BLG433E
COMPUTER COMMUNICATIONS
HOMEWORK2
"Network Analyzing with Wireshark "

Instructor: Prof. Dr. Sema F. OKTUG (oktug@itu.edu.tr)
Assistant: Res. Asst. Müge EREL ÖZÇEVİK (erelmu@itu.edu.tr)
Due Date: 03.12.2017 , 23:55

OBJECTIVES

The purpose of this homework is to give you experience on network analyzing with Wireshark tool. You will meet different protocol types, and performance metrics such as Throughput, Round Trip Time (RTT) and Window Size. Moreover, transport layer protocols will be compared according to their characteristics.

QUESTIONS

You are expected to answer the following questions with Wireshark screenshots:

1. **(25 Points) DHCP protocol analysis:**

   - Shortly explain DHCP stages and show the DHCP interaction between your device and a DHCP Server. To do this, firstly shut-down your Ethernet interface and bring it up. This should force your computer to get an IP address.

2. **(25 Points) DNS protocol analysis:**

   - Shortly explain DNS stages. To do this, type the address of a previously unknown website in your browser. Show each stage in Wireshark. What is the IP address of the DNS server, what is the IP address of the website?

3. **(50 Points) TCP-UDP comparison analysis:**

   Please build a scenario to compare TCP and UDP characteristics. There are two different traffics to analyze:

   - Foreground traffic (always TCP)
   - Background traffic (TCP or UDP)

   Please study on "iperf" to create TCP and UDP traffic flows that have following characteristics:

   - Flow duration: 10 sec
   - Bandwidth: **'B'** should be arranged according to your environment. (In case not seen any difference between following analyzes, please increase this metric.)
   - Packet length: 500bytes
   - The number of generated packets per flow: 100M

   For the following analyzes, please build I/O graphs including TCP and UDP packets by defining specific filter equations. 'B' is monotonously increased such as [B, B+a, B+2a, …]

Analysis 1:
Foreground traffic: TCP, bandwidth B
Background traffic: UDP, bandwidth initially equals to 'B' and it is monotonously increased in different runs.

Analysis 2:
Foreground traffic: TCP, bandwidth B
Background traffic: TCP, bandwidth initially equals to 'B' and it is monotonously increased in different runs.

The interpretation of the results:

- What are the protocol numbers of TCP and UDP (Please show them in a related packet headers)
- Despite having same circumstances in the analyzes, you are expected to observe less throughput (packets/s) for the foreground TCP traffic served by UDP background. Why? Please support your answer with performance metrics shown in Wireshark.

ORGANIZING YOUR SUBMISSIONS

The homework will be built individually. The report should be named with the student number. For example:"150120001.pdf". Please support your answers with screenshots taken from Wireshark and upload your report to Ninova.