Question 4: Network commands in Linux

4.a.1 At the command prompt, type in “`ifconfig`” to find out all the interfaces that your computer has been configured with.
4.a.2 From the output of ifconfig, can you figure out which interface is the ethernet interface, and which one is the “loopback interface”? (Hint: Loopback interface is always assigned the IP address 127.0.0.1).

```
ethernet is usually eth0 or em0 etc.
```

4.a.3 Google for “loopback interface” and find out what it can be useful for.
4.a.4 List the flags assigned to the ethernet interface. Use google to find out what each flag means.

4.b.1 At the command prompt, type in “`netstat -i`”. This should give you an equivalent view of network interfaces available on your computer.
4.b.2 netstat is a generic command for printing all sorts of network information. Try typing in “`netstat -r`” and just “`netstat`”, and explain the output that you see. (Hint: Use “man netstat” to understand the output you see.

4.c.1 We discussed how mappings get established between IP addresses at the network layer and the corresponding ethernet address at the data link layer. Type in “`arp`” to see the arp cache on your machine.

4.c.2 You can also obtain equivalent information about ARP mappings by typing in “`ip neighbour`”. Try other related commands such as “`ip route`” and “`ip link`”. What information did you obtain? What previous commands (from Question 4) gave you similar information as ip route and ip link?

```
the command ip is new to linux. Other unices and even some linux
distributions don't have the ip command. The other commands such as
ifconfig, netstat and arp provide similar information.
```

4.d ***Optional*** Next you will listen to packets passing through your network using `tcpdump`. `tcpdump` can only be run as a superuser (i.e., as “root”. To run as root, you will need to prepend all commands with “sudo” (e.g., “`sudo tcpdump`”). If you do not have sudo permission on your system, you can try this on a virtual machine at http://linuxzoo.net (you will have to register a username. Linuxzoo gives root access by default so you do not have to use “sudo”).
4.d.1 Listen to all packets on the ethernet interface. You can do this by “`sudo tcpdump -i <ethernet-interface-name>`”. What is the name of the ethernet interface? (Hint: Can any of the commands from 4.a or 4.b help here?)
4.d.2 Listening to all packets prints out too much information (there are a lot of packets!). For normal operation and diagnostics, you will want to filter information. This can be done by specifying BPF filters. For example, the following will restrict to only http packets

```
sudo tcpdump icmp
```

Now if you visit some website (say google.com[1]) it should show up in the tcpdump window.
4.d.3 You can restrict to seeing a fixed number of packets, for example the ping and its response (pong). To do this type in `sudo tcpdump -c2 icmp`. Try the ping command again. Notice that tcpdump finishes after 2 packets, whereas the ping command continues to receive responses back. What are the types of the two packets.

[1] google.com is not pingable from the Labs because of security reasons (From the Lecture slides, can you name the attack which used spoofed ICMP Ping packets?). You can instead use calcium.dcs.kcl.ac.uk, wherever you see google.com in this document.

4.d.4 [2]When you ping ‘google.com’, you expect a response from google.com. What host were you getting the response from in 4.d.3? (Hint: use the lecture slides or “man tcpdump” to identify the source of the ICMP echo request or the destination of the echo reply (pong)). Is this the host you were expecting? Why or why not? (Hint: can a single host have multiple DNS names?)

This question does not make sense if you are using calcium instead of google.

4.d.5 You can avoid dealing with DNS names, by asking tcpdump to use IP addresses (use the -n switch: `sudo tcpdump -n —c2 icmp`

Repeat the ping. Does the IP address for google correspond to the ping output?

Obivously it should

4.d.6. You can get more details about the packet by using the -v, -vv and -vvv options. Read about the differences in the manual page for tcpdump, and summarise what you learn.

4.d.7 You can get the details of the packet itself by using the -XX option.

e.g., sudo tcpdump -XX -n dst google.com

By default this prints 95 bytes. To get the full packet, identify what the Maximum Transfer Unit (MTU) is, on your interface, and use the -s option to specify a snaplen larger than that, e.g.

sudo tcpdump -s 1514 XX -n dst google.com

4.e You can obtain much of the above functionality in a GUI using wireshark (if it is installed). Type in “sudo wireshark” to start it up and explore.

4.d.0 When wireshark starts, you need to choose a network interface to monitor. Which one would you choose, based on the above experience?

4.d.1 See if you can right click and follow a TCP stream.

4.d.2 If you only want to obtain http traffic, explore how you might do this by entering a filter expression at the top of the window. What filter expression is needed for http?

you can just type in http. This is a convenience which is not possible in tcpdump. (try typing it in as a BPF program.

[2] This question is irrelevant if you are pinging calcium rather than google. Try this command outside of the college network if you are interested.