Lab on Traffic Monitoring and Throughput Measurement using TTCP

CSE398: Network Systems Design, Lehigh University
Instructor: Dr. Liang Cheng, Assistant Professor, Computer Science and Engineering
Lab Assistant: Yaoyao Zhu, Ph.D. student in Computer Science and Engineering

Introduction

This lab session includes two parts:

1. `TTCP` and throughput measurement;
2. Using `ethereal` to capture network packets and observe the packets in various layers;

Each machine has two network interface cards (NIC), `eth0` and `eth1`. Their IP-address configurations are DHCP enabled.

The `eth1` interface belongs to a private 192.168.1.0/24 network and is connected with a switch, which enables an Internet connection via NAT supports.

The `eth0` interface belongs to a private 192.168.3.0/24 network and is connected with a hub, which is isolated from the Internet. A machine with an IP address 192.168.3.80 is configured and activated in this private 192.168.3.0/24 network to be used for `ping` checking functionality.

Please type `knoppix26 lang=us` after boot prompt to launch the X Windows at the Knoppix CD.

Procedure and Homework 3.1

1. Launch the Konsole window and make a temporary directory called "temp" and perform the rest of the steps under "temp" directory.
2. Download a copy of `ttcp` at: http://www.cse.lehigh.edu/~cheng/Teaching/CSE398-05/schedule.html
3. Compile `ttcp` to obtain a binary: `gcc -o ttcp ttcp.c` and type `./ttcp` to study the configuration options supported by `ttcp`.
4. Test `ttcp` in loopback interface on a single computer.
    a. Start one copy in receive mode: `./ttcp -r >/dev/null`
    b. Start another copy in transit mode using `ttcp` with a large file (size>1MB, such as 1M.zip) as the input:
    `./ttcp -t localhost < 1M.zip`
5. `ttcp` reports the size of the data sent in bytes and the time taken. Record the loopback throughput in Kbps.
6. Change buffer sizes ranging from 16K bytes to 256K bytes in increments of 16K using the "`-l`" option to specify the buffer size and measure the throughput. An example of the command for changing buffer size:

`./ttcp -t -l buffersize localhost < 1M.zip`
Plot the throughput vs. buffer size. (HW3.1a)

7. The `-T` option causes the sending `ttcp` to "touch" each byte of data as it is written (i.e., to emulate packet processing). Here is an example of the command: `./ttcp -t -T localhost < 1M.zip`. Repeat the measurement with the –T option set. How much is throughput affected? (HW3.1b)
8. Repeat the measurement with output from the receiving `ttcp` directed to a file instead of `/dev/null`. Does it affect the throughput? It yes, how much is throughput affected? (HW3.1c)
9. Repeat the measurement with various size files. Does throughput vary with file size? If yes, how much does it vary? (HW3.1d)

Ethereal

10. Try to ping `localhost` and www.lehigh.edu. They both should be ping-able, otherwise please ask the lab graduate assistant for help.
11. In the Konsole window, log in as root by typing `su root` and then run the `ethereal` application by typing `ethereal`.
12. From the "Capture" menu click "Start", choose `eth1` from the popup dialog, then click "OK" button to start capturing packets across `ethe1`. Note that `eth1` is connected to the Internet.
13. Go to the course website: http://www.cse.lehigh.edu/~cheng/
14. After the webpage has been correctly displayed, stop packets capturing. Order the packets according to Protocol by clicking on "Protocol" column heading.
15. Observe TCP three-way handshaking process and the sequence number mechanism.
16. Choose the captured TCP packet with SYN and ACK flag, and observe packet details in various layers:
    Ethernet layer: destination and source MAC addres*ses*
    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
17. Restart the capture procedure, enter capture filter into the `ethereal` "Capture Filter" dialog box in the popup dialog as follows: *`tcp port 80 and host 128.180.120.4`* and see that only HTTP traffic from 128.180.120.4 (www.cse.lehigh.edu) are captured.
18. Repeat the same procedure as the step `17` except entering the capture filter as follows: *tcp port 80 and not host 128.180.120.4* and see that what packets are captured