New York University
Computer Science Department
Courant Institute of Mathematical Sciences

Course Title: Data Communication & Networks   **Course Number:** CSCI-GA.2662-001
Instructor: Jean-Claude Franchitti   **Session:** 1

Assignment #1 Solution

I.   Due

Thursday September 21, 2017 at the beginning of class.

II.   Objectives

1. Learn basic networking concepts.

III.   References

1. Slides and handouts posted on the course Web site
2. Textbook chapters as applicable

IV.   Software Required

1. Microsoft Word.
1. Win Zip as necessary.

V.   Assignment

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

    (a) If the distances between all nodes in a network were constant (D) and each node (end systems and routers are nodes) could transmit R bits per second, what would the end-to-end delay equation look like for both circuit and packet switching? (The only constant that you may assume is that the speed of light in the given transmission medium is $2*10^8$ m/sec)

    Assume:
    n: number of routers
    dproc: processing delay
    dqueue: queuing delay
    l: packet length
    R: link bandwidth in bits per second
    D: length of physical link

s: propagation speed ($2*10^8$ m/s).

End-to-end delay equation for packet switching:

$$delay = n * (dproc + dqueue + (l/R) + (D/s))$$

End-to-end delay equation for circuit switching:

$$delay = n * (dproc + D/s) + l/R$$

(b) Give four examples of network variables (e.g., number of ISPs) that you expect to remain constant in the Internet and explain why in each case.

- 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).
- 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 number of layers in the Internet protocol stack: Changing the stack structure would require major changes to the end point operating systems and the network core devices, which would be cost prohibitive.
- Internet exchange points: the number of global ISPs will not change very fast.

2. Problem 2 – IoT Networks

    (a) Catalog the main IoT protocols in use today.

    MQTT, XMPP, CoAP, AMQP, DDS

    (b) Why is the proliferation of IoT protocols difficult to handle within the current Internet network stack and is there a solution to this issue?

    The proliferation of proprietary IoT protocols lead to a lack of interoperability that makes it difficult to handle scalability and solve common problems such as security. Standardization of IoT protocols is the only solution to this problem.

3. Problem 3 – Network Models:

    (a) What is the difference between the TCP/IP network and the OSI network model?

- The OSI model was developed before the Internet and was developed by agreement by the US and European nations (CCITT). The Internet TCP/IP network stack and its protocols is by far the dominant network technology on our planet.
- 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) Explain the main architecture heuristics that are used to design network models and elaborate on their advantages and drawbacks.

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.

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.

4. Problem 4 – Segmentation:

(a) Why was segmentation introduced in IPv4?

Dividing of the datagram/packet into smaller fragments is referred to as "Segmentation". It was introduced so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size.

(b) How does segmentation relate to encapsulation and where/when does it take place in the network?

Segmentation 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.

(c) Give examples of negative side effects of segmentation

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.

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.

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.

Positive effects of segmentation are as follows:

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.

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.

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.

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

5. Problem 5 – IETF Standards (www.ietf.org/rfc.html):

(a) What is RFC 2026 about?

RFC 2026 specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

More specifically:
- It documents the process used by the Internet community for the standardization of protocols and procedures.
- It defines the stages in the standardization process, the requirements for moving a document between stages and the types of documents used during this process.
- It addresses the intellectual property rights and copyright issues associated with the standards process.

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

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.

(c) How many RFCs are there for TCP and UDP and why is there multiple RFCs for each of these protocols?

The number of standardized RFCs for TCP and UDP are as follows:

1. TCP – 10 Standardized RFCs
2. UDP – 3 Standardized RFCs.

6. Problem 6 – Packet vs. Circuit-Switched Communications:

    (a) Is it preferable to use circuit-switched or packet-switched communication when operating in a wireless context? Please explain you answer as well as the service guarantee you would expect.

    It depends as to whether the data transmission is occurring at a steady rate and involves long sessions with predictable bandwidth requirements. In this case, circuit-switching is better suited. If data transmission is performed in bursts, packet-switched is best. This is true in both the wireless and wired contexts.

    (b) Give two examples of applications for which circuit switching and packet switching would be more suitable respectively.

    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). 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.

    Typical client-server applications developed for and used on the Internet operate by sending bursts over the network. Packet switching is well suited for this type of applications as it makes it possible to optimize the use of the overall network bandwidth available.

    (c) Describe a model that could be implemented to compute a utilization percentage at all times for overall network paths in circuit-switched communications.

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

    (Transmission time / (Transmission Time + Propagation Time)) * 100

7. Problem 7 - Protocols:

(a) Is there a general protocol that may be used and specialized (i.e., by you and Luke and by the two blue armies respectively) to avoid defeat in cases 1 and 2 below? If there is such a protocol, please use an Event-Condition-Action (ECA) architecture (i.e., name the corresponding events, conditions, and actions associated to the protocol)

Case 1: 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?

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.

Case 2: 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 attach 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.

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:

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.

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.

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.

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>

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

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 in the way humans and network node interact and exchange information as both types of communications typically follow an Event-Condition-Action (ECA) model.

a) Save the file as a Word document.

b) Name the file "**firstname_lastname_hw_#.doc**" (e.g., "john_doe_hw_1.doc").

c) Email your assignment file to the course grader, and submit a hard copy to the professor by the due date.

Use the following naming convention in the subject line of the eMail:
"**DCN - firstname lastname - homework #**" (e.g.: "DCN – John Doe - homework 1").

In the case source code is submitted, include your name as a comment at the top of each file
(Note: all files submitted should include your name).

VI.   <u>Deliverables</u>

1. Electronic:

Your assignment file must be emailed to the course grader. The file must be created and sent by the beginning of class. After the class period, the homework is late. The email clock is the official clock.

2. Cover page and other formatting requirements:

The cover page supplied on the next page must be the first page of your assignment file.

Fill in the blank area for each field.

<u>NOTE</u>:

The sequence of the hardcopy submission is:

1. **Cover sheet**
2. **Assignment Answer Sheet(s)**

VII.   Sample Cover Sheet:

Name _____ Date: _____
     (last name, first name)
Section: _____

Assignment 1

Assignment Layout (25%)

o Assignment is neatly assembled on 8 1/2 by 11 paper.

o Cover page with your name (last name first followed by a comma then first name), username and section number with a signed statement of independent effort is included.

o Answers to Questions 1 to 7 are correct.

o File name is correct.

Answers to Individual Questions:

(100 points total, all questions weighted equally)

o Assumptions provided when required.

Total in points (100 points total):   _____

Professor's Comments:

Affirmation of my Independent Effort: _____
                                         (Sign here)