

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

Sommaire

1. Rappels.....	2
2. Configuration réseau du serveur DS1.....	3
3. Ajout de l'interface enp0s8.....	6
4. Transformation du serveur en routeur.....	9
5. Configuration du poste client Ubuntu (Desktop 24.04 LTS).....	9
6. Configuration du NAT sur le serveur DS1.....	12

1. Rappels.

Récupération de la dernière liste des paquets disponibles a l'aide de la commande apt-get update

```
root@DEB13Server: ~#apt-get update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Réception de : 2 http://security.debian.org/debian-security trixie-security InRelease [43,4 kB]
Réception de : 3 http://deb.debian.org/debian trixie-updates InRelease [47,3 kB]
Réception de : 4 http://security.debian.org/debian-security trixie-security/main Sources [117 kB]
Réception de : 5 http://security.debian.org/debian-security trixie-security/main amd64 Packages [94,2 kB]
Réception de : 6 http://security.debian.org/debian-security trixie-security/main Translation-en [59,3 kB]
361 ko réceptionnés en 0s (738 ko/s)
Lecture des listes de paquets... Fait
```

Vérification dans le fichiers bashrc qu'il y a bien la variables d'environnement PS1 et de l'activation de l'alias grep

```
GNU nano 8.4 /root/.bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.

# Note: PS1 is set in /etc/profile, and the default umask is defined
# in /etc/login.defs. 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'
alias grep='grep --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\$ \[\033[00m\]'
```

On renomme serveur debian en DS1 en modifiant les fichiers /etc/hostname et /etc/hosts
Puis redémarrage de la machine a l'aide de la commande reboot

```
GNU nano 8.4 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 DS1.sio-exupery.local DS1

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

```
GNU nano 8.4 /etc/hostname *
DS1
```

```
root@DEB13Server: ~#reboot
```

2. Configuration réseau du serveur DS1.

Vérification de la configuration réseau actuelle

```
root@DS1: ~#ip -4 address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   altname enx08002791104d
   inet 172.17.1.23/16 brd 172.17.255.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86060sec preferred_lft 75260sec
```

Installation du paquet resolvconf

```
root@DS1: ~#apt-get install resolvconf
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  resolvconf
0 mis à jour, 1 nouvellement installés, 0 à enlever et 30 non mis à jour.
Il est nécessaire de prendre 57,1 kB dans les archives.
Après cette opération, 190 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 resolvconf all 1.94 [57,1 kB]
57,1 ko réceptionnés en 0s (488 ko/s)
Préconfiguration des paquets...
Sélection du paquet resolvconf précédemment désélectionné.
(Lecture de la base de données... 61259 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../resolvconf_1.94_all.deb ...
Dépaquetage de resolvconf (1.94) ...
Paramétrage de resolvconf (1.94) ...
Created symlink '/etc/systemd/system/sysinit.target.wants/resolvconf.service' -> '/usr/lib/systemd/system/resolvconf.service'.
Created symlink '/etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.path' -> '/usr/lib/systemd/system/resolvconf-pull-resolved.path'.
Unit '/usr/lib/systemd/system/resolvconf-pull-resolved.path' is added as a dependency to a non-existent unit 'systemd-resolved.service'.
Created symlink '/etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.service' -> '/usr/lib/systemd/system/resolvconf-pull-resolved.service'.
Unit '/usr/lib/systemd/system/resolvconf-pull-resolved.service' is added as a dependency to a non-existent unit 'systemd-resolved.service'.
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différées (« triggers ») pour resolvconf (1.94) ...
```

Désactivation de la carte réseau enp0s3 à l'aide de la commande ifdown enp0s3

```
root@DS1: ~#ifdown enp0s3
sending signal ALRM to pid 674
waiting for pid 674 to exit
root@DS1: ~#
```

Modification à l'aide de l'éditeur Nano, le fichier /etc/network/interfaces pour l'interface enp0s3 et configuration IP de DHCP :

```
GNU nano 8.4 /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
auto enp0s3
iface enp0s3 inet dhcp
#address 10.1.1.
#netmask 255.0.0.0
#network 10.56.239.203
#broadcast 10.255.255.255
# This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto
```

```
GNU nano 8.4 /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
auto enp0s3
iface enp0s3 inet static
address 172.17.101.219
netmask 255.255.0.0
network 172.17.0.0
gateway 172.17.250.3
broadcast 172.17.255.255
dns-nameservers 172.17.254.1
# This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto
```

Réactivation de la carte réseau à l'aide de la commande `ifup enp0s3`

```
root@DS1: ~#ifup enp0s3
root@DS1: ~#
```

Vérification de la configuration IP à l'aide de la commande ip a

```
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 08:00:27:91:10:4d brd ff:ff:ff:ff:ff:ff
    altname enx08002791104d
    inet 172.17.101.219/16 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
```

Affichage du contenu du fichier /etc/resolv.conf à l'aide de la commande cat et vérification qu'il y a bien l'adresse IP du serveur DNS que l'on a configuré dans le fichier /etc/network/interfaces

```
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
nameserver 172.17.254.1
```

Consultation de la table de routage de DS1 à l'aide de la commande ip route, visualisation de la passerelle par défaut

```
root@DS1: ~#ip route
default via 172.17.250.3 dev enp0s3 onlink
172.17.0.0/16 dev enp0s3 proto kernel scope link src 172.17.101.219
```

Ping du serveur DNS roi (172.17.254.1) pour s'assurer de la bonne connectivité IP

```
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=1.43 ms
64 bytes from 172.17.254.1: icmp_seq=2 ttl=128 time=0.994 ms
64 bytes from 172.17.254.1: icmp_seq=3 ttl=128 time=1.62 ms
64 bytes from 172.17.254.1: icmp_seq=4 ttl=128 time=1.44 ms
^C
--- 172.17.254.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.994/1.372/1.621/0.230 ms
```

Vérification de l'accès à Internet ainsi que la résolution DNS à l'aide, des ping 8.8.8.8 et www.ac-nice.fr

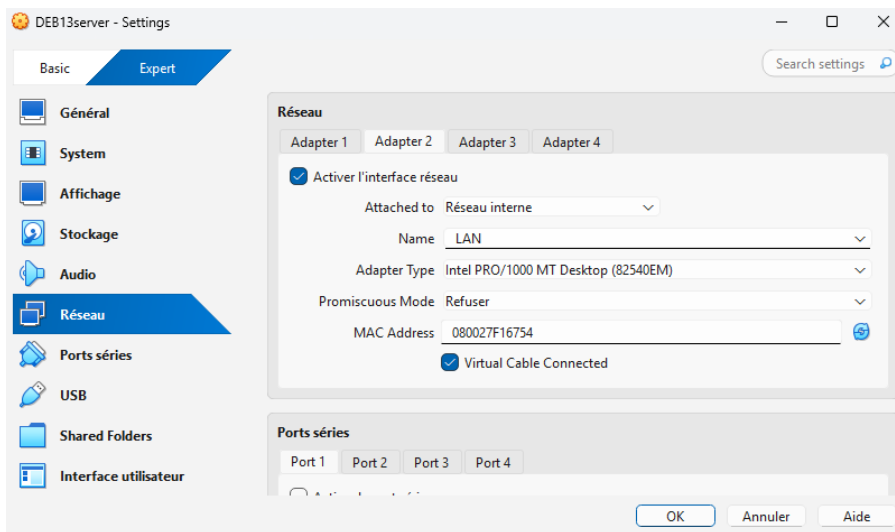
```
root@DS1: ~#ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=7.77 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=6.35 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=6.24 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=6.69 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 6.236/6.760/7.769/0.605 ms
root@DS1: ~#ping -c 4 www.ac-nice.fr
PING www.ac-nice.fr.cdn.cloudflare.net (141.101.90.107) 56(84) bytes of data.
64 bytes from 141.101.90.107: icmp_seq=1 ttl=53 time=21.1 ms
64 bytes from 141.101.90.107: icmp_seq=2 ttl=53 time=18.2 ms
64 bytes from 141.101.90.107: icmp_seq=3 ttl=53 time=17.2 ms
64 bytes from 141.101.90.107: icmp_seq=4 ttl=53 time=17.3 ms

--- www.ac-nice.fr.cdn.cloudflare.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3034ms
rtt min/avg/max/mdev = 17.237/18.441/21.050/1.550 ms
```

3. Ajout de l'interface enp0s8.

Arrêt de la machines et ajout d'une seconde carte réseaux depuis le gestionnaire des machines



Vérification de la prise en compte de la nouvelle carte enp0s8 à l'aide de la commande ip a

```
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 08:00:27:91:10:4d brd ff:ff:ff:ff:ff:ff
    altname enx08002791104d
    inet 172.17.101.219/16 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe91:104d/64 scope link dadfailed tentative proto kernel_ll
        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:f1:67:54 brd ff:ff:ff:ff:ff:ff
    altname enx080027f16754
```

Ajout de l'interface enp0s8 dans le fichiers /etc/network/interfaces

```
GNU nano 8.4 /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
auto enp0s3
iface enp0s3 inet static
address 172.17.101.219
netmask 255.255.0.0
network 172.17.0.0
gateway 172.17.250.3
broadcast 172.17.255.255
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
# This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto
```

Activation de la carte et vérifiez la bonne configuration réseau avec la commande ip a

```
root@DS1: ~#ifup enp0s8
root@DS1: ~#ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    altname enx08002791104d
    inet 172.17.101.219/16 brd 172.17.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    altname enx080027f16754
    inet 192.168.4.254/24 brd 192.168.4.255 scope global enp0s8
        valid_lft forever preferred_lft forever
```

Vérification de la bonne configuration réseau de la machine DS1 avec la commande ping sur ses deux interfaces

```
root@DS1: ~#ping -c 4 192.168.4.254
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=0.127 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.035 ms

--- 192.168.4.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.030/0.056/0.127/0.040 ms
root@DS1: ~#ping -c 4 172.17.101.219
PING 172.17.101.219 (172.17.101.219) 56(84) bytes of data.
64 bytes from 172.17.101.219: icmp_seq=1 ttl=64 time=0.075 ms
64 bytes from 172.17.101.219: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 172.17.101.219: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 172.17.101.219: icmp_seq=4 ttl=64 time=0.030 ms

--- 172.17.101.219 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3065ms
rtt min/avg/max/mdev = 0.030/0.043/0.075/0.018 ms
root@DS1: ~#
```

Affichage de la table de routage de DS1

```
root@DS1: ~#ip route
default via 172.17.250.3 dev enp0s3 onlink
172.17.0.0/16 dev enp0s3 proto kernel scope link src 172.17.101.219
192.168.4.0/24 dev enp0s8 proto kernel scope link src 192.168.4.254
root@DS1: ~#_
```

4. Transformation du serveur en routeur.

Utilisation de la commande `echo > /proc/sys/net/ipv4/ip_forward` pour que la valeur dans le fichier `ip_forward` soit 1 et pas 0 par défaut afin d'activer le routage

```
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 création dans le répertoire `/etc/sysctl.d/` un fichier nommé `sysctl.conf` comportant la ligne `net.ipv4.ip_forward=1`

```
GNU nano 8.4 /etc/sysctl.d/sysctl.conf
net.ipv4.ip_forward=1
```

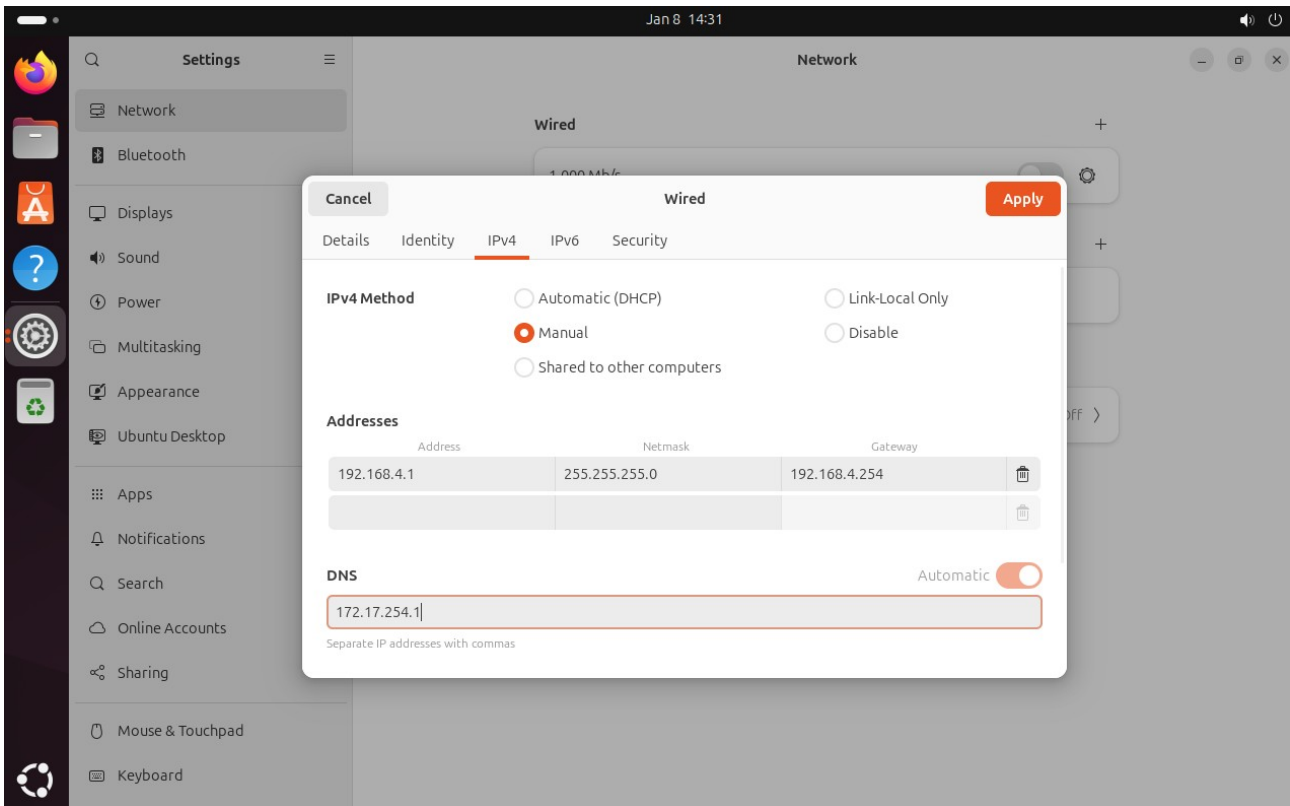
Redémarrage de la machine avec la commande `reboot` et vérification que le routage soit bien mis en place

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

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

Récupération de l'iso `ubuntu-24.04.1-desktop-amd64` et création de la VM UD1

Sélection du mode d'accès 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

```
root@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 08:00:27:1e:c0:78 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
```

Consultation de la table de routage de UD1 et plus particulièrement la route par défaut et la passerelle à l'aide de la commande ip route

```
root@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
```

Ping depuis le client Linux des deux interfaces du serveur DS1 afin de vérifier la connectivité entre les deux machines ainsi que le bon fonctionnement du routage

```
root@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=0.692 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.753 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=1.19 ms

--- 192.168.4.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2136ms
rtt min/avg/max/mdev = 0.692/0.877/1.188/0.220 ms
root@UD1:~# ping -c 3 172.17.101.219
PING 172.17.101.219 (172.17.101.219) 56(84) bytes of data.
64 bytes from 172.17.101.219: icmp_seq=1 ttl=64 time=0.678 ms
64 bytes from 172.17.101.219: icmp_seq=2 ttl=64 time=0.623 ms
64 bytes from 172.17.101.219: icmp_seq=3 ttl=64 time=0.870 ms

--- 172.17.101.219 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2069ms
rtt min/avg/max/mdev = 0.623/0.723/0.870/0.105 ms
```

Ping du serveur ROI (172.17.254.1)

Que constatez-vous ? Le ping ne fonctionne pas

Quelle en est la raison ? La raison est que le paquet de ping arrive bien jusqu'au routeur Stormshield mais il ne renvoie aucune réponse. Comme l'ICMP n'est pas autorisé sur ses interfaces le routeur ne renvoie pas d'Echo Reply, donc ça explique l'absence de retour.

```
root@UD1:~# ping -c1 172.17.254.1
PING 172.17.254.1 (172.17.254.1) 56(84) bytes of data.

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

6. Configuration du NAT sur le serveur DS1.

Installation du paquet iptables à l'aide de la commande apt-get install 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
Les paquets supplémentaires suivants seront installés :
  libip4tc2 libip6tc2 libnetfilter-contrack3 libnfnetlink0
Paquets suggérés :
  firewalld
Les NOUVEAUX paquets suivants seront installés :
  iptables libip4tc2 libip6tc2 libnetfilter-contrack3 libnfnetlink0
0 mis à jour, 5 nouvellement installés, 0 à enlever et 30 non mis à jour.
Il est nécessaire de prendre 458 kB dans les archives.
Après cette opération, 2 799 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o_
```

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 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
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source      destination
  1    60 MASQUERADE  all  --  any    enp0s3  192.168.4.0/24  anywhere
```

Afin que la translation d'adresses NAT soit activée à chaque démarrage, On installe 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
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 30 non mis à jour.
Il est nécessaire de prendre 18,5 kB dans les archives.
Après cette opération, 96,3 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o_
```

```
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 iptables-save(8) pour connaître la manière de garder à jour le fichier des règles.

Faut-il enregistrer les règles IPv6 actuelles ?
<Oui>                                     <Non>
```

On relance le système (commande reboot) et on vérifie 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 4 packets, 1146 bytes)
 pkts bytes target      prot opt in     out     source destination
Chain INPUT (policy ACCEPT 2 packets, 612 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
```

On vérifie le bon fonctionnement du routage et de la translation d'adresse NAT à partir du client Ubuntu en pinguant le serveur ROI (172.17.254.1)

```
root@UD1:~# 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=127 time=1.55 ms
64 bytes from 172.17.254.1: icmp_seq=2 ttl=127 time=1.63 ms
64 bytes from 172.17.254.1: icmp_seq=3 ttl=127 time=1.96 ms
64 bytes from 172.17.254.1: icmp_seq=4 ttl=127 time=2.04 ms
^C
--- 172.17.254.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3020ms
rtt min/avg/max/mdev = 1.550/1.792/2.035/0.207 ms
```

Installation sur DS1 du paquet tcpdump à l'aide de la commande apt-get install 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 :
 libpcap0.8t64
Les NOUVEAUX paquets suivants seront installés :
 libpcap0.8t64 tcpdump
0 mis à jour, 2 nouvellement installés, 0 à enlever et 30 non mis à jour.
Il est nécessaire de prendre 640 kB dans les archives.
Après cette opération, 1 775 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
```

```
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
16:44:44.469296 IP 172.17.101.219 > 172.17.254.1: ICMP echo request, id 9140, seq 1, length 64
16:44:44.470098 IP 172.17.254.1 > 172.17.101.219: ICMP echo reply, id 9140, seq 1, length 64
16:44:45.472933 IP 172.17.101.219 > 172.17.254.1: ICMP echo request, id 9140, seq 2, length 64
16:44:45.474413 IP 172.17.254.1 > 172.17.101.219: ICMP echo reply, id 9140, seq 2, length 64
16:44:46.481193 IP 172.17.101.219 > 172.17.254.1: ICMP echo request, id 9140, seq 3, length 64
16:44:46.482324 IP 172.17.254.1 > 172.17.101.219: ICMP echo reply, id 9140, seq 3, length 64
16:44:47.489295 IP 172.17.101.219 > 172.17.254.1: ICMP echo request, id 9140, seq 4, length 64
16:44:47.490124 IP 172.17.254.1 > 172.17.101.219: ICMP echo reply, id 9140, seq 4, length 64
```

Réalisation d'un test en ouvrant le navigateur afin de vérifier la possibilité d'aller, par exemple, sur le site de l'Académie de Nice

