# Translation d'adresses NAT/PAT
# Network Address Translation

Xavier Merrheim

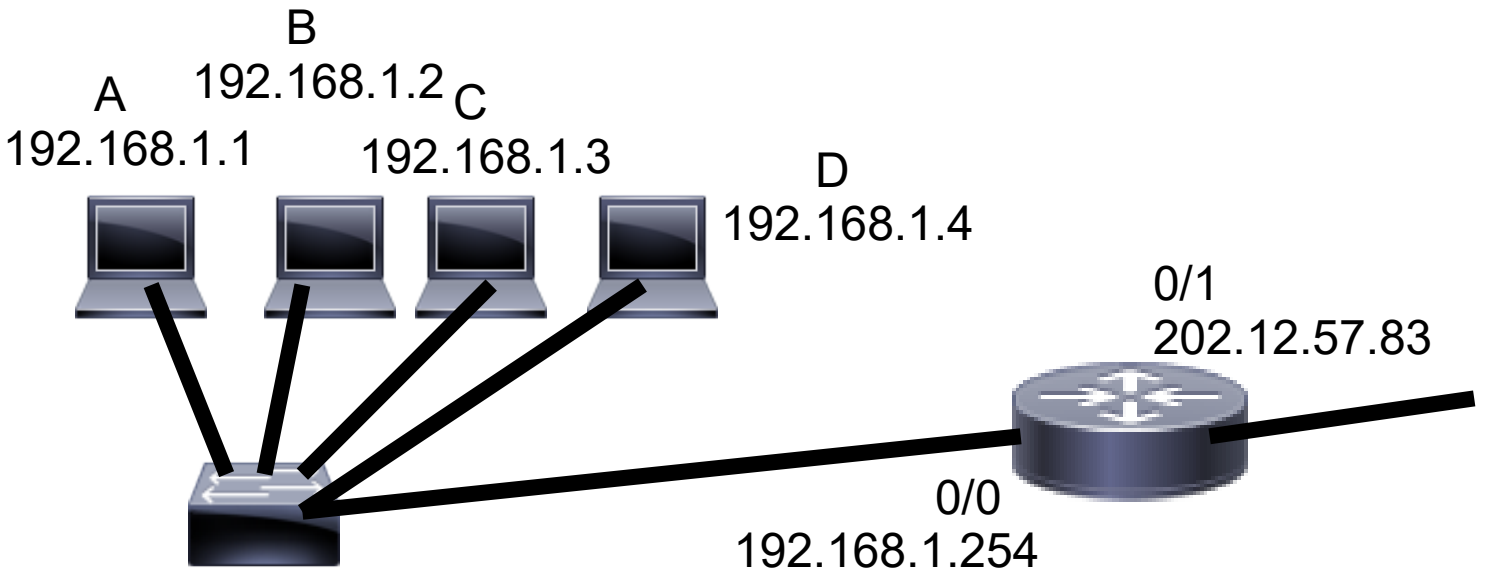
# Translation d'adresses NAT

- La translation d'adresses est un dispositif où les machines communiquent en interne au sein d'un réseau privé en utilisant une adresse privée.
- Lorsqu'une machine communique avec internet, on lui attribue une adresse publique à la volée, le processus étant transparent pour la machine.
- Ce dispositif est en général assuré par un routeur.
- Il permet d'économiser des adresses IP publiques et améliore également la sécurité.

# Différentes variantes NAT ou PAT

- Il existe différentes variantes :
  - Nous parlerons de NAT lorsqu'on fournit au routeur une liste d'adresses publiques utilisables pour communiquer sur Internet.
  - Nous parlerons de PAT lorsque le routeur utilise une seule adresse IP publique qu'il partage avec tout le réseau privé.

# NAT




Internet

Serveur S
201.17.87.67

**Réseau public**

Routeur R
NAT
Pool d'adresses :
de 200.29.1.1 à 200.29.1.254

**Réseau privé**

192.168.1.0 /24

# Réseau privé

- Sur le réseau privé on utilise des adresses réservées qui sont interdites sur Internet.
- Ces adresses appartiennent aux réseaux 10.0.0.0 /8 ou 172.16.0.0 /12 ou 192.168.0.0
- Pour notre exemple, il y a 4 machines A, B, C et D sur le réseau privé et celui-ci est le réseau 192.168.1.0 /24

# Pool d'adresses publiques

- Le routeur a à sa disposition un pool d'adresses publiques qu'il va utiliser pour permettre au réseau privé de communiquer avec Internet.
- Ici on imagine qu'on utilise le pool d'adresses de 200.29.1.1 à 200.29.1.254

# Fonctionnement (1)

- Imaginons que la machine C d'adresse IP privée 192.168.1.3 communique avec un serveur S situé sur Internet d'adresse IP publique 201.17.87.67.
- C va envoyé un datagramme IP avec
  - adresse IP source : 192.168.1.3
  - adresse IP destination : 201.17.87.67
- Ce datagramme va être envoyé au routeur R

# Fonctionnement (2)

- Le routeur va s'apercevoir qu'une machine du réseau privé veut communiquer avec une machine du réseau public. Il est interdit d'utiliser une adresse privée telle que 192.168.1.3 sur internet.
- Le routeur va choisir dans le pool d'adresses publiques une adresse disponible par exemple 200.29.1.12

# Fonctionnement (3)

- Le routeur va changer l'adresse IP source du datagramme IP qu'il vient de recevoir.
- Ce datagramme aura donc les caractéristiques suivantes :
  - adresses IP source : 200.29.1.12
  - adresse IP destination : 201.17.87.67
- Ce datagramme va être envoyé sur Internet et va arriver jusqu'au routeur.

# Fonctionnement (4)

- Le routeur va mémoriser dans la table de translation la correspondance

| IP privée | IP publique |
| --- | --- |
| 192.168.1.3 | 200.29.1.12 |

# Fonctionnement (5)

- S va recevoir ce datagramme IP. L'adresse IP source est 200.29.1.12.
- Il va donc envoyer une réponse avec les caractéristiques suivantes :
  - adresse IP source : 201.17.87.67
  - adresse IP destination : 200.29.1.12
- Ce datagramme va arriver jusqu'au routeur R

# Fonctionnement (6)

- Le routeur va s'apercevoir qu'un datagramme venant du réseau public veut communiquer avec une machine du réseau privé.
- L'adresse IP destination de ce datagramme est 200.29.1.12
- Il va rechercher dans la table de translation l'adresse privée correspondant à l'adresse publique 200.29.1.12. Il va obtenir 192.168.1.3.

# Fonctionnement (7)

- Le routeur va changer l'adresse IP de destination du datagramme et la remplacer par 192.168.1.3.
- Ce datagramme aura donc comme caractéristique :
  - adresse IP source : 201.17.87.67
  - adresse IP destination : 192.168.1.3
- Ce datagramme va être envoyé sur le réseau privé et va arriver jusqu'à C.

# Point de vue de C

- C a envoyé un datagramme IP avec comme caractéristique :
  - adresse IP source : 192.168.1.3
  - adresse IP destination : 201.17.87.67
- C a reçu en retour un datagramme IP avec comme caractéristique :
  - adresse IP source : 201.17.87.67
  - adresse IP destination : 192.168.1.3
- C a donc l'illusion qu'avec son adresse IP privée, il peut communiquer avec tout Internet.
- Remarque : C ne connait pas son adresse publique !

# Point de vue du serveur S

- S a reçu un datagramme IP avec comme caractéristique :
  - adresse IP source : 200.29.1.12
  - adresse IP destination :  201.17.87.67
- S a envoyé en retour un datagramme IP avec comme caractéristique :
  - adresse IP source : 201.17.87.67
  - adresse IP destination : 200.29.1.12
- S a donc l'illusion qu'il a communiquer avec une machine d'adresse IP 200.29.1.12
- Remarque : S ne connait pas l'adresse privée de C !

# Economie d'adresse IP

- Si le pool d'adresses est plus petit que le nombre de machines de réseau privé, on économise des adresses IP publiques.
- Attention toutefois au risque qu'une machine ne puisse pas communiquer sur internet en raison du manqque d'adresses publiques.

# Amélioration de la sécurité

- Si on dit, par exemple,  au routeur de ne pas attribuer d'adresse publique la machine 192.168.1.4 celle-ci ne pourra pas communiquer avec Internet.
- En revanche, il sera difficile de l'attaquer à partir d'Internet !

# Commandes CISCO (1)

- Imaginons que R soit un routeur CISCO.
- Pour chaque interface du routeur, il faudra indiquer si elle est connectée au réseau public ou privé.
- Dans le mode config-if, on tapera :
  - **ip nat inside** si l'interface est connectée au réseau privé
  - **ip nat outside** si l'interface est connectée au réseau public

# Commandes CISCO (2)

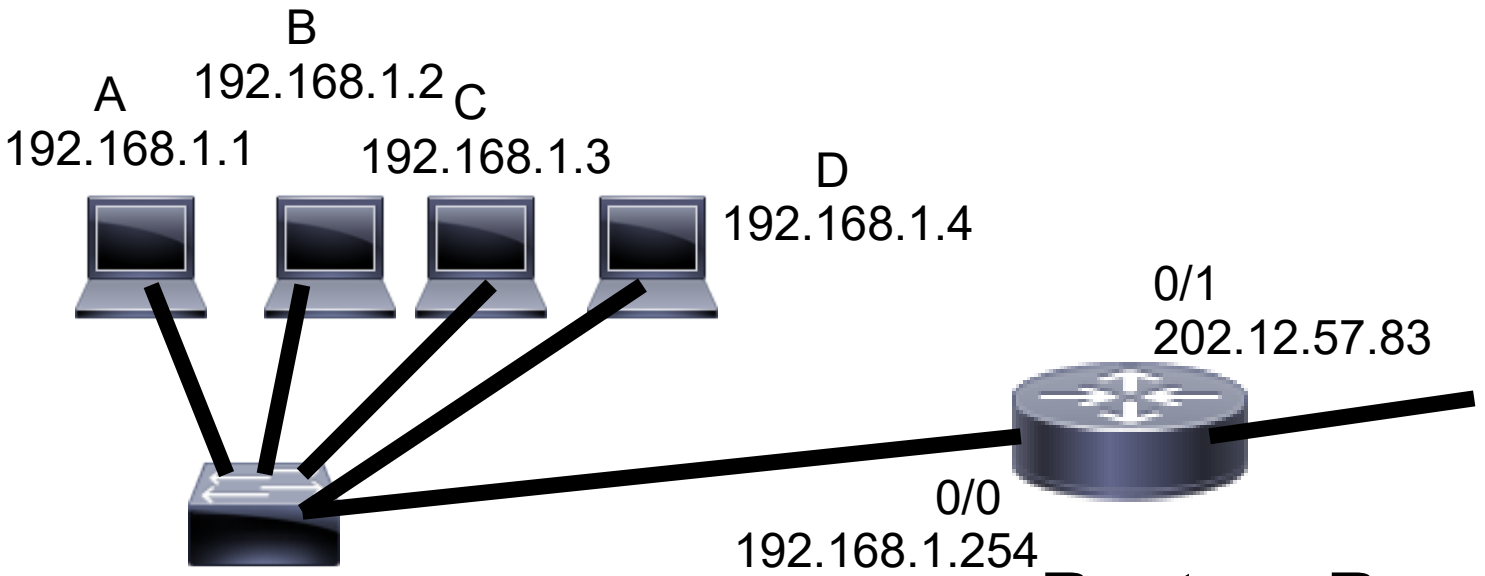
Pour la translaation d'adresses, il faudra procéder en 3 étapes :

- Définir une access-list définie par un numéro regroupant toutes les adresses du réseau privé
- Définir un pool d'adresses en indiquant la première et la dernière adresse du pool
- Associer l'access-list au pool.

# Configuration de R

```
enable
configure terminal
interface fastethernet 0/0
ip address 192.168.1.254 255.255.255.0
ip nat inside
no shutdown
exit
interface fastethernet 0/1
ip address 202.12.57.83 255.255.255.0
ip nat outside
no shutdown
exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool toto 200.29.1.1 200.29.1.254 netmask 255.255.255.0
ip nat inside source list 1 pool toto
exit
disable
```

# PAT




Internet

Serveur S
201.17.87.67

**Réseau public**

Routeur R
PAT

**Réseau privé**

192.168.1.0 /24

# Plus de pool

- La translation d'adresses de type PAT n'utilise plus un pool d'adresse publique.
- Toutes les machines du réseau privé vont utiliser l'adresse publique de R ici 202.12.57.83
- Pour distinguer les machines du réseau privé, on utilisera les ports TCP

# Fonctionnement (1)

- Imaginons que la machine C d'adresse IP privée 192.168.1.3 communique avec un serveur web S situé sur Internet d'adresse IP publique 201.17.87.67.
- C va envoyé un datagramme IP avec
  - adresse IP source : 192.168.1.3
  - port TCP source 2000
  - adresse IP destination : 201.17.87.67
  - Port TCP destination : 80
- Ce datagramme va être envoyé au routeur R

# Fonctionnement (2)

- Le routeur va s'apercevoir qu'une machine du réseau privé veut communiquer avec une machine du réseau public.
- Le routeur va choisir un port TCP libre pour l'adresse IP publique 202.12.57.83

# Fonctionnement (3)

- Le routeur va changer l'adresse IP source et le port TCP source du datagramme IP qu'il vient de recevoir.
- Ce datagramme aura donc les caractéristiques suivantes :
  - adresses IP source : 202.12.57.83
  - Port TCP source 3000
  - adresse IP destination : 201.17.87.67
  - Port TCP desstination 80
- Ce datagramme va être envoyé sur Internet et va arriver jusqu'au routeur.

# Fonctionnement (4)

- Le routeur va mémoriser dans la table de translation la correspondance

| protocole-IP privée-port | protocole-IP publique-port |
| --- | --- |
| TCP 192.168.1.3:2000 | TCP 202.12.57.83:3000 |

# Fonctionnement (5)

- S va recevoir ce datagramme IP.
- Il va donc envoyer une réponse avec les caractéristiques suivantes :
  - adresse IP source : 201.17.87.67
  - port TCP source 80
  - adresse IP destination : 202.12.57.83
  - Port TCP destination 3000
- Ce datagramme va arriver jusqu'au routeur R

# Fonctionnement (6)

- Le routeur va s'apercevoir qu'un datagramme venant du réseau public veut communiquer avec une machine du réseau privé.

- Il va rechercher dans la table de translation l'adresse privée et le port de TCP correspondant à TCP 202.12.57.83:3000
- Il va obtenir  TCP 192.168.1.3:2000

# Fonctionnement (7)

- Le routeur va changer l'adresse IP de destination et le port TCP du datagramme.
- Ce datagramme aura donc comme caractéristique :
  - adresse IP source : 201.17.87.67
  - port TCP source 80
  - adresse IP destination : 192.168.1.3
  - port TCP destination 2000
- Ce datagramme va être envoyé sur le réseau privé et va arriver jusqu'à C.

# Commandes CISCO (2)

Pour la translaation d'adresses, il faudra procéder en 3 étapes :

- Définir une access-list définie par un numéro regroupant toutes les adresses du réseau privé
- Définir un pool d'adresses en indiquant la première et la dernière adresse du pool
- Associer l'access-list au pool.

# Commandes CISCO PAT

Pour la translation d'adresses, il faudra procéder en 2 étapes :

- Définir une access-list définie par un numéro regroupant toutes les adresses du réseau privé
- Associer l'access-list au l'interface en utilisant le mot clé overload.

# Commandes CISCO (2)

Pour la translaation d'adresses, il faudra procéder en 3 étapes :

- Définir une access-list définie par un numéro regroupant toutes les adresses du réseau privé
- Définir un pool d'adresses en indiquant la première et la dernière adresse du pool
- Associer l'access-list au pool.

# Configuration de R

```
enable
configure terminal
interface fastethernet 0/0
ip address 192.168.1.254 255.255.255.0
ip nat inside
no shutdown
exit
interface fastethernet 0/1
ip address 202.12.57.83 255.255.255.0
ip nat outside
no shutdown
exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface fastethernet 0/1 overload
exit
disable
```

# Economie d'adresses IP

- On n'utilise qu'une seule adresse IP publique

# Limitation

- Il y a au total $2^{16}$=65536 ports TCP
- Toutes les machines du réseau privé se partagent ces ports.
- Il est envisageable d'avoir une centaine de machines sur le réseau privé (il y aura 655 ports TCP par machines) mais pas des milliers sinon le nombre de ports TCP sera insuffisant.

# Conclusion

- PAT et NAT a permis d'économiser les adresses IP.
- Il a été indispensable à cause de la pénurie d'adresses IP version 4
- Il a retardé la migration vers IP version 6 !
- Il y a tant d'adresses IP version 6, qu'il n'est pas recommandé d'utiliser NAT/PAT dans cette version d'IP.