Routing (SNAT)

De cele mai multe ori utilizatorii casnici folosesc o conexiune broadband de tip ADSL sau CaTV pentru conectarea la Internet.

Nota

In ultima vreme datorita cresterii vitezei oferite de ADSL, acest timp de tehnologie de WAN incepe sa fie folosita si pentru companii. ADSL+ ofera un Bandwidth Downstream de peste 22Mbs.

Indiferent de tehnologia de WAN folosita ISP-ul furnizeaza un singur IP public sau in cel mai bun caz cateva IP-uri publice.

Solutia folosita pentru a lega mai multe calculatoare la Internet (neavand atatea IP-uri publice cate calculatoare) este configurea unui Router care sa realizeze NAT (Network Address Translation).

Se foloseste asfel un router dedicat sau un calculator care ruleaza Linux cu cel putin 2 placi de retea Ethernet (leaga 2 retele si anume LAN-ul si Internetul). O interfata si anume cea care se conecteaza cu providerul se configureaza cu IP-ul public, iar cealalata interfata numita interfata de LAN se configureaza cu un IP privat.

Nota

IETF a definit in RFC 1918 3 clase de IP-uri private care pot fi folosite in mod liber pentru adresarea unui LAN.

Acestea sunt:
10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0-192.168.255.255

Procesul prin care hosturile din LAN (din spatele routerului) pot comunica pe Internet si anume procesul de NAT presupune inlocuirea IP-ului privat de catre router din pachetele generate de hosturile din LAN cu unicul IP public si trimiterea acestora pe Internet.
Efectul este ca pe Internet intreg LAN-ul este ascuns si nu se poate determina ce host din LAN a generat pachetul sau ca exista LAN-ul. Pachetele par sa vina de la Router.

Avantaje NAT:

- Economia de IP-uri publice. Cu un singur IP public putem crea o retea localta conectata la Internet formata din zeci sau sute de hosturi;
- Securitate. Lan-ul este izolat, nu se pot initializa conexiuni din exterior catre un host din interior fara configuratii speciale ale routerului (port forwarding);

Un host Linux poate fi transformat intr-un router nededicat. Componenta software care realizeaza NAT este NETFILTER (unica posibilitatea).

Nota

Procesul de NAT descris mai sus este referit de multe ori ca SNAT (source NAT) pentru faptul ca se modifica IP-ul sursa privat cu IP-ul public. Aceasta referire nu este in totalitate corecta fiindca SNAT este insotit intotdeauna de DNAT (destination NAT) si anume la intoarcerea pachetului de pe Internet se inlocuieste IP-ul destinatie public cu IP-ul destinatie privat, iar pachetul este trimis la hostul din LAN de catre Router

Din punct de vedere al configurarii NETFILTER urmatoarele aspecte sunt importante:

- SNAT se realizeaza pe chainul POSTROUTING folosind tabelul nat care este suficient sa contina o singura regula;
- se foloseste targetul SNAT. Se poate folosi si targetul MASQUERADE in momentul in care IP-ul public nu este static ci este obtinut dinamic;
- default hostul Linux nu ruteaza. Pentru a fi transformat intr-un router trebuie ca in fisierul /proc/sys/net/ipv4/ip_forward sa se gaseasca valoarea 1 (unu);

Exemplu transformare host in router si configurare pentru SNAT (configuratie completa):

```
#presupunem ca ip-ul public este 213.232.32.3, subnetul local este 10.0.0.0/24 iar interfata de WAN se numeste eth0
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j SNAT --to-source 213.232.32.3
#activeaza procesul de rutare
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Nota

Se recomanda rularea scriptului de mai sus la butare automat folosind scripturi de management a serviciilor din directorul `/etc/init.d`