Vidyalekhan
DATE
PAGE

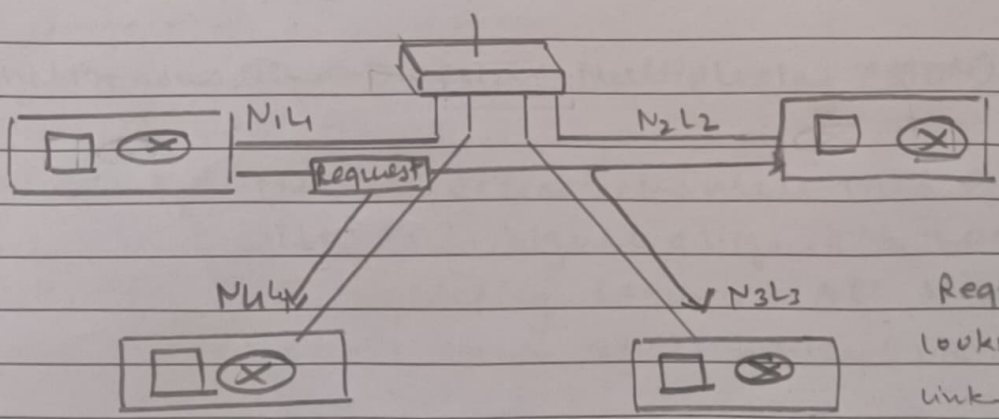
Q.1 Explain ARP with diagram?

Address Resolution Protocol (ARP) is a network protocol used to map an IP address (a logical address) to a MAC address (a physical address) on a local area network (LAN). It plays a crucial role in ensuring that data packets are properly routed within a network by associating the 32 bit IP addresses with the 48 bit MAC addresses.

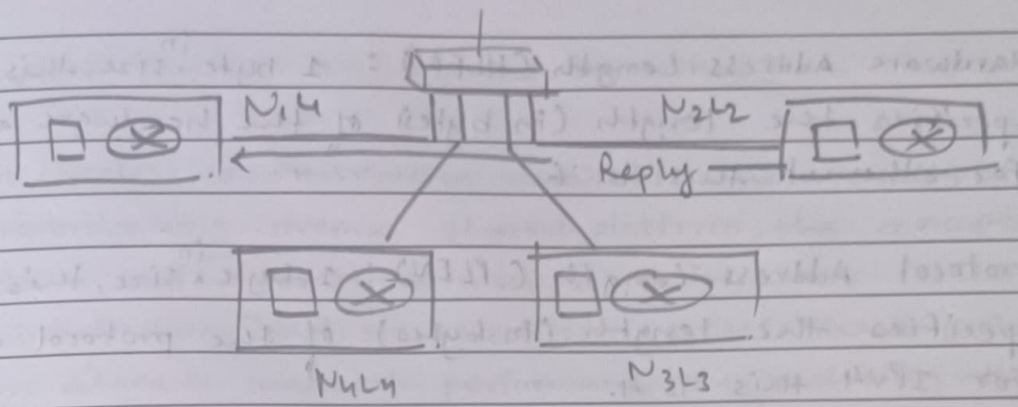
ARP Request: When a computer wants to communicate with another device on the same network, it checks its ARP cache to see if it already knows the MAC address corresponding to the destination IP. If not found it broadcasts an ARP Request packet to all devices on the local network. This packet contains the sender's IP and MAC address.

ARP Reply: The device on the network with the matching IP address responds with an ARP Reply packet, which contains its MAC address.

Communication: The source computer can now use the MAC address to send packets directly to the target device.



Request: looking for link-layer address of a node with IP



Q.2. Discuss ~~ARP~~ Packet format?

An Address Resolution Protocol packet is structured to ~~encoded~~ include essential information for mapping a network-layer IP address to a link-layer MAC address. The ARP packet formate consists of several fields each serving a specific purpose.

0	8	16	31
Hardware type		Protocal Type	
Hardware length	Protocal length	Operation Request:1 Reply:2	
Source hardware address			
Source protocol address			
Destination hardware address			
Destination protocol address			

Explanation of fields :

→ Hardware Type (HTYPE) : 2 bytes Field indicates the type of hardware or link-layer protocol used. For ethernet, this value is 1.

→ Protocol Type (PTYPE) : 2 bytes field defines the type of network layer protocol being ~~so~~ resolved. For IPv4 this value is 0x0800.

→ Hardware Address Length (HLEN) : 1 byte in size, this Field specifies the length (in bytes) of the hardware address For ethernet this is 6.

→ Protocol Address Length (PLEN) : 1 byte in size, this Field specifies the length (in bytes) of the protocol address For IPV4 this is 4.

→ Operation : 2 bytes in size, this field specifies the type of ARP message. It can be ① for ARP request, and ② For ARP Reply.

→ Sender Hardware address (SHA) : 6 bytes in size, It gives the MAC address of the sender (link-layer address)

→ Sender Protocol Address (SPA) : This is a variable length field defining the IP address of the sender of the packet for IPv4, this is 4 bytes long.

→ Target Hardware Address (THA) : This is a variable length field define the link-layer address of the intended receiver This field set to 00:00:00:00:00:00 (All zeros) because the sender does not know the target MAC address. In an ARP reply, this field contains the target's MAC ~~address~~. address. (Ethernet: 6)

→ Target Protocol Address (TPA) : This is a variable length field specifies the IP address of the ~~intended~~ intended recipient of the ARP Packet. In an ARP request, it's IP address sender wants to resolve. In ARP reply, It's IP Adress of the sender.

Vidyalekhan
DATE
PAGE

Q.3. Explain Hidden and Exposed terminal?

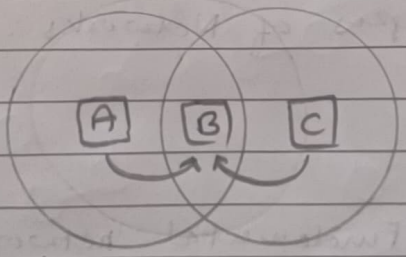
In wireless communication networks when multiple devices communicating over a shared platform, the concepts of hidden and exposed terminals arise when issues related to interference and signal collision occur. These problems can degrade network performance by reducing the efficiency of the data transmission.

→ Hidden Terminal Problem

↳ The ~~the~~ hidden terminal problem occurs in wireless networks when 2 devices are outside each other's communication range but within the range of common reciver. As a result, these devices cannot detect each other's transmission leading them to transmit data simultaneously to the common reciver causing signal collisions at the receiver as it gets overlapping signals. from different devices.

↳ Consequences:
- Data loss due to collision
- Reduced network throughput and efficiency due to increased retransmissions.

↳ Mitigation Techniques:
- Use of Request to Send / Clear to send (RTS/CTS) protocol.
- Use of different channels.

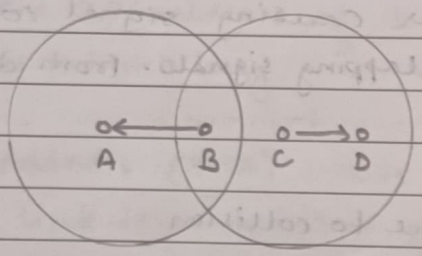


→ Exposed Terminal Problem

The exposed terminal problem occurs when a device is prevented from transmitting because it detects a transmission from a near by device that is communicating with other device even though its transmission would not cause any interference.

Consequences:
- Underutilization of network resources.
- Reduce network throughput as

Mitigation Techniques:
- Use of RTS/CTS protocol.
- Directional Antennas
- Network Allocation Vector (NAV).



Q4. Explain Bluetooth architecture in details?

→ Bluetooth is a wireless technology standard designed for short-range communication between devices typically within 10 meters. The ~~increased~~ usual data rate is 1 Mbps with a 2.4 GHz bandwidth. The Bluetooth architecture is defined by 2 types of Networks: Piconet and Scatternet

→ Piconet

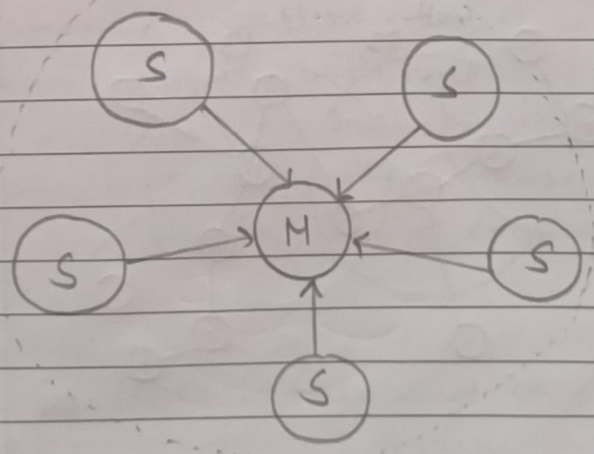
↳ A piconet is the Fundamental network unit in a bluetooth

system. In a piconet there is a single primary device (master) and up to seven active secondary devices (slave).

- Primary Devices: Initiates the connection and controls the communication. Determines the frequency-hopping pattern and timing.
- Secondary Devices: Devices that respond to the master's commands and are synchronized with the mater's frequency-hopping pattern.

↳ Characteristics :

- A piconet can have up to 7 active slave devices simultaneously but multiple additional devices can be in a 'Parked' state which means connected but inactive. These parked devices do not participate in communication but can be activated by master.
- Communication within a piconet can occur in either one-to-one or one-to-many modes. Only the primary device can initiate communicati and secondary must wait for permission from primary.
- Data transfer occurs in Time Divisim Duplex (TDD) manner, meaning the master and slave alternat their transmissions times.



M = Master Device
S = Slave device.

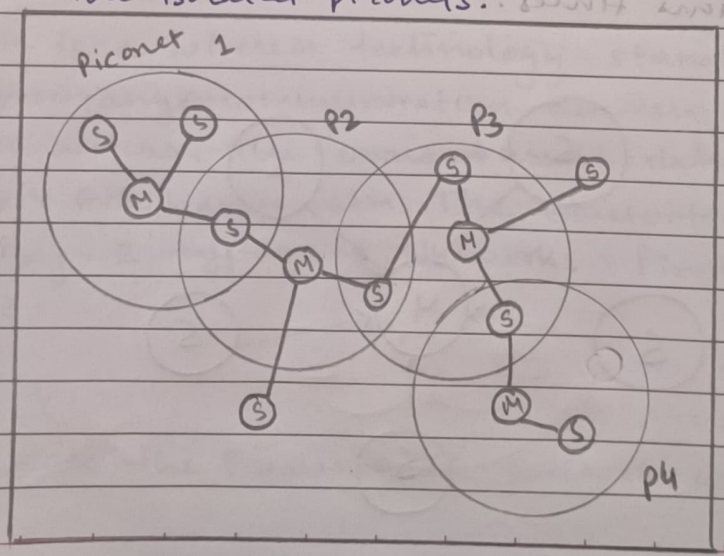
→ Scatternet.

↳ A scatternet consist of multiple piconets that overlap and are interconneted. Devices can participate in multiple piconates simultaneously acting as bridges between them.

↳ Device Role Flexibility: A device in a scatternet act as,
- Primary in one piconet while being a secondary in another.
- Secondary in multiple piconates.

↳ Characteristics:

- Scatternets enable multiple piconets to be connected, facilitating communication across a large network area.
- Devices participating in a scatternet must manage multiple connections, frequency-hopping pattern, and timing schedules to avoid collisions and interference.
- Scatternets enhance bluetooth network flexibility scalability and the ability to support more complex use cases.
- The overlapping of piconets allows devices to communicate across different group which helps facilitate communication between the isolated piconets.



Q.5 Explain Scatternet with diagram?

- explained in Question (21)

Q.6 Discuss different services provided by data link layer

The data link layer is the second layer in the OSI model, sitting just above the physical layer. Its primary purpose is to provide reliable node-to-node data transfer across a physical link, ensuring that data is properly framed, transmitted and error checked.

Here are the key services provided by the data link layer:

1. Framing
- The data-link layer encapsulate network layer datagrams into frames for transmission over the physical network.
- It also decapsulates received ~~data frame and data~~ frames to extract the datagram for further processing.
- This process includes adding header and sometimes a trailer to the data, defining frame format.

2. Flow Control
- To manage the rate of the data transmission and prevent buffer overflow, flow control mechanism are employed.
- These mechanism ensure that the sender does not overwhelm the reciver with too many frames too quickly.
- Strategies include feedback-based approches to adjust the sender's rate or buffer management to handle difference in production and consumption rates.

3. Error Control
- The data-link layer detects and in some cases, corrects errors that occur during transmission.

- Error control involves method for detecting corrupt frames and requesting retransmission if necessary.
- Main purpose is to insure data integrity and reliable communication across the link.

4. Congestion Control:

- Although congestion control is not always directly handled at the data-link layer, it involves monitoring and managing network traffic to prevent and alleviate congestion.
- Typically, this function is associated with higher layers such as network or transport layer but some data-link protocol may incoporate basic congestion mangement mechanisms.

// [5. Addressing

- Addressing involves identifying devices on a network link with unique identifiers.
- The data link layer employs MAC addresses for device identification within a logcal segment and uses protocols like ARP to map IP addresses to these MAC Address.
- This ensure that frames are delivered accurately to the intended destination device on the network.]

Q.7 Explain parity check error detection technique with suitable example.

Parity check is an error detection method used to determine if data has been transmitted accurately. It involves adding an extra bit known as parity bit, to a data unit to make the number of 1's in the codeword is even or odd.

Parity-check code is a type of liner block code. In this code, a dataword of k bits is transformed into a

codeword of n bits where n = k+1. The additional bit, is calculated to ensure an even or odd number of 1's

The minimum hamming distance d_min = 2 for parity check code which means it can detect single bit errors.

- Sender side: Before transmission sender calculates the parity based on the data. For even parity, if the number of 1's is even, the parity bit is set to 0 same goes for odd but the parity bit is set to 1.

- Receiver Side: Upon receiving the data, the receiver recalculates the parity by counting the number of 1s in the received date, including parity bit. If parity does not match the expected even or odd parity, an error is detected.

Advantages:
- Simple and easy to e implement
- Provides basic error detection capability

Disadvantage/Limitation:
- Can only detect single bit errors or odd number error.
- cannot detect 2 bits are altered or more complex error pattern.

example: dataword : 1011

Send codeword : 10111	~~Send~~ codeword : 10111
Received codeword : 10111	recived codeword : 10011
Result : No error detected ✓	Result : Error detected ✗
NO ERROR OCCURS	SINGLE BIT IN DATA

SINGLE BIT ERROR IN RARITY	TWO BIT ERROR
sent codeword : 10111	Sent codeword : 10111
received codeword : 10110	received codeword : 00110
Result : Error detected ⊗	Result : No error detected (The data wrongly accepted)

Limitations →

Q.8 Discuss pure-ALOHA and slotted-ALOHA and describe which one is better.

→ Pure ALOHA and slotted ALOHA are two fundamental protocols used in networking to ~~mag~~ manage access to a shared communication channel in a way that minimizes collisions and maximizes efficiency.

→ Pure ALOHA

- Pure ALOHA is a simple protocol for managing access to a shared communication medium. In this protocol a node can send data at any time without synchronization with other nodes.

  - A Node transmits its data frame whenever it wants.
  - After transmission the node waits for an acknowledgment from receiver.
  - IF no acknowledgment is received within a specified time, the node assumes a collision or failure and retries after a random backoff period.

- Collision : IF two or more stations transmit data simultaneously, a collision occurs and all data lost. It works on the principle of randomly retrying transmission attempts after collision.

- The theoretical maximum throughput of pure ALOHA is about 18.4% of the channel capacity, meaning that only 18.4% of the time is effectively used for successful transmission.

→ Slotted ALOHA

- Slotted ALOHA improves on Pure ALOHA by introducing time slots into which nodes are restricted to sending their data. This approch helps in reducing collision and increasing efficiency.

- Time is divided into discrete slots of equal length.
- Nodes are allowed to send data only at the beginning of these time slots.
- If a node has data to send it waits until the stat of the next time slot
- Like pure ALOHA after sending data, the node waits for an acknowledgment. If the acknowledgment is not received, it retries after a random backoff period.

- Collision: By aligning transmissions to time slots, slotted ALOHA reduces the probability of collisions because the data transmission starts at the beginning of a slot, minimizing overlap.

- The theoretical maximum throughput of slotted ALOHA is about 36.8% of the channel capacity which is higher than Pure ALOHA due to reduced collision chances.

→ Comparison of Pure ALOHA and Slotted ALOHA.

Feature	Pure ALOHA	Slotted ALOHA
Transmission Time	Any time	only at the beginning of a time slot
Collision Probability	Higher	Lower
Efficiency	Less efficient	More efficient
Implementation Complexity	Simpler to implement	Slightly more complex.
Throughput	Lower maximum throughput	Higher maximum throughput

- Slotted ALOHA is generally considered better than Pure ALOHA due to its higher efficiency, reduced collision probability and better utilization of the medium.

Q9 Explain CRC with suitable example.

The cyclic Redundancy check (CRC) is an error detecting code used to ensure the integrity data during transmission. The data is divided by a fixed generator polynomial to produce a reminder which is appended to the data. The reciver performs the same division to check IF the reminder matches the expected value. IF ~~recait~~ remainder do not match errors are detected.

Operational Mechanism.

1. Polynomial Representation: The data to be transmitted is represent as a binary polynomial. A fixed binary polynomial known as the generator polynomial (G(x)) is used for divison

2. Encoding: Append a number of zeros to the end of the data equivalent to the degree of G(x). Using XOR perfor. binary polynomial division on the modified data with the g(x). The remainder from divisim is CRC checksum This remainder is appended to the orignial data to

3. Form codeword CRC.

3. Transmission: The codeword (original data + CRC checksum) is transmitted.

4. Decoding: The receiver performs the same divisim on the received codeword. If remainder is zero, the data is considered error-free. If not, an error is detected.

Example:

- here G(x) = x^3+x+1
  Data : 1101 (4 bits).
- So Append 3 zeros to data,

  1101000

- Remainder: 001
- CRC codeword : 1101001

```
      1011 | 1101000
             1011↓
             -----
             01100
              1011↓
              -----
              01110
               1011↓
               -----
               01010
                1011
                ----
                0001
```

reciver check : 1101001

```
        1011 | 1101001
               1011
               ----
               0110
                1011
                ----
                0111
                 1011
                 ----
                 0110
                  1011
                  ----
                  0101
                   1011
                   ----
                   0000
```

Remainder is zero, the data is correct.

Q.10 Explain CSMA technique with different methods

→ Carrier Sense Multiple Access is a network protocol used in wired and wireless networks to manage data transmission and avoid collision. CSMA operats on a principle of "Listen before talk" meaning a device checks wheter the communication channel is clear before attempting to send data. the channel is busy, device waits until it become free.

→ Persistent and Non Persistent CSMA

- 1- Persistent CSMA:
  - IF channel is busy, the node keeps sensing the channel continously.
  - As soon as the channel is free the node transmit immediately.
  - IF collision occurs each device involved in the collision waits for a random amount of time before attempting to retransmit.
  - Advantage: High utilization, simple to implement
  - Disadvantage: High chance of collision if multiple nodes are waiting.

- Non-Persistent CSMA:
  - In non-persistent CSMA, device also listens to the channels but if the channel is busy it waits for random amount of time before trying again instead of continuously sensing the channel.
  - Advantage: Reduce collision as the waiting time is random.
  - Disadvantage: Lower channel utilization compared to 1-persistent CSMA.

- p- persistent CSMA:
  - Used mainly in slotted channels, in p-persistent CSMA device listens to the channel and if it is free transmit with probability p. If the channel is busy the device waits for the next time slot to try again.
  - Advantage: Balances channel utilization and collision chances.
  - Disadvantage: Still some of the chance of collision when multiple nodes choose to transmit at the same slot time.

→ CSMA / CD

- Carrier sense multiple Access with collision Detection is used in wired network like Ethernet, it improves on basic CSMA by detecting collisions in real-time while transmitting data.
- If collision is detected during transmission all devices in the collision immediately stop transmission send a jamming signal and wait for random back-off period before trying again.
- Advantage: Minimizing the time wasted due to collision.
- Disadvantage: Only suitable for wired network because it requires all device in network to hear each other's signal's clearly.

→ CSMA/CA

- Carrier sense Multiple Access with collision Avoidance is commonly used in wireless network, it aims to avoid collisions before they happen.
- Device listen to the channel, if it is free they wait for a random back-off time before transmitting
- Instead of detecting collision it tries to avoid them. It may also use additional techniques like RTS/CTS to ensure that the channel is reserved or not.
- Advantages: Works well in wireless network. Prevents collisions before they occur, reducing retransmissions.
- Disadvantages: The overhead of waiting times and the use of control messages can reduce overall network throughput

Q.11 Discuss ARP Protocol with suitable example.

Discussed in Question (1).

Q.13 Explain CSMA/CD technique.

Explained in question (10)

Q.12 Given the data word "101001111" and the divisor '10111', show the generation of CRC codeword at the sender site.

Here, the dataword is 101001111

$Q(x)$ = '10111

∴ degree = 4

So appended zero will be 4.

∴ 101001111 0000 ÷ 10111

```
10111 | 1 0 1 0 0 1 1 1 1 0 0 0 0
        1 0 1 1 1 ↓
        ---------
        0 0 0 1 1 1
          0 0 0 0 0 ↓
          ----------
          0 0 1 1 1 1
          0 0 0 0 0 0
          -----------
            0 1 1 1 1 1
              1 0 1 1 1
              ---------
              0 1 0 0 0 1
                1 0 1 1 1
                ---------
                0 0 1 1 0 0
                  0 0 0 0 0
                  ---------
                  0 1 1 0 0 0
                    1 0 1 1 1
                    ---------
                    0 1 1 1 1 0
                      1 0 1 1 1
                      ---------
                      0 1 0 0 1 0
                        1 0 1 1 1
                        ---------
                        0 0 1 0 1
```

Remainder : 0101

∴ Codeword at sender site will be,

1 0 1 0 0 1 1 1 1 0 1 0 1

Q.14 Discuss types of data transmission errors. Describe the difference between error detection and error correction.

→ Data transmission errors can occur due to various reason like noise, signal attenuation, interference or synchronization issues.

The common types of data transmission errors are:

1. Single-Bit Error:

- A single-bit error occurs when only one bit in a data unit (such as a byte, frame or packet) is altered during transmission.
- Occurrence: This type of error is rare in most modern communication system due to error detection and correction.
- Cause: Often caused by random noise or minor
- disturbances in the transmission medium (such as interference).
- Detection: Single-bit errors are easy to detect using simple error detection methods like parity checks or Cyclic Redundancy Check (CRC).

Example: if original data is '1011001'.
data after transmitted is '1010001'

2. Burst Error

A burst error occurs when 2 or more consecutive bits in a data unit are altered during transmission. A burst error can ~~vary~~ vary in length depending on how ~~many~~ many bits in a row are affected.

- Occurrence: Burst errors are more common than single bit errors especially over noisy or unreliable communication channels.
- Cause: Typically caused by a sudden disturbance in the trasmission medium, such as electrical interference or crosstalk.

- Detection: Detecting burst errors is more complex than single-bit errors. Techniques like CRC and checksums are often used, which are capable of detecting longer bursts of errors.
- Length: The length of a burst error is measured from the first corrupted bit to the last corrupted bit including any unaffected bits in between.

Example: If original data is '1011001'
data after transmision is '1000111'
(2nd to 5th bit - 0110 0 to 0001 1)

→ Difference between Error Detection and Error correction

Feature	Error Detection	Error correction
Definitation	Identifying whether an error has occured	Identifying and correcting errors.
Method	Adds reclundaney to deteet errors	Adds redlundancy to detect and correct errors.
Techniques used	Parity Checks, CRC, checksums	Humming codes, FEC, Reed-Solomon.
Action on Error	Request retransmission of data.	Correct errors without retrasmission.
Efficiency	Less complex, faster	More complex, require more processing
Use cases	Used in system where retransmission is possible like TCP/IP	Used in system where retrans-mission is costly or impossible like satellite communication

Vidyalekhan

DATE

PAGE

Q.15 Given dataword '1001000' and the divisor '1011', show the generation of CRC codeword at the sender site.

here, the dataword is '1001000'.

$G(x) = 1011$

$\therefore$ degree = 3

So appended zero will be 3.

$\therefore$ 1001000000

```
          1
     ------------------
1011 | 1 0 0 1 0 0 0 0 0 0
       1 0 1 1
       -------
       0 0 1 0 0
         0 0 0 0
         -------
         0 1 0 0 0
           1 0 1 1
           -------
           0 0 1 1 0
             0 0 0 0
             -------
             0 1 1 0 0
               1 0 1 1
               -------
               0 1 1 1 0
                 1 0 1 1
                 -------
                 0 1 0 1 0
                   1 0 1 1
                   -------
                   0 0 0 1
```

remainder : 0001

Codeword at sender site will be,

1001000001

Q.16 Write a short note on reservation and polling controlled access protocols.

In networking controlled access protocols are used to manage how multiple device share a communication medium. Two common type of controlled access protocols:

1. Reservation Protocol

- Reservation protocols allocate transmission opportunities to devices based on predefined schedules or requests ensuring that each has a fair share of the communication medium.

- Devices request permission or reserve a time slot for communication. Once reserved, no other device can use that slot.
- Reduces collision as access is pre-scheduled suitable for environments where high reliability and predictable access times are needed.
- Implementation of protocol is common in time-division multiplexing (TDM) system, where time slots are allocated to different devices in repeating cycle.

- Advantages : Predicatable Access and Reduced collision.

- Disadvantages : Less Flexible, Reservation can introduce additional overhead

2. Polling Protocol

- Manage access by having a central controller or coordinator poll nodes to determine if they have data to send, thereby controlling the access to the shared medium.

- A central node controls the access to the medium by polling each device in turn.
- Can be efficient in managing access as only the polled device can transmit data at a given time.
- Token Ring protocol and the polling mechanism in certain LANs are the major example.

- Advantages : Simple to implement and collision are effectively avoided.
- Disadvantages : Single point of failure (Master node) affecting the entire network's performance. Time taken for device can introduce latency.

Q.17 Error Detection with any one ~~one~~ technique.

Explained in Question (9).

Q.18 Given that dataword polynomial is $x^8+x^6+x^3+x^2+x+1$ and the divisor x^4+x^2+x+1, show the generation of CRC codeword at the sender site.

~~here~~ here,

the polynomial $G(x)$
$= x^4+x^2+x+1$

dataword polynomial
$= x^8+x^6+x^3+x^2+x+1$

$$
\begin{array}{r|l}
x^4+x^2+x+1 & x^4+x+1 \\
\cline{2-2}
x^8+x^6+x^5+x^4 & x^8+x^6+x^5+x^4+x^3+x^2+x+1 \\
\cline{2-2}
 & x^5+x^4+x^3+x^2+x+1 \\
 & x^5+x^3+x^2+x \\
\cline{2-2}
 & x^4+1 \\
 & x^4+x^2+x+1 \\
\cline{2-2}
 & x^2+x
\end{array}
$$

were the remainder is 'x^2+x'.

Now,

$$(x^8+x^6+x^3+x^2+x+1) \oplus (x^2+x)$$

$$= x^8+x^6+x^3+1.$$

$\therefore$ codeword $= x^8+x^6+x^3+1$

- $D_A = 1 \times [1,-1,1,-1] = [1,-1,1,-1]$
  $D_B = -1 \times [1,1,-1,-1] = [-1,-1,1,1]$
  $D_C = 1 \times [1,-1,-1,1] = [1,-1,-1,1]$

  Data bit 1 represented by '+1'. and 0 by '-1'.

- $S = D_A + D_B + D_C$

  $= [1-1+1, -1-1-1, 1+1-1, -1-1+1]$
  $= [1, -3, 1, 1]$

- Received signal for A $= S \cdot D_A$
  $= [1,-3,1,1] \cdot [1,-1,1,-1]$
  $= (1+3+1-1)$
  $= 4$ (+ve)

  bit for User A is 1.

  similarly For User B → 0 (-4 → -ve)
  For User C → 1. (4 → +ve)

Q.19 Explain CDMA channelization protocol with suitable example.

Code Division Multiple Access (CDMA) is communication protocol used to allow multiple users to share the same frequency channel by assigning unique codes to each user. This allows simultaneous communication without interference, leveraging the unique properties of the codes.

Operational Mechanism

- Each user is assigned a unique spreading code or code sequence. These codes are orthogonal meaning they are designed to be distinct.
- The user's data signal is multiplied by unique spreading code, expanding it over a wider frequency range to create a spread spectrum. This result in a broader bandwidth signal that appears as noise.
- All users transmit spread ~~sing~~ signals on the same frequency simultaneously without interference thanks to unique code.
- At the receiver, signals are matched with the receiver's code to isolate and decode the original data from the combined transmission.

Example:

- U1 = [1, -1, 1, -1] → data bit = 1
  U2 = [1, 1, -1, -1] → data bit = 0
  U3 = [1, -1, -1, 1] → data bit = 1