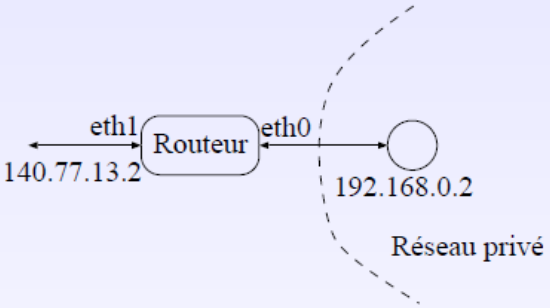
FILTER (filtrage des paquets)		NAT (translation d'adresses)	
INPUT	paquet entrant sur le routeur	PREROUTING	NAT de destination
OUTPUT	paquet émis par le routeur	POSTROUTING	NAT de source
FORWARD	paquet traversant le routeur	OUTPUT	NAT sur les paquets émis localement

Fonctionnalités NAT d'Iptables

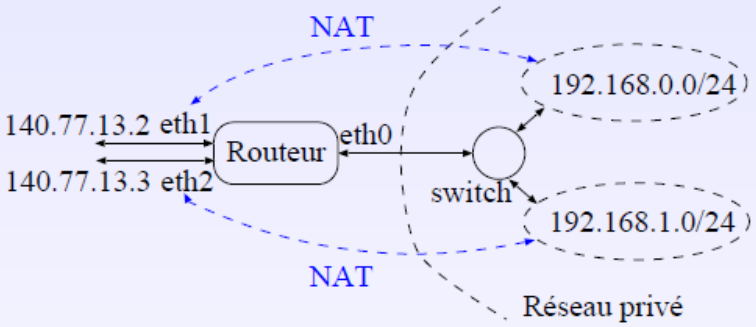


Modification de la destination du paquet avant le routage (paquet reçu de l'extérieur).

```
iptables -t nat -A PREROUTING -d 140.77.13.2 -i eth1 -j DNAT
-to-destination 192.168.0.2
```

Modification de la source du paquet après le routage (paquet émis à partir du réseau privé).

```
iptables -t nat -A POSTROUTING -s 192.168.0.2 -o eth1 -j
SNAT -to-source 140.77.13.2
```



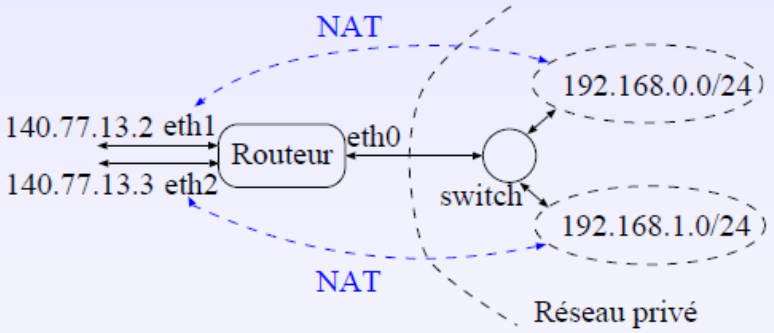
Association entre toutes les adresses privées du sous-réseau 192.168.0.0/24 avec l'interface eth1.

```
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j
MASQUERADE
```

Association entre toutes les adresses privées du sous-réseau 192.168.1.0/24 avec l'interface eth2.

```
iptables -t nat -A POSTROUTING -o eth2 -s 192.168.1.0/24 -j
MASQUERADE
```

Transfert de ports

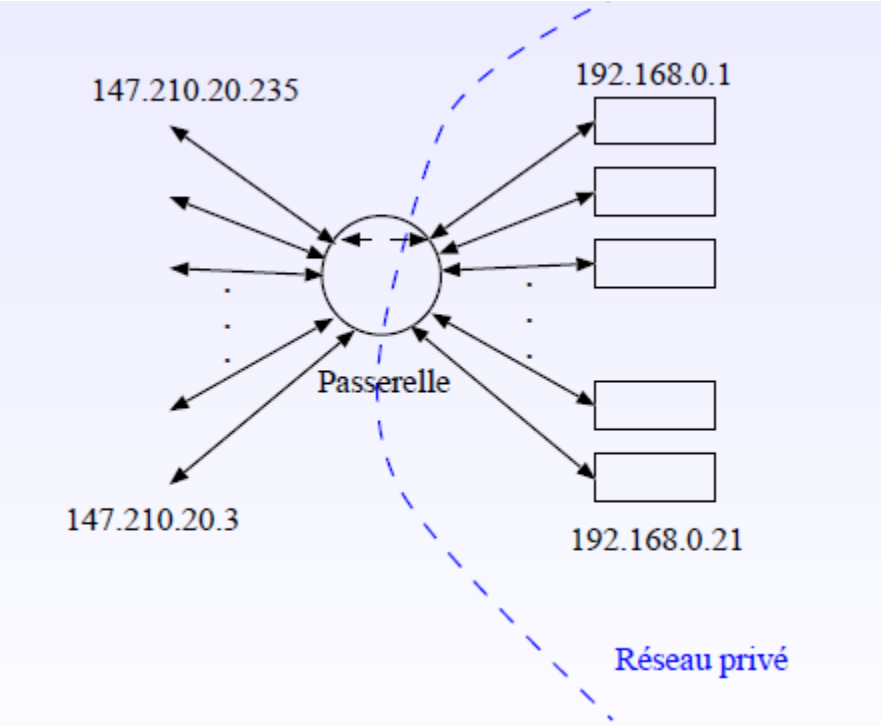


Transférer les connexions sur le port 80 de l'adresse 140.77.13.2 sur la machine ayant l'adresse privée 192.168.0.200 sur le port 8080 :

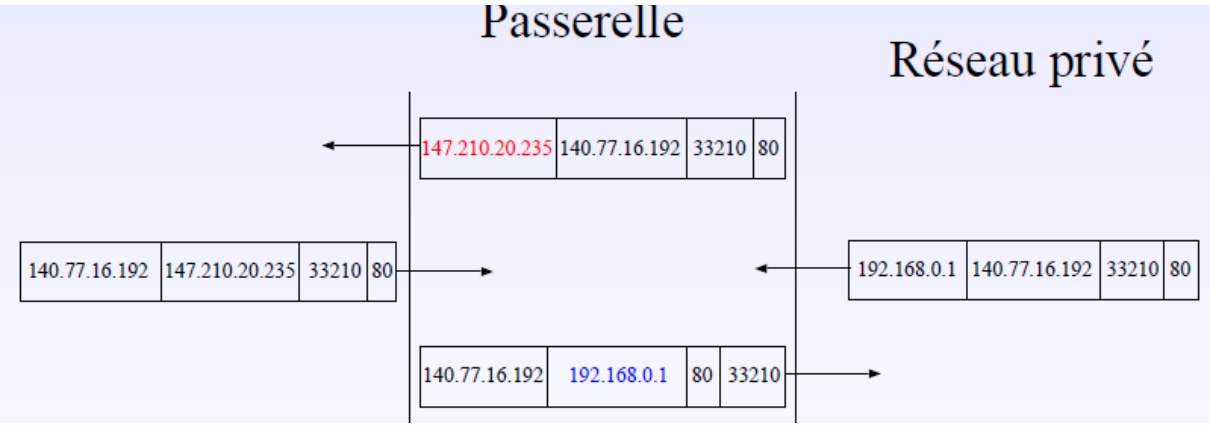
```
iptables -t nat -A PREROUTING -p tcp -i eth0 -d 140.77.13.2
-dport 80 -sport 1024:65535 -j DNAT -to 192.168.0.200:8080
```

NAT statique

Association entre une adresse publique et une adresse privée.

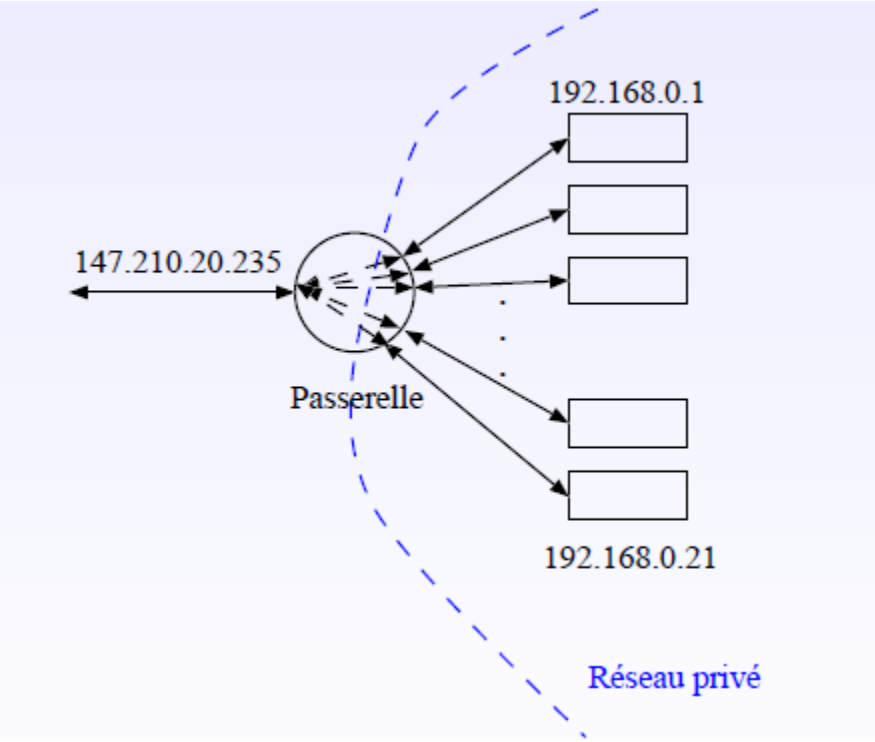


Pour chaque paquet sortant (resp. entrant), la passerelle modifie l'adresse source (resp. destination).



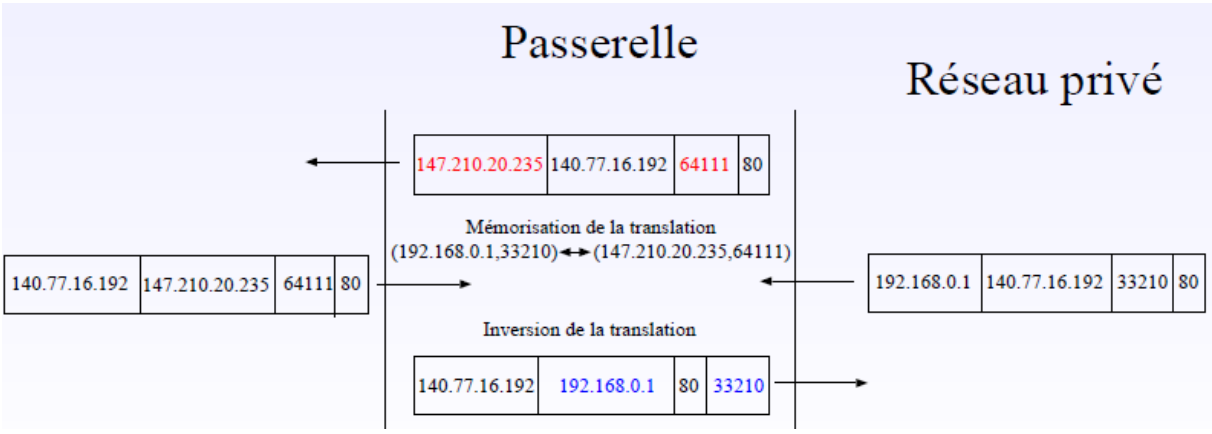
NAT dynamique : Masquerading

Association entre m adresses publiques et n adresses privées ($m < n$).



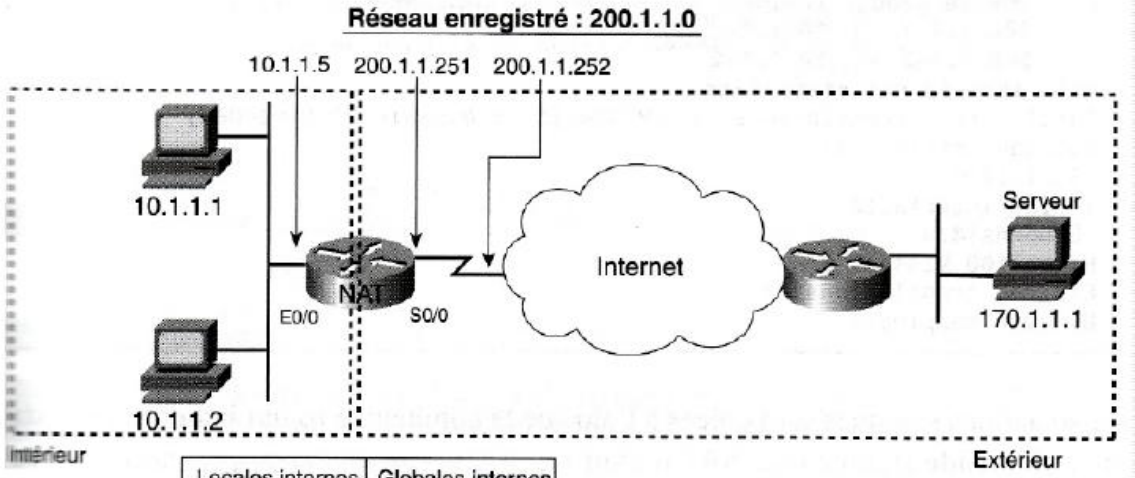
L'association de *n* adresses privées à 1 adresse publique nécessite, au niveau de la passerelle, de :

- ★ modifier l'adresse source (resp. destination) des paquets sortant (resp. entrants)
- ★ changer le numéro de port source pour les flux sortant



Configuration NAT statique Cisco

- Définition du NAT statique
  - (config)#ip nat inside source static 10.1.1.1 200.1.1.1
  - (config)#ip nat inside source static 10.1.1.2 200.1.1.2



Locales internes	Globales internes
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Configuration NAT statique Cisco

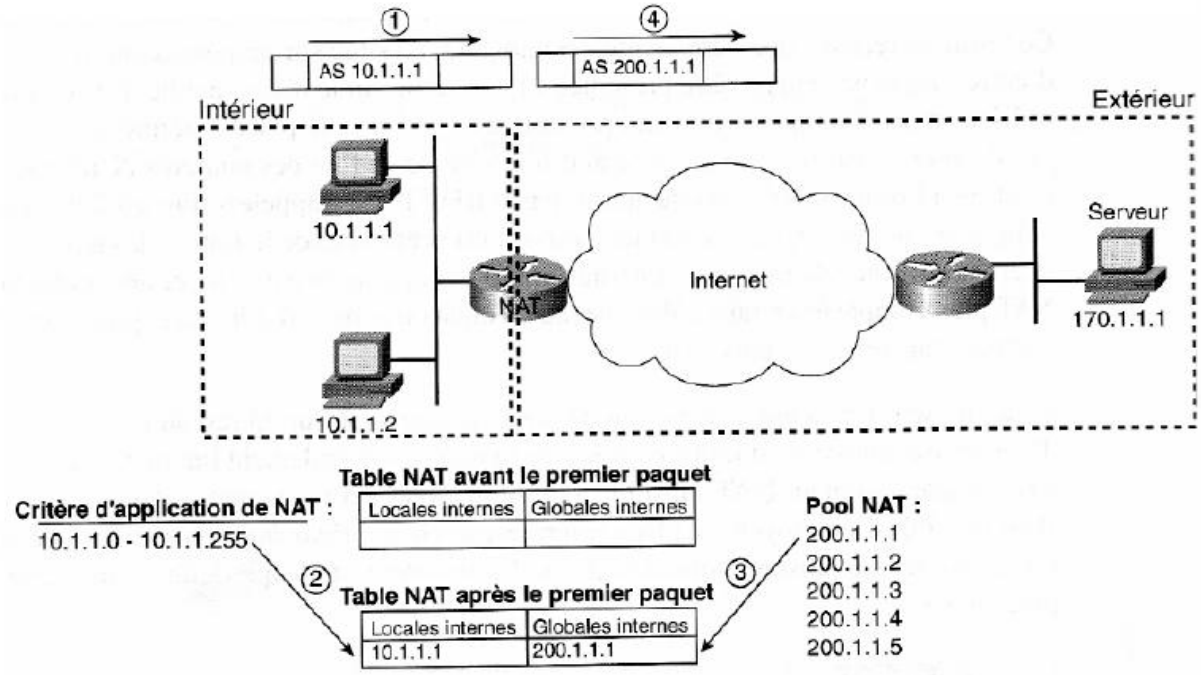
- Définition des interfaces Inside/Outside
  - (config)#interface Ethernet 0/0
    (config-if)#ip nat inside
    (config)# interface Serial 0/0
    (config-if)#ip nat outside
- Contrôle de la configuration des interfaces
  - (config)#show ip interface brief
    interface Ethernet 0/0
    ip address 10.1.1.5 255.255.255.0
    ip nat inside
    !
    interface Serial 0/0
    ip address 200.1.1.251 255.255.255.0
    ip nat outside
    !
    ip nat inside source static 10.1.1.2 200.1.1.2
    ip nat inside source static 10.1.1.1 200.1.1.1

Traduction NAT dynamique

- Appelée aussi **IP masquerading**

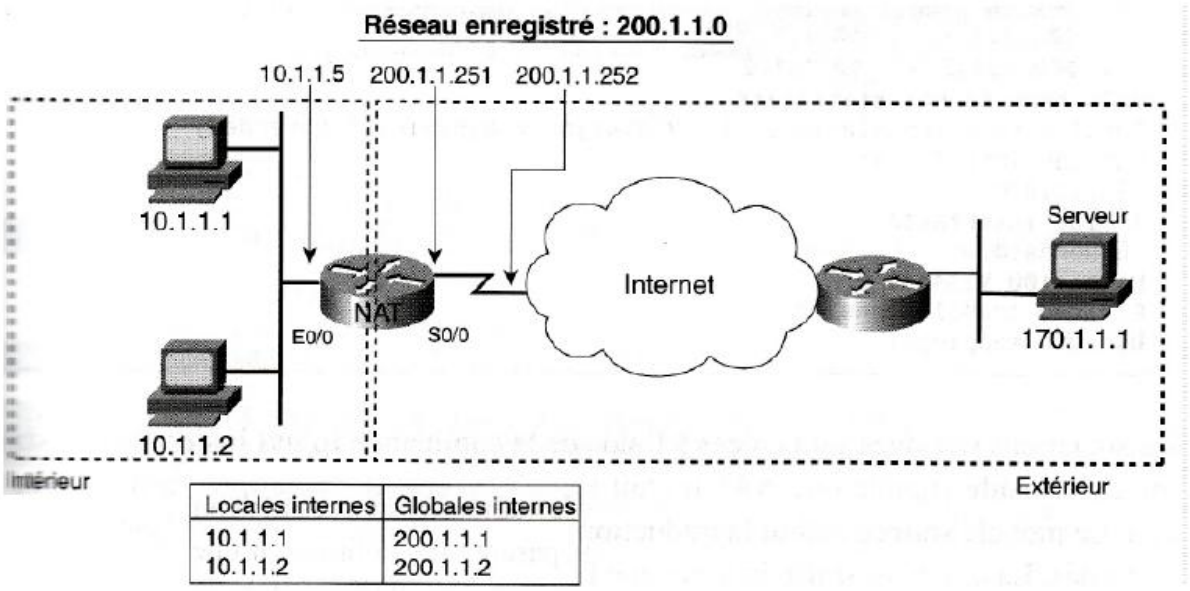
- Permet d'attribuer (associer) dynamiquement lors des connexions des adresses IP publiques aux adresses privées
- L'adresse source des paquets devient l'adresse externe du routeur
  - Problème : comment le routeur se rappelle-t-il des correspondances ?
- La configuration définit un pool d'adresses globales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

- Pool d'adresses publiques NAT allouées à la demande



Configuration Cisco du NAT dynamique

- Adresses locales soumises au NAT
  - (config)#access-list *<access-list_num>* permit *<source_ip>* *<wildcard_mask>*
- Pool d'adresses globales
  - (config)#ip nat pool *<name>* *<start_ip>* *<end_ip>*
- Définition du NAT
  - (config)#ip nat inside source list *<access-list_num>* pool *<name>*
- Définition des interfaces Inside/Outside
  - (config)#interface *<type>* *<number>*
    (config-if)#ip nat inside
    (config)# interface *<type>* *<number>*
    (config-if)#ip nat outside



Locales internes	Globales internes
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

- (config)#show ip interface brief
  interface Ethernet 0/0
  ip address 10.1.1.5 255.255.255.0
  ip nat inside
  !
  interface Serial 0/0
  ip address 200.1.1.251 255.255.255.0
  ip nat outside
  !
  ip nat pool monpool 200.1.1.1 200.1.1.2 netmask 255.255.255.252
  ip nat inside source list 1 pool monpool
  !
  access-list 1 permit host 10.1.1.2
  access-list 1 permit host 10.1.1.1