- Compte-rendu TPs -
DESR5 : bases des services réseaux

par Édouard Lumet & [redacted]

Sommaire

1. Installation et configuration d'un serveur DHCP

Nous allons ici résumer les étapes et les commandes pour installer un serveur DHCP, sous la forme d'un tutoriel expliqué. Dans ce compte-rendu, chaque partie sera sous cette forme.

Soit un réseau composé de 4 machines et divisé en trois sous-réseaux. Dans le réseau A on trouve un client et un routeur (sa passerelle), le réseau B contient un serveur DHCP et un autre routeur. Enfin le réseau C est le réseau entre les deux routeurs directement connectés.

On procède dans un premier temps à l'installation et à la configuration du serveur DHCP, objet de cette première partie :

- on installe les paquets nécessaires :

```
$sudo apt-get update
$sudo apt-get install isc-dhcp-server
```

- on modifie le fichier de configuration **/etc/dhcp/dhcpd.conf** :

```
default-lease-time 600 ;
max-lease-time 7200 ;
option subnet-mask 255.255.255.0 ;
option broadcast-address @broadcast_B ;
subnet B.B.B.B netmask 255.255.255.0 {
        range B.B.B.x B.B.B.y ;
}
```

- on modifie également le fichier **/etc/default/isc-dhcp-server** :

```
INTERFACES="ethx"
```

  'ethx' est le nom de l'interface où le serveur DHCP doit écouter en attente de DHCP DISCOVER

- on redémarre alors le serveur DHCP :

```
$sudo service isc-dhcp-server restart
```

- Pour attribuer une adresse IP fixe à un routeur par exemple, on ajoute dans le subnet les lignes suivantes :

```
host nom_routeur {
        hardware ethernet xx:xx:xx:xx:xx:xx ;
        fixed-address B.B.B.z ;
}
```

A noter que le serveur DHCP ne peut attribuer d'adresse qu'à la machine (routeur) du réseau B. Pour attribuer des adresses dans les autres réseau, il faut un relais DHCP.

2. NAT et filtrage IP

Pour effectuer de la traduction d'adresse (NAT) et du filtrage d'adresse IP, on peut utiliser sous Linux la commande *iptable*. La NAT permet d'emprunter l'adresse IPv4 publique d'une machine (comme un border router) afin de communiquer sur Internet en ayant seulement une adresse IPv4 privée.

- Pour le pare-feu, on commence par interdire tout le trafic en entrée et en sortie (policy DROP) :

```
$sudo iptables -t filter -P INPUT DROP
$sudo iptables -t filter -P FORWARD DROP
$sudo iptables -t filter -P OUTPUT DROP
```

- Ensuite on autorise au cas par cas, c'est-à-dire interface par interface, port par port et protocole par protocole :
  - on autorise tout le trafic pour la boucle locale :

```
$sudo iptables -t filter -A INPUT -i lo -j ACCEPT
```

  - on autorise, pour TCP puis pour UDP, port par port le trafic en entrée :

    NB: ${IFACE} est l'interface côté WAN (Internet) et ${PORT} est le port TCP ou UDP à autoriser

```
$sudo iptables -A INPUT ${IFACE} -p tcp --dport ${PORT} -j ACCEPT
$sudo iptables -A INPUT ${IFACE} -p udp --dport ${PORT} -j ACCEPT
```

    NB2: pour accepter <u>tout</u> le trafic en entrée on exécute :

```
$sudo iptables -t filter -A INPUT -j ACCEPT
```

  - on autorise, pour TCP puis pour UDP, port par port le trafic en entrée :

```
$sudo iptables -A OUTPUT ${IFACE} -p tcp --dport ${PORT} -j ACCEPT
$sudo iptables -A OUTPUT ${IFACE} -p udp --dport ${PORT} -j ACCEPT
```

    NB2: pour accepter <u>tout</u> le trafic en entrée on exécute :

```
$sudo iptables -t filter -A OUTPUT -j ACCEPT
```

- Pour la NAT, $ethx et $ethy désignent respectivement les interfaces côté LAN et côté Internet. Elles doivent donc être configurées avec une IP privée (ethx) et une IP publique (ethy) :

```
$sudo iptables -A INPUT -i $ethx -j ACCEPT
$sudo iptables -A FORWARD -i $ethy -o $ethx -m state --state RELATED,ESTABLISHED -j ACCEPT
$sudo iptables -A FORWARD -i $ethx -o $ethy -j ACCEPT
$sudo iptables -t nat -A POSTROUTING -o $ethy -j MASQUERADE
```

3. Relais DHCP

Comme nous l'avons vu dans la partie 1, le serveur DHCP ne peut pas attribuer d'adresse IP aux machines en dehors de son réseau. En effet, les broadcasts limités (comme leur nom l'indique) sont stoppés au niveau du routeur. Ensuite, le serveur DHCP doit avoir un moyen de « savoir » à quel réseau appartient la machine demandant une adresse.

- On commence par l'installation du relais DHCP sur un routeur :

```
$sudo apt-get install isc-dhcp-relay
```

- Lors de l'installation, trois paramètres sont demandés, ce sont ceux présents dans le fichier de configuration **/etc/default/isc-dhcp-relay** :
  - l'adresse du serveur DHCP (ou du prochain relais),
  - l'interface sur laquelle le relais doit écouter (surveiller les DHCP DISCOVER),
  - un argument à ajouter à l'exécution du relais (optionnel).
- Il ne reste plus qu'à redémarrer l'agent de relais DHCP :

```
$sudo service isc-dhcp-relay restart
```