Lab 2: Network Traffic Monitoring and Performance Measurement

Instructor: Ning Weng, Office EGRE 119, Office hour: MW 2:15-3:45pm
Lab Assistant: Fahad A. Alduraibi; Office EGRE 112, Office hour Tu: 11:00am-12:00pm; Fri: 10:00-11:00am
Lab due: Sep. 26, Wed. in class

The goal of this lab is to use basic network tools to capture network packets and measure network performance (delay and throughput). It is recommended that you follow the steps. Be sure to record and save what your observed, which will be part of your lab report.

To perform this lab, you need one machine (either linux, unix or windows with cygwin) with Internet access. In case that your system doesn't have the tools, you can download them from the following links:

- wireshark: http://www.wireshark.org
- iperf: http://dast.nlanr.net/projects/Iperf/#download

I. Network Packets Capture

A. Case 1: ping

- Launch wireshark.
- Click "start" from the "capture" menu.
- ping -n 10 heera.engr.siu.edu (-n for windows, -c for linux machine, ping heera.engr.siu.edu 56[count 10] for cygwin).
- Click "stop" button of wireshark when ping is finished.
- Order the packets according to Protocol by clicking on "Protocol" column heading.
- Record:
  1. How many packets are there in your ping console window?
  2. How many packets are there in your wireshark window for ICMP packet?
  3. Choose one ICMP packet in wireshark window, what is the protocols in frame?

B. Case 2: http

- Launch wireshark.
- Click "start" from the "capture" menu.
- Visit SIUC engineering website: http://www.engr.siu.edu.
- Click "stop" button of wireshark after the webpage is correctly displayed.
- Order the packets according to Protocol by clicking on "Protocol" column heading.
- Record:
  1. Observe TCP three-way handshaking process and the sequence number mechanism.
  2. Choose the captured TCP packet with SYN and ACK flag, and observe packet details in various layers: Ethernet layer: destination and source MAC addresses IP layer: version, header length, TTL, flag, protocol, source and destination IP addresses Transmission layer: source port and destination port, SN, ACK number, header length, Flag, window size, checksum.

II. Network Delay Measurement

A. Case 1: ping

- ping -n 5 64.233.167.104 (-n for windows, -c for linux machine, ping 64.233.167.104 56[count 5] for cygwin).
- record: what is the average, minimum and maximum delay between your test machine with target machine?

B. Case 2: traceroute

- Open page http://network-tools.com/
- Change the destination IP address to 206.166.70.78 and hit enter.
- Record:
  1. Copy the traceroute output.
  2. How many routers are there between 206.166.70.78 and http://network-tools.com/?
  3. What is the average, minimum and maximum delay between 206.166.70.78 and http://network-tools.com/?
  4. Explain the mechanisms that traceroute generates delays to different hops. Should the delay incrementally increase with the hop increasing?
  5. Based on your own trace, you might find the delay actually decrease (If not, run traceroute again by clicking submit button.) What is the possible reasons this delay decrease in your opinion (you can make your assumptions as long as it is right)?

III. Network Throughput Measurement

** To perform throughput measurement, you are in either inside the SIUC network, or VPN is required from outside of SIUC network)

A. TCP

- iperf -p 8888 -c 131.230.191.178 (./iperf.exe -p 8888 -c 131.230.191.178 for cygwin)
- Record the throughput in unit Mbitssec.
- Please repeat the above steps for another two times.

B. UDP

- iperf -p 9999 -c 131.230.191.178 -u (./iperf.exe -p 9999 -c 131.230.191.178 -u for cygwin)
- Record the throughput in unit Mbits/sec.
- Please repeat the above steps for another two times.

IV. Report Requirement

1. Your report should include all the records.
2. Describe TCP three-way handshaking process using the packet captured by .
3. What is the four sources packet delay? From the result of traceroute, can you argue which kind of delay is the most important?