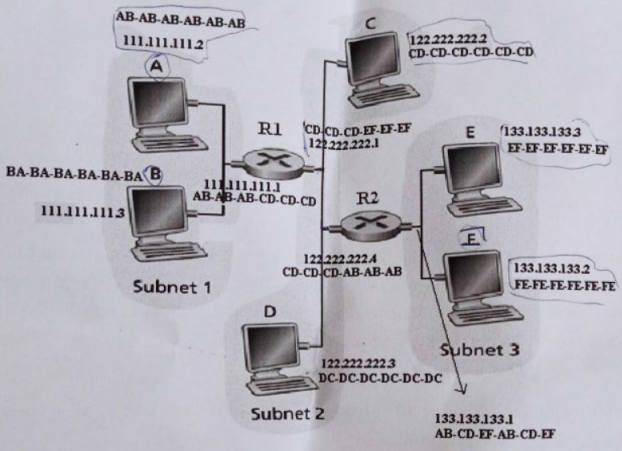
ISPIT IZ PREDMETA RAČUNARSKE MREŽE

04.12.2019.

1. Slici 1 su prikazane tri LAN mreže povezane preko dva rutera. Host A šalje datagram hostu F. Redom navesti kako će se korišćenjem ARP protokola datagram preneti od hosta A do hosta F.



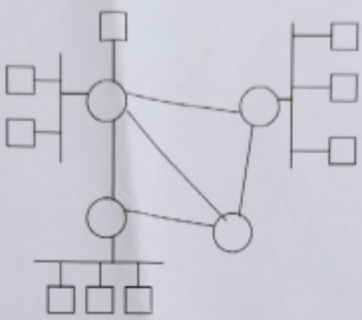
Slika 1.

2. Hostovi A i B komuniciraju i na transportnom nivou koriste TCP protokol. Pretpostavimo da su nakon three-way-handshake procedure oba hosta krenula sa numeracijom svojih segmenata od nule. Pretpostavimo da su zaglavlja svih segmenata veličine 20 byte. Neka se komunikacija između Ai B odvija na sledeći način:

- A šalje segment sa 20 byte podataka
- B odgovara slanjem segmenta sa 30 byte podataka
- B šalje novi segment sa 40 byte podataka
- A odgovara slanjem segmenta sa 50 byte podataka

Za svaki od poslatih segmenata navest koje vrednosti će se naći u poljima redni broj (sequence number) i r.broj. potvrde (acknowledgement number)

3. Na Slici 2 svaki kružić predstavlja ruter a kvadratić host. Koliko je podmreža mreža, u smislu IP adresa, na slici 2. Zaokružiti svaku od mreža i dati obrazloženje.



Slika 2.

4. Pretpostavimo da Alisa i Bob koriste kriptografiju sa javnim ključem i svako od njih ima svoj par privatni/javni ključ. Alisin par ključeva je K_A^P / K_A^J, a Bobov K_B^P / K_B^J. 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 poruku koja je prvo šifrirana Bobovim javnim ključem K_B^J a zatim Alisinim privatnim ključem K_A^P.

a) Da li ovaj prilaz obezbeđuje ostvarivanje bezbednosnih ciljeva koje je Alisa postavila?

b) Ako ne, šta je potrebno modifikovati?

Predmetni nastavnik