Protocoles réseaux
TD n° 6 : Protocole de configuration DHCP et routeurs NAT

Exercice 1 : DHCP

Le protocole DHCP sert à configurer automatiquement les paramètres de couche réseau d'un hôte : l'adresse IP de son interface réseau, le préfixe du lien attaché, adresse du serveur DNS, adresse d'une passerelle par défaut, etc. Il y a 76 options DHCP pour configurer plein de choses. Le protocole se déroule en quatre étapes :

1. le client DHCP envoie en *broadcast* un message `DHCPDISCOVER` ;
2. tous les serveurs DHCP répondent en unicast par un message `DHCPOFFER` avec l'IP qu'ils proposent au client ;
3. le client choisit un serveur, puis envoie en *broadcast* un message `DHCPREQUEST` ; avec sa nouvelle IP comme adresse d'émission
4. le serveur répond en unicast par un message `DHCPACK` avec tous les paramètres réseau affectés au client, la durée `lease_time` du bail (voir plus loin) et deux temps T1 < T2 < `lease_time` ; ou alors par un message `DHCPNAK` s'il décide de ne pas affecter ces paramètres.

1. On suppose qu'un client accepte les paramètres proposés par le premier serveur qui répond. Dessinez l'automate qui décrit le comportement de ce client.

2. On suppose qu'un client attend 2 secondes pour collecter toutes les offres de serveur avant d'en choisir une. Dessinez l'automate de ce client.

3. Aux étapes 2 et 4, le serveur envoie un unicast alors que le client n'a pas encore d'adresse. Commentaire ?

4. Le serveur DHCP inclus dans shncpd [1] évite ce problème en utilisant des *broadcasts* aux étapes 2 et 4. Qu'en pensez-vous ?

5. Le serveur DHCP maintient la liste des adresses affectées aux clients pour éviter d'affecter la même adresse à deux clients distincts. Que se passe-t-il s'il y a plusieurs serveurs sur le même lien ?

6. Que doit faire le serveur lorsqu'il envoie un `DHCPOFFER` ? Pourquoi le `DHCPREQUEST` de l'étape 3 est-il envoyé en broadcast ?

Lorsqu'il quitte le réseau, le client envoie un message `DHCPRELEASE` pour libérer l'adresse qui lui a été attribuée. Modifiez l'automate dessiné à la question 2 pour prendre en compte l'envoi de `DHCPRELEASE`. Le message `DHCPRELEASE` peut être perdu, ou le client peut quitter le réseau sans envoyer de `DHCPRELEASE` [2]. Pour éviter de perdre des adresses IP indéfiniment, les adresses sont louées (*leased*) au client pour un temps fini (de l'ordre de quelques heures ou quelques jours). Un client maintient un *timer* qui mesure le temps depuis lequel il a acquis un bail (*lease*). Lorsque le bail arrive à expiration, le client abandonne l'adresse et recommence à l'étape 1.

7. Modifiez l'automate de la question 2 pour prendre en compte la perte d'un bail.

Le protocole décrit à la question précédente fait que le client perd temporairement son adresse, et ne garantit pas la stabilité des adresses. Pour éviter ce problème, le comportement du client est le suivant :

5. au temps T1 (typiquement T1 = 50% lease_time), le client envoie un `DHCPREQUEST` unicast au serveur sélectionné. Si le serveur répond par un `DHCPACK`, le client repart pour une pleine durée de bail ; s'il répond par `DHCPNAK`, il recommence à l'étape 1 ;
6. en cas de non réponse à l'étape 5, alors au temps T2 (typiquement T2 = 87,5% lease_time), le client envoie un `DHCPDISCOVER` (broadcast) tout en conservant sa vieille adresse. Si un serveur répond par `DHCPOFFER`, le client peut envoyer un `DHCPREQUEST` tout en conservant sa vieille adresse. Si un serveur répond alors par `DHCPACK`, il abandonne l'ancienne adresse et s'affecte la nouvelle.
7. au temps lease_time, il abandonne l'adresse et recommence à l'étape 1.

8. Pourquoi les étapes 6 et 7 existent-elles ?

9. (S'il reste du temps) Modifiez l'automate de la question 2 pour qu'il implémente le protocole complet.

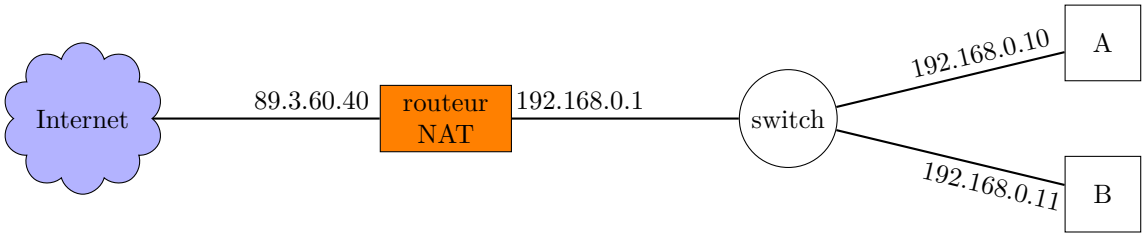
1. `https://github.com/jech/shncpd`
2. En fait, la plupart des clients DHCP n'envoient pas de `DHCPRELEASE`.

Exercice 2 : NAT

Un routeur NAT fait de la *traduction d'adresses*, il remplace des adresses IP par d'autres adresses IP. Dans cet exercice, on s'intéresse au cas d'un NAT dynamique avec traduction d'adresses et de numéros de ports. Un tel routeur NAT est **asymétrique** :

- il possède une IP publique sur une interface externe (connecté à Internet),
- il possède une IP privée sur une interface interne (connecté à un réseau local).

On considère la situation suivante, avec deux machines A et B sur un réseau local. On suppose que le CPE (*Customer Premises Equipment*, la « box » qui fait routeur NAT, routeur et serveur DHCP) a assigné à A et B des adresses IP et leur a donné l'adresse de la passerelle par défaut et le préfixe local.



1. Donnez la table de routage de A et B.
2. Supposons que le routeur NAT n'agisse que comme un routeur IP normal. Expliquez le problème si A essaye de communiquer avec un hôte C sur l'Internet.

Un routeur NAT dynamique maintient une table de traductions dont les entrées sont de la forme :

$$\text{IP privée : port privé} \rightarrow \text{IP publique : port public}$$

Au début la table est vide. L'algorithme du routeur NAT est le suivant. Lorsqu'il reçoit un paquet avec comme IP source X, port source p, IP de destination Y et port de destination q. Si le paquet arrive par **l'interface privée :**

1. chercher une entrée de la forme $X : p \rightarrow Y, r$ dans la table (r peut être quelconque),
2. s'il n'y en a pas, ajouter l'entrée $X : p \rightarrow Y : r$ avec $r = p$,
3. envoyer le paquet sur l'interface publique en remplaçant l'IP source par l'IP publique du routeur NAT et le port source par r.

Si le paquet arrive par **l'interface publique :**

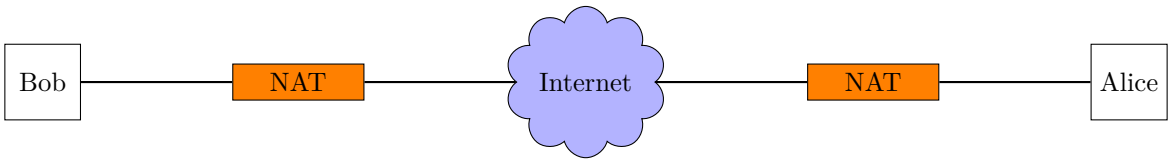
1. chercher une entrée de la forme $Z, r \rightarrow X, q$ dans la table (Z et r peuvent être quelconques),
2. s'il n'y en a pas, jeter le paquet,
3. sinon envoyer le paquet sur l'interface privée en remplaçant l'IP de destination par Z et le port de destination par r.

3. La table de traductions est mise à jour lorsque le NAT reçoit un paquet de données. Commentaire ?
4. A envoie un message (depuis le port 3000), à C (sur l'Internet, sur le port 80), qui lui répond. Détaillez ce qui se passe lorsque que les paquets traversent le NAT et donnez la table de traductions du routeur NAT.
5. B envoie maintenant un message (depuis le port 3000), à D (sur l'Internet, sur le port 80), qui lui répond. Détaillez ce qui se passe lorsque que les paquets traversent le NAT et donnez la nouvelle table de traductions du routeur NAT.
6. A envoie maintenant un message (depuis le port 3001), à C (sur l'Internet, sur le port 80), qui lui répond. Détaillez ce qui se passe lorsque que les paquets traversent le NAT et donnez la nouvelle table de traductions du routeur NAT.
7. B envoie maintenant un message (depuis le port 3001), à C (sur l'Internet, sur le port 80), qui lui répond. Détaillez ce qui se passe lorsque que les paquets traversent le NAT et expliquez pourquoi il y a un problème.

On modifie l'algorithme du routeur NAT de la façon suivante : au lieu d'ajouter bêtement une entrée $X : p \rightarrow Y : r$ avec $r = p$, comme ci-dessus, on choisit r de façon à ce qu'il n'apparaisse comme port public dans aucune entrée dont l'IP publique est Y.

8. Reprenez la question précédente et expliquez pourquoi cela marche. Quelle est la conséquence principale de cette astuce ?

On imagine la situation suivante, où Alice et Bob sont sur deux réseaux locaux connecté à l'Internet par des routeurs NAT dynamiques. Ils veulent jouer à un jeu vidéo qui nécessite l'un deux de lancer un serveur et l'autre un client.



9. Bob propose de lancer le serveur sur sa machine. Il dit à Alice de se connecter à 192.16.0.10 sur le port 3000. Alice lui dit que cela ne va pas marcher, pourquoi ?

10. Bob comprend son erreur, il trouve son IP publique et la donne à Alice. Celle-ci lance son client mais il ne parvient pas à se connecter, pouruqoi ?

11. Le serveur a justement option pour inviter un client en initiant la connexion depuis le serveur lorsqu'il est derrière un NAT. Bob entre l'IP publique et le port de Alice mais il ne parvient pas à inviter Alice, pourquoi ?

12. Clara, une de leur amie, leur propose de les aider en leur fournissant temporairement, uniquement pour initier la connexion, un hôte sur l'Internet qui n'est pas derrière un NAT. Voyez-vous en quoi cela peut être utile ? Est-ce que cela marche dans tous les cas ?

Parenthèse culturelle : la solution classique à ce problème est le « hole punching ». Elle est utilisée par tous les services de visioconférences pair-à-pair et jeux vidéo en ligne lorsqu'ils sont derrières un NAT.