

Napredno korištenje operacijskog sustava Linux

3. Mreže

Dominik Barbarić

Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

04.03.2018

Sadržaj

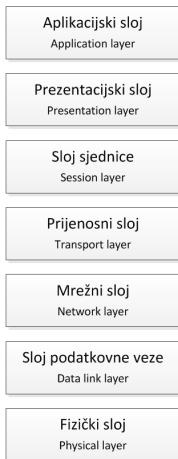
- 1 TCP/IP
 - IP konfiguracija
 - Routing
 - DNS
 - iptables

- 2 WLAN

Modeli mreža

Prisjetimo se...

OSI referentni model



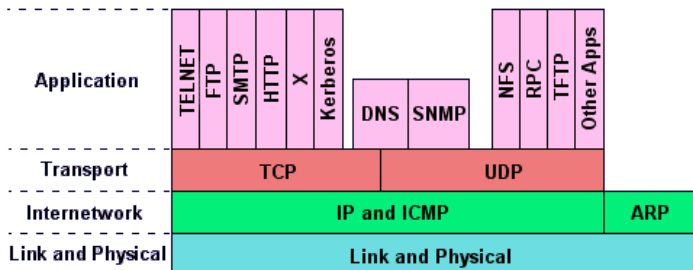
TCP/IP model



Modeli mreža

Prisjetimo se...

- TCP/IP je najraširenija implementacija OSI modela
- Komutacija paketa
- IP omogućuje globalnu komutaciju



Adresiranje u TCP/IP modelu

Sloj pristupa mreži

- Različito implementiran za svaku metodu pristupa (Ethernet, WLAN, ADSL, DOCSIS, ...)
- **MAC (Media Access Control)**
 - Odgovara drugom sloju (*Layer 2*) OSI modela
 - Osigurava pristup mediju, tj. dijelu mreže s kojom je uređaj izravno povezan
 - Svaki mrežni uređaj ima jedinstvenu (hardversku) *MAC adresu* oblika
0a:1b:2c:3d:4e:5f (48b u hex zapisu)
- MAC protokol omogućuje komunikaciju između izravno povezanih uređaja

Adresiranje u TCP/IP modelu

Internetski sloj

- Odgovara trećem sloju (*Layer 3*) OSI modela
- Omogućuje komutaciju između Layer 2 mreža
- Adresiranje *IPv4* i *IPv6* adresama oblika

192.168.100.100

(IPv4 - 32b u dec zapisu)

fc00:0000:0000:0000:0000:0000:0001:00db

fc00::1:db

(IPv6 -128b u potpunom i skraćenom zapisu)

Adresiranje u TCP/IP modelu

IPv4

- ARPANET 1983.
- Adrese se sastoje od 4 okteta = 32 bita
- Ukupno adresabilno
 $2^{32} = 4,294,967,296$ adresa

IPv6

- Adrese se sastoje od 8 grupa od 16 bita = 128 bita
- Prikaz heksadekadskim znamenkama
- Ukupno adresabilno
 $2^{128} = 3.403 \cdot 10^{38}$ adresa

Adresiranje u TCP/IP modelu

Subnet

- Dio mreže s vlastitim rasponom IP adresa koji nema izravnu vezu s drugim takvim dijelom mreže
- Subnet je definiran IP adresom mreže i *subnet maskom*

Adresiranje u TCP/IP modelu

Primjer određivanja subneta

Mreža je određena adresom mreže i subnet maskom

Network: 172.16.64.0

Mask: 255.255.192.0

Subnet mask se raspisom u binarni oblik može zapisati:

11111111.11111111.11000000.00000000

Na isti način adresa mreže se može zapisati:

10101100.00010000.01000000.00000000

Dvije IP adrese pripadaju istom subnetu ako su im svi bitovi na mjestima gdje se u maski nalazi 1 isti. Zadana mreža obuhvaća sve IP adrese oblika:

10101100.00010000.01*****.*****

U decimalnom zapisu:

172.16.64.0 – 172.16.127.255

Adresiranje u TCP/IP modelu

Network: 172.16.64.0

Mask: 255.255.192.0

- **Uočiti** - U svakoj subnet maski jedinice se nužno nalaze na višim bitovima, a nule na nižim
- Nemoguća je maska u kojoj se 0 nalazi između dvije 1
- **CIDR notacijom** adresa mreže se zapisuje u obliku
172.16.64.0/18
- Broj iza adrese mreže (/18) odgovara broju jedinica u subnet maski

Adresiranje u TCP/IP modelu

Posebni rasponi i adrese

Lokalne mreže

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

fc00::/7

Link-local mreže

169.254.0.0/16

fe80::/10

Multicast adrese

224.0.0.0/4

Loopback adresa

127.0.0.1

::1

Adresiranje u TCP/IP modelu

Posebni rasponi i adrese

- Unutar raspona subneta postoje dvije posebne adrese
- Računala na mreži **ne mogu** zauzeti navedene adrese

Adresa mreže

- Prva adresa u rasponu
- Primjer

192.168.20.0

Broadcast adresa

- Posljednja adresa u rasponu
- Primjer

192.168.20.255

Primjeri su dani za subnet s rasponom 192.168.20.0/24

IP konfiguracija

IP adresa se dodjeljuje

- Dinamički - DHCP protokol
- Statički

Konfiguracija se obavlja kroz

- networking
- netctl
- systemd-networkd
- NetworkManager
- wicd

IP konfiguracija

/etc/network/interfaces

```
auto eth0
iface eth0 inet static
    address 192.168.1.5
    netmask 255.255.255.0
    gateway 192.168.1.254
```

```
auto eth1
iface eth1 inet dhcp
```

- `auto eth0` - eth0 se omogućuje pri startupu
- `iface eth0 inet static` - eth0 ima dodijeljenu statičku IP adresu
- `iface eth1 inet dhcp` - eth1 traži dinamičku IP adresu

IP konfiguracija

- `/etc/network/interfaces` se čita prilikom uključivanja i isključivanja mrežnog adaptera
`ifup eth0` `ifdown eth0`
- Neke naredbe za promjenu konfiguracije

Operacija	ifconfig	ip
Pregled konfiguracije	ifconfig	ip addr show ip link show
Uključenje i isključenje sučelja	ifconfig <interface> up down	ip link set <interface> up down
Podešavanje IP adrese	ifconfig <interface> <IP>	ip address add del <IP> dev <interface>

Routing

- Povezivanje subneta ostvaruje se *routingom*
- Računalo ima konfigurirane rute preko kojih ostvaruje povezanost sa drugim mrežama
- Rute su određene odredišnom adresom i adresom routera ili gatewaya

```
# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.0.0	192.168.1.2	255.0.0.0	UG	1	0	0	eth0
0.0.0.0	192.168.1.10	0.0.0.0	UG	0	0	0	eth0

```
# ip route show
```

```
192.168.99.0/24 dev eth0 scope link  
10.0.0.0/8 via 192.168.1.2 scope link dev eth0 metric 1  
default via 192.168.1.10 dev eth0
```


DNS

- Prevođenje imena računala (tekstualne adrese) u IP adresu
- DNS server
- IP adresu servera klijenti dobivaju
 - Putem DHCP-a
 - Ručnom konfiguracijom
`/etc/resolv.conf`
Uređivanje pomoću spomenutih alata

```
nameserver 8.8.8.8
```

```
nameserver 8.8.4.4
```

DNS

DNS server - bind

- Svaka domena (npr. `fer.hr`) ima svoj *authority*
`$ dig soa fer.hr`
- Primary i secondary DNS server
`$ dig ns fer.hr`
- Svi zapisi o nekoj domeni (*records*) nalaze se u *zone file*
- Proučiti bind konfiguraciju

```
$ dig www.fer.hr
```

```
www.fer.hr.      3600    IN      A       161.53.72.119
```

DNS

Reverse DNS lookup

- Prevođenje IP adresa u domain nazive
- Posebne zone s PTR recordima

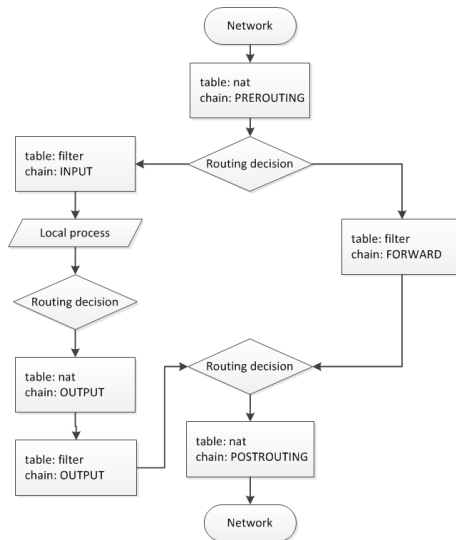
```
$ dig -x 161.53.72.119  
119.72.53.161.in-addr.arpa. 86400 IN PTR skynet.cc.fer.hr.
```

iptables

iptables

- Firewall na Linuxu
- *Netfilter* framework u kernelu
- Provjerava, mijenja, prosljeđuje ili odbacuje pakete prema pravilima u tablici
- Tablica se sastoji od lanaca (*chains*), a lanci od pravila (*rules*)
- Svako pravilo je definirano oblikom paketa na koji se odnosi i akcijom koju obavlja nad tim paketom (*target*)

iptables



Network address translation (NAT)

- Za povezivanje lokalnih mreža koristi se prevođenje adresa
- Sva računala koja koriste NAT kao routu prema nekoj drugoj mreži dobivaju *istu IP adresu* na odredišnoj mreži
- Implementirano u iptables

Razlikovati

- **SNAT** (Source NAT)
Postupak prevođenja adrese odlaznim paketima
- **DNAT** (Destination NAT)
Postupak prevođenja adrese dolaznim paketima

Network address translation (NAT)

NAT za sve pakete od eth1 na eth0

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# iptables -A FORWARD -i eth0 -o eth1 -m state
--state RELATED,ESTABLISHED -j ACCEPT
# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

DNAT za HTTP server na internoj adresi 192.168.20.20

```
# iptables -t nat -A PREROUTING -p tcp -d 161.53.66.200
--dport 80 -j DNAT --to-destination 192.168.20.20
```

NAT 1:1

```
# iptables -t nat -A PREROUTING -d 161.53.66.202 -j DNAT
--to-destination 192.168.20.30
# iptables -t nat -A POSTROUTING -s 192.168.20.30 -j SNAT
--to-destination 161.53.66.202
```

Dodatne IP adrese

- Jedan mrežni adapter može imati više IP adresa
- Linux svaku adresu tretira kao da se radi o zasebnim mrežnim uređajima

`/etc/network/interfaces`

```
auto eth0
iface eth0 inet dhcp

auto eth0:0
iface eth0:0 inet dhcp

auto eth0:1
iface eth0:1 inet static
    address 192.168.20.4
    netmask 255.255.255.0
```


VLAN

Virtual LAN

- Omogućuje ga standard 802.1Q
- Svaki mrežni paket može nositi "naljepnicu" (**tag**) koja označava kojem dijelu mreže paket pripada
- VLAN tag sadrži **VLAN ID** (VID)
- Layer 2 mrežna oprema (konfigurabilni switchevi) usmjeravaju pakete među priključcima koji pripadaju istom VLAN-u
- Ostvareno je **Layer 2 odvajanje**
- VLAN se na svakom priključku koristi kao
 - Tagged promet Računalo postavlja 802.1Q tag prije slanja paketa
 - Untagged promet Switch postavlja 802.1Q tag nakon što primi paket

VLAN

```
# apt-get install vlan
# modprobe 8021q

# ifup eth0
# vconfig add eth0 100
Added VLAN with VID == 100 to IF -:eth0:-
# ifconfig eth0.100 192.168.10.20/24

# ifconfig eth0.100
eth0.100  Link Encap: Ethernet  ...
...      inet addr:192.168.10.20

# vconfig rem eth0.100
Removed VLAN -:eth0.100:-
```

Konfiguracija mreže

NetworkManager

Editing Auto eth1

Connection name: Auto eth1

☒ Connect automatically

Wired 802.1x Security IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.99	255.255.255.0	192.168.1.254

DNS servers: 192.168.1.254

Search domains:

DHCP client ID:

☒ Require IPv4 addressing for this connection to complete

Routes...

☒ Available to all users

Cancel Apply...

Konfiguracija IP adrese

☐ Wired Network

Wireless Networks

☐ eduroam

☐ ICWLAN

☐ Imperial-Parkeray

☒ Imperial-WPA

☐ Wifi Zone - The Cloud

VPN Connections

Connect to Other Wireless Network...

Create New Wireless Network...

Manual configuration...

Thu 17 Apr, 10:24

Odabir WLAN mreže

WLAN

- 802.11 a/b/g/n

Bežična mreža je određena s

- SSID - naziv mreže
- BSSID - identifikator AP-a
- Sigurnosna razina
 - Otvorena mreža
 - WEP
 - WPA - Personal i Enterprise

Podešavanje pristupa mreži

Pregled naredbi

Pretraživanje mreža	<code>iwlist scan wl0</code>
Odabir mreže (ESSID)	<code>iwconfig wl0 essid Ne_kradi</code>
Odabir mreže (SSID)	<code>iwconfig wl0 ap 00:11:22:33:44:55</code> <code>iwconfig wl0 any</code>
Spajanje na WEP mrežu (hex ključ)	<code>iwconfig wlan0 essid</code> <code>Ne_kradi key 0123456789</code>
Spajanje na WEP mrežu (string ključ)	<code>iwconfig wlan0 essid</code> <code>Ne_kradi key s:password</code>

- Nakon spajanja na bežičnu mrežu slijedi uobičajena IP konfiguracija
- Za WPA mreže koristi se `wpa_supplicant`

WLAN

wpa_supplicant

- Konfiguracija kroz `wpa_cli` ili izravno `/etc/wpa_supplicant.conf`

```
$ wpa_passphrase MYSSID passphrase
network={
    ssid="MYSSID"
    #psk="passphrase"
    psk=59e0d07fa4c7741797a4e394f38a5c321e3bed51d54ad5fcbd3f84bc7415d73d
}
```

[/etc/wpa_supplicant/eduroam.conf](#)

```
network={
    ssid="eduroam"
    proto=WPA2 WPA
    key_mgmt=WPA-EAP
    pairwise=CCMP TKIP
    group=CCMP TKIP
    ca_cert="<path_to_cert>/eduroam_fer.hr_CA.pem"
    subject_match="freeradius.fer.hr"
    identity="<USER>"
    eap=TTLS
    password="<PASSWORD>"
    phase2="auth=PAP"
}
```

Literatura

<https://wiki.debian.org/NetworkConfiguration>

https://wiki.archlinux.org/index.php/Network_configuration

<https://wiki.archlinux.org/index.php/iptables>

https://wiki.archlinux.org/index.php/Simple_stateful_firewall

https://wiki.archlinux.org/index.php/Wireless_network_configuration

https://wiki.archlinux.org/index.php/WPA_supPLICANT