Traduction d'adresses réseau (NAT) **Network Address Translation**

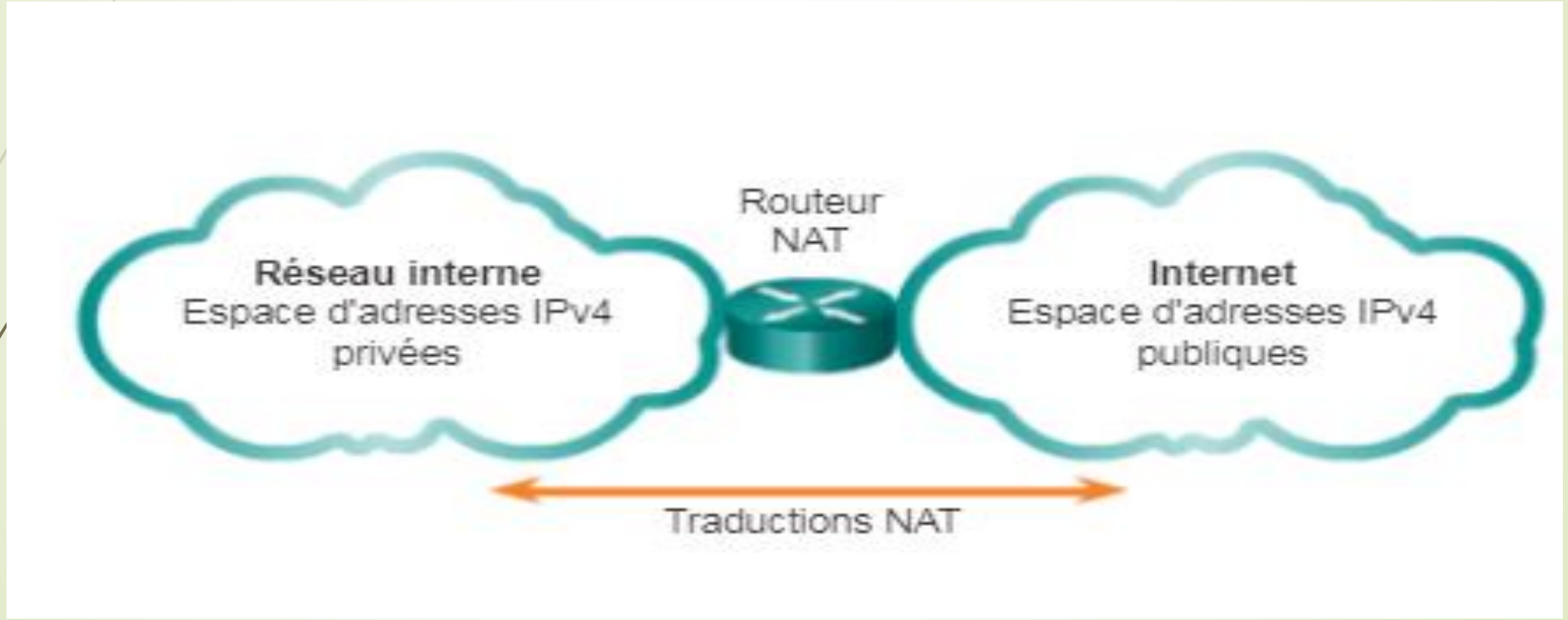
- Permet d'utiliser des adresses IP privées sur le réseau publique: l'Internet
- Remplace l'adresse IP privée par une adresse publique
- Avantage du NAT
  - Masque les adresses IP des périphériques internes
  - Un attaquant qui capture le paquet sur Internet ne peut pas déterminer l'adresse IP réelle de l'expéditeur

Espace d'adressage privé IPv4

Les adresses Internet privées sont définies dans la RFC 1918 :

Classe	Plage d'adresses internes RFC 1918	Préfixe CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Network Address Translation



La translation d'adresses (NAT)

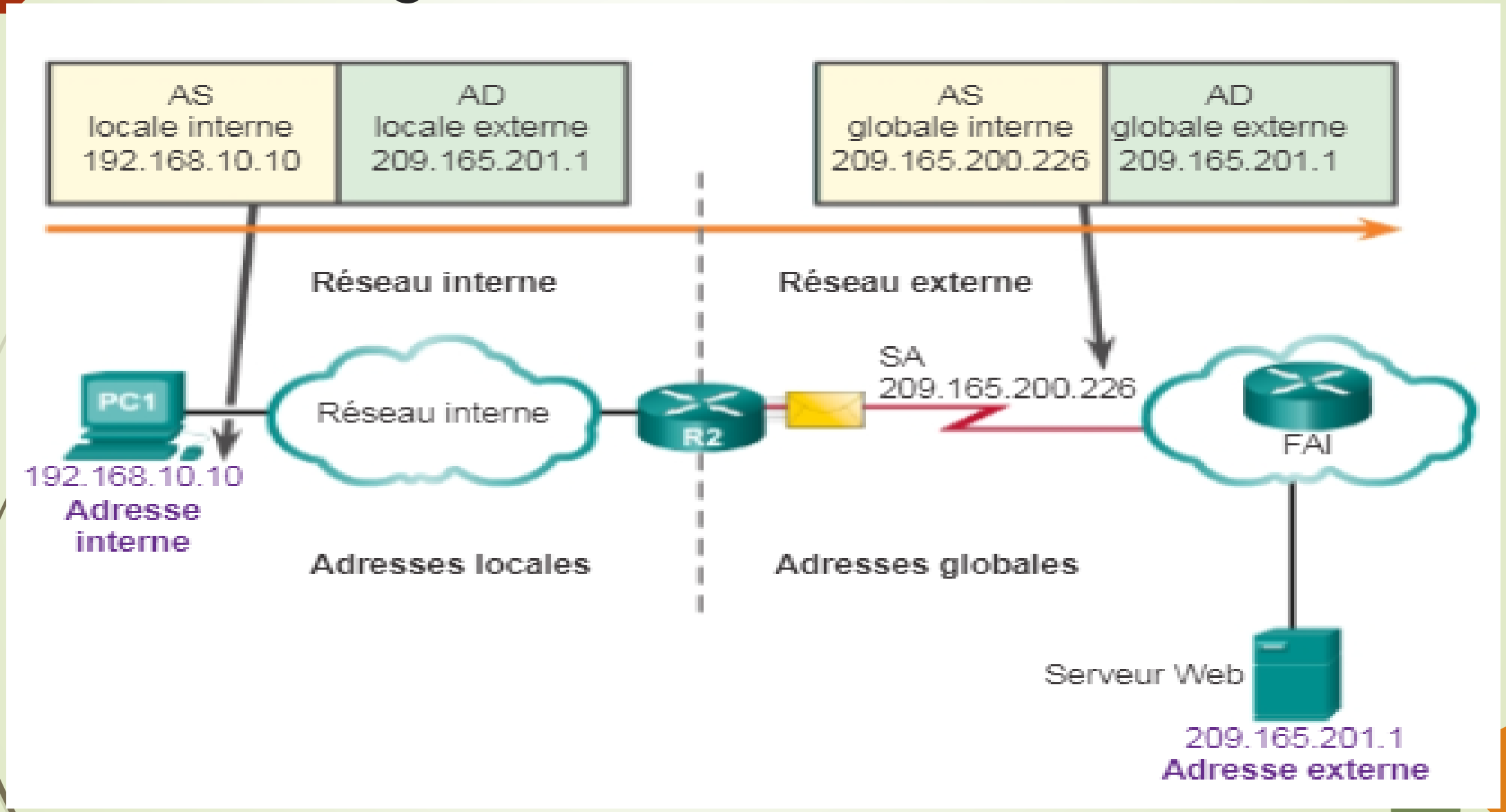
- Permet de masquer le plan d'adressage interne
- Autorise **plusieurs machines** adressées en IP « **privées** » (RFC 1918) à **accéder à Internet** par une seule IP « publique »
- **Empêche** les **connexions entrantes** depuis Internet vers un client en RFC 1918 (non routable sur Internet).

Network Address Translation

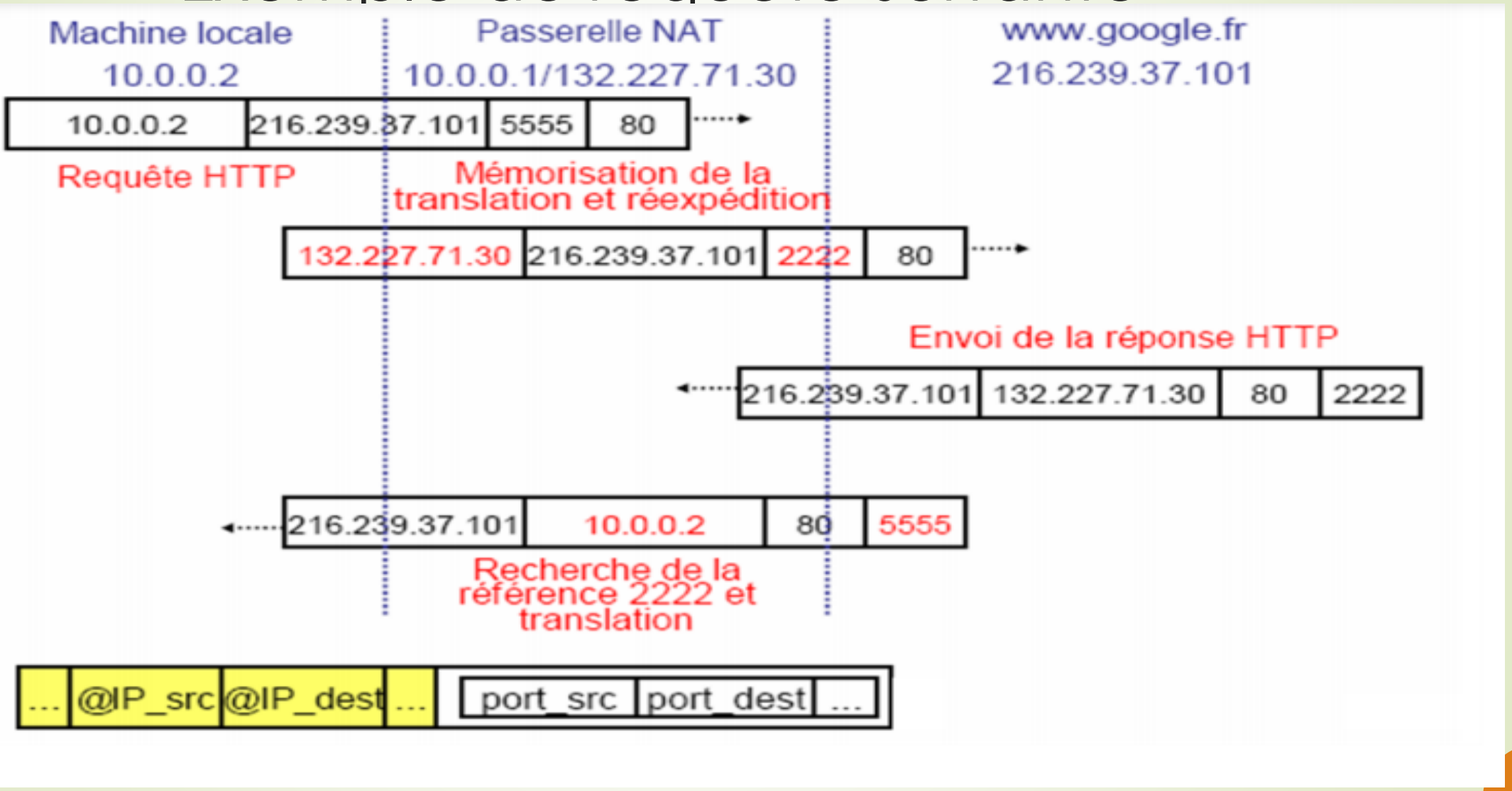
La NAT permet également d'ajouter un niveau de confidentialité et de sécurité à un réseau, car elle empêche les réseaux externes de voir les adresses IPv4 internes.

Les routeurs configurés pour la NAT peuvent être configurés avec une ou plusieurs adresses IPv4 publiques valides.
Ces adresses publiques sont appelées collectivement « pool NAT ».
Lorsqu'un périphérique interne envoie du trafic hors du réseau, le routeur configuré pour la NAT traduit l'adresse IPv4 interne du périphérique en une adresse publique du pool NAT.

Terminologie NAT



Exemple de requête sortante

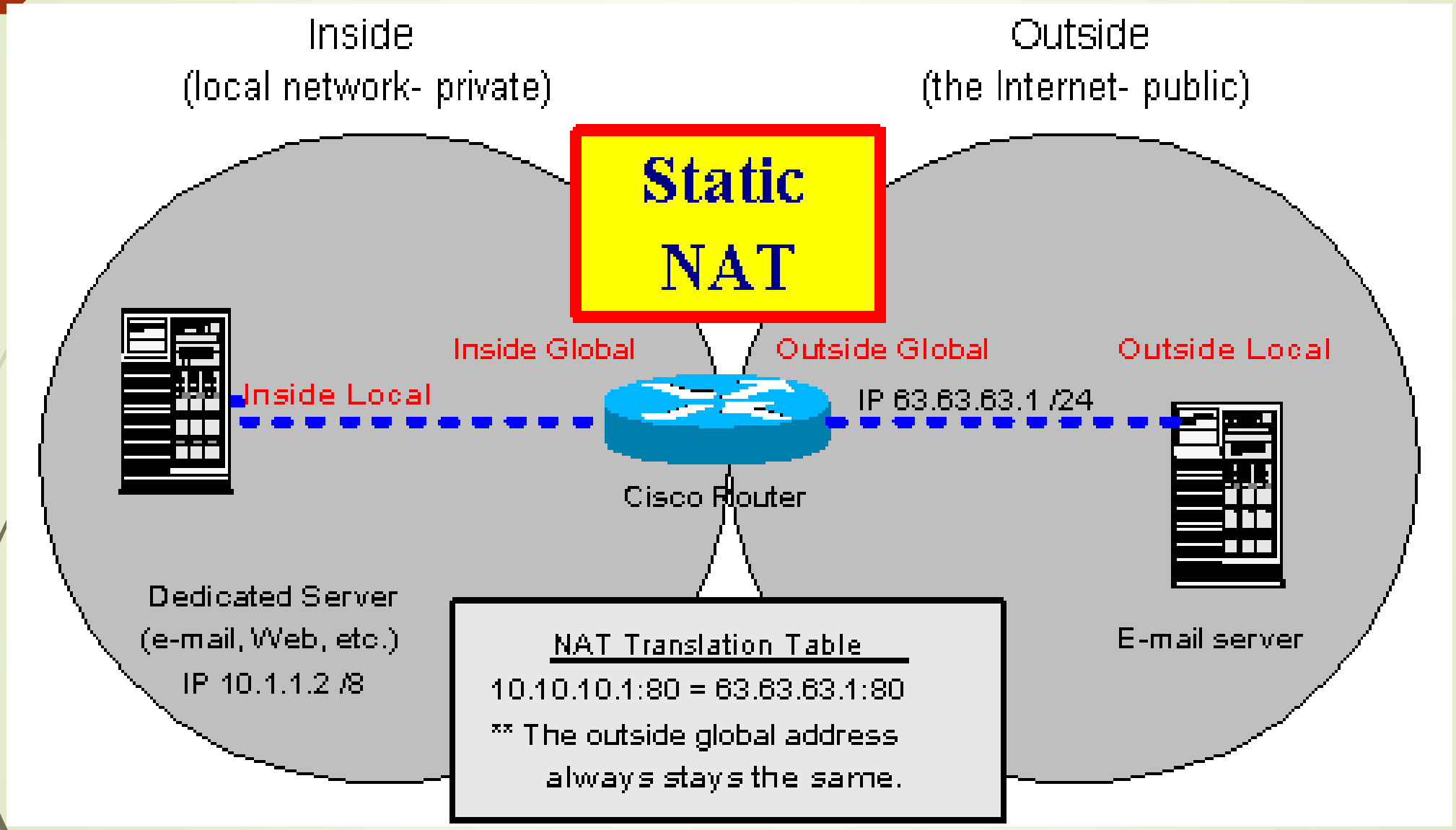


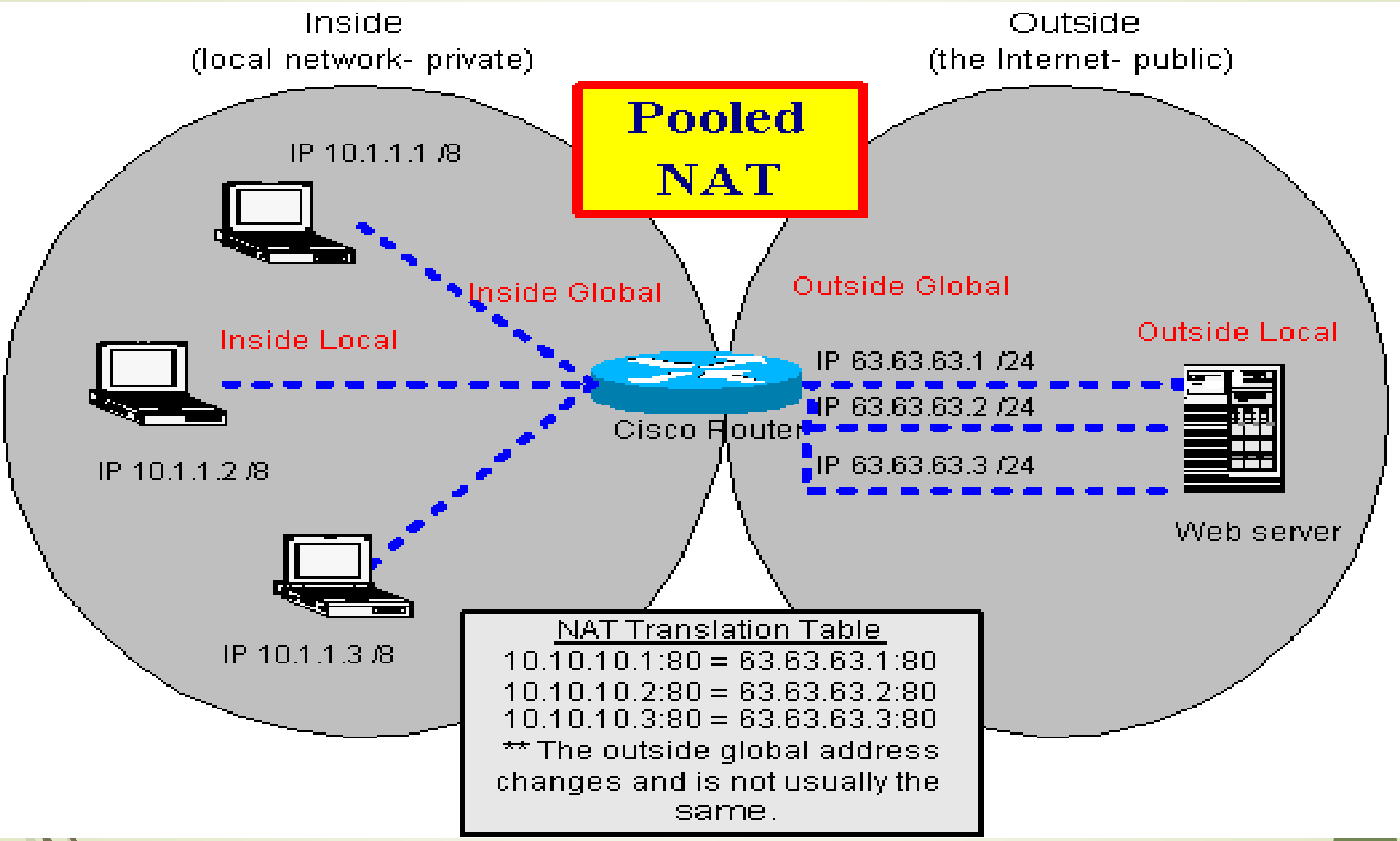
La translation d'adresses statique

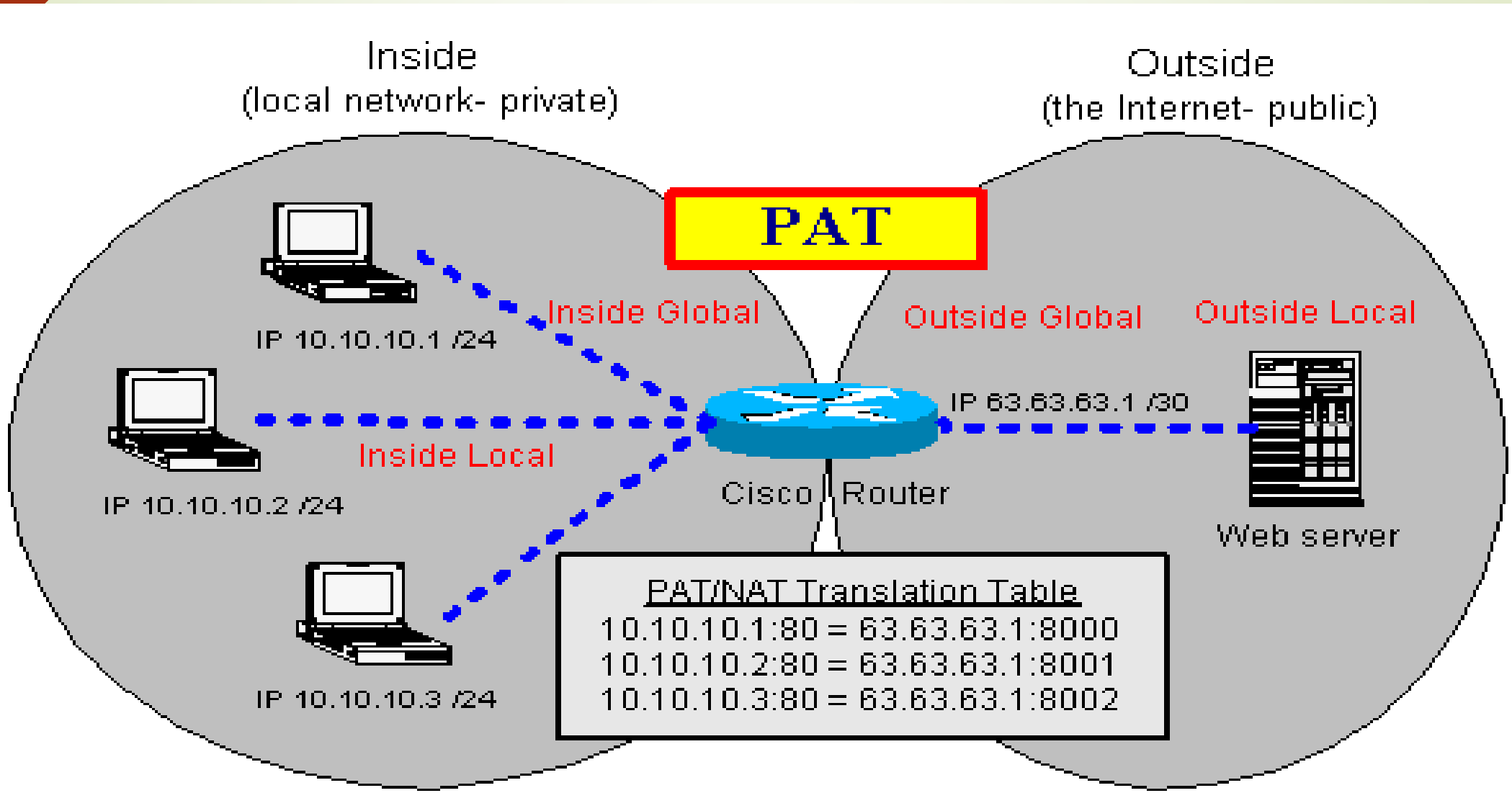
- A **une adresse officielle** (celle du pare-feu), on fait correspondre **une seule adresse** (celle du serveur)
- Utilisation :
- Serveurs devant être accessibles depuis Internet (site web, mail, DNS, etc…)

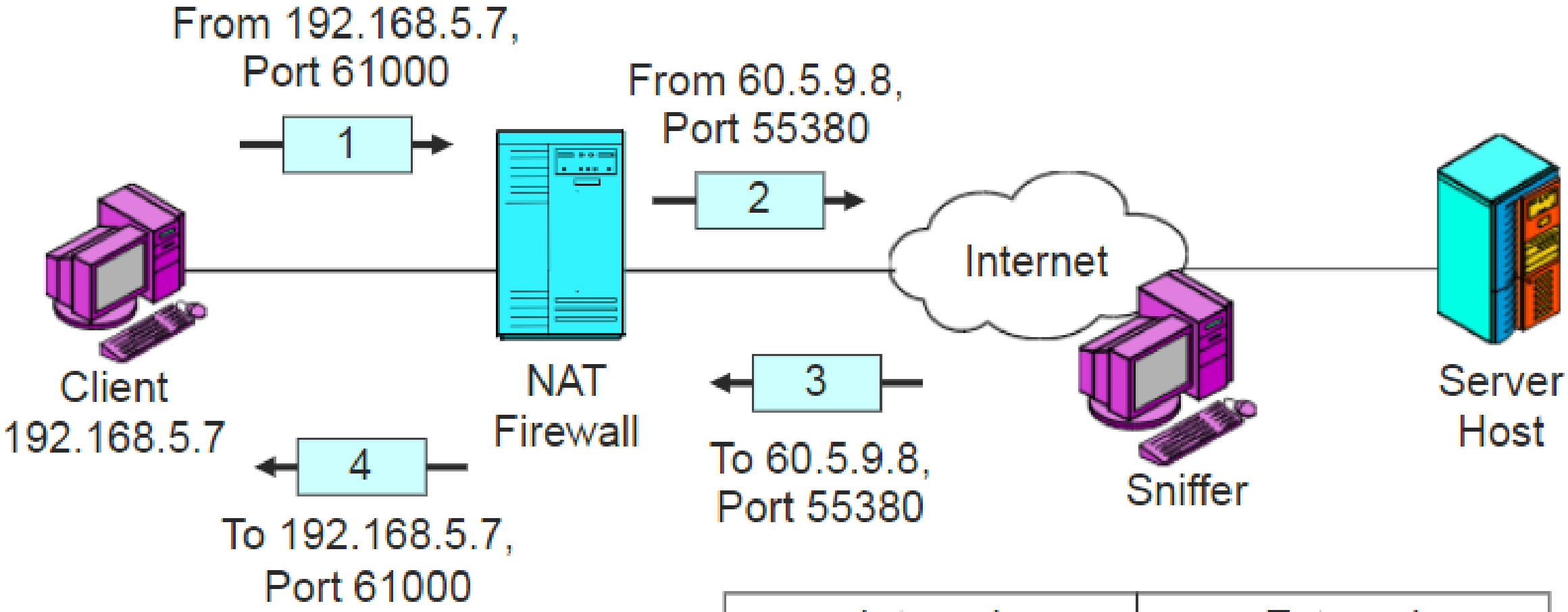
La translation d'adresses dynamique

- A **toute adresse interne**, on fait correspondre **1 seule adresse officielle** (celle du pare-feu)
- Utilisation
  - Accès des clients à Internet
- Avantages
  - Economie d'adresse IP Internet (très intéressant tant que l'on est en IPv4)
- Inconvénients
  - Difficultés avec certains protocoles à négociation de port (FTP, H323, etc…)
  - Un réseau dans le réseau


Inside
(local network- private)
Outside
(the Internet- public)
Static
NAT
Inside Global
Outside Global
Outside Local
Inside Local
IP 63.63.63.1 /24
Cisco Router
Dedicated Server
(e-mail, Web, etc.)
IP 10.1.1.2 /8
E-mail server
NAT Translation Table
10.10.10.1:80 = 63.63.63.1:80
** The outside global address
always stays the same.


Inside
(local network- private)
Outside
(the Internet- public)
Pooled
NAT
IP 10.1.1.1 /8
Inside Global
Outside Global
Inside Local
Outside Local
IP 63.63.63.1 /24
IP 63.63.63.2 /24
IP 63.63.63.3 /24
Cisco Router
IP 10.1.1.2 /8
Web server
IP 10.1.1.3 /8
NAT Translation Table
10.10.10.1:80 = 63.63.63.1:80
10.10.10.2:80 = 63.63.63.2:80
10.10.10.3:80 = 63.63.63.3:80
** The outside global address changes and is not usually the same.


Inside
(local network- private)
Outside
(the Internet- public)
PAT
Inside Global
Outside Global
Outside Local
IP 10.10.10.1 /24
IP 10.10.10.2 /24
IP 10.10.10.3 /24
Inside Local
IP 63.63.63.1 /30
Cisco Router
Web server
PAT/NAT Translation Table
10.10.10.1:80 = 63.63.63.1:8000
10.10.10.2:80 = 63.63.63.1:8001
10.10.10.3:80 = 63.63.63.1:8002



Translation Table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

Configuration du NAT statique

Une translation statique consiste à associer une adresse IP privée à une adresse IP publique routable qui lui est réservée.

Pour indiquer au routeur qu'il doit faire une translation d'adresse statique pour une machine particulière, on utilise la commande :

Router(config)#ip nat inside source static @IP-privée-machine @IP-publique

```
Router(config)#ip nat inside source static 192.168.1.2 10.0.0.1
Router(config)#
```

R1(config)#int fa0/1

R1(config-if)#ip nat **inside**

R1(config-if)#exit

R1(config)#int s0/0

R1(config-if)#ip nat **outside**

R1(config-if)#exit

Configuration du NAT avec pool d'adresses

Définir le groupe d'adresses publiques en utilisant la commande ip nat pool

Router(config)#ip nat pool nom-plage @IP_départ @IP_fin netmask masque_réseau

Définir la traduction NAT en utilisant la commande ip nat inside source

Router(config)#ip nat inside source list numero_liste_acces pool nom-plage

```
Router(config)#ip nat pool POOL-NAT 10.0.0.1 10.0.0.4 netmask 255.255.255.240
Router(config)#ip nat inside source list 1 pool POOL-NAT
```

Configuration du NAT dynamique avec surcharge (sans pool) = PAT = Translation d'adresse et de port

Puis il suffit d'indiquer au routeur de faire une translation d'adresse et de port au même temps pour toutes les adresses dans la liste d'accès grâce au mot clé overload :

Router(config)# ip nat inside source list <numéro> interface <nom-if> overload

— numéro : numéro de la liste d'acces dans le router

— nom-if : nom de l'interface du routeur dont l'adresse IP sera utilisé comme adresse publique

```
Router(config)#ip nat inside source list 1 interface fa0/1 overload
```

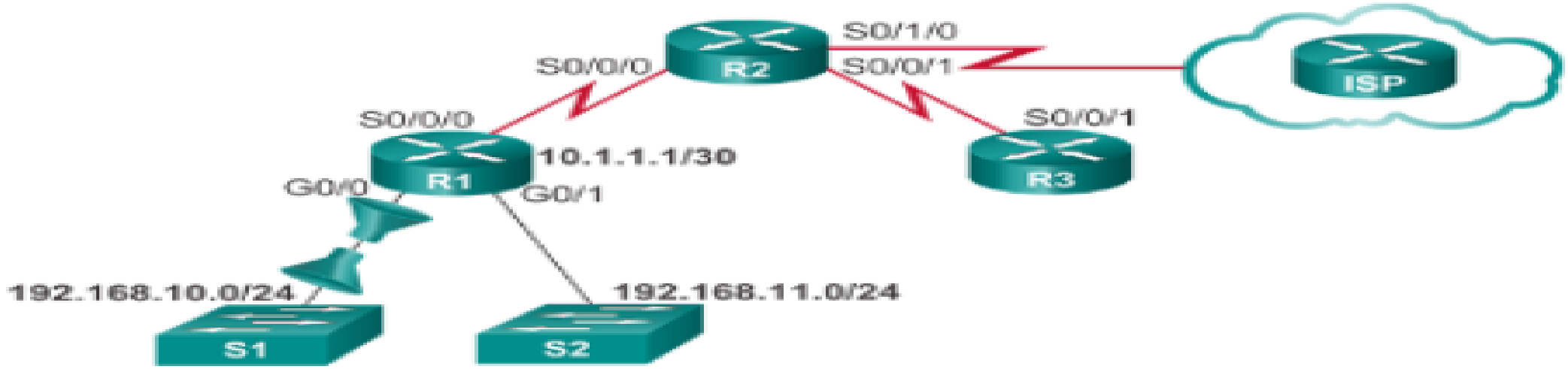
Les Access Control Lists (ACL) avancées

Les ACL TCP Established

Ce type d'ACL est utilisé notamment lorsque du trafic TCP est mis en œuvre sur le réseau. On les utilise principalement lorsque l'on souhaite autoriser des sessions TCP initiées depuis notre réseau "de confiance" à destination d'un réseau de "non-confiance",

Nous devons donc créer une ACL qui va laisser passer les paquets par l'interface Ethernet0 lorsqu'ils possèdent des flags ACK (confirmation)

Création de listes de contrôle d'accès étendues nommées




```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255
established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```

established : autorise le trafic TCP si les paquets utilisent une connexion établie (bit de ACK)

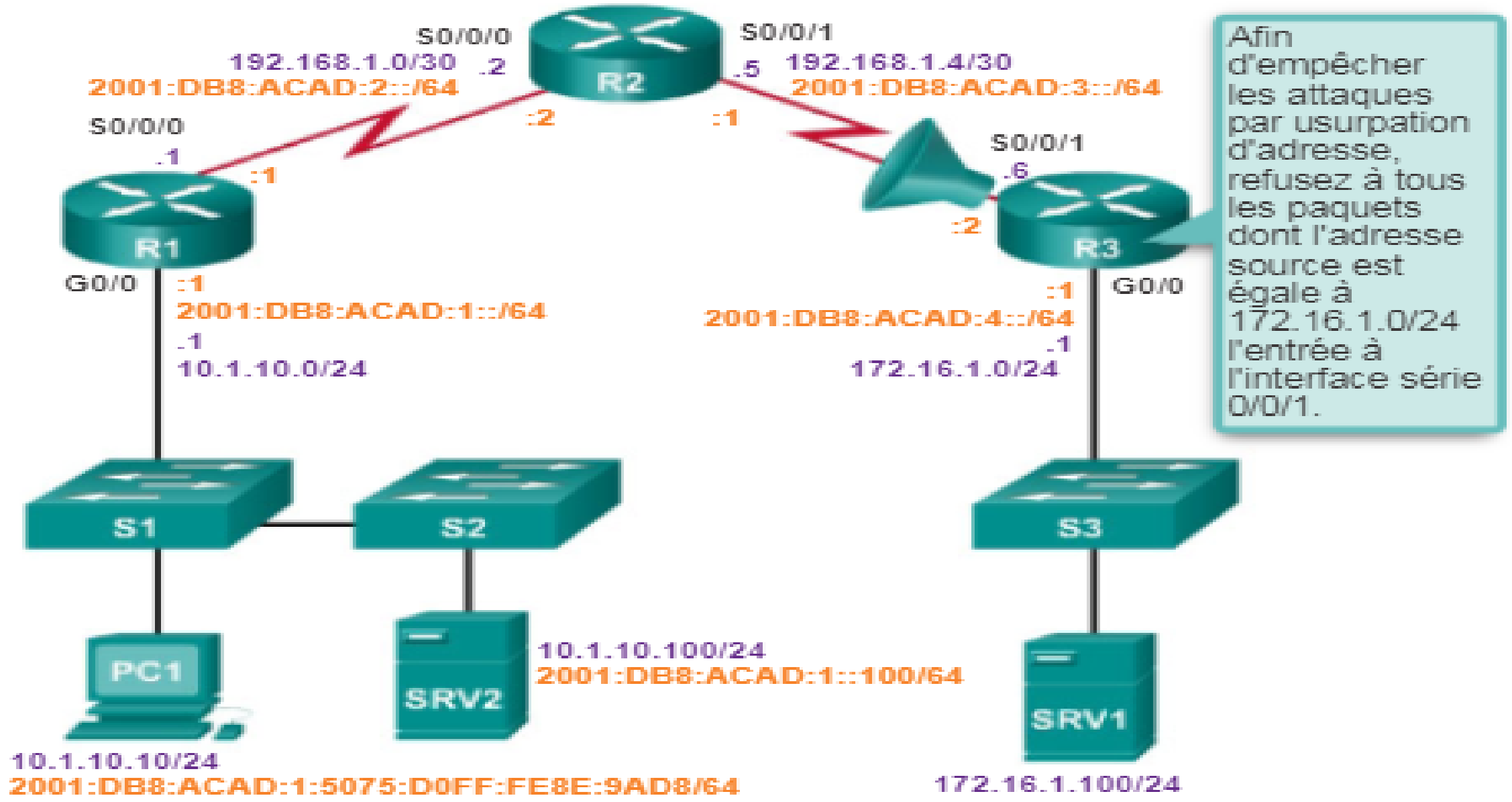
Modification des listes de contrôle d'accès étendues

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.11.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq
www
R1(config-ext-nacl)# end
R1#
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

Devrait être 192.168.10.0.

Modification des listes de contrôle d'accès standard nommées


```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
     15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```


S0/0/0
192.168.1.0/30
.2
2001:DB8:ACAD:2::/64
S0/0/1
.5
192.168.1.4/30
2001:DB8:ACAD:3::/64
R2
:2
:1
S0/0/0
.1
:1
R1
S0/0/1
.6
:2
R3
G0/0
:1
2001:DB8:ACAD:1::/64
.1
10.1.10.0/24
:1
2001:DB8:ACAD:4::/64
.1
172.16.1.0/24
G0/0
Afin d'empêcher les attaques par usurpation d'adresse, refusez à tous les paquets dont l'adresse source est égale à 172.16.1.0/24 l'entrée à l'interface série 0/0/1.
S1
S2
S3
PC1
SRV2
10.1.10.100/24
2001:DB8:ACAD:1::100/64
SRV1
10.1.10.10/24
2001:DB8:ACAD:1:5075:D0FF:FE8E:9AD8/64
172.16.1.100/24