

DNS SERVIS

II DEO

Predmet: Mrežni servisi

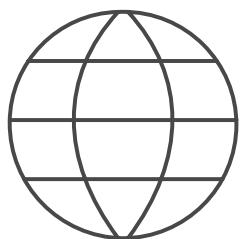
Predavač: dr Dušan Stefanović

DNS ZAPISI

DNS zapis (Resource Record) je osnovna jedinica podataka u DNS bazi.

Svaki zapis povezuje određeni domen sa nekim tipom informacije.

format DNS zapisa: <ime> <TTL> <klasa> <tip> <podatak>



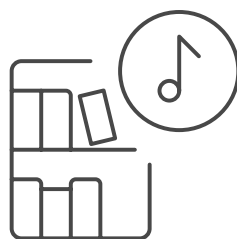
Ime domena

Definiše naziv domena



TTL

Vreme u sekundama koliko se čuva keširani podatak



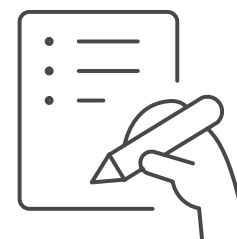
Klasa

DNS klasa zapisa (najčešće IN - Internet)



Tip

Tip DNS zapisa



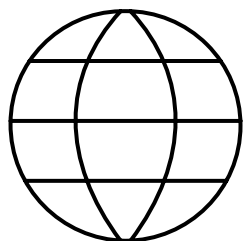
Vrednost

Sadrži vrednost zapisa

KOMPONENTE DNS ZAPISA

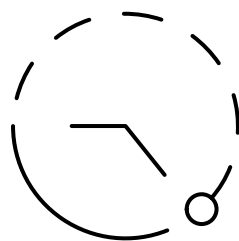
PRIMER

odseknis.akademijanis.edu.rs. 3600 IN A 160.99.37.100



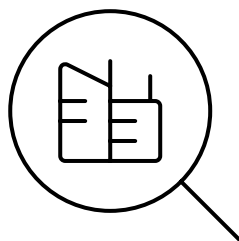
Ime hosta

ime hosta u DNS zapisu.



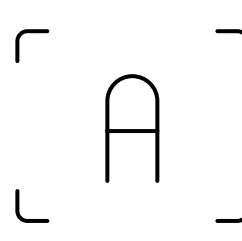
TTL

3600 sek.
predstavlja vreme
trajanja keširanog
podatka.



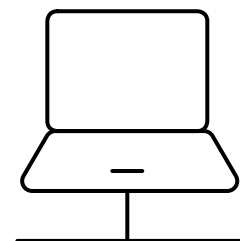
IN

IN (Internet)
označava klasu
zapisa.



Tip zapisa

A označava tip DNS
zapisa.



IP adresa

160.99.37.100 je
adresa koja
odgovara imenu
hosta.

OSNOVNI DNS ZAPISI



A Record

Preslikava ime hosta u IPv4 adresu



AAAA Record

Preslikava ime hosta u IPv6 adresu



CNAME Record

Alias jednog domena ka drugom



MX Record

Definiše mejl server za domen



SOA Record

Početni zapis DNS zone



NS Record

Označava autoritativne DNS servere



SRV Record

Locira specifične servise u domenu



TXT Record

Unosi proizvoljne tekstualne podatke



PTR Record

Omogućava obrnutu DNS rezoluciju

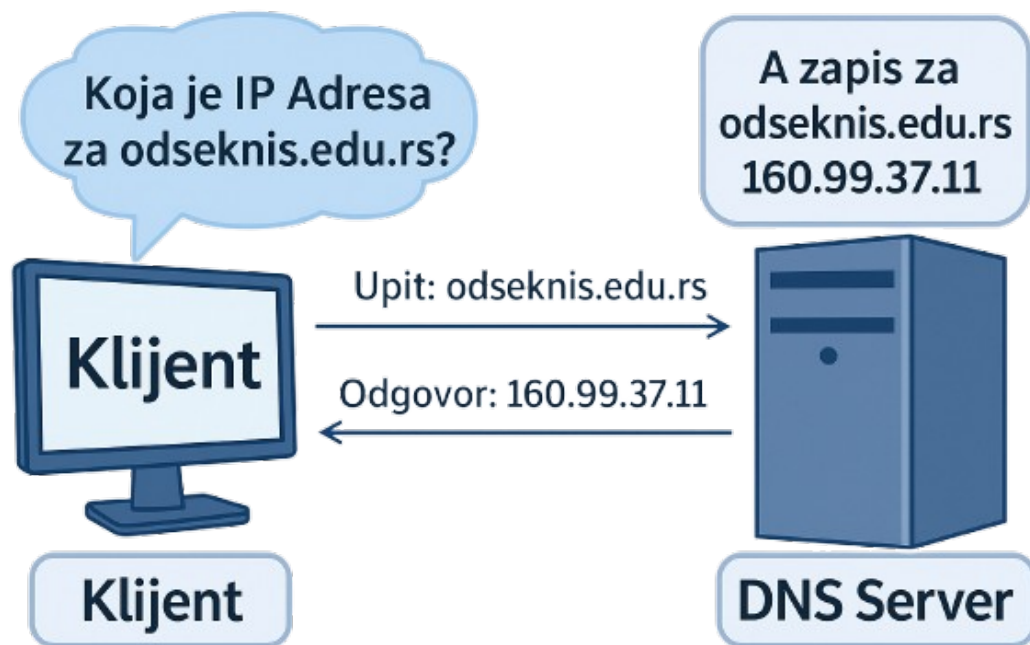
A I AAAA HOST ZAPIS

HOST zapis čuva IP adresu za dato DNS ime

Najčešći tip zapisa jer ime svakog uređaja se razrešava korišćenjem Host zapisa

A zapis se koristi za IPv4 adrese

AAAA zapis se koristi za IPv6 adrese



<ime> <TTL> IN A <IPv4 adresa>

www.odseknis.edu.rs. 3600 IN A 192.0.2.1

LOAD BALANCING A ZAPIS

Round-Robin Load Balancing

odseknis.edu.rs

160.99.37.11



Prvi
korisnik

160.99.37.12



Drugi
korisnik

160.99.37.13



Treći
korisnik

Round-Robin Load Balancing

odseknis.edu.rs. 3600 IN A 160.99.37.11

odseknis.edu.rs. 3600 IN A 160.99.37.12

odseknis.edu.rs. 3600 IN A 160.99.37.13

Geografski Load Balancing (GeoDNS)

odseknis.edu.rs. 3600 IN A 160.99.37.11 ; Evropa

odseknis.edu.rs. 3600 IN A 203.0.113.8 ; Azija

odseknis.edu.rs. 3600 IN A 192.0.2.5 ; SAD

CNAME ZAPIS

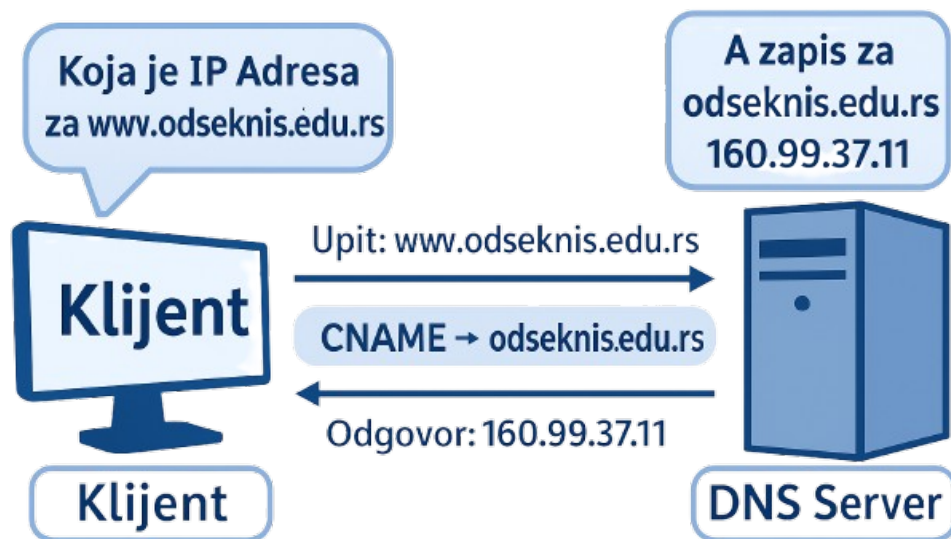
Alternativno ime ili alias

Upotrebom alijasa možemo promeniti naziv računara koji obezbeđuje neki Internet servis(Web,Ftp,..) a da mu ne menjamo adresni (A) zapis.

Omogućava **više imena za isti server**

Klijent će najpre tražiti CNAME zapis, a zatim dobiti odgovarajući **A zapis** za kanoničko ime.

www.odseknis.edu.rs. IN CNAME odseknis.edu.rs.
odseknis.edu.rs. IN A 160.99.37.11



NAME SERVER (NS) ZAPIS

NS zapisi ukazuju na DNS servere koji su autorativni za taj domen

NS zapis se navodi za primarni i sve sekundarne NS servere

<ime domena> IN NS <ime servera>

<ime domena> je naziv domena za koji naznačeni server poseduje zonsku konfiguraciju

<ime servera> je naziv hosta koji je autorativan za taj domen



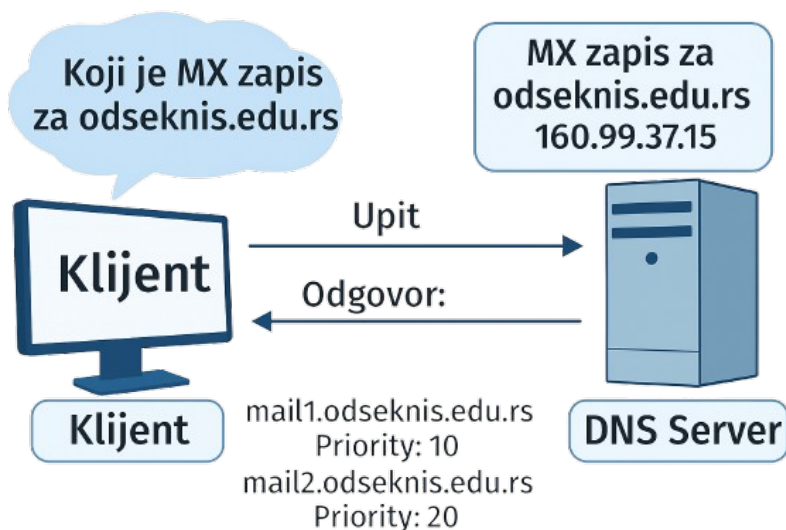
odseknis.edu.rs. IN NS ns1.odseknis.edu.rs.
IN NS ns2.odseknis.edu.rs.

MX (MAIL EXCHANGE) ZAPIS

Identifikuje mail server za dato DNS ime

MX zapis sadrži i priority vrednost koja se koristi ukoliko isti domen opslužuju više mail servera

Manja **priority** vrednost se prvo uzima, ukoliko su priority vrednosti iste, izbor je slučajan



mail1	A	160.99.37.15
mail2	A	160.99.37.16
odseknis.edu.rs.	MX	10 mail1
odseknis.edu.rs.	MX	20 mail2

SOA (START OF AUTHORITY) ZAPIS

SOA (Start of Authority) zapis je ključni DNS zapis koji definiše osnovne informacije o DNS zoni, kao što su autoritet, vremenski intervali za keširanje i sinhronizaciju među serverima.

SOA zapis je obavezan u svakoj DNS zoni.

Mora biti prvi zapis u datoteci zone.

Koristi se i za sinhronizaciju između primarnog i sekundarnih DNS servera

odseknis.edu.rs. IN SOA ns1.odseknis.edu.rs.
admin.odseknis.edu.rs. (

2025050301 ; Serial

3600 ; Refresh (1h)

600 ; Retry (10min)

1209600 ; Expire (14d)

86400) ; Minimum TTL (1d)

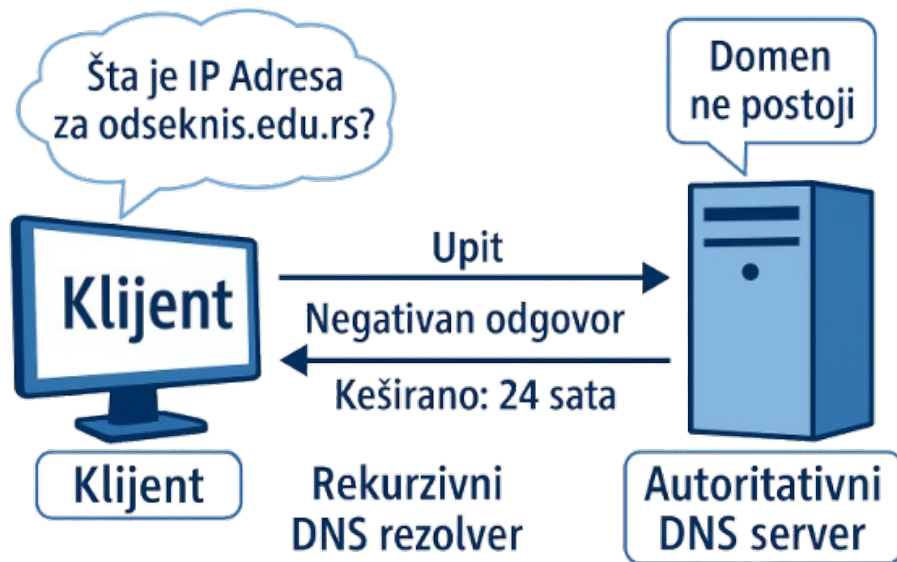
Polje	Opis
Primary NS	ns1.odseknis.edu.rs. – primarni DNS server za zonu
Email admina	admin.odseknis.edu.rs. – kontakt osoba za zonu (zameni @ sa .)
Serial	2025050301 – broj verzije zone (godina+mesec+dan+revizija)
Refresh	3600 – na svakih 1h sekundarni proverava da li ima novih podataka
Retry	600 – ako refresh ne uspe, ponavlja pokušaj za 10 minuta
Expire	1209600 – posle 14 dana sekundarni smatra zonu nevažećom
Minimum TTL	86400 – koliko dugo rekurzivni resolveri keširaju negativne odgovore (npr. NXDOMAIN)

NEGATIVNI ODGOVORI

Rekurzivni DNS resolveri keširaju negativne odgovore (npr. da neki domen ne postoji) u polju Minimum TTL (poznato i kao Negative TTL)

U ovom primeru: 86400 sekundi = 24 sata

To znači da, ako DNS server sazna da neki zapis ne postoji (npr. xyz.odseknis.edu.rs), on će zapamtiti (keširati) tu informaciju kao negativan odgovor 24 sata.



```
odseknis.edu.rs. IN SOA ns1.odseknis.edu.rs.
admin.odseknis.edu.rs. (
```

```
2025050301 ; Serial
```

```
3600 ; Refresh (1h)
```

```
600 ; Retry (10min)
```

```
1209600 ; Expire (14d)
```

```
86400 ) ; Minimum TTL (1d)
```

SRV (SERVICE) ZAPIS

SRV (Service) zapis je DNS zapis koji omogućava lociranje specifičnih servisa unutar domena, kao što su VoIP, LDAP, SIP i drugi.

_ldap._tcp.odseknis.edu.rs. 3600 IN SRV 10 0 389 ldap1.odseknis.edu.rs.

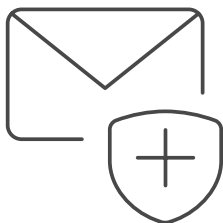
Polje	Vrednost	Objašnjenje
Servis	_ldap	Traži se LDAP servis
Protokol	_tcp	LDAP koristi TCP protokol
Domen	odseknis.edu.rs	Za koji domen se traži LDAP servis
TTL	3600	Vreme keširanja (1 sat)
Priority	10	Niža vrednost = veći prioritet
Weight	0	Nema balansiranja jer postoji samo jedan server
Port	389	Standardni port za LDAP
Target	ldap1.odseknis.edu.rs.	DNS ime servera koji nudi LDAP uslugu

TXT (TEXT) ZAPIS

TXT (Text) zapis u DNS-u služi za **unošenje proizvoljnog teksta** vezanog za neki domen.

U praksi, koristi se za brojne **sigurnosne i verifikacione svrhe**

odseknis.edu.rs. IN TXT "v=spf1 ip4:160.99.37.0/24 -all"



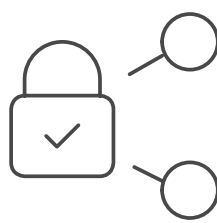
SPF

Verifikacija okvira
politike pošiljaoca.



DKIM

Protokol
bezbednosti
identifikovanih
domena.



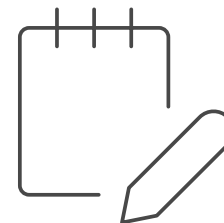
DMARC

Verifikacija poruka,
izveštavanje i
usklađenost.



Verifikacija domena

Verifikacija domena
za usluge.



Napomene

Skladištenje
napomena i
informacija o
vlasništvu.

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

SPF (Sender Policy Framework) je DNS mehanizam za zaštitu od lažiranja pošiljalaca e-pošte (spoofing).

On definiše koje IP adrese imaju dozvolu da šalju mejlove u ime određenog domena.

odseknis.edu.rs. IN TXT "v=spf1 ip4:160.99.37.0/24 -all"

Deo	Značenje
v=spf1	Verzija SPF protokola (uvek počinje ovako)
ip4:160.99.37.0/24	Dozvoljeno slanje mejlova sa bilo koje IP adrese iz ovog opsega
-all	Sve ostale IP adrese su izričito zabranjene (hard fail)

"v=spf1 ip4:160.99.37.10 ip4:160.99.37.11 include:_spf.google.com -all"

Dozvoljene IP:160.99.37.10 i 160.99.37.11

Takođe svi koji su u SPF zapisu za google.com (npr. ako se koristi Gmail za slanje)

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

DKIM (DomainKeys Identified Mail) je mehanizam za autentifikaciju e-pošte koji omogućava digitalno potpisivanje poruka tako da primalac može da proveriti:

1. da poruka nije izmenjena u transport
2. da je zaista poslata sa servera ovlašćenog za domen

Pošiljalac (mail server) generiše digitalni potpis iz sadržaja poruke + zaglavlja.

Potpis se dodaje u zaglavlje mejla kao DKIM-Signature:

Primalac vidi DKIM-Signature zaglavlje. Primalac pronalazui javni ključ u DNS zapisu pomoću koga proverava da li se potpis poklapa sa sadržajem poruke

default._domainkey.odseknis.edu.rs. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GC...QAB"

Element	Opis
v=DKIM1	Verzija DKIM
k=rsa	Algoritam za enkripciju
p=...	Javni RSA ključ koji koristi primalac za verifikaciju potpisa

PRIMERI PRAKTIČNE UPOTREBE TXT ZAPISA

DMARC (Domain-based Message Authentication, Reporting and Conformance) je mehanizam za autentifikaciju e-pošte koji se nadovezuje na SPF i DKIM i omogućava domenu da:

1. Sopšti serverima šta da urade ako SPF i/ili DKIM provera ne uspe (npr. da odbace mejl).
2. Prati i prijavljuje pokušaje zloupotrebe domena za slanje lažnih mejlova (phishing).
3. Štiti brend i korisnike od prevara u e-pošti.

DMARC politika u TXT zapisu za domen odseknis.edu.rs

_dmarc.odseknis.edu.rs. IN TXT

"v=DMARC1; p=reject; rua=mailto:dmarc@odseknis.edu.rs; ruf=mailto:forenzika@odseknis.edu.rs; fo=1"

Element	Značenje
v=DMARC1	Verzija protokola
p=reject	Odbaci mejlove koji ne prođu SPF/DKIM
rua=	Adresa za agregatne izveštaje (ko šalje, koliko, rezultati)
ruf=	Adresa za forenzičke (detaljne) izveštaje
fo=1	Pošalji forenzički izveštaj za bilo koji neuspeh

FORMAT DNS PORUKE

DNS poruke:

Upiti (*query*) i **odgovori** (*reply*) imaju isti format poruke

Zaglavlje DNS poruke

identification: 16 bit broj za identifikaciju upita, odgovor sadrži istu vrednost

flags:

- 1bit: upit (0) ili odgovor (1)
- 1bit: rekurzivni upit se traži (1) ili ne (0)
- 1bit: rekurzija podržana (1) ili ne (0)
- 1 bit: odgovor je od autorizovanog n.s.(1)

Sadrži informacije o upitu koji se traži: ime, tip zapisa za upit (npr. tip A-ime hosta)

RR zapisi kao odgovor na pitanje

Zapisi o autorizovanim serverima

Dodatne “korisne” informacije (npr. ako je u polju “answers” bio MX zapis: ime mail servera, tada u ovom polju može biti njegova IP adresa)

identification	flags
number of questions	number of answer RR
number of authority RR	number of additional RR
questions (variable number of questions)	
answers (variable number of resource records)	
authority (variable number of resource records)	
additional information	



PRIMER DNS UPITA I ODGOVORA

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.116	192.168.1.1	DNS	69	Standard query 0x9926 A cisco.com
2	0.060677000	192.168.1.1	192.168.1.116	DNS	85	Standard query response 0x9926 A 72.163.4.161
3	0.072862000	192.168.1.116	72.163.4.161	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
4	0.151182000	72.163.4.161	192.168.1.116	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=238
5	1.074030000	192.168.1.116	72.163.4.161	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128
6	1.147913000	72.163.4.161	192.168.1.116	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=238
7	2.076166000	192.168.1.116	72.163.4.161	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128
8	2.148068000	72.163.4.161	192.168.1.116	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=238

dns upit

dns odgovor

Frame 2: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0	
Ethernet II, Src: CiscoCon_cc:a0:85 (c8:d7:19:cc:a0:85), Dst: IntelCor_45:5d:c4 (24:77:03:45:5d:c4)	
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.116 (192.168.1.116)	
User Datagram Protocol, Src Port: domain (53), Dst Port: 64103 (64103)	
Domain Name System (response)	
[Request In: 1]	
[Time: 0.060677000 seconds]	
Transaction ID: 0x9926	
Flags: 0x8180 standard query response, No error	
Questions: 1	
Answer RRs: 1	
Authority RRs: 0	
Additional RRs: 0	
Queries	
cisco.com: type A, class IN	
Name: cisco.com	
Type: A (Host address)	
Class: IN (0x0001)	
Answers	
cisco.com: type A, class IN, addr 72.163.4.161	

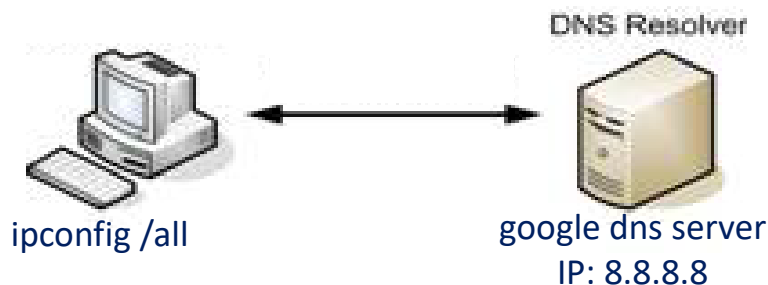
Ovaj paket sadrži odgovor na 1 upit u vidu jednog RR zapisa, ne sadrži informaciju o autorativnom NS serveru za taj zapis kao ni dodatne zapise

informacije o dns upitu

odgovor na upit

DNS ODGOVOR

INFORMACIJE O LOKALNOM DNS SERVERU



```
C:\Users\Korisnik>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Korisnik-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

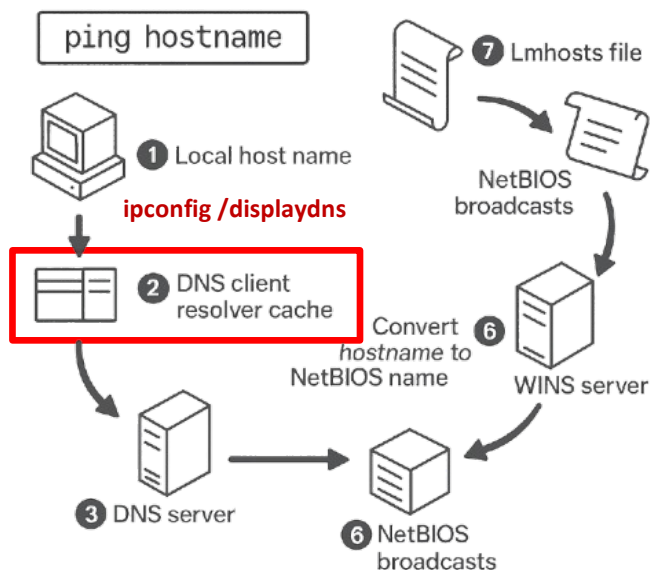
Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 38-59-F9-17-23-66
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . . :
Description . . . . . : Dell Wireless 1702 802.11b/g/n
Physical Address. . . . . : 38-59-F9-17-23-65
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::51a8:395a:a2d4:58db%12(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 24. august 2014 18:58:18
Lease Expires . . . . . : 25. august 2014 19:52:50
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 322460153
DHCPv6 Client DUID. . . . . : 00-01-00-01-16-30-01-FD-18-03-73-5E-ED-53
DNS Servers . . . . . : 8.8.8.8
NetBIOS over LCP . . . . . : Enabled
```

LOKALNI DNS KEŠ



ipconfig /displaydns

Prikaz lokalnog DNS keša na hostu, nakon isteka TTL vrednosti, DNS zapis se briše iz keša.

ipconfig /flushdns

Ručno brisanje svih zapisa iz lokalnog DNS keša hosta

Podrazumevana TTL vrednost za pozitivne odgovore je 86,400 sekunde (1 dan).

Podrazumevana TTL vrednost za negativne odgovore je 300 sekunde.

```
C:\Users\Korisnik>ipconfig /displaydns

Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : localhost

www.youtube.com
Record Name . . . . . : www.youtube.com
Record Type . . . . . : 5
Time To Live . . . . . : 294
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : youtube-ui.l.google.com

dijasporanis.com
Record Name . . . . . : dijasporanis.com
Record Type . . . . . : 1
Time To Live . . . . . : 294
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 194.9.95.45

www.google-analytics.com
Record Name . . . . . : www.google-analytics.com
Record Type . . . . . : 5
Time To Live . . . . . : 68
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : www-google-analytics.l.google.com

103.110.101.79.in-addr.arpa
Record Name . . . . . : 103.110.101.79.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : pretrazivac

vtsnis.edu.rs
Record Name . . . . . : vtsnis.edu.rs
Record Type . . . . . : 1
Time To Live . . . . . : 294
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 194.9.94.7
```

HOSTS FAJL

Computer > Local Disk (C:) > Windows > System32 > drivers > etc

Name	Date modified	Type
hosts	11.4.2012 1:05	File
lmhosts.sam	10.6.2009 23:00	SAM File
networks	10.6.2009 23:00	File

hosts - Notepad

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
# name. The IP address and the host name should be separated by at least
# one space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
79.101.110.103          pretrazivac
127.0.0.1               localhost
```

pretrazivac/

pretrazivac - Google

pretrazivac/ - Bing Search

pretrazivac

pretrazivaci interneta

pretrazivaci

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

```
ipconfig /displaydns
```

Shows IP Configuration

```
1.0.0.127.in-addr.arpa
-----
Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : localhost

103.110.101.79.in-addr.arpa
-----
Record Name . . . . . : 103.110.101.79.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : pretrazivac

pretrazivac
-----
Record Name . . . . . : pretrazivac
Record Type . . . . . : 1
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 79.101.110.103

pretrazivac
-----
No records of type AAAA
```



Google Search

I'm Feeling Lucky

Google.rs offered in: cpmku

PRIMER DNS UPITA ZA WWW.BLIC.RS

Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3210	0	192.168.1.3	224.0.0.252	LLMNR	64	Standard query A wpad
3439	0	192.168.1.3	8.8.8.8	DNS	71	Standard query A www.blic.rs

Frame 3439: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)

Ethernet II, Src: HonHaiPr_17:23:65 (38:59:f9:17:23:65), Dst: AskeyCom_82:35:aa (00:24:d2:82:35:aa)

Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 8.8.8.8 (8.8.8.8)

User Datagram Protocol, Src Port: 59390 (59390), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0xbd49

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- www.blic.rs: type A, class IN
 - Name: www.blic.rs
 - Type: A (Host address)
 - Class: IN (0x0001)

PRIMER DNS ODGOVORA ZA WWW.BLIC.RS UPIT

No.	Time	Source	Destination	Protocol	Length	Info
3445	0	8.8.8.8	192.168.1.3	DNS	113	Standard query response CNAME www.blic.ha.rs A 91.222.6.35
3447	0	192.168.1.3	8.8.8.8	DNS	76	Standard query A www.facebook.com

Domain Name System (response)

[Request In: 3439]

[Time: 0.053249000 seconds]

Transaction ID: 0xbd49

Flags: 0x8180 (Standard query response, No error)

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

www.blic.rs: type A, class IN

Name: www.blic.rs

Type: A (Host address)

Class: IN (0x0001)

Answers

www.blic.rs: type CNAME class IN, cname www.blic.ha.rs

Name: www.blic.rs

Type: CNAME (Canonical name for an alias)

Class: IN (0x0001)

Time to live: 3 hours, 24 minutes, 57 seconds

Data length: 14

Primaryname: www.blic.ha.rs

www.blic.ha.rs: type A, class IN, addr 91.222.6.35

Name: www.blic.ha.rs

Type: A (Host address)

Class: IN (0x0001)

Time to live: 1 minute, 52 seconds

CNAME dns zapis za alias
www.blic.rs , i vreme koliko host
da čuva ovaj zapis TTL

Host A zapis za kanonično(puno) ime,
na kome se nalazi web server

DETALJNIJA PRETRAGA DNS ZAPISA

NSLOOKUP ALAT

```
Administrator: C:\Windows\system32\cmd.exe - nslookup

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Korisnik>nslookup www.vtsnis.edu.rs
Server: Unknown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.vtsnis.edu.rs
Address: 194.9.94.7

C:\Users\Korisnik>nslookup
Default Server: Unknown
Address: 192.168.1.1

> _
```

Ne interaktivni mod

Interaktivni mod

Obezbeđuje nam više mogućnosti u ispitivanju DNS servera

PRIMER MX DNS UPITA ZA VTSNIS.EDU.RS DOMEN

Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
41603	0	8.8.8.8	192.168.1.3	DNS	380	Standard query response CNAME safebrowsing.cache.l.google.com A 79.101.110.148 A 79.101.110.148
41806	0	192.168.1.3	8.8.8.8	DNS	73	Standard query MX vtsnis.edu.rs
41821	0	8.8.8.8	192.168.1.3	DNS	116	Standard query response MX 10 mail.vtsnis.edu.rs MX 20 mail2.vtsnis.edu.rs
43376	0	192.168.1.3	8.8.8.8	DNS	93	Standard query A liveupdate.symantecliveupdate.com

Frame 41806: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)

Ethernet II, Src: HonHaiPr_17:23:65 (38:59:f9:17:23:65), Dst: AskeyCom_82:35:aa (00:24:d2:82:35:aa)

Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 8.8.8.8 (8.8.8.8)

User Datagram Protocol, Src Port: 56721 (56721), Dst Port: domain (53)

Domain Name System (query)

Response In: 41821

Transaction ID: 0x0002

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

vtsnis.edu.rs: type MX, class IN

Name: vtsnis.edu.rs

Type: MX (Mail exchange)

Class: IN (0x0001)

Tražimo da nam dns server pošalje MX zapis (naziv mail servera) za domen vtsnis.edu.rs

PRIMER MX DNS ODGOVORA ZA VTSNIS.EDU.RS DOMEN

Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
41806	0	192.168.1.3	8.8.8.8	DNS	73	Standard query MX vtsnis.edu.rs
41821	0	8.8.8.8	192.168.1.3	DNS	116	Standard query response MX 10 mail.vtsnis.edu.rs MX 20 mail2.vtsnis.edu.rs

Ethernet II, Src: AskeyCom_82:35:aa (00:24:d2:82:35:aa), Dst: HonHaiPr_17:23:65 (38:59:f9:17:23:65)

Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.1.3 (192.168.1.3)

User Datagram Protocol, Src Port: domain (53), Dst Port: 56721 (56721)

Domain Name System (response)

[Request In: 41806]

[Time: 0.157586000 seconds]

Transaction ID: 0x0002

Flags: 0x8180 (Standard query response, No error)

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

vtsnis.edu.rs: type MX, class IN

Name: vtsnis.edu.rs

Type: MX (Mail exchange)

Class: IN (0x0001)

Answers

vtsnis.edu.rs: type MX, class IN, preference 10, mx mail.vtsnis.edu.rs

Name: vtsnis.edu.rs

Type: MX (Mail exchange)

Class: IN (0x0001)

Time to live: 4 minutes, 59 seconds

Data length: 9

Preference: 10

Mail exchange: mail.vtsnis.edu.rs

vtsnis.edu.rs: type MX, class IN, preference 20, mx mail2.vtsnis.edu.rs

```
C:\Users\Korisnik>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> set type=mx
> vtsnis.edu.rs
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

Non-authoritative answer:

vtsnis.edu.rs MX preference = 10, mail exchanger = mail.vtsnis.edu.rs
vtsnis.edu.rs MX preference = 20, mail exchanger = mail2.vtsnis.edu.rs

Prikaz imena odgovornih mail
servera za domen vtsnis.edu.rs

PRIMER HOST DNS ODGOVORA ZA VTSNIS.EDU.RS

Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
202621	0	fe80::51a8:395a:a2dff02::1:3		LLMNR	84	Standard query A wpad
202623	0	192.168.1.3	224.0.0.252	LLMNR	64	Standard query A wpad
203621	0	192.168.1.3	8.8.8.8	DNS	77	Standard query MX www.vtsnis.edu.rs
203622	0	8.8.8.8	192.168.1.3	DNS	135	Standard query response
207853	0	192.168.1.3	8.8.8.8	DNS	78	Standard query A mail.vtsnis.edu.rs
207854	0	8.8.8.8	192.168.1.3	DNS	94	Standard query response A 194.9.94.72

User Datagram Protocol, Src Port: domain (53), Dst Port: 53291 (53291)

Domain Name System (response)

Request In: 207853

[Time: 0.167608000 seconds]
Transaction ID: 0x0005

Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries

- mail.vtsnis.edu.rs: type A, class IN
Name: mail.vtsnis.edu.rs
Type: A (Host address)
Class: IN (0x0001)

Answers

- mail.vtsnis.edu.rs: type A, class IN, addr 194.9.94.72
Name: mail.vtsnis.edu.rs
Type: A (Host address)
Class: IN (0x0001)
Time to live: 4 minutes, 59 seconds
Data length: 4
Addr: 194.9.94.72 (194.9.94.72)

```
> set type=A
> mail.vtsnis.edu.rs
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: mail.vtsnis.edu.rs
Address: 194.9.94.72
>
```

DNS odgovor u vidu
prosleđivanja IP adrese za mail
server, mail.vtsnis.edu.rs

PRIMER NS DNS ODGOVORA ZA VTSNIS.EDU.RS DOMEN

Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
280584	0	192.168.1.3	8.8.8.8	DNS	72	Standard query A um.simpli.fi
280592	0	8.8.8.8	192.168.1.3	DNS	139	Standard query response CNAME west.um.simpli.fi A 50.97.23
280708	0	192.168.1.3	8.8.8.8	DNS	77	Standard query A bh.contextweb.com
280728	0	8.8.8.8	192.168.1.3	DNS	148	Standard query response CNAME contextweb.map.fastly.net A
282888	0	192.168.1.3	8.8.8.8	DNS	73	Standard query NS vtsnis.edu.rs
282912	0	8.8.8.8	192.168.1.3	DNS	118	Standard query response NS ns2.loopia.se NS ns1.loopia.se

Domain Name System (response)

[Request In: 282888]

[Time: 0.169545000 seconds]

Transaction ID: 0x0007

Flags: 0x8180 (Standard query response, No error)

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

- vtsnis.edu.rs: type NS, class IN
 - Name: vtsnis.edu.rs
 - Type: NS (Authoritative name server)
 - Class: IN (0x0001)

Answers

- vtsnis.edu.rs: type NS, class IN, ns ns2.loopia.se
 - Name: vtsnis.edu.rs
 - Type: NS (Authoritative name server)
 - Class: IN (0x0001)
 - Time to live: 59 minutes, 59 seconds
 - Data length: 15
 - Name Server: ns2.loopia.se
- vtsnis.edu.rs: type NS, class IN, ns ns1.loopia.se

```
>
> set type=NS
> vtsnis.edu.rs
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
vtsnis.edu.rs    nameserver = ns2.loopia.se
vtsnis.edu.rs    nameserver = ns1.loopia.se
>
```

DNS odgovor u vidu autorativnih DNS (NS) servera za vtsnis.edu.rs domen

NSLOOKUP KOMANDE

```
C:\Users\Korisnik>nslookup www.vtsnis.edu.rs
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name: www.vtsnis.edu.rs
Address: 194.9.94.7
```

DNS server kome je prosleđen upit nije autoritativan za zonu vtsnis.edu.rs

```
C:\Users\Korisnik>nslookup www.vtsnis.edu.rs ns1.loopia.se
Server: ns1.loopia.se
Address: 93.188.0.20
Name: www.vtsnis.edu.rs
Address: 194.9.94.7
C:\Users\Korisnik>_
```

DNS server (ns1.loopia.se) kome je prosleđen upit je autoritativan za zonu vtsnis.edu.rs

```
C:\Users\Korisnik>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> server ns1.loopia.se
Default Server: ns1.loopia.se
Address: 93.188.0.20
>
```

Konekcija na DNS server sa nazivom ns1.loopia.se

PRIKAZ SVIH DNS ZAPISA ZA DOMEN VTSNIS.EDU.RS

```
>
> set type=any
> vtsnis.edu.rs
Server:  ns1.loopia.se
Address:  93.188.0.20

vtsnis.edu.rs  nameserver = ns1.loopia.se
vtsnis.edu.rs
primary name server = ns1.loopia.se
responsible mail addr = registry.loopia.se
serial  = 1408579200
refresh = 10800 (3 hours)
retry   = 3600 (1 hour)
expire  = 604800 (7 days)
default TTL = 86400 (1 day)

vtsnis.edu.rs  nameserver = ns2.loopia.se
vtsnis.edu.rs  internet address = 194.9.94.7
vtsnis.edu.rs  MX preference = 20, mail exchanger = mail2.vtsnis.edu.rs
vtsnis.edu.rs  MX preference = 10, mail exchanger = mail.vtsnis.edu.rs
ns1.loopia.se  internet address = 93.188.0.20
mail.vtsnis.edu.rs  internet address = 194.9.94.72
ns2.loopia.se  internet address = 93.188.0.21
mail2.vtsnis.edu.rs  internet address = 194.9.94.3
```