Preddiplomski studij

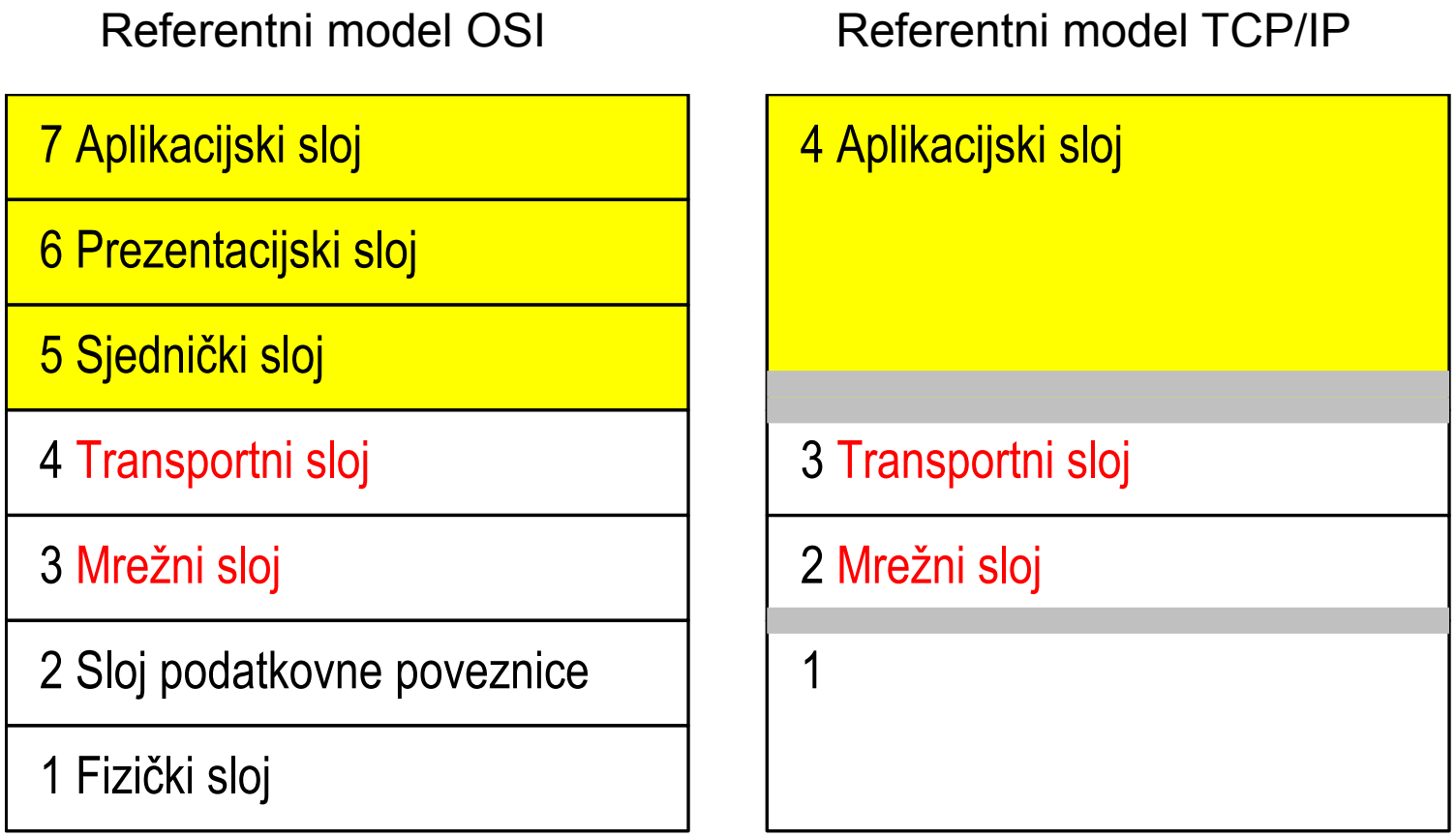
Računarstvo

Komunikacijske mreže

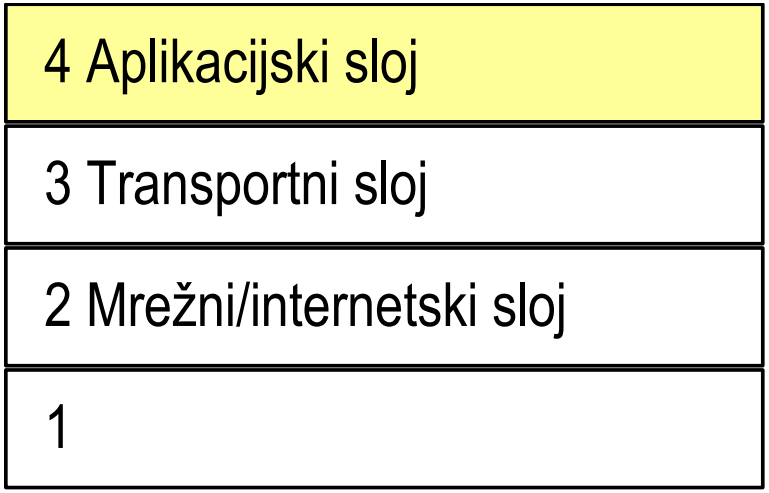
9. Aplikacijski sloj u Internetu.
   Sustav domenskih imena (DNS).

Ak.g. 2014./2015.

Podsjetimo se...



Internetski model: 4. aplikacijski sloj



- aplikacijski protokoli za različite usluge i primjene
- korisnički, npr.:
  - SMTP (*Simple Mail Transfer Protocol*): elektronička pošta
  - HTTP (*Hyper Text Transfer Protocol*): WWW
- sustavski, npr.:
  - DNS (*Domain Name System*): sustav imenovanja domena

Sadržaj predavanja

- **Osnove internetskih usluga**
  - usluge i aplikacijski protokoli
  - modeli izvedbe usluga
  - pronalaženje usluga
  - programska podrška
- **Sustav domenskih imena**
  - prostor domenskih imena
  - registracija imena
  - organizacija i izvedba sustava DNS

Osnove internetskih usluga

- aplikacijski protokol
  - vrste poruka
  - sintaksa poruka – propisani formati poruka
  - semantika poruka – značenje polja u poruci
  - pravila kako se poruke razmjenjuju
- model izvedbe usluge
  - najčešći model: klijent/poslužitelj
  - postoje i drugi modeli (o tome kasnije)
- program klijenta
- program poslužitelja

Usluge i aplikacijski protokoli u Internetu

- usluge:
  - prijenos datoteka
  - rad na daljinu
  - elektronička pošta
  - mrežne novosti
  - interaktivne usluge
  - imenička usluga
  - globalni informacijski sustav
  - ...
- aplikacijski protokoli:
  - FTP, ...
  - TELNET, ...
  - SMTP, POP, IMAP, ...
  - NNTP, ...
  - IRC, H.323, ...
  - LDAP, X.500, ...
  - HTTP, ...
  - ...

Modeli izvedbe usluge

- model klijent-poslužitelj (engl. *client-server*)
  - više izvedbi: model s jednim poslužiteljem i model s više poslužitelja
  - posebni slučajevi:
    - posrednički (proxy) poslužitelji
    - međuspremnički (caching) poslužitelji
- model s ravnopravnim procesima (engl. *peer-to-peer*)
  - svaki proces je i “klijent” i “poslužitelj”, uloge nisu odvojene
- postoje i druga rješenja:
  - pokretni kôd, pokretni agenti, i dr.

Uz pojmove klijenta i poslužitelja ...

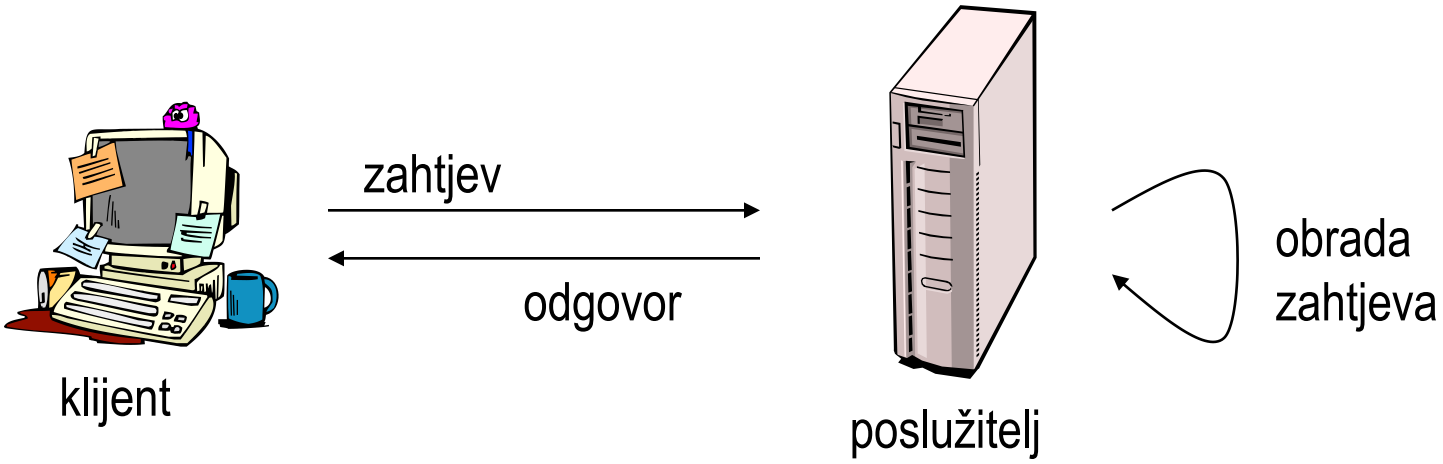
- ovisno o kontekstu, pojmovi klijent, odnosno poslužitelja, mogu se odnositi na:
  - klijentsko računalo ili klijentski proces
  - poslužiteljsko računalo ili poslužiteljski proces

- proces je instanca izvođenja (klijentskog ili poslužiteljskog) programa
- programi klijenta i poslužitelja mogu se izvoditi na istom računalu, ali glavna prednost je u mrežnom radu

- u daljnjim razmatranjima, uglavnom ćemo govoriti o klijentima i poslužiteljima u smislu procesa

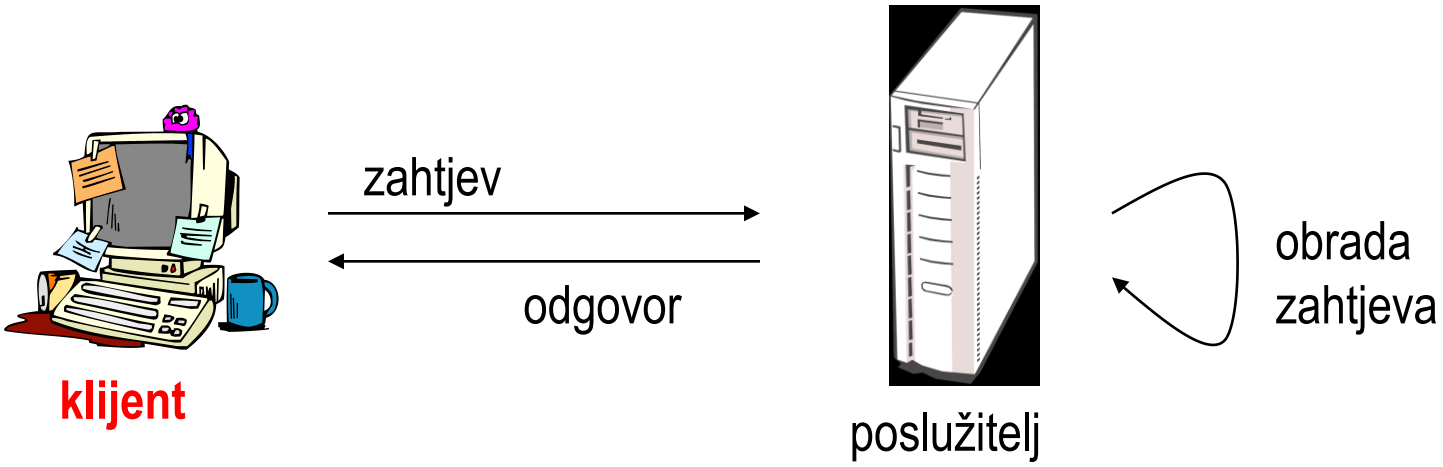
Model klijent-poslužitelj

- izvedba usluge u modelu klijent/poslužitelj podijeljena je između programa *klijenta* i programa *poslužitelja*
- koristi se u većini internetskih usluga
- komunikacija se temelji na nizu zahtjeva i odgovora:
  - klijent traži uslugu od poslužitelja (slanjem zahtjeva)
  - poslužitelj obrađuje zahtjev i odgovara klijentu šaljući rezultat obrade



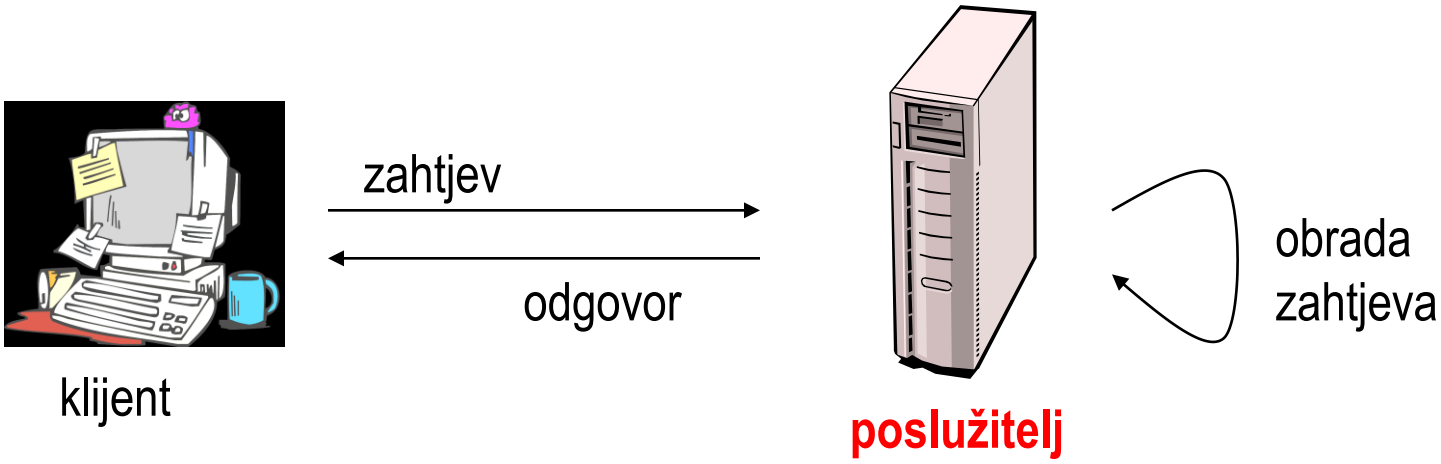
Program klijenta

- "program klijenta" je programska podrška koja omogućuje računalu da djeluje kao *klijent* u opisanom modelu
- proces izvođenja klijentskog programa najčešće pokreće korisnik
- osnovni zadaci:
  - pruža korisničko sučelje koje korisniku omogućuje slanje zahtjeva poslužitelju
  - odgovarajuće formatira zahtjev kako bi ga poslužitelj mogao "razumjeti"
  - odgovarajuće formatira poslužiteljev odgovor kako bi ga korisnik mogao razumjeti



Program poslužitelja

- program poslužitelja je programska podrška koja omogućuje računalu da djeluje kao *poslužitelj* u opisanom modelu
- proces izvođenja poslužiteljskog programa najčešće se pokreće automatski, prilikom pokretanja operacijskog sustava
- osnovni zadaci:
  - osluškuje i prihvaća zahtjeve klijen(a)ta
  - obrađuje zahtjeve i odgovara šaljući rezultat obrade klijentu(ima)

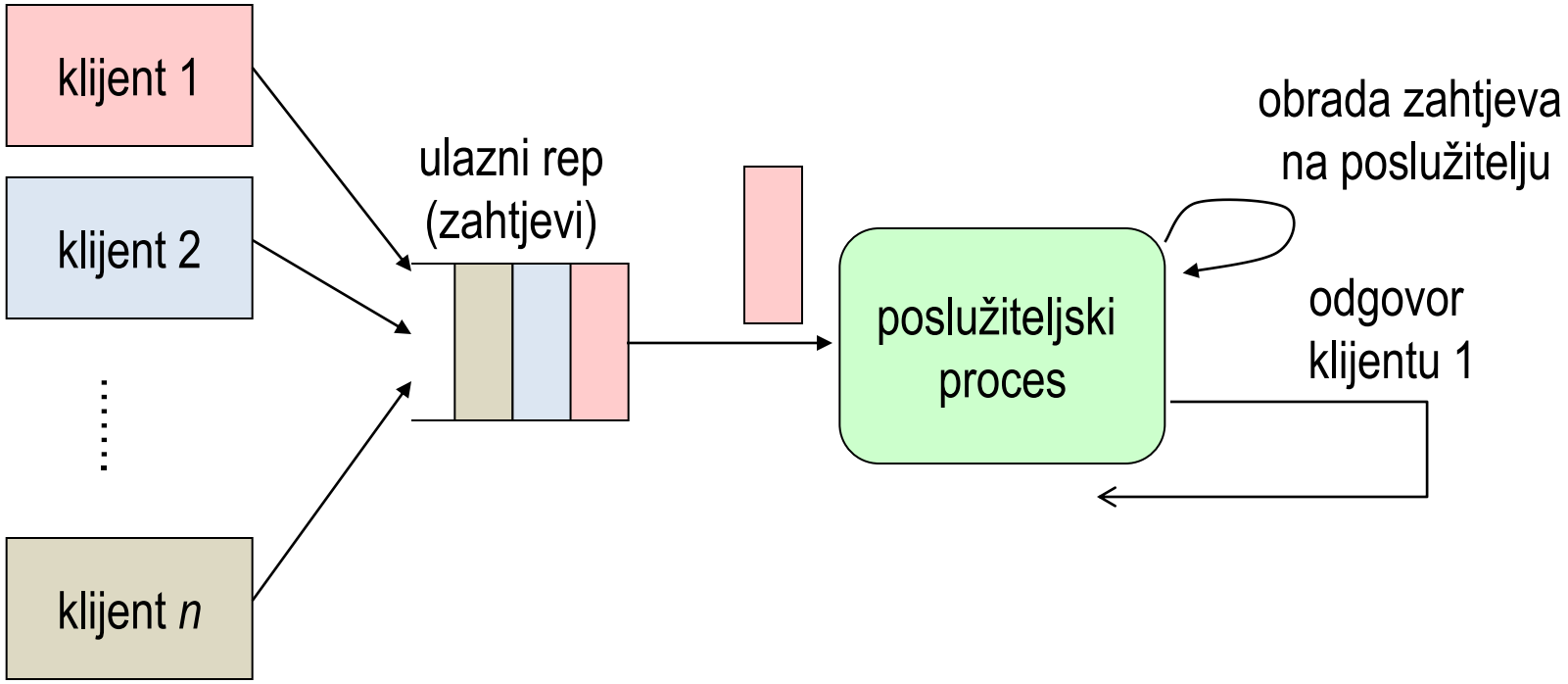


Način rada poslužitelja

- klasifikacija prema pamćenju stanja može biti:
  - memorijski, čuva (pamti) stanje (engl. *stateфull*)
    - obrada zahtjeva ovisi o rezultatu obrade prethodnih zahtjeva
    - pogodan za obradu niza međusobno povezanih zahtjeva
    - može se modelirati automatom stanja
  - bezmemorijski, ne čuva (ne pamti) stanje (engl. *stateless*)
    - obrada svakog zahtjeva je neovisna o prethodnima
    - pogodan za obradu pojedinačnih, međusobno neovisnih zahtjeva
    - jednostavan model, samo jedno stanje - “obradi i zaboravi”
- klasifikacija prema načinu obrade zahtjeva:
  - iterativan
  - konkurentan

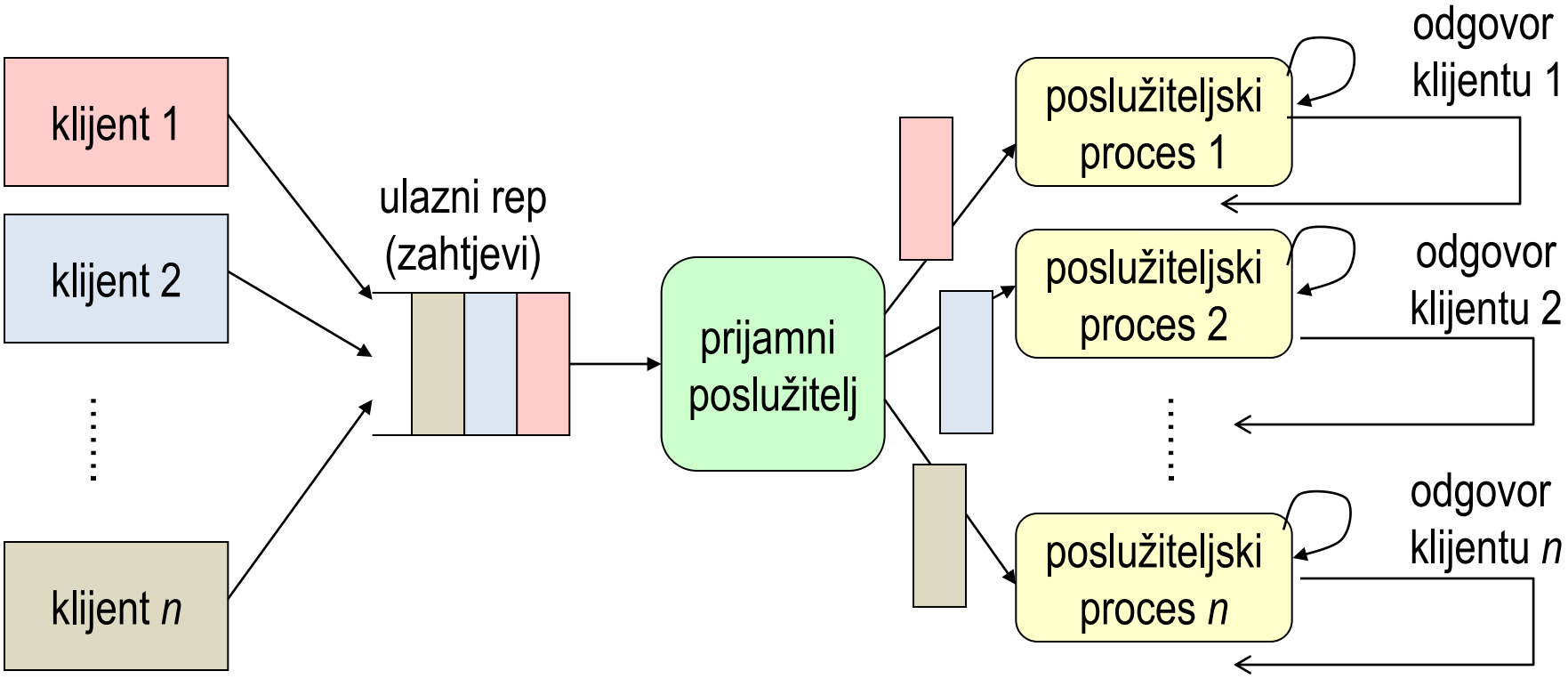
Iterativni poslužitelj

- zahtjevi se obrađuju *iterativno*, tj. jedan-po-jedan
- poslužiteljski proces obrađuje zahtjeve i šalje odgovore
- jednostavniji; pogodan za zahtjeve s kratkim vremenom obrade



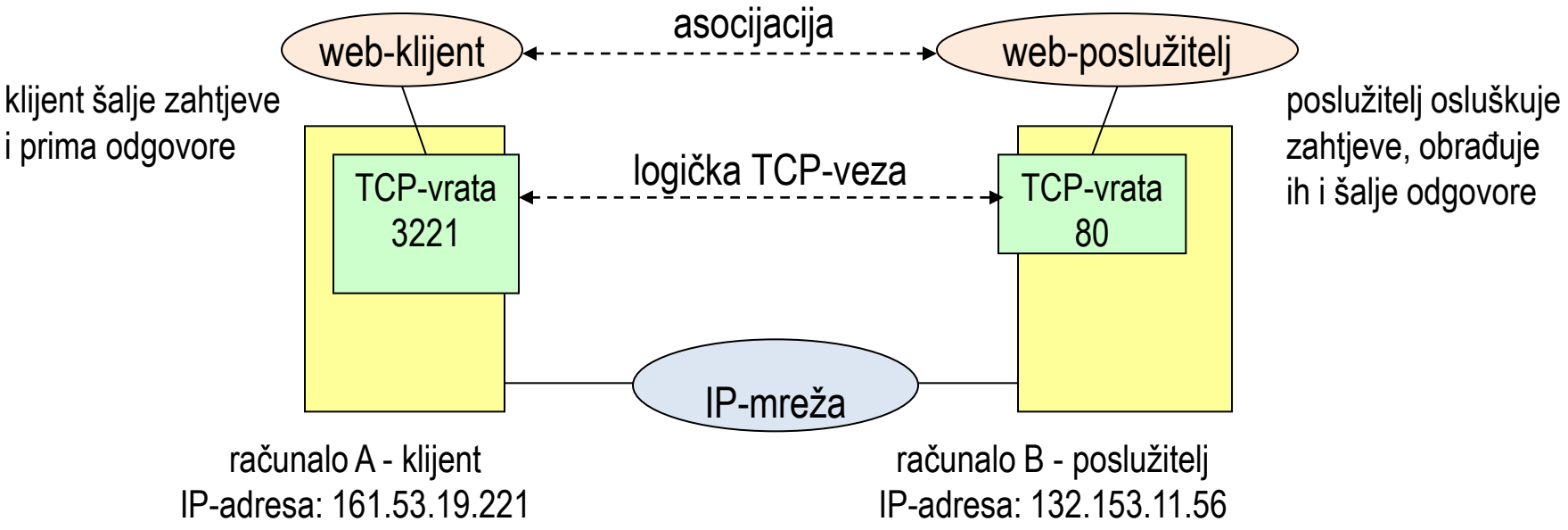
Konkurentni poslužitelj

- zahtjevi se obrađuju *konkurentno*
- prijamni poslužitelj prima zahtjeve, ali ih ne obrađuje sam, već raspoređuje posao obrade i odgovora na poslužiteljske procese
- složeniji; pogodan za više istovremenih ili dugotrajnijih obrada zahtjeva



Asocijacija klijenta i poslužitelja

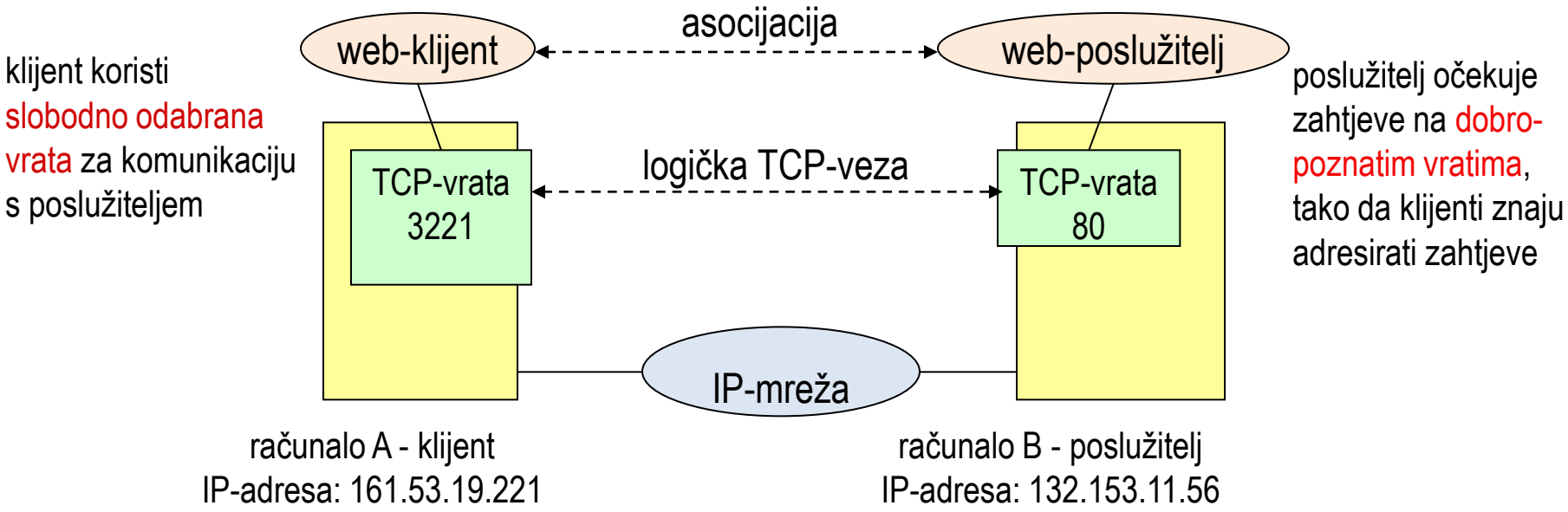
- asocijacija: uspostavljen odnos između procesa klijenta i poslužitelja povrh jedne transportne veze (npr. logička TCP-veza) ili povezanosti (npr. UDP-*binding*)
- za asocijaciju između klijenta i poslužitelja mora se znati:
  - aplikacijski protokol
  - IP-adrese klijenta i poslužitelja
  - transportni protokol (TCP/UDP) i brojeve vrata za klijentski i poslužiteljski proces



pitanje: kako klijent "zna" kamo uputiti zahtjev?

Pronalaženje usluga

- klijent mora unaprijed znati adresu poslužitelja da bi mu pristupio
- na razini cijelog Interneta, unaprijed su definirana *dobro-poznata vrata* (engl. *well-known port*) za standardne internetske usluge
- za usluge koje nemaju dobro-poznata vrata, mora postojati neki drugačiji način (npr. imenička usluga)



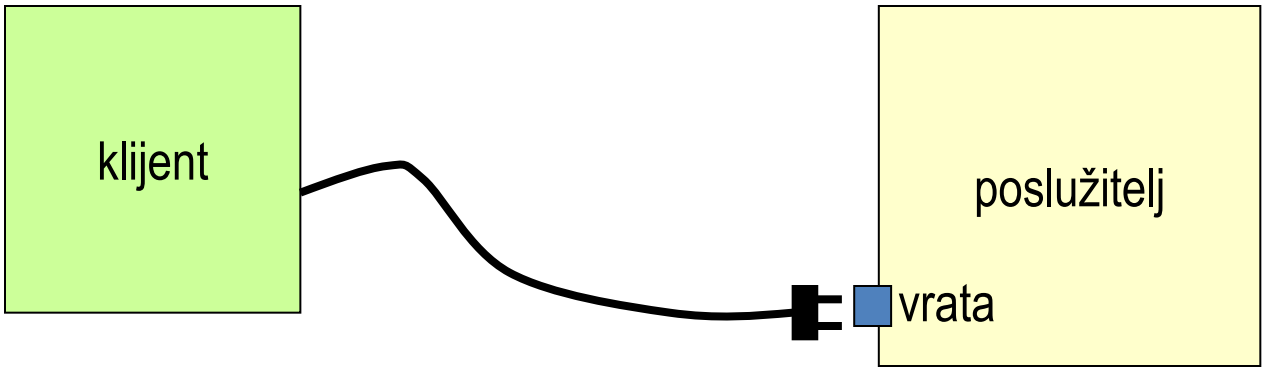
Neka dobro-poznata vrata

- *dobro-poznata vrata*: 0-1023 su “rezervirana” za standardne usluge
- primjeri nekih dobro-poznatih vrata:

```
Keyword        Decimal    Description
-------        -------    -----------
ftp-data        20/tcp    File Transfer [Default Data]
ftp-data        20/udp    File Transfer [Default Data]
ftp             21/tcp    File Transfer [Control]
ftp             21/udp    File Transfer [Control]
ssh             22/tcp    SSH Remote Login Protocol
ssh             22/udp    SSH Remote Login Protocol
telnet          23/tcp    Telnet
telnet          23/udp    Telnet
...
smtp            25/tcp    Simple Mail Transfer
smtp            25/udp    Simple Mail Transfer
...
domain          53/tcp    Domain Name Server
domain          53/udp    Domain Name Server
...
http            80/tcp    World Wide Web HTTP
```

Programsko sučelje (*socket API*)

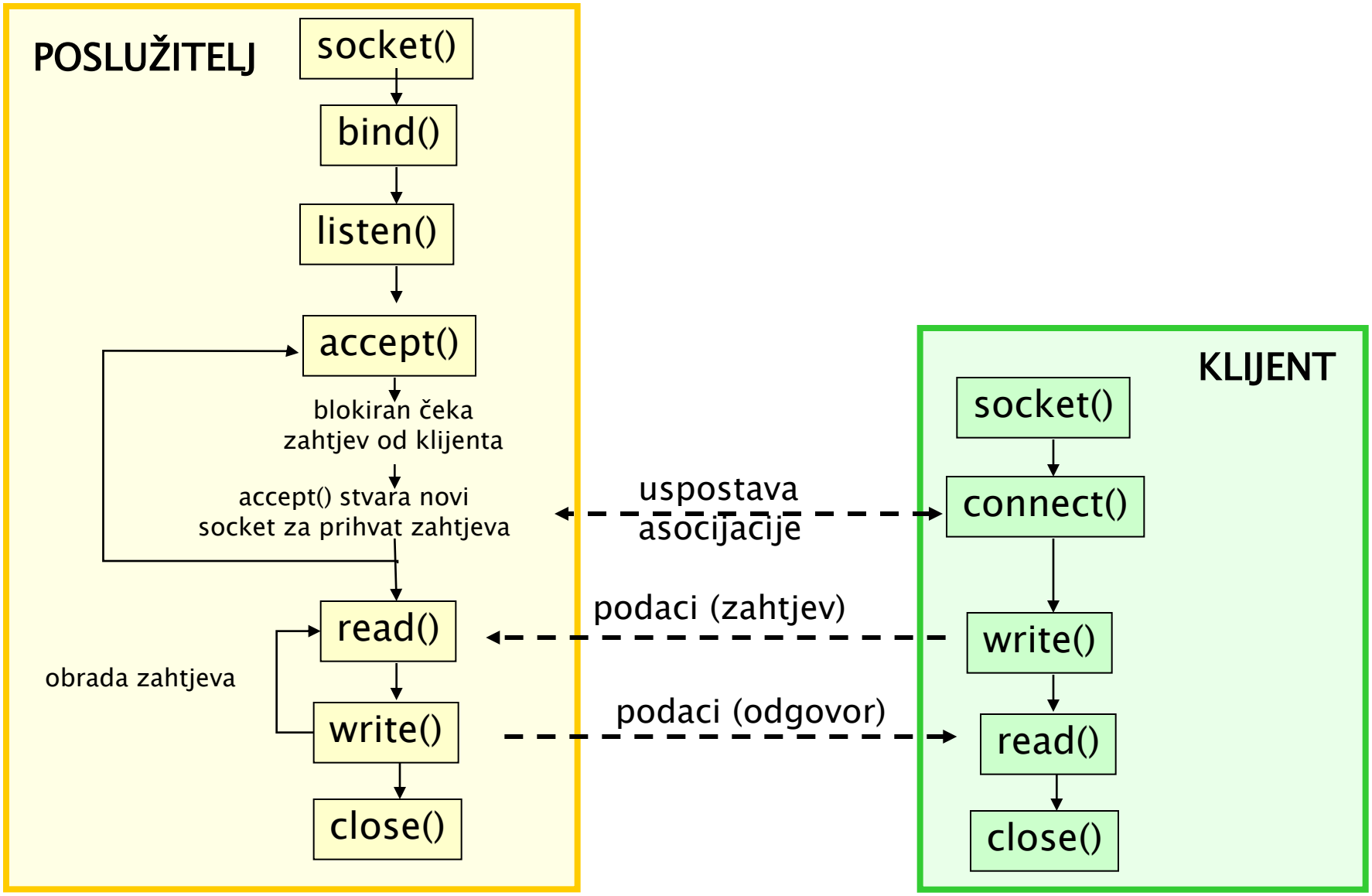
- *socket* (priključnica) je programska apstrakcija krajnje točke komunikacije između klijenta i poslužitelja



- ideja: klijent se "priključi" na vrata poslužitelja
- "priključenjem" se stvara asocijacija između procesa – to je pretpostavka za daljnju komunikaciju

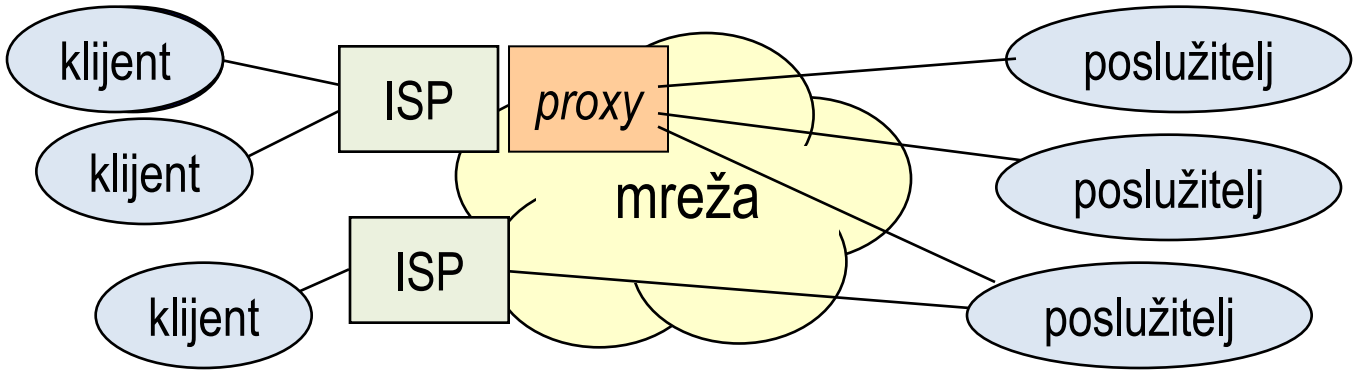
  socket = (IP-adresa, transportni protokol, broj vrata)
  - primjer: priključnica na strani web-poslužitelja (161.53.19.220, TCP, 80)

Socket API - tipične radnje klijenta i poslužitelja



Gdje usluge mogu biti smještene?

- na poslužitelju (uobičajen slučaj)
  - npr. pretraživači, e-trgovina, poslužitelji sadržaja i drugih usluga vezanih za odredište
- djelomično (i) na klijentu (npr. Java, JavaScript, ActiveX dodaci za Web, AJAX)
  - npr. provjera unesenih podataka na web-obrascu prije slanja zahtjeva
- "negdje između"
  - posrednički poslužitelj (engl. *proxy*)



Uloge i primjeri posredničkih poslužitelja

- "klasična" posrednička uloga
  - dobavljanje podataka za klijenta od nekog drugog poslužitelja
  - posredovanje pri dohvatu sadržaja (kompresija, filtiranje, anonimizacija, jezično prevođenje, ...)
  - prikupljanje sadržaja s više poslužitelja
- međuspremnička uloga
  - privremeno pohranjivanje sadržaja (engl. *caching*)
  - pohranjivanjem sadržaja dobiva se brži odziv jer se često traženi podaci uzimaju iz lokalnog spremnika umjesto s udaljenog poslužitelja (primjeri primjene: Web, DNS)
- nadzor i ograničenje pristupa
  - filtriranje prometa (primjer: *firewall*)
  - ograničenja u dolasku ili odlasku, najčešće na rubu interne poslovne mreže

Sadržaj predavanja

- **Osnove internetskih usluga**
  - usluge i aplikacijski protokoli
  - modeli izvedbe usluga
  - pronalaženje usluga
  - programska podrška
- **Sustav domenskih imena**
  - prostor domenskih imena
  - registracija imena
  - organizacija i izvedba sustava DNS

Sustav domenskih imena

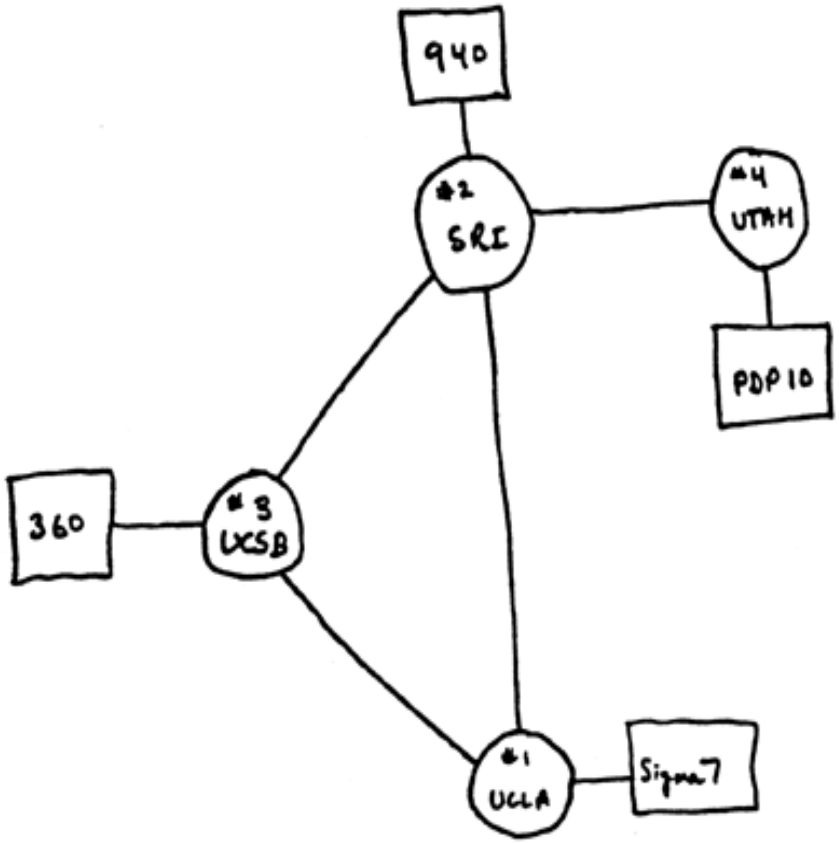
- engl. **Domain Name System (DNS)**
- “imenik Interneta”
- pridružuje razne vrste informacija imenu domene
- najčešća uporaba: pridruživanje numeričke IP adrese lako pamtljivom imenu računala (postoje i druge uporabe)
- primjeri:

www.fer.hr	↔	161.53.72.23
www.hakom.hr	↔	213.149.32.101
www.croatiaairlines.hr	↔	193.47.246.68

- DNS je jedna od sustavskih (infrastrukturnih) usluga u Internetu – njome se služe druge internetske usluge, a krajnji korisnici (uglavnom) ne

Imenovanje računala

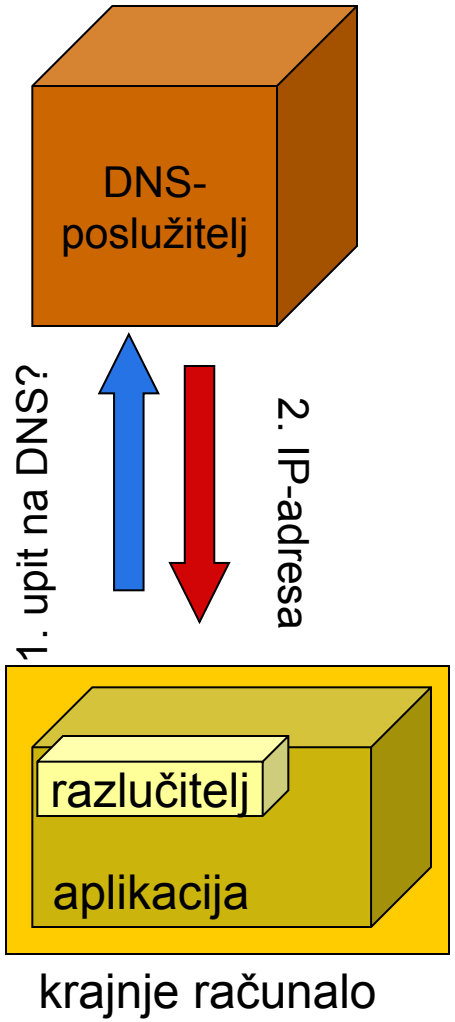
- IP adrese su od početka namijenjene strojnom adresiranju
- ljudima je lakše pamtiti simbolička imena računala, nego brojeve
- prvo rješenje - popis IP adresa i imena svih računala s kojima se komunicira – datoteka *hosts.txt*
- sredinom 1980.-tih godina javlja se potreba za skalabilnijim rješenjem – uvodi se ***Domain Name System***



Skica ARPANET-a iz 1969. godine, 4 čvora
http://www.computerhistory.org/internet_history/

Uporaba DNS-a, osnovna ideja

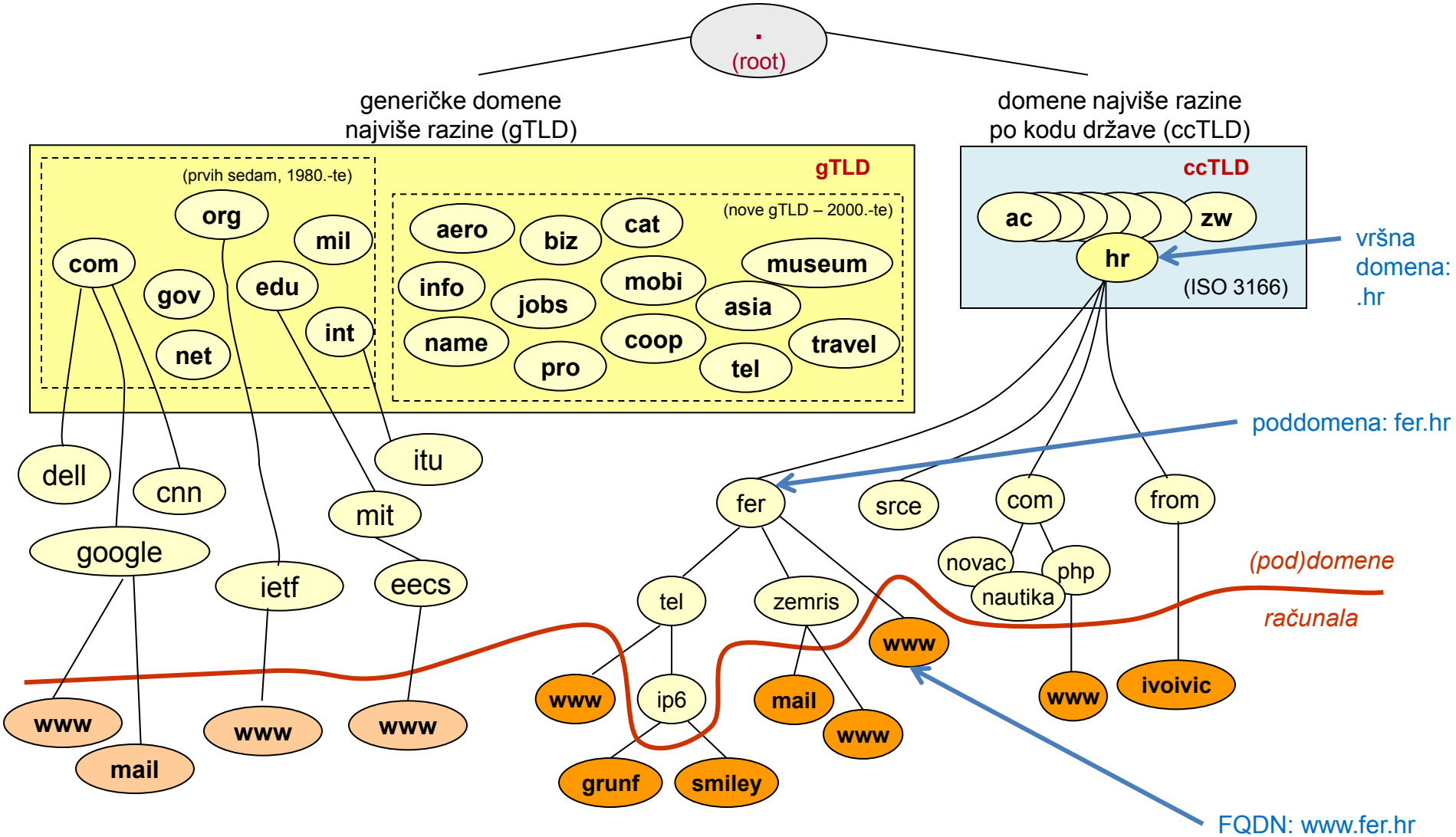
- korisnik pamti i rabi simboličke adrese, npr.:
  - pristupa stranici weba na poslužitelju www.fer.hr
  - piše poruku elektroničke pošte prijatelju na ivo.ivic@fer.hr
- računalni uređaji/procesi rabe IP-adrese
  - aplikacijski program će prvo "u pozadini" pozvati funkciju razlučitelja (engl. *resolver*) sa simboličkim imenom kao parametrom
  - razlučitelj će poslati upit DNS-poslužitelju i saznati IP-adresu odredišta
  - aplikacija koristi dobivenu IP-adresu za, npr., uspostavu TCP-veze prema web-poslužitelju



Terminologija

- sustav domenskih imena
  - "(...) ideja *hijerarhijskog sustava imena*, *gdje hijerarhija grubo odgovara organizacijskoj strukturi, a za odvajanje razina hijerarhije u imenima koristi se znak '.' (točka).*" (RFC 1034)
  - domena
    - skupina (mrežnih sučelja) računalnih uređaja koje (najčešće) karakterizira pripadnost određenoj organizaciji
    - može imati pod-domene, na primjer: .hr, .fer.hr, .tel.fer.hr, .zemris.fer.hr
  - potpuno kvalificirano domensko ime (engl. *Fully Qualified Domain Name*, FQDN)
    - daje jedinstvenu identifikaciju krajnjeg mrežnog sučelja – preslikava se na IP-adresu(e)
    - općeniti oblik: host.poddomena.domena, primjer: www.fer.hr

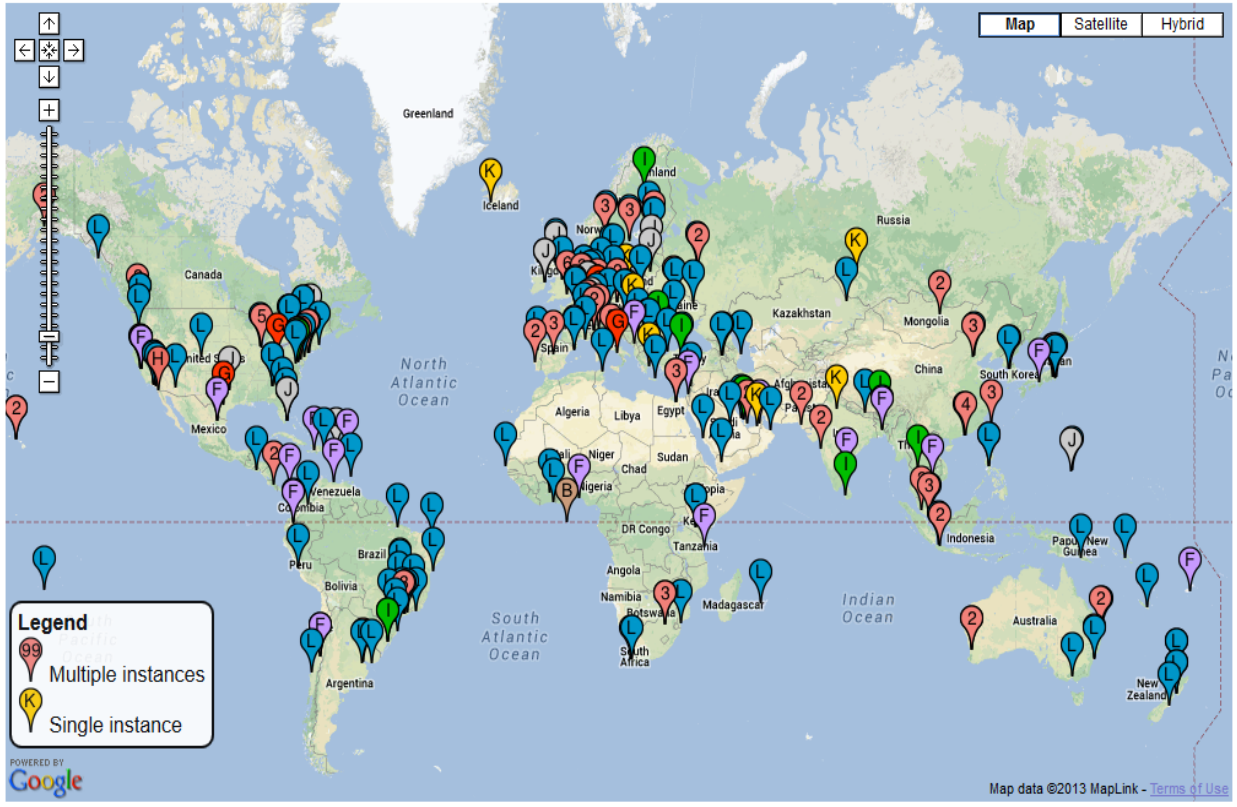
Prostor domenskih imena



*TLD - Top Level Domain

Hijerarhija domena (1/2)

- Vrhovni ili “korijenski” DNS-poslužitelj na vrhu hijerarhije (engl. *root DNS server*)
  - u praksi, “root server” čini 13 poslužitelja (označenih slovima od a do m, npr. a.root-servers.net) uz više identičnih instalacija širom svijeta (stanje 10/2013, 377 poslužitelja)



Izvor:
http://www.root-servers.org/

Hijerarhija domena (2/2)

- Domene najviše razine – vršne domene
  - generičke domene najviše razine
    - engl. *generic Top Level Domain* (gTLD)
    - ima ih samo 20: sedam početnih (.com, .edu, .gov, .int, .mil, .net, .org), te trinaest dodanih kasnije te posebna domena (.arpa) za reverzni DNS upit
    - u 2007. postignut dogovor o pravilima za otvaranje novih gTLD; uklanjanje ograničenja s obzirom na aktualne potrebe - početak primjene 2012. godine
  - domene najviše razine prema kodu države
    - engl. *country code Top Level Domain* (ccTLD) - ccTLD za Hrvatsku - oznaka **.hr**
    - ima ih više od 250; standardne dvoslovne oznake država i teritorija (popis ISO 3166-1);
    - internacionalizirane domene (engl. *internationalized country code top-level domains* (IDN ccTLD): državne domene koje ne primjenjuju skup znakova latinične abecede (npr. arapski, kineski, grčki)
  - posebna domena .arpa za potrebe internetske infrastrukture
- Poddomene, hijerarhijski organizirane (stablo)

Internacionalizacija i sigurnosna proširenja DNS-a

- Internacionalizacija domenskih imena (IDN)
  - motivacija: više od 60% korisnika Interneta ne govori engleskim jezikom, niti se služi latiničnim pismom
  - primjena lokalnih jezika i znakovnih sustava
  - **http://실례.테스트** (“example.test” u korejskom pismu Hangul)
  - uvođenje kroz uspostavu novih gTLD i ccTLD s primjenom lokalnih naziva i pisma
- Sigurnosna proširenja
  - DNSSEC (skraćeno od *DNS Security Extensions*)
  - pružaju Internetu zaštitu od nekih vrsta napada na sigurnost
  - skup proširenja koja osiguravaju a) autentičnost izvora DNS podataka, b) integritet podataka i c) autentičnost nepostojanja unosa u DNS-u
  - u suradnji ICANN-a i VeriSigna

Upravljanje registracijom imena u DNS-u

- hijerarhijom domena upravlja ICANN, odn. IANA
  - postoje tijela kojima se delegira odgovornost za domenu
  - u Hrvatskoj: **CARNet**
    - upravljanje vršnom domenom .hr
    - registracija besplatnih domena unutar domene .hr
    - domene uz naplatu registriraju se putem ovlaštenih registrara
  - Pravilnik o ustrojstvu i upravljanju vršnom nacionalnom internetskom domenom (NN 038/2010)

CARNet DNS služba
http://www.dns.hr/

Vrste zapisa u DNS-u

- podaci:
  - zapisi o domeni i o pojedinim računalima (engl. *Resource Record*)
  - svaki zapis ima postavljen "rok trajanja" (engl. *Time To Live*)

- vrste zapisa:
  - za razlučivanje IP-adrese krajnjeg računala:

    zapis tipa **A**:

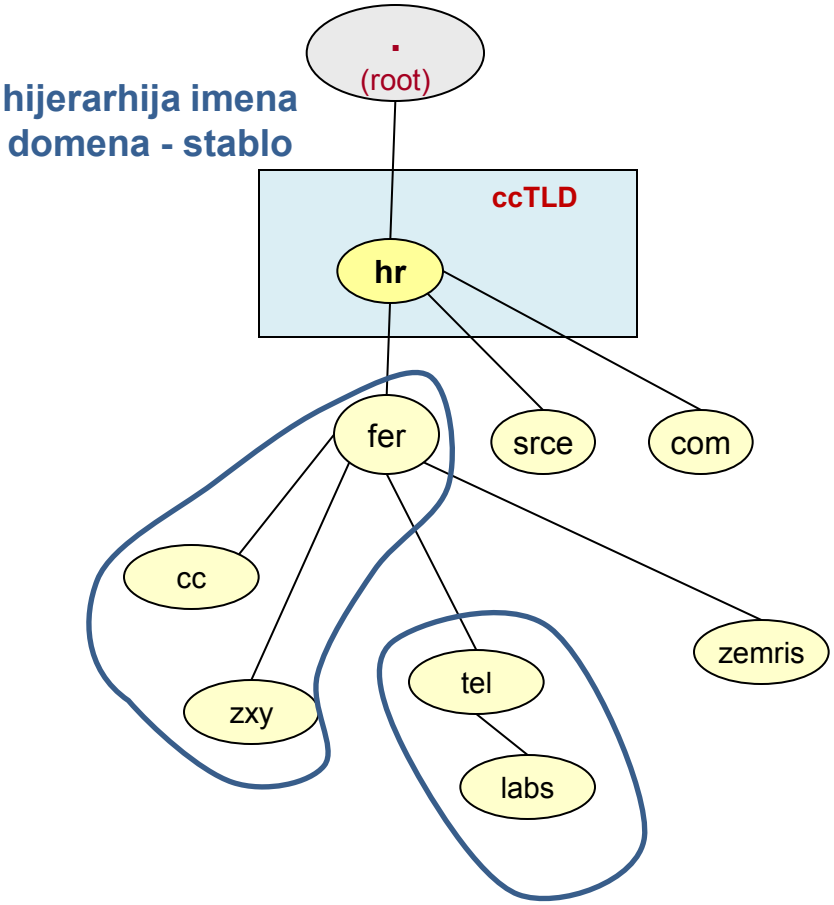
```
quark     IN     A          161.76.21.4
```

  - za razlučivanje imena i IP-adrese poslužitelja elektroničke pošte,

    zapis tipa **MX** (mail exchange)
  - postoje i druge vrste zapisa, definira ih IANA

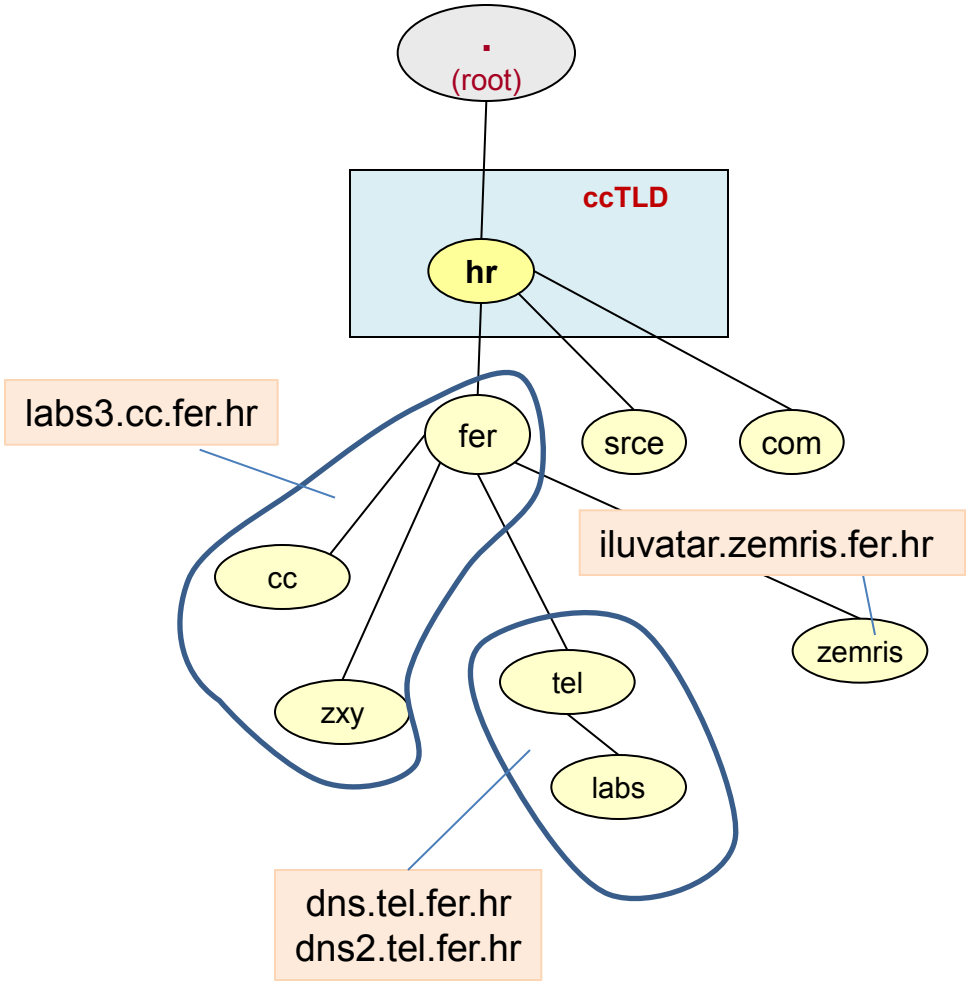
Organizacija sustava DNS (1/2)

- DNS je organiziran kao hijerarhijska distribuirana baza podataka
  - postoji vrhovni ili “korijenski” DNS-poslužitelj na vrhu hijerarhije
  - niti jedan DNS-poslužitelj nema popis svih domenskih imena!
  - neki DNS-poslužitelji nadležni su za dio prostora domenskih imena – to može biti domena ili zona (= više domena, dio “stabla”)



Organizacija sustava DNS (2/2)

- pitanje: podjela “odgovornosti” za točnost podataka?
- DNS-poslužitelj nadležan za domenu (zonu) ima potpun i ispravan popis podataka o toj domeni (zoni)
- ostali DNS-ovi, za upite koji se odnose na tu zonu, djeluju kao posrednici: “pitaju” nadležne i privremeno pohranjuju odgovor, kojeg (dok vrijedi) mogu vraćati na upite za istom adresom



Postupak razlučivanja IP-adrese

- logički gledano:

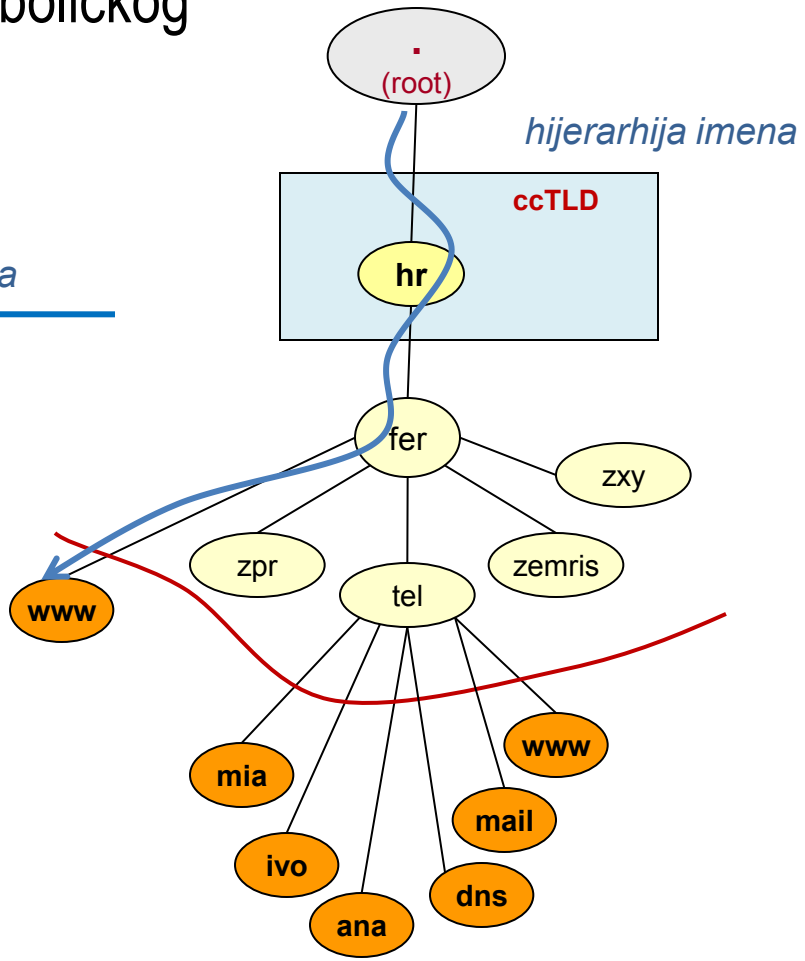
  razlučivanje adrese = preslikavanje simboličkog imena u IP-adresu

hijerarhija imena

računalo.poddomena.domena

- izvedbeno:

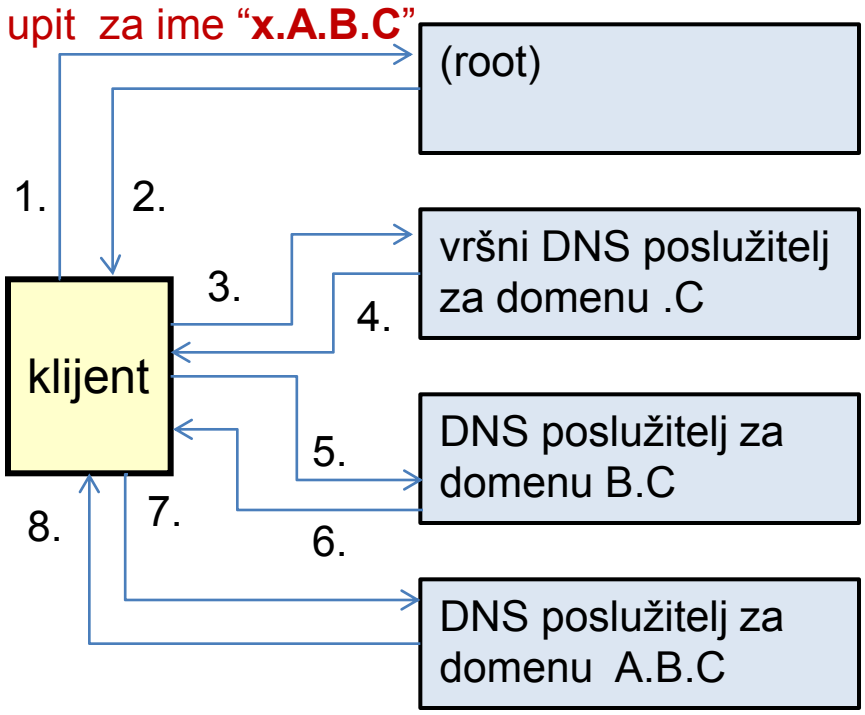
  "prolaz" kroz hijerarhiju stabla domenskih imena odgovara nizu upita prema poslužiteljima nadležnima za zonu/domenu



Načini razlučivanja adrese

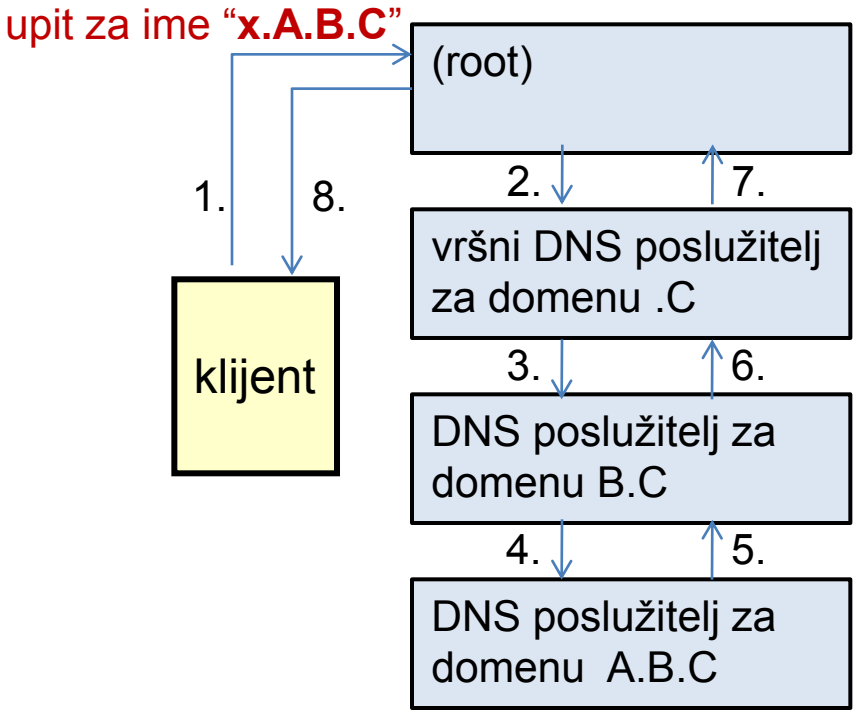
iterativni način

- klijent uzastopno formira i šalje zahtjeve dok sam ne dođe do poslužitelja koji ima traženu informaciju

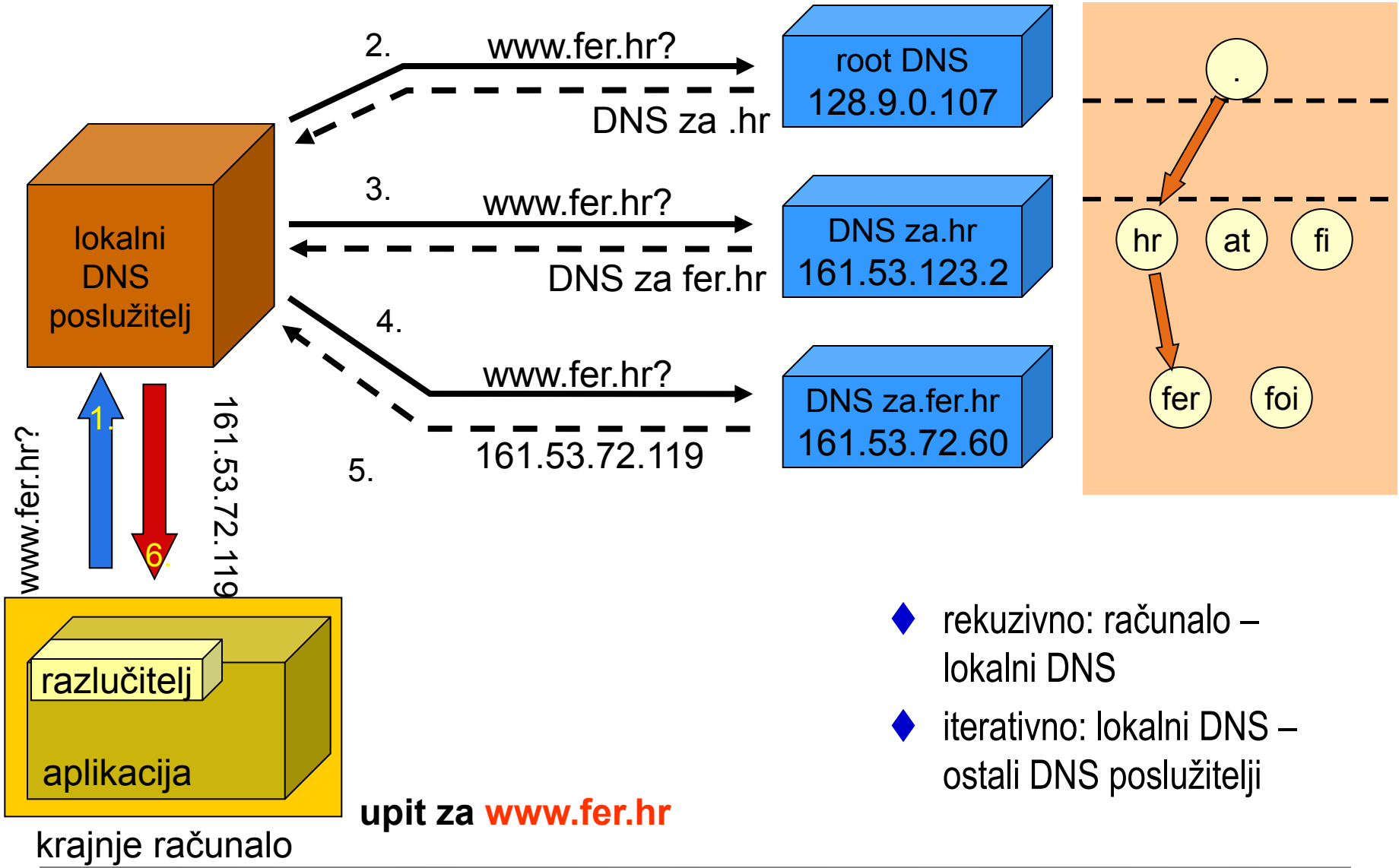


rekurzivni način

- poslužitelj vraća traženu informaciju ako je ima; inače "pita dalje" (ponaša se kao klijent – rekurzija)



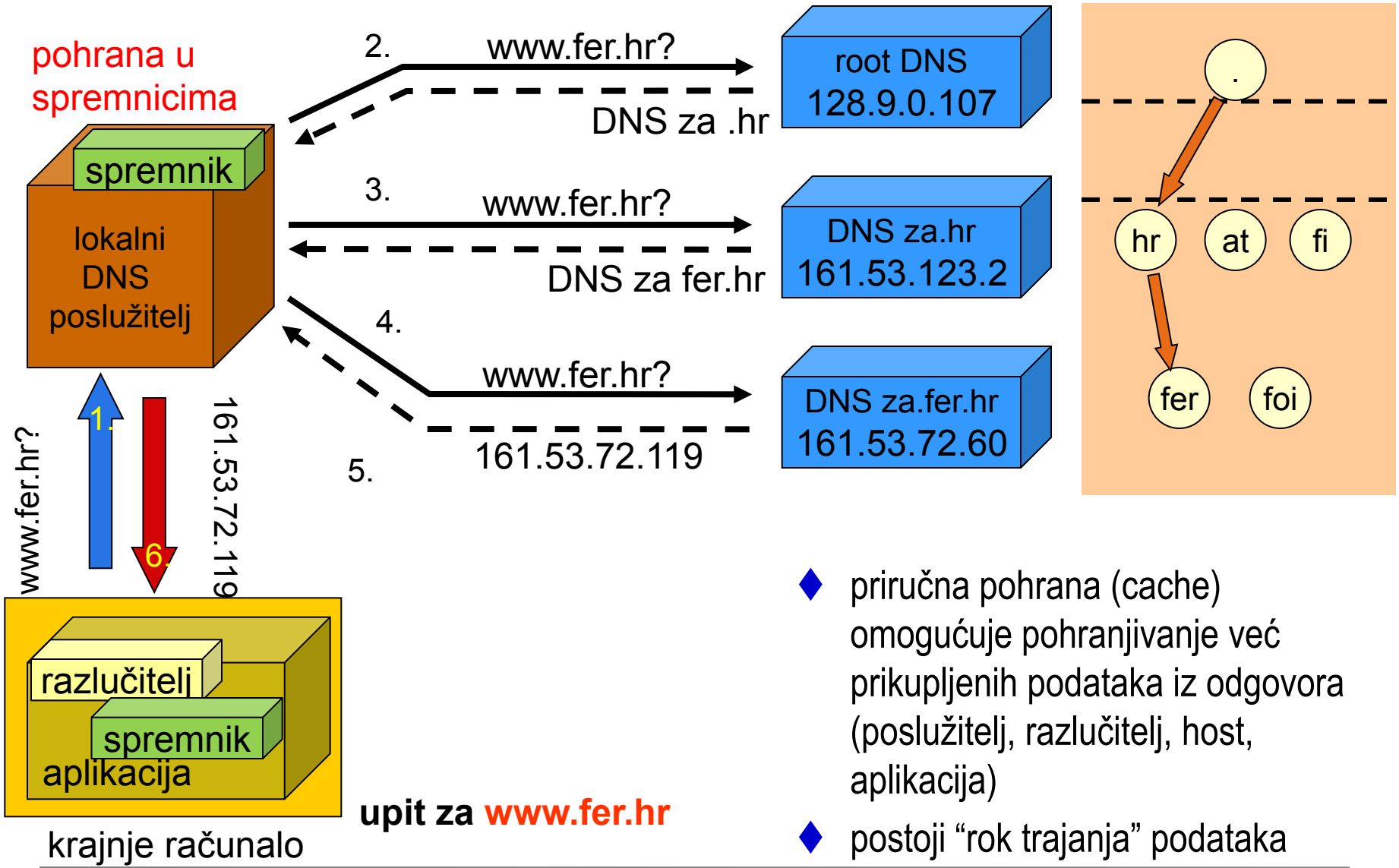
Način razlučivanja u praksi: rekurzivno + iterativno



- rekuzivno: računalo – lokalni DNS
- iterativno: lokalni DNS – ostali DNS poslužitelji

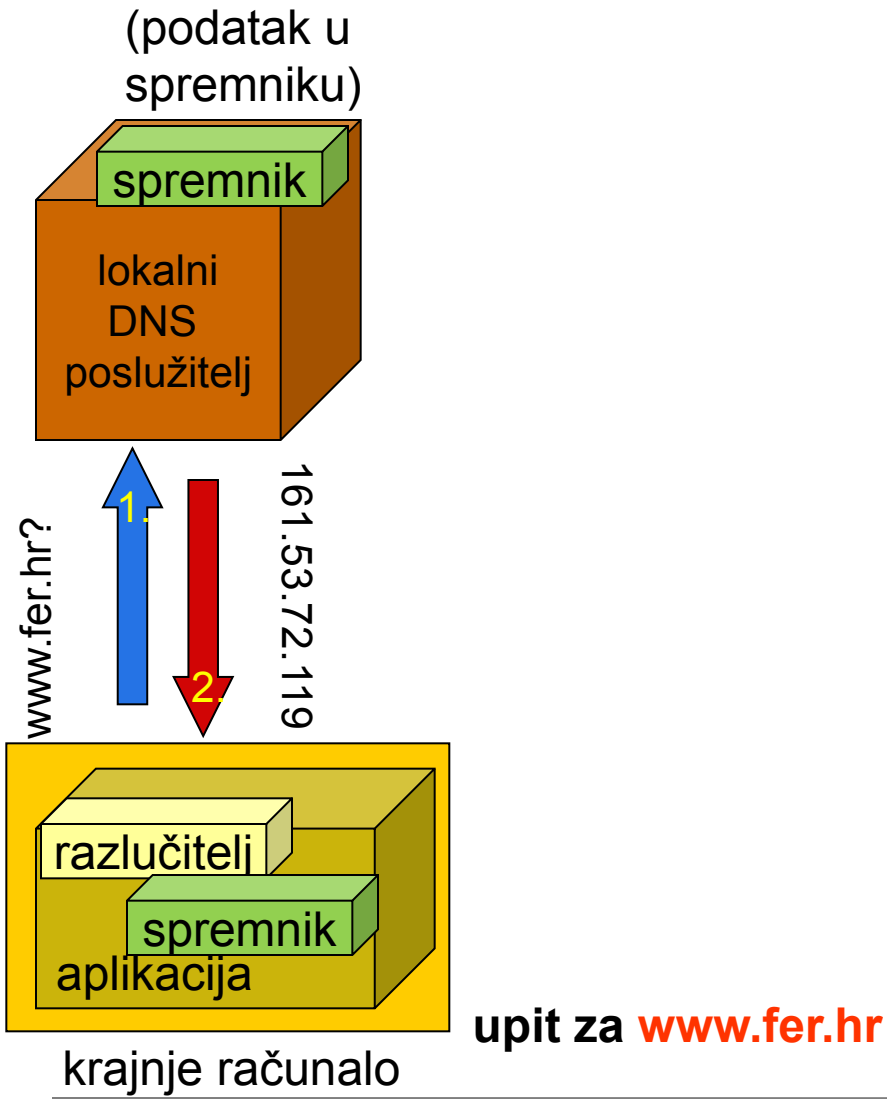
upit za www.fer.hr

Način razlučivanja u praksi: priručna pohrana



- priručna pohrana (cache) omogućuje pohranjivanje već prikupljenih podataka iz odgovora (poslužitelj, razlučitelj, host, aplikacija)
- postoji “rok trajanja” podataka

Način razlučivanja u praksi: priručna pohrana



upit za www.fer.hr

- svi ranije pribavljeni podaci pohranjuju se u spremnicima i mogu se (za vrijeme roka važenja) ponovno iskoristiti
- u ovom primjeru to su.:
  - traženi podatak
  - adresa DNA-a za domenu fer.hr
  - adresa DNS-a za domenu .hr
- prednosti priručne pohrane:
  - brži odgovor na upit
  - smanjivanje opterećenja DNS poslužitelja prema vrhu hijerarhije

Primjer – nslookup (korisnik spojen putem ADSL-a)

```
C:\>nslookup
Default Server:  mygateway1.ar7
Address:  192.168.1.1

> www.fer.hr
Server:  mygateway1.ar7
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.fer.hr
Address:  161.53.72.119
.....
> www.zxyyz.hr
Server:  mygateway1.ar7
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
*** Request to mygateway1.ar7 timed-out
>
```

nslookup – alat za postavljanje DNS upita

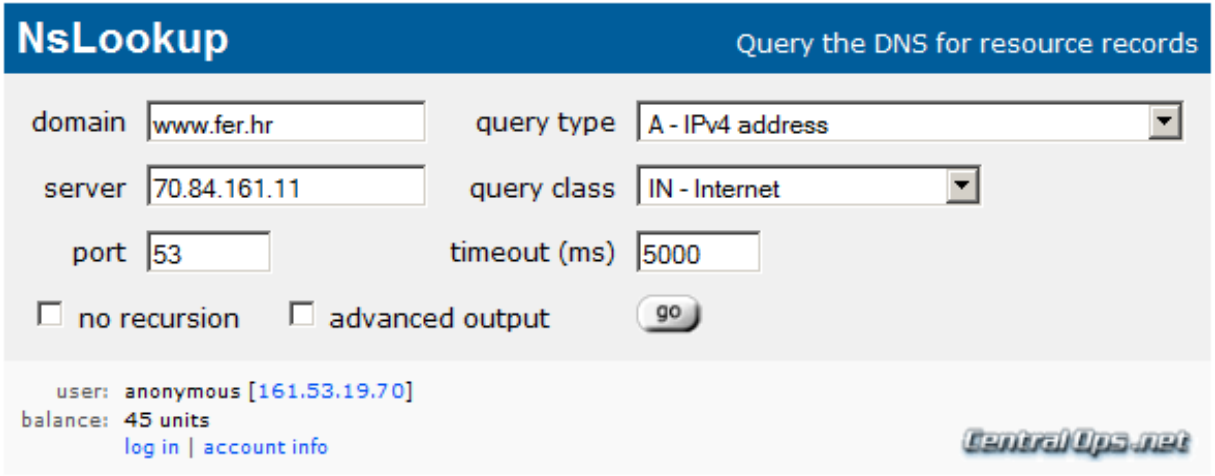
primjer 1:
upit za ime www.fer.hr

tražena IP-adresa

primjer 2:
upit za nepostojeće ime
(ili greška u pisanju ☺)

neuspješni ishod

Primjer – upit tipa A za računalo www.fer.hr



NsLookup — Query the DNS for resource records

domain: www.fer.hr — query type: A - IPv4 address

server: 70.84.161.11 — query class: IN - Internet

port: 53 — timeout (ms): 5000

☐ no recursion ☐ advanced output go

user: anonymous [161.53.19.70]
balance: 45 units
log in | account info

CentralOps.net

Sending DNS query for **www.fer.hr**...

[70.84.161.11] returned a **non-authoritative** response in 190 ms:

Answer records

name	class	type	data	time to live
www.fer.hr	IN	A	161.53.72.119	3600s (01:00:00)

"rok trajanja" zapisa

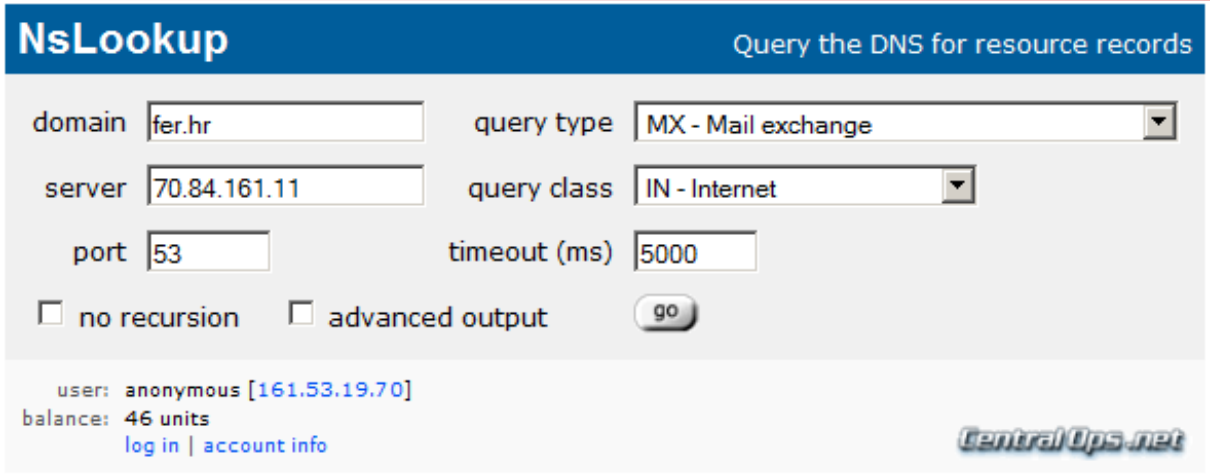
tražena IP-adresa

Authority records

name	class	type	data	time to live
fer.hr	IN	NS	branka.zesoi.fer.hr	3600s (01:00:00)
fer.hr	IN	NS	labs3.cc.fer.hr	3600s (01:00:00)

nadležni DNS

Primjer – upit tipa MX za domenu fer.hr



Sending DNS query for **fer.hr**...

[70.84.161.11] returned a **non-authoritative** response in 290 ms:

Answer records

name	class	type	data	time to live
fer.hr	IN	MX	preference: 10 exchange: labs3.cc.fer.hr	600s (00:10:00)

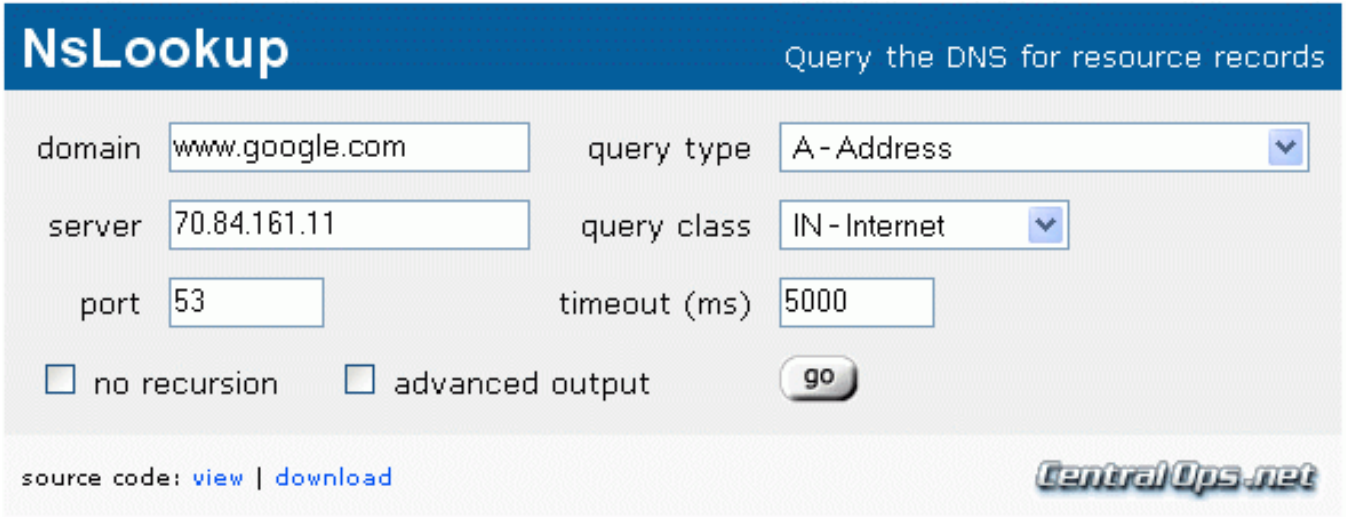
....

Authority records

name	class	type	data	time to live
fer.hr	IN	NS	branka.zesoi.fer.hr	3600s (01:00:00)
fer.hr	IN	NS	labs3.cc.fer.hr	3600s (01:00:00)

domensko ime traženog poslužitelja

Primjer – upit tipa A za računalo www.google.com



[70.84.161.11] returned a **non-authoritative** response in 0 ms:

Answer records

name	class	type	data	time to live
www.google.com	IN	CNAME	www.l.google.com	542395s (6d 6h 39m 55s)
www.l.google.com	IN	A	209.85.165.103	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.147	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.99	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.104	176s (2m 56s)

kanonsko ime (jedinstveno)

više IP-adresa

kraći "rok trajanja" zapisa – mogućnost raspoređivanja opterećenja