AfNOG Workshop, May 2009, Cairo, Egypt

Track SA-E - 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 196.200.218.x netmask 0xffffff00 broadcast 196.200.218.255
```

... where 'x' is your IP

* If you em0 netcard does not have a 196.200.218.x IP, then configure it:

```
# ifconfig em0 196.200.218.x/24
# route add default 196.200.218.254
```

* Remember to add your IPv6 address:

```
# ifconfig em0 inet6 2001:4348:0:218:196:200:218:X
# route add -inet6 default  2001:4348:0:218:196:200:218:254
```

* Check the network configuration again with ifconfig

```
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
      options=19b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4>
      ether 00:1e:0b:b5:a3:c9
      inet 196.200.218.X netmask 0xffffff00 broadcast 196.200.218.255
      inet6 2001:4348:0:218:196:200:218:X prefixlen 64
      media: Ethernet autoselect (10baseT/UTP <full-duplex>)
      status: active
```

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

```
nameserver 196.200.223.1
```

(you can also try 2001:4348:0:218:196:200:218:253 - it should work!)

2. NETSTAT

* Look at your routing table:

```
# netstat -rn
```

and

```
# netstat -rn -f inet6
```

-> What do you notice ? Is the default gateway configured ?
-> How do you know ?
-> Is this true for both IPv4 and IPv6 ?

3. PING

* Let's ping the default gateway:

```
      # ping 196.200.218.254
```

    (Stop it with CTRL+C)

      Try again with 2001:4348:0:218:196:200:218:254

* Let's ping something outside, on the Internet. For example, www.afrinic.net

```
      # ping www.afrinic.net
```

-> Do you get an answer ?

      What about IPv6 ?

```
      # ping6 2001:42d0::200:80:1
      # ping6 www.afrinic.net
```

  If not, check:

  - that you have a gateway in IPv4 **AND** IPv6
  - 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
  # route delete -inet6 default
```

* Control that the default gateway is gone using the netstat -r, and netstat -r -f inet6, commands.

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

* Now, try to ping:

  - the local NOC machine:

```
      # ping 196.200.218.253
      # ping6 2001:4348:0:218:196:200:218:253
```

  - www.afrinic.net:

```
      # ping www.afrinic.net
      # ping6 www.afrinic.net
```

  - The IP address of www.afrinic.net

```
      # ping 196.216.2.1
      # ping6 2001:42d0::200:80:1
```

-> What do you observe ?

-> What is the consequence of removing the default gateway (in V4 and V6) ?

* Re-establish the default gateway:

```
      # route add default 196.200.218.254
      # route add -inet6 default 2001:4348:0:218:196:200:218:254
```

* Check that the default gateway is enabled again by pinging www.afrinic.net:

```
      # ping www.afrinic.net
      # ping6 www.afrinic.net
```

4. TRACEROUTE

```
* Traceroute to www.afrinic.net

      # traceroute www.afrinic.net
      # traceroute6 www.afrinic.net

* Try again, this time with the -n option:

      # traceroute -n www.afrinic.net
      # traceroute6 -n www.afrinic.net

-> Observe the difference with and without the '-n' option
```

5. ROUTE (IPv4 only)

```
* Remove your default routes

      # route delete default

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

      # route add 196.200.223.0/24 196.200.218.254

* Try to ping the backbone NOC:

      # ping 196.200.223.1

* Try to ping www.afrinic.net:

      # ping www.afrinic.net

* Try to ping 196.216.2.1:

      # ping 196.216.2.1

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

* Restore the default route:

      # route add default 196.200.218.254

* 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 196.200.218.250

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

6. TCPDUMP (IPv4 only)

* Run tcpdump on your system:

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

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

* Ask someone else in the room to ping your machine, and look at your screen

* Delete the default route on your system:

```
# route delete default
```

* Repeat the ping

-> What do you notice ?