Višeprotokolno komutiranje podatkovnog prometa u virtualnim privatnim mrežama temeljeno na oznakama

Pavin, Sara

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:076269

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-03-21**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Diplomski studij

VIŠEPROTOKOLNO KOMUTIRANJE PODATKOVNOG PROMETA U VIRTUALNIM PRIVATNIM MREŽAMA TEMELJENO NA OZNAKAMA

Diplomski rad

Sara Pavin

Osijek, 2018.

SADRŽAJ:

1. UVOD 1
1.1. Zadatak diplomskog rada 3
2. ARHITEKTURA TELEKOMUNIKACIJSKIH MREŽA 4
2.1. Prikaz mrežne arhitekture 4
2.2. Slojevi mrežnih modela 6
3. VIŠEPROTOKOLNO KOMUTIRANJE PODATKOVNOG PROMETA U MREŽI TEMELJENO NA OZNAKAMA - MPLS 10
3.1. Razvoj MPLS tehnologije 10
3.2. Implementacija MPLS rješenja 10
3.3. Osnovni elementi MPLS rješenja 12
3.3.1. Zaglavlje MPLS paketa 12
3.3.2. Usmjerivači u MPLS mreži 13
3.3.3. Put paketa kroz MPLS mrežu 14
3.3.4. Određivanje sljedećeg skoka paketa u MPLS mreži 15
3.3.5. Baza podataka za prosljeđivanje paketa prema oznakama 15
3.3.6. Prosljeđivanje skupa MPLS paketa 15
3.4. Protokoli u MPLS mrežama 16
3.4.1. Protokoli za distribuciju oznaka 16
3.4.1.1. LDP protokol 16
3.4.1.2. CR-LDP protokol 17
3.4.1.3. RSVP-TE protokol 18
3.4.2. Protokoli usmjeravanja 19
3.4.2.1. Usmjeravanje izborom najkraćeg puta 19
3.4.2.2. Poboljšani protokol za unutrašnje usmjeravanje 19
3.5. Struktura MPLS mreže 20
3.6. Funkcionalnost MPLS mreže 21
4. MPLS APLIKACIJE 22
4.1. MPLS tehnike upravljanja mrežnim prometom 22
4.2. MPLS profil mrežnog prometa 23
4.3. MPLS virtualne privatne mreže 25
4.4. Mehanizmi očuvanja kvalitete usluga u MPLS mreži 26
4.5. Primjena GMPLS tehnologije 27

5. INAČICE MPLS VPN MREŽA 29
5.1. Funkcionalnost MPLS VPN mreža na trećem sloju mrežnih modela 32
5.2. Funkcionalnost MPLS VPN mreža na drugom sloju mrežnih modela 36
5.2.1. VPWS usluge 38
5.2.2. VPLS usluge 43
6. PLANIRANJE MREŽE 46
6.1. Proces planiranja mreže 46
6.1.1. Telekomunikacijsko predviđanje 47
6.1.2. Dimenzioniranje mreže 49
6.1.3. Upravljanje mrežnim prometom 50
6.2. Različite faze MPLS mrežnog planiranja 50
6.2.1. Faza predviđanja 52
6.2.2. Ugovor o razini usluge 52
6.2.3. Faza definiranja mreže 52
6.2.4. Simulacija i analiza mrežnih scenarija 54
6.2.5. Optimizacija, upravljanje i konfiguracija čvorova u mreži 54
6.2.6. Planiranje zahtjeva za kapacitetom te dijeljenjem mrežnih resursa 55
6.2.7. Faza definiranja funkcionalnosti mreže 55
6.3. Izazovi pri implementiranju MPLS mreža 56
6.3.1. Izazovi pri skaliranju MPLS mreža 57
6.3.2. Izazovi funkcionalnosti MPLS mreža 58
7. POSTOJEĆI ALATI ZA PLANIRANJE MPLS MREŽE 60
7.1. IP/MPLSView 60
7.2. iVNT 65
8. KONFIGURACIJA UREĐAJA U TESTNOJ MREŽI 68
8.1 OSPF postavke na usmjerivačima u kreiranoj mreži 76
8.1.1. OSPF postavke na usmjerivaču MikroTik P1 76
8.1.3. OSPF postavke na usmjerivaču MikroTik P2 82
8.1.3. OSPF postavke na usmjerivaču MikroTik P3 85
8.1.4. OSPF postavke na usmjerivaču MikroTik PE-1 88
8.1.5. OSPF postavke na usmjerivaču MikroTik PE-2 92
8.2. Testiranje konekcije u kreiranoj testnoj mreži 95
8.3. Povezivanje lokalne računalne mreže na Internet 99
8.3.1. Konfiguriranje rubnog usmjerivača za pristup Internetu 100

8.3.2. Prevođenje lokalnih IP adresa u javne 102
8.4. MPLS postavke na usmjerivačima u kreiranoj mreži 105
8.4.1 MPLS postavke na usmjerivaču MikroTik P1 105
8.4.2. MPLS postavke na usmjerivaču MikroTik P2 108
8.4.3. MPLS postavke na usmjerivaču MikroTik P3 109
8.4.4. MPLS postavke na usmjerivaču MikroTik PE-1 111
8.4.5. MPLS postavke na usmjerivaču MikroTik PE-2 112
8.5. VPLS postavke na usmjerivačima u kreiranoj mreži 114
8.5.1. VPLS postavke na usmjerivaču MikroTik PE-1 114
8.5.2. VPLS postavke na usmjerivaču MikroTik PE-2 117
9. ZAKLJUČAK 121
LITERATURA 124
POPIS KRATICA I AKRONIMA 129
SAŽETAK 132
ABSTRACT 132
ŽIVOTOPIS 133

1. UVOD

Sve više mrežnih operatora počinje koristiti mrežne tehnike nove generacije u telekomunikacijskim mrežama. Jedna od takvih tehnika je i višeprotokolno komutiranje temeljeno na oznakama (engl. *MultiProtocol Label Switching* - MPLS[1]). MPLS omogućuje brzo i pouzdano usmjeravanje mrežnih paketa u usporedbi sa standardnim postupcima usmjeravanja koje se koristi u IP mrežama i širok raspon funkcionalnosti i veliku skalabilnost kako bi se zadovoljili zahtjevi sve većeg broja korisnika u mrežama. Zbog povećanja složenosti strukture današnjih mreža, povećana je i potreba za njihovim detaljnim planiranjem.

MPLS virtualna privatna mreža (engl. *MultiProtocol Label Switching Virtual Private Network* - MPLS VPN[2]) je fleksibilna metoda za transport i usmjeravanje nekoliko vrsta mrežnog prometa koristeći MPLS jezgrenu mrežu. Na rubovima mreže nalazi se jedan ili više rubnih korisničkih (engl. *Customer Edge* - CE[3]) usmjerivača koji se priključuju na jedan ili više rubnih mrežnih (engl. *Provider Edge* - PE[4]) usmjerivača, tj. usmjerivača pružatelja telekomunikacijskih usluga. Ti usmjerivači koriste odgovarajuće usmjerivačke protokole za razmjenu podataka unutar te između pojedinih autonomnih sustava kako bi mogli dinamički međusobno komunicirali.

U virtualnim privatnim mrežama (engl. *Virtual Private Network* – VPN) ostvaruje se sigurna (kriptirana) komunikacija putem javne (internetske) mreže. To znači da je korisnicima VPN mreža omogućeno slanje i primanje povjerljivih podataka putem javne mreže, kao u slučaju kada su njihova računala izravno povezana na istu privatnu lokalnu mrežu (engl. *Local Area Network* - LAN[5]), iako se fizički ne nalaze u istoj mreži.

Rad je podijeljen u 9 cjelina.

1. Uvod
2. Mreže pružatelja usluga
3. Implementacija MPLS-a
4. MPLS aplikacije
5. MPLS VPN inačice
6. Planiranje mreže
7. Postojeći alati za planiranje MPLS mreže

[1] MPLS - Višeprotokolno prospajanje oznaka, koristi se u jezgrenim mrežama pružatelja usluga.
[2] VPN - Računalna mreža koja spaja daleke mreže koristeći javne komunikacijske mreže kao što je Internet.
[3] CE - Rubni usmjerivač smješten u prostoru korisnika koji je povezan s PE usmjerivačem.
[4] PE - Rubni usmjerivač u mreži pružatelja usluga na kojem se postavlja i uklanja oznaka.
[5] LAN – Mreža namijenjena povezivanju računala i drugih mrežnih uređaja na manjim udaljenostima.

8. Konfiguracija
9. Zaključak

U drugom poglavlju opisani su dijelovi mreže pružatelja usluga; pristupna i jezgrena mreža te su dani primjeri za svaku od mreža. Također, definirana je PDH/SDH mreža kao primjer jezgrene mreže fizičkog sloja i ATM i IP mreža kao primjer jezgrenih mreža podatkovnog i mrežnog sloja. Osim toga, definirana je arhitektura mreža pružatelja usluga s tri sloja: jezgreni, distribucijski i pristupni sloj.

U trećem poglavlju opisan je razvoj MPLS-a, neki od ciljeva njegova razvoja te prednosti koje pruža njegova primjena. Također, definirani su glavni elementi MPLS mreže: zaglavlje, LSR, LSP, NHLFE, LFIB, FEC te glavni MPLS protokoli koji su podijeljeni na protokole za distribuciju oznaka i protokole usmjeravanja. Nakon toga, objašnjen je način rada MPLS mreže te su navedeni dijelovi od kojih se sastoji sama mreža.

U četvrtom poglavlju objašnjena su neka od MPLS aplikacijskih proširenja: MPLS TE, MPLS TP, MPLS VPN, MPLS QoS i GMPLS.

Budući da je MPLs VPN najprihvaćenije aplikacijsko proširenje MPLS mreže, u petom poglavlju opisane i MPLS VPN inačice: MPLS Layer 3 VPN, MPLS Layer 2 VPN, Virtual Private Wire Service i Virtual private LAN service.

U šestom poglavlju opisan je proces planiranja telekomunikacijske mreže koji se sastoji od predviđanja, dimenzioniranja i procjene prometnih zahtjeva u mreži. Zatim su navedene faze iteracijskog kruga planiranja: predviđanje u MPLS mreži, ugovor o razini usluge, otkrivanje mreže, simulacija i analiza neuspjelog slučaja, optimizacija, tehnike upravljanja mrežnim prometom i konfiguracija mreže, zahtjevi za kapacitetom te dijeljenje mrežnih resursa. Također, navedeni su i pojedini izazovi s kojima se susreću MPLS mreže. Izazovi su podijeljeni na izazove skaliranja i na izazove funkcionalnosti.

U sedmom poglavlju opisana su dva najčešće korištena alata za planiranje MPLS mreže: IP/MPLSView i iVNT.

U osmom poglavlju objašnjen je postupak konfiguracije uređaja u primjeru kreirane testne MPLS, odnosno VPLS mreže.

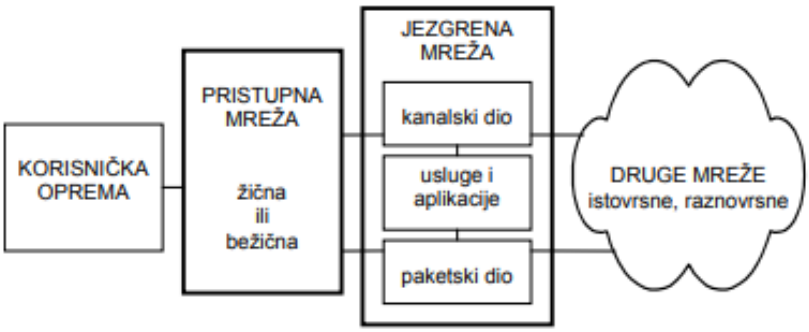
1.1. Zadatak diplomskog rada

Zadatak ovog diplomskog rada je analizirati višeprotokolno komutiranje temeljeno na oznakama - MPLS (engl. *Multiprotocol Label Switching*). U radu je potrebno dati pregled primjene MPLS virtualnih privatnih mreža - VPN (*Virtual private Networks*), njihovih inačica definiranih na pojedinim slojevima mrežnih modela te alata koji se koriste pri planiranju i analizi takvih mreža.

2. ARHITEKTURA TELEKOMUNIKACIJSKIH MREŽA

2.1. Prikaz mrežne arhitekture

Internetsku mrežu, globalnu paketnu podatkovnu mrežu, čini veliki broj međusobno povezanih mreža namijenjenih pružanju telekomunikacijskih usluga. U svakoj od mreža pružatelja telekomunikacijskih usluga razlikuju se dva osnovna dijela: pristupna i jezgrena mreža (Slika 2.1.). [1]



Slika 2.1. Arhitektura mreže [2]

Pristupna mreža (engl. *access network*) se može definirati kao mreža preko koje se priključuju korisnici, odnosno njihova oprema (npr. pokretni telefon, fiksni telefon, osobno računalo). Pristupna mreža može biti izvedena žično (engl. *wireline*) ili bežično (engl. *wireless*). Obilježje fiksne mreže je žični pristup, dok bežični pristup omogućuje komunikaciju u pokretu (npr. radijski kanal u pokretnoj mreži), uz napomenu da je u pokretnim mrežama samo pristup riješen radijskim prijenosom. [2]

Neki od primjera širokopojasnih rješenja u pristupnim mrežama temelje se na primjeni: digitalnih pretplatničkih linija (engl. *x Digital Subscriber Line* - xDSL[6]), optičkih niti (engl. *Fiber To The x* - FTTx[7]), mikrovalnog pristupa (engl. *Worldwide Interoperability for Microwave Access* - WiMAX[8]), kabelskih vodova.

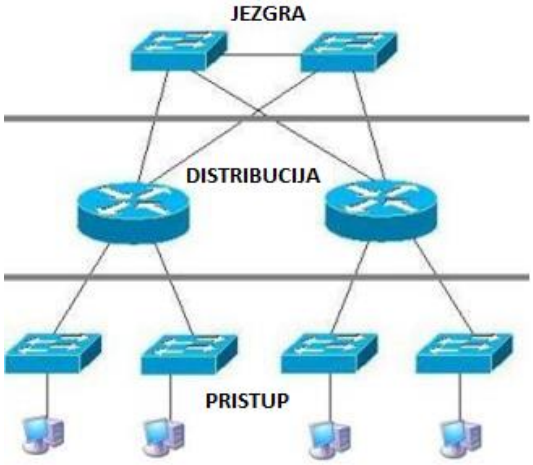
Jezgrena mreža (engl. *Core Network*) je mreža koja povezuje sustave u pristupnoj mreži te omogućuje komunikaciju s drugim mrežama. Sastoji se od sustava velikih kapaciteta i visokih performansi. Uz komutiranje i usmjeravanje informacijskih tokova, jezgrena mreža omogućuje

[6] xDSL - tehnologija koja se temelji na prijenosu informacija preko bakrene parice.
[7] FTTx - tehnologija koja se temelji na prijenosu informacija preko optičkih vlakana.
[8] WiMAX - bežični digitalni komunikacijski sustav namijenjen za formiranje bežičnih regionalnih mreža.

primjenu telekomunikacijskih usluga i aplikacija, njihovu prilagodbu zahtjevima korisnika i zaštitu te lociranje korisnika u pokretnim mrežama. [2] Neki od primjera rješenja koja se koriste u jezgrenim mrežama su višeprotokolno komutiranje temeljeno na oznakama (eng. *Multiprotocol Label Switching* - MPLS), asinkroni način prijenosa podataka (engl. *Asynchronous Transfer Mode* - ATM[9]), te sinkrona digitalna hijerarhija (engl. *Synchronous Digital Hierarchy* - SDH[10]).

Pružatelji usluga posjeduju, koriste i nadograđuju svoje pristupne mreže, no s porastom zahtjeva korisnika nužne su promjene i u jezgrenim mrežama. Kako jezgrena mreža povezuje pojedine čvorove pristupnih mreža, da bi bilo moguće prenositi podatke mora postojati središnja mreža koja povezuje dva kraja pristupne mreže.

Mrežna arhitektura ovisi o puno čimbenika, poput: zahtjeva korisnika, vrsti telekomunikacijskih usluga te proizvođaču mrežne opreme. Cisco system predlaže hijerarhijski model mreže s tri razine: jezgreni sloj, sloj distribucije i pristupni sloj (Slika 2.2.).



Slika 2.2. Arhitektura ISP mreže [3]

Jezgreni sloj sastoji se od najvećih, najbržih i najskupljih usmjerivača, a smatra se jezgrenom mrežom. Usmjerivači jezgrenog sloja koriste se za spajanje geografski odvojenih mreža te mijenjaju informacije na mreži što je brže moguće. Preklopnici koji rade na jezgrenom sloju prebacuju pakete što je brže moguće.

[9] ATM - Tehnika je prijenosa u telekomunikacijama koja se zasniva na asinkronom vremenskom .multipleksiranju odsječaka prometa veličine 53 bajta, od kojih je 48 koristan promet, a 5 čini zaglavlje.
[10] SDH - Dominantna tehnologija za multipleksiranje i prijenos digitalnih signala u transportnoj mreži, od govora i podataka do video signala.

Distribucijski i agregacijski sloj se nalazi između pristupnih i jezgrenih slojeva. Svrha ovog sloja je osigurati graničnu definiciju primjenom pristupnih lista i drugih filtara. Stoga distribucijski sloj definira pravila za mrežu i osigurava da su paketi pravilno usmjereni između podmreža i Virtualnih lokalnih mreža (engl. *Virtual Local Area Network* - VLAN[11]).

Pristupni sloj uključuje pristupne preklopnike koji su povezani s krajnjim uređajima (računala, pisači, poslužitelji i sl.). Preklopnici pristupnog sloja osiguravaju da se paketi isporučuju na krajnje uređaje. [4]

2.2. Slojevi mrežnih modela

Kako bi se smanjila složenost sustava, u mrežne modele uvedeni su mrežni slojevi. Broj slojeva i njihove funkcije mogu se u različitim mrežama razlikovati. U pravilu svaki sloj koristi usluge nižeg, a nudi usluge višem sloju. Slojevi razmjenjuju informacije preko odgovarajućih komunikacijskih sučelja i uz primjenu odgovarajućih komunikacijskih protokola. Slojevi i protokoli zajedno definiraju mrežnu arhitekturu.

U primjeni se razlikuju slojevi kod OSI modela te kod TCP/IP modela mrežne arhitekture. Pod fizičkim slojem TCP/IP modela se obično podrazumijeva mreža kojom je ostvaren pristup Internetu, što odgovara fizičkom sloju i sloju podatkovnog linka kod OSI modela. Na mrežnom sloju OSI modela, odnosno internetskom sloju TCP/IP modela ostvaruje se međusobno povezivanje mreža i podmreža. Najvažniji protokol ovog sloja je IP, a osim njega na ovom sloju prisutni su i neki usmjerivački i kontrolni protokoli. Na transportnom sloju modela najvažniji protokoli su TCP i UDP, dok se na aplikacijskom sloju modela nalaze rješenja za različite internetske aplikacije.

Transmisijska, odnosno prijenosna mreža može se promatrati u jezgrenoj i pristupnoj razini. Jezgrenom transmisijskom mrežom prenosi se agregirani promet korisnika iz svih pristupnih mreža između komutacijskih čvorova. Kao prijenosni medij u jezgrenoj mreži najviše se primjenjuju optički mediji, satelitski prijenos i žični mediji - parice i koaksijalni kabeli. U Republici Hrvatskoj jezgrena mreža je u potpunosti digitalizirana, a koristi optički prijenos i u manjoj mjeri usmjerene mikrovalne radiorelejne veze.

[11] VLAN - izvedba lokalne mreže u kojoj se logička podjela na domene prostiranja ostvaruje neovisno o fizičkoj povezanosti mrežnih uređaja na mrežne preklopnike

Promatrajući jezgrenu mrežu kroz osnovni referentni model za interkonekciju otvorenih sustava (engl. *Open Systems Interconnection Basic Reference Mode* - ISO/OSI[12]), možemo uočiti promjene. U početku je telekomunikacijska mreža radila na fizičkom sloju koji je zadužen za prijenos podataka, bit po bit, preko fizičkog medija. Primjer takve mreže je PDH/SDH mreža. Plesinkrona digitalna hijerarhija (engl. *Plesiochronous Digital Hierarchy* - PDH[13]) se zasniva na plesinkronom multipleksiranju. Termin plesinkron označava da svi uređaji rade na 'istim' frekvencijama, ali da nisu međusobno sinkronizirani. Veliki problem PDH mreža bila je njihova nefleksibilnost. Da bi se pristupilo samo jednom korisničkom kanalu od 64kb/s na višoj razini hijerarhije, bilo je nužno izvršiti demultipleksiranje do najniže razine hijerarhije, što je nepraktičan i neekonomičan proces. S početkom upotrebe optičkih linkova pojavila se mogućnost instaliranja još većih protoka u transportnim mrežama.[5] Također, razvoj tehnologije je omogućio upotrebu sofisticiranijih tehnika i algoritama u transportnim mrežama, pri čemu je došlo do razvoja SDH tehnologije u Europi i SONET tehnologije u Americi.

Sinkrona digitalna hijerarhija (engl. *Synchronous Digital Hierarchy* - SDH) je standardna tehnologija za sinkroni prijenos podataka na optičkim medijima. Ona omogućuje bržu i jeftiniju mrežnu povezanost od tradicionalne PDH opreme. U digitalnom telefonskom prijenosu pojam "sinkroni" znači da se bitovi iz jednog poziva prenose unutar jednog prijenosnog okvira. SDH koristi sljedeće sinkrone transportne module (engl. *Synchronous Transport Modules* - STM[14]) i brzine prikazane na slici 2.3.: STM-1 (155 Mbps), STM-4 (622 Mbps), STM-16 (2,5 Gbps) i STM-64 (10 Gbps).[6]

SONET	SDH RAZINE	BRZINA PRIJENOSA
STS-1 / OC-1	—	51.84 Mbps
STS-3 / OC-3	STM-1	155.52 Mbps
STS-12 / OC-12	STM-4	622.08 Mbps
STS-24 / OC-24	—	1244.16 Mbps
STS-48 / OC-48	STM-16	2488.32 Mbps
STS-192 / OC-192	STM-64	9953.28 Mbps

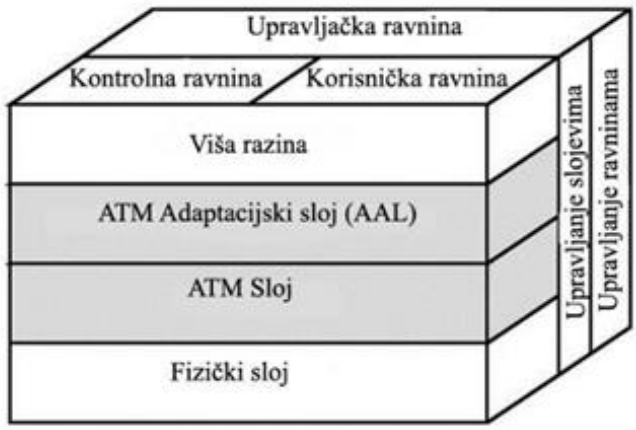
Slika 2.3. SDH i SONET transportni moduli i brzine [7]

[12] ISO/OSI model - Apstraktni, slojeviti model koji služi kao preporuka stručnjacima za razvoj računalnih mreža i protokola.
[13] PDH - tehnologija koja se koristi u telekomunikacijskim mrežama za prijenos velikih količina podataka preko digitalne transportne opreme kao što su svjetlovodni i mikrovalni radio sustavi
[14] STM - standard za prijenos podataka preko SONET-a.

Optička transportna mreža (engl. *Optical Transport Network* - OTN[15]) je noviji tip mreže, a obuhvaća skup optičkih mrežnih elemenata povezanih optičkim vezama koji mogu pružiti funkcionalnost transporta, multipleksiranja, prebacivanja, upravljanja, nadzora i izdržljivost optičkih kanala koji nose korisničke signale. [8]

Pri implementiranju protokola viših slojeva prvo su se počele koristiti ATM i IP mreže koje su definirale fizički i mrežni sloj. Asinkrona transportna mreža (engl. *Asynchronous Transfer Mode* - ATM) definirana je kao komunikacijska širokopojasna digitalna mreža u kojoj se koristi asinkroni način prijenosa signala. Upotrebljavaju se uređene skupine impulsa, tzv. paketi ili ćelije, koji moraju biti stalne duljine i koji u mrežama putuju velikim brzinama. Svaka od ćelija sastoji se od zaglavlja s adresom i od informacijskog polja s korisnom informacijom. U ATM mreži ćelije se mogu pojavljivati u nepravilnim intervalima. [9] ATM ima vlastiti referentni slojeviti model, koji se razlikuje od OSI modela i od TCP/IP modela. ATM se sastoji od tri sloja; fizički sloj, ATM sloj i ATM prilagodni sloj (AAL) (Slika 2.4.).

Zadatak ATM prilagodnog sloja je segmentacija informacija iz različitih izvora u pakete duljine 48 okteta i isporuka paketa ATM sloju. ATM sloj svakom paketu dodaje zaglavlje od 5 okteta pri čemu završava tvorba ATM ćelije, nakon čega se ćelija isporučuje fizičkom sloju. Fizički sloj pakira dobivene ćelije u različite vrste okvira¸ ovisno o vrsti prijenosa na fizičkom mediju. Slojevi su podijeljeni u tri osnovne ravnine: korisničku, kontrolnu i upravljačku. Teško konfiguriranje, održavanje i visoka cijena ATM uređaja bili su osnovni problemi ATM mreže zbog čega je zamijenjena s MPLS mrežom. [10]



Slika 2.4. ATM arhitektura [11]

[15] OTN – Optička prijenosna mreža koja se sastoji od skupa optičkih elemenata koji su povezani optičkim vlaknima.

IP mreža je komunikacijska mreža koja koristi Internet Protokol (IP) za slanje i primanje poruka između jednog ili više računala. Kao jedna od najčešće korištenih globalnih mreža, IP mreža se provodi u Internet mrežama, lokalnim mrežama (engl. *Local Area Network* - LAN) i poslovnim mrežama. IP mreža zahtijeva konfiguriranje svih domaćina ili mrežnih čvorova s paketom Prijenosnog kontrolnog protokola/Internet protokola (engl. *Transmission Control Protocol/ Internet Protocol* - TCP/IP[16]).

Svaki čvor koristi jedinstvenu logičku IP adresu, koja ga razlikuje od ostalih čvorova i pomaže inicirati podatkovnu komunikaciju s drugim domaćinima. IP mrežna komunikacija nastaje kada čvor šalje paket podataka drugom čvoru adresiranjem svoje IP adrese. Na sličan način, primatelj identificira pošiljatelja svojom IP adresom. IP mreža zahtijeva da svi povezani uređaji (poslužitelji, preklopnici, usmjerivači) budu konfigurirani s TCP/IP paketom i imaju valjanu IP adresu za obavljanje bilo koje mrežne komunikacije.

[16] TCP/IP – Protokoli putem kojih se podaci razmjenjuju između računala putem internetske veze.

3. VIŠEPROTOKOLNO KOMUTIRANJE PODATKOVNOG PROMETA U MREŽI TEMELJENO NA OZNAKAMA - MPLS

3.1. Razvoj MPLS tehnologije

Početak razvoja višeprotokolnog komutiranja temeljenog na oznakama (engl. *Multi-Protocol Label Switching* - MPLS) započeo je sredinom 90-ih godina prošlog stoljeća u brojnim pokušajima kombinacije IP i ATM tehnologija. Prvi takav pokušaj zabilježen na tržištu pripada tvrtki Ipsilon, a neke od zapaženijih proizvoda ponudili su Cisco Systems (*Tag Switching*), IBM (*Aggregate Route Based IP Switching*) i Cascade (*IP Navigator*).

Svrha svih tih proizvoda bilo je poboljšanje propusnosti i kašnjenja kod usmjeravanja koje se temelji na IP protokolu. Svi proizvodi temeljili su se na istom pristupu koji je podrazumijevao korištenje usmjerivačkog protokola, primjerice protokola za usmjeravanje izborom najkraćeg puta (engl. *Open Shortest Path First* - OSPF[17]), kako bi se definirao put te kako bi se dodijelili paketi tim putevima u mreži u kojoj se nalaze ATM komutatori koji su odgovorni za usmjeravanje paketa. IETF[18] (engl. *Internet Engineering Task Force*) organizacija je 1997. godine definirala MPLS radnu skupinu koja je radila na razvoju zajedničkog, standardiziranog pristupa. Do prvog skupa propisanih standarda čekalo se čak do 2001. godine. [12]

Neki od ciljeva razvoja MPLS-a su:

- Zadovoljavanje sve većih prometnih zahtijeva postavljenih u IP mrežama;
- QoS podrška u IP mrežama;
- Osiguranje diferencijalnih razina usluga temeljenih na IP protokolu;
- mogućnost povezivanja glasa, videa i aplikacija preko jedne IP mreže;
- veća efikasnost uz nižu cijenu;
- virtualne privatne mreže.

3.2. Implementacija MPLS rješenja

Višeprotokolno komutiranje temeljeno na oznakama - MPLS je tehnologija koja osigurava tradicionalni model prosljeđivanja paketa kroz mrežu, ali na efikasniji i brži način, nego što je to

[17] OSPF - Usmjerivački protokol, protokol stanja veze koji zahtjeva slanje obavijesti o stanju veze ostalim usmjerivačima unutar istog hijerarhijskog prostora.
[18] IETF – Svjetska organizacija koja oblikuje i publicira norme za Internet u obliku dokumenata pod nazivom Request For Comment – RFC

omogućeno putem protokola u ATM ili FR (engl. *Frame Relay* - FR[19]) mrežama. Prilikom standardizacije MPLS protokola od strane IETF-a, uveden je konekcijsko orijentirani koncept u beskonekcijske mreže.

Prilikom usmjeravanja u ATM i FR mrežama, zaglavlje svakog paketa koji prolazi kroz mrežu analizira se pri svakom skoku na putu od izvorišnog do odredišnog usmjeritelja. Za razliku od toga, MPLS tehnologija prilikom transporta paketa kroz mrežu koristi postupak komutacije oznaka. Vrlo bitna prednost takvog postupka je da se informacije iz zaglavlja paketa analiziraju samo jednom, na ulaznom rubnom usmjerivaču u mreži, tzv. LER[20] (engl. *Label Edge Router*) usmjerivaču, a daljnji postupak usmjeravanja paketa temelji se samo na provjeri oznaka koje predstavljaju identifikacijske oznake paketa. S razvojem tehnologije napredniji su postali i mrežni čvorovi, pa se navedeni problem usmjeravanja mogao zaobići i bez MPLS-a, no u IP mrežama postojao je nedostatak mehanizama za očuvanje kvalitete usluge (engl. *Quality of Service* - QoS[21]) i potpuni izostanak tehnika upravljanja mrežnim prometom, koji je dolazio do izražaja s većim prometnim opterećenjem. [13]

U odnosu na prethodne metode usmjeravanja podataka u mreži, korištenje MPLS tehnologije pruža brojne prednosti, neke od njih su:

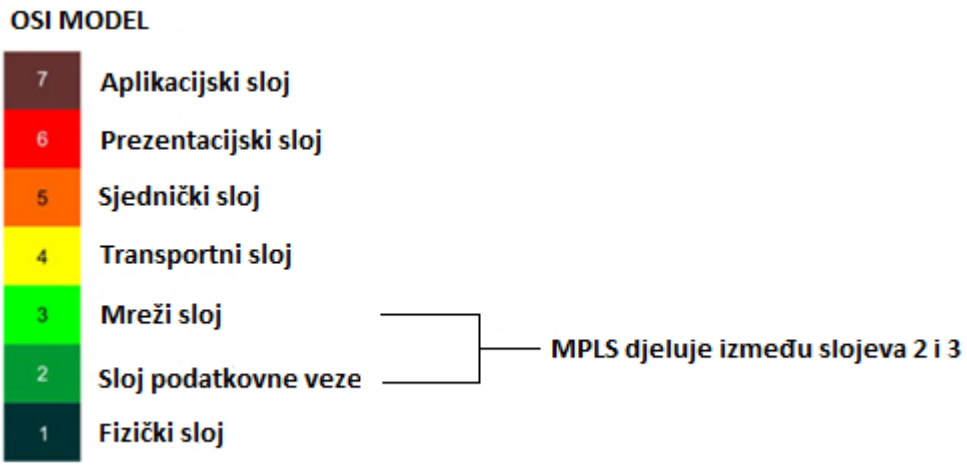
- integracija brzine i značajki drugog sloja mreže sa inteligencijom i skalabilnošću karakterističnima za treći sloj mreže;
- prijenos zasnovan na primjeni okvira i ćelija;
- primjena mehanizama za očuvanje definiranih razina kvalitete usluga (QoS) te tehnika upravljanja mrežnim prometom;
- mogućnost beskonačnog slaganja oznaka;
- mogućnost prilagođavanja većeg broja korisnika MPLS tehnologiji;
- mogućnost ugradnje MPLS mreže u već postojeće mreže.

MPLS koristi više protokola za distribucija oznaka, od kojih su najpopularniji protokol distribucije oznaka (engl. *Label Distribution Protocol* - LDP[22]) i protokol rezervacije resursa za tehnike upravljanja mrežnim prometom (engl. *Resource Reservation Protocol – Traffic Engineering –*

[19] FR - je visokoučinkoviti WAN protokol koji djeluje na fizičkim i podatkovnim veznim slojevima OSI referentnog modela.
[20] LER - Usmjerivači koji se nalaze na ulaznim i izlaznim točkama MPLS mreže, oni rukuju i s označenim i neoznačenim paketima.
[21] QoS - Mehanizam za kontrolu rezervacije mrežnih resursa (npr., propusnosti mreže).
[22] LDP - protokol koji osigurava razmjenu pridruženih oznaka između usmjerivača.

RSVP-TE[23]). Usmjerivački protokol temeljen na ograničenjima protokola distribucije oznaka (engl. *Constraint-based Routing LDP* - CR-LDP[24]) je ekstenzija LDP protokola i predstavlja jedan od signalnih protokola za tehnike upravljanja mrežnim prometom.

MPLS pripada mrežnom ili podatkovnom sloju OSI modela, budući da ima funkcije pojednostavljenog konekcijskog prosljeđivanja paketa na podatkovnom sloju i mogućnost proširivanja i fleksibilnost mrežnog sloja. Prema tome, MPLS predstavlja nadogradnju mrežnog i podatkovnog sloja, pa je on protokol „2.5“ sloja (Slika 3.1.). [14]



Slika 3.1. Pozicija MPLS-a u OSI modelu [15]

3.3. Osnovni elementi MPLS rješenja

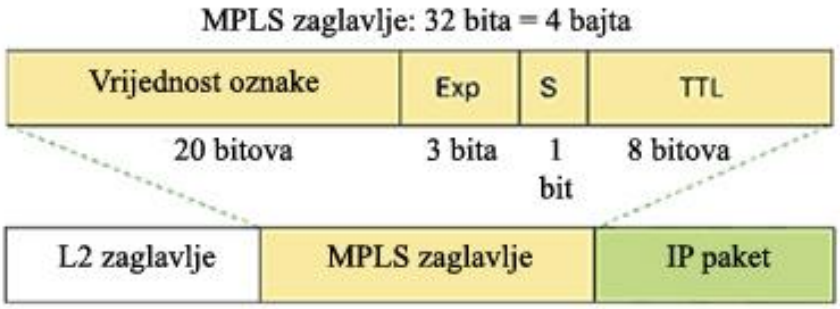
3.3.1. Zaglavlje MPLS paketa

Zaglavlje MPLS oznake (engl. *label header*) dugo je 32 bita. Budući da MPLS djeluje između drugog i trećeg sloja OSI modela ovo zaglavlje naziva se još i umetnuto zaglavlje (engl. *shim header*) jer se umeće iza zaglavlja podatkovnog sloja, a ispred zaglavlja mrežnog sloja.
Zaglavlje MPLS-a podijeljeno je na četiri različita polja (Slika 3.2.):

- *Label* - polje dugo 20 bita, označava broj oznake, njime se prosljeđuju MPLS paketi i ono određuje klasu ekvivalentnog prosljeđivanja (FEC);
- *Experimental* - ovo polje izvorno je rezervirano za eksperimentalnu upotrebu, no danas se obično upotrebljava za klasu implementacije usluge. Usmjerivač koriste ovo polje veličine tri bita kako bi odlučili gdje će se u redu čekanja postaviti paket;

[23] RSVP-TE - Koristi se za uspostavljanje MPLS transportnih LSP-ova kada postoje zahtjevi za tehnikama upravljanja mrežnim prometom.
[24] CR-LDP – Protokol koji sadrži proširenja za LDP protokol, omogućuje širenje informacija korištenih za postavljanje putova izvan onoga što je dostupno za protokol usmjeravanja.

- *Bottom of Stack* – ovo polje predstavlja zadnju oznaku u nizu oznaka prije IP paketa. Osim toga, moguće je grupirati više oznaka u jednu oznaku, polje duljine jedan bit;
- *Time To Live* (TTL) - polje koje se koristi se za praćenje puta i opisuje životni vijek MPLS paketa. Pri prolasku paketa kroz LSR, TTL vrijednost smanjuje se za jedan. Ukoliko je prije odredišnog čvora TTL vrijednost jednaka nuli, paket će se odbaciti. [16]



Slika 3.2. MPLS zaglavlje [18]

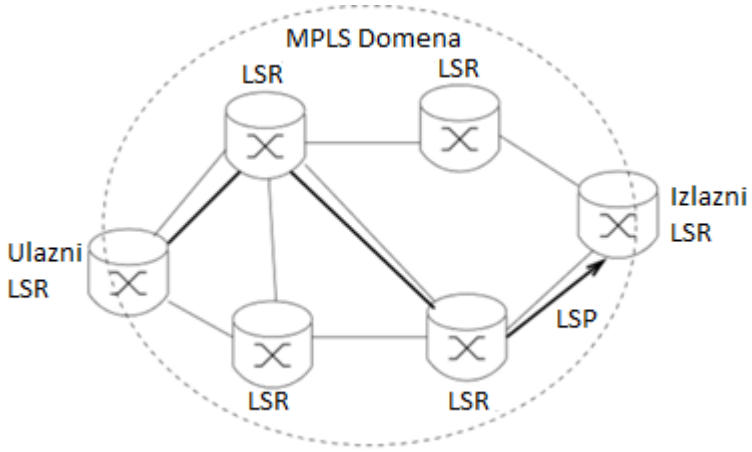
3.3.2. Usmjerivači u MPLS mreži

U MPLS mrežama primjenjuju se dvije vrste usmjerivača – LSR (engl. *Label Switched Router*[25]) usmjerivači i LER (engl. *Label Edge Router*) rubni usmjerivači. LSR usmjerivač je usmjerivač koji spada pod fizički dio mreže. LSR usmjerivači mogu brzo usmjeravati podatkovne pakete bez potrebe za provjerom tablica usmjeravanja ili odrađivanjem puta usmjeravanja koje bi u obzir uzelo vrijeme slanja/primanja podataka. Budući da oznake već sadrže upute o putevima paketa, usmjerivač mora jednostavno usmjeravati pakete na temelju uputa na oznakama. [17]

Postoje tri različite vrste LSR-a, diferencirane prema lokaciji i položaju na LSP[26] (engl. *Label Switched Path*) putu paketa, a to su (Slika 3.3.):

- ulazni LSR (engl. *ingress LSR*) – rubni LSR koji prima neoznačeni paket kojem zatim dodaje oznaku te ga šalje u MPLS domenu;
- tranzitni usmjerivač (engl. *transit LSR*) - nalazi se usred LSP-a, prebacuje MPLS pakete na sljedeći put u LSP-u, a koristi sučelje iz kojeg dolazi paket i MPLS zaglavlje za informacije o odredištu.
- izlazni LSR (engl. *egress LSR*) – rubni LSR koji prima označene pakete kojima zatim uklanja oznaku i isporučuje ih dalje.

[25] LSR - MPLS usmjerivač koji obavlja usmjeravanje samo na temelju oznake.
[26] LSP - Jednosmjerni put kroz MPLS mrežu.

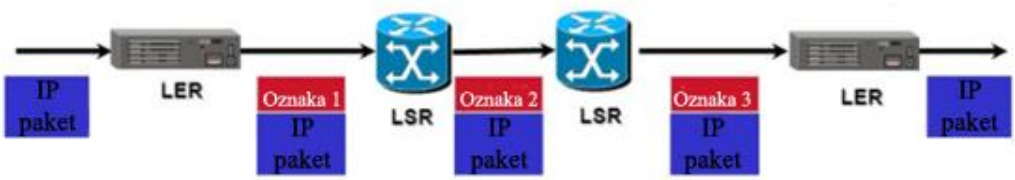


Slika 3.3. Prikaz MPLS domene i pripadajućih LSR-ova [17]

Operacije koje obavlja LSR su: stavljanje jedne ili više oznaka na stog, skidanje oznake sa stoga i mijenjanje oznake pri skoku. *Imposing* i *disposing* LSR predstavljaju ulazni odnosno izlazni LSR. Kod ulaznog LSR-a, oznake se stavljaju na neoznačene pakete, a kod izlaznog LSR-a te oznake se uklanjaju.

3.3.3. Put paketa kroz MPLS mrežu

LSP (engl. *Label Switched Path*) put je jednosmjerni put kroz MPLS mrežu. Usmjerivači u MPLS mreži mijenjaju MPLS informacije kako bi postavili te putove za različite izvorišno-odredišne parove. LSP je moguće postaviti pomoću bilo kojeg signalnog protokola kao što su LDP, RSVP ili BGP. LSP predstavlja put u MPLS mreži kojim putuju označeni paketi jedne veze. Prvi LSR na LSP putu je ulazni LSR, dok je posljednji LSR na LSP putu izlazni LSR. Svi usmjerivači prebacivanja oznaka između ulaznog i izlaznog su posredni. Paket na ulaznim i izlaznim usmjerivačima dobiva oznaku pri čemu može putovati LSR-ovima kroz mrežu. Na rubnom izlaznom usmjerivaču ta oznaka se ponovno skida i paket nastavlja svojim putem (Slika 3.4.). [18]



Slika 3.4. Prikaz prolaska paketa kroz LSP [19]

3.3.4. Određivanje sljedećeg skoka paketa u MPLS mreži

U MPLS mreži koristi se NHLFE[27] (engl. *Next Hop Label Forwarding Entry*) tablica za prosljeđivanje označenog paketa mrežom prema idućem čvoru. NHLFE sadrži informacije o:

- sljedećem skoku paketa;
- akciji koja se mora izvršiti na stogu oznaka paketa:
    - zamjena oznake na vrhu stoga s određenom novom oznakom;
    - zamjena oznake na vrhu stoga s određenom novom oznakom, a zatim uklanjanje jedne ili više navedenih novih oznaka na stogu.

Svaka oznaka dolazećeg paketa može biti povezana sa određenom NHLFE. U slučaju da se prometni tok podjeli na različite puteve postoji mogućnost za više NHLFE za jednu oznaku. [20]

3.3.5. Baza podataka za prosljeđivanje paketa prema oznakama

Baza podataka LFIB[28] (engl. *Label Forwarding Information Base*) definira način upravljanja prosljeđivanjem paketa pri kojem su odredišta i dolazne oznake povezane s odlaznim sučeljima i oznakama. Paradigma prosljeđivanja koju koristi MPLS temelji se na pojmu zamjene oznaka. Kada LSR primi paket s oznakom, prekidač koristi oznaku kao indeks u svojoj LFIB bazi. LFIB tablica je ekvivalent IP tablici usmjeravanja (Slika 3.5.) [21]

```
R1#sh mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     2.2.2.2/32        0          Fa1/0      10.0.12.2
17     17          3.3.3.3/32        0          Fa1/0      10.0.12.2
18     18          4.4.4.4/32        0          Fa1/0      10.0.12.2
19     Pop tag     10.0.24.0/24      0          Fa1/0      10.0.12.2
20     Pop tag     10.0.23.0/24      0          Fa1/0      10.0.12.2
```

Slika 3.5. LFIB tablica [21]

3.3.6. Prosljeđivanje skupa MPLS paketa

FEC[29] (engl. *Fowarding Equivalence Class*) se definira kao grupa ili tok paketa koji se prosljeđuju istom putem i jednako se tretiraju u skladu s postupkom prosljeđivanja. Svi paketi koji pripadaju istoj klasi prosljeđivanja imaju iste oznake, dok svi paketi s istim oznakama ne moraju pripadati istoj klasi prosljeđivanja, budući da se mogu razlikovati po EXP oznakama. Ako im se razlikuju

[27] NHLFE - Koristi se prilikom prosljeđivanja označenog paketa, sadrži informacije o sljedećem skoku paketa.
[28] LFIB - Tablica koju usmjerivač koristi za prosljeđivanje paketa označenih putem mreže.
[29] FEC – Grupa dolaznih paketa sa sličnim karakteristikama.

EXP oznake, paketi mogu imati drugačiji postupak prosljeđivanja i mogu pripadati drugačijim FEC klasama. Ulazni LSR odlučuje kojoj klasi pripada koji FEC, on klasificira pakete i dodaje im oznaku. [17]

3.4. Protokoli u MPLS mrežama

3.4.1. Protokoli za distribuciju oznaka

3.4.1.1. LDP protokol

LDP protokol (engl. *Label Distribution Protocol*) kontrolni je protokol koji u MPLS mreži omogućava MPLS usmjerivačima razmjenu informacija na temelju kojih će formirati tablice usmjeravanja LFIB (engl. *Label Forwarding Information Base*) baze podataka. Na temelju oznaka koje služe kao izravni indeksi za adresiranje LFIB tablice, usmjeravanje paketa bit će osigurano pomoću oznaka koje su kraće od IP adrese. Svaki usmjerivač šalje svojim susjedima podatke o tome koja oznaka predstavlja koju FEC grupu dok će susjedni MPLS usmjerivači koristiti te oznake kada im se budu prosljeđivali paketi za te FEC klase. MPLS usmjerivač svakom od svojih susjeda šalje onoliki broj poruka koliko ima aktivnih oznaka. Susjedni usmjerivači dalje šalju ove podatke svojim susjedima, koristeći različite vrijednosti oznaka za označavanje istih FEC grupa. Tako se informacije šire kroz MPLS mrežu i svaki MPLS usmjerivač u mreži ima informacije o svim FEC grupama u mreži. Vrlo bitno je spriječiti pojavljivanje petlji prilikom usmjeravanja paketa na temelju oznaka. Kako bi se to izbjeglo, svakoj poruci koja nosi informacije o tome na koju FEC grupu se odnosi pojedina oznaka, dodaje se ID usmjerivača kojeg je FEC grupa koristila.

Kada MPLS usmjerivač primi poruku od strane sučelja preko kojeg on inače ne bi slao pakete prema usmjerivaču čiji se ID nalazi u LDP poruci, on tu poruku zanemaruje, jer bi prihvaćanjem te poruke i daljnjim prosljeđivanjem napravio petlju svojim susjedima. Posljedica ovoga bilo bi dodjeljivanje više oznaka istim FEC grupama i neoptimalno usmjeravanje prometa putem MPLS protokola. Protokoli viših slojeva koji rade s IP adresama i koji koriste tablicu usmjeravanja, svakom sučelju prosljeđuju informacije o tome koji je usmjerivač dostupan preko tog sučelja na temelju njegovog ID-a. MPLS dobiva potvrdu kada njegov susjed primi LDP poruku o ažuriranju oznaka, ali ne zna da li je ažurirao LFIB tablicu pa mu nastavlja periodički slati LDP poruke. Budući da susjedni usmjerivači odbacuju neke od ovih poruka, one čine beskorisni promet, a ukoliko bi neka veza otkazala, te poruke pomažu pri rekonfiguraciji LSP puta i oporavku mreže. Ukoliko je preko tog sučelja usmjerivač čiji se ID nalazi u poruci, postao dostupan na temelju tablice usmjeravanja, susjedni će usmjerivač početi prihvaćati LDP poruke i pomoću njih ažurirati svoju tablicu.

Vrlo bitno je uočiti kako MPLS usmjerivač ne donosi odluke o klasifikaciji paketa na temelju vlastite tablice usmjeravanja, nego na temelju baza podataka koje dobiva od susjednih usmjerivača. Također je bitno uočiti i da se LFIB tablica koristi za usmjeravanje korisnog prometa u jednom smjeru, dok se tablica koju koristi LDP protokol koristi za usmjeravanje kontrolnih paketa u suprotnom smjeru. [22]

3.4.1.2. CR-LDP protokol

CR-LDP protokol (engl. *Constraint-based Routing Label Distribution Protocol*) je jednostavan, skalabilan, otvoren, prometni, inženjerni, signalni protokol za MPLS IP mreže. To je produžetak LDP protokola, jednog od protokola u MPLS arhitekturi. CR-LDP sadrži proširenja za LDP kako bi proširio njegove mogućnosti, kao što su definiranje rute na temelju podataka koji nisu usko vezani uz usmjeravanje. Na primjer, LSP se može postaviti na temelju jasnih ograničenja na putu, ograničenja kvalitete usluga i drugih ograničenja. Usmjeravanje na temelju ograničenja (CR) je mehanizam koji se koristi za ispunjavanje uvjeta tehnika upravljanja mrežnim prometom. CR-LDP je gotovo isti kao i osnovni LDP u strukturi paketa, ali sadrži neke dodatne vrste, duljinu, vrijednost (TLV) koji u osnovi postavljaju LSP na temelju ograničenja.

CR-LDP osigurava mehanizme za uspostavljanje eksplicitno usmjerenih LSP-ova. Ti su mehanizmi definirani kao proširenja na LDP. Budući da je LDP *peer-to-peer* protokol koji se temelji na uspostavljanju i održavanju TCP sjednica, moguće je navesti sljedeće prednosti CR-LDP protokola:

- CR-LDP poruke pouzdano su isporučene od strane temeljnog TCP-a, a informacije o stanju podataka povezane s eksplicitno usmjerenim LSP-ovima ne zahtijevaju periodično osvježavanje.
- CR-LDP poruke kontroliraju se putem TCP-a.

CR-LDP omogućuje specifikaciju skupova parametara koji se signaliziraju uz zahtjev za postavljanje LSP-ova. Štoviše, mreža može biti opremljena skupom prometnih funkcija na temelju modela integriranih usluga (engl. *Integrated Services* - intServ[30]), što može uključivati označavanje, mjerenje, održavanje poretka i oblikovanje. [23]

[30] intSERV - Arhitektura koja određuje elemente koji jamče kvalitetu usluge (QoS) na mrežama.

3.4.1.3. RSVP-TE protokol

RSVP-TE (engl. *Resource Reservation Protocol-Traffic Engineering*) protokol je poboljšani RSVP protokol za MPLS. RSVP-TE nije pravi protokol za usmjeravanje, ali radi s protokolima usmjeravanja. RSVP-TE koristi se za uspostavljanje MPLS transportnih LSP putova kada postoje zahtjevi za tehnikama upravljanja mrežnim prometom. Uglavnom se koristi za pružanje QoS-a i balansiranje opterećenja preko mrežne jezgre, a uključuje sposobnost upravljanja svim optičkim mrežama. [24]

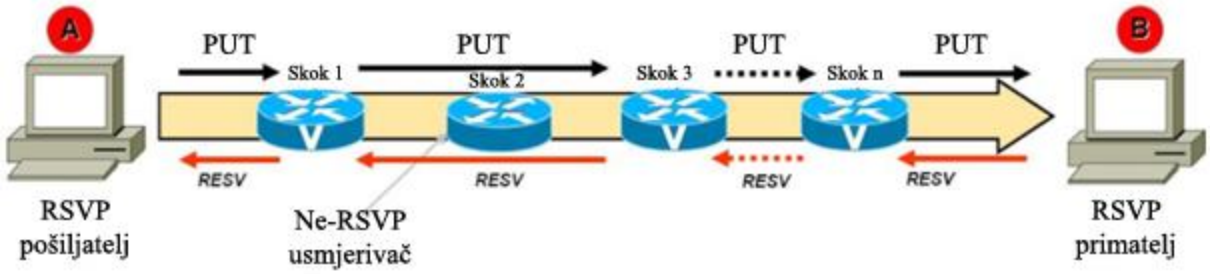
Za RSVP-TE potreban je dvosmjerni protok. Kako bi se to omogućilo, moraju postojati dvije RSVP sesije, budući da je RSVP-TE jednosmjeran protokol.

RSVP-TE donosi prednosti MPLS-u. Neke od prednosti su:

- sposobnost definiranja LSP staza i odabir puta od strane administratora;
- napredni izračun troškova, ne ograničavajući se na vrijednosti troškova IGP[31] (engl. *Interior Gateway Protocol*) protokola;
- sposobnost izrade funkcionalne rezervacije resursa.

Postoje dvije glavne vrste RSVP - TE poruka (Slika 3.6.) :

- *Path* poruka – šalje se od pošiljatelja do primatelja i pohranjuje stanje puta u svakom čvoru duž puta;
- *Resv* poruka – šalje se od primatelja do pošiljatelja. *Resv* poruka uključuje podatkovni objekt *flowspec* koji identificira resurse potrebne za protok.



Slika 3.6. RSVP - TE poruke [25]

[31] IGP – protokol koji se koristi za distribuciju informacija o rutama unutar autonomnih sustava.

3.4.2. Protokoli usmjeravanja

3.4.2.1. Usmjeravanje izborom najkraćeg puta

Protokol usmjeravanja izborom najkraćeg puta, tj. OSPF (engl. *Open Shortest Path First*) protokol je protokol za usmjeravanje razvijen za IP mreže i baziran na algoritmu prvog najkraćeg puta (engl. *Shortest Path First* - SPF[32]). OSPF je otvoreni protokol, što znači da su njegove specifikacije u javnoj domeni. Računanje optimalnog puta računa se na temelju vektora udaljenosti (engl. *distance-vector*). Podaci o usmjeravanju distribuiraju se na način da usmjerivač dijeli svoju tablicu usmjeravanja sa susjednim usmjerivačima.

OSPF je *link-state* protokol koji zahtjeva slanje *link-state* obavijesti (LSA-s) ostalim usmjerivačima unutar istog hijerarhijskog prostora. Unutar obavijesti nalaze se zapamćene rute kojima se želi poslati podatak kroz mrežu. OSPF izabire najbolju rutu do odredišta. Pri komunikaciji sa susjednim usmjeriteljima, iz tablice usmjeravanja šalju se samo informacije o stanju pojedinog linka. [26]

3.4.2.2. Poboljšani protokol za unutrašnje usmjeravanje

Poboljšani protokol za unutrašnje usmjeravanje, tj. EIGRP[33] (engl. *Enhanced Interior Gateway Routing Protocol*) je protokol koji ima osobine protokola koji prate stanja linkova i protokola koji prate vektore udaljenosti. EIGRP se ipak oslanja na *analize vektora udaljenosti* gdje se informacije o ostatku mreže dobivaju od izravno povezanih susjeda. Pronalaženje najpovoljnijeg puta između dva čvora u mreži obavlja se usporedbom udaljenosti svih puteva koji postoje između čvorova. Pri izračunu udaljenosti koriste se fizički parametri linkova duž puta: propusni opseg, kašnjenje, opterećenje, pouzdanost. Kada je mreža stabilna, EIGRP protokol šalje informacije o usmjeravanju samo u slučaju promjene u mreži.

EIGRP koristi *hello* mehanizam za određivanje dostupnosti susjednih usmjerivača. Za proračun najkraćeg puta do odredišta u mreži koristi se DUAL[34] (engl. *Diffusing Update* Algorithm) algoritam pomoću kojeg se osigurava određivanje puteva bez petlji. Korištenjem DUAL algoritma EIGRP čuva rezervne puteve i na taj način se može brzo prilagoditi određenim promjena u mreži. Podržavanje jednakog i nejednakog raspoređivanja opterećenja, EIGRP omogućava mrežnim administratorima da bolje organiziraju distribuciju prometa kroz mrežu. [27]

---

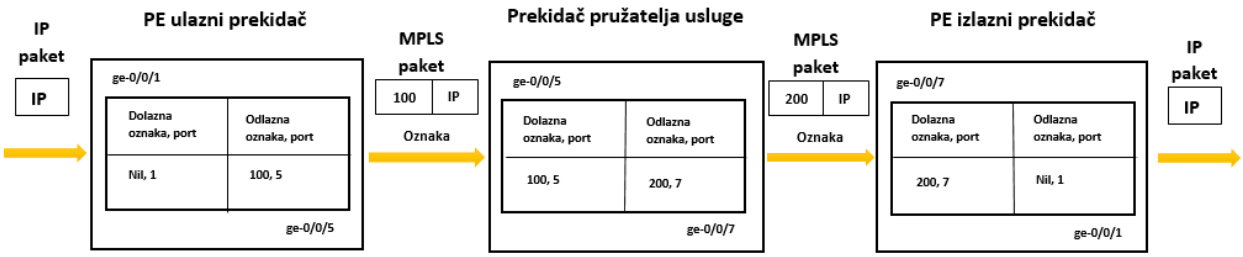
[32] SPF - Algoritam usmjeravanja u kojem usmjerivač izračunava najkraći put između svakog para čvorova u mreži.
[33] EIGRP - Protokol usmjeravanja koji omogućava dobru skalabilnost kao i izuzetno brzu konvergenciju mreže.
[34] DUAL - Konvergencijski algoritam koji se koristi kako bi se spriječile petlje usmjeravanja putem kontinuiranog izračuna rute.

3.5. Struktura MPLS mreže

MPLS mrežni usmjerivači podijeljeni su na dvije različite vrste uređaja: jezgrene usmjerivače i rubne uređaje. Položaj uređaja u mreži određuje funkcije i zadatke uređaja. Rubni uređaji nalaze se na rubovima MPLS domene i nazivaju se LE (engl. *Label Edge*) usmjerivačima ili PE (engl. *Provider Edge*) usmjerivačima. Jezgreni usmjerivači poznati su kao LS (engl. *Label Switching*) usmjerivači ili P[35] (engl. *Provider*) usmjerivači. Kada IP paket dođe pred ulazni čvor MPLS mreže, između ulaznog i izlaznog PE usmjerivača uspostavlja se LSP put. Bitno je zaključiti kako za svaki ulazno-izlazni par postoji unaprijed postavljen (statički ili dinamički) LSP put, koji može prolaziti kroz različite P usmjerivače.

Na temelju FEC grupe kojoj paket pripada, određuju se P usmjerivači kroz koje će prolaziti paketi te se određuje kako će se oni testirati. Ovo je jedino vrijeme kada je potrebno donijeti odluku u određenoj domeni i jedini trenutak u kojem se analizira zaglavlje. Nakon toga, sve se odluke o usmjeravanju obavljaju pomoću oznaka. PE usmjerivač na samom ulazu u mrežu odrađuje poveznicu između oznake, paketa i FEC grupe. [28]

Kod prijenosa paketa kroz MPLS mrežu, usmjeritelji zamjenjuju oznake paketa i prosljeđuju ih prema unaprijed definiranom putu, proces se naziva zamjena oznaka (engl. *label swapping*).



Slika 3.7. Postupak zamjene oznaka [29]

Slika 3.7. prikazuje IP paket bez oznake koji dolazi na rubno korisničko sučelje (ge-0/0/1) ulaznog PE preklopnika. Ulazni PE preklopnik pregledava paket i označava odredište tog paketa kao izlazni PE preklopnik. Ulazni PE preklopnik primjenjuje oznaku 100 na paket i šalje MPLS paket na odlazno MPLS jezgreno sučelje (ge-0/0/5). MPLS paket se prenosi preko MPLS tunela kroz

[35] P – Usmjerivač koji funkcionira kao tranzitni usmjerivač jezgrene mreže, on je obično povezan s jednim ili više PE usmjerivača.

preklopnik pružatelja usluge, gdje stiže na sučelje ge-0/0/5 s oznakom 100. Preklopnik pružatelja usluge zamjenjuje oznaku 100 s oznakom 200 i prosljeđuje MPLS paket preko svog jezgrenog sučelja (ge -0/0/7) do sljedećeg skoka na tunelu, što je izlazni PE preklopnik. Izlazni PE preklopnik prima MPLS paket preko svog jezgrenog sučelja (ge-0/0/7), uklanja MPLS oznaku i šalje IP paket izvan rubnog korisničkog sučelja (ge-0/0/1) do odredišta koje je izvan tunela. [29]

3.6. Funkcionalnost MPLS mreže

MPLS mreža sastoji se od PE i P usmjerivača. PE usmjerivač dodaje MPLS zaglavlje u IP paket podataka. Nakon što PE usmjerivač odradi enkapsulaciju i poveže paket s odgovarajućom FEC grupom, paket se prosljeđuje drugom P usmjerivaču na putu prema krajnjem PE usmjerivaču. Umetanje i uklanjanje oznaka odrađuju rubni usmjerivači, a zamjenu jedne oznake s drugom odrađuju P usmjerivači. Tri su funkcije MPLS čvora: „SWAP, PUSH, POP“. Prilikom distribuiranja oznaka do susjednih i drugih mrežnih čvorova, uspostavlja se LSP put za različite FEC grupe. Postoje dva tipa puta; jasno odabrani put između dva PE usmjerivača ili skok po skok odabrani put. Na temelju toga, jasno je kako čvorovi na putu sami biraju izlazno sučelje poznavajući topologiju mreže, koja je dobivena od jednog protokola usmjeravanja. Za pravilno distribuiranje oznaka važno je imati signalizacijske protokole koji mogu pouzdano prenijeti informacije o vezama između oznake i FEC-a. Najpopularniji takvi protokoli su LDP i RSVP-TE. Osim njih, za distribuciju veza između oznaka i LSP-a koriste se i IP protokoli kontrolne ravnine; BGP (engl. *Border Gateway Protocol*) protokol, RVSP (engl. *Resource Reservation Protocol*) protokol i PIM[36] (engl. *Protocol Independent Multicast*) protokol. LSR usmjerivač će u ovisnosti o potrebi i zahtjevima koristiti i LDP i RSVP-TE protokol. Unatoč različitim protokolima za prijenos oznaka i informacija vezanih uz MPLS mrežu, upotrebljavaju se i IP protokoli usmjeravanja; EIGRP ili OSPF protokol; koji su vrlo bitni u kontrolnoj ravnini. Oni omogućavaju čvorovima u mreži da pronađu susjedne čvorove i dobiju informacije o topologiji MPLS mreže. [30]

[36] PIM - skup usmjerivačkih protokola za višesmjerno slanje od kojih je svaki optimiziran za drugačije okruženje.

4. MPLS APLIKACIJE

Osim što je primjena MPLS tehnologije pogodna zbog njenih značajki i vrlo jednostavne implementacije, ona omogućuje i primjenu dodatnih aplikacijskih proširenja. Aplikacijska proširenja obuhvaćaju usluge zasnovane na primjeni MPLS tehnologije koje nisu odmah omogućene pri uspostavi MPLS mrežnog okruženja. Funkcionalnost svake takve aplikacije dijeli se na kontrolni i podatkovni dio.

Neka od MPLS aplikacijskih proširenja su:

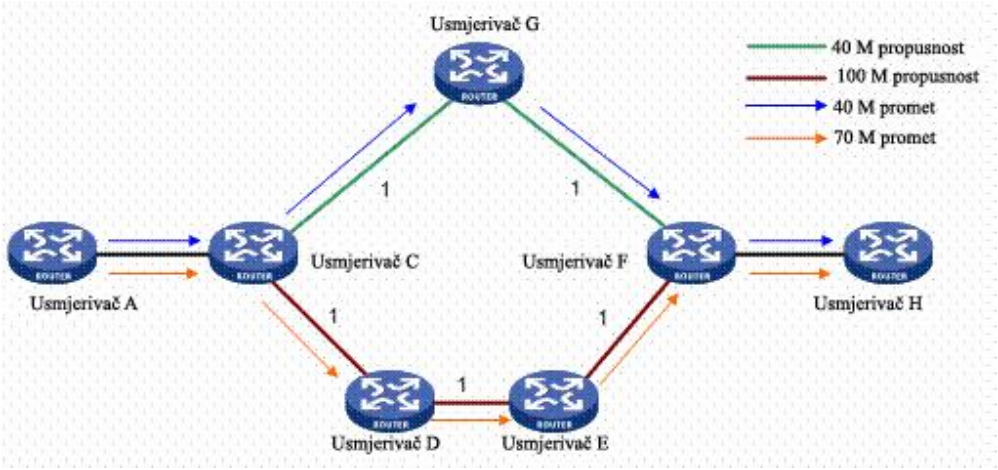
- MPLS tehnike upravljanja mrežnim prometom (engl. *MPLS Traffic Engineering* – MPLS TE);
- MPLS profil mrežnog prometa (engl. *MPLS Transport Profile* – MPLS TP);
- MPLS virtualne privatne mrže (engl. *MPLS Virtual Private Networks* – MPLS VPN);
- Mehanizmi očuvanja kvaliteta usluga u MPLS mrežama (engl. *MPLS Quality of Service* – MPLS QoS);
- Poopćenje primjene MPLS tehnologije (engl. *Generalize MPLS* - GMPLS).

4.1. MPLS tehnike upravljanja mrežnim prometom

MPLS tehnike su iznimno bitne pri upravljanju mrežnim prometom. MPLS TE[37] (engl. *MPLS Traffic Engineering*) mehanizmi imaju važnu ulogu u implementaciji mrežnih usluga koje zahtijevaju određena jamstva na kvalitetu usluge (*QoS*). Mreže zasnovane na MPLS tehnologiji koriste TE mehanizme da bi minimizirali zagušenja u mreži i na taj način poboljšali izvedbu mreže. MPLS TE obično se koristi u mrežama pružatelja usluga, kada u takvoj mreži postoje različiti putevi kojima se mogu usmjeravati paketi od izvora ka odredištu.

Kod usmjeravanja temeljenog na IP protokolu, odabire se najkraći put kojim se promet isporučuje do odredišta, ne vodeći računa da se takvim načinom može uzrokovati zagušenje u mreži zbog preopterećenja pojedinih linkova i neiskorištenosti drugih linkova. [31]

[37] TE - Metoda optimizacije performansi telekomunikacijske mreže dinamičkom analizom, predviđanjem i regulacijom ponašanja podataka prenesenih preko te mreže.



Slika 4.1. MPLS TE [34]

Kao što je vidljivo na slici 4.1., između usmjerivača A i usmjerivača H dostupna su dva puta:

- PUT 1: Usmjerivač A -> Usmjerivač C -> Usmjerivač G -> Usmjerivač F -> Usmjerivač H
- PUT 2: Usmjerivač A -> Usmjerivač C -> Usmjerivač D -> Usmjerivač E -> Usmjerivač F -> Usmjerivač H

PUT 1 ima propusnost od 40 Mbps, a PUT 2 100 Mbps. Ako su usluga koja zahtijeva propusnost puta od 40 Mbps i usluga koja zahtijeva propusnost puta od 70 Mbps prisutne između usmjerivača A i usmjerivača H, prema odgovarajućem mehanizmu upravljanja mrežnim prometom moguće je dodijeliti uslugu čija je propusnost 40 Mbps PUTU 1 i uslugu čija je propusnost 70 Mbps PUTU 2. Na taj se način može izbjeći zagušenje linka [32]

TE može izmijeniti postojeće sheme usmjeravanja u svrhu što efikasnijeg raspoređivanja prometnih tokova prema raspoloživim mrežnim resursima. Kako bi se smanjilo zagušenje u mreži, kašnjenje pri dolasku paketa na odredište te broj pogrešno poslanih i izgubljenih bitova, potrebno je koristiti efikasnije sheme usmjeravanja. MPLS tehnologija za razliku od IP protokola koji koristi usmjeravanje na osnovu odredišne IP adrese, podržava istodobno usmjeravanje na temelju odredišne adrese i eksplicitno usmjeravanje koje se može koristiti zahvaljujući primjeni RVSP i LDP protokola.

4.2. MPLS profil mrežnog prometa

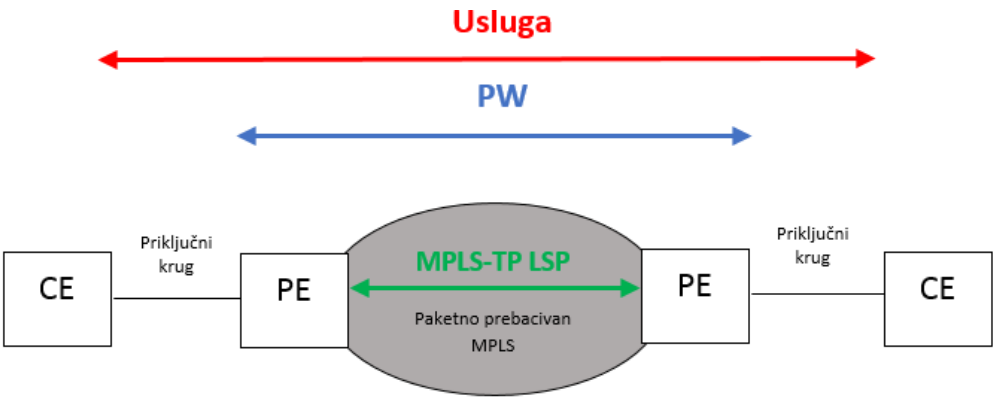
MPLS profil mrežnog prometa, tj. MPLS-TP (engl. MPLS Transport Profile) je proširenje osnovnog MPLS protokola koje omogućuje prosljeđivanje većine paketa na drugom, a ne na trećem sloju mrežnih modela. MPLS-TP predstavlja pojednostavljenu verziju MPLS-a, a

dizajniran je kako bi ubrzao i oblikovao mrežni promet u telekomunikacijskim transportnim mrežama. Transportna mreža sastoji se od opreme i vlakana koja fizički prenose signale. Prijenosne mreže obično su izgrađene pomoću SONET/SDH uređaja s višestrukim prijenosom s vremenskom podjelom (engl. *Time Division Multiplexed* - TDM), koji su vrlo skupi i nedjelotvorni. Iz tog razloga, pružatelji usluga implementiraju više opreme temeljene na paketima u svoje prometne mreže. MPLS TP morao je imati slične karakteristike kao SDH mreža - predvidljivost, upravljivost i redundantnost. Kako bi se to moglo realizirati, neke od mogućnosti MPLS mreže morale su se isključiti, kao npr. više puteva sa istom cijenom (engl. *Equal-cost multi-path* - ECMP[38]), povezivanje LSP puta te PHP[39] (engl. *Penultimate Hop Popping*) skok. Bilo je potrebno napraviti tehnologiju koja bi osigurala da se LSP-om informacije mogu prenijeti u oba smjera, pri čemu je jedan smjer za podatke, a drugi za signal o dojavi pogreške (engl. Fault Signal).

MPLS TP koristi *pseudowire*[40] tehniku (Slika 4.2.). Ona omogućuje prijenos okvira kroz MPLS mrežu, bez obzira koji protokol koristi CE usmjerivač. Tehnika je nazvana *pseudowire* jer kroz MPLS mrežu postoji virtualni put. Na takvom principu radi i MPLS VPN mreža, koja će biti opisana u sljedećim odlomcima rada.

Nadalje, MPLS-TP omogućuje dinamičko postavljanje MPLS-TP transportnih putova putem kontrolne ravnine. Kontrolna ravnina uglavnom se koristi za osiguravanje funkcija obnavljanja, radi poboljšanja izdržljivosti mreže u prisutnosti kvarova i olakšava pružanje end-to-end puteva preko mrežnih domena ili domena operatera. Operater može odabrati hoće li omogućiti upravljačku ravninu ili će upravljati mrežom na tradicionalan način bez upravljačke ravnine, pomoću sustava upravljanja mrežom (engl. *Network Management System* - NMS[41]). Valja napomenuti da kontrolna ravnina ne čini NMS zastarjelim - NMS mora konfigurirati kontrolnu ravninu, a također treba i komunicirati s kontrolnom ravninom u svrhu upravljanja vezama. [33]

[38] ECMP - Mehanizam prosljeđivanja za usmjeravanje paketa duž više putova jednakih troškova.
[39] PHP - Postupak kojim se vanjska oznaka MPLS označenog paketa uklanja pomoću LSR usmjerivača, prije nego što se paket prenese na susjedni LER usmjerivač.
[40] PSEUDOWIRE - Veza između dva rubna uređaja PE uređaja koja povezuje dvije krajnje usluge istog tipa.
[41] NMS – Sustav dizajniran za praćenje, održavanje i optimizaciju mreže.



Slika 4.2. MPLS TP *Pseudowire* [34]

4.3. MPLS virtualne privatne mreže

MPLS daje efikasno rješenje za VPN usluge koje uključuju privatnost podataka i podržavanje korištenja nejedinstvenih privatnih IP adresa. MPLS VPN predstavlja najprihvaćenije aplikacijsko proširenje u MPLS mrežama. Virtualna privatna mreža (*engl. Virtual Private Network* - VPN) je interkonekcija lokalne mreže koja koristi sigurne načine međusobne komunikacije, uglavnom putem Interneta. To znači da VPN produžava privatnu mrežu preko javne mreže, što omogućuje korisnicima slanje i primanje povjerljivih podataka, kao da su njihova računala izravno povezana na isti privatni LAN. [35]

Virtualna privatna mreža koristi sljedeće zaštitne mehanizme:

- Vatrozid[42] (engl. *Firewall*) – može ili ne mora biti prisutan, ali njegova prednost je osiguravanje sigurnog sučelja prema Internetu;
- Autentifikacija – mogućnost instaliranja određenog softvera koji će omogućiti kreiranje sigurne veze. Taj program će vršiti kriptiranje i dekriptiranje podataka, što zahtijeva korisničko ime i lozinku kako bi se potvrdio identitet korisnika;
- Enkripcija – zaštita podataka od neovlaštenog pregledavanja pri njihovom prosljeđivanju kroz javnu mrežu.
- Tuneliranje - VPN stvara privatni „tunel“, zatvorenu vezu koju ne može dekriptirati neka druga strana, kao npr. pružatelji usluga (ISP) ili neke web stranice. To znači da se podaci koje šalje korisnik ne mogu presresti i/ili ukrasti.

[42] Vatrozid - Mrežni uređaj čija je namjena filtriranje mrežnog prometa tako da se stvori sigurnosna zona.

4.4. Mehanizmi očuvanja kvalitete usluga u MPLS mreži

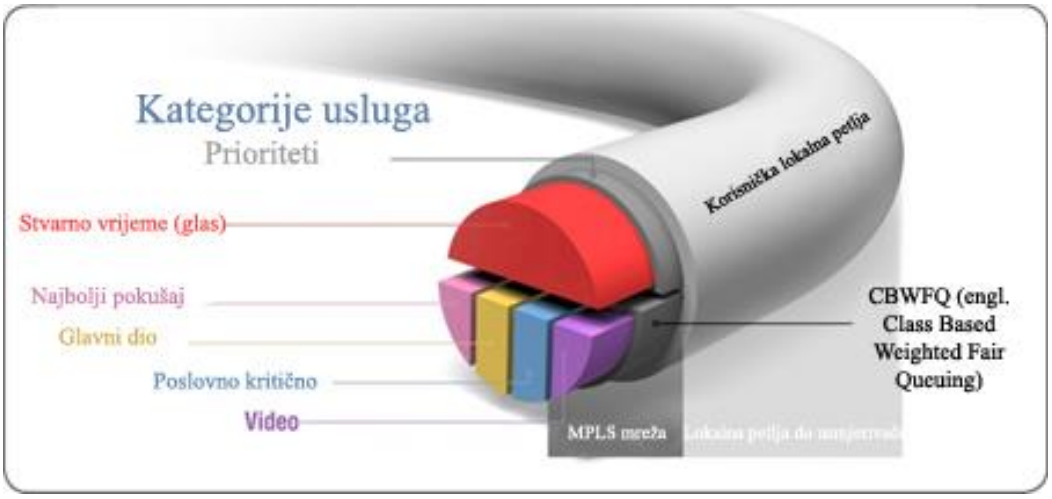
IETF je definirao dva načina pružanja kvalitete usluge (engl. *Quality of service* - QoS) u IP mreži; diferencirane usluge (engl. *Differentiated Service* - DiffServ[43]) i integrirane usluge (engl. *Integrated Service* - IntServ[44]). DiffServ je model unutar kojeg je promet grupiran u klase koje imaju svoj prioritet i način obrade u mreži. Kvaliteta usluge za multimedijski promet osigurana je kombinacijom MPLS-a i DiffServe-a. Proširenje DiffServe usluge moguće je putem tehnika upravljanja mrežnim prometom pri čemu se garantira bolje iskorištenje resursa i bolja kvaliteta usluge od strane operatora. [36]

Osnovne funkcije QoS-a opisane su u nastavku:

- Označavanje i klasifikacija prometa – obavlja se na temelju izvorišne i odredišne adrese, vrste aplikacije i vrste protokola koji se koriste, pri čemu se dobivena oznaka nalazi unutar polja koje definira vrstu usluge (engl. *Type of Service* - ToS[45]) ili polja diferencirane usluge (engl. *Differentiated Services* - DS[46]) IP zaglavlja;
- Nadgledanje – provjera da li su interval i brzina slanja podataka u skladu s predefiniranim pravilima upravljanja, a ukoliko nisu, paketi se odbacuju;
- Raspoređivanje – temelji se na rasporedu koji definira redoslijed posluživanja redova uz mogućnost dodavanja težinskog faktora koji stavlja veći prioritet na pojedini promet;
- Odašiljanje – veće pakete potrebno je podijeliti na više manjih paketa, npr., ne smije se dogoditi da paketi koji prenose glas zapnu iza većih paketa;
- Stavljanje u redove i nasumično odbacivanje – promet je potrebno složiti u redove kako ne bi došlo do odbacivanja paketa.

Unutar MPLS-a postoji klasa usluge (engl. *Class of Service* - CoS[47]) (Slika 4.3.). Klasa usluge je način upravljanja prometom u mreži grupiranjem sličnih vrsta prometa (npr. elektroničke pošte, toka podataka u obliku video ili audio zapisa, prijenosa velikih dokumenata) i obrađivanje svake vrste prometa kao klase s vlastitim razinama prioriteta usluge. [37]

[43] DiffServ - Arhitektura koja omogućava diferenciranje usluga u mreži tako da se različitim aplikacijama dodijeli odgovarajuća razina usluge uz zadržavanje visokog stupnja skalabilnosti.
[44] Intserv - arhitektura koja specificira elemente koji jamče kvalitetu usluge (QoS) na mrežama.
[45] ToS - Bajt u IPv4 zaglavlju koji se koristi za kategoriziranje prometnih klasa.
[46] DS - Zamjensko polje zaglavlja koje definira diferencirane usluge.
[47] CoS - Način upravljanja višestrukim profilima prometa preko mreže, dajući određenim vrstama prometa prioriteta nad ostalima.



4.3. MPLS klasa usluge [38]

4.5. Primjena GMPLS tehnologije

Generalizirani MPLS (engl. *Generalized Multi-Protocol Label Switching* - GMPLS) pruža rješenje za osiguravanje opće razine kontrole mrežnog prometa koja bi omogućila prijenos i komutaciju prometa preko različitih vrsta mreža: paketnih, mreža temeljenih na prijenosu informacija vremenskim kanalima – višestruki prijenos s vremenskom pojelom (engl. *Time Division Multiplexing* - TDM) i optičkih mreža.

GMPLS proširuje MPLS skup protokola kako bi omogućio signalizaciju i usmjeravanje uređaja koji komutiraju na bilo koju od gore navedenih domena prijenosa. To je omogućeno potpunim razdvajanjem kontrolne razine i razine podataka različitih mreža, na temelju načina IP usmjeravanja i adresiranja.

GMPLS koristi IPv4 i/ili IPv6 adrese za identifikaciju sučelja, ali koristi i tradicionalno IP usmjeravanje s proširenim protokolima usmjeravanja. Tehnologija koja se koristi za GMPLS kontrolnu ravninu ostaje zasnovana na IP-u, dok podatkovna matrica obuhvaća raznovrstan promet. Zbog te raznolikosti nužno je da GMPLS podržava više načina komutiranja. [39]

GMPLS proširuje funkcionalnost MPLS-a pružanjem i uspostavljanjem:

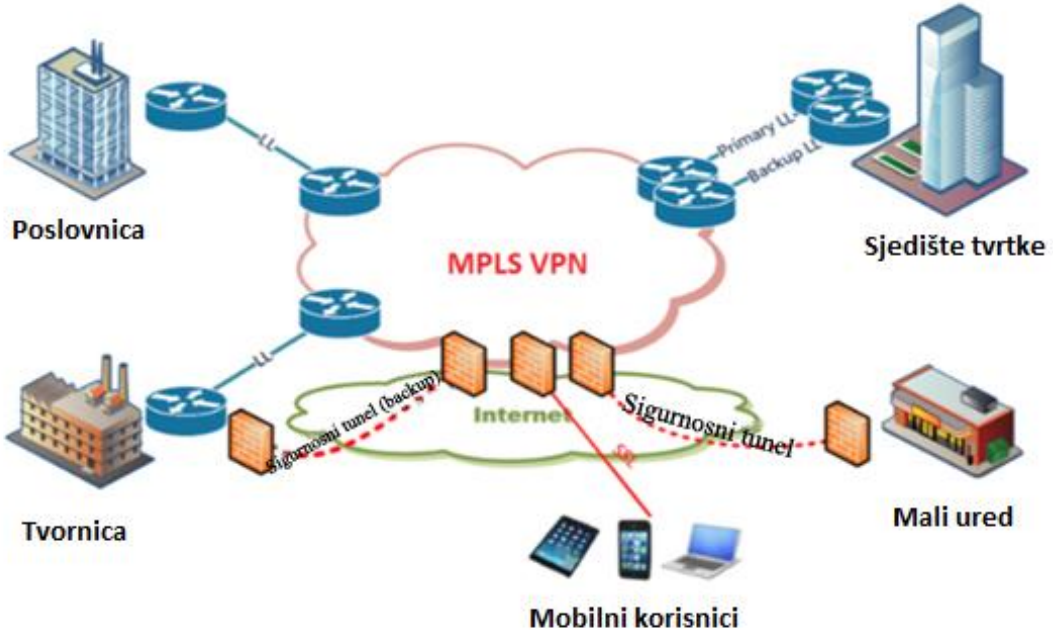
- puteva višestrukog prijenosa s vremenskom podjelom (engl. *Time Division Multiplexing* - TDM),

- puteva višestrukog prijenosa s frekvencijskom podjelom (engl. *Frequency Division Multiplexing* - FDM[48]),
- prostorno multipleksiranih puteva.

[48] FDM - Tehnika kojom je ukupna širina pojasa dostupna u komunikacijskom mediju podijeljena u niz neusklađenih frekvencijskih pojasa, od kojih se svaka koristi za nošenje zasebnog signala.

5. INAČICE MPLS VPN MREŽA

MPLS VPN možemo definirati kao najprihvaćenije aplikacijsko proširenje MPLS mreže (Slika 5.1.). Virtualna privatna mreža (engl. *Virtual Private Network* - VPN) naziva se virtualnom zato što svaki korisnik dijeli dio resursa sa drugim korisnikom, a privatne su zato što su međusobno logički odvojene - mrežni promet jednog korisnika razdvojen je od prometa drugog korisnika. VPN se primjenjuje za povezivanje udaljenih računala u jednu lokalnu mrežu, pomoću druge nesigurne mreže (najčešće Interneta). VPN radi na principu "tuneliranja" podataka putem Interneta; kriptira se promet između računala koja nisu fizički povezana u lokalnu mrežu te se kriptirani promet šalje putem Interneta do drugog računala u virtualnoj mreži koje zatim dekriptira primljeni promet.



Slika 5.1. MPLS VPN [40]

MPLS VPN grupa mreža dijeli se na podgrupe - VPN trećeg sloja (engl. *Layer 3* - L3) i drugog sloja (engl. *Layer 2* - L2), koji se dalje dijele na nekoliko podvrsta. Podvrste L3 VPN-ova su *MPLS L3VPN* i virtualni usmjerivač (engl. *Virtual Router*), dok su podvrste L2 VPN-ova: komunikacija od točke do točke (*Point to Point*[49]), *Ethernet*[50], virtualna privatna žična usluga (engl. *Virtual*

[49] Point to Point – protokol koji se koristi za izravno povezivanje dvaju čvorova računalne mreže.
[50] Ethernet - mrežna tehnologija za LAN mreže kod koje se podaci šalju u paketima koji su prilagođeni za slanje preko računalne mreže.

Private Wire Service - VPWS[51]) i virtualna privatna LAN usluga (engl. *Virtual Private LAN services* - VPLS[52]). [41]

MPLS VPN kombinira karakteristike MPLS-a i BGP (engl. *Border Gateway Protocol*) protokola. MPLS se koristi za prosljeđivanje paketa preko mreže pružatelja usluge, dok se BGP protokol koristi za distribuciju ruta preko jezgrene mreže.

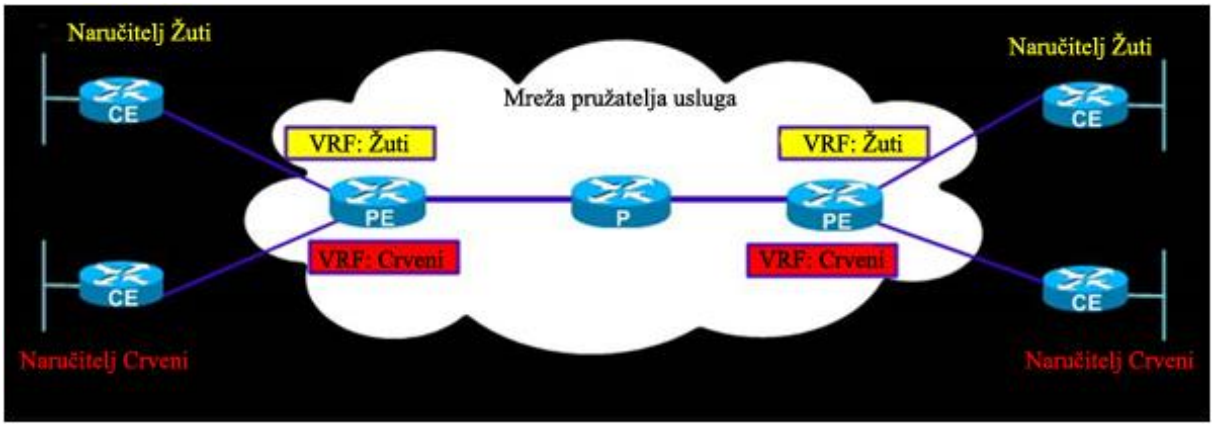
MPLS virtualna privatna mreža (VPN) sastoji se od sljedeće opreme:

- korisničkih (engl. *Customer Edge* - CE) usmjerivača – smješteni su u prostoru korisnika, pružaju Ethernet sučelje između LAN-a korisnika i jezgrene mreže pružatelja usluge;
- mrežnih (engl. *Provider Edge* - PE) usmjerivača – njima se povezuju CE usmjerivači, uvijek su u vlasništvu pružatelja usluga;
- usmjerivača pružatelja usluga (engl. *Providers* - P) - obično se nazivaju i "tranzitni usmjerivači", nalaze se u jezgrenoj mreži pružatelja usluga.

Informacije o usmjeravanju prosljeđuju se od CE usmjerivača do PE usmjerivača koristeći ili statičke rute ili protokol usmjeravanja kao što je BGP. PE usmjerivač sadrži tablicu usmjeravanja i prosljeđivanja (engl. *VPN routing and forwarding* - VRF[53]), za prosljeđivanje po mjestu, poznatu kao virtualnu tablicu usmjeravanja i prosljeđivanja. Na PE usmjerivaču, svaka VRF tablica služi određenom sučelju ili skupu sučelja koje pripada svakom pojedinom VPN-u. Svaki PE usmjerivač konfigurira pružatelja usluga uz primjenu vlastite VRF tablice koja je jedinstvena. Usmjerivači unutar MPLS VPN mreže ne dijele izravno VRF podatke. [42]

Slika 5.2. prikazuje tipičnu mrežu u kojoj su VRF tablice jedinstvene za svaki VPN povezan s određenim PE usmjerivačem.

[51] VPWS - Najjednostavniji oblik za omogućavanje Ethernet usluga preko MPLS-a.
[52] VPLS - Klasa VPN-a koja podržava povezivanje više mjesta u jednoj premoštenoj domeni preko upravljane IP/MPLS mreže.
[53] VRF – virtualna tablica prosljeđivanja i usmjeravanja koja se koristi za prosljeđivanje po mjestu.



Slika 5.2. MPLS VPN mrežni dijagram [42]

Razlika između MPLS i MPLS VPN-a zapravo je jednostavna. MPLS je tehnologija koja omogućuje pružateljima usluga da korisnicima nude velike brzine prijenosa podataka u privatnim mrežama. Pružatelj usluga pruža virtualne sklopove za svakog korisnika, izolirajući podatke jednog korisnika od drugog, iako su oba korisnika povezana uz primjenu iste fizičke telekomunikacijske opreme. Ovisno o zahtjevima korisnika, MPLS može isporučiti povezanost bilo na drugom sloju (Ethernet) ili na trećem sloju (internetski).

Većina VPN usluga stvara jedan-na-jedan vezu između dvije krajnje točke mreže (*point-to-point model*). U *point-to-point* modelu koristi se namjenski hardver ili softver za šifriranje prometa između dviju točaka. Za podatkovni promet koji putuje između dva udaljena čvora, ovaj model stvara dodatni skok. Kako bi se došlo do udaljenog odredišnog čvora, promet s izvorišnog čvora mora proći VPN tunel do sjedišta, a zatim mora proći drugi tunel do konačnog odredišta. Ovo dodatno zaustavljanje na čvorištu ne samo da povećava kašnjenje u usmjeravanju tih paketa nego i zahtijeva da koncentrator u ovoj konfiguraciji bude opremljen s dovoljnom širinom pojasa za obradu postojećih prometnih zahtjeva s više udaljenih lokacija. Ova vrsta VPN usluge osmišljena je za stvaranje sigurnih, šifriranih veza na javnim mrežama, uključujući internetske širokopojasne veze.

MPLS VPN usluge, s druge strane, dizajnirane su kao rješenje s više točaka, pri čemu je stvaranje specifičnog VPN tunela nepotrebno. Kada se podaci premjeste s jednog čvora na drugi, pregledava se zapis u tablici usmjeravanja, dodaje se oznaka za tu lokaciju i šalje se paket na sljedeći usmjerivač. Ovaj pristup smanjuje kašnjenje paketa pri prijenosu podataka između lokacija, ali i zahtjeva da sve udaljene lokacije budu povezane s MPLS mrežom.

Visoke performanse i jednostavnost implementacije često se navode kao prednosti MPLS VPN-a pred drugim rješenjima. Za razliku od tradicionalnih VPN-ova, koji pretpostavljaju da se poslovni podaci prenose putem javnih mreža, MPLS VPN-ovi koriste izoliranu privatnu mrežu, zbog čega je potrebno šifrirati podatke koji se prosljeđuju između čvorova. [43]

5.1. Funkcionalnost MPLS VPN mreža na trećem sloju mrežnih modela

MPLS VPN trećeg sloja (L3) karakterizira nešto složenija konfiguracija i primjena složenijih mrežnih tehnologija i protokola, u odnosu na druge dvije vrste MPLS VPN-ova. Kod ovog VPN-a ISP preuzima potpuni nadzor i upravljanje nad adresiranjem i logičkim procesima na mrežnom sloju. MPLS L3 VPN realiziran je pomoću proširenja BGP protokola, višeprotokolnog BGP protokola (engl. *Multiprotocol BGP* - MP-BGP[54]). U jezgrenoj mreži glavnu ulogu imaju LDP ili RSVP-TE protokol, dok MP-BGP protokol ostvaruje vezu između krajnjih PE usmjerivača. [44]

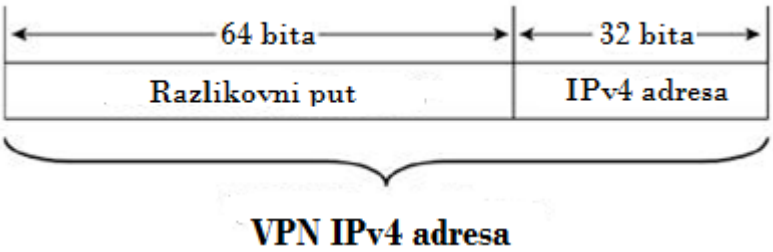
Neki pojmovi koji se koriste u MPLS L3 VPN-u navedeni su u nastavku:

- Oznaka (engl. *Label*) – 32-bitni identifikator koji je dodan svakom paketu koji ulazi u MPLS mrežu. Koriste ga MPLS mreže za potrebe promjena oznaka;
- LSR usmjerivač (engl. *Label Switch Router*) – bilo koji usmjerivač na kojem MPLS radi i koji se koristi za prebacivanje oznaka;
- MP-BGP – protokol kojeg koriste PE uređaji za distribuciju rute korisnika na odgovarajuće PE uređaje preko MPLS jezgrene mreže;
- PE (engl. *Provider Edge*) usmjerivač – rubni usmjerivač u mreži pružatelja usluge, uređaj na kojem se postavlja i uklanja oznaka;
- P (engl. *Provider*) usmjerivač – naziva se i glavni ili jezgreni usmjerivač, a nalazi se u mreži pružatelja usluge, nije rubni uređaj i u njemu ne radi BGP protokol;
- CE (engl. *Customer Edge*) usmjerivač – rubni usmjerivač smješten u prostoru korisnika, koji je povezan s PE usmjerivačem;
- IPE (engl. *Ingress Provider Edge*) usmjerivač – rubni LSR usmjerivač kojem je oznaka umetnuta paketu koji dolazi od CE usmjerivača prema PE usmjerivaču;
- EPE (engl. *Egress Provider Edge*) usmjerivač – prima označene pakete, raspoređuje oznake koje su priključene na pakete i prosljeđuje jednostavne IP pakete korisnicima;
- IP tablica usmjeravanja - naziva se i globalna tablica usmjeravanja, ona sadrži putove pružatelja usluga koji nisu uključeni u VRF tablicu. Uređaji pružatelja usluga trebaju ovu

[54] MP-BGP – Proširenje BGP protokola koje omogućuje paralelnu distribuciju različitih vrsta adresa.

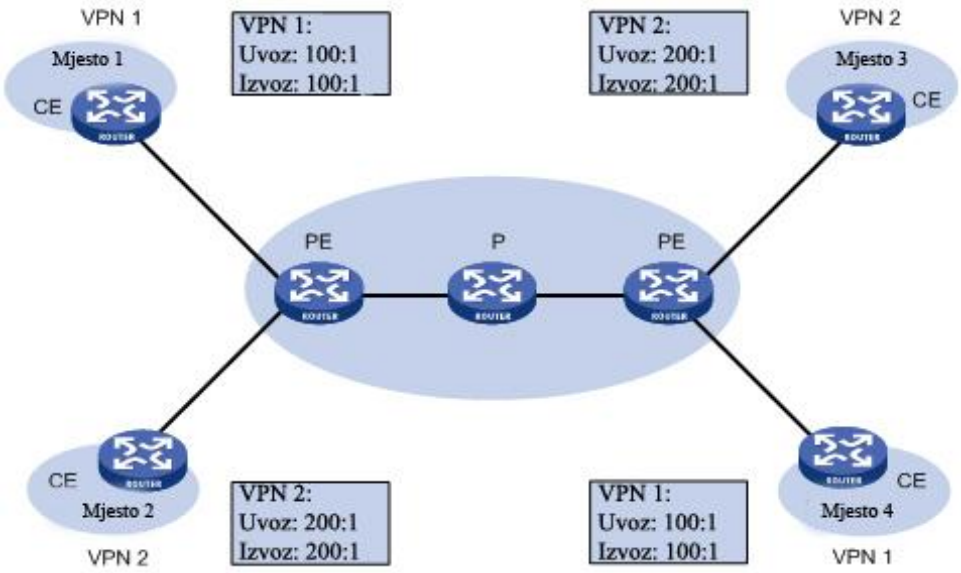
tablicu da bi se mogli međusobno povezati, dok je VRF tablica potrebna za pristup svim korisničkim uređajima u određenoj virtualnoj privatnoj mreži;

- Oznaka rute (engl. *Route Distinguisher* - RD) – ova veličina služi za jednoznačno određivanje korisnika, koristi se za kreiranje VPNv4 adrese veličine 96 bita (Slika 5.3.). Ona omogućuje korisnicima da imaju iste adrese na svojim CE usmjerivačima, budući da je RD broj jedinstven bez obzira na IP adresu koju koristi korisnik;



Slika 5.3. VPNv4 adresa [45]

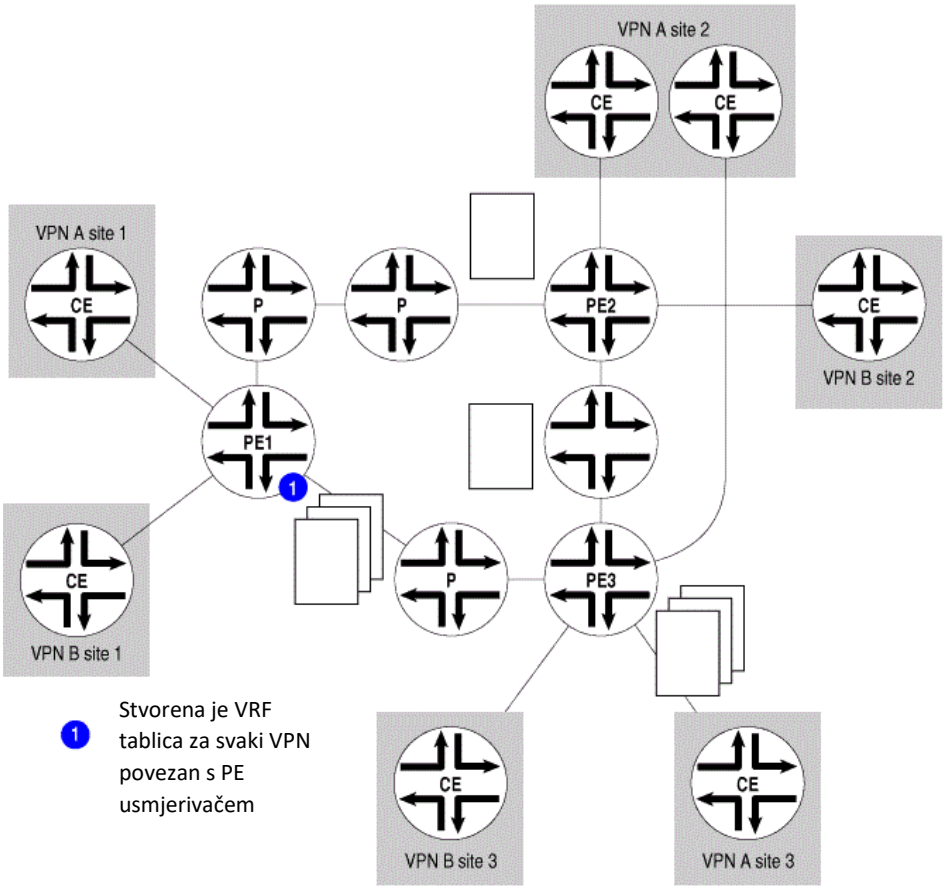
- Ciljane rute (engl. *Route Target* - RT) – 64-bitna vrijednost koja se koristi za označavanje puteva u mreži, odnosno govori PE usmjerivaču koje mrežne adrese može oglasiti (Slika 5.4.);



Slika 5.4. Route target [46]

Na slici 5.4. RT za VPN 1 je 100:1, dok je za VPN 2 200:1. Dvije VPN 1 stranice mogu međusobno komunicirati, kao i dvije VPN 2 stranice. Međutim, VPN 1 stranica ne može komunicirati s VPN 2 stranicom.

- VPN-IPv4 ruta – ruta koja se sastoji od 96-bitne sekvence sastavljene od 64-bitne RD oznake predane 32-bitnoj IPv4 adresi;
- Virtualna tablica za usmjeravanje i prosljeđivanje (engl. *Virtual Routing and Forwarding* - VRF) – razlikuje rute za različite korisnike, kao i rute korisnika od ruta pružatelja usluga na PE uređaju. VRF primjerak sastoji se od jedne ili više tablica usmjeravanja, izvedene tablice prosljeđivanja, sučelja koja koriste tablicu prosljeđivanja te pravila i protokola usmjeravanja koji određuju što se događa u tablici za prosljeđivanje. Budući da je svaki primjerak konfiguriran za određenu virtualnu privatnu mrežu, svaka virtualna privatna mreža ima zasebne tablice - i pravila koja upravljaju njezinim radom.



Slika 5.5 VRF tablice [47]

Slika 5.5. prikazuje VRF tablice koje su stvorene na PE usmjerivačima. Tri PE usmjerivača imaju vezu s CE usmjerivačima koji se nalaze u dvije različite virtualne privatne mreže, pa svaki PE usmjerivač stvara dvije VRF tablice, po jednu za svaku virtualnu privatnu mrežu.

Treći sloj virtualnih privatnih mreža povezuje korisničke CE usmjerivače s mrežnim PE usmjerivačima. On koristi istorazinski (engl. *peer*) model usmjeravanja između lokalnih PE i CE

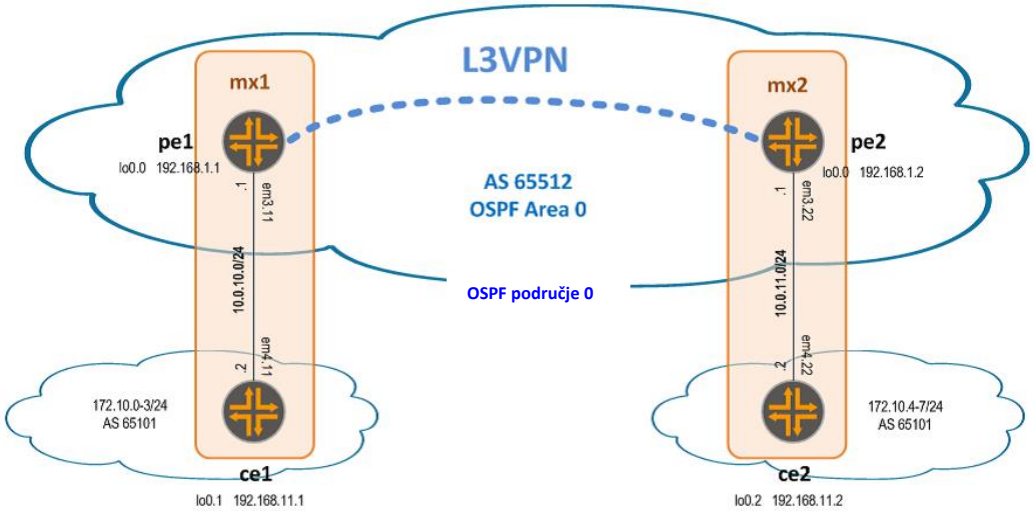
usmjerivača koji se izravno povezuju. PE usmjerivači distribuiraju informacije o usmjeravanju svim CE usmjerivačima koji pripadaju istoj virtualnoj privatnoj mreži. Svaka virtualna privatna mreža ima vlastitu tablicu usmjeravanja koja je koordinirana s tablicama usmjeravanja CE i PE istorazinskih usmjerivača. CE i PE usmjerivači imaju različite VRF tablice. Svaki CE usmjerivač ima samo jednu VRF tablicu zato što su druge virtualne privatne mreže nevidljive za CE usmjerivač. PE usmjerivač može se povezati s više CE usmjerivača, tako da PE usmjerivač ima opću IP usmjerivačku tablicu i VRF tablicu za svaki priključeni CE usmjerivač s virtualnom privatnom mrežom.

PE usmjerivač zna koja se VRF tablica treba koristiti za pakete koji dolaze s udaljenih virtualnih privatnih mrežnih stranica, jer svaka VRF tablica ima jedan ili više proširenih zajedničkih atributa. Zajednički atributi prepoznaju put kao pripadnost određenoj zbirci usmjerivača. Zajednički RT atribut identificira zbirku stranica (točnije, zbirku njihovih VRF tablica) na koje PE usmjerivač distribuira rute. PE usmjerivač koristi RT za uvoz ispravnih udaljenih puteva u svoje VRF tablice.

Uvoz i izvoz VPN ruta između VPN stranica nije automatski. Taj proces kontroliraju pravila usmjeravanja definirana BGP protokolom. Ona definiraju način razmjene informacija o usmjeravanju podataka preko MPLS mreže pružatelja usluga. Ta pravila moraju biti ispravno konfigurirana i osvježavana pri promjeni topologije mreže.

PE usmjerivač klasificira IPv4 rute proslijeđene od CE usmjerivača i primljene od PE usmjerivača kao VPN-IPv4 rute. Kada ulazni PE usmjerivač prima rute oglašene od strane izravno povezanog CE usmjerivača, ulazni PE usmjerivač provjerava primljenu rutu prema VRF pravilima za taj VPN. To jest, ulazni PE usmjerivač odlučuje koji udaljeni PE usmjerivači trebaju znati o oglašenim rutama. Ovaj postupak provodi se u dva koraka:

- Ako pravila definiraju prihvaćanje rute, PE usmjerivač pretvara podatke u VPN-IPv4 format, dodavanjem RD veličine na IPv4 adresu. PE usmjerivač tada oglašava VPN-IPv4 rutu do udaljenih PE usmjerivača.
- Ako pravila definiraju odbacivanje rute, PE usmjerivač ne prosljeđuje rutu na druge PE usmjerivače, već ju koristi lokalno. [44]



Slika 5.6. L3VPN [48]

Iz slike 5.6. je vidljivo kako je u L3VPN-u mreža pružatelja internetskih usluga jedan veliki usmjerivač. Korisnički (CE) usmjerivači konfigurirani su s drugačijim mrežnim adresama od mrežnih (PE) usmjerivača. Dva udaljena CE usmjerivača imaju iste mrežne adrese. Takvu mrežu u takvom okruženju nazivamo virtualnom privatnom usmjerivačkom mrežom (engl. *Virtual Private Routed Network* - VPRN[55]). Svaka VPRN mreža sastoji se od skupa korisničkih stranica povezanih s jednim ili više PE usmjerivača. Svaki povezani PE usmjerivač čuva zasebnu tablicu za prosljeđivanje IP adresa za svaki VPRN.

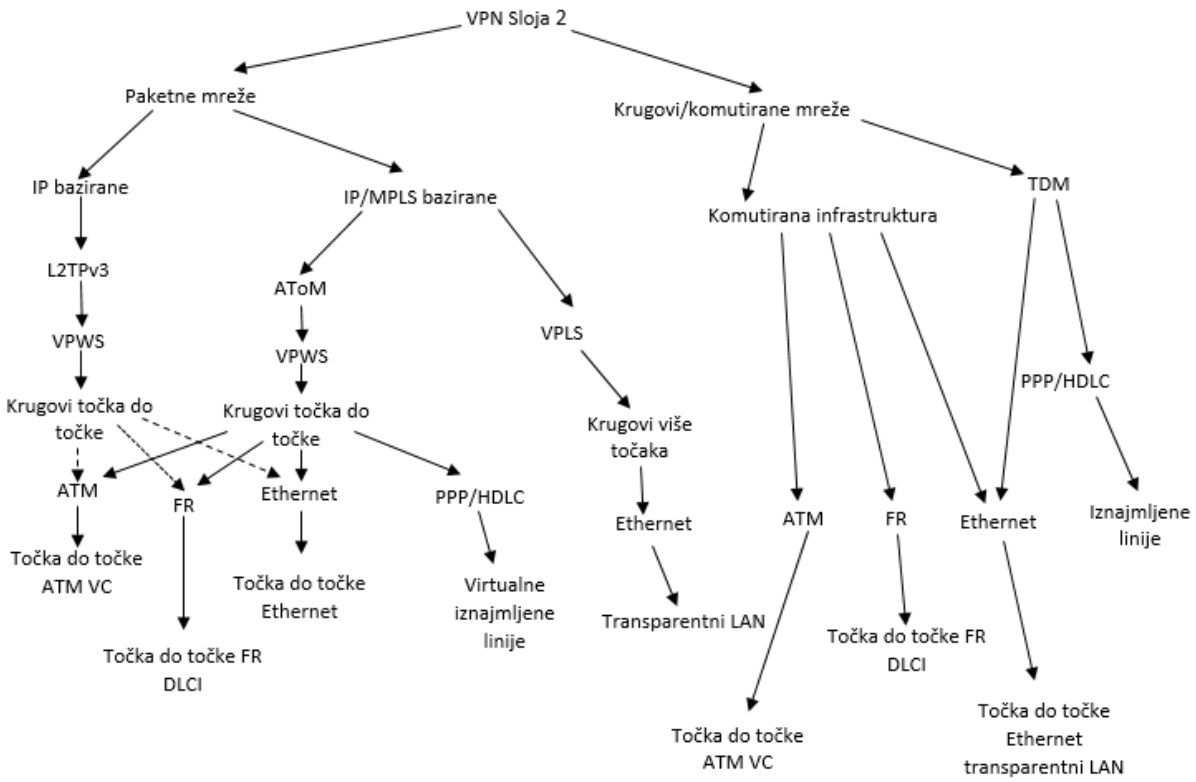
5.2. Funkcionalnost MPLS VPN mreža na drugom sloju mrežnih modela

VPN drugog sloja (L2) može se definirati kao grupa mrežnih mjesta povezanih preko drugog sloja ATM vezama od točke do točke, FR DLCI[56] (engl. *Frame Relay Data Link Connection Identifiers*) konekcijama ili sesijama PPP protokola (engl. *Point-to-Point Protocol*). Svaka uspostavljena veza na drugom sloju čini posebnu spregu za usmjeravanje podataka koje se provodi na rubovima mreže drugog sloja, bez sudjelovanja pružatelja usluge. Pružatelj usluga omogućuje korisnicima organiziranje IP WAN[57] mreže ili povezivanje putem Ethernet mostova.

[55] VPRN - Usluga koja povezuje više grana u jednoj logičkoj usmjerenoj arhitekturi preko IP/MPLS mreže pružatelja usluga.
[56] FR DLCI - Broj pohranjen u zaglavlju okvira koji prolazi kroz Frame Relay mrežu.
[57] WAN - podatkovna mreža koja pokriva veće zemljopisno područje: gradove, države ili kontinente.

Virtualne privatne mreže drugog sloja mogu se temeljiti na paketskoj ili komutiranoj strukturi (FR, ATM i Ethernet). Najviše mrežnih operatera koristi ATM i FR komutirane strukture, pri čemu je iskorištavanje naslijeđenih mrežnih struktura važan razlog za razvoj VPN mreža drugog sloja. VPN mreže drugog sloja imaju prednost nad VPN mrežama trećeg sloja, jer mogu prenositi ne samo okvire drugog sloja, nego i pakete razmijenjene putem IPX[58] (engl. *Internetwork Packet Exchange*) sustava, SNA[59] (engl. *Systems Network Architecture*) sustava i tradicionalnih TDM privatnih linija. [36]

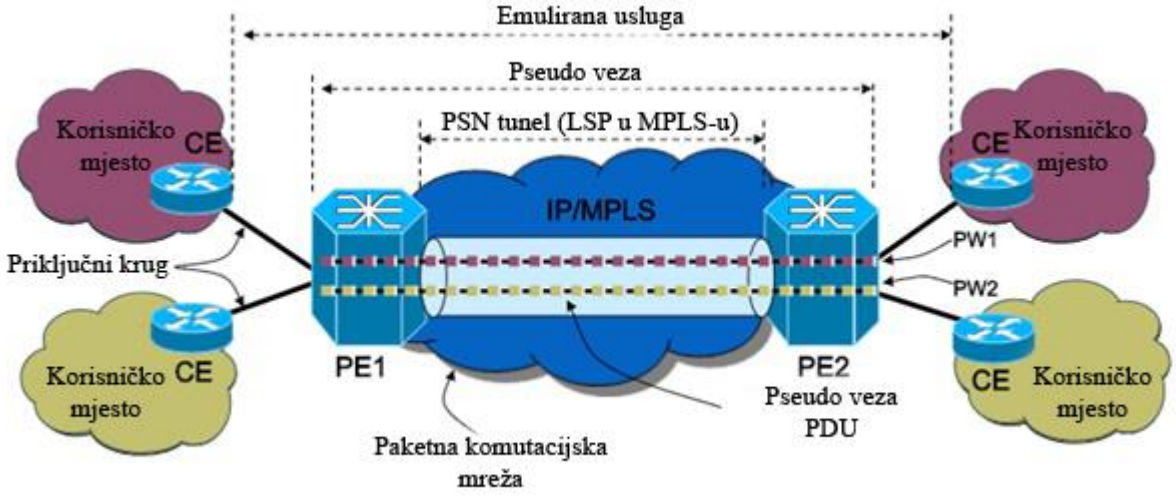
Dijagram VPN mreža drugog sloja prikazan je na slici 5.7. Na dijagramu možemo uočiti podtipove VPN mreža drugog sloja: virtualnu privatnu žičnu uslugu (engl. *Virtual Private Wire Service* - VPWS) i virtualnu privatnu LAN uslugu (engl. *Virtual Private LAN Services* - VPLS). Oba podtipa mreža grade se koristeći virtualno ožičavanje (engl. *pseudowire*).



Slika 5.7. Podjela VPN mreža drugog sloja [49]

[58] IPX - Skup paketnih komutacijskih i paketnih sekvencijalnih protokola koji su dizajnirani za funkcioniranje u malim i velikim mrežama.
[59] SNA - Arhitektura podatkovne komunikacije koju je utemeljio IBM kako bi odredio uobičajene konvencije za komunikaciju između širokog raspona IBM hardverskih i softverskih komunikacijskih proizvoda i drugih platformi.

Okviri drugog sloja oblikuju se u IP/MPLS pakete i šalju se preko paketne mreže, pri čemu se na udaljenom kraju paketi raspakiravaju u originalni format i prenose se na lokaciju korisnika. IETF je definirao referentni model PWE3[60] (engl. *Pseudowire Emulation Edge-to-Edge*) koji je primjenjiv za IP i MPLS mreže (Slika 5.8.).



Slika 5.8. PWE3 model [50]

Veza između CE i PE usmjerivača se naziva priključni krug (engl. *Attachment Circuit*). Veza između dva PE uređaja naziva se *pseudowire*; a PWES je veza koja povezuje dvije *pseudowire* krajnje usluge (engl. *Pseudo-Wire End-Services*) istog tipa. *Pseudowire* se uspostavlja pomoću usmjerenog LDP protokola u slučaju IP/MPLS mreže ili L2TPv3[61] protokola u slučaju klasičnih IP mreža. Nakon što okviri drugog sloja stignu sa CE usmjerivača na PE usmjerivač, pakiraju se na odgovarajući način i zatim se šalju na *pseudowire*. *Pseudowire* se preslikava na tunel paketne komutirane mreže (engl. *Packet Switched Network* - PSN[62]) nekim od mehanizama preslikavanja. PSN tunel predstavlja način prosljeđivanja okvira od PE1 usmjerivača do PE2 usmjerivača.

5.2.1. VPWS usluge

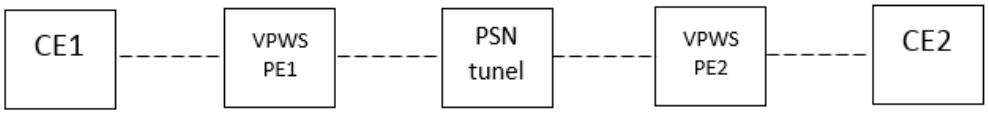
VPWS (engl. *Virtual Private Wire Service*) je najjednostavniji oblik Ethernet usluga putem MPLS mreže. Također je poznat kao Ethernet preko MPLS-a (engl. *Ethernet over MPLS* - ETHoMPLS) ili virtualna iznajmljena linija (engl. *Virtual Leased Line* - VLL). VPWS upotrebljava usluge

[60] PWE3 – Arhitektura koja određuje enkapsulaciju, transport, kontrolu, upravljanje, međusobnu suradnju i sigurnost usluga emuliranih preko IETF-ovih specificiranih PSN-ova.
[61] L2TPv3 - Protokol za kontrolu baze i enkapsulaciju za tuneliranje višestrukih veza drugog sloja između dva IP čvora.
[62] PSN - Vrsta računalne komunikacijske mreže koja grupira i šalje podatke u obliku malih paketa.

drugog sloja preko MPLS-a za izgradnju topologije *point-to-point* veze koja povezuje stranice krajnjih korisnika u VPN mreži. Ovi VPN-ovi drugog sloja pružaju alternativu privatnim mrežama koje su osigurane putem namjenskih zakupljenih vodova ili pomoću virtualnih sklopova drugog sloja koji koriste ATM ili Frame Relay. Tradicionalni VPN-ovi preko sklopova drugog sloja zahtijevaju opremanje i održavanje zasebnih mreža za IP i VPN usluge. Nasuprot tomu, VPWS omogućuje razmjenu osnovne mrežne infrastrukture pružatelja usluge između IP i VPN usluga drugog sloja, smanjujući troškove pružanja tih usluga.

VPWS može imati dvije vrste topologija: potpunu povezanost (engl. *full-mesh*[63]) ili topologiju zvijezde (engl. *hub-and-spoke*[64]). Mehanizam tuneliranja u osnovnoj mreži obično je MPLS, no VPWS može koristiti i druge protokole tuneliranja, kao što je protokol inkapsulacije generičnog usmjeravanja (engl. *Generic Routing Encapsulation* - GRE[65]). Kao što je prethodno navedeno, VPWS je VPN usluga drugog sloja. Ponekad VPWS može biti definiran i kao VPN usluga na prvom sloju, jer se u toj usluzi ne određuje MAC[66] (engl. *Media Acces Control*) adresa svakog čvora u mreži. [51]

VPWS je ponuđen potrošaču preko PE usmjerivača i PSN mreže (Slika 5.9.).



Slika 5.9. VPWS referentni model [52]

VPWS omogućuje međusobnu komunikaciju putem Ethernet, ATM, Frame-Relay i TDM standarda putem zajedničke IP/MPLS mreže. Postoji pet vrsta VPWS usluga [53]:

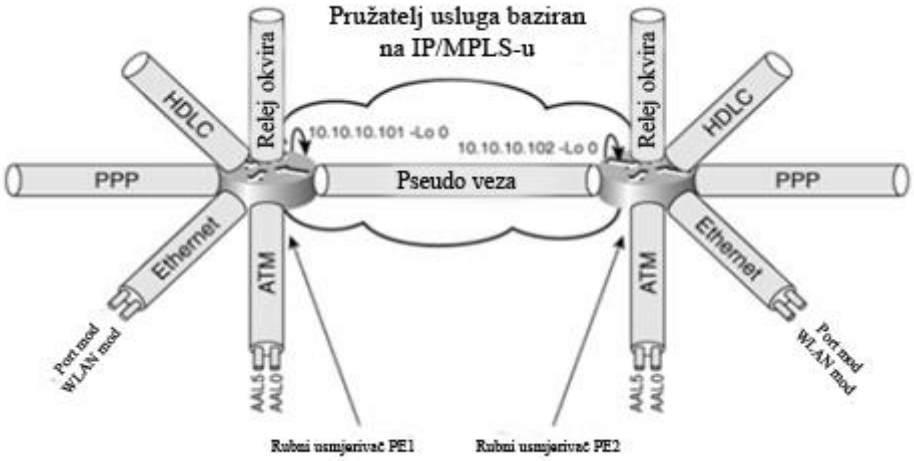
- Epipe – simulira point-to-point Ethernet uslugu (engl. *point-to-point*);
- Fpipe – simulira FR (engl. *Frame Relay*) uslugu od točke do točke;
- Apipe – simulira ATM uslugu od točke do točke;
- Cpipe – simulira TDM uslugu od točke do točke;

[63] full-mesh – Topologija u kojoj je svaki mrežni čvor povezan je izravno sa svakim od ostalih.
[64] hub-and-spoke - Arhitektura u kojoj jedan čvor (*HUB*) upravlja drugim čvorovima (*SPOKE*).
[65] GRE - Protokol za tuneliranje koji je razvio Cisco Systems, koji može obuhvatiti širok raspon protokola mrežnog sloja unutar virtualnih point-to-point veza preko IP mreže.
[66] MAC - adresa kodirana u ROM memoriji svakog mrežnog uređaja. Sastoji se od 48 bita i jedinstvena je za svaki uređaj.

- Ipipe – simulira IP uslugu između različitih tehnologija drugog sloja.

U VPWS-u se koriste dvije vrste *pseudowire* tehnologija, jedna je tehnologija bilo kojeg transporta preko MPLS-a (engl. *Any transport over MPLS* - AToM[67]), koja pruža point-to-point usluge od PE do PE usmjerivača, a druga je L2TPv3, *pseudowire* tehnologija za izvorne IP mreže.

AToM je naziv za transportnu uslugu drugog sloja preko MPLS jezgrene mreže. CE usmjerivači međusobno se povezuju s PE usmjerivačima na drugom sloju uz primjenu Ethernet, HDLC[68] (engl. *High-Level Data Link Protocol*), PPP (engl. *Point-to-Point Protocol*), ATM ili Frame Relay) protokola (Slika 5.10.). Time se eliminira potreba za naslijeđenom mrežom od pružatelja usluga koja nosi takav promet i integrira tu uslugu u MPLS mrežu koja već prevozi MPLS VPN promet. Naziv AToM vezan je uz sposobnost prijenosa bilo kojeg okvira preko MPLS mreže, koristeći MPLS kao mehanizam za enkapsulaciju i LDP kao signalni mehanizam. AToM omogućuje pružateljima usluga povezivanje korisničkih stranica s postojećim mrežama drugog sloja pomoću integrirane, mrežne infrastrukture temeljene na paketima; MPLS mreže.



Slika 5.10. Osnovni AToM model [54]

AToM koristi usmjerenu LDP sesiju između rubnih usmjerivača za postavljanje i održavanje veza. Prosljeđivanje se odvija uz primjenu dviju oznaka:

- vanjske oznake (oznake tunela) – za prebacivanje između rubnih usmjerivača; usmjerava paket preko MPLS jezgrene mreže od izlaznog PE usmjerivača do ulaznog PE usmjerivača;

[67] AToM - Rješenje koje rješava potrebe pružatelja usluga koji bi željeli implementirati MPLS i ponuditi usluge kao što su agregacija drugog sloja i virtualne zakupljene linije.
[68] HDLC - Skup protokola ili pravila za prijenos podataka između mrežnih mjesta. Podaci se organiziraju u jedinicu (okvire) i šalju se preko mreže na odredište koje potvrđuje uspješan dolazak.

- oznake virtualnog kruga (engl. *Virtual Circuit* - VC[69]) – za određivanje izlaznog sučelja i povezivanje izlaznog sučelja drugog sloja na oznaku tunela.

Razmjena VC oznaka između završnih točaka *pseudowire-a* odvija se putem LDP protokola. VC oznake identificiraju *pseudowire* i omogućuju multipleksiranje više *pseudowire-a* preko jednog PSN tunela. Sam tunel je signaliziran LDP ili RSVP-TE protokolom i ima svoje oznake koje se nalaze na vrhu stoga oznaka. P usmjerivači unutar mreže pružatelja usluga ne razmatraju VC oznake i nisu svjesni AToM rješenja.

AToM ima mogućnost korištenja kontrolnih riječi, kako bi sačuvao bitne informacije u prenesenim jedinicama protokola podatkovnih jedinica (engl. *Protocol Data Unit* - PDU[70]); npr. bit povratne eksplicitne dojave zagušenja (engl. *Backward Explicit Congestion Notification* - BECN[71]), bit unaprijednog izravnog obavješćivanja o zagušenju (engl. *Forward Explicit Congestion Notification* - FECN[72]) te bit oznake prioriteta odbacivanja (engl. *Discard Eligibility* - DE[73]). Osim toga, AToM može surađivati s protokolima kontrole usluga, kao što su integrirano lokalno nadzorno sučelje/lokalno upravljačko sučelje (engl. *Integrated Local Management Interface/Local Management Interface* - ILMI[74]/LMI[75]) kako bi se prikazao status lokalnih sklopova na udaljenim čvorovima. [55]

L2TPv3 (engl. *Layer 2 Tunnel Protocol Version 3*) je IETF standard koji je povezan sa L2TP[76] (engl. *Layer 2 Tunnel Protocol*) protokolom. Budući da je L2TPv2 protokol bio osmišljen samo za prijenos PPP prometa, L2TPv3 mijenja L2TP protokol tako da osim PPP prometa može nositi i formate podatkovnih okvira. L2TPv3 se može koristiti kao alternativni protokol MPLS-a za enkapsulaciju višeprotokolnog komunikacijskog prometa drugog sloja putem IP mreža. Poput L2TP protokola, L2TPv3 pruža *pseudowire* uslugu. Može se smatrati da je L2TPv3 standard MPLS-u, što i IP ATM-u: pojednostavljena verzija istog koncepta, s mnogo istih prednosti

[69] VC - sredstvo prijenosa podataka preko paketne komutirane računalne mreže na takav način da se čini kako postoji odvojena fizička slojna veza između izvora i odredišnih krajnjih sustava tih podataka.
[70] PDU - jedinica podataka koja je specificirana u protokolu određenog sloja i koja se sastoji od informacija o kontroli protokola i mogućih korisničkih podataka tog sloja.
[71] BECN - Bit zaglavlja koji odašilje odredišni terminal koji traži da izvorni terminal sporije šalje podatke.
[72] FECN - Bit zaglavlja kojeg odašilje izvor (slanje) terminala koji traži da terminal (primanje) usporava svoje zahtjeve za podacima.
[73] DE - bit koji se koristi za označavanje da okvir ima manju važnost od ostalih okvira i trebao bi se najprije ispustiti ako mreža doživljava zagušenje.
[74] ILMI –Protokol koji se koristi za razmjenu informacija o statusu i konfiguraciji, kao što su prefiks registriranih ATM mreža, registrirane ATM adrese i dr.
[75] LMI - Skup proširenja Frame Relay protokola koji su dizajnirani za pružanje informacija o statusu Frame Relay mreža i proširenje mogućnosti tehnologije.
[76] L2TP - Protokol za tuneliranje koji se koristi za podršku virtualnim privatnim mrežama (VPN) ili kao dio isporuke usluga ISP-ova.

ostvarenih uz jednostavniji postupak, ali na uštrb gubitka nekih tehničkih značajki koje se smatraju manje važnima na tržištu. U slučaju L2TPv3 protokola, izgubljene značajke su značajke telekomunikacijskog prometa koje se smatraju važnima u MPLS-u.

L2TPv3 koristi usmjerenu sjednicu kontrolnog kanala između rubnih usmjerivača za stvaranje i održavanje veza. Postupak prosljeđivanja se odvija prosljeđivanjem IP paketa između dva rubna uređaja. IP zaglavlje i L2TPv3 zaglavlje koriste se za slanje paketa između usmjerivača. Vanjsko zaglavlje je IP zaglavlje koje usmjerava tunelirane pakete preko IP jezgrene mreže na PE usmjerivač. L2TPv3 zaglavlje određuje izlazno sučelje i veže izlazno sučelje drugog sloja za tunel.

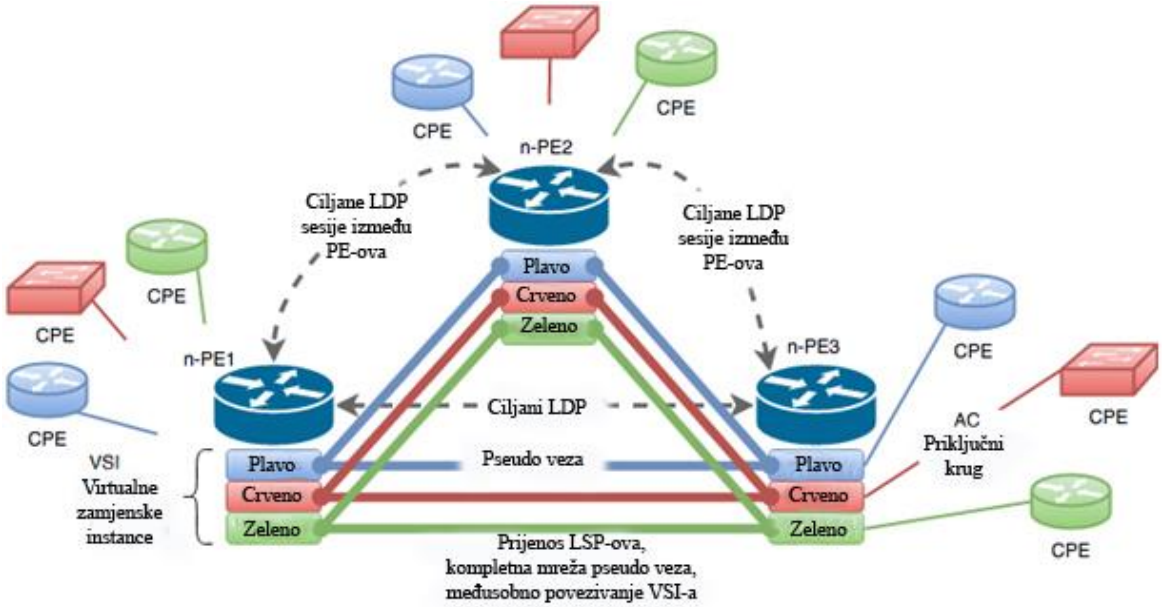
L2TPv3 donosi sljedeća poboljšanja L2TP protokola:

- L2TPv3 se može prenijeti izravno preko IP-a, bez UDP[77] protokola, dok se L2TPv2 može prenositi samo preko UDP protokola;
- L2TPv3 paketi imaju opcionalnu oznaku, što može biti korisno za otkrivanje i odbacivanje pogrešno usmjerenih paketa podataka koji imaju pogrešan ID sesije. To omogučuje zaštitu od nekih napada umetanjem paketa;
- Autentifikacija L2TPv3 kontrolne poruke provodi se preko cijele poruke, dok L2TPv2 pokriva samo pojedinačne atribute specifičnih poruka. Zbog toga je L2TPv3 manje osjetljiv na napade s posrednikom - napad na čovjeka u sredini (engl. *Man-in-the-middle attack* - MITM[78]) kada tunel nije zaštićen uz primjenu IPSec[79] protokola (engl. *Internet Protocol Security*);
- L2TPv3 tunel i ID-ovi sesija su 32-bitne vrijednosti; L2TPv2 koristi 16-bitne vrijednosti. Stoga L2TPv3 može podržati više od 65535 tunela ili više od 65535 sjednica u jednom tunelu;
- L2TPv3 omogućava konfiguriranje sesija bez kontrolnog kanala; svaka L2TP krajnja točka se ručno konfigurira sa statičkim parametrima. To omogućuje postavljanje L2TPv3 *pseudowire-a* bez posebne L2TP kontrole usluge. [56]

[77] UDP – Protokol koji omogućuje slanje kratkih poruka (datagrama) između aplikacija na umreženim računalima.
[78] MITM - Napad u kojem napadač potajno odašilje i eventualno mijenja komunikaciju između dviju stranaka koji vjeruju da izravno komuniciraju jedni s drugima.
[79] IPSec - Skup protokola koji pružaju sigurnost za IP protokol.

5.2.2. VPLS usluge

VPLS (engl. *Virtual private LAN service*) su telekomunikacijske usluge koja klijentima omogućuju stvaranje logičke strukture lokalne mreže (LAN) između geografski odvojenih mjesta. Razlog primjene ovih usluga zasniva se na činjenici da u usporedbi s BGP/MPLS mehanizmom klijent ne mora konfigurirati svaki protokol usmjeravanja ili statičke rute između CE i PE usmjerivača. Sve usluge u VPLS-u pojavljuju se na istom LAN-u, bez obzira na lokaciju. Za razliku od tradicionalne WAN (engl. *Wide-Area Network*) povezanosti ili virtualnih privatnih mreža temeljenih na IP-u, VPLS se može koristiti za prijenos prometa koji nije IP promet bez potrebe za konverzijom ili enkapsulacijom. VPLS koristi MPLS za stvaranje izgleda VPN mreže na svakoj pretplatničkoj lokaciji. Ethernet paketi su tunelirani koristeći *pseudowire* kroz mrežu pružatelja usluge, neovisno o prometu koji dolazi od drugih korisnika internetske mreže. Okviri se prosljeđuju prema standardima prebacivanja drugog sloja, a tolerancija na pogreške osigurava da svaki paket stiže netaknut na njegovu točnu destinaciju. [57]



Slika 5.11. VPLS arhitektura [58]

Osnovne komponente VPLS arhitekture su (Slika 5.11.):

- AC (engl. *Attachment Circuit*) - priključni krug namijenjen spajanju PE uređaja na CE uređaj; može biti fizički ili logički Ethernet priključak;

- VSI (engl. *Virtual Switching Instance*) - jedinica koja jednoznačno predstavlja svakog korisnika i logički ih međusobno odvaja u PE usmjerivaču;
- VC (engl. *Virtual Circuit*) - sredstvo prijenosa podataka preko paketne komutirane računalne mreže, djeluje kao izravna veza, iako može biti fizički povezana.

VPLS prema svojoj strukturi, ima mnogo zajedničkog s VPN-om drugog sloja. U VPLS-u, paket koji je podrijetlom iz korisničke mreže pružatelja usluge, najprije se šalje CE uređaju (usmjerivaču ili Ethernet preklopniku), a zatim se šalje PE usmjerivaču unutar mreže pružatelja usluge. Paket prelazi mrežu pružatelja usluga preko MPLS LSP-a, dolazi na izlazni PE usmjerivač, koji zatim prosljeđuje promet na CE uređaj. U VPLS-u, paketi mogu prolazi kroz mrežu pružatelja usluga prema konceptu točka-više točaka (engl. *point-to-multipoint*), što bi značilo da se paketi koji potiču od CE uređaja mogu prenositi na sve PE usmjerivače koji sudjeluju u instanci VPLS usmjeravanja. Nasuprot tome, VPN drugog sloja prosljeđuje pakete koristeći točka-točka (engl. *point-to-point*) način prosljeđivanja. [58]

Postoje dvije standardizirane VPLS implementacije koje podržava IETF: RFC 4761[80] - VPLS implementacija pomoću BGP protokola i RFC 4762[81] - VPLS implementacija pomoću LDP protokola.

VPLS kontrolna ravnina ima dvije osnovne funkcije: automatsko otkrivanje i signalizaciju. Automatsko otkrivanje odnosi se na proces pronalaženja svih PE usmjerivača koji sudjeluju u danoj VPLS instanci. PE usmjerivač može se konfigurirati s identitetom svih ostalih PE usmjerivača u određenoj VPLS instanci ili može koristiti određeni protokol kako bi otkrio druge PE usmjerivače. Svaki par PE usmjerivača u VPLS mreži mora biti u stanju međusobno uspostaviti *pseudowire*, a u slučaju promjene članstva PE usmjerivač mora biti u stanju raskinuti uspostavljene *pseudowire* konekcije. Taj je proces poznat kao signalizacija.

BGP-VPLS kontrolna ravnina omogućuje PE usmjerivaču da otkrije koji su udaljeni PE usmjerivači članovi određenog VPLS-a (automatsko otkrivanje) te da zna koja će se *pseudowire* oznaka određenog udaljenog PE usmjerivača koristiti prilikom slanja podataka na lokalni PE usmjerivač (signalizacija). Pomoću BGP-VPLS kontrolne ravnine, BGP nosi dovoljno podataka da istodobno omogući automatsko otkrivanje i signalizaciju. Za razliku od BGP-VPLS kontrolne

[80] RFC 4761 – IETF standard o dostupnosti mrežnog sloja BGP-a, koji u BGP ažuriranjima sadrži podatke za automatsko otkrivanje i signalizaciju.
[81] RFC 4762 - IETF standard o dostupnosti mrežnog sloja BGP-a, koji u LDP ažuriranjima sadrži podatke za automatsko otkrivanje i signalizaciju.

ravnine, LDP-VPLS kontrolna ravnina omogućuje samo signalizaciju, ali ne i automatsko otkrivanje. U ovoj kontrolnoj ravnini, LDP se koristi za signalizaciju *pseudowire* koji se koriste za povezivanje VPLS instanci određenog korisnika sa PE usmjerivačima. U nedostatku mehanizma automatskog otkrivanja, identitet svih udaljenih PE usmjerivača koji su dio VPLS instance mora biti konfiguriran na svakom PE usmjerivaču. [59]

6. PLANIRANJE MREŽE

U ovom poglavlju fokus je na procesu planiranja koji se koristi pri projektiranju računalnih mreža, na fazama koje se koriste pri MPLS mrežnom planiranju i na postojećim izazovima vezanima uz primjenu MPLS tehnike.

6.1. Proces planiranja mreže

Prije kreiranja nove telekomunikacijske mreže, vrlo je važno planirati različite aspekte mreže. Planiranje mreže sastoji se od pet različitih slojeva, pri čemu svi slojevi moraju biti ispravno odrađeni kako bi mreža mogla ispravno funkcionirati. Pet različitih slojeva su navedeni u nastavku:

- Poslovno planiranje;
- Dugoročno i srednjeročno planiranje mreže;
- Kratkoročno planiranje mreže;
- Nabavka opreme;
- Menadžment i održavanje.

Kako bi planiranje mreže bilo uspješno, prvi korak koji treba poduzeti jest prikupljanje relevantnih informacija. Te informacije uključuju načine na koje funkcioniraju nove mreže ili usluge, ekonomske podatke i tehničke detalje o pojedinim karakteristikama mreže.

Prije početka mrežnog planiranja potrebno je napraviti izbor protokola i prijenosnih tehnologija. Nakon što su odrađeni prethodno navedeni početni koraci, proces planiranja mreže sastoji se od tri različite faze:

- dizajniranja topologije;
- mrežne sinteze;
- kreiranje mreže.

Dizajniranje topologije uključuje stvarni smještaj traženih komponenti i načina na koje ih se treba povezati kako bi se formirala mreža koja može prenositi promet po što nižoj cijeni. U ovoj fazi najviše se koristi teorija grafova za određivanje troškova prebacivanja i prijenosa podataka. Faza mrežne sinteze uključuje određivanje veličine potrebnih komponenata. U toj fazi obično se koristi metoda koja se zove nelinearna optimizacija. Ona uključuje određivanje potrebne razine usluge, troškova prijenosa i nekih drugih parametara. Podaci prikupljeni iz prethodne faze koriste se za izračunavanje plana usmjeravanja i veličine korištenih komponenti. Faza kreiranja mreže određuje kako zadovoljiti zahtjeve kapaciteta i osigurati pouzdanost unutar mreže. U toj se fazi obično

upotrebljava metoda koja se naziva optimizacija protoka s višestrukim uvjetima koja uključuje određivanje informacija vezanih uz potražnju, troškove i pouzdanost. Te se informacije zatim koriste za izračun stvarnog plana fizičkog sklopa. [60]

6.1.1. Telekomunikacijsko predviđanje

Svi pružatelji telekomunikacijskih usluga vrše predviđanje koje im pomaže pri planiranju njihovih mreža. Točno predviđanje pomaže operatorima da donose ključne investicijske odluke, koje se odnose na razvoj proizvoda, oglašavanje, cijenu itd., i to prije lansiranja proizvoda. Predviđanje se može provesti u mnoge svrhe pa je vrlo važno da razlog za obavljanje proračuna bude jasno definiran i razumljiv. Neki od uobičajenih razloga za predviđanje su [61]:

- Planiranje i određivanje budžeta - korištenje postupaka predviđanja može pomoći kod donošenja odluke o kupovini mrežne opreme, koliko opreme kako bi se osiguralo optimalno upravljanje prometnim opterećenjima;
- Procjena - predviđanje može pomoći kod upravljanja odlukom, hoće li donesena odluka biti prednost ili će pak naštetiti;
- Provjera - kada podaci o novim predviđanjima postanu dostupni, potrebno je provjeriti podržavaju li nova predviđanja ishode predviđene starim postupcima predviđanja.

Metoda telekomunikacijskog predviđanja uključuje sljedeće korake:

- Definiranje problema;
- Prikupljanje podataka;
- Izbor metode predviđanja;
- Analizu predviđanja;
- Dokumentaciju i analizu rezultata.

Prva faza je tipična za svaki proces predviđanja. To u osnovi znači da projektant mora biti siguran u problem za koji pokušava pronaći rješenje. Cilj predviđanja mora se definirati što je moguće detaljnije kako bi se dobio model predviđanja za simuliranje dovoljno preciznih budućih mrežnih prometnih karakteristika.

U fazi prikupljanja podataka, potrebno je da prikupljeni podaci budu spremni za proces predviđanja. Ukoliko podaci sadrže pogreške i predviđanje će biti pogrešno. Taj proces poznat je pod nazivom "pročišćavanje" podataka (engl. *Data scrubbing*). Pročišćavanje podataka koncentrira se na uklanjanju određenih točaka podataka, koje se nazivaju točke odudaranja (engl. *outliers*). Točke odudaranja su podaci koji se nalaze izvan normalnog uzorka, uzrokovani su

nepravilnim događajima i vjerojatno se neće ponoviti. Uklanjanje tih podatkovnih točaka poboljšava "integritet podataka" i tako povećava točnost predviđanja.

Postoji nekoliko metoda predviđanja koje su danas u upotrebi. U nastavku su navedene neke od metoda [61]:

- Metode temeljene na prosudbi
    - Delphi metoda
    - Ekstrapolacija
- Metode istraživanja
- Metode vremenskih nizova
    - Eksponencijalno izglađivanje
    - Ciklični i sezonski trendovi
    - Statistički modeli
- Analogne metode
- Uzročni modeli

Metode temeljene na prosudbi oslanjaju se na mišljenje i znanje ljudi koji imaju znatno iskustvo u području u kojem se provodi predviđanje. Delphi metoda uključuje usmjeravanje niza pitanja stručnjacima za područje za koje se traži predviđanje. Stručnjaci daju svoje procjene glede budućeg razvoja. Istraživači rezimiraju odgovore i šalju sažetak odgovora stručnjacima, pri čemu stručnjaci mogu revidirati svoje odgovore. Delphi metoda nije pouzdana i uspješna je u vrlo rijetkim slučajevima. Ekstrapolacija je uobičajena metoda predviđanja koja se temelji na pretpostavci da će se budući događaji nastaviti razvijati uz iste granice kao i prethodna događanja, tj. prošlost je dobar prediktor budućnosti. Istraživač najprije dobije podatke o prethodnim događajima i obrađuje ih. Nakon toga, određuje postoji li obrazac, ako postoji, pokušava proširiti obrazac u budućnost i tako počinje generirati predviđanje onoga što će se vjerojatno dogoditi. Kako bi proširili obrasce, istraživači općenito upotrebljavaju jednostavno pravilo ekstrapolacije, poput logističke sigmoidne funkcije.

Metode istraživanja temelje se na mišljenjima korisnika. U obavljanju istraživanja potrebno je identificirati ciljnu skupinu istraživanja. Kada je ciljna skupina identificirana, mora se odabrati uzorak. Uzorak je podskup ciljne skupine i mora biti odabran tako da točno odražava sve u željenoj ciljnoj skupini. Istraživanje se sastoji od niza pitanja koja se postavljaju grupi uzoraka, pri čemu se bilježe njihovi odgovori. Zabilježeni odgovori moraju se zatim analizirati pomoću statističkih i analitičkih metoda. Rezultati istraživanja trebaju se provjeriti pomoću alternativnih metoda

predviđanja i rezultati se zatim mogu objaviti. Važno je imati na umu da je ova metoda točna samo ako je uzorak uravnotežen i ukoliko je skupina uzoraka točno odgovorila na postavljena pitanja.

Metode vremenskih serija koriste uzorke podataka koji su periodično mjereni. Ove metode koriste takve podatke za razvoj modela koji se zatim mogu koristiti za ekstrapolaciju u budućnost, čime se generira predviđanje. Svaki model funkcionira prema drugom skupu pretpostavki i oblikovan je za drukčiju svrhu. Eksponencijalno zaglađivanje temelji se na pomičnim prosječnim podacima. Ciklični i sezonski trendovi pretražuju podatke iz nekih uzoraka ili trendova koji se ponavljaju u cikličkim ili sezonskim razdobljima. Istraživači tada mogu koristiti trenutne podatke kako bi prilagodili uzorak, tako da odgovara podacima iz tog razdoblja te se na taj način može predvidjeti što će se dogoditi tijekom ostatka tekuće sezone ili ciklusa. Statistički modeli omogućuju istraživačima razvijanje statističkih odnosa između varijabli. Ovi se modeli temelje na trenutačnim podacima te je pomoću ekstrapolacije moguće stvoriti budući model. Tehnike ekstrapolacije temelje se na standardnim statističkim zakonima, čime se poboljšava točnost predviđanja. Statističke tehnike ne samo da proizvode prognoze već i kvantificiraju preciznost i pouzdanost. Primjeri toga su ERLANG B[82] i C[83] formule, koje je 1917. godine razvio danski matematičar Agner Erlang.

Analogne metode uključuju pronalaženje sličnosti između vanjskih događaja i događaja koji se proučavaju. Vanjski događaji obično imaju više uzoraka podataka nego proučavani. Analogne metode primjenjuju dvije skupine modela: kvalitativne modele i kvantitativne modele. Pri kvalitativnim metodama usporedba vanjskih događaja je načinjena tako da tvori simboličnu sličnost. U kvantitativnom postupku količina se uspoređuje i predviđa.

Uzročni modeli su najprecizniji i najsloženiji oblik predviđanja. Oni uključuju stvaranje složenog i cjelovitog modela predviđenih događaja. Model mora sadržavati sve moguće varijable i mora biti u stanju predvidjeti svaki mogući ishod. Uzročni modeli često su tako složeni da se mogu stvoriti samo na računalima. Razvijeni su pomoću podataka iz skupa događaja.

6.1.2. Dimenzioniranje mreže

Glavna svrha ove faze planiranja mreže je odrediti minimalne zahtjeve na kapacitet koji omogućuje postizanje tražene razine usluge (engl. *Grade of Service* - GoS[84]). Iz tog razloga,

[82] ERLANG B - Formula za modeliranje koja se uglavnom koristi u raspoređivanju pozivnih centara.
[83] ERLANG C - Formula za modeliranje prometa koja se koristi za planiranje pozivnih centara, kod izračunavanja kašnjenja ili predviđanja vremena čekanja za pozive.
[84] GoS - Vjerojatnost korištena u telekomunikacijama za izražavanje kvalitete govorne usluge.

dimenzioniranje uključuje planiranje prometa u „vršnom“ satu; onom satu tijekom dana tijekom kojeg je intenzitet prometa na vrhuncu.

Proces dimenzioniranja uključuje određivanje topologije mreže, izradu plana usmjeravanja i matrice prometa te izradu GoS zahtjeva. Informacije primljene iz tih pod-faza koriste se za određivanje maksimalnog kapaciteta koji podržava pojedini prespojnik (engl. *switch*) i maksimalnog broja kanala koji su potrebni između prespojnika.

Pravilo dimenzioniranja nalaže da projektant mora osigurati da prometno opterećenje ne dostigne sto postotno opterećenje. Za izračunavanje točnog opterećenja u skladu s gore navedenim pravilom, projektant mora provoditi mjerenja mrežnog prometa i kontinuirano održavati i nadograđivati resurse, kako bi udovoljili promjenjivim zahtjevima. U slučaju kvara u mreži, potrebno je osigurati dodatnu propusnost, kako bi se promet mogao preusmjeriti. [60]

Budući da je dimenzioniranje mreže vrlo složen proces, on se vrši pomoću specijaliziranih softverskih alata. Dok istraživači obično razvijaju prilagođeni softver za proučavanje određenog problema, mrežni operatori obično koriste softver za komercijalno planiranje mreže.

6.1.3. Upravljanje mrežnim prometom

Za razliku od postupaka upravljanja mrežnim prometom koji u mrežu dodaju resurse kao što su prijenosni linkovi, usmjerivači i preklopnici, u primjeni su bitni i postupci upravljanja mrežnim prometom koji se usmjeravaju na kontrolu puta kojim se promet prosljeđuje kroz mrežu.

Postoje mnogi razlozi zašto mrežni operatori žele utjecati na put kojim se promet prosljeđuje kroz mrežu. Najčešći razlog upravljanja mrežnim prometom trenutno je poboljšanje korištenja mrežnih resursa. Cilj postupaka upravljanja mrežnim prometom je izbjegavanje situacija u kojoj su dijelovi mreže zagušeni dok su drugi nedovoljno iskorišteni. Ostali razlozi uključuju osiguravanje da podaci putuju putem koji ima određene željene karakteristike, osiguravajući na taj način da su prijenosni resursi dostupni na tom putu te određivanje prioritetnog prometa u trenutku nedostatka resursa. [62]

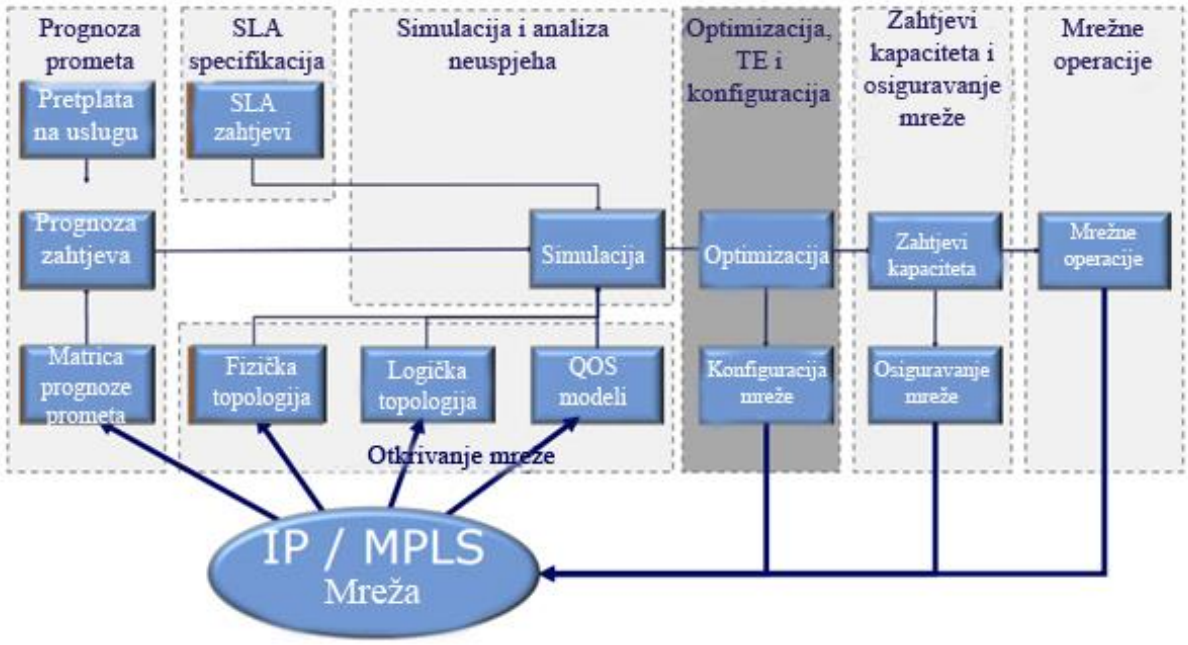
6.2. Različite faze MPLS mrežnog planiranja

Baš kao i sve druge vrste mreža, MPLS mreže imaju mnogo različitih faza planiranja. U ovom poglavlju definirat će se faze planiranja i opisat će se njihovo značenju u MPLS shemi.

Možemo reći kako je MPLS planiranje mreže rezultat mnogih područja planiranja. Slika 6.1. prikazuje različita područja planiranja MPLS mreže, pri čemu su sve faze mrežnog planiranja

podijeljene na manje dijelove. Predviđanje prometa stvara se na temelju matrice potražnje prometa i pretplate na telekomunikacijske usluge. Faza otkrivanja mreže je zbroj fizičke i logičke topologije te se u toj fazi odlučuje i o QoS modelima. Fizička topologija obuhvaća uređaje i veze u dizajniranoj mreži, dok logička struktura obuhvaća raspored uređaja u mreži i način na koji ti uređaji međusobno komuniciraju.

Sljedeća faza je ugovor o razini usluge (engl. *Service-Level Agreement* - SLA[85]) specifikacija, koja se temelji na zahtjevima koji su uglavnom dogovoreni u suradnji s korisnikom. Nakon ove dvije faze, mrežni projektant može napraviti svoj prvi simulacijski prikaz, kako bi analizirao ponašanje mreže. Nakon prve simulacije, mrežni projektant može nastaviti s optimizacijom mreže, kao i s tehnikama upravljanja mrežnim prometom koje mogu uravnotežiti i optimizirati promet koji se isporučuje u mreži. Ova faza pomaže i sljedećoj fazi koja sadrži definiranje zahtjeva za kapacitetom i pružanje mrežnih elemenata za usluge različitih korisnika. Posljednja faza su mrežne operacije koje obuhvaćaju nadzor, kontroliranje i održavanje mreže. Nakon ovih faza planira se prvi model mreže. [62]



Slika 6.1. Faze planiranja mreže [63]

[85] SLA - Ugovor između pružatelja usluga i krajnjeg korisnika koji definira razinu usluge koja se očekuje od davatelja usluga.

6.2.1. Faza predviđanja

Faza predviđanja u MPLS mreži vrši se matricom potražnje prometa (koja se naziva i prometnom matricom) i cijenom pretplate usluge. Odluka o odabiru prometne matrice koja se koristi za modeliranje prometa MPLS mreže nije jednostavan zadatak. Teškim ga čini širok izbor različitih vrsta modela i činjenica da MPLS mreže mogu biti vrlo različite. Mogu se razlikovati po veličini (količina čvorova, veza i pretplatnika koji se poslužuju), obliku (model topologije koji se koristi), funkcionalnosti i vrsti prometa. [64]

Faza pretplate usluga definira razinu usluge koja se može dati određenom korisniku. Mreža ima ograničenu količinu resursa koja se može podijeliti između korisnika. Pretplata na usluge uključuje mnoge parametre koji određuju usluge koje se mogu ponuditi korisnicima.

6.2.2. Ugovor o razini usluge

Ugovor o razini usluge (*Service Level Agreement* - SLA) je alat kojim se stvara međusobni dogovor o uslugama i isporuci usluga između davatelja usluga i njihovih korisnika. Njime se određuju očekivanja, razjašnjavaju odgovornosti i stvara objektivna osnova za procjenu učinka usluge. U slučaju MPLS-a, SLA zahtijeva širi raspon mjernih podataka o razini usluge od tradicionalnih tehnologija. Ugovori o razini usluge mogu se razlikovati unutar regije, no unatoč razlikama, obično uključuju neke ključne mjerne podatke koji se mogu pronaći u većini ugovora. Mjerni podaci obuhvaćaju dostavu paketa od mjesta do mjesta, kašnjenje, varijacije kašnjenja, dostupnost stranica i maksimalno vrijeme za popravak.

SLA za kašnjenje i varijacije kašnjenja obično pokriva samo jezgrene mreže, a ne i rubne dijelove. Podaci navedeni u SLA dokumentima često se temelje na mjesečnom prosjeku, što je dobar pokazatelj ukupne uspješnosti. Svako kašnjenje i varijacija kašnjenja mora biti niže od navedene razine u SLA dokumentu. SLA dokument omogućuje korisnicima da shvate je li pružatelj usluga u mogućnosti podržavati osjetljive i kritične aplikacije kao što su audio i videozapis. [65]

6.2.3. Faza definiranja mreže

Faza definiranja mreže podijeljena je na definiranje fizičkih topologija, definiranje logičkih topologija i definiranje QoS-a. Fizička i logička topologija često se definiraju u istoj fazi, pomoću istog alata. Topologija mreže može biti vrlo raznovrsna u mrežama koje koriste MPLS tehnike zbog različitih karakteristika korištene opreme i zbog rada na različitim mrežnim slojevima.

Proces definiranja topologije mreže obično se sastoji od jedne ili dvije metode. U prvoj metodi, definiranje se obavlja dodavanjem pojedinog uređaja ili logičke veze. Prvo se dodaju pristupne točke, (engl. *Point of Presence* - POP[86]) a zatim se u topologiju umeću poveznice koje povezuju POP-ove, nakon čega se generira logička topologija. Dodavanje jednog po jednog uređaja obično se vrši putem grafičkog korisničkog sučelje (eng. *Graphical User Interface* - GUI[87]) pri čemu cjelokupna konfiguracija mora biti ručno umetnuta na uređaje ili logičke veze u mreži. Konfiguracija se sastoji od sučelja uređaja, vrste uređaja, protokola i tehnologija koje se pokreću na uređaju, virtualnih veza itd.

Drugi metoda za obavljanje procesa definiranja mreže podrazumijeva uvoz željene mrežne topologije kao cjeline pomoću neke vrste uvoznih značajki modeliranja/planiranja ili alata za upravljanje MPLS mrežom. Alat dobiva topološke informacije iz nekog drugog alata za upravljanje ili iz neke datoteke koja sadrži topološke informacije spremljene u formatu kojem se može pristupiti pomoću alata za modeliranje/planiranje. Ovo je metoda koja se uglavnom koristi u aktualnim MPLS mrežama u realnim mrežnim okruženjima, uglavnom zbog svoje skalabilnosti. Formiranje topologije mreže u slučaju velike mreže s više tisuća POP-ova nije moguće uz pomoć prve metode.

Današnje mreže uglavnom koriste automatsko otkrivanje, gdje se informacije o POP-u automatski šalju u bazu podataka, što se općenito naziva baza podataka o upravljanju (engl. *Management Information Base* - MIB[88]), kada se stanje elementa promijeni ili se novi element dodaje u mrežu koristeći poruke jednostavnog protokola za upravljanje mrežom (engl. *Simple Network Management Protocol* SNMP[89]) ili neku drugu vrstu poruke. Kada se informacije pohranjuju na jednom mjestu, mrežni administratori ili druge osobe im lako pristupaju. Ti se podaci obično šalju alatu za planiranje/upravljanje putem različitih shema slanja poruka kao što su jezik za

[86] POP - Točka umjetnog razgraničenja ili sučelja između komunikacijskih entiteta.
[87] GUI - Vrsta korisničkog sučelja koje korisnicima omogućuje interakciju s elektroničkim uređajima putem grafičkih ikona i vizualnih pokazatelja kao što je sekundarna notacija, umjesto korisničkog sučelja temeljenog na tekstu, upisivanjem naredbi ili navigacije tekstom.
[88] MIB - Računalni informacijski repozitorij koji koristi SNMP (engl. Simple Network Management Protocol) i druge implementacije.
[89] SNMP - Jednostavni protokol koji se danas najčešće koristi za nadzor i upravljanje mrežnim uređajima u TCP/IP mrežama. On omogućava mrežnim administratorima da upravljaju mrežnim performansama, nalaze i rješavaju mrežne probleme te planiraju potrebe za rastom mreže.

označavanje podataka (engl. *Extensible Markup Language* - XML[90]) ili datoteka sa vrijednostima odvojenim zarezom (engl. *Comma-Separated Values* - CSV[91]). [66]

Posljednji dio definiranja mreže je QoS modeliranje. QoS funkcionalnost u MPLS-u se kreira uz primjenu *DiffServ* ili *IntServ* modela. *Intserv* se zbog loše skalabilnosti ne primjenjuje u realnim MPLS mrežama. *DiffServ* je trenutno jedina odluka koja se koristi u komercijalnim MPLS mrežama.

6.2.4. Simulacija i analiza mrežnih scenarija

Simulacijski dio je u fokusu svih alata za mrežno planiranje. U simulacijskom djelu moguće je promatrati atribute postojeće/planirane mreže, simulirati učinke mogućih budućih mrežnih topologija i promjene atributa/funkcija ili se mogu pokrenuti različiti scenariji neuspjeha kako bi se provjerilo kako se mreža ponaša u pojedinim slučajevima.

Simulacija MPLS mreže zahtijeva malo više funkcionalnosti nego simulacija IP prometa. Budući da MPLS ima puno različitih funkcija i može se izvoditi na različitim slojevima, to omogućuje vrlo širok izbor postojećih simulacija. Simulacija može uključivati različite vrste VPN-a, kao i osnovne MPLS funkcije (prebacivanje oznaka, RSVP-TE, LDP, CR-LDP i dr.).

6.2.5. Optimizacija, upravljanje i konfiguracija čvorova u mreži

Nakon što su željeni simulirani slučajevi pokrenuti, simulirana mreža je spremna za optimiziranje. Optimizacija se može provesti na više načina: može biti strukturna, provedena kroz tehnike upravljanja mrežnim prometom, financijska (što najčešće i je), itd. U MPLS mrežama najvažniji, ali u istom trenutku i najisplativiji dio optimizacije uključuje tehnike upravljanja mrežnim prometom, jer ono može biti provedeno bez dodatnih ulaganja u mrežu, te čak može i omogućiti dodavanje novih korisnika u slobodni mrežni prostor nakon optimizacije. Također, upravljanje mrežnim prometom može pomoći kod problema sa zagušenjem, na način da preusmjerava određeni promet iz zagušenih linkova ili čvorova.

Nakon što je završena optimizacija mreže na rezultatima dobivenim iz različitih simuliranih slučajeva, rezultati su spremni za primjenu u stvarnoj mreži. To se radi na način da se konfiguriraju određeni parametri ili uređaji unutar mreže. Kako bi takva konfiguracija bila uspješna, željene

[90] XML - Skup pravila za kodiranje dokumenata elektroničkim putem. Također se koristi za razmjenu podataka preko Interneta.
[91] CSV - Ograničena tekstualna datoteka koja koristi zarez da se odvoji vrijednosti. Pohranjuje tablične podatke (brojeve i tekst) u običan tekst.

promjene konfiguracije moraju se distribuirati ostalim uređajima na način da nakon toga treba što manje ručnih postavki.

Dva su razloga zbog kojih je bitno da je konfiguracija uspješna; prvi je taj da se mogućnost pogreške povećava ukoliko se radi ručno, a drugi jer su promjene koje se mogu učiniti na konfiguraciji vrlo širokog raspona. Bilo bi vrlo neekonomično zapošljavati brojne stručnjake kako bi odradili ovakvu vrstu optimizacije mrežne konfiguracije. Mnogi alati za planiranje nude opciju izvoza konfiguriranih postavki iz simulacije u stvarnu mrežu. [62]

6.2.6. Planiranje zahtjeva za kapacitetom te dijeljenjem mrežnih resursa

Nakon što se završi postupak definiranja prometnih zahtjeva za mrežu temeljenu na postojećim zahtjevima za kapacitetom, pristupa se postupcima analize načina na koje se procijenjeni zahtjevi mogu smanjiti. Unutar postupka planiranja, to se može provesti u nekim dijelovima mreže zbog preusmjeravanja prometa.

Dijeljenje MPLS mreže se može izvesti prilično jednostavno, koristeći pojednostavljenje metode. Dijeljenje resursa između različitih servisa može se izvršiti gotovo u potpunosti koristeći VPN-ove. Zbog različitih vrsta i end-to-end usmjeravanja pomoću dijeljenja LSP-ova, mrežni administrator mreže može upotrijebiti, za primjer, BGP da omogući dijeljenje zadataka LSP-a od početka do kraja. Jedini dijelovi koji zahtijevaju specifičnu konfiguraciju su ulazni i izlazni usmjerivači LSP-a. Ova se konfiguracija također može automatizirati upotrebom određenih alata za planiranje ili upravljanje. Primijenjeni alat može omogućiti izvoz definirane konfiguracije putem određenih komunikacijskih protokola te konfiguriranjem uređaja kao "udaljenog uređaja". [62]

6.2.7. Faza definiranja funkcionalnosti mreže

Zadnji dio iteracijskog kruga planiranja je faza definiranja mrežnih operacija. Mrežne operacije se uglavnom sastoje od upravljačkih zadataka u mreži. U ovoj fazi alat za planiranje dobiva dodatne informacije o modelu, tako da se može prilagoditi modelu mreže, njegovoj funkcionalnosti i prometu u mreži. U ovoj fazi su predviđena i sva održavanja elemenata . Ti elementi imaju različite funkcionalnosti, ali obično imaju zajedničke osnovne funkcije. Za ovaj dio pružatelji usluga obično koriste neke vrste centraliziranih operacijskih alata ili uređaja. Ti alati obično uključuju hvatanje i pohranu svojstva informacijskih tokova. Jedan od takvih alata je *Lancope StealthWatch*. Njegove ključne značajke su [67]:

- Pruža integrirani, stvarno-vremenski pregled korištenja mreže i mrežnih performansi;

- Korištenje postojećih NetFlow[92] ™ i sFlow[93]® usmjerivača i preklopnika, kao i izvornih informacija o smanjemom protoku kako bi pružio sveobuhvatan pristup mrežnoj sigurnosti i optimizaciji;
- Smanjuje vrijeme potrebno za otkrivanje i razdvajanje sigurnosnih i mrežnih događaja, kao i vrijeme za generiranje odgovora;
- Podržava segmentirane, velike brzine internih mreža i potpuno povezano mrežno okruženje;
- Analizira trendova koji ubrzavaju planiranje kapaciteta mreže i napredno upravljanje resursima.

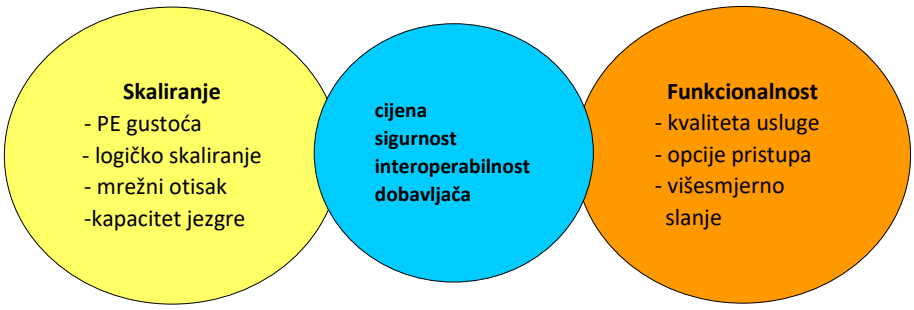
6.3. Izazovi pri implementiranju MPLS mreža

Prije navođenja izazova vezanih uz MPLS alate za planiranje, potrebno je navesti neke od izazova pri implementiranju MPLS mreža, budući da se zahtjevi vezani uz primjenu MPLS mreža kontinuirano povećavaju. Najznačajniji izazovi s kojima se MPLS mreže susreću su skalabilnost te ostvarivanje postavljenih zahtjeva vezanih uz funkcionalnost mreže kako bi se omogućilo praćenje rastućeg broja korisnika i potrebnih usluga.

Sa vrstama prometa koji je osjetljiviji na kašnjenje kao što su VoIP[94] (engl. *Voice over Internet Protocol* - VoIP[95]) ili video promet, pojavila se potreba za kategorizacijom prometa. Istodobno, s razvojem korisničkih mreža koje su sve veće i kompleksnije, povećava se i broj različitih tehnika koje se koriste u prijenosu.

Kako bi rast mreža bio održiv, pružatelji usluga moraju zadržati mogućnost podržavanja VPN usluge u istom omjeru te nastaviti razvijati niz uslužnih značajki. Razvojni i funkcionalni aspekti se uvijek moraju planirati zajedno s troškovima te sigurnosnim aspektima te interoperabilnošću dobavljača, odnosno pružatelja mrežne opreme i usluga, kako bi unaprjeđenja bila još održivija Izazovi u inženjerstvu vezani za MPLS pružatelje usluga i njihove odnose prikazani su na slici 6.2.

[92] NetFlow - Mrežni protokol kojeg je razvila tvrtka Cisco za prikupljanje informacija o IP prometu i praćenje mrežnog prometa.
[93] sFlow - Standardna tehnologija za praćenje brzih preklopnih mreža. Ona daje potpunu vidljivost u korištenju mreža koje omogućuju optimizaciju performansi, predračun/naplatu za upotrebu i obranu od sigurnosnih prijetnji.
[94] VOiP - komunikacijska tehnologija koja omogućava prijenos zvučne komunikacije preko internetske mreže.
[95] VOiP - komunikacijska tehnologija koja omogućava prijenos zvučne komunikacije preko internetske mreže.



Slika 6.2. Inženjerski izazovi za MPLS pružatelje usluga [68]

6.3.1. Izazovi pri skaliranju MPLS mreža

Na slici 6.2. prikazana su četiri glavna izazova koji utječu na skalabilnost MPLS platforme: PE gustoća, logičko skaliranje, mrežni trag i kapacitet jezgre.

Jedan od kritičnih aspekata skalabilnosti fizičke mreže je sposobnost podržavanja brzog rasta količine korisničkih zahtjeva bez potrebe za implementacijom velike količine PE pristupnih usmjerivača. Troškovi po portu mogu biti smanjeni, a skaliranje se može ojačati implementacijom zbijenih PE uređaja. Ne potiče samo aspekt ekonomičnosti zadržavanje broja PE usmjerivača u odnosu na gusto agregiranje velikog broj korisničkih pristupnih krugova. Također vrlo je važno i odražavanje logičke skalabilnosti. U VPN BGP/MPLS mreži potrebno je logičko stanje kako bi se održala povezanost i dostupnost između PE uređaja u obliku LSP i BGP jednačenja (engl. *peering*[96]). LSP-ovi su stvoreni u kontrolnoj ravnini i nakon što su uspostavljeni olakšavaju MPLS prosljeđivanje paketa u podatkovnoj ravnini. BGP jednačenje formira se u kontrolnoj ravnini preko TCP sesija, što zauzvrat olakšava razmjenu korisničkih specifičnih VPN usmjerenih informacija, pohranjenih u PE usmjerivačima. Gomilanje logičkog stanja izravno je povezano s brojem PE usmjerivača u mreži koji se koriste za ukidanje korisničkih pristupnih veza.

Sposobnost podrške prilično velikom mrežnom otisku koji pruža široku geografsku pokrivenost također je kritičan aspekt fizičkog skaliranja. Izgradnja pristupnih točaka (POP) i WAN povezanosti među njima može predstavljati značajan trošak, no mnogi pružatelji VPN usluga ciljaju na određene geografske lokacije poput velikih urbanih sredina. Kada operator ne može ulagati u mrežnu infrastrukturu u svim zemljama u kojima želi poslovati sklapa komercijalni

[96] peering - dobrovoljno povezivanje administrativno odvojene internetske mreže u svrhu razmjene prometa između korisnika svake mreže.

ugovor s pružateljima usluga, kako bi formirali strateško partnerstvo i došli do željenog geografskog područja.

Stvaranje jezgrenih mreža više-autonomnog sustava (engl. *Multi - Autonomous System* - multi-AS[97]) donosi više rizika, jer cijela jezgrena mreža više nije pod kontrolom samo pružatelja usluga.

Posljednji element skalabilnosti povezan je s rastućim izazovom upravljanja velikim brojem korisnika u mreži. Temeljni cilj djelotvornog upravljanja jezgrenom mrežom jest implementiranje potrebne jezgrene WAN veze koja omogućuje posluživanje prometnih zahtjeva i ispunjava potrebne kriterije uspješnosti kao što su propusnost paketa, kašnjenje i varijacije kašnjenja. To mora biti učinjeno na ekonomičan način, pa se zbog toga nadogradnje kapaciteta WAN veze odgađaju ili izbjegavaju gdje god je to moguće.

Odgađanje nadogradnje WAN veza može se postići optimiziranjem toka prometa podataka u osnovnoj mreži tako da se mrežno opterećenje širi ravnomjerno oko dostupnih WAN veza. MPLS-TE je način uravnoteženja opterećenja u mreži. Tuneli izrađeni s MPLS TE omogućuju izbjegavanje veze s visokim i korištenje veze s nižim troškovima, čime se osigurava prosljeđivanje prometa mrežom na optimalan način. [68]

6.3.2. Izazovi funkcionalnosti MPLS mreža

U današnje vrijeme "*DiffServ*" tehnologija se primjenjuje u MPLS mrežama. U ovom trenutku postoje dvije različite tehnike koje mogu klasificirati različite tipove prometa do 8 (E-LSP[98]) ili 64 (L-LSP[99]). U ovom trenutku, pružatelji usluga uglavnom ne trebaju više od 8 različitih klasa prometa, tako da su za većinu pružatelja usluga E-LSP-ovi dovoljno adekvatni za određivanje prioriteta različitih vrsta prometa. Unatoč tome, vrste klasa (engl. *Class Type* - CT[100]) moraju se i dalje pažljivo planirati. Vrlo je važno postaviti prioritete, stoga će najhitniji i najvažniji tipovi prometa biti označeni kao "prioritet".

Korisnici MPLS VPN mreža obuhvaćaju širok i raznolik raspon s obzirom na broj pristupnih krugova, geografsku pokrivenost i širine pristupnog pojasa. Korisnici IP VPN usluga kontinuirano zahtijevaju najisplativije načine isporuke usluga.

---

[97] AS - Mreža ili zbirka mreža kojom upravlja i nadzire samo jedan entitet ili organizacija.
[98] E-LSP - LSP na kojem čvorovi zaključuju QoS postupak za MPLS paket isključivo od EXP bita u MPLS zaglavlju.
[99] L-LSP - je LSP na kojem čvorovi zaključuju QoS postupak za MPLS pakete iz paketa oznaka i EXP bita.
[100] CT – Skup koji se upotrebljava u svrhu raspodjele širine pojasa veze, usmjeravanja na temelju ograničenja i kontrole pristupa.

Jedinstvene karakteristike širokog raspona mogućih pristupih rješenja važne su za pružatelje usluga jer su s time tehnički zahtjevi za PE uređaje mnogo kompleksniji. Sukladno tome, funkcionalnost PE uređaja koji isporučuje promet korisničkoj mreži temeljenoj na Ethernetu najvjerojatnije neće biti optimalna zamjena za korisničke mreže temeljenje na xDSL-u. Pružatelj usluga mora ispuniti zahtjeve koji su ponuđeni od strane drugačijih pristupnih tehnologija. PE uređaji moraju biti ujednačeni u uvjetima pružanja usluga ponuđenih od strane VPN pružatelja usluga (na primjer QoS i mogućnost slanja podataka na više računala), bez obzira na pristupnu tehnologiju koja se koristi.

IP višesmjerno slanje (engl. *multicast*[101]) podataka uključuje učinkovito prenošenje paketa podataka na odabrani broj primatelja s odgovarajućom adresom i prosljeđivanje paketa u mreži. Višesmjerno odašiljanje ima široku upotrebu u današnjim jezgrenim mrežama te u mrežnom poslovanju u cijelosti. Na primjer, IT kompanije mogu koristiti višesmjerno odašiljanje kako bi distribuirali redovne nadogradnje softvera svojim zaposlenicima. Osim toga, višesmjerno odašiljanje koristi se i u financijskom sektoru kako bi se razmjenjivale stvarne tržišne informacije između pružatelja usluga i klijenata.

Prilikom planiranja MPLS mreže, ostvarivanje funkcionalnosti višesmjernog slanja i funkcionalnosti između jedne krajnje točke i drugih točaka (engl. *point-to-multipoint* - P2MP[102]) vrlo je izazovan zadatak, ponajviše zbog prirode potrebnih tehničkih dostignuća. Višesmjerno odašiljanje utječe na većinu mrežnih segmenata, uključujući QoS, upravljanje mrežnim prometom, dimenzioniranje i dijagnostiku mreže te izvješćivanje o efikasnosti. [68]

[101] Multicast - Grupna komunikacija u kojoj je prijenos podataka istodobno adresiran na skupinu odredišnih računala.
[102] P2MP - Komunikacijska mreža koja pruža put s jednog mjesta na više lokacija.

7. POSTOJEĆI ALATI ZA PLANIRANJE MPLS MREŽE

U ovom trenutku postoji veliki broj alata za planiranje MPLS mreža koji pripomažu u planiranju i upravljanju mrežama. Većina ovih alata se koristi u komercijalne svrhe, ali se također mogu pronaći i neke aplikacije koje su besplatne za korištenje. U ovom odlomku fokus je na postojećim alatima. Analizirat će se funkcionalnost dva različita alata za planiranje MPLS-a, a to su: IP/MPLSView kreiran od strane "*Wanl, Inc*" te *iVNT* kreiran od strane "*Aria Networks Ltd*."

Postoje drugi alati za planiranje MPLS-a, no za njih postoje vrlo male količine dostupnih informacija. Neki od alata koji su dizajnirani za planiranje MPLS mreža su:

- MATE
- SP Guru
- OnePlan

7.1. IP/MPLSView

IP/MPLSView je alat kreiran od strane WANDL Laboratorija (engl. *Wide Area Network Design Laboratory*) za višeslojno upravljanje prometom i tehnike upravljanja mrežnim prometom. IP/MPLSView nudi različite funkcionalnosti za dizajniranje mreža i planiranje kao i za mrežno inženjerstvo te operacije u MPLS mrežama.

Slika 7.1. Funkcionalnost IP/MPLSView-a [69]

Slika 7.1. pokazuje da je funkcionalnost IP/MPLSView-a podijeljena u dvije kategorije: dizajniranje mreže i zahtjeve za planiranje te mrežno upravljanje i operacijske zahtjeve. Oba ova aspekta su bitna kada govorimo o planiranju/dizajniranju MPLS mreže. Dobro i temeljito

planiranje je ključan dio za predstojeće postupke upravljanja i održavanja mreže. Može se reći da to funkcionira u oba smjera: dobro mrežno upravljanje i održavanje daje dobre preduvjete za sve buduće nadogradnje i promjene u mreži.

Minimalni zahtjevi za pokretanje IP/MPLSView-a, ovise o veličini simulirane mreže te detaljima mreže koju želimo simulirati. Kompanija "*Wandl*" objavila je preporučenu sistemsku konfiguraciju pri kojoj bi IP/MPLS radit bez većih problema. Ti su sistemski zahtjevi prikazani na slici 7.2.

Preporučena konfiguracija sustava

Poslužitelj
- Sun radna stanica*
- Solaris 10 ili više
- 4 GB ili više RAM
- 6 GB prostora na disku poslužitelja

Klijent (Sun radna stanica)
- Solaris 10 ili više
- 1 GB ili više RAM
- 600 MB prostora na disku

Klijent (PC)
- Windows 2000/NT/XP/Vista
- Linux (podržava Sun VM)
- 1 GB ili više RAM

Slika 7.2. Preporučena konfiguracija sustava za IP/MPLSView [70]

Glavne funkcije IP/MPLSView alata odnose se na dizajniranje i planiranje. Kompanija *Wandl* podijelila je planiranje na tri različita modula kada se govori o funkcionalnosti IP/MPLSViewa: simulacija, dizajniranje i optimizacija.

Govoreći o simulaciji, IP/MPLSView nudi podršku za sljedeće protokole usmjeravanja: ISIS[103] (engl. *Intermediate System-to-Intermediate System*), OSPF, IGRP[104] (engl. *Interior Gateway Routing Protocol*), RIP[105] (engl. *Routing Information* Protocol), EIGRP, GRE[106] (engl. *Generic*

[103] ISIS - Protokol za usmjeravanje dizajniran za učinkovito premještanje informacija unutar računalne mreže, grupe fizički povezanih računala ili sličnih uređaja.
[104] IGRP – Protokol kojeg koriste usmjerivači za razmjenu podataka usmjeravanja u autonomnom sustavu.
[105] RIP - Najstariji usmjerivački protokol koji se primjenjuje na Internetu. On šalje nove usmjerivačke poruke u pravilnim intervalima ili kada se promjeni topologija mreže.
[106] GRE - Protokol IP enkapsulacije koji se koristi za prijenos IP paketa preko mreže.

Routing Encapsulation), BGP i MPLS. Također podržava konfiguraciju statičkih i zadanih ruta. [71]

Alat za simulaciju IP/MPLSView-a nudi mogućnost simuliranja različitih scenarija pokušaja i pogrešaka [71]:

- višeslojnih pogrešaka u LSP tunelima i IP sloju;
- niza pogrešaka;
- pogrešaka više mrežnih elemenata;
- pogrešaka u pojedinim dijelovima mreže;
- uspjeh najboljeg/najgoreg slučaja;
- pojave "uskog grla" (engl. *Bottleneck analysis*[107]).

Zadnja funkcija u alatu za simulaciju podrazumijeva potvrdu mrežnih promjena. IP/MPLSView osigurava sigurno okruženje za testiranje utjecaja promjena nastalih u mreži, prije nego su one zapravo i nastupile. *WANDL* je izradio listu funkcija za simulaciju promjena u mreži [71]:

- provođenje "što-ako" analize (engl. *What-if analysis*[108]);
- mogućnost izmjene topologije mreže (dodaj, obriši, izmijeni);
- izmjena bilo kojeg mrežnog elementa (čvorovi, veze, LSP-ovi);
- promjena protokola usmjeravanja, atributa i mjernih jedinica;
- promjena uzorka opterećenja;
- promjena dizajna.

Što se tiče samog dizajniranja mrežne topologije, dizajn može krenuti iz temelja, pri čemu je potrebno voditi računa o predviđenom prometu, tarifama i podacima o cijenama. Nužno je osigurati da dizajn mreže može izdržati sve razine različitih zahtjeva korisnika (čvorove, poveznice, neuspjehe i sl.).

IP/MPLSView nudi sljedeće funkcije za dizajniranje i modeliranje tehnika upravljanja mrežnim prometom [71]:

- dizajniranje različitih scenarija koji štite od potencijalnih rizika;

[107] Bottleneck analysis – Analiza koja pomaže timu identificirati korake u kojima je protok ograničen, pronaći korijene uzroka tih ograničenja i odgovoriti na osnovne uzroke koji su identificirani.
[108] What-if analysis – Alat koji koristiti nekoliko različitih skupova vrijednosti u jednoj ili više formula kako bi se istražili svi različiti rezultate.

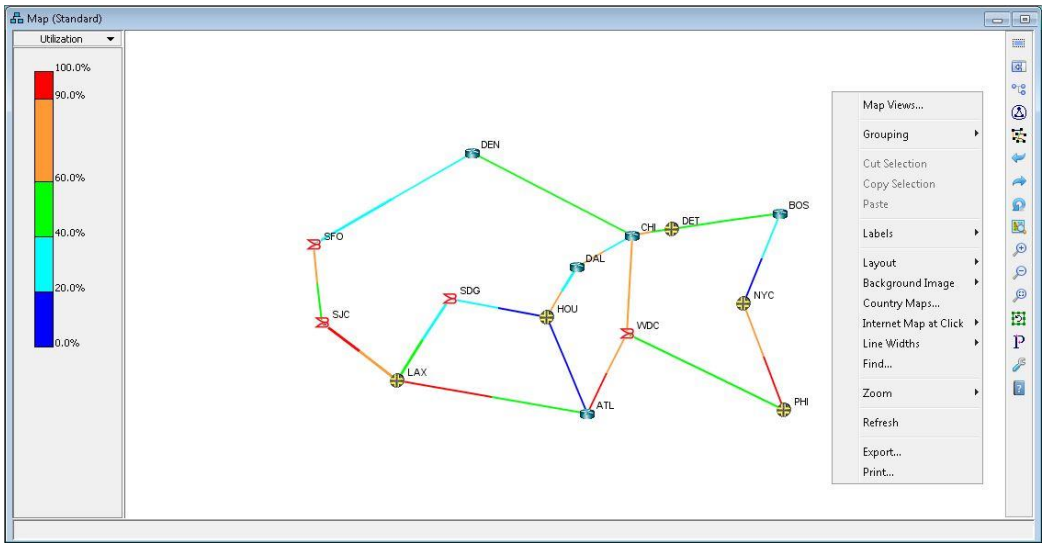
- dizajniranje tunela za brzo preusmjeravanje prometa (engl. *Fast ReRoute* - FRR[109]);
- dizajniranje i simuliranje LSP tunela;
- dizajniranje različitih P2MP-TE stabala za višesmjerno slanje;
- provedbu "*Route Reflector*[110]" dizajna i analize;
- dizajniranje kapaciteta u VoIP mreži;
- modeliranje CoS klasa;
- modeliranje distribucijskih stabala i smjerova za višesmjerno slanje.

IP/MPLSView nudi mogućnost simulacije za mnoge tehnologije i protokole koji se koriste u MPLS mrežama. Na sljedećoj listi se vide tehnologije koje se mogu simulirati unutar IP/MPLSView-a [71]:

- IP jezgra
- MPLS-VPN
- MPLS-TE
- VLAN BGP
- CoS
- Višesmjerno slanje
- Analiza prometnog opterećenja
- IPv6
- VoIP

IP osnovna simulacija provodi se od strane specifičnog modula u IP/MPLSView-u. Taj modul može konstruirati željenu mrežnu topologiju iz konfiguracijskih datoteka uvezenih u IP/MPLSView (Slika 7.3). Modul podržava sljedeće IGP-ove: OSPF, RIP, ISIS, IGRP te EIGRP. Također, podržava i statične smjerove te usmjeravanje bazirano na pravilima. Usmjerivači se mogu modelirati kao logički usmjerivači, a CoS prometni tokovi mogu se modelirati modulom. Mrežna topologija predstavlja se grafikom baziranom na Javi.

[109] FRR - MPLS i IP tehnologija otpornosti koja osigurava brzi oporavak prometa od kvarova veze ili usmjerivača za kritične usluge.
[110] Route Reflector - značajka iBGP-a koja eliminira potrebu za BGP „full-mesh" topologijom.



Slika 7.3. Topologija ilustrirana u IP/MPLSView [72]

Sa gledišta tehnika upravljanja mrežnim prometom, IP/MPLS uključuje značajnu količinu različitih funkcionalnosti. LSP tuneli mogu se uvesti iz već postojećih mreža ili mogu biti dizajnirani od početka. Podaci mogu putovati i u obrnutom smjeru: konfiguracija testirana u simulatoru može se učitati natrag u mrežu koja je označena kao gotova. Prilikom dizajniranja i simuliranja LSP-a za željenu mrežu, IP/MPLSView ima mogućnost dodavanja povratnih tunela za kreiranje LSP-a. Dizajniranje puteva može biti automatizirano kako bi se optimizirao obujam rada. Također, putevi mogu biti redizajnirani za optimizaciju ako su postali neoptimalni tijekom vremena.

IP/MPLSView također sadrži simulacijske/projektantske mogućnosti za većinu tehnika dodanih MPLS funkcijama, kao što su FRR dizajniranje, P2MP-TE stablo za višesmjerno slanje i DiffServ svjesnog TE. Utjecaji dodavanja ili izmjene tunela ili postavki poveznice mogu se pregledavati iz GUI-a baziranog na Javi. [71]

IP/MPLSView nudi podršku za VPN-ove sljedećih tipova [71]:

- Sigurnost prijenosa podataka (engl. *Transport Layer Security* - TLS[111])
- VPN-Draft-Martini[112] (drugi sloj LDP)
- VPN-Draft-Kompella[113] (drugi sloj BGP)
- BGP/MPLS VPN

[111] TLS - Kriptografski protokol koji omogućuje sigurnu komunikaciju putem Interneta za stvari kao što su Internet bankarstvo (preko HTTP protokola), e-mail, Internet fax i ostale načine prijenosa podataka.
[112] Draft-Martini – Draft koji koristi LDP za signalizaciju point to point pseudowire-a kroz MPLS jezgrenu mrežu.
[113] Draft-Kompella - Draft koji koristi BGP za signalizaciju point to point pseudowire-a kroz MPLS jezgrenu mrežu.

- VPLS-LDP
- VPLS-BGP

VPN modul uključuje mogućnosti testiranja i nadgledanja neuspjelih simulacija kako bi se vidjeli efekti istih, provjere integriteta konfiguracijskih datoteka, dijagnostiku VPN-a i praćenje puteva za VPN promet.

IP/MPLSView nudi sljedeće funkcionalnosti za BGP analizu [71]:

- Proračun tablice usmjeravanja;
- Provođenje "*Route Reflector*" analize;
- Uvoz BGP tablica puta;
- Provođenje BGP *peering* analize;
- Provođenje ocjenjivanja IBGP pravila;
- Različiti pogledi na BGP mapu zajedno s BGP susjednim vezama te "*Route Reflector*" hijerarhijom.

Za potrebe CoS-a, DiffServ-TE je postao dio IP/MPLSView alata za dizajniranje. CoS modul unutar IP/MPLSView-a uključuje sljedeće funkcionalnosti [71]:

- CoS modul može modelirati CoS klase, pravila i druge sheme;
- Definicija tokova aplikacije može biti zasnovana na CoS-u;
- Analiza gubitka paketa i statistike kašnjenja mogu se kreirati za svaki CT odvojeno;
- IP/MPLSView podržava mapiranje klasa, pravila, CBWFQ, MDRR te hijerarhijski WRR.

7.2. iVNT

iVNT (engl. *Intelligent Virtual Network Topologies*) je softverski paket rješenja za planiranje, predviđanje i optimizaciju, napravljen od strane Aria Networks-a. iVNT rješenje podijeljeno je na module, pri čemu svaki modul obrađuje određenu vrstu funkcije i vrstu mreže. U nastavku su navedeni moduli i njihovi kratki opisi:

- iVNT MPLS-TE - softver za planiranje i optimizaciju MPLS-TE mreže;
- iVNT Optical - softver za planiranje i optimizaciju multipleksne mreže s valnom duljinom;
- iVNT IP - softver za mrežne operatore i poduzeća koji se korist za planiranje i dizajn njihovih mreža i usluga koristeći IP protokol i MPLS;
- iVNT Ethernet - modul usmjeren na mrežne operatore, koriste se za dizajniranje, planiranje, optimizaciju i upravljanje njihovom mrežom i uslugama

- iVNT Matrix-Maker - modul za mrežne operatere koji kreiraju matrice potražnje prometa;
- iVNT VPN - modul za mrežne operatere koji se koristi za planiranje i modeliranje IP-VPN usluga;
- iVNT TDM - modul za planiranje i optimizaciju SDH/SONET mreža i za migraciju usluga mrežama nove generacije;
- iVNT Server - pruža središnju mrežnu platformu za planiranje, vizualizaciju i dizajniranje mreže;
- Capacity Planner - modul za pružatelje usluga koji im pruža uvid u njihovu potrošnju resursa planiranih usluga;
- iAdapt - okvir za uvoz i izvoz podataka u iVNT - omogućuje integraciju s jednim ili više izvorom podataka (npr. mrežna oprema, proračunske tablice) pomoću iAdapt adaptera;
- iCustomise - okvir za prilagodbu koji omogućuju da iVNT bude prilagođen i konfiguriran kako bi se zadovoljili specifični zadaci planiranja i optimizacije, omogućila automatizacija zadataka koje treba redovito provoditi te podržala mogućnost transformacije i manipulacije podataka;
- iVNT Inside - modul za ugradnju funkcionalnosti proizvoda drugih obitelji u iVNT;
- iVNT Element - modul za ugradnju napredne mogućnosti računanja u IP/MPLS usmjerivačima ili optičkim preklopnicima;
- iForecast - softver za poslovnu analizu i podršku odlučivanju koji osigurava predviđanje mrežne infrastrukture nove generacije, korisničkih usluga te kapitalnih i operativnih troškova.

Od prethodno navedenih modula, izravnu upotrebu u planiranju ili dizajnu MPLS mreže imaju iVNT MPLS-TE i iVNT IP modul. iVNT MPLS-TE nudi rješenja za dizajn, optimizaciju, upravljanje mrežnim kapacitetima i osiguranje usluge. On omogućuje brži početak korištenja i jednostavnije korištenje postojećih izvora planiranja i mrežnih podataka. iVNT MPLS-TE automatizira operativne MPLS procese za brzu, besplatnu isporuku LSP usluga. Osim toga, on se integrira s postojećim sustavima za upravljanje dobavljačima ili OSS izvorima podataka i podržava scenarije planiranja koji analiziraju i najveće MPLS mreže. Ovaj modul korisnicima nudi niz pogodnosti: pojednostavljivanje i kraće cikluse planiranja, učestalije i agilnije planiranje, smanjivanje prekida rada i vremena za vraćanje, vrhunsku uslugu i kvalitetu mreže. [73] Vrlo je važna činjenica da iVNT MPLS-TE podržava linearne, linijske, prstenaste i isprepletene mrežne topologije (ili njihove kombinacije) koje sadrže P, PE ili CE usmjerivače. Prilikom planiranja mreže i LSP-ova, modul može koristiti različite karakteristike i ograničenja: propusnost, kašnjenje,

troškove veze i tarife, analitičke troškove, udaljenost, iskoristivost, afinitete resursa i dr. Nadalje, modul podržava planiranje temeljeno na različitim vrstama troškova, što uključuje planiranje financijskih troškova, kao i troškovno planiranje upravljano metrikom. Troškovi su podijeljeni u tri kategorije prema vrsti troškova: tarifni troškovi, analitički troškovi i troškovi resursa. Također, iVNT MPLS-TE omogućuje analizu pojedinačnih ili višestrukih neuspjelih događaja te analizu kapaciteta. Na kraju, bitno je za napomenuti kako ovaj modul ima podršku za više operacijskih sustava: na Microsoftu podržava Vista, XP i 2003 poslužitelj, na Linux-u podržava Redhat Linux 5 i Debian Linux 5, dok na UNIX-u podržava Sun Solaris 10+. [74]

iVNT IP omogućuje mrežnim operatorima da oblikuju, modeliraju i optimiziraju IP i LDP mreže temeljene na mjerenjima koja se koriste u OSPF, IS-IS i IGP protokolu, kako bi se osiguralo da su prometni tokovi pravilno uravnoteženi preko mreže. IVNT IP modul radi u IGP topologijskoj bazi podataka, koja se uvozi iz informacija topologije mreže. Modul također djeluje i na matrici potražnje prometa koja predstavlja tokove IP prometa ili skup usluga temeljenih na LSP-u, kao što su IP-VPN ili VoIP. iVNT IP omogućuje korisniku da definira objekte za modeliranje, kao npr. scenarij pogreške pri uspostavi veze. iVNT djeluje na matricu prometa, mrežnu topologiju i ciljeve modeliranja kako bi se odredili IGP mjerni podaci koji će optimizirati tokove prometa u željenoj mreži. iVNT IP modul nudi alate za planiranje prometnih zahtjeva i kapaciteta mreže, modeliranje višestrukih troškova, postojećih i budućih mrežnih topologija i usluga, itd. Modul ima značajke za simulaciju i analizu pojedinačnih i višestrukih usmjerivača i veza te za analizu scenarija - simulaciju, analizu i validaciju mreža i promjenu prometa.

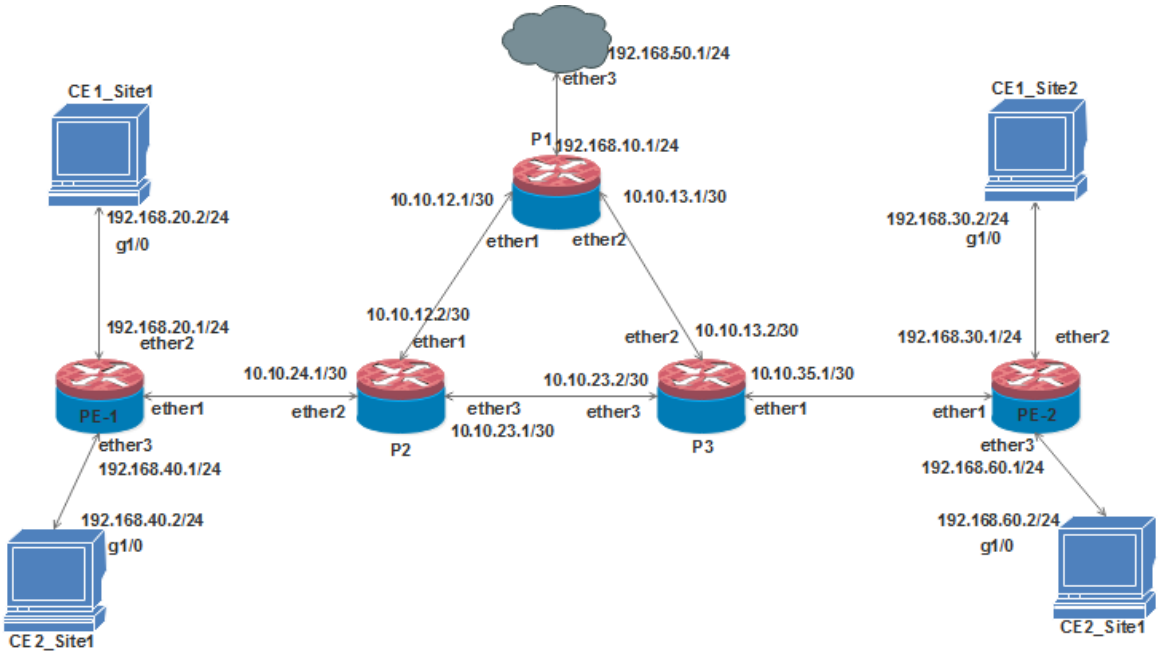
Osnovna tehnologija koju koristi Aria Networks naziva se distribuirana umjetna neuronska inteligencija (engl. *Distributed Artificial Neural Intelligence* - DANI[114]), ona je fleksibilna, stabilna, dokazana, skalabilna i distribuirana računalna platforma. [74]

[114] DANI - Multi-algoritamski softver koji se koristi u planiranju, predviđanju i optimizaciji.

8. KONFIGURACIJA UREĐAJA U TESTNOJ MREŽI

U praktičnom djelu rada povezana je topologija prema Slici 8.1. Korištena topologija sastoji se od četiri računala (*CE1_Site1*, *CE1_Site2*, *CE2_Site1* i *CE2_Site2*) koji su povezani s PE usmjerivačima. Dva PE usmjerivača (*PE-1* i *PE-2*) koriste se za postavljanje i uklanjanje oznake. Tri P usmjerivača (*P1*, *P2* i *P3*) funkcioniraju kao tranzitni usmjerivači i povezani su s PE usmjerivačima.

Korišteno je više računala, pet MikroTik usmjerivača i *patch* kabeli. Načinjene su konfiguracije OSPF-a, MPLS-a i VPLS-a pomoću *Winbox* softvera i prethodno navedene opreme.



Slika 8.1: Mrežna topologija

Model korištenog *MikroTik* usmjerivača je *hAP Lite* (RB941-2nD) (engl. *Home Access Point*) (Slika 8.2.). Ovaj uređaj prilagođen je radu prema standardu 802.11n sa radnom frekvencijom na 2,4 GHz i maksimalnim deklariranim protokom podataka koji iznosi 300 Mbit/s. Od konekcija, sadrži konektor za napajanje u obliku USB porta, jedan WAN i tri LAN porta. Za konfiguriranje uređaja korišten je mali portabilni softver *Winbox*. [75]

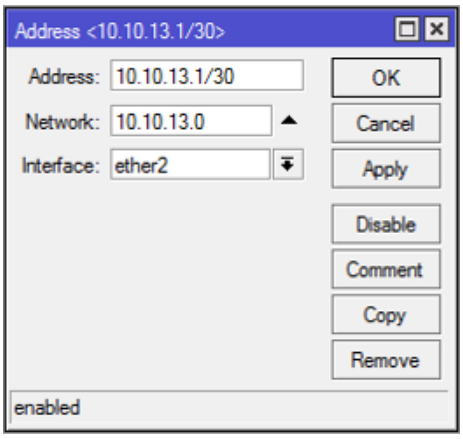
Slika 8.2. Usmjerivač *hAP Lite* (*RB941-2nD*), [76]

Winbox je besplatan administratorski alat s grafičkim sučeljem tvrtke MikroTik, koji se koristi za konfiguriranje, nadzor i upravljanje MikroTik uređajima.

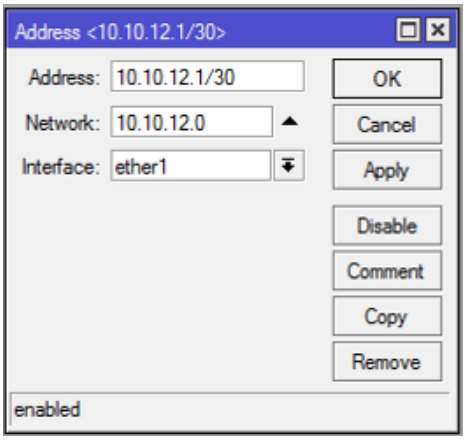
Prije konfiguracije OSPF-a, za svaki MikroTik dodane su adrese njemu povezanih sučelja.

Adrese su dodane na sljedeći način: *IP* ⟶ *Addresses* ⟶ *Address List* ⟶ *Add*

IP adrese aktivnih sučelja usmjerivača MikroTik P1

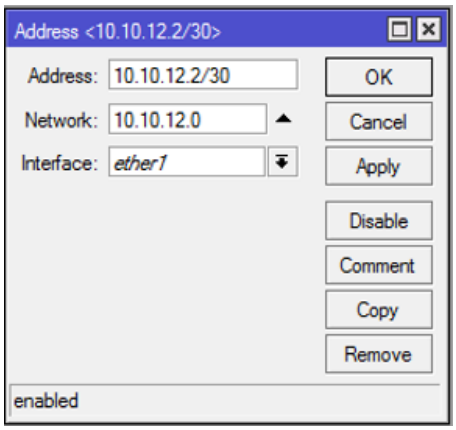


Slika 8.3. Adresa sučelja *ether1*

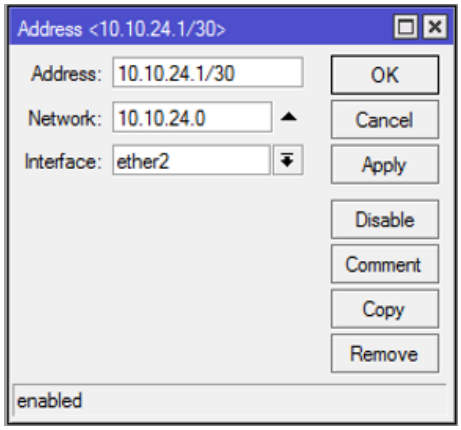


Slika 8.4. Adresa sučelja *ether2*

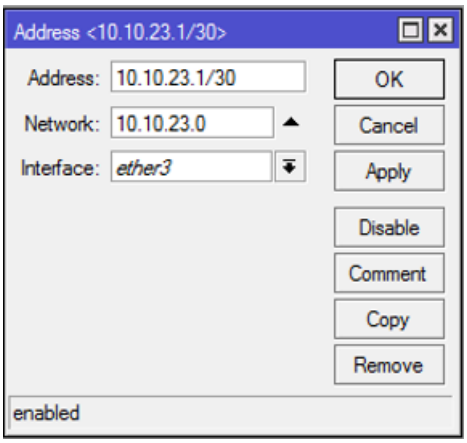
IP adrese aktivnih sučelja usmjerivača MikroTik P2



Slika 8.5. Adresa sučelja *ether1*

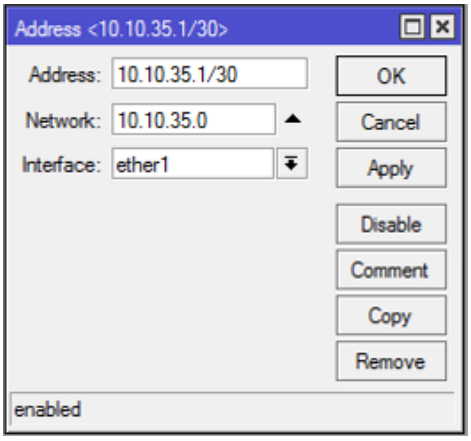


Slika 8.6. Adresa sučelja *ether2*

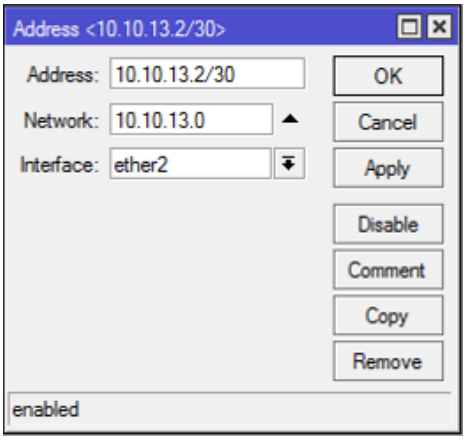


Slika 8.7. Adresa sučelja *ether3*

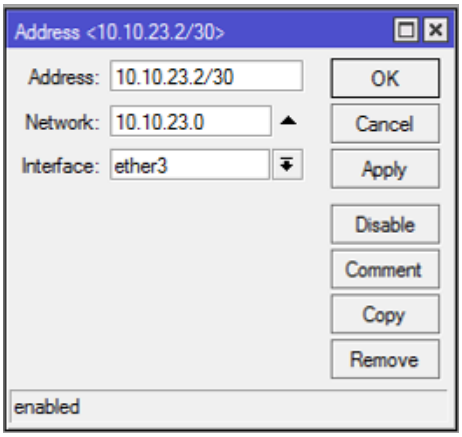
IP adrese aktivnih sučelja usmjerivača MikroTik P3



Slika 8.8. Adresa sučelja *ether1*

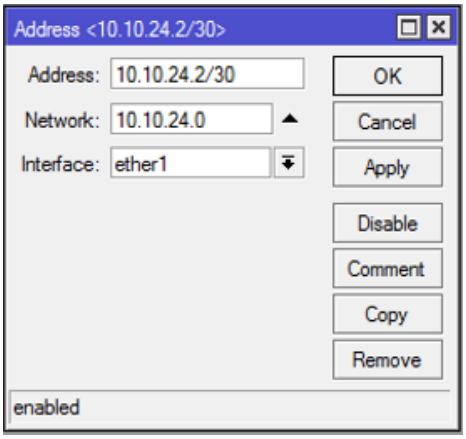


Slika 8.9. Adresa sučelja *ether2*

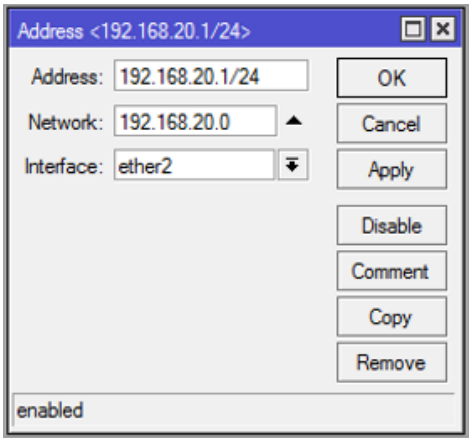


Slika 8.10. Adresa sučelja *ether3*

IP adrese aktivnih sučelja usmjerivača MikroTik PE-1

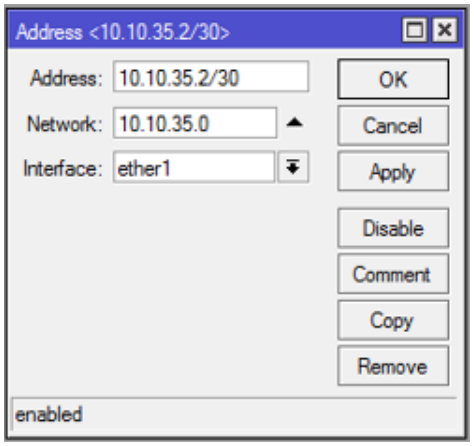


Slika 8.11. Adresa sučelja *ether1*

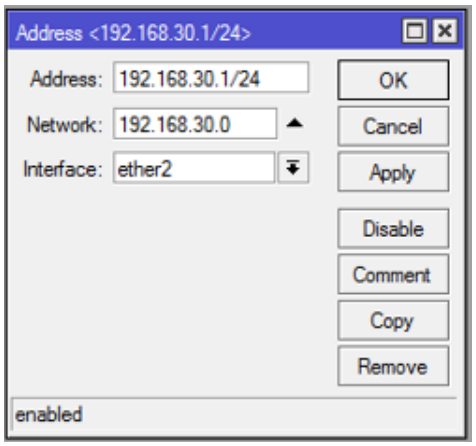


Slika 8.12. Adresa sučelja *ether2*

IP adrese aktivnih sučelja usmjerivača MikroTik PE-2



Slika 8.13. Adrese sučelja *ether1*

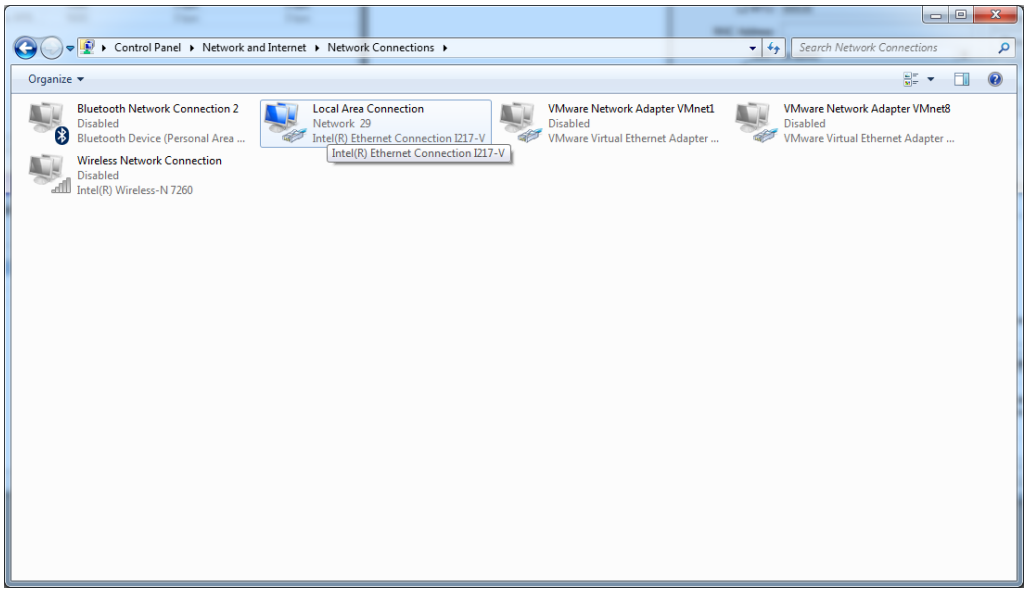


Slika 8.14. Adrese sučelja *ether2*

Nakon postavljanja adresa za svaki MikroTik iz topologije, potrebno je onemogućiti sve mrežne konekcije osim LAN na sljedeći način:

Control Panel → *Network and Sharing Center* → *Change Adapter Settings* → desni klik na sve mrežne adaptere osim LAN → *Disable*

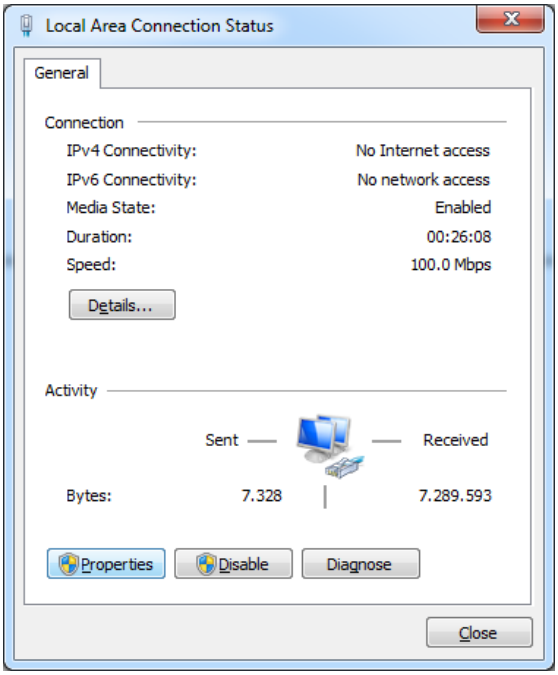
Nakon prethodno navedenog postupka samo LAN ostaje omogućen (Slika 8.15.).



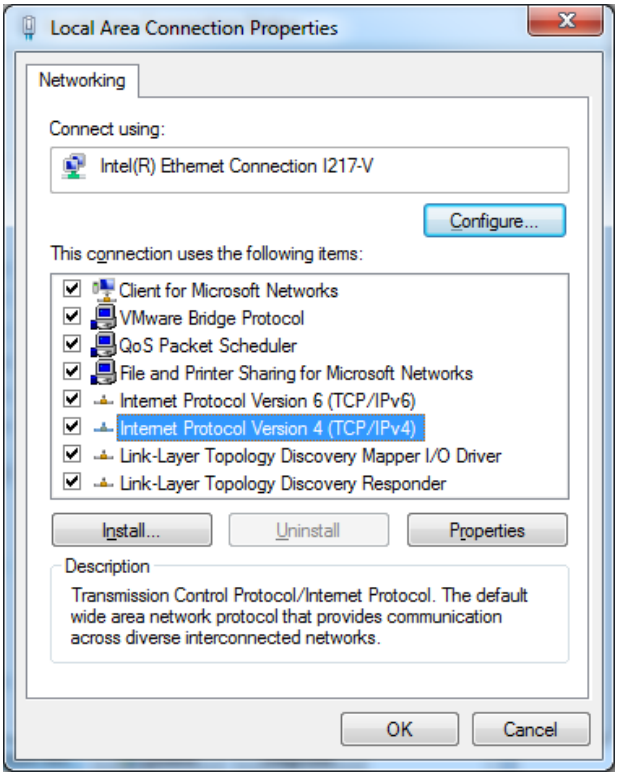
Slika 8.15. Onemogućeni mrežni adapteri

Nakon toga, na računalima CE1_Site1 i CE1_Site2 postavljene su odgovarajuće IP adrese:

Control Panel → *Network and Sharing Center* → *Change Adapter Settings* → *desni klik na Local Area Connection* → *Properties* → *Internet Protocol Version 4 (TCP/IP)* → *Use the following IP address:* → *IP address*: …→ *Default gateway*: …→ *OK* (Slika 8.16. Slika 8.17.).

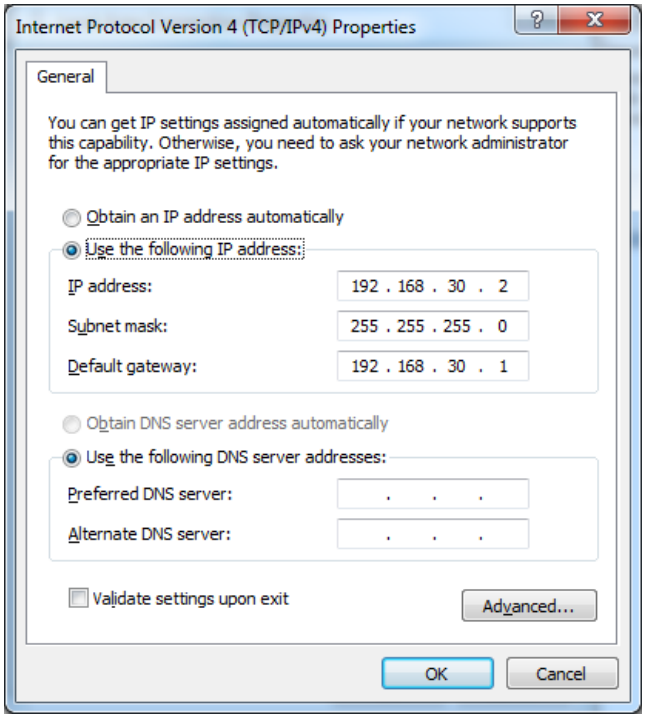


Slika 8.16. Status lokalne veze



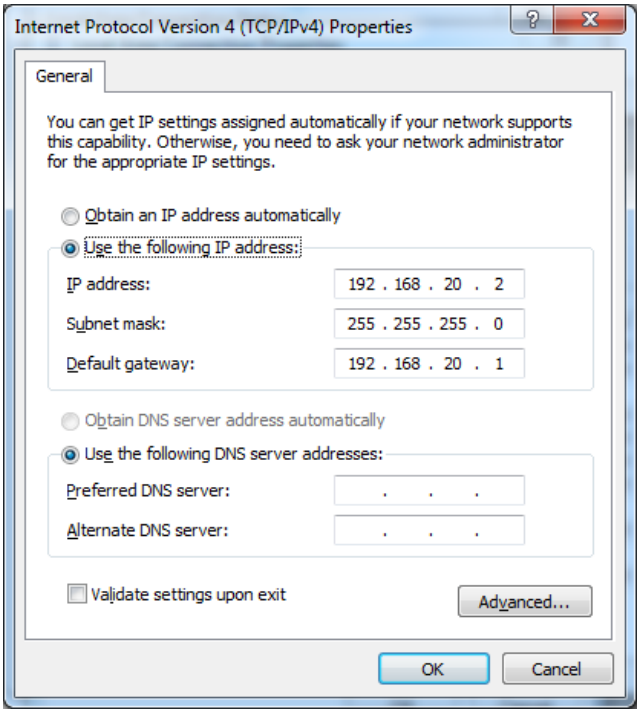
Slika 8.17. Svojstva lokalne mreže

Za računalo *CE1_Site1* postavljene su sljedeće adrese (Slika 8.18.):



Slika 8.18. Adrese računala *CE1_Site1*

Za računalo *CE1_Site2* postavljene su sljedeće adrese (Slika 8.19.):



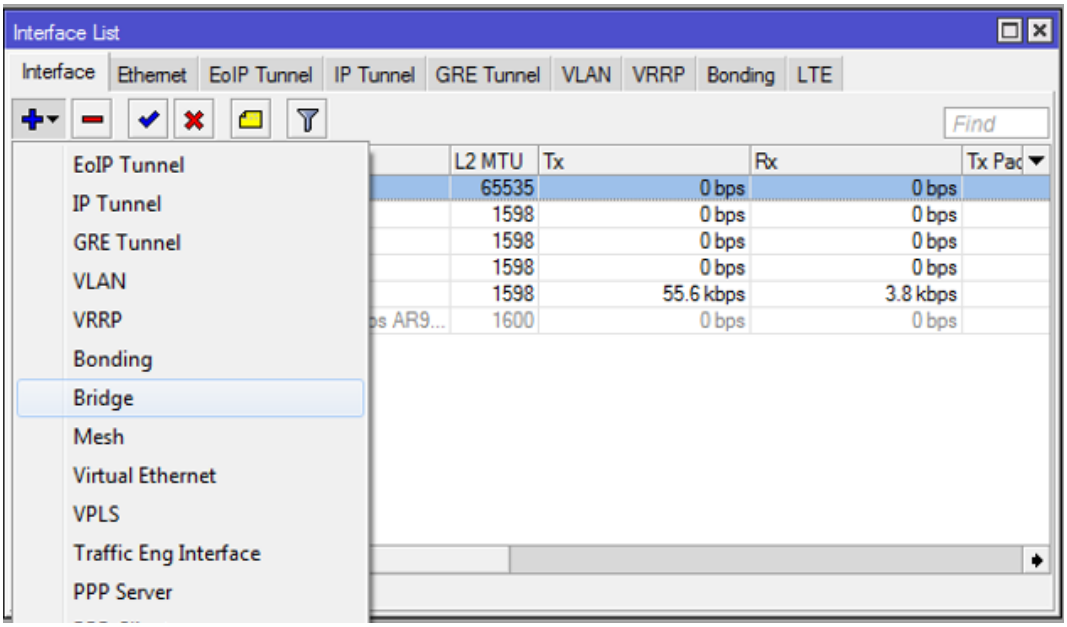
Slika 8.19. Adrese računala *CE1_Site2*

8.1 OSPF postavke na usmjerivačima u kreiranoj mreži

Kako je već prethodno navedeno, OSPF je protokol za usmjeravanje razvijen za IP mreže i zasnovan na SPF algoritmu za pronalaženje najkraćeg puta. OSPF konfiguracija načinjena je na svakom od pet MikroTik-ova.

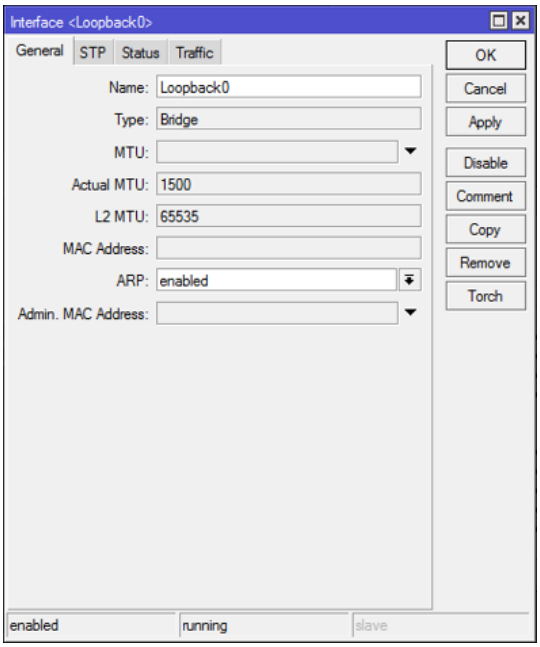
8.1.1. OSPF postavke na usmjerivaču MikroTik P1

U *Winbox* softveru, iz izbornika s lijeve strane odabran je *Interfaces*, pri čemu se otvara *Interface List*. Klikom na *Add* u gornjem lijevom kutu otvara se padajući izbornik u kojem je odabran *Bridge*. Postupak je prikazan na Slici 8.20.



Slika 8.20. Kreiranje *bridge*-a

Bridge je nazvan *Loopback0*. (Slika 8.21.)

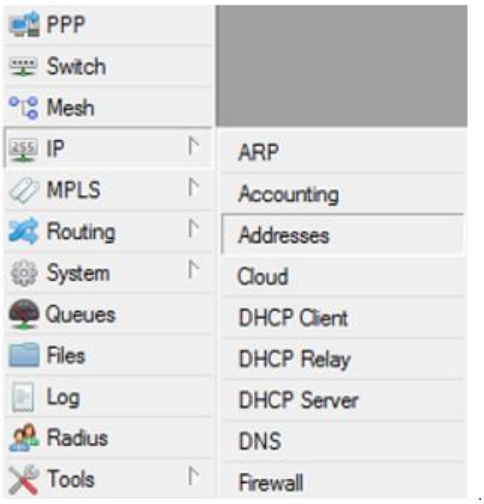


Slika 8.21. Imenovanje mosta

Actual MTU je maksimalna veličina paketa koja se umeće u L2 Ethernet okvir. *L2MTU* označava maksimalnu veličinu okvira bez MAC zaglavlja kojeg ovo sučelje može poslati. [77] ARP protokol

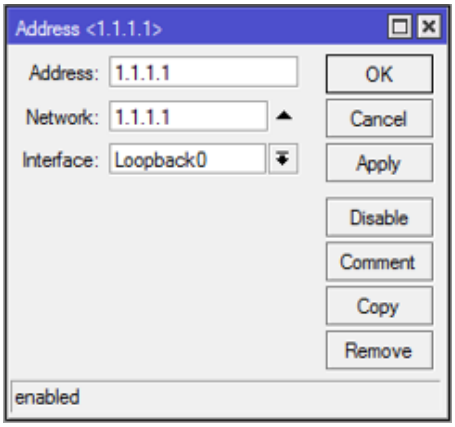
(engl. *Address Resolution Protocol*) je komunikacijski protokol koji se koristi za povezivanje MAC adresa s određenom adresom mrežnog sloja, obično IPv4 adresom. [78]

U sljedećem koraku u glavnom izborniku odabran je *IP*, pri čemu se otvara padajući izbornik u kojem je odabran *Addresses* kako bi se mogla dodati IP adresa prethodno kreiranog *bridge-a* (Slika 8.22.).

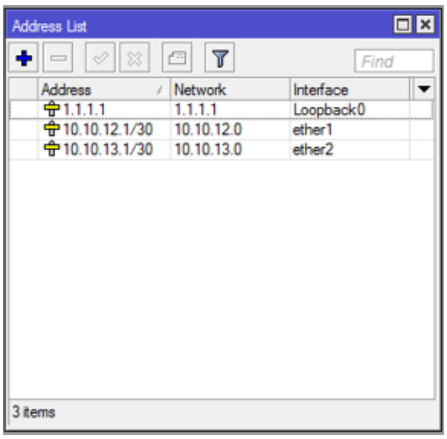


Slika 8.22. Izbornik IP

Klikom na *Addresses* otvoren je prozor *Address List* u kojem je moguće dodati novu IP adresu klikom na *Add* u gornjem lijevom kutu. U polje *Address* upisana je adresa 1.1.1.1, dok je *Interface*: *Loopback0* (Slika 8.23.).

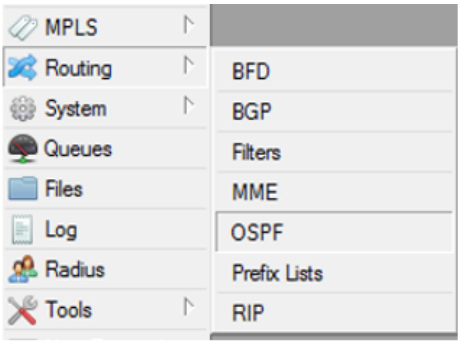


Slika 8.23. Dodavanje IP adrese za *Loopback0*



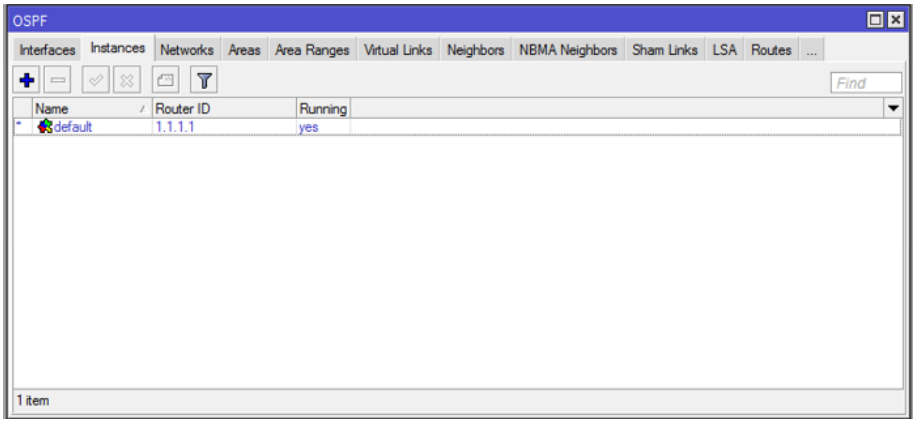
Slika 8.24. Prikaz svih postavljenih adresa

U glavnom izborniku odabran je *Routing*, pri čemu se otvara izbornik u kojem je odabran *OSPF*. (Slika 8.25.)



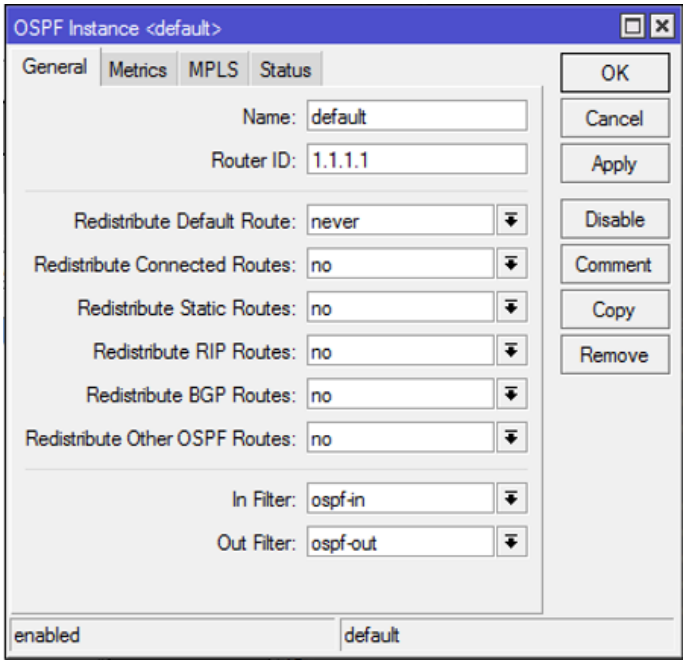
Slika 8.25. *Routing* izbornik

Klikom na *OSPF*, otvara se prozor u kojem je odabran *Instances*. Novu instancu moguće je dodati klikom na *Add* u gornjem lijevom kutu. U našem slučaju, instanca je *default* (Slika 8.26.).



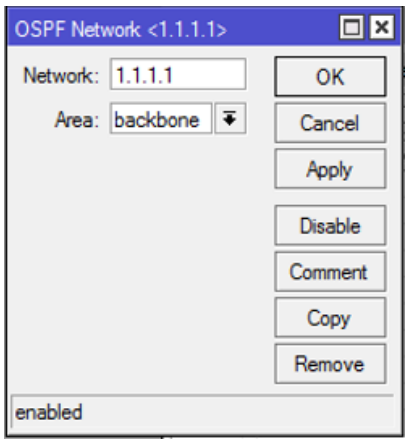
Slika 8.26. Instanca *default*

Instanci *default* dodan je *Router ID*: 1.1.1.1 (Slika 8.27.). *Router ID* je ID OSPF usmjerivača. Ako nije navedeno, OSPF koristi najnižu IP adresu konfiguriranu na aktivnom sučelju.

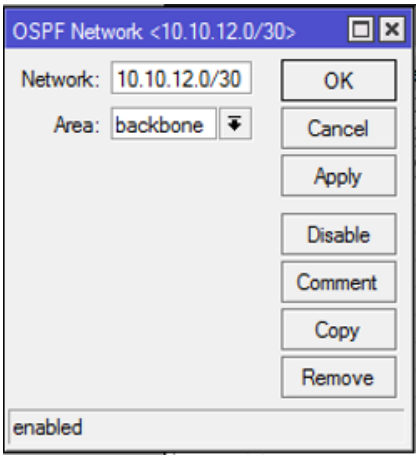


Slika 8.27. Postavljanje *Router ID-a*

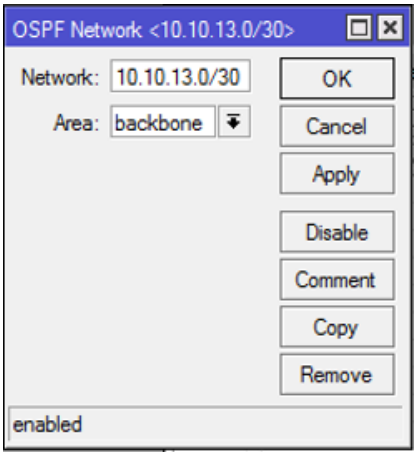
Nakon što je dodana instanca, u prozoru OSPF odabran je *Networks* (Slika 8.31.). Za dodavanje mreže potrebno je kliknuti na *Add* u gornjem lijevom kutu. Prema korištenoj topologiji, dodane su mreže MikroTik-ova koji su povezani na MikroTik *P1*. Za svaku mrežu odabrano je područje (engl. *Area*): *backbone* (Slika 8.28., Slika 8.29., Slika 8.30.). To je OSPF područje koje treba povezati s navedenim rasponom adresa.



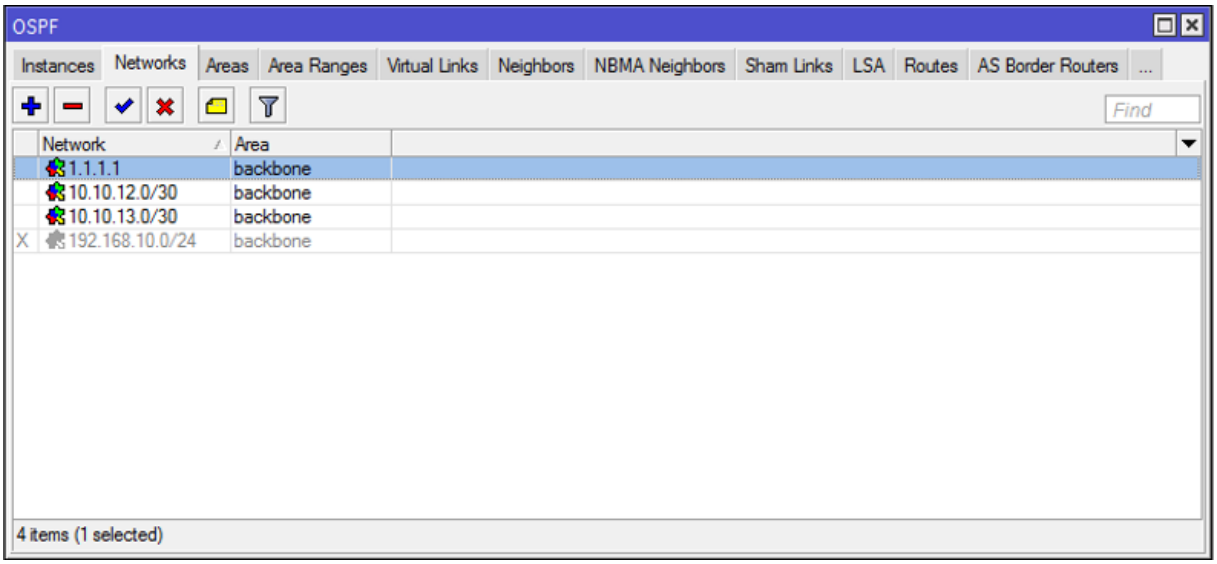
Slika 8.28. Mreža 1.1.1.1



Slika 8.29. Mreža 10.10.12.0/30



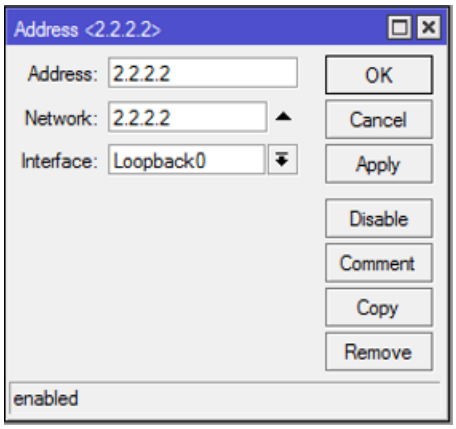
Slika 8.30. Mreža 10.10.13.0/30



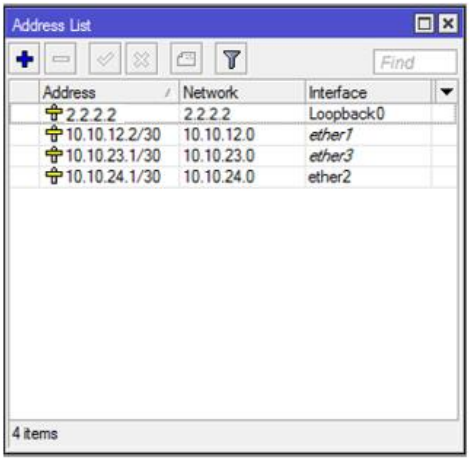
Slika 8.31. Prikaz svih dodanih mreža

8.1.3. OSPF postavke na usmjerivaču MikroTik P2

Na isti način kao i kod P1, kreiran je *bridge* i nazvan je *Loopback0*. Nakon toga, dodana je IP adresa prethodno kreiranog bridge-a. Za adresu je upisano 2.2.2.2 i odabran je *Interface*: *Loopback0* (Slika 8.40.).

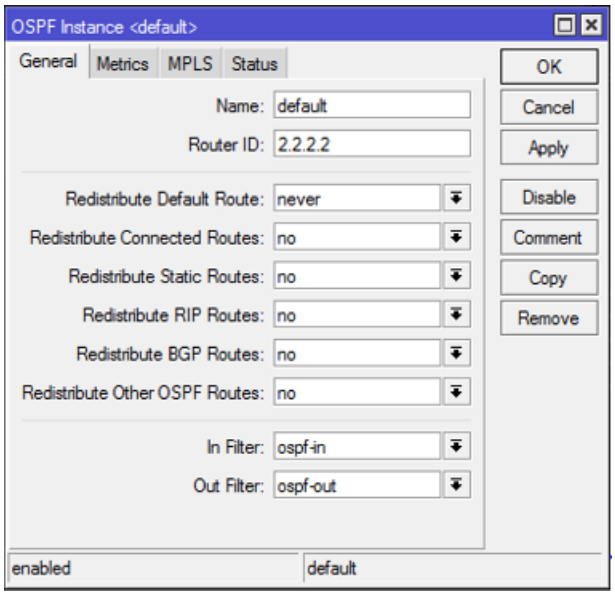


Slika 8.32. Dodavanje IP adrese za *Loopback0*



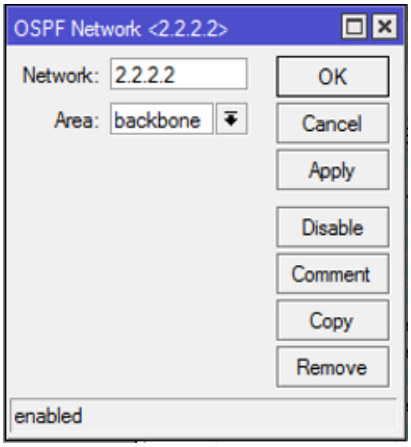
Slika 8.33. Prikaz svih postavljenih adresa

Također, kao u prethodnom primjeru dodana je instanca *default*. Instanci *default* dodan je *Router ID*: 2.2.2.2 (Slika 8.34).

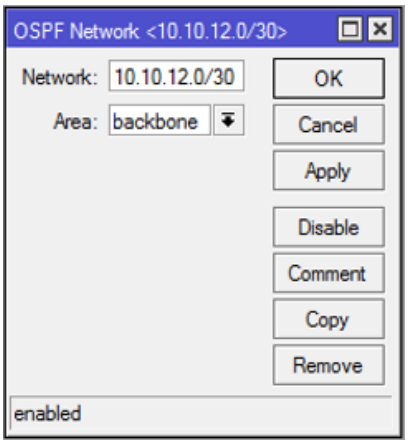


Slika 8.34. Postavljanje *Router ID-a*

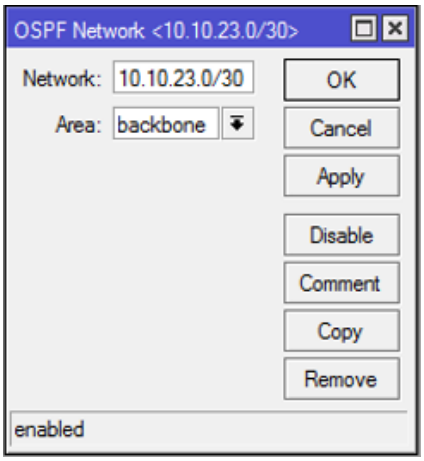
Osim toga, dodane su i mreže MikroTik-ova prema korištenoj topologiji, koji su povezani na MikroTik P2 (Slika 8.39.). Za svaku mrežu odabrano je područje (engl. *Area*): *backbone* (Slika 8.35., Slika 8.36., Slika 8.37., Slika 8.38.).



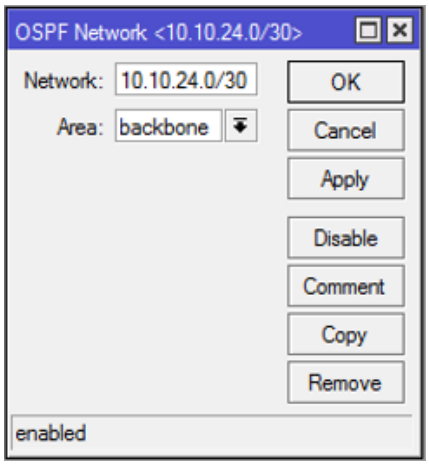
Slika 8.35. Mreža 2.2.2.2



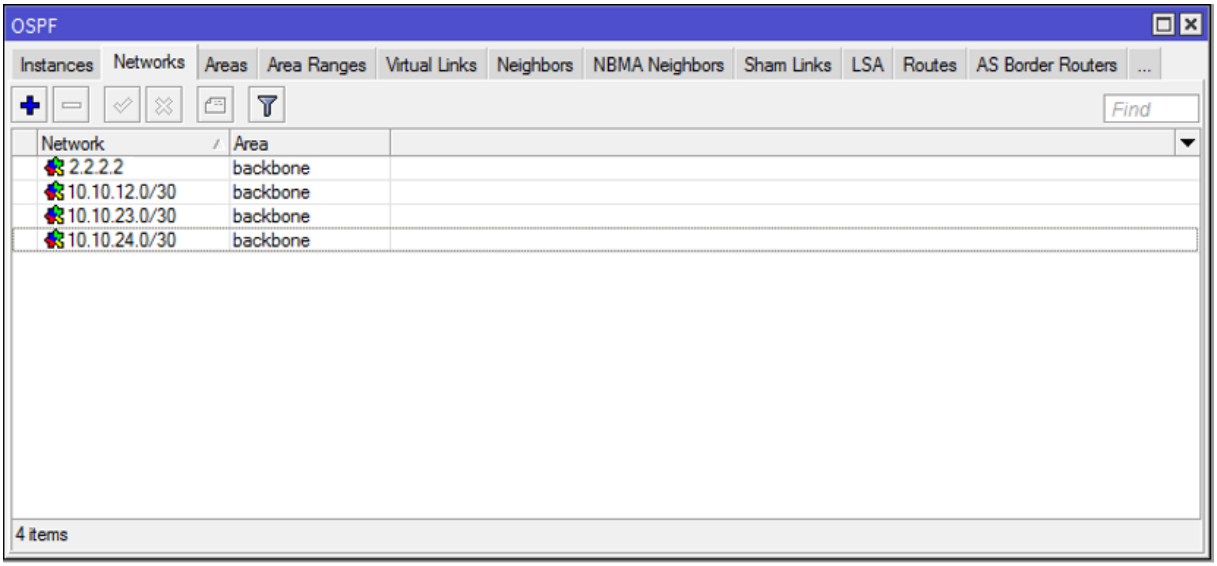
Slika 8.36. Mreža 10.10.12.0/30



Slika 8.37. Mreža 10.10.23.0/30



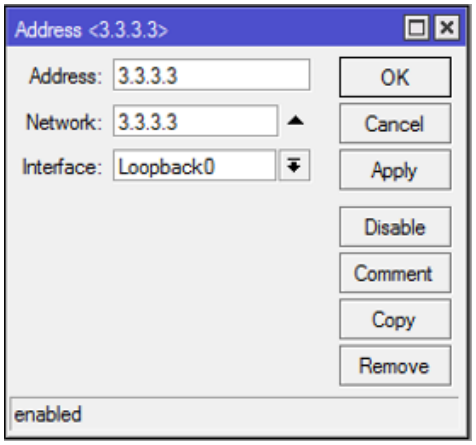
Slika 8.38. Mreža 10.10.24.0/30



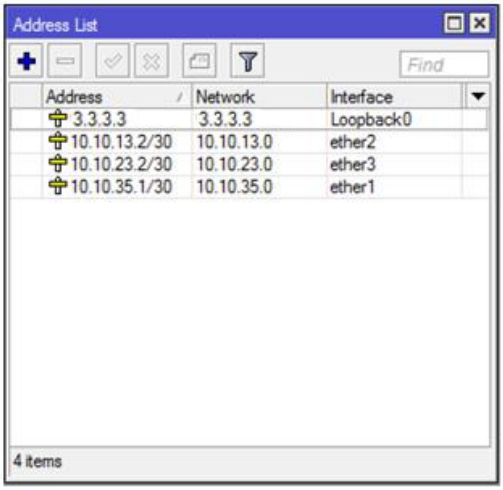
Slika 8.39. Prikaz svih dodanih mreža

8.1.3. OSPF postavke na usmjerivaču MikroTik P3

Na isti način kao i kod prethodna dva MikroTik-a, kreiran je *bridge* i nazvan je *Loopback0*. Nakon toga, dodana je IP adresa prethodno kreiranog *bridge-a*. Za adresu je upisano 3.3.3.3 i odabran je *Interface*: Loopback0 (Slika 8.40.).

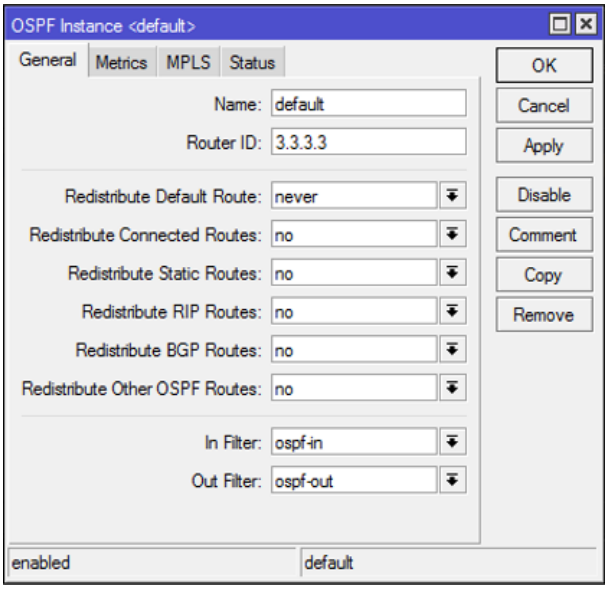


Slika 8.40. Dodavanje IP adrese za *Loopback0*



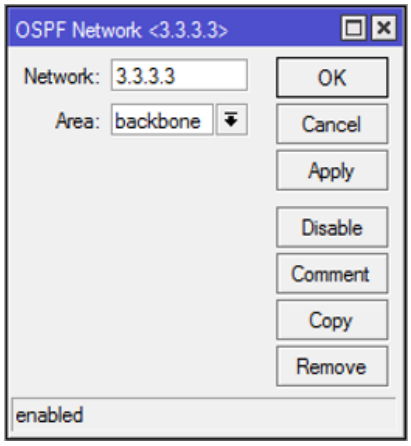
Slika 8.41. Prikaz svih postavljenih adresa

Nakon što je kreiran *bridge* dodana je instanca *default*, na isti način kao i u prethodna dva primjera. Instanci *default* dodan je *Router ID*: 3.3.3.3. (Slika 8.42.).

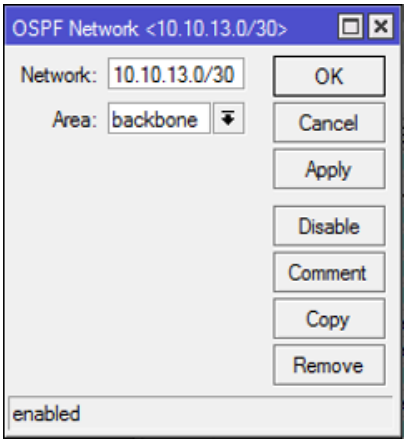


Slika 8.42. Postavljanje *Router ID-a*

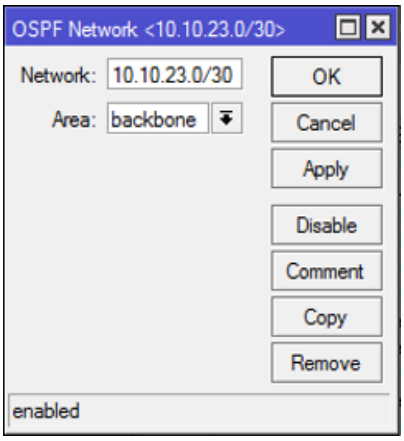
Nakon što je dodana instanca, kreirane su mreže na isti način kao i kod P1 i P2. Prema korištenoj topologiji, dodane su mreže MikroTik-ova koji su povezani na MikroTik P3 (Slika 8.47.). Za svaku mrežu odabrano je područje (engl. Area): *backbone* (Slika 8.43., Slika 8.44., Slika 8.45., Slika 8.46.).



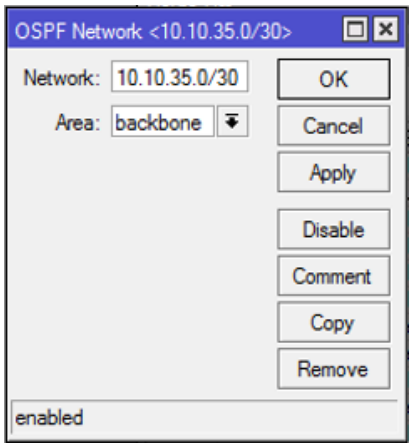
Slika 8.43. Mreža 3.3.3.3



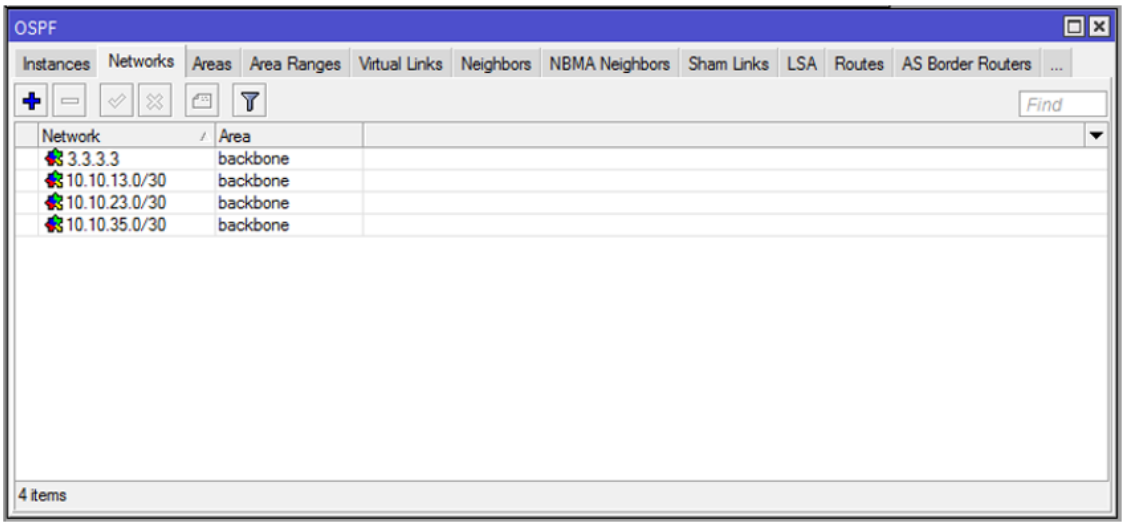
Slika 8.44. Mreža 10.10.13.0/30



Slika 8.45. Mreža 10.10.23.0/30



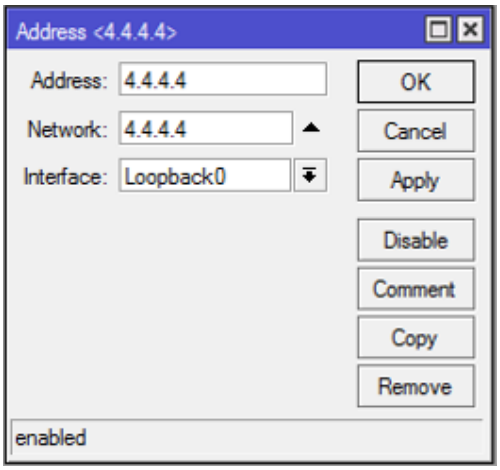
Slika 8.46. Mreža 10.10.12.0/30



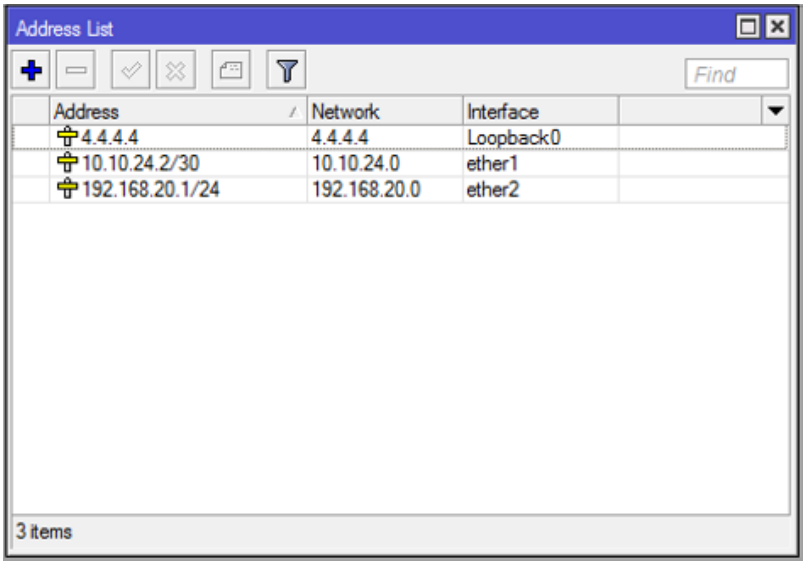
Slika 8.47. Prikaz svih dodanih mreža

8.1.4. OSPF postavke na usmjerivaču MikroTik PE-1

Kao i u prethodnim slučajevima, kreiran je *bridge* koji je nazvan *Loopback0* i kojem je dodana adresa 4.4.4.4 dok je *Interface*: *Loopback0* (Slika 8.48.).

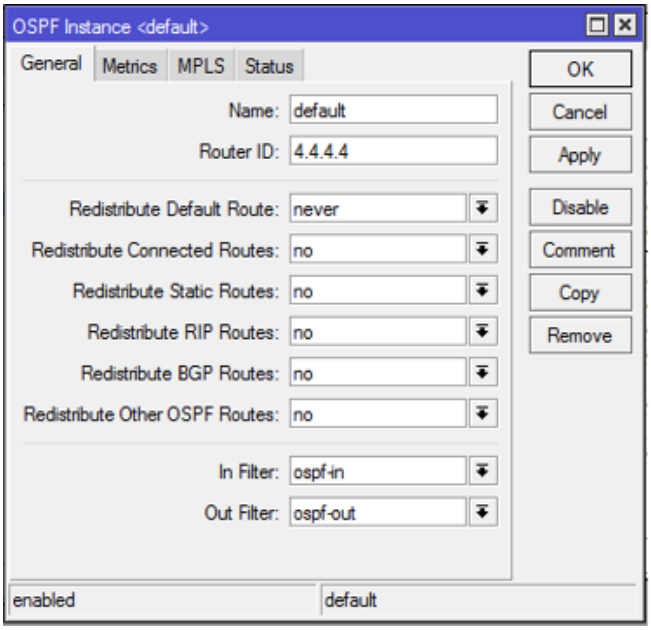


Slika 8.48. Dodavanje IP adrese za *Loopback0*



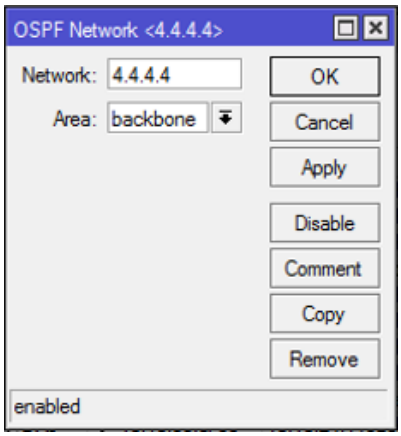
Slika 8.49. Prikaz svih postavljenih adresa

Nakon kreiranja *bridge-a*, dodana je instanca *default*. Instanci *default* dodan je *Router ID*: 4.4.4.4 (Slika 8.50.).

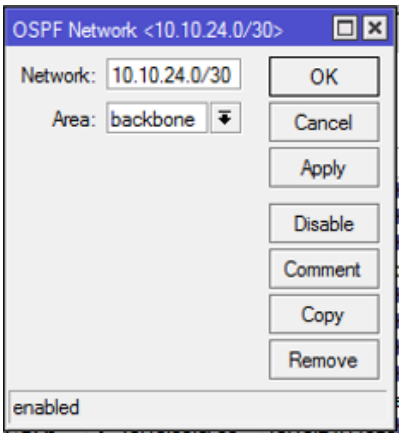


Slika 8.50. Postavljanje *Router ID-a*

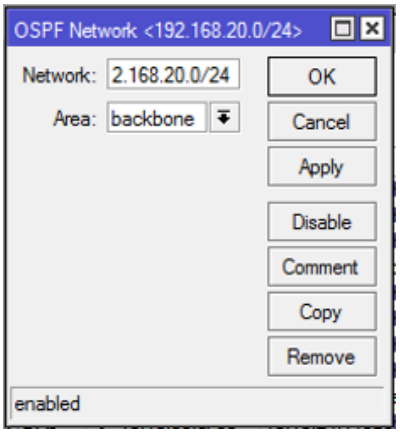
Zatim su dodane mreže MikroTik-ova koji su povezani na MikroTik *PE-1* (Slika 8.54.). Za svaku mrežu odabrano je područje (engl. *Area*): *backbone* (Slika 8.51., Slika 8.52., Slika 8.53.).



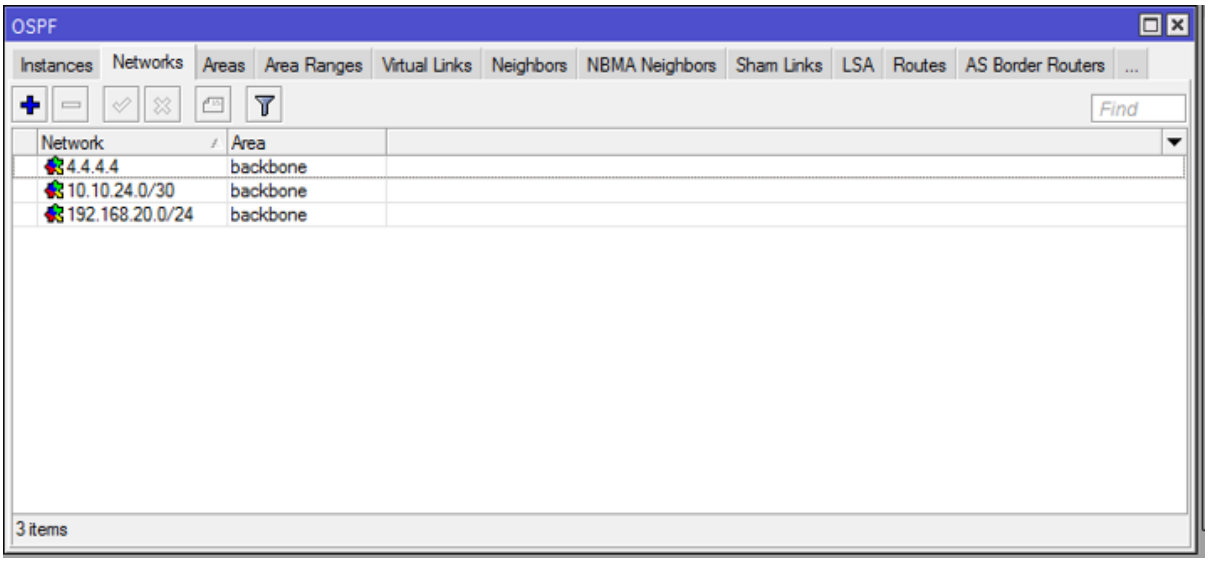
Slika 8.51. Mreža 4.4.4.4



Slika 8.52. Mreža 10.10.24.0/30



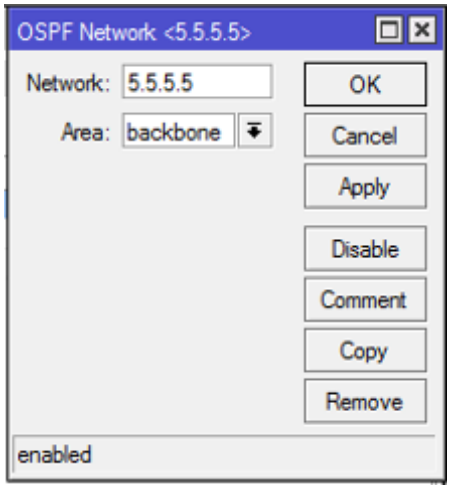
Slika 8.53. Mreža 192.168.20.0/24



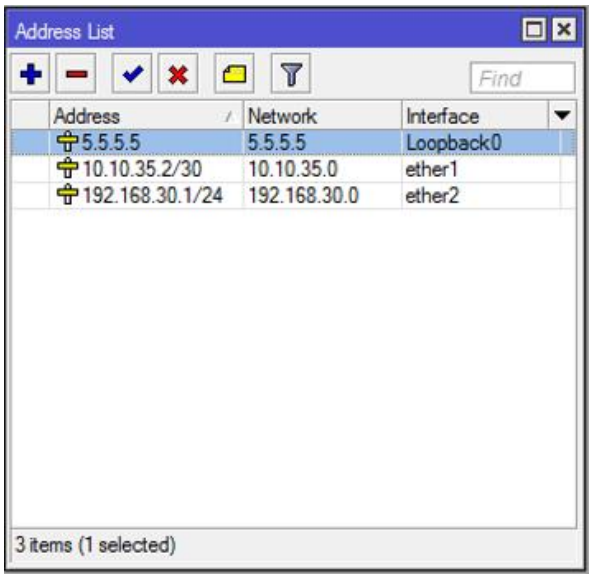
Slika 8.54. Prikaz svih dodanih mreža

8.1.5. OSPF postavke na usmjerivaču MikroTik PE-2

Kao i kod svih prethodnik MikroTik-ova, kreiran je *bridge* koji je nazvan *Loopback0*, dodana mu je IP adresa: 5.5.5.5 i odabran je *Interface*: *Loopback0* (Slika 8.55.).

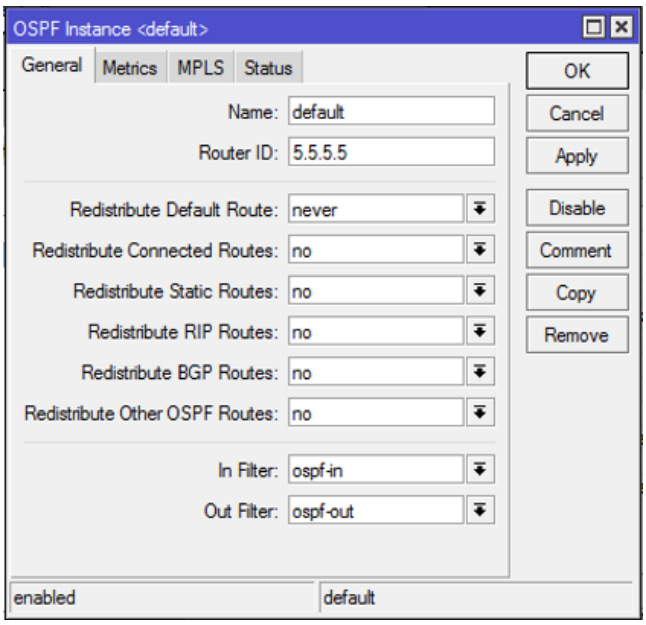


Slika 8.55. Dodavanje IP adrese za *Loopback0*



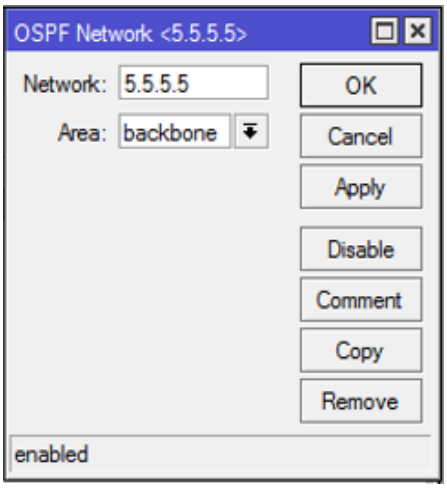
Slika 8.56. Prikaz svih postavljenih adresa

Nakon što je kreiran *bridge*, kao i u prethodnim primjerima dodana je instanca *default*. Instanci *default* dodan je *Router ID*: 5.5.5.5 (Slika 8.57.).

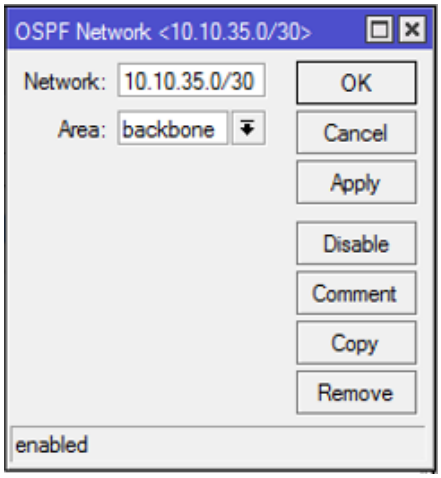


Slika 8.57. Postavljanje *Router ID-a*

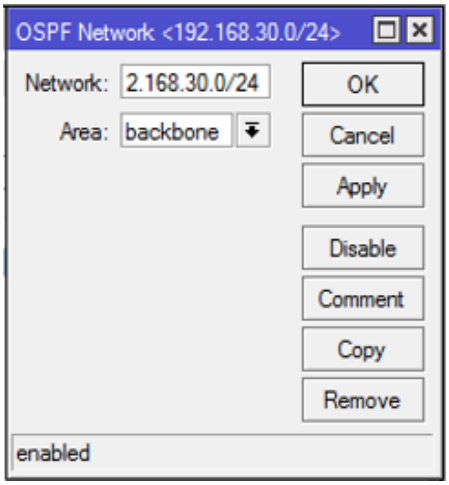
U posljednjem koraku, na isti način kao i u prethodnim slučajevima dodane su mreže MikroTik-ova koji su povezani na MikroTik *PE-2* (Slika 8.61.). Za svaku mrežu odabrano je područje (engl. *Area*): *backbone* (Slika 8.58., Slika 8.59., Slika 8.60.).



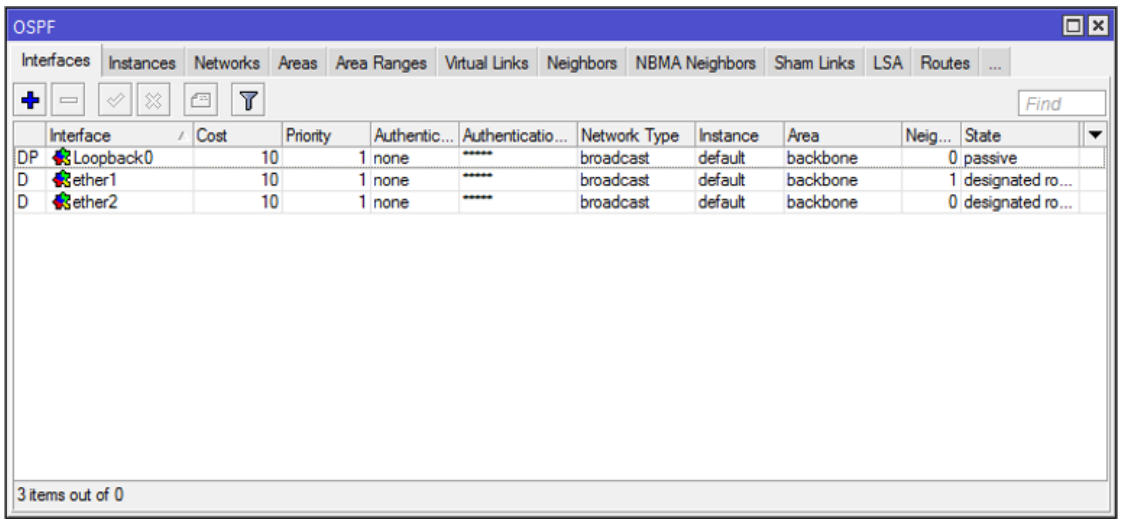
Slika 8.58. Mreža 5.5.5.5



Slika 8.59. Mreža 10.10.35.0/30



Slika 8.60. Mreža 192.168.30.0/24



Slika 8.61. Prikaz svih dodanih mreža

8.2. Testiranje konekcije u kreiranoj testnoj mreži

Nakon što su postavljene IP adrese i konfiguriran OSPF, potrebno je provjeriti postoji li konekcija između računala. Provjera je izvršena između dva računala: *CE1_Site1* i *CE1_Site2*.

Za provjeru je korišten *Command Prompt* na oba računala i unešena *ping* naredba IP adrese svih čvorova iz kreirane topologije. Ping se koristi za mjerenje brzine odziva u mreži. Nakon što primatelj dobije odgovor na *ping* naredbu, moguće je izmjeriti vrijeme koje je bilo potrebno da paket ode do primatelja i vrati se nazad; to vrijeme mjeri se u milisekundama.

Provjera konekcije između računala CE1_Site1 i svih ostalih sučelja u mreži:

```
C:\Users\Korisnik>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=415ms TTL=64
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 415ms, Average = 103ms
```

Slika 8.62. Provjera konekcije prema sučelju s adresom 192.168.20.1

```
C:\Users\Korisnik>ping 10.10.24.2

Pinging 10.10.24.2 with 32 bytes of data:
Reply from 10.10.24.2: bytes=32 time<1ms TTL=64
Reply from 10.10.24.2: bytes=32 time<1ms TTL=64
Reply from 10.10.24.2: bytes=32 time<1ms TTL=64
Reply from 10.10.24.2: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.24.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.63. Provjera konekcije prema sučelju s adresom 10.10.24.2

```
C:\Users\Korisnik>ping 10.10.24.1

Pinging 10.10.24.1 with 32 bytes of data:
Reply from 10.10.24.1: bytes=32 time<1ms TTL=63
Reply from 10.10.24.1: bytes=32 time<1ms TTL=63
Reply from 10.10.24.1: bytes=32 time<1ms TTL=63
Reply from 10.10.24.1: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.24.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.64. Provjera konekcije prema sučelju s adresom 10.10.24.1

```
C:\Users\Korisnik>ping 10.10.12.2

Pinging 10.10.12.2 with 32 bytes of data:
Reply from 10.10.12.2: bytes=32 time<1ms TTL=63
Reply from 10.10.12.2: bytes=32 time<1ms TTL=63
Reply from 10.10.12.2: bytes=32 time<1ms TTL=63
Reply from 10.10.12.2: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.65. Provjera konekcije prema sučelju s adresom 10.10.12.2

```
C:\Users\Korisnik>ping 10.10.23.1

Pinging 10.10.23.1 with 32 bytes of data:
Reply from 10.10.23.1: bytes=32 time<1ms TTL=63
Reply from 10.10.23.1: bytes=32 time<1ms TTL=63
Reply from 10.10.23.1: bytes=32 time<1ms TTL=63
Reply from 10.10.23.1: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.23.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.66. Provjera konekcije prema sučelju s adresom 10.10.23.1

```
C:\Users\Korisnik>ping 10.10.12.1

Pinging 10.10.12.1 with 32 bytes of data:
Reply from 10.10.12.1: bytes=32 time=1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.67. Provjera konekcije prema sučelju s adresom 10.10.12.1

```
C:\Users\Korisnik>ping 10.10.13.1

Pinging 10.10.13.1 with 32 bytes of data:
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.13.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.68. Provjera konekcije prema sučelju s adresom 10.10.13.1

```
C:\Users\Korisnik>ping 10.10.23.2

Pinging 10.10.23.2 with 32 bytes of data:
Reply from 10.10.23.2: bytes=32 time=1ms TTL=62
Reply from 10.10.23.2: bytes=32 time<1ms TTL=62
Reply from 10.10.23.2: bytes=32 time<1ms TTL=62
Reply from 10.10.23.2: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.69. Provjera konekcije prema sučelju s adresom 10.10.23.2

```
C:\Users\Korisnik>ping 10.10.13.2

Pinging 10.10.13.2 with 32 bytes of data:
Reply from 10.10.13.2: bytes=32 time<1ms TTL=62
Reply from 10.10.13.2: bytes=32 time<1ms TTL=62
Reply from 10.10.13.2: bytes=32 time<1ms TTL=62
Reply from 10.10.13.2: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.13.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.70. Provjera konekcije prema sučelju s adresom 10.10.13.2

```
C:\Users\Korisnik>ping 10.10.35.1

Pinging 10.10.35.1 with 32 bytes of data:
Reply from 10.10.35.1: bytes=32 time<1ms TTL=62
Reply from 10.10.35.1: bytes=32 time<1ms TTL=62
Reply from 10.10.35.1: bytes=32 time<1ms TTL=62
Reply from 10.10.35.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.71. Provjera konekcije prema sučelju s adresom 10.10.35.1

```
C:\Users\Korisnik>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time=1ms TTL=61
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.72. Provjera konekcije prema sučelju s adresom 10.10.30.1

```
C:\Users\Korisnik>ping 10.10.35.2

Pinging 10.10.35.2 with 32 bytes of data:
Reply from 10.10.35.2: bytes=32 time=1ms TTL=61
Reply from 10.10.35.2: bytes=32 time<1ms TTL=61
Reply from 10.10.35.2: bytes=32 time<1ms TTL=61
Reply from 10.10.35.2: bytes=32 time<1ms TTL=61

Ping statistics for 10.10.35.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.73. Provjera konekcije prema sučelju s adresom 10.10.35.2

```
C:\Users\Korisnik>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:
Reply from 192.168.30.2: bytes=32 time=1ms TTL=124
Reply from 192.168.30.2: bytes=32 time=1ms TTL=124
Reply from 192.168.30.2: bytes=32 time=1ms TTL=124
Reply from 192.168.30.2: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Slika 8.74. Provjera konekcije prema sučelju s adresom 192.168.30.2

Provjera konekcije između računala CE1_Site2 i svih ostalih sučelja u mreži:

```
C:\Users\Korisnik>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=1ms TTL=61
Reply from 192.168.20.1: bytes=32 time<1ms TTL=61
Reply from 192.168.20.1: bytes=32 time<1ms TTL=61
Reply from 192.168.20.1: bytes=32 time<1ms TTL=61

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.75. Provjera konekcije prema sučelju s adresom 192.168.20.1

```
C:\Users\Korisnik>ping 10.10.24.2

Pinging 10.10.24.2 with 32 bytes of data:
Reply from 10.10.24.2: bytes=32 time<1ms TTL=61
Reply from 10.10.24.2: bytes=32 time<1ms TTL=61
Reply from 10.10.24.2: bytes=32 time<1ms TTL=61
Reply from 10.10.24.2: bytes=32 time<1ms TTL=61

Ping statistics for 10.10.24.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.76. Provjera konekcije prema sučelju s adresom 10.10.24.2

```
C:\Users\Korisnik>ping 10.10.24.1

Pinging 10.10.24.1 with 32 bytes of data:
Reply from 10.10.24.1: bytes=32 time<1ms TTL=62
Reply from 10.10.24.1: bytes=32 time<1ms TTL=62
Reply from 10.10.24.1: bytes=32 time<1ms TTL=62
Reply from 10.10.24.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.24.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.77. Provjera konekcije prema sučelju s adresom 10.10.24.1

```
C:\Users\Korisnik>ping 10.10.12.2

Pinging 10.10.12.2 with 32 bytes of data:
Reply from 10.10.12.2: bytes=32 time<1ms TTL=62
Reply from 10.10.12.2: bytes=32 time<1ms TTL=62
Reply from 10.10.12.2: bytes=32 time<1ms TTL=62
Reply from 10.10.12.2: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.78. Provjera konekcije prema sučelju s adresom 10.10.12.2

```
C:\Users\Korisnik>ping 10.10.23.1

Pinging 10.10.23.1 with 32 bytes of data:
Reply from 10.10.23.1: bytes=32 time=1ms TTL=62
Reply from 10.10.23.1: bytes=32 time<1ms TTL=62
Reply from 10.10.23.1: bytes=32 time<1ms TTL=62
Reply from 10.10.23.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.23.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.79. Provjera konekcije prema sučelju s adresom 10.10.23.1

```
C:\Users\Korisnik>ping 10.10.12.1

Pinging 10.10.12.1 with 32 bytes of data:
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62
Reply from 10.10.12.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.80. Provjera konekcije prema sučelju s adresom 10.10.12.1

```
C:\Users\Korisnik>ping 10.10.13.1

Pinging 10.10.13.1 with 32 bytes of data:
Reply from 10.10.13.1: bytes=32 time=1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62
Reply from 10.10.13.1: bytes=32 time<1ms TTL=62

Ping statistics for 10.10.13.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.81. Provjera konekcije prema sučelju s adresom 10.10.13.1

```
C:\Users\Korisnik>ping 10.10.23.2

Pinging 10.10.23.2 with 32 bytes of data:
Reply from 10.10.23.2: bytes=32 time<1ms TTL=63
Reply from 10.10.23.2: bytes=32 time<1ms TTL=63
Reply from 10.10.23.2: bytes=32 time<1ms TTL=63
Reply from 10.10.23.2: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.82. Provjera konekcije prema sučelju s adresom 10.10.23.2

```
C:\Users\Korisnik>ping 10.10.13.2

Pinging 10.10.13.2 with 32 bytes of data:
Reply from 10.10.13.2: bytes=32 time<1ms TTL=63
Reply from 10.10.13.2: bytes=32 time<1ms TTL=63
Reply from 10.10.13.2: bytes=32 time<1ms TTL=63
Reply from 10.10.13.2: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.13.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.83. Provjera konekcije prema sučelju s adresom 10.10.13.2

```
C:\Users\Korisnik>ping 10.10.35.1

Pinging 10.10.35.1 with 32 bytes of data:
Reply from 10.10.35.1: bytes=32 time=1ms TTL=63
Reply from 10.10.35.1: bytes=32 time<1ms TTL=63
Reply from 10.10.35.1: bytes=32 time<1ms TTL=63
Reply from 10.10.35.1: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 8.84. Provjera konekcije prema sučelju s adresom 10.10.35.1

```
C:\Users\Korisnik>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time<1ms TTL=64
Reply from 192.168.30.1: bytes=32 time<1ms TTL=64
Reply from 192.168.30.1: bytes=32 time<1ms TTL=64
Reply from 192.168.30.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.85. Provjera konekcije prema sučelju s adresom 192.168.30.1

```
C:\Users\Korisnik>ping 10.10.35.2

Pinging 10.10.35.2 with 32 bytes of data:
Reply from 10.10.35.2: bytes=32 time<1ms TTL=64
Reply from 10.10.35.2: bytes=32 time<1ms TTL=64
Reply from 10.10.35.2: bytes=32 time<1ms TTL=64
Reply from 10.10.35.2: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.35.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Slika 8.86. Provjera konekcije prema sučelju s adresom 10.10.35.2

```
C:\Users\Korisnik>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=1ms TTL=124
Reply from 192.168.20.2: bytes=32 time=1ms TTL=124
Reply from 192.168.20.2: bytes=32 time=1ms TTL=124
Reply from 192.168.20.2: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Slika 8.87. Provjera konekcije prema sučelju s adresom 192.168.20.2

Kao što se može vidjeti na prethodnim slikama, dobiveni su rezultati *ping* naredbe. Najvažnija informacija pokazuje koliko vremena je potrebno paketu da prođe zadani put. To vrijeme ovisi o više faktora. Naredba *ping* daje i statistiku: broj poslanih i primljenih paketa, broj izgubljenih paketa, najkraće, najduže i srednje vrijeme trajanja ping-a. Osim toga, *ping* za svako mjerenje vraća i podatak *bytes* koji pokazuje kolika je dužina ping paketa, te podatak o vremenu života (engl. *Time to Live* - *TTL*). TTL je brojač. Kada se paket pošalje, vrijednost TTL postavlja se na 255, a svaki prolazak kroz neki od mrežnih uređaja smanjuje tu vrijednost za jedan. Ukoliko se dogodi da vrijednost TTL-a postane nula, prekida se prosljeđivanje paketa, jer se smatra da je paket prošao preko previše uređaja, što predstavlja zaštitu od mrtvih petlji.

Naredba *tracert* pokazuje kroz koji je paket prošao do odredišta. Na taj način moguće je utvrditi točno mjesto na kojem se javlja problem. U načinjenom primjeru, poslan je *tracert* prema računalu čija je IP adresa 192.168.20.2 (Slika 8.88.). Dobivena je optimalna ruta kojom putuju paketi od računala *CE1_Site2* do računala čija je adresa 192.168.20.2. Dakle, paket od jednog računala do drugog stiže tako što usput prođe kroz pet čvorova. Prvi stupac daje informacije o broju koraka; važno je napomenuti da *tracert* ne radi više od 30 koraka. Drugi, treći i četvrti stupac prikazuju vrijeme odziva u milisekundama od računala čije su adrese navedene u posljednjem stupcu. Ukoliko je poznata struktura mreže, upotrebom naredbe *tracert* može se lako utvrditi postoji li prekid ili veliko usporenje. [79]

```
C:\Users\Korisnik>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\Korisnik>tracert 192.168.20.2

Tracing route to 192.168.20.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.30.1
  2    <1 ms    <1 ms    <1 ms  10.10.35.1
  3    <1 ms    <1 ms    <1 ms  10.10.23.1
  4    <1 ms    <1 ms    <1 ms  10.10.24.2
  5     1 ms     1 ms     1 ms  192.168.20.2

Trace complete.
```

Slika 8.88. Tracert adrese 192.168.20.2

8.3. Povezivanje lokalne računalne mreže na Internet

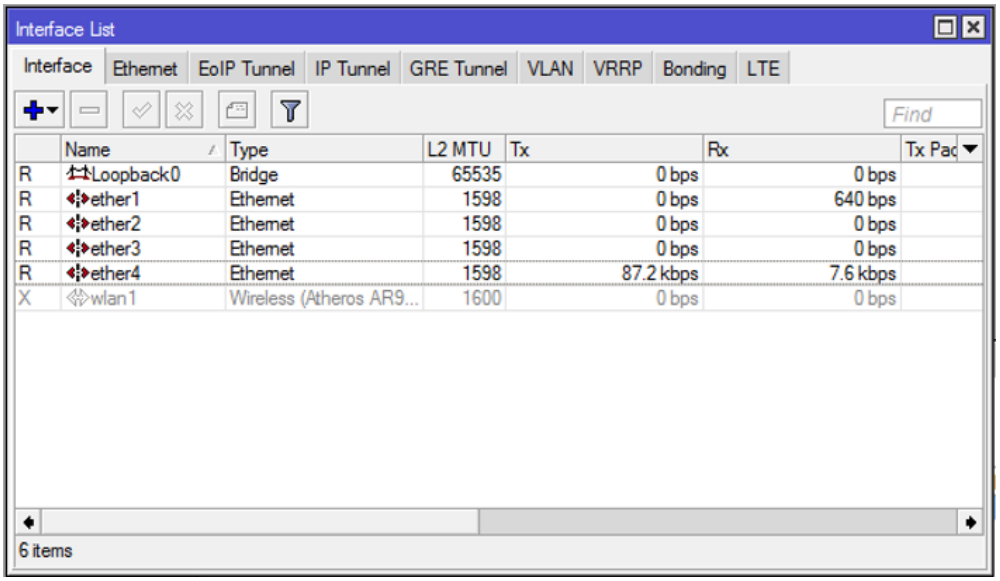
Kako bi bio omogućen pristup Internetu, sučelje ether3 Mikrotik-a *P1* povezano je pomoću *patch* kabela direktno s računalom. Kako bi usmjeravanje paketa bilo pravilno, svako od aktivnih sučelja na uređajima povezanima u mrežu mora imati dodijeljenu IP adresu. Dodijeljene IP adrese unutar Internet mreže moraju biti jedinstvene i jednoznačne, inače uređaji s dupliciranim adresama ne bi ispravno funkcionirali pri spajanju na Internet.

U svrhu povezivanja lokalnih mreža s Internetom potrebno je koristi postupak koji se naziva prevođenje mrežnih adresa (eng. *Network Address Translation* - NAT). Postupak prevođenja mrežnih adresa najčešće se provodi na rubnim usmjerivačima lokalnih mreža koji lokalnu mrežu povezuju na javnu mrežu (Internet).

Postupak prevođenja mrežnih adresa definira se kao zamjena izvorišne i odredišne IP adrese paketa koji prolazi kroz rubni usmjerivač. NAT usmjerivač smješten je u lokalnoj mreži i služi toj mreži kao zadani prospojnik. Javna mreža (Internet) prepoznaje aktivno sučelje usmjerivača definirano kao klijentsko sučelje protokola za dinamičko konfiguriranje računala (engl. *Dynamic Host Configuration Protocol* - DHCP) klijentsko sučelje, na kojem se izvršava postupak maskiranja (eng. *masquerade*) – postupak prevođenja IP adresa iz lokalnih u javne i obrnuto.

Na slici 8.117. su prikazana sva definirana sučelja koja bi se trebala nalaziti u ispisu unutar izbornika *Interfaces* na usmjerivaču *P1*.

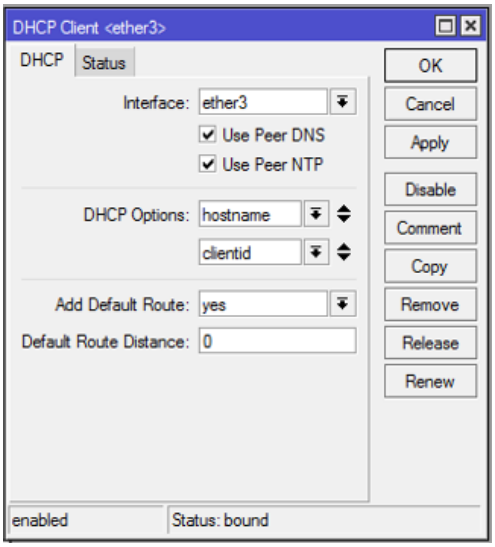
8.3.1. Konfiguriranje rubnog usmjerivača za pristup Internetu



Slika 8.117. Prikaz aktivnih sučelja usmjerivača

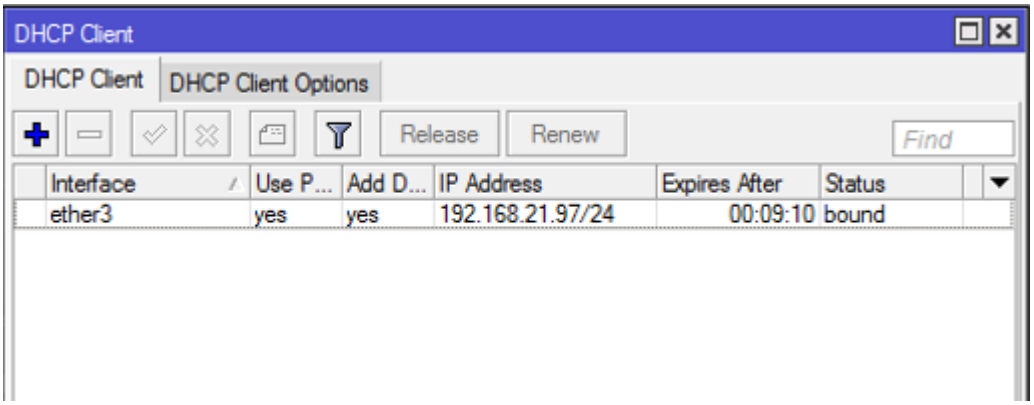
Iz izbornika *IP*→ *DHCP*→*DHCP Client* odabrana je opcija *Add* za definiranje klijentskog sučelje

U otvorenom prozoru (Slika 8.118.) pod opcijom *Interface* odabrano je *Ethernet3* sučelje.



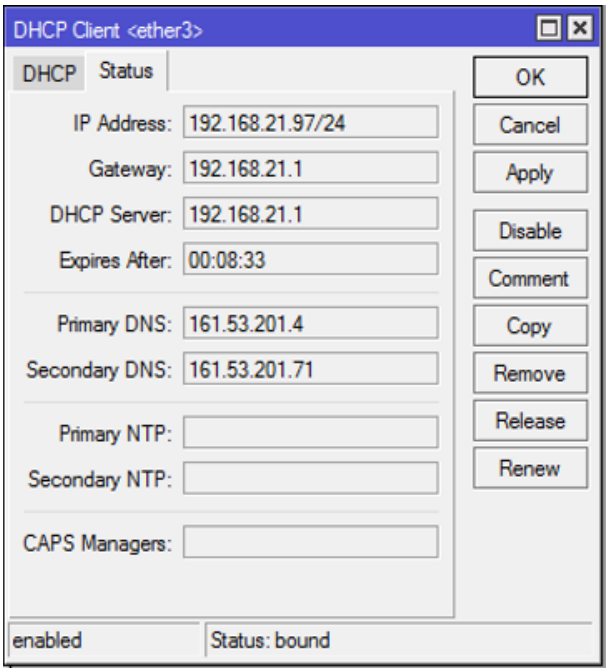
Slika 8.118. Izbornik za definiranje DHCP klijenta

Nakon definiranja DHCP klijenta, vidljiva je IP adresa dodijeljena DHCP klijentu – sučelju *ether3* na usmjerivaču *P1* (Slika 8.119.).



Slika 8.119. Izbornik s popisom definiranih DHCP klijenata

Na slici 8.120. vidljive su dodijeljene adrese i oznake.



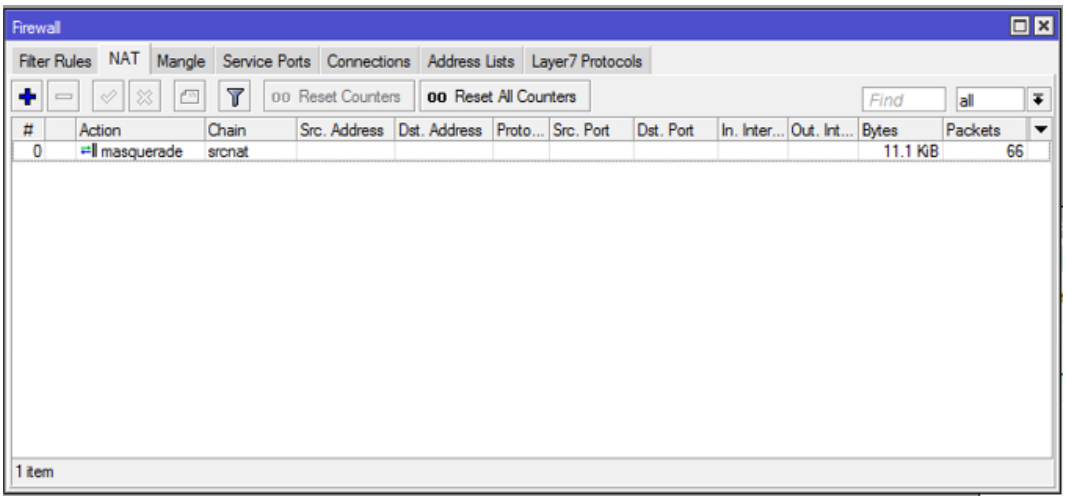
Slika 8.120. Automatski dodijeljene javne adrese na sučelju *ether3* MikroTik-a *P1*

Nakon prethodno opisanog postupka, adresa ether3 sučelja vidljiva je i unutar izbornika *IP* → *Adresses* → *Add.*

Također, u izborniku *IP* → *Routes* vidljiva je i nova ruta, ruta prema Internetu.

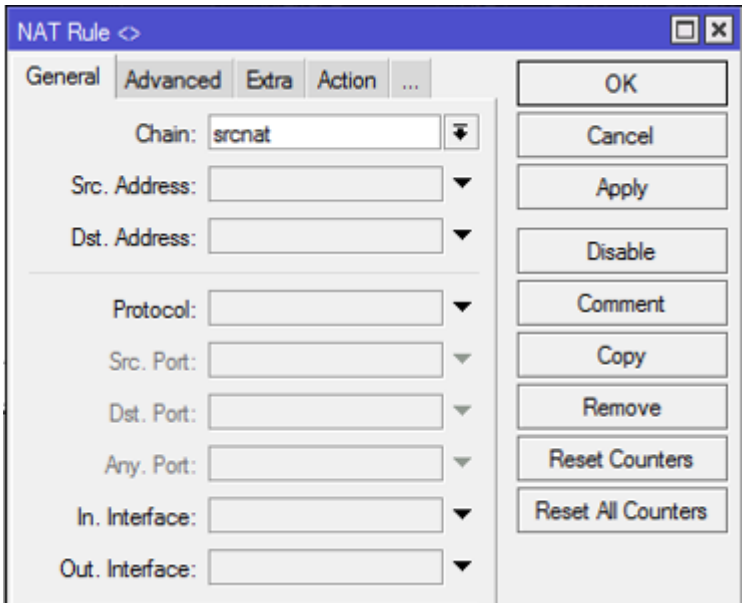
8.3.2. Prevođenje lokalnih IP adresa u javne

Za prevođenje IP adresa iz lokalnih u javne (NAT) pokrenut je postupak maskiranja (*masquerade*) IP adresa (Slika 8.121.). U izborniku *IP* → *Firewall* odabran je tab *NAT* i pomoću opcije *Add* dodano je novo pravilo.



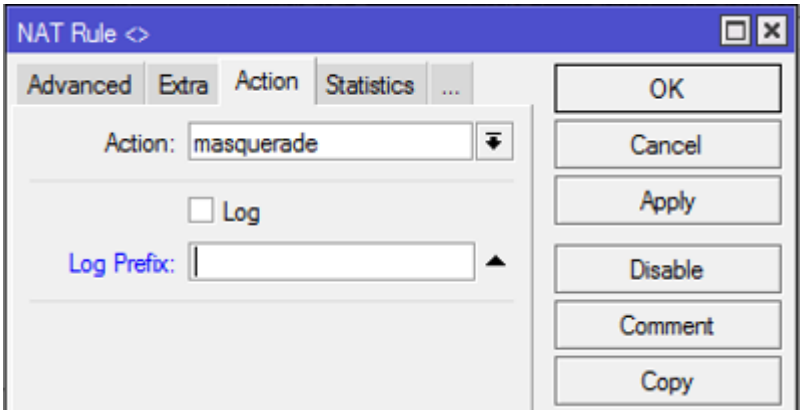
Slika 8.121. Izbornik NAT

Unutar taba *General* postavljen je *Chain* na *srcnat* (Slika 8.122.).



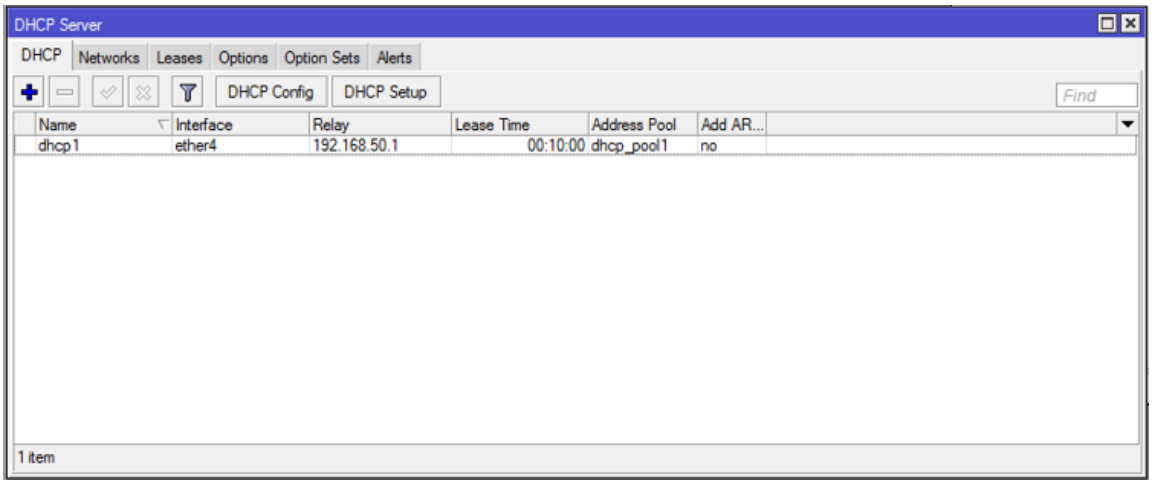
Slika 8.122. Definiranje pravila za prevođenje IP adresa

U sljedećem koraku unutar taba *Action* odabrana je opcija *masquerade* (Slika 8.123.), čime započinje postupak prevođenja IP adresa na MikroTik-u P1.



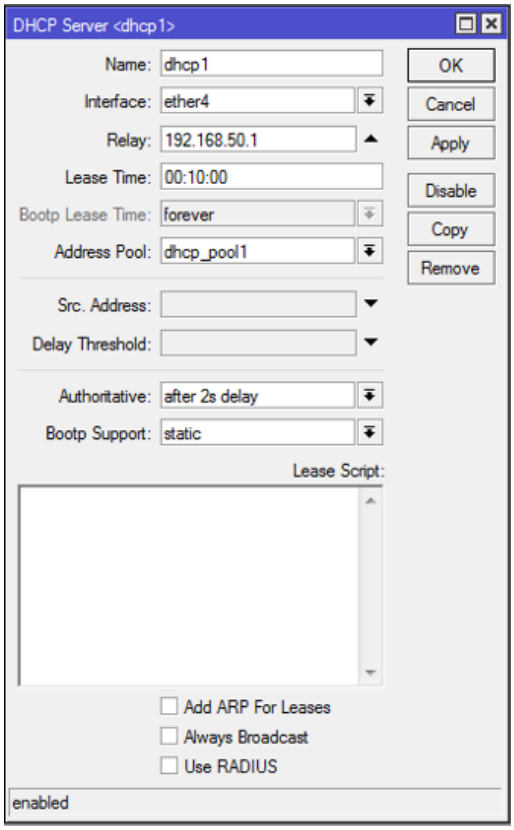
Slika 8.123. Izbor opcije za maskiranje IP adresa

U prozoru *DHCP Server* prikazani su svi dodani serveri (Slika 8.124.).



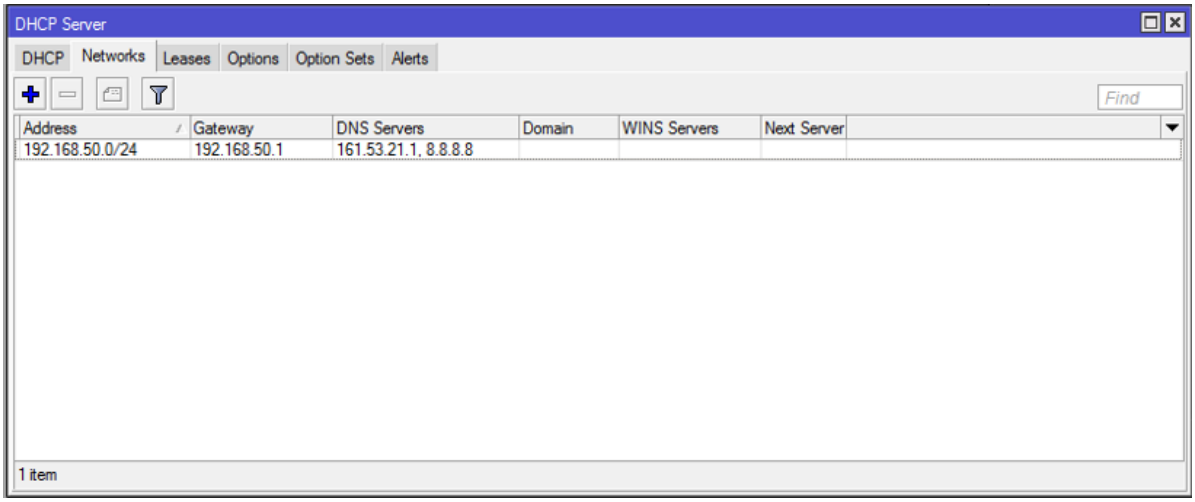
Slika 8.124. Izbornik s popisom definiranih DHCP Servera.

Iz izbornika *IP* → *DHCP* → *DHCP Server* odabrana je opcija *Add* za dodavanje novog servera. Server je nazvan *dhcp1*, pod opcijom *Interface* odabrano je *Ethernet4* sučelje, za *Relay* je postavljena adresa 192.168.50.1. *Relay* je samo proxy koji može primiti DHCP zahtjev i ponovno ga poslati na pravi DHCP poslužitelj (Slika 8.125.).



Slika 8.125. Izbornik za definiranje DHCP servera

Na kraju su unesene IP adrese *Google* DNS (eng. *Domain Name System*) servera. U izborniku DHCP Server pod tabom *Networks* vidljiva je postavljena adresa klijenta, adresa *gateway*-a i DNS serveri (slika 8.126.). DNS se može definirati kao jedna baza podataka koja sadrži sva imena i odgovarajuće IP adrese pojedinih računala, čija je uloga dobivanje IP adresa iz simboličkih naziva koji se mnogo lakše pamte.



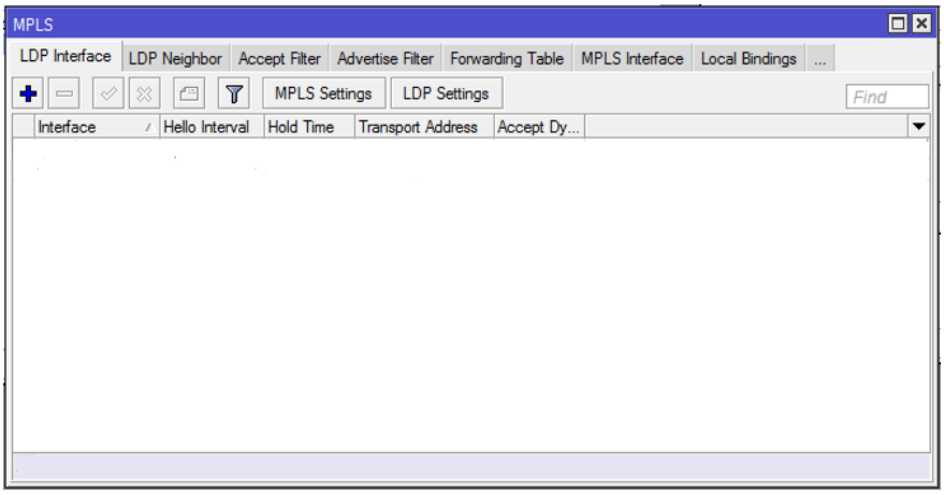
Slika 8.126. Izbornik s popisom DHCP mreža

8.4. MPLS postavke na usmjerivačima u kreiranoj mreži

MPLS može pri prijenosu koristiti bilo koje rješenje, od IP VPN-a do Ethernet-a. Kroz sljedeći primjer pokazan je postupak kreiranja MPLS-a. Osnovna ideja bila je stvaranje prometa između računala CE1_Site1 i CE2_Site2 i usmjeravanje tog prometa pomoću MPLS-a. Na svakom od pet usmjerivača načinjena je MPLS konfiguracija.

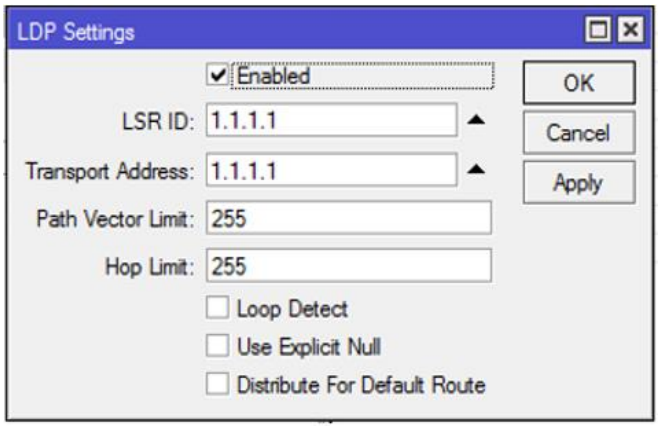
8.4.1 MPLS postavke na usmjerivaču MikroTik P1

U glavnom izborniku odabran je *MPLS* pri čemu se otvara sljedeći prozor (Slika 8.89.) u kojem je odabran *LDP Settings*.



Slika 8.89. MPLS prozor

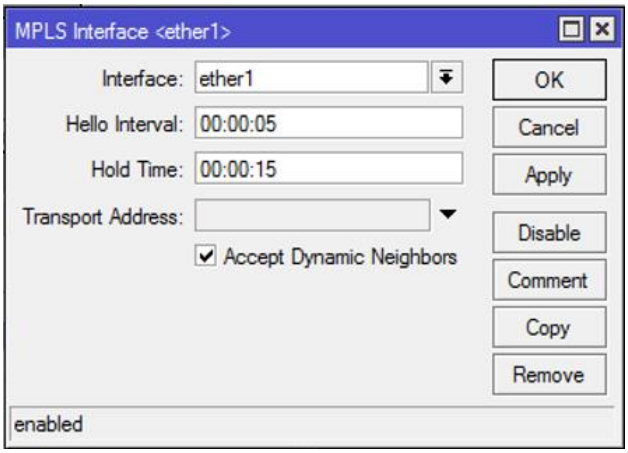
Klikom na *LDP Settings* otvara se prozorčić u kojem je postavljen *LSR ID*: 1.1.1.1 i *Transport Address*: 1.1.1.1. Osim toga, stavljena je kvačica na *Enabled* (Slika 8.90.). *LSR ID* je jedinstveni ID za prebacivanje oznaka usmjerivača. Ako je postavljen na 0.0.0.0, koristi se najviša IP adresa na usmjerivaču. *Transport Address* određuje adresu podrijetla LDP sesije i oglašava tu adresu LDP susjedima kao adresu za transport. Ako je postavljena na 0.0.0.0, koristi se najviša IP adresa na usmjerivaču. [77]



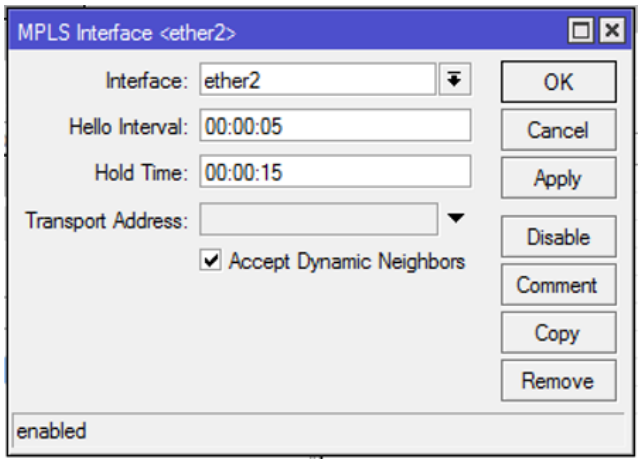
Slika 8.90. Postavke za LDP

Path Vector Limit je maksimalna granična vrijednost vektora za praćenje koji se koristi za otkrivanje petlje, dok je *Hop Limit* maksimalna granična vrijednost skoka koji se koristi za otkrivanje petlje. Obje vrijednosti koriste se u kombinaciji u cilju otkrivanja petlje. [77]

Nakon što upisane postavke za LDP, kreirana su MPLS LDP sučelja prema korištenoj topologiji. U MPLS prozoru odabire se *LDP Interface* (Slika 8.89.). Za dodavanje sučelja potrebno je kliknuti na *Add* pri čemu se otvara sljedeći prozorčić u kojem se odabire jedno od ponuđenih sučelja (Slika 8.91., Slika 8.92.).



Slika 8.91. Postavljanje *ether1* sučelja

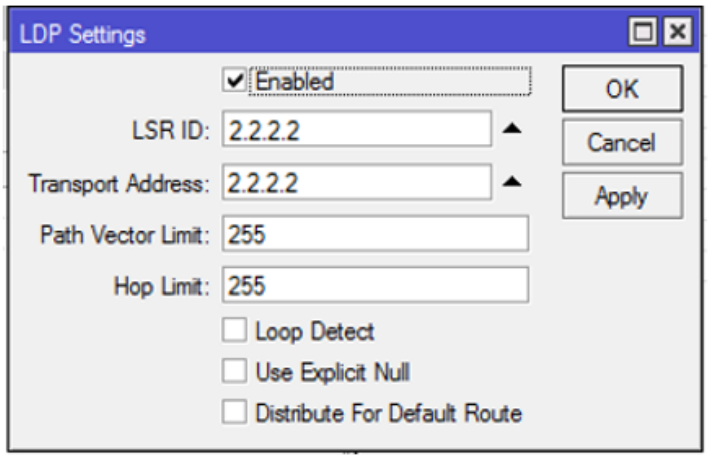


Slika 8.92. Postavljanje *ether2* sučelja

Hello Interval je interval između *hello* paketa koje usmjerivač šalje na ovo sučelje. *Hold Time* određuje interval nakon kojeg je susjed proglašeno nepristupačnim (engl. *Not reachable*). *Accept Dynamic* određuje hoće li se pristupiti dinamičkom otkrivanju susjeda ili će koristiti samo statička konfiguracija navedena u izborniku *LDP Neighbors*. [77]

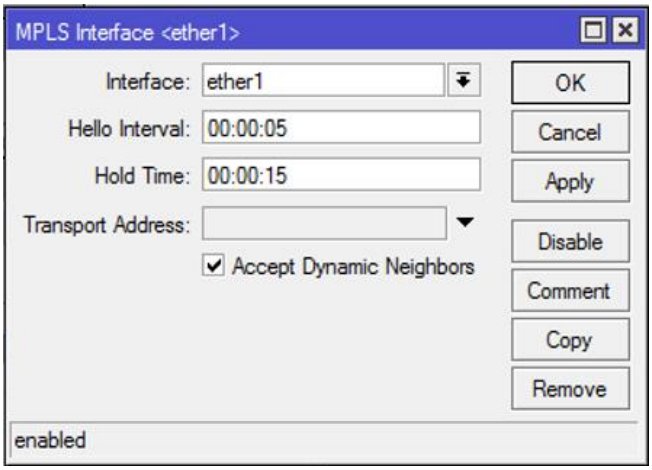
8.4.2. MPLS postavke na usmjerivaču MikroTik P2

Kao i kod prethodnog MikroTik-a, odabran je *LDP Settings* pri čemu se otvara prozorčić u kojem je postavljen *LSR ID*: 2.2.2.2 i *Transport Address*: 2.2.2.2. Također je stavljena kvačica na *Enabled* (Slika 8.93.).

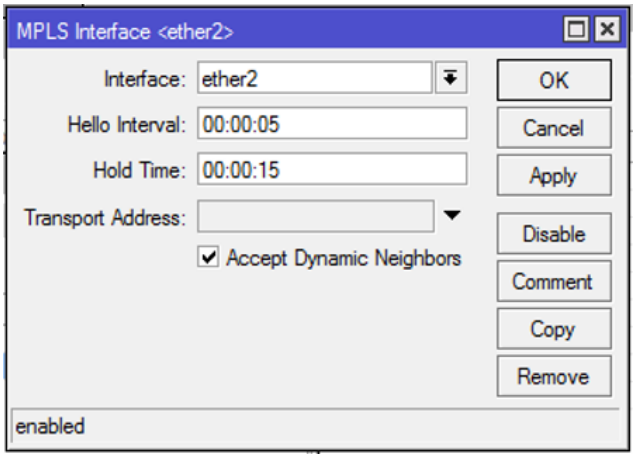


Slika 8.93. Postavke za LDP

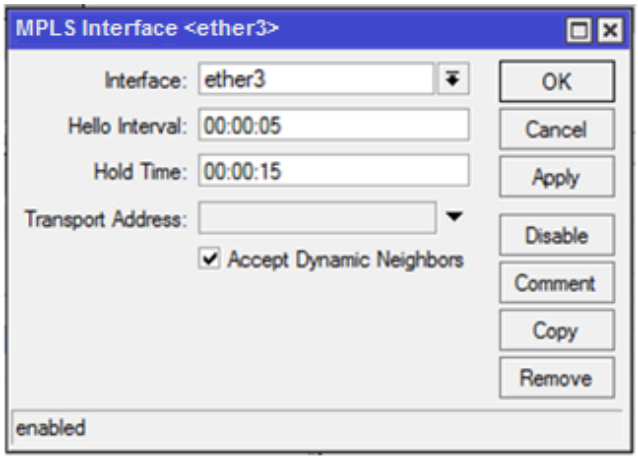
Nakon toga, kreirana su MPLS LDP sučelja prema kreiranoj topologiji, na isti način kao i kod prethodnog usmjerivača. (Slika 8.94., Slika 8.95., Slika 8.96.)



Slika 8.94. Postavljanje *ether1* sučelja



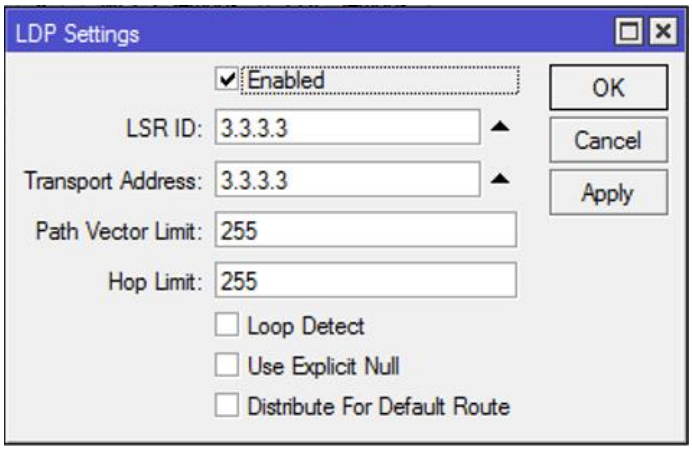
Slika 8.95. Postavljanje *ether2* sučelja



Slika 8.96. Postavljanje *ether3* sučelja

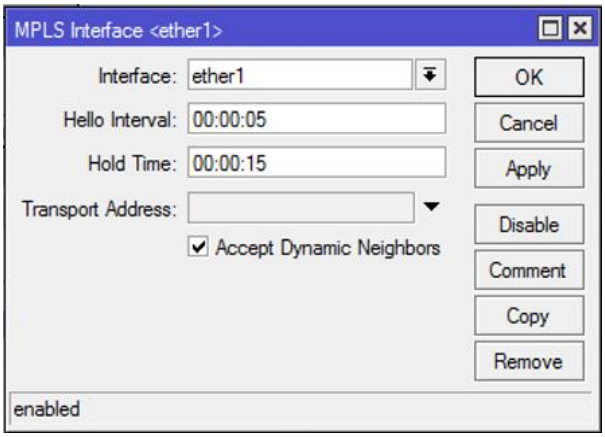
8.4.3. MPLS postavke na usmjerivaču MikroTik P3

Kao i kod prethodna dva usmjerivača, odabran je *LDP Settings* pri čemu se otvara prozorčić u kojem se postavlja *LSR ID*: 3.3.3.3 i *Transport Address*: 3.3.3.3. Također je stavljena kvačica na *Enabled*. (Slika 8.97.)

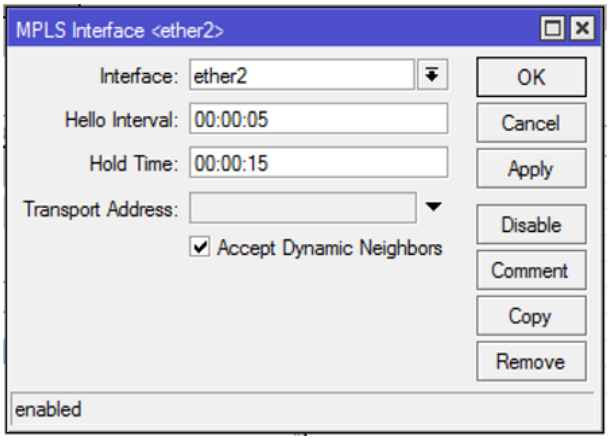


Slika 8.97. Postavke za LDP

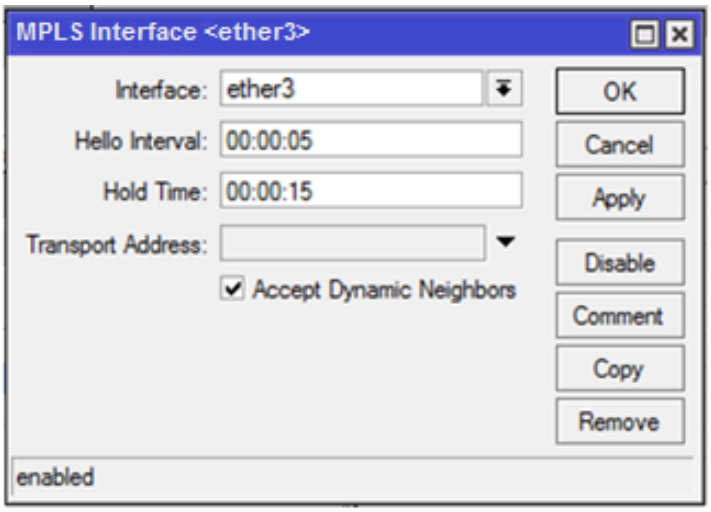
Zatim su kreirana MPLS LDP sučelja prema kreiranoj topologiji, na isti način kao i kod prethodnih usmjerivača. (Slika 8.98., Slika 8.99., Slika 8.100.)



Slika 8.98. Postavljanje *ether1* sučelja



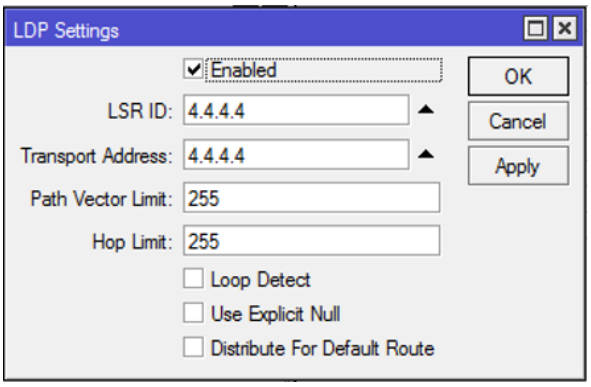
Slika 8.99. Postavljanje *ether2* sučelja



Slika 8.100. Postavljanje *ether3* sučelja

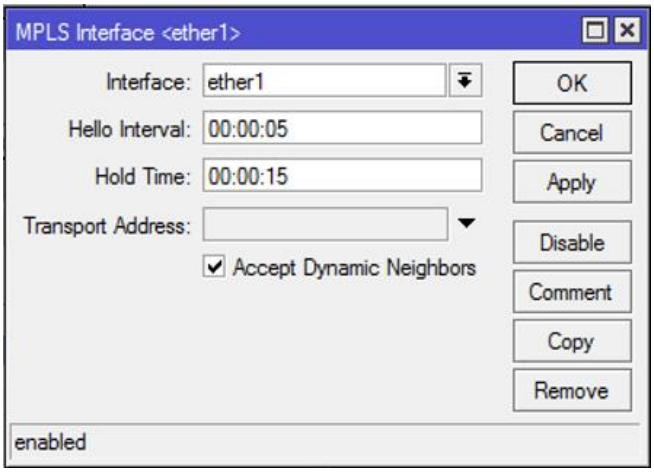
8.4.4. MPLS postavke na usmjerivaču MikroTik PE-1

Odabran je *LDP Settings* pri čemu se otvara prozorčić u kojem se postavlja *LSR ID*: 4.4.4.4 i *Transport Address*: 4.4.4.4. Stavljena je kvačica na *Enabled* (Slika 8.101.).

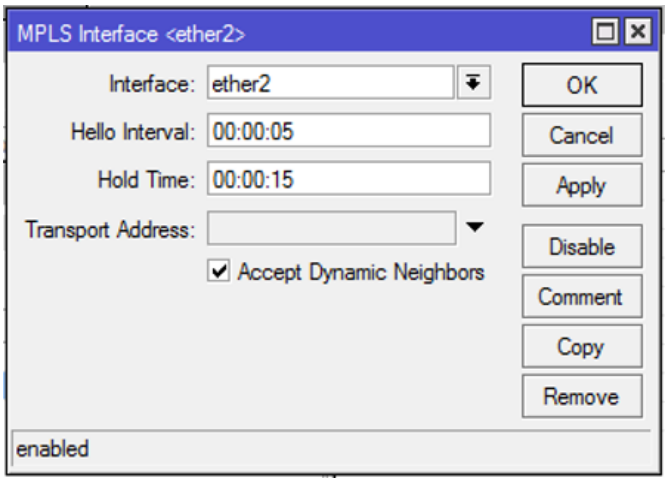


Slika 8.101. Postavke za LDP

Nakon postavljanja LDP postavki, kreirana su MPLS LDP sučelja prema korištenoj topologiji, na isti način kao i kod prethodnih usmjerivača. (Slika 8.102., Slika 8.103.)



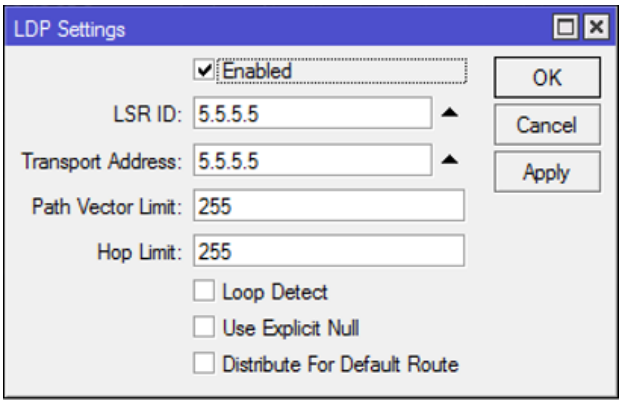
Slika 8.102. Postavljanje *ether1* sučelja



Slika 8.103. Postavljanje *ether2* sučelja

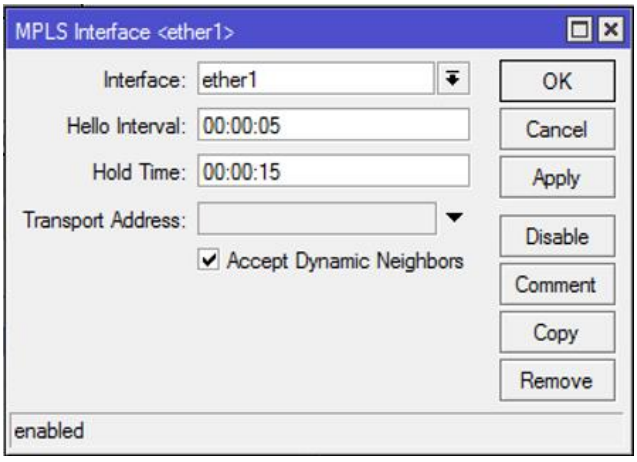
8.4.5. MPLS postavke na usmjerivaču MikroTik PE-2

Na kraju, i kod posljednjeg usmjerivača odabran je *LDP Settings* pri čemu se otvara prozorčić u kojem se postavlja *LSR ID*: 5.5.5.5 i *Transport Address*: 5.5.5.5. Stavljena je kvačica na *Enabled*. (Slika 8.104.)

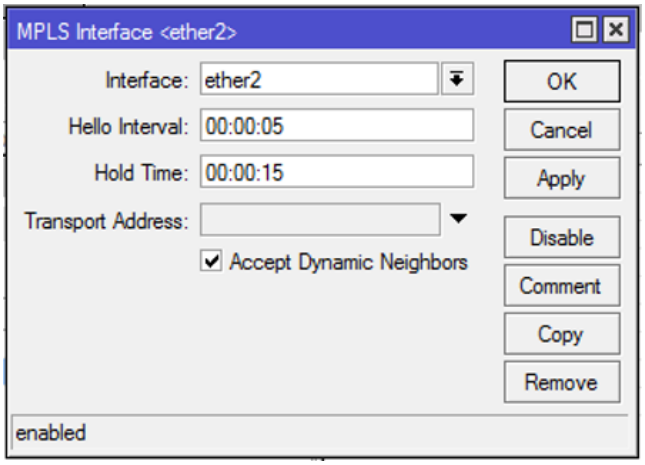


Slika 8.104. Postavke za LDP

Konfiguracija MPLS-a završava kreiranjem MPLS LDP sučelja prema korištenoj topologiji, na identičan način kao i kod prethodna četiri usmjerivača (Slika 8.105., Slika 8.106.).



Slika 8.105. Postavljanje *ether1* sučelja



Slika 8.106. Postavljanje *ether2* sučelja

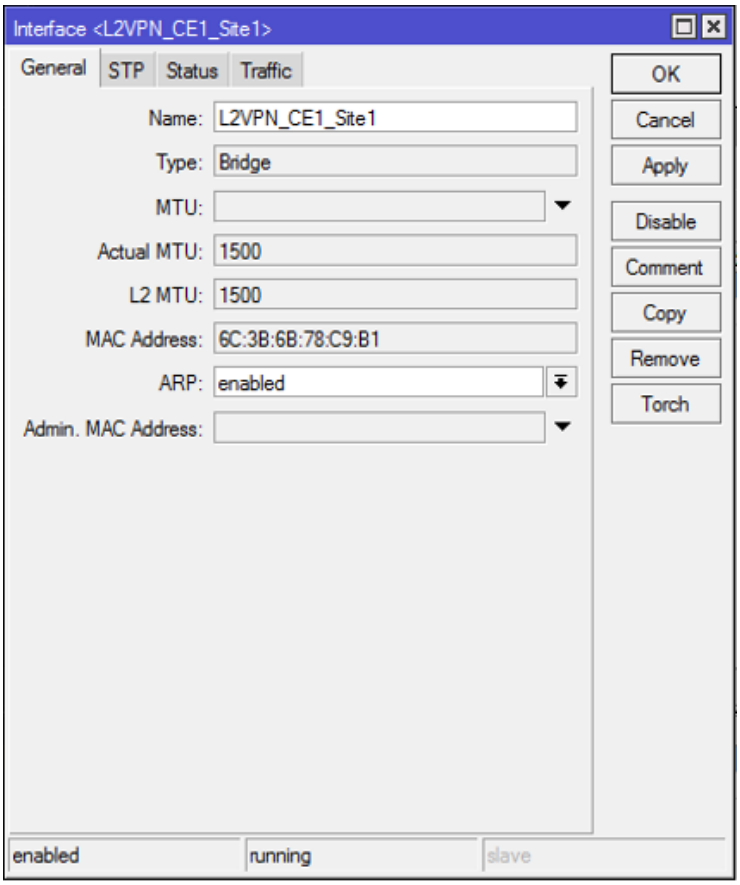
8.5. VPLS postavke na usmjerivačima u kreiranoj mreži

VPLS sučelje može se smatrati tunelskim sučeljem, baš kao i *EoIP* sučelje. Svaki postupak konfiguracije tunela uključuje stvaranje VPLS sučelja. Definiranje VPLS tunela obavlja se LDP protokolom - obje krajnje točke tunela razmjenjuju oznake koje će se koristiti za tunel. Prosljeđivanje podataka u tunelu odvija se implicitnim postavljanjem dvije oznake u paketu: oznake tunela i oznake prijenosa. *VPLS ID* parametar identificira svaki tunel i mora biti jedinstven za svaki tunel između ovog i udaljenog peer tunela.

Odrađena je VPLS konfiguracija na računalima *CE1_Site1* i na *CE1_Site2*.

8.5.1. VPLS postavke na usmjerivaču MikroTik PE-1

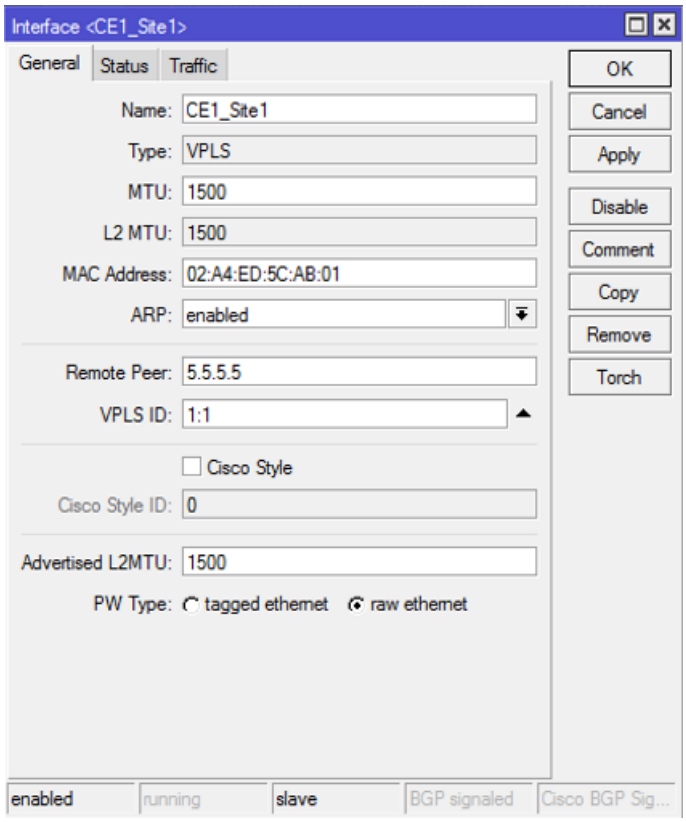
Prvo je na računalu *CE1_Site1* dodan *bridge* koji je nazvan *L2VPN_ CE1_Site1* (Slika 8.107.).



Slika 8.107. Postavljanje *L2VPN_ CE1_Site1 bridge-a*

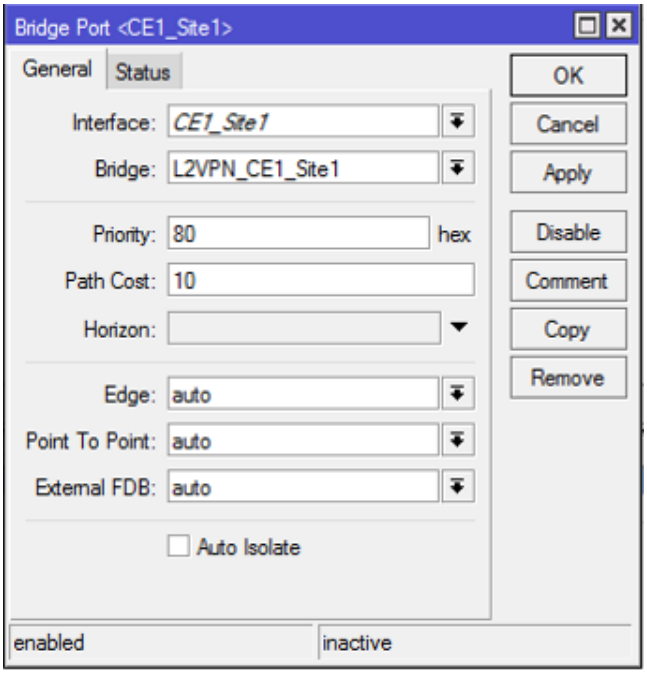
Nakon dodavanja *L2VPN_CE1_Site1 bridge-a*, dodano je sučelje *CE1_Site1*, klikom na *Interfaces* u izborniku s lijeve strane pa zatim klikom na *Add*. Za *CE1_Site1* sučelje postavljen je *Remote Peer*: 5.5.5.5 i *VPLS ID*: 1:1. (Slika 8.108.). *Remote Peer* je IP adresa udaljenog *peer-a*, dok je

VPLS ID Jedinstveni broj koji identificira VPLS tunel. Kodiranje se provodi prema jednom od sljedećih koncepat: (2 bajta + 4 bajta) ili (4 bajta + 2 bajta). [77]

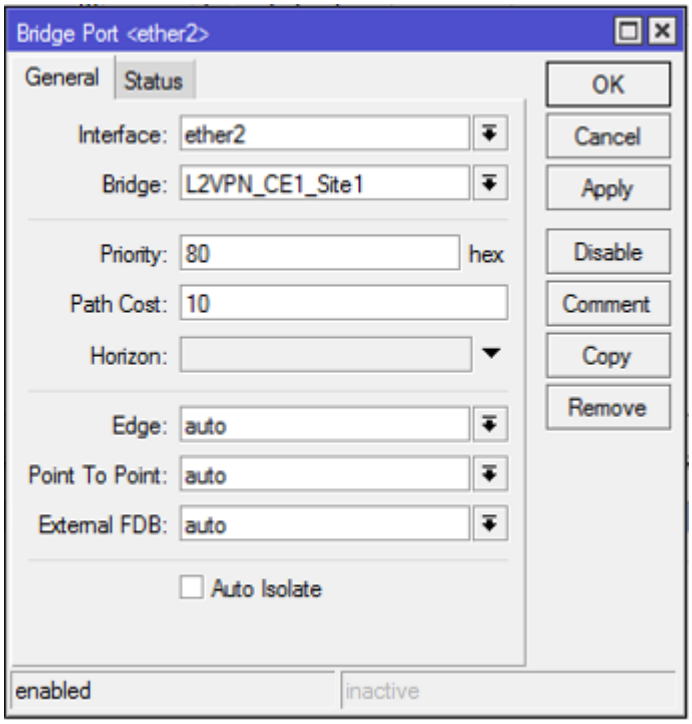


Slika 8.108. Postavke za *CE1_Site1* sučelje

Na kraju je potrebno dodati dva *bridge port-a*. Klikom na *Bridge* u izborniku s lijeve strane, otvara se prozor u kojem je potrebno kliknuti na *Ports* te se zatim odabire *Add*. Prvi *bridge port* je dodan sa *ether2* sučelja na *L2VPN_CE1_Site1 bridge* (Slika 8.109.). Drugi *bridge port* je dodan sa *CE1_Site1* sučelja na *L2VPN_CE1_Site1 bridge* (Slika 8.110.).



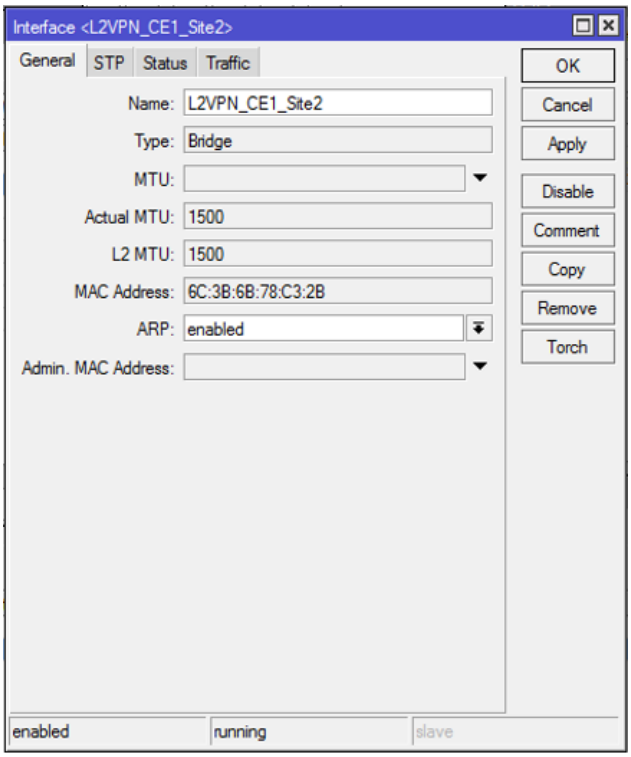
Slika 8.109. *Bridge Port* sa *CE1_Site1* sučelja na *L2VPN_CE1_Site1 bridge*



Slika 8.110. *Bridge Port* sa *ether2* sučelja na *L2VPN_CE1_Site1 Bridge*

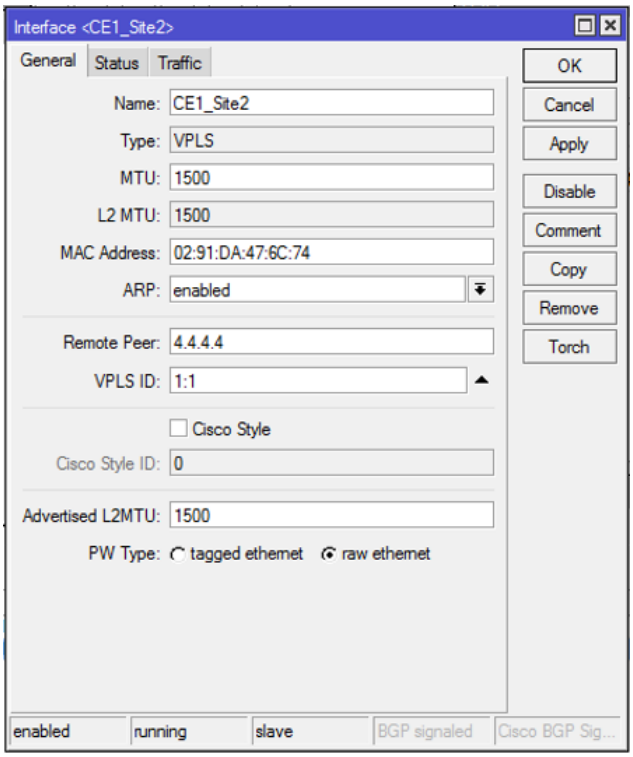
8.5.2. VPLS postavke na usmjerivaču MikroTik PE-2

Prvo je na dodan *bridge* koji je nazvan *L2VPN_CE1_Site2* (Slika 8.111.).



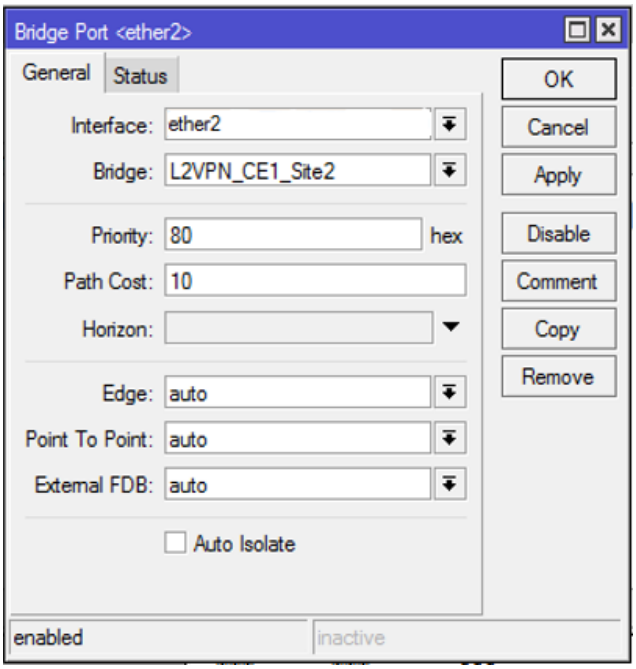
Slika 8.111. Postavljanje *L2VPN_CE1_Site2* bridge-a

Nakon dodavanje *L2VPN_CE1_Site2 bridge-a*, dodano je sučelje *CE1_Site2*, na isti način kao i u prethodnom slučaju. Za *CE1_Site2* sučelje postavljen je *Remote Peer*: 4.4.4.4 i *VPLS ID*: 1:1 (Slika 8.112.).

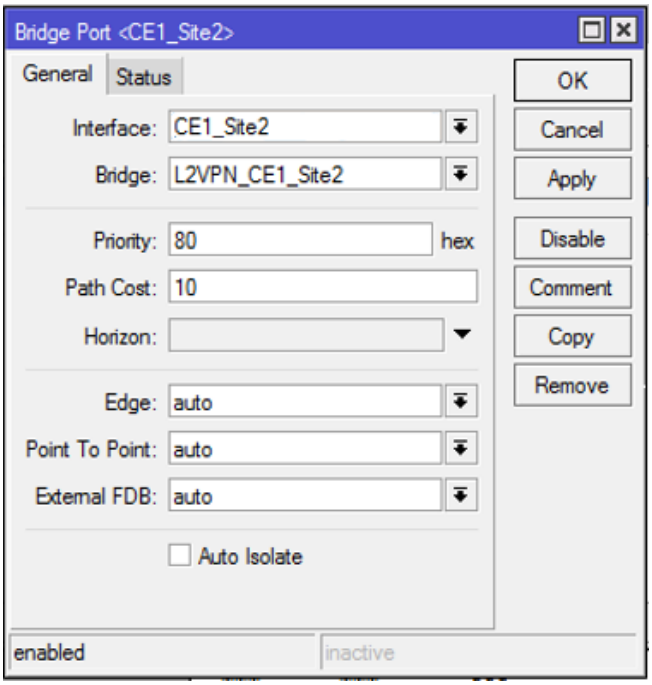


Slika 8.112. Postavke za *CE1_Site2* sučelje

Na kraju su dodana dva *bridge port-a*, na isti način kao i u prethodnom slučaju. Prvi *bridge port* je dodan sa *ether2* sučelja na *L2VPN_CE1_Site2 bridge* (Slika 8.113.). Drugi *bridge port* je dodan sa *CE1_Site2* sučelja na *L2VPN_CE1_Site2 bridge* (Slika 8.114.).



Slika 8.113. *Bridge* Port sa *ether2* sučelja na *L2VPN_CE1_Site2 bridge*



Slika 8.114. *Bridge* Port sa *CE1_Site2* sučelja na *L2VPN_CE1_Site2 bridge*

Nakon što je konfiguriran VPLS, u prozoru *Terminal* upisana je sljedeća naredba koja prikazuje trenutni status VPLS sučelja (Slika 8.115.).

```
[admin@MikroTik] > interface
[admin@MikroTik] /interface> vpls
[admin@MikroTik] /interface vpls> monitor
numbers: 0
```

Slika 8.115. Naredba za prikaz trenutnog statusa VPLS sučelja

Prethodna naredba daje sljedeća svojstva dostupna samo za čitanje (Slika 8.116.):

```
[admin@MikroTik] > interface
[admin@MikroTik] /interface> vpls
[admin@MikroTik] /interface vpls> monitor
numbers: 0
       remote-label: 26
        local-label: 25
      remote-status:
          transport: 4.4.4.4/32
  transport-nexthop: 10.10.35.1
     imposed-labels: 16,26
```

Slika 8.116. Rezultat naredbe za prikaz trenutnog statusa VPLS sučelja

Remote-label prikazuje udaljenu VPLS oznaku.

Local-label prikazuje lokalnu VPLS oznaku.

Transport prikazuje naziv prijenosnog sučelja. Postavlja se ako je VPLS pokrenut preko tunela za tehnike upravljanja mrežnim prometom.

Transport-nexthop prikazuje transportnu adresu, obično je to *Loopback* adresa.

Imposed-labels prikazuje nametnutu VPLS oznaku. [80]
Nakon provjere načinjene VPLS i MPLS konfiguracije, potvrđeno je postojanje konekcije između dva računala *CE1_Site1* i *CE1_Site2*.

9. ZAKLJUČAK

Posljednjih godina pružatelji telekomunikacijskih usluga suočavaju se sa sve većim zahtjevima vezanima uz prosljeđivanje mrežnog prometa. Pružatelji usluga moraju otkrivati nove i poboljšane metode prosljeđivanja prometa kroz mrežu, budući da dosadašnje metode temeljene na *IP-over-ATM* modelu ne mogu zadovoljiti sve postavljene korisničke zahtjeve. Jedna od takvih metoda je primjena višeprotokolnog komutiranja podatkovnog prometa u mreži temeljenog na oznakama (MPLS), koja pokazuje značajna poboljšanja u odnosu na *IP-over-ATM* model. Karakterizira ga jednostavni mrežni dizajn te dokazana prilagodljivost različitim promjenama i prometnim zahtjevima u mreži. Svakako je jedna od najvećih prednost MPLS-a omogućavanje pružateljima usluga isporuku novih usluga koje nisu bile podržane ustaljenim IP tehnikama usmjeravanja. MPLS pruža fleksibilnost pri rješavanju kontrolnih funkcija bez potrebe za mijenjanjem mehanizma za prosljeđivanje, budući da je kontrolna komponenta odvojena od komponente za prosljeđivanje.

MPLS VPN predstavlja najprihvaćenije aplikacijsko proširenje u MPLS mrežama. Brojni su čimbenici koji su MPLS VPN mrežama omogućili da postanu prikladne za primjenu u različitim poslovnim okruženjima. Budući da se MPLS paketi formiraju na MPLS rubnim usmjerivačima, moguće je definirati put kojim će promet morati proći kroz mrežu, tj. svaka klasa prometa (podaci, glas, video) može zahtijevati različite načine prijenosa podataka. U MPLS mrežama je omogućena mrežna konvergencija, slanje prometnih podataka preko nižeg prioritetnog puta i osjetljivih govornih/video paketa u realnom vremenu preko visokog prioritetnog, ali slabije korištenog, kraćeg puta.

MPLS jezgrena mreža dizajnirana je i izgrađena kako bi se prevladala pojedina hardverska ograničenja. U takvim slučajevima, podaci se preusmjeravaju na sljedeći optimalni put s vremenom kašnjenja manjim od 50 ms. Važno je napomenuti kako MPLS mreže mogu prenositi bilo koju vrstu paketa (IP, Frame Relay ili ATM) putem iste mreže. Neovisno koja vrsta paketa dolazi, MPLS oznake su povezane zbog prijenosa podataka preko MPLS mreže i te oznake su neovisne o protokolu.

Za razliku od IP mreža, MPLS je mrežno orijentirana tehnologija pa se može reći kako prijenos podataka MPLS mrežom mnogo pouzdaniji. Pružatelji usluga definiraju odgovarajuće razine kvalitete usluga u MPLS mreži pružajući jamstvo da će zastoj u radu mreže tijekom ugovorenog razdoblja biti minimalan. To je naravno moguće, jer se MPLS mreže mogu proaktivno pratiti i

održavati. MPLS mreže dopuštaju dinamičku raspodjelu širine prijenosnog pojasa, pa se stoga mogu koristiti za pružanje širine prijenosnog pojasa na zahtjev. Vrlo bitna činjenica je da pružatelji usluga preuzimaju punu odgovornost za sigurnost informacija koje se šalju putem MPLS mreže.

U praktičnom dijelu ovog rada načinjena je OSPF, MPLS i VPLS konfiguracija uređaja – MikroTik usmjerivača te računala u kreiranoj testnoj mreži.

Prije konfiguracije OSPF-a svakom MikroTik-u su pridružene adrese njegovih aktivnih sučelja. Na svakom od računala onemogućene su sve mrežne konekcije osim LAN-a. Na računalima *CE1_Site1* i *CE1_Site2* postavljene su odgovarajuće IP adrese. Kako bi se konfigurirao OSPF, na svakom od pet MikroTik-ova kreiran je *bridge* koji je nazvan *Loopback0* te mu je dodana odgovarajuća IP adresa; od 1.1.1.1 do 5.5.5.5. Nakon toga je na svakom MikroTik-u dodana instanca koja je nazvana *default*, a svakoj instanci *default* pridružena je oznaka Router ID; od 1.1.1.1 do 5.5.5.5. Na svakom MikroTik-u su definirane mreže njemu susjednih usmjerivača, pri čemu je za svaku mrežu definirano područje jezgrene (engl. *backbone*) mreže. Nakon konfiguracije OSPF-a odrađena je provjera svih mreža i konekcija između uređaja nakon čega je utvrđeno da svi uređaji mogu međusobno komunicirati.

Konfiguracija MPLS-a također je odrađena na svakom od pet MikroTik usmjerivača. Osnovna ideja bila je omogućiti prosljeđivanje prometa između računala *CE1_Site1* i *CE2_Site2* i omogućiti usmjeravanje tog promet pomoću MPLS-a. Na svakom od MikroTik-ova iz izbornika MPLS odabran je *LDP Settings* gdje je postavljen *LSR ID* i *Transport Address*, koji su jednaki kao i IP adresa prethodno kreiranog *bridge-a* za svaki pojedini MikroTik. Nakon toga, kreirana su *MPLS LDP* sučelja, pri čemu je bilo bitno pratiti zadanu topologiju, kako bi se utvrdilo koji MikroTik koristi koje od sučelja.

VPLS konfiguracija MikroTik-a *PE-1* i *PE-2* odrađena je na računalima *CE1_Site1* i na *CE1_Site2*. Za MikroTik *PE-1* na računalu *CE1_Site1* dodan je *bridge* koji je nazvan *L2VPN_ CE1_Site1*, a zatim sučelje *CE1_Site1* za koje je postavljen *Remote Peer:* 5.5.5.5 i *VPLS ID*: 1:1. Nakon toga dodana su dva *bridge* porta; prvi *bridge port* je dodan sa *ether2* sučelja na *L2VPN_CE1_Site1 bridge*, dok je drugi *bridge port* dodan sa *CE1_Site1* sučelja na *L2VPN_CE1_Site1 bridge*. Za MikroTik *PE-2* na računalu *CE1_Site2* dodan je *bridge L2VPN_CE1_Site2* te sučelje *CE1_Site2* na kojem je *Remote Peer* postavljen na 4.4.4.4, a *VPLS ID* na 1:1. Kao i kod prethodnog MikroTik-a, na kraju su dodana dva *bridge port-a*; prvi *bridge port* je dodan sa *ether2* sučelja na *L2VPN_CE1_Site2 Bridge*, dok je drugi *bridge port* dodan sa *CE1_Site2* sučelja na *L2VPN_CE1_Site2 bridge*.

Nakon što su odrađene sve planirane konfiguracije, omogućen je pristup Internetu na usmjerivaču P1 preko sučelja *ether3*. Kako bi se konfigurirao usmjerivač P1, definirano je DHCP klijentsko sučelje gdje je vidljiva IP adresa dodijeljena DHCP klijentu. U svrhu povezivanja lokalnih mreža s Internetom korišten je postupak koji se naziva prevođenje mrežnih adresa - NAT.

Načinjena MPLS konfiguracija pokazala je kako MPLS uvelike olakšava stvaranje „virtualne veze“ između udaljenih čvorova. Također, MPLS pruža brz i pouzdan prijenos podataka te omogućava međusobnu komunikaciju svih lokacija u nekoj mreži. Vrlo je važna činjenica kako se MPLS odlikuje s jednostavnošću implementacije

LITERATURA

[1] Davatelj usluga na internetu. Dostupno na: https://mreze.wikispaces.com/davatelj+internetskih+usluga (06. travnja 2018.)

[2] Lovrek, I., (2007.) Telekomunikacijska tehnologija i specifičnosti telekomunikacijskog tržišta, Zagreb: Element. Dostupno na: https://element.hr/artikli/file/1355 (06. travnja 2018.)

[3] Cisco & Cisco Router, Network Switch, (2018.). Cisco ONE Software Device Tiering Guide-Part 1. Dostupno na: http://ciscorouterswitch.over-blog.com/article-cisco-network-design-model-overview-123463634.html (06. travnja 2018.)

[4] Cisco & Cisco Router, Network Switch, Cisco Three Layer / Three-tier Hierarchical Network Model. Dostupno na: http://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php (06. travnja 2018.)

[5] Širokopojasne telekomunikacione mreže. Dostupno na: http://telekomunikacije.etf.rs/predmeti/te4ks/docs/STM/STM_02.pdf (06. travnja 2018.)

[6] Rouse, M., SDH (Synchronous Digital Hierarchy). Dostupno na: https://searchnetworking.techtarget.com/definition/SDH (06. travnja 2018.)

[7] PDH vs SDH | Difference between PDH and SDH. Dostupno na: http://www.rfwireless-world.com/Terminology/PDH-vs-SDH.html (06. travnja 2018.)

[8] Schultz, B., (2011.), Optical transport network (OTN) primer. Dostupno na: https://searchtelecom.techtarget.com/feature/Optical-transport-network-OTN-primer (06. travnja 2018.)

[9] ATM mreža. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=4462 (06. travnja 2018.)

[10] FER, (2012.), ATM (Asynchronous Transfer Mode). Dostupno na: http://spvp.zesoi.fer.hr/seminari/1999/atm/atm.htm (06. travnja 2018.)

[11] Mercy, I., (2012.) Asynchronous transfer mode http://shareengineer.blogspot.hr/2012/10/asynchronous-transfer-mode.html (06. travnja 2018.)

[12] Jacobsen. J., (2001), The Internet Protocol Journal. Dostupno na: https://www.cisco.com/c/dam/en_us/about/ac123/ac147/archived_issues/ipj_4-3/ipj_4-3.pdf (06. travnja 2018.)

[13] Arhitektura, protokoli i servisi Interneta. Dostupno na: http://eukallos.edu.ba/public_html/Knjige/Arhitektura-protokoli-i-servisi-interneta.pdf (09. travnja 2018.)

[14] MPLS Layer 2.5. Dostupno na: http://lightriver.com/wp-content/uploads/2015/07/LightRiverTechByte_MPLS_Layer-2_5.pdf (09. travnja 2018.)

[15] What is MPLS? Dostupno na: http://www.mplsinfo.org/ (09. travnja 2018.)

[16] https://supportforums.cisco.com/t5/tkb/articleprintpage/tkb-id/4441-docs-service-providers/article-id/1684 (09. travnja 2018.)

[17] xthuijs, Cisco employee, (2012.). Service Providers Documents. Dostupno na: https://www.netlab.tkk.fi/tutkimus/fit/publ/thesis_Susitaival_04.pdf (09. travnja 2018.)

[18] Ruela. J., Ricardo. M. MPLS – Multiprotocol Label Switching. Dostupno na: https://web.fe.up.pt/~mricardo/doc/ieeehandbook/ieeehandbook.pdf (09. travnja 2018.)

[19] Bond, C., Short repetition of two important facts. Dostupno na: http://slideplayer.com/slide/7319159/ (09. travnja 2018.)

[20] Gray, W. Eric. (2001.) MPLS Architecture. Dostupno na: http://www.informit.com/articles/article.aspx?p=167856 (09. travnja 2018.)

[21] Prat., L. (2012.) MPLS Layer 3 VPNs. Dostupno na: https://aitaseller.wordpress.com/2012/09/10/mpls-layer-3-vpns/ (09. travnja 2018.)

[22] Cisco Systems, (1999.) MPLS Label Distribution Protocol (LDP). Dostupno na: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/12_2sr/mp_12_2sr_book/mp_ldp_overview.pdf (09. travnja 2018.)

[23] Sing, M., Constraint-based Routing LDP (CR-LDP). Dostupno na: http://networkshorizon.blogspot.hr/2012/01/constraint-based-routing-ldp-cr-ldp.html (09. travnja 2018.)

[24] What is RSVP-TE? Dostupno na: https://www.metaswitch.com/knowledge-center/reference/what-is-rsvp-te (09. travnja 2018.)

[25] RSVP Message, (2007.). Dostupno na: https://ccie11440.blogspot.hr/2007/07/rsvp-message.html (09. travnja 2018.)

[26] Sović, M., Protokoli za usmjeravanje. Dostupno na: http://spvp.zesoi.fer.hr/seminari/2006/SovicMarina_Protokolizausmjeravanje.pdf (09. travnja 2018.)

[27] Cisco Systems, (2005.). Introduction to EIGRP. Dostupno na: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html (09. travnja 2018.)

[28] Rosen, E., Viswanathan, A., Callon, R., Multiprotocol Label Switching Architecture, RFC 3031, January 2001.

[29] Juniper, (2017.). Understanding MPLS Label Operations. Dostupno na: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-label-operations-qfx-series.html (10. travnja 2018.)

[30] Osborne, E.,Simha, A.: *Traffic Engineering with MPLS* (5th Edition), Cisco Press, USA, 2002.

[31] Nikolić. N., (2013.). MPLS-Poboljšanje funkcionalnosti usmeravanja i aplikacije. Dostupno na: http://infoteh.etf.unssa.rs.ba/zbornik/2013/radovi/STS/STS-16.pdf (10. travnja 2018.)

[32] MPLS TE Technology White Paper, (2008.). Dostupno na: http://www.h3c.com.hk/products___solutions/technology/mpls/technology_white_paper/200806/608770_57_0.htm (10. travnja 2018.)

[33] Beller. D., Sperber. R., MPLS-TP – The New Technology for Packet Transport Networks. Dostupno na: https://www.dfn.de/fileadmin/3Beratung/DFN-Forum2/118.pdf (10. travnja 2018.)

[34] Moore. P., Carrier ethernet-network-solutions. Dostupno na: https://www.slideshare.net/Metaswitch_NTD/carrier-ethernetnetworksolutions2010 (10. travnja 2018.)

[35] S. M., (2016.) Što je VPN? Za što se koristi? Dostupno na: http://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/ (10. travnja 2018.)

[36] https://www.scribd.com/doc/110757653/UPOREDNA-ANALIZA-ATM-MPLS-I-GMPLS-MRE%C5%BDA (10. travnja 2018.)

[37] Guichard, J.,Le Faucheur, F., Vasseur, J.P. Cisco Press, USA, (2005.) *Definitive MPLS Network Designs* (1st Edition)

[38] Ćulibrk. D., (2007.) Uporedna analiza ATM, MPLS i GMPLS mreža. Dostupno na: https://www.slideshare.net/aserna1988/multiprotocol-label-switching-a-brief-introduction-to-the-most-relevant (10. travnja 2018.)

[39] Ilić. D., Pavlović. B., Jevtović. M., Analiza karakteristika GMPLS protokola. Dostupno na: http://www.telfor.rs/telfor2005/radovi/TM-2.21.pdf (10. travnja 2018.)

[40] http://www.chief.com.tw/dispPageBox/ct.aspx?ddsPageID=ENDATASERVICE&dbid=4852930447 (10. travnja 2018.)

[41] Pepelnjak, I., Guichard, J., Apcar, J.:*MPLS and VPN Architectures, Volume II (1st Edition)*, Cisco Press, USA,2003.

[42] Partsenidis., C., (2001.). MPLS VPN tutorial. Dostupno na: https://searchenterprisewan.techtarget.com/tutorial/MPLS-VPN-tutorial (10. travnja 2018.)

[43] Brandenburg. M., 2010. MPLS VPN basics. Dostupno na: https://searchenterprisewan.techtarget.com/tutorial/MPLS-VPN-basics (10. travnja 2018.)

[44] Understanding Layer 3 VPNs. Dostupno na: https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-3-vpn-overview.html (10. travnja 2018.)

[45] Pignataro. C., Kazemi. R., Dry. B., (2002.). IP Virtual Private Network Services https://flylib.com/books/en/4.280.1.47/1/ (10. travnja 2018.)

[46] MPLS Configuration Guide. Dostupno na: http://www.h3c.com.hk/Technical_Support___Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/Configuration/Operation_Manual/H3C_S12500_CG-Release7128-6W710/08/201301/772669_1285_0.htm (10. travnja 2018.)

[47] Juniper, (2017.), Understanding Virtual Routing and Forwarding Tables. Dostupno na: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-routing-tables-vpn-forwarding-tables.html (13. travnja 2018.)

[48] Inter-AS L3VPN Option B, (2014.). Dostupno na: https://packetcorner.wordpress.com/category/mpls/l3vpn/ (13. travnja 2018.)

[49] Sayeed. A., Morrow., J. Monique, (2006.), Taxonomy. Dostupno na: https://flylib.com/books/en/3.2.1.44/1/ (13. travnja 2018.)

[50] http://slideplayer.com/slide/8112522/ (13. travnja 2018.)

[51] Wang. S., Computer Networks II. Dostupno na: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpws-overview.html (13. travnja 2018.)

[52] Scripcariu., L., Bogdan. I., (2009.) Virtual Private Netorks. Dostupno na: http://www.agir.ro/buletine/743.pdf (13. travnja 2018.)

[53] Virtual Leased Line, (2018.). Dostupno na: https://en.wikipedia.org/wiki/Virtual_Leased_Line (13. travnja 2018.)

[54] Lakshman., U., Lobo. L., (2006.) Introduction to Layer 2 VPNs. Dostupno na: https://flylib.com/books/en/2.686.1/introduction_to_layer_2_vpns.html (13. travnja 2018.)

[55] Cisco Systems, (2004.). Any Transport over MPLS. Dostupno na: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fsatom28.html (13. travnja 2018.)

[56] Introduction to L2TPv3, (2002.). Dostupno na: http://www.prol2tp.com/documentation.html?page=l2tpv3.html (13. travnja 2018.)

[57] Virtual private LAN service (VPLS), (2007.) Dostupno na: https://searchnetworking.techtarget.com/definition/virtual-private-LAN-service (13. travnja 2018.)

[58] Juan, (2017.) VPLS fundamentals. Dostupno na: https://learningnetwork.cisco.com/thread/117406 (13. travnja 2018.)

[59] Juniper Networks, (2010.). LDP-BGP VPLS Interworking. Dostupno na: https://www.juniper.net/us/en/local/pdf/whitepapers/2000282-en.pdf (13. travnja 2018.)

[60] Penttinen A., *Introduction to Teletraffic Theory*, Helsinki University of Technology, 1999.

[61] https://en.wikipedia.org/wiki/Telecommunications_forecasting (13. travnja 2018.)

[62] Telecommunications forecasting, (2018.). Dostupno na: https://www.slideshare.net/huy_le42/mpls-enabled-applications-emerging-developments-and-new-technologies (13. travnja 2018.)

[63] Evans. J., (2010.), A Practical Perspective on Traffic Engineering. Dostupno na: https://www.uknof.org.uk/uknof15/Evans-TrafEng.pdf (13. travnja 2018.)

[64] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.3152&rep=rep1&type=pdf (13. travnja 2018.)

[65] Stuart. R., (2014.), What to look for when gauging MPLS performance. Dostupno na: https://searchenterprisewan.techtarget.com/tip/What-to-look-for-when-gauging-MPLS-performance (18. travnja 2018.)

[66] Morris. B. Stephen., Network Management, MIBs and MPLS: Principles, Design and Implementation. Dostupno na:

https://www.safaribooksonline.com/library/view/network-management-mibs/0131011138/ch01.html (18. travnja 2018.)

[67] Cisco Systems, Lancope StealthWatch. Dostupno na: https://www.cisco.com/c/m/en_us/products/security/cisco-lancope.html (18. travnja 2018.)

[68] Veitch, P., Scalability and functionality challenges for MPLS VPN Networks, The Journal of The Communications Networks, Volume 6 Part 2

[69] Wang. D., (2016.), IP/MPLS Network Planning, Design, Simulation, Audit and Management. Dostupno na: http://docplayer.net/6759993-Ip-mpls-network-planning-design-simulation-audit-and-management-dave-wang-wandl.html (18. travnja 2018.)

[70] Juniper Networks, (2012.) IP/MPLSView. Dostupno na: https://www.yumpu.com/en/document/view/10558882/ip-mplsview-design-planning-suite-brochure-a-wandl (18. travnja 2018.)

[71] Juniper Networks, (2014.), Management and Monitoring Guide For IP/MPLSView. Dostupno na: https://www.juniper.net/documentation/en_US/ip-mplsview6.1.0/information-products/topic-collections/ip-mplsview-management-and-monitoring.pdf (18. travnja 2018.)

[72] Juniper Networks, (2016.), Topology Window Overview. Dostupno na: https://www.juniper.net/documentation/en_US/ip-mplsview6.2.0/information-products/topic-collections/user-guide/topic-96256.html (18. travnja 2018.)

[73] Aria Networks, (2011.), New Features in iVNT MPLS-TE 2.3. Dostupno na: http://www.aria-networks.com/news/new-features-in-ivnt-mpls-te-2-3/ (18. travnja 2018.)

[74] Aria Networks shows the optimal path, (2006.) Dostupno na: https://technologyinside.com/2007/04/26/aria-networks-shows-the-optimal-path/ (18. travnja 2018.)

[75] Kućni profesionalac. Dostupno na: https://www.sk.rs/2015/08/sktd06.html (30. svibnja 2018.)

[76] https://www.cyberbajt.com/product/7404/hap-lite-rb9412ndtc.html (30. svibnja 2018.)

[77] Manual:TOC, (2018.). Dostupno na: https://wiki.mikrotik.com/wiki/Manual:TOC (30. svibnja 2018.)

[78] Address Resolution Protocol. Dostupno na: https://en.wikipedia.org/wiki/Address_Resolution_Protocol (30. svibnja 2018.)

[79] Šta je ping i tracert (traceroute). Dostupno na: https://brakussale.wordpress.com/2012/09/20/sta-je-ping-i-tracert-traceroute/#more-120 (30. svibnja 2018.)

[80] Manual:Interface/VPLS. Dostupno na: https://wiki.mikrotik.com/wiki/Manual:Interface/VPLS (30. svibnja 2018.)

POPIS KRATICA I AKRONIMA

Kratice	Značenje kratica
AC	engl. Attachment Circuit
AS	engl. Autonomous System
ARP	engl. Address Resolution Protocol
ATM	engl. Asynchronous Transfer Mode
AToM	engl. Any transport over MPLS
BECN	engl. Backward Explicit Congestion Notification
BGP	engl. Multiprotocol-Border Gateway Protocol
BNG	engl. Broadband Network Gateway
CE	engl. Customer Edge
CoS	engl. Class of Service
CR-LDP	engl. Constraint-based Routing LDP
CSV	engl. Comma-Separated Values
CT	engl. Class Type
DANI	engl. Distributed Artificial Neural Intelligence
DE	engl. Discard Eligibility
DiffServe	engl. Differentiated Service
DHCP	engl. Dynamic Host Configuration Protocol
DNS	eng. Domain Name System
DSLAM	engl. Digital Subscriber Line Access Multiplexer
DUAL	engl. Diffusing Update Algorithm
ECMP	engl. Equal-cost multi-path
EIGRP	engl. Enhanced Interior Gateway Routing Protocol
ETHoMPLS	engl. Ethernet over MPLS
FDM	engl. Frequency Division Multiplexing
FEC	engl. Fowarding Equivalence Class
FECN	engl. Forward Explicit Congestion Notification
FR	engl. Frame Relay
FR DLCI	engl. Frame Relay Data Link Connection Identifiers
FTTx	engl. Fiber To The x
GMPLS	engl. Generalize MPLS
GoS	engl. Grade of Service
GRE	engl. Generic Routing Encapsulation
GUI	eng. Graphical User Interface
hAP	engl. Home Access Point
HDLC	engl. High-Level Data Link Protocol
IETF	engl. Internet Engineering Task Force
IGP	engl. Interior Gateway Protocol

ILMI/LMI	engl. Integrated Local Management Interface/Local Management Interface
IGRP	engl. Interior Gateway Routing Protocol
IntServ	engl. Integrated Services
IP	engl. Internet Protocol
IPLS	engl. IP LAN like Services
IPSec	engl. Internet Protocol Security
IPX	engl. Internetwork Packet Exchange
ISIS	engl. Intermediate System-to-Intermediate System
ISO/OSI	engl. Open Systems Interconnection Basic Reference Model
ISP	engl. Internet Service Provider
iVNT	engl. Intelligent Virtual Network Topologies
LAN	engl. Local Area Network
LDP	engl. Label Distribution Protocol
LE	engl. Label Edge
LER	engl. Label Edge Router
LFIB	engl. Label forwarding information base
LS	engl. Label Switching
LSR	engl. Label Switched Router
LSP	engl. Label Switched Path
L2TPv3	engl. Layer 2 Tunnel Protocol Version 3
L2TP	engl. Layer 2 Tunnel Protocol
MAC	engl. Media Acces Control
MIB	Management Information Base
MITM	engl. Man-in-the-middle attack
MPLS	engl. MultiProtocol Label Switching
MPLS VPN	engl. MultiProtocol Label Switching Virtual Private Network
MPLS QoS	engl. MPLS Quality of Service
MPLS TE	engl. MPLS Traffic Engineering
MPLS TP	engl. MPLS Transport Profile
MPLS VPN	engl. MPLS Virtual Private Networks
NAT	eng. Network Address Translation
NHLFE	engl. Next Hop Label Forwarding Entry
NMS	engl. Network Management System
OSPF	engl. Open Shortest Path First
OTN	engl. Optical Transport Network
P	engl. Provider
PDH	engl. Plesiochronous Digital Hierarchy
PDU	engl. Protocol Data Unit
PE	engl. Provider Edge
PHP	engl. Penultimate Hop Popping
PIM	engl. Protocol Independent Multicast
POP	engl. Point of Presence
PPP	engl. Point-to-Point Protocol
PSN	engl. Packet Switched Network
PW	engl. Pseudowire

PWE3	engl. Pseudowire Emulation Edge-to-Edge
PWES	engl. Pseudo-Wire End-Services
P2MP	engl. point-to-multipoint
QoS	engl. Quality of Service
RD	engl. Route Distinguisher
RIP	engl. Routing Information Protocol
RSVP-TE	ngl. Resource Reservation Protocol – Traffic Engineering
RT	engl. Route Target
RVSP	engl. Resource Reservation Protocol
SDH	engl. Synchronous Digital Hierarchy
SLA	engl. Service-Level Agreement
SNA	engl. Systems Network Architecture
SNMP	engl. Simple Network Management Protocol
SPF	engl. Shortest Path First
STM	engl. Synchronous Transport Modules
TCP/IP	engl. Transmission Control Protocol/Internet Protocol
TDM	engl. Time Division Multiplexed
TLS	engl. Transport Layer Security
ToS	engl. Type of Service
TTL	engl. Time to Live
VC	engl. Virtual Circuit
VLAN	engl. Virtual Local Area Network
VLL	engl. Virtual Leased Line
VoIP	engl. Voice over Internet Protocol
VPLS	engl. Virtual Private LAN services
VPN	engl. Virtual Private Network
VPRN	engl. Virtual Private Routed Network
VPWS	engl. Virtual Private WireService
VRF	engl. VPN routing and forwarding
VSI	engl. Virtual Switching Instance
WAN	engl. Wide-Area Network
WANDL	engl. Wide Area Network Design Laboratory
WiMAX	engl. Worldwide Interoperability for Microwave Access
xDSL	engl. x Digital Subscriber Line
XML	engl. eXtensible Markup Language

SAŽETAK

U ovom diplomskom radu opisana je arhitektura mreža pružatelja telekomunikacijskih usluga. Nadalje, definiran je način rada, ciljevi razvoja te prednosti primjene MPLS tehnologije. Također, definirani su osnovni elementi MPLS mreže, protokoli koji se primjenjuju za distribuciju oznaka i usmjeravanje paketa te neka od MPLS aplikacijskih proširenja. Budući da se MPLS VPN smatra najprihvaćenijim aplikacijskim proširenjem, opisane su njegove inačice po slojevima: MPLS Layer 3 VPN, MPLS Layer 2 VPN, Virtual Private Wire Service i Virtual private LAN service. Osim toga, opisan je proces planiranja mreže koji se sastoji od telekomunikacijskog predviđanja dimenzioniranja te tehnika upravljanja mrežnim prometom, pri čemu su opisana dva najčešće korištena alata za planiranje MPLS mreže: IP/MPLSView i iVNT. U praktičnom djelu rada odrađena je OSPF, MPLS i VPLS konfiguracija MikroTik-ova prema zadanoj testnoj mrežnoj topologiji (Slika 8.1.) te je omogućen pristup Internetu putem MikroTik-a P1.

Ključne riječi: pružatelj usluga; MPLS, VPN, protokoli, aplikacijska proširenja, planiranje mreže, IP/MPLSView, iVNT, OSPF, VPLS, MikroTik

ABSTRACT

This graduate thesis is based on trends according to Internet service provider's core networks – ISP, MPLS development, operation mode, some of it's development goals and advantages of it's application. Also, in this thesis are defined some of main elements of MPLS networks, main MPLS protocols which are used for distribution and routing, and some of MPLS application extensions. Since we consider MPLS VNP as most successful application extension, here are desribed his variants by layers: MPLS Layer 3 VPN, MPLS Layer 2 VPN, Virtual Private Wire Service and Virtual private LAN service. Beside that, this thesis is describing network planning process which consists of telecommunication predictions, dimensioning and traffic engineering whereby are described two most used tools for MPLS network planning: IP/MPLSView and iVNT. Practical part of this thesis consist of OSPF, MPLS and VPLS configuration of MikroTik's according to default network topology (picture 8.1.) and Internet access is enabled via MicroTik P1.

Keyword: service provider, MPLS, VPN, protocols, application extensions, network planning, IP/MPLSView, iVNT, OSPF, VPLS, MicroTik

ŽIVOTOPIS

Sara Pavin rođena je 23.10.1994. godine u Osijeku. Od rođenja živi u Podravskoj Moslavini, gdje stječe osnovnoškolsko obrazovanje u OŠ Ante Starčevića. Godine 2009. upisuje Opću gimnaziju u Donjem Miholjcu te sve razrede prolazi s vrlo dobrim uspjehom. Nakon završetka srednje škole i polaganja mature, 2013. godine upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, preddiplomski studij elektrotehnike, smjer Komunikacije i informatika. Nakon završenog preddiplomskog studija elektrotehnike 2016. godine upisuje diplomski studij - Mrežne tehnologije.