université de BORDEAUX

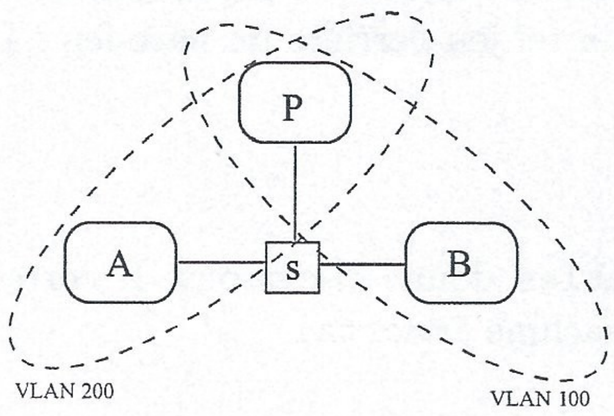
Master 1 *Sciences Technologies*

Année 2017-2018
Étape : Master Sciences Technologies (semestre 2)
Épreuve de : Administration des réseaux
Date : 27 Avril 2018
Heure : 9h00

Session de Avril 2018
UE : 4TIN808
Durée : 1h30
Documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer brièvement le principe de la translation d'adresses dynamique.
2. Expliquer comment les réseaux locaux virtuels (VLAN) sont gérés au niveau du protocole Ethernet. Dans le réseau décrit ci-dessous, expliquer ce qui se passe lorsque la machine A veut communiquer avec la machine B. P représente la passerelle et s un switch. Il vous est demandé de particulièrement insister sur la gestion des VLANs.



3. Dans un réseau local, expliquer ce qui se passe lorsque deux machines ont la même adresse IP. Même question lorsqu'elles ont la même adresse physique (MAC).
4. Que se passe-t-il du point de vue du réseau lorsqu'un utilisateur saisit une URL dans son navigateur web dans le but d'en consulter le contenu ?
5. Expliquer le principe de la résolution `DNS`. Il est demandé de considérer les deux cas suivants : le serveur de nom local connait la réponse, le serveur de nom local ne connait pas la réponse.

Exercices

1. L'utilitaire `ping` sert à envoyer un datagramme ICMP à une adresse IP et demande au destinataire d'envoyer un datagramme ICMP en réponse. Donnez une cause possible pour chacune des situations suivantes :

   (a)
   ```
   root@syl:~ #ping 172.16.0.2
   ...
   connect: Network is unreachable
   ```

   (b)
   ```
   root@syl:~ #ping 172.16.0.2
   ...
   From 172.16.0.1 icmp_seq=1 Destination Host Unreachable
   ```

   (c)
   ```
   root@syl:~ #ping 172.16.0.2
   ...
   From 172.16.0.254: icmp_seq=1 Redirect Host(New nexthop: 172.16.0.2)
   ```

2. 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 et 3 serveurs (dont un avec beaucoup d'espace disque) ont été achetés. De plus, la société a pris un abonnement auprès d'un fournisseur d'accès à internet lui permettant d'avoir 3 adresses IP publiques. 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 (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 demander de détailler la mise en place des mécanismes de sécurité. Il ne vous est pas nécessairement demandé de donner des règles `iptables`.

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

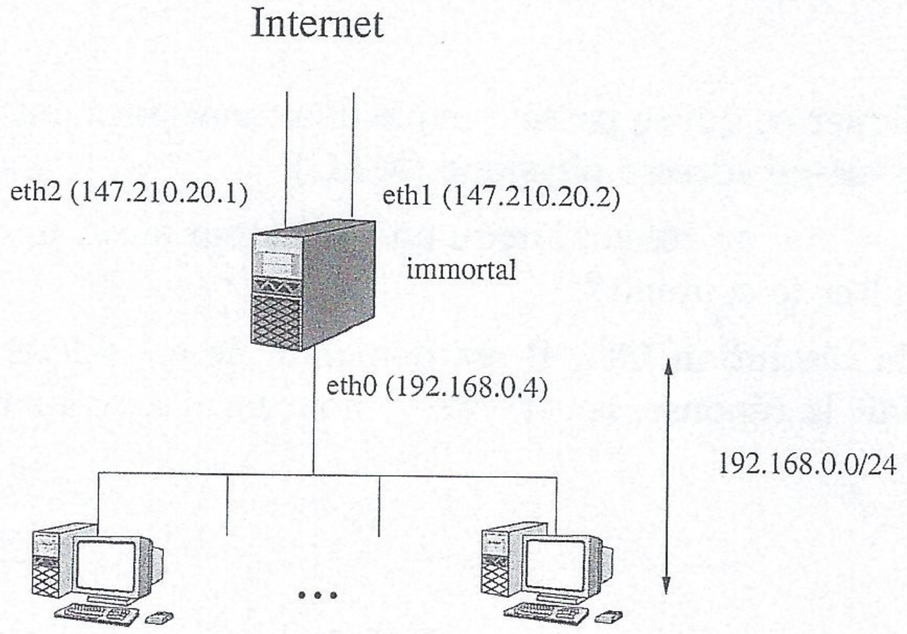


FIGURE 1 – Architecture du réseau.

```
#!/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 192.168.0.0/28 -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. Dans le cas où la connexion ne pourrait pas être établie, proposer une ou plusieurs règles pour corriger le problème.
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.