Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

USPOREDNA ANALIZA MPLS I SD-WAN MREŽNIH TEHNOLOGIJA

COMPARISON ANALYSIS OF MPLS AND SD-WAN TECHNOLOGIES

Mentor: doc. dr. sc. Ivan Grgurević

Studentica: Gabriela Barišić
JMBG: 0135237258

Zagreb, rujan 2019.

USPOREDNA ANALIZA MPLS I SD-WAN MREŽNIH TEHNOLOGIJA

SAŽETAK

MPLS i SD-WAN su tehnologije koje na različit način osiguravaju kvalitetu usluge. MPLS je mrežna tehnologija koja svojim načinom usmjeravanja mrežnih paketa osigurava uslugu s kraja na kraj za korisnika. S druge strane SD-WAN osigurava globalni pregled cijele mreže i centralno upravljanje čime se omogućava laka konfiguracija ili izmjena već postojeće konfiguracije sustava. Tema ovog diplomskog rada je komparativna analiza tih dviju mrežnih tehnologija tako što su prvo simulirane u programskom alatu GNS3, a zatim je obavljena i analiza mrežnog prometa. S obzirom na sve brži razvoj mrežnih tehnologija, dat je pregled SD-WAN tehnologije kao nove paradigme te njene potencijalne buduće primjene.

KLJUČNE RIJEČI: MPLS; SD-WAN; GNS3; softverski definirane mreže; simulacija mrežnih tehnologija; analiza mrežnog prometa

COMPARISON ANALYSIS OF MPLS AND SD-WAN TECHNOLOGIES

SUMMARY

MPLS and SD-WAN are technologies which with different approaches ensure quality of service. MPLS is network technology which with its routing of network packages manages to provide end-to-end service for user. On the other hand, SD-WAN gives global view on entire network and central management which enables simple configuration, or change of the existing configuration of system. The subject of this major thesis is comparative analysis these two network technologies by firstly simulating them in GNS3 software tool and then doing network traffic analysis. Considering rapid evolution of network technologies, it was also shown how will SD-WAN be potentially used as new paradigmi in future.

KEYWORDS: MPLS; SD-WAN; GNS3; software defined networks; network technology simulation; network traffic analysis

SADRŽAJ

1. Uvod

MPLS (engl. *Multi-Protocol Label Switching*) je tehnologija koja pruža novu metodu usmjeravanja IP paketa pri čemu se zadovoljava i razina kvalitete usluge. MPLS je postala popularna tehnologija za poboljšanje *Ethernet* povezanosti. Kako je skalabilnost i pouzdanost postala sve veća briga za tvrtke, posebno za one s podatkovnim centrima, MPLS je pružio korisnicima postavljanje prioriteta unutar usluge.

U usporedbi s tradicionalnim usmjeravanjem, gdje usmjernici analiziraju svaki paket i odlučuju rutu, MPLS koristi komutiranje labela gdje krajnji usmjernici određuju rutu sve do krajnje lokacije. Kao rezultat takvog usmjeravanja, usmjernici kroz mrežu ne trebaju pregledavati IP zaglavlje jer su sve informacije sadržane u labeli. MPLS je privatno upravljana okosnica, s toga osigurava visoku dostupnost, nisku latenciju te gubitak paketa. MPLS se danas smatra već starom tehnologijom, a sve nedostatke MPLS mreže nastoji adresirati nova tehnologija SD-WAN.

SD-WAN (engl. *Software defined WAN*) je nova paradigma koja iskorištava značajke softverski definiranih mreža u podatkovnim centrima, ali s primjenom na mrežu širokog područja te tvrtke i njihove podružnice. SD-WAN i SDN virtualiziraju resurse kako bi pružili bolje performanse, veću dostupnost i automatsko upravljanje mrežom. Pri tome, smanjuju se znatno troškovi naročito naspram MPLS tehnologije.

Osnovni princip rada softverski definiranih mreža je apstrakcija mrežnih sposobnosti, odnosno odvajaju se usluge mrežnog softvera od hardverskih WAN uređaja. SD-WAN odvaja funkcionalnost kontrolnog sloja i podatkovnog sloja. Kontrolni sloj donosi odluke o usmjeravanju, pa podatkovni sloj prenosi aplikacijske i korisničke podatke. Ovakav pristup pojednostavljuje kontrolu i upravljanje mreže.

Svrha diplomskog rada je utvrditi primjenjivost i upravljivost softverski definiranog WAN-a kao koncepta softverski definiranih mreža. Prepoznati će se uloga telekomunikacijskog operatora odnosno davatelja telekomunikacijskih usluga (engl. *Internet Service Provider* - ISP) s obzirom na broj direktnih *peeringa*, odnosno količinu podatkovnog prometa koja ide direktno između dva operatora bez posrednika. Javni *peering* kao što je *Internet exchange* (IX) osigurava optimalnu latenciju i sve ostale nužne parametre za stabilnu vezu, kao i otklanjanje eventualnih problema.

Cilj diplomskog rada je provesti usporednu analizu IP MPLS i SD-WAN mrežnih tehnologija prema različitim prepoznatim čimbenicima (upravljanje, latencija, kvaliteta usluge, cijena i dr.). Rad je podijeljen u sedam (7) poglavlja:

1. Uvod
2. Značajke IP MPLS-a
3. Značajke SD-WAN-a
4. Prednosti i nedostatci IP MPLS i SD-WAN mrežnih tehnologija

5. Studija slučaja: simulacija IP MPLS i SD-WAN mrežnih tehnologija u programskom alatu GNS3
6. Budući razvoj softverski definiranih mreža
7. Zaključak.

U prvom poglavlju, *Uvod*, definirana je tema koja se obrađuje u radu, napravljen je kratki uvod o tehnologijama MPLS i SD-WAN, definirani su cilj i svrha rada te su opisana poglavlja rada.

U drugom poglavlju, *Značajke MPLS-a*, definirana je tehnologija MPLS-a, njen način rada, razlika naspram tradicionalnog usmjeravanja te novi mehanizmi usmjeravanja koji osiguravaju pouzdani prijenos prometa. Opisani su mrežni elementi koji su potrebni za ostvarenje MPLS usluge te su definirani elementi paketa u MPLS mreži pri usmjeravanju.

U trećem poglavlju, *Značajke SD-WAN-a*, opisane su prvo softverske definirane mreže kao temelj SD-WAN-a. Nadalje, definirana je arhitektura SDN-a te je opisan OpenFlow standard. Nakon toga, definiran je SD-WAN, prikazana je njegova topologija i arhitektura te je obrađena uloga pružatelja usluga s obzirom na *peering* i IXP.

U četvrtom poglavlju, *Prednosti i nedostatci IP MPLS i SD-WAN mrežnih tehnologija*, definirane su glavne karakteristike MPLS i SD-WAN mrežnih tehnologija te su svrstane kao prednost ili nedostatak pojedine tehnologije kako bi se napravila usporedba istih.

U petom poglavlju, *Studija slučaja: simulacija IP MPLS i SD-WAN mrežnih tehnologija u programskom alatu GNS3*, napravljena je mrežna simulacija dvaju tehnologija koristeći programski alat GNS3. Pri simulaciji MPLS mrežne tehnologije, prikazana je konfiguracija preklopnika, a pri simulaciji SD-WAN mrežne tehnologije dodano je i Mininet okruženje za upravljanje cjelokupnom mrežom. Također, u ovom poglavlju napravljena je analiza mrežnog prometa koristeći programski alat *Wireshark* te Mininet okruženje.

U šestom poglavlju, *Budući razvoj softverski definiranih mreža*, napravljen je prikaz budućeg razvoja softverski definiranih mreža, predviđanja vezana uz tu tehnologiju te je napravljen pregled istraživanja o utjecaju SDN-a na druge tehnologije poput umjetne inteligencije i interneta stvari.

U posljednjem poglavlju, *Zaključku*, sustavno su prikazani glavni elementi rada te je donesen zaključak na temelju istraživanja provedenog kroz rad. Na kraju rada nalazi se popis kratica i akronima, te popis slika i tablica koje su prikazane u završnom radu.

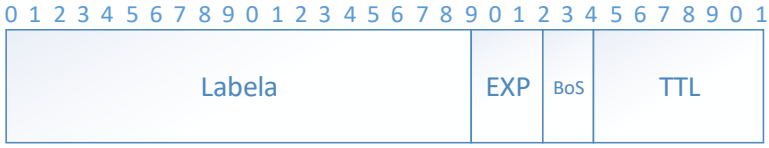
2. Značajke IP MPLS-a

Višeprotokolarno komutiranje labela (engl. *Multi-Protocol Label Switching* - MPLS) je je IETF standard temeljen na Ciscovom komutiranju oznaka (eng. *Tag switching*), a omogućava interoperabilnost s drugim proizvođačima mrežne opreme, [1]. U ovom poglavlju su definirane glave karakteristike i mehanizmi MPLS mrežne tehnologije poput načina usmjeravanja, elemenata labele, načina distribucije labela i slično.

2.1. Labela MPLS-a i stog labela

MPLS je mrežna tehnologija koja omogućava tradicionalno prosljeđivanje paketa kroz mrežu, ali na kvalitetniji i efikasniji način nego što su to omogućavale prijašnje tehnologije poput ATM-a i *Frame Relaya*. Naime, MPLS omogućava prosljeđivanje paketa kroz mrežu tako da se informacije u zaglavlju paketa analiziraju samo jednom, a daljnje prosljeđivanje se temelji na provjeravanju labela. Labele predstavljaju identifikacijske oznake paketa te su fiksne duljine, [2].

MPLS oznaka je 32-bitno polje s određenom strukturom koja je prikazana na slici 1. MPLS oznaka se naziva i *shim* zaglavlje.



Slika 1 Prikaz MPLS oznake

Izvor: [3]

Prvih 20 bita označavaju vrijednost labele. Vrijednost može biti između 0 i 2^{20} - 1, odnosno 1,048,575. Bitovi 20 do 22 su tri eksperimentalna (EXP) bita koji se isključivo koriste za kvalitetu usluge (engl. *Quality of Service* – QoS). EXP bitovi su bitni za upravljanje redovima te raspoređivanje posluživanja. Bit 23 je bit koji označava položaj u stogu te se naziva *Bottom of Stack* – BoS. Ovaj bit je 0, osim ako je posljednja labela u stogu, a u tom slučaju postavljen je na 1. Stog je kolekcija labela na paketu. Stog se može sastojati od samo jedne oznake ili ih može imati više. Bitovi 24 do 31 se koriste za *Time To Live* – TTL koji ima istu ulogu kao i u IP zaglavlju, [3].

Ponekad je potrebno za usmjernike, koji podržavaju MPLS, više od jedne oznake na paketu kako bi usmjerili taj paket kroz MPLS mrežu. To se radi tako se labele slažu u stog. Prva labela se naziva *top label*, a posljednja labela se naziva *bottom label*. Između njih moguće je imati neograničen broj labela. Neke MPLS aplikacije zahtijevaju više od jedne labele u stogu kako bi proslijedili označene pakete. Primjeri takvih MPLS aplikacija je MPLS VPN i AToM (engl. *Any Transport over MPLS - ATOM*), [3].

2.2. Enkapsulacija MPLS-a

Enkapsulacija linka na drugom sloju može biti bilo koja enkapsulacija koju Cisco IOS podržava, poput PPP ili Etherneta. Pretpostavljajući da je transportni protokol IPv4, enkapsulacija linka je PPP[1]. Stog labela je prisutan nakon PPP zaglavlja, ali prije IPv4 zaglavlja, [3].

Slika 2 Enkapsulacija MPLS označenog paketa

Izvor: [3]

S obzirom na to da je stog labela u okviru drugog sloja postavljen prije zaglavlja trećeg sloja ili nekog transportnog protokola, moraju se dodati nove vrijednosti za polje sloja podatkovne veze. Takve vrijednosti označavaju da je ono što prati zaglavlje drugog sloja je MPLS označeni paket. Polje protokola sloja podatkovne veze je vrijednost koja označava tip podatka kojeg okvir drugog sloja prenosi. Na slici 2 je prikazana enkapsulacija označenog paketa, [3].

2.3. MPLS i OSI referentni model

Kad je riječ o OSI referentom modelu i u kojem se sloju MPLS nalazi, MPLS nije moguće svrstati točno ni u jedan sloj. Naime, OSI referentni model se sastoji od sedam slojeva, a to su: fizički sloj, sloj podatkovne mreže, mrežni, transportni, sesijski, prezentacijski i aplikacijski sloj, [4].

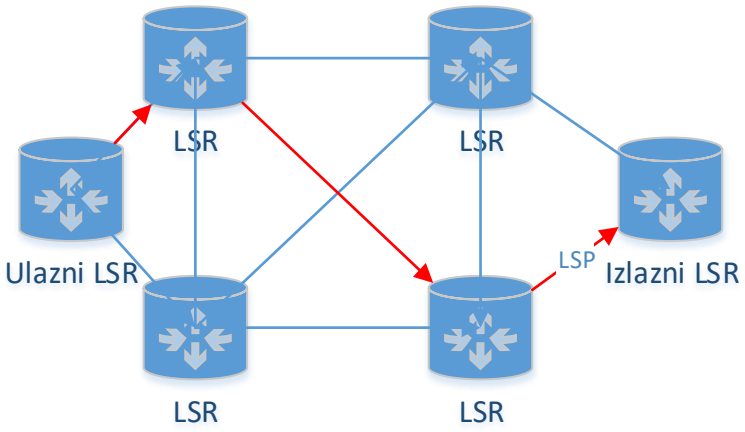
Donji sloj je prvi sloj, odnosno fizički sloj, a prvi ili sedmi sloj je aplikacijski sloj. Fizički sloj se brine o kabliranju, mehaničkim i električnim karakteristikama. Sloj podatkovne veze stvara okvire, a primjer toga je *Ethernet*, PPP ili *Frame Relay*. Značaj sloja podatkovne veze je samo na jednog vezi između dva uređaja. Odnosno, zaglavlje sloja podatkovne veze uvijek zamjenjuje uređaj na drugoj strani veze. Treći sloj, mrežni, se brine o formiranju paketa s kraja na kraj, [4].

MPLS nije protokol drugog sloja jer je enkapsulacija drugog sloja prisutna u označenim paketima. MPLS također nije zapravo nije protokol trećeg sloja jer je prisutan i protokol trećeg sloja. S toga, moglo bi se reći da se MPLS u OSI referentom modelu nalazi između drugog i trećeg sloja, tj. da je on 2.5 sloj, [4].

[1] PPP (engl. *Point-to-Point Protocol* - PPP) je mrežni protokol koji prenosi datagram između dva izravno povezana uređaja, [70].

2.4. MPLS mrežna domena

MPLS domena se sastoji od jednog ili više MPLS usmjernika za komutaciju labela (engl. *Label Switch Router* – LSR) koji pregledava i zamjenjuje MPLS labele paketa kako bi ih prosljeđivao kroz mrežu. LSR je bilo koji usmjernik ili preklopnik koji podupire prosljeđivanje MPLS-enkapsuliranih paketa temeljem samo ulaznog sučelja i informacije u *shim* zaglavlju. Kao što je prikazano na slici 3, postoje tri vrste LSR-a u mrežnoj domeni MPLS-a, a to su: ulazni LSR, izlazni LSR i srednji LSR, [5].

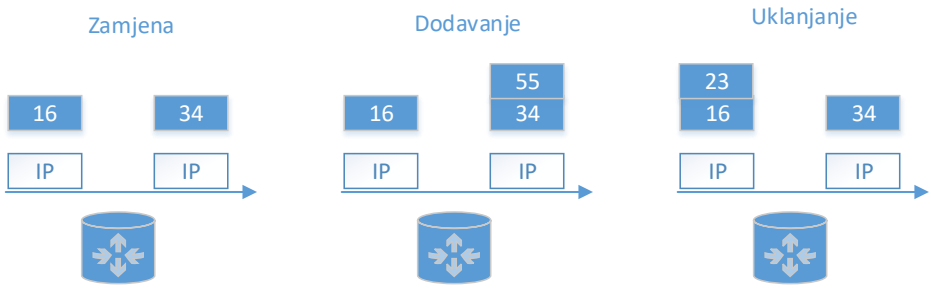


Slika 3 Mrežna domena MPLS-a

Izvor: [5]

LSR koji se nalazi na rubu MPLS domene te prosljeđuje promet unutar i izvan MPLS domene se naziva LER (engl. *Label Edge Router - LER*). LER je mjesto gdje se MPLS *shim* zaglavlje prvotno postavlja na nadolazeći paket i gdje se uklanja zaglavlje, a paket se prosljeđuje koristeći njegovu originalnu enkapsulaciju trećeg sloja. LER mora povezivati ulaznu tehnologiju s MPLS-om, tj. tunelirati ulazne tehnologije kroz MPLS mrežu tako što ih enkapsulira unutar MPLS paketa, [5]. LER se naziva izlazni LSR (engl. *egress LSR*) tamo gdje paket napušta MPLS domenu, a ulazni LSR (engl. *ingress LSR*) gdje paket ulazi u MPLS domenu, [6].

Kao što je prikazano na slici 4, LSR radi tri operacije: uklanjanje, zamjenu i dodavanje. Kada je označeni paket primljen, analizira se vrijednost labele pri vrhu stoga kako bi se odlučile dvije stvari: idući skok i izlazno sučelje na koje treba proslijediti paket te koja će se operacija izvesti na stogu labela prije prosljeđivanja paketa, [7].



Slika 4 Operacije koje obavlja LSR

Izvor: [3]

Operacija dodavanja (engl. *push*) dodaje novu labelu na IP paket ili na MPLS stog labela. Operaciju dodavanja obično obavlja ulazni LSR. Operacija zamjene (engl. *swap*) znači da se labela na vrhu zamjeni s drugom prije nego što se paket proslijedi na sljedeći LSR. Ovu operaciju najčešće obavljaju posrednički LSR-ovi. Operacija uklanjanja (engl. *pop*) uklanja labelu koja je na vrhu stoga labela kako bi se paket pripremio za krajnju destinaciju. Ovo najčešće obavlja izlazni LSR, [7].

2.5. *Label Switched Path*

LSP (engl. *Label Switched Path - LSP*) je niz LSR-ova koji komutiraju označene pakete kroz MPLS mrežu ili dio MPLS mreže. Odnosno, LSP je put kroz MPLS mrežu. Prvi LSR za LSP je ulazni LSR, a posljednji LSR za taj LSP je izlazni LSR. LSP je jednosmjeran put, [3].

LSP se najčešće kreira koristeći informacije o topologiji koje se nalaze u LSR bazi podataka za usmjeravanje. Kad se konvertira, baza podataka za usmjeravanja sadrži popis najkraćih puteva bez petlje unutar MPLS domene. Ove puteve koriste usmjerivački procesi za određivanje najkraćeg puta na kojeg se prosljeđuje promet. U kontekstu MPLS-a, ista informacija se može koristiti za kreiranje najkraćeg puta kroz MPLS domenu, osim što se umjesto prosljeđivanja prometa prema odredištu koristeći IP enkapsulaciju, promet enkapsulira koristeći MPLS zaglavlje i prosljeđuje se preko LSP-a. LSP se prvi put uspostavlja koristeći LDP protokol (engl. *Label Distribution Protocol - LDP*), [8].

2.6. *Forwarding Equivalence Class*

FEC (engl. *Forwarding Equivalence Class - FEC*) je grupa ili tok paketa koji se prosljeđuju istim putem i tretiraju se jednako u smislu prosljeđivanja. Svi paketi koji pripadaju istom FEC-u imaju istu labelu. Ipak, svi paketi koji imaju istu labelu ne pripadaju nužno istom FEC-u, zato što se njihove EXP vrijednosti i tretman prosljeđivanja mogu razlikovati. Ulazni LSR je usmjernik koji odlučuje koji paketi pripadaju kojem FEC-u, jer ulazni LSR klasificira i označuje pakete. Ovo su neki primjeri FEC-a:

- Paketi s odredišnom IP adresom i odgovarajućim prefiksom,
- *Multicast* paketi koji pripadaju određenoj grupi,
- Paketi s istim tretmanom prosljeđivanja temeljem prednosti ili DSCP poljem[2],
- Okviri nošeni kroz MPLS mrežu primljeni na jednom sučelju ulaznog LSR-a i prenošeni na sučelje izlaznog LSR-a,
- Paketi s odredišnim IP adresama koje pripadaju skupini BGP prefiksa s istim idućim BGP[3] skokom, [3].

2.7. Distribucija labela

Prva labela se postavlja na ulaznom LSR-u i labela pripada jednom LSP-u. Put paketa kroz MPLS mrežu je vezan za taj jedan LSP. Jedina promjena je što pri svakom skoku se promijeni labela koja je na vrhu u stogu. Ulazni LSR postavlja jednu ili više labela na paket. Posrednički LSR-ovi zamjenjuju labelu koja je na vrhu (ulazna labela) primljenog paketa s drugom labelom (odlazna labela) i prenose paket na izlazni link. Izlazni LSR tog LSP-a skida labele i prosljeđuje paket, [3].

Na primjeru jednostavnog IP MPLS-a, mreža se sastoji od LSR-ova koji pokreću IPv4 IGP[4]. Ulazni LSR pogleda odredišnu IPv4 adresu paketa, postavi labelu i proslijedi paket. Idući LSR primi označeni paket, zamijeni ulaznu labelu s izlaznom labelom te proslijedi paket. Izlazni LSR ukloni labelu i proslijedi IP paket bez labela na izlazni link. Kako bi ovo radilo, pridruženi LSR-ovi se moraju dogovoriti koju labelu koriste za svaki IGP prefiks. S toga, svaki posrednički LSR treba znati s kojom izlaznom labelom će zamijeniti ulaznu labelu. Odnosno, potrebni su mehanizmi koji će reći usmjernicima koje labele koristiti pri prosljeđivanju paketa. Labele su lokalne za svaki par pridruženih usmjernika i nemaju globalno značenje kroz mrežu. Kako bi usmjernici znali koja izlazna labela odgovara ulaznoj labeli potreban je distribucijski protokol LDP.

Distribucija labela je moguća na dva načina:

- *Piggyback* labela na postojeći IP usmjerivački protokol,
- Pokretanje odvojenog protokola za distribuciju labela [3].

2.7.1. Piggyback labela na postojeći IP usmjerivački protokol

Prednost ove metode je ta da nije potrebno pokretati novi protokol na LSR-ovima, ali svaki postojeći IP usmjerivački protokol mora biti proširen da nosi labele. Ovo nije uvijek

[2] DSCP (engl. *DiffServ Code Point* - DSCP) je 6-bitna oznaka u 8-bitnom polju za diferencijalne usluge u IP zaglavlju kako bi se definirao prioritet i kvalifikacija paketa, [71].
[3] BGP (engl. *Border Gateway Protocol* - BGP) je protokol za razmjenu usmjerivačkih informacija između usmjernika u različitim autonomnim sustavima, [72].
[4] IGP (engl. *Interior Gateway Protocol* - IGP) je protokol za razmjenu usmjerivačkih informacija između usmjernika unutar autonomnog sustava, a u tu skupinu spadaju OSPF, IS-IS i EIGRP.

jednostavno. Kad usmjerivački protokol prenosi labele, usmjeravanje i distribucija labela su uvijek sinkronizirane, odnosno ne može postojati labela ako nedostaje prefiks i obrnuto. Također eliminira potrebu za drugim protokolom koji će distribuirati labele. Na primjer, implementacija protokola s vektorom udaljenosti je izravna, jer svaki usmjernik kreira prefiks iz svoje tablice usmjeravanja. Usmjernik onda samo poveže labelu s tim prefiksom, [3].

Protokoli temeljeni na stanju veze ne funkcioniraju na takav način. Naime, svaki usmjernik kreira obavijesti o stanju veze koji se prenose svim usmjernicima u jednom području. Ovo je problem za MPLS, jer svaki usmjernik treba distribuirati labelu za svaki IGP prefiks, čak i kad nisu izvori tog prefiksa. Protokoli temeljeni na stanju veze trebaju biti promijenjeni kako bi se ovo napravilo. Činjenica da usmjernik treba kreirati labelu za svaki prefiks kojeg oni nisu oni kreirali je kontraproduktivna načinu na koji protokoli temeljeni na stanju veze rade. Dakle, za protokole koji se temelje na stanju veze, preporuča se primjena odvojenog protokola za distribuciju labela, [3].

2.7.2. Pokretanje odvojenog protokola za distribuciju labela

Druga metoda je pokretanje odvojenog protokola za distribuciju labela, a njena prednost je ta da je neovisan o usmjerivačkom protokolu. Bez obzira na to koji je IP usmjerivački protokol i može li distribuirati labele, odvojeni protokol distribuira labele te prepušta usmjerivačkom protokolu da distribuira prefikse. Nedostatak ove metode je to što se treba implementirati na LSR-ove, [3].

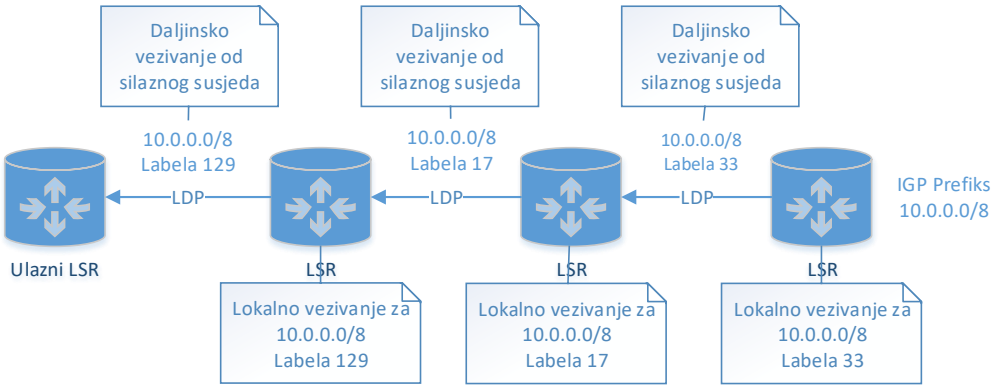
Izbor svih proizvođača usmjernika je bio da novi protokol distribuira labele za IGP prefikse. To je LDP, ali nije i jedini protokol koji može distribuirati MPLS labele. Postoji više različitih vrsta protokola distribuiraju labele:

- *Tag Distribution Protocol* (TDP),
- *Label Distribution Protocol* (LDP),
- *Resource Reservation Protocol* (RSVP), [3].

2.7.3. Distribucija labela primjenom LDP-a

Za svaki IGP IP prefiks u svojoj IP usmjerivačkoj tablici, svaki LSR kreira lokalno vezivanje, tj. spaja labelu s IPv4 prefiksom. LSR tada distribuira ovo vezivanje svim LDP susjedima. Ova primljena vezivanja postaju daljinska vezivanja. Susjedi pohranjuju daljinska i lokalna vezivanja u posebnu tablicu koja se naziva LIB (engl. *Label Information Base - LIB*), [3].

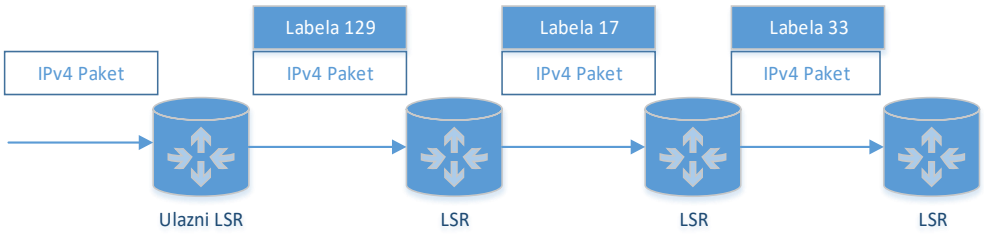
LIB je softverska tablica koju održavaju MPLS usmjernici kako bi pohranili detalje o portovima i odgovarajućim MPLS labelama koje se trebaju pridodati ili ukloniti na ulaznim ili izlaznim MPLS paketima. Zapise u tablici unosi LDP, [9].



Slika 5 IP MPLS mreža s LDP protokolom

Izvor: [3]

Tablica usmjeravanja odlučuje koji je idući skok IPv4 prefiksa. LSR na temelju informacija u primljenom daljinskom vezivanju, definira tablicu o informacijama prosljeđivanja (engl. *Label Forwarding Information Base* – LFIB)[5]. U toj tablici, labela iz lokalnog vezivanja služi kao ulazna labela, a labela iz daljinskog vezivanja služi kao izlazna labela. Dakle, kad LSR primi označeni paket, u mogućnosti je zamijeniti ulaznu labelu s izlaznom labelom koja je dodijeljena s uparenim idućim LSR-om. Na slici 5 je prikazan rad LDP-a pri vezivanju između LSR-ova za IPv4 prefiks 10.0.0.0/8. Svaki LSR raspoređuje jednu labelu po IPv4 prefiksu. Lokalno vezivanje je jedan prefiks i njegova dodijeljena labela, [3].



Slika 6 IP MPLS mreža s LDP protokolom: komutiranje paketa

Izvor: [3]

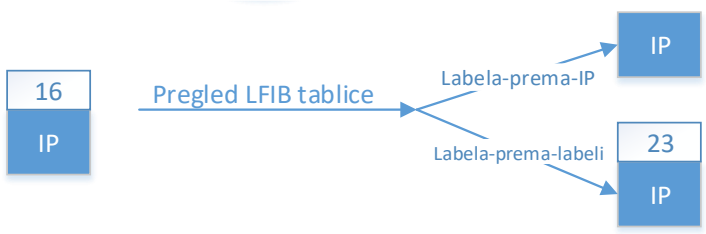
Na slici 6 prikazan je IPv4 paket s odredištem 10.0.0.0/8 kako ulazi u MPLS mrežu na ulazni LSR gdje mu se postavlja labela 129 i komutira se prema idućem LSR-u. Drugi LSR zamjenjuje ulaznu labelu 129 s izlaznom labelom 17 i prosljeđuje paket prema trećem LSR-u. Treći LSR zamjenjuje ulaznu labelu 17 s izlaznom labelom 33, itd.

[5] LFIB je tablica za prosljeđivanje označenih paketa, a sastoji se od ulaznih i izlaznih labela za LSP. LFIB odabire samo jednu od svih potencijalnih izlaznih labela od svih potencijalnih daljinskih vezivanja u LIB te ih pohranjuje. Daljinska labela se odabire na kriteriju najboljeg puta prema tablici usmjeravanja, [3].

2.8. Prosljeđivanje označenih paketa

Pregledom labele koja se nalazi na vrhu primljenog označenog paketa i odgovarajućeg zapisa u LFIB, LSR zna kako proslijediti paket. LSR određuje koju operaciju treba obaviti (zamjena, dodavanje ili uklanjanje) i koji je idući skok na kojeg treba proslijediti paket.

Kada usmjernik primi IP paket, putem LFIB-a paket može napustiti usmjernik označen ili neoznačen, a LFIB tablica je prikazana na slici 7 ispod, [3].



Slika 7 LFIB tablica načini usmjeravanja

Izvor: [3]

Na slici 8 je prikazana LFIB tablica, s koje se može vidjeti primjer slučajeva prosljeđivanja labela-prema-labeli i labela-prema-IP, [3].

```
lactometer#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Untagged    10.1.1.0/24      0          Et0/0/0     10.200.200.2
17     16          10.200.202.0/24  0          Et0/0/0     10.200.200.2
18     Pop tag     10.200.203.0/24  0          Et0/0/0     10.200.200.2
19     Pop tag     10.200.201.0/24  0          Et0/0/0     10.200.200.2
20     18          10.200.254.4/32  0          Et0/0/0     10.200.200.2
21     Pop tag     10.200.254.2/32  0          Et0/0/0     10.200.200.2
22     17          10.200.254.3/32  0          Et0/0/0     10.200.200.2
24     Untagged    l2ckt(100)       4771050    Fa9/0/0     point2point
```

Slika 8 Prikaz LFIB tablice, [3]

Naime, lokalna labela je labela koju LSR dodijeli i distribuira prema drugim LSR-ovima. Kao takav, ovaj LSR očekuje označene pakete da dođu do njega s ovim labelama na vrhu stoga. Ako LSR primi označi paket s labelom 22 na vrhu, on će zamijeniti labelu s labelom 17 i proslijediti je na sučelje *Ethernet0/0/0*.

Ako LSR primi paket s labelom 16 na vrhu, on uklanja sve labele i prosljeđuje paket kao IP paket, jer je izlazna labela u tablici *Untagged*. Ovo je primjer labela-prema-IP slučaja. Ako LSR primi paket s labelom 18 na vrhu, on uklanja labelu i prosljeđuje paket kao označeni ili kao IP paket.

Labele 0 do 15 su rezervirane labele. Njih ne može koristiti LSR pri normalnom slučaju za prosljeđivanje paketa. LSR dodjeljuje posebnu funkciju svakoj od ovih labela. Labela 0 je

eksplicitna NULL labela, a labela 3 je implicitna NULL labela. Labele 1 i 14 su za upozorenja, a ostale rezervirane labele još nisu dodijeljene, [10].

Osim rezerviranih labela, sve ostale vrijednosti labela se mogu koristiti za prosljeđivanje paketa. S obzirom na to da labela ima 20 bita, labele od 16 do 1 048 575 se koriste za normalno prosljeđivanje paketa, [10].

2.9. Label Distribution Protocol

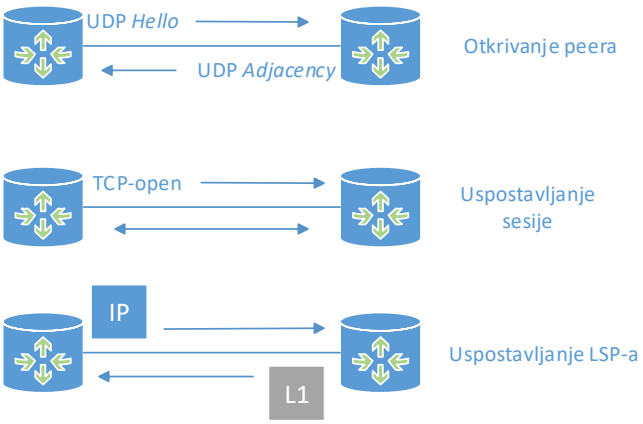
Kako bi se paketi prenijeli preko LSP-a kroz MPLS mrežu, LSR mora pokretati LDP. Kad svi LSR-ovi imaju labele za pojedinačni FEC, paketi se mogu proslijediti na LSP. Operacije labela (dodavanje, zamjena i uklanjanje) su poznate za svaki LSR koji pogleda u LFIB. LFIB je tablica koja prosljeđuje označene pakete, a puni se pridruženim labelama pronađenim u LIB-u. LIB se puni pridruženim labelama koje primi od LDP-a, [3].

Dva LSR-a koja koriste LDP za razmjenu labela su poznati kao LDP sudionici (engl. *peers*) te među njima postoji LDP sesija. Komunikacija pri LDP sesiji je dvosmjerna. Postoje četiri kategorije LDP poruka:

- Poruke otkrivanja koje najavljuju i održavaju prisutnost LSR-a u mreži,
- Sesijske poruke koje uspostavljaju, održavaju i prekidaju sesije između LDP sudionika,
- Poruke oglašavanja koje kreiraju, mijenjaju i brišu mapiranja labela za FEC,
- Obavijesti koje pružaju savjetodavne informacije i signalizacijske informacije o kvaru, [11].

Otkrivanje LDP-a je mehanizam pomoću kojeg LSR otkriva potencijalne LDP sudionike te ono može biti osnovni i prošireni. Osnovni mehanizam služi za otkrivanje LSR susjeda koji su izravno povezani na link razini, a prošireni mehanizam služi za lociranje LSR-ova koji nisu izravno povezani na link razini. Obadva mehanizma se temelje na razmjeni *Hello* i *Adjacency* poruka, [11].

Razmjena LDP poruka između dva LSR-a je okidač za uspostavljanje sesije. Sesija se ostvaruje u dva koraka: uspostava transportne veze i inicijalizacija sesije, [11]. Nakon što se uspostavi sesija, moguće je započeti mapiranje labela. Cijeli proces je prikazan na slici ispod.



Slika 9 LDP koraci

Izvor: [12]

MPLS arhitektura dozvoljava LSR-u distribuciju FEC labela kao odgovor na eksplicitni zahtjev od drugog LSR-a. Ovo je poznato kao silazno preuzimanje na zahtjev (engl. *Downstream on Demand*). Drugi način, netraženo silazno preuzimanje (engl. *Unsolicited Downstream*), omogućava da LSR može distribuirati vezivanja labela LSR-ovima koji ih nisu eksplicitno zahtijevali, [11].

Obje distribucijske tehnologije mogu biti korištene u istoj mreži u isto vrijeme. Ipak, za bilo koju datu LDP sesiju, svaki LSR mora poznavati distribucijsku metodu labela koju koristi njegov sudionik, [11].

3. Značajke SD-WAN-a

WAN (engl. *Wide Area Network - WAN*) je mreža koja se prostire preko većeg geografskog područja. WAN povezuje manje mreže, uključujući LAN-ove (engl. *Local Area Network - LAN*), [13]. SD-WAN (engl. *Software-Defined WAN – SD-WAN*) je specifična primjena tehnologije softverski definiranih mreža na WAN konekcije poput širokopojasnog interneta ili LTE-a[6]. On povezuje korporacijske mreže, uključujući podružnice i podatkovne centre, na velikim geografskim udaljenostima, [14]. U ovom poglavlju opisane su glavne značajke SD-WAN tehnologije, načini implementacije te topologija i arhitektura SD-WAN mrežne tehnologije.

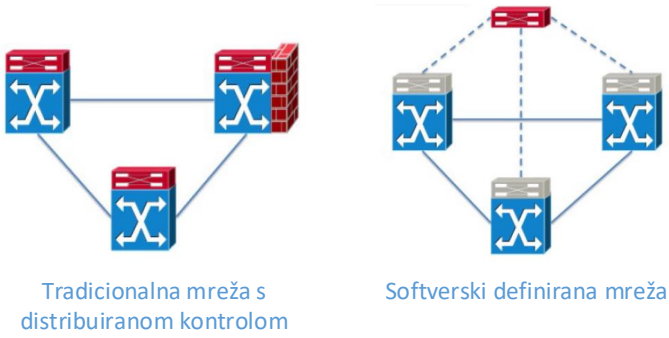
3.1. Softverski definirane mreže

Jedan od velikih problema današnje mrežne infrastrukture je vertikalna integracija mrežnih uređaja, odnosno proizvođač pruža hardver i softver koji se ne mogu prilagođavati korisniku. Drugi problem je što ne postoji globalni pogled na mrežu u velikim sustavima. Današnji usmjernici komuniciraju jedni s drugima i nisu u mogućnosti odabrati put iz globalnog pogleda, [15].

SDN je nova mrežna paradigma koja predstavlja primjer programskih mreža čija je temeljna ideja odvajanje upravljačkog dijela od podatkovnog dijela. Upravljački dio je sva logika koja odlučuje što se treba učiniti i daje instrukcije podatkovnom dijelu kako implementirati odluku. Upravljački dio sadrži kontrolno i usmjeravajuće ponašanje poput praćenje topoloških promjena, instalacija pravila prosljeđivanja, izračunavanje ruta, itd. Podatkovna razina prosljeđuje promet na temelju pravila koje je odredio upravljački dio. Centralizirani upravljački dio se naziva kontroler te on upravlja sa svim podatkovnim dijelovima te se softverski instalira u hardver, [15].

S druge strane, mrežni uređaji postaju jednostavni uređaji za prosljeđivanje paketa (podatkovni dio) koji se može programirati preko otvorenog sučelja poput *ForCES* i *OpenFlow*. Na slici 10, prikazana je usporedba tradicionalne mreže i SDN-a. Pune linije na slici predstavljaju linkove podatkovnog sloja, a isprekidane linije predstavljaju linkove kontrolnog sloja. Iz slike se vidi odvajanje ta dva sloja te jednostavnije mrežno upravljanje kod SDN-a, [16].

[6] LTE (engl. *Long Term Evolution* - LTE) je posljednja generacija mobilnih komunikacijskih tehnologija, a karakteriziraju je veće prijenosne brzine korisničkih podataka i spektralna efikasnost, [73].



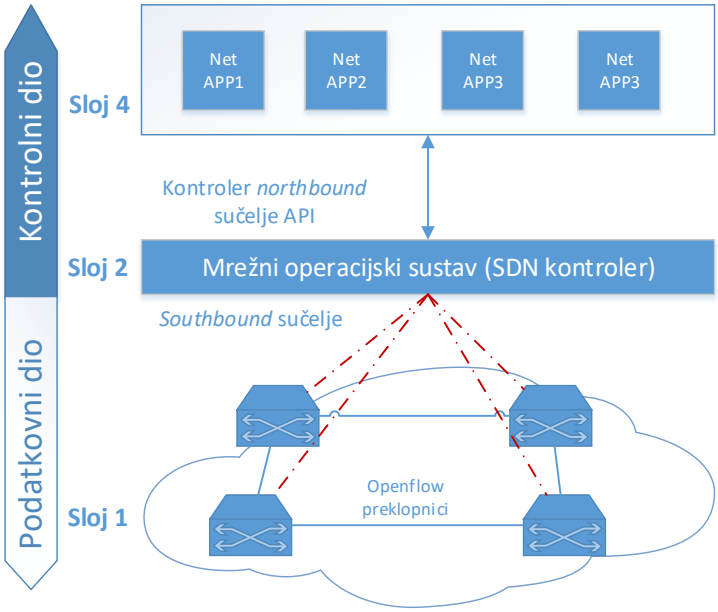
Slika 10 Usporedba tradicionalne mreže i SDN-a

Izvor: [16]

Ovo odvajanje daje globalni pregled mreža gdje kontroler može vidjeti status svih usmjernika i preklopnika te efikasno odlučiti koja je ruta najbolja. Uz to, omogućena je horizontalna integracija mreže što znači da se hardver i softver mogu odvojeno i nezavisno implementirati u mrežu, [17].

3.1.1. Arhitektura softverski definiranih mreža

SDN arhitektura se može podijeliti u 3 sloja kao što je prikazano na slici 11. Ovakva arhitektura SDN mreža je temeljena na definicijama SDN-a prema *Open Networking Foundation* (ONF)[7].



Slika 11 Slojevita arhitektura SDN mreže

Izvor: [18]

[7] ONF je Američka zaklada koja okuplja vodeće telekomunikacijske operatore i proizvođače opreme kako bi surađivali na izgradnji SDN principa koristeći otvorene platforme i definirane standarde, [26].

Prvi sloj je sloj infrastrukture koji se naziva i podatkovnim dijelom, a sastoji se od mrežnih elemenata za prosljeđivanje. Odgovornosti ovog sloja su prosljeđivanje podataka, praćenje lokalnih informacija i prikupljanje statistika, [19].

Na sloju iznad se nalazi kontrolni sloj. On je odgovaran za programiranje i upravljanje sloja za prosljeđivanje. Kako bi to ostvario, koristi informacije koje mu pruža prvi sloj. Također, obuhvaća jedan ili više softverskih kontrolera koji komuniciraju s mrežnim elementima za prosljeđivanje kroz standardizirana sučelja koja se nazivaju *southbound* sučelja. *OpenFlow*, koji je jedan od najčešće korištenih *southbound* sučelja se najviše sastoji od preklopnika, gdje neka druga SDN rješenja koriste i usmjernike, [19].

Posljednji sloj je aplikacijski sloj koji sadrži mrežne aplikacije. One mogu uvesti nove mrežne značajke kao što su sigurnost i upravljanje, sheme prosljeđivanja ili pomoć kontrolnom dijelu pri mrežnoj konfiguraciji. Aplikacijski sloj može prihvatiti apstraktni i globalni pogled mreže od kontrolera i koristiti tu informaciju kako bi dao prikladno navođenje kontrolnom sloju. Sučelje između aplikacijskog sloja i kontrolnog sloja se naziva *northbound* sučelje, [19].

SDN kontroler je centralni uređaj za pregled mreže, implementaciju politika, kontrolu SDN uređaja koji čine cijelu infrastrukturu te pruža *northbound* API[8] za aplikacije. Jezgrene značajke kontrolera su:

- Otkrivanje krajnjih korisničkih uređaja poput laptopa, mobilnih uređaja i sl.
- Otkrivanje mrežnih uređaja koji sačinjavaju mrežnu infrastrukturu poput preklopnika, usmjernika, itd.
- Upravljanje topologijom mrežnih uređaja – održavanja informacije o međusobnoj povezanosti mrežnih uređaja i povezanost s krajnjim uređajima.
- Upravljanje tokom – održavanje baze podataka o tokovima koje upravlja kontroler i obavljanje potrebne koordinacije s uređajima kako bi se sinkronizirali.

Kontroler također održava *flow cache* koji zrcali tablice toka na različitim preklopnicima koje on kontrolira, [20].

Northbound API sučelje se koristi za komunikaciju SDN kontrolera s uslugama i aplikacijama koje su na mreži. *Northbound* API se može koristiti za efikasnu orkestraciju i automatizaciju mreže kako bi ju se prilagodilo različitim potrebama aplikacija. Važnost ovog API-ja je u tome da je čitava vrijednost SDN-a zapravo povezana s potencijalnom podrškom različitih inovativnih aplikacija, [21].

Southbound API sučelje omogućava pristup elementima podatkovnog dijela za konfiguraciju, kontrolu i praćenje kroz standardizirane protokole kako bi se nosili s heterogenim elementima i proizvođačima podatkovnog dijela. Glavna funkcija *southbound* sučelja je komunikacija između SDN kontrolera s mrežnim čvorovima (fizičkim i virtualnim preklopnicima ili usmjernicima) tako da uređaji mogu definirati mrežnu topologiju, mrežne tokove i implementirati zahtjeve od strane *northbound* API-ja, [22].

[8] API (engl. *Application Program Interface* - API) je skup pravila i alata za kreiranje softverskih aplikacija. API definira građevne blokove za razvoj programa, a koriste se pri programiranju komponenti grafičkog sučelja, [74].

ForCES predlaže pristup fleksibilnom mrežnom upravljanju bez mijenjanja mrežne arhitekture. *OpFlex* distribuira dio upravljačkih elemenata na uređaje za prosljeđivanje kako bi dao dio inteligencije podatkovnom dijelu. *Protocol oblivious forwarding* (POF) cilja na to da SDN dio prosljeđivanja ne bude vezan za protokol tako što se postavi set generičkih instrukcija o toku. Najpoznatije *soutbound* API rješenje je *OpenFlow* koji će se detaljnije obraditi u idućem odlomku, [23].

3.1.2. OpenFlow

OpenFlow je specifikacija protokola koja opisuje komunikaciju između *OpenFlow* preklopnika i *OpenFlow* kontrolera. Osnovne operacije *OpenFlow* rješenja su:

- Kontroler popunjava preklopnike zapisima tablice toka.
- Preklopnik evaluira zaglavlja ulaznih paketa i pronalazi podudarajući tok, a zatim obavlja asociranu akciju. Ovisno o kriteriju podudaranja, evaluacija počinje na drugom sloju zaglavlja te se onda potencijalno nastavlja do četvrtog sloja.
- Ako nije pronađeno podudaranje, preklopnik proslijedi paket kontroleru.
- Najčešće će kontroler ažurirati preklopnik s dolaskom novih entiteta toka kad se prime novi uzorci paketa kako bi s njima upravljao preklopnik, [20].

U *OpenFlow* standardu, tablice prosljeđivanja se nazivaju tablice toka. Ove tablice definiraju kako se okvir prosljeđuje iz preklopnika ili usmjernika u mreži. Tablice toka spajaju specifična polja zaglavlja (npr. IP adresa odredišta) i kad se dogodi preklapanje, okvir se prosljeđuje na određeni izlazni port. *OpenFlow* 1.0 specifikacija je definirala 12 polja zaglavlja okvira koji bi se trebali koristiti pri spajanju u tablici toka. *OpenFlow* kontroler treba popuniti ta polja u tablici tokova za svaki preklopnik koristeći API, [24].

Postoje tri klase komunikacije u *OpenFlow* protokolu:

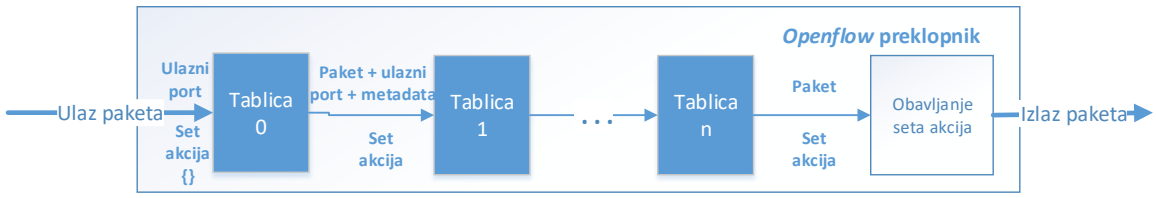
- Kontroler-prema-preklopniku,
- Asinkrona komunikacija,
- Simetrična komunikacija.

Komunikacija kontroler-prema-preklopniku je odgovorna za otkrivanje značajki i konfiguracije te programiranje preklopnika. Asinkronu komunikaciju inicira *OpenFlow* preklopnik bez zahtjeva kontrolera. Ona se koristi za obavještavanje kontrolera o dolascima paketa, promjenama stanja na preklopniku i pogreškama. Na posljetku, simetrične poruke se šalju bez zahtjeva s obje strane, odnosno i preklopnik i kontroler slobodno mogu inicirati komunikaciju bez zahtjeva druge strane. Primjeri simetrične komunikacije su *hello* ili *echo* poruke koje se šalju za provjeru je li kontrolni kanal dostupan, [25].

Kada preklopnik primi paket, on analizira zaglavlje paketa koje se uspoređuje s tablicom toka. Ako je pronađen zapis u tablici toka gdje se *wildcards* podudaraju, taj zapis se uzima u obzir. Ukoliko je pronađeno više zapisa, paketi se uspoređuju na temelju prioriteta, tj. odabire se zapis koji je najspecifičniji ili onaj koji ima *wildcard* s najvišim prioritetom, [25].

Paketi se procesiraju koristeći cjevovod tablica usmjeravanja. Kao što je prikazano na slici 12, to je skup organiziranih tablica usmjeravanja. Kad se paket podudara, ulaz se sastoji od paketa, identifikatora ulaza, pridruženih vrijednosti metapodataka te seta aktivnosti. Za tablicu 0, vrijednost metapodatka je prazna i radnje je nula. Obrađivanje podatka se dalje obavlja na idući način:

- Prvo se pronalazi najveći prioritet podudaranja, a ako se ne podudara ni s jednim ulazom, paket se ispušta. Ako se podudaraju samo na ulazu propuštanja tablice, tada se mogu dogoditi tri radnje:
  - slanje paketa na kontroler,
  - prosljeđivanje paketa prema sljedećoj tablici ili
  - ispuštanje paketa.
- Ako se podudara s barem još jednim ulazom osim ulaza u tablicu, to se podudaranje smatra kao ulaz s najvećim prioritetom podudaranja. Tada su moguće iduće radnje:
  - Ažuriranje svih brojila povezanih s ovim ulazom,
  - Izvršavanje svih uputa povezanih s ovim ulazom,
  - Paket se prosljeđuje prema sljedećoj tablici u cjevovodu.



Slika 12 Openflow cjevovod tablica usmjeravanja

Izvor: [26]

Posljednja tablica u cjevovodu ne može prosljeđivati paket dalje. Kad se paket usmjeri na izlazni port, izvršava se dodijeljeni set aktivnosti, [26].

3.2. Definicija SD-WAN-a

U današnjem korporacijskom okruženju, velika je potražnja za adaptacijom pri mobilnom i IoT[9] prometu, SaaS[10] aplikacijama te *cloud* rješenjima. Nadalje, sigurnosni zahtjevi se povećavaju, a aplikacije trebaju prioritetni pristup i optimizaciju. Pri tome, kako kompleksnost sustava raste, postoji i potreba za smanjenjem troškova, [27].

Tradicionalna uloga WAN mreže je povezivanje korisnika u poslovnici ili na kampusu s aplikacijama koje su pohranjene na servere u podatkovnim centrima. Takve naslijeđene WAN tehnologije se najčešće sastoje od više MPLS transporta gdje je Internet ili SaaS promet

[9] IoT (engl. *Internet of Things* - IoT) je nova paradigma koja opisuje povezivanje fizičkih objekata na Internet te njihovu međusobnu komunikaciju koristeći različite tehnologije, [75].
[10] SaaS (engl. *Software as a Service* - SaaS) je model *cloud* usluge gdje je korisniku pružena aplikacija pokrenuta na *cloud* infrastrukturi, [76].

prenošen okosnicom do podatkovnog centra ili regionalnog središta za pristup Internetu. Ovakav pristup više nije poželjan s obzirom da se aplikacije premještaju s podatkovnih centara u cloud što pruža korisnicima veću mobilnost. Nadalje, problemi s takvom arhitekturom su nedovoljna propusnost s visokim troškovima, vrijeme nedostupnosti aplikacije, loš SaaS performans, kompleksne operacije i procesi za cloud povezanost i sigurnosne poteškoće mreže, [27].

SD-WAN rješenja su evoluirala da riješe ove probleme. SD-WAN je dio šire tehnologije SDN koja je opisana u prošlom odlomku. Obadvije su softverski-definirane tehnologije, ali SDN je namijenjen za interne podatkovne centre na kampusima, a SD-WAN iskorištava slične softverski-definirane koncepte odvajanja kontrolnog i podatkovnog dijela na WAN mrežu. Gartner definira SD-WAN s četiri karakteristike:

- Podržava različite tipove povezivanja poput MPLS-a, Interneta, LTE, itd.,
- Ima sposobnost dinamičkog odabira puta, odnosno podjela tereta na WAN konekcije,
- Pruža jednostavno sučelje za upravljanje mrežom,
- Treba podržavati VPN-ove[11] kao i druge usluge treće strane, [28].

Još jedna važna karakteristika SD-WAN tehnologije je ZTP (engl. *Zero touch provisioning - ZTP*). To je karakteristika preklopnika koja omogućava automatsku konfiguraciju. Naime, kad se preklopnik upali, šalje DHCP[12] zahtjev kako bi dobio lokaciju centralno pohranjene slike i konfiguracije, koju onda preuzme i pokrene, [29].

Ne postoji jedinstven pristup SD-WAN tehnologijama sa stajališta proizvođača. Na primjer, *Silver Peak* se fokusira na akceleraciju SaaS aplikacija u *cloudu*. *VMware* je napravio vlastiti *VeloCloud* proizvod koji sadrži rubne aplikacije, orkestraciju i *cloud* pristupnike. *Aryaka* je izgradila globalnu mrežu gdje tvrtke mogu koristit WAN u obliku mreže kao usluge. S druge strane, *Cisco* i *Riverbed* se fokusiraju na WAN optimizaciju i rubne WAN opcije, [14].

3.3. Tipovi implementacije SD-WAN-a

Prema [30], postoje tri osnovna tipa implementacije SD-WAN tehnologije na tržištu. Ovisno o potrebama globalnih korisnika i aplikacija, potrebno je odabrati najbolju implementaciju:

- SD-WAN temeljen na Internetu,
- Upravljana usluga SD-WAN-a ili
- SD-WAN kao usluga.

[11] VPN (engl. *Virtual Private Network* - VPN) je privatna mreža koja koristi enkripciju i druge sigurnosne mehanizme za osiguranje autoriziranim korisnicima pristup mreži. Ovakva mreža je dizajnirana kao siguran tunel za prijenos podataka između udaljenog korisnika i korporacijske mreže, [77].
[12] DHCP (eng. *Dynamic Host Configuration Protocol* - DHCP) je protokol koji osigurava automatsko i centralno upravljanje distribucijom IP adresa kroz mrežu, [78].

SD-WAN temeljen na Internetu se implementira na korisničkoj lokaciji (engl. *on premise*). Mrežni promet se prosljeđuje preko naslijeđenih MPLS linkova ili Interneta. Ovaj način olakšava povezivanje sa SaaS aplikacijama, ali kašnjenja i gubitci paketa ovise o javnom Internetu te se povećaju s udaljenošću.

Pri upravljanoj usluzi SD-WAN-a, korisnik plaća pružatelju usluge da instalira i pruži povezanost, kao i uređaje koje usluga zahtjeva. Upravljana usluga SD-WAN-a je usluga s dodanom vrijednošću i može doći sa SLA[13]. Ova usluga se također oslanja na javni Internet za pristup SaaS aplikacijama što znači da performanse aplikacija mogu biti lošije s povećanjem udaljenosti.

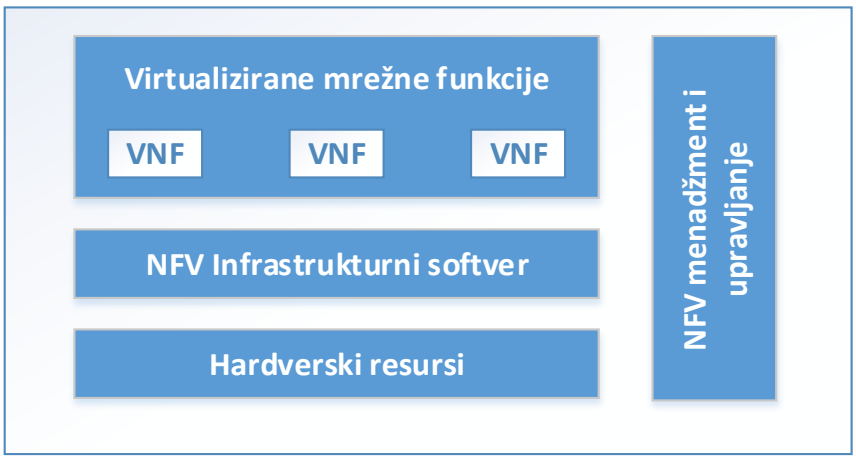
SD-WAN kao usluga je implementacijski model proizvođača Aryaka koji se temelji na ideji da korisnici ostvare SD-WAN povezanost na isti način na koji kupuju *cloud* usluge.

3.4. SD-WAN i virtualizacija mreže

NFV (engl. *Network Functions Virtualization - NFV*) je tehnologija koja omogućava odvajanje mrežnih funkcija od njihovih dodijeljenih hardverskih uređaja te implementacija tih funkcija kao softverskih komponenti u potpuno virtualizirane mrežne infrastrukture. NFV je komplementaran softverski definiranim mrežama, mada su zapravo neovisni jedni od drugih. SDN osigurava mrežnu jednostavnost i resursnu fleksibilnost nižih slojeva (L2-L4), a NFV izbjegava isključivosti proizvođača te pruža resursnu fleksibilnost viših slojeva (L4-L7). S obzirom da standard *OpenFlow* izbjegava isključivost proizvođača, beneficije povezane implementacije ovih tehnologija je očigledna, [31].

Kao što je prikazano na slici, NFV su VNF-ovi (engl. *Virtual Network Functions - VNF*) koji upravljaju specifičnim mrežnim funkcijama. Individualni VNF-ovi mogu biti povezani ili spojeni skupa kao građevni blokovi kako bi se kreiralo potpuno virtualizirano okruženje. VNF-ovi su pokrenuti na virtualnim mašinama (VM) na hardveru mrežne infrastrukture, [32].

[13] SLA (engl. *Service Level Agreement* - SLA) je sporazum dvaju ili više stranki koji određuje karakteristike usluga, cijena, model naplate i dostupnost usluge, [79].



Slika 13 Grafički prikaz NFV i VNF

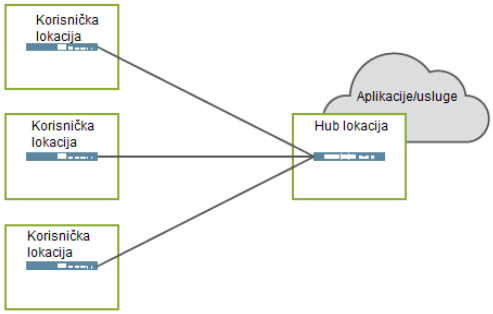
Izvor: [33]

Prema *VeloCloud*-u, odvojeni kontrolni i podatkovni sloj SD-WAN mreže predstavlja implementaciju SDN i NFV arhitektura. Centralni orkestrator (kontroler) predstavljaju kontrolni sloj, a rubovi i pristupnici predstavljaju podatkovni sloj. Orkestrator održava globalni pregled mreže i programira rubove koji mogu prilagođeni ili generički (VNF) hardver raspoređen na udaljene lokacije. Rubovi uče rute što omogućava centralno donošenje odluka s udaljenim izvođenjem od strane ruba. Ova arhitektura osigurava dostupnost ako je orkestrator ili pristupnik nedostupan, pa rubni uređaj može donijeti lokalnu odluku temeljem posljednjih instrukcija, [33].

3.5. Topologija SD-WAN-a

U ovom poglavlju će biti prikazane dvije vrste topologije SD-WAN-a prema definicijama mrežnog proizvođača Juniper.

Prva vrsta topologije je *hub-and-spoke* koja je prikazana na slici 14. *Spoke* predstavlja

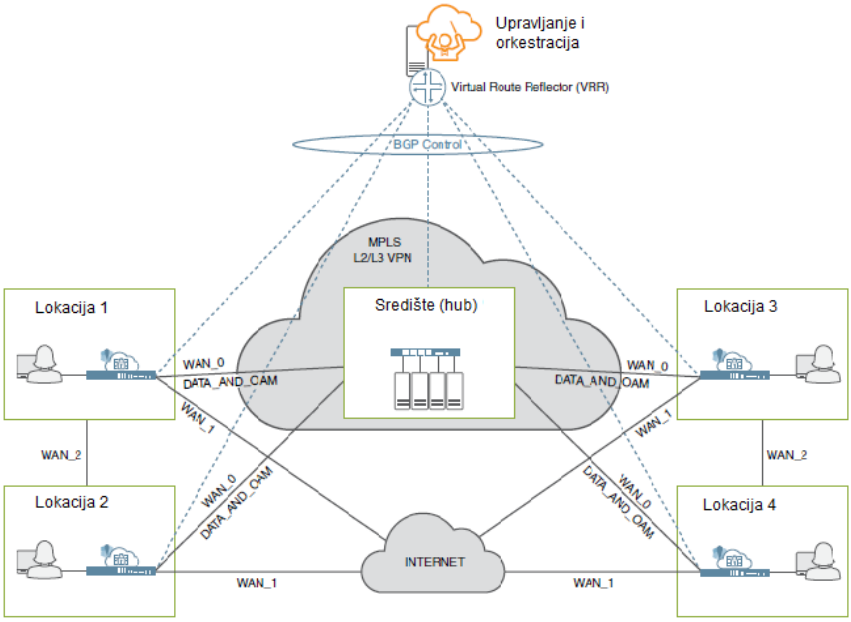


Slika 14 Topologija *hub-and-spoke*

Izvor: [34]

Ova topologija omogućava komunikaciju od lokacije do lokacije tako što sva komunikacija prolazi kroz SD-WAN pristupnik (engl. *gateway*).

Druga topologija je dinamički *mesh*. Ovdje je dozvoljena direktna komunikacija između svake lokacije i sve su lokacije međusobno povezane. Ovakva topologija se preporuča gdje aplikacije i usluge nisu centralizirane.



Slika 15 Topologija dinamički *mesh*

Izvor: [34]

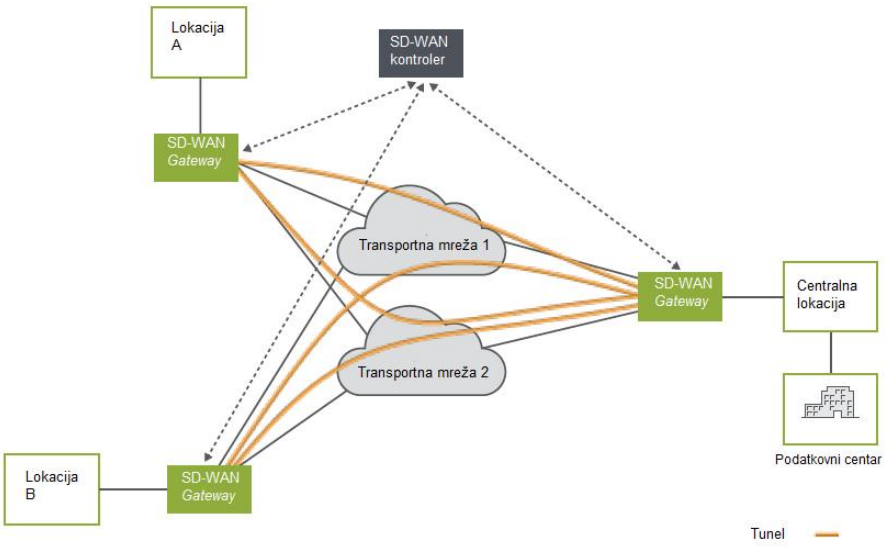
Ova topologija zahtjeva više resursa, a VNF-ovi se mogu implementirati na bilo kojoj prikazanoj lokaciji. Tuneli s jedne lokacije na drugu se kreiraju po zahtjevu kako bi se sačuvali resursi i poboljšao ukupni performans, [34].

3.6. Arhitektura SD-WAN-a

SD-WAN implementacija osigurava fleksibilan i automatski način usmjeravanja prometa s jedne lokacije na drugu. Osnovni elementi arhitekture uključuju:

- Više lokacija,
- Višestruke konekcije između lokacija,
- Kontroler,
- Više tunela.

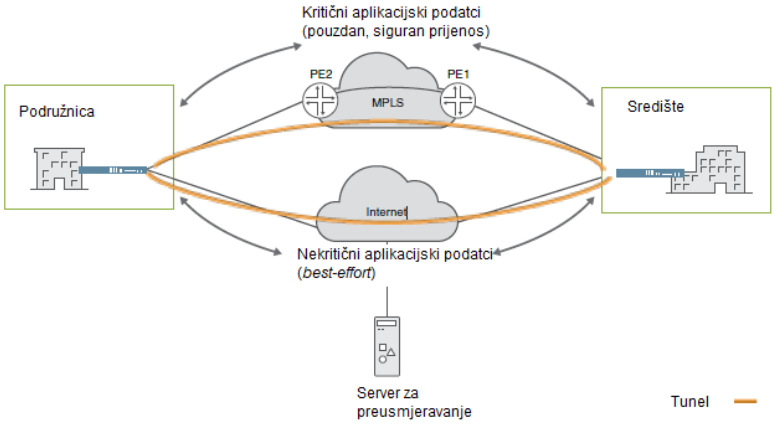
Na slici 16 su prikazani osnovni elementi SD-WAN tehnologije. SD-WAN kontroler je centralni orkestrator koji služi kao sučelje za operatora da upravlja uređajima na lokacijama, [34].



Slika 16 Općeniti prikaz arhitekture SD-WAN-a

Izvor: [34]

Juniperovo rješenje arhitekture se temelji na *hub-and-spoke* topologiji gdje svaka komunikacija između lokacija prolazi preko SD-WAN pristupnika. VNF-ovi se mogu postaviti na bilo koju lokaciju. Korisnički uređaji se nalaze na korisničkim podružnicama. Na lokalnoj strani lokacije, uređaji se povezuju u LAN segmente, a na WAN strani uređaji se preko jednog ili više linkova povezuju na SD-WAN pristupnika (slika 17), [34].



Slika 17 Rješenje SD-WAN arhitekture

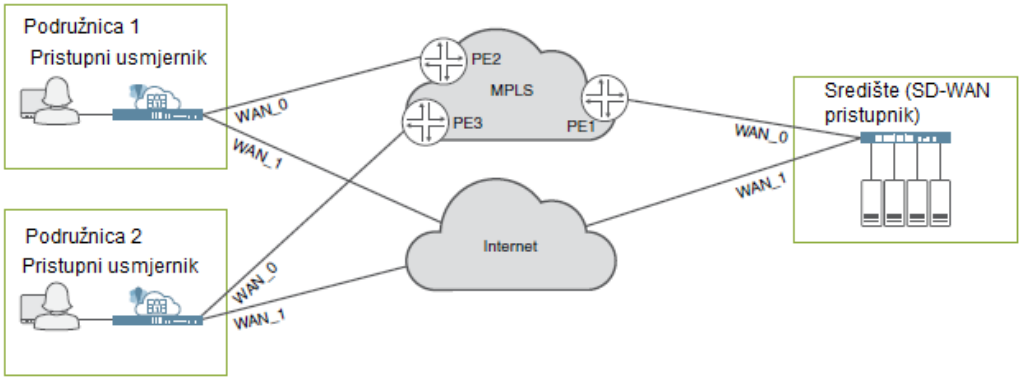
Izvor: [34]

Korisnički uređaji se nalaze na podružnicama i ponašaju se kao pristupni usmjernik u SD-WAN modelu pri čemu osigurava povezanost od podružnice s drugim lokacijama i Internetom.

Hub uređaj je zapravo SD-WAN pristupnik. U dinamičkoj *mesh* topologiji, svaka lokacija ima korisnički uređaj koji se povezuje s drugim lokacijama i pristupnik. U *hub-and-spoke* implementaciji, postoji najmanje jedan SD-WAN pristupnik i jedan ili više korisničkih

uređaja. SD-WAN pristupnik je završna točka između MPLS-a i IPsec[14] tunela od korisničkih uređaja, [34].

Fizička mreža u SD-WAN arhitekturi uključuje povezanost između uređaja. Ovaj sloj nema saznanja o korisničkim LAN segmentima te jednostavno osigurava dostupnost između uređaja na lokacijama. Slika 18 prikazuje da jednostavna mreža pri SD-WAN implementaciji ima više puteva do SD-WAN pristupnika, u ovom slučaju jednu preko privatnog MPLS-a, a drugu preko Interneta, [34].



Slika 18 Mreža SD-WAN arhitekture

Izvor: [34]

WAN sučelja mogu biti *tagged* ili *untagged*, a uređaji na lokacijama mogu biti spojeni na različite mreže pružatelja usluga. WAN pristupne opcije mogu biti: MPLS, Ethernet, LTE, ADSL/VDSL[15], satelitska veza. WAN sučelja se koriste primarno za slanje i primanje korisničkih podataka, a najmanje jedno WAN sučelje se mora koristiti i za upravljački promet (engl. *operation, administration, management - OAM*). OAM sučelje se koristi za komunikaciju s kontrolerom i omogućava kontroleru upravljanje uređajima na lokaciji, [34].

Logički tuneli služe za povezivanje uređaja u SD-WAN okruženju. Ovaj sloj ima saznanje o korisničkim LAN segmentima te je odgovoran za prenošenje korisničkog prometa između lokacija, [34].

3.7. Uloga pružatelja usluga

U ovom odlomku definirat će se bitni elementi za odabir pružatelja usluga. Naime, iznimno je važan broj direktnih *peeringa* između pružatelja usluga, a javni *peering* Internet *exchange* osigurava smanjenu latenciju i stabilniju vezu, [35].

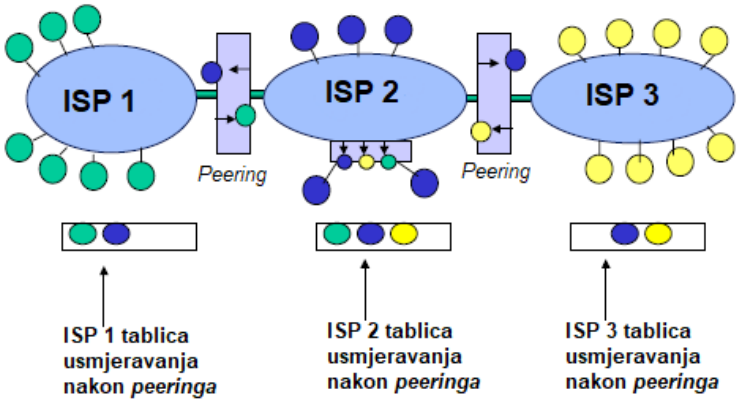
[14] *IPSec* (engl. *IP security* - IPSec) je standardni skup protokola između dvije komunikacijske točke preko IP mreže koji osiguravaju autentikaciju, integritet i povjerljivost podataka. Također definira kriptirane, dekriptirane i autenticirane pakete, [80].

[15] xDSL (engl. *Digital Subscriber Line* - xDSL) osigurava brzi prijenos podatkovnog prometa preko bakrene parice. ADSL predstavlja asinkroni xDSL, gdje je kapacitet silaznog linka znatno veći od uzlaznog, a VDSL predstavlja noviju tehnologiju koja pruža veće brzine (engl. *Very High*), [81].

Peering pružatelja usluga (engl. *Internet Service Provider* – ISP) je jedan od najvažnijih načina za poboljšanje efikasnost ISP operacija. *Peering* je poslovni odnos gdje ISP-ovi osiguravaju povezanost jednih korisnika s drugima. On smanjuje troškove i latenciju inter-AS[16] prometa. Kako bi ISP-ovi ostvarili interkonekciju s Internetom, postoje dva načina: tranzit i *peering*, [36].

Tranzit je veza gdje jedan ISP pruža pristup svim odredištima u svojoj tablici usmjeravanja. ISP koji prodaje tranzitne usluge se naziva *Upstream* ISP. ISP koji kupuje tranzit, prima pristup svim mrežnim rutama u *Upstream* ISP tablici usmjeravanja. Zauzvrat, *Upstream* ISP primi i objavi sve rute od ISP-a. Tranzit se naplaćuje u količini prenesenih podataka, [36].

Peering je poslovni odnos gdje ISP-ovi recipročno ostvaruju pristup korisnicima (slika 19). U ovom primjeru, ISP 1 ima *peering* vezu s ISP 2 u kojoj ISP 2 objavljuje dostupnost svojih plavih korisnika ISP-u 1, a ISP 1 svojih zelenih ISP-u 2. ISP 3 također ima *peering* vezu s ISP 2. U ovoj situaciji, tablice usmjeravanja prikazuje odredišne mreže koje svaki ISP može doseći. Potrebno je primijetiti da *peering* veza nije isto što i tranzitivna veza. Naime, ISP 3 korisnici ne mogu dosegnuti korisnike ISP-a 1, [36].



Slika 19 ISP *peering*, [36]

Tier 1 ISP je ISP koji ima pristup tablicama usmjeravanja globalnog Interneta, a ne kupuje tranzit od nikoga. *Tier* 1 ISP, s toga, ulaze u *peering* veze iz tehničkih razloga. *Peering* smanjuje latenciju, ostvaruje bolju kontrolu nad usmjeravanjem i kao posljedica toga manji je gubitak paketa, .

Točka gdje se dvije ili više ISP mreža sastaje se generalno naziva *Internet exchange point*. Logički, IXP se sastoji od ISP usmjernika povezanih kroz različite mehanizme drugog i trećeg sloja. IXP je gdje jedan ISP oglašava rute (odredišne mreže) drugima i gdje podatkovni paketi putuju od jednog ISP-a prema drugom. Javni IXP je u vlasništvu i upravljan od strane treće stranke, a otvoren je svakom ISP-u koji se želi povezati s drugim ISP-ovima na toj točki. Privatni IXP je direktna *point-to-point* veza između ISP-ova, [37].

[16] AS (autonomni sustav) je mreža ili skup mreža kojim upravlja jedan entitet ili organizacija. AS ima mnogo različitih pod-mreža povezanih zajedničkim politikama usmjeravanja, [82].

Za razmjenu ruta između ISP-a, odnosno autonomnih sustava, koristi se BGP protokol (engl. *Border Gateway Protocol* - BGP). Kad BGP usmjernik objavljuje rutu drugom BGP usmjerniku, to uključuje i mnoge atribute povezane s tom rutom. ISP operatori i BGP usmjernici koriste te atribute kako bi održali stabilno usmjeravanje između AS te za odabir ruta koje reflektiraju ISP-ove politike međupovezivanja.

Kako bi osigurali da su korisničke rute propagirane na sve usmjernike unutar i između AS-ova, BGP podržava dva načina operacije. eBGP (engl. *external BGP*) operira između dva BGP usmjernika u različitim AS-ovima. iBGP (engl. *internal BGP*) operira između BGP usmjernika unutar AS-a te zahtjeva da usmjernici budu povezani u potpuni *mesh* od iBGP konekcija. Potpuni iBGP *mesh* osigurava da svaki BGP usmjernik unutar AS-a može naučiti o eksternim korisničkim rutama koje je primio eBGP usmjernik. Kako bi se spriječile petlje, iBGP usmjernicima nije dozvoljena propagacija ruta drugim iBGP usmjernicima, [37].

4. Prednosti i nedostatci IP MPLS i SD-WAN mrežnih tehnologija

U ovom poglavlju je napravljen pregled prednosti i nedostataka MPLS i SD-WAN mrežnih tehnologija. Za obje tehnologije, definirane su neke od glavnih osobnosti kao što je pouzdanost, sigurnost, skalabilnost, cijena, itd.

4.1. Prednosti MPLS-a

Prednosti MPLS-a opisane u ovom odlomku su:

- Pouzdana usluga i QoS,
- Usmjeravanje od treće stranke,
- Ugovor o razini usluge (SLA),
- Sigurnost i
- Skalabilnost.

Jedna od glavnih prednosti MPLS-a je pouzdana dostava paketa i osigurana kvaliteta usluge. Naime, ovo je jako bitno za tvrtke pri prijenosu vremenski osjetljivih aplikacija poput VoIP-a ili video konferencije. Sve komercijalne usluge MPLS-a sadrže razine QoS-a, što znači da korisnik može definirati prioritet paketa u MPLS mreži. Tako se paketima osjetljivijima na kašnjenje dodjeli viši prioritet čime se osigurava manji gubitak prometa, [38].

Druga prednost MPLS-a je usmjeravanje od treće stranke. Odnosno, implementacija i održavanje MPLS mreže je u rukama pružatelja usluge. S toga, korisnici ne trebaju upravljati velikom usmjeravajućom mrežom te je iz njihove perspektive pojednostavljen menadžment mreže, [38].

Za razliku od korisničkih usluga, MPLS dolazi s ugovorom o razini usluge i garancijom dostave. MPLS usluge su visoko dostupne, pa je SLA najčešće 99.99%, a stvarna mrežna dostupnost bude i viša. Uz to, gubitak paketa je najčešće .1%. Na ovu prednost se povezuje i mrežno vrijeme neprekinutog rada koje je poboljšano zbog *mesh* dizajna i brzog preusmjeravanja, pa je vrijeme opravka od greške manje od 50ms, [39].

Iz sigurnosne perspektive, MPLS se smatra djelomično sigurnim unatoč tome što se nalazi na dijeljenom mediju. Razlog tome su jedinstvene labele koje se dodjeljuju paketu. Naime, paket unutar tih labela mogu pročitati samo MPLS čvorovi koji se nalaze na tom MPLS putu, [39].

Mnoge organizacije odabiru MPLS tehnologiju zbog njene skalabilnosti. MPLS ne treba dodatni fizički hardver kako bi radio, tako da pri rastu mreže nije potrebno kupovati još skupe opreme. Za veće organizacije, ovo može uštedjeti mnogo novca i smanjiti komplikacije koje nastaju kad se konfigurira nova oprema pri svakom proširenju mreže, [40].

4.2. Nedostatci MPLS-a

Nedostatci MPLS-a opisani u ovom poglavlju su:

- Cijena,
- Vrijeme implementacije,
- Slaba optimizacija sa SaaS uslugama,
- Sigurnost.

Jedan od najvećih nedostataka MPLS-a je zasigurno njegova cijena. Naime, u većini slučajeva, Internet povezanost je jeftinija od MPLS-a, pa su uštede pri prelasku na Internet čak 30-40%. Također, raste zahtjev za dodijeljenom Internet pristupu s pojasom 500Mb/1Gb/2Gb, pa čak i 10Gb. Veći prijenosni pojas na MPLS-u je teže sa ostvariti, jer su potrebni i prikladni usmjernici, [41].

Vrijeme implementacije MPLS-a može trajati jako dugo, a sam proces nije jednostavan. Za udaljene ili internacionalne lokacije, razvoj može trajati do godinu dana. Na primjer, MPLS usluge se moraju implementirati na jednu lokaciju prije nego što se može prijeći na drugu. Uz to, naknadna promjena prethodno ugovorenog prijenosnog pojasa također može biti kompliciranа ovisno o ISP-u, [41].

MPLS je optimiziran za povezanost *point-to-point*, ali ne i *point-to-cloud*, što znači da ne postoji direktan pristup *cloudu* ili SaaS aplikacijama preko MPLS-a. Samo 2% pružatelja *cloud* usluga pruža pristup, ali sa značajnim premijama, [41].

Prema [42], MPLS se ne može nazvati sigurnom mrežom, nego isključivo privatnom mrežom. Ne postoji inherentno kriptiranje unutar MPLS-a. On je samo usmjeravajući mehanizam koji stvara dojam privatne linije tako što usmjerava promet na unaprijed definirane označene puteve unutar mreže koja sadrži dijeljene mrežne elemente (npr. mrežni rubni elementi pružatelja usluga).

Organizacije koje se pouzdaju na MPLS mogu kriptirati podatke prije nego što napuste njihovu lokaciju. Kao dodatnu zaštitu, Cisco smatra da interna struktura MPLS jezgrene mreže ne smije biti vidljiva vanjskim mrežama (Internetu), [42].

4.3. Prednosti SD-WAN-a

U ovom odlomku opisane su glavne prednosti SD-WAN tehnologije, a to su:

- Cjenovna isplativost,
- Visoka dostupnost aplikacija,
- Vidljivost i kontrola WAN prometa,
- Centralizirano upravljanje,
- Fleksibilnost i redundancija,

- Sigurnost.

Povrat od uloženog kapitala[17] sa SD-WAN tehnologijom je dramatičan i trenutačan. Sa *Silver Peak* SD-WAN rješenjem, MPLS konekcije se mogu zamijeniti sa širokopojasnim Internet uslugama za povezivanje korisnika s aplikacijama te smanjiti WAN troškove za 90%, [43].

Nadalje, centralno upravljana SD-WAN arhitektura također smanjuje operativne troškove. Naime, primjenom ZTP-a, omogućene su brze implementacije. Postavljanje nove podružnice ili udaljene lokacije online je jednostavno te se obavlja u samo par minuta, [43].

SD-WAN donosi novu razinu visoke dostupnosti prema aplikacijama. Prethodno, promet specifične aplikacije se mapirao na jednu WAN uslugu. Tuneli spajaju konekcije od različitih izvora kako bi stvorili jednu logičku konekciju od jednog ili više WAN linkova. Na primjer, MPLS link plus širokopojasni link (jedan ili više) mogu biti dio tunela. Najčešće se različiti logički tuneli konfiguriraju za SD-WAN kako bi dostavio različite razine prioriteta i kvalitete usluge što je definirano s aplikacijskim SLA, [43].

Vidljivost prometa koji putuje kroz WAN je prvi korak prema ostvarivanju kontrole. Tvrtke ostvaruju korist od visokih razina vidljivosti u naslijeđene i *cloud* usluge jer time ostvaruju i kontrolu za dodjeljivanje politika za siguran i kontroliran WAN promet. SD-WAN omogućava *real-time* praćenje aplikacijskih i mrežnih performansi krajnjeg korisnika. Orkestrator prati propusnost, gubitak, latenciju i *jitter*[18] za sve mrežne puteve s alarmima što omogućava brže rješavanje problema pružatelja usluga, [43].

Vidljivost dolazi s kontrolom, jer inspekcija paketa identificira aplikacije temeljem prvih paketa. Ovo omogućavam SD-WAN-u da brzo donese odluku na temelju prirode paketa. Jednom kad se aplikacije identificira, moguće je optimizirati WAN put temeljem zahtijevanog QoS-a i *real-time* kvalitete WAN usluge (Internet, MPLS, LTE ili kombinacija), [43].

SD-WAN tehnologija iskorištava Internet kako bi kreirala sigurne konekcije s visokim performansama pri čemu eliminira prenošenje prometa na okosnicu kao kod MPLS-a. Zbog toga, SD-WAN dostavlja poslovne aplikacije s cjenovnom efektivnošću te optimizira SaaS i druge *cloud* usluge, [44].

Upravljanje tradicionalne MPLS WAN mreže je skupo, vremenski zahtjevno i traži sposobne vještine na rubu. SD-WAN koristi automatizaciju i centraliziranu dostavu kako bi se smanjili troškovi i vrijeme povezano sa svakidašnjim upravljačkim aktivnostima. Sposobnost da se riješe mrežni problemi s minimalnim ili nikakvim utjecajem na performanse krajnjeg korisnika i pri tome simultano optimiziranje aplikacijskih tokova smanjuje količinu posla za IT upravljanje, [45].

SD-WAN može koristiti više transportnih tehnologija što daje značajnu fleksibilnost. Odnosno, omogućava udaljenim krajnjim točkama konfiguraciju s MPLS-om, širokopojasnim

[17] Povrat od uloženog kapitala (engl. *return on investment* – ROI) je pokazatelj rentabilnosti, odnosno profitabilnosti uloženog kapitala ili investicije, [83].
[18] *Jitter* je razlika kašnjenja susjednih paketa iste sesije, [84].

Ethernetom, LTE mrežama i dr. Ova fleksibilnost pojednostavljuje povezivanje podružnica neovisno o njihovoj fizičkoj lokaciji ili restrikcijama nositelja usluga. Nadalje, osigurava se redundancija. Ako više prijenosnih puteva ne radi, sav promet se može automatski prebaciti na preostale puteve bez ometanja konekcije, [46].

Kad je riječ o sigurnosti, unatoč tome što SD-WAN iskorištava javnu širokopojasnu mrežu, postoje određene prednosti naspram MPLS tehnologije. Naime, centralizirano upravljanje sigurnosnim politikama uspostavlja kontrolu nad cijelom mrežom. Uz to, SD-WAN osigurava granulirane segmentacijske politike povezane za aplikacijske karakteristike i mrežne konfiguracije koje se distribuiraju na sve čvorove. Temeljem segmentacijskih politika, SD-WAN kreira tunele koristeći *IPSec* za dinamičku segmentaciju LAN-a te WiFi korisnika i uređaja na svim lokacijama, [47].

4.4. Nedostatci SD-WAN-a

U ovom odlomku, objašnjeni su nedostatci SD-WAN-a, a to su:

- Sigurnost,
- Kompleksnost,
- Softver,
- Rješavanje problema.

SD-WAN koristi nesigurni javni Internet za prijenos podataka. On koristi tehnologije poput enkapsulacije i SDN-a koje se ne smatraju stabilnima poput MPLS-a. SDN ima mnogo područja koja su izložena napadima. SDN-ov centralizirani kontroler je potencijalna jedina točka napada ili kvara, a njegovo *southbound* sučelje je izloženo napadima koji mogu ugroziti performanse mreže. Nadalje, korisnička oprema se konfigurira automatski na korisničkom mjestu. Tom opremom upravlja osoba kod korisnika, dok u MPLS-u opremu na korisničkoj strani pruža i implementira pružatelj usluga, [48].

Implementacijom SD-WAN-a, povećava se i kompleksnost sustava. Naime, u tradicionalnim mrežama, WAN konekcije su jedna usluga od jedne tvrtke. SD-WAN postavlja dodatnu komponentu, gdje se dodaje *overlay* postojećoj WAN konekciji, [49].

Razlog zašto su WAN pružatelji preferirali funkcije unutar hardvera je stabilnost. Softver je više podložan greškama i kvarovima. Prelaskom na SD-WAN, korisnici će ostvariti fleksibilnost koja dolazi pod cijenu specifičnosti i ograničenosti softvera, [49].

S obzirom SD-WAN uključuje *overlay* i postojeću WAN povezanost te kombiniranje različitih proizvođača opreme, pronalaženje pogreške postaje kompleksnije. WAN problemi zbog toga zahtijevaju istragu na dva mjesta, [49].

5. Studija slučaja: simulacija IP MPLS i SD-WAN mrežnih tehnologija u programskom alatu GNS3

GNS3 (engl. *Graphical Network Simulator-3* – GNS3) je mrežni softverski emulator koji omogućava kombinaciju virtualnih i stvarnih uređaja kako bi se simulirala kompleksna mreža. Za simulaciju, potrebne su slike Cisco operativnog sustava (IOS) na mrežnim uređajima, a kako bi se to ostvarilo GNS3 koristi *Dynamips* emulacijski softver, [50].

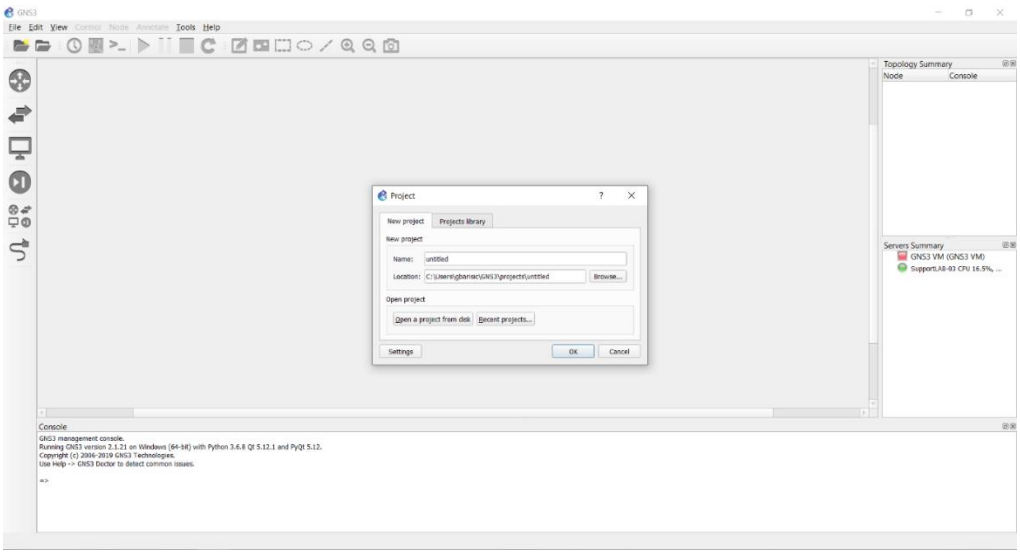
GNS3 se sastoji od dvije softverske komponente: *GNS3-all-in-one* softver te GNS3 virtualne mašine. U ovom radu, koristi se *GNS3-all-in-one* (GUI), a kreirani uređaji su pokrenuti na lokalnom GNS3 serverom. Lokalni GNS3 server se pokreće lokalno na istom računalu na kojem je instaliran GNS3 GUI, [51].

5.1. Simulacija IP MPLS mrežne tehnologije

U ovom odlomku, opisano je sučelje GNS3 te je napravljena simulacija IP MPLS mrežne tehnologije. MPLS topologija se sastoji od tri usmjernika u MPLS jezgrenoj mreži te dvije udaljene lokacije unutar istog VRF-a koji pokreće OSPF usmjeravajući protokol.

5.1.1. Pregled GNS3 sučelja

Prije samog konfiguriranja i simulacije IP MPLS mrežne tehnologije, potrebno je opisati GNS3 programski alat. Na slici 20 prikazano je početno sučelje pri pokretanju GNS3 (verzija 2.2.9). Programski alat se mora spojiti na lokalni server te je potrebno kreirati novi projekt.



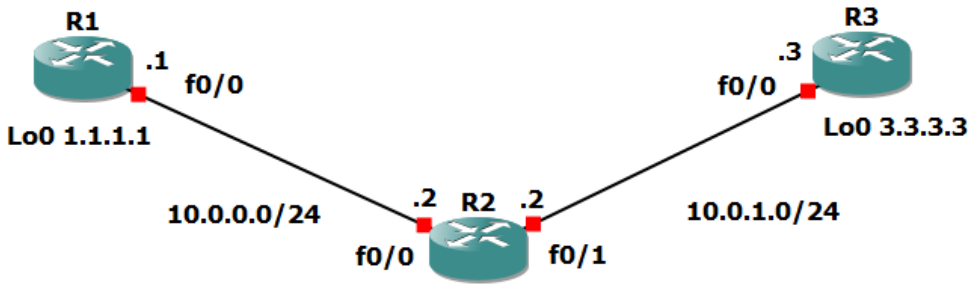
Slika 20 GNS3 sučelje

Nadalje, kao što se vidi na slici, s lijeve strane nalazi se izbornik uređaja: usmjernici, preklopnici, terminalni uređaji, sigurnosni uređaji, svi zajedno te ikona za povezivanje uređaja. U gornjem dijelu, nalazi se traka izbornika te alatna traka. Na alatnoj traci nalaze se alati za kreiranje i otvaranje projekta te ikone za pokretanje, zaustavljanje i uređivanje objekata, odnosno otvaranje CLI-ja (engl. *Command Line Interface* - CLI). S desne strane se nalazi popis objekata koji su dodani te broj servera.

Kao što je već navedeno, za rad u GNS3 potrebne su slike operacijskog sustava Ciscove mrežne opreme. Za mrežnu topologiju MPLS-a korišten je usmjernik Cisco C3725 sa slikom *c3725-adventerprisek9-mz.124-15.T14.*

5.1.2. Konfiguracija MPLS jezgrene mreže

Prvi dio simulacije MPLS mreže je konfiguracija jezgrene mreže koja se sastoji od tri usmjernika Cisco C3725. Usmjernicima su dodijeljene *loopback* adrese te IP adrese sučelja. Na svakom usmjerniku pokrenut je OSPF usmjeravajući protokol te je omogućen LDP. Između rubnih usmjernika, pokrenuta je *Multi Protocol* BGP sesija konfiguracijom vpnv4. Na slici 21 je prikazana topologija jezgrene mreže:



Slika 21 Topologija MPLS jezgrene mreže

Detaljne konfiguracije za svaki usmjernik se nalaze u prilogu rada, a u nastavku će na primjeru usmjernika R1 biti opisan proces konfiguracije:

interface lo0

ip address 1.1.1.1 255.255.255.55

ip ospf 1 area 0

interface f0/0

ip address 10.0.0.1 255.255.255.0

no shutdown

ip ospf 1 area 0

Prvo je konfigurirana IP adresa za *loopback* sučelje koje uvijek radi (stanje *up*), s toga će ga OSPF protokol prepoznati kao *Router ID*, a OSPF je pokrenut s posljednjom linijom koda te mu je dodijeljen proces 1, a područje je 0 za jezgrenu mrežu MPLS-a.

Sučelje f0/0 je sučelje prema R2. Sučelju je dodijeljena IP adresa iz mreže 10.0.0.0/24 te je također pokrenut OSPF protokol. U tablici 1 ispod, nalaze se definirane IP adrese za preostala dva usmjernika:

Tablica 1 Konfiguracija sučelja za usmjernike R2 i R3

Usmjernik	*Loopback sučelje*	*F0/0*	*F0/1*
R2	2.2.2.2/32	10.0.0.2	10.0.1.2
R3	3.3.3.3/32	10.0.1.3	

Kao što je bilo vidljivo na slici topologije, mreža između R2 i R3 je 10.0.1.0/24. Također, za sva sučelja na ova dva usmjernika omogućen je OSPF s *area* vrijednošću nula te su administrativno podignuti sučelja f0/0 i f0/1.

Nakon ove konfiguracije, omogućena je potpuna povezanost između usmjernika koja se može provjeriti funkcijom *ping*. Dalje, potrebno je omogućiti MPLS. Postoje dva načina: unošenjem *mpls ip* linije koda na svako sučelje ili pod OSPF proces omogućiti *mpls ldp autoconfig*. Linija koda za konfiguraciju MPLS LDP-a je ista na svim usmjernicima:

router ospf 1

mpls ldp autoconfig

Poslije konfiguracije, pojave se log zapisi da su LDP susjedi *up*. Kako bi se provjerila MPLS sučelja, koristi se linija koda *show mpls interface*, a za provjeru LDP susjeda se koristi *show mpls ldp neighbors*.

Kako bi provjerili koriste li usmjernici MPLS za komunikaciju, moguće je napraviti *trace* između R1 i R3.

```
R1#trace 3.3.3.3

Type escape sequence to abort.
Tracing the route to 3.3.3.3

  1 10.0.0.2 [MPLS: Label 16 Exp 0] 28 msec 32 msec 20 msec
  2 10.0.1.3 24 msec 20 msec 20 msec
R1#
```

Slika 22 Funkcija *trace* između usmjernika R1 i R3

Kao što je vidljivo na slici 22, R2 je koristi MPLS labelu na putu, a s obzirom na to da je ovo mala mreža, korištena je samo jedna labela, jer je R3 posljednji skok.

Dakle, konfigurirane su IP adrese u MPLS jezgrenoj mreži, omogućen je OSPF i potpuna IP povezanost između svih usmjernika te omogućen MPLS na svim sučeljima što je

uspostavilo LDP susjede između svih usmjernika. Idući korak je konfiguracija MP-BGP protokola između R1 i R3 čime se ostvaruje L3 VPN.

MP-BGP (engl. *MultiProtocol BGP* – MP-BGP) je proširenje BGP protokola, a koristi se slanje i oglašavanje adresa između korisnika putem BGP-a preko MPLS okosnice. MP-BGP je potrebno konfigurirati na svim PE (engl. *Provider Edge* - PE). BGP propagira informacije o VPN-IPv4 prefiksima između PE. IP prefiks je član IPv4 adresne obitelji, nakon što PE uređaj nauči IP prefiks, PE ga konvertira u VPN-IPv4 prefiks. Ovime se jedinstveno identificira korisnička adresa iako je lokacija definirana koristeći privatne IP adrese, [52].

Konfiguracija R1 izgleda ovako:

router bgp 1

neighbor 3.3.3.3 remot-as 1

neighbor 3.3.3.3 update-source Loopback0

no auto-summary

!

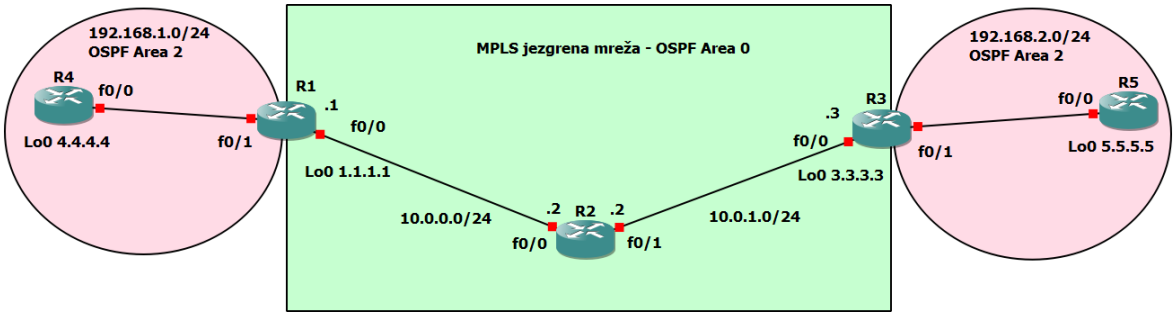
address-family vpnv4

neighbor 3.3.3.3 activate

BGP sesija između R1 i R3 se može provjeriti preko linije koda: *show bgp vpnv4 unicast all summary*. U idućem odlomku, proširit će se topologija mreže s dvije korisničke lokacije, odnosno dva dodatna usmjernika.

5.1.3. Konfiguracija korisničkih lokacija i VRF-a

U ovom odlomku nastavlja se konfiguracija MPLS mreže. Potrebno je konfigurirati dvije korisničke lokacije koje će također pokretati OSPF protokol, a na PE usmjernicima će se konfigurirati VRF (engl. *Virtual Routing and Forwarding* - VRF).



Slika 23 Topologija MPLS mreže

Kao što je prikazano na slici 23, obadva područja će imati OSPF područje 2 te će se adresirati privatnim IPv4 adresama. Područje s usmjernikom R4 je adresirano sa 192.16.1.0/24,

a područje s usmjernikom R5 je adresirano sa 192.168.2.0/24. Također, usmjernicima su dodijeljene *loopback* adrese.

Konfiguracija R4 je iduća:

int lo0

ip address 4.4.4.4 255.255.255.255

ip ospf 2 area 2

int f0/0

ip address 192.168.1.4 255.255.255.0

ip ospf 2 area 2

no shutdown

Na R1 je konfigurirano sučelje f0/1 s IP adresom 192.168.1.1/24. Nakon tog koraka, potrebno je konfigurirati VRF.

VRF je tehnologija uključena u IP usmjernike koja omogućava više instanci tablica usmjeravanja unutar usmjernika te njihov simultani rad. VRF osigurava automatsku segregaciju prometa što je primjenjivo pri kreiranju odvojenih virtualnih privatnih mreža za korisnike. S toga su PE usmjernici u mogućnosti pohranjivati rute i prosljeđivati pakete čak i ako korisnici koriste identično adresiranje, [53].

Konfiguracija VRF-a na R1 izgleda ovako:

ip vrf RED

rd 4:4

route-target both 4:4

int f0/1

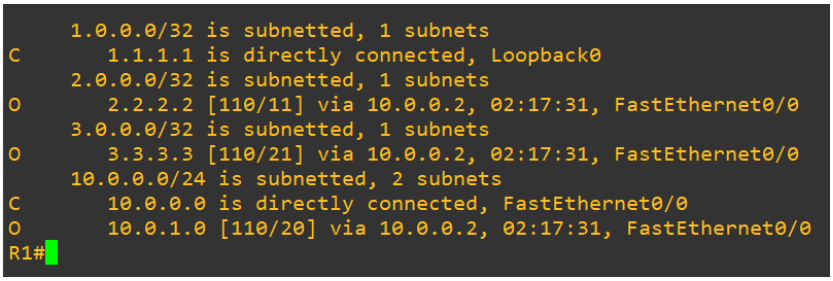
ip vrf forwarding RED

ip address 192.168.1.1 255.255.255.0

ip ospf 2 area 2

Nakon konfiguriranja VRF-a, potrebno je pomaknuti sučelje f0/1 u taj VRF. Nakon dodavanja, sučelju se izbriše IP adresa, pa je potrebno ponovno je dodijeliti. Da je VRF uspješno konfiguriran, može se provjeriti pokretanjem linije koda *show run int f0/1*.

Sada, u usmjerniku R1, postoje dvije tablice usmjeravanja: globala tablica usmjeravanja i tablica usmjeravanja za VRF RED. Pokretanjem *show ip route* dobije se tablica usmjeravanja na slici 24.



Slika 24 Globalna tablica usmjeravanja na usmjerniku R1

Sa slike 24 se vidi da u globalnoj tablici usmjeravanja nema mreže 192.168.1.0/24. Za prikaz tablice usmjeravanja za VRF RED potrebna je linija koda *show ip route vrf RED*.

Isti postupak konfiguracije potrebno je ponoviti za usmjernike R3 i R5. Usmjernik R5 obavlja OSPF *peering* s procesnim brojem 2 te područjem 2 na VRF koji je konfiguriran na R3. Sučelja su adresirana iz adresnog prostora 192.168.2.0/24.

Nakon konfiguracije usmjernika, izgrađena je MPLS jezgrena mreža koja pokreće OSPF s *loopback* adresama. R1 i R3 imaju *peering* s MP-BGP. LDP je omogućen na svim internim sučeljima, a eksterna sučelja MPLS jezgrene mreže su postavljena u VRF pod nazivom RED kojem su pridruženi i lokalni usmjernici.

Posljednji korak za potpunu povezanost preko MPLS jezgre je redistribucija OSPF ruta na R1 i R3 u MP-BGP te MP-BGP u OSPF. Potrebno je redistribuirati:

- OSPF rute iz R4 u MP-BGP u VRF na R1,
- MP-BGP rute u OSPF u R1,
- OSPF rute iz R5 u MP-BGP u VRF na R3,
- MP-BGP rute u OSPF u R3.

Linije koda za redistribuciju OSPF ruta u MP-BGP su iduće:

router bgp 1

address-family ipv4 vrf RED

redistribute ospf 2

Ovime je omogućena redistribucija OSPF ruta u BGP. Linija koda *show ip bgp vpnv4 vrf RED* omogućava provjeru jesu li rute iz R4 i R5 u BGP tablici za njihov VRF (slika 25).

```
R1#sh ip bgp vpnv4 vrf RED
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf RED)
*> 4.4.4.4/32       192.168.1.4             11         32768 ?
*>i5.5.5.5/32       3.3.3.3                 11    100      0 ?
*> 192.168.1.0      0.0.0.0                  0         32768 ?
*>i192.168.2.0      3.3.3.3                  0    100      0 ?
R1#
```

Slika 25 BGP tablica usmjernika R1 nakon redistribucije OSPF-a

Sa slike 25 je vidljivo da je 4.4.4.4 u BGP tablici u VRF RED na R1 s idućim skokom 192.168.1.4 (R4) te 5.5.5.5 s idućim skokom 3.3.3.3 (što je *loopback* za R3 čime se pokazuje da ide preko MPLS-a). Ista tablica se pojavi na R3 (slika 26).

```
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf RED)
*>i4.4.4.4/32       1.1.1.1                 11    100      0 ?
*> 5.5.5.5/32       192.168.2.5             11         32768 ?
*>i192.168.1.0      1.1.1.1                  0    100      0 ?
*> 192.168.2.0      0.0.0.0                  0         32768 ?
R3#
```

Slika 26 BGP tablica usmjernika R3 nakon redistribucije OSPF-a

Posljednji korak je postavljanje ruta koje su došle preko MPLS-a natrag u OSPF na usmjernicima R1 i R3. Linija koda glasi:

router ospf 2

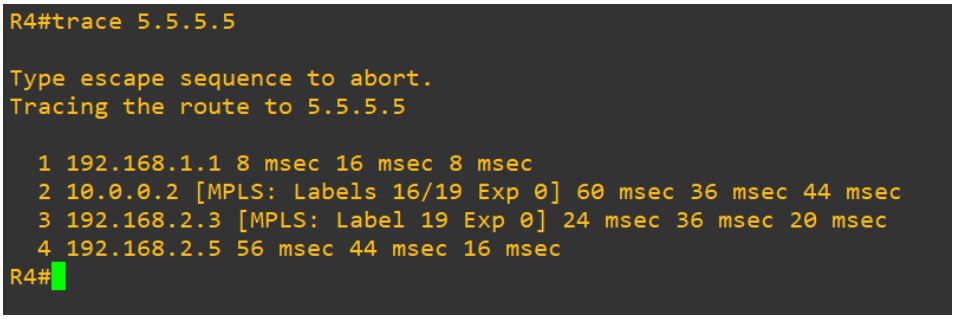
redistribute bgp 1 subnets

Nakon redistribucije MP-BGP-a, tablica usmjeravanja na R4 izgleda kao na slici 27:

```
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     5.0.0.0/32 is subnetted, 1 subnets
O IA    5.5.5.5 [110/21] via 192.168.1.1, 03:30:12, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/11] via 192.168.1.1, 03:30:12, FastEthernet0/0
R4#
```

Slika 27 Tablica usmjeravanja na usmjerniku R4

S usmjernika R4 je moguće napraviti *ping* 5.5.5.5, a *trace* izgleda kao na slici 28.



Slika 28 Funkcija *trace* na usmjerniku R4

Sa slike 28 je vidljivo da paket putuje preko MPLS te da se komutiraju labele.

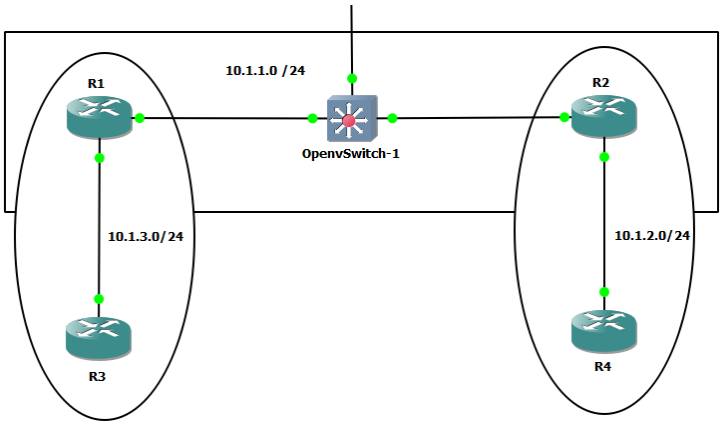
5.2. Simulacija SD-WAN mrežne tehnologije

U ovom dijelu rada opisana je simulacija SD-WAN mrežne tehnologije. Kao temeljni simulacijski program, korišten je GNS3 simulator u kojem su pokrenuti fizički Cisco c3725 usmjernika, OpenvSwitch te Mininet kontroler.

OpenvSwitch je virtualni preklopnik dizajniran za mrežnu automatizaciju kroz programske ekstenzije, pri čemu i dalje pruža standardna sučelja i protokole, [54]. Nadalje, Mininet virtualno okruženje omogućava upravljanje softverski-definiranim mrežama te podržava OpenFlow protokol, [55] .

5.2.1. Konfiguracija fizičkog dijela mreže

Fizička topologija mreže se sastoji od četiri Cisco c3725 usmjernika između kojih se nalazi OpenvSwitch kao što je prikazano na slici 29.



Slika 29 Topologija fizičkih usmjernika

Usmjernici su međusobno povezani RIP usmjeravajućim protokolom te je ostvarena komunikacija s kraja na kraj, kao što je vidljivo sa slike 30 gdje prolazi ping s R3 na R4.

```
R3#
R3#ping 10.1.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R3#
```

Slika 30 Prikaz povezanosti fizičkih usmjernika

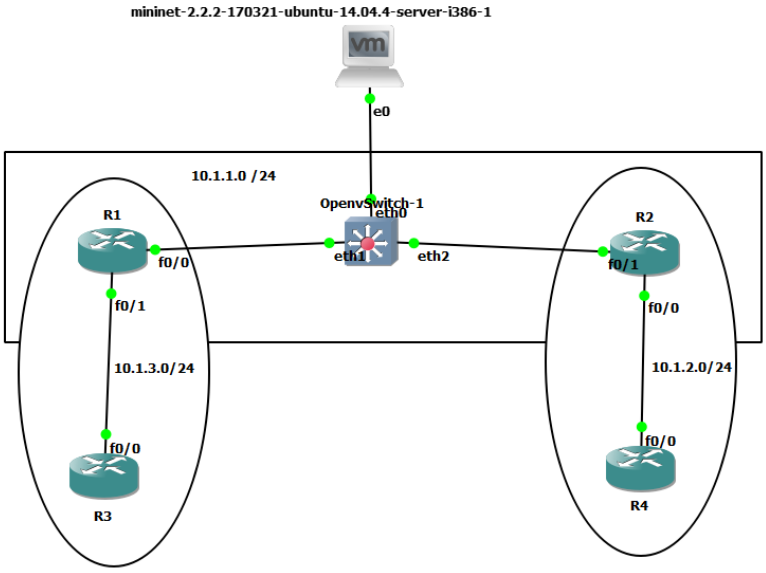
```
/ # ovs-ofctl dump-ports br0
OFPST_PORT reply (xid=0x2): 17 ports
  port LOCAL: rx pkts=14, bytes=1076, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=54, bytes=4305, drop=1, errs=0, coll=0
  port  8: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 10: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 14: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 11: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 13: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 16: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  5: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  9: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 12: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port 15: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  7: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  6: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  4: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  1: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
  port  2: rx pkts=179, bytes=17827, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=42, bytes=3442, drop=0, errs=0, coll=0
  port  3: rx pkts=48, bytes=5374, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=87, bytes=7231, drop=0, errs=0, coll=0
```

Slika 31 Prikaz prometa na OpenVSwitch-u

Također, da preko OpenVSwitcha prolazi promet, vidljivo je i po primljenim paketima na portovima 2 i 3 OpenVSwitcha, kao što je prikazano na slici 31.

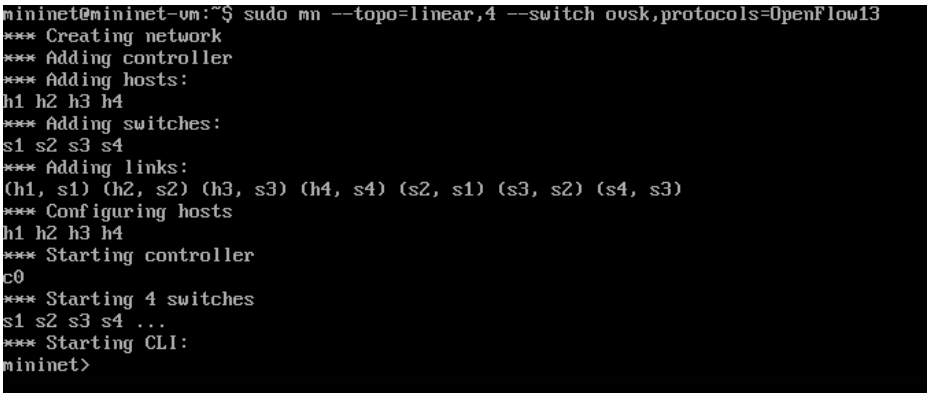
5.2.2. Povezivanje Mininet kontrolera

Idući korak pri konfiguraciji softverski definirane mreže je dodavanje Mininet kontrolera u mrežnu topologiju, kao što je prikazano na slici 32.



Slika 32 Topologija s Mininet kontrolerom

Kreiranje mrežne topologije unutar Mininet okruženja je napravljeno prema slici 33.



Slika 33 Kreiranje topologije

Naredba za kreiranje:

mininet@mininet-vm:~$ sudo mn –topo=linear,4 –switch ovsk,protocols=OpenFlow13

S ovom naredbom kreirana je linearna topologija s četiri usmjernika gdje je na svaki povezan jedan host te jednim OpenVSwitch kontrolerom. Iz prikazanih konfiguracija, vidljivo je kako SDN tehnologija omogućava centralizirano upravljanje sa svim mrežnim uređajima u topologiji. Odnosno, pri korištenju SDN rješenja, nije potrebno spajanje na svaki uređaj pojedinačno kako bi se konfigurirao, nego se sve radi centralizirano.

U idućem poglavlju bit će prikazana analiza prometa i parametara SD-WAN mreže te njihova usporedba s MPLS mrežnom tehnologijom.

5.3. Analiza mrežnih performansi

U ovom poglavlju opisana je analiza mrežnih performansi MPLS i SD-WAN mrežnih tehnologija. Za analizu mrežnih performansi MPLS mreže korišten je Wireshark program koji omogućava prikupljanje paketa u mreži te njihovu analizu. Za analizu mrežnih performansi SD-WAN rješenja korišten je sam kontroler Mininet unutar SD-WAN topologije.

5.3.1 Analiza mrežnih performansi MPLS-a

Kako bi se analizirale mrežne perfomanse MPLS mreže s kraja na kraj u simulacijskom programu GNS3, generirana je velika količina (<10000) ping paketa između krajnjih uređaja.

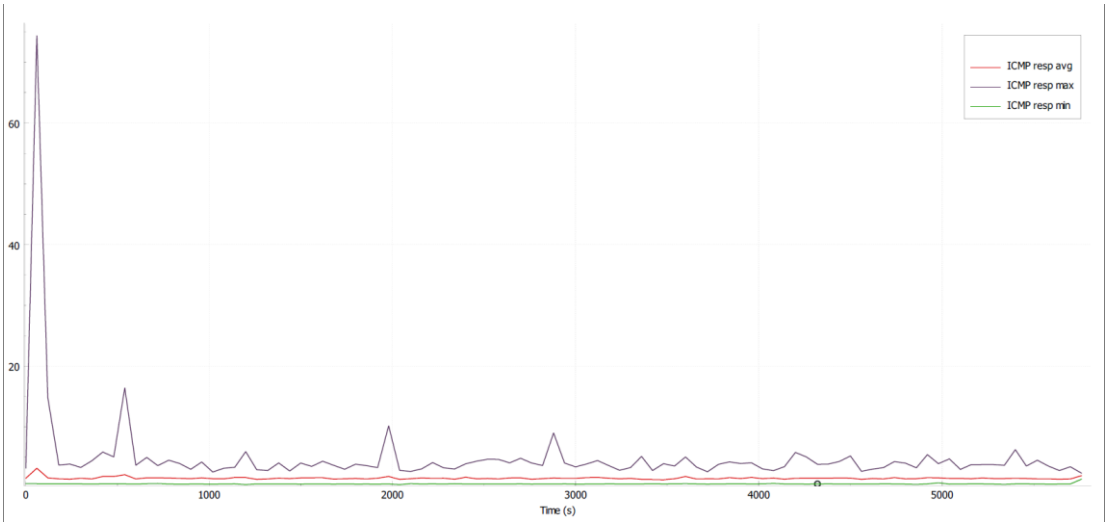
Statistics

Measurement	Captured	Displayed
Packets	13098	11474 (87.6%)
Time span, s	5762.292	5743.598
Average pps	2.3	2.0
Average packet size, B	97	98
Bytes	1268754	1124452 (88.6%)
Average bytes/s	220	195
Average bits/s	1761	1566

Slika 34 Statistike mrežnih performansi MPLS-a

Na slici 34, prikaz je statistika mrežnih performansi MPLS-a pri analizi prikupljenih paketa na odredišnom uređaju. Kao što je vidljivo, prikupljeno je 13098 paketa, a prosječna propusnost je 1761 bits/s. Nadalje, prosječan broj paketa po sekundi (pps) iznosi 2.3, dok je prosječna veličina paketa 97 bajta.

Iz grafa na slici 35, vidljiv je prosječno, maksimalno te minimalno vrijeme odgovora na ICMP pakete.



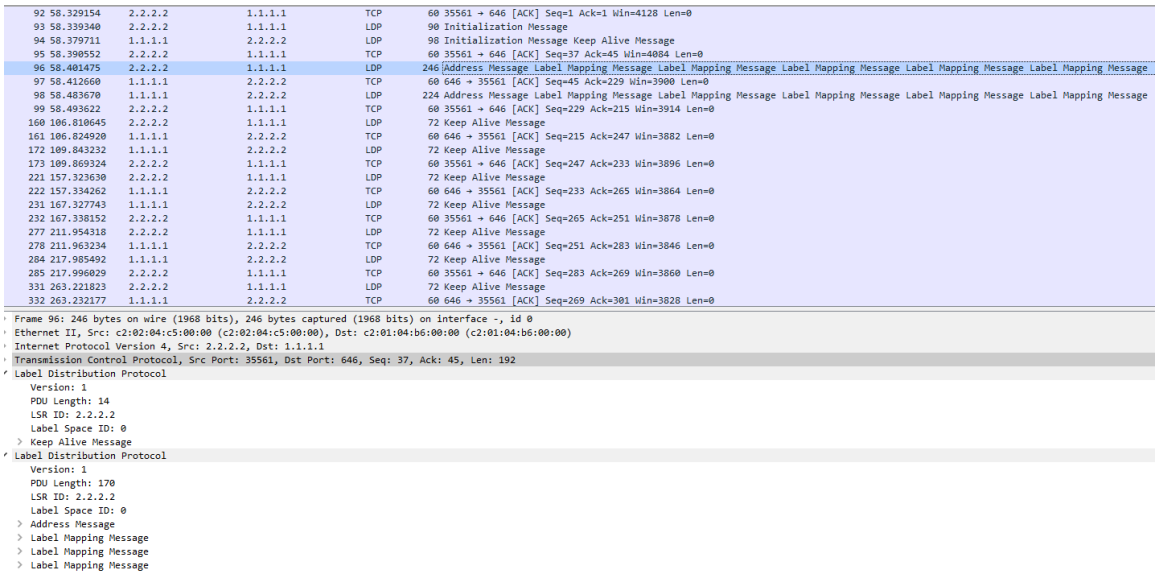
Slika 35 Graf vremena odgovora na ICMP pakete

Kao što je vidljivo iz grafa, prosječno vrijeme odgovora ping paketa je stabilno cijelo vrijeme te da je maksimalna vrijednost 0,66 ms. Dakle, iz grafa se može zaključiti kako nije bilo velikih oscilacija u vremenu odgovora na ping pakete.

Uključivanjem filtera *icmp.no_resp* na prikupljene podatke, vidljivo je da nema izgubljenih paketa.

Nadalje, iduće prikupljanje paketa je napravljeno između jezgrenog i rubnog MPLS usmjernika.

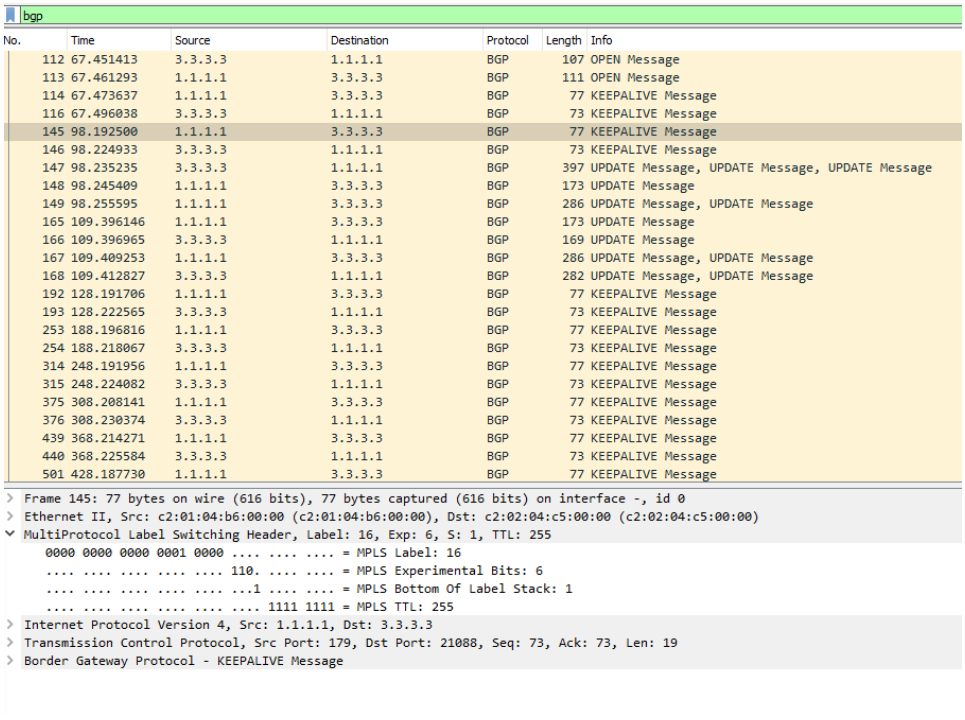
Prvo, možemo flitrirati LDP protokol koji je zaslužan za distribuciju labela u mreži. Nakon što su uspješno poslane *hello* poruke u mreži te je ostvaren TCP konekcija između jezgrenog i rubnog usmjernika, prema slici 37, vidljiva je razmjena poruka između ta dva usmjernika.



Slika 36 Analiza LDP MPLS protokola

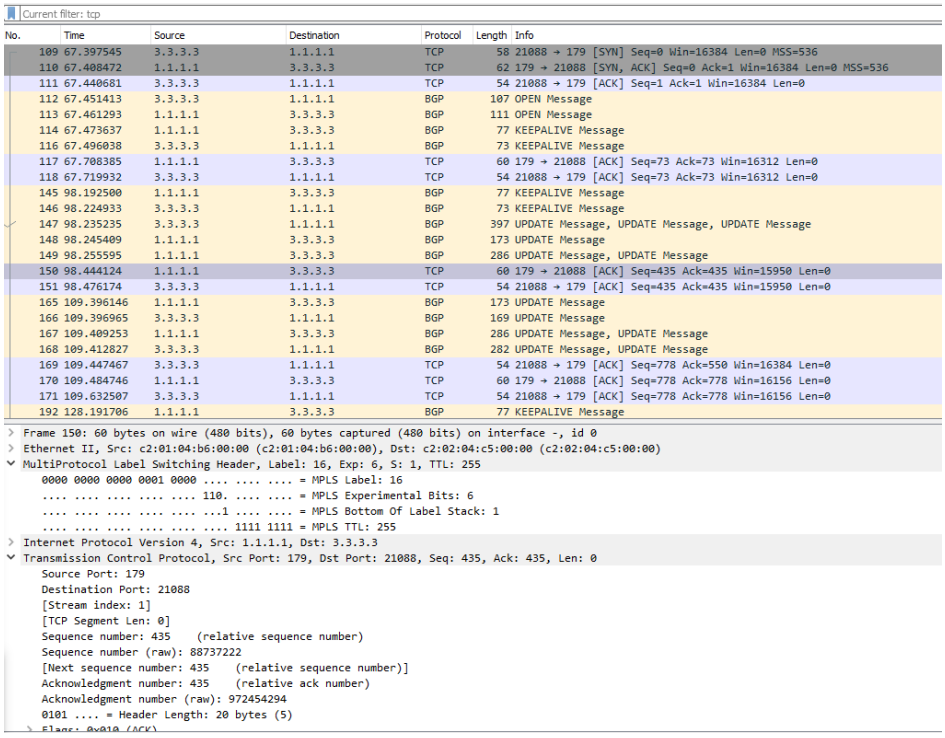
Preko LDP poruka vidljivo je da je ID usmjernika *loopback* adresa koju smo konfigurirali na usmjerniku. LDP poruke razmjenjuju informacije o rutama, labelama i adresnim obiteljima.

Drugo filtriranje je filtriranje BGP protokola čime je vidljiv mehanizam zamjene labela, što je prikazano na slici 38.



Slika 37 MPLS zamjena labela prikazana u Wiresharku

Sa slike 38 je vidljivo da je korištena MPLS labela 16 te da je posljednja labela u stogu.



Slika 38 TCP konekcija rubnih usmjernika

Na slici 39 prikazana je TCP konekcija između dva rubna usmjernika u MPLS topologiji te kako je ostvarena uspješna konekcija.

5.3.2 Analiza mrežnih performansi SD-WAN-a

U ovom dijelu analize mrežnih performansi, odrađena je analiza SD-WAN mrežne tehnologije. Za razliku od MPLS tehnologije, SD-WAN mrežnu tehnologiju i njene performanse je moguće analizirati izravno na mrežnom kontroleru, pa je s toga i u nastavku analiza rađena na prethodno korištenom Mininet kontroleru.

Za analizu mrežnih performansi korištene su performanse s kojima se u mrežama mjeri kvaliteta usluge, a to su: dostupnost, propusnost, kašnjenje te gubitak paketa.

Kao što je vidljivo iz primjera MPLS-a, pri analizi tradicionalnih mrežnih tehnologija, potrebno je spojiti se na određeni mrežni uređaj, generirati određenu količinu prometa te je nakon toga analizirati u prikladnom softverskom alatu. Takav proces može trajati dugo vremena, pogotovo u kompleksnim sustavima koji broje više desetaka pa čak i stotina uređaja.

S druge strane, analiza softverski-definiranih mreža je moguća centralizirano te nije potrebno spajanje ni na jedan drugi uređaj. Za početak, napravljena je provjera dostupnosti svih krajnjih uređaja u mreži.

Prva korištena naredba je *pingpair* koja provjerava dostupnost između dva *hosta* putem ping paketa u oba smjera. Kao što je prikazano na slici 40, ping je uspješno prošao između hostova h1 i h2.

```
mininet> pingpair
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
```

Slika 39 Pingpair naredba

Nadalje, Mininet omogućava provjeru dostupnosti između svih *hostova* jednostavnom naredbom *pingall* kojom se sa svakog *hosta* šalje ping pakete prema svim *hostovima* u mreži. Sa slike 41 je vidljivo da nema nikakvih gubitaka u mreži te da je dostupnost 100%.

```
*** Ping: testing ping reachability
h1 -> h2 h3 h4
h2 -> h1 h3 h4
h3 -> h1 h2 h4
h4 -> h1 h2 h3
*** Results: 0% dropped (12/12 received)
```

Slika 40 Provjera dostupnosti svih hostova u mreži

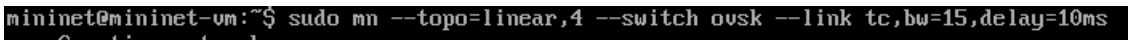
S ovom provjerom je zapravo vidljivo koliko je pojednostavljena provjera međusobne dostupnosti hostova. U tradicionalnoj mreži bi se za ovakvu provjeru trebalo spojiti na svaki *host* pojedinačno te generirati ping pakete prema svakom *hostu* u mreži.

Nadalje, na slici 42 je vidljivo kako je naredbom *iperf* moguće analizirati TCP mrežna širina pojasa i mrežna propusnost na linku između *h1* i *h2*. Za ovakvu analizu u tradicionalnim mrežama, bila bi potrebna analiza nad generiranim prometom u alatu poput *Wireshark-a* kako bi se izračunala prosječna propusnost linka.

Slika 41 Analiza mrežne širine pojasa i propusnosti na linku

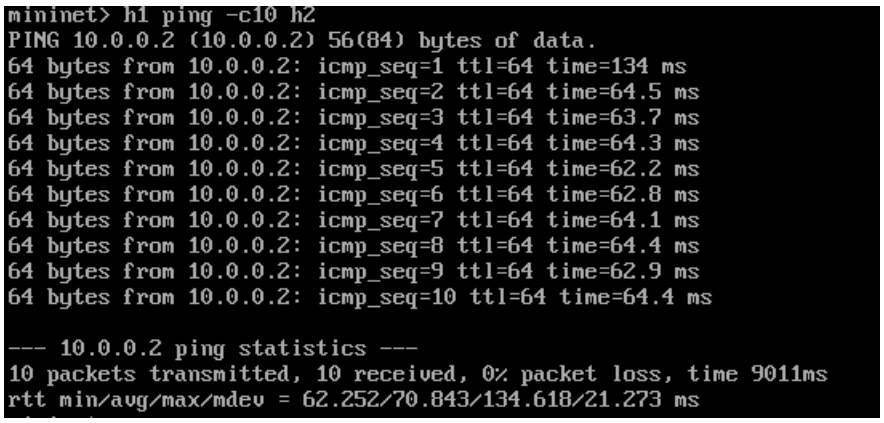
Kako je moguće konfigurirati detaljnije QoS performanse preko softverski-definiranih mreža, možemo vidjeti na idućem primjeru definiranjem propusnosti i kašnjenja na linkovima .

Izvođenjem naredbe sa slike 43, definirana je propusnost od 15 Mbit/s te kašnjenje od 10 sekundi. Povećanjem propusnosti na jednom linku, a smanjenjem na drugom, moguće je poboljšati kvalitetu usluge u realnom vremenu prema trenutnim zahtjevima korisnika. S obzirom da različite aplikacije zahtijevaju različitu propusnost, detaljnijim konfiguriranjem propusnosti prema linkovima i tipu prometa u mreži, moguće je optimizirati mrežne performanse sustava.



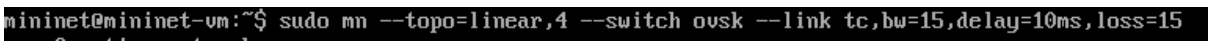
Slika 42 Konfiguriranje mrežne širine pojasa i kašnjenja na linku

Na slici 44, napravljen je prikaz kašnjenja koji je prouzrokovan kašnjenjem od 10 ms na tri linka između dva hosta što rezultira prosječnim RTT (engl. *Roud trip time* - RTT)[19] od 60 ms.



Slika 43 Provjera RTT između dva hosta

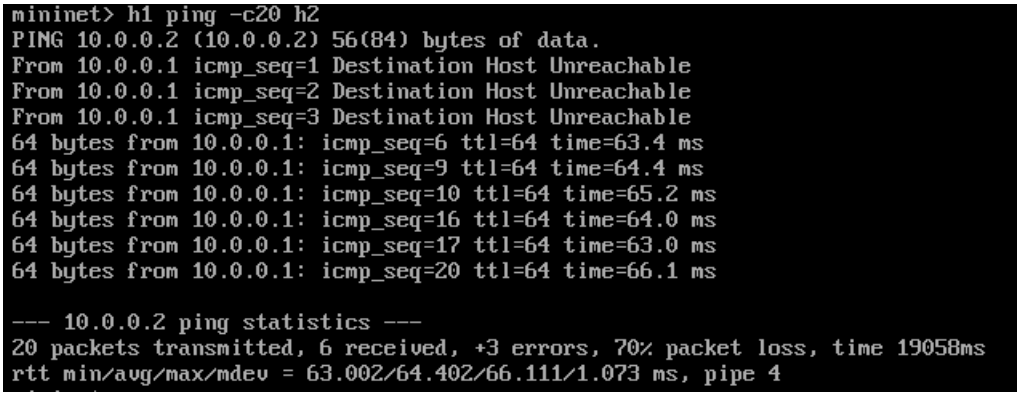
Kao posljednja analiza SD-WAN-a, definiran je gubitak od 15 % s naredbom na slici 45.



Slika 44 Konfiguracija gubitaka na linkovima

Gubitak paketa je jedan od najvažnijih parametara kvalitete usluge pri *real-time* aplikacijama kao što su VoIP, video konferencije i slično, gdje je bitno da je gubitak paketa što manji kako bi korisnici imali što bolje iskustvo.

[19] RTT je ukupno vrijeme potrebno da paket dođe do odredišne lokacije te natrag do izvorišta, [85]



Slika 45 Test gubitaka paketa preko ping paketa

Na slici 46 je vidljivo da definiranjem gubitaka paketa od 15 % na svakom linku, od 20 ping paketa između *hostova* h1 i h2 gubitak je čak 70 % paketa.

Iz ovoga se može zaključiti važnost ovog parametra te njegovog utjecaja na kvalitetu usluge koja je u modernim tehnologijama najvažniji faktor pri odabiru usluge.

6. Budući razvoj softverski definiranih mreža

U ovom poglavlju opisani su potencijalni budući razvoji softverski definiranih mreža. Neka od predviđanja su *SD-WAN-first* pristup, povećanje korisnički temeljenih politika te uključivanje trećih stranki pri upravljanju mrežom. Nadalje, opisane su primjena umjetne inteligencije u SDN tehnologijama kako bi se poboljšalo upravljanje kompleksnim zadatcima, primjenom SDN obilježja u IoT okruženju bi se utjecalo na senzorske mreže, upravljanje mrežama te na sigurnost. U posljednjem odlomku opisana je buduća virtualizacija IXP točki te što bi to značilo za pružatelje usluga.

6.1. Predviđanja o SDN tehnologijama

Rane implementacije SD-WAN-a su najčešće postavljane unutar postojeće WAN strukture gdje je najčešće primarni link bio Ethernet. S obzirom na to da se SD-WAN pokazao kao efektivna tehnologija, idući korak je reevaluacija postojeće WAN arhitekture kako bi se bolje iskoristile performanse i troškovna efikasnost SD-WAN-a. Prema Ciscu, *SD-WAN-first* pristup zapravo znači da će se povezanost s udaljenim lokacijama krojiti na temelju očekivanih performansi ostvarenih preko SD-WAN obilježja,.

Nadalje, buduće SD-WAN implementacije će pružati još veću zrnatost i tretiranje podatkovnih tokova u skladu odlukama individualnog korisnika. Kompleksnost upravljanja korisnički temeljenih politika će se povećati. Za neke, upravljanje temeljnom infrastrukturom uz korisničke politike može biti previše, s toga postoji mogućnost da će se neki upravljački zadatci prebacivati na treću stranku, [56].

Najjednostavniji način da korisnici danas implementiraju SD-WAN tehnologije je da to učine sami koristeći postojeću WAN rubnu arhitekturu. Ipak, postaje jasno da će trebati vremena i truda za kreiranje i upravljanje aplikacijski ili korisnički specifičnih politika. Jedno od rješenja je, na primjer, *SD-WAN-as-a-service* gdje pružatelji mogu upravljati cijelom mrežom, [56].

SD-WAN je već započeo mijenjati način upravljanja podružnica s ciljem povećanja otpornosti i smanjenja latencije. U idućem odlomku će biti detaljnije opisano kako uz primjenu umjetne inteligencije se može poboljšati takav model. Primjena AI bi poboljšala *real-time* analitiku temeljenu na definiranim aplikacijski-specifičnim postavkama koje indiciraju koji podatkovni tokovi trebaju imati prioritet, [56].

IDC procjenjuje da će svjetsko tržište SDN podatkovnih centara u 2022. godini vrijediti 12 milijardi dolara, dok je ostvarena dobit u 2017. iznosila 5,15 milijardi dolara što je više od 30% nego u prethodnoj godini. Prema Gartneru, 30% korporacija će implementirati SD-WAN tehnologije u svoje ogranke do kraja 2019., a do kraja 2023. taj broj će se popeti do 90%, [57].

U 2017. godini, fizička mreža je predstavljala najveći segment svjetskog tržišta SDN podatkovnih centara, gdje je dobit bila 2,2 milijarde dolara ili 42% ukupne dobiti. Ipak, u 2022,

očekuje se da će fizička mreža imati prihode oko 3,65 milijardi dolara, što je malo manje od 3,68 milijardi dolara kojih se pridodaje SDN tehnologijama, [57].

6.2. SDN potpomognut umjetnom inteligencijom

SDN koristi koncept programskih mreža koristeći logički centralizirano upravljanje čime se pojednostavljuju kompleksni zadatci poput prometnog inženjeringa[20], mrežne optimizacije i orkestracije. Nadalje, rukovođenje modernim mrežnim aplikacijama zahtjeva skalabilnu arhitekturu koja pruža pouzdane i dosljedne usluge temeljene na specifičnom tipu prometa. Ovo se može ostvariti primjenom SDN arhitekture koja održava globalni pregled mrežnog stanja te kontrolu tokova, [58].

Umjetna inteligencija (engl. *Artificial Intelligence – AI*) je područje koje uključuje širok opseg pod-područja, kao što je predstavljanje znanja, planiranje, donošenje odluka, optimizacija, strojno učenje i meta-heuristički algoritmi, [58].

Neuronske mreže su skupovi algoritama modelirani prema uzoru na biološke neurone u ljudskom mozgu koji se koriste za prepoznavanje uzoraka. Prema istraživanjima, primjena neuronskih mreža se koristi za detekciju i sprječavanje napada, rješavanje problema pozicioniranja kontrolera, *load balancinga*[21], predikcije performansi, itd. Na primjer, primjenom neuronskih mreži se može pospješiti detekcija DDoS napada ili smanjiti latencija za 19,3%. Nadalje, inteligentni sustavi mogu pospješiti i prijenos multimedije u SDN okruženju. Eksperimentalni rezultati su pokazali da se *jitter* smanjio u prosjeku 70%, a gubitci su reducirani s 9% na 1,16%, [59], [60].

Primjenom stabala odluke[22] (engl. *decision trees*) moguće je identificirati promet prema aplikaciji, klasificirati paketi i promet, detektirati promet, rješavati zagušenja tablica tokova i slično. Na primjer, prema istraživanju skalabilna aplikacijska klasifikacija za mobilne aplikacije je pokazala točnost od 94% u prosjeku. Meta-heuristički algoritmi[23] se primjenjuju za rješenje mrežnih problema poput usmjeravanja, *load balancinga,* mrežne sigurnosti te maksimiziranja mrežne iskoristivosti, [58] [61].

Dakle, AI tehnologije mogu riješiti širok opseg mrežnih problema i adresirati izazove SDN paradigme. Općenito, AI pristup se može smatrati jako korisnim alatom u SDN-u, ali potrebno je još istraživanja robusnosti AI pristupa, [58].

[20] Prometni inženjering je metoda optimizacije performansi telekomunikacijskih mreža dinamičkom analizom, predikcijama i regulacijama ponašanja podataka prenošenih preko mreže, [86].
[21] *Load balancing* je upravljanje prometom tako što se promet distribuira preko više poslužitelja ili virtualnih mašina unutar klastera kako bi se poboljšao performans, [87].
[22] Stabla odluke klasificiraju probleme tako što opisuju podatke u stablastoj strukturi gdje ulazni podatci mogu biti diskretni ili kontinuirani, a glavna im je prednost mogućnost interpretiranja, [58].
[23] Meta-heuristički algoritmi formiraju efikasni općeniti pristup koji uključuje širok opseg primjene, a koristi se za rješavanje teških optimizacijskih problema koji se ne mogu riješiti nijednom deterministčkom metodom unutar razumnog vremena, [58].

6.3. Uloga SDN-a u IoT okruženju

IoT i SDN su dvije novonastale tehnologije. IoT cilja na povezivanje objekata preko Interneta, a SDN osigurava orkestraciju mrežnog upravljanja odvajanjem podatkovnog i kontrolnog sloja. Broj povezanih objekata je u milijardama, a njihovo upravljanje i kontrola je kompleksni zadatak u velikim distribuiranim mrežama. SDN osigurava fleksibilnost i programibilnost u IoT mrežama bez opterećivanja arhitekture postojećih implementacija, [62].

Razna rješenja primjene SDN-a u okruženju IoT su predložena u području bežičnih senzorskih mreža (engl. *Wireless Sensor Network – WSN*). S toga je omogućena WSN mreža koja se re-konfigurira prema potrebama korisnika i zajednička infrastruktura za više aplikacija u senzorskoj mreži primjenom NFV-a, [54], [64].

Nadalje, SDN igra vitalnu ulogu u upravljanju heterogene mreže gdje je konfiguracija i dodjeljivanje resursa postalo teško. Tako postoji rješenje gdje se IoT mreža dijeli u manje mrežne klastere gdje onda svaku particiju kontrolira fizički distribuiran SDN kontroler. Drugi primjer je organizacija uređaja i njihovo grupiranje prema redoslijedu zahtijevanih usluga od strane korisnika, [65], [66].

IoT uređaji postaju sve više ranjivi na sigurnosne rizike, a neke od sigurnosnih rješenja može donijeti SDN. Jedno od predloženih rješenja je autentikacija IoT uređaja na kontroleru. Kontroler i uređaj razmjenjuju informacije te ukoliko je uređaj autenticiran, kontroler će početi slati tok prema uređaju, [67].

S obzirom na slabu agilnost, sigurnost i podatkovno upravljanje IoT-a, visoko se očekuje programibilnost i centralizirana kontrola IoT menadžmenta te integracija sa SDN-om. Cijeli koncept povezivanja ove dvije tehnologije je tek u začetcima te je potrebna standardizacija, [62].

Veliki faktor u nedostatku obuhvatne arhitekture SDN temeljenog IoT-a je i nedostatak konkretnog radnog okvira za IoT arhitekturu. Postojeći transportni protokoli nisu prilagođeni IoT scenarijima, jer mehanizmi kontrole zagušenja zahtijevaju veliku propusnost i kontrolu toka kroz mrežu, a TCP konekcija zahtjeva *buffering* što je veliko ograničenje u IoT uređajima. Tradicionalne mrežne sigurnosne politike se ne mogu primijeniti u IoT okruženju. Autentikacija i autorizacija zahtijevaju pohranu autentikacijskih profila u maloj pohrani. Zbog velike količine podataka koja se generira u IoT mreži, privatnost podataka ostaje kritični problem IoT mreža, [62].

6.4. Softverski definirani IXP

BGP ograničava kako mreža može dostaviti promet preko Interneta. Današnje mreže mogu prosljeđivati promet samo na temelju odredišnog IP prefiksa, tako što odabiru ponuđenu

rutu između svojih izravnih susjeda. SDN može promijenit dostavu prometa u širokom području, pružajući direktnu kontrolu nad pravilima procesiranja paketa. IXP je odlično mjesto za početi s obzirom na njihovu centralnu mrežu pri povezivanju više mreža, [68].

Za realizaciju softverski definiranog IXP-a, potrebno je napraviti aplikacije koje bi omogućavale *peering* između dvije mreže samo za određeni promet (npr. video *streaming*). Kako bi se realizirao SDX (engl. *Software Defined Exchange* - SDX) potrebno je adresirati iduće izazove:

- Aplikacije – uspješnost SDX-a ovisi o identificiranju aplikacija za dostavu WAN prometa koje je teško razviti. Takve aplikacije su: aplikacijski specifičan *peering*, prometni inženjering ulaznog prometa, balansiranje opterećenja i preusmjeravanje prometa kroz posrednike.
- Programska apstrakcija – sudjelujuće mreže trebaju način za kreiranje i pokretanje aplikacija bez konflikta jednih s drugim ili globalnim usmjeravajućim sustavom.
- Skalabilna operacija – SDX treba podržavati stotine sudionika, stotine tisuća IP prefiksa i politika koje se podudaraju na više polja zaglavlja paketa pri korištenju SDN preklopnika,
- Realna implementacija, [68].

SDX je IXP koji se sastoji od programirajuće SDN tehnologije povezane s BGP usmjeravajućim poslužiteljem koji osigurava IXP sudionicima razmjenu informacija preko BGP-a te SDN kontrolera koji osigurava sudionicima da promijene BGP ponašanje usmjeravanje sa SDN politikama. SDX kontroler dodjeljuje svakom AS sudioniku apstraktni preklopnik kojeg sudionik može programirati koristeći politike za kontrolu prometnih tokova na temelju mehanike *match-action.* Sudionici mogu izraziti SDN politike na svom ulaznom i izlaznom prometu, a SDX kontroler osigurava da nijedna SDN politika ne rezultira u prosljeđivanju prometa na susjedni AS koji nije objavio BGP rutu za prefiks koji odgovara odredišnoj adresi IP paketa, [69].

Svaki sudionik pokreće SDN kontrolu aplikaciju na centralnom kontroleru, a njegov rubni usmjernik razmjenjuje BGP ažurirajuće poruke s IXP-ovim usmjeravajućim poslužiteljem. SDN kontroler kombinira SDN politike od svih sudionika, spaja rezultantnu politiku s BGP usmjeravajućom informacijom i instalira zapise usmjeravajuće tablice u IXP, [69].

7. Zaključak

MPLS mrežna tehnologija nastala je kao *Ciscov* odgovor kako bi se korisnicima pružila usluga s kraja na kraj uz osiguranje kvalitete usluge. S obzirom da je u tradicionalnim mrežama bilo bitno osiguranje povezanosti odvojenih poslovnica sa serverima i aplikacijama koje su pokrenute na njih, MPLS se nametnuo kao sigurno rješenje za ostvarenje usluge.

MPLS uz to što pruža osiguranu kvalitetu usluge putem ugovora o razini usluge, prebacuje ulogu održavanja mreže na pružatelja usluge što za korisnika znači da ne treba kupovati novu opremu, a ima zagarantiranu kvalitetu usluge. Ipak, razvojem modernih tehnologija poput računalstva u oblaku, aplikacije više nije potrebno pokretati na lokalnim serverima, nego im se može pristupati bilo gdje i bilo kada. MPLS nema tehničko rješenje za sve veću prisutnost *cloud* usluga koje su također usko povezane s IoT rješenjima kojima se pristupa preko otvorenog Interneta te nije potrebna dedicirana linija i kompleksno komutiranje uz visoku naplatu propusnosti.

S druge strane, softverski-definirana mreža je novonastalo tehnologijsko rješenje koje nudi pojednostavljeno upravljanje kompleksnim mrežnim sustavima razdvajanjem kontrolnog i podatkovnog dijela. Time je omogućen globalni pregled cijelog sustava te centralizirano upravljanje svim mrežnim elementima. SD-WAN je proširenje SDN tehnologije gdje se definira primjena SDN rješenja na WAN gdje veliku ulogu imaju pružatelji usluga i njihova transformacija iz tradicionalnih tehnologija u programske mreže.

S obzirom na veliku fleksibilnost, jednostavnu implementaciju i mogućnost granuliranog konfiguriranja postavki usmjeravanja i kvalitete usluge, SD-WAN će zasigurno imati veliku ulogu u razvoju mrežnih tehnologija i sustava, kako za korisnike, tako i za pružatelje usluga. Ipak, povećanjem kompleksnosti WAN mreža, postavlja se pitanje mrežne sigurnosti za tvrtke.

Provedena simulacija mrežnih tehnologija u programskom alatu GNS3, pokazala je kompleksnost i dubinu potrebnog znanja za konfiguriranje MPLS mrežne tehnologije. S toga možemo zaključiti kako u velikim sustavima proces implementacije MPLS tehnologije može potrajati. Nadalje, kako bi se analizirao mrežni promet u MPLS mreži, bilo je potrebno generirati određeni promet te ga analizirati koristeći programski alat *Wireshark*.

Za razliku od MPLS-a, simulacija SD-WAN tehnologije je jednostavnija te sama konfiguracija svih mrežnih elemenata je moguća centralizirano primjenom Mininet kontrolera s kojeg je kasnije napravljena i cjelovita analiza prometa.

Usporedbom jednostavnosti obavljanja analize prometa, softverski-definirane tehnologije omogućavaju puno jednostavnije rješenje gdje se s jednom naredbom mogu definirati i provjeriti različiti parametri kvalitete usluge (npr. kašnjenje, propusnost, gubitak paketa). Nasuprot tome, analiza prometa i performansi MPLS mreže zahtijevala je prikupljanje podataka te njihovu detaljnu analizu kako bi se provjerila uspješnost simulacije.

SD-WAN mrežna tehnologija omogućava prilagođavanje mrežnih parametara u stvarnom vremenu što može biti iznimno korisno tijekom velikih video konferencija i sl, gdje se performanse na linkovima prilagode trenutnim prometnim tokovima bez prevelikog utroška za korisnika.

Ovakav pristup mrežnom inženjeringu i fleksibilnom prilagođavanju zahtjevima korisnika može transformirati način poimanja mrežne usluge naspram tradicionalnog pristupa. Nadalje, razvijanjem umjetne inteligencije i primjenom takve tehnologije u SDN okruženju, moguće će biti napraviti predikcije o mrežnom prometu, potrebama i politikama korisnika, što će sveukupno dovesti do poboljšanja razine usluge ali i mrežnih performansi.

Literatura

[1] Cisco community. Preuzeto sa: https://community.cisco.com/t5/networking-documents/how-to-configure-tag-switching-and-mpls/ta-p/3128570 [Pristupljeno: lipanj 2019.]

[2] Perić B., Osiguravanje kvalitete usluge u MPLS mrežama, Diplomski rad, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2018.

[3] de Ghein L., MPLS Fundamentals, Cisco, Indianapolis, 2007.

[4] Cisco certified expert. Preuzeto sa: https://www.ccexpert.us/mpls-network/mpls-and-the-osi-reference-model.html [Pristupljeno: lipanj 2019.]

[5] Science direct. Preuzeto sa: https://www.sciencedirect.com/topics/computer-science/label-switching-router [Pristupljeno: lipanj 2019.]

[6] Chauhan N., Kumar V., A Detail Review on Multiprotocol Label Switching (MPLS), vol. 4, no. 4, pp. 1547–1551, 2015.

[7] Networkers online. Preuzeto sa: http://www.networkers-online.com/blog/2010/03/mpls-label/. [Pristupljeno: lipanj 2019.]

[8] Science direct. Preuzeto sa: https://www.sciencedirect.com/topics/computer-science/label-switched-path. [Pristupljeno: lipanj 2019.]

[9] Semanics scholar. Preuzeto sa: https://www.semanticscholar.org/topic/Label-Information-Base/2763152. [Pristupljeno: lipanj 2019.]

[10] Cisco press. Preuzeto sa: http://www.ciscopress.com/articles/article.asp?p=680824&seqNum=2. [Pristupljeno: lipanj 2019.]

[11] IETF tools. Preuzeto sa: https://tools.ietf.org/html/rfc5036. [Pristupljeno: lipanj 2019.]

[12] Yasin W., Ibrahim H., Improving Triple Play Services Using Multi Protocol Label Switching Technology Label Switching Technology, Journal of Computer Science, 2010.

[13] Technopedia. Preuzeto sa: https://www.techopedia.com/definition/5409/wide-area-network-wan. [Pristupljeno: lipanj 2019.]

[14] SDxCentral. Preuzeto sa: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/. [Pristupljeno: lipanj 2019.]

[15] Ranjan P., Pande P., Oswal R., Qurani Z., A Survey of Past , Present and Future of Software Defined Networking, vol. 7782, pp. 238–248, Institute of Electrical and Electronics Engineers, 2014.

[16] Astuto B. N., A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks, Institute of Electrical and Electronics Engineers, 2014.

[17] Ominike A., Osisanwo F. Y., Remo I., Introduction to Software Defined Networks (SDN), International Journal of Applied Information Systems (IJAIS), New York, 2016.

[18] Mousa M., Bahaa-eldin A., Software Defined Networking Concepts and Challenges, no. April, IEEE, Egipat, 2018.

[19] Braun W., Menth M., Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices, no. May, University of Tuebingen, Njemačka, 2014.

[20] Goransson P., Black C., Culver T., *Software Defined Networks: A Comprehensive Approach*. 2016.

[21] SDxCentral. preuzeto sa: https://www.sdxcentral.com/networking/sdn/definitions/north-bound-interfaces-api/. [Pristupljeno: lipanj 2019.]

[22] ICT COSIGN, Combining Optics and SDN in next generation data centre networks, Denmark, 2015.

[23] Li Y., Zhang D., Taheri J., Li K., SDN components and OpenFlow, *Big Data Softw. Defin. Networks*, pp. 49–67, 2018.

[24] Lee G., *Developing Cloud-Based Data Center Networks*, SAD, 2014.

[25] Braun W., Menth M., Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices, *Futur. Internet*, vol. 6, no. 2, pp. 302–336, 2014.

[26] Vlajčić M., Pregled i analiza performanski softverski definiranih mreža, Diplomski rad, Fakultet prometnih znanosti, Zagreb, 2018.

[27] Cisco, Cisco SD-WAN Cloud scale architecture, Cisco2018.

[28] Network world. Preuzeto sa: https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html. [Pristupljeno: srpanj 2019.]

[29] Juniper. Preuzeto sa: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/zero-touch-provision.html. [Pristupljeno: srpanj 2019.]

[30] Aryaka. Preuzeto sa: https://www.aryaka.com/blog/what-is-sd-wan-which-one-right-for-your-business/. .

[31] Prashanth M., Manthena V., Lucent A., Network-as-a-Service Architecture with SDN and NFV : A Proposed Evolutionary Approach for Service Provider, Nizozemska, 2016.

[32] SDxCentral. Preuzeto sa: https://www.sdxcentral.com/networking/nfv/definitions/virtual-network-function/. [Pristupljeno: srpanj 2019.]

[33] VeloCloud, Guide to SDN, SD-WAN, NFV, and VNF, VeloCloud, 2016.

[34] Juniper Networks, Contrail ServiceOrchestration (CSO) Deployment Guide, Juniper Networks, 2019.

[35] BUG portal. Preuzeto sa: https://mreza.bug.hr/msd26-mpls-vs-sd-wan-buducnost-je-nekima-vec-stigla/. [Pristupljeno: srpanj 2019.]

[36] Peering portal. Preuzeto sa: http://drpeering.net/white-papers/Internet-Service-Providers-And-Peering.html. [Pristupljeno: srpanj 2019.]

[37] Metz C., Interconnecting ISP Networks, *IEEE Internet Comput.*, 2001.

[38] Search networking. Preuzeto sa: https://searchnetworking.techtarget.com/tip/MPLS-

advantages-and-disadvantages-for-WAN-connectivity. [Pristupljeno: srpanj 2019.]

[39] Silver peak. Preuzeto sa: https://blog.silver-peak.com/mpls-or-sd-wan-a-systems-engineering-analysis. [Pristupljeno: srpanj 2019.]

[40] Comparitech. Preuzeto sa: https://www.comparitech.com/net-admin/mpls-guide/#Scalability. [Pristupljeno: srpanj 2019.]

[41] Expereo. Preuzeto sa: https://www.expereo.com/9-reasons-make-switch-mpls/. [Pristupljeno: srpanj 2019.]

[42] RCR Wireless. Preuzeto sa: https://www.rcrwireless.com/20140513/wireless/mpls-security. [Pristupljeno: kolovoz 2019.]

[43] Silver peak. Preuzeto sa: https://www.silver-peak.com/sd-wan/top-benefits-sd-wan. [Pristupljeno: kolovoz 2019.]

[44] BizTech Magazine. Preuzeto sa: https://biztechmagazine.com/article/2016/12/6-advantages-software-defined-wan-implementation. [Pristupljeno: kolovoz 2019.]

[45] Network computing. Preuzeto sa: https://www.networkcomputing.com/networking/sd-wans-benefits-extend-beyond-cost-savings. [Pristupljeno: kolovoz 2019.]

[46] Search networking. Preuzeto sa: https://searchnetworking.techtarget.com/tip/How-SD-WAN-architectures-improve-network-flexibility-and-efficiency. [Pristupljeno: kolovoz 2019.]

[47] Riverbed. Preuzeto sa: https://www.riverbed.com/blogs/star-wars-network-security-and-the-force-of-sd-wan.html [Pristupljeno: kolovoz 2019.]

[48] Rajendran A., Security Analysis of a Software Defined Wide Area Network Solution Security, KTH Royal Institute of Technology Stockholm, Švedska, 2016.

[49] Search Networking. Preuzeto sa: https://searchnetworking.techtarget.com/answer/Despite-its-advantages-what-are-the-top-disadvantages-of-SD-WAN. [Pristupljeno: kolovoz 2019.]

[50] Wikipedia GNS3. Preuzeto sa: https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3 [Pristupljeno: rujan 2019.]

[51] GSN3 docks. Preuzeto sa: https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html [Pristupljeno: rujan 2019.]

[52] Cisco. Preuzeto sa: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html [Pristupljeno: rujan 2019.]

[53] Plixer. Preuzeto sa: https://www.plixer.com/blog/what-is-vrf-virtual-routing-and-forwarding/ [Pristupljeno: rujan 2019.]

[54] OpenvSwitch. Preuzeto sa: https://www.openvswitch.org/ [Pristupljeno: kolovoz 2020.]

[55] Mininet. Preuzeto sa: http://mininet.org/. [Pristupljeno: kolovoz 2020.]

[56] Cisco. Preuzeto sa: https://www.cisco.com/c/en_au/solutions/enterprise-networks/sd-wan/sd-wan-trends.html. [Pristupljeno: kolovoz 2020.]

[57] Network world. Preuzeto sa: https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html. . [Pristupljeno: kolovoz 2020.]

[58] Latah M., Toker L., Artificial intelligence enabled software-defined networking: A comprehensive overview, *IET Networks*, vol. 8, no. 2, pp. 79–99, 2019.

[59] Rego A., A. Canovas, Jimenez J. M., Lloret J., An Intelligent System for Video Surveillance in IoT Environments, *IEEE Access*, vol. 6, pp. 31580–31598, 2018.

[60] Cui C. X., Bin Xu Y., Research on load balance method in SDN, *Int. J. Grid Distrib. Comput.*, vol. 9, no. 1, pp. 25–36, 2016.

[61] Qazi Z. A., Lee J., Jin T., Bellala G., Arndt M., Noubir G., Application-awareness in SDN, *Comput. Commun. Rev.*, vol. 43, no. 4, pp. 487–488, 2013.

[62] Tayyaba S. K., Shah M. A., Khan O. A., Ahmed A. W., Software defined network (SDN) based internet of things (IoT): A road ahead, *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, no. December, 2018.

[63] Miyazaki T. *et al.*, A software defined wireless sensor network, *2014 Int. Conf. Comput. Netw. Commun. ICNC 2014*, pp. 847–852, 2014.

[64] Leontiadis I., Efstratiou C., Mascolo C., Crowcroft J., Transforming Sensor Networks Into Multi-Application Sensing Infrastructures, *Ad Hoc & Sensor Wireless Networks*, no. May, p. 273, 2012.

[65] Boussard M. *et al.*, Software-Defined LANs for Interconnected Smart Environment, *Proc. - 2015 27th Int. Teletraffic Congr. ITC 2015*, pp. 219–227, 2015.

[66] Wu D., Arkhipov D. I., Asmare E., Qin Z., McCann J. A., Mobility management in urban-scale software defined IoT, *Proc. - IEEE INFOCOM*, vol. 26, pp. 208–216, 2015.

[67] Sahoo K. S., Sahoo B., Panda A., A secured SDN framework for IoT, *Proc. - 2015 Int. Conf. Man Mach. Interfacing, MAMI 2015*, pp. 1–4, 2016.

[68] Gupta A. *et al.*, SDX: A Software Defined Internet Exchange, *Comput. Commun. Rev.*, vol. 44, no. 4, pp. 551–562, 2015.

[69] Gupta A. *et al.*, An Industrial-Scale Software Defined Internet Exchange Point, *Nsdi*, pp. 1–14, SAD, 2016.

[70] Technopedia. Preuzeto sa: https://www.techopedia.com/definition/25315/point-to-point-protocol-ppp. [Pristupljeno: kolovoz 2019.]

[71] Electronics research group. Preuzeto sa: https://erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/dscp.html. [Pristupljeno: kolovoz 2019.]

[72] Juniper. Preuzeto sa: https://www.juniper.net/documentation/en_US/junos/topics/concept/bgp-routing-overview.html. [Pristupljeno: kolovoz 2019.]

[73] Mrvelj Š., Predavanja iz kolegija Tehnologija telekomunikacijskog prometa 2., Fakultet Prometnih Znanost Zagreb, Sveučilište Zagreb, Zagreb, 2017.

[74] Webopedia. Preuzeto sa: https://www.webopedia.com/TERM/A/API.html. [Pristupljeno: kolovoz 2019.]

[75] Atzori L., Iera A., Morabito G., The Internet of Things: A survey, *Comput. Networks*,

vol. 54, no. 15, pp. 2787–2805, 2010.

[76] Mell P., Grance T., The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, 2011.

[77] Webopedia. Preuzeto sa: https://www.webopedia.com/TERM/V/VPN.html. [Pristupljeno: rujan 2019.]

[78] Lifewire. Preuzeto sa: https://www.lifewire.com/what-is-dhcp-2625848. [Pristupljeno: rujan 2019.]

[79] Stupar I., Ostvarivanje kvalitete usluge u računarstvu u oblaku putem skalabilnosti i sporazuma o razini usluge, 2012.

[80] Geeks for geeks. Preuzeto sa: https://www.geeksforgeeks.org/ip-security-ipsec/. [Pristupljeno: rujan 2019.]

[81] Informit. Preuzeto sa: http://www.informit.com/articles/article.aspx?p=21317. [Pristupljeno: rujan 2019.]

[82] Techopedia. Preuzeto sa: https://www.techopedia.com/definition/11063/autonomous-system-as. [Pristupljeno: kolovoz 2019.]

[83] Poslovni portal. Preuzeto sa: http://www.poslovni.hr/leksikon/roi-1513. [Pristupljeno: kolovoz 2019.]

[84] Ćorković I., Pregled rezultata istraživanja granica QoS parametara različitih usluga, 2018.

[85] Wikipedia RTT. Preuzeto sa: https://en.wikipedia.org/wiki/Round-trip_delay. [Pristupljeno: rujan 2020.]

[86] Search networking. Preuzeto sa: https://searchnetworking.techtarget.com/definition/traffic-engineering. [Pristupljeno: kolovoz 2020.]

[87] Search Server Virtualziation. Preuzeto sa: https://searchservervirtualization.techtarget.com/definition/Network-Load-Balancing-NLB [Pristupljeno: rujan 2019.]

Popis kratica i akronima

AI	*engl. Artificial Intelligence*
API	*engl. Application Program Interface*
AS	*engl. Autonomous system*
AToM	*engl. Any Transport over MPLS*
BGP	*engl. Border Gateway Protocol*
CLI	*engl. Command Line Interface*
DHCP	*engl. Dynamic Host Configuration Protocol*
DSCP	*engl. DiffServ Code Point*
FEC	*engl. Forwarding Equivalence Class*
GNS3	*engl. Graphical Network Simulator 3*
IGP	*engl. Interior Gateway Protocol*
IoT	*engl. Internet of Things*
IPSec	*engl. IP security*
ISP	*engl. Internet Service Provider*
LAN	*engl. Local Area Network*
LDP	*engl. Label Distribution Protocol*
LER	*engl. Label Edge Router*
LFIB	*engl. Label Forwarding Information Base*
LIB	*engl. Label Information Base*
LSP	*engl. Label Switched Path*
LSR	*engl. Label Switch Router*
LTE	*engl. Long Term Evolution*
MP-BGP	*engl. MultiProtocol BGP*
MPLS	*engl. Multi-Protocol Label Switching*
NFV	*engl. Network Functions Virtualization*
OAM	*engl. Operation, administration, management*
PE	*engl. Provider Edge*

PPP	*engl. Point to Point Protocol*
QoS	*engl. Quality of Service*
ROI	*engl. Return on investment*
RTT	*engl. Roud trip time*
SaaS	*engl. Software as a Service*
SD-WAN	*engl. Software Defined WAN*
SDX	*engl. Software Defined Exchange*
SLA	*engl. Service Level Agreement*
VNF	*engl. Virtual Network Functions*
VPN	*engl. Virtual Private Network*
VRF	*engl. Virtual Routing and Forwarding*
WAN	*engl. Wide Area Network*
WSN	*engl. Wireless Sensor Network*
xDSL	*engl. Digital Subscriber Line*
ZTP	*engl. Zero touch provisioning*

Popis slika i tablica

Popis slika

Popis tablica