Preddiplomski studij
Računarstvo

Komunikacijske mreže

Upute za izvođenje 1. laboratorijskih vježbi
Uvod u internetske mreže

Ak.g. 2007./2008.

Sadržaj

1 Uvod

Zadatak u ovoj vježbi je upoznavanje s osnovnim svojstvima protokola mrežnog sloja i mehanizmima vezanim uz njihov rad u Internet mreži. Za analizu ponašanja protokola koristit ćemo simulator Imunes te unutar njega dvije naredbe pomoću kojih se daju izvesti bitni zaključci o radu Internetske mreže. To su naredba ping i analizator mrežnog prometa Ethereal (www.ethereal.com).

Materijal u ovoj skripta izložen je na način da su, u svakom odjeljku, prvo opisani primjeri na stvarnoj mreži, a nakon toga slijede zadaci vezani za rad u simulatoru Imunes koje je u sklopu vježbi potrebno riješiti. Primjere nije potrebno izvoditi u laboratoriju, odnosno, zbog specifičnosti laboratorija nije ih niti moguće izvesti. U nekim zadacima potrebno je, u simulator Imunes, učitati gotove scenarije. Ovi scenariji nalaze se u direktoriju `/mem/root/EXAMPLES/tkmreze`.

2 Naredba ping

Kad se pojavi problem u radu neke mrežne aplikacije, prva stvar koja se obično provjerava je postojanje povezanosti na mrežnom sloju. Jednostavno rečeno, potrebno je ustanoviti prolaze li uopće IP paketi od jednog do drugog računala između kojih se pojavio problem u komunikaciji. Upravo u tu svrhu koristi se naredba *ping*.

Naredba *ping* omogućava ispitivanje povezanosti između računala na kojem se naredba koristi i bilo kojeg od ostalih računala i čvorova u mreži. Kroz niz primjera, upoznat ćemo se s ovom naredbom i s informacijom koju ona pruža o radu mreže.

Način korištenja naredbe ping je sljedeći:

```
ping <adresa ili ime odredišnog računala>
```

Ova naredba šalje upit prema navedenom odredišnom računalu. Na ovaj upit odredišno računalo odgovara. Ukoliko naredba ping primi odgovor, ona ga ispiše i korisnik ima informaciju da je odredišno računalo dostupno. U slučaju da se ne primi odgovor, postoji problem povezanosti između dotičnih računala.

Primjer. S jednog od računala u ZZT mreži, čija adresa je 161.53.19.3, pokrenuta je naredba *ping* i kao argument joj je dano računalo s imenom www.google.com. Prikazana je naredba i njen ispis.

```
> ping www.google.com
Pinging www.google.akadns.net [216.239.59.147] with 32 bytes of data:

Reply from 216.239.59.147: bytes=32 time=91ms TTL=228
Reply from 216.239.59.147: bytes=32 time=91ms TTL=228
Reply from 216.239.59.147: bytes=32 time=73ms TTL=234
Reply from 216.239.59.147: bytes=32 time=90ms TTL=228

Ping statistics for 216.239.59.147:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
      Minimum = 73ms, Maximum = 91ms, Average = 86ms
```

Ovaj ispis sadrži mnoštvo korisnih i zanimljivih podataka. Prva linija (`Pinging...`) nam kazuje da je odredišno računalo www.google.akadns.net i da je njegova adresa 216.239.59.147. Također, naznačena je i veličina paketa koji sadrži upit i ona u ovom slučaju iznosi 32 okteta.

Svaka od sljedeće četiri linije ispisa (`Reply from...`) predstavlja po jedan upit prema odredišnom računalu 216.239.59.147. Navedena je veličina upita (32 okteta), vrijeme koje je proteklo od slanja upita do primanja odgovora te Time To Live, TTL polje u zaglavlju IP paketa koji je primljen kao odgovor.

Vidimo da prva dva upita imaju potpuno identične podatke. Treći upit je, međutim, zanimljiv. Vidljivo je da je kod njega TTL polje bilo veće nego kod ostalih upita te da je time polje manje. Prisjetimo se značenja TTL polja. U svaki IP paket koji se šalje upisuje se TTL broj koji može biti između 0 i 255. Podrazumijevana, tzv. default vrijednost TTL-a podešava se u operacijskom sustavu. Na putu svakog IP paketa do odredišta, pri prolasku kroz mrežne

čvorove, svaki čvor umanjuje vrijednost TTL polja za jedan. Ukoliko u nekom čvoru, nakon umanjivanja TTL polja u određenom paketu, vrijednost TTL polja postane 0, čvor uništava paket te prema izvorištu paketa (čija se adresa, naravno, nalazi u zaglavlju) šalje poruku o grešci (*engl.* `time to live exceeded`). Efektivno, to znači da TTL polje broji skokove na putu paketa kroz mrežu. Što je paket prešao više skokova, TTL polje je manje.

Zbog čega je, dakle, TTL polje u trećem upitu veće nego kod ostalih upita? Razlog je to što je odgovor na treći upit kroz mrežu najvjerojatnije putovao putem s manjim brojem skokova nego ostali odgovori. Ako je putovao putem s manjim brojem skokova, konačna vrijednost TTL polja bit će veća. Osim toga, s obzirom da je put bio kraći, i vrijeme prolaska paketa je kraće te je stoga i *time* polje manje.

Preostale linije u ispisu naredbe *ping* daju pregled konačne statistike za sve poslane upite.

Računalo `www.google.com` nalazi se u SAD-u i do njega paketi prolaze kroz desetak čvorova. Napravimo sada *ping* prema nekom od računala u mreži Zavoda za telekomunikacije na FER-u, koje je bliže izvorišnom računalu s kojeg se izvodi *ping*.

Primjer. S računala `mail.tel.fer.hr` koje ima adresu `161.53.19.25`, napravimo *ping* prema računalu `www.tel.fer.hr`.

```
> ping www.tel.fer.hr
Pinging premijer.tel.fer.hr [161.53.19.221] with 32 bytes of data:

Reply from 161.53.19.221: bytes=32 time=5ms TTL=255
Reply from 161.53.19.221: bytes=32 time=2ms TTL=255
Reply from 161.53.19.221: bytes=32 time=3ms TTL=255
Reply from 161.53.19.221: bytes=32 time=2ms TTL=255

Ping statistics for 161.53.19.221:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

Ispis prekidamo pritiskanjem `CTRL-C`.

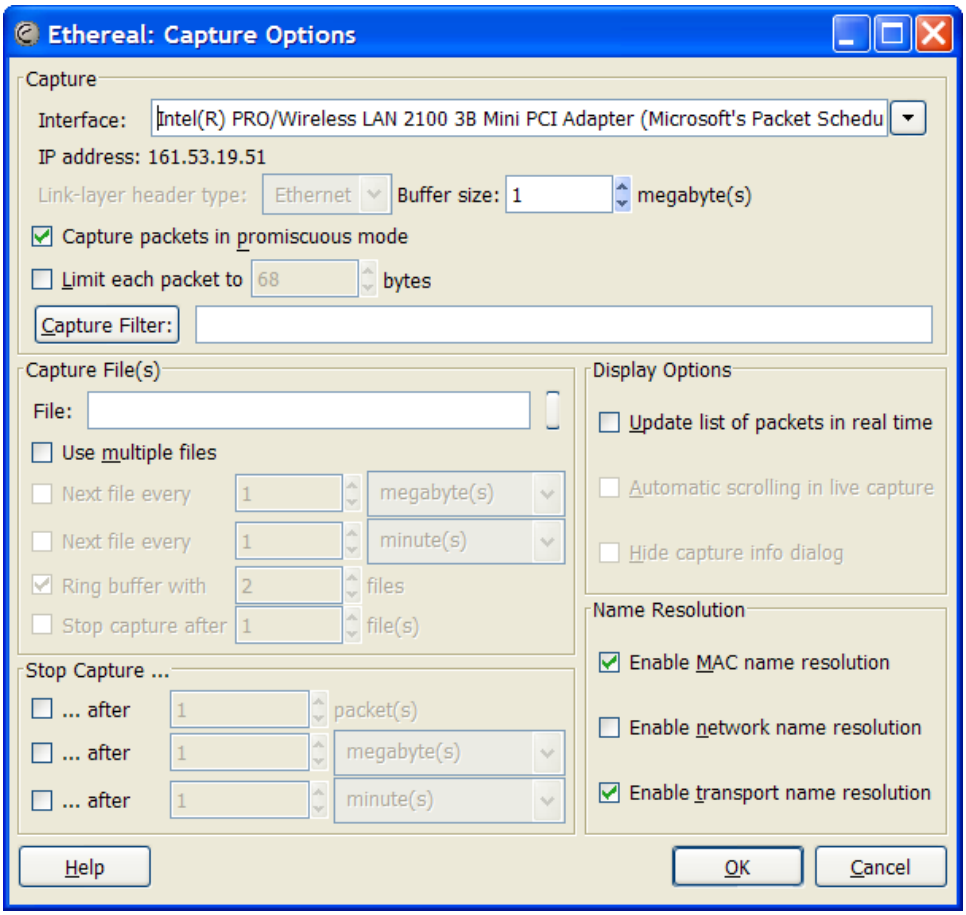
Primjećujemo da je TTL polje jednako 255. To znači da je računalo u istoj lokalnoj mreži kao i računalo s kojeg je poslan upit. Primjećujemo da su IP adrese oba računala vrlo slične. Dapače, duljina mrežnog prefiksa podmreže Zavoda za telekomunikacije iznosi 24 bita, što znači da te dvije adrese, s obzirom da su u istoj podmreži, moraju imati jednakih prvih 24 bita. (O mrežnim prefiksima i podmrežama će biti više riječi u narednim vježbama te ovdje nećemo detaljnije ulaziti u objašnjenje tih pojmova).

Zadatak 1. Učitajte u Imunes simulator primjer `ping.imn` te isprobajte korištenje naredbe *ping*. Obratite pažnju na veličine paketa, vrijeme potrebno za odziv te vrijednosti TTL polja. Odgovaraju li TTL i *time* polja očekivanim?

Na pakete koje šalje naredba *ping* moguće je utjecati uporabom niza opcija koje naredba prihvaća: Neke od opcija su sljedeće:

```
-c broj obavlja samo 'broj' pingova
-i interval interval između slanja pingova, u sekundama
-n prikaz svih adresa u brojčanom, a ne simboličkom obliku
-s veličina paketa s kojim se pinga
-m ttl postavljanje TTL vrijednosti poslanih paketa na iznos 'ttl'
```

Zadatak 2. Utvrdite i objasnite što se događa pri slanju paketa koji u TTL polju ima vrijednost 3, a odredišno računalo je neko računalo udaljeno više od 3 skoka.



Slika 1: Postavke za hvatanje paketa u Ethereal alatu

Zadatak 3. Utvrdite i objasnite što se događa kad je *ping* paket koji se šalje velik 10000 okteta. Kolika je maksimalna moguća veličina paketa koji se može postaviti u ping-u? O čemu ona ovisi?

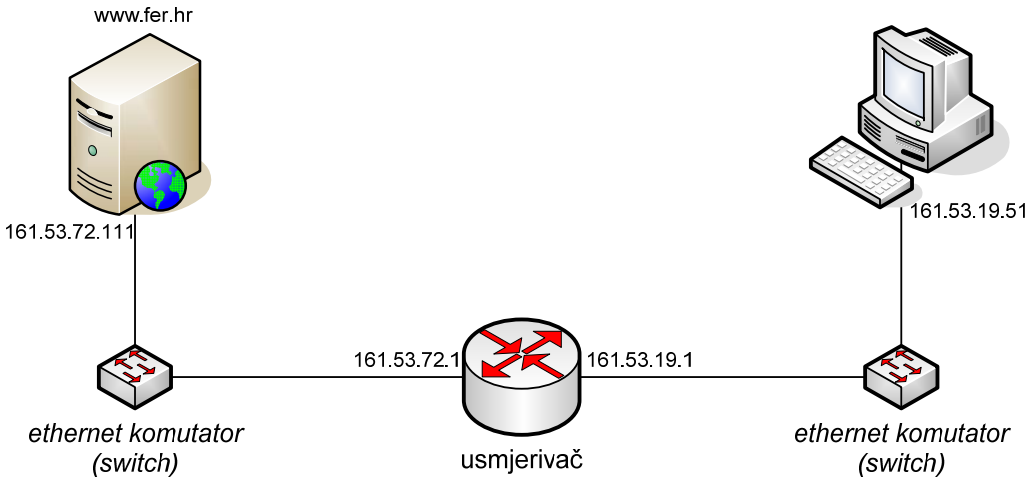
Zadatak 4. Utvrdite i objasnite kako veličina paketa koji se šalje utječe na vrijeme koje prijavljuje naredba *ping* (tzv. *ping time*). Ispitajte kako se mijenjaju vrijednosti koje vraća naredba *ping* ako se u mreži spoje usmjerivači R6 i R1?

3 Ethereal - alat za praćenje i analizu prometa

U prethodnom odjeljku vidjeli smo način korištenja i informacije koje pruža naredba *ping*. Sama naredba *ping* za svoj rad koristi ICMP protokol. Da bismo mogli detaljnije proučiti način njenog rada, kao i rad ostalih protokola i aplikacija, potreban nam je alat za praćenje i analizu prometa u mreži. Postoji velik broj alata s tom namjenom kao što su Tcpdump, Snoop i Ethereal. U ovom poglavlju opisan je alat Ethereal dostupan na adresi http://www.ethereal.com. Slijedi nekoliko osnovnih naputaka vezanih uz korištenje ovog alata.

Alat Ethereal u simulatoru Imunes pokreće se pritiskanjem desnog gumba miša na računalo na kojem se želi prikupljati promet, izborom stavke Ethereal te izborom sučelja na kojem se želi prikupljati promet. Nakon pokretanja Ethereal alata, izborom `Capture/Start` ili pritiskanjem `CTRL-k` otvara se dijalog za konfiguraciju parametara hvatanja prometa kao što je prikazano na slici 1.

- Pod `Capture/Interface` potrebno je izabrati sučelje na kojem će se hvatati promet. To je sučelje preko kojeg ide sav dolazni i odlazni promet na računalo i obično predstavlja ethernet mrežnu karticu u računalu,
- Opciju `Capture packet in promiscuous mode` potrebno je uključiti. Ova opcija označava da će mrežna kartica raditi u posebno načinu rada u kojem se ne odbacuju paketi koji nisu poslani na njenu MAC adresu. Zaustavljanjem miša na toj stavci, otvara se opis ove opcije,
- Opcija `Name Resolution/Enable network name resolution` (u donjem desnom kutu) omogućava da se u ispisu paketa nakon završetka hvatanja ispisuju imena računala s kojih su paketi upućeni umjesto njihovih IP adresa. Ovu opciju moguće je postaviti po vlastitoj želji, s tim da treba voditi računa da se imena računala ne nalaze u uhvaćenim IP paketima, nego se pretvaranje IP adresa iz IP zaglavlja u imena računala obavlja neovisno o procesu hvatanja paketa.

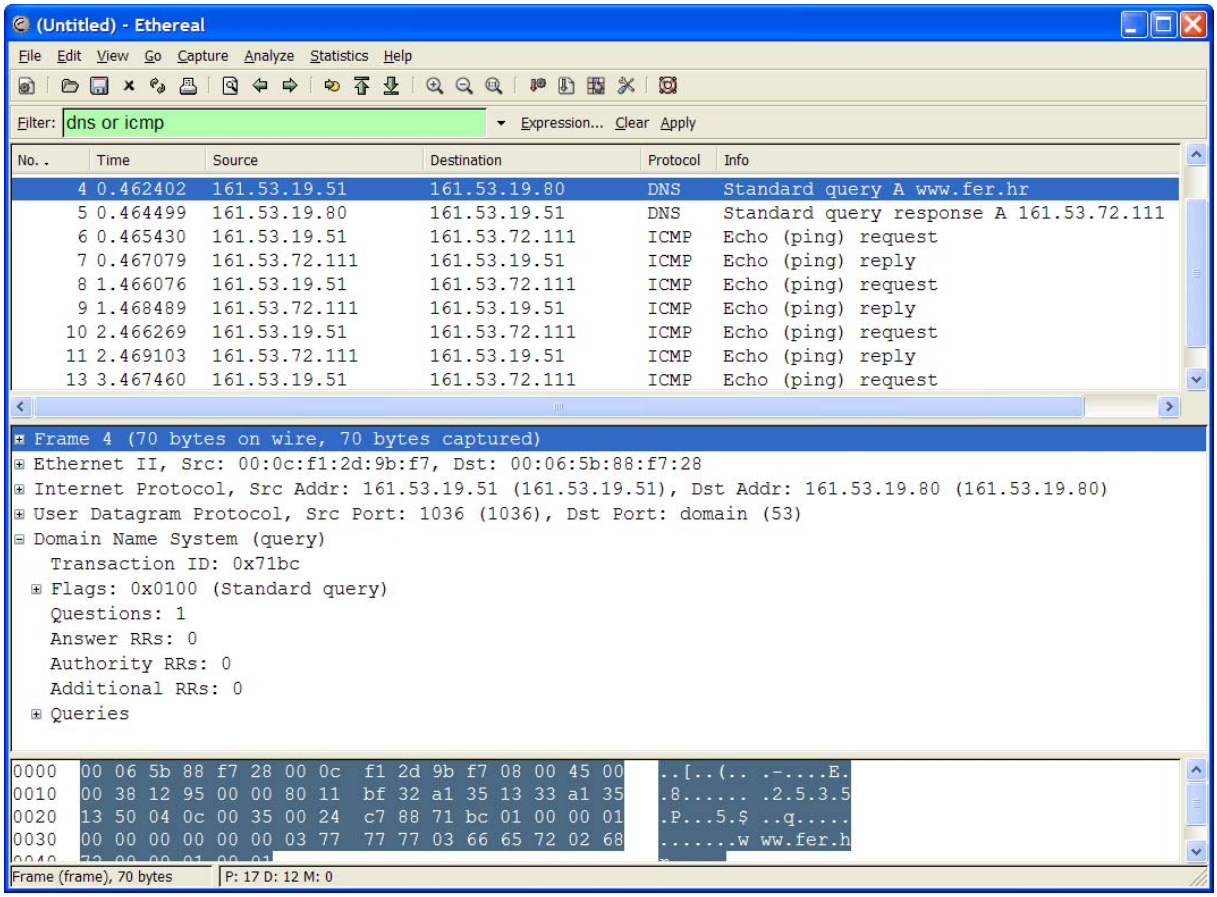


Slika 2 Topologija ispitivane mreže

Pritiskom na tipku „`OK`" pokreće se proces hvatanja paketa. Program kontinuirano ispisuje ukupan broj uhvaćenih paketa razvrstanih po protokolima. Sljedeći primjer odnosi se na mrežu prikazanu na slici 2. Pokrenimo hvatanje paketa na računalu 161.53.19.51 i u komandnoj liniji nakon toga pokrenimo *ping* `www.fer.hr`. Nakon što je naredba *ping* završila svoj rad (tj.

nakon što smo ju prekinuli s CTRL-C), zaustavimo hvatanje paketa u Ethereal-u. Otvara se prozor s prikazom svih „uhvaćenih" paketa. S obzirom da se u mreži odvijaju razne aktivnosti, vrlo je vjerojatno da će osim prometa koji je u mreži generirala naša naredba *ping* biti uhvaćen i drugi promet. Da bismo lakše pratili onaj dio koji nas zanima, filtrirat ćemo uhvaćeni promet i to tako da ćemo u polje filter, koje se nalazi neposredno ispod glavnog izbornika, upisati „icmp or dns". Zašto baš ova dva protokola vidjet ćemo u nastavku.

Primjer uhvaćenog prometa prikazan je na slici 3. Prikaz uhvaćenih paketa u Ethereal-u sastoji se od tri dijela. U gornjem dijelu dan je kratak opis paketa uz izvorišnu i odredišnu adresu. U srednjem dijelu prikazan je detaljniji izgled paketa koji uključuje prikaz svih zaglavlja koji pripadaju različitim protokolima. U trećem dijelu, na dnu prikaza, nalazi se niz okteta koji predstavljaju sam paket.



Slika 3 Promet generiran pri korištenju „ping www.fer.hr" naredbe

Prva dva uhvaćena paketa pripadaju DNS sustavu. IP protokol radi isključivo s IP adresama. Za njega niz znakova `www.fer.hr` ne predstavlja adresu i paket ne može biti poslan na adresu čija vrijednost je `www.fer.hr`. IP adresa računala koje mi nazivamo `www.fer.hr` je 161.53.72.111. Kad u komandnoj liniji napišemo `ping www.fer.hr` ono što naredba *ping* prvo napravi je da za ime `www.fer.hr` pokuša saznati IP adresu. Prva dva paketa uhvaćena Ethereal-om (sa slike 3) predstavljaju ovaj događaj. Protokol DNS bit će detaljnije obrađen u narednim laboratorijskim vježbama.

Na računalu na kojem je izvođena naredba *ping* administrativno je podešeno da se za sva pitanja u vezi imena računala i njihovih IP adresa treba obratiti na adresu 161.53.19.80. Stoga je prvi paket upućen na adresu 161.53.19.80, a pitanje je glasilo: „Koju IP adresu ima

računalo čije ime je www.fer.hr?" U sljedećem retku prikazan je odgovor koji je stigao s adrese 161.53.19.80 i glasi 161.53.72.111.

Nakon što je naredba *ping* uspjela saznati IP adresu odredišnog računala, na odredišnu adresu upućen je `ICMP Echo Request` paket. Ovaj paket, i njemu pripadajući `ICMP Echo Reply` paket čine temelj rada *ping* naredbe.

Zadatak 5. Na primjeru `ping.imn` u simulatoru Imunes proučite i detaljno analizirajte uhvaćeni slijed paketa koji je generirala naredba *ping* između različitih računala u mreži. Utvrdite koji su sve protokoli iskorišteni kao posljedica izvođenja *ping* naredbe i koji je odnos među njima (tj. koje druge protokole svaki pojedini protokol koristi).

Zadatak 6. Proučite utjecaj raznih parametara koje je moguće proslijediti naredbi *ping* na sadržaj paketa koji se šalju. Parametri se mogu dobiti izvođenjem *ping* bez argumenata ili na stranici s uputama koja se dobiva pozivanjem `man ping`.

Zadatak 7. Kojim protokolom se IP paketi prenose između računala smještenih unutar jedne lokalne mreže? Čemu pri tome služi ARP protokol? Pokušajte uhvatiti proizvoljan promet koji pripada ARP protokolu i objasnite način na koji radi ARP. Čemu služe višeodredišne adrese u Ethernet protokolu? Koristi li ih ARP? (udžbenik, str. 249.)

Zadatak 8. Na koji način Ethernet protokol „pamti" vrstu paketa koji se prenosi u podatkovnom dijelu Ethernet okvira? A kako to čini protokol IP?

Zadatak 9. Utvrdite postoji li način da se iz primljenog IP paketa očita put kojim je paket prošao kroz mrežu.

Zadatak 10. Utvrdite postoji li način da se odredi propusnost od jednog računala prema nekom drugom? Postoji li način da se odredi kašnjenje?

Zadatak 11. Utvrdite što se sve mijenja u Ethernet okviru kad se koristi naredba ping s različitim veličinama paketa koji se šalju.

Zadatak 12. Utvrdite što se događa u mreži kad se ping-a adresa koja ne postoji u mreži. Ima li razlike u ponašanju u ovisnosti koja adresa se koristi ili je ponašanje potpuno identično za sve adrese koje ne postoje?

Zadatak 13. Utvrdite kakav promet se generira na Ethernet sučelju računala kad se ping-a adresa 127.0.0.1. A kad se ping-a 127.1.1.1?

Zadatak 14. Pokušajte u heksadecimalnom ispisu sadržaja Ethernet okvira utvrditi dijelove koji pripadaju pojedinim protokolima koji su upakirani u okvir. Postoje li neke karakteristične vrijednosti po kojima se relativno lako mogu prepoznati ovi dijelovi?

Zadatak 15. Utvrdite kolike su minimalna i maksimalna vrijednost MTU (engl. *maximum transfer unit*) na Ethernet sučelju. Pokušajte podesiti MTU i veličinu ping paketa tako da ostvarite što veći broj fragmenata. Način podešavanja MTU-a pronađite u uputama od naredbe `ifconfig(8)`, dakle, upisivanjem `man ifconfig`.

Zadatak 16. Utvrdite utječe li fragmentacija na propusnost i kašnjenje.

Zadatak 17. Utvrdite maksimalni i minimalni odnos između veličine korisničke informacije i protokolnih zaglavlja za ping pakete (analitički i mjerenjem!).

Zadatak 18. Utvrdite na koji način IP protokol može utvrditi da je poslani paket stvarno i primljen na odredištu?