Devoir de TP de L3 Réseaux

Evan JUGE & Baptiste MESSIN

Configuration

adresse publique pour box	bloc d'adresses privées
1.2.3.147/24	192.168.32.0/19

Les enregistrements pcap sont stocker dans un dossier caché .pcap.
Tout le projet a été suivie par un git et un depos github disponible ici :
https://github.com/Ayce45/labdev

> L'objectif de ce devoir est de configurer le réseau de votre petite entreprise raccordée à internet : configuration des interfaces, des routes, DHCP, DNS, NAT, pare-feu.

== 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.

Ces 3 réseaux sont tous reliés à un routeur (box) qui dispose en plus d'une interface sur le réseau 1.2.3.0/24 et d'une connexion à internet en utilisant la passerelle 1.2.3.4 (machine isp). La machine (isp) vous servira aussi de résolveur DNS et de serveur DNS administrant les noms de votre domaine : "ara.com".

Vous utiliserez comme paramètres (bloc d'adresses privées et adrese publique de (box)) le couple de paramètres proposé sur celene pour l'un ou l'autre des membres du binôme.

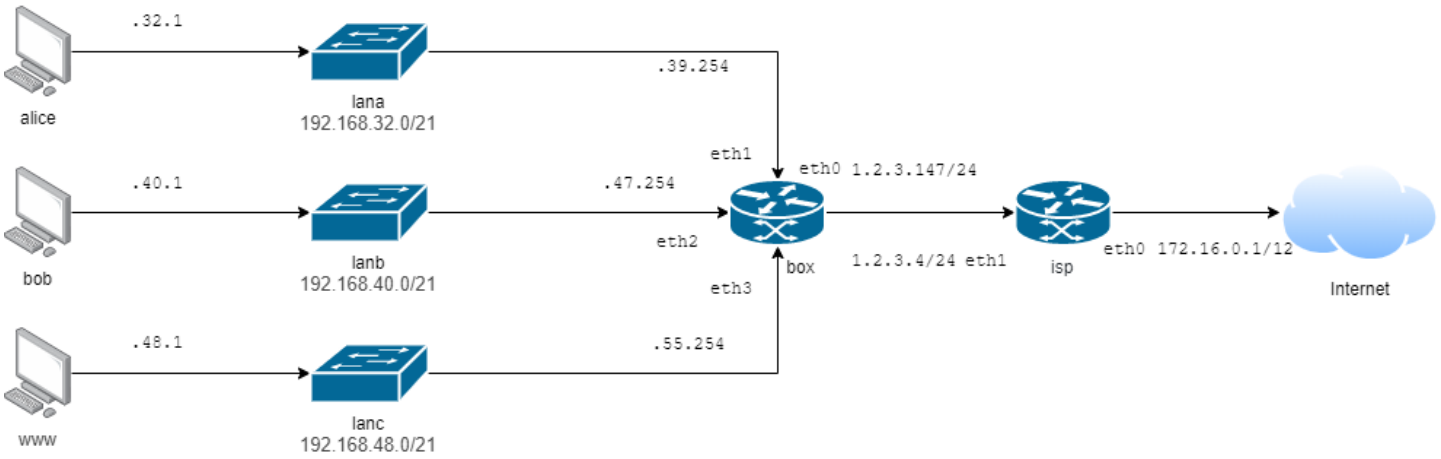
Il est interdit de modifier "lab.conf", la structure du réseau ne doit pas être modifiée !

== Ce qui est à configurer ==

Seuls sont à modifier les fichiers mentionnés dans cette section. Des tests vous sont proposés suite à certaines parties de la configuration.

Votre travail consiste à configurer les machines et services suivants : (4 points)

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



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

```
box.startup
   ifconfig eth0 1.2.3.147 netmask 255.255.255.0
   ifconfig eth1 192.168.39.254 netmask 255.255.248.0
   ifconfig eth2 192.168.47.254 netmask 255.255.248.0
   ifconfig eth3 192.168.55.254 netmask 255.255.248.0

   route add default gw 1.2.3.4
```

(4 points)

- 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. ✔ - (alice) ping @bob ✔ - (alice) ping 1.2.3.4 ✔ - (alice) ping @www ✔

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

```
box/etc/dhcp3/dhcpd.conf
   subnet 192.168.32.0 netmask 255.255.248.0 {
      option subnet-mask 255.255.248.0;
      option routers 192.168.39.254;
      option domain-name-servers 1.2.3.4;
      range 192.168.32.1 192.168.39.253;
   }
   subnet 192.168.40.0 netmask 255.255.248.0 {
      option subnet-mask 255.255.248.0;
      option routers 192.168.47.254;
      option domain-name-servers 1.2.3.4;
      range 192.168.40.1 192.168.47.253;
   }
   subnet 192.168.48.0 netmask 255.255.248.0 {
      option subnet-mask 255.255.248.0;
      option routers 192.168.55.254;
      option domain-name-servers 1.2.3.4;
      range 192.168.48.1 192.168.55.253;

      host www {
         hardware ethernet 0a:5d:cf:21:93:a5;
         fixed-address 192.168.48.100;
      }
   }
```

```
.pcap/1.pcapng
```

- configurer le serveur HTTP (www) : modifier le fichier /etc/apache2/httpd.conf pour ajouter l'adresse de l'hôte.✔ - (alice) lynx @www ✔

```
/etc/apache2/httpd.conf
   - Servername :80 #TODO
   + Servername localhost:80
```

```
.pcap/2.pcapng
```

(4 points)

- 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
```

```
.pcap/3.pcapng
```

- 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). (fichiers "/etc/bind/db.com.ara" et "db.1.2.3") ✔ (diane) dig www.ara.com ✔

```
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.
```

```
.pcap/4.pcapng
```

- configurer un service de NAT sur (box) pour autoriser des connexions depuis internet vers "www.ara.com". ✔ (diane) lynx www.ara.com ✔

```
box.startup
   iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.48.100
```

```
.pcap/5.pcapng
```

(8 points) 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. ✔ (bob) lynx www.perdu.com ✔ (diane) lynx www.ara.com ✔

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

```
.pcap/6_bob.pcapng
.pcap/6_diane.pcapng
```

- démarrer un serveur ssh sur (box) et autoriser la connexion depuis lana uniquement. ✔ (alice) ssh @box ✔ PAS DE CONNEXION (bob) ssh @box ✔

```
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
```

```
.pcap/7_alice.pcapng
```

- 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 192.168.32.0/19 -d 1.2.3.147 -p TCP --dport 80 -
```

```
.pcap/8.pcapng
```

- 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. ✔ PAS DE CONNEXION (bob) lynx www.ahcaira.com ✔ (bob) lynx www.perdu.com ✔ (alice) lynx www.ahcaira.com ✔

```
box.startup
   iptables -t nat -A PREROUTING -s 192.168.40.0/21 -d 9.9.9.9 -j DROP
```

```
.pcap/9_bob.pcapng
.pcap/9_alice.pcapng
```

== Modalités de retour du devoir ==

Le devoir est à traiter en binôme (ou monôme). La solution est à déposer sous la forme d'une archive nommée nom1.prenom1_nom2.prenom2.tar.gz sur la page Celene du cours.

L'archive doit contenir :

- un rapport au format PDF qui reprend les noms des membres du binôme, les paramètres utilisés et qui explique brièvement le travail effectué.
- des enregistrements pcap (modalités ci-dessous) d'échanges illustrant le résultat des commandes de configuration.
- le lab modifié par vos soins.

Pour obtenir un enregistrement pcap, vous lancerez wireshark (vdump rezo | wireshark -i - -k &), effectuerez les opérations choisies puis : - arrêterez la capture (bouton STOP de wireshark); - choisirez "Enregistrer sous" dans Fichier; - sauvegarderez dans le format par défaut (pcapng).