Introduction to Unix

May 10, 2009

Exercises: More Networking

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

NOTE: These exercises should be carried out as the '*root*' user

1. Remember to check your network configuration!

* Check it with:

```
      # ifconfig em0 inet
```

-> Do you see an IP address on your network card ?

It should look like this:

```
      em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
            options=8<VLAN_MTU>
            inet 196.200.219.x netmask 0xffffff00 broadcast 196.200.219.255
```

... where 'x' is your IP

* Just in case, kill the DHCP client

```
      # killall dhclient
```

* If you em0 netcard does not have a 196.200.918.x IP, then configure it:

```
      # ifconfig em0 196.200.219.x/24
      # route add default 196.200.219.254
```

* Additionnally, configure your /etc/resolv.conf by editing it and adding:

```
  nameserver 196.200.223.1
```

2. NETSTAT

* Look at your routing table:

```
      # netstat -rn
```

-> What do you notice ? Is the default gateway configured ?
-> How do you know ?

3. PING

* Let's ping the default gateway:

```
      # ping 196.200.219.254
```

(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:

  # 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 196.200.219.1

  - 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:

      # route add default 196.200.219.254

* 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
```

5. ROUTE

```
* Remove your default route

      # route delete default
```

* Add a route to the AfNOG backbone network through the gateway:

```
      # route add 196.200.223.0/24 196.200.219.254
```

* Try to ping the backbone NOC:

```
      # ping 196.200.223.1
```

* Try to ping afnog.org:

```
      # ping afnog.org
```

* Try to ping 196.216.2.34:

```
      # ping 196.216.2.34
```

-> What do you notice ?
-> What do you conclude ?

* Restore the default route:

```
      # route add default 196.200.219.254
```

* Look at the routing table with the netstat -rn command:

```
      # netstat -rn
```

-> What do you notice ?

-> Which route will be used to reach 196.200.223.1 ?

-> Which route will be used to reach 196.216.2.34 ?

* Let's imagine we have a network 10.10.10.0/24, which is reachable via another router 196.200.219.250

-> What command would you type if you wanted to add this route to your machine ?

6. TCPDUMP

* Run tcpdump on your system:

```
      # tcpdump -n -i em0 icmp
```

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

* Ask the instructor(s) to ping your machine, and look at your screen, we will do this in turn

* Delete the default route on your system:

```
      # route delete default
```

* Repeat the ping (ask the instructor)

-> What do you notice ?