

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

1. Rappels :

>>> Récupération de la dernière liste des paquets disponibles :

```
root@DS1: ~#apt-get install
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 43 non mis à jour.
```

>>> Nouveau nom « DS1 » du serveur Debian et redémarrage pour appliquer les changements :

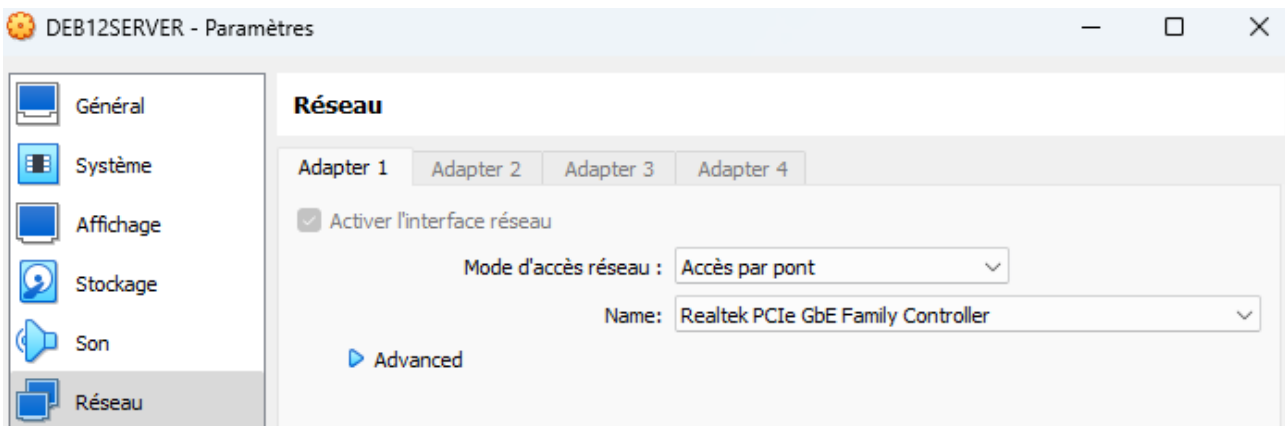
```
root@DS1: ~#echo DS1 > /etc/hostname_
root@DS1: ~#echo DS1 > /etc/hosts
```

2. Configuration réseau du serveur DS1 :

>>> Vérification de la configuration réseau actuelle (Mode d'accès 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
: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d0:d5:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86102sec preferred_lft 86102sec
    inet6 fe80::a00:27ff:fed0:d5d1/64 scope link
        valid_lft forever preferred_lft forever
root@DS1: ~#
```

>>> Modification du mode d'accès réseau en Accès par pont :



>>> Désactivation de la carte réseau enp0s3 :

```
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:d0:d5:d1
Sending on   LPF/enp0s3/08:00:27:d0:d5:d1
Sending on   Socket/fallback
DHCPRELEASE of 10.0.2.15 on enp0s3 to 10.0.2.2 port 67
root@DS1: ~#
```

>>> Modification du fichier /etc/network/interfaces pour enp0s3 :

```
# 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
auto enp0s3
iface enp0s3 inet static
    address 172.17.101.204
    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
```

>>> Réactivation de la carte réseau + vérification de la configuration IP :

```
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 noprefixroute
        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:d0:d5:d1 brd ff:ff:ff:ff:ff:ff
    inet 172.17.101.204/24 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed0:d5d1/64 scope link
        valid_lft forever preferred_lft forever
```

>>> Affichage du contenu /etc/resolv.conf avec cat pour vérifier la présence de l'IP du DNS :

```
root@DS1: ~#cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "resolvectl status" to see details about the actual nameservers.

nameserver 172.17.254.1
root@DS1: ~#
```

>>> Table de routage de DS1 :

```
root@DS1: ~#ip route
default via 172.17.250.2 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
172.17.101.0/24 dev enp0s3 proto kernel scope link src 172.17.101.204
root@DS1: ~#
```

>>> Ping de la passerelle (172.17.250.2) ainsi que le serveur DNS (172.17.254.1) :

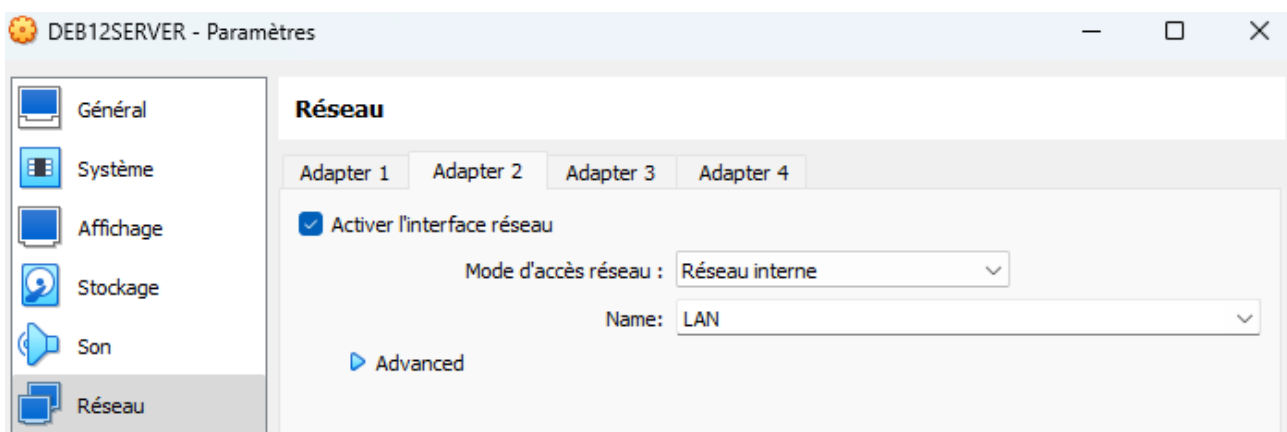
```
root@DS1: ~#ping 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
64 bytes from 172.17.250.2: icmp_seq=1 ttl=255 time=1.87 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=255 time=0.971 ms
64 bytes from 172.17.250.2: icmp_seq=3 ttl=255 time=1.45 ms
64 bytes from 172.17.250.2: icmp_seq=4 ttl=255 time=1.62 ms
64 bytes from 172.17.250.2: icmp_seq=5 ttl=255 time=1.04 ms
64 bytes from 172.17.250.2: icmp_seq=6 ttl=255 time=1.07 ms
64 bytes from 172.17.250.2: icmp_seq=7 ttl=255 time=0.923 ms
^C
--- 172.17.250.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.923/1.277/1.867/0.339 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=2.13 ms
64 bytes from 172.17.254.1: icmp_seq=2 ttl=128 time=1.08 ms
64 bytes from 172.17.254.1: icmp_seq=3 ttl=128 time=0.993 ms
64 bytes from 172.17.254.1: icmp_seq=4 ttl=128 time=1.02 ms
^C
--- 172.17.254.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.993/1.303/2.125/0.475 ms
root@DS1: ~#
```

>>> Ping à Google et www.ac-nice.fr :

```
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=32.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=32.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=32.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=32.5 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 31.933/32.231/32.538/0.256 ms
root@DS1: ~#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=33.5 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=2 ttl=56 time=32.7 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=3 ttl=56 time=32.7 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=4 ttl=56 time=32.5 ms
64 bytes from 93.184.221.161 (93.184.221.161): icmp_seq=5 ttl=56 time=32.7 ms
^C
--- cs234.wpc.alphacdn.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 32.512/32.825/33.490/0.340 ms
root@DS1: ~#
```

3. Ajout de l'interface enp0s8 :

>>> Ajout d'une seconde carte réseau depuis le gestionnaire des machines + mode d'accès en réseau interne (LAN) pour celle-ci :



>>> Vérification de la prise en compte de la nouvelle carte 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 noprefixroute
        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:d0:d5:d1 brd ff:ff:ff:ff:ff:ff
    inet 172.17.101.204/24 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed0:d5d1/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:65:ac:b4 brd ff:ff:ff:ff:ff:ff
root@DS1: ~#
```

>>> Ajout de l'interface enp0s8 dans /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
auto enp0s3
iface enp0s3 inet static
address 172.17.101.204
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
```

>>> Activation de la carte et vérification de la bonne configuration réseau avec 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 noprefixroute
        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:d0:d5:d1 brd ff:ff:ff:ff:ff:ff
    inet 172.17.101.204/24 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed0:d5d1/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:65:ac:b4 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:fe65:acb4/64 scope link
        valid_lft forever preferred_lft forever
root@DS1: ~#

```

>>> Vérification de la bonne configuration réseau de DS1 en faisant un ping sur les deux interfaces (premier ping (192.168.4.254) → enp0s8 /// deuxième ping (172.17.101.204) → enp0s3)

```

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=0.035 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.032 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.031 ms
^C
--- 192.168.4.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.031/0.032/0.035/0.001 ms
root@DS1: ~#ping 172.17.101.204
PING 172.17.101.204 (172.17.101.204) 56(84) bytes of data.
64 bytes from 172.17.101.204: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 172.17.101.204: icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from 172.17.101.204: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 172.17.101.204: icmp_seq=4 ttl=64 time=0.051 ms
^C
--- 172.17.101.204 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3065ms
rtt min/avg/max/mdev = 0.023/0.038/0.051/0.010 ms
root@DS1: ~#

```

>>> Table de routage de DS1 :

```
root@DS1: ~#ip route
default via 172.17.250.2 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
172.17.101.0/24 dev enp0s3 proto kernel scope link src 172.17.101.204
192.168.4.0/24 dev enp0s8 proto kernel scope link src 192.168.4.254
root@DS1: ~#
```

4. Transformation du serveur en routeur :

>>> Application d'un drapeau pour le processus ip_forward :

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

>>> Suppression du # à la ligne net.ipv4.ip_forward=1 dans /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
```

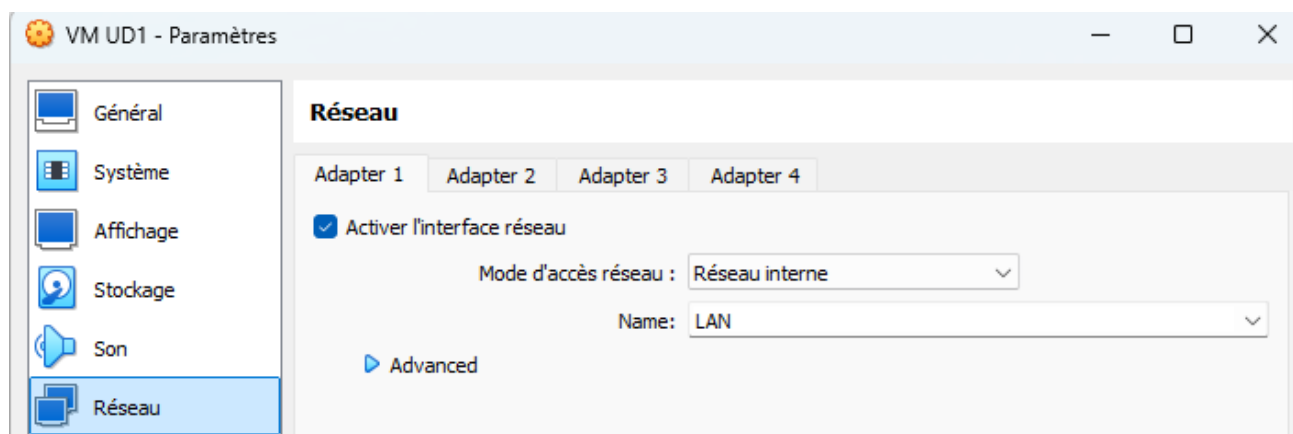
>>> Redémarrage de la machine et vérification de la bonne mise en place du routage (valeur 1) :

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

5. Configuration du poste client Ubuntu (Desktop 24.04 LTS) :

Note : La machine Ubuntu a été configurée et installée au préalable.

>>> Mode d'accès en Réseau Interne (LAN) et établissement de la configuration IP de UD1 via l'interface Network Manager :



>>> Vérification de la configuration IP de la carte réseau d'UD1 :

```
UD1@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 noprefixroute
        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 08:00:27:9c:99:3d 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
UD1@UD1:~$
```

>>> Table de routage de UD1 (route par défaut en rouge) :

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

>>> Ping des deux interfaces pour vérifier la connectivité entre les deux machines et le bon fonctionnement du routage :

```
UD1@UD1:~$ 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=0.523 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.679 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.439 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.813 ms
^C
--- 192.168.4.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.439/0.613/0.813/0.143 ms
UD1@UD1:~$ ping 172.17.101.204
PING 172.17.101.204 (172.17.101.204) 56(84) bytes of data.
64 bytes from 172.17.101.204: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 172.17.101.204: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 172.17.101.204: icmp_seq=3 ttl=64 time=0.988 ms
64 bytes from 172.17.101.204: icmp_seq=4 ttl=64 time=0.577 ms
^C
--- 172.17.101.204 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.483/0.789/1.110/0.265 ms
UD1@UD1:~$
```

>>> Ping de l'interface du routeur Cisco :

```
UD1@UD1:~$ ping 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
^C
--- 172.17.250.2 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18467ms
UD1@UD1:~$
```

→ Le ping envoie les paquets mais ne reçoit pas de réponses.

→ La translation dynamique n'est pas mise en place, l'adresse IP n'est pas changée lors du renvoi de la réponse et ne peut donc pas aboutir. UD1 ne peut donc pas communiquer avec l'extérieur.

6. Configuration du NAT sur le serveur DS1 :

>>> Installation du paquet iptables sur le serveur DS1 :

```
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
Les paquets supplémentaires suivants seront installés :
  libip6tc2 libnetfilter-contrack3 libnfnetlink0
Paquets suggérés :
  firewallld
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 libnetfilter-contrack3 libnfnetlink0
0 mis à jour, 4 nouvellement installés, 0 à enlever et 43 non mis à jour.
Il est nécessaire de prendre 435 ko dans les archives.
Après cette opération, 2 728 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19,4 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 libnfnetlink0 amd64 1.0.2-2 [15,1 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 libnetfilter-contrack3 amd64 1.0.9-3 [40,7 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
435 ko réceptionnés en 0s (1 075 ko/s)
Sélection du paquet libip6tc2:amd64 précédemment désélectionné.
(Lecture de la base de données... 30115 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libip6tc2_1.8.9-2_amd64.deb ...
Dépaquetage de libip6tc2:amd64 (1.8.9-2) ...
Sélection du paquet libnfnetlink0:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libnfnetlink0_1.0.2-2_amd64.deb ...
Dépaquetage de libnfnetlink0:amd64 (1.0.2-2) ...
Sélection du paquet libnetfilter-contrack3:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libnetfilter-contrack3_1.0.9-3_amd64.deb ...
Dépaquetage de libnetfilter-contrack3:amd64 (1.0.9-3) ...
Sélection du paquet iptables précédemment désélectionné.
Préparation du dépaquetage de .../iptables_1.8.9-2_amd64.deb ...
Dépaquetage de iptables (1.8.9-2) ...
Paramétrage de libip6tc2:amd64 (1.8.9-2) ...
Paramétrage de libnfnetlink0:amd64 (1.0.2-2) ...
Paramétrage de libnetfilter-contrack3:amd64 (1.0.9-3) ...
Paramétrage de iptables (1.8.9-2) ...
update-alternatives: utilisation de « /usr/sbin/iptables-legacy » pour fournir « /usr/sbin/iptables » (iptables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/ip6tables-legacy » pour fournir « /usr/sbin/ip6tables » (ip6tables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/iptables-nft » pour fournir « /usr/sbin/iptables » (iptables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/ip6tables-nft » pour fournir « /usr/sbin/ip6tables » (ip6tables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/arptables-nft » pour fournir « /usr/sbin/arptables » (arptables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/ebrtables-nft » pour fournir « /usr/sbin/ebrtables » (ebrtables) en mode automatique
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u8) ...
root@DS1: ~#
```

>>> Mise en place de l'IP Masquerading :

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

>>> Vérification de la bonne prise en compte de la règle :

```
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
  12  812 MASQUERADE  all  --  any    enp0s3  192.168.4.0/24  anywhere
root@DS1: ~#
```

>>> Installation du paquet iptables-persistent pour que la translation d'adresses NAT soit activée à chaque démarrage :

Outil de configuration des paquets

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 ». Des 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 IPv6 actuelles ?
<Oui> <Non>

sélection du paquet netfilter-persistent précédemment désélectionné.
Lecture de la base de données... 30331 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ../netfilter-persistent_1.0.20_all.deb ...
Dépaquetage de netfilter-persistent (1.0.20) ...
sélection du paquet iptables-persistent précédemment désélectionné.
Préparation du dépaquetage de ../iptables-persistent_1.0.20_all.deb ...
Dépaquetage de iptables-persistent (1.0.20) ...
Paramétrage de netfilter-persistent (1.0.20) ...
created symlink /etc/systemd/system/iptables.service → /lib/systemd/system/netfilter-persistent.service.
created symlink /etc/systemd/system/ip6tables.service → /lib/systemd/system/netfilter-persistent.service.
created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service.
Paramétrage de iptables-persistent (1.0.20) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
root@DS1: ~#

```

>>> Vérification après redémarrage de la règle NAT :

```

root@DS1: ~# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 7 packets, 1457 bytes)
 pkts bytes target      prot opt in      out     source      destination
Chain INPUT (policy ACCEPT 7 packets, 1457 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
  0      0 MASQUERADE all  --  any     enp0s3  192.168.4.0/24  anywhere
root@DS1: ~#

```

>>> Ping du routeur Cisco pour vérifier le bon fonctionnement du routage sur le client UD1 (trames ICMP) :

```
UD1@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=7.56 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=254 time=1.30 ms
64 bytes from 172.17.250.2: icmp_seq=3 ttl=254 time=1.79 ms
64 bytes from 172.17.250.2: icmp_seq=4 ttl=254 time=1.99 ms

--- 172.17.250.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.301/3.158/7.559/2.552 ms
^CUD1@UD1:~$
```

>>> Installation du paquet tcpdump :

```
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 43 non mis à jour.
Il est nécessaire de prendre 624 ko dans les archives.
Après cette opération, 1 741 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libpcap0.8 amd64 1.10.3-1 [157 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 tcpdump amd64 4.99.3-1 [467 kB]
624 ko réceptionnés en 1s (1 155 ko/s)
Sélection du paquet libpcap0.8:amd64 précédemment désélectionné.
(Lecture de la base de données... 30357 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libpcap0.8_1.10.3-1_amd64.deb ...
Dépaquetage de libpcap0.8:amd64 (1.10.3-1) ...
Sélection du paquet tcpdump précédemment désélectionné.
Préparation du dépaquetage de .../tcpdump_4.99.3-1_amd64.deb ...
Dépaquetage de tcpdump (4.99.3-1) ...
Paramétrage de libpcap0.8:amd64 (1.10.3-1) ...
Paramétrage de tcpdump (4.99.3-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u8) ...
root@DS1: ~#
```

>>> Capture de trames ICMP sur chaque interface du routeur/NAT DS1 pour voir la translation sur enp0s3. L'adresse IP de UD1 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[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:38:47.731063 IP 172.17.101.204 > 172.17.250.2: ICMP echo request, id 8137, seq 1, length 64
16:38:47.732029 IP 172.17.250.2 > 172.17.101.204: ICMP echo reply, id 8137, seq 1, length 64
16:38:48.736060 IP 172.17.101.204 > 172.17.250.2: ICMP echo request, id 8137, seq 2, length 64
16:38:48.736942 IP 172.17.250.2 > 172.17.101.204: ICMP echo reply, id 8137, seq 2, length 64
16:38:49.739036 IP 172.17.101.204 > 172.17.250.2: ICMP echo request, id 8137, seq 3, length 64
16:38:49.740033 IP 172.17.250.2 > 172.17.101.204: ICMP echo reply, id 8137, seq 3, length 64
16:38:50.743260 IP 172.17.101.204 > 172.17.250.2: ICMP echo request, id 8137, seq 4, length 64
16:38:50.744225 IP 172.17.250.2 > 172.17.101.204: ICMP echo reply, id 8137, seq 4, length 64
```

>>> Même test sur enp0s8 (l'adresse est toujours celle de UD1 car elle est mise en place en POSTROUTING):

```
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
16:40:08.061735 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8139, seq 1, length 64
16:40:08.062693 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8139, seq 1, length 64
16:40:09.063512 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8139, seq 2, length 64
16:40:09.064490 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8139, seq 2, length 64
16:40:10.065308 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8139, seq 3, length 64
16:40:10.066342 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8139, seq 3, length 64
16:40:11.066820 IP 192.168.4.1 > 172.17.250.2: ICMP echo request, id 8139, seq 4, length 64
16:40:11.067819 IP 172.17.250.2 > 192.168.4.1: ICMP echo reply, id 8139, seq 4, length 64
```

>>> ping www.ac-nice.fr depuis UD1 :

```
UD1@UD1:~$ 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: icmp_seq=1 ttl=55 time=33.3 ms
64 bytes from 93.184.221.161: icmp_seq=2 ttl=55 time=33.7 ms
64 bytes from 93.184.221.161: icmp_seq=3 ttl=55 time=34.1 ms
64 bytes from 93.184.221.161: icmp_seq=4 ttl=55 time=34.4 ms
^C
--- cs234.wpc.alphacd.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 33.304/33.881/34.363/0.399 ms
UD1@UD1:~$
```

>>> Vérification de pouvoir aller sur internet :

