Assignment #1 Solution

1. **Problem 1** – Modeling delay in a communications network:

(a) Identify and describe in ONE sentence the main components of delay in communications networks that use either of circuit or packet switching.

(b) Develop an equation for the end-to-end delay along a communications path including various routers (please consider circuit and packet switching separately as/if needed). The only constant that you may assume is that the speed of light in the given transmission medium is $2\times10^8$ m/sec. Identify each of the variables in your equation.

(c) If the distances between nodes were constant ($D$) and each node (end systems and routers are nodes) can transmit $R$ bits per second, what would the equation in (b) look like for both circuit and packet switching?

(d) In the Internet, which of these would you expect to remain constant and which of these would you expect to change. Explain (in one sentence).

Don’t look for an obscure answer – choose the most obvious answer.

- The numbers of ISPs
- The lease contracts across ISPs
- The number of levels of ISPs
- The number of routers in the Internet
- The distance between a ground station and a satellite in geosynchronous orbit.
- The size of IP packets transmitted in any given HTTP session (i.e., Web browser connected to Web server).
- The average round-trip time in any Internet based client server application (round-trip time is the interval between the time you send a request and the time that you receive a response).

**Sample Solution:**

a) The four components of delay in a communication delay are:

- Nodal processing: This is the delay that occurs at nodes due to the processing for bit errors and determining the output link.
- Queuing: This is the delay due to the packet waiting at output link for transmission.
- Transmission delay: This is the delay caused by the data rate of the link.
• Propagation delay: This delay is the amount of time it takes for the head of the signal to travel from the sender to the receiver over a medium.

b) The equations would be:

• Packet Switching:
  \[ \text{delay} = n \times (d_{\text{proc}} + d_{\text{queue}} + \left( \frac{l}{r} \right) + \left( \frac{d}{s} \right)) \]
  
  where \( n \) is the number of routers, \( d_{\text{proc}} \) is the processing delay, \( d_{\text{queue}} \) is the queuing delay, \( l \) is the packet length, \( r \) is the link bandwidth, \( d \) is length of physical link and \( s \) is the propagation speed \( (2 \times 10^8 \text{ m/s}) \).

• Circuit Switching:
  \[ \text{delay} = n \times \left( d_{\text{proc}} + \frac{d}{s} \right) + \frac{l}{r} \]
  
  where \( n \) is the number of routers, \( d_{\text{proc}} \) is the processing delay, \( l \) is the packet length, \( r \) is the link bandwidth, \( d \) is length of physical link and \( s \) is the propagation speed \( (2 \times 10^8 \text{ m/s}) \).

c) The equations would be:

• Packet Switching:
  \[ \text{delay} = N \times (d_{\text{proc}} + d_{\text{queue}} + \left( \frac{l}{r} \right) + \left( \frac{d}{s} \right)) \]

• Circuit Switching:
  \[ \text{delay} = N \times (d_{\text{proc}} + D/s) + l/R \]

d)  
  • The number of ISPs: This will change or increase since any firm can purchase bandwidth and provide internet services to its customers and act as a service provider.
  • The Lease Contracts across ISPs: This will change as lease contracts can be renewed, terminated or added as new vendors provide internet services.
  • The number of levels of ISPs: This will remain the same as new ISP’s will get added to the already existing tiers (International/National ISPs, Regional ISPs and Local ISPs).
  • The number of routers in the internet: This will change as more links keep getting created and will require more routers.
  • Distance between a ground station and a satellite in geosynchronous orbit: This would remain constant as the distance for a satellite to be in geosynchronous orbit is fixed at 42,164 km.
  • The size of IP packet transmitted in any given HTTP session: This would change as the standard transitions from IPv4 to IPv6.
  • The average roundtrip in any Internet based client server application: This would change because as delays in communication will decrease as new technologies keeps developing.

2. Problem 2 – Network Models:
(a) The OSI model was developed before the Internet and was developed by agreement by the US and European nations (CCITT), yet the Internet and its protocols is by far the dominant network technology on our planet. Why?

(b) List the major disadvantages with the layered approach to protocols

(c) How are the presentation and session layers implemented in the Internet?

(d) List the major disadvantages with the layered approach to protocols

Sample Solution:

a) The reason behind TCP/IP’s dominance over OSI can be summarized as a result of technical, political and economic reasons:

The reasons for the popularity of TCP/IP over the OSI are:

- TCP/IP answers an immediate, almost desperate need - data communications in heterogeneous networks - very well.
- It is relatively simple and robust compared to other alternatives.
- TCP/IP is bundled within Berkeley Software Distribution (BSD) UNIX. Hence, TCP/IP became the minimum networking capability for any vendor entering the market for scientific and engineering graphics workstations.
- Its available on virtually every hardware and operating system platform (often free, as its open source)
- Thus, it’s the lingua franca of the Internet.
- It’s more credible than OSI, making greater utilization of bandwidth at a lower cost.
- It supports multiplexing and being connectionless, supports more communication devices.
- Existence of Internet layer reduces error handling overhead on the transport layer with the help of intelligent hosts, thus increasing throughput and efficiency at the transport layer.

b) A layered architecture was chosen to design network models because it allows for specific services to be handled by the various layers in a high-cohesion and low coupling fashion. Each layer implements its highly cohesive functionality by using services provided by the layer directly below, which ensures low-coupling and an optimal architectural design. In addition, the functionality provided by each layer can be modified without requiring modifications to the overall system.

c) The presentation and session layer implementations are left up to the application layer. It’s up to the application developer to decide if a particular presentation or session layer service is needed and if it is the case that service should be implemented within the application layer.

d) The Major disadvantages with a layered approach to protocols include: processing overhead (as multiple services may be provided within the different layers to handle the same function such as security and need to be invoked separately to process and encapsulate/extract data as it passes through the various layers on the sending and receiving ends), data overhead (as headers get added in various layers to encapsulate the data coming from the layer above on the sending side), and each layer uses its own protocols and related standards that keep evolving, which must be maintained, learned, and may lead to possible conflicts across various protocol stack implementations.

Problem 3 – Segmentation:
(a) What is segmentation? What other terminologies (than “segmentation”) are used in networking to refer to the “chunking” of packets?

(b) Why do we need it?

(c) What is the effect of segmentation on application messages encapsulation?

(d) Is segmentation restricted to the network layer, or might it be required at other layers? Why? Include the application layer in your answer.

(e) What effect do you think segmentation has on the following:

   1. Reliability
   2. Throughput
   3. Time to resend damaged transmission.
   4. Flexibility (ease with which we can adapt to new lower layers)
   5. Congestion
   6. Medium sharing
   7. Packet Drops

**Sample Solution:**

a) Dividing of the datagram/packet into smaller fragments is referred to as “Segmentation”.

b) So that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size.

c) It renders application message encapsulation more complex as it has to re-assemble the message chunks into their original order. Message encapsulation adds header to packets that contains information about where the packet needs to travel. Segmentation creates several small packets from one large data packet. So there is more effort required to encapsulate all the resulting packets on both the sending and receiving ends.

d) At present, segmentation is restricted to the network layer. Application layer cannot determine the packet size which can be sent on network. Therefore, it should restrict itself to the message passing.

e) Segmentation has the following effects:

   1. **Reliability** - If the IP fragments are out of order, a firewall may block the non-initial fragments because they do not carry the information that would match the packet filter. This would mean that the original IP datagram could not be reassembled by the receiving host, thus endangering reliability.
   2. **Throughput** - decreases overall speed because of associated overhead. Reassembly is very inefficient on a router whose primary job is to forward packets as quickly as possible.
   3. **Time to resend damaged transmission** - If one fragment of an IP datagram is dropped, then the entire original IP datagram must be resent, and it will also be fragmented, therefore takes considerably longer time to resend damaged transmission.
   4. **Flexibility (ease with which we can adapt to new lower layers)** - It increases flexibility as it provides a solution to the use of different maximum packet sizes by splitting the datagrams that originally did not fit into the packet size of the lower layer to be traversed, and to coalesce the pieces at the receiving node.
5. **Congestion** - It reduces congestion under normal operational conditions as smaller data packets seek out the most efficient route as links become available. Each packet may go a different route; each packet header address tells it where to go and drive the sequence of actions that allows reassembly at the destination.

6. **Medium Sharing** - With segmentation, the medium can be shared more effectively by multiple senders while allowing full usage of the existing bandwidth available on all transmission paths. Each sending node takes up little or none of the capacity when idle, and can utilize the entire capacity if transmitting while all other users are idle.

7. **Packet Drops** - It reduces packet drop as congestion is reduced and control flow made easier with segmentation.

**Problem 4 – IETF Standards:**

Go to [www.ietf.org/rfc.html](http://www.ietf.org/rfc.html) and look up RFC 2026 and read it. Answer these questions:

(a) What is an Internet Draft?

(b) What are the differences between a Proposed Standard, Draft Standard, and Standard?

(c) Was HTML standardized by IETF? Why or why not?

(d) How many RFCs are there for TCP and UDP?

(e) Why is it the case that multiple RFCs were submitted for TCP?

**Sample Solution:**

a) An Internet Draft is a series of working documents published by the IETF. Typically, they are drafts for RFCs, but may be other works in progress not intended for publication as RFCs. During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF’s Internet-Drafts directory. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision.

Internet-Drafts have no formal status, and are subject to change or removal at any time; therefore they should not be cited or quoted in any formal document.

b) What are the differences between a Proposed Standard, Draft Standard, and Standard?

<table>
<thead>
<tr>
<th></th>
<th>Proposed Standard</th>
<th>Draft Standard</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>The entry-level maturity for the standards track is &quot;Proposed Standard&quot;. A specific action by the IESG is required to move a specification onto the standards track at the &quot;Proposed Standard&quot; level.</td>
<td>A specification from which at least two independent and interoperable implementations from different code bases have been developed, and for which sufficient successful operational experience has been obtained, may be elevated.</td>
<td>A specification for which significant implementation and successful operational experience has been obtained may be elevated to the Internet Standard level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>elevated to the &quot;Draft Standard&quot; level.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2)</td>
<td>A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well-understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable.</td>
<td>A Draft Standard must be well-understood and known to be quite stable, both in its semantics and as a basis for developing an implementation.</td>
<td>An Internet Standard (which may simply be referred to as a Standard) is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.</td>
</tr>
<tr>
<td>3)</td>
<td>Further experience might result in a change or even retraction of the specification before it advances.</td>
<td>A Draft Standard is normally considered to be a final specification, and changes are likely to be made only to solve specific problems encountered.</td>
<td>All specifications unconditionally accepted.</td>
</tr>
<tr>
<td>4)</td>
<td>Usually, neither implementation nor operational experience is required for the designation of a specification as a Proposed Standard. However, such experience is highly desirable, and will usually represent a strong argument in favor of a Proposed Standard designation.</td>
<td>The requirement for at least two independent and interoperable implementations apply to all of the options and features of the specification. In cases in which one or more options or features have not been demonstrated in at least two interoperable implementations, the specification may advance to the Draft Standard level only if those options or features are removed.</td>
<td>Has cleared requirements of both Proposed and Draft and beyond.</td>
</tr>
</tbody>
</table>
5) It is desirable to implement them in order to gain experience and to validate, test, and clarify the specification. However, since the content of Proposed Standards may be changed if problems are found or better solutions are identified, deploying implementations of such standards into a disruption-sensitive environment is not recommended.

In most circumstances, it is reasonable for vendors to deploy implementations of Draft Standards into a disruption sensitive environment.

Completely acceptable to run in a disruption sensitive environment.

6) A Proposed Standard should have no known technical omissions with respect to the requirements placed upon it. However, the IESG may waive this requirement in order to allow a specification to advance to the Proposed Standard state when it is considered to be useful and necessary (and timely) even with known technical omissions.

In cases in which one or more options or features have not been demonstrated in at least two interoperable implementations, the specification may advance to the Draft Standard level only if those options or features are removed.

All features have been time tested.

c) HTML was not standardized by IETF. Several draft relating to HTML expired but IETF established HTML working group, which published RFC 1866 – HTML 2.0 as a standard. HTML received international standard in 2000 when it was maintained by W3C.

d) The number of standardized RFCs for TCP and UDP are as follows:
   1. TCP – 10 Standardized RFCs
   2. UDP – 3 Standardized RFCs.

e) Multiple RFCs were submitted for TCP to improve performance and transaction oriented services. Newer RFCs may render (part of) older RFCs obsolete (e.g., RFC 835 replaces RFC 834).

**Problem 5 – Packet vs. Circuit-Switched Communications:**

(a) You are about to receive the world’s first telemetry controlled electronic heart. Since you don’t want to be encumbered by wires, you choose the WiFi9000 model over the ONOaWiRe1000 model. You will notice in the brochure that both models can be configured for circuit-switched and packet switched communications – which do you specify? Why?

What kinds of service guarantees would you hope to have?
(b) Consider an application that transmits data at a steady rate (e.g., the sender generates an N-bit unit of data every k time units, where k is small and fixed). Also, when such an application starts, it will continue running for a relatively long period of time. Would a packet-switched network or a circuit-switched network be more appropriate for this application? Why?

(c) How would you measure overall network paths utilization in circuit-switched communications (describe a model that could be implemented to generate an utilization percentage at all times)?

Sample Solution:

a) Specify circuit switched communication:

The reason is that it establishes a dedicated end-to-end connection and once a link is established, it is solely used by the single connection, in this case the link to the telemetry controlled electronic heart which guarantees consistent performance. This is unlike Packet Switching where the resources are not reserved but accessed on demand, and as a consequence the transmission may have to wait. This is unacceptable for a device like the electronic heart which needs to run non-stop.

The service guarantees that I hope to have are as follows:

- Once established, continuous network availability.
- Increased performance as there is no delay or waiting.
- Reliability due to reserved resources.
- No loss of packets as there is no delay.

b) A circuit-switched network would be well suited to the application described, because the application involves long sessions with predictable bandwidth requirements. Since the transmission rate is known and predictable, bandwidth can be reserved for each application session circuit to reduce waste. Additionally, the overhead costs of setting up and tearing down circuit connections is short compared to the average duration of an application session.

c) Overall network paths utilization in circuit-switched communications is obtained as follows:

\[
\left(\frac{\text{Transmission time}}{\text{Transmission Time} + \text{Propagation Time}}\right) \times 100
\]

Problem 6 - Protocols:

(a) You and Luke Sky Walker are commanders in the rebel army preparing to attack Darth Vader and his Death Star. By yourselves, neither you nor Luke possesses enough fire power to defeat Darth Vader, but together you can destroy the Death Star. However, you must come to agreement on the precise moment to attack, but you cannot communicate using the normal communications else your presence and location will be detected by Darth Vader. But you each possess an unlimited number of R2D2 messenger droids that you can use to send messages to each other. But, the droids may be destroyed by the enemy’s PatrolBots, so you have no way of knowing if your message gets through unless Luke sends a droid back to you with a confirmation message. Suppose your droid gets through to Luke and Luke sends a droid back to you with a confirmation message agreeing to the time to attack, but it is destroyed by a PatrolBot? Should he attack? You haven’t received a confirmation, so what will you do?
Is there a protocol that you and Luke can use to avoid defeat? If not, explain why not. If there is a protocol that would work, please explain it.

(b) Two blue armies are each poised on opposite hills preparing to attack a single red army in the valley. The red army can defeat either of the blue armies separately but will fail to defeat both blue armies if they attack simultaneously. The blue armies communicate via an unreliable communications system (i.e., a foot soldier). The commander of one of the blue armies would like to attack at noon. However, if he sends a message to the other blue army ordering the attack, he cannot be sure that the message will get through. He could ask for acknowledgement but that might not get through either. Is there a protocol that the two blue armies can use to avoid defeat?

(c) Formalize the protocols in (a) and (b) above using an Event-Condition-Action (ECA) architecture (i.e., name the corresponding events, conditions, and actions associated to the two protocols)

(d) Explain the main differences between human and network protocols? Is comparing the two a viable metaphor/analogy, why or why not?

Answer:

a) The Transmission Control Protocol (TCP) may be used to avoid defeat in this scenario. TCP enables two hosts to exchange data after establishing a connection. It also guarantees in-order delivery of data packets. In the event where a droid is lost, the TCP layer will attempt to resend packets until it receives a confirmation that they have reached the destination.

b) The problem may be solved by using the approach taken by TCP when setting up a connection. TCP uses a Three Way Handshake to establish a connection as follows:

1. **SYN:** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value $A$.
2. **SYN-ACK:** The server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (i.e., $A+1$) and the sequence number that the server chooses for the packet is another random number $B$.
3. **ACK:** The client sends an ACK back to the server. The sequence number is set to the received acknowledgement value (i.e., $A+1$), and the acknowledgement number is set to one more than the received sequence number (i.e., $B+1$).

At this point, both the client and server have received an acknowledgment that the connection has been established. Steps 1 and 2 establish the sequence number as a connection parameter in one direction and allow its acknowledgement. Steps 2 and 3 establish the sequence number as a connection parameter in the other direction and allow its acknowledgement. Both steps allow the establishment of a full-duplex communication.

c) Sample ECA rule set:

```
RULE <R1> [(I, Luke L, Droid D)]
  WHEN <Attack>
  IF <I sends D to L for attack>
  THEN <Wait for confirmation from L>
  IF <D conveying attack message is destroyed by PatrolBots>
  THEN <do not attack and resend the D containing the Attack message>
ENDRULE <R1>

RULE <R2> [(I, Luke L, Droid D)]
```
WHEN <Attack>
 IF <L sends D to I for attack>  
 THEN <Wait for confirmation from I>  
 IF <D conveying Confirmation message is destroyed by the PatrolBots>  
 THEN <do not attack and resend the D containing the Attack message>  
 ENDRULE <R2>

RULE <R3> [(I, Luke L, Droid D)]
WHEN <Attack>
 IF <I send D to L for attack>  
 THEN <Wait for confirmation via D from L>  
 IF <I get confirmation via D from L>  
 THEN <send D for acknowledgement of confirmation>  
 IF <the D conveying confirmation acknowledgement is destroyed by the enemy’s PatrolBots >  
 THEN <do not attack and resend the D containing the attack message>  
 ENDRULE <R3>

RULE <R4> [(I, Luke L, Droid D)]
WHEN < Attack>
 IF <I send D to L for attack>  
 THEN <Wait for confirmation via D from L>  
 IF <I get confirmation via D from L>  
 THEN <send D for acknowledgement of confirmation>  
 IF <L receives confirmation acknowledgement D from I>  
 THEN <attack>  
 ENDRULE <R4>

d) The primary difference between a human and network protocol is that human protocols are numerous and ambiguous as they may not follow any standards or rigor other than what is expected assuming good manners, which may be different in the various cultures. In most cases, human protocols guarantee acknowledgement. Network protocols are standardized and non-ambiguous. However, acknowledgements may be lost in transmission and may have to be resent. Comparing human and network protocol is a viable analogy because there are similarities between the way humans and network node interact and exchange information as both types of communications typically follow an Event-Condition-Action (ECA) model.