Académie Cisco
Reims
Champagne-Ardenne

UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

DHCP - NAT

DHCP - NAT

NAT et sa configuration

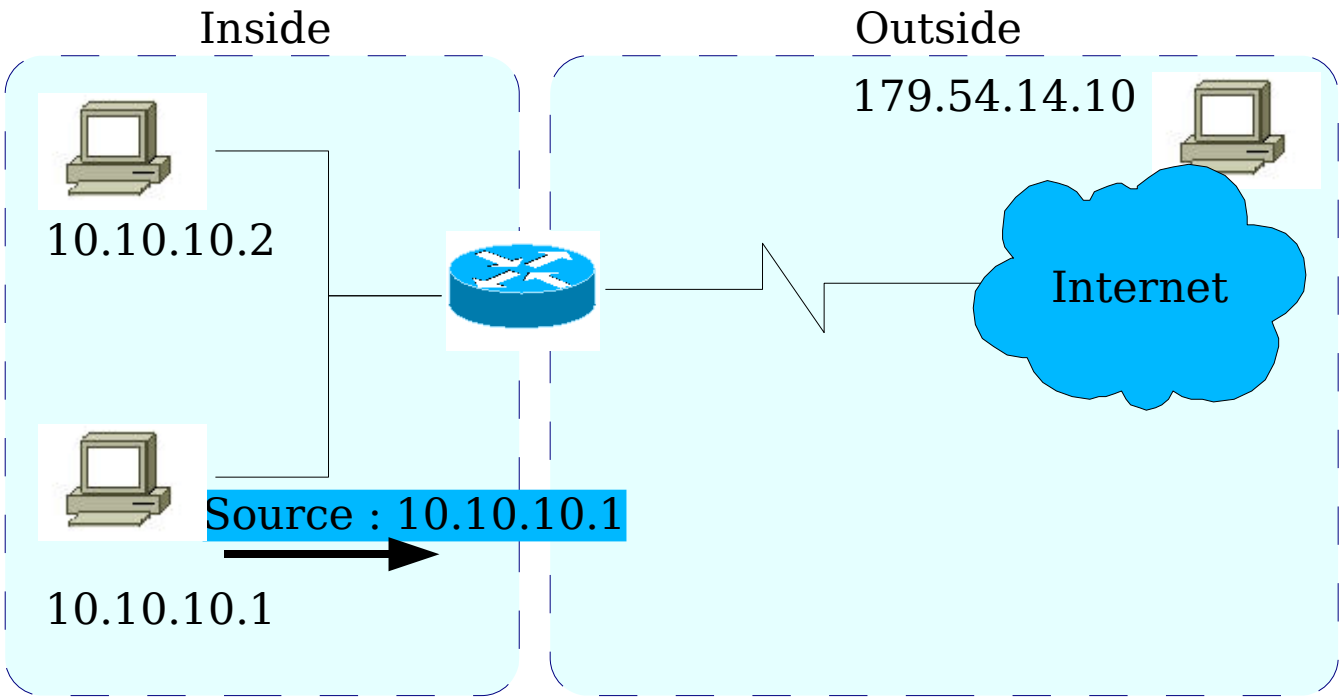
Introduction

- 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)

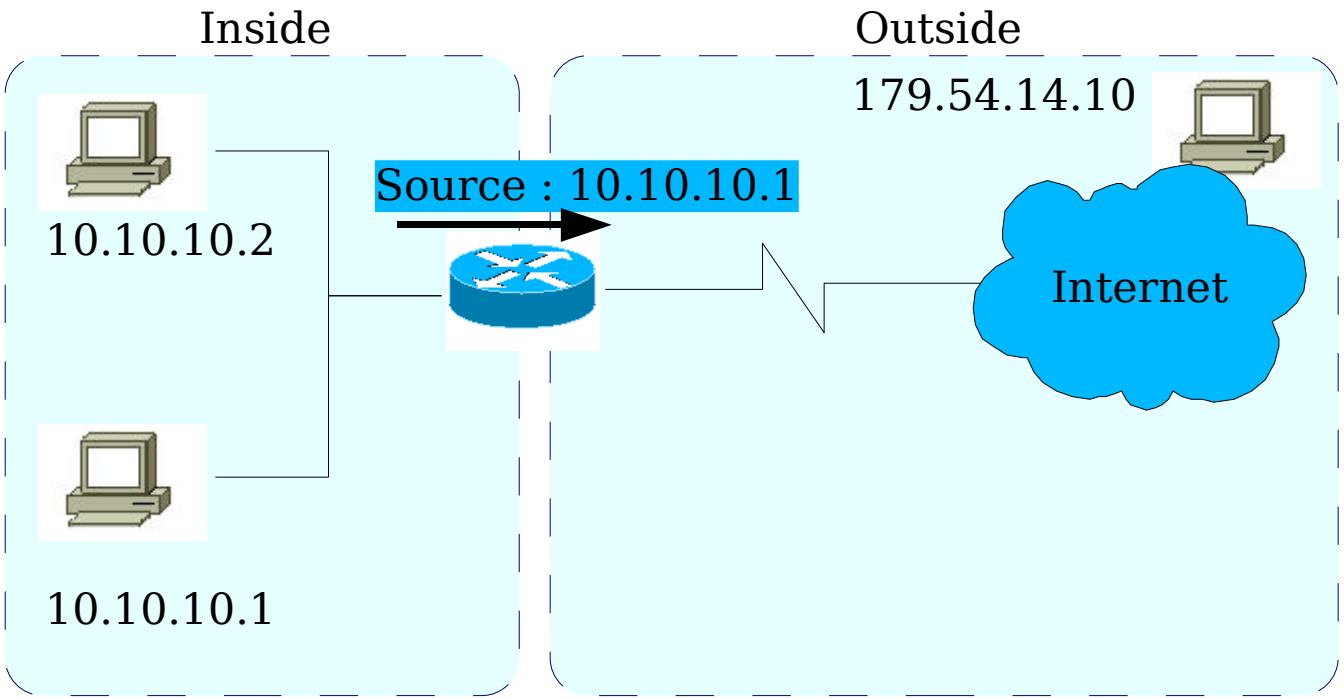
Le NAT

- 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

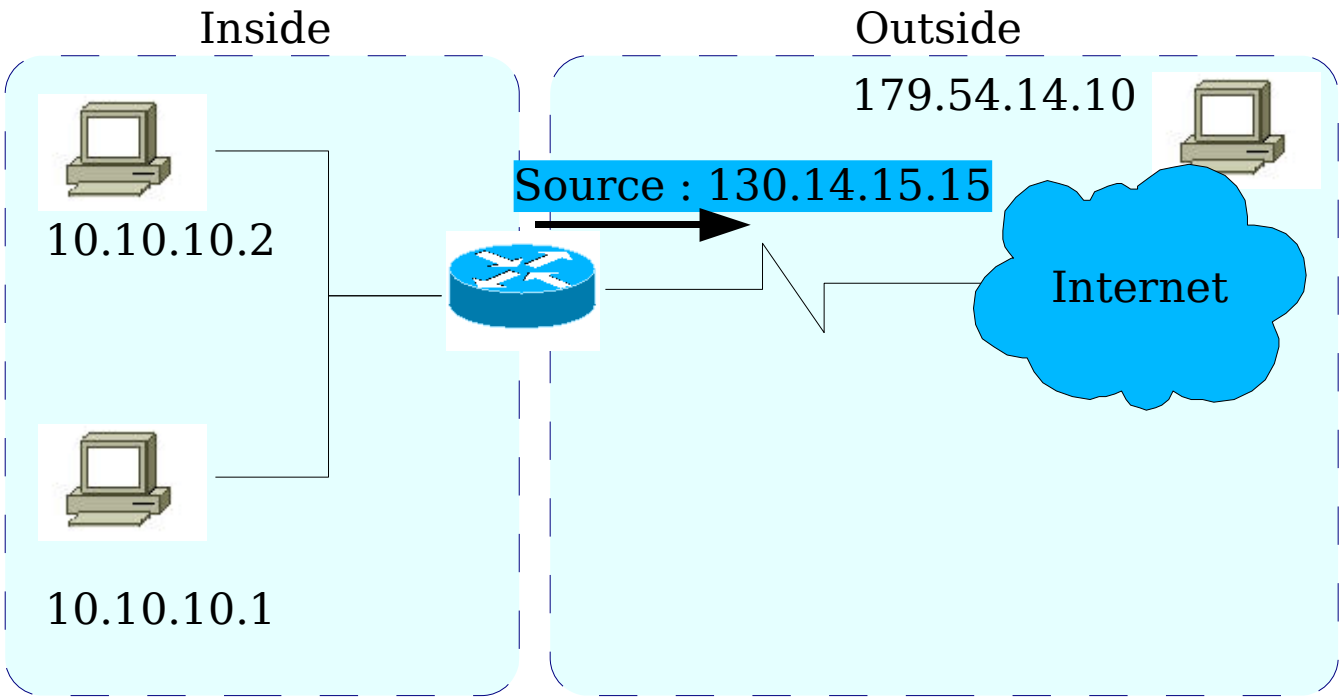


Exemple



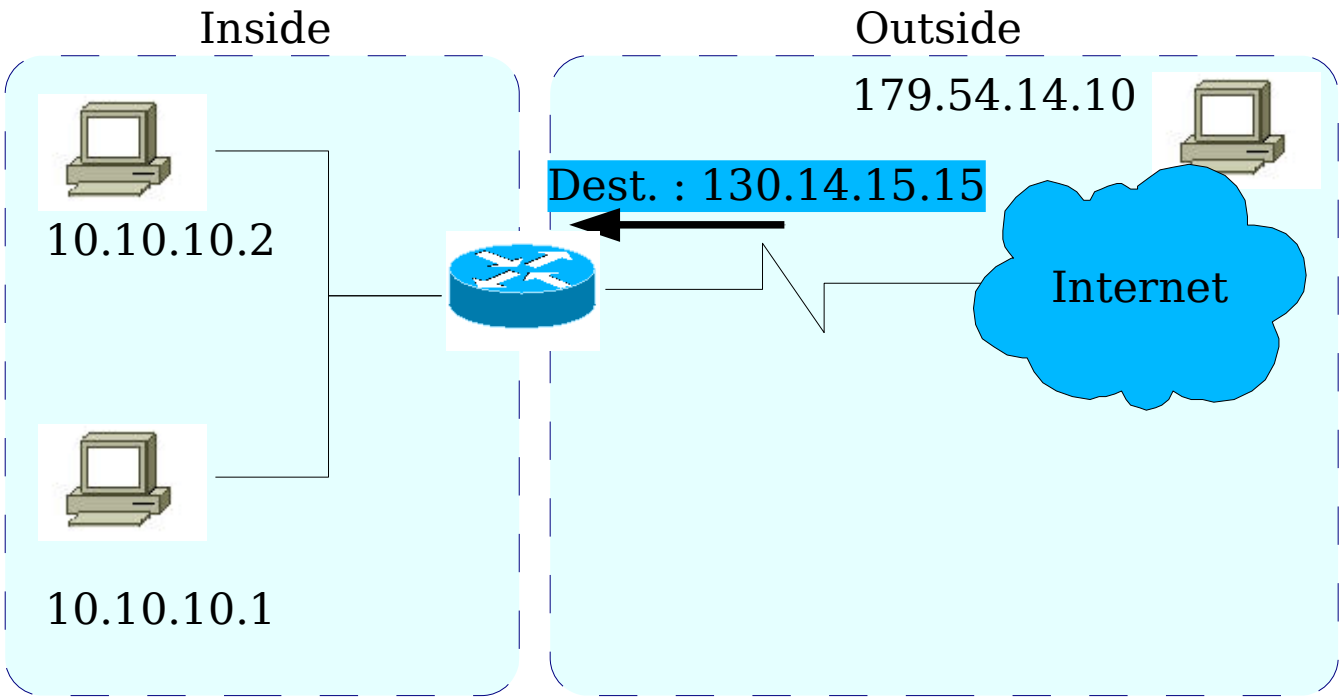
Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



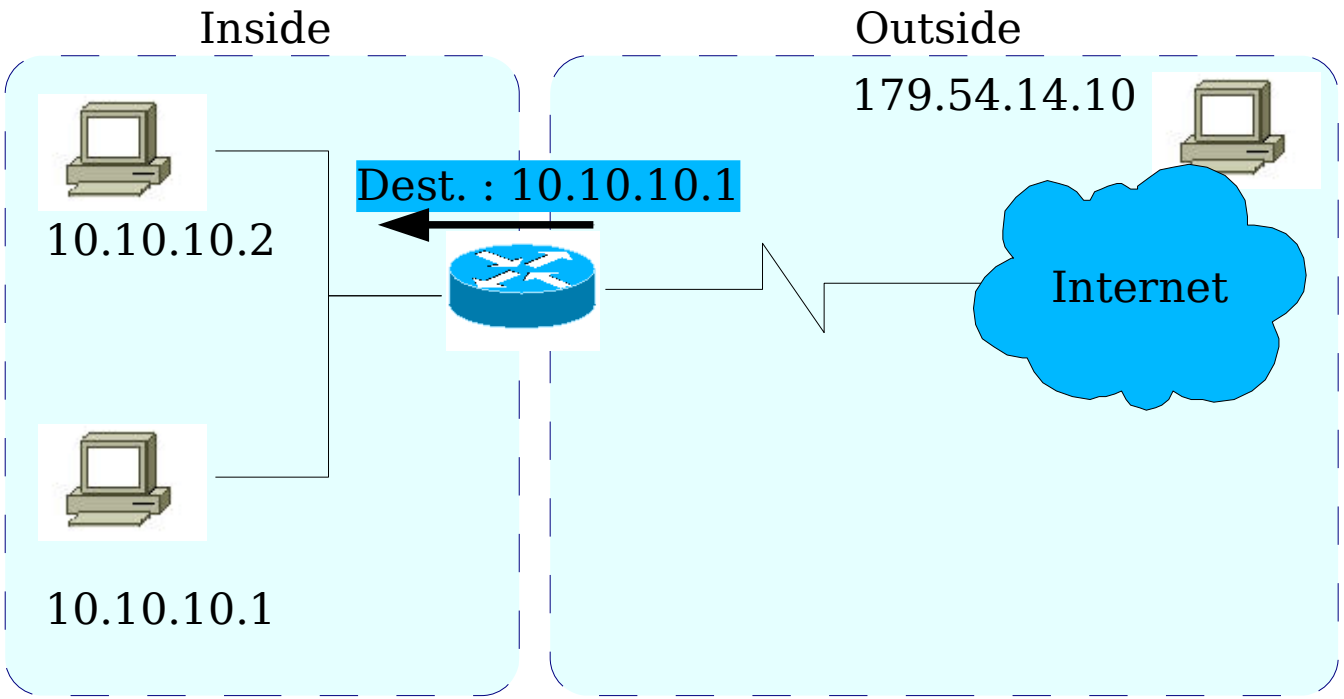
Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



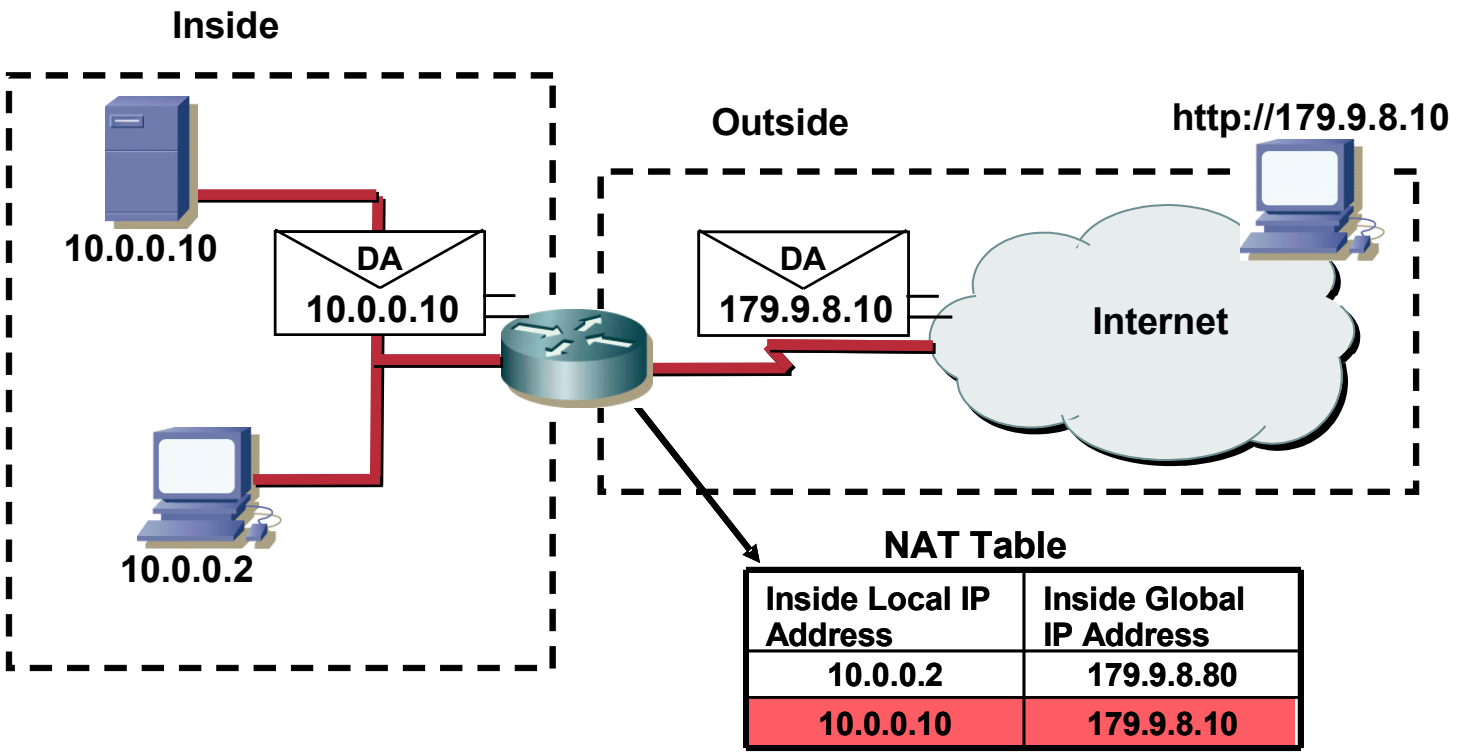
Local Inside	Global Inside	Global Outside
10.10.10.1	130.14.15.15	179.54.14.10

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 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

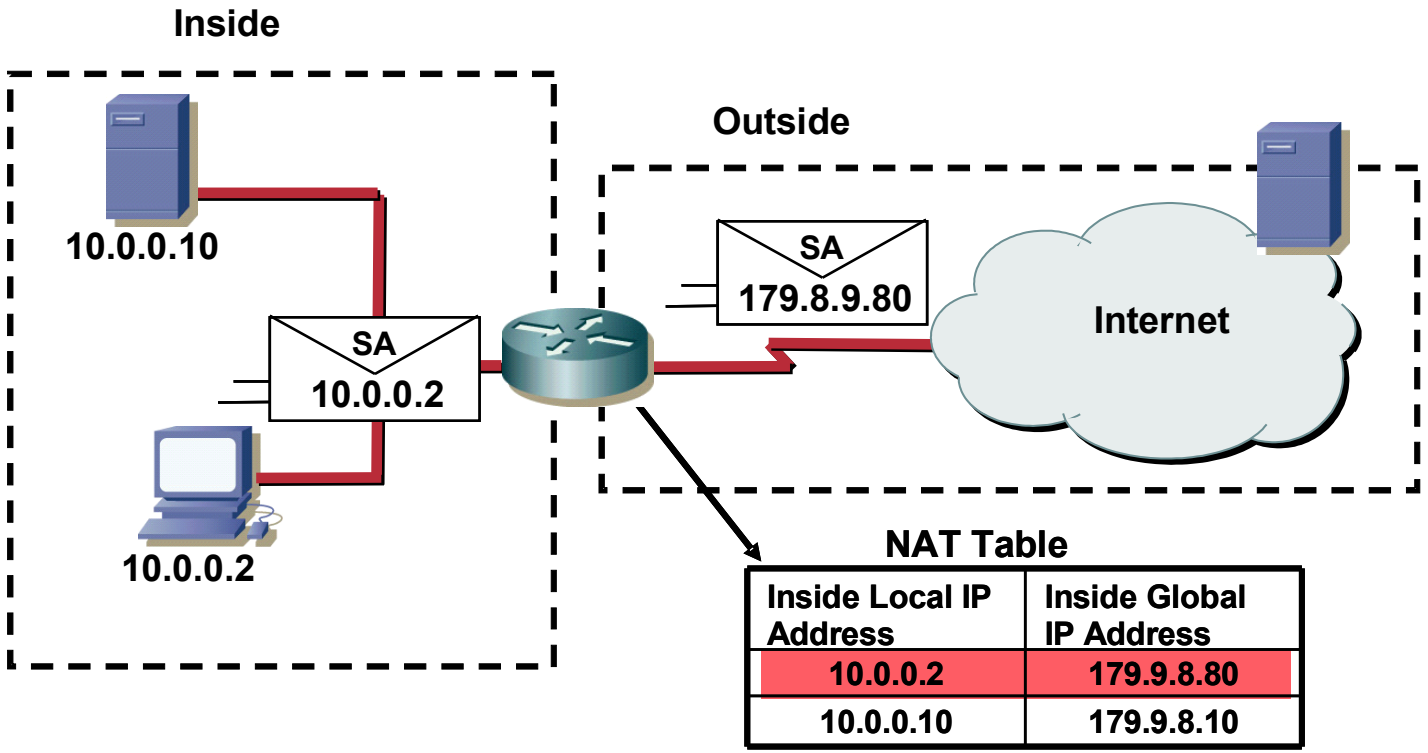
Static NAT

- NAT Statique fait une association d'une adresse locale vers une seule adresse globale : one-to-one mapping

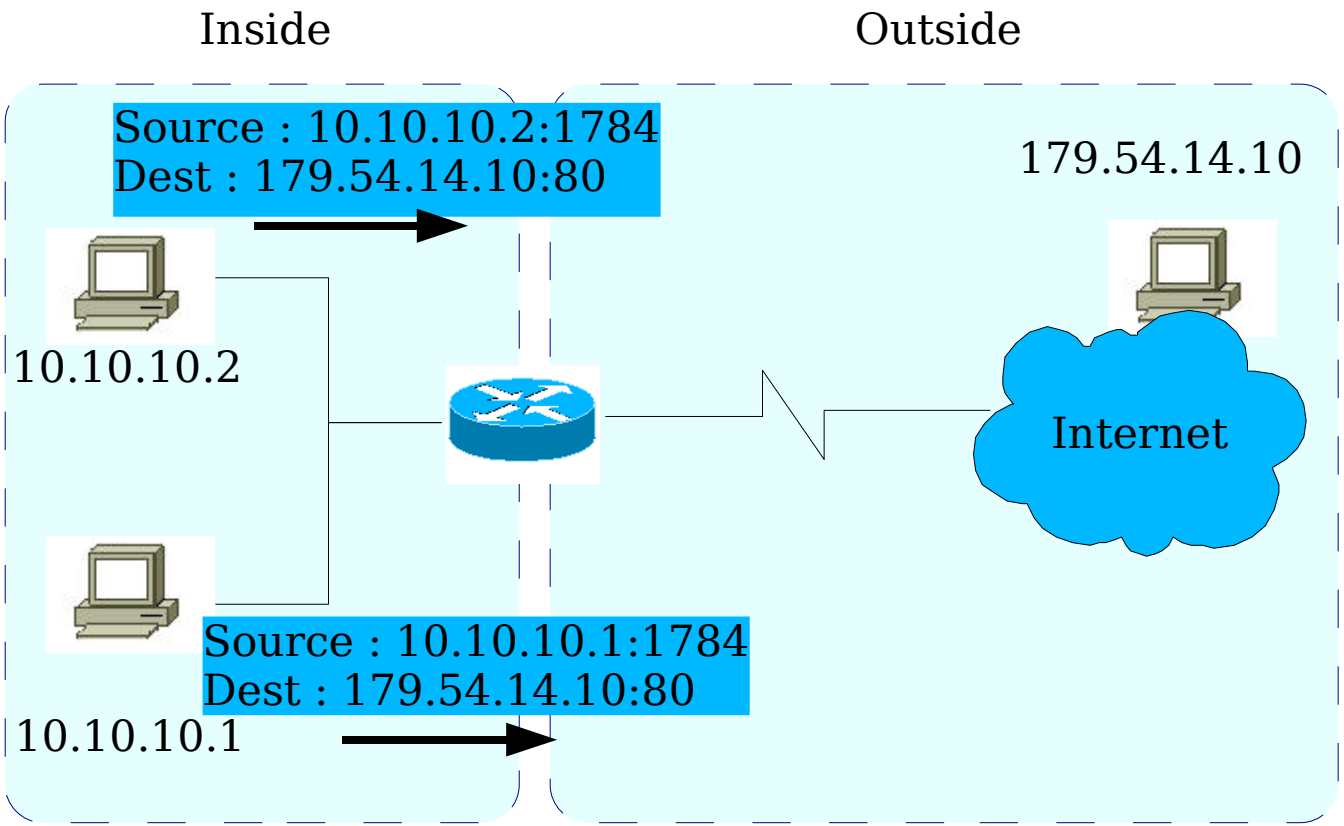


Dynamic NAT

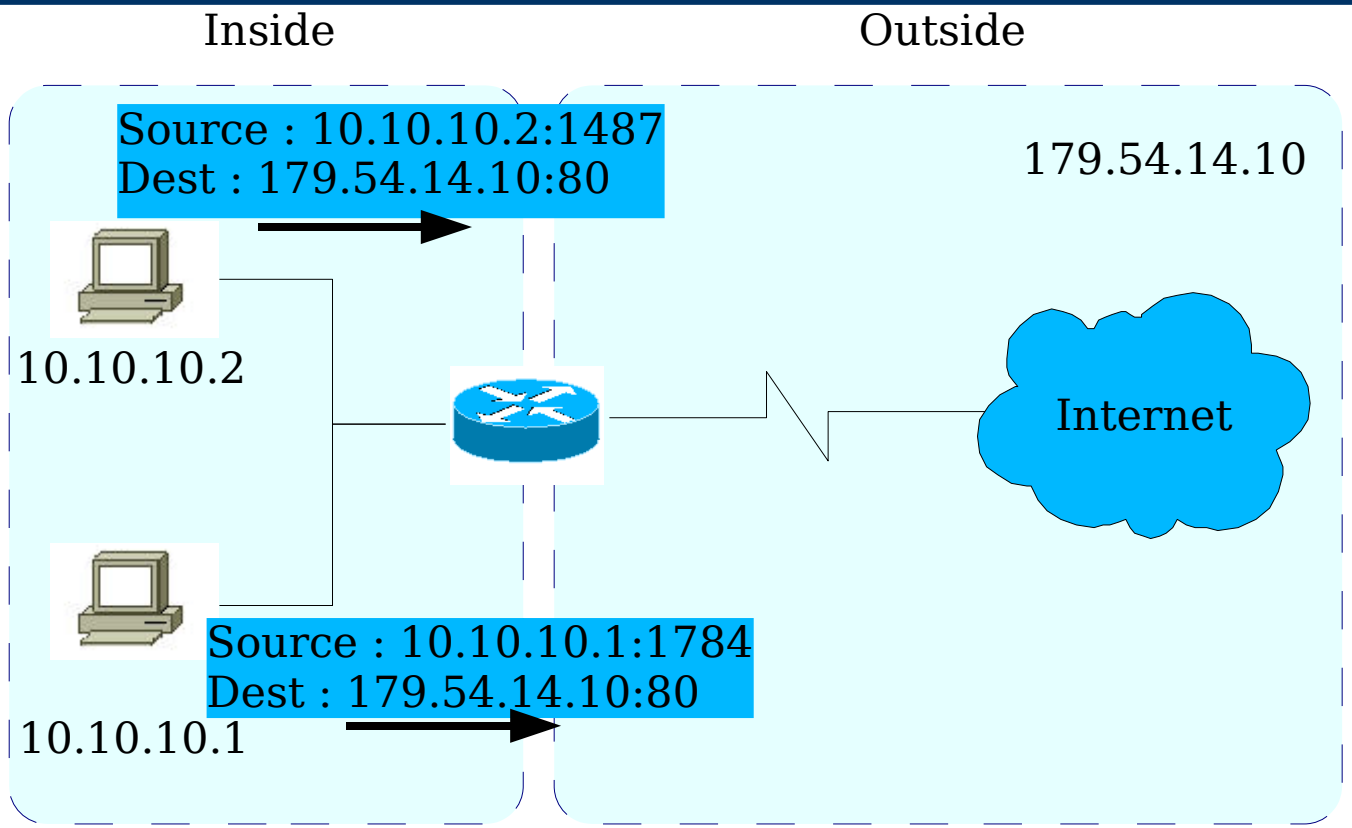
- Le NAT Dynamique permet de faire des correspondances entre une adresse locale vers une adresse globale, choisi parmi un pool



Le PAT



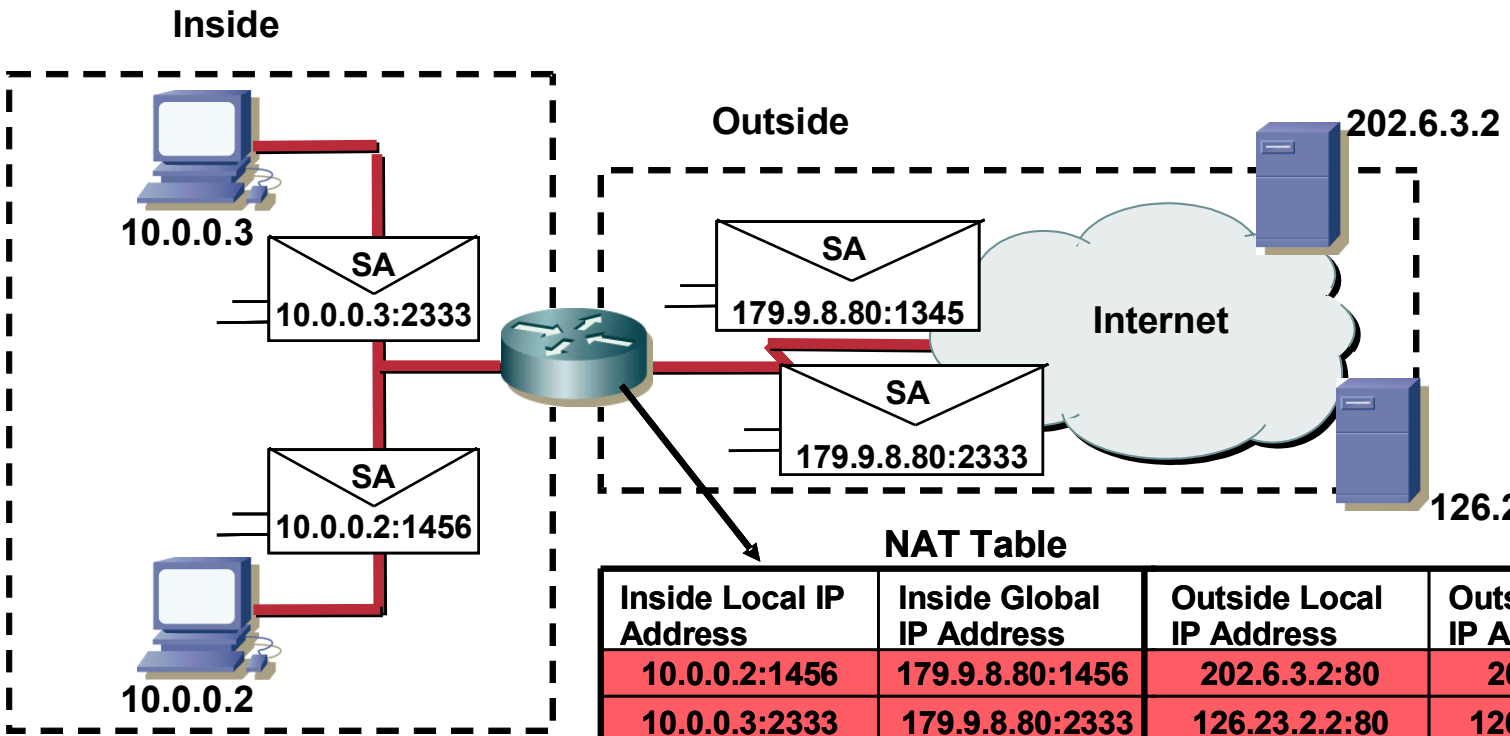
Le PAT



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

Les Outsite Local ?

- Il existe aussi des adresses Outside Local !



NAT Table

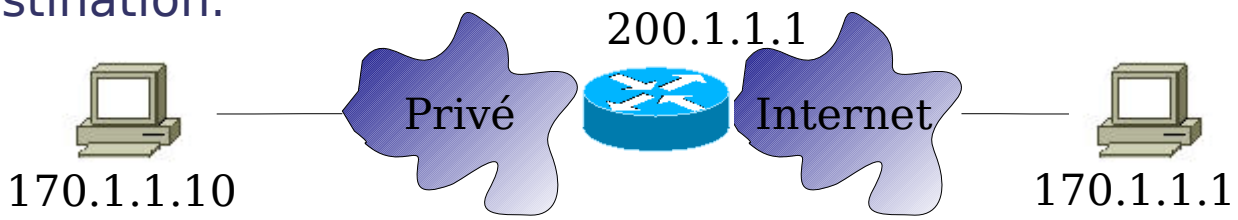
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
10.0.0.2:1456	179.9.8.80:1456	202.6.3.2:80	202.6.3.2:80
10.0.0.3:2333	179.9.8.80:2333	126.23.2.2:80	126.23.2.2:80

Les types d'adresses

- **Inside Local Addresses –** An IP address assigned to a host inside a network. This address is likely to be a RFC 1918 private address.
- **Inside Global Address –** A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP address to the outside world.
- **Outside Local Address -** The IP address of an outside host as it known to the hosts in the inside network.
- **Outside Global Address -** The IP address assigned to a host on the outside network. The owner of the host assigns this address.

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 Outside 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 de la machine de destination.

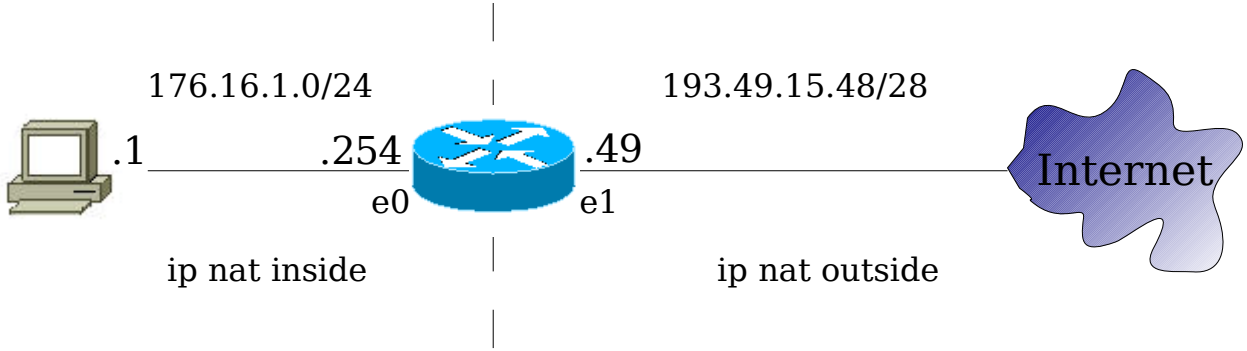


Inside Local	Outside Local	Inside Global	Outside Global
170.1.1.10	192.168.1.1	200.1.1.1	170.1.1.1

DHCP - NAT

Configuration du NAT en IOS

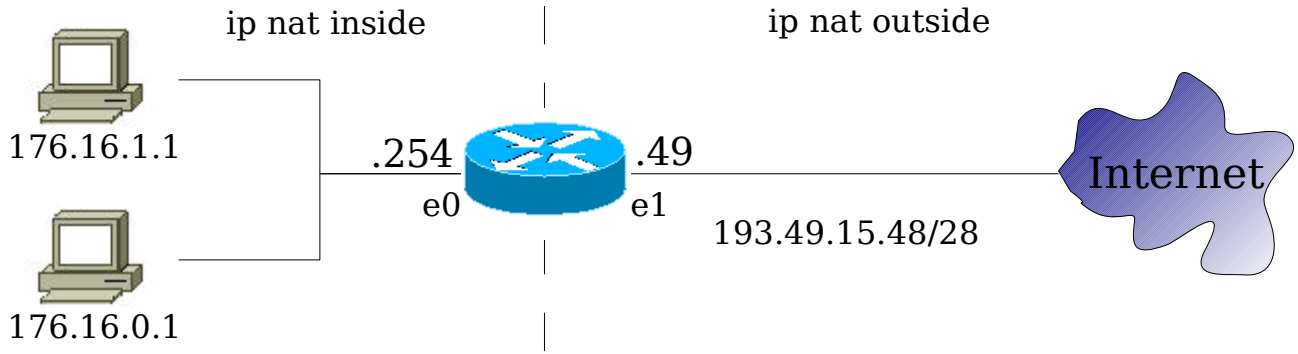
NAT statique



- 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
```

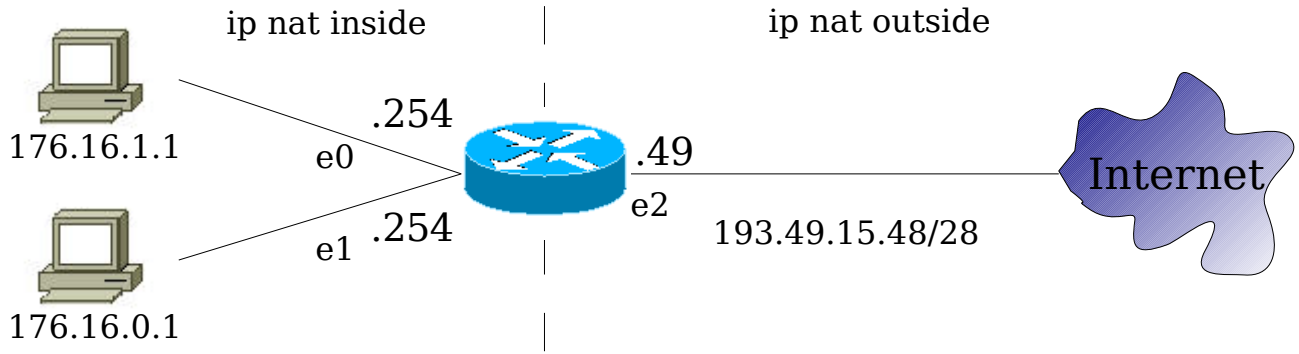
NAT dynamique



- 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 ]`*

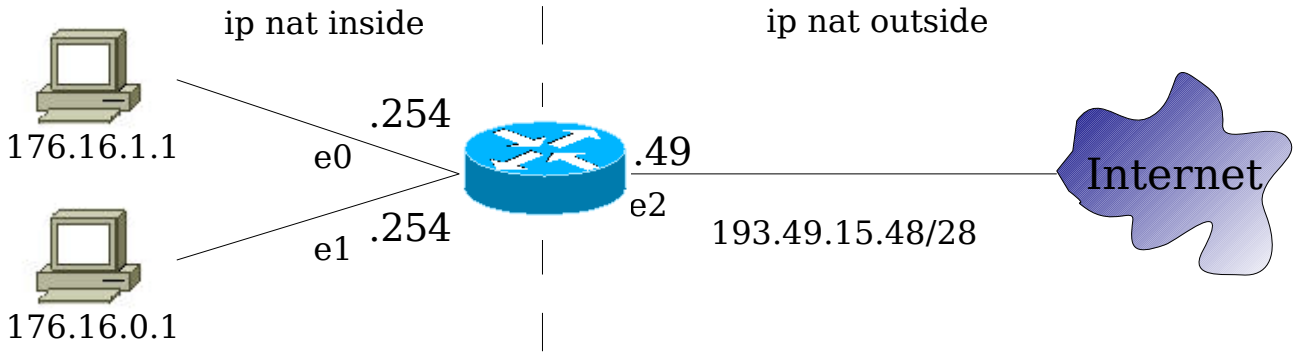
```
ip nat pool plage1 193.49.15.50 193.49.15.60
ip nat inside source liste 1 pool plage1
interface FastEthernet 0
      ip address 176.16.1.254 255.255.0.0
      ip nat inside
interface FastEthernet 1
      ip address 193.49.15.49 255.255.255.240
      ip nat outside
access-list 1 permit 176.16.1.0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

Vider la table de translation NAT

```
Router#clear ip nat translations *
```

Vérifier les configurations NAT et PAT

```
Router#show ip nat translations [verbose]
```

- Displays active translation

```
Router#show ip nat translation
Pro Inside global     Inside local      Outside local  Outside global
172.16.131.1          10.10.10.1             ---            ---
```

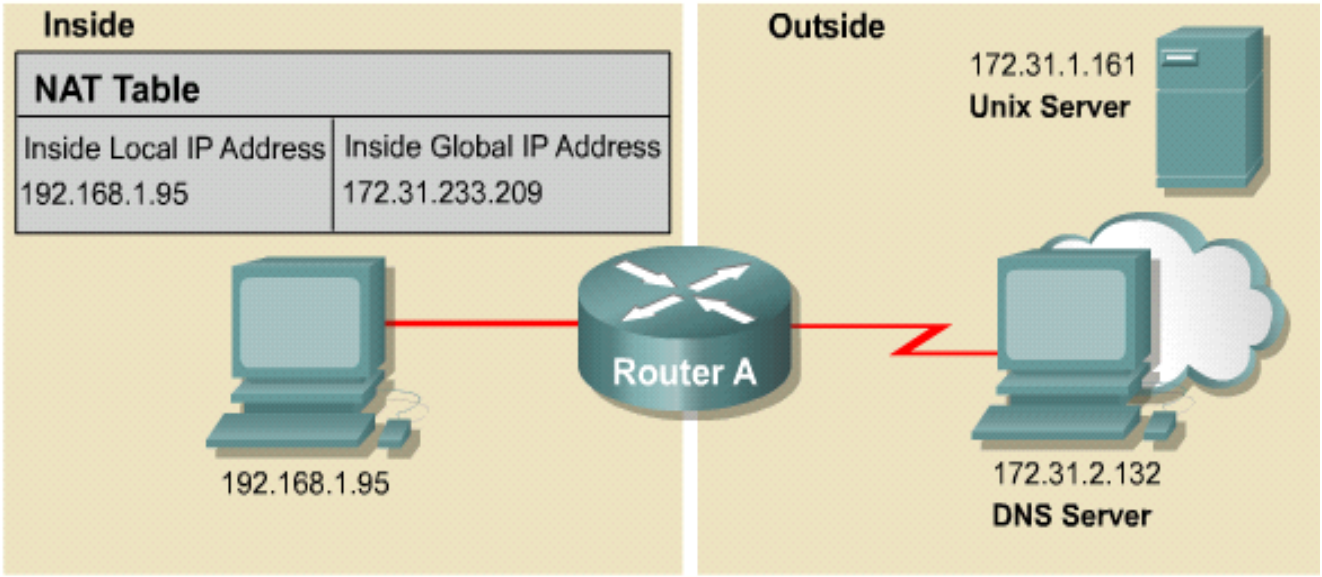
```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Command	Description
`show ip nat translations`	Displays active translations
`show ip nat statistics`	Displays translation statistics

Débugger




```
RouterA#debug ip nat
NAT:   s= 192.168.1.95    → 172.31.233.209,          d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,      → 192.168.1.95 [21852]
NAT:   s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,      → 192.168.1.95 [23311]
NAT*:  s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161      d=172.31.233.209,      → 192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,      → 192.168.1.95 [23313]
```

DHCP - NAT

DHCP

Requête du client

Ethernet Frame	IP	UDP	DHCP Request	
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: ? IP DST: 255.255.255.255	UDP 67	CIADDR: ? Mask:?	GIADDR: ? CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

Popup Window

The DHCP Client sends a directed IP broadcast, with a DHCP request packet. In the simplest case, there is a DHCP server on the same segment, which will pick up this request. The server notes the GIADDR field is blank, so the client is on the same segment. The server also notes the hardware address of the client in the request packet.

Réponse du serveur

Ethernet Frame	IP	UDP	DHCP Reply
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 GIADDR: ? Mask: 255.255.255.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

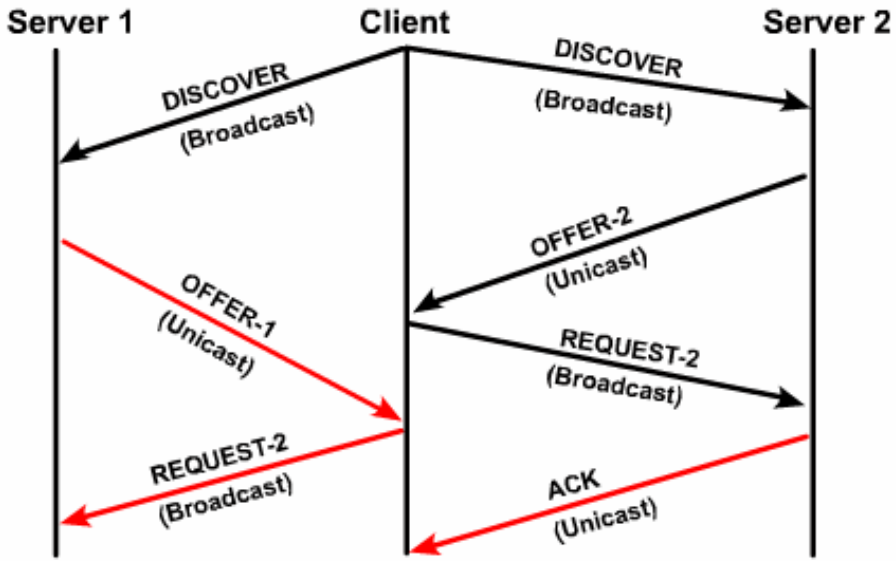
Popup Window

The DHCP server picks an IP address from the available pool for that segment, as well as the other segment and global parameters. It puts them into the appropriate fields of the DHCP packet. It then uses the hardware address of A (in CHADDR) to construct an appropriate frame to send back to the client.

Les fonctionnalités de DHCP

- Mécanismes DHCP :
  - Fournie une adresse IP pour une durée déterminée
  - Possibilité de la renouveller
- Les fonctions :
  - Allocation automatique
  - Allocation dynamique
  - Allocation manuelle

Les messages



- DHCP client broadcasts DHCP DISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCP REQUEST packet
- Selected DHCP server sends DHCP ACK packet

La configuration DHCP sur IOS

```
Router(config)#ip dhcp pool pool-name1
```

Specify the DHCP pool

```
Router(dhcp-config)#network ip-address mask
```

Specify the range of addresses in the pool

- Creates an IP DHCP pool, and gives it a name
- Up to multiple DHCP pools can be created on one server
- Specify the IP range of addresses using an IP network address and mask

Exclure des adresses

```
Router(config)#ip dhcp excluded-address
ip-address [end-ip-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

Vérification

```
Router#show ip dhcp binding
```

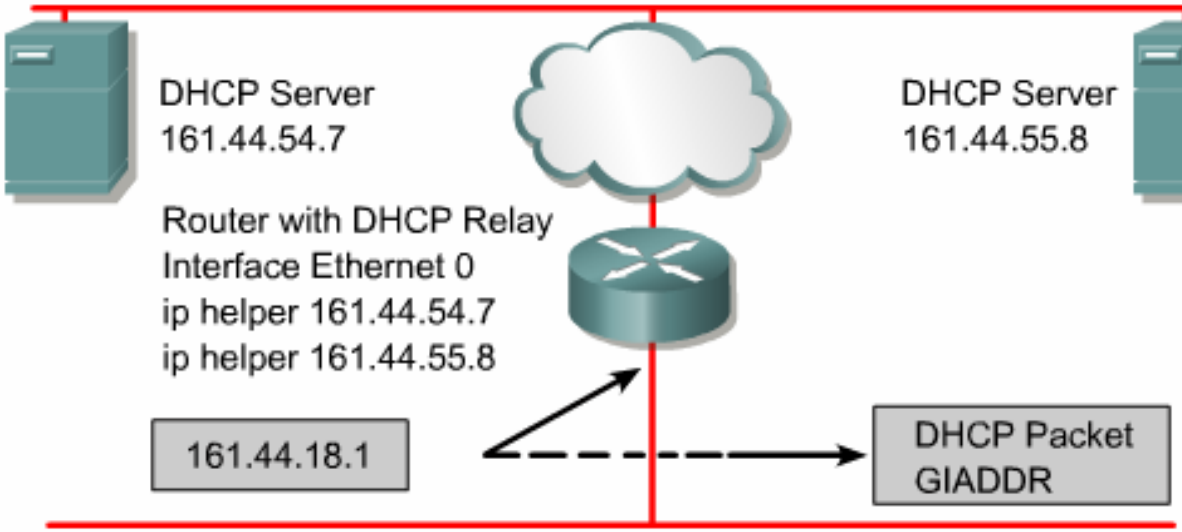
```
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration        Type
172.16.12.11    0100.10a4.97f4.6d   Mar 02 1993 12:38 AM    Automatic
Router#
```

Le débugage

```
Router#debug ip dhcp server events
```

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

LE DHCP relais



Physical Network
161.44.18.0

DHCP Client

- DHCP clients broadcasts a DHCP discover packet.
- DHCP relay (ip helper address) on the router hears the DHCP. Discover packet and fowards (unicast) the packet to the DHCP server.
- DHCP relay fills in the GIADDR field with IP address primary interface of router.
- DHCP relay can be configured to forward the packet to multiple DHCP servers; client will choose the "best" server.