CS-374/672 Computer Networks: Fall 2014

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.

1. 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, 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 (tracert on Windows)*: 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 10.208.26.0/24

    Write a script that you can keep running for a week, and which periodically samples the number of hosts online. 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 10.208.26.0/24

    You can even find out what OS is running on these computers:

    nmap –n –O 10.208.26.135

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.

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 Bharti building over wireless, Bharti over wired, CSC, 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:
    - 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`
    - IIT Delhi (India): `103.27.9.20`

  And consider the following web servers of large content providers:
    - Google: `173.194.36.80`
    - Facebook: `173.252.88.66`
- Pick some dozen traceroute servers from around the world, and do a traceroute to these six 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
- Study the following:
    a. Frequency distribution of the number of hops from traceroute servers in Europe/USA/Africa/Australia, 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 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?
- Now do the same exercise of tracerouting to the six destinations from a cellular data network in India. If you are not already using a 2G/3G data card, you can purchase a GPRS connection on your phone and use your phone as a modem from your computer.

d. 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? [4a]

b. Now visit an internal website such as http://www.iitd.ernet.in from your browser and capture all traffic. Do an *ipconfig /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

v. Any TCP losses/retransmits noticed [4b]

5. What to submit: A .zip or .tar.gz file containing the following

i. /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, for the script. It should take as parameters the subnet to probe (eg. *10.208.26.0/24)* and the probing frequency in terms of number of probes per hour (eg. 1). And produce an output in a CSV format with [time of day, number of hosts] fields. [2a]

ii. /doc directory, with a pdf for question 2, with the following

- Timeline graph of the number of hosts online over the duration of the test. [2a]
- List of hosts and servers discovered on your LAN [2b]
- Gateways and DNS servers used in different parts of the campus LAN [2c]

iii. /data directory, with 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 [3a]
- Latency table, with the same format as above [3b]
- Correlation calculated separately for each destination server probed, between the number of hops and latency from different traceroute servers [3c]
- 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

iv. /doc directory, with a pdf file for question 3, with the following

- Brief writeup of your observations from the tables above, as asked in the questions [3a, 3b, 3c, 3d, 3e]

v. /doc directory, with a pdf file for question 4, with the following

- List of applications generating background traffic [4a]
- 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 [4b]

Open Traceroute servers

Austria http://traceroute.utanet.at/

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

Czeck Republic http://www.snlink.net/

Faroe Islands http://netcon.internet.fo/cgi-bin/nph-traceroute.pl

Finland http://www.zmailer.org/traceroute.html

Germany http://www.helios.de/ http://sites.inka.de/lina/tracer.html http://bandit.probe-networks.de/cgi-bin/trace http://www.space.net/cgi-bin/webtrace http://www.traceroute66.com/ http://www.tnib.de/cgi-bin/traceroute.pl

Greece http://www.ntua.gr/nmc/traceroute.html

Latvia http://www.ntua.gr/nmc/traceroute.html 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://dwhome.dataway.ch/support/traceroute.aqua http://traceroute.deckpoint.ch/ http://www.switch.ch/cgi-bin/network/nph-traceroute

Ukraine http://lg.teleportsv.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://visualroute.visualware.com/ http://voa.his.com/cgi-bin/trace http://www.fluidhosting.com/traceroute.php

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