## 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.

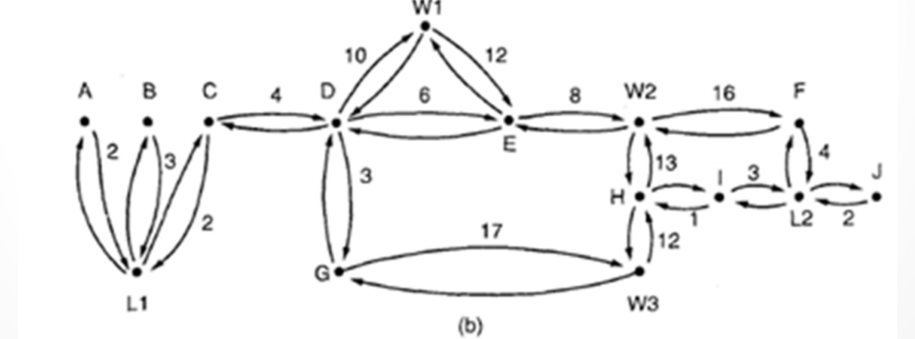
Dinamčki protokoli rutiranja

• 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)