

```
/*
 * @Author: Nikola Jokic
 * @Year: 2017
 */
```

```
===== 1
=====
```

1. Ne postoji razlika između hosta i krajnjeg sistema (sinonimi). Krajnji sistemi su: PC računar, mobilni telefon, Mail server, Web server, ... Web server jeste krajnji sistem.

2. Protocol is commonly described as a set of international courtesy rules. These well-established and time-honored rules have made it easier for nations and people to live and work together. Part of protocol has always been the acknowledgment of the hierarchical standing of all present. Protocol rules are based on the principles of civility.—Dr. P.M. Forni on behalf of the International Association of Protocol Consultants and Officers. (Wikipedia)

3. Da bi omogućili da dva različita uređaja komuniciraju. U koliko ne bi postojali standardi, krajnji sistemi ne bi znali kako da interpretiraju poruke.

- 4.1) dial-up preko telefonske linije (domaćinstva)
- 2) DSL (digital subscriber line) tj. česce ADSL kao asinhroni DSL (domaćinstva, mala preduzeća)
- 3) Kablovski i HFC (hybrid fiber and coax) (domaćinstva)
- 4) FTTH (domaćinstva)
- 5) Satelitski (domaćinstva)
- 6) Ethernet (preduzeća i domaćinstva)
- 7) Wifi (preduzeća i domaćinstva)

5. Da, deli se. U nizvodnom kanalu (downstream), svi paketi se šalju od jedne tačke ka hostovima tako da nema kolizije.

6. /

7. Od 10Mbps do 10Gbps u zavisnosti od kategorije kabla.

8. UTP (unshield twisted pair) kabl.

9. Dial-up 56Kbps, nije deljeni  
HFC 42.8 downstream 30.7 upstream, deljeni  
DSL (ADSL) 24Mbps nizvodni (downstream) 2.5Mbps upstream, nije deljeni  
FTTH nije napisano, samo je naglaseno da je brzi od DSL i da je prosečan downstream u SAD bio 20Mbps u poredjenju sa 13Mbps ADSL. Može biti deljeni, a i ne mora.

10.1) Wifi, komunikacija se odvija do bazne stanice poznatije kao WAP (wireless access point). Radio talasi obuhvataju opseg od nekoliko desetina metara. WAP je najčešće povezan kablom ka ostatku interneta.  
2) 3G, 4G, LTE se koriste kod mobilnih računara. Baznim stanicama upravlja mobilni operater, a za razliku od Wifi tehnologija, korisnik može da se nalazi na nekoliko desetina km od bazne stanice.

11. U trenutku  $t_0$  paket kreće da putuje kroz mrežu i ceo stize od rutera u vremenu  $t_1 = L/R_1$ . Kako zanemarujemo red cekanja, trenutak kada paket stigne do destinacije  $t_2 = t_1 + L/R_2$   
pa sledi da je resenje  $L/R_1 + L/R_2$ .

L-broj bitova koje ima paket  
R-brzina (bita po sekundi)

12. Nema gubitka paketa usred zauzetosti cvora. Kako je mreza rezervisana, podaci se salju/primaju zagantovanom brzinom.

TDM je fleksibilniji jer postoji mogucnost davanja veceg vremenskog odsecka signalima kojima je potreban veci protok od signala kojima je potreban manji

13. a) dva korisnika mogu da dele link jer im je potrebno tacno pola linka.  
b) Jer je propusni opseg linka 2Mbps a svaki od njih koristi po 1Mbps, tako da cak i da u isto vreme koriste link, koriste njegov pun opseg => nema cekanja. Za 3 korisnika,  
protok bi trebao da bude 3Mbps (svakom po 1Mbps) a kako link ima max kapacitet 2Mbps, jedan bi morao da saceka da se link oslobodi.  
c)  $P=0.2$   
d)  $P=0.008 (0.2^3)$

14. Zato sto bi u suprotnom saobraćaj od regije koj upravlja jedan ISP do regije kojom upravlja drugi ISP morao ici preko ISP koji je iznad njih, a za koji bi morali da plate usluge i jedan i drugi ISP. IXP zaradjuje tako sto obicno naplacuje od ISP koji koriste IXP malu naknadu najcesce izracunatu u odnosu na kolicinu saobraćaja koju ISP koristi od IXP.

15. Veca kontrola nad mrezom i smanjenje placanja internet posrednicima viseg reda.

16. Kasnjenje usled obrade, kasnjenje usled cekanja u redu, kasnjenje usled prostiranja, kasnjenje usled prenosa. Kasnjenja usled prostiranja, prenosa i obrade su uvek ista, dok je kasnjenje usled cekanja u redu promenljivo.

17./

18. Stamparska greska je u knjizi. U originalnoj verziji knjige je 2500 km i  $2.5 \cdot 10^8$ . Iz tog razloga, rezultat je 10 ms. Formula je  $d/s$  gde je  $d$  rastojanje a  $s$  brzina. Ne zavisi ovakvo kasnjenje od njegove duzine. Kasnjenje ove vrste ne zavisi ni od brzine prenosa.

19. 500kb/s  
64sekunde, jer je 4 miliona BAJTOVA a protok se meri u bitima  
100kb/s, 320 sekundi

20. Krajnji sistem A deli datoteku na pakete (paketi u zavisnosti od nacina na koji se prenose imaju max velicinu). Svaki paket se enkapsulira protokolom koji koristi u protokol staku  
(pocevsi od transportnog sloja pa do data link layer-a. Fizicki sloj nema ni jedan protokol a samim tim ni zaglavlje). Kada paket stigne do rutera, on ga "odmotava" i proverava informacije koje se nalaze u zaglavlju data link layer-a i network layer-a. Na osnovu zaglavlja mreznog sloja (network layer-a) cita IP adresu i odredjuje na koji port treba da prosledi paket. Ovde se misli o fizickom portu koji je vezan za drugi ruter ili host u krajnjem slucaju. Slicnost je u tome sto je pitanje kojim putem da krene logicki isto kao i pitanje ka kom ruteru dalje paket treba biti prosledjen.

21./

22. Provera gresaka, kontrola zagusenja, segmentacija, multipleksiranje i uspostavljanje konekcije (ovo sam nasao na net-u nisam pronasao u knjizi). Zadaci smeju biti isti na razlicitim nivoima kao na primer provega gresaka (check sum u zaglavljima pogledajte RFC dokumenta). IP i TCP imaju check sum.

23. Aplikativni, transportni, mrežni, sloj veze podataka i fizički. Osnovni zadatak aplikativnog sloja je da omogući format poruke kako bi dve aplikacije mogle da komuniciraju.

Zadatak transportnog sloja je da odredi tip veze (TCP sa "sigurnim" prenosom ili UDP gde nije "sigurno" da će svi paketi stići). Mrežni sloj je zadužen za adresiranje i prenosenje podataka kroz mrežu. Sloj veze podataka je ogovoran za prenos podataka kroz medijum dok je fizički sloj sam medijum kroz koji prolaze podaci.

24. Poruka aplikativnog sloja je poruka koja jedna aplikacija šalje drugoj. Segment se naziva poruka enkapsulirana zaglavljem protokola transportnog sloja. Datagram se naziva segment

enkapsuliran protokolom mrežnog sloja. Datagram enkapsuliran zaglavljem protokola sloja veze podataka naziva se frejms odnosno okvir.

25. Ruteri slojeve 1, 2 i 3 ne računajući rutere koji se ponasaju i kao firewall. Svičevi imaju slojeve 1 i 2. Hostovi implementiraju svih 5 slojeva.

26. Virus mora biti pokrenut od strane korisnika dok se crv može sam aktivirati i putuje bez asistencije čoveka.

27. Pravljenje botneta podrazumeva prvo da napadac pronađe rupu u aplikaciji. Nakon što to uradi, potrebno je da pronađe hostove sa tom verzijom ranjive aplikacijom koji će ciniti

deo njegovog botneta. Napadac može da poziva komande nad svim čvorovima njegovog botnet-a pa tako bi DDoS napad bio izvršen tako što bi napadac svom botnetu naredio komandu za uspostavljanje konekcije na krajnji sistem koji on želi da napadne.

28. Ovaj napad je poznat kao man in the middle. Sa te pozicije, Trudi može da menja sadržaj paketa, generise svoj paket kojim se lažno predstavlja da je jedan od učesnika, u ovom slučaju

Alisa ili Bob, ili da odbaci paket kako on ne bi stigao do odredista.

===== 2  
=====

- 1) Web koristi HTTP
- 2) DNS koristi DNS
- 3) e-mail koristi SMTP, POP3 ili IMAP
- 4) P2P file sharing koristi BitTorrent
- 5) remote login, telnet ili SSH

2. Arhitektura mreže je sa stanovista programera nepromenljiva, dok je arhitektura softvera odnosno aplikacije promenljiva, a jedno od pitanja kojima developer treba da se odluči jeste

da li je arhitektura client-server ili P2P. Arhitektura mreže je organizovana po nivoima i definiše način i protokole za komunikaciju putem mreže između udaljenih računara.

3. Klijent je proces koji inicira konekciju dok je server proces koji prima zahtev, procesira ga i vraća odgovor.

4. Ne slažem se. Računar koji inicira komunikaciju i, u ovom slučaju, traži fajl se u P2P aplikacijama može smatrati kao klijent dok je računara koji deli datoteku, i ka kome je usmeren request, server.

5. Pomocu IP adrese (prepoznaje udaljeni računara) i broja porta (broj dodeljen mrežnoj aplikaciji na udaljenom računaru).

6. UDP protokol. Nije rečeno da je bitno da svi podaci budu preneti, već je samo brzina prenosa bitna. U tom slučaju UDP protokol je pravi izbor jer, za razliku od

TCP, nema kontrolu da li je paket stigao

i timestamp koji u koliko istekne a da nije primio ACK paket od drugog hosta, salje ponovo isti paket. UDP protokol samo salje pakete na mrezu "nadajuci se" da ce svi stici do svog odredista.

7.Da, Google Docs

8. 1)Usluga sigurnog prenosa(TCP garantuje)
- 2)Usluga zagarantovanog protoka (ni jedan)
- 3)Usluga zagarantovanog vremena isporuke(ni jedan)
- 4)Integritet podataka (enkripcija, ni jedan ne garantuje, ostavljeno je protokolima sa aplikativnog sloja)

9.SSL pripada aplikativnom sloju i ne predstavlja transportni protokol vec samo nadogradnju transportnog protokola. Kako bi koristio SSL, aplikacija mora imati sertifikat odnosno SSL kod.

10.Protokol usaglasavanja je protokol koji se koristi prilikom iniciranja konekcije kako bi dve strane bile usaglasene slanjem kontrolnih paketa pre pocetka slanja podataka. SMTP koristi handshaking

11.Jer aplikacije koje koriste ove protokole ne tolerisu gubljenje delova podataka.

12.Cookie(odnosno kolacici) sluze kako bi server znao koji user je upravo poslao request. Kako je HTTP stateless protokol(protokol bez stanja, znaci da se posle izvršavanja requesta (bilo to slanje fajla ili slicno, konekcija prekida), u koliko klijent u HTTP poruci ne posalje i cookie, server ne bi znao o kom klijentu je rec.

13.Tako sto zahtev ne mora da ide preko celog interneta u koliko je stranica(objekat) kesiran u proxy serveru. Proxy server se nalazi blize klijentu => vreme odziva je krace. Ne smanjuje za sve, vec samo za najskorije trazene objekte. U koliko se trazi prvi put odredjeni objekat, taj zahtev mora ici do servera.

14./

15.Zato sto koristi dva kanala za komunikaciju. Jedan za kontrolne poruke (port 21), drugi za data transfer (port 20)

16.Alisa salje svom mail serveru preko SMTP protokola poruku. Mail server salje Bobovom mail serveru poruku pomocu SMTP protokola poruku. Bob, kako bi procitao poruku, koristi POP3 protokol jer je tako naglaseno.

To sto alisa koristi Web based e-mail aplikaciju, ne pravi nikakvu razliku jer protokol kojim se mail salje jeste SMTP, dok se HTTP koristi za preuzimanje a Bob ne koristi web based aplikaciju.

17.mozete videti na gmail-u sami.Show original opcija.

18.Razlika je sto kod preuzimanja i brisanja korisnik moze da procita poruku, a kada je preuzme na jednom racunaru, iz njegovog mail sanduceta se brise tako da se na drugom racunaru ne moze procitati. Kod rezima preuzimanje i zadrzavanje, poruke ostaju na mail serveru tako da, i u koliko preuzmete i procitate poruku na jednom racunaru, sa drugog ponovo mozete pristupiti mail serveru i preuzeti iz svog sanduceta poruku

19.Da, moguće je.MX je zapis je zaduzen da mapira server ime IP adresom mail servera.

20.Moguće je videti IP adrese maila. IP adrese se nalaze na mreznom sloju koji je obavezan bez obzira na aplikaciju koja se koristi. Gmail ponovo ima opciju show original.

21.Ne mora da znaci. U koliko je Alisa u Bobovih top 4, tada bi i Bob slao delove datoteka Alisi. Ponovo, ne mora da uzvaca istom brzinom.

22. Tako što alisa šalje svojim susedima cije IP adrese je dobila priključenjem u torrent, traži preko TCP veze odsecke koje nema (u ovom slučaju bilo koji)

23. Preklopljena mreža je logička mreža računara umreženih fizičkom mrežom s toga ne obuhvata rutere i ostale mrežne uređaje.

24. Prednost je što računar zna svaki susedni računar tako da mu je potreban tačno jedan skok do tog računara. Nedostatak je što u velikim mrežama, svaki računar sadrži podatke o svakom računaru što je sa stanovista memorije ne efikasno. Cirkularna, svaki član zna IP adrese prethodnika i sledbenika. Nedostatak je što prosečno po upitu ima  $N/2$  skokova gde je  $N$  broj računara u preklopljenoj mreži.

25. Distribucija datoteka, instant messaging, video stream, pozivi, distribuirano računarstvo (komunikacija između više servera može da teče P2P a ne client-server što bi bilo neefikasno)

26. Kod UDP, ne postoji soket koji sluša, pa pravi novu nit za komunikaciju čime bi se otvorio nov soket. UDP otvara soket na koji prima sve pakete. TCP sa druge strane sadrži i odgovore (ACK, SYNACK, FIN...).

U slučaju n konekcija bilo bi  $n+1$  soket, jedan soket na kom sluša i  $n$  soketa pomoću kojih "hendluje" n komunikacija sa udaljenim računarima.

27. TCP protokol je protokol koji uspostavlja vezu. Three-way handshake ne može biti uspostavljeno sa serverom tako da prvi SYN paket nema odgovor, ne može se uspostaviti veza sa serverom tako da se ni paket

ne može poslati preko mreže. Sa druge strane, UDP je protokol koji nema three way handshake i šalje podatke kroz svoj soket bez obzira gde su adresirani. U koliko ne postoji proces sa brojem porta na određenoj računaru (serveru), paket se u kernelu operativnog sistema odbacuje. To je razlog zašto nije moguće poslati kroz soket TCP u koliko proces na serveru nije pokrenut dok je moguće kod UDP protokola.

===== 3  
=====

1.a) Kako je rečeno da napravimo najjednostavniji protokol koji će nas paket perneti do drugog računara, zaglavlje će biti veličine 4 bajta i sadržace samo određeni port procesa na udaljenom računaru. Nije

rečeno da komunikacija treba da bude dvosmerna (pa ne stavljamo naš broj porta) nit da je bitno da paket ne bude oštećen (nema potrebe ni checksum). Naš protokol bi prihvatao maksimalno 1196 bajtova od protokola na aplikativnom sloju. Primetite da je rečeno da SEGMENT može da bude 1200 bajtova najviše. Segment je naziv paketa enkapsuliranog samo zaglavljem transportnog sloja. Ne uvrstavamo zaglavlje mrežnog niti sloja veze podataka.

b) Transportni sloj sadrži samo informacije o broju porta a ne o adresi tako da bismo samo dodali još 4 bajta za source port (port posiljaoca) kako bi server znao na koji port da adresira odgovor. To znači da bi nova verzija protokola primala od aplikativnog sloja najviše 1192 bajta podataka.

c) Ne. Transportni sloj se nalazi samo na host računarima (krajnjim sistemima).

2.a) Poštarska služba imitira mrežni protokol u ovom slučaju a koverta na kojoj je samo adresa imitira zaglavlje IP protokola sa IP adresom na njemu. Osoba zadužena da u kući distribuirati pisma bi otvorila poruku

(odmotala zaglavlje mrežnog sloja), na poruci bi moralo da u prvom redu bude napisano ime primaoca koje bi ta osoba pročitala a zatim prosledila pismo.

b) Ne naravno, poštanska služba je zadužena da prenese od jedne adrese do druge adrese, gde su sve adrese jedinstvene. Njihov zadatak nije da dostavi osobi unutar kuće već samo do kuće.

3. Izvorni port od B ka A je y, odredisni port x

4. U koliko je brzina pristizanja informacija bitnija, a da pritom aplikacija dozvoljava odredjene "rupe" u informacijama nastale gubljenjem paketa.

5. Zato sto je kapacitet i brzina linkova, kao i rad rutera dovoljno brza da moze da obezbedi gotovo jednaku uslugu, ali sa sigurnoscu paketa. Drugi razlog moze biti jer firewall je cesto konfigurisan da blokira UDP saobracaj.

6. Da. Tada je kontrola sigurnog prenosa ostavljena aplikativnom nivou.

7. Da jer UDP ima jedan soket na koji slusa i prima sve pakete, a znace na osnovu IP adrese i broja porta sa koje je segment poslat. IP adresa je u zaglavlju IP protokola a broj porta u zaglavlju UDP protokola.

8. Za svaku konekciju kod TCP-a se kreira poseban soket, ali zahtev za konekciju ide ka jednom socketu koji slusa za konekcije. U koliko nije SYN request od oba racunara (request za pocetak komunikacije), ovi request-ovi su upuceni na razlicite sokete koje determinisu IP adresa servera, broj porta servera, IP adresa klijenta i broj porta klijenta. Na osnovu toga se saobracaj usmerava ka zeljenom socketu. Da, oba soketa bi imala broj porta 80. Broj porta 80 predstavlja broj porta procesa, a kako je paket adresiran ka tom procesu, destination port je port 80. Iako ima isti broj porta svaki soket, kao sto sam rekao, definisan je i sa klijentovom IP adresom i klijentovim brojem porta tako da ce se podaci slati kroz soket namenjen tacno jednom klijentu.

9. Da bismo znali koji podaci su stigli do odredisnog racunara. Takodje zbog preklapanja u koliko koristi vise TCP veza sa istim hostom.

10. Ako se ACK izgubi negde u mrezi, ni jedan ni drugi host nece znati da se to dogodilo i cekao bi na ACK jako dugo jer ni jednim protokolom nije definisano tacno vreme u kom ce podaci od jednog hosta doci do drugog hosta.

11. Tajmer ce takodje biti jako bitan samo sto cemo u ovom slucaju tacno znati na koju vrednost da ga postavi i na osnovu koje, kada tajmer istekne, sigurni smo da je izgubljen ACK paket ili nas paket.

12. /

13. /

14. a) Ne  
b) Ne  
c) Da  
d) Ne  
e) Da  
f) Ne  
g) Ne

15. a) 20  
b) 90

16. 3 segmenta kao sto je bio slucaj i za slovo 'C'. Salje se slovo "R" sa seq=43 ack=80. Server salje nazad "R" seq=80 ack=44, a treci segment je od klijenta seq=44, ack=81

17. R/2

18. Nije tacno. Postavlja se na polovinu vrednosti prozora zagusenja (congestion window)

=====  
===== 4  
=====

1. Paket mreznog sloja se naziva datagram. Komutator sloja veze (switch) nalazi se na drugom sloju i radi sa MAC adresama, unutar jedne podmreze dok ruter radi sa IP adresama.

Switch (komutator sloja veze) se koristi za prosledjivanje paketa unutar podmreze dok se ruter koristi za slanje paketa u udaljenu podmrezu (preko niza podmreza).

2. Prosledjivanje i rutiranje. U VC pored ova dva, trece bi bilo uspostavljanje konekcije.

3. Prosledjivanje je prenosenje sa jednog interfejsa na drugi kako bi paket presao iz jedne podmreze u drugu dok je rutiranje "izracunavanje" rute sa kraja na kraj kojom bi paket trebao da ide kroz mrezu.

4. Da, koriste

5. Sigurnu isporuku recimo. Za tok paketa, isporuku po redu. Postoje za tok paketa u mreza sa virtuelnim kolima (VC) dok na internetu ne postoje ni jedna. CBR postoje obe. ABR ni jedna.

6. IP telefonija

7. Kako bi se decentralizovala ta funkcija sa jednog procesora i "izraunavanje" na koji port treba da se prosledi ne bi bila centralizovana funkcija koja ceka na procesorsko vreme vec bi se vise paketa "procsuiralo" paralelno.

8. Komutiranje preko memorije, preko centralne magistrale i preko visestruko povezane mreze. Komutiranje preko memorije pomocu prekida obavestava procesor da je pristigao paket na "ulazni port". Paket se kopira

u memoriju iz koje se procesuira, izvlati se adresa a zatim iz memorije, kopira na izlazni port. Preko centralne magistrale portovi stavljaju podatke na magistralu (u koliko je slobodna ako ne, onda cekaju), sa koje izlazni port uzima paket i salje dalje kroz mrezu. Visestruko povezane mreze omogucava 2n magistrala sa "raskrsnicama" kako bise omogucilo da vise paketa u koliko je putanja do izlaznih portova takva da nema zajednickih cvorova ni puteva, mogu da se prenose istovremeno. Ovo je odgovor i na trece pitanje.

9. Do gubitka moze dolazi tako sto prenos sa ulaznog porta na izlazni port zahteva vise vremena nego sto paketi pristizu. Bafer se puni na ulaznom portu a u jednom trenutku, paketi nece imati vise mesta u

privremenoj memoriji zbog koje se odbacuju. Moze se izbeci povecanjem brzine prenosa sa ulaznog porta na izlazni port (hardverski impementirano naravno)

10. Ako paketi doalze do izlaznog porta pre nego sto mogu biti poslani kroz medijum. Ne, jer nije problem brzina komutiranja, vec fizicka svojstva medijuma gde ne moze primiti podatke brze.

11. HOL blokira paket sa bafera ulaznog porta da predje u bafer izlaznog porta jer je izlazni port pun. Svi paketi iza tog sa istog ulaznog porta su takodje blokirani iako mozda treba da budu preneti na drugi izlazni port.

12. Da. Imaju IP adresa koliko imaju i interfejsa.

13. 11011111 00000001 00000011 00011100

14. / (individualno je)

15. 8 interfejsa. Prvi interfejs izlaznog hosta drugi ulazni interfejs na ruteru itd. 3 tabele rutiranja.
16. 50% podaci 50% zaglavlja (40 bajtova podaci + 20 bajtova TCP zaglavlje (bez opcija) + najverovatnije 20 bajtova IP zaglavlje (bez dodatnih opcija))
17. Ima polje u IP zaglavlju koje kaže koji protokol enkapsulira (6 - TCP, 17 - UDP)
18. Da koristi NAT jer je ruter dobio jednu IP adresu (javnu adresu) koja je vidljiva na internetu. Kako koristi NAT protokol, interfejs ka lokalnoj mrezi ima NAT privatnu adresu na osnovu koje se i raspoznaje unutar lokalne mreze.
19. Postoje zajednicka polja (verzija i TTL i protokol koji je enkapsuliran IP zaglavljem). Razlika je sto je fiksne velicine IPv6 zaglavlje od IPv4. Ne postoje opcije nego se dodatna zaglavlja "umecu".
20. Da, jer se zaglavlje IPv6 enkapsulira IPv4 zaglavljem u tom slucaju.
21. LS (link state) algoritmi se racunaju globalno odnosno da svaki ruter mora da zna celu mrezu pre nego sto krene sa izracunavanjem putanje. DV (distance vector) zna samo svoje "komsije".
22. Ruteri ne bi mogli da izvrse izracunavanje rute sa tako velikim grafom cvorova. Ruteri organizovani po autonomnim sistemima gde postoje protokoli rutiranja van i izmedju autonomnih sistema, omogucilo je rad na manjim grafovima.
23. Ne moraju. Algoritmi rutiranja su napravljeni da ruteri znaju kome da prosledjuju pakete i autonomni sistemi mogu bilo kojim protokolom informacije da distribuiraju. Izmedju AS radi BGP tako da za odlazak paketa izmedju AS koristi isti protokol a u tom AS svi ruteri znaju kako da prosledjuju.
24. Ne. Tabela kaže da D preko A može da dođe do z sa 11 skokova sto je više nego sto ruter D ima izracunato da može sa manje skokova da dođe do z.
25. RIP šalje do rutera sa kojima je povezan dok OSPF šalje poruku svim ruterima unutar autonomnog sistema u kom se koristi ovaj protokol rutiranja. OSPF koristi i polja u kojima naglasava rutere komsije i distancu do njih. RIP šalje samo komsijama.
26. niz autonomnih sistema
27. strana 398. Pravila: U odnosu izmedju autonomnih sistema vrlo su bitna pravila. Po nekad je vazno da se ne dozvoli prolazanje saobraćaja od jednog AS kroz drugi AS (ISP koji su zaduzeni za taj AS ne žele to). Slicno, neki AS možda želi da kontrolise saobraćaj koji prenosi izmedju drugih AS kao sto to radi BGP. Unutar istog AS sve je uslovljeno pod istom administrativnom kontrolom pa pravila imaju veliki značaj za biranje ruta. Prosirljivost: Mogucnost da se algoritam rutiranja i struktura njegovih podataka prilagode tako da mogu da se izbere sa rutiranjem prema većem broju mreza ili rutiranjem izmedju velikog broja mreza, a izuzetno bitno izmedju autonomnih sistema. Unutar AS je manje bitna prilagodljivost jer ukoliko previse poraste AS, može se podeliti na dva AS. Performanse: Posto rutiranje izmedju AS često zavisi od odnosa uspostavljenih izmedju njih, performanse ruta koje često nisu bitne toliko. Ali unutar pojedinačnih autonomnih sistema, vodi se racuna više o performansama jer se o odnosima vodi manje racuna.
28. Zato sto nema potrebe da se opterećuje saobraćaj unutar autonomnog sistema ukoliko paket ulazi i izlazi iz tog sistema. On se može regulisati "kontrolisanim



objavama"(397 strana)

29.Podmreza je deo jedne mreze. Prefiks je mreznii deo adrese i signalizira kojoj mrezi pripada adresa. BGP ruta je zargonski naziv za objavu koju ruter koristeci BGP protokol objavi i koju cini prefix zajedno sa atributima specificiranim u BGP protokolu.

30.Ruteri AS-PATH koriste kako bi sprecili netacne objave u mrezama sa petljama. Koristi se i u biranju putanje za istu mrezu (sa istim prefix-om). NEXT-HOP sadrzi IP adresu prvog rutera kao putanju do odredjene mreze. Koristi se u konfiguraciji tabela rutiranja.

31.Ako je jedan ISP recimo A povezan sa ISP B i ISP C, ali ne zeli da bude posrednik u komunikaciji izmedju B i C, tada A kod C ne objavljuje da zna rutu do C i A kod C ne objavljuje da zna rutu do B.

32.Razlika je sto visestruko jednoznacno rutiranje source ruter kreira N paketa koje salje u mrezu sto je problem sa efikasnosti dok je drugi nacin bolji jer svaki ruter pravi kopiju za interfejse ka podmrezama sa kojima je povezan. Drugi problem je sto source ruter mora da zna adrese svih drugih rutera dok kod difuznog rutiranja koje podrzavaju mreza i ruter ne mora.

33. a)Tacno za nekontrolisano plavljenje, tacno za kontrolisano i netacno za spanning tree.  
b)Tacno za nekontrolisano, netacno za kontrolisano i netacno za spanning tree.

34.Ne

35.IGMP omogucava da se racunar prikljuci multicast grupi i radi samo od racunara do njegovog rutera (koji je najcesce default gateway). Na protokolu za visestruko rutiranje sirokopojasne mreze je da uskladi rutere.

36.Tako sto stablo zajednicko za grupu koriste svi racunari i isto je za sve racunare u multikast krupi dok je stablo koje zavisi od izvora stablo koje pravi host racunar i koje se moze razlikovati od stabala kreiranih od strane drugih racunara u multikast grupi

===== 5  
=====

1.Ako je putnik datagram, onda je auto okvir.

2.Cak i ako bi linkovi bili sigurni, nemamo sigurnost da bi mreznii sloj koji radi rutiranje rutirao pakete do odredista. Mozda bi se paket izgubio istekom TTL. Sigurnost veze podataka nije dovoljna vec tu sigurnost bi morao imati i mreznii sloj.

3.Pristup linku, sigurnost isporuke, kontrola zagusenja, kontrola gresaka, korekcija gresaka, full duplex komunikacija, adresiranje... Kontrolu zagusenja ima TCP i sigurnost isporuke. IP ima kontrolu gresaka.TCP posle 3 way handshake radi u full duplex. Adresiranje recimo u LAN-u koji nije preveliki, koristimo MAC adrese za svicem umesto IP adresa sa rutiranjem.

4.Kao uslov dobili smo ta je  $t < L/R$  sto nam nista ne znaci. Kako je t zajednicko i za jedan i za drugi host koji salje podatke difuzno jer nije drugacije naglaseno, i kako je naglaseno da oni krecu slanje iste velicine podataka u isto vreme, tada ce do svica, hub-a ili drugog uredjaja stici u isto vreme => doci ce do kolizije.

5.1. osobina, kad samo jedan cvor salje, 3. decentralizacija i 4. jednostavan je. Ne postize prosečno R/N gde je R brzina a N broj cvorova. Izvedeno je da u proseku ako N cvorova salje podatke samo 37% zaista uspesno to uradi. Kod zetona, 1. do nekle jer ako jedan salje postoji kasnjenje

usled prozivanja, 2. da, jer se prosečno R/N postize brzina, 3. da, jer se predavanje zetona vrsi od hosta do hosta i 4. da

6. Posle 4. kolizije, adapter bira jedan broj iz zatvorenog intervala [0,31]. Verovatnoca da izabere 4 je 1/32. Kako je bitsko vreme dato formulom  $1/(\text{NIC speed})$  dobijamo za 10mbps da je 0.1 mikrosekunda. 512 bitskih vremena se cekaju za 1 tako da  $4 * 512 = 2048$ . Iz tog razloga, cekace 204.8 mikrosekundi.

7. Svaki ucesnik govori dok drugi slusaju, a sledeci govori u principu round-robina (setite se arosa). Ucesnik drzi casu vise koji prica a zatim spusta tako da sledeci moze da podigne i bude taj koji prica (kakvo pitanje takva i analogija...)

8. Jer bi cvor kreirao jedan okvir i poslao do sledeceg, koji bi poslao do sledeceg i tako u krug. To bi zahtevalo puno vremena.

9.  $2^{48} \cdot 2^{32} \cdot 2^{128}$

10. Adapter cvora C hoce obradivati do mreznog sloja ne ukljucujuci mrežno zaglavlje kako bi utvrdio da li je paket adresiran na njega. Nece slati mreznom sloju vec odbacuje paket. Izmenio bi se jer bi C tada paket tumacio da je adresiran i na njega kao i na B (u slucaju da ima vise hostova u LAN mrezi onda bi svi obradjivali pakete). U koliko je broadcast adresa, svaki host sem A (pa i C) bi procesuirao i prosledio paket mreznom sloju.

11. Zato sto host koji generise ARP zahtev ne zna MAC adresu racunara sa poznatom IP adresom za koju i salje upit. On ipak salje kao source MAC adresu svoju MAC adresu tako da je moguće adresirati odgovor na tacno odredjeni host koji je i poslao ARP zahtev.

12. Ne, svaki mrezni interfejs ima posebnu MAC adresu a ni jedan interfejs ne moze biti u dva LANa istovremeno

13. Ni u cemu.

14.2 (posto su ovo svicevi a ne ruteri) jedna je adresa intrne mreze druga interfejsa ka internetu

15. Kako protokol 802.1Q ima oznaku 12bitnu, moze podrzati  $2^{12}$  odnosno 4096 VLAN-ova

16. N sviceva, 1. i poslednji svic koriste 1 port za povezivanje sa srednjim N-2 sviceva koji koriste 2 porta. drugim recima  $2 \text{ porta} * (N-2)$  sviceva u sredini + 2 porta krajnjih sviceva (1. i poslednji) dobijamo  $2N-2$