CS F303 Computer Networks: 2019-20 semester II

Assignment 1

You are free to write scripts to automate the analyses in this assignment. This assignment is to be done in groups of 4 students. You are free to form your own groups. Only one group member needs to submit the assignment on the designated link on CMS. All code and other submissions will be run through similarity check software, so please be honest with your work. Read the course handout for the dishonesty policy. Deadline for submission of this assignment is 8th February, 2020, 23:59 hours.

This assignment is a follow-up on your lab sessions. In this assignment, we will learn to use some handy tools such as traceroute, nmap, wireshark, ifconfig, etc. on a Linux system to get a real-life feel of computer networks.

1. Read the man pages or reference guides of these tools to understand the different options
   - **ifconfig**: This tells you the IP address, gateway, network mask, hardware address, etc. for the network cards on your computer
   - **route**: This shows you different routes configured on your computer. Should be simple to understand if you just have one network interface active
   - **ping**: You can use this to discover whether a particular IP address is online or not
   - **traceroute**: This gives you the sequence of routers that a packet traverses to get to a particular destination
   - **nslookup**: This command helps you communicate with different DNS servers
   - **nmap**: This is a handy network diagnostics tool that you can use to discover which hosts are online in the network, ports open on these hosts, etc.
   - **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

2. Local network analysis
   a) Query your LAN using nmap to discover which hosts are online. Use a command such as: `nmap –n –sP 172.16.89.175/24` (use your own IP address in your hostel, read about CIDR addressing).
      Write a script that you can run repeatedly at different times of the day, and find the number of hosts online. Do it for at least 5 days. Plot a graph against time to see if there are any hourly trends to when computers are switched ON or OFF in your hostels.
   b) Find out what servers are running in your LAN. Use a command such as:
      `nmap –n 172.16.89.175/24`
      You can even find out what OS is running on these computers:
      `nmap –n –O 172.16.89.175`
      You need not query all hosts in your LAN, a small sample will be sufficient to get an idea. For example, you can discover hosts using nmap –sP on a /16 block and then do more detailed nmap –O etc. on specific hosts or smaller IP address blocks. Read about CIDR notation of IP address blocks.
   c) Use ifconfig to find out local DNS servers and gateway assigned to your machine in different parts of the campus. You can probe from your hostels, from the Data Science Lab over wireless, Data Science Lab over wired, CC Labs, etc.

3. Internet architecture

The end of this document contains a list of several working traceroute servers around the world. Consider the following web servers of educational institutions in different continents:

- ETHZ (Switzerland): 129.132.19.216
- University of Waterloo (Canada east): 129.97.208.23
- University of Cape Town (South Africa): 137.158.158.44
- BITS Pilani (India): 14.139.243.30

And consider the following web servers of large content providers:

- Google: 216.58.219.196
- Facebook: 31.13.75.36

1. Pick some six traceroute servers from different continents, and do a traceroute to these six web servers (educational institutions and content providers listed above)
2. Consult whois services to figure out when traffic gets into the local ISP, transits to other intermediate ISPs, and finally into the destination domains
3. Study the following:
    a) Frequency distribution of the number of hops from traceroute servers to the above destinations in different continents. Are the number of hops between nodes in the same continent lower than hops between nodes in different continents? Do Google and Facebook differ in the number of hops required to reach them?
    b) Frequency distribution of the latencies between the traceroute servers and web servers. Is the latency related to the number of hops?
    c) How many countries of traceroute servers did you find that have local ISPs directly peered with Google and Facebook?
    d) Now do the same exercise of tracerouting to the six destinations from a cellular data network in India (mobile hotspot). 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. What do you find is the greatest source of latency?
    e) 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?

4. Packet analysis
    a) Use wireshark to grab all packets on your wireless interface. Turn off all applications such as your browser and email clients, and see what kind of background traffic is being generated, both outgoing and incoming. What applications are responsible for this background traffic?
    b) Now visit an internal website such as http://10.2.102.21:9000/psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT from your browser and capture all traffic. Do an ifconfig / flushdns before you do this activity to clear your local DNS cache. Report the following:
        i. Servers for which a DNS query was launched
        ii. Number of HTTP requests generated
        iii. Number of TCP connections opened
        iv. Total time taken for download of the entire webpage measured as the time at which the first request was sent and the time when the last packet was received
        v. Any TCP losses/retransmits noticed

5. What to submit: A .zip or .tar.gz file containing the following
    i. A readme.txt file with the group members' names and ID numbers in a clean csv format
    ii. /src directory, with script for tracking the number of hosts online in your LAN, using nmap. You can use simple bash, or perl, or python, or any other language for the script. It should take as parameters the subnet to probe (e.g. 10.208.26.0/24) and the probing frequency in terms of number of probes per hour (e.g. 1), and produce an output in a CSV format with [time of day, number of hosts] fields.

iii. In a /doc directory, a pdf for question 2, with the following
    - Number of hosts observed online over the duration of the tests performed.
    - List of hosts and servers discovered on your LAN
    - Gateways and DNS servers used in different parts of the campus LAN
iv. In a /data directory, an Excel (or odt) file for question 3, with the following worksheets
    - Number of hops table, with rows for each traceroute server used, and columns for each destination server probed
    - Latency table, with the same format as above
    - Qualitative/quantitative analysis of any correlations observed between the number of hops and latency from different traceroute servers
    - Latency table for your local ISP using cellular data connections, with rows for each destination probed, and columns for the total number of hops to the destination, number of hops inside the local ISP's network, %age of hops inside the local ISP to the total number of hops, total latency, latency inside the local ISP, and %age of latency incurred inside the local ISP
v. In the /doc directory, a pdf file for question 3, with the following
    - Brief writeup of your observations from the tables above, as asked in the questions
vi. In the /doc directory, a pdf file for question 4, with the following
    - List of applications generating background traffic
    - Analysis of the webpage download in terms of the number of HTTP connections, etc, and screenshots of wireshark showing DNS packets, HTTP requests, TCP headers, IP headers, etc

Open Traceroute servers

- Austria http://traceroute.utanet.at/
- Canada http://www.tera-byte.com/cgi-bin/nph-trace
- Czeck Republic http://www.snlink.net/
- Finland http://www.zmailer.org/traceroute.html
- Germany http://www.traceroute66.com/ http://www.tnib.de/cgi-bin/traceroute.pl
- http://www.han.de/cgi-bin/nph-trace.cgi
- Greece https://foss.aueb.gr/network_tools/index.php
- Latvia http://www.eunet.lv/cinfo/connect/index.phtml
- New Zealand http://www.kcbbs.gen.nz/cgi-bin/trace
- Russia http://www.radio-msu.net/se_traceroute.htm
- South Africa http://services.truteq.com/cgi-bin/nph-traceroute
- Sweden http://www.macomnet.net/ru/testlab/cgi-bin/nph-trace?
- Switzerland http://traceroute.deckpoint.ch/ http://lg.uar.net
- Ukraine http://traceroute.xilo.net
- United Kingdom http://www.hotlinks.co.uk/traceroute.htm
- USA http://www.area.com/ralphs/traceroute.html http://www.ntplx.net/traceroute/ http://www.net.princeton.edu/traceroute.html http://voa.his.com/cgi-bin/trace

Public DNS servers

- Level 3: 4.2.2.2
- Google DNS: 8.8.8.8
- Google DNS: 8.8.4.4
- Open DNS: 208.67.222.222
- Open DNS: 208.67.220.220
- http://beebom.com/2015/06/best-dns-servers