Komunikacijski protokoli in omrežna varnost
2010/11
Prvi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena.
Čas pisanja izpita je 50 minut.
Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Naš prijatelj Peter Zmeda je malce preslišal, da za prenos sporočil po omrežju bootp protokol uporablja UDP prenosni protokol, ter se je lotil implementacije s TCP protokolom.

VPRAŠANJA:

1. Kje vse mora popraviti programsko opremo (na katerih računalnikih), da bo svojo novo idejo spravil v delovanje?

2. Ali bo njegova ideja sploh delovala? Če menite da bo, ali bo kaj izboljšala kakovost prenosa? Utemeljite odgovor.

3. Eden od razlogov, čemu se je Peter odločil implementirati svojo inačico bootp oziroma DHCP protokola, je bil ta, da je ob zagonu želel poslati odjemalcu še posebno sporočilo o vremenskih podatkih (Bog si ga vedi čemu), ki ga naj bi odjemalec shranil. Kot vemo, ta razlog ni dovoljšen, da bi se lotili svoje implemetacije protokola, saj strežniki že sedaj omogočajo pošiljanje takšnih podatkov. Kako?

2. naloga: V nekem podjetju že dlje časa uporabljajo orodja za nadzor in upravljanje z omrežji. Odgovori na naslednja vprašanja v zvezi s tem:

VPRAŠANJA:

1. Nadzor in upravljanje sta vzpostavljena le do te mere, da lahko administratorji konfigurirajo nastavitve naprav, spremljajo varnostne mehanizme in sledijo dostopom drugih uporabnikov. Kateri aspekt (oz. vrsta) upravljanja v tem sistemu ni implementirana - poimenujte in obrazložite, kaj omogoča.

2. Dopolnite: Upravljalec omrežja komunicira s programsko opremo v nadzorovanih napravah imenovano _____ z uporabo _____. Slednje ponujajo strukturiran dostop do svojih podatkov v obliki _____, ki je definiran na osnovi jezika za zapis teh podatkov, imenovanega _____.

3. Protokol SNMP uporablja dve obliki sporočil. Za vse štiri oblike/vrste upravljanja in nadzorovanja (torej za $2 \times 4 = 8$ primerov) podaj možen primer uporabe takega sporočila.

4. V podjetju se odločijo uporabiti varnostne mehanizme za zaščito SNMP komunikacij, zaščititi jih želijo predvsem pred ponovitvami že opravljenih komunikacij (*replay attack*). Denimo, da se pri tem uporablja naslednja dogovorjena funkcija kriptiranja sporočil:

f(sporočilo, žeton) =
[sporočilo s krožnim zamikom 1 črke v desno] + [žeton]

kjer „+“ pomeni preprost stik obeh nizov. Primer: sporočilo *geslo* bi s funkcijo f in žetonom XXX zakriptirali v *ogeslXXX*.

Denimo, da je bil drugi sprejemnik v komunikaciji zagnan prvič, od zagona pa je minilo toliko časa, kolikor od začetka pisanja tega kolokvija. Na osnovi podanih informacij kriptiraj *sporočilo* `GET1.3.6.1.2.1.7.2`. Pojasni, kako takšnen način kriptiranja brani pred ponovitvijo komunikacije. Pred katerimi drugimi napadi še brani?

5. S principom kodiranja TLV želimo prejemniku poslati en sam celoštevilski podatek (tip=2) z vrednostjo 32. Zapišite zakodiran podatek.

3. naloga: Peter ni od muh, saj sledi tudi znanstvenim dosežkom po svetu. Tokrat je prebral, da so v pospeševalniku v CERNu uspeli izolirati za delček sekunde nekaj anti-protonov. Pri tem so uporabili napravo, ki se imenuje LHC (*The Large Hadron Collider*). Delovanje naprave med delovanjem opazuje več detektorjev, ki odčitujejo podatke v stvarnem času in jih fiziki kasneje obdelujejo. Precej programske opreme za nadzor in delovanje detektorjev je ustvarilo slovensko podjetje CosyLab.

VPRAŠANJA:

1. Za potrebe te naloge predpostavimo, da imamo 1024 senzorjev, s katerih bi rad Peter prejemal k sebi v Spodnje Butale v stvarnem času. Zato se je za prenos odločil za RTP protokol. Kako naj Peter v toku podatkov razlikuje s katerega senzorja prihajajo podatki? Opišite tudi s konkretnim primerom RTP paketa.

2. Zahteve za protokol stvarnega časa smo razdelili na dva dela ter za enega zadolžili sam protokol ter za drugega aplikacijo. Za kateri del zahtev smo zadolžili protokol?

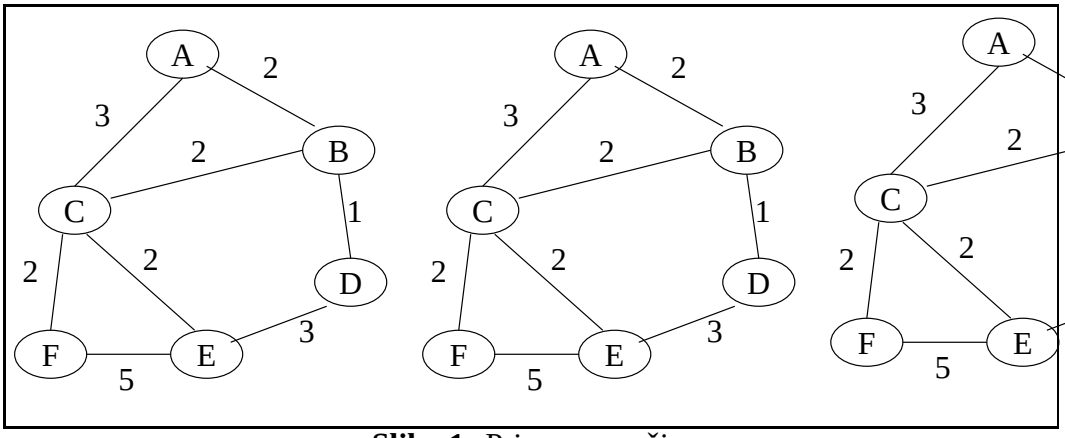
3. Kateri je drugi del in čemu smo za zanj zadolžili aplikacijo?

4. naloga: V omrežju uporabljamo razpošiljanje s protokoloma IGMP in PIM.

VPRAŠANJA:

1. Kje v omrežju se uporablja kateri izmed protokolov in kakšen je njegov namen?

2. Na grafu omrežja na sl. 1 (levo) določite skupno razpošiljevalno drevo z metodo minimalne skupne cene. Na sredinskem grafu določite drevo (posameznega) pošiljatelja E. Na desnem grafu določite razpošiljevalno drevo, ki optimizira število hopov.



Slika 1: Primer omrežja.

3. Denimo, da se v omrežju, ki uporablja skupno razpošiljevalno drevo, uporablja centralno vozlišče F. Usmerjevalnik A, ki se še ni pridružil razpošiljevalnemu drevesu, pošlje usmerjevalniku F nek paket. Kdaj se bo A pridružil razpošiljevalnemu drevesu, zakaj?