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

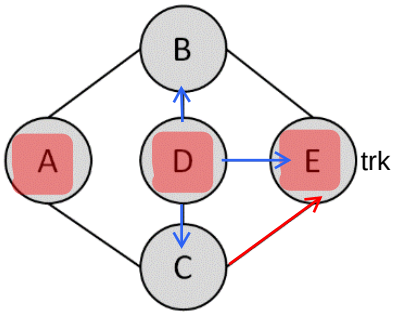
SKUPAJ	

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.

liha paritetna shema -> liho 1 = 0, sodo 1 = 1

11101 1 ok
00001 1 X -> popravi na 0
11101 1 ok
11110 0 X
vsi ok

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?



A in E sta prejela CTS od B in zato molčita, C ne molči pa bi lahko pošiljal ampak ker je E v dosegu D-ja bo prišlo do trka

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:` upper layer

`hop limit:` TTL

`flow label:` X

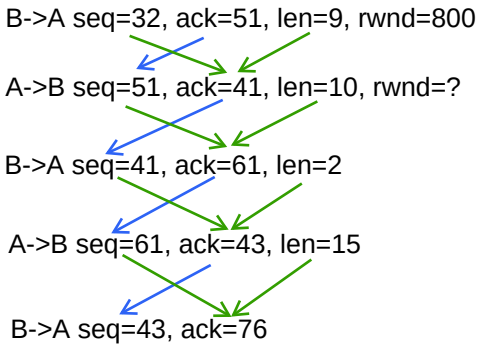
`priority (traffic class):` Type of service

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

1. za tekoče potrjevanje ki je hitreje in bolj učinkovito nam je nujno imeti vrsto na obe strani

2. ne vem. oddly specific vprašanje

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.

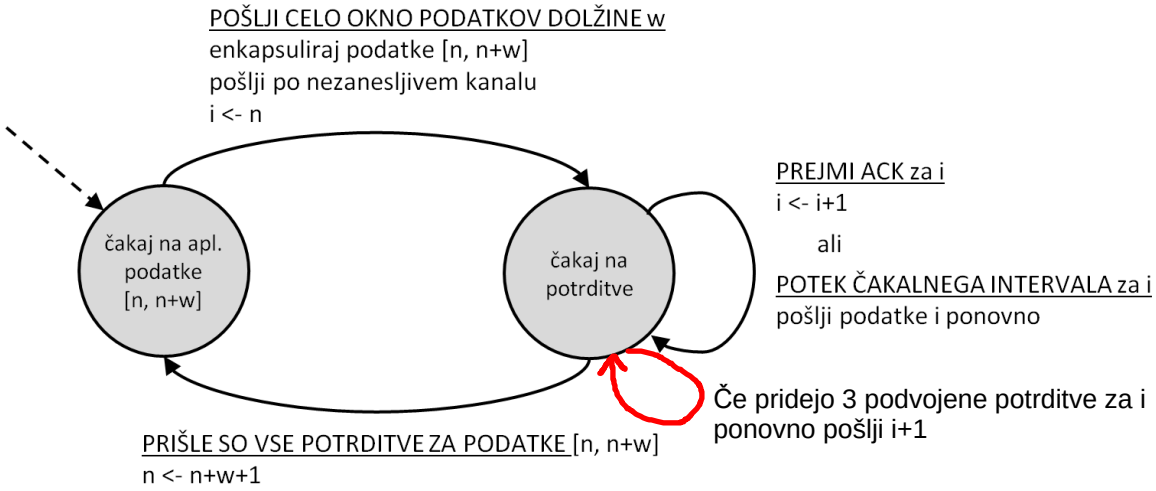


modra = prenesi
zelena = seštej

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?

cwnd=28 (prag 32) -> še vedno slow start, za vsak segment je cwnd+=1 -> sprejme 4 segmenta in pride do 32
cwnd=32 -> prehod v izogibanje zasičenju, preostalih 46 segmentov, mora sprejeti 32 da bi cwnd+=1
cwnd=33 -> preostalih 14 segmentov, ni dovolj da se poveča cwnd

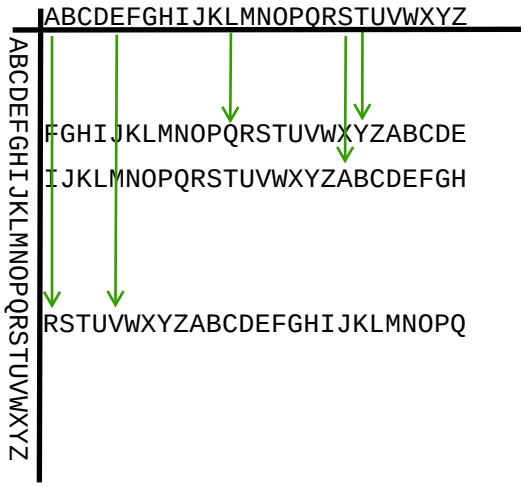
7. Na sliki je podan močno poenostavljen končni avtomat TCP pošiljatelja, ki na vsakem koraku pošlje okno podatkov dolžine w in nato čaka na potrditve. Dopolni končni avtomat tako, da izvaja tudi hitro ponovno pošiljanje (fast retransmit).
Pojasnilo: zapis [n, n+w] predstavlja celo okno segmentov s številkami 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? TLD za com: avtoritativni za domena1.com? avtoritativni za domena1.com: IP za a.domena1.com?
a.b.domena1.com	(zgornje je v predpomnilniku) avtoritativni za domena1.com: avtor. za b.domena1.com? avtoritativni za b.domena1.com: IP za a.b.domena1.com?
b.domena1.org	(vse je v predpomnilniku)

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



FRI
TES -> YVA
LA -> QR

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.

h(42) = 43mod9 = 7
A pošlje B sporočilo (m,H(m)) oziroma (42, 7)

rojstnodnevni napad: poišči neko drugo število ki slika v isto vrednost
Napadalec prestreže paket (42,7). Ne pozna zgoščevalne funkcije, samo njeno vrednost.
Lahko bi pa brute-forceal in poskusil vse možnosti. Uspešne bojo rešitve enačbe:
(x+1) mod 9 = 7
x+1 = 9k + 7
x = 9k + 6
Torej za k=0,1,2,... so možne (6, 15, 24, 33, 42, 51, 60,...)
Potem bi napadalec lahko poslal na primer sporočilo (15, 7) in sprejemnik ne bi vedel da je sporočilo spremenjeno.