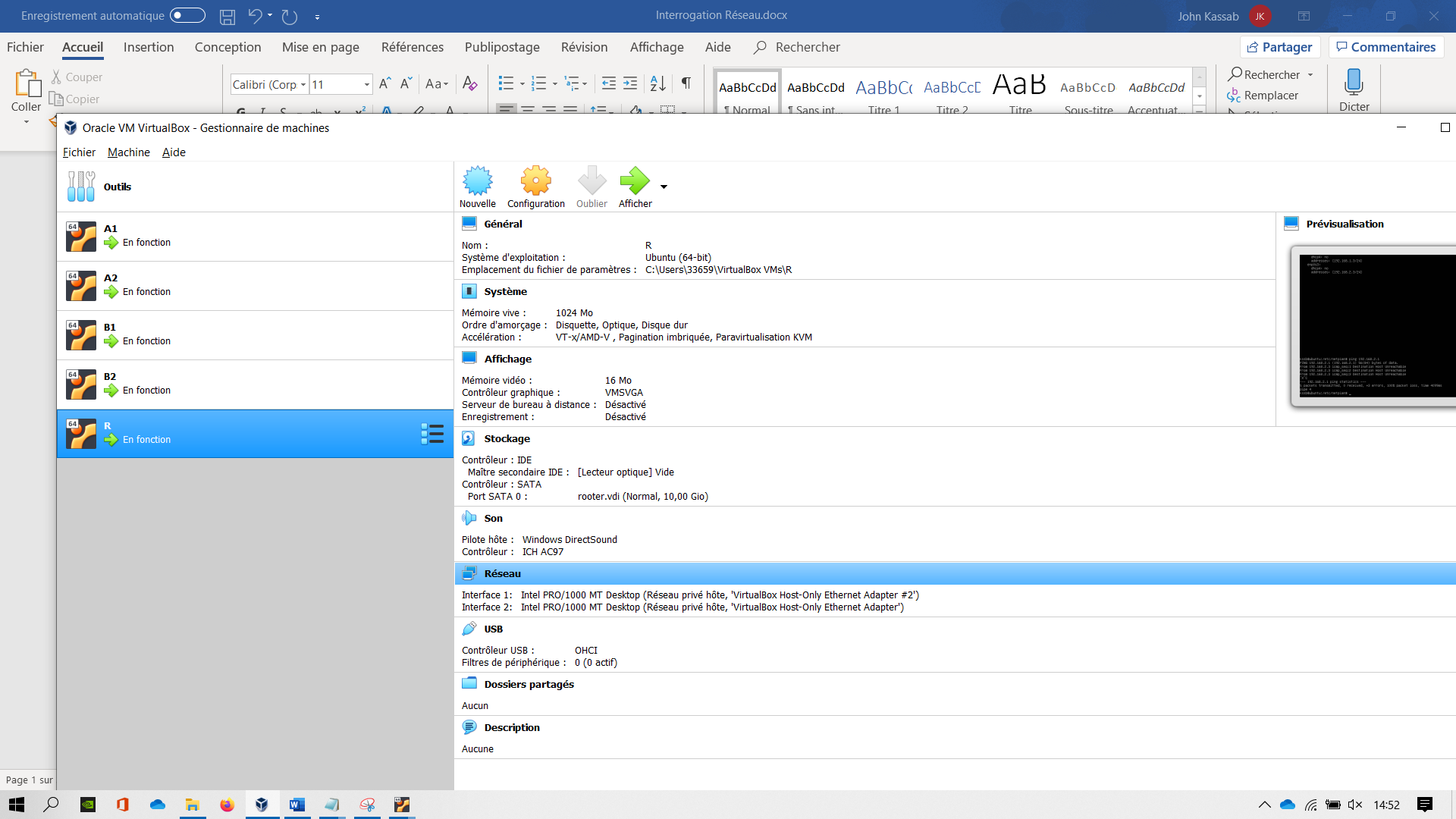
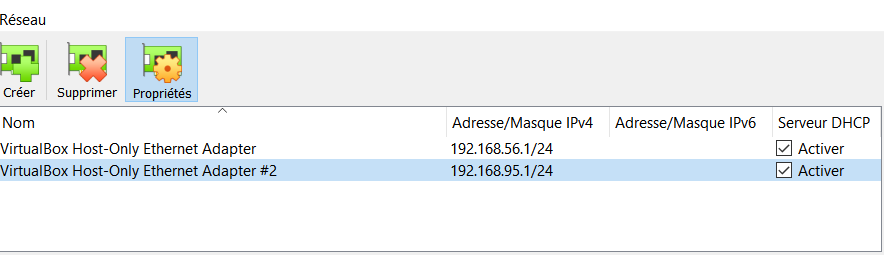
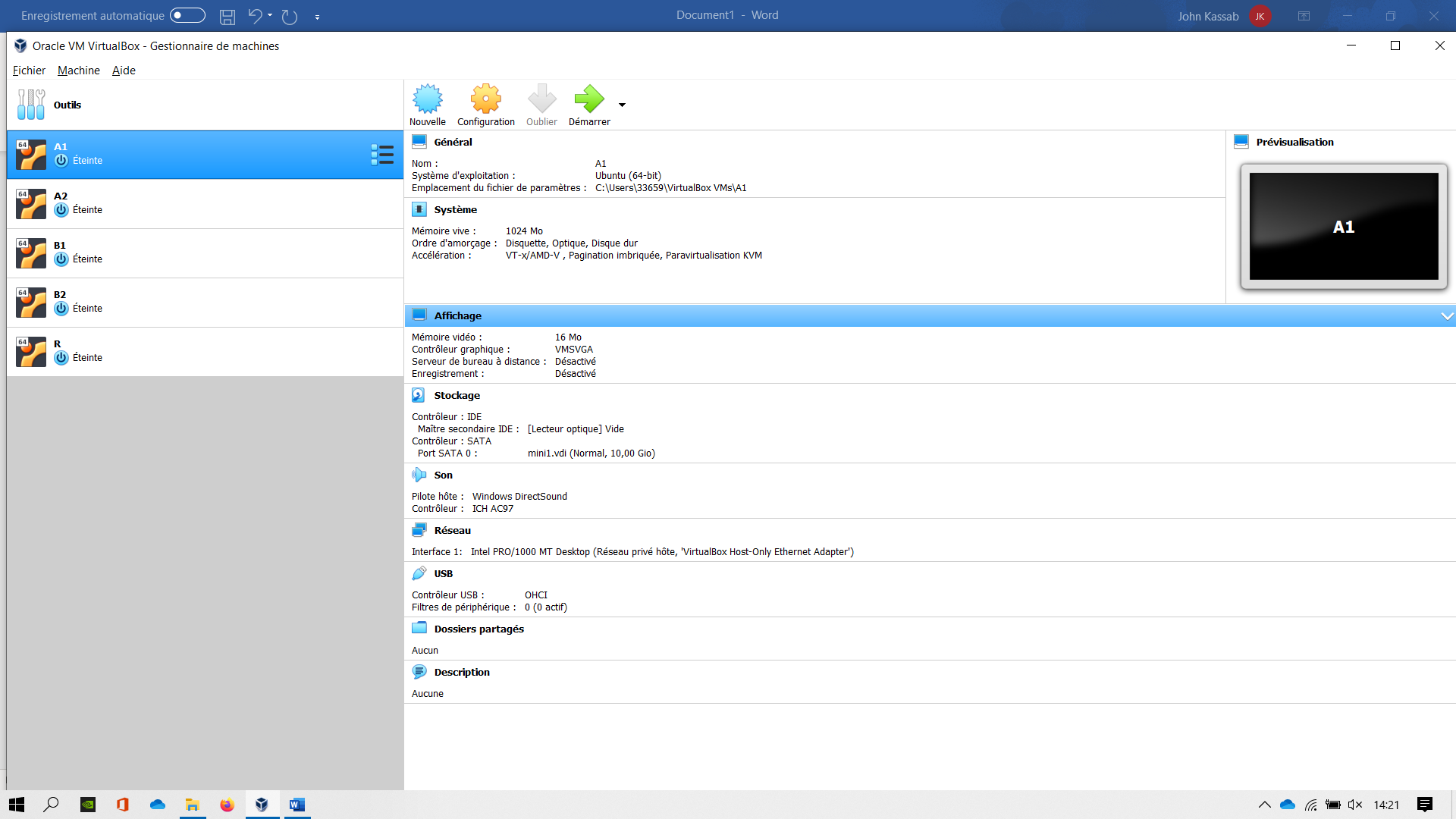
Interrogation Réseau | John KASSAB

On place les 5 machines en réseau privé hôte



2 interfaces réseaux pour le rooter (interface 1 et 2)





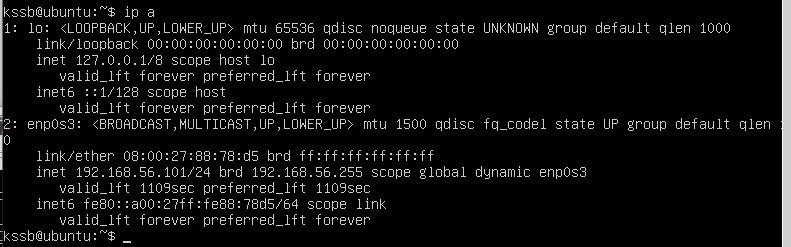
Interface 1 pour A1 et A2

Interface 2 pour B1 et B2

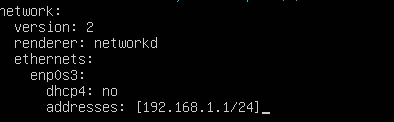
Dans chaque VM :

Commencer par faire un ip a. On note pr chaque VM si elles sont en enp0s3 ou enp0s8.

Ici elles sont toutes en enp0s3.



Puis sudo nano /ect/netplan/01-netcfg.yaml



On met le dhcp4 en « no » sur toutes les VM puis on attribue une adresse IP a chacune des VM

Pour la A1 : 192.168.1.1/24

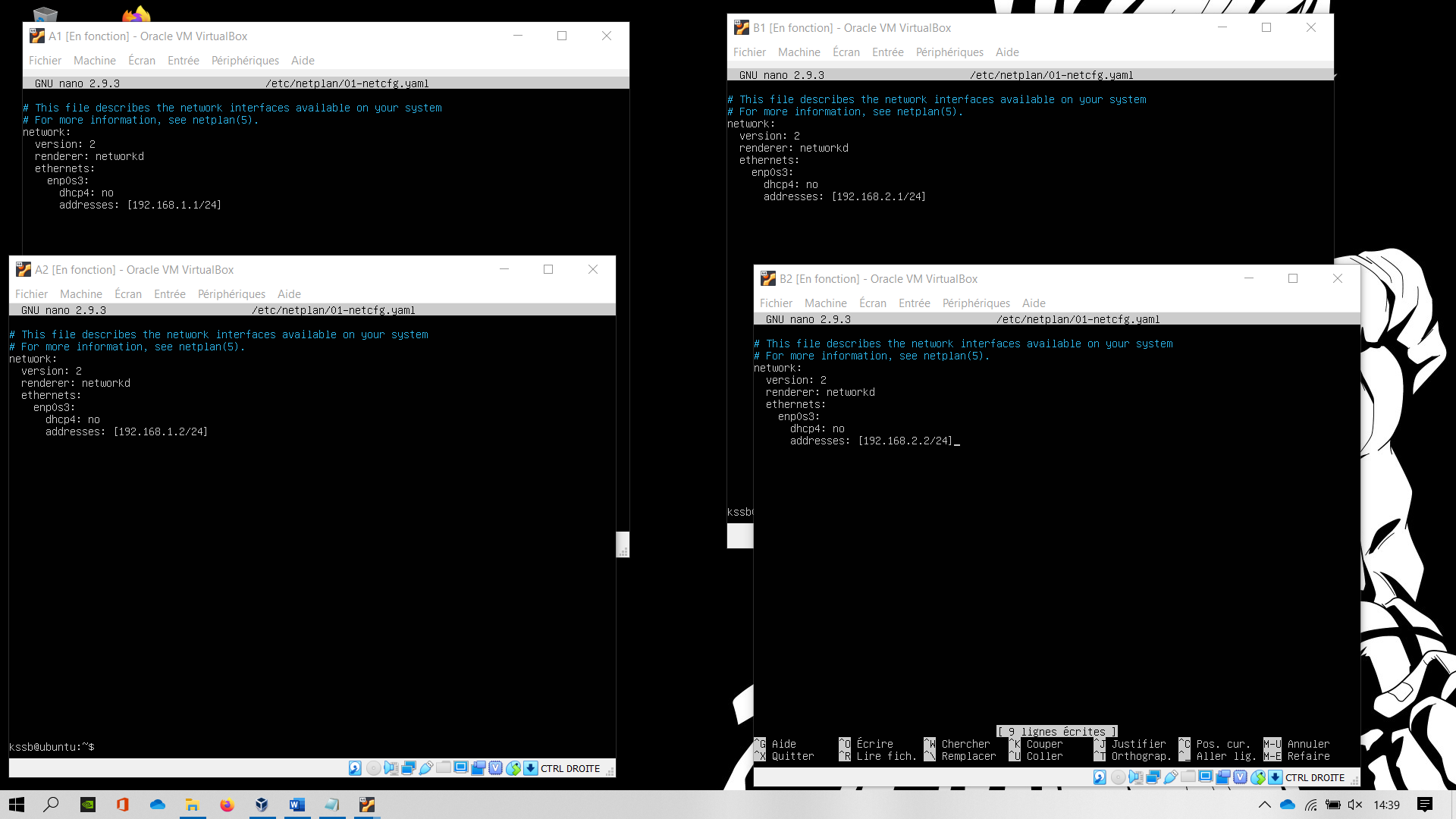
A2 : 192.168.1.2/24

B1 : 192.168.2.1/24

B2 : 192.168.2.2/24

Dans le rooter on placera deux sous réseau avec comme IP 192.168.1.3 pour A1 et A2

Et 192.168.2.3 pour B1 et B2.



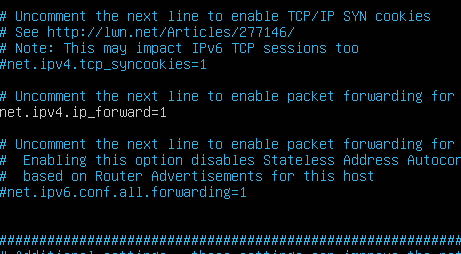
Ce qui nous donne la première étape pour les VM A1,A2,B1 et B2.

Puis on applique les changements avec la commande « sudo netplan apply »

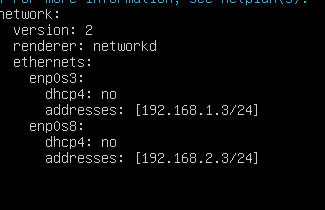
Dans le rooter :

Commencer par faire un sudo nano /etc/sysctl.conf ---> supprimer le "#" devant la ligne

« net.ipv4.ip\_forward=1. »



Faire un sudo nano /etc/netplan/01-netcfg.yaml

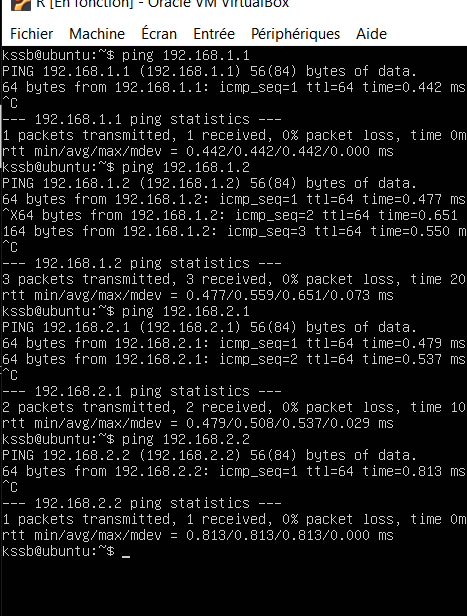


[192.168.1.3/24] reliera au rooter A1 et A2

[192.168.1.3] reliera au rooter B1 et B2

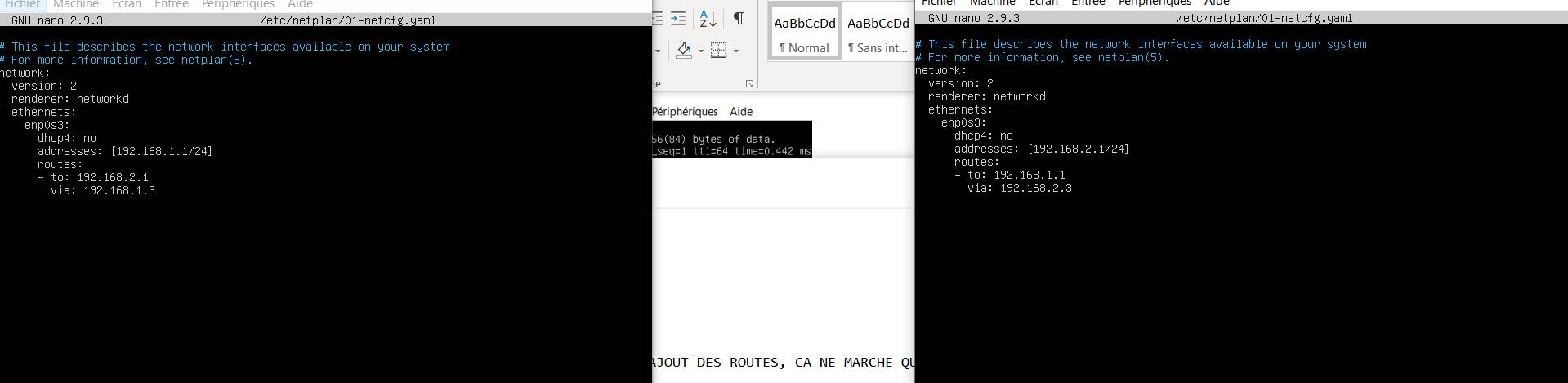
Puis sudo netplan apply sur R pour appliquer les changements.

A partir de la on peut pinger toutes les VM à partir de R.

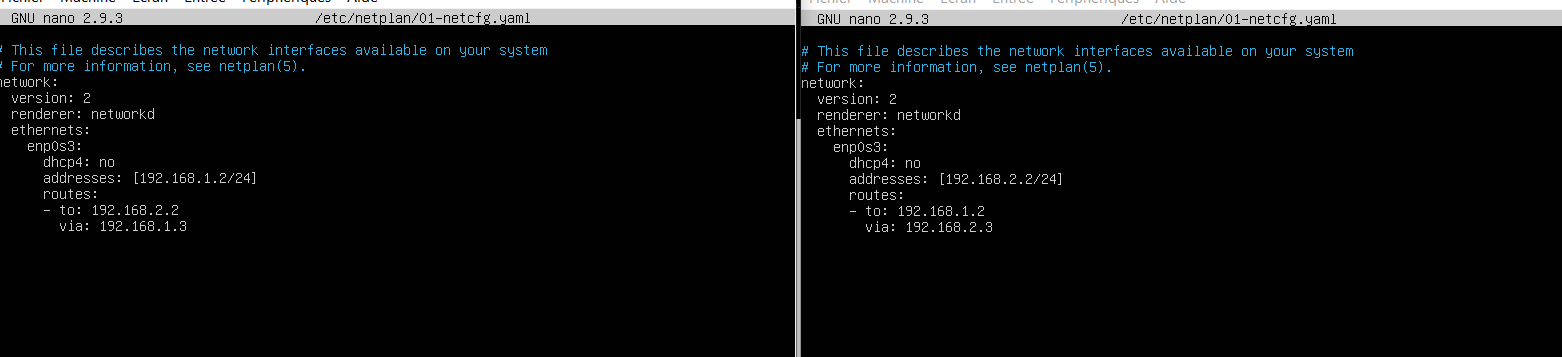


Etape suivante :

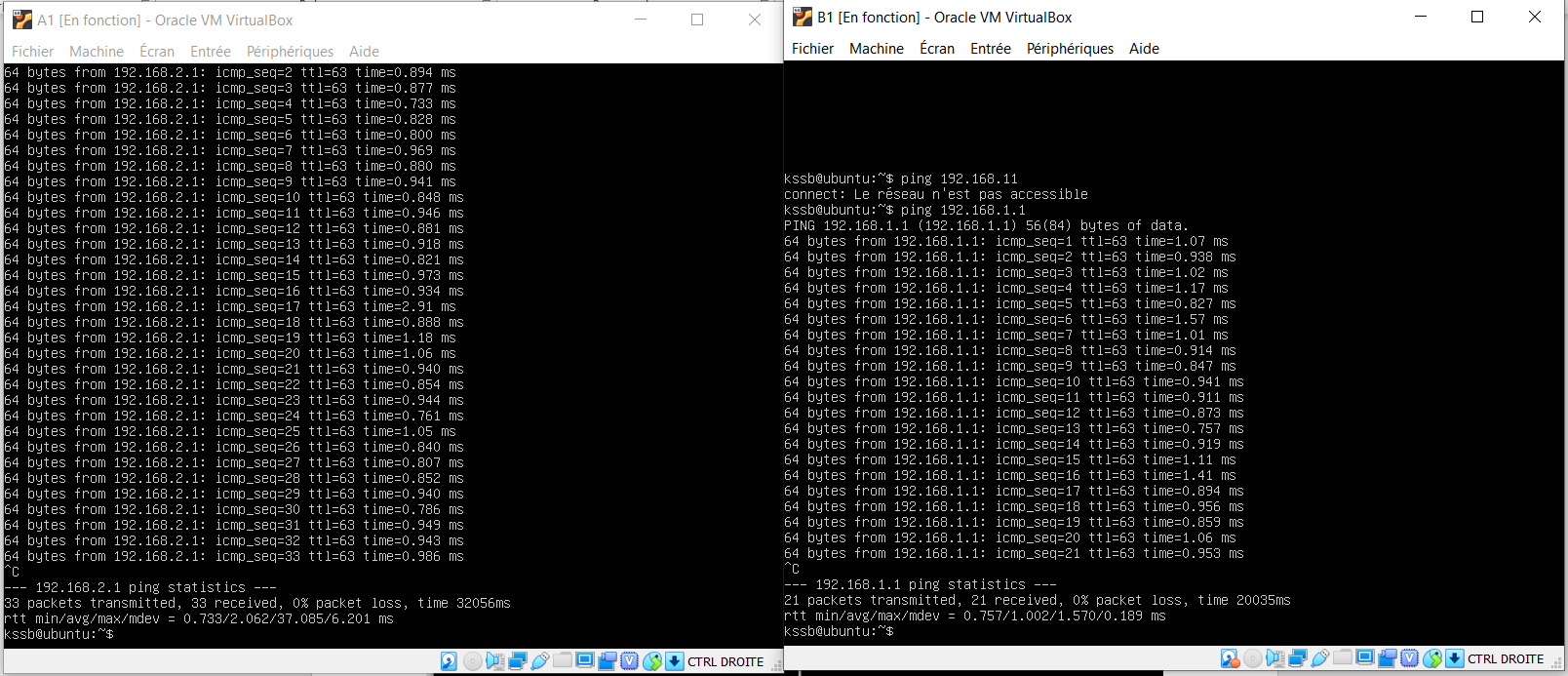
On ajoute les routes de A1 à B1 et vice versa :



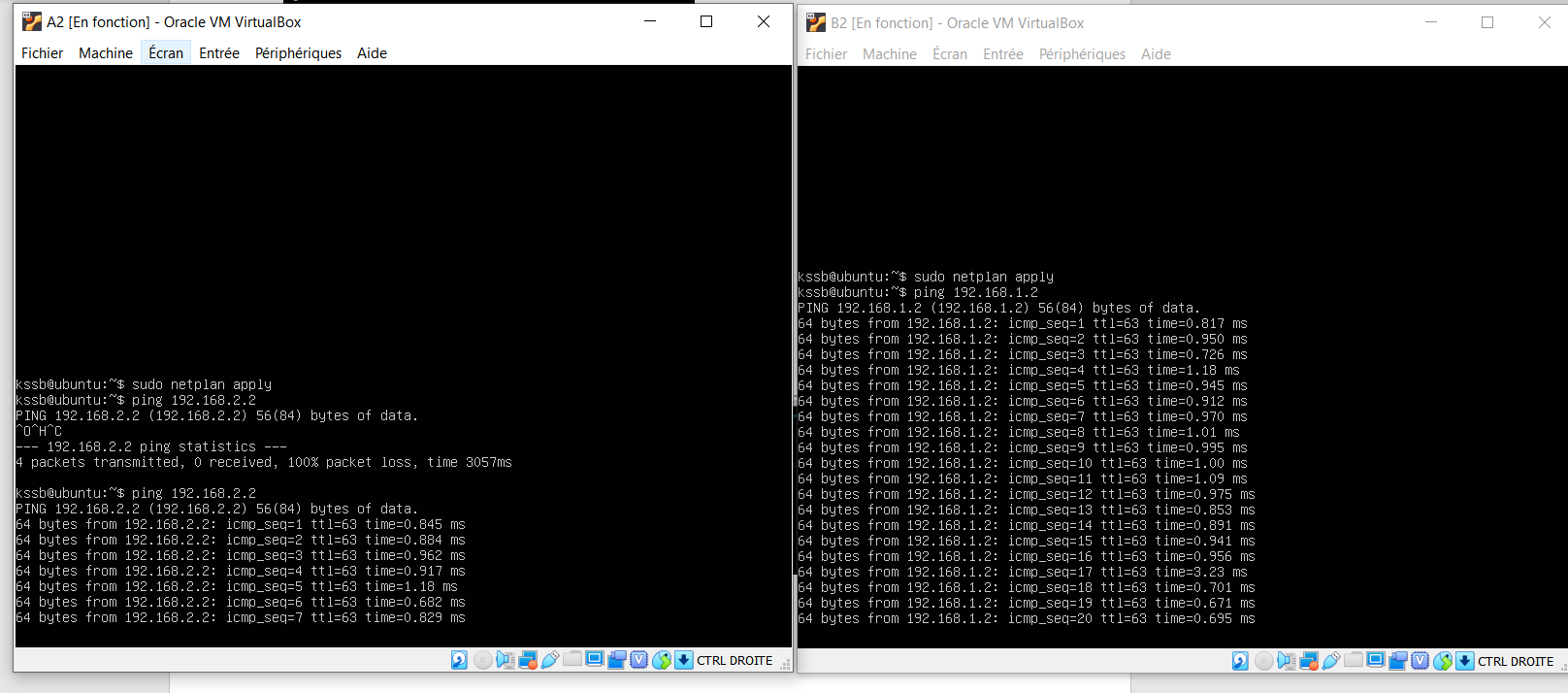
Puis de A2 à B2 :



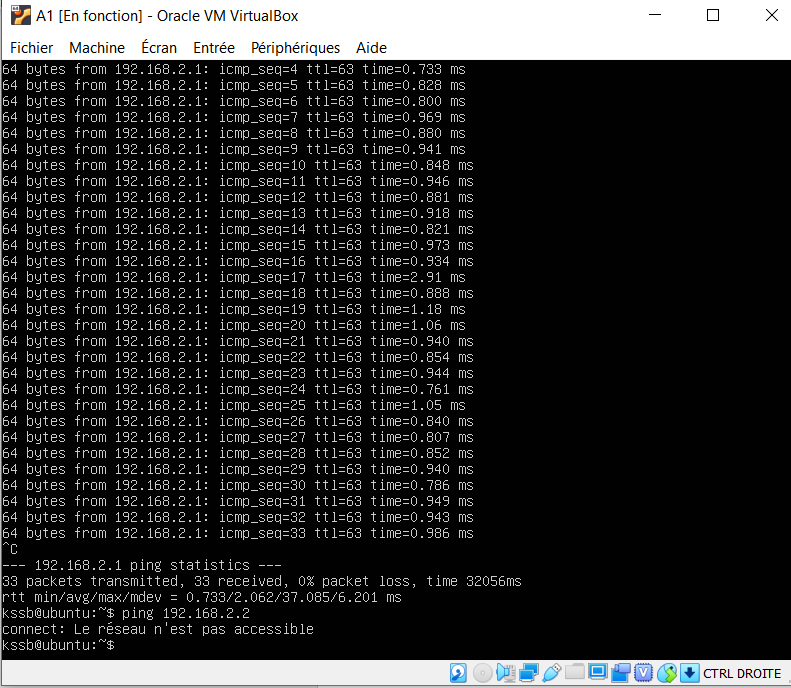
Test de ping entre A1 et B1 :

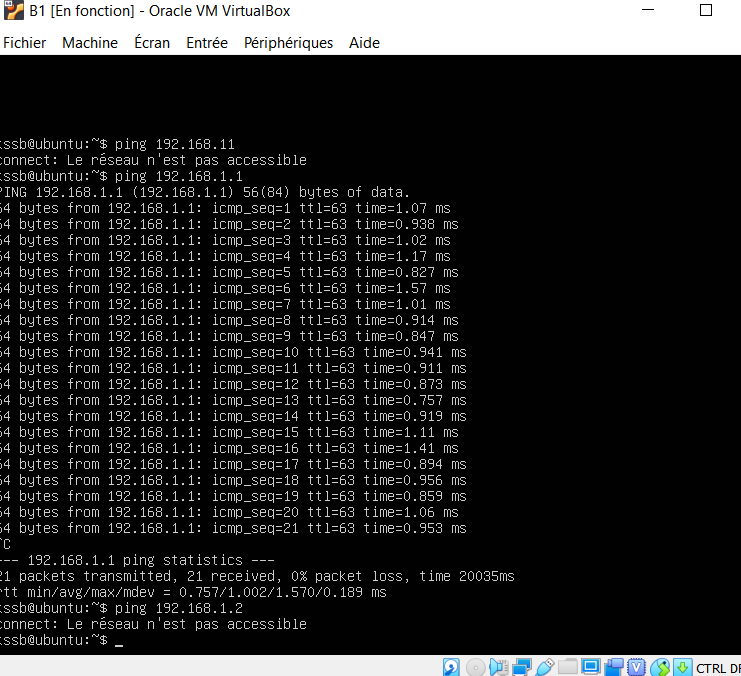


Test de ping entre A2 et B2 :

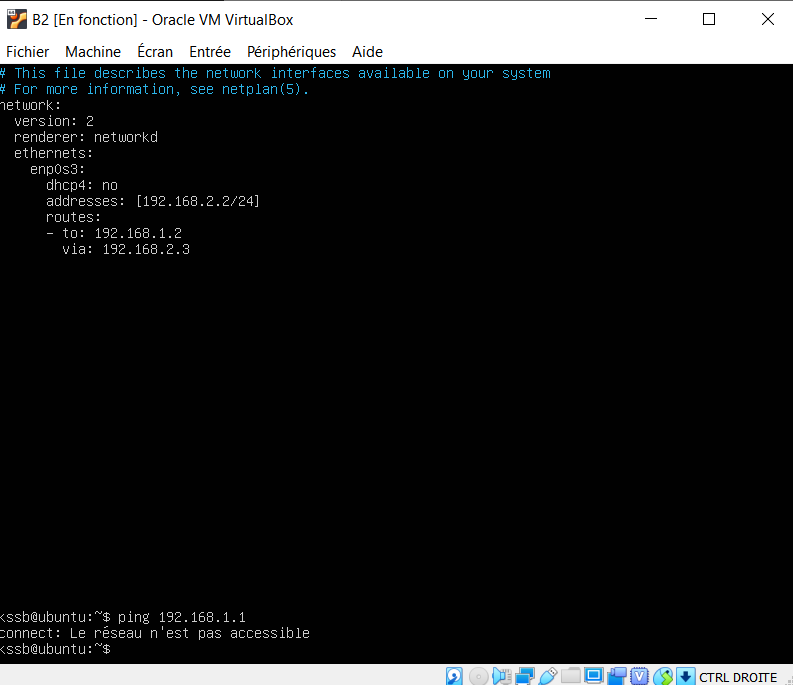


A1 et B2 ainsi que A2 et B1 ne sont pas censées pouvoir se pinger :

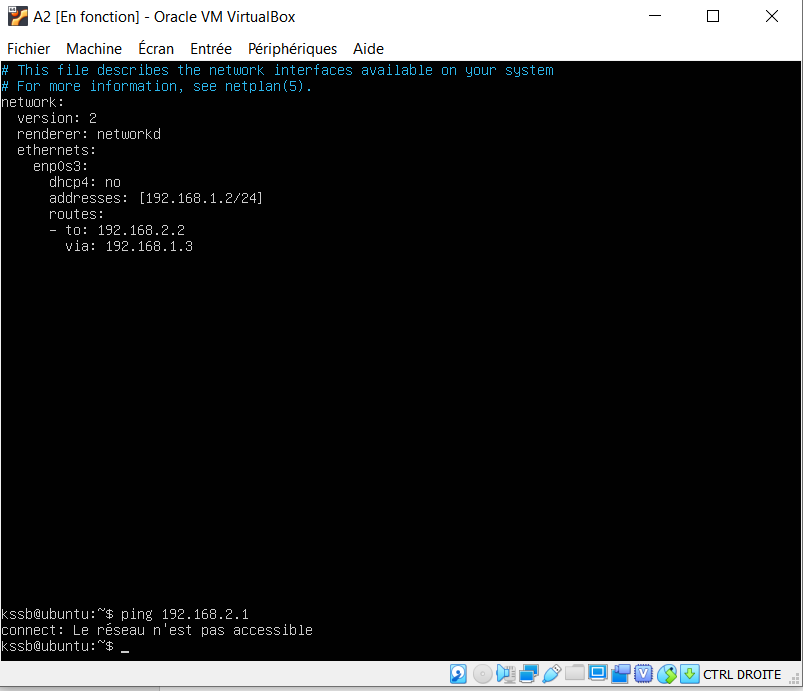
  
Donc on ping B2 à partir de A1 et on voit que le réseau n’est pas accessible ce qui est logique étant donné que nous n’avons pas fourni la route qui permet de les relier



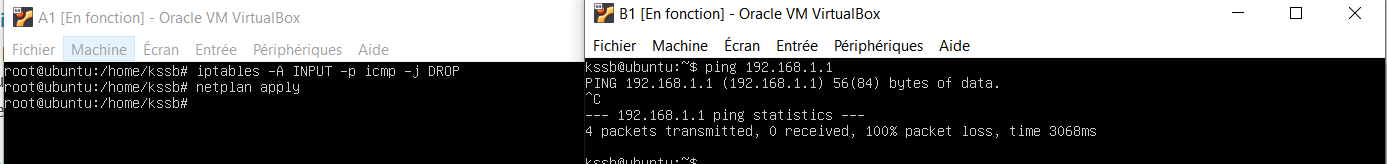
Idem pour B1 envers A2



Idem à partir de B2 vers A1

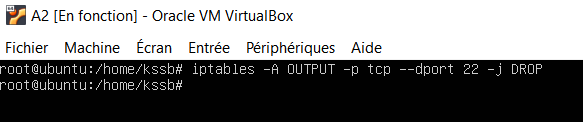


Puis pour finir idem à partir de A2 vers B1

²

Grâce à la ligne de commande :

Iptables -A INPUT -p icmp -j DROP éxecuté à partir de A1, on empêche toutes les autres machines de nous ping (en l’occurrence B1 ici, vu que nous n’avons pas faites des routes entre A1 et B2)



On bloque le port 22 dans A2 avec la commande : iptables -A OUTPUT -p tcp –dport 22 -j DROP

Pour réinitialiser les tables :



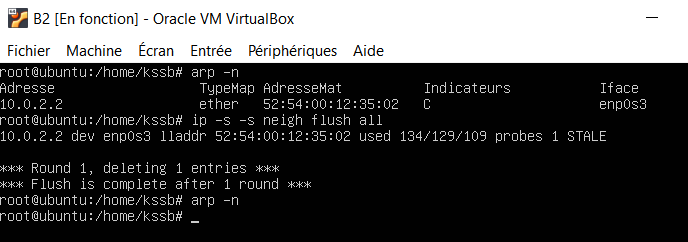
Iptables -F

Mais on peut aussi utiliser :

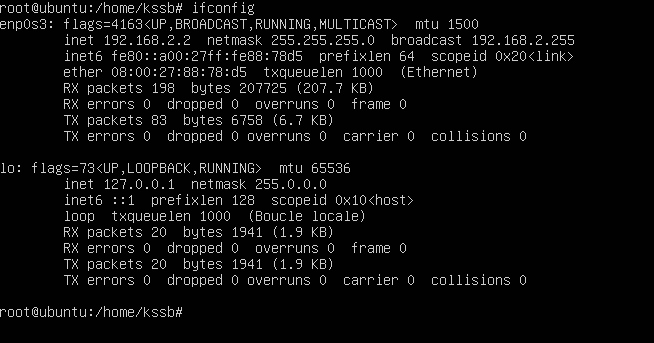
iptables -F INPUT

iptables -F OUTPUT

iptables -F FORWARD

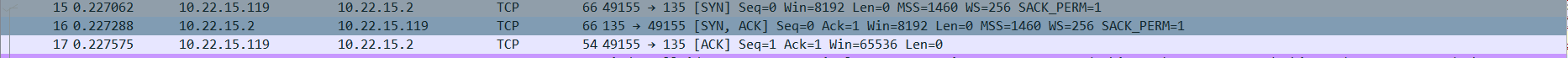


(Screenshot avant et après suppression du cache ARP)

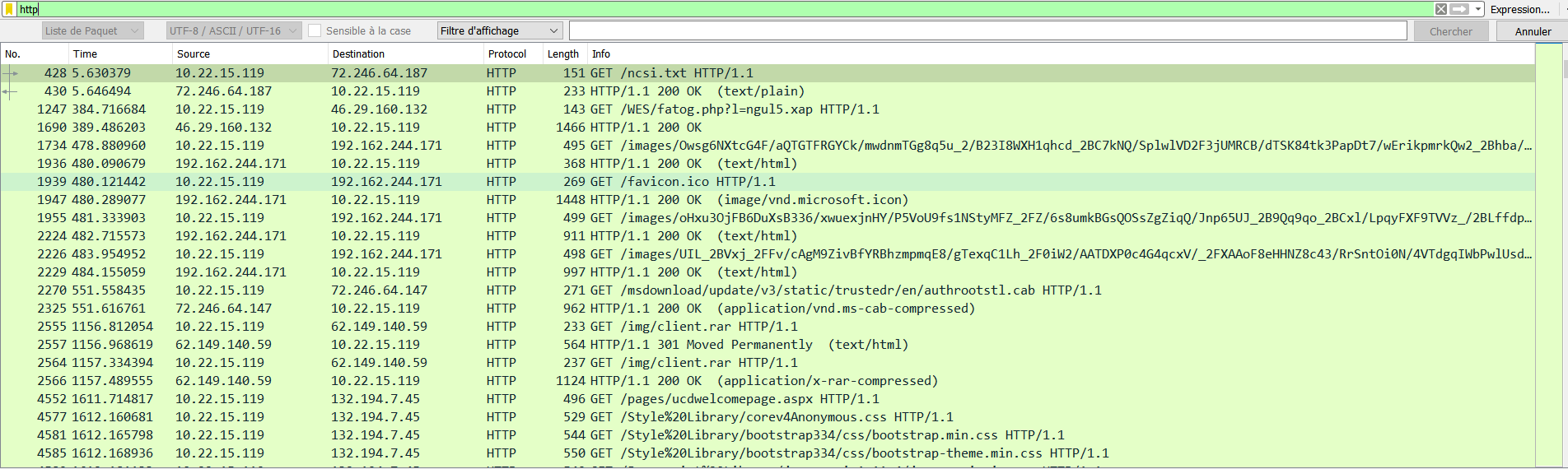


Ifconfig pour lister les adresses physiques présentes sur le réseau

WIRESHARK



La ligne 15-16-17 représente le premier three-way handshake



Deux adresses IP possibles :

72.246.64.187

10.22.15.119

On a un utilisateur qui récupère :

des templates bootstraps (/Style Library/bootstrap334/js/bootstrap.min.js)

des images(/PublishingImages/CriticalPath/CTA/cta\_calendar\_small.jpg)

du Js et du Jquery(/Javascript Library/jquery-ui-1-11-4/jquery-ui.min.js)

On dirait qu’il cherche à créer son propre site en recherchant des images, des themes

Et des fichiers