Comp312 class project on
A Report on My Residential Network
October 27, 2011

Objectives

1. Review the fundamental networking concepts learnt in classes, and
2. Review the basic usage of Wireshark learnt in the labs, in the context of studying your residential network at home.

Deliverables

1. This is a group/individual project. If you choose to partner with another classmate, the group size cannot be more than two.
2. The deliverable is a report answering the questions below. Wherever possible, you should give sufficient evidence for backing up your answers using, for example, Wireshark screenshots and screenshots from other command/tools.
3. The deadline of the report is 9 Dec (one week after the last lecture). Please submit a hardcopy of the report, along with a CD containing the softcopy of the report and the data that you have collected.

A. Network configurations (34 pt)

Q1: (2 pt) What kind of access network do you use? (e.g., is it wireless? If not, is it ADSL?)

Q2: (2 pt) What kind of client do you use? (e.g., laptop/desktop/mobile device)

Q3: (2 pt) Which ISP do you use?

Q4: (4 pt) Use Speedtest services to test your upload and download bandwidths. Is download or upload speed faster? Do you think this setting make sense?

Q5: (2 pt) Are the speeds the same with what your ISP has advertised?

Q6: (4 pt) Try different Speedtest services and see whether they report the same results.

Q7: (4 pt) What is your IP address? How can you look it up? Which AS does it belong to? (Hint: use an online IP-to-AS conversion service.)

Q8: (4 pt) Is the IP address dynamically assigned to you? How could you tell?

Q9: (2 pt) How many DNS servers do you have? Please list them out. What does a DNS server do?

Q10: (2 pt) Use nslookup to resolve a website, and see which DNS server(s) it has used.

Q11: (4 pt) Does your DNS server use TCP or UDP protocol?

Q12: (2 pt) What is the IP address of your gateway? What does a gateway do?

Q13: If you have another group member, repeat the tests in his/her home and list their differences.

B. Network experiments (32 pt)

Q14: (4 pt) What is a "ping" program? What types of information does it report? Please ping a web server in Hong Kong, and another in US. Does the ping to the US server take longer time? How could you tell?

Q15: (4 pt) What is a "traceroute" program? What types of information does it report? Please traceroute to the two servers you used before and record the results. How long are the network paths in terms of numbers of intermediate routers?

Q16: (4 pt) How do you think "traceroute" works? If you are given only a "ping" program (e.g., in Windows or Linux), which argument could you use to obtain the network path?

Q17: (4 pt) Use Wireshark to capture the packets sent by your "ping" program to a website. Which filter would you use? In the packet capture, how many packet types do you see? Please list them.

Q18: (4 pt) Use Wireshark to capture the packets sent by your "traceroute" program to a website. Which filter would you use? For the packet types you see, are they the same with the "ping" program's?

Q19: (4 pt) Use an online IP-to-AS service to look up the AS number of each IP address returned by traceroute. How many different ASes could you see?

Q20: (4 pt) Use an online IP-to-Geolocation service to look up the country name of each IP address returned by traceroute. How many different countries do you have?

Q21: (4 pt) Does a more "distant" IP address along the path always respond with a higher latency? Do you think the latency reported by the program is accurate?

C. Networking concepts (34 pt)

Visit a website and write a report addressing the following issues. Please answer each question in details and relate it to your packet captures. Read 5.9 of the textbook for this section.

Q22: (4 pt) How did your browser obtain the IP address of the URL you have entered.

Q23: (4 pt) How did your browser start a TCP connection before an HTTP request was sent? Which packets correspond to the connection initiation?

Q24: (4 pt) Which HTTP request mechanism did your browser use? What is the response from the server? Apart from the HTTP content, please list some other fields you can see from the packet capture that are important for describing that HTTP session.

Q25: (4 pt) If there are multiple web objects in the content, can they be transferred all at the same time?

Q26: (4 pt) The TCP sequence number of a packet you saw from the Wireshark is only a relative sequence number. How can you tell its absolute sequence number?

Q27: (2 pt) Please give an example from your capture to explain the relationship between sender's sequence number and receiver's ACK number.

Q28: (4 pt) Which port did the web server use? How does the server decide which port to use? Could it use some other port number?

Q29: (4 pt) Which port did your side use? How is it decided? Could it use some other ports?

Q30: (4 pt) How (using which packets) is the TCP connection finished?

~~~ END ~~~
~~~