IIT Goa CS 378 (Computer Networks LAB)
Instructor: Neha Karanjkar

LAB 1: Basic Networking Tools

Instructions:

- You can complete this lab exercise individually OR in teams of 2 persons (choose your teammate). If working in a team, all persons in the team should work on each problem together. Do **not** divide up the questions among team members.
- You **are allowed** to use Google search and the www for information and commands.
- If you plan to use your own laptop, you need to have a Linux distro. Only Linux-specific commands will be accepted as answers.
- Write your answers legibly on this question sheet and submit to the TAs.

ROLL NUMBER:_____NAME:_____

ROLL NUMBER:_____NAME:_____

PART 1: THE IP COMMAND

1. 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.

2. Find out and list the following information for the computer that you are using.
   For each field, also mention the **command/tool/online service** you have used for obtaining the answers:

   a) Find out how many network interfaces your computer has. For each network interface, list down the following information:
      1. it's type (Ethernet/Wifi/Bluetooth ...)
      2. MAC address
      3. Manufacturer of this NIC (Network Interface Card)
      4. IPv4 address
      5. IPv6 address

Name	Type	MAC	Manufacturer	IPv4	IPv6

b) Your computer may be part of a local network (say a lab-wide or building-wide network within IIT Goa). What is the IP address of this network and what is the range of IP addresses that can belong to individual computers within this network?

c) What is the max number of hosts that can be uniquely addressed within this local network?

d) What is the IP address for sending broadcast messages to your local network?

e) What is your public IP address (as seen by a server outside of IIT Goa)?

3. Just like a router, your computer also maintains a routing table. Each entry in this routing table contains a range of destination IP addresses and the IP address of the "next hop" that should be chosen to forward a packet with the matching destination address. In addition, there is also an entry called "default" which is the route chosen if a destination address does not match any of the other more-specific entries. For a given destination IP address, the entries in the table are searched in the order of the longest prefix to shortest prefix until a match is found. (This is called the "Longest Prefix Match" approach). When a match is found, the computer chooses this entry as the next hop for forwarding the packet. You can view your computer's routing table using the `ip route show` command in Linux. Read up about this command to get a rough understanding of what this command does, what are its options, and how to interpret its output.

   a) What is your default Gateway's IP address as shown in the routing table? What is meant by a Gateway?

   b) Re-write the first 3 entries of your routing table here in the format: <destination IP-address/prefix-length>, <next hop's IP address where this packet should be forwarded>

   c) Sometimes, the next hop's IP address may be shown as 0.0.0.0. What does this indicate?

   d) You might notice an address that looks like 169.254.x.x. What are such addresses called and what do they indicate?

PART 2: PING and TRACEROUTE

4. Explore the Ping command, and report the approximate round-trip time for a ping to :
   a) www.iitgoa.ac.in
   b) www.iceland.is

5. 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`

   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.

   g) Paste the output of traceroute in online services such as https://stefansundin.github.io/traceroute-mapper/ to view the geographic location of individual hops on a map.

PART 3: PACKET SNIFFING USING WIRESHARK

6. Find out the IP address of "www.iitgoa.ac.in". Since you are inside IIT Goa's private network, this might be a private address, such as 10.x.x.x. 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?

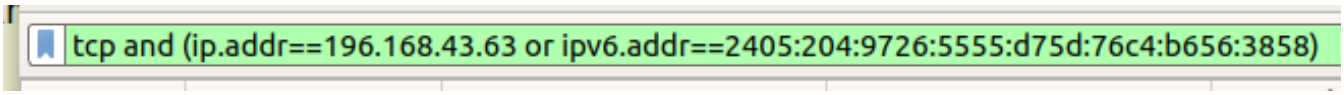
b) Examine the first SYN packet. Observe how the packet corresponding to each layer of the TCP/IP stack is wrapped inside the packet of the lower layers. Examine the IP datagram and its header. What are the source and destination IP addresses for this packet? Check if the destination IP address matches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

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?

e) 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:



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

f) Find out the IP address of the computer being used by another team. Apply the filter ip.addr=<your neighbour's IP addr>. Check if you can sniff packets meant for your neighbouring team's computer on the same local network.

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