Simulacija MPLS mreže u Dynamipsu

Marinko Smiljanić
Vojna akademija u Beogradu

Sadržaj – U ovom radu razmotreno je rešenje pouzdanog prenosa informacija preko javnih mreža. Ovo je moguće ostvariti primenom virtuelnih privatnih mreža. Objašnjena je tehnika višeprotokolske komutacije labela, kao pogodna tehnika za podršku privatnim mrežama. Za potrebe rada napravljena je simulacija jedne takve mreže i pokazana je privatnost poruka koju razmenjuju korisnici sa različitih lokacija.

Ključne reči – Dynamips, IP, komutacija labela, virtuelne privatne mreže

I.UVOD

Mreže zasnovane na Internet protokolu *IP (*engl. *Internet Protocol)* dominiraju u oblasti telekomunikacionih mreža u ovoj deceniji. S obzirom na svoju jednostavnost Internet servisi kao što su WWW, e-mail, FTP (engl. *File Transfer Protocol*) itd. postali su opšte prihvaćeni standardi i uneli su pravu revoluciju i u život običnog čoveka. Više se skoro i ne može zamisliti rad bez mogućnosti pristupa Internetu, a E-biznis i intraneti i ekstraneti su neminovnost današnjeg poslovanja. Usled toga broj korisnika sve više raste (broj hostova na Internetu se približno udvostručava svake godine), ali rastu i zahtevi korisnika u pogledu brzine, vrste i kvaliteta ponuđenih servisa. Pored toga sve je izraženija potreba za multimedijalnom primenom što zahteva mnogo više od mreže nego što je tradicionalni put saobraćaja preko Interneta.

Internet protokol sam po sebi ne nudi nikakvu mogućnost obezbeđivanja kvaliteta servisa korisnicima (nema mogućnosti QOS (engl. *Quality of Service)* garancije). Znači, veliki problem za provajdere internet servisa *(*engl. *Internet Service Provider)* je da ponude rešenja koja će omogućiti skalabilnost ali i ponudu ugovorenog kvaliteta usluge SLA, (engl. *Service Level Agreement)*. Kako bi svi ti uslovi bili zadovoljeni vremenom su se javljali mnogi protokoli koji su svaki od problema rešavali pojedinačno. Uvođenje protokola kao što su: protokol rezervacije resursa RSVP (engl. *Recourse Reservation Protocol)*, diferencijalni servisi DiffServ (engl. *Differentiated services)*, sve je više komplikovalo rutiranje. Razvojem ATM (engl. *Asynchronous Transfer Mode)* tehnologije, koja je ponuđena za izgradnju okosnice (*backbone)* Interneta omogućen je prenos podataka i multimedijalnih informacija preko jedne mreže poštujući pri tome dogovoren kvalitet servisa. Ipak problem preslikavanja IP protokola u ATM je kompleksan i usled svoje komplikovanosti i problema skalabilnosti i za sada ne predstavlja pravo rešenje. Tako, da bi se zadovoljile potrebe za skalabilnošću, boljim performansama rutiranja, upravljanjem saobraćajem na osnovu administrativno zadatih pravila itd. započet je rad na definisanju novog protokola zasnovanog na komutaciji korišćenjem labela.

II. KARAKTERISTIKE MPLS PROTOKOLA

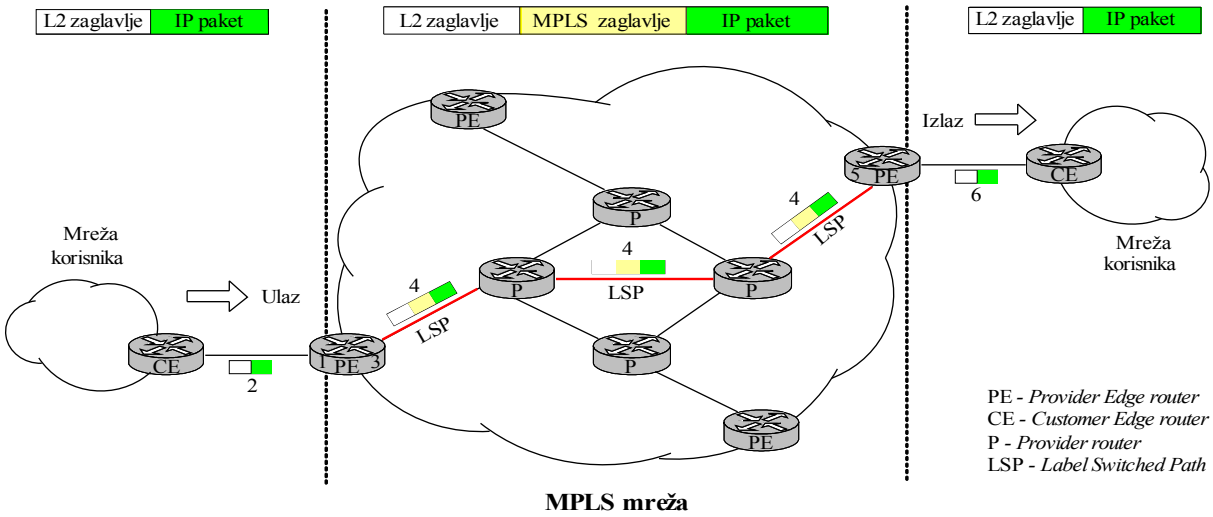
MPLS (*engl*. *MultiProtocol Label Switching*), razvijen od strane IETF-MPLS grupe 1997. godine predstavlja tehniku komutacije labela između linkova kojom se podržava više različitih protokola (engl. *multiprotocol*) sa mrežnog sloja OSI modela, dok odrednica (engl. *label switching*) označava upotrebljenu tehniku komutacije labela između linkova .[1]

Komutacija labela višestrukim protokolom, MPLS, predstavlja arhitekturu u okviru IETF standarda koja omogućava takvo upravljanje saobraćajem i QoS podršku, čijom primenom se ubrzava prosleđivanje paketa. Prosleđivanje paketa se vrši na osnovu labela (etiketa) kratke dužine koje se smeštaju između zaglavlja sloja linka podataka i sloja mreže. Na osnovu sadržaja labele vrši se prosleđivanje paketa kroz mrežu, pri čemu je značaj labele na lokalnom nivou. Na ovaj način se izbegava veliko kašnjenje pri prenosu paketa. Pri usmeravanju paketa kroz čvor, labela se skida sa paketa i menja se odgovarajućom kojom se dalje usmerava kroz mrežu. Ovim mehanizmom se postiže velika brzina prenosa kroz kičmenu MPLS mrežu. MPLS smanjuje iznos procesiranja po paketu koji je potreban kod svakog rutera u mreži sa IP, povećavajući još više performanse rutera. MPLS kombinuje karakteristike IP rutiranja na trećem nivou i komutacije na drugom sloju. Zbog toga se ovaj protokol ponekad naziva protokol sloja „2½“. Dok ruteri zahtevaju inteligentan mrežni nivo koji određuje gde treba proslediti pakete, sa druge strane komutatori imaju jednostavan zadatak da pošalju paket na sledeći čvor, i samim tim su jednostavniji, brži i jeftiniji.

Kod MPLS-a prenos podataka se vrši preko putanja komutiranih na osnovu labele LSP (engl. *Label-Switched Paths*). To je sekvenca labela na svakom pojedinačnom čvoru duž puta od izvora do odredišta. LSP se uspostavljaju ili pre prenosa podataka (engl. "*control-driven*") ili po detekciji određenih tokova podataka (engl. "*data-driven*"). Labele, na kojima se baziraju specifični identifikatori za protokol, prosleđuju se korišćenjem protokola za prosleđivanje labela LDP (engl. *Label Distribution Protocol*), korišćenjem protokola rezervacije resursa, ili pak uz pomoć protokola rutiranja kao što su protokol graničnog mrežnog prolaza BGP (engl. *Border Gateway Protocol*) i OSPF (engl. *Open Shortest Path First)*. Svaki paket podataka sa sobom nosi labele tokom svog puta do odredišta. Velika brzina komutacije podataka moguća je jer su labele fiksne dužine umetnute na samom početku paketa (ili ćelije) i mogu biti iskorišćene za brzu komutaciju paketa između linkova.

Rad MPLS mreža, predstavljen na Sl.1, bazira se na sledećim elementima i funkcijama:

CE (engl. *Customer Edge*) – pristup korisnika,



Sl.1 Osnovni elementi MPLS mreže

PE (engl. *Provider Edge*) ili LER (engl. *Label Edge Router*) – ulazni ruter sa labelom.

1. Pre nego što se saobraćaj prosledi kroz MPLS mrežu, PE (LER) ruteri uspostavljaju LSP putanje prema ostalim ruterima.
2. Saobraćaj koji ne pripada MPLS domenu (*Frame Relay*, ATM, *Ethernet* i dr.) šalje se od strane korisničke mreže preko CE rutera ka ulaznom PE ruteru na granici MPLS mreže.
3. PE ruter dodeljuje paket određenoj klasi FEC (engl. *Forwarding Equivalence Class*), a zatim dodaje ogovarajuću MPLS labelu (labele) paketu.
4. Paket se dalje šalje preko LSP, pri čemu svaki unutrašnji P (engl. *Provider*) ruter menja labele shodno informaciji iz LIB-a (engl. *Label Information Base*) radi prenosa paketa prema sledećem skoku.
5. Na izlaznom PE ruteru se uklanja poslednja labela i paket se dalje prosleđuje na bazi tradicionalnih postupaka rutiranja.
6. Na kraju paket se prenosi ka odredišnom CE ruteru i dalje ka korisničkoj mreži.

Pošto je uspostavljena signalizacija u mreži, svaki MPLS ruter stvara informacionu bazu o labeli (LIB), odnosno tabelu koja određuje kako se paketi prosleđuju. Ova tabela povezuje svaku labelu sa odgovarajućim FEC-om i izlaznim portom kako bi se usmeravali paketi kroz mrežu. LIB se uspostavlja sa sličnom ulogom kao i informaciona baza prosleđivanja, FIB (engl. *Forwarding Information Base*) koja se javlja kod tradicionalnih rutera.

III. VIRTUELNE PRIVATNE MREŽE

Virtuelne privatne mreže VPN (engl. *Virtual Private Networks*) nude sposobnost da se obavljaju privatne komunikacije preko javne mreže kao što je Internet. Termin se odnosi na kombinaciju tehnologija i tehnika koje osiguravaju komunikacije između dve krajnje tačke uspostavljanjem tunela neprobojnog za prisluškivanje i ometanje.

Postoje dva tipa praktične realizacije mreže preko koje mogu da se ostvare VPN. To su pokriveni (engl. *Overlay*) i ravnopravni (engl. *Peer*) model.[2]

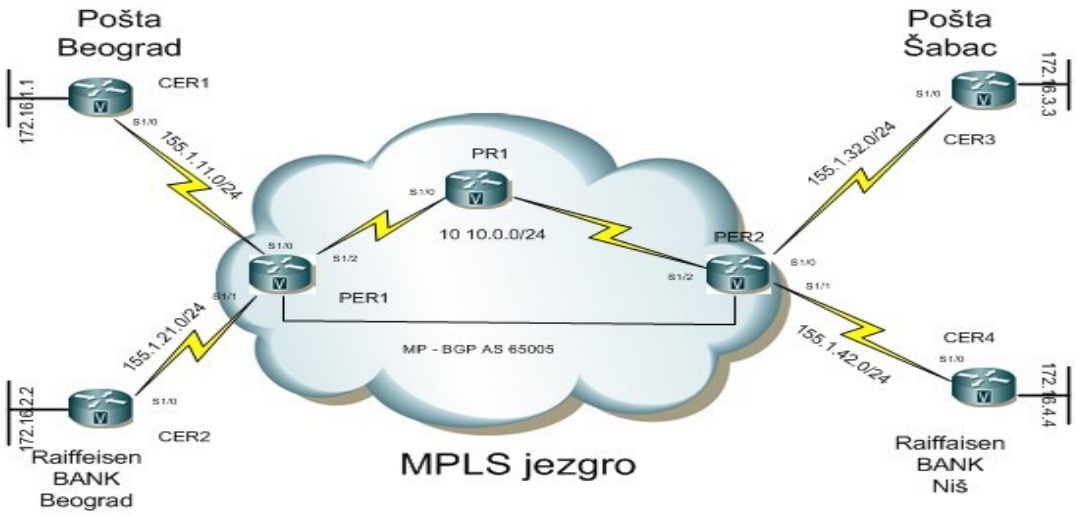
Ravnopravni model će najverovatnije potisnuti pokriveni model. Iako su VPN rešenja zasnovana na ovom drugom modelu uobičajena danas, ovi tipovi rešenja imaju nekoliko velikih problema koji ograničavaju razvoj VPN servisa. *Overlay* model zasniva se na kreiranju veza, a ne mreža. Svako mesto (čvor) poseduje ruter koji je povezan linkovima tačka-tačka do rutera na drugim mestima unutar VPN-a. Ovo komplikuje, odnosno povećava broj potrebnih izmena u konfiguraciji, prilikom dodavanja novog čvora u postojeću mrežu. Kod VPN-a gde se zahteva potpuna povezanost čvorova u mreži, to uključuje promene u konfiguraciji na svim postojećim čvorovima, zbog toga što je svakom od njih potrebna dodatna veza tačka-tačka do tog novog mesta.

Zbog toga VPN koriste *peer* model i nekonektivnu arhitekturu na sloju 3. *Peer* model zahteva da korisnički čvor "gleda" na samo jedan PE ruter, nasuprot svim drugim CE ruterima ili krajnjim korisničkim ruterima u istoj VPN. Nekonektivna arhitektura dozvoljava kreiranje VPN-a na sloju 3, eliminišući potrebu za tunelima.

MPLS obezbeđuje efikasan mehanizam za podržavanje VPN. Sa VPN, saobraćaj određene grupe korisnika prolazi transparentno kroz mrežu na način koji uspešno razvrstava taj saobraćaj od ostalih paketa u mreži, pružajući garancije u pogledu performansi i sigurnosti.

Ove mreže moraju da budu skalabilne, ekonomične i sposobne da izađu u susret širokom opsegu zahteva korisnika, gde spadaju pouzdanost i sigurnost, kvalitet servisa i mogućnost povezivanja svakog-sa-svakim. One moraju da ponude kompletno pružanje multimedijalnih servisa kako bi privukle nove korisnike. MPLS se javlja kao ključna tehnologija za mreže nove generacije, posebno u optičkim mrežama. VPN bazirane na MPLS obezbeđuju fleksibilnu povezanost i skalabilnost što su odlike mreža sa IP, kao i tajnost i kvalitet servisa.

S obzirom na to da MPLS bazirane VPN umanjuju kompleksnost i cenu mreže, one dozvoljavaju davaocima servisa da svoje usluge pružaju mnogo raznovrsnijoj bazi malih i srednjih organizacija i ustanova. Za realizaciju MPLS VPN mreža je dovoljna samo jedna konekcija od njihovog rutera do krajnjeg rutera provajdera. Krajnji



Sl.2 Praktičan primer MPLS mreže

ruter stavlja labele na pakete i prenosi ih kroz MPLS jezgro sve do krajnjeg rutera najbližeg odredištu. Sa ovom tehnologijom, davaoci servisa sada mogu ponuditi korisnicima VPN sa QoS, omogućenim Internetom, intranetom i ekstranetom, i paketskom telefonijom bez kompleksnosti koje su ove aplikacije prethodno zahtevale kako bi proširile servisne ponude i stvorile dodatne prihode.

IV. PRAKTIČAN PRIMER MPLS MREŽE U DINAMIPSU

Za potrebe ovoga rada, napravljena je simulacija MPLS mreže u Dynamips-u. *Dynamips* je Cisco ruter simulator, koji može da simulira 2691, 3620, 3640, 3660, 3725, 3745 i 7206 Cisco rutere.[3]

Simulacija sadrži sedam rutera Cisco serije 3600, tačnije Cisco 3640. Tri rutera čine MPLS jezgro, dok četiri rutera predstavljaju rutere ka opremi korisnika. Postoje dva korisnika. **Korisnik 1 -** Pošta, koji je lociran na dve lokacije, u Beogradu i u Šapcu. **Korisnik 2** - Raiffeisen BANK, takođe ima korisnike na dve lokacije, jedan u Beogradu, a drugi u Nišu.

Korišćena su dva protokola rutiranja. MP – BGP (engl. *Multi Protocol Border Gateway Protocol*), koji je iskonfigurisan između PER1 i PER2 rutera i igra ulogu mrežnog prolaza između dve mrežne grupe.

Ovaj protokol davaoci Internet usluga koriste za međusobnu razmenu informacija o usmeravanju. Nije uobičajeno da davalac usluga korisniku pruža uslugu usmeravanja pomoću protokola BGP, ali je to moguće kada korisnik ima više lokacija ili kada je povezan na više davalaca Internet usluga. Protokol BGP je je projektovan za usmeravanje između velikih mreža; svakom od graničnih usmerivača (davalaca Internet usluga) omogućava preko sto hiljada putanja, čime se postiže efikasno prosleđivanje podataka kroz Internet.

Drugi protokol je OSPF. To je protokol rutiranja sa otvorenim standardima, koji implementira veliki broj proizvođača mrežnih uređaja, uključujući i Cisco. [4]

Koristi algoritam Dijkstra. Prvo se konstruiše stablo najkraće putanje, a zatim se tabela rutiranja popunjava najboljim rezultirajućim putanjama. OSPF vrši brzu konvergenciju i podržava više ruta jednakih troškova do istog odredišta. On je protokol rutiranja stanja veze i kao metriku putanje koristi propusni opseg.

Šema simulacije je prikazana na Sl.2. Na slici vidimo da MPLS jezgro čine PER1, PR1 i PER2 ruteri. Na ruterima PER1 i PER2 vrši se redistribucija, tj. ubacivanje ruta iz jednog protokola u drugi, iz OSPF u BGP i obratno.

Ivični ruteri, PER1 i PER2 ruteri, smeštaju informacije o rutiranju u tabelu virtuelnog rutiranja i usmeravanja, (engl. *Virtual Routing and Forwarding)*. Ovi ruteri upravljaju različitim VRF tabelama za svaku VPN, na taj način obezbeđujući razdvojenost i zaštitu svake posebno. Znači, Pošta u Beogradu ne bi trebala da ima u svojoj tabeli rutiranja IP adresu Raiffeisen BANK-e u Nišu i u Beogradu.

Komanda *show ip route* direktno će nam omogućiti uvid u tabele rutiranja prisutne na ruteru. U tabeli 1 prikazana je tabela rutiranja na ruteru CER1.

TABELA 1. TABELA RUTIRANJA RUTERA CER1

```
CER1#show ip route
Codes: 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

Gateway of last resort is not set

    155.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       155.1.11.0/24 is directly connected, Serial1/0
C       155.1.11.11/32 is directly connected, Serial1/0
O IA        155.1.32.3/32 [110/65] via 155.1.11.11, 00:28:01, Serial1/0
```

```
O IA      155.1.32.0/24 [110/65] via 155.1.11.11, 00:28:01, Serial1/0
    172.16.0.0/32 is subnetted, 4 subnets
O IA      172.16.22.22 [110/65] via 155.1.11.11, 00:28:01, Serial1/0
O      172.16.11.11 [110/65] via 155.1.11.11, 00:56:25, Serial1/0
O IA   172.16.3.3 [110/129] via 155.1.11.11, 00:28:01, Serial1/0
C      172.16.1.1 is directly connected, Loopback0
```

Iz ove tabele mogu da se vide rute koje je pronašao OSPF za ruter CER1. Vidi se i veza sa mrežom 155.1.32.0/24, koja predstavlja mrežu u kojoj je ruter CER3. Takođe se vidi da u sadržaju tabele je i IP adresa virtuelnog interfejsa 172.16.3.3, koji simulira ono što se u realnoj situaciji može nalaziti iza rutera, a to je obično neka mreža koju održava sam korisnik.

U tabeli rutiranja rutera CER1 nema rute do mreže 155.1.42.0/24, koja predstavlja mrežu sa ruterom CER4. Znači, podaci koji se šalju sa rutera CER1 biće prosleđivani samo na CER3.

Postoji još jedan način da se proveri privatnost poruka između različitih korisnika. Poruke koje razmenjuje Korisnik 1 ne smeju da završe na ruterima koji pripadaju Korisniku 2.

U *Dynamips*-u ovo je omogućeno komandom *ping*. Ova komanda omogućava proveru konektivnosti bazičnim testom slanja ICMP *(*engl. *Internet Control Message Protocol)* poruka. Zapravo, komandom *ping 172.16.3.3* sa rutera CER1 šalje se ICMP poruka prema ruteru CER3.

U tabeli 2 je prikazan izgled sadržaja prozora u *Dynamips*-u posle izvršenja komande *ping*. Sadržaj prozora ukazuje da je ova komanda uspešno izvršena i da je ostvarena komunikacija između rutera CER1 i CER3.

TABELA 2. PINGOVANJE IP ADRESE 172.16.3.3 SA RUTERA CER1

```
CER1#ping 172.16.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 360/454/740 ms
CER1#
```

Ali, proverom konektivnosti između rutera CER1 i rutera CER4 (Tabela 3) komandom *ping 172.16.4.4* sa rutera CER1, dobija se negativna potvrda. Konektivnost nije uspostavljena.

TABELA 3. PINGOVANJE IP ADRESE 172.16.4.4 SA RUTERA CER1

```
CER1#ping 172.16.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CER1#
```

Dodatna bezbednost podataka pri prenosu može se ostvariti dodatnom enkripcijom podataka na ruterima koji koriste korisnici. U ovom slučaju to su ruteri ka opremi korisnika (CER1, CER2, CER3, CER4).

Postoji mnogo mehanizama da se ovo ostvari. Jedan od njih je i korišćenje IPSec protokola, koji je okosnica otvorenog standarda razvijen od IETF da osigura privatnost podataka, autentifikaciju podataka, i autentifikaciju korisnika na javnoj mreži.

Na ruterima CER1 i CER3 iskonfigurisana je osnova za dalju nadogradnju i korišćenje simetričnog algoritma DES (engl. *Data Encryption Standard*)za enkripciju podataka. Simetrični algoritmi su najčešći u kriptografiji koji koriste složene algoritme i isti ključ za šifrovanje i dešifrovanje, a svoju sigurnost uglavnom baziraju na kvalitetu i dovoljnoj dužini ključa, u ovom slučaju 56 bita.

TABELA 4. ENKRIPCIJA PODATAKA NA CER1

```
CER1#show crypto isakmp policy
Global IKE policy
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
lifetime:  86400 seconds, no volume limit
```

V. ZAKLJUČAK

Činjenica da MPLS može da zadovolji sve veće zahteve korisnika koji se postavljaju pred jezgreni deo mreže, čini ovu tehnologiju sve popularnijom. U radu je pokazano i da po pitanju sigurnosti ne postoji razlog za brigu za korisnike, tj. moguće je ostvariti sigurnu komunikaciju koristeći virtuelne privatne mreže u MPLS-u. Simulaciju je moguće doraditi, i to konfiguracijom IPSec protokola na ruterima ka opremi korisnika. Na taj način bi se dodatno zaštitili podaci.

LITERATURA

[1] Lawrency J. *Designing Multiprotocol Label Switching Networks*, IEEE Communications Magazine, Jul 2001.

[2] International Technical Support Organization, *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, November 1999.

[3] Todd Lammle, CCNA - Cisco Certified Network Associate, Sybex, 2006

[4] www.cisco.com

ABSTRACT

In this paper the MPLS network has been explained as effective mechanism for Virtual Private Networks support and some characteristics of VPN have been counted and have also been presented a MPLS network simulation and transparency of users' communication over MPLS network have been shown and from that we can see that MPLS networks are some sort of private networks.

DYNAMIPS MPLS NETWORK SIMULATION

Marinko Smiljanic