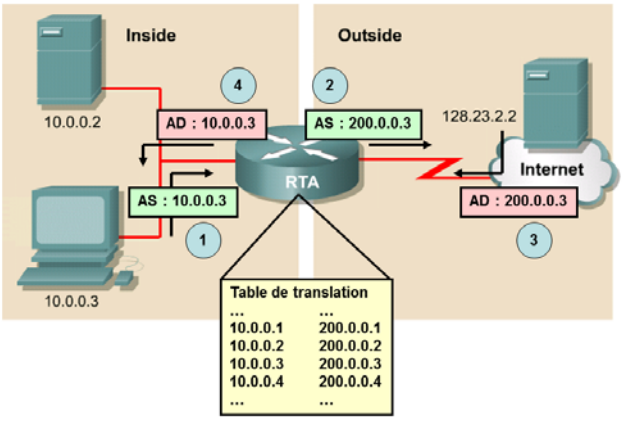
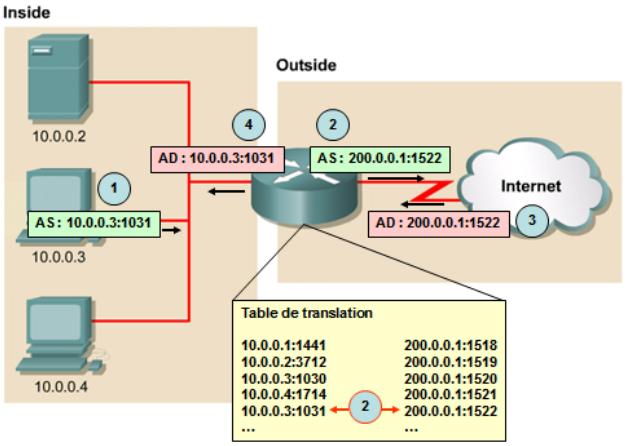




Objectifs du COURS :

Ce cours traitera essentiellement les points suivants :

- principe de la NAT :
  - statique
  - dynamique
- principe de la PAT (variante de la NAT) :
  - le port Forwarding
  - le port Trigerring
- exemples de configuration de la NAT / PAT pour :
  - freebox
  - routeur GNU/Linux

Toutes les machines connectées (clients, serveurs, imprimantes réseau, ...) disposent d'une adresse IP permettant de l'identifier sur le réseau. Il existe deux sortes d'adresse : les **privées** et les **publiques.**

Une adresse privée est seulement valable sur un réseau privé et ne peut donc pas être utilisée pour communiquer sur un réseau public comme Internet. Internet n'accepte de véhiculer que des adresses publiques. Le principal intérêt de l'utilisation d'adresses IP privées est de disposer d'un grand nombre d'adresses pour bâtir des réseaux privées (entreprise, lycée, domicile...) et ainsi de palier au cruel manque d'adresse IP publiques du réseau IPv4 (2^{32} adresses possibles soit 4 294 967 296).

La version 6 (IPv6) permettra de résoudre en partie ce problème en proposant 2^{128} adresses IP possibles.

En attendant le déploiement d'IPv6, il est indispensable d'utiliser les technologies de la NAT et de la PAT pour permettre aux machines disposant d'adresses privées de pouvoir communiquer sur internet.

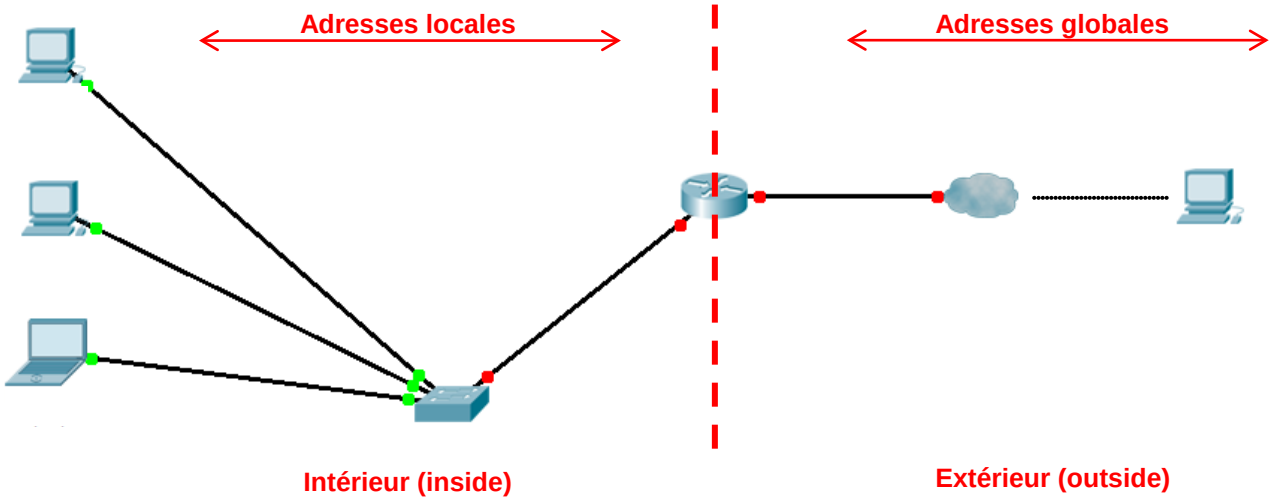
PRINCIPE DE LA NAT (NETWORK ADRESS TRANSLATION)

Les traductions NAT peuvent avoir de nombreuses utilisations et peuvent indifféremment être attribuées de façon **statique** ou **dynamique**.

Remarques :

Les termes ci-dessous ont été définis par « CISCO » :

Adresse Locale Interne (**ALI**) = adresse IP attribuée à un hôte du réseau interne, il s'agit d'une adresse privée.
Adresse Locale Externe (**ALE**) = adresse IP attribuée par le FAI qui représente une ou plusieurs adresses IP locales internes pour le monde extérieur.
Adresse Globale Externe (**AGE**) = adresse IP d'un hôte externe telle que la connaisse les hôtes du réseau externe.
Adresse Globale Interne (**AGI**) = adresse IP attribuée à un hôte du réseau externe, c'est le propriétaire de l'hôte qui attribue cette adresse.



Pour les messages sortants : (inside → outside)

Les adresses locales sont traduites en adresses globales.

Pour les messages entrants : (inside ← outside)

Les adresses globales sont traduites en adresses locales.

Sur un routeur « CISCO » on définit les adresses publiques à utiliser pour la traduction dans un pool (groupe).

ip nat pool adrpub 82.3.4.6 82.3.4.10 netmask 255.0.0.0 définit un pool de cinq adresses publiques nommé adrpub.

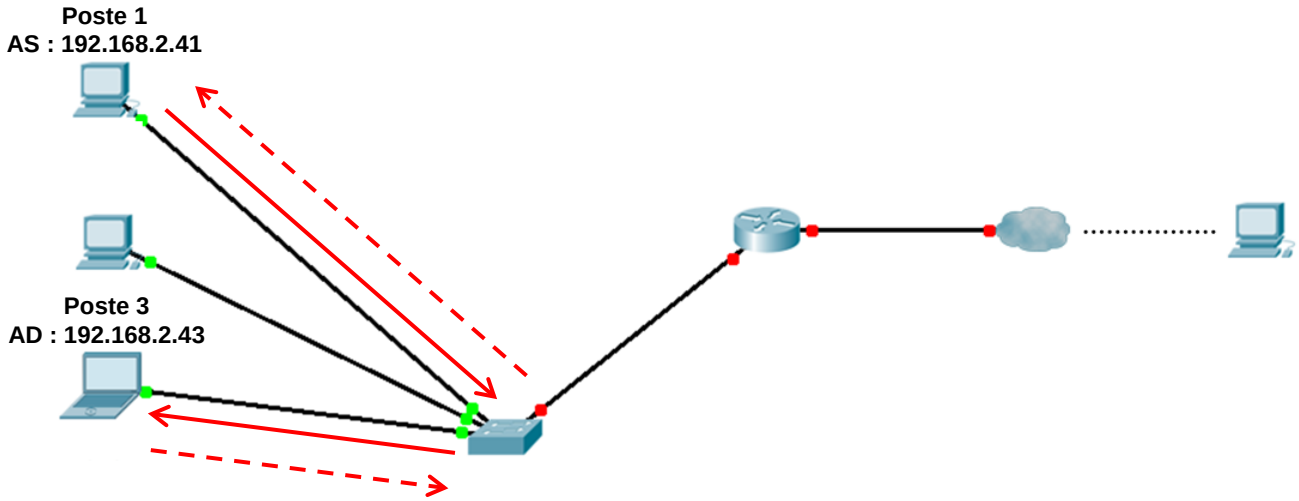
Remarque :

Les machines du LAN n'ont pas connaissance des adresses publiques du routeur (configuration NAT) et ne les utilisent pas.

Rappel : les adresses privées (RFC 1918)

10.0.0.0/8	soit **16 777 216 hôtes**	**(de 10.0.0.0 à 10.255.255.255)**
172.16.0.0/12	soit **1 048 576 hôtes**	**(de 172.16.0.0 à 172.31.255.255)**
192.168.0.0/16	soit **65 536 hôtes**	**(de 192.168.0.0 à 192.168.255.255)**

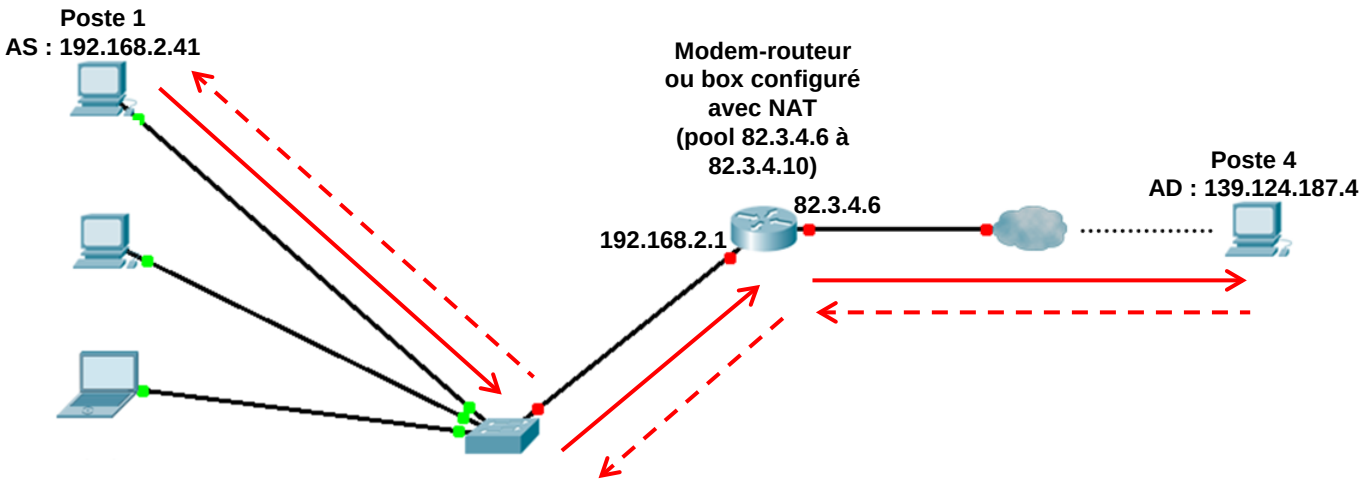
LA NAT ET LA DISCUSSION EN INTERNE



Le poste 1 veut discuter avec le poste 3 :

Le dialogue étant interne la NAT n'est pas concernée par ce trafic.
Les datagrammes contiennent les adresses du poste 1 et du poste 3.

LA NAT ET LA DISCUSSION AVEC L'EXTÉRIEUR



Le poste 1 veut discuter avec le poste 4 :

Le poste 1 envoie le datagramme qui parvient au routeur.
La NAT remplace l'adresse source privée par une adresse publique disponible (82.3.4.6), enregistre une association (192.168.2.41, 82.3.4.6) dans sa table de traductions, et transmet son datagramme vers le poste 4.
Le poste 4 répond à l'adresse source du datagramme (82.3.4.6).
Le routeur reçoit le datagramme, consulte sa table de traductions, trouve l'association (192.168.2.41, 82.3.4.6), remplace la destination par 192.168.2.41 et retransmet le datagramme au poste 1.

Remarques :

Il est possible de configurer le routeur suivant les traductions à opérer :

Traduction inside : traduire les adresses internes
Dans le cas normal c'est la seule traduction nécessaire.

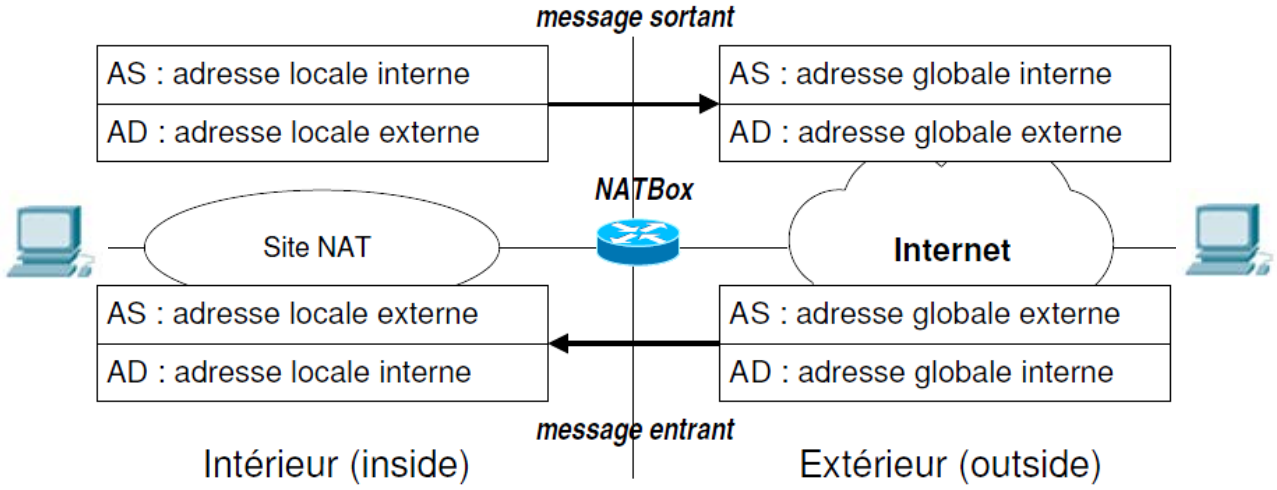
Traduction outside : traduire les adresses externes
Cette traduction est utile en cas « d'overlapping » (chevauchement d'adresses).

Ou les deux à la fois (réalisé en pratique pour traiter l'overlapping).

Exemple : une entreprise a eu la mauvaise idée de ne pas utiliser les adresses privées pour son site NAT. Les adresses qu'elle a choisies pour ses ALI sont déjà utilisées dans le WAN (AGE).

Sans traduction des adresses externes, il y aurait ambiguïté car une même adresse désignerait à la fois une machine interne et une machine externe.

SCHÉMA GÉNÉRAL DE LA TRADUCTION NAT



La NATBox traduit les AS et les AD qui franchissent la frontière « inside/outside ».

NAT STATIQUE

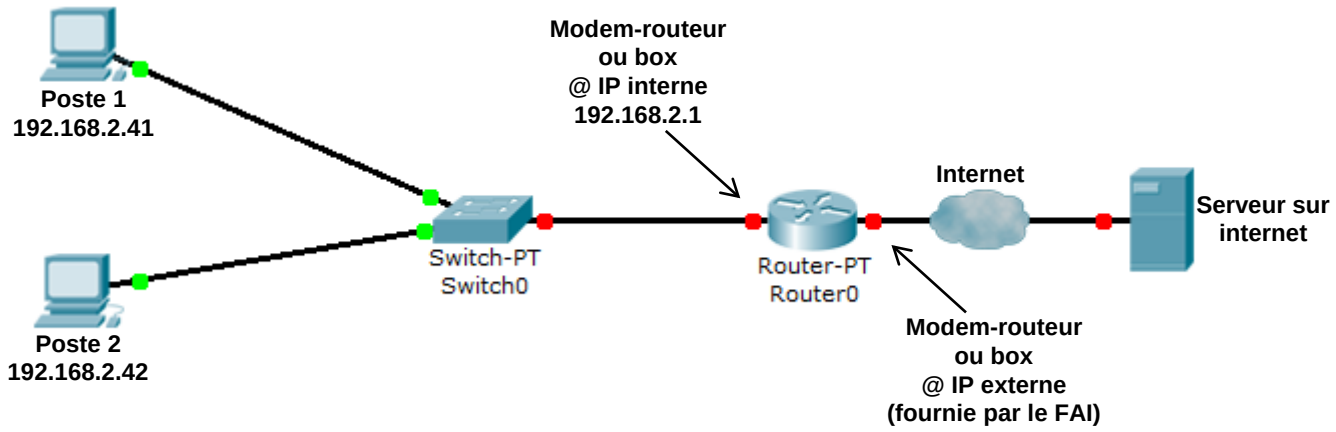
La NAT statique consiste à associer une adresse IP privée fixe et permanente à une adresse IP publique fixe et permanente. Ne pouvant se connecter sur internet avec une adresse IP privée, le routeur doit remplacer l'adresse IP source par l'adresse IP de l'interface publique donnée par le FAI.

La NAT statique permet à un poste d'accéder à Internet.
Elle permet aussi à une machine possédant une adresse IP privée d'être vue sur Internet.
Ceci est intéressant si l'on souhaite héberger des services vus de l'extérieur.
En revanche, il est nécessaire d'avoir autant d'adresses publiques que d'adresses privées.

La pénurie d'adresse publique (IPv4) ne permet pas d'utiliser cette solution.

NAT DYNAMIQUE

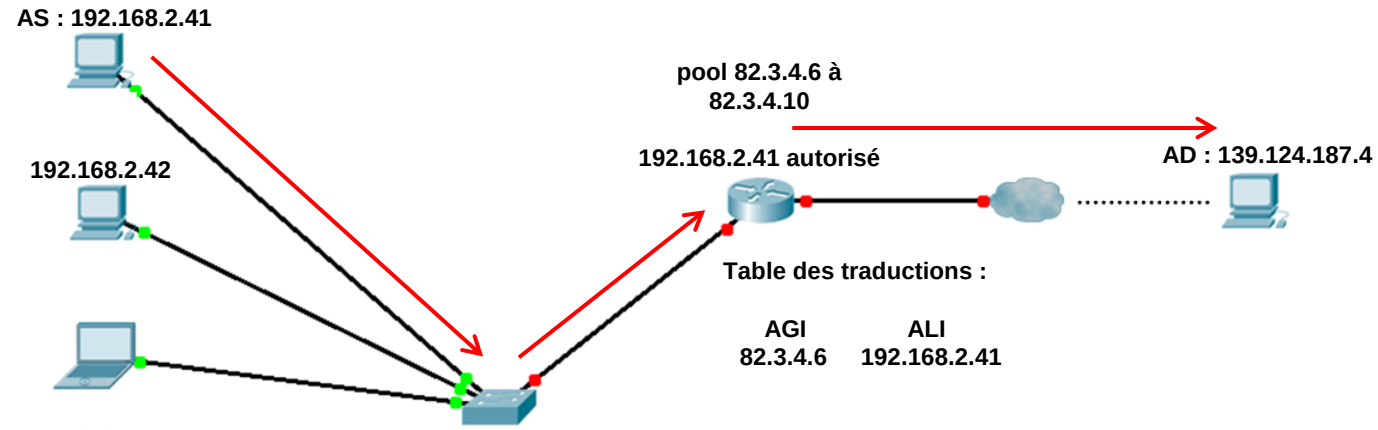
La NAT dynamique consiste à associer une adresse IP publique à plusieurs adresses IP privées.
La NAT dynamique est aussi appelée « **IP masquerading** », on dit que l'on masque les adresses privées.

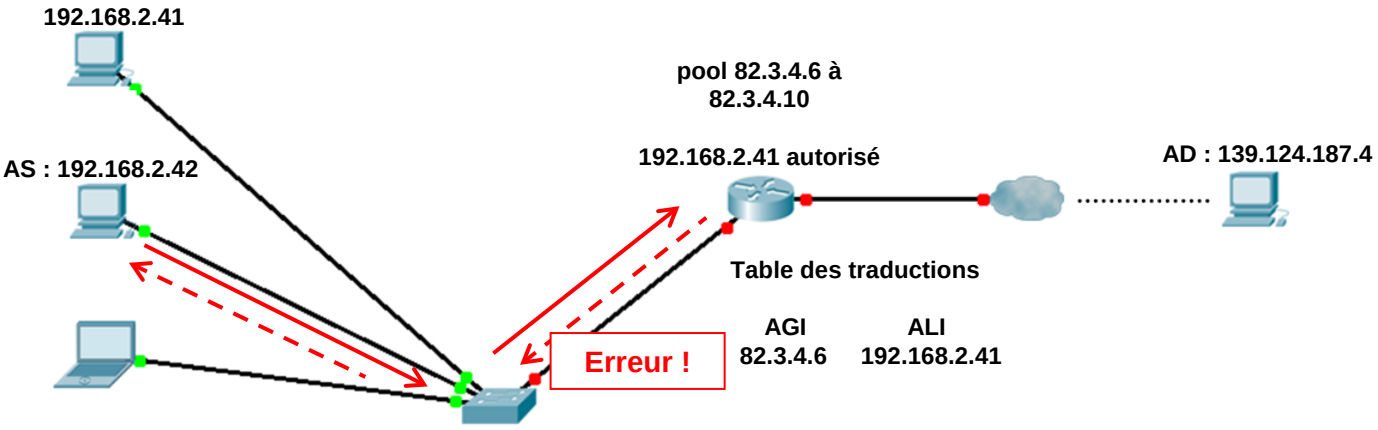


Lorsqu'une machine (Poste 1 ou 2 par exemple) souhaite accéder à un serveur sur Internet, elle envoie sa requête au routeur.
Celui-ci remplace l'adresse IP privée par l'adresse IP publique.
Le serveur sur Internet peut donc répondre puisque l'adresse de retour est publique (celle du routeur).
Lorsque la réponse arrive, le routeur ne peut pas à ce stade renvoyer l'information à la machine concernée.

En effet dans la trame c'est sa propre adresse publique qui est la destination.

Exemples de message sortant avec NAT dynamique : association créée ou réutilisée pour les ALI uniquement autorisées (ici 192.168.2.41).





Pour les messages entrants : ils sont acceptés et traduits uniquement s'il y a une association existante pour l'AGI.

Alors que la NAT limite l'accès simultané à l'extérieur (Internet) à ***n*** stations si l'on dispose de ***n*** AGI, la PAT permet cet accès à plusieurs milliers de machines même si ***n=1***.
Les box des FAI utilisent la PAT pour permettre à plusieurs ordinateurs d'un foyer d'accéder à Internet, puisqu'un foyer ne possède qu'une seule adresse IP.

On peut donc cacher plusieurs machines derrière une seule adresse publique.

Question :

Comment le routeur peut-il transmettre les trames à la bonne machine ?

……

……

……

Si une machine fait une requête avec comme port : « 2542 » par exemple, le routeur saura que lorsqu'il recevra un paquet venant de l'extérieur avec ce port de destination, il faudra le réexpédier à cette machine.

Question :

Que se passe-t-il si deux postes du réseau local ouvrent en même temps un numéro de port identique ?

……

……

……

……

Remarque :

Afin de rendre un réseau privé accessible depuis l'extérieur, il faut utiliser le port « **Forwarding** ».

PRINCIPE DE LA PAT AVEC PORT FORWARDING

La PAT gère et traduit les adresses d'application, là où la NAT crée et gère des associations (AGI, ALI) avec des adresses IP.

Remarques :

Les adresses d'application sont des triplets : (IP, Protocole, Port).

La PAT associe **une adresse d'application globale** à une application d'un hôte interne qui entame un dialogue avec l'extérieur.

Comme les adresses IP, les ports sont aussi traduits. Une association a alors la forme :

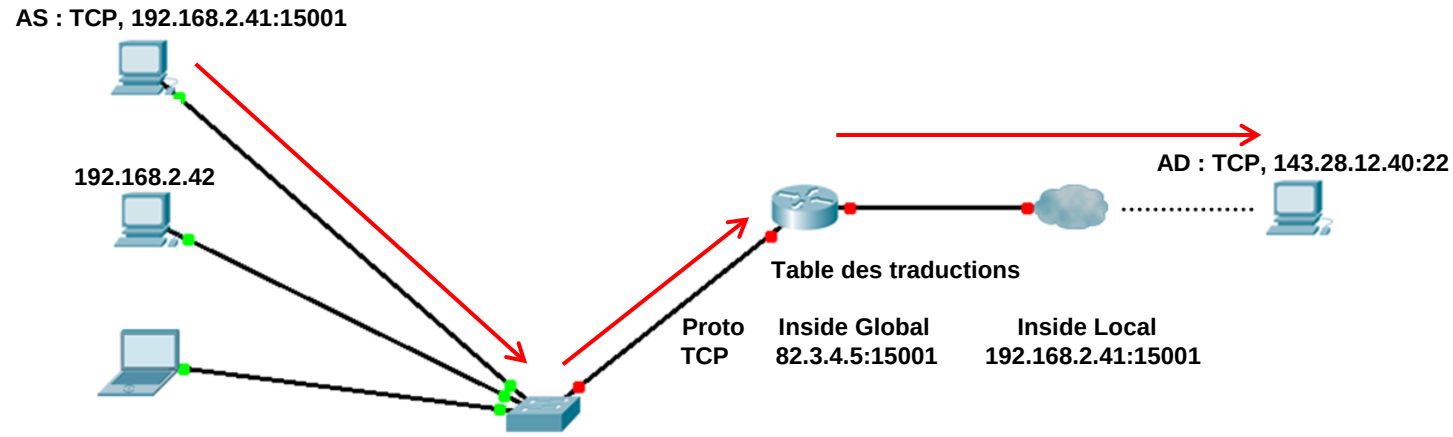
(Protocole, ALI:PLI, AGI:PGI)

avec :

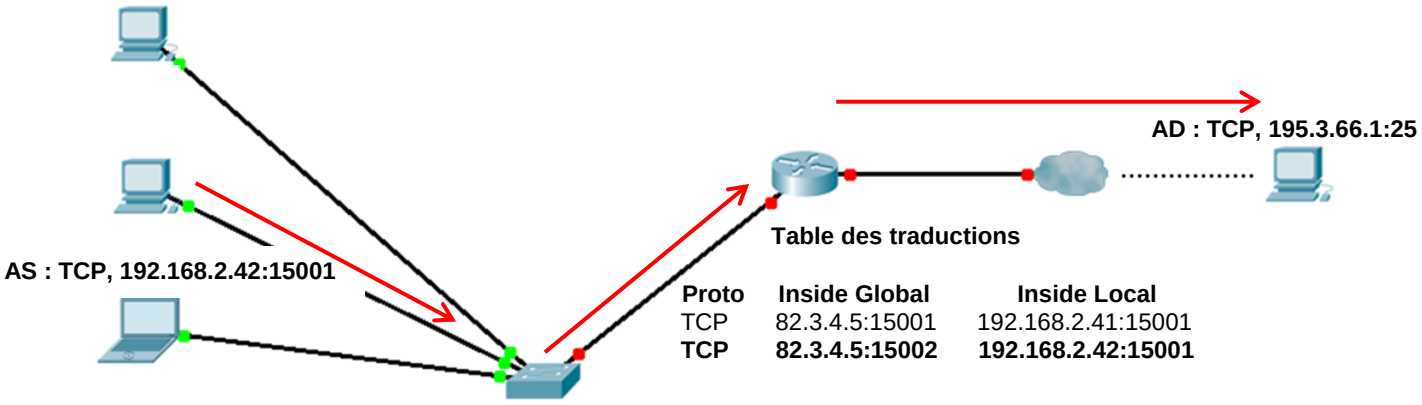
Protocole : UDP, TCP ou ICMP
PLI (Port Local Interne) : est le port utilisé par l'application locale
PGI (Port Global Interne) : est le port associé pour l'adresse globale de l'application

Tout le bénéfice de la PAT réside dans la traduction des ports.
Pour un protocole donné, en attribuant un PGI différent aux applications ayant besoin d'un accès externe, une seule AGI suffit !

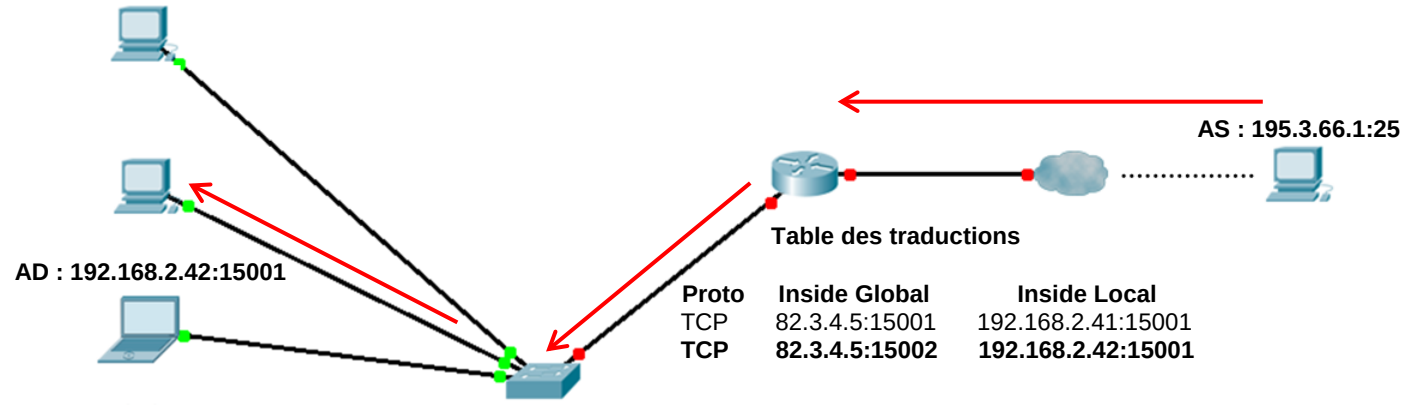
Exemple avec une AGI unique (82.3.4.5) : un client SSH (192.168.2.41) se connecte au serveur SSH externe (143.28.12.40).



Exemple avec AGI unique (82.3.4.5) : un client SMTP (192.168.2.42) se connecte au serveur SMTP externe (195.3.66.1).



Le serveur SMTP répond au routeur qui transmet au client (192.168.2.42) :

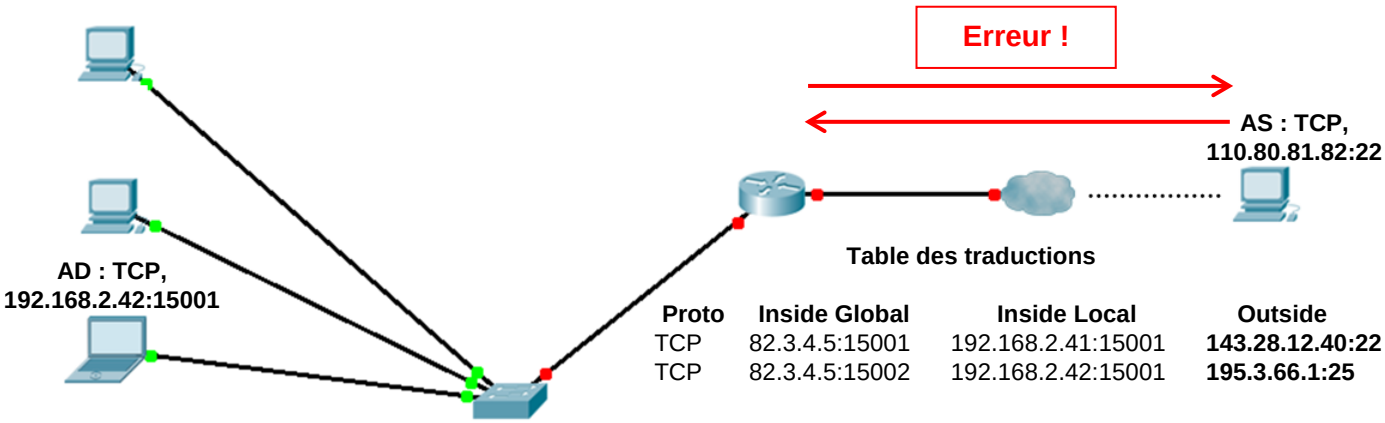


Le serveur SMTP répond au routeur qui transmet au client 192.168.2.42.

FILTRAGE DES MESSAGES ENTRANTS

Un message entrant ne peut créer d'association dans la table des traductions : seul un message sortant peut le faire.
Un message entrant n'est accepté et traduit que s'il fait partie d'un dialogue en cours.
Outre les associations en cours, les dialogues doivent être enregistrés et notamment les adresses des applications externes.
Quand un message entrant arrive, le routeur vérifie que les adresses d'application correspondent à celles d'un dialogue existant.

Exemple : les adresses des applications externes des deux connexions précédentes figurent en réalité dans la table des traductions.
Les messages entrants qui n'appartiennent pas à ces connexions sont rejetées.



ICMP ne fournit pas de ports. Les messages d'erreur ICMP contiennent toutefois les en-têtes IP et TCP/UDP des datagrammes en cause et peuvent donc être traduits.
Les messages ICMP de demande (echo request) contiennent un identificateur. L'identificateur est traduit comme s'il s'agissait d'un port. Une traduction PAT pour un message ICMP (hors messages d'erreur) envoyé vers l'extérieur par une ALI aura donc la forme suivante :

(ICMP, AGI:IGI, ALI:ILI)

ou **ILI** est l'**I**denticateur **L**ocal **I**nterne et **IGI** est l'**I**denticateur **G**lobal **I**nterne.

Ainsi la réponse, qui aura comme IP de destination l'AGI et comme identificateur IGI pourra être traduite et retransmise à l'ALI correspondante.
Comme pour TCP et UDP, les adresses externes sont enregistrées, et les messages entrants ICMP étrangers à un dialogue en cours sont rejetés.

Question :

Comment un serveur interne peut-il être contacté depuis l'extérieur ?

……

……

……

Exemple : la règle suivante sur le routeur ajoute une entrée statique dans la table qui permet à l'extérieur de se connecter au serveur SMTP de la machine 10.1.1.1 :

 # ip nat inside source static tcp 10.1.1.1 25 82.3.4.5 25
 # show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	82.3.4.5:25	10.1.1.1:25	---	---

Ainsi, les segments TCP destinés au port 25 du routeur seront redirigés (traduits) vers le serveur 10.1.1.1.
Certains routeurs permettent de configurer des redirections de plages de ports vers d'autres plages, ainsi que les adresses externes autorisées.

PRINCIPE DE LA PAT AVEC PORT TRIGGERING

Question :

Comment faire si une application utilise plusieurs numéros de ports ? (par exemple FTP port « 21 » pour l'établissement de la connexion et le port « 20 » pour le transfert des données).

……

……

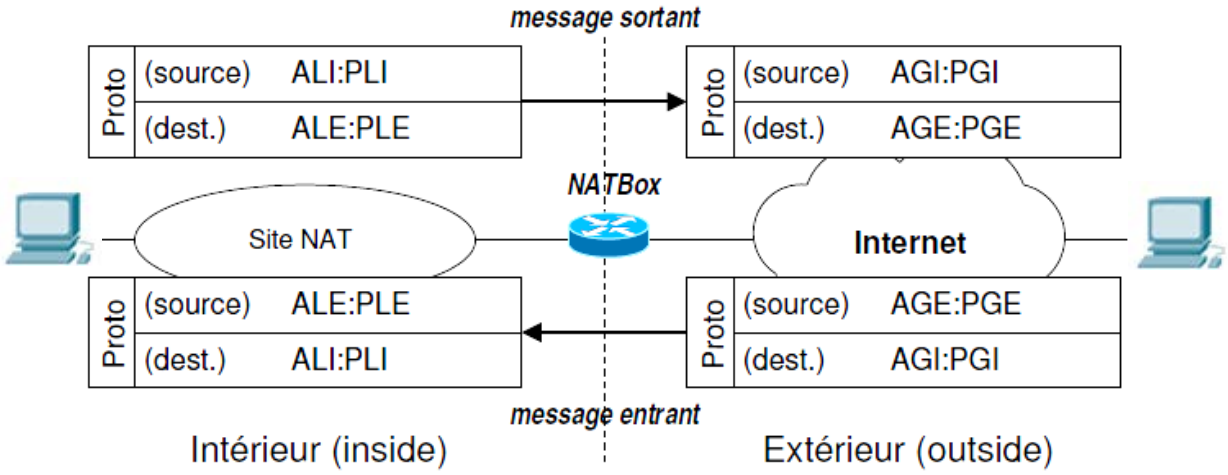
Remarque :

Pour vous en rendre compte, vous pouvez entrer la commande ci-dessous (mode CLI sous OS windows) :

netstat -a

Vous serez surpris du nombre de ports ouverts et/ou à l'écoute (listening) sur votre machine.

SCHÉMA GÉNÉRAL DE LA TRADUCTION PAT



GESTION DE LA TABLE DES TRADUCTIONS

Pour les variantes dynamiques de la NAT et de la PAT, la NATBox doit maintenir un état des "dialogues" (ou sessions) en cours :
- connexions TCP,
- dialogues avec UDP,
- dialogues avec ICMP (essentiellement ping),

car les adresses globales internes, temporairement allouées doivent être rendues à nouveau disponibles dès que possible.
Pour la NAT : l'AGI associée à une ALI devra être à nouveau disponible lorsque les dialogues de l'ALI avec l'extérieur sont terminés.
Pour la PAT : les couples AGI:PGI (de TCP et ceux d'UDP) et AGI:IGI (ICMP) doivent être aussi restitués lorsque les applications ont terminé leur dialogue.

La NATBox doit détecter la fin des dialogues en cours, afin de pouvoir réallouer dès que possible les adresses globales internes.

EFFETS DE LA TRADUCTION SUR LES PROTOCOLES

La traduction opérée par la NAT/PAT doit être transparente, autant pour les ordinateurs que pour les protocoles de TCP/IP.
Or, la modification des adresses/ports source et destination n'est pas anodine pour de nombreux protocoles comme IP, ICMP, TCP, UDP, FTP, et bien d'autres :
IP, TCP et UDP incluent les adresses IP dans le calcul de leur Checksum.
TCP et UDP y incluent aussi les ports et les données.
Les messages d'erreur d'ICMP contiennent une partie (au moins en-têtes IP et TCP/UDP) des datagrammes ayant provoqué l'erreur.
FTP envoie, dans la commande PORT et en réponse de la commande PASV, une adresse d'application à utiliser pour établir une connexion de données.

La NAT doit en tenir compte et modifier tous les messages des protocoles qui utilisent les informations qu'elle traduit !
Cela implique parfois de constamment modifier les numéros de séquence et d'acquittement d'une connexion TCP.

EXEMPLES DE CONFIGURATIONS DE LA NAT DYNAMIQUE

SUR FREEBOX

La NAT est activé par défaut sur les Freebox. Pour vérifier que votre Freebox est bien en "mode routé" (et donc avec la NAT activée), il faut se rendre dans l'interface d'administration (Configurer mon routeur FreeBox). Puis vérifier que l'option est bien activée.

SUR ROUTEUR GNU/LINUX

Voici un exemple de configuration d'un PC routeur sous GNU/Linux placé derrière une box et permettant de remplacer la fonction NAT de cette dernière (qu'il faudra configurer en "mode bridgé").

Votre PC doit disposer :

- d'une interface eth0 dans le plan d'adressage IP privée (vers le LAN)
- d'une interface eth1 dans le plan d'adressage IP public de votre FAI (vers la box)
- d'une configuration IP correcte (serveur DNS, passerelle par défaut...)

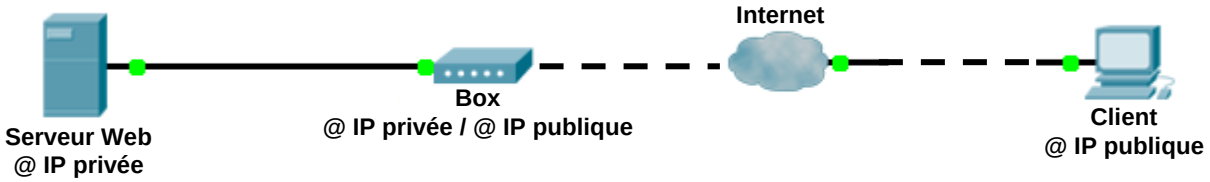
Il faut saisir les lignes suivantes dans un script shell lancé au démarrage de la machine :

iptables --table nat --flush
iptables --table nat --delete-chain
iptables --table nat --append POSTROUTING --out-interface eth1 -j MASQUERADE
iptables --append FORWARD --in-interface eth0 -j ACCEPT
echo 1 > /proc/sys/net/ipv4/ip_forward
service iptables restart

EXEMPLES DE CONFIGURATIONS DE LA PAT

Si vous souhaitez héberger un serveur dans un réseau disposant d'une plage d'adresses IP privées, la NAT n'est d'aucune utilité car elle ne fonctionne que pour les sessions à l'initiative des machines se trouvant sur le réseau privée. Il faut un mécanisme permettant de rendre visible une machine depuis internet. C'est la PAT qui permet cette fonctionnalité.

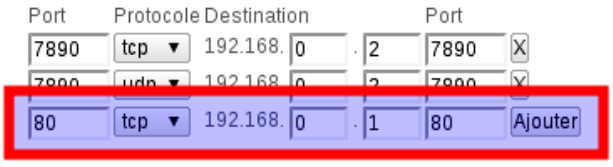
Prenons l'exemple d'une personne voulant héberger son serveur Web (en écoute sur le port TCP/80) chez lui, derrière sa box.



Le client va envoyer une requête http (port 80) vers l'adresse IP publique de la Box (via la résolution DNS). La box, préalablement configurée avec une redirection du port 80 vers le serveur (PAT), va remplacer l'adresse de destination du paquet (l'adresse publique de la box) par celle du serveur (l'adresse privée du serveur). Le serveur va ensuite répondre en utilisant son adresse IP privée comme adresse source. La box va ensuite remplacer celle-ci par son adresse IP publique. Le PC client aura donc l'impression que le serveur Web est hébergé par votre box.

SUR FREEBOX

Il faut vous rendre dans l'interface d'administration de la FreeBox (Configurer mon routeur FreeBox) puis saisir une nouvelle ligne dans le formulaire "Redirection des ports". Pour reprendre l'exemple et en partant sur l'hypothèse ou votre serveur à l'adresse IP privée : 192.168.0.1, il faudra saisir la ligne page suivante.



SUR ROUTEUR GNU/LINUX

Voici un exemple de configuration d'un PC routeur sous GNU/Linux placé derrière une box et permettant de remplacer la fonction PAT de cette dernière (qu'il faudra configurer en "mode bridgé").

Votre PC doit disposer :

- d'une interface eth0 dans le plan d'adressage IP privée (vers le LAN)
- d'une interface eth1 dans le plan d'adressage IP public de votre FAI (vers la box)
- d'une configuration IP correcte (serveur DNS, passerelle par défaut...)

Il faut saisir les lignes suivantes dans un script shell lancé au démarrage de votre machine :

iptables --table nat --flush
iptables --table nat --delete-chain
iptables -t nat -A PREROUTING -p tcp --dport 80 -p DNAT
--to-destination 192.168.0.1
echo 1 > /proc/sys/net/ipv4/ip_forward
service iptables restart