

Partager une connexion Internet.

<http://nassih.com>

© MOHAMED NASSIH.

1. La translation d'adresse.

NAT, pour -Network Address Translation- est la translation de plusieurs adresses privées qui ne peuvent pas aller sur Internet (non routables) en une adresse publique (en général une seule).

Les adresses privées sont utilisées dans les réseaux locaux. Les plages adresses suivantes sont les plus utilisées **RFC 1918: Address Allocation for Private Internets**).

Classe	Première adresse	Dernière adresse
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Figure 1.1 : Adresses pour les réseaux privés

Le natting ou la translation d'adresse permet à plusieurs machines du réseau interne d'accéder à Internet en utilisant seulement une seule adresse publique. Il fournit une manière de cacher les adresses du réseau interne.

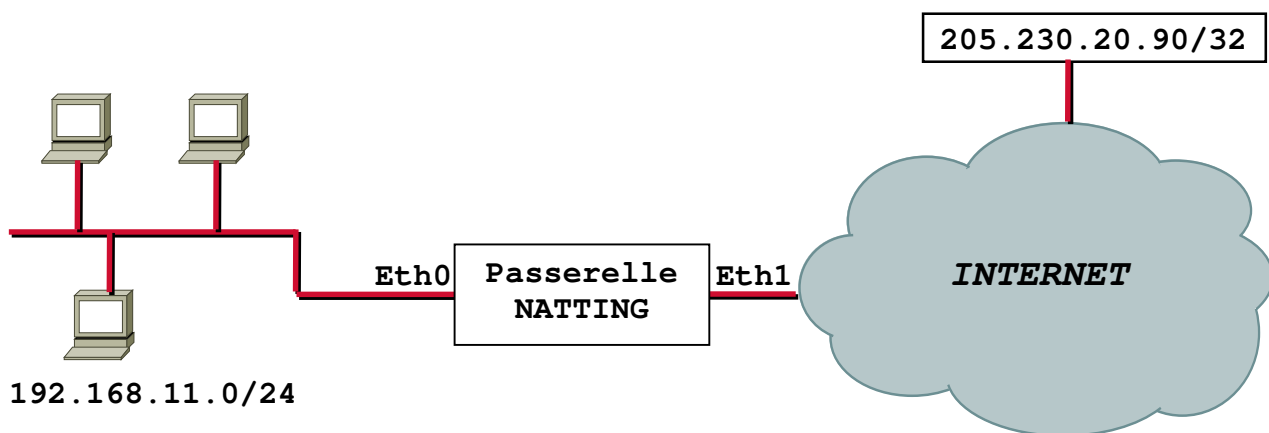


Figure 1.2 : exemple de réseau qui utilise la translation d'adresse

Une passerelle (en général un routeur) est utilisée pour séparer les deux réseaux et fournir le service de translation.

La passerelle gère une table de translation d'adresse voir figure 2, qui maintient la correspondance entre les adresses (adresse IP, port) du réseau interne et les adresses de sorties.

Lors de l'établissement d'une connexion vers une machine sur Internet, une ligne est ajoutée dans la table de la forme (**adresse IP du host source, port source, adresse IP publique de la passerelle, un numéro de port qui identifie la connexion**).

Si on suppose que l'adresse sur le port Eth1 de la passerelle est 220.0.0.1 et les adresses des trois stations sur le réseau local sont respectivement : 192.168.11.1, 192.168.11.2, 192.168.11.3, alors la table de translation d'adresse pourra contenir les informations de la figure 1.3.

Adresse et port en local	Adresse et port utilisée sur le Net
192.168.11.1 3001	220.0.0.1 2100
192.168.11.2 1900	220.0.0.1 2200
192.168.11.3 1043	220.0.0.1 2300

Figure 1.3 : exemple de la table de translation d'adresse

Comme déjà expliqué le réseau interne est configuré avec des adresses IP non routables (n'est pas assigné par IANA –Internet Assigned Numbers Authority-). La passerelle est configurée sur le port Eth1 avec une adresse IP publique assignée par IANA.

Lorsque la station 192.168.11.1, par exemple, essaie de se connecter à un serveur Web sur Internet, la passerelle reçoit le paquet de la station. Après la vérification du paquet et le routage, la passerelle sauvegarde l'adresse IP de la station (192.168.11.1) avec le port source (3001 par exemple) puis elle remplace l'adresse source du paquet par l'adresse du Eth1 (220.0.0.1) et le port source par un autre numéro de port (2100), qui identifie cette connexion et ajoute une ligne dans la table de translation avec les deux adresses IP et les deux numéros de ports (figure 2). La table de translation d'adresse a maintenant une correspondance entre l'adresse non routable privée et l'adresse publique.

Lorsqu'une réponse arrive avec l'adresse de destination 220.0.0.1 et le port de destination 2100, la passerelle examine le port de destination du paquet (qu'est 2100) et cherche dans la table la ligne correspondante. Dans notre cas il s'agit de la ligne 1. Elle change donc l'adresse de destination à 192.168.11.1 et le port de destination à 3001 et envoie le paquet à cette station. Les adresses et les numéros de port sur la ligne 1 sont valides durant la connexion.

Un timer est initialisé à chaque fois que la passerelle accède à la ligne dans la table de translation. Si la passerelle n'a pas utilisé cette ligne pendant un certain temps, la ligne sera supprimée de la table.

Les stations, sur le réseau local, ont l'impression qu'elles communiquent directement avec le serveur Web sur Internet. Le natting est totalement transparent pour les utilisateurs du réseau.

2. Le partage d'une connexion Internet.

On utilisant la translation d'adresse on pourra partager une seule connexion Internet sur plusieurs ordinateurs du réseau local, et donc ces ordinateurs peuvent se connecter à Internet en utilisant une seule connexion, et une seule adresse IP.

Cela pourra être réalisé en deux étapes, la première étape consiste à activer la redirection de port (**IP forwarding**). La deuxième étape consiste à faire la mise en place de la translation d'adresse source (**masquerading**). Avant de passer à la phase pratique je vais expliquer ces deux notions.

2.1. IP Forwarding.

C'est une technique qui consiste à retransmettre les paquets qui entrent sur un port vers un autre. La redirection de port ne garantit aucune sécurité. Elle ne fait que transmettre les paquets reçus sur un port vers un autre.

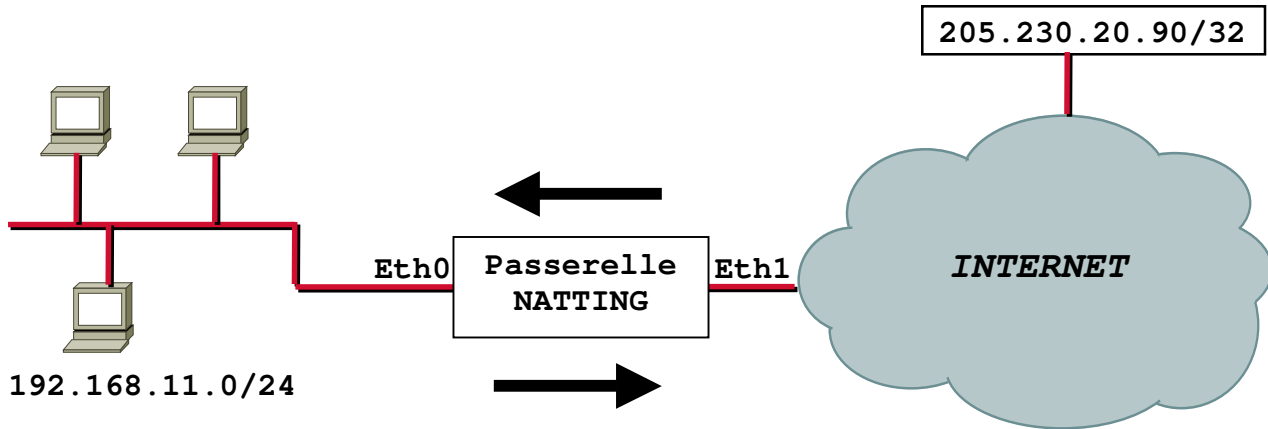


Figure 2.1. Exemple d'un réseau avec le IpForwarding activé.

En pratique pour activer le IP Forwarding, il suffit d'exécuter la commande de la figure 2.2.

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Figure 2.2. Activation de l'acheminement IP –Ipforwarding-

2.2. Masquerading.

La translation d'adresse source consiste à remplacer l'adresse source de la station qui existe sur le réseau local par l'adresse IP publique de la passerelle. Les paquets des stations du réseau local apparaissent sur Internet comme s'ils proviennent de la même machine (La passerelle).

Pour activer le masquerading sur la passerelle de la figure 2.3. , exécuter :

```
iptables -t nat -A POSTROUTING -s 192.168.11.0/24 -o eth1 -j MASQUERADE
```

Figure 2.3. Activation du masquerading

Une autre notion aussi très importante est la translation d'adresse de destination ou le portforwarding, cela consiste à changer l'adresse de destination des paquets qui rentrent vers la passerelle par l'adresse d'un serveur ou station qui existe sur le réseau local.

Cela va permettre d'implanter par exemple un serveur de messagerie sur le réseau local et avec une adresse privée !!

Supposons que nous avons un serveur de messagerie sur le réseau local avec l'adresse 192.168.11.1.

Premièrement il faut permettre au paquets en provenance de l'Internet et qui se dirigent vers le serveur de messagerie (port 25) de traverser la passerelle –Voir Figure 2.4.

```
iptables -A FORWARD -i eth1 -p tcp --dport 25 -j ACCEPT
```

Figure 2.4. Permettre le passage des paquets à destination le serveur de messagerie.

Enfin on active la translation d'adresse de destination en utilisant la commande de la figure 2.5.

```
iptables -t nat -A PREROUTING -j DNAT -i eth1 -p TCP --dport 25 --to-destination 192.168.11.1
```

Figure 2.5. Activation de la translation d'adresse de destination.