RAČUNALNIŠKE KOMUNIKACIJE 2023/24

Ime in priimek: _____

2. izpit, 17. 6. 2024

Vpisna številka: _____

Literatura (npr. zapiski, prosojnice, knjige) ni dovoljena. Dovoljen je preprost kalkulator.
Nalogo rešujte v za to predviden prostor. Podpišite se na vse liste, ki jih oddate.
Na vprašanja odgovarjajte kratko (največ 2 povedi), daljši odgovori štejejo 0 točk.
Odgovori na vprašanja morajo biti utemeljeni. Čas pisanja je 70 minut.

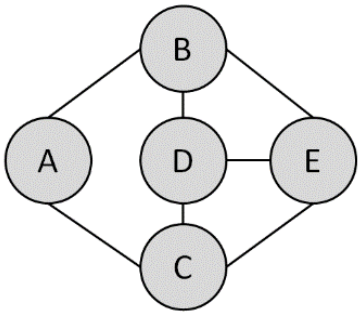
izpolni ocenjevalec

SKUPAJ	

1. Prejemnik prejme zaporedje 15 bitov (črno), ki je opremljeno z 2D paritetnimi biti (modro), ki uporabljajo liho paritetno shemo. Določi bite, pri katerih je prišlo do napake. Odločitev utemelji.

11101 1
00001 1
11101 1
11110 0

2. V omrežju imamo zaporedje petih brezžičnih terminalov, ki so medsebojno dosegljivi tako, kot prikazuje slika na desni. Terminali za komunikacijo uporabljajo protokol CSMA/CA. Če je D vzpostavil komunikacijo z B (že zaključena sekvenca RTS/CTS) in trenutno izvaja prenos okvirja, ali lahko C vzpostavi komunikacijo z E?



3. Paket potuje preko več usmerjevalnikov, ki uporabljajo mehanizem dvojnega sklada (IPv4/IPv6). Nato pride do usmerjevalnika, ki podpira samo IPv4. Zapiši, v katera polja protokola IPv4 se preslikajo naslednja polja paketa IPv6, ko paket pride do zadnjega usmerjevalnika:

`next header:`

`hop limit:`

`flow label:`

`priority (traffic class):`

4. Pojasni dva glavna razloga, zakaj je potrebno, da imajo omrežne naprave, ki uporabljajo TCP, vhodno in izhodno čakalno vrsto:

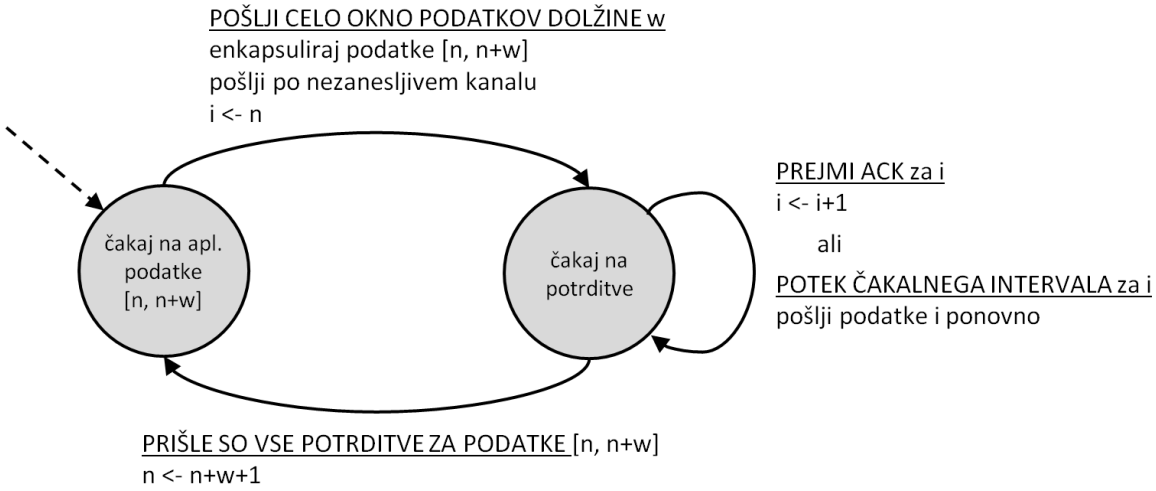
1. _____

2. _____

5. Končna sistema A in B uporabljata TCP za komunikacijo. Po vzpostavitvi povezave in nato izmenjavi večjega števila segmentov v obe smeri B pošlje segment z zaporedno številko 32 in z 9 bajti podatkov, številko potrditve 51 in z vrednostjo rwnd 800b. V nadaljevanju želi A poslati B-ju najprej 10 bajtov podatkov, B bo odgovoril z 2 bajti podatkov in A nato ponovno s 15 bajti. Vsi podatki se uspešno prenesejo brez izgube, vsak prejemnik jih v celoti potrdi. Kakšno številko segmenta (seq) in potrditve (ack) bo B uporabil v svojem naslednjem segmentu po zaključeni zgornji komunikaciji?. Na kratko utemelji.

6. Pošiljatelju, ki uporablja TCP Reno, v nekem trenutku postane cwnd=28, vrednost praga pa znaša 32. Kolikšna je nova vrednost cwnd po prejemu 50 (različnih) potrditev segmentov?

7. Na sliki je podan močno poenostavljen končni avtomat TCP pošiljatelja, ki na vsakem koraku pošlje okno podatkov dolžine w in nato čaka na potrditve. Dopolni končni avtomat tako, da izvaja tudi hitro ponovno pošiljanje (fast retransmit).
Pojasnilo: zapis [n, n+w] predstavlja celo okno segmentov s številkami od n do n+w (w je širina okna), torej zaporedje podatkov n, n+1, ..., n+w.



8. Uporabljamo lokalni strežnik DNS, ki za nas izvaja rekurzivne poizvedbe in predpomnjenje zapisov o strežnikih v hierarhiji DNS. Od strežnika zahtevamo spodnje zaporedje DNS poizvedb. Ob vsakem zahtevku zapiši, katere poizvedbe dejansko izvede na Internetu (in jih ne prebere iz predpomnilnika). Vsako poizvedbo navedi v spodnji tabeli v obliki, kot jo podaja primer (v spodnjem primeru: korenski strežnik vprašamo po TLD strežniku za domeno com).

poizvedba	**poizvedbe (komu: kaj?)**
a.domena1.com	korenski: TLD za com?
a.b.domena1.com	
b.domena1.org	

9. Kakšen je Vigenèrjev kriptogram čistopisa »TESLA« s ključem »FRI«? Uporabljamo angleško abecedo: ABCDEFGHIJKLMNOPQRSTUVWXYZ.

10. Pošiljatelj in prejemnik uporabljata funkcijo za zgoščanje $h(m) = (m + 1)\ mod\ 9$. Pošiljatelj pošlje prejemniku sporočilo 42 in ga za varovanje integritete opremi z ustrezno zgoščeno vrednostjo. Sporočilo in zgoščeno vrednost prestreže aktivni napadalec. Ker zgoščevalne funkcije ne pozna, želi izvesti rojstnodnevni napad nanjo. Podaj primer sporočila, ki ga napadalec lahko posreduje prejemniku tako, da bo rojstnodnevni napad uspel.