TCP/IP Networking Exercises

The purpose of this exercise is to get some practice with using **ping**, **netstat**, **tcpdump**, **traceroute**, **arp**, and **route**.

Before we start we need to make sure that we have tcpdump and traceroute installed on our PC.

To do this, run:

```
sudo apt-get install traceroute tcpdump
```

If the packages are already installed, apt-get will simply say so. If they are not installed, it will download and install the two packages (and any supporting packages required).

Check your network configuration

Check it with:

```
$ ifconfig eth0
```

Do you see an IP address on your network card? It should look like this:

```
eth0      Link encap:Ethernet  HWaddr 52:54:8e:12:66:49
          inet addr:10.10.0.xx  Bcast:10.10.0.255  Mask:255.255.255.0
```

where **xx** is your machine's IP address.

DO NOT DO THE FOLLOWING - it is just for information.

If the eth0 network card does not have a 10.10.0.xx IP address, then it would be configured as follows:

```
$ sudo ifconfig eth0 10.10.0.xx/24
$ sudo route add default gw 10.10.0.254
```

You were asked not to do the above because you are logging in using ssh via the network interface, so you **will** end up breaking your access to your machine.

You machine has other interfaces. Use what you've just done above to look at the other interfaces **eth1** and **lo**.

netstat

Look at your routing table:

```
$ netstat –rn
```

What do you notice? Is the default gateway configured? How do you know? Review the presentation if you are not sure. What is your default gateway? On what network interface is your default gateway valid for?

Here's another way to look at your routing table:

```
$ ip route
```

ping

Let's ping the default gateway:

```
$ ping 10.10.0.254
```

(Stop it with CTRL+C)

Let's ping something outside, on the Internet. For example, nsrc.org

```
$ ping nsrc.org
```

Do you get an answer ?

If not, check:

- That you have a gateway configured
- That in the file /etc/resolv.conf there is an entry for “nameserver”
- Do you notice anything about the response time? How far away is nsrc.org?

Verify 10.10.0.254 is configured as your default gateway:

```
$ ip route
```

Now, remove your default gateway:

```
$ sudo ip route delete default via 10.10.0.254
```

Check that it's gone

```
$ ip route
```

How can you be sure that the default gateway is no longer configured? Now, try to ping the local WWW machine.

```
$ ping 10.10.0.248
```

Now let's ping a machine outside our network (nsrc.org):

```
$ ping nsrc.org
```

The ip address of nsrc.org is 128.223.157.25

```
$ ping 128.223.157.25
```

What do you observe?

What is the consequence of removing the default gateway?

Re-establish the default gateway:

```
$ sudo ip route add default via 10.10.0.254
```

Check that the default gateway is enabled again by pinging nsrc.org:

```
$ ping nsrc.org
```

traceroute

Traceroute to nsrc.org

```
$ traceroute nsrc.org
```

Try again, this time with the -n option:

```
$ traceroute -n nsrc.org
```

Observe the difference with and without the '-n' option. Do you know what it is?

tcpdump

Run tcpdump on your system:

```
$ sudo tcpdump -n -i eth0 icmp
```

(Note the use of the icmp keyword to limit viewing ICMP traffic)

Ask the instructor(s) or your neighbour to ping your machine, and look at your screen.