TP4: Network Address Translation & Port Address Translation

Contexte

En IPv4, on distingue entre les adresses publiques et les adresses privés. Les Adresses publiques (routables) sont utilisées pour se connecter à Internet. Tant dit que les adresses privées (non routables) sont eux, utilisées en interne pour l'entreprise.

Adresses IP privées

Classe	Plage d'adresses	Notation CIDR
Classe A	10.0.0.0 - 10.255.255.255	10.0.0.0 /8
Classe B	172.16.0.0 - 172.31.255.255	172.16.0.0 /12
Classe C	192.168.0.0 - 192.168.255.255	192.168.0.0 /16

L'ensemble de ces adresses ne sont pas acheminées sur internet. Les routeurs Internet sont tous configurés pour éliminer toutes les adresses privées. C'est-à-dire, qu'elles ne sont pas routables sur internet. Lorsqu'un réseau qui utilise des adresses privées veut se connecter à Internet, il faudra, alors faire, une translation des adresses privées en adresses publiques.
Network Address Translation (NAT) (« traduction d'adresse réseau » ou « translation d'adresse réseau »). Ce processus, qui transforme les adresses privées en public, pour pouvoir aller sur internet, s'appelle le NAT. Et le périphérique réseau qui s'occupe du NAT est le routeur !

Adresse IP publique

Classe	Plage d'adresses		
Classe A	1.0.0.0 -> 9.255.255.255	et	11.0.0.0 - 126.255.255.255
Classe B	128.0.0.0 -> 172.15.255.255	et	172.32.0.0 - 191.255.255.255
Classe C	192.0.0.0 -> 192.167.255.255	et	192.169.0.0 – 223.255.255.255

Les adresses IP publiques sont utilisées sur des hôtes, qui doivent être accessibles au public depuis Internet.

Manque d'adresse IPv4

Avec la croissance rapide d'Internet, les adresses IP publiques viennent à manquer. C'est pourquoi de nouveaux mécanismes ont vu le jour comme :

- Le NAT
- Le CIDR
- Le VLSM
- L'IPv6

L'ensemble de ces mécanismes ont été développés pour pallier au problème du manque d'adresse IPv4. Dans ce TP l'objectif est de voir comment ça fonction le NAT.

Solution NAT

Les petits réseaux utilisent en général des adresses privées. Car elles offrent aux entreprises une grande flexibilité pour la conception de leurs réseaux. Cet adressage permet une administration plus pratique et une croissance plus facile. Mais par contre, avec des adresses privées, il n'est pas possible de surfer sur Internet. Et comme il n'y a pas assez d'adresses publiques pour équiper le réseau privé de toutes les

entreprises, la seule solution, c'est d'utiliser un mécanisme qui permet de traduire les adresses privées en adresses publiques. Et c'est le NAT qui permet de faire cette translation d'IP. Le NAT permet donc aux utilisateurs privés d'accéder à Internet en partageant une ou plusieurs adresses IP publiques.

Type d'adresse NAT

- Inside local : C'est l'adresse d'un l'hôte sur le réseau intérieur
- Inside globale : C'est l'adresse traduite à l'intérieur de l'adresse locale

Dans le fonctionnement du NAT :

- Le réseau intérieur est l'ensemble des réseaux soumis à la traduction.
- Le réseau extérieur est toutes les autres adresses.

Terme Cisco À connaitre

- L'Adresse Inside local : Ce sont les IP attribués aux Hosts, qui sont des adresses IP privées. Le terme Inside, signifie le réseau interne à l'entreprise !
- L'Adresse Inside Global : C'est la nouvelle adresse IP nattée de l'host, pour pouvoir aller sur le NET. Le routeur change l'adresse «inside local » par cette adresse « inside globale ». C'est généralement une adresse IP publique.
- L'Adresse Outside global : est l'adresse IP qui réside dans la partie extérieure du réseau. Elle représente donc l'adresse IP de destination que l'hôte interne souhaite joindre.
- L'Adresse Outside Local : est L' IP externe de l'hôte de destination. En principe, elle est identique à l'adresse « Outside globale ».

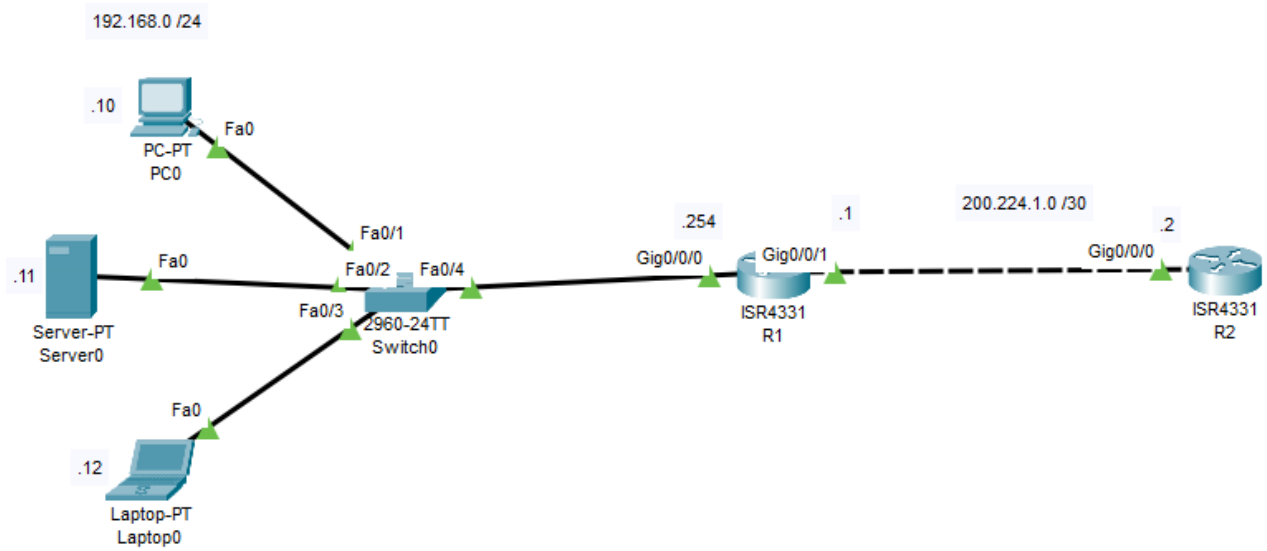
Les trois Catégories du NAT

- NAT statique : 1'adresse IP locale correspond à une seule adresse IP publique.
- NAT dynamique : Plusieurs adresses IP locales correspondent à plusieurs adresses IP publiques.
- PAT : Mappe plusieurs adresses privées vers une seule et même adresse publique en utilisant différents ports pour permettre de suivre la connexion.

Le PAT est également connu sous le nom de NAT OVERLOAD. C'est une forme de NAT dynamique. Il s'agit de l'utilisation la plus courante du NAT.

Topologie de travail

Nous allons essayer de travailler sur la topologie donnée dans la figure suivante pour configurer et tester les trois catégories de NAT



Les trois types de NAT

A-Nat Statique

Le NAT statique c'est un mappage une à une entre une adresse interne privée et une adresse externe publique. On peut comparer l'adresse interne à celle de notre PC à la maison, et l'adresse externe c'est l'IP public du box internet. Celle qui vous permet de surfer sur internet.

Configuration Nat statique sur R1

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shutdown
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#ip address 200.224.1.1 255.255.255.252
R1(config-if)#ip nat outside
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.10 200.224.1.10
R1(config)#ip nat inside source static 192.168.1.11 200.224.1.11
R1(config)#ip nat inside source static 192.168.1.12 200.224.1.12

Pour vérifier les configurations NAT du routeur, il faut utiliser la commande «show ip nat translation». Le NAT statique permet un mappage permanent entre une adresse interne et une adresse publique. C'est de la translation de une à une. Pour modélise l'accès à internet et la translation des adresses, le routeur R2 va nous indiquer les adresses utilisées lorsque on fait des Ping à son interface GigabitEthernet0.

On configure l'interface GigabitEthernet0 de R2 de la façon suivante
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2

R2(config)# interface GigabitEthernet0/0/0
R2(config-if)#ip address 200.224.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
Pour voir les messages ICMP arrivant sur le routeur R2, on utilise la commande CLI
R2# debug ip icmp

Puis il faut pinger 200.224.1.2 à partir des trois machines d'adresses 192.168.1.10, 192.168.1.11 et 192.168.1.12 vu du côté des routeurs R2 d'adresse 200.224.1.24 qui schématise l'internet, les messages icmp sont issues de 200.224.1.10, 200.224.1.11 et 200.224.1.12 globales et non du LAN privé. Notons qu'au niveau des machines il faut configurer la passerelle par défaut l'adresse de l'interface GigabitEthernet0/0/0 du routeur R1à savoir 192.168.1.254.
Cette méthode de NAT Statique sécurise les machines en interne en l'occurrence des serveurs dont des adresses globales sont associés par le NAT statique mais en réalité, se sont dans le LAN privé.

B-NAT dynamique

Le NAT dynamique permet de traduire des IP privés, vers des adresses publiques qui proviennent d'un pool d'IP. Sa configuration diffère un peu du NAT statique, mais il y'a tout de même beaucoup de similitudes. Comme pour le NAT statique, il faut identifier chaque interface comme une interface intérieure, dite «Inside» ou extérieure, dite «Outside».
Et ensuite, plutôt que de créer une carte statique d'une seule adresse IP, la translation se fera sur un groupe d'adresse interne globale.

Configuration NAT dynamique

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#ip address 200.224.1.1 255.255.255.248
R1(config-if)#ip nat outside
R1(config-if)#no shut
R1(config-if)#exit
R1(config)# acces-list 10 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat pool Dynamic_NAT 200.224.1.3 200.224.1.5 netmask 255.255.255.248
R1(config)#ip nat inside source list 10 pool Dynamic_NAT

Faites des pings sur le routeur R2(200.224.1. 2) à partir des machines ayant les adresses 192.168.1.10, 192.168.1.11 et 192.168.1.12 et voir les adresses utilisés en sortie. Vérifier les adresses translatées à partir des statistiques par la commande CLI sur le routeur R1 « show ip nat statistics ».

C-PAT : NAT Dynamique overload

L'une des principales formes du NAT est le PAT, qui se fait aussi appeler «*overload*». Plusieurs adresses locales internes peuvent être traduites en utilisant le NAT dans une ou plusieurs adresses globales internes. La plupart des boxes internet à domicile fonctionnent en PAT. Le fournisseur d'accès à internet attribue une adresse publique à la boxe, qui fonctionne comme un routeur, et plusieurs personnes peuvent surfer sur Internet à partir d'une seule et même adresse publique. Avec le PAT plusieurs adresses peuvent être traduites en une ou plusieurs adresses grâce à un numéro de port TCP

ou UDP qui seront attribués automatiquement et aléatoirement sur chaque adresse privée.

Configuration PAT

Pour la configuration du PAT, et comme toute sorte de nat, il faut taguer les interfaces en entrée et sortie. Ensuite, comme pour le nat dynamique, il faut créer une acess-list pour définir les adresses locales qui pourront être translatées. Et pour finir, il faut indiquer au routeur de translater notre access-list, à travers notre interface sortie, interface GigabitEthernet1, avec la commande «ip nat inside». Ne pas oublier le petit mot «overload» à la fin de la commande.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#ip address 200.224.1.1 255.255.255.252
R1(config-if)#ip nat outside
R1(config-if)#no shut
R1(config-if)#exit
R1(config)# acces-list 10 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 10 interface GigabitEthernet0/0/1 overload
```

Au lieu d'utiliser une interface de sortie0/0/1, on peut à la place utiliser un pool d'adresse de sortie qui contient une seule adresse (200.224.1.1 par exemple) comme suit

```
R1(config)#ip nat pool PAT_pool 200.224.1.1 200.224.1.1 netmask 255.255.255.255
R1(config)#ip nat inside source list 10 pool PAT_pool overload
```

Les commandes CLI suivantes aident à voir clairement ce que le routeur est en train de translater

Commande CLI	**Interprétation**
show ip nat translations	Affiche la table nat du routeur
show access-list	Vérifie que l'ACL associée à la commande NAT comprend bien l'ensemble des réseaux qui doivent être nattés
show ip nat statistics	Permets de vérifier que les interfaces du routeur sont correctement définies en inside et outside
clear ip nat translation	Permets d'effacer toutes les entrées des adresses translatées dynamiquement. Par défaut, elle s'efface après 24 heures