

## Questions générales

1. Expliquer comment un switch fait pour associer une adresse MAC au numéro d'un de ses ports. À quel moment cette association est-elle faite ?
2. Dans LDAP donner deux points illustrant l'intérêt d'utiliser le mécanisme de réplication ?
3. Dans IPv6, à quoi correspond une adresse de lien local (*link local*) ? Comment cette adresse est-elle générée ? Comment fait la machine pour vérifier que l'adresse sélectionnée n'est pas utilisée actuellement par un autre hôte ?
4. Dans un système de stockage (DAS, NAS, SAN), quel est l'intérêt de l'utilisation du RAID ? Quelle sont les fonctions de base sur lesquelles tous les niveaux de RAID sont contruits ?
5. Expliquer le principe de la résolution DNS. Il est demandé de considérer les deux cas suivants : le serveur de nom local connaît la réponse, le serveur de nom local ne connaît pas la réponse.

## Exercices

6. Un système de translation d'adresses dynamique est utilisé pour donner accès à Internet à 20 postes de travail. Ce système disposant de deux adresses IP publiques, combien (en théorie) de connexions TCP simultanées sur le port 80 du serveur web dont l'adresse IP est 74.125.230.210 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.
7. Supposons que je dispose d'un abonnement internet standard (via une box) qui me permet de donner accès à internet à tous les terminaux du foyer (ordinateurs, téléphones, ...) en utilisant IPv4.
  - (a) Quel rôle joue la box pour permettre à tous les terminaux d'avoir accès à Internet de manière transparente. Les machines de mon réseau sont-elles accessibles depuis l'extérieur ?
  - (b) Supposons maintenant que mon opérateur me donne la possibilité de passer en adressage IPv6 (toujours via ma box).
    - i. Qu'est ce qui va changer pour les machines de mon réseau ? Auront-elles accès à Internet ? Seront-elles accessibles depuis l'extérieur ?
    - ii. Que dois-je mettre en place pour retrouver un niveau de sécurité équivalent à celui de la question 7a.
8. Une entreprise souhaite mettre en place un réseau pour connecter les différentes machines utilisées par ses employés et centraliser la gestion des utilisateurs des ressources informatiques de la société. Pour ce faire, un parc de machines, 3 serveurs (dont un avec beaucoup d'espace disque) et un switch de capacité suffisante ont été achetés. De plus, la société a pris un abonnement auprès d'un fournisseur d'accès à internet lui permettant d'avoir 1 adresse IP publique. Le réseau de l'entreprise devra être structuré en deux parties :
  - Les machines de la direction qui ont accès à toutes les ressources de l'entreprise
  - Les autres machines qui ont accès à tout sauf aux machines de la direction
  - (a) Proposer une architecture ainsi qu'un schéma d'adressage pour le réseau de l'entreprise (nombre de sous-réseaux, masques de sous-réseaux, mécanisme de translation d'adresses si besoin est, ...)
  - (b) La société veut disposer d'un serveur WEB et veut donner l'accès au réseau de l'entreprise à partir de l'extérieur à l'aide du service ssh. Étendre l'architecture proposée ci-dessus de manière à isoler un serveur (le serveur ne pourra pas accéder aux machines du réseau interne de l'entreprise autrement que par ssh) qui sera accessible de l'extérieur sur les ports correspondants aux services http et ssh. Il vous est particulièrement demandé de détailler la mise en place des mécanismes de sécurité. Il ne vous est pas nécessairement demandé de donner des règles iptables. Enfin, pour cette question, il est possible d'ajouter un switch à l'architecture si besoin est.



- (c) Le directeur de l'entreprise constate que la productivité d'un des meilleurs développeurs laisse soudainement à désirer. Il réalise que son employé joue des heures durant à un jeu en ligne. Le directeur, surpris que la configuration du réseau de l'entreprise laisse fonctionner ce jeu, qui utilise un protocole bloqué par les pare-feu, demande des explications à l'administrateur réseau. Ce dernier lui répond que la configuration du réseau de l'entreprise n'est pas mise en cause (les paquets correspondants au protocole utilisé par le jeu sont effectivement détruits). Comment est-il possible de faire fonctionner un tel jeu derrière un pare-feu ? Donner au moins deux possibilités.

## Problème

Soit le script de configuration d'iptables donné ci-dessous. Il correspond au réseau représenté par la figure fournie ci-dessous (le script étant exécuté sur la machine à trois interfaces 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
```

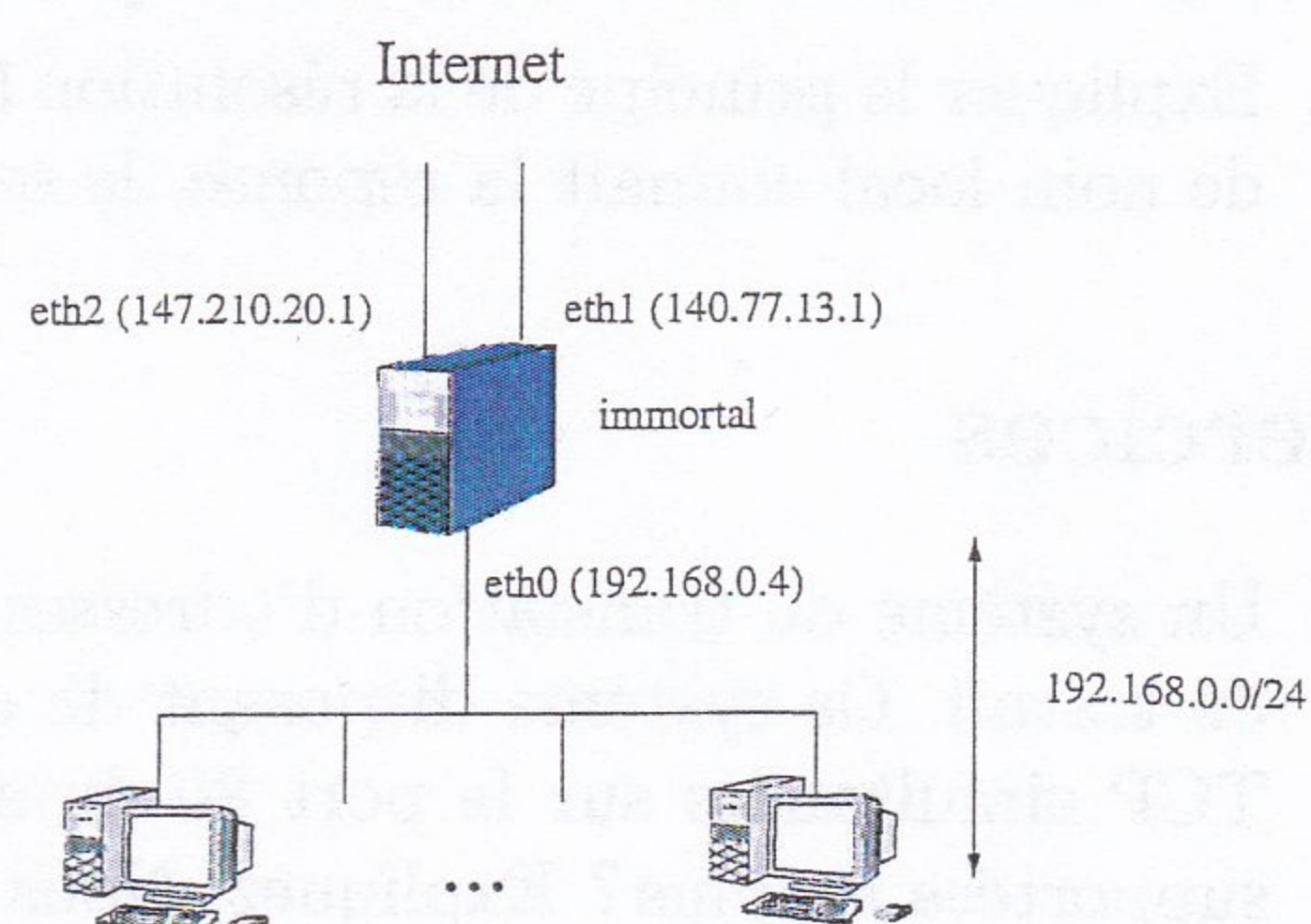
```
[6] iptables -A INPUT -i eth0 -j ACCEPT
[7] iptables -A INPUT -i lo -j ACCEPT

[8] iptables -A OUTPUT -o eth0 -j ACCEPT
[9] iptables -A OUTPUT -o lo -j ACCEPT
```

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

```
[11] iptables -t nat -A POSTROUTING -s 192.168.0.254 -j SNAT --to-source 147.210.20.1
[12] iptables -t nat -A PREROUTING -d 147.210.20.1 -j DNAT --to-destination 192.168.0.254
```

```
[13] iptables -A FORWARD -i eth0 -o eth1 -s 192.168.0.0/24 -j ACCEPT
```



9. 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.
10. Est-ce que le paquet d'ouverture de connexion envoyé par la machine dont l'adresse IP est 192.168.0.254 vers la machine dont l'adresse IP est 209.85.135.99 arrivera à destination ? Qu'en est-il de la connexion correspondante ? Corriger.
11. Est-ce que l'hôte dont l'adresse IP est 209.85.135.99 peut ouvrir une connexion sur le port 21 (ftp) du serveur dont l'adresse IP privée est 192.168.0.3 (on supposera qu'un serveur ftp est exécuté sur la machine correspondante) ? Que faut-il mettre en place dans le cas où cette ouverture de connexion ainsi que l'échange correspondant seraient impossibles ? Détailler dans ce cas les règles iptables correspondantes en les commentant.
12. Expliquer pourquoi une communication initiée par la machine dont l'adresse IP est 192.168.0.1 vers la machine dont l'adresse IP est 147.210.20.23 ne pourra pas fonctionner. Corriger.

**Remarque :** À chaque question il est nécessaire de prendre en compte les modifications effectuées dans les questions précédentes.