Exercices: Réseaux

ping, netstat, tcpdump, traceroute, arp, route

1. VERIFIER VOTRE CONFIGURATION RESEAU!

```
$ sudo ifconfig eth0
```

Voyez-vous l'adresse IP de votre carte réseau ?

Il devrait ressembler a:

eth0 Link encap:Ethernet HWaddr 00:17:08:53:3D:2D
inet addr:10.55.1.2 Bcast:196.200.57.63
Mask:255.255.255.192
inet6 addr: fe80::217:8ff:fe53:3d2d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST
MTU:1500 Metric:1

... ou est votre adresse IP ?

Si votre carte réseau n'a pas d'adresse IP, configurer une (les formateurs vous donneront les adresses a utiliser:

```
$ sudo ifconfig eth0 10.55.1.x/26
$ sudo route add default 10.55.1.1
```

x vous sera donné par les formateurs.

Configurer aussi votre `/etc/resolv.conf` en l'éditant avec le serveur DNS local:
Faites ceci uniquement s'il n'était fait

2. NETSTAT

Regarder votre table de routage

```
$ sudo netstat –rn
```

Que remarquez-vous ? La passerelle par défaut est configurée ?

3. PING

Pinguer la passerelle par défaut:

```
$ ping 10.55.1.1
```

(Arrêter avec CTRL+C)

Pinguer quelque chose sur l'Internet

```
$ ping afnog.org
```

Avez-vous une réponse?

Si non, verifier:

- que vous avez une passerelle
- que `/etc/resolv.conf` contient un serveur

Que constatez-vous en terme de temps de réponse (time=.. ms)?

Enlevez votre passerelle par défaut:

```
$ sudo route delete default
```

Vérifiez que la passerelle est supprimée avec netstat -r

Maintenant, essayer de pinguer 196.1.95.3

```
$ ping 196.1.95.3
```

www.ucad.sn

```
$ ping www.ucad.sn
```

Qu'observez-vous ?

Quelle est la conséquence de la suppression de la passerelle par défaut ?

Remettez la passerelle par defaut:

```
$ sudo route add default gw 10.55.1.1
```

Vérifiez que la passerelle par défaut est de nouveau active en pingant de nouveau www.ucad.sn:

```
$ ping www.ucad.sn
```

4. TRACEROUTE

Tracez la route vers nsrc.org

```
$ traceroute nsrc.org
```

Essayez de nouveau avec l'option –n :

```
$ traceroute -n nsrc.org
```

Quelle est la différence ?

5. TCPDUMP

Lancez tcpdump sur votre système :

```
$ sudo tcpdump -n -i eth0 icmp
```

(icmp limite le trafic aux PAQUETS ICMP)

Demandez aux formateurs ou voisins de pinguer votre machine et regardez sur votre écran

Supprimer la route par défaut sur votre système:

```
$ sudo route delete default
```

Répétez le ping (Demandez aux formateurs ou voisins)

Que constatez-vous ?