ELEKTROTEHNIČKI FAKULTET
UNIVERZITET U BEOGRADU

KOMPARATIVNA ANALIZA INTERNIH PROTOKOLA RUTIRANJA

Master rad

Mentor:
Doc. dr. Zoran Čiča

Kandidat:
Marko Stojanović 2015/3424

Beograd, Septembar 2016.

SADRŽAJ

SADRŽAJ **2**
1. UVOD **3**
2. PROTOKOLI RUTIRANJA **4**
2.1. KARAKTERISTIKE PROTOKOLA RUTIRANJA 4
2.2. KLASIFIKACIJA PROTOKOLA RUTIRANJA 5
2.3. STATIČKO I DINAMIČKO RUTIRANJE 6
3. RUTER (*ROUTER*) **8**
3.1. TIPOVI RUTERA 8
3.2. DELOVI RUTERA 9
3.3. KONFIGURACIJA RUTERA 9
3.4. CISCO1841 RUTER 11
4. SVIČ (*SWITCH*) **12**
4.1. PRINCIP FUNKCIONISANJA SVIČA 12
4.2. VRSTE SVIČEVA 13
4.3. CISCO CATALYST 2960 SWITCH 16
5. EIGRP **17**
5.1. IDEJA I RAZVOJ EIGRP PROTOKOLA 17
5.2. GLAVNE KARAKTERISTIKE EIGRP PROTOKOLA 17
5.3. PRINCIPI FUNKCIONISANJA EIGRP PROTOKOLA 18
5.4. DIFFUSING UPDATE ALGORITHM (DUAL) 20
5.5. EIGRP METRIKA 20
5.6. RELIABLE TRANSPORT PROTOCOL (RTP) 21
5.7. NEDOSTACI EIGRP PROTOKOLA 21
6. OSPF **23**
6.1. IDEJA I RAZVOJ OSPF PROTOKOLA 23
6.2. GLAVNE KARAKTERISTIKE I PREDNOSTI OSPF PROTOKOLA 23
6.3. PRINCIP FUNKCIONISANJA 25
6.4. NEDOSTACI OSPF PROTOKOLA 30
7. CISCO PACKET TRACER **31**
8. PRAKTIČNI DEO ..... ERROR! BOOKMARK NOT DEFINED.
8.1. KONFIGURISANJE MREŽE 35
8.2. KONFIGURISANJE OSPF PROTOKOLA 40
8.3. KONFIGURISANJE EIGRP PROTOKOLA 42
8.4. POREĐENJE PROTOKOLA NA OSNOVU BRZINE KONVERGENCIJE 43
8.5. POREĐENJE PERFORMANSI PROTOKOLA PRI RAZLIČITIM PARAMETRIMA LINKA 45
9. ZAKLJUČAK **48**
LITERATURA **49**

1. UVOD

Informacija je ključ uspeha! Rečenica koja se sve više čuje kako u svakodnevnom, tako i u poslovnom razgovoru. Ovo pravilo nije proizvod savremenog sveta, ono se prožima kroz čitavu ljudsku istoriju, ostaje nepromenjeno i svakim danom se sve više potvrđuje. Jedino što se neprestano menja jeste način i brzina distribuiranja informacija. Počevši od dimnih signala, pa sve do najsavremenijih komunikacionih tehnologija, od presudnog značaja je da poslate informacije stignu na vreme i tačno onome kome su namenjene. Upravo se zbog toga neprestano teži ka unapređenju komunikacionih metoda, izboru komunikacionih medijuma i traženju najboljih načina i pravila za njihovo zajedničko funkcionisanje.

U oblasti savremenih komunikacionih tehnologija, brzina prenosa informarcija zavisi, kako od kapaciteta mrežne infrastrukture, tako i od načina prenosa informacija. Često se dešava da je poboljšanje mrežnih performansi moguće samo što efikasnijim iskorišćenjem postojećih resursa, odnosno da samo "fizičko" unapređenje nije tehnički izvodljivo. U ovakvim situacijama, neophodno je sagledati sve mogućnosti i zahteve i na osnovu toga odrediti protokol rutiranja koji će obezbediti najveći benefit u postojećoj mreži.

Predmet ovog rada jeste upravo odabir odgovarajućeg protokola rutiranja, kao i poređenje različitih protokola koji se koriste u telekomunikacionim mrežama. Najveći deo rada biće posvećen OSPF i EIGRP protokolima, njihovim principima funkcionisanja, načinu implementacije i poređenju njihovih performansi.

Na samom početku teze upoznaćemo se sa protokolima rutiranja, njihovom namenom i osnovnim podelama. U drugom delu rada, izdvojićemo par reči kako bismo se upoznali sa osnovnim mrežnim komponentama, tj. upoznali uređaje na kojima funkcionišu protokoli koji su nam od interesa. Treći deo rada biće posvećen upoznavanju sa OSPF i EIGRP protokolima, njihovim principima funkcionisanja, načinu implementacije, prednostima i manama. U završnom delu, kroz simulaciju u softverskom alatu *Cisco Packet Tracer,* na praktičnom primeru izvršićemo analizu i komparaciju gore navedenih protokola. Na kraju ćemo prikazati rezultate i izneti zaključak našeg rada, kao i smernice za dalja istraživanja.

2. PROTOKOLI RUTIRANJA

Protokol rutiranja predstavlja skup pravila kojim ruteri dinamički razmenjuju informacije o putanjama kojima paket treba da se kreće da bi dostigao željenu destinaciju. Primarni cilj rutiranja je pronalazak optimalne putanje kroz mrežu, što se postiže primenom različitih algoritama u zavisnosti od protokola rutiranja. Kada se dogodi neka izmena u topologiji računarske mreže, najbliži ruter kod koga se desila promena, zapisuje je u svoju tabelu rutiranja, a zatim protokoli rutiranja pokreću mehanizme kojima se informacija o promeni u topologiji mreže prosleđuje ostalim uređajima u mreži. Ovako ruteri dinamički ažuriraju svoje tabele rutiranja, koje određuju najbolji put paketa.

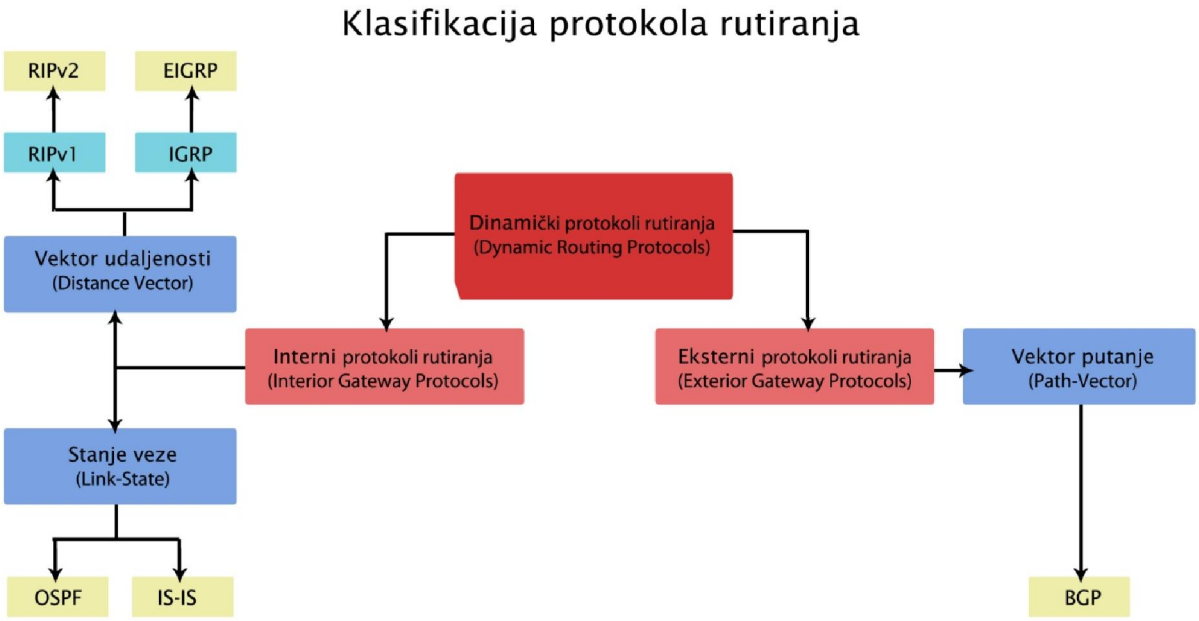
2.1. Karakteristike protokola rutiranja

Glavne karakteristike protokola rutiranja su [1]:

- Vreme konvergencije (za mrežu kažemo da je konvergentna kada su tabele rutiranja kod svih rutera unutar mreže kompletne i ispravne, pa je vreme konvergencije vreme za koje mreža konvergrira nakon izvršene promene u topologiji). U vreme konvergencije su uključeni:
    - razmena informacija
    - obrada informacija, procena najboljih ruta
    - unošenje izmena u tabele rutiranja
- Skalabilnost – podržana veličina mreže u zavisnosti od korišćenog protokola.
- Klasnost – protokoli rutiranja mogu da budu:
    - klasni – stariji protokoli (RIPv1 i IGRP) koji podrazumevaju da adresa pripada nekoj od klasa (A, B, C).
    - besklasni – pri razmeni informacija uključuju podmrežnu masku uz adresu mreže.
- Zauzetost resursa – protokoli rutiranja pri razmeni i obradi informacija zauzimaju hardverske resurse (memoriju, procesorsko vreme ili propusni opseg linka). Veća potrebna zauzetost resursa od strane protokola rutiranja zahteva jaču opremu unutar mreže.
- Implementacija i održavanje – definiše nivo znanja koji je potreban administratoru mreže, koji radi sa određenim protokolima rutiranja, kako bi pravilno održavao mrežu.

2.2. **Klasifikacija protokola rutiranja**

Na osnovu oblasti rutiranja, unutar autonomnog sistema ili između autonomnih sistema, protokole rutiranja možemo da klasifikujemo kao interne i eksterne. Interni protokoli, koji će biti obrađeni u radu, dele se na dva osnovna tipa protokola rutiranja, a to su *distance vector* (vektor udaljenosti) i *link-state* (stanje veze). Slika 2.2.1 daje prikaz klasifikacije protokola rutiranja.



Slika 2.2.1 Klasifikacija protokola rutiranja

Distance vector protokoli donose odluke na osnovu informacije o „udaljenosti“ (*distance*) do odredišne mreže. To može biti broj rutera do krajnjeg odredišta, ali i neka kompleksnija metrika. U ovom slučaju informacije o rutama se prenose kao vektori, definisani rastojanjem i pravcem. Pravac predstavlja izlazni interfejs na ruteru ili susedni ruter na putanji ka odredištu. Razmena informacija o rutama se vrši periodičnim slanjem tabele rutiranja susednim ruterima, što opet ima uticaja na smanjenje propusnog opsega za korisnički saobraćaj. Uključuju protokole kao što su: RIP, IGRP i EIGRP. Nedostatak *distance vector* protokola predstavlja i veće vreme konvergencije u poređenju sa *link-state* protokolima. Međutim, osnovna prednost ovih protokola je mala kompleksnost realizacije i održavanja.

Link-state protokolima se rad zasniva na Dajkstrinom (SPF) algoritmu. Tu pripadaju i OSPF, DNA Phase V, IS-IS, NSLP i AURP. *Link-state* protokoli se razlikuju od *distance vector* protokola po tome što se odluke donose na osnovu kompletne topologije mreže. Na osnovu informacija o linkovima, koje prosleđuju susednim ruterima, kreira se baza sa podacima o topologiji cele mreže. Primenom SPF (*Shortest Path First*) algoritma svaki ruter pronalazi najbolju putanju. U ovom slučaju ne postoji periodično slanje informacija o rutama, već se one šalju samo kada se dogodi neka promena u mreži. Još jedna prednost *link-state*, u odnosu na *distance vector* protokole je i malo vreme konvergencije. Zbog kompleksnog principa funkcionisanja, *link-state* protokoli rutiranja su zahtevniji za implementaciju i održavanje u poređenju sa *distance vector* protokolima.

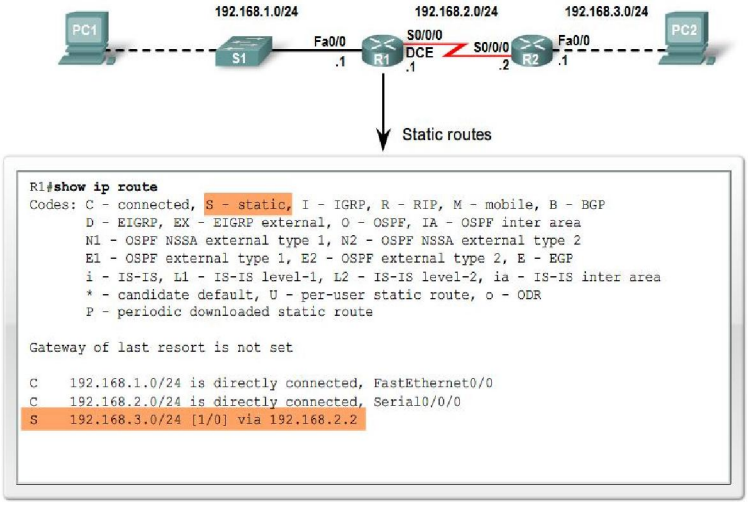
2.3. **Statičko i dinamičko rutiranje**

Direktno povezana mreža je mreža koja je direktno povezana za jedan od interfejsa rutera. Kada je interfejs konfigurisan sa IP adresom i subnet maskom, interfejs postaje host na toj povezanoj mreži. Mrežna adresa i subnet maska, zajedno sa tipom i brojem interfejsa, upisuju se u tabelu rutiranja kao direktno povezane mreže.

Udaljena mreža je mreža koja nije direktno povezana sa ruterom, drugim rečima, udaljena mreža je mreža do koje se može doći samo slanjem paketa na drugi ruter. Udaljene mreže se dodaju u tabelu rutiranja koristeći dinamički protokol za rutiranje ili konfigurisanjem statičkih putanja. Koristeći dinamički protokol za rutiranje, ruteri su sposobni da nauče dinamičke putanje do udaljenih mreža. Statičke putanje su putevi do mreža koje administrator mora ručno da konfiguriše.

Zadatak protokola rutiranja je da na efikasan način prenesu relevantne informacije o udaljenim mrežama, ali i da dinamički propagiraju informacije o promenama u mreži (uključenje/isključenje linka, aktivacija novog rutera u mreži i sl.). Upravo iz tog razloga dinamičko rutiranje je nezamenljivo u današnjim računarskim mrežama, pošto uspešno rešava problem skalabilnosti u mrežama koji postoji kod statičkog rutiranja.

Statičko rutiranje – Statička putanja uključuje mrežnu adresu i subnet masku udaljene mreže, zajedno sa IP adresom narednog hopa rutera ili izlaznim interfejsom. Statičke putanje su označene sa S u tabeli rutiranja kao što je prikazano na slici 2.3.1.

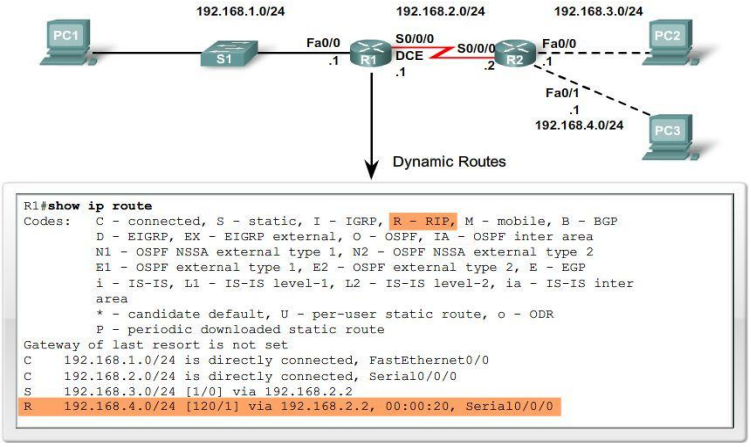


Slika 2.3.1 Statičko rutiranje – putanje u tabeli

Ako se mreža sastoji od samo nekoliko rutera, pri čemu postoji samo jedan izlaz na internet, najbolje je koristiti statičko rutiranje, jer dinamičko rutiranje samo može povećati administrativne troškove.

Dinamičko rutiranje - Udaljene mreže se takođe mogu dodati u tabelu rutiranja pomoću protokola za dinamičko rutiranje. RIP (*Routing Information Protocol*) je jedan od prvih protokola za dinamičko rutiranje. U dinamičkom rutiranju protokol rutiranja ima ulogu da deli informacije između rutera o dostupnosti i statusu udaljenih mreža. Dinamičko rutiranje je neophodno u velikim

mrežama. U dinamičke protokole rutiranja spadaju RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*), EIGRP (*Enhanced Interior Gateway Routing Protocol*) [2]. Primer jednog zapisa u tabeli rutiranja generisanog dinamičkim protokolom rutiranja je dat na slici 2.3.2.



Slika 2.3.2. Dinamičko rutiranje – putanje u tabeli

3. RUTER (*ROUTER*)

Ruter je mrežni uređaj koji usmerava pakete između računarskih mreža. On funkcioniše tako što za svaki paket odredi putanju kojom taj paket treba da ide i taj isti paket prosledi sledećem ruteru u nizu, do konačnog odredišta.

Ruter je povezan sa dva ili više linka iz različitih mreža, za razliku od sviča koji povezuje linkove iz samo jedne mreže. Kada paket dođe do rutera, ruter čita informacije o adresi koja se nalazi u paketu, kako bi utvrdio sledeći hop paketa (to može biti sledeći ruter u nizu ili odredišna mreža). Ruter na osnovu tabele rutiranja, koja sadrži mrežne adrese, i odredišne adrese paketa, dalje određuje na koji interfejs (logičku adresu) se prosleđuje paket tj. određuje sledeći hop.

3.1. Tipovi rutera

Najpoznatiji tipovi rutera su [1]:

- Softverski ruteri: u pitanju su serveri koji nemaju specijalizovan hardver za prosleđivanje paketa već to rade softverski; da bi igrao ulogu pravog rutera mora da sadrži bar dva mrežna porta.
- Hardverski ruteri: u sebi sadrže specijalizovan hardver za usmeravanje paketa; znatno su brži od softverskih rutera.
- Ruteri Internet provajdera: oni čine osnovu Interneta i namenjeni su za kontrolu saobraćaja između provajdera (*edge routers*), ali i u okviru same mreže provajdera (*core routers*).
- Korporacijski ruteri: uglavnom se koriste u velikim korporacijama, jer obezbeđuju povezanost sa Internetom, rade distribuciju saobraćaja radi ravnomernog opterećenja mreže i obezbeđuju rezervni izlaz sa mreže. Oni dostavljaju podatke pri velikoj brzini, duž optičkih vlakana.
- Kućni ruteri: njihova jedina funkcija je najčešće da povežu kućnu mrežu sa Internetom preko provajdera. Ako se konekcija ostvaruje preko ADSL veze, onda se taj ruter zove *ADSL Router*. Ako ruter obezbeđuje i bežično povezivanje, onda je to bežični – *Wireless Router*.

Napomenimo da prve dve stavke definišu tip izrade rutera, a sledeće tri stavke poziciju rutera u mreži.

3.2. **Delovi rutera**

Ruter čine četiri osnovne komponente: ulazni i izlazni portovi (tzv. linijski moduli), kontrolna ravan (procesor) i komutatorska matrica. Ulazni port je zadužen za funkcije rutera koje se odnose na fizički sloj veze.

Ulazni port prima okvir sa linije, detektuje greške u prenosu i iz okvira izdvaja paket. Dodatno, ulazni port sadrži bafer za čuvanje paketa pre usmeravanja ka komutatorskoj matrici.

Izlazni port obavlja iste funkcije kao ulazni, samo u obrnutom smeru. Odlazni paketi se smeštaju u red čekanja, pakuju u okvire, a onda se taj okvir konvertuje u signal koji se šalje na liniju.

Kontrolna ravan obavlja funkciju mrežnog sloja. Ona implementira protokole rutiranja i definiše sadržaj tabele rutiranja na linijskim modulima. Ulazni port u procesu određivanja izlaznog porta pristiglog paketa pretražuje dotičnu tabelu.

Komutatorska matrica omogućava prenos paketa iz bilo kog ulaznog bafera u bilo koji izlazni bafer, a da pri tome bude u stanju da istovremeno obavlja prenos više od jednog paketa.

3.3. **Konfiguracija rutera**

Mrežni uređaji, ruteri i svičevi međusobno povezuju više uređaja. Iz tog razloga, ove komponente imaju nekoliko tipova portova i interfejsa koji se koriste za povezivanje kablova sa uređajem. Ove veze mrežnih rutera se mogu podeliti na konfiguracioni port (*Menagement Port*) i korisnički interfejs (*Inband Router*).

Konfiguracioni port su konzola i pomoćni portovi koji se koriste za konfigurisanje, upravljanje i debagovanje rutera. Ne koriste se za prosleđivanje paketa, za razliku od LAN i WAN interfejsa.

Korisnički interfejs su LAN i WAN interfejsi konfigurisani jedinstvenom IP adresom za prenos korisničkog saobraćaja. *Ethernet* interfejsi su najčešće LAN veze, a zajedničke WAN veze uključuju serijski i DSL interfejs.

Postoji nekoliko načina da se pristupi podešavanjima rutera (komandnoj liniji). Najčešće metode su:

- Konzola - koristi serijsku ili USB vezu male brzine kako bi obezbedio direktnu konekciju *out-of-band* pristupa upravljanja.
- *Telnet* ili SSH – dve metode za daljinski pristup CLI sesiji preko aktivnog mrežnog interfejsa.
- AUX port – koristi se za daljinsko upravljanje rutera, koristeći *dial-up* konekciju preko telefonske linije i modema. Konzola i AUX priključak se nalaze na ruteru.

Pored ovih portova, ruteri imaju i mrežne interfejse za prijem i slanje IP paketa. Ruteri imaju više interfejsa koji se koriste za povezivanje više mreža. Interfejsi povezuju različite tipove

mreža, pa su zato potrebne različite vrste medija i konektora. Svaki interfejs na ruteru je domaćin ili član na različitoj IP adresi i mora na različitoj adresi i da bude konfigurisan sa IP adresom i subnet maskom. Najčešće nije dozvoljeno da na ruteru postoje dva aktivna interfejsa koja pripadaju istoj mreži.

Interfejs rutera može da se podeli u dve grupe: *Ethernet* LAN i *Serial* WAN interfejs. *Ethernet* LAN interfejs se koristi da poveže kablove koji se prekidaju sa LAN uređaja (kompjutera ili sviča) i da poveže rutere međusobno. *Serial* WAN interfejs se koristi za povezivanje rutera sa spoljnim mrežama, koje su najčešće na velikoj geografskoj udaljenosti. Slično LAN interfejsu, svaki WAN interfejs ima svoju IP adresu i subnet masku, koja ga identifikuje kao člana određene mreže. Na slici 3.3.1 je prikazan izgled Cisco rutera 1841, gde se mogu videti različiti tipovi portova.

Slika 3.3.1. Cisco ruter 1841

3.4. Cisco1841 ruter

U okviru ovog rada, preciznije, u simulaciji izvedenoj u softveru *Cisco Packet Tracer,* koristiće se ruter kompanije Cisco sa oznakom 1841, čije su performanse navedene na slici 3.4.1.

General	
Authentication Method	Secure Shell v.2 (SSH2)
RAM	128 MB SDRAM
Encryption Algorithm	Secure Shell v.2 (SSH2)
Manufacturer	Cisco
Networking	
Form Factor	Desktop
Type	Router
Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fest Ethernet
Network / Transport Protocol	IPSec
Features	Intrusion Prevention System (IPS), URL filtering, VPN support, firewall protection, hardware
Remote Management Protocol	SNMP
Power Device	
Power Provided	50 Watt
Nominal Voltage	AC 120/230 V
Frequency Required	50/60 Hz
Type	Internal power supply
Camera	
Installed Size	64 MB
Interface provided	
Type	Management, Network, Serial
Interface	Ethernet 10Base-T/100Base-TX, auxiliary, console
Qty	1, 2
Connector Type	RJ-45
Miscellaneous	
Rack Mounting Kit	Optional
Encryption Algorithm	AES, DES, SSL, Triple DES
Height (Rack Units)	1 m
RAM	
Installed Size	128 MB
Technology	SDRAM
Flash Memory	
Max Supported Size	128 MB
Software / System Requirements	
Type	Cisco IOS IP Base
Header	
Brand, Product Line	Cisco
Model	1841
Compatibility	PC
Dimensions & Weight	
Dimensions	10.8x13.5x1.9 in
Weight	5.95 lbs
Expansion Slots	
Type	Memory
Total Qty	1,2
Free Qty	1
Slot Required	

Slika 3.4.1 Performanse rutera 1841 [10]

4. SVIČ (*SWITCH*)

Sa konstantnim povećanjem broja personalnih računara, a samim tim i veličine i kompleksnosti samih računarskih mreža, došlo se do zaključka da *hub,* kao mrežni uređaj, ne može da zadovolji novonastale zahtevane mrežne performanse. Naime, *hub* je imao samo električnu, ali ne i logičku funkciju, tj. samo je pojačavao signal i prosleđivao saobraćaj ka svim čvorovima. Za razliku od *hub*-a, svič kao mrežni uređaj ima mogućnost dostave saobraćajnih paketa tačno onim korisnicima kojima su inicijalno namenjeni. Takođe, svič ima mogućnost da obezbedi korisniku konekciju po punoj brzini, dok je kod *hub*-a ta konekcija bila deljena između korisnika, što bi često bilo neupotrebljivo ukoliko bismo u okviru jedne mreže imali veći broj računara.

4.1. Princip funkcionisanja sviča

Sam princip funkcionisanja sviča zasniva se na povezivanju dva segmenta LAN (*Local Area Network*) mreže na 2. sloju OSI referentnog modela odnosno na sloju veze (*Data Link Layer*). Mrežni uređaji se priključuju na svič preko RJ-45 portova i jednoznačno su definisani svojim MAC adresama (*Media Access Control address*) koje su nepromenljive i predstavljaju osnovni parametar za prosleđivanje saobraćaja na sloju veze. Ovakav princip funkcionisanja sviča omogućio je mnogo veću efikasnost rada mreže, kao i veći nivo sigurnosti podataka.

Osnova rada sviča jeste da pakete podataka koji su pristigli sa porta A prosledi ka portu B, odnosno ka korisniku kome su namenjeni. Logično pitanje koje se ovde postavlja jeste, kako svič "zna" koji port je odredišni. Odgovor je u poznavanju MAC adresa, odnosno, u vezama ulaznih i izlaznih portova sa MAC adresama uređaja koji su na njih povezane. Informaciju o tome svič čuva u svojoj internoj memoriji, u takozvanim CAM tabelama. Kada paket stigne na port A, svič iz zaglavlja paketa saznaje MAC adresu odredišnog čvora. Nakon toga, u svojoj tabeli pronalazi tu MAC adresu i port koji je sa njom uparen. Ukoliko svič u svojoj tabeli nema uparenu MAC adresu i port, pokreću se mehanizmi za saznavanje te adrese. Takođe, princip je nešto drugačiji kada je reč o *broadcast* porukama koje se po prijemu sa ulaznog porta prosleđuju ka svim izlaznim portovima.

MAC adresa (*Media Access Control address*) odnosno fizička adresa predstavlja jedinstveno obeležje eternet mrežnih uređaja. Osnovna uloga MAC adrese jeste identifikacija uređaja na mreži. Sama dodela MAC adresa regulisana je konvencijom od strane posebne međunarodne organizacije (IEEE), čime je obezbeđeno da se na mreži nikad ne mogu naći dva uređaja sa istim MAC adresama. MAC adresa je takozvana "*burned-in address*" (BIA), što znači da zauvek ostaje nepromenjena. Ipak, zlonamerni korisnici pronalaze način da softverski promene fizičku adresu nekog mrežnog uređaja radi različitih zloupotreba i prisluškivanja saobraćaja.

Sama adresa sastoji se od 48 bita što znači da se teorijski može dodeliti 2^{48} mogućih različitih MAC adresa, iz čega se može zaključiti da je njihov broj izuzetno veliki. Najčešće

predstavljanje MAC adresa je u obliku 6 parova heksadecimalnih cifara razdvojenih dvotačkom 01:23:45:67:89:ab, odnosno crticom 01-23-45-67-89-ab ili u 3 grupe sa po 4 cifre i tačkama između njih 0123.4567.89ab. Prvih 6 heksadecimalnih cifara predstavljaju identifikator proizvođača, dok preostale cifre predstavljaju serijski broj mrežne kartice [1].

4.2. **Vrste svičeva**

Podelu svičeva možemo izvršiti na nekoliko načina. Prva podela jeste ona na osnovu upravljivosti, gde razlikujemo dva tipa svičeva: upravljivi (*managed*) i neupravljivi (*unmanaged*). Osnovna razlika ova dva tipa leži u tome, što se upravljivi svič može konfigurisati pre samog korišćenja kako bi se njegove mogućnosti i karakteristike prilagodile zahtevima same mreže, dok se neupravljivi svič koristi po principu "*plug and play*" tj. koristi se bez prethodnog podešavanja.

1) Upravljivi svič ima sve mogućnosti kao i neupravljivi, uz niz izuzetno korisnih mogućnosti koje povećavaju perfomanse i kvalitet rada same mreže. Jedna od glavnih prednosti jeste mogućnost kontrole protoka i prioritizacije saobraćaja. Na ovaj način se servisima koji su višeg priroriteta dodeljuje veća količina mrežnih resursa. Takođe, jedna od bitnih karakteristika upravljivih svičeva jeste mogućnost kontrole pristupa korisnika, čime se povećava nivo sigurnosti mreže, a moguće je i kreiranje VLAN-ova čime se postiže razdvajanje pojedinih delova LAN mreže. Redudantnost mreže je još jedna od bitnih karekteristika, jer se prilikom otkaza nekog linka, korišćenjem određenih protokola (*Spanning Tree Protocol*) može efikasno odrediti alternativna ruta za prenos podataka. To omogućava sprečavanje kreiranja zatvorenih petlji, a samim tim posao administratora mreže čini daleko lakšim [4].
2) Za razliku od upravljivih svičeva, neupravljivi svičevi imaju daleko manje mogućnosti, ali je samim tim njihova cena daleko niža. Upravo zbog toga su veoma popularni u malim mrežama gde ne postoje potrebe za posebnim servisima, već samo za brzo i jednostavno povezivanje [4].

Slika 4.2.1 Upravljivi (*Managed*) svič

Slika 4.2.2 Neupravljivi (*Unmanaged*) svič

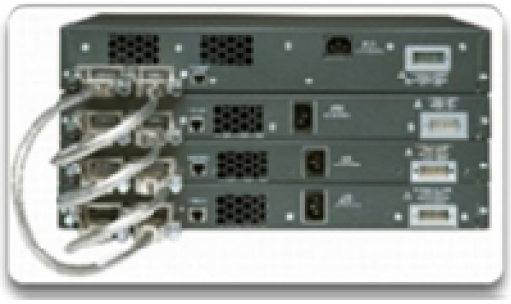
Zaključak koji se nameće jeste da oba tipa imaju svoju primenu, svoje prednosti i svoje mane. Ono što je sigurno, jeste da mreže gotovu uvek rastu jako brzo, kao i to da se najčešće uvode novi servisi (na primer: bežični LAN i IP telefonija). Imajući to u vidu, nekako se ipak nameće zaključak da je bolje rešenje, posebno dugoročno, odabrati upravljivi svič.

Druga podela svičeva jeste na osnovu njihove forme. Naime, kao što je ranije napomenuto, u različitim situacijama potrebni su različiti svičevi. Ipak, ono što se u ovom trenutku postavlja kao pitanje jeste, da li će se zahtevi za određenim performansama menjati i da li će to usloviti "fizičke" promene na sviču. Upravo zbog toga, na raspolaganju imamo dve forme svičeva. Razlikujemo svičeve sa fiksnom konfiguracijom i modularne svičeve.

1) Svičevi sa fiksnom konfiguracijom, kao što im samo ime kaže, ne mogu menjati svoje performanse nadogradnjom fizičkih komponenti. Na primer, ukoliko se odlučimo za svič sa fiksnom konfiguracijom, koji ima 24 gigabitna porta, nismo u mogućnosti da dodamo nove portove, čak i ukoliko se javi potreba za njima [4].
2) Modularni svičevi, za razliku od svičeva sa fiksnom konfiguracijom, nude mnogo veću fleksibilnost. Javljaju se u različitim dimenzijama sa različitim brojem rekova koji se koriste za instalaciju takozvanih modularnih linija. Modularne linije su slične karticama koje se instaliraju u računarima, tj. mogu se uvek menjati u slučaju potrebe za poboljšanjem performansi sistema. Ovde važi pravilo što više - to bolje, tj. koliko imamo rekova, toliko modularnih linija možemo dodati. Na primer, ako kupimo svič koji sadrži jednu modularnu liniju sa 24 gigabitna porta, ali to u jednom trenutku prestane da zadovoljava naše potrebe, vrlo lako možemo instalirati još jednu modularnu liniju i tako dobiti svič sa 48 portova [4].

Slika 4.2.3 Svič sa fiksnom konfiguracijom

Slika 4.2.4 Modularni svičevi



Slika 4.2.5 Stekabilni svičevi

Takođe, važno je napomenuti da se svičevi mogu na određeni način povezati kako bi funkcionisali kao jedan svič sa većim brojem portova. To su takozvani stekabilni svičevi koji se povezuju posebnim kablovima. Benefiti ovakve strukture su mnogo lakše upravljanje mrežom i mogućnost lake i brze nadogradnje sistema sa već postojećom opremom.

4.3. Cisco Catalyst 2960 switch

Product Specifications	
Type	Fixed
Topology	Ethernet (10/100BaseTX) Ethernet (10/100/1000BaseT)
Maximum Port density	24 10/100 ports
Uplinks	2 10/100/1000 ports
Modular/Expansion Slots	n/a
Architecture	Layer 2 Switching (basic connectivity), Layer 2 Switching (intelligent services), Voice Enabled
Form Factor	Fixed, Rack Mountable, Standalone/Clustering
Dimensions	1.73 x 17.5 x 9.3 in.
DRAM	16 MB
Features	
Specialized Service Modules	n/a
Security	
DHCP Snooping	✓
Dynamic ARP Inspection	
IP Source Guard	
RP Rate Limiters	
TCP Intercept	
802.1x	✓
Port Security	✓
Dynamic VLANs	✓
Private VLANs	
Private VLAN Edge	✓
Secure Shell	✓
SNMPv3	✓
Unicast RPF	
ACLs (L2-L4)	✓
Kerberos	✓
TACACS+	✓
RADIUS	✓
High Availability/Resilliency	
Hardware Redundancy	External Redundant Power Supply
High Availability/Resilliency	PVST, Broadcast Suppression, Unicast Suppression, Mulitcast Suppression, Spanning Tree, Portfast, Uplink Fast, Backbone Fast, 802.1s, 802.1w
Management	
Management features	SPAN, RSPAN, CiscoView, Cisco Discover Protocol (CDP), Virtual Trunking Protocol (VTP), Telnet Client, BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clustering, Web-Based Management
Scalability	
WAN Interface Support	n/a
Throughput	6.5 Mpps
Backplane Capacity	16 Gbps
Number of VLANs	255

Slika 4.3.1 Performanse sviča Catalyst 2960 [10]

U okviru ovog rada, preciznije, u simulaciji izvedenoj u softveru *Cisco Packet Tracer,* koristiće se Cisco svič sa oznakom Catalyst 2960, čije su performanse navedene na slici 4.3.1.

5.EIGRP

5.1. Ideja i razvoj EIGRP protokola

Enhanced Interior Gateway Routing Protocol, odnosno EIGRP, je protokol koji je za svoje potrebe razvila kompanija CISCO i koji se izvršava na ruterima ove kompanije. EIGRP protokol razvijen je 1992. godine i pojavio se kao naslednik IGRP protokola, koji je takođe vlasništvo CISCO kompanije i koji se u svom prvobitnom obliku pojavio 1985. godine. EIGRP se, kao što i samo ime kaže, smatra usavršenom, odnosno unapređenom verzijom IGRP protokola [2].

Glavni razlog koji je doveo do neophodnog usavršavanja IGRP protokola jeste taj što je on takozvani *classful* protokol rutiranja, a sa razvojem informacionih tehnologija broj IP adresa se rapidno smanjivao. IGRP je ubrzo počeo da pokazuje svoje nedostatke, jer je zbog fiksne dužine subnet maske podrazumevao da svi elementi jedne klase pripadaju istom subnetu. Rešenje ovog problema doneo je EIGRP korišćenjem subnet maske promenljive duzine (*variable length subnet masks* (VLSM)). Pored ovog poboljšanja, EIGRP je promenio mehanizam korišćen za obradu i razmenu informacija o rutama, pa je umesto dotadašnjeg Belman-Fordovog algoritma (*Bellman-Ford Algorithm*) počeo sa korišćenjem mnogo efikasnijeg DUAL algoritma (*Diffusing Update Algorithm*) [6]. O samom DUAL algoritmu će biti dato više detalja kasnije u poglavlju.

5.2. Glavne karakteristike EIGRP protokola

EIGRP se ranije često nazivao hibridnim protokolom zbog toga što u sebi nosi karakteristike kako *distance vector* protokola, tako i *link-state* protokola. Ipak, ovaj naziv je pomalo zastareo tj. korišćen je u starijoj dokumentaciji. Ovaj naziv je pomalo varljiv, jer je EIGRP u potpunosti *distance vector* protokol, a pomisao da je hibrid proizilazi iz nekih njegovih osobina koje se sreću i kod *link-state* protokola. Naime, EIGRP oglašava svoje putanje kao *distance vector* protokoli, a stvara odnose sa susedima kao *link-state* protokoli. Na primer, EIGRP ne šalje pakete o stanju veze (*link-state* pakete), kao što to rade neki drugi protokoli (primer: OSPF), umesto toga, EIGRP šalje tradicionalne *distance vector update* pakete, koji sadrže informacije o mrežama, kao i troškove dolaska do tih mreža iz perspektive rutera koji ih oglašavaju. Sa druge strane, EIGRP ima karakteristike *link-state* protokola jer sinhronizuje tabele rutiranja između suseda na početku, a zatim šalje specifična ažuriranja samo kad dođe do izmena u topologiji mreže. Ova karakteristika EIGRP se ističe u prvi plan kada je reč o velikim mrežama.

Pored navedenog, bitne karakteristike koje daju veliku prednost EIGRP protokolu u odnosu na druge protokole su [6]:

- Podrška za IP, IPX i Apple Talk preko modula zavisnih od protokola
- Smatra se besklasnim protokolom (kao RIPv2 i OSPF)

- Podrška za VLSM/CIDR
- Podrška za sumarizaciju mreža
- Efikasno otkrivanje suseda
- Komunikacija preko *Reliable Transport Protocol-a* (RTP)
- Odabir najbolje rute korišćenjem DUAL algoritma
- Autentifikacija

5.3. Principi funkcionisanja EIGRP protokola

EIGRP koristi niz različitih tipova paketa kako bi razmenjivao informacije sa susednim ruterima. Razlikujemo pet tipova paketa koji se šalju korišćenjem RTP (*Reliable Transport Protocol*) protokola:

1) *Hello packets* - Služe za otkrivanje suseda i uspostavljanje susedskih odnosa. Za njihovo slanje koristi se *multicast* način slanja bez garantovane dostave.
2) *Update packets* - Služe za propagiranje informacija o rutama ka EIGRP susedima. Za njihovo slanje može se koristiti *multicast* ili *unicast* način slanja sa garantovanom dostavom.
3) *Acknowledgment packets* - Služe za potvrdu prijema EIGRP poruka koje su poslate sa garantovanom dostavom. Za njihovo slanje koristi se *unicast* način slanja bez garantovane dostave.
4) *Query packets* - Služe za slanje upita o ruti od suseda. Za njihovo slanje može se koristiti *multicast* ili *unicast* način slanja sa garantovanom dostavom.
5) *Reply packets* - Služe za slanje odgovora na upit o ruti. Za njihovo slanje koristi se *unicast* način slanja sa garantovanom dostavom.

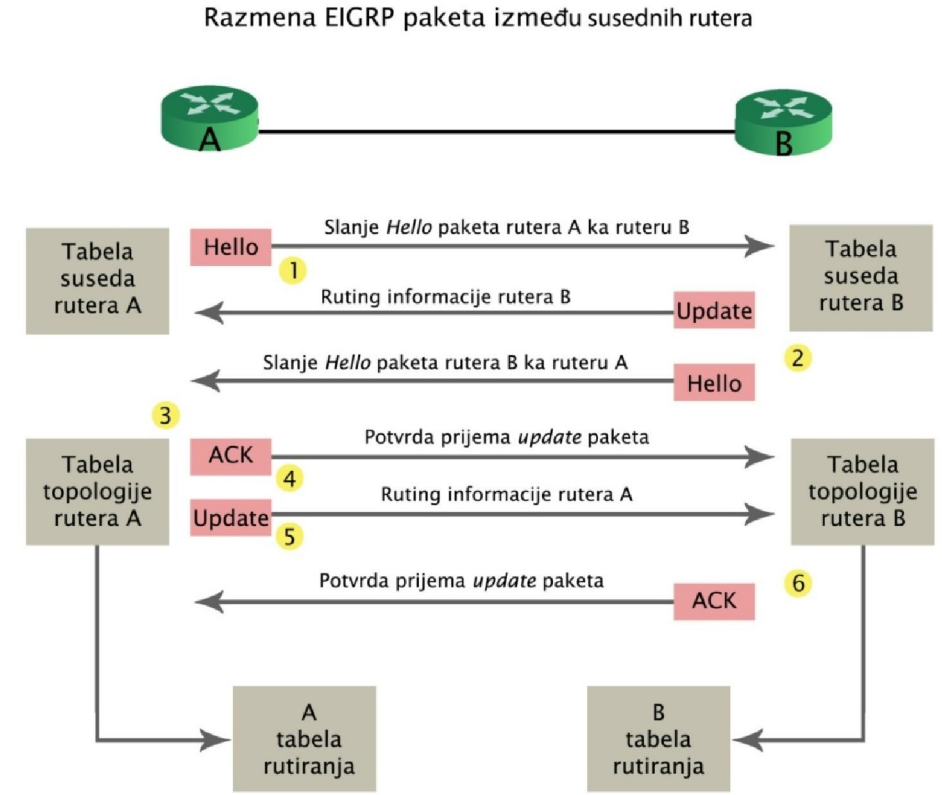
Pre nego što se postigne stanje konvergencije u okviru domena i ruteri nauče kako da dosegnu udaljene mreže, potrebno je najpre obaviti niz operacija u kojima se koriste gorenavedeni tipovi EIGRP paketa. "Podizanje" EIGRP protokola se obavlja u nekoliko faza:

1) Da bi ruteri mogli da razmenjuju informacije o rutama prvo moraju da uspostave odnos sa susednim ruterima. Ovo se ostvaruje slanjem *hello* paketa ka svim interfejsima na kojima je uključen EIGRP. Ipak, slanje, odnosno prijem *hello* paketa, nije dovoljan uslov da bi dva rutera postali susedi. Takođe, oni moraju da usaglase niz parametara. Na primer, oba rutera moraju da pripadaju istom autonomnom sistemu tj. da budu konfigurisani sa istim brojem autonomnog sistema i da koriste istu EIGRP metriku. Svaki ruter kreira tabelu suseda u kojoj sadrži listu svih suseda sa kojima je "uparen" i koja služi za praćenje statusa EIGRP suseda.
2) Kada ruter B na EIGRP interfejsu od rutera A primi *hello* paket, odgovara mu sa svojim *update* paketom, u kome se nalaze sve rute koje on u tom trenutku poseduje u svojoj tabeli rutiranja, osim onih koje je naučio preko tog interfejsa. Ipak, susedski odnosi nisu uspostavljeni sve dok ruter B ne pošalje svoj *hello* paket ka ruteru A. Nakon što oba

rutera prime *hello* pakete, smatra se da je uspostavljeno susedstvo (*adjacency*), a njihove tabele suseda su ažurirane.

3) Nakon što primi *update* paket od strane rutera B sa svim informacijama koje on oglašava, ruter A započinje ažuriranje svoje tabele topologije. Ruter A u svoju tabelu rutiranja upisuje sve rute koje je primio od rutera B zajedno sa "cenama" (metrikom) za svaku udaljenu mrežu.
4) Ruter A odgovara na *update* paket koji je primio od rutera B slanjem *acknowledgment* paketa kako bi potvrdio prijem informacija.
5) Nakon potvrde prijema, ruter A šalje *update* paket ka ruteru B sa svim informacijama iz svoje tabele topologije, osim onih koje je naučio od rutera B.
6) Ruter B takođe odgovara slanjem *acknowledgment* paketa, kako bi potvrdio prijem informacija koje je dobio od rutera A.
7) Nakon prijema *update* paketa od rutera B, ruter A ažurira svoju tabelu rutiranja na osnovu informacije iz tabele topologije. Upisi u tabeli rutiranja sadrže informacije o najboljoj putanji do svake mreže, uključujući metriku i sledeći ruter u putanji (*next-hop*) ruter.
8) Slično kao i ruter A, ruter B ažurira svoju tabelu rutiranja sa najboljim putanjama ka svakoj mreži.

Slika 5.3.1 ilustruje prethodno opisanu razmenu EIGRP paketa između rutera A i B.



Slika 5.3.1 Razmena EIGRP paketa

Nakon ovih koraka, može se smatrati da se oba rutera nalaze u stanju konvergencije, odnosno da je EIGRP protokol spreman za obavljanje svojih aktivnosti[4].

5.4. **Diffusing Update Algorithm (DUAL)**

EIGRP koristi *Diffusing Update Algorithm* (DUAL) za odabir i održavanje najbolje rute do svake udaljene mreže. Ovaj algoritam omogućava sledeće:

- Određivanje rezervne rute (pod uslovom da ona postoji)
- Garantuje nepostojanje zatvorenih petlji
- Podrška za *subnet mask-e* različitih dužina (VLSM)
- Oporavak dinamičkih ruta
- Slanje upita za alternativnu rutu, ako nijedna ruta ne može da se pronađe

DUAL omogućava EIGRP protokolu najbrže moguće vreme konvergencije rute među svim protokolima. Ključ za brzu konvergenciju kod EIGRP protokola je dvostruk [6]:

- EIGRP ruteri održavaju kopiju ruta svih svojih suseda, koju koriste za izračunavanje sopstvenih troškova do svake udaljene mreže. Ako najbolja putanja padne, potrebno je samo da se pogleda sadržaj tabele topologije i da se pronađe najbolja zamena.
- Ako u lokalnoj tabeli topologije ne postoji nijedna dobra alternativna ruta, EIGRP ruteri veoma brzo traže pomoć od svojih suseda za pronalaženje nove rute. Oslanjanje na druge rutere i korišćenje informacija koje oni pružaju je objašnjenje za difuzni karakter DUAL algoritma.

5.5. **EIGRP metrika**

Jedna od izuzetno bitnih karakteristika koja EIGRP čini veoma kvalitetnim protokolom rutiranja, jeste i mogućnost korišćenja više različitih faktora za odabir najbolje moguće putanje. Do metrike koja se koristi u okviru EIGRP protokola dolazi se kombinacijom 4 faktora:

- Propusni opseg (b*andwith*) - Predstavlja "najuži" propusni opseg na putanji od izvora do konačnog odredišta
- Kašnjenje (*delay*) - Kumulativno kašnjenje na svim interfejsima duž putanje
- Opterećenje (*Load*) - Predstavlja najveće opterećenje na linku od izvora do odredišta. Računa se na osnovu brzine prenosa paketa i propusnog opsega interfejsa
- Pouzdanost (*Reliability*) - Predstavlja najgoru pouzdanost na celoj dužini linka od izvora do odredišta

Postoji i peti element, a to je veličina jedinice maksimalnog prenosa (MTU). Ovaj parametar se nikad ne koristi za izračunavanje metrike, ali je obavezan parametar u nekim EIGRP

komandama, posebno u onim koje uključuju redistribuciju. MTU predstavlja najveću jedinicu prenosa (najveću dužinu okvira) duž putanje do odredišne mreže.

Takođe, preporuka je da se za izračunavanje metrike koriste samo prva dva parametra (propusni opseg i kašnjenje), jer se preostala dva često menjaju zbog promena topologije mreže [4] [6].

5.6. Reliable Transport Protocol (RTP)

Reliable Transport Protocol (RTP) jeste protokol koji je razvijen od strane kompanije Cisco, kako bi se omogućilo upravljanje komunikacionim porukama (EIGRP paketa) između rutera koji koriste EIGRP protokol. Već iz samog naziva zaključujemo da je najveća briga ovog protokola pouzdanost. Pouzdan prenos podrazumeva da će paketi garantovano stići na odredište i to u zahtevanom redosledu. Garantovana dostava se postiže korišćenjem algoritma koji se naziva *reliable multicast.* U okviru ovog procesa, koristi se adresa klase D 224.0.0.10. Svaki susedni ruter prima *reliable multicast* paket i odgovara slanjem *unicast acknowledgment*-a. Ruter koji je poslao *reliable multicast* paket zna ko su njegovi susedi i za svaki poslati paket održava listu suseda koji su odgovorili. Ukoliko ruter ne dobije potvrdu od suseda, prelazi se na slanje *unicast* paketa. Ukoliko ni posle 16 *unicast* paketa susedni ruter ne pošalje potvrdu, on se proglašava "mrtvim".

Praćenje poslatih informacija ostvaruje se tako što ruteri svakom poslatom paketu dodeljuju dva sekvencijalna broja. Prvi broj predstavlja redni broj poslatog paketa i on se svakim slanjem inkrementira za jedan. Drugi broj predstavlja redni broj poslednjeg paketa koji je izvorišni ruter primio od odredišnog rutera. Korišćenjem tehnike sekvencijalnih brojeva, moguća je detekcija starih, redudantnih ili informacija van redosleda.

U okviru *neighbor discovery* procesa, tj. za slanje *hello* i *ack paketa,* može se koristiti "*unreliable delivery*", ali je za slanje *update* paketa neophodno koristiti "*reliable delivery*" zbog principa funkcionisanja EIGRP protokola, odnosno zbog činjenice da se *update* paketi ne šalju periodično, već samo u trenucima kad dođe do izmene u topologiji mreže. Upravo zbog ove činjenice, neophodno je da prenos *update* paketa bude pouzdan, jer u slučaju gubitka ili nepravilnog redosleda izvršenja paketa može doći do oštećenja baze podataka rutiranja [7].

5.7. Nedostaci EIGRP protokola

Pored brojnih korisnih osobina i unapređenja koje je uneo u proces rutiranja, EIGRP ima i nekoliko loših osobina. One ne umanjuju značaj EIGRP protokola, ali mogu pomoći pri izboru odgovarajućeg protokola rutiranja za potrebe konretne mreže:

- Kod EIGRP protokola ne postoji koncept regija (*areas*) tako da se ne može implementirati hijerarhijski princip rutiranja kao kod OSPF protokola. Postoji varijanta da se delovi mreže podele u više različitih autonomnih sistema, a zatim se importuju tabele rutiranja. Ovaj princip ipak nije preporučljiv i na ovakav način funkcioniše mali broj mreža.

- Drugi nedostatak je i taj što ovaj protokol spada u takozvane "*property*" protokole tj. vlasništvo je kompanije Cisco i može se koristiti jedino na uređajima proizvedenim u okviru ove kompanije.

6. OSPF

6.1. Ideja i razvoj OSPF protokola

Open Shortest Path First (OSPF) je protokol rutiranja sa otvorenim standardima. Ovo zapravo podrazumeva da se za razliku od EIGRP-a može implementirati na mrežnim uređajima velikog broja proizvođača mrežnih komponenti, a ne samo na onim koji su proizvedeni u okviru Cisco kompanije. OSPF je *link state* protokol rutiranja, koji je razvijen kao zamena za *distance vector* protokol RIP. U početku samog razvoja Interneta, RIP je bio prihvatljiv kao protokol rutiranja i uspevao je da odgovori na tehničke zahteve. Međutim, kako se Internet razvijao, a mreže postajale sve veće, način koji je RIP koristio za određivanje najboljih ruta kojim će paketi biti prosleđivani postajao je sve neefikasniji. Naime, RIP je za određivanje najbolje rute koristio jedino metriku broja skokova (*houp count*), odnosno, izračunavao je broj rutera kroz koje paket treba da prođe od izvora ka odredištu i na taj način predlagao najbolju putanju. U mrežama koje imaju veći broj različitih putanja, a koje pritom imaju različite brzine, ovaj metod se očekivano pokazao veoma neefikasnim. Imajući ovo u vidu, OSPF je ponudio mnogo bolja rešenja na polju skalabilnosti i brzine konvergencije [6].

Sami počeci razvoja OSPF protokola rutiranja vraćaju nas u 1987. godinu, kada je Internet još uvek bio samo još jedan od projekata finansiran od strane američke vlade, a IETF (*Internet Engineering Task Force*) oformio radnu grupu za razvoj OSPF-a. Ubrzo, 1989. godine, u okviru dokumenta RFC 1131, publikovana je prva specifikacija za OSPFv1, koja je sadržala dve implementacije. Prva implementacija bila je namenjena za korišćenje na ruterima, dok je druga korišćena na UNIX radnim stanicama. OSPFv2 objavljena je 1991. godine u okviru dokumenta RFC 1247. U odnosu na prethodnu verziju, novija verzija je sadržala značajna tehnička unapređenja, od kojih su najznačajnija ona vezana za VLSM i CIDR. Verzija OSPFv3 koja je namenjena za IPv6 publikovana je 1999. godine, u okviru RFC 2740 dokumenta. Pored specifikacija vezanih za IPv6, u okviru RFC 2740 dokumenta, nalaze se i unapređenja o samom protokolu. 2008. godine, OSPFv3 je u okviru RFC 5340 deklarisan kao protokol namenjen IPv6 [1].

6.2. Glavne karakteristike i prednosti OSPF protokola

Glavne odlike OSPF protokola su:

- Skalabilnost - OSPF se pokazao vrlo efikasnim kako u malim, tako i u velikim mrežama. Zamišljen je tako da se dizajnira na hijerarhijski način, tj. da se veliko mrežno okruženje razdvoji na manje mreže, tzv. regione (*area*).
- Besklasnost - OSPF je besklasni protokol koji podržava VLSM i CIDR.

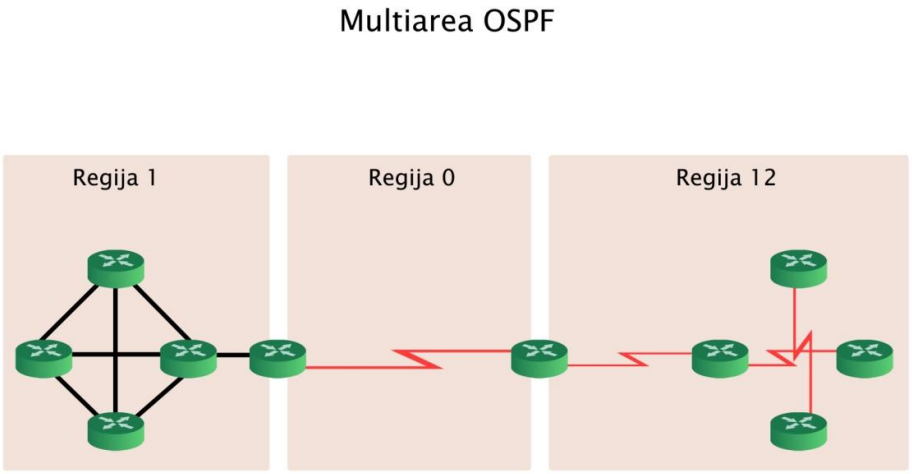
- Brza konvergencija - Sve promene na mreži, odnosno ažuriranja, se brzo propagiraju ka svim OSPF ruterima.
- Sigurnost - Podržava MD5 (*Message Digest 5*) autentifikaciju, što izuzetno podiže nivo sigurnosti. Kada je ova opcija omogućena, OSPF ruteri prihvataju samo ona enkriptovana ažuriranja koja potiču od rutera, sa ranije definisanom šifrom.
- Efikasnost - Efikasnost protokola se postiže slanjem ažuriranja, jedino u trenucima kada se dogode promene na mreži, a ne periodičnim ažuriranjem. Korisiti se SPF algoritam za odabir najbolje rute.

Samo ime *Open Shortest Path First* protokola (najpre otvoriti najkraću putanju) podrazumeva da ruteri moraju poznavati kompletnu topologiju mreže, jer to je jedini način da odrede koja je to putanja "najkraća" do željenog odredišta. Do ovih saznanja dolazi se razmenom IP informacija rutiranja u okviru jednog autonomnog sistema (*Autonomous System*). OSPF je *link-state* protokol, što znači da ruteri razmenjuju informacije o topologiji sa njihovim najbližim susedima. Te informacije se šire dalje kroz mrežu, sve do trenutka kada svaki ruter u okviru autonomnog sistema ima kompletnu sliku o topologiji tog autonomnog sistema. Samo prikupljanje informacija o topologiji nije dovoljno, potrebno je te informacije na neki način obraditi i tako odrediti koja putanja je najbolja za prenos korisničkih paketa. Za ovaj proces se koriste različite verzije Dijkstra algoritma.

Glavna prednost *link-state* protokola, a samim tim i OSPF-a, je ta što znanje o kompletnoj mrežnoj topologiji daje mogućnost ruterima da najbolje rute proračunavaju na osnovu različitih kriterijuma. To može biti izuzetno korisno prilikom projektovanja mrežnog saobraćaja, odnosno u situacijama kada je potrebno da pojedine rute ispune određene zahteve u pogledu kvaliteta servisa. Sa druge strane, glavna mana *link-state* protokola je što se u slučaju povećanja broja rutera u okviru jednog domena povećava veličina i učestalost ažuriranja, a takođe se povećava vreme koje je potrebno za izračunavanje najoptimalnije *end-to-end* putanje. Ovaj nedostatak pokazuje zašto se *link-state* protokoli ograničavaju na rutiranje saobraćaja u okviru jednog administrativnog domena [4].

Jedna od glavnih odlika koja OSPF čini skalabilnijim i mnogo efikasnijim protokolom jeste podrška hijerarijskom rutiranju korišćenjem OSPF regija (*OSPF* A*reas*). Jednu regiju čini grupa rutera koji razmenjuju LSA pakete i imaju zajednički ID regije (*Area ID*). OSPF može biti implementiran na dva načina:

1) *Single-Area OSPF* - Svi ruteri se nalaze u jednoj regiji koja predstavlja okosnicu mreže (*Backbone area*) i naziva se nultom regijom.
2) *Multiarea OSPF* - OSPF je implementiran tako da se sastoji od više regija koje su povezane sa Regijom 0. Ruteri koji povezuju dve regije nazivaju se granični ruteri (*Area Border Routers*).



Slika 6.2.1 Multiarea OSPF

Osnovna ideja korišćenja *Multiarea OSPF*-a jeste mogućnost da se jedan veliki autonomni sistem podeli na više manjih regija (poput primera sa slike 6.2.1), kako bi se podržalo hijerarhijsko rutiranje. Na ovaj način se podaci i dalje rutiraju između regija (*interarea routing*), dok se svi procesi koji opterećuju mrežu ostaju na nivou regije. Na primer, svaki put kada ruter primi informaciju o promeni topologije mreže u jednoj regiji (dodavanje, brisanje ili modifikacija linka), mora nakon toga ponovo da pokrene SPF algoritam, kreira novo SPF stablo i ažurira tabelu rutiranja. Ovaj proces može biti jako zahtevan, posebno u slučaju velikih regija sa mnogo rutera. Informacije o promeni topologije se prosleđuju ruterima u drugim regijama, ali oni ne pokreću SPF algoritam, već samo ažuriraju svoje tabele rutiranja.

Kao što je već napomenuto, veliki broj rutera u okviru jedne regije prouzrokuje stvaranje velike LSDB, što izaziva veliku opterećenost CPU-a. Imajući to u vidu, jasno je da grupisanje rutera u manje celine dovodi do "razbijanja" potencijalno velikih baza podataka u nekoliko manjih, lakše upravljivih baza podataka.

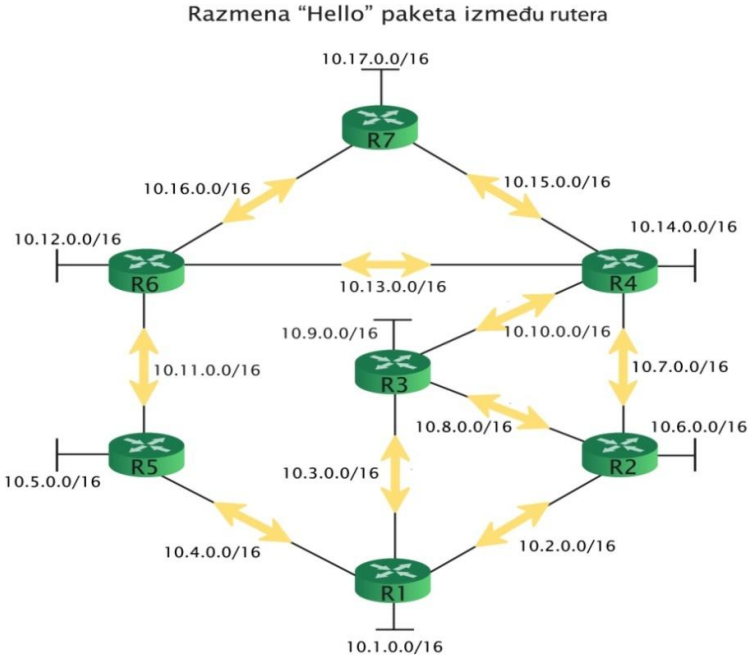
Hijerarhijska topologija u okviru *Multiarea* OSPF pruža i sledeće prednosti:

- Manje tabele rutiranja - U tabelama rutiranja nalazi se manji broj upisa pošto postoji mogućnost da se izvrši sumarizacija određenih mrežnih adresa između regija.
- Minimiziranje procesorskih i memorijskih zahteva
- Smanjenja broja SPF proračuna - Broj LSA paketa koji se obrađuju je smanjen, jer se njihovo prostiranje (rasejavanje) zaustavlja na granicama regije.

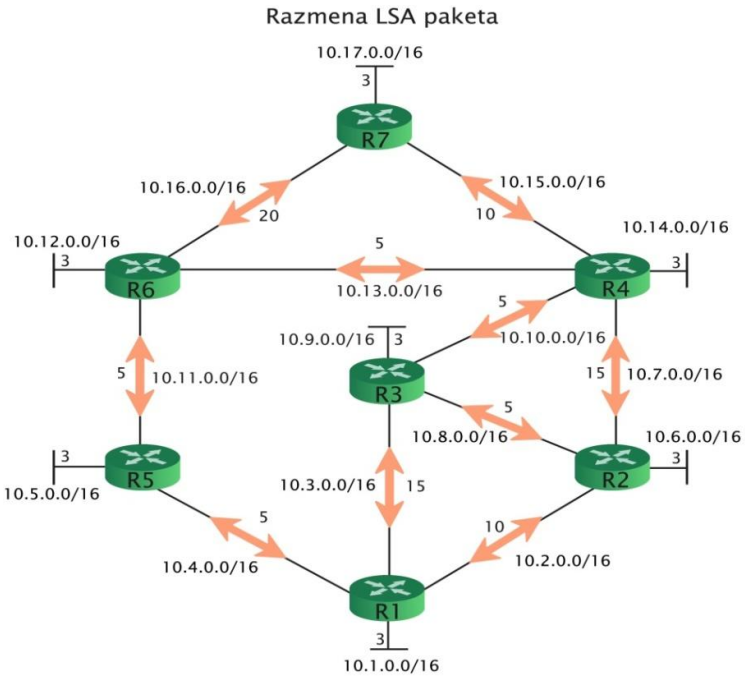
6.3. **Princip funkcionisanja**

Pre nego što postignu operativno stanje, OSPF ruteri najpre moraju da obave *link-state* ruting proces kako bi postigli stanje konvergencije. Ovaj proces se odvija u nekoliko koraka, odnosno, faza:

1. Prvi korak jeste takozvano "upoznavanje sa susedima" (*Neighbor Adjacencies).* Rutere smatramo susedima ukoliko imaju interfejse na zajedničkoj mreži (primer: serijska veza tačka-tačka između dva rutera). Da bi ruteri mogli da komuniciraju međusobno, odnosno da razmenjuju informacije o rutiranju, nije dovoljno da dva rutera budu susedi (*Neighbors),*već je potrebno da između njih postoji i takozvana "bliskost" (*Adjacency*). Ovo zapravo znači da za razliku od EIGRP, koji direktno deli rute sa svim svojim susedima, OSPF bira sa kojim ruterima će postati blizak i samo sa njima će deliti rute. Sa kojim ruterima će postati blizak zavisi od vrste mreže i konfiguracije rutera. Proces uspostavljanja *Neighbor Adjacencies-a* započinje se slanjem *Hello* paketa na svim interfejsima koji pripadaju OSPF-u, a pritom je na drugom kraju linka sused koji takođe koristi OSPF. Faza 1 je ilustrovana na slici 6.3.1.

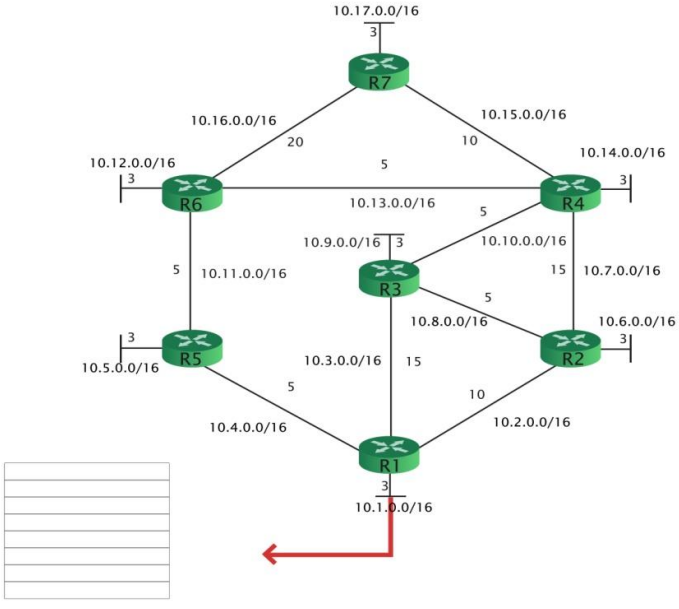


Slika 6.3.1 Razmena Hello paketa između rutera



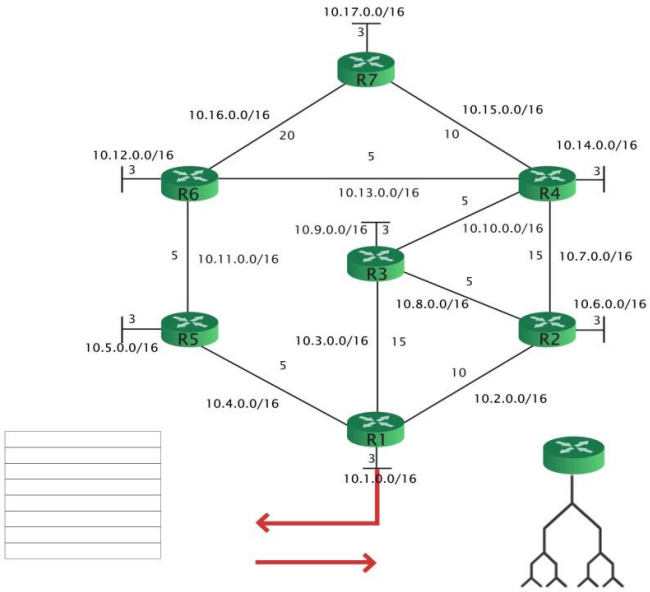
Slika 6.3.2 Razmena LSA paketa

2. Nakon razmene *Hello* paketa i uspostavljanja *Neighbor Adjacencies-a,* ruteri započinju sa razmenom paketa o stanju linka (*Link State Advertisement - LSA).* LSA paketi sadrže informacije o stanju i ceni svakog direktnog linka. Ruter "rasipa" svoje LSA ka svim susedima. Susedi primaju te LSA pakete i odmah ih dalje "rasipaju" ka ostalim direktnim susedima. Ovaj proces se nastavlja sve do trenutka dok svi ruteri u jednom OSPF regionu nemaju sve LSA pakete. Faza 2 je ilustrovana na slici 6.3.2.



Slika 6.3.3 Formiranje tabele topologije

3. Treći korak jeste formiranje tabele topologije (*Topology Table).* Nakon prijema LSA paketa, OSPF ruteri započinju kreiranje tabele topologije, odnosno bazu podataka topologije (*Link-State Database-LSDB)*. Ova baza podataka na kraju sadrži sve informacije o topologiji mreže. Faza 3 je ilustrovana na slici 6.3.3.



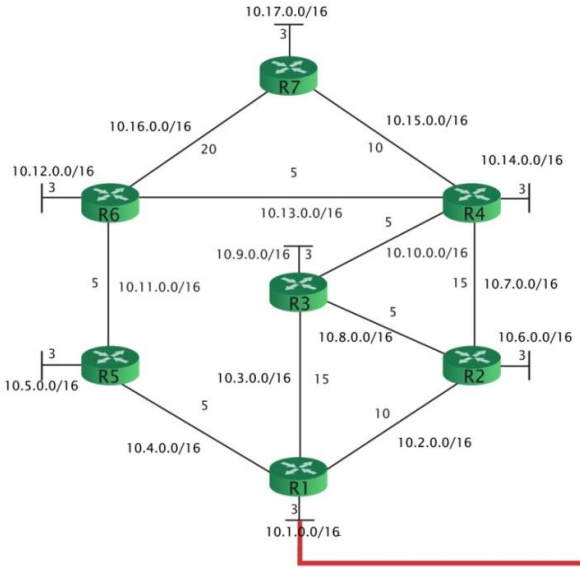
Slika 6.3.4 Formiranje SPF stabla

4. Nakon prikupljanja potrebnih informacija, ruteri započinju izvršavanje SPF algoritma. Rezultat izvršavanja SPF algoritma je formiranje SPF stabla sa koga se najbolje putanje prosleđuju u tabele rutiranja. Na osnovu unosa koji se nalaze u tabeli rutiranja, donose se odluke o putanjama rutiranja saobraćaja. Faza 4 je ilustrovana na slici 6.3.4.

Nakon završetka SPF algoritma, ruter u svojoj bazi podataka poseduje SPF stablo, na osnovu kog može odabrati putanju do željene destinacije. Najbolje putanje se zatim upisuju u tabelu rutiranja i koriste se za buduće rutiranje saobraćaja [4]. Izgled jednog SPF stabla prikazan je na slici 6.3.5.

Većina protokola rutiranja, pa tako i OSPF, svoj rad bazira na razmeni informacija između rutera, slanjem odgovarajućih poruka. Ove poruke se koriste za razmenu informacija o rutama i za formiranje određenih struktura podataka, koje se kasnije koriste u samom algoritmu rutiranja. Kod OSPF protokola to su takozvani paketi o stanju linka (*Link-state packets - LSP)* među kojima po svojoj funkcionalnosti razlikujemo sledeće:

- *Hello packets* - Otkrivanje suseda i uspostavljanje "međususedskih" odnosa
- *Database Description (DBD)* - Provera usaglašenosti baza podataka između rutera
- *Link-State Request (LSR)* - Zahtev za isporuku određenog *link-state* zapisa između rutera
- *Link-State Update (LSU)* - Slanje zahtevanog određenog *link-state* zapisa
- *Link-State Acknowledgement (LSAck)* - Potvrda prijema paketa



DESTINACIJA	NAJKRAĆI PUT	CENA
10.5.0.0	R1→R5	8
10.6.0.0	R1→R2	13
10.7.0.0	R1→R2	25
10.8.0.0	R1→R2	15
10.9.0.0	R1→R3	18
10.10.0.0	R1→R3	20
10.11.0.0	R1→R5	10
10.12.0.0	R1→R5→R6	13
10.13.0.0	R1→R5→R6	15
10.14.0.0	R1→R5→R6→R4	18
10.15.0.0	R1→R5→R6→R4	28
10.16.0.0	R1→R5→R6	30
10.17.0.0	R1→R5→R6→R7	33

Slika 6.3.5 SPF stablo

Pre nego što postigne stanje potpune konvergencije, OSPF ruter prolazi kroz određenja stanja u okviru kojih se vrši razmena potrebnih informacija i u kojima se izvršavaju neophodne operacije:

- *Down state* - Stanje u kom ruteri još uvek nisu primili *Hello* pakete. Započinje se njihovo slanje i prelazak u naredno stanje.
- *Init state* - Stanje u kom su ruteri od svojih suseda primili *Hello* pakete, koji sadrže identifikacioni broj rutera (*Router ID).*
- *Two-Way State* - U slučaju eternet linka između rutera, vrši se izbor DR i BDR.
- *ExStart State* - Određivanje *master* i *slave* rutera. *Master* ruter inicira utvrđivanje sekvencijalnog broja DBD paketa.
- *Exchange State* - Ruteri razmenjuju DBD pakete. Ukoliko su nekom od rutera potrebne dodatne informacije prelazi se u *Loading state,* u suprotnom prelazi se u *Full state.*
- *Loading State* - Dodatni podaci se razmenjuju korišćenjem LSR i LSU paketa, koji se procesiraju korišćenjem SPF algoritma. Nakon toga, prelazi se u sledeće stanje.
- *Full state* - Ruteri se sada nalaze u stanju potpune konvergencije.

Akcija koja će se odvijati u *Two-Way* stanju zavisi od tipa konekcije između rutera. Ukoliko je veza tipa tačka-tačka, automatski će se nastaviti sa tranzicijom u sledeće stanje. Ako je konekcija između rutera izvedena pomoću eternet kabla, potrebno je izvršiti izbor *designated router*-a (DR) i *backup designated router*-a (BDR). Izbor DR-a i BDR-a neophodan je iz dva razloga. Prvi razlog je taj, što u slučaju eternet mreže, mnogo OSPF rutera može koristiti zajednički link. Posledica toga jeste, što se u tom slučaju može ostvariti nepotrebno veliki broj susedskih odnosa, što opterećuje

mrežu. Drugi razlog je taj, što se slanje LSA paketa izvršava pri svakoj inicijalizaciji OSPF ili pri bilo kojoj promeni u topologiji mreže. Navedeni problemi možda ne deluju previše značajno u slučaju malog broja rutera, ali zato sa porastom njihovog broja ovaj problem postaje jako ozbiljan. Rešenje jeste upravo u odabiru *designated router*-a (DR). OSPF vrši proglašava određeni ruter *designated router*-om i predaje mu zaduženja za prikupljanje i distribuciju LSA paketa. Ovo zapravo, znači da je dovoljno da svi ruteri u mreži pošalju svoj LSA jedino ka DR-u i da budu sigurni da će svi ruteri u mreži ažurirati baze podataka sa poslatim informacijama. Kako bi se obezbedilo da mreža neometano radi, čak i u situaciji kada DR nije u operativnom stanju, proglašava se *backup designated router*-a (BDR). BDR se aktivira u slučaju kada DR zakaže i tom prilikom preuzima sva njegova zaduženja. Svi ostali ruteri se proglašavaju *drother*-ima [5].

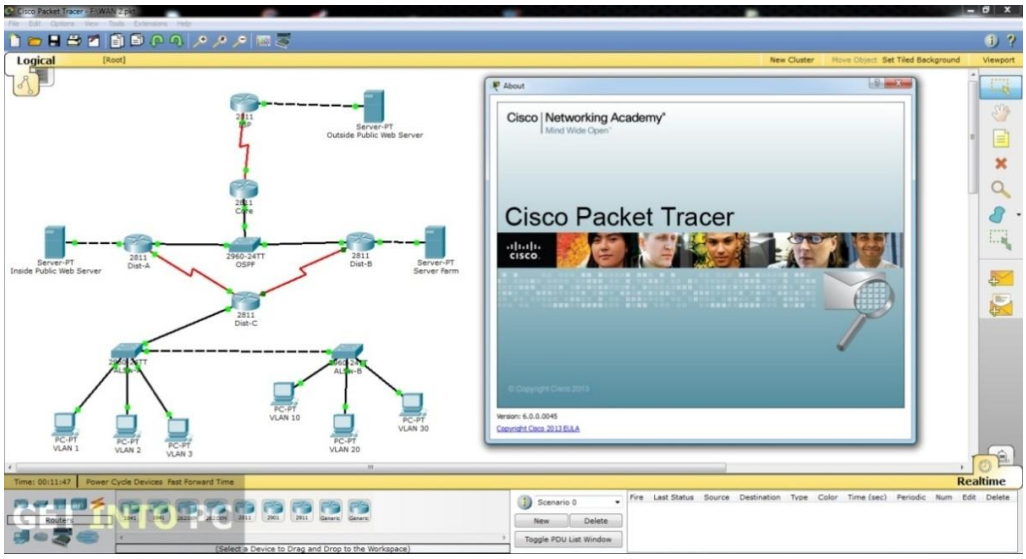
6.4. **Nedostaci OSPF protokola**

Pored brojnih dobrih osobina i poboljšanja koje je OSPF protokol uneo u svet rutiranja, postoje određeni nedostaci koji u velikoj meri ne umanjuju značaj OSPF protokola, ali je ipak korisno spomenuti ih.

- OSPF protokol je prilično procesorski zahtevan
- U slučaju dodatka novih rutera u mrežu, povećava se vreme potrebno za postizanje konvergentnosti mreže, a povećavaju se potrebe za memorijom zbog sve veće OSPF baze podataka
- OSPF protokol nije lak za učenje i razumevanje poput nekih drugih protokola
- U slučaju da je neki od linkova ili rutera nestabilan, odnosno da menja svoje "prisustvo" na mreži na svakih nekoliko sekundi, OSPF može napraviti veliki problem čestim oglašavanjem promena na mreži (slanjem *hello* paketa i LSA). Slanje ovih paketa u jednom trenutku može dominirati mrežom i na taj način onemogućiti slanje korisničkog saobraćaja [7].

7. CISCO PACKET TRACER

Imajući u vidu da se mrežni sistemi sve više razvijaju i sve su kompleksniji, potrebni su programi i obrazovni sistemi koji bi olakšavali učenje o mrežnoj tehnologiji. *Cisco Networking Academy* obrazovni sistem je osmišljen tako da održi korak sa razvijanjem mrežnih sistema time što će pružiti inovativne programe i obrazovne alatke, koje pomažu studentima da razumeju složenost informacionih i komunikacionih tehnologija. U sklopu ovog programa, napravljen je *Cisco Packet Tracer* softver za elektronsko učenje, osmišljen da pomogne studentima kako bi stekli praktična znanja o mrežnim tehnologijama. Studenti mogu da koriste prednosti kao što su dostupnost programa na mreži, mogućnosti za zajedničko učenje, saradnju, kreativno i kritičko mišljenje, rešavanje problema i takmičenja.



Slika 7.1 Cisco Packet Tracer

Ovaj softver pruža mogućnosti korisniku da ekesperimentiše i postavlja „šta ako“ pitanja. On obezbeđuje još i stimulaciju, vizuelizaciju, svojstvenost, procenu i mogućnosti za saradnju kako bi se olakšalo učenje. Dopunjuje fizičku opremu u učionicama i dozvoljava studentima da kreiraju mrežu sa skoro neograničenim brojem uređaja, omogućava predavačima laku demonstraciju o kompleksnosti i dizajnu mrežnih sistema. Predavači mogu lako da organizuju individualna ili grupna predavanja i aktivnosti, pa tako i studenti grade, konfigurišu i rešavaju problem mreže koristeći virtuelnu opremu i simulirane veze, samostalno ili u saradnji sa drugim studentima. *Packet Tracer* nudi efikasno, interaktivno okruženje za učenje koncepta mreže i protokola [8].

Packet Tracer nije zamena za pravu opremu, ali omogućava studentima da vežbaju koristeći komandne linije interfejsa. Ova sposobnost je osnovna komponenta učenja o podešavanjima rutera i svičeva. Program ima simulacioni režim rada, gde predavač može da demonstrira procese koji su

prethodno skriveni i to uz pomoć tabela, dijagrama i drugih vizuelnih prezentacija. Time može da pojednostavi proces učenja nekih unutrašnjih funkcija, kao što je npr. dinamički prenos podataka. *Packet Tracer* pomaže u učenju kompleksnih mreža na sledeći način:

- Pruža vizuelnu demonstraciju složenih tehnologija i konfiguracija
- Dozvoljava prilagođene, vođene aktivnosti, koje pružaju neposrednu povratnu informaciju koristeći *Activity Wizard*.
- Olakšava brojne aktivnosti učenja kao što su predavanja, laboratorijske vežbe, domaći zadaci, procene, igre, dizajn mreže, rešavanje problema, studije slučaja i takmičenja
- Omogućava vizuelizaciju, animaciju i detaljno modeliranje za istraživanje, eksperimentisanje i objašnjenje
- Podržava učenje u bilo kom vremenu, sa sopstvenim tempom i van učionice
- Podržava proces učenja u grupama time što omogućava saradnju i konkurenciju

Studenti koji provedu više vremena u praktičnom načinu učenja koristeći simulacione i interaktivne mogućnosti, bolje su pripremljeni za primenu u realnom okruženju. U toku učenja se stiču praktična iskustva sa zadacima kao što su konfiguracije i rešavanje problema, pa se tako kroz saradnju studenata i kroz međusobno takmičenje kroz igre student dodatno informiše i uči za primenu teorijskog znanja u stvarnosti.

Packet Tracer ima dva radna prostora: logički i fizički. Logički radni prostor dozvoljava korisniku da gradi mrežnu tipologiju postavljanjem, povezivanjem i grupisanjem virtuelnih mrežnih uređaja. Fizički radni prostor daje grafički prikaz logičke mreže, pružajući osećaj skalabilnosti i postavljanja mreže u kojoj bi uređaji kao što su ruteri, svičevi i hostovi izgledali kao da su u realnom okruženju. Omogućava da sagledamo geografski prikaz mreže na nivou zemalja, gradova pa sve do zgrada i električnih ormara.

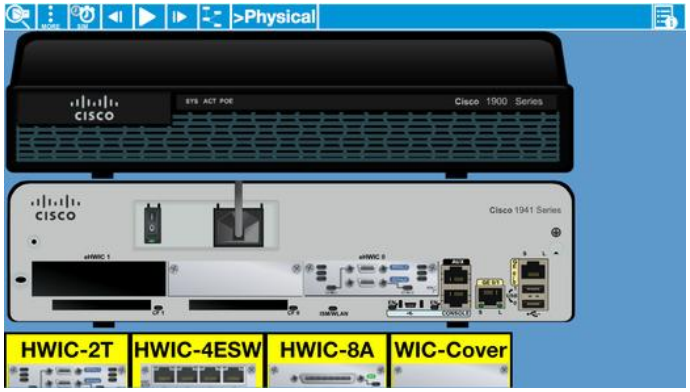
Packet Tracer omogućava dva operativna režima za vizuelizaciju ponašanja mreže: režim u realnom vremenu (*Real Time*) i simulacioni (*Simulation*) režim. U režimu u realnom vremenu, mreža se ponaša kao pravi uređaj, sa trenutnim odgovorom za sve mrežne aktivnosti. Režim realnog vremena daje održivu alternativu stvarne opreme i omogućava sticanje prakse za konfiguraciju pre rada sa pravom opremom. U simulaciji korisnik može da vidi i kontroliše vremenske intervale u unutrašnjim poslovima prenosa podataka, kao i propagiranje podataka preko mreža.

Packet Tracer podržava sledeće protokole prikazane na slici 7.2.

Slojevi	Podržani protokoli
Aplikacioni	• FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transportni	• TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Mrežni	• BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/ v2/ng, Multi-Area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL , Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Sloj veze	• Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP

Slika 7.2 Podržani protokoli u CPT-u

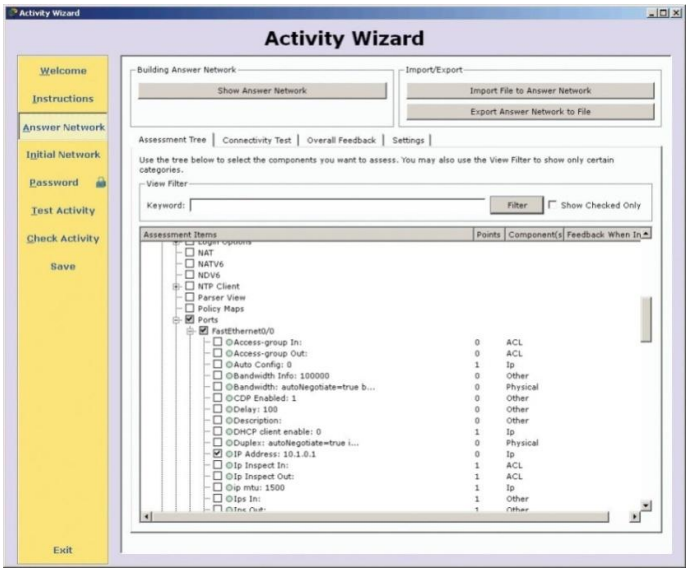
Grafičke prezentacije vizuelno simuliraju hardver i nude mogućnost ubacivanja interfejs kartice u ruter i svič, koji zatim postaju deo te simulacije.



Slika 7.3 Prikaz rutera u CPT-u

Packet Tracer je mrežno sposobna aplikacija, sa mogućnošću kreiranja konekcije između korisnika i kreiranja virtuelne mreže korišćenjem resursa stvarne mreže. Višekorisnička funkcija omogućava uzbudljivu saradnju, interaktivno učenje, pružajući mogućnost napredovanja od pojedinca do grupnog učenja, pruža mogućnosti za saradnju, konkurenciju, udaljenu interakciju, društveno umrežavanje i igranje.

Activity Wizard dozvoljava korisniku da autorizuje sopstvene aktivnosti učenja, tako što postavlja scenarije koristeći tekst sa instrukcijama i kreiranje početne i završne topologije mreže i unapred definisanog paketa. On takođe i uključuje ocenjivanje i mogućnosti povratne informacije [8].



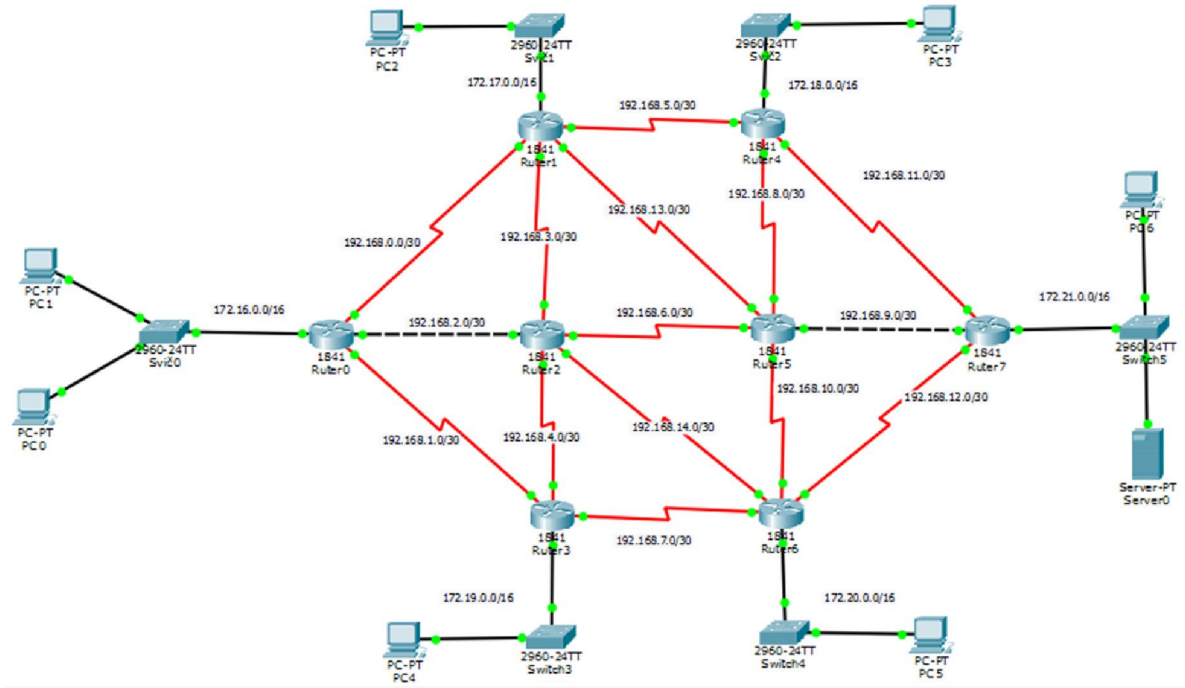
Slika 7.4 Activity Wizard u CPT-u

8. KOMPARATIVNA ANALIZA

8.1. Konfigurisanje mreže

U okviru praktičnog dela teze, na primeru jedne konkretne računarske mreže, komparativnom analizom sagledane su karakteristike OSPF i EIGRP protokola. Za potrebe naše simulacije u laboratorijskom okruženju, korišćen je *Cisco Packet Tracer* (CPT), softverski alat kompanije Cisco.

Praćenje i analiza performansi protokola izvršeni su na primeru srednje kompleksne računarske mreže u okviru koje su implementirane komponente koje srećemo u realnom okruženju (ruteri, svičevi, računari, serveri...). Korišćeni su Cisco 1841 ruteri i Cisco 2960 svičevi. Izgled kompletne topologije kreirane u okviru CPT prikazan je na slici 8.1.1.



Slika 8.1.1 Topologija mreže u laboratorijskom okruženju

Na ruterima i svičevima izvršena su osnovna konfigurisanja koja se odnose na ime uređaja, adresiranje i karakteristike interfejsa i protokole rutiranja. Na slici 8.1.2 dat je tabelarni prikaz IP adresa interfejsa svih uređaja koji su implementirani u okviru mreže. Takođe, u tabeli se nalaze informacije o konekciji između uređaja tj. koji interfejsi su upotrebljeni za povezivanje. Konekcija između rutera izvedena je korišćenjem serijskih i FastEthernet interfejsa, dok su za povezivanje svičeva i ostalih komponetni korišćeni isključivo FastEthernet interfejsi.

Uređaj	Interfejs	IP konfiguracija	Konekcija
Ruter0	Fa 0/0	172.16.0.1/16	Svič1; Fa 0/3
Ruter0	Fa 0/1	192.168.2.1/30	Ruter2; Fa 0/0
Ruter0	S 0/0/0	192.168.0.1/30	Ruter1; S 0/0/0
Ruter0	S 0/0/1	192.168.1.1/30	Ruter3; S 0/0/0
Ruter1	Fa 0/0	172.17.0.1/16	Svič1; Fa 0/1
Ruter1	S 0/0/0	192.168.0.2/30	Ruter0; S 0/0/0
Ruter1	S 0/0/1	192.168.3.1/30	Ruter2; S 0/0/0
Ruter1	S 0/1/0	192.168.5.1/30	Ruter4; S 0/0/0
Ruter1	S 0/1/1	192.168.13.1/30	Ruter5; S0/1/1
Ruter2	Fa 0/0	192.168.2.2/30	Ruter0; Fa 0/1
Ruter2	S 0/0/0	192.168.3.2/30	Ruter1; s 0/0/1
Ruter2	S 0/0/1	192.168.4.1/30	Ruter3; S 0/0/1
Ruter2	S 0/1/0	192.168.6.1/30	Ruter5; s 0/1/0
Ruter2	S 0/1/1	192.168.14.1/30	Ruter6; s 0/1/1
Ruter3	Fa 0/0	172.19.0.1/16	Svič3; Fa 0/1
Ruter3	S 0/0/0	192.168.1.2/30	Ruter0; S 0/0/1
Ruter3	S 0/0/1	192.168.4.2/30	Ruter2; S 0/0/1
Ruter3	S 0/1/0	192.168.7.1/30	Ruter6; S 0/0/0
Ruter4	Fa 0/0	172.18.0.1/16	Svič2; Fa 0/1
Ruter4	S 0/0/0	192.168.5.1/30	Ruter1; S 0/1/0
Ruter4	S 0/0/1	192.168.8.1/30	Ruter5; S 0/0/0
Ruter4	S 0/1/0	192.168.11.1/30	Ruter7; S 0/0/0
Ruter5	Fa 0/0	192.168.9.1/30	Ruter7; Fa 0/0
Ruter5	S 0/0/0	192.168.8.2/30	Ruter4; S 0/0/1
Ruter5	S 0/0/1	192.168.10.2/30	Ruter6; S 0/0/1
Ruter5	S 0/1/0	192.168.6.2/30	Ruter2; S 0/1/0
Ruter5	S 0/1/1	192.168.13.2/30	Ruter1; s 0/1/1
Ruter6	Fa 0/0	172.20.0.1/16	Svič4; Fa 0/1
Ruter6	S 0/0/0	192.168.7.2/30	Ruter3; S 0/1/0
Ruter6	S 0/0/1	192.168.10.1/30	Ruter5; S 0/0/1
Ruter6	S 0/1/0	192.168.12.1/30	Ruter7; S 0/0/1
Ruter6	S 0/1/1	192.168.14.2/30	Ruter2; S 0/1/1
Ruter7	Fa 0/0	172.21.0.1/16	Svič5; Fa 0/1
Ruter7	Fa 0/0	192.168.9.2/30	Ruter5; Fa 0/0
Ruter7	S 0/0/0	192.168.11.2/30	Ruter4; S 0/1/0
Ruter7	S 0/0/1	192.168.12.2/30	Ruter6; S 0/1/0
PC0	Fa 0/0	172.16.0.3/16	Svič0; Fa 0/1
PC1	Fa 0/1	172.16.0.4/16	Svič0; Fa 0/2
PC2	Fa 0/0	172.17.0.3/16	Svič1; Fa 0/2
PC3	Fa 0/0	172.18.0.3/16	Svič2; Fa 0/2
PC4	Fa 0/0	172.19.0.3/16	Svič3; Fa 0/2
PC5	Fa 0/0	172.20.0.3/16	Svič4; Fa 0/2
PC6	Fa 0/0	172.21.0.4/16	Svič5; Fa 0/3
Server PT	Fa 0/0	172.21.0.3/16	Svič5; Fa 0/2
Svič0	vlan 1	172.16.0.2/16	
Svič1	vlan 1	172.17.0.2/16	
Svič2	vlan 1	172.18.0.2/16	
Svič3	vlan 1	172.19.0.2/16	
Svič4	vlan 1	172.20.0.2/16	
Svič5	vlan 1	172.21.0.2/16	

Slika 8.1.2 IP adrese interfejsa

Router>enable	// Komanda enable za prelazak iz korisničkog u privilegovani mod
Router# configure terminal	// Ulazak u globalni konfiguracioni mod
Router(config)#hostname Ruter0	//Promena imena rutera
Ruter0(config)# interface fastEthernet 0/0	//Ulazak u mod za konfigurisanje interfejsa fa 0/0
Ruter0 (config-if)# ip address 172.16.0.1 255.255.0.0	// Konfigurisanje ip-adrese interfejsa fa 0/0
Ruter0 (config-if)#no shutdown	//Uključivanje (dizanje) interfejsa fa 0/0
Ruter0 (config-if)# exit	//Povratak u globalni konfiguracioni mod
Ruter0(config)# interface serial 0/0/0	//Ulazak u mod za konfigurisanje interfejsa s 0/0/0
Ruter0(config-if)# ip address 192.168.0.1 255.255.255.252	// Konfigurisanje ip-adrese interfejsa s 0/0/0
Ruter0(config-if)# clock rate 64000	//Definisanje brzine takta na interfejsu s 0/0/0
Ruter0(config-if)# bandwidth 64	//Definisanje propusnog opsega interfejsa s 0/0/0
Ruter0 (config-if)#no shutdown	//Uključivanje (dizanje) interfejsa s 0/0/0
Ruter0# copy running-config startup-config	//Memorisanje trenutne konfiguracije rutera
Ruter0# clock set 22:41 AUG 31 2016	//Podešavanje sata i datuma na ruteru

Slika 8.1.3 Opis komandi za konfigurisanje rutera

Komande korišćene za konfigurisanje rutera prikazane su na slikama 8.1.4-8.1.11. Detaljna objašnjenja komandi data su na primeru rutera Ruter0 radi upoznavanja sa postupkom osnovnog konfigurisanja rutera i same mreže (slika 8.1.3). Sa druge strane, za ostale rutere komande su samo taksativno navedene, jer je razlika u odnosu na Ruter0 samo u IP adresama interfejsa.

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter0
Ruter0(config)# interface fastEthernet 0/0
Ruter0(config-if)# ip address 172.16.0.1 255.255.0.0
Ruter0(config-if)# no shutdown
Ruter0(config-if)# exit
Ruter0(config)# interface fastEthernet 0/1
Ruter0(config-if)# ip address 192.168.2.1 255.255.255.252
Ruter0(config-if)# no shutdown
Ruter0(config)# interface serial 0/0/0
Ruter0(config-if)# ip address 192.168.0.1 255.255.255.252
Ruter0(config-if)# no shutdown
Ruter0(config)# interface serial 0/0/1
Ruter0(config-if)# ip address 192.168.1.1 255.255.255.252
Ruter0(config-if)# no shutdown
```

Slika 8.1.4 Osnovna konfiguracija Ruter 0

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter1
Ruter1(config)# interface fastEthernet 0/0
Ruter1(config-if)# ip address 172.17.0.1 255.255.0.0
Ruter1(config-if)# no shutdown
Ruter1(config-if)# exit
Ruter1(config)# interface serial 0/0/0
Ruter1(config-if)# ip address 192.168.0.2 255.255.255.252
Ruter1(config-if)# no shutdown
Ruter1(config)# interface serial 0/0/1
Ruter1(config-if)# ip address 192.168.3.1 255.255.255.252
Ruter1(config-if)# no shutdown
Ruter1(config)# interface serial 0/1/0
Ruter1(config-if)# ip address 192.168.5.1 255.255.255.252
Ruter1(config-if)# no shutdown
Ruter1(config)# interface serial 0/1/1
Ruter1(config-if)# ip address 192.168.13.1 255.255.255.252
Ruter1(config-if)# no shutdown
```

Slika 8.1.5 Osnovna konfiguracija Ruter 1

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter2
Ruter2(config)# interface fastEthernet 0/0
Ruter2(config-if)# ip address 192.168.2.2 255.255.255.252
Ruter2(config-if)# no shutdown
Ruter2(config-if)# exit
Ruter2(config)# interface serial 0/0/0
Ruter2(config-if)# ip address 192.168.3.2 255.255.255.252
Ruter2(config-if)# no shutdown
Ruter2(config)# interface serial 0/0/1
Ruter2(config-if)# ip address 192.168.4.1 255.255.255.252
Ruter2(config-if)# no shutdown
Ruter2(config)# interface serial 0/1/0
Ruter2(config-if)# ip address 192.168.6.1 255.255.255.252
Ruter2(config-if)# no shutdown
Ruter2(config)# interface serial 0/1/1
Ruter2(config-if)# ip address 192.168.14.1 255.255.255.252
Ruter2(config-if)# no shutdown
```

Slika 8.1.6 Osnovna konfiguracija Ruter 2

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter3
Ruter3(config)# interface fastEthernet 0/0
Ruter3(config-if)# ip address 172.19.0.1 255.255.0.0
Ruter3(config-if)# no shutdown
Ruter3(config-if)# exit
Ruter3(config)# interface serial 0/0/0
Ruter3(config-if)# ip address 192.168.1.2 255.255.255.252
Ruter3(config-if)# no shutdown
Ruter3(config)# interface serial 0/0/1
Ruter3(config-if)# ip address 192.168.4.2 255.255.255.252
Ruter3(config-if)# no shutdown
Ruter3(config)# interface serial 0/1/0
Ruter3(config-if)# ip address 192.168.7.1 255.255.255.252
Ruter3(config-if)# no shutdown
```

Slika 8.1.7 Osnovna konfiguracija Ruter 3

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter4
Ruter4(config)# interface fastEthernet 0/0
Ruter4(config-if)# ip address 172.18.0.1 255.255.0.0
Ruter4(config-if)# no shutdown
Ruter4(config-if)# exit
Ruter4(config)# interface serial 0/0/0
Ruter4(config-if)# ip address 192.168.5.1 255.255.255.252
Ruter4(config-if)# no shutdown
Ruter4(config)# interface serial 0/0/1
Ruter4(config-if)# ip address 192.168.8.1 255.255.255.252
Ruter4(config-if)# no shutdown
Ruter4(config)# interface serial 0/1/0
Ruter4(config-if)# ip address 192.168.11.1 255.255.255.252
Ruter4(config-if)# no shutdown
```

Slika 8.1.8 Osnovna konfiguracija Ruter 4

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter5
Ruter5(config)# interface fastEthernet 0/0
Ruter5(config-if)# ip address 192.168.9.1 255.255.255.252
Ruter5(config-if)# no shutdown
Ruter5(config-if)# exit
Ruter5(config)# interface serial 0/0/0
Ruter5(config-if)# ip address 192.168.8.2 255.255.255.252
Ruter5(config-if)# no shutdown
Ruter5(config)# interface serial 0/0/1
Ruter5(config-if)# ip address 192.168.10.2 255.255.255.252
Ruter5(config-if)# no shutdown
Ruter5(config)# interface serial 0/1/0
Ruter5(config-if)# ip address 192.168.6.2 255.255.255.252
Ruter5(config-if)# no shutdown
Ruter5(config)# interface serial 0/1/1
Ruter5(config-if)# ip address 192.168.13.2 255.255.255.252
Ruter5(config-if)# no shutdown
```

Slika 8.1.9 Osnovna konfiguracija Ruter 5

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter6
Ruter6(config)# interface fastEthernet 0/0
Ruter6(config-if)# ip address 172.20.0.1 255.255.0.0
Ruter6(config-if)# no shutdown
Ruter6(config-if)# exit
Ruter6(config)# interface serial 0/0/0
Ruter6(config-if)# ip address 192.168.7.2 255.255.255.252
Ruter6(config-if)# no shutdown
Ruter6(config)# interface serial 0/0/1
Ruter6(config-if)# ip address 192.168.10.1 255.255.255.252
Ruter6(config-if)# no shutdown
Ruter6(config)# interface serial 0/1/0
Ruter6(config-if)# ip address 192.168.12.1 255.255.255.252
Ruter6(config-if)# no shutdown
Ruter6(config)# interface serial 0/1/1
Ruter6(config-if)# ip address 192.168.14.2 255.255.255.252
Ruter6(config-if)# no shutdown
```

Slika 8.1.10 Osnovna konfiguracija Ruter 6

```
Router> enable
Router# configure terminal
Router(config)# hostname Ruter7
Ruter7(config)# interface fastEthernet 0/0
Ruter7(config-if)# ip address 172.21.0.1 255.255.0.0
Ruter7(config-if)# no shutdown
Ruter7(config)# interface fastEthernet 0/0
Ruter7(config-if)# ip address 192.168.9.2 255.255.255.252
Ruter7(config-if)# no shutdown
Ruter7(config-if)# exit
Ruter7(config)# interface serial 0/0/0
Ruter7(config-if)# ip address 192.168.11.2 255.255.255.252
Ruter7(config-if)# no shutdown
Ruter7(config)# interface serial 0/0/1
Ruter7(config-if)# ip address 192.168.12.2 255.255.255.252
Ruter7(config-if)# no shutdown
```

Slika 8.1.11 Osnovna konfiguracija Ruter 7

8.2. **Konfigurisanje OSPF protokola**

Na slici 8.2.1 su prikazane komande za konfigurisanje OSPF protokola na ruterima.

```
Ruter0(config)# router ospf 10
Ruter0(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruter0(config-router)# network 192.168.0.0 0.0.0.3 area 0
Ruter0(config-router)# network 192.168.1.0 0.0.0.3 area 0
Ruter0(config-router)# network 192.168.2.0 0.0.0.3 area 0
```

```
Ruter1(config)# router ospf 10
Ruter1(config-router)# network 172.17.0.0 0.0.255.255 area 0
Ruter1(config-router)# network 192.168.0.0 0.0.0.3 area 0
Ruter1(config-router)# network 192.168.3.0 0.0.0.3 area 0
Ruter1(config-router)# network 192.168.5.0 0.0.0.3 area 0
Ruter1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

```
Ruter2(config)# router ospf 10
Ruter2(config-router)# network 192.168.2.0 0.0.0.3 area 0
Ruter2(config-router)# network 192.168.3.0 0.0.0.3 area 0
Ruter2(config-router)# network 192.168.4.0 0.0.0.3 area 0
Ruter2(config-router)# network 192.168.6.0 0.0.0.3 area 0
Ruter2(config-router)# network 192.168.14.0 0.0.0.3 area 0
```

```
Ruter3(config)# router ospf 10
Ruter3(config-router)# network 172.19.0.0 0.0.255.255 area 0
Ruter3(config-router)# network 192.168.1.0 0.0.0.3 area 0
Ruter3(config-router)# network 192.168.4.0 0.0.0.3 area 0
Ruter3(config-router)# network 192.168.7.0 0.0.0.3 area 0
```

```
Ruter4(config)# router ospf 10
Ruter4(config-router)# network 172.18.0.0 0.0.255.255 area 0
Ruter4(config-router)# network 192.168.5.0 0.0.0.3 area 0
Ruter4(config-router)# network 192.168.8.0 0.0.0.3 area 0
Ruter4(config-router)# network 192.168.11.0 0.0.0.3 area 0
```

```
Ruter5(config)# router ospf 10
Ruter5(config-router)# network 192.168.6.0 0.0.0.3 area 0
Ruter5(config-router)# network 192.168.8.0 0.0.0.3 area 0
Ruter5(config-router)# network 192.168.9.0 0.0.0.3 area 0
Ruter5(config-router)# network 192.168.10.0 0.0.0.3 area 0
Ruter5(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

```
Ruter6(config)# router ospf 10
Ruter6(config-router)# network 172.20.0.0 0.0.255.255 area 0
Ruter6(config-router)# network 192.168.7.0 0.0.0.3 area 0
Ruter6(config-router)# network 192.168.10.0 0.0.0.3 area 0
Ruter6(config-router)# network 192.168.12.0 0.0.0.3 area 0
Ruter6(config-router)# network 192.168.14.0 0.0.0.3 area 0
```

```
Ruter7(config)# router ospf 10
Ruter7(config-router)# network 172.21.0.0 0.0.255.255 area 0
Ruter7(config-router)# network 192.168.9.0 0.0.0.3 area 0
Ruter7(config-router)# network 192.168.11.0 0.0.0.3 area 0
Ruter7(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

Slika 8.2.1 Konfigurisanje OSPF-a na ruterima

8.3. **Konfigurisanje EIGRP protokola**

Na slici 8.3.1 su prikazane komande za konfigurisanje EIGRP protokola na ruterima.

```
Ruter1(config)# router eigrp 10
Ruter1(config-router)# network 172.17.0.0 0.0.255.255
Ruter1(config-router)# network 192.168.0.0 0.0.0.3
Ruter1(config-router)# network 192.168.3.0 0.0.0.3
Ruter1(config-router)# network 192.168.5.0 0.0.0.3
Ruter1(config-router)# network 192.168.13.0 0.0.0.3
```

```
Ruter2(config)# router eigrp 10
Ruter2(config-router)# network 192.168.2.0 0.0.0.3
Ruter2(config-router)# network 192.168.3.0 0.0.0.3
Ruter2(config-router)# network 192.168.4.0 0.0.0.3
Ruter2(config-router)# network 192.168.6.0 0.0.0.3
Ruter2(config-router)# network 192.168.14.0 0.0.0.3
```

```
Ruter3(config)# router eigrp 10
Ruter3(config-router)# network 192.168.1.0 0.0.0.3
Ruter3(config-router)# network 192.168.4.0 0.0.0.3
Ruter3(config-router)# network 192.168.7.0 0.0.0.3
Ruter3(config-router)# network 172.19.0.0 0.0.255.255
```

```
Ruter4(config)# router eigrp 10
Ruter4(config-router)# network 172.18.0.0 0.0.255.255
Ruter4(config-router)# network 192.168.5.0 0.0.0.3
Ruter4(config-router)# network 192.168.8.0 0.0.0.3
Ruter4(config-router)# network 192.168.11.0 0.0.0.3
```

```
Ruter5(config)# router eigrp 10
Ruter5(config-router)# network 192.168.6.0 0.0.0.3
Ruter5(config-router)# network 192.168.8.0 0.0.0.3
Ruter5(config-router)# network 192.168.9.0 0.0.0.3
Ruter5(config-router)# network 192.168.10.0 0.0.0.3
Ruter5(config-router)# network 192.168.13.0 0.0.0.3
```

```
Ruter6(config)# router eigrp 10
Ruter6(config-router)# network 172.20.0.0 0.0.255.255
Ruter6(config-router)# network 192.168.7.0 0.0.0.3
Ruter6(config-router)# network 192.168.10.0 0.0.0.3
Ruter6(config-router)# network 192.168.12.0 0.0.0.3
Ruter6(config-router)# network 192.168.14.0 0.0.0.3
```

```
Ruter7(config)# router eigrp 10
Ruter7(config-router)# network 172.21.0.0 0.0.255.255
Ruter7(config-router)# network 192.168.9.0 0.0.0.3
Ruter7(config-router)# network 192.168.11.0 0.0.0.3
Ruter7(config-router)# network 192.168.12.0 0.0.0.3
```

Slika 8.3.1 Konfigurisanje EIGRP-a na ruterima

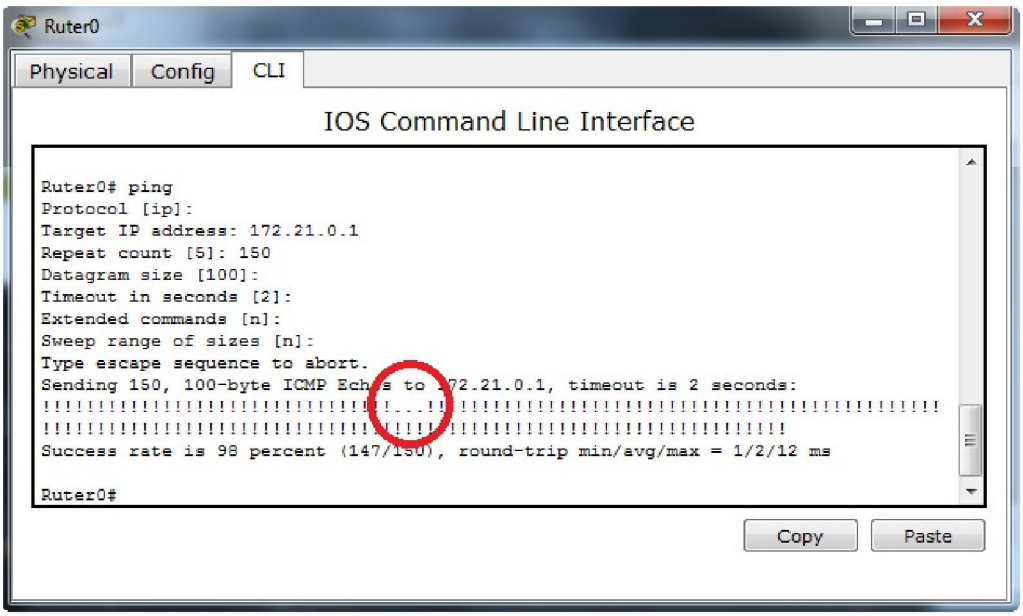
8.4. **Poređenje protokola na osnovu brzine konvergencije**

Jedan od izuzetno važnih parametara u komparaciji OSPF i EGRP protokola jeste vreme konvergencije mreže. U okviru laboratorijske analize simuliraćemo dva različita scenarija koja će oslikavati nepredviđene situacije (kvarove) koje se mogu desiti na mreži, preciznije, na ruteru koji učestvuje u prenosu saobraćaja. U okviru prvog scenarija simuliraćemo pad jednog linka isključivanjem interfejsa na ruteru i njegovo ponovno uključivanje. Drugi scenario prikazaće situaciju u slučaju otkaza jednog rutera i njegovo ponovno uključivanje. Konkretno, analiza će se izvršiti praćenjem kontinualnog prenosa ICMP paketa (korišćenjem *extended ping* komande) između rutera Ruter0 i Ruter7, dok će se otkaz linka i otkaz rutera simulirati na ruteru Ruter5.

Scenario 1 – Prekid linka:

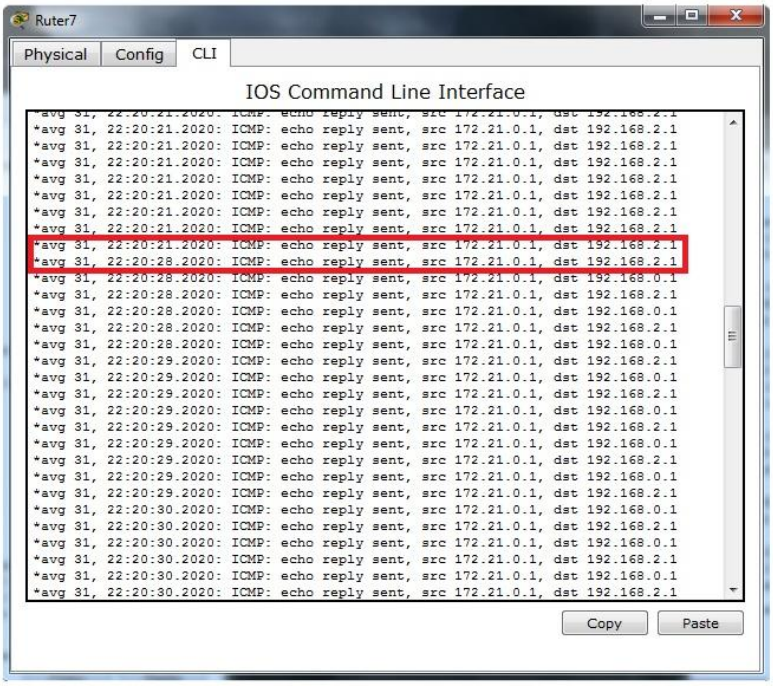
Za prenos podataka od rutera Ruter0 do rutera Ruter7 inicijalno se koristi putanja Ruter0 -> Ruter2 ->Ruter5 ->Ruter7. Simuliranje pada linka (serijska veza izmedju Ruter2 i Ruter5) izvodi se isključivanjem serijskog interfejsa S0/1/0 na ruteru Ruter5.

Pri korišćenju OSPF protokola, nakon pada linka, pronalazi se nova ruta, tj. u ovom slučaju više ravnopravnih ruta (*load balancing*). Testiranje je izvršeno kontinualnim slanjem ICMP paketa sa rutera Ruter0 korišćenjem *extended ping* komande. Poslato je 150 paketa uz standardni *time-out* interval u trajanju od 2 sekunde (*slika 8.27*).



Slika 8.4.1 Slanje ICMP paketa od strane rutera Ruter0 - OSPF

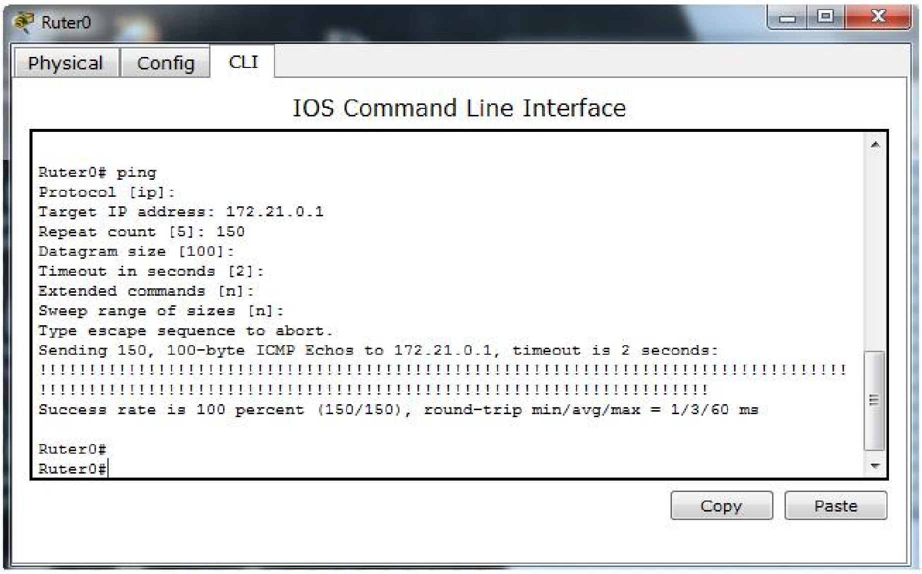
Komunikacija između rutera (prenos ICMP paketa) praćena je korišćenjem komande *debug ip icmp* na ruteru Ruter7 (slika 8.4.2).



Slika 8.4.2 Praćenje prenosa ICMP paketa od strane rutera Ruter7

Na osnovu rezultata prikazanim u terminalu rutera Ruter7, dolazimo do zaključka da je vreme potrebno za konvergenciju mreže, ukoliko se koristi OSPF protokol, između 6 i 7 sekundi. Takođe, do ovog zaključka mogli smo doći i jednostavnim proizvodom broja izgubljenih paketa koje je poslao ruter Ruter0 i poznavanjem trajanja *time-out* intervala.

Pri korišćenju EIGRP protokola, istim postupkom, dobijeni su znatno bolji rezultati. EIGRP za prenos takođe koristi rutu Ruter0 -> Ruter2 ->Ruter5 ->Ruter7, a prilikom pada te rute koristi se ruta Ruter0 -> Ruter1 -> Ruter5 -> Ruter7. EIGRP za razliku od OSPF bira ovu rutu, jer koristi više faktora (u odnosu na OSPF) za određivanje nove rute. Nakon identične analize, dolazi se do zaključka da je vreme konvergencije mreže, u slučaju korišćenja EIGRP protokola, oko 1ms i da u ovom slučaju čak i ne dolazi do gubitka ICMP paketa (slika 8.4.3).



Slika 8.4.3 Slanje ICMP paketa od strane rutera Ruter0 - EIGRP

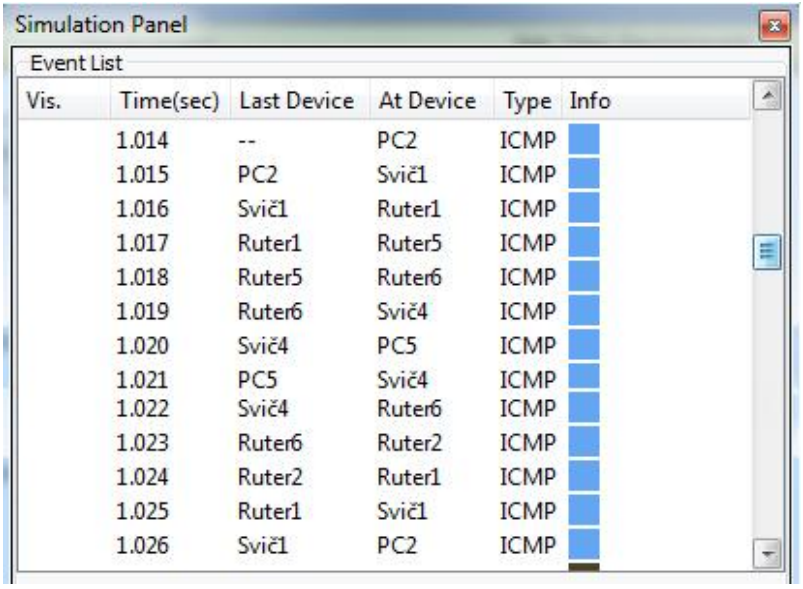
Scenario 2 – Pad rutera:

U slučaju simulacije isključenja rutera, vreme konvergencije je isto kao i u okviru scenarija 1. Za konvergenciju u slučaju korišćenja OSPF protokola potrebno je 6 sekundi, dok se u slučaju korišćenja EIGRP potrebna 1 sekunda. Jedino što se u ovom slučaju razlikuje jesu nove putanje koje ruteri biraju za dalji prenos paketa u odnosu na scenario 1.

8.5. **Poređenje performansi protokola pri različitim parametrima linka**

U okviru ovog dela analize posmatrani su parametri protokola rutiranja u zavisnosti od vrednosti propusnog opega (*bandwith*) i kašnjenja na linku (*latency*).

U prvom delu simulacije praćena je brzina prenosa ICMP paketa od PC2 ka PC5 u zavisnosti od širine propusnog opsega serijskih interfejsa. Na serijskim linkovima korišćene su vrednosti *bandwith-a* od 64kbit/s, 128kbit/s, 256kbit/s, 512kbit/s, 1544kbit/s, 2048kbit/s, 4096kbit/s. U slučaju kada je na mreži podignut EIGRP protokol, a širina propusnog opsega je standardnih 1544kbit/s, za prenos podataka koriste se putanje PC2->Svič1->Ruter1->Ruter2->Ruter6->Svič4->PC5 i PC2->Svič1->Ruter1->Ruter5->Ruter6->Svič4->PC5. Praćenjem kretanja ICMP paketa kroz mrežu utvrđeno je da je za prenos ovog paketa potrebno 6ms (slika 8.5.1). Kada je na mreži podignut OSPF protokol, situacija je potpuno ista.



Slika 8.5.1 Kretanje ICM paketa kroz mrežu

Nakon menjanja širine propusnog opsega na linku između rutera R1 i R5 dolazi se do sledećih zaključaka:

- Ukoliko se širina linka smanji, bez obzira na to koji protokol je podignut, podaci će se prenositi samo rutom PC2->Svič1->Ruter1->Ruter2->Ruter6->Svič4->PC5, dok će vreme potrebno za prenos poruke ostati isto.
- Ukoliko se širina linka poveća, bez obzira na to koji protokol je podignut, podaci će se prenositi samo rutom PC2->Svič1->Ruter1->Ruter5->Ruter6->Svič4->PC5, dok će vreme potrebno za prenos nešto kraće u slučaju EIGRP.

U ovom slučaju videli smo da oba protokola od prvobitne dve rute biraju onu koja nakon promena ima veći propusni opseg, pokušaćemo da "nateramo" protokole da izaberu neku treću putanju. Promenili smo širinu propusnog opsega između rutera Ruter0 i rutera Ruter1 na 4096kbit/s.

U ovom slučaju OSPF koristi novu rutu PC2->Svič1->Ruter1->Ruter0->Ruter2->Ruter6->Svič4->PC5, a vreme potrebno za slanje paketa sada iznosi 7ms. Sa druge strane, EIGRP nastavlja da koristi stare putanje i ICMP paket isporučuje za 6 ms. Na osnovu ovoga vidimo da je EIGRP u datom slučaju efikasniji. Takav ishod je očekivan i opravdan time što, za razliku od OSPF, EIGRP ne koristi samo vrednost propusnog opsega pri izračunavanju optimalne rute.

U drugom delu ispitivanja ponašanja protokola rutiranja u zavisnosti od parametara linka, posmatrali smo kašnjenje na linku (*latency*). Kao i u proučavanju protokola, u zavisnosti od širine propusnog opsega i u ovom slučaju smo posmatrati prenos ICMP paketa između računara PC2 i PC5. Kao i u prethodnoj analizi, pri standardnim vrednostima na serijskim linkovima (*bandwidth =1544 kbit/s, latency = 20ms*) oba protokola koriste rute PC2->Svič1->Ruter1->Ruter2->Ruter6->Svič4->PC5 i PC2->Svič1->Ruter1->Ruter5->Ruter6->Svič4->PC5.

Analiza je sprovedena promenom vrednosti kašnjenja na linku između rutera Ruter1 i Ruter5. U slučaju OSPF-a, bilo da se radi o smanjenju ili povećanju kašnjenja na linku, putanje koje se koriste ostaju iste. Ono što se menja jeste brzina kojom se ICMP poruke dostavljaju između rutera. Ono što je očekivano jeste brzina dostave, koja se u slučaju povećanja kašnjenja očekivano smanjuje. Sa druge strane, EIGRP protokol je svestan promene kašnjenja na link tj. za jedinu rutu proglašava onu koja ima manje kašnjenje.

U slučaju pokušaja pronalaska "treće" rute, odnosno povećanja kašnjenja istovremeno na linkovima Ruter1-Ruter2 i Ruter1-Ruter5 dolazimo do zaključka da EIGRP pronalazi i koristi novu rutu PC2->Svič1->Ruter1->Ruter0->Ruter2->Ruter6->Svič4->PC5, dok je OSPF, očekivano, "nesvestan" svih ovih pogoršanja na linku i pakete nastavlja da distribuira starim rutama.

9.ZAKLJUČAK

Već nakon teorijske analize OSPF i EIGRP protokola moglo se naslutiti da nije moguće doneti konačan i jednoznačan odgovor o tome koji od ova dva protokola treba odabrati pri konfigurisanju mreže, već da ta odluka zavisi od konkretnog primera, odnosno konkretne mrežne topologije. Laboratorijskom analizom ova pretpostavka je u velikoj meri potvrđena, ali na osnovu našeg primera, malu prednost možemo dati EIGRP protokolu, pre svega zbog rezultata dobijenih nakon merenja konkretnih parametara.

Na osnovu brzine prenosa podataka (pri različitim karatkeristikama linka) i vremenu potrebnom za konvergenciju mreže (usled različitih događaja na mreži), možemo konstatovati da je EIGRP protokol bolji za korišćenje u okviru manjih računarskih mreža. Ono što je ograničenje i nešto što uvek stoji u senci EIGRP protokola, je to da je on vlasništvo kompanije Cisco. To zapravo znači da u određenim situacijama protokol rutiranja nećemo moći da biramo na osnovu onoga što nam je "potrebno" već na osnovu onoga što "imamo" jer EIGRP radi samo na Cisco uređajima. Takođe, bitno je napomenuti da EIGRP troši znatno manje sistemskih resursa.

Predmet daljeg istraživanja i nešto što bi pomoglo u donošenju konačne odluke o pobedniku u "dvoboju" između EIGRP i OSPF protokola, jeste komparacija na osnovu nekih drugih parametara, kao i analiza zahtevnijih računarskih mreža, gde je neophodno hijerarhijsko rutiranje (ovde se očekuju bolje performanse OSPF protokola). Takođe, potrebno je izvršiti komparaciju OSPFv3 i EIGRPv6 verzija rotokola koji su namenjeni rutiranju u IPv6 mrežama, imajući u vidu sve veći značaj IPv6 tehnologija.

LITERATURA

[1] Z. Čiča, Komutacioni sistemi – predavanja, (http://telekomunikacije.etf.bg.ac.rs/predmeti/te4ks/ks.php)

[2] www.cisco.com

[3] www.ciscopress.com

[4] Cisco Networking Academy

[5] https://networklessons.com

[6] Cisco Certified Network Associate, Todd Lammle, 2005

[7] https://learningnetwork.cisco.com/

[8] http://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

[9] Umrežavanje računara od vrha ka dnu, James F. Kurose, Keith W. Ross, 2014.

[10] http://www.cnet.com/

[11] http://routingpacket.blogspot.com