Homework 1

Name – Sati, Ankit Date – 9/14/2021

Section – 001

SID – as14128

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

Answers

1. Delays
   a.
      - Packet switching Delay – Sending one packet from source to destination over a path consisting on N links each at rate R. The delay is mentioned below

      D = Delay
      N = number of routers/links (store and forward transmission)
      L = no of bits
      R = bits per second

      Total end to end delay – Td
      Processing delay - Pr
      Queuing Delay – Q
      P – Propagation delay(L = length of bits, R = transmission rate) = L/R
      T – Transmission delay (d = length of physical link, c=speed of light) = d/s

      Td = n(Pr +Q+P+T)

      - Circuit switching Delay - There are a total of 3 causes of delay in the circuit switched networks in a single hop.

      S – Setup delay
      P – Propagation delay(L = length of bits, R = transmission rate) = L/R
      T – Transmission delay (d = length of physical link, c=speed of light) = d/s
      Circuit delay at a node = S+P+T

      Multiple hops
      N – hops
      Pr- Process time
      Delay =N*(Pr+P) +T

   b. A few network variables that are taken as constants are
      - Global ISP – until and unless there is a major change for the provider the Global ISP will never change. It is one of the largest network blocks and is generally taken as a constant.
      - Categories of ISP – International (1), National(2), State(3). These remain constant. (for eg) If there is a new regional ISP it will be imposed upon the original State ISP.
      - Protocol Stack – The stack models are pretty standard. They can differ from each other slightly but most of the properties are same. New protocols are imposed upon the existing stacks.
      - Range - The range of various technologies such as Wifi6 and 5g remains constant. Best examples is of network satellites which always sit at an equal distance from earth.
      - Finally the IPv4 Settings – Although in some cases IPv6 is out but IPv4 is still taken as an constant due to hardware ability

2.

a. Few IOT protocols that are being used today
   - Data-Distribution Service (DDS)
   - Advanced Message Queuing Protocol (AMQP)
   - Bluetooth
   - ZigBee
   - Extensible Messaging and Presence Protocol (XMPP)
   - Constrained Application Protocol(CoAP)

b. IOT has created a lot of problems and opportunities in the field of networking. However the sudden increase in the number of devices has created more problems than solutions in the field of networking, The biggest difficult is the **implementation** and **scalability** on the existing **OSI model**. Bluetooth is a common example as it does not fit in the existing network stack and there are many other protocols like this.

   Solution 1– Most of these protocols operate in the network layer (Layer 3) We can use a probabilistic approach with a learning algorithm so that we can make things a bit easier for the system for every new occurrence.
   Solution 2 – Just Keep adding new protocols to the stack for every new IOT technology so that they can be a part of the network.

3.

a. The key difference between the two protocols are.
   - OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
   - In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
   - TCP/IP more credible than OSI, making greater utilization of bandwidth.
   - The OSI has seven layers while the TCP/IP has four layers.
   - OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.

b. Almost all the network models use the Layered model approach in order to facilitate all the required operations in a network. Each of these layers has a specific function and a communication scope which gives the network model stability and makes it easier to understand.
   - Advantages
   - It is a layered framework for the design of network systems.
   - It is easy to add multiple network models in a proper way.
   - It prevents changes in one layer from affecting other layers.

   - Disadvantages

- It is very complex to understand and manage the models since there are many new protocols added.
- Less privacy and easy to access.
- Due to the complexity of layered model, the first implementations were pretty heavy and slow.
- With the new devices being launced every day, it becomes very difficult to place them in the already defined models.
- Many real time operations are hindered as there might be many routes and models that can be followed. In some extreme cases, we might even need a new stack.

4.

a. Segmentation in IPv4
   This means that the packets were broken down to smaller parts in IPv4. This was done in order to reduce the load on the link layer and passing the smaller segments which would result in a reduced **MTU**. This took care of the biggest setback in layered stack and had separate host and data address.
b. Difference between Encapsulation and Segmentation.
   As discussed above, Segmentation is a simple process of breaking up the packets into smaller parts. As a result of this we get a reduced MTU and an increased efficiency.
   In the case of **Encapsulation**, we need to go a step beyond and wrap up all the data. This is done with the help of a header which contains the location to which a specific packet needs to be sent. This makes it certain that the data will be delivered to the location that is present in the header.
c. Disadvantages of Segmentation
   - Segmented packet drops caused due to order– Since the packets have been broken down into smaller pieces without a header, they might end up getting dropped if they do not reach the destination in order. This will impact the entire Packet as discussed in the next point.
   - Entire Packet loss – As mentioned above, if due to any reason a single data set of a packet is lost then we will have to send that entire packet again. This will increase the overlay and brings us to our next point.
   - Overlay – If the packets are dropped and sent again and again, this will create a **bottleneck,** which means that the throughput of the network will be decreased.
   - Packets can also be dropped if they are missing a critical data set that is arriving late which adds to all the above cases.

5. RFC 2026
   a. All so-called Internet standards are published as RFCs, but only a small fraction of RFCs are standards. RFCs are a collection of documents which describe various actual and suggested practices relevant to the Internet. The collection is heterogenous both as regards to the topic

of a document and as regards to its status. Most RFCs deal with technical arrangements and conventions, often called protocols.

RFCs cover a wide range of topics in addition to Internet Standards, from early discussion of new research concepts to status memos about the Internet.

b. No, Html was not standardized in the beginning by IETF as several drafts were expired. Later when RFC 1866 was published, HTML received its standardization by IETF and is maintained by W3C.

c. Number of RFC
   - TCP =14
   - UDP = 3

     There are multiple versions of these RFC because they need to be updated from time to time. As soon as there are major changes in the older version RFC, a new version takes its place.

6.

a. In wireless constraints there are situations where you will need a steady connection of data for a long duration. Also there are situations especially real time situations that require a sudden burst of data. In conclusion, Irrespective of the constraints, if the network demands a steady connection without any packet loss – use circuit switching. For any operation that requires real data bursts, use the packet switching as there will be no waste of bandwidth.

b.
   - Circuit switching over packet switching

     . Communication over switches in a data center - The communication between the severs and enterprise storage devices happens through switches where an IP is always established as the packets can never be dropped.

     . Any medical or banking transactions where the end users cannot loose the critical packets happen over circuit switching. A network needs to be established in order to secure the packets.
   - Packet switching over circuit switching

     . Most application over the internet with packet switching as we want to utilize most of the bandwidth.

     .Surfing online videos and read ahead operations online are all done with packet switching.

c.

Network Utilization - utilization % = (data bits x 100) / (bandwidth x interval)

In case of circuit switched networks = L*100/(bandwidth x interval)

At a given time = Transmission time* 100 / (Transmission rate + Propagation time)

7.

Case 1

This is a very good example of using a TCP. Over here multiple number of droid basically mean a huge amount of **bandwidth** which can be used to send the packets again and again. Apart from

that we need to have a steady communication **without packet drops.** So it is better to use TCP as there are no packets that are lost moreover in the case if one of the packets is shot down, we can always send a new packet out since we have so much bandwidth.
In the case of one of the droids getting shot down, Luke should wait for the confirmation. In other words, TCP will be sending the packet again until the destination gives an acknowledgement. With the help of TCP, they can defeat the Empire.

Case 2

This is again a classic example of TCP. Whenever we are posed with a question of **reliability** of delivering a packet, we should always choose TCP. However in this case, we should use the modern day **(3 way handshake process).** This is a full duplex method that happens in 3 basic steps as listed below.

1. A----→-SyncToken----→B
2. A←-----SyncToken+ACK←-----B
3. A------→Full ACK----→B

As shown above first step will have the synchronization request and will keep on sending the packets until receives the acknowledgement. Apart from the acknowledgement it also receives another synchronization token from the other host. B will keep on sending the ACK token as well as the SYNC token again until it receives the final part of the acknowledgement. Once this is completed, we know that the handshake has been completed.

Now that the handshake has been completed, the two blue armies can prepare their attack exactly at noon and defeat the red army sitting in the valley.

B Humans vs network protocols.

In my opinion, in most cases the human protocols are much more advanced than the network protocols as they do not need to fit in a layered model. If the major protocols are followed correctly, humans can easily resolve many situations thrown their way. In the case of networks, a single new technology can change a lot of details and might not even fit in the existing layered model. Humans often change their protocols depending upon the situation but networks hold there protocols with great rigour. As we all know that in the end it has been the dream of networking protocols to incorporate the efficient human ways.

Having said that, humans and network protocols are not completely different. They all need a set of basic rules in order to survive in the society. The way we interact among different levels and send information to selective levels. Often before sending the new data bits we wait for some acknowledgement. And most importantly we both drop the packets after a specific amount of time.