COL374/672 Computer Networks: 2020-21 semester I

Assignment 1

The purpose of this assignment is to make students familiar with handy tools such as traceroute, nmap, wireshark, ifconfig, etc, to get a real-life feel of computer networks.

Preparatory tasks

Read the man pages or reference guides of these tools to understand the different options

- *ifconfig (ipconfig on Windows)*: This tells you the IP address, gateway, network mask, hardware address, DNS server, etc for the network interfaces on your computer. Find out what these terms actually mean. Run the commands with your computer connected on WiFi, or via your smartphone acting as a hotspot. Also find out how you can check the IP address of your phone when it is connected via WiFi or 2G/3G/4G networks.

- *ping*: You can use this to discover whether a particular IP address is online or not. Try sending pings with different packet sizes, TTL values, etc. Check if the behavior changes when your computer is connected via different network interfaces.

- *traceroute (tracert on Windows)*: This gives you the sequence of routers that a packet traverses to get to a particular destination. Run this for different destinations and when connecting via different networks.

- *nslookup*: This command helps you communicate with DNS servers to get the IP address for a particular hostname. You can change the DNS server to use, try searching for “open DNS servers” on the web and configure them to answer DNS queries. See how the answers change for popular destinations like www.google.com or www.facebook.com when you change the DNS server to use

- *nmap*: This is a handy network diagnostics tool that you can use to discover which hosts are online in the network, and even try to infer what operating system the hosts might be running.

- *wireshark*: This is a very useful tool to sniff packets on the wire (or wireless medium). Sniffed data is parsed by wireshark and presented in an easily readable format with details of the protocols being used at different layers

Tinker with your network settings

- Find out where you can configure the IP address and DNS server for your network interfaces, on both Windows and Linux. Is this set by default to dynamic assignment?

- Can you configure the IP address on your Android smartphones as well, when connected over data services like 2G/3G/4G? How would you find out your smartphone's IP address?

- Read about the difference between statically assigning an IP address to an interface, or letting it get dynamically assigned. Why do you think dynamic assignment facilities are provided on most networks, and in fact even enforced at times?

- For a network which dynamically assigns IP addresses, such as the cellular network, check over a couple of days whether each time you turn on your smartphone's network, do you get the same IP address? If you initialize the IP address statically to a different value, are you still able to communicate?

Tasks to perform

1. Network analysis

   a. At your home, run traceroute via your Ethernet and WiFi networks for www.iitd.ac.in, and note the IP addresses seen on the path. If your ISP seems to be blocking packets on the path to the www.iitd.ac.in network then try with different destinations like www.google.com or www.facebook.com or www.nytimes.com or www.indianexpress.com, etc.

   b. Report any curious things you notice, like some paths that default to IPv6 and how you can force traceroute to use IPv4, any private IP address spaces you notice like 10.0.0.0 to 10.255.255.255, or 172.16.0.0 to 172.31.255.255, or 192.168.0.0 to 192.168.255.255, missing routers along the path that do not seem to reply to the traceroute requests, etc.

   c. Ping allows you to specify the size of packets to send. What is the maximum size of ping packets that you are able to send?

2. Can you replicate the traceroute functionality using ping? Ping allows you to initialize a TTL. Write a simple script in which you use ping to replicate traceroute. You can write this script in bash or perl or python or any of your favourite scripting languages.

3. Internet architecture

- Consider the following web servers of educational institutions in different continents:

   - University of Utah (US mid-west): `www.utah.edu`

   - University of Cape Town (South Africa): www.uct.ac.za

   - IIT Delhi (India): `www.iitd.ac.in`

  And consider the following web servers of large content providers:

  - Google: www.google.com
  - Facebook: www.facebook.com

- The end of this document contains a list of several working traceroute servers around the world, which allow you to issue a traceroute command from there to any other hosts on the Internet. Pick some 2 traceroute servers from different continents, and one being your own device, and do a traceroute from there to these five web servers.

- Consult whois services to figure out when traffic gets into the local ISP, transits to other intermediate ISPs, and finally into the destination domains. One such service is https://whois.domaintools.com/

- Study the following:

  a. In a neat tabular format, report the number of hops from the (3) traceroute sources to the above (5) destinations. Are the number of hops between nodes in the same continent lower than the number of hops between nodes in different continents? Do Google and Facebook differ from the others in the number of hops required to reach them? Why would this be so?
  b. Also report the latencies between the traceroute sources and the web-servers. Does the latency seem to be related to the number of hops, being higher when there are more hops? Why is this the case?
  c. Which of the destination web-servers are resolved to the same IP address irrespective of from where you do a traceroute to them? Why do you think some web-servers are resolved to different IP addresses when queried from different parts of the world? You can also use nslookup to change the DNS server that you want to use.
  d. If you do traceroutes from the same starting point to different IP addresses you found for the same web-server, do the paths appear different? Which ones are longer?
  e. Try tracerouting to Google and Facebook from different countries of traceroute servers around the world. Are you able to find any countries that do not seem to have their local ISPs directly peered with Google and Facebook?

What to submit

A neat report in pdf, using Latex. Watch these simple videos to learn Latex.

https://www.overleaf.com/learn/latex/LaTeX_video_tutorial_for_beginners_(video_1)

Please use the exact same question numbering as above.

You will present your report over a viva with a TA, and also run your script to replicate the traceroute functionality.

Open Traceroute servers

- Canada http://www.tera-byte.com/cgi-bin/nph-trace

- Czech Republic http://www.snlink.net/

- Germany http://www.han.de/cgi-bin/nph-trace.cgi

- Greece https://foss.aueb.gr/network_tools/index.php

- Sweden http://www.macomnet.net/ru/testlab/cgi-bin/nph-trace

- USA http://www.net.princeton.edu/traceroute.html

Some large traceroute services with probes around the world are also:

- http://www.cogentco.com/en/network/looking-glass

- http://www.lg.he.net/

Public DNS servers

Cloudflare: 1.1.1.1

Verisign: 64.6.64.6

Open DNS: 208.67.222.222

AdGuard: 176.103.130.130