Elektrotehnički fakultet u Beogradu
Katedra za elektroniku

Praktikum iz računara – 13E043PIR

Laboratorijska vežba

Elektronska pošta, bežični pristup i zaštitne barijere

Autor: Dragomir El Mezeni

Beograd, 2017.

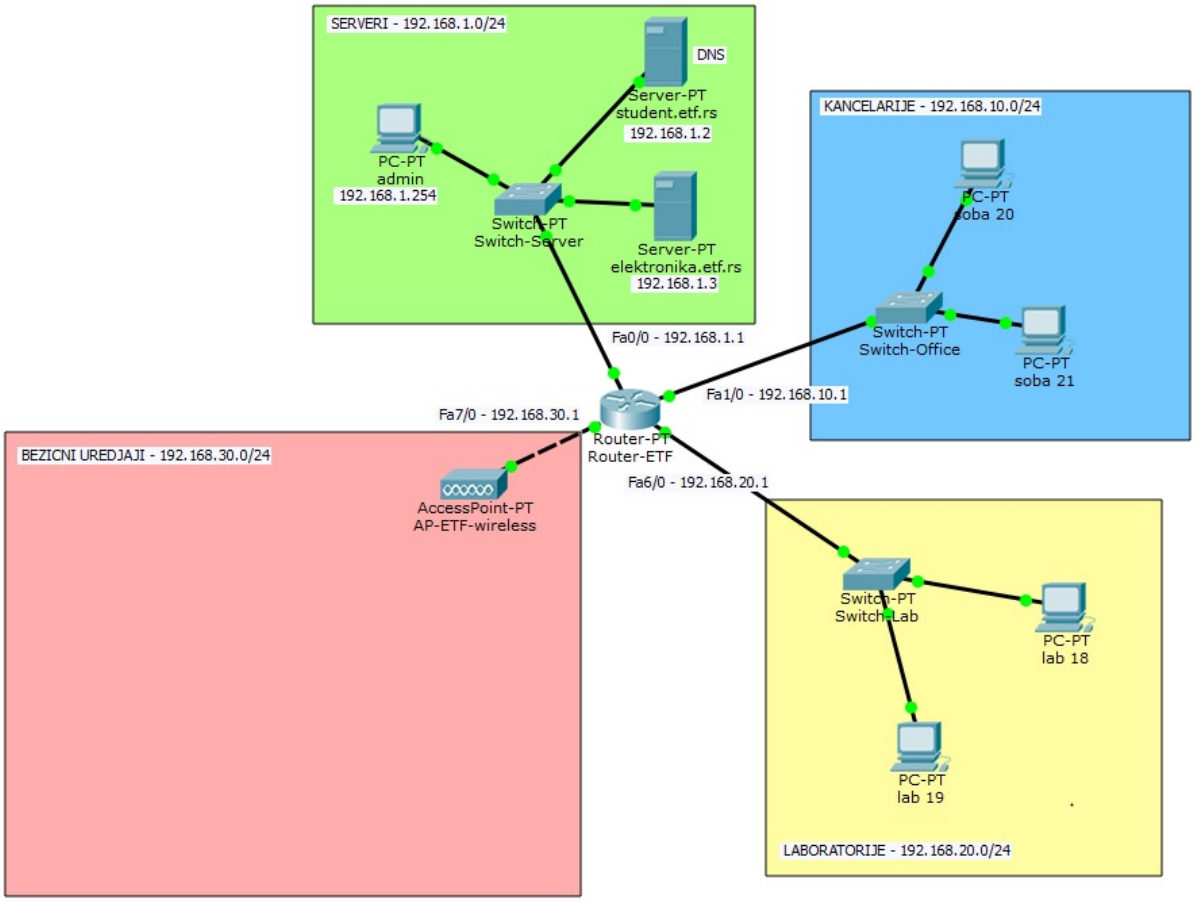
1. Cilj vežbe

Cilj ove laboratorijske vežbe je da se studenti upoznaju sa konceptima slanja i primanja elektronske pošte, sa povezivanjem bežičnih uređaja u mrežu kao i sa konceptom zaštitne barijere (*firewall*) koji predstavlja jedan od vidova bezbednosti lokalnih mreža.

2. Kreiranje osnovne strukture mreže

Potrebno je projektovati mrežu Elektrotehničkog fakulteta koja se sastoji iz 4 dela: serverske sale, kancelarija zaposlenih, studentskih laboratorija i ima mogućnost povezivanja bežičnih uređaja. U sistemu postoji samo jedan ruter odgovoran za usmeravanje saobraćaja kroz mrežu. Kako standardna komponenta Router-PT ima samo 2 FastEthernet porta potrebno ju je nadograditi dodavanjem 2 dodatna porta. Za postupak nadogradnje rutera, kako bi se obezbedila mogućnost povezivanja većeg broja mreža, pogledati Dodatak 1. Takođe smatra se da se sva razmena podataka odvija lokalno u mreži, odnosno da ne postoji pristup internetu i zbog toga će sve korišćene adrese biti iz opsega lokalnih adresa.

Na Slici 1. je prikazan izgled mreže sa naznačenim opsegom adresa za svaki deo mreže. Adrese u okviru segmenta gde se nalaze serveri i administratori se dodeljuju statički dok se ostale adrese dodeljuju dinamički korišćenjem DHCP protokola koji je potrebno podesiti na ETF ruteru. Podrazumevani prolaz (*default gateway*) za svaku od lokalnih mreža je naznačen pored odgovarajućeg priključka rutera. U sistemu postoji jedinstveni DNS server i u tu svrhu se koristi server **student.etf.rs** sa adresom **192.168.1.2**. Na Slici 2. je prikazan postupak konfigurisanja DHCP-a na ETF ruteru.



Slika 1. Topologija fakultetske mreže

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool IP10
Router(dhcp-config)#net 192.168.10.0 255.255.255.0
Router(dhcp-config)#default 192.168.10.1
Router(dhcp-config)#dns 192.168.1.2
Router(dhcp-config)#exit
Router(config)#ip dhcp pool IP20
Router(dhcp-config)#net 192.168.20.0 255.255.255.0
Router(dhcp-config)#default 192.168.20.1
Router(dhcp-config)#dns 192.168.1.2
Router(dhcp-config)#exit
Router(config)#ip dhcp pool IP30
Router(dhcp-config)#net 192.168.30.0 255.255.255.0
Router(dhcp-config)#default 192.168.30.1
Router(dhcp-config)#dns 192.168.1.2
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Slika 2. Konfigurisanje DHCP tako da dodeljuje odgovarajuće adrese svakom segmentu mreže

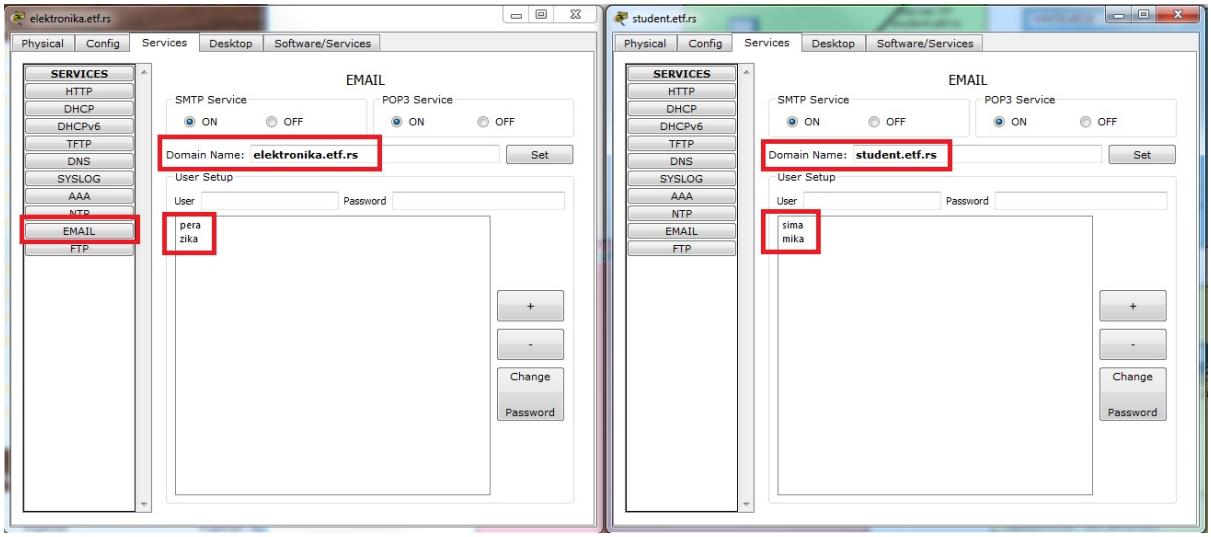
Podesiti DNS tabelu tako da serveri **student.etf.rs** i **elektronika.etf.rs** budu vidljivi pod tim imenima. Proveriti funkcionalnost pristupanjem odgovarajućim HTML stranicama.

Proveriti da li su oba servera vidljiva iz svih delova mreže pod odgovarajućim imenima.

3. Podešavanje elektronske pošte

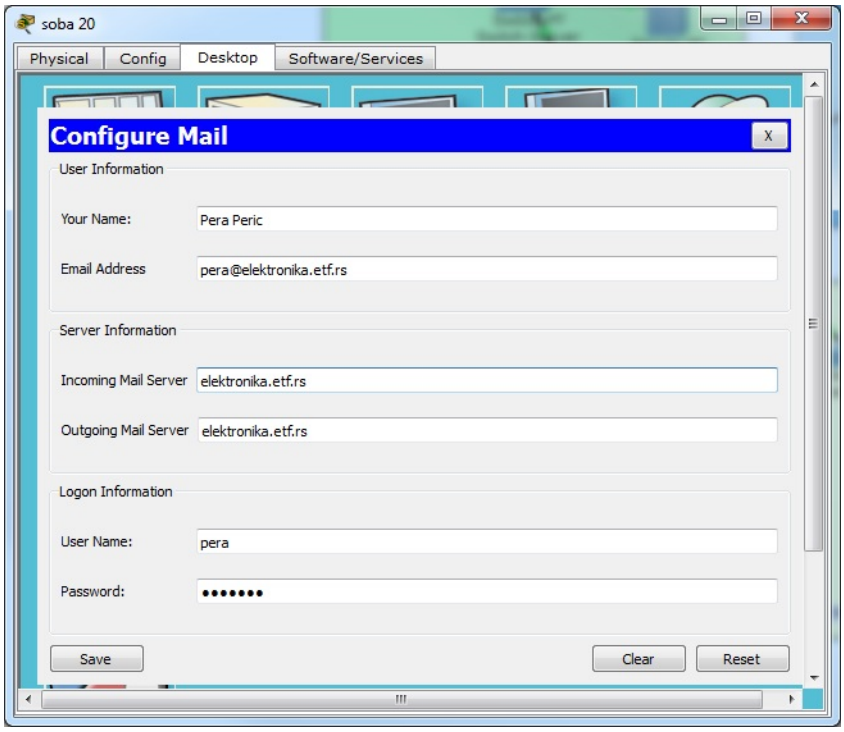
Proces slanja i primanja elektronske pošte najčešće se obavlja korišćenjem SMTP i POP3 protokola na aplikacionom sloju. Oba ova protokola kao osnov koriste TCP konekciju sa odgovarajućim serverom elektronske pošte. SMTP (*Simple Mail Transfer Protocol*) se koristi za slanje poruke ka serveru elektronske pošte i ova komunikacija obično koristi TCP konekciju na portu 25. Za čitanje elektronske pošte mogu se koristiti POP3 (*Post Office Protocol Version 3*) ili IMAP (*Internet Message Access Protocol*). Glavna razlika između ova dva protokola je ta što se korišćenjem POP3 protokola po preuzimanju poruka briše sa servera na kom se do tad čuvala. Korišćenjem IMAP protokola poruka ostaje na serveru i može joj se pristupiti sa više različitih uređaja. Kako je u trenutnoj verziji *Packet Tracer*-a podržan samo POP3 protokol, mi ćemo ga koristiti u okviru ove vežbe.

Za početak je potrebno konfigurisati odgovarajuće servere elektronske pošte. Ideja je da se elektronske poruke zaposlenih čuvaju na internim serverima u ovom slučaju **elektronika.etf.rs** dok se elektronske poruke studenata čuvaju na studentskom serveru **student.etf.rs**. Dodati nekoliko korisnika na svaki od servera. Proces dodavanja korisnika je prikazan na Slici 3. **Nakon dodavanja imena domena obavezno kliknuti na taster Set.**



Slika 3. Podešavanje servera elektronske pošte

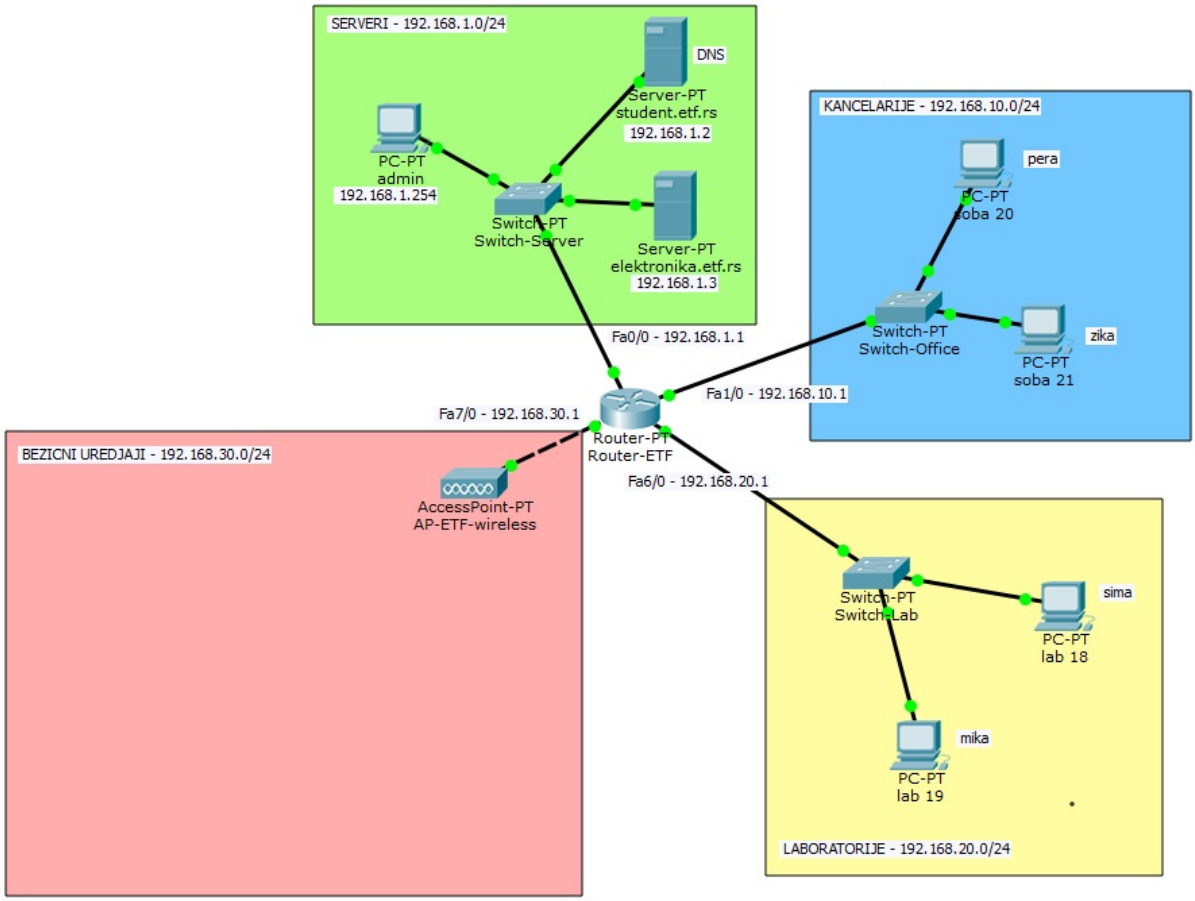
Nakon podešavanja servera potrebno je na svakom računaru podesiti prijem i slanje elektronske pošte. Primer podešavanja elektronske pošte za Peru Perića iz sobe 20 je prikazano na Slici 4.



Slika 4. Podešavanje elektronske pošte na korisničkim računarima

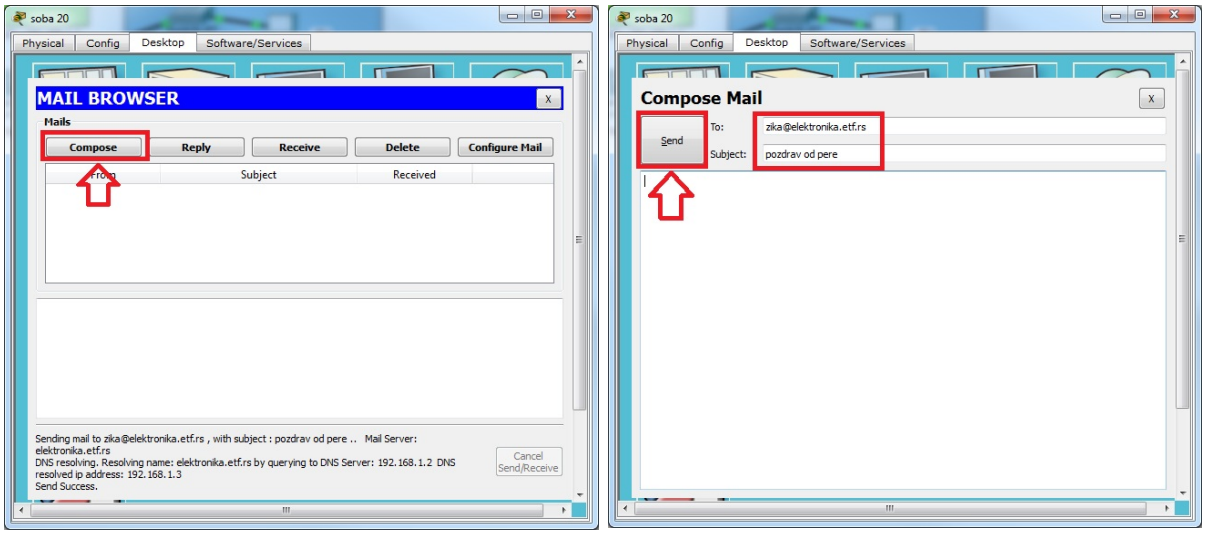
Podesiti elektronsku poštu i na ostalim računarima ako su imena korisnika prikazana na Slici 5. **Voditi računa koji server koriste studenti a koji zaposleni!!!**

Kako bi vam bilo lakše da ispratite identitete preporuka je da stavite oznake sa imenima korisnika pored svakog računara kao što je to urađeno na Slici 5.



Slika 5. Imena korisnika odgovarajućih računara

Nakon uspešne konfiguracije elektronske pošte poslati poruku od Pere Perića (pera@elektronika.etf.rs) ka Žiki Žikiću (zika@elektronika.etf.rs). Koristite simulacioni mod i obratite pažnju na tok poruka. Na Slici 6. je prikazan postupak slanja poruke.



Slika 6. Slanje poruke

Nakon poslate poruke u donjem delu prozora pojavljuje se izveštaj o uspešnosti slanja poruke kao što je prikazano na Slici 7.

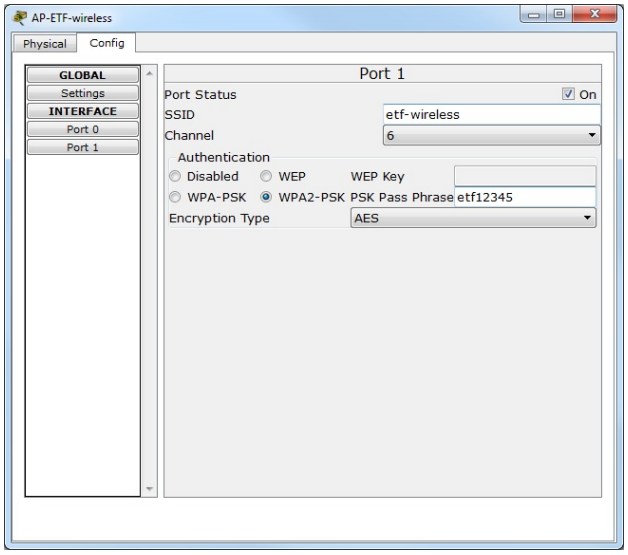
Slika 7. Izveštaj o uspešno poslatoj poruci

U simulacionom modu kod Žike na računaru u Sobi 21 kliknuti na taster *Receive* u okviru programa elektronske pošte. Obratiti pažnju na poruke koje se razmenjuju ovom prilikom.

Testirati i slanje poruke sa naloga studenta Sime Simića asistentu Peri Periću. **Obratiti pažnju na putanje poruka i u ovom slučaju.**

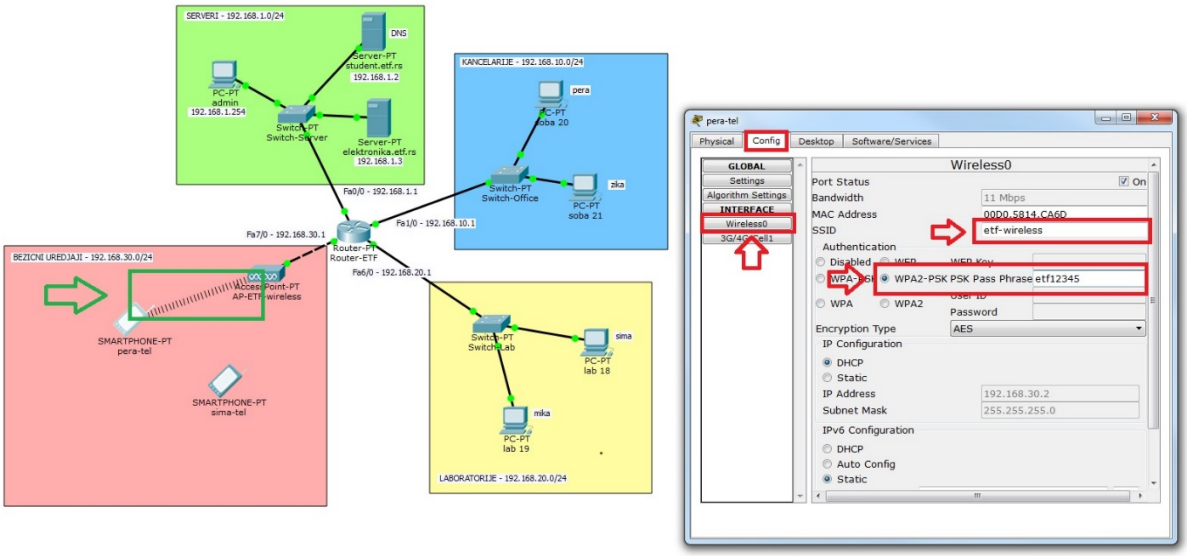
4. Bežični pristup

Kako bi se obezbedila mogućnost da studenti i zaposleni pristupe mreži sa svojih bežičnih uređaja (telefona, laptop računara i sl) u sistem je dodata jedna pristupna tačka (*access point*) AP-ETF-wireless. Opasnost korišćenja bežičnog prenosa je što se signal odašilje u okolinu i mogu ga prihvatiti svi uređaji koji se nalaze u dometu a ne samo oni kojima je signal namenjen. Problem postoji i u obrnutom smeru pošto poruku koja može imati i štetan sadržaj mogu poslati svi uređaji koji se nalaze u dometu pristupne tačke. Zbog toga je pre puštanja u rad potrebno obezbediti pristupnu tačku uključivanjem odgovarajuće enkripcije. Na raspolaganju su WEP, WPA i WPA2 algoritmi. WEP algoritam predstavlja jako slab metod zaštite i veoma ga je lako razbiti pomoću javno dostupnih alata. Zbog toga je potrebno koristiti neki od WPA ili WPA2 algoritama. U ovom primeru biće korišćen WPA2 algoritam za koji je potrebno definisati odgovarajuću lozinku. Lozinka korišćena u ovom primeru je **etf12345** a postupak konfigurisanja pristupne tačke je prikazan na Slici 8.



Slika 8. Konfigurisanje pristupne tačke

Na ovaj način je omogućen pristup lokalnoj mreži svim uređajima čiji korisnici znaju odgovarajuću lozinku za pristup pristupnoj tački. Recimo da su Pera Perić i Sima Simić povezali svoje telefone na lokalnu mrežu. Potrebno je u sistem dodati dva pametna telefona iz grupe End Devices. Nakon toga je potrebno podesiti bežični pristup mreži **etf-wireless** za svaki od ovih uređaja. Postupak podešavanja je prikazan na Slici 9.



Slika 9. Podešavanje pristupa bežičnih uređaja lokalnoj mreži

Obratite pažnju kako se nakon ispravnog podešavanja pojavljuje oznaka za prenos podataka obeležena zelenom bojom na Slici 9. **Proverite da li su bežični uređaji dobili odgovarajuće IP adrese iz opsega 192.168.30.0/24.**

Nakon ispravnog konfigurisanja pristupa mreži pokušajte da pristupite serverima **student.etf.rs** i **elektronika.etf.rs** iz WEB čitača. Takođe pokušajte da razmenite poruke elektronske pošte korišćenjem bežičnih uređaja.

5. Zaštitne barijere

Bežični pristup daje puno mogućnosti međutim takođe vrlo je osetljiv za najrazličitije vrste napada. Na primer ako neko od studenata sazna Žikinu lozinku za elektornsku poštu može slati poruke predstavljajući se kao nastavno osoblje fakulteta. Takođe svako u ovoj mreži može pomoću ftp-a pristupiti serveru **elektronika.etf.rs** i skinuti potencijalno poverljive fajlove. Jedan od načina da se ovo spreči je postavljanje zaštitnih barijera (*firewall*) kojim se filtriraju poruke koje pripadaju određenim servisima a dolaze ili idu ka posebno naznačenim uređajima ili grupi uređaja.

Kako bismo obezbedili mrežu potrebno je obezbediti sledeća prava pristupa:

1) Svi zaposleni na fakultetu imaju pristup svim serverima i servisima iz svojih kancelarija.

2) Studenti iz laboratorija imaju HTML i FTP pristup serveru **student.etf.rs** dok je FTP pristup serveru **elektronika.etf.rs** zabranjen. Takođe zabranjene su i sve poruke SMTP i POP3 ka i od servera **elektronika.etf.rs**.

3) Bežična mreža ima iste pristupe kao i studentske laboratorije sa sledećom razlikom. Dozvoljen je POP3 pristup serveru **elektronika.etf.rs** kako bi se omogućilo čitanje poruka nastavnicima i van kancelarija. I zabranjen je FTP pristup svim računarima u unutar lokalne mreže (kancelarije, lab i serveri). Takođe zabranjen je ping računara zaposlenih na fakultetu.

Zaštitna barijera se postavlja na ruteru formiranjem odgovarajućih lista pristupa. U ovom primeru definisaćemo 2 različite liste pristupa za zabranu odgovarajućeg saobraćaja koji dolazi iz studentskih laboratorija i iz bežične mreže. Liste pristupa se definišu u konfiguracionom modu rutera korišćenjem komande **access-list**. Argumenti access-list komande su sledeći:

1) Broj koji predstavlja oznaku liste pristupa. Za složenije liste brojevi počinju od 100.
2) Komanda **deny/permit** u zavisnosti da li se zabranjuje ili dozvoljava određeni saobraćaj.
3) Protokol na koji se dozvola/zabrana odnosi. Najkorišćeniji su **tcp**, **ip**, **icmp** (za ping poruke), **udp**.
4) Izvorišna adresa koja se može zadati u 3 različite forme:
    a. Korišćenjem adrese grupe računara i maske.
    b. Korišćenjem adrese jednog određenog računara. U ovom slučaju pre te adrese treba navesti ključnu reč **host**.
    c. Korišćenjem ključne reči **any** kojom se označava bilo koje izvorište.
5) Odredišna adresa važe ista pravila kao i za izvorišnu adresu.
6) Ako se navede ključna reč **eq** mogu se filtrirati samo poruke po određenom portu. Na primer **eq smtp** se odnosi samo na tcp poruke koje koriste smtp port.

Primer definisanja liste pristupa za bežičnu mrežu:

```
access-list 101 deny tcp any any eq ftp
access-list 101 deny tcp any host 192.168.1.3 eq smtp
access-list 101 deny icmp any 192.168.10.0 0.0.0.255
access-list 101 permit ip any any
```

Obratiti pažnju na poslednju komandu. Ona označava da je sav saobraćaj koji nije naveden u zabranama dozvoljen. U suprotnom bi i sav ostali saobraćaj koji nije eksplicitno naveden u pravima pristupa bio zabranjen. **Kako se poruka poredi sa pravilima redom od vrha ka dole sve dok ne naiđe na poklapanje veoma je važno da pravilo *permit ip any any* stoji na samom kraju liste!**

U slučaju da je potrebno obrisati sadržaj pristupne liste 101 to se izvodi komandom **no access-list 101**. Komanda **no** se generalno koristi za poništavanje prethodno navedenih komandi.

Nakon definisanja liste pristupa potrebno je dodeliti je odgovarajućem interfejsu. Ovde je ideja da se filtrira sav saobraćaj koji iz bežične mreže ulazi na ruter. Kako je pristupna tačka povezana na port FastEthernet7/0 rutera potrebno je konfigurisati zaštitnu barijeru na ovom priključku. Zaštitina barijera se konfiguriše u okviru podešavanja odgovarajućeg inerfejsa komandom **ip access-group** čiji argumenti su oznaka liste pristupa i oznaka **in** ili **out** koja označava da li se filtrira saobraćaj na ulazu ili na izlazu iz navedenog priključka. Primer konfigurisanja zaštitne barijere za bežičnu mrežu prikazan je na Slici 10.

```
Router(config)#access-list 101 deny tcp any any eq ftp
Router(config)#access-list 101 deny tcp any host 192.168.1.3 eq smtp
Router(config)#access-list 101 deny icmp any 192.168.10.0 0.0.0.255
Router(config)#access-list 101 permit ip any any
Router(config)#interface Fa7/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Slika 10. Podešavanje zaštitne barijere za bežičnu mrežu

Na osnovu prethodno opisanog primera konfigurisati zaštitnu barijeru na postu Fa6/0 koji je povezan sa studentskim laboratorijama.

Proveriti da li su zaista primenjena gore zahtevana prava pristupa.

6. Daljinsko podešavanje rutera

U sistemu često postoji dosta različitih rutera koji se nalaze na različitim fizičkim lokacijama. Kako administrator sistema održava se ove komponente sistema bilo bi dobro da mu se nekako omogući pristup ruteru sa neke udaljene lokacije, odnosno iz svoje kancelarije. Protokol koji se koristi za udaljeni pristup je **telnet** mada s obzirom na nezadovoljavajući nivo bezbedosti u praksi se uglavnom koristi **ssh**. Iako PacketTracer podržava testiranje **ssh** pristupa njegovo konfigurisanje je previše napredno za ovu laboratorijsku vežbu. Tako da će u ovoj vežbi biti konfigurisan **telnet**. Da bi se omogućio udaljeni pristup potrebno je postaviti kakvu-takvu sigurnost na ruter postavljanjem lozinke za ulazak u **enable** mod rutera. Ovo se radi pozivanjem komande **enable pass** _____ u okviru konfiguracinog moda rutera. Na primer:

```
Router(config)#enable pass etf
```

Sada će ruter svaki put pri kucanju komande **enable** tražiti odgovarajuću lozinku. Nakon toga je potrebno omogućiti povezivanje udaljenih računara na virtualne terminale postavljanjem odgovarajućih lozini za pristup.

```
Router(config)#line vty 0 1
Router(config-line)#pass etf
Router(config-line)#login
Router(config-line)#exit
```

Pokušajte sada da pristupite ETF ruteru sa računara administratora korišćenjem telnet protokola. Komanda kojom se ovo postiže je:

```
telnet 192.168.1.1
```

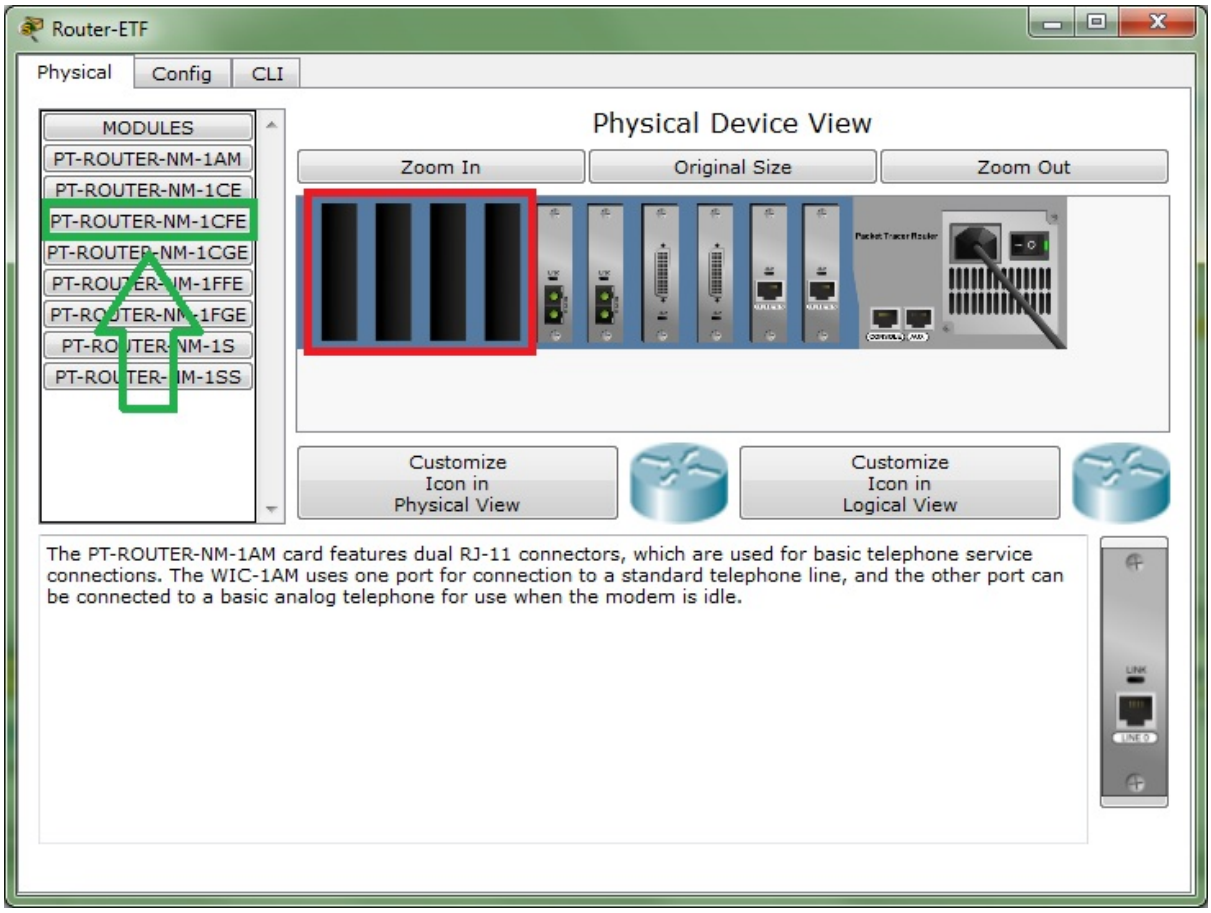
Ako ste uspeli onda svaka čast pošto ste upravo omogućili administratoru da se manje šeta. Međutim takođe ste omogućili i svima ostalima koji su se dokopali ovih lozinki da promene podešavanja rutera i eventualno skinu neke od nametnutih zabrana.

Rešite ovo ako znate da **telnet** koristi **tcp** protokol. Cilj vam je da obezbedite **telnet** pristup drugim uređajima u mreži **samo sa računara administratora**. Svima ostalima (čak i zaposlenima) je zabranjeno korišćenje **telnet** protokola.

Hint: Formirajte novu listu pristupa kojom se samo administratoru dozvoljava telnet pristup i primenite ovo pravilo na sve portove rutera.

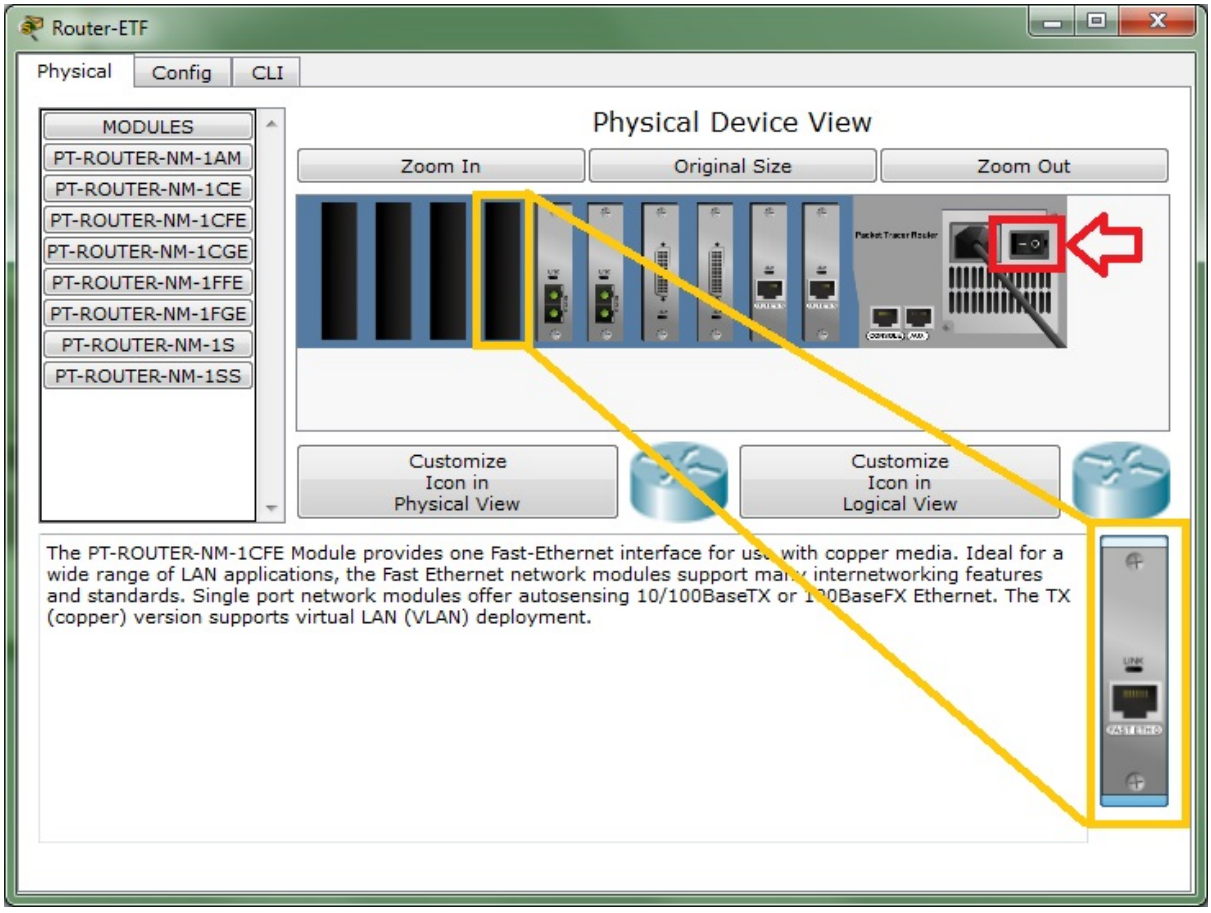
Dodatak 1. Nadogradnja rutera

Kako standardna komponenta rutera Router-PT podrazumevano ima dva FastEthernet porta potrebno je dodati još dve mrežne kartice kako bismo povezali 4 odvojena segmenta mreže. Klikom na komponentu rutera otvara se fizički pogled na uređaj kao na Slici D1.1.

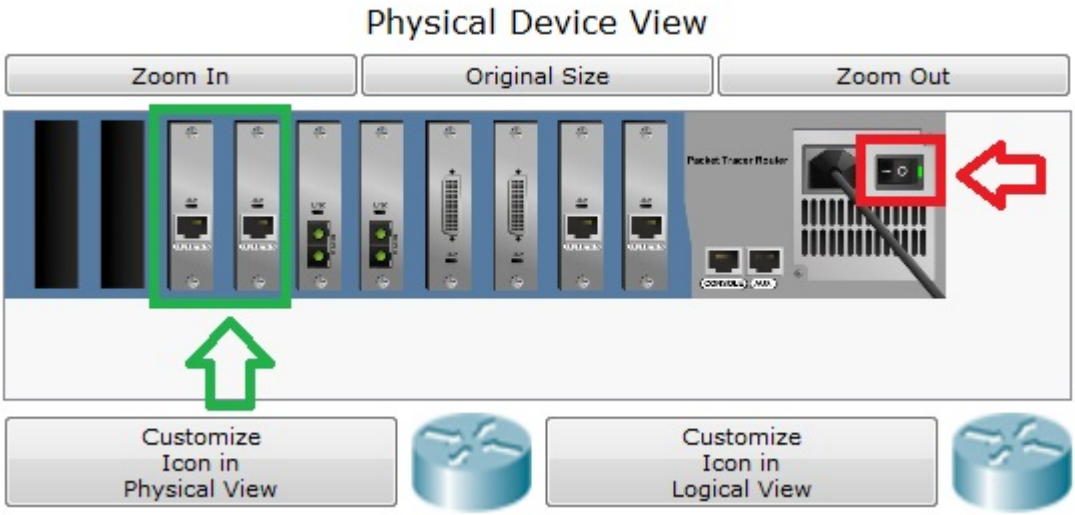


Slika D1.1. Fizički prikaz rutera

Sa Slike D1.1. se može uočiti da postoje 4 slobodna mesta za dodavanje proizvoljnih mrežnih kartica (označeno crvenom bojom). Spisak dostupnih mrežnih interfejsa naveden je u listi sa leve strane. Zelenom bojom na Slici D1.1. je označen standardni FastEthernet interfejs. Klikom na ovo polje u donjem delu prozora se pojavljuje opis interfejsa, kao i komponenta mrežne kartice u donjem desnom uglu. Na Slici D1.2. je prikazan postupak dodavanja novog mrežnog interfejsa. Da bi se ovaj postupak obavio najpre je potrebno isključiti ruter klikom na glavni prekidač, označen crvenom strelicom na Slici D1.2. Zatim je potrebno instalirati mrežnu karticu u odgovarajući slot jednostavnim prevlačenjem (*drag and drop*) pomoću miša. Fizički izgled rutera nakon instalirane dve dodatne mrežne kartice je prikazan na Slici D1.3. Nakon postupka nadogradnje obavezno ponovo uključiti ruter kako bi mogao da se koristi dalje u sistemu.



Slika D1.2. Instaliranje dodatne mrežne kartice



Slika D1.3. Izgled rutera nakon uspešno instalirane dve nove mrežne kartice