Wireshark for Network Layer

Capture and analyze the packet traces using the Wireshark to answer all the questions. Use appropriate filters, helper windows, properties in Wireshark. Place the screenshots of wireshark where appropriate inline to answers, as a proof of analysis in answering the question.

Task1: Ping to destination

Start the Wireshark packet sniffer and start capturing.
Open a terminal. Execute **ping -s 3500 ping-ams1.online.net -c 5**
Stop the wireshark capture and save the file for further analysis.

Answer the following using the captured trace file.

1. What does the above ping command do ?

2. How many total IP packets are exchanged in the communication between your host and the remote server representing **ping-ams1.online.net ?**

3. What is the size of each ping request sent from your host to remote server ?

4. Make a table for each ping request packet sent from your host to remote, the respective field indicating it, if the request packet is fragmented or not. If packet is fragmented (add details on number of IP fragments and on each fragment), Time of sending each individual fragment/packet, length of the individual fragment/packet), time of receiving ping response, the respective field indicating if response packet is fragmented or not, if response packet is fragmented, include the number of IP fragments, total actual length of data carried by the respective fragment in respective ping request and response.

5. Pick any fragmented ping request and response used in question #4. Explain how you find the length of actual data in individual fragments of the associated ping request and response ? Where is the total/final length of the respective ping request and response at IP level visible in Wireshark ?

6. In the saved file used for analysis, export only those IP packets involved in either direction (in communication) using appropriate Wireshark display filters and save it to another file to upload during submission.

Task2: Traceroute to destination

You will require **traceroute** software to execute this experiment. (If you don't have it already, install it using **sudo apt-get install traceroute**).

Start the Wireshark packet sniffer and start capturing. Open a terminal.
Execute **traceroute -q 5 ping-ams1.online.net 3500.**
Stop the wireshark capture and save the file for further analysis.

Answer the following using the captured trace file.

1. What is the IP address of **ping-ams1.online.net**?

2. How many hops are involved in finding the route to this **ping-ams1.online.net ?**

3. How many total IP packets are exchanged in the communication to get the final traceroute output of **ping-ams1.online.net**? How many of them are sent from client to remote machine (server/router) ? How many of them are sent from the remote machine (hop/server/router) to the local client ? Tabulate this with an entry for a router/server and the client too.

4. Why and how does the hop/router involved send the response to the packet sent by your client machine ?

5. Which upper layer protocol is used in sending the packet from local client to remote machine ? Which upper layer protocol is used in sending the packet from remote server/router to local client ? Identify within the protocol the type/name of this message (within the protocol) from server to client ?

6. Which fields in the IP datagram always change from one datagram to the next within this series of IP packets sent by your host/client ? Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

7. Describe the pattern you see in the values in the Identification field of the IP datagram both from client to server and hop/router/server to your client ?

8. Make a table with an entry for each request sent from your client/host, listing what is the value in the IP Identification field and the TTL field for the request and respective response (Include entries if the packet is fragmented). Do these values remain unchanged for all of the replies sent to your computer by the respective (hop) router? If yes why? If not why ?

9. Calculate the average RTT for each request sent by traceroute w.r.t its respective response (from the related hop) using the different IP fields and wireshark display filters. There shall be a proof of screenshot(s) showing this calculation for at least 1 packet with respective response(s). Plot a graph of hop name/IP address which sent the response versus the RTT using the calculations done.

10. Pick any packet from client towards server. Has this IP datagram been fragmented? Explain how you determine whether or not the datagram has been fragmented and where does the fragmentation end.

11. In the saved file used for analysis, export only those IP packets involved in either direction (in communication) using appropriate Wireshark display filters and save it to another file to upload during submission.

Task3 Ping versus Traceroute

1. Comment on your understanding of differences between traceroute and ping command executed for **ping-ams1.online.net** (in **Task1 and Task2**) using the respective wireshark traces. List the IP fields which indicate the differences in the behaviour of execution. Place at least 1 screenshot of wireshark from respective traces showing relevant display filters as a proof of explaining the difference.

Submission

Prepare a detailed **observation and analysis report** for listed questions with specific details asked in individual tasks along with **respective wireshark trace files (for what is being mentioned only in the final question of task1 and task2; Please don't upload the entire trace file captured)**. Zip all these files into a single zip file **<assignment5_roll no>.zip** and submit to google classroom in the posted assignment section.

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name of the student
Roll No