

Chapitre 1 - Serveur Debian DS1 : routage et translation d'adresses.

Sommaire :

- 1) Rappels
- 2) Configuration réseau du serveur DS1
- 3) Ajout de l'interface enp0s8
- 4) Transformation du serveur en routeur
- 5) Configuration du poste client Ubuntu Desktop 20.04
- 6) Configuration du NAT sur le serveur DS1

1) Rappels.

```
root@DS1 ~#apt-get update
Réception de :1 http://security.debian.org/debian-security bullseye-security InRelease [44,1 kB]
Réception de :2 http://deb.debian.org/debian bullseye InRelease [116 kB]
Réception de :3 http://security.debian.org/debian-security bullseye-security/main Sources [76,5 kB]
Réception de :4 http://deb.debian.org/debian bullseye-updates InRelease [39,4 kB]
Réception de :5 http://deb.debian.org/debian bullseye/main Sources [8 626 kB]
Réception de :6 http://security.debian.org/debian-security/main amd64 Packages [102 kB]
Réception de :7 http://security.debian.org/debian-security/main Translation-en [68,2 kB]
Réception de :8 http://deb.debian.org/debian bullseye/main amd64 Packages [8 183 kB]
Réception de :9 http://deb.debian.org/debian bullseye/main Translation-en [6 243 kB]
23,5 Mo réceptionnés en 5min 10s (75,9 ko/s)
Lecture des listes de paquets... Fait
N: Le dépôt « http://deb.debian.org/debian bullseye InRelease » a modifié sa valeur « Version » de < 11.1 > à < 11.2 >
root@DS1 ~#
```

1^{ère} étape : Cette commande permet de mettre à jour la machine en récupérant les derniers paquets disponibles.

```
root@DS1: ~#_
```

2^{ème} étape : Via le fichier **nano root/.bashrc** et la variable d'environnement PS1, la couleur du prompt est modifié, par ailleurs l'alias **grep** est créé dans ce fichier.

2) Configuration réseau du serveur DS1

```
root@DS1: ~ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:b0:79 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
            valid_lft 85799sec preferred_lft 85799sec
        inet6 fe80::a00:27ff:fed7:b079/64 scope link
            valid_lft forever preferred_lft forever
```

1^{ère} étape : Nous constatons d'abord que le réseau est en mode d'accès **NAT**, nous le modifions par la suite en **Accès par pont**.

```
root@DS1: ~# ifdown enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:d7:b0:79
Sending on   LPF/enp0s3/08:00:27:d7:b0:79
Sending on   Socket/fallback
DHCPRELEASE of 172.17.2.1 on enp0s3 to 172.17.254.1 port 67
```

2^{ème} étape : Nous désactivations la carte réseau afin de lui attribuer par la suite une adresse IP fixe.

```
GNU nano 5.4                               /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
    address 172.17.1.211
    netmask 255.255.0.0
    network 172.17.0.0
    broadcast 172.17.255.255
    gateway 172.17.250.2
    dns-nameservers 172.17.254.1
```

3^{ème} étape : La configuration IP étant en DHCP, celle-ci sera désormais en IP fixe avec réseau SIO du lycée.

```
root@DS1: ~#ifup enp0s3
root@DS1: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:b0:79 brd ff:ff:ff:ff:ff:ff
        inet 172.17.1.211/16 brd 172.17.255.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fed7:b079/64 scope link
            valid_lft forever preferred_lft forever
```

4^{ème} étape : Réactivation de la carte réseau, puis, vérification de la prise en compte de la modification.

```
root@DS1: ~$ cat /etc/resolv.conf
domain prince.local
search prince.local
nameserver 172.17.254.1
nameserver 208.67.222.222
nameserver 208.67.220.220
```

5^{ème} étape : Seconde vérification cette fois-ci en observant le contenu du fichier **resolv.conf**.

```
root@DS1: ~# ip route
default via 172.17.250.2 dev enp0s3 onlink
172.17.0.0/16 dev enp0s3 proto kernel scope link src 172.17.1.211
```

6^{ème} étape : Troisième et dernière vérification, pour la bonne prise en compte de la passerelle par défaut dans la **table de routage**.

```
root@DS1: ~$ ping 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
64 bytes from 172.17.250.2: icmp_seq=1 ttl=255 time=1.01 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=255 time=1.03 ms
64 bytes from 172.17.250.2: icmp_seq=3 ttl=255 time=1.08 ms
64 bytes from 172.17.250.2: icmp_seq=4 ttl=255 time=1.04 ms
^C
--- 172.17.250.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.009/1.037/1.081/0.026 ms
```

```
root@DS1: ~$ ping 172.17.254.1
PING 172.17.254.1 (172.17.254.1) 56(84) bytes of data.
64 bytes from 172.17.254.1: icmp_seq=1 ttl=128 time=1.26 ms
64 bytes from 172.17.254.1: icmp_seq=2 ttl=128 time=0.789 ms
64 bytes from 172.17.254.1: icmp_seq=3 ttl=128 time=0.832 ms
64 bytes from 172.17.254.1: icmp_seq=4 ttl=128 time=0.823 ms
^C
--- 172.17.254.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.789/0.926/1.262/0.194 ms
```

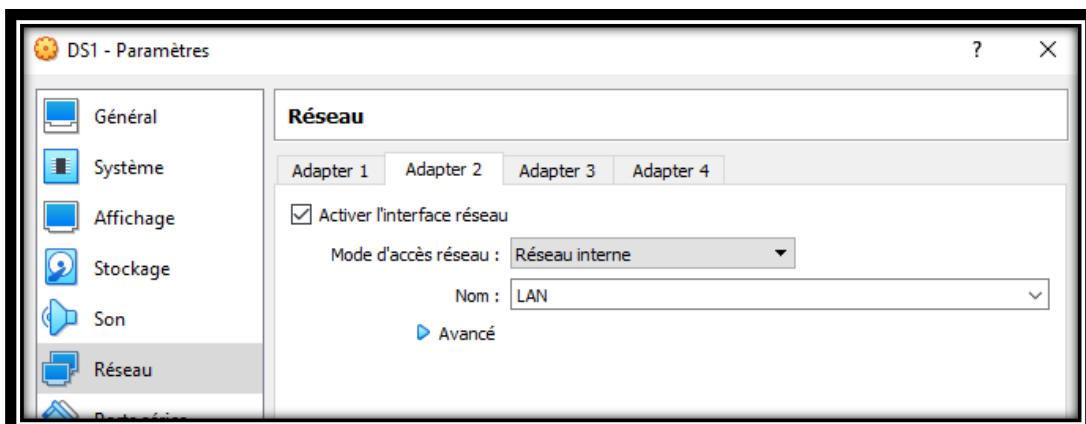
7^{ème} étape : Afin de vérifier la bonne connectivité IP nous effectuons un ping de la passerelle en **172.17.250.2** ainsi que le serveur **DNS en 172.17.254.1**.

```
root@DS1: ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=25.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=25.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 25.593/25.712/25.883/0.122 ms
```

```
root@DS1: ~$ ping www.ac-nice.fr
PING cs234.wpc.alphacd.net (93.184.221.161) 56(84) bytes of data.
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=1 ttl=57 time=26.1 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=57 time=25.9 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=57 time=25.6 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=57 time=25.5 ms
^C
--- cs234.wpc.alphacd.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 25.488/25.781/26.104/0.249 ms
```

8^{ème} étape : Via les pings 4x8 ainsi que le domaine ac-nice.fr nous vérifions l'accès à internet et la résolution DNS.

3) Ajout de l'interface enp0s8



1^{ère} étape : Après avoir arrêté la machine, nous ajoutons une seconde carte réseau configurer en mode d'accès réseau : Réseau interne (LAN).

```
root@DS1: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:b0:79 brd ff:ff:ff:ff:ff:ff
        inet 172.17.1.211/16 brd 172.17.255.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fed7:b079/64 scope link
            valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:6f:5c:7b brd ff:ff:ff:ff:ff:ff
```

2^{ème} étape : Nous vérifions la prise en compte de la nouvelle **carte réseau enp0s8**.

```
GNU nano 5.4                               /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 172.17.1.211
netmask 255.255.0.0
network 172.17.0.0
broadcast 172.17.255.255
gateway 172.17.250.2
dns-nameservers 172.17.254.1

allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.4.254
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255
```

3^{ème} étape : Nous modifions de nouveau le fichier, cette fois-ci pour configurer une IP fixe à la carte enp0s8.

```
root@DS1: ~#ifup enp0s8
root@DS1: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:b0:79 brd ff:ff:ff:ff:ff:ff
        inet 172.17.1.211/16 brd 172.17.255.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fed7:b079/64 scope link
            valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6f:5c:7b brd ff:ff:ff:ff:ff:ff
        inet 192.168.4.254/24 brd 192.168.4.255 scope global enp0s8
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe6f:5c7b/64 scope link
            valid_lft forever preferred_lft forever
```

4^{ème} étape : Nous activons la carte enp0s8 puis vérifions la prise en compte de la configuration effectuer à l'avance.

```
root@DS1: ~#ping 192.168.4.254
PING 192.168.4.254 (192.168.4.254) 56(84) bytes of data.
64 bytes from 192.168.4.254: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.022 ms
^C
--- 192.168.4.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.018/0.020/0.022/0.001 ms
```

```
root@DS1: ~#ping 172.17.1.211
PING 172.17.1.211 (172.17.1.211) 56(84) bytes of data.
64 bytes from 172.17.1.211: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 172.17.1.211: icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from 172.17.1.211: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 172.17.1.211: icmp_seq=4 ttl=64 time=0.020 ms
^C
--- 172.17.1.211 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.015/0.019/0.021/0.002 ms
```

5^{ème} étape : Afin de vérifier la bonne configuration de la machine DS1 nous effectuons un ping sur ses deux interfaces.

```
root@DS1: ~#ip route
default via 172.17.250.2 dev enp0s3 onlink
172.17.0.0/16 dev enp0s3 proto kernel scope link src 172.17.1.211
192.168.4.0/24 dev enp0s8 proto kernel scope link src 192.168.4.254
```

6^{ème} étape : Dernière commande permettant d'afficher la table de routage.

4) Transformation du serveur en routeur

```
root@DS1: ~#echo 1 > /proc/sys/net/ipv4/ip_forward
root@DS1: ~#
```

```
root@DS1: ~#cat /proc/sys/net/ipv4/ip_forward
1
```

1^{ère} étape : Nous activons le routage, positionnant par la suite un drapeau pour le processus **ip_forward**, nous constatons la valeur **1** dans le fichier **ip_forward** alors que celui-ci est **par défaut à 0**.

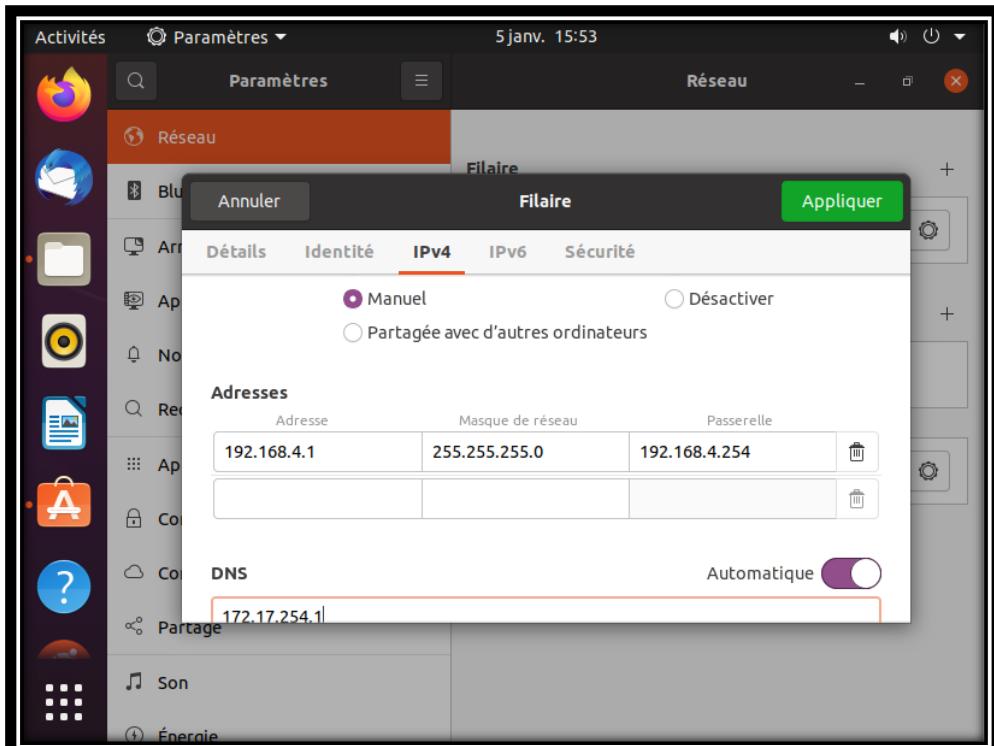
```
GNU nano 5.4                               /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
#
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
#
root@DS1: ~#reboot_
```

2^{ème} étape : Afin que le routage soit mis en place après chaque démarrage de la machine, nous enlevons le # de commentaire à la ligne **net.ipv4.ip_forward=1** dans le fichier ici présent. Puis nous redémarrons la machine avec la **commande reboot**.

```
rroot@DS1: ~#cat /proc/sys/net/ipv4/ip_forward
1
```

3^{ème} étape : Nous vérifions par la suite que le routage soit bien mis en place.

5) Configuration du poste client Ubuntu Desktop 20.04.



```
sio@UD1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9c:f9:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.1/24 brd 192.168.4.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::3fac:1089:27cd:9233/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

1^{ère} étape : Nous téléchargeons l'**iso ubuntu-20.04.1-desktop-amd64** et créons la **VM UD1**. Nous sélectionnons par la suite le **mode d'accès Réseau Interne (LAN)** et établissons la **configuration IP de UD1** via l'interface Network Manager afin d'attribuer une IP fixe à la carte réseau de cette machine. Nous vérifions ensuite la prise en compte de cette manipulation.

```
sio@UD1:~$ ip route
default via 192.168.4.254 dev enp0s3 proto static metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.4.0/24 dev enp0s3 proto kernel scope link src 192.168.4.1 metric 100
```

2^{ème} étape : En consultant la table de routage nous observons la **route par défaut** ainsi que la **passerelle**.

```
sio@UD1:~$ ping -c 3 192.168.4.254
PING 192.168.4.254 (192.168.4.254) 56(84) bytes of data.
64 octets de 192.168.4.254 : icmp_seq=1 ttl=64 temps=0.430 ms
64 octets de 192.168.4.254 : icmp_seq=2 ttl=64 temps=0.408 ms
64 octets de 192.168.4.254 : icmp_seq=3 ttl=64 temps=0.387 ms

--- statistiques ping 192.168.4.254 ---
3 paquets transmis, 3 reçus, 0 % paquets perdus, temps 2027 ms
rtt min/avg/max/mdev = 0.387/0.408/0.430/0.017 ms
```

```
sio@UD1:~$ ping -c 3 172.17.1.211
PING 172.17.1.211 (172.17.1.211) 56(84) bytes of data.
64 octets de 172.17.1.211 : icmp_seq=1 ttl=64 temps=0.394 ms
64 octets de 172.17.1.211 : icmp_seq=2 ttl=64 temps=0.412 ms
64 octets de 172.17.1.211 : icmp_seq=3 ttl=64 temps=0.416 ms

--- statistiques ping 172.17.1.211 ---
3 paquets transmis, 3 reçus, 0 % paquets perdus, temps 2027 ms
rtt min/avg/max/mdev = 0.394/0.407/0.416/0.009 ms
```

3^{ème} étape : Nous effectuons un **ping** des deux interfaces du serveur DS1 depuis la machine **Ubuntu** afin de vérifier la connectivité entre les deux machines et le bon fonctionnement du routage.

```
sio@UD1:~$ ping -c1 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.

--- statistiques ping 172.17.250.2 ---
1 paquets transmis, 0 reçus, 100 % paquets perdus, temps 0 ms
```

4^{ème} étape : Nous vérifions l'accès à Internet en pinguant maintenant l'interface du routeur permettant de quitter le réseau local en **172.17.250.2**, nous constatons que celui-ci ne fonctionne pas, nous obtenons aucune réponse.

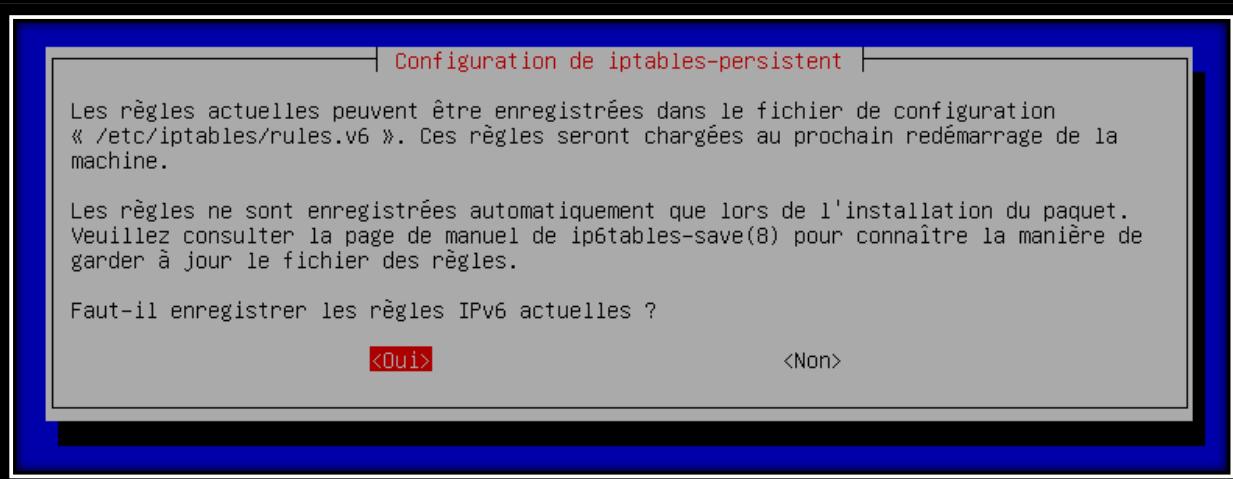
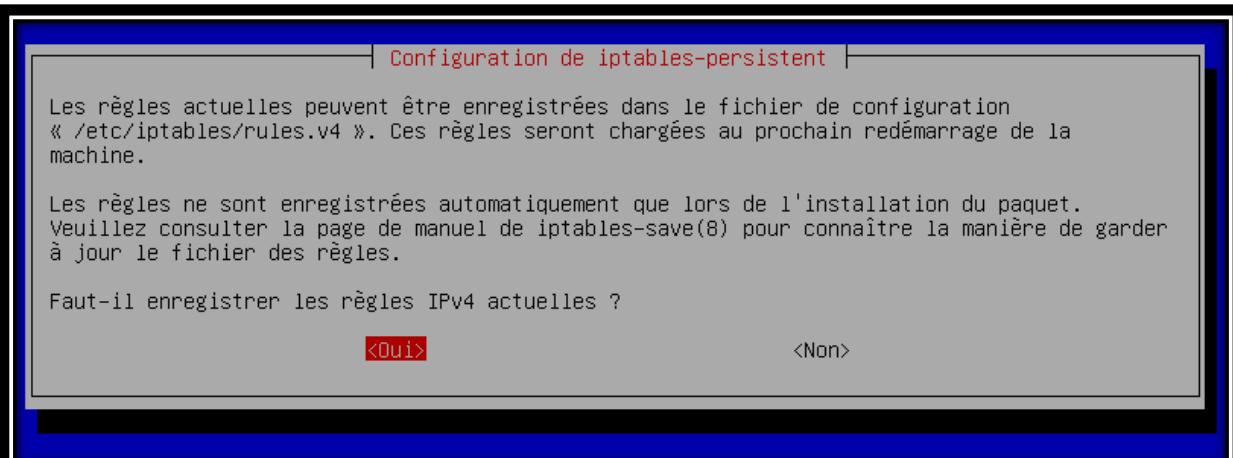
6) Configuration du NAT sur le serveur DS1

```
root@DS1: ~#iptables -t nat -A POSTROUTING -o enp0s3 -s 192.168.4.0/24 -j MASQUERADE
root@DS1: ~#
```

1^{ère} étape : Nous mettons en place **l'IP Masquerading**.

```
root@DS1: ~#iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
46   2812 MASQUERADE  all    --    any      enp0s3  192.168.4.0/24      anywhere
```

2^{ème} étape : Nous vérifions la bonne prise en compte de la règle par **iptables -t nat -L -v**.



3^{ème} étape : Afin que la translation d'adresses **NAT** soit activée à chaque démarrage, nous installons le **paquet iptables-persistent**. Pendant, l'installation du paquet, on nous demande si l'on souhaite que les règles actuellement en cours d'utilisation soient enregistrées dans les fichiers de configuration **/etc/iptables/rules.v4** et **/etc/iptables/rules.v6**. Nous répondons donc oui.

```
root@DS1: ~#iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all  --  192.168.4.0/24      anywhere
```

4^{ème} étape : Nous redémarrons le système avec la commande **reboot** et vérifions à nouveau l'existence de la règle **NAT**.

```
sio@UD1:~$ ping 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
64 octets de 172.17.250.2 : icmp_seq=1 ttl=254 temps=1.22 ms
64 octets de 172.17.250.2 : icmp_seq=2 ttl=254 temps=1.70 ms
64 octets de 172.17.250.2 : icmp_seq=3 ttl=254 temps=1.44 ms
64 octets de 172.17.250.2 : icmp_seq=4 ttl=254 temps=1.36 ms
^C
--- statistiques ping 172.17.250.2 ---
4 paquets transmis, 4 reçus, 0 % paquets perdus, temps 3005 ms
rtt min/avg/max/mdev = 1.224/1.431/1.698/0.172 ms
```

5^{ème} étape : Nous vérifions le bon fonctionnement du routage et de la translation d'adresse **NAT** à partir du client Ubuntu en pinguant une nouvelle fois la passerelle en **172.17.250.2**. Nous constatons que cette fois-ci le ping fonctionne contrairement à celui effectué auparavant.

```
root@DS1: ~#apt-get install tcpdump
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libpcap0.8
Les NOUVEAUX paquets suivants seront installés :
  libpcap0.8 tcpdump
0 mis à jour, 2 nouvellement installés, 0 à enlever et 17 non mis à jour.
Il est nécessaire de prendre 625 ko dans les archives.
Après cette opération, 1 744 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 libpcap0.8 amd64 1.10.0-2 [159 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 tcpdump amd64 4.99.0-2 [466 kB]
625 ko réceptionnés en 25s (24,7 ko/s)
Sélection du paquet libpcap0.8:amd64 précédemment désélectionné.
(Lecture de la base de données... 60319 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libpcap0.8_1.10.0-2_amd64.deb ...
Dépaquetage de libpcap0.8:amd64 (1.10.0-2) ...
Sélection du paquet tcpdump précédemment désélectionné.
Préparation du dépaquetage de .../tcpdump_4.99.0-2_amd64.deb ...
Dépaquetage de tcpdump (4.99.0-2) ...
Paramétrage de libpcap0.8:amd64 (1.10.0-2) ...
Paramétrage de tcpdump (4.99.0-2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u2) ...
```

6ème étape : Nous installons sur **DS1** le **paquet tcpdump**.

```
root@DS1: ~#tcpdump -i enp0s3 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:48:31.239936 IP 172.17.1.211 > 172.17.250.2: ICMP echo request, id 7, seq 1, length 64
16:48:31.240736 IP 172.17.250.2 > 172.17.1.211: ICMP echo reply, id 7, seq 1, length 64
16:48:32.242249 IP 172.17.1.211 > 172.17.250.2: ICMP echo request, id 7, seq 2, length 64
16:48:32.243270 IP 172.17.250.2 > 172.17.1.211: ICMP echo reply, id 7, seq 2, length 64
16:48:33.244153 IP 172.17.1.211 > 172.17.250.2: ICMP echo request, id 7, seq 3, length 64
16:48:33.245159 IP 172.17.250.2 > 172.17.1.211: ICMP echo reply, id 7, seq 3, length 64
16:48:34.246400 IP 172.17.1.211 > 172.17.250.2: ICMP echo request, id 7, seq 4, length 64
16:48:34.247245 IP 172.17.250.2 > 172.17.1.211: ICMP echo reply, id 7, seq 4, length 64
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
root@DS1: ~#
```

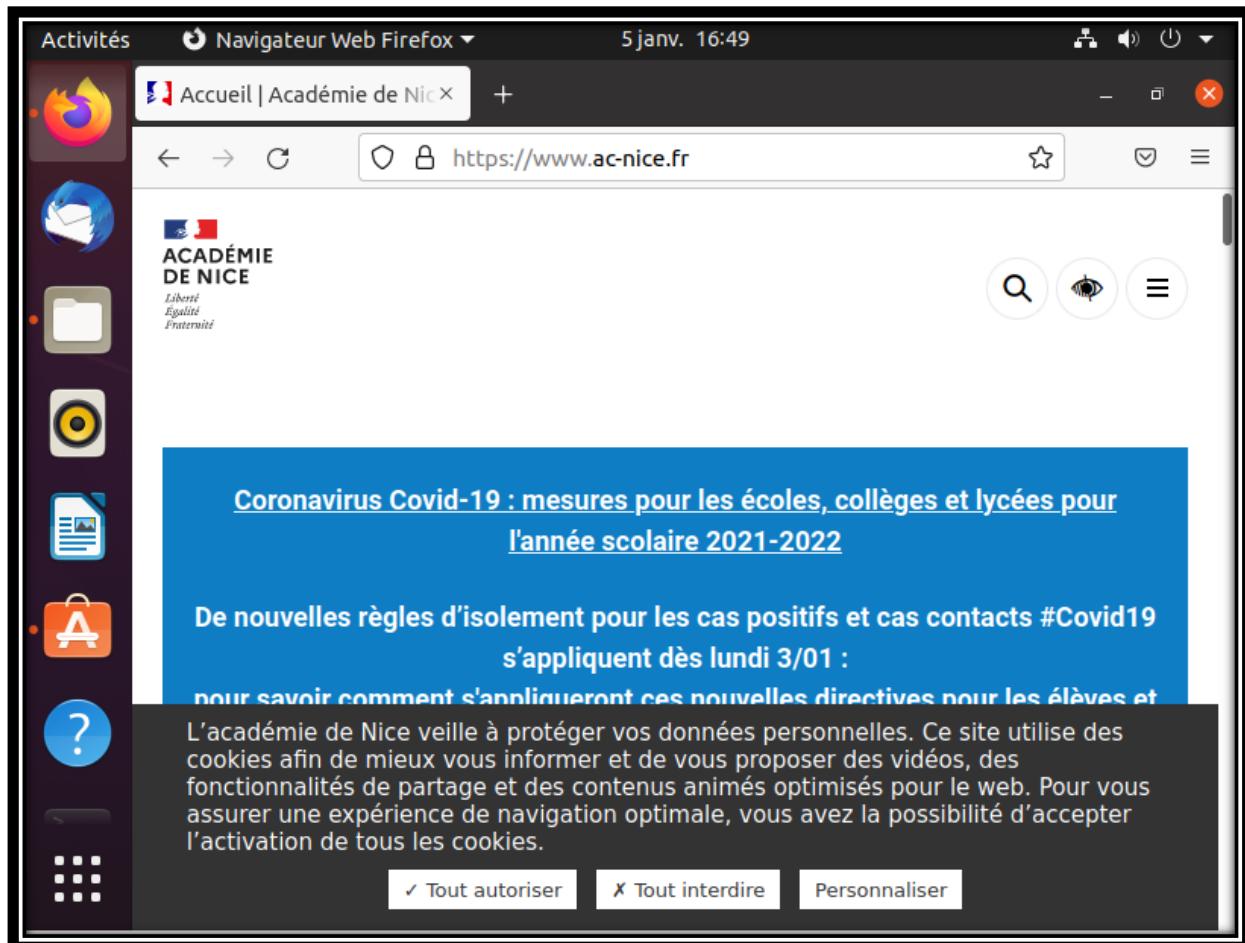
7ème étape : Nous effectuons une capture **des trames ICMP** sur chaque interface du routeur (NAT DS1), puis constatons la translation sur **enp0s3**. Dans la trame **ICMP Echo request**, l'adresse IP de **UD1 192.168.4.1** a été remplacée par celle de l'interface côté extérieur de **DS1 en 172.17.1.211**.

```
root@DS1: ~#tcpdump -i enp0s8 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:53:22.369402 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8, seq 1, length 64
16:53:22.370509 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8, seq 1, length 64
16:53:23.371974 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8, seq 2, length 64
16:53:23.372831 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8, seq 2, length 64
16:53:24.374236 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8, seq 3, length 64
16:53:24.375132 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8, seq 3, length 64
16:53:25.375747 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8, seq 4, length 64
16:53:25.376731 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8, seq 4, length 64
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

8ème étape : Cette fois-ci sur **enp0s8**, l'IP source de la trame **ICMP Echo request** est encore celle de **UD1**, puisque la translation a été mise en place dans la chaîne **POSTROUTING**.

```
sio@UD1:~$ ping www.ac-nice.fr
PING cs234.wpc.alphacd.net (93.184.221.161) 56(84) bytes of data.
64 octets de 93.184.221.161 (93.184.221.161) : icmp_seq=1 ttl=56 temps=126 ms
64 octets de 93.184.221.161 (93.184.221.161) : icmp_seq=2 ttl=56 temps=127 ms
64 octets de 93.184.221.161 (93.184.221.161) : icmp_seq=3 ttl=56 temps=122 ms
64 octets de 93.184.221.161 (93.184.221.161) : icmp_seq=4 ttl=56 temps=25.8 ms
^C
--- statistiques ping cs234.wpc.alphacd.net ---
4 paquets transmis, 4 reçus, 0 % paquets perdus, temps 3005 ms
rtt min/avg/max/mdev = 25.798/100.164/126.859/42.971 ms
```

9ème étape : Nous vérifions le bon fonctionnement de la translation et de la résolution **DNS** avec la commande **ping www.ac-nice.fr** depuis le client **UD1**.



10^{ème} étape : Nous lançons le navigateur et vérifions la possibilité d'aller sur internet, effectivement cela fonctionne.