**PITANJA SA PRETHODNIH BLANKETA IZ RM**

**(u zagradi su ponavljanja)**

1. Ukratko objasniti šta se podrazumeva pod računarskom mrežom. Navesti podelu računarskih mreža u odnosu na tehnologiju prenosa.

- Racunarska mreza je skup medjusobno spregnutih (mogu da razmenjuju informacije), autonomnih (ne postoji odnos master-slave izmedju njih) racunara. U odnosu na tehologiju prenosa, dele se na emisione (broadcast) i point-to-point.

1. Pobrojati redom nivoe u OSI referentnom modelu.

* fizicki
* nivo veze (data link layer)
* mrezni
* transportni
* nivo sesije (sastanka)
* prezetacioni
* aplikativni

1. Šta su funkcije prezentacionog nivoa u OSI referentnom modelu? (1)

- Bavi se sintaksom podataka koji se prenose kroz mrezu (aplikativni procesi koji se izvrsavaju na razlicitim hostovima mogu koristiti razlicite nacine predstavljanja podataka, da bi se obavila komunikacija mora postojati zajednicki sintaksni oblik koji oba procesa razumeju), kompresijom podataka i sifrovanjem.

1. Koji nivo obavlja sekvenciranje poruka, potvrdjivanje i kontrolu toka?

- Transportni

1. Koji od ISO nivoa se bavi: (2)

a) problemom niza bitova na okvire - data link layer

b) određivanjem putanje poruka kroz komunikacionu podmrežu - mrezni

c) za logicko adresiranje i rutiranje - mrezni

d) formatima za predstavljanje podataka i sifriranjem - prezetacioni

1. Pobrojati i ukratko objasniti tri tehnike za detekciju grešaka. (1)

* Kontrolna cifra parnosti
* Kontrolna suma bloka (BCC) i kontrolna suma (Checksum)
* Poliomski kodovi

1. Šta se podrazumeva pod kontrolom grešaka a šta pod kontrolom toka? (1)

- Kontrola gresaka sluzi da odrediste utvrdi da li je poruka korektno primljena i da izvor utvrdi da li je poruka korektno stigla u odrediste. Kontrola toka numerise pakete, vodi racuna da stizu ispravnim redosledom.

1. Kako se rešava problem pojavljivanja kontrolne sekvence koja označava kraj okvira (frame) ako se za uramljivanje koriste specijalni karakteri, a kako kada se koristi specijalni bajt? (1)

- Ako se koriste specijalni karakteri nakon svakog pojavljivanja DLE u tekstu dodaje se jos jednom DLE karakter. Ako se koristi specijalni bajt 01111110 nivo veze u izvoru automatski dodaje nakon pet uzastopnih 1 jednu 0, a nivo veze u odredistu automatski brise 0 koja sledi nakon pet uzastopnih 1.

1. 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? (1)

- DLE STX **DLE** DLE **STX A** **DLE** DLE **B** **DLE** DLE **ETX** DLE ETX

1. Pretpostavimo da se na data link nivou za uramljivanje koristi sekvenca 01110 i da se koristi 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?

- 0 1 1 1 0 **1 0 1 1** 0 **1 1** 0 **1 1** 0 **0 0 1 1** 0 **1** **0 0 0 1 1** 0 **1 1** 0 0 1 1 1 0

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 prosledjuje mrežnom nivou u odredištu?

- 0 0 1 0 1 0 0 1 1 0 1 1 1 1 0 0 1 1 0 1 1 1 0 0

1. Za numeraciju poruka koriste se 3 bita. Koliko je poruka moguće otposlati, a da ne budu potvrđene ako se koristi

a) go-back-N - najvise 7 (?)

b) selektivna retransmisija - najvise 4 (?)

1. Kako se vrši numeracija poruka kod: (3)

a) stani-i-čekaj - dovoljno je 0 i 1

b) go-back-N - N0>=w+1

c) protokola sa klizajucim prozorom - N0>=2\*w (?)

d) selektivne retransmisije - N0>=2\*w

1. Kako se ponaša izvor ako se naruši ACK ram kod protokola koji koriste go-back-N a kako kod protokola sa klizajućim prozorom? (npr primio je ramove 1,2,3,5,6) (2)

- Kod protokola koji koriste go-back-N kada stigne potvrda za neki ram to znaci da su i svi ramovi pre njega primljeni, tako da ako se na primer narusi ACK4 kad stigne ACK5 on potvrdjuje i ram 4. Kod protokola sa selektivnom retransmisijom ukoliko ne stigne ACK za neki ram i istekne timeout poslace se opet isti ram, a u odredistu ce na osnovu prozora da se odbije jer je duplikat i poslace se ACK izvoru.

1. Nacrtaj izgled polja CONTROL za informacione, supervizorske i nenumerisane ramove kod HDLC protokola i objasni značenje pojedinih polja. (1)
2. Čemu služi polje „protokol“ u zaglavlju PPP rama?

- Oznacava kom protokolu je namenjen ram.

1. Navesti tri opcije o kojima se može pregovarati u fazi uspostavljanja PPP konekcije. (3)

- Koja je maksimalna velicina paketa, koji protokol se koristi za autentifikaciju, kompresija rama (izostavljanje polja address i control).

1. Nacrtati dijagram promene stanja kod PPP protokola. (4)
2. Za prenos poruka na nivou veze koristi se PPP protokol. Ako je potrebno poslati poruku 11100111 01111110 01111110 00011101, kako izgleda poruka u komunikacionom kanalu?

- 01111110 **11100111** 01111101 **01111110** 01111101 **01111110 00011101** 01111110

1. Navesti podelu protokola za pristum emisionom kanalu (MAC protokola). (1)

* Protokoli sa podelom kanala
* Protokoli sa slucajnim pristupom (Random access)
* Taking turns protokoli

1. Nacrtati format Ethernet rama i objasniti značenje pojedinih polja. (2)
2. Kolika je maksimalna i minimalna veličina Ethernet rama? (3)

- Maksimalna 1572B. Minimalna 64B. (?)

1. Zašto je SLOTED ALOHA protokol efikasniji od ALOHA protokola?

- Kod slotted ALOHA protokola vreme je podeljeno na slotove jednake velicine, velicina je jednaka vremenu potrebnom da se prenese jedan ram, cvorovi pocinju sa slanjem ramova samo na pocetku slota. Cvorovi su sinhronizovani i ako 2 ili vise cvorova prenose ram u istom slotu svi detektuju koliziju. A kod ALOHA protokola ako dodje do kolizije centralni cvor ne salje potvrdu i onda host ceka slucajno odabrano vreme pre ponovnog slanja paketa.

1. Ethernet host dobija ram (frame). Proverom FCS ustanovljava da je ram narušen. Šta će od sledećeg host učiniti (zaokružiti):

a) host će odbaciti ram,

b) host će normalno procesirati ram i proslediti ga višem nivou,

c) tražiće od izvora da izvrši retransmisiju rama.

1. Objasniti rad mosta (bridge). (2)

- Most deli jedinstveni LAN na LAN segmente i odvojene kolizione domene. Ramovi koje treba proslediti u isti LAN segment se ne prosledjuju drugim LAN segmentima.

1. Objasniti kako most (bridge) formira tablicu prosledjivanja. (1)

- Tabela sadrzi adresu LAN cvora, oznaku interfejsa i vreme kreiranja. Kada neki ram stigne u most, most saznaje lokaciju posiljaoca (izvora), tj. saznaje sa kog LAN segmenta pristize ram i na osnovu toga pravi zapis u tabeli.

1. Šta će uraditi most (bridge) ako primi ram sa MAC adresom koja se ne nalazi u njegovoj tabeli:

a) odbacice ram,

b) ignorisace ram,

c) poslace ram na odgovarajuci port,

d) poslace ram po svim portovima osim po izvornom portu

1. Koji od navedenih mrežnih uredjaja koristi MAC adresu u svom radu:

a) bridge,

b) hub,

c) switch,

d) repeate,

e) router

1. Koji mrežni uredjaji će kreirati više kolizionih domena: : a) bridge, b) hub, c) switch, d) repeate, e) router
2. Objasniti razlike izmedju konekciono orijentisanog i bezkonekcionog servisa? Imenovati 4 protokola, koji su radjeni na predavanjima, i za svaki navesti da li je konekcioni ili bezkonekcioni. Mora biti naveden primer bar jednog konekcionog i bezkonekcionog protokola. (8)

- Konekcioni servis je obicno implementiran preko virtuelnog kanala. Kada se uspostavi veza izmedju izvora i odredista svi paketi koriste isti kanal, paketi ne sadrze adrese izvora i odredista vec samo broj virtuelnog kanala. Bezkonekcioni servis ne pruza nikakvu garanciju, implementiran je preko datagrama, nema uspostavljanja veze vec se svaki paket salje nezavisno od prethodnog i sadrzi i adresu izvora i odredista.

UDP - bezkonekcioni.

TCP - konekcioni.

IP - bezkonekcioni.

HTTP - bezkonekcioni.

1. Navesti razlike izmedju Distance Vector i Link State algoritma (odakle prikupljaju podatke, kako ih prenose). (2)

- DV prikuplja podatke tako sto sa susedima razmenjuje tablice rutiranja. Tablice rutiranja sadrze vrstu za svaki ruter u mrezi. Kada ruteru stignu tabele od suseda on nalazi najmanje rastojanje do svakog rutera i na njega dodaje svoje rastojanje do rutera od koga je dobio tablicu. LS ima pogled na celu topologiju mreze. Na pocetku on pronalazi svoje susede, njhove mrezne adrese i meri kasnjenje do suseda. Na osnovu tih podataka konstruise Link State paket koji salje pomocu bujice svim ruterima u mrezi. Da bi se bujica drzala pod kontrolom svaki paket ima redni broj koji se povecava svakim prolaskom kroz neki ruter. Ruteri pamte par izvor i redni broj koji su vec videli i na osvnovu toga odbacuju duplikate. Pored rednog broja pamti se i starost, da prilikom otkaza rutera ili narusavanja bita ruter ne bi greskom odbacivao pakete.

1. Sa kojim ruterima se razmenjuju prikupljene informacije ako se koristi

a) Distance Vector algoritam - sa susedima.

b) Link State algoritam - sa svim ruterima u mrezi.

1. Koje informacije su sadržane u Link State paketu? I objasniti kako se vrši distribucija Link State paketa? (4)

- U Link State paketu se nalazi adresa izvora, redni broj, starost, lista suseda i kasnjenja do odredjenog suseda. Distribucija se vrsi pomocu bujice, paketi se salju svim ruterima u mrezi.

1. Objasniti problem brojanja do beskonačnosti kod Distance Vector algoritma i njegovu modifikaciju Split Horizon. (3)

- Do problema brojanja do beskonacnosti dolazi ukoliko npr. ruter X vidi ruter Z preko Y (rastojanje 2) i ruter Z otkaze. Y odmah oznacava da mu je rastojanje do Z jednako beskonacno, ali X jos uvek misli da ima rastojanje do Z jednako 2. U sledecoj razmeni X salje Y da on ima rastojanje do Z jednako 2, X na to dodaje svoje rastojanje i smesta vrednost u svoju tabelu. Tako se prilikom svake razmene polako povecava rastojanje do Z i ide do beskonacnosti. Split Horizon se koristi za resavanje ovog problema tako sto ukoliko kao u ovom slucaju X vidi Z preko Y, on ce ruteru Y uvek pricati da mu je rastojanje do Z jednako beskonacno.

1. Zaokruziti koje od sledecih tvrdnji se odnose na Distance Vector, a koje na Link State algoritam (pogresan odgovor -2 poena): (3)

1) LS ili DV: zahteva poznavanje kompletne topologije mreže,

2) LS ili DV: šalje svoju kompletnu tabelu rutiranja svojim susedima,

3) LS ili DV: koristi bujicu,

4) LS ili DV: ima problem brojanja do beskonačnosti

1. Objasniti hijerarhijsko rutiranje.

- Hijerarhijsko rutiranje se koristi da bi se smanjila potrebna memorija i CPU vreme. Ruteri se grupisu u regione. Svaki ruter koristi isti algoritam rutiranja kao i ostali iz istog regiona, ima informacije o svim ruterima iz svog regiona, a o ruterima iz drugih regiona dobija informacije preko jednakog ili vise rutera (gateway ruteri) koji su zaduzeni za komunikaciju sa drugim regionima.

1. Pretpostavimo da A, B i C jednovremeno prenose bit 0 (predstavljen -1V) koriscenjem CDMA sistema sa kod 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 sistema? (1)

-

1. Tri cvora A,B,C koriste CDMA. Cvorovi redom koriste kodne sekvence (-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), CDMA prima (0,-2,+2,0,+2,+2,0,0). Koje stranice su prenosile podatke i koji bit je svaka od njih prenela? Bitska vrednost 0 je predstavljena sa -1V a jedinica sa +1V.

-

1. Za prenos podataka se koristi CDMA. U odredište je stigla poruka sa vrednošću (3,1,1,1,-1,1,-3,1). Ako je poruku odredištu poslao izvor koji za šifriranje koristi kodnu sekvencu (-1,-1,-1,+1,+1,-1,+1,+1), koja binarna vrednost je primljena ako je 0 predstavljena sa -1V, a 1 sa +1V?

-

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 - Postavljanje window size na 0 (?)

b) Koristi se za raportiranje o greškama i slanje upita u IP baziranim mrežama - ICMP

c)Vrši retransmisiju TCP segmenta pre isteka timeout-a - Brza retransmisija

d) podela IP paketa na manje delove koji se reasembluju u odredištu - fragmentacija

e)Transportni protokol koji se koristi za slanje DNS upita i odgovora - UDP

f) Obavlja prevodjenje IP adresa u adrese data link nivoa - ARP g) Distribuirani servis koji obavlja preslikavanje imena hosta u IP adresu - DNS h) protokol rutiranja kod koga je oznaka za beskonačno 16 - RIP i) Koristi ga HTTP za pouzdani prenos podataka - SSL

1. Da bi povezali racunar na internet, potrebno je da definišete 4 parametra. Koji su to parametri i koja je njihova svrha?

* IP adresa - sluzi za identifikaciju hosta u mrezi
* Maska - pokazuje kojoj podmrezi host pripada
* DNS server - prevodi ime hosta u IP adresu
* Default gateway - host preko njega komunicira sa drugim mrezama

1. Objasniti specijalne IP adrese.

* 0.0.0.0 host tvrdi da je to njegova adresa dok mu se ne dodeli adresa. Moze i da oznacava sve IPv4 adrese.
* adresa koja ima sve nule na mreznim pozicijama oznacava hosta na toj mrezi
* 255.255.255.255 je broadcast na lokalnoj mrezi
* adresa koja ima sve jedinice na pozicijama hosta je broadcast na udaljenoj mrezi
* adrese koje pocinju sa 127 su loopback adrese i koriste se za testiranje mreznih aplikacija.

1. Ukratko objasniti razlike izmedju port adrese, logičke adrese i fizičke adrese.

- Fizicka adresa (MAC adresa) je adresa vezana za hardversku mreznu komponentu, koristi se na data link nivou. Logicke adrese su IP adrese, nisu povezane sa hardverom, koriste se za identifikaciju na mreznom nivou. Port adresa se koristi da identifikuje odredjeni proces na nekom hostu.

1. Objasniti zašto se kontrolna suma u zaglavlju IP paketa mora ponovo određivati pri svakom prolasku kroz ruter. (1)

- TTL (Time to live) tajmer se smanjuje pri svakom prolasku kroz ruter, tako da se i vrednost checksum-a menja.

1. Ukratko objasniti šta je NAT i kako funkcioniše. (2)

- NAT omogucava da lokalna mreza koristi samo jednu adresu sto se tice spoljnjeg sveta. NAT ruter odlaznim datagramima menja izvorisnu IP adresu i broj porta i postavlja NAT IP adresu i novi broj porta, u tabeli transliranja pamti translaciju koju je obavio. Za dolazne datagrame pronalazi u tabeli odgovarajucu IP adresu i port i postavlja njih umesto NAT IP adrese i porta koji su u datagramu.

1. Šta je ICMP i čemu služi?

- ICMP je Internet Control Message Protocol. To je upravljacki protokol, sluzi za raportiranje o greskama i slanje upita.

1. Kada polje TTL u IP paketu dostigne vrednost 0, koja ICMP poruka će biti poslata izvornom hostu:

a) destination-unreachable, b) time-exceeded, c) parametar-problem, d) ništa od navedenog

1. Kolika je veličina ICMP poruka: a) 16B, b) 32B, c)8B, d)ništa od navedenog

- velicina zaglavlja je 8B

1. RIP protokol koristi nekoliko časovnika (tajmera). Koji su to časovnici i čemu služe.

* Period timer - pomocu njega se odredjuje kada ce biti sledeca razmena paketa, to je random vrednost izmedju 25 i 35 sekundi
* Expiration timer - kada za neku destinaciju ne stigne informacija 180 sekundi, ona postaje nevalidna i u polju Distance se upisuje 16.
* Garbage Collector timer - kada neka destinacija postane nevalidna, ruter jos 120 sekundi saopstava da mu je broj skokova do te destinacije 16. Nakon sto istekne 120 sekundi podaci o toj destinaciji se brisu iz tabele rutiranja.

1. Objasniti rad ARP protokola. (2)

- ARP protokol omogucava preslikavanje IP adresa u fizicke adrese, koje se koriste na data link nivou. Radi tako sto kada je potrebna fizicka adresa nekog rutera, ARP salje broadcast na lokalnoj mrezi sa pitanjem cija je data IP adresa, host cija je ta IP adresa odgovorice sa svojom fizickom adresom. Rezultat se kesira, da ukoliko uskoro opet kontaktira isti host nema potrebe za ponovnim broadcast-om.

1. Ko obavlja preslikavanje logičkog imena hosta u IP adresu? Ko obavlja preslikavanje IP adresa u fizičke adrese. Gde se ovi protokoli nalaze u protokol steku? (2)

- Preslikavanje logickog imena u IP adresu radi DNS server. IP adrese u fizicku adresu radi ARP. DNS se nalazi na aplikativnom nivou, ARP se nalazi ispod IP protokola.

1. Objasniti kako se uz pomoć ARP ostvaruje preslikavanje IP adrese u fizičke adrese.
2. Nacrtati format ARP poruka i objasniti značenje pojedinih polja.
3. Objasniti rad DHCP protokola.

- DHCP protokol sluzi za dinamicku dodelu adresa hostovima. Host prvo salje DHCPDISCOVEER poruku, koja za adresu odredista ima 255.255.255.255 a za adresu izvora 0.0.0.0. Ako se u lokalnoj mrezi nalazi DHCP server on obradjuje zahtev, ako se nalazi DHCP agent on prosledjuje poruku serveru. Nakon sto server dobije poruku salje hostu DHCPOFFER poruku, u kojoj se nalazi IP adresa, subnet maska, adresa gateway rutera i vreme vazenja dodeljene adrese. Klijent moze dobiti vise ponuda, bira jednu i odgovara sa DHCPREQUEST porukom u kojoj se nalaze podaci koje je dobio u ponudi. Server odgovara sa DHCPACK, tako potvrdjuje parametre i oni se vezuju za dati host.

1. Pretpostavimo da IP paket koji nosi HTTP zahtev iz lokalne mreze ka internetu ide preko NAT rutera. Navesti koja će se sve polja u TCP i IP zaglavlju poslatog paketa NAT rutera morati promeniti. Obrazložiti odgovor. (1)

- NAT ruter ce zameniti privatne izvorisne IP adrese javnom NAT adresom koju ta mreza koristi za komunikaciju sa spoljasnjim svetom.

1. Host sa adresom 131.15.46.59 obavlja broadcast u lokajnoj mreži. Koja će adresa biti u polju adresa odredišta u zaglavlju IP datagrama:

a) 131.15.46.255,

b) 131.15.255.255,

c) 255.255.255.255,

d) ništa od navedenog. (1)

1. Koja od sledećih IP adresa ne može da se dodeli hostu ako se koristi subnet maska 255.255.254.0? (3 odgovora)

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.

1. Ako je IP adresa oblika 200.23.30.14/20 koja je adresa mreže?

- 200.23.16.0

1. Šta je od dole navedeneog broadcast IP adresa: a) IP adresa hosta koji šalje broadcast 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 255.
2. Šta od sledeceg nije deo IP datagrama? a) Fragment ofset, b) identifikator paketa, c) Tip servisa, d) TTL, e) Ethernet adresa odredista, f) Duzina zaglavlja.
3. Klasa IP adresa se može odrediti na osnovu: a) prvih 8bitova, b) prva 3 bajta, c) poslednjih 8 bitova, d) prva tri bita, e) prva 4 bita, f) mrežne maske. (?)
4. Objasniti razliku izmedju welcome soketa i connection soketa.

- Welcome soket je soket na serverskoj strani koji sluzi da ga klijent kontaktira (“pokuca na vrata”) kada zeli da uspostavi konekciju. Connection soket je takodje soket na serverskoj strani, on se kreira nakon sto klijent kontaktira welcome soket i preko njega se vrsi razmena poruka.

1. Navesti primitive pomoću kojih se uspostavlja konekcioni transportni servis.

- LISTEN, CONNECT, SEND, RECEIVE, DISCONNECT

1. Objasniti uspostavljenje veze izmedju klijenata i servera na transportnom nivou ako se koristi TCP protokol.

- Aplikativni proces u klijentu obavestava TCP sw da zeli da uspostavi konekciju sa serverom, TCP sw na klijentskoj strani salje specijalni TCP segment serveru. Server odgovara slanjem drugog specijalnog segmenta, nakon toga klijent odgovara trecim specijalnim segmentom. Prva dva segmenta ne sadrze podatke sa aplikativnog nivoa, a treci moze da ih ima. Ova procedura se zove three-way handshake.

- Da bi se uspostavila veza potrebno je da klijent kontaktira server, a da bi to mogao da uradi potrebno je da je server aktivan, tj. da ima kreiran welcome soket koji klijent moze da kontaktira. Klijent kontaktira server tako sto kreira svoj soket i navodi ime servera ili njegovu IP adresu i broj porta aplikacije. Nakon kreiranja soketa, TCP sw na klijentskoj strani inicira three-way handshake proceduru. U toku three-way handshake procedure server kreira konekcioni soket preko koga razmenjuje poruke sa klijentom.

1. Čemu služe brojevi portova? Zašto se koriste dva broja porta u zaglavlju TCP (UDP) protokola?

- Brojevi portova sluze za identifikaciju procesa. DP je broj odredisnog porta, a SP broj izvornog porta. Koriste se dva porta zato sto se na hostu moze izvrsavati vise procesa istog tipa, pa samo broj porta aplikacije nije dovoljan da se identifikuje proces.

1. Koji je prvi TCP segment koji može sadržati podatke sa aplikativnog nivoa?

- Treci specijalni segment koji klijent salje serveru.

1. Kako se obavlja numeracija segmenata kod TCP? (1)

- TCP implicitno numerise bajtove, segmenti dobijaju redni broj jednak prvom bajtu u tom segmentu.

1. Navesti koji se segmenti razmenjuju kod uspostavljanja TCP veze.

- Kod uspostavljanja veze se razmenjuju tri specijalna segmenta. Prvi salje klijent serveru i bit SYN je postavlje na 1, a ACK na 0. Drugi salje server klijentu, ukoliko prihvata konekciju SYN=1 i ACK=1, ako odbija konekciju RST=1. Treci salje klijent serveru ako dobije potvrdu konekcije i u njemu je SYN postavljen na 0. Prva dva ne sadrze podatke sa aplikativnog nivoa, treci moze da ih ima.

1. Šta radi TCP prijemnik kada primi segment van očekivanog rednog broja?

- Salje se duplikat prethodnog ACK-a i ukazuje na broj ocekivanog segmenta. Nije definisano sta radi sa segmentima koji su primljeni van reda, postoje dve mogucnosti. Prva je da odbaci sve segmente koji su primljeni van redosleda, to je lakse za programiranje, ali je lose za propusnost mreze. Druga opcija se cesce koristi, to je da zapamti segment koji je primljen van redosleda dok se ne popuni praznina, ona je teza za programiranje, ali je efikasnije.

1. Objasniti brzu retransmisiju kod TCP. (3)

- Kod brze retransmisije nakon sto izvor dobije 3 puta ACK za istu poruku, pretpostavi da se sledeca poruka izgubila i radi retransmisiju i pre nego sto istekne timeout.

1. Da li TCP koristi selektivnu retransmisiju ili go-back-N? Obrazložiti odgovor. (1)

- TCP je hibrid, ne potvrdjuje segmente primljenje van redosleda, vrsi retransmisiju samo segmenata za koje je istekao timeout.

1. Ko obavlja preslikavanje logičkog imena hosta u IP adresu? Ko obavlja preslikavanje IP adresa u fizičke adrese. Gde se ovi protokoli nalaze u protokol steku? (2)

- DNS. ARP. DNS se nalazi u aplikativnom nivou, a ARP u mreznom ispod IP-a.

1. Kako se obavlja kontrola zagušenja kod TCP? (3)

- Zagusenje se detektuje kada se prime 3 ACK-a sa istim rednim brojem ili kada istekne timeout. TCP obavlja kontrolu zagusenja tako sto podesava velicinu prozora u izvoru prema trenutnim mogucnostima mreze i odredista. Koristi dve vrednosti, prozor zagusenja (maksimalni broj segmenata koji mogu biti poslati a nepotvrdjeni) i prozor koji je odobrilo odrediste. Stvarna velicina prozora je uvek manja vrednost od te dve. Ako nema simptoma zagusenja prozor se postepeno i kontinualno povecava da bi se iskoristio trenutno raspolozim kapacitet mreze. Kada se detektuje zagusenje dolazi do trenutnog i velikog smanjenja prozora.

1. Kako se obavlja kontrola toka kod TCP? (1)

- Obavlja se uz pomoc polja Window size u TCP zaglavlju. Window size odredjuje koliko bajtova moze biti poslato, pocev od poslednjeg potvrdjenog. Ukoliko se postavi na 0 kaze izvoru da privremeno prestane sa slanjem.

1. Šta je funkcija transportnog nivoa u TCP/IP protokol steku.

- Funkcija transportnog nivoa je da pruzi aplikativnim procesima konekcioni i bezkonekcioni servis. On obezbedjuje pouzdan komunikacioni kanal, multipleksiranje, demultipleksiranje, kontrolu gresaka, kotrolu toka, kotrolu zagusenja, full-duplex.

1. Koji od navedenih protokola su primeri transportnih protokola u TCP/IP protokol steku? a) Ethernet, b) HTTP, c) IP, d) UDP, e) SMTP, f) TCP
2. Koji od sledećih protokola se bave pristupom prenosnom medijumu u TCP/IP?

a) Ethernet, b) HTTP, c) IP, d) UDP, e) SMTP, f) TCP (1)

1. Koja od sledecih tvrdnji se odnose na TCP protokol – tačno (T), netačno (N): a) To je konekciono orijentisani protokol, T b) pruža best effort uslugu, N c) obezbedjuje je polu-duplex komunikaciju, N d) To je protokol nivoa sesije, N e) izmedju dva računara u jednom trenutku može postojati samo jedna TCP sesija, N f) koristi piggybacking za potvrdjivanje, N g) podržava do 256 portova, N h) Koristi se da implementira IP protokol N
2. Koji tipovi servera imena (name server) postoje?

* lokalni name server
* root name server
* serveri vrsnih domena (TLD)
* autorizovani name serveri

1. Kako izgleda struktura zapisa u bazi servera imena (resource records)?

- (name, value, type, ttl)

1. Šta je DNS?

- DNS je distribuirana baza podataka, koristi veliki broj name servera koji su hijerarhijski uredjeni. Sluzi za preslikavanje imena hostova u IP adrese.

1. Dati format DNS zapisa i objasniti značenje pojedinih polja.
2. U čemu je razlika izmedju iterativnih i rekurzivnih DNS upita? (4)
3. Pretpostavimo da ste osnovali kompaniju SNOOPY i da zelite da je registrujete pod tim imenom ispod domena .rs. Ime vašeg autorizovanog servera imena (Name servera) je dnsl.snoopy.rs, mail servera mail.snoopy.rs i web servera [www.snoopy.rs](http://www.snoopy.rs). Objasniti koje zapise je neophodno ubaciti u DNS bazu TLD servera za domen RS, a koje u autorizovani server dnsl.snoopy.rs da bi moglo da se iz spoljnjeg sveta pristupa vasem web serveru i mail serveru?
4. Pretpostavimo da želimo da promenimo IP adresu hosta gaia.cs.umass.edu sa 128.119.49.186 na 128.119.40.187 i da smo te promene zapamtili u autorizovanom DNS serveru za host gaia.cs.umass.edu. Da li će nakon što smo izvršili promene u autorizovanom DNS serveru sva buduća obraćanja hostu gaia.cs.umass.edu inicirana sa bilo kog hosta u Internetu biti poslata na IP adresu 128.119.40.187? Objasniti odgovor. (1)

1. Objasniti razliku izmedju simetričnih i asimetričnih sistema za šifriranje.
2. Pobrojati redom korake prilikom kreiranja digitalnog potpisa.
3. Šta je funkcija sažetka (hash) i koje osobine ima? (1)
4. Gde se SSL nalazi u protokl steku? Od kojih protokola se sastoji SSL protokol? (2)
5. Koja osobina RSA algoritma je ključna za kreiranje digitalnog potpisa?
6. Ako par (e,n) čini javni ključ za šifriranje, a par (d,n) tajni ključ za dešifriranje kako se obavlja šifriranje i dešifriranje kod RSA algoritma?
7. Ako par (e,n) čini javni ključ za šifriranje, a par (d,n) tajni ključ za dešifriranje. Koji od sledecih parova kljuceva moze iskoristiti u RSA (zanemarujucu cinjenicu da su vrednosti male): a) (5,31) (11,31) , b) (7,77) (43,77), c) (7,55) (41,55)
8. Pretpostavimo da Alisa i Bob koriste kriptografiju sa javnim ključem i svako od njih ima svoj par privatni/javni ključ. Alisin par ključeva je i , a Bobovi i . Alisa želi da pošalje poruku m Bobu tako da se može garantovati autentičnost poruke (tj. da ona zaista potiče od Alise), integritet i tajnost. Alisa šalje Bobu prouku koja je prvo šifrirana Bobovim javnim ključem , a zatim Alisinim privatnim ključem . a) Da li ovaj prilaz obezbedjuje ostvarivanje bezbednosnih ciljeva koje je Alisa postavila? b) Ako ne, šta je potrebno za modifikovati?
9. Ako Alisa želi da pošalje šifrovanu poruku Bobu, koji od dole navedenih ključeva će koristiti: a) Alisin javni ključ, b) Alisin tajni (privatni) ključ, c) Bobov javni ključ, d) Bobov tajni (privatni) ključ
10. Ako Alisa želi da pošalje digitalno potpisanu poruku Bobu, koji od dole navedenih ključeva će koristiti: a) Alisin javni ključ, b) Alisin tajni (privatni) ključ, c) Bobov javni ključ, d) Bobov tajni (privatni) ključ