Serveur DHCP basique

Encadrant : **P. Spathis**

Etudiants : **L. Merlin, E. Giang**

Table des matières

1 Introduction

Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est la configuration des paramètres IP des machines arrivant sur le réseau. Le protocole permet entre autres d'attribuer une adresse IP, un masque de sous réseau, l'adresse de la passerelle par défaut ou encore les serveurs de noms DNS. Ce protocole est généralement géré par un serveur DHCP qui pour un réseau domestique par exemple est souvent dans la box internet. Le but de ce travail est donc de réaliser un serveur DHCP capable de remplacer ou bien de cohabiter avec un autre serveur DHCP afin que tous les appareils aient des paramètres IP configurés correctement. Nous détaillerons dans un premier temps les fonctionnalités que nous avons implémentées dans notre serveur DHCP. Nous expliquerons ensuite le fonctionnement du serveur basé sur ces fonctionnalités pour enfin parler de notre gestion du projet.

2 Fonctionnalités du serveur

2.1 IP Fixe/Dynamique

Lors de la connexion à un réseau, le serveur DHCP nous attribue une adresse IP. Cette adresse peut être toujours la même, on dira alors que nous avons une adresse fixe, ou alors cette adresse peut être différente à chaque connexion, on dira alors que nous avons une adresse dynamique. Attribuer les adresses IP de manière fixe sur un réseau permet de trouver efficacement une machine car celle-ci se trouve toujours à la même adresse IP. Cependant cela facilite donc aussi la tâche pour quelqu'un de malintentionné et donc l'IP dynamique permet de rendre cela plus difficile pour un intrus. Notre serveur DHCP propose donc cette fonctionnalité ce qui permet à tout utilisateur connu du réseau de demander la dernière adresse IP qu'il s'est vu attribuer et si le serveur est configuré pour donner des adresses fixes lui donnera, sinon le serveur lui donnera une IP dynamique et donc une différente que la dernière adresse donnée à cette machine.

2.2 Association MAC/IP

Sur un réseau local, nous pouvons vouloir qu'une adresse MAC et donc une machine ait toujours une même adresse IP. Cela permet de retrouver toujours la même machine à une certaine adresse IP et ce peu importe la configuration du serveur. En effet, si le serveur est en configuration IP dynamique, il attribuera tout de même l'adresse IP donnée pour cette adresse MAC et ce même si c'est la dernière adresse IP qu'avait la machine sur le réseau. Via le fichier de configuration, nous pouvons donc forcer l'adresse IP d'une machine afin qu'elle garde son ancienne adresse ou bien lui en donner une précise peu importe le reste de la configuration du serveur.

2.3 Blacklist

Certains appareils sont parfois présents dans un réseau local alors qu'ils n'ont rien à y faire ou que nous voulons plus de leur présence en son sein. La "blacklist" nous permet donc d'interdire l'attribution d'une adresse IP à une machine et donc l'empêcher de faire partie du réseau local. Pour donner la possibilité d'interdire l'accès à une machine sur le réseau, notre serveur DHCP permet d'entrer une adresse MAC dans le fichier de configuration afin qu'on ne lui attribue pas d'adresse IP.

2.4 Plage d'attribution d'adresses du serveur DHCP

Lorsqu'une machine n'ayant pas d'adresse IP tente de se connecter à un réseau, le serveur DHCP doit lui attribuer une adresse IP disponible, c'est-à-dire une adresse n'ayant pas déjà été attribuée à une station du réseau. A la configuration de ce serveur, une plage d'adresses doit lui être définie, afin qu'il puisse choisir, en fonction du mode d'attribution (fixe ou dynamique), l'adresse à suggérer à une station cliente. Notre serveur DHCP pourra gérer une seule plage d'adresses, ou alors plusieurs plages disjointes ou contiguës. Il s'assurera à ne distribuer que les adresses présentes dans les plages spécifiées. Les adresses ne se situant pas dans cette plage peuvent être utilisées pour les stations nécessitant une adresse IP fixe. Dans le cas d'un réseau possédant plusieurs serveurs DHCP, les plages d'adresses qui leur sont attribuées ne doivent pas se chevaucher, sous peine de problèmes de synchronisation et d'attribution valide des adresses IP. Notre fichier de configuration supporte une configuration d'une seule plage d'adresses IP, écrite sous la forme : ([192.168.0.1]-[192.168.0.210]) par exemple, ou celle de plusieurs plages disjointes ou contiguës écrites sous la forme ([192.168.0.1]-[192.168.0.210])([192.168.0.222]-[192.168.0.235]) par exemple.

2.5 Bail

L'attribution d'une adresse IP par le serveur DHCP à une station cliente est faite sur une durée limitée et déterminée appelée bail. Lors de l'expiration de son bail, une adresse IP redevient disponible et le serveur peut l'attribuer à une autre station demandeuse. Lorsqu'une station connectée voit son bail expirer, elle peut demander à son serveur un renouvellement du bail par l'émission d'une requête DHCPREQUEST. Par inversement, lorsqu'un serveur remarque un bail d'un de ses clients qui arrive à échéance, il peut lui envoyer un DHCPNAK pour une demande de prolongation de bail. En l'absence de réponse, le serveur considère cette adresse comme libre. Le bail permet donc d'éviter un problème d'épuisement de ressources si les machines ne libèrent jamais leur adresse IP attribuée. La durée du bail est attribuée lors d'une émission d'un DHCPOFFER par le serveur DHCP pour son client via le champ d'option 51. Dans notre fichier de configuration, la durée du bail est définie en secondes puis transformée grâce à notre fonction set bail dans le format adéquat à la transmission du message. Notre serveur DHCP gère le bail par la mise en place d'un timer qui ne cesse de tourner en parallèle de l'exécution du serveur. A chaque fin de timer, notre serveur ping toutes les stations clientes dont une adresse IP a été attribuée le serveur, afin de déterminer les stations actives et inactives et rendre libre les adresses IP des stations inactives. Faire tourner le timer en parallèle de l'exécution du serveur et l'envoi de ping aux clients nécessitent l'utilisation de threads.

2.6 DHCP Starvation Attack

L'attaque DHCP par épuisement de ressources permet à un attaquant d'épuiser les adresses IP disponibles dans sa plage d'adresses en inondant le serveur DHCP de messages de demandes DHCP DISCOVER. En effet, le serveur DHCP répondra à toutes les requêtes jusqu'à épuisement de toutes les adresses IP disponibles. Une demande supplémentaire après épuisement sera refusée, le serveur ne pourra donc plus assurer son service. En conséquence, les stations peuvent rechercher d'autres serveurs DHCP disponibles dont un serveur hostile, configuré par l'attaquant. Ce serveur pourra dont espionner le trafic du client qui lui a demandé son service. Pour parer cette attaque, nous avons décidé d'imposer une limite d'adresses IP à attribuer. Ainsi, au-delà d'un certain nombre de demandes, il n'est plus possible pour le serveur DHCP d'accepter des messages DHCPDISCOVER. On limite ainsi le risque d'inondation de ces demandes. Dans notre cas, nous avons décidé d'imposer une limite de 3/4 des ressources disponibles.

3 Fonctionnement du serveur DHCP

Lorsque notre serveur est actif, il est possible de recevoir plusieurs types de messages DHCP. Ces différents messages doivent être traités différemment. Lors de la réception d'un message sur notre serveur nous regardons donc de quel type il est afin de le traiter de la manière adéquate.

3.1 DISCOVER

Lors de son arrivée sur un réseau, un appareil va envoyer un message DHCPDISCOVER contenant aucune information IP. Le serveur DHCP lui répond alors avec un message DHCPOFFER lui proposant une adresse IP avec un bail ainsi que les autres informations utiles sur le réseau.

A la réception d'un message DHCPDISCOVER, nous vérifions tout d'abord si la limite du nombre d'adresses attribuables n'est pas atteinte, ce qui signifierait que nous avons à faire à une attaque par épuisement de ressources. Si tel est le cas, le serveur ignore le message. Dans le cas contraire, si l'adresse MAC de la station cliente est présente dans la Blacklist, le serveur devra aussi ignorer le message. Maintenant que nous savons que nous pouvons traiter le message, le serveur regarde si l'adresse MAC doit être associée à une adresse IP précise dans le fichier de configuration. Si oui, nous envoyons notre message DHCPOFFER avec l'adresse IP précisée dans le fichier de configuration, sinon nous regardons si le serveur doit attribuer les adresses de façon statique. Si nous devons attribuer de manière fixe l'adresse IP nous regardons dans le fichier "historique.txt" si l'adresse MAC est connue par le serveur, si oui, nous lui envoyons un message DHCPOFFER proposant à la station cliente, la dernière adresse IP qui lui a été attribuée dans le réseau. Cependant, si la machine n'est pas connue du serveur ou que nous procédons à un adressage dynamique, nous envoyons un message DHCPOFFER avec une adresse IP aléatoire comprise dans la plage d'adresse et qui ne soit pas encore attribuée.

3.2 REQUEST

Après réception du message DHCPOFFER, l'appareil doit confirmer au serveur DHCP si la proposition faite dans le DHCPOFFER l'intéresse en envoyant un message DHCPREQUEST confirmant les informations qu'il souhaite prendre. Le serveur vérifie alors si l'appareil lui demande bien ce qui lui a été proposé précédemment, lui envoie un message DHCPNAK si tel n'est pas le cas, et sinon lui envoie un message DHCPACK pour lui confirmer l'attribution. Cependant un appareil peut directement envoyer un message DHCPREQUEST sans passer par un DHCPDISCOVER si il connaît déjà le serveur.

A la réception d'un message DHCPREQUEST, nous procédons dans le même ordre de priorité que pour un message DHCPDISCOVER. Tout d'abord, si l'adresse est blacklistée, le serveur ignore le message. Dans le cas contraire, nous vérifions si l'adresse MAC est associée à une adresse IP dans le fichier de configuration et si oui nous vérifions que l'adresse IP demandée dans le message DHCPREQUEST correspond à celle qu'on doit lui associer. Si c'est le cas, nous envoyons un message DHCPACK. Sinon nous envoyons un message DHCP NAK. Si l'adresse MAC n'est associée à aucune adresse IP, nous regardons si nous attribuons les adresses dynamiquement ou non. Si c'est le cas, nous regardons dans le fichier "historique.txt" si l'adresse MAC est déjà répertoriée et est associée à l'adresse IP demandée. Si tel est le cas, et que l'ID de la transaction correspond également, nous envoyons un message DHCPACK car cela signifie que la station cliente a reçu un DHCPOFFER de la part de notre serveur. Si au contraire l'adresse IP ou l'ID de la transaction ne correspond pas, cela signifie que le message reçu est un DHCPREQUEST envoyé par la station cliente afin de demander son adresse IP anciennement attribuée pour ce réseau. A ce dernier, nous répondons un message DHCPNAK car nous attribuons les adresses dynamiquement. Si nous sommes alors en adressage fixe et que l'adresse IP demandée dans le message DHCPREQUEST correspond à celle associée à l'adresse MAC dans le fichier "historique.txt", nous envoyons un message DHCPACK. Si la station demande une adresse anciennement attribuée, nous vérifions qu'elle correspond à celle que nous avons conservée dans notre fichier "historique.txt" et envoyons un message DHCPACK. Sinon nous envoyons un message DHCPNAK.

3.3 DECLINE

La réception d'un message DHCPDECLINE signifie que l'adresse IP que nous avons attribuée à un appareil est en réalité déjà attribuée et donc nous le prenons en compte et l'appareil nous envoyant le message DHCPDECLINE recommence un cycle en envoyant un message DHCPDISCOVER.

4 Gestion du projet

Le serveur DHCP a besoin d'être configuré selon les besoins de l'administrateur pour pouvoir correspondre au réseau auquel nous voulons le rattacher. Notre fichier "config.txt" rassemble toutes ces informations essentielles. Les paramètres configurables sont donc le masque du réseau, l'adresse du serveur DHCP, l'adresse de la box, l'adresse broadcast, la (ou les) plage(s) d'adresses, si l'attribution des adresses est fixe ou dynamique (0 pour fixe, 1 pour dynamique), la durée du bail en secondes, la liste d'association adresses MAC/IP, les adresses MAC blacklistées et enfin l'adresse du réseau.

4.1 Initialisation du serveur

Au lancement de notre serveur, nous exécutons plusieurs fonctions en parallèle à l'aide de threads.

- Une fonction (thread ip) permet de tester les adresses IP actives déjà présentes dans le réseau au lancement du serveur et qui ne sont donc pas attribuables par le serveur aux stations clientes. Elle consiste à envoyer un ping à toutes les adresses de la plage d'adresse configurée du serveur DHCP et à placer les adresses IP actives dans une liste d'adresses à ne pas attribuer.

- La fonction verif bail utilise la fonction d'envoi de ping pour tester l'activité ou l'inactivité des stations ayant des adresses IP situées dans la liste des adresses IP déjà attribuées par le serveur et ainsi vérifier si leur bail est toujours d'actualité.

- Une fenêtre de commandes s'ouvre en parallèle à l'exécution du serveur. L'implémentation de cette fenêtre de commandes a été rendue possible grâce à la bibliothèque « tkinter » toutes les fonctionnalités graphiques dont nous avions besoin. La commande « ipocc » permet d'afficher les adresses IP déjà attribuées par le serveur. La commande « iplib » permet d'afficher les adresses IP disponibles.

4.2 Les fichiers annexes

Lors de l'exécution du serveur, plusieurs fichiers sont alimentés en parallèle et ont des fonctions spécifiques :

- Le fichier "historique.txt" liste la dernière adresse IP attribuée à une adresse MAC particulière. En effet, à la réception d'un DHCPDISCOVER, le serveur envoie un message DHCPOFFER afin d'attribuer une adresse IP à une station cliente. Lors de cette attribution, le serveur conserve cette adresse IP correspondant à l'adresse MAC de la station dans le fichier. Si l'adresse MAC n'est pas dans le fichier, on la rajoute et on y associe

l'adresse IP ainsi que l'ID de la transaction. Si elle s'y trouve déjà, il suffit de remplacer l'adresse IP correspondante par la nouvelle adresse IP à associer et le nouvel ID.

- Un logger nous permet de tracer les messages reçues et émises par le serveur. Différents évènements sont donc sauvegardés dans le fichier "journal.txt" : la réception d'un DCHPDISCOVER, DHCPREQUEST, DHCPDECLINE, l'émission d'un DHCP OFFER, DHCPACK, DHCPNAK ou encore lorsque le serveur doit faire fasse à une attaque de type « épuisement de ressources » qui entraîne une atteinte de la limite du nombre d'adresses attribuables.

4.3 Choix techniques

Plusieurs bibliothèques permettent le traitement de messages DHCP comme la bibliothèque scapy par exemple. Cependant, nous avons préféré construire nous même les messages afin d'avoir une manipulation directe des différents champs des messages et de les modifier à notre convenance, selon les informations dont nous disposons (par exemple la configuration du champ de bail, ou celui de l'adresse IP attribuée). Procéder de cette manière nous a aussi permis de comprendre plus aisément le fonctionnement des messages puisqu'il a fallu disséquer nous même chaque champ pour y comprendre leur utilité.

Finalement, pour vérifier le bon fonctionnement de notre serveur, nous nous sommes servis du logiciel Wireshark qui nous a permis de tracer les messages DHCP envoyées à notre serveur DHCP et émises par celui-ci.

5 Conclusion

Pour la réalisation de ce serveur DHCP remplissant toutes les fonctionnalités requises, nous avons dû manipuler et structurer les différents messages DHCP, ce qui nous a permis de mieux comprendre le protocole réseau DHCP. De plus, ce projet est une expérience supplémentaire pour la réalisation de travaux en équipe.