Assignment 4

Name – Sati, Ankit   Date – 10/28/2021

Section – 001

SID – as14128

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

Question 1

1. Definitions.

a. Differences between a Router and a Switch.

1. Routers operate at Layer 3 (Network) of the OSI model whereas Network switches operate at layer two (Data Link Layer) of the OSI model.
2. In Router, every port has its own broadcast domain, and the switch has one broadcast domain except VLAN implemented.
3. Router store IP address in the routing table whereas Switch store MAC address in a lookup table
4. Routers can work within both wired and wireless network situations on the other hand, switches are restricted to wired network connections.
5. In various types of network environments (MAN/ WAN), the router works faster whereas Switch is faster than a Router in a LAN environment.

b. The MAC protocols can be divided into 3 main parts.

1. **Channel Partitioning** – Divide channel into smaller "pieces" (time slots, frequency, code)
   It is a time division based channeling access. In this we access the location on the basis on time and in multiple rounds. Each station gets divides into length in each round and the used slots are idle. It can be subdivided into 2 sub categories : frequency based and time based .
   example: 6-station LAN, 1,3,4 have packet, frequency bands 2,5,6 idle

2. **Random Access** – Channel not divided, allow collisions
   It works to find the collisions in the transmitting nodes. It studies how to detect collisions and how to recover from it. If there are 2 or more transmitting nodes then it may be in a state of collision.
   It is basically due to no prior coordination between nodes.
   Example: ALOHA, slotted ALOHA.

3. **Token Ring** –
   A token ring is a data link for a local area network (LAN) in which all devices are connected in a ring or star topology and pass one or more tokens from host to host. A token is a frame of data transmitted between network points. Nodes take turns, but nodes with more to send can take longer turns protocol is used to define the order in which stations are send

c. Size of MAC address

This 48-bit address space contains potentially 248 (over 281 trillion) possible MAC addresses. The IEEE manages allocation of MAC addresses, originally known as MAC-48 and which it now refers to as EUI-48 identifiers. The IEEE has a target lifetime of 100 years (until 2080) for applications using EUI-48 space and restricts applications accordingly. The IEEE encourages adoption of the more plentiful EUI-64 for non-Ethernet applications.

2. 2 dimensional data bit rate is as follows.

a.

1	0	1	0	0	1	0	1	0

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

b. Find below

Data – 10101101

G - 1001

Calculation of CRC using : 010

Data new – 10101101**010**

G -> 1001 -> $2^3 + 1$ -> Degree 3

Therefore appending 3 zeros and dividing by G.

Answer – 10111010

C. Finding the probability

After the 4th collision = $2^4 = 16$

We have to chose K= 3

Subset = {1,2,3,4,5,……..16}

Probability of K= 3,

Probability = 1/16 = 0.0625

Percentage = 6.25%

3. CRC errors

a. In the given question, P(X) = $X^4 + X^3 + X^2 + 1$, Hence the CRC key generator = 11101

We append four 0's to our 11Bit sequence so that it becomes a 15bit sequence.

Our new sequence is - 101010111000000

XORing the given sequence and the generator:

11101| 101010111000000

11101

10000

11101

011011

11101

10011

11101

001100

11101

```
0010100
 11101
 010010
 11101
 011110
 11101
 00011
```

Using the CRC generator, we get CRC as 0011.

Therefore the data sequence that is transmitted is 101010111000011

b. To check whether the data received is correct or no, we check the remainder of this calculation.

   It should be a sequence of zeroes (The CRC key generator 11101 in this case is known to both sender and receiver).At the receiver side:

```
 11101|101010111000011
 11101
 010000
 11101
 011011
 11101
 0011011
 11101
 0011000
 11101
 0010100
 11101
 010011
 11101
 011101
 11101
 00000
```

   If the 9th data bit is changed we won’t get the remainder as zero. Calculation is follows:

```
 11101|101010110000011
 11101
 010000
 11101
 011011
 11101
 0011010
 11101
 0011100
 11101
```

000010011
11101
01110 (which isn't a sequence of 0')

With this technique the receiver is able to detect whether any error is there in the data bit stream.

4. In CSMA/CD, the contention interval time should at least be 2t slot width, where 't' is time for signal to propagate between two farthest signals. This will acknowledge the station for successful transmission.
   The time 2t should be enough for the front of the frame to reach the end of the cable and then for an error message to be sent back before the entire frame is transmitted.
   As a result for a 100 km cable the one way propagation time = 1/500000
   = 20 x 10^-6
   = 20 µsec
   For two ways = 2 x 20 µsec = 40 µsec
   At 100 Gbps, all frames shorter than 4x106 bits can be completely transmitted in under 40 µsec, so the minimum frame is 4x10^6 bits or 500000 bytes.
   This can be shown using the following calculations:
   1011 bps x 40 x 10^-6 sec = 4 * 106 bits
   In terms of bytes, 4 * 106 bits / 8 = 500000 bytes

5. Question
   a. Propagation delay from A to B
      The propagation delay will be given by the propagation delay between A and B plus the repeater
      days between the nodes. This is given by the following:
      1000m/2*108 m/sec + 4* 33 bits/108 bps = **6.32 * 10^{-6} seconds.**

   b. Transmission time = 1500bits/(100*10^6bps)
      = 15*10^{-6} seconds
      This will be more than the propagation time.
      At time = 0, both A and B will transmit. At time t = 6.32 microsecond, A and b detect collision and abort. A picks up K = 0 and waits for the channel to become idle. At time t = 12.64 microseconds, last bit of B arrives at A, and A retransmits at the same time. At time t = 18.96 microseconds, A finishes transmission. At time t = (18.96 + 15) microseconds, last bit from A arrives at B.
      Hence packet from A is completely delivered to B at **time t = 33.96 microseconds**.

   c. If the repeaters are replaced by switches, the channel will be divided into 5 segments by the switches.
      The propagation delay between a host and switch = (1000/5) / (2*10*^8) = .1 microsecond.
      The transmission time of a single frame = 1500 / 100*10^6 = 15 microseconds.

The processing delay = 20 / 100 * 10^6 = 0.2 microseconds. The delay at each switch = 15 + 0.2
= 15.2 microseconds. Total delay introduced by all 4 switches = 15.2*4 = 60.8 microseconds
Therefore the packet from Node A is completely delivered to Node B in: (60.8 + 15 + .1) microseconds = **79.9 microseconds**

6. A bridge is used to interconnect two LANS. If both the Lans use the same underlying protocol, the bridge need not do any protocol conversion.
   However if the two Lans run different set of Protocols, the bridge needs to do the protocol conversion. A bridge receives and sends three different types of packets in each port: user terminals data frames from the connected Lans; control packets such as token used for the operation of certain LAN technologies; such as token ring; and bridge protocol data unit; which is protocol for communication among different bridges. Each bridge has a separate MAC address to connect to different LANs. The functionality of the bridge is to learn about the terminals connected to each port, forward frames to appropriate ports, filter unwanted frames, execute routing algorithm and convert the MAC and PHY layer of the packets to fit the associated LAN technology connected to each port.

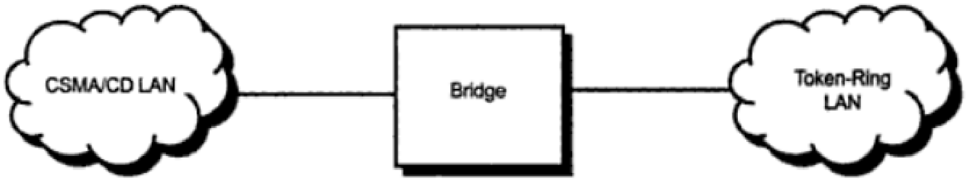
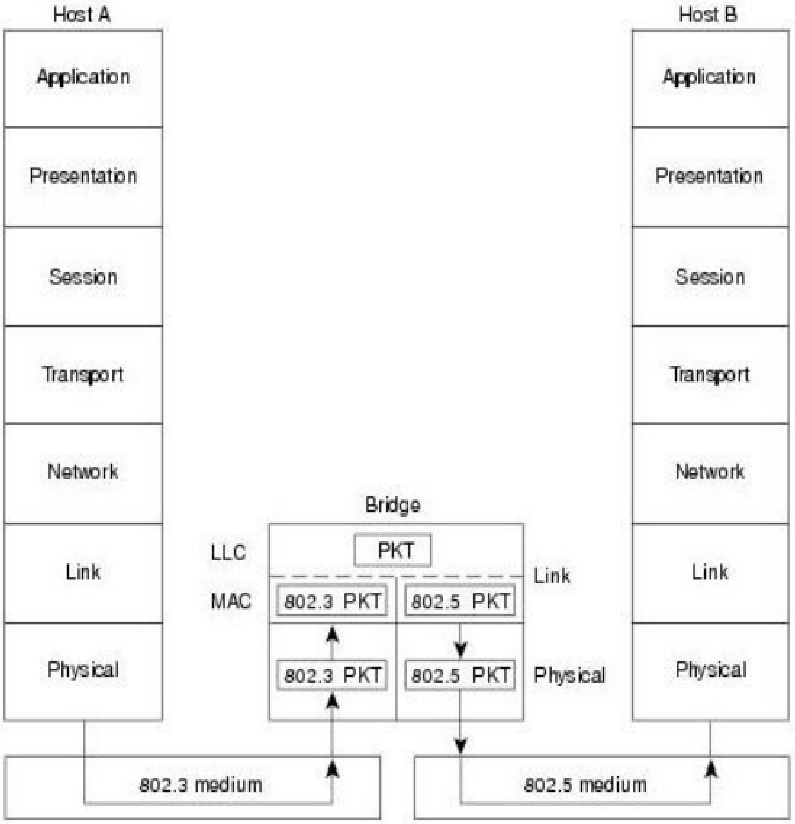
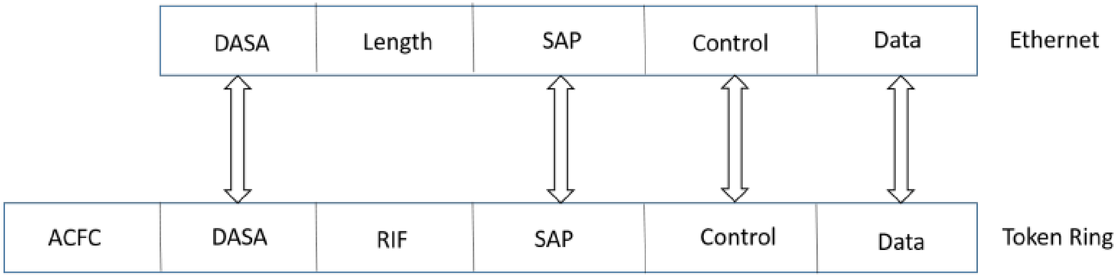


Figure: A MAC-Layer Bridge Connects the IEEE 802.3 and IEEE 802.5 Networks



The above figure illustrates an IEEE 802.3 host (Host A) formulating a packet that contains application information and encapsulating the packet in an IEEE 802.3-compatible frame for0 transit over the IEEE 802.3 medium to the bridge. At the bridge, the frame is stripped of its IEEE 802. header at the MAC sublayer of the link layer and is subsequently passed up to the LLC sublayer for further processing. After this processing, the packet is passed back down to an IEEE 802.5 implementation, which encapsulates the packet in an IEEE 802.5 header for transmission on the IEEE 802.5 network to the **IEEE 802.5 host (Host B).**

Four fields remain the same in frame conversion between IEEE 802.3 Ethernet and Token Ring. The destination and source addresses (DASA), service-access point (SAP), Logical Link Control (LLC) information, and data are passed to the corresponding fields of the destination frame. The destination and source address bits are reordered. When bridging from IEEE 802.3 Ethernet to Token Ring, the length field of the IEEE 802.3 Ethernet frame is removed. When bridging from Token Ring to IEEE 802.3, the access-control byte and the RIF are removed. The RIF can be cached in the translational bridge for use by return traffic.



A bridge's translation between networks of different types is never perfect because one network likely will support certain frame fields and protocol functions not supported by the other network. Bridges cannot maintain the integrity of data transmission in the case of received errors. For example suppose there is a error in one frame and that frame is not transmitted properly the bridge will not give any acknowledgement to retransmit that frame. If the bridge becomes congested the frames can be discarded to make the traffic smooth. On the other hand the bridges are easy to implement and no need to configure them.

7. Then Link Layer Frame is given by:

Source Mac Address	Destination Mac address	Source IP address	Destination IP address	Source Port	Destination Port	Data	CRC

a. The link layer frame created by the application on A: Here the destination will the MAC address of Router R, since the data is first being sent to Router R before sending it to the next Subnet.

(Source Mac Address) aa	(Destination Mac address) dd	(Source IP address) 1.1	(Destination IP address) 2.2	(Source Port) 2401	(Destination Port) 1608	(Data) HELLO	(CRC) Checksum

b. The link layer frame when it leaves R:
This is transmission of data between two routers. The Destination Mac address will be the Mac address of S. Here a forwarding table is used to decide the frame path. The Source Mac Address will be the address of Router R itself.

(Source Mac Address) gg	(Destination Mac address) hh	(Source IP address) 1.1	(Destination IP address) 2.2	(Source Port) 2401	(Destination Port) 1608	(Data) HELLO	(CRC) Checksum

c. The link layer frame when the data leaves S:
Using the forwarding table, the Mac Address of S is used as the Source Mac Address and Destination Mac Address will be the Address of E.

(Source Mac Address)	(Destination Mac address)	(Source IP address)	(Destination IP address)	(Source Port)	(Destination Port)	(Data)	(CRC)
kk	ee	1.1	2.2	2401	1608	HELLO	Checksum

8. Top-down approach to networking.
   a. No. E can check the subnet prefix of Host F's IP address, and then learn that F is on the same LAN segment. Thus, E will not send the packet to S2.
   Ethernet frame from E to F:
   Source IP = E's IP address
   Destination IP = F's IP address
   Source MAC = E's MAC address
   Destination MAC = F's MAC address

   b. Yes, E perform an ARP query to find B's MAC address. It so because E would like to find B's MAC address. In this case, E will send an ARP query packet with destination MAC address being the broadcast address

   This query packet will be re-broadcast by switch 1, and eventually received by Host B.
   Ethernet frame from E to S2:
   Source IP = E's IP address
   Destination IP = B's IP address
   Source MAC = E's MAC address
   Destination MAC = broadcast MAC address: FF-FF-FF-FF-FF-FF

   c. Assuming Host A would like to send an IP datagram to Host B, and neither A's ARP cache contains B's MAC address nor does B's ARP cache contain A's MAC address Switch S1 will broadcast the Ethernet frame via both its interfaces as the received ARP frame's destination address is a broadcast address. And it learns that A resides on Subnet 1 which is connected to S1 at the interface connecting to Subnet 1. And, S1 will update its forwarding table to include an entry for Host A.
   Yes, router S2 also receives this ARP request massage, and S2 will broadcast this query packet to all its interfaces. B won't send ARP query message asking for A's MAC address, as this address can be obtained from A's query message.

9. Delays in packet.
   a. **Packetization delay**
      The time required to fill the bits in terms of L is.
      L * 8 /(128*10^3) sec = L/16 msec

   b. **For L = 1,500, the delay in packetization,**
      1500/6 msecs = 93.75 msec.

      For L = 50, the packetization delay is
      50/16 msecs = 3.125msec

   c. Store and forward delay = L*8 + 40/ R
      For L = 1500, the delay calculated is
      (1500*8)+ 40/ (622 *10^6) = 19.37 microseconds

      L=50, store and forward delay is <1 micro seconds

   d. Store and forward delay is small for both the cases with typical link speeds. As we witnessed that the packet size of L=1500 was too large and the delay was subsequently larger than compared to a packet size of L = 50.
      From the above we can conclude our case to use a small packet size for transmissions as it warrants shorter delay time.

10. Email and Video distributions.
   a. Both email and video application uses the fourth rack for **0.1 percent** of the time.
   b. Probability that both applications need fourth rack is 0.001*0.001 = 10^{-6}
   c. Suppose the first three racks are for video, the next rack is a shared rack for both video and email, and the next three racks are for email. Let's assume that the fourth rack has all the data and software needed for both the email and video applications. With the topology of Figure 5.31, both applications will have enough intra-bandwidth as long as both are not simultaneously using the fourth rack. From part b, both are using the fourth rack for no more than .00001 % of time, which is within the .0001% requirement.

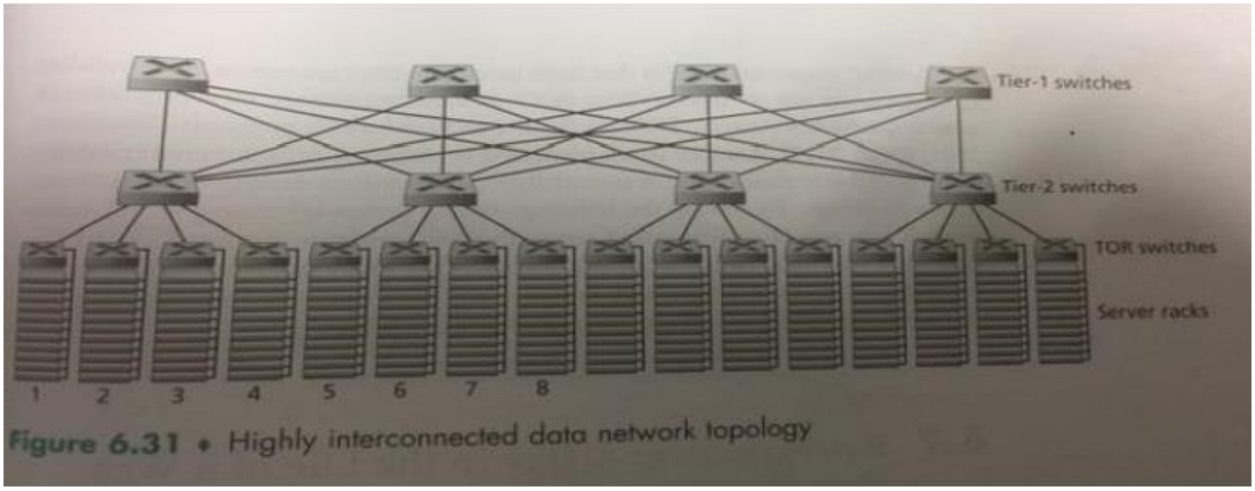


Figure 6.31 • Highly interconnected data network topology