IP LAB EXPERIMENT – 4 [CYS 2022 - 2024] 27-10-2022

(Note: Total 25 marks for this lab assignment which includes 20 marks + 5 marks for your report)

For each of the following steps, describe your results, give the syntax of the command you used, and, where appropriate, the output produced. Include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and answer each question in your report.

1. Open the pcap file “tcp” in Wireshark to answer the following questions.

a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
b. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Since this lab is about TCP rather than HTTP, let’s change Wireshark’s “listing of captured packets” window so that it shows information about the TCP segments containing the HTTP messages rather than about the HTTP messages. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the HTTP box and select OK.

c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
d. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
e. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.
f. Plot the RTT graph using Wireshark.
g. What is the length of each of the first six TCP segments (HTTP POST)?
h. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
i. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

2. Open the pcap file “udp” in Wireshark to answer the following questions

j. Select one UDP packet from your trace. From this packet, determine how many fields the are in the UDP header. Name these fields.
k. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
l. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

m. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.
n. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.