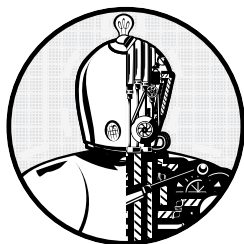


9

MREŽA I NJENO KONFIGURISANJE



Umrežavanje je postupak međusobnog povezivanja više računara i razmene podataka između njih. To zvuči baš jednostavno, ali da biste razumeli kako to funkcioniše, morate sebi postaviti dva suštinska pitanja:

- Kako računar koji šalje svoje podatke zna *gde* da ih pošalje?
- Kada računar na odredištu primi podatke, kako zna *šta* je upravo primio?

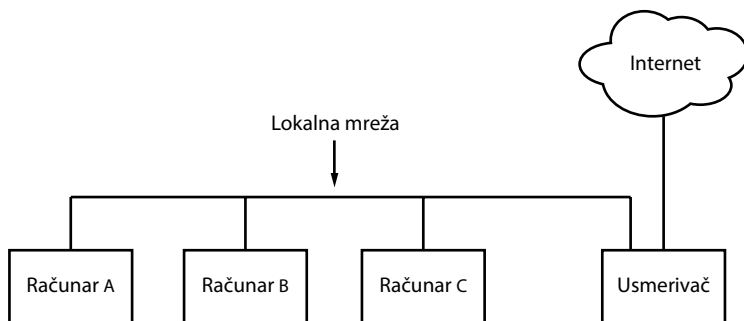
Računar odgovara na ta pitanja tako što koristi niz raznih komponenata, a svaka je odgovorna za određeni aspekt slanja, primanja i prepoznavanja podataka. Komponente su raspoređene u grupe koje čine *mrežne slojeve*, a oni se slažu jedan preko drugog da bi se formirao kompletan sistem. Linuxovo jezgro omogućava rad u mreži slično kao SCSI podsistem opisan u poglavlju 3.

Budući da je svaki sloj projektovan tako da ne zavisi od drugih slojeva, moguće je graditi mreže pomoću velikog broja raznih kombinacija komponenata. U toj fazi, konfiguracija mreže može postati vrlo složena, pa ovo poglavlje započinjemo razmatranjem slojeva u vrlo jednostavnim mrežama. Naučićete kako da pregledate parametre svoje mreže, a kada savladate osnove načina rada svakog sloja, bićete spremni da naučite kako da sami konfigurirate te slojeve. I

najzad, preći ćete na naprednije teme kao što su građenje vlastitih mreža i po-
dešavanje zaštitnih bedema. (Ako ste počeli da širite oči u čuđenju, preskočite
ovaj materijal; na njega se uvek možete vratiti kasnije.)

9.1 Osnove mreža

Pre nego što krenemo s teorijom mrežnih slojeva, pogledajte jednostavnu
mrežu prikazanu na slici 9-1.



Slika 9-1: Tipična lokalna mreža sa usmerivačem koji omogućava pristup internetu

Ova vrsta mreže je univerzalna; većina kućnih mreža i mreža manjih orga-
nizacija konfigurisana je u tom obliku. Svaki računar povezan s mrežom zove
se *umrežen računar*. Svi računari u mreži povezani su s *mrežnim usmerivačem*
(engl. *router*), što je računar koji zna kako da usmerava podatke ka jednoj ili
druvoj mreži. Sve te mašine (u ovom primeru, umreženi računari A, B i C) i
usmerivač zajedno čine *lokalnu mrežu* (engl. *local area network*, LAN). Veze iz-
među računara unutar jednog LAN-a mogu biti žičane ili bežične.

Usmerivač je povezan i na internet – na slici je to oblak. Pošto je usmeri-
vač istovremeno povezan i u lokalnu mrežu i na internet, svi računari unutar
lokalne mreže takođe imaju pristup internetu kroz usmerivač. Jedan od cilje-
va ovog poglavlja je da shvatite kako usmerivač omogućava taj pristup.

Vaš početni predmet razmatranja biće Linux mašina kao što je Računar A
u lokalnoj mreži na slici 9-1.

9.1.1 Paketi

Računar šalje podatke u mrežu u obliku malih blokova koji se zovu *paketi* i
sastoje se od dva dela: *zaglavlja* (engl. *header*) i *korisnog dela* (engl. *payload*).
Zaglavlje sadrži identifikacione podatke kao što su izvorni/odredišni računar
i osnovni protokol. S druge strane, korisni deo čine stvarni podaci aplikaci-
je koje računar želi da pošalje (na primer, HTML podaci ili podaci koji čine
sliku).

Paketi omogućavaju izvornom računaru da komunicira s drugima „isto-
vremeno“ zato što računari mogu da šalju, primaju i obrađuju pakete pro-
izvoljnim redosledom, bez obzira na to da odakle su stigli ili kuda su upućeni.
Deljenje poruka na manje jedinice takođe olakšava otkrivanje i ispravljanje
grešaka tokom prenošenja poruka.

Najvećim delom nećete morati da brinete o prevođenju između sirovih paketa i podataka s kojim radi vaša aplikacija, zato što su u operativni sistem ugrađene komponente koje to rade za vas. Međutim, korisno je da znate ulogu paketa u mrežnim slojevima koje ćemo sada razmotriti.

9.2 Mrežni slojevi

Potpuno funkcionalna mreža sastoji se od skupa mrežnih slojeva koji se zove *mrežni slog* (engl. *network stack*). Svaka funkcionalna mreža ima takav slog. Tipičan internet slog, redom od najvišeg ka najnižem sloju, izgleda ovako:

Sloj aplikacija Sadrži „jezik“ kojim međusobno komuniciraju aplikacije i serveri; najčešće neka vrsta protokola visokog nivoa. Uobičajeni protokoli sloja aplikacija su HTTP (Hypertext Transfer Protocol, koristi se za veb), SSL (Secure Socket Layer) i FTP (File Transfer Protocol). Protokoli sloja aplikacija često se mogu međusobno kombinovati. Na primer, SSL se često koristi u kombinaciji s HTTP-om.

Transportni sloj Definiše karakteristike za prenošenje podataka iz sloja aplikacija i u njega. Ovaj sloj obuhvata proveravanje integriteta podataka, izvorne i odredišne priključke i specifikacije za razdvajanje podataka iz aplikacija na pakete (ako to nije već obavio sloj aplikacija). TCP (Transmission Control Protocol) i UDP (User Datagram Protocol) najuobičajeniji su protokoli transportnog sloja. Transportni sloj se ponekad zove i *sloj protokola*.

Mrežni ili internet sloj Definiše kako treba prenositi pakete od izvornog do odredišnog računara. Pravila za prenošenje konkretnog paketa na internetu poznata su kao IP (Internet Protocol). Pošto ćemo u ovoj mreži razmatrati samo mreže internet tipa, govorićemo zapravo samo o internet sloju. Međutim, pošto su mrežni slojevi osmišljeni tako da ne zavise od konkretnog hardvera, na istom umreženom računaru možete konfigurisati više međusobno nezavisnih mrežnih slojeva (kao što su IP, IPv6, IPX i AppleTalk).

Fizički sloj Definiše kako se sirovi podaci prenose kroz dati fizički medijum, kao što je Ethernet ili modem. To se ponekad zove i *sloj veza* ili *sloj računar/mreža*.

Važno je da razumete strukturu mrežnog sloga zato što vaši podaci moraju proći kroz te slojeve barem dvaput pre nego što dođu do odredišne aplikacije. Na primer, ako šaljete podatke iz Računara A Računaru B na slici 9-1, vaši bajtovi napuštaju sloj aplikacija na Računaru A i putuju nadole kroz transportni i mrežni sloj na istom računaru; zatim prelaze niže u fizički medijum, putuju kroz njega, a onda na sličan način nagore kroz razne niže slojeve do sloja aplikacija na Računaru B. Ako šaljete nešto odredišnom računaru na internetu kroz usmerivač, to će proći kroz neke (ali uglavnom ne sve) slojeve na usmerivaču i na svemu drugom između njih.

Ponekad se slojevi međusobno preklapaju na čudne načine zato što može biti neefikasno da se svi redom obrađuju. Na primer, uređaji koji su tokom razvoja mreža „poslovali“ samo s fizičkim slojem, danas „zaviruju“ u podatke transportnog i internet sloja da bi te podatke brže filtrirali i usmeravali. (Nemojte brinuti o tome dok savladavate osnove.)

Prvo ćemo razmotriti kako naša Linux mašina uspostavlja vezu s mrežom da bismo odgovorili na pitanje *gde* s početka ovog poglavlja. To je najniži nivo mrežnog sloja – fizički i mrežni slojevi. Kasnije, razmotrićemo najviša dva sloja koja pružaju odgovor na pitanje *šta*.

NAPOMENA *Možda ste čuli za još jedan skup slojeva, poznat kao Referentni OSI (Open Systems Interconnection) model. To je sedmoslojni model mreže koji se često koristi za učenje i projektovanje mreža, ali u ovoj knjizi nećemo razmatrati OSI model zato što ćete vi raditi direktno s četiri ovde opisana sloja. Da biste saznali znatno više o slojevima (i uopšte o mrežama), pogledajte knjigu Računarske mreže, Andrew S. Tanenbaum i David J. Wetherall, 5. izdanje, 2010 (prevod Mikro knjiga, 2013).*

9.3 Internet sloj

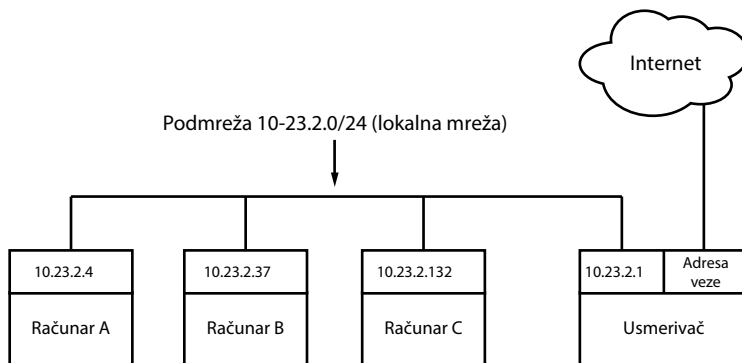
Umesto da krenemo od samog dna mrežnog sloja s fizičkim slojem, počecemo od mrežnog sloja zato što se on možda najlakše razume. Internet kakvog ga danas poznajemo zasniva se na IP-u (Internet Protocol), verzija 4 (IPv4), mada je i verzija 6 (IPv6) sve prihvaćenija. Jedan od najvažnijih aspekata internet sloja jeste to da je zamišljen kao softverska mreža koja ne postavlja nikakve zahteve koji bi se odnosili na dati hardver ili operativni sistem. Suština je u tome da možete slati i primati internet pakete na proizvoljnom hardveru i pod bilo kojim operativnim sistemom.

Internet topologija je decentralizovana; čine je manje mreže koje se zovu *podmreže* (engl. *subnets*). Suština je to da su sve podmreže na određeni način međusobno povezane. Na primer, na slici 9-1, lokalna mreža bi bila jedna od podmreža.

Jedan umreženi računar može biti povezan istovremeno s više podmreža. Kao što ste videli u odeljku 9.1, ta vrsta umreženog računara zove se usmerivač ako zna kako da prosleđuje podatke iz jedne podmreže u drugu (drugi izraz za usmerivač je *mrežni prolaz* /engl. *gateway*/). Slika 9-2 precizira slici 9-1 tako što lokalnu mrežu definiše kao podmrežu i navodi internet adrese za svaki računar u mreži i usmerivač. Usmerivač na slici ima dve adrese: 10.23.2.1 u lokalnoj podmreži i vezu s internetom (ali je adresa veze sa internetom zasad nevažna pa je samo napisano „adresa veze“). Prvo ćemo razmotriti notaciju adresa a zatim i notaciju podmreža.

Svaki računar na internetu ima barem jednu numeričku *IP adresu* u formatu *a.b.c.d*, kao što je 10.23.2.37. Adresa u takvoj notaciji zove se *čtetvorodelna sekvenca s tačkama* (engl. *dotted-quad sequence*). Ako je računar povezan s više podmreža, ima barem jednu IP adresu po podmreži. Trebalo bi da IP adresa svakog umreženog računara bude jedinstvena na celom internetu, ali kao što ćete videti u nastavku poglavlja, privatne mreže i NAT mogu to malo da zakomplikuju.

NAPOMENA *Tehnički govoreći, IP adresa se sastoji od 4 bajta (tj. 32 bita), abcd. Bajtovi a i d su brojevi u opsegu od 1 do 254, a b i c su brojevi u opsegu od 0 do 255. Računar obrađuje IP adrese kao niz sirovih bajtova. Međutim, ljudima je znatno razumljivije da čitaju i pišu četvorodelnu adresu s tačkama, kao što je 10.23.2.37, umesto nečeg ružnog kao što je heksadecimalni oblik 0x0A170225.*



Slika 9-2: Mreža sa IP adresama

IP adrese su donekle nalik kućnim adresama. Da bi komunicirala s određenim računarom u mreži, vaša mašina mora da zna njegovu IP adresu.

Sada ćemo razmotriti adresu vaše mašine.

9.3.1 Prikazivanje IP adresa računara

Jedan računar može imati više IP adresa. Da biste videli adrese koje su aktivne na vašoj Linux mašini, zadajte komandu

```
$ ifconfig
```

Verovatno ćete dobiti mnogo izlaznih podataka, ali trebalo bi da budu slični sledećem:

```
eth0      Link encap:Ethernet  HWaddr 10:78:d2:eb:76:97
          inet addr:10.23.2.4  Bcast:10.23.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1278:d2ff:feeb:7697/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:85076006  errors:0  dropped:0  overruns:0  frame:0
          TX packets:68347795  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:86427623613 (86.4 GB)  TX bytes:23437688605 (23.4 GB)
          Interrupt:20  Memory:fe500000-fe520000
```

Rezultati komande `ifconfig` sadrže brojne podatke i iz internet sloja i iz fizičkog sloja. (Ponekad se čak ni ne prikazuje nikakva internet adresa!) U nastavku poglavlja razmotrićemo detaljnije te podatke, ali zasad, obratite pažnju na drugi red, koji pokazuje da je računar konfigurisan tako da ima jednu IPv4 adresu (`inet addr`) 10.23.2.4. U isto vreme, vrednost polja `Mask` je 255.255.255.0. To je *maska podmreže*, koja definiše podmrežu kojoj IP adresa pripada. Sada ćemo videti kako to radi.

NAPOMENA Komandu `ifconfig`, kao i neke druge koje ćete videti u nastavku ovog poglavlja (kao što su `route` i `arp`), tehnički nadmašuje novija komanda `ip`. Komanda `ip` može uraditi više nego starije komande i preporučljivija je kada pišete

skriptove. Međutim, mnogi ljudi i dalje koriste stare komande kada ručno rade s mrežom, a te komande se mogu koristiti i u drugim verzijama Unixa. Iz tih razloga, korišćićemo starije komande.

9.3.2 Podmreže

Podmreža jeste grupa računara povezanih pomoću IP adresa određenog zajedničkog formata. Ti računari su najčešće u istoj fizičkoj mreži, kao što je ona na slici 9-2. Na primer, svi računari sa adresama od 10.23.2.1 do 10.23.2.254 mogu činiti jednu podmrežu, kao i računari čije su adrese u opsegu od 10.23.1.1 do 10.23.255.254.

Podmrežu definišete pomoću dva elementa: *prefiksa mreže* i maske podmreže (kao što je ona u rezultatima komande `ifconfig` u prethodnom odeljku). Recimo da želite da formirate podmrežu koja sadrži IP adrese od 10.23.2.1 do 10.23.2.254. Prefiks mreže je deo koji je *zajednički* svim adresama u podmreži; u ovom primeru, to je 10.23.2.0, a maska podmreže je 255.255.255.0. Pogledajmo zašto su to ispravne vrednosti.

Nije odmah jasno kako prefiks i maska deluju zajedno da bi vam dali sve moguće IP u podmreži. Razmatranje tih brojeva u binarnom obliku doprinosi lakšem razumevanju. Maska obeležava mesta svih bita dela IP adrese koji je isti za celu podmrežu. Na primer, ovako izgledaju binarni oblici adresa 10.23.2.0 i 255.255.255.0:

10.23.2.0:	00001010 00010111 00000010 00000000
255.255.255.0:	11111111 11111111 11111111 00000000

Sada ćemo istaći podebljanim znacima mesta bita u 10.23.2.0 gde se nalaze jedinice u 255.255.255.0:

10.23.2.0:	00001010 00010111 00000010 00000000
------------	---

Pogledajte bite koji *nisu* istaknuti. Da biste dobili ispravnu IP adresu u ovoj podmreži, možete dodeliti jedinice proizvoljnoj kombinaciji tih bita, izuzev svima nule, ili svima jedinice.

Kada sklopimo sve u celinu, vidi se da računar čija je IP adresa 10.23.2.1 i maska podmreže 255.255.255.0 pripada istoj podmreži kao i svi drugi računari čije IP adrese počinju sa 10.23.2. Kompletnu podmrežu možete definisati kao 10.23.2.0/255.255.255.0.

9.3.3 Uobičajene maske podmreža i CIDR notacija

Ako imate sreće, bavićete se samo s lako razumljivim maskama podmreže kao što je 255.255.255.0 ili 255.255.0.0, ali možda vam sreća nije naklonjena, pa ćete naići na nešto poput 255.255.255.192, gde nije baš tako lako odrediti skup adresa koje pripadaju podmreži. Dalje, verovatno ćete naići i na drugačiji oblik predstavljanja podmreža, koji se zove CIDR (*Classless Inter-Domain Routing – besklasno međudomensko usmeravanje*) notacija, gde se podmreža kao što je 10.23.2.0/255.255.255.0 piše kao 10.23.2.0/24.

Da biste razumeli šta to znači, pogledajte binarni oblik maske (kao u primeru u prethodnom odeljku). Otkrićete da je gotovo svaka maska podmreže samo niz jedinica kojem sledi niz nula. Na primer, upravo ste videli da se binarni oblik adrese 255.255.255.0 sastoji od 24 jedinice kojima sledi 8 nula. CIDR notacija identifikuje masku podmreže pomoću broja *vodećih* jedinica u maski podmreže. Iz tog razloga, kombinacija kao što je 10.23.2.0/24 sadrži i prefiks podmreže i masku podmreže.

Tabela 9-1 prikazuje više primera maski podmreža i njihove CIDR oblike.

Tabela 9-1: Maske podmreža

Dugačak oblik	CIDR oblik
255.0.0.0	8
255.255.0.0	16
255.240.0.0	12
255.255.255.0	24
255.255.255.192	26

NAPOMENA *Ako ne poznajete dobro konverzije između decimalnog, binarnog i heksadecimalnog formata, možete upotrebiti neku kalkulatorsku alatku kao što je bc ili dc da biste konvertovali između raznih numeričkih osnova. Na primer, s programom bc, možete zadati komandu obase=2; 240 da biste broj 240 prikazali u binarnom obliku (osnova 2).*

Prepoznavanje podmreža i računara koji im pripadaju prvi je gradivni blok za razumevanje rada interneta. Međutim, i dalje morate povezati podmreže.

9.4 Mrežne putanje i tabela rutiranja jezgra

Međusobno povezivanje internet podmreža uglavnom se svodi na postupak prepoznavanja računara koji su povezani u više od jedne podmreže. Ako se vratimo na sliku 9-2, razmotrite Računar A na IP adresi 10.23.2.4. Taj računar je povezan s lokalnom mrežom 10.23.2.0/24 i zato može direktno da dosegne ostale računare u toj mreži. Da bi dosegao računare u preostalom delu interneta, mora da komunicira kroz usmerivač na adresi 10.23.2.1.

Kako Linuxovo jezgro razlikuje ta dva odredišta? Tako što koristi određi-šnu konfiguraciju koja se zove *tabela rutiranja* (engl. *routing table*) na osnovu koje prilagođava odredište podataka. Da biste videli sadržaj tabele rutiranja, zadajte komandu `route -n`. Evo šta biste mogli da vidite u slučaju nekog jedno-stavnog umreženog računara kao što je 10.23.2.4:

```
$ route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          10.23.2.1      0.0.0.0        UG    0      0      0 eth0
10.23.2.0        0.0.0.0        255.255.255.0 U      1      0      0 eth0
```

Poslednja dva reda sadrže podatke za rutiranje (usmeravanje) podataka. Kolona Destination (odredište) sadrži prefiks mreže, a kolona Genmask sadrži masku koja odgovara toj mreži. Prikazani rezultati definišu dve mreže: 0.0.0.0/0 (koja predstavlja svaku adresu na internetu) i 10.23.2.0/24. Obe mreže u koloni Flags imaju znak U, što znači da je putanja upotrebljiva („up“ – u aktivnom stanju).

Odredišta se razlikuju po kombinacijama vrednosti u njihovim kolonama Gateway i Flags. Mreža 0.0.0.0/0 ima znak G u koloni Flags, što znači da se komunikacija s tom mrežom mora odvijati kroz mrežni prolaz (engl. *gateway*) u koloni Gateway (10.23.2.1, u ovom slučaju). Međutim, mreža 10.23.2.0/24 nema znak G u koloni Flags, što znači da s tom mrežom postoji određena vrsta direktne veze. Vrednost 0.0.0.0 u koloni Gateway te mreže predstavlja bilo koju adresu. Zasad zanemarite vrednosti u ostalim kolonama.

Postoji jedna začkoljica: recimo da računar želi da pošalje nešto na adresu 10.23.2.132, koja ispunjava oba uslova u tabeli rutiranja, tj. odgovara i za mrežu 0.0.0.0/0 i za mrežu 10.23.2.0/24. Kako jezgro zna da treba da je odredište druga mreža? Tako što bira najduži odredišni prefiks koji odgovara adresi. Tu se CIDR notacija za mreže pokazuje kao posebno praktična: odgovara mreži 10.23.2.0/24, a dužina njenog prefiksa je 24 bita; mreža 0.0.0.0/0 takođe odgovara, ali je dužina njenog prefiksa nula bita (tj. ona nema prefiks), pa se zato primenjuje pravilo 10.23.2.0/24.

NAPOMENA *Opcija -n nalaže komandi route da prikazuje IP adrese računara i mreža umesto njihovih imena. To je važna opcija koju treba zapamtiti zato što ćete je koristiti i uz druge komande za rad s mrežama, kao što je netstat.*

9.4.1 Podrazumevani mrežni prolaz

Stavka 0.0.0.0/0 u tabeli rutiranja ima specijalno značenje zato što predstavlja svaku adresu na internetu. To je *podrazumevana putanja* (engl. *default route*), a adresa zadata u koloni Gateway (u rezultatima komande route -n) podrazumevane putanje jeste *podrazumevani mrežni prolaz* (engl. *default gateway*). Kada nije ispunjen nijedan uslov za neku drugu putanju u tabeli rutiranja, uvek je ispunjen uslov za podrazumevanu putanju i podrazumevani mrežni prolaz je odredište na koje se šalju poruke kada ne preostane nijedna druga mogućnost. Umreženi računar možete konfigurisati i bez podrazumevanog mrežnog prolaza, ali onda on neće moći da dosegne druge računare koji se nalaze izvan eksplicitno zadatih odredišta u tabeli rutiranja.

NAPOMENA *U većini mreža čija je mrežna maska 255.255.255.0, usmerivač se obično nalazi na adresi 1 podmreže (na primer, 10.23.2.1 u mreži 10.23.2.0/24). Budući da je to obična konvencija, može biti izuzetaka.*

9.5 Osnovne ICMP i DNS alatke

Sada je vreme da razmotrimo neke osnovne praktične alatke za rad s umreženim računarima. Te alatke koriste dva posebno zanimljiva protokola: ICMP (Internet Control Message Protocol – Internet protokol za upravljačke

poruke), koji može biti od koristi kada rešavate probleme pri uspostavljanju veza i usmeravanju poruka, i DNS (Domain Name Service – servis za ime-na domena) sistem, koji preslikava imena u IP adrese kako ne biste morali da pamтите gomile brojeva.

9.5.1 Alatka ping

Alatka ping (videti na <http://ftp.arl.mil/~mike/ping.html>) jedna je od najosnovnijih alatki za otkrivanje grešaka u mreži. Ona šalje ICMP eho pakete pomoću kojih zahteva od odredišnog računara da primljeni paket vrati pošiljaocu. Ako odredišni računar primi taj paket i konfigurisan je tako da odgovori na njega, on vraća pošiljaocu ICMP odzivni eho paket.

Na primer, zadali ste **ping 10.23.2.1** i dobili sledeće rezultate:

\$ ping 10.23.2.1

```
PING 10.23.2.1 (10.23.2.1) 56(84) bytes of data.  
64 bytes from 10.23.2.1: icmp_req=1 ttl=64 time=1.76 ms  
64 bytes from 10.23.2.1: icmp_req=2 ttl=64 time=2.35 ms  
64 bytes from 10.23.2.1: icmp_req=4 ttl=64 time=1.69 ms  
64 bytes from 10.23.2.1: icmp_req=5 ttl=64 time=1.61 ms
```

Prvi red pokazuje da šaljete 56-bajtnе pakete (ukupne veličine 84 bajta, ako se uračunaju i zaglavlja) na odredišnu adresu 10.23.2.1 (standardno, po jedan paket u sekundi), a ostali redovi predstavljaju odgovore od 10.23.2.1. U ovim rezultatima, najvažniji delovi su redni broj paketa (`icmp_req`) i ukupno vreme prenošenja paketa (`time`). Veličina vraćenih paketa jednaka je veličini poslatog paketa plus 8. (Sadržaj paketa je nebitan za vas.)

Nedostajući redni brojevi paketa, kao što je onaj između 2 i 4, najčešće znače da postoji neki problem sa uspostavljanjem veze. Paketi mogu stizati izvan redosleda, a ako se to događa, postoji neki problem zato što ping šalje samo po jedan paket svake sekunde. Ukoliko odgovoru treba više od sekunde (1000 ms) da bi stigao, veza je izuzetno spora.

Ukupno vreme prenošenja paketa jeste vreme koje je proteklo od trenutka kada je paket sa zahtevom krenuo ka odredištu, do trenutka prijema odzivnog paketa. Ako je odredište nedosegljivo, poslednji usmerivač na putanju kroz koji je paket uspešno prošao vraća alatki ping ICMP paket „host unreachable“ (odredište nije dosegljivo).

U lokalnoj mreži sa žičanim vezama, trebalo bi da se ne gubi nijedan jedini paket i da ukupna vremena prenošenja budu vrlo niske vrednosti. (U prethodnom primeru prikazani su rezultati za bežičnu mrežu.) Osim toga, za očekivati je i da nema gubljenja paketa između vaše mreže i vašeg davaoца internet usluga i da su ukupna vremena prenošenja uvek približno jednake vrednosti.

NAPOMENA *Iz bezbednosnih razloga, na ICMP eho pakete ne odazivaju se svi računari na internetu, pa se zato može dogoditi da uspešno uspostavljate vezu s određenom veb lokacijom, ali ne dobijate odziv na komandu ping za nju.*