Cours 44 : Network Address Translation (Partie 1)

Dans ce cours nous verrons le fonctionnement de NAT (Network Address Translation), qui est utilisé pour traduire la source et/ou l'adresse IP de destination d'un paquet vers une adresse IP différente.
Nous verrons tout d'abord les différents adressages d'adresses IP privée, puis nous verrons le fonctionnement de NAT, avec également le fonctionnement du NAT statique et de sa configuration.

IPV4 ne fournit pas assez d'adresses IP privées pour tous les appareils qui en ont besoin dans le monde, car il n'y en a pas suffisamment, la solution à long terme à ce problème est de changer le protocole vers l'IPv6. De changer toutes les adresses IPv4 disponibles en adresses IPv6 est une tâche compliqué, c'est pour cela qu'a été adopté 3 solutions à court terme :
1) CIDR (Classless Inter Domain Routing)
2) Les adresses IP privées
3) NAT

Le Request For Comment (RFC) 1918 spécifie le classement d'adressage IPv4 comme privée :
- Classe A : 10.0.0.0/8 (10.0.0.0 à 10.255.255.255)
- Classe B : 172.16.0.0/12 (172.16.0.0 à 172.31.255.255)
- Classe C : 192.168.0.0/16 (192.168.0.0 à 192.168.255.255)

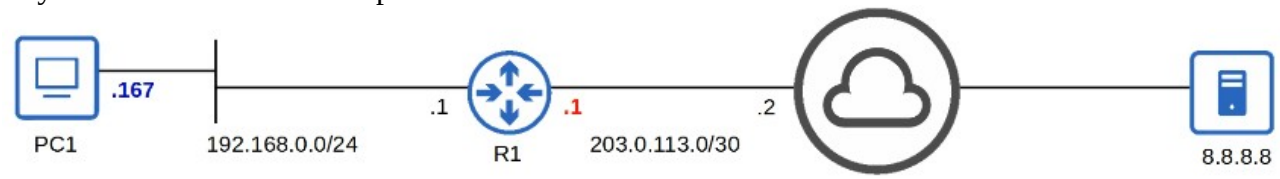
Il est permis d'utiliser le classement de ces adresses dans un réseau privée. Elles ne peuvent pas être utilisés de manière globale.
Un ordinateur connecté à un réseau utilise très probablement des adresses IP privées, par exemple comme on peut le voir ci dessous.

```
C:\Users\user>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.167
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

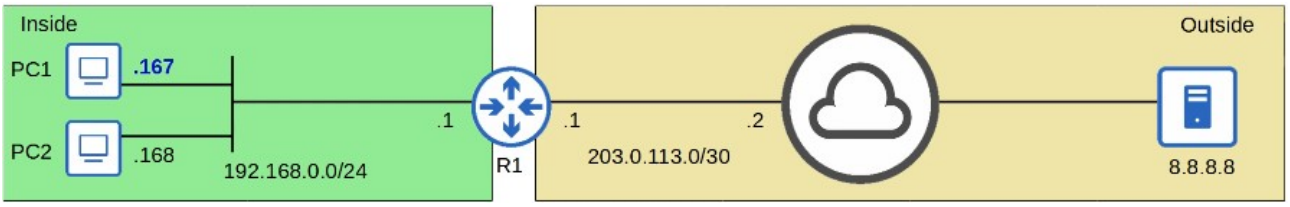
Les adresses IP privées ne peuvent pas être utilisés à travers Internet. L'ISP ne fournit pas de telles adresses.
Dans le réseau suivant, deux problèmes sont présent, premièrement les deux PC utilisent tout deux la même adresse IP, et deuxièmement les adresses IP privées ne peuvent pas être utilisés à travers Internet, donc les PC n'accéderont pas à Internet.

NAT permet de résoudre ces deux problèmes, car les routeurs pourront utiliser une adresse IP publique vers Internet. Bien que les adresses IP privées ne peuvent pas être unique, les adresses IP publiques peuvent l'être.

Network Address Translation (NAT) est utilisé pour modifier la source et/ou l'adresse IP de destination d'un paquet.
Il y a nombreuses raisons d'utiliser NAT, mais la raison la plus commune est pour permettre à un hôte avec une adresse IP privée de communiquer avec d'autre hôtes à travers Internet.
Voyons une démonstration rapide de NAT sur le réseau suivant :



Le PC1 veut communiquer avec le serveur pour cela il crée un paquet avec pour adresse IP source : 192.168.0.167 et pour adresse de destination : 8.8.8.8, il envoie le paquet à sa passerelle par défaut R1. C'est à ce moment que le NAT se passe, R1 traduit 192.168.0.167 en 203.0.113.1,
C'est pour cela que ce procédé est appelé source NAT, car il traduit l'adresse IP source, le routeur à ici traduit l'adresse IP privée par une adresse de sa propre interface.
R1 envoie ensuite le paquet vers l'adresse du serveur, ici 8.8.8.8
Le serveur envoie ensuite une réponse, avec l'adresse IP source : 8.8.8.8 et adresse IP de destination : 203.0.113.1, le paquet est ensuite traduit de la même façon que lors de la première requête.
Voyons à présent le fonctionnement de statique source NAT avec le réseau suivant :



Le NAT statique implique de configurer de manière statique en cartographiant une à une les adresses IP privées vers des adresses IP publiques.
Les adresses peuvent être traduite du publique vers le publique, ou du privée vers le privée, mais voyons comment est traduit une adresse du privée vers le publique.
Une adresse IP local intérieur est cartographié vers une adresse IP intérieur globale.
« Intérieur local » fait références aux adresses IP du réseau local. À l'opposé du « intérieur global » qui fait référence aux adresses IP du réseau externe des hôtes.
Par exemple le PC1 veut communiquer avec le serveur 8.8.8.8, il utilisera tout d'abord l'adresse intérieur local qui sera traduite par le routeur avec l'IP 100.0.0.1, le routeur envoie ensuite le paquet vers le serveur 8.8.8.8 qui lui envoie la réponse vers l'adresse IP publique du routeur R1.
Voyons à présent comment le PC2 communique avec le serveur, pour cela il aura besoin de sa propre adresse IP. Le routeur ne permet pas de pouvoir cartographier les adresses de PC1 et PC2 en utilisant le NAT statique car il lui faudra une seconde fois l'adresse 100.0.0.1, c'est pour cela qu'en configurant une deuxième adresse IP en NAT statique 100.0.0.2, le deuxième PC pourra communiquer avec le réseau extérieur.
Le NAT statique permet aux appareils avec une adresse IP privée de communiquer à travers Internet. Puisque cela requiert une cartographie d'adresse une par une cela ne permet pas de préserver les adresses IP.

Voyons comment configurer le NAT statique :

```
R1(config)#int g0/1
R1(config-if)#ip nat inside

R1(config-if)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit

R1(config)#ip nat inside source static 192.168.0.167 100.0.0.1
R1(config)#ip nat inside source static 192.168.0.168 100.0.0.2
R1(config)#exit

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---
```

On commence tout d'abord par définir l'interface « intérieur » connecté au réseau interne avec la commande :

```
R1(config)#int g0/1
R1(config)#ip nat inside
```

On définit l'interface « extérieur » connecté au réseau externe avec les commandes :

```
R1(config)#int g0/0
R1(config-if)#ip nat outside
```

On configure ensuite la cartographie des adresses IP avec les commandes :

```
R1(config)#ip nat inside source static 192.168.0.167 100.0.0.1
R1(config)#ip nat inside source static 192.168.0.168 100.0.0.2
```

Le format de la commande est : `ip nat inside` source static suivi de l'adresse ip local intérieur puis de l'adresse ip global intérieur

Pour afficher la configuration du nat on utilise la commande :

```
R1#show ip nat translations
```

On peut voir affiché le protocole utilisé ainsi que les adresses local extérieur et global extérieur, on remarque que les adresses du serveur se terminent toutes deux par :53, il s'agit du protocole DNS qui permet aux PC d'accéder au serveur.

Voyons d’autres commandes qui peuvent être utiles lorsque l’on utilise NAT :
Il est possible de retirer les adresses IP de traduction avec la commande :
`R1#clear ip nat translations *`

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---

R1#clear ip nat translation *

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 100.0.0.1          192.168.0.167      ---                 ---
--- 100.0.0.2          192.168.0.168      ---                 ---
```

La commande suivante permet d’afficher de manière plus détaillé les tables NAT de chaque interfaces
`R1#show ip nat statistics`

```
R1#show ip nat statistics
Total active translations: 2 (2 static, 0 dynamic; 0 extended)
Peak translations: 4, occurred 02:29:00 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 34  Misses: 0
CEF Translated packets: 30, CEF Punted packets: 4
Expired translations: 4
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```