

Konfiguriranje Debian GNU/Linux gatewaya

Pod pojmom gatewaya možemo smatrati kompjuter preko kojega se ostali kompjuteri u jednoj lokalnoj mreži (LAN-u) spajaju na neku drugu mrežu. Najčešće tu drugu mrežu predstavlja internet. U primjeru konfiguriranja gatewaya koji ćemo ovdje razmotriti, a radi se o informatičkoj "infrastrukturi" u mom stanu, situacija je bila slijedeća - Htio sam u mrežu spojiti dva kompjutera, od kojih je jedan priključen na internet preko kablovskog LAN modema i to tako da se sa drugog također može pristupiti internetu. Na prvom kompjuteru instaliran je Debian 5.0 (Lenny), a na drugom Debian 3.0 (Woody).

Inače pristup internetu s drugih kompjutera u slučaju "kućnih" korisnika rješava se i pomoću WLAN - Wireless LAN modema na koje se kompjuteri spajaju bežično ili pomoću LAN modema koji na sebi imaju više mrežnih priključaka. No takvi su modemi skuplji, a oni bežični su uz to i izvor elektromagnetskog zračenja čiji utjecaj na zdravlja čovjeka nije detaljnije ispitan.

Pretpostavka od koje polazimo je, naravno, da je sa kompjutera predviđenog da služi kako gateway moguće pristupiti internetu. Pošto se modem spaja na kompjuter pomoću mrežnog kabla, da bismo isti kompjuter spojili i sa onim drugim, trebao nam još jedan mrežni priključak. To smo dobili ugradnjom još jedne mrežne kartice - u konkretnom slučaju uz mrežnu karticu ugrađenu na matičnu ploču dodana je PCI kartica RTL 8139C. Ovu karticu Debian Lenny prepoznaje bez problema (kao i većinu drugih PCI mrežnih kartica). Nakon toga trebalo je iskonfigurirati još jedan network interface - **eth1** (uz postojeći **eth0**). Taj se interface odnosi na lokalnu mrežu za čiju smo adresu uzeli broj **192.168.198.0** (za adresu samog interfacea uzeli smo **192.168.198.1**), dok se **eth0** odnosi na "vanjsku" mrežu (internet), i on se prema pravilima moga internet providera konfigurira preko njihovog DHCP servera. Dakle u konfiguracijskom fileu za mrežu **/etc/network/interfaces** na Lennyju treba stajati slijedeće:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
# The secondary network interface
allow-hotplug eth1
iface eth1 inet static
    address 192.168.198.1
    netmask 255.255.255.0
    network 192.168.198.0
    broadcast 192.168.198.255
```

Nakon dodavanja podataka za konfiguraciju interfacea **eth1**, potrebno je taj interface staviti u funkciju. To se postiže naredbom

```
ifup eth1
```

Inače, pri svakoj promjeni podataka u **/etc/network/interfaces** treba odgovarajući interface "spustiti" (što se vrši naredbom **ifdown oznaka_interfacea**), pa opet "podići", tj. restartati.

Mrežnu konfiguraciju možemo nakon toga provjeriti naredbom

```
ifconfig -a
```

Sad je i na drugom kompjuteru (Woodyju) potrebno konfigurirati mrežne postavke, a ako je to već napravljeno, onda samo dodati podatak o adresi gatewaya u konfiguracijski file **/etc/network/interfaces**. Nakon toga ovaj file treba izgledati ovako:

```
# The loopback interface
auto lo
iface lo inet loopback
```

```

# The first network card
auto eth0
iface eth0 inet static
    address 192.168.198.199
    netmask 255.255.255.0
    network 192.168.198.0
    broadcast 192.168.198.255
    gateway 192.168.198.1

```

Primijetimo da se radi se o istoj mreži (adresa mreže je ista kao i na prvom kompjuteru (Lennyju)). LAN adresa drugog kompjutera (Woodyja) odnosno njegovog interfecea **eth0** je dakle **192.168.198.199**.

Nakon ove promjene slijedi dizanje interfecea **eth0** odnosno njegovo restartanje, kako je već rečeno.

Sada na Lennyju treba konfigurirati "tablicu rutiranja" za lokalnu mrežu (**192.168.198.0**) i internet (koji se označava adresom **0.0.0.0**) sa:

```

route add -net -n 192.168.198.0 netmask 255.255.255.0 dev eth1
route add -net -n 0.0.0.0 dev eth0

```

Tablicu rutiranja možemo izlistati naredbom **route**.

Nakon toga, potrebno je podesiti konfiguraciju firewalla na istom kompjuteru tako da omogući IP Forwarding tj. prienos podataka između ostalih kompjutera na lokalnoj mreži i interneta, kao i IP Masquerading ili Network Address Translation (NAT) što omogućava ovu komunikaciju premda ti kompjuteri nemaju vlastitu IP adresu na internetu (postoji samo IP adresa gatewaya). Ovdje najprije treba obrisati postojeće postavke firewalla naredbama:

```

iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain

```

a zatim konfigurirati IP Forwarding i IP Masquerading na firewallu (iptables) naredbama:

```

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT

```

Sad još treba omogućiti IP Forwarding naredbom:

```

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

```

Inače, gore navedeno podešavanje firewalla na Debian GNU/Linuxu vrši se automatski ako instaliramo deb paket **ipmasq** (instalacija se pokreće naredbom **apt-get install ipmasq** - uz to je pri svakom dizanju sustava potrebno izvršiti naredbu **ipmasq**).

Da bi se sa kompjutera na lokalnoj mreži (Woodyja) moglo pristupiti internetu, potrebni su nam još podaci o DNS serveru(ima) našeg internet providera koji se upisuju u file **/etc/resolv.conf** na svakom od tih kompjutera. Ako ove podatke nismo dobili od internet providera, onda možemo pogledati isti takav file (dakle **/etc/resolv.conf**) na gatewayu (Lennyju) i jednostavno ih prepisati (ti podaci ovdje se zapisuju pri dodjeli IP adrese od strane DHCP servera). U konkretnom slučaju dodali smo slijedeća dva retka:

```

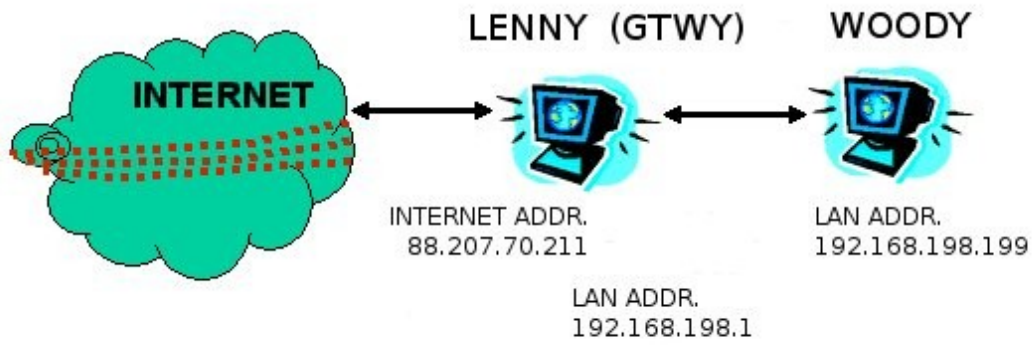
nameserver 83.139.105.2
nameserver 83.139.104.2

```

Nakon toga na kompjuteru na lokalnoj mreži (Woodyju) još treba restartati network interface i time bi njegov pristup internetu bio omogućen. Internetu se pristupa na isti način kao kad bi kompjuter bio spojen direktno.

U slučaju problema sa ovim načinom pristupa internetu, treba najprije pokušati pingati internet (primjerice sa **ping www.google.com**) ili network interface na gatewayu povezan s internetom, pa vidjeti kakve su poruke sustava. Dakako najprije treba provjeriti da li lokalna mreža uopće "radi" i je li spajanje na internet moguće sa gatewaya.

Radi sigurnosti, preporučljivo je spustiti sve nepotrebne mrežne servise na svim kompjuterima spojenim na lokalnu mrežu, kao što su port mapper, mail transport agent, NFS-server, telnet, ftp, web server i sl. No, ova priča sad već spada u network security.



Sl. 1 - Shema mreže opisane u primjeru