NAT et sa configuration

NAT et sa configuration

Introduction

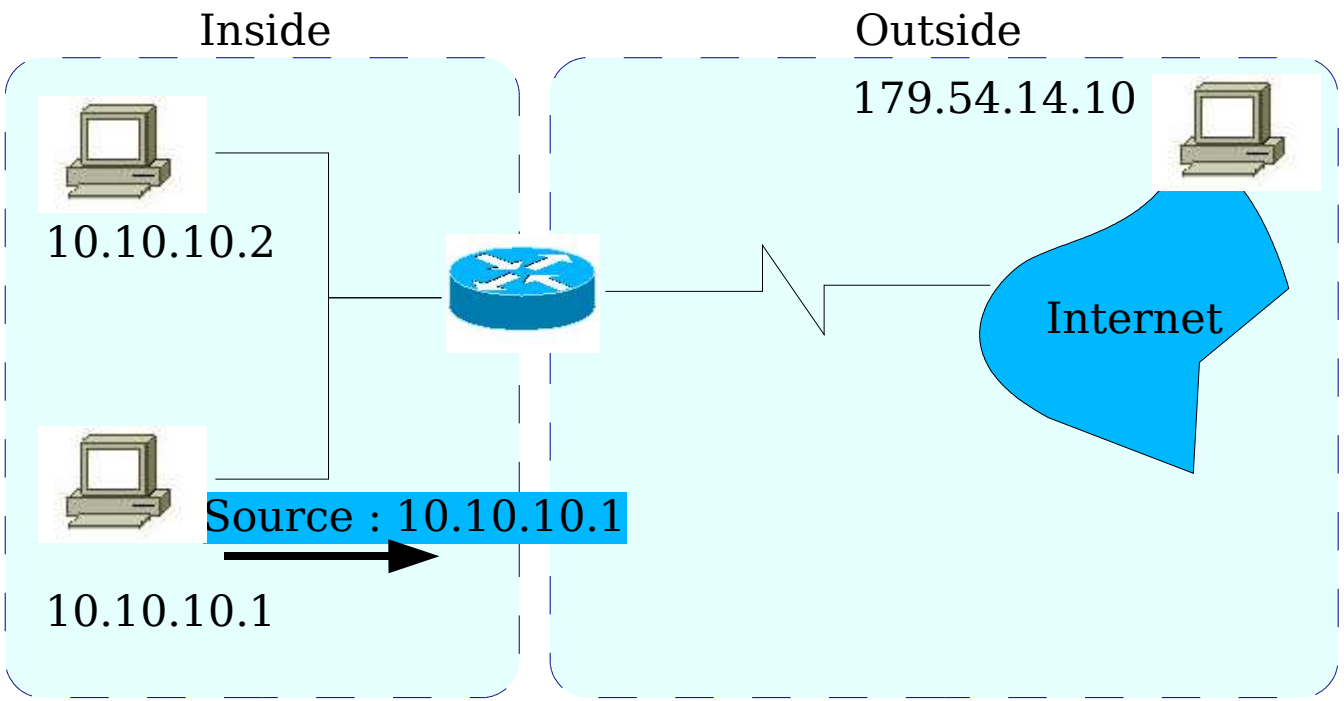
Introduction

- La RFC 1918 a défini des plages d'adresses IP dites privées dans les 3 classes A, B et C
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Ces adresses ne sont jamais routées par un routeur donc impossible d'aller sur Internet
- De même si une entreprise utilise en interne des adresses enregistrées officiellement par une autre entreprise
- La solution : NAT (Network Address Translation)

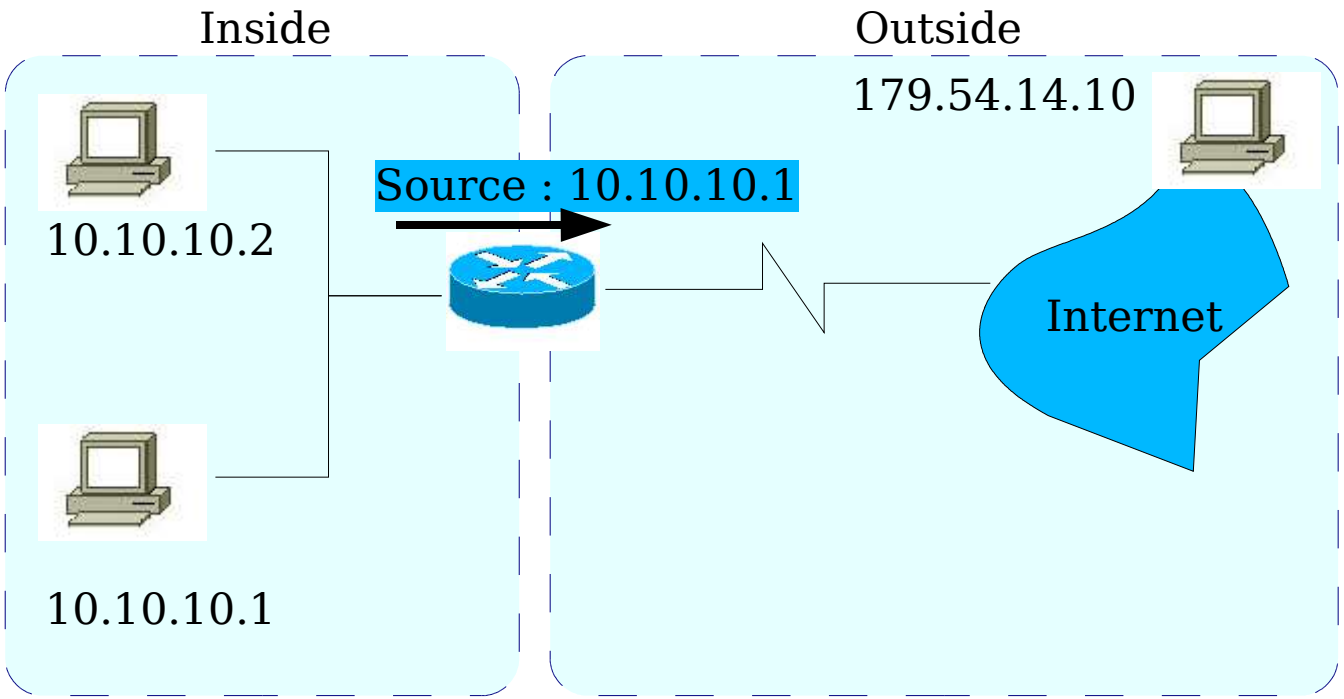
Le NAT

- Quand une machine interne à un réseau veux communiquer avec un hôte sur Internet
  - Transmission du paquet au routeur de sortie
  - Translation de l'adresse de réseau privé en adresse publique
  - Transmission du paquet modifié au hôte de destination
- 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

Exemple

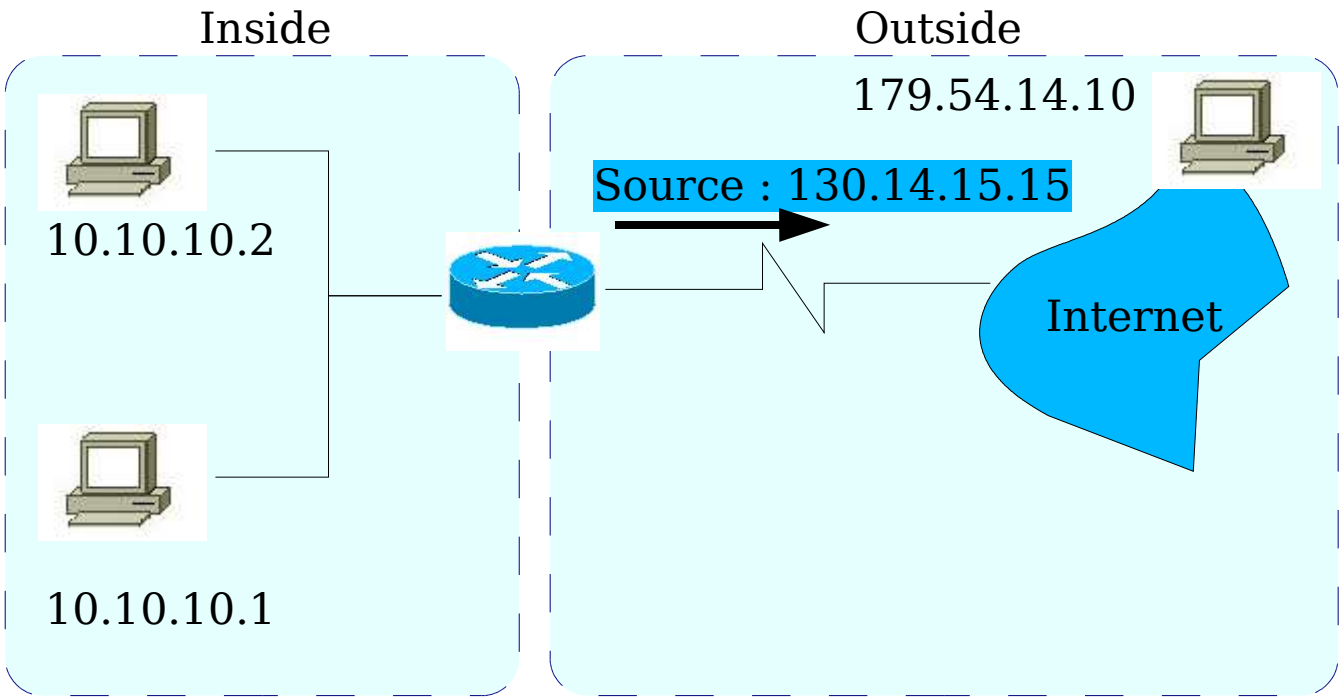


Exemple



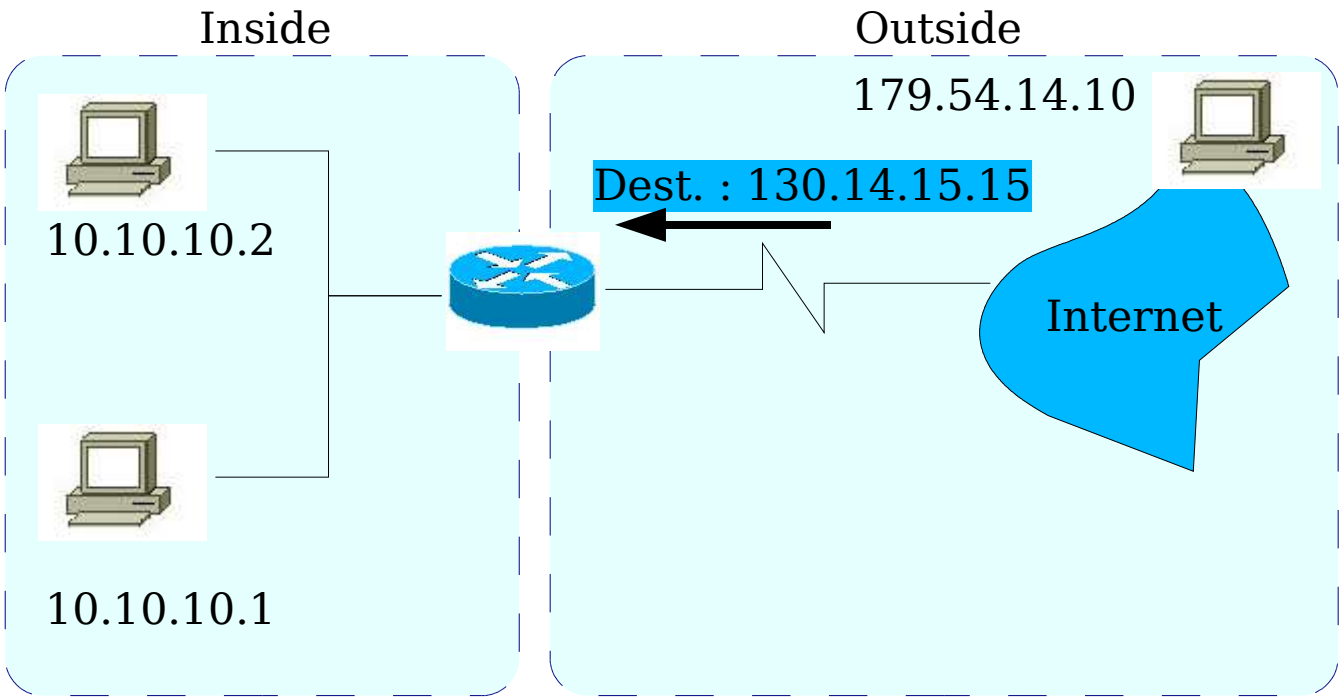
Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



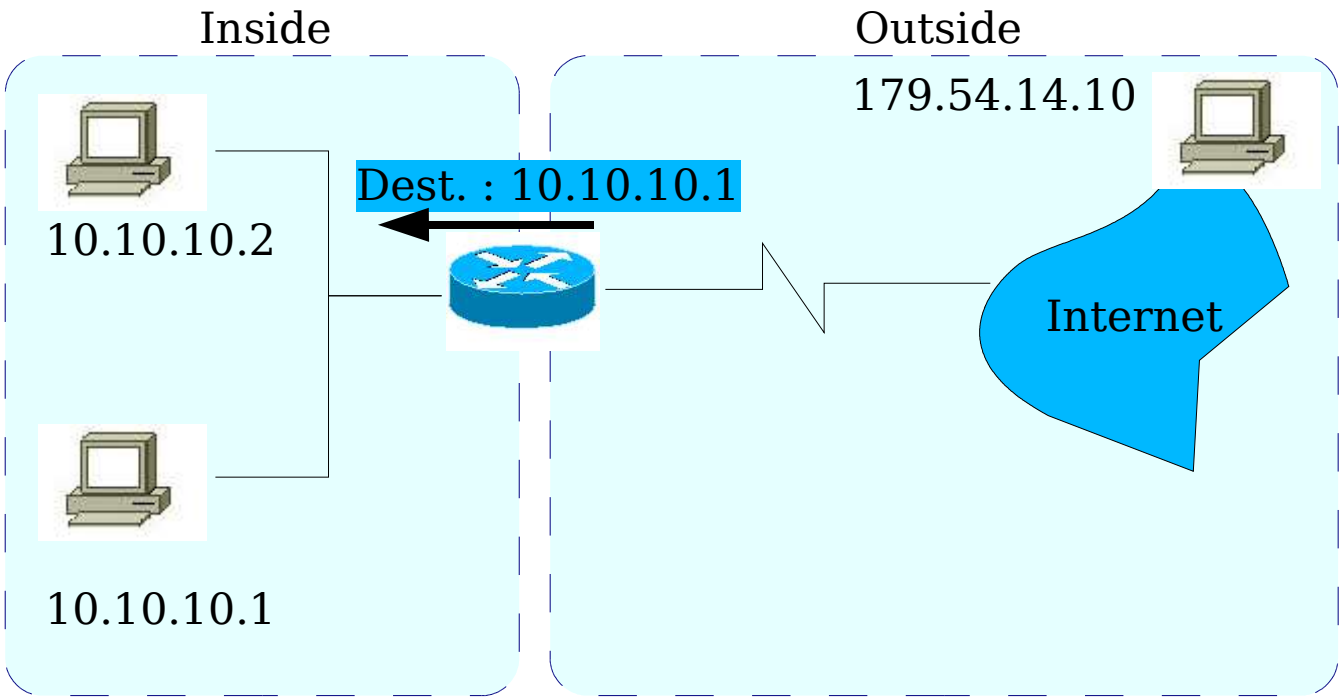
Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple

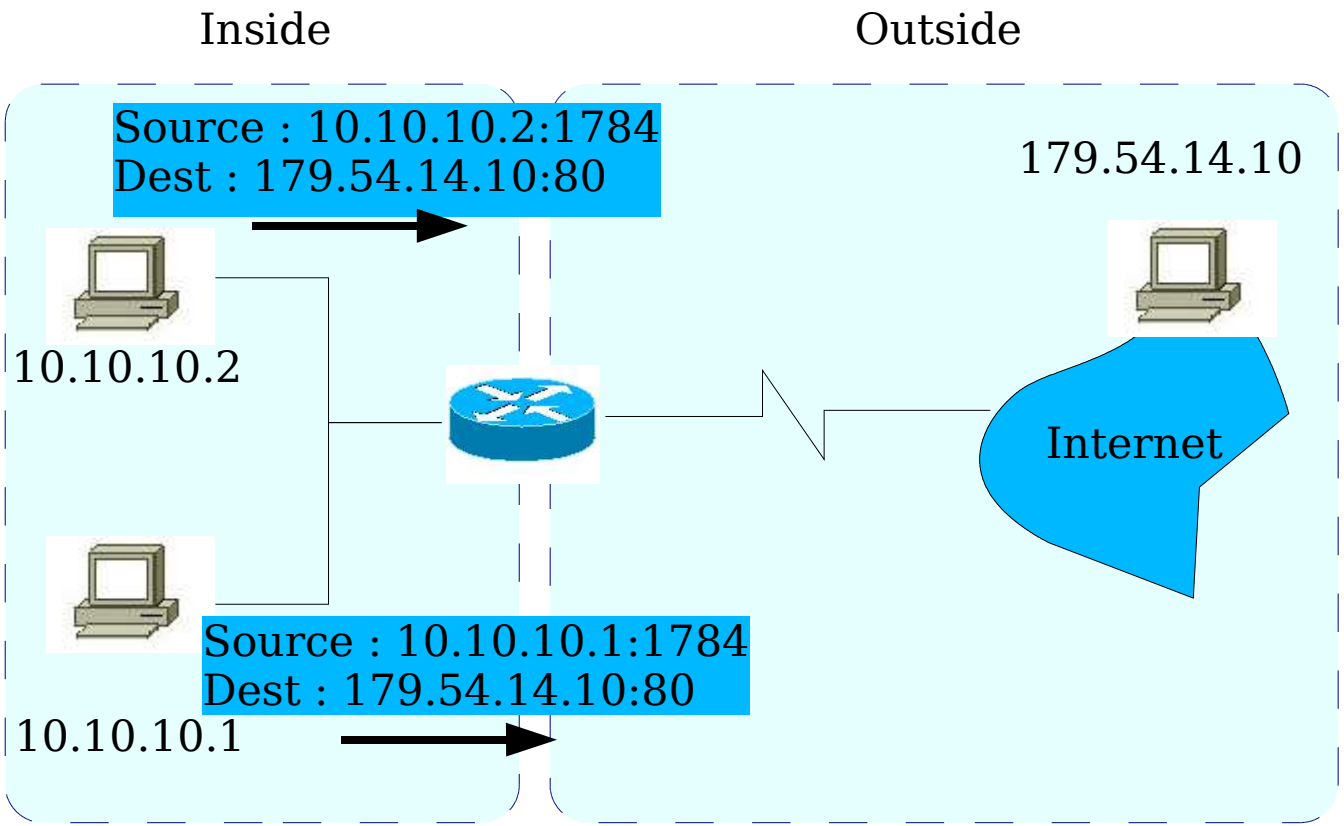


Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

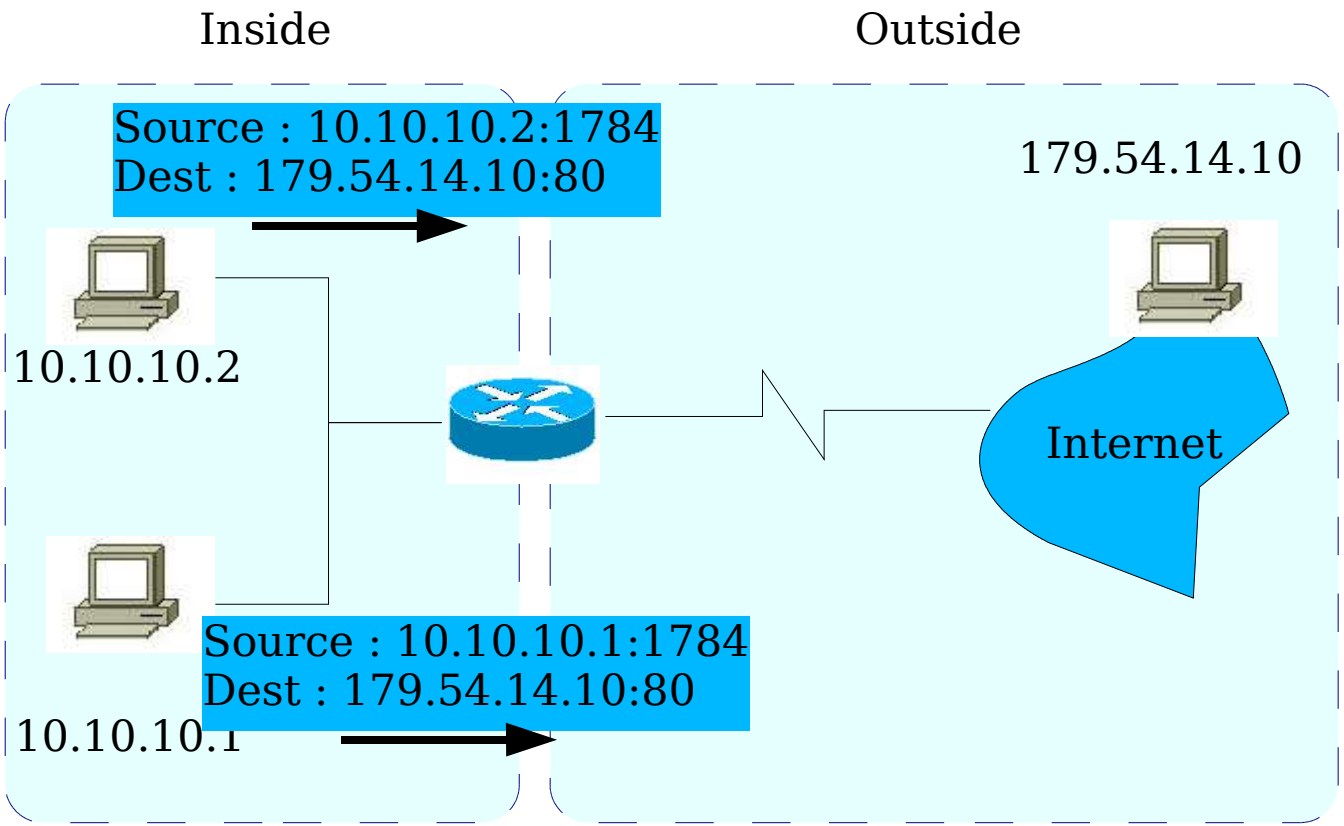
Fonctionnalités NAT et PAT (ou NAPT)

- Il existe plusieurs types de translations
- NAT statique : A exactement une adresse IP local correspond exactement une adresse IP globale
- 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
  - Si qu'une seule adresse IP publique est disponible, dans ce cas, on parle de Network Address Port Translation (NAPT) ou Port Address Translation (PAT)
- 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

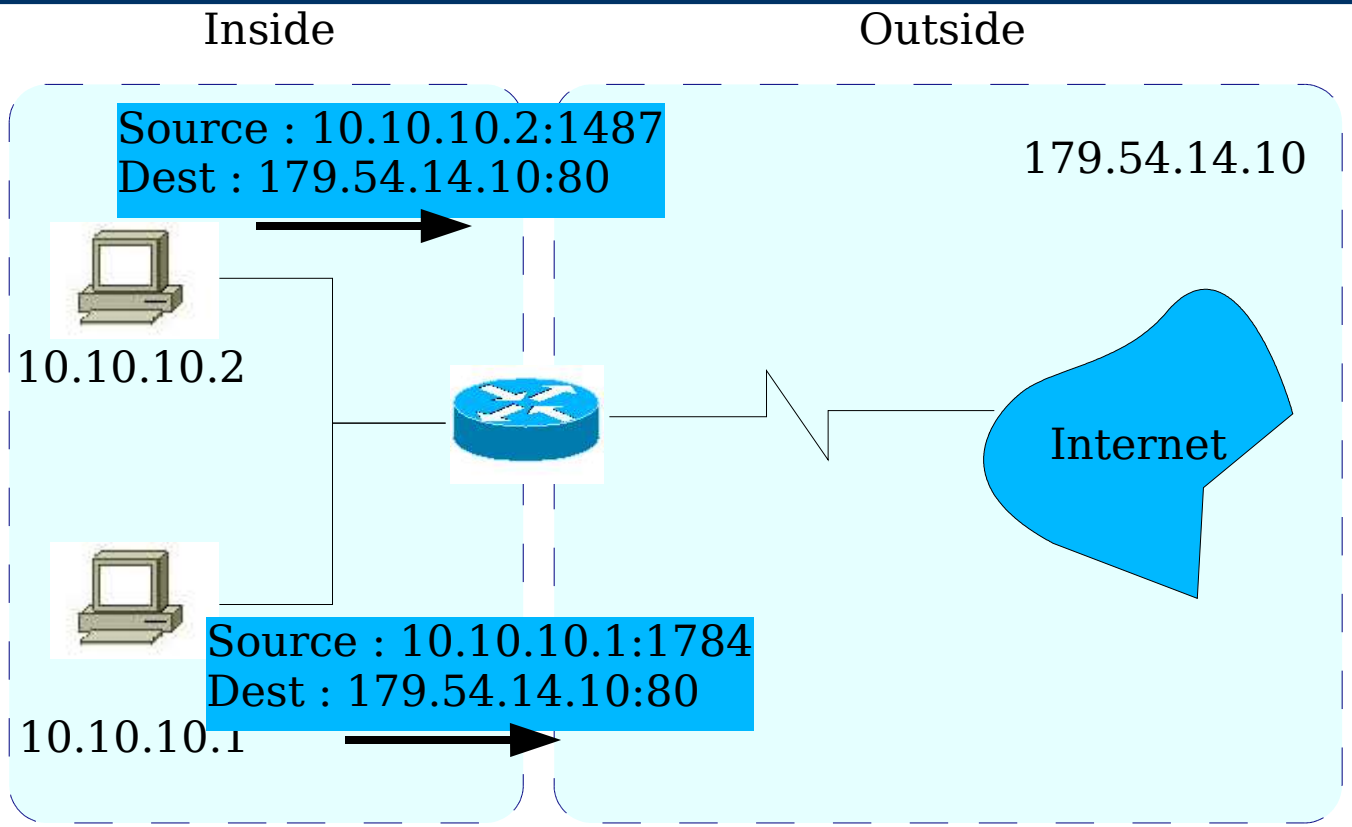
Exemple



Exemple



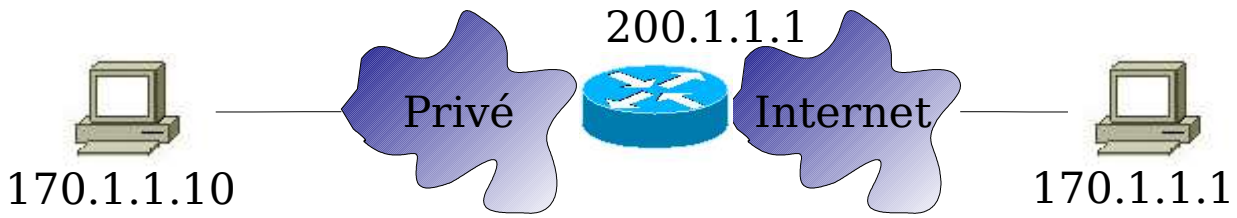
Exemple



Local Inside	Global Inside	Global Outside
10.10.10.1:1784	130.14.15.15:1784	179.54.14.10:80
10.10.10.2:1487	130.14.15.15:1487	179.54.14.10:80

Autre exemple

- Si une entreprise utilise des adresses réseaux déjà enregistrées
- Le routeur NAT fera croire aux clients en interne que les adresses externes sont tout autre
- Ces adresses sont appelées Inside Local address
- Cette solution est basée sur l'utilisation d'une DNS. La requête DNS du client est interceptée par le routeur qui va retourner une adresse non ambiguë routable sur le réseau privé.

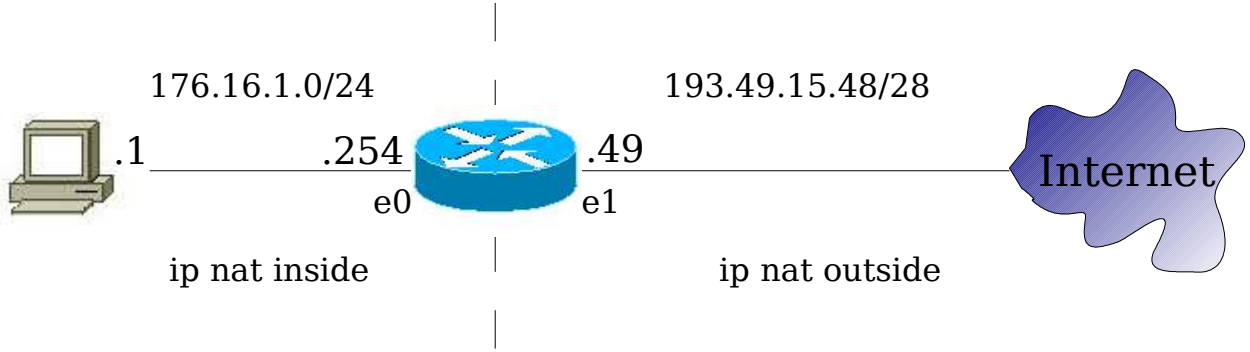


Inside Local	Outside Local	Inside Global	Outside Global
170.1.1.10	192.168.1.1	200.1.1.1	170.1.1.1

NAT et sa configuration

Configuration sur routeur Cisco

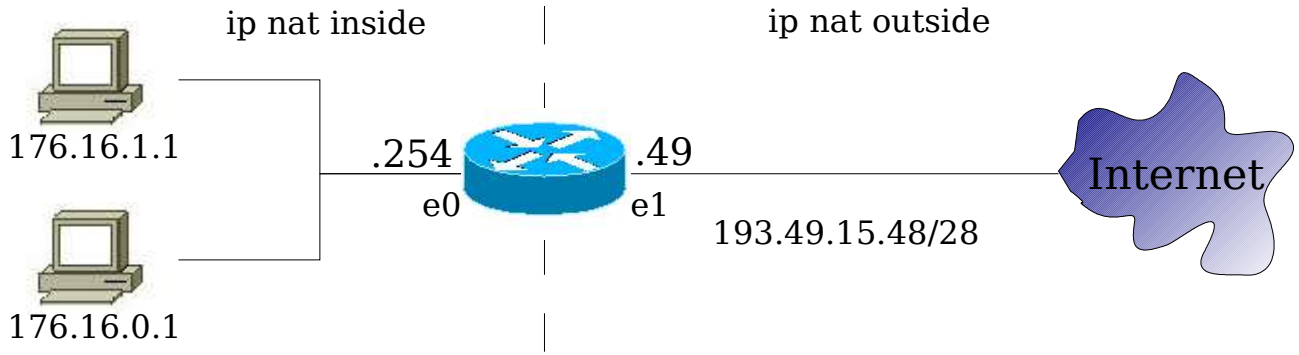
NAT statique



- Sur les interfaces du routeur
  - soit `ip nat inside`, soit `ip nat outside` selon la position de l'interface par rapport à Internet
  - définir la translation static : `ip nat inside source static` *`ip_source ip_dest`*

```
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
```

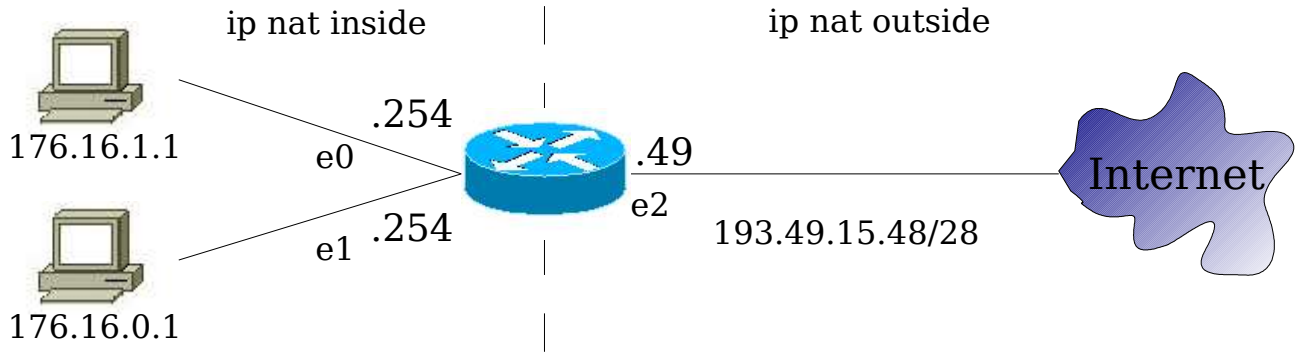
NAT dynamique



- Définir un pool d'adresses d'IP globales interne : `ip nat pool` *`nom start-ip end-ip`*
- Définir par une access-list quelles sont les IP locales internes qui ont le droit de sortir
  - `access-list` *`number`* `permit` *`source [ source-wildcard ]`*

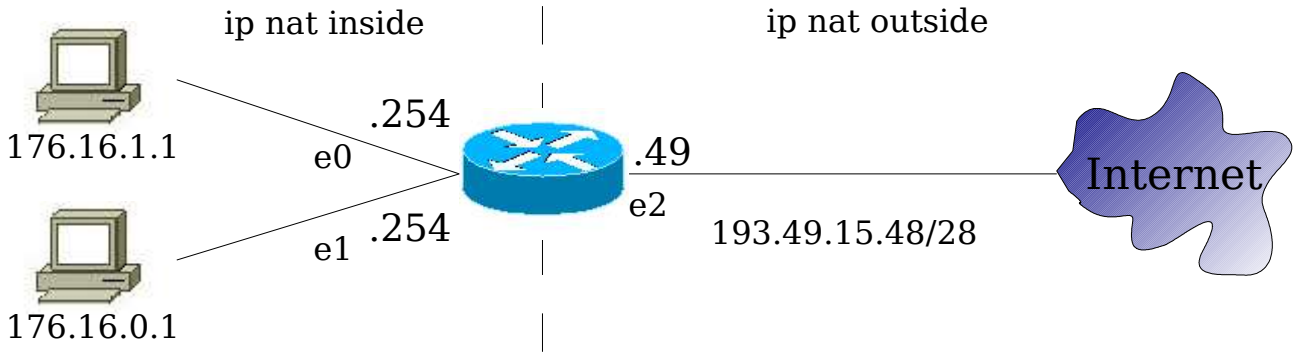
```
ip nat pool plage1 193.49.15.50 193.49.15.60
ip nat inside source liste 1 pool plage1
interface FastEthernet 0
      ip address 176.16.1.254 255.255.0.0
      ip nat inside
interface FastEthernet 1
      ip address 193.49.15.49 255.255.255.240
      ip nat outside
access-list 1 permit 176.16.1.0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

PAT (1/2)



- Définir par une access-list quelles sont les IP locales internes qui ont le droit de sortir
- Définir l'interface de sortie dont l'IP sera dite surchargée : `ip nat inside source list` *`number`* `interface` *`interface`* `overload`
- Ou bien définir une adresse dans un pool puis faire la surcharge :
  - ip nat pool *name ip_addr*
  - `ip nat inside source list` *`number`* `pool` *`name`* `overload`

PAT (2/2)




```
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
```