National University of Singapore
School of Computing

CS2105 **DIY Exercise 1** Semester 2 13/14

You may run the following tools on Solaris (e.g., SunFire), Linux, Mac OS X, or Microsoft Windows. The behavior may be slightly different (but should not impact your learning).

To access the SunFire server, use any ssh client and ssh into: `sunfire.comp.nus.edu.sg`. Use your SoC UNIX username and password to login. If you do not have an account on SunFire, apply for one here: `http://mysoc.comp.nus.edu.sg/~newacct`.

HAVE FUN, AND BE CURIOUS

1. netstat

   `netstat` is a command line tool that displays various information about your computer's network stack.

   Find out what are some open sockets on your computer. Can you recognize some of the establish connections? Do you see some sockets that are in listening state?

   - If you are running Windows or Linux, type the command `netstat -a`.
   - If you are running Mac OS X, type the command `netstat -a -f inet`.

2. traceroute

   `traceroute` is a command line tool that prints the route a packet takes to go from the current host to a destination.

   On your computer, run traceroute to `mail.google.com`. Repeat several times at different time of the day. Do you see the same results?

   (Note: the equivalent of `traceroute` utility on Windows is `tracert`.)

   (Note: the utility `traceroute` is located under `/usr/sbin` on SunFire. To run `traceroute`, you need to either add `/usr/sbin` to your `PATH` environment variable, or type the full path every time.)

3. dig

   Use `dig` to answer the following questions. You may have to download and install `dig` if it is not already available. One of many online instructions for installing dig on Windows is available at `https://www.cites.illinois.edu/dns/tools.html`.

   (a) Find the IP addresses of `mail.google.com`. Repeat several times and observe the changes. Why do you think different answers are given out at different time?

   (b) Use the dig server at URL `http://www.kloth.net/services/dig.php` (using your Web browser) and find the IP addresses of `mail.google.com`. Do you get the same results as part (b)? Why do you think that the same hostname provides a different answer when `dig` is run from different places?

   (c) Find the TTL value for the A-type DNS record of the following hosts at their authoritative DNS server: (a) `sentosa.comp.nus.edu.sg`, (b) `liubei.ddns.comp.nus.edu.sg`. What do you think there are differences in the range of TTL values of these records? (Hint: ddns stands for Dynamic DNS.)

   (d) Observe the TTL values for DNS record of `www.apple.com`. Why do you think the TTL values are so small? (Hint: the DNS servers are provided by Akamai. Google to find out how Akamai works)

   (e) Is your local DNS server the fastest? You can use `dig` to find out.
   First, use dig to look up your favorite domain name a few times, note down the query time. This step uses your default local DNS server (either by your ISP or by the university, depending on where you run the experiments).

Now, you can tell dig to perform DNS lookup using a specific DNS server by passing in the IP address of the server, prefixed with `@`. For example, try to run `dig` with the argument `@8.8.8.8`, like this:

```
dig @8.8.8.8 www.apple.com
```

The IP address 8.8.8.8 refers to one of the public DNS servers ran by Google (see `https://developers.google.com/speed/public-dns/`).

Is Google's public DNS server faster or slower? Repeat this experiment using different access networks (e.g., with Wireless@SG).

4. ping

   The tool `ping` is useful to measure the round trip time to another host.

   For instance, to measure the round trip time to `www.nus.edu.sg`, you run:

   ```
   ping www.nus.edu.sg
   ```

   You will see output that looks like:

   ```
   PING www.nus.edu.sg (137.132.21.27): 56 data bytes
   64 bytes from 137.132.21.27: icmp_seq=0 ttl=122 time=1.591 ms
   64 bytes from 137.132.21.27: icmp_seq=1 ttl=122 time=1.458 ms
   64 bytes from 137.132.21.27: icmp_seq=2 ttl=122 time=1.550 ms
   64 bytes from 137.132.21.27: icmp_seq=3 ttl=122 time=1.673 ms
   ```

   On UNIX-based platforms, `ping` will continuously. In this case, type Control-C to stop. The following statistics will be shown.

   ```
   --- www.nus.edu.sg ping statistics ---
   6 packets transmitted, 6 packets received, 0.0% packet loss
   round-trip min/avg/max/stddev = 1.458/1.566/1.673/0.086 ms
   ```

   The last line gives the information about the round trip time to `www.nus.edu.sg`.

   Earlier, you found that DNS returns different IP addresses for `mail.google.com` when you run `dig` from different host. Use `ping` to find the average round trip time to different IP addresses you found in Question 3, Parts (a) and (b).

5. whois

   The tool `whois` queries domain name databases and provides information about the registrar of a domain name, contact of the organization/person responsible, domain name servers, etc. The tool should be available on UNIX and Mac OS X. You may need to download Windows version of whois here: `http://technet.microsoft.com/en-us/sysinternals/bb897435`.

   (a) Find out who is the domain registrar for the domain `nus.edu.sg` and `google.com` by typing: `whois <domain name>`. For the latter, observe how hackers exploit the WHOIS database for advertisement.

   (b) The WHOIS database also publishes information about the administrator of a domain, if they choose not to hide it. Type `whois jiku.org` to see an example.

THE END