Inženjering saobraćaja u MPLS VPN mrežama

Ognjen Josipović

***Sadržaj* — Sa porastom broja uređaja na Internetu koji imaju svoje IP adrese, klasični protokoli rutiranja, koji usmeravaju pakete na bazi njegove IP adrese, postali su neefikasni, tj. nisu bili u stanju da odgovore sve većim zahtevima u pogledu brzine obrade i prosleđivanja paketa. Postali su uočljivi nedostaci da klasičan IP ne može da pruži neke servise koji su vremenom postali značajni za ozbiljne primene u oblasti pružanja telekomunikacionih servisa (QoS, traffic engineering, VPN,...), kao protokol bez uspostavljanja konekcije IP nema garancija za QoS, problem sa rutiranjem saobraćaja. Rad je baziran na MP-BGP protokolu kao osnovom za implementaciju MPLS VPN mreže. Zahvaljujući TE (traffic engineering) resursi mreže se mogu koristiti mnogo efikasnije i optimalnije**

***Ključne reči* — MPLS, VPN, TE-traffic engineering, BGP, OSPF, QoS**

I. UVOD

RAZLOG nastanka i današnje masovne implementacije MPLS tehnologije leži u činjenici da klasični IP protokol ne može da podrži efikasan prenos servisa koji su vremenom postali značajni za različite primene u oblasti pružanja telekomunikacionih servisa. Jedan od problema IP protokola jeste to što svi IGP (*Interior Gateway Protocol*) protokoli rutiranja rutiraju po jednoj putanji najmanje metrike, tako da se može desiti da imamo dve veze ka istoj lokaciji i da jedna bude opterećena, dok se druga uopšte ne koristi (neizbalansiranost).

O. Josipović, Saga d.o.o., Milentija Popovića 9, 11070 Beograd, Srbija; (e-mail: ognjen.josipovic@saga.rs).

II. MPLS

MPLS jeste mehanizam za brzo prosleđivanje paketa uz uvođenje tehnologije virtuelnih kanala. Ideja je u sledećem: Saobraćaj razvrstati u FEC (*Forwarding Equvalence Class*) klase i za svaku FEC klasu odrediti *Next Hop*. Paketi se označavaju labelom prema FEC klasi na ulazu u mrežu (PE uređaj). Labele se dobijaju na osnovu destinacione IP adrese, mada mogu da se dobijaju i na osnovu nečeg drugog, npr. porta na koji je stigao paket, rutera na koji je došao. Na ovaj način se menja osnovna paradigma IP rutiranja zasnovana na odredišnoj adresi, što nam je zapravo i cilj, a što će nam omogućiti mnogo novih funkcionalnosti koje sada uvodimo i koje će zahvaljujući MPLS-u biti dostupne.

Kao što vidimo na slici 1 labela se umeće između zaglavlja slojeva 2 i 3.

Slika 1 Paket sa labelom

Labele nekoj FEC dodeljuje ruter bliži destinaciji (*downstream*) i one se se kasnije propagiraju ka *upstream* ruterima. Ruteri informišu jedan drugog o načinu povezivanja FEC i labele putem različitog protokola:

1. LDP (*label distribution protocol*)

Koristi TCP po portu 646, uspostavlja susedske odnose putem HELLO paketa i vrši razmenu labela i prefiksa. Jedan je od protokola koji se mogu koristiti za automatsku distribuciju informacija o labelama. LDP *peers* (susedi) su dva LSR-a (ili LER) koji koriste LDP za razmenu informacija o labelama kroz LDP sesiju.

2. MP BGP

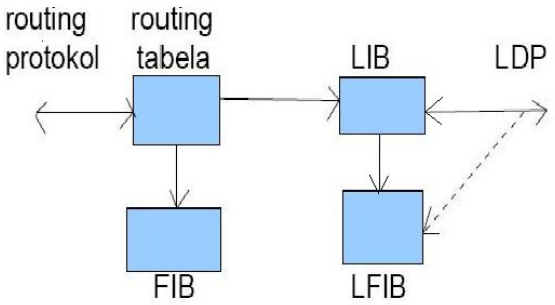
BGP/MPLS rešenje se zasniva na *peer connectionless* modelu što je i očekivano. Kao prvo, PE bazirane VPN mreže su veoma atraktivno rešenje sa stanovišta korisnika zbog jednostavnog rutiranja i lakog dodavanja novih VPN sajtova. Drugo, stare PE-zasnovane VPN su koristile običan IP u *Core* mreži za transport paketa. Tunelovanje je eliminisalo ovaj nedostatak, a MPLS u koru je omogućio potrebne tunele. BGP/MPLS VPN model je prvi put formalno izdat u RFC-u 2547, dokumentujući rešenje koje je razvio CISCO. Servis operatori su želeli da CISCO rešenje postane IETF standard. Oformili su novu grupu, zvanu PPVPN (*provider provisioned VPNs*). Ona standardizuje MPLS/VPN-ove koji se danas u praksi, iz prethodno navedenih razloga, zovu 2547bis. Ciljevi ovog VPN rešenja su:

- Razdvajanje saobraćaja između različitih VPN-ova

- Konekcija između korisničkih lokacija
- Korišćenje privatnog adresnog opsega na svim lokacijama

Tabele u MPLS ruterima:

- RT-*Routing Table* (dobijena na osnovu protokola rutiranja, tu se nalaze sve rute)
- FIB-*Forwarding Information Base* (izvedena iz ruting tabele nakon što je protokol rutiranja izračunao optimalnu putanju)
- LIB-*Label Information Base* (tabela koja povezuje svaku mrežu ili interfejs sa svakom labelom dobijenom preko LDP-a ili na drugi način)
- LFIB-*Label Forwrding Information Base* (izvedena iz LIB-a, koristi se za prosleđivanje)



Slika 2 Tabele u MPLS ruterima

Mreža treba da ispuni sledeće zahteve:

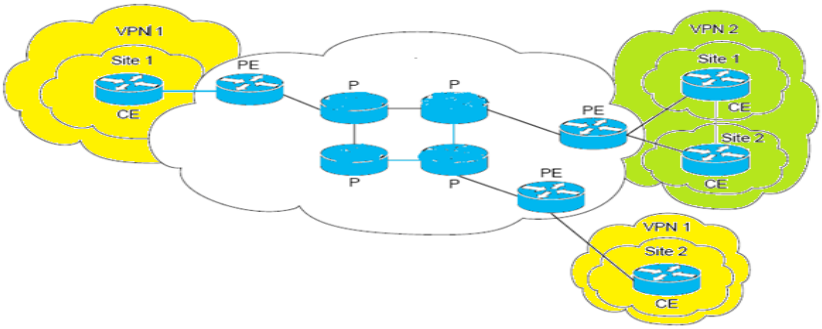
Privatnost-Sve VPN povezane preko zajedničke mreže moraju da obezbede privatnost. Ne sme se dozvoliti da korisnici unutar jedne VPN imaju uvid u drugu VPN, a da ova to ne želi.

Skalabilnost i Fleksibilnost-Infrastruktura treba da omogući lako dodavanje nove lokacije i lako dodavanje novog servisa u sistem. To znači da se prilikom dodavanja nove lokacije mora menjati konfiguracija što manje uređaja (skalabilnost), kao i to da jezgro ne zavisi od opreme na samim lokacijama i od tipa saobraćaja koji se prenosi; dakle system treba da ima jako fleksibilnu infrastrukturu koja će mu omogućiti prihvatanje i transport bilo kakvog tipa saobraćaja (fleksibilnost).

Predviđanje performansi-Različiti tipovi servisa različito zauzimaju resurse; potrebno je da predvidimo performanse tako da što je moguće bolje iskoristimo resurse koje imamo, dakle da na različite načine procesiramo različite korisnike i različite servise.

Ruteri u VPN se dele prema tome gde su u VPN-u ili kome pripadaju, tako da imamo:

- **CE-*Customer Edge router***
- **P-*Provider router***
- **PE-*Provider Edge router***



Slika 3 VPN-ovi sa okosnicom mreže

III. MP-BGP

BGP/MPLS rešenje se zasniva na *peer connectionless* modelu što je i očekivano. Kao prvo, PE bazirane VPN mreže su veoma atraktivno rešenje sa stanovišta korisnika zbog jednostavnog rutiranja i lakog dodavanja novih VPN sajtova. Drugo, stare PE-zasnovane VPN su koristile običan IP u *Core* mreži za transport paketa. Tunelovanje je eliminisalo ovaj nedostatak, a MPLS u koru je omogućio potrebne tunele. BGP/MPLS VPN model je prvi put formalno izdat u RFC-u 2547, dokumentujući rešenje koje je razvio CISCO. Servis operatori su želeli da CISCO rešenje postane IETF standard. Oformili su novu grupu, zvanu PPVPN (*provider provisioned VPNs*). Ona standardizuje MPLS/VPN-ove koji se danas u praksi, iz prethodno navedenih razloga, zovu 2547bis. Ova grupa je dugo izdavala standarde i za L2 i za L3 VPN-ove, dok sada postoje odvojene grupe. U ovom poglavlju ćemo biti reči o BGP/MPLS VPN-ovima. Ciljevi ovog VPN rešenja su:

- Razdvajanje saobraćaja između različitih VPN-ova
- Konekcija između korisničkih lokacija
- Korišćenje privatnog adresnog opsega na svim lokacijama

BGP *version* 4 (BGP-4) je godinama standardni protokol za rutiranje između domena. Praktično, on omogućava prenos saobraćaja na Internet mreži. Servis provajderi pokreću eBGP za rutiranje između svojih domena, a iBGP

unutar sopstvenih domena. BGP je protokol koji je sposoban da nosi stotine hiljada ruta. Jako je fleksibilan, i zahvaljujući tome razne politike rutiranja mogu biti primenjene. Iz svega ovoga, idealan je kandidat da se njime razmenjuju MPLS VPN rute. Kombinacija RD-a sa IPv4 rutom daje vpnv4 prefiks i takav prefiks je iBGP-om potrebno preneti između PE rutera.
Multiprotocol Extensions za BGP-4 definiše dva nova BGP atributa: *Multiprotocol Reachable NLRI* i *Multiprotocol Unreachable NLRI*. Ova dva atributa oglašavaju postojanje ili prestanak postojanja rute. Oba imaju isti format sa dva polja: *Address Family Identifier* (AFI) i Subsequent *Address Family Identifier* (SAFI). Zajedno opisuju koja vrsta rute se nosi BGP-om.

AFI/SAFI Format

Address Family Identifier (2 Octets)
Subsequent Address Family Identifier (1 Octet)

Slika 4 AFI/SAFI formati

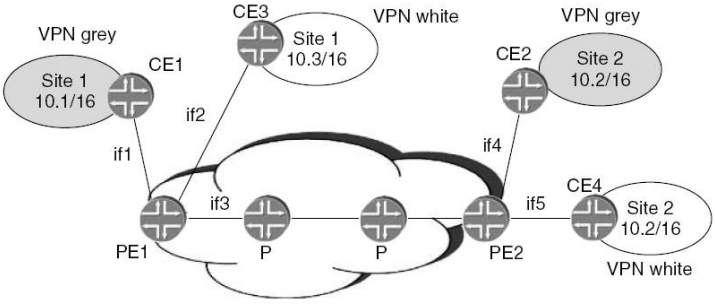
Some Address Family Numbers

Number	Description
0	Reserved
1	IP (IP version 4)
2	IP6 (IP version 6)
11	IPX
12	AppleTalk

Slika 5 Neke vrednosti AFI-ja

Kao što vidimo AFI nam govori tip adresiranja (IPv4, IPv6), a SAFI nam specifira da li je u pitanju *unicast*, *multicast* ili VRF. Za podršku *Multiprotocol*-arnih ekstenzija na CISCO IOS-u, u okviru konfiguracije BGP procesa koristi se koncept *address families*. Četiri *address families* su trenutno podržane: IPv4, IPv6, vpnv4 (VPN-IPv4), vpnv6 (VPN-IPv6).

Pod razdvajanjem saobraćaja između različitih VPN-ova podrazumeva se da korisnici iz jednog VPN-a ne mogu slati saobraćaj u drugi VPN. Slika 6 nam prikazuje 2 korisnička VPN-a označena sa „*Grey*“ i „*White*“:



Slika 6 VPN Grey i VPN White

Paketi ne mogu biti prosleđivani od sajta do sajta kao obični IP paketi. P ruteri uopšte nemaju VRF informacije. Ali prosleđivanje kroz okosnicu mreže nam je omogućeno zahvaljujući MPLS-u. Dakle, prosleđivanje paketa kroz okosnicu se radi na osnovu labela. P ruteri moraju imati samo korektnu informaciju o labelama na osnovu kojih će prosleđivati pakete.

Najčešće konfigurišemo LDP (*Label Distribution Protocol*) na svim P i PE ruterima, pa je ceo IP saobraćaj, kako se to u žargonu kaže, *label-switch*-ovan između njih. Takođe, možemo da izaberemo da koristimo ekstenziju RSVP protokola za *traffic engineering* (TE), u slučaju kada želimo da implementiramo MPLS TE u okosnici mreže.

Međutim, u slučaju MPLS VPN servisa najčešće se koristi LDP. Dakle, paket se prosleđuje na osnovu labela, kroz okosnicu od ulaznog do izlaznog PE rutera, pa P ruteri ne koriste *lookup* u *destination IP address*. Ove labele se nazivaju IGP labele, zbog toga što se labela veže za IPv4 prefiks iz globalne *routing* tabele u P i PE ruterima, koji oglašava IGP unutar mreže.

IV. TRAFFIC ENGINEERING

MPLS traffic engineering (MPLS TE) skup metoda kojima se optimalno iskorišćavaju resursi mreže. Osnovna ideja je da se kreira više *Label Switch Path*-ova (putanja od ulaznog PE-a do izlaznog PE-a) i na taj način da se racionalno koriste resursi mreže (kako imamo više LSP-ova moramo samim tim imati vise FEC-ova). Kriterijumi po kojima se svrstava po klasama su:

1. destinacija

2. propusni opseg (treba da se kreira LSP koji ima garanciju propusnog opsega)

3. Afinitet (32 "boje", recimo dupli link izmedju dva rutera, od kojih je jedan preko optike, drugi preko UTP kabla; tada kažemo da optika ima boju 3, a UTP boju 5. Npr. hoćemo da naš saobraćaj ide po boji 3)
4. *preemption* (preče pravo) (rasporediti saobraćaj po prioritetima; pa tako kažemo da ruterski saobraćaj je *max* prioritet, zatim recimo *real-time* saobraćaj i tako redom do recimo *http* saobracaja. Viši prioritet ima pravo da prekine saobraćaj nižeg; tako recimo ukoliko nema dovoljno propusnog opsega za dodelu višem prioritetu, bice prvo odbačen saobracaj nižeg i dodeljen protok višem prioritetu)
5. *fast reroute* (mehanizam kojim se omogućava brzo pronalaženje alternativne putanje (alternativni LSP). On se formira prilikom formiranja primarnog LSP-a)
6. Optimizovana metrika (Neka "druga" metrika pomoću koje se formiraju najkraće putanje u MPLS mreži)

Ako nijedan TE LSP ne zadovoljava uslove, potrebno je kreirati više različitih uslova za dati TE LSP (tipa ako prvi propusni opseg ne može da se dodeli, neka se dodeli drugi iz navedene liste i tako redom). Prilikom reoptimizacije ponovo se pokušava uspostavljanje primarnog kriterijuma.

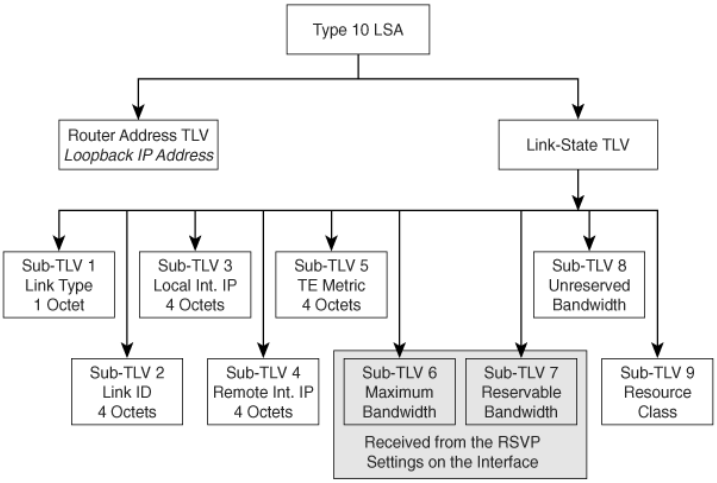
RSVP - Kako paket dolazi do "*headend*" rutera, ruter čita zeljeni propusni opseg, iz topologije odstranjuje sve linkove koji su manji od željenog propusnog opsega i računa dijkstra algoritam. Sada se šalju PATH poruke koje ispituju da li može da se rezerviše propusni opseg. Ako može poruka se prosledjuje do narednog rutera, ako ne odbacuje se (moguć dogadjaj odbacivanja zato sto "headend" ruter nema 100%-nu sliku mreže po pitanju propusnog opsega). Kada PATH poruka stigne do destinacije, destinacija šalje RESV poruku kojom rezerviše dati propusni opseg. RESV poruka sadrži Labelu! Što se reoptimizacije tiče, ukoliko je neka LSP završila, tada "lošija" LSP može da dobije putanju sa boljom metrikom.

Najvažniji zahtev MPLS TE-a je da ruteri u mreži imaju što bolju sliku trenutnog stanja u njoj. Za propagaciju ovih informacija se koriste ekstenzije IGP ruting protokola, tačnije ekstenzija OSPF-a, kao i ekstenzija IS-IS protokola. Ovi protokoli su po svojoj prirodi *link-state* protokoli, i omogućavaju *flooding updates* unutar mreže u slučaju promene stanja linkova, ili bolje rečeno kada je u pitanju TE, npr. informaciju o preostalom propusnom opsegu. Može se slobodno reći da su ekstenzije IGP protokola zadužene za transport informacija o stanju linkova, koje će kasnije biti korišćene za uspostavljanje dinamičkih TE tunela. *Link-state updates* se šalju kada se stanje linka promeni (na primer ručnom konfiguraciom ili je promenjen neki od atributa, npr. nakon uspostavljanja jednog LSP-a, dostupni opseg nije više isti), ili periodično da bi se potvrdilo trenutno stanje

(što je u prirodi *link-state* protokola), ili kada na LSP putanji koja je uspostavljena dođe do nekakvog kvara (otkaz rutera ili linka na toj putanji).

OSPF je odličan izbor za TE. Kao što znamo, to je *link-state protocol*, koji informacije o promenama stanja linkova oglašava *flooding*-om. Za potrebe TE, LSA paketi su veći, u sebi nose dodatne informacije, na osnovu kojih se posle radi CSPF. Postoji više tipova LSA. OSPF, takođe, sada poseduje TLV (Type-Length-Value) i sub-TLV atribute koji mogu biti konfigurisani da propagiraju informacije o dostupnosti resursa u *link-state update*-ima.
Najznačajniji LSA-ovi su tipovi 9, 10 i 11, od kojih se za TE skoro uvek koristi tip 10. CISCO trenutno jedino podržava ovaj tip koji se koristi za *flooding* unutar oblasti.

Tip 10 LSA, koji se koristi za TE, ima brojne TLV i *sub*-TLV vrednosti u kojima se nalaze specifične osobine nekog resursa (najčešće linka) u MPLS TE domenu. Na slici 7 vidimo od čega se sve sastoji tip 10 LSA.



Slika 7 Tipovi LSA paketa

Najznačajnije *sub*-TLV vrednosti korišćene u TE su 6, 7 i 8. Vrednosti za *sub*-TLV 6 i 7 se primaju iz RSVP konfiguracije na specifičnom interfejsu. *Sub*-TLV 8 definiše trenutno dostupni opseg za svaki od 8 prioriteta. Ova vrednost se definiše prilikom rezervacije na specifičnom interfejsu.

V. QOS

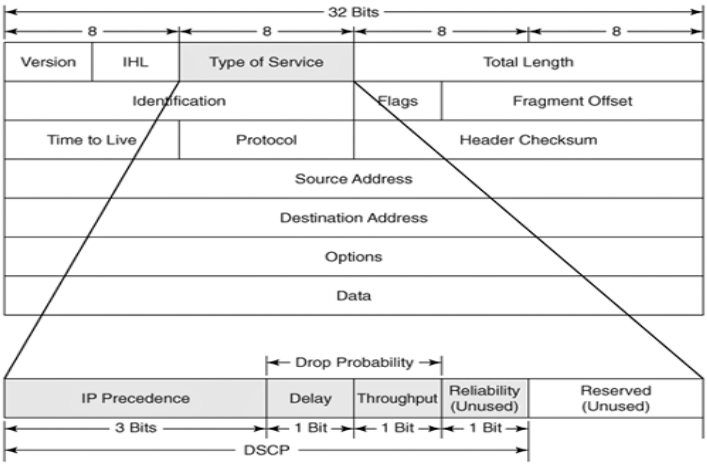
Osnovne osobine koje definišu kvalitet prenosa su:
1. gubici paketa - Najčesce zbog zagušenja u mreži. Naročito opasno kad koristimo UDP-a. Orijentaciono pravilo je da mreža treba da ima gubitke <1%.
2. kašnjenje - Za govor <150ms za žične i 250ms-300ms za satelitske komunikacije.
3. jitter - *jitter* za govor < 30ms

Propusni opseg je naravno najvažniji, iz prostog razloga što se ne mogu ispuniti QoS ukoliko nema dovoljno propusnog opsega. Isto tako i prevelik propusni opseg ne mora da znači da će pružiti bolji QoS od manjeg, ali dovoljnog propusnog opsega.
QoS zavisi od mnogo čega. Primer prioritiziranja saobraćaja je sledeći:

- **Gold-**transakcije i poslovni telefonski i operativni saobracaj
- **Silver**-*striming video*
- **Bronze (best effort)**-http
- **less than best effort-**FTP, P2P i sl.

Ovo je bilo prioritiziranje na osnovu aplikacija. Takođe, prioritiziranje se može raditi na druge načine.
Postoje 3 QoS modela:
1. Best effort - aplikacija šalje podatke koje hoće i koliko hoće, bez prethodne najave. Mreža isporučuje pakete, ako može, bez ikakvih garancija u pogledu pouzdanosti, kašnjenja i propusnosti.
2. Integrated Services(IntServ) - *IntServ*-aplikacija unapred zahteva specifičnu vrstu servisa u pogledu propusnosti i kašnjenja. Očekuje se da aplikacija počne da salje podatke, tek nakon što dobije odobrenje mreže. Aplikacije koriste RSVP. Postoje dva tipa RSVP servisa:
-*Guaranteed rate service*-rezerviše propusni opseg koji ce biti ispostovan
-*Controlled load Service*-teži se malom kašnjenju i velikom proposnom opsegu, ali to ne mora da bude ispoštovano.
3. Differentiated Services(DiffServ) - *DiffServ*- model koji se najviše koristi za realizaciju QoS. Osnovne QoS tehnike nad paketima:
a. Klasifikacija i obeležavanje
b. Ograničavanje i poravnavanje
c. Kontrola zagušenja
d. Izbegavanje zagušenja
e. Specifične tehnike na linku

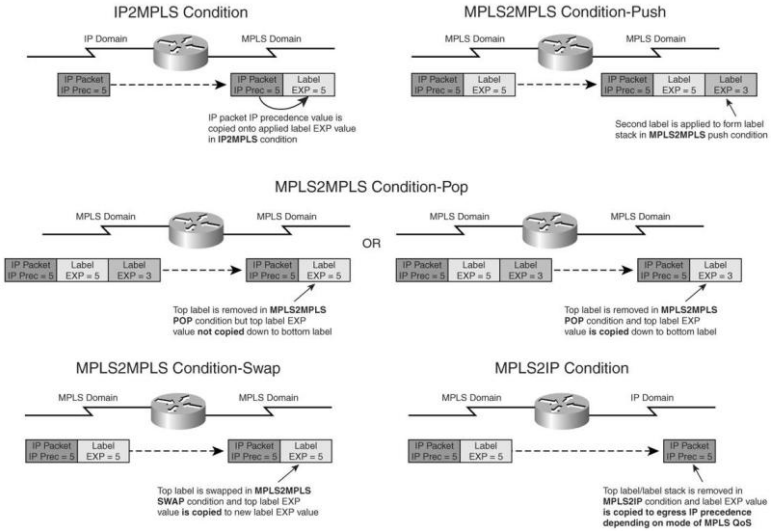
Cilj je da se saobraćaj razvrsta na više klasa, koje će imati različite QoS tretmane. Može da se razvrsta po kriterijumima na bilo kom *layer*-u. Obeležavanje treba raditi sto je moguće pre, a idealno je da se to uradi na granici mreže, na pristupnom sloju. Ukoliko je reč o L2 sloju imamo CoS (*class of service*), a ako je reč o L3 imamo ToS (*Type of service*) polje. DSCP jeste bolje iskorišcenje ToS polja.Veoma je bitno gde se saobraćaj obeležava. Ako se radi na L2 sloju, to je saobraćaj koji nije namenjen za IP, ali se drugačije ne može obezbediti QoS u LAN-u. Zbog navedenog radi se sledeće: ulazni *switch* postavlja CoS vrednost i nakon toga LAN ruter prilikom slanja van LAN-a translira odgovarajuću CoS vrednost u odgovarajuću ToS ili DSCP.



Slika 8. IP Packet Header

Kada implementiramo QoS preko MPLS infrastrukture, *Edge* LSR između IP i MPLS domena mora raditi prevođenje IP QoS u MPLS QoS, ili obrnuto. Ako IP paket ulazi u MPLS domen (na primer na putu od CE ka PE), ovo se naziva IP2MPLS slučaj. U nekim situacijama, paket sa jednom labelom koji dođe u P ruter, napušta ruter sa drugom labelom i promenjenim EXP poljem; ovo je MPLS2MPLS slučaj. Konačno, kada labelovan paket mora da napusti MPLS domen (na izlaznom LER ruteru), to se naziva MPLS2IP slučaj.

Kada imamo IP2MPLS slučaj, procedura na ulaznom PE ruteru je sledeća: IP *Precedence* vrednost iz IP paketa se kopira u MPLS EXP polje, kao što ćemo videti na Slici 9.



Slika 9. *MPLS QoS Implementation and Function*

U slučaju MPLS2MPLS situacije, dolazni paket je labelovan paket. Prema tome, u ovom slučaju 3 akcije su moguće, i one se nazivaju *Push, Pop* i *Swap*. Sve ove slučajeve možemo videti na prethodnoj slici.

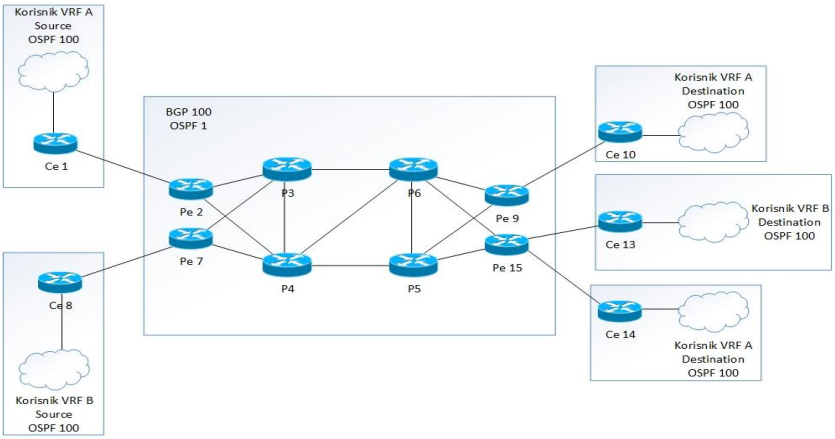
U slučaju MPLS2IP, dolazni paket je labelovan paket, a odlazni paket je običan IP paket. U ovom slučaju, EXP vrednost se kopira nazad u IP *precedence* vrednost.

VI. SIMULACIJA I ANALIZA REZULTATA

Na slici 10 je prikazana topologija mreže koja je konfigurisana i na kojoj su rađeni testovi. Alati koji su se koristili za simulaciju su:

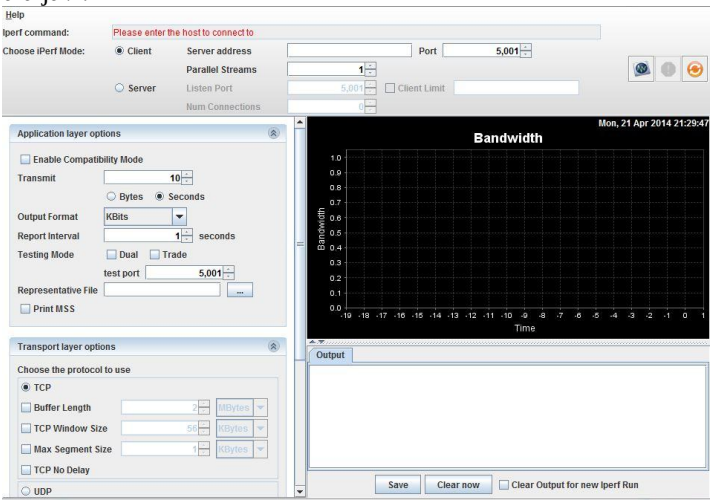
- GNS 3 – U njemu smo radili celokupnu topologiju mreže i konfiguraciju uređaja
- Vmware Workstation – Na njemu smo podigli hostove (Ubuntu Linux, Windows 7) čiji virtuelni mrežni interfejs je diretkno povezan na GNS3 topologiju. Svaki oblak na topologiji predstavlja po jedan virtuelni host.
- Iperf i Jperf – Jperf je grafički interfejs Iperf alata koji smo koristili za generisanje saobraćaja i analizu saobraćaja kroz grafički interfejs

- D – ITG – Alat koji smo koristili za generisanje i detaljnu analizu saobraćaja u tekstualnom obliku



Slika 10. Topologija mreže

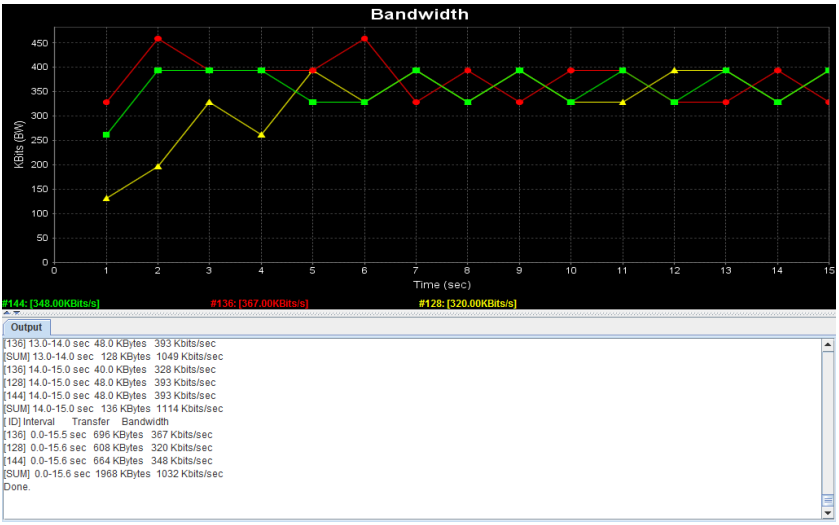
Iperf je najčešće korišćen mrežni alat za testiranje, koji može generisati Transmission Control Protocol (TCP) i User Datagram Protocol (UDP) pakete podataka i izmeriti propusni opseg mreže. Iperf je alatka za merenje performansi mreža pisana u C-u. Jperf je GUI *front-end* aplikacija Iperf-a pisana u javi.



Slika 11. Jperf

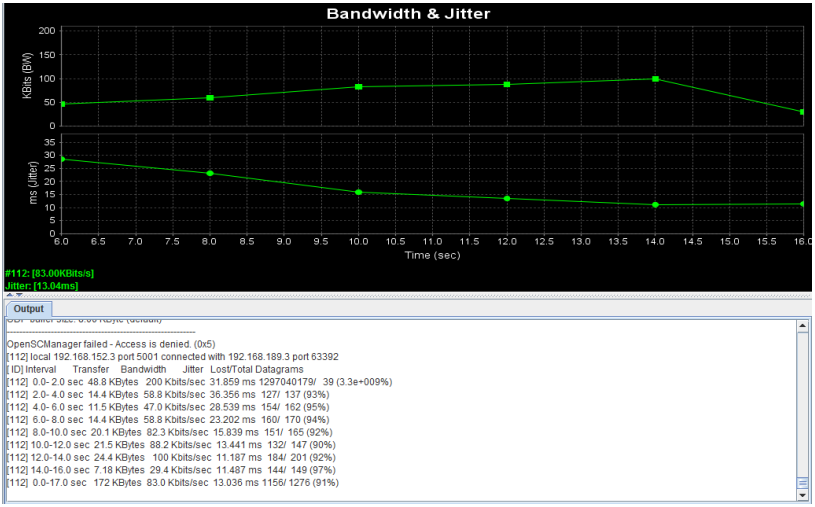
Server se pokreće na source strani VPN_A korisnika sa adresom 192.168.152.3. Postavićemo 3 različita toka podataka pod opcijom *Num Connections* po portu 5001.

Na slici 12 su rezultati na destination strani:



Slika 12. Rezultati

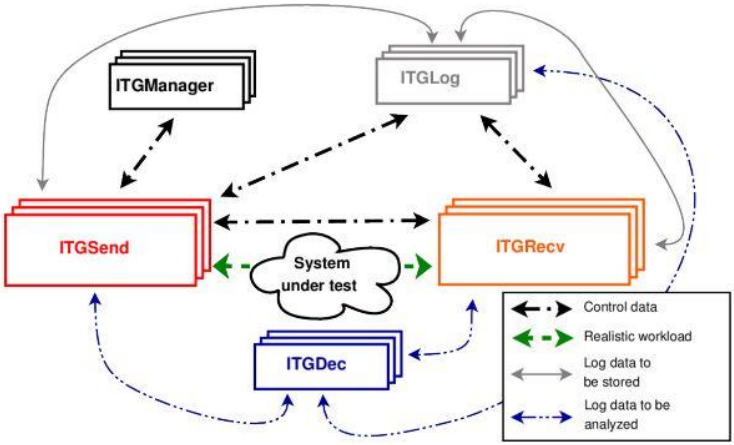
Ovo su rezultati na source strani:



Slika 13. Rezultati

D - ITG je platforma sposobna da proizvede IPv4 i IPv6 saobraćaj i tačno replicira opterećenje postojećih internet aplikacija. Istovremeno D - ITG je takođe instrument može da meri najčešće pokazatelje učinka (npr. propusna moć, kašnjenje , jitter, gubitak paketa) na nivou paketa. D - ITG može generisati saobraćaj stohastičkim modelom za veličinom paketa (PS) i inter polaska (IDT) da koji imitiraju ponašanje aplikacija na nivou protokola. D - ITG je u stanju da pokaže statističke osobine saobraćaja različitih poznatih aplikacija (npr. telnet , VoIP - G.711 , G.723 , G.729 , *Voice activity detection*, kompresovan RTP - DNS , mrežne igre). Na transportnom sloju , D - ITG trenutno podržava TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), SCTP1 (*Stream Transmission Control Protocol*) , i DCCP1 (*Datagram Congestion Control Protocol*).On takođe podržava ICMP (*Internet Control Message Protocol*) . Među nekoliko dole navedenih karakteristikama , FTP pasivni režim je takođe podržan da sprovede eksperimente u prisustvu NAT-a, a moguće je podesiti TOS (DS) i TTL IP zaglavlja polja. Arhitektura D-ITG je prikazana na slici 11.

Glavne komponente su ITGSend i ITGRecv. ITGSend služi za generisanje saobraćaja prema ITGRecv. Koristeći *multithread* dizajn, ITGSend može poslati paralelno više tokova saobraćaja prema ITGRecv, koji takođe može primiti više tokova saobraćaja. Signalni kanal je napravljen izmedju komponenti kako bi se kontrolisao tok saobraćaja između njih. Postoje log fajlovi koji mogu da se naprave nakon izvrsenog generisanja saobraćaja, mogu da se sačuvaju lokalno ili udaljeno, u ITGlod komponentu(korisno radi skladištenja svih merenja na jedno mesto). Log fajlovi se snimaju u kriptovanom formatu, a komponenta ITGDec ih dekriptuje.



Slika 14. D-ITG

Paketi se šalju u istom vremenskom intervalu, veličina im varira. Primer testa se izvodi tako što se na destinacionom hostu koji ima adresu 192.168.189.3 pokrene ITGRecv, koji sluša pakete. Na hostu koji šalje pakete, čija je adresa 192.168.152.3 se otkuca sledeća komanda:

```
ITGSend -a 192.168.189.3 -rp 9501 -C 1000 -u 500
1000 -l send_log_file
```

Na hostu koji prima pakete:

```
ITGRecv -l recv_log_file
```

-a – na koju adresu šaljemo
-rp – destinacioni port
-C – konstantan protok 1000 packets/s
-u – veličina paketa varira izmedju 500-1000 bajtova
-l – uključujemo logovanje u send_log_file na predajnoj strani

Dekodujemo outpute komandom: ITGDec recv_log_file i ITGDec send_log_file:

********** TOTAL RESULTS **********

TCP Test 1	
Number of flows	1
Total time	11.719000 s
Total packets	1159
Minimum delay	0.091000 s
Maximum delay	1.850000 s
Average delay	1.650582 s
Average jitter	0.007634 s
Delay standard deviation	0.370000 s
Bytes received	872811
Average bitrate	595.826265 Kbit/s
Average packet rate	98.899223 pkt/s
Packets dropped	8818 (88.38 %)
Average loss-burst size	13.821317 pkt
Error lines	0

Tabela 1. Rezultati

Generisanje voice saobraćaja se obavlja na sledeći način:

- Na *reciever* hostu pokrenemo: ITGRecv -l recv1_log_file
- Na *source* hostu napravimo skriptu:
- cat > script_file <<END
  -a 192.168.189.3 -rp 10001 VoIP -x G.711.2 -h RTP –VAD
  END
- Na source hostu pokrenemo: ITGSend script_file -l send_log_file
- Dekodujemo outpute, na *source* hostu send_log_file sa outputom:

********** TOTAL RESULTS **********

Number of flows	2
Total time	10.071890 s
Total packets	953
Minimum delay	0.000000 s
Maximum delay	0.000000 s
Average delay	0.000000 s
Average jitter	0.000000 s
Delay standard deviation	0.000000 s
Bytes received	110548
Average bitrate	87.807154 Kbit/s
Average packet rate	94.619778 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0 pkt
Error lines	0

Tabela 2. Rezultati

Dekodujemo outpute, na *reciever* hostu recv_log_file sa outputom:

********** TOTAL RESULTS **********

Number of flows	2
Total time	10.027659 s
Total packets	951
Minimum delay	0.031162 s

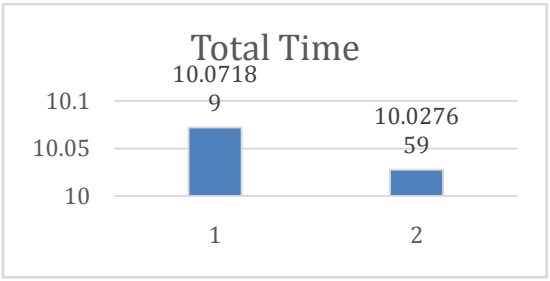
Maximum delay	0.074110 s
Average delay	0.048258 s
Average jitter	0.002023 s
Delay standard deviation	0.007978 s
Bytes received	110316
Average bitrate	88.009375 Kbit/s
Average packet rate	94.837688 pkt/s
Packets dropped	1 (0.11 %)
Average loss-burst size	0.000000 pkt
Error lines	0

Tabela 3. Rezultati

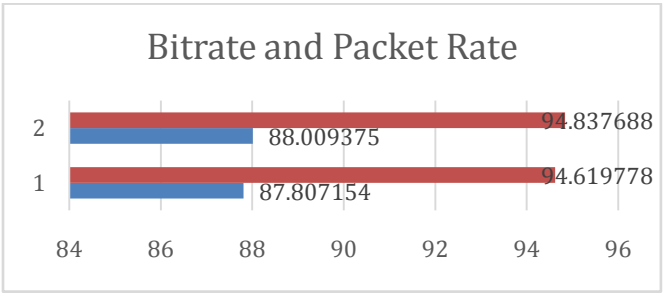
Kada uporedimo rezultate na *souce* i *destination* strani dobijamo:

Number of flows	2		Number of flows	2
Total time	10.071890 s		Total time	10.027659 s
Total packets	953		Total packets	951
Minimum delay	0.000000 s		Minimum delay	0.031162 s
Maximum delay	0.000000 s		Maximum delay	0.074110 s
Average delay	0.000000 s		Average delay	0.048258 s
Average jitter	0.000000 s		Average jitter	0.002023 s
Delay standard deviation	0.000000 s		Delay standard deviation	0.007978 s
Bytes received	110548		Bytes received	110316
Average bitrate	87.807154 Kbit/s		Average bitrate	88.009375 Kbit/s
Average packet rate	94.619778 pkt/s		Average packet rate	94.837688 pkt/s
Packets dropped	0 (0.00 %)		Packets dropped	1 (0.11 %)
Average loss-burst size	0 pkt		Average loss-burst size	0.000000 pkt
Error lines	0		Error lines	0

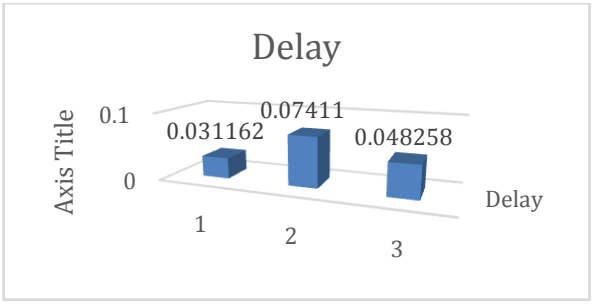
Tabela 4. Rezultati



Slika 15 Ukupno vreme



Slika 16 *Bitrate i Packet Rate*



Slika 17 Kašnjenje

VII. ZAKLJUČCI I PREPORUKE

Postoji mnogo razloga koji utiču na primenu MPLS-a, ali je inženjering saobraćaja *(Traffic Engineering)* najveći. Inženjering saobraćaja se bavi optimizacijom rada već instaliranih mreža kombinujući različita saznanja iz teorije saobraćaja. Cilj je da se optimalno iskoriste resursi mreže i da se poboljša kvalitet usluga koje se nude. Inženjering saobraćaja 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).

U okviru projekta predstavljeno je rešenje za realizaciju Core mreže multiservisnog provajdera koja podržava prenos različitih aplikacija i servisa. Mreža je sposobna da podrži različite različite servise koje su danas zastupljeni kao što su prenos govora, multimedijalne aplikacije, *on-line* igre i mnoge druge. Takođe, predstavljeno rešenje je veoma skalabilno jer su predložen dizajn i topologija lako nadogradivi u slučaju da se mreža širi i da se povećava broj korisnika i aplikacija.

Prilikom dizajniranja tehničkog rešenja maksimalno se vodilo računa i o budućim potrebama korisnika tako da se predloženo rešenje može prilagoditi svim očekivanim budućim zahtevima korisnika.

Korišćeni su moćni alati na kojima je urađena je detaljna analiza saobraćaja i analiza QoS parametara alatima kako na linux tako i na windows platformi. Rezultati verno prikazuju QoS parametre *jitter,* gubitak paketa i kašnjenje, preko kojih možemo jasno odlučiti kako da prioritizujemo saobraćaj radi što boljih rezultata.

Treba uzeti u obzir da je sve urađeno u virtuelnom okruženju, tako da testovi ne oslikavaju u potpunosti realno stanje ali daju detaljan uvid u prirodu i karakteristike prenosa u mrežama nove generacije.

LITERATURA

[1] http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html
[2] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html
[3] http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html
[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-cfg-layer3-vpn.html
[5] http://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/15_0s/mp_15_0s_book/mp_vpn_gre.html
[6] http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swqos.html
[7] http://en.wikipedia.org/wiki/Iperf
[8] http://iperf.fr/

ABSTRACT

Traffic engineering deals with the optimization of work in already installed networks combining different knowledge of the theory of traffic. The aim is to optimally utilize network resources and to improve the quality of services offered. Traffic engineering can be oriented to improve traffic flows and service parameters or to improve utilization of network resources. One of the functions of the label is to provide a mechanism that integrates with the packet in the routing process, and in this way provide "guidance" of packet at a predetermined paths through the network. With further administrative manipulations it is possible to provide manual load distribution in the network and thus the maximum utilization of the available bandwidth in the network (it is possible that some, most attractive parts of the network carry the maximum load, while other parts remain unused).

Inženjering saobraćaja u MPLS VPN mrežama

Ognjen Josipović