Administracija računarskih mreža

DNS – Domain Name System

Literatura

- "Computer Networking" Kurose, Ross
  - poglavlje DNS
- "Principles of Network and System Administration"
  - poglavlje „Setting up the DNS nameservice"

Usluge aplikativnog nivoa

- Suština postojanja računarskih mreža
- Pristup uslugama
  - IP adresa + TCP/UDP port
- TCP / UDP port “adresa” usluge na računaru

Usluge aplikativnog nivoa

- DNS
- E-pošta
  - SMTP
  - POP i IMAP
- WWW
- Te mnoge druge

DNS: *Domain Name System*

Ljudi: razni identifikatori:

- JMBG, ime, br. pasoš

Internet računari i ruteri:

- IP adresa (32 bit) – koristi se za adresiranje datagrama
- "ime", npr., www.facebook.com – koriste ljudi

P: mapiranje između IP adresa i imena?

Domain Name System:

- *distribuirana baza podataka* izvedena kroz hijerahiju mnogo *name servera* (imena)
- *protokol aplikativnog nivoa* za komunikaciju računari, ruteri, serveri imena rade *resolve* imena (prevod adresa/ime)
  - napomena: *core* (unutrašnja) Internet funkcija, izvedena kao protokol aplikativnog nivoa
  - kompleksnost na mrežnoj "ivici"

DNS

DNS usluge

- prevod imena računara (*hostname*) u IP adresu
- *host aliasing*
  - kanonička, *alias* imena
- *mail server aliasing*
- distribucija opterećenja
  - replicirani Web serveri: skup IP adresa za jedno kanoničko ime

Zašto ne centralizirani DNS?

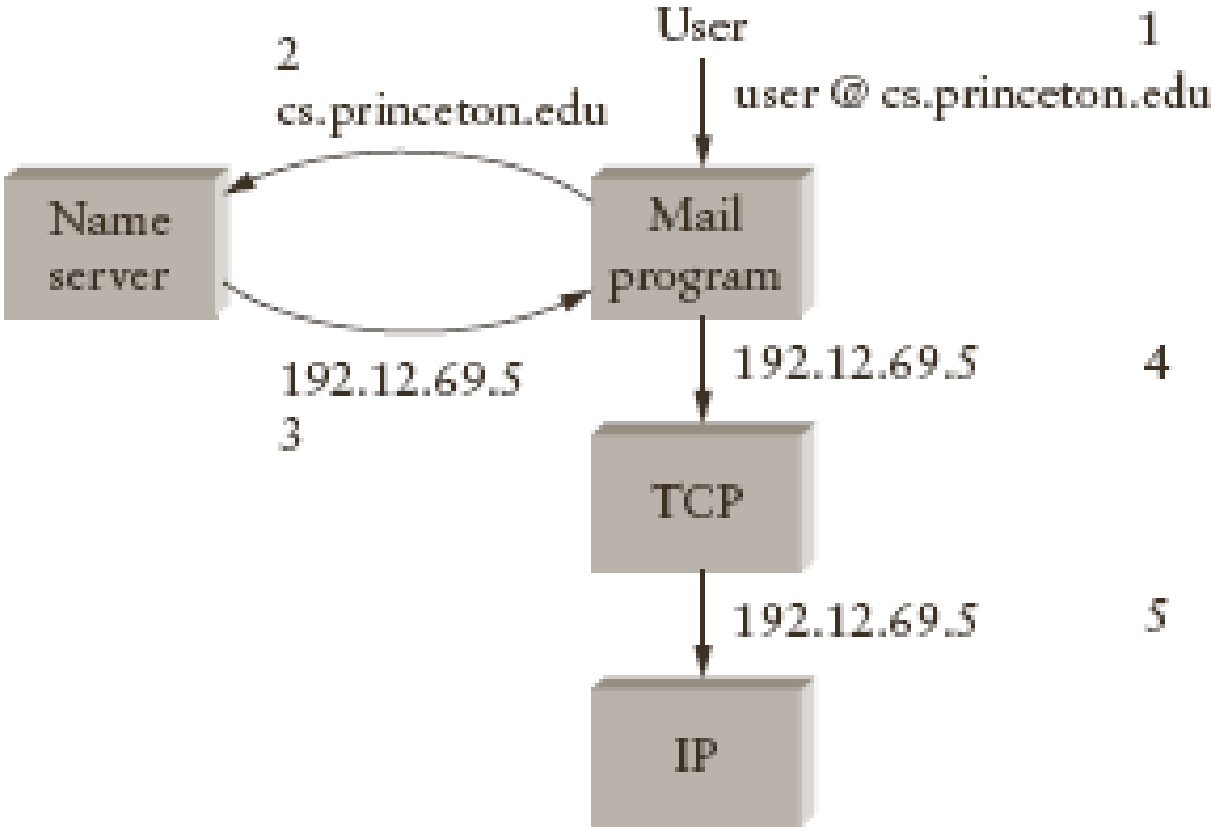
- jedinstveno mjesto otkaza
- količina saobraćaja
- udaljena centralizirana baza podataka
- održavanje

ne *skalira !* (dobro)

DNS – Domain Name System

- Usluga koja omogućava mapiranje između domenskih imena čvorova u mreži i njihovih IP adresa
- RFC 1034 i 1035
- Nije prava (korisnička) aplikacija
  - Ne koriste ga ljudi (direktno)
  - Koriste ga aplikacije (koje koriste ljudi)
- Distribuirana baza podataka
- Prije DNS hosts.txt (održavan od strane NIC)

Pozicija DNS u komunikaciji



DNS elementi

- Prostor domenskih imena
- Baza DNS podataka
- Poslužitelji imena (*Name Servers*)
- Programi za upite – DNS klijenti (*Resolvers*)

Prostor domenskih imena

- Skup mogućih domenskih imena
- Domen – grupa računara pod kontrolom jedne organizacije
- Organizacija domena je hijerarhijska
- Domen može imati poddomene
- Cjelokupni Internet je podijeljen manji broj osnovnih (*top level*) domena
- Svi ostali domeni su poddomeni osnovnih

DNS osnovni domeni (stari)

- GTLD (*Generic Top Level Domains*) – stari 1985
  - .com
  - .edu
  - .gov
  - .mil
  - .net
  - .org
  - .arpa
- ccTLD - dvoslovni kod države ISO 3166
  - .ba (naš, a ima ih oko 300)

Podjela osnovnih domena (2015)

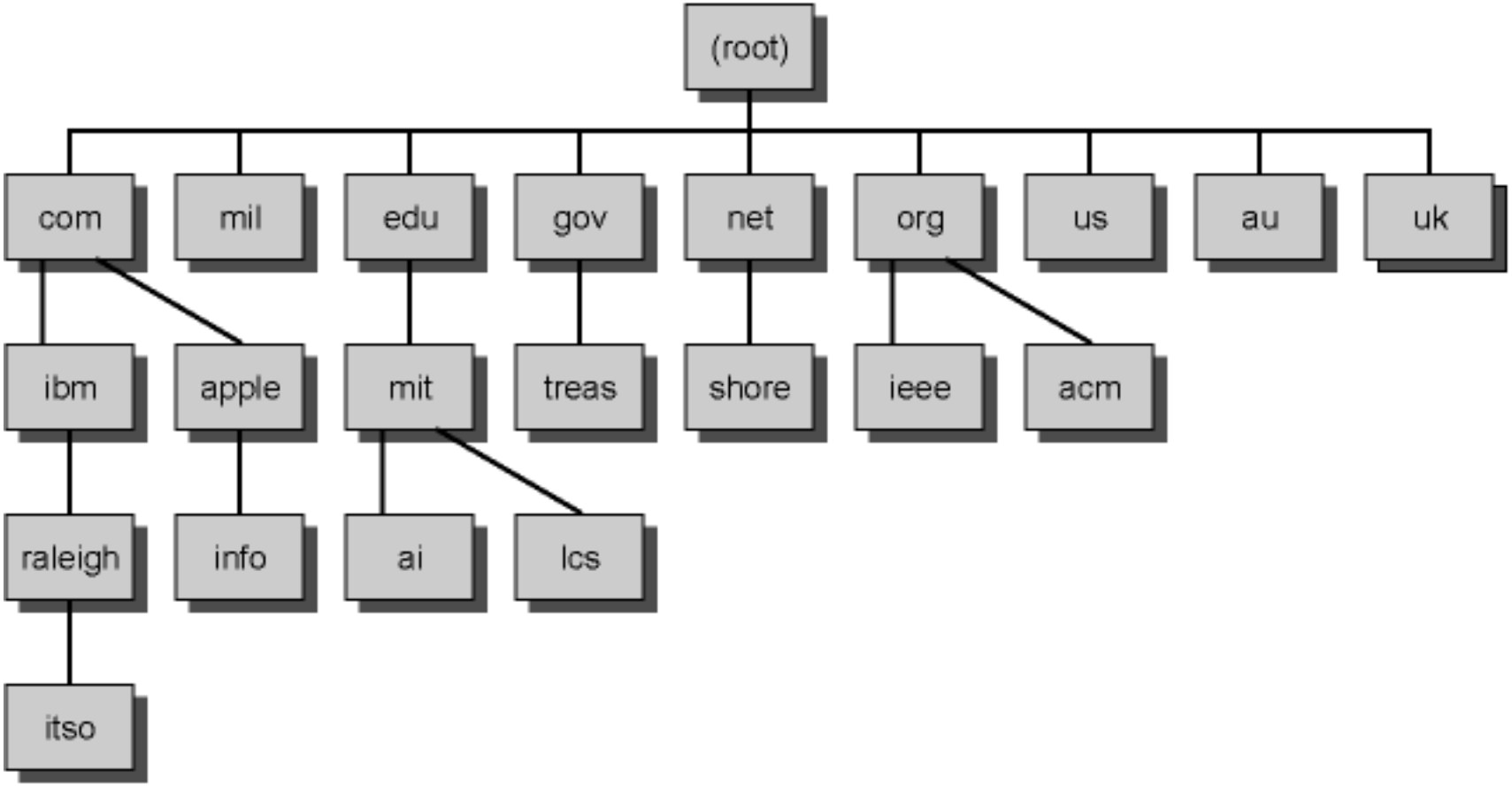
- Generički (gTLD)
- Državni (ccTLD)
- Infrastrukturni (ARPA)
- Testni (tTLD)
- Ograničeni (grTLD)
- Sponzorisani (sTLD)

- Internet Corporation for Assigned Names and Numbers (ICANN)
  - Internet Assigned Numbers Authority (IANA)

DNS poddomeni

- etf.unsa.ba (naša zona i naš *Name Server*)
- ba
  - unsa
    - etf
- Vlasnik domena kreira (iznajmljuje) poddomene
  - .ba domen - UTIC
- Do 127 nivoa
- Cijelo ime domena maksimalno 255 znakova
- Pojedina polja do 63 znaka

Dio Internet DNS stabla



Baza DNS podataka

- Zapisi o resursima (*Resource Records* – RR)
- Upit ka DNS serveru sa imenom vraća zapise (RR) vezane uz to ime
- RR format
  - Domain_name – ime po kom se pretražuje
  - TTL – u sekundama – vremenska promjenljivost
  - Class – IN (za Internet), može i drugo
  - Type – SOA, A, MX, NS, CNAME, PTR, HINFO, TXT
  - Value – vrijednost, zavisno od tipa zapisa

Tipovi i vrijednosti DNS zapisa

Tip	Značenje	Vrijednost
SOA	Start of Authority	Parametri za ovu zonu
A	IP adresa za ime	32 bitni cjeli broj
MX	Mail exchange	Prioritet, ime računara
NS	Name Server	Ime servera za domen
CNAME	Canonical name	Ime domena
PTR	Pointer	Alias za IP adresu
HINFO	Opis računara	CPU i OS
TXT	Tekst	Slobodni tekst

Ima još i MINFO, SRV, WKS

DNS zapisi

DNS: distribuirana db pohranjuje *resource records* (RR)

RR format: **(*name, value, type*, ttl)**

- Type=A
  - **name** je hostname
  - **value** je IP adresa
- Type=NS
  - **name** is domen (npr. foo.com)
  - **value** je *hostname* autoritativnog servera imena za ovaj domen
- Type=CNAME
  - **name** je nadimak (*alias*) za neko “canonical” (pravo) ime
    www.ibm.com je zapravo servereast.backup2.ibm.com
  - **value** je kanonsko ime
- Type=MX
  - **value** je ime *mail* servera vezano (asocirano) za ime

etf.unsa.ba zapisi

```
; /var/named/master/etf.unsa.ba
;
; Zone file for etf.unsa.ba
; type:   MASTER
; by:     Ime Administratora <ime.administratora@etf.unsa.ba>
```

Start of Authority – osnovni podaci i parametri

```
@     IN          SOA      ns.etf.unsa.ba. hostmaster.etf.unsa.ba. (
                           2007101410       ; serial, todays date + todays ser
                           10800            ; refresh, seconds, 3H
                           3600             ; retry, seconds, 1H
                           360000           ; expire, seconds, 100H
                           86400 )          ; minimum, 1D
```

etf.unsa.ba zapisi (2)

Name server

```
NS      ns
```

Mail Exchanger

```
MX      10      igman.etf.unsa.ba.
```

Tekstualne informacije o domenu

```
TXT     "Faculty of Electrical Engineering Sarajevo"
```

etf.unsa.ba zapisi (3)

Zapisi tipa A (IP adrese za imena)

```
localhost    A     127.0.0.1
ns           A     80.65.65.66 ; reserved
...
dev          A     80.65.65.71 ; reserved
win          A     80.65.65.72 ; reserved
majevica     A     80.65.65.73 ; reserved
...
igman        A     80.65.65.78 ; reserved
```

etf.unsa.ba zapisi (4)

Zapisi tipa CNAME (zamjenska imena)

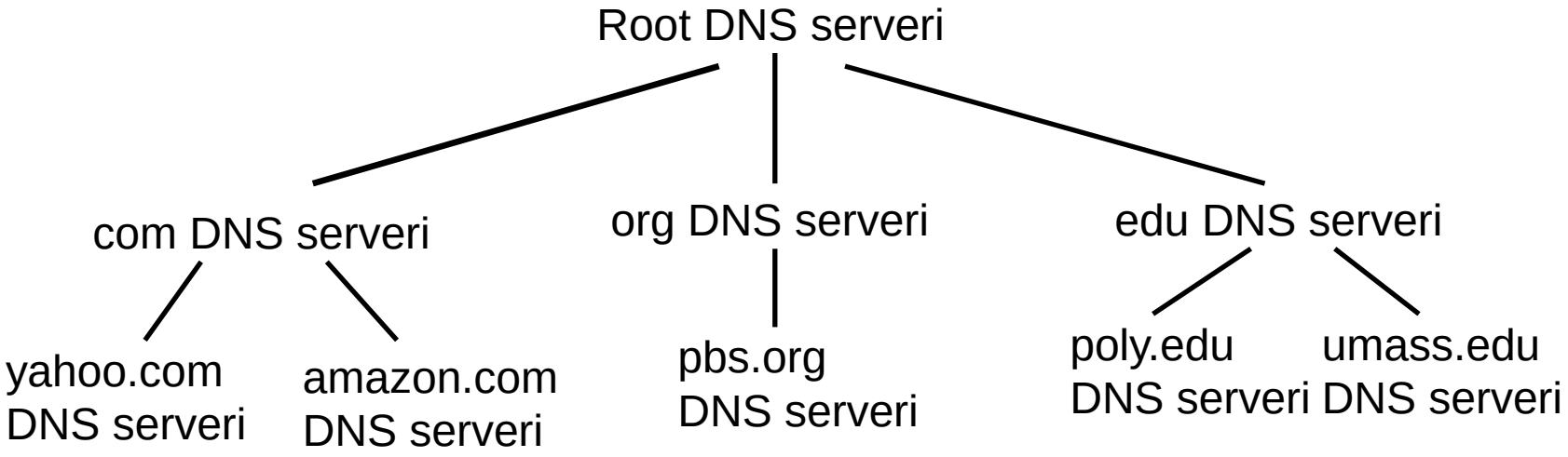
```
ns1          CNAME ns
hostmaster   CNAME ns
...
winsrv       CNAME win
...
webmail      CNAME igman
c2           CNAME majevica
...
```

etf.unsa.ba zapisi (5)

Još zapisa tipa A (IP adrese za imena) – web serveri

```
nastava     A     80.65.65.71   ; nastava
icat        A     80.65.65.71   ; ICAT Site
...
courses     A     80.65.65.72   ; Coursware
people      A     80.65.65.71   ; People from ETF
...
portal      A     80.65.65.71   ; ETF web portal
www         A     80.65.65.71   ; CNAME portal  ;
...
zamger      A     80.65.65.73  ;
...
```

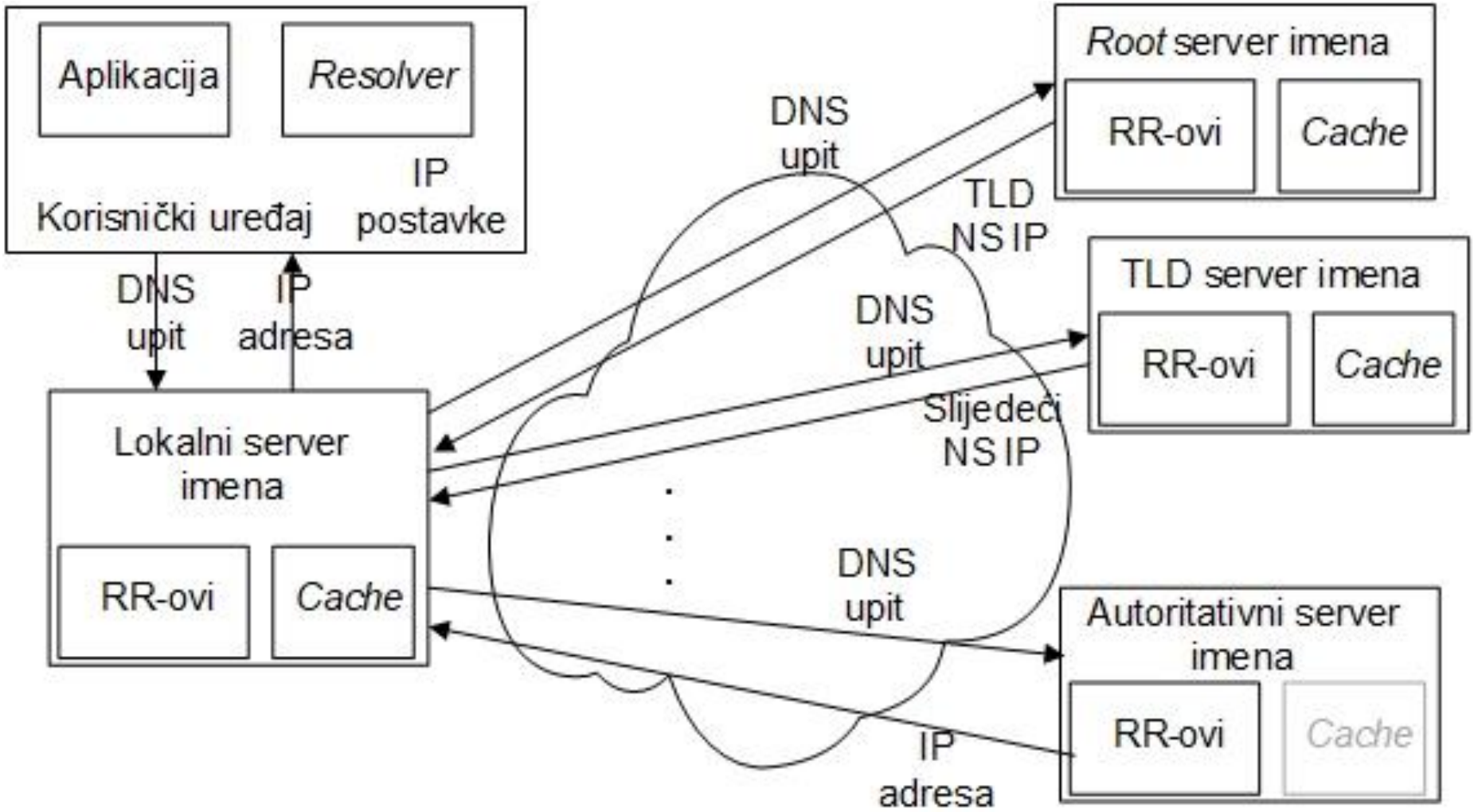
Distribuirana hijerarhijska baza podataka



Klijent želi IP za www.amazon.com; osnovna procedura:

- klijent pita *root* server za com DNS server
- klijent pita com DNS server za amazon.com DNS server
- klijent pita amazon.com DNS server za IP adresu www.amazon.com

Kako radi DNS



Kako radi DNS

- Korisnički program traži IP adresu za ime nekog domena
- *Resolver* (u lokalnom računaru) pravi upit za definisani *name server* (najčešće lokalni koji je u istom domenu)
- (Lokalni) *name server* provjerava lokalnu bazu
  - Ako pronađe, vraća IP adresu onom ko je tražio
  - Ako ne, pita druge dostupne *name server*-e
    - Počinje od korijena DNS stabla ili koliko visoko na stablu je moguće
- Korisnički program dobiva traženu IP adresu ili poruku o grešci

TLD i autoritativni serveri

- *Top-level domain* (TLD) serveri:
  - odgovorni za com, org, net, edu, itd i sve domene zemalja: ba, uk, fr, ca, jp...
    - Network Solutions održava servere za com TLD
    - Educause za edu TLD
- Autoritativni DNS serveri:
  - DNS serveri organizacije, daju autoritativna mapiranja imena u IP za servere organizacije (npr., Web, mail).
  - može ih održavati organizacija ili davalac usluge povezivanja na Internet (ISP)

Lokalni serveri imena

- formalno ne pripadaju hijererhiji
- svaki ISP (ISP za građanstvo, kompanija, univerzitet) ga ima
  - naziva se i "*default name server*"
- kada računar pravi DNS upit, upit šalje svom lokalnom DNS serveru
  - ponaša se kao posrednik (*proxy*), prosljeđuje upit u hijerarhiju

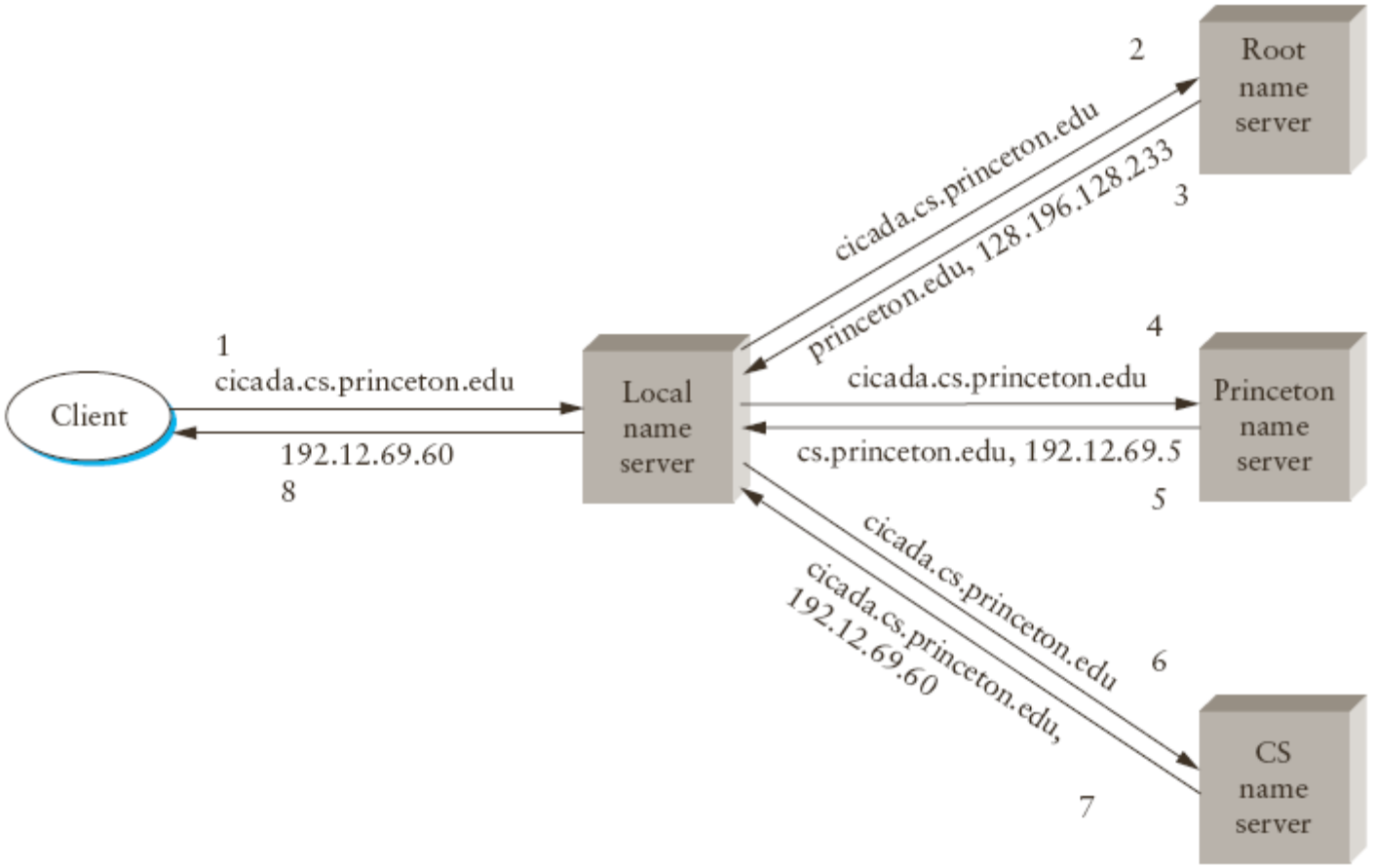
DNS predmemorisanje (*cache*)

- Radi uštede vremena i mrežnih resursa dobiveni odgovori na DNS upite se pamte na određeno vrijeme (*cache*) na više mjesta u lancu upita
  - Aplikacije (Web preglednici)
  - OS
  - (Svi) *Name server*-i
- Odgovor se pamti onoliko dugo koliko kaže TTL u odgovoru

DNS odgovori na upite

- Kada *name server* dobije upit na koji nema odgovor u lokalnoj bazi ili *cache*
  - Pita drugi *name* server i vraća dobiveni odgovor – rekurzivno ponašanje
  - Vraća adresu slijedećeg *name* servera kome treba biti upućem upit – iterativno ponašanje
    - Ako je pitanje postavio DNS klijenti (*Resolver*) – rekurzivno ponašanje
    - DNS serveri međusobno koriste i jedno i drugo – zavisno od upita i mogućnosti

DNS iterativno ponašanje



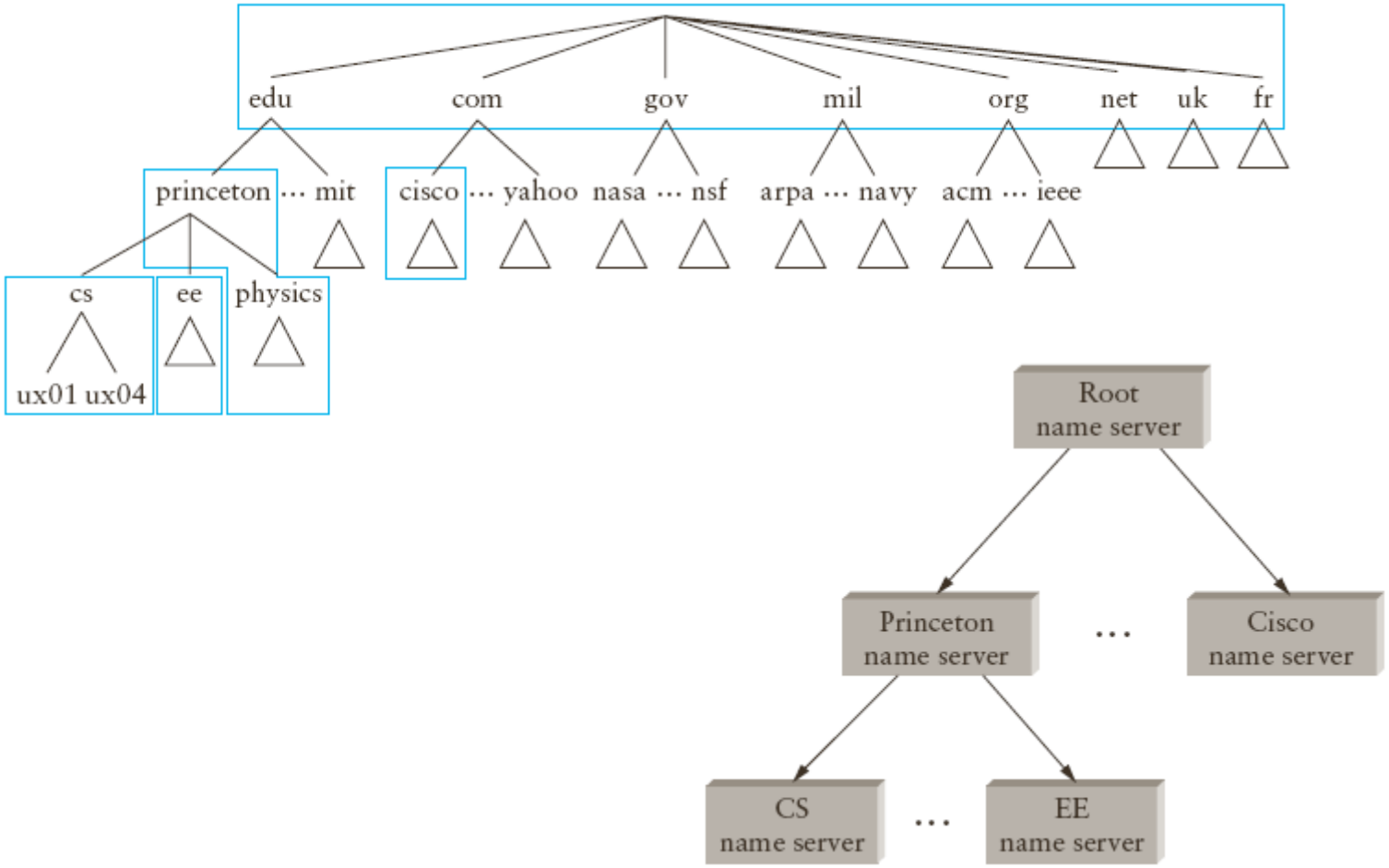
Format DNS poruke

Identifikator (16 bita)	QR 1b	*Opcode* (4 bita)	AA 1b	TC 1b	RD 1b	RA 1b	Z 1b	AD 1b	CD 1b	Kod odgov. (4 bita)
Broj pitanja (16 bita)	Broj odgovora (16 bita)									
Broj servera imena (16 bita)	Broj dodatnih zapisa (16 bita)									
Domensko ime koje se traži (varijabilne dužine)										
Tip upita (16 bita)	Klasa upita (16 bita)									
Domensko ime na koje se odgovor odnosi (varijabilne dužine)										
Tip RR zapisa (16 bita)	Klasa RR zapisa (16 bita)									
TTL (period pamćenja odgovora) (32 bita)										
Dužina RR zapisa (16 bita)	Sadržaj RR zapisa (varijabilne dužine)									

DNS hijerarhija

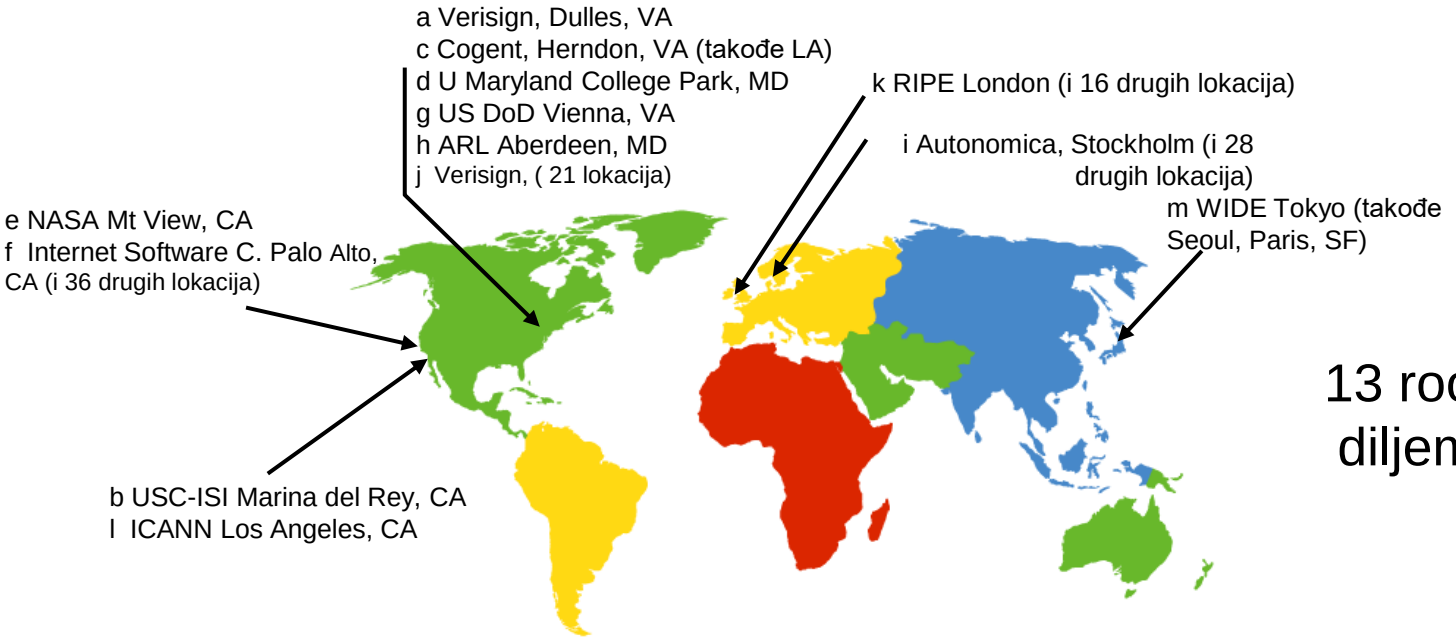
- Podjela DNS stabla na nepreklapajuće zone
- Zona – dio DNS stabla sa NS za tu zonu
- Skup zapisa (RR) za zonu – autoritativan
- Zona – proizvoljan broj hijerarhijskih nivoa
- Neke (ili sve) grane iz zone – posebne zone

Zone – Poslužitelji imena



DNS: Root serveri imena

- kontaktiraju ih lokalni server imena kad ne mogu “razrješiti” (*resolve*) ime
- root server imena (u principu, ali ne i u praksi):
  - kontaktira autoritativni server imena ako ne zna mapiranje IP adrese za ime
  - dobiva mapiranje
  - vraća mapiranje lokalnom serveru imena



13 root servera diljem svijeta

Root name servers

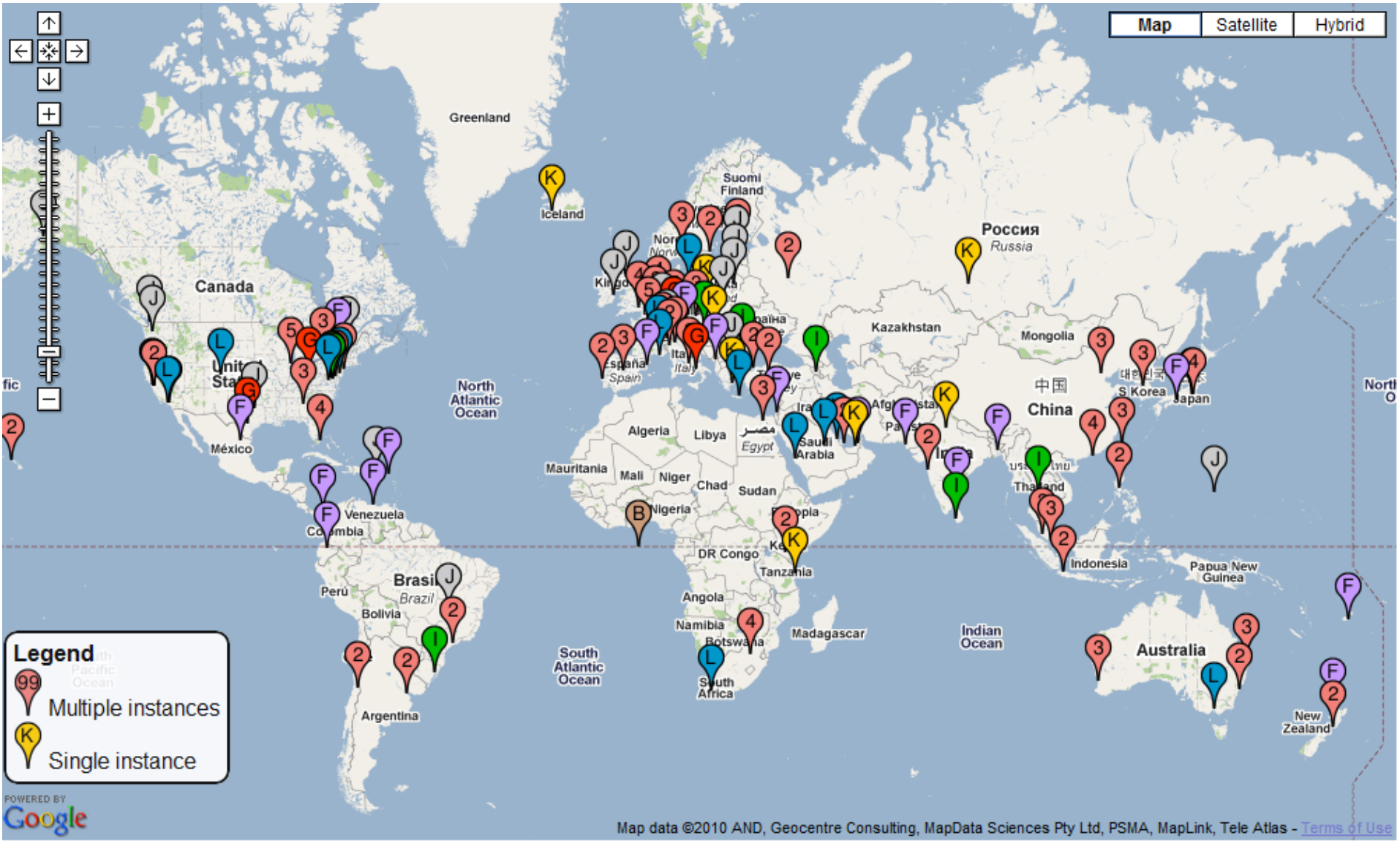
- 13 po cijelom svijetu (a-m.root-servers.net)
- Replicirani zapisi o NS svih osnovnih domena
- Prilično zauzeti
  - Internet Software Consortium server (F) skoro 300 miliona DNS upita dnevno
- Njihove adrese u konfiguracijskim datotekama DNS servera
- http://www.internic.net/zones/named.root

Root name serveri (1)

Server	Operator	Locations	IP Addresses
A	VeriSign, Inc.	**Sites: 14**	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30
B	Information Sciences Institute (University of South California)	**Sites: 6**	IPv4: 192.228.79.201 IPv6: 2001:500:200::b
C	Cogent Communications	**Sites: 10**	IPv4: 192.33.4.12 IPv6: 2001:500:2::c
D	University of Maryland	**Sites: 22**	IPv4: 199.7.91.13 IPv6: 2001:500:2d::d
E	NASA Ames Research Center	**Sites: 117**	IPv4: 192.203.230.10 IPv6: 2001:500:a8::e
F	Internet Systems Consortium, Inc.	**Sites: 119**	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f
G	Defense Information Systems Agency	**Sites: 6**	IPv4: 192.112.36.4 IPv6: 2001:500:12::d0d

Root name serveri (2)

Server	Operator	Locations	IP Addresses
H	U.S. Army Research Lab	**Sites: 8**	IPv4: 198.97.190.53 IPv6: 2001:500:1::53
I	Netnod	**Sites: 63**	IPv4: 192.36.148.17 IPv6: 2001:7fe::53
J	VeriSign, Inc.	**Sites: 63**	IPv4: 192.58.128.30 IPv6: 2001:503:C27::2:30
K	RIPE NCC	**Sites: 70**	IPv4: 193.0.14.129 IPv6: 2001:7fd::1
L	ICANN	**Sites: 165**	IPv4: 199.7.83.42 IPv6: 2001:500:9f::42
M	WIDE Project	**Sites: 4**	IPv4: 202.12.27.33 IPv6: 2001:dc3::35


Map
Satellite
Hybrid
Greenland
Iceland
Suomi
Finland
Россия
Russia
Canada
Kazakhstan
Mongolia
China
S Korea
Japan
North
Atlantic
Ocean
México
Algeria
Libya
Egypt
Saudi
Arabia
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
DR Congo
Tanzania
Angola
Namibia
Botswana
South
Africa
Madagascar
Indian
Ocean
Venezuela
Perú
Brazil
Bolivia
Argentina
South
Atlantic
Ocean
Indonesia
Papua New
Guinea
Australia
New
Zealand
Legend
Multiple instances
Single instance
POWERED BY
Google
Map data ©2010 AND, Geocentre Consulting, MapData Sciences Pty Ltd, PSMA, MapLink, Tele Atlas - Terms of Use

Pretraga za www.etf.unsa.ba

- Krenimo od Root Name Sever m

```
> server 202.12.27.33
Default Server:  M.ROOT-SERVERS.NET
Address:  202.12.27.33

> www.etf.unsa.ba
Server:  M.ROOT-SERVERS.NET
Address:  202.12.27.33

Name:    www.etf.unsa.ba
Served by:
- SAVA.UTIC.NET.ba
          195.130.35.3
          ba
- MUNNARI.OZ.AU
          202.12.74.196
          ba
- NS-BA.RIPE.NET
          193.0.12.28
          ba
- AUTH03.NS.UU.NET
          198.6.1.83
          ba
- NS.ba
          195.130.35.5
          ba
```

Pretraga za www.etf.unsa.ba

- Pitamo prvi na koji nas je Root uputio

```
> server 195.130.35.3
DNS request timed out.
    timeout was 2 seconds.
Default Server:  [195.130.35.3]
Address:  195.130.35.3

> www.etf.unsa.ba
Server:  [195.130.35.3]
Address:  195.130.35.3

Name:    www.etf.unsa.ba
Served by:
- ns.etf.unsa.ba
          217.75.199.34
          etf.unsa.ba
- ns-01.etf.unsa.ba
          217.75.199.36
          etf.unsa.ba
- ns-02.etf.unsa.ba
          78.47.195.203
          etf.unsa.ba
```

Pretraga za www.etf.unsa.ba

- Pitamo konačno onaj koji tačno zna

```
> server 217.75.199.34
199.75.217.in-addr.arpa nameserver = dns-srv-02.lol.ba
199.75.217.in-addr.arpa nameserver = dns-srv-01.lol.ba
Default Server:  [217.75.199.34]
Address:  217.75.199.34

> www.etf.unsa.ba
Server:  [217.75.199.34]
Address:  217.75.199.34

Name:    www.etf.unsa.ba
Address:  78.47.195.203
```

Umetanje zapisa u DNS

- primjer: nova organizacija “ARM studenti”
- registruje ime armstudenti.ba kod *DNS registrara* (npr., UTIC)
  - daje imena i IP adrese autoritativnih servera imena (primarni i sekundarni)
  - registrar umeće dva RR u ba TLD server:

```
(armstudenti.ba, dns1.armstudenti.ba, NS)
(dns1.armstudenti.ba, 212.212.212.1, A)
```

- pravi, na autoritativnom serveru, Type A zapis za www.armstudenti.ba; i Type MX zapis za mreznautopia.ba
- Kako ljudi dolaze do IP adrese naše Web lokacije?

Sigurnost DNS

- DNSSEC
- DoT, DoH, ODoH

DNS server softveri

- BIND – Prva UNIX implementacija, najčešći, 5 (8) *root name* servera koristi BIND
- Microsoft DNS (2000, 2003, 2008, NT4, ...)
- NSD – 4 (7) *root name* servera
- Knot DNS – 3 *root name* servera (skupa sa NSD i/ili BIND)

BIND – Berkley Internet Name Domain

- Master server – DNS podaci iz datoteka na računaru
- Slave server(i) – DNS podaci sa master servera redovno se ažuriraju
- Rezervni DNS
- Raspoređivanje opterećenja

BIND – struktura datoteka

- Poseban direktoriji – `named` ili `dns`
- Podirektoriji `master` (i `slave`)
- Datoteka u `master` koja se zove kao domen `etf.unsa.ba`
- Datoteka (e) u `master` za obratni upit (IP u ime) `rev.IP3.IP2.IP1`
- Datoteka u `master` za *loopback* `rev.127.0.0`
- Datoteka `named.cache` sa root name serverima
- Datoteka `named.conf`

BIND – named.conf

- options – bind direktoriji i druge opcije
- zone

```
zone "zone_name" [class] {
    // zone statements
};
```

  - Root name serveri

```
zone "." in{
    type hint;
    file "named.cache";
};
```

BIND – named.conf (2)

- zone – nastavak
  - Local host

```
zone "localhost" in{
    type master;
    file "master.localhost";
};
```

  - Reverzibilno mapiranje 127.0.0.1

```
zone "0.0.127.in-addr.arpa" in{
  type master;
  file "localhost.rev";
};
```

BIND – named.conf (3)

- zone – nastavak
  - Localni domen

```
zone "etf.unsa.ba" in{
    type master;
    file "master/etf.unsa.ba";
};
```

  - Reverzibilno mapiranje lokalnog domena

```
zone "IP3.IP2.IP1.in-addr.arpa" in{
  type master;
  file "rev.IP3.IP2.IP1";
};
```

BIND - named.cache (root)

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Jan 29, 2004
;       related version of root zone:   2004012900
;
;
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
...
```

BIND - etf.unsa.ba

```
; /var/named/master/etf.unsa.ba
;
; Zone file for etf.unsa.ba
; type:   MASTER
; by:     Ernedin Zajko <ernedin.zajko@etf.unsa.ba>
```

Start of Authority – osnovni podaci i parametri

```
@     IN          SOA      ns.etf.unsa.ba. hostmaster.etf.unsa.ba. (
                           2007101410       ; serial, todays date + todays ser
                           10800            ; refresh, seconds, 3H
                           3600             ; retry, seconds, 1H
                           360000           ; expire, seconds, 100H
                           86400 )          ; minimum, 1D
```

BIND - etf.unsa.ba zapisi (2)

Name server

```
NS      ns
```

Mail Exchanger

```
MX      10      igman.etf.unsa.ba.
```

Tekstualne informacije o domenu

```
TXT     "Faculty of Electrical Engineering Sarajevo"
```

BIND - etf.unsa.ba zapisi (3)

Zapisi tipa A (IP adrese za imena)

```
localhost    A     127.0.0.1
ns           A     80.65.65.66 ; reserved
...
dev          A     80.65.65.71 ; reserved
win          A     80.65.65.72 ; reserved
majevica     A     80.65.65.73 ; reserved
...
igman        A     80.65.65.78 ; reserved
```

BIND - etf.unsa.ba zapisi (4)

Zapisi tipa CNAME (zamjenska imena)

```
ns1          CNAME ns
hostmaster   CNAME ns
...
winsrv       CNAME win
...
webmail      CNAME igman
c2           CNAME majevica
...
```

BIND - etf.unsa.ba zapisi (5)

Još zapisa tipa A (IP adrese za imena) – web serveri

```
nastava     A     80.65.65.71   ; nastava
icat        A     80.65.65.71   ; ICAT Site
...
courses     A     80.65.65.72   ; Coursware
people      A     80.65.65.71   ; People from ETF
...
portal      A     80.65.65.71   ; ETF web portal
www         A     80.65.65.71   ; CNAME portal  ;
...
zamger      A     80.65.65.73  ;
...
```

BIND – poddomeni delegiranje

- Upis u datoteku RR domena (etf.unsa.ba)

```
...
podomen              86400 IN  NS ns_poddom.etf.unsa.ba
ns_pd.etf.unsa.ba 86400 IN  A  80.65.65.?
...
```

- Informacija krovnoj organizaciji o promjeni radi reverzibilnih upita

BIND - rev.IP3.IP2.IP1

```
$ORIGIN 23.168.192.IN-ADDR.ARPA.
@  IN   SOA    ns1.example.com. hostmaster.example.com. (
               2003080800 ; serial number
               3h ; refresh
               15m ; update retry
               3w ; expiry
               3h ; minimum )
   IN   NS     ns1.example.com.
   IN   NS     ns2.example.com.
1  IN PTR www.example.com. ; qualified name
2  IN PTR joe.example.com.
...
17 IN PTR bill.example.com.
...
74 IN PTR fred.example.com.
...
```

Microsoft DNS server

- Na Windows Server OS
- DNS Server service