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

Sommaire :

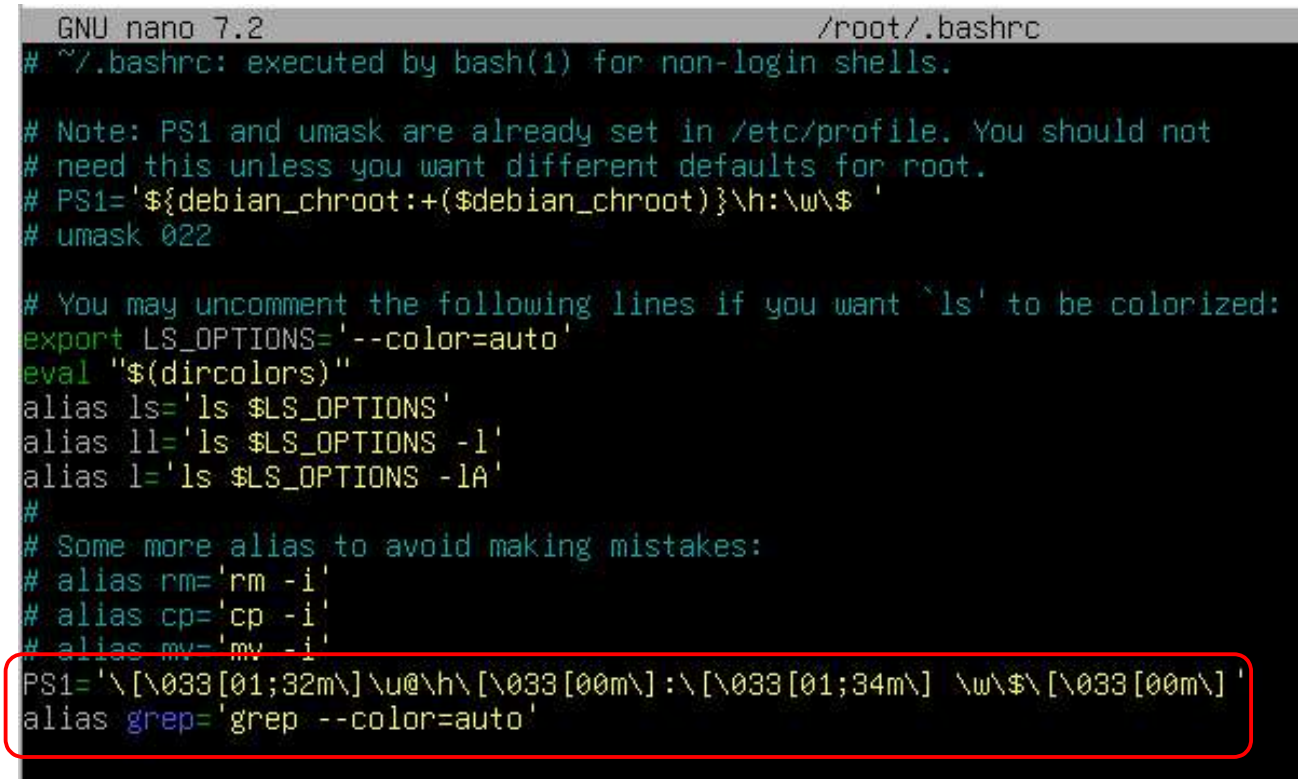
1. Rappels.

- Récupérez la dernière liste des paquets disponibles :

Pour ça, on utilise la commande **« apt-get update »**

```
root@DEB12Server: ~#apt-get update
Réception de :1 http://deb.debian.org/debian bookworm InRelease [151 kB]
Réception de :2 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [52,1 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main Sources [72,9 kB]
Réception de :5 http://deb.debian.org/debian bookworm/main Sources [9 488 kB]
Réception de :6 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [13
4 kB]
Réception de :7 http://security.debian.org/debian-security bookworm-security/main Translation-en [80
,0 kB]
Réception de :8 http://deb.debian.org/debian bookworm-updates/main Sources.diff/Index [9 483 B]
Ign :8 http://deb.debian.org/debian bookworm-updates/main Sources.diff/Index
Réception de :9 http://deb.debian.org/debian bookworm-updates/main amd64 Packages.diff/Index [9 483
B]
Réception de :10 http://deb.debian.org/debian bookworm-updates/main Translation-en.diff/Index [9 483
 B]
Réception de :11 http://deb.debian.org/debian bookworm-updates/main amd64 Packages T-2023-12-29-1403
.39-F-2023-12-15-1408.04.pdiff [7 381 B]
Réception de :11 http://deb.debian.org/debian bookworm-updates/main amd64 Packages T-2023-12-29-1403
.39-F-2023-12-15-1408.04.pdiff [7 381 B]
Réception de :12 http://deb.debian.org/debian bookworm-updates/main Translation-en T-2023-12-29-1403
.39-F-2023-12-15-1408.04.pdiff [10,2 kB]
Réception de :12 http://deb.debian.org/debian bookworm-updates/main Translation-en T-2023-12-29-1403
.39-F-2023-12-15-1408.04.pdiff [10,2 kB]
Réception de :13 http://deb.debian.org/debian bookworm/non-free-firmware Sources [6 168 B]
Réception de :14 http://deb.debian.org/debian bookworm/main amd64 Packages [8 787 kB]
Réception de :15 http://deb.debian.org/debian bookworm/main Translation-en [6 109 kB]
Réception de :16 http://deb.debian.org/debian bookworm/non-free-firmware amd64 Packages [6 208 B]
Réception de :17 http://deb.debian.org/debian bookworm-updates/main Sources [17,4 kB]
25,0 Mo réceptionnés en 18s (1 398 ko/s)
Lecture des listes de paquets... Fait
N: Le dépôt « http://deb.debian.org/debian bookworm InRelease » a modifié sa valeur « Version » de «
 12.2 » à « 12.4 »
root@DEB12Server: ~#
```

- Si ce n'est déjà fait, mettez le prompt en couleur à l'aide du fichier **« nano /root/.bashrc »** et de la variable d'environnement PS1. Activez ou créez également l'alias grep :



- Déconnectez-vous (exit ou logout) puis reconnectez-vous.
- Veillez à bien renommer votre serveur Debian (sans environnement de bureau) en DS1. Modifiez pour cela les fichiers **« /etc/hostname »** et **« /etc/hosts »**. Redémarrez votre machine à l'aide de la commande **« reboot »**.

Premièrement, on commence par le fichier **« /etc/hostname »** à l'aide de **nano :**

A la place initialement de DEB12Serveur on le remplace par son nouveau nom qui est DS1 :

Puis, par le fichier **« /etc/hosts »**

On remplace aussi DEB12Serveur par DS1 :

```
  GNU nano 7.2                                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       DS1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Puis on redémarre la machine à l'aide de la commande « reboot »

2. Configuration réseau du serveur DS1.

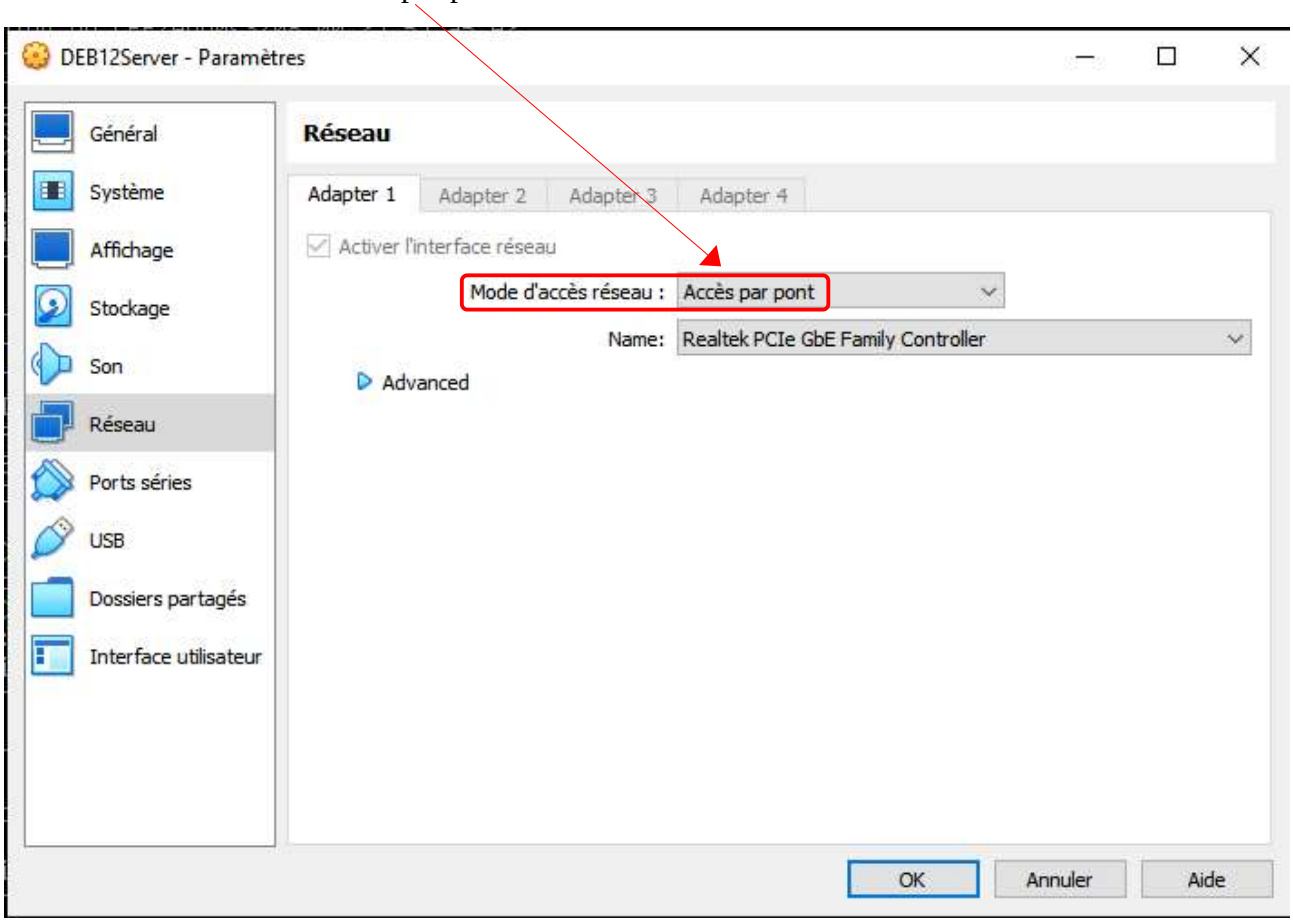
On constate que le changement du nom du serveur a été effectué :

```
Debian GNU/Linux 12 DS1 tty1

DS1 login: root
Password:
Linux DS1 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 19 12:24:53 CET 2024 on tty1
root@DS1: ~#_
```

▪ Configuration réseau actuelle (mode d'accès réseau NAT).

```
root@DS1: ~#ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:57:a5:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86360sec preferred_lft 86360sec
    inet6 fe80::a00:27ff:fe57:a5e2/64 scope link
       valid_lft forever preferred_lft forever
root@DS1: ~#_
```

▪ Mode d’accès réseau : Accès par pont.



▪ Désactivez la carte réseau enp0s3 avant de spécifier une adresse IP fixe :

```
root@DS1: ~#ifdown enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhc

Listening on LPF/enp0s3/08:00:27:57:a5:e2
Sending on   LPF/enp0s3/08:00:27:57:a5:e2
Sending on   Socket/fallback
DHCPRELEASE of 10.0.2.15 on enp0s3 to 10.0.2.2 port 67
root@DS1: ~#
```

La commande **« ifdown »** permet de désactiver la carte réseau.

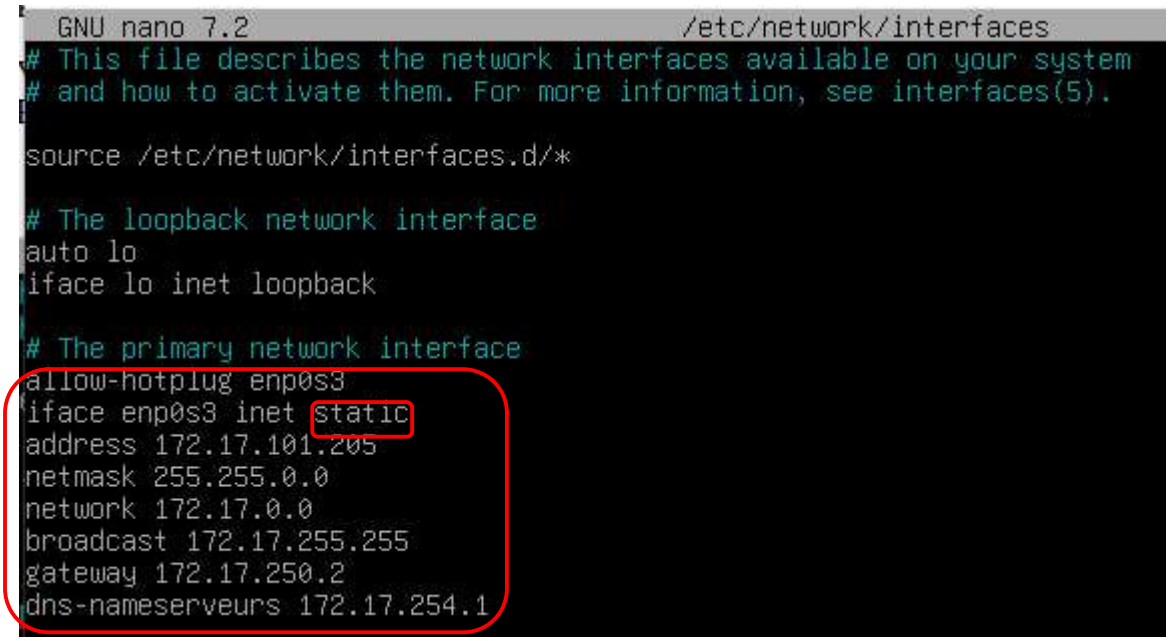
```
root@DS1: ~#ifdown enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:57:a5:e2
Sending on   LPF/enp0s3/08:00:27:57:a5:e2
Sending on   Socket/fallback
DHCPRELEASE of 172.17.177.16 on enp0s3 to 172.17.244.1 port 67
root@DS1: ~#
```

▪ Modifiez, avec l'éditeur de texte Nano, le fichier **« /etc/network/interfaces »** pour l'interface **enp0s3**. Configuration IP actuelle en DHCP à passer en IP fixe :

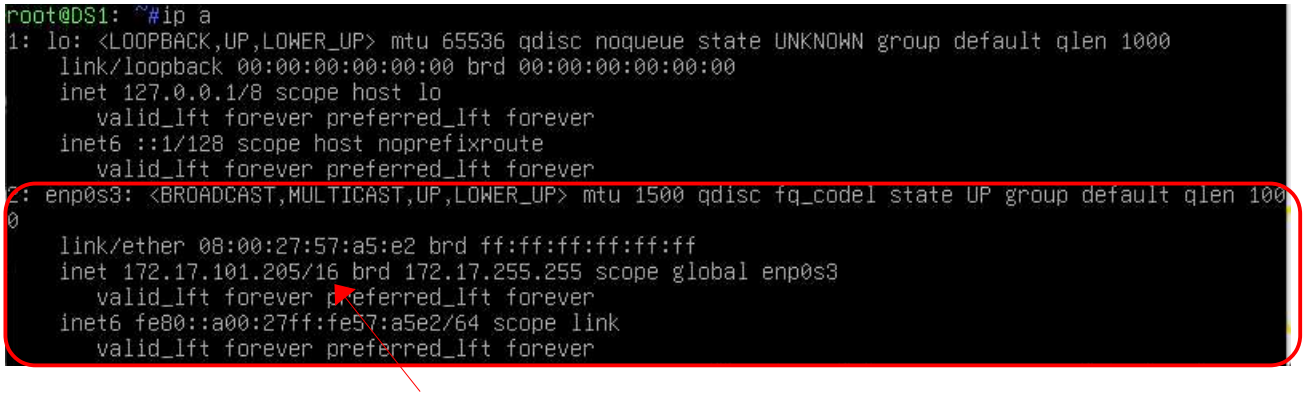
Ici, on se trouve dans l'éditeur de texte nano afin de pouvoir éditer le fichier **« /etc/network/interfaces »** pour faire la Configuration IP :

L'adresse IP fixe cohérente avec le réseau SIO 172.17.1.205 /16 (l'adresse réseau : 172.17.0.0/16). Le Gateway : 172.17.250.2 (Routeur ou box (si on le fait chez soi) ;

DNS : 172.17.254.1 (serveur ROI)



▪ Réactivez la carte réseau (ifup enp0s3) et vérifiez la configuration IP (ip a).



On peut observer que les modification ont bien été effectuer

▪ Affichez le contenu du fichier **« /etc/resolv.conf »** à l'aide de la commande **« cat »**. Vérifiez la présence de l'adresse IP du serveur DNS.

```
root@DS1: ~#cat /etc/resolv.conf
domain prince.local
search prince.local
nameserver 172.17.254.1
nameserver 172.17.244.1
nameserver 80.10.246.2
nameserver 8.8.8.8
root@DS1: ~#
```

▪ Consultez la table de routage de DS1 (visualisez la prise en compte de la passerelle par défaut) :

```
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 172.17.1.205
root@DS1: ~#_
```

Gateway = Passerelle donc c'est **172.17.250.2**

▪ Pinguez la passerelle (172.17.250.2) ainsi que le serveur DNS (172.17.254.1) pour vous assurer de la bonne connectivité IP :

Premièrement, on **ping la passerelle** :

```
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=0.658 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=255 time=0.449 ms
64 bytes from 172.17.250.2: icmp_seq=3 ttl=255 time=0.439 ms
64 bytes from 172.17.250.2: icmp_seq=4 ttl=255 time=0.448 ms
64 bytes from 172.17.250.2: icmp_seq=5 ttl=255 time=0.431 ms
64 bytes from 172.17.250.2: icmp_seq=6 ttl=255 time=0.423 ms
^C
--- 172.17.250.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5143ms
rtt min/avg/max/mdev = 0.423/0.474/0.658/0.082 ms
root@DS1: ~#_
```

On voit que le PC **arrive a communiquer** avec la passerelle

Pour finir, on **ping le serveur DNS** :

```
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=0.557 ms
64 bytes from 172.17.254.1: icmp_seq=2 ttl=128 time=0.392 ms
64 bytes from 172.17.254.1: icmp_seq=3 ttl=128 time=0.397 ms
64 bytes from 172.17.254.1: icmp_seq=4 ttl=128 time=0.393 ms
64 bytes from 172.17.254.1: icmp_seq=5 ttl=128 time=0.381 ms
64 bytes from 172.17.254.1: icmp_seq=6 ttl=128 time=0.388 ms
^C
--- 172.17.254.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5142ms
rtt min/avg/max/mdev = 0.381/0.418/0.557/0.062 ms
root@DS1: ~#_
```

Le PC **communique** avec le serveur DNS.

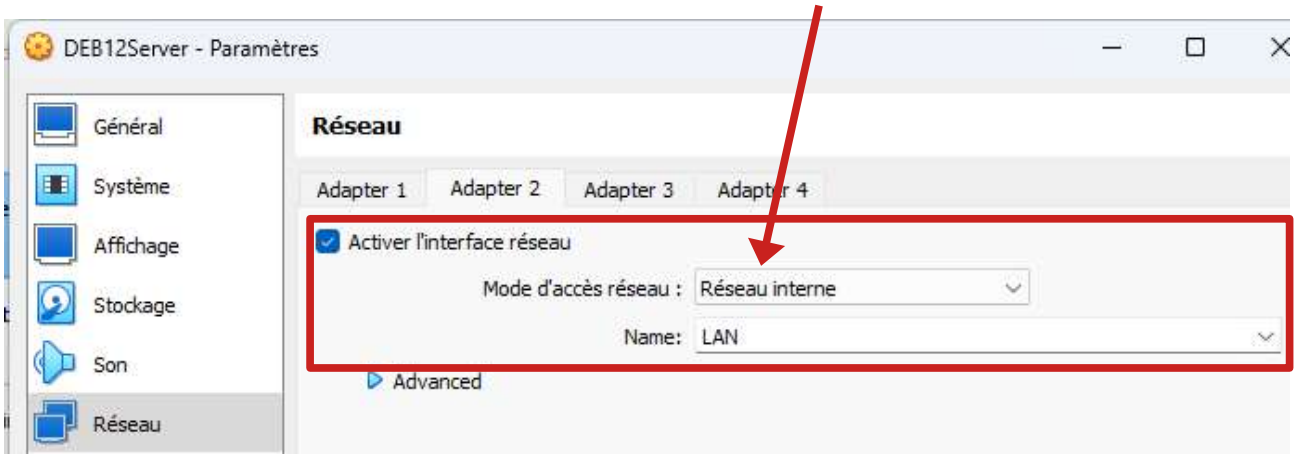
▪ Vérifiez l'accès à Internet ainsi que la résolution DNS à l'aide, par exemple, des commandes ping **8.8.8.8** et ping **www.ac-nice.fr** :

```
root@DS1: ~#ping -c 4 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=36.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=78.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=108 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=33.5 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 33.536/63.906/107.666/30.808 ms
root@DS1: ~#ping -c 4 www.ac-nice.fr
PING cs234.wpc.alphacdn.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=56 time=33.2 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=56 time=33.7 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=56 time=32.3 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=56 time=33.0 ms

--- cs234.wpc.alphacdn.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 32.264/33.044/33.708/0.523 ms
root@DS1: ~#
```

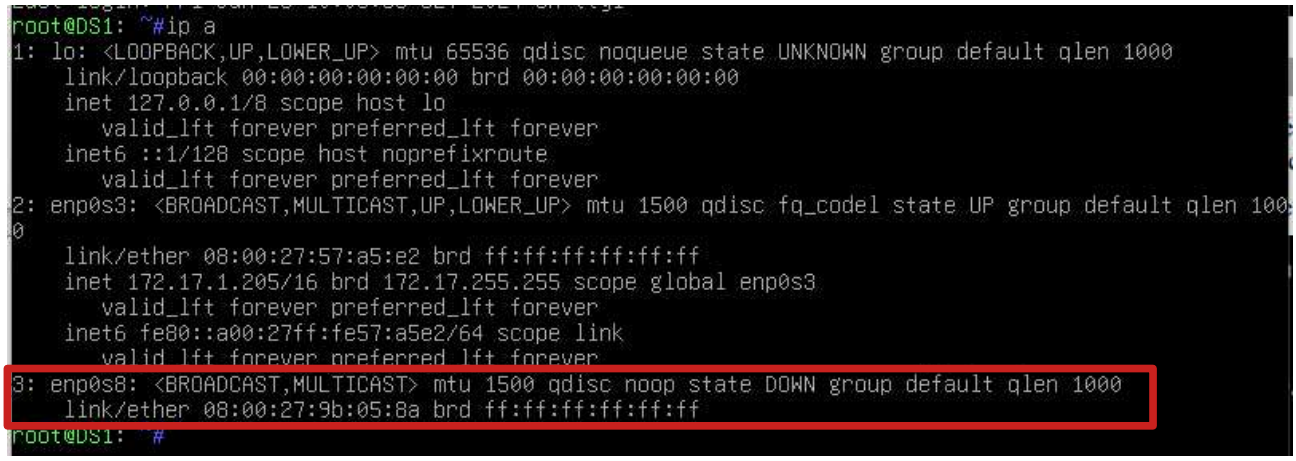
On arrive a ping « **8.8.8.8 »** et « **www.ac-nice.fr** »

3. Ajout de l'interface enp0s8.

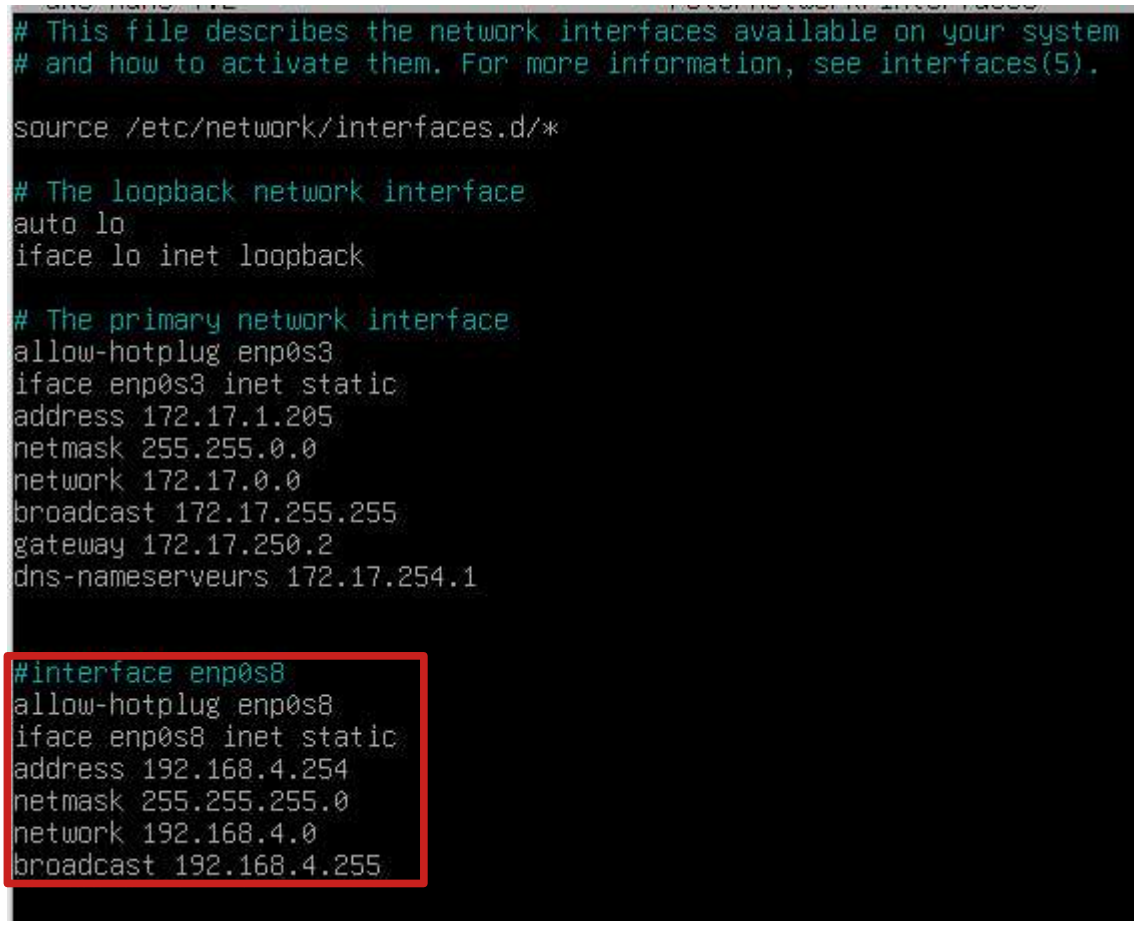
- On arrête la machine virtuelle et on ajoute une seconde carte réseau depuis le Gestionnaire de machines. On sélectionne le mode Réseau Interne (LAN) pour cette seconde carte.



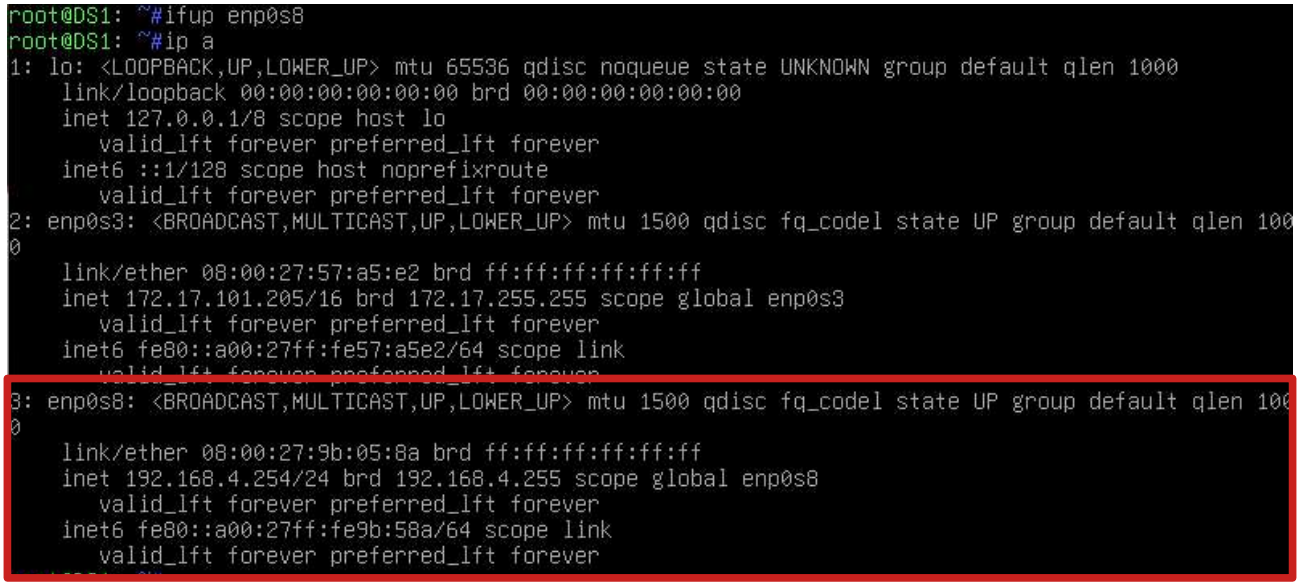
- Puis, on vérifie la prise en compte de la nouvelle carte enp0s8 à l'aide de la commande ip address (ip a):



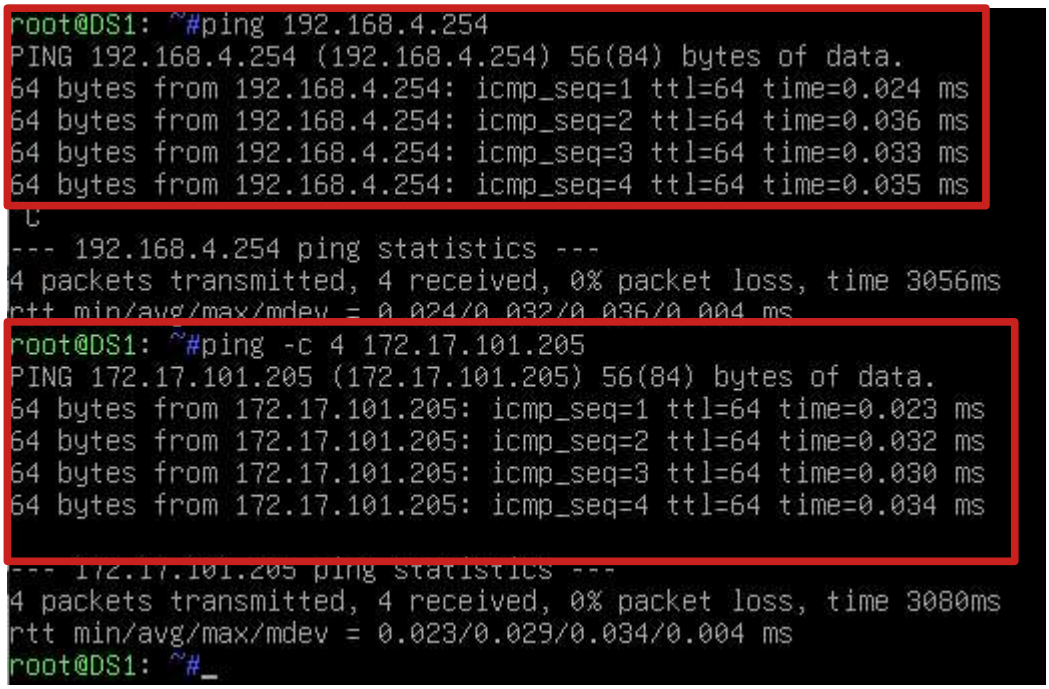
- Ensuite, on ajoute l'interface enp0s8 dans le fichier /etc/network/interfaces. @IP fixe : 192.168.4.254 /24.



- Ensuite, on active la carte et vérifiez la bonne configuration réseau avec la commande ip a :

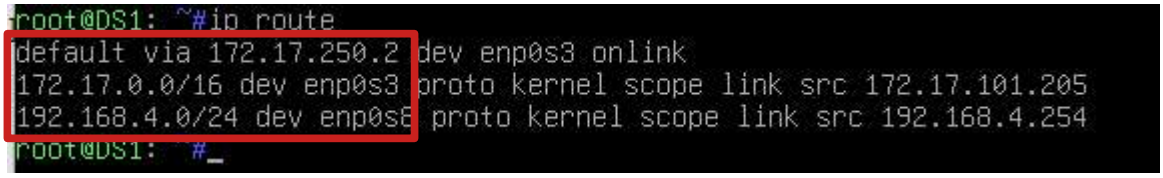


- Puis, on vérifie la bonne configuration réseau de la machine DS1 avec la commande ping sur ses deux interfaces :



On voit que les interfaces enp0s3 et enp0s8 sont bien configurés.

- Pour finir, on affiche la table de routage de DS1 :



4. Transformation du serveur en routeur.

Transformer le serveur DS1 en routeur consiste à faire transiter les paquets arrivant par l'interface enp0s8 vers enp0s3 et vice-versa.

- Afin d'activer le routage, saisissez la commande positionnant un drapeau pour le processus ip_forward (valeur 1 dans le fichier ip_forward au lieu de 0 par défaut) :

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

- Afin que le routage soit mis en place après chaque démarrage de la machine, on enleve le # de commentaire à la ligne **net.ipv4.ip_forward=1** dans le fichier « /etc/sysctl.conf » :

On tape la commande :

```
root@DS1: ~#nano /etc/sysctl.conf
```

```
  GNU nano 7.2                                  /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
```

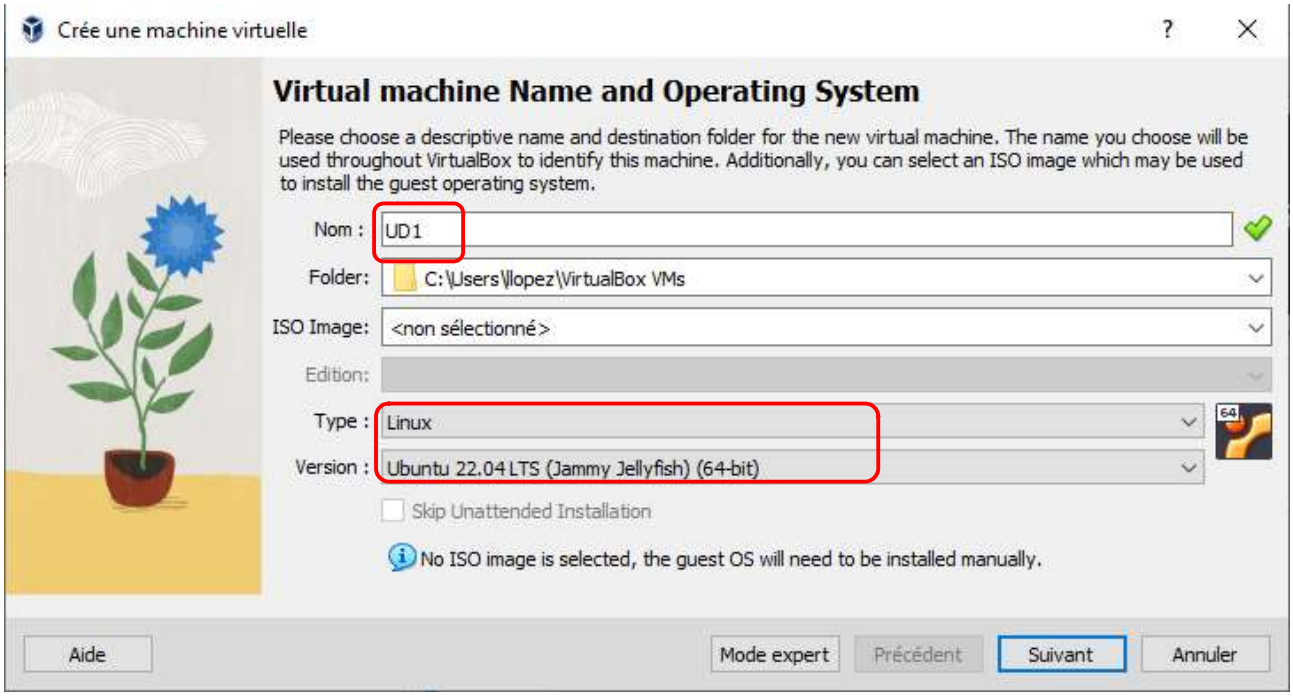
On redémarre la machine avec la commande reboot et à l'aide de la commande « cat » on vérifie que le routage soit bien mis en place (valeur 1 dans le fichier ip_forward) :

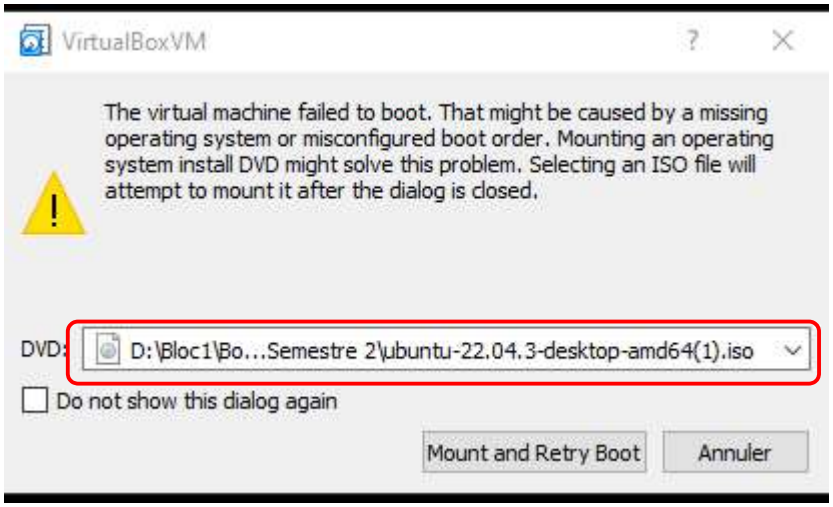
```
root@DS1: ~#cat /proc/sys/net/ipv4/ip_forward
1
root@DS1: ~#
```

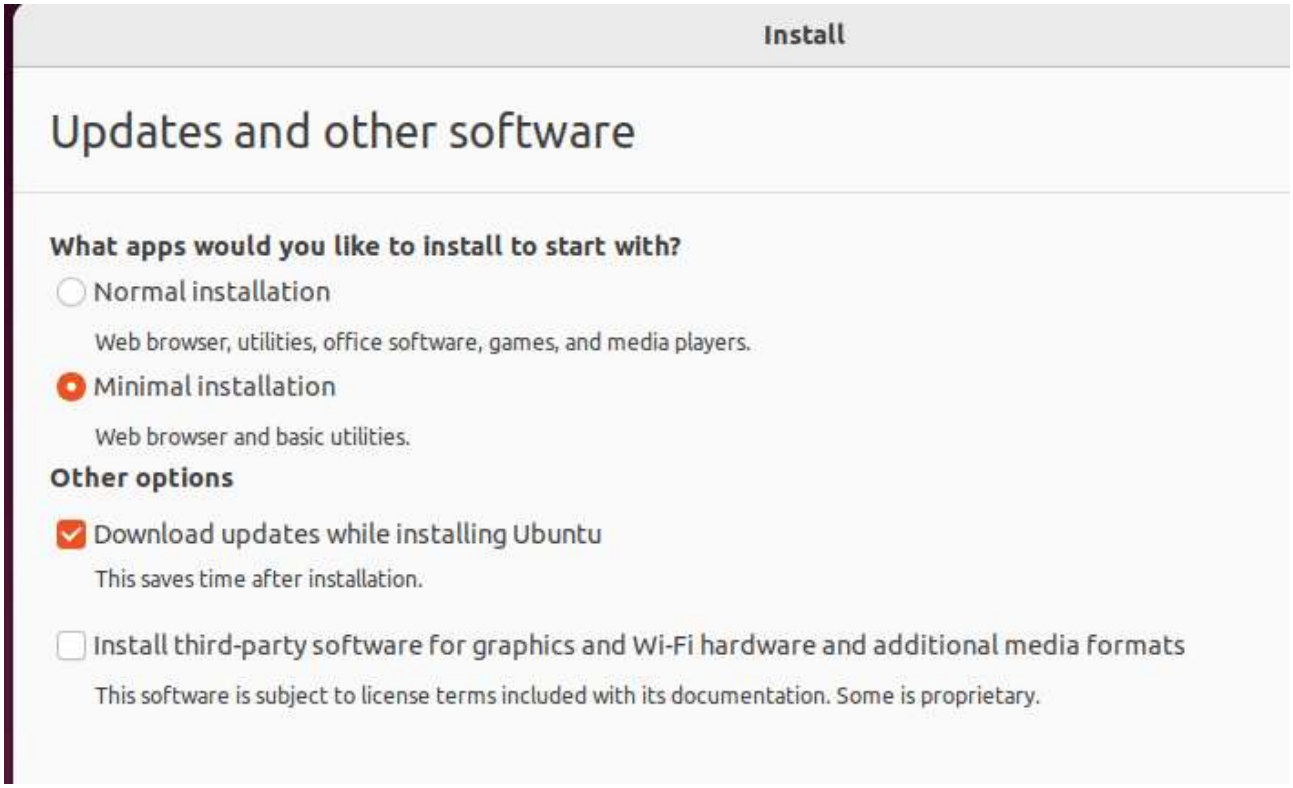
5. Configuration du poste client Ubuntu Desktop 22.04.

Premièrement, on télécharge **l'iso ubuntu-22.04.3-desktop-amd64** et créer la VM UD1.

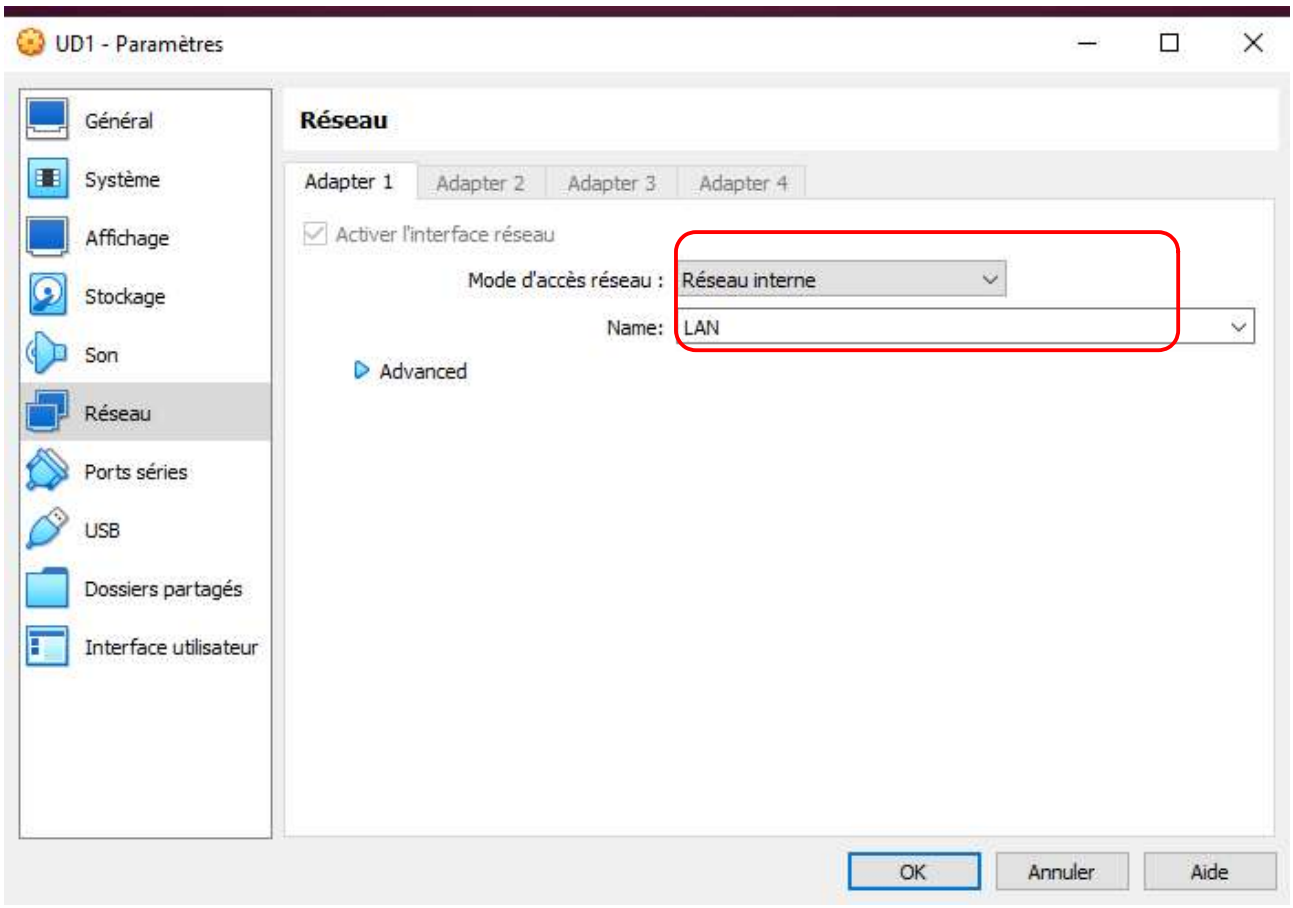
Voici, les différentes étapes e l'installation.







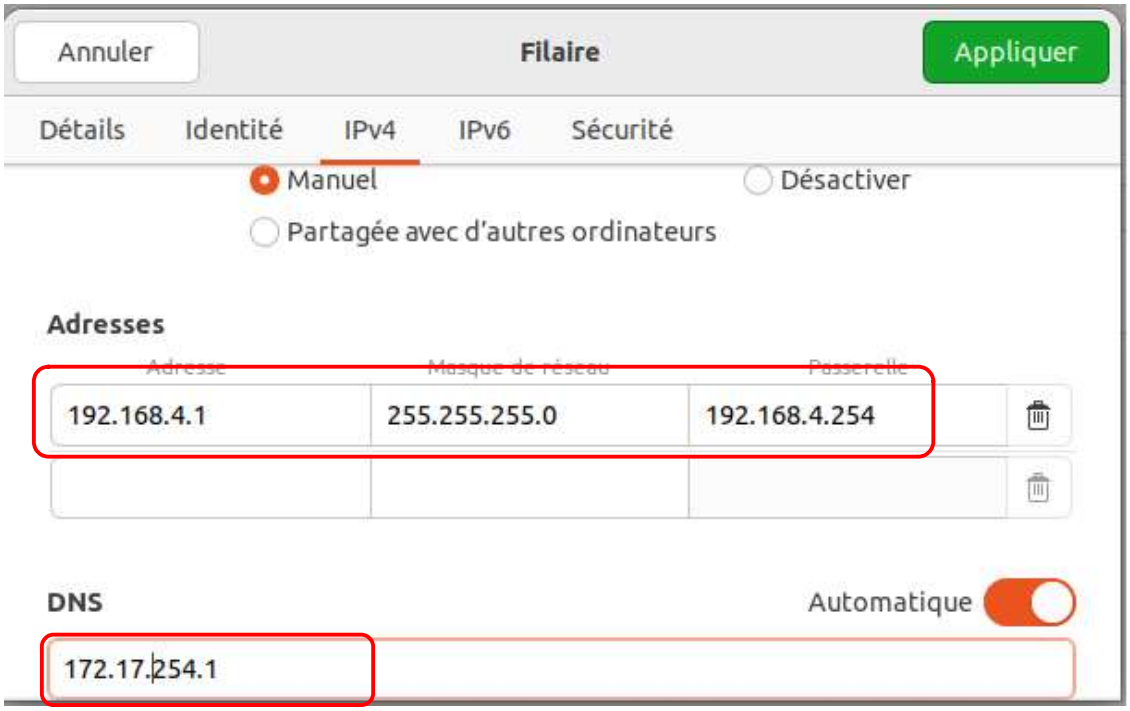
Une fois installé, on sélectionne le mode d'accès **Réseau Interne (LAN)**



Puis, on établit la configuration IP de UD1 via l'interface Network Manager :

@IP : 192.168.4.1/24 ; GW : 192.168.4.254

DNS : 172.17.254.1 (à la maison : @ de la box)



On vérifie grâce à la commande « ip a » les configuration précédemment faites.

```
sio@UD1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 gr
oup default qlen 1000
    link/ether 08:00:27:9a:8c:e1 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::46d4:c97d:838c:bf57/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
sio@UD1:~$
```

A l’aide de la commande « ip route », on consulte la table de routage de UD1 et plus particulièrement la route par défaut et la passerelle afférente

```
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
```

Puis, on pingue depuis le client Linux les deux interfaces du serveur DS1 afin de vérifier la connectivité entre les deux machines ainsi que le bon fonctionnement du routage :

On ping enp0s3 en premiere :

```
sio@UD1:~$ ping -c 3 172.17.101.205
PING 172.17.101.205 (172.17.101.205) 56(84) bytes of data.
64 bytes from 172.17.101.205: icmp_seq=1 ttl=64 time=0.221 ms
64 bytes from 172.17.101.205: icmp_seq=2 ttl=64 time=0.191 ms
64 bytes from 172.17.101.205: icmp_seq=3 ttl=64 time=0.210 ms
```

Puis enp0s8 :

```
sio@UD1:~$ ping -c 3 192.168.4.254
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=0.234 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.199 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.203 ms
```

- Vérifiez l'accès à Internet en pinguant maintenant l'interface du routeur Cisco permettant de quitter le réseau local (172.17.250.2).

```
sio@UD1:~$ ping -c1 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
From 192.168.4.254 icmp_seq=1 Destination Host Unreachable

--- 172.17.250.2 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

sio@UD1:~$ S
```

Que constatez-vous ?

On constate que l'on peut transmettre des paquets mais, on ne peut pas en recevoir.

Quelle en est la raison ?

Le routeur Cisco ne connaît pas la route qui mène à UD1.

6. Configuration du NAT sur le serveur DS1.

Premierement, on installe Iptables :

```
root@DS1: ~#apt-get install iptables
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
iptables est déjà la version la plus récente (1.8.9-2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 67 non mis à jour.
root@DS1: ~#
```

Il faut mettre en place l'IP Masquerading (politique MASQUERADE) :

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

- **« -t nat »** indique l'utilisation de la table NAT.
- **« -A POSTROUTING »** ajoute la règle dans la chaîne POSTROUTING.
- **« -o enp0s3 »** indique l'interface (celle sur l'extérieur).
- **« -j MASQUERADE »** indique le remplacement de l'adresse IP source du paquet par celle de l'interface enp0s3 du serveur.

On vérifie la bonne prise en compte de la règle par **« iptables -t nat -L -v »** :

```
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
  279 18255 MASQUERADE  all  --  any    enp0s3  192.168.4.0/24       anywhere
root@DS1: ~#
```

Afin que la translation d'adresses NAT soit activée à chaque démarrage, il faut installer le paquet **« iptables-persistent »** :

```
root@DS1: ~#apt-get install iptables-persistent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
iptables-persistent est déjà la version la plus récente (1.0.20).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 67 non mis à jour.
root@DS1: ~#
```

```
┤ Configuration de iptables-persistent ├

Les règles actuelles peuvent être enregistrées dans le fichier de configuration
« /etc/iptables/rules.v4 ». Ces règles seront chargées au prochain redémarrage de la
machine.

Les règles ne sont enregistrées automatiquement que lors de l'installation du paquet.
Veuillez consulter la page de manuel de iptables-save(8) pour connaître la manière de garder
à jour le fichier des règles.

Faut-il enregistrer les règles IPv4 actuelles ?

                    <Oui>                    <Non>
```

```
┤ Configuration de iptables-persistent ├

Les règles actuelles peuvent être enregistrées dans le fichier de configuration
« /etc/iptables/rules.v6 ». Ces règles seront chargées au prochain redémarrage de la
machine.

Les règles ne sont enregistrées automatiquement que lors de l'installation du paquet.
Veuillez consulter la page de manuel de ip6tables-save(8) pour connaître la manière de
garder à jour le fichier des règles.

Faut-il enregistrer les règles IPv6 actuelles ?

                    <Oui>                    <Non>
```

Relancez le système (commande reboot) et vérifiez à nouveau l'existence de la règle NAT à l'aide de la commande **« iptables -t nat –L -v »** :

```
root@DS1: ~#iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 10 packets, 1264 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 2 packets, 398 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 2 packets, 398 bytes)
 pkts bytes target     prot opt in     out     source               destination
    7   536 MASQUERADE  all  --  any    enp0s3  192.168.4.0/24       anywhere
root@DS1: ~#_
```

Ensuite on vérifie le bon fonctionnement du routage et de la translation d'adresse NAT à partir du client Ubuntu en pinguant la passerelle 172.17.250.2.

```
sio@UD1:~$ 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=254 time=0.658 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=254 time=0.633 ms
64 bytes from 172.17.250.2: icmp_seq=3 ttl=254 time=0.663 ms
64 bytes from 172.17.250.2: icmp_seq=4 ttl=254 time=0.672 ms
^C
--- 172.17.250.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.633/0.656/0.672/0.014 ms
sio@UD1:~$
```

Ensuite, on installe sur DS1 le paquet tcpdump, puis on effectue, à l'aide de la commande tcpdump, une capture des trames ICMP sur chaque interface du routeur/NAT DS1 la translation sur enp0s3 :

```
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
17:15:29.896260 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 1, length 64
17:15:29.896702 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 1, length 64
17:15:30.917118 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 2, length 64
17:15:30.917568 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 2, length 64
17:15:31.940006 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 3, length 64
17:15:31.940426 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 3, length 64
17:15:32.965519 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 4, length 64
17:15:32.965946 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 4, length 64
17:15:33.990020 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 5, length 64
17:15:33.990470 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 5, length 64
17:15:35.013625 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 6, length 64
17:15:35.014066 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 6, length 64
17:15:36.037918 IP 172.17.101.205 > 172.17.250.2: ICMP echo request, id 13, seq 7, length 64
17:15:36.038342 IP 172.17.250.2 > 172.17.101.205: ICMP echo reply, id 13, seq 7, length 64
```

Sur enp0s8, l'IP source de la trame ICMP Echo request est encore celle de UD1:

```
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
17:20:58.620482 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 18, seq 1, length 64
17:20:58.620984 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 18, seq 1, length 64
17:20:59.624748 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 18, seq 2, length 64
17:20:59.625199 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 18, seq 2, length 64
17:21:00.649453 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 18, seq 3, length 64
17:21:00.649892 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 18, seq 3, length 64
17:21:01.674149 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 18, seq 4, length 64
17:21:01.674590 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 18, seq 4, length 64
^[
```

Il faut vérifier le bon fonctionnement de la translation et de la résolution DNS avec la commande ping www.ac-nice.fr depuis le client UD1.

```
sio@UD1:~$ ping www.ac-nice.fr
PING cs234.wpc.alphacdn.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=55 time=85.6 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=55 time=85.1 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=55 time=87.2 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=55 time=122 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=5 ttl=55 time=97.5 ms
^C
--- cs234.wpc.alphacdn.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4325ms
rtt min/avg/max/mdev = 85.105/95.474/121.961/13.991 ms
sio@UD1:~$
```

Pour finir, on lance le navigateur et vérifiez la possibilité d'aller sur internet.