

IP/Unix Preparation Course

May 23, 2010

Exercises: Networking

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

1. Remember to 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 00:12:3f:9d:03:88
          inet addr:67.218.55.67  Bcast:67.218.55.127 Mask:255.255.255.192
```

... where 'xxx' is your IP

If you eth0 network card does not have a 67.218.55.xxx IP, then you could configure it:

```
$ sudo ifconfig eth0 67.218.55.xxx/26
$ sudo route add default 67.218.55.65
```

Additionally, configure your `/etc/resolv.conf` by editing it and adding:

```
nameserver 67.218.55.67
```

Only do this if it has not already been done.

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.

3. PING

Let's ping the default gateway:

```
$ ping 67.218.55.65
```

(Stop it with CTRL+C)

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

```
$ ping lpnz.org
```

Do you get an answer ?

If not, check:

- That you have a gateway
- That you have an `/etc/resolv.conf` that contains a nameserver! (see 1.)

What do you notice about the response time (time=.. ms)?

Remove your default gateway:

```
$ sudo route delete default
```

Control that the default gateway is gone using the `netstat -r` command.

How can you be sure that the default gateway is no longer configured?

Now, try to ping the local NOC machine.

```
$ ping 67.218.55.65
```

lpnz.org

```
$ ping lpnz.org
```

The IP address of lpnz.org

```
$ ping 202.8.44.44
```

What do you observe?

What is the consequence of removing the default gateway?

Re-establish the default gateway:

```
$ sudo route add default 67.218.55.65
```

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

```
$ ping lpnz.org
```

4. TRACEROUTE

Traceroute to lpnz.org

```
$ traceroute lpnz.org
```

Try again, this time with the -n option:

```
$ traceroute -n lpnz.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.

Delete the default route on your system:

```
$ sudo route delete default
```

Repeat the ping (ask the instructor or neighbor)

What do you notice?

Linux specific alternatives

1. Remember to check your network configuration!

Check it with:

```
$ sudo ip address show dev eth0
```

Do you see an IP address on your network card?

It should look like this:

```
ip address show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP qlen 1000
    link/ether 00:12:3f:9d:03:88 brd ff:ff:ff:ff:ff:ff
    inet 67.218.55.67/26 brd 67.218.55.127 scope global eth0
    inet6 fe80::212:3fff:fe9d:388/64 scope link
        valid_lft forever preferred_lft forever
```

... where 'xxx' is your IP

If your eth0 network card does not have a 67.218.55.xxx IP, then you could configure it:

```
$ sudo ip address add 67.218.55.xxx/26 dev eth0
$ sudo ip route add default via 67.218.55.65
```

Additionally, configure your `/etc/resolv.conf` by editing it and adding:

```
nameserver 67.218.55.67
```

Only do this if it has not already been done.

2. NETSTAT

Look at your routing table:

```
$ sudo ip route
```

What do you notice? Is the default gateway configured? How do you know? Review the presentation if you are not sure.