## Skripta Mreže

Algoritmi za rutiranje (usmeravanje):

* Algoritam za rutiranje je onaj deo mrežnog softvera koji je odgovoran za odluku o tome na kojoj izlaznoj liniji će ulazni paket da se prosledi.
* Ruter sadrži dva procesa:

Jedan upravlja dolazećim paketima: za svaki pronalazi izlaznu liniju iz ruting tabele: prosleđivanje (forwarding).  
 Drugi proces je zadužen za popunjavanje i održavanje tabela rutiranja - algoritmi usmeravanja.

* **Statički algoritmi rutiranja** - Nije adaptivno, ne oslanja se na aktuelne procene o saobraćaju,   
  **Rutiranje na osnovu najkraćeg puta** (treba da se izradi graf podmreže).   
  algoritam traži najkraći put između dva rutera.  
  Dužina puta se može meriti na primer sa brojem skokova. Jedna druga mera može biti udaljenost u kilometrima.  
  U opštem slučaju se težine lukova grafa mogu izračunati kao funkcije udaljenosti, širine kanala, prosečnog saobraćaja, troškova komunikacije, prosečnog reda čekanja, merenog vremena kašnjenja.

**Plavljenje (flooding)**

svaki dolazni paket se prosleđuje na svaku izlaznu liniju osim na onu sa koje je stigao

stvara se mnogo dupliranih paketa, zbog toga u zaglavlju paketa ima brojač skokova (hop counting)

plavljenje bira uvek najkraći put, jer bira sve puteve istovremeno

korisno je na primer za osvežavanje baze podataka

* **Dinamčki protokoli rutiranja:   
  Unutrašnji:** Unutar jednog AS. Npr. RIP ima maksimalni hop count 15   
  **Spoljašnji:** Koriste ga Internet Service Provider-i. Spajaju AS-eve. Ovakav je npr. BGP (Border Gateway Protocol)
* Adaptivni

Rutiranje na osnovu vektora razdaljine (distance vector routing).Svaki ruter održava tabelu (vektor) koji sadrži najkraći poznati put do svakog cilja

Zapis sadrži dva dela: preferirana izlazna linija za dati cilj i procenjeno vreme ili udaljenost.U periodima od T ms svaki ruter šalje svim svojim susedima listu o procenjenim kašnjenjima do svakog cilja. I dobija sličnu listu od svakog suseda.

Ruter može da sazna koja je procena najbolja, i u budućnosti koristi tu procenu i pripadajuću liniju u tabeli rutiranja.

* Rutiranje na osnovu stanja linije (linka) (link state routing)

Zasniva se na Dijkstra algoritmu Brže konvergira od DVR-a.

U upotrebi je više vrsta ovog algoritma

Svaki ruter čini sledećih pet koraka:

Pronalazi susede i saznaje njihove mrežne adrese (HELLO).

Izmeri kašnjenje ili troškove do svakog suseda (ECHO).

Sastavlja paket koji sadrži dobijene informacije u koraku 1 i 2.

Prosleđuje ovaj paket svim drugim ruterima.

Izračunava najkraći put do svih ostalih rutera.

* Hierarhijsko rutiranje

Kako raste veličina mreže, tako rastu tabele rutiranja rutera.

Postaje nemoguće da se u svakom ruteru održava zapis o svakom drugom ruteru, zato se rutiranje izvodi hierarhijski.

Ruteri se dele na oblasti (regions). Svaki ruter zna kako da usmerava pakete ka ciljevima iz svoje oblasti.

Dvostepena hierarhija često nije dovoljna, potrebna je podela na oblasti, okruge, zone, grupe.

* **Algoritmi za upravljanje zagušenjem**

Ako saobraćaj previše poraste, ruteri ga ne mogu pratiti, i paketi počinju da se gube. Dalji rast saobraćaja brzo dovodi do potpunog kolpasa, i nijedan paket neće biti isporučen.  
Rešenja otvorene petlje ne dozvoljavaju nastanak zagušenja. Nakon oživljavanja sistema se ne vrše korekcije u toku rada. Alati sprečavanja zagušenja su odluke kada treba baciti paket, kada dozvoliti saobraćaj, itd. i donose se bez obzira na aktuelno stanje mreže.

Sistemi zatvorene petlje se baziraju na petlji sa povratnom spregom.

Posmatranje sistema da bi se ustanovilo gde i kada se dešava zagušenje.

Prosleđivanje ove informacije na ona mesta na kojima se može intervenisati (izvor saobraćaja).

Modifikovanje funkcionisanja sistema da se problem ukloni (smanjenje opterećenja).

* **Povezivanje mreža**

**Nadovezivanje virtuelnih kola** -

Garantovan kvalitet usluge je lakše postići konekcionim mrežama nego bez njih.

Različita virtuelna kola su povezana multiprotokolskim ruterima, i čine jedno dugačko virtuelno kolo.

Svaki gateway po potrebi konvertuje formate paketa i brojeve virtuelnih kola.

**Povezivanje datagramskih mreža-**Različite datagramske mreže su povezane multiprotokolnim ruterima. Nema zahteva da svaki paket prođe istu sekvencu gateway-a.

**Tuneliranje -** Slučaj kada su izvorišni i ciljni host na isim tipovima mreže, a između njih se nalazi neka druga vrsta mreže.  
**Fragmentiranje -** Kada veliki paket želi da prođe kroz mrežu čija je maksimalna dužina paketa previše mala, jedino rešenje je razbijanje paketa na manje delove.

**Prva strategija** je da se fragmentiranje učini transparentnim za naredne mreže kroz koje će paket da prođe do konačnog cilja – **transparentno fragmentiranje**.

Naredne mreže ne znaju da je bilo fragmentiranja.

Problemi:

U svaki paket mora da se smesti polje za numerisanje (brojač fragmenta) ili polje za oznaku kraja paketa.

Svaki paket mora da napusti mrežu kroz isti gateway

**Druga strategija**: u usputnim gateway-ima se ne vrši ponovo sastavljanje paketa, nego samo u ciljnom hostu – netransparentno fragmentiranje.

Problemi:

zahteva od hostova da budu sposobni da sastave pakete

povećava se količina podataka koja treba da se prenese, jer svaki fragment ima svoj header

Prednost:

– može se koristiti više izlaznih gateway-a

* **Sloj mreže na Internetu**

Na nivou mrežnog sloja se Internet može smatrati skupom povezanih autonomnih

sistema. Nema određenu strukturu, ali sadrži mnogo glavnih okosnica (backbone),

koji se sastoje od linija velike propusne moći i brzih rutera.  
**IP Datagram: Opcije**

Opcije su promenljive dužine. Svaka počinje identifikatorom opcije dužine 1 B.

Zatim dolazi kod nekih opcija polje dužine (isto 1B) i zatim jedan ili više B

podataka.

– Bezbednost: u praksi se ne koristi

– Strogo usmeravanje sa izvora: Kompletna putanja se zadaje u obliku sekvence

IP adresa. Korisno je na primer prilikom merenja.

– Približno usmeravanje sa izvora: zahteva od paketa da kroz određene rutere

prođe određenim redosledom, ali može da prođe i kroz druge rutere. (Razlozi

su ekonomski ili politički.)

– Beleženje putanje: upućuje rutere da dodaju svoju adresu polju opcija.

Koristilo se za otkrivanje grešaka na ruterskim algoritmima.

– Vremenska oznaka: upućuje da svaki ruter pored 32 bitne IP adrese beleži i 32

bitnu vremensku oznaku. Namenili su za pronalaženje grešaka.

**IP adresiranje:** Na Internetu svaki host i ruter ima IP adresu koja kodira broj mreže i broj hosta.

Svaka IP adresa je 32 bitna i sadržana je u poljima Adresa izvora i Adresa cilja u IP

paketima.

IP adresa je dodeljena interfejsu (ne hostu), pa se host može priključivati i na više

mreža).

ICANN (Internet Corporation for Assigned Nantes and Numbers, Korporacija za

dodeljivanje imena i brojeva na Internetu) organizacija je zadužena za dodeljivanje

imena, radi izbegavanja konfliktnih situacija.

ICANN zadužuje regionalne vlasti za dodeljivanje dela adresnih prostora

provajderima internet servisa i drugim kompanijama.

Adrese se pišu decimalno, tačkom odvojeno bajt po bajt. U ovom formatu se adresa

sastoji od 4 decimalne cifre od 0 do 255.

57IP adresiranje

32 bitni IPv4 adresa pruža 4294967296 adresa.

Od toga je otprilike 18120 miliona rezervisano za privatne mreže.

Najmanja IP adresa je 0.0.0.0 a najveća 255.255.255.255.

Adrese sa ispravnom mrežnom adresom i jedinicama na mestu adrese hosta

omogućavaju broadcast na udaljene LAN mreže.

Sve adrese formata 127.xx.yy.zz su rezervisane za testiranje sa povratnom petljom.

Specijalne IP adrese

* **IP rutiranje**

**Prosleđivanje paketa (forwarding) - Zadaci svičeva**

• Svičevi na osnovu SAT (Source Address Table) – zove se još i tabela

MAC adresa prosleđuju ram (a u ramu paket)

• Svič dobije ram, čita MAC adresu, proverava CRC i prosleđuje ram

na odgovarajući port.

• Multicast i broadcast ramove prosleđuju na svaki port osim odakle

je došao. Svič može da izvodi IGMP snooping da sazna za portove

na koje treba da proledi multicast ramove.

• U SAT-u su informacije i o VLAN-u.

**Prosleđivanje paketa (forwarding) -** Hostovi su konfigurtisani ili statički ili DHCP (Dynamic Host

Configuration Protocol) protokolom.

• Hostovi šalju sve što nije na njihovoj mreži default gateway-u. Ako

dg nije definisan, operativni sistem daje poruku Destination

unreachable.

• Šta radi host prvo kada treba da pošalje paket?

• Proverava tabelu rutiranja i obrađuje podatke iz tabele i adrese cilja

(da bi saznao da li je cilj na njegovoj ili na udaljenoj mreži.)  
 **Zadaci rutera:**

• Prosleđuje paket sa svog jednog porta na neki svoj drugi port

• Koriste ARP: Naime Ethernet ram biva uništen kada dođe u

ruter. Ruter gradi novi Ethernet ram sa svojom MAC adresom

kao izvorom i MAC adresom sledećeg rutera ili hosta kuda

prosleđuje paket.

• Može da radi i NAT (Network Address Translation)

• Može da sprovodi i QoS

• **NAT - Network Address Translation -** Preslikavanje mrežne adrese

Pravni korisnici (a i kućni) raspolažu sa više računara, koji su povezani

LAN-om. Obično je na LAN-u jedan ruter koji je povezan iznajmljenom

linijom sa provajderom radi kontinuiranog pristupa. Svaki računar zahteva

svoju IP adresu tokom celog dana.

Servis provajder ne može imati više korisnika nego što ima IP adresa.

Rešenje je IPv6

Privremeno rešenje je NAT

Svakom preduzeću ili ustanovi se dodeljuje jedna (ili mali broj) IP adresa

za internet saobraćaj.

• Unutar preduzeća svaki računar ima svoju IP adresu.

• Međutim, kada paket napusti preduzeće, i izađe prema internet servis

provajderu, vrši se konverzija adrese.

• Dodeljeno je tri adresna prostora za privatno korišćenje. Na Internetu ne

sme da se pojavi paket koji sadrži adrese iz ovih adresnih prostora:

10.0.0.0 -10.255.255.255/8 (16 777 216 hostova)

172.16.0.0 -172.31.255.255/12 (1 048 576 hostova)

192.168.0.0 -192.168.255.255/16 (65 536 hostova)

Nedostaci

– NAT beskonekcioni Internet pretvara u jednu vrstu konekcione mreže. Ako

NAT ruter ispadne, i tabela se izgubi, sve TCP konekcije prestaju. Inače, bez

NAT-a ispad rutera nema uticaja na TCP.

– NAT povređuje najvažniji princip slojevitosti protokola: k.-ti sloj ne sme da

čini nikakve pretpostavke o tome šta je k +1. sloj stavio u polje podataka.

Promene u jednom sloju ne smeju zahtevati promene drugih slojeva.

– Procesi na Internetu ne koriste obavezno TCP ili UDP.

– Nekoliko aplikacija (npr. FTP) smešta IP adrese u polje podataka, i zbog toga u

prisustvu NAT-a može da bude problema (rešava se često na nivou aplikacije).   
  
• **Internet Control Message Protocol ICMP**

− Neizostavni deo IP-a

− Služi za korektnu obradu grešaka

− Sa ICMP komunicira 3. sloj

− Niži slojevi barataju ICMP paketima

kao i sa svim drugim vrstama.

− Obično se ovakav paket i vrati

pošiljaocu, jer mu je potreban

izveštaj o grešci.

− Zaglavlje se malo razlikuje od IP

zaglavlja.

**DHCP**

• Dynamic Host Configuration Protocol

• Ovo je klijent-server protokol pomoću kojeg se hostovima (ređe

ruterima) mogu dodeliti konfiguracione informacije.

• Klijenti DHCP-om traže IP adresu, masku podmreže, adresu rutera,

IP adresu DNS servera, i slično.

• DHCP server održava bazu podataka

• DHCP server dodeljuje IP adresu na zahtev, koji klijent vraća nakon

završetka konekcije.

• Na taj način više hostova može da koristi istu IP adresu.

Tri načina dodeljivanja IP adrese:

– Dinamčko: Administrator dodeljuje DHCP serveru jedan IP interval,

računari na LAN-u traže IP adresu prilikom inicijalizacije mreže, i

dobiju je na određeno vreme - leasing. DHCP server može da oduzme

adresu koja nije obnovljena na vreme i da je dodeli nekom drugom.

– Statičko: administrator unapred odredi kojoj MAC adresi koju IP

adresu treba dodeliti, i to će DHCP server da dodeli.

– Automatsko: Slično kao dinamičko, samo DHCP server u tabeli sačuva

ko je koju adresu dobio, i ubuduće dodeljuje uvek te adrese.

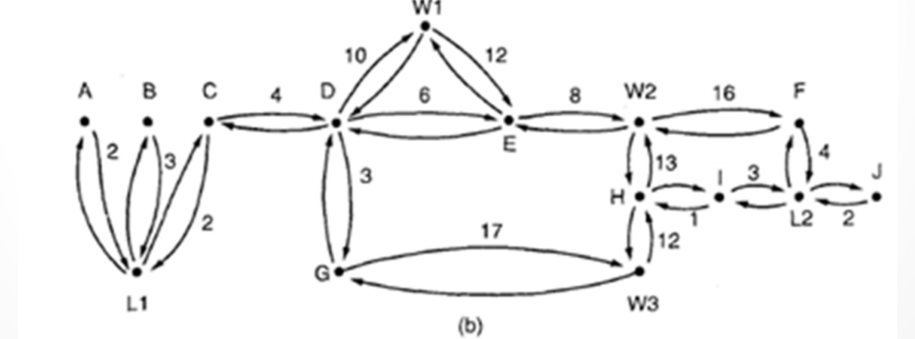
Dinamčki protokoli rutiranja

• OSPF (Open Shortest Path First) unutrašnji protokol za mrežni prolaz

Standard važi unutar jednog autonomnog sistema (routing domain)

– OSPF preslikava stvarnu mrežu u ovakav graf, zatim izračunava

najkraću putanju od svakog rutera ka svakom drugom ruteru.



Svaki AS ima područje okosnice koje se zove nulto područje.

– Svako područje se spaja sa okosnicom (eventualno tunelom)

– Unutar jednog područja svaki ruter raspolaže istom bazom podataka o

stanju linka, i koristi isti algoritam za pronalaženje najkraćeg puta.

– Zadatak mu je da izračuna najkraći put od sebe do svakog rutera unutar

područja, uključujući i ruter koji ga povezuje sa okosnicom.

– Ruter koji se spaja na dva područja, ima dve baze podataka (za svako

područje jednu), i za svako područje izvršava algoritam najkraćeg puta.

• Neighbor: Designated router (bira se na osnovu ID broja,

koji je obično i IP adresa, odnosno loopback adresa)

• Hello paketi: Dead time- nakon ovog vremena se smatra

susedni ruter mrtvim.

• Link State Database: update preko flooding-a (ima više

tipova slanja link state-a, npr. može samo DR da šalje)

• Cost: RRT vreme (podešen bandwidth)

* **Transportni sloj**

Cilj transportnog sloja je da obezbedi efikasnu, pouzdanu i ekomomičnu uslugu svojim

korisnicima, procesima koji se izvršavaju u sloju aplikacije.

Element transporta (transport entity): element hardvera ili softvera koji izvršava radnju

Koja je glavna razlika između sloja mreže i sloja transporta?

Kod transportnog sloja se izvršava na računarima korisnika, dok u slučaju sloja mreže

kodovi se izvršavaju uglavnom na ruterima koji su vlasništvo provajdera.

Programeri sloja aplikacije mogu da pišu kod za standardizovan set osnovnih operacija, i

tako napisani programi će raditi na širokom dijapazonu mreža.

Kada proces aplikacije (korisnik TCP usluge) želi da uspostavi

konekciju sa udeljenim procesom, treba da naznači sa kojim

procesom želi vezu.

Kome da se šalju pojedine poruke?

Definišu se zasebne transportne adrese za procese, na kojima mogu

da čekaju na zahteve za konekcijom: portovi (opšti naziv je TSAP

Transport Service Access Point, u sloju mreže je to NSAP, a na

internetu IP)  
**Multipleksiranje -** Ako npr. na jednom hostu stoji na raspolaganju samo jedna mrežna adresa,

tada svaka konekcija transporta treba da koristi tu adresu.

**TCP model -** TCP entitet rastavlja tok podataka (koji dolazi od lokalnih procesa) na jedinice ne veće

od 64 KB.

U praksi je to često 1460 B da bi sa zaglavljima stao u Ethernet okvir.

Pojedini delovi se šalju kao IP datagrami

Portovi ispod 1024 se zovu dobro poznati portovi (well-known port) i rezervisani su za

uobičajene usluge.

Ovi portovi su defisani od strane IANA. Ostale adrese se mogu dodeliti po želji.

U TCP vezama su tokovi bajtova.

Kada aplikacija prosledi podatak TCP-u, TCP odlučuje da li da odmah šalje ili

baferuje neko vreme, pa odjednom pošalje više podataka

Može da sakupi podatke više instrukcija pisanja u jedan segment, ili da podeli

podatke jedne instrukcije u više segmenata

Podatke sa oznakom Urgent data (hitan podatak) TCP prosleđuje odmah.

TCP entiteti koriste vrstu protokola kliznih prozora:

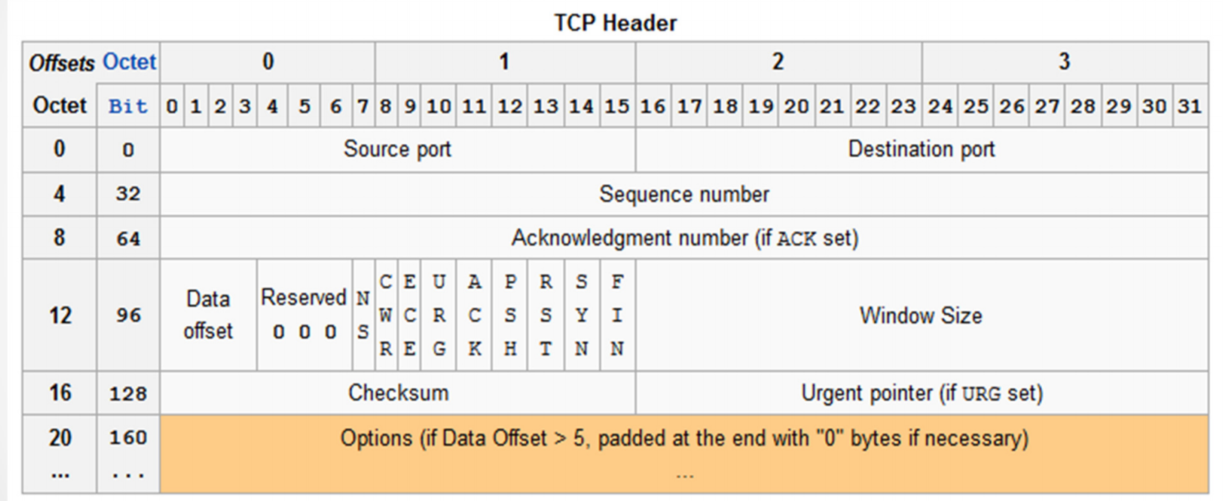
– potvrda: TCP entitet na prijemu vraća takav segment (pun podataka ako ima šta za

slanje, inače prazan) u kojem potvrđuje prijem rednim brojem narednog segmenta

koji očekuje.

– Ako na strani izvora tajmer istekne pre dobijanja potvrde, segment se ponovo

pošalje.



**Uspostavljanje TCP veze -** Jedna strana (server) pasivno čeka zahteve izvršavanjem elementarnih operacija

(primitives) LISTEN i ACCEPT.

Druga strana, klijent izvršava operaciju CONNECT.

CONNECT šalje jedan TCP-segment sa vrednostima SYN = 1 i ACK=0, zatim

očekuje odgovor.

Kada segment stigne na odredište, tamošnji TCP entitet proverava da li proces

postoji koji je izvršio LISTEN operaciju na portu koji je naznačen u polju

ciljnog porta. Ako ne, tada odgovorom RST = 1 odbija zahtev za konekcijom.

Ako neki proces sluša zadati port, tada on dobija pristigli TCP segment, i na

njemu je odluka da li će da prihvati zahtev za konekcijom ili ne. Ako prihvata,

tada šalje segment sa potvrdom.

**Raskidanje TCP veze -** Za raskidanje veze bilo koja strana može da pošalje jedan TCP segment sa

FIN = 1 čime označava da ne želi više podataka da šalje.

Čim stigne potvrda na FIN, taj smer se zatvara.

U drugom smeru se prenos podataka može nastaviti bez ograničenja i bez

obzira na zatvaranje jednog smera.

Kada se zatvore oba smera, konekcija se završava.

Prva potvrda (ACK) i drugi FIN se može staviti u isti segment.

Ako na FIN ne stigne odgovor tokom dva životna veka paketa, pošiljaoc

FIN paketa raskida vezu.

Druga strana na kraju primećuje da ga niko ne sluša, i istekne mu tajmer.

**TCP rad s prozorom -** Kada je veličina prozora 0 bajta, pošiljaoc u normalnom slučaju ne može da šalje

segment, međutim postoje dva izuzetka:

– hitan podatak se može poslati

– može da pošalje segment od 1 bajta u kojem traži od prijemnika da saopšti redni

broj sledećeg segmenta koji očekuje i veličinu prozora – ovim se izbegava mrtva

tačka koja može nastati ako se izgubi segment koji obaveštava o veličini prozora

Pošiljaoc nije obavezan da momentalno prosledi podatak dobijen od aplikacije.

Prijemnik takođe nije obavezan da momentalno potvrdi primljene segmente.

Kada se šalje mnogo malih podataka, i svi su u posebnom segmentu, neefikasno se

opterećuje mreža. Rešenje je Nagle algoritam: kada podaci pristižu bajt po bajt, samo se

prvi pošalje, a ostali se baferuju dok ne stigne potvrda za prvi. (Kod aplikacija u realnom

vremenu nije pogodan.)

**TCP upravljanje zagušenjem -** Ideja je da se ne šalje novi paket na mrežu dok je prethodni ne napusti (stigne na

odredište). TCP pokušava ovo postići dinamičkom promenom veličine prozora.

Svaki TCP algoritam pretpostavlja da se prekoračenje vremena dešava zbog zagušenja, i

zato to proverava, da bi primetio zagušenje.

Rešenje Interneta se bazira na tome da se mogu pojaviti dva potencijalna problema –

kapacitet mreže i kapacitet prijemnika. Ova dva problema se rešavaju posebno. Svaki

pošiljaoc koristi dva prozora: jedan kontroliše prijemnik, a drugi je prozor zagušenja

(congestion window).

– Broj bajtova koji se mogu poslati je minimum vrednosti ova dva prozora.

– Prozor zagušenja pošiljaoc stavi na veličinu najvećeg segmenta, zatim pokušava da

ga povećava (eksponencijalno) – spori start (slow start)

**UDP -** User Datagram Protocol – protokol za korisničke datagrame

beskonekcioni protokol

• Procesi se priključuju na neki port nekom osnovnom

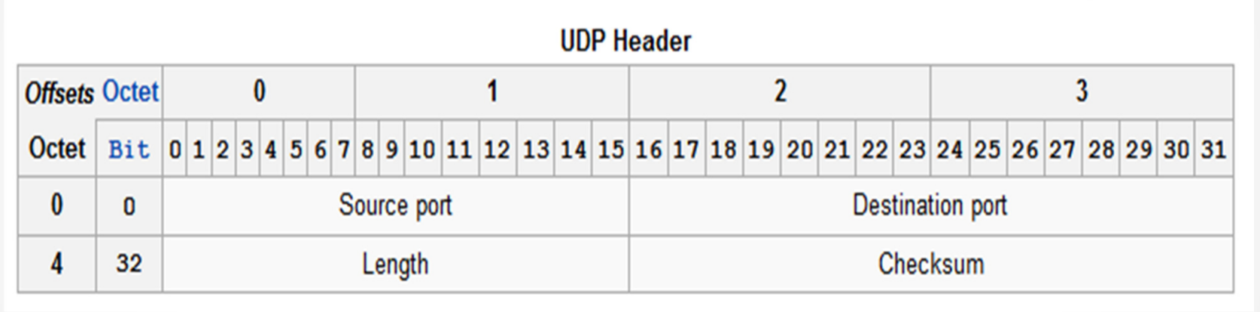
operacijom kao što je BIND

• Kada UDP segment pristigne, tada se njegovo polje podataka

isporuči procesu koji je povezan na adresirani port.

• Prednost upotrebe UDP naspram IP je da se u zaglavlju nalazi

adresa porta pošiljaoca i prijemnika.



**TCP upravljanje tajmerima**

Tajmer za ograničenje čekanja (persistence timer)

– da ne dođe do kružnog blokiranja, ako se slučajno izgubi osvežavanje prozora

Tajmer za proveru stanja veze (keepalive timer)

– Kada je konekcija neko vreme neaktivna, tajmer istekne, i TCP proverava da li

njegov partner još funkcioniše. Ako udaljeni entitet ne odgovara, konekcija se

završi.

Time-Wait (2MSL maximum segment lifetime)

– pokreće se nakon raskidanja veze sa drugom stranom

– konekcija se raskida tek nakon isteka ovog tajmera, i port se nakon toga može

ponovo upotrebiti

– na taj način je svaki paket sigurno stigao ili je bio odbijen (ne preklapa se sa drugom

konekcijom)

UDP usluge -

Ne radi sledeće:

– kontrola saobraćaja

– kontrola greške

– ponovno sanje u slučaju prijema pogrešnog segmenta

Sposoban da:

– osigura interfejs za korišćenje IP protokola

– da demultipleksira više procesa istovremeno

UDP je koristan u slučaju kratkih pitanja klijenta i kratkih odgovora servera

(npr. DNS Domain Name System – Sistem imena domena).

* **Protokoli sloja aplikacije -**

Određuju:

– tip poruka (request, response)

– sintaksu poruka

– značenje pojedinih polja u poruci

– pravila koja određuju kada i kako se šalju i odgovaraju na

poruke

• Ovi protokoli su opisani u RFC dokumentima, npr.

HTTP, SMTP (a neki u vlasništvu npr. Skype)  
  
Web

• Web stranica se sastoji od objekata

– html fajl

– jpeg slika

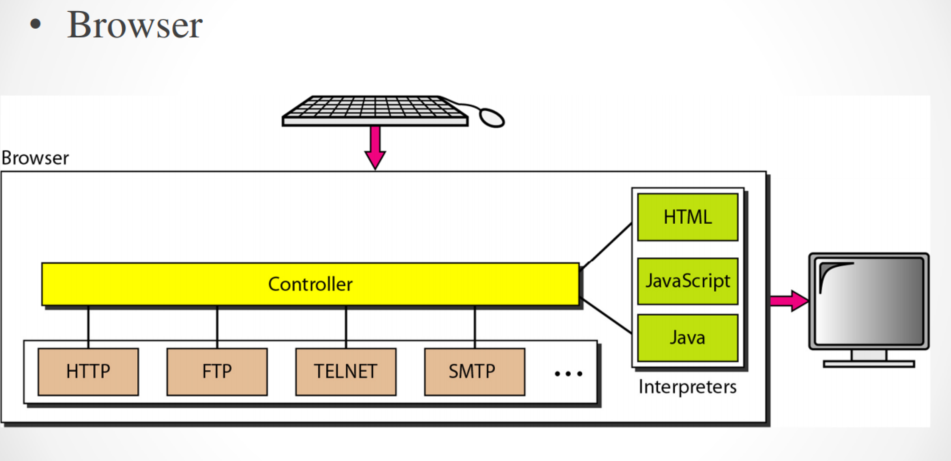
– Java applet

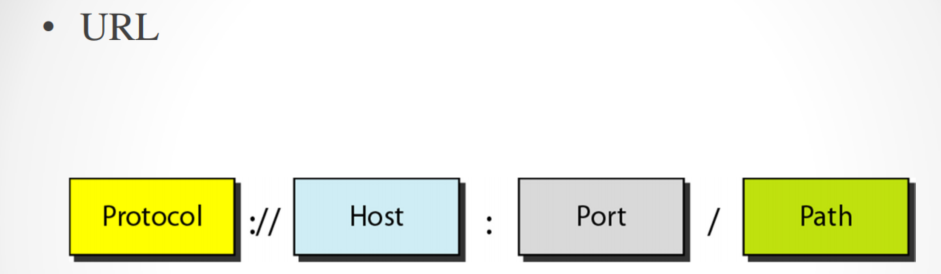
– audio fajl...

• Osnovna html stranica sadrži nekoliko referenci objekata,

koji su adresibilni preko URL.

• Web dokumenti mogu biti: statični, dinamični, i aktivni



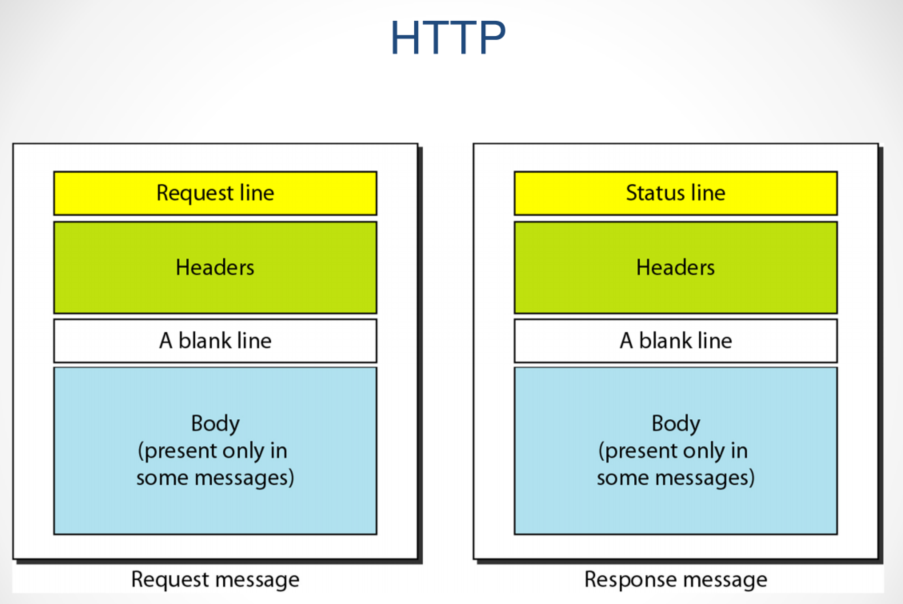


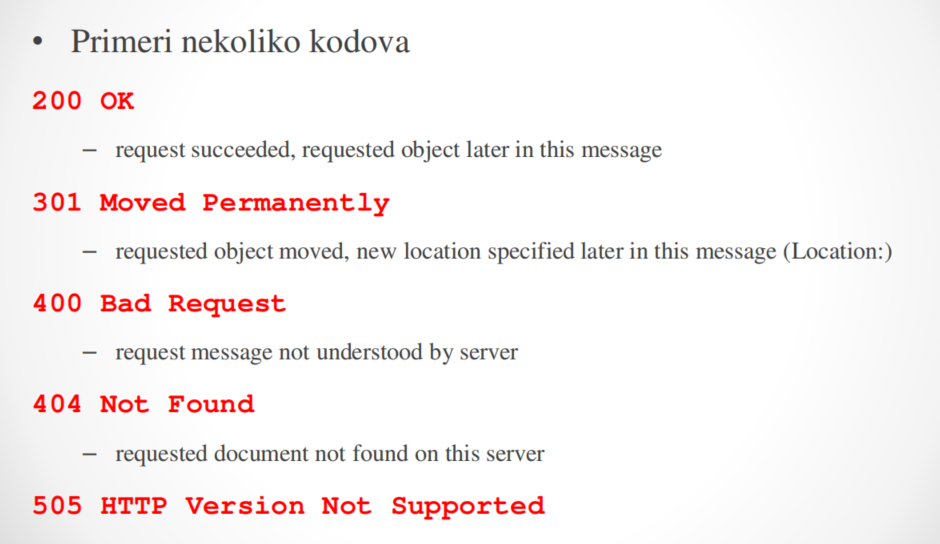
**Hypertext Transfer Protocol HTTP**

Protokol nivoa aplikacije Web-a, koristi TCP servise na portu 80

Klijent server model: Klijent traži i prima Web objekte

Server šalje objekte na zahtev klijenta





**TELNET -** Primer protokola (IAC: Interpretiraj sledeće kao kontrolni karakter): Klijent

pregovara o opcijama, moli server da pošalje echo posle svakog karaktera.

Server pristaje, i obaveštava o pristanku.  
telnet vts.su.ac.rs 80

• GET /sr/about/ HTTP/1.1

• host:vts.su.ac.rs (2 Enter)

**MDA**

• Slično kao poštansko sanduče (mailbox)

• IMAP, POP3

• zaštićeni lozinkom

**IMAP**

• Internet Message Access Protocol

• Klijent-server protokol za pristup mailovima sa lokalnog

servera

• E-mail ostaje na serveru (IMAP klijent ne briše osim ako to

korisnik baš traži)

• Na serveru je moguće raditi modifikacije i organizaciju mail

ova

• IMAP server sluša port 143

• Istim mailbox-om može upravljati više klijenata

Omogućava pojedinačno pristupanje pojedinim

delovima MIME Multipurpose Internet Mail

Extensions (npr. samo tekst, bez preuzimanja

prikačenih fajlova)

• Kroz flag-ove je moguće označiti poruke (pročitano,

važno, odgovoreno, itd)

• Omogućeno pretraživanje po raznim kriterijumima

Unique Identifier (UID) Message Attribute

32 bita, i sa unique identifier validity value čini 64 bitni broj

nijedna druga poruka nikada više ne sme imati taj broj u mailbox-u

Next unique identifier value: je broj koji će sledeća poruka

dobiti. Ovaj broj se menja isključivo onda kada stigne nova

poruka

* Message Sequence Number Message Attribute

– Daju se porukama po rastućem redosledu.

– Pokazuje relativnu poziciju poruku u mailboxu

– Može da se promeni, npr. kada se obriše neka poruka,

svaka naredna menja ovaj broj (smanjuje se).

– Može da se koristi u izračunavanjima

**Post Office Protocol 3 POP3**

• Jednostavan i standardizovan način preuzimanja poruka

na računar

– Server sluša client na TCP portu 110.

– Vrši autentikaciju klijenta

– Klijent traži servis, na šta server šalje pozdrav. Komunikacija za

vreme konekcije se vrši određenim ključnim rečima, nakon kojih

slede argumenti i CRFL.

– Case insensitive su, osim +OK i –ERR status indikatora.

• Stanja konekcije

– Authorization (User, Pass)

– Transaction

– Quit

– Update

• Server odgovara na poznate poruke i na pogrešnu sintaksu

negativnim status indikatorom.

• Server može da ima tajmer za inactivity (barem 10

minuta)

**Simple Mail Transfer Protocol SMTP**

• Ovaj protokol koristi MTA da isporuči mail na mail server

primaoca.

• Koristi se samo za slanje (ne za primanje)

• Na zahtev korisnika pošiljaoc SMTP uspostavlja dvosmerni

prenosni kanal sa SMTP primaocem.

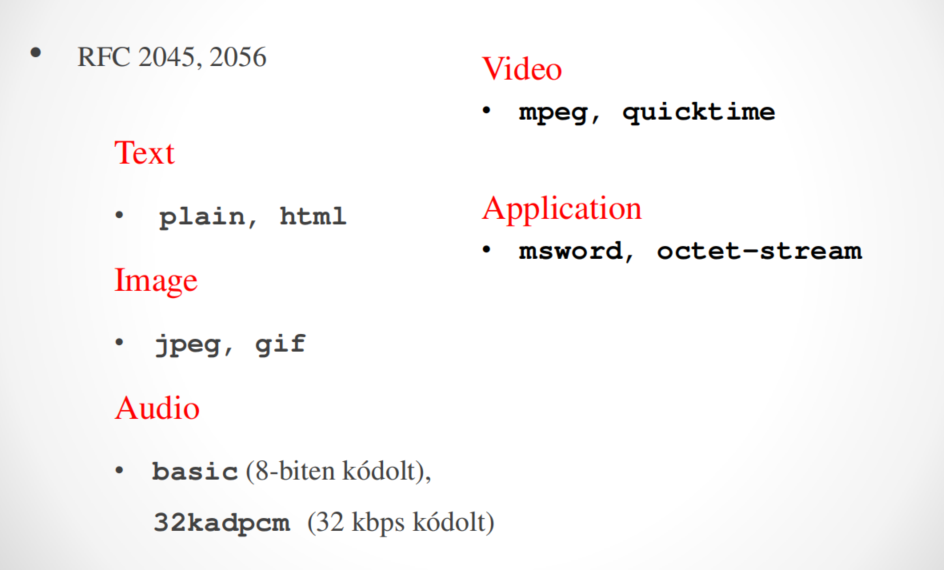
• Primaoc može biti odredišna, ali i međustanica.

• TCP 25 (poruke u ASCII kodu), perzistentno

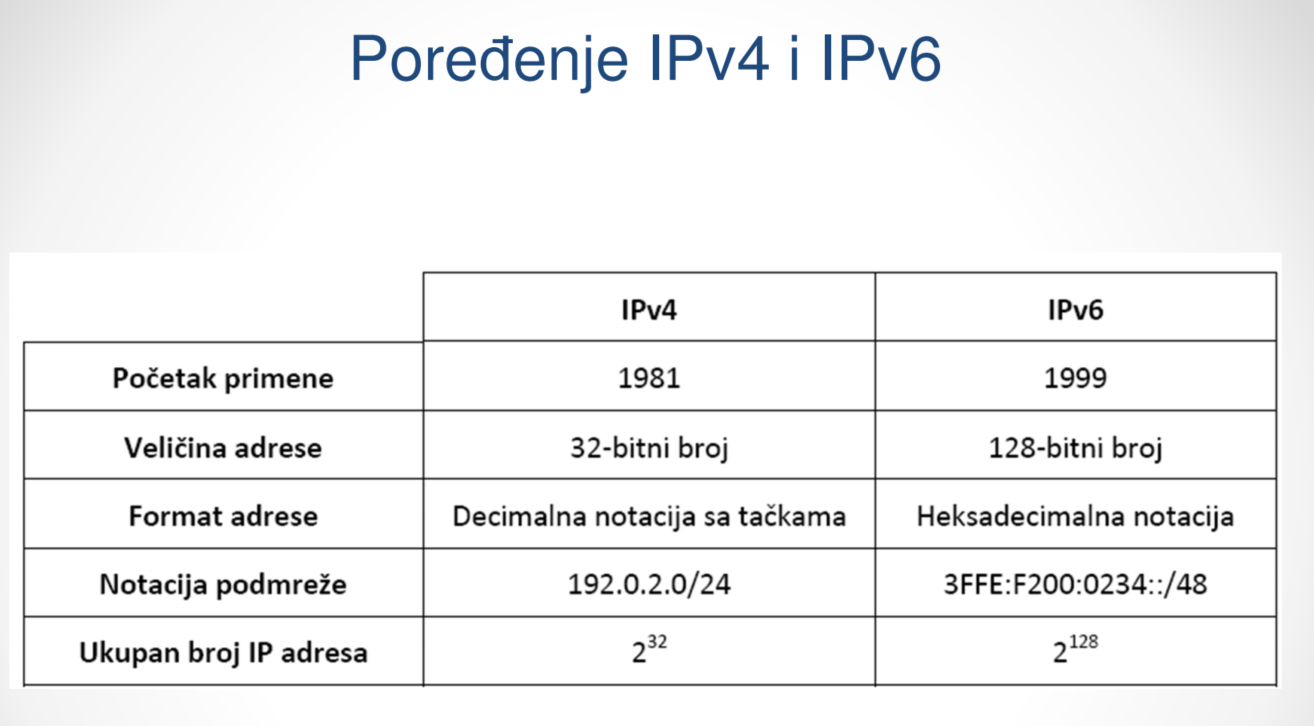
• Nije zaštićeno lozinkom, zato se zaključava server, i

dozvoljavaju samo određeni korisnici

MIME: multimedia mail extension - označava tip medije u mejlu



* **IPV6**



IPv6 donosi sledeće karakteristike

• Veći adresni prostor

• Jednostavnije zaglavlje za efikasniju obradu paketa

• Hijerarhijsku strukturu mreže za efikasnije rutiranje

• Podršku za široko primenjene protokole rutiranja

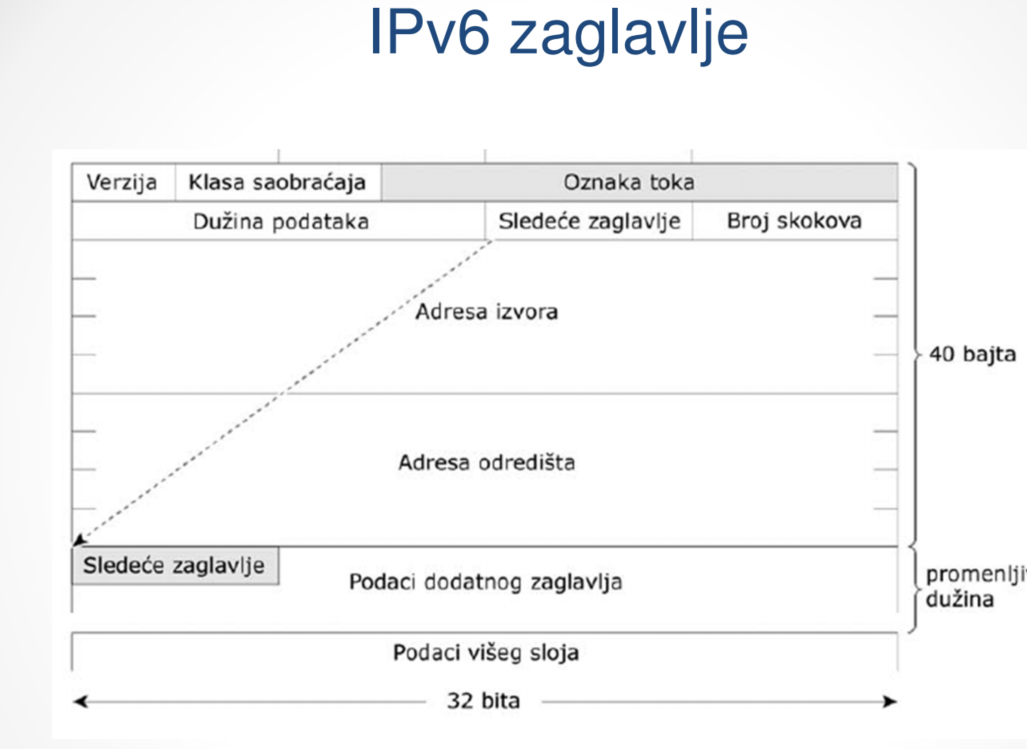
• Podršku za autokonfiguraciju računara

• Ugrađenu podršku za bezbednost podataka sa IPSec implementacijom.

• Poboljšana podrška za Mobile IP

• Ugrađena podrška za kvalitet servisa (QoS)

• Povećan broj multicast adresa



U odnosu na prethodnu verziju protokola izbačena su

nepotrebna i retko korišćena polja i uvedena su

dodatna zaglavlja. Izbacivanje ovih polja dovelo je do

brže obrade osnovnog zaglavlja, ali ukupna efikasnost

i brzina obrade zavise od dodatnih zaglavlja.

U IPv6 većina dodatnih opcija se nalazi u dodatnim

zaglavljima. Ovo omogućava veću efikasnost u prenosu

paketa, jer se šalju samo potrebna zaglavlja.

• Ne postoji fiksan broj zaglavlja u paketu, već zaglavlja

čine određen lanac, u kome polje Next Header

identifikuje sledeće zaglavlje u lancu. Poslednje dodatno

zaglavlje u lancu, u polju Next Header sadrži vrednost za

TCP ili UDP. Dužina svakog zaglavlja mora biti

celobrojni umnožak 64 bita.

IPv6 koristi poboljšanu verziju ICMP (Internet Control Message Protocol)

pod nazivom ICMPv6 koja ima iste funkcije u prijavljivanju grešaka i

slanju jednostavnih echo poruka kao i ICMP za IPv4. Međutim ICMPv6

ima i dodatne funkcije koje se ogledaju u pomoći pri funkcionisanju dva

IPv6 protokola:

• Multicast Listener Discovery (MLD) – MLD koristi tri različite ICMPv6

poruke koje zamenjuju IGMP protokol verzije 2 koji se koristio u IPv4.

• Neighbor Discovery (ND) – koristi pet različitih ICMPv6 poruka koje

omogućavaju komunikaciju među uređajima na lokalnom linku. ND

zamenjuje ARP, ICMPv4 Router Discovery i ICMPv4 Redirect.

Format IPv6 adrese

Niz 16-bitnih heksadecimalnih brojeva odvojenih znakom dvotačke ":".

Primer IPv6 adrese: 2031:0000:130F:0000:0000:09C0:876A:0001

Uvedena su sledeća pravila:

- Početne nule u svakom polju su opcione i mogu se izostaviti pri predstavljanju adrese.

Primer:

2031:0000:130F:0000:0000:09C0:876A:0001 = 2031:0:130F:0:0:9C0:876A:1

FF01:0000:0000:0000:0000:0000:0000:0001 = FF01:0:0:0:0:0:0:1

- Znak "::" predstavlja uzastopna polja koja se sastoje samo od 0. Ovaj znak se može

upotrebiti samo na jednom mestu u IPv6 adresi.

Primer:

2031:0000:130F:0000:0000:09C0:876A:0001 = 2031:0:130F::9C0:876A:1

FF01:0000:0000:0000:0000:0000:0000:0001 = FF01::1

Prefiks u IPv6 adresi predstavlja određen broj bita najveće

vrednosti i predstavlja mrežni deo IPv6 adrese.

• IPv6 prefiks se zapisuje u obliku IPv6-prefiks/dužina-prefiksa,

slično kao IPv4 adresa u besklasnom zapisu.

• Dužina prefiksa je decimalna vrednost koja predstavlja broj

bita najveće vrednosti IPv6 adrese, koji predstavljaju prefiks.

• Primer: 2031:0:130F::9C0:876A:1/64 predstavlja prefiks

2031:0:130F:0/64

**Serveri imena i zone :**

Za menadžment pojedinih delova DNS polja imena su

odgovorni pojedinci ili organizacije.

• DNS usluge predstavljaju i ostvaruju serveri. Svakoj oblasti

imena treba da pripada barem dva servera, master i slave (radi

redundantnosti).

• Serveri imena (name server): služe za preslikavanje imena u

adresu za potrebe korisnika

Kada se nekoj zoni doda novi zapis, DNS administrator zone

stavlja u bazu podataka servera: ime-IP adresu.

• Administrator jedne zone (zbog geografskih, topoloških ili

strukturalnih razloga) može da delegira pravo administracije

delova svoje zone drugima.

• Sekundarni server prima bazu podataka primarnog servera

putem prenosa zone (zone transfer)

• "domain" znači set imena, koji sadrži jedan domain name.

• Npr. svako ime domena koji se završava sa .com, pripada com

domenu.

• Zona je jednaka domenu bez poddomena koji su delegirani

drugim DNS serverima (domen manje poddomeni drugih DNS

servera)

• Npr. xyz.com je jedna zona, a abc.xyz.com je jedna druga

zona (ali ne obavezno).

**DNS cache -** Server imena (NS) dobija informacije iz 3 izvora:

– direktno iz baze podataka zone (authoritative server)

– putem zone transfer (ako je slave server)

– od drugog servera tokom razrešavanja imena

• Serveri imena (osim root i TLD servera) stavljaju naučene

informacije u cache.

– smanjuje se DNS saobraćaj, i opterećenje

– svakom zapisu je zadat TTL u sekundama

– u Windows-u po defaultu ima cache, u Unixu treba podesiti

**DNS protokol -**  Kako se pristupa jednom root DNS serveru kada ih ima mnogo

na istoj adresi?

• Nauči vremenom sa kojeg dobije najbrži odgovor, gde je

najmanji RTT, pa koristi taj.

• Anycast adresiranjem među više servera (u IPv4 se uzima

subnet unicast za anycast, ne postoje specijalne adrese)

• Anycast adrese ruteri prosleđuju najbližem mogućem cilju.

Fleksibilno rešenje, jer ako neki server i ne radi, automatski se

prosleđuje sledećem, i moguć je pristup najbližem sledećem.

**DNS protokol -** root serveri sadrže fajl root zone. U ovome se nalaze IP adrese

svih TLD servera imena (com, edu, gov,…).

• Kako se dešava osvežavanje fajla zone ako upravlja 12

organizacija?

1. root zone fajl je pod kontrolom ICANN

2. US Department of Commerce treba da odobri promenu

3. Verisign Inc promeni zonu i prosledi svim drugim root

serverima

**DNS razrešenje imena -** Vreme života zapisa TLD servera imena je najčešće (Time To

Live) 172800, tj. 48h. To znači, da server imena ISP-a može

toliko vremena da drži u cache-u zapis koji je saznao od TLD

servera imena.

• Uzmimo na primer razrešenje imena www.example.com : ovo

server čita unazad.

1. upit prema najbližem root serveru

2. root DNS server odgovara listom TLD servera koji imaju Com

3. TLD serveri imena šalju listu servera imena koji su odgovorni za example domen.

4. poslednji korak je da se od dobijenog servera imena zatraži adresa hosta www.

**DNS ima dobro poznati port 53.**

• Obično se koristi UDP. Ako ne može da stane u 512 Byte-a

tada TC flag to javlja, i može da se otpočne TCP konekcija.

**Tipovi DNS zapisa**

• A, AAAA: IP4 i IP6 adrese

foo.example.com. A 192.0.2.23

• CNAME (Canonical Name): Dodeljuje alias ime kanoničkom

imenu. Sve informacije, poddomeni, IP adrese, sve je dodeljeno

kanoničkom imenu (kanoničko ime je ovo drugo). Kanoničko

može biti u drugom domenu nego alias.

bar.example.com. CNAME foo.example.com.

foo.example.com. A 192.0.2.23

SOA (Start of Authority)

• Zona ima jedan SOA zapis koji opisuje opšte karakteristike

zone (npr timestamp).

• Sadrži ime zone, e-mail adresu odgovornog lica, serijski broj,

intervale refresh, retry i expire, kao i TTL vreme keširanja

upita (uputstvo i informacija koliko drugi da keširaju podatke

(stari protokol) ili negativne odgovore(novi protokol)

**MX (mail exchanger)**: određuje e-mail server koji pripada

domenu. Koristi ga SMTP protokol. Tu spada i broj

preferencije, ukoliko više servera opslužuje isto ime. Prilikom

slanja e-mail-e, prvo se traži MX u tabeli, pa kada sazna

domen ime servera, tada traži na osnovu A zapisa IP adresu

servera. (MX ne može pokazivati na alias ime)

– Kod raspodele opterećenja je broj preferencije isti, i SMTP

ih randomizuje

**NS (name server)**: delegira poddomen listi jednog servera

imena (name servera). NS zapisi sadrže DNS servere za datu

zonu. Zona mora da sadrži i svoje servere zbog zone transfer.

• Npr. a com zona sadrži NS zapise za sve svoje poddomene

(jako mnogo).

• subname.example.com zapis se nalazi u zoni example.com i i

pokazuje npr. na server ns1.subname.example.com, ali server

na koji pokazuje može da bude i u drugoj zoni, npr.

ns1.othername.net

Ako NS zapis pokazuje na sopstvenu zonu, tada mora da postoji takođe i A

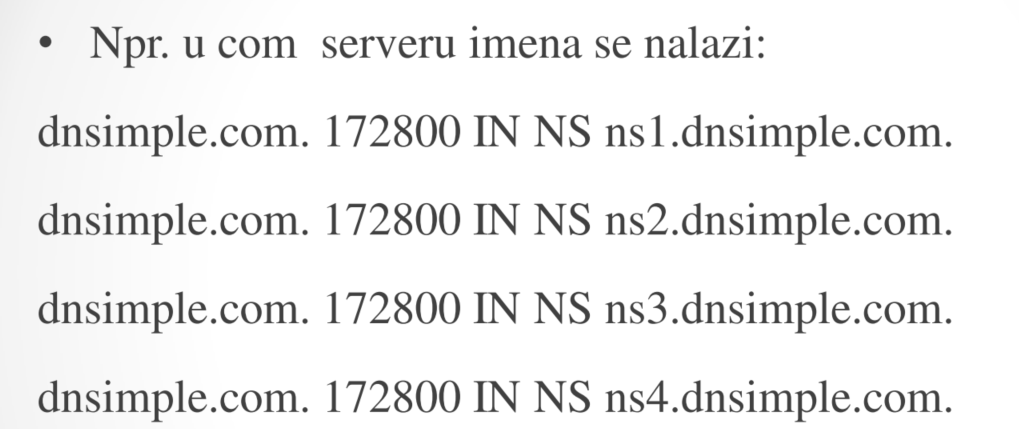
zapis da bismo saznali IP adresu name servera. Pošto ovo zapravo nije zona

roditelja, ovakav zapis se zove glue record. (Primetimo, da su ovo zapisi

com zone, a ns.example.com nije direktan potomak, ne pripada tu, ali je

ipak potreban, jer je ovo adresa servera imena, inače nikada ne bismo našli

example.com)



**PTR**: slično kao CNAME, ali u ovom slučaju se proces DNS

ne nastavlja, samo dobijemo ime. Koristi se za reverzno

traženje.

• Na primer, ako kreiramo poddomen, tada ISP treba da delegira

reverznu zonu našem DNS serveru.

• Reverz DNS dodeljuje IP adresu imenu domena, i radi sa

drugim setom podataka, nego forward DNS. (Bez ovoga je

moguće pristuiti web stranici, ali email serveri obično odbiju

adrese koji nemaju reverzni DNS zapis.

**Zone transfer -** Kada se u podacima primarnog DNS servera desi promena,

treba da se podeli promena i a sekundarnim serverima zone.

• Dešava se na TCP portu, i uvek ga započinje klijent.

• Obično DNS serveri automatski javljaju jednim NOTIFY

upitom kada se desi promena ali sekundarni ipak proveri

serijski broj pre transfera, da nije neko slao zlonamerno notify.

• Sekundarni serveri periodično proveravaju primarni, provere u

SOA serijski broj, naime kod promene se serijski broj

povećava.