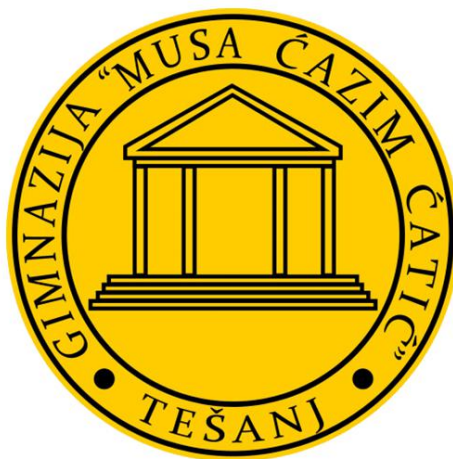


JU Gimnazija Musa Ćazim Ćatić, Tešanj
Ul. Patriotske lige br. 65
74260 Tešanj



Maturski rad iz predmeta
Računarskih mreža
Tema: Upravljanje računarskim mrežama
pod Linux OS

Učenik:
Harun Bajrić

Mentor:
prof. Estela Ramić

April 2021.godine

SADRŽAJ

SADRŽAJ	1
1. UVOD	2
2. MREŽNI RAD I LINUX	3
2.1. Mrežni rad i Linux	3
2.2. Mrežni servisi	3
3. KONFIGURISANJE LINUX MREŽNOG OKRUŽENJA	4
3.1. Potrebni servisi i programi	4
3.2. Konfiguracione datoteke	5
3.2.1. /etc/hostname i /etc/hosts	5
3.2.2. /etc/hosts.allow i /etc/hosts.deny	6
3.2.3. /etc/networks	6
3.2.4. /etc/network/interfaces	6
3.2.5. /etc/protocols	6
3.2.6. /etc/services	7
4. UPRAVLJANJE LINUX PROGRAMIMA ZA UPRAVLJANJE MREŽOM	7
4.1. Sistemske komande	7
4.1.1. ifdown, ifup, ifquery	7
4.1.2. ifconfig	7
4.1.3. netstat	8
4.1.4. arp	8
4.1.5. ping	9
4.1.6. nslookup	9
4.1.7. traceroute	10
4.1.8. whois	10
4.1.9. ss	11
4.2. Dodatne komande za upravljanje mrežom	12
4.2.1. Termshark/Wireshark	12
4.2.2. iftop	13
4.2.3. ifplugstatus	13
5. OTKRIVANJE GREŠAKA UNUTAR MREŽE	13
5.1. ip	13
5.2. nmcli	14
5.3. Host	15
5.4. ethtool	16
6. ZAKLJUČAK	17
7. IZVORI	18

1. UVOD

Današnji svijet predvođen je Linux operativnim sistemom iz razloga što je njegov Kernel pravljen kao Open-Source¹. Ovo umnogotome daje veliki značaj Linux operativnom sistemu nad ostalim, njega može bilo ko sa znanjem o programiranju i strukturi Unix operativnih sistema modifikovati prema svojim potrebama i može ga u potpunosti izmijeniti. Danas, 96.4% servera pokreće Linux operativni sistem od jednog miliona najbitnijih web servera.² Također danas je Linux jedini operativni sistem koji radi na 500 najboljih superkompjuteru svijeta (od Novembra 2017, kada su skoro svu svoju konkurenciju eliminisali).³ Jedan veliki razlog zašto je Linux na vrhu ljestvica u korištenju je to što je on lightweight⁴ i što daje izbor korisniku prilikom instalacije sistema šta će instalirati i koje verzije će čega instalirati. Iz gore navedenih razloga, u ovom radu ću detaljnije opisivati rad sa Linux OS u cilju upravljanja mreža, jer kao što smo iz navedenog vidjeli, Linux je trenutno vodeći operativni sistem za servere i za upravljanje mrežama i podacima.

¹ Open Source - softver čiji je originalni kod besplatno dostupan javnosti i može biti redistribuiran i modifikovan (Oxford Languages definicija)

² [OS Market Share and Usage Trends](#) - W3cook.com, arhivirano iz originala Augusta 6, 2015

³ Vaughan-Nichols, Steven J. (2017) [Linux totally dominates supercomputers](#), ZDNet (objavljeno Novembra 14, 2017)

⁴ Lightweight - zauzima malo prostora kao OS i ne instalira za sobom nepotrebne programe koji čine sistem sporijim i koji zauzimaju prostor.

2. MREŽNI RAD I LINUX

2.1. Mrežni rad i Linux

Za administratora računarske mreže značajne su serverske funkcije (web, mail, firewall ...), rutiranje i filtriranje paketa. Sve ove opcije nudi Linux kroz svoje server orijentirane distribucije, većina tih distribucija dolazi sa već prethodno instaliranim network paketima (npr. routed, openssh, mrouted, networkmanager), također on dolazi i sa drugim prethodno instaliranim paketima pogodnim za server administraciju (npr. Apache2, PHP, MYSQL, Docker). Kada sagledamo ovo shvaćamo zašto je način administracije olakšan pod Linux operativnim sistemom. Sam Linux sistem sa instaliranim routed (Route Daemon) ili mrouted (Multicast Route Daemon) može služiti za rutiranja paketa unutar mreže, ako imamo na to dodatno instaliran ufw (Uncomplicated Firewall) možemo filtrirati pakete i blokirati pristup.

2.2. Mrežni servisi

U multitasking operativnim sistemima, servis (daemon) je program koji se pokreće u pozadini i korisnik nad njim nema direktnu kontrolu. Mrežni servisi (daemons) prihvataju zahtjeve za uspostavljanje konekcije na određenom portu. Imena servisa su određena dokumentom /etc/services koja povezuje servis sa odgovarajućim protokolom (TCP⁵ ili UDP⁶) i odgovarajućim brojem porta⁷. Na Linux-u imamo ogroman broj mrežnih servisa koji pružaju različite usluge, oni se tradicionalno završavaju većinom na d (sshd, syslogd). U Unix okruženju, parent proces servisa je init proces. Daemon je većinom kreiran od strane nekog procesa kao njegov child process, parent process daemona se odmah prekida i daemon postaje child process init procesa. Za primjer rada jednog daemon-a koji je pokrenut na boot time-u ćemo uzeti inetd proces. Inetd proces je Internet Daemon i on je započet tokom boot time-a, kada je započet, inetd čita konfiguraciju iz /etc/inetd.conf dokumenta.

Idući su neki od tih servisa:

Httpd iz paketa Apache2 - pristup web stranicama preko http protokola

ftpd - servis za FTP zahtjeve sa udalejnog računara

sendmail - SMTP-ov daemon za slanje elektronske pošte

dhcpcd - konfigurisanje TCP/IP informacija za klijenta

inetd - prisluškuje zahtjeve za mrežnu konekciju

ntpd - Network Time Protocol daemon koji omogućava sinhronizaciju vremena putem mreže.

⁵ TCP - Transmission Control Protocol standard koji definiše kako se uspostavlja i održava mrežna komunikacija kroz koju se razmjenjuju podaci između programa. On radi sa IP-om, koji definiše kako računari šalju pakete i podatke jedni drugim.

⁶ UDP - User Datagram Protocol je komunikacijski protokol koji je korišten za omogućavanje konekcije koja toleriše gubitke u toku prenosa podataka između aplikacija. On ubrzava prijenos tako što ga započinje prije nego što strana koja prima podatke prihvati zahtjev za njima.

⁷ Broj porta - 16-bitni broj od 0 do 65535. U TCP broj 0 je rezerviran i ne može biti korišten. Često korišteni portovi su 20 (FTP), 53 (DNS), 67, 68 (DHCP), 80 (HTTP), 110 (POP3),

3. KONFIGURISANJE LINUX MREŽNOG OKRUŽENJA

3.1. Potrebni servisi i programi

Za upravljanje mrežom pod Linux operativnim sistemom nam treba par programa koji su esencijalni, da bismo odradili mapiranje mreže potreban nam je open-source software pod nazivom opennms⁸. Da bismo instalirali opennms na Debian based distribuciji potrebno nam je Oracle Java 8 okruženje instalirano, PostgreSQL 9.1 ili iznad te verzije, potom pratimo uputstva kao na Slici 1.

```
1 # Postupak instalacije opennms-a pod Debianom koristeći Bash shell
2 |
3 deb http://debian.opennms.org ${snapshot} main
4 deb-src http://debian.opennms.org ${snapshot} main
5 wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY | apt-key add -
6 apt-get update
7 apt-cache show opennms
```

Slika 1. - Postupak instalacije opennms programa

Testirano na: <https://cocalc.com/doc/terminal.html>

Još jedan jako koristan program je Wireshark koji služi za nadgledanje protokola i mrežnog protoka. Na Slici 2. prikazan je metod instalacije Wireshark pod Debian based distribucijama.

```
root@linuxhint:/# apt install wireshark -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  analog apache2-data
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  wireshark
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 50.2 kB of archives.
After this operation, 64.5 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 wireshark amd64 2.6.8-1.1 [
50.2 kB]
Fetched 50.2 kB in 0s (117 kB/s)
Selecting previously unselected package wireshark.
(Reading database ... 357411 files and directories currently installed.)
Preparing to unpack .../wireshark_2.6.8-1.1_amd64.deb ...
Unpacking wireshark (2.6.8-1.1) ...
Setting up wireshark (2.6.8-1.1) ...
root@linuxhint:/#
```

Slika 2. - Postupak instalacije Wireshark programa

Izvor: https://linuxhint.com/install_wireshark_debian/ (pregledano 29.03.2021.)

Potom su nam potrebni programi koji u većini Linux distribucija dolaze već instalirani, a to su ifconfig, netstat, arp, ping, traceroute... U idućem dijelu teksta ću detaljno objasniti korištenje ovih programa.

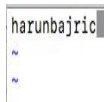
⁸OpenNMS je software za mapiranje mreža i upravljanje mrežom, više o njemu na <https://www.opennms.com>

3.2. Konfiguracione datoteke

Administratori mreže mogu konfigurirati mrežno okruženje ručnom izmjenom konfiguracionih datoteka. Prvobitne konfiguracije su automatski generirane nakon instalacije sistema u direktoriju /etc. No, međutim, često dolazi do potrebe za izmjenom i podešavanjem konfiguracionih datoteka. Kako se na serverima ne koristi grafičko okruženje (zbog sigurnosti i zbog toga što bi samo grafičko okruženje zauzelo prostor potreban za ostale stvari) potrebno je da se znamo koristiti sa jednim od uređivača teksta koje Linux nudi (Vim, Vi, Nano). Svi ovi uređivači teksta dolaze već prethodno instalirani na svakoj distribuciji za servere. Da bismo ove dokumente uređivali moramo biti super-user, to jeste moramo imati root pristup.

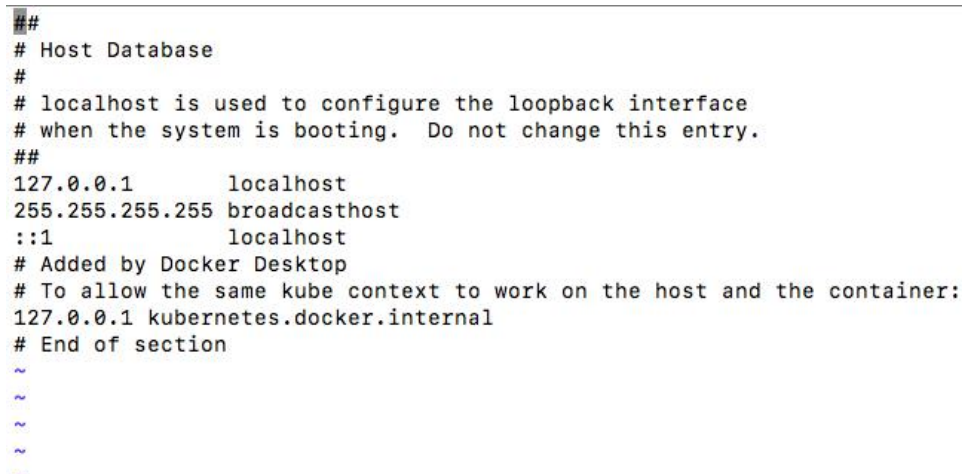
3.2.1. /etc/hostname i /etc/hosts

U datoteci /etc/hostname postoji ime računara koje je već generirano po želji sistem administratora prilikom instalacije servera. Ovo ime je ime računara po kojem je on prepoznatljiv unutar računarske mreže. U datoteci /etc/hosts, u formi tabele, osim imena računara nalaze se i sva imena dodijeljena odgovarajućim IP adresama. Na slici 3. je prikazan dokument /etc/hostname u Vim tekstualnom editoru na OSX operativnom sistemu, a na slici 4. je prikazan /etc/hosts dokument na OSX operativnom sistemu. Na slici 5. nalazi se shema kako možemo sami napraviti svoj /etc/hosts dokument i modifikovati ga. Na slici 5. vidimo da nam je za /etc/hostnames potrebna IP adresa računara koji je u mreži, hostname je nepotreban ali poželjan jer ga je lakše prepoznati unutar mreže, na kraju svega nam treba alias koji je zapravo domena koju koristimo na internetu za taj server, ako nemamo domen u možemo upisati IP adresu.



```
harunbajric
```

*Slika 3. /etc/hostname datoteka
Testirano na UNIX-based sistemu
OSX*



```
##  
# Host Database  
#  
# localhost is used to configure the loopback interface  
# when the system is booting. Do not change this entry.  
##  
127.0.0.1        localhost  
255.255.255.255 broadcasthost  
::1             localhost  
# Added by Docker Desktop  
# To allow the same kube context to work on the host and the container:  
127.0.0.1 kubernetes.docker.internal  
# End of section  
~  
~  
~  
~  
~
```

*Slika 4. - /etc/hosts datoteka
Testirano na UNIX-based sistemu OSX*

```
# /etc/hostnames

IPAddress      Hostname      Alias
127.0.0.1      localhost.myDomain.com
208.164.186.1  email.myDomain.com
208.164.186.2  web.myDomain.com
208.164.186.3  cpanel.myDomain.com
```

*Slika 5. - prikaz sheme za /etc/hostnames
Testirano na UNIX-based sistemu OSX*

3.2.2. /etc/hosts.allow i /etc/hosts.deny

Ove dvije datoteke definišu kojim je računarima dozvoljen pristup mreži, to jeste sistemu, odnosno kojim je računarima zabranjen pristup. Pisanje ova dva dokumenta imaju svoje norme i imaju neke svoje ključne riječi koje možemo pronaći na <https://linux.die.net/man/5/hosts.allow> (pregled 29.03.2021). i na <https://linux.die.net/man/5/hosts.deny> (pregled 29.03.2021).

3.2.3. /etc/networks

Slično datoteci /etc/hosts, na Linux serverima postoji datoteka /etc/networks u kojoj se čuvaju podaci sa imenima računarskih mreža i IP adrese mreže. Na slici 6. imamo prikaz dokumenta /etc/networks.

```
#route
Kernel IP routing table
Destination      Gateway          Genmask          Flags      Metric  Ref    Use    Iface
default          192.166.1.252   0.0.0.0          UG         0       0      0      eth0
myLocalNet       *               255.255.254.0    U          0       0      0      eth0
```

*Slika 6. - Prikaz /etc/networks dokumenta
Testirano na UNIX-based sistemu OSX*

3.2.4. /etc/network/interfaces

Konfiguraciona datoteka koja se kreira pri samom podizanju sistema, i u njoj su opisane mrežne kartice koje su prisutne na sistemu trenutno. U ovom dokumentu se definiše preko koje kartice i kako se naša mašina povezuje na mrežu, ovdje su prikazana imena kartica, njihove adrese, netmaske, gateways i broadcast.

3.2.5. /etc/protocols

Ovaj dokument sadrži informacije vezane za poznate protokole koji su korišteni. Za svaki protokol imamo jednu liniju informacija koja glasi kao slijedeće:
oficijelno_ime_protokola broj_protokola aliasi_protokola.

3.2.6. /etc/services

Ova datoteka sadrži servise i portove na kojima ti servisi pružaju usluge. Sama datoteka izgleda kao tabela, prva kolona je ime servisa, druga broj porta i protokol (TCP ili UDP). Nakon toga slijedi alternativni naziv servisa. Na UNIX sistemima imamo raspon portova koji su poznati kao “trusted ports”, ti portovi su u rasponu od 0-1023. UNIX sistemi zahtijevaju da je korisnik super-user i da ima root access da pristupi ovim portovima radi sigurnosti, ukoliko ovo nije omogućeno, obični korisnik povezan na mrežu može pristupiti portu 23, koji je standard za telnet server, onda preko toga taj korisnik može primiti zahtjeve za povezivanje od korisnika i uzimati njihove šifre, kompromišući sigurnost cijelog sistema. Iz ovog razloga je bitno koristiti “trusted ports” u ovom dokumentu, da osoba koja nije administrator ne može pristupiti tim portovima niti ih može prisluškivati.

4. UPRAVLJANJE LINUX PROGRAMIMA ZA UPRAVLJANJE MREŽOM

Linux posjeduje već ugrađene programe koji mu omogućavaju da na efikasan način upravlja mrežom. U ovom radu će biti spomenute pojedine komande koje su ključne za administratora mreže, te komande su za pregled mrežne kartice (ifconfig), da li se routing ispravno vrši (netstat), da li sistem koji se promatra može slati i primiti podatke (ping i traceroute). Neke od programa potrebno je i instalirati putem terminala jer ne dolaze instalirane sa samim serverom.

4.1. Sistemske komande

Sistemske komande su sve one koje su dostupne od momenta kada po prvi put uđemo na novu instalaciju servera. Ove komande pomažu nam da uspostavimo mrežu i da je konfigurišemo prema svojim potrebama, one nam također nagovještavaju na greške u konfiguraciji mreže ili greške u prijenosu podataka.

4.1.1 ifdown, ifup, ifquery

Komande ifdown, ifup, ifquery se koriste za manipulaciju mrežne kartice. Ifup komanda pokreće mrežnu karticu, čineći ju dostupnom za slanje i primanje podataka. Ifdown komanda radi suprotno, ona gasi mrežnu karticu i skida je sa mreže. Ifup i ifdown mogu biti korištene da se konfigurišu mrežne kartice koje su definirane u dokumentu /etc/network/interfaces. Ifquery naredba prikazuje informacije o mrežnoj kartici i njenoj konfiguraciji.

4.1.2. ifconfig

Ovo je komanda koja se često koristi. Ona se koristi za konfiguraciju mrežnih kartica i omogućava postavljanje parametara: IP adresa, maska mreže, broadcast adresa. Može se prikazati i trenutna konfiguracija kao što je prikazano na slici 7. Ova komanda se koristi za dijagnostiku mreže nakon što je server pokrenut, a prilikom pokretanja se koristi za namještanje mrežnih kartica.


```
|192:~ harunbajric$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
EHC253: flags=0<> mtu 0
EHC250: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
    ether 40:6c:8f:00:13:2e
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (none)
    status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 68:a8:6d:4b:7b:d4
    inet6 fe80::1840:b988:a12d:de2a%en1 prefixlen 64 secured scopeid 0x7
    inet 192.168.1.9 netmask 0xffffffff broadcast 192.168.1.255
    inet6 2a02:27b0:4b02:aaf0:105d:b625:85b1:1438 prefixlen 64 autoconf secured
    inet6 2a02:27b0:4b02:aaf0:b580:8544:7d87:ba7a prefixlen 64 autoconf temporary
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
```

*Slika 7. - ispis ifconfig komande
Testirano na UNIX-based sistemu OSX*

4.1.3. netstat

Ova komanda je dijagnostički alat koji koriste administratori računarske mreže da dobiju detaljne izvještaje o mrežnim karticama, tabelama rutiranja, mrežnim konekcijama, statistikama korištenja raznih mrežnih protokola. Sve ove informacije pomažu administratoru da uspješno uoči i otkloni probleme unutar sistema. Ova komanda posjeduje brojne funkcije koje su jako korisne, o njima možemo pročitati više u man stranicama⁹.

4.1.4. arp¹⁰

Arp komanda manipulira i prikazuje sadržaj arp tabele koja sadrži podatke o imenima računara u mreži i njihove MAC adrese. Na slici 8. imamo prikazano korištenje arp komande. Najčešće se koristi za dinamično mapiranje mrežnih adresa trećeg sloja na adresu data-link sloja. ARP predmemorija je jako ranjiva i stoga trebamo paziti kada koristimo ovu komandu jer je lahko da dođe do ARP poisoning i do ARP spoof attack. Zbog ovoga sistem administrator ne bi trebao dozvoliti običnim korisnicima pristup ARP komandi jer onda svaki korisnik može biti u žiži svih komunikacija i sa lahkoćom može sve da sazna.

⁹ Linux ima svoje man stranice koje daju informacije o programu ili komandi. Potrebno je samo da upišemo man ime_komande.

¹⁰ Adress Resolution Protocol

```
192:~ harunbajric$ arp -a
csp1.zte.com.cn (192.168.1.1) at 50:78:b3:da:79:cc on en1 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en1 ifscope permanent [ethernet]
```

Slika 8. - ispis arp komande
Testirano na UNIX-based sistemu OSX

4.1.5. ping

Ova komanda prosljeđuje ICMP ECHO_REQUEST¹¹ paket ka ciljnom čvoru mreže. Na osnovu dobijenog izvještaja, administrator može da zaključi da li je ciljani čvor dostupan ili ne. Također, ovom komandom administrator može utvrditi kakvo je stanje računarske mreže i gdje dolazi do prekida u funkcionisanju te iste mreže. Ova komanda je korisna no može biti ranjiva za sistem ako čvorovi dozvoljavaju ICMP ECHO_REQUEST. Ukoliko je dozvoljen pristup čvoru zlonamjerni korisnik može poslati veliki broj ping paketa na neki čvor mreže i izazvati pad tog čvora. Na slici 9. je prikazan ispis ping komande.

```
192:~ harunbajric$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=111 time=36.468 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=38.023 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=39.962 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=64.273 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=42.948 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=38.134 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=37.499 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=111 time=73.005 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 36.468/46.289/73.005/13.214 ms
192:~ harunbajric$
```

Slika 9. - ispis ping komande
Testirano na UNIX-based sistemu OSX

4.1.6. nslookup

Komandom nslookup (name server look up) šalje se zahtjev DNS serveru da na osnovu imena čvora vrati IP adresu tog čvora. Na slici 10. imamo prikaz ispisa nslookup komande za provjeravanje informacije o website-u.

¹¹ ICMP (Internet Control Message Protocol) je jedan od protokola na TCP/IP-u. ICMP echo request i ICMP echo su poznati kao ping poruke koje šalju informacije o čvorovima i o mreži.

```

[192:~ harunbajric$ nslookup harunbajric.xyz
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   harunbajric.xyz
Address: 18.159.128.50
Name:   harunbajric.xyz
Address: 206.189.58.26

192:~ harunbajric$ █

```

*Slika 10. - provjeravanje informacija o website-u koristeći nslookup
Testirano na UNIX-based sistemu OSX*

4.1.7. traceroute

Komandom traceroute daje izvještaj administratoru mreže o putanji paketa do ciljanog čvora mreže. Najčešće se koristi za odredbu mjesta čvora gdje je došlo do prekida u komunikaciji između izvorne i odredišne adrese ukoliko je odredišni čvor nedostupan.

```

192:~ harunbajric$ traceroute daria.ba
traceroute to daria.ba (168.119.149.198), 64 hops max, 52 byte packets
 1 csp3.zte.com.cn (192.168.1.1)  1.720 ms  2.147 ms  0.958 ms
 2 100.80.0.1 (100.80.0.1)  16.913 ms  15.594 ms  16.451 ms
 3 10.100.199.21 (10.100.199.21)  18.613 ms  17.829 ms  17.847 ms
 4 10.100.199.21 (10.100.199.21)  15.895 ms *  19.166 ms
 5 185.12.77.109 (185.12.77.109)  19.766 ms  23.286 ms  19.012 ms
 6 bhtelecom-ic335909-zgb-b1.ip.twelve99-cust.net (213.248.81.41)  19.854 ms  18.263 ms  18.609 ms
 7 zgb-b1-link.ip.twelve99.net (80.239.195.34)  24.242 ms
   zgb-b1-link.ip.twelve99.net (62.115.155.106)  27.783 ms
   zgb-b1-link.ip.twelve99.net (213.248.81.40)  27.140 ms
 8 zgb-b2-link.ip.twelve99.net (62.115.122.173)  28.066 ms  28.763 ms  26.513 ms
 9 win-bb4-link.ip.twelve99.net (62.115.122.176)  46.840 ms  45.829 ms  46.551 ms
10 ffm-bb2-link.ip.twelve99.net (62.115.138.22)  46.344 ms  46.740 ms
   ffm-bb1-link.ip.twelve99.net (62.115.137.202)  50.906 ms
11 ffm-b5-link.ip.twelve99.net (62.115.114.89)  48.878 ms  45.385 ms  48.106 ms
12 hetzner-ic326013-ffm-b5.ip.twelve99-cust.net (213.248.70.3)  64.670 ms  52.535 ms  50.704 ms
13 core24.fsn1.hetzner.com (213.239.224.253)  56.213 ms
   core23.fsn1.hetzner.com (213.239.224.249)  53.741 ms
   core24.fsn1.hetzner.com (213.239.224.253)  55.487 ms
14 ex9k1.dc16.fsn1.hetzner.com (213.239.229.218)  51.479 ms  53.208 ms  53.503 ms

```

*Slika 11. - traceroute na stranicu daria.ba
Testirano na UNIX-based sistemu OSX*

4.1.8. whois

Komandom whois provjeravamo informacije o umreženom korisniku ili domeni na internetu. Ova komanda nam može pomoći u informisanju o korisniku u mreži i kako bismo mogli lakše otkloniti kvar. Na slici 12. je prikazano korištenje whois domene na webstranicu linije.ba koristeći IP adresu te stranice, a ne domenu.


```

192:~ harunbajric$ whois 195.130.35.3
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:          whois.ripe.net

inetnum:        195.0.0.0 - 195.255.255.255
organisation:    RIPE NCC
status:          ALLOCATED

whois:          whois.ripe.net

changed:        1993-05
source:          IANA

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '195.130.32.0 - 195.130.47.255'

% Abuse contact for '195.130.32.0 - 195.130.47.255' is 'abuse@utic.ba'

inetnum:        195.130.32.0 - 195.130.47.255
netname:         UTIC_UNSA_195_130_32
descr:           Used by University of Sarajevo
country:         BA
admin-c:         CS14166-RIPE
tech-c:          EH3721-RIPE

```

*Slika 12. - prikaz whois komande na IP adresi 195.130.35.3.
Testirano na UNIX-based sistemu OSX*

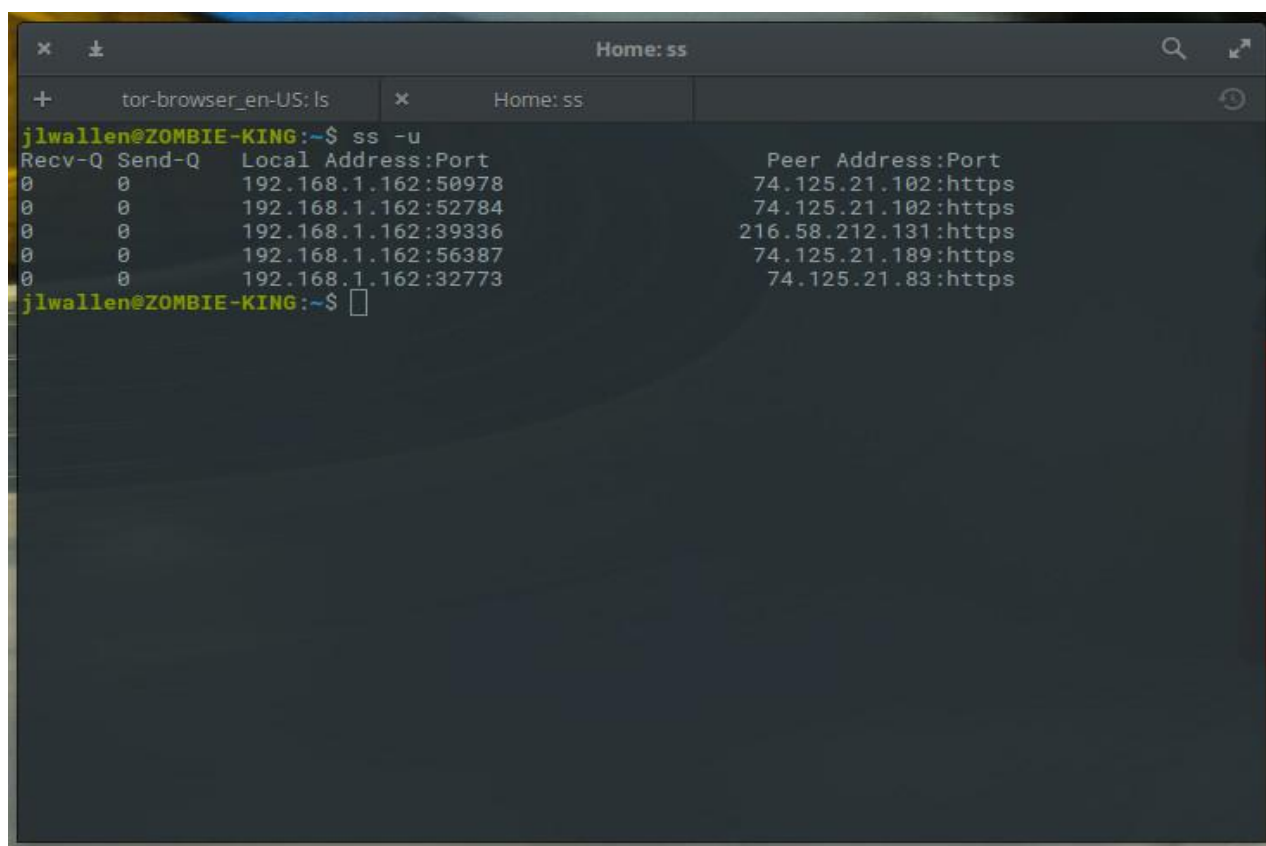
4.1.9. ss

Komanda ss je potpuno ista kao netstat komanda, međutim, zbog brzine i većeg broja informacija koju nudi ova komanda je veći favorit kod administratora mreža. Brzina ss je omogućena time što on sve informacije prikuplja direktno iz kernelovog userspace-a. Ova komanda također može prikazati informacije vezane za TCP, UDP, DCCP¹², RAW¹³ i Unix-ove domain socket-e¹⁴.

¹² DCCP - Datagram Congestion Control Protocol message-oriented transport layer protokol koji implementira siguran setup konekcije.

¹³ RAW je protokol za sisteme koji ne koriste standardni TCP/IP, on je poznat kao Port 9100. Ovaj protokol šalje podatke bez da ih dalje procesira.

¹⁴ Unix domain socket - ovo predstavlja krajnju tačku u podatkovnoj komunikaciji za razmjenu podataka između procesa na istoj mreži.



```
jllwallen@ZOMBIE-KING:~$ ss -u
Recv-Q Send-Q Local Address:Port Peer Address:Port
0      0      192.168.1.162:50978 74.125.21.102:https
0      0      192.168.1.162:52784 74.125.21.102:https
0      0      192.168.1.162:39336 216.58.212.131:https
0      0      192.168.1.162:56387 74.125.21.189:https
0      0      192.168.1.162:32773 74.125.21.83:https
jllwallen@ZOMBIE-KING:~$
```

Slika 13. prikaz ss komande

Izvor: <https://www.linux.com/topic/networking/introduction-ss-command/>

4.2. Dodatne komande za upravljanje mrežom

Razni stručnjaci i administratori mreža su uvidjeli manjkavosti u sistemskim komandama (manjak informacija, poteškoće pri korištenju, spor execution time), zbog toga su oni počeli razvijati svoje programe za servere koji pružaju mnoštvo mogućnosti jednom administratoru. Većina ovih komandi je easy-to-install na UNIX based sistemima, dok ako koristimo Windows server moramo proći kroz neke teže korake.

4.2.1. Termshark/Wireshark

Wireshark je program za koji nam treba grafičko okruženje da bismo ga pokrenuli, iz tog razloga većina administratora mreže preferira alternativu ovom naprednom programu, Termshark, koji se pokreće unutar konzole i preko njega možemo manipulirati i nadgledati mrežu baš kao iz Wireshark-a. Wireshark je alatka za analizu paketa u mreži, danas ga većina administratora koristi da bi brže pronašli probleme unutar mreže i da nadgledaju sigurnost iste.

4.2.2. iftop

Iftop naredba se koristi za nadgledanje mrežnog saobraćaja. Ova naredba ne dolazi ugrađena u sistem i moramo ju instalirati posebno prateći komande koje su istaknute na slici 14.

```
wget http://www.ex-parrot.com/pdw/iftop/download/iftop-0.17.tar.gz
tar zxvf iftop-0.17.tar.gz
cd iftop-0.17
./configure
make
make install
```

*Slika 14. - instalacija iftop naredbe na UNIX-based sistemima
Testirano na UNIX-based sistemu OSX*

4.2.3. ifplugstatus

Komanda ifplugstatus se koristi da bismo provjerili da li je kabal povezan sa mrežnom karticom, ova komanda nije prisutna u osnovnom paketu no možemo je instalirati preko apt menadžera na Debian based distribucijama.

5. OTKRIVANJE GREŠAKA UNUTAR MREŽE

Otkrivanje grešaka unutar mreže je krucijalan zadatak koji svaki administrator mreže mora znati, ovaj zadatak znači da će naša mreža uvijek biti sigurna i da ćemo uvijek znati šta se dešava unutar naše mreže. Ovaj zadatak može biti jako izazovan, no srećom, postoji niz komandi koji nam pomažu u tome i koje nam mogu brzo i efikasno ukazati na grešku.

5.1. ip

Ip komanda je novija komanda unutar UNIX based sistema i ona mijenja stari “bundle” komandi pod nazivom net-tools¹⁵. Ova komanda dodaje još više mogućnosti nego “bundle” net-tools, preko ip komande možemo vidjeti IP adresu, MAC adresu mrežne kartice, možemo manipulirati IP adrese unutar mreže, kontrolirati status mrežne kartice (tj. odrediti da li će ona biti korištena ili ne), možemo obavljati routing uz pomoć ove komande te možemo kontrolirati arp tabele. Na slici 15. imamo prikaz korištenja ip komande uz njene najbitnije i najkorisnije tagove, -s i -h, -s tag prikazuje statistiku mreže u čitkoj formi, a -h određuje mrežnu karticu.

¹⁵ Net-tools je skup komandi koje dolaze već instalirane na UNIX sistemima, a to su ifconfig, route i arp komande koje smo već spominjali u ovom tekstu.

```
$ ip -s -h 1 show dev enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:b5:c7:2b brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    820M      303k      0       182k      0         0
    TX: bytes  packets  errors  dropped carrier collsns
    19.9M      60.9k      0         0         0         0
```

Slika 15. prikaz korištenja ip komande

Izvor: <https://www.redhat.com/sysadmin/five-network-commands> (pregled 30.03.2021.)

5.2. nmcli

Nmcli je komanda koja dolazi u paketu Network Manager. Paket Network Manager je do sada najpouzdaniji i najbolji paket koji se ponaša kao “daemon”, ovaj paket čini konfiguraciju i nadgledanje mreže lakšim i bržim, unutar ovog paketa sve je automatizovano. Ovaj paket nudi i svoj GUI program, no iz razloga što radimo na serverima, većinom ćemo koristiti servere bez grafičkog okruženja i zato ćemo više puta koristiti nmcli koji je Network Manager-ov program za CLI. Putem nmcli možemo kreirati, brisati, aktivirati, deaktivirati konekcije unutar mreže, također možemo kontrolisati mrežne kartice i prikazivati ih. Putem ove komande možemo vidjeti koja kartica ima pristup mreži, a koja ne.

5.3. dig

Dig (Domain Information Groper) je komanda za prikaz DNS name server-a. Dig naredba nam omogućava da prikažemo razne DNS informacije. Putem dig komande možemo saznati da li možemo pristupiti određenom serveru ili određenoj IP adresi, te koja je brzina konekcije, ovo je ključno za administratore mreže jer ako dig pokaže da je konekcija timeout-ovana znači da negdje u mreži postoji problem. Na slici 16. imamo prikaz ispisa dig komande kada pokušamo dobiti informacije o webstranici linije.ba.


```

192:~ harunbajric$ dig www.linije.ba

; <<>> DiG 9.10.6 <<>> www.linije.ba
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51375
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.linije.ba.                IN      A

;; ANSWER SECTION:
www.linije.ba.                14400   IN      CNAME   linije.ba.
linije.ba.                    14400   IN      A       136.243.76.141

;; Query time: 96 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Sun Apr 04 23:07:59 CEST 2021
;; MSG SIZE rcvd: 72

```

*Slika 16. - prikaz ispisa dig komande
Testirano na UNIX based sistemu OSX*

5.3. Host

Host komanda je jedna od najkorisnijih komandi koje se nalaze u okviru otkrivanja greški, ukoliko imamo sistem unutar jedne firme i želimo saznati ko je iza IP adrese 109.175.99.4 tu će nam pomoći host komanda, host komanda također radi i na drugi način, da unesemo ime korisnika i saznamo njegov IP. Na slici 17. imamo prikaz korištenja host metode bez -t taga i sa -t tagom. Tag -t nam omogućava da prikazemo DNS podatke poput CNAME, NS, MX, SOA itd.

```

192:~ harunbajric$ host linije.ba
linije.ba has address 136.243.76.141
linije.ba mail is handled by 0 linije.ba.
192:~ harunbajric$ host -t CNAME www.linije.ba
www.linije.ba is an alias for linije.ba.
192:~ harunbajric$

```

*Slika 17. korištenje host naredbe
Testirano na UNIX based sistemu OSX*

5.4. ethtool

Ethtool je komanda koju većina administratora koristi za podešavanje i za prikaz konfiguracije mrežne kartice. Ova komanda je korisna za dijagnosticiranje Ethernet uređaja, kontroliranje brzine i nadgledanje putanje paketa. Koristeći ovaj paket možemo podešavati maksimalnu brzinu uređaja što nam može omogućiti raspoređivanje resursa unutar mreže. Putem ethtool-a možemo odrediti koji duplex će naša mrežna kartica koristiti. Jedan uređaj može biti full duplex, half duplex i auto-negotiation. Full duplex nam omogućava slanje i primanje paketa istovremeno, ovo se koristi kada je uređaj povezan sa switch-em. Half duplex nam samo daje slanje ili primanje podataka u datom momentu. Ovo se koristi kada je uređaj povezan na hub. Auto-negotiation je najsigurnija opcija od svih jer ona daje uređaju da odlučuje da li će koristiti half duplex ili full duplex, uređaj to odlučuje na osnovu toga na što je povezan. Ovo je dobro jer se može desiti da ćemo promijeniti uređaj na koji povezujemo mrežnu karticu, onda bismo i konfiguraciju mrežne kartice morali mijenjati što možemo izbjeći koristeći auto-negotiation.

```
# ethtool eth0

Settings for eth0:

    Current message level: 0x00000007 (7)
    Link detected: yes
```

Slika 18. Ethtool dijagnostika nad eth0 mrežnim uređajem

Izvor: <https://www.tecmint.com/linux-network-configuration-and-troubleshooting-commands/>
(pregled 30.03.2021.)

6. ZAKLJUČAK

Ukoliko sve sagledamo objektivno i realno, upravljanje mrežama i konfigurisanje mreža je jedna od težih stvari koje administrator sistema može raditi, no međutim, Linux i UNIX based operativni sistemi olakšavaju tu situaciju sa svojim ugrađenim komponentama i ugrađenim programima. Oni daju sigurnost, brzinu i lakhoću korištenja koja je neprisutna na ostalim operativnim sistemima za server administraciju. Također, iz ovog svega navedenog možemo uvidjeti da je za administraciju mreža potrebno teoretsko poznavanje strukture mreža ali i praktično poznavanje Unix sistema i Linuxovog kernela za rad sa mrežama i sa mrežnim karticama. Iz ovog svega uviđamo da je Linuxov kernel najpouzdaniji za rad sa mrežama i serverima jer nam nudi potpunu moć nad sistemom i potpunu sigurnost već ugrađenu u sistem.

7. IZVORI

<https://www.redhat.com/sysadmin/>

<https://man7.org/linux/man-pages/>

<https://linux.die.net/man/>

<https://github.com/crhuber/linux-cheatsheet#networking>

<https://web.archive.org/web/20150806093859/http://www.w3cook.com/os/summary/>

<https://linux.die.net/man/5/hosts.allow>

TEMA: Upravljanje računarskim mrežama pod Linux OS

KOMENTAR:

Komisija:

Predsjednik: _____

Ispitivač: _____

Član: _____

Datum: _____

Ocjena: _____ ()