TP4 : Réseau Domestique

Ces deux séances de TP proposent d'appréhender les principaux éléments et protocoles d'un réseau domestique, là où le grand public accède à Internet.

Objectifs :

- Savoir mettre en œuvre la configuration automatique d'équipement réseau (DHCP)
- Permettre à des réseaux privés de communiquer sur Internet (SNAT)

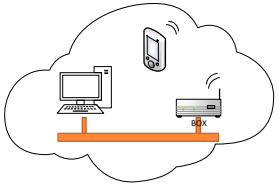

Figure 1 : Un réseau domestique

La figure 1 illustre un réseau domestique classique. Il s'agit d'un réseau à domicile d'un client qui est composé des différents équipements connectés. Dans les années 2000 ce réseau était souvent restreint à un seul équipement : l'ordinateur fixe directement relié à Internet via un modem. Ce schéma s'est diversifié avec l'apparition des *boxes* Internet et l'ouverture à Internet d'un grand nombre d'équipements : télévision, tablettes, téléphones, objets connectés… Actuellement, les deux technologies communément utilisées dans le réseau domestique sont le WiFi et l'Ethernet.

Pour la suite du TP, vous allez travailler en binôme sur deux PCs. L'un sera la box de votre réseau domestique et l'autre un équipement du réseau connecté à la box par un câble en Ethernet.

Partie I : Dynamic Host Configuration Protocol

Il n'est plus souvent question aujourd'hui qu'un équipement soit configuré manuellement par son utilisateur, même si cela reste possible. D'une part la plupart des personnes n'a pas de connaissances poussées en réseau et en système, et, d'autre part, il faut savoir quelle configuration prendre. Un protocole souvent déployé et utilisé aujourd'hui est `dhcp`. C'est un protocole client/serveur que nous avons vu en cours et qui est déployé en tant que serveur sur la *box*.

1.1 – Distribution d'une plage d'adresses publique

Dans un premier temps, on considère que chaque groupe dispose d'une adresse entre la box et son FAI de type `80.1.x.10/24` où x est le numéro du groupe et d'une plage d'adresse pour son réseau domestique de type `80.2.x.0/24`. La box est connectée sur le routeur du FAI. L'adresse de son routeur de FAI est `80.1.x.20`. (Fig. 2)

Exercice 1 :
Configurer la box de votre réseau pour qu'elle puisse se connecter avec le routeur du FAI. Testez la connectivité entre la box et le router, puis entre les boxes.

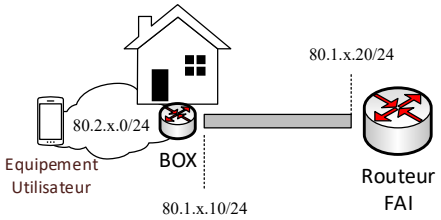

Figure 2 : Adressage publique

A partir de là, on souhaite que la box fournisse une configuration automatique à votre équipement. Pour cela il faut s'occuper d'une part de la mise en place du réseau (a) et d'autre part, configurer et lancer le serveur `dhcp` (b).

a – Mise en place du réseau domestique

Exercice 2 :
Câbler votre box à l'équipement utilisateur et configurer l'interface de votre box avec son adresse IP. La box doit aussi être mise en mode routeur. L'équipement utilisateur doit avoir son interface activée mais sans configuration.

b – DHCP

Ici nous allons illustrer le fonctionnement du protocole d'auto-configuration le plus commun, DHCP, et l'observer.

Le serveur `dhcp` est installé sur la box, il se nomme *`isc-dhcp-server`*. C'est aujourd'hui le serveur recommandé.

Le serveur `dhcp` a besoin de deux fichiers de configuration pour fonctionner :

- */etc/default/isc-dhcp-server* qui contient les interfaces où le serveur `dhcp` écoute. Il faudra donc y rajouter entre les guillemets l'interface qui connecte votre box au réseau domestique.
- */etc/dhcp/dhcpd.conf* qui contient la configuration que le serveur `dhcp` donne à ses clients. Un exemple de fichier `dhcpd.conf` vous est donné ci-après. A vous de comprendre ce qu'il fait.

```
# Exemple pour TPReZO /etc/dhcp/dhcpd.conf
# Ceci est un commentaire

default-lease-time 600;
max-lease-time 7200;

authoritative;

subnet 192.168.31.0 netmask 255.255.255.0 {
  range 192.168.31.10 192.168.1.99;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.31.255;
}
```

Comme un grand nombre de services ou démons sur Linux, il se lance en utilisant *systemctl*, comme pour *quagga*. On peut donc l'activer avec la commande :

```
systemctl start isc-dhcp-server
```

Pour vérifier qu'il fonctionne correctement, vous pouvez mettre *status* à la place de *start* ou regarder la fin du fichier /var/log/syslog avec la commande *tail*.

> ***Exercice 3 :***
> Mettez en place le serveur dhcp pour qu'il puisse configurer automatiquement l'adresse IP de votre box (attention aux erreurs de syntaxe dans le fichier dhcpd.conf).

Maintenant que le serveur est configuré et activé, nous allons pouvoir utiliser dhcp sur les clients. Pour cela la commande suivante permet d'activer le client dhcp sur l'interface ethX :

```
dhclient ethX
```

Si vous souhaitez le désactiver, il vous faut utiliser l'option –r pour release :

```
dhclient -r ethX
```

> ***Exercice 4 :***
> Lancez Wireshark sur vos interfaces du réseau domestique et activer le client dhcp. Vous observez alors l'échange protocolaire, votre objectif est d'expliquer les principales étapes de dhcp.

1.2 – Ajout d'information de routage

Le serveur dhcp ne permet pas simplement que de configurer les adresses IP de ses clients, mais d'autres paramètres sont disponibles pour une bonne configuration réseau des clients. Puisque nous avons déjà étudié le routage, nous allons rajouter à notre configuration une route par défaut. Pour cela il faut utiliser l'option routers dans la configuration du serveur. Le mieux est d'insérer cette option comme suit :

```
subnet 192.168.31.0 netmask 255.255.255.0 {
  range 192.168.31.10 192.168.1.99;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.31.255;
  option routers 192.168.31.100;
}
```

> ***Exercice 5 :***
> Mettez en place la nouvelle configuration automatique pour obtenir une route par défaut. Observez les changements dans les échanges et tester la connectivité entre tous les équipements de la salle.

On peut remarquer que beaucoup d'autres options sont disponibles pour le serveur dhcp, vous trouverez une documentation assez complète sur https://doc.ubuntu-fr.org/isc-dhcp-server.

1.3 – Distribution d'une plage d'adresses privées

Pour le moment, nous avons considéré que chaque réseau domestique disposé de plusieurs adresses IP, à savoir une adresse vers le FAI, et une plage publique pour son réseau. Toutefois, le nombre d'adresses IP est limité et il n'est plus possible d'utiliser pour le réseau des particuliers des adresses publiques. C'est un adressage privé qui est utilisé de type 192.168.0.0/16. On utilise rarement toute la plage en /16 mais plutôt une sous-plage de cet ensemble en /24. Ici nous choisirons la même plage pour tout le monde, à l'instar des boxes des FAIs actuels : 192.168.1.0/24 (Fig.3).

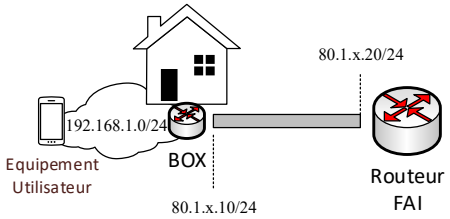

Figure 3 : Adressage privé

> ***Exercice 6 :***
> Changez la configuration de votre serveur dhcp et de votre box (son adresse IP sur l'interface du réseau domestique) pour qu'elle distribue un réseau privé et non publique.
> Pouvez-vous toujours communiquer avec les autres box ? Les autres équipements utilisateurs ? Le routeur ? Quelles en sont les raisons ?

Partie II : Network Address Translation

Comme vous venez de l'observer, l'utilisation d'un adressage privé implique une perte de connectivité avec le reste d'Internet. Toutefois, la box, elle, possède une adresse publique. L'idée est donc de l'utiliser pour se « cacher » derrière elle et faire croire au reste du monde que l'on est cette machine. Ce *déguisement* porte le terme de *masquarade* mais l'on préfère aujourd'hui parler de traduction d'adresse source, SNAT en anglais.

Pour mettre en place le SNAT, on utilise les tables IP (*iptables*) de Linux. Le fascicule qui vous a été distribué au début des TPs vous donne les principales commandes *iptables*. Après avoir fait un point avec votre intervenant de TP sur le principe vu en cours du SNAT et la logique des commandes *iptables*, vous pourrez répondre à ce dernier exercice du TP4.

> ***Exercice 7 :***
> Mettez en place une règle de NAT sur la box permettant à l'équipement du réseau domestique d'accéder aux équipements publics du réseau (ici le routeur et les *boxes*). Observez la communication et les changements effectués, et expliquez comment fonctionne le SNAT.