COL374/672 Computer Networks: 2023-24 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 behaviour 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 – a few public DNS servers are listed at the end of this document, you can ask nslookup to use these servers 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?
- 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?

Find who else is on your network

- From your home or hostel room or cellular connection, run traceroute via your Ethernet and WiFi networks for www.iitd.ac.in, and note the IP addresses seen on the path.
- 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 –sL 10.208.26.0/24

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

  nmap –PS –O 10.208.26.135

Assignment begins here

1. Network analysis

   a. At your home (not hostel room which is on the IITD network) or from a 4G or other cellular connection, 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, plus one being your own device, and do a traceroute from there to these five web servers.
- Consult an AS-IP lookup service 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://hackertarget.com/as-ip-lookup/. FYI, you can also check how different ASes are connected with one another from this collated dataset here: https://bgp.potaroo.net/cidr/autnums.html
- Study the following:
    a. In a neat tabular format, report the number of hops from the (3) traceroute sources to the above (5) destinations. If the pair of (traceroute source, destination) are geographically close to each other, does it roughly translate into fewer hops? Do Google and Facebook differ from the others in the number of hops required to reach them, irrespective of which traceroute source is used? 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. You can also use this dig web interface which may help speed up things for you: https://www.digwebinterface.com/

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?

4. Packet analysis

- Use wireshark to grab all packets on your wired or wireless interface, while visiting an HTTP website such as http://act4d.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:

  a. 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?

  b. 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?

  c. 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. Is this the same as the number of HTTP requests for content objects that you found in the previous part? Do you find that some content objects are fetched over the same TCP connection? Note that TCP connections are distinguished from one another based on the source port and destination port.

  d. Now 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? What just happened?

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

These services allow you to choose a traceroute source from where you can run probes to any IP address:

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

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

Some additional open traceroute servers are:

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

- 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

Public DNS servers

This web page lists several public DNS servers and their location: https://public-dns.info/

A few more open DNS services are listed below, although it is not clear exactly where these servers are located.

- Cloudflare: 1.1.1.1

- Verisign: 64.6.64.6

- Open DNS: 208.67.222.222

- AdGuard: 176.103.130.130