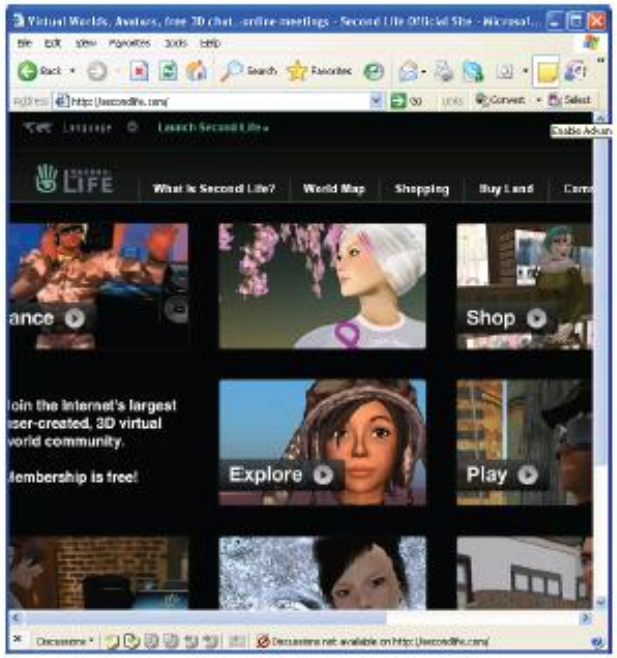
UNIVERZITET CRNE GORE

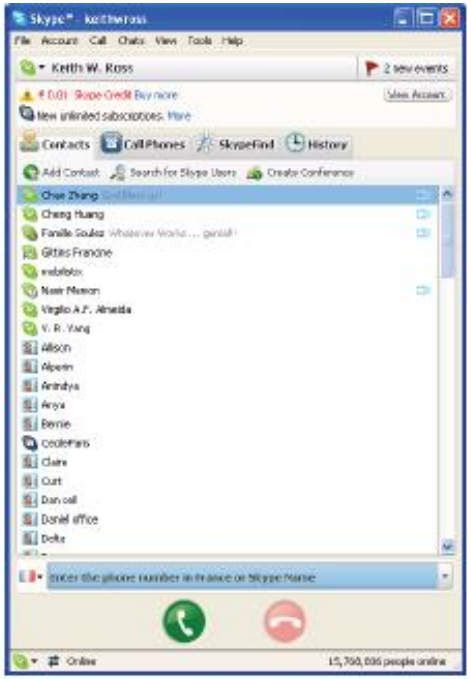
RAČUNARSKE MREŽE

Doc. dr Uglješa Urošević

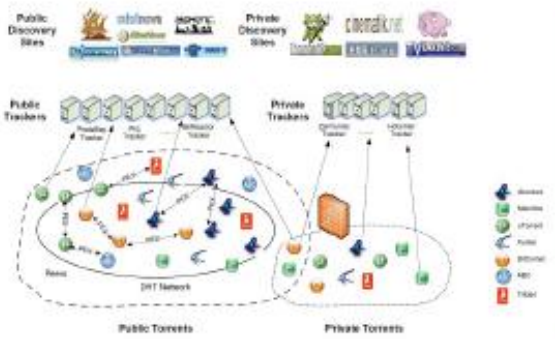
ugljesa@ucg.ac.me

Nivo aplikacije


What is Second Life?
World Map
Shopping
Buy Land
Shop
Explore
Play


Keith W. Ross
Contacts
Call Phones
SkypeFind
History


facebook
Keith Ross


Public Trackers
Private Trackers
DHT Network
Public Torrents
Private Torrents


YouTube
polytechnic of NYU
Search
We will be phasing out support for your browser soon.
Please upgrade to one of these more modern browsers


WhatsApp
WhatsApp Messenger


ONE-CLICK
ACCESS TO
LYRICS AND
MUSIC VIDEOS.


Dropbox


My Dropbox (N:)
Google Drive (L:)
SkyDrive (M:)

Primjeri mrežnih aplikacija

- E-mail
- Web
- "Instant messaging"
- "Remote login"
- "P2P file sharing"
- "Multi-user" mrežne igre
- "Streaming stored" video klipovi (Netflix, Hulu, YouTube,...)
- Internet telefon
- "Real-time" video konferencija
- "Grid computing"
- Društvene mreže
- Cloud computing
- Fog computing

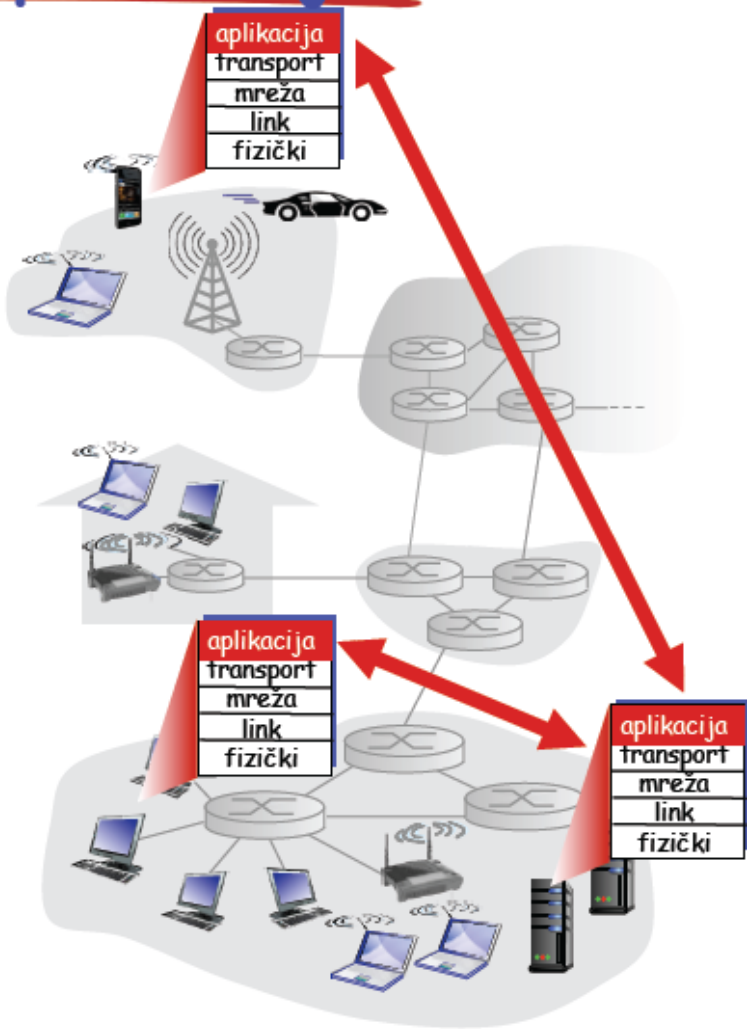
Kreiranje mrežne aplikacije

Napisati programe koji

- se izvršavaju na različitim krajnjim sistemima i
- komuniciraju preko mreže.
- npr., Web: Web server software komunicira preko browser software

Ne piše se softver za uređaje na kičmi mreže

- mrežni uređaji na kičmi uglavnom ne funkcionišu na nivou aplikacije
- ovakav dizajn dozvoljava brzi razvoj aplikacija



Google Data Centri

- Procijenjena cijena jednog data centra: stotine miliona $
- Google je svake godine potroši nekoliko milijardi $ u nove data centre
- Svaki data centar troši stotine MWh električne energije

Google Data Centri

North America

Berkeley County, South Carolina

Council Bluffs, Iowa

The Dalles, Oregon

Douglas County, Georgia

Henderson, Nevada

Jackson County, Alabama

Lenoir, North Carolina

Loudoun County, Virginia

Mayes County, Oklahoma

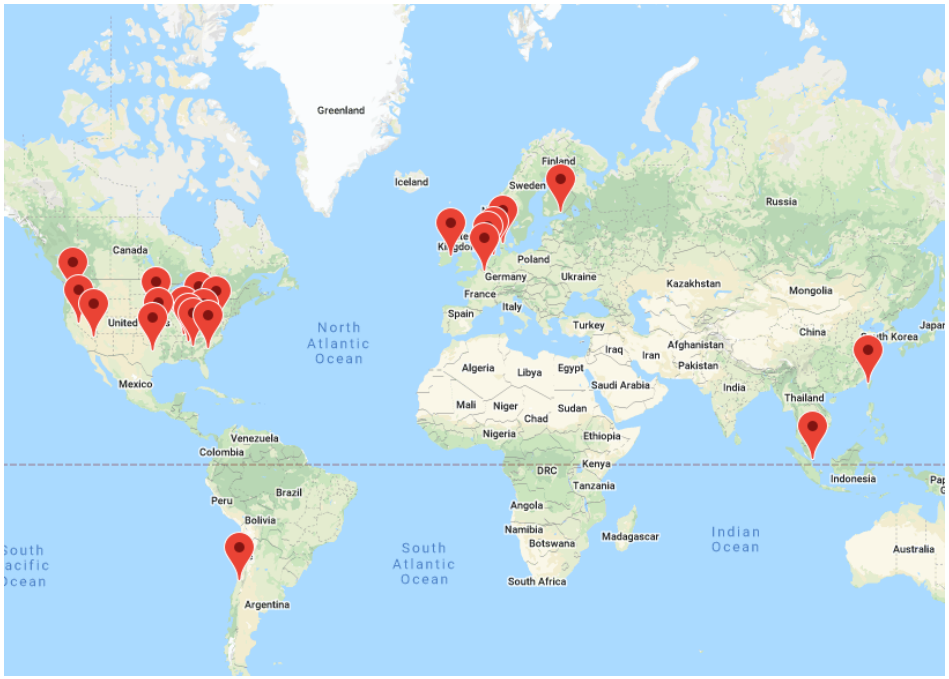
Midlothian, Texas

Montgomery County, Tennessee

New Albany, Ohio

Papillion, Nebraska

Storey County, Nevada



South America

Quilicura, Chile

Europe

Dublin, Ireland

Eemshaven, Netherlands

Fredericia, Denmark

Hamina, Finland

Middenmeer, Netherlands

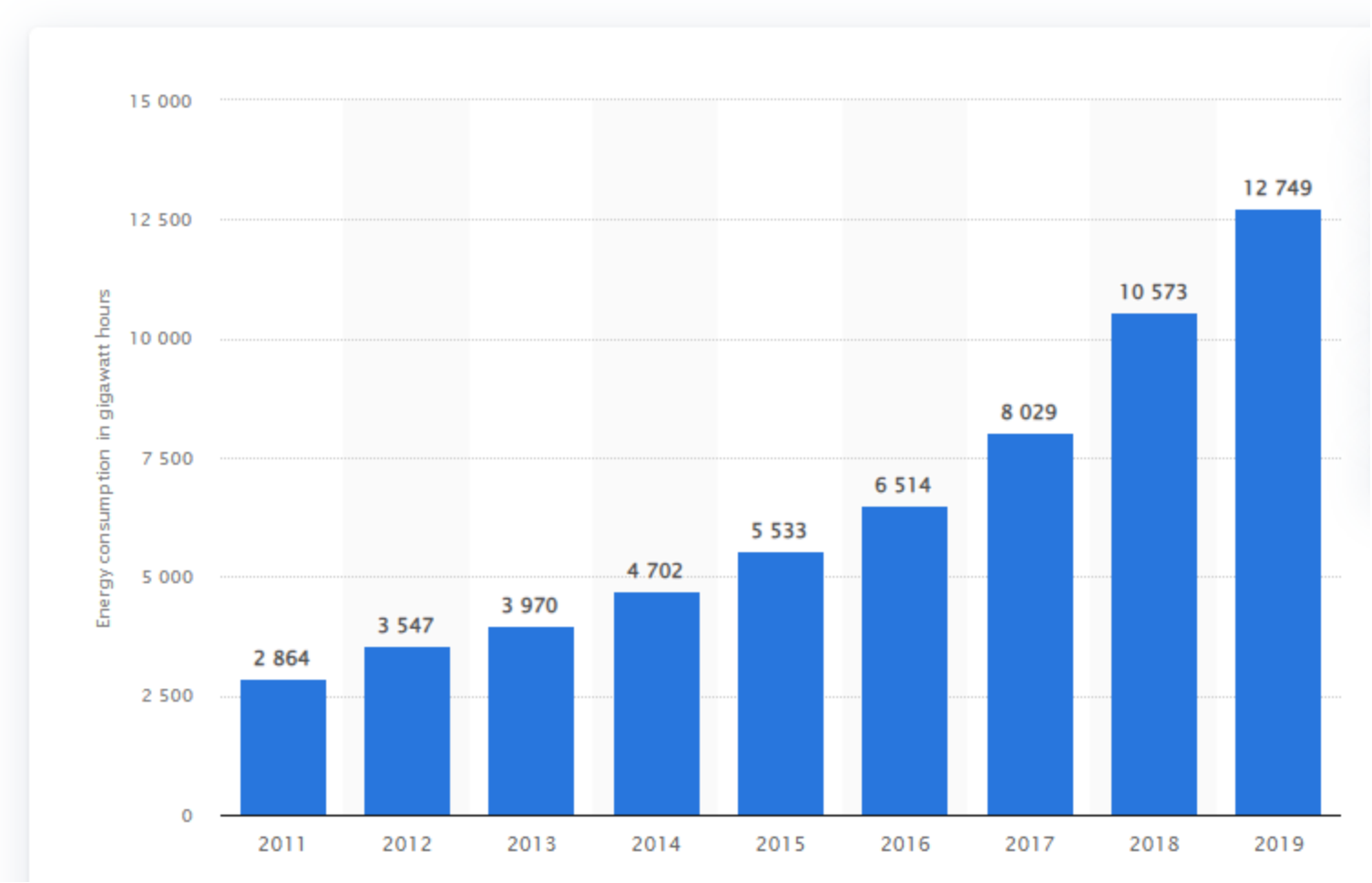
St. Ghislain, Belgium

Asia

Changhua County, Taiwan

Singapore

Google Data Centri



*Potrošnja energije - Alphabet (Google) 2011 do 2019 (**GWh**)*

Poređenje sa energetskom proizvodnjom u CG

Snaga CG elektroenergetskog sistema bazira se na kapacitetima proizvodnih postrojenja HE „Perućica", HE „Piva" i TE „Pljevlja".

Ukupni instalisani proizvodni kapaciteti elektrana iznose 874 MW, od čega hidroelektranama pripada 649 MW ili 74,3%, a termoelektrani 225 MW ili 25,7%.

HE Perućica - instalisana snaga je 307 MW, a moguća godišnja proizvodnja oko 1.300 GWh.

HE Piva - instalisana snaga je 342 MW, a moguća godišnja proizvodnja oko 860 GWh.

TE Pljevlja - instalisana snaga je 225MW, U 2018. godini proizvedeno je 1443,8 GWh energije.

Google Data Centri

U rijetkim slučajevima kada Gugl data centar doživi nestanak struje, treba omogućiti milione vati rezervne električne energije u sekundi. Ovo je težak izazov, sa kojim se industrija obično suočava koristeći dizel generatore.

Prelazak na obnovljive izvore energije.

Plan da se u Belgiji po prvi put umjesto dizel generatora korise baterije za skladištenje energije...

Google Data Centri

Oklahoma data center

Google Data Centri

Google data center

Komuniciranje procesa

Proces: program koji se izvršava na hostu.

- U samom hostu, dva procesa komuniciraju na bazi inter-procesne komunikacije (definisane u OS).
- Procesi na različitim hostovima komuniciraju razmjenom poruka

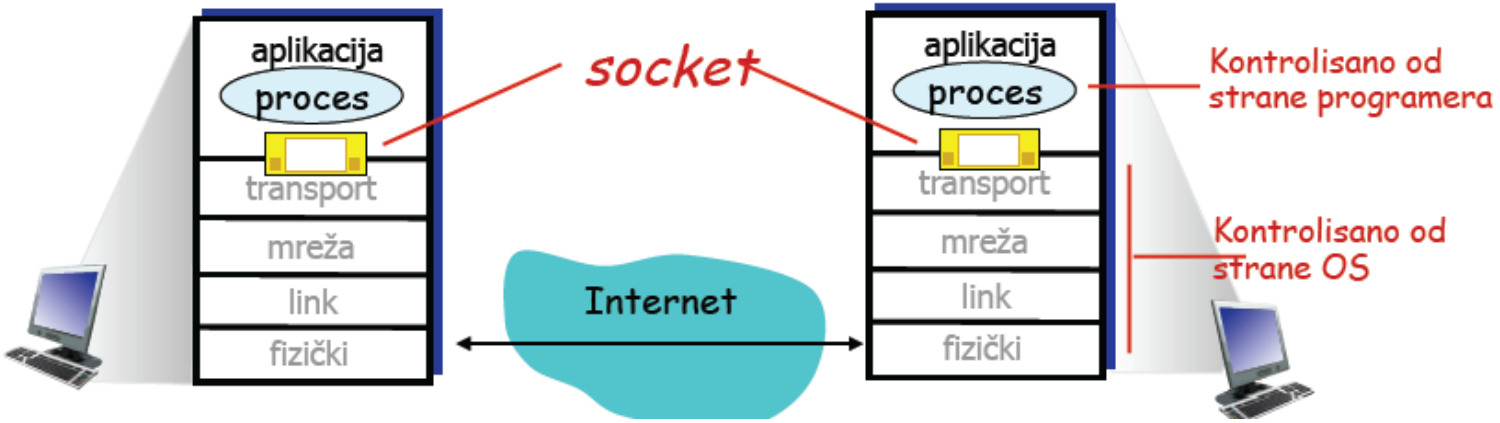
Klijent proces: proces koji inicijalizuje komunikaciju

Server proces: proces koji čeka da bude kontaktiran

- Napomena: aplikacije sa P2P arhitekturom imaju i klijent i server procese

Soketi

- Proces šalje/prima poruke preko svog "socket"-a
- "socket" je analogan vratima
  - Proces šalje poruke preko socketa
  - proces koji šalje se oslanja na transportnu infrastrukturu na drugoj stani vrata koja prenosi poruku do "socket" prijemnog procesa
- API: (1) izbor transportnog protokola; (2) mogućnost specificiranja nekoliko parametara (maksimalna veličina bafera i maksimalna veličina segmenta)



Adresiranje

- Za proces koji prima poruke, mora postojati identifikator
- Svaki host ima jedinstvenu 32-bitnu IP adresu
- Komanda ipconfig...
- P: Da li je IP adresa hosta na kojem se proces izvršava dovoljna za identifikaciju procesa?

- Identifikator uključuje i IP adresu i broj porta vezan za proces na hostu.
- Primjer brojeva porta:
  - HTTP server: 80
  - Mail server: 25
- VIŠE KASNIJE

O: Ne, mnogi procesi se mogu izvršavati na istom hostu

Protokol nivoa aplikacije definiše

- Tipove poruka koje se razmjenjuju, npr., zahtjevi & poruke odgovora
- Tipove sintaksi poruka: koja su polja & kako su odvojena
- Semantika polja, npr., značenje informacija u poljima
- Pravila vezana kada i kako se šalju poruku i kako se odgovara na njih

Javni (public) protokoli:

- Definisani u RFC-ovima
- Dozvoljavaju interoperatibilnost
- npr, HTTP, SMTP

Privatni (proprietary) protokoli:

- npr, Skype,...

Koji transportni servisi su potrebni aplikacijama?

Gubici podataka

- Neke aplikacije (audio) mogu tolerisati određeni nivo gubitaka
- Druge aplikacije (file transfer, telnet) zahtijevaju 100% pouzdani transfer podataka

Vrijeme

- Neke aplikacije (Internet telefonija, interaktivne igre) zahtijevaju malo kašnjenje

Brzina prenosa

- Neke aplikacije (multimedija) zahtijevaju preciziranje minimalne dostupne brzine prenosa
- Druge aplikacije ("elastične aplikacije") koriste onoliko opsega koliko mogu dobiti

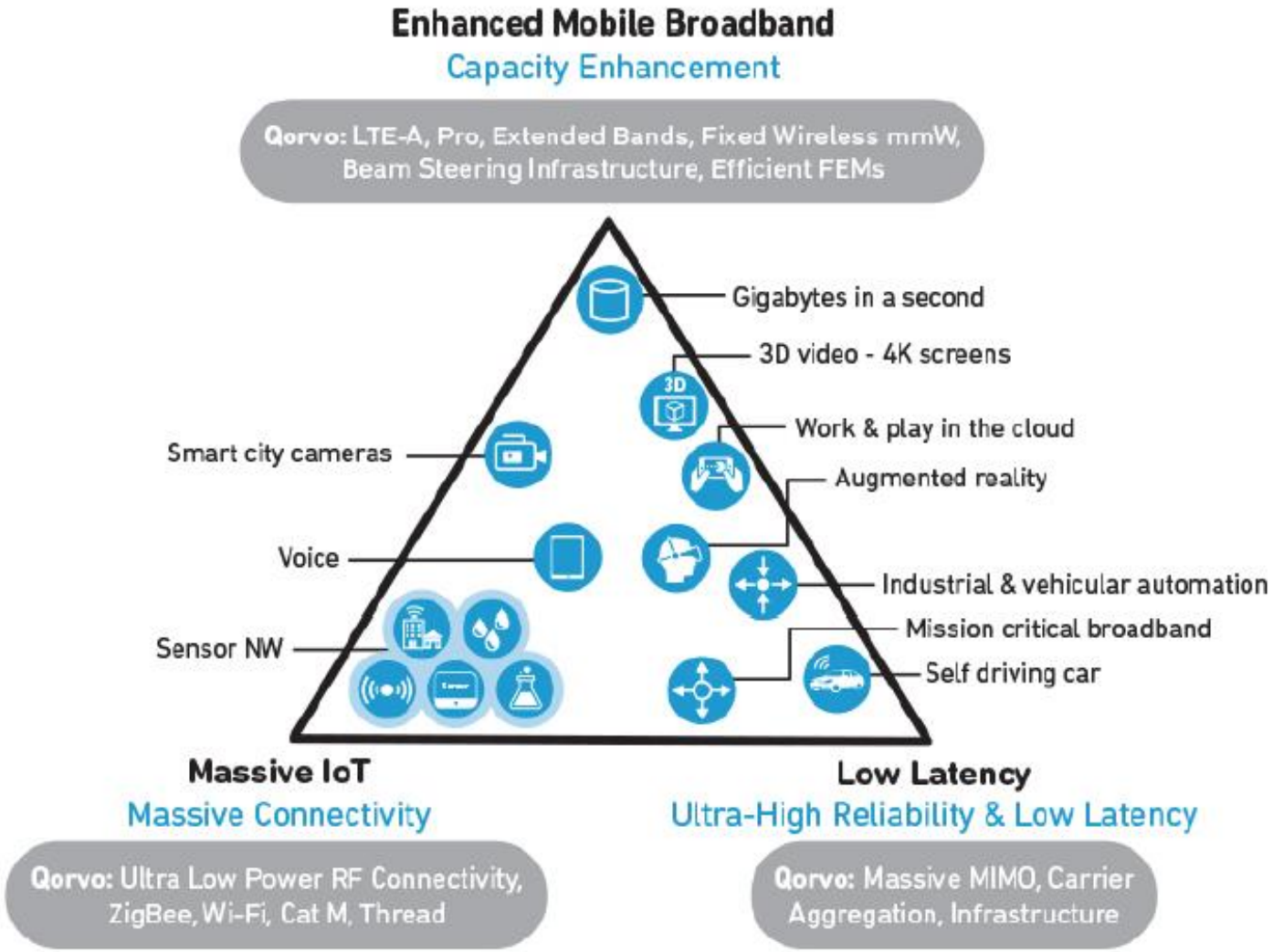
Zaštita

- Enkripcija, integritet podataka, …

Transportni servisni zahjevi zajednički za sve aplikacije

Aplikacija	Gubici	Brzina prenosa	Vrem. osjet.
file transfer	bez	elastičan	ne
e-mail	bez	elastičan	ne
Web dokumenti	bez	elastičan	ne
real-time audio/video	tolerantne	audio: 5kb/s-1Mb/s video:10kb/s-5Mb/s	da, 100-tinak ms
stored audio/video	tolerantne	Isti kao gore	da, nekoliko s
Interaktivne igre	tolerantne	nekoliko kb/s i više	da, 100-tinak ms
instant messaging	bez	elastičan	da i ne

"5G trougao"


Enhanced Mobile Broadband
Capacity Enhancement
Qorvo: LTE-A, Pro, Extended Bands, Fixed Wireless mmW, Beam Steering Infrastructure, Efficient FEMs
Gigabytes in a second
3D video - 4K screens
3D
Work & play in the cloud
Smart city cameras
Augmented reality
Voice
Industrial & vehicular automation
Mission critical broadband
Sensor NW
Self driving car
Massive IoT
Massive Connectivity
Qorvo: Ultra Low Power RF Connectivity, ZigBee, Wi-Fi, Cat M, Thread
Low Latency
Ultra-High Reliability & Low Latency
Qorvo: Massive MIMO, Carrier Aggregation, Infrastructure

Servisi transportnih protokola Interneta

TCP servisi:

- *konektivnost:* uspostavljanje komunikacije se zahtijeva između klijentskih i serverskih procesa
- *pouzdani transport* između procesa slanja i prijema
- *kontrola protoka:* pošiljalac ne smije da "zaguši" prijemnik
- *kontrola zagušenja:* usporava pošiljaoca kada je mreža zagušena
- *Ne obezbjeđuje:* tajming, garantovanje minimalnog opsega, zaštitu

UDP servisi:

- Nepouzdani prenos podataka između procesa slanja i prijema
- Ne obezbjeđuje: uspostavljanje veze, pozdanost, kontrolu protoka, kontrolu zagušenju, tajming, garantovani opseg, zaštitu

P: Zašto oba? Zašto UDP?

Internet aplikacije: aplikacija, transportni protokoli

Aplikacija	Protokoli nivoa aplikacije	Transportni protokol
e-mail	SMTP [RFC 2821]	TCP
udaljeni terminal	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
file transfer	FTP [RFC 959]	TCP
streaming multimedia	HTTP (e.g., YouTube), RTP [RFC 1889]	TCP ili UDP
Internet telefonija	SIP, RTP, proprietary (e.g., Skype)	TCP ili UDP

Zaštita i TCP

TCP & UDP

- Nema kriptovanja
- Tekstualne lozinke se prenose preko Interneta

SSL

- Omogućava enkripciju TCP konekcije
- Integritet podataka
- Autorizacija od kraja do kraja

SSL je na nivou aplikacije

- Aplikacije koriste SSL biblioteke, koje "komuniciraju" sa TCP

SSL socket API

- Tekstualna lozinka se šalje kriptovana preko Interneta

Web i HTTP

Termini

- Web stranica se sastoji od objekata
- Objekat može biti HTML fajl, JPEG slika, Java "applet", audio fajl,...
- Web stranica se sastoji od osnovnog HTML-fajla koji sadrži više referenci objekata
- Svaki objekat se adresira sa URL (Uniform Resource Locators)
- Primjer URL:

http://www.cftmn.ac.me/index.html

ime hosta ime puta

Pregled HTTP-a

HTTP: hypertext transfer protokol

- Web-ov protokol nivoa aplikacije
- klijent/server model
  - *klijent:* "browser" koji zahtijeva, prima, prikazuje Web objekte
  - *server:* Web server šalje objekte kao odgovor na zahtjeve

Pregled HTTP-a (nastavak)

Koristi TCP:

- klijent inicijalizuje TCP vezu (kreira socket) prema serveru, port 80
- server prihvata TCP vezu od klijenta
- HTTP poruke zahtjeva i poruke odgovora (poruke protokola nivoa aplikacije) se razmjenjuju između "browser"-a (HTTP klijent) i Web servera (HTTP server)
- TCP veza se zatvara

HTTP je "stateless"

- server ne čuva informacije o prethodnim korisnikovim zahtjevima (ne raspoznaje korisnike)

Pored toga

Protokoli koji nadziru "stanje" su kompleksni!

- Ranije stanje mora biti nadzirano
- ako server/klijent "padne", njihovi uvidi u "stanje" mogu biti inkonzistentni, moraju biti ponovo razmotreni

HTTP konekcije

Neperzistentni (neistrajan) HTTP

- Najviše jedan objekat je poslat preko TCP konekcije.
- Povlačenje više objekata podrazumijeva otvaranje više konekcija

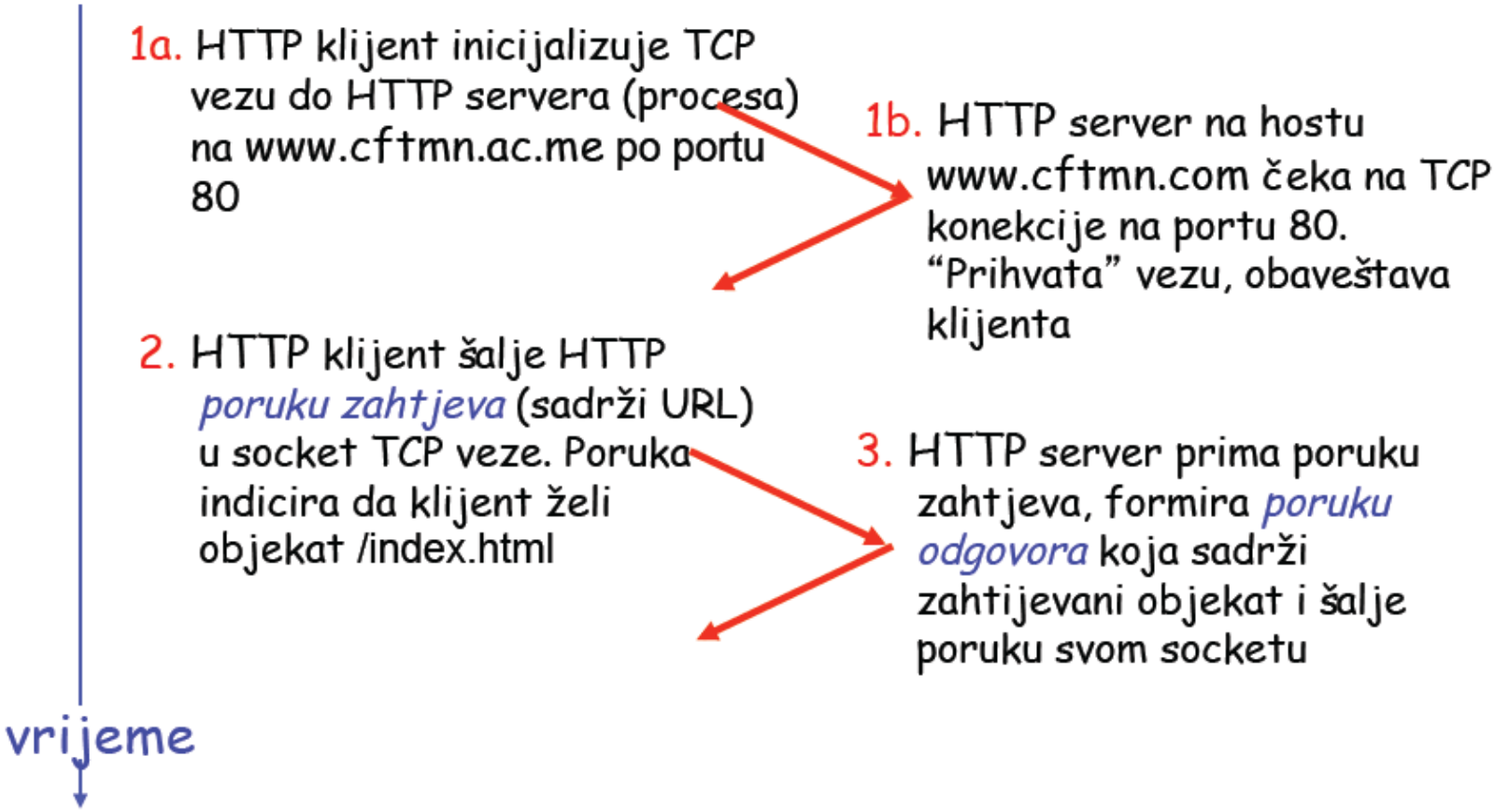
Perzistentni HTTP

- Više objekata može biti poslato preko jedne TCP veze između klijenta i servera.

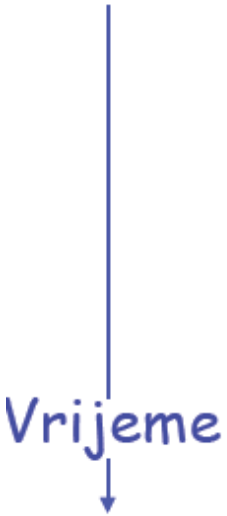
Neperzistentni HTTP

Pretpostavimo da korisnik unese sledeći URL

http://www.cftmn.ac.me/index.html



Neperzistentni HTTP(nastavak)



4. HTTP server zatvara TCP vezu.

5. HTTP klijent prima poruku odgovora koja sadrži html fajl, prikazuje html, tumači html fajl, pronalazi upućene objekte

6. Koraci 1-5 se ponavljaju za svaki objekat

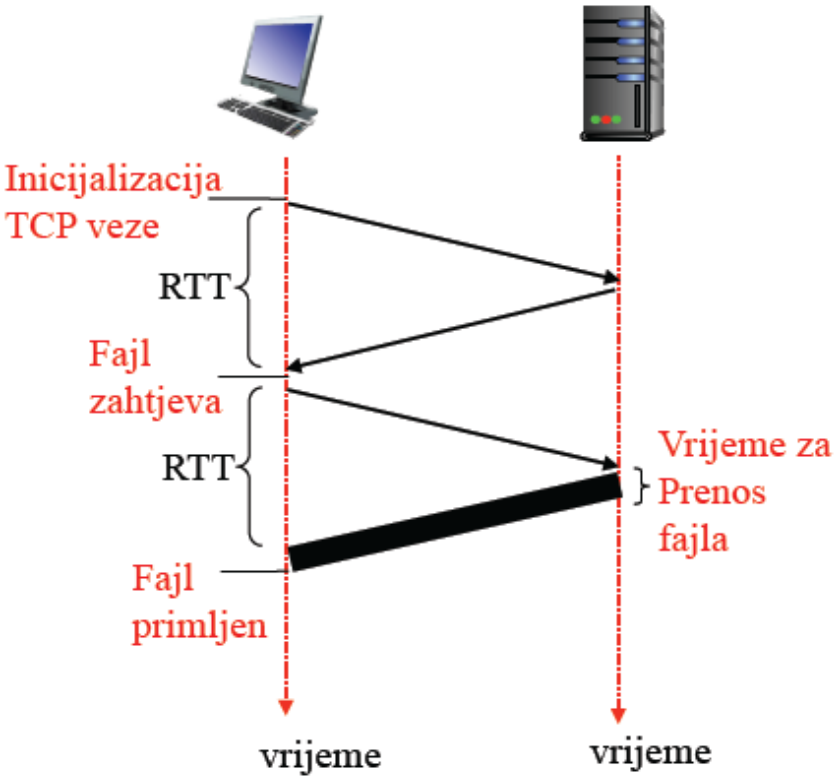
Modelovanje vremena odgovora

Definicija RTT (Round Trip Time): vrijeme prenosa malog paketa od klijenta do servera i nazad.

Vrijeme odgovora:

- jedan RTT za inicijalizaciju TCP veze
- jedan RTT za HTTP zahtjev i vraćanje prvih nekoliko bajtova HTTP odgovora
- Vrijeme prenosa fajla

ukupno = 2RTT+vrijeme prenosa fajla



Persistentni HTTP

Problemi neperzistentnog HTTP-a:

- zahtijeva 2 RTT po objektu
- OS mora raditi i dodijeliti resurse hosta za svaku TCP vezu
- Problem je što browser-i često otvaraju paralelne TCP veze za povlačenje zahtijevanih objekata

Perzistentni HTTP

- server zadržava vezu otvorenu poslije slanja odgovora
- sekvencijalne HTTP poruke između istog klijent/servera se šalju istom vezom
- Zatvara konekciju poslije određenog vremena neaktivnosti

Perzistentni bez "pipelining":

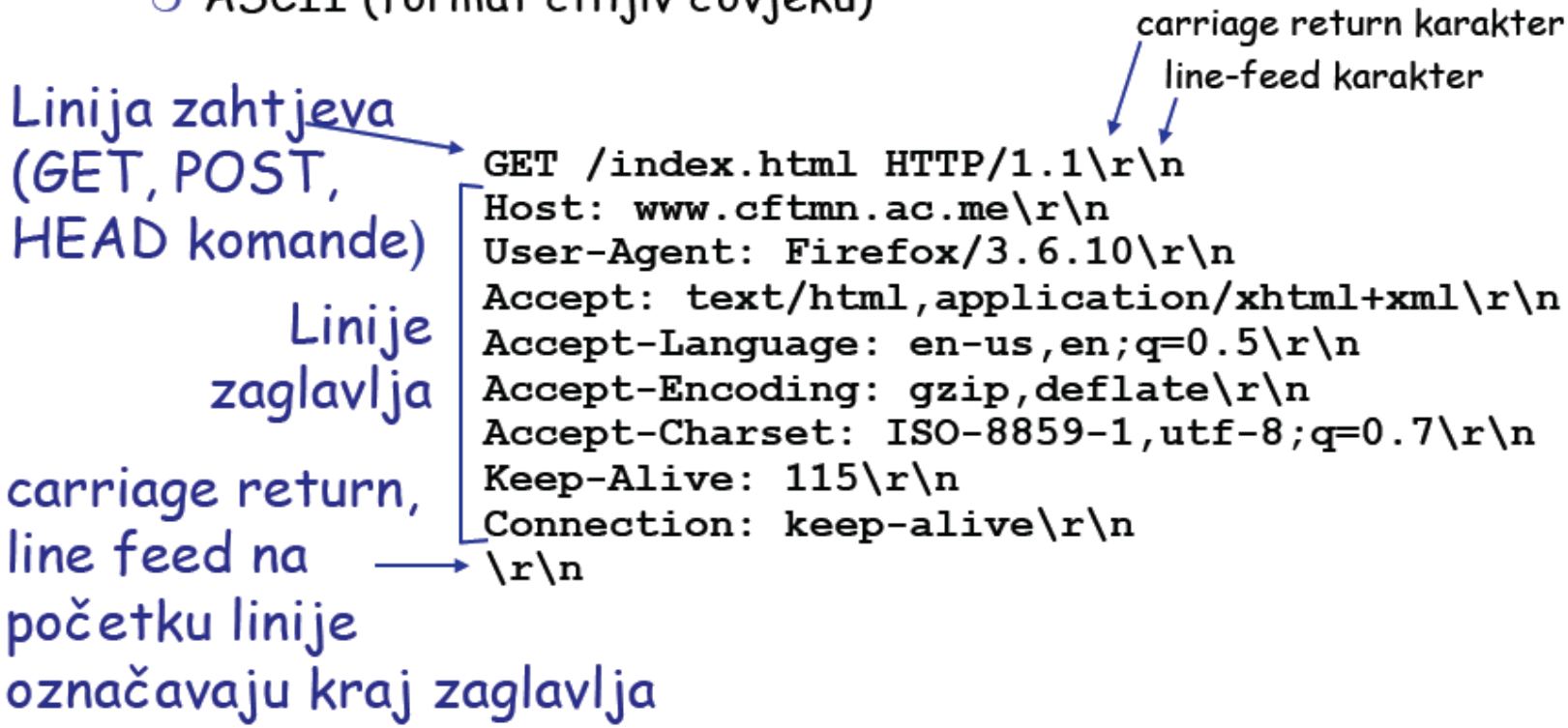
- Klijent šalje novi zahtjev samo kada je prethodni odgovor primljen
- jedan RTT za svaki upućeni objekat
- Kada nema zahtjeva TCP konekcija je slobodna

Perzistentni sa "pipelining":

- klijent šalje zahtjeve odmah po dobijanju referenci objekata
- Veličine svega po jedan RTT za svaki referencirani objekat

HTTP poruka zahtjeva

- Dva tipa HTTP poruka: *zahtjev, odgovor*
- HTTP poruka zahtjeva:
  - ASCII (format čitljiv čovjeku)



Tipovi

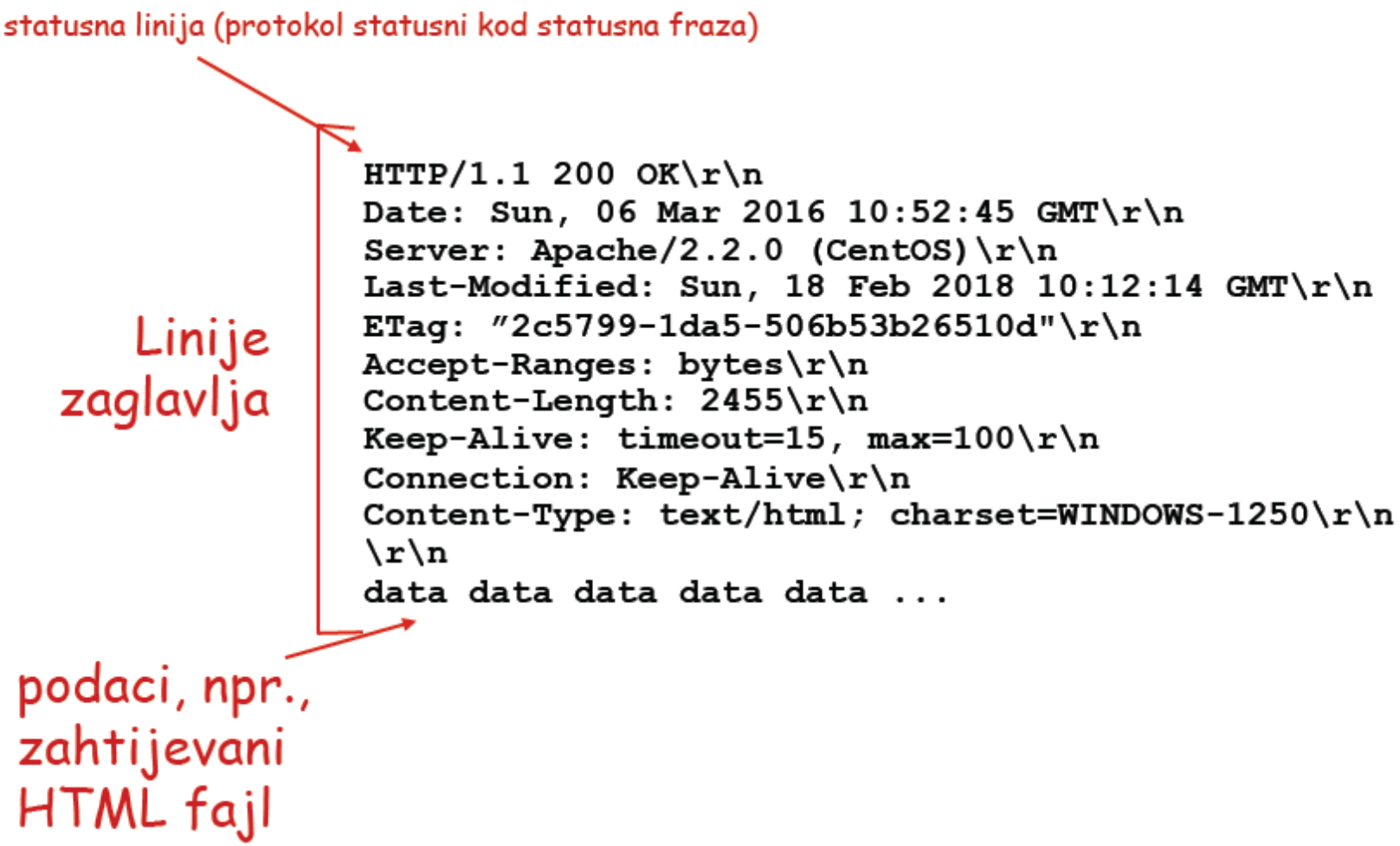
HTTP/1.0

- GET
- POST
- HEAD
  - Pita servera da pusti traženi sadržaj (otklanjanje grešaka)

HTTP/1.1

- GET, POST, HEAD
- PUT
  - Uploaduje fajl na mjesto u Web serveru definisano u URL polju
- DELETE
  - Briše fajl definisan u URL polju

HTTP poruka odgovora



HTTP kodovi statusnog odgovora

U prvoj liniji u server->klijent poruci odgovora.

Nekoliko primjera kodova statusa i odgovarajućih poruka:

200 OK

- Zahtjev uspješan, zahtijevani objekat se nalazi u poruci

301 Moved Permanently

- Zahtijevani objekat preseljen, nova lokacija specificirana u poruci (Lokacija:)

400 Bad Request

- Server ne razumije poruku zahtijeva

404 Not Found

- Zahtijevani dokument nije pronađen na ovom serveru

505 HTTP Version Not Supported

https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

Cookies: vode računa o "stanju"(RFC 6265)

Mnogi Web sajtovi koriste cookies

Četiri komponente:

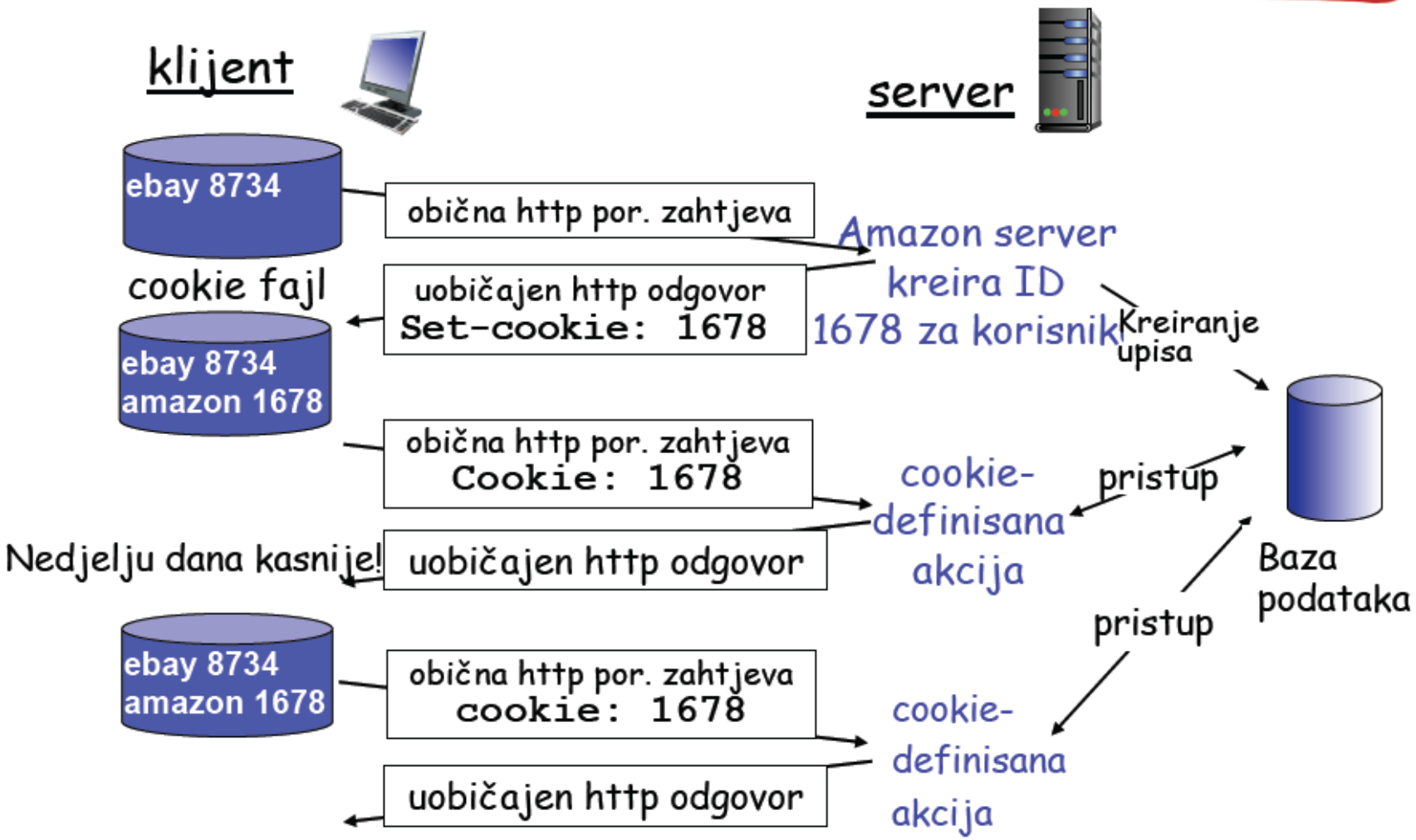
1) Linija zaglavlja Set-cookie u HTTP poruci odgovora
2) Linija zaglavlja Cookie u HTTP poruci zahtjeva
3) Cookie fajl se čuva na korisnikovom hostu i održava se od strane korisnikovog browser-a
4) Baza podataka na Web sajtu

Primjer:

- Neko pristupa Internetu uvijek preko istog PC-a
- Posjećuje specifične e-commerce sajtove po prvi put
- Kada inicijalni HTTP zahtjevi dođu na sajt, sajt kreira jedinstveni ID i kreira odgovarajuću informaciju u bazi podataka za ID

https://tools.ietf.org/html/rfc6265

Cookies: vode računa o "stanju"(nastavak)



Cookies: vode računa o "stanju"(nastavak)

Šta cookies donose:

- autorizaciju
- "shopping cards"
- preporuke
- stanje korisnikove sesije (Web e-mail)

Pored toga

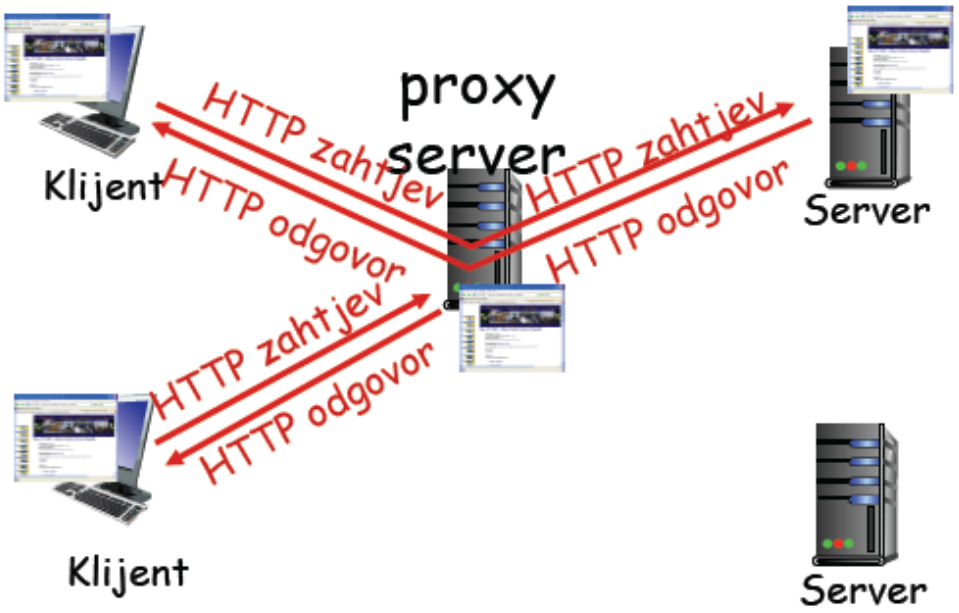
Cookies i privatnost:

- Cookies dozvoljavaju sajtu da dosta nauči o korisniku
- Mogu se dostaviti imena i kontakt podaci
- Pretraživači koriste cookies da nauče više o korisnicima
- Kompanije dobijaju dodatne informacije preko weba

Web "caches" (proxy server)

Cilj: zadovoljenje klijentovog zahtjeva bez uključivanja originalnog servera

- Korisnik setuje browser: Web pristup preko proxy servera
- browser šalje sve HTTP zahtjeve proxy serveru
  - objekat u proxy-u: proxy šalje objekat
  - ili proxy zahtijeva objekat od željenog servera, tada vraća objekat klijentu



https://tools.ietf.org/html/rfc7234

Više o proxy serveru

- Proxy server radi i kao klijent i kao server
- Tipično proxy instalira ISP (univerzitet, kompanija, rezidencijalni ISP)

Zašto proxy server?

- Smanjuje vrijeme odziva na zahtjev.
- Smanjuje saobraćaj na linku institucije prema Internetu.
- Internet sa proxy serverom omogućava "slabim" provajderima sadržaja efikasniju predaju sadržaja

Primjer:

Pretpostavke:

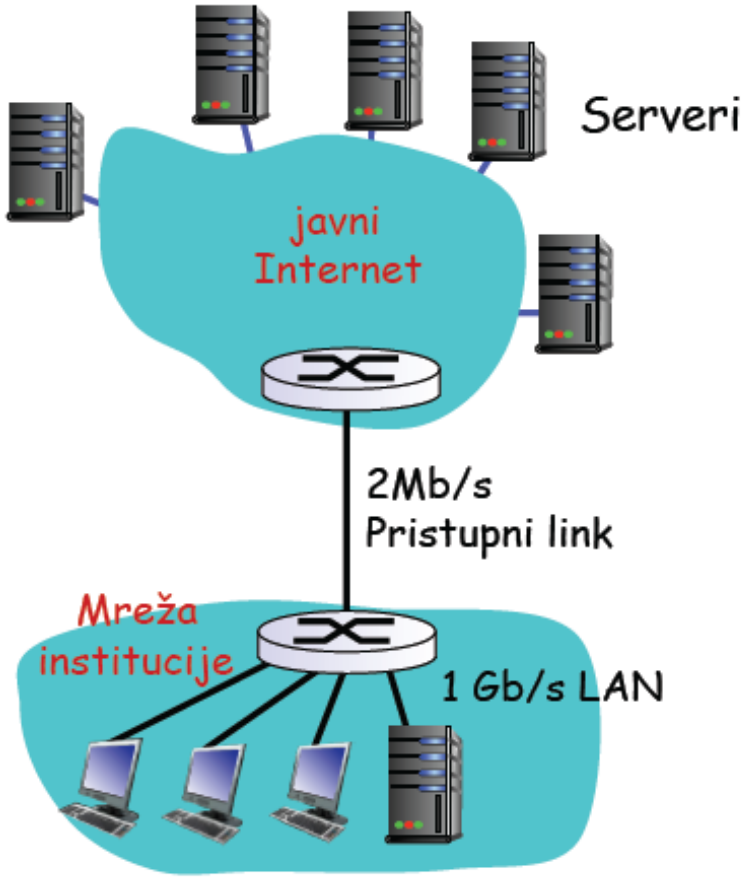
- Srednja veličina objekta: 100000 bita
- Srednji broj zahtjeva prema željenim serverima: 19 zahtjeva/s
- Srednja brzina : 1.9Mb/s
- RTT od rutera institucije do željenog servera: 2s
- Brzina na pristupnom linku: 2Mb/s

Posledice:

problem!

- Iskorišenje LAN-a: 0.19%
- Iskorišenje pristupnog linka = 95%
- Ukupno kašnjenje= kašnjenje na Internetu+ kašnjenje u pristupu+ LAN kašnjenje

  = 2s + minuti + μs



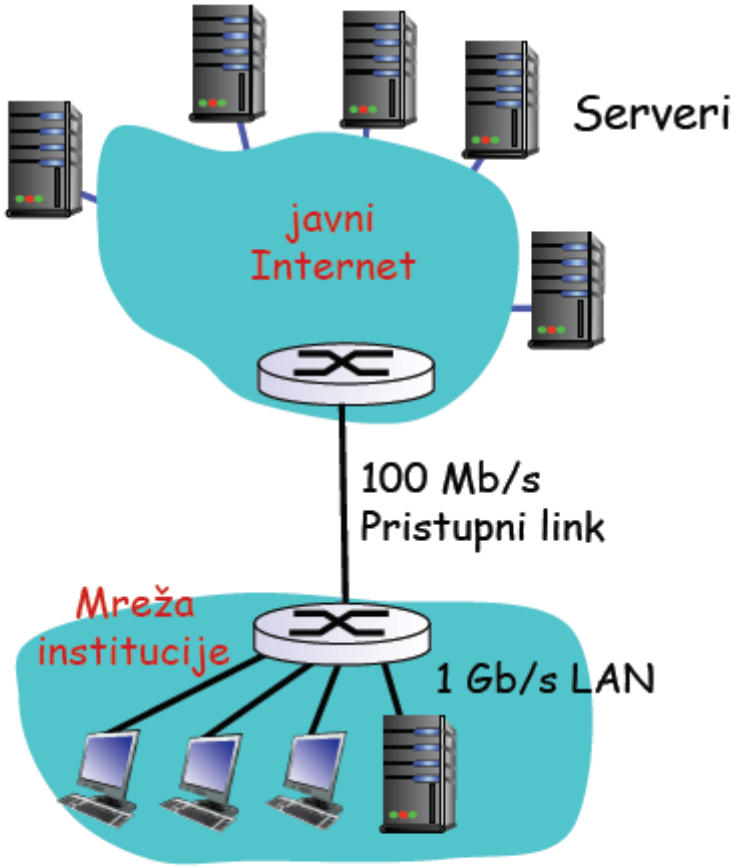
Primjer: brži pristupni link

pretpostavke:

- Srednja veličina objekta: 100000 bit
- Srednji broj zahtjeva: 19 zahtjeva/s
- Srednja brzina: 1.9Mb/s
- RTT od rutera institucije do željenog servera: 2s
- Brzina pritupnog linka: 100Mb/s

posledice:

- Iskorišenje LAN-a: 0.19%
- Iskorišćenje linka= 1.9%
- Ukupno kašnjenje= Internet kašnjenje + pristupno kašnjenje+ LAN kašnjenje
  = 2s + ms + μs



Troškovi: povećanje brzine pristupa je skupo!

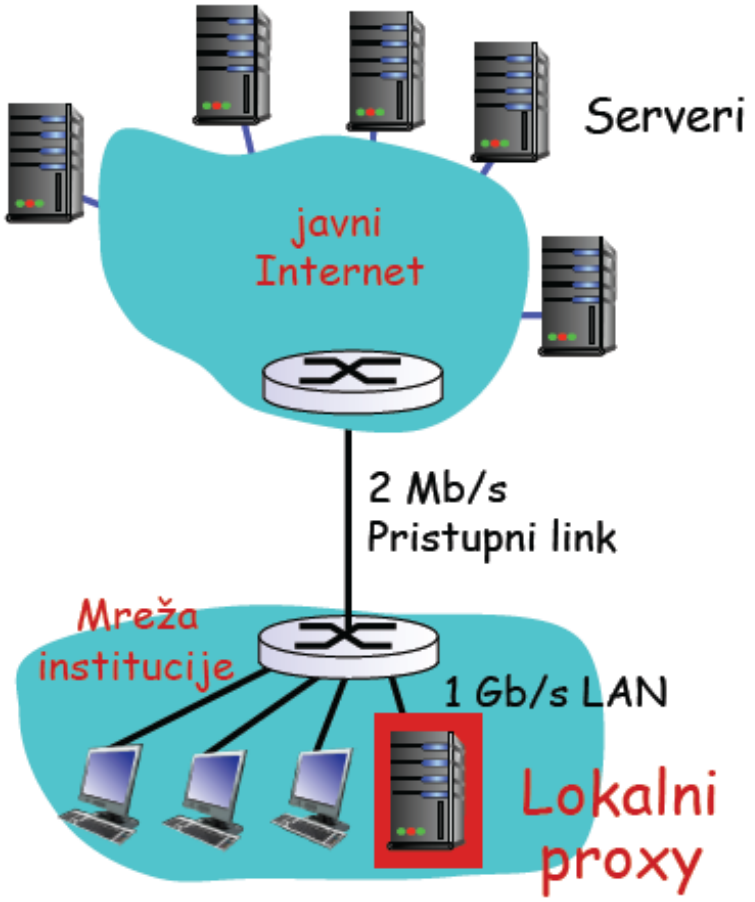
Primjer: Lokalni proxy

pretpostavke:

- Srednja veličina objekta: 100000 bita
- Srednja brzina zahtjeva: 19 zahtjeva/s
- Srednja brzina: 1.9Mb/s
- RTT od rutera institucije do željenog servera: 2s
- Brzina pristupa: 2Mb/s

posledice:

- LAN utilization: 0.19%
- Iskorišćenje pristupnog linka= ?
- Ukupno kašnjenje= ?



Kako izračunati iskorišćenje i kašnjenje?

Troškovi: proxy nije skup!

Primjer: Lokalni proxy

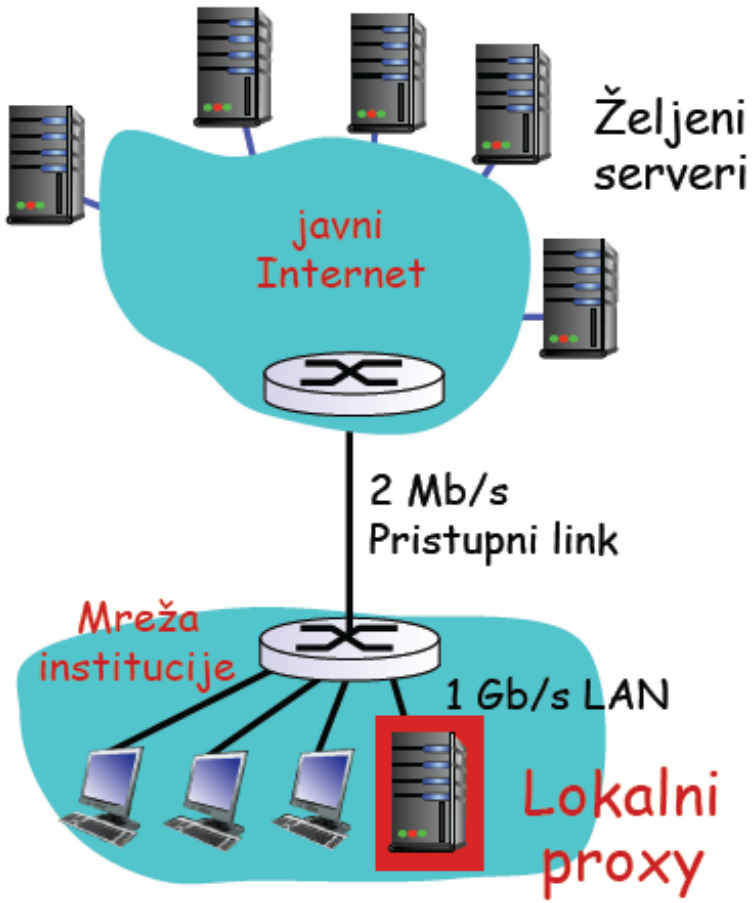
Izračunavanje iskorišćenja i kašnjenja:

- Pretpostavimo da je vjerovatnoća pogađanja 0.4
  - 40% zahtjeva se posluži na proxy serveru, 60% zahtjeva na željenom serveru

Iskorišćenje pristupnog linka:

- 60% zahtjeva koristi pristupni link

- Brzina prenosa preko pristupnog linka= 0.6*1.9Mb/s = 1.14Mb/s
  - iskorišćenje = 1.14/2 = .57
    - Ukupno kašnjenje
      - = 0.6 * (kašnjenje od željenih servera) +0.4 * (kašnjenje do proxy servera)
      - = 0.6 (2.0) + 0.4 (~ms)
      - = ~ 1.2 s
      - Manje nego pristupni link od 100Mb/s

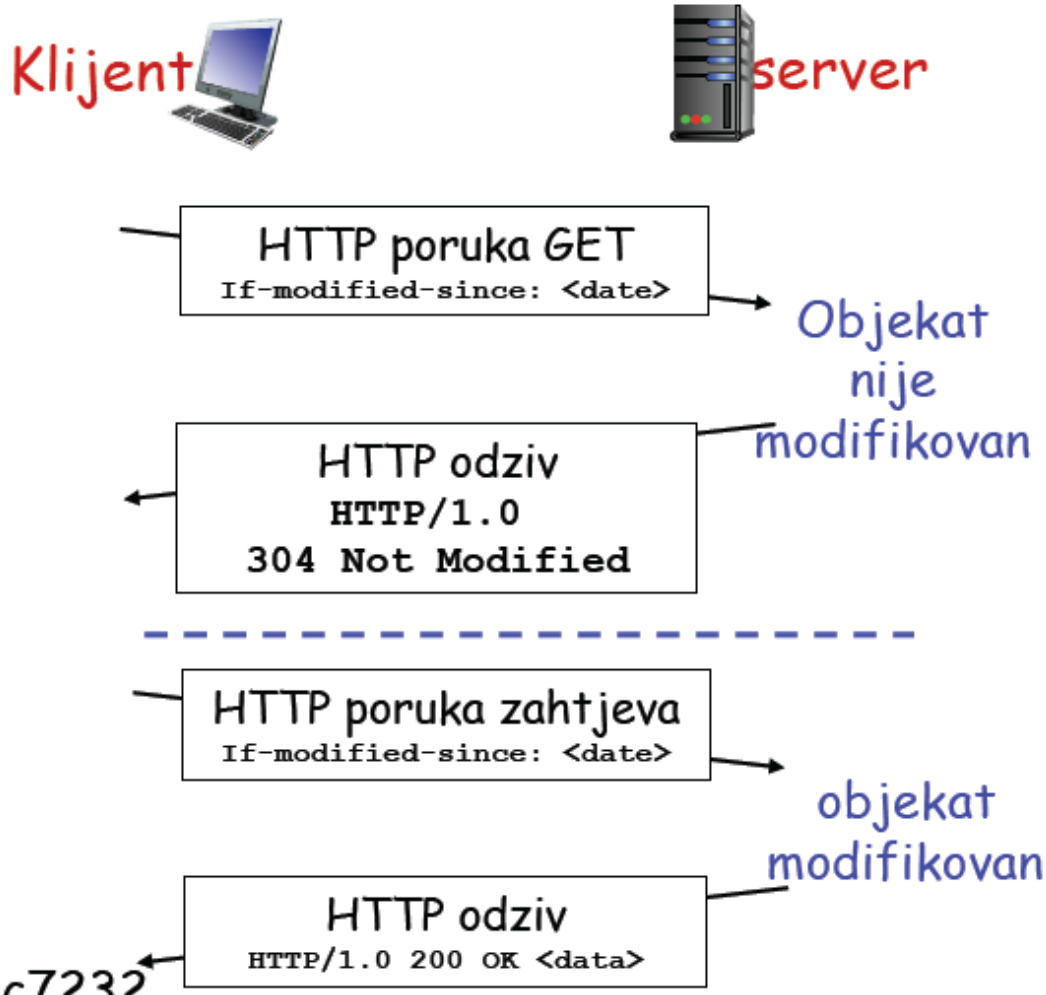


Conditional GET

- Cilj: ne slati objekat ako cache ima up-to-date sačuvanu verziju
- cache: specificira datum čuvanja kopije u HTTP zaglavlju

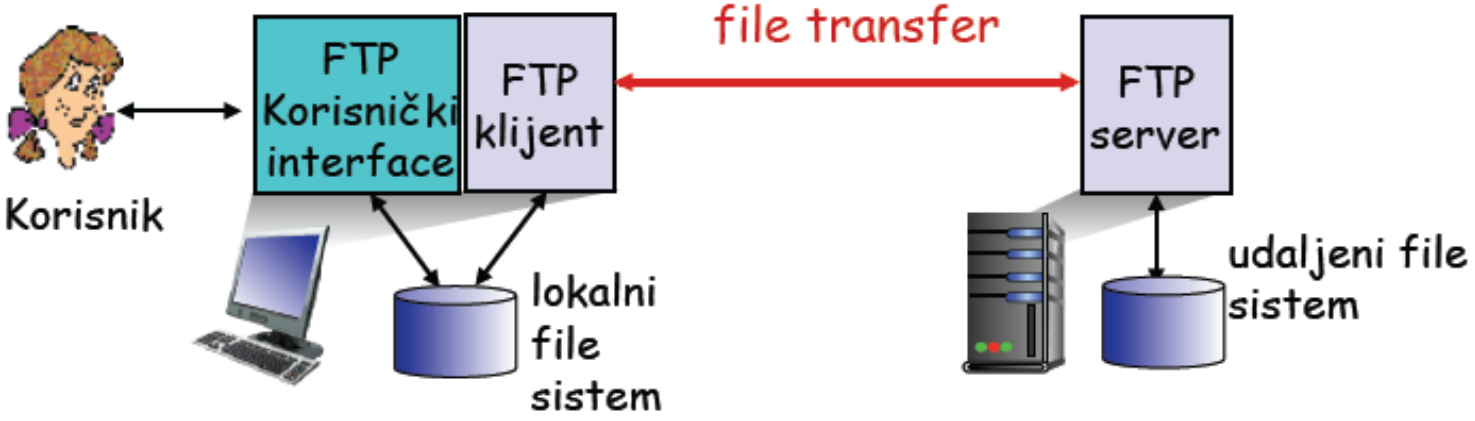
  `If-modified-since: <date>`
- server: odgovor ne sadrži objekat ako je sačuvana kopija up-to-date:

  `HTTP/1.0 304 Not Modified`



https://tools.ietf.org/html/rfc7232

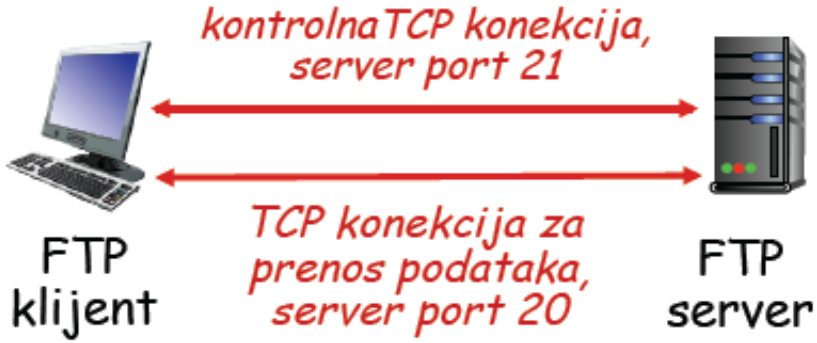
FTP: the file transfer protocol



- transfer fajla od/do udaljenog hosta
- klijent/server model
  - *klijent:* strana koja inicijalizuje prenos (ili od/do udaljenog hosta)
  - *server:* udaljeni host
- ftp: RFC 959
- ftp server: port 21

FTP: kontrolna veza i veze za prenos podataka

- FTP klijent kontaktira FTP server na port 21, definišući TCP kao transportni protokol
- Klijent dobija autorizaciju preko kontrolne veze
- Klijent pregleda udaljene direktorijume slanjem komandi preko kontrolne veze.
- Kada server primi komandu za prenos fajla, server otvara TCP vezu za prenos podataka do klijenta (port 20)
- Poslije slanja jednog fajla server zatvara vezu.



- Server otvara drugu TCP vezu podataka za prenos drugog fajla.
- Kontrola veze: "out of band", kao kod RTSP.
- FTP server nadzire "state": trenutni direktorijum, ranija identifikacija. "statefull"

FTP komande, odgovori

Primjeri komandi:

- Šalje kao 7 bitni ASCII tekst preko kontrolnog kanala, identično kao HTTP.
- `USER` *`ime`*
- `PASS` *`lozinka`*
- `LIST` vraća spisak fajlova u direktorijumu
- `RETR` *`imefajla`* povlači fajl
- `STOR` *`imefajla`* smješta fajl na udaljeni host

Primjer kodova odgovora

- status kodovi i fraze (kao u HTTP)
- `331 Username OK, password required`
- `125 data connection already open; transfer starting`
- `425 Can't open data connection`
- `452 Error writing file`

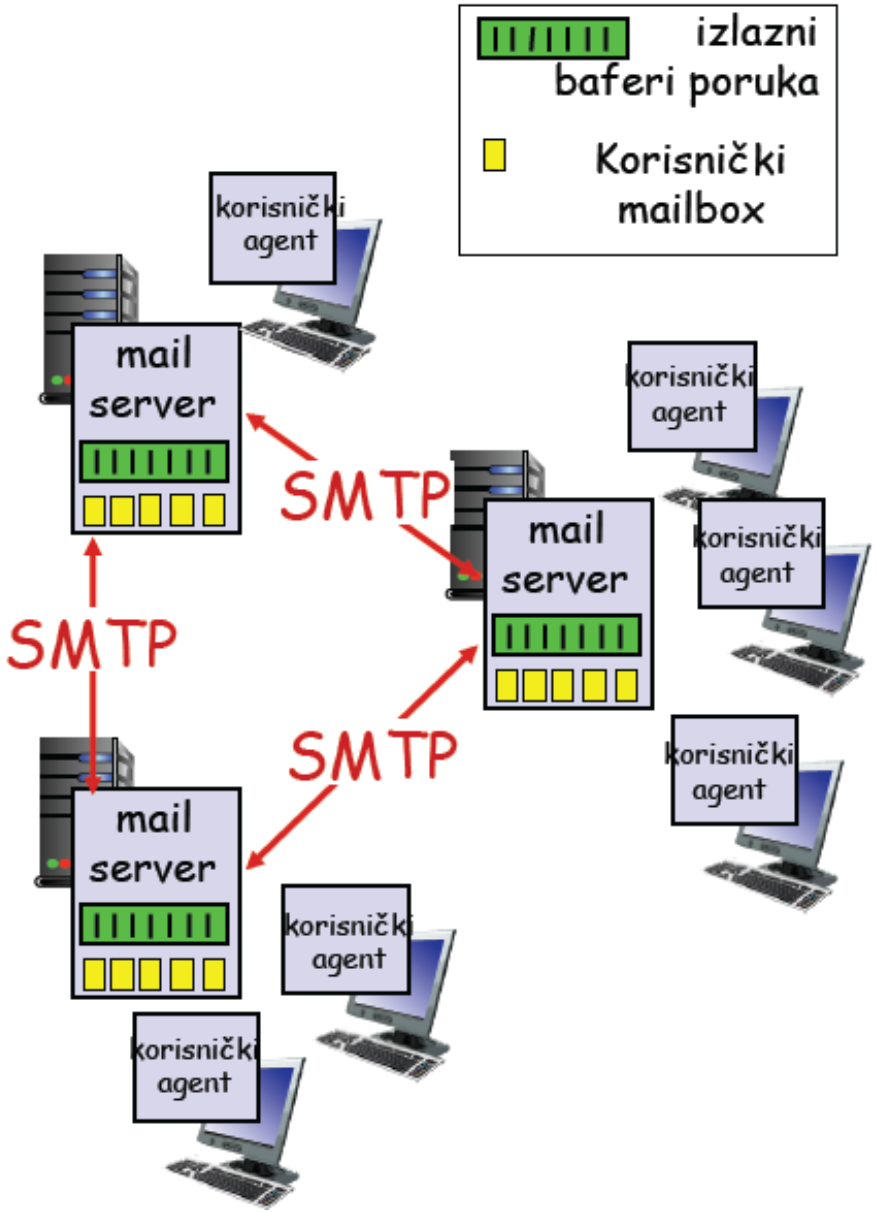
Elektronska Pošta

Tri glavne komponente:

- korisnički agenti
- mail serveri
- SMTP (Simple Mail Transfer Protocol)

Korisnički Agent

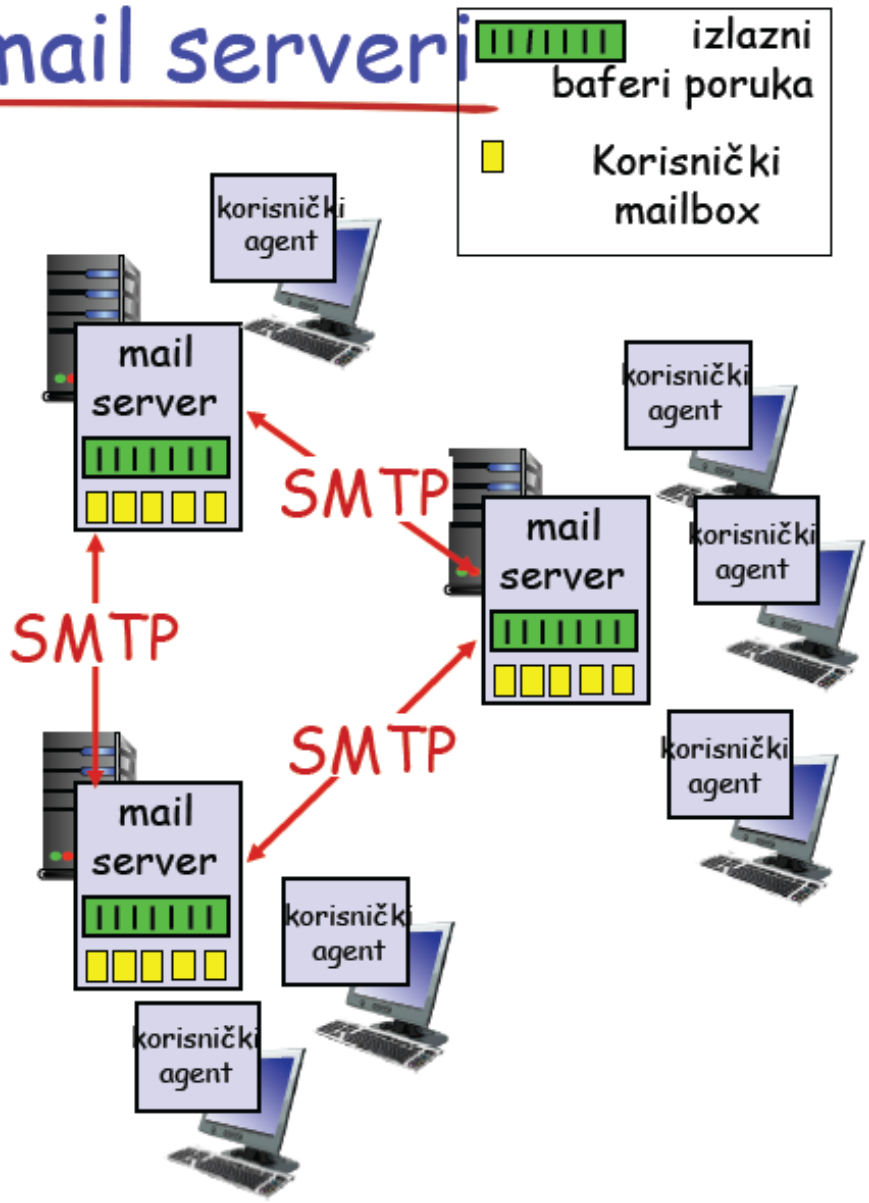
- "mail reader"
- sastavljanje, editovanje, čitanje mail poruka
- Eudora, Thunderbird, iPhone mail client
- odlazne, dolazne poruke se čuvaju na hostu



Elektronska Pošta: mail serveri

Mail Serveri

- Mailbox sadrži dolazne poruke korisnika
- Red čekanja odlaznih poruka koje trebaju da se pošalju
- SMTP protokol između mail servera za slanje email poruka
  - klijent: slanje mail serveru
  - "server": prijem sa mail servera

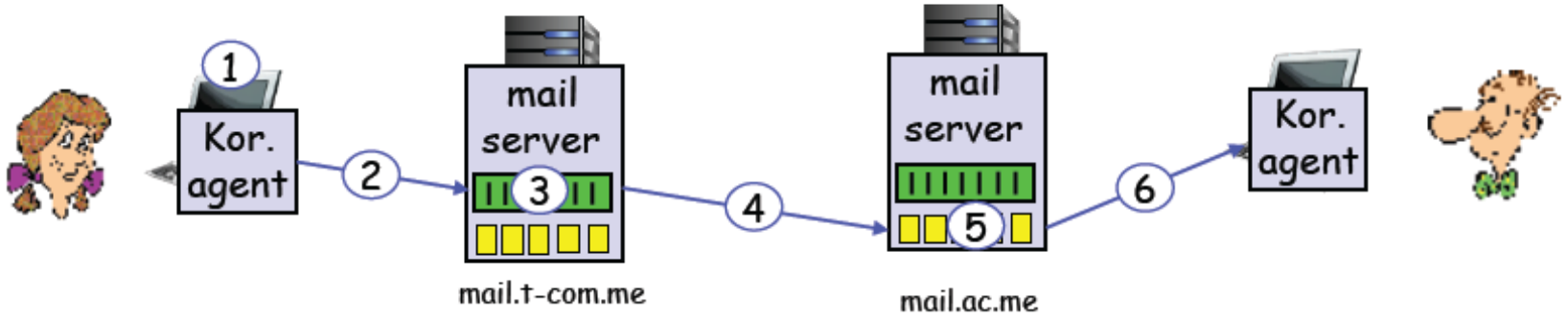


Elektronska Pošta: SMTP [RFC 5321]

- koristi TCP za pouzdani transfer email poruke od klijenta do servera po portu 25
- direktan transfer: od servera pošiljaoca do servera primaoca
- Tri faze transfera
  - handshaking (upoznavanje)
  - prenos poruke
  - zatvaranje
- komanda/odgovor interakcije
  - komande: ASCII tekst
  - odgovor: status kod ili fraza
- Poruke moraju u kompletu biti 7-bitne ASCII.

Scenario slanja poruke

1) Korisnik A koristi korisnički agent da sastavi poruku i adresira je na `korisnikb@ac.me`
2) Korisnički agent korisnika A šalje poruku njenom mail serveru; poruka se smješta u red čekanja
3) Klijentska strana SMTP otvara TCP vezu sa mail serverom korisnika B
4) SMTP klijent šalje poruku poruku Korisnika A preko TCP veze
5) Mail server korisnika B prima poruku i SMTP-ov serverski dio smješta poruku u mailbox Korisnika B
6) Korisnik B aktivira svoj korisnički agent da pročita poruku



Primjer SMTP interakcije

```
S: 220 mail.ac.me
C: HELO mail.t-com.me
S: 250  Hello mail.t-com.me, pleased to meet you
C: MAIL FROM: <korisnika@mail.t-com.com>
S: 250 korisnika@mail.t-com.me... Sender ok
C: RCPT TO: <korisnikb@ac.me>
S: 250 korisnikb@ac.me ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C:   How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 ac.me closing connection
```

SMTP: kraj

- SMTP koristi perzistentne konekcije
- SMTP zahtijeva poruke u 7-bit ASCII formatu
- SMTP server koristi `CRLF.CRLF` da odredi kraj poruke

Upoređenje sa HTTP:

- HTTP: "pull"
- SMTP: "push"
- Oba imaju ASCII komande/ odgovore, kodove statusa, ali se razlikuju po tijelima poruke.
- HTTP: svaki objekat se smješta u sopstvenoj poruci odgovora
- SMTP: više objekata se šalje u višedjelnoj (multipart) poruci

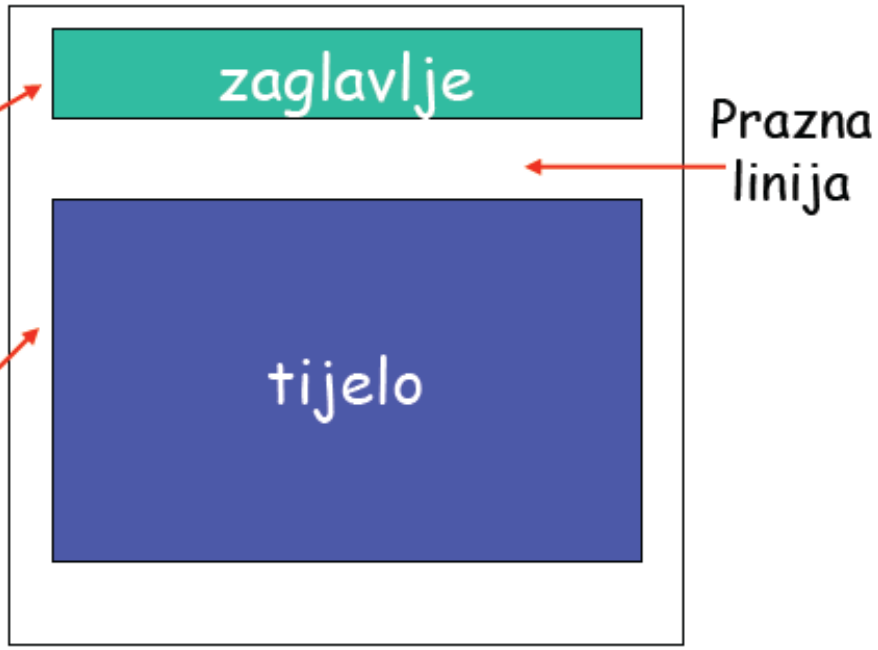
Format mail poruke (RFC 5322)

SMTP: protokol za razmjenu email poruka

RFC 5322: standard za format tekstualnih poruka

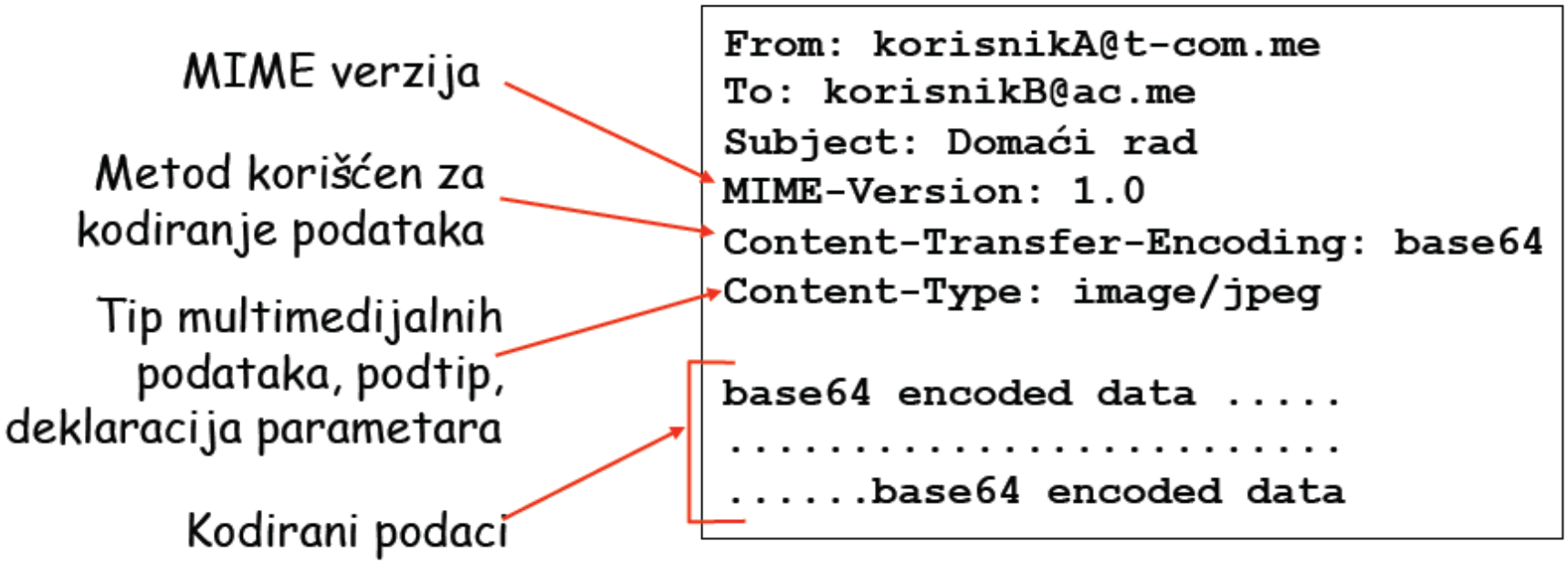
- Zaglavlja linija, npr.,
  - To:
  - From:
  - Subject:

  Različito od SMTP komandi SMTP MAIL FROM, RCPT TO: !
- tijelo
  - poruka, samo ASCII karakteri



Format poruke: multimedija

- MIME: multimedia mail extension, RFC 2045, 2046, 2047, 2048, 2049
- Dodatne linije u zaglavlju poruke deklarišu tip MIME sadržaja



MIME tipovi

Tip sadržaja: tip/podtip; parametri

Tekst

- Primjeri podtipova: `plain`, `html`

Slike

- Primjeri podtipova : `jpeg`, `gif`

Audio

- Primjeri podtipova : `basic` (8-bit mu-law kodiranje), `32kadpcm` (32 kb/s kodiranje)

Video

- Primjeri podtipova : `mpeg`, `quicktime`

Aplikacije

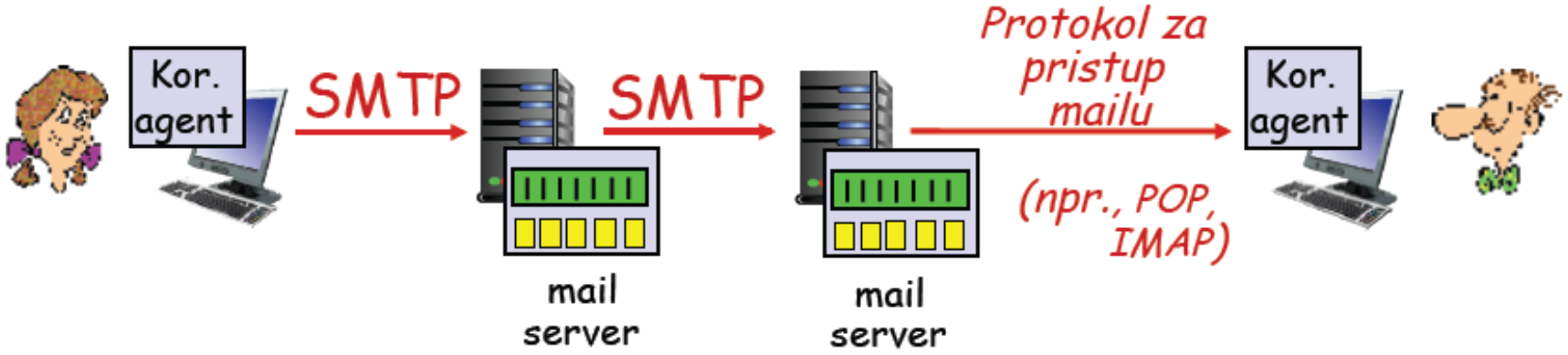
- Drugi podaci koji moraju biti obrađeni odgovarajućim programom prije "gledanja"
- Primjeri podtipova : `msword`, `octet-stream`

Višedjelni tip

```
From: korisnikA@t-com.me
To: korisnikB@ac.me
Subject: Picture
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=StartOfNextPart

--StartOfNextPart
Dear Bob, Please find a picture of me.
--StartOfNextPart
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
base64 encoded data .....
.........................
......base64 encoded data
--StartOfNextPart
Do you want the recipe?
```

Protokoli Mail pristupa



- SMTP: predaja/smještanje na serveru primaoca
- Protokol mail pristupa: povlačenja sa servera
  - POP: Post Office Protocol [RFC 1939]
    - autorizacija (agent <-->server) i povlačenje sadržaja
    - Port 110
  - IMAP: Internet Mail Access Protocol [RFC 3501]
    - Više funkcija (složeniji)
    - Port 143
    - Manipulacija sačuvanim porukama na serveru
  - HTTP: Hotmail , Yahoo! Mail, itd.

DNS: Domain Name System

Ljudi: imaju mnogo dokumenata za identifikaciju:
- ime, broj pasoša,...

Internet hostovi, ruteri:
- IP adresa (32 bit) – koristi se za adresiranje datagrama
- "ime", npr., mail.ac.me – koriste ga ljudi

P: Kako mapirati IP adrese i imena?

Domain Name System:
- *Distribuirana baza podataka* implementirana kao hijerarhija velikog broja *servera imena*
- *Protokol nivoa aplikacije* host, ruteri, serveri imena komuniciraju za *utvrđivanje* imena (adresa/ime translacija)
  - napomena: ključna Internet funkcija, implementirana kao protokol nivoa aplikacije
  - Kompleksnost na "ivici" mreže
- Port 53,
- UDP,
- RFC 1034 i 1035.

DNS

Zašto ne centralizovani DNS?

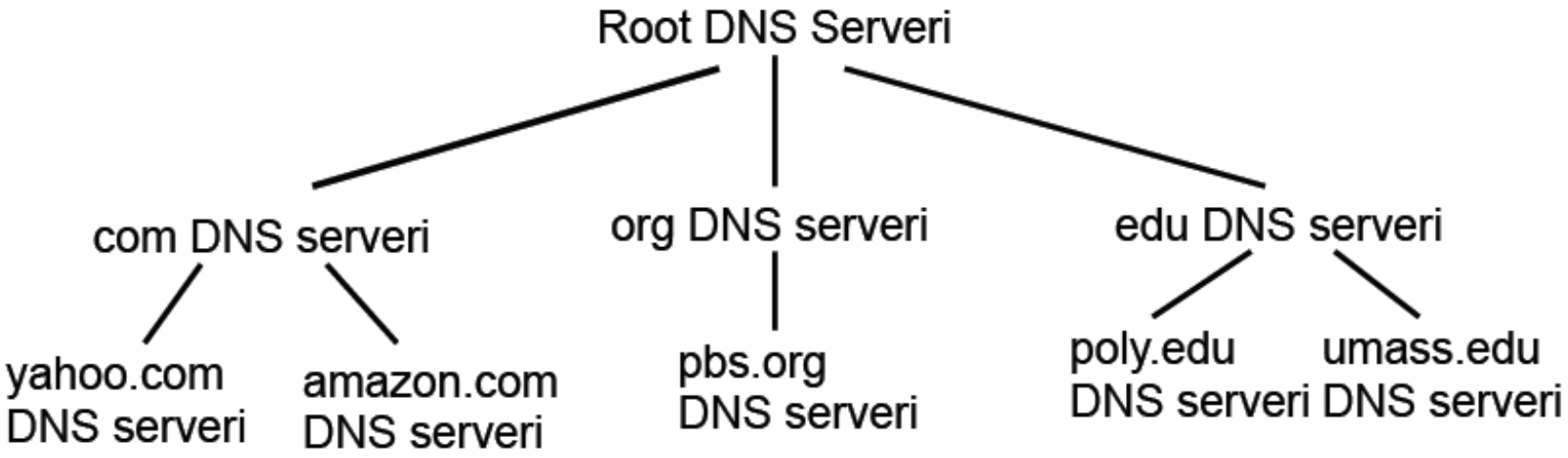
- Jedna tačka otkaza
- Obim saobraćaja
- Centralizovana baza podataka
- Nadzor

Ne odgovara!

DNS servisi

- Translacija imena hosta u IP adresu
- Host "aliasing"
  - Kanonska (www.yahoo.akadns.com) i alias imena (www.yahoo.com)
- Mail server "aliasing" "mail.ac.me" u "ac.me"
- Distribucija opterećenja
  - Replikacija Web servera: setovanje IP adresa za jedno kanoničko ime

Distribuirana i hijerarhijska baza podataka



Klijent želi IP adresu za "www.amazon.com" prva aproksimacija:

- Klijent pita root server da nađe com DNS server
- Klijent pita jedan od com DNS servera da nađe amazon.com DNS server
- Klijent pita amazon.com DNS server da mu pošalje IP adresu www.amazon.com

DNS: "Root" serveri imena

- Kontaktiraju ih lokalni serveri imena kada ne mogu da pronađu ime
- root server imena:
  - kontaktira autoritativni server imena ako mapiranje nije poznato
  - dobija mapiranje
  - vraća mapiranje lokalnom serveru imena

postoji 13 svetskih "root" servera imena!

www.root-servers.org

DNS: "Root" serveri imena

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

DNS: "Root" serveri imena

Zašto postoji samo 13 adresa DNS root servera?

Uobičajena zabluda je da na svijetu postoji samo 13 root servera. U stvarnosti postoji mnogo više, ali i dalje je samo 13 IP adresa koje se koriste za root servere.
Ograničenja u originalnoj arhitekturi DNS-a zahtijevaju da u osnovnoj zoni postoji najviše 13 adresa servera. U ranim danima Interneta, postojao je samo jedan server za svaku od 13 IP adresa, od kojih se većina nalazila u Sjedinjenim Državama.

Danas svaka od 13 IP adresa ima više servera, koji koriste Anycast rutiranje za distribuciju zahtjeva na osnovu opterećenja i blizine. Trenutno postoji preko 600 različitih DNS root servera raspoređenih na svakom naseljenom kontinentu na zemlji.

DNS: "Root" serveri imena

Ko upravlja DNS root serverima?

Internet korporacija za dodijeljena imena i brojeve (ICANN - Internet Corporation for Assigned Names and Numbers) upravlja serverima za jednu od 13 IP adresa u osnovnoj zoni i delegira rad sa ostalih 12 IP adresa raznim organizacijama uključujući NASA, Univerzitet Maryland, zatim Verisign, koji je jedina organizacija koja upravlja dvijema od osnovnih IP adresa.

TLD DNS serveri

- TLD server održava informacije za sva imena domena koja dijele zajedničku ekstenziju domena, kao što su .com, .net ili šta god dolazi posle poslednje tačke u URL-u.
- Na primjer, .com TLD server imena sadrži informacije za svaku web lokaciju koja se završava na „.com".
- Ako je korisnik tražio google.com, nakon što je primio odgovor od root servera, rekurzivni resolver bi zatim poslao upit .com TLD serveru, koji bi odgovorio tako što bi ukazao na autoritativni server imena za taj domen.

TLD DNS serveri

- Upravljanje TLD serverima imena obavlja Internet Assigned Numbers Authority (IANA), koja je ogranak ICANN-a. IANA dijeli TLD servere u dvije glavne grupe:
- Generički TLD domeni: Ovo su domeni koji nisu specifični za zemlju, a neki od najpoznatijih generičkih TLD-ova uključuju .com, .org, .net, .edu i .gov.
- ccTLD domeni koda zemlje (country code TLD): Ovo uključuje sve domene koji su specifični za zemlju ili državu. Primjeri uključuju .uk, .us, .ru i .jp.

TLD DNS serveri

- Top-level domain (TLD) serveri: odgovorni za com, org, net, edu, etc, i sve "top-level" domene zemalja uk, fr, ca, jp,me.
  - "VeriSign" nadzire servere za com TLD
  - "Educause" za edu TLD

Mexico	.mx
Micronesia (officially: Federated States of Micronesia)	.fm
Moldova	.md
Monaco	.mc
Mongolia	.mn
Montenegro	.me
Montserrat	.ms
Morocco	.ma (stands for Maroc)
Mozambique	.mz
Myanmar	.mm
Namibia	.na

Autoritativni DNS serveri

- Autoritativni DNS serveri: DNS serveri organizacije obezbjeđuju mapiranja imena hostova u IP adrese za servere organizacije (npr., Web i mail).
  - Može biti nadziran od strane organizacije ili servis provajdera

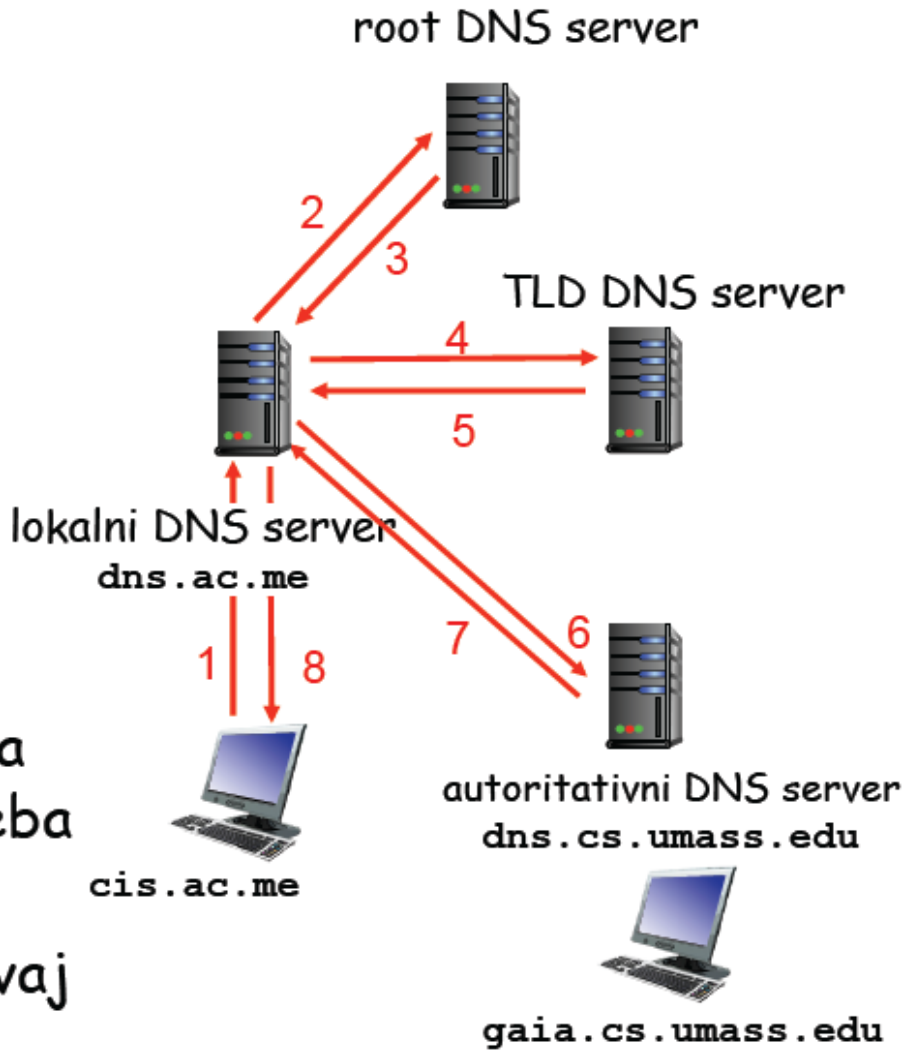
- Autoritativni server je obično poslednji korak na putu za IP adresu. Sadrži informacije specifične za ime domena koji opslužuje (npr. google.com).

Lokalni DNS

- Striktno ne pripada hijerarhiji
- Svaki ISP (rezidencijalni ISP, kompanijski, univerzitet) ima jedan.
  - Još se zove "default DNS"
- Kada host napravi DNS upit, upit se šalje na njegov lokalni DNS server
  - Ponaša se kao DNS proxy, prosleđuje upite u hijerarhiju.

Primjer 1

- Host cis.ac.me želi IP adresu za gaia.cs.umass.edu



Iterativni upit:

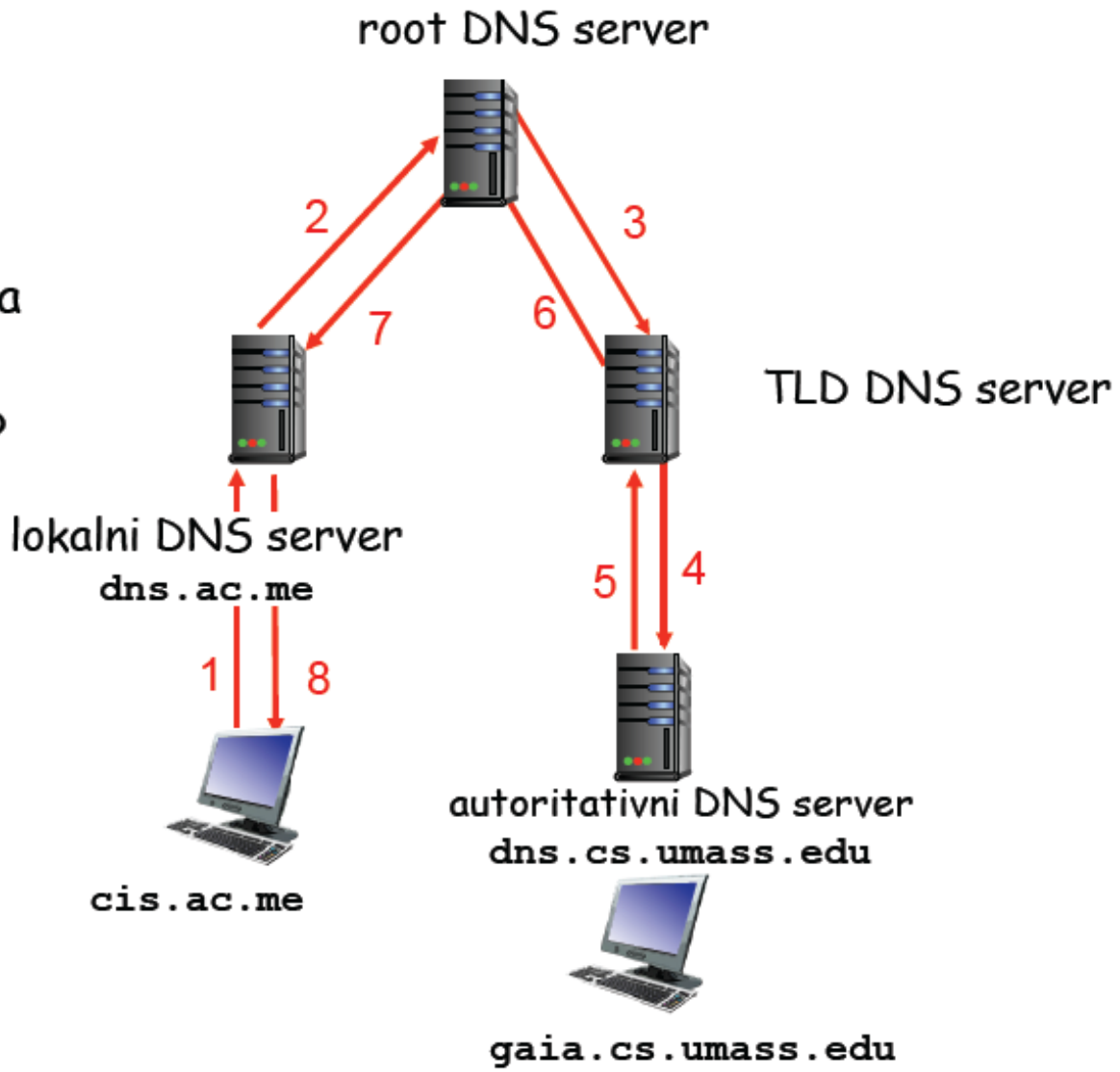
Kontaktirani server odgovara sa imenom servera kojeg treba kontaktirati

"Neznam ovo ime, ali pitaj ovaj server"

Primjer 2

Rekurzivni upit:

- Stavlja problem utvrđivanja imena na kontaktirani DNS
- Veliko opterećenje?



DNS: "caching" i "updating"

- Kada server imena definiše mapiranje on ga *čuva:*
  - Pri čemu se sačuvani podaci posle izvjesnog timeout perioda brišu
  - TLD serveri su tipično sačuvani u lokalnim DNS-ovima
    - Na taj način se root name serveri rijetko posjećuju
- "update/notify" mehanizmi su definisani od IETF
  - RFC 2136

DNS zapisi

DNS:
distribuirana baza podataka koja sadrži zapise resursa (resource records (RR))

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

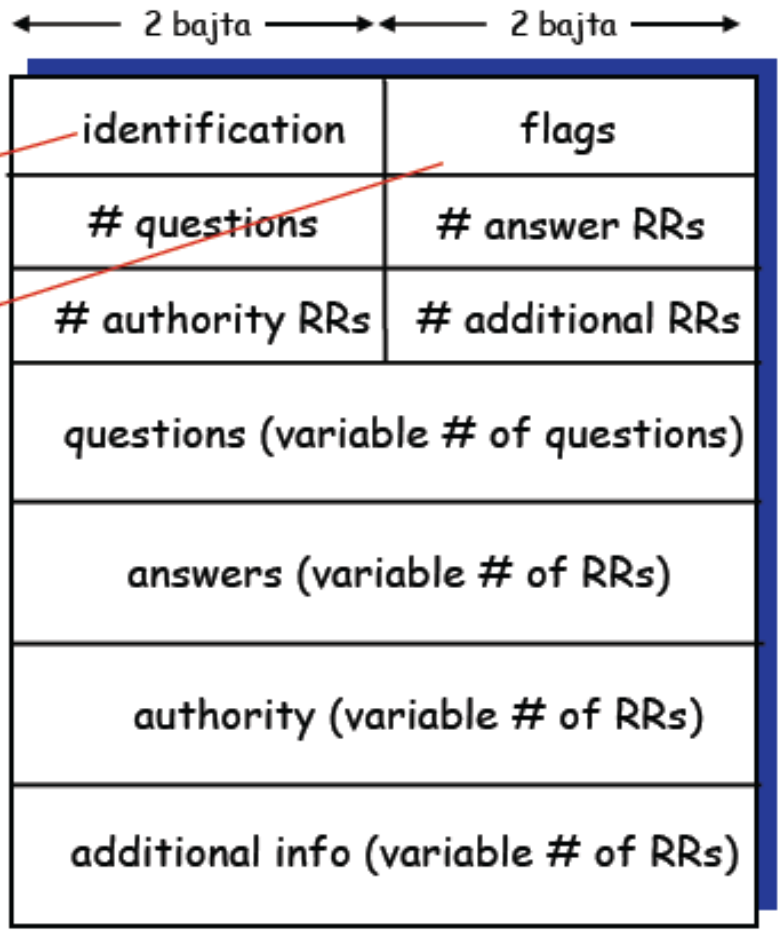
- Type=A
  - name je ime hosta
  - value je IP adresa
- Type=NS
  - name je domen
  - value je IP adresa autoritativnog name servera za ovaj domen
- Type=CNAME
  - name je alias ime nekog "kanoničkog" (stvarnog) imena
  - value je kanoničko ime
  - www.ibm.com je u stvari e2874.x.akamaiedge.net
- Type=MX
  - value je kanonično ime mail servera čiji je name **alias** ime.

DNS protokol, poruke

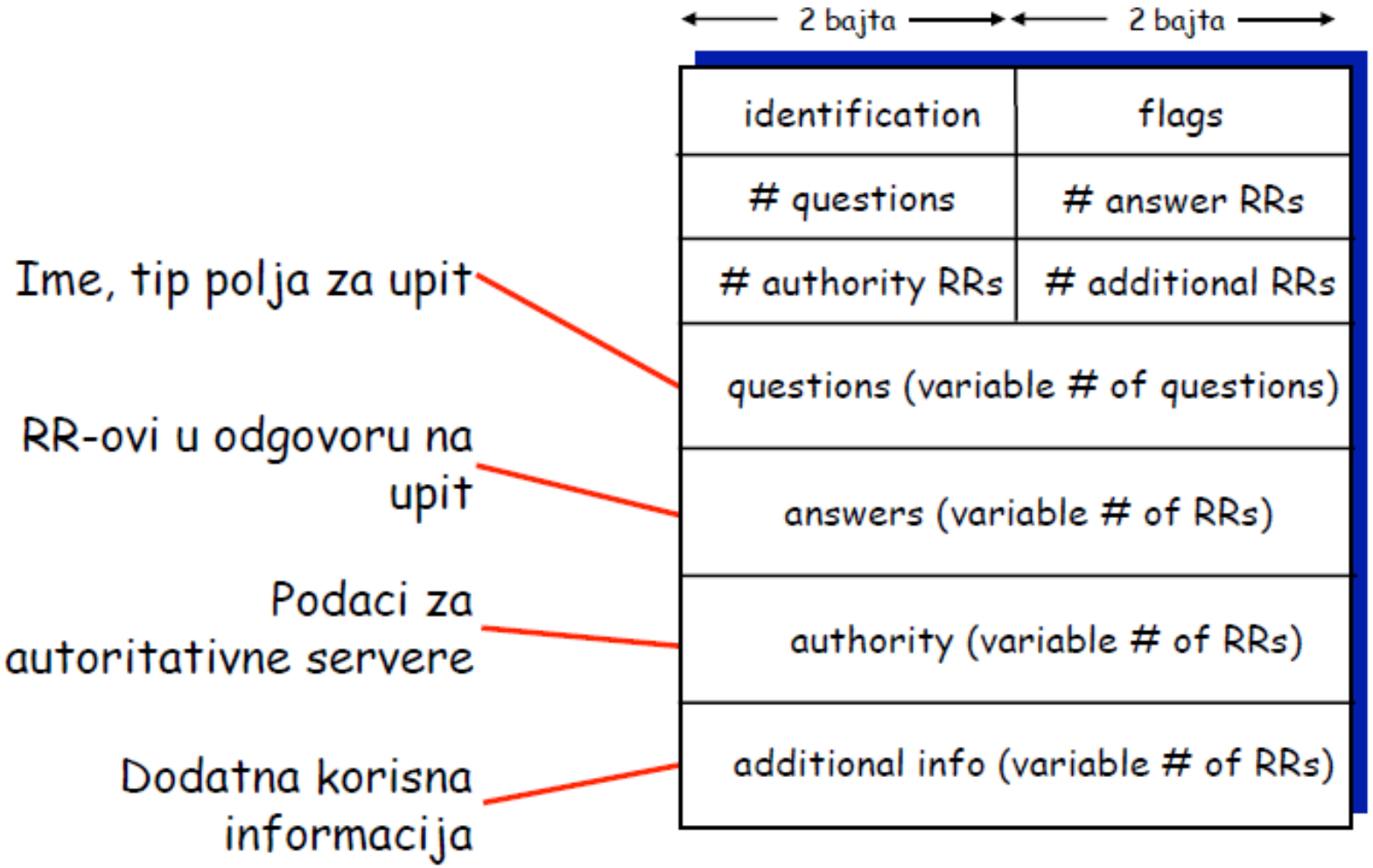
Upiti i *odgovori*, imaju isti format

Zaglavlje poruke

- identifikacija: 16 bitni broj za upit, odgovor na upit koristi isti broj
- oznake:
  - Upit ili odgovor
  - Poželjne rekurzije
  - Dostupne rekurzije
  - Odgovor (broj pojavljivanja tipova)



DNS protokol, poruke



Ubacivanje zapisa u DNS

- Primjer: osnovan je novi start up "Network Utopia"
- Registracija imena networkuptopia.com u registar (VeriSign)
  - Potrebno je dostaviti registru imena i IP adrese autoritativnog name server (primarnog i sekundarnog)
  - Registar ubacuje dva RR u sve com TLD servere:

```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- Postavlja u autoritativni server Type NS zapis za www.networkutopia.com i Type A zapis za dns1.networkutopia.com
- Kako ljudi mogu saznati IP adresu nekog Web sajta?

Kako poslati DNS poruku upita direktno DNS serveru?

- nslookup komanda sa MSDOS comand prompta
- Pomoću odgovarajućih sajtova

Napadi na DNS

DDoS napadi

- Bombardovanje root servera prekomjernim saobraćajem
  - Neuspješan do sada
  - Filtriranje saobraćaja
  - Lokalni DNS serveri keširaju IP adrese TLD servera, što obezbjeđuje zaobilaženje root servera
- Bombardovanje TLD servera
  - Mnogo opasnije!

Indirektni napadi

- Man-in-middle
  - Presrijetanje upita
- DNS "poisoning"
  - Slanje pogrešnih odgovora povezanih sa DNS serverom, koji se keširaju

Korišćenje DNS za DDoS

- Slanje upita sa ukradenih IP adresa: cilj je IP
- Zahtijeva potvrdu

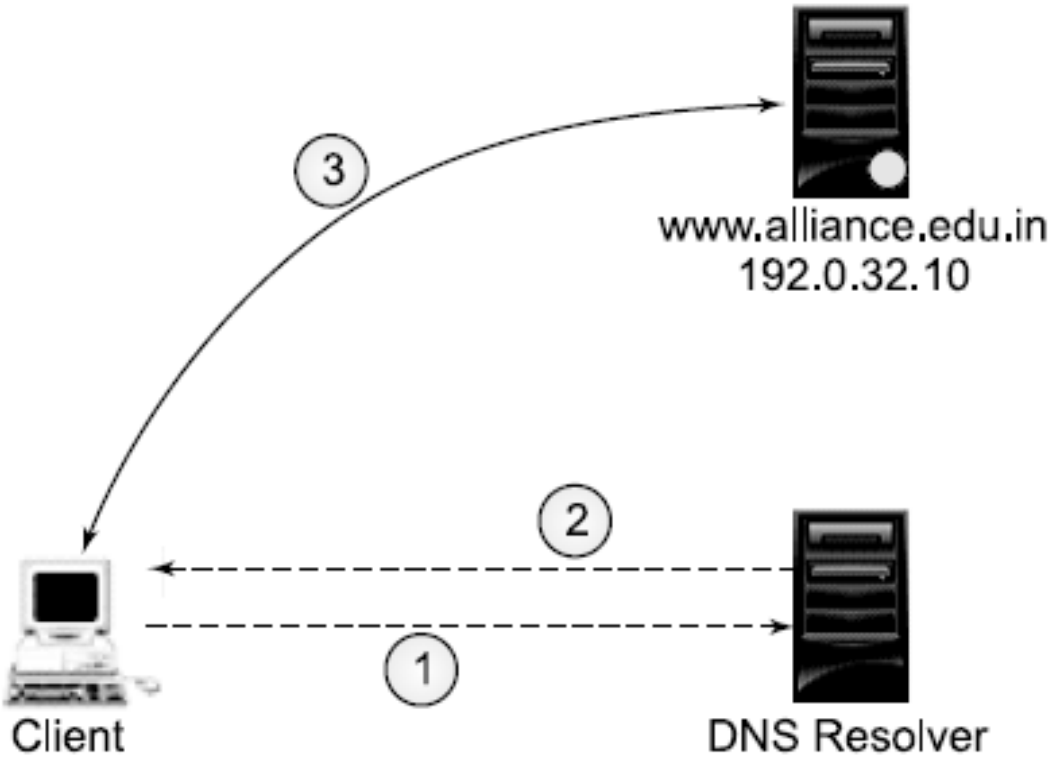
DNS spoofing - cache poisoning

- **DNS Cache Poisoning**: Poznato i kao DNS spoofing, je vrsta napada koji iskorišćava ranjivosti u DNS-u kako bi se internet saobračaj preusmjerio s legitimnog servera na lažni server. Jedan od razloga zašto je DNS poisoning vrlo opasan je taj što se može širiti s DNS servera na DNS server.
- Cache Poisoning znači promjenu stvarnih vrijednosti URL-ova. Na primjer, cyber kriminalci mogu stvoriti web stranicu koja izgleda kao, recimo, www.abc.com i unijeti njen DNS zapis u DNS cache. Dakle, kada se ukuca www.abc.com, računar će pokupiti IP adresu lažne web stranice i uspostaviti vezu s njom, umjesto prave web stranice.
- Ovo se naziva pharming. Koristeći ovaj metod, cyber kriminalci mogu phishout-ovati login kredencijale i druge infoemacije kao što su podaci platnih kartica, brojeve telefona... DNS poisoning se također obavlja tako što se ubaca malware u računar ili mrežu.

DNS spoofing - cache poisoning

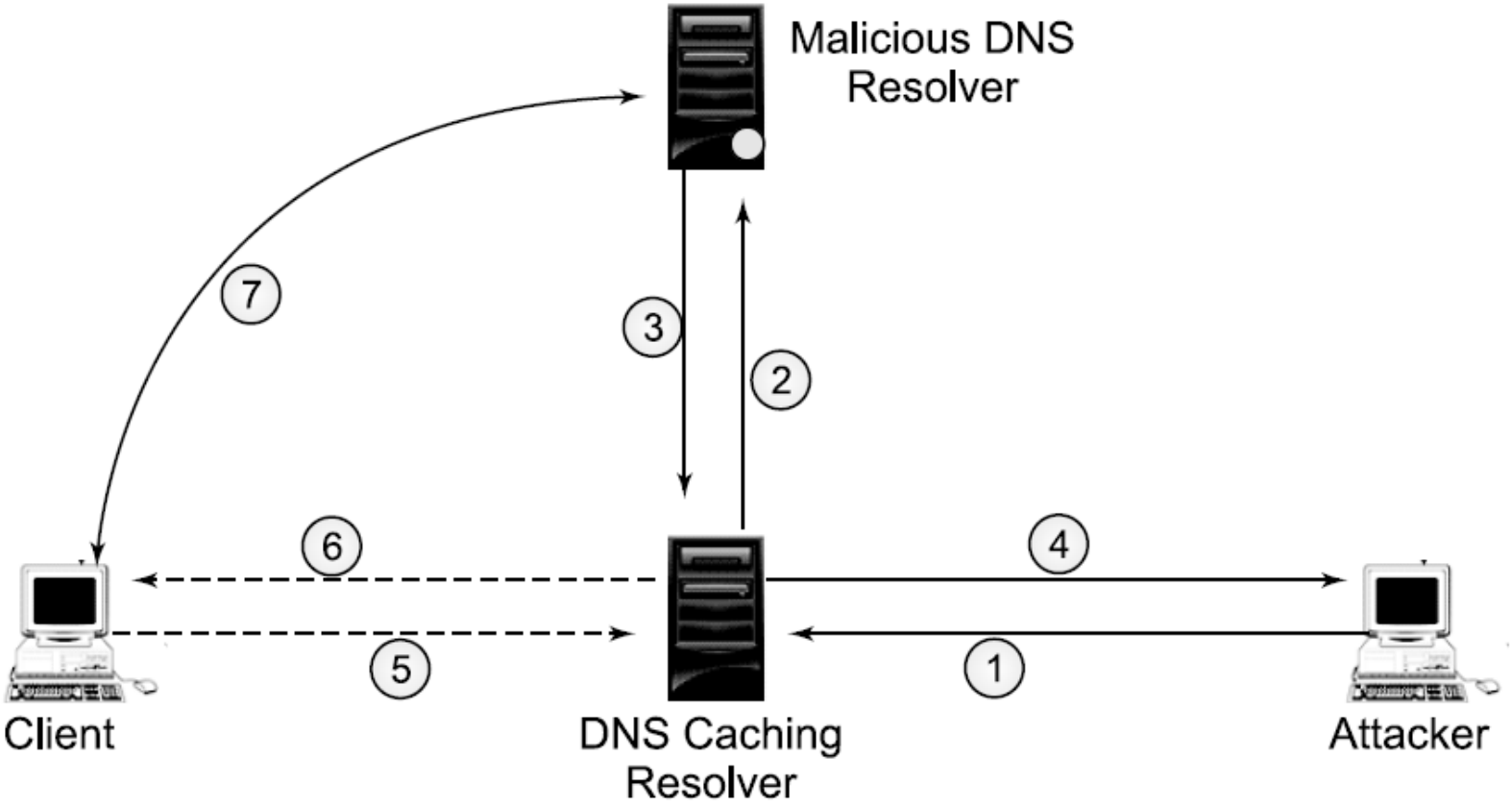
- Ponekad, umjesto lokalnog keša, kriminalci mogu postaviti i lažne DNS servere, tako oni mogu da daju lažne IP adrese.
- Ovo je DNS Poisoning visokog nivoa i kvari većinu DNS keša u određenoj oblasti, što utiče na mnogo više korisnika.

DNS cache poisoning



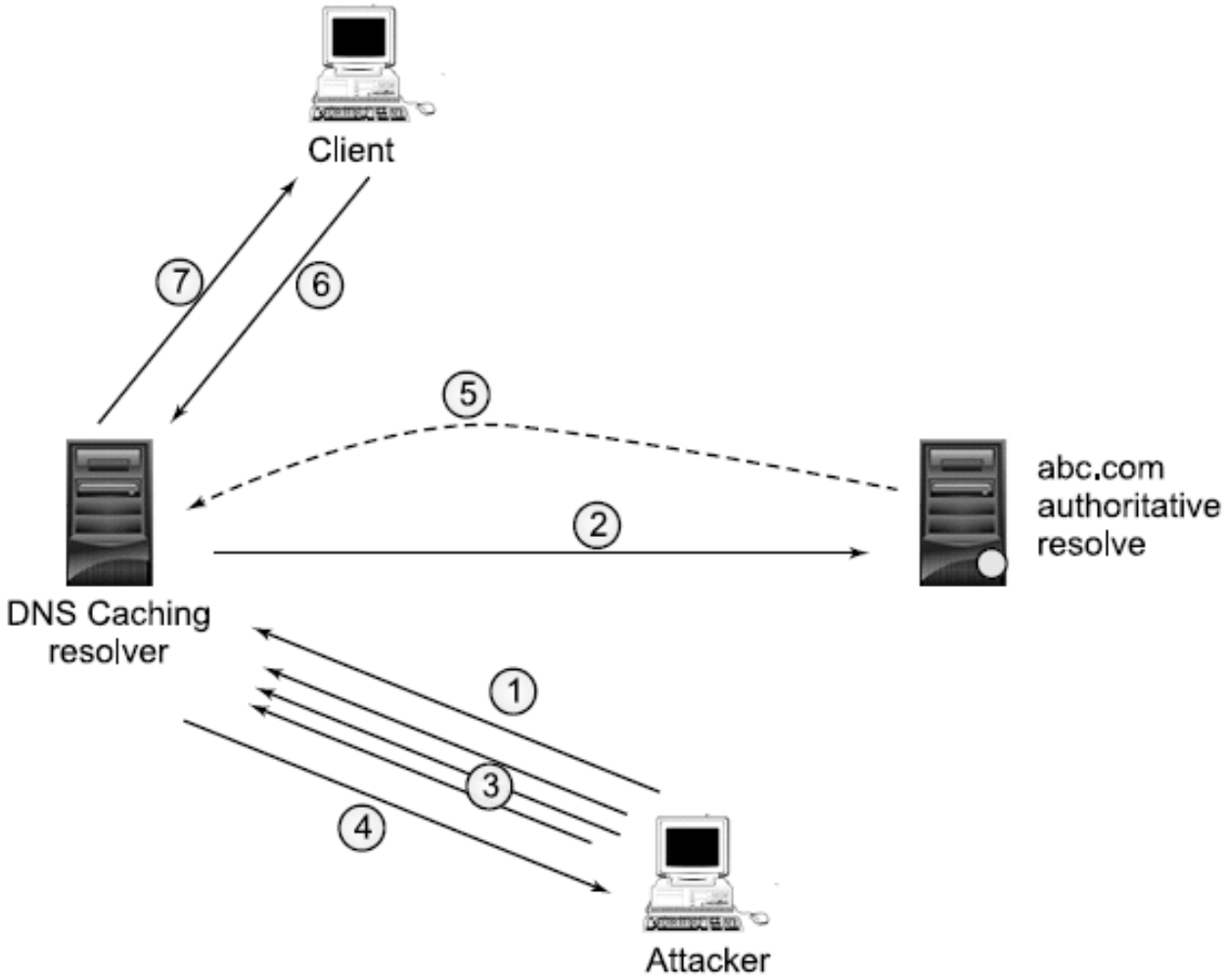
Proces rešavanja DNS upita

DNS cache poisoning



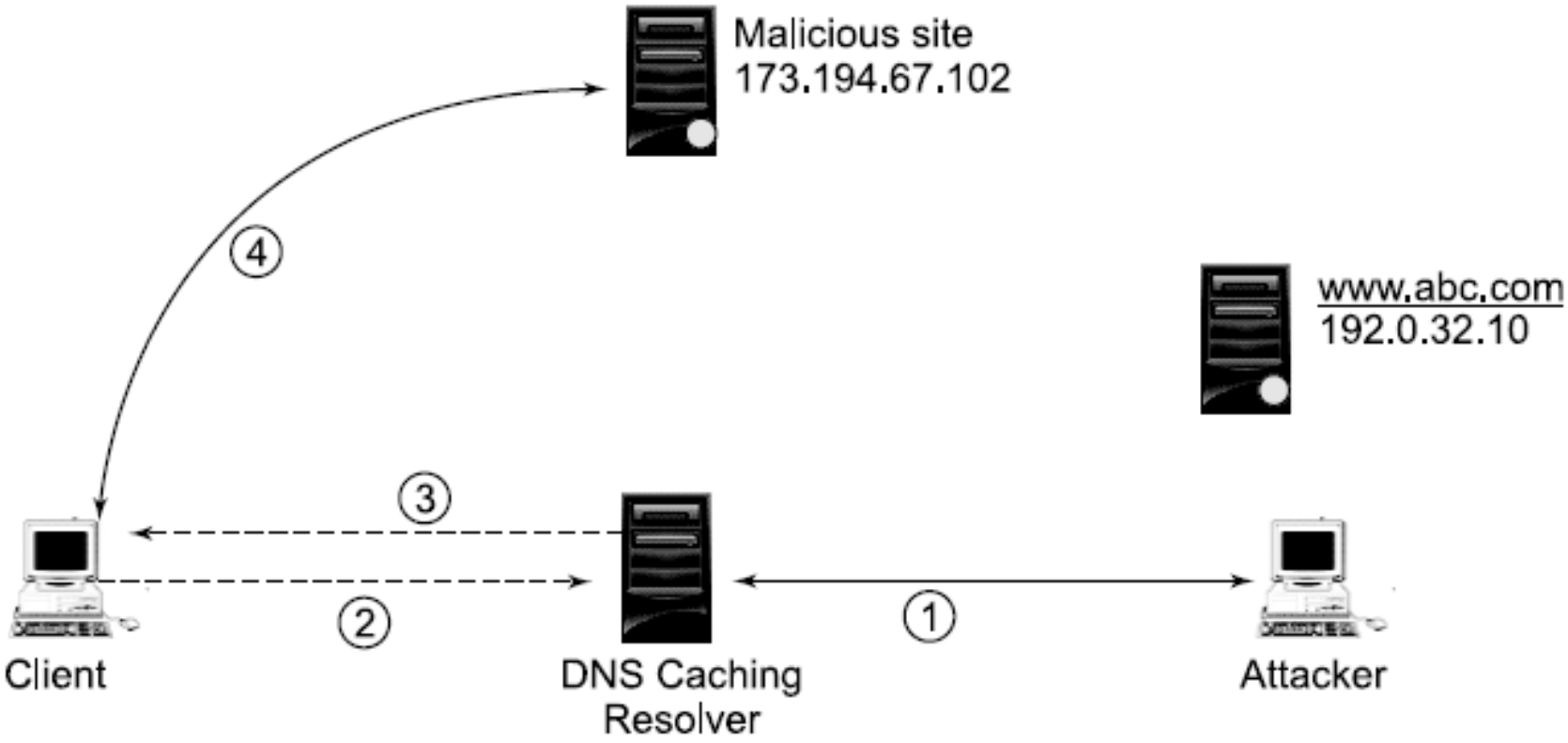
Proces rešavanja DNS upita izmijenjen DNS poisoning-om

DNS Cache Poisoning - Flooding



Proces rešavanja DNS upita izmijenjen DNS poisoning-om uz flooding

DNS spoofing



Normalan proces rešavanja DNS upita izmijenjen DNS spoofing-om

DNS Amplification za DDoS

Nisu direktna prijetnja protiv DNS sistema. Umjesto toga, oni iskorišćavaju otvorenu prirodu DNS usluge za pojačanje DDoS napada (distribuiranog uskraćivanja usluge).

U DDoS napadima napadač koristi mrežu kompromitovanih računara za slanje velike količine saobraćaja do cilja, kao što je server. Cilj je preopteretiti metu i usporiti je ili oboritii. U pitanju su mnogostruki napadi.

Umjesto da šalje saobraćaj direktno sa botneta žrtvi, botnet šalje zahtjeve drugim sistemima. Ti sistemi reaguju slanjem još većeg obim saobraćaja do žrtve.

DNS Amplification su savršen primjer. Napadači koriste botnet da pošalju hiljade lookup zahtjeva prema DNS serverima. Zahtjevi imaju lažnu izvorišnu adresu i konfigurisani su da maksimiziraju količinu podataka koje svaki DNS server vraća.

DNS Attacked by DDoS

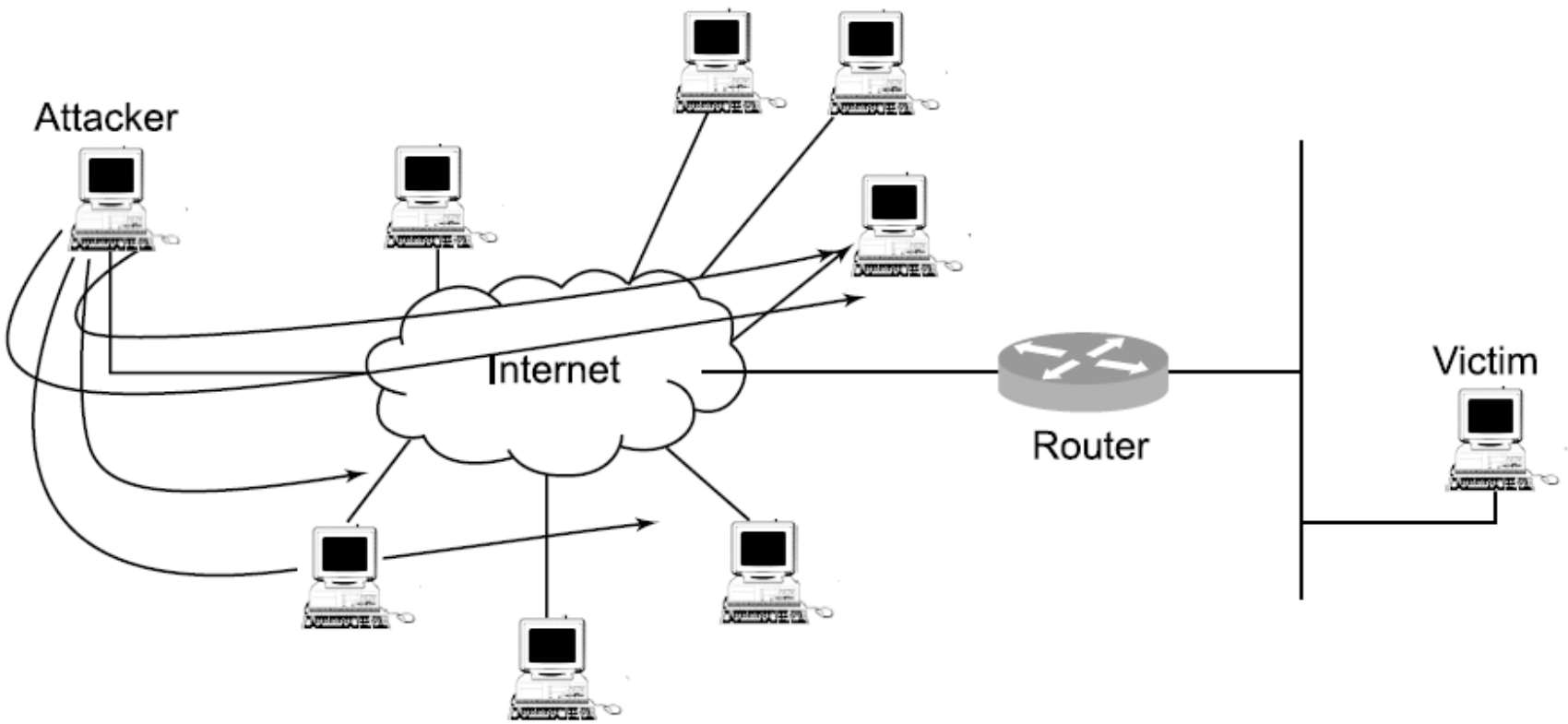
DDoS napadi se mogu koristiti protiv različitih tipova sistema. Ovo uključuje DNS servere. Uspješan DDoS napad na DNS server može da dovede do njegovog ispada, zbog čega korisnici koji se oslanjaju na server ne mogu da pretražuju web. Korisnici će vjerovatno i dalje moći da dođu do web lokacija koje su nedavno posjetili, pod pretpostavkom da je DNS zapis sačuvan u lokalnoj keš memoriji.

Reflektovani napadi

Reflektovani napadi šalju hiljade zahtjeva sa imenom žrtve kao izvorišnom adresom.

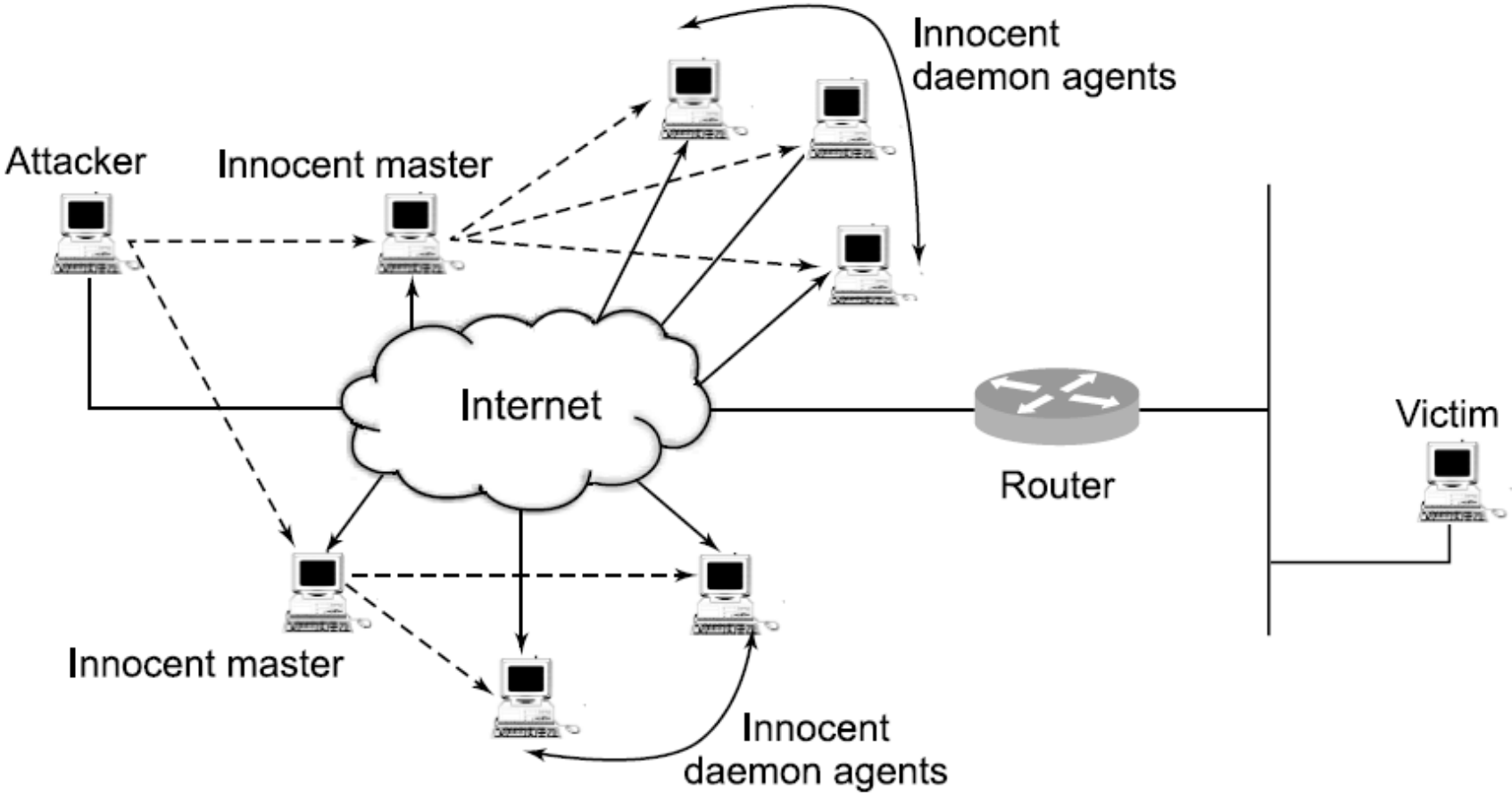
Kada primaoci odgovore, svi odgovori se šaljju zvaničnom pošiljaocu, čija je infrastruktura tada pogođena.

Distributed Denial of Service (DDoS)



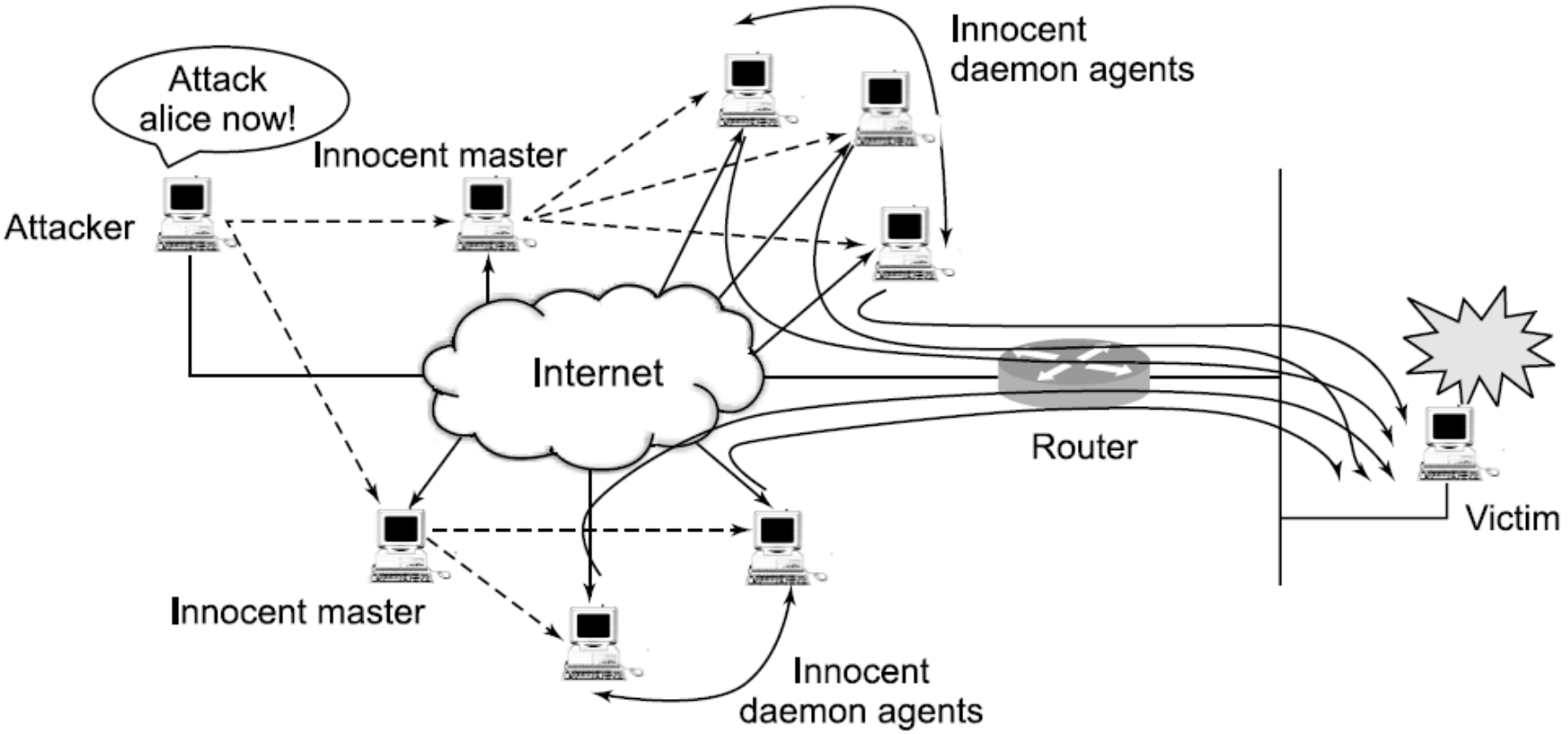
(a) Step 1

Distributed Denial of Service (DDoS)



(b) Step 2

Distributed Denial of Service (DDoS)



(c) Step 3