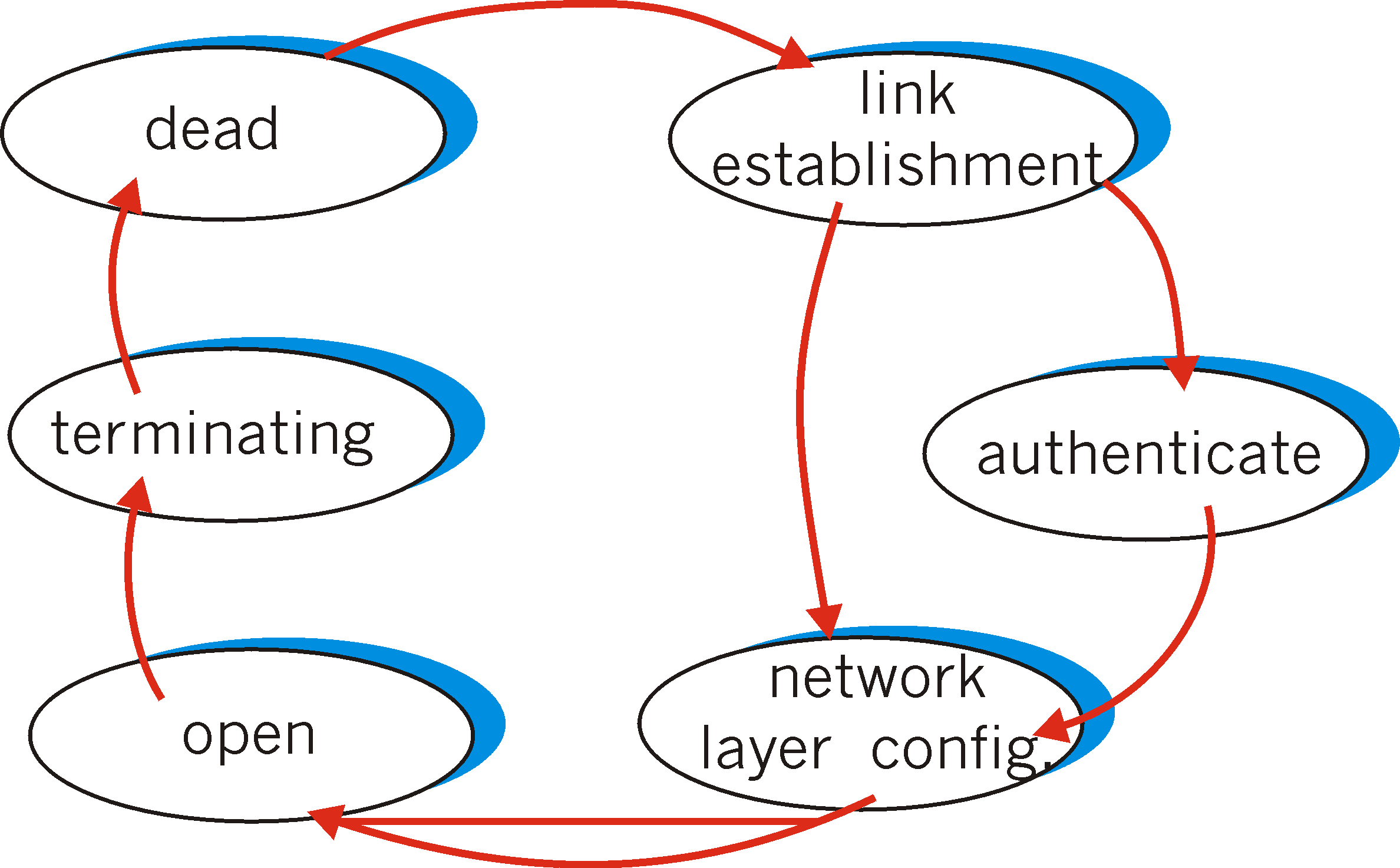
1. **.Koji od ISO nivoa se bavi:  
   -podelom niza bitova na okvire:**Ovu funkciju obavlja nivo veze (Data Link Layer), jer fizicki nivo samo prenosi sekvencijalno niz bitova.  
    **-odredjivanjem putanje poruka kroz komunikacionu podmrezu:**Ovu funkciju obavlja mrezni nivo na osnovu tablica – staticki ili dinamicki.
2. **Sledeci niz karaktera se nalazi u polju podataka: DLE, STX, A, DLE, B, DLE, ETX. Ako se koristi metod ubacivanja karaktera za postizanje transparentnosti podataka kako izgleda poruka u komunikacionom kanalu?**

DLE STX DLE DLE STX A DLE DLE B DLE DLE ETX DLE ETX  
Bajtovi | Podaci | Bajtovi  
za za  
ram ram

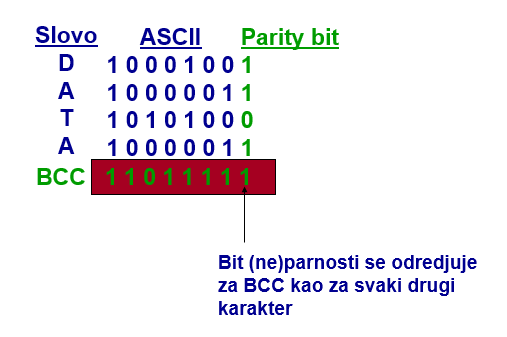
1. **Nacrtati dijagram promene stanja za PPP protocol.**

****

1. **Navesti razlike izmedju Distance Vector i Link State algoritama rutiranja (odakle prikupljaju podatke i kako ih prenose).**

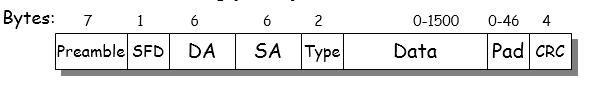
Kod *Distance Vector* algoritma svaki ruter ima tabelu sa vrstom, za svaki drugi ruter u mrezi, u kojoj se nalazi najpozeljnija linija za datu destinaciju i procena rastojanja do te destinacije. Ruter periodicno razmenjuje tablice rutiranja sa svojim susedima, obavi izracunavanja za sve svoje susede i odredi najmanja kasnjenja do svih rutera u mrezi.

Kod *Link State* algoritma ruter otkriva svoje susede slanjem HELLO poruke po svim Point-to-Point vezama i odredjuje njihove mrezne adrese. Kada se izmeri kasnjenje do svih suseda, konstruise se paket koji sadrzi sve sto ruter zna i salje taj paket svim ruterima. Najbolji put do svih rutera se racuna pomocu Dijkstrinog algoritma.

1. **Pobrojati i ukratko objasniti tri tehnike za detekciju gresaka.**-*Kontrolna cifra parnosti*: jedan bit se dodaje svakom karakteru (parna parnost – kada je broj jedinica paran u kodnoj reci i neparna parnost – kada je broj jedinica neparan u kodnoj reci). Omogucava otkrivanje jednostrukih gresaka, jer ako je jedan bit u toku prenosa bio narusen, primljeni bit ce se razlikovati od izracunatog. Ako paran broj bitova bude narusen, greska nece biti otkrivena. Otkriva pribizno 50% gresaka.  
     
   -*Kontrolna suma bloka*: Bloku koji se prenosi umesto jednog bita dodaje se jos jedan karakter (BCC – Block Check Character). BCC se odredjuje kao parity bit za svaku bitsku poziciju u bloku karaktera koji se prenose. Za svaki karakter se i dalje koristi parity bit. Povecana mogucnost gresaka.  
   ****

*-Checksum* – (kontrolne cifre se formiraju sabiranjem polureci u jedinicnom komplementu I komplementiraljem rezultata. ). Izracunava se sabiranjem decimalnih vrednosti svakog karaktera u poruci. Suma se podeli sa 255 i ostatak deljenja (jednobajtna vrednost) se koristi jao kontrola(checksum). Prijmenik po istom principu vrsi izracunavanje. Ako postoji razlika, detektuje se greska, i efikasnost mi je oko 95%.

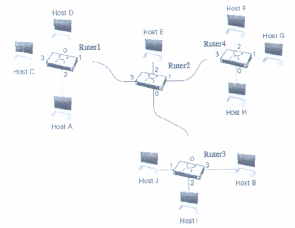
-*Polinomski kodovi (CRC-Cyclic Redundancy Code):* Elementi m-bitne poruke se posmatraju kao koeficijenti polinoma stepena m-1. Polinom koji odgovara poruci obelezimo sa M(X). Neka je r stepen generatorskog polinoma G(X), ciji stepen je manji od stepena polinoma M(X). Dodaje se r nula na kraj poruke, tako da ona sadrzi m+r bitova (Xr M(X)) i podeli se sa G(X). Oduzme se ostatak od Xr M(X) i to prestavlja rezultat sa CRC kodom, neko T(X). Kada poruka sa CRC kodom stigne u odrediste, vrsi se deljenje T(X) sa G(X), ako je ostatak 0 , nema greske u suprotnom greska postoji.

1. **Kako se vrsi numeracija poruka kod:  
     
   -Stani i cekaj protokola:** Dovoljno je izvrsiti numeraciju poruka po mod 2 (0 i 1), tako da su dve uzastopne poruke numerisane sa dva razlicita broja.  
    **-Vrati se nazad na N:** Neophodno je izvrsiti numeraciju poruka sa W+1 razlicitih rednih brojeva. W predstavlja velicinu prozora izvora. (W=3, => p = {0,1,2,3})  
    **-Selektivna retransmisija:** Da ne bi doslo do preklapanja dva susedna prozora, numeracija poruka se izvrsava sa 2W razlicitih rednih brojeva. (W=3 , => p = {0,1,2,3,4,5})
2. **Nacrtati format Ethernet rama i objasniti znacenje pojedinih polja.  
   **Preamble:  
    - 7 bajtova oblika 10101010 koji se koriste da se sinhronizuju brzine prenosa izvora i odredista.  
   - SFD – Start of Frame Delimiter 10101011 (pocetak rama).  
   DA i SA – adrese odredista i izvora velicine 6 byte, respektivno.  
   Type – Ukazuje na protokol viseg nivoa, uglavnom IP  
   Data – Polje podataka velicine 0-1500 byte.  
   Pad – nule koje se dodaju da bi se postigla minimalna velicina okvira od 0-46 byte, da bi se detektovala kolizija.  
   CRC – Polje za detekciju gresaka.
3. **Pretpostavimo da A, B i C jednovremeno prenose bit 0 (predstavljen -1V) koriscenjem CDMA sistema sa sekvencama (-1, -1, -1, +1, +1, -1, +1, +1),   
   (-1, -1, +1, -1, +1, +1, +1, -1) i (-1, +1, -1, -1, -1, -1, +1, -1) respektivno. Kako izgleda rezultujuci izlaz iz sitema?**

(3, 1, 1, 1, -1, 1, -3, 1)

1. **Za mrezu prikazanu na slici dati izgled tabela virtuelnih kola u svakom ruteru, pod pretpostavkom da numeracija virtuelnih kola pocinje od 0 u svakom hostu i da ni jedno virtuelno kolo u medjuvremenu nije zatvoreno, ako se redom uspostavlja konekcija izmedju sledecih hostova:**
   1. **A sa C**
   2. **D sa B**
   3. **D sa I**
   4. **A sa B**
   5. **F sa J**
   6. **H sa A**

????

****

1. **Objasniti rad i osobine mosta (bridge).**  
   To su uredjaji data link nivoa koji pamte i prosledjuju Ethernet ramove. Analiziraju zaglavlje rama i selektivno prosledjuju ram na osnovu odredisne MAC adrese. Koristi CSMA/CD za pristupanje segmentima. Mostovi se ne konfigurisu, to su samo-uceci uredjaji. Transparenti: hostovi nisu “svesni” prisustva mostova (bridges). Postavljanje mosta deli jedinstveni LAN na LAN segmente i odvojene kolizione domene. Mostovi filtriraju pakete: Ramovi koje treba proslediti u isti LAN segment se ne prosledjuju drugim LAN-segmentima. Segmenti postaju odvojeni domeni kolizije. Kako utvrditi na koji LAN segment proslediti ram? Na osnovu tabele koju poseduje most (bridge). Svaki most poseduje tabelu (bridge table) koju stalno ažurira. Vrsta tabele sadrži: Adresu LAN čvora, oznaku interfeisa mosta, vreme kreiranja); Stari zapisi u tabeli se brišu (posle 60 min). Mostovi *uče* preko kog interfeisa se može pristupiti odredjenom hostu. Kada ram stigne u most, most “uči” (saznaje) lokaciju pošiljaoca (izvora), tj. detektuje sa kog LAN segmeta pristiže ram. Pravi zapis u tabeli: adresa i broj interfeisa i vreme.

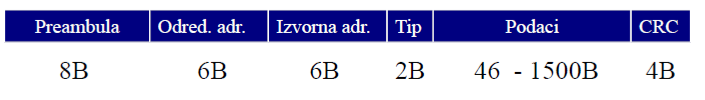
Neke osobine mosta: Izoluje domene kolizije i na taj nacin povecava maksimalnu propusnost LANa. Moze povezati Ethernet-e razlicitog tipa (10BaseT , 100BaseT). Relativno mali broj cvorova se moze povezati jednim mostom.

1. **Objasniti pojam brojanja do beskonacnosti kod Distance Vector algoritma za rutiranje.**Kod ovog algoritma susedni ruteri periodicno razmenjuju svoje tabele rutiranja i na osnovu njih vrse izracunavanja i odredjuju najkrace puteve do svih rutera. U slucaju da jedan ruter otkaze, ostali ruteri ce i dalje izmedju sobom razmenjivati tabele rutiranja u kojima se i dalje nalazi neki put do tog rutera koji vise nije u funkciji. Kako ruter od svog suseda dobije broj skokova do tog rutera, on toj vrednosti dodaje 1, jer to predstavlja skok do tog suseda od koga je naucio koliko je udaljen ruter koji je otkazao. I pri svakoj razmeni tabela, vrednost najkraceg puta do nefunkcionalnog rutera se u tabelama svih rutera postepeno povecava, odnosno sporo konvergira ka resenju (broji do beskonacnosti).
2. **Pobrojati redom nivoe u OSI referentnom nivou.**1.Fizicki nivo  
   2.Nivo veze (Data Link).  
   3.Mrezni nivo.  
   4.Transportni nivo.  
   5.Nivo sesije.  
   6.Prezentacioni nivo.  
   7.Aplikativni nivo.
3. **Kako se ponasa izvor kada primi naruseni ACK ram u slucaju:  
     
   -Selektivne retransmisije:** Izvor vrsi retransmisiju samo poruke za koju nije primio potvrdu (ne pravi se razlika izmedju narusavanja I-rama i ACK rama).  
    **-Vrati se nazad na N:** Nakon isteka time outa, izvor otpocinje sa slanjem I-ramova pocev od rama za koji je dobio naruseni ACK.
4. **Postoje tri velike klase MAC protokola. Koje su to? Ukratko objasniti kako rade.**-*Protokoli sa podelom kanala (Channel Partitioning):* Kanal se deli na manje delove (vremenske slotove (TDMA), frekvencije (FDMA), kodove (CDMA)). Kod TDMA pristup kanalu se obavlja kruzno, u ciklusima. Svaki cvor dobija vremenski interval fiksne velicine i ako nema podataka za slanje slot ostaje neiskoriscen. Kod FDMA kanalni spektar je podeljen na frekventne bandove i svakoj stanici je dodeljen fixni frekventni band. Ako nema podataka za slanje, band ostaje prazan. Kod CDMA je svakom korisniku dodeljen jedinstveni kod (sifra). Svi korisnici koriste istu frekvenciju, ali svaki korisnik ima svoju kodnu sekvencu za sifriranje podataka.  
     
   -*Protokoli sa slucajim pristupom (Random Access):*Kada cvor ima paket za slanje, prenosi ga punom brzinom kanala. Ako dva ili vise cvorova prenose nastaje kolizija. Ovaj protokol definise: kako se detektuje kolizija, kako se vrsi oporavak od kolizije. Primeri su ALOHA, slotted ALOHA i CSMA, CSMA/CD.

-*Protokoli sa definisanim redosledom pristupa (Taking Turns):*Javljaju se u dva vida: sa prozivkom i sa zetonima. U slucaju sa prozivkom, master cvor poziva sluge cvorove da obave prenos. U drugom slucaju se kontrolni zetoni prenose od cvora do cvora sekvencijalno i samo vlasnik zetona ima pravo prenosa. Nakon obavljenog prenosa oslobadja se zeton.

1. **Navesti bar tri opcije o kojima se moze pregovarati u toku uspostavljanja PPP konekcije.**Strana koja zeli uspostavljanje veze salje ram za konfigurisanje veze koriscenjem configure-request rama. Druga strana odgovara sa configure-ack ramom (ako su opcije prihvatljive) ili configure-nak (ako su opcije shvacene ali nisu prihvatljive) ili configure-reject (opcije nisu prepoznatljive ili prihvatljive). ????  
   Maksimalna velicina rama, specifikacija protokola za autentifikaciju, opcije da se preskoci koriscenje address I control polja u ppp ramu.
2. **Koliko OSI nivoa imaju sledece mrezne komponente i koji su to nivoi:  
   -Hub:   
   -Bridge  
   -Switch  
   -Router**
   1. 1 – fizicki
   2. 2 – fizicki, nivo veze
   3. 2 – fizicki, nivo veze
   4. fizicki, nivo veze, mrezni nivo
3. **Sta rade hub-ovi i repeater-i?**

Repeater pojacava dolazni signal, sluzi za prenosenje signala na velike daljine. Hub je repeater sa vise portova.  
Hub-ovi su u sustini repeateri gde bitovi koji dolaze po jednom interfejsu se prosledjuju na sve ostale. Ne može povezati dva segmenta sa različitim brzinama prenos. Port se iskljucuje posle 30 uzastopnih kolizija. Povećava maksimalno moguće rastojanje izmedju čvorova. ????

1. **Sta znaci skracenica CSMA/CD?**CSMA/CD – Carrier Sense Multiple Access With Collision Detection  
   Osluskivanje nosioca signala sa detekcijom kolizije
2. **Zasto je minimalna velicina Ethernet rama 64 byte ?**Minimalna velicina Ethernet rama je 64 byte iz razloga sto se ne racuna preambula (koja sluzi za sinhronizaciju brzina prenosa podataka izmedju izvora i odredista) I sfd  
   ****  
   Sabiranjem vrednosti za izvornu i odredisnu adresu, tip protokola, dela za podatke i CRC kod, dobija se da je minimalna vrednost Ethernet rama 64 byte.

**????** sto se ne racuna preambula? I valjda nisu podaci 46-1500, nego od 0 I Pad koji je od 0-46

1. **Koliko bitova ima Ethernet adresa?**Ethernet adresa je fizicka adresa i ima 48bitova.
2. **Kako se ponasa Ethernet kada detektuje koliziju?**Posle detektovanja kolizije adapter ulazi u eksponencijalno povlacenje (Exponential Backoff), sto znaci da, posle i-te kolizije adapter ceka K\*512 bitskih intervala, pri cemu K bira slucajno iz intervala {0,1,2,…2i-1}, nakon cega opet osluskuje kanal i ako je slobodan pocinje sa prenosom ramova.
3. **Koje informacije se prenose u slucaju  
   -Distance Vector:** Razmenjuju se liste ustanovljenih kasnjenja.(slanjem echo paketa) **-Link State:** Prenosi se paket koji sadrzi sve informacije koje ruter zna o drugim ruterima.

**?**????

**Od kojih rutera se primaju informacije kod   
-Distance Vector:** Informacije se primaju od susednih rutera. **-Link State:** Informacije se primaju od svih rutera u mrezi.  
????

Mislim da je neka malena greskica ovde xd nista mi nije jasno

1. **Objasniti split horizon kao tehniku za resavanje brojanja do beskonacnosti kod distance vector algoritma.**Koristi se princip da ako ruter Z koristi ruter Y da stigne do rutera X, onda ce tokom razmene tablica Z reci Y da ima beskonacno rastojanje do X, i tako ce Z nastaviti da govori laz rutetu Y sve dok put do rutera X vodi preko njega. Kako Y veruje da Z nema put do X , tako nece nikad pokusati da do X stigne preko Z.
2. **Objasniti kako bridge formira tablicu prosledjivanja.**Tablica sadrzi adresu LAN cvora, oznaku interfejsa mosta i vreme kreiranja. Stari zapisi se brisu posle 60min. Mostovi uce preko kog interfejsa se moze pristupiti odredjenom hostu. Kada ram stigne u most on uci lokaciju izvora, odnosno detektuje sa kog LAN segmenta pristize ram. Onda pravi novi zapis u tabeli gde unosi adresu i broj interfejsa i vreme kreiranja.
3. **Dati izgled Link State paketa i objasniti znacenja pojedinih polja.  
     
   **Adresa izvora – adresa rutera ciji je paket  
   Redni broj – redni broj paketa  
   Starost – Broj koji se dekrementira svaki put kada prodje kroz neki ruter. Kada dostigne 0 odbacuje se.  
   Lista suseda – Adrese susednih rutera  
   Kasnjenje – Vreme od slanja paketa do pristizanja odgovora za datog suseda.
4. **Koje tvrdnje se odnose na Distance Vector, a koje na Link State (zaokruziti):  
   -LS, DV: Zahteva poznavanje kompletne topologije mreze.** (LS) ???? **-LS, DV: Salje kompletnu tabelu rutiranja svojim susedima** (DV)???? **-LS, DV: Koristi bujicu** (LS) **-LS, DV: Ima problem brojanja do beskonacnosti** (DV)
5. **Koja je razlika izmedju konekciono orijentisanog i beskonekcionog servisa. Imenovati 4 protokola, koji su obradjeni na predavanjima, I za svaki navesti da li je kon. Ili bezkn orjentisan. Navesti bar jedan primer.***Konekcioni servis* je implementiran preko virtuelnog kanala. Pre pocetka slanja podataka, salje se specijalni paket CALL REQUEST kojim se uspostavlja veza i odredjuje put izmedju izvornog i odredisnog hosta. Paket sadrzi adresu izvora, adresu odredista i broj virtuelnog kanala. Kada se veza uspostavi, svi paketi koriste isti put od izvora do odredista.  
     
   *Bezkonekcioni servis* se realizuje preko datagrama gde nema inicijalnog uspostavljanja veze. Svaki paket se salje nezavisno od prethodnog i sadrzi punu adresu izvora i odredista. Paketi mogu putovati razlicitim putanjama i pristizati u odrediste van redosleda slanja.

**-** IP pruža bezkonekcioni servis transportnom nivou (Ne obavlja nikakvu kontrolu grešaka.)

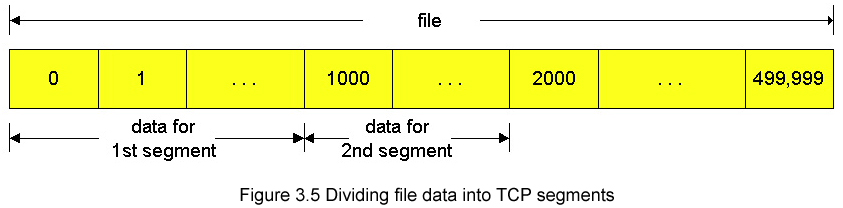
- ICMP bezkonekcioni ; ne obavlja nikakvu kontrolu grešaka (ne koriguje greške, on samo raportira izvoru da je nastupila greška)

- ARP konekcioni

- DHCP konekcioni

1. **Sta se podrazumeva pod kontrolom gresaka a sta pod kontrolom toka?**  
   Pod kontrolom gresaka se podrazumeva kako odrediste moze da utvrdi da je poruka korektno primljena ili kako izvor moze da utvrdi da li je poruka korektno stigla u odrediste. Da bi odrediste utvrdilo da li je poruka korektno primljena, moraju se dodati kontrolni bitovi u poruci koja se prenosi, a da bi izvor utvrdio da li je poruka korektno stigla u odrediste koristi se mehanizam potvrdjivanja.  
   Kod kontrole toka problem nastaje kada posiljalac salje frejmove brze nego sto je primalac u stanju da ih primi. Da bi se sprecilo prenatrpavanje primaoca i gubitak poruka uvodi se kontrola toka koja je organizovana kao povratna sprega. Primaoc vraca posiljaocu informaciju sta je primio omogucavajuci da nastavi sa slanjem novih frejmova.
2. **Kako se resava problem pojavljivanja kontrolne sekvence koja oznacava kraj okvira(frame) ako se za uramljivanje koriste specijalni karakteri a kako kada se koristi specijalni bajt?**Ako se koristi uramljivanje karakterima, nivo veze na izvornoj strani posle nailaska DLE karaktera ubacuje jos jedan DLE karakter. Kada se u odredistu detektuju dva uzastopna DLE karaktera, drugi se odbacuje i na taj nacin je sekvenca DLE ETX ucinjena jedinstvenom.  
   Specijalni bajt je oblika 01111110. Nivo veze u izvoru automatski nakon nailaska 5 uzastopnih jedinica u polju podataka ubacuje nulu. U odredistu se automatski brise nula nakon 5 uzastopnih jedinica.
3. **Narcrtati izgled polja CONTROL za informacione, supervizorske i nenumerisane ramove kod HDLC protokola i objasniti znacenje pojedinih polja.**-Informacioni ram  
     
   ****  
     
   P/F: Poll/Final – bit prozivke u komandama, krajnji bit u odgovorima  
   N(S): Redni broj rama  
   N(R): Redni broj rama koji se ocekuje (sluzi za potvrdjivanje)  
     
   -Nenumerisani ram  
     
   ****Koriste se za uspostavljanje i raskidanje veze. Ne numerisu se i ne sadrze informacije o potvrdjivanju.  
     
   -Supervizorski ram  
     
   ****  
   Koriste se za kontrolu toka i kontrolu gresaka kada druga strana nema poruka za slanje.00 – RR(Receave Ready). 01 – RNR(Receave Not Ready). 10 – REJ (Reject) – nastupila greska u toku prenosa – zahteva se retransmisija po pirncipu gp-back-n. 11 – SREJ – selektivna retransmisija. N(R) – redni broj poruke koja se ocekuje da se primi.
4. **Objasniti kako se vrsi distribucija Link State paketa.**Za distribuciju Link State paketa koristi se bujica. Svaki paket sadrzi redni broj koji se inkrementira kod slanja svakog novog paketa. Ruteri vode racuna o svakom paru (izvor , redni broj) koji su videli. Ako je paket vec vidjen ruter ga odbacuje, inace ga salje po svim linijama izuzev one po kojoj je dobio paket. Ako se primi paket sa rednim brojem koji je nizi od vec vidjenog, paket se odbacuje kao zastareo.

**II Kolokvijum**

1. **Navesti primitive pomocu kojih se uspostavlja konekcioni transportni servis.**- LISTEN – server izvrsava listen. Server se blokira dok se ne pojavi klijent.  
   -CONNECT – klijent izvrsava connect. Transportni nivo blokira klijenta, salje connection request serveru. Transportni entitet proverava da li je server blokiran na listen, ako jeste onda salje connection accepted klijentu. Po prijemu klijent se deblokira i veza je uspostavljena.  
   - SEND/RECEIVE – primitive za razmenu informacija.  
   - DISCONNECT – bilo koja strana moze izdati disconnect primitivu za raskidanje veze.
2. **Kako se obavlja numeracija segmenata kod TCP?**Redni brojevi oznacavaju redne brojeve prenetih bajtova, a ne segmenata. Redni broj segmenata jednak je rednom broju prvog bajta u segmentu. Npr. ako niz podataka sadrzi 500.000 bajtova, a maksimalna velicina segmenta je 1000 bajtova, bice 500 segmenata. Ako je prvi bajt numerisan sa 0, prvi segment dobija redni broj 0, drugi 1000, treci 2000 itd.  
   
3. **Kako se obavlja kontrola toka kod TCP?**Kontrola toka se obavlja koriscenjem WIN polja u TCP segmentu koje kazuje koliko bajtova moze biti poslato, pocev od potvrdjenog. WIN = 0 kaze izvoru da privremeno prestane sa slanjem.  
   Mislim da se ovo odnosi na to sta radi izvoriste a sta odrediste kada se salju paketi

Tipa da izvoriste salje pakete onoliko koliko mu je prozor

Da kada odrediste primi paket salje ACK brojem sledeceg paketa koji ocekuje.Sta se desava ako stigne nesto preko reda, kada se vrsi retransmisija, sta se retransmituje ?????  
****

1. **Pomocu kojih prozora TCP obavlja kontrolu zagusenja?**

Trenutna veličina prozora izvora definiše količinu podataka koja u datom trenutku može biti poslata. Mali prozor – mala količina podataka, veliki prozor – velika količina podatakaTCP obavlja kontrolu zagusenja podesavajuci velicinu prozora izvora trenutnim mogucnostima mreze. TCP koristi dve vrednosti: prozor zagusenja i prozor koji je odobrilo odrediste, da bi drzao zagusenje pod kontrolom. Npr. ako je odrediste odobrilo velicinu prozora 8KB, a prozor zagusenja je 4KB, poslace se 4KB. Ako je odrediste odobrilo 8KB, a prozor zagusenja je 32KB, poslace se 8KB.

1. **Koji tipovi servera imena (name server) postoje?**Postoje cetiri tipa servera imena:
   1. Lokalni serveri imena
   2. Root serveri imena
   3. Serveri visih domena (Top-Level Domain - TLD)
   4. Autorizovani serveri imena
2. **Kako izgleda struktura zapisa u bazi servera imena (resource records)?  
     
     
     
   Type = A**

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

**name** je ime hosta; **value** je IP adresa hosta;  
(relay1.bar.foo.com, 45.37.93.126, A)  
  
**Type = NS  
name** je domen; **value** je ime autorizovanog DNS servera za ovaj domen;  
(foo.com, dns.foo.com, NS)  
  
**Type = CNAME  
name** je alias za neko kanonicko (realno) ime; **value** je kanonicko ime;  
(www.ibm.com, servereast.backup2.ibm.com, CNAME)  
  
**Type = MX  
value** je ime mail servera koji ima alias **name;**(foo.com, mail.bar.foo.com, MX)

1. **U cemu je razlika izmedju iterativnih i rekurzivnih DNS upita?**Kod rekurzivnih upita teziste razresenja imena je na kontaktiranom name serveru.

• Host cis.poly.edu želi IP adresu hosta gaia.cs.umass.edu 1. host kontaktira lokalni DNS server 2. Lokalni DNS server konatktira root DNS server 3. Root DNS server kontaktira TLD DNS server 4. TLD kontaktira autorizovani DNS server 5. autorizovani DNS server odgovara TLD serveru IP adresom hosta 6. TLD prosledjuje odgovor root DNS serveru 7. root DNS server prosledjuje odgovor lokalnom DNS serveru 8. lokalni DNS server prosledjuje odgovor hostu cis.poly.edu

Kod iterativnih upita kontaktirani name server odgovara IP adresom sledeceg name servera u nizu, radi po principu “ne prepoznajem ovo ime, ali pitaj ovaj server”.

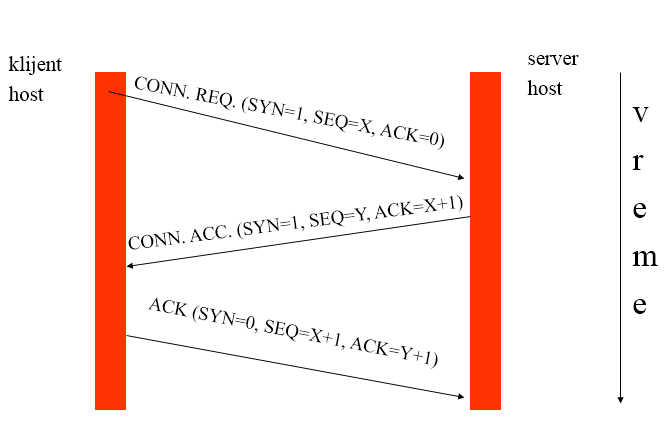
• Host na cis.poly.edu želi IP adresu za gaia.cs.umass.edu 1. host kontatktira svoj lokalni DNS server 2. lokalni DNS server kontaktira root DNS server 3. root DNS server odgovara adresom TLD DNS servera 4. lokalni DNS server kontaktira TLD DNS server 5. TLD DNS server odgovara adresom autorizovanog DNS servera 6. lokalni DNS server kontaktira auorizovani DNS server koji vraća IP adresu hosta gaia.cs.umass.edu

1. **Sta je ICMP i cemu sluzi?**ICMP (Internet Control Message Protocol) je protokol koji koriste hostovi i ruteri za razmenu upravljackih paketa. ICMP ne koriguje greske, on samo obavesti izvor da je nastupila greska. ICMP se cesto tretira kao deo IP, ali se u protokol steku on hijerarhijski nalazi iznad IP jer se ICMP poruke prenose preko IP paketa. Postoji 13 tipova ICMP poruka i svaka je enkapsulirana u IP paketu.

Moze da se koristi za otkrivanje da li je neki destination aktivan slanjem echo “paketa”, moze da signalizira da treba da se upori/obustavi slanje paketa jer je bafer odredista pun itd

1. **Objasniti kako se uz pomoc ARP ostvaruje preslikavanje IP adresa u fizicke adrese.**

ARP protocol omogućava preslikavanje IP adresa u adrese data link nivoa. Prvo treba da znamo o kojoj IP adresi je rec. IP saznajemo na osnovu DNS (deo aplikativnog nivoa). Softver višeg nivoa gradi paket sa tom IP adresom u polje „adresa odredišta“ i predaje ga IP softveru za prenos. IP softver može da ustanovi da je destinacija u sopstvenoj mreži, ali mu je potrebna ETHERNET adresa odredišta. Jedno rešenje je da postoji konfiguracioni fajl koji pamti preslikavanje IP adrese u ETHERNET. Drugo recenje je da host posalje broadcast paket na Ethernet i pita ko poseduje tu IP adresu. Poruka ce stici do svih masina na tom Ethernetu i svaka ce proveriti svoju IP adresu. Onaj host koji ima tu IP adresu odgovorice svojom Ethernet adresom. Protokol kojim se postavalja pitanje i dobija odgovor je ARP.

1. **Objasniti uspostavljanje veze izmedju klijenta i servera na transportnom nivou ako se koristi TCP protokol.**Veza se uspostavlja 3-way handshake procedurom. Server pasivno ceka i izvrsava listen i accept primitive. Klijent izvrsava connect primitivu, definisuci IP adresu i broj porta sa kojim zeli da upostavi vezu i maksimalnu velicinu segmenta koji moze da prihvati. Connect primitiva salje segment sa SYN = 1 i ACK = 0 i ceka odgovor. Kada segment stigne u odrediste i ako neki proces osluskuje dati port, TCP mu prosledjuje taj segment. Proces moze da prihvati ili odbije vezu. Ako u klijent stigne segment potvrde konekcije (connection accept), on salje potvrdu sa SYN = 0. Okoncanje vece se uspostavlja slanjem PIN=1 signala s bilo koje strane.  
     
   ****
2. **Objasniti brzu retransmisiju kod TCP.**Ako se desi da je segment izgubljen a da je time-out predugacak moze se dugo cekati pre nego sto se izvrsi retransmisija. Izvor moze detektovati gubitak segmenta pre isteka time-outa tako sto ce primiti duplirani ACK. To je ACK koji ponovo potvrdjuje segment za koji je ranije primljena potvrda. Kada prijemnik primi segment sa rednim brojem koji je veci od ocekivanog, on detektuje nedostajuci segment. TCP ne koristi NAK tj. negativne potvrde, nego kad stigne segment van redosleda posalje ACK za poslednji korektno primljeni segment sa ocekivanim rednim brojem, odnosno generise duplikat ACK. Kada izvor tri puta primi ACK za isti segment pre nego sto istekne time-out, on vrsi retransmisiju nedostajuceg segmenta.
3. **Da li je TCP protokol tipa “vrati se nazad na N” ili “selektivne retransmisije”?**TCP je hibridni protokol jer ne potvrdjuje segmente koji su primljeni van redosleda i vrsi retransmisiju samo segmenata za koji je istekao time-out.

**????? sto znaci selektivna?**

TCP protokol ima hibridnu kontrolu toka. Nije vrati se nazad na N jer radi retransmisiju samo za segment kome je istekao time-out, a nije selektivna retransmisija jer ne potvrdjuje segmente koji stignu van redosleda.

1. **Pretpostavimo da ste osnovali kompaniju SNOOPY i da zelite da je registrujete pod tim imenom ispod domena .RS. Ime vaseg autorizovanog servera imena je dns1.snoopy.rs, mail servera mail.snoopy.rs i web servera www.snoopy.rs. Objasniti koje zapise je neophodnoo ubaciti u DNS bazu TLD servera za domen RS, a koje u autorizovani server dns1.snoopy.rs da bi moglo da se iz spoljnjeg sveta pristupi vasem web serveru i mail serveru.**U TLD za domen RS:  
   (snoopy.rs, dns1.snoopy.rs, NS)  
   (dns1.snoopy.rs, 212.19.43.1, A) **????**  
     
   U autorizovani server dns1.snoopy.rs:  
   (www.snoopy.rs, 212.19.43.21, A)  
   (mail.snoopy.rs, 212.19.43.25, MX)

**------------------------------------------**

(snoopy.rs, dns1.snoopy.rs, NS)

([www.snoopy.rs](http://www.snoopy.rs), snoopy.rs, CNAME)  
(snoopy.rs, mail.snoopy.rs, MX)

**????**

1. **Ukratko objasniti NAT i kako funkcionise.**NAT (Network Address Translation) omogucava da lokalna mreza koristi samo jednu IP adresu sto se tice spoljasnjeg sveta. NAT vrsti prevodjenje lokalnih u javne adrese. Motivacija: Ušteda IP adresa .

NAT ruter mora da :



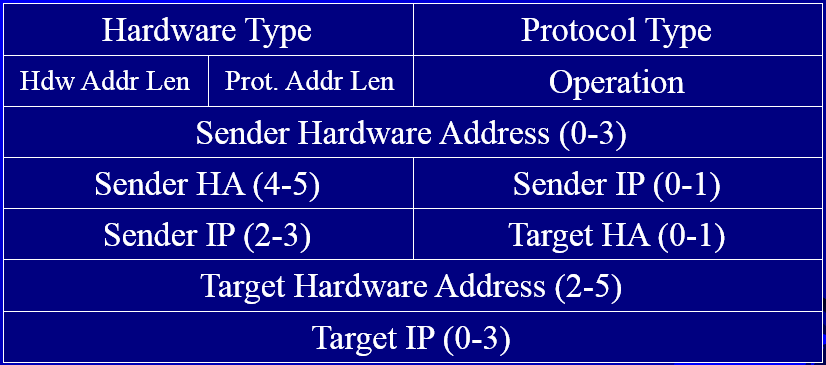
za odlazne datagrame : zameni (izvorišnu IP adresu, broj porta) svakog odlaznog datagrama sa (NAT IP adresu, novi broj porta) . . . udaljeni klijenti/serveri će odgovarati koristeći (NAT IP adresu, novi broj porta) kao odredišnu adresu.



zapamti ( u N A T tabeli r ansliranja ) sve translacije sa (adresu izvorišta IP, broj porta) na (NAT IP adresu, novi broj porta)



za dolazne datagrame : zameni (NAT IP adresu, novi broj porta) u poljima odredišta svakog dolazećeg datagrama sa odgovarajućom (izvorišnom IP adresom, brojem porta) uskladištenim u NAT tabeli

1. **Ko obavlja preslikavanje logickog imena hosta u IP adresu? Ko obavlja preslikavanje IP adrese u fizicke adrese? Gde se ovi protokoli nalaze u protokol steku?**Preslikavanje logickog imena hosta u IP adresu obavlja DNS (Domain Name System) koji je deo aplikativnog nivoa. A preslikavanje IP adrese u fizicke adrese obavlja ARP (Address Resolution Protocol) koji je deo nivoa veze.
2. **Ako je adresa oblika 200.23.30.14/20, koja je adresa mreze?**11001000 00010111 00011110 00001110 – adresa 200.23.30.14  
   11111111 11111111 11110000 00000000 – maska 255.255.240.0  
   11001000 00010111 00010000 00000000 – adresa mreze 200.23.16.0/20
3. **Nacrtati format ARP poruka i objasniti znacenje pojedinih polja.  
     
     
     
   //objasnjenje nema na prezentacijama**
4. **Objasniti zasto se kontrolna suma u zaglavlju IP paketa mora ponovo odredjivati pri svakom prolasku kroz ruter.**Kontrolna suma se mora ponovo odredjivati iz razloga sto se polje TLL, odnosno polje vreme zivota dekrementira pri svakom prolasku kroz ruter. To je brojac koji sluzi da se ogranici vreme zivota paketa, da ne bi beskonacno kruzili kroz mrezu. To vreme iznosi 255 sekundi. Kada dosegne vrednost 0, paket se odbacuje.
5. **Navesti koji se segmenti razmenjuju kod uspostavljanja TCP veze.**Kada klijent izvrsi CONNECT primitivu, ona salje segment sa SYN = 1 i ACK = 0 i ceka odgovor. Kada segment stigne u odrediste on moze biti prihvacen SYN = 1 i ACK = 1, ili odbijen RST =1. Ako u klijentu stigne segment potvrde konekcije on salje potvrdu sa SYN = 0; Za prekidanje veze se salje PIN=1;
6. **Gde se SSL nalazi u protokol steku? Od kojih protokola se sastoji SSL protokol?  
     
   **

SSL se sastoji od dva podprotokola

- Protokol za uspostavljanje bezbedne konekcije

- Protokol koji koristi bezbednu konekciju za prenos podataka

1. **Ako Alisa zeli da posalje digitalno potpisanu poruku Bobu, koji od dole navedenih kljuceva ce koristiti:**
   1. **Alisin javni kljuc** za desifrovanje
   2. **Alisin tajni (privatni) kljuc** za sifrovanje
   3. **Bobov javni kljuc**
   4. **Bobov tajni (privatni) kljuc**

Alisa ne moze poreći da je ona poslala poruku jer se digitalni potpis moze dešifrovati jedino njenim javnim ključem, a šifrovati njenim tajnim ključem!

1. **Ako Alisa zeli da posalje sifrovanu poruku Bobu, koji od dole navedenih kljuceve ce koristiti:**
   1. **Alisin javni kljuc**
   2. **Alisin tajni (privatni) kljuc**
   3. **Bobov javni kljuc**
   4. **Bobov tajni (privatni) kljuc**

?????

c.Bovov javni kljuc

1. **Pobrojati redom korake prilikom kreiranja digitalnog potpisa.**

1. Hash funkcijom posiljalac računa sažetak poruke koju šalje primaocu

2. Posiljalac šifrira svojim tajnim ključem sažetak poruke i na taj način kreira digitalni potpis.

3. Zajedno s orginalnim dokumentom Posiljalac šalje i digitalni potpis.

4. Primalac dobija potpisanu poruku. Iz orginalne poruke izračuna sazetak.

5. Primalac dešifruje digitalni potpis posiljaocevim javnim ključem i uporedjuje dešifrovani sazetak sa onim koji je sam izračunao.

Ako su jednaki, Primalac je siguran da je posiljalac poslao poruku i da poruka nije menjana tokom slanja (integritet poruke). Posiljalac ne moze poreći da je on poslao poruku jer se digitalni potpis moze dešifrovati jedino njegovim javnim ključem, a šifrovati njegovim tajnim ključem!

1. **Navesti osobine hash funkcije.**

Funkcija sazetka **H** (eng. hash) je jednosmerna funkcija koja ulazni niz proizvoljne dužine, poruku m, pretvara u niz fiksne dužine (najčešće 128-256 bita) koji se naziva sažetak poruke **h** (message digest). **h=H(m)**

Iz dobijenog sažetka poruke **h** je nemoguće dobiti izvornu poruku m, zbog jednosmernosti funkcije sažetka, te je na taj način osiguran **integritet** poruke.

Svojstvo funkcije sažetka je da i najmanja promena orginalne poruke uzrokuje drastične promena u njenom sažetku.

Verovatnoća da se za dve različite poruke generiše isti sažetak je jako mala.

Sažetak poruke je i prvi korak u kreiranju digitalnog potpisa - izračuna se sažetak orginalnog dokumenta koji se digitalno potpisuje.

1. **Koja osobina RSA algoritma je kljucna za kreiranje digitalnog potpisa?**

Potrebno je da algoritam za šifriranje i dešifriranje sa javnim ključem ima osobinu

E(D(P))=P, pored uobičajene, D(E(P))=P**,** ( E je javni ključ za šifriranje a D tajni ključ za dešifriranje). RSA algoritam ima ovu osobinu!

1. **Korisnik na hostu PC1 B1 na Slici 1 ne može da pristupi Serveru A. On može pristupiti Serveru B i hostu PC B2. Korisnik na hostu PC B2 može da pristupi Serveru A. Šta je od navedenog najverovatniji uzrok problema:** 
   1. Tačan odgovor donosi 3 poena

A. Hub ne funkcioniše korektno

B. Ruter B ne funkcioniše korektno

C. PC B1 ima pogrešno konfigurisan default gateway.

D. Server A nije povezan na mrežu.

|  |  |
| --- | --- |
|  |  |

**Slika1**  **Slika 2.**

1. **Za mrežu na Slici 2 odgovoriti:** 
   1. Svaki tačan odgovor sa korektnim obrazloženjem nosi po 2 poena. Svi tačni odgovori daju dodatni bonus od 1 poena.
   2. **Da li hostovi A i C imaju iste mrežne delove IP adrese? Obrazložiti odgovor**.
      * Da, Host A može direktno pristupati hostu C na data link nivou, jer je most transparentan za hostove.
   3. **Da li host C može pristupiti serveru WWW u isto vreme kada host B pristupa Internetu preko rutera? Obrazložiti odgovor.**
      * Da. U ovom slučaju most neće proslediti (forward) saobraćaj iz segmenta S1 u S2. Ova dva segmenta predstavljaju posebne (odvojene) kolizione domene
   4. **Može li host A pristupiti serveru WWW u isto vreme kada host B pristupa Internetu preko rutera? Obrazložiti odgovor.**
      * Ne. Host A koristi isti mrežni segment (S1) koji koriste host B i www server
   5. **Kada host A šalje ARP upit da bi doznao adresu data link nivoa rutera, da li do hosta C dolazi ovaju upit? Obrazložiti odgovor.**
      * Da. Host A šalje BROADCST ram (frame) i most će proslediti ovaj ram na drugi mrežni segment.
2. **Da bi proverio da li se može pristupiti novopridodatom hostu 192.168.2.5 , mrežni administrator je u komand promptu otkucao ping 192.168.2.5. Koji protokoli su korišćeni tokom ovog testiranja:** 
   1. Zadatak nosi 4 poena (2+2)

(a). ARP (b). RARP (c). DHCP (d). DNS (e). ICMP

1. **Fakultetska mreža je napravljena kao jedinstvena LAN. Odlučili ste da segmentirate ovu LAN na dve mreže pomoću rutera. Šta će biti efekat ove promene:** 
   1. Zadatak nosi 2 poena

A. Broj broadcast domena će se smanjiti.

B. Povećaće se broj kolizija

C. Sprečiće se da broadcast iz segmenta 1 stigne do segmenta 2

D. Broadcast iz segmenta 1 će stići do segmeta 2

1. **Koji uređaj prosleđuje podatke svim hostovima u jednom LAN segmentu:**
   1. Zadatak nosi 2 poena
      * 1. hub B. router C. switch D. gateway
2. **Šta je od sldećeg validna karakteristika mosta (bridge)**
   1. Svaki tačan odgovor nosi 1 poen (ukupno 4)

A. Most ne može obavljati rutiranje

B. Most može filtrirati podatke između mrežnih segmenata

C. Most može povezati segmente sa različitim brzinama prenosa

D. Most se može iskoristiti da se poveća maksimalno rastojanje između hostova

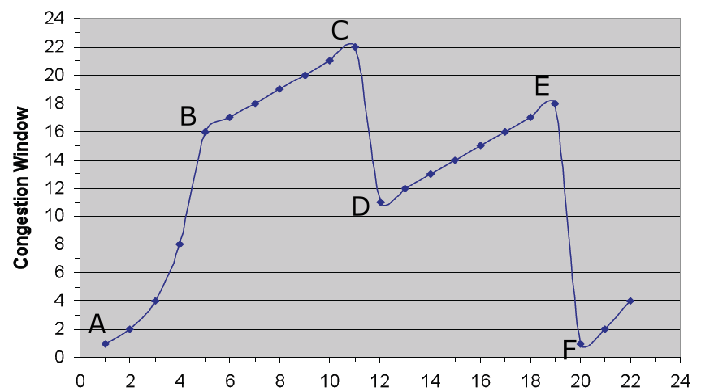
1. **Kolika je veličina zaglavlja kod IPv6:**
   1. Zadatak nosi 2 poena

a) ista kao kod IPv4 b) promenljiva c) 20 byte d) 40 byte e)60 byte

1. **IPv6 adresa može imati do \_\_\_\_32\_\_\_\_ hexadecimalne cifre.**
   1. Zadatak nosi 2 poena

a) 16 b) 32 c) 8 d) none of the above

1. **Na slici dole je prikazana promena veličine prozora zagušenja kod TCP protokola. Za svaku od tačka označenih sa A, B,..., F navesti koji su događaji nastupili i vrednosti karakterističnih parametara (veličina prozora zagušenja, prag sporog starta)**



* 1. Zadatak nosi 6 poena: svaki tačan odgovor za svaku tačku po 1 poen

A: početak sporog starta (veličina prozora zagušenja je 1, a prag sporog starta 16). Prozor zagušenja se menja eksponencijalno

B: Veličina prozora zagušenja dostigla nivo praga sporog starta. Nakon tačke B, prozor zagušenja se menja linearno.

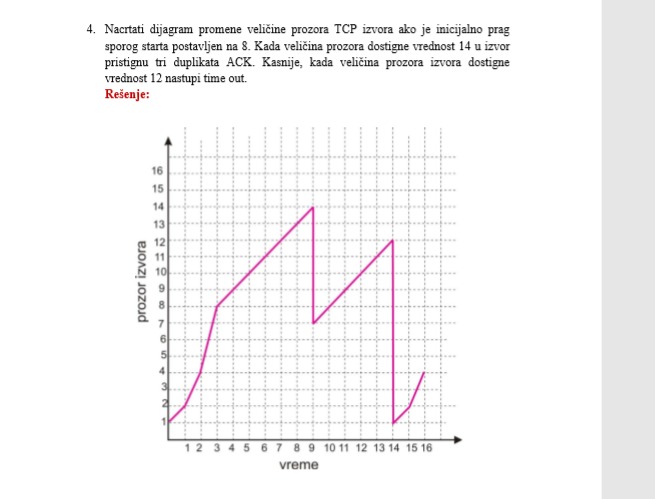
C: primljena su 3 uzastopna ACK za isti segment

D:prozor zagušenja prepolovljen (11) i prag sporog starta postavljen na 11

E: istekao time out.

F: Prag sporog starta se postavlja na polivinu trenutnog prozora zagušenja , tj. Na 9, a novi progor zagušenja se postavlja na 1.

?????????????????????????????????????????????

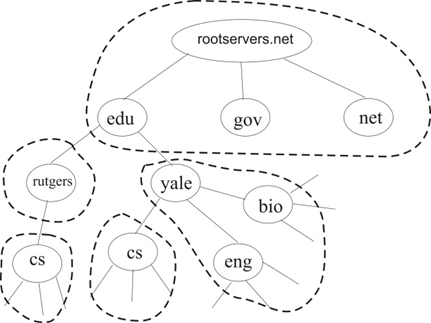


1. **Na slici dole je prikazana DNS topologija u kojoj su različite DNS zone označene isprekidanim linijama. U svakoj zoni postoji po jedan DNS server i zove se isto kao i najviši čvor u zoni: yale.edu, cs.yale.edu, ruthgers.edu, cs.rutgers.edu, i rootservers. net.**
   1. Na katedri za biologiju na Yale-u postoji računar *lab1.bio.yale.edu* i korisnik na računaru *eden.rutgers.edu*  želi da mu pristupi. Navesti u kom redosledu će se posećivati DNS serveri. (odgovor dati u obliku *name-saerver*1→*name-server*2→....)

rutgers.edu→root-server.net→yale.edu (3 poena)

* 1. Korisnik na *lab1.bio.yale.edu* želi da pristupi računaru *aul.cs.rutgers.edu.* Navesti u kom redosledu će se posećivati DNS serveri.

yale.edu→root-server.net→rutgers.edu→cs.rutgers.edu (3 poena)



1. **Koji od navedenih protokola su primeri transportnih protokola u TCP/IP protokol steku?  
   a.Ethernet   
   b.HTTP**

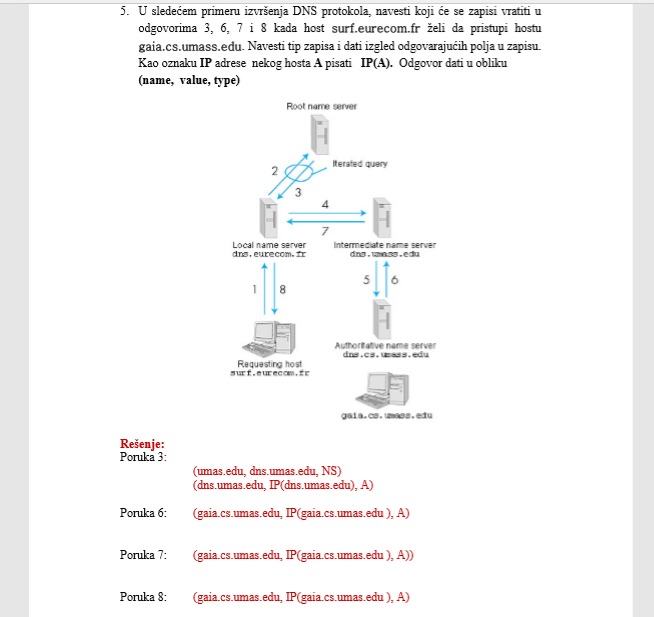
**c.IP  
d.UDP  
c.SMTP  
e.TCP**

UDP, TCP

1. **Koji od sledecih protokola se bave pristupom prenosnom medijumu u TCP/IP?**  
   **a.Ethernet   
   b.HTTP**

**c.IP  
d.UDP  
c.SMTP  
e.TCP  
f.PPP**

Ethernet, PPP



1. **Koji OSI nivo je zaduzen za logicko adresiranje I rutiranje?  
   a. nivo1 b.nivo2… do nivo 7**  
   Mrezni (nivo 3)

1. **Koji OSI nivo je zaduzen za predstavljanje podataka I sifriranje?**Nivo prezentacije (nivo 6)
2. **Host sa adresom131.15.46.59 obavlja broadcast u lokalnoj mrezi.Koja ce adresa biti u polju adresa odredista u zaglavlju IP datagrama?**

**a) 131.15.46.255  
b) 131.15.255.255  
c) 255.255.255.255  
d) nista od navedenog**

c) 255.255.255.255

**.????**

1. **Koji nivo obavlja sekvenciranje poruka, potvrdjivanje I kontrolu toka?  
   a) Layer4(transportni)  
   b) Layer3(mrezni)  
   c) Lauer5(sesija)  
   d) Layer2(data link)**

Transportni

1. **Kada polje TTL u IP paketu dostigne vrednost 0, koja ICMP poruka ce se poslati izvornom hostu:  
   a) destination-unreachable  
   b) time-exceeded  
   c) parameter-problem  
   d) nista od navedenog**

time-exceeded

1. **Kolika je velicina zaglavlja ICMP poruka?**

Mislim da je 8byte-a

4byte-a tu ono type code I checksum

Onda ide jos 4byte-a koja se uglavnom ne koriste

I onda idu podaci

Tako da msm da je zaglavlje 8byte-a

1. **Ukratko objasniti razlike izmedju port adrese, logicke adrese I fizicke adrese.**  
   Port adresa specificira koji se servis koristi na transportnom nivou, logicka adresa predstavlja adresu na mreznom nivou, fizicka je adresa koja se koristi na nivou veze ???

Pa u principu port adresa identikuje aplikativno proces, I ona se koristi na transportom nivou da bi se odgovarajuci segment prosledio odgovarajucem procesu

Logicka adresa je ip adresa, sad tu malo napises o njoj, hehe

I koristi se na mreznom nivou, aka svaki uredjaj na internetu ima jedinstvenu ip adresu ali to te adrese nisu zavisne od hardvera I mogu da se menjaju

A fizicka adresa je definisana mreznom karticom u uredjaju, takodje je jedinstvena ali nije nesto sto mozes da promenis I korisi se na data link nivou ?

1. **Sta je funkcija transportnog nivoa u TCP/IP protokol steku?**  
   Kontrola toka, korekcija gresaka, obezbedjuje logicku komunikaciju izmedju procesa koji se izvrsavaju na razlicitim hostovima ???

E da ovde bi rekla da je pitanje samo sta je funkcija transportnog sloja

Segmentacija poruka, reasembliranje, multipleksiranje, demultipleksiranje, kotrola toka I kontrola zagusenja

U principu, transportni sloj sluzi za pouzdanu komunikaciju izmedju mreznog sloja I aplikativnog sloja ?

1. **Koja od sledecih ip adresa se moze dodeliti hostu ako se koristi subnet maska 255.255.254.0?   
   a) 113.10.4.0  
   b) 186.54.3.0  
   c) 175.33.3.255  
   d) 26.35.2.255  
   e) 152.135.7.0  
   f) 17.35.36.0**  
   b, d, e

1. **Ukratko objasniti šta se podrazumeva pod računarskom mrežom. Navesti podelu računarskih mreža u odnos na tehnologiju prenosa.**  
   Racunarska mreza je skup spregnutih(povezani) , autonomnih(ne postoji odnos master-slave) racunara. Emisione I point to point.

Emisione: vise racunara povezano na isti komunikacioni kanal (preko magistrale, prstena). Kada jedan salje svi primaju poruku. Onaj kome je poruka namenjena, prihvata poruku a ostali ju je odbacuju.

Point-to-point – su povezane na ruter (zvezda, prsten, stablo, kompletno,…)

1. **Zašto je SLOTED ALOHA protokol efikasniji od ALOHA protokola?**   
   Zato sto je vreme podeljeno u slotove i svaki ram se salje u jednom slotu, postoji sinhronizacija za razliku od ALOHA i dolazi do manje kolizija jer ramovi iz susednih slotova ne mogu da izazovu koliziju.

ALOHA protokol: svi hostovi koriste istu frekvenciju za slanje do centralnog cvora. Centralni cvor reemituje ono sto je primio, ali na drugoj frekvenciji. Ako vise hostova prenosi u isto vreme dolazi do kolizije u centralnom cvoru.

Slotted ALOHA pretpostavke: svi ramovi su iste velicine. Vreme je podeljeno na slotove jednake velicine. Cvorovi pocinju sa slanjem ramova samo na pocetku slota. Cvorovi su sinhornizovani. Rad protokola Kada cvor dobije novi ram, prenosi ga u sledecem slotu. Ako nema kolizije, cvor moze poslati novi ram u sledecem slotu. Ako postoji kolizija, cvor pokusava sa retranmisijom u sledecem slotu sa verovatnocom p, sve dok ne uspe sa posalje ram.

1. **Ethernet host dobija ram (frame). Proverom FCS ustanovljava da je ram narušen. Šta će od sledećeg host učiniti (zaokružiti odgovor)   
   a. host će odbaciti ram   
   b. host će normalno procesirati ram i proslediti ga višem nivou.**

**c. tražiće od izvora da izvrši retransmisiju rama.**  
B)  
????

1. **Koji od navedenih mrežnih uređaja koristi MAC adresu u svom radu   
   a. bridge   
   b. hub   
   c. switch   
   d. repeater   
   e. router**  
   A), C), E)  
   ????
2. **Koji mrežni uređaji će kreirati više kolizionih domena(isto ponudjeno kao u 82.)**  
   A), C), E)  
   ????
3. **Šta će uraditi most (bridge) ako primi ram sa MAC adresom koja se ne nalazi u njegovoj tabeli   
   d. odbaciće ram   
   e. ignorisaće ram   
   f. poslaće ram na odgovarajući port   
   g. poslaće ram po svim portovima osim po izvornom portu**   
   G)
4. **Pretpostavimo da se na data link nivou za uramljivanje koristi sekvenca 01110 i da se koristi „bit stuffing“ (umetanje bitova) tehnika**

**a) Izvor je od mrežnog nivoa primio poruku 1 0 1 1 1 1 1 1 0 0 1 1 1 0 0 0 1 1 1 1. Kako izgleda poruka u komunikacionom kanalu koju šalje izvor?**

**b) U odredištu je sa fizičkog nivoa data link nivou stigla poruka 0 1 1 1 0 0 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 1 0 0 0 1 1 1 0 Kako izgleda niz bitova koji se prosleđuje mrežnom nivou u odredištu? Napomena: a) i b) su nezavisni** #

01110 10 110 110 110

* 1. 01110 10 110 110 110 00 110 1000 110 110 01110
  2. 001010011011110011011100

1. **Zasto je minimalna veličina Ethernet rama 64 byte?**  
   Zbog detekcije kolizije ???
2. **Koje prozore TCP koristi za kontrolu zagušenja?**

Prozor zagusenja I prozor koji je odobrilo odrediste.

1. **Sta ce uraditi odrediste kada primi ram van redosleda (npr primio je remove sa rednim brojevima 1,2,3,5,6) u slucaju da se koristi:**
2. **Vrati se nazad na N**
3. **Selektivna retransmisija**  
   #
   1. Odrediste vraca NAK ram u kome saopstava izvoru koji je zadnji korektno primljen ram (ovde 3)
   2. Odrediste potvrdjuje ramove koji nisu ocekivani i stavlja ih u bafer(ovde 5,6).
4. **Objasniti rad SSL protokola**

SSL uspostavlja bezbedan komunikacioni kanal i omogućava:

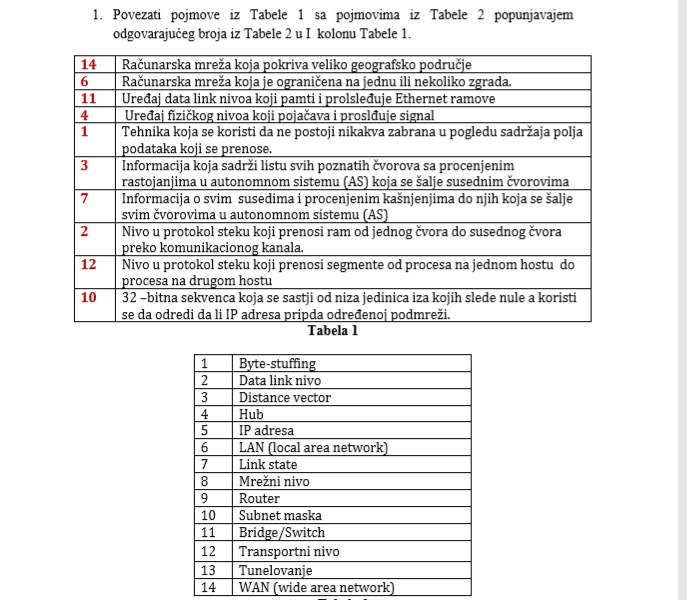
- Pregovaranje parametara izmedju klijenta i servera

- Uzajamno utvrdjivanje identiteta klijenta i servera

- Očuvanje tajnosti podataka

- Očuvanja integriteta podataka  
SSL se sastoji od dva protokola:

* 1. Protokol za uspostavljanje sigurne veze: klijent salje zahtev server za uspostavljanjem veze (verziju ssl, algoritme za sifriranje, izazov Ra), server odgovara koja ce se verzija koristiti, koji algoritam I salje izazov Rb, server salje svoj sertifikat I javni kljuc, server obavestava da je zavrsio sa slanjem svojih podataka, klijent odgovara sifriranim serverovim javnim kljucem, na osnovu kojeg ce se izracunati tajni kljuc, klijent obavestava da se predje na sifriranje sa ustanovljenim kljucem I da je okoncao sa procedurom za uspostavljanje veze, server obavestava da prelazi na koriscenje ustanovljenog kljuca I okoncava proceduru uspostavljanja veze, prelazi se na razmenu
  2. Protokol za koriscenje sigurne veze za razmenu podataka: poruke se dele na blokove velicine 16KB, kompresuju se blokovi, dodaje se sazetak poruke, vrsi se sifriranje, predaje se TCP-u da doda zaglavlje I otpocne prenos



1. **Šta od sledećeg nije deo IP datagrama?**

**a) Fragment ofset**

**b) Identifikator paketa**

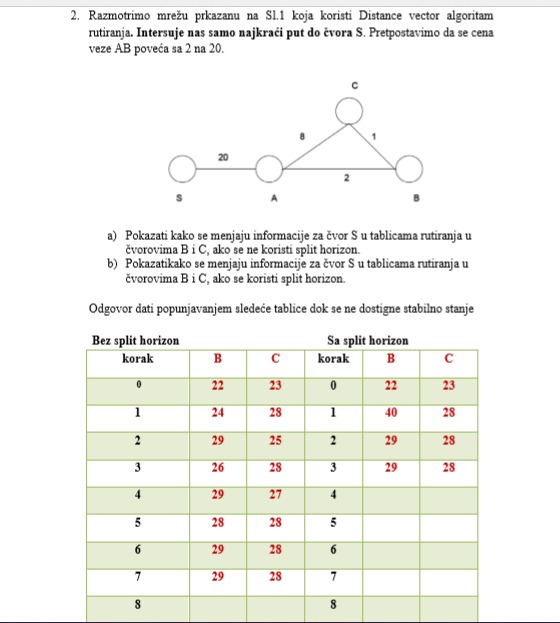
**c) Tip servisa (Type of service)**

**d) TTL**

**e) Eternet adresa odredišta**

**f) Dužina zaglavlja (Header length)**

E)



1. **Navedeni iskazi označavaju protokol ili pojam ili mehanizam koji se koristi u računarskim mrežama. Označiti kako se zove protokol/mehanizam/pojam koji odgovara navedenom iskazu.**

**a) Sprečava gubitak podataka zato što je bafer prijemnika pun.**

**b) Koristi se za raportiranje o graškama i slanje upita u IP baziranim mrežama.**

**c) Vrši retransmisiju TCP segmenta pre isteka timeout-a.**

**d) Podela IP paketa na manje delove koji se reasembliraju u odredištu.**

**e) Transportni protokol koji se koristi za slanje DNS upita i odgovora.**

**f) Obavlja prevođenje IP adresa u adrese data link nivoa.**

**g) Distribuirani servis koji obavlja preslikavanje imena hosta u IP adresu.**

**h) Protokol rutiranja kod koga je oznaka za beskonačno 16.**

**i) Koristi ga HTTP za pouzdani prenos podataka**  
#

* 1. ICMP

Pise tamo mislim kod ICMP da on moze da posalje poruku da se obustavi slanje jer je buffer pun

* 1. ICMP
  2. Brza retransmisija
  3. IP protokol
  4. UDP
  5. ARP
  6. DNS
  7. Distance Vector

Protokol rutanje pise… RIP ? Distance vector je algoritam

* 1. SSL

1. **Objasniti razliku između welcome soketa i connection soketa.**  
   Welcome socket uvek postoji, izvrsava LISTEN primitivu I sluzi da mu se klijent javi sa zahtevom za konekciju. Ukoliko je konekcija uspostavljena, kreira se connection soket koji sluzi za razmenu podataka, a welcome socket nastavlja da izvrsava LISTEN da bi ostali klijenti mogli da ga kontaktiraju.
2. **Koja od sledećih tvrdnji koje se odnose na TCP protokol je tačna (T) a koja netačna (N)**

**a) To je konekciono orjentisani protokol**

**b) Pruža „best effort“ uslugu (najbolje što može)**

**c) Obezbeđuje je polu-duplex (half-duplex) komunikaciju**

**d) To je protokol nivoa sesije**

**e) Između dva računara u jednom trenutku može postojati samo jedna TCP sesija**

**f) Koristi piggybacking za potvrđivanje**

**g) Podržava do 256 portova**

**h) Koristi se da implementira IP protokol**  
#

* 1. T
  2. T
  3. F
  4. F
  5. ???

Prilicno sam sigurna da je ovo netacno

* 1. T
  2. F
  3. ???

Nesto mislim da je I ovo netacno

1. **Šta je od dole navedenog broadcast IP adresa (zaokružiti tačan odgovor)**

**a) IP adresa hosta koji šalje brodcast poruku**

**b) IP adresa u kojoj su svi bitovi host adrese postavljeni na 0**

**c) IP adresa u kojoj su svi bitovi mrežnog dela adrese postavljeni na 1**

**d) IP adresa u kojoj su svi bitovi host adrese postavljeni na 1**

**e) IP adresa u kojoj je poslednji bajt postavljen na 25**  
D)

1. **Klasa IP adresa se može odrediti na osnovu (zaokružiti tačan odgovor)**

**a) prvih 8 bitova**

**b) prva 3 bajta (bytes)**

**c) poslednjih 8 bitova**

**d) prva 3 bita**

**e) prva 4 bita**

**f) mrežne maske**  
  
A), B), E) (ako se misli na najmanji broj, onda E))

Pod e je

1. **Pretpostavimo da imamo Host C, lokalni name server L, i autorizovane name servere Aroot, Acom, i Agoogle.com, pri čemu oznaka Ax znači da name server poseduje podatke za zonu (domen) x (Ax je promenljiva a ne ime hosta). Server L zna da je Aroot root name server i da ima IP adresu 198.41.0.4. Pretpostavimo da su inicijalno svi keševi name servera prazni.**

**a) Korišćenjem podataka datih u tabeli odrediti imena i IP adrese name servera Acom, i Agoogle.com**

**b) Dati redom niz DNS upita i sadržaje izvornih zapisa (resource records) koji se razmenjuju kada host C želi da pristupi hostu www.google.com. (usvojiti da se koriste iterativni upiti)**

* 1. Acom (a.gtld-servers.net, 192.5.6.30), Agoogle.com(ns1.google.com, 216.129.32.10)
  2. #
     1. Host c kontaktira server L da bi dobio preslikavanje za [www.google.com](http://www.google.com)
     2. Server L kontaktira server Aroot na adresi 198.41.0.4 da bi dobio preslikavanje za [www.google.com](http://www.google.com)
     3. Aroot vraca zapise R1 i R2
     4. Server L kontaktira Acom na adresi 192.5.6.30 za preslikavanje [www.google.com](http://www.google.com)
     5. Acom vraca R3 i R4
     6. Server L kontaktira Agoogle.com na adresi 216.129.32.10 za preslikavanje [www.google.com](http://www.google.com)
     7. Agoogle.com vraca R5
     8. Server L vraca Hostu C R5
     9. Host pristupa [www.google.com](http://www.google.com) na adresi 66.102.7.104