USN | | | | | | | | | | |

Internal Assessment Test 1 – November 2024

Sub:	**Computer Networks**					Sub Code:	**BCS502**	Branch:	**AIML**
Date:	**/11/24**	Duration:	**90 minutes**	Max Marks:	**50**	Sem/Sec:	**V**		**OBE**

		Answer any FIVE FULL Questions	**MARKS**	**CO**	**RBT**
1	a	How would you describe the working of Go-Back-N protocol and how it is different from stop and wait protocol?	[10]	2	L2
2	a	Explain TCP/IP protocol suite of computer network with a neat diagram. Also represent the protocols used in each layer of the model.	[10]	1	L2
3	a	How would you compare between guided media and unguided media with examples?	[10]	1	L2
4	a	Write the steps for computing CRC. Find the codeword for the message frame 1101011111 and generator polynomial $G(x)= x^4+x+1$ using CRC.	[10]	2	L3
5	a	With a neat diagram, explain the working of CSMA/CD protocol.	[05]	2	L2
	b	Describe Pure ALOHA & Slotted ALOHA.	[05]	2	L2
6	a	Explain how the differences between IPv4 and IPv6 impact internet connectivity and address management in practical scenarios?	[10]	3	L3

1.a.How would you describe the working of Go-Back-N protocol and how it is different from stop and wait protocol? 5+5

The **Go-Back-N (GBN)** protocol and the **Stop-and-Wait** protocol are both methods of flow control used in data communications, specifically in reliable data transfer. Here's an overview of how each works and the differences between them:

Go-Back-N Protocol

1. **Sliding Window Protocol**: GBN uses a sliding window mechanism where the sender can send multiple frames (packets) before needing an acknowledgment for the first one. The size of the window (N) determines how many frames can be sent without waiting for an acknowledgment.
2. **Frame Transmission**: The sender transmits frames numbered sequentially and keeps a buffer of sent frames that have not yet been acknowledged.
3. **Acknowledgment**: The receiver acknowledges the last frame received in order. If a frame is lost or arrives out of order, the receiver will discard that frame and all subsequent frames. This means the sender must go back and retransmit that frame and all frames sent after it, hence the name "Go-Back-N."
4. **Efficiency**: GBN is more efficient than Stop-and-Wait because it allows for better utilization of the network capacity. Multiple frames can be in transit at the same time, reducing the idle time of the sender.

Stop-and-Wait Protocol

1. **Simple Protocol**: In Stop-and-Wait, the sender transmits a single frame and then waits for an acknowledgment from the receiver before sending the next frame.
2. **Frame Transmission**: The sender sends one frame and stops until it receives an acknowledgment for that frame. If the acknowledgment is not received within a certain timeframe (due to loss or delay), the sender will retransmit the same frame.

3. **Acknowledgment**: Each frame is acknowledged individually. The sender does not send the next frame until it receives confirmation that the previous frame has been received correctly.
4. **Efficiency**: Stop-and-Wait is less efficient than GBN, especially in high-latency environments, because the sender is idle while waiting for an acknowledgment after each frame is sent.

Key Differences

Feature	Go-Back-N Protocol	Stop-and-Wait Protocol
Frame Transmission	Multiple frames can be sent before waiting for acknowledgment.	Only one frame can be sent at a time.
Efficiency	More efficient, better utilization of bandwidth.	Less efficient, more idle time.
Retransmission Mechanism	Retransmits the lost frame and all subsequent frames.	Retransmits only the lost frame.
Window Size	Allows a window of frames (N frames).	Window size is 1 (only one frame).

2.a.Explain TCP/IP protocol suite of computer network with a neat diagram. Also represent the protocols used in each layer of the model. 5+5

The TCP/IP protocol suite, also known as the Internet Protocol Suite, is a set of communication protocols used for the Internet and similar networks. It organizes its protocols into a layered architecture, allowing different protocols to work together seamlessly. The model consists of four layers: Application, Transport, Internet, and Link.

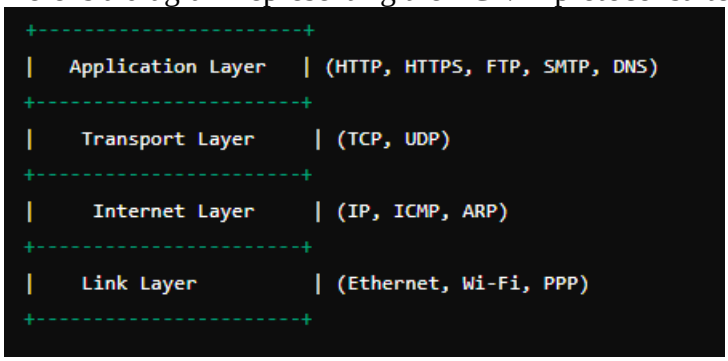
TCP/IP Protocol Suite Layers

1. **Application Layer**:
    - This layer is responsible for providing network services to end-user applications.
    - **Protocols**:
        - **HTTP** (Hypertext Transfer Protocol) - Used for web browsing.
        - **HTTPS** (HTTP Secure) - Secure version of HTTP.
        - **FTP** (File Transfer Protocol) - Used for transferring files.
        - **SMTP** (Simple Mail Transfer Protocol) - Used for email transmission.
        - **DNS** (Domain Name System) - Resolves domain names to IP addresses.
2. **Transport Layer**:
    - This layer is responsible for providing communication services directly to the application layer. It ensures complete data transfer and controls the flow of data.
    - **Protocols**:
        - **TCP** (Transmission Control Protocol) - Provides reliable, connection-oriented communication.
        - **UDP** (User Datagram Protocol) - Provides connectionless communication with minimal overhead.
3. **Internet Layer**:
    - This layer is responsible for addressing, routing, and forwarding packets of data across networks.
    - **Protocols**:

        - **IP** (Internet Protocol) - Responsible for addressing and routing packets (both IPv4 and IPv6).
        - **ICMP** (Internet Control Message Protocol) - Used for error messages and operational queries.
        - **ARP** (Address Resolution Protocol) - Resolves IP addresses to MAC addresses.
4. **Link Layer** (also called the Network Interface Layer):
    - This layer is responsible for the physical transmission of data over the network hardware.
    - **Protocols**:
        - **Ethernet** - Commonly used in wired networks.
        - **Wi-Fi** (IEEE 802.11) - Used in wireless networks.
        - **PPP** (Point-to-Point Protocol) - Used in direct connections between two nodes.

Diagram of the TCP/IP Protocol Suite

Here is a diagram representing the TCP/IP protocol suite:



3.a.How would you compare between guided media and unguided media with examples? 5+5

Guided and unguided media are two primary categories of communication channels used in networking. Here's a comparison between them:

Guided Media

Guided media (also known as wired media) refers to physical pathways that direct the transmission of signals. The signals are contained within a medium, which guides the signal along a specific path.

Characteristics:

- **Physical Connections**: Uses cables or fibers to connect devices.
- **Signal Direction**: The signal follows a predetermined path.
- **Higher Bandwidth**: Typically supports higher data transfer rates.
- **Less Interference**: Less prone to external interference compared to unguided media.

Examples:

1. **Twisted Pair Cable**:
    - Commonly used in telephone and Ethernet networks.
    - Consists of pairs of wires twisted together to reduce electromagnetic interference.
2. **Coaxial Cable**:
    - Used for cable television and broadband Internet.
    - Has a central conductor, insulating layer, and an outer conductive shield to minimize interference.
3. **Fiber Optic Cable**:

- Uses light signals for data transmission.
- Provides high-speed data transfer over long distances with minimal signal loss.

Unguided Media

Unguided media (also known as wireless media) does not require physical connections and transmits data through the air or space. Signals are transmitted as electromagnetic waves, which can travel freely without a defined pathway.

Characteristics:

- **No Physical Medium**: Does not rely on physical connections.
- **Signal Propagation**: Signals spread out in all directions, making them less constrained.
- **Lower Bandwidth**: Generally supports lower data transfer rates compared to guided media.
- **More Interference**: Prone to interference from various sources (e.g., buildings, weather, other electronic devices).

Examples:

1. **Radio Waves**:
   - Used for broadcasting television and radio signals.
   - Supports long-range communication but has limited bandwidth.
2. **Microwaves**:
   - Used for point-to-point communication links, such as in satellite communications.
   - Requires a direct line of sight between transmitting and receiving antennas.
3. **Infrared**:
   - Used for short-range communication, such as remote controls and some wireless data transmission (e.g., IR data transfer between devices).
   - Limited by obstacles and requires a direct line of sight.

Comparison Summary

Feature	Guided Media	Unguided Media
Physical Pathway	Yes (wires, cables, fibers)	No (wireless transmission)
Signal Direction	Directional (follows a specific path)	Omnidirectional (spreads in all directions)
Bandwidth	Generally higher	Generally lower
Interference	Less prone to interference	More prone to interference
Examples	Twisted pair, coaxial, fiber optic	Radio waves, microwaves, infrared

4.a.Write the steps for computing CRC. Find the codeword for the message frame 1101011111 and generator polynomial G(x)= x4+x+1 using CRC. 5+5

Cyclic Redundancy Check (CRC) is a method used to detect errors in data transmission. It involves appending a checksum (or CRC code) to the message, which is computed using polynomial division.

Steps to Compute CRC

1. **Represent the Data and Generator**:
   - Convert the message into a binary string.
   - Convert the generator polynomial G(x)G(x)G(x) into its binary representation.
2. **Append Zeros**:

- Append nnn zeros to the end of the message, where nnn is the degree of the generator polynomial. For G(x)=x4+x+1G(x) = x^4 + x + 1G(x)=x4+x+1, the degree is 4, so append 4 zeros to the message.

3. **Perform Polynomial Division**:
   - Use binary division (XOR operation) to divide the modified message by the generator polynomial. Only consider the leading bits of the dividend that are equal to the degree of the generator.
   - Repeat the process until all bits have been processed.
4. **Obtain the Remainder**:
   - The final result of the division will be a remainder of fewer bits than the generator. This remainder will be the CRC code.
5. **Form the Codeword**:
   - Append the CRC remainder to the original message to create the final codeword.

Example: Compute the Codeword for Message Frame 1101011111110101111111101011111 and Generator Polynomial G(x)=x4+x+1G(x) = x^4 + x + 1G(x)=x4+x+1

Step 1: Represent the Data and Generator

- Message: M=1101011111M = 1101011111M=1101011111
- Generator Polynomial: G(x)=x4+x+1G(x) = x^4 + x + 1G(x)=x4+x+1 (binary representation: 101011010110101)

Step 2: Append Zeros

- Append 4 zeros to the message: M′=1101011111 0000M' = 1101011111 \, 0000M′=11010111110000

Step 3: Perform Polynomial Division

1. **Initial Dividend**: 11010111110000110101111100001101010111110000
2. **Perform Binary Division**:
   - **Step 1**: Divide 110101101011010 by 101011010110101:

Copy code
11010

XOR 10101
01111

- **Step 2**: Bring down the next bit (1):
  01111 XOR 00000 (no XOR here as 10101 can't be divided)
  11110
- **Step 3**: Bring down the next bit (1):
  11110 XOR 10101
  01011
- **Step 4**: Bring down the next bit (1):
  01011 XOR 00000 (no XOR here as 10101 can't be divided)
  10111
- **Step 5**: Bring down the next bit (0):
  10111 XOR 10101
  00010
- **Step 6**: Bring down the next bit (0):
  00010 XOR 00000 (no XOR here as 10101 can't be divided)
  00100
- **Step 7**: Bring down the last bit (0):
  00100 XOR 00000 (no XOR here as 10101 can't be divided)

01000
- **Step 8**: Finally, bring down the last bit (0):
01000 XOR 00000 (no XOR here as 10101 can't be divided)
10000
Final Remainder: The remainder after the division is 100010001000.

Step 4: Form the Codeword

- Append the CRC remainder 100010001000 to the original message 11010111111101011111101011111:

Codeword=M+CRC=1101011111 1000\text{Codeword} = M + \text{CRC} = 1101011111 \, 1000Codeword=M+CRC=11010111111000

5.a.With a neat diagram, explain the working of CSMA/CD protocol. 2.5+2.5

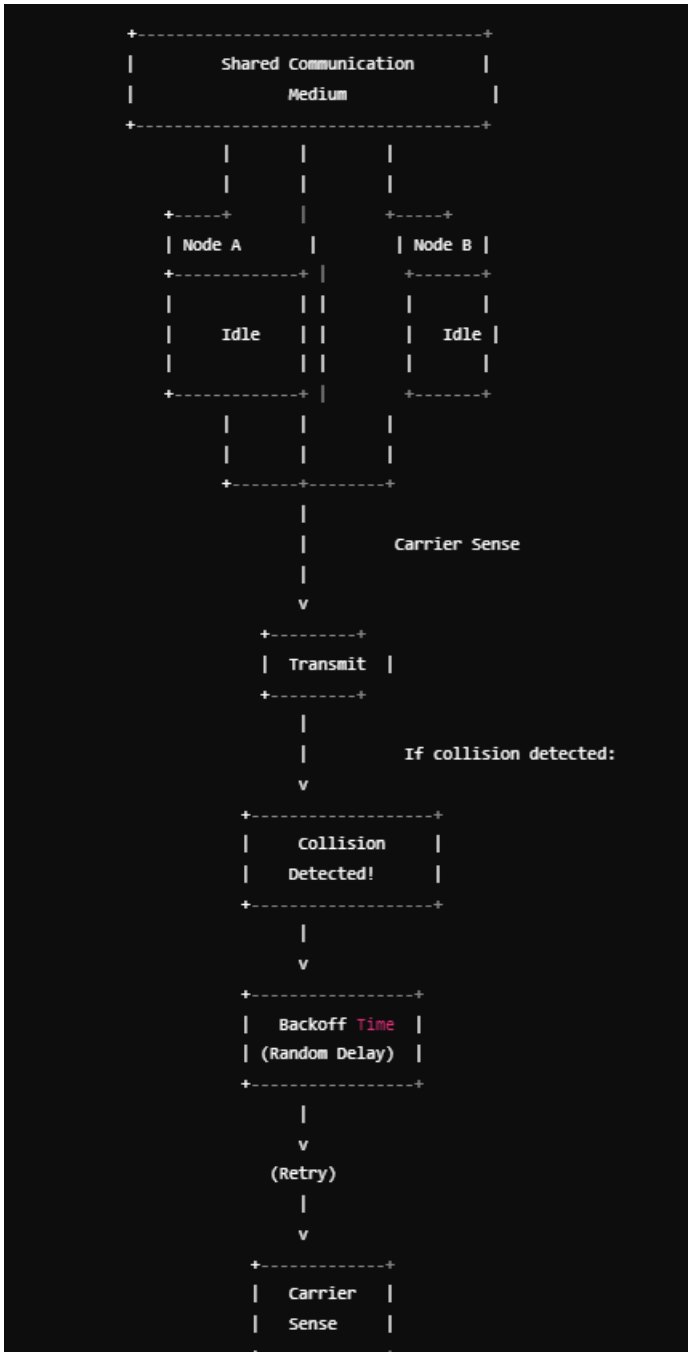
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for managing access to a shared communication medium. It is widely used in wired Ethernet networks. Below is an explanation of how CSMA/CD works, accompanied by a diagram.

How CSMA/CD Works

1. **Carrier Sensing**:
    - Before a device (node) attempts to transmit data, it listens to the network to determine if the communication medium is free (i.e., if no other device is currently transmitting).
    - If the channel is idle, the device can proceed to transmit its data. If the channel is busy, the device must wait.
2. **Data Transmission**:
    - Once the channel is sensed to be free, the device begins to transmit its data frame.
3. **Collision Detection**:
    - While transmitting, the device continues to monitor the network to detect any collisions (i.e., when two devices transmit simultaneously).
    - If a collision is detected, both devices stop transmitting immediately.
4. **Backoff Algorithm**:
    - After detecting a collision, each device waits for a random amount of time before attempting to retransmit. This waiting period is determined using a backoff algorithm, usually exponential backoff.
    - The devices then return to the carrier sensing phase to check if the channel is free before retransmitting.

Diagram of CSMA/CD Protocol

Below is a simple diagram illustrating the working of the CSMA/CD protocol:



Summary of CSMA/CD Steps

1. **Carrier Sensing**: Devices check if the medium is free.
2. **Transmit Data**: If free, the device transmits the data.
3. **Collision Detection**: Devices monitor for collisions during transmission.
4. **Handle Collision**: If a collision occurs, devices stop transmitting.
5. **Backoff and Retry**: Devices wait for a random time before retrying the transmission.

5.b.Describe Pure ALOHA & Slotted ALOHA. 2.5+2.5

ALOHA is a simple communication protocol used in computer networks for managing access to a shared communication medium. There are two variants of the ALOHA protocol: **Pure ALOHA** and **Slotted ALOHA**. Both protocols allow multiple users to access the channel but differ in their approach to managing collisions. Here's a detailed description of both:

1. Pure ALOHA

Description:

- In Pure ALOHA, a device can send data whenever it has data to transmit. There is no synchronization with other devices.
- After transmitting a frame, the device waits for an acknowledgment (ACK) from the receiver.

Working:

- If an acknowledgment is received within a specified time (called the acknowledgment time), the device assumes the transmission was successful.
- If no acknowledgment is received, the device assumes a collision has occurred (meaning two or more devices transmitted at the same time) and retransmits the frame after a random time delay.

Collision Handling:

- Since there is no time slot coordination, collisions can occur at any time, leading to a higher chance of overlap.
- The maximum utilization of the channel is 18.4%18.4\%18.4% (which is the theoretical limit).

2. Slotted ALOHA

Description:

- Slotted ALOHA improves upon Pure ALOHA by dividing time into discrete slots. Devices can only transmit at the beginning of a time slot.
- This synchronization reduces the chances of collisions since devices must wait for the next time slot to begin transmitting.

Working:

- A device waits for the beginning of a time slot before transmitting.
- If a device transmits a frame and does not receive an acknowledgment within the acknowledgment time, it assumes a collision has occurred and will attempt to retransmit in the next time slot after a random delay.

Collision Handling:

- Since transmissions only occur at the start of time slots, the chance of collisions is reduced compared to Pure ALOHA.
- The maximum utilization of the channel is 36.8%36.8\%36.8% (which is the theoretical limit).

Key Differences Between Pure ALOHA and Slotted ALOHA

Feature	**Pure ALOHA**	**Slotted ALOHA**
Time Slots	No fixed time slots	Divided into discrete time slots
Transmission Timing	Can transmit at any time	Must wait for the start of a time slot
Collision Probability	Higher probability of collisions	Lower probability of collisions
Channel Utilization	Maximum 18.4%18.4\%18.4%	Maximum 36.8%36.8\%36.8%
Complexity	Simpler implementation	Slightly more complex due to timing

6.a.Explain how the differences between IPv4 and IPv6 impact internet connectivity and address management in practical scenarios? 5+5

The transition from IPv4 to IPv6 represents a significant evolution in internet protocol standards. The differences between these two versions of the Internet Protocol (IP) impact internet connectivity and address management in various practical scenarios. Below are key differences and their implications.

Key Differences Between IPv4 and IPv6

1. **Address Length**:
    - **IPv4**: Uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses (2^32).
    - **IPv6**: Uses 128-bit addresses, enabling approximately 340 undecillion unique addresses (2^128).
2. **Address Format**:

    - **IPv4**: Addresses are written in decimal format, divided into four octets (e.g., 192.168.1.1).
    - **IPv6**: Addresses are written in hexadecimal format, divided into eight groups of four hexadecimal digits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
3. **Header Complexity**:
    - **IPv4**: The header is complex with 12 fields, which can slow down packet processing.
    - **IPv6**: The header is simplified with 8 fields, improving processing efficiency and performance.
4. **Address Configuration**:
    - **IPv4**: Supports both manual configuration and DHCP (Dynamic Host Configuration Protocol).
    - **IPv6**: Supports Stateless Address Autoconfiguration (SLAAC) in addition to DHCPv6, allowing devices to generate their own addresses without a server.
5. **NAT (Network Address Translation)**:
    - **IPv4**: NAT is commonly used due to address exhaustion, allowing multiple devices to share a single public IP address.
    - **IPv6**: NAT is generally not required because of the vast address space, allowing every device to have a unique global address.

Impact on Internet Connectivity and Address Management

1. Address Availability and Management

- **IPv4**: The limited address space has led to exhaustion, making it challenging to allocate unique addresses for all devices, especially with the growth of the Internet of Things (IoT). Address management requires careful planning, and organizations often resort to NAT to manage the limited pool of addresses.
- **IPv6**: The expansive address space simplifies address management. Organizations can assign unique addresses to every device without concern for running out of addresses. This is particularly advantageous for large networks and IoT devices, enabling easier device connectivity and management.

2. Improved Connectivity

- **IPv4**: Connectivity issues can arise due to NAT, which complicates peer-to-peer communication and introduces potential performance bottlenecks.
- **IPv6**: Direct addressing enhances connectivity by allowing end-to-end communication without NAT. This facilitates easier configuration of services like VoIP, gaming, and peer-to-peer applications, improving overall user experience.

3. Simplified Network Configuration

- **IPv4**: Manual configuration or reliance on DHCP can lead to configuration errors, especially in large networks. NAT adds complexity to network design and troubleshooting.
- **IPv6**: SLAAC simplifies network configuration by enabling devices to automatically configure their own addresses. This reduces manual effort and configuration errors, making networks easier to manage.

4. Security Enhancements

- **IPv4**: Security features like IPsec are optional, and implementation varies.
- **IPv6**: IPsec is mandatory in IPv6, providing built-in security features for data encryption and authentication. This improves the overall security of data transmitted over the internet.

5. Future-Proofing

- **IPv4**: Limited scalability poses challenges for future growth and development of new internet services.

- **IPv6**: Designed with future scalability in mind, IPv6 supports emerging technologies and the exponential growth of internet-connected devices, ensuring long-term viability and adaptability.

Practical Scenarios

1. **Home Networks**:
    - In an IPv4 home network, users might experience connectivity issues when adding multiple devices (smartphones, tablets, IoT devices) due to limited addresses, requiring NAT configuration.
    - In an IPv6 home network, each device can have a unique address, simplifying connectivity and reducing issues related to NAT.
2. **Corporate Networks**:
    - Companies using IPv4 may spend considerable resources on managing IP address allocations, configuring NAT, and ensuring compliance with address limits.
    - With IPv6, companies can easily assign unique addresses to devices and servers, enhancing connectivity for applications such as cloud services, video conferencing, and remote access.
3. **IoT Deployments**:
    - In IPv4 scenarios, IoT devices may struggle with address availability, leading to reliance on NAT and potentially limiting their functionality.
    - In an IPv6 scenario, each IoT device can be assigned a unique global address, enabling seamless communication and data exchange, facilitating the growth of smart cities and automated systems.