TP 6

1. Routage

1.1. Préliminaires

Lancez la commande `/sbin/route -n`

```
thmoreau@avoranfix:~/espaces/travail/L2/Reseau/TP6$ /sbin/route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         10.0.103.254    0.0.0.0         UG    0      0        0 eth0
10.0.103.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Comparez avec l'adresse d'une machine voisine dans la même salle : êtes-vous bien dans le même réseau ?

Ma machine :

```
thmoreau@avoranfix:~/espaces/travail/L2/Reseau/TP6$ ping -4 avoranfix
PING avoranfix.emi.u-bordeaux.fr (10.0.103.9) 56(84) bytes of data.
64 bytes from avoranfix.emi.u-bordeaux.fr (10.0.103.9): icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from avoranfix.emi.u-bordeaux.fr (10.0.103.9): icmp_seq=2 ttl=64 time=0.122 ms
64 bytes from avoranfix.emi.u-bordeaux.fr (10.0.103.9): icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from avoranfix.emi.u-bordeaux.fr (10.0.103.9): icmp_seq=4 ttl=64 time=0.021 ms
64 bytes from avoranfix.emi.u-bordeaux.fr (10.0.103.9): icmp_seq=5 ttl=64 time=0.021 ms
^C
--- avoranfix.emi.u-bordeaux.fr ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 78ms
rtt min/avg/max/mdev = 0.016/0.043/0.122/0.040 ms
```

Machine voisine :

```
thmoreau@avoranfix:~/espaces/travail/L2/Reseau/TP6$ ping -4 babaorum
PING babaorum.emi.u-bordeaux.fr (10.0.103.10) 56(84) bytes of data.
64 bytes from babaorum.emi.u-bordeaux.fr (10.0.103.10): icmp_seq=1 ttl=64 time=0.191 ms
64 bytes from babaorum.emi.u-bordeaux.fr (10.0.103.10): icmp_seq=2 ttl=64 time=0.489 ms
64 bytes from babaorum.emi.u-bordeaux.fr (10.0.103.10): icmp_seq=3 ttl=64 time=0.123 ms
64 bytes from babaorum.emi.u-bordeaux.fr (10.0.103.10): icmp_seq=4 ttl=64 time=0.127 ms
64 bytes from babaorum.emi.u-bordeaux.fr (10.0.103.10): icmp_seq=5 ttl=64 time=0.136 ms
^C
--- babaorum.emi.u-bordeaux.fr ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 80ms
rtt min/avg/max/mdev = 0.123/0.213/0.489/0.140 ms
```

On remarque bien qu'elles sont sur le même réseau.

La route par défaut (`0.0.0.0`), qui utilise une passerelle (quelle est son adresse IP ?)

La route par défaut utilise la passerelle 10.0.103.254.

On peut aussi utiliser la version plus moderne `ip route ls` . À quoi correspond le suffixe `/24` ?

```
thmoreau@avoranfix:~/espaces/travail/L2/Reseau/TP6$ ip route ls
default via 10.0.103.254 dev eth0 onlink
10.0.103.0/24 dev eth0 proto kernel scope link src 10.0.103.9
```

Le suffixe /24 correspond au masque du réseau.

Pour observer en IPv6, on utilise `ip -6 route ls`

```
thmoreau@avoranfix:~/espaces/travail/L2/Reseau/TP6$ ip -6 route ls
::1 dev lo proto kernel metric 256 pref medium
2001:660:6101:800:103::/80 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
default via fe80::5a20:b1ff:feb1:2300 dev eth0 proto ra metric 1024 expires 8475sec hoplimit 25 pref
 medium
```

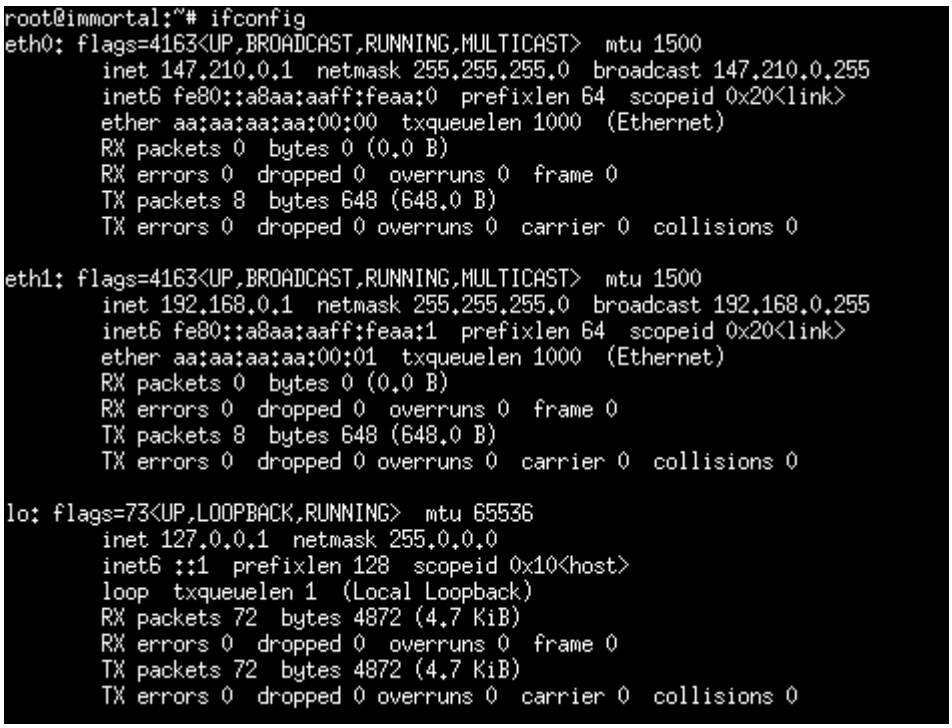
1.2. Routage basique

Grave :

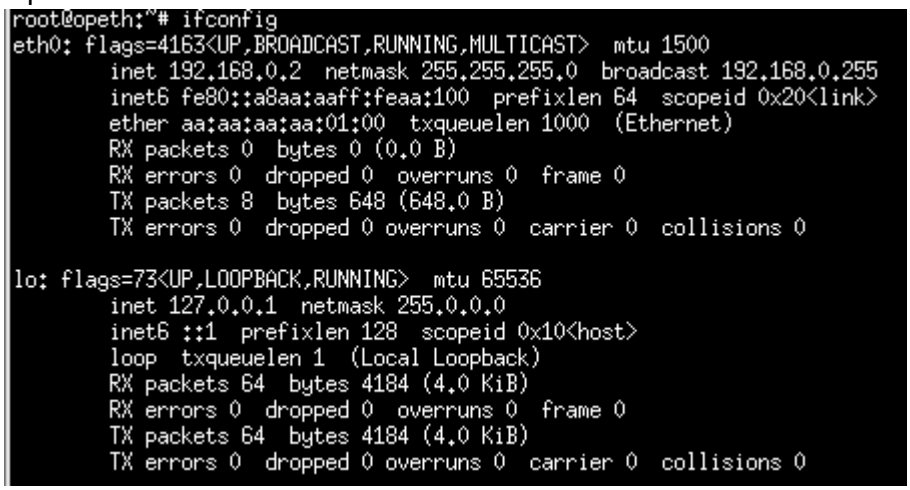
```
root@grave:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 147.210.0.2  netmask 255.255.255.0  broadcast 147.210.0.255
        inet6 fe80::a8aa:aaff:feaa:300  prefixlen 64  scopeid 0x20<link>
        ether aa:aa:aa:aa:03:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 648 (648.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 64  bytes 4184 (4.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 4184 (4.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Immortal :



Opeth :



Syl :

Vérifiez avec 'ping' que les machines peuvent communiquer dans leurs réseaux locaux respectifs.

```
root@grave:~# ping 147.210.0.1
PING 147.210.0.1 (147.210.0.1) 56(84) bytes of data.
64 bytes from 147.210.0.1: icmp_seq=1 ttl=64 time=0.329 ms
64 bytes from 147.210.0.1: icmp_seq=2 ttl=64 time=0.313 ms
64 bytes from 147.210.0.1: icmp_seq=3 ttl=64 time=0.306 ms
^C
--- 147.210.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.306/0.316/0.329/0.009 ms
root@grave:~# ping 192.168.0.2
ping: connect: Network is unreachable
root@grave:~# ^C
root@grave:~# ping 192.168.0.3
ping: connect: Network is unreachable
```

grave peut communiquer avec immortal mais pas avec opeth et syl.

```
root@immortal:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=0.575 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=0.243 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=0.277 ms
^C
--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.243/0.365/0.575/0.149 ms
root@immortal:~# ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=0.532 ms
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=0.290 ms
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.234 ms
^C
--- 192.168.0.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.234/0.352/0.532/0.129 ms
root@immortal:~# ping 147.210.0.2
PING 147.210.0.2 (147.210.0.2) 56(84) bytes of data.
64 bytes from 147.210.0.2: icmp_seq=1 ttl=64 time=0.268 ms
64 bytes from 147.210.0.2: icmp_seq=2 ttl=64 time=0.253 ms
64 bytes from 147.210.0.2: icmp_seq=3 ttl=64 time=0.307 ms
^C
--- 147.210.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.253/0.276/0.307/0.022 ms
```

En revanche, immortal peut communiquer avec toutes les autres machines.

Afficher les tables de routage avec la commande 'route -n'.

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

```
root@immortal:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

```
root@opeth:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Congurez les tables de routage des différentes machines à l'aide de la commande 'route', pour que tout le monde puisse communiquer avec tout le monde

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.0.1     0.0.0.0         UG    0      0        0 eth0
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.0.1     0.0.0.0         UG    0      0        0 eth0
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Faites un ping entre opeth et grave. Lancez `tcpdump -n -i any` sur immortal afin d'affcher le trafic qui circule..

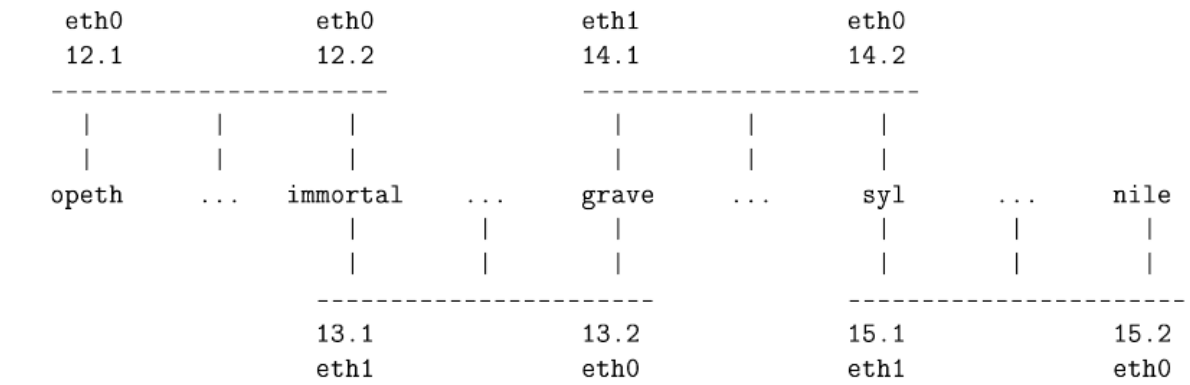
```
root@immortal:~# tcpdump -n -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
15:59:25.642603 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 1, length 64
15:59:25.642644 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 1, length 64
15:59:25.642990 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 1, length 64
15:59:25.642997 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 1, length 64
15:59:26.643920 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 2, length 64
15:59:26.643933 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 2, length 64
15:59:26.645068 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 2, length 64
15:59:26.645072 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 2, length 64
15:59:27.645180 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 3, length 64
15:59:27.645191 IP 147.210.0.2 > 192.168.0.2: ICMP echo request, id 718, seq 3, length 64
15:59:27.646544 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 3, length 64
15:59:27.646549 IP 192.168.0.2 > 147.210.0.2: ICMP echo reply, id 718, seq 3, length 64
15:59:30.645646 ARP, Request who-has 147.210.0.1 tell 147.210.0.2, length 46
15:59:30.645678 ARP, Reply 147.210.0.1 is-at aa:aa:aa:aa:00:00, length 28
15:59:30.647864 ARP, Request who-has 192.168.0.2 tell 192.168.0.1, length 28
15:59:30.649092 ARP, Reply 192.168.0.2 is-at aa:aa:aa:aa:01:00, length 46
```

```
16:00:58.137899 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 1, length 64
16:00:58.137919 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 1, length 64
16:00:58.139018 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 1, length 64
16:00:58.139023 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 1, length 64
16:00:59.139349 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 2, length 64
16:00:59.139365 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 2, length 64
16:00:59.141138 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 2, length 64
16:00:59.141142 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 2, length 64
16:01:00.140611 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 3, length 64
16:01:00.140623 IP 147.210.0.2 > 192.168.0.3: ICMP echo request, id 719, seq 3, length 64
16:01:00.141526 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 3, length 64
16:01:00.141528 IP 192.168.0.3 > 147.210.0.2: ICMP echo reply, id 719, seq 3, length 64
16:01:03.141622 ARP, Request who-has 147.210.0.1 tell 147.210.0.2, length 46
16:01:03.141644 ARP, Reply 147.210.0.1 is-at aa:aa:aa:aa:00:00, length 28
16:01:03.143316 ARP, Request who-has 192.168.0.1 tell 192.168.0.3, length 46
16:01:03.143324 ARP, Reply 192.168.0.1 is-at aa:aa:aa:aa:00:01, length 28
```

grave peut maintenant communiquer avec opeth ainsi que syl.

1.3. Routage Avancé

Voici une nouvelle configuration, composée de 4 sous-réseaux /24 dans le réseau 147.210.0.0/16 :



Voici la liste des configurations :

```
root@opeth:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.12.2    0.0.0.0         UG    0      0        0 eth0
147.210.12.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

```
root@immortal:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.13.2    0.0.0.0         UG    0      0        0 eth1
147.210.12.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.13.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.12.0    147.210.13.1    255.255.255.0   UG    0      0        0 eth0
147.210.13.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.14.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
147.210.15.0    147.210.14.2    255.255.255.0   UG    0      0        0 eth1
```

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.14.1    0.0.0.0         UG    0      0        0 eth0
147.210.14.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.15.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

```
root@nile:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.15.1    0.0.0.0         UG    0      0        0 eth0
147.210.15.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Tentative de communication opeth -> nile :

```
root@opeth:~# traceroute 147.210.15.2
traceroute to 147.210.15.2 (147.210.15.2), 30 hops max, 60 byte packets
 1  147.210.12.2 (147.210.12.2)  0.376 ms  0.287 ms  0.268 ms
 2  147.210.13.2 (147.210.13.2)  0.862 ms  0.852 ms  0.837 ms
 3  147.210.14.2 (147.210.14.2)  1.998 ms  1.979 ms  1.955 ms
 4  147.210.15.2 (147.210.15.2)  1.941 ms  1.927 ms  1.897 ms
```

Tentative de communication nile -> opeth :

```
root@nile:~# traceroute 147.210.12.1
traceroute to 147.210.12.1 (147.210.12.1), 30 hops max, 60 byte packets
 1  147.210.15.1 (147.210.15.1)  0.252 ms  0.269 ms  0.251 ms
 2  147.210.14.1 (147.210.14.1)  0.651 ms  0.639 ms  0.624 ms
 3  147.210.13.1 (147.210.13.1)  1.135 ms  1.114 ms  1.255 ms
 4  147.210.12.1 (147.210.12.1)  2.019 ms  1.999 ms  1.977 ms
```

Aucun échec dans les deux sens donc le routage a bien été effectué.

2. Firewall

Au sein d'un réseau d'entreprise, quelle différence y a-t-il entre la DMZ et le réseau interne des employés ?

La DMZ a pour but de renforcer la sécurité du réseau local, donc des employés.

Nous venons donc d'activer le firewall sur immortal. Plus aucun trafic réseau n'est autorisé vers ou à travers immortal. Vérifiez avec ping.

```
root@nile:~# ping 147.210.0.2
PING 147.210.0.2 (147.210.0.2) 56(84) bytes of data.
^C
--- 147.210.0.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1007ms
```

Autorisez le ping (c'est-à-dire le protocole icmp) du réseau Interne vers Internet, sans autoriser l'inverse.

```
root@immortal:~# iptables -A FORWARD -i eth2 -o eth0 -p icmp -j ACCEPT
```

Faites un test ping, constatez que cela ne fonctionne pas

```
root@nile:~# ping 147.210.0.2
PING 147.210.0.2 (147.210.0.2) 56(84) bytes of data.
^C
--- 147.210.0.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Autorisez l'accès au web depuis les machines du réseau interne.

Maintenant on active le « catch all » des réponses :

```
root@immortal:~# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
[  312.354708] nf_conntrack version 0.5.0 (1536 buckets, 6144 max)
```

```
root@nile:~# ping 147.210.0.2
PING 147.210.0.2 (147.210.0.2) 56(84) bytes of data.
64 bytes from 147.210.0.2: icmp_seq=1 ttl=63 time=0.474 ms
64 bytes from 147.210.0.2: icmp_seq=2 ttl=63 time=0.443 ms
^C
--- 147.210.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.443/0.458/0.474/0.015 ms
```

A présent il n’y a plus de pertes de paquets.