**COL374/672 Computer Networks: 2019-20 semester I**

**Assignment 1**

In this assignment, we will learn to use some 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 connected over Ethernet, or via your smartphone acting as a hotspot.

- *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, spoofing your IP address, 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 IITD WiFi network in the academic area, check over a couple of days whether each time you turn on your computer's or smartphone's WiFi, do you get the same IP address each time? If you initialize the IP address statically to a different value, are you still able to communicate?

**Assignment begins here**

1. Local network analysis

    a. In your hostel, run traceroute via your Ethernet and WiFi networks for www.iitd.ac.in, and note the IP addresses seen on the path

    b. For each of the network segments you find out above (ie. your immediate 1-hop network, the 2-hop network around you, the 3-hop network, etc), use *nmap* to find other devices on these networks. Use a command such as:

    *nmap –sn 10.208.26.0/24*

    Of course, you will need to use different target network addresses in the *nmap* command for each of the different network segments you want to probe! Repeat this at different times of the day, and for 2-3 days. Report your observations in a tabular format about the number of hosts seen over the days at different times of the day.

    Also write about any trends that you notice, such as which devices are seen all the time, which ones are transitory, when do you see more devices, etc.

    c. You can even find out what OS is probably running on these devices:

    *nmap –O 10.208.26.135*

    Report this for at least 5 permanent and 5 transitory devices you noticed in different network segments.

2. Internet architecture

- Consider the following web servers of educational institutions in different continents:
    - University of Waterloo (Canada east): `www.uwaterloo.ca`
    - 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 3 traceroute servers from different continents, 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://tools.keycdn.com/geo

- Study the following:

  a. In a neat tabular format, report the number of hops from the (3) traceroute servers 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?
  b. Also report the latencies between the traceroute servers and the web-servers. Does the latency seem to be related to the number of hops?
  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?
  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?

- Now do the same exercise of tracerouting to the five destinations from a cellular data network in India. You can do this by turning your smartphone into a hotspot, or via a 2G/3G/4G USB Internet dongle.
  f. Contrast the number of hops and latency incurred inside the network of your cellular ISP, to the total number of hops and latency to the destinations. Which part of the network do you find is the greatest source of latency?
  g. Do you find routes to some destinations to be closer than others? What does this tell you about the connectivity of your ISP to the rest of the world?

3. Packet analysis

   a. Use *wireshark* to grab all packets on your wireless interface, while visiting a website such as http://www.iitd.ac.in from your browser. Do an *ipconfig /flushdns* before you do this activity to clear your local DNS cache. And also clear your browser cache. Report the following:

i. Apply a “dns” filter on the packet trace, and see if you can find DNS queries and responses for www.iitd.ac.in. How long did it take for the DNS request-response to complete?

ii. Apply an “http” filter on the packet trace and report the approximate number of HTTP requests that were generated. What can you tell from this observation about how web-pages are structured, and how browsers render complex pages with multiple images and files?

iii. Apply a filter such as “((*ip.src==192.168.1.3 && ip.dst==10.7.174.111) || (ip.src==10.7.174.111 && ip.dst==192.168.1.3)) && tcp*”. As would be self-explanatory, this will filter for TCP packets moving between your browser and the web-server. Recall that the source and destination IP addresses are a part of the network layer header, which is also called the IP layer since IP (Internet Protocol) is the most common network layer protocol in use. Find the number of TCP connections that were opened between your browser and the web-server. The signature for a new TCP connection is a 3-way handshake: The client sends a SYN message to the server, the server replies with a SYN-ACK message, and the client then sends an ACK. You will find that several TCP connections were opened between your browser and the web-server. What does this tell you about optimizations that the browser might be performing, when fetching multiple files and images to display? Do you find that some content objects are fetched over the same TCP connection? TCP connections are distinguished from one another based on the source port and destination port.

iv. Report the total time taken for download of the entire webpage measured as the time at which the first DNS request was sent and the time when the last content object was received

v. Try doing a trace for http://www.indianexpress.com and filter for “http”. What do you find, is there any HTTP traffic? Browse through the entire trace without any filters, are you able to see the contents of any HTML and Javascript files being transferred? Confirm that you were indeed able to see them earlier when accessing http://www.iitd.ac.in.

What to submit: A neat report in pdf. Please use the exact same question numbering as above.

**Open Traceroute servers**

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

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

- Germany http://www.tnib.de/cgi-bin/traceroute.pl or 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