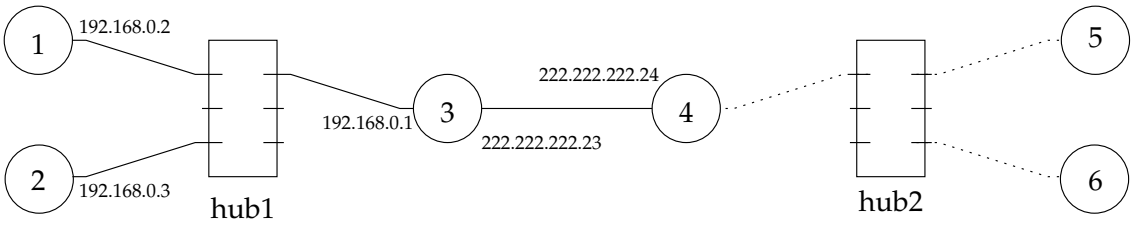
Network Address Translation

1 Création d'une topologie



1 Réalisez la topologie ci-dessus, en annotant le schéma avec le nom des machines et des interfaces réseaux utilisées. Nous utiliserons pour l'instant uniquement les liens pleins. Prenez garde à utiliser des câbles croisés là où ils sont nécessaires.

1 Configurez les différentes tables de routage pour que les machines 1 à 4 puisse se parler entre elles. Vérifiez à l'aide de *ping*.

2 Adressage d'un réseau privé avec NAT

Nous allons dans cette partie rendre le sous-réseau 192.168.0.0 privé. Pour ce faire, nous allons mettre en place des mécanismes de translation d'adresse (NAT) au niveau du nœud passerelle 3.

Pour commencer, nous ne voulons plus que les paquets ayant pour adresse source 192.168. ?. ? (adresse privée) soit traités en 4. Sur la machine 4, on empêche leur traitement par :

```
iptables -t filter -A INPUT -s 192.168.0.0/24 -j REJECT
```

2.1 Translation statique

3 À l'aide de *iptables*, rajoutez les règles NAT pour que la passerelle fasse les translations d'adresses publique/privée 192.168.0.2/222.222.222.23.

4 Affichez les règles *iptables* actives.

5 Faites communiquer la machine 4 avec la machine 1. À l'aide de *tcpdump* et/ou *ethereal*, regardez ce qui se passe sur les machines 1, 3 et 4. Dessinez les diagrammes des échanges en spécifiant les adresses sources et destinations ainsi que les ports utilisés quand vous les connaissez.

2.2 Translation dynamique et redirection de ports

6 Supprimez toutes les règles *iptables* actives.

7 Rajoutez des règles de *masquerading* au niveau de la passerelle 3 pour une translation dynamique.

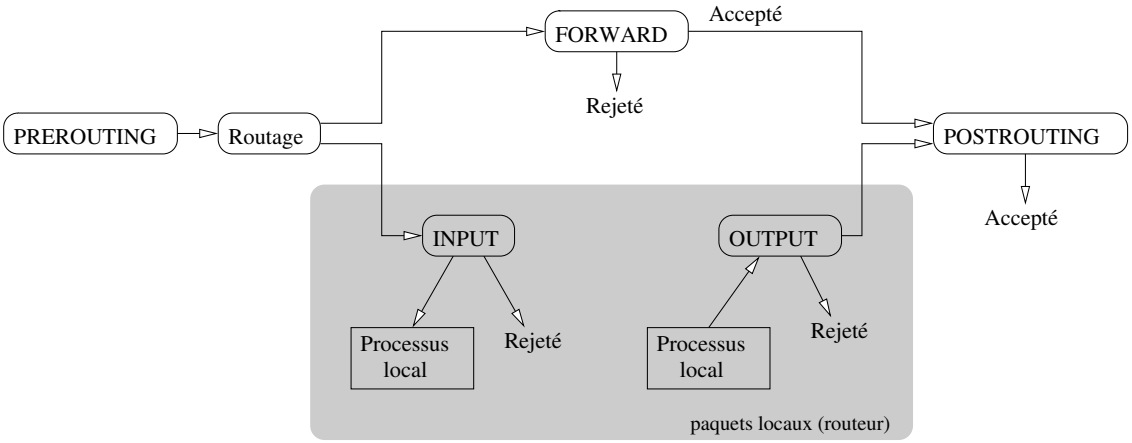
8 On suppose que le nœud 2 est en charge du service *ssh* (port 22) pour le réseau privé, alors que le nœud 1 est en charge du service *http* (port 80). Faites en sorte que les connexions à 222.222.222.1 soient redirigées sur les bonnes machines.

Deux réseaux privés

Faites la même chose pour le deuxième réseau privé (machine 4,5 et 6) en utilisant la même plage d'adresse IP (192.168.0.1 à 192.168.0.3) et de la translation dynamique, puis faites communiquez les deux sous-réseaux obtenus.

Annexe : fonctionnement d'*iptables*

iptables est un module du noyau Linux réalisant le filtrage de paquets. Il possède plusieurs tables : *filter*, *nat* et *mangle*. Nous utiliserons ici la table *nat* qui contient les chaînes de traitement PREROUTING, POSTROUTING et OUTPUT, utilisées comme précisé par le schéma ci-dessous.



affichage Pour afficher les règles d'une table :

`iptables -t` *table* `-L -v`

suppression Pour supprimer une règle :

`iptables -t` *table* `-D` *chaîne numéro_de_la_règle*

Pour supprimer toutes les règles d'une table :

`iptables -t` *table* `-F`

translation statique Pour transformer les paquets entrants dans réseau privé :

`iptables -t nat -A PREROUTING -d` *IP_cible_publique* `-j DNAT --to-destination` *IP_cible_privée*

Pour transformer les paquets sortants d'un réseau privé :

`iptables -t nat -A POSTROUTING -s` *IP_source_privée* `-j SNAT --to-source` *IP_source_publique*

Dans le premier cas, c'est l'adresse destination qui est changé (d'où le `-d` et le `--to-destination`) de *IP_cible_publique* vers *IP_cible_privée*. Dans le second cas, c'est l'adresse source qui est modifiée (d'où le `-s` et le `--to-source`) de *IP_source_privée* en *IP_source_publique*.

translation dynamique Pour utiliser une translation dynamique pour tout un sous-réseau, il faut disposer de son écriture courte (CIDR), comme 192.168.0.0/24 signifiant que le masque vaut 255.255.255.0 (24 bits à 1), puis faire

`iptables -t nat -A POSTROUTING -o` *interface_de_sortie* `-s` *réseau_privé* `-j MASQUERADE`

redirection de ports Pour rediriger les connexions sur un port spécifique vers une machine du réseau privé :

`iptables -t nat -A PREROUTING -p tcp -d` *IP* `--dport` *port_initial* `-j DNAT --to` *IP_privée/port_final*

Ceci redirige toutes les connexions entrantes à *IP* sur le port *port_initial* vers *IP_privée/port_final*.

Vous pouvez bien sûr en savoir plus sur *iptables* en consultant sa page de manuel.

Remerciements
Ce TP n'aurait pu avoir lieu sans la coopération exceptionnelle du Dr Guermouche.