Lab 1: Osnovni mrežni alati u Linux-u

Cilj ove laboratorijske vježbe je upoznavanje sa važnim softverskim alatima za upravljanje mrežnom konfiguracijom u Linux operativnom sistemu.

Kada konfigurišete i upravljate računarskom mrežom ili dijagnostikujete probleme u mreži, morate da koristite odgovarajuće alate. Najčešće su ovi alati softverske aplikacije. Postoji veći broj alata koji su dostupni na većini računara, a koji se mogu koristiti za uobičajene zadatke umrežavanja kao što su:

- Pregled i promjena konfiguracije mrežnog interfejsa računara, na primer IP adrese i parametara protokola;
- Testiranje mrežne konektivnosti, tj. mogućnosti povezivanja sa drugim računarima;
- Analiza saobraćaja koji šalje/prima vaš računar ili neki drugi računar u mreži.

Alati koji se mogu koristiti za upravljanje mrežom razlikuju se na različitim operativnim sistemima. Na primjer, alati na Microsoft Windows-u se razlikuju od onih na Unix-ovim verzijama operativnog sistema kao što su Ubuntu i Apple MAC OS. Iako se programi mogu razlikovati (uključujući interfejs i opcije), većina njih pruža sličan nivo funkcionalnosti. Stoga, nakon što naučite funkcionalnost pomoću jednog alata, neće vam biti teško izvršiti istu funkciju pomoću drugog.

Za realizaciju ove lab vježbe koristićemo Ubuntu operativni sistem. Ovaj operativni sistem je odabran jer se Linux danas dominantno koristi na web serverima, a pored toga čini i osnovu operativnog sistema rutera i brojnih drugih mrežnih uređaja.

Pregled osnovnih komandi u Linux-u

cd promjena radnog direktorijuma

ls izlistava fajlove u direktorijumu

man pregled dokumentacije za korišćenje komande

cp kopira fajl

mv premješta/preimenuje fajl

rm brisanje fajla

less prikaz sadržaja fajla

cat prikaz sadržaja fajla

echo prikazuje tekst na ekranu (standardni izlaz)

pwd prikazuje apsolutnu putanju radnog direktorijuma

wc prikazuje broj linija, riječi i bajtova u fajlu

> preusmjerava izlaz u fajl

< prusmjerava fajl na ulaz

ps izlistava trenutno pokrenute procese

& izvršava program u pozadini (*background* proces)

Ctrl-c stopira (ubija) trenutno aktivni proces

Ctrl-z obustavlja trenutno aktivni process

bg pokreće obustavljeni proces u pozadini

fg pokreće obustavljeni proces *foreground*

Primjer korišćenja osnovnih Linux komandi:

```
$ pwd
/home/sgordon
$ mkdir test
$ cd test
$ pwd
/home/sgordon/test
$ nano example.txt # use the text editor to write 'Hello, my name is Steve.'
$ cat example.txt
Hello, my name is Steve.
$ ls
example.txt
$ ls -l
total 4
-rw-r--r-- 1 sgordon sgordon 25 2009-11-06 16:34 example.txt
$ wc example.txt
 1  5 25 example.txt
$ cp example.txt copy-of-example.txt
$ ls
copy-of-example.txt example.txt
$ rm example.txt
$ ls
copy-of-example.txt
$ mv copy-of-example.txt example.txt
```

```
$ ls
example.txt
$ rm example.txt
$ ls
$ ls -al
total 12
drwxr-xr-x 2 sgordon sgordon 4096 2009-11-06 16:36 .
drwxr-xr-x 75 sgordon sgordon 8192 2009-11-06 16:33 ..
$ echo 'Hello'
Hello
$ echo 'Hello' > another-example.txt
$ cat another-example.txt
Hello
$ wc another-example.txt
1 1 6 another-example.txt
$ rm another-example.txt
$ ls
$ cd ..
$ rmdir test
```

Editovanje teksta i koda:

Dva standardna editora za Linux sisteme su:

- gedit: GUI editor
- nano: koristi se iz komandne linije

Instalacija softvera

Ubuntu ima jednostavan CLI (*Command Line Interface*) za instalaciju softvera. Instalacija softverskog paketa vrši se na sledeći način:

```
$ apt install paket
```

gdje je *paket* naziv softverskog paketa koji se želi instalirati. Naravno, za izvršavanje ove komande neophodne su administratorske privilegije (**sudo**).

Pregled i konfiguracija mrežnih parametara

Računar se povezuje na LAN (*Local Area Network*) preko jedne od svojih mrežnih kartica (*Network Interface Cards* – NICs). Skoro svi operativni sistemi dozvoljavaju korisniku da vidi informacije o aktivnim mrežnim karticama, uključujući:

- MAC (ili hardversku) adresu
- IP adresu i *subnet* masku

- Adrese važnih čvorišta (servera) u mreži
- Saobraćaj koji se šalje/prima preko NIC

Operativni sistemi takođe često dozvoljavaju administrator da mijenja neke od ovih parametara.

Ključna komanda koja omogućava pregled i mijenjanje parametara mrežnih interfejsa je **`ifconfig`**. Za pregled informacija o svim mrežnim interfejsima koristi se u osnovnom obliku:

```
$ ifconfig
```

Operativni sistem dodjeljuje ime svakom interfjesu, npr **eth0** za prvu Ethernet NIC i **eth1** za drugu. S obzirom da se dodjela imena/broja vrši automatski, ne može se pretpostaviti da će se isti nazivi dodjeliti mrežnim karticama kada se one koriste na drugim računarima. Među izlistanim interfjesima možete primijetiti i **loopback** interfejs kojem je dodijeljen naziv **lo**. Ovaj interfejs nije fizički već virtuelni, implementiran u softveru. Za pregled informacija o specifičnom interfejsu, npr. **eth0**, koristi se sledeći oblik komande:

```
$ ifconfig eth0
```

Kada je mrežni interfjes aktivan, on može da šalje i prima podatke. Kada je neaktivan ne može da prima i šalje podatke. Komanda **`ifconfig`** se može koristiti za promjenu statusa mrežnog interfejsa iz aktivnog u neaktivno i obrnuto. Za aktiviranje interfejsa (npr. **eth0**) koristi se komanda.

```
$ sudo ifconfig eth0 up
```

Na sličan način moguće je deaktivirati interfejs:

```
$ sudo ifconfig eth0 down
```

`ifconfig` komanda se može koristiti i za konfigurisanje mrežnog interfejsa. Ovo je često nepotrebno jer se konfiguracija obično automatski očitava preko posebne skripte prilikom podizanja sistema. Ukoliko ipak želite da to uradite manuelno, potrebne su vam *root* privilegije, tj. morate ukucati **sudo** prije unosa komande.

Za dodjelu statičke adrese interfejsu može se koristiti komanda:

```
$ sudo ifconfig naziv_interfejsa ip_adresa
```

Na sličan način konfiguriše se i *subnet* maska:

```
$ sudo ifconfig naziv_interfejsa netmask subnet_maska
```

Prethodne dvije komande je moguće spojiti u jednu. Na primjer, ukoliko želimo da **eth0** interfjesu dodijelimo IP adresu 192.168.0.2 i subnet masku 255.255.255.0, to možemo uraditi komandom:

```
$ sudo ifconfig eth0 192.168.0.2 netmask 255.255.255.0
```

Testiranje mrežne konektivnosti

Ispitivanje konektivnosti, tj. mogućnosti komunikacije jednog računara sa drugim, obično se sprovodi korišćenjem ICMP (*Internet Control Message Protocol*) protokola. Korisnička aplikacija koja implementira ovaj protokol za potrebe testiranja konektivnosti je **`ping`**. **`Ping`** šalje poruke (pakete) sa klijentskog računara prema nekom destinacionom računaru koji zatim šalje poruke odgovora. **Ping** mjeri vrijeme potrebno za slanje paketa do destinacije i nazad (RTT), kao i broj poslatih i izgubljenih paketa. Najednostavniji način korišćenja ove aplikacije je:

```
$ ping destinacija
```

gdje je *destinacija* IP adresa ili naziv domena računara prema kojem se konektivnost testira. Izvršavanje komande se može prekinuti sa **Ctrl-C**. Broj paketa koji se šalju moguće je ograničiti pomoću opcije **-c**:

```
$ ping -c broj destinacija
```

Za testiranje mrežne konektivnosti često se koristi i **`traceroute`** aplikacija. Ova aplikacija otkriva nam preko kojih rutera se poslate poruke prenose do destinacije. Kao i kod **ping** aplikacije, pošiljalac šalje ICMP pakete prema destinaciji, koja zatim odgovara na svaki primljeni paket. Međutim, kod *traceroute* aplikacije svaki ruter na ruti takođe odgovara na pakete pošiljaoca. Aplikacija se pokreće komandom:

```
$ traceroute destinacija
```

Na Windows-u slična aplikacija se pokreće komandom **tracert**.

Konverzija između IP adresa i domenskog imena

Za konvertovanje domenskog imena u IP adresu koristi se DNS protokol. Takođe, moguće je izvršiti i konverziju IP adrese u domensko ime (tzv. obrnuti DNS). Ubuntu posjeduje više alata za korišćenje DNS funkcionalnosti. U ovoj lab vježbi korističemo **`nslookup`**[1] komandu. Princip

[1] Alternativne komande su **dig** i **host**. Ispitajte ih da bi uočili razliku.

korišćenja skoro svih DNS alata je isti. Kao argument se zadaje domensko ime, a kao rezultat se dobija odgovarajuća IP adresa (za obrnuti DNS je suprotno).

```
$ nslookup domen # vraće IP adresu
$ nslookup ip_adresa # vraće domensko ime
```

Po *default*-u, **nslookup** prvo pokušava da dobije potrebne informacije od lokalnog DNS servera. Kako znamo koji je naš lokalni DNS server? Na Ubuntu-u IP adrese jednog ili više lokalnih DNS servera se čuvaju u **resolv.conf** fajlu u **/etc/** direktorijumu. Ukoliko želimo da upit šaljemo nekom drugom DNS serveru, onda IP adresu ili domensko ime tog DNS servera navodimo kao dodatni argument komande.

Napomena: Linux tipično koristi (najmanje) dva servisa za konverziju domenskih imena u IP adrese: DNS i jednostavni fajl koji sadrži listu domenskim imena i odgovarajućih IP adresa (**hosts** fajl).

Pregled i konfigurisanje tabele rutiranja

IP koristi tabelu rutiranja za utvrđivanje putanje (rute) kojom će se slati datagrami. Tabela rutiranja hostova je dosta jednostavnija od tabele rutiranja rutera jer se paketi obično sa hosta usmjeravaju na lokalni (*default*) ruter. Sadržaj tabele rutiranja na vašem računaru možete provjeriti komandom:

```
$ route -n
```

Opcija **-n** idicira da rezultat treba da sadrži numeričke IP adrese umjesto domenskih imena. Po *default*-u ova komanda prikazuje glavnu tabelu rutiranja. Međutim, operativni sistem čuva i keširanu tabelu rutiranja, koja se generiše na osnovu informacija o tome kako su usmjeravani prethodno poslati paketi. Kada IP sloj protokol steka primi datagram, prvo provjerava keširana pravila rutiranja, a zatim (ukoliko nema odgovarajućeg zapisa u kešu) koristi glavnu tabelu rutiranja. Listu keširanih pravila rutiranja možete dobiti koripćenjem opcije **-C**:

```
$ route -n -C
```

Rezultat ove komande ukazuje na gejtvej adrese koje koriste različiti parovi izvor-destinacija.

Komandom **route** je moguće i modifikovati sadržaj tabele rutiranja. Na primjer, ukoliko želimo da promijenimo adresu *default* gejtveja, to možemo uraditi komandom:

```
$sudo route add default gw adresa_gejtveja
```

Da onemogućimo rutiranje prema određenoj IP adresi koristimo komandu:

```
$sudo route add -host ip_adresa reject
```

Da izbrišemo default gejtvej:

```
$ route del default
```

Konvertovanje IP adresa u hardverske adrese

IP adrese su logičke adrese. Ukoliko host A želi da pošalje datagram hostu B u istoj mreži, on mora znati ne samo IP adresu već i MAC adresu hosta B. ARP protokol se koristi za otkrivanje MAC adrese koja odgovara nekoj IP adresi. Komanda **arp** kao rezultat vraće ARP tabelu koja sadrži listu parova IP adresa – MAC adresa koji su trenutno poznati hostu:

```
$ arp -n
```

ARP automatski dodaje nove zapise u ARP tabelu. Međutim, **arp** komanda se može koristiti i za manuelno dodavanje/brisanje zapisa iz ARP tabele.

Mrežne statistike

Alat koji omogućava uvid u razne mrežne statistike je **netstat**. Unosom ove komande možete dobiti informacije o statistikama na nivou interfejsa, statistikama tabele rutiranja, statistikama aktivnih konekcija i statistikama TCP/IP paketa. Aktivne TCP konekcije je moguče provjeriti komandom:

```
$ netstat -n -t
```

a uvid u TCP/IP statistike moguć je komandom:

```
$ netstat -s
```

Česta primjena ove komande je pronalaženje procesa koji "sluša" na određenom portu. Na primjer:

```
$ netstat -ltnp | grep -w ':80'
```

Značenje opcija u prethodoj komadi je sledeće:

- **l** – uzima u obzir samo sokete koji slušaju (*listenning*)
- **t** – prikazuje samo TCP konekcije

- **n** – prikazuje samo numeričke vrijednosti.
- **p** – omogučava prikazivanje ID-a procesa i njegovog imena
- **grep -w** – filtrira rezultate koji sadrže string ":80"

Slično se može positići **lsof** komandom koja je lakša za pamćenje:

```
$ lsof -i :80
```

Fajlovi sa važnim informacijama o mreži

Dodatne informacije o mrežnim parametrima možete naći u raznim fajlovima na vašem računaru. Važan direktorijum koji sadrži dosta informacija o konfiguraciji vašeg operativnog sistema je **/etc** direktorijum. Neki od korisnih fajlova u ovom direktorijumu su:

- **/etc/hosts** – Sadrži listu lokalnih domenskih imena i odgovarajućih IP adresa. Koristi se pored DNS servisa. Obično služi za dodjeljivanje imena računaru ili drugim računarima u istoj mreži.
- **/etc/resolv.conf** – Indicira lokalni DNS server za računar.
- **/etc/network/interfaces** – Čuva informacije o konfiguraciji mrežnih interfejsa.
- **/etc/services** – Čuva informacije o brojnim servisima koje klijentske aplikacije koriste na računaru. U fajlu su navedeni nazivi servisa, brojevi portova, protokoli koji se koriste, kao i odgovarajući aliasi servisa (ukoliko su definisani).

Dinamička konfiguracija IP adrese

Kao što je već objašnjeno, komandom **`ifconfig`** moguće je dodjeliti statičku IP adresu mrežnom interfejsu. Međutim, ukoliko postoji DHCP server u mreži, uglavnom je praktičnije koristiti DHCP servis za automatsku dodjelu IP adresa, *subnet* maski, DNS servera i gejtveja. Na koji način su konfigurisani mrežni interfejsi možemo vidjeti u **/etc/network/interfaces** fajlu. Ukoliko interfejs koristi DHCP servis, u fajlu će se nalaziti zapisi tipa:

```
auto interfejs
iface interfejs inet dhcp
```

Ukoliko želite da koristiti statičku IP adresu, fajl je potrebno izmijeniti na sledeći način:

```
iface interfejs inet static
address ip_adresa
```

Informacije o parametrima konfigursanim preko DHCP servisa čuvaju se u **/var/lib/dhcp3/dhclient.X.lease** fajlu, gdje je **X** identifikator interfejsa (npr. **eth2** ili **eth3**). Ovaj fajl može sadržati više od jednog zapisa, pri čemu poslednji zapis odgovara parametrima koji su trenutno u upotrebi. Ukoliko želite *refresh*-ovati IP adresu, dovoljno je *refresh*-ovati interfejs. Druga opcija je korišćenje *dhclient* komande, čiji je opcioni argument naziv interfejsa čiji se parametri žele *refresh*-ovati.

```
$ dhclient
```

Zadaci za samostalan rad:

1. Provjerite konfiguraciju, uključujući IP adrese, mrežnih interfejsa sa na vašem računaru.
2. Testirajte konektivnost između vašeg računara i nekog drugog računara u laboratoriji ili udaljenog web servera.
3. Odrediti preko kojih rutera se prenosi saobraćaj izmežu vašeg servera i servera **www.google.com**
4. Pronaći IP adrese nekoliko web servera na osnovu poznatog domenskog imena korišćenjem različitih DNS servera.
5. Pokušajte obrnuti DNS lookup.
6. Provjerite sadržaj tabele rutiranja i keširana pravila rutiranja.
7. Provjerite sadržaj APR tabele.
8. Pronađite MAC adresu nekog od računara iz iste mreže korišćenjem **arp** komande.
9. Provjerite aktivne TCP konekcije na vašem računaru nakon što posjetite neki web sajt.
10. Provjerite DHCP informacije za vaš računar i provjerite kako se one mijenjaju nakon refresh-ovanja DHCP servisa.