NAT / PAT

Network Address Translation

CHAPITRE1
-- NAT / PAT--

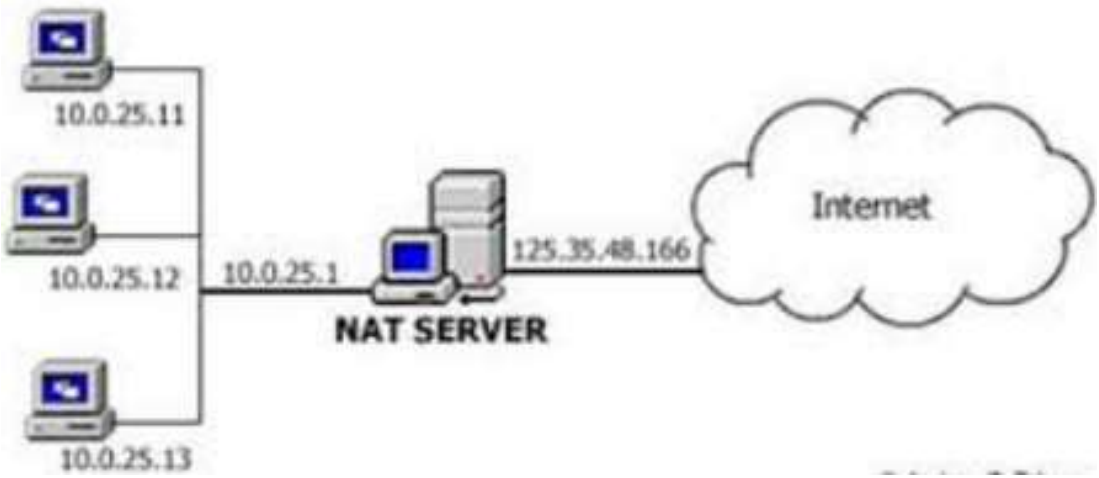
1. Introduction:

- La croissance rapide d'Internet connait une évolution importante.
- Sans le développement de nouvelles méthodologies d'assignation d'adresses IP, cette croissance rapide aurait épuisé la réserve existante d'adresses IP.
- Pour pallier à cette pénurie d'adresses IP, plusieurs solutions ont été développées. L'une de ces solutions, largement mise en œuvre, est la traduction d'adresses réseau (**NAT**)

CHAPITRE1
-- NAT / PAT--

2. Principe de fonctionnement:

- Lorsqu'un paquet est routé par un équipement de réseau, l'adresse IP source, c'est à dire une adresse réseau interne privée, est traduite en une adresse IP publique routable



CHAPITRE1
-- NAT / PAT--

2. Principe de fonctionnement:

Adresses Privées:

- Les adresses IP privées représentent toutes les adresses IP de classe A, B et C que l'on peut utiliser dans un réseau local (LAN)
- Les adresses IP privées ne peuvent pas être utilisées sur internet (car elles ne peuvent pas être routées sur internet)
- Les classes A, B et C comprennent chacune une plage d'adresses IP privées à l'intérieur de la plage globale.
  - Classe A: **10.0.0.0 à 10.255.255.255**
  - Classe B: **172.16.0.0 à 172.31.255.255**
  - Classe C: **192.168.1.0 à 192.168.255.255**

CHAPITRE1
-- NAT / PAT--

2. Principe de fonctionnement:

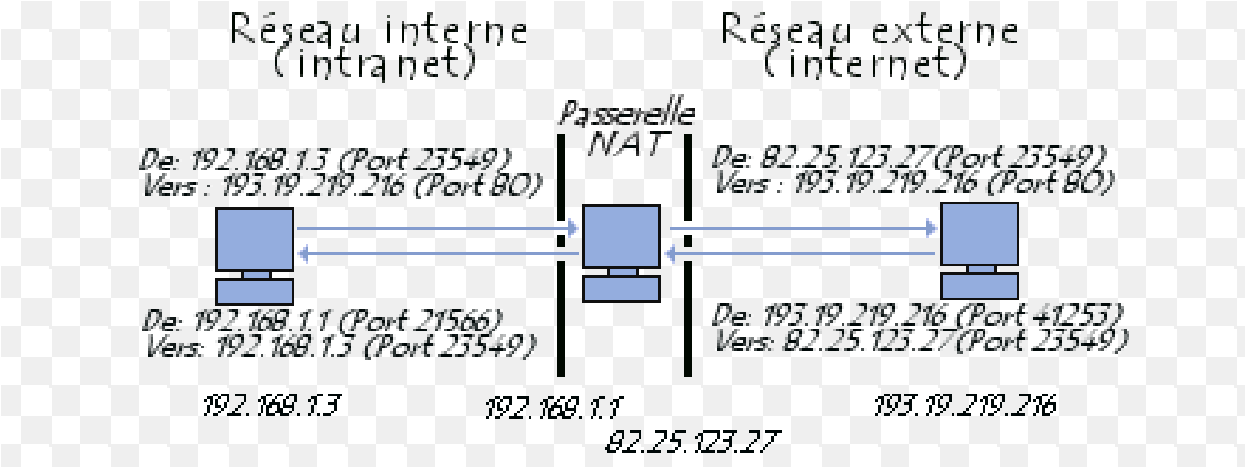
Adresses Publiques:

- Contrairement aux adresses IP privées, les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet.
- Les routeurs disposent d'une adresse IP publique côté internet
- Une adresse IP publique est unique dans le monde, ce qui n'est pas le cas des adresses privées qui doivent être unique dans un même réseau local mais pas au niveau planétaire étant donné que ces adresses ne peuvent pas être routées sur internet.
- Les adresses IP publiques représentent toutes les adresses IP des classes A, B et C qui ne font pas partie de la plage d'adresses privées de ces classes.

CHAPITRE1
-- NAT / PAT--

2. Principe de fonctionnement:

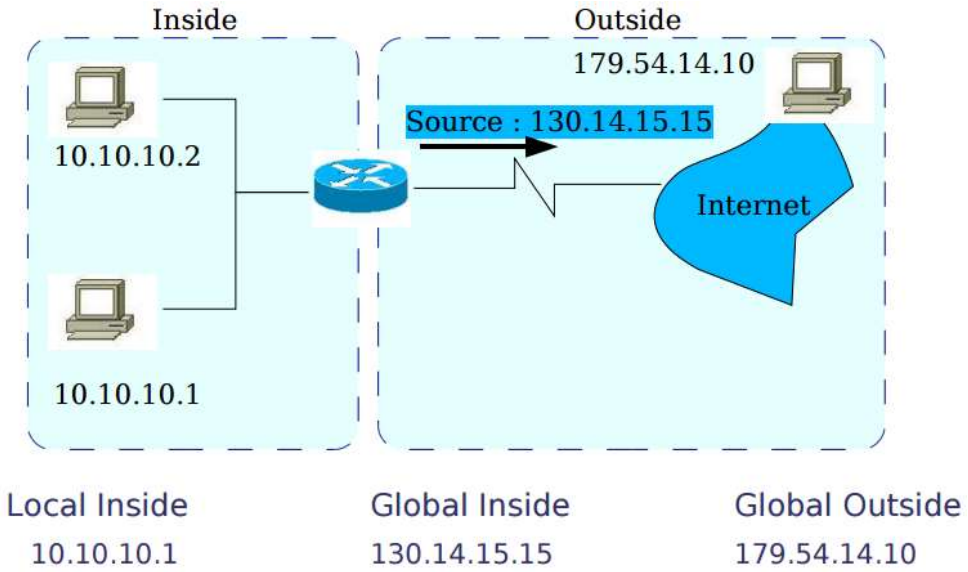
- Quand un hôte situé à l'intérieur du réseau d'extrémité souhaite émettre vers un hôte de l'extérieur, il transfère le paquet au routeur périphérique frontière.
- Ce routeur périphérique frontière effectue le processus NAT et traduit l'adresse privée interne d'un hôte en une adresse publique externe routable.



CHAPITRE1
-- NAT / PAT--

2. Principe de fonctionnement:

- 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 du réseau privé



CHAPITRE1
-- NAT / PAT--

3. Types de translations:

NAT Statique:

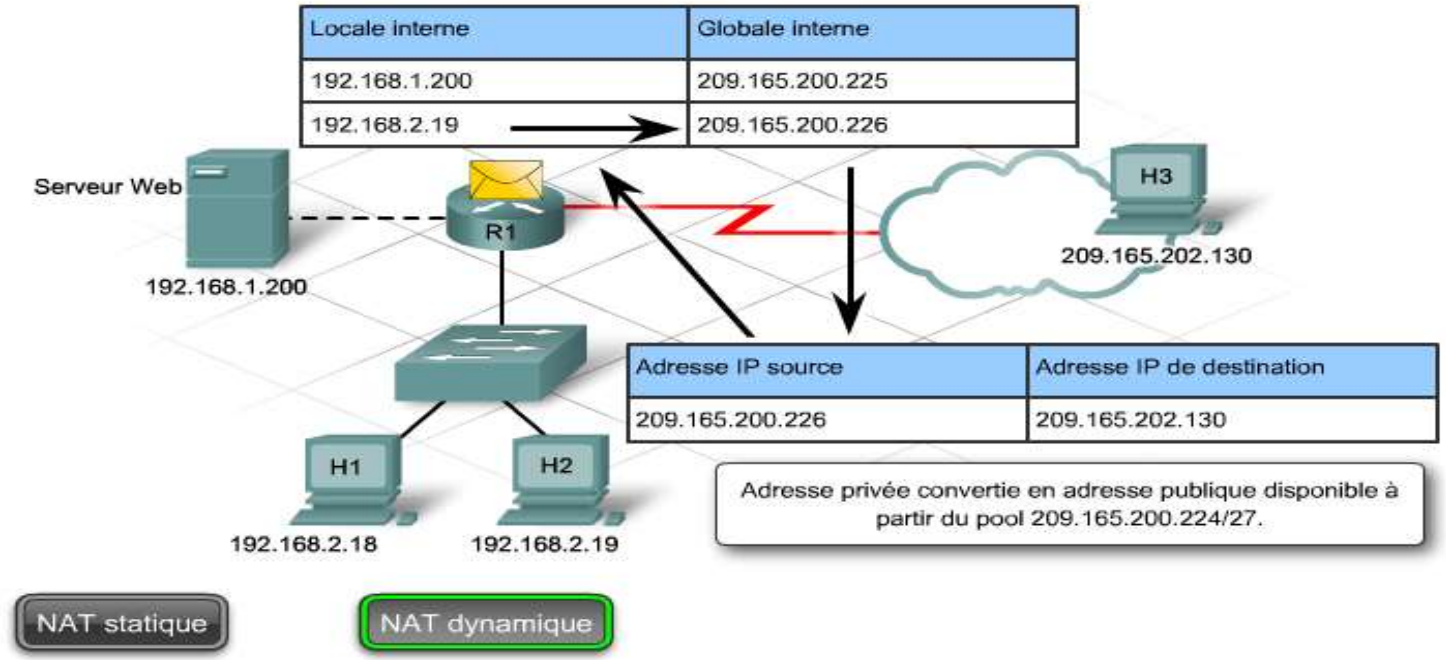
- Le principe du **NAT statique** consiste à associer une adresse IP publique à une adresse IP privée interne au réseau.
- Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée une adresse IP publique routable sur Internet.
- La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où *n* adresses IP routables sont nécessaires pour connecter *n* machines du réseau interne.

CHAPITRE1
-- NAT / PAT--

3. Types de translations:

NAT Dynamique:

- A plusieurs adresses IP locales correspondent plusieurs adresses IP globales.
- Dans ce cas, on parle de pool d'adresses IP publiques disponibles pour le NAT

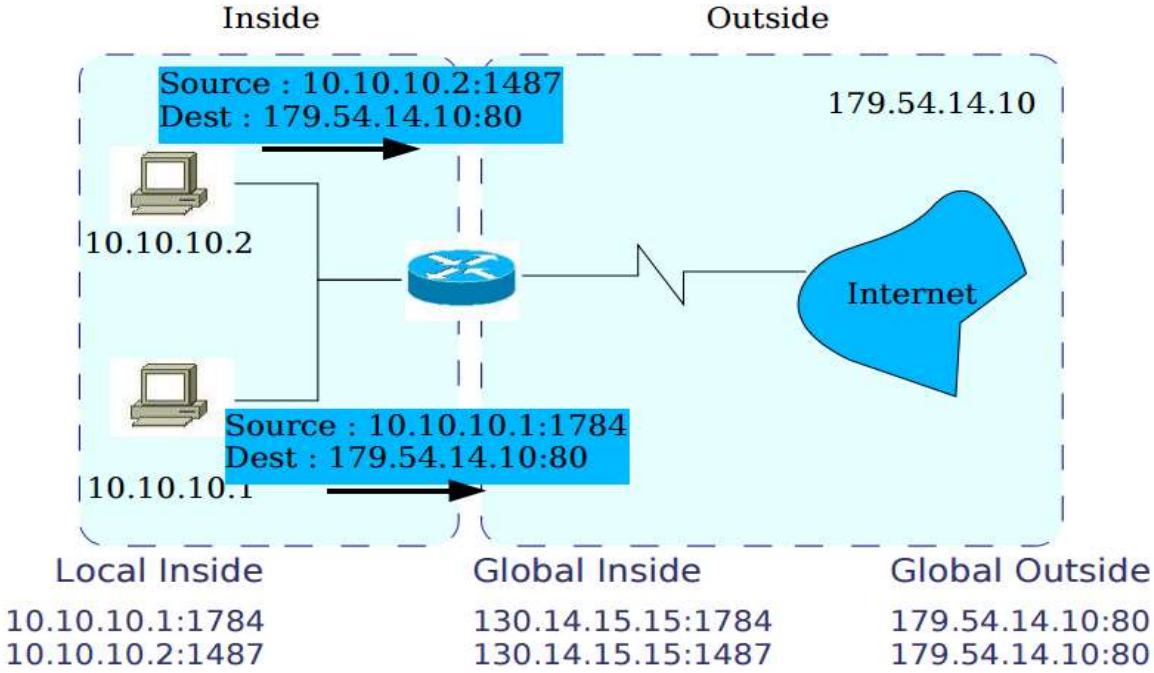


CHAPITRE1
-- NAT / PAT--

3. Types de translations:

PAT:

- A plusieurs adresses IP locales correspondent une seule adresse IP globale. Le suivi de la connexion se fait alors par l'utilisation de numéro de port



CHAPITRE1
-- NAT / PAT--

4. Les avantages offerts par NAT / PAT :

- Elle économise les adresses au moyen d'un multiplexage au niveau du port de l'application.
- Elle protège le réseau. En effet, comme les réseaux privés ne divulguent pas leurs adresses ou leur topologie interne, ils restent raisonnablement sécurisés quand ils sont utilisés conjointement à la fonction NAT pour obtenir un accès externe.

CHAPITRE1
-- NAT / PAT--

5. Configuration du NAT:

NAT Statique:

- Une translation statique consiste à associer une adresse IP privée à une adresse IP publique routable qui lui est réservée.
- Pour configurer un mappage NAT d'adresses IP statiques, utilisez la commande:

  Router(config)#**ip nat inside source static** [*adresse_privée*] [*adresse_publique*]

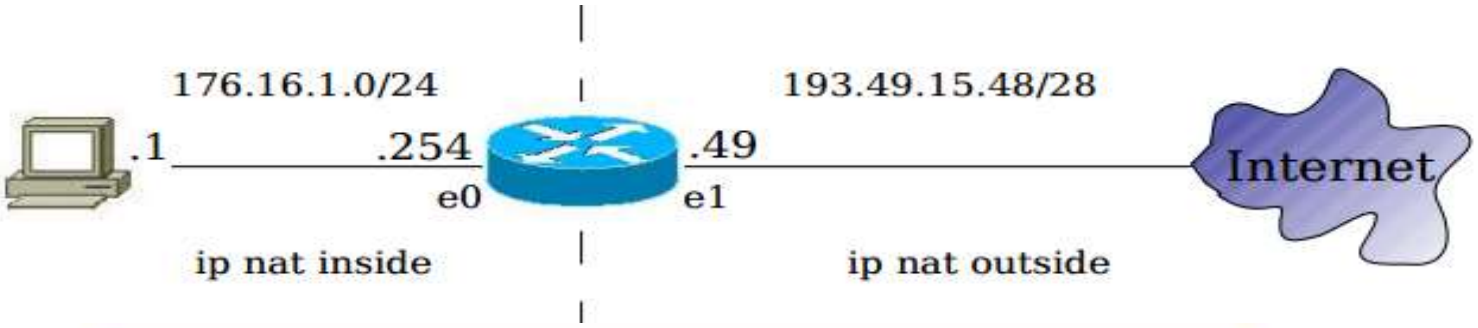
- Sur les interfaces du routeur: soit *ip nat inside*, soit *ip nat outside* selon la position de l'interface par rapport à Internet

CHAPITRE1
-- NAT / PAT--

5. Configuration du NAT:

NAT Statique:

Exemple:




```
ip nat inside source static 176.16.1.1 193.49.15.50
interface FastEthernet 0
     ip address 176.16.1.254 255.255.255.0
     ip nat inside
interface FastEthernet 1
     ip address 193.49.15.49 255.255.255.240
     ip nat outside
```

CHAPITRE1
-- NAT / PAT--

5. Configuration du NAT:

NAT Dynamique:

- Définir par une access-list quelles sont les IP locales internes qui ont le droit de sortir

  Router(config)#**access-list** [*numero_acl]* **permit** [**@ip** *source]* *[masque_générique]*

- Définir le pool d'adresses publiques:

  Router(config)#**ip nat pool** *nom-pool* *[@IP_départ]* *[@IP_fin]* ***netmask*** *[masque]*

- Définir la traduction NAT:

  Router(config)#**ip nat inside source list** [*numero_acl]* **pool** [*nom-pool]*

Remarque:*s'il s'agit de NAT Dynamique avec surcharge, on utilise:*

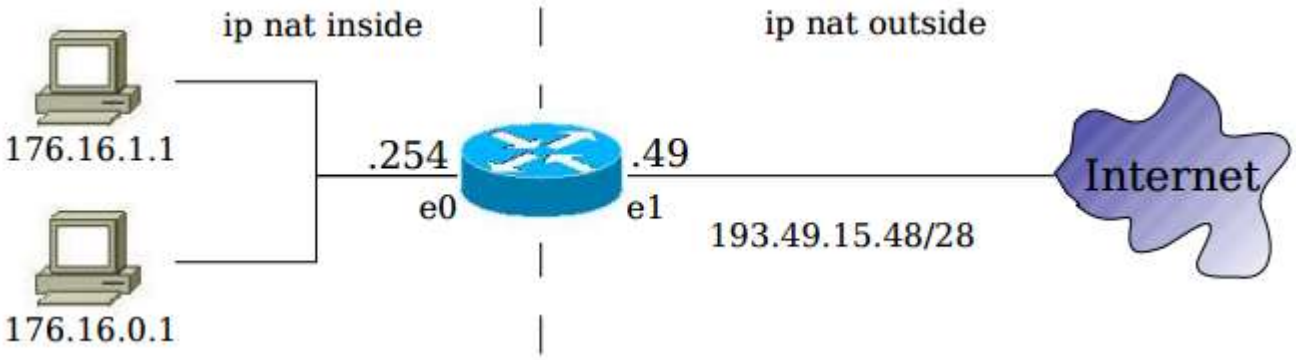
Router(config)#**ip nat inside source list** [*numero_acl]* **pool** [*nom-pool]* ***Overload***

CHAPITRE1
-- NAT / PAT--

5. Configuration du NAT:

NAT Dynamique:

Exemple:




```
ip nat pool plage1 193.49.15.50 193.49.15.60
ip nat inside source liste 1 pool plage1
interface FastEthernet 0
      ip address 176.16.1.254 255.255.0.0
      ip nat inside
interface FastEthernet 1
      ip address 193.49.15.49 255.255.255.240
      ip nat outside
access-list 1 permit 176.16.1.0 0.0.0.255
```

CHAPITRE1
-- NAT / PAT--

6. Configuration du PAT:

- Définir la liste de contrôle d'accès correspondant aux adresses locales internes:

  Router(config)#**access-list** [*numero_acl]* **permit** [**@ip** *source]* *[masque_générique]*

- Configurer la traduction PAT.

  Méthode N°1: En utilisant une seule adresse publique:

  Router(config)#**ip nat inside source list** [*numero_acl]* **interface** [*nom_interface]* **overload**

  Méthode N°2: En utilisant un groupe d'adresses publiques:

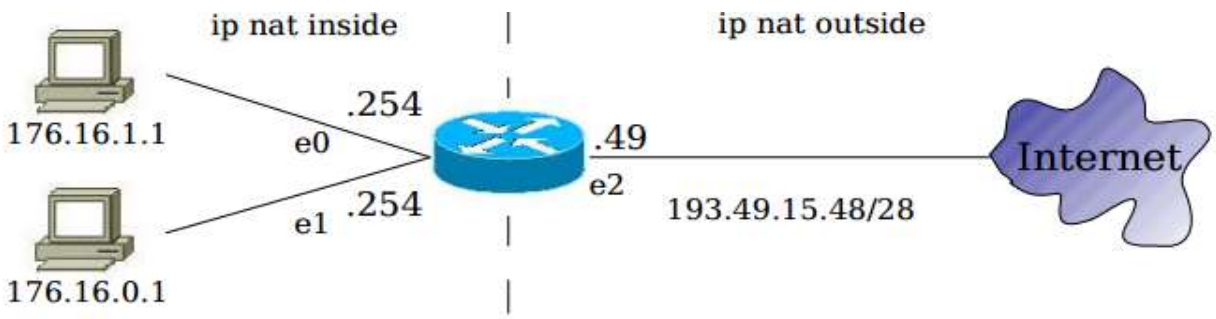
- Router(config)#**ip nat pool** *nom-pool* *[@IP_début]* *[@IP_fin]*

- Router(config)#**ip nat inside source list** [*numero_acl]* **pool** [*nom-pool]* **overload**

CHAPITRE1
-- NAT / PAT--

6. Configuration du PAT:

Exemple:




```
ip nat inside source liste 1 interface FastEthernet 2 overload

interface FastEthernet 0
      ip address 176.16.1.254 255.255.255.0
      ip nat inside
interface FastEthernet 1
      ip address 176.16.0.254 255.255.255.0
      ip nat inside
interface FastEthernet 2
      ip address 193.49.15.49 255.255.255.240
      ip nat outside

access-list 1 permit 176.16.1.0 0.0.0.255
```

CHAPITRE1
-- NAT / PAT--

7. Vérifier la configuration:

Show ip nat translations:

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 201.49.10.30:33598 192.168.1.100:33598 8.8.8.8:33598 8.8.8.8:33598
icmp 201.49.10.30:33854 192.168.1.100:33854 8.8.8.8:33854 8.8.8.8:33854
icmp 201.49.10.30:34366 192.168.1.100:34366 8.8.8.8:34366 8.8.8.8:34366
icmp 201.49.10.30:34622 192.168.1.100:34622 8.8.8.8:34622 8.8.8.8:34622
icmp 201.49.10.30:34878 192.168.1.100:34878 8.8.8.8:34878 8.8.8.8:34878
--- 201.49.10.30 192.168.1.100 --- ---
R1#
```