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 bge0 inet
```

Do you see an IP address on your network card?

It should look like this:

```
bge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
      options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
inet 196.200.218.x netmask 0xffffff00 broadcast 196.200.218.255
```

... where 'x' is your IP

If you bge0 network card does not have a 196.200.218.x IP, then configure it:

```
      $ sudo ifconfig bge0 196.200.219.x/24
      $ sudo route add default 196.200.218.254
```

Additionally, configure your `/etc/resolv.conf` by editing it and adding: nameserver 196.200.223.1. 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 196.200.218.254
```

(Stop it with CTRL+C)

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

```
$ ping afnog.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 196.200.223.1
```

afnog.org

```
$ ping afnog.org
```

The IP address of afnog.org

```
$ ping 196.216.2.34
```

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

Re-establish the default gateway:

```
$ sudo route add default 196.200.218.254
```

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

```
$ ping afnog.org
```

4. TRACEROUTE

Traceroute to afnog.org

```
$ traceroute afnog.org
```

Try again, this time with the -n option:

```
$ traceroute -n afnog.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 bge0 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?