

Travaux Pratiques R&T 1^{ère} année

Durée : 3 heures

SAE21 - Routage et NAT sous Linux avec iptables



Noms : LAURET Alexis

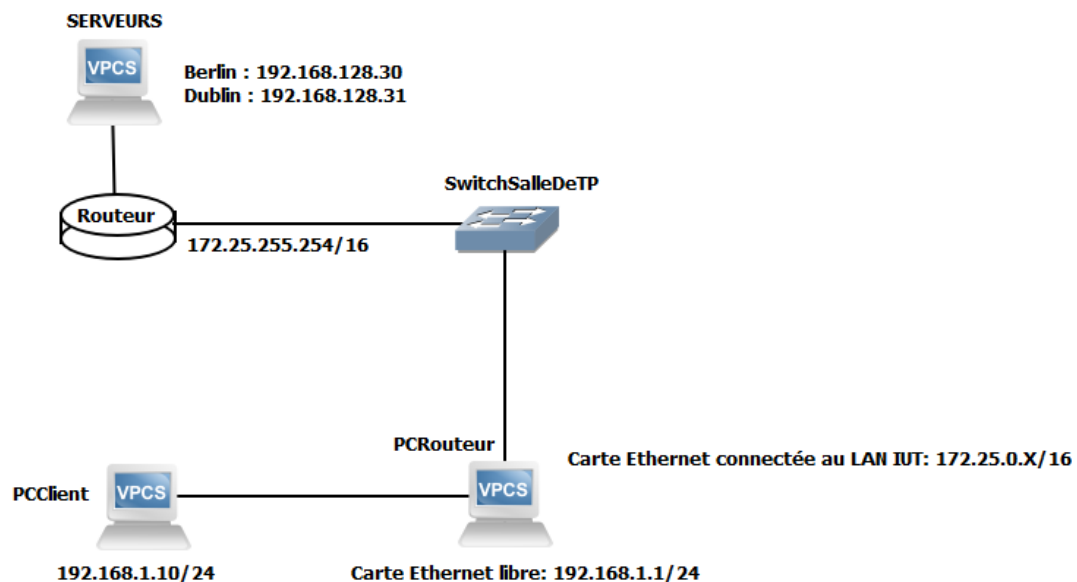
Groupe : tda

Date :

OBJECTIFS - TOPOLOGIE

Mise en œuvre de la fonctionnalité de translation d'adresse avec iptables sous Linux.

Vous utiliserez deux machines sous **Linux Debian** selon la topologie suivante :

**QUESTIONS THEORIQUES**

1. Expliquez le principe de fonctionnement du NAT (translation d'adresse) et du PAT (translation de ports).

NAT : Le nat (translation d'adresse) permet à un routeur de convertir une adresse IP en une autre. Il à été inventé pour appoter une réponse à la future pénurie ipv4.

PAT : Permet de transformer un numéro de port en un autre.

2. Présentez l'outil iptables et son fonctionnement en quelques lignes.

C'est un logiciel libre de l'espace utilisateur linux grâce auquel l'administrateur système peut configurer les chaînes et des règles de par-feu. On peut également y faire de la translation d'adresse ainsi que de la translation de port.

MANIPULATIONS

Pour l'ensemble des questions suivantes vous décrirez votre façon de procéder dans votre compte rendu de TP.

1. Activez l'ip forwarding sur le PC-Routeur. Qu'apporte cette manipulation ?

On active l'ip_forwarding avec `echo 1 > /proc/sys/net/ipv4/ip_forward` :

```
root@iutclrtc714:~# cat /proc/sys/net/ipv4/ip_forward
1
```

Cette manipulation permet de faire communiquer les deux cartes Ethernet du Pc pour qu'il puisse échanger des paquets. Elle va permettre au pc de faire du routage entre les deux cartes ?

On branche un pc au routeur. On débranche un des pc du réseau de la salle qui deviendra notre pc client, l'autre ayant deux interfaces occupée, sera le pc routeur.

Voici un schéma du réseaux :

[photo]

On configure l'interfaces du pc routeur avec 'ip a add' :

```
root@iutclrtc714:~# ip a add 192.168.1.1/24 dev enp2s0
```

```
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 0.0.0.0
    ether b4:96:91:cb:3c:49 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 1104 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x6e800000-6e8fffff
```

On effectue les mêmes commandes avec le pc client (son ip est public)

On oublie d'affecter une route par défaut au pc client vers 192,168,1,1

2. Peut-on communiquer à partir du PC client avec le routeur 172.25.255.254, pourquoi ?
Quelles solutions sont possibles pour que cela fonctionne ?

Non car aucune routes n'est configurer sur le pc routeur, par conséquent, le pc client ne sait par ou envoyer ces paquets. De plus le routeur n'a pas probablement par la route pour pouvoir répondre.

3. Affichez la configuration iptables par défaut et l'expliquer.

On effectue la commande iptables -L :

```
root@iutclrtc714:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@iutclrtc714:~# █
```

On peut voir qu'aucune règle n'est définie ce qui est normal car on vient de configurer ip_forward et aucune règle n'a été définie.

4. Configurez le NAT avec iptables sur le PC Routeur pour permettre au PC client de communiquer avec le réseau extérieur (par exemple naviguer sur internet). Expliquer.

On effectue la commande suivant en relevant bien l'interface vers le réseau de l'iut :

```
root@iutclrtc714:~# iptables -t nat -A POSTROUTING -o enp0s31f6 -j MASQUERADE
```

On fait bien attention de renseigner l'interface connecter au réseau de la salle
Cette commande permet au Pc routeur de 'cacher' l'ip 172.25.0.X devant l'ip 192.168.1.10

5. Faites une capture Wireshark sur le PC Routeur pendant que le PC client génère du trafic sur internet. Observez et commentez ce qu'il se passe au niveau des adresses IP.

9104	247.842261051	172.25.0.74	8.8.8.8	ICMP	98 Echo (ping) request	id=0xf282, seq=1/256, ttl=63 (reply in 9105)
9105	247.851440995	8.8.8.8	172.25.0.74	ICMP	98 Echo (ping) reply	id=0xf282, seq=1/256, ttl=111 (request in 9104)
9108	248.843649996	172.25.0.74	8.8.8.8	ICMP	98 Echo (ping) request	id=0xf282, seq=2/512, ttl=63 (reply in 9109)
9109	248.852392816	8.8.8.8	172.25.0.74	ICMP	98 Echo (ping) reply	id=0xf282, seq=2/512, ttl=111 (request in 9108)
9110	249.844768179	172.25.0.74	8.8.8.8	ICMP	98 Echo (ping) request	id=0xf282, seq=3/768, ttl=63 (reply in 9111)
9111	249.853504087	8.8.8.8	172.25.0.74	ICMP	98 Echo (ping) reply	id=0xf282, seq=3/768, ttl=111 (request in 9110)
9113	250.846528150	172.25.0.74	8.8.8.8	ICMP	98 Echo (ping) request	id=0xf282, seq=4/1024, ttl=63 (reply in 9114)
9114	250.855933022	8.8.8.8	172.25.0.74	ICMP	98 Echo (ping) reply	id=0xf282, seq=4/1024, ttl=111 (request in 9113)

On observe que l'adresse source change car j'ai fait un ping vers google depuis mon pc en 192.168.1.10 mais l'adresse destination est celle du routeur

6. Installer un serveur Web (apache2) et un serveur FTP (vsftpd) sur le PC-client.

On installe le serveur :

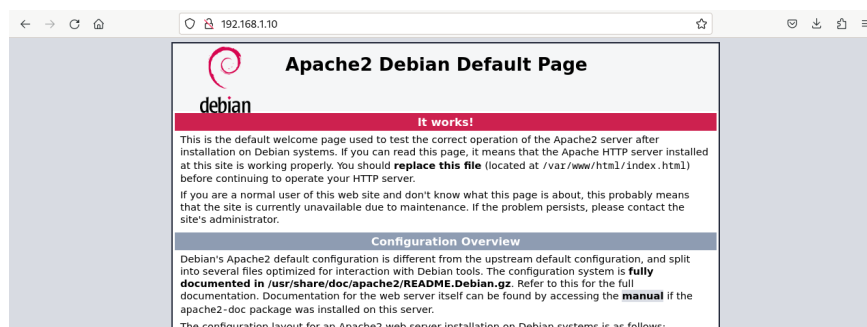
```
$apt update
```

```
$apt install apache2 vsftpd
```

Sur le serveur on créer un utilisateur du nom de 'bond' et on se connecte sur le routeur :

```
root@iutclrtc714:~# ftp bond@192.168.1.10
Connected to 192.168.1.10.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
 229 Entering Extended Passive Mode (|||46725|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> exit
221 Goodbye.
```

De même on tente de se connecter sur le routeur au serveur apache (on entre l'ip du serveur dans un navigateur) :



7. Nous souhaitons pouvoir accéder au site internet hébergé sur le PC client et à son serveur FTP à partir de n'importe quel poste de la salle. Configurer iptables pour que cela soit fonctionnel. Testez votre configuration.

On effectue les commandes suivantes :

```
iptables -t nat -A PREROUTING -p tcp -d 172.25.0.74 --dport 80 -j DNAT --to-destination 192.168.1.10
iptables -t nat -A PREROUTING -p tcp -d 172.25.0.74 --dport 21 -j DNAT --to-destination 192.168.1.10
```

Sur un autre pc on tape l'ip du pc routeur (externe) sur un navigateur :



et on tente de se connecter en ftp :

```
root@iutclrtc712:~# ftp bond@172.25.0.74
Connected to 172.25.0.74.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
```

On a bien entrée l'ip externe du routeur pour accéder à l'interface

8. Observez le comportement de cette connexion réseau avec Wireshark

Connexion ftp :

349	273.610735430	192.168.1.10	172.25.0.72	FTP	86 Response: 220 (vsFTpd 3.0.3)
351	273.611315380	172.25.0.72	192.168.1.10	FTP	77 Request: USER bond
353	273.611895405	192.168.1.10	172.25.0.72	FTP	100 Response: 331 Please specify the password.
357	280.374081237	172.25.0.72	192.168.1.10	FTP	79 Request: PASS 123456
358	280.403436402	192.168.1.10	172.25.0.72	FTP	89 Response: 230 Login successful.
360	280.404225850	172.25.0.72	192.168.1.10	FTP	72 Request: SYST
361	280.404624455	192.168.1.10	172.25.0.72	FTP	85 Response: 215 UNIX Type: L8
362	280.405453887	172.25.0.72	192.168.1.10	FTP	72 Request: FEAT
363	280.406090055	192.168.1.10	172.25.0.72	FTP	81 Response: 211-Features:
364	280.406090321	192.168.1.10	172.25.0.72	FTP	87 Response: EPRT
365	280.406090391	192.168.1.10	172.25.0.72	FTP	110 Response: PASV

Pour la connexion http :

251	142.665993906	172.25.0.70	192.168.1.10	HTTP	430 GET / HTTP/1.1
253	142.668225641	192.168.1.10	172.25.0.70	HTTP	3446 HTTP/1.1 200 OK (text/html)
255	142.719587940	172.25.0.70	192.168.1.10	HTTP	391 GET /icons/openlogo-75.png HTTP/1.1
256	142.721055972	192.168.1.10	172.25.0.70	HTTP	6106 HTTP/1.1 200 OK (PNG)
258	142.727111127	172.25.0.70	192.168.1.10	HTTP	381 GET /favicon.ico HTTP/1.1
259	142.728146841	192.168.1.10	172.25.0.70	HTTP	555 HTTP/1.1 404 Not Found (text/html)
269	159.728068589	172.25.0.72	192.168.1.10	HTTP	430 GET / HTTP/1.1
271	159.730915863	192.168.1.10	172.25.0.72	HTTP	3446 HTTP/1.1 200 OK (text/html)
273	159.795552493	172.25.0.72	192.168.1.10	HTTP	391 GET /icons/openlogo-75.png HTTP/1.1
274	159.796853387	192.168.1.10	172.25.0.72	HTTP	6106 HTTP/1.1 200 OK (PNG)
276	159.801003548	172.25.0.72	192.168.1.10	HTTP	381 GET /favicon.ico HTTP/1.1
277	159.802075597	192.168.1.10	172.25.0.72	HTTP	555 HTTP/1.1 404 Not Found (text/html)

On observe dans les deux cas que l'ip destination n'est pas la même pour le serveur selon où l'on se trouve.

Dans le cas où tente de se connecter l'extérieur on entrera l'ip de l'interface externe du routeur, celle qui est connecté au réseau de l'ut puis par la suite dans le routeur cette ip sera transformer en celle du réel serveur.

9. Avec un autre binôme faites les configurations nécessaires pour le succès d'un ping entre les deux PCs clients.

On effectue une route dans les deux sens

```

root@iutclrtc711:~# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=2.08 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=2.27 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=2.45 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=2.48 ms
64 bytes from 192.168.2.10: icmp_seq=5 ttl=62 time=2.31 ms
^C
--- 192.168.2.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 2.075/2.316/2.484/0.145 ms

```

