System Administration and IP Services
TCP/IP Networking Exercises

Practice: ping, netstat, tcpdump, traceroute, arp, route

1. Check your network configuration

Check it with:

```
$ sudo 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
```

Is your machine's IP address.

If you eth0 network card does not have a 10.10.0.xx IP address, then you could configure it:

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

However, as we are using ssh sessions don't do this or you may end up breaking your network connection to your machine.

2. netstat

Look at your routing table:

```
$ sudo 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:

```
$ sudo ip route
```

3. 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, lpnz.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:

```
$ netstat -r
```

Now, remove your default gateway:

```
        $ sudo route delete default
```

Check that it's gone

```
        $ netstat -r
```

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

```
        $ ping 10.10.0.250
```

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

```
        $ ping nsrc.org
```

The ip address of nsrc.org is 128.223.157.19

```
        $ ping 128.223.157.19
```

What do you observe?
What is the consequence of removing the default gateway?

Re-establish the default gateway:

```
     $ sudo route add default gw 10.10.0.254 dev eth0
```

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

```
     $ ping nsrc.org
```

4. 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?

6. 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 neighbor to ping your machine, and look at your screen.
Now delete the default route on your system:

```
     $ sudo route delete default
```

Repeat the ping (ask the instructor or neighbor) What do you notice?