EECS 863
Homework

Download and run Wireshark on your own machine. Wireshark can be downloaded from wireshark.org. Install on your own machine; you need to install and run Wireshark as administrator.

1. Measure the upload and download speeds from your home ten times (You can use the speed test at https://www.speedtest.net/). Report the ISP service you are using, e.g., cable modem, DSL, or campus dorm. Include the 95% confidence interval of your measurement's, report the date/time of the measurement. Include a figure of the topology of your home network, e.g., draw a figure of how your computer is connected to the Internet.

2. From your home computer execute ping to measure the round-trip time to www.google.com. Collect 25 RTTs times and report the average RTT and standard deviation and document the date/time of the measurement. The ping command can be executed from the Windows Command prompt. (To force ping to use IPv4 use ping www.google.com -4.)

3. Repeat part 2) with the target of www.canterbury.ac.nz. and explain the differences observed between part RTT measurement to www.google.com vs www.canterbury.ac.nz.

4. From your home computer execute a traceroute command and report the results. Perform a traceroute to www.google.com and www.canterbury.ac.nz (or from windows command use tracert) and the date/time of the measurement. The tracert command can be executed from the Windows Command prompt. discuss the differences between the two traceroutes.

Wireshark
Use Wireshark and Ping to examine transmit and received ICMP packets.

Process:

a) Start Wireshark
b) Under capture → options select the interface your computer uses to send and receive packets. On my computer it is:
    a. Intel(R) PRO/1000 GT Desktop Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{5CD5C7FA-3D38-42E3-976B-F091496A5295}
c) Under capture → options click off the "Capture packets in promiscuous mode"
d) In the main window → use the ICMP capture filter, click down arrow on left and select icmp (Or type icmp into the capture filter field).
e) Click on Apply
f) Click start
g) Get one round trip time to www.google.com using ping,

    ping –n 1 www.google.com

h) Under Capture → stop wireshark
i) Repeat for ping –n 1 –l 256 www.google.com (it is –l 16, -l is length option, not -1 [one])

Questions:

5) From the wireshark output find the IP address of destination: www.google.com?
6) What are the sent data bytes.
7) What is the MAC address (physical address) of your NIC? Find the MAC address by examining the Echo (ping) request in the Packet Bytes Plane (the bottom window)
8) In Wireshark, generate a flow graph under Statistics→Flow graph, select "All Packets", "General flow", and "Standard source destination addresses". Discuss the resulting flow graph.

Part IV Summary

Discuss how the Wireshark output demonstrates protocol layering and encapsulation. Discuss how network protocol analyzers are used to examine the operation of network protocols. What are some possible applications of a network protocol analyzer?