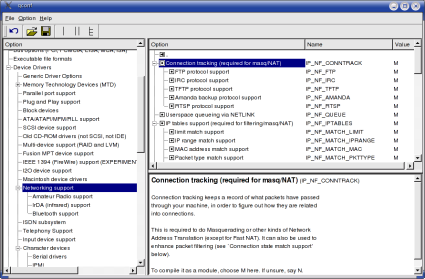
**La traduction d'adresse - NAT**

La traduction d'adresse est gérée avec les chaînes PREROUTING, POSTROUTING et OUTPUT. Dans la chaîne PREROUTING (avant routage), on ne peut modifier que l'adresse de destination. L'adresse source est conservée. On fait donc du DNAT. On dit qu'on fait du "NAT destination". Dans la chaîne POSTROUTING, (après routage) on ne peut modifier que l'adresse source. L'adresse de destination est conservée. On fait donc du SNAT. On dit qu'on fait du "NAT source".

Certaines applications arp, ftp, irc ... nécessitent des options. Ces options sont compilées directement dans votre noyau ou sous forme de modules.

**Figure 62.1. Compilation du noyau pour netfilter**



Les modules sont dans :

/lib/modules/VotreNoyau/kernel/net/ipv4/netfilter/

**Le DNAT ou NAT Destination**

On substitue à l'adresse de destination des paquets provenant du réseau public, une adresse du réseau local privé. Dans l'exemple, les paquets à destination de la machine 195.x sont redirigés vers la machine 172.y. On ne tient pas compte du port.

iptables -F INPUT ; iptables -P INPUT ACCEPT

iptables -F OUTPUT ; iptables -P OUTPUT ACCEPT

iptables -F FORWARD ; iptables -P FORWARD ACCEPT

iptables -t nat -F PREROUTING

iptables -t nat -A PREROUTING -d 195.115.19.35/32 \

-j DNAT --to-destination 172.16.0.1/32

**Le SNAT ou NAT Source**

Le SNAT consiste à substituer une adresse source dans un paquet sortant à son adresse source d'origine. On substitue ici, aux requêtes provenant du réseau 192.168.0.0/24, une des 10 adresses publiques.

iptables -F INPUT ; iptables -P INPUT ACCEPT

iptables -F OUTPUT ; iptables -P OUTPUT ACCEPT

iptables -F FORWARD ; iptables -P FORWARD ACCEPT

iptables -t nat -F POSTROUTING

iptables -t nat -A POSTROUTING -s 192.168.0.0/24 \

-j SNAT --to-source 195.115.90.1-195.115.90.10

**L'IP Masquerade**

Dans ce cas, les adresses privées, utilisent toutes la même adresse publique. C'est le procédé qui est utilisé avec ipchains. Il s'agit en fait de translation de port avec ipchains ou de SNAT (Nat Source) avec iptables.

iptables -F INPUT ; iptables -P INPUT ACCEPT

iptables -F OUTPUT ; iptables -P OUTPUT ACCEPT

iptables -F FORWARD ; iptables -P FORWARD ACCEPT

iptables -t nat -F POSTROUTING

iptables -t nat -A POSTROUTING -s 10.10.10.0/8 \

-j SNAT --to-source 139.63.83.120

Une autre option consiste à utiliser l'option "MASQUERADE"

iptables -t nat -F POSTROUTING

iptables -t nat -A POSTROUTING -s 10.10.10.0/8 -j MASQUERADE

**Exemple sur un réseau privé**

L'exemple ci-dessous indique comment partager un accès internet chez soi pour plusieurs machines. Vous voulez partager un accès "dial" sur votre réseau.

#ifconfig

eth0 Lien encap:Ethernet HWaddr 00:80:C8:7A:0A:D8

inet adr:192.168.0.1 Bcast:192.168.0.255 Masque:255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:19950 errors:0 dropped:0 overruns:0 frame:0

TX packets:24988 errors:0 dropped:0 overruns:0 carrier:0

collisions:2 lg file transmission:100

RX bytes:2830076 (2.6 Mb) TX bytes:12625623 (12.0 Mb)

Interruption:5 Adresse de base:0x240

ppp0 Lien encap:Protocole Point-à-Point

inet adr:212.47.248.114 P-t-P:212.47.251.49 Masque:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1524 Metric:1

RX packets:27 errors:0 dropped:0 overruns:0 frame:0

TX packets:29 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 lg file transmission:3

RX bytes:4924 (4.8 Kb) TX bytes:1365 (1.3 Kb)

#echo 1 > /proc/sys/net/ipv4/ip\_forward

#iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE

iptables -t nat -L

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

MASQUERADE all -- 192.168.90.0/24 anywhere

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Le tour est joué, vous n'avez plus qu'à configurer les autres clients avec un DNS et une passerelle par défaut. Votre accès wan est partagé.