


Faculté des Sciences et Techniques
Marrakech



جامعة المراكش
UNIVERSITE UAM MARRAKECH
FACULTE DES SCIENCES ET TECHNIQUES - MARRAKECH

NAT (Network Address Translation)

Pr. M. AIT HEMAD
ait.hemad.m@gmail.com

Introduction

- Pour pallier la pénurie d'adresses IPv4
 - Utilisation des VLSM
 - Et/ou utilisation du NAT (Network Address Translation)

Introduction

- Origine du NAT :
 - Difficulté à obtenir suffisamment d'adresse IP pour un réseau local, coût de ces adresses IP.
 - Carence d'adresses IPv4
- Idée : Faire correspondre à n adresses externes publiques visibles sur Internet à toutes les adresses d'un réseau privé (non uniques et non routables)

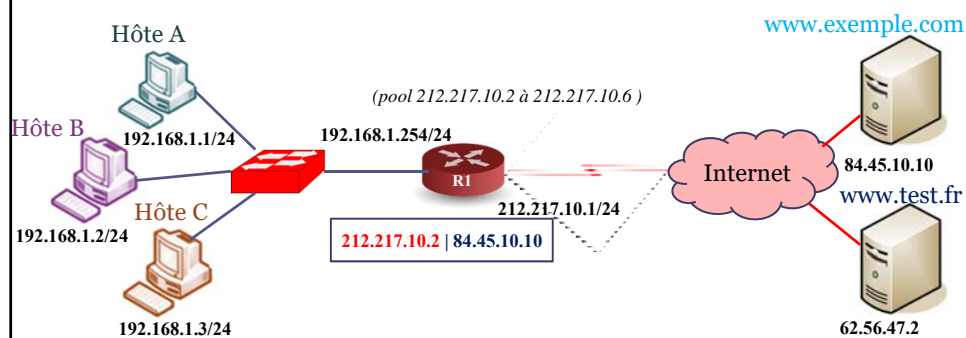
NAT : Définition

- Le NAT permet d'attribuer des adresses privées aux machines internes du réseau, et cependant de leur permettre d'accéder à Internet

Principe du NAT

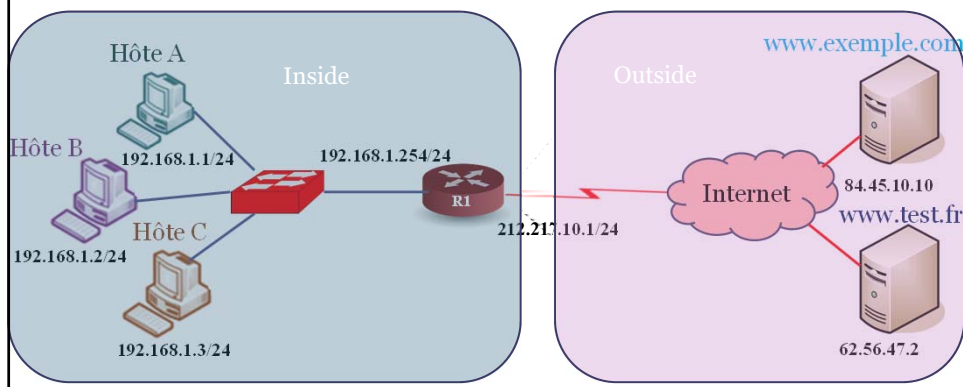
- Le routeur NAT de sortie va modifier l'entête IP de tout paquet provenant d'une machine locale interne en remplaçant l'adresse source IP privée par une adresse publique globale unique avant d'envoyer les paquets vers le réseau externe

NAT : Exemple



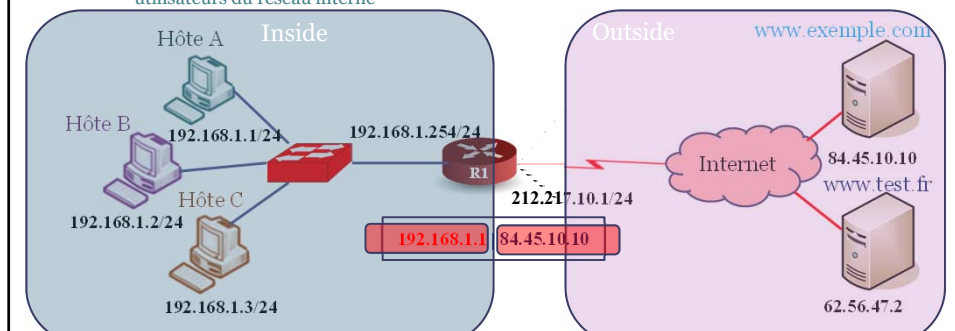
Terminologie de Cisco

- Inside / outside



Terminologie de Cisco

- Cisco définit les termes suivant pour la configuration du NAT
 - Adresse locale interne : adresse IP de l'hôte sur le réseau privé
 - Adresse globale interne : adresse IP publique derrière laquelle se trouve le réseau privée
 - Adresse globale externe : adresse IP publique extérieure au réseau privé
 - Adresse local externe : Adresse IP d'un hôte du réseau externe telle qu'elle est connue par les utilisateurs du réseau interne



Types de NAT

- Deux types de NAT :
 - Statique : la correspondance adresse Privée / adresse publique est fixe.
 - Dynamique : elle peut changer dans le temps

NAT statique

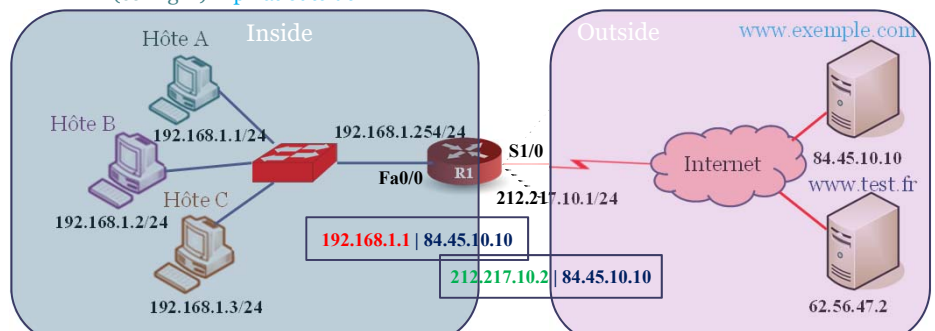
- Fonctionne à l'aide d'une table statique
 - la correspondance adresse privée / adresse publique est fixe
 - A chaque adresse privée correspond à une adresse publique
- Utilisé pour des serveurs locaux devant être accessible de l'Internet

Configuration NAT statique Cisco

- En mode de configuration globale
 - Routeur(config)# **ip nat inside source static** *local-ip global-ip*
- Sur l'interface interne (LAN)
 - Routeur(config-if)# **ip nat inside**
- Sur l'interface externe (WAN)
 - Routeur(config-if)# **ip nat outside**

Configuration NAT statique : Exemple

- R1(config)# **ip nat inside source static** 192.168.1.1 212.217.10.2
- R1(config)# interface Fa0/0
- R1(config-if)# **ip nat inside**
- R1(config)# interface S1/0
- R1(config-if)# **ip nat outside**

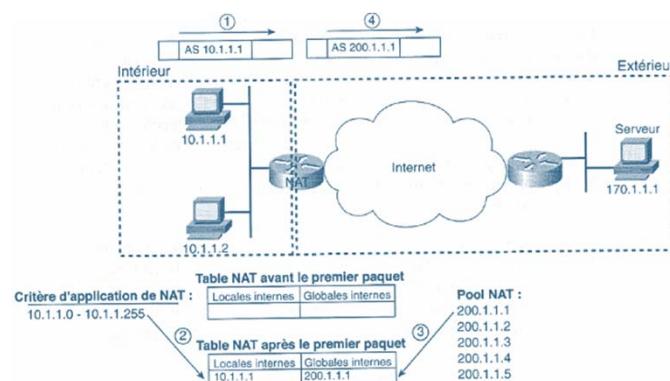


NAT dynamique

- Appelée aussi IP masquerading
- Permet d'attribuer (associer) dynamiquement lors des connexions des adresses IP publiques aux adresses privées
- Problème : comment le routeur se rappelle-t-il des correspondances ?
 - La configuration définit un pool d'adresses globales internes et des critères pour désigner l'ensemble des adresses locales internes qui doivent être remplacées.

NAT dynamique

- Pool d'adresses publiques NAT allouées à la demande



Configuration NAT dynamique Cisco

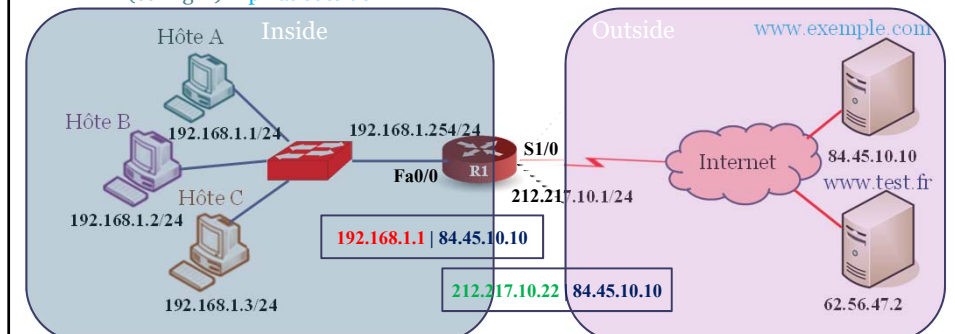
- Créer un pool de mappage
 - Router(config)#ip nat pool *nom-du-pool* start-ip *end-ip* netmask *netmask*
- Définir une ACL pour indiquer qui aura le droit d'être traduit
 - Routeur(config)# access-list *numéro* permit *adresse-ip* masque-générique

Configuration NAT dynamique Cisco

- Créer le mappage
 - Routeur(config)# ip nat inside source list *numéro-acl* pool *nom-du-pool*
- Sur l'interface locale (LAN)
 - Routeur(config-if)# ip nat inside
- Sur l'interface sortante (WAN)
 - Routeur(config-if)# ip nat outside

Configuration NAT dynamique: Exemple

- R1(config)# `ip nat pool test 212.217.10.20 212.217.10.30 netmask 255.255.255.0`
- R1(config)# `access-list 20 permit 192.168.1.0 0.0.0.255`
- R1(config)# `ip nat inside source list 20 pool test`
- R1(config)# `interface Fa0/0`
- R1(config-if)# `ip nat inside`
- R1(config)# `interface S1/0`
- R1(config-if)# `ip nat outside`

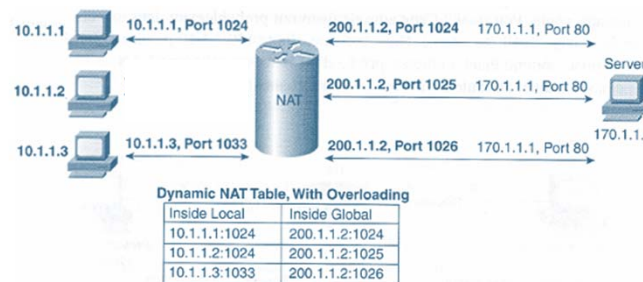


Traduction PAT (overloading)

- Dans la traduction NAT dynamique, il faut avoir suffisamment d'adresses publiques pour assurer une bonne connectivité des postes clients.
 - Autant d'adresses publiques que de clients (adr. privées) connectés en même temps.
 - Adapté à une utilisation de type « roulement ».
 - Pb si le nombre d'adresses publiques disponibles est inférieur à celui des clients à servir.
- L'overloading, ou traduction PAT (Port Address Translation), permet à NAT de mieux s'adapter à l'augmentation des clients Internet d'une entreprise, au moyen de quelques adresses publiques seulement.

Overloading (PAT)

- Pour servir une grande quantité d'adresses locales internes à l'aide d'une ou quelques adresses globales internes enregistrées, la traduction étendue PAT emploie les ports en plus de l'adresse

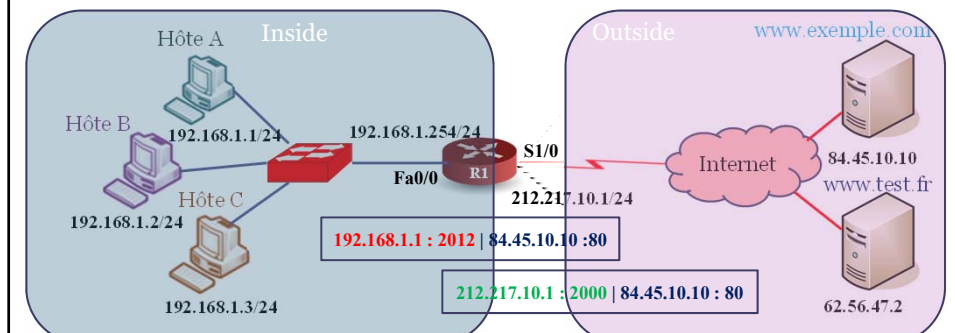


PAT avec 1 seule adresse publique

- Adresses locales soumises au NAT
 - Routeur(config)# *access-list numéro permit adresse-ip masque-générique*
- Définition du NAT
 - Routeur(config)# *ip nat inside source list numéro-acl interface type number overload*
- Sur l'interface locale (LAN)
 - Routeur(config-if)# *ip nat inside*
- Sur l'interface sortante (WAN)
 - Routeur(config-if)# *ip nat outside*

PAT avec 1 seule adresse publique

- R1(config)# `access-list 10 permit 192.168.1.0 0.0.0.255`
- R1(config)# `ip nat inside source list 10 interface S1/o overload`
- R1(config)# `interface Fa0/0`
- R1(config-if)# `ip nat inside`
- R1(config)# `interface S1/0`
- R1(config-if)# `ip nat outside`



Port Forwarding (redirection de port)

- Inconvénient du PAT : on ne peut pas initier une connexion depuis l'extérieur car on ne connaît pas le port source réel (impossible d'avoir un serveur WEB par exemple dans l'Intranet)
- Solution : port forwarding
 - Le port forwarding consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet.
 - Ainsi, lorsque l'on n'a qu'une seule adresse publique avec plusieurs machines derrière en adressage privé, on peut initialiser une connexion de l'extérieur vers l'une de ses machines (une seule par port TCP/UDP)

Port Forwarding et port mapping

- On met en dur dans la table NAT du routeur
 - port fixe: port privé/ adresse privée
 - Exemple : la machine 10.0.0.1 possède un serveur Web.
- Port Forwarding 80: 80/10.0.0.1
 - Les paquets arrivant de l'extérieur vers le routeur 195.0.0.254:80 seront redirigés vers 10.0.0.1:80
- Pb si deux serveurs Web sur 2 machines différentes
 - Le "port mapping" consiste à mapper le port de la machine interne à un port fixe différent
 - Ex : 8080:80/10.0.0.2 et serveur Web sur 10.0.0.2



Port Forwarding avec Cisco

- Configuration :


```
ip nat inside source static { tcp | udp } <localaddr>
<localport> <globaladdr> <globalport>
```
- Exemple
 - `ip nat inside source static tcp 10.0.0.1 80 195.0.0.254 80`
 - `ip nat inside source static tcp 10.0.0.2 80 195.0.0.254 8080`
- Dans cet exemple, les paquets arrivants depuis l'extérieur sur le port 80 sont envoyées au port 80 de la machine 10.0.0.1, et ceux arrivants depuis l'extérieur sur le port 8080 sont envoyées au port 80 de la machine 10.0.0.2