IIT Goa CS212 (Computer Networks LAB)
Instructor: Neha Karanjkar

LAB 1: Basic Networking Tools and Wireshark

Instructions:

- This is an INDIVIDUAL lab. Sharing solutions will be considered as plagiarism. Directly copying/pasting solutions from the web will also be considered as plagiarism. You can use the web for information but write the solutions in your own words.
- Submit the solutions as a brief report in pdf format. Clearly state the corresponding question numbers for each answer.
- The report must be named: LAB1_<NAME>.pdf where NAME is exactly how your name appears on Google Classroom in capitals. Eg: "LAB1_RAHUL_KUMAR.pdf"

PART 1: IP, PING and TRACEROUTE commands

1. **[1 marks]** Read up about the `ip` command in Linux, in particular the `ip addr show` command. You should have a rough understanding of what this command does, what are its options, and how to interpret its output.

   a) List the loopback ip address

   b) List the ip address used by your computer for connecting to the internet, and state its type (ipv6 or ipv4). Also state what type of interface it belongs to (WiFi/Ethernet etc)

2. **[1 marks]** Explore the 'Ping' command, and report the approximate round-trip time for a ping to :
   a) www.iitgoa.ac.in
   b) www.iceland.is

3. **[2 marks]** Read up about the `traceroute` command. You can view its manual by typing `man traceroute` in the Linux terminal. Get a broad idea of what this command does, how it works and how to interpret its output. (Note the "-m" option in traceroute, which you may need to tweak in order to get proper results. Also note the difference between `traceroute -I`, `traceroute -T` and `traceroute -U`)

   Briefly explain (in 4-5 sentences) how traceroute works, by utilizing the TTL field in the Network-layer header.

4. **[2 marks]** Consider the website https://alaska.gov/. We wish to check if the webserver for this site is indeed located physically in Alaska, and trace the route that our packets take to reach this webserver.

   a) Find out the IP address of this webserver.
   b) Use traceroute command to trace the path followed by packets flowing from your computer to this webserver. How many total hops were taken to reach the destination ?
   c) Some hops may not be shown (appearing as * * * in the output of the traceroute command. What do these lines mean?
   d) Traceroute does 3 trials (sends 3 messages) to each hop by default. What is the command to get traceroute to do 5 trials instead?
   e) What is the average round-trip delay (in mili-seconds) for reaching the final destination?
   f) Use online services such as "ipinfo.io" to find and list the geographical location (City, State, Country) where the last hop is located.

PART 2: PACKET SNIFFING USING WIRESHARK

Read up about Wireshark in the introductory reference material provided to you.

5. **[2 marks]** Find out the IP address of "www.iitgoa.ac.in". Now start up wireshark selecting "any" interface.

   Apply a filter "ip.addr == <the ip address you found for iitgoa>" for example, "ip.addr==10.250.36.36". Now, open a web browser and open IIT Goa's website. Observe the traffic captured in Wireshark for this filter.

   a) Look out for the SYN, SYN/ACK, ACK sequence of packets. What protocol is being used at the Transport Layer?

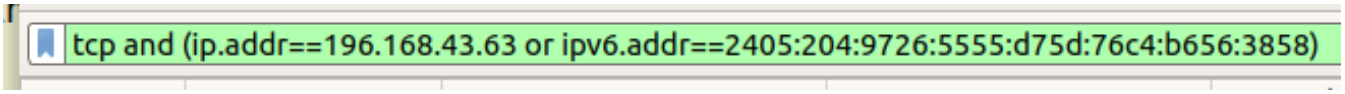
   b) Examine the first SYN packet. Observe how the packet corresponding to each layer of the TCP/IP stack is wrapped inside the packet of the lower layers. Examine the IP datagram and its header. What are the source and destination IP addresses for this packet? Check if the destination IP address matches that of iitgoa.ac.in. List your observation.

   c) Examine the transport-layer segment in the first SYN packet. What are the source and the destination **port numbers** for the first SYN message?

d) Now remove all filters, and take a broad view of all packets flowing through the interface. What kind of packets make up a majority of the traffic to your computer/device?

6. **[2 marks]** In wireshark, you can apply a filter that displays packets only belonging to a certain protocol (such as TCP or UDP) as follows:

Two or more conditions can be combined using and/or to create more complex filters. For example:



a) Now, you wish to find out whether **YouTube** operates over the TCP protocol or the UDP protocol. Open YouTube in Firefox browser and filter out its traffic in Wireshark using the appropriate IP address in the filter. Observe the packets. Does YouTube use TCP or UDP?

b) Does your conclusion change if you open YouTube in Google Chrome, instead of Firefox? List your observation. Check if your conclusion is correct, using a web search about what protocol YouTube actually uses.

7. **[Bonus question, carries no marks]** Try connecting two different devices in the same network. For example, connect your mobile phone on the same network as your laptop. Apply the filter ip.addr=<other device's IP addr>. Check if you can sniff packets meant for another device on the same local network.

----------END----------