

UNIVERZITET U BEOGRADU
ELEKTROTEHNIČKI FAKULTET



**ISPITIVANJE MEHANIZAMA ZAŠTITE U MPLS MREŽI
PRIMENOM MREŽNOG SIMULATORA**

Master rad

Mentor:

Dr Zoran Čiča, docent

Kandidat:

Sofija Vasiljević 2014/3152

Beograd, April 2016.

SADRŽAJ

SADRŽAJ	2
1. UVOD.....	3
2. MPLS TE	4
2.1. OSPF	7
2.2. LDP PROTOKOL	8
2.3. MPBGP	10
2.4. TRAFFIC ENGINEERING.....	12
3. SIMULACIONI SOFTVER.....	15
3.1. GNS3	15
3.2. IPERF	19
4. KONFIGURACIJA MREŽE	23
4.1. KONFIGURACIJA INTERFEJSA	24
4.2. KONFIGURACIJA OSPF-A	27
4.3. USPOSTAVLJANJE MPLS-A.....	29
4.4. USPOSTAVLJANJE MPBGP-A	33
4.5. KREIRANJE L3VPN-A.....	35
5. SIMULACIJE.....	37
5.1. PRIMARNA I SEKUNDARNA PUTANJA.....	39
5.2. DINAMIČKA PUTANJA.....	44
5.3. FRR ZAŠTITA.....	46
5.4. IPERF TESTIRANJA.....	53
5.5. DISKUSIJA	61
6. ZAKLJUČAK.....	62
LITERATURA.....	63
SPISAK SKRAĆENICA	64
SPISAK SLIKA	66

1. UVOD

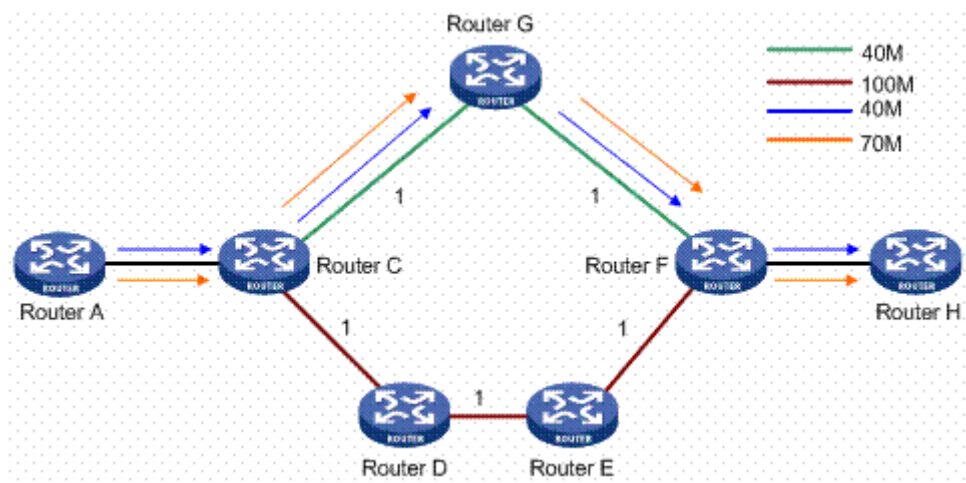
Razvoj novih servisa za obradu i prenos podataka, glasa i slike na Internetu je doveo do velikog povećanja saobraćaja. Prenosna mreža telekomunikacionih operatora, koja bi trebalo da podrži to povećanje, uglavnom je realizovana korišćenjem optičkih veza i MPLS (*Multiprotocol Label Switching*) protokolom. Jednostavno povećanje kapaciteta je često ekonomski neisplativo, zbog čega je potrebno pribеći optimizaciji postojeće mreže. Ograničenje predstavljaju nedovoljan kapacitet postojećih veza, visoka cena izgradnje/zakupa i korišćenja novih veza i opreme za te veze, a dodatno ograničenje predstavlja i postojanje radio-relejnih linkova, koji su značajno manjih kapaciteta od optičkih veza, koji postoje u postojećim mrežama sistema prenosa i koji se koriste za zaštitu postojećih servisa. MPLS mreža predstavlja robusno rešenje za slučaj prekida u prenosnoj mreži, ali se bez korišćenja QoS (*Quality of Service*) ne može koristiti za realizaciju transportne mreže u okruženju Servis Provajdera zbog zagušenja linkova, kojima se ne može upravljati.

U ovom radu će biti prikazan dodatni skup funkcionalnosti koji se dobija korišćenjem RSVP (*Resource Reservation Protocol*) protokola u transportnoj mreži telekomunikacionog operatora. Biće pokazano da se korišćenjem različitih softvera i protokola može ostvariti željena optimizacija prenosne mreže. Biće ispitano ponašanje mreže u strogo kontrolisanim situacijama i pokazano da nema potrebe da u mreži postoje zagušeni linkovi, dokle god postoje nepotpuno iskorišćeni kapaciteti.

U drugom poglavlju date su osnovne informacije o MPLS mrežnoj tehnologiji, opisane su i raznovrsne primene RSVP-TE (*Resource Reservation Protocol Traffic Engineering*) protokola, kao i tehnologije poput FRR (*Fast Reroute*). Trećim poglavljem predstavljeni su softverski paketi upotrebljeni za realizaciju ove mreže i testiranje nad istom. U četvrtom poglavlju kreirana je neophodna mreža za potrebe eksperimenata i analize, gde su dodate konfiguracije samih mrežnih elemenata i provera uspostava odgovarajućih protokola. U petom poglavlju su vršene simulacije nad postojećom mrežom i data je diskusija o različitim pristupima optimizacije mreže. Priloženi su dobijeni rezultati sprovedenih istraživanja. Na kraju rada, nakon analize urađenih testova, predstavljeni su zaključci o optimizaciji transportne mreže telekomunikacionog operatora.

2.MPLS TE

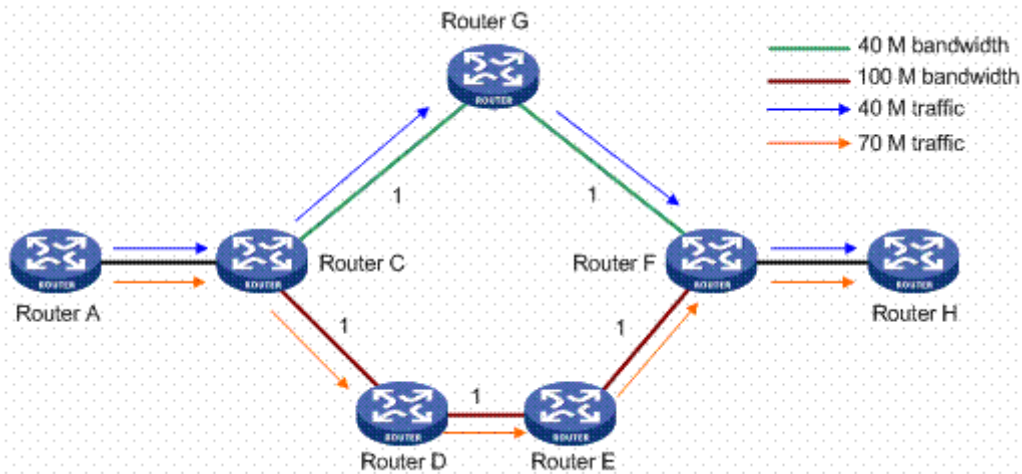
Klasični protokoli rutiranja koji usmeravaju pakete na osnovu njihovih IP (*Internet Protocol*) zaglavlja nisu više efikasni kad su u pitanju sve veći zahtevi za brzinom obrade i prosleđivanja paketa jer se paketski procesor preopterećuje u značajnoj meri. IP takođe nije u mogućnosti da pruži neke od servisa (*QoS, Traffic Engineering, VPN*), a postoji i izazov sa rutiranjem na osnovu najkraće metrike.



Slika 2.1. Rutiranje saobraćaja na osnovu IGP-a [11]

Na slici 2.1. dat je primer usmeravanja saobraćaja na osnovu najbolje cene, pri čemu na toj putanji nema dovoljno propusnog opsega za sav saobraćaj, čime će doći do gubitaka paketa. Čak i prilikom zagušenja, saobraćaj se ne preusmerava na druge putanje u mreži koje ostaju neiskorišćene.

Slikom 2.2. saobraćaj je prerutiran drugom putanjom, od strane administratora mreže, koja može da podrži zahtevane protoke, i na taj način neće doći do gubitka saobraćaja.



Slika 2.2. Rutiranje saobraćaja na osnovu TE [11]

IP rutiranje procesorski je zahtevno zbog provera kontrolnih suma (*checksum*), menjanja izvorišnih i odredišnih MAC (*Medium Access Control*) adresa, dekrementiranja TTL (*Time to Live*) polja i to na svakom hopu duž putanje. ATM (*Asynchronous Transfer Mode*) tehnologija je uvedena kao rešenje nekih od problema: podržava QoS, fiksna dužina paketa i integracija različitih vrsta saobraćaja. Nažalost ATM se pokazao kao kompleksno i skupo tehničko rešenje.

MPLS je tehnologija koja omogućava rutiranje saobraćaja (paketa, okvira ili ćelija) preko IP infrastrukture, ali na takav način da čvorovi mreže odredišne odluke usmeravanja (na koji interfejs treba proslediti paket), donose na osnovu labela, a ne na osnovu IP destination adrese. MPLS tehnologija ne pripada ni mrežnom sloju (sloj 3 OSI referentnog modela), ni sloju 2 OSI (*Open Systems Interconnection*) modela. Po funkcionalnosti MPLS je između ta dva nivoa.

MPLS usmeravanje saobraćaja omogućava da se na IP infrastrukturi realizuje sledeće:

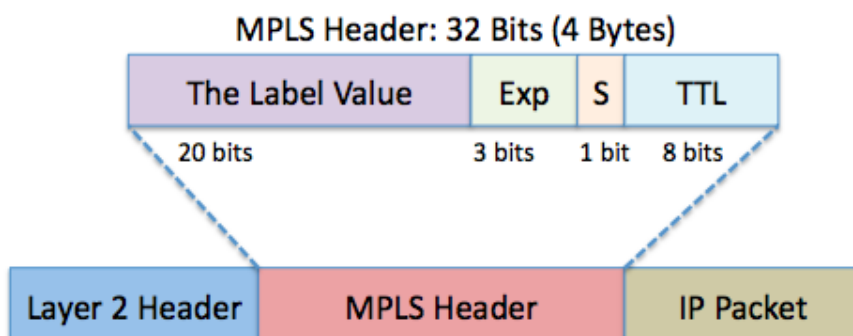
- Prenos saobraćaja koji nije IP, koji može biti: FR (*Frame Relay*), ATM, Ethernet, .1Q, PPP (*Point-to-Point*), HDLC (*High-Level Data Link Control*) ili drugi.
- Realizacija virtuelnih privatnih mreža – VPN (*Virtual Private Network*).
- TE (*Traffic engineering*), koji predstavlja usmeravanje saobraćaja onim rutama, koje administrator mreže smatra najboljim za dati saobraćaj, a koje su različite od trasa kojima bi sami mrežni uređaji usmeravali saobraćaj na osnovu protokola rutiranja.
- Rezervacija resursa u mreži.

VPN je generički naziv za čitav niz servisa. Realizuje se određenom konfiguracijom PE (*Provider Edge*) rutera, različitom za svaku vrstu VPN-a. VPN se sastoji od dve ili više lokacija. Konfigurisanjem ovih servisa moguće je obezbediti da korisnici VPN servisa imaju utisak da imaju sopstvenu mrežnu infrastrukturu.

Integracija MPLS aplikacijskih komponenti, uključujući L3VPN (*Layer 3 VPN*), L2VPN (*Layer 2 VPN*), TE, QoS, GMPLS (*Generalized MPLS*) i IPv6 (*IP version 6*) omogućavaju razvoj visoko efikasnih, skalabilnih i sigurnih mreža koje garantuju SLA (*Service Level Agreement*).

MPLS mreža ima rutere u jezgru i na obodu mreže. Oni u mreži i dalje rade na sličan način: analiziraju zaglavlje paketa i odlučuju kuda da ga proslede. Za svaki paket se određuje pripadna

klasa ekvivalentnog prosleđivanja odnosno FEC (*Forwarding Equivalence Class*), a za svaku klasu sledeći hop. FEC je skup paketa koji će se na isti način prosleđivati kroz mrežu.



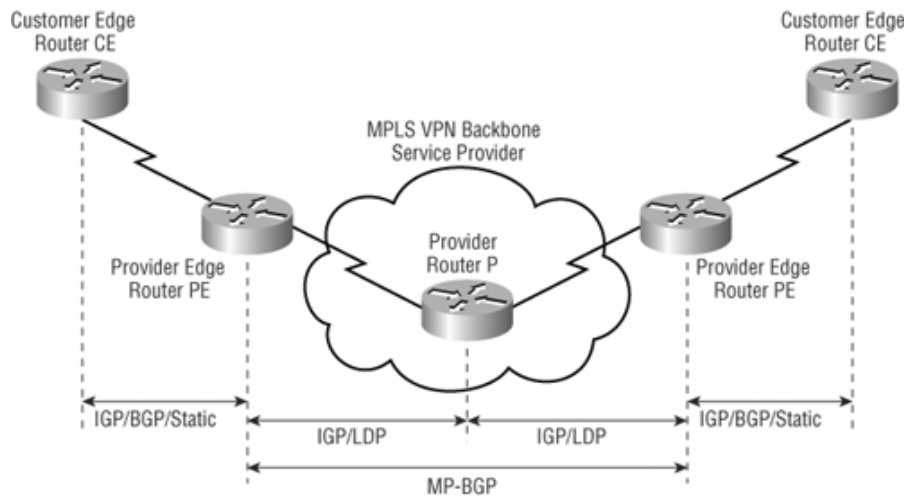
Slika 2.3. MPLS zaglavlje [12]

Na slici 2.3. prikazano je MPLS zaglavlje, u kom je labela najvažniji deo. Labela je dužine 20 bita i služi za usmeravanje paketa. EXP polje je tu da obezbedi QoS funkcionalnost. MPLS čvorovi mogu, ako su tako konfigurisani, da pakete sa različitom kombinacijom EXP bita, tretiraju različito prilikom rutiranja. S (*Stack*) polje označava da postoji više MPLS zaglavlja. TTL polje je iste namene kao i TTL u IP zaglavlju, sa svakim pređenim hopom ono se dekrementira, dok ne padne na 1, tada se paket odbacuje. Ovim mehanizmom se sprečava da paket beskonačno kruži u mreži.

Prosleđivanje paketa se vrši na osnovu MPLS tabele usmeravanja. *Label imposition* je dodavanje labele na izvorni paket, i to obavlja ulazni (*ingress*) ruter. *Label swapping* je zamena labele na paketu na kom već postoji labela. *Label popping* je skidanje labele sa paketa. To radi izlazni (*egress*) ruter, ili ruter neposredno pre egress rutera (tada se to zove *penultimate label popping*). Put od ulaznog do izlaznog rutera zove se LSP (*Label Switched Path*). Čvorovi koji obavljaju usmeravanje paketa poznati su i kao LSR (*Label Switching Router*).

Korisnički ruter prosleđuje IP paket ka svom SP-u i on stiže na PE ruter servis provajdera. Ruter PE analizira IP zaglavlje, i pridružuje paket određenoj klasi ekvivalentnog prosleđivanja. Zatim pregleda svoju MPLS tabelu usmeravanja, nalepi labelu pridruženu tom FEC-u i pošalje ga kroz određeni interfejs. Paket stiže do P (*Provider*) rutera u mreži. On vrši zamenu labele, međutim iako je labela zamenjena drugom one se obe odnose na isti FEC. Taj korak se ponavlja do poslednjeg P rutera na putanji, koji nakon *penultimate hop popping*-a prosleđuje paket ka egress PE ruteru. On analizira samo IP zaglavlje, pronalazi da je adresa odredišta direktno povezana ruta, i ka njoj prosleđuje paket. P ruteri nisu svesni postojanja te korisničke mreže, dok PE ruteri jesu. MPLS labela ima samo lokalni značaj za prijemni ruter, samo ruter koji prima paket zna šta predstavlja ta labela, i na osnovu nje zna kako da usmeri paket.

Neophodno za postojanje MPLS mreže je protokol rutiranja i najčešće su to OSPF (*Open Shortest Path First*) i/ili ISIS (*Intermediate System to Intermediate System*) i BGP (*Border Gateway Protocol*). OSPF ili ISIS se koriste samo za razmenu *loopback* adresa i adresa interfejsa preko kojih su realizovane P-P i P-PE veze. Ruterima su dovoljne ove informacije kako bi naučili topologiju mreže. BGP se koristi za prenos svih ostalih ruta, gde se ubrajaju eksterne rute naučene od eksternih BGP *peer*-ova, kao i adrese interfejsa preko kojih su realizovane PE-CE (*Customer Edge*) veze. Svaki PE ruter ima svoje konektovane rute, i preko BGP protokola obaveštava svoje *peer*-ove o tim rutama. Na P ruterima nije konfigurisan BGP protokol [1, 2].



Slika 2.4. Primer podržanih protokola u MPLS mreži [13]

Kao što se može primetiti sa slike 2.4. koja predstavlja kontrolnu ravan MPLS mreže, u jezgru te mreže koriste se IGP (*Interior Gateway Protocol*) protokoli uz LDP (*Label Distribution Protocol*) protokol. A na samom obodu mreže se može koristiti neki od IGP protokola, BGP ili statičke rute kako bi se ostvarila IP povezanost između korisnika i servis provajdera.

2.1. OSPF

OSPF predstavlja jedan od najšire korišćenih protokola rutiranja koji je zasnovan na stanju linka (*link state protocol*). Njegova najveća prednost je što je javni protokol i svi proizvođači mrežnih uređaja ga mogu iskoristiti. Kod protokola zasnovanih na stanju linka svaki ruter u mreži ima informacije o topologiji mreže.

Ažuriranja se vrše jedino kada se desi promena u mrežnoj topologiji. U slučaju promene tj. promene linka, ruter kreira LSA (*Link-State Advertisement*). Ova informacija se šalje svim susednim uređajima. Svi LSA zapisi se čuvaju u specijalnoj bazi podataka LSDB (*Link-State Data Base*). U trenutku startovanja protokola kreira se LSDB koja sadrži samo jedan zapis tj. sopstveni LSA.

OSPF ima dve primarne karakteristike. Prva je ta da je protokol otvoren. OSPF specifikacije su objavljene kao RFC (*Request For Comments*) 1247. Druga glavna karakteristika je da je OSPF baziran na SPF (*Shortest Path First*) algoritmu. Informacija na pridruženim interfejsima, koja koristi metriku i druge varijable je uključena u OSPF LSA-ove.

Metrika je mera poželjnosti neke rute za čiji se proračun koristi broj skokova, propusni opseg, opterećenje, kašnjenje i pouzdanost dok je sledeći skok direktno spojena mreža ili ruter kojem se može proslediti paket za traženo odredište. Kako OSPF ruteri skupljaju informacije, koriste SPF algoritam da izračunaju najkraći put do sledećeg čvora. Ako ruter sazna više pravaca do odredišta, prvo će pronaći najduže poklapanje prefiksa u tabeli. U slučaju istih podmreža, gledaće najnižu administrativnu distancu od protokola koji su objavili tu rutu. U poslednjem koraku, ako je

ruta potekla od istog protokola, gledaće najnižu metriku do nje. OSPF cena je obrnuto proporcionalna protoku interfejsa, odnosno što je viši protok niža je cena.

$$\text{Metrika} = \frac{10^8 \text{bps}}{\text{Protok}}$$

Ovo znači da će interfejs od 100Mbps imati cenu od 1, kao i svi interfejsi sa protokom većim od 100Mbps. Rezultat toga je da ruteri u mreži ne mogu da naprave tačne proračune kad se uporede Fast Ethernet interfejsi sa Gigabit Ethernet interfejsima, jer oba imaju cenu 1. Ovo je rešeno modifikovanjem referentnog protoka na interfejsu, što se postiže komandom *auto-cost reference bandwidth*.

Još jedna prednost protokola stanja linka u odnosu na protokole vektora rastojanja je brža konvergencija odnosno nakon promena u topologiji brže se formiraju putanje u mreži.

Najveća jedinica bez hijerarhije je autonomni sistem, što je mreža ili skup mreža pod javnom upravom koje dele zajedničku politiku rutiranja. Iako je OSPF unutrašnji protokol rutiranja, sposoban je primati smerove od drugih AS (*Autonomous System*) i slati ih njima. Ovi ruteri koji se zovu ruteri za granična područja vode zasebnu topološku bazu podataka za svako područje. Topološka baza podataka sadrži skup LSA-ova od svih rutera u istom području. S obzirom na to da ruteri unutar istog područja dele istu informaciju, imaju jednake topološke baze podataka.

Postoji nekoliko tipova OSPF paketa:

- *Hello* – koristi se pri uspostavljanju i održavanju susedstva sa ostalim OSPF ruterima. Takođe se koristi pri izboru DR (*Designated Router*) i BDR (*Backup Designated Router*).
- *Database Description* – sadrži kraću listu zapisa koja se proverava sa glavnom bazom
- *LSR (Link-State Request)* – prijemni ruteri koriste ovaj paket za izvršavanje upita nad bazom
- *LSU (Link-State Update)* – koristi se kao odgovor na LSR kao i za ažuriranje sa novim informacijama
- *Link-State Acknowledgement* – potvrda da je LSU paket primljen

Svaki ruter ima sopstveni ID, istog formata kao IP adresa, 32-bitni broj. Služi kako bi se ruteri međusobno razlikovali i radi određivanja DR i BDR. To su ruteri sa ulogom distribucije u brodkast mrežama.

Velike mreže deli na oblasti i omogućava hijerarhijsku strukturu. Oblast 0 ili area 0 se naziva *backbone area*, i sve ostale oblasti su povezane direktno s njom. Svaka OSPF mreža mora imati ovu oblast [3].

2.2. LDP protokol

MPLS tabela usmeravanja može se kreirati preko dva protokola: LDP i RSVP. Cisco ruteri rade *label-binding* za sve prefikse u IP tabeli rutiranja osim za BGP prefikse. LDP je razvijen specijalno za signalizaciju labela, dok je RSVP postojao i pre MPLS-a. Za potrebe signalizacije labela razvijena je ekstenzija istog. Kako bi se tabela pravilno ispunila potrebno je da ruteri

signaliziraju jedni drugima svoje labele. Nizvodni smer je onaj kojim se šalje korisnički saobraćaj. U slučaju RSVP-a, dodela labela uvek je na zahtev.

LDP koristi TCP (*Transmission Control Protocol*) protokol po portu 646, i vrši razmenu poruka između rutera preko Hello paketa.

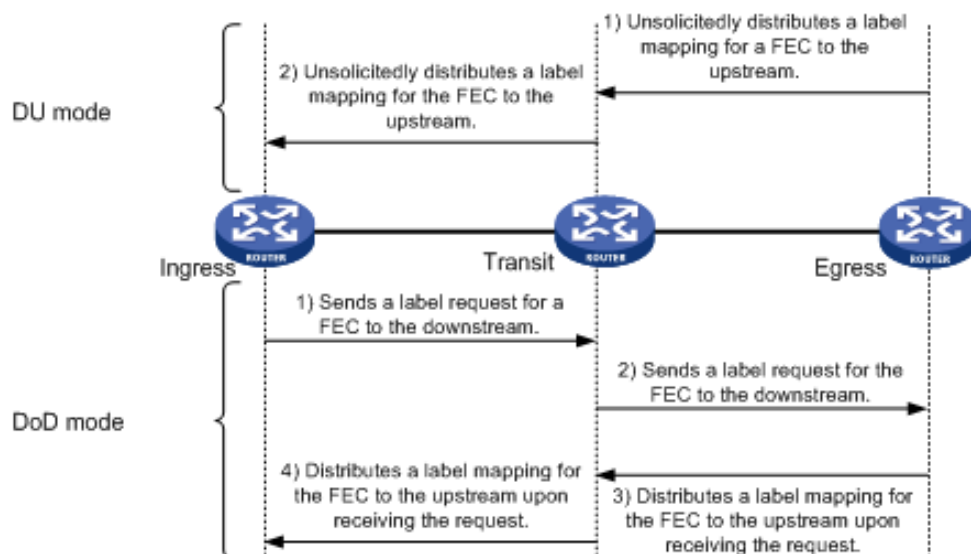
LDP poruke su:

- Discovery messages - oglašavanje postojanja LSR
- Session messages - uspostava, održavanje i raskidanje sesije
- Advertisement messages - kreiranje, promena i brisanje mapiranja labela
- Notification messages - razmena informacija (npr. o greškama).

Tri su pristupa u pridruživanju labela FEC-u:

- Unsolicited vs. On demand: *unsolicited* - gde ruter šalje FEC i njemu pridruženu labelu svim susedima, drugi ruteri upoređuju rute i ukoliko je dobio od nizvodnog rutera prihvata odnosno *on demand* – uzvodni čvor inicira pridruživanje zahtevom ka nizvodnom ruteru.
- Independent vs. Ordered control: *independent* - ruter dodeljuje labele prefiksima u svojoj tabeli usmeravanja i šalje ih bez obzira na to da li je ruter dobio mapiranje u labelu za tu rutu od nizvodnog rutera odnosno *ordered* - ruter šalje svoje (*FEC, Labela*) parove samo za one FEC za koje ima mapiranje dobijeno od nizvodnog rutera.
- Liberal retention vs. Conservative retention: *liberal* - ruter čuva sve parove (*FEC, Labela*) dobijene od svih suseda, a prosleđuje pakete na osnovu labela dobijenih od nizvodnog rutera odnosno *conservative* - ruter čuva samo one parove (*FEC, Labela*) dobijene od nizvodnog suseda za dati FEC (*od Next Hop*).

Izlazni PE ruter može zahtevati od P rutera ili da u potpunosti skine labelu ili da stavi labelu *explicit-null* [1, 2].

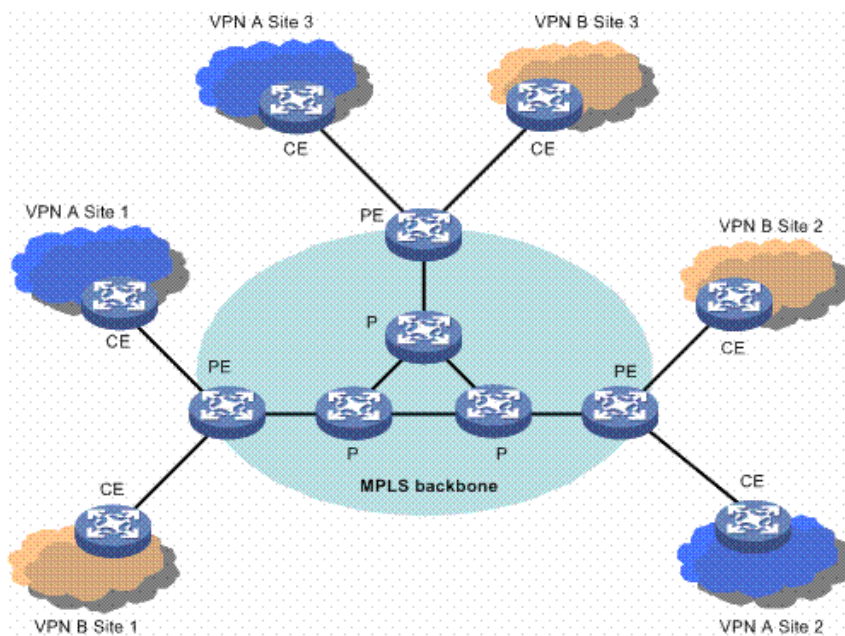


Slika 2.2.1. Koraci oglašavanja labela [14]

Na slici 2.2.1. prikazano je dodeljivanje labela bez zahteva i na zahtev. U prvom slučaju nizvodni ruter šalje labele ka uzvodnom ruteru bez zahteva, dok u drugom šalje odgovarajuće labele tek nakon prijema zahteva.

2.3. MPBGP

Na svakom PE ruteru se za potrebe jednog VPN-a izdvoji deo resursa rutera i pridruži se tom VPN-u. U resurse koji se pridružuju VPN-u spadaju obavezno i interfejsi (logički ili fizički), memorija i labele, a u zavisnosti od tipa VPN-a i neki drugi specifičniji resursi kao što su *route-distinguisher*-i, *route-target*-i, AS brojevi itd. Pridruživanje ovih resursa određenom VPN-u zove se virtuelizacija.



Slika 2.3.1. MPLS L3VPN arhitektura [15]

Slikom 2.3.1. prikazan je primer arhitekture L3VPN-ova dva različita korisnika u jednoj MPLS mreži, gde oba imaju po 3 udaljene lokacije. VPN postoji kako bi obezbedio razdvajanje saobraćaja za različite korisnike. To znači da nijedan paket koji potiče sa bilo koje lokacije VPN-a 1 ne sme da bude upućen ni na jednu lokaciju koja pripada VPN-u 2. Kom VPN-u neki saobraćaj pripada ulazni PE ruter zaključuje na osnovu interfejsa po kom mu taj saobraćaj dolazi.

Kad sazna kom VPN-u saobraćaj pripada, ulazni PE ruter treba da otpremi paket. U tu svrhu stavlja na njega stek od dve labele. Spoljna labele služi da mreža može pravilno da usmeri paket do izlaznog PE rutera, dok unutrašnja služi izlaznom PE ruteru da odredi kom VPN-u paket pripada. Spoljna labele je zajednička za bilo koji saobraćaj između dva PE rutera, bilo da je u pitanju IP ili VPN saobraćaj. Unutrašnja je različita za svaki VPN. Unutrašnje labele omogućavaju da se izvrši razdvajanje servisa, a razmenjuju se putem MPBGP (*Multiprotocol BGP*) protokola.

Svaki PE ruter u svojoj memoriji mora da ima posebnu tabelu usmeravanja za svaki VPN u koji je uključen. Ta tabela se naziva VRF (*Virtual Routing and Forwarding*). U njoj se nalaze svi prefiksi iz jednog VPN-a. U različitim VRF-ovima prefiksi mogu da se preklapaju.

MPBGP je proširenje BGP protokola koje omogućava prenošenje *routing* informacija za različite adresne familije. Neke adresne familije su IPv6, VPNv4 (*VPN version 4*), VPNv6 (*VPN version 6*), a ima ih još. Svaki PE ruter uspostavlja MPBGP sesiju sa svim ostalim PE ruterima u mreži, što znači da postoji potpuna meš BGP sesija. Pomoću MPBGP protokola se popunjavaju VRF tabela na PE ruterima.

Za potrebe prenosa *routing* informacija za različite adresne familije izmišljeni su i potpuno novi BGP atributi koji se nazivaju *extended attributes*, a za MPLS L3 VPN su bitni „*route-distinguisher*“, „*route-target-export*“ i „*route-target-import*“.

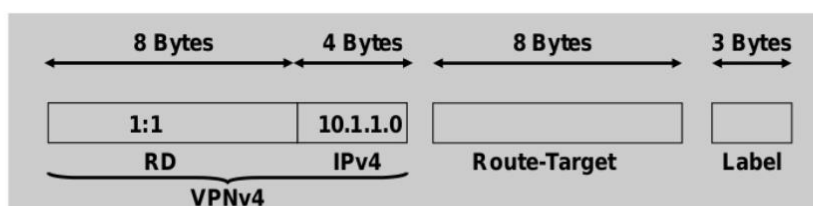
Problem nastaje kada za više organizacija treba uspostaviti MPLS L3 VPN, a adrese se preklapaju u smislu istih adresa. Jedini način da se taj problem reši je proširenje adresnog prostora što znači dodavanje novih bita na postojeću adresu. Upravo zbog toga je uveden *route-distinguisher* atribut. *Route-distinguisher* je samo jedan niz od 32 bita koji se dodaje na regularne IP adrese tako da svaka privatna adresa postaje jedinstvena na nivou jedne MPLS mreže. Na taj način, privatne IP adrese sa dodatim *route-distinguisher* atributom, postaju jedinstvene i problem preklapanja adresa između organizacija time je rešen. Dodavanjem *route-distinguisher* na IPv4 adresu, ona postaje VPNv4 adresa.

Svaki PE ruter za svaki korisnički VPN u koji je uključen mora da održava posebnu VRF tabelu. *Route-target-export* i *route-target-import* atributi služe BGP procesu da svaki korisnički prefiks smesti u tačno određenu VRF tabelu. Administrator mora da vodi računa kako dodeljuje ove attribute.

Adresna familija interesantna za MPLS L3VPN je VPNv4. VPNv4 adresna familija je skup VPNv4 adresa. Ove adrese nastaju od običnih IP adresa dodavanjem *route-distinguisher* atributa.

MPLS-VPN Technology: Control Plane

The Control Plane for MPLS VPN Is Multi-Protocol BGP



MP-BGP UPDATE message showing only VPNv4 address, RT, Label

Slika 2.3.2. VPNv4 adresna familija [16]

Na slici 2.3.2. prikazana je VPNv4 adresa, gde se vidi da je nastala dodavanjem *route-distinguisher* atributa IPv4 adresi. Uz nju, nalazi se *route-target* za odgovarajući VPN, kao i dodeljena labela potrebna za usmeravanje saobraćaja tog korisnika.

MPBGP sesije uspostavljaju se između PE rutera po principu svaki sa svakim. Preko jedne MPBGP sesije se razmenjuju sve labela za sve VPN-ove između dva PE rutera.

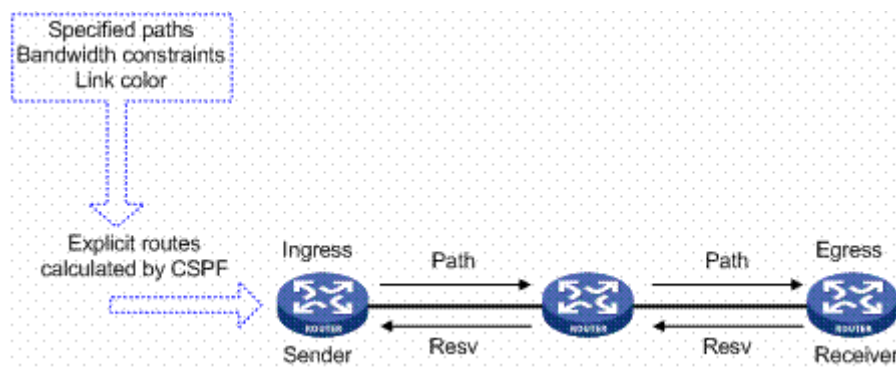
U našoj mreži potrebni preduslovi za konfiguraciju MPLS L3VPN-a su uspostavljene MPBGP sesije između svih PE rutera i postojanje MPLS tunela između dva PE rutera. Kad je to ispunjeno može se krenuti sa konfiguracijom VPN-a [4].

2.4. Traffic Engineering

Postoji mnogo razloga koji utiču na primenu MPLS-a, ali je saobraćajni inženjering (*TE*) najveći. TE se bavi optimizacijom rada već integrisanih mreža kombinujući različita saznanja iz teorije saobraćaja. Cilj je da se optimalno iskoriste resursi mreže i da se poboljša kvalitet usluga koje se nude. TE može biti orijentisan na poboljšanje saobraćajnih parametara usluga i tokova ili na poboljšanje iskorišćenja resursa mreže. Jedna od funkcija labele je da obezbedi mehanizam koji se integriše sa prosleđivanjem paketa u procesu rutiranja, i na taj način omogući "vođenje" paketa po unapred određenim putanjama kroz mrežu. Daljim administrativnim manipulacijama moguće je obezbediti manuelnu raspodelu opterećenja u mreži i time maksimalno iskorišćenje raspoloživog propusnog opsega u mreži (moguće je da određeni, najatraktivniji, delovi mreže ponesu maksimalno opterećenje, dok drugi delovi ostaju neiskorišćeni).

Atributi za optimalni LSP su destinacija, propusni opseg, prioritet, zaštita preko *Fast Reroute* mehanizma. Implementacijom RSVP protokola tj. njegove ekstenzije postiže se realizacija IntServ QoS arhitektura.

Za razliku od LDP protokola kod koga se MPLS tuneli između PE rutera uspostavljaju automatski, kod RSVP protokola je potrebna manuelno uneti podatke za svaki tunel između PE rutera. Ovi tuneli su unidirekcionni. Kako bi se uspostavio tunel, postoje dve vrste poruka: PATH i RESV. Ulazni PE ruter šalje PATH poruku svom nizvodnom susedu, a to je neki P ruter. Svaki od rutera na putanji proverava ovu poruku i alokira potrebna sredstva za tunel. Ruter PE postavlja Router Alert flag u IP zaglavlju PATH poruke, kojim navodi sve usputne rutere do izlaznog PE, da treba da analiziraju poruku pre nego što je proslede dalje. Na taj način P ruteri dobijaju informaciju da će oni biti P ruteri za taj tunel, čiji je identifikator tunela u poruci, a da su PE ruteri početni (*head*) odnosno završni (*tail*) ruteri za taj tunel. Po prijemu PATH poruke poslednji ruter, PE, alokira neophodnu labelu i prosleđuje tu informaciju svom uzvodnom P ruteru, putem RESV poruke. PATH poruka se šalje sa kraja na kraj tunela, dok se RESV poruka šalje samo svom uzvodnom susedu.



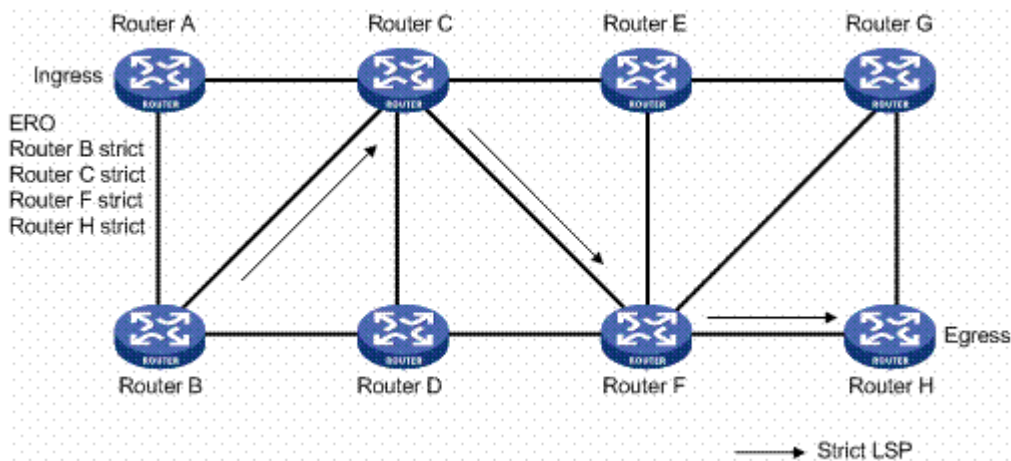
Slika 2.4.1. RSVP-TE signalizacija [11]

Slikom 2.4.1. predstavljen je put kojim idu PATH i RESV poruke. PATH poruka, kojom P ruteri saznaju da će biti P ruteri tog tunela, ide od ulaznog do izlaznog PE ruteru. RESV poruka kreće se u suprotnom smeru uz slanje labela ka svom uzvodnom ruteru. Kako su resursi duž ovog puta rezervisani, servisi koji se prenose tom putanjom imaju zagarantovan protok.

Po defaultu putanja tunela je ona koju uspostavi IGP na osnovu metrike. Moguće je u okviru PATH poruke postaviti eksplicitno čvorove kroz koje će poruka ići i na taj način uspostaviti tunel preko te određene putanje. Uspostavljanje takve putanje koja nije najkraća u smislu IGP metrike je poznata kao TE.

RSVP protokol ima ugrađene mehanizme za zaštitu saobraćaja. Svi oni se svode na signalizaciju nekih drugih putanja u slučaju da dođe do otkaza na primarnoj putanji. Kod LDP protokola ne postoje mehanizmi za zaštitu saobraćaja, ali LDP će uspostaviti novi MPLS tunel drugom putanjom. Za to će mu trebati malo više vremena nego RSVP protokolu jer ne zna unapred kojom putanjom će ići novi tunel. Kod RSVP mehanizma putanja kojom će ići novi tunel je poznata, u nekim slučajevima tunel je već uspostavljen i čeka da primarni tunel otkáže.

Za jedan MPLS odnosno LSP moguće je putem RSVP-a konfigurirati primarnu putanju i jednu ili više sekundarnih putanja. Svaka od sekundarnih putanja može biti signalizirana ili ne. Ukoliko su razmenjene labela ili ne, uvek su poznate, tj. poznati su ruteri preko kojih će biti uspostavljene. Slično statičkom rutiranju, i statička LSP putanja ne zahteva signalizaciju, ali zahteva konfigurisanje na svakom hopu po pitanju labela i drugih resursa. Što se tiče labavog eksplicitnog puta, čvorovi kroz koje će LSP proći mogu biti zahtevani ali čvor i njegov prethodni hop mogu imati druge uređaje između sebe.



Slika 2.4.2. Primer eksplicitne putanje [11]

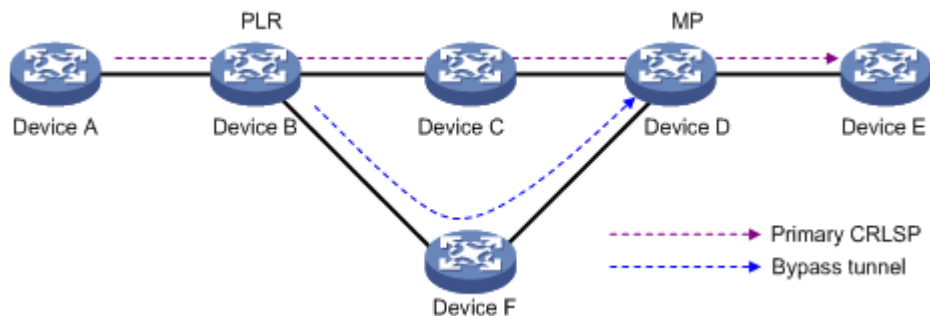
Na slici 2.4.2. dat je primer eksplicitne putanje, pri čemu su navedeni konkretni sledeći hopovi do samog odredišta. Time se mogu i izbeći neki od čvorova u mreži. Na takvoj putanji dva susedna hoba su direktno povezani ruteri.

Prebacivanje na sekundarnu putanju vrši se uvek kad se otkrije otkaz nekog linka ili čvora na primarnoj putanji. Prebacivanje je samo privremeno. Po ispadu primarnog MPLS tunela i prebacivanja saobraćaja na sekundarni, posle isteka vremenskog intervala koji je konfigurabilan,

ulazni ruter će pokušati da uspostavi primarni tunel. Ukoliko postoji putanja preko koje će se realizovati primarni tunel on će biti uspostavljen, a odmah zatim saobraćaj prerutiran na primarni tunel. Ukoliko ne, ulazni ruter će sačekati neko vreme, opet konfigurabilno, sve dok ne uspostavi primarni tunel. Iako je možda neki P ruter detektovao otkaz linka, on ne sme da preusmeri saobraćaj, jedino što sme je da obavesti početak tunela tj. ulazni PE ruter.

Fast Reroute jedan je od načina zaštite MPLS tunela. Realizuje se tako što ulazni ruter prilikom inicijalizacije MPLS tunela saopšti svim nizvodnim ruterima da treba da iniciraju rezervni tunel, i da razmene labela za njega. Taj rezervni tunel počinje od nekog nizvodnog rutera a može se završiti na nekom od nizvodnom rutera uključujući i izlazni ruter. FRR zaštita je samo privremenog karaktera, gde je svakom ruteru dopušteno da sam preusmeri saobraćaj, tako da saobraćaj nesmetano teče dok ulazni ruter ne shvati da treba da preusmeri saobraćaj. Za razliku od primarne i sekundarne putanje, ovde je i ostalim ruterima dopušteno da preusmeravaju saobraćaj. U oba slučaja svaki ruter koji detektuje neki otkaz mora obavestiti ulazni ruter.

Postoje dve varijante FRR zaštite: zaštita linka i zaštita čvora. U slučaju zaštite čvora ruteri su slobodni da uspostavljaju rezervne tunele koji će se završavati na bilo kom nizvodnom ruteru koji im nije susedni. U slučaju zaštite linka, ruter može da uspostavi rezervni tunel i do svog prvog nizvodnog suseda. *FRR Facility backup* koristi mogućnost stavljanje labela na stek, i omogućava zaštitu više MPLS tunela. Razlika u odnosu na one to one FRR je ta što se ovde ne radi zamena labela već se na postojeću labelu dodaje još jedna labela, koja se naziva spoljna labela. Kad paket stigne do kraja tunela, taj ruter skida ovu spoljnu labelu, i dalje usmerava saobraćaj po unutrašnjoj labeli koja postaje prva na steku. MPLS TE FRR nije od pomoći kad otkaze PE ruter koji je početna odnosno završna tačka TE tunela. PLR (*Point of Local Repair*) je početni ruter *bypass* tunela na putu primarnog LSP-a. MP (*Merge Point*) je izlazni ruter *bypass* tunela.



Slika 2.4.3. TE FRR [17]

Na slici 2.4.3. prikazan je MPLS TE FRR koji koristi unapred uspostavljene bekap tunele za zaštitu primarnog LSP-a. Svrha FRR je da se preusmeri saobraćaj u slučaju otkaza linka ili čvora.

Za TE izgrađena je mreža za rutiranje predviđenog saobraćaja, i to tako da administrator mreže manipuliše saobraćajem na način koji mreži odgovara. Iako su u mreži simetrična topologija i simetričan protok, opterećenje može biti i često jeste asimetrično. TE se može izvesti na osnovu IGP cena, ATM/FR ili MPLS-a.

Motivacija za TE: povećanje efikasnosti resursa protoka, sprečavanje previše iskorišćenih (zagušenih) linkova dok su drugi neiskorišćeni; osigurati najpoželjniji/odgovarajući put za neki/sav saobraćaj, premošćavanje najkraćeg puta izabranog od strane IGP-a; zamena ATM/FR jezgra mreže, ultimativni cilj je smanjenje troškova, kao i razvoj usluga koje servis provajder može ponuditi [5].

3. SIMULACIONI SOFTVER

Za potrebe testiranja u postojećoj mreži korišćen je GNS3 (*Graphical Network Simulator 3*). GNS3 je besplatan, softver otvorenog koda, koji može biti upotrebljen od strane svakoga. Ovaj alat omogućava kreiranje virtuelnih uređaja, i može se koristiti za simulacije kompleksnih mrežnih topologija. Koristi Dynamips emulacioni softver kako bi simulirao Cisco IOS (*Internetwork Operating System*).

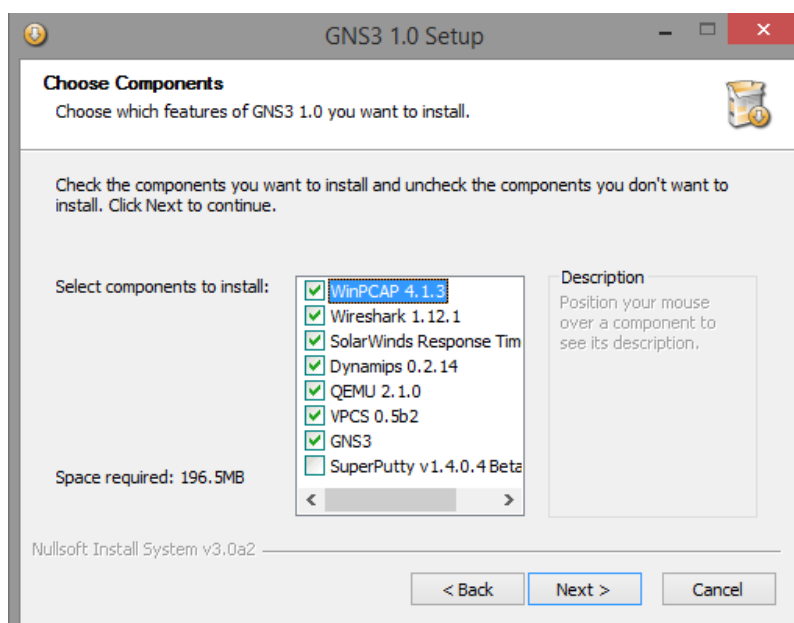
Cisco IOS MPLS dostavlja visoko skalabilnu, diferenciranu, IP uslugu s kraja na kraj sa jednostavnim konfiguracijama, upravljanjem za korisnike i provajdere. Širok spektar platformi podržava ovo rešenje, koje je od suštinskog značaja za servis provajdera i *enterprise* mrežu.

3.1. GNS3

GNS3 alat se može naći na sajtu: <https://www.gns3.com/software/download>. Preuzimanje je besplatno, i potrebna je registracija putem mail-a.

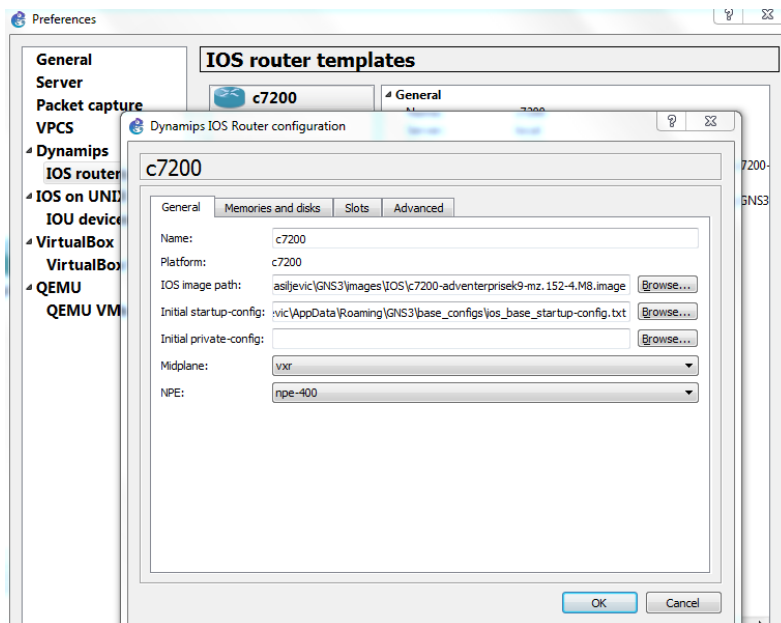
Instalacija softvera sama po sebi je jednostavna, potrebno je pratiti uputstva kao i instalirati sve potrebne dodatne programe: WinpCAP, Dynamips, Wireshark.

U ovom radu je korišćena trenutno najnovija verzija 1.3.11.



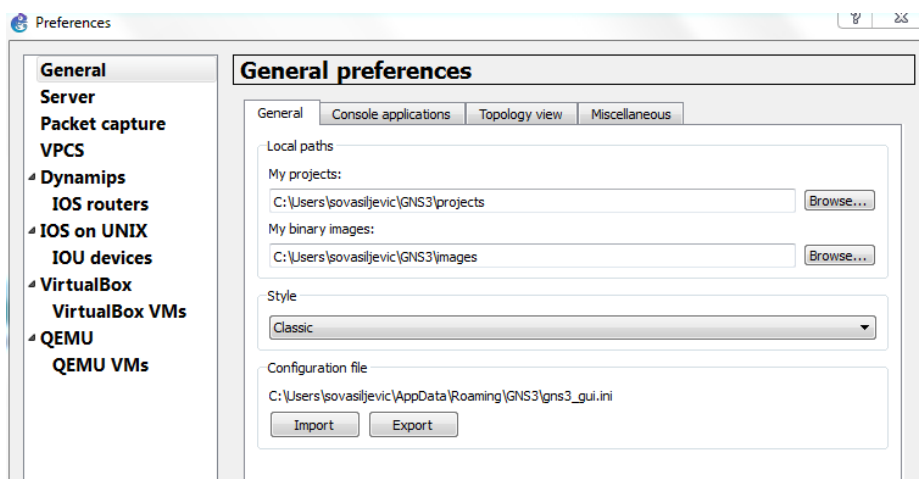
Slika 3.1.1. GNS3 komponente koje se instaliraju

Na slici 3.1.1. prikazan je prozor prilikom instalacije simulatora odnosno izbor mogućih komponenti koje se mogu odabrati.



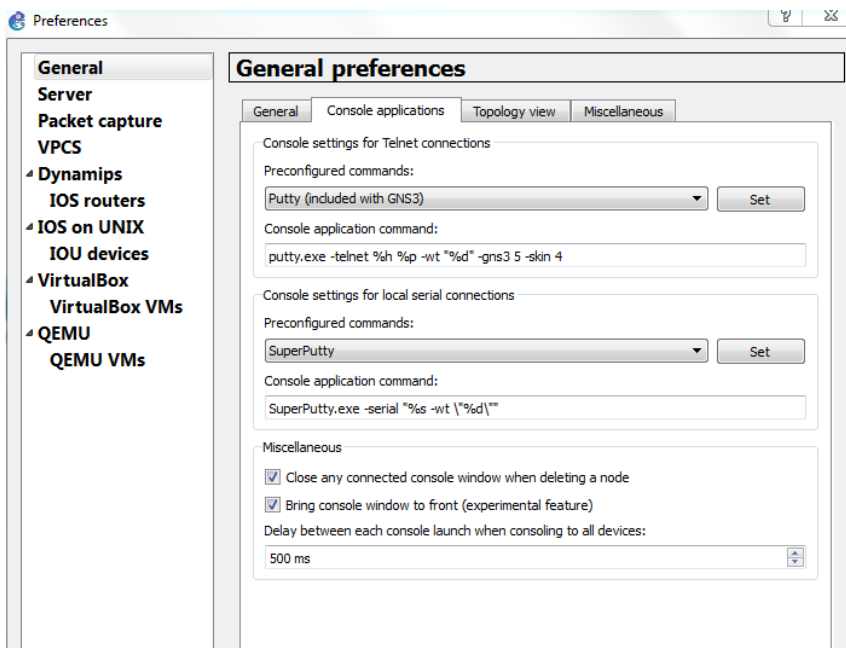
Slika 3.1.2. IOS image izbor

Kako bi se koristili uređaji, prvo se mora nabaviti *image* za platformu koja se emulira, kako je to prikazano na slici 3.1.2. Za potrebe ovog rada korišćen je *image* za Cisco 7200 platformu. Nakon instalacije samog softvera potrebno je izvršiti neka dodatna podešavanja. To se radi opcijom Edit → Preferences → Dynamips → IOS Routers.



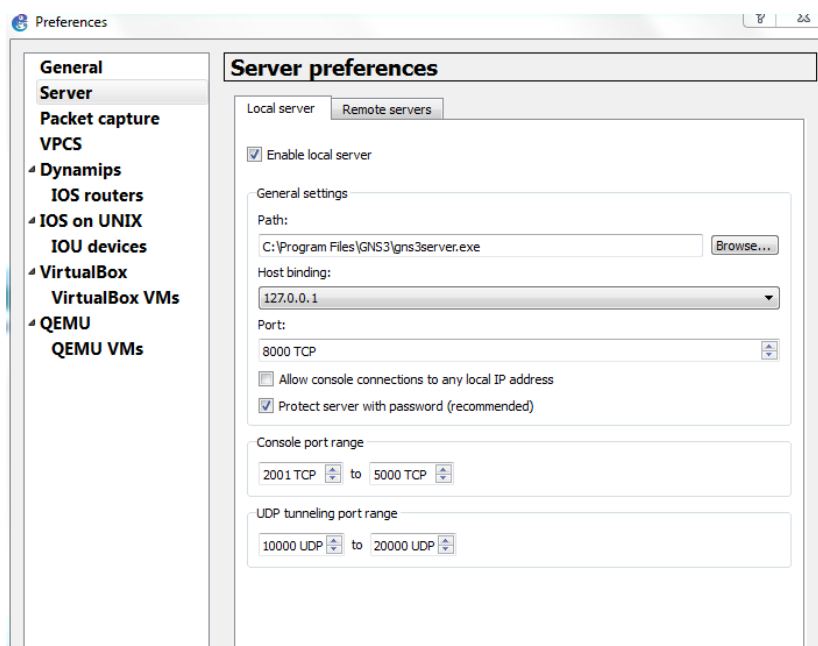
Slika 3.1.3. Put ka odgovarajućim folderima

Potrebno je proveriti put ka folderima **projects** i **images** radi sigurnosti da su na željenom mestu, kako je to urađeno na slici 3.1.3. Početna podešavanja su dovoljna, osim u slučaju ako je GNS3 pokrenut na više mašina, tada treba obratiti pažnju na ista.



Slika 3.1.4. Terminal podešavanja

Na slici 3.1.4. prikazana su konzolna podešavanja. Uz instalaciju GNS3 uključen je Putty. Takođe su podržane sve konzolne aplikacije koje omogućavaju pristup preko protokola kao što su Telnet i SSH (SecureCRT, Telnet i Teraterm).

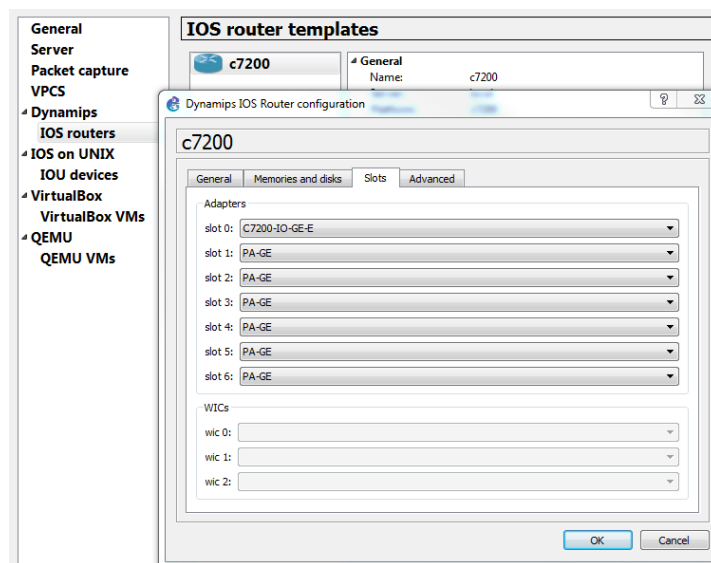


Slika 3.1.5. Server opcije

Na slici 3.1.5. dat je prikaz opštih opcija za server. U pitanju su portovi koje server koristi za primanje i slanje TCP/UDP paketa. Za potrebe ovog rada početna podešavanja nisu menjana.

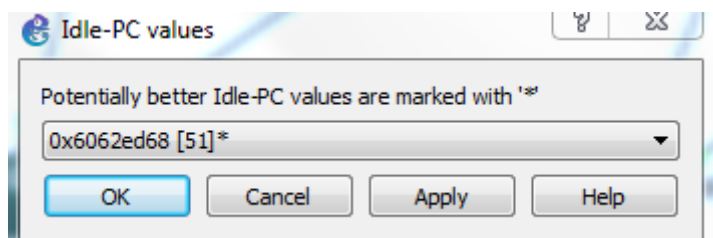
GNS3 softverski paket može se koristiti sa lokalnim serverom ili udaljenim serverom (*remote server*). Kada se koristi lokalni server, za izvršavanje komandi na ruterima i emulacije rutera, koriste se lokalni resursi (resursi računara na kome je instaliran GNS3 softverski paket).

Jedina opcija koja bi mogla biti promenjena je količina memorije koja je dozvoljena po jednoj sesiji dynamips-a.



Slika 3.1.6. Izbor interfejsa na ruteru

Nakon toga, u opcijama za IOS rutere, postoji prozor slots, na kojem se vrši odabir željenih interfejsa. Za potrebe ovog rada, iskorišćeni su Gigabit Ethernet interfejsi kao što je prikazano na slici 3.1.6.



Slika 3.1.7. Podešavanje idle PC vrednosti

GNS3 koristi idle PC vrednost za svoje rutere, kao na slici 3.1.7. Ova vrednost kontroliše uzorak CPU (*Central processing unit*) koji je iskorišćen od strane softvera, u suprotnom iskorišćenost procesora je na 100% i izvođenje drugih zadataka je znatno sporije.

Ponekad prilikom rada nije dovoljno podesiti samo ovu vrednost idle PC, kako bi se smanjila CPU iskorišćenost. Tad je potrebno otvoriti konzolne prozore pokrenutih uređaja i sačekati još neko vreme [6, 7].

3.2. IPERF

IPERF je alat za merenje performansi mreže, koji meri TCP/UDP protok kroz mrežu. Kod prenosa podataka, protok je količina podataka uspešno prenesena preko linka sa jednog na drugi kraj u datom vremenskom periodu, izražava se bitima u sekundi.

IPERF na osnovu svojih klijent-server funkcionalnosti može da meri protok između dva kraja, unidirekciono ili bidirekciono. On dozvoljava korisniku skup najraznovrsnijih parametara koji mogu biti iskorišćeni za testiranje mreže, ili alternativno za optimizaciju i podešavanje mreže.

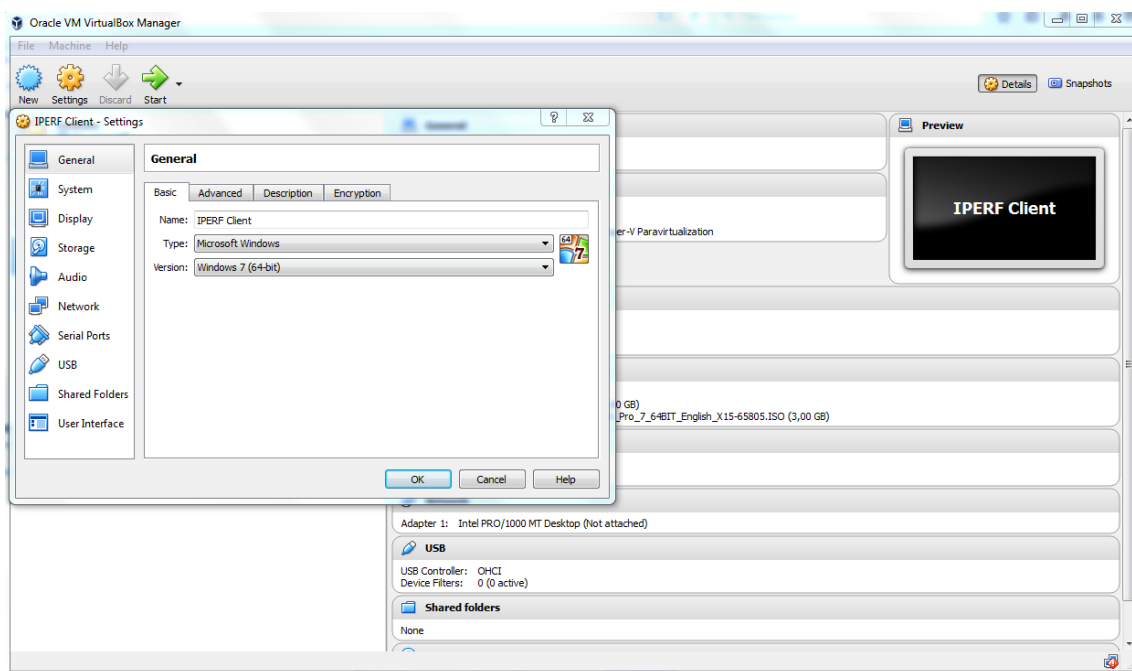
Ovaj alat je sposoban za generisanje saobraćaja koji koristi TCP i UDP (*User Datagram Protocol*) protokole.

Testovi TCP/UDP korisni su za obavljanje različitih vrsta testova:

- Kašnjenje (vreme odziva), može da se meri sa ping komandom
- Džiter, može da se meri sa IPERF UDP testom
- Gubitak paketa, može da se meri sa IPERF UDP testom
- *Throughput* testovi, mogu se meriti pomoću TCP testova

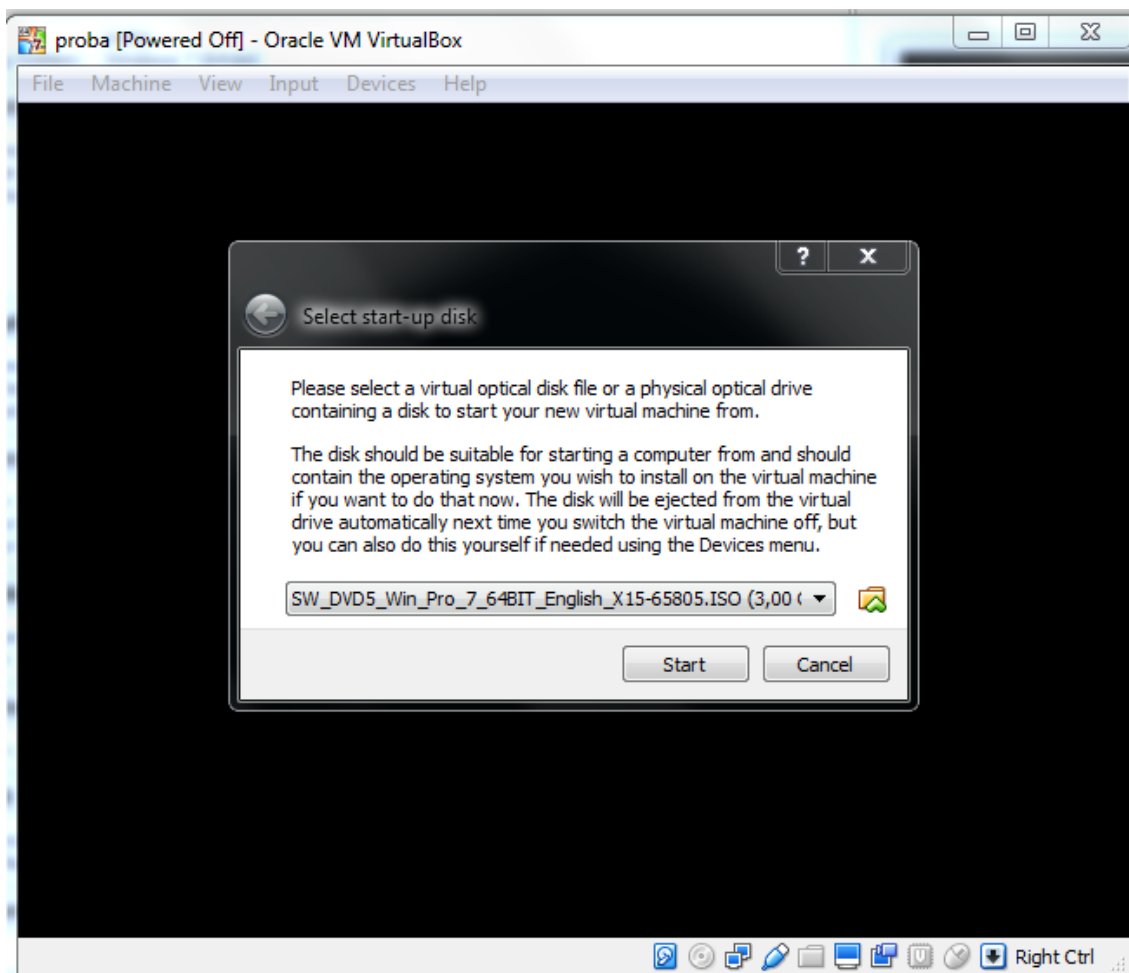
U postojećoj mreži IPERF je iskorišćen na sledeći način: instaliran je VirtualBox, koji se može naći na sledećem sajtu <https://www.virtualbox.org/wiki/Downloads>.

Zatim su u okviru VirtualBox-a kreirane virtuelne mašine na sledeći način:



Slika 3.2.1. Dodavanje nove virtualne mašine u VirtualBox-u

Prilikom pokretanja iste, pojaviće se sledeći ekran kao na slici 3.2.1., gde je potrebno uneti disk za startovanje nove virtuelne mašine. U ovom slučaju je korišćen Windows operativni sistem, što je prikazano na slici 3.2.2. Network manager na windows mašini se konektuje preko DHCP (*Dynamic Host Configuration Protocol*) na mrežu što je opcija koja na primer ne postoji kod Ubuntu OS-a, gde je potrebno statički uneti adresu.



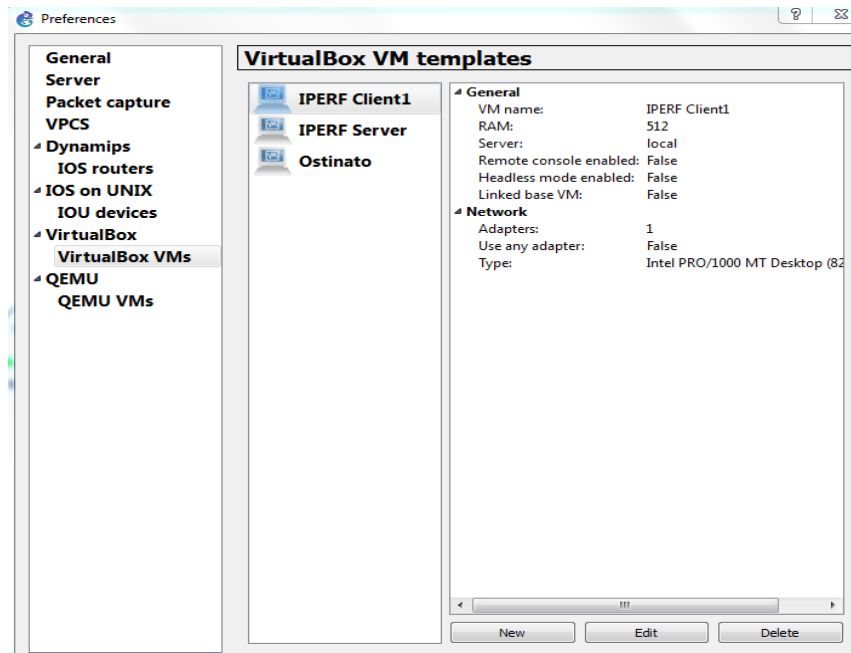
Slika 3.2.2. Instalacija operativnog sistema na virtuelnoj mašini

Zatim je potrebno nakon instalacije Windows operativnog sistema na samoj mašini instalirati IPERF alat koji se može naći na sledećem sajtu: <https://iperf.fr/iperf-download.php>

Postoji GUI (*Graphical User Interface*) za IPERF i zove se jperf. Command shell ostaje i dalje preferirana metoda upotrebe.

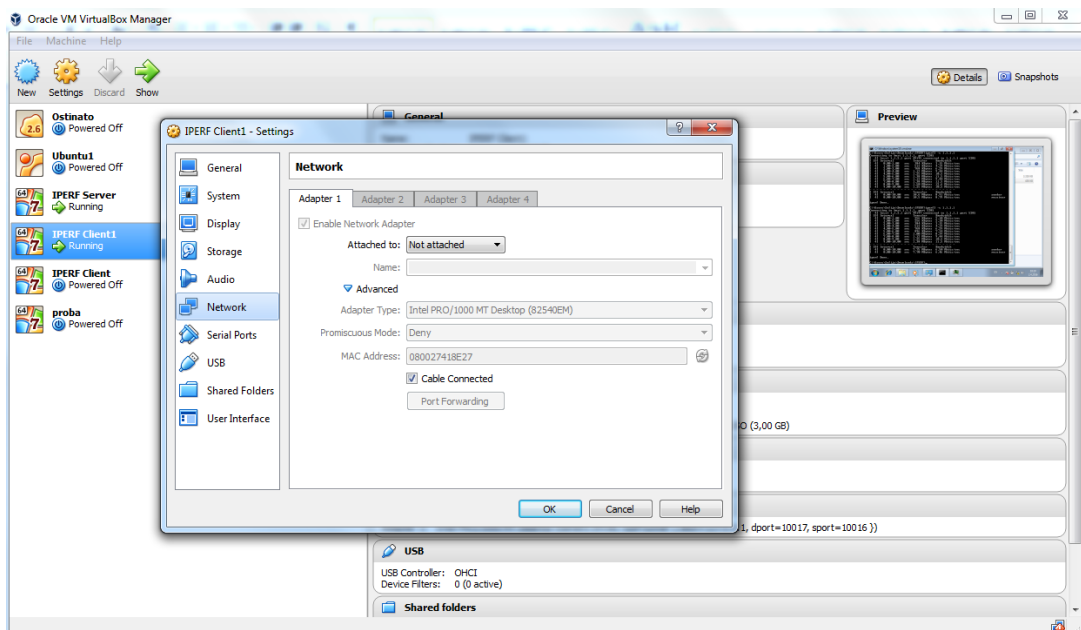
Potom je potrebno instalirati IPERF kao i zapamtiti folder u kojem se aplikacija trenutno nalazi. Preporuka je da taj IPERF folder ostane u folderu **Downloads**. Potrebno je kreirati dve virtuelne mašine IPERFClient i IPERFServer.

Dalje je potrebno povezati te dve virtuelne mašine sa ruterima u GNS3. To se radi i u VirtualBox-u i u GNS3. Kako je na slici 3.2.3. prikazano, potrebno je u okviru GNS3 u opciji Edit → Preferences → VirtualBox → Add, dodati nove virtuelne mašine.



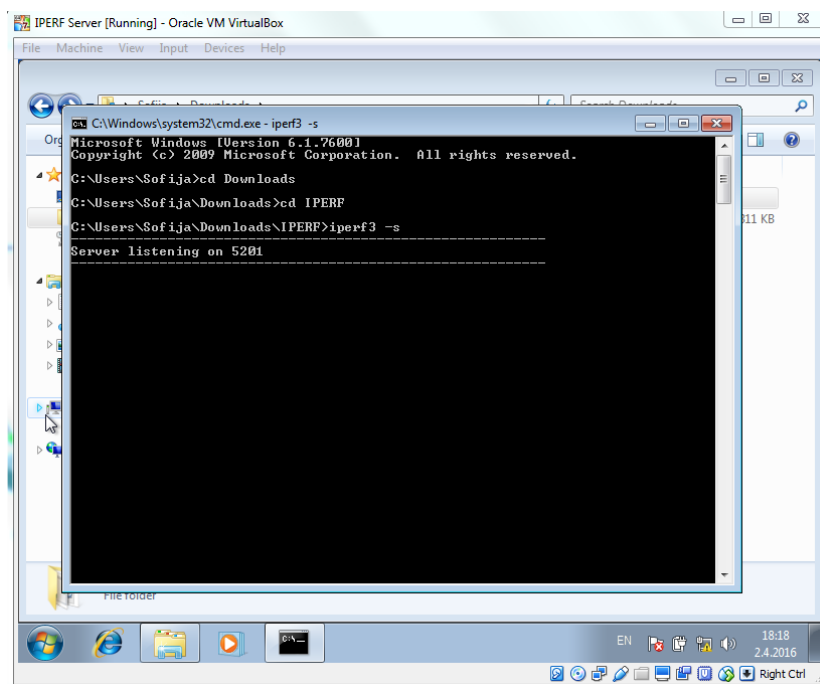
Slika 3.2.3. Dodavanje novih virtuelnih mašina kroz GNS3

U okviru VirtualBox-a potrebno je u opciji **Settings** na svakoj od mašina naći karticu **Network**, i izabrati **Not Attached**, kako je to urađeno na slici 3.2.4. Na taj način podešeno je da mrežna kartica tih virtuelnih mašina ne izabere kao izlaz na mrežu mrežu stvarnog računara odnosno zaista izađe na Internet, ukoliko postoji mogućnost za to. Takođe, GNS3 ne može da pristupi ovim mašinama bez uključivanja te opcije.



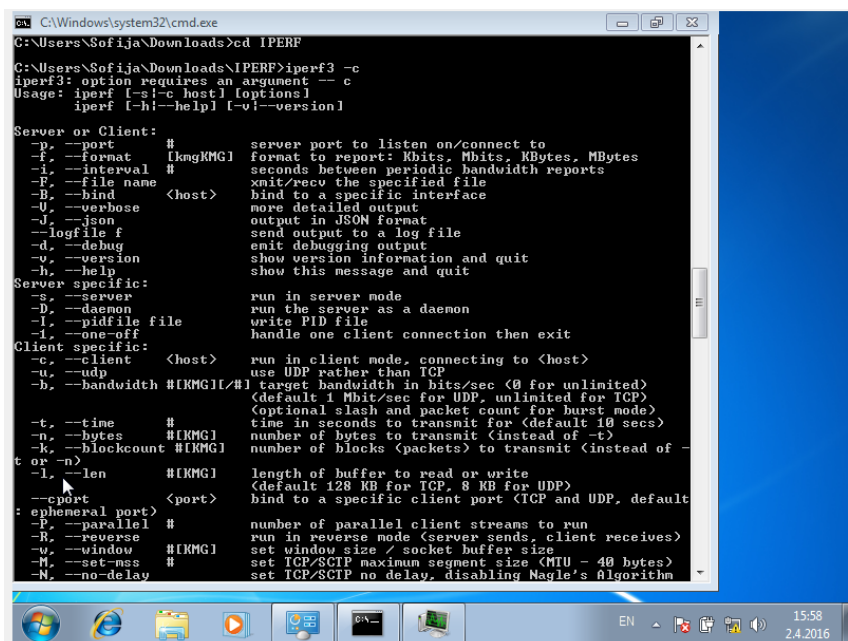
Slika 3.2.4. Podešavanje mrežnih kartica virtuelnih mašina

Zatim su u okviru GNS3 dodate End Devices IPERF Client i IPERF Server, povezane su na interfejsse postojećih PE rutera, ostvarena je IP povezanost kroz mrežu između uređaja i IPERF alat je spreman za korišćenje [8].



Slika 3.2.5. Pristupanje IPERF-u kroz command shell

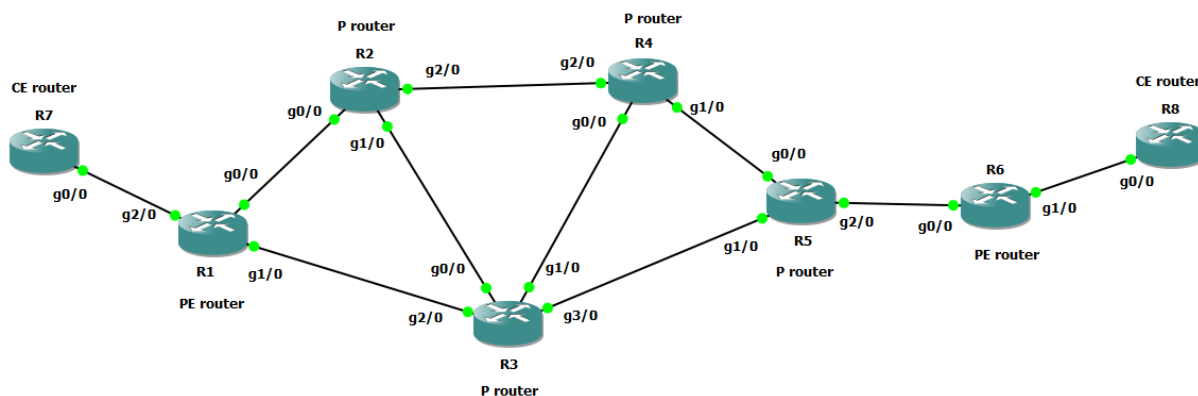
Sa slike 3.2.5. vidimo način za pristupanje serveru i klijentu kroz command shell prozor.



Slika 3.2.6. Opcije koje IPERF alat nudi

Na slici 3.2.6. su izlistane opcije koje IPERF alat nudi, poput protokola, intervala, paralelnih tokova podataka itd.

4. KONFIGURACIJA MREŽE



Slika 4.1. Postojeća topologija mreže

Cilj testiranja je ustanoviti iskorišćenost kapaciteta na linkovima između P-P i P-PE rutera MPLS mreže. Za te potrebe je kreirana mreža na način koji je opisan u četvrtom i petom poglavlju. Topologija je prikazana na slici 4.1.

Potrebno je konfigurirati sve interfejsne međusobno povezanih rutera, i za te potrebe korišćene su adrese u opsegu 10.10.10.0/24. Za *loopback* adrese rutera uzete su adrese iz opsega 217.65.197.0/24. Interfejsi na Cisco ruterima su po osnovnim podešavanjima isključeni pa ih je potrebno manuelno uključiti. Opcija *autonegotiation* služi da se izvrše pregovori o parametrima na linku između dva rutera, poput brzine i činjenice da li će se slati u celom vremenskom intervalu ili samo polovinom intervala. Ukoliko se podaci šalju jednom polovinom vremenskog intervala, drugom polovinom podaci se samo primaju.

Za potrebe virtuelne mreže potrebno je uključiti i dinamički protokol rutiranja, kako bi ruteri razmenili rute i uspostavila se IP povezanost između njih. U te svrhe će biti uključen OSPF protokol. Na željenim interfejsima potrebno je uneti OSPF cene, na taj način će se napraviti razlika između ruta koje se propagiraju kroz mrežu. Konfiguracije rutera R7 i R8 nisu navedene u ovom delu poglavlja i biće objašnjene kasnije kroz rad, kad bude reči o konfiguraciji L3VPN-a.

Ruter R1 najpre je konfigurisan sa komandom kojom mu je zadato ime, R1. Zatim je sledećom naredbom kreiran interfejs *loopback*, kojem je pridružena adresa 217.65.197.28/32. *Loopback* interfejs je uvek u podignutom stanju dokle god ruter radi, za razliku od fizičkih interfejsa. Potom su konfigurisani gigabitni interfejsi sa određenim adresama, i uključeni su. Na

jednom od interfejsa podešena je veća OSPF cena od podrazumevane, koja iznosi 1, kako je u ranijim poglavljima već objašnjeno. To je urađeno kako bi ruta koja ide kroz taj interfejs imala veću cenu od ostalih, i time bila manje poželjna za slanje saobraćaja. Zatim je sačuvana konfiguracija u memoriji rutera poslednjom komandom (*copy running-config startup-config*). Ruteri R2 do R6 konfigurisani su po sličnom principu.

4.1. Konfiguracija interfejsa

Konfiguracija R1

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface loopback0
R1(config-if)# ip address 217.65.197.28 255.255.255.255
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip ospf cost 100
R1(config-if)# negotiation auto
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# interface GigabitEthernet1/0
R1(config-if)# ip ospf cost 200
R1(config-if)# negotiation auto
R1(config-if)# ip address 10.10.10.5 255.255.255.252
R1(config-if)# no shutdown
R1(config)# end
R1# copy running-config startup-config
```

Konfiguracija R2

```
Router# configure terminal
Router(config)# hostname R2
R2(config)# interface loopback0
R2(config-if)# ip address 217.65.197.29 255.255.255.255
R2(config)# interface GigabitEthernet0/0
R2(config-if)# negotiation auto
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# interface GigabitEthernet1/0
R2(config-if)# ip ospf cost 200
R2(config-if)# negotiation auto
R2(config-if)# ip address 10.10.10.10 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# interface GigabitEthernet2/0
R2(config-if)# ip ospf cost 50
R2(config-if)# negotiation auto
R2(config-if)# ip address 10.10.10.13 255.255.255.252
R2(config-if)# no shutdown
R2(config)# end
```


R2# copy running-config startup-config

Konfiguracija R3

```
Router# configure terminal
Router(config)# hostname R3
R3(config)# interface loopback0
R3(config-if)# ip address 217.65.197.32 255.255.255.255
R3(config)# interface GigabitEthernet0/0
R3(config-if)# negotiation auto
R3(config-if)# ip ospf cost 200
R3(config-if)# ip address 10.10.10.9 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet1/0
R3(config-if)# ip ospf cost 200
R3(config-if)# negotiation auto
R3(config-if)# ip address 10.10.10.17 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet2/0
R3(config-if)# ip ospf cost 200
R3(config-if)# negotiation auto
R3(config-if)# ip address 10.10.10.6 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet3/0
R3(config-if)# ip ospf cost 200
R3(config-if)# negotiation auto
R3(config-if)# ip address 10.10.10.26 255.255.255.252
R3(config-if)# no shutdown
R3(config)# end
R3# copy running-config startup-config
```

Konfiguracija R4

```
Router# configure terminal
Router(config)# hostname R4
R4(config)# interface loopback0
R4(config-if)# ip address 217.65.197.33 255.255.255.255
R4(config)# interface GigabitEthernet0/0
R4(config-if)# negotiation auto
R4(config-if)# ip address 10.10.10.18 255.255.255.252
R4(config-if)# no shutdown
R4(config-if)# interface GigabitEthernet1/0
R4(config-if)# ip ospf cost 100
R4(config-if)# negotiation auto
R4(config-if)# ip address 10.10.10.22 255.255.255.252
R4(config-if)# no shutdown
R4(config-if)# interface GigabitEthernet2/0
R4(config-if)# negotiation auto
R4(config-if)# ip address 10.10.10.14 255.255.255.252
R4(config-if)# no shutdown
```

```
R4(config)# end
R4# copy running-config startup-config
```

Konfiguracija R5

```
Router# configure terminal
Router(config)# hostname R5
R5(config)# interface loopback0
R5(config-if)# ip address 217.65.197.34 255.255.255.255
R5(config)# interface GigabitEthernet0/0
R5(config-if)# negotiation auto
R5(config-if)# ip address 10.10.10.21 255.255.255.252
R5(config-if)# no shutdown
R5(config-if)# interface GigabitEthernet1/0
R5(config-if)# negotiation auto
R5(config-if)# ip address 10.10.10.25 255.255.255.252
R5(config-if)# no shutdown
R5(config-if)# interface GigabitEthernet2/0
R5(config-if)# negotiation auto
R5(config-if)# ip address 10.10.10.29 255.255.255.252
R5(config-if)# no shutdown
R5(config)# end
R5# copy running-config startup-config
```

Konfiguracija R6

```
Router# configure terminal
Router(config)# hostname R6
R6(config)# interface loopback0
R6(config-if)# ip address 217.65.197.35 255.255.255.255
R6(config)# interface GigabitEthernet0/0
R6(config-if)# negotiation auto
R6(config-if)# ip address 10.10.10.30 255.255.255.252
R6(config-if)# no shutdown
R6(config)# end
R6# copy running-config startup-config
```

Ruteri R7 i R8 zamišljeni su kao CE odnosno *Customer Edge* ruteri. Ruteri R1 i R6 su PE ruteri tj. PE, dok su svi ostali P ruteri u okviru ove MPLS mreže. Kao unutrašnji (*interior*) protokol rutiranja uzet je OSPF, o kome je ranije bilo reči.

Kako je trenutna mreža prilično jednostavna nema potrebe za više oblasti od okosnice mreže, odnosno area 0.

Pre uključenja OSPF procesa postojale su samo adrese na interfejsima povezanih rutera uz *loopback* adrese. Adrese u istoj podmreži se mogu međusobno pingovati, kao što je prikazano na slici 4.1.1., međutim druge podmreže se ne mogu međusobno pingovati [9].

```

R5#ping 10.10.10.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#ping 10.10.10.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/44/52 ms

```

Slika 4.1.1. Ping ka direktno povezanim interfejsima

4.2. Konfiguracija OSPF-a

Kako bi se uključio OSPF proces na ruteru R1, neophodno je navesti *router-id* OSPF procesa, na taj način se ruteri identifikuju u mreži. Kao najjednostavnije rešenje, uzete su adrese *loopback* interfejsa svakog od rutera. Zatim su naredbom *network* objavljeni adresni opsezi kroz OSPF, koji su dodeljeni interfejsima na ruteru R1. Takođe je objavljena i adresa *loopback* interfejsa drugim OSPF susedima. Za svaku od objavljenih mreža naglašen je *area 0* kao onaj kome pripada taj opseg. Ruteri R2 do R6 konfigurisani su po sličnom principu.

Konfiguracija R1

```

R1(config)# router ospf 1
R1(config-router)# router-id 217.65.197.78
R1(config-router)# network 10.10.10.0 0.0.0.3 area 0
R1(config-router)# network 10.10.10.4 0.0.0.3 area 0
R1(config-router)# network 217.65.197.28 0.0.0.0 area 0

```

Konfiguracija R2

```

R2(config)# router ospf 1
R2(config-router)# router-id 217.65.197.29
R2(config-router)# network 10.10.10.0 0.0.0.3 area 0
R2(config-router)# network 10.10.10.8 0.0.0.3 area 0
R2(config-router)# network 10.10.10.12 0.0.0.3 area 0
R2(config-router)# network 217.65.197.29 0.0.0.0 area 0

```

Konfiguracija R3

```

R3(config)# router ospf 1
R3(config-router)# router-id 217.65.197.32
R3(config-router)# network 10.10.10.4 0.0.0.3 area 0
R3(config-router)# network 10.10.10.8 0.0.0.3 area 0
R3(config-router)# network 10.10.10.16 0.0.0.3 area 0
R3(config-router)# network 10.10.10.24 0.0.0.3 area 0
R3(config-router)# network 217.65.197.32 0.0.0.0 area 0

```

Konfiguracija R4

```
R4(config)# router ospf 1
R4(config-router)# router-id 217.65.197.33
R4(config-router)# network 10.10.10.12 0.0.0.3 area 0
R4(config-router)# network 10.10.10.16 0.0.0.3 area 0
R4(config-router)# network 10.10.10.20 0.0.0.3 area 0
R4(config-router)# network 217.65.197.33 0.0.0.0 area 0
```

Konfiguracija R5

```
R5(config)# router ospf 1
R5(config-router)# router-id 217.65.197.34
R5(config-router)# network 10.10.10.20 0.0.0.3 area 0
R5(config-router)# network 10.10.10.24 0.0.0.3 area 0
R5(config-router)# network 10.10.10.28 0.0.0.3 area 0
R5(config-router)# network 217.65.197.34 0.0.0.0 area 0
```

Konfiguracija R6

```
R6(config)# router ospf 1
R6(config-router)# router-id 217.65.197.72
R6(config-router)# network 10.10.10.28 0.0.0.3 area 0
R6(config-router)# network 217.65.197.35 0.0.0.0 area 0
```

Formiranje cena na linkovima, zamišljeno je tako da ruta R1-R2-R4-R5 bude najbolja IGP ruta u smislu metrike. Formula za OSPF cenu je:

$$\text{Interface Cost} = \text{Reference bandwidth} / \text{interface bandwidth}.$$

Postoji više načina za dodeljivanje cena interfejsima. Jedan je postavljanje *auto-cost reference-bandwidth* komande koja dozvoljava da se promeni referentna vrednost protoka koju OSPF koristi da izračuna svoju metriku. Drugi način je primena komande *ip ospf cost* direktno na interfejsima rutera.

```

R1#sh ip route ospf 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O       10.10.10.8/30 [110/300] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       10.10.10.12/30 [110/150] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       10.10.10.16/30 [110/151] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       10.10.10.20/30 [110/250] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       10.10.10.24/30 [110/251] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       10.10.10.28/30 [110/251] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
217.65.197.0/32 is subnetted, 8 subnets
O       217.65.197.29 [110/101] via 10.10.10.2, 00:00:26, GigabitEthernet0/0
O       217.65.197.32 [110/152] via 10.10.10.2, 00:00:27, GigabitEthernet0/0
O       217.65.197.33 [110/151] via 10.10.10.2, 00:00:27, GigabitEthernet0/0
O       217.65.197.34 [110/251] via 10.10.10.2, 00:00:27, GigabitEthernet0/0
O       217.65.197.35 [110/252] via 10.10.10.2, 00:00:27, GigabitEthernet0/0
O       217.65.197.72 [110/252] via 10.10.10.2, 00:00:27, GigabitEthernet0/0
R1# █

```

Slika 4.2.1. Tabela usmeravanja OSPF protokola

U tabeli usmeravanja prikazanoj na slici 4.2.1. vide se rute naučene putem OSPF protokola, čija je administrativna cena 110, kao i izlazni interfejsi na ruteru za svaku od tih mreža. U ovom slučaju je to za svaku mrežu na ruteru R1, GigabitEthernet 0/0, što predstavlja najbolju IGP rutu na osnovu metrike. To se primećuje iz cena za svaku od mreža, gde su cene prikazane kao druga vrednost u uglastim zagradama, odmah nakon administrativne. Najbolje rute su one sa najmanjom cenom [9].

4.3. Uspostavljanje MPLS-a

Nakon što je postignuta IP povezanost između rutera u mreži, sledeći korak je uspostavljanje MPLS mreže na postojećoj mreži. Neophodno je uspostaviti LDP protokol, kako bi se vršila razmena labela. Objavljivanje labela se uvek vrši u uzvodnom smeru, bez obzira da li postoji zahtev ili ne. To se postiže unosom komandi na ruterima u globalnom konfiguracionom režimu rada. Kao na primeru rutera R1, potrebno je na nivou celog rutera omogućiti MPLS tehnologiju komandom *mpls ip*. Zatim u istom režimu rada uneti opseg labela koje će biti dodeljivane od strane tog rutera za odgovarajuće FEC. Ograničen je opseg labela za svaki ruter u mreži na maksimalnih 50 jer više od toga nije potrebno za simulaciju u ovom radu. Naposletku je potrebno na interfejsima, između P-P kao i P-PE rutera, omogućiti MPLS LDP tehnologiju, što se postiže istom komandom kao u globalnom režimu rada. Svi ruteri konfigurisani su po sličnom principu kao R1.

Konfiguracija R1

```
R1(config)# mpls ip
R1(config)# mpls label range 100 199
R1(config)# interface GigabitEthernet0/0
R1(config-if)# mpls ip
R1(config)# interface GigabitEthernet1/0
R1(config-if)# mpls ip
```

Konfiguracija R2

```
R2(config)# mpls ip
R2(config)# mpls label range 200 250
R2(config)# interface GigabitEthernet0/0
R2(config-if)# mpls ip
R2(config)# interface GigabitEthernet1/0
R2(config-if)# mpls ip
R2(config)# interface GigabitEthernet2/0
R2(config-if)# mpls ip
```

Konfiguracija R3

```
R3(config)# mpls ip
R3(config)# mpls label range 300 350
R3(config)# interface GigabitEthernet0/0
R3(config-if)# mpls ip
R3(config)# interface GigabitEthernet1/0
R3(config-if)# mpls ip
R3(config)# interface GigabitEthernet2/0
R3(config-if)# mpls ip
R3(config)# interface GigabitEthernet3/0
R3(config-if)# mpls ip
```

Konfiguracija R4

```
R4(config)# mpls ip
R4(config)# mpls label range 400 450
R4(config)# interface GigabitEthernet0/0
R4(config-if)# mpls ip
R4(config)# interface GigabitEthernet1/0
R4(config-if)# mpls ip
R4(config)# interface GigabitEthernet2/0
R4(config-if)# mpls ip
```

Konfiguracija R5

```
R5(config)# mpls ip
R5(config)# mpls label range 500 550
R5(config)# interface GigabitEthernet0/0
R5(config-if)# mpls ip
R5(config)# interface GigabitEthernet1/0
R5(config-if)# mpls ip
R5(config)# interface GigabitEthernet2/0
```

```
R5(config-if)# mpls ip
```

Konfiguracija R6

```
R6(config)# mpls ip
```

```
R6(config)# mpls label range 600 650
```

```
R6(config)# interface GigabitEthernet0/0
```

```
R6(config-if)# mpls ip
```

```
R3#sh mpls ldp neighbor
Peer LDP Ident: 217.65.197.33:0; Local LDP Ident 217.65.197.32:0
TCP connection: 217.65.197.33.16284 - 217.65.197.32.646
State: Oper; Msgs sent/rcvd: 157/156; Downstream
Up time: 02:00:59
LDP discovery sources:
  GigabitEthernet1/0, Src IP addr: 10.10.10.18
Addresses bound to peer LDP Ident:
  10.10.10.18      217.65.197.33      10.10.10.22      10.10.10.14
Peer LDP Ident: 217.65.197.34:0; Local LDP Ident 217.65.197.32:0
TCP connection: 217.65.197.34.31119 - 217.65.197.32.646
State: Oper; Msgs sent/rcvd: 157/157; Downstream
Up time: 02:00:59
LDP discovery sources:
  GigabitEthernet3/0, Src IP addr: 10.10.10.25
Addresses bound to peer LDP Ident:
  10.10.10.21      217.65.197.34      10.10.10.25      10.10.10.29
Peer LDP Ident: 217.65.197.29:0; Local LDP Ident 217.65.197.32:0
TCP connection: 217.65.197.29.646 - 217.65.197.32.12688
State: Oper; Msgs sent/rcvd: 156/155; Downstream
Up time: 02:00:55
LDP discovery sources:
  GigabitEthernet0/0, Src IP addr: 10.10.10.10
Addresses bound to peer LDP Ident:
  10.10.10.2      217.65.197.29      10.10.10.10      10.10.10.13
Peer LDP Ident: 217.65.197.28:0; Local LDP Ident 217.65.197.32:0
TCP connection: 217.65.197.28.646 - 217.65.197.32.36778
State: Oper; Msgs sent/rcvd: 146/148; Downstream
Up time: 01:52:05
LDP discovery sources:
  GigabitEthernet2/0, Src IP addr: 10.10.10.5
Addresses bound to peer LDP Ident:
  10.10.10.1      217.65.197.28      10.10.10.5      217.65.197.78
R3#
```

Slika 4.3.1. LDP susedi rutera R3

Na slici 4.3.1. dat je prikaz LDP susedstva koje je ruter R3 uspostavio nakon unosa pomenutih komandi. Tu su navedene *loopback* adrese rutera R1, R2, R4 i R5 kao identifikacije za ova susedstva. Takođe se mogu videti adrese, objavljene OSPF procesom, za određene susede, što je dato poslednjim ispisanim redom za svakog od njih.

Kad paket stigne do određenog rutera, on gleda informacije sloja 2, i iz odredišne MAC adrese tog paketa dobija informaciju da je paket namenjen njemu. U okviru svoje *label forwarding* tabele ima zapis da, ukoliko dobije paket sa specifičnom labelom treba da izvrši zamenu te labele drugom labelom. Ruter prilikom zamene labele, neće pogledati informaciju sa sloja 3. Samim tim, MPLS je odlična tehnologija za prenos IPv6 preko IPv4 mreže.

U slučaju da u *label forwarding* tabeli P rutera čiji je nizvodni ruter PE ruter, stoji *implicit-null*, kao u primeru sa slike 4.3.2., to znači da je labela rezervisana. Ona predstavlja labelu koju će ruter dodeliti za lokalno povezanu mrežu na P ruteru. R2 je primio tu labelu od R1, što za njega znači da je R1 direktno povezan sa tom mrežom, i kako bi uštedeo vreme koje će R1 provesti ispitujući MPLS zaglavlje umesto samo IP deo paketa, R2 uradi *penultimate hop popping*.

```
R2#sh mpls ldp bindings 217.65.197.28 ?
<0-32> Mask length
A.B.C.D Destination mask

R2#sh mpls ldp bindings 217.65.197.28 32
lib entry: 217.65.197.28/32, rev 14
  local binding: label: 203
  remote binding: lsr: 217.65.197.28:0, label: imp-null
  remote binding: lsr: 217.65.197.32:0, label: 303
  remote binding: lsr: 217.65.197.33:0, label: 403
R2#
```

Slika 4.3.2. Prikaz primera dodeljivanja labela

Na slici 4.3.3. je prikazan put od rutera R4 do R1, i labele koje su dodeljivane. U slučaju da mu je izlazni interfejs ka toj mreži Gi2/0, dodeljuje paketu labelu 208 i usmerava je ka ruteru R2. Postoji i druga ruta ka R3, gde dodeljuje labelu 311 za tu mrežu. Lokalna labela na ruteru R4 za tu mrežu je u ovom slučaju 405. Kad ima izbor između više dodeljenih labela za istu mrežu, odluku će doneti na osnovu najbolje rute u svojoj IP tabeli usmeravanja.

```
R4#sh mpls forwarding-table 217.65.197.28
Local   Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label   Label     or Tunnel Id    Switched     interface
405     208       217.65.197.28/32 0             Gi2/0      10.10.10.13
        311       217.65.197.28/32 0             Gi0/0      10.10.10.17
R4#
```

Slika 4.3.3. Primer MPLS forwarding tabele

Za primer je korišćen Wireshark softverski paket, za snimanje paketa uspostave LDP susedstva, kao što je prikazano na slici 4.3.4. Ono što se vidi na pomenutoj slici je *Hello* poruka čije je izvoriste 10.10.10.1, odnosno adresa fizičkog interfejsa na ruteru R1, ka multikast adresi za sve rutere 224.0.0.2. Na sloju 4 koristi se UDP protokol, gde su izvorišni i odredišni portovi 646. Unutar LDP Hello poruke nalazi se LSR ID, 217.65.197.28. LSP put će se uspostaviti preko *loopback* adresa (transportnih), umesto fizičkih.


```

⊞ Frame 55: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
⊞ Ethernet II, Src: ca:01:09:64:00:08 (ca:01:09:64:00:08), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
  ⊞ Destination: IPv4mcast_02 (01:00:5e:00:00:02)
  ⊞ Source: ca:01:09:64:00:08 (ca:01:09:64:00:08)
  Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 224.0.0.2 (224.0.0.2)
⊞ User Datagram Protocol, Src Port: 646 (646), Dst Port: 646 (646)
⊞ Label Distribution Protocol
  Version: 1
  PDU Length: 30
  LSR ID: 217.65.197.28 (217.65.197.28)
  Label Space ID: 0
⊞ Hello Message
  0... .... = 0 bit: Unknown bit not set

```

Slika 4.3.4. Uspostava LDP susedstva

67	78.8930000	10.10.10.25	224.0.0.5	OSPF	94	Hello Packet
68	79.3030000	10.10.10.26	224.0.0.2	LDP	76	Hello Message
69	79.4730000	217.65.197.34	217.65.197.32	LDP	72	Keep Alive Message
70	79.7140000	217.65.197.32	217.65.197.34	TCP	60	646-47214 [ACK] Seq=19 Ack=37 Win=3840 Len=0
71	79.9650000	10.10.10.25	224.0.0.2	LDP	76	Hello Message
72	80.5250000	ca:03:1e:60:00:54	ca:03:1e:60:00:54	LOOP	60	Reply
73	83.3830000	217.65.197.34	217.65.197.32	RSVP	222	PATH Message. SESSION: IPv4-LSP, Destination 217.65.197.32, Tunnel ID 1, E
74	84.2010000	10.10.10.26	224.0.0.5	OSPF	94	Hello Packet
75	84.5710000	10.10.10.26	224.0.0.2	LDP	76	Hello Message
76	85.2910000	10.10.10.25	224.0.0.2	LDP	76	Hello Message

```

⊞ Frame 70: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: ca:03:1e:60:00:54 (ca:03:1e:60:00:54), Dst: ca:05:17:78:00:1c (ca:05:17:78:00:1c)
  ⊞ Destination: ca:05:17:78:00:1c (ca:05:17:78:00:1c)
  ⊞ Source: ca:03:1e:60:00:54 (ca:03:1e:60:00:54)
  Type: IP (0x0800)
  Padding: 000000000000
⊞ Internet Protocol Version 4, Src: 217.65.197.32 (217.65.197.32), Dst: 217.65.197.34 (217.65.197.34)
  Version: 4
  Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class selector 6; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
  Total Length: 40
  Identification: 0x238e (9102)
  ⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: TCP (6)

```

Slika 4.3.5. Razmena poruka između aktivnog i pasivnog LDP rutera

Na slici 4.3.5 je prikazana TCP poruka, gde ruter sa najvećim *router-id*-em postaje aktivni LDP ruter, dok drugi postaje pasivni. U ovom slučaju aktivni je onaj sa adresom 217.65.197.34, a pasivni sa 217.65.197.32. Prva poruka koju aktivni ruter prosledi je SYN, pasivni na to odgovara SYN,ACK porukom, i na kraju aktivni šalje *Keep Alive* poruku, i zatim ta dva rutera razmenjuju labele za svoje IP prefikse.

Ovde se može primetiti poruka SYN,ACK gde je adresa izvorišta zaista ona sa manjim *router-id*-em. To je ujedno i adresa odredišta *Keep Alive* poruke [9].

4.4. Uspostavljanje MPBGP-a

MPLS LDP protokol služi za razmenu transportnih labela, ali nije dovoljan prilikom razdvajanja saobraćaja prema servisima. Zato je neophodan MPBGP, koji se uspostavlja između PE rutera. Ovaj protokol se koristi za razmenu servisnih labela kojima se razlikuju servisi. Kako postojeća mreža nema više od dva PE rutera konfiguracija je jednostavna. U pitanju je interna bgp sesija jer se oba rutera nalaze u istom AS-u. Na ruteru R1 kreiran je bgp proces, u okviru kog je

naglašeno da mu je bgp sused ruter R6 sa *loopback* adresom 217.65.197.35, i da se nalaze u istom AS-u 65536. Zatim je kao izvoriste ove sesije naznačena *loopback* adresa rutera R1. Nakon što je bgp process aktiviran on (sa osnovnim podešavanjima) podržava ipv4 adresnu familiju. U postojećoj mreži nije od interesa ipv4 adresna familija već oglašavanje vpnv4 ruta, pa je iz tog razloga urađena deaktivacija bgp suseda u okviru ipv4 adresne familije. U okviru konfiguracije za vpnv4 aktiviran je sused R6, i objavljeni su *community* atributi, koji su *route targeti* o kojima će biti više reči kasnije. Na taj način kontrolisano je gde su vpnv4 rute oglašene. Ruter R6 konfigurisan je po sličnom principu.

Konfiguracija R1

```
R1(config)# router bgp 65536
R1(config-router)# neighbor 217.65.197.35 remote-as 65536
R1(config-router)# neighbor 217.65.197.35 update-source Loopback0
R1(config-router)# address-family ipv4
R1(config-router-af)# no neighbor 217.65.197.35 activate
R1(config-router)# address-family vpnv4
R1(config-router-af)# neighbor 217.65.197.35 activate
R1(config-router-af)# neighbor 217.65.197.35 send-community both
```

Konfiguracija R6

```
R6(config)# router bgp 65536
R6(config-router)# neighbor 217.65.197.28 remote-as 65536
R6(config-router)# neighbor 217.65.197.28 update-source Loopback0
R6(config-router)# address-family ipv4
R6(config-router-af)# no neighbor 217.65.197.28 activate
R6(config-router)# address-family vpnv4
R6(config-router-af)# neighbor 217.65.197.28 activate
R6(config-router-af)# neighbor 217.65.197.28 send-community both
```

Biće izvršena provera uspostave bgp vpnv4 susedstva, kao što je prikazano na slici 4.4.1.

```
R1#sh ip bgp vpnv4 all neighbors | section capabilities
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family VPNv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
```

Slika 4.4.1. Provera uspostave MPBGP-a

4.5. Kreiranje L3VPN-a

U ovom delu rada biće kreiran vrf po imenu korisnik_1. Potreba za L3VPN-om korisnik_1 postoji u smislu neophodnih kapaciteta kroz mrežu koje treba obezbediti za korisnika. PE ruter može imati više vrf-ova, ali ima jednu bgp tabelu usmeravanja. Kad se ruta objavi u bgp iz vrf-a, *route distinguisher* je asociran sa tom rutom, čineći je jedinstvenom u okviru cele bgp tabele usmeravanja.

Neophodno je na R1 i R6 kreirati ovaj vrf sa istim nazivom na oba ruteru. Mora se voditi računa i da *route-target export* na ruteru R1 bude ista vrednost kao *route-target import* na R6, i obrnuto, gde se parovi tih vrednosti mogu razlikovati. Na taj način je postignuto da rute iz tog vrf-a koje objavi R1 prihvati njegov bgp sused R6 i obrnuto. Uz *route-target-e* potreban je i *route distinguisher*. Potom je potrebno konfigurisati interfejs ruteru R1 i R6 na koje dolazi ovaj korisnik. Od konfiguracija je promenjen naziv interfejsa na ruteru, i data je proizvoljna hardverska adresa. Zatim je interfejs pridružen vrf-u korisnik_1, i dodeljena ip adresa, koja nakon pridruživanja interfejsa vrf-u više nije ipv4 već vpnv4. Kako bi te rute bile oglašene kroz bgp njegovom susedu R6, u bgp procesu je potrebno aktivirati adresnu familiju za ipv4 vrf korisnik_1 i kroz nju objaviti direktno povezane rute. Po sličnom principu konfigurisan je ruter R6.

Zatim su prikazane konfiguracije ruteru R7 i R8. U pitanju su CE ruteri. Zadate su im adrese *loopback* interfejsa, iz istog razloga kao i za ostale rutere. Interfejsi ka ruterima R1 odnosno R6, konfigurisani su sa ip adresom i podignuti. Naposletku je dodata ruta na R7 za mrežu na ruteru R8 gde je kao gejtvej stavljena adresa konfigurisana na ruteru R1. To je urađeno kako bi ruter R7 znao odredište kad ima pakete za slanje ka mreži na R8. Slična konfiguracija je i na ruteru R8, sa rutom ka mreži ruteru R7. Na ruterima R1 i R6 nema potrebe za rutom jer su to direktno povezane mreže [9].

Konfiguracija R1

```
R1(config)# ip vrf korisnik_1
R1(config-vrf)# rd 1.1.1.1:1
R1(config-vrf)# route-target export 1.1.1.1:101
R1(config-vrf)# route-target import 6.6.6.6:101
R1(config)# interface GigabitEthernet2/0
R1(config-if)# description access_korisnika_1
R1(config-if)# mac-address 0000.1111.1111
R1(config-if)# ip vrf forwarding korisnik_1
R1(config-if)# ip address 172.16.1.1 255.255.255.252
R1(config-if)# negotiation auto
R1(config)# router bgp 65536
R1(config-router)# address-family ipv4 vrf korisnik_1
R1(config-router-af)# redistribute connected
```

Konfiguracija R6

```
R6(config)# ip vrf korisnik_1
R6(config-vrf)# rd 1.1.1.1:1
R6(config-vrf)# route-target export 6.6.6.6:101
R6(config-vrf)# route-target import 1.1.1.1:101
R6(config)# interface GigabitEthernet1/0
R6(config-if)# description access_korisnika_1
```

```
R6(config-if)# mac-address 0000.6666.6666
R6(config-if)# ip vrf forwarding korisnik_1
R6(config-if)# ip address 192.168.1.1 255.255.255.252
R6(config-if)# negotiation auto
R6(config)# router bgp 65536
R6(config-router)# address-family ipv4 vrf korisnik_1
R6(config-router-af)# redistribute connected
```

Konfiguracija R7

```
R7(config)# interface loopback0
R7(config-if)# ip address 172.16.100.2 255.255.255.255
R7(config)# interface GigabitEthernet0/0
R7(config-if)# ip address 172.16.1.2 255.255.255.252
R7(config-if)# negotiation auto
R7(config)# ip route 192.168.1.0 255.255.255.252 172.16.1.1
```

Konfiguracija R8

```
R8(config)# interface loopback0
R8(config-if)# ip address 192.168.100.1 255.255.255.255
R8(config)# interface GigabitEthernet0/0
R8(config-if)# ip address 192.168.1.2 255.255.255.252
R8(config-if)# negotiation auto
R8(config)# ip route 172.16.1.0 255.255.255.252 192.168.1.1
```

5. SIMULACIJE

Kako bi mreža mogla biti optimizovana, administrator mreže mora navesti saobraćaj drugim putanjama u mreži, ne samo rutom sa najboljom cenom. To se može postići uspostavom MPLS TE tunela. Iz tog razloga neophodno je omogućiti MPLS TE i RSVP protokole duž cele putanje kojom će tuneli ići. RSVP je potreban kako bi se manuelno unele putanje kroz MPLS.

Na ruteru R1 u globalnom konfiguracionom režimu rada omogućeni su MPLS TE i RSVP. Nakon toga kreiran je novi interfejs *loopback1*. Ovaj interfejs biće iskorišćen kao izvoriste svih tunela kreiranih na ruteru R1. U okviru OSPF procesa potrebno je navesti *router-id* identifikaciju rutera u MPLS TE tehnologiji. Izabran je novokreirani *loopback1* u te svrhe. Takođe treba navesti da se MPLS TE aktivira u okviru *area 0* OSPF procesa, i objaviti adresu *loopback* interfejsa svim OSPF susedima. Na samim interfejsima kuda je zamišljeno da idu tuneli, omogućeni su MPLS TE i RSVP. Konfiguracije ostalih rutera urađene su po sličnom principu, s tim što se novi *loopback* interfejsi konfiguriraju samo na ruterima R1 i R6 kao početne tačke tunela. Kod ostalih rutera iskorišćene su postojeće *loopback* adrese. Ovo je urađeno radi male razlike u konfiguracijama, kao i radi provere da li tuneli rade sa drugim *loopback* adresama kao adresama izvorišta.

Konfiguracija R1

```
R1(config)# mpls traffic-eng tunnels
R1(config)# interface Loopback1
R1(config-if)# ip address 217.65.197.78 255.255.255.255
R1(config)# interface GigabitEthernet0/0
R1(config-if)# mpls traffic-eng tunnels
R1(config-if)# ip rsvp bandwidth
R1(config)# interface GigabitEthernet1/0
R1(config-if)# mpls traffic-eng tunnels
R1(config-if)# ip rsvp bandwidth
R1(config)# router ospf 1
R1(config-router)# mpls traffic-eng router-id Loopback1
R1(config-router)# mpls traffic-eng area 0
R1(config-router)# network 217.65.197.78 0.0.0.0 area 0
```

Konfiguracija R2

```
R2(config)# mpls traffic-eng tunnels
R2(config)# interface GigabitEthernet0/0
R2(config-if)# mpls traffic-eng tunnels
R2(config-if)# ip rsvp bandwidth
R2(config)# interface GigabitEthernet1/0
R2(config-if)# mpls traffic-eng tunnels
R2(config-if)# ip rsvp bandwidth
R2(config)# interface GigabitEthernet2/0
R2(config-if)# mpls traffic-eng tunnels
```

```
R2(config-if)# ip rsvp bandwidth
R2(config)# router ospf 1
R2(config-router)# mpls traffic-eng router-id Loopback0
R2(config-router)# mpls traffic-eng area 0
```

Konfiguracija R3

```
R3(config)# mpls traffic-eng tunnels
R3(config)# interface GigabitEthernet0/0
R3(config-if)# mpls traffic-eng tunnels
R3(config-if)# ip rsvp bandwidth
R3(config)# interface GigabitEthernet1/0
R3(config-if)# mpls traffic-eng tunnels
R3(config-if)# ip rsvp bandwidth
R3(config)# interface GigabitEthernet2/0
R3(config-if)# mpls traffic-eng tunnels
R3(config-if)# ip rsvp bandwidth
R3(config)# interface GigabitEthernet3/0
R3(config-if)# mpls traffic-eng tunnels
R3(config-if)# ip rsvp bandwidth
R3(config)# router ospf 1
R3(config-router)# mpls traffic-eng router-id Loopback0
R3(config-router)# mpls traffic-eng area 0
```

Konfiguracija R4

```
R4(config)# mpls traffic-eng tunnels
R4(config)# interface GigabitEthernet0/0
R4(config-if)# mpls traffic-eng tunnels
R4(config-if)# ip rsvp bandwidth
R4(config)# interface GigabitEthernet1/0
R4(config-if)# mpls traffic-eng tunnels
R4(config-if)# ip rsvp bandwidth
R4(config)# interface GigabitEthernet2/0
R4(config-if)# mpls traffic-eng tunnels
R4(config-if)# ip rsvp bandwidth
R4(config)# router ospf 1
R4(config-router)# mpls traffic-eng router-id Loopback0
R4(config-router)# mpls traffic-eng area 0
```

Konfiguracija R5

```
R5(config)# mpls traffic-eng tunnels
R5(config)# interface GigabitEthernet0/0
R5(config-if)# mpls traffic-eng tunnels
R5(config-if)# ip rsvp bandwidth
R5(config)# interface GigabitEthernet1/0
R5(config-if)# mpls traffic-eng tunnels
R5(config-if)# ip rsvp bandwidth
R5(config)# interface GigabitEthernet2/0
R5(config-if)# mpls traffic-eng tunnels
```

```
R5(config-if)# ip rsvp bandwidth
R5(config)# router ospf 1
R5(config-router)# mpls traffic-eng router-id Loopback0
R5(config-router)# mpls traffic-eng area 0
```

Konfiguracija R6

```
R6(config)# mpls traffic-eng tunnels
R6(config)# interface Loopback1
R6(config-if)# ip address 217.65.197.72 255.255.255.255
R6(config)# interface GigabitEthernet0/0
R6(config-if)# mpls traffic-eng tunnels
R6(config-if)# ip rsvp bandwidth
R6(config)# router ospf 1
R6(config-router)# mpls traffic-eng router-id Loopback1
R6(config-router)# mpls traffic-eng area 0
R6(config-router)# network 217.65.197.72 0.0.0.0 area 0
```

5.1. Primarna i sekundarna putanja

Kako bi bila izvršena provera kojom putanjom proizvoljni tunel ide, odnosno da li će se tunel ponovo uspostaviti nakon otkaza jedne od putanja, konfigurisan je sledeći tunel. Na ruteru R1 kreiran je tunel 158 čija je adresa izvorišta njegova *loopback1* adresa interfejsa.

Naglašeno je da je vrsta tunela MPLS TE, zatim je stavljena adresa njegovog odredišta. Ping ne prolazi sve dok se ne unese komanda *tunnel mpls traffic-eng autoroute announce*.

Ukoliko se ne naglasi prioritet tunela vrednost se postavlja na najmanji prioritet 7. Izabere se propusni opseg tunela i rezervišu sredstva tunela RSVP protokolom, gde postoji mogućnost da se celokupan kapacitet nekog linka pridruži odgovarajućem tunelu.

U okviru tunela naglašene su specifične putanje kojima administrator mreže želi da usmeri saobraćaj. Te putanje se međusobno razlikuju preko prioriteta koji su im pridruženi. Potom su u globalnom konfiguracionom režimu rada kreirane odgovarajuće specifične putanje, u kojima su navedeni sledeći hopovi duž cele putanje do samog odredišta.

```
R1(config)# interface Tunnel158
R1(config-if)# ip unnumbered Loopback1
R1(config-if)# tunnel mode mpls traffic-eng
R1(config-if)# tunnel destination 217.65.197.72
R1(config-if)# tunnel mpls traffic-eng autoroute announce
R1(config-if)# tunnel mpls traffic-eng priority 0 0
R1(config-if)# tunnel mpls traffic-eng bandwidth 158
R1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name R3-R4-R5_R6
R1(config-if)# tunnel mpls traffic-eng path-option 2 explicit name R2-R3-R5_R6
R1(config-if)# no routing dynamic
R1(config-if)# ip rsvp bandwidth 500
```

```

R1(config)# ip explicit-path name R2-R3-R5_R6 enable
R1(cfg-ip-expl-path)# next-address 10.10.10.2
R1(cfg-ip-expl-path)# next-address 10.10.10.9
R1(cfg-ip-expl-path)# next-address 10.10.10.25
R1(cfg-ip-expl-path)# next-address 10.10.10.30
R1(config)# ip explicit-path name R3-R4-R5_R6 enable
R1(cfg-ip-expl-path)# next-address 10.10.10.6
R1(cfg-ip-expl-path)# next-address 10.10.10.18
R1(cfg-ip-expl-path)# next-address 10.10.10.21
R1(cfg-ip-expl-path)# next-address 10.10.10.30

```

```

R1#sh mpls traffic-eng tunnels tunnel 158

Name: R1_t158                               (Tunnel158) Destination: 217.65.197.72
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 1, type explicit R3-R4-R5_R6 (Basis for Setup, path weight 501)
  path option 2, type explicit R2-R3-R5_R6

Config Parameters:
  Bandwidth: 158      kbps (Global) Priority: 0 0  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled  LockDown: disabled Loadshare: 158      bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel  : -
OutLabel  : GigabitEthernet1/0, 302
RSVP Signalling Info:
  Src 217.65.197.78, Dst 217.65.197.72, Tun_Id 158, Tun_Instance 262
RSVP Path Info:
  My Address: 10.10.10.5
  Explicit Route: 10.10.10.6 10.10.10.17 10.10.10.18 10.10.10.22
                  10.10.10.21 10.10.10.29 10.10.10.30 217.65.197.72
  Record Route: NONE
  Tspec: ave rate=158 kbits, burst=1000 bytes, peak rate=158 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=158 kbits, burst=1000 bytes, peak rate=158 kbits
Shortest Unconstrained Path Info:
  Path Weight: 251 (TE)
  Explicit Route: 10.10.10.1 10.10.10.2 10.10.10.13 10.10.10.14
                  10.10.10.22 10.10.10.21 10.10.10.29 10.10.10.30
                  217.65.197.72

History:
Tunnel:
  Time since created: 1 hours, 54 minutes
  Time since path change: 16 seconds
  Number of LSP IDs (Tun_Instances) used: 262
Current LSP:
  Uptime: 16 seconds
R1#

```

Slika 5.1.1. Stanje tunel interfejsa

Na slici 5.1.1. se vidi da je tunel 158 uspostavljen uspešno, kao i adresa izvorišta i odredišta. Prikazano je koja mu je aktivna putanja, sa svim adresama interfejsa kroz koje mora proći.

No.	Time	Source	Destination	Protocol	Length	Info
122	85.0245010	217.65.197.78	217.65.197.72	RSVP	254	PATH Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. SENDER TEMPLATE: IPv4-LSP, Tunnel So
123	86.0316020	10.10.10.17	224.0.0.2	LDP	76	Hello Message
124	86.0416030	ca:04:05:cc:00:08	ca:04:05:cc:00:08	LOOP	60	Reply
125	89.1259120	10.10.10.18	224.0.0.2	LDP	76	Hello Message
126	90.1680160	10.10.10.18	224.0.0.5	OSPF	94	Hello Packet
127	90.9110900	10.10.10.17	224.0.0.2	LDP	76	Hello Message
128	90.9210910	217.65.197.32	217.65.197.33	LDP	72	Keep Alive Message
129	91.1251110	217.65.197.33	217.65.197.32	TCP	60	38082-646 [ACK] Seq=37 Ack=37 Win=3804 Len=0
130	92.0192010	ca:03:1e:60:00:1c	ca:03:1e:60:00:1c	LOOP	60	Reply
131	92.7832770	10.10.10.17	224.0.0.5	OSPF	94	Hello Packet
132	93.0583050	10.10.10.18	224.0.0.2	LDP	76	Hello Message
133	93.8363830	217.65.197.29	217.65.197.32	TCP	54	646-38415 [ACK] Seq=37 Ack=37 Win=3804 Len=0
134	94.5444530	10.10.10.18	10.10.10.17	RSVP	142	RESV Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. FILTERSPEC: IPv4-LSP, Tunnel Source:
135	95.2365230	10.10.10.17	224.0.0.2	LDP	76	Hello Message


```

Frame 122: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
Ethernet II, Src: ca:03:1e:60:00:1c (ca:03:1e:60:00:1c), Dst: ca:04:05:cc:00:08 (ca:04:05:cc:00:08)
Internet Protocol Version 4, Src: 217.65.197.78 (217.65.197.78), Dst: 217.65.197.72 (217.65.197.72)
Resource Reservation Protocol (RSVP): PATH Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. SENDER TEMPLATE: IPv4-LSP, Tunnel Source: 217.65.197.78, LSP ID: 279
RSVP Header. PATH Message.
SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e.
HOP: IPv4, 10.10.10.17
TIME VALUES: 30000 ms
EXPLICIT ROUTE: IPv4 10.10.10.18, IPv4 10.10.10.22, IPv4 10.10.10.21, ...
LABEL REQUEST: Basic: LSPID: IP (0x0800)
SESSION ATTRIBUTE: SetupPrIo 0, HoldPrIo 0, SE style, [R1_t158]
SENDER TEMPLATE: IPv4-LSP, Tunnel Source: 217.65.197.78, LSP ID: 279.
SENDER TSPEC: Intserv, Token Bucket, 19750 bytes/sec.
ADSPEC
    
```

Slika 5.1.2. Razmena PATH i RESV poruka za Tunel158

Na slici 5.1.2. prikazano je snimanje paketa na jednom od interfejsa za tunel 158. Kroz ovo hvatanje prošle su PATH i RESV poruke koje se razmenjuju između početka i kraja tunela, pri čemu je tunel unidirekcion. Izvorište je adresa *loopback1* interfejsa na ruteru R1, a odredište adresa *loopback1* interfejsa na ruteru R6. U okviru snimljenih paketa vidi se još i eksplicitna putanja kojom se tunel kreće, odnosno da je prva putanja aktivna u tom trenutku.

TunnelID je identifikator tunela. Svaki ruter do kog dođe PATH poruka, proveriti istu, i zatim ustanovi da li na interfejsu ima dovoljno slobodnog kapaciteta tj. koliko je tunel zatražio definisanjem RSVP protoka u okviru tunela. RESV poruka se šalje u uzvodnom smeru, i sa sobom nosi odgovarajuće labele pridružene ovom tunelu. Nakon što RESV poruka stigne do početka tunela, tunel se aktivira.

Zatim je jedan od interfejsa na primarnoj putanji ugašen. Ovo je urađeno sa ciljem provere da li se tunel zaista prerutira na sekundarnu eksplicitnu putanju. Treba obratiti pažnju da nema nikakvog rezervnog tunela, i da bi ispadom i sekundarne putanje, sam tunel pao.

```

93 67.5517550 10.10.10.25 224.0.0.2 LDP 76 Hello Message
94 68.1608160 10.10.10.26 224.0.0.2 LDP 76 Hello Message
95 68.2718270 ca:03:1e:60:00:54 ca:03:1e:60:00:54 LOOP 60 Reply
96 69.1779170 10.10.10.26 224.0.0.5 OSPF 82 LS Update
97 69.3209320 10.10.10.25 224.0.0.5 OSPF 82 LS Update
98 69.8739870 217.65.197.78 217.65.197.72 RSVP 238 PATH Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. SENDER TEM
99 69.9829980 10.10.10.25 224.0.0.5 OSPF 122 LS Update
100 70.0810080 10.10.10.25 224.0.0.5 OSPF 94 LS Update
101 70.2830280 10.10.10.25 10.10.10.26 RSVP 142 RESV Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. FILTERSPEC
102 71.6081600 10.10.10.26 224.0.0.5 OSPF 94 Hello Packet
103 71.7431740 10.10.10.26 224.0.0.5 OSPF 118 LS Acknowledge
104 72.3252320 10.10.10.25 224.0.0.2 LDP 76 Hello Message
105 72.4442440 10.10.10.26 224.0.0.2 LDP 76 Hello Message

```

```

Frame 98: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface 0
Ethernet II, Src: ca:03:1e:60:00:54 (ca:03:1e:60:00:54), Dst: ca:05:17:78:00:1c (ca:05:17:78:00:1c)
Internet Protocol Version 4, Src: 217.65.197.78 (217.65.197.78), Dst: 217.65.197.72 (217.65.197.72)
Resource Reservation Protocol (RSVP): PATH Message. SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e. SENDER TEMPLATE: IPv4-LSP, Tunnel Source
RSVP Header. PATH Message.
  SESSION: IPv4-LSP, Destination 217.65.197.72, Tunnel ID 158, Ext ID d941c54e.
  HOP: IPv4, 10.10.10.26
  TIME VALUES: 30000 ms
  EXPLICIT ROUTE: IPv4 10.10.10.25, IPv4 10.10.10.29, IPv4 10.10.10.30,
  LABEL REQUEST: Basic: L3PID: IP (0x0800)
  SESSION ATTRIBUTE: SetupPrio 0, HoldPrio 0, SE style, [R1_t158]
  SENDER TEMPLATE: IPv4-LSP, Tunnel Source: 217.65.197.78, LSP ID: 281.
  SENDER TSPEC: IntServ, Token Bucket, 19750 bytes/sec.
  ADSPEC

```

```

300 ca 05 17 78 00 1c ca 03 1e 60 00 54 08 00 46 c0 ...x.....T..F
310 00 e0 32 06 00 00 fd 2e b8 0a d9 41 c5 4e d9 41 ..2.....A.N.A
320 c5 48 94 04 00 00 10 01 7b be fd 00 00 c8 00 10 ...H.....{
330 01 07 d9 41 c5 48 00 00 00 9e d9 41 c5 4e 00 0c ...A.H...A.N.
340 03 01 0a 0a 0a 1a 18 00 04 15 00 08 05 01 00 00 ...o.f.....
350 75 20 00 24 14 01 01 08 0a 03 02 10 20 00 01 08 ...o.f.....

```

Slika 5.1.3. Rutiranje preko sekundarne eksplicitne putanje

Na slici 5.1.3. je priloženo snimanje paketa između rutera R3-R5 gde se uspostavlja sekundarna rezervna putanja. Sa ove slike se može primetiti da je eksplicitna putanja za tunnel sa *TunnelID*-em 158 drugačija u odnosu na prvobitnu.

Uneta je komanda *debug* u cilju otkrivanja problema i njihovog rešavanja:

```

R1#debug mpls traffic-eng tunnels events
MPLS traffic-eng tunnels system events debugging is on

```

```

*Mar 31 20:04:49.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Mar 31 20:04:49.799: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 02-Apr-15 08:50 by prod_rel_team
*Mar 31 20:04:49.955: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar 31 20:04:50.251: %LINK-5-CHANGED: Interface GigabitEthernet4/0, changed state to administratively down
*Mar 31 20:04:50.259: %LINK-5-CHANGED: Interface GigabitEthernet5/0, changed state to administratively down
*Mar 31 20:04:50.267: %LINK-5-CHANGED: Interface GigabitEthernet6/0, changed state to administratively down
*Mar 31 20:04:50.699: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is OFF
*Mar 31 20:04:50.703: %CRYPTO-6-GDOI ON OFF: GDOI is OFF
*Mar 31 20:04:51.479: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/0, changed state to down
*Mar 31 20:04:51.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet5/0, changed state to down
*Mar 31 20:04:51.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/0, changed state to down
*Mar 31 20:05:30.503: %OSPF-5-ADJCHG: Process 1, Nbr 217.65.197.29 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
*Mar 31 20:05:30.595: %OSPF-5-ADJCHG: Process 1, Nbr 217.65.197.32 on GigabitEthernet1/0 from LOADING to FULL, Loading Done
*Mar 31 20:05:31.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel150, changed state to up
*Mar 31 20:05:32.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel158, changed state to up
*Mar 31 20:05:35.995: %LDP-5-NBRCHG: LDP Neighbor 217.65.197.29:0 (1) is UP
*Mar 31 20:05:44.179: %LDP-5-NBRCHG: LDP Neighbor 217.65.197.32:0 (2) is UP
*Mar 31 20:05:44.723: %BGP-5-ADJCHANGE: neighbor 217.65.197.35 Up
*Mar 31 20:12:11.931: %SYS-5-CONFIG I: Configured from console by console
*Mar 31 20:13:26.047: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:13:26.047:         verify all LSPs
*Mar 31 20:13:26.051: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:13:26.059: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:13:26.059:         verify all LSPs
*Mar 31 20:13:42.399: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:13:42.403:         verify all LSPs
*Mar 31 20:13:42.403: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:13:42.411: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:13:42.411:         verify all LSPs
*Mar 31 20:13:46.715: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:13:46.715:         LSP path lookup
*Mar 31 20:13:46.719: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:13:46.727: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:13:46.727:         LSP path lookup
*Mar 31 20:13:47.587: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:13:47.587:         LSP path lookup
*Mar 31 20:13:47.591: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:13:47.599: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:13:47.599:         LSP path lookup
*Mar 31 20:14:35.423: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:14:35.423:         verify all LSPs
*Mar 31 20:14:35.427: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:14:35.435: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:14:35.435:         verify all LSPs
*Mar 31 20:14:50.135: LSP-TUNNEL: posting action(s) to all-tunnels:
--More--

```

Slika 5.1.4. Debug nakon gašenja interfejsa

Na slici 5.1.4. prikazane su sve poruke koje ruter razmenjuje, kao i stanja kroz koje prolazi posle unosa komande *debug*. Posle pada interfejsa koji se nalazi na primarnoj putanji, poziva se funkcija *LSP path lookup*.

Primećuje se da je tunel prerutiran na sekundarnu putanju tek nakon ispada interfejsa sa primarne putanje, što je problematično u smislu gubitaka paketa sve dok se sekundarna putanja ne uspostavi. Ovo ipak predstavlja olakšicu u smislu zauzetih resursa na putanjama najmanje metrike što je i cilj telekomunikacionih operatera.

Kad se link koji je otkazao ponovo uspostavi, tunel će opet krenuti prvobitnom putanjom, kao što je prikazano na slici 5.1.5.

```

*Mar 31 20:17:00.113:          verify all LSPs
*Mar 31 20:17:40.567: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:17:40.571:          verify all LSPs
*Mar 31 20:17:40.571: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:17:40.583: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:17:40.587:          verify all LSPs
*Mar 31 20:19:50.135: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:19:50.135:          perform auto bandwidth maintenance
*Mar 31 20:19:50.139: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:19:50.139: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:19:50.139:          perform auto bandwidth maintenance
R1#
*Mar 31 20:21:46.051: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:21:46.055:          LSP path lookup
*Mar 31 20:21:46.055: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:21:46.067: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:21:46.067:          LSP path lookup
*Mar 31 20:21:46.671: LSP-TUNNEL: posting action(s) to all-tunnels:
*Mar 31 20:21:46.675:          LSP path lookup
*Mar 31 20:21:46.675: LSP-TUNNEL: scheduling pending actions on all-tunnels
*Mar 31 20:21:46.683: LSP-TUNNEL: applying actions to all-tunnels, as follows:
*Mar 31 20:21:46.687:          LSP path lookup
R1#

```

Slika 5.1.5. Prebacivanje tunela na primarnu putanju nakon podizanja interfejsa

Na slici 5.1.5. može se videti da se tunel prerutirao na primarnu putanju nakon podizanja interfejsa na njoj (pozvana je funkcija *LSP path lookup* nakon podizanja interfejsa). To je određeno samom prioritizacijom *path* opcija u okviru tunela [9, 10].

5.2. Dinamička putanja

Zamisao ove simulacije je provera da li će saobraćaj tunela krenuti IGP putanjom u slučaju gašenja eksplicitne putanje. U te svrhe kreiran je Tunnel150 sa adresom izvorišta *loopback1*. Naznačena je vrsta tunela kao MPLS TE. Kao odredište je postavljena *loopback* adresa rutera R6. Prioritet nije postavljen te mu je dodeljen najmanji. Kao primarna putanja ovog tunela postavljena je ruta koja ide preko R2-R3-R5-R6 rutera. Kao sekundarna ruta dodeljena je dinamička putanja. To se postiže prioritizacijom putanja u okviru samog tunela. Ispraćeno je da li se tunel uspostavio, i koja mu je aktivna ruta.

```

R1(config)# interface Tunnel150
R1(config-if)# ip unnumbered Loopback1
R1(config-if)# tunnel mode mpls traffic-eng
R1(config-if)# tunnel destination 217.65.197.72
R1(config-if)# tunnel mpls traffic-eng autoroute announce
R1(config-if)# tunnel mpls traffic-eng priority 7 7
R1(config-if)# tunnel mpls traffic-eng bandwidth 150
R1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name R2-R3-R5_R6
R1(config-if)# tunnel mpls traffic-eng path-option 2 dynamic

```

Urađen je *shutdown* na R2 ruteru, interfejs ka R3.

```

R1#sh mpls traffic-eng tunnels tunnel 150

Name: R1_t150 (Tunnel150) Destination: 217.65.197.72
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 2, type dynamic (Basis for Setup, path weight 251)
  path option 1, type explicit R2-R3-R5_R6

Config Parameters:
  Bandwidth: 150 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 150 bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: dynamic path option 2 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0, 214
RSVP Signalling Info:
  Src 217.65.197.78, Dst 217.65.197.72, Tun_Id 150, Tun_Instance 20
RSVP Path Info:
  My Address: 10.10.10.1
  Explicit Route: 10.10.10.2 10.10.10.13 10.10.10.14 10.10.10.22
                  10.10.10.21 10.10.10.29 10.10.10.30 217.65.197.72
  Record Route: NONE
  Tspec: ave rate=150 kbits, burst=1000 bytes, peak rate=150 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=150 kbits, burst=1000 bytes, peak rate=150 kbits
Shortest Unconstrained Path Info:
  Path Weight: 251 (TE)
  Explicit Route: 10.10.10.1 10.10.10.2 10.10.10.13 10.10.10.14
                  10.10.10.22 10.10.10.21 10.10.10.29 10.10.10.30
                  217.65.197.72

History:
Tunnel:
  Time since created: 2 hours, 34 minutes
  Time since path change: 22 seconds
  Number of LSP IDs (Tun_Instances) used: 20
Current LSP:
  Uptime: 22 seconds
  Selection: reoptimization
Prior LSP:
  ID: path option 1 [18]
  Removal Trigger: label reservation removed
  Last Error: PCALC:: Can't use link 10.10.10.10 on node 217.65.197.29
R1#

```

Slika 5.2.1. Uspostava dinamičke putanje nakon otkaza eksplicitne

Nakon što je ugašen interfejs na eksplicitnoj putanji, očekivano ponašanje je da će tunel biti preusmeren IGP putanjom. Izvršena je provera stanja tunela nakon otkaza odgovarajućeg linka, odnosno interfejsa GigabitEthernet 3/0 na ruteru R3, kao što je prikazano na slici 5.2.1. Pokazano je da je u tom trenutku aktivna putanja dinamička kao i da je vreme nakon promene putanje 22 sekunde, dok je tunel kreiran duže vreme od navedenog.

```

R1#traceroute mpls traffic-eng tunnel 150
Tracing MPLS TE Label Switched Path on Tunnel150, timeout is 2 seconds

Codes: '.' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
 0 10.10.10.1 MRU 1500 [Labels: 217 Exp: 0]
L 1 10.10.10.2 MRU 1500 [Labels: 401 Exp: 0] 112 ms
L 2 10.10.10.14 MRU 1500 [Labels: 500 Exp: 0] 136 ms
L 3 10.10.10.21 MRU 1504 [Labels: implicit-null Exp: 0] 116 ms
! 4 10.10.10.30 76 ms
R1#

```

Slika 5.2.2. Dinamički uspostavljena putanja gašenjem interfejsa na eksplicitnom putu

Na slici 5.2.2. ispraćena je putanja tunela 150 nakon otkaza eksplicitne rute. Može se primetiti da mu je sledeći hop sa rutera R1 na R2, a ne ruter R3, kako je i očekivano.

5.3. FRR zaštita

Mehanizam zaštite tokom pada tunela je unapred definisani zaštitni tunel koji preuzima saobraćaj u slučaju pada linka ili čvora na putanji glavnog tunela. Ovaj zaštitni mehanizam je poznat kao *Fast Reroute*. Zaštitni put preuzima saobraćaj prilikom preusmeravanja sa putanje, koja je otkazala, na radnu putanju. Zaštita saobraćaja odigraće se od početnog čvora prvobitnog tunela. Na taj način vreme prebacivanja na novu putanju uključuje vreme koje je potrebno da čvor koji je otkrio otkaz obavesti početni čvor tunela, i vreme potrebno da se izvrši preusmeravanje. U toku tog vremenskog intervala dolaziće do gubitaka paketa.

FRR zaštita je inicirana od strane čvora na početku tunela. U slučaju pada, početni čvor će izračunati sledeći dostupan put i iniciraće LSP, pa zatim preusmeriti saobraćaj novom putanjom. S jednog na drugi kraj tunela saobraćaj će biti zaštićen u vremenskom intervalu od 50ms.

```

R6#traceroute 217.65.197.28
Type escape sequence to abort.
Tracing the route to 217.65.197.28
VRF info: (vrf in name/id, vrf out name/id)
 1 10.10.10.29 [MPLS: Label 517 Exp 0] 116 msec 68 msec 68 msec
 2 10.10.10.22 [MPLS: Label 415 Exp 0] 88 msec 68 msec 68 msec
 3 10.10.10.13 [MPLS: Label 209 Exp 0] 68 msec 52 msec 32 msec
 4 10.10.10.1 76 msec 72 msec 76 msec
R6#

```

Slika 5.3.1. IGP putanja na R6 pre uspostave TE tunela i FRR TE tunela

Na slici 5.3.1. je prikazana IGP putanja kojom sav saobraćaj ide od rutera R6 do R1. To stanje će biti promenjeno tunelima i njihovim eksplicitnim putanjama, radi očuvanja kapaciteta na IGP-u.

Kreirani su tuneli 200 i 400 na ruteru R6, izvorište im je interfejs *loopback1* na ruteru R6, a odredište adresa *loopback1* interfejsa rutera R1. Vrste tunela su MPLS TE, i u okviru oba je postavljena jedna eksplicitna putanja. Kako bi FRR zaštita bila aktivirana neophodno je u okviru ta dva tunela navesti da za njih postoji zaštita, u smislu protoka. Protok tunela 200 je 200kb/s, a rezervisani protok za tunel 400 je 100kb/s.

Ruter R6

```
R6(config)# interface Tunnel200
R6(config-if)# ip unnumbered Loopback1
R6(config-if)# tunnel mode mpls traffic-eng
R6(config-if)# tunnel destination 217.65.197.78
R6(config-if)# tunnel mpls traffic-eng autoroute announce
R6(config-if)# tunnel mpls traffic-eng bandwidth 200
R6(config-if)# tunnel mpls traffic-eng priority 7 7
R6(config-if)# tunnel mpls traffic-eng path-option 1 explicit name PRI_LSP
R6(config-if)# tunnel mpls traffic-eng fast-reroute
R6(config-if)# no routing dynamic
R6(config)# interface Tunnel400
R6(config-if)# ip unnumbered Loopback1
R6(config-if)# tunnel mode mpls traffic-eng
R6(config-if)# tunnel destination 217.65.197.78
R6(config-if)# tunnel mpls traffic-eng autoroute announce
R6(config-if)# tunnel mpls traffic-eng bandwidth 100
R6(config-if)# tunnel mpls traffic-eng priority 7 7
R6(config-if)# tunnel mpls traffic-eng path-option 1 explicit name PRI_LSP
R6(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
R6(config-if)# no routing dynamic
```

Na ovaj način kad ruter mapira LSP na rezervne tunele, *bw-protect* opcija osigurava da LSP koristi date rezervne tunele samo ako oni podržavaju dovoljnu količinu protoka za iste.

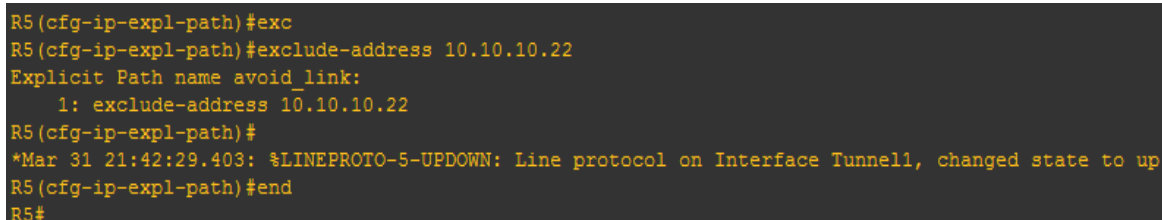
```
R6(config)# ip explicit-path name PRI_LSP
R6(cfg-ip-expl-path)#next-address 10.10.10.29
R6(cfg-ip-expl-path)#next-address 10.10.10.22
R6(cfg-ip-expl-path)#next-address 10.10.10.17
R6(cfg-ip-expl-path)#next-address 10.10.10.5
R6(cfg-ip-expl-path)#next-address 217.65.197.78
```

Putanja je zamišljena na sledeći način, R6-R5-R4-R3-R1. U slučaju otkaza interfejsa rutera R5 ka R4 mora postojati zaštita i to će biti izvedeno premošćavanjem putanje ka ruteru R3.

Potom je na ruteru R5 konfigurisan zaštitni tunel 1, adresa izvorišta mu je *loopback* interfejs rutera R5, tunel je iste vrste MPLS TE, ali je adresa njegovog odredišta *loopback* adresa rutera R3.

Sam tunel ima definisanu eksplicitnu putanju za obilaženje linka. U okviru te eksplicitne putanje navedena je adresa na linku između rutera R4 i R5, 10.10.10.22, koju treba izbeći. Za zaštitu interfejsa, u eksplicitnoj putanji se unosi IP adresa koju treba izbeći, dok se u zaštiti čvora unosi odgovarajući *router-id*.

```
R5(config)# interface Tunnel1
R5(config-if)# ip unnumbered Loopback0
R5(config-if)# tunnel mode mpls traffic-eng
R5(config-if)# tunnel destination 217.65.197.32
R5(config-if)# tunnel mpls traffic-eng autoroute announce
R5(config-if)# tunnel mpls traffic-eng path-option 1 explicit name avoid_link
R5(config-if)# no routing dynamic
R5(config)# ip explicit-path name avoid_link enable
R5(cfg-ip-expl-path)# exclude-address 10.10.10.22
```



```
R5(cfg-ip-expl-path)#exc
R5(cfg-ip-expl-path)#exclude-address 10.10.10.22
Explicit Path name avoid_link:
  1: exclude-address 10.10.10.22
R5(cfg-ip-expl-path)#
*Mar 31 21:42:29.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R5(cfg-ip-expl-path)#end
R5#
```

Slika 5.3.2. Prvi rezervni tunel je uspostavljen

Na slici 5.3.2. se može primetiti da se u toku konfiguracije eksplicitne putanje uspostavio prvi pomoćni (rezervni) tunel.

Zatim je kreiran zaštitni tunel 2 na ruteru R4. Kreiran je na ovom ruteru, jer u slučaju otkaza čvora R3, saobraćaj tunela 200 i 400 nemaju drugu putanju kroz mrežu do svog odredišta, a nakon što R4 otkrije pad jednog od svojih interfejsa, ka ruteru R3, mora da izvrši preusmeravanje saobraćaja na drugi interfejs.

Tunel 2 kao odredište ima *loopback* adresu rutera R4, a za odredište mu je postavljena adresa interfejsa *loopback1* rutera R1. To je takođe i odredište originalnih tunela 200 i 400. Tunel 2 ima eksplicitnu putanju u slučaju otkaza celog čvora, i u njoj je naglašeno da se izbegne adresa *loopback* interfejsa rutera R3.

```
R4(config)# interface Tunnel2
R4(config-if)# ip unnumbered Loopback0
R4(config-if)# tunnel mode mpls traffic-eng
R4(config-if)# tunnel destination 217.65.197.78
R4(config-if)# tunnel mpls traffic-eng autoroute announce
R4(config-if)# tunnel mpls traffic-eng path-option 1 explicit name avoid_node
R4(config-if)# no routing dynamic
```



```

R4(cfg-ip-expl-path)#exclude-address 217.65.197.32
Explicit Path name avoid_node:
  1: exclude-address 217.65.197.32
R4(cfg-ip-expl-path)#e
*Mar 31 22:12:44.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
R4(cfg-ip-expl-path)#exit
R4(config)#do sh ip int br

```

Slika 5.3.3. Drugi rezervni tunel je uspostavljen

Na slici 5.3.3. se može videti potvrda da je tunel 2 uspostavljen po završetku konfigurisanja istog.

```

R4(config)# ip explicit-path name avoid_node enable
R4(cfg-ip-expl-path)# exclude-address 217.65.197.32

```

Kako bi zaštitni tuneli bili primenjeni na odgovarajućim interfejsima, potrebno je na interfejsu rutera R5 odnosno R4, navesti da su pomoćni (rezervni) tuneli upravo tuneli 1, odnosno 2, respektivno.

```

R5(config)# interface GigabitEthernet0/0
R5(config-if)# mpls traffic-eng backup-path Tunnel1
R4(config)# interface GigabitEthernet0/0
R4(config-if)# mpls traffic-eng backup-path Tunnel2

```

```

R5#sh ip rsvp sender
To          From          Pro DPort Sport Prev Hop      I/F      BPS
217.65.197.32 217.65.197.34 0   1    2    none  none      0
217.65.197.72 217.65.197.78 0  150  23   10.10.10.26 Gi1/0    150K
217.65.197.72 217.65.197.78 0  158  26   10.10.10.22 Gi0/0    158K
217.65.197.78 217.65.197.72 0  200  7    10.10.10.30 Gi2/0    200K
217.65.197.78 217.65.197.72 0  400  7    10.10.10.30 Gi2/0    100K
R5#

```

Slika 5.3.4. Postojeći tuneli

Postoji više komandi kojima se može potvrditi da li su zaista tuneli uspostavljeni, koje resurse zauzimaju, koje su im destinacije, sledeći hopovi i izlazni interfejsi, kao što je prikazano na slici 5.3.4.

```

R4#sh ip rsvp reservation
To          From          Pro DPort Sport Next Hop      I/F      Fi Serv BPS
217.65.197.72 217.65.197.78 0  158  26   10.10.10.21  Gi1/0    SE LOAD 158K
217.65.197.78 217.65.197.33 0   2    2    10.10.10.13  Gi2/0    SE LOAD 0
217.65.197.78 217.65.197.72 0  200  7    10.10.10.17  Gi0/0    SE LOAD 200K
217.65.197.78 217.65.197.72 0  400  7    10.10.10.17  Gi0/0    SE LOAD 100K
R4#

```

Slika 5.3.5. Verifikacija uspostavljenih tunela

Na slici 5.3.5. mogu se videti tuneli koji su trenutno aktivni. Primarni tuneli na ruteru R5 su prikazani na slici 5.3.5. sa propusnim opsegom od 100 i 200, dok je sekundarni odnosno rezervni tunel označen 0 (na slici 5.3.5. - poslednja kolona).

```
R5#sh ip rsvp reservation detail
Reservation:
  Tun Dest:    217.65.197.32  Tun ID: 1  Ext Tun ID: 217.65.197.34
  Tun Sender: 217.65.197.34  LSP ID: 2
  Next Hop: 10.10.10.26 on GigabitEthernet1/0
  Label: 0 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 0200040F.
  Created: 21:42:29 UTC Thu Mar 31 2016
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
Reservation:
  Tun Dest:    217.65.197.72  Tun ID: 150  Ext Tun ID: 217.65.197.78
  Tun Sender: 217.65.197.78  LSP ID: 23
  Next Hop: 10.10.10.30 on GigabitEthernet2/0
  Label: 0 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 05000413.
  Created: 21:05:28 UTC Thu Mar 31 2016
  Average Bitrate is 150K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
Reservation:
  Tun Dest:    217.65.197.72  Tun ID: 158  Ext Tun ID: 217.65.197.78
  Tun Sender: 217.65.197.78  LSP ID: 26
  Next Hop: 10.10.10.30 on GigabitEthernet2/0
  Label: 0 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 06000418.
  Created: 20:35:22 UTC Thu Mar 31 2016
  Average Bitrate is 158K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
Reservation:
  Tun Dest:    217.65.197.78  Tun ID: 200  Ext Tun ID: 217.65.197.72
  Tun Sender: 217.65.197.72  LSP ID: 7
  Next Hop: 10.10.10.22 on GigabitEthernet0/0
  Label: 419 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 27000412.
  Created: 22:17:17 UTC Thu Mar 31 2016
  Average Bitrate is 200K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
```

Slika 5.3.6. Provera rada tunela

Unosom komande `sh ip reservation detail`, dat je detaljan prikaz tunela koji prolaze kroz ruter R5 sa odgovarajućim zahtevanim kapacitetima. Ovo je prikazano na slici 5.3.6.

Kako bi bilo provereno da FRR zaista funkcioniše, urađeni su sledeći koraci:

```
R4#sh mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label Out intf/label   FRR intf/label   Status
LSP midpoint frr information:
LSP identifier           In-label Out intf/label   FRR intf/label   Status
217.65.197.72 200 [7]             419      Gi0/0:304       Tu2:implicit-nul ready
217.65.197.72 400 [7]             420      Gi0/0:319       Tu2:implicit-nul ready
R4#
```

Slika 5.3.7. FRR baza podataka

Na slici 5.3.7. prikazana je FRR baza podataka svih zaštitnih tunela rutera R4. Tuneli su uspostavljeni i očekuju prebacivanje saobraćaja kad se za tim javi potreba. Sa iste slike mogu se videti i izlazni interfejsi kao i dodeljene labele namenjene tunelima.

```
R5#sh mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Number of protected interfaces: 1
  Number of protected tunnels: 2
  Number of backup tunnels: 1
  Number of active interfaces: 0
LSP identifier 217.65.197.72 200 [7], ready
  Input label 514, Output label Gi0/0:419, FRR label Tu1:304
  Role Mid Head Hop 217.65.197.72 Tail Hop 217.65.197.78
LSP identifier 217.65.197.72 400 [7], ready
  Input label 521, Output label Gi0/0:420, FRR label Tu1:319
  Role Mid Head Hop 217.65.197.72 Tail Hop 217.65.197.78
R5#
```

Slika 5.3.8. FRR baza podataka na R5 ruteru sa detaljima

Slika 5.3.8. predstavlja detaljniji prikaz FRR baze podataka rutera R5, gde se jasno vidi prikaz broja zaštićenih interfejsa, zaštićenih tunela i rezervnih tunela. Tunnel i 200 i 400 sa prioritetima 7 su u statusu „spremni“, kao što se može videti sa slike 5.3.8.

RSVP-Hello funkcija, daje funkcionalnost RSVP čvorovima u mreži da detektuju kad susedni čvorovi nisu pristupačni. Ovo omogućava detekciju otkaza sa kraja-na-kraj. Može biti korišćen od strane FRR kad obaveštenje o *link-layer* otkazima nije dostupno ili kad mehanizmi detekcije otkaza nisu dovoljno efikasni po pitanju brzine detekcije. Ovo se postiže omogućavanjem pomenute funkcionalnosti u globalnom režimu rada, a potom i na svakom od interfejsa gde je potrebno brže otkriti otkaz.

```

R5(config)#ip rsvp signalling hello
R5(config)#int gi 0/0
R5(config-if)#ip rsvp signalling hello
R4(config)#ip rsvp signalling hello
R4(config)#int gi 1/0
R4(config-if)#ip rsvp signalling hello

```

Potom je proverena FRR zaštita. Očekivano ponašanje je da će se tuneli preusmeriti nakon otkaza linka na ruteru R5 ka R4. Preusmerenje saobraćaja će se odigrati na ruteru R5 ka R3. Zatim saobraćaj nastavlja putanjom koja mu je eksplicitno zadata [9, 10].

```

*Mar 31 23:46:30.379: %LDP-5-NBRCHG: LDP Neighbor 217.65.197.33:0 (3) is DOWN (Received error notification from peer: Holddown time expired)
R5(config)#exit
R5#sh
*Mar 31 23:46:36.163: %SYS-5-CONFIG_I: Configured from console by console
R5#sh ip rsvp se
R5#sh ip rsvp sender
To          From          Pro DPort Sport Prev Hop      I/F      BPS
217.65.197.32 217.65.197.34 0 1 2 none none 0
217.65.197.72 217.65.197.78 0 150 23 10.10.10.26 Gi1/0 150K
217.65.197.72 217.65.197.78 0 158 26 10.10.10.22 Gi0/0 158K
217.65.197.72 217.65.197.78 0 158 28 10.10.10.26 Gi1/0 158K
217.65.197.78 217.65.197.72 0 200 7 10.10.10.30 Gi2/0 200K
217.65.197.78 217.65.197.72 0 400 7 10.10.10.30 Gi2/0 100K
R5#
*Mar 31 23:46:56.771: %OSPF-5-ADJCHG: Process 1, Nbr 217.65.197.33 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R5#

```

Slika 5.3.9. Provera bekap LSP-ova

Na slici 5.3.9. gde je uneta komanda *sh ip rsvp sender* može se primetiti da postoji otkaz linka ka ruteru R4, što se vidi iz OSPF notifikacija da je sused 217.65.197.33 nedostupan. Ovom komandom prikazani su svi konfigurisani tuneli, kao i njihov prethodni čvor na putanji i interfejs odakle je saobraćaj prosleđen.

Kako bi bila proverena FRR zaštita čvora, biće urađen stop procesa preko GNS3-a za ceo ruter R3.

```

R5#
*Apr 1 00:06:40.510: %LDP-5-NBRCHG: LDP Neighbor 217.65.197.32:0 (1) is DOWN (Discovery Hello Hold Timer expired)
R5#
*Apr 1 00:06:57.546: %OSPF-5-ADJCHG: Process 1, Nbr 217.65.197.32 on GigabitEthernet1/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R5#
*Apr 1 00:07:13.034: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnell, changed state to down

```

Slika 5.3.10. Pad R3 čvora u mreži

Slikom 5.3.10. prikazan je otkaz čvora R3 u mreži. Vidi se da su Hello brojač i Dead Interval brojač OSPF procesa za ovaj ruter istekli, odnosno ruter nije uspeo da odgovori na OSPF poruke, pa se proglašava prestanak njegovog rada.

```

R4#
*Apr 1 00:05:00.111: %LDP-5-NBRCHG: LDP Neighbor 217.65.197.32:0 (3) is DOWN (Discovery Hello Hold Timer expired)
R4#
*Apr 1 00:05:27.187: %OSPF-5-ADJCHG: Process 1, Nbr 217.65.197.32 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R4#
R4#show mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Number of protected interfaces: 1
  Number of protected tunnels: 2
  Number of backup tunnels: 1
  Number of active interfaces: 0
LSP identifier 217.65.197.72 200 [72], ready
  Input label 412, Output label Gi0/0:313, FRR label Tu2:implicit-null
  Role Mid Head Hop 217.65.197.72 Tail Hop 217.65.197.78
LSP identifier 217.65.197.72 400 [73], ready
  Input label 418, Output label Gi0/0:314, FRR label Tu2:implicit-null
  Role Mid Head Hop 217.65.197.72 Tail Hop 217.65.197.78
R4#

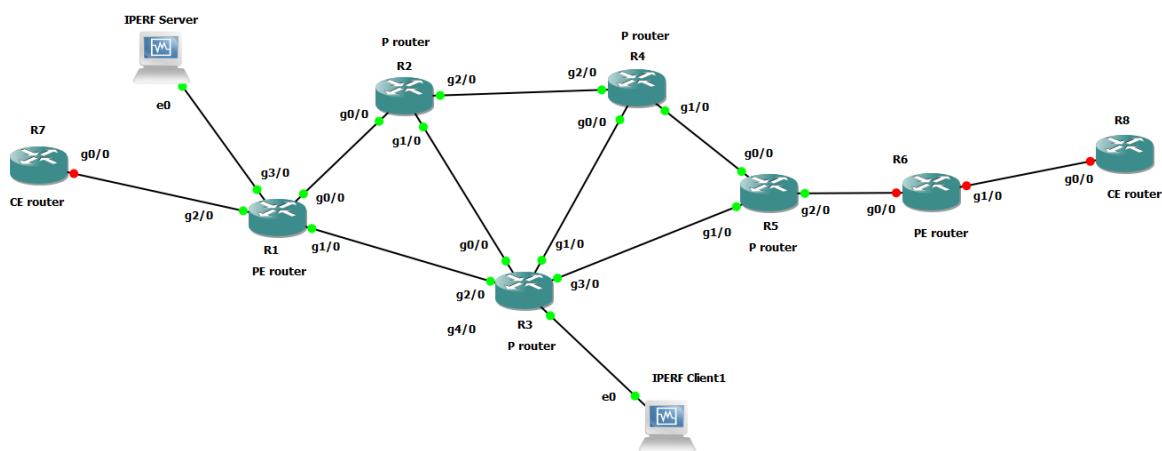
```

Slika 5.3.11. Uspostava bekap tunela nakon otkaza čvora

Zatim je urađena verifikacija očekivanog stanja prikazana na slici 5.3.11., tj. da li se saobraćaj preusmerio na ruter R2 sa rutera R4. Može se videti da je tunel 2 koji služi za obilaženje čvora R3, uspostavljen, odnosno preuzeo je saobraćaj.

5.4. IPERF testiranja

IPERF alat je iskorišćen radi dodatnih testiranja i u cilju posmatranja iskorišćenih protoka kroz core linkove MPLS mreže. On nudi opcije testiranja i TCP i UDP paketa što je odlična stvar u smislu provere svih vrsta saobraćaja kroz mrežu, kako korisnikovih tako i od operatora. IPERF generiše tok podataka između klijenta i servera i meri prenetu količinu podataka u Mb/s. U skladu sa tim izmenjena je topologija kao na slici 5.4.1.

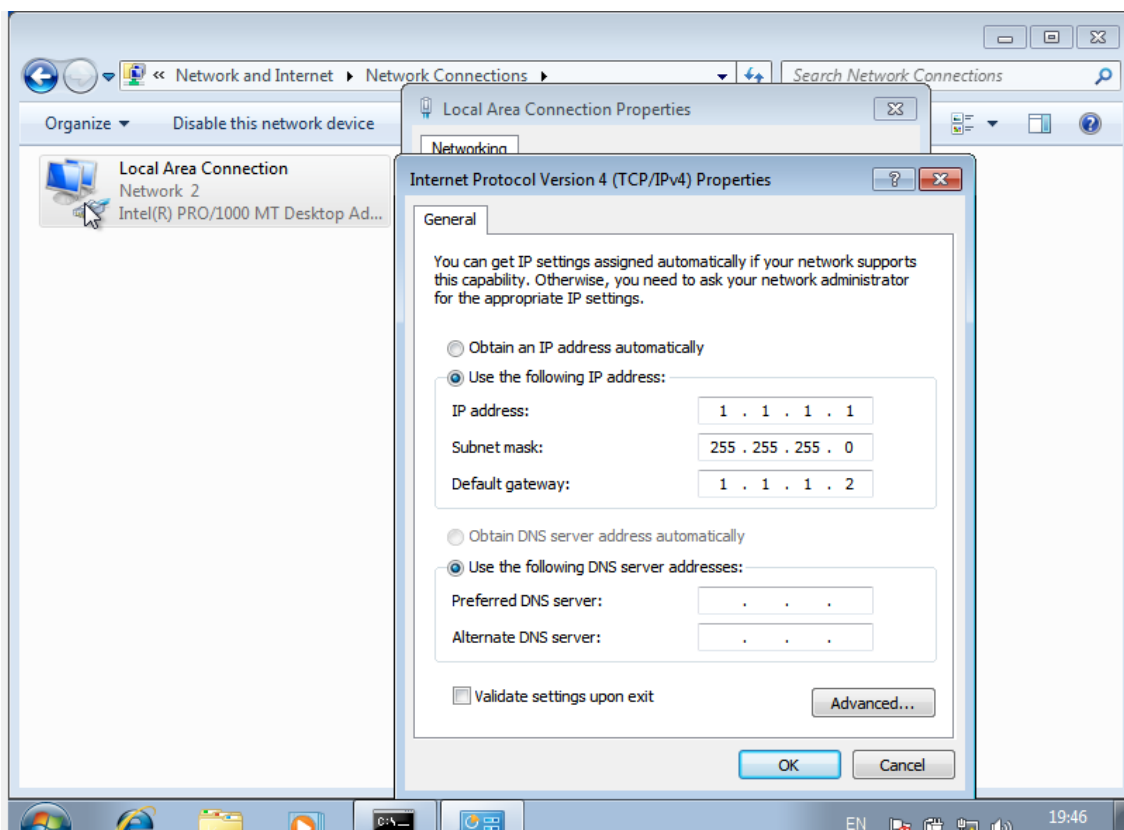


Slika 5.4.1. Izmenjena topologija mreže

Prvo je potrebno postići IP povezanost između samih mašina, što je postignuto dodavanjem proizvoljnih LAN adresa na interfejsima i mrežnim karticama virtuelnih mašina kao što je prikazano na slici 5.4.2.

Na ruterima je neophodno uraditi komandu *no shutdown* i dodati IP adresu sa odgovarajućom podmrežom.

Na Windows mašinama je potrebno podesiti parametre za LAN konekciju ka interfejsu rutera u GNS3 i obavezno čekirati opciju *turn off* za *firewall*-e na vitruelnim mašinama:

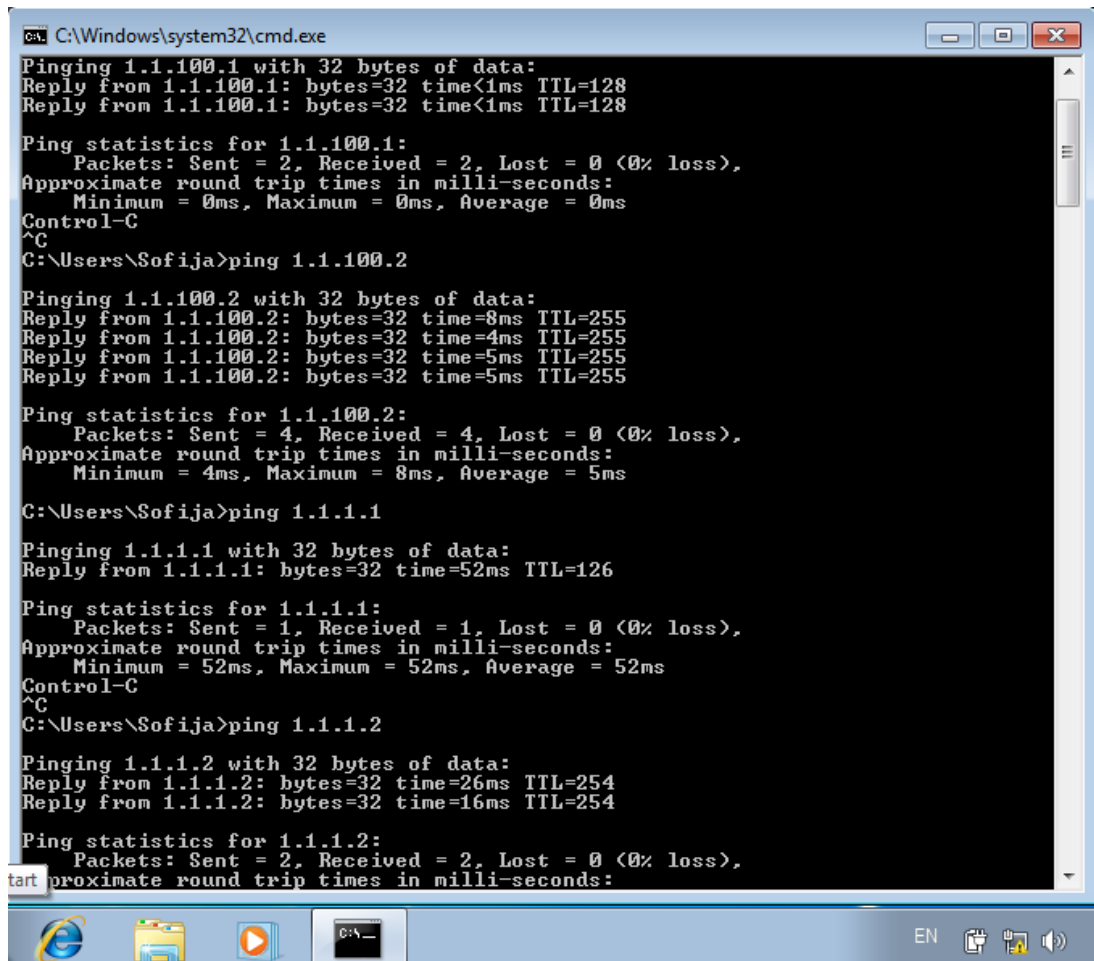


Slika 5.4.2. Podešavanje mrežnih kartica na IPERF serveru i klijentu

Dalje kad se gejtvej i računar međusobno vide, potrebne su rute kroz mrežu kako bi mašine mogle da se pinguju. To se može postići najjednostavnijim dodavanjem rute npr.

```
ip route 1.1.100.0 255.255.255.252 10.10.10.2
```

Na slici 5.4.3. je prikazana IP povezanost između virtuelizovanog računara, na koji je smešten IPERF softverski alat, i interfejsa rutera R1. Na slici 5.4.3. je takođe prikazana IP povezanost između virtuelizovanog računara označenog na slici 5.4.1. sa IPERF server, i interfejsa R3 rutera kao i virtuelizovanog računara označenog na slici 5.4.1. sa IPERF klijent. Ovime je demonstrirano da postoji IP povezanost ovih računara u mreži.



```
C:\Windows\system32\cmd.exe
Pinging 1.1.100.1 with 32 bytes of data:
Reply from 1.1.100.1: bytes=32 time<1ms TTL=128
Reply from 1.1.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 1.1.100.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Sofija>ping 1.1.100.2

Pinging 1.1.100.2 with 32 bytes of data:
Reply from 1.1.100.2: bytes=32 time=8ms TTL=255
Reply from 1.1.100.2: bytes=32 time=4ms TTL=255
Reply from 1.1.100.2: bytes=32 time=5ms TTL=255
Reply from 1.1.100.2: bytes=32 time=5ms TTL=255

Ping statistics for 1.1.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
C:\Users\Sofija>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=52ms TTL=126

Ping statistics for 1.1.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 52ms, Average = 52ms
Control-C
^C
C:\Users\Sofija>ping 1.1.1.2

Pinging 1.1.1.2 with 32 bytes of data:
Reply from 1.1.1.2: bytes=32 time=26ms TTL=254
Reply from 1.1.1.2: bytes=32 time=16ms TTL=254

Ping statistics for 1.1.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Slika 5.4.3. IP povezanost između mašina

S obzirom da je ostvarena potpuna povezanost između krajnjih uređaja, meriće se sledeće: link sa najmanjim slobodnim kapacitetom duž putanja i kapaciteti između krajnjih uređaja na putanjama. Klijent predstavlja izvorište, odnosno onog koji šalje podatke dok server prima. Klijent može da šalje TCP ili UDP pakete.

TCP-om mogu se meriti gubici, zagušenja, dostavljenje paketa van rasporeda, praznina bafera. UDP saobraćaj se koristi kod *Real-Time* aplikacija, kao što je prenos slike, govora i videa, retransmisija nije ostvariva i gubici se teže tolerišu. Zbog činjenice da se gubici teže tolerišu i manjeg opterećenja na procesorima virtuelizovanih rutera, za potrebe zagušenja na linkovima, sa IPERF alatom generisaće se UDP saobraćaj.

```

C:\Users\Sofija\Downloads\IPERF>iperf3 -s
-----
Server listening on 5201
-----
Accepted connection from 1.1.100.1, port 49158
[ 5] local 1.1.1.1 port 5201 connected to 1.1.100.1 port 49159
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-1.00   sec    1.15 MBytes  9.61 Mbits/sec
[ 5]  1.00-2.00   sec    1.84 MBytes 15.5 Mbits/sec
[ 5]  2.00-3.00   sec    1.82 MBytes 15.3 Mbits/sec
[ 5]  3.00-4.00   sec    1.62 MBytes 13.6 Mbits/sec
[ 5]  4.00-5.00   sec    1.50 MBytes 12.6 Mbits/sec
[ 5]  5.00-6.00   sec    1.73 MBytes 14.5 Mbits/sec
[ 5]  6.00-7.00   sec    1.82 MBytes 15.3 Mbits/sec
[ 5]  7.00-8.00   sec    1.79 MBytes 15.0 Mbits/sec
[ 5]  8.00-9.00   sec    1.82 MBytes 15.3 Mbits/sec
[ 5]  9.00-10.00  sec    1.81 MBytes 15.2 Mbits/sec
[ 5] 10.00-10.22  sec     428 KBytes 16.0 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-10.22  sec     0.00 Bytes  0.00 bits/sec      sender
[ 5]  0.00-10.22  sec    17.3 MBytes 14.2 Mbits/sec      receiver
-----
Server listening on 5201

```

Slika 5.4.4. TCP protok snimljen na server strani

Opcija-w za IPERF se može koristiti prilikom zahteva za određenom bafer veličinom.

```

IPERF Client1 [Running] - Oracle VM VirtualBox
C:\Windows\system32\cmd.exe
iperf Done.
C:\Users\Sofija\Downloads\IPERF>iperf3 -c 1.1.1.1 -w 1800
Connecting to host 1.1.1.1, port 5201
[ 4] local 1.1.100.1 port 49167 connected to 1.1.1.1 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.00   sec    31.6 KBytes 259 Kbits/sec
[ 4]  1.00-2.00   sec    56.2 KBytes 461 Kbits/sec
[ 4]  2.00-3.00   sec    56.2 KBytes 461 Kbits/sec
[ 4]  3.00-4.00   sec    58.0 KBytes 475 Kbits/sec
[ 4]  4.00-5.00   sec    56.2 KBytes 461 Kbits/sec
[ 4]  5.00-6.00   sec    51.0 KBytes 418 Kbits/sec
[ 4]  6.00-7.00   sec    58.0 KBytes 475 Kbits/sec
[ 4]  7.00-8.00   sec    58.0 KBytes 475 Kbits/sec
[ 4]  8.00-9.00   sec    58.0 KBytes 475 Kbits/sec
[ 4]  9.00-10.00  sec    58.0 KBytes 475 Kbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-10.00  sec     541 KBytes 444 Kbits/sec      sender
[ 4]  0.00-10.00  sec     540 KBytes 442 Kbits/sec      receiver
iperf Done.
C:\Users\Sofija\Downloads\IPERF>iperf3 -c 1.1.1.1 -w 8000
Connecting to host 1.1.1.1, port 5201
[ 4] local 1.1.100.1 port 49169 connected to 1.1.1.1 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  1.00-2.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  2.00-3.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  3.00-4.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  4.00-5.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  5.00-6.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  6.00-7.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  7.00-8.00   sec     258 KBytes 2.11 Mbits/sec
[ 4]  8.00-9.00   sec     250 KBytes 2.05 Mbits/sec
[ 4]  9.00-10.00  sec     250 KBytes 2.11 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-10.00  sec     2.46 MBytes 2.06 Mbits/sec      sender
[ 4]  0.00-10.00  sec     2.45 MBytes 2.06 Mbits/sec      receiver
iperf Done.

IPERF Server [Running] - Oracle VM VirtualBox
C:\Windows\system32\cmd.exe - iperf3 -s
Server listening on 5201
Accepted connection from 1.1.100.1, port 49166
[ 5] local 1.1.1.1 port 5201 connected to 1.1.100.1 port 49167
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-1.00   sec     19.7 KBytes 153 Kbits/sec
[ 5]  1.00-2.00   sec     56.2 KBytes 461 Kbits/sec
[ 5]  2.00-3.00   sec     56.2 KBytes 461 Kbits/sec
[ 5]  3.00-4.00   sec     58.0 KBytes 475 Kbits/sec
[ 5]  4.00-5.00   sec     56.2 KBytes 461 Kbits/sec
[ 5]  5.00-6.00   sec     51.0 KBytes 418 Kbits/sec
[ 5]  6.00-7.00   sec     58.0 KBytes 475 Kbits/sec
[ 5]  7.00-8.00   sec     58.0 KBytes 475 Kbits/sec
[ 5]  8.00-9.00   sec     58.0 KBytes 475 Kbits/sec
[ 5]  9.00-10.00  sec     56.2 KBytes 461 Kbits/sec
[ 5] 10.00-10.22  sec     13.0 KBytes 486 Kbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-10.22  sec     0.00 Bytes  0.00 bits/sec      sender
[ 5]  0.00-10.22  sec     540 KBytes 433 Kbits/sec      receiver
Server listening on 5201
Accepted connection from 1.1.100.1, port 49168
[ 5] local 1.1.1.1 port 5201 connected to 1.1.100.1 port 49169
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-1.00   sec     195 KBytes 1.59 Mbits/sec
[ 5]  1.00-2.00   sec     251 KBytes 2.05 Mbits/sec
[ 5]  2.00-3.00   sec     254 KBytes 2.08 Mbits/sec
[ 5]  3.00-4.00   sec     251 KBytes 2.06 Mbits/sec
[ 5]  4.00-5.00   sec     251 KBytes 2.06 Mbits/sec
[ 5]  5.00-6.00   sec     244 KBytes 2.00 Mbits/sec
[ 5]  6.00-7.00   sec     250 KBytes 2.05 Mbits/sec
[ 5]  7.00-8.00   sec     258 KBytes 2.11 Mbits/sec
[ 5]  8.00-9.00   sec     256 KBytes 2.10 Mbits/sec
[ 5]  9.00-10.00  sec     256 KBytes 2.09 Mbits/sec
[ 5] 10.00-10.17  sec     42.6 KBytes 2.03 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-10.17  sec     0.00 Bytes  0.00 bits/sec      sender
[ 5]  0.00-10.17  sec     2.45 MBytes 2.02 Mbits/sec      receiver
Server listening on 5201

```

Slika 5.4.5. Različite veličine bafera za TCP saobraćaj

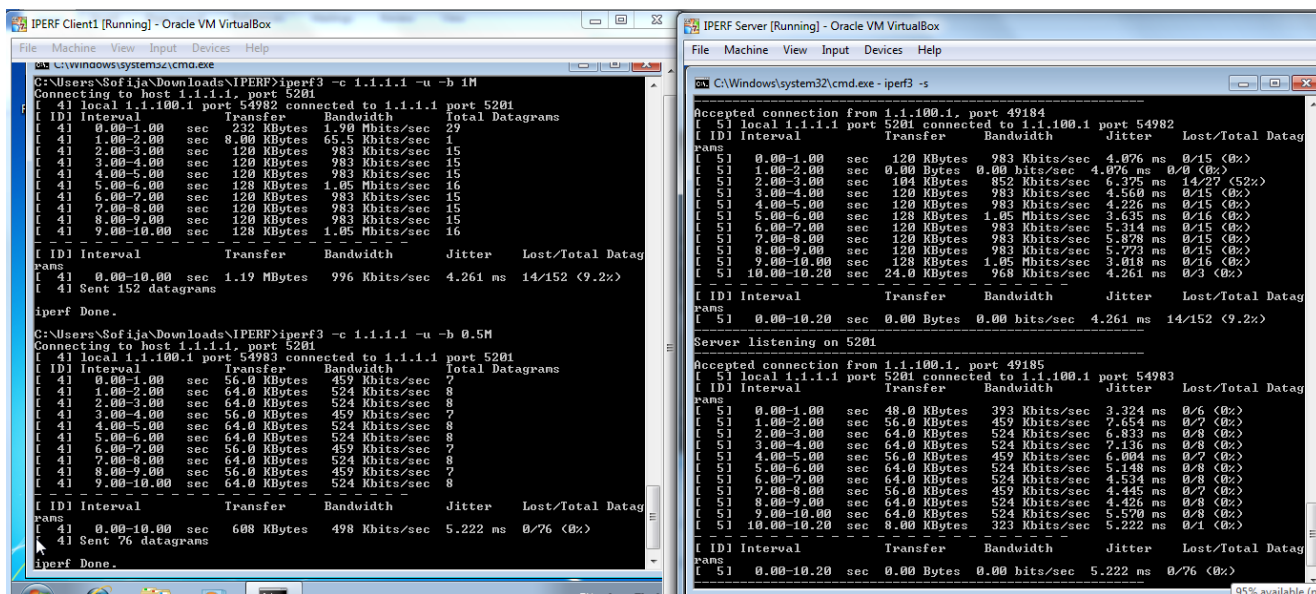
Na slikama 5.4.4. i 5.4.5. prikazane su opcije IPERF alata. Za prikazivanje opcija IPERF alata korišćeni su TCP paketi, od IPERF klijenta ka IPERF server strani, i izabrane su veličine prozora 1800 i 8000, respektivno. Kod TCP protokola u ovom slučaju, klijent vodi evidenciju o preostalom prostoru u odnosu na maksimalnu veličinu prozora koja je dozvoljena na linku, i šalje samo onoliko bajtova koliko server može trenutno da prihvati.

Na slici 5.4.5. prikazano je koliko se u zavisnosti od veličine prozora razlikuju i protoci na linku. Svaki čvor, odnosno uređaj koji učestvuje u TCP konekciji oglašava svoju bafer veličinu

koristeći TCP veličinu prozora. Bafer veličina predstavlja deo memorije uređaja, izdvojen da bi se u njega beležili podaci, potrebni za međukorake pri izvođenju određenih radnji, odnosno predstavlja maksimalnu veličinu memorijskog prostora za privremeni smeštaj podataka dobijenih od pošiljaoca na jednom linku, a pri čemu pošiljalac ne dobija TCP ACK poruku od primaoca. Kao što se vidi sa slike 5.4.5. odnosno rezultata dobijenih u simulaciji, kada je veličina TCP prozora manja manji je i protok na linku.

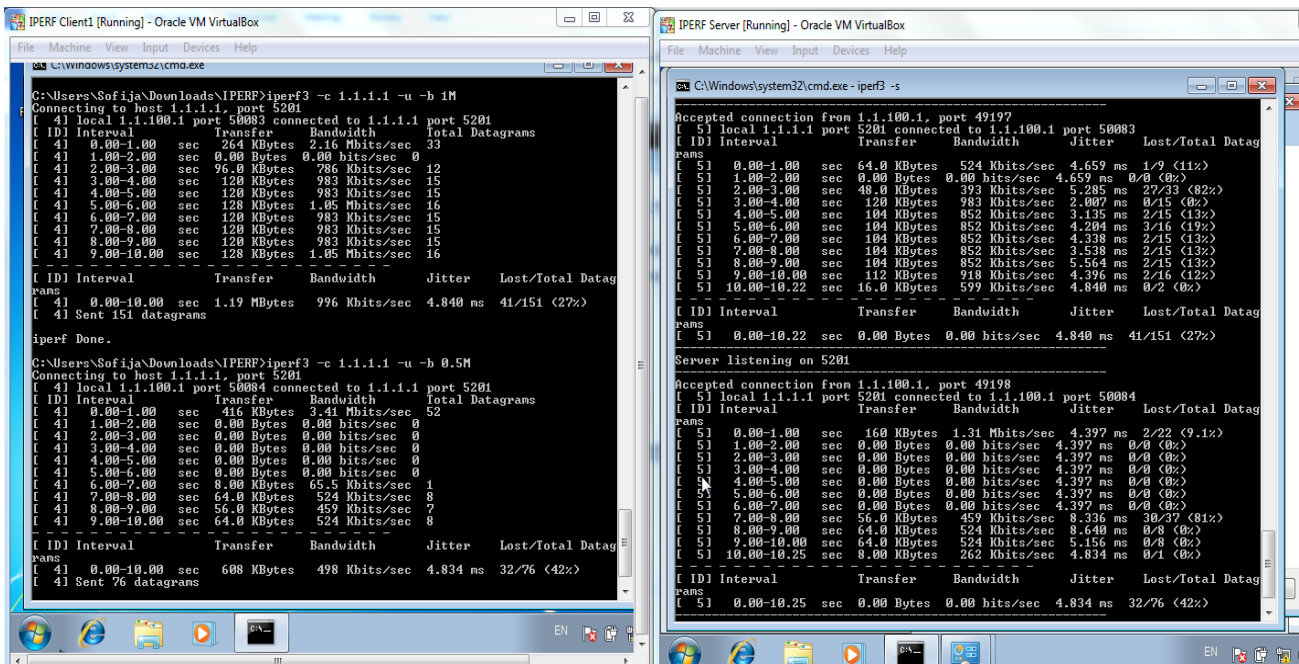
Prilikom generisanja UDP paketa na IPERF alatu, u osnovnim podešavanjima maksimalni protok je podešen na 1Mb/s. Ova vrednost će postepeno biti uvećavana dok link ne bude u potpunosti zagušen IPERF paketima odnosno na taj način će se dobiti informacija o slobodnom kapacitetu. Sa UDP paketima može se posmatrati sledeće: gubici, džiter, slanje van rasporeda itd. Džiter je varijacija u kašnjenju paketa na prijemnoj strani informacija. Parametar *latency* je kašnjenje u procesiranju od pošiljaoca do primaoca.

Na slikama 5.4.6. i 5.4.7. prikazana je provera na linku između R1 i R2, odnosno R3 i R5 sa zadatim protocima od 1Mb/s i 0.5Mb/s. Može se primetiti da se na tim interfejsima gubici javljaju pri veličini od 1Mb/s protoka. Na interfejsu između R1 i R2 postoji slobodan protok od 0.5Mb/s, dok je neiskorišćen kapacitet na linku između R3 i R5 manji od 0.5Mb/s.

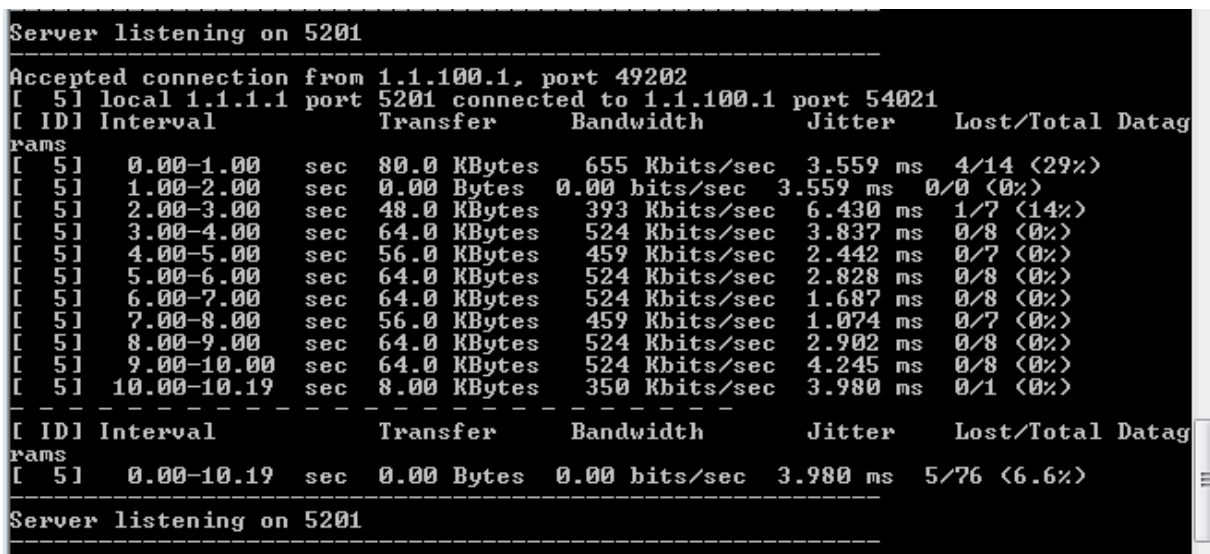


Slika 5.4.6. UDP saobraćaj kapaciteta 1Mb/s i 0.5Mb/s na linku između R1 i R2

QoS zahtevi za VoIP saobraćaj su: gubitak paketa ne sme da bude veći od 1%, jednosmerno kašnjenje ne sme biti duže od 150ms, i jednosmeran džiter ne sme biti duži od 30ms. To su parametri koje telekomunikacioni operatori nude u svojim SLA.



Slika 5.4.7. Link između R3 i R5 sa manje od 0.5Mb/s slobodnog kapaciteta



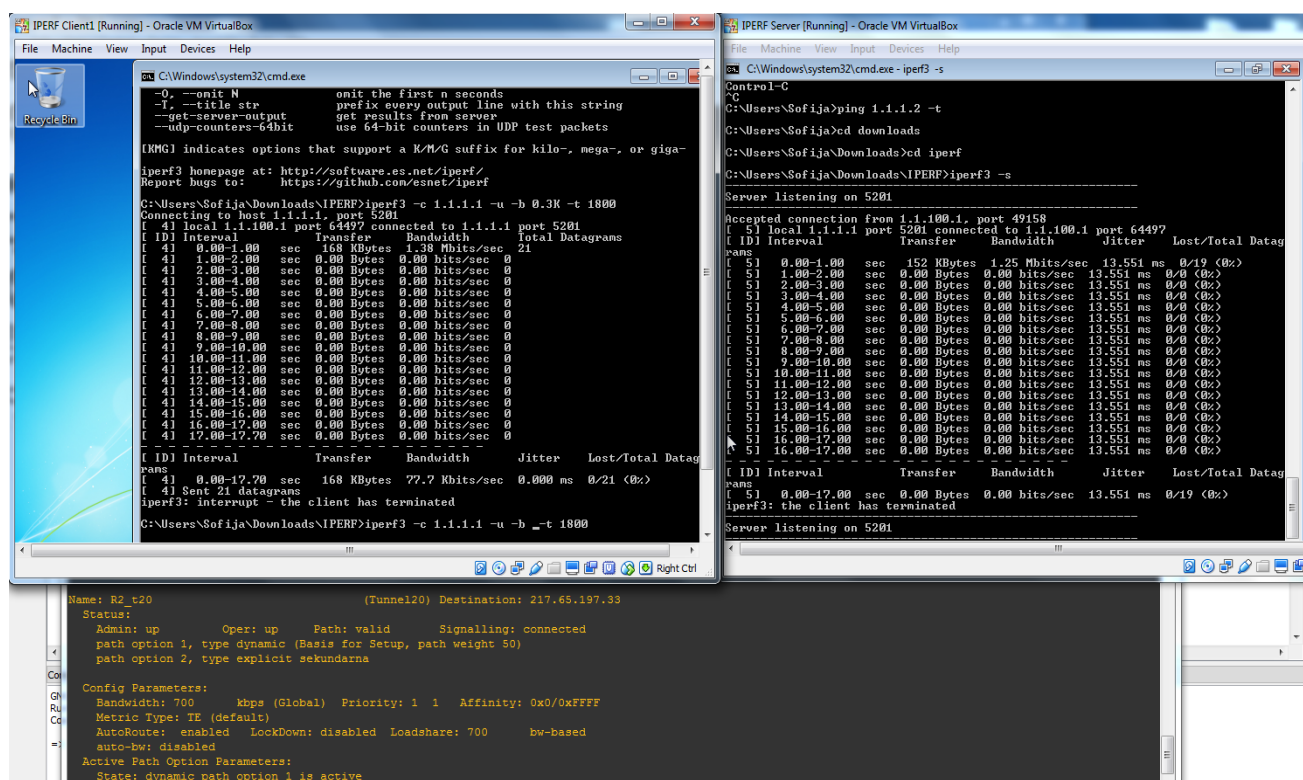
Slika 5.4.8. Interfejs između R3 i R4

Na interfejsima između rutera R3 i R4 nema 0.5Mb/s slobodnog kapaciteta, što je prikazano na slici 5.4.8. (ovo je uslovljeno ograničenim virtuelizacionim resursima koje pruža računar na kojem su vršene simulacije). Proverom je utvrđeno da dolazi do gubitaka paketa, odnosno grešaka, već pri protoku od 0.3Mb/s. U sličnom je stanju i interfejs između R4 i R5, koji ima 0.2Mb/s neiskorišćenog kapaciteta.

U ovom radu na slici 5.4.9. prikazan je urađen test sa novokreiranim tunelom 20, čija je prvobitna putanja preko IGP-a, a sekundarna eksplicitna. Za potrebe tunela rezervisan je kapacitet na toj putanji od 700kb/s, i posmatrano ponašanje kad je pušten preko IPERF-a protok od 1Mb/s,

koji će uz već iskorišćeni, biti previše za taj link. Testiranjem je izmeren ukupan slobodan protok na IGP putanji od oko 1Mb/s pre rezervisanja resursa od strane tunela.

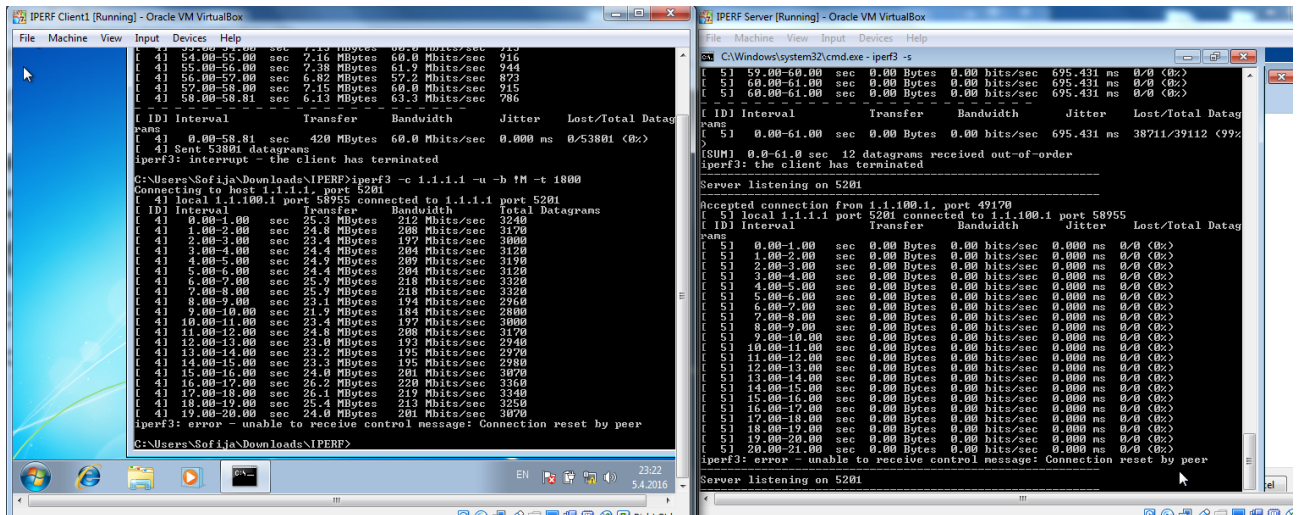
```
R2(config)# interface Tunnel20
R2(config-if)# ip unnumbered Loopback0
R2(config-if)# tunnel mode mpls traffic-eng
R2(config-if)# tunnel destination 217.65.197.33
R2(config-if)# tunnel mpls traffic-eng autoroute announce
R2(config-if)# tunnel mpls traffic-eng priority 1 1
R2(config-if)# tunnel mpls traffic-eng bandwidth 1200
R2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
R2(config-if)# tunnel mpls traffic-eng path-option 2 explicit name sekundarna
R2(config-if)# no routing dynamic
R2(config-if)# ip rsvp bandwidth 700
R2(config)# ip explicit-path name sekundarna enable
R2(cfg-ip-expl-path)# next-address 10.10.10.9
R2(cfg-ip-expl-path)# next-address 10.10.10.18
R2(cfg-ip-expl-path)# next-address 217.65.197.33
```



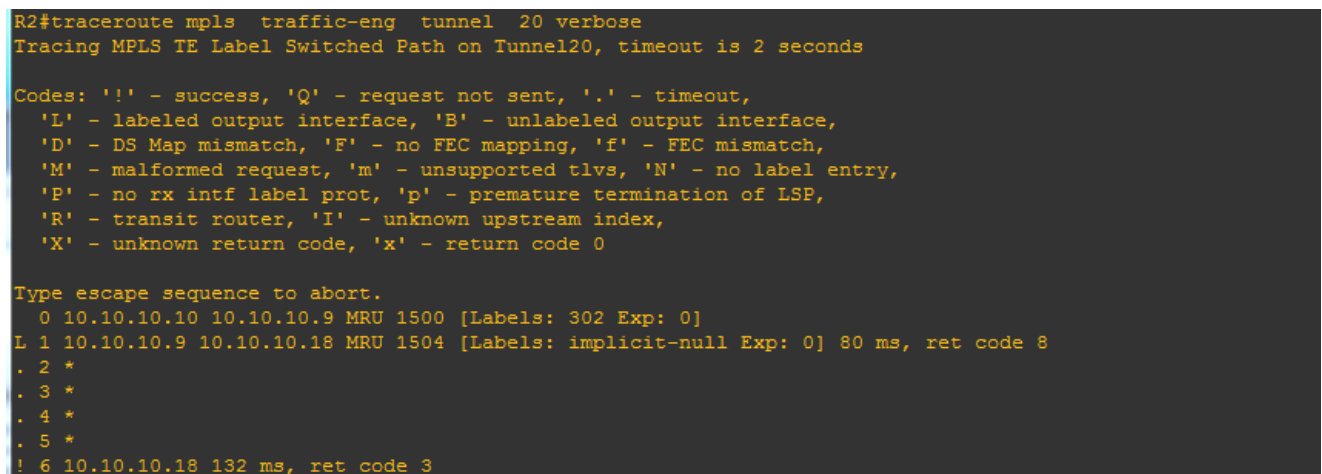
Slika 5.4.9. Protok od 0.3Mb/s kroz IPERF uz aktivnu dinamičku putanju

Slika 5.4.9. predstavlja situaciju pre ograničavanja protoka na interfejsima rutera. Može se primetiti da je pušten protok od 0.3kb/s bez gubitaka paketa. Opcija `-t` označava period slanja tih paketa, u ovom slučaju 1800 sekundi.

Na samim interfejsima IGP putanje je postavljeno ograničenje protoka od 1000kb/s. Očekivano ponašanje je da će tunnel morati da se prerutira na sekundarnu putanju. Potom je kroz IPERF pušten saobraćaj, pri čemu na server stranu ništa od paketa nije stizalo zbog nedovoljnog kapaciteta, što je prikazano na slici 5.4.10. Za IPERF je podešeno da nema drugu putanju osim kroz IGP rutu.



Slika 5.4.10. Nedovoljno slobodnog kapaciteta na IGP putanji



Slika 5.4.11. Tunnel 20 prerutiran na sekundarnu putanju

Na slici 5.4.11. pokazano je da usled nedovoljno kapaciteta tunnel usmerava saobraćaj sekundarnom putanjom, koja može da podrži resurse zahtevane od strane tunela. Može se primetiti kojim je interfejsima saobraćaj tunela usmeren, na osnovu adresa interfejsa [8].

5.5. Diskusija

Numeričke vrednosti prikazane u ovom radu nisu jednako relevantne kao u realnim situacijama gde se testiranja vrše na hardverskim uređajima. Glavni razlog za to, je što se prilikom simulacija koristio GNS3 softverski paket koji koristi virtuelizacioni sloj računara HP Elitebook. Pomenuti virtuelizacioni sloj ima velike nedostatke jer koristi samo deo kapaciteta Haswell arhitekture te ne prikazuje maksimalne vrednosti koje neki link ili uređaj mogu da ostvare.

Korišćenjem LSP putanje, koja je ujedno i najbolja IGP putanja, lako može doći do zagušenja. Mrežnim operatorima nije u cilju da imaju gubitke paketa, kako za servise svojih korisnika tako i u sopstvenim prenosima podataka. Ono što TE omogućava je da, uz uslov „uzmi najbolju IGP putanju“, doda i zahtev – “koja ima slobodan kapacitet“.

Prvim testom uspostavljene su samo eksplicitne putanje i dinamičko rutiranje nije dozvoljeno, tako da u slučaju pada obe putanje pao bi i sam tunel. Međutim ovim testom, uspešno je preusmeren saobraćaj ka drugim putanjama kako bi npr. core link u mreži operatora imao slobodan propusni opseg za neke druge VPN-ove, npr. nadzor samih uređaja u mreži, ili čak i za signalizaciju protokola rutiranja.

U narednom testu, pokušano je da se koristeći TE, navode različiti servisi drugim tunelima, kako bi se oslobodili resursi neophodni za više klase servisa. U krajnjem slučaju pokazano je da prilikom ispada nekih od interfejsa, saobraćaj bi bio primoran da ide LSP putanjom umesto RSVP.

U trećem testiranju korišćena je FRR tehnologija. Prikazane su dve mogućnosti FRR, zaštita linka i zaštita čvora. Ovde je cilj bio potpuno oslobađanje IGP rute, osim u slučaju otkaza celog čvora na eksplicitnoj putanji, gde nema drugog izbora. Otkazom samo jednog linka i dalje postoji opcija bekapa tunela, manje iskorišćenim rutama. Otkazom P čvora, saobraćaj je prerutiran jedinom radnom putanjom.

Testiranjem pomoću IPERF alata proveravan je kapacitet linkova u mreži kojima idu eksplicitne putanje kao i bekap tuneli. Interfejsi koji nisu na dinamičkoj putanji su iskorišćeni u pogledu rezervisanih resursa za potrebe tunela, međutim i sami linkovi na IGP putanji su skoro nepostojećeg slobodnog kapaciteta. Zato se javila potreba da sav saobraćaj, u mreži operatora, prerutiramo na sve moguće načine što dalje od glavne putanje.

Osim samog rasterećenja core linkova, korisnički osećaj servisa (*user-experience*) je takođe bitan za mrežnog operatora. To znači, upotreba linkova koje ne bi trebalo zagušiti saobraćajem, kako ne bi došlo do potpunog gubitka paketa za korisničke servise kada ne postoji drugačiji način prenosa saobraćaja.

6. ZAKLJUČAK

U ovom radu su rađena ispitivanja primena tehnologije *Traffic Engineering*-a. Prikazane su primene RSVP i FRR protokola. Za platformu projekta, i adekvatnih simulacija koje je projekat zahtevao, korišćen je softverski paket GNS3. Softverski paket GNS3 odlikuju ograničenja, kako u vidu iskorišćenja procesora, tako i kapaciteta (kapacitet se odnosi na broj uređaja koji mogu da se pokrenu u okviru virtuelizacionog sloja na hardverskoj platformi HP Elitebook računara kao i na broj paketa koje GNS3 može da obrađuje, pri čemu su zadržane sve funkcionalnosti simuliranih uređaja koje su bile neophodne kako bi se izveli rezultati i pravovremeni zaključak). Testovima smo postigli promene rute (putanje) saobraćaja sa putanje najmanje metrike, u cilju sprečavanja zagušenja. Testovima smo takođe uspeli da usmerimo saobraćaj, u slučaju otkaza linka ili celog čvora, alternativnim putanjama između Core rutera. Primenom IPERF generatora saobraćaja ispitivali smo prenos TCP/UDP paketa, kroz linkove u našoj mreži. Time smo emulirali korisnički saobraćaj, pri čemu testovi sa TCP saobraćajem nisu davali dovoljno informacija o raspoloživim kapacitetima. Puštanjem UDP paketa dobili smo vrednosti približne 1Mb/s sa minimalnim ili nepostojećim gubitkom paketa, gde je vrednost tih protoka u realnim mrežama mnogo viša. Pomenutoj projektnoj simulaciji protoci su uslovljeni izvesnim ograničenjima kako hardverskim, tako i ograničenjima softverskog paketa i računara koji se koristio za testiranja. U skladu sa tim zaključkom, optimizovani su protoci samih interfejsa, u cilju podržavanja najvećih vrednosti protoka uz najmanje gubitke paketa. Sa resursima koji su na raspolaganju pokazali smo da generisanjem više saobraćaja od onog što core linkovi mogu da obrade, korisnički saobraćaj mora i biva usmeren ka linkovima sa slobodnim kapacitetima, što je u stvari i zamisao *Traffic Engineering*-a.

Na osnovu prikazanih rezultata zaključuje se da usled zagušenja veza između Core rutera, dolazi do preusmeravanja saobraćaja na veze koje nemaju opterećenja ili nisu iskorišćeni do svojih predviđenih kapaciteta. U mrežama servis provajdera, koje su velike, brzo menjajuće i široko rasprostranjene, teško je u okviru svakog core uređaja menjati kuda će saobraćaj i u kom obimu prolaziti. Dalji pravci razvoja ovog rada i simulacija obuhvaćenih istim, su da treba posmatrati kako se mreža servisnog provajdera može ponašati usled *auto bandwidth* opcije postavljene na linkovima, kao i da se vidi kako je moguće kroz odgovarajuće softverske modifikacije (skripte) poboljšati preusmeravanje saobraćaja u mrežama i na vezama koje su pod velikim opterećenjem.

LITERATURA

- [1] Mr Nenad Krajnović,
(<http://telekomunikacije.etf.bg.ac.rs/predmeti/ot4ptm/MPLS.pdf>, (14.03.2016.)
- [2] http://webcache.googleusercontent.com/search?q=cache:yItgjIfREeoJ:www.ktios.net/stari/images/stories/clanovi_katedre/emil_secerov/tmsg/MPLS.ppt+&cd=1&hl=sr&ct=clnk&gl=rs (15.03.2016.)
- [3] Mr Nenad Krajnović,
(<http://telekomunikacije.etf.bg.ac.rs/predmeti/ot4ai/OSPF.pdf>, 16.03.2016.)
- [4] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html (21.02.2016.)
- [5] http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multiprotocol-label-switching-traffic-engineering/prod_presentation0900aecd80312824.pdf,(20.02.2016.)
- [6] <https://www.gns3.com/support> (01.02.2016.)
- [7] <https://www.pluralsight.com/blog/tutorials/gns3-initial-configuration>, 01.02.2016.
- [8] <https://www.es.net/assets/Uploads/201007-JTIperf.pdf>, 30.03.2016.
- [9] <http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/29828-mplsvpnte.html> (22.02.2016.)
- [10] http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/troubleshooting/guide/tr40asr9kbook/tr40mpl.pdf (26.02.2016.)
- [11] http://www.h3c.com.hk/Products_Technology/Technology/MPLS/Technology_White_Paper/200806/608770_57_0.htm (15.03.2016.)
- [12] <http://networkengineering.stackexchange.com/questions/23985/in-mpls-vpn-which-one-become-first-mpls-label-tag-or-vpn-encapsulation> (15.03.2016.)
- [13] <https://lvyang.wordpress.com/2010/11/04/> (15.03.2016.)
- [14] http://www.h3c.com.hk/technical_support_documents/technical_documents/switches/h3c_s12500_series_switches/configuration/operation_manual/h3c_s12500_cg-release7128-6w710/08/201301/772668_1285_0.htm (15.03.2016.)
- [15] http://h3c.com/portal/Products_Solutions/Technology/MPLS/Technology_White_Paper/200804/602785_57_0.htm (15.03.2016.)
- [16] <http://gponsolution.com/mpls-vpn-components-basic-knowledge.html> (15.03.2016.)
- [17] [http://www.h3c.com.cn/Service/Document_Center/Routers/Catalog/MSR/MSR_5600/Configure/Typical_Configuration_Example/H3C_\(V7\)-6W100/201411/843977_30005_0.htm](http://www.h3c.com.cn/Service/Document_Center/Routers/Catalog/MSR/MSR_5600/Configure/Typical_Configuration_Example/H3C_(V7)-6W100/201411/843977_30005_0.htm) (15.03.2016.)

SPISAK SKRAĆENICA

AS	<i>Autonomous System</i>
ATM	<i>Asynchronous Transfer Mode</i>
BGP	<i>Border Gateway Protocol</i>
CE/PE/P	<i>Customer Edge/Provider Edge/Provider</i>
CPU	<i>Central processing unit</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DR/BDR	<i>Designated Router/ Backup Designated Router</i>
FEC	<i>Forwarding Equivalence Class</i>
FR	<i>Frame Relay</i>
FRR	<i>Fast Reroute</i>
GMPLS	<i>Generalized Multi-Protocol Label Switching</i>
GNS3	<i>Graphical Network Simulator 3</i>
GUI	<i>Graphical User Interface</i>
HDLC	<i>High-Level Data Link Control</i>
IGP	<i>Interior Gateway Protocol</i>
IOS	<i>Internetwork Operating System</i>
IP	<i>Internet Protocol</i>
IPV6	<i>Internet Protocol version 6</i>
ISIS	<i>Intermediate System to Intermediate System</i>
L3/L2 VPN	<i>Layer3/Layer2 Virtual Private Network</i>
LDP	<i>Label Distribution Protocol</i>
LSA	<i>Link-State Advertisement</i>
LSDB	<i>Link-State Data Base</i>
LSP	<i>Label Switched Path</i>
LSR	<i>Label Switching Router</i>
MAC	<i>Medium Access Control</i>
MP	<i>Merge Point</i>
MPBGP	<i>Multiprotocol Border Gateway Protocol</i>
MPLS	<i>Multiprotocol Label Switching</i>
OSI	<i>Open Systems Interconnection</i>
OSPF	<i>Open Shortest Path First</i>
PLR	<i>Point of Local Repair</i>
PPP	<i>Point-to-Point</i>
RFC	<i>Request For Comments</i>
RSVP	<i>Resource Reservation Protocol</i>
RSVP-TE	<i>Resource Reservation Protocol Traffic Engineering</i>
SLA	<i>Service Level Agreement</i>
SPF	<i>Shortest Path First</i>
TCP/UDP	<i>Transmission Control Protocol/User Datagram Protocol</i>
TTL	<i>Time to Live</i>

QoS	<i>Quality of Service</i>
UDP	<i>User Datagram Protocol</i>
VRF	<i>Virtual Routing and Forwarding</i>
VPN	<i>Virtual Private Network</i>
VPNv4/v6	<i>Virtual Private Network version 4/version 6</i>

SPISAK SLIKA

Slika 2.1. Rutiranje saobraćaja na osnovu IGP-a [11]	4
Slika 2.2. Rutiranje saobraćaja na osnovu TE [11].....	5
Slika 2.3. MPLS zaglavlje [12]	6
Slika 2.4. Primer podržanih protokola u MPLS mreži [13].....	7
Slika 2.2.1. Koraci oglašavanja labela [14]	9
Slika 2.3.1. MPLS L3VPN arhitektura [15].....	10
Slika 2.3.2. VPNv4 adresna familija [16]	11
Slika 2.4.1. RSVP-TE signalizacija [11].....	12
Slika 2.4.2. Primer eksplicitne putanje [11].....	13
Slika 2.4.3. TE FRR [17]	14
Slika 3.1.1. GNS3 komponente koje se instaliraju	15
Slika 3.1.2. IOS image izbor	16
Slika 3.1.3. Put ka odgovarajućim folderima.....	16
Slika 3.1.4. Terminal podešavanja	17
Slika 3.1.5. Server opcije	17
Slika 3.1.6. Izbor interfejsa na ruteru.....	18
Slika 3.1.7. Podešavanje idle PC vrednosti.....	18
Slika 3.2.1. Dodavanje nove virtualne mašine u VirtualBox-u	19
Slika 3.2.2. Instalacija operativnog sistema na virtuelnoj mašini.....	20
Slika 3.2.3. Dodavanje novih virtuelnih mašina kroz GNS3.....	21
Slika 3.2.4. Podešavanje mrežnih kartica virtuelnih mašina.....	21
Slika 3.2.5. Pristupanje IPERF-u kroz command shell.....	22
Slika 3.2.6. Opcije koje IPERF alat nudi	22
Slika 4.1. Postojeća topologija mreže	23
Slika 4.1.1. Ping ka direktno povezanim interfejsima	27
Slika 4.2.1. Tabela usmeravanja OSPF protokola	29
Slika 4.3.1. LDP susedi rutera R3	31
Slika 4.3.2. Prikaz primera dodeljivanja labela	32
Slika 4.3.3. Primer MPLS forwarding tabele.....	32
Slika 4.3.4. Uspostava LDP susedstva.....	33
Slika 4.3.5. Razmena poruka između aktivnog i pasivnog LDP rutera	33
Slika 4.4.1. Provera uspostave MPBGP-a.....	34
Slika 5.1.1. Stanje tunel interfejsa.....	40
Slika 5.1.2. Razmena PATH i RESV poruka za Tunel158.....	41
Slika 5.1.3. Rutiranje preko sekundarne eksplicitne putanje	42
Slika 5.1.4. Debug nakon gašenja interfejsa	43
Slika 5.1.5. Prebacivanje tunela na primarnu putanju nakon podizanja interfejsa	44
Slika 5.2.1. Uspostava dinamičke putanje nakon otkaza eksplicitne.....	45

Slika 5.2.2. Dinamički uspostavljena putanja gašenjem interfejsa na eksplicitnom putu	46
Slika 5.3.1. IGP putanja na R6 pre uspostave TE tunela i FRR TE tunela.....	46
Slika 5.3.2. Prvi rezervni tunel je uspostavljen.....	48
Slika 5.3.3. Drugi rezervni tunel je uspostavljen	49
Slika 5.3.4. Postojeći tuneli.....	49
Slika 5.3.5. Verifikacija uspostavljenih tunela	49
Slika 5.3.6. Provera rada tunela	50
Slika 5.3.7. FRR baza podataka	51
Slika 5.3.8. FRR baza podataka na R5 ruteru sa detaljima.....	51
Slika 5.3.9. Provera bekap LSP-ova	52
Slika 5.3.10. Pad R3 čvora u mreži.....	52
Slika 5.3.11. Uspostava bekap tunela nakon otkaza čvora	53
Slika 5.4.1. Izmenjena topologija mreže.....	53
Slika 5.4.2. Podešavanje mrežnih kartica na IPERF serveru i klijentu.....	54
Slika 5.4.3. IP povezanost između mašina.....	55
Slika 5.4.4. TCP protok snimljen na server strani	56
Slika 5.4.5. Različite veličine bafera za TCP saobraćaj.....	56
Slika 5.4.6. UDP saobraćaj kapaciteta 1Mb/s i 0.5Mb/s na linku između R1 i R2	57
Slika 5.4.7. Link između R3 i R5 sa manje od 0.5Mb/s slobodnog kapaciteta	58
Slika 5.4.8. Interfejs između R3 i R4.....	58
Slika 5.4.9. Protok od 0.3Mb/s kroz IPERF uz aktivnu dinamičku putanju.....	59
Slika 5.4.10. Nedovoljno slobodnog kapaciteta na IGP putanji	60
Slika 5.4.11. Tunel 20 prerutiran na sekundarnu putanju	60