

VIRTUELNE PRIVATNE MREŽE ZASNOVANE NA INTERNET PROTOKOLU I KOMUTACIJI KORIŠĆENJEM LABELA

Zoran Petrović⁽¹⁾ Ivana Kragović⁽²⁾ Milan Janković⁽²⁾

⁽¹⁾Elektrotehnički fakultet, Bul. Revolucije 73, 11000 Beograd

⁽²⁾Zajednica Jugoslovenskih PTT, Palmotićeva 2, 11000 Beograd

1. UVOD

Mreže zasnovane na Internet protokolu IP dominiraju u oblasti telekomunikacionih mreža u ovoj deceniji. S obzirom na svoju jednostavnost Internet servisi kao što su WWW, e-mail, FTP 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 kakav je FTP (*File Transfer Protocol*). Arhitektura Interneta je zasnovana na konceptu prosleđivanja datagrama. Svaki IP datagram se rutira korak po korak ka krajnjem odredištu u skladu sa jedinstvenom IP odredišnom adresom, koja se nalazi u IP zaglavlju. Svaki ruter na koji se naiđe će pregledati tu adresu i potražiti put u svojoj tabeli rutiranja kako bi pronašao odgovarajuće izlazni interfejs za sledeći korak. Sam IP ne obezbeđuje pouzdanu isporuku podataka. Protokoli viših slojeva kakav je TCP (*Transport Control Protocol*) prate putanju datagrama i vrše ponovno slanje ako je to neophodno, u slučaju neispravnog prenosa. Ti protokoli ne obezbeđuju prenos u realnom vremenu, tako da IP sam po sebi ne nudi nikakvu mogućnost obezbeđivanja kvaliteta servisa korisnicima (nema mogućnosti QoS (*Quality of Service*) garancije). Javna i privatna IP mreža se sve više koristi za prenos aplikacija, audio i video tokova, kod kojih ne mogu da se tolerišu nepredvidljivi gubici. Karakteristike QoS kao što su: minimizacija vremena kašnjenja, minimizacija varijacija kašnjenja, obezbeđivanje potrebnog propusnog opsega, moraju da se obezbede. Pored toga veliki problem za provajdere internet servisa (*Internet Service Provider ISP*) je da ponude rešenja koja će omogućiti skalabilnost ali i ponudu ugovorenog kvaliteta usluge SLA, (*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 (*Reserve Reservation Protocol*), diferencijalni servisi DiffServ (*Differentiated services*), sve je više komplikovalo rutiranje. Razvojem ATM tehnologije, koja je ponuđena za izgradnju okosnice (*backbone*) Interneta omogućen je prenos podataka i multimedijalnih informacija preko jedne mreže i poštovanje pri tome dogovorenog kvaliteta 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 (*Multi Protocol label Switching*).

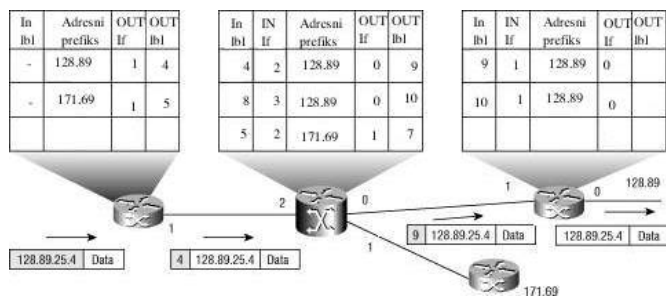
2. KOMUTACIJA KORIŠĆENJEM LABELA

MPLS kombinuje skalabilnost i fleksibilnost komutiranja sa kontrolom saobraćaja. U stvari MPLS ne nasleđuje ATM već ga dopunjuje; zamena labela koja se koristi predstavlja isti mehanizam koji ATM komutatori koriste za prosleđivanje ATM ćelija, s tim što se informacija o labeli nalazi u ATM zaglavlju, u VPI i VCI poljima. Bez MPLS, IP transport preko ATM mreže zahteva složene protokole za mapiranje IP adresa u ATM adrese, rutiranje i za ATM komutacione tabele. U tom slučaju su neophodni protokoli za ostvarivanje sprega između mreže a PNNI (*Private Network Network Interface*), protokol za razrešavanje adresa ATM ARP (*Address Resolution Protocol*) i protokol za rutiranje između podmreža a NHRP (*Next Hop Resolution Protocol*). MPLS sada zadovoljava i ono najvažnije: omogućava i koristi postojeće i profitabilne tehnologije Frame Relay i ATM.

Paketi koji ulaze u MPLS domen su paketi 3. sloja OSI modela, IP paketi. Ulazni ruter MPLS domena, LSR (*Label Switching Router*) analizira zaglavlje IP paketa i na osnovu dostupnih informacija dodeljuje mu odgovarajuću labelu. To LSR radi uz pomoć tabele koja mapira informaciju o klasi prosleđivanja u informaciju o labeli koja se koristi pri prosleđivanju, FEC (*Forwarding Equivalence Class*) to NHLFE (*Next Hop Label Forwarding Entry*) Map, koja sadrži informacije neophodne za dodeljivanje labela neoznačenim paketima koji ulaze u MPLS domen. Na slici 1. je prikazano funkcionisanje MPLS-a i metoda zamena labela koja se koristi. **Labele** se definišu kao kratki identifikatori lokalnog značaja i fiksne dužine koji se nalaze u zaglavlju paketa i koji logički predstavljaju FEC kome je paket dodeljen.

FEC je klasa ekvivalencije u prosleđivanju paketa, koja se određuje na osnovu odredista paketa i dodatnih pravila rutiranja. U MPLS protokolu svi paketi koji pripadaju jednoj klasi ekvivalencije biće prosleđeni na isti izlaz u datom evoru. Nakon toga **LSR** određuje sledeći skok za dati paket. Podaci o njemu se nalaze u NHLFE tabeli. Kada paket izađe iz ulaznog LSR njemu je dodeljena labela na osnovu koje će naredni LSR vršiti prosleđivanje. Iz ovoga se vidi da se analiza mrežnog sloja paketa vrši i samo u ulaznom LSR pa je samim tim smanjeno i vreme potrebno da se paket obradi i prosledi, a na taj način su značajno poboljšane performanse rutiranja. Kada paket stigne do izlaznog LSR-a labela se skida i paket će opet postati običan IP paket, a dalje prosleđivanje će biti zasnovano samo na njegovom zaglavlju. Dakle u MPLS domenu prosleđivanje paketa je zasnovano samo na 32-bitnoj labeli koja se dodeljuje paketu iza zaglavlja sloja 2 i ispred IP zaglavlja. Putanja koju paket prolazi i koja je određena labelom (pripadnošću nekom paketu određenoj FEC klasi) zovemo **LSP** (*Label Switching Path*). Cilj MPLS protokola je da se svakom

paketu koji ulazi u MPLS domen odmah pridruži i LSP putanja kojom će paket prolaziti kroz domen, tj. da na samom ulazu bude poznata cela putanja paketa.



Slika1. Funkcionisanje MPLS-a

Za uspostavljanje LSP putanje odgovoran je protokol za distribuciju labela **LDP** (*Label Distribution Protocol*). To je skup procedura pomoću kojih jedan LSR ruter informiše drugi o značenju labela koje se koriste za prosleđivanje saobraćaja između LSR rutera u MPLS domenu, tj. pomoću kojih LSR uspostavljaju LSP putanje kroz mrežu, preslikavajući informacije o rutiranju sa mrežnog nivoa u direktno komutirane putanje nivoa linka podataka (*data link*) nivoa. Koristi se protokol za distribuiranje labela u saradnji sa protokolima rutiranja OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*), BGP (*Border Gateway Protocol*) uspostavlja se putanja kroz MPLS mrežu i u rezervišu neophodni resursi za zadovoljavanje pre-definisanih zahteva za datu putanju. Pri tome svaki LSR donosi odluku prosleđivanja jedino u skladu sa sadržajem labela. LDP ima sledeće karakteristike:

- Posедуje mehanizme za omogućavanje LSR-ima da pronađu jedni druge i uspostave komunikaciju.
- Definiše četiri klase poruka: DISCOVERY, ADJACENCY, LABEL ADVERTISEMENT i NOTIFICATION.
- Funkcioniše preko TCP kako bi se obezbedila pouzdanost poruka (kada nije potrebna potvrda prijema poruke koristi se UDP)
- Dizajniran je da bude lako proširiv

Dva LSR koji koriste LDP da ramene preslikavanje labela i FEC nazivaju se LDP parovi i oni razmenjuju 4 tipa LDP poruka:

- Poruke otkrivanja, za pronalaznje LSR rutera
- Poruke sesije, za uspostavljanje održavanja i zatvaranje sesija između LDP parova
- Poruke oglasavanja, za stvaranje, menjanje i brisanje labela u FEC klase
- Poruke obaveštenja, za signalizaciju grešaka

MPLS donosi i mnoge pogodnosti u odnosu na IP mreže:

- *Traffic Engineering* – sposobnost uspostavljanja putanje saobraćaja i uspostavljanje performansi karakterističnih za određenu klasu saobraćaja. *Traffic engineering* omogućava ISP da prebace saobraćaj sa najkraće putanje izračunate korišćenjem IGP (*Interior Gateway Protocol*) protokola na potencijalno manje zakrčenu putanju.
- VPN -ISP-i su ponudili korisnicima VPN MPLS kao jednostavno rešenje za obezbeđivanje privatnosti podataka i podršku za korišćenje ne-jedinstvenih privatnih IP adresa, jer se tu odluke prosleđivanja

donose samo u skladu sa vrednošću labela, a ne određuju IP adrese koja se nalazi u zaglavlju paketa.

- Eliminacija viših slojeva - tipično vešina koristi sveobuhvatan model gde je ATM korišćen na sloju 2 i IP na sloju 3. Korišćenjem MPLS moguće je mnoge funkcije ATM upravljačke ravni prebaciti na nivo 3, a time se pojednostavljuje upravljanje mrežom kao i složenost mreže.

3. VPN ZASNOVANE NA MPLS-u

Velike firme koje imaju filijale na različitim lokacijama morale su da povezuju računare radi efikasnijeg poslovanja. Njima je potrebna privatna mreža a VPN (*Virtual Private Network*) koju bi mogli da administriraju u skladu sa sopstvenim potrebama sigurnosti, rutiranja i dozvola. Virtualnost se ogleda u tome što ta infrastruktura koja se koristi u toj mreži i ne pripada samo njoj. Ona u stvari pripada provajderima Internet servisa, jednom ili više njih i predstavlja backbone koji mogu da koriste jedna ili više VPN. Postoje dva tipa praktične realizacije mreže i preko koje mogu da se ostvare VPN. To je:

- *Overlay* model VPN mreže:

Taj model je danas još uvek prisutniji i podrazumeva da se na svakoj korisničkoj lokaciji nalazi jedan ili više rutera, koji su sa ruterima na drugim udaljenim lokacijama povezani point-to-point (tačka - tačka) vezama (iznajmljenim linijama, ATM ili Frame Relay vezama). Ovaj model efikasno funkcionisalo ali postoji značajan problem skalabilnosti, i zahteva koji se postavljaju korisnicima da sami upravljaju ruterima koji održavaju vezu između udaljenih lokacija, kao i problemi menjanja konfiguracije pri svakom novom dodavanju nove lokacije.

- *Peer model* VPN mreže

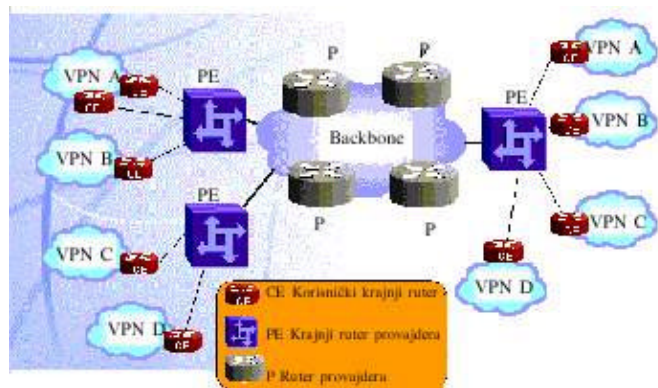
Ovaj model treba da omogućio provajderima opsluživanje veoma velikog broja korisnika, i ujedno preuzimanje funkcije administriranja njihovih mreža a tako da oni mogu da se posvete samo svom primarnom biznisu, ne upuštajući se u pravila IP rutiranja. *Peer model* se sastoji od 4 komponente:

- ograničena distribucija informacija o rutama: pošto su korisnički ruteri direktno spojeni na ruteru VPN provajdera, moramo na neki način ograničiti protok, tako da samo ruteri koji pripadaju istoj VPN mreži i mogu razmenjivati saobraćaj.
- upotreba višestrukih tabela rutiranja: neophodno je da PE ruter održava ne jednu, već više tabela rutiranja jer on najčešće služi i za povezivanje više VPN korisnika, pa njegova tabela rutiranja sadrži i u sebi sve rute dobijene od svih lokacija koje su preko njega povezane.
- korišćenje novog tipa adresa (VPN-IP adrese)
- upotreba MPLS protokola

Na primeru Intranet mreže će kasnije biti prikazano kako se ostvaruju te komponente.

Primer peer mreže je prikazan na slici 2. Sa CE (*Customer Edge*) su označeni ruteri na korisničkim lokacijama, a sa PE (*Provider Edge*) ruteri provajdera koji su direktno vezani na korisničke, pri čemu između njih mora biti obezbeđena direktna IP veza. Sa P su označeni *core* ruteri *backbone*-a. CE uređaj može biti vezan na PE ruter bilo kojim tipom linka podataka (na primer ATM VCC, Frame Relay, Ethernet...). Korisnička lokacija može biti vezana na provajdera preko višeg PE rutera, a PE ruter može i obezbeđivati vezu za više od jedne korisničke lokacije. Ovaj model nosi naziv *peer* zato što korisnički ruteri direktno razmenjuju saobraćaj sa ruterima VPN provajdera, za razliku od *overlay* modela gde su korisnički

ruteri na udaljenim lokacijama direktno povezani jedni sa drugima, bilo putem virtuelnih kola na data link sloju, bilo putem IP tunela.



Slika 2. Peer model VPN mreže

Svaka VPN nosi oznaku koja u implementaciji predstavlja 8-o bajtnu "oznaku rute" *Route Distinguisher RD* [1]. Ona se sastoji od tri polja:

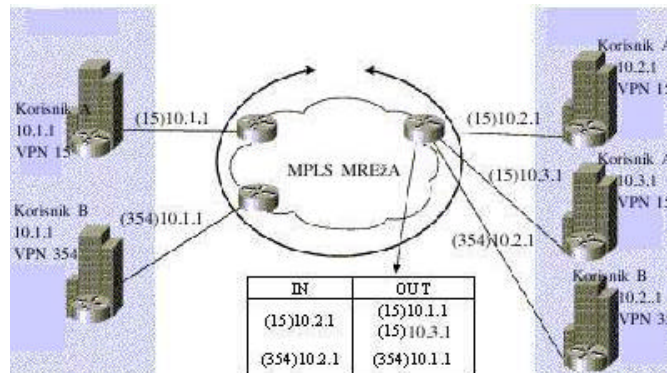
- Tip –2 okteta
- AS broj autonomnog sistema koji je dodeljen VPN provajderu –2 okteta
- VPN broj – 4 okteta

RD se koristi kao prefiks IP adresama tog sajta. Konfigurisane su na interfejsu koji je vezan za određenu lokaciju. Na primer podmreža 10.1.1.0 za VPN 15 se razlikuje od podmreže 10.1.1.0 za VPN 354. Sa gledišta MPLS VPN provajdera to su u stvari adrese 15:10.1.1.0 i 354:10.1.1.0. Dodeljivanje 8-o bajtne oznake rute ispred IP adrese dobija se VPN-IP adresa. Sa stanovišta BGP protokola, rukovanje rutama koje imaju VPN-IP adrese se ne razlikuje od standardne procedure za IP adrese, zahvaljujući osobini BGP protokola da generički rukuje adresama, bez obzira na njihov format. Na ovaj način se samo prenosi informacije o VPN drugim ruterima koji imaju interfejse sa istom vrednošću RD. Na taj način se sprečava slučajno curenje informacija korisnika A korisniku B. To takođe znači da svaki PE ruter samo prati rute korisnika koji su povezani na taj PE, a ne prefikse za sve lokacije i korisnike koji su vezani na ISP. Pri tome ostaje problem i činjenica da su to VPN-IP rute, a da je ipak mreža provajdera zasnovana na IP protokolu, tako da je u PE ruterima neophodno da se izvrši pretvaranje IP u VPN-IP adrese. To se ostvaruje tako što ruter identifikuje VPN mrežu u kojoj korisnik pripada na osnovu interfejasa po kojem stiže paket i dodeljuje VPN IP adresu koristeći oznaku rute za datu VPN mrežu. Zatim tu VPN-IP rutu prosleđuje svojim BGP susedima koristeći BGP opšti atribut (*community*) atribut za datu mrežu. Pri tome se javljaju sledeći problemi:

- neophodno je konvertovati IP zaglavlje tako da se koriste duže adrese na ulaznim PE ruterima
- unutrašnji ruteri treba da znaju kako da prosleđuju ovaj novi mrežni protokol
- neophodno je na izlaznim ruterima ponovo izvršiti konverziju u IP adrese

Zato se rešenje za taj problem našlo uvođenjem MPLS-a. Sa stanovišta MPLS-a ulazni PE ruter nije ništa drugo do ulazni LSR ruter. Kada ulazni PE ruter primi IP paket od CE rutera, on konsultuje svoju odgovarajuću FIB tabelu rutiranja (identifikovanu na osnovu porta po kom je došao IP paket). Na osnovu informacije iz tabele rutiranja, utvrđuje se sledeći hop

paketa kao i labela koja će biti stavljena na njegovo IP zaglavlje. U stvari na paket se stavljaju 2 labela: prva na vrhu steka labela, govori o putanji paketa kroz mrežu u VPN provajdera do izlaznog PE rutera i prosleđuje se LDP protokolom. Druga labela ispod prethodne, govori izlaznom PE ruteru kako i kom korisniku treba proslediti paket koji je primljen i prosleđuje se BGP protokolom, upotrebom VPN-IP adresa.



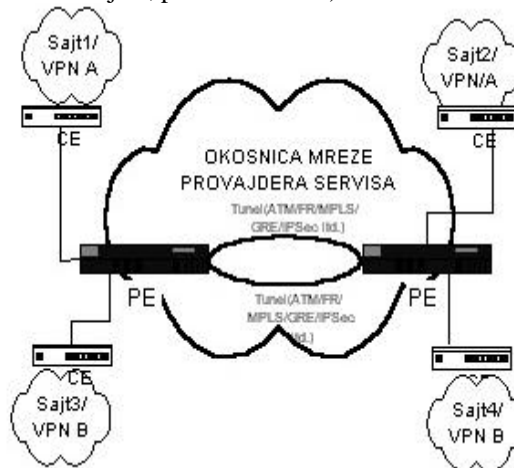
Slika 3. Uvođenje Route Distinguisher-a

Nadalje će biti prikazani neki primeri i data objašnjenja VPN [3]

4. SCENARIJI RAZVOJA VPN

4.1. Intranet (veza sajtova u istoj organizaciji):

U ovom slučaju VPN je formirana između sajtova koji pripadaju istoj organizaciji. To je slučaj kada se različite filijale međusobno povezuju ili kada se povezuju sa upravom. Na slici 4. na provajderove rutere PE (*Provider Edge Device*) se vezuju sajtovi korisnika preko korisnikovog krajnjeg uređaja CE rutera. Ta veza može biti ostvarena na različite načine (na primer statičkim rutiranjem, preko ATM VC).



Slika 4. Primer intranet scenarija

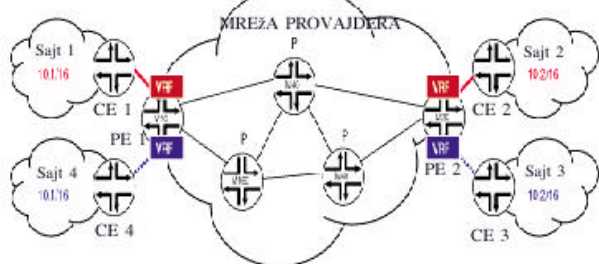
Na slici 5. je detaljniji prikaz i na njemu će biti objašnjen mehanizam VPN intranet mreže.

U BGP/MPLS VPN modelu razlikuju se dva tipa saobraćaja:

- upravljački tok *control flow* za distribuciju informacija o rutama između PE i CE i za uspostavljanje LSP
- tok podataka, *data flow* za prosleđivanje saobraćaja korisnika

U ovom primeru PE1 je konfigurisan tako da mu je interfejsu po kom stiže u rute od CE1 dodeljena VRF Red tabela. Kada on od rutera CE1 primi informacije o ruti 10.1/16 on ih pretvara u VPN-IP format, zatim tako dobijenoj ruti dodaje BGP opšti atribut (*community*) atribut, a za PE1 određuje vrednost MPLS labela

(na primer 222) i eksportuje ih u BGP sistem provajdera. Kada PE2 putem BGP protokola primi tu informaciju on VPN-IP adresu pretvara nazad u standardnu IP adresu i smešta je u tabelu rutiranja za odgovarajuću VPN mrežu.

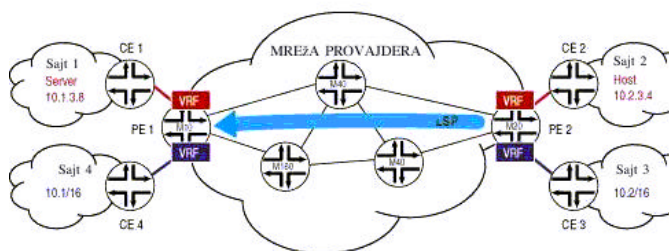


CE-Korisnički krajnji ruter
PE-Provajderov krajnji ruter
P-Ruter provajdera
VRF-VPN tabela rutiranja i prosledivanja

Slika 5. Detaljnije objašnjenje formiranja intraneta

Kako bi se VPN saobraćaj preko backbone-a provajdera prenosio korišćenjem MPLS-a između PE rutera mora da se ostvari LSP. Ona može da se ostvari i održava korišćenjem ili LDP ili RSVP. Ako provajder koristi LDP on želi da uspostavi *best-effort* LSP između PE, a ako koristi RSVP on želi da LSP dodeli određen propusni opseg ili da ostvari *Traffic Engineering* za određivanje tačne putanje. LSP zasnovane na RSVP nude QoS garancije.

Na slici 6. je prikazan tok podataka sa jednog korisničkog sajta na drugi.



Slika 6. Uspostavljanje LSP za data flow

Pretpostavimo da hostovi 10.1.3.8 sa sajta 1 i 10.2.3.4 sa sajta 2 žele da komuniciraju. Kada 10.2.3.4 pošalje paket njega CE2 prosledi PE2 ruteru. On utvrđuje tabelu rutiranja za taj interfejs i iz nje uzima informaciju o sledećem hopu unutar mreže i VPN provajdera za dati paket (o PE1 ruteru) i labelu na osnovu koje će PE1 prosluditi paket ruteru CE1 (labela 222).

Korisnički saobraćaj se prosleđuje od PE2 ka PE1 korišćenjem MPLS -a sa stekom na kojemu se nalaze dve labela. Za taj tok PE2 je ulazni LSR, a PE1 izlazni LSR za LSP. Pre početka prenošenja paketa PE2 stavlja na dno steka labelu 222 (labelu koju je PE1 oglasio sa rutom). Ta labela je instalirana u VRF Red kada je PE2 od PE1 primio preko BGP informaciju o ruti 10.1/16 PE1 utvrđuje i labelu koju treba da stavi na vrh steka labela, kako bi paket stigao do PE1 i tako formirani paket sa dve labela prosleđuje na LSP putanju *core* ruterima. Oni u skladu sa MPLS protokolom menjaju labelu na vrhu i dalje prosleđuju paket. Kada preposlednji core ruter primi paket on skida gornju labelu i takav paket šalje ka PE1. PE1 na kraju samo skine labelu 222 i na osnovu nje identifikuje direktno vezan CE1 i prosleđuje mu IP paket.

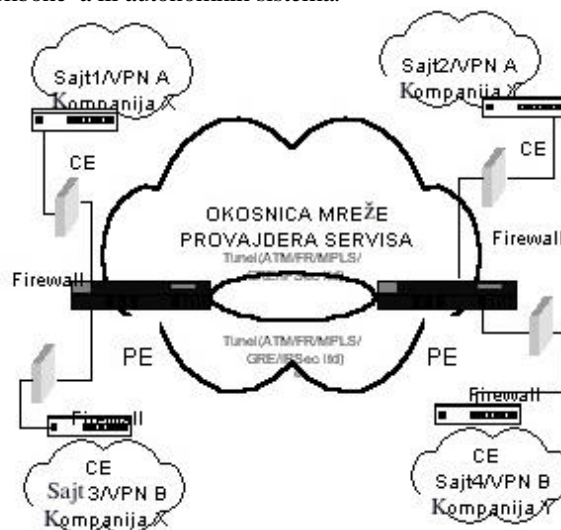
Pošto se umesto IP adresa u mreži i provajdera koriste labela, korisnici mogu da zadrže svoje privatne adresne šeme bez potrebe za pretvaranjem privatnih u javne adrese NAT *Network address translation* kako bi se saobraćaj ostvario preko mreže i provajdera. Saobraćaj je razdvojen između VPN korišćenjem razdvojenih tabela rutiranja za svaku VPN. Na osnovu dolaznog interfejsa ruter selektuje određenu tabelu.

4.2. Extranet (veza sajtova koji pripadaju različitim organizacijama):

U ovom scenariju, dve ili više organizacija imaju pristup ograničenom broju zajedničkih lokacija. Da bi se kompanija X povezala sa svoji poslovnim partnerom kompanijom Y neophodno je da uveze rute za VPN iz B (najverovatnije i da izvrši i njihovo filtriranje, da bi imala pristup samo određenim lokacijama kompanije B).

Osnovna razlika između extraneta i interneta je da provajder mora eksplicitno da konfigurise dostupnost između VPN i da obezbedi postojanje neke vrste kontrolnog pristupnog mehanizma pri povezivanju različitih organizacija. Ta kontrola pristupa može biti ostvarena *firewall*-om, listom pristupa na ruterima ili sličnim mehanizmima koji omogućiti primenu kontrole pristupa zasnovanu na postojanju polisa tranzitnom saobraćaju. Svi ti mehanizmi kontrole pristupa mogu biti postignuti korišćenjem posebnih uređaja ili mogu biti integrirani u PE uređajima. Taj scenario je prikazan na slici 7.

U tom primeru su formirane dve VPN koje povezuju Kompaniju X i Kompaniju Y. Za kontrolu pristupa koristi se *firewall*. Dodatni mehanizmi autentifikacije kao što je razmenjivanje sertifikata o autoritetu je takođe poželjno. Moguće je da sajt pripada i više estrukim VPN, koji mogu da uključuju sa jedne strane intranet, a sa druge extranet. Extranet može da postoji duž backbone-a jednog provajdera ili duž više backbone-a ili autonomnih sistema.

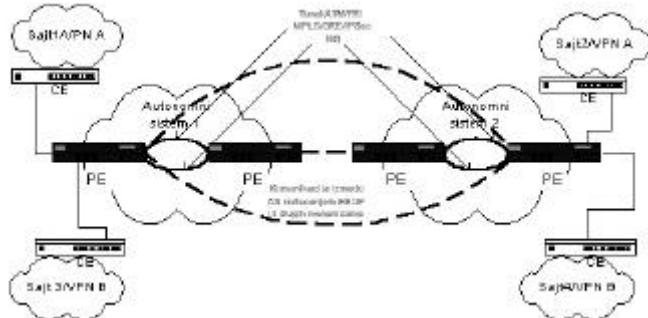


Slika 7. Primer Extranet scenarija

4.3. VPN duž višestrukih autonomnih sistema ili provajdera servisa:

Po ovom scenariju virtualna privatna mreža može da se širi preko mreža i više provajdera servisa ili Autonomnih sistema (AS - *Autonomous Systems*). Osnovni predmet u tim slučajevima je pitanje komunikacije i sigurnosti između PE uređaja koji pripadaju različitim AS. Komunikacija između njih može biti ostvarena na različite načine u zavisnosti od pristupa koji je primenjen pri formiranju IP VPN. Pitanje sigurnosti između PE koji pripadaju različitim AS može biti

rešeno korišćenjem PE-PE tunela (na primer IPSec tuneli mogu biti korišćeni da obezbede enkripciju duž AS). VPN ruta distribucije preko AS treba da bude ostvarena tako da izgleda kao da postoji jedan tunel od ulaznog PE u jednom AS do izlaznog PE u drugoj AS. Ovaj scenario je prikazan na slici 8. Isprekidana linija prikazuje kako se tunel "ulaz PE - izlaz PE" pojavljuje kada je komunikacija između AS ispravno ostvarena. Naravno, pri tome treba voditi računa o preduslovu da bi ta veza bila ostvarena, a to je postojanje dogovora o poverenju između uključenih provajdera servisa.



Slika 8. VPN preko više Autonomnih sistema

4.4. Istovremen VPN i Internet pristup:

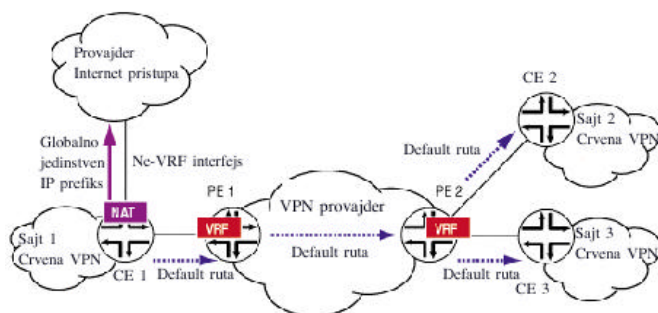
Mnoge hostovima na Internetu treba istovremeno omogućiti i pristup Internetu, kao i drugim VPN sajtovima. Tu je mogao da nastane problem jer mnoga preduzeća koriste sopstveni privatni adresni prostor.

Generalno postoje tri načina kako VPN mogu da koriste globalno jedinstvene adrese za komunikaciju sa drugim hostovima.

- da svi sistemi na privatnoj mreži koriste globalno jedinstvene IP adrese, što baš i nije odgovarajuće, kada su adrese već dodeljene, pa ih treba menjati
- ako samo mali broj korisnika treba da ima mogućnost pristupa Internetu onda samo njima dodeliti javne IP adrese. Uobičajeno je u mnogim firmama da neki korisnici imaju privatne IP adrese, a da istovremeno neki sistemi koriste javne.
- korišćenje Network Address Translator (NAT) servera u privatnoj mreži može da omogućiti korisnicima VPN kojima su dodeljene privatne IP adrese da pristupe Internetu.

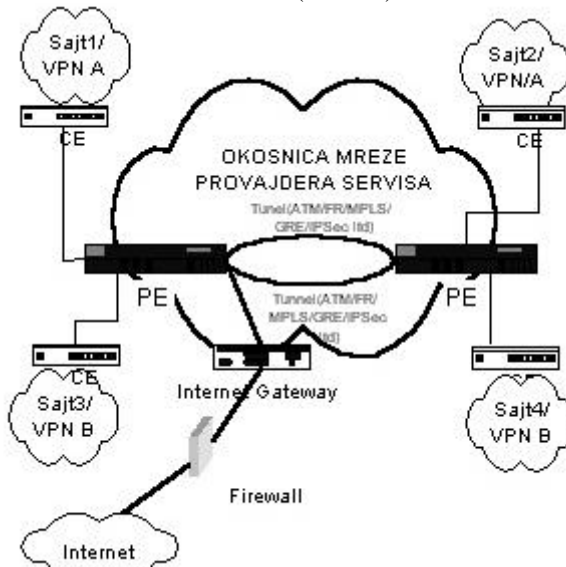
Postoje i metode u okviru BGP/MPLS VPN modela koje mogu da se iskoriste to. Jedan način za to je i korišćenje ne-VRF Internet pristupnog mehanizma.

Korisnici VPN sajta mogu direktno da pristupe Internetu preko Internet gateway. On može da se ostvari na ne-VRF interfejsu ili na CE ruteru ili na nekom drugom ruteru na korisničkoj strani. Interfejs na ruteru koji omogućava Internet pristup je konfigurisan tako da ima funkciju Internet firewall-a i NAT (slika 9). Sada kako bi se omogućilo korisnicima VPN da pristupe javnom Internetu, CE1 na sajtu 1 šalje default rutu PE1, koja se postavlja u njegovu VRF, a zatim je BGP protokolom šalje PE2 ruteru, a on dalje CE2 na sajtu 2 i CE3 na sajtu 3. Kao rezultat toga svi hostovi VPN prosleđuju Internet saobraćaj CE1 ruteru na sajtu 1, koji rutira saobraćaj preko NAT interfejsa na Internet. NAT translira svaku privatnu izvorišnu adresu u javnu adresu. Kako bi se omogućilo hostovima na Intranetu da odgovore hostovima na VPN, CE1 dodaje javni IP prefiks u Internet tabelu rutiranja. Kada paket stigne na CE1 NAT interfejs, NAT servis translira javne u privatne određene adrese.



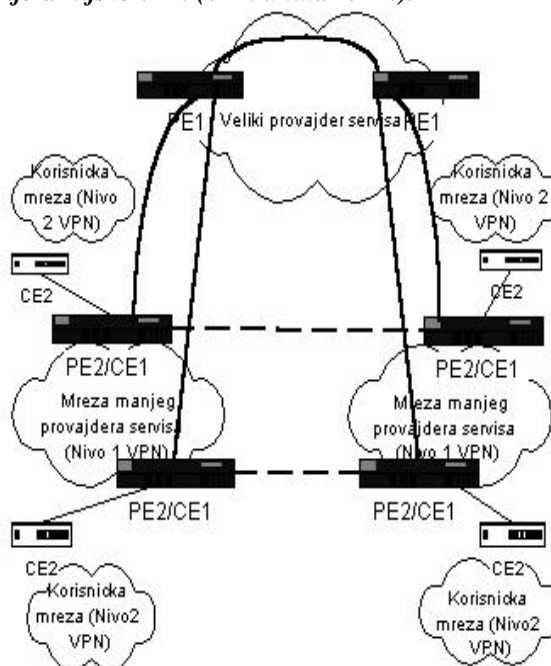
Slika 9. Primer uspostavljanja default rute za istovremeni pristup VPN i Internetu

Saobraćaj koji sa Interneta stiže na odgovarajući sajt u VPN prosleđuje se Internet rutama koji vode na sajtove u VPN. Unutrašnja struktura VPN je nevidljiva za Internet. Postojanje firewall može biti poželjno kako bi se smanjio pristup privatnim mrežama sa Interneta (slika 10).



Slika 10. Istovremeni VPN i Internet pristup

4.5. Hijerarhijske VPN (VPN unutar VPN):

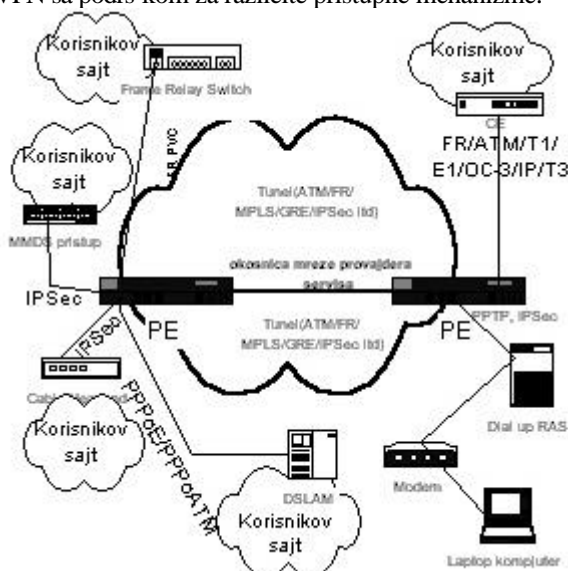


Slika 11. Hijerarhijske VPN

U ovom scenariju provajderi servisa koji obezbeđuju VPN mogu u stvari biti korisnici nekog većeg provajdera. Takav provajder može biti jedna velika VPN sa više malih VPN u okviru nje. Takvog provajdera ćemo nadalje označiti sa Nivo-1, a VPN u okviru njega sa Nivo-2, prikazano na slici 11. PE uređaj Nivoa 2 PE2 je CE uređaj Nivoa1 (CE1) VPN. Logički tuneli Nivoa 2 VPN su prikazani isprekidanom linijom, dok puna linija predstavlja stvarne CE1-CE1 (tj. PE2-PE2) tunele preko velike mreže provajdera servisa. Stoga, CE uređaji Nivoa 1 VPN treba da budu uključeni u mehanizme uspostavljanja VPN.

4.6. Scenario višestrukog pristupa

IP VPN treba da podrži više tipova pristupnih scenarija, na primer treba da budu podržani statičko rutiranje, ATM PVC, korišćenje različitih protokola rutiranja, xDSL modema i dial pristup. Pri tome se mogu koristiti različiti uređaji za razdvajanje različitih pristupnih mehanizama ili te funkcije mogu biti integrisane u PE uređajima. Na slici 12. je ilustrovan IP VPN sa podrškom za različite pristupne mehanizme.



Slika 12. Scenario višestrukog pristupa

5. OSOBINE MPLS VPN

MPLS VPN omogućavaju provajderima servisa da izgrade skalabilne VPN i da pri tome ponude sledeće servise :

- Servise bez uspostavljanja veze: kada se VPN formiraju bez predhodnog uspostavljanja veze nisu potrebni tuneli i enkripcija za mrežnu privatnost, pa se na taj način značajno umanjuje složenost mreže.
- Centralizovane servise: izgradnja VPN na Sloju 3. OSI modela dozvoljava isporuku servisa grupi korisnika, koji su u VPN. Njima se mogu ponuditi novi IP servisi kao što su:
 - Višedifuzija (*Multicast*)
 - Kvalitet servisa QOS
 - Telefonska podrška
Moguće je pri tome prilagoditi više kombinacija specijalizovanih servisa za pojedinačne korisnike. Na primer, servisi koji kombinuju IP multicast sa servisima sa malim kašnjenjem *low-latency service* omogućavaju videokonferenciju u intanetu.
- Skalabilnost: Ako se VPN formira korišćenjem modela orijentisanih na vezu, tačka-tačka overlay modelu, Frame

Relay ili ATM , glavni nedostatak će pri tome biti nedostatak skalabilnosti. Pored toga VPN orijentisane na vezu, bez potpune povezanosti između korisničkih sajtova, nije optimalna. Nasuprot tome VPN zasnovane na MPLS-u koriste peer model i arhitekturu bez predhodnog uspostavljanja veze Sloja3. za visoko skalabilna VPN rešenja. Takva arhitektura dozvoljava kreiranje VPN eliminišući pri tome potrebu za tunelima ili VC-ima. Skalabilnost se ogleda i u deljenju VPN i IGP ruta između PE rutera i core rutera provajdera P. PE ruteri moraju da održavaju VPN rute za korisnike određene VPN, dok P ruteri ne održavaju nikakve VPN rute. To povećava skalabilnost provajderovog jezgra i osigurava da nijedan uređaj ne može biti usko grlo za skalabilnost.

- Sigurnost: MPLS VPN nude isti stepen sigurnosti kao i VPN orijentisane na vezu. Paketi iz jedne VPN ne mogu nepažnjom da stignu do druge VPN.
- Na ivici mreže provajdera, garantovano je smeštanje primljenih paketa korisnika na pravu VPN.
- Na okosnici, VPN saobraćaj se održava odvojeno. Zlonamerno ometanje (*spoofing*) je praktično nemoguće jer su paketi dobijeni od korisnika IP paketi. Ti paketi moraju da se prime na određenom interfejsu da bi bili jedinstveno identifikovani VPN labelom.
- Jednostavnost kreiranja: Za potpuno iskorišćenje VPN, korisnicima mora biti jednostavno da kreiraju nove VPN i nove korisničke lokacije. Pošto je MPLS VPN bez predhodnog uspostavljanja veze, nisu potrebne nikakve predhodne tačka-tačka mape ni topologije. Moguće je dodati sajtove intanetima i ekstranetima i oformiti zatvorene korisničke grupe. Kada se VPN ostvari na taj način, omogućeno je dodavanje bilo kog sajta u VPN, i samim tim je maksimizirana fleksibilnost u formiranju intraneta i ekstraneta.
- Fleksibilno adresiranje: Kako bi se VPN servisi načinili prihvatljivijim, korisnici provajdera servisa mogu da koriste sopstveni adresni plan, nezavisan od adresnog plana drugih korisnika. Mnogi korisnici imaju privatni adresni prostor i ne žele da investiraju u vreme i novac u konvertovanje u public IP adrese kako bi omogućili povezivanje u intranet. MPLS VPN dozvoljavaju korisnicima da nastave sa korišćenjem sopstvenih adresnih prostora bez potrebe za NAT , obezbeđujući javni i privatni izgled adresa. NAT je neophodan samo ako dve VPN sa preklapajućim adresnim prostorima žele da komuniciraju. Tako korisnici mogu da koriste sopstvene neregistrovane privatne adrese, i komuniciraju slobodno sa javnom IP mrežom.
- Podrška integrisanim klasama servisa (CoS): Klasa servisa je karakteristika MPLS koja omogućava mrežnim administratorima da obezbede različite tipove servisa duž MPLS mreže. Različiti servisi zadovoljavaju zahteve korisnika, tako što se paketima koji se prenose preko mreže određena vrsta servisa specificirana za paket njegovom CoS. Servisi mogu biti specificirani na različite načine, na primer podešavanjem IP bita prioriteta u IP paketu. U snabdevanju različitim servisima, MPLS CoS nudi klasifikaciju paketa, izbegavanje i upravljanje zakrčenjem. Tabela 1 daje listu tih funkcija i njihove opise:

SERVIS	CoS FUNKCIJA	OPIS
Klasifikacija paketa	Committed access rate (CAR) Paketi su klasifikovani na ivici mreže pre nego što im se pridruže labele	CAR koristi bit tip servisa TOS u IP zaglavlju za klasifikaciju paketa u skladu sa ulaznom i izlaznom brzinom prenosa. CAR komanda se najčešće konfiguriše na interfejsu na ivici mreže kako bi se kontrolisao saobraćaj koji ulazi ili izlazi iz mreže.
Izbegavanje zagušenja	Weighted random early detection (WRED) Razdvajaju se klase paketa prema verovatnoći propadanja.	WRED monitoriše mrežu ni saobraćaj, pokušavajući da predvidi i spreči zakrčenje na najčešćim mrežnim uskim grlima. WRED može selektivno da odbaci saobraćaj niskog prioriteta kada se pojavi zagušenje. Takođe može da obezbedi različite performanse za različite klase servisa.
Upravljanje zagušenjem	Weighted fair queueing (WFQ). Razlikuju se klase paketa u zavisnosti od propusnog opsega i graničnog kašnjenja.	WFQ je automatski sistem praćenja koji obezbeđuje nepristrasnu dodelu propusnog opsega mrežnom saobraćaju. WFQ koristi težinu (prioritet) za odlučivanje koliko propusnog opsega je potrebno dodeliti svakoj klasi saobraćaja.

Tabela 1. MPLS CoS

Za više informacija o konfigurisanju CoS funkcija (CAR, WRED, WFQ) videti *Cisco IOS Quality of Service Solutions Configuration Guide*.

- CoS je veoma bitan zahtev za mnoge IP VPN korisnike. Obezbeđuje mogućnost adresiranja dva osnovna VPN zahteva:

- predvidljive performanse i uvođenje prava pristupa. Mrežni saobraćaj je klasifikovan i obeležen na ivici mreže pre nego što je spojen prema zahtevima definisanim od strane pretplatnika i implementiran od strane provajdera i prenešen preko provajderovog jezgra. Saobraćaj na ivici i u jezgru mreže tada može biti podeljen u različite klase.

- Otvorena (*Straightforward*) migracija: provajderi servisa za brz razvoj VPN servisa, koriste otvorene putanje migracije (*Straightforward migration path*). MPLS VPN su jedinstvene jer mogu da se izgrade preko višestruke mrežne arhitekture, uključujući tu IP, ATM, Frame Relay i hibridne mreže. Migracija krajnjih korisnika je pojednostavljena jer nema zahteva za podrškom MPLS na CE ruterima tako da nema potrebe za modifikacijama na korisnikovom intranetu. Samo su PE ruteri svesni VPN.

6. ZAKLJUČAK

Internet protokol VPN predstavljaju jedan od servisa koji su zabeležili ili najviše rast i popularnost u biznis-biznis komunikacijama - trend za koji analitičari predviđaju da će se još više razviti 2001. godine i nadalje. RFC2547bis je omogućio provajderima servisa da isporučuju ekstremno velike skalabilne VPN servise zasnovane na peer modelu kako bi se prevazišao problem ograničene skalabilnosti VPN overlay modela. To omogućava korisnicima da pitanja i probleme složenog upravljanja rutiranjem prebace na provajdere servisa, da samostalno održavaju složenih veza između svojih rutera prebace na PE rutere koji koriste BGP protokol, i omogućava korisnicima da koriste zajedničku MPLS infrastrukturu za prenos javnih i privatnih podataka. Model BGP/MPLS VPN servisa preuzima jednu od vodećih uloga u današnjem

komunikacijama što se vidi i na sajtovima najznačajnijih proizvođača CISCO-a i Juniper-a.

Abstract: Limitations of IP as a protocol on which the architecture of Internet is based were not considered as a problem for the applications as web, e-mail, file transfer etc. The new video/audio applications request a wider bandwidth and a guarantee of QoS. Public and private IP networks are used for transfer of information, so no unexpected losses could be tolerated. Due to that, as a solution for needs of scalability, better routing performances and offer for different classes of MPLS has been introduced. In IP networks, the service providers use the end routers which enable VPN, and use in core network mechanisms which enable the reservation of resources, such as MPLS protocol. The users should be enabled to realize VPN, and the quality of service should be guaranteed too. Basic characteristics of MPLS will be presented in this paper, the importance for VPN as well as the ways of implementation and application of VPN.

LITERATURA:

- [1] www.cisco.com
- [2] www.mpls.com
- [3] ITU-T New ITU-T Recommendations Y.ipvpn, Draft, COM 13-R4-E, Geneva, January 2001.
- [4] www.juniper.com
- [5] <draft-rosen-rfc2547bis-02.txt>, July 2000
- [6] Petrović Z., Krajnović N., *Unapređenje performansi rutiranja saobraćaja na Internetu*, XVII Simpozijum o novim tehnologijama u PTT saobraćaju, SF, Beograd 1999.
- [7] www.QoSForum.com
- [8] Torsten Braun, Manuel Guenter, Ibrahim Khalil: *Management of Quality of Service Enabled VPNs* - Communications Magazine, Vol.39, May 2001

VIRTUAL PRIVATE NETWORKS BASED ON IP AND MPLS, Petrović Z., Kragović L., Janković M.