Name - Rakesh Suthar
Registration No - 22BCS10178
Subject - Computer Networks
Faculty - Dr. Vikas Kumar Jain

Mid Term

1)

Fully Connected Mesh Topology

Number of Links - $\frac{n(n-1)}{2}$

Explanation - Each device is connected to every other device. For n devices, each device needs to be connected to n-1 other devices. However, to avoid double counting, we divide by 2.

Advantages -

* Highly Reliable - Failure of one link or device doesn't affect the entire network.
* High Fault Tolerance - Easy to identify and isolate faulty components
* High Bandwidth - Multiple Paths for Data Transmission.

Disadvantages -

* Expensive to implement due to the larger number of cables.
* Complex to configure and maintain

Star Topology -

Number of Links = n

Explanation - Each device is connected to a central hub So, n devices require n links

Advantages -

* Easy to install and manage
* Centralized control and Monitoring
* Easy to Add or Remove Devices

Disadvantages -

* Single Point of Failure - If the hub fails, the entire network goes down.
* Performance Bottleneck - The hub can become overloaded with heavy traffic.

Ring Topology -

Number of Links = n

Explanation - Each device is connected to two other devices, forming a closed loop. So, n devices requires n links.

Advantages -

* Simple to understand and Implement
* Efficient for Data Transmission
* Easy to Add or Remove Devices

Disadvantages -

* Single Point of Failure - A break in the ring can disrupt the entire network.
* Difficult to troubleshoot and reconfigure
* Limited Scalability

2) Analog to Analog Conversion techniques are essential in computer networks for transmitting analog signals effectively. These techniques modify an analog signal to convey information while maintaining its analog nature.

Amplitude Modulation (AM)

Definition - In amplitude modulation, the amplitude of the carrier signal is varied in proportion to the amplitude of the modulating signal, which contains the information to be transmitted. The frequency and phase of the carrier remain constant.

Implementation - AM can be implemented using a multiplier that adjusts the carrier's amplitude based on the modulating signal's amplitude changes.

Ex - AM is commonly used in radio broadcasting. A radio station transmits a carrier wave at a specific frequency, and the audio signal alters the amplitude of this wave. For instance, when a singer voice is louder, the amplitude of the carrier increases, resulting in a strong signal being transmitted.

Frequency Modulation (FM)

Definition- In frequency modulation, the frequency of the carrier signal is varied according to the amplitude of the modulating signal. The amplitude and phase of the carrier remain unchanged.

Implementation - FM can be implemented using a voltage controlled oscillator (VCO), which changes its output frequency based on the input voltage from the modulating signal.

Ex- FM is widely used in high fidelity broadcast such as FM Radio. When a sound wave amplitude increases, the frequency of the carrier wave shift slightly higher. Conversely, when the sound wave amplitude decreases, the frequency shifts lower. This method provides better sound quality and resistance to interference compared to AM.

Phase Modulation (PM) -

Definition - In phase modulation, the phase of the carrier signal is altered in accordance with changes in the amplitude of the modulating signal. The amplitude and frequency remain constant.

Implementation - PM can also be implemented using a voltage controlled oscillator. However in PM, the instantaneous change in phase is proportional to the amplitude change of the modulating signal.

Ex - PM is often used in digital communication system and can be found in technologies like GPS and satellite communication.

4) The Sliding Window Protocol is a fundamental technique in computer networking that facilitates efficient data transmission between devices. It allow multiple frames to be sent before requiring an acknowledgment (ACK) for the first frame, thus optimizing the flow of data and reducing latency

Overview of Sliding Window Protocol

Functionality -

* Window Size - The protocol defines a "window" that determines how many frames can be sent without waiting for an acknowledgment. This window size can vary based on network conditions and application requirements.

* Sequence Numbers - Each frame is assigned a unique sequence number, which helps the receiver identify missing frames and manage the order of received frames.

* Sliding Mechanism - As acknowledgments are received, the window "slides" forward, allowing new frames to be sent. This sliding mechanism ensures continous data flow and efficient use of bandwidth.

Working Principle -

* Sender Side - The sender maintains a buffer for frames that have been sent but not yet acknowledged. It can send multiple frames up to the window size limit.

* Receiver Side - The receiver also has a buffer that tracks expected sequence numbers. If a frame is received correctly, an acknowledgment is sent back, if it's corrupted or lost, the receiver may request transmission based on the protocol variant used.

Types of Sliding Window Protocols

Go Back - N ARQ -

* Mechanism - In this protocol, if any frame is lost or corrupted, all subsequent frames must be resent. The sender's window size is N, while the receiver's window size is always 1.

* Efficiency - This method can lead to significant bandwidth waste if errors are frequent as it requires retransmission of all frames after the lost one, regardless of whether they were received correctly.

Selective Repeat ARQ-

* Mechanism - Unlike Go Back N, this protocol allows only the specific lost or corrupted frames to be resent. Both sender and receiver windows are of size N.

* Efficiency - This method is generally more efficient in environments with high error rates because it minimizes unnecessary retransmissions by only resending affected frames.

Note - The Selective Repeat ARQ Protocol is generally considered better than Go Back N in scenarios with higher error rates because it reduces bandwidth wastage by only retransmitting necessary frames rather than all subsequent frames after an error occurs. This selective approach leads to improved overall efficiency and performance in data transmission systems where reliability is critical.

5)

Hubs -

Layer- Physical Layer (Layer 1)

Hubs are basic networking devices that connect multiple Ethernet devices, making them act as a single network segment. They operate by receiving data packets from one device and broadcasting them to all other connected devices without any filtering or addressing. This broadcasting can lead to data collisions, as multiple devices may attempt to send data simultaneously. Hubs do not manage traffic or filter data, they simply repeat signals across all ports

Repeaters -

Layer - Physical Layer (Layer 1)

Repeaters are similar to hubs in that they also operate at the physical layer. Their primarily function is to regenerate and amplify signals that weaken over distance. By doing this, repeaters extend the range of a network by ensuring that signals can travel further without degradation. They do not interpret or manage data, they merely boost the signal strength.

Bridges

Layer - Data Link Layer (Layer 2)

Bridges operate at the data link layer and are used to connect two or more network segments making them act as a single network. Unlike hubs, bridges can filter traffic based on MAC Addresses, which helps reduce collisions and improve overall network efficiency. They learn the MAC Addresses of devices on each segment and use this information to forward packets only to the intended recipient segment.

Switches

Layer- Data Link Layer (Layer 2)

Switches are more advanced than hubs and bridges functioning at the data link layer as well. They connect multiple devices on a network and intelligently forward data only to the device that needs it, using MAC addresses to determine the destination. This capability significantly reduces collisions compared to hubs and enhances network performance by creating separate collision domains for each connection

Routers

Layer - Network Layer (Layer 3)

Routers operate at the network layer and are responsible for forwarding data packets between different networks. They use IP addresses to determine the best path for data transmission across interconnected networks. Routers manage traffic based on between local networks and external networks (like the internet) making decisions based on routing tables and protocols such as RIP or OSPF. They also provide functionalities like NAT (Network Address Translation) and firewall capabilities for enhanced security.

3)

$10111\ (x^4+x^2+x+1)$

Sender Data

```
10111 | 10100111110000
        10111
        -----
        00111
        00000
        -----
         01111
         00000
         -----
          11111
          10111
          -----
           10001
           10111
           -----
            01100
            00000
            -----
             11000
             10111
             -----
              11110
              10111
              -----
               10010
               10111
               -----
                01010
                00000
                -----
                 1010
```

Transmitted Data - 10100111101010

```
10111 | 10100111101010 - Received Data
        10111
        -----
        00111
        0000
        -----
         11111
         10111
         -----
          10001
          10111
          -----
           01100
           00000
           -----
            11001
            10111
            -----
             11100
             10111
             -----
              10111
              10111
              -----
               00000
               00000
               -----
                0000 - No ERROR
```