

Routage NAT

I) Introduction

L'adresse IP (Internet Protocole) est un protocole qui permet d'identifier les machines et de router les informations sur Internet. Ces adresses sont codées sur 4 octets, soit 32 bits ; ce qui nous permet d'avoir 2^{32} adresses disponibles (un peu plus de 4 milliards d'adresses). D'ici peu, nous manquerons d'adresses disponibles.

En attendant un nouveau standard d'adressage permettant d'avoir plus d'adresses disponibles (IPv6= $3,4 \times 10^{38}$ adresses), il a fallu trouver des solutions temporaires. Le NAT a notamment été une réponse à cette future pénurie d'adresses.

Le routage NAT permet de faire de la translation d'adresse. Quand un paquet traverse le routeur NAT, l'adresse IP d'une machine dans le réseau local est échangée par l'une des adresses publiques du routeur. De ce fait, une machine avec une adresse privée (non routable sur Internet) pourra dialoguer avec une machine sur internet.

a) Plage d'adresses privées

Les adresses privées sont des adresses particulières, elles ne peuvent pas être utilisées sur Internet. Voici les plages d'adresses privées :

- plage de 10.0.0.0 à 10.255.255.255 pour la classe A;
- plage de 172.16.0.0 à 172.31.255.255 pour la classe B;
- plage de 192.168.0.0 à 192.168.255.255 pour la classe C.

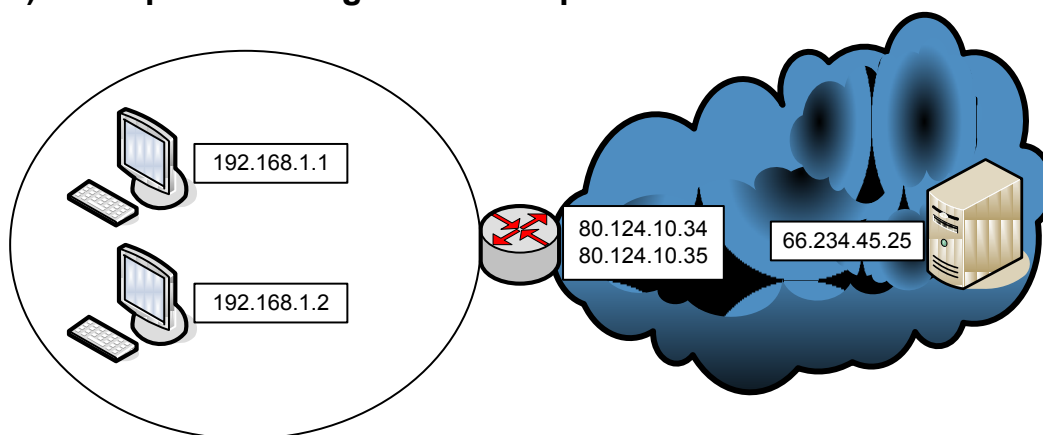
II) Le NAT statique

a) Principe

Une adresse IP Privée est associée une adresse IP publique. Par exemple : s'il y a trois machines dans le réseau local, il faudra trois adresses IP publiques. Pour 1000 machines, il faudra 1000 adresses IP publiques.

Dans ce cas, la seule action qui sera effectuée par le routeur sera de remplacer l'adresse privée l'adresse publique.

b) Exemple de routage NAT Statique



- Pour l'exemple suivant, compléter les tableaux suivants :

Table NAT du routeur :

@ IP Privée source	@ IP Publique source

1) Les PC envoient un paquet IP à destination du serveur WEB sur Internet.

Adresse IP des paquets entre Pc et routeur NAT	
IP source	IP destination

Adresse IP des paquets entre routeur NAT et serveur	
IP source	IP destination

2) Le serveur répond aux PC

Adresse IP des paquets entre serveur et routeur NAT	
IP source	IP destination

Adresse IP des paquets entre routeur NAT et PC	
IP source	IP destination

Seule l'association entre l'adresse privée et l'adresse publique est réalisée par le routeur NAT.

c) Avantages et inconvénients du NAT statique

- Avantages

Il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si l'on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche.

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible d'Internet.

- Inconvénients

On remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP...

III) Rappel sur les échanges entre clients et serveurs

Un numéro de port sert à identifier une application. On peut différencier deux types d'application : les applications serveur et cliente.

a) Application serveur

Dans le cas d'application serveur, le numéro de port sert à identifier le type de service. En effet, un serveur peut héberger plusieurs services. Pour que les clients contactent le bon service, ils doivent utiliser le bon port. A chaque service est associé un numéro de port. Ce numéro de port est généralement inférieur à 1024.

b) Application cliente

Dans le cas d'une application cliente, le numéro de port ne sert pas à identifier le type d'application mais l'application elle-même. C'est grâce à ce procédé que l'on peut ouvrir, par exemple, deux pages web sur un même site, sans que les réponses du serveur soient mélangées. Ce numéro est choisi au hasard parmi les ports libres et il est toujours supérieur à 1024.

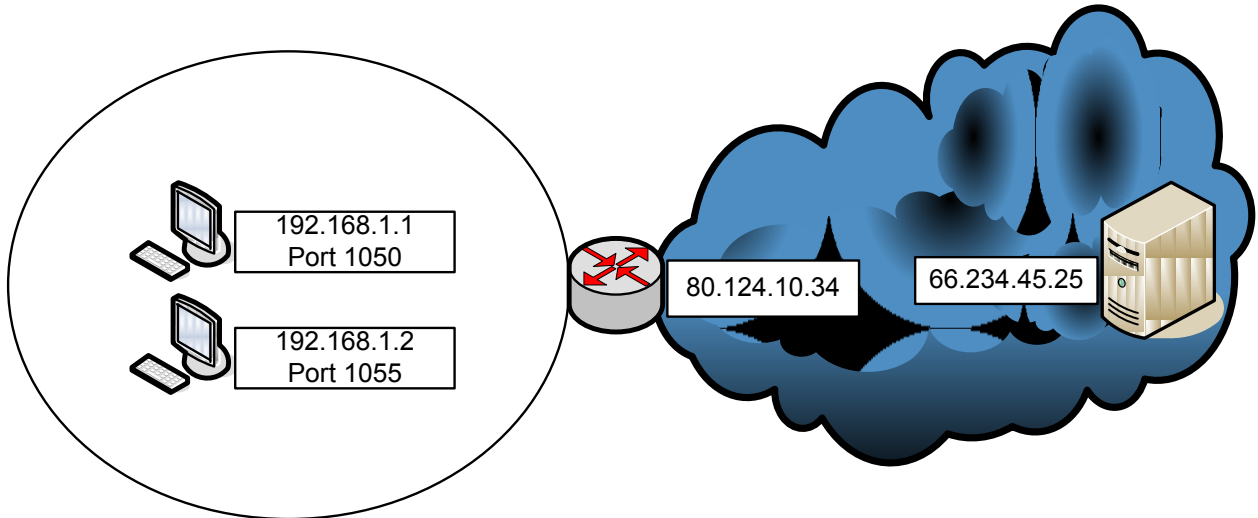
IV) Le NAT dynamique

a) Le principe

Le NAT dynamique est aussi appelé IP masquerading. Contrairement au NAT statique, on peut associer une adresse publique à plusieurs adresses privées et permettre ainsi à un grand nombre de machines ayant des adresses privées d'accéder à Internet.

Par contre, nous verrons que cette méthode possède quelques inconvénients. Contrairement au NAT statique, le routeur qui effectue le NAT devra à la fois modifier les adresses IP mais aussi les ports TCP/UDP (on appelle la modification des ports PAT, Port Address Translation).

b) Exemple de routage NAT dynamique



Pour l'exemple, compléter les tableaux suivants :

- 1) Les PC envoient un paquet IP à destination du serveur WEB sur Internet.

Numéro de port pour les paquets entre le Pc et le routeur NAT			
IP source	Port Source	IP destination	Port destination

Numéro de port pour les paquets entre le routeur NAT et le Serveur			
IP source	Port Source	IP destination	Port destination

Table NAT du routeur :

@ IP Privé source	Port source Privé	@ IP Publique source	Port source public	@ IP Publique Destination	Port destination public

- 2) Le serveur répond aux PCs

Numéros de ports pour les paquets entre le Serveur et le routeur NAT			
IP source	Port Source	IP destination	Port destination

Numéros de ports pour les paquets entre le routeur NAT et le PC			
IP source	Port Source	IP destination	Port destination

c) Avantages et inconvénients du NAT dynamique

- Avantages

Le NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet.

Etant donné que l'on peut "cacher" un grand nombre de machines derrière une seule adresse publique, cela permet de répondre à notre problème de pénurie d'adresses.

Les machines n'étant pas accessibles de l'extérieur, cela augmente un peu le niveau de la sécurité.

- Inconvénients

Le NAT ne permet pas d'être joint par une machine de l'Internet. Effectivement, si le NAT dynamique fonctionne, c'est parce que le routeur qui fait le NAT reçoit les informations de la machine en interne (Adresse IP, port TCP ou UDP). Le paquet arrivera, avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en interne.

- Conclusion

Le NAT dynamique ne permet donc que de sortir sur Internet, et non pas d'être joignable. Il est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible.

V) Statique ou dynamique ?

- Entourer la bonne réponse.

Rendre une application disponible sur Internet, (comme un serveur web, mail ou un serveur FTP.)

Nat Statique

Ajouter un petit plus en terme de sécurité.

Nat Dynamique

Economiser les adresses IP.

Nat Dynamique

Partager un accès à Internet à des machines qui n'ont pas besoin d'être joignables de l'extérieur.

Nat Dynamique

Peut-on combiner les deux méthodes ?

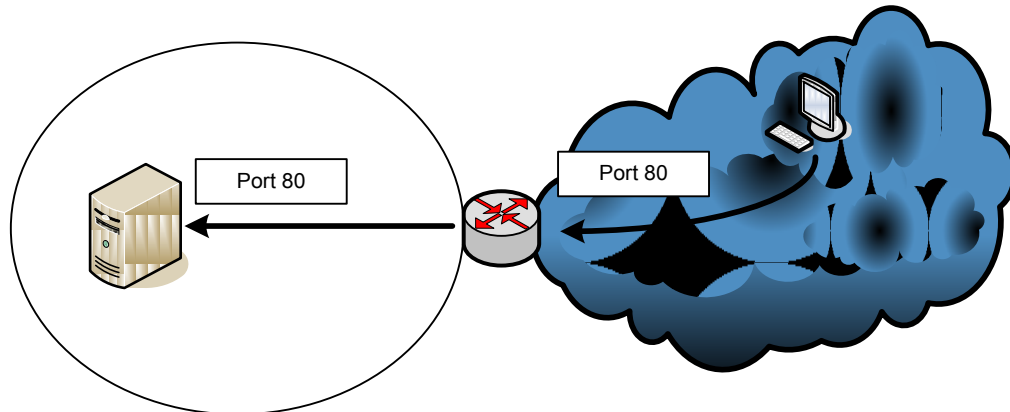
Oui

VI) *Rendre joignables les machines du réseau local avec une seule adresse publique.*

C'est notamment le cas quand on possède un accès ADSL ou câble, une seule adresse publique vous est fournie. Il devient alors compliqué de rendre disponibles plusieurs serveurs du réseau local. (exemple de la section SEN). Une solution à ce problème est le port forwarding.

a) **Le port forwarding.**

Le port forwarding consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet.



Exemple : Toutes les requêtes venant d'Internet à destination du port 80 de l'adresse publique du routeur, seront redirigés le port 80 de la machine à l'adresse privée 192.168.10.254.