Devoir de TP de L3 Réseaux

#Toumany Doumbouya & Charles Diaw
Configuration

adresse publique pour box	bloc d'adresses privées
1.2.3.229/24	192.168.124.0/22

== The big picture ==

Vous disposez pour votre petite entreprise d'un bloc d'adresses privées que vous allez découper en 3 sous-réseaux :
- le réseau de la direction lana contient la machine (alice) de la pdg et doit pouvoir accueillir au moins 10 hôtes différents.
- le réseau principal lanb contient la machine du tourneur-fraiseur (bob) et doit pouvoir accueillir au moins 250 hôtes différents.
- le réseau des services lanc contient le serveur web (www) et doit pouvoir accueillir au moins 200 hôtes différents.

- faire un plan d'adressage de votre réseau privé en attribuant des blocs d'adresses à lana, lanb et lanc.

LAN	Subnet Address	Host Address Range	Broadcast Address
A	192.168.125.0	192.168.125.1 - 192.168.125.254	192.168.125.255
B	192.168.126.0	192.168.126.1 - 192.168.126.254	192.168.126.255
C	192.168.127.0	192.168.127.1 - 192.168.127.254	192.168.127.255

- configurer les interfaces et routes de (box) pour permettre la transmission du traffic intérieur.

```
box.startup
      ip addr add 1.2.3.229/24 dev eth0
      ip addr add 192.168.125.1/24 dev eth1
      ip addr add 192.168.126.1/24 dev eth2
      ip addr add 192.168.127.1/24 dev eth3

      ip route add default via 1.2.3.4
```

- configurer le serveur DHCP sur (box) en donnant une adresse statique à (www) et en distribuant des adresses dynamiques sur les réseaux lana, lanb et lanc. On proposera 1.2.3.4 comme adresse de résolveur DNS.

```
box.startup
   /etc/init.d/dhcp3-server start
```

```
subnet 192.168.125.0 netmask 255.255.255.0 {
    # Adresse du masque du reseau
    option subnet-mask 255.255.255.0;
    # Adresse de broadcast
    option broadcast-address 192.168.125.255;
    # Adresse de routeur
    option routers 192.168.125.1;
    # Adresse du domain name serveur
    option domain-name-servers 1.2.3.4;

    range 192.168.125.2 192.168.125.254;

}

subnet 192.168.126.0 netmask 255.255.255.0 {
    # Adresse du masque du reseau
    option subnet-mask 255.255.255.0;
    # Adresse de broadcast
    option broadcast-address 192.168.126.255;
    # Adresse de routeur
    option routers 192.168.126.1;
    # Adresse du domain name serveur
    option domain-name-servers 1.2.3.4;

    range 192.168.126.2 192.168.126.254;

}

subnet 192.168.127.0 netmask 255.255.255.0 {

    # Adresse du masque du reseau
    option subnet-mask 255.255.255.0;
    # Adresse de broadcast
    option broadcast-address 192.168.127.255;
    # Adresse de routeur
    option routers 192.168.127.1;
    # Adresse du domain name serveur
    option domain-name-servers 1.2.3.4;

    range 192.168.127.2 192.168.127.254;

    host www {
        hardware ethernet 06:89:ee:98:59:a0;
        fixed-address 192.168.127.50;
    }

}
```

```

 -  configurer un service de NAT sur (box) avec iptables pour autoriser
    les hôtes de lana, lanb et lanc à accéder à internet.
                      (bob) lynx www.perdu.com
```
box.startup
   iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

 -  configurer le serveur DNS sur (isp) pour qu'il gère les machines de
    votre domaine : "www.ara.com" et "dnsara.ara.com" hébergé par (isp).

```
isp/etc/bind/db.com.ara
   - dnsara   IN   A   #TODO
   - www   IN   A   #TODO
   + dnsara   IN   A   1.2.3.4
   + www   IN   A   1.2.3.147
```
```
isp/etc/bind/db.1.2.3
   - #TODO PTR   www.ara.com.
   + 4.3   PTR   www.ara.com.
```

 -  configurer un service de NAT sur (box) pour autoriser des connexions
    depuis internet vers "www.ara.com".
```
box.startup
   iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.127.50
```

 Pour la suite de la configuration, on se propose d'interdire autant que
possible le transit de paquets non nécessaires par (box).

 Pour cela on ajoute les lignes suivantes au début du fichier
"box.startup" :

 ```
 box.startup
      #initialiser les chaines
      iptables -t filter -F FORWARD
      iptables -t filter -F INPUT
      iptables -t filter -F OUTPUT
      iptables -t nat -F PREROUTING
      iptables -t nat -F POSTROUTING

      #comportement par defaut : drop
      iptables -t filter -P FORWARD DROP
      iptables -t filter -P INPUT DROP
      iptables -t filter -P OUTPUT DROP
```
```

```
      #connexions locales
      iptables -t filter -A INPUT -i lo -j ACCEPT
      iptables -t filter -A OUTPUT -o lo -j ACCEPT
```

 - ajouter des règles à la chaîne FORWARD pour que les services de NAT déjà configurés continuent d'opérer.

```
box.startup
   iptables -A FORWARD -o eth0 -j ACCEPT
   iptables -A FORWARD -i eth0 -j ACCEPT
```

 - démarrer un serveur ssh sur (box) et autoriser la connexion depuis lana uniquement.

```
box.startup
   /etc/init.d/ssh start
   iptables -t filter -i eth1 -A INPUT -p TCP --dport 22 -j ACCEPT
   iptables -t filter -A OUTPUT -p TCP --sport 22 -j ACCEPT
```

 - ajouter des règles de NAT sur (box) pour autoriser des connexions depuis lana et lanb vers "www.ara.com".
                    (alice) lynx www.ara.com

```
box.startup
   iptables -A FORWARD -i eth1 -o eth3 -j ACCEPT
   iptables -A FORWARD -i eth3 -o eth1 -j ACCEPT
   iptables -A FORWARD -i eth2 -o eth3 -j ACCEPT
   iptables -A FORWARD -i eth3 -o eth2 -j ACCEPT
   iptables -t nat -A PREROUTING -s 192.168.124.0/22 -d 1.2.3.229 -p TCP -
-dport 80 -j DNAT --to-destination 192.168.127.50
```

 - vous ne souhaitez pas autoriser vos salariés ayant des machines dans lanb à se connecter sur le site subversif "www.ahcaira.com", il faut donc ajouter une règle de filtrage avec l'utilitaire iptables sur (box). Évidemment les utilisateurs connectés sur lana gardent le droit d'accéder à cette page web.

```
box.startup
   iptables -t nat -A PREROUTING -s 192.168.126.0/24 -d 9.9.9.9 -j DROP
```