National University of Singapore
School of Computing

CS2105 **DIY Exercise 3** Semester 2 13/14

You may run the following on Linux, Mac OS X, or Microsoft Windows. The behaviour may be slightly different (but should not impact your learning).

You need a network connection for this exercise.

HAVE FUN, AND BE CURIOUS

We will continue to explore network protocols using wireshark.

1. Launch Wireshark. In the field "Filter:", enter

   ```
   udp.port == 67 or udp.port == 68
   ```

   and click "Apply."

   Start capturing packets by typing Ctrl-E. Now, disable and reenable your network interface (how to do this depends on your OS and whether you are using WiFi or wired connection). This action should trigger some exchanges of DHCP packets.

   Now, look at the content of the DHCP ACK packets, and pay attention to the option fields:

   - DHCP Server Identifier
   - IP Address Lease Time
   - Subnet Mask
   - Router
   - Domain Name Server

   (a) What is the meaning of each of these options?

   (b) Now repeat this using different network connections (e.g., at home, at school, public WiFi such as Wireless@SG, Internet tethering with 3G/4G, etc.). Do you see a different set of values? Which network gives the longest lease time? the shortest lease time?

2. Restart your capture. Run `traceroute` to `www.google.com` (or `tracert` on Windows). Let the IP address of the host www.google.com being tracerouted to be x. In the field "Filter:", enter `ip.dst == x`. You should now see a sequence of packets sent and received during the traceroute operation.

   Analyze the sequence of UDP and ICMP messages sent and received, and related it to how `traceroute` works. Pay attention to the TTL field in the IP header of UDP packets and the source IP addresses of the ICMP packets.

3. Find out all the interfaces on your computer. On Windows, run `ipconfig /all` in a command window. If you are using a Mac or Linux, run `ifconfig`.

   What is the IP addresses associated with each of the interface, if any? Are they public IPs or private IPs? What is your current active interface?

4. Print out the routing table on your computer. If you are on Windows, type `ROUTE PRINT` in a command window. If you are using Mac or Linux, run `netstat -rn`.

   Identify the columns that correspond to the destination IP, the gateway, and the interface.

   What is the meaning of the column labeled "gateway"?

5. Use `dig` to look up the IP address of `cs2105-z.comp.nus.edu.sg` when you are not connecting to the NUS campus network (and are not use SoC-VPN).

   Does this IP address explain why you cannot access this host from outside the NUS campus network without SoC-VPN? Why is that?

THE END