# TP 3 - Routeur réseau (DHCP, DNS, NAT)

Pour ce TP on se propose de mettre en place un serveur qui fera office de routeur sur notre réseau (*istycorp.fr*). Nous utiliserons deux machines virtuelles. La première, nommée *client1*, fera office de client et correspondra à la station de travail d'un employé. La machine *router* sera notre point de travail principal et devra fournir :

— La configuration dynamique des IP au client et de leur résolution DNS.
— Un cache DNS.
— Le pont entre internet et le réseau interne.

## préparation des machines virtuelles

## Exercice 3.1

Cloner votre VM gentoo de façon a avoir une VM appelé *client1* et une deuxiéme appelé *router*. Assurez-vous de configurer leurs réseaux de sorte que :

1. La machine *router* doit avoir deux interfaces :
   (a) Une interface permettant l'accès à internet (NAT).
   (b) Une interface sur le réseau interne simulé (réseau interne que vous devez créer et nommé : istycorp).
2. La machine *client1* doit avoir une unique interface sur le réseau interne simulé.

## Exercice 3.2

Pourquoi ne connecte-t-on pas directement les machines clients sur le réseau internet ? Citez au moins trois raisons.

## Exercice 3.3

Rappelez le rôle du serveur DHCP et des serveurs DNS.

## Configuration manuelle

Afin de bien comprendre le rôle des composants nous allons dans un premier temps configurer les IP manuellement, démarrez les deux machines virtuelles.

## Exercice 3.4

Afin de faciliter le travail, on pourra installer un serveur SSH sur le routeur et ouvrir la redirection de port sur l'interface publique (dans VirtualBox) pour pouvoir s'y connecter.

## Exercice 3.5

L'image fournie est configurée pour le client, commencez par changer le nom d'hôte de la machine et vérifiez le nom de domaine local.

## Exercice 3.6

Configurez manuellement (*ifconfig*) le client et le routeur de sorte à avoir :

1. IP du routeur : 192.168.0.1.
2. IP du client : 192.168.0.2.

Testez le ping entre les deux clients et regardez les deux tables de routages avec la commande *route*. Expliquez.

## Exercice 3.7

Configurez le DNS du client de manière similaire au routeur. Tester la résolution de nom et l'accès à internet ? Pourquoi ne marche-t-elle pas ?

## Mise en place du NAT

Afin de partager la connexion internet du routeur avec les clients, il nous faut mettre en place le re routage des paquets et le support du NAT.

## Exercice 3.8

Rappelez l'objectif du NAT. Que peut apporter ipv6 par rapport à ce problème ?

## Exercice 3.9

Activez le routage des paquets sur le routeur en éditant le fichier /etc/sysctl.conf. Vous pouvez aussi activer ce dernier sans redémarrer en utilisant une des deux commandes :

```
sysctl -w net.ipv4.ip_forward=1
echo 1 > /proc/sys/net/ipv4/ip_forward
```

## Exercice 3.10

Activez le support du NAT sur le routeur. Ce protocole doit être activer dans *iptables* afin d'adapter les règles de routage des paquets.

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```

On peut rendre cette règle persistante en installant le paquet *iptables-persistent* et en générant le fichier de configuration :

```
iptables-save > /etc/rules.ipv4
```

### Exercice 3.11

Sur le client, vous devez rediriger les paquets à destination d'internet vers le routeur, pour cela, activez l'utilisation d'une passerelle :

```
route add default gw 192.168.0.1 eth0
```

### Exercice 3.12

Tester la connexion internet, vous pouvez visualiser le routage à l'aide de l'outil *traceroute* sur le client ou bien avec *tcpdump* sur le routeur.

### Exercice 3.13

Si l'on considère des outils tels que *tcpdump* ou *wireshark* sur le routeur, quelle remarque pouvez-vous faire quand à la sécurité des protocoles de communications non cryptées (ex. Http) ?

### Exercice 3.14

Tester la connexion sur un serveur FTP (par exemple un site miroir de distribution Linux ou du noyau). Pourquoi est-ce que le mode actif de FTP ne fonctionne pas ?

## Configuration dynamique : DHCP

En pratique on utilise habituellement le protocole DHCP pour configurer automatiquement les clients de notre réseau.

### Exercice 3.15

Installez un serveur DHCP sur le routeur et configurez-le avec les paramètres suivants :

1. Plage d'IP : 192.168.0.2 – 192.168.0.10
2. Masque d'IP : 255.255.255.0
3. Passerelle : 192.168.0.1
4. Domaine : istycorp.fr
5. DNS : Celui de l'université, regardez dans /etc/resolve.conf

### Exercice 3.16

Validez le fonctionnement en redémarrant le client.

## Cache DNS

### Exercice 3.17

Installez le cache DNS *dnsmasq* de sorte que ce dernier soit intercalé entre votre client et internet.

### Exercice 3.18

Définissez proprement les résolutions de noms pour les machines du réseau internes (en éditant /etc/hosts sur le routeur). Vérifiez la propagation au client au travers du cache DNS.

### Exercice 3.19

Ajoutez une entrée écrasant la résolution de nom de Google et renvoyant sur un autre site. Que pensez-vous de la sécurité des traductions d'adresse sur un réseau dont on n'est pas maitre ? Comment assurer la sécurité de la connexion dans ce cas ?

## Bonus : serveur NFS

### Exercice 3.20

S'il vous reste du temps installez un serveur NFS et montez-le sur le client pour disposer d'un dossier home centralisé.

### Exercice 3.21

Discutez la sécurité des droits utilisateurs dans cette configuration, les restrictions d'accès aux fichiers seront-elles nécessairement toujours vérifiées ?

## Bonus : redirection SSH

Installez un serveur ssh sur le client et tentez de le rejoindre. Pour cela il faut activer la redirection au niveau du NAT de la VM du routeur et du NAT du routeur lui même. Utilisez le port 2223 pour cela.