network resources, making it highly scalable and adaptable to changing traffic loads.
    - Datagram networks are flexible in handling variable data rates, allowing devices to send data whenever needed without reserving network resources in advance.

Packet Routing and Delivery in a Datagram Network

Datagram networks use **dynamic routing algorithms** to forward packets to their destinations. Here's how packet routing and delivery typically work in such networks:

1. **Addressing and Forwarding**:
    - Each datagram includes a **destination address** that routers use to determine the packet's next hop. Routers do not keep state information for each connection; instead, they examine each packet independently.
    - Upon receiving a datagram, a router reads the destination address, consults its **routing table**, and forwards the packet to the appropriate next hop toward its destination.
2. **Dynamic Routing**:
    - Datagram networks often use dynamic routing protocols (e.g., **OSPF**, **BGP**) that allow routers to adapt to changes in network topology, congestion, or link failures.
    - Routing protocols periodically update routing tables, enabling packets to be rerouted as network conditions change. This flexibility allows for alternate paths in case of link failures but can also lead to packets from the same source taking different routes.
3. **Handling Packet Loss and Errors**:
    - Since datagram networks do not guarantee packet delivery, packets may be dropped if a router's buffer is full or if a transmission error occurs.

- Higher-layer protocols, like TCP, can request retransmission of lost packets or reorder packets to ensure reliable, in-sequence delivery. However, if an application uses the User Datagram Protocol (UDP), packet loss is not managed by the transport layer, making it suitable for real-time applications like streaming, where occasional packet loss is acceptable.

4. **Lack of Congestion Control**:
    - In a datagram network, there is no built-in mechanism for controlling congestion at the network level. However, modern network protocols, such as TCP, include flow and congestion control mechanisms to manage data flow between endpoints.
    - This approach allows applications to manage their own flow and ensures that datagram networks remain efficient by adapting to congestion at the endpoints rather than across the network.

Advantages and Disadvantages of Datagram Networks

Advantages:

- **Flexibility and Scalability**: Datagram networks can easily accommodate a large number of devices and adapt to changes in network topology and traffic.
- **Efficiency**: No resources are reserved in advance, allowing efficient bandwidth use.
- **Resilience**: Dynamic routing enables packets to be rerouted around network failures, improving network robustness.

Disadvantages:

- **Unreliable Delivery**: Datagram networks do not guarantee packet delivery, order, or reliability, making it necessary to rely on higher-layer protocols for these functions.
- **Variable Latency**: Packets may experience different delays if they follow different paths, resulting in jitter for real-time applications.
- **Increased Overhead for Reliability**: Applications that need reliable delivery may experience additional overhead from retransmissions and acknowledgments.

(b)	What is the Hamming distance for each of the following codewords?	[5]	CO2	L3

a) d (10000, 00000)
b) d (10101, 10000)
c) d (00000, 11111)
d) d (00000, 00000)

Explanation: - 1 Marks
Problem: - 1*4=4 Marks

The **Hamming distance** between two codewords is the number of bit positions in which the corresponding bits differ. Let's calculate the Hamming distance for each pair of codewords:

1. **d(10000,00000)d(10000, 00000)d(10000,00000)**
    - Compare each bit position:

	■ 1 ≠ 0 ■ 0 = 0 ■ 0 = 0 ■ 0 = 0 ■ 0 = 0 ○ **Hamming distance** = 1 (only one bit differs) 2. **d(10101,10000)d(10101, 10000)d(10101,10000)** ○ Compare each bit position: ■ 1 = 1 ■ 0 ≠ 1 ■ 1 ≠ 0 ■ 0 = 0 ■ 1 ≠ 0 ○ **Hamming distance** = 3 (three bits differ) 3. **d(00000,11111)d(00000, 11111)d(00000,11111)** ○ Compare each bit position: ■ 0 ≠ 1 ■ 0 ≠ 1 ■ 0 ≠ 1 ■ 0 ≠ 1 ■ 0 ≠ 1 ○ **Hamming distance** = 5 (all five bits differ) 4. **d(00000,00000)d(00000, 00000)d(00000,00000)** ○ Compare each bit position: ■ 0 = 0 ■ 0 = 0 ■ 0 = 0 ■ 0 = 0 ■ 0 = 0 ○ **Hamming distance** = 0 (no bits differ) **Summary** ● d(10000,00000)=1d(10000, 00000) = 1d(10000,00000)=1 ● d(10101,10000)=3d(10101, 10000) = 3d(10101,10000)=3 ● d(00000,11111)=5d(00000, 11111) = 5d(00000,11111)=5 ● d(00000,00000)=0d(00000, 00000) = 0d(00000,00000)=0			
6 (a)	In the Stop-and-Wait Protocol, assume that the sender has only one slot in which to keep the frame to send or the copy of the sent frame. What happens if the network layer delivers a packet to the data-link layer at this moment? **Explanation: - 3 Marks** **Approaches: - 2 Marks** In the Stop-and-Wait protocol, the sender can only handle one frame at a time. If the sender is still waiting for an acknowledgment (ACK) for a previously sent frame, its single slot is occupied by the copy of that frame. The sender cannot send a new frame until it receives the ACK for the current frame in the slot.	[5]	CO2	L1

	If the network layer delivers a new packet to the data-link layer while the sender is still waiting for an acknowledgment, the new packet cannot be immediately processed because there is no available slot to store it. In this case, the Stop-and-Wait protocol typically handles the new packet as follows: 1. **Buffering or Discarding the Packet**: The sender may either buffer the packet in a waiting queue or discard it, depending on the specific protocol implementation and resources available. 2. **Waiting for ACK Before Sending**: The sender will wait until it receives the acknowledgment for the current frame. Once the ACK is received, the slot becomes available, and the sender can then store the new packet in the slot, frame it, and send it to the receiver. In Stop-and-Wait, if a new packet arrives while the sender's slot is occupied with an unacknowledged frame, the packet will have to wait until the slot is free. This waiting introduces some delay but maintains the simplicity and reliability of the protocol by ensuring that each frame is acknowledged before moving to the next packet.			

(b)	Explain Media access protocol.
	
	Definition: - 1 Marks
	Types: -3 Marks
	Example: - 1 Marks
	
	Media **Access Protocols** (MAPs) are essential rules and procedures used in networking to control how devices on a shared communication medium (such as a network cable or wireless spectrum) access and transmit data. These protocols are critical in environments where multiple devices may attempt to send data simultaneously, as they help prevent collisions and manage the orderly transmission of data packets.
	
	Key Functions of Media Access Protocols
	
	1. **Channel Access Control**:
	    ○ MAPs determine how devices access the shared medium, ensuring that only one device transmits at any given time (in case of contention) or managing time slots for each device (in case of scheduled access).
	2. **Collision Management**:
	    ○ Protocols handle collisions that occur when two or more devices attempt to send data simultaneously. MAPs define strategies for detecting collisions and resolving them, often by allowing devices to wait before retrying their transmission.
	3. **Fairness**:
	    ○ They aim to provide fair access to the medium for all devices, preventing any single device from monopolizing the bandwidth and ensuring that all devices get a chance to communicate.
	4. **Efficiency**:
	    ○ MAPs strive to optimize the use of the communication medium, maximizing throughput while minimizing delays and collisions.
	
	Types of Media Access Protocols
		[5]	CO2	L2

Media access protocols can be broadly classified into two categories: **contention-based protocols** and **controlled access protocols**.

1. Contention-Based Protocols

These protocols allow devices to compete for the medium and include:

- **Carrier Sense Multiple Access (CSMA)**:
  - Devices sense the channel before transmitting. If the channel is clear, they transmit; if it is busy, they wait.
  - Variants include:
    - **CSMA/CD (Collision Detection)**: Used in wired networks (like Ethernet). Devices listen for collisions during transmission and stop transmitting if a collision is detected, then use a backoff algorithm to retry.
    - **CSMA/CA (Collision Avoidance)**: Used in wireless networks (like Wi-Fi). Devices avoid collisions by waiting a random period before transmitting after detecting the medium is clear.
- **ALOHA**:
  - A simple protocol where devices transmit whenever they have data. If a collision occurs, the devices wait a random time before retrying. It has low efficiency but is easy to implement.

2. Controlled Access Protocols

These protocols impose rules to control how devices can access the medium:

- **Token Ring**:
  - A token circulates around the network. Only the device holding the token can transmit data, ensuring no collisions occur.
- **Polling**:
  - A central controller polls devices to see if they have data to send. Only the polled device is allowed to transmit, preventing collisions.
- **Time Division Multiple Access (TDMA)**:
  - The medium is divided into time slots, and each device is assigned a specific time slot for transmission, ensuring orderly access without collisions.

Applications of Media Access Protocols

- **Local Area Networks (LANs)**: MAPs are crucial in Ethernet and Wi-Fi networks, allowing multiple devices to share the same communication medium.
- **Wireless Networks**: MAPs help manage access in environments with fluctuating channel conditions and varying numbers of devices.
- **Telecommunications**: Protocols like TDMA are used in mobile communication networks to manage user access to the radio spectrum.