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

1. Rappels.

- Récupérez la dernière liste des paquets disponibles :

  root@DS1:~# **apt-get update**

- 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** :

```
  GNU nano 2.7.4                          Fichier : .bashrc

# ~/.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 --color=auto'
# 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'
```

- 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**.

2. Configuration réseau du serveur DS1.

- Vérifiez la configuration réseau actuelle (mode d'accès réseau **NAT**).

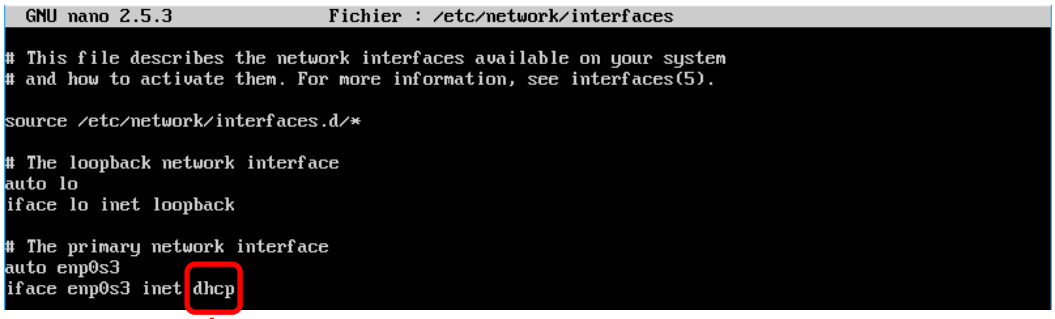
```
root@US5:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:99:15:1c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe99:151c/64 scope link
       valid_lft forever preferred_lft forever
root@US5:~#
```

- Modifiez le mode d'accès réseau : **Accès par pont**.
- Désactivez la carte réseau enp0s3 avant de spécifier une adresse IP fixe :

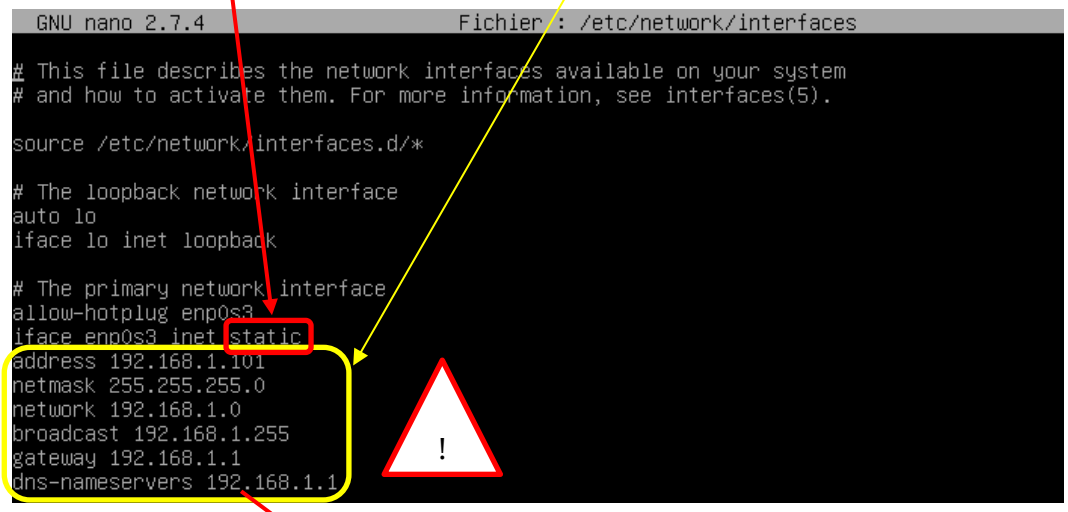
```
root@US5:~# ifdown enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:99:15:1c
Sending on   LPF/enp0s3/08:00:27:99:15:1c
Sending on   Socket/fallback
DHCPRELEASE on enp0s3 to 10.0.2.2 port 67 (xid=0x7be02f16)
root@US5:~# _
```

Rappel : vous utilisez les commandes **ifdown enp0s3** et **ifup enp0s3** pour prendre en compte les modifications de la configuration IP de la carte enp0s3 (commande **ifdown** à utiliser avant la modification du fichier **interfaces** lorsque la carte est configurée en dhcp et que l'on veut passer en IP fixe).

- 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 :

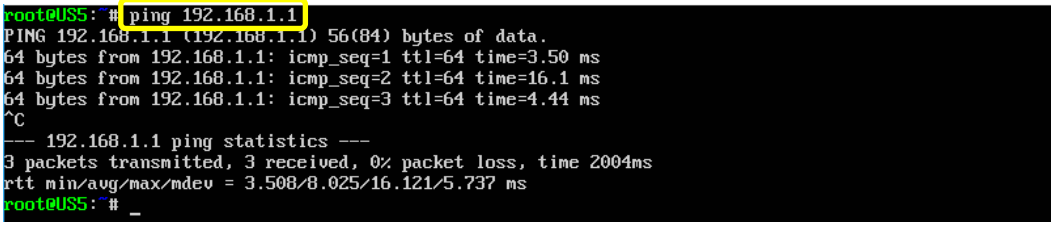


@IP fixe cohérente avec le réseau SIO 172.17.101.201→224 /16 (@ Réseau : 172.17.0.0/16) GW : 172.17.250.2 (Routeur Cisco) ; DNS : 172.17.254.1 (serveur ROI)



- Réactivez la carte réseau (**ifup enp0s3**) et vérifiez la configuration IP (**ip a**). Effectuez une capture d'écran.
- 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.
- Consultez la table de routage de DS1 (visualisez la prise en compte de la passerelle par défaut 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 :



- 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=122 time=26.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=122 time=27.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=122 time=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=122 time=26.6 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 26.660/26.838/27.097/0.177 ms
root@DS1 ~ #ping -c 4 www.ac-nice.fr
PING mars.ac-nice.fr (194.167.84.155) 56(84) bytes of data.
64 bytes from mars.ac-nice.fr (194.167.84.155): icmp_seq=1 ttl=49 time=51.2 ms
64 bytes from mars.ac-nice.fr (194.167.84.155): icmp_seq=2 ttl=49 time=50.7 ms
64 bytes from mars.ac-nice.fr (194.167.84.155): icmp_seq=3 ttl=49 time=51.2 ms
64 bytes from mars.ac-nice.fr (194.167.84.155): icmp_seq=4 ttl=49 time=51.2 ms

--- mars.ac-nice.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 50.789/51.130/51.273/0.255 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@US5:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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 1
000
    link/ether 08:00:27:99:15:1c 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 2a01:cb1d:5b:1900:a00:27ff:fe99:151c/64 scope global mngtmpaddr dynamic
       valid_lft 1781sec preferred_lft 581sec
    inet6 fe80::a00:27ff:fe99:151c/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 08:00:27:26:7b:d4 brd ff:ff:ff:ff:ff:ff
root@US5: # _
```

- Ajoutez l'interface **enp0s8** dans le fichier **/etc/network/interfaces**. @IP fixe : 192.168.4.254 /24.

```
# 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 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 08:00:27:8d:1c:99 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 2a01:cb1d:490:1500:a00:27ff:fe8d:1c99/64 scope global dynamic mngtmpaddr
       valid_lft 86347sec preferred_lft 547sec
    inet6 fe80::a00:27ff:fe8d:1c99/64 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 100
0
    link/ether 08:00:27:05:10:40 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:fe05:1040/64 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=0.082 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 192.168.4.254: icmp_seq=4 ttl=64 time=0.067 ms
^C
--- 192.168.4.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3091ms
rtt min/avg/max/mdev = 0.041/0.058/0.082/0.016 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=0.038 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=0.066 ms

--- 192.168.1.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3105ms
rtt min/avg/max/mdev = 0.038/0.045/0.066/0.011 ms
root@DS1: ~#_
```

172.17.101.201→224

- 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.

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

```
  GNU nano 7.2                                /etc/sysctl.conf *

# 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
```

- 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: ~#_
```

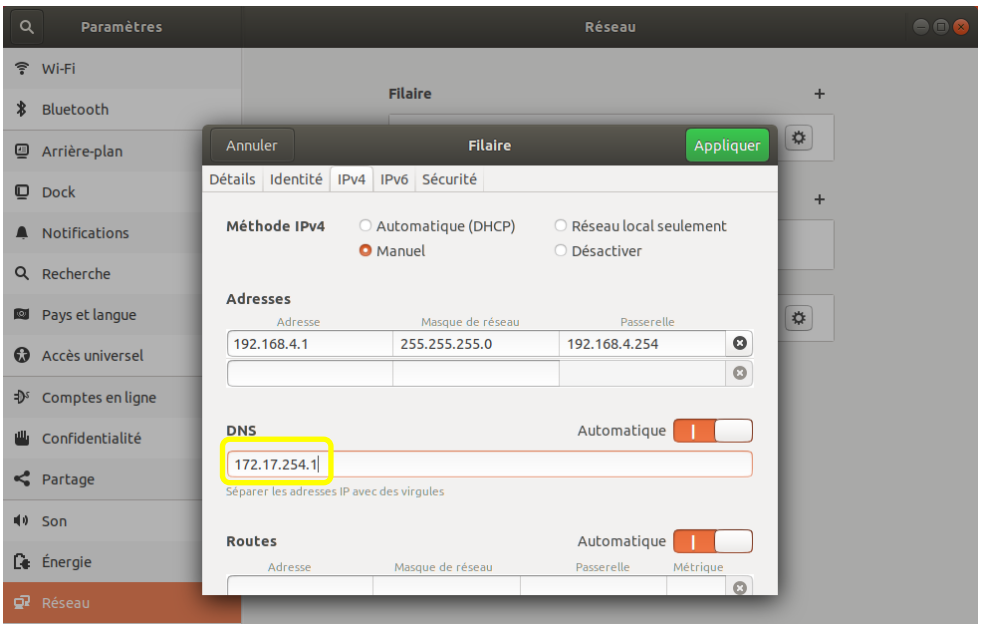
5. Configuration du poste client Ubuntu (Desktop 24.04 LTS).

- Téléchargez l'iso ubuntu-24.04.1-desktop-amd64 et créez la VM UD1.

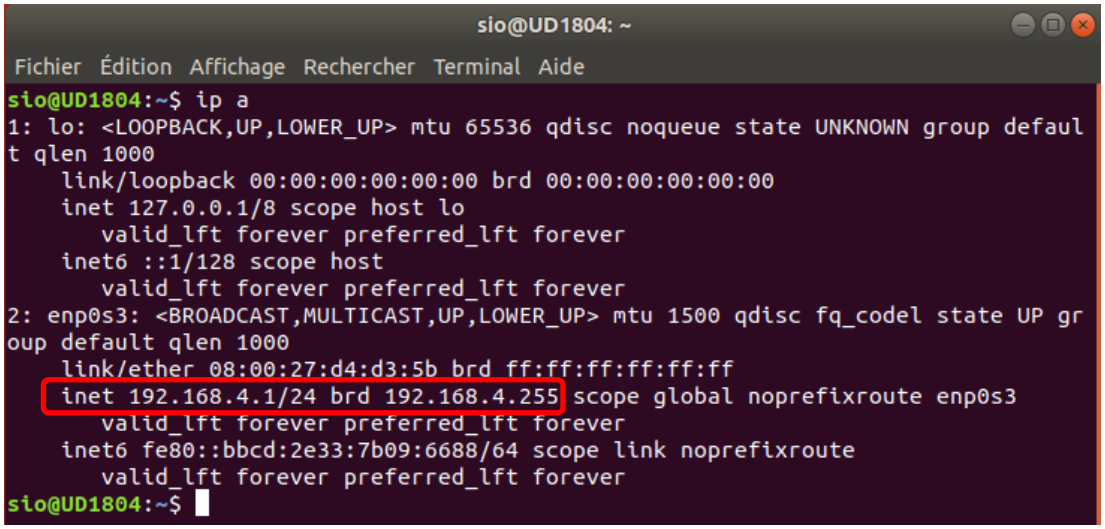
  https://ubuntu.com/download/desktop

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

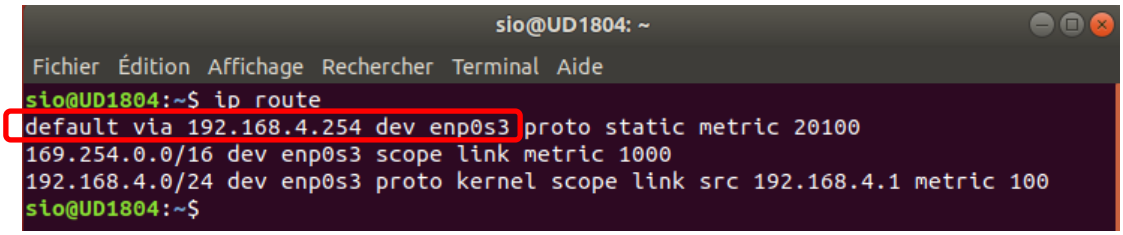
  @IP : 192.168.4.1/24 ; GW : 192.168.4.254 (IP de la carte enp0s8 de DS1)
  DNS : 172.17.254.1 (à la maison : @ de la box)



- Vérifiez la configuration IP de la carte réseau d'UD1 :



- 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**.



- 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@UD1804: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
sio@UD1804:~$ 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=0.417 ms
64 bytes from 192.168.4.254: icmp_seq=2 ttl=64 time=0.236 ms
64 bytes from 192.168.4.254: icmp_seq=3 ttl=64 time=0.345 ms

--- 192.168.4.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2064ms
rtt min/avg/max/mdev = 0.236/0.332/0.417/0.077 ms
sio@UD1804:~$ 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=0.345 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.406 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.411 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.345/0.387/0.411/0.034 ms
sio@UD1804:~$
```

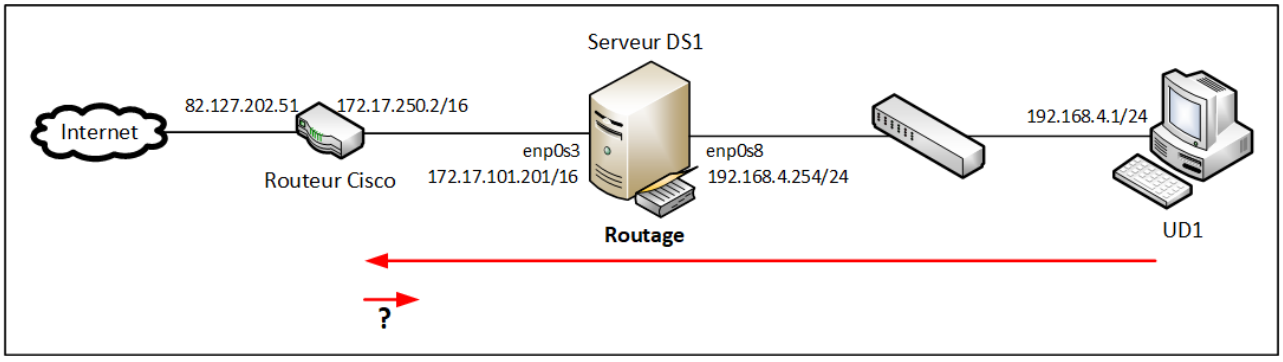
172.17.101.201→224

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

  Que constatez-vous ? _____

  Quelle en est la raison ? _____

```
sio@UD1804: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
sio@UD1804:~$ 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@UD1804:~$
```



6. Configuration du NAT sur le serveur DS1.

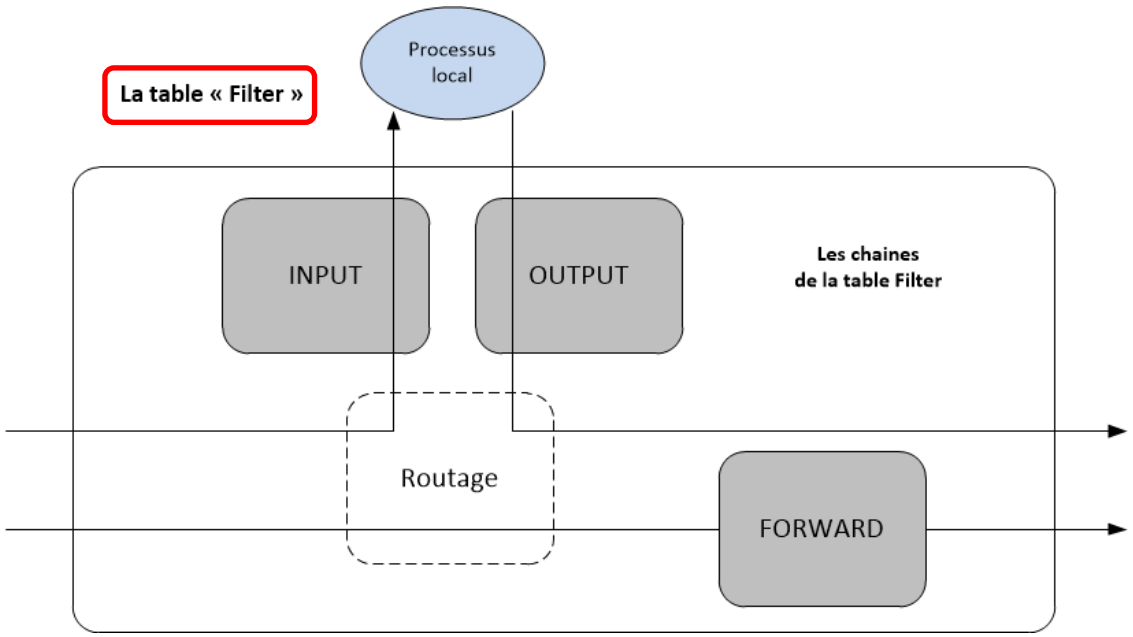
Votre client UD1 ne peut pas encore communiquer avec l'extérieur. Il faut paramétrer le serveur DS1 pour faire de la **translation d'adresses** (NAT).

Vous allez mettre en place le NAT via le pare-feu **Netfilter**. Trois interfaces en ligne de commande permettent de configurer ce dernier : **UFW**, **iptables et nftables**. Vous utiliserez **iptables**.

Présentation d'iptables :

Le pare-feu **Netfilter/iptables** implémente un routeur filtrant. Il permet ainsi de filtrer les paquets en les autorisant ou en les bloquant (table **Filter**). Il permet également de faire de la translation d'adresses (table **Nat**) : NAT dynamique (modification de l'IP source en sortie) et NAT statique appelé également redirection (modification de l'IP destination en entrée).

- **Les concepts de tables, chaînes et règles**



- **Les chaînes et les règles :**

Une chaîne est composée d'une **pile de règles** (cf. schéma ci-après). Chaque règle d'une chaîne est composée de deux parties : un **critère** et une **politique**. Le critère précise les cas d'application. La politique précise l'action accomplie.

✓ **Exemple 1** : la chaîne **INPUT** est composée des **règles qui filtrent les paquets destinés aux processus locaux**. Une des règles peut avoir comme critère la provenance du paquet, par exemple le serveur DNS, et comme politique l'acceptation du paquet :

iptables -A INPUT -p udp -s 172.17.254.1 --sport 53 -j ACCEPT

La commande iptables ci-dessus ajoute une règle à la fin de la chaîne **INPUT**. Cette règle autorise les datagrammes udp provenant de la machine 172.17.254.1 ayant comme port source le port 53. Ces paquets pourront être transmis aux applications locales.

✓ **Exemple 2** : la commande **iptables** ci-dessous interdit l'accès au service telnet au poste 192.168.0.2 via la carte enp0s3.

iptables -A INPUT -p tcp -s 192.168.0.2 --dport 23 -i enp0s3 -j DROP

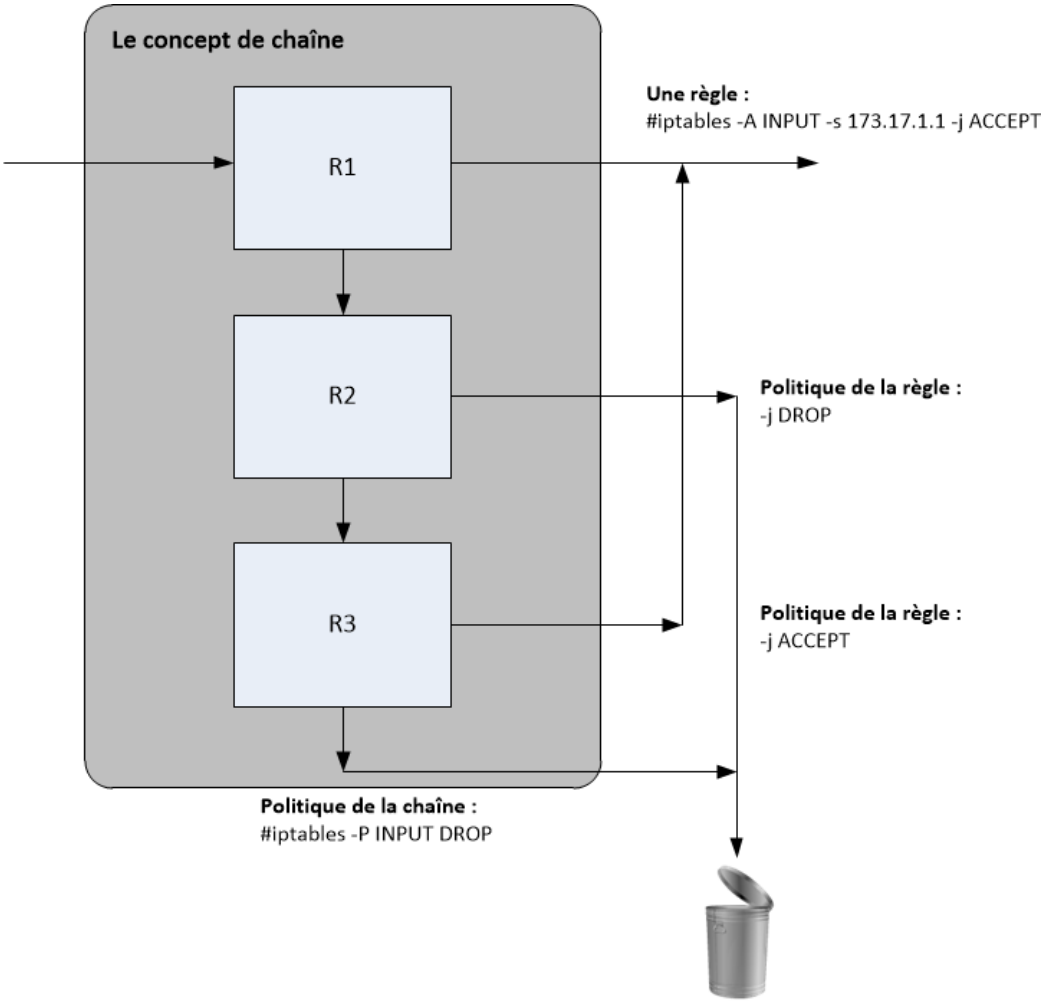
- ✓ **Exemple 3** : les commandes **iptables** ci-dessous autorisent le service Web.

  iptables -A INPUT -p tcp --dport 80 -j ACCEPT

  iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

Si le critère ne s'applique pas au paquet, on examine la règle suivante de la chaîne. Si aucune règle ne s'applique au paquet, on exécute la **politique associée à la chaîne**. Cette dernière pourrait être par exemple de rejeter le paquet :

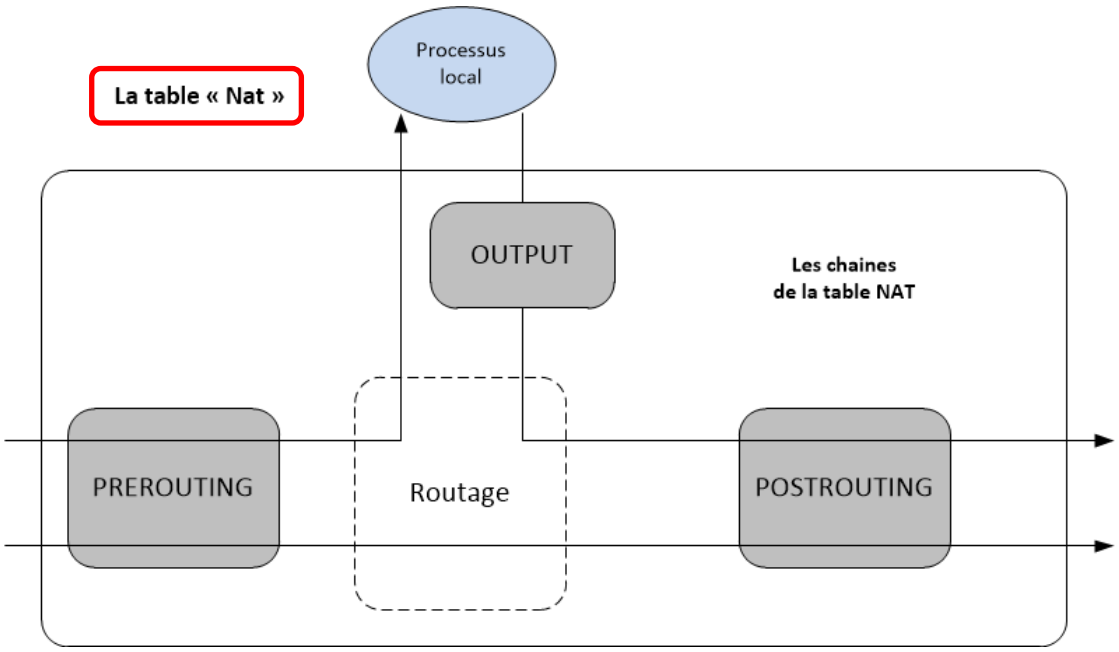
iptables -P INPUT DROP



- Les tables :

Les chaînes gérées par Netfilter sont incluses dans des entités plus vastes appelées « **table** ». Chaque table correspond aux différentes possibilités d'iptables :

- ✓ La table **filter** filtre les paquets IP. Elle est constituée des chaînes **INPUT**, **OUTPUT** et **FORWARD** ;
- ✓ La table **nat** effectue le NAT (NAT dynamique et redirection). Elle est constituée essentiellement des chaînes **PREROUTING** et **POST-ROUTING**.



- **Les différentes chaînes prédéfinies**
  - **INPUT** : les paquets destinés aux processus locaux passent par la chaîne INPUT.
  - **OUTPUT** : les paquets réseaux issus des processus locaux passent par la chaîne OUTPUT.
  - **FORWARD** : les paquets en transit provenant d'un réseau et destinés à un autre réseau passent par la chaîne FORWARD.
  - **PREROUTING** : la chaîne PREROUTING modifie un paquet dès qu'il **entre** dans le système **avant qu'il ne soit routé**.
  - **POSTROUTING** : la chaîne POSTROUTING modifie un paquet juste avant sa **sortie** du système **après être passée par le module de routage**.

- **Masquerading**

  Le masquerading est réalisé grâce à la table **nat** qui manipule les chaînes PREROUTING et POSTROUTING grâce aux politiques SNAT, DNAT et MASQUERADE.

  ✓ **La politique SNAT**
  La politique SNAT n'est valable que pour la table **nat** et la chaîne **POSTROUTING**. L'adresse IP source du paquet est modifiée.

  ✓ **La politique DNAT**
  La politique DNAT n'est valable que pour la table **nat** et les chaînes **PREROUTING** et **OUTPUT**. L'adresse IP de destination du paquet est modifiée.

  ✓ **La politique MASQUERADE**
  La politique MASQUERADE n'est valable que pour la table **nat** dans la chaîne **POSTROUTING**. Comme pour SNAT, l'adresse source du paquet est modifiée.

Exemple de NAT : tous les paquets destinés au réseau externe seront « masqueradés », c'est-à-dire qu'ils auront l'apparence de provenir du pare-feu car leur adresse IP source sera remplacée par celle de la carte enp0s3 dite **outside** (celle qui relie le pare-feu au réseau externe).

```
echo 1 > /proc/sys/net/ipv4/ip_forward        # Routage
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE      # Translation d'adresse
```

Exemple de redirection : on veut transférer les requêtes Web provenant de l'extérieur vers le serveur interne Web 172.16.0.100.

iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j DNAT --to 172.16.0.100:80

- Installez le paquet **iptables** à l'aide de la commande **apt-get install** iptables.
- 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: ~#_
```

-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.

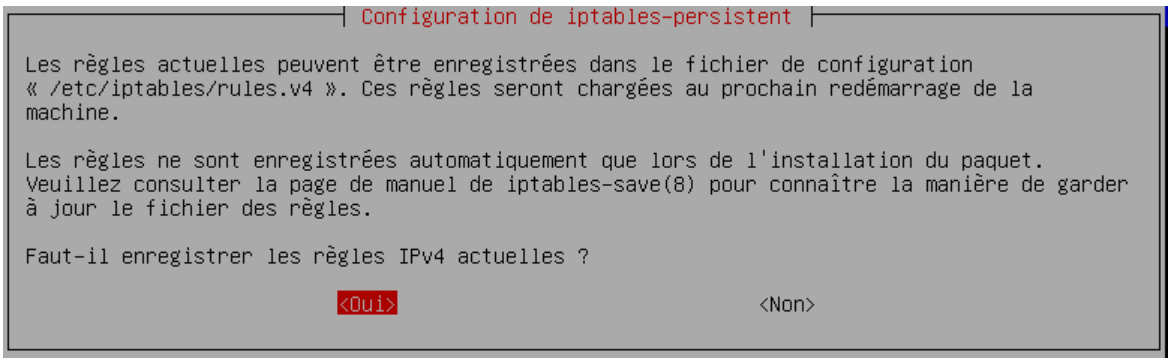
- Vérifiez la bonne prise en compte de la règle par **iptables -t nat -L -v** :

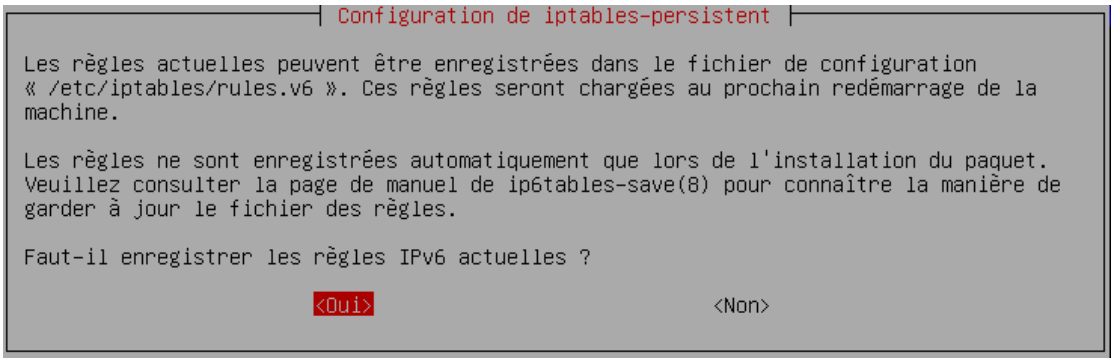
```
root@DS1: ~#iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain 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: ~#
```

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

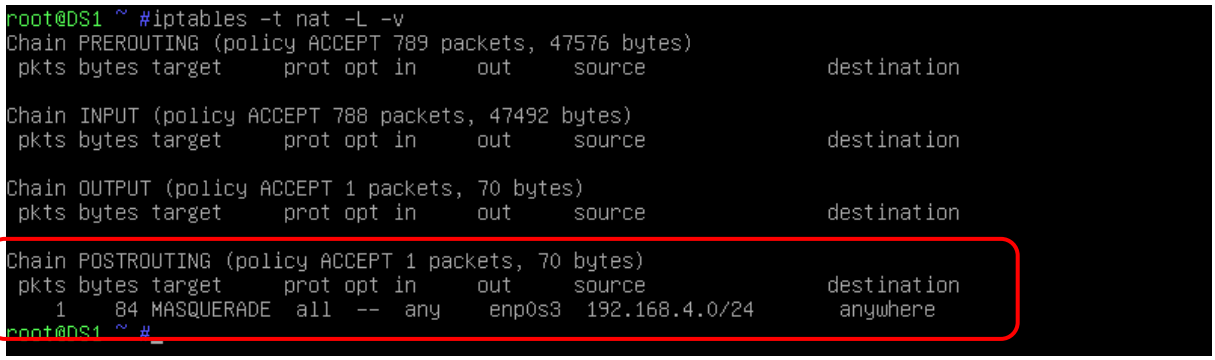
```
root@DS1 ~ #apt-get install iptables-persistent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
The following additional packages will be installed:
  netfilter-persistent
Les NOUVEAUX paquets suivants seront installés :
  iptables-persistent netfilter-persistent
0 mis à jour, 2 nouvellement installés, 0 à enlever et 9 non mis à jour.
Il est nécessaire de prendre 19,5 ko dans les archives.
Après cette opération, 79,9 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

Pendant, l'installation du paquet, on vous demande si vous souhaitez que les règles actuellement en cours d'utilisation (celle saisie ci-dessus en l'occurrence) soient enregistrées dans les fichiers de configuration **/etc/iptables/rules.v4** et **/etc/iptables/rules.v6.** Répondez **oui.**

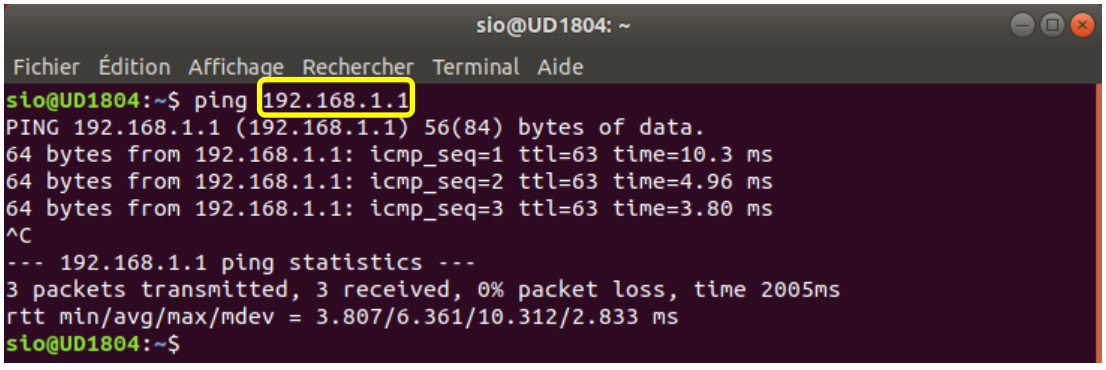




- Relancez le système (commande **reboot**) et vérifiez à nouveau l'existence de la règle NAT à l'aide de la commande **iptables -t nat –L** :



- Vérifiez le bon fonctionnement du routage et de la translation d'adresse NAT à partir du client Ubuntu en pinguant la passerelle (routeur Cisco 172.17.250.2). Contrairement à votre ping de la page 7, vous devez maintenant recevoir la trame ICMP Echo reply :



- 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
The following additional packages will be installed:
  libpcap0.8
Les NOUVEAUX paquets suivants seront installés :
  libpcap0.8 tcpdump
0 mis à jour, 2 nouvellement installés, 0 à enlever et 9 non mis à jour.
Il est nécessaire de prendre 553 ko dans les archives.
Après cette opération, 1 553 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 (172.17.101.201→224).

```
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
23:51:30.628375 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 1894, seq 1, length 64
23:51:30.632806 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 1894, seq 1, length 64
23:51:31.629994 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 1894, seq 2, length 64
23:51:31.634776 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 1894, seq 2, length 64
23:51:32.641168 IP 192.168.1.101 > 192.168.1.1: ICMP echo request, id 1894, seq 3, length 64
23:51:32.646120 IP 192.168.1.1 > 192.168.1.101: ICMP echo reply, id 1894, seq 3, 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
23:54:06.413553 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 1897, seq 1, length 64
23:54:06.418565 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 1897, seq 1, length 64
23:54:07.426323 IP 192.168.4.1 > 192.168.1.1: ICMP echo request, id 1897, seq 2, length 64
23:54:07.430696 IP 192.168.1.1 > 192.168.4.1: ICMP echo reply, id 1897, seq 2, 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.
- Lancez le navigateur et vérifiez la possibilité d'aller sur internet (effectuez une capture d'écran).