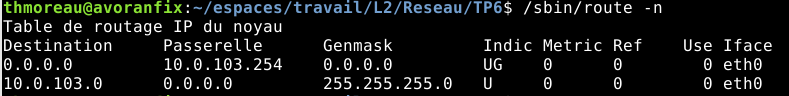
TP 6

# 1. Routage

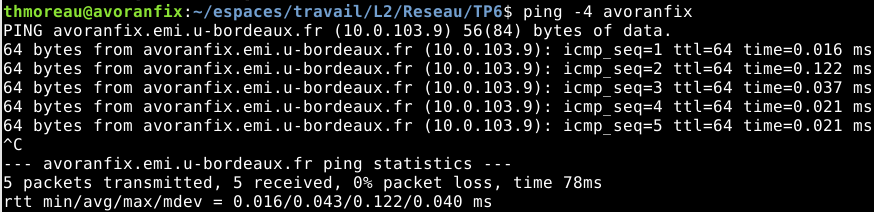
## 1.1. Préliminaires

### Lancez la commande /sbin/route -n

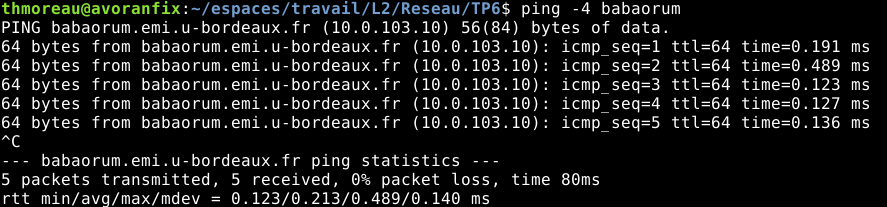


### Comparez avec l'adresse d'une machine voisine dans la même salle : êtes-vous bien dans le même réseau ?

Ma machine :



Machine voisine :



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 ?)

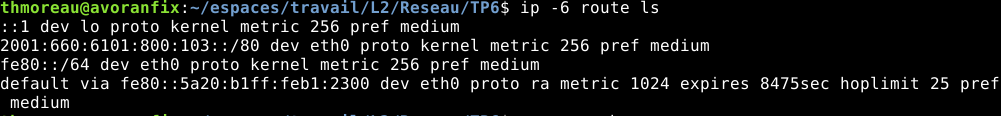
La route par défaut utilise la passerelle 10.0.103.254.

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



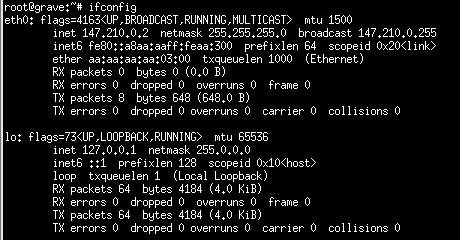
Le suffixe /24 correspond au masque du réseau.

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

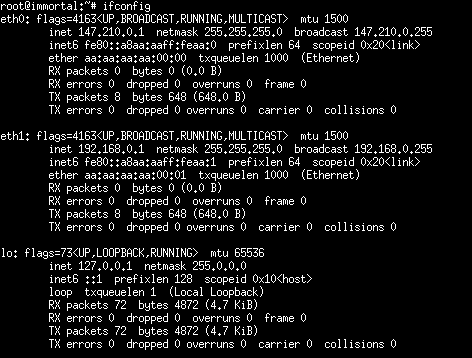


## 1.2. Routage basique

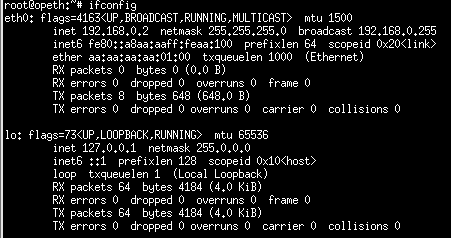
Grave :



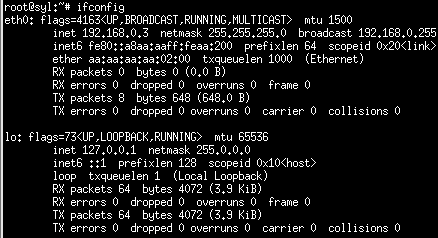
Immortal :



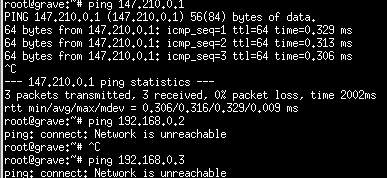
Opeth :



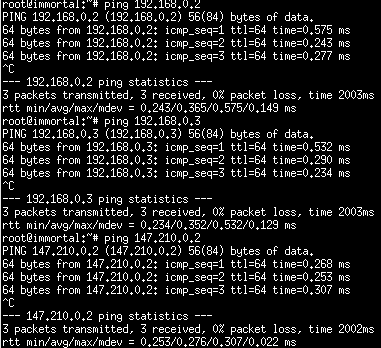
Syl :



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



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



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

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

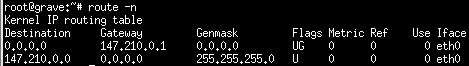


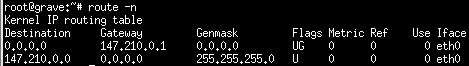


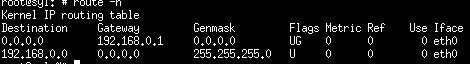




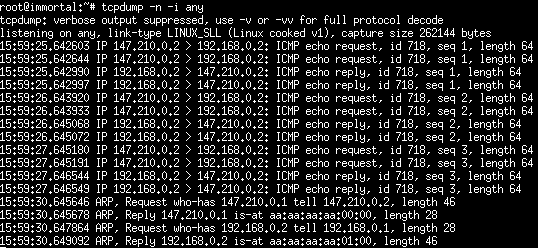
### Congurez les tables de routage des différentes machines à l'aide de la commande 'route', pour que tout le monde puisse communiquer avec tout le monde







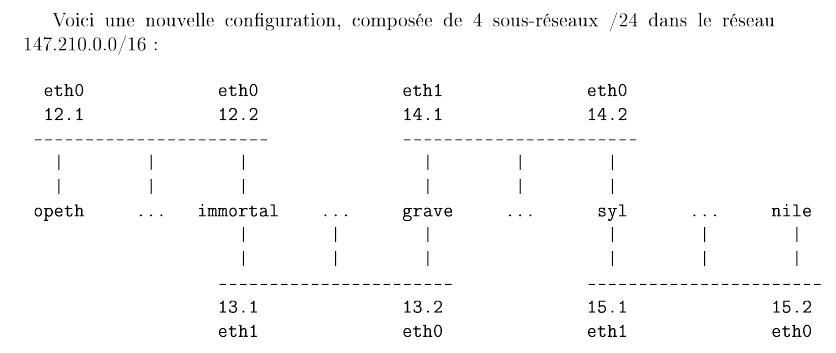
### Faites un ping entre opeth et grave. Lancez tcpdump -n -i any sur immortal afin d'affcher le trafic qui circule..



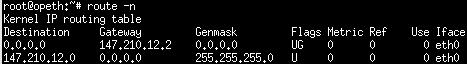


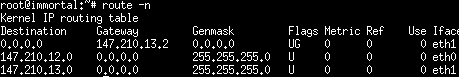
grave peut maintenant communiquer avec opeth ainsi que syl.

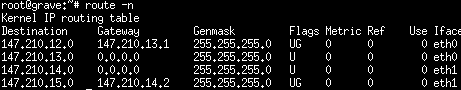
## 1.3. Routage Avancé

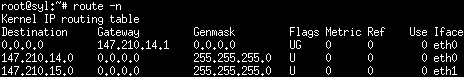


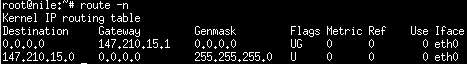
Voici la liste des configurations :



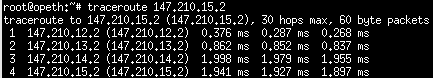




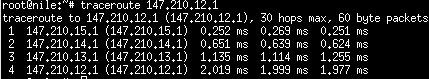




Tentative de communication opeth -> nile :



Tentative de communication nile -> opeth :



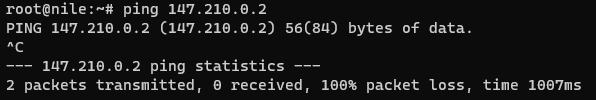
Aucun échec dans les deux sens donc le routage a bien été effectué.

# 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.

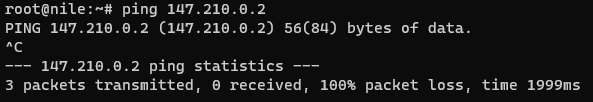
### Nous venons donc d'activer le firewall sur immortal. Plus aucun trafic réseau n'est autorisé vers ou à travers immortal. Vérifiez avec ping.



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



### Faites un test ping, constatez que cela ne fonctionne pas



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

Maintenant on active le « catch all » des réponses :



Text

Description automatically generated

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