

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

1. Premiers réglages

- 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. Créez également l'alias grep :

```
GNU nano 3.2 /root/.bashrc Modifié
# ~/.bashrc: executed by bash(1) for non-login shells.

# Note: PS1 and umask are already set in /etc/profile. You should not
# need this unless you want different defaults for root.
# PS1='${debian_chroot:+($debian_chroot)}\h:\w\$ '
# umask 022

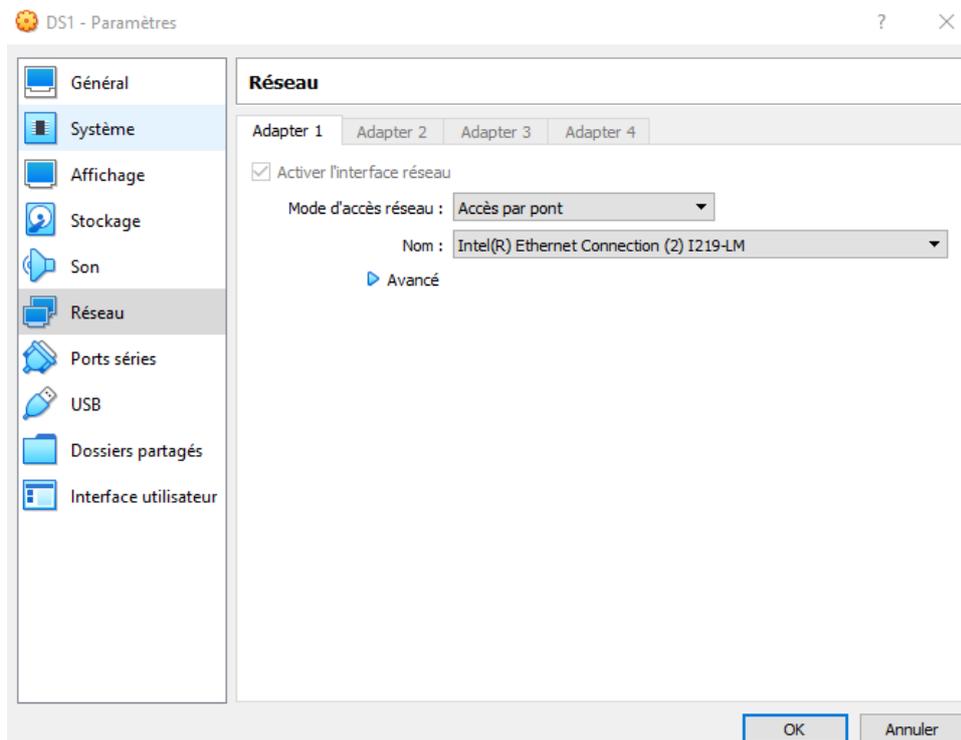
# You may uncomment the following lines if you want `ls' to be colorized:
export LS_OPTIONS='--color=auto'
# eval "dircolors"
alias ls='ls $LS_OPTIONS'
# alias ll='ls $LS_OPTIONS -l'
# alias l='ls $LS_OPTIONS -lA'
#
# Some more alias to avoid making mistakes:
# alias rm='rm -i'
# alias cp='cp -i'
# alias mv='mv -i'
PS1='\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\] \w\$ \[\033[00m\] '
alias grep='grep --color=auto'
```

2. Configuration réseau du serveur 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
        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 08:00:27:7a:53:31 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85949sec preferred_lft 85949sec
    inet6 fe80::a00:27ff:fe7a:5331/64 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 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:71:86:85
Sending on   LPF/enp0s3/08:00:27:71:86:85
Sending on   Socket/fallback
DHCPRELEASE of 10.0.2.15 on enp0s3 to 10.0.2.2 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 :

```
GNU nano 3.2 /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 192.168.1.101
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns-nameservers 192.168.1.1
```

- Réactivez la carte réseau (ifup enp0s3) et vérifiez la configuration IP (ip a). Effectuez une capture d'écran.

```
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 08:00:27:71:86:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe71:8685/64 scope link
        valid_lft forever preferred_lft forever
root@DS1: ~#
```

- 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. Effectuez une capture d'écran.

```
root@DS1: ~# cat /etc/resolv.conf
domain home
search home
nameserver 192.168.1.1
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 192.168.1.1 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.101
root@DS1: ~#
```

- Pinguez la passerelle ainsi que le serveur DNS pour vous assurer de la bonne connectivité IP :

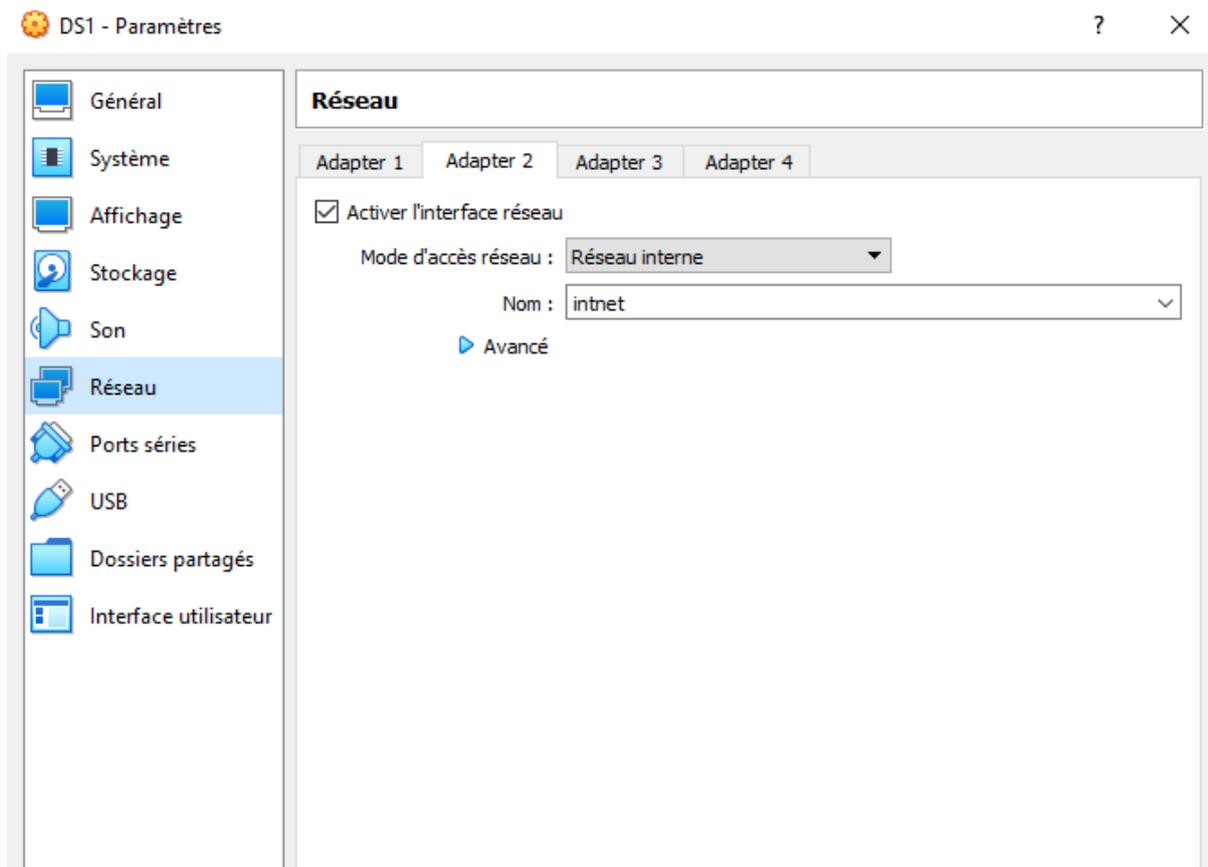
```
root@DS1: ~#ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=7.23 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=6.96 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=7.09 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 6.960/7.091/7.229/0.129 ms
root@DS1: ~#
```

- 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=116 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=14.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=13.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=19.7 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 13.593/15.436/19.733/2.498 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=57 time=14.1 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=57 time=15.0 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=57 time=14.2 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=57 time=13.5 ms
--- cs234.wpc.alphacdn.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 13.474/14.190/15.046/0.580 ms
root@DS1: ~#
```

3. Ajout de l'interface enp0s8.

- Arrêtez la machine virtuelle et ajoutez une seconde carte réseau depuis le Gestionnaire de machines. Sélectionnez le mode Réseau Interne (LAN) pour cette seconde carte.



- Vérifiez la prise en compte de la nouvelle carte enp0s8 à l'aide de la commande ip address :

```
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 08:00:27:71:86:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe71:8685/64 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:f6:88:48 brd ff:ff:ff:ff:ff:ff
root@DS1: ~#
```

- Modifiez, avec l'éditeur de texte VIM, le fichier /etc/network/interfaces pour l'interface enp0s8.

```
# 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 192.168.1.101
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns-nameservers 192.168.1.1

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
```

- Activez la carte et vérifiez la bonne configuration réseau avec la commande ip a :

```
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 08:00:27:71:86:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe71:8685/64 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:f6:88:48 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:fef6:8848/64 scope link
        valid_lft forever preferred_lft forever
root@DS1: ~#
```

- Vérifiez la bonne configuration réseau de la machine DS1 avec la commande ping sur ses deux interfaces :

```
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=0.047 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 192.168.4.254: icmp_seq=5 ttl=64 time=0.049 ms
64 bytes from 192.168.4.254: icmp_seq=6 ttl=64 time=0.049 ms
^C
--- 192.168.4.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 0.034/0.046/0.049/0.006 ms
root@DS1: ~# ping -c 4 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data:
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.051 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=0.018 ms
--- 192.168.1.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 28ms
rtt min/avg/max/mdev = 0.018/0.033/0.051/0.017 ms
root@DS1: ~#
```

- Affichez la table de routage de DS1 :

```
root@DS1: ~# ip route
default via 192.168.1.1 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.101
192.168.4.0/24 dev enp0s8 proto kernel scope link src 192.168.4.254
root@DS1: ~#_
```

4. Transformation du serveur en routeur

- 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: ~#_
```

```
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, enlevez-le # de commentaire à la ligne net.ipv4.ip_forward=1 dans le fichier /etc/sysctl.conf :

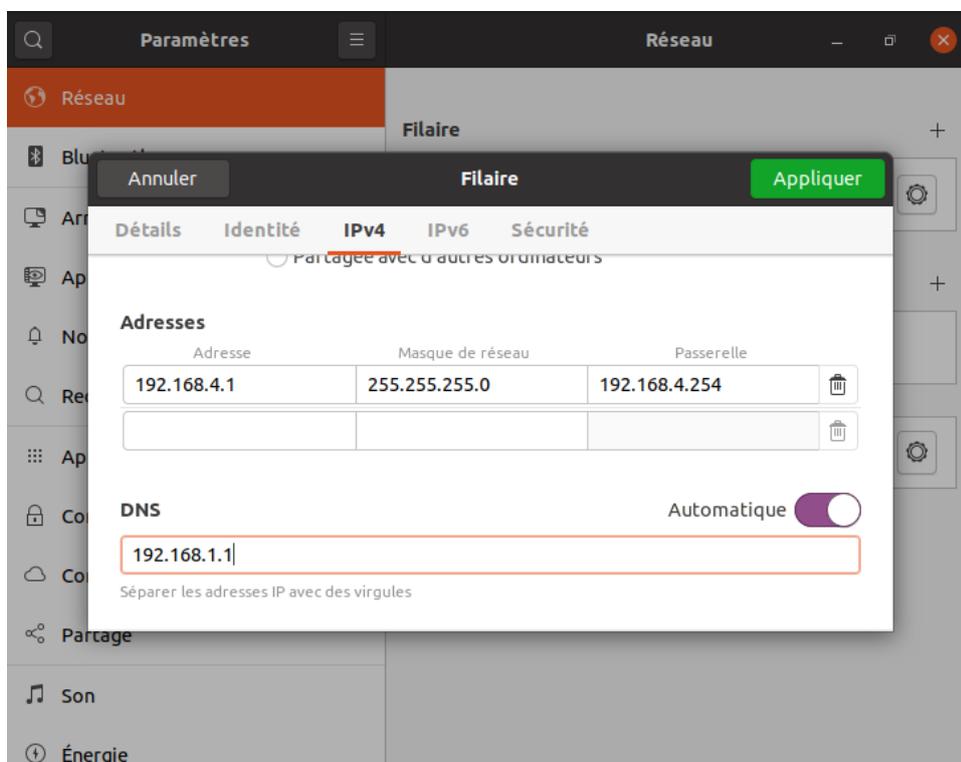
```
GNU nano 3.2 /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####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
```

- Redémarrez la machine avec la commande reboot et vérifiez 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 20.04.

- Sélectionnez le mode d'accès Réseau Interne (LAN) et établissez la configuration IP de UD1 via l'interface Network Manager :



```
sio@sio-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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 g
roup default qlen 1000
    link/ether 08:00:27:03:fe:54 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::3ab1:38a8:c96b:427b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
sio@sio-VirtualBox:~$
```

- Consultez la table de routage de UD1 et plus particulièrement la route par défaut et la passerelle afférente à l'aide de la commande ip route.

```
sio@sio-VirtualBox:~$ 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
sio@sio-VirtualBox:~$
```

- Pinguez 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 :

```
sio@sio-VirtualBox:~$ 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=0.374 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.406 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.458 ms

--- 192.168.4.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.374/0.412/0.458/0.034 ms
sio@sio-VirtualBox:~$ ping -c 3 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.343 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.923 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.378 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2021ms
rtt min/avg/max/mdev = 0.343/0.548/0.923/0.265 ms
sio@sio-VirtualBox:~$
```

- Vérifiez l'accès à Internet en pinguant maintenant l'interface du routeur permettant de quitter le réseau local. Que constatez-vous ?

On constate que UD1 ne peut communiquer en dehors du réseau local.

```
sio@sio-VirtualBox:~$ ping -c1 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

--- 192.168.1.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

sio@sio-VirtualBox:~$
```

6. Configuration du NAT sur le serveur DS1.

- Mettez 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: ~#
```

- Vérifiez 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 POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in     out     source      destination
    18 1150 MASQUERADE all  --  any    enp0s3  192.168.4.0/24  anywhere
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in     out     source      destination
root@DS1: ~#_

```

- Afin que la translation d'adresses NAT soit activée à chaque démarrage, installez le paquet iptables-persistent :

```

root@DS1: ~#apt-get install iptables-persistent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
 netfilter-persistent
Les NOUVEAUX paquets suivants seront installés :
 iptables-persistent netfilter-persistent
0 mis à jour, 2 nouvellement installés, 0 à enlever et 27 non mis à jour.
Il est nécessaire de prendre 22,0 ko dans les archives.
Après cette opération, 81,9 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o

```

- 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 :

```

root@DS1: ~#iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 36 packets, 8349 bytes)
 pkts bytes target      prot opt in     out     source      destination
Chain INPUT (policy ACCEPT 2 packets, 464 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
    7  484 MASQUERADE all  --  any    enp0s3  192.168.4.0/24  anywhere
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in     out     source      destination
root@DS1: ~#_

```

- Vérifiez le bon fonctionnement du routage et de la translation d'adresse NAT à partir du client Ubuntu en pinguant la passerelle. Contrairement à votre ping de la page 7, vous devez maintenant recevoir la trame ICMP Echo reply :

```
slo@slo-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=7.39 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=7.63 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=7.71 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=11.2 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=8.18 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 7.391/8.420/11.198/1.411 ms
slo@slo-VirtualBox:~$
```

- Installez sur DS1 le paquet tcpdump :

```
root@DS1: ~#apt-get install tcpdump
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
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 27 non mis à jour.
Il est nécessaire de prendre 400 ko/539 ko dans les archives.
Après cette opération, 1 470 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

- Effectuez, à l'aide de la commande tcpdump, une capture des trames ICMP sur chaque interface du routeur/NAT DS1 (relancez si besoin votre ping depuis UD1) et constatez 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.

```
root@DS1: ~#tcpdump -i enp0s3 icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:32:41.739528 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 7, seq 1, length 64
10:32:41.747336 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 7, seq 1, length 64
10:32:42.741628 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 7, seq 2, length 64
10:32:42.748501 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 7, seq 2, length 64
10:32:43.743633 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 7, seq 3, length 64
10:32:43.750647 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 7, seq 3, length 64
10:32:44.745395 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 7, seq 4, length 64
10:32:44.754379 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 7, seq 4, length 64
10:32:45.747520 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 7, seq 5, length 64
10:32:45.755340 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 7, seq 5, length 64
```

- Sur enp0s8, l'IP source de la trame ICMP Echo request est encore celle de UD1 (c'est normal puisque la translation a été mise en place dans la chaine POSTROUTING) :

```
root@DS1: ~#tcpdump -i enp0s8 icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
10:34:18.582159 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 8, seq 1, length 64
10:34:18.589371 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 8, seq 1, length 64
10:34:19.584152 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 8, seq 2, length 64
10:34:19.591194 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 8, seq 2, length 64
10:34:20.586235 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 8, seq 3, length 64
10:34:20.594115 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 8, seq 3, length 64
10:34:21.587698 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 8, seq 4, length 64
10:34:21.594935 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 8, seq 4, length 64
```

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

```
sio@sio-VirtualBox:~$ 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=56 time=16.3 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=56 time=13.6 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=56 time=13.6 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=56 time=14.1 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=5 ttl=56 time=16.3 ms
^C
--- cs234.wpc.alphacdn.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 13.567/14.780/16.345/1.285 ms
sio@sio-VirtualBox:~$
```

- Lancez le navigateur et vérifiez la possibilité d'aller sur internet (effectuez une capture d'écran).

