Networking Labs

ECE

ING4 (SI)

2018/2019

TCP Study With Wireshark

Lab A

Nassim KOBEISSY

Session Requirements:

- At the end of the session do not forget to save your work into any available storage device (USB key for example).
- The different parts of this lab session are correlated. Execute the different steps sequentially.
- All the questions shall be answered and included in the report. Screen shots can be used in some cases.
- Each group (composed of 2 persons at most) shall submit a report.
- The report shall be uploaded on the campus page before:
  - 28/10/2018
  - Late reports will be penalized (2 points/day)
- **Only PDF format is accepted**
  - **3 points penalty for other formats**

Objective:

The goal of this lab is to analyze and understand the transport control protocol TCP and its features like connection management and flow control

For this purpose, a file transfer with FTP shall be performed and analyzed. At the end, you shall be able to understand and describe FTP and Telnet as well.

Prerequisites:

FTP server

1. Install FileZilla FTP server for windows
2. Create 2 user accounts from the FTP server interface. Let's call them **user1** and **user2**. These accounts will be used by your neighbors to access your FTP server.
3. For each account, attribute a password and define the set of shared folders that can be accessed as well as the permissions. Give all the permissions for one of them (super user).

FTP client

Check if FileZilla Client is installed on your machine or not. If not, please install it. It shall be used to access the FTP server for downloading and eventually uploading some files.

Wireshark

Check for a Wireshark installation on your machine. If it is not found, please install it. It will be used for analyzing a file transfer between the server and the client.

Procedure

1. Copy/create a big file (size about 5 MB) in the shared folder.
2. Launch the FTP server
3. Launch wireshark and capture traffic on Ethernet interface (or WiFi).
4. Launch Filezilla FTP Client
5. With FTP client connect to the FTP server of your neighbor using **user1** credentials (login, password) that he created for you.
6. Download the file into your machine.
7. When the download finishes, close filezilla and stop capturing. You have got the necessary frames for TCP analysis.

In the purpose of rendering the captured traffic easier to understand:

- Avoid downloading the file from your neighbor's FTP server while he is downloading his file from your FTP server. Schedule the transfers with your neighbor, one after the other.
- Capture only the traffic that corresponds to your download.

Analysis and Study (12 points)

1. Use a filter that displays only the frames that correspond to the file transfer.
2. Identify the connection establishment and connection release of this file transfer.
   - Capture and analyze the segments used for this purpose.
   - Identify the important flags, sequence and ACK numbers of these segments.
   - Give the IP and MAC addresses and TCP port numbers on both sides
   - Use a sequence diagram to illustrate the connection establishment and release
     a. You can use http://www.plantuml.com/plantuml/uml/
3. Identify the sequence numbers and size of the first 10 **data** segments sent.
4. Identify the segments that acknowledge the reception of these segments.
5. Are there any re-transmission? How can you know?
   a.
6. Display TCP time/sequence graph (Stevens) to illustrate the evolution of sequence numbers over time in both directions. Comment.
7. Determine the transmission time of the first 6 data segments and calculate the corresponding round-trip-time (RTT)
8. Give the RTT graph of the TCP connection in both directions (with Wireshark). Comment.
9. Study and analyze the impact of the receiver's buffer space on the sender (based on window size advertisement). Display the window scaling graph.
10. Display throughput graphs in both connection directions. Analyze.

FTP Understanding (8 points)

11. How many TCP connections are used to accomplish this data transfer (provide screenshots)? Give the source and destination port numbers for each connection
12. Create 3 text files on the FTP server in the shared folder. Start a new Wire shark capture on the network interface. Let the FTP client download these files at the same time. How many TCP connections are used for the transfer of these 3 files? Give the source and destination port numbers for each connection.
13. Are you able to read the content of the files with Wireshark? If it is the case, is it secure? Comment.
14. With a sequence diagram, explain FTP behavior:
    a. Show all the messages (commands and/or codes) exchanged for establishing connection with FTP server, authentication, listing and changing directories, requesting transfer (GET or PUT)…
    b. Data transfer
    c. Connection release

Annex

To force Wire shark to display information of TCP rather than FTP do the following:

- Click on ***Analyze***
- Select ***Enable protocols***
- Uncheck ***FTP***
- Click **OK**