

1.5 Protokoli aplikacijskog sloja

Protokoli aplikacijskog sloja u internetskim mrežama objašnjeni su u udžbeniku Komunikacijske mreže [2].

Protokoli TCP i UDP omogućavaju prijenos informacija između dva udaljena procesa. Na toj podlozi aplikacijski sloj definira komunikaciju potrebnu za realizaciju različitih usluga u mreži. Na primjer, usluga elektroničke pošte se temelji na protokolu SMTP (*Simple Mail Transfer Protocol*) koji definira slanje elektroničke pošte od strane klijenta i njezino primanje od strane SMTP-poslužitelja. S druge strane, protokol HTTP (*HyperText Transfer Protocol*) definira uslugu prijenosa web sadržaja između računala. Ta dva protokola za prijenos vlastitih informacija koriste protokol TCP.

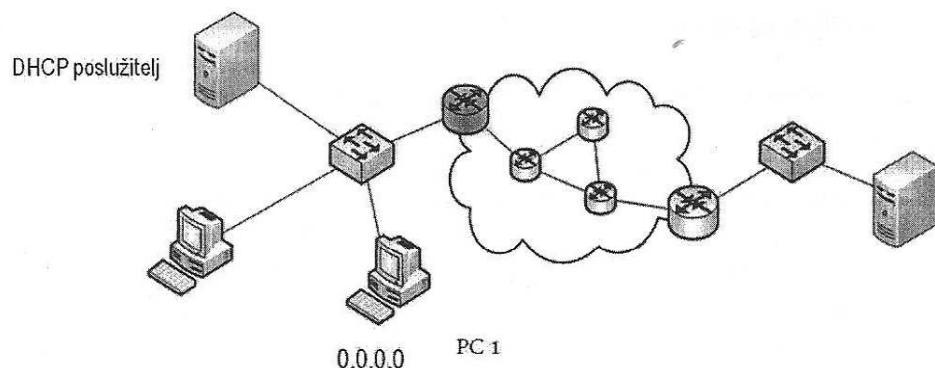
Cilj ovog poglavlja je upoznavanje s osnovnim načelima rada protokola DHCP (*Dynamic Host Configuration Protocol*), DNS (*Domain Name System*), SMTP, POP (*Post Office Protocol*) i HTTP. Mreža, pomoću koje se rješavaju zadaci u emulatoru/simulatoru IMUNES vezani uz aplikacijske protokole, nalazi se u datotekama *DHCP/DHCP.inm* i *DNS+Mail+WEB/NETWORK.inm*. Za korisničko ime, gdje je to potrebno, koristite *root*, a kao lozinku *imunes*.

1.5.1 Protokol DHCP

U dosadašnjim primjerima smo pretpostavljali da su IP adrese mrežnim sučeljima pridijeljene trajno (statičke IP adrese), npr., od strane mrežnog administratora. U praksi se računalima adrese dodjeljuju dinamički, pomoću protokola DHCP (*Dynamic Host Configuration Protocol*). Računala prilikom svakog novog priključivanja u lokalnu mrežu, dobivaju nove IP adrese (dinamičke IP adrese). Nadalje, protokol DHCP služi i za dinamičko podešavanje ostalih mrežnih parametara računala u internetskoj mreži: maske podmreže, podrazumijevanog odlaznog sučelja (engl. *gateway*), adrese DNS-poslužitelja, itd.

Bitno je naglasiti da protokol DHCP računalima omogućava najam (engl. *lease*) određene IP adrese neki period vremena. Ako računalo nije spojeno u podmrežu duže od vremena određenog najmom (engl. *lease time*), najam adrese ističe i ona može biti pridijeljena nekom drugom mrežnom sučelju. Vrijeme najma ovisi o vrsti i namjeni podmreže: od razine sata (npr., bežična mreža u zračnoj luci) do razine mjesec dana (npr., računala u istraživačkom laboratoriju).

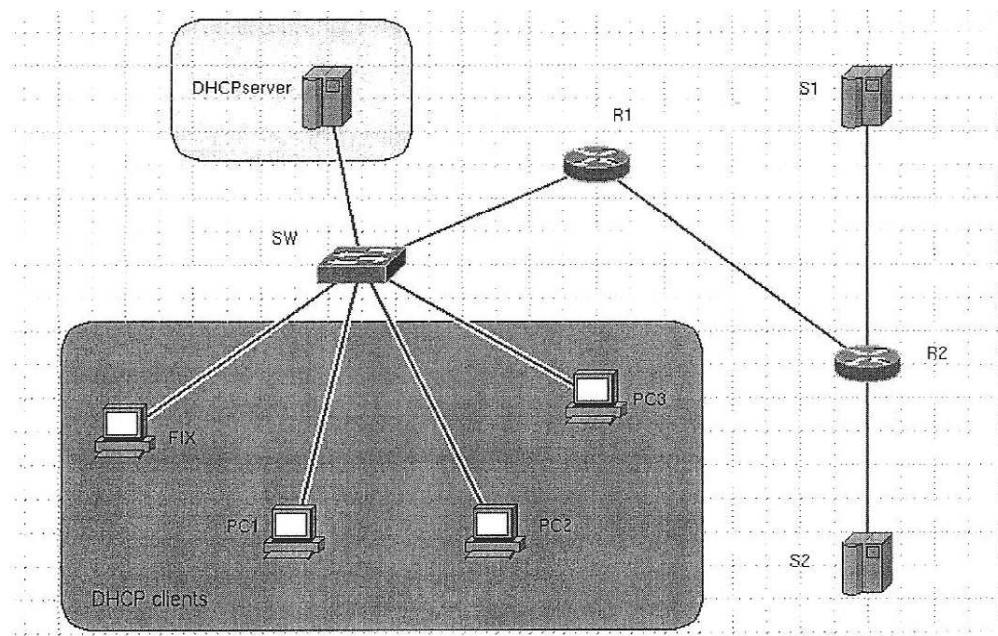
Budući da u svom radu koristi i mehanizme transportnog sloja internetskog (TCP/IP) složaja, DHCP se logički smješta u aplikacijski sloj. Za ispravan rad protokola potreban je DHCP-poslužitelj koji se smješta u podmrežu za koju je nadležan (Slika 1.11). Poslužitelju je na raspolaganju određeni broj IP-adresa (obično iz zadanog raspona) koje prema potrebi dodjeljuje računalima. Pritom se koristi dvama spremnicima: spremnikom za pohranu nedodijeljenih adresa i spremnikom za pohranu dodijeljenih adresa, kako bi u svakom trenutku znao koja adresa je dodijeljena kojem računalu, te koje adrese su slobodne.



Slika 1.11. Smještaj DHCP-poslužitelja u lokalnoj mreži

Prepostavimo da se računalo *PCI* uključuje u mrežu prikazanu slikom 1.11. U procesu dodjele IP-adresa izmjenjuje se 4 vrste poruka:

- *DHCP Discover* - Poslan od strane računala PCI s izvořenom IP-adresom 0.0.0.0 (jer računalo tek treba dobiti adresu) i odredišnom adresom postavljenom na *broadcast* adresu 255.255.255.255 (računalo PCI ne zna adresu DHCP-poslužitelja, pa mora adresirati sva računala),
 - *DHCP Offer* - DHCP poslužitelj šalje ponuđenu IP-adresu, podatke o nadležnim DNS-poslužiteljima, podrazumijevanom usmjeritelju i mrežnoj masci,
 - *DHCP Request* - Računalo PCI šalje *broadcast* zahtijevajući ponuđenu adresu,
 - *DHCP ACK* - DHCP-poslužitelj odobrava zahtjev za adresom, definira vrijeme „najma“ adrese, te potvrđuje podatke o podrazumijevanom usmjeritelju i DNS-poslužiteljima.



Slika 1.18: Topologija *DHCP/DHCP.imn*

Zadatak 30. Proučite primjer DHCP/DHCP.inm (Slika 1.18). Svrha ovog primjera je pokazati kako se dinamički računalima dodjeljuje IP-adresa. Scenarij vježbe je sljedeći:

1. Započnite simulaciju.
2. Kroz konzolu (*Xfce Menu -> Terminal*) **računala na kojem je pokrenut IMUNES** (dakle, konzolu operacijskog sustava FreeBSD) pozicionirajte se u direktorij */root/Examples/DHCP/* te izvršite skriptu *start_dhcp*:

```
# ./start_dhcp
```

Skripta podešava odgovarajuće klijente i poslužitelje za ovaj primjer.

3. Otvorite konzolu na računalu *pc3* te pokrenite alat *Wireshark* tako da snima mrežni promet na mrežnom sučelju računala.
4. U konzoli na računalu *pc3* izvršite naredbu:

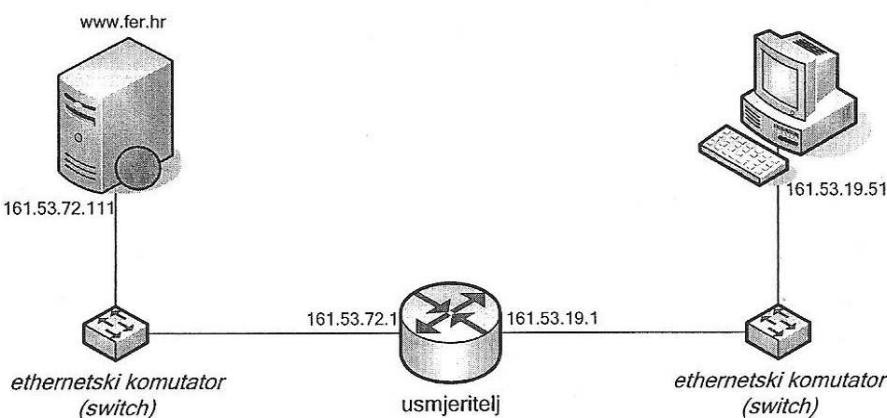
```
# dhclient eth0
```

Ovom naredbom se za mrežno sučelje *eth0* računala *pc3* zahtijeva od DHCP-poslužitelja dodjela IP-adrese.

5. Provjerite je li računalu *pc3* dodijeljena IP-adresa (naredba *ifconfig eth0*).
6. Zaustavite snimanje mrežnog prometa, te pomoću prikaza snimljenog u alatu *Wireshark* proučite proces dobivanja IP-adrese od DHCP-poslužitelja i identificirajte pripadajuće DHCP-poruke.

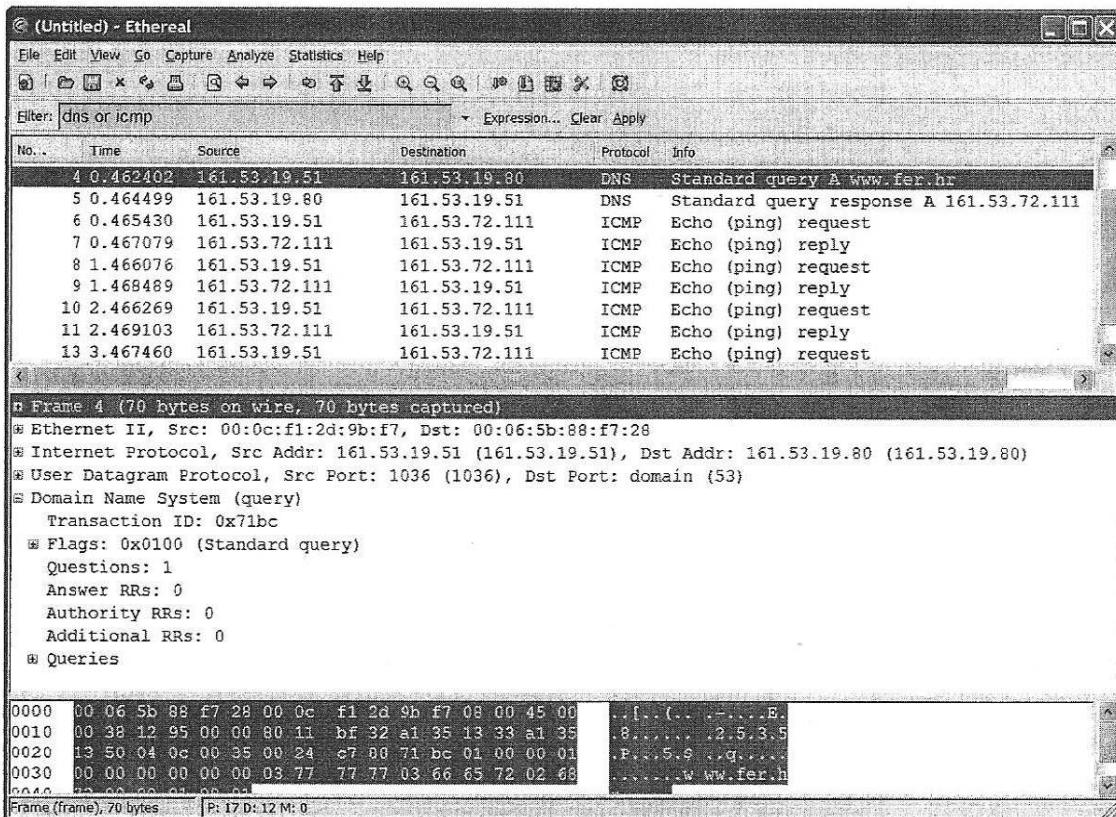
1.5.2 Protokol DNS

Pokrenimo alat *Wireshark* na računalu 161.53.19.51 (Slika 1.19) i u komandnoj liniji nakon toga pokrenimo izvršavanje naredbe *ping www.fer.hr*. Nakon što je naredba *ping* završila svoj rad (tj., nakon što smo ju prekinuli s kombinacijom tipki *CTRL+C*), zaustavimo snimanje mrežnog prometa u alatu *Wireshark*. Otvara se prozor s prikazom svih snimljenih paketa. S obzirom da se u mreži odvijaju razne aktivnosti, vrlo je vjerojatno da će osim prometa koji je u mreži generirala naredba *ping* biti uhvaćen i drugi mrežni promet. Da bismo lakše pratili onaj dio koji nas zanima, filtrirat ćemo uhvaćeni promet i to tako da se u polje *filter*, koje se nalazi neposredno ispod glavnog izbornika alata *Wireshark*, upiše *icmp or dns*. Zašto baš ova dva protokola vidjet ćemo u nastavku.



Slika 1.19 Topologija ispitivane mreže

Prikaz snimljenih paketa u alatu *Wireshark* dan je na sljedećoj slici (Slika 1.20). Prva dva uhvaćena paketa pripadaju sustavu DNS. Protokol IP radi isključivo s IP-adresama. Za njega niz znakova *www.fer.hr* ne predstavlja adresu i paket ne može biti poslan na adresu čija je vrijednost *www.fer.hr*. IP-adresa računala koje se naziva *www.fer.hr* je 161.53.72.111. Kada se u komandnoj liniji napiše ping *www.fer.hr*, ono što alat *ping* prvo napravi je da za ime *www.fer.hr* pokuša sazнати IP-adresu. Prva dva paketa snimljena alatom *Wireshark* predstavljaju ovaj događaj. Na računalu na kojem je izvedena 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, a on glasi 161.53.72.111.



Slika 1.20 Promet generiran prilikom izvršavanja naredbe
ping www.fer.hr

Nakon što je alat *ping* uspio sazнати IP-adresu odredišnog računala, na tu je odredišnu adresu upućena ICMP poruka *Echo Request*.

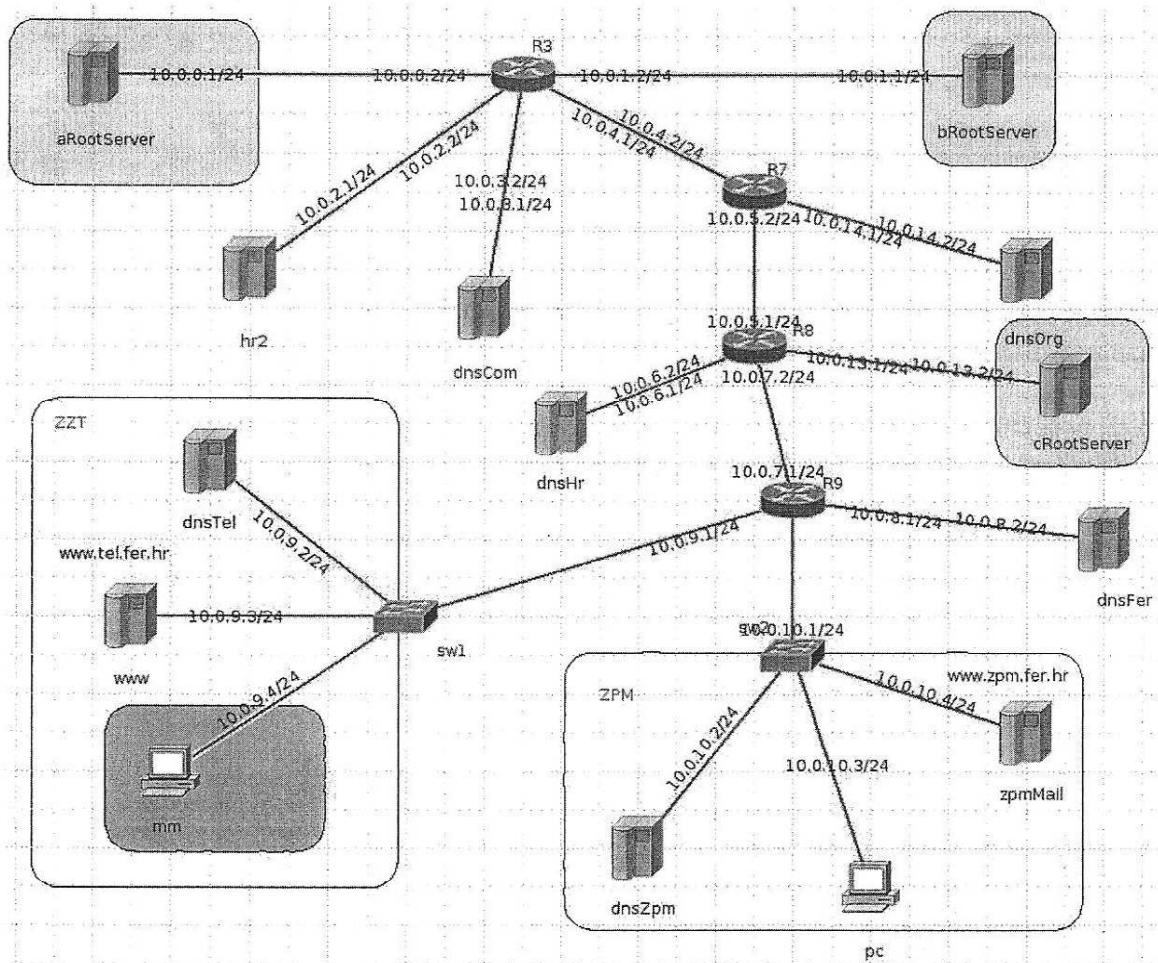
Topologija mreže podešena za analizu protokola DNS nalazi se u datoteci Examples\DNS+Mail+WEB\NETWORK.inm (Slika 1.21). Za ispravno generiranje DNS-prometa potrebno je na odgovarajućim računalima pokrenuti DNS-poslužitelje. To se radi u sljedećim koracima:

1. Pokrenuti simulaciju nakon učitavanja mreže
 2. U konzoli (*Xfce Menu -> Terminal*) računala na kojem je pokrenut IMUNES, pozicionirati se u direktorij *DNS+Mail+WEB*:

```
# cd /root/Examples/DNS+Mail+WEB/
```

- ### 3. Pokrenuti DNS-poslužitelje naredbom:

```
# ./start dns
```



Slika 1.21 Primjer topologije mreže za slanje i primanje DNS-upita

Naredbom

```
# ./start dns
```

konfigurirat će se odgovarajući poslužitelji i klijenti u mreži za potrebe ove analize. Na taj način svako računalo je u mogućnosti poslati neki DNS-upit te potom primiti DNS-odgovor od svog nadležnog DNS-poslužitelja. Na klijentskim računalima postoji alat koji omogućuje saznavanje informacija o imenima i IP-adresama ostalih računala, zatim nadležnim poslužiteljima elektroničke pošte te nadležnim DNS-poslužiteljima. Alat se izvodi pokretanjem naredbe *host*, koja potom generira određeni DNS-upit i šalje ga u mrežu. Naredba *host* može se pokrenuti korištenjem više opcija, od

kojih su najvažnije ispisane u tablici (Tablica 5). Ostale opcije naredbe *host* mogu se saznati pokretanjem naredbe

```
# man host
```

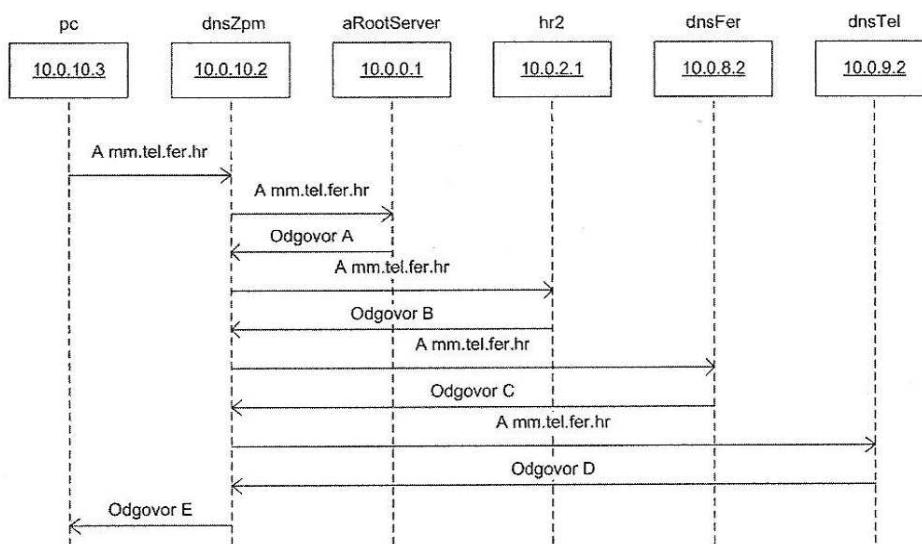
Tablica 5 Opcije naredbe *host* za slanje DNS-upita

Naredba	Značenje naredbe
host -t A mm.tel.fer.hr	traži se IP-adresa računala za koje je zadano njegovo ime
host -t MX tel.fer.hr	traži se računalo nadležno za primanje pošte
host -t NS fer.hr	traži se nadležni DNS-poslužitelj
host -t PTR 10.0.0.1	traži se ime računala za koje je zadana njegova IP-adresa

Analizirajmo rad protokola DNS pomoću primjera. Uključimo snimanje prometa alatom Wireshark na računalu *dnsZpm.zpm.fer.hr*. Otvorimo konzolu računala *pc.zpm.fer.hr* te saznajmo IP-adresu računala *mm.tel.fer.hr* izvođenjem naredbe

```
# host -t A mm.tel.fer.hr
```

U konzoli se ispisuje tražena IP-adresa: 10.0.9.4. Analizirajući snimljeni promet može se identificirati slijed poruka protokola DNS izmijenjenih u mreži od trenutka slanja upita s računala *pc* do primitka odgovora (Slika 1.22). Računalo *pc* šalje DNS-upit svom nadležnom DNS-poslužitelju: računalu *dnsZpm*. S obzirom da *dnsZpm* u svom priručnom spremniku nema traženu adresu, šalje dodatne upite u mrežu kako bi je saznao. Prvo se obraća jednom od vršnih (korijenskih) DNS-poslužitelja: računalu *aRootServer*, tražeći IP-adresu računala *mm.tel.fer.hr*. S obzirom da vršni DNS-poslužitelj mora imati pohranjene zapise samo o DNS-poslužiteljima vršnih domena, niti on ne zna traženu adresu. Stoga šalje poruku *Odgovor A* računalu *dnsZpm*.



Slika 1.22 Slijedni dijagram DNS-upita i DNS-odgovora za upit
`# host -t A mm.tel.fer.hr`

Analiziramo li sadržaj poruke *Odgovor A* (Slika 1.23), vidimo karakteristična polja protokola DNS. Primjerice, polje *Queries* sadrži inicijalni upit za adresom računala *mm.tel.fer.hr*. Polje *Authoritative Nameservers* sadrži podatke o sljedećem DNS-poslužitelju (ili nekolicini njih) kojem je potrebno proslijediti upit. U ovom slučaju radi se o vršnim poslužiteljima domene *hr*: računalima *dnsHr* i *hr2*. Nakon što primi *Odgovor A*, računalo *dnsZpm* ponovno šalje isti upit, ali ovaj put nekom od „predloženih“ DNS-poslužitelja. U ovom slučaju upit se šalje računalu *hr2*. Na jednak način, porukom *Odgovor B* računalo *hr2* vraća adresu DNS-poslužitelja nadležnog za domenu *fer.hr*, a porukom *Odgovor C* računalo *dnsFer* vraća adresu DNS-poslužitelja nadležnog za domenu *tel.fer.hr*. S obzirom da ime traženog računala pripada domeni za koju je zadužen DNS-poslužitelj *dnsTel*, poruka *Odgovor D* će vratiti traženu IP-adresu. Konačno, *dnsZpm* vraća *Odgovor E* s traženom IP-adresom računala *pc*. Navedeni primjer opisao je proces dohvaćanja adrese računala u slučaju da su sva priručna spremišta DNS-poslužitelja prazna. Ukoliko bi postojao zapis o traženoj IP-adresi u bilo kojem od DNS-poslužitelja na putu, ona bi se vratila u odgovoru, umjesto podatka o sljedećem poslužitelju kojeg „treba pitati“.

```
▶ Frame 9 (157 bytes on wire, 157 bytes captured)
▶ Ethernet II, Src: 40:00:aa:00:00:25 (40:00:aa:00:00:25), Dst: 40:00:aa:00:00:2b (40:00:aa:00:00:2b)
▶ Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.10.2 (10.0.10.2)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: 62937 (62937)
▼ Domain Name System (response)
  [Request In: 7]
  [Time: 0.020574000 seconds]
  Transaction ID: 0x8bcf
  ▶ Flags: 0x8000 (Standard query response, No error)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 2
    Additional RRs: 3
  ▶ Queries
    ▶ mm.tel.fer.hr: type A, class IN
  ▶ Authoritative nameservers
    ▶ hr: type NS, class IN, ns dnsHr.hr
    ▶ hr: type NS, class IN, ns hr2.com
  ▶ Additional records
    ▶ hr2.com: type A, class IN, addr 10.0.2.1
    ▶ dnsHr.hr: type A, class IN, addr 10.0.6.2
    ▶ <Root>: type OPT
```

Slika 1.23 Sadržaj poruke *Odgovor A*

S obzirom na način na koji vraćaju odgovore, DNS-poslužitelje možemo svrstati u dvije kategorije. U prvu kategoriju spada DNS-poslužitelj *dnsZpm*, koji, nakon što primi upit za koji ne zna odgovor, šalje dodatne upite u mrežu ostalim DNS-poslužiteljima. To znači da će kao odgovor na originalni upit uvijek vratiti ili traženi podatak (nakon što ga sazna), ili poruku o pogrešci (npr. ako traženo računalo ne postoji). Za takav DNS-poslužitelj kažemo da rekursivno razlučuje adrese.

U drugu kategoriju spadaju svi ostali DNS-poslužitelji iz opisanog scenarija. Oni na traženi upit uvijek odmah vraćaju odgovor bez generiranja dalnjih upita. Odgovor može biti traženi odgovor (ako je poznat) ili adresa sljedećeg DNS-poslužitelja kojeg treba pitati. Za takve DNS-poslužitelje kažemo da iterativno razlučuju adrese.

Transportni protokol koji se koristi za slanje DNS-upita i DNS-odgovora je UDP. S obzirom da se radi o kratkim upitim i odgovorima koji moraju biti što brže preneseni kroz mrežu, praktičnije je koristiti UDP za koji ne mora biti uspostavljena i raskinuta veza prilikom prijenosa svakog upita /odgovora. Naravno, upotreba protokola TCP za tu svrhu nije zabranjena, ali se ne preporuča i nije česta u praksi.

Zadatak 31. Koristeći naredbu host u konzoli računala *pc.zpm.fer.hr*, saznajte:

- a. IP-adresu računala *dnsHr.hr*.
- b. koje računalo je nadležno za primanje pošte na domeni *zpm.fer.hr*.
- c. koje računalo je nadležno za primanje pošte na domeni *tel.fer.hr*.
- d. koji su DNS-poslužitelji nadležni za domenu *hr*.
- e. koji su DNS-poslužitelji nadležni za domenu *fer.hr*.
- f. koji su DNS-poslužitelji nadležni za domenu *tel.fer.hr*.
- g. koji su DNS-poslužitelji nadležni za vršnu domenu ("").
- h. ime računala s IP-adresom 10.0.9.4.

Zadatak 32. Kakav se mrežni promet generira prilikom izvršavanja prethodnih naredbi? Skicirajte i obrazložite slijed upita i odgovora za zadatak 31.c.

Zadatak 33. Analizirajte korištena UDP-vrata za scenarij iz zadatka 31.g.

1.5.3 Protokoli elektroničke pošte

Elektronička pošta je sustav koji omogućuje primanje i slanje elektroničkih poruka. Za primanje poruka koriste se protokoli POP i IMAP, a za njihovo slanje protokol SMTP. U zadacima koji slijede ukratko će se proučiti protokoli SMTP i POP.

Prije nego što se započne s proučavanjem protokola za slanje (SMTP) odnosno primanje (POP) elektroničke pošte u IMUNES-u, potrebno je na odgovarajućim računalima konfigurirati SMTP- i POP-poslužitelje. To se obavlja u sljedećim koracima:

1. Pokrenuti primjer *Examples\DNS+Mail+WEB\NETWORK.i mn*
2. U konzoli (*Xfce Menu -> Terminal*) računala na kojem je pokrenut emulator/simulator IMUNES, potrebno se pozicionirati u direktorij *DNS+Mail+WEB*:

```
# cd Examples\DNS+Mail+WEB
```

3. Pokrenuti DNS-poslužitelje.
4. Iz direktorija *DNS+Mail+WEB* pokrenuti SMTP- i POP-poslužitelje naredbom:

```
# ./start_mail
```

Protokol SMTP (*Simple Mail Transfer Protocol*) definira postupak razmjene poruka elektroničke pošte između dva udaljena računala. Svi podaci se, u toku prijenosa elektroničke pošte s jednog na drugo računalo, prenose u ASCII-obliku, a sastoje se od niza naredbi te samog sadržaja poruke.

Zadatak 34. Analizirajte rad protokola kroz sljedeći scenarij:

1. Pokrenite snimanje mrežnog prometa na mrežnim sučeljima računala *mm* i *www*.
2. Iz konzole računala *mm*, koristeći program *cone* (naredba *man cone* daje detaljnije informacije), pošaljite poruku korisniku na adresu *imunes@zpm.fer.hr*. Izvršite naredbu:

```
# cone
```

Na tipkovnici odaberite tipku *M* (koja odgovara pozivu glavnog izbornika programa), a zatim tipku *W* (koja odgovara odabiru opcije za sastavljanje nove elektroničke poruke). Nakon što popunite potrebna zaglavlja (*To* i *Subject*) te napišete poruku, istu šaljete odabirom kombinacije tipki *Ctrl+X*.

3. Zaustavite snimanje mrežnog prometa, te pomoću prikaza snimljenog u alatu *Wireshark* odgovorite na sljedeća pitanja:
 - a. Koji su se protokoli pojavili kao rezultat slanja elektroničke poruke? Koja je njihova osnovna uloga?
 - b. Koji su koraci prilikom slanja elektroničke poruke s računalima *mm* na adresu *imunes@zpm.fer.hr*?
 - c. Gdje se sve koristi protokol DNS u ovom slučaju?
Koje računalo je nadležni poslužitelj elektroničke pošte za domenu *tel.fer.hr*? Kako računalo *mm* saznaće IP-adresu tog poslužitelja?
Koje računalo je nadležni poslužitelj elektroničke pošte za domenu *zpm.fer.hr*? Kako računalo *www* saznaće IP-adresu tog poslužitelja?
 - d. Koliko se TCP-konekcija uspostavlja u ovom primjeru i koja se vrata pritom koriste? Odaberite opciju *Statistics → Conversation List → TCP (IPv4 & IPv6)* u izbornoj traci alata. Čemu služe te konekcije?
 - e. Pronađite TCP-segment kojim započinje uspostava konekcije s računalima *mm* prema njegovom nadležnom SMTP-poslužitelju. Označite ga, zatim pritisnite desnu tipku miša te odaberite opciju *Follow TCP stream*. Kako teče komunikacija protokolom SMTP između tog računala i njegovog nadležnog poslužitelja? Skicirajte dobiveni tijek poruka. Pronađite segment u kojem se prenosi sadržaj elektroničke poruke.

Protokol POP (*Post Office Protocol*) definira postupak pristupa elektroničkoj pošti koja je pohranjena u poštanskom sandučiću na POP-poslužitelju. Svi podaci se prenose u ASCII-obliku, a sastoje se od niza naredbi te samog sadržaja poruke.

Zadatak 35. Analizirajte rad protokola kroz sljedeći scenarij:

1. Pokrenite snimanje mrežnog prometa na mrežnom sučelju računala *pc*.
2. Iz konzole računala *pc*, korištenjem programa *cone*, pristupite POP-poslužitelju na računalu *zpmMail* kako bi pročitali pristiglu poruku. Izvršite naredbu:

```
# cone
```

Nakon izvršavanja naredbe, odaberite opciju *imunes@zpm.fer.hr*: , kojom se otvara poštanski sandučić. Koristite lozinku *imunes*. Otvorite pristiglu poruku.

3. Zaustavite snimanje mrežnog prometa, te pomoću prikaza snimljenog u alatu *Wireshark* odgovorite na sljedeća pitanja:
 - a. Koji su se protokoli pojavili kao rezultat pristupanja elektroničkoj pošti na POP-poslužitelju računala *zpmMail*?
 - b. Koliko se TCP-konekcija uspostavlja u ovom primjeru i koja se vrata pritom koriste?
 - c. Za što se koristi protokol DNS u ovom slučaju?

- d. Pronadite TCP-segment kojim započinje uspostava konekcije s računalom *pc* prema njegovom nadležnom POP-poslužitelju. Označite ga, zatim pritisnite desnu tipku miša te odaberite opciju *Follow TCP stream*. Kako teče razmjena POP-poruka između računala *pc* i njegovog nadležnog poslužitelja? Skicirajte dobiveni tijek poruka. Čemu služe POP-poruke *LIST* i *RETR*? Analizirajte njihove odgovore.
- e. Pogledajte sadržaj elektroničke poruke i analizirajte polja *Received*. Kojim „putem“ je poruka stigla na poslužitelj *zpmMail*?
- f. Je li komunikacija između ovih računala šifrirana? Analizirajte slanje segmenata koji se odnose na prijenos lozinke.

1.5.4 Protokol HTTP

HTTP (*HyperText Transfer Protocol*) je aplikacijski protokol koji definira uslugu prijenosa web-sadržaja između računala. Izvorno je HTTP bio namijenjen za prijenos tzv. hiperteksta, ali danas ima gotovo univerzalnu primjenu - koristi se za prijenos datoteka (umjesto protokola FTP), kod usluga prilagođenih webu (npr., *web-mail*) i sl.

Topologija mreže podešena za analizu protokola HTTP nalazi se u datoteci *Examples\DNS+Mail+WEB\NETWORK.inm*. Za ispravno generiranje HTTP-prometa potrebno je na odgovarajućim računalima pokrenuti DNS-poslužitelje i HTTP-poslužitelj. To se radi u sljedećim koracima:

1. Pokrenuti simulaciju nakon učitavanja mreže
2. U konzoli (*Xfce Menu -> Terminal*) računala na kojem je pokrenut IMUNES, pozicionirati se u direktorij *DNS+Mail+WEB*:

```
# cd /root/Examples/DNS+Mail+WEB/
```

3. Konfigurirati poslužitelje naredbama:

```
# ./start_dns  
# ./start_http
```

Webu se pristupa s računala *pc*, te je na njemu potrebno uključiti snimanje prometa alatom *Wireshark*. Odabirom računala *pc*, desnom tipkom miša otvara se izbornik, te se pokreće web-preglednik *Links* (*Links Browser*). Pritom je poželjno izbrisati priručno spremište web-preglednika. To se radi tako da se klikne mišem na vrh prozora preglednika *Links* (siva traka) kako bi se pojavio izbornik te se onda odabere opcija *File → Flush all caches*.

Početna stranica web-sjedišta na poslužitelju *www.tel.fer.hr* otvara se pritiskom na tipku G u web-pregledniku *Links*, nakon čega se u traku za unos URI-a unese *http://www.tel.fer.hr*.

Uvidom u promet snimljen alatom *Wireshark*, mogu se primijetiti DNS-upiti i DNS-odgovori, te protokoli TCP i HTTP. DNS-upit šalje računalo *pc* svom nadležnom DNS-poslužitelju *dnsZpm* kako bi saznao IP-adresu računala *www.tel.fer.hr*, s obzirom da se u traku za unos URI-a upisalo FQDN (*Full Qualified Domain Name*) web-poslužitelja. Računalo *dnsZpm* potom vraća traženu IP-adresu računalu *pc*. Znanje o IP adresi web-poslužitelja je nužno kako bi se HTTP-poruke uspješno usmjerile od izvorišta do odredišta korištenjem mrežnog protokola IP.

Transportni protokol TCP koristi se kao spojna usluga protokolu HTTP. Pritom se na računalu *pc* koriste proizvoljna TCP-vrata, dok se na web-poslužitelju koriste dobro znana vrata 80. Nakon uspostave TCP-sjednice između klijenta i poslužitelja, klijent može započeti sa slanjem HTTP-zahtjeva. S obzirom da je u ispisu alata *Wireshark* vidljivo nekoliko TCP-konekcija (što se može vidjeti odabirom opcije *Statistics → Conversation List → TCP (IPv4 & IPv6)* u izbornoj traci alata), analizirajmo pobliže prvu konekciju. Označi li se prva TCP-poruka koja se pojavljuje u ispisu, a zatim se pritisnite desna tipka miša te odabere opcija *Follow TCP stream*, dobije se ispis kao na slici (Slika 1.24) koji omogućava lakše praćenje svih poruka protokola HTTP koje su se izmijenile u toj TCP-konekciji.

Prva poruka koja se javlja je poruka GET, koju šalje računalo *pc*. Tom porukom traži se dohvatanje resursa s web-poslužitelja. U ispisu su vidljiva su dva karakteristična dijela poruke protokola HTTP:

- prvi redak - sadrži metodu zahtjeva, lokaciju traženog resursa (u ovom slučaju lokacija je / jer se traži početna stranica web-sjedišta), te verziju protokola
- zaglavje – sadrži ime poslužitelja na kojem se nalazi traženi resurs (*www.tel.fer.hr*), ime korištenog web-preglednika te ostale parametre

Kao odgovor web-poslužitelja (tj. računala *www.tel.fer.hr*) na zahtjev GET šalje se odgovor 200 OK. Tim odgovorom signalizira se računalu *pc* da je traženi resurs dostupan te se on istovremeno i dostavlja. U zaglavljima odgovora nalaze se dodatni podaci o resursu, poput vremena zadnje promjene, duljine resursa, itd. Također je vidljiv treći karakterističan dio poruke protokola HTTP – tijelo poruke. U tijelu poruke nalazi se traženi resurs: u ovom slučaju radi se o dokumentu pisanom jezikom HTML.

```
GET / HTTP/1.0
Host: www.tel.fer.hr
User-Agent: Links (2.2; FreeBSD 8.1-RELEASE i386; x)
Accept: */*
Accept-Encoding: gzip, deflate, bzip2
Accept-Charset: us-ascii, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8,
ISO-8859-9, ISO-8859-10, ISO-8859-13, ISO-8859-14, ISO-8859-15, ISO-8859-16, windows-1250, windows-1251, windows-1252,
windows-1256, windows-1257, cp437, cp737, cp850, cp852, cp866, x-cp866-u, x-mac, x-mac-ce, x-kam-cs, koi8-r, koi8-u, koi8-
ru, TCVN-5712, VISCII, utf-8
Accept-Language: en, *;q=0.1

HTTP/1.0 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "-515416085"
Last-Modified: Fri, 04 Feb 2011 16:51:32 GMT
Content-Length: 348
Connection: close
Date: Fri, 04 Feb 2011 16:52:13 GMT
Server: lighttpd/1.4.26

<HTML>
<H1>Test file - www.tel.fer.hr</H1>
<img src=freedom.gif height=94 width=306 border=0>
<p>This is a starting page of Web servera www.tel.fer.hr
<p>Just a few lines of text...
<p>bla bla bla
<br>Horizontal line
<br>
<p><a href=form.html>Link on form</a>
<p><a href="http://www.zpm.fer.hr">Link on ZPM</a>
<br>
<p>Copyright (MM) 2008
</HTML>
```

Slika 1.24 Poruke protokola HTTP izmijenjene u jednoj TCP-konekciji

Zadaci 36. Otvorite početnu stranicu web-poslužitelja *www.zpm.fer.hr* (*zpmMail*) korištenjem poveznice *Link on ZPM*. Koliko se HTTP-konekcija uspostavi u ovom primjeru? Čemu služe te konekcije? Odredite transportne adrese u svakoj od njih.

Zadaci 37. Vratite se na početnu web-stranicu Zavoda za telekomunikacije (poveznica *Link on ZZT*). Zašto se pritom nije stvorila nova HTTP-konekcija, koja bi dohvatala početnu web-stranicu s poslužitelja www.tel.fer.hr?

1.5.5 Pitanja

Pitanje 21. Koja je uloga DNS-a?

- a. pridruživanje numeričke IP adrese na osnovu poznate MAC adrese.
- b. pridruživanje MAC adrese na osnovu poznate IP adrese.
- c. pridruživanje simboličke adrese na osnovu poznate numeričke IP adrese.
- d. pridruživanje simboličke adrese na osnovu poznate MAC adrese.

Pitanje 22. Koja od navedenih tvrdnji je istinita?

- a. u javnom Internetu može postojati više računala s istom IP adresom, ali u tom slučaju moraju imati različite simboličke adrese.
- b. u javnom Internetu svako računalo ima jedinstvenu IP adresu, ali simboličke adrese ne moraju biti jedinstvene.
- c. u javnom Internetu može postojati više računala s istom IP adresom.
- d. u javnom internetu ne mogu postojati dvije identične simboličke adrese

Pitanje 23. Na koji transportni protokol se oslanjaju protokoli za čitanje pošte?

- a. ICMP.
- b. IP.
- c. UDP.
- d. TCP.

Pitanje 24. Prilikom slanja elektroničke pošte putem protokola SMTP, poslužitelj na zahtjeve klijenta odgovara:

- a. DATA zahtjevima.
- b. ACK zahtjevima.
- c. SUCCESS ili FAILURE zahtjevima.
- d. statusnim kodom.

Pitanje 25. Shema URI-ja:

- a. identificira virtualnog poslužitelja.
- b. određuje protokol koji se koristi.
- c. određuje aplikaciju kojom se pristupa resursu.
- d. određuje pojedini resurs na poslužitelju.