Vaje PRK, 2013/2014

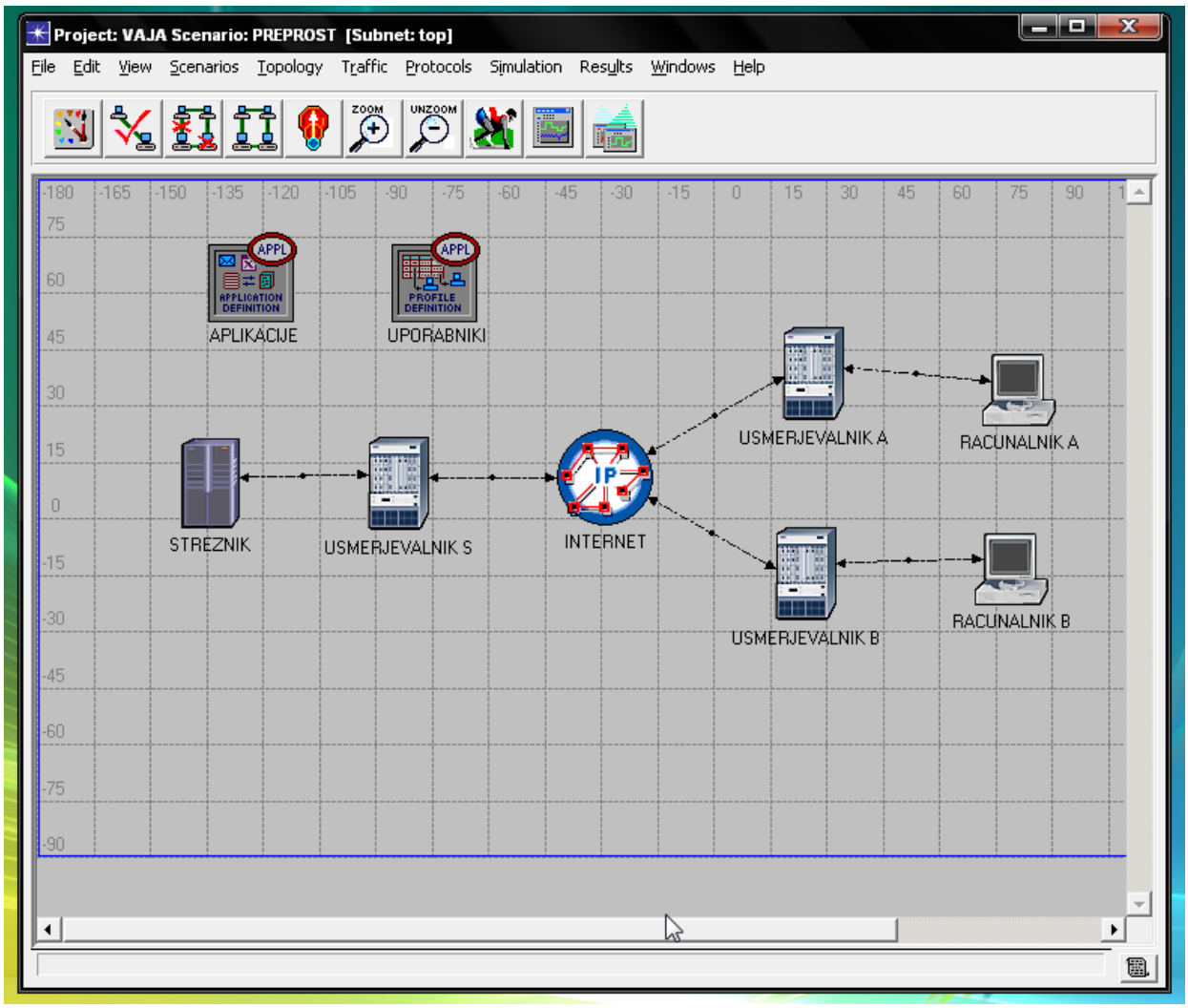
VAJA S SIMULATORJEM OPNET

Pri tej nalogi boste simulirali računalniško omrežje, ki ga sestavljata dva računalnika imenovana kar A in B, ki sta vsak preko svojega usmerjevalnika povezana z internetom. Zanima nas predvsem povezava do oddaljenega strežnika, ki v internet dostopa preko svojega usmerjevalnika. Dodatno boste predpostavili, da računalnika A in B do podatkov na strežniku dostopata tako, da z njim vzpostavita navidezno privatno omrežje (VPN).

Navodila za izdelavo naloge

1. Tvorite nov projekt. Začetni scenarij imenujte PREPROST. Za izdelavo naloge boste potrebovali gradnike iz skupine **internet_toolbox**.

2. V model dodajte naslednje gradnike: **Application Config**, **Profile Config**, **ip32_cloud**, **ppp_server**, trikrat **ethernet4_slip8_gtwy** in dvakrat **ppp_wkstn**. Gradnike povežite s povezavami **PPP DS1**. Pri razporeditvi in imenovanju se zgledujte po spodnji sliki.



3. Pri aplikacijah izberite možnost **Default**, da boste imeli vse na voljo.

4. Pri uporabnikih izberite možnost **Sample Profiles**, da boste imeli na voljo nekaj tipičnih uporabnikov.

5. Na strežniku pri **Application: Supported Services** izberite **All**, da bodo vse na voljo.

6. Na vsakem od računalnikov A in B nastavite enega uporabnika in sicer **Sales Person**.

7. Določite, da se naj zbirajo statistike **Global Statistics -> DB Query -> Response Time** in **Global Statistics -> HTTP -> Page Response Time**. Dodatno na računalnikih A in B izberite statistiki **Client DB -> Traffic Received** in **Client Http -> Traffic Received**.

8. V nadaljevanju bomo model dopolnili. Da bo možna primerjava z originalnim modelom, tvorite sedaj duplikat scenarija in ga imenujte FIREWALL.

9. V novem scenariju spremenite USMERJEVALNIK S tako, da polje **model** postavite na vrednost **ethernet2_slip8_firewall**, polje **Proxy Server Information -> row 1 (Database application) -> Proxy Server Deployed** pa postavite na vrednost **No**. S temi spremembami dosežemo, da podatki iz baze na strežniku ne morejo preko usmerjevalnikovega požarnega zidu in torej niso dosegljivi na računalnikih A in B.

10. Sedaj bomo dodali še en scenarij in sicer želimo omogočiti računalniku A, da pride do podatkov v bazi kljub požarnemu zidu. Izbrali bomo možnost, pri kateri se med računalnikom A in strežnikom vzpostavi navidezno privatno omrežje (VPN), torej bo USMERJEVALNIK S obravnaval računalnik A tako, kot da bi bil na njegovi levi strani in zato pravilo filtriranja zanj ne bo veljalo. Tvorite duplikat scenarja in ga imenujte VPN.

11. V novem scenariju zbrišite povezavo med usmerjevalnikom S in strežnikom. Nato na sliko dodajte USMERJEVALNIK D (gradnik **ethernet4_slip8_gtwy**) in **IP VPN Config**. S povezavama PPP DS1 povežite USMERJEVALNIK D z obstoječim usmerjevalnikom S in s strežnikom.

12. Pri nastavitvah **IP VPN Config** dodajte pri **VPN Configuration** eno vrstico, v katero pri **Tunnel Source Name** vnesete vrednost USMERJEVALNIK A, pri **Tunnel Destination Name** pa vnesete vrednost USMERJEVALNIK D. Tudi pri **Remote Client List** dodajte eno vrstico in pri **Client Node Name** vnesite vrednost RACUNALNIK A.

13. Za vse tri scenarije v meniju **Scenarios -> Manage Scenarios** določite, da se naj statistika zbira 1 uro in potem kliknite OK.

14. Oglejte si vse rezultate in pripravite poročilo, v katerem opišete ugotovitve. Zanima nas predvsem vpliv požarnega zidu in vzpostavitve VPN na komunikacijo med računalnikoma A in B ter bazo podatkov na strežniku. Ugotovite tudi, kako se v vseh treh scenarijih razlikujejo odzivni časi za povpraševanja v bazi in http zahteve.

15. Dodatna naloga: poskušajte spremeniti model tako, da bo baza podatkov dosegljiva le z računalnika A (kot imamo že sedaj), spletne strani (http promet) pa bodo dosegljive le z računalnika B. Po potrebi dodajte kakšen požarni zid.