**Even if TCP guarantees reliable data transfer on an end to end basis, why do we need reliable data transfer protocol between two ends of a link?**

Wireless links introduces lots of bit errors in the link because of interference and noise. Whenever TCP detects that there is a problem with a packet, it takes a congestion control action by lowering the congestion window. The delivery of a packet will not be possible in two cases: Congestion in the network or bit errors. The bit errors appear most of the time in wireless links which is at the end of the network nearby the host. From the TCP senders point of view, there is no mechanism in TCP in order to distinguish between these two events. If there would not be reliable data transfer protocol at the wireless link, the entire packet had to be retransmitted from the sender to receiver in case of a bit error happening in wireless link. The reliable data transfer enables to retransmit the packet from the previous link and hence, there is no need to retransmit the packet again from the sender..

**If we sense that the channel is already occupied by somebody else, we do not start transmission. However, does CSMA avoid all collisions? On what conditions can CSMA have collision ?**

Because of propagation delay, CSMA can have collision. If the distance between the nodes is large, due to propagation delay, another packet might occupy the node while transmitting the packet which faces a longer propagation delay. This is not a very huge problem if the distance between the node is short because propagation delay is less compared to larger distance. This approach can be used in LAN because of having close nodes.

**Although Carrier Sensing is available, collisions are possible. What are the reasons of having collisions?**

Because pf propagation delay. Two nodes might concurrently listening the channel or there might be an already ongoing transmission in the channel but because the signal takes some time to propagate over the medium because of the propagation delay, the current node may start the transmission before arrival of the signal and collision might occur..

**Why do we need MAC addresses while already having IP addresses that indicates the same network interface?**

First of all, the IP address is related to the network layer, on the other hand, the MAC addresses refer to the physical interface of a link and a link is not used in conjunction with a network layer. When building a link from the business point of view, it is not desired to attach the link in such a way that it can only be used as a common network layer. Because the link needs to work with different network layers, the IP address network layer identifier can not be used because different network layers have different ways of identifying network interfaces.

**Why should not we change MAC addresses ?**

MAC addresses are given in the manufacturing phase and they should not be changed and have to be unique. If it is changed afterwards, there is a possibility that, two network interface cards can be assigned the same identifier which result in the disfunctioning of the network interface cards. Although it is highly improbable because of 2^-48, we should not change it.

**Why do we have flat addresses in Mac and not hierarchical addressing as it was in IP ?**

Hierarchical addressing was used for scalability reasons and reducing the forwarding table sizes in the routers. In MAC addressing, scalability is not a big issue because the interfaces in a subnet suc h as a LAN are much more less in comparison to all of the possible destinations in the internet. Therefore, the forwarding tables in link layer are smaller in size around 100 entries and scalability is not an issue. There is also another advantage of using flat addresses which is the problem with IP address is that when we move from one network to another, the IP address cannot be used over another subnet due to hierarchical addressing. Therefore, from the mobility point of view, using hierarchical addressing is not easy to handle because IP addresses needs to be reconfigured. Since MAC addresses are flat, any MAC address is valid in any LAN. When we move from one network to another, the MAC address will not change. There is no reconfiguration problem because of not having hierarchical structure.

**Is there any advantage of having flat addresses in the internet?**

When we move from one network to another, the IP address cannot be used over another subnet due to hierarchical addressing. Therefore, from the mobility point of view, using hierarchical addressing is not easy to handle because IP addresses needs to be reconfigured. Since MAC addresses are flat, any MAC address is valid in any LAN. When we move from one network to another, the MAC address will not change. There is no reconfiguration problem because of not having hierarchical structure.

**Why is Ethernet unreliable?**

Even though CRC error detection is available, in the Ethernet, we do not have retransmission mechanism.

**What is Carrier Sensing ?**

Each node listens to the channel before initiating a transmission. If the node senses that the channel is idle, the sender starts transmission. Otherwise, if the channel is busy, it defers the transmission and waits until the channel becomes idle and thus, the current ongoing transmission finishes.

**Even though in the Internet, CRC Error detection is available, internet is accounted for unreliable. Why?**

Even though CRC is available, there is no retransmission mechanism. Errors are detected but the packet is not retransmitted, they are discarded without notifying the sender.

**Exponential Back-off Question. The random delay that each node experiences after a collision is determined by a random number which is chosen from the interval of K {0, 1, 2, … 2^m-1}. Why do we wait more by experiencing collisions?**

Consequtive collisions may point out that there is a severe congestion or collision. If there are large number of nodes, the probability of choosing one node one and the others 0 is very low if K = 1. Hence, the K increases overtime through experiencing collisions and at some point, the probability distribution enables the system to transmit the packets.

**If the data contained in the internet is shorter than 56 bytes which is the available data portion in a 64 byte frame, what should be done?**

TCP ACK messages are 40 bytes long and covers 40 percent of the traffic. In these cases, padding is applied in order to make sure that the frame is 64 bytes. In the receiver, the padded bytes are removed by the help of IP header because the size of the packet is present there.

**If we have a very large frame, what would be the disadvantage?**

Transmission time will be too long and during the transmission of the fragment, no other node will be able to sent anything. Importantly, the internet could be used by some time critical applications such as skype. From the network point of view, fairness is neglected. That is why, the maximum frame size is limited by 1500 byte.

**What are the advantages of having a large frame ?**

The overhead is going to be small. Also, when frames are very large, collisions will be at minimum level because of carrier sensing. As a result we have a very high efficiency. However, fairness is violated.

**What are the advantages of switches over Hubs?**

Hubs don’t have e carrier sensing and they are prone to collisions. Hubs do not have a collision detection and error detection mechanism. On the other hand, switches are able to buffer frames and before forwarding a packet, switches are capable of doing link layer functionalities such as carrier sensing and collision detection. Furthermore, hub repeats and sends the signal to all its ports, whereas, switches are able to send it to a specific address. That way, the internet traffic can easily hinder unnecessary traffic.

Switches selectively forwards the fragments and avoid unnecessary forwardings. Also, switches support ports at different speed. More importantly, since switches uses CSMA /CD mechanism while forwarding a packet, it basically isolates the networks from each other such that each of the isolated networks constitute a separate collision domain. As a result, the isolated systems can send frames to the network simultaneously because the switch is capable of buffering the frames.

**How does a switch constructs it’s switch table?**

Switches construct their switch table by the courtesy of source mac address in the link layer header. After learning the corresponding MAC address of a frame, in the switch table, the corresponding MAC address and the interface where the frame comes from is recorded.

**What are the advantages and disadvantageous of using a switch instead of a router ?**

A router runs a routing algorithm and a routing algorithm typically requires a configuration by the network administrator and in order to work properly for the routing algorithm, the interfaces need to be defined which are the links that are adjacent to them and link state advertisement is required. On the other hand, the setup of a switch is much simpler and does not require a complex algorithm to setup the switch table. It can be plugged into a system easily.

In addition, there is also a disadvantageous part of switches. While doing an ARP query, the switch broadcast the query to entire network and between the switches, to much flooding occurs and the system operates excessively and broadcast storm occurs. This congestion or traffic might be so heavy that it might cause the entire network not to function.

**TDM FDM**

TDM synchronization is needed but FDM no need for synchronization, however filter needs to be available for distingiusihing frequencies.

Single bit parity can detect only odd number bit error. Error detection capability of single bit parity code is 1 bit.