

Dovoljen je 1 A4 list z lastnimi zapiski. Druga literatura (npr. prosojnice, knjige) in elektronski pripomočki niso dovoljeni.

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.

Čas pisanja je 70 minut.

izpolni ocenjevalec

1	
2	
3	
4	
SKUPAJ	

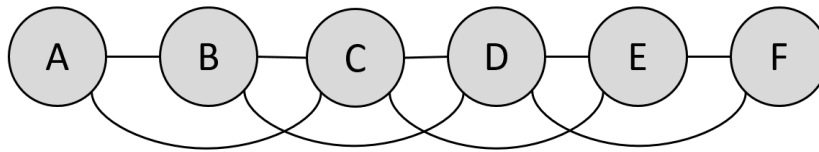
1. NALOGA (5t):

Dopolni naslednje izjave:

1. Algoritem 3DES je _____ in _____ kriptografska metoda (podaj klasifikacijo metode v skupine kriptografskih metod, ki smo jih obravnavali) .
2. Velikost paketa pri tuneliranju je *enako velika* / *večja* / *manjša* (obkroži) od velikosti paketa pri dvojnem skladu, ker _____.
3. Pri IPv6 več ne uporabljamo fragmentacije, iz dveh poglavitnih razlogov, ki sta: _____ in _____.
4. IP naslov je v relaciji s protokolom ARP enako kot je _____ v relaciji s protokolom DNS.
5. _____ in _____ sta protokola za dostop do skupinskega medija, ki potrebujeta dodatno režijo (angl. overhead) za usklajevanje, kdo lahko pošilja.
6. Če 56-bitna zaporedja bitov shranjujemo v matriko velikosti 7x8, jo pri uporabi lihe 2D paritetne sheme moramo opremiti s/z _____ dodatnimi biti, pri uporabi sode 2D paritetne sheme pa s/z _____ dodatnimi biti.
7. _____ je usmerjevalni protokol, ki ga lahko uporabljamo bodisi znotraj ali zunaj avtonomnih sistemov.
8. Protokol bittorrent vzpodbuja P2P odjemalce k sodelovanju tako, da _____.
9. Prenos po vztrajni HTTP povezavi dela hitreje kot po nevztrajni, ker udeleženca izvedeta samo eno _____ in ker transportni protokol pri kontroli pretoka _____.
10. Različne tehnologije protokola Ethernet označimo z opisnimi kraticami oblike xxxBASE-yy, pri čemer xxx označuje _____, yy pa _____.

2. NALOGA (5t):

Podan je sistem 6 terminalov, katerih medsebojno dosegljivost prikazuje slika:



Odgovori na spodnja vprašanja in odgovor na kratko utemelji:

a.) Medtem ko A izvaja pošiljanje okvirja vozlišču C, komu vse lahko uspešno pošilja vozlišče D?

b.) Medtem ko C izvaja pošiljanje okvirja vozlišču A, katere ostale komunikacije so še možne?

c.) Medtem ko A izvaja pošiljanje okvirja vozlišču B, katere ostale komunikacije so še možne?

d.) Zapiši vsa zaporedja 3 terminalov, v katerih nastopa A kot eden od skritih terminalov.

e.) Zapiši vsa zaporedja 4 terminalov, v katerih nastopa B kot eden od izpostavljenih terminalov, prvi in zadnji terminal v verigi pa si ne bosta v dosegu.

3. NALOGA (5t):

Pošiljatelj uporablja potrjevanje samo izbranih paketov (angl. *selective repeat*). Nariši shemo komunikacije med pošiljateljem in prejemnikom, če pošiljatelj uporablja okno velikosti 4, poslati pa želi 6 segmentov. Od teh se 2. segment izgubi pri njegovem prvem pošiljanju, 3. pa pri njegovem prvem in drugem pošiljanju (torej naj prispe uspešno šele v 3. poskusu).

Shemo komunikacije jasno opremi z zapisi, kako se spreminja vsebina prejemnikovega medpomnilnika.

4. NALOGA (5t):

Uporabljamo lokalni DNS strežnik in računalnik, ki tudi lahko predpomni rezultate DNS poizvedb. Za vsako poizvedbo za končno simbolično ime preda računalnik (če odgovor ni v predpomnilniku) zahtevo lokalnemu DNS strežniku, ki izvede rekurzivno poizvedbo.

Na začetku so vsi predpomnilniki prazni, nato pa izvedemo 100 DNS poizvedb po zapisih tipa A/AAAA za nek končni sistem z naslovom oblike xx.yy.zz (3 nivoji hierarhije DNS). Analiziraj naslednje scenarije in za vsakega zapiši, koliko poizvedb bo izvedel lokalni DNS strežnik.

Vsak odgovor argumentiraj (številčno):

a.)

- lokalni strežnik ne izvaja predpomnjenja
- naš računalnik ne izvaja predpomnjenja

Število poizvedb: _____

Utemeljitev:

b.)

- lokalni strežnik predpomni samo imena TLD strežnikov, verjetnost uporabnosti zapisa v predpomnilniku je 50%
- naš računalnik ne izvaja predpomnjenja

Število poizvedb: _____

Utemeljitev:

c.)

- lokalni strežnik predpomni imena TLD strežnikov, verjetnost uporabnosti zapisa v predpomnilniku je 50%
- lokalni strežnik predpomni tudi imena avtoritativnih strežnikov, verjetnost uporabnosti zapisa (zadetka) v predpomnilniku je 10%
- naš računalnik ne izvaja predpomnjenja

Število poizvedb: _____

Utemeljitev:

d.)

- lokalni strežnik predpomni samo imena TLD strežnikov, verjetnost uporabnosti zapisa v predpomnilniku je 50%
- naš računalnik izvaja predpomnjenje, verjetnost zadetka zapisa je 60%

Število poizvedb: _____

Utemeljitev:

e.)

- lokalni strežnik predpomni imena TLD strežnikov, verjetnost uporabnosti zapisa v predpomnilniku je 50%
- lokalni strežnik predpomni tudi imena avtoritativnih strežnikov, verjetnost uporabnosti zapisa (zadetka) v predpomnilniku je 10%
- naš računalnik izvaja predpomnjenje, verjetnost zadetka zapisa je 60%

Število poizvedb: _____

Utemeljitev: