**Assignment HDC-DCN Part 2**

**Student Details:**

Student No. : 2997677

Student Name : Krishna Dhar Akella

Course and Module :(HDC-DCN)

**Part 2: Questions and Answers (50 marks)**

**Answer the following questions:**

**Q1) Describe a protocol that will eliminate collision entirely in multiple access to a shared media channel. Give at least two advantages and two disadvantages of the protocol you describe.**

**Answer:**

**CSMA/CD :**

**CSMA/CD** also known as **Carrier Sense Multiple Access with Collision Detection** is a protocol that can be used to remove collisions completely in a multiple access to a shared channel. **Carrier Sense Multiple Access with Collision Detection** as the name suggests is a collision detection protocol which automatically detects the occurrence of collision during the transmission of packets in a shared channel. All the processes are checked at each stage of transmission, when a packet is sent it makes sure that the packet has reached the destination. It waits for the acknowledgement to send another packet.

**Advantages of CSMA/CD :**

* It detects the collision in the network in a very small amount of time.
* When a collision is concurred the packet is retransmitted once the channel is free.

**Disadvantages of CSMA/CD :**

* It does not have any effect on the number of collisions occurring in the shared channel. It does not help in collision reduction.
* For large networks the protocol is not very effective.

**Q2) Describe or explain some aspect of each of the following devices. Must write at least ten correct statements on each device.**

**1) A repeater.**

**2) A hub.**

**3) A bridge.**

**4) A switch.**

**5) A router.**

**Answer :**

1. **HUB:**

A hub behaves like a repeater with multiple ports, a hub can be used to connect multiple stations like in star topology. They are not active devices so they do not have logic like filtering data, so data is sent to all the connected devices to the hub. Hubs broadcast the data received on one port to all other ports. They work on the physical layer of the OSI layer of the network.

There are two types of hub:

* **Active Hub** : These types of hub have their own power and can have the ability to boost weak signals across the network, same as a repeater with multiple ports.
* **Passive Hub** : These hubs do not have their own power so they can only be used to connect devices together in a network however they do not help in boosting the signal strength.

**2. REPEATER:**

Repeaters are integrated into networks to broaden their service range. They are often regarded as signal boosters. If an electronic signal is received by a channel, it attenuates the signal based on the channel's existence or technologies. This represents a constraint on the duration of the LAN or the cellular network coverage area. This problem is removed by adding repeaters at such intervals. Repeaters reproduce the attenuated signal and instead retransmit it. Electronic repeaters may also recreate signals corrupted from propagation loss. Repeaters are popularly implemented to communicate between two LANs into a broad single LAN.

**3. BRIDGE:**

A bridge works on the DLL or data link layer of the OSI network model. A bridge is an active device that means it has some programmable logic. A bridge can be considered as a repeater with the functionality to filter the content of the network by checking the MAC address of the source of the packet and the destination of the packet. It is a 2 port device, thus can be used to connect two networks together. A bridge can also be used as a repeater to extend the network and also help in reducing the collision in the network.

There are two types of bridges:

* **Transparent Bridges :** Transparent Bridges are the bridges where the stations do not have the information about whether a bridge is there in the channel or not.
* **Source Routing Bridges :**  In source routing bridges the routing can be done by source station . The frame determines which route it will be going through.

**4. ROUTER:**

A router is an active device and can be used to route packets by using the IP address of sender and receiver just like the switch. Routers are Network Layer device that connects Local Area Networks and Wide Area Networks together. Router consist of a routing table that keeps on updating dynamically and helps in routing the data packets to a correct destination. It works on the third layer of OSI model. One can move within the area freely while connecting to the internet through router. Routers transfers data across a network using a routing protocol. It also shares information within the network. It is costlier than hubs and switches. Each packet header consists of a IP address with the help of which router analyzes and compares it with the routing table and sends it to the respective destination.

**5. SWITCH:-**

A switch is type of bridge having multiple ports. Switch comes with a buffer and has a design that can boost its efficiency. It is a small device having multiple ports that causes less traffic and thus increases the performance. A switch centralizes communications between devices connected within a network, basically a Local Area Network (LANs).

The switch usually performs error checking before forwarding the data to the destination making it efficient as it forwards error free packets correctly to destined ports only. The most common type of switches are Ethernet switches. Optimized switches are found in ATM, Fiber Channel, and Token Ring network architectures. No special configuration is required to connect switches that are used in consumer routers except plugging in cables and power.

High-end devices that are used in large enterprise networks has a wide range of advanced features compared to the unmanaged switches. These switches are designed in such a way that can only be controlled by professional administrators. Switch manages the flow of data across a network by analyzing the destination MAC address and forwarding it to the host with the correct message.

Every switch has a MAC address table that is dynamic in nature and keeps a mapping of MAC addresses and ports. A switch is better than an Ethernet hub, that simply retransmits packets out to every other ports except the port on which the packet was received causing lower network efficiency. Switches are mostly used as the network connection point for hosts at the edge of a network.

**Q3) Explain how the following errors on received frames at the data link layer can be detected and describe briefly how such errors may be corrected.**

**1) A damaged frame due to addition of a few bits or missing of a few bits.**

**2) Out of sequence frame**

**3) A lost frame**

**4) A duplicated frame**

**5) A frame is too big or too small**

**6) Bits changed in a frame during transmission.**

**7) Received frame or receiving an acknowledgment for a frame with a sequence number ahead of the window**

**8) Multiple copies of a frame are sent and no acknowledgements are received over a long period of time.**

**9) On regular bases multiple copies of each frame are received.**

**10) The sender forgot to put the flag between two frames.**

**Answer :**

**ERROR CORRECTION AND DETECTION AT DATA-LINK LAYER** **:**

**1.**A damaged frame due to addition of a few bits or missing of a few bits. :

It groups the physical layer bit stream into units called **frames**. Frames are ‘packets’ or ‘messages’ that a sender sends over a network. Sender usually checksums the frame i.e., packets or messages and sends the checksum along with the data. The checksum allows the receiver to identify when a frame has been damaged during transmission. After transmission, receiver recomputes the checksum and compares it with the received value. If there is any difference, an error occurs and the frame is discarded and an acknowledgment is send back to the sender whether the packet has been received correctly without damage or not. Usually it returns a positive or negative acknowledgement to the sender. A positive acknowledgment means the frame was received without errors, while a negative acknowledgment means the frame was not transmitted properly and thus error occurred during packet transit. Further more the error can be corrected by the sender and then the same packets could be retransmitted.

**2.** Out of sequence frame :

A frame header usually consist of a :

* **destination address** : The destination where the packets are to be sent.
* **source address** : The source from where the packets are transmitted.
* **control fields** : There are 3 control fields. They are **kind, seq** and **ack.**

**Control Fields**

* kind: It tells us whether the transmitted frame is a data frame or it is used as controlling functions. Control functions usually control the error and flow or manages the links.
* seq: Each frame consists of a sequence in an order to keep a check on it is sent to the recipient. It helps in maintaining an order it is sent and also in case of re-sending the frame to the sender.
* ack: This contains the acknowledgment number of frames. If an error occurs or if the packet is submitted successfully an acknowledgement is sent back to the sender.

Here by SEQ we can detect OUT OF SEQUENCE FRAME error and recover by negative acknowledgment by retransmission.

**3.A lost frame :**

Each frame consist of a sequence. The FCS field of a frame consists of a number that is calculated by the source node based on the data in the frame. This number calculated by the source node is added to the end of a frame that is sent over a network. When the destination node receives the frame, this FCS number is re-calculated and compared with the FCS number included in the framereceived. If the FCS of a frame received does not match with the re-calculated FCS then the frame is discarded and hence frame is lost.

This error can be corrected or recovered by retransmission by giving negative acknowledgment.

**4.A duplicated frame**

When a frame is transmitted over a network, there might be a chance that the data-frame can be lost in the transit or received corrupted at the recipient end. In both scenarios, the receiver gets the incorrect data-frame or no data-frame while sender remains unaware of about any such loss. In such cases, both the sender and the receiver have some protocols which helps them to identify transmission is done correctly or not or an error such as loss of data-frame has occurred. Same data-frame sent twice is also checked. Hence, there could be a possibility that sender retransmits the data-frame or the receiver may request to resend the previous data-frame received.

By using ARQ and GO-BACK N ARQ we can resolve.

**5.A frame is too big or too small :**

A Frame is too big or too small is an error we get sometime then to resolve.We need to fix the frame size, then we won't get the error of frame size.

**6.Bits changed in a frame during transmission. :**

While transmitting a message over a network, a message could be destroyed due to noise present in the network. Also there is a possibility that the data gets misplaced and thus in return data frame is corrupted. In order to avoid this, an error-detecting codes are used that are additional data added to a data frame or message in order to detect if any error has occurred while transmission of the message across a network.

Some of the techniques used for error detection are listed below:

1. Simple Parity check
2. Cyclic redundancy check
3. Two-dimensional Parity check
4. Checksum

**8.Multiple copies of frames are sent and no acknowledgements are received for long time**

If sender have sent multiple copies of a frame and no acknowledgements are being received for long time then there exist some issue. According to Automatic Repeat Request or Selective Repeat, then the sender sends again the frames after some time.

We can use GO-BACK N for recovery of this error.

**9.On regular basis multiple copies of each frame are received**

There are chances when the sender sends frame on a regular basis without receiving the acknowledgement from the receiver side. Hence duplicate copies are being transmitted continuously. The receiver can detect duplicates by rejecting the frames whose data is same as that of the previous frame received. There might be a probability that the data sent may contain the same value in successive frames that are received and hence causing deadlock. By using sequence number we can detect this error and resolve. If sender sends a sequence starting from 101,then receiver accepts the frames only after the 101 seq number if sender sends multiple copies of same frame.

**10. The sender did not put the flag between two frames** **:**

The flag bit is used to find the start/end of a frame. When the flag is missed, then we can use the size of the frame to complete the task. The error is that we do not no the start and end of the frame, when sender forget to put the flag between two frames.

We don't know the starting and ending of the first and second frame.