

## Vežba 2 – Mrežni dijagnostički alati

### 1. Provera funkcionisanja IP protokola - Ping

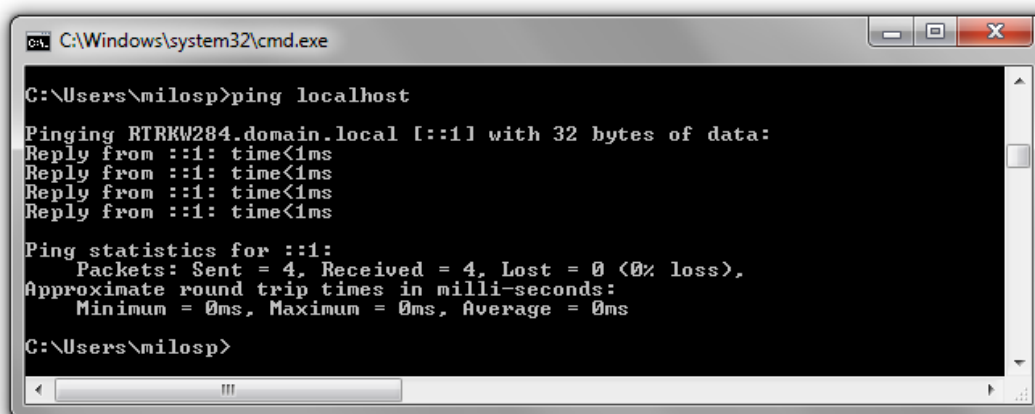
Postoji uobičajena procedura za proveru funkcionisanja IP protokola na računaru i otkrivanje problema. Procedura se oslanja na jednostavnu komandu – *ping*. Ovaj dijagnostički alat, dostupan na velikoj većini mrežnih operativnih sistema omogućava da se na proizvoljnu adresu pošalju posebne poruke “*Echo Request*”. Računar koji primi ovakvu poruku odgovara sa “*Echo Replay*” porukom. Ukoliko računar dobije odgovor na svoju “*Echo*” poruku može se zaključiti da između dva računara mreža funkcioniše na 1., 2., i 3. sloju OSI modela. Za slanje poruka se koristi protokol pod nazivom ICMP (engl. *Internet Control Message Protocol*) koji funkcioniše na 3. sloju OSI modela.

U komandnoj liniji (terminalu) uneti: **ping <127.0.0.1>**

Ovo je adresa takozvane lokalne petlje (engl. *loopback*), softverski implementiranog interfejsa na svakom računaru koji ima instaliran TCP/IP. Ukoliko se ne dobiju nikakvi ECHO odgovori to znači da IP protokol nije instaliran na računaru.

U komandnoj liniji uneti: **ping <ip\_adresa\_lokalnog\_računara>**

odnosno *ping* na sopstvenu IP adresu (slika 1). Ukoliko se ne dobiju ECHO odgovori, to bi moglo da sugeriše da IP protokol nije vezan za mrežni adapter, zbog pogrešne konfiguracije ili fizičkog kvara adaptera.



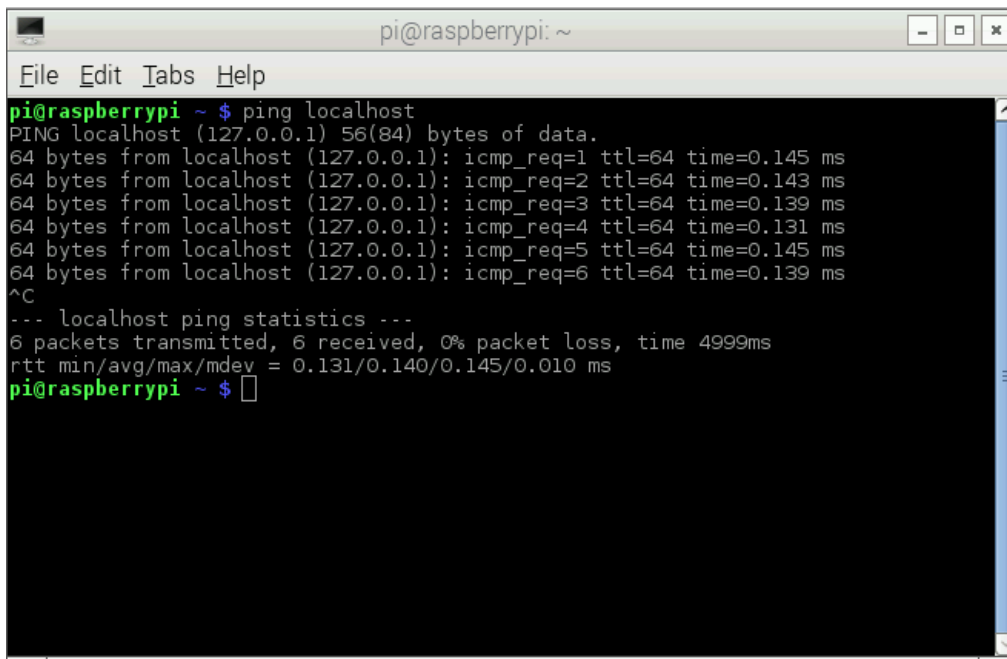
```
C:\Windows\system32\cmd.exe

C:\Users\milosp>ping localhost

Pinging RTRKW284.domain.local [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\milosp>
```



```
pi@raspberrypi ~ $ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_req=1 ttl=64 time=0.145 ms
64 bytes from localhost (127.0.0.1): icmp_req=2 ttl=64 time=0.143 ms
64 bytes from localhost (127.0.0.1): icmp_req=3 ttl=64 time=0.139 ms
64 bytes from localhost (127.0.0.1): icmp_req=4 ttl=64 time=0.131 ms
64 bytes from localhost (127.0.0.1): icmp_req=5 ttl=64 time=0.145 ms
64 bytes from localhost (127.0.0.1): icmp_req=6 ttl=64 time=0.139 ms
^C
--- localhost ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.131/0.140/0.145/0.010 ms
pi@raspberrypi ~ $
```

Slika 1. Primer *ping*-a sopstvene IP adrese u Windows/Raspbian terminalu

U komandnoj liniji uneti: **ping <ip\_adresa\_default\_gateway-a>**

Za ovaj korak bi se mogla koristiti bilo koja adresa u lokalnoj mreži (npr. adresa susednog računara) a obično je to IP adresa podrazumevanog mrežnog prolaza (engl. *default gateway*). Ovaj korak proverava povezanost računara u lokalnoj mreži. Ukoliko se ne dobiju ECHO odgovori to bi moglo da znači da postoji problem sa vezom računara na mrežu.

U komandnoj liniji uneti: **ping <10.0.0.5>**

predstavlja adresu nekog računara na drugoj mreži. Ukoliko se dobiju ECHO odgovori možemo znati da je konfigurisani podrazumevani mrežni prolaz ispravan.

U komandnoj liniji uneti: **ping <www.blic.rs>**

ukoliko se u *ping* komandi referišemo na ime računara i dobijemo ECHO odgovor, posredno znamo i da razrešavanje imena uz konfigurisani DNS server funkcioniše.

Obratiti pažnju i na odgovore na *ping*. Prikazano je povratno vreme RTT (engl. *Round Trip Time*) i TTL (engl. *Time To Live*) vrednost koja je poslata u paketima. Posle *N* odgovora (za Windows OS *N* je jednako 4 kao unapred definisana (engl. *default*) vrednost) prikazano je i minimalno, maksimalno i prosečno povratno vreme kao i procenat izgubljenih paketa.

#### Napomena:

Windows OS: Ostale opcije Ping komande se mogu pogledati **ping /?** komandom.

Raspbian (Linux): Ostale opcije Ping komande se mogu pogledati sa **man ping** ili **info ping** komandama.

Za zaustavljanje izvršavanja *ping* komande tj. procesa koristi se kombinacija tastera *CTRL+C* na tastaturi.

## Pingovanje udaljenog računara – poruke o grešci

Ukoliko *ping* prema računaru na nekoj bližoj ili daljoj mreži ne uspe, moguće su četiri poruke o greškama:

<i>TTL Expired in Transit</i>	<p>Broj potrebnih skokova (čvorova) da bi se stiglo do odredišta veći je od vrednosti TTL koju je računar pošiljalac postavio za slanje paketa.</p> <p>Potrebno je povećati TTL koristeći opciju <b>ping -i TTL</b> (max. do 255) (Windows) tj. <b>ping -t TTL</b>(Raspbian)</p>
<i>Destination Host Unreachable</i>	<p>Lokalni ili udaljeni računar nema put do željenog odredišta.</p> <p>Ukoliko poruka glasi “<i>Destination Host Unreachable</i>“ znači da ne postoji putanja od lokalnog računara i da paketi koje treba poslati nisu ni postavljeni na prenosni medijum.</p> <p>Ako poruka glasi “<i>Replay from &lt;IP adresa&gt;: Destination Host Unreachable</i>“ znači da je do problema u preusmeravanju paketa kroz mrežu došlo na usmerivaču čija je IP adresa navedena u poruci.</p>
<i>Request Timed Out</i>	<p>U podrazumevanom vremenskom intervalu od 1 sekunde nije primljen ICMP odgovor <i>Echo Replay</i>. Razloga ima više: zagušenje mreže, neuspeh ARP zahteva, filtriranje paketa, greška u rutiranju itd.</p> <p>Najšeeće ova poruka znači da odredišni računar ili neki od usmerivača (moguće i defaultni gateway odredišnog računara) “ne zna” put nazad ka računaru koji je inicirao ping.</p> <p>Zagušenje mreže može se prepoznati ako jednostavno produžimo vreme čekanja koristeći <b>ping-w timeout</b> opciju (u milisekundama-Windows) tj. <b>ping-w timeout</b> (u sekundama-Raspbian)</p>
<i>Unknown host</i>	<p>Zahtevano ime računara ne može se prevesti u IP adresu. Potrebno je proveriti da li je ime mrežnog čvora pravilno napisano i da li su dostupni DNS serveri.</p>

## 2. Tracert (Windows) / traceroute (Raspbian)

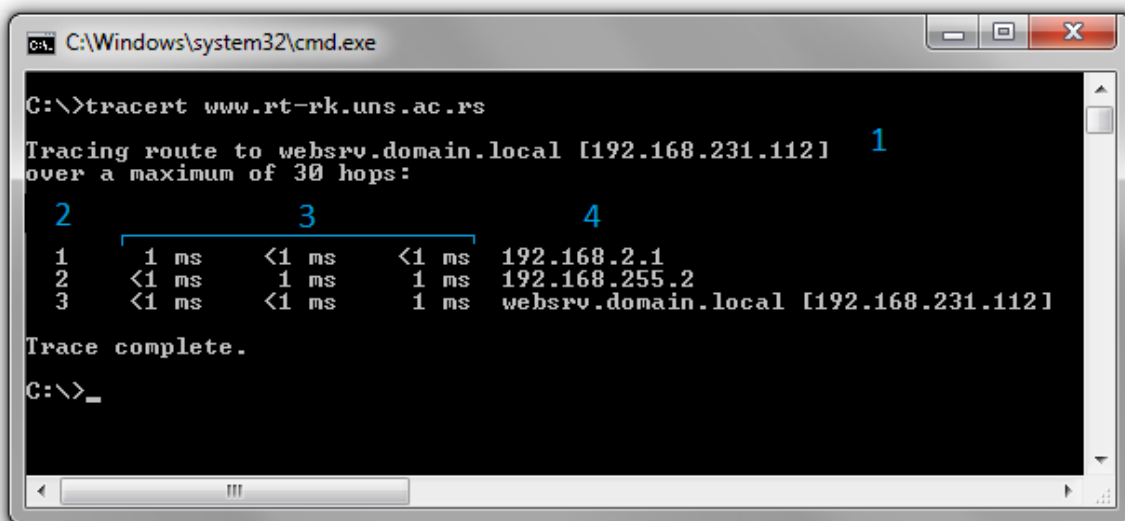
Predstavljaju pomoćne programe za proveravanje putanje kojom paket putuje na svom putu od izvorišnog računara do odredišta. Rezultat programa je lista interfejsa svih usmerivača (engl. *router*) kroz koje je paket prošao na svom putu ka odredištu.

Koristeći TTL polje u ICMP poruci “*Echo Request*” i ICMP poruku “*Time Exceeded*”, *tracert* je u mogućnosti da odredi putanju od izvora do odredišta kroz međusobno povezane IP mreže.

Raspbian (Linux) verzija *traceroute* programa se razlikuje od Windows *tracert* verzije po tome što koristi Van Jacobson-ovu modifikaciju koristeći neregistrovani odredišni broj UDP

porta (*outbound*) i oslanjajući se na ICMP *Destination Unreachable/Port Unreachable* poruke o grešci kao naznaku kraja *traceroute* procesa.

Neki usmerivači ne vraćaju “*Time Exceeded*” poruku za pakete sa nultim TTL vrednostima pa su kao takvi “nevidljivi” za *tracert* tj. *traceroute*. U tom slučaju, red zvezdica (\*) se prikazuje za taj čvor (izvorišni računar očekuje odgovor u zadatom vremenskom intervalu – ako u okviru istog ne pristigne odgovor ispisuje se red zvezdica (\*)) . Slanje paketa iz jednog sistema u drugi *tracert* tj. *traceroute* označavaju kroz skokove (engl. *hops*), gde svaki mrežni čvor kroz koji paket prolazi predstavlja jedan skok. Svaki red tabele predstavlja informacije dobijene od čvora na putanji između izvorišnog čvora i odredišta.



```
C:\Windows\system32\cmd.exe

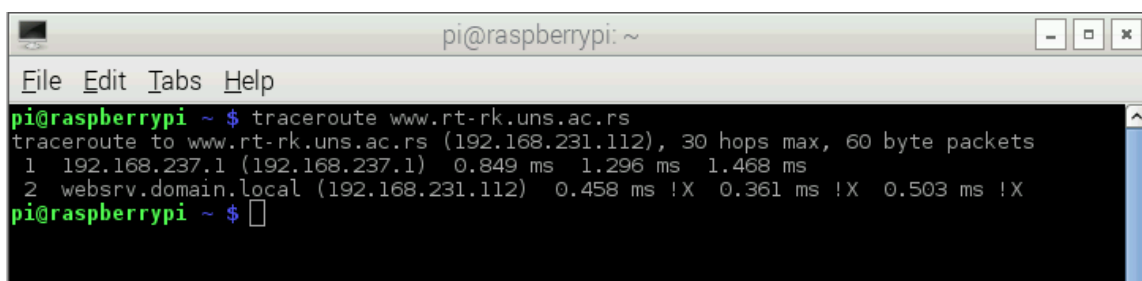
C:\>tracert www.rt-rk.uns.ac.rs

Tracing route to webserv.domain.local [192.168.231.112] 1
over a maximum of 30 hops:

 2      3      4
 1      1 ms  <1 ms  <1 ms  192.168.2.1
 2      <1 ms  1 ms  1 ms  192.168.255.2
 3      <1 ms  <1 ms  1 ms  webserv.domain.local [192.168.231.112]

Trace complete.

C:\>_
```



```
pi@raspberrypi: ~
File Edit Tabs Help

pi@raspberrypi ~ $ traceroute www.rt-rk.uns.ac.rs
traceroute to www.rt-rk.uns.ac.rs (192.168.231.112), 30 hops max, 60 byte packets
 1  192.168.237.1 (192.168.237.1)  0.849 ms  1.296 ms  1.468 ms
 2  webserv.domain.local (192.168.231.112)  0.458 ms !X  0.361 ms !X  0.503 ms !X
pi@raspberrypi ~ $
```

Slika 2. *Tracert* (Windows) i *traceroute* (Raspbian) programi daju tabelarni prikaz mrežnih čvorova na putanji do odredišta

Prva kolona u izlaznoj tabeli (*Tracert* (Windows) - broj 2 na slici 2) prikazuje potreban broj skokova (čvorova) do odredišnog računara. Druga, treća i četvrta kolona (broj 3 na slici 2) prikazuje RTT parametar u milisekundama za svaki ICMP paket u setu. Ovaj parametar govori koliko vremena je potrebno paketu da od izvorišta dođe do određenog čvora i nazad. *Tracert* uvek šalje tri paketa ka odredištu kako bi se dobilo što realnije RTT vreme. Svaka RTT vrednost za pojedini čvor do 500 milisekundi smatra se prihvatljivom. Peta kolona (broj 4 na slici 2) daje pregled IP adresa (a po mogućnosti i domenskih adresa) za svaki čvor na putanji do odredišta.

## Tracert / Traceroute osnovne razlike:

### Tracert:

- Windows i Windows Server operativni sistemi.
- Zasnovana na ICMP tipu-8 i tipu-0 paketa.

### Traceroute:

- Linux/Unix zasnovani operativni sistemi.
- Zasniva se na UDP “*probel*” paketima (*default*) sa određištanim brojem porta u opsegu od 33434 do 33534.
- Ukoliko se koristi “-I” opcija koriste se ICMP paketi.
  - Ukoliko je mrežna bezbedonosna barijera (engl. *Firewall*) duž putanje podešena da blokira ICMP, može se pokušati sa UDP porukama. Slično tome, ako *Firewall* blokira UDP može se pokušati sa ICMP porukama.
  - Da bi se omogućilo da neko uz pomoć programa *traceroute* dobavi adresu mrežnog čvora, *Firewall* na istom mora biti podešen da to dozvoljava.
    - Za ICMP, mora se omogućiti prihvatanje ICMP paketa tipa 0 (“*Echo Replay*”), 8 (“*Echo Request*”) i 30 (*traceroute*).
    - Podešavanje *Firewall*-a za UDP je malo drugačije. Za UDP, potrebno je omogućiti da se UDP paketi sa određištanim brojem porta u opsegu od 33434 do 33534 ne odbacuju (pogledati opciju “-p *port*” kod *traceroute*).
- Ukoliko se koristi “-T” opcija koriste se TCP SYN paketi.
- Koristi se slučajna celobrojna vrednost (engl. *random*) kao broj izvorišnog UDP porta.

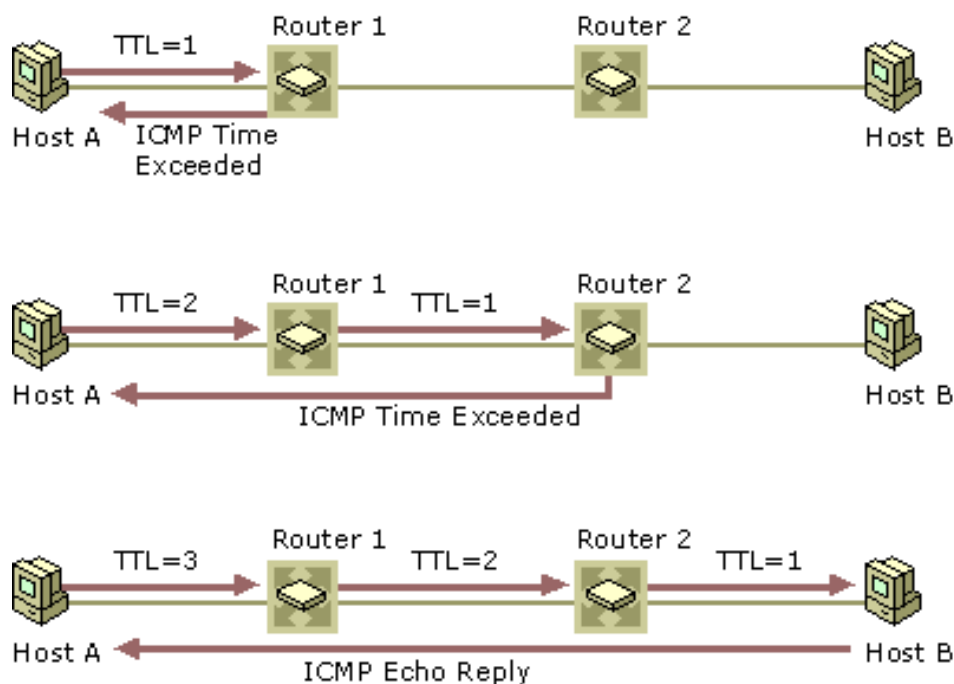
## Princip rada alata Tracert (Windows)

Kao što smo videli *ping* komanda šalje ICMP zahtev “*Echo Request*” na određenu IP adresu i čeka ICMP odgovor “*Echo Replay*” sa te IP adrese. Na osnovu broja primljenih odgovora i vremenskog perioda od slanja zahteva do dobijanja odgovora, *ping* pravi izveštaj o stanju IP konekcije prema nekom računaru unutar TCP/IP mreže.

Da bi razumeli način na koji *tracert* program radi, neophodno je razumeti značaj TTL polja unutar zaglavlja svakog IP paketa. Vrednost ovog polja predstavlja u stvari maksimalno vreme trajanja IP paketa na mreži. Njegovu vrednost postavlja pošiljalac IP paketa (pre slanja paketa) da bi ga svaki čvor (usmerivač ili host) na putu ka odredištu smanjio za određeni iznos. Ukoliko vrednost TTL polja padne na nulu pre nego što paket stigne na svoje odredište, paket se odbacuje a ICMP poruka o grešci (“*Time Exceeded*”) šalje se nazad pošiljaocu paketa. Svrha ovog polja je izbegavanje situacija u kojima paket koji je nemoguće dostaviti odredištu beskonačno kruži mrežom, sprečavajući time mogućnost zagušenja mreže ovim “besmrtnim” paketima. Teoretski gledano, TTL parametar se meri u sekundama (tačnije milisekundama), mada svaki čvor kroz koji paket prolazi na svom putu ka odredištu umanjuje njegovu vrednost za jedan.

Na slici 3 prikazan je princip rada programa *tracert* koji se izvršava na računaru A, a prati putanju do računara B. Program radi tako što vrednost TTL-a za svaki sledeći ICMP paket “*Echo Request*” povećava za jedan i čeka na ICMP poruku “*Time Exceeded*”. Vrednost TTL-a u *tracert* paketu počinje od jedan i svaki put se povećava za jedan. Paket koji *tracert* pošalje putuje svaki put jedan skok (čvor) dalje.

*Tracert* određuje IP adresu *N*-tog skoka tj. čvora (usmerivač ili host) uvidom u polje izvorišne adrese IP zaglavlja u okviru koga je enkapsulirana ICMP poruka “*Time Exceeded*”.



Slika 3. Princip rada Tracert programa

Na usmerivačima 1 i 2 TTL se smanjuje na nulu, što dovodi do slanja ICMP poruke “*Time Exceeded*”. Kad ICMP paket “*Echo Request*” stigne do računara B, on vraća ICMP paket “*Echo Reply*”.

### Princip rada alata Traceroute (Raspbian)

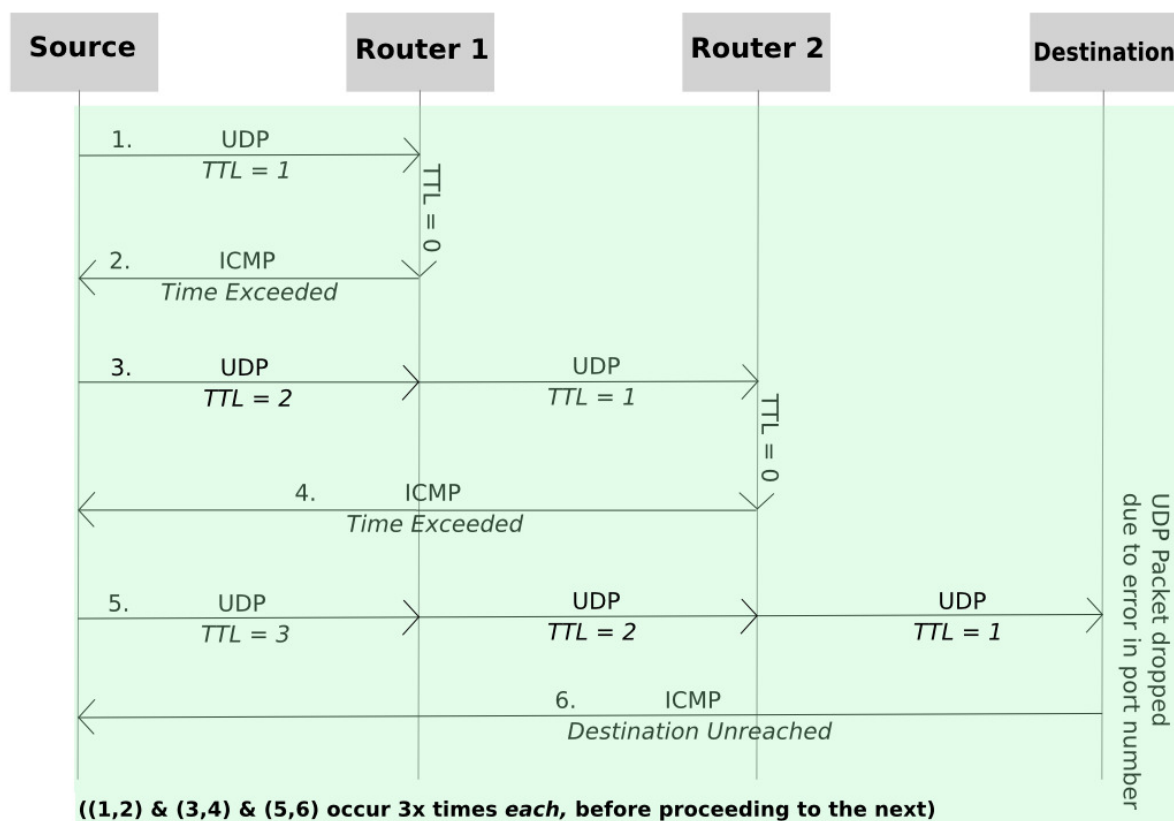
Princip rada programa *traceroute* je dosta sličan principu rada programa *tracert*, i ogleda se u korišćenju TTL polja u okviru zaglavlja IP paketa. Razlika je što *traceroute* klijent za slanje koristi jednostavne UDP datagrame (*default*) koristeći neregistrovani odredišni broj UDP porta (*outbound*).

Da bi se utvrdilo krajnje odredište UDP datagrama, *traceroute* postavlja broj odredišnog UDP porta u okviru UDP datagrama na veliku vrednost (opseg od 33434 ili više). Kada *host* primi UDP datagram sa neregistrovanim brojem odredišnog porta, šalje ICMP poruku o grešci *Destination Unreachable/Port Unreachable*. Poruka o grešci ukazuje *traceroute* programu da je originalna poruka stigla do odredišta.

U nastavku je dat citat odgovora gospodina Jacobsona na pitanje zašto je koristio UDP protokol sa odredišnim brojem porta u opsegu 33434-33534:

“ The original ip spec (rfc791) said that you should never send an icmp error in reponse to an icmp packet. Several years later this was amended to "... in response to an icmp \*error\* packet" but, at the time that traceroute was written, most router vendors had implemented according to the original spec & wouldn't send an icmp time exceeded in response to an icmp echo or echo reply. I then tried using an unassigned ip protocol instead of udp but it turned out that crashed HP/UX systems (remember this was ten years ago, IP was new & there were lots of flakey implementations). The only thing that worked & didn't appear to do damage was udp to a port range that wasn't (& still isn't) used very often.”.

Na slici 4 prikazan je princip rada programa *traceroute*.



Slika 4. Princip rada Traceroute programa

### 3. Pathping (Windows) / mtr (Raspbian)

Alatka *pathping* u kojoj se kombinuju funkcije *ping* i *tracert* alatki uz dodatne informacije koje ne pruža nijedna od tih alatki, služi za proveravanje putanje. *Pathping* jedno određeno vreme šalje pakete svakom usmerivaču na putu do konačnog odredišta i zatim izračunava rezultate na osnovu paketa vraćenih sa svakog usmerivača. Pošto *pathping* prikazuje stepen gubitka paketa na svakom usmerivaču ili vezi, tačno se može odrediti koji usmerivači ili veze izazivaju probleme na mreži.

Postoji niz opcija koje se mogu pogledati pomoću *pathping /?* komande.

Na sledećoj slici prikazan je primer izveštaja *pathping* komande. Primetimo da zbirna statistika iza liste skokova znači gubitak paketa na svakom pojedinačnom usmerivaču.

```

C:\Users\milosp>pathping -n www.MIT.edu

Tracing route to e9566.b.akamaiedge.net [2.21.110.184]
over a maximum of 30 hops:
 0  192.168.2.40
 1  192.168.2.1
 2  147.91.177.142
 3  147.91.168.1
 4  147.91.5.157
 5  147.91.6.86
 6  62.40.125.177
 7  62.40.98.111
 8  62.40.98.63
 9  * * 193.203.0.168
10  2.21.110.184

Computing statistics for 250 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0             Lost/Sent = Pct  Lost/Sent = Pct  192.168.2.40
 1      0ms      0/ 100 = 0%      0/ 100 = 0%      192.168.2.1
 2      2ms      0/ 100 = 0%      0/ 100 = 0%      147.91.177.142
 3      2ms      0/ 100 = 0%      0/ 100 = 0%      147.91.168.1
 4      2ms      0/ 100 = 0%      0/ 100 = 0%      147.91.5.157
 5      3ms      0/ 100 = 0%      0/ 100 = 0%      147.91.6.86
 6     10ms      0/ 100 = 0%      0/ 100 = 0%      62.40.125.177
 7     12ms      0/ 100 = 0%      0/ 100 = 0%      62.40.98.111
 8     14ms      0/ 100 = 0%      0/ 100 = 0%      62.40.98.63
 9     ---     100/ 100 =100%   100/ 100 =100%   193.203.0.168
10     13ms      0/ 100 = 0%      0/ 100 = 0%      2.21.110.184

Trace complete.

```

Slika 5. Primer *pathping* komande

Kada se pokrene program *pathping*, prvo se prikazuje putanja koja se testira. To je ista putanja koju će prikazati *tracert*. *Pathping* zatim prikazuje poruku da je zauzet narednih 250 sekundi (ovo vreme zavisi od broja skokova, potrebno je oko 25 sekundi po skoku-čvoru). Za to vreme *pathping* prikuplja informacije od svih prethodno navedenih usmerivača i linkova između njih. Na kraju tog perioda prikazuju se rezultati testa.

Dve poslednje kolone na desnoj strani – “*This Node/Link, Lost/Sent = %*” i “*Address*” sadrže najkorisnije informacije. Npr. link između 192.168.2.1 i 147.91.177.142 gubi 0 procenata paketa, svi linkovi rade normalno osim linka pod rednim brojem 9 koji gubi sve pakete. Usmerivač na skoku 9 takođe gubi pakete adresirane na njega, ali to ne utiče na njegovu sposobnost usmeravanja saobraćaja koji nije direktno namenjen njemu.

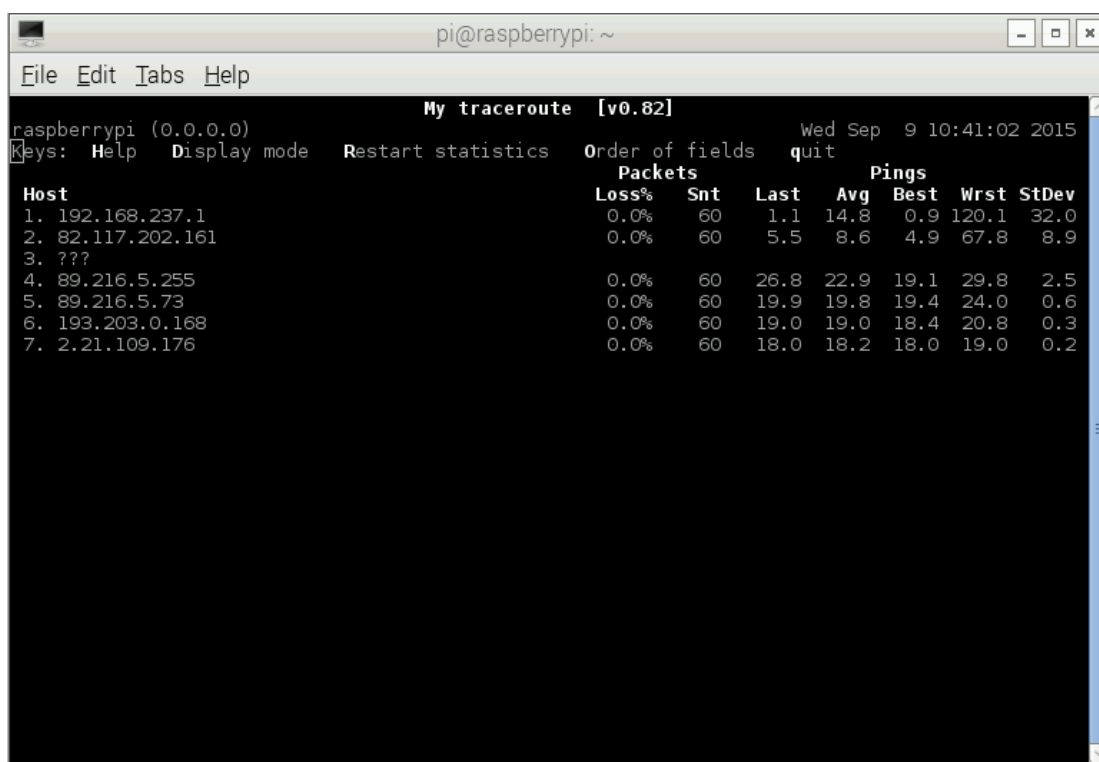
Procenti gubitaka prikazani za linkove (oznaka “l” u poslednjoj koloni) označava gubitak paketa koji se prosleđuju duž te putanje a predstavlja zagušenje linka. Procenti gubitaka za usmerivače (njihova IP adresa u poslednjoj koloni) mogu da znače da su na tim usmerivačima procesori ili bufferi preopterećeni. Ovi zagušeni usmerivači mogu da utiču na sveukupne performanse, pogotovo ako pakete prosleđuju softverski usmerivači.



U operativnom sistemu Raspbian tj. Linux odgovarajuća komanda ima naziv *mtr* (skraćeno od “*my traceroute*”). Komanda *mtr* praktično kombinuje *ping* i *traceroute* u jednom. *Mtr* aplikacija šalje pakete do zadatog odredišta sa namerno malim TTL beležeći odgovore usmerivača između izvorišnog računara i odredišta. Na ovaj način se dobijaju procenat i vremena odgovora između izvorišnog računara i odredišta na svakom skoku.

Raspbian (Linux) instalacija (u terminalu uneti): **sudo apt-get install mtr-tiny**

Primer korišćenja (u terminalu uneti): **mtr google.com**



```
pi@raspberrypi: ~
File Edit Tabs Help
My traceroute [v0.82]
raspberrypi (0.0.0.0) Wed Sep 9 10:41:02 2015
Keys: Help Display mode Restart statistics Order of fields quit
Packets
Host Loss% Snt Last Avg Best Wrst StDev
1. 192.168.237.1 0.0% 60 1.1 14.8 0.9 120.1 32.0
2. 82.117.202.161 0.0% 60 5.5 8.6 4.9 67.8 8.9
3. ???
4. 89.216.5.255 0.0% 60 26.8 22.9 19.1 29.8 2.5
5. 89.216.5.73 0.0% 60 19.9 19.8 19.4 24.0 0.6
6. 193.203.0.168 0.0% 60 19.0 19.0 18.4 20.8 0.3
7. 2.21.109.176 0.0% 60 18.0 18.2 18.0 19.0 0.2
```

Slika 6. Primer *mtr* komande (Raspbian)

## 4. Pregled stanja utičnica (socketa) na lokalnom računaru

Netstat dijagnostički program prikazuje statistike protokola i trenutne TCP/IP konekcije sa i prema drugim mrežnim uređajima. U komandnoj liniji upišite **netstat -a** da bi se prikazale sve konekcije i portovi na kojima se te konekcije uspostavljaju. Opcija **-n** upućuje Netstat da ne prevodi adrese i brojeve portova u imena, čime se ubrzava izvršavanje. Moguće je kombinovati različite opcije-prekidače (engl. *options/switches*) unutar jedne komande. Na slici 7 prikazani su primeri komandi:

- **netstat -a -n** (Windows)
- tj. **netstat -an** (Raspbian).

```
C:\Windows\system32\cmd.exe
C:\Users\nilospi>netstat -a -n

Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:*	LISTENING
TCP	0.0.0.0:135	0.0.0.0:*	LISTENING
TCP	0.0.0.0:443	0.0.0.0:*	LISTENING
TCP	0.0.0.0:445	0.0.0.0:*	LISTENING
TCP	0.0.0.0:902	0.0.0.0:*	LISTENING
TCP	0.0.0.0:912	0.0.0.0:*	LISTENING
TCP	0.0.0.0:2343	0.0.0.0:*	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:*	LISTENING
TCP	0.0.0.0:3580	0.0.0.0:*	LISTENING
TCP	0.0.0.0:3582	0.0.0.0:*	LISTENING
TCP	0.0.0.0:8080	0.0.0.0:*	LISTENING
TCP	0.0.0.0:12793	0.0.0.0:*	LISTENING
TCP	0.0.0.0:26143	0.0.0.0:*	LISTENING
TCP	0.0.0.0:48080	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49286	0.0.0.0:*	LISTENING
TCP	0.0.0.0:52582	0.0.0.0:*	LISTENING
TCP	0.0.0.0:57000	0.0.0.0:*	LISTENING
TCP	0.0.0.0:59110	0.0.0.0:*	LISTENING
TCP	0.0.0.0:59111	0.0.0.0:*	LISTENING
TCP	0.0.0.0:59112	0.0.0.0:*	LISTENING
TCP	127.0.0.1:898	0.0.0.0:*	LISTENING
TCP	127.0.0.1:899	0.0.0.0:*	LISTENING
TCP	127.0.0.1:49156	127.0.0.1:49157	ESTABLISHED
TCP	127.0.0.1:49157	127.0.0.1:49156	ESTABLISHED
TCP	127.0.0.1:49158	127.0.0.1:49159	ESTABLISHED
TCP	127.0.0.1:49159	127.0.0.1:49158	ESTABLISHED
TCP	127.0.0.1:49163	127.0.0.1:49164	ESTABLISHED
TCP	127.0.0.1:49164	127.0.0.1:49163	ESTABLISHED
TCP	127.0.0.1:49173	127.0.0.1:49174	ESTABLISHED
TCP	127.0.0.1:49174	127.0.0.1:49173	ESTABLISHED
TCP	127.0.0.1:49175	127.0.0.1:49176	ESTABLISHED
TCP	127.0.0.1:49176	127.0.0.1:49175	ESTABLISHED
TCP	127.0.0.1:49179	0.0.0.0:*	LISTENING
TCP	127.0.0.1:49179	127.0.0.1:49196	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49225	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49226	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49227	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49228	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49231	ESTABLISHED
TCP	127.0.0.1:49179	127.0.0.1:49381	ESTABLISHED
TCP	127.0.0.1:49182	0.0.0.0:*	LISTENING
TCP	127.0.0.1:49183	127.0.0.1:49184	ESTABLISHED
TCP	127.0.0.1:49184	127.0.0.1:49183	ESTABLISHED
TCP	127.0.0.1:49192	127.0.0.1:49193	ESTABLISHED
TCP	127.0.0.1:49193	127.0.0.1:49192	ESTABLISHED

```
pi@raspberrypi ~
File Edit Tabs Help
pi@raspberrypi ~ $ netstat -an
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
tcp	0	0	192.168.237.127:35464	205.234.175.173:80	CLOSE_WAIT
tcp	0	0	192.168.237.127:47027	216.58.209.74:80	ESTABLISHED
tcp	0	0	192.168.237.127:42231	104.16.26.235:80	ESTABLISHED
tcp	1	0	192.168.237.127:32080	93.93.130.39:443	CLOSE_WAIT
tcp	1	0	192.168.237.127:35461	205.234.175.173:80	CLOSE_WAIT
tcp	0	0	192.168.237.127:40350	64.233.167.157:443	ESTABLISHED
tcp	1	0	192.168.237.127:35458	205.234.175.173:80	CLOSE_WAIT
udp	0	0	0.0.0.0:68	0.0.0.0:*	
udp	0	0	192.168.237.127:123	0.0.0.0:*	
udp	0	0	127.0.0.1:123	0.0.0.0:*	
udp	0	0	0.0.0.0:123	0.0.0.0:*	
udp	0	0	0.0.0.0:7954	0.0.0.0:*	

```
Active UNIX domain sockets (servers and established)

```

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ ACC ]	STREAM	LISTENING	7552	@/tmp/.X11-unix/X0
unix	2	[ ]	DGRAM		6460	/var/run/thd.socket
unix	2	[ ACC ]	STREAM	LISTENING	5808	/tmp/.menu-cached:0-pi
unix	2	[ ACC ]	STREAM	LISTENING	12303	/tmp/.lxterminal-socket:0.0-pi
unix	7	[ ]	DGRAM		6479	/dev/log
unix	2	[ ACC ]	STREAM	LISTENING	5065	/tmp/.pcmanfm-socket-0-pi
unix	2	[ ACC ]	STREAM	LISTENING	5758	/var/run/dbus/system_bus_socket
unix	2	[ ACC ]	SEQPACKET	LISTENING	4484	/run/udev/control
unix	2	[ ACC ]	STREAM	LISTENING	5836	@/tmp/dbus-ItZAQ3E7Ly
unix	2	[ ACC ]	STREAM	LISTENING	7553	/tmp/.X11-unix/X0
unix	2	[ ACC ]	STREAM	LISTENING	6572	/tmp/ssh-5L07yhHtyy1N/agent.2104
unix	3	[ ]	STREAM	CONNECTED	12290	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	6708	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	11824	/var/run/dbus/system_bus_socket
unix	3	[ ]	STREAM	CONNECTED	11140	
unix	3	[ ]	STREAM	CONNECTED	7555	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	9216	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	12290	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	11141	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	13757	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	6713	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	5883	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	12292	@/tmp/dbus-ItZAQ3E7Ly
unix	3	[ ]	STREAM	CONNECTED	6665	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	5050	@/tmp/.X11-unix/X0
unix	3	[ ]	STREAM	CONNECTED	12557	
unix	3	[ ]	STREAM	CONNECTED	9923	
unix	3	[ ]	STREAM	CONNECTED	6684	
unix	3	[ ]	STREAM	CONNECTED	12039	
unix	3	[ ]	STREAM	CONNECTED	6675	
unix	3	[ ]	STREAM	CONNECTED	5080	
unix	3	[ ]	STREAM	CONNECTED	12587	@/tmp/dbus-ItZAQ3E7Ly
unix	2	[ ]	DGRAM		7538	
unix	3	[ ]	STREAM	CONNECTED	12304	
unix	3	[ ]	STREAM	CONNECTED	5079	
unix	3	[ ]	STREAM	CONNECTED	6671	

Slika 7. Primeri netstat komande (Windows i Raspbian)

Broj iza dvotačke je u stvari broj porta koji konekcija koristi. Kolone na slici govore same za sebe, potrebno je jedino pojasniti četvrtu kolonu State koja predstavlja trenutno stanje konekcije po pojedinoj adresi i portu (tj. utičnici). Postoji veći broj (tačnije 10) mogućih stanja konekcije od kojih ćemo izdvojiti samo neke:

- LISTENING – Server je spreman za prihvatanje konekcije
- ESTABLISHED – Uspostavljena konekcija sa udaljenim hostom
- CLOSED – Zatvorena konekcija prema udaljenom hostu
- CLOSE\_WAIT – Server je u procesu raskida konekcije prema klijentu
- TIME\_WAIT – Klijent je u procesu raskida konekcije prema serveru

Napomena:

Windows OS: Ostale opcije *netstat* komande se mogu pogledati **netstat /?** komandom.

Raspbian (Linux): Ostale opcije *netstat* komande se mogu pogledati sa **man netstat** komandom.

## ZADACI VEŽBE

- Analiza i tumačenje sadržaja rezultata **ping** dijagnostičkog mrežnog alata.
- Analiza i tumačenje sadržaja rezultata **tracert/traceroute** dijagnostičkog mrežnog alata.
- Analiza i tumačenje sadržaja rezultata **pathping/mtr** dijagnostičkog mrežnog alata.
- Analiza i tumačenje sadržaja rezultata **netstat** dijagnostičkog mrežnog alata.