% System Administration and IP Services
% TCP/IP Networking Exercises

## Notes: {-}

These exercises are to practice ping, netstat, tcpdump, traceroute, mtr, route

* lines starting with $ are commands to be typed
* sometimes you will have to replace x and y with actual digits: see below

# 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.y.x  Bcast:10.10.y.255  Mask:
255.255.255.0
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

10.10.y.x is your machine's IP address.

*       x is your pc number
*       y can be calculated from x as follows:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                $ echo '(x+4-1)/4' | bc
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Since we are using SSH to access your machine it definitely has an IP address but if you did want to set it you'd type:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo ifconfig eth0 inet 10.10.y.x/24
$ sudo route add default gw 10.10.y.254
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# 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
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# ping

Let's ping the default gateway on your machine:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```
$ ping 10.10.y.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.y.254 is configured as your default gateway: (see above for how to calcualte it)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```
$ netstat -r
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Since we are using SSH we need to ensure we have a route for the class network before toying with the gateway.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```
$ sudo route add -net 10.10.0.0/16 gw 10.10.y.254
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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.y.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?

# mtr

A usefull tool that combines both ping and traceroute is mtr. It is not installed by default so first let's install it. We don't have a graphical interface installed so we won't install the full mtr package - just the ncurses version (mtr-tiny).

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install mtr-tiny
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Now we can use it to do both ping and traceroute to nsrc.org

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ mtr nsrc.org
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Press q to quit. Now lets' try it again with the -n option

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ mtr -n nsrc.org
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Again press q to quit. If you want to generate a report you can copy/paste into an email asking for support you could use the -r (report) option.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ mtr -r -n nsrc.org
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# 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?