Tin Plavec,
0036522334

Labos 3
Komunikacijske mreže

34. Snimljen promet na eth0@pc3:

```
2 5.913079857   0.0.0.0           255.255.255.255   DHCP    342 DHCP Discover
3 5.913495606   42:00:aa:00:00:03 Broadcast         ARP      42 Who has 10.0.0
4 6.917197498   10.0.0.1          10.0.0.12         DHCP    342 DHCP Offer
5 8.934216427   0.0.0.0           255.255.255.255   DHCP    342 DHCP Request
6 8.935322819   10.0.0.1          10.0.0.12         DHCP    342 DHCP ACK
```

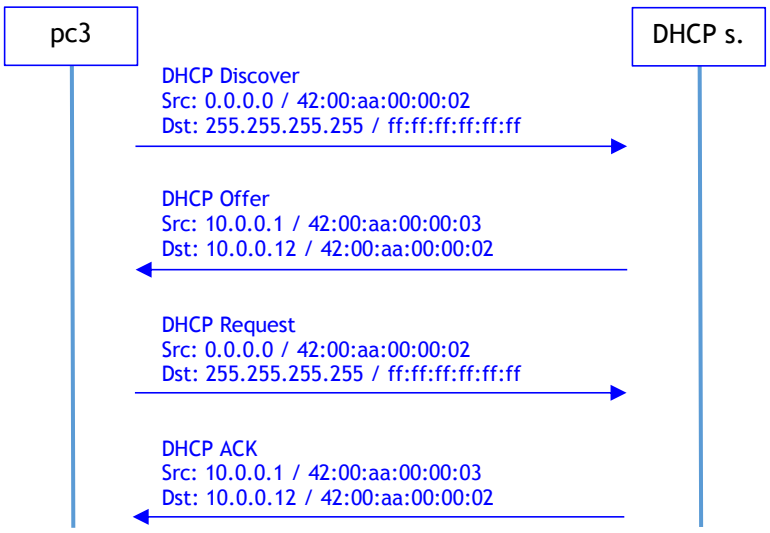
DHCP je protokol za dodjelivanje IP adresa. Prva DHCP poruka je Discover. Tom porukom pc3 zahtjeva dodjelu IP adrese. Izvorišna IP adresa poruke je 0.0.0.0 jer pc3 jednostavno još nema IP adresu. Odredišna IP adresa je broadcast adresa jer pc3 još ne zna IP adresu DHCP poslužitelja. Poruka također sadrži (klijentsku) MAC adresu od pc3. DHCP poslužitelj odgovara porukom Offer u kojoj nudi pc3 IP adresu. Ponuđena IP adresa ujedno je i odredišna adresa ove poruke. Poruka sadrži još neke informacije vezane za DNS i defaultni usmjeritelj:

```
▸ Option: (53) DHCP Message Type (Offer)
▸ Option: (54) DHCP Server Identifier (10.0.0.1)
▸ Option: (51) IP Address Lease Time
▸ Option: (1) Subnet Mask (255.255.255.0)
▸ Option: (3) Router
▾ Option: (15) Domain Name
    Length: 10
    Domain Name: imunes.net
▾ Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 10.0.0.53
    Domain Name Server: 10.0.0.54
```

Zatim pc3 šalje broadcast zahtjev za ponuđenu IP adresu. Ukoliko je sve u redu, DHCP poslušitelj uzvraća ACK, odsnosno potvrdnu poruku. pc3 sada ima svoju IP adresu te svaki sljedeći paket od pc3 ima adresu `10.0.0.12` kao izvorišnu. Ova poruka sadži i vrijeme najma adrese, nakon kojeg treba opet potvrditi postojeću ili zahtjevati novu IP adresu:

```
▾ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (600s) 10 minutes
```

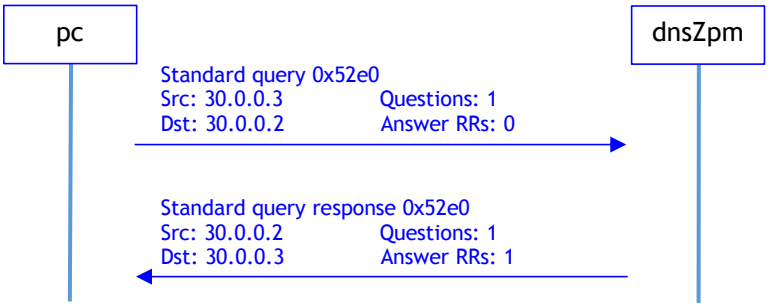
Iznos vremena određuje administrator sustava. Načelno, što je frekventnija izmjena uređaja u mreži, to vrijeme treba biti manje kako bi se osiguralo da svaki uređaj može dobiti IP adresu čim uđe u mrežu, a ne da mora čekati zbog nedostatka IP adresa (pod)mreže.



35. Rješenja su u tablici:

IP adresa računala *dnsHr.hr*	7.0.0.2
računalo nadležno za primanje pošte u domeni *zpm.fer.hr*	zpmMail.zpm.fer.hr
računalo nadležno za primanje pošte u domeni *tel.fer.hr*	www.tel.fer.hr
DNS poslužitelji nadležni za domenu *hr*	dnsHr.hr | hr2.com
DNS poslužitelji nadležni za domenu *fer.hr*	dnsFer.fer.hr
DNS poslužitelji nadležni za domenu tel.fer.hr	dnsTel.tel.fer.hr
DNS poslužitelji nadležni za vršnu domenu .	cRootServer | bRootServer | aRootServer
ime računala s IP adresom 20.0.0.4	mm.tel.fer.hr

36. Naredba `host -t MX tel.fer.hr` vraća nadležno računalo za poštu te domene.
eth0@pc:



Ovdje vidimo komunikaciju između pc i lokalnog DNS poslužitelja. No, ovo nije potpun prikaz. Naime, dnsZpm ne zna ništa o domeni te.fer.hr, te mora iterativno slati upite nadređenim DNS poslužiteljima.

```
    5 11.961316916  30.0.0.2        2.0.0.2         DNS      85 Standard query 0xa0e6 NS hr OPT
    6 12.079823280  2.0.0.2         30.0.0.2        DNS     174 Standard query response 0xa0e6 NS hr NS hr2.com NS dnsHr.hr A 7.0.0.2 A 4
    7 12.080298176  30.0.0.2        7.0.0.2         DNS      85 Standard query 0x9000 NS hr OPT
    8 12.159803230  7.0.0.2         30.0.0.2        DNS     142 Standard query response 0x9000 NS hr NS hr2.com NS dnsHr.hr OPT
    9 12.160572719  30.0.0.2        4.0.0.2         DNS      89 Standard query 0xae7c NS fer.hr OPT
   10 12.279834705  4.0.0.2         30.0.0.2        DNS     142 Standard query response 0xae7c NS fer.hr NS dnsFer.fer.hr A 8.0.0.2 OPT
   11 12.280770601  30.0.0.2        8.0.0.2         DNS      89 Standard query 0x94f5 NS fer.hr OPT
   12 12.359837251  8.0.0.2         30.0.0.2        DNS     126 Standard query response 0x94f5 NS fer.hr NS dnsFer.fer.hr OPT
   13 12.360586663  30.0.0.2        8.0.0.2         DNS     109 Standard query 0x5dfa MX tel.fer.hr OPT
   14 12.360761877  30.0.0.2        1.0.0.2         DNS     112 Standard query 0xdf70 AAAA dnsFer.fer.hr OPT
   15 12.409805199  8.0.0.2         30.0.0.2        DNS     146 Standard query response 0x5dfa MX tel.fer.hr NS dnsTel.tel.fer.hr A 20.0.
   16 12.410240372  30.0.0.2        20.0.0.2        DNS      93 Standard query 0x357c MX tel.fer.hr OPT
   17 12.479846780  1.0.0.2         30.0.0.2        DNS     187 Standard query response 0xdf70 AAAA dnsFer.fer.hr NS hr2.com NS dnsHr.hr
   18 12.480213807  30.0.0.2        7.0.0.2         DNS     112 Standard query 0x8280 AAAA dnsFer.fer.hr OPT
   19 12.529867211  20.0.0.2        30.0.0.2        DNS     129 Standard query response 0x357c MX tel.fer.hr MX 10 www.tel.fer.hr OPT
   20 12.530132901  30.0.0.2        30.0.0.3        DNS      90 Standard query response 0x22da MX tel.fer.hr MX 10 www.tel.fer.hr
   21 12.559817453  7.0.0.2         30.0.0.2        DNS     142 Standard query response 0x8280 AAAA dnsFer.fer.hr NS dnsFer.fer.hr A 8.0.
   22 12.560111211  30.0.0.2        8.0.0.2         DNS     112 Standard query 0x07b7 AAAA dnsFer.fer.hr OPT
   23 12.620569333  8.0.0.2         30.0.0.2        DNS     173 Standard query response 0x07b7 AAAA dnsFer.fer.hr SOA dnsFer.fer.hr OPT
```

Prvo kontaktira vršni poslužitelj (u ovom slučaju bRootServer). On mu pak vraća informaciju o .hr. Zatim dnsZpm traži poslužitelj za .hr, odnosno za fer.hr. Završetkom ovog iterativnog postupka dolazi do tel.fer.hr. dnsZpm sada do pc šalje query response s traženim informacijama. Taj zadnji korak je pak rekurzivni postupak.

37. Naredba `host -t NS .` vraća vršnog DNS poslužitelja.
Poruka zahtjeva ima odredišna vrata 53:

```
▾ User Datagram Protocol, Src Port: 47750, Dst Port: 53
    Source Port: 47750
    Destination Port: 53
    Length: 25
    Checksum: 0xb757 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

Ovo su standardna vrata za DNS poslužitelje. DNS poruke obično se razmjenju putem UDP-a. U slučajevima kada je veličina poruke prevelika za jedan paket UDP-a koristi se TCP.

38. Protokoli prilikom slanja jednostavne mail poruke:

Address Resolution Protocol : sloj podatkovne poveznice
- već poznat protokol za prevođenje IP adresa u MAC adrese

Transmission Control Protocol : transportni sloj
- već poznat protkol za transmisiju segmenata između dva udaljena procesa
- pouzdan jer razmjenjuje potvrde

Domain Name System : aplikacijski sloj
- protokol za prevođenje domenskih naziva u IP adrese

Simple Mail Transfer Protocol : aplikacijski sloj
- protokol za transimisiju elektroničke pošte

Internet Message Format : aplikacijski sloj
- protokol za kodiranje i format poruka
- nužan za SMTP

❖ Koraci prilikom slanja elektroničke pošte:

izvorišni MUA (mm) -> izvorišni MTA (www)
- mm zbog DHCP zna IP adresu lokalnog DNS poslužitelja
- mm koristi ARP da sazna MAC adresu lokalnog DNS poslužitelja
- mm koristi DNS i ARP kako bi pronašao lokalni MTA (IP, pa MAC adresu)
- uspostavlja se TCP veza mm:40529 <-> www:25
- SMTP protokolom se razmjenjuju mail informacije te se veza zatvara

Address A	Port A	Address B	Port B	Packets	Bytes
20.0.0.3	54326	30.0.0.4	25	14	1931
20.0.0.4	40529	20.0.0.3	25	24	2270

izvorišni MTA (www) -> odredišni MTA (zpmMail)
- www koristi DNS i ARP kako bi pronašao MTA za domenu e-poruke (IP, pa MAC adresu)
- uspostavlja se TCP veza www:54326 <-> zpmMail:25
- SMTP protokolom se razmjenjuju mail informacije te se veza zatvara

odredišni MTA (zpmMail) -> odredišni MUA
- mail stiže korisniku kojem pripada odredišna adresa e-poruke

Nakon jednog slanja, računala će zapamtiti DNS zapise te ih neće morati svaki put tražiti iznova.

❖ Komunikacija SMTP protokolom:

- www šalje prvu poruku ESMTP Postfix
- mm se predstavlja porukom HELO
- www prihvaća
- mm šalje zaglavlje e-poruke (polja od, do)
- www prihvaća
- mm najavljuje slanje podataka te ih šalje
- www prihvaća te pozdravlja

```
220 www.tel.fer.hr ESMTP Postfix (3.3.4)
HELO mm.tel.fer.hr
250 www.tel.fer.hr
MAIL FROM:<root@tel.fer.hr>
250 2.1.0 Ok
RCPT TO:<imunes@zpm.fer.hr>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Wed, 26 May 2021 18:27:48 +0000
From: Tin Plavec <root@tel.fer.hr>
To: imunes@zpm.fer.hr
Subject: Pozdrav
Message-Id: <20210526182748.59d0403b776ec948526940d8@tel.fer.hr>
X-Mailer: Sylpheed 3.7.0 (GTK+ 2.24.32; i386-portbld-freebsd11.2)
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

Hello world!

--
Tin Plavec <root@tel.fer.hr>
.
250 2.0.0 Ok: queued as 2DF2C160E8E
QUIT
221 2.0.0 Bye
```

39. Protokoli prilikom pristupanja POP poslužitelju:

Address Resolution Protocol : sloj podatkovne poveznice
- već poznat protokol za prevođenje IP adresa u MAC adrese

Transmission Control Protocol : transportni sloj
- već poznat protkol za transmisiju segmenata između dva udaljena procesa
- pouzdan jer razmjenjuje potvrde

Domain Name System : aplikacijski sloj
- protokol za prevođenje domenskih naziva u IP adrese

Post Office Protocol : aplikacijski sloj
- protokol za klijentsko dohvaćanje e-pošte s poslužitelja

Za pristup se uspostavila samo jedna TCP veza na vratima 110:

Address A	Port A	Address B	Port B	Packets	Bytes
30.0.0.3	61892	30.0.0.4	110	18	1271

To je i logično jer smo izvršili jedan (jednosmjerni) zahtjev prema poslužitelju.
DNS protokol koristi se za prevođenje naziva zpmMail.zpm.fer.hr u IP adresu.

❖ Komunikacija POP protokolom:

- poslužitelj se javlja klijentu
- klijent šalje USER i PASS kako bi se autentificirao na poslužitelju
- klijent šalje STAT, UIDL, LIST kako bi saznao metapodatke o e-porukama (npr. količinu, duljinu)
- poslužitelj mu daje odgovore
- klijent naredbom RETR <i> zahtjeva točno određen mail (namijenjen njemu)
- poslužitelj šalje zathjevane mail poruke
- klijent zatvara vezu naredbom QUIT

Primljena poruka išla je od računala mm.tel.fer.hr (MUA) preko tel.fer.hr (MTA) te zpmMail.zpm.fer.hr (MTA) pa konačno do pc.zpm.fer.hr (MUA).
Ova komunikacija nije šifrirana. Ime korisnika i lozinka prenose se *plaintextom*.

40. Prilikom otvaranja stranice www.zpm.fer.hr otvorile su se 3 TCP veze:

Address A	Port A	Address B	Port B	Packets	Bytes
30.0.0.3	10001	30.0.0.4	80	11	1579
30.0.0.3	10002	30.0.0.4	80	18	7701
30.0.0.3	10000	30.0.0.4	80	7	478

Da su ovo HTTP veze, možemo prepoznati po općepoznatom portu 80.

Prva veza (vrata 10001) služi za prijenos HTML stranice:

```
GET / HTTP/1.1
Host: www.zpm.fer.hr
User-Agent: Mozilla/5.0 (X11; FreeBSD i386; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "767125387"
Last-Modified: Wed, 26 May 2021 22:35:39 GMT
Content-Length: 309
Date: Wed, 26 May 2021 22:36:49 GMT
Server: lighttpd/1.4.53

<HTML>
<H1>Probni index fajl - zpmMail.zpm.fer.hr</H1>
<img src=powerlogo.gif height=64 width=160 border=0>
<p>>This is a starting page of Web servera zpmMail.zpm.fer.hr
<p>bla bla bla ...
<p><a href="http://www.tel.fer.hr/">Link on ZZT</a>
<p>
<br>Horizonal ruler
<hr>
Copyright (MM) 2008
</HTML>
```

Druga veza (vrata 10002) služi za prijenos logotipa i favicona:

```
GET /powerlogo.gif HTTP/1.1
Host: www.zpm.fer.hr
User-Agent: Mozilla/5.0 (X11; FreeBSD i386; rv:67.0) Gecko/20100101 Firefox/
67.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.zpm.fer.hr/
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: image/gif
Accept-Ranges: bytes
ETag: "3516108184"
Last-Modified: Wed, 26 May 2021 22:35:39 GMT
Content-Length: 5279
Date: Wed, 26 May 2021 22:36:49 GMT
Server: lighttpd/1.4.53

GIF89a..@.............!........*....%4..%#.P$$0%.R% )&.)'.U(0A*.Y*"4+.S+.N+'9,.
[-.^00.0001)=2.T2.@26E3/@4..5$36)?8(78F\90@90H:3J:6D<.H<+
<=O=0#>5H>>&?8J@.IC6IC9MD=VD>DD>NE.HEEZF3:G.:H.EHHOJ?WJHaJc.K+:L"?L(?
MD]MMbMS`OZoP.@Q?MQI\Qn.R7GS#=U'@W/
```

Treća veza (vrata 10000) nema sadržaja.

41. Http zahtjev (GET) na vratima 10001:

Host : naziv poslužitelja
User-Agent : informacije o pregledniku koji korisnik koristi
Accept : prihvatljive vrste datoteka
Accept-Language : prihvatljivi jezici stranice
Accept-Encoding : prihvatljiva kodiranja
Connection : mogućnosti veze
Upgrade-Insecure-Requests : HTTP zahtjeve pretvaraj u HTTPS

- Http odgovor (200 OK) na vratima 10001:

Content-Type : vrsta datoteke
Accept-Ranges : prihvaćanje djelomičnih zahtjeva
ETag : identifikator resursa
Last-Modified : trenutak posljednje izmjene resursa
Content-Length : duljina datoteke
Date : trenutak slanja
Server : aplikacija za posluživanje
- Sadržaj datoteke -

42. Parametar If-Modified-Since služi za mrežnu optimizaciju. Parametar se šalje prilikom HTTP zahtjeva. On pohranjuje kada je klijent zadnji put dohvatio stranicu s poslužitelja. Ukoliko poslužitelj uvidi da se od tada stranica (ili bilo što što je sadržaj zahtjeva) nije promijenila, tijelo HTTP odgovora (304 Not Modified) bit će prazno. Internetski preglednik zna da treba učitati stranicu iz lokalnog spremnika. Na ovaj način stranica će biti učitana brže, a mrežni promet sačuvan.