CS 145 Lab Exercise 7
Wireshark Lab: TCP
A.Y. 2017-2018, 2nd Semester

1 Introduction

In this laboratory exercise you are going to explore the connection establishment procedure of TCP, as well as TCP's acknowledgement mechanism. As such, it would be helpful for you to review Lecture 10 (as well as Laboratory Exercise 1) before doing the laboratory exercise.

2 Restrictions

For this laboratory exercise the following restrictions apply:

- Trace file generation must be done in a DCS Teaching Laboratory machine, using the Ethernet (not WiFi) connection.
- Trace analysis may be done in any machine with the Wireshark software installed.

3 Instructions: Trace Generation

1. Start up a web browser, which will display your selected homepage.
2. Clear the browser's history - I assume that you already know how to do this. Also, throughout the exercise, avoid using multiple tabs, even if your browser is capable of tabbed browsing. That is, while doing the laboratory exercise, do **not** surf any other websites, as that would affect the trace that you would generate.
3. Start up the Wireshark software.
4. Select the appropriate interface and begin packet capture.
5. While Wireshark is running, enter the URL `http://xmpp.org/rfcs/rfc3920.html` and have the web page displayed in your web browser. Wait for the entire web page to load completely before proceeding to the next step.

6. Enter the URL `http://www.december.com/html/demo/hello.html` and have the web page displayed in your web browser. Wait for the entire web page to load completely before proceeding to the next step.

7. Stop packet capture.

8. Save the packet trace file as `labexercise7.pcapng`. You can use this if you wish to work on the laboratory report at a later time.

9. At this stage, you are now ready to work on the laboratory report.

4 What to hand in

Answer the following questions in the laboratory report, based on your Wireshark experimentation:

1. Filter out (remove) all non-TCP-related packets by applying the "tcp" filter. You should see among the remaining packets the HTTP GET and the HTTP OK messages associated with the website access transaction you made. HTTP transactions happen over a TCP connection (we will discuss more about this in the lectures) - before an HTTP GET message can be sent from your computer to the server, a TCP connection between your computer and the server must be established first. In the generated trace, identify the three segments associated with the *three way handshake*. Discuss the role of each segment. Do **not** just rely on Wireshark identifying/annotating a certain segment as the SYNACK or SYN - *justify* through the **TCP header fields** why the segment is the SYNACK, ACK, etc. Include annotated screenshots (I expect several) supporting your answer.

2. `rfc3920.html` is a *single* file. Was it sent from the server to your computer as a *single* segment? Include an annotated screenshot supporting your answer.

3. `hello.html` is a *single* file. Was it sent from the server to your computer as a *single* segment? Include an annotated screenshot supporting your answer.

4. How are the sequence numbers of the segments from the server to your computer determined? Are they always incremented by 1? That is, if there are three segments with the first one having the sequence number 28, would the second and third segments have the sequence numbers 29 and 30? Include annotated screenshots supporting your answer.

5. TCP provides reliable transport service. To provide reliable transport, it depends on acknowledgements. Based on the behavior of *your* computer (which is the client in the transaction) as it receives segments from the server, would you say that a TCP receiver acknowledges each and every segment that it receives from the sender *one-by-one*? Before answering this question, we suggest that you analyze the tracefile `Lab7Reference.pcapng` as well (it should be made available to you through the UVLE course webpage). Include an annotated screenshot supporting your answer.

6. What determines the sequence number of an acknowledgement packet? What does it (the sequence number) signify? Include an annotated screenshot supporting your answer.

Note: If the Wireshark software is still running, shut it down.

5 Submission

You can submit the laboratory report via UVLE. Deadline should also be posted in UVLE, along with this document.