Pristup mreži

- Originalno, UNIX sistemi su predviđeni da budu povezani na mrežu
- Istu filozofiju je usvojio i Linux
- U ovoj prezentaciji će biti pokrivena osnovna mrežna podešavanja, kao i prikupljanje mrežnog saobraćaja za kasniju analizu, ali i udaljeni pristup (telnet i SSH)
- Napomenimo da su mrežna podešavanja na računaru mesto gde se preklapaju odgovornosti mrežnog i sistemskog administratora

Podešavanja mrežnih interfejsa

- Postoji više komandi kojima se aktiviraju i deaktiviraju mrežni interfejsi, podešavaju statičke IP adrese i sl.
- Najpoznatije komande su **ifconfig** i **ip**
- Komanda **ifconfig** je nešto starija komanda koja je još uvek popularna, ali u novije vreme se preporučuje (forsira) više upotreba **ip** komande
- Postoje i dodatne komande poput **ifup**, **ifdown** i **ifcfg**, za aktivaciju, deaktivaciju i konfiguraciju interfejsa, respektivno, ali preporuka je da se koriste **ifconfig** ili **ip**
- Navedimo i komandu **iwconfig** koja je slična **ifconfig** komandi, ali je namenjena bežičnim mrežnim interfejsima

ifconfig

- Ova komanda je još uvek popularna i često korišćena
- Omogućava pregled mrežnih interfejsa, kao i njihovih podešavanja poput promene IP adrese, aktivacije/deaktivacije i dr.
- Kucanjem komande bez opcija i argumenata dobija se prikaz mrežnih interfejsa, njihovih podešavanja i stanja (aktivni ili ne)
- Ako se kao argument navede interfejs, onda se dobija isti prikaz, ali samo za taj interfejs
- Tipično se za ethernet portove stavlja skraćenica *eth*, za bežične interfejse *wlan*, a lokalni loopback port je označen sa *lo*

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:bc:e9
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:bce9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10226 (10.2 KB)  TX bytes:16473 (16.4 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:7042 (7.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:269 errors:0 dropped:0 overruns:0 frame:0
          TX packets:269 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28303 (28.3 KB)  TX bytes:28303 (28.3 KB)
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:7042 (7.0 KB)
```

ifconfig

- Opcija -a daje prikaz za sve mrežne interfejse koji postoje, pa i one koji su trenutno deaktivirani
- Opcija -s daje skraćeni prikaz
- Navođenjem *up* i *down* flagova se vrši aktivacija i deaktivacija mrežnog interfejsa - u ovom slučaju se mora specificirati interfejs
- Za aktivaciju i deaktivaciju mrežnih interfejsa moraju se koristiti administratorske privilegije

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 down
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:bc:e9
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:bce9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:149 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11882 (11.8 KB)  TX bytes:17898 (17.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:279 errors:0 dropped:0 overruns:0 frame:0
          TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29520 (29.5 KB)  TX bytes:29520 (29.5 KB)

ubuntu@ubuntu-VirtualBox:~$ ifconfig -a
```

Primetiti da nakon deaktivacije eth1 interfejsa, isti se ne prikazuje u ifconfig ispisu.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:bc:e9
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:bce9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:149 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11882 (11.8 KB)  TX bytes:17898 (17.8 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:7149 (7.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:279 errors:0 dropped:0 overruns:0 frame:0
          TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29520 (29.5 KB)  TX bytes:29520 (29.5 KB)

ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 up
```

Primetiti da opcija -a daje ispis i deaktiviranog eth1 interfejsa.
Komanda na dnu slike vrši ponovnu aktivaciju eth1 interfejsa.

ifconfig

- Za konfigurisanje statičke IPv4 adrese na interfejsu dovoljno je samo iza interfejsa navesti IP adresu u formatu a.b.c.d, gde su a-d decimalni brojevi
- Za konfigurisanje mrežne maske (net maske) koja definiše koji deo u IPv4 adresi predstavlja net ID deo potrebno je navesti *netmask* iza čega sledi vrednost maske isto u formatu a.b.c.d (setite se sa predmeta iz treće godine da je maska niz jedinica kojih ima kolika je i dužina net ID dela i iza tih jedinica idu nule do kraja)
- Za konfigurisanje IPv6 adrese neophodno je navesti *add* iza čega sledi adresa u formatu *adresa/dužina_prefiksa*
- Prefiks je isto što i net ID
- Ako se umesto *add* navede *del*, onda se briše navedena IPv6 adresa

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 11.0.1.1
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.1  Bcast:11.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:16532 (16.5 KB)
```

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 netmask 255.255.254.0
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.1  Bcast:11.0.1.255  Mask:255.255.254.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:19880 (19.8 KB)
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 11.0.1.2 netmask 255.255.255.0
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.2  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:26329 (26.3 KB)
```

Može se u istoj liniji navesti više podešavanja. VAŽNA NAPOMENA: Prvo podešavanje koje je nevalidno tj. ne može da se uradi prekida izvršenje komande i sva ostala podešavanja iza se neće uraditi što može dovesti do neželjenih posledica, pa treba biti oprezan sa višestrukim podešavanjima u jednoj liniji.

Primetiti format IPv6 adrese, on se razlikuje od formata IPv4 adrese.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 311.0.1.2 netmask 255.255.254.0
311.0.1.2: Unknown host
ifconfig: `--help' gives usage information.
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.2  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:27779 (27.7 KB)

ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 11.0.1.3 netmask 355.255.254.0
355.255.254.0: Unknown host
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.3  Bcast:11.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:30237 (30.2 KB)
```

Primetiti u drugom primeru da je promena adrese interfejsa urađena i pored greške u definisanju mrežne maske.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 del fe80::a00:27ff:fe9b:b28d/64
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.3  Bcast:11.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:31977 (31.9 KB)

ubuntu@ubuntu-VirtualBox:~$ sudo ifconfig eth1 add fe80::a00:27ff:fe9b:b28d/64
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.3  Bcast:11.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:34098 (34.0 KB)
```

Primer skidanja i dodavanja IPv6 adrese interfejsa.

ifconfig

- Postoje i brojne druge opcije (mnoge od njih nema potrebe menjati ili su automatski podešene kako treba od strane drajvera mrežnog interfejsa)
- Opcija arp vrši aktivaciju ARP protokola na interfejsu (ako se navede -arp onda se deaktivira ARP protokol)
- Opcija promisc vrši aktivaciju promiskuitetnog moda na interfejsu (ako se navede -promisc onda se deaktivira taj mod)
- Opcija allmulti aktivira mod u kom se primaju svi multikast paketi koji dođu na interfejs (-allmulti deaktivira mod)
- Opcija mtu *dužina* menja vrednost MTU (*Maximum Transfer Unit*) veličine

ifconfig

- Opcija metric *vrednost* menja vrednost metrike na interfejsu
- Opcija txqueuelen *dužina* menja vrednost dužine predajnog reda za čekanje
- Postoje i druge opcije koje se mogu videti u man uputstvu za **ifconfig** komandu
- U uobičajenim situacijama većinu opcija nije potrebno koristiti (jer difolt vrednosti su sasvim odgovarajuće), uglavnom se koriste opcije za aktivaciju i deaktivaciju interfejsa, promenu adrese i mrežne maske interfejsa, kao i sam prikaz stanja interfejsa

ifconfig

- Opisana promena statičke IP adrese je privremena, tj. kada se sistem restartuje statička IP adresa ranije uneta će biti izgubljena tj. moraće se ponovo konfigurisati na ranije opisani način
- Da bi promena bila trajna mora se editovati odgovarajući konfiguracioni fajl (editovati sa administratorskim privilegijama) - /etc/network/interfaces (fajl u slučaju Ubuntu distribucije, za ostale distribucije proveriti da li je u pitanju ovaj fajl ili neki drugi)

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
          inet addr:11.0.1.1  Bcast:11.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:b28d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:9767 (9.7 KB)

ubuntu@ubuntu-VirtualBox:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

# definicija staticke adrese za eth1 interfejs
auto eth1
iface eth1 inet static
address 11.0.1.1
netmask 255.255.255.0
gateway 11.0.1.100
```

U donjem delu slike je prikazan sadržaj /etc/network/interfaces fajla sa podešavanjima za eth1 interfejs. Sada će svaki put kada se ponovo podigne operativni sistem, interfejs eth1 biti konfigurisan sa postavljenom statičkom IP adresom. Kada se izvrši editovanje /etc/network/interfaces fajla, da bi promena bila aktivirana neophodno je restartovati mrežni servis sa **sudo /etc/init.d/networking restart**

ip

- Ova komanda je alternativa za **ifconfig**
- U novijim verzijama Linux distribucija se preporučuje upotreba ove komande umesto **ifconfig**
- Komanda ip se zadaje u formatu **ip** *opcije objekat komanda*
- Opcija -s ispisuje dodatne informacije - uglavnom se dodatne informacije odnose na statistiku
- -f *tip_adrese* definiše koja adresa se koristi u nastavku (inet je za IPv4, inet6 za IPv6,...) - ako se ne navede ova opcija onda ip komanda pokušava da na osnovu ostatka linije dedukuje koji tip adrese se koristi i ako ne uspe onda se koristi difolt tip što je tipično IPv4
- -4 je skraćenica za -f inet, a -6 je skraćenica za -f inet6

ip

- Objekat u komandi predstavlja nad čim se vrši komanda koja se zadaje iza objekta
- Definisan je velik broj objekata
- Objekat address predstavlja adresu mrežnog interfejsa
- Objekat link predstavlja sam mrežni interfejs
- Objekat maddress predstavlja multikast adresu
- Objekat route predstavlja zapis u tabeli usmeravanja
- Objekat rule predstavlja pravilo u politici rutiranja
- ....
- Neki objekti se mogu pisati u skraćenoj formi npr. address se može pisati kao addr ili a

ip

- Komanda se odnosi na akciju koja se vrši na objektu
- Svaki objekat ima svoj skup komandi
- Komanda help je dostupna za sve objekte i prikazuje sve komande za taj objekat
- Većina objekata podržava komande show (ili list), add i delete

ip link

- Objekat link omogućava podešavanje mrežnih interfejsa, poput aktivacije i deaktivacije samog interfejsa, veličine reda za čekanje predajnika, promiskuitetnog moda, prijema multikast paketa, arp protokola, MTU veličine i dr.
- Sa **ip link set** *interfejs* se vrši konfigurisanje interfejsa pri čemu se iza *interfejs* navode atributi koji se žele promeniti
- Atributi up i down se koriste za aktivaciju i deaktivaciju interfejsa, respektivno
- arp on i arp off se koriste za aktivaciju/deaktivaciju ARP protokola na interfejsu
- promisc on i promisc off se koriste za aktivaciju/deaktivaciju promiskuitetnog moda interfejsa

ip link

- allmulticast on i allmulticast off se koriste za aktivaciju/deaktivaciju prijema svih multikast paketa
- txqueuelen *veličina* menja dužinu reda za čekanje predajnika interfejsa
- mtu *veličina* menja veličinu MTU
- Napomena: i ovde kao i u slučaju **ifconfig** važi pravilo da se izvršenje prekida na nailazak prve greške, ali svi atributi navedeni pre greške će biti postavljeni što može dovesti do neželjenog stanja
- Sa **ip link show** se prikazuje stanje svih interfejsa, a ako se iza navede reč *up* onda se prikazuje stanje svih aktivnih interfejsa, a ako se navede naziv interfejsa onda samo stanje navedenog interfejsa

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:1b:bc:e9 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
ubuntu@ubuntu-VirtualBox:~$ ip link show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
ubuntu@ubuntu-VirtualBox:~$ ip -s link show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    0          0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    162579     2615     0       0       0       0
```

Poslednji primer prikazuje upotrebu -s opcije koja prikazuje dodatnu statistiku za interfejs.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ip link set eth1 down
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~$ ip link show up
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:1b:bc:e9 brd ff:ff:ff:ff:ff:ff
ubuntu@ubuntu-VirtualBox:~$ sudo ip link set eth1 up
ubuntu@ubuntu-VirtualBox:~$ ip link show up
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:1b:bc:e9 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
```

Isto kao i kod **ifconfig** komande, i ovde se za podešavanja interfejsa moraju koristiti administratorske privilegije.

ip address

- Ovaj objekat se koristi za prikaz i promenu adresa mrežnog interfejsa
- **ip address** prikazuje adrese za sve interfejse, a ako se iza navede interfejs onda samo za navedeni interfejs
- Sa **ip address add** može se postaviti adresa interfejsa, odnosno sa **ip address delete** se može skinuti adresa interfejsa
- Sa **ip address show** se daje prikaz adresa interfejsa uz mogućnost filtriranja rezultata po nekom kriterijumu
- Sa **ip address flush** se skidaju adrese interfejsa po nekom kriterijumu ili sve adrese ako nema navedenog kriterijuma (treba biti pažljiv jer se može desiti da se obrišu i adrese interfejsa koje se nisu želele obrisati)

Primer

Umesto **ip address show** se može koristiti i samo **ip address**

```
ubuntu@ubuntu-VirtualBox:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:1b:bc:e9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
       valid_lft 81380sec preferred_lft 81380sec
    inet6 fe80::a00:27ff:fe1b:bce9/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:b28d/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$ ip address show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:b28d/64 scope link
       valid_lft forever preferred_lft forever
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ip address show eth1 to 11.0.1.0/24
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$ ip address show eth1 to 11.2.1.0/24
ubuntu@ubuntu-VirtualBox:~$ ip address show eth1 to 11.0.1.5/24
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$ ip address show to 11.0.1.5/24
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
```

Ovde je dat primer jednog dodatnog atributa za show komandu address objekta. U pitanju je atribut to kojim se filtrira prikaz samo onih adresa koje odgovaraju zadatom prefiksu. Primetiti da nije bitno šta se upisuje u deo koji ne pripada prefiksu (host id deo adrese) - poslednja dva primera. Takođe u poslednjem primeru je vidljiva upotreba samo to atributa bez navođenja interfejsa čime se traže adrese koje odgovaraju navedenom prefiksu na svim interfejsima. Liste atributa za svaku komandu nekog objekta se mogu videti u man uputstvu **ip** komande.

ip address

- Sa **ip address add** može se postaviti adresa interfejsa
- Iza navedenog se navodi *adresa* pa *dev naziv interfejsa*
- U delu *adresa* se može ispred same vrednosti adrese navesti tip adrese ali ne u smislu protokola (za to služi opcija -f **ip** komande) već u smislu njenog značenja poput brodkast adresa (*broadcast*) ili lokalna adresa (*local* - ovo je ustvari adresa interfejsa) - ako se ništa ne navede podrazumeva se local
- Takođe, na kraju same vrednosti se može navesti dužina prefiksa u formatu */n* gde je *n* dužina prefiksa
- Sa **ip address delete** može se skinuti adresa interfejsa, a format je isti kao za add varijantu, ako se ne navede adresa tada se skida prva adresa interfejsa

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:b28d/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$ sudo ip addr add local 11.0.1.2 dev eth1
ubuntu@ubuntu-VirtualBox:~$ sudo ip addr add 11.0.1.3 dev eth1
ubuntu@ubuntu-VirtualBox:~$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 11.0.1.2/32 scope global eth1
       valid_lft forever preferred_lft forever
    inet 11.0.1.3/32 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:b28d/64 scope link
       valid_lft forever preferred_lft forever
```

Primetiti da se local ne mora pisati. Da smo hteli i dužinu prefiksa definisati, moglo se pisati u formatu 11.0.1.3/24 npr. za zadnji primer i ako želimo da dužina prefiksa bude 24.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo ip addr delete local 11.0.1.3 dev eth1
Warning: Executing wildcard deletion to stay compatible with old scripts.
         Explicitly specify the prefix length (11.0.1.3/32) to avoid this warnin
g.
         This special behaviour is likely to disappear in further releases,
         fix your scripts!
ubuntu@ubuntu-VirtualBox:~$ sudo ip addr delete 11.0.1.2/32 dev eth1
ubuntu@ubuntu-VirtualBox:~$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:9b:b2:8d brd ff:ff:ff:ff:ff:ff
    inet 11.0.1.1/24 brd 11.0.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:b28d/64 scope link
       valid_lft forever preferred_lft forever
```

Primetiti u prvom primeru da je poželjno da se pri navođenju adrese koja se želi obrisati ona navede zajedno sa prefiksom. U drugom primeru je navedena i dužina prefiksa pa nije došlo do ispisa upozorenja.

ip

- Kao što smo naveli ranije u prezentaciji postoje i brojni drugi objekti koji mogu biti veoma važni u pojedinim konfiguracijama i primenama Linux baziranih uređaja
- Na primer, *route* koji upravlja tabelama usmeravanja, *neighbour* koji je podešava vezivanja mrežnih adresa i adresa sa drugog sloja OSI modela, *rule* koji definiše politiku usmeravanja....

Primer

```
ubuntu@ubuntu-VirtualBox:~$ ip rule show
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default
ubuntu@ubuntu-VirtualBox:~$ ip neighbour show
10.0.2.2 dev eth0 lladdr 52:54:00:12:35:02 STALE
ubuntu@ubuntu-VirtualBox:~$ ip neighbour show dev eth1
ubuntu@ubuntu-VirtualBox:~$ ip neighbour show dev eth0
10.0.2.2 lladdr 52:54:00:12:35:02 STALE
ubuntu@ubuntu-VirtualBox:~$ ip route show
default via 10.0.2.2 dev eth0  proto static  metric 100
10.0.2.0/24 dev eth0  proto kernel  scope link  metric 100
11.0.1.0/24 dev eth1  proto kernel  scope link  src 11.0.1.1
ubuntu@ubuntu-VirtualBox:~$ ip route show dev eth1
11.0.1.0/24  proto kernel  scope link  src 11.0.1.1
```

U prikazanim primerima je korišćena samo komanda show za prikaz. Za dodavanje i brisanje zapisa se koriste komande add i delete, a postoje i druge komande zavisno od objekta. Preporuka je da se pročita man uputstvo za **ip** komandu.

arp

- Ova komanda omogućava prikaz i manipulaciju sadržaja ARP tabele koja sadrži vezivanja mrežnih adresa i adresa sloja 2 (tj. MAC adresa)
- Ako se navede samo naziv komande prikazaće se sadržaj ARP tabele
- Opcija -d omogućava brisanje zapisa (navodi se adresa hosta)
- Opcija -s omogućava dodavanje zapisa (navodi se adresa hosta koju sledi MAC adresa)
- Opcija -f *fajl* je slična -s opciji samo što se zapisi koji se dodaju čitaju iz navedenog fajla (ako se fajl ne navede onda se podrazumeva /etc/ethers fajl)

Primer

```
ubuntu@ubuntu-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:54:00:12:35:02   C                     eth0
11.0.1.7                 ether   08:00:27:f5:27:2a   C                     eth1
ubuntu@ubuntu-VirtualBox:~$ sudo arp -s 11.0.1.5 09:aa:b4:76:98:10
ubuntu@ubuntu-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:54:00:12:35:02   C                     eth0
11.0.1.7                 ether   08:00:27:f5:27:2a   C                     eth1
11.0.1.5                 ether   09:aa:b4:76:98:10   CM                    eth1
ubuntu@ubuntu-VirtualBox:~$ sudo arp -d 11.0.1.5
ubuntu@ubuntu-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:54:00:12:35:02   C                     eth0
11.0.1.7                 ether   08:00:27:f5:27:2a   C                     eth1
11.0.1.5                         (incomplete)                              eth1
```

Za modifikaciju sadržaja tabele su potrebne administratorske privilegije. Kada se obriše zapis, kod njega stoji incomplete, a posle izvesnog vremena će zapis nestati iz tabele. Generalno i aktivni zapisi imaju svoj vek validnosti i moraju se osvežavati.

```
ubuntu@ubuntu-VirtualBox:~$ arp -i eth1
Address                  HWtype  HWaddress           Flags Mask            Iface
11.0.1.7                 ether   08:00:27:f5:27:2a   C                     eth1
11.0.1.5                         (incomplete)                              eth1
```

Opcija -i omogućava da se prikaže samo deo tabele koji se odnosi na navedeni interfejs.

route

- Ova komanda omogućava prikaz i manipulaciju sadržaja tabele usmeravanja - čak i hostovi koji nemaju ulogu rutera imaju određene odluke prilikom usmeravanja paketa (npr. ako ima više mrežnih interfejsa, na koji interfejs poslati paket)
- Ako se navede samo naziv komande prikazaće se sadržaj tabele usmeravanja
- Opcija -A definiše tip adrese koji se koristi (difolt je inet koji predstavlja IPv4, inet6 predstavlja IPv6)
- Opcija -F definiše da se radi sa kernelovom FIB (Forwarding Information Base) tabelom usmeravanja
- Opcija -C definiše da se radi sa kernelovom keš memorijom za usmeravanje

route

- Opcija -e definiše prikaz u netstat formatu
- Opcije del i add se koriste za dodavanje i brisanje zapisa
- Opcija target iza koje sledi adresa definiše odredišnu adresu hosta ili mreže (zavisno na šta se zapis odnosi)
- Opcija -net definiše da je target mreža
- Opcija -host definiše da je target host
- Opcija netmask koju sledi vrednost maske definiše mrežnu masku
- Opcija dev iza koje sledi naziv mrežnog interfejsa definiše na koji interfejs se odnosi zapis
- Opcija reject je za blokiranje ruta

route

- Postoje i opcije koje definišu parametre TCP-a poput inicijalnog round-trip vremena, veličine prozora, max. veličine segmenta
- Takođe, može da se postavi i vrednost metrike za rutu
- U većini slučajeva nema potrebe manuelno podešavati tabelu usmeravanja, ali se mogu postaviti statičke rute, odnosno za neke adrese (hostove/mreže) može se forsirati željeni mrežni interfejs

Primer

```
ubuntu@ubuntu-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
ubuntu@ubuntu-VirtualBox:~$ route -C
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
ubuntu@ubuntu-VirtualBox:~$ route -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo route add -net 13.103.0.0 netmask 255.255.0.0 dev eth1
ubuntu@ubuntu-VirtualBox:~$ sudo route add -host 12.12.107.5 dev eth1
ubuntu@ubuntu-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
12.12.107.5     *               255.255.255.255 UH    0      0        0 eth1
13.103.0.0      *               255.255.0.0     U     0      0        0 eth1
ubuntu@ubuntu-VirtualBox:~$ sudo route del -net 13.103.0.0 netmask 255.255.0.0 dev eth1
ubuntu@ubuntu-VirtualBox:~$ sudo route del -host 12.12.107.5 dev eth1
ubuntu@ubuntu-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
```

DHCP

- Tipičan slučaj je da se ne koristi statička IP adresa, nego da se koristi DHCP protokol za dinamičku dodelu adresa
- Iz tog razloga Linux OS treba da ima aplikaciju koja će vršiti ulogu DHCP klijenta
- dhclient predstavlja aplikaciju DHCP klijenta
- dhclient.conf predstavlja konfiguracioni fajl za dhclient (nalazi se u folderu /etc/dhcp)

ping

- Koristan za ispitivanje dostupnosti zadate ip adrese ili naziva hosta
- Postoji i dosta opcija
- Opcija -c *n* definiše broj ping paketa koji će se poslati (bez ove opcije slanje će biti beskonačno i ping se mora nasilno prekinuti npr. Sa CTRL+C)
- Opcija -p *pattern* definiše pattern koji će dopuniti paket
- Opcija -i *interval* definiše interval između slanja paketa
- Opcija -t *ttl* definiše ttl vreme ping paketa

ping

```
ubuntu@ubuntu-VirtualBox:~$ ping -c 3 11.0.1.7
PING 11.0.1.7 (11.0.1.7) 56(84) bytes of data.
64 bytes from 11.0.1.7: icmp_seq=1 ttl=64 time=0.456 ms
64 bytes from 11.0.1.7: icmp_seq=2 ttl=64 time=0.548 ms
64 bytes from 11.0.1.7: icmp_seq=3 ttl=64 time=0.654 ms

--- 11.0.1.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.456/0.552/0.654/0.085 ms
ubuntu@ubuntu-VirtualBox:~$ ping -c 3 www.google.rs
PING www.google.rs (216.58.214.195) 56(84) bytes of data.
64 bytes from bud02s23-in-f3.1e100.net (216.58.214.195): icmp_seq=1 ttl=56 time=17.1 ms
64 bytes from bud02s23-in-f3.1e100.net (216.58.214.195): icmp_seq=2 ttl=56 time=13.6 ms
64 bytes from bud02s23-in-f3.1e100.net (216.58.214.195): icmp_seq=3 ttl=56 time=14.0 ms

--- www.google.rs ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 13.664/14.928/17.108/1.551 ms
```

traceroute

- Koristan za ispitivanje rute koju prolazi paket do odredišta
- Postoji velik broj opcija kojima se može podesiti ova komanda
- Na primer, može se definisati da li će se slati traceroute preko UDP-a, TCP-a ili ICMP-a (ICMP je tradicionalni metod, a TCP se tipično koristi da se zaobiđe firewall zaštita) - po difoltu se koristi UDP
- Opcija -I (štampano i) šalje preko ICMP-a - za ovu opciju su potrebne administratorske privilegije
- Opcija -T šalje preko TCP-a - za ovu opciju su potrebne administratorske privilegije
- Kao i kod pinga adresa destinacije se navodi ili kao IP adresa ili kao naziv hosta

Analiza mrežnog saobraćaja

- Prikupljanje i analiza mrežnog saobraćaja je važna u dijagnostici problema u mreži, ali i za uočavanje potencijalnih problema u budućnosti što je bitno za proces planiranja unapređivanja mreže
- Svakako, jedan od najpopularnijih besplatnih alata je Wireshark koji je dostupan i za Linux (dobar prikaz mogućnosti ovog alata može sa naći i u master radu "Aplikacija za prikaz rezultata analize mrežnog saobraćaja" koji je dostupan na istom sajtu gde se nalaze i ove prezentacije (na stranici za master radove))
- U ovoj prezentaciji će fokus biti na alatima (**netstat**, **tcpdump**) koji ne zahtevaju grafičko okruženje tj. GUI

netstat

- Ovaj alat omogućava prikaz otvorenih soketa, sadržaja tabela usmeravanja, statistika mrežnog saobraćaja...
- Ako se kuca bez opcija i argumenata onda se prikazuje lista otvorenih soketa
- Iza **netstat** se može prvo navesti opcija koja definiše koji tip informacije se prikazuje
- Opcija -r daje prikaz tabele usmeravanja
- Opcija -g daje prikaz pripadnosti multikast grupama
- Opcija -i daje prikaz svih mrežnih interfejsa
- Opcija -M daje prikaz tzv. *masqueraded* konekcija (nešto slično NAT) - na linku http://www.tldp.org/HOWTO/IP-Masquerade-HOWTO/ipmasq-background2.5.html može se naći osnovni opis
- Opcija -s daje prikaz zbirne statistike za protokole

Primer

Deo prikaza za **netstat**

Dobar deo otvorenih soketa su Unix soketi za komunikaciju među procesima

```
ubuntu@ubuntu-VirtualBox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       1      0 ip6-localhost:55754     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55757     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55753     ip6-localhost:ipp       CLOSE_WAIT
udp        0      0 localhost:52578         ubuntu-VirtualBo:domain ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    9218     /run/systemd/journal/
syslog
unix  2      [ ]         DGRAM                    8598     /run/systemd/notify
unix  14     [ ]         DGRAM                    8622     /run/systemd/journal/
dev-log
unix  6      [ ]         DGRAM                    8636     /run/systemd/journal/
socket
unix  2      [ ]         DGRAM                    8897     /run/systemd/shutdown
d
unix  3      [ ]         STREAM     CONNECTED     17343    @/tmp/.X11-unix/X0
```

Prikaz tabele usmeravanja

```
ubuntu@ubuntu-VirtualBox:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         11.0.1.100      0.0.0.0         UG        0 0          0 eth1
default         10.0.2.2        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
11.0.1.0        *               255.255.255.0   U         0 0          0 eth1
link-local      *               255.255.0.0     U         0 0          0 eth1
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0          2      0      0 0             68      0      0      0 B
MRU
eth1       1500 0          0      0      0 0            760      0      0      0 B
MRU
lo        65536 0       2040      0      0 0           2040      0      0      0 L
RU
ubuntu@ubuntu-VirtualBox:~$ netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      224.0.0.1
eth0            1      224.0.0.251
eth0            1      224.0.0.1
eth1            1      224.0.0.251
eth1            1      224.0.0.1
lo              1      ip6-allnodes
getnameinfo failed
lo              1      [UNKNOWN]
```

Primer

Deo prikaza statistike po protokolima

```
ubuntu@ubuntu-VirtualBox:~$ netstat -s
Ip:
    2345 total packets received
    2 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    2343 incoming packets delivered
    3717 requests sent out
    60 outgoing packets dropped
Icmp:
    1490 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 1490
    1490 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 1490
IcmpMsg:
        InType3: 1490
        OutType3: 1490
Tcp:
    7 active connections openings
    3 passive connection openings
    4 failed connection attempts
    0 connection resets received
    0 connections established
```

netstat

- Iza opcija navedenih na slajdu 45 (tu spada i varijanta kada se **netstat** navede sam za sebe) se mogu pisati dodatne opcije koje specificiraju netstat ponašanje u ispisu izveštaja
- Opcija -c vrši kontinualan ispis tj. svake sekunde
- Opcija -e daje ispisuje dodatne informacije (dvostruka upotreba ove opcije ispisuje sve dodatne informacije)
- Opcija -l prikazuje samo sokete koji osluškuju
- Opcija -a prikazuje sve sokete
- Opcija -p daje prikaz ID-a procesa i naziva programa kome odgovara soket
- Opcija -o daje prikaz i tajmera vezanih za sokete
- Postoje i druge opcije, a koje od opcija navedenih na ovom slajdu se mogu koristiti u kombinaciji sa opcijama sa slajda 45, može se videti u man uputstvu **netstat** komande

Primer

Deo prikaza za -l. Na primer, ova opcija se može navesti samo uz varijantu netstat.

```
ubuntu@ubuntu-VirtualBox:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ubuntu-VirtualBo:domain *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 *:mdns                  *:*
```

Primer jednostruke i dvostruke upotrebe opcije -e

```
ubuntu@ubuntu-VirtualBox:~$ netstat -r -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         11.0.1.100      0.0.0.0         UG    0      0        0 eth1
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
link-local      *               255.255.0.0     U     1000   0        0 eth1
ubuntu@ubuntu-VirtualBox:~$ netstat -r -e -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
 MSS   Window irtt
default         11.0.1.100      0.0.0.0         UG    0      0        0 eth1
 0     0      0
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
 0     0      0
10.0.2.0        *               255.255.255.0   U     100    0        0 eth0
 0     0      0
11.0.1.0        *               255.255.255.0   U     0      0        0 eth1
 0     0      0
link-local      *               255.255.0.0     U     1000   0        0 eth1
 0     0      0
```

Primer

Deo prikaza za -l -o. I za opciju -o važi napomena data na prethodnom slajdu za opciju -l.

```
ubuntu@ubuntu-VirtualBox:~$ netstat -l -o
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Timer
tcp        0      0 ubuntu-VirtualBo:domain *:*                     LISTEN
off (0.00/0/0)
tcp        0      0 localhost:ipp           *:*                     LISTEN
off (0.00/0/0)
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
off (0.00/0/0)
udp        0   1536 *:10927                 *:*
off (0.00/0/0)
```

Deo prikaza. Može se videti da ispis dodatnih informacija za -i opciju odgovara formatu ifconfig ispisa.

```
ubuntu@ubuntu-VirtualBox:~$ netstat -i -e
Kernel Interface table
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:bc:e9
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:bce9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KB)  TX bytes:10630 (10.6 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:9b:b2:8d
```

netstat

- U slučaju opcije -r ili kada se ne koriste opcije sa slajda 45, može se navesti tip mrežne adrese,
- U slučaju opcije -s ili kada se ne koriste opcije sa slajda 45, može se navesti tip transportnog protokola koji je otvorio soket za dodatno filtriranje rezultata
- -4 označava IPv4, a -6 označava IPv6 adrese
- -t označava TCP soket
- -u označava UDP soket
- -w označava raw soket (ne koristi se transportni sloj)
- -x označava Unix soket (koristi se za komunikaciju između procesa) - ova opcija ne može da se navede uz -s opciju za razliku od prethodne 3

Primer

```
ubuntu@ubuntu-VirtualBox:~$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:35677         ubuntu-VirtualBo:domain ESTABLISHED
ubuntu@ubuntu-VirtualBox:~$ netstat -l -u
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:mdns                  *:*
udp        0      0 *:37619                 *:*
udp        0      0 *:31494                 *:*
udp        0   1536 *:7488                  *:*
udp        0      0 *:10577                 *:*
udp        0      0 *:43511                 *:*
udp        0      0 *:2608                  *:*
udp        0      0 ubuntu-VirtualBo:domain *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:18505                 *:*
udp        0   1536 *:15952                 *:*
udp        0      0 *:48755                 *:*
udp        0      0 *:ipp                   *:*
udp        0      0 *:30874                 *:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:34634              [::]:*
udp6       0      0 [::]:23945              [::]:*
```

Primetiti razliku u ispisu kad se doda opcija -l.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       1      0 ip6-localhost:55754     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55757     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55753     ip6-localhost:ipp       CLOSE_WAIT
ubuntu@ubuntu-VirtualBox:~$ netstat -t -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       1      0 ip6-localhost:55754     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55757     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55753     ip6-localhost:ipp       CLOSE_WAIT
udp        0      0 localhost:33923         ubuntu-VirtualBo:domain ESTABLISHED
ubuntu@ubuntu-VirtualBox:~$ netstat -4 -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
ubuntu@ubuntu-VirtualBox:~$ netstat -6 -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       1      0 ip6-localhost:55754     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55757     ip6-localhost:ipp       CLOSE_WAIT
tcp6       1      0 ip6-localhost:55753     ip6-localhost:ipp       CLOSE_WAIT
ubuntu@ubuntu-VirtualBox:~$ netstat -4 -t -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:46254         ubuntu-VirtualBo:domain ESTABLISHED
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ netstat -r -4
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         11.0.1.100      0.0.0.0         UG        0 0          0 eth1
default         10.0.2.2        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
11.0.1.0        *               255.255.255.0   U         0 0          0 eth1
link-local      *               255.255.0.0     U         0 0          0 eth1
ubuntu@ubuntu-VirtualBox:~$ netstat -r -6
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
fe80::/64                      ::                         U    256 0     0 eth1
fe80::/64                      ::                         U    256 0     0 eth0
::/0                           ::                         !n   -1  1     1 lo
::1/128                        ::                         Un   0   7    13 lo
fe80::a00:27ff:fe1b:bce9/128   ::                         Un   0   1     0 lo
fe80::a00:27ff:fe9b:b28d/128   ::                         Un   0   1     0 lo
ff00::/8                       ::                         U    256 0     0 eth1
ff00::/8                       ::                         U    256 0     0 eth0
::/0                           ::                         !n   -1  1     1 lo
```

Primetiti da opcija -r po difoltu prikazuje tabelu za IPv4 (slajd 46).

Primer

```
ubuntu@ubuntu-VirtualBox:~$ netstat -s -t
IcmpMsg:
    InType3: 4418
    OutType3: 4418
Tcp:
    7 active connections openings
    3 passive connection openings
    4 failed connection attempts
    0 connection resets received
    0 connections established
    57 segments received
    57 segments send out
    0 segments retransmited
    0 bad segments received.
    4 resets sent
UdpLite:
TcpExt:
    3 TCP sockets finished time wait in fast timer
    3 delayed acks sent
```

```
ubuntu@ubuntu-VirtualBox:~$ netstat -s -u
IcmpMsg:
    InType3: 4294
    OutType3: 4294
Udp:
    2122 packets received
    120 packets to unknown port received.
    0 packet receive errors
    6429 packets sent
    IgnoredMulti: 6
UdpLite:
IpExt:
    InMcastPkts: 60
    OutMcastPkts: 64
    InBcastPkts: 6
    OutBcastPkts: 6
    InOctets: 565272
    OutOctets: 844708
    InMcastOctets: 8192
    OutMcastOctets: 8352
    InBcastOctets: 284
    OutBcastOctets: 284
    InNoECTPkts: 6555
```

Primetiti da se neki delovi ispisa za -u i -t opcije poklapaju (IcmpMsg).

tcpdump

- Ovaj alat omogućava funkcionalnosti slične onima koje ima Wireshark, a to je snimanje paketa na mrežnom interfejsu
- Postoji velik broj opcija kojima se može podesiti snimanje paketa
- Snimljeni paketi se mogu sačuvati u fajlu čime se omogućava kasnija analiza i upotreba drugih alata za analizu
- Opcija -c *N* aktivira snimanje *N* paketa nakon čega se gasi **tcpdump** - ako se ova opcija ne koristi onda **tcpdump** kontinualno snima pakete i potrebno je nasilno gašenje (CTRL+C ili **kill** komanda)

tcpdump

- Opcija -A ispisuje paket (deo iznad sloja 2) u ASCII formatu
- Opcija -w *fajl* zadaje fajl u koji treba da se snime paketi (ako se ne koristi -w onda se ispis radi na stdout)
- Opcija -C definiše max. veličinu fajla u koji se snimaju uhvaćeni paketi - ako se vidi da je dostignuta max. veličina fajla onda se zatvara tekući fajl i otvara novi za snimanje - baza imena fajla je uvek ona zadata -w opcijom
- Opcija -W definiše max. broj fajlova koji može da se kreira ako se koristi -C opcija - kada se dostigne taj broj upis počinje od početnog fajla - u suštini kružna lista fajlova se pravi
- Opcija -D ispisuje interfejse na kojima mogu da se snimaju paketi
- Opcija -e ispisuje i zaglavlje sloja 2

tcpdump

- Opcija -F *fajl* definiše da se definicija filtra za snimanje uzme iz navedenog fajla, ako je istovremeno filtar definisan i u ostatku linije unete **tcpdump** komande, taj filtar definisan u komandnoj liniji će se ignorisati
- Opcija -i *interfejs* definiše da se snimaju paketi sa navedenog interfejsa - ako se ne navede ova opcija snimanje se radi na interfejsu najnižeg rednog broja - u verzijama kernela 2.2 do 2.4 može se navesti za interfejs *any* čime se traži snimanje sa svih interfejsa
- Opcija -n forsira da se ne radi konverzija adresa u domenska (i druga imena zavisno od tipa adrese) imena
- Opcija -r *fajl* vrši čitanje ranije smimljenog sadržaja iz navedenog fajla (u ovom slučaju se ne radi snimanje)

filtri

- Komanda tcpdump omogućava definisanje filtara kojima se može specificirati koje pakete treba snimiti
- Kompleksniji izrazi se mogu formirati upotrebom logičkih operatora and, or i not (alternativa ovim operatorima su &&, ||, !) pri čemu se potencijalno moraju koristiti zagrade ako je redosled izvršenja bitan
- Na linku http://www.tcpdump.org/manpages/pcap-filter.7.txt se može naći detaljno uputstvo za kreiranje filtara

filtri

- dst host *host* - paketi čija se odredišna IP(4 ili 6) adresa poklapa sa navedenom
- src host *host* - paketi čija se izvorišna IP(4 ili 6) adresa poklapa sa navedenom
- host *host* - paketi čija se odredišna ili izvorišna IP(4 ili 6) adresa poklapa sa navedenom
- U prethodna tri slučaja adresa se navodi direktno ili kao naziv hosta
- Takođe, ispred filtara u prethodna tri slučaja se može navesti protokol - ip, ip6, arp ili rarp

filtri

- ether dst *host* - paketi čija se odredišna MAC adresa poklapa sa navedenom
- ether src *host* - paketi čija se izvorišna MAC adresa poklapa sa navedenom
- ether host *host* - paketi čija se odredišna ili izvorišna MAC adresa poklapa sa navedenom
- U prethodna tri slučaja adresa se navodi direktno ili kao naziv iz fajla /etc/ethers

filtri

- dst net *net* - paketi čija se odredišna IP adresa poklapa sa navedenom mrežnom adresom
- src net *net* - paketi čija se izvorišna IP adresa poklapa sa navedenom mrežnom adresom
- net *net* - paketi čija se odredišna ili izvorišna IP adresa poklapa sa navedenom mrežnom adresom
- U prethodna tri slučaja IPv6 mrežna adresa se mora kompletno navesti, a IPv4 ne mora tj. mogu se navesti i samo 3 broja (a.b.c), 2 broja (a.b) ili 1 broj (a), pri čemu se maska uvek podrazumeva na nivou bajtova, npr. za slučaj dva broja podrazumeva se maska 255.255.0.0
- U prethodna tri slučaja dužina prefiksa (mrežnog dela adrese) se može eksplicitno navesti odmah iza *net* vrednosti sa nalepljenim *duz* delom

filtri

- dst port *port* - paketi čiji se odredišni port poklapa sa navedenim
- src port *port* - paketi čiji se izvorišni port poklapa sa navedenim
- port *port* - paketi čiji se odredišni ili izvorišni port poklapa sa navedenim
- U prethodna tri slučaja port se navodi kao broj ili kao naziv (koji je definisan u /etc/services)
- Pri tome navedeni filtri su od značaja za pakete koji koriste udp ili tcp protokol
- Ako se ispred navedenih filtara navede udp ili tcp onda se specificira na koji transportni protokol se odnosi port

filtri

- dst portrange *port1-port2* - paketi čiji odredišni port upada u navedeni opseg
- src portrange *port1-port2* - paketi čiji izvorišni port upada u navedeni opseg
- portrange *port1-port2* - paketi čiji odredišni ili izvorišni port upada u navedeni opseg
- Pri tome navedeni filtri su od značaja za pakete koji koriste udp ili tcp protokol
- Ako se ispred navedenih filtara navede udp ili tcp onda se specificira na koji transportni protokol se odnosi port

filtri

- less *veličina* - paketi čija je veličina manja ili jednaka od navedene
- greater *veličina* - paketi čija je veličina veća ili jednaka od navedene
- ip proto *protokol* - definiše koji protokol je enkapsuliran u IPv4 paket (*protokol* može biti naziv: icmp, icmp6, igmp, igrp, pim, ah, esp, vrrp, udp, tcp - ili broj iz protocol ID polja) - u slučaju upotrebe naziva ispred tcp, udp i icmp treba staviti \ da se ne bi tumačili kao ključne reči u postavci filtra već kao argument ip proto
- ip6 proto *protokol* je varijanta za IPv6 pakete, a proto *protokol* je varijanta za IPv6 i IPv4 zajedno

filtri

- ether broadcast - ethernet brodkast paket
- ip broadcast - IPv4 brodkast paket (IPv6 ne podržava brodkast pakete)
- ether multicast - eternet multikast paket
- ip multicast - IPv4 multikast paket
- ip6 multicast - IPv6 multikast paket
- ether proto *protokol* - protokol enkapsuliran u eternet okvir - protokol se navodi ili kao broj ili kao naziv (ip, ip6, arp, rarp, ... - i ovde važi napomena da ako neki naziv može da se tumači kao ključna reč treba ispred njega staviti \)

filtri

- Mogu se vršiti i poređenja između izraza upotrebom relacionih operatora >, <, >=, <=, =, !=
- Može se pristupati delovima zaglavlja pojedinih protokola tako što se koriste uglaste zagrade u formatu *protokol [ofset:dužina]* gde *protokol* predstavlja protokol, *ofset* predstavlja od koje pozicije u zaglavlju tog protokola uzimamo bajtove, a *dužina* kaže koliko bajtova uzimamo pri čemu su dozvoljene vrednosti 1, 2 i 4 (*dužina* je opciona i ako se ne navede podrazumeva se vrednost 1)
- Za neke protokole se mogu koristiti i dodatni nazivi za određena polja umesto broja za ofset, ali i vrednosti za flegove koji se mogu koristiti u izrazima
- Na primer, za TCP se mogu koristiti sledeći nazivi za flegove - tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack,tcp-urg, a samo polje ima naziv tcpflags

Primer

```
ubuntu@ubuntu-VirtualBox:~$ tcpdump -D
1.eth0 [Up, Running]
2.eth1 [Up, Running]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.lo [Up, Running, Loopback]
5.bluetooth-monitor (Bluetooth Linux Monitor)
6.nflog (Linux netfilter log (NFLOG) interface)
7.nfqueue (Linux netfilter queue (NFQUEUE) interface)
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
10:53:17.556334 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:53:18.555405 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:53:19.555033 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:53:22.561542 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
4 packets captured
13 packets received by filter
7 packets dropped by kernel
```

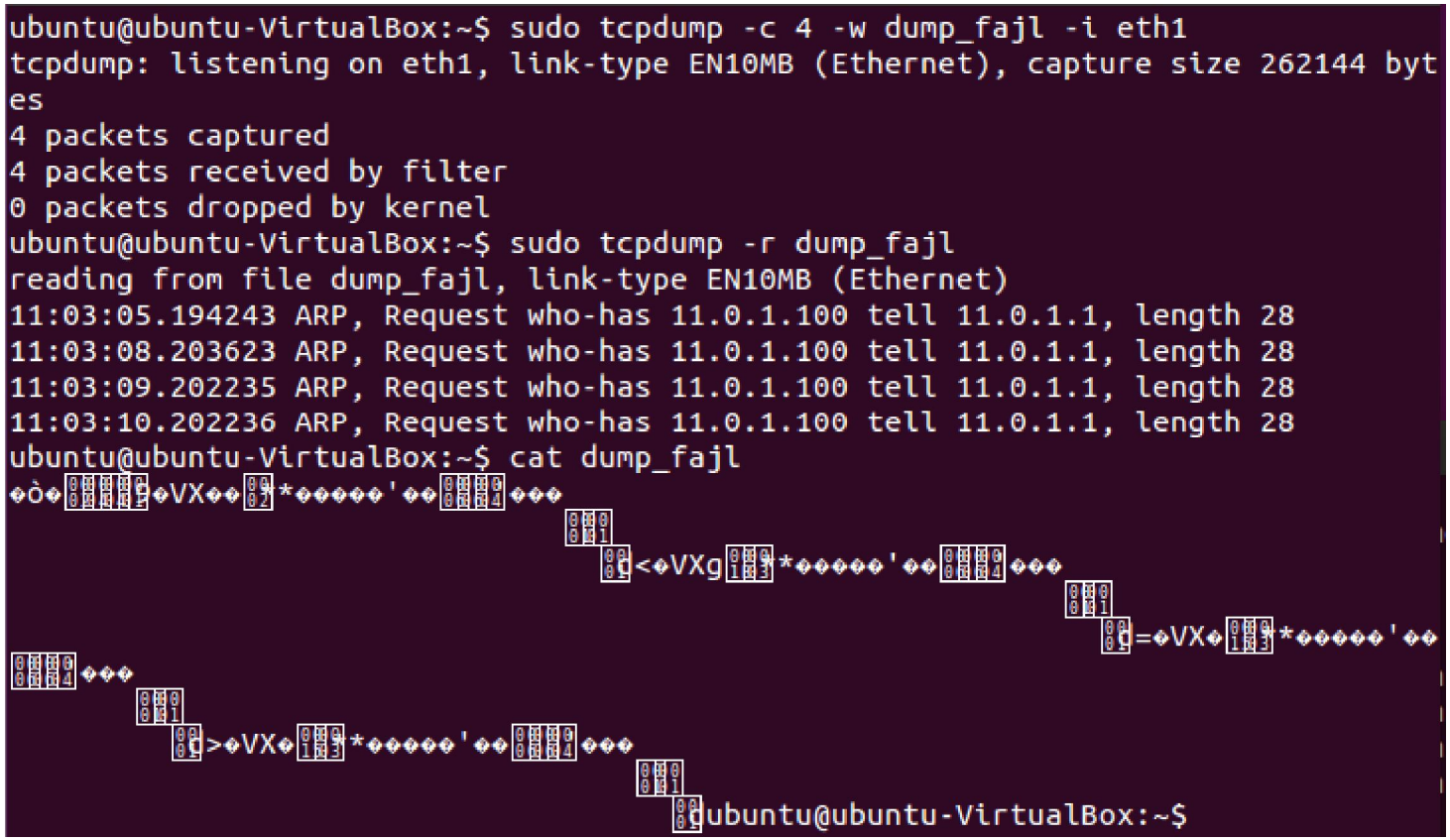
Moraju se koristiti administratorske privilegije za snimanje mrežnog saobraćaja.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i 2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
10:56:57.796478 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:56:58.794237 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:56:59.794239 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
10:57:02.801623 ARP, Request who-has 11.0.1.100 tell 11.0.1.1, length 28
4 packets captured
15 packets received by filter
7 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
10:57:25.822282 IP 11.0.1.1 > 11.0.1.1: ICMP host 89.216.1.30 unreachable, lengt
h 75
10:57:25.822294 IP 11.0.1.1 > 11.0.1.1: ICMP host 89.216.1.50 unreachable, lengt
h 75
10:57:25.822300 IP 11.0.1.1 > 11.0.1.1: ICMP host 89.216.1.30 unreachable, lengt
h 75
10:57:25.822305 IP 11.0.1.1 > 11.0.1.1: ICMP host 89.216.1.50 unreachable, lengt
h 75
4 packets captured
134 packets received by filter
97 packets dropped by kernel
```

Interfejs se može navesti i kao redni broj sa spiska dobijenog opcijom -D. Ako se ne koristi opcija -i onda se interfejs pod rednim brojem 1 u ispisu -D opcijom snima.

Primer



Primer snimanja u fajl i potom čitanja iz njega. Kao što se vidi iz rezultata **cat** komande, zapis nije u čitljivom formatu. Fajl kreiran **tcpdump** komandom i u koga je zapisan sadržaj snimanja se može učitati i u Wireshark alat.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i eth1 ip host 11.0.1.7
[sudo] password for ubuntu:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:19:02.253644 IP 11.0.1.7.45208 > 11.0.1.1.telnet: Flags [S], seq 1234272073,
win 14600, options [mss 1460,sackOK,TS val 402714 ecr 0,nop,wscale 7], length 0
11:19:02.253682 IP 11.0.1.1.telnet > 11.0.1.7.45208: Flags [R.], seq 0, ack 1234
272074, win 0, length 0
11:19:51.652251 IP 11.0.1.7.45209 > 11.0.1.1.telnet: Flags [S], seq 1097553671,
win 14600, options [mss 1460,sackOK,TS val 415064 ecr 0,nop,wscale 7], length 0
11:19:51.652300 IP 11.0.1.1.telnet > 11.0.1.7.45209: Flags [R.], seq 0, ack 1097
553672, win 0, length 0
4 packets captured
16 packets received by filter
12 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i eth1 ether host 08:00:27:f5:27:
2a
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:21:26.632153 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2089, seq 1, lengt
h 64
11:21:26.632204 IP 11.0.1.1 > 11.0.1.7: ICMP echo reply, id 2089, seq 1, length
64
11:21:27.633452 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2089, seq 2, lengt
h 64
11:21:27.633491 IP 11.0.1.1 > 11.0.1.7: ICMP echo reply, id 2089, seq 2, length
64
4 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 4 -i eth1 ether src host 08:00:27:f5
:27:2a
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:22:55.803075 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2091, seq 1, lengt
h 64
11:22:56.802603 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2091, seq 2, lengt
h 64
11:22:57.801711 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2091, seq 3, lengt
h 64
11:22:58.802345 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2091, seq 4, lengt
h 64
4 packets captured
7 packets received by filter
2 packets dropped by kernel
```

Primetiti razliku u odnosu na drugi primer sa prethodnog slajda. Ovde se vidi samo ping request (slat sa drugog hosta), ali ne i reply (od hosta čiji je skrinšot terminala prikazan) jer je u filtru postavljena samo izvorišna MAC adresa.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip src 11.0.1.7
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:25:47.022698 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2092, seq 1, lengt
h 64
11:25:48.023501 IP 11.0.1.7 > 11.0.1.1: ICMP echo request, id 2092, seq 2, lengt
h 64
2 packets captured
4 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip dst 11.0.1.7
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:26:25.278673 IP 11.0.1.1 > 11.0.1.7: ICMP echo reply, id 2094, seq 1, length
64
11:26:26.279208 IP 11.0.1.1 > 11.0.1.7: ICMP echo reply, id 2094, seq 2, length
64
2 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Filtriranje po IP adresi. I ovde je slat ping zahtev sa drugog hosta i može se jasno videti razlika u filtriranju po odredišnoj i izvorišnoj IP adresi. Može se videti iz ova dva primera da reč host može da se izostavi kad se navodi samo izvorišna, odnosno odredišna adresa (tj. ključne reči src i dst)

Primer

Filtriranje po TCP-u i IP-u. U oba primera je podešena izvorišna IP adresa.

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip src 11.0.1.7 and 'tcp[t
cpflags] == tcp-syn'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:43:17.829080 IP 11.0.1.7.45210 > 11.0.1.1.telnet: Flags [S], seq 453787090, w
in 14600, options [mss 1460,sackOK,TS val 766609 ecr 0,nop,wscale 7], length 0
11:43:21.398546 IP 11.0.1.7.45211 > 11.0.1.1.telnet: Flags [S], seq 4068621320,
win 14600, options [mss 1460,sackOK,TS val 767502 ecr 0,nop,wscale 7], length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip src 11.0.1.7 and 'tcp[t
cpflags] & tcp-syn != 0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:44:32.974743 IP 11.0.1.7.45212 > 11.0.1.1.telnet: Flags [S], seq 1441561934,
win 14600, options [mss 1460,sackOK,TS val 785396 ecr 0,nop,wscale 7], length 0
11:44:35.942382 IP 11.0.1.7.45213 > 11.0.1.1.telnet: Flags [S], seq 2986378853,
win 14600, options [mss 1460,sackOK,TS val 786138 ecr 0,nop,wscale 7], length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

U prvom primeru FLAGS polje u TCP zaglavlju treba da ima aktiviran samo SYN fleg (i nijedan drugi), a u drugom primeru takođe treba biti aktiviran SYN fleg, ali istovremeno mogu biti aktivirani i drugi flegovi. Prvi primer bi trebao hvatati samo otvaranje TCP konekcije (prvi paket) pokrenuto sa navedene IP adrese, a drugi potencijalno može hvatati i paket koji je prvi odgovor na otvaranje TCP konekcije koju je pokrenuo host čiji je skrinšot prikazan ka hostu sa adresom 11.0.1.7.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip host 11.0.1.7 and 'tcp[
tcpflags] & tcp-syn != 0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
12:15:50.861713 IP 11.0.1.7.45218 > 11.0.1.1.telnet: Flags [S], seq 1935766996,
win 14600, options [mss 1460,sackOK,TS val 1254870 ecr 0,nop,wscale 7], length 0
12:15:50.861758 IP 11.0.1.1.telnet > 11.0.1.7.45218: Flags [S.], seq 1794810252,
 ack 1935766997, win 28960, options [mss 1460,sackOK,TS val 4363928 ecr 1254870,
nop,wscale 7], length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Slično drugom primeru sa prethodnog slajda, samo sada IP adresa može biti i izvorišna i odredišna. Može se videti da je filtar uhvatio i paket koji je drugi po redu u otvaranju TCP veze (i koji ima i ACK fleg aktivan). Primetiti da je na prethodnom i ovom slajdu deo izraza vezan za definisanje filtra stavljen pod navodnike da se izbegnu greške u tumačenju pojedinih karaktera od strane shell-a.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip proto '\tcp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
12:54:45.989896 IP 11.0.1.7.45219 > 11.0.1.1.telnet: Flags [P.], seq 944850496:9
44850499, ack 1786045880, win 115, options [nop,nop,TS val 1838655 ecr 4936147],
 length 3
12:54:45.990037 IP 11.0.1.1.telnet > 11.0.1.7.45219: Flags [P.], seq 1:5, ack 3,
 win 227, options [nop,nop,TS val 4947710 ecr 1838655], length 4
2 packets captured
23 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 2 -i eth1 ip proto 6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
12:55:32.950397 IP 11.0.1.7.45220 > 11.0.1.1.telnet: Flags [S], seq 440578076, w
in 14600, options [mss 1460,sackOK,TS val 1850395 ecr 0,nop,wscale 7], length 0
12:55:32.950455 IP 11.0.1.1.telnet > 11.0.1.7.45220: Flags [S.], seq 4012489685,
 ack 440578077, win 28960, options [mss 1460,sackOK,TS val 4959451 ecr 1850395,n
op,wscale 7], length 0
2 packets captured
70 packets received by filter
65 packets dropped by kernel
```

Primetiti da pored upotrebe escape karaktera ispred tcp treba staviti i navodnike. Drugi primer pokazuje da se može koristiti i brojna vrednost - vrednost 6 odgovara TCP protokolu (to je vrednost protocol ID polja u IPv4 zaglavlju za TCP pakete).

Detaljniji prikaz

- Ako se želi detaljniji prikaz može se koristiti opcija -v ili -vv za još detaljniji prikaz

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -vv -c 2 -i eth1 ip proto 6
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 byt
es
13:01:37.750891 IP (tos 0x10, ttl 64, id 8331, offset 0, flags [DF], proto TCP (
6), length 60)
    11.0.1.7.45221 > 11.0.1.1.telnet: Flags [S], cksum 0x1534 (correct), seq 263
684304, win 14600, options [mss 1460,sackOK,TS val 1941595 ecr 0,nop,wscale 7],
length 0
13:01:37.750926 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
length 60)
    11.0.1.1.telnet > 11.0.1.7.45221: Flags [S.], cksum 0x1836 (incorrect -> 0xd
944), seq 1945337450, ack 263684305, win 28960, options [mss 1460,sackOK,TS val
5050651 ecr 1941595,nop,wscale 7], length 0
2 packets captured
70 packets received by filter
65 packets dropped by kernel
```

Može se videti da je prikaz detaljniji nego za isti slučaj kada nije korišćena -vv opcija na prethodnom slajdu.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 8 ip host 147.91.14.197
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:35:52.001659 IP 10.0.2.15.37189 > vhost4.etf.bg.ac.rs.http: Flags [S], seq 38
70192824, win 29200, options [mss 1460,sackOK,TS val 208041 ecr 0,nop,wscale 7],
 length 0
13:35:52.009727 IP vhost4.etf.bg.ac.rs.http > 10.0.2.15.37189: Flags [S.], seq 1
6960001, ack 3870192825, win 65535, options [mss 1460], length 0
13:35:52.009751 IP 10.0.2.15.37189 > vhost4.etf.bg.ac.rs.http: Flags [.], ack 1,
 win 29200, length 0
13:35:52.012457 IP 10.0.2.15.37189 > vhost4.etf.bg.ac.rs.http: Flags [P.], seq 1
:289, ack 1, win 29200, length 288
13:35:52.012614 IP vhost4.etf.bg.ac.rs.http > 10.0.2.15.37189: Flags [.], ack 28
9, win 65535, length 0
13:35:52.025236 IP vhost4.etf.bg.ac.rs.http > 10.0.2.15.37189: Flags [P.], seq 1
:495, ack 289, win 65535, length 494
13:35:52.025236 IP 10.0.2.15.37189 > vhost4.etf.bg.ac.rs.http: Flags [.], ack 49
5, win 30016, length 0
13:35:52.025236 IP vhost4.etf.bg.ac.rs.http > 10.0.2.15.37189: Flags [F.], seq 4
95, ack 289, win 65535, length 0
8 packets captured
289 packets received by filter
0 packets dropped by kernel
```

Prikaz paketa pri povezivanju na sajt fakulteta.

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 8 -vv ip host 147.91.14.197
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
13:37:53.096254 IP (tos 0x0, ttl 64, id 30552, offset 0, flags [DF], proto TCP (
6), length 60)
    10.0.2.15.37229 > vhost4.etf.bg.ac.rs.http: Flags [S], cksum 0xae5d (incorre
ct -> 0x6ebd), seq 2929972659, win 29200, options [mss 1460,sackOK,TS val 238315
 ecr 0,nop,wscale 7], length 0
13:37:53.104592 IP (tos 0x0, ttl 64, id 6502, offset 0, flags [none], proto TCP
(6), length 44)
    vhost4.etf.bg.ac.rs.http > 10.0.2.15.37229: Flags [S.], cksum 0x73c2 (correc
t), seq 34496001, ack 2929972660, win 65535, options [mss 1460], length 0
13:37:53.104618 IP (tos 0x0, ttl 64, id 30553, offset 0, flags [DF], proto TCP (
6), length 40)
    10.0.2.15.37229 > vhost4.etf.bg.ac.rs.http: Flags [.], cksum 0xae49 (incorre
ct -> 0x196f), seq 1, ack 1, win 29200, length 0
13:37:53.104788 IP (tos 0x0, ttl 64, id 30554, offset 0, flags [DF], proto TCP (
6), length 328)
    10.0.2.15.37229 > vhost4.etf.bg.ac.rs.http: Flags [P.], cksum 0xaf69 (incorr
ect -> 0xaf7b), seq 1:289, ack 1, win 29200, length 288
13:37:53.105038 IP (tos 0x0, ttl 64, id 6503, offset 0, flags [none], proto TCP
(6), length 40)
    vhost4.etf.bg.ac.rs.http > 10.0.2.15.37229: Flags [.], cksum 0x8a5f (correct
), seq 1, ack 289, win 65535, length 0
13:37:53.115337 IP (tos 0x0, ttl 64, id 6504, offset 0, flags [none], proto TCP
(6), length 534)
    vhost4.etf.bg.ac.rs.http > 10.0.2.15.37229: Flags [P.], cksum 0xade6 (correc
t), seq 1:495, ack 289, win 65535, length 494
```

Prikaz paketa pri povezivanju na sajt fakulteta ali uz opciju -vv.

Upotreba -XX opcije

Opcije -X i -XX daju prikaz i ASCII i heksadecimalnog formata zaglavlja i data dela. Razlika je što -XX uključuje i sloj 2 informacije.

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 8 -XX ip host 147.91.14.197
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:40:59.286095 IP 10.0.2.15.37427 > vhost4.etf.bg.ac.rs.http: Flags [S], seq 24
65497950, win 29200, options [mss 1460,sackOK,TS val 284862 ecr 0,nop,wscale 7],
 length 0
        0x0000:  5254 0012 3502 0800 271b bce9 0800 4500  RT..5...'.....E.
        0x0010:  003c dbe0 4000 4006 b0ac 0a00 020f 935b  .<..@.@........[
        0x0020:  0ec5 9233 0050 92f4 835e 0000 0000 a002  ...3.P...^......
        0x0030:  7210 ae5d 0000 0204 05b4 0402 080a 0004  r..]............
        0x0040:  58be 0000 0000 0103 0307                 X.........
13:40:59.296521 IP vhost4.etf.bg.ac.rs.http > 10.0.2.15.37427: Flags [S.], seq 6
8736001, ack 2465497951, win 65535, options [mss 1460], length 0
        0x0000:  0800 271b bce9 5254 0012 3502 0800 4500  ..'...RT..5...E.
        0x0010:  002c 3ee7 0000 4006 8db6 935b 0ec5 0a00  .,>...@....[....
        0x0020:  020f 0050 9233 0418 d401 92f4 835f 6012  ...P.3......._`.
        0x0030:  ffff 68f6 0000 0204 05b4 0000            ..h.........
```

Varijanta sa -x i -xx radi samo prikaz heksadecimalnih vrednosti.

```
        0x0030:  7210 b09a 0000 4745 5420 2f20 4854 5450  r.....GET./.HTTP
        0x0040:  2f31 2e31 0d0a 486f 7374 3a20 7777 772e  /1.1..Host:.www.
        0x0050:  6574 662e 6267 2e61 632e 7273 0d0a 5573  etf.bg.ac.rs..Us
        0x0060:  6572 2d41 6765 6e74 3a20 4d6f 7a69 6c6c  er-Agent:.Mozill
        0x0070:  612f 352e 3020 2858 3131 3b20 5562 756e  a/5.0.(X11;.Ubun
        0x0080:  7475 3b20 4c69 6e75 7820 7838 365f 3634  tu;.Linux.x86_64
        0x0090:  3b20 7276 3a34 342e 3029 2047 6563 6b6f  ;.rv:44.0).Gecko
        0x00a0:  2f32 3031 3030 3130 3120 4669 7265 666f  /20100101.Firefo
        0x00b0:  782f 3434 2e30 0d0a 4163 6365 7074 3a20  x/44.0..Accept:.
        0x00c0:  7465 7874 2f68 746d 6c2c 6170 706c 6963  text/html,applic
        0x00d0:  6174 696f 6e2f 7868 746d 6c2b 786d 6c2c  ation/xhtml+xml,
        0x00e0:  6170 706c 6963 6174 696f 6e2f 786d 6c3b  application/xml;
        0x00f0:  713d 302e 392c 2a2f 2a3b 713d 302e 380d  q=0.9,*/*;q=0.8.
        0x0100:  0a41 6363 6570 742d 4c61 6e67 7561 6765  .Accept-Language
        0x0110:  3a20 656e 2d55 532c 656e 3b71 3d30 2e35  :.en-US,en;q=0.5
        0x0120:  0d0a 4163 6365 7074 2d45 6e63 6f64 696e  ..Accept-Encodin
        0x0130:  673a 2067 7a69 702c 2064 6566 6c61 7465  g:.gzip,.deflate
```

Primer

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -X -c 1 -i eth0 ip proto 6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:52:09.306966 IP 10.0.2.15.50572 > muc03s14-in-f10.1e100.net.http: Flags [.],
ack 117538105, win 65320, length 0
        0x0000:  4500 0028 a65d 4000 4006 dcfe 0a00 020f  E..(.]@.@.......
        0x0010:  d83a d32a c58c 0050 3e36 0b39 0701 7d39  .:.*...P>6.9..}9
        0x0020:  5010 ff28 b78e 0000                      P..(....
1 packet captured
2 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -XX -c 1 -i eth0 ip proto 6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:52:19.323022 IP 10.0.2.15.50572 > muc03s14-in-f42.1e100.net.http: Flags [.],
ack 117538105, win 65320, length 0
        0x0000:  5254 0012 3502 0800 271b bce9 0800 4500  RT..5...'.....E.
        0x0010:  0028 a65e 4000 4006 dcfd 0a00 020f d83a  .(.^@.@........:
        0x0020:  d32a c58c 0050 3e36 0b39 0701 7d39 5010  .*...P>6.9..}9P.
        0x0030:  ff28 b78e 0000                           .(....
1 packet captured
2 packets received by filter
0 packets dropped by kernel
```

4500 predstavlja standardni početak IPv4 zaglavlja u heksadecimalnom formatu. Može se videti u drugom primeru da ispred njega sada stoji i zaglavlje sloja 2. Na slajdu 4 se može videti da je MAC adresa eth0 interfejsa 0800271bbce9.

Primer

Primetiti da su svi podaci upisani u fajl, a možemo kontrolisati format ispisa kada čitamo ranije snimljen sadržaj iz fajla.

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 1 -i eth0 ip proto 6 -w dumpfajl
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
1 packet captured
13 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -r dumpfajl
reading from file dumpfajl, link-type EN10MB (Ethernet)
13:59:03.049275 IP 10.0.2.15.37473 > vhost4.etf.bg.ac.rs.http: Flags [S], seq 25
4643658, win 29200, options [mss 1460,sackOK,TS val 555803 ecr 0,nop,wscale 7],
length 0
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -XX -r dumpfajl
reading from file dumpfajl, link-type EN10MB (Ethernet)
13:59:03.049275 IP 10.0.2.15.37473 > vhost4.etf.bg.ac.rs.http: Flags [S], seq 25
4643658, win 29200, options [mss 1460,sackOK,TS val 555803 ecr 0,nop,wscale 7],
length 0
        0x0000:  5254 0012 3502 0800 271b bce9 0800 4500  RT..5...'.....E.
        0x0010:  003c f6d1 4000 4006 95bb 0a00 020f 935b  .<..@.@........[
        0x0020:  0ec5 9261 0050 0f2d 8dca 0000 0000 a002  ...a.P.-........
        0x0030:  7210 ae5d 0000 0204 05b4 0402 080a 0008  r..]............
        0x0040:  7b1b 0000 0000 0103 0307                 {.........
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -xx -r dumpfajl
reading from file dumpfajl, link-type EN10MB (Ethernet)
13:59:03.049275 IP 10.0.2.15.37473 > vhost4.etf.bg.ac.rs.http: Flags [S], seq 25
4643658, win 29200, options [mss 1460,sackOK,TS val 555803 ecr 0,nop,wscale 7],
length 0
        0x0000:  5254 0012 3502 0800 271b bce9 0800 4500
        0x0010:  003c f6d1 4000 4006 95bb 0a00 020f 935b
        0x0020:  0ec5 9261 0050 0f2d 8dca 0000 0000 a002
        0x0030:  7210 ae5d 0000 0204 05b4 0402 080a 0008
        0x0040:  7b1b 0000 0000 0103 0307
```

Napomena

- U većini komandi (tcpdump, netstat, route, arp) rađenih u ovoj prezentaciji postoji i opcija -n
- Ova opcija sprečava da se vrednosti adresa ili portova prevedu u nazive
- Na primer, na slajdu 80 se može videti naziv veb servera fakulteta - opcija -n bi sprečila prevođenje što se vidi na primeru datom na ovom slajdu

```
ubuntu@ubuntu-VirtualBox:~$ sudo tcpdump -c 8 -n ip host 147.91.14.197
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:04:38.227321 IP 10.0.2.15.37479 > 147.91.14.197.80: Flags [S], seq 2541199635
, win 29200, options [mss 1460,sackOK,TS val 639598 ecr 0,nop,wscale 7], length
0
14:04:38.236627 IP 147.91.14.197.80 > 10.0.2.15.37479: Flags [S.], seq 161216001
, ack 2541199636, win 65535, options [mss 1460], length 0
14:04:38.236753 IP 10.0.2.15.37479 > 147.91.14.197.80: Flags [.], ack 1, win 292
00, length 0
```

Udaljeni pristup

- Omogućavanje udaljenog pristupa nekom računaru može biti korisno iz više razloga - više korisnika može istovremeno da koristi resurse računara, debagovanje prilikom razvoja i dr.
- Telnet udaljeni pristup predstavlja jedno od najstarijih rešenja
- Drugo popularno rešenje je SSH

Telnet

- Telnet udaljeni pristup predstavlja jedno od najstarijih rešenja
- Prednost telneta je što je veoma jednostavan za konfigurisanje i upotrebu
- Na mašini kojoj se želi pristupiti je potrebno podignuti telnet server, a na klijent računaru treba imati instaliran telnet klijent (što je uglavnom uvek prisutno u distribucijama)
- Najveća mana telneta je što nije dovoljno siguran - po difoltu se ne vrši enkripcija i npr. lozinka je vidljiva
- Ali zbog jednostavnosti se još uvek koristi kada sigurnost nije bitna ili je fizički obezbeđeno da ne može doći do prisluškivanja

Telnet

- Telnet klijent je uglavnom već prisutan u većini distribucija, dok telnet server uglavnom treba instalirati
- Uz telnet server je potrebno instalirati i xinetd (ako nije instaliran)
- Na ubuntu distribuciji instalacija se vrši sa **sudo apt-get install xinetd telnetd**
- Potrebno je kreirati fajl *telnet* u */etc/xinetd.d* folderu i popuniti ga odgovarajućim sadržajem koje predstavlja postavke telnet servera
- Isto tako potrebno je u fajl /etc/inetd.conf dopisati liniju

telnet stream tcp nowait telnet /usr/sbin/tcpd /usr/sbin/in.telnetd

- U novijim distribucijama inetd.conf fajl ne postoji i potrebno ga je kreirati (xinetd predstavlja naslednika inetd, ali zbog problema kompatibilnosti telnet aplikacije potrebno je kreirati ovaj fajl)
- Restartovati xinetd servis sa **sudo service xinetd restart**

Telnet

- Primer sadržaja fajla *telnet* u */etc/xinetd.d* folderu

```
service telnet
{
  disable = no
  flags = REUSE
  socket_type = stream
  wait = no
  user = root
  server = /usr/sbin/in.telnetd
  log_on_failure += USERID
  log_on_success+= PID HOST EXIT
  log_type = FILE /var/log/xinetd.log
}
```

Primer

Primer povezivanja sa drugog računara. U ovom slučaju je korišćen računar na kome je instaliran Linux Mint (mogao je biti i Windows računar). Kao što se vidi dovoljno je ukucati iza **telnet** komande IP adresu udaljenog računara. Ispis **whoami** komande pokazuje da je zaista ostvaren udaljen pristup.

```
mint@mint-VirtualBox ~ $ ls
Desktop    Downloads  novidocument  Public     Videos
Documents  Music      Pictures      Templates
mint@mint-VirtualBox ~ $ whoami
mint
mint@mint-VirtualBox ~ $ telnet 11.0.1.1
Trying 11.0.1.1...
Connected to 11.0.1.1.
Escape character is '^]'.
Ubuntu 15.04
ubuntu-VirtualBox login: ubuntu
Password:
Last login: Sun Dec 18 14:29:24 EST 2016 from 11.0.1.7 on pts/1
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

ubuntu@ubuntu-VirtualBox:~$ whoami
ubuntu
ubuntu@ubuntu-VirtualBox:~$ exit
logout
Connection closed by foreign host.
```

Telnet

- Na prethodnom slajdu je dat jednostavan prikaz udaljenog povezivanja
- Sve komande koje su dostupne kada se samo aktivira **telnet** ili sve opcije koje su na raspolaganju se mogu videti u man uputstvu **telnet** komande

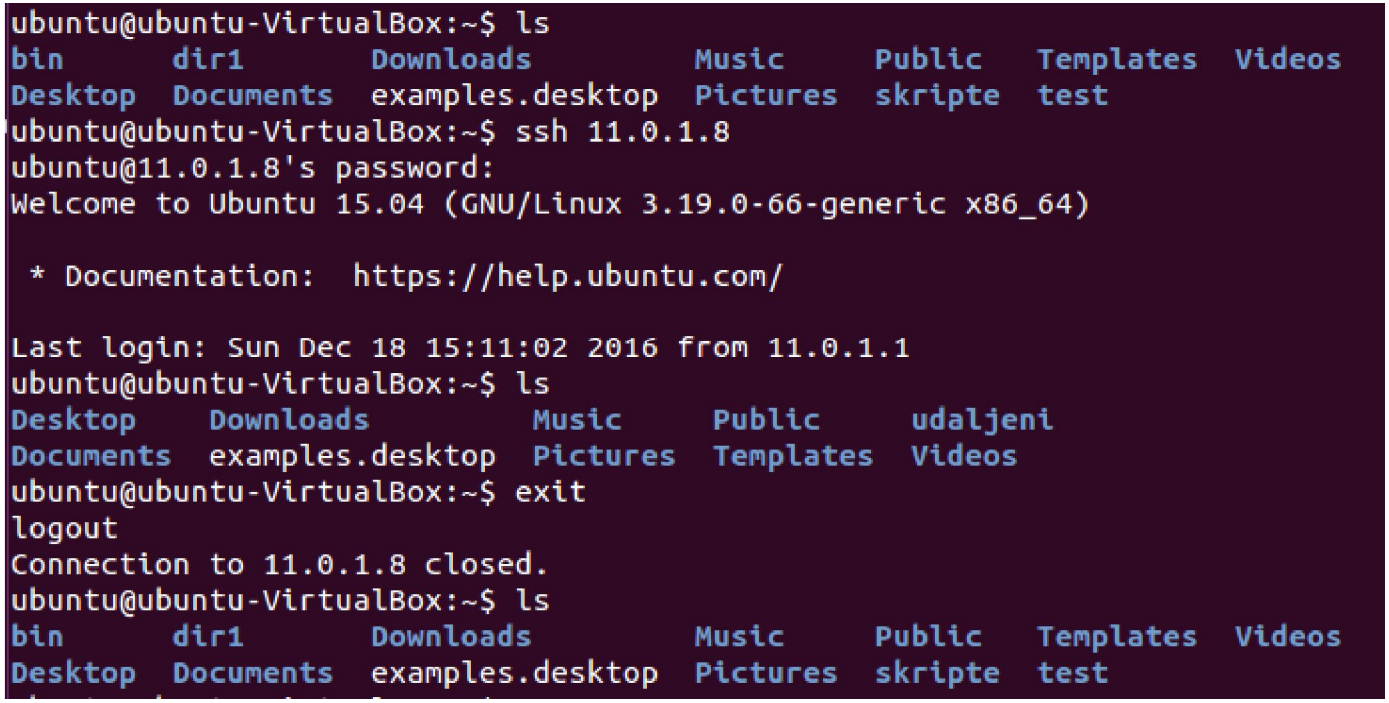
Komanda **open** u telnet promptu otvara konekciju ka navedenom udaljenom hostu.

```
mint@mint-VirtualBox ~ $ telnet
telnet> open 11.0.1.1
Trying 11.0.1.1...
Connected to 11.0.1.1.
Escape character is '^]'.
Ubuntu 15.04
ubuntu-VirtualBox login: ubuntu
Password:
Last login: Sun Dec 18 14:30:18 EST 2016 from 11.0.1.7 on pts/1
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

ubuntu@ubuntu-VirtualBox:~$ logout
```

OpenSSH

- Preporuka za udaljeni pristup je upotreba SSH zbog bolje bezbednosti u odnosu na telnet
- Kao i kod telnet-a potrebno je da se na udaljenoj strani instalira SSH server, a na klijent strani SSH klijent
- Da bi se server instalirao na Ubuntu distribuciji **sudo apt-get install openssh-server**
- Fajl */etc/ssh/sshd_config* predstavlja konfiguracioni fajl za SSH server, a */etc/ssh/ssh_config* za SSH klijenta
- Postoji velik broj opcija koje se mogu videti u man uputstvu za **ssh** komandu
- Samo logovanje na udaljeni računar u svojoj najjednostavnijoj varijanti se izvodi sa **ssh** *udaljenihost* ako se korisnička imena poklapaju, odnosno sa **ssh** *ime@udaljenihost* ako se ne poklapaju (korisničko ime naloga na udaljenom računaru)

OpenSSH



Primer logovanja u slučaju kada nalog na udaljenom računaru ima isto korisničko ime.

OpenSSH

```
ubuntu@ubuntu-VirtualBox:~$ ssh marko@11.0.1.1
The authenticity of host '11.0.1.1 (11.0.1.1)' can't be established.
ECDSA key fingerprint is d0:92:67:f3:b4:0e:28:0b:9d:b5:ff:49:14:62:21:7f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '11.0.1.1' (ECDSA) to the list of known hosts.
marko@11.0.1.1's password:
```

Prilikom prvog povezivanja prijavljuje se da je u pitanju nepoznati udaljeni računar i postavlja se pitanje da li da se doda u listu poznatih hostova tako da se ovo pitanje ne pojavljuje u budućnosti.

Primer kada se korisnička imena razlikuju. Sa **whoami** komandom možemo videti da je ostvaren udaljen pristup. Primetiti da sada nema pitanja kao na slici iznad.

```
ubuntu@ubuntu-VirtualBox:~$ whoami
ubuntu
ubuntu@ubuntu-VirtualBox:~$ ssh marko@11.0.1.1
marko@11.0.1.1's password:
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Sun Dec 18 15:29:00 2016 from 11.0.1.8
marko@ubuntu-VirtualBox:~$ whoami
marko
marko@ubuntu-VirtualBox:~$ exit
logout
Connection to 11.0.1.1 closed.
ubuntu@ubuntu-VirtualBox:~$
```