Architecture des Réseaux / M1 RID: NAT-PAT

Ali Benzerbadj

Ain Temouchent University Belhadj Bouchaïb (ATUBB)

16 avril 2021

- La très forte croissance et popularité d'Internet dans le début des années 90 ont menée très rapidement à la saturation des adresses IP version 4.
- le système d'adressage privé a été élaboré, de manière à ralentir l'inévitable, à savoir l'épuisement de toutes les adresses IPv4.
- Les adresses privées étant réservée à un usage interne, ces adresses ne peuvent pas être utilisées directement sur Internet. C'est pourquoi les routeurs de bordure des FAI sont configurés pour empêcher le routage de ces adresses.
- Les plages d'adresses privées définies par la RFC 1918 sont décrites dans le Tableau 2 :

Classe d'adresses	Plage d'adresses privées	Masque réseau	CIDR correspondant	Espace adressable
A	De 10.0.0.0 à 10.255.255.255	255.0.0.0	10.0.0.0/8	24 bits, soit 16 777 216 terminaux
B	De 172.16.0.0 à 172.31.255.255	255.240.0.0	172.16.0.0/12	20 bits, soit 1 048 576 terminaux
C	De 192.168.0.0 à 192.168.255.255	255.255.0.0	192.168.0.0/16	16 bits, soit 65 536 terminaux

Table 1 – Plages d'adresses privées définies par la RFC 1918.

Translation d'adresses

Remarque

- L'ensemble des adresses privées (Tableau 2) ne sont pas acheminées dans ce qu'on appelle le backbone internet.
- Les routeurs internet sont tous configurés pour éliminer toutes les adresses privées, c'est à dire qu'elles ne sont pas routables sur internet.

Translation d'adresses

La translation d'adresse est un processus générique permettant la substitution d'une adresse par une autre, et permet ainsi de masquer les adresses privées des réseaux locaux derrière une adresse publique. Ce processus existe sous deux variantes :

- NAT (Network Address Translation)
  - Statique (particulièrement utile lorsqu'un périphérique doit être accessible depuis l'extérieur, par ex. un serveur Web).
  - Dynamique
- PAT (Port Address Translation)

Le périphérique réseau qui s'occuppe du NAT (Network Address Translation) est le routeur.

Translation d'adresses

- L'adressage privé peut être utilisé librement par n'importe quel administrateur ou utilisateur au sein de son réseau local.
- Au contraire, l'adressage public est soumis à des restrictions de déclaration et d'enregistrement de l'adresse IP auprès d'un organisme spécialisé, l'IANA (Internet Assigned Numbers Authority), ce que les FAI effectuent globalement en acquérant une plage d'adresses IP pour leurs abonnés.
- FAI (fournisseur d'accès Internet), en anglais ISP (Internet Service Provider) : opérateur qui commercialise des accès à Internet.

Classe d'adresses	Plage d'adresses public
A	1.0.0.0 - 9.255.255.255 11.0.0.0 - 126-255.255.255
B	128.0.0.0 - 172.15.255.255 172.32.0.0 - 191-255.255.255
C	192.0.0.0- 192.167.255.255 à 192.169.0.0 - 223-255.255.255

Table 2 – Plages d'adresses public.

Translation d'adresses Réseaux

Reamarques

- La stabilité d'internet dépend du fait que chaque adresse publique soit unique.
- L'organisme qui veuille sur cette stabilité est InterNIC (Internet Network Information Centre). Aujourd'hui ce nom a changé pour laisser place à l'IANA (Internet Assigned Numbers Authority).
- Pour obtenir une IP publique ou un bloc d'adresses IP publiques, il faut se rapprocher de son Fournisseur d'Accès à Internet (FAI), en Anglais ISP (Internet Service Provider), ou il faut prendre contact avec le LIR (Local Internet Registry) car c'est eux qui peuvent obtenir des pools d'IP du registre internet de sa région (RIR, Regional Internet Registry)

Translation d'adresses

- Pour permettre à un terminal disposant d'une adresse IP privée de communiquer avec le réseau public, le processus de NAT fait intervenir une entité tierce entre un terminal, ayant une adresse IP privée, et tout autre terminal ayant une adresse IP publique.
- Ce mécanisme consiste à insérer un boîtier entre le réseau Internet et le réseau local afin d'effectuer la translation de l'adresse IP privée en une adresse IP publique.
- Aujourd'hui, la plupart des boîtiers, ou InternetBox, des FAI proposent à leurs abonnés cette fonctionnalité.
- Toutes les machines qui se connectent reçoivent par le biais du service DHCP (Dynamic Host Configuration Protocol) une adresse IP privée, que le boîtier se charge de translater en une adresse IP publique.

Translation d'adresses

- La Figure 7 illustre un exemple dans lequel une passerelle NAT réalise une translation d'adresses pour quatre terminaux.
- Cette passerelle possède deux interfaces réseau. La première est caractérisée par une adresse IP publique (132.227.165.221). Connectée au réseau Internet, elle est reconnue et adressable normalement dans le réseau.
- La seconde interface est caractérisée par une adresse IP non publique (10.0.0.254). Connectée au réseau local, elle ne peut communiquer qu'avec les terminaux qui possèdent une adresse IP non publique de la même classe.

Translation d'adresses

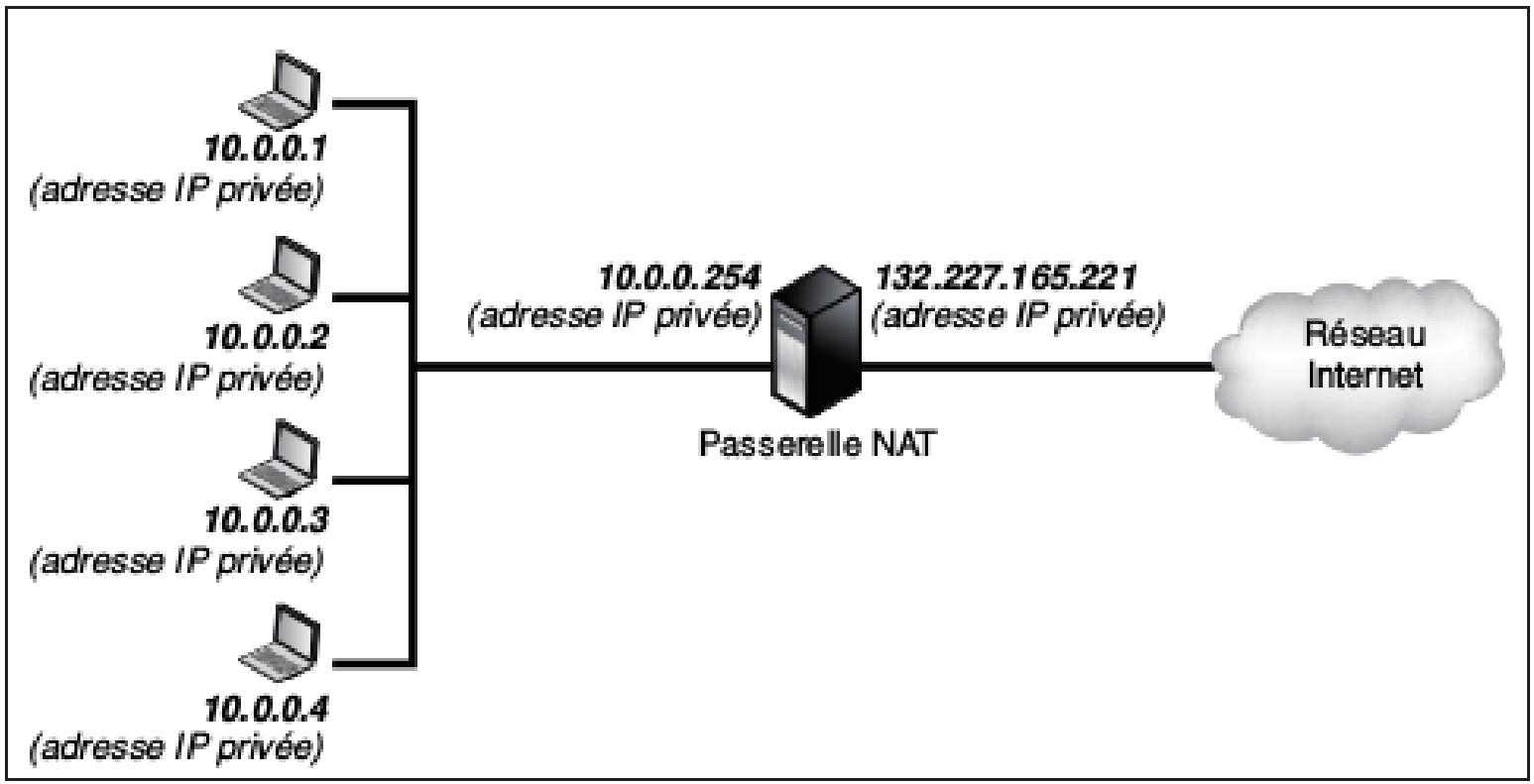


Figure 1 – Translation d'adresses

Translation d'adresses

Lorsqu'un terminal ayant une adresse IP privée tente de se connecter au réseau Internet, il envoie ses paquets vers la passerelle NAT. Celle-ci remplace l'adresse IP privée d'origine par sa propre adresse IP publique (132.227.165.221). On appelle cette opération une translation d'adresse. De cette manière, les terminaux avec une adresse IP privée sont reconnus et adressables dans le réseau Internet par une adresse IP publique.

Translation d'adresses

La translation d'adresse est bien sûr réalisée dans les deux sens d'une communication, afin de permettre l'émission de requêtes aussi bien que la réception des réponses correspondantes. Pour cela, le boîtier NAT maintient une table de correspondance des paquets de manière à savoir à qui distribuer les paquets reçus.

Translation d'adresses

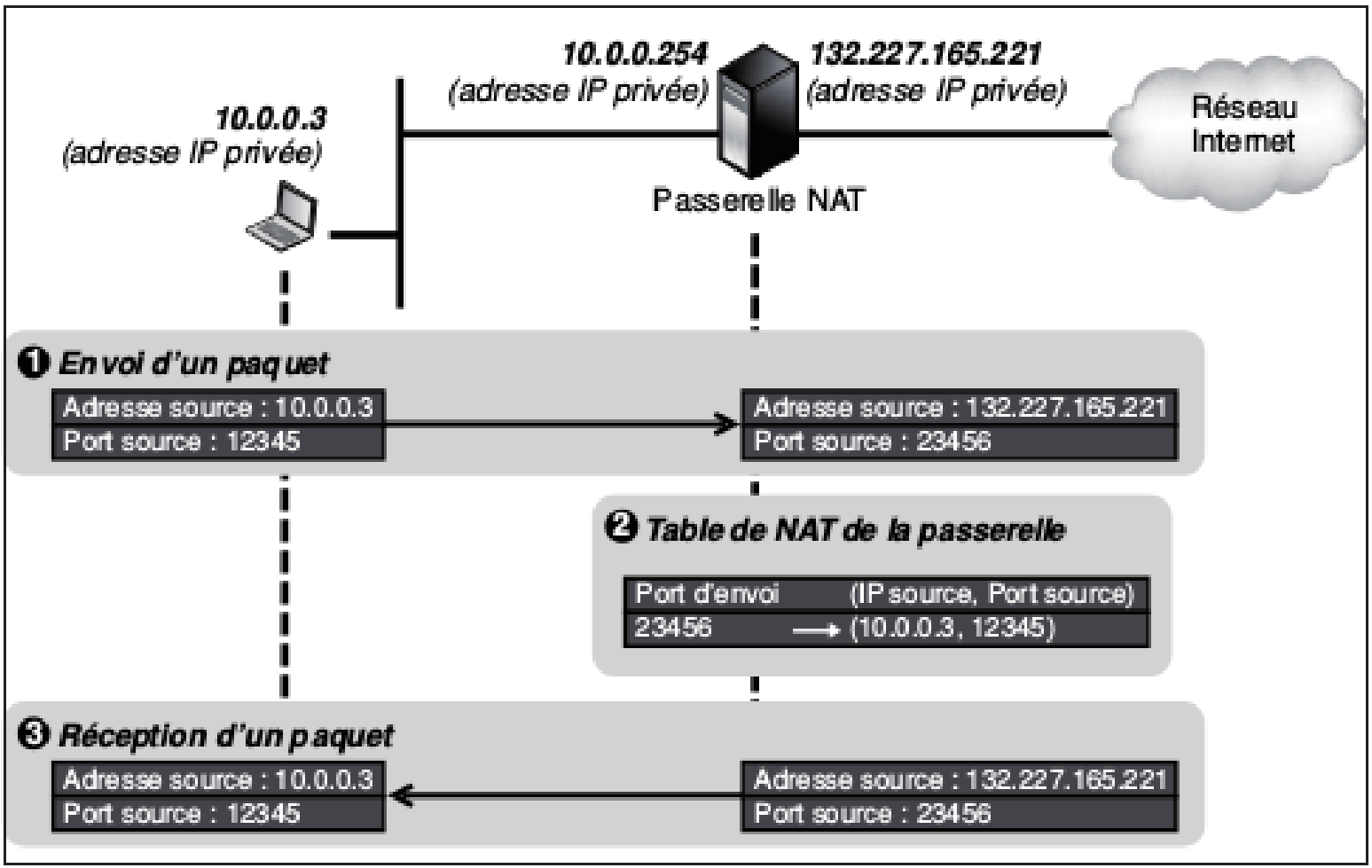


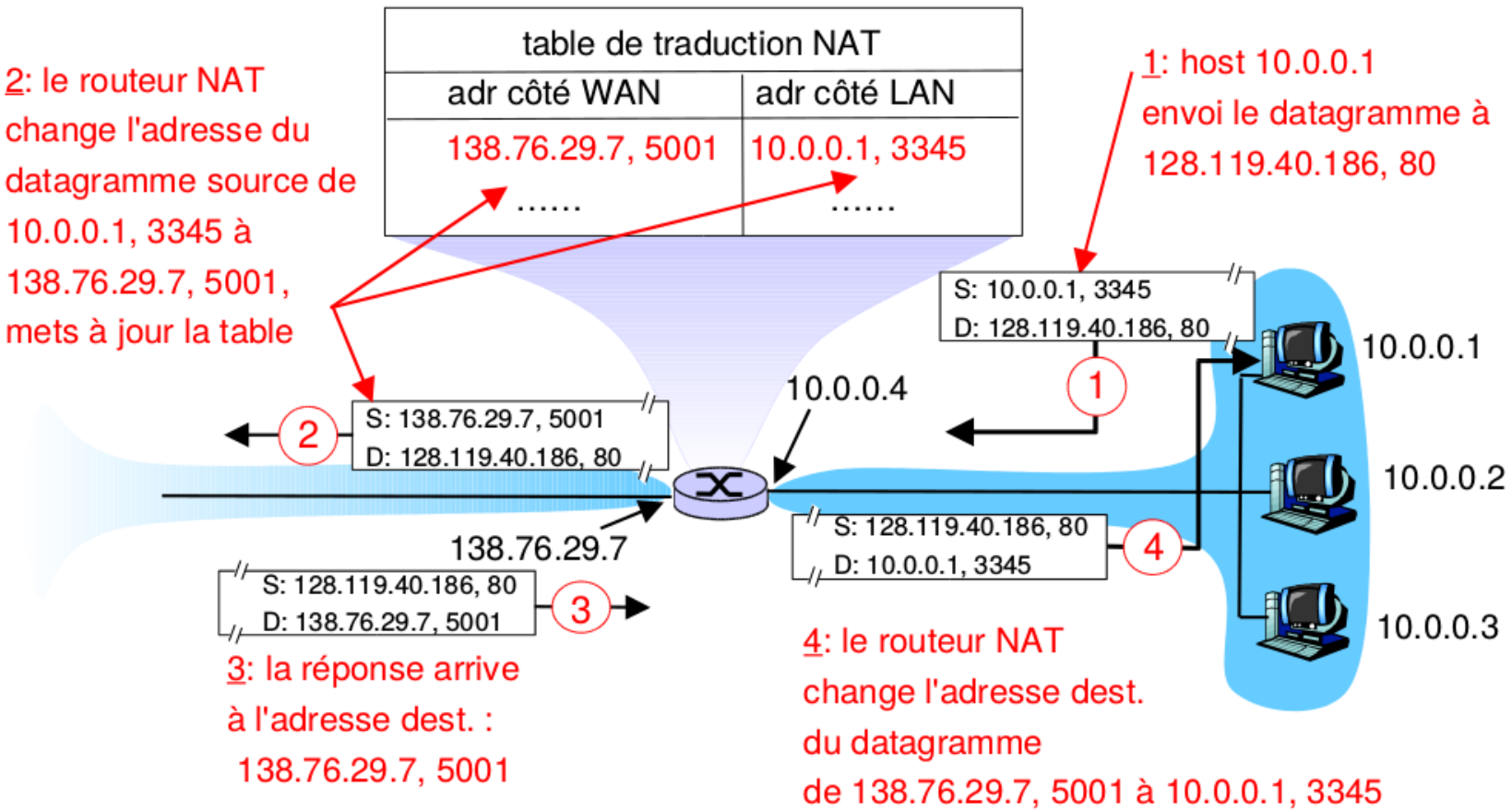
Figure 2 – Modification des paquets lors du NAT

Translation d'adresses

Par exemple, si un émetteur dont l'adresse IP est 10.0.0.3 envoie vers la passerelle NAT un paquet à partir de son port 12345, la passerelle NAT modifie le paquet en remplaçant l'adresse IP source par la sienne et le port source par un port quelconque qu'elle n'utilise pas, par exemple 23456. Elle note cette correspondance dans sa table de NAT. De cette manière, lorsqu'elle recevra un paquet à destination du port 23456, elle cherchera cette affectation de port dans sa table et retrouvera la source initiale.

Translation d'adresses

NAT : Network Address Translation



Translation d'adresses

- Le NAT a été conçu pour économiser des adresses IP en permettant la translation d'adresses IP privées (RFC 1918), internes a une entité (une entreprise, une école etc.) en une ou plusieurs adresses IP publiques routable sur Internet.
- Remarque : l'adresse IP utilisée pour la translation n'est pas forcement une adresse IP public et peut être à nouveau une adresse IP privée qui, à son tour, pourra être translatée.

Translation d'adresses

- Cette translation d'adresse est effectuée principalement sur les routeurs de bordure d'une entreprise connectée à Internet.
- Le réseau utilisant les adresses IP privées est ainsi appelé le réseau interne (inside), tandis que la partie du réseau utilisant des adresses IP publiques (Internet) est appelé le réseau externe (outside).
- Quand un utilisateur du réseau interne (inside) souhaite communiquer avec un hôte du réseau externe (outside), le routeur reçoit le paquet avec l'adresse IP privée et réécrit le paquet en changeant l'adresse IP source avec l'adresse IP public du routeur (c'est l'opération de translation).

Translation d'adresses

- Le routeur consulte ensuite sa table de routage pour acheminer le paquet jusqu'à la bonne destination.
- Le destinataire recevra le paquet avec comme source l'adresse IP public du routeur et non l'adresse IP privée de l'hôte qui envoie le paquet dans le réseau interne.

Translation d'adresses

- Le NAT statique translate une adresse IP privée avec toujours la même adresse IP public. S'il y a 4 utilisateurs nécessitant une translation d'adresse, il faudra donc utiliser 4 adresses IP publiques.
- Le NAT dynamique translate une adresse privée avec une adresse IP publique appartenant à un pool d'adresses. L'adresse IP publique utilisée pour la translation n'est donc pas toujours la même. S'il n'y a pas assez d'adresses IP publiques disponibles, les utilisateurs devront attendre qu'une adresse se libère pour pouvoir être translaté.

Translation d'adresses

- Le PAT (Port Address Translation) ou Overloading permet d'attribuer une seule adresse IP publique pour la translation de plusieurs adresses IP privées. Chaque utilisateur est différencié grâce à un numéro de port unique qui lui est attribué lorsqu'il souhaite communiquer.
- Etant donné qu'il existe 65536 ports différents, un routeur pourrait translater jusqu'à 65536 adresses IP privées différentes. Cependant en réalité, un équipement ne peut gérer en moyenne que la translation d'environ 4000 ports par adresse IP publique.

NAT/PAT

Defénitions

Cisco définit 4 types d'adresses pour le NAT :

- Inside local address : Adresse IP attribuée à un hôte dans le LAN.
- Inside global address : Adresse(s) IP attribuée(s) par le FAI reconnue(s) par l'Internet pour représenter le LAN.
- Outside local address : Adresse IP d'un hôte du réseau externe telle qu'elle est connue par les utilisateurs du réseau interne. La plupart du temps, celle-ci est identique à l' "outside global address".
- Outside global address : Adresse IP attribuée à un hôte dans le réseau externe.

Network Address Translation / Static

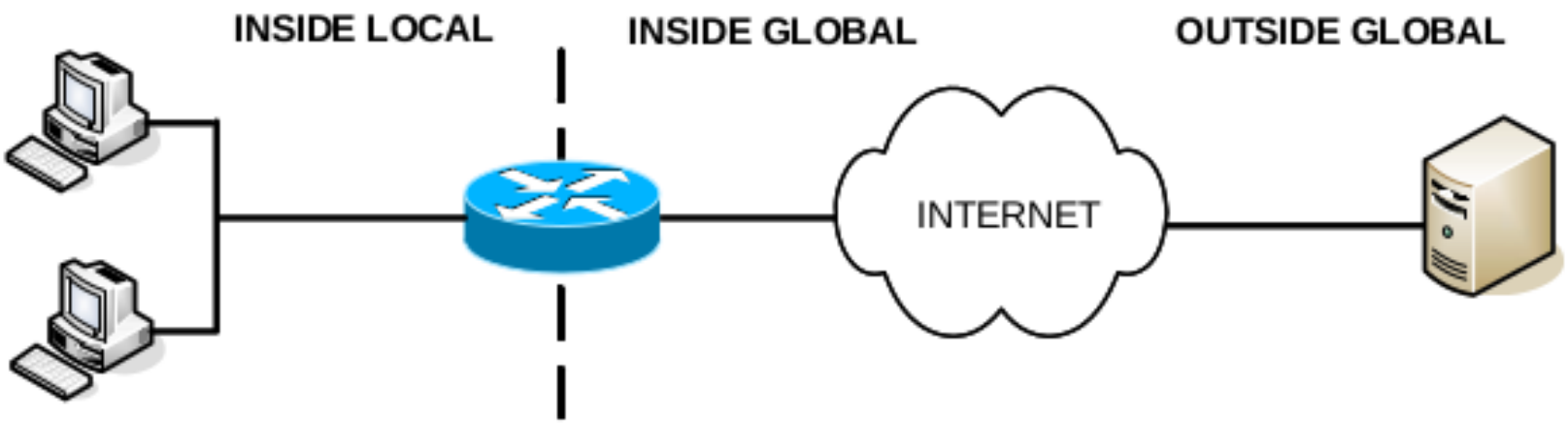


Figure 4 – Cisco Definitions (SupInfo)

Network Address Translation / Static

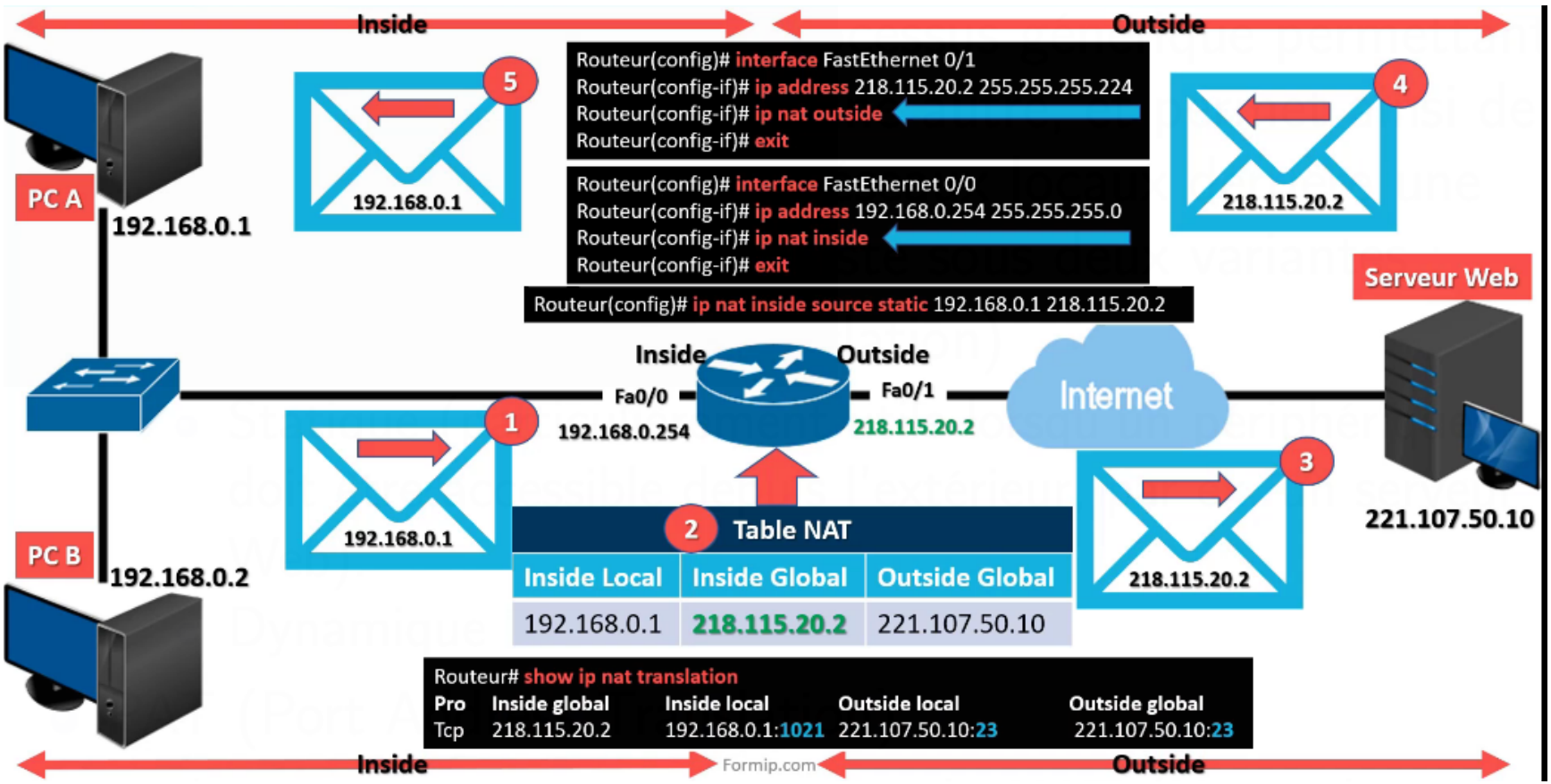


Figure 5 – Static NAT (FormIP)

Network Address Translation / Dynamic

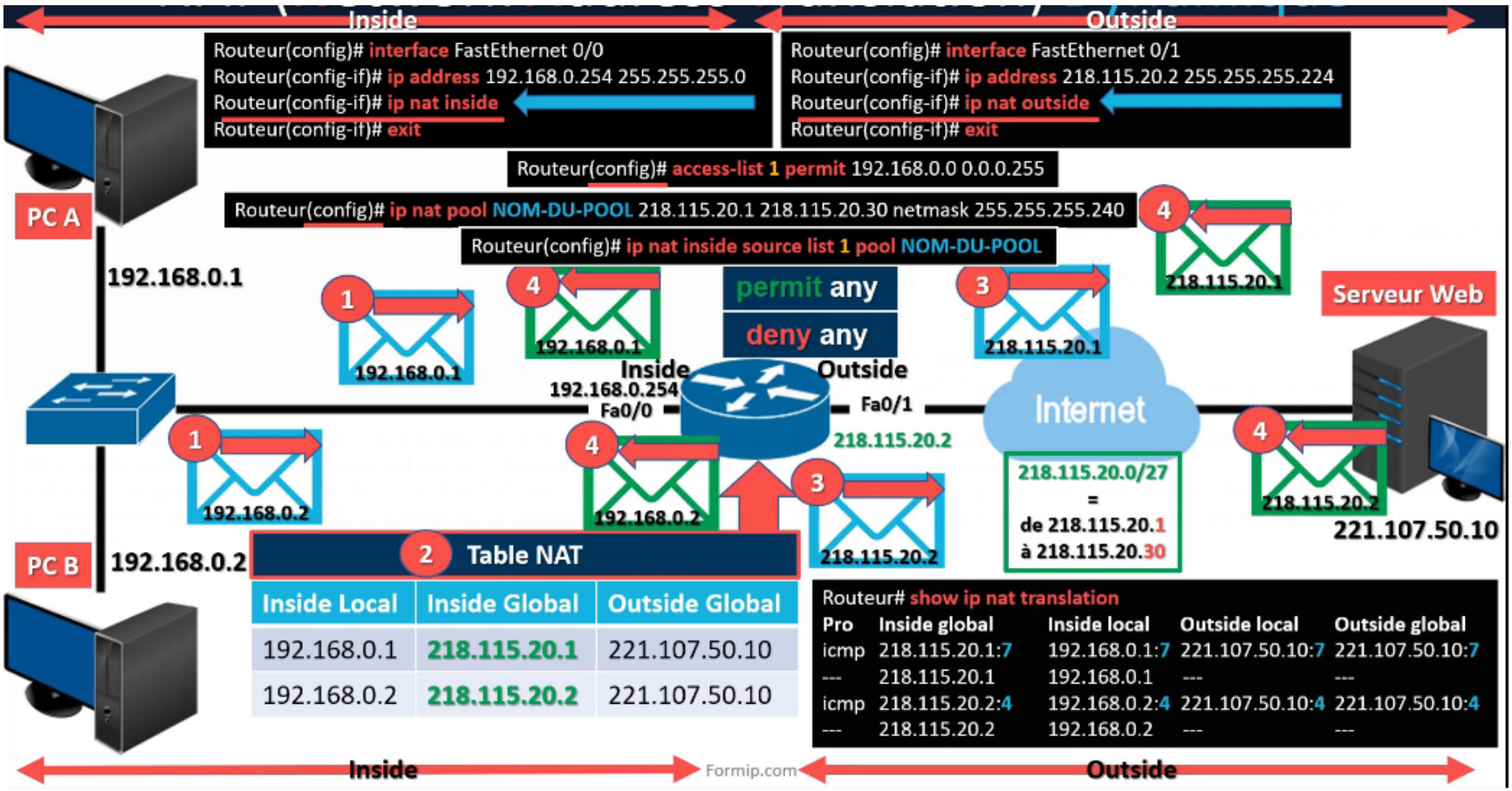


Figure 6 – Dynamic NAT (FormIP)

Port Address Translation (Overload)

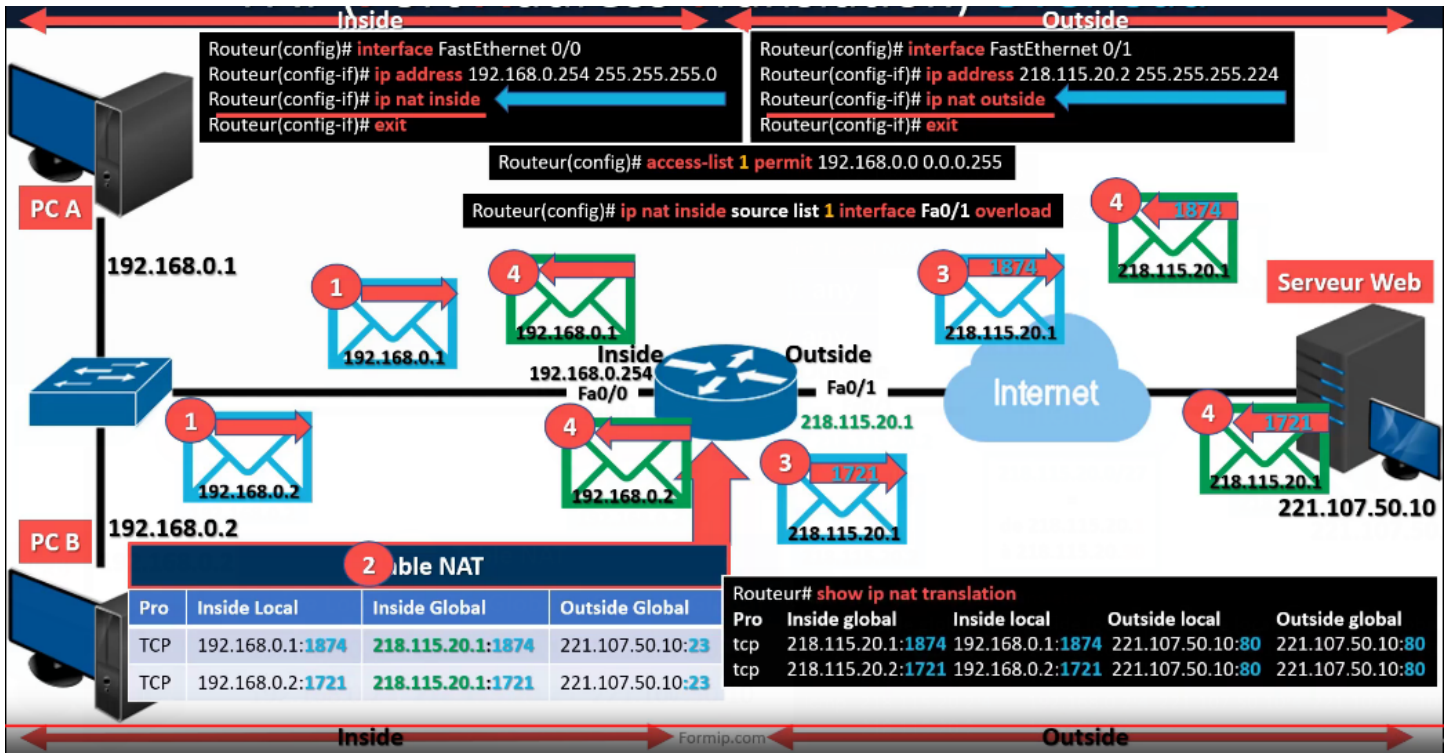


Figure 7 – Port Address Translation (Overload) (FormIP)