Année 2009-2010 — Session de Avril 2010

Étape : Master Sciences Technologies (semestre 2) — **UE :** INF470
Épreuve de : Administration des rseaux — **Durée :** 1h30
Date : 22 Avril 2010
Heure : 14h00
Documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Pourquoi le protocole `DHCP` est basé sur un mécanisme de *broadcast* ?
2. Expliquer la différence entre une recherche itérative et une recherche récursive en `DNS`.
3. À quoi sert le champ `MX` dans les zones `DNS` ? Donner un exemple d'utilisation de ce dernier.
4. Quelles sont les propriétés d'une DMZ ? Quel est l'intérêt de mettre en place une DMZ ?
5. Expliquer brièvement le principe de la translation d'adresses dynamique.

Petits exercices

1. Un système de translation d'adresses personnel (freebox, neufbox, ...) est utilisé pour donner accès à Internet à 15 postes de travail. Combien de connexions TCP simultanées sur le port 80 du serveur web `www.google.com` peuvent être supportées au plus ? Expliquez. Nous considérerons le cas où le serveur web n'a pas de mécanisme lui permettant de limiter le nombre de connexions simultanées.
2. Nous nous plaçons dans le contexte d'un jeu en ligne dans lequel un joueur peut se connecter de manière "anonyme" à une partie. Un utilisateur veut pouvoir rejoindre des parties en ligne en utilisant sa connexion ADSL dans laquelle la "box" joue le rôle de passerelle NAT.
   (a) Est ce qu'il sera possible pour l'utilisateur de rejoindre une partie ? Expliquer ce qui se passe au niveau du réseau.
   (b) Supposons maintenant qu'un(e) ami(e) de notre utilisateur veuille rejoindre la partie à partir d'une autre machine utilisant la même passerelle ("box"). Sera-t-il possible pour ce deuxième utilisateur de rejoindre la partie dans le cas où le serveur central du jeu identifie les clients uniquement par leur adresse IP ? Expliquer.
   (c) Dans le cas où le scénario de la question précédente ne fonctionnerait pas, proposer deux solutions.

Problème

Soit le script de configuration `iptables` donné ci-dessous. Il correspond au réseau représenté par la figure 1 (le script étant exécuté sur la machine `immortal`).

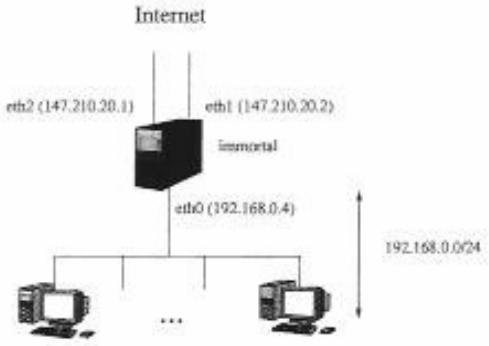

Figure 1 – Architecture du réseau.

```
#!/bin/sh
[1] iptables -F
[2] iptables -t nat -F

[3] iptables -P INPUT DROP
[4] iptables -P OUTPUT DROP
```

```
[5] iptables -P FORWARD DROP

[6] iptables -A INPUT  -i lo -j ACCEPT

[7] iptables -A OUTPUT  -o lo -j ACCEPT

[8] iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -o eth1 -j MASQUERADE

[9] iptables -t nat -A POSTROUTING -s 192.168.0.254 -j SNAT --to-source 147.210.20.1
[10] iptables -t nat -A PREROUTING -d 147.210.20.1 -j DNAT --to-destination 192.168.0.254

[11] iptables -A FORWARD -i eth0  -s 192.168.0.0/24 -j ACCEPT
```

1. Détailler les modifications que subit un paquet (correspondant à une ouverture de connexion) envoyé par l'hôte 192.168.0.1 à la machine d'adresse IP 209.85.135.99 (`www.google.com`) sur le port 80. Ce paquet arrivera-t-il à destination ? Expliquer. Qu'en est il de la connexion correspondante ? Pourra-t-elle être établie ? Dans le cas où elle ne le pourrait pas, ajouter une (ou plusieurs) règle(s) pour que ce soit possible.
2. Expliquer pourquoi le paquet envoyé par la machine dont l'adresse IP est 192.168.0.250 vers la machine dont l'adresse IP est 209.85.135.99 ne peut pas arriver à destination.
3. Est ce que l'hôte dont l'adresse IP est 209.85.135.99 peut ouvrir une connexion sur le port 22 du serveur dont l'adresse IP privée est 192.168.0.254 (on supposera qu'un serveur ssh est exécuté sur la machine correspondante) ? Expliquer et détailler ce qui se passe.
4. Même question que précédemment lorsque l'hôte dont l'adresse IP est 209.85.135.99 veut ouvrir une connexion sur le port 22 du serveur dont l'adresse IP privée est 192.168.0.3 (on supposera qu'un serveur ssh est exécuté sur la machine correspondante). Que faut-il mettre en place dans le cas où cette ouverture de connexion serait impossible ? Détailler dans ce cas les règles iptables correspondantes en les commentant.