Network Address Translation

- Généralités
  - Adresses privées
  - Problématique et solution
  - Définition et type de traduction
  - Avantages /Inconvénients
- Mise en œuvre "classique" de la traduction

Constat

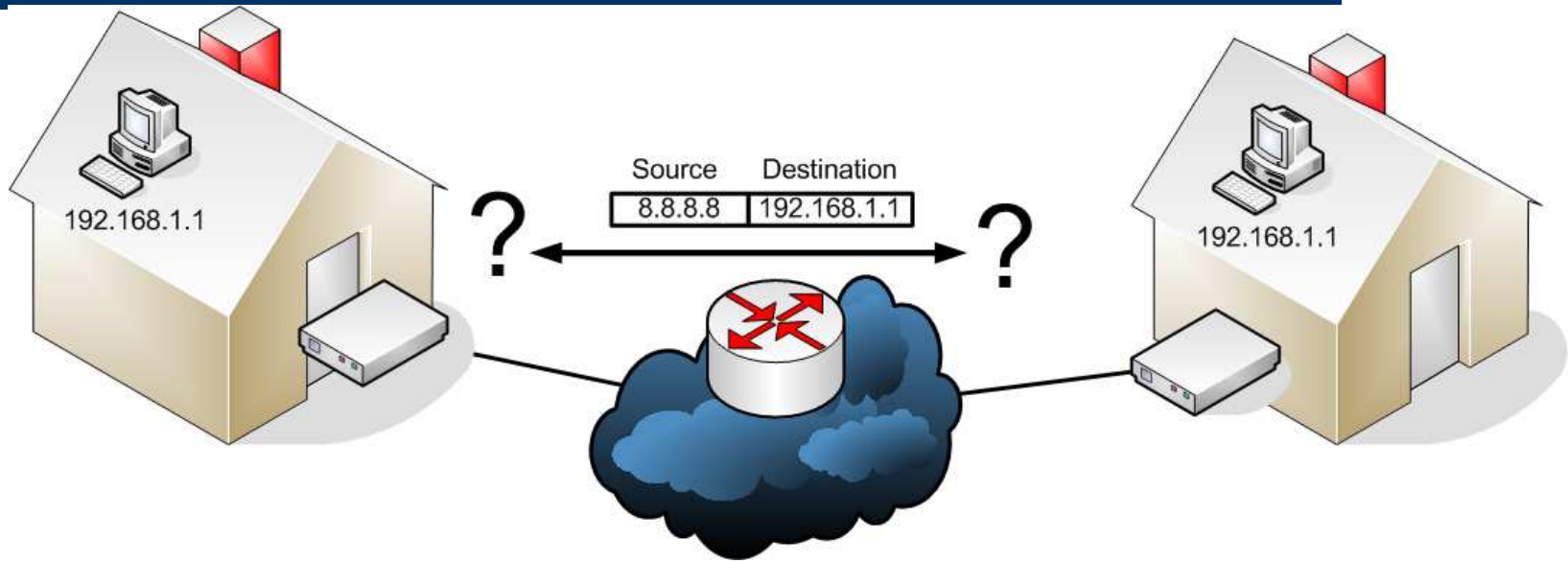
- Plus aucune adresses IPv4 disponibles vers 2021
- Solutions
  - VLSM
  - Protocole NAT (Network Address Translation)
  - Passage à IPv6

Adresses privées

- Adresses dîtes non-routable
- Adresses pouvant être utilisées par tous (mais pas n'importe comment) sans accord du FAI/RIR/IANA
- 3 plages possibles

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

Problème hypothétique de l'adressage privé

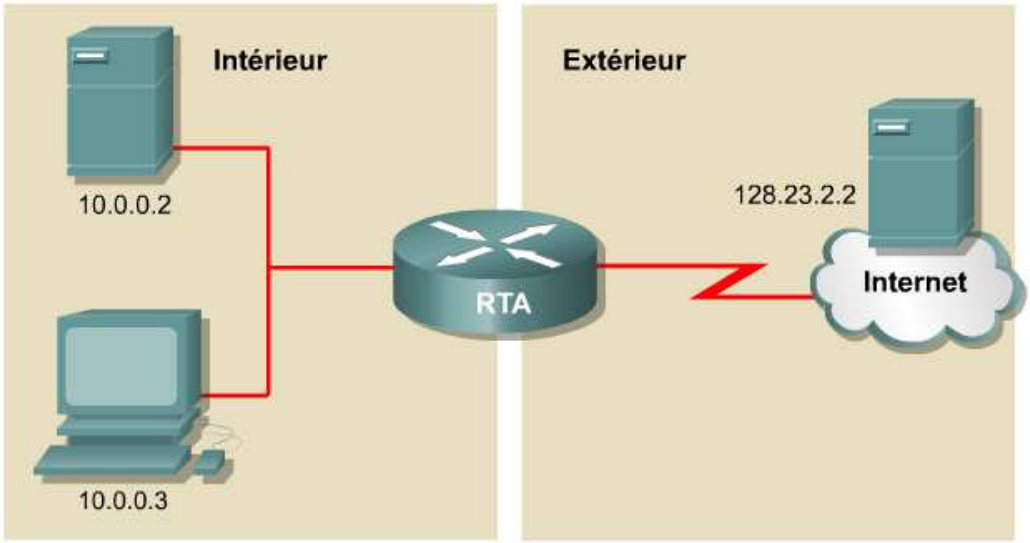


- Comme plusieurs machines pourraient avoir la même adresse, il pourrait y avoir un conflit d'adressage !

  Pour empêcher ces conflits, les routeurs ne doivent jamais acheminer d'adresses privées dans le réseau public

Problème du non routage des adresses privées

- Comment les utilisateurs du réseau intérieur vont-ils accéder à internet (le réseau extérieur) ?

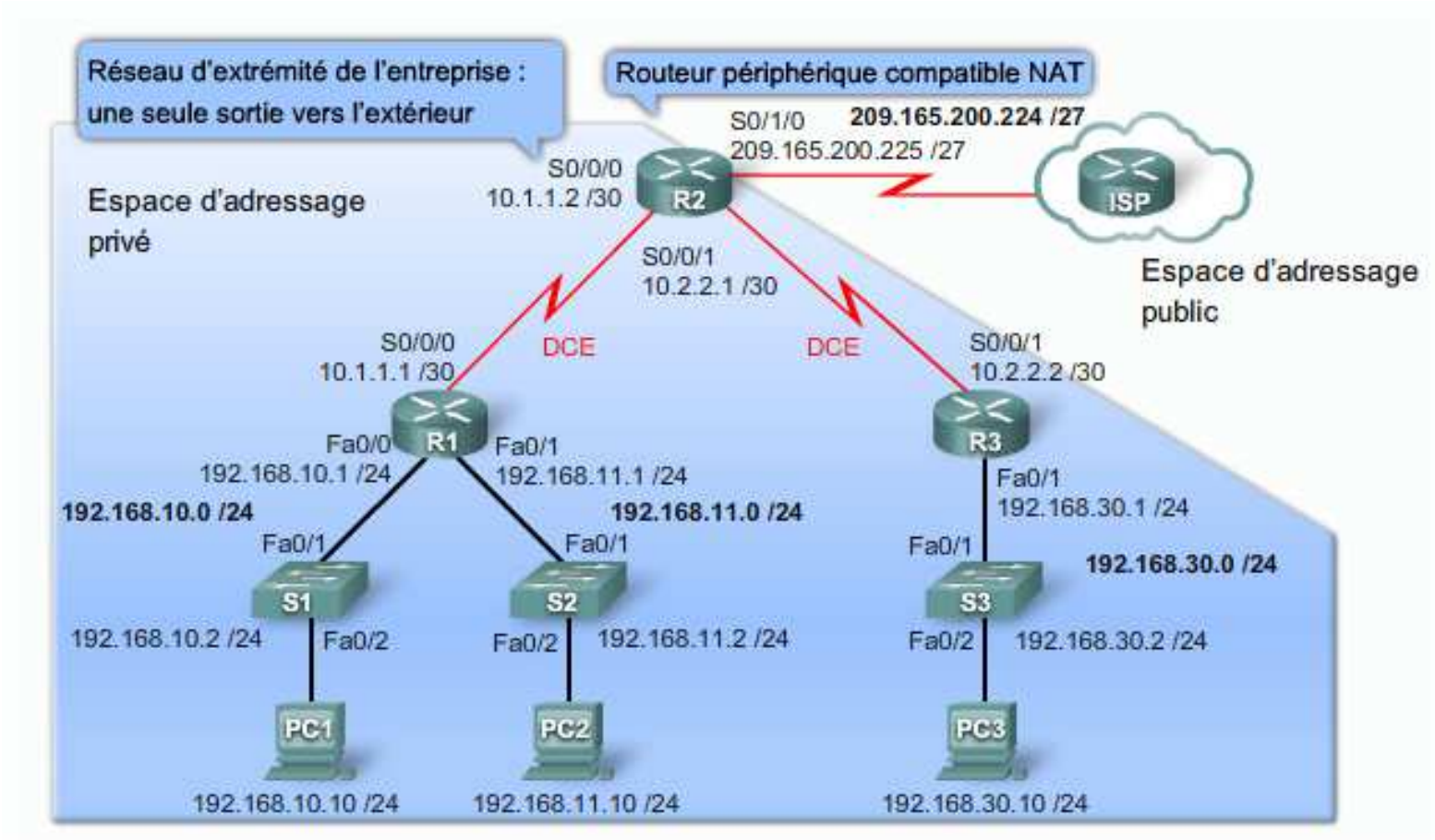


- Solution : traduction des adresses privées en adresses publiques

Avantages

- Ménage le modèle d’adressage enregistré légalement
  - Utilisation de plage d'adresses à des fins spécifiques
  - Autorise sur une même adresse publique le multiplexage au niveau du port de l’application
- Assure la cohérence des schémas d’adressage du réseau interne
  - Plus de réattribution d’une nouvelle adresse IP à chaque hôte lors du passage à un nouveau FAI
  - Facilite la migration de serveur
- "Assure la sécurité du réseau" : les réseaux internes ne divulguent pas leurs adresses ou leur topologie

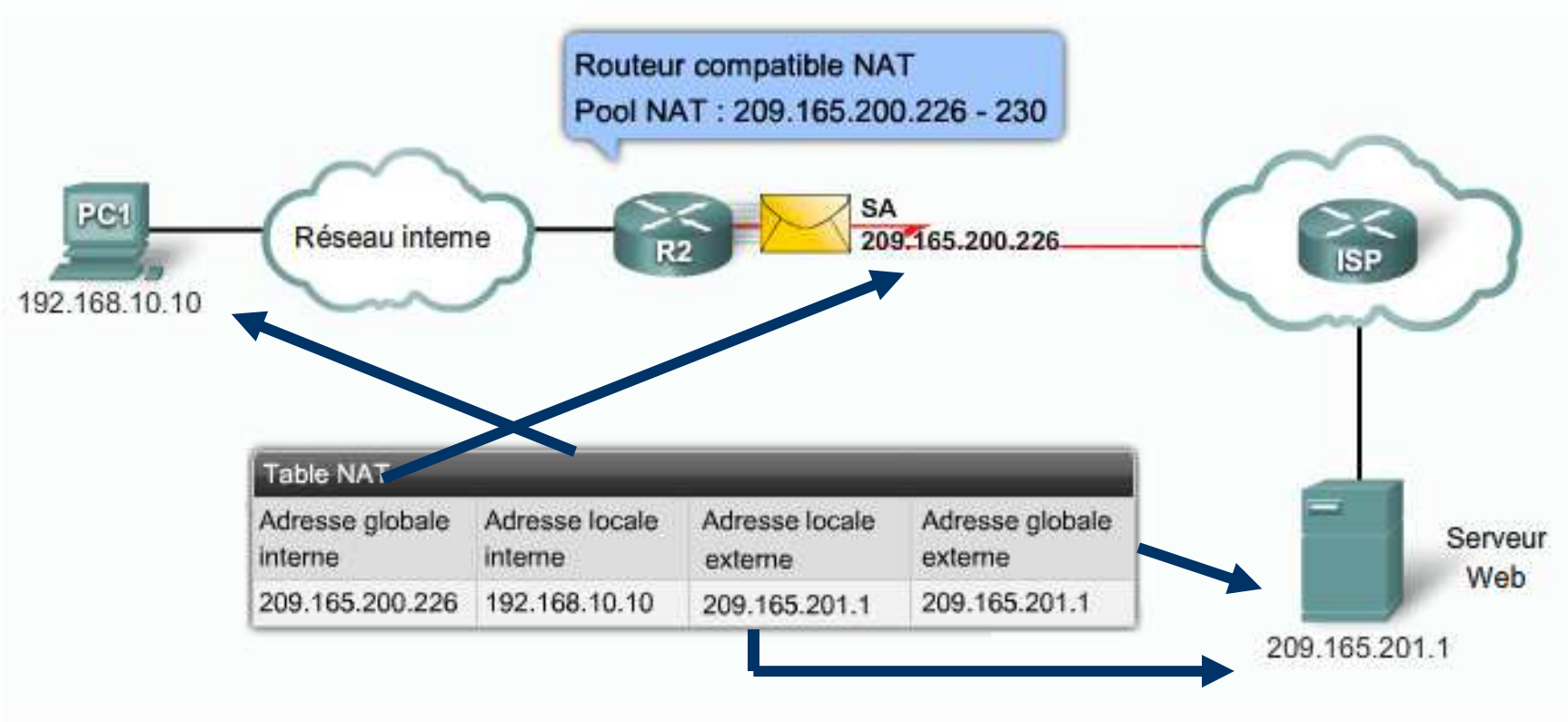
Cas typique d'utilisation



Inconvénients

- Les performances sont affectées
- Les fonctionnalités de bout en bout sont affectées (notamment quand un protocole transporte les adresses IP dans les données – FTP, NetBios, H.323, etc. -)
- La traçabilité IP de bout en bout est perdue
- La transmission tunnel est plus compliquée

Définition (I)



Définition (II)

- **Adresse locale interne (Inside local address)** - L'adresse de la machine interne dans le réseau intérieur. Il s'agit probablement d'une adresse privée
- **Adresse globale interne (Inside global address)** : L'adresse de que prendra la machine interne dans le réseau extérieur. Il s'agit probablement d'une adresse publique
- **Adresse globale externe (Outside global address)** : L'adresse de la machine externe dans le réseau extérieur
- **Adresse locale externe (Outside local address)** - L'adresse de la machine externe dans le réseau intérieur. Cette adresse sera très souvent identique à l'adresse globale externe.

Types de traduction NAT

- Statique : correspondance unique entre une adresse locale et une adresse globale ;
  - la correspondance est permanente
  - utilisée pour "externaliser" des serveurs situés en interne
- Dynamique : mise en correspondance, selon la méthode du premier arrivé - premier servi, des adresses locales avec une plage d’adresses globales, et vice-versa
  - la correspondance est temporaire
- Traduction de port (Port Address Translation) :
  - en plus d'une correspondance entre adresses, une correspondance sur les ports est réalisée
  - utilisable en statique et en dynamique

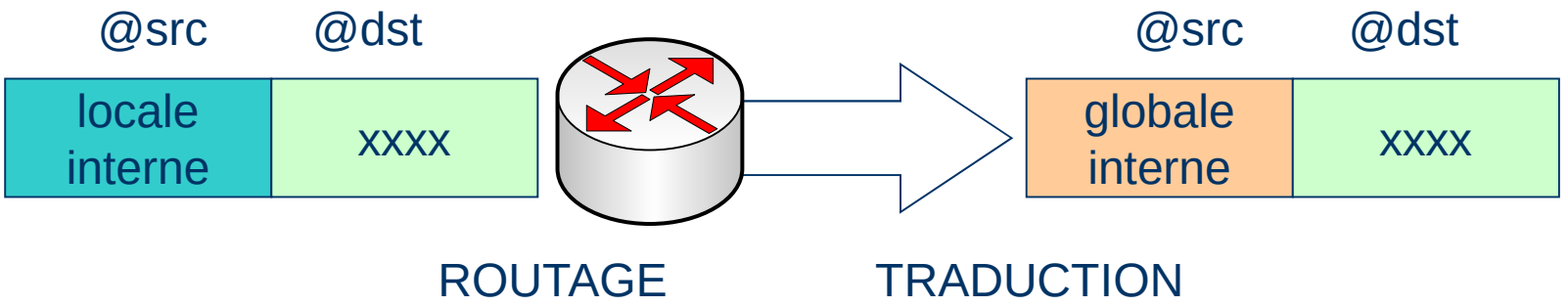
- Généralités
- Mise en œuvre classique de la traduction
  - Routage VS Traduction
  - Traduction statique
  - Traduction dynamique
  - Traduction de port

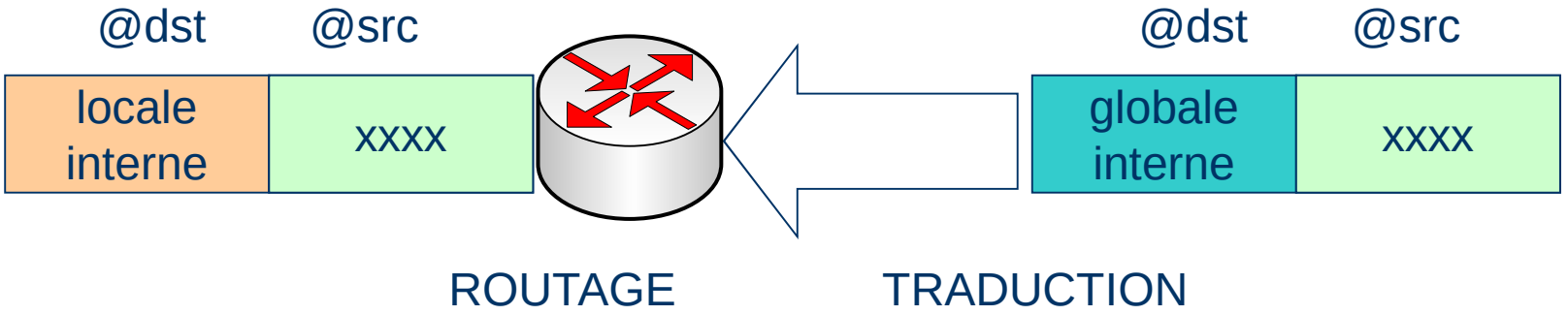
IP NAT INSIDE SOURCE

- Effet :
  - traduit l'adresse source du paquet partant de la zone interne et sortant sur la zone externe
    (adresse locale interne)  (adresse globale interne)
  - traduit l'adresse de destination du paquet revenant de la zone externe en entrant la zone interne

- ip nat inside source "le trafic à traduire " "ce par quoi il sera traduit"

Routage VS Traduction





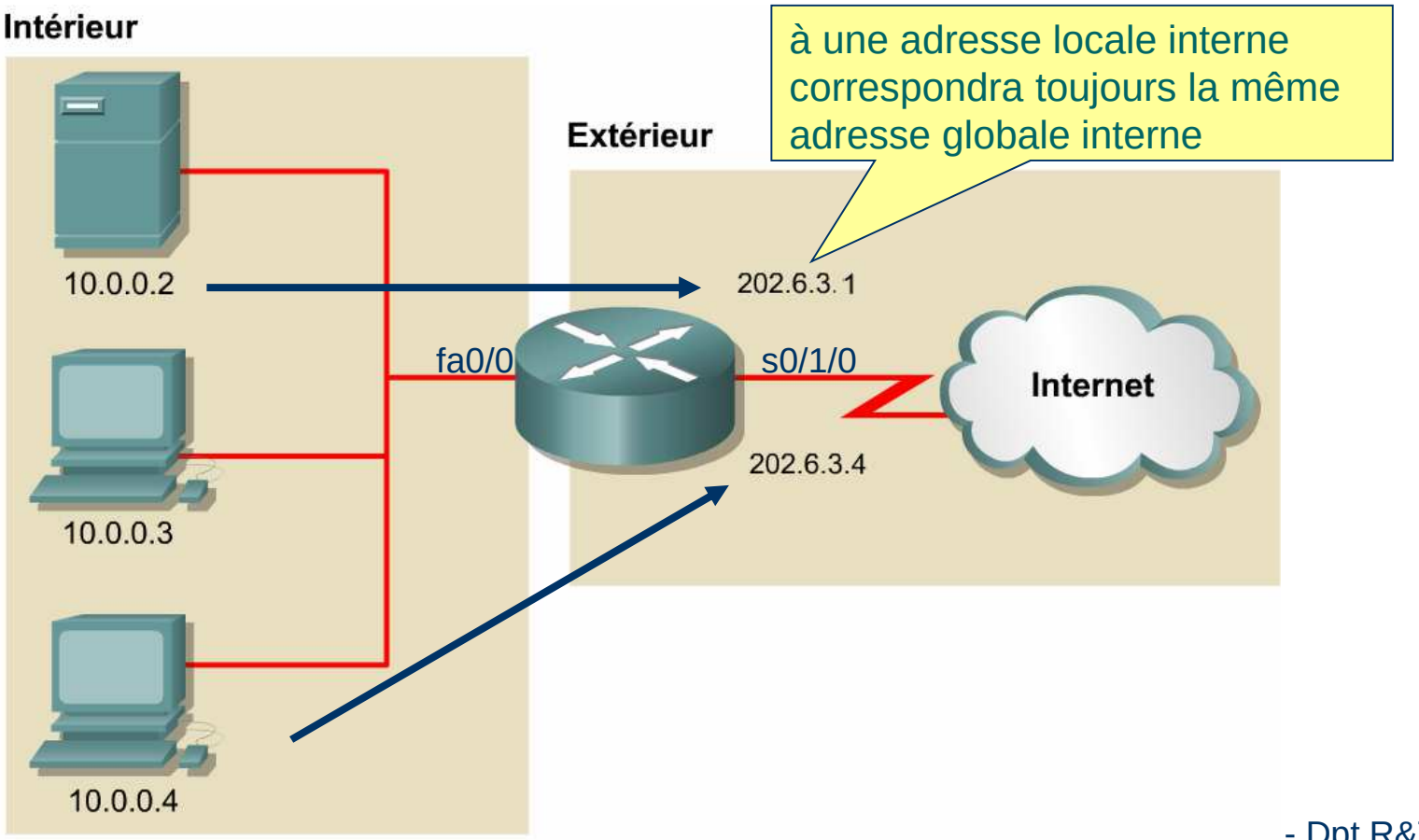
Principes de la configuration

1. Indiquer la/les zone(s) interne(s)
   commande *(config-if)ip nat inside*

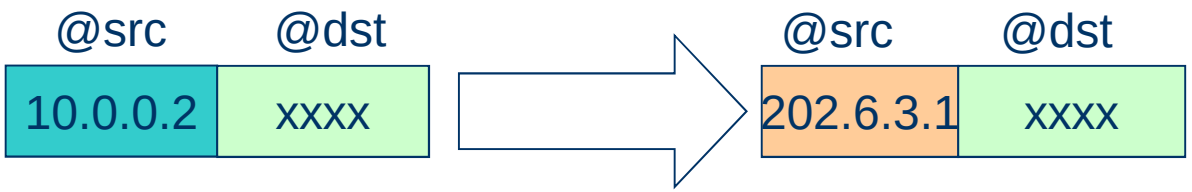
2. Indiquer la/les zone(s) externe(s)
   commande *(config-if)ip nat outside*

3. Spécifier le type de traduction
   commande *(config)#ip nat inside source*

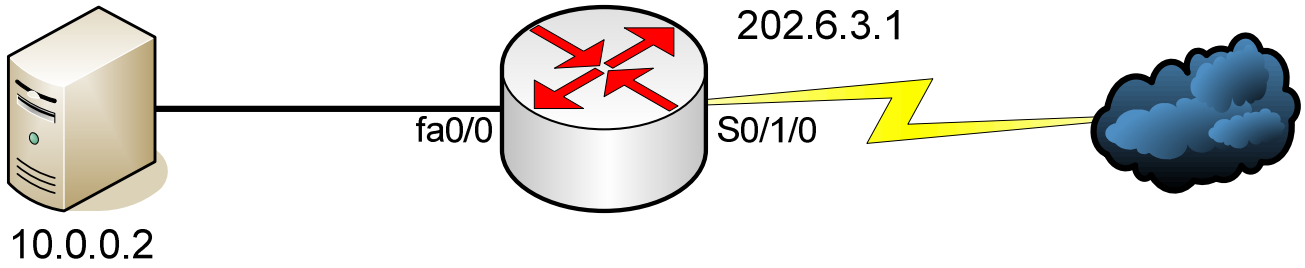
Traduction statique : principe



Traduction statique : configuration



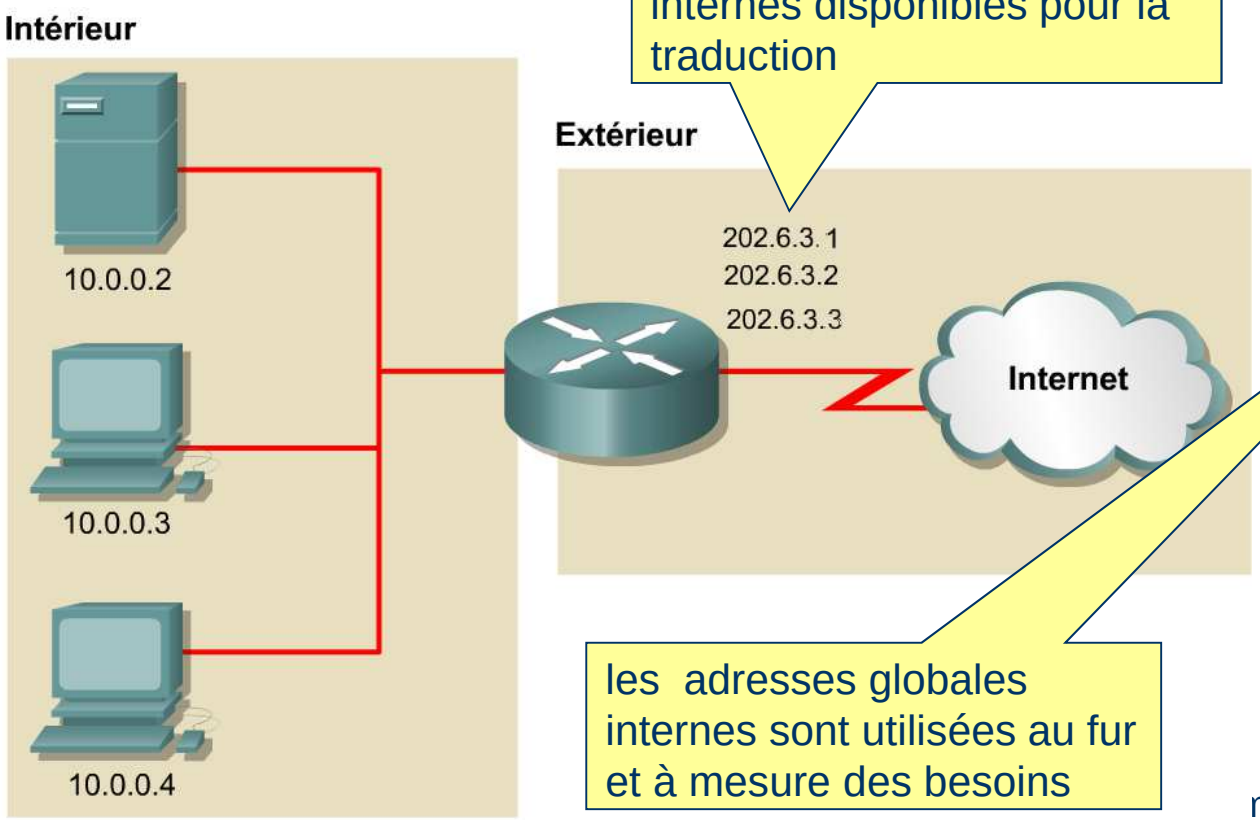
int fa0/0
ip nat inside



int s0/1/0
ip nat outside

ip nat inside source static 10.0.0.2 202.6.3.1

Traduction dynamique : principe



la plage d'adresses globales internes disponibles pour la traduction

locale interne	globale interne
10.0.0.2	202. 6.3.1
10.0.0.3	202. 6.3.2
10.0.0.4	202. 6.3.4

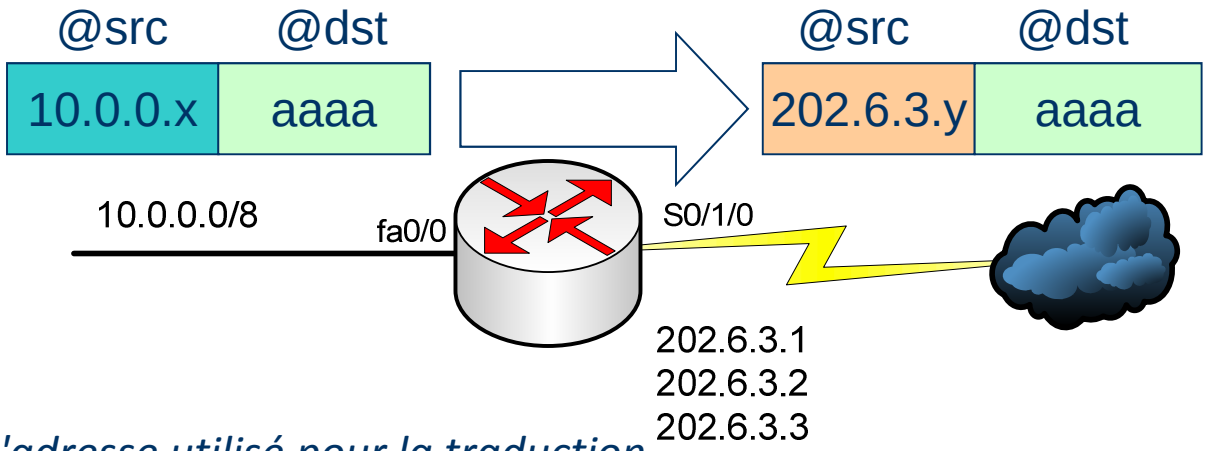
A l'instant t

locale interne	globale interne
10.0.0.3	202. 6.3.2
10.0.0.2	202. 6.3.3
10.0.0.4	202. 6.3.1

A l'instant t+1000

les adresses globales internes sont utilisées au fur et à mesure des besoins

Traduction dynamique : configuration



int fa0/0
ip nat inside

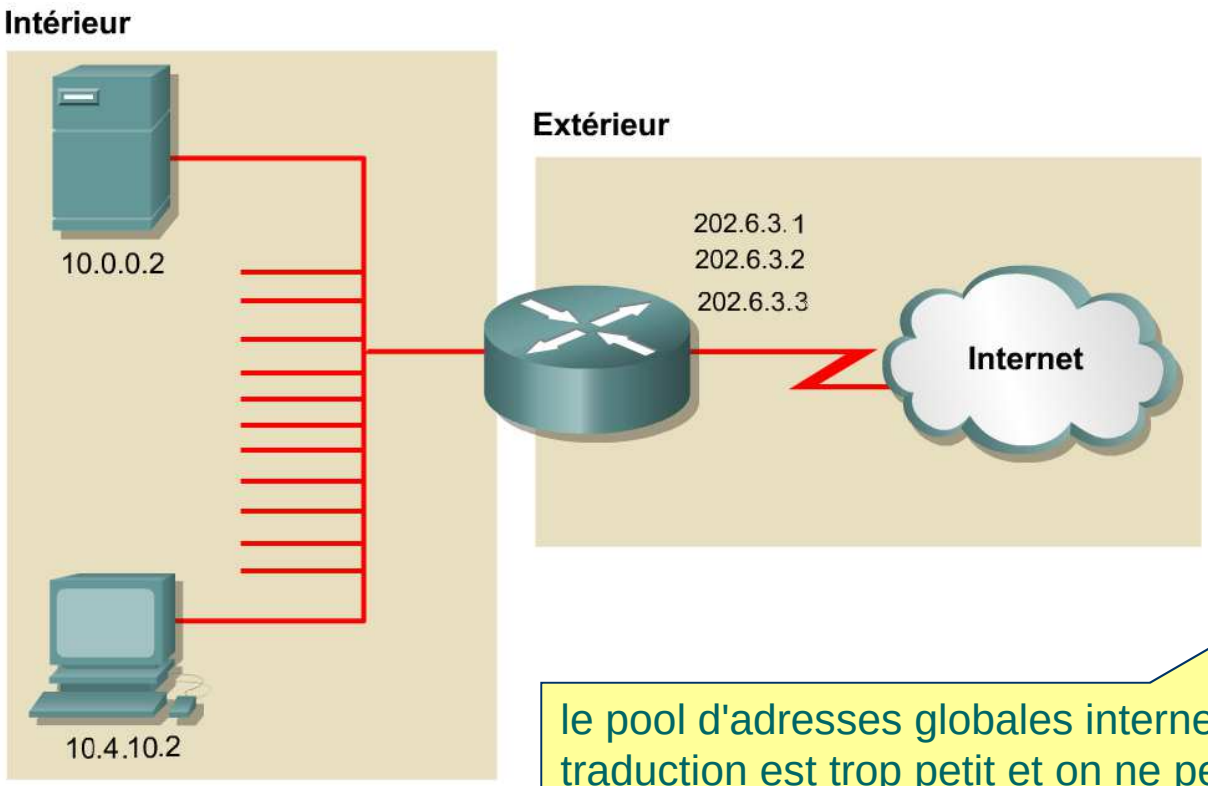
int s0/1/0
ip nat outside

! définition de la plage d'adresse utilisé pour la traduction
ip nat pool PLAGE_NAT 202.6.3.1 202.6.3.3 netmask 255.255.255.0

! définition d'une ACL capturant le trafic à traduire
access-list 1 permit 10.0.0.0 0.255.255.255

! mise en place de la traduction
ip nat inside source list 1 pool PLAGE_NAT

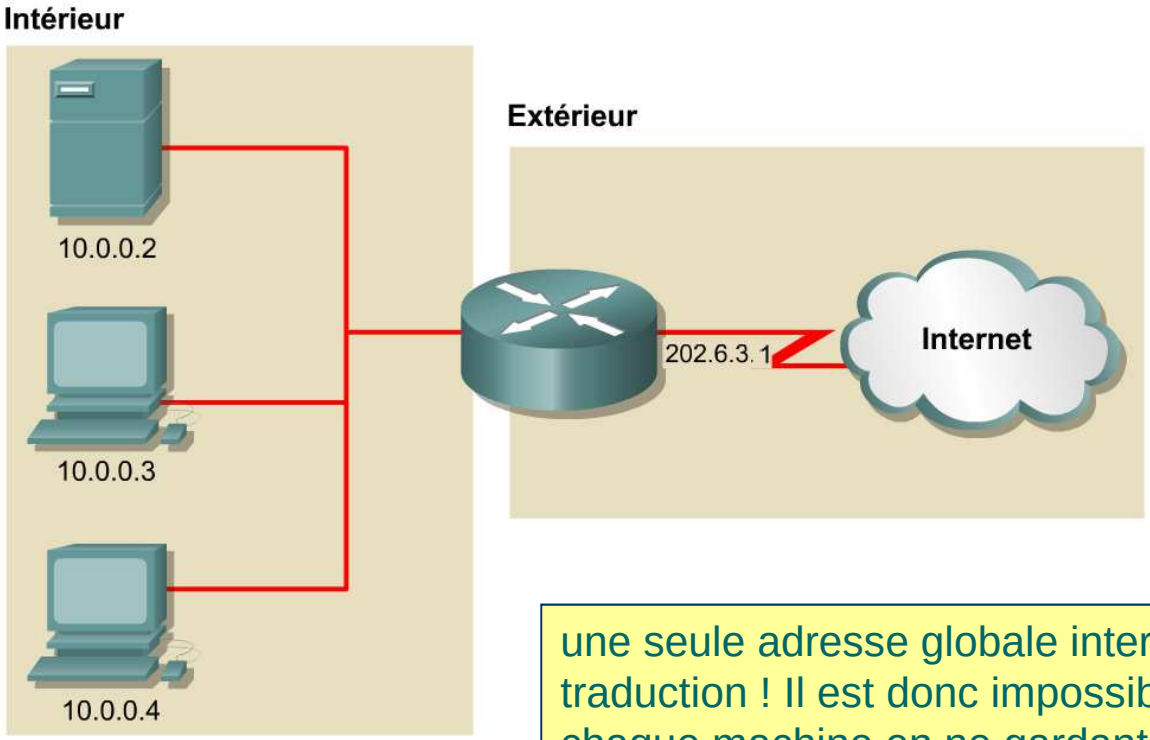
Problème (I)



locale interne	globale interne
10.0.0.3	202. 6.3.2
10.0.0.2	202. 6.3.3
10.0.0.4	202. 6.3.1
10.4.10.2	PB !

le pool d'adresses globales internes utilisé pour la traduction est trop petit et on ne peut satisfaire toutes les demandes simultanées

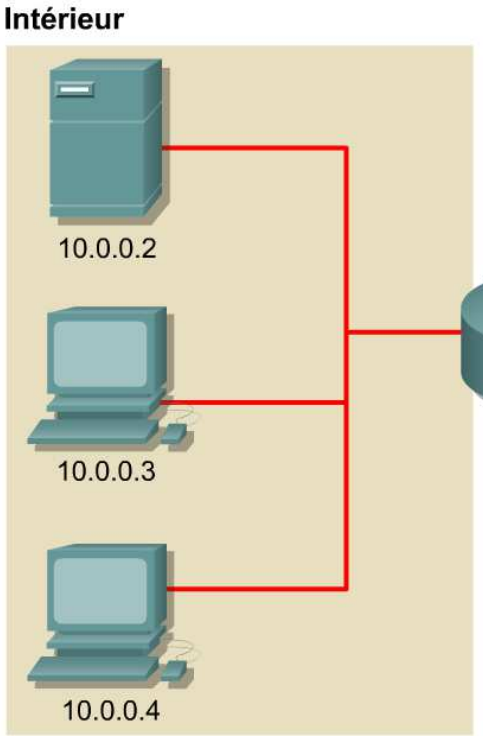
Problème (II)

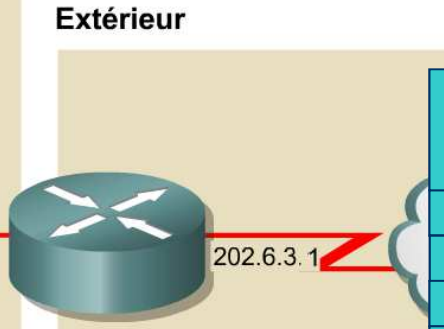


locale interne	globale interne
10.0.0.2	202. 6.3.1
10.0.0.3	202. 6.3.1
10.0.0.4	202. 6.3.1

une seule adresse globale interne est disponible pour la traduction ! Il est donc impossible de différencier les flux de chaque machine en ne gardant que la correspondance @locale interne / @globale interne

La traduction de port (PAT) : principe

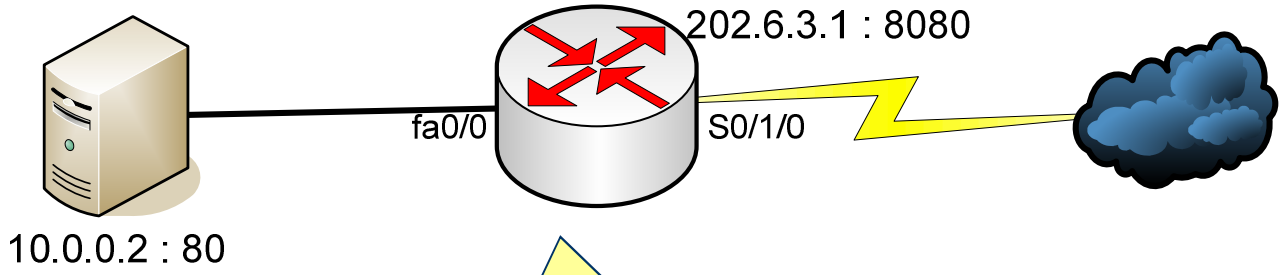




locale interne	globale interne
10.0.0.2 : 1050	202. 6.3.1 : 1050
10.0.0.2 : 1220	202. 6.3.1 : 1220
10.0.0.3 : 1310	202. 6.3.1 : 1310
10.0.0.4 : 1310	202. 6.3.1 : 1502

en plus de la correspondance @locale interne / @globale interne, on mémorise les ports associés aux adresses locale interne et globale interne

Traduction statique de port (redirection de port)



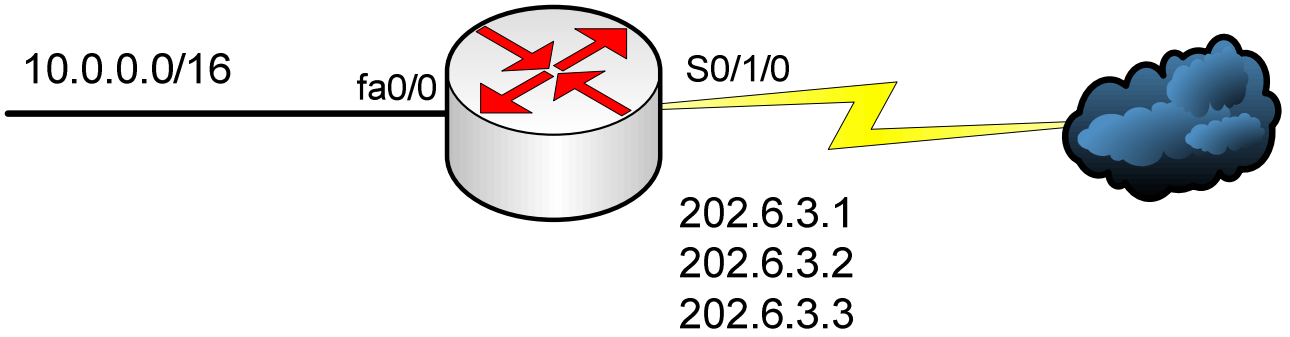
int fa0/0
ip nat inside

int s0/1/0
ip nat outside

à une adresse locale interne correspondra toujours la même adresse globale interne, mais en plus le port 80 a été redirigé sur le port 8080

*ip nat inside source static **tcp** 10.0.0.2 **80** 202.6.3.1 **8080***

Traduction dynamique avec surcharge de port sur un pool d'adresses



int fa0/0
ip nat inside

int s0/1/0
ip nat outside

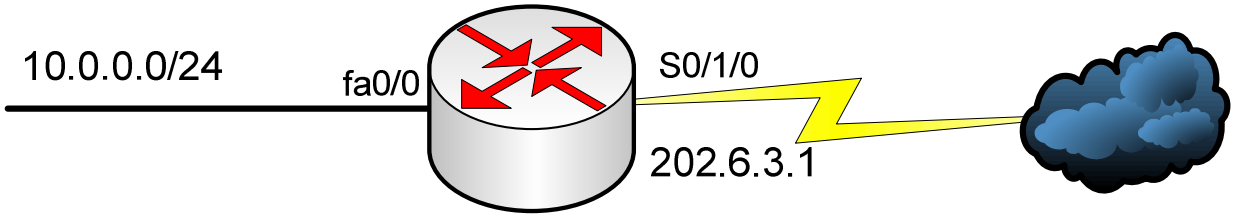
ip nat pool PLAGE 202.6.3.1 202.6.3.3 netmask 255.255.255.0

access-list 1 permit 10.0.0.0 0.0.255.255

ip nat inside source list 1 pool PLAGE ***overload***

le mot clef overload indique la surcharge de port

Traduction dynamique avec surcharge de port sur une adresse



int fa0/0
ip nat inside

int s0/1/0
ip address 202.6.3.1 255.255.255.0
ip nat outside

access-list 1 permit 10.0.0.0 0.0.0.255

ip nat inside source list 1 ***interface s0/1/0 overload***

l'adresse disponible pour la traduction est celle de l'interface de sortie

Quelques commandes utiles

- visualisation de la table des traductions
  show ip nat translations
- effacement de la table des traductions
  *clear ip nat translation **
- debug du processus de traduction
  debug ip nat