Arhitektura i implementacija tehnologije SD-WAN na primjeru rješenja Versa

Turudić, Matija

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

Arhitektura i implementacija SD-WAN tehnologije na primjeru rješenja Versa

Architecture and Implementation of SD-WAN Technology in the Versa Solution

Mentor: izv. prof. dr. sc. Ivan Grgurević

Student: Matija Turudić

JMBAG: 0135225304

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. travnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 6811

Pristupnik: **Matija Turudić (0135225304)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Arhitektura i implementacija tehnologije SD-WAN na primjeru rješenja Versa**

Opis zadatka:

Opisati značajke SD-WAN mreža kroz razdvajanje funkcionalnosti upravljačke i kontrolne razine te prikaza mogućnosti SD WAN-a. Prikazati arhitekturu platforme SD-WAN-a. Analizirati i usporediti tradicionalne WAN i SD-WAN mreže. Prikazati mogućnosti implementacije SD WAN-a na primjeru rješenja Versa (Versa Analytics, Versa director, Versa controller i Versa head end design). Utvrditi probleme integracije kod implementacije SD WAN tehnologije.

Mentor:

izv. prof. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

ARHITEKTURA I IMPLEMENTACIJA SD-WAN TEHNOLOGIJE NA PRIMJERU RJEŠENJA VERSA

SAŽETAK

Završni rad se temelji na prikazu značajki jednog od mogućih smjerova razvoja mrežne WAN tehnologije SD-WAN. Kroz prikaz značajki i arhitekture pokušava se dati dojam o benefitima koje tehnologija pruža velikim poduzećima. SD-WAN pruža poslovnu agilnost, inteligentan način umrežavanja i samu poslovnu transformaciju čime se pruža zadovoljenje dinamične poslovne potražnje. Osnovnim mrežnim komandama poput testiranja odziva i *traceroute*a među udaljenim branchevima spojenim na Versa opremu daje se prikaz rezultata temeljenim na različitim pristupnim mrežama i koegzistenciji obje infrastrukture - MPLS i *Versa Networks*. Zaključno poglavlje ukazuje na moguće probleme koji se trebaju uzeti u razmatranje pri implementaciji svake SD-WAN mreže na MPLS poput naprednih prijetnji, sigurnosnih rizika, izazova praćenja prometa i same standardizacije.
KLJUČNE RIJEČI: MPLS, Versa, odziv, SD-WAN, *traceroute*, velika poduzeća

SUMMARY

The elementary principles of this thesis are founded upon the demonstration of features on behalf of one of the possible developments of SD-WAN network technologies. By demonstrating the specific features and arhitecture of SD-WAN the aim is to present the benefits of SD-WAN technology in big businesses. SD-WAN network allows business agility, intelligent way of networking and transformation of business practices which meet the requirements of dynamic business demand. Basic network commands like ping and traceroute between remote branches connected to Versa equipment display the results founded on different access networks and coexistence of both MPLS and Versa Network structure. The final chapter demostrates the inclusion of possible problems which need to be considered during the implementation of every SD-WAN network on MPLS such as advanced threats, safety risks, challenges in traffic tracing and network standardization.
KEYWORDS: MPLS, Versa, ping, SD-WAN, traceroute, big businesses

Sadržaj

1. UVOD

Temeljna premisa završnog rada odnosi se na definiranje trenutačno dostupnih mrežnih modela za prijenos podataka uz poseban osvrt na razliku između najzastupljenije MPLS (engl. *Multi-Protocol Label Switching*) tehnologije koja omogućava tradicionalni model prosljeđivanja paketa kroz mrežu i SD-WAN (engl. *Software Defined Wide Area Network*) tehnologije koja podrazumijeva suvremeniji oblik mrežne funkcionalnosti kojim se nastoji optimizirati mrežna infrastruktura uz novo prilagođavanje mreže poslovnim potrebama, aplikacijama i prometu. S pojavom tehnologije u oblaku, IT zahtjevi poduzeća uvelike su olakšani. Poduzeća i organizacije više ne moraju kupovati i upravljati softverom za kreiranje SD-WAN rješenja. Osim toga, nema potrebe za kupnjom hardvera ili bilo koje vrste komunikacijskog softvera ili posebnih uređaja. SD-WAN u velikoj mjeri zamjenjuje tradicionalne VPN-ove jer VPN uspostavlja jednu vezu preko interneta i sav promet teče kroz njega. SD-WAN uspostavlja višestruke istovremene veze.

U tehničkom smislu suvremeni SD-WAN predstavlja tehnološki pristupačnije, intuitivnije rješenje te odgovor novim zahtjevima za probleme osiguravanja QoE (engl. *Quality of Experience*) i QoS (engl. *Quality of Service*) u velikim višeuslužnim mrežama.

Izvršit će se i analiza arhitekture SD-WAN platforme te njezinih specifičnosti i temeljnih funkcionalnih odrednica. Nadalje, rad se temelji i na komparativnoj analizi infrastrukture navedenih mrežnih modela i kvalitete usluga u MPLS i SD-WAN mrežama uz isticanje temeljnih značajki spomenutih mreža i pripadajućih aplikacija. Pojedinačne značajke MPLS i SD-WAN mreža također će biti detaljnije obrađene u nadolazećim poglavljima, jednako kao i posebne pojedinačne odlike koje jamče osiguranje kvalitete usluge. Posebno poglavlje rada namijenjeno je i detaljnijoj usporedbi modela i načina funkcioniranja "tradicionalnih" WAN i SD-WAN mreža.

Posljednji dio rada predviđen je detaljnijem pregledu implementacije SD WAN mreže na temelju *Versa Networks* rješenja, pri čemu je dodatna pozornost usmjerena na pojedine integralne komponente SD WAN rješenja i posebnih značajki korištenih u njihovoj integraciji u specifičan SD-WAN sustav.

Uz detaljan prikaz i objašnjenje mrežnih modela cilj rada je dati uvid u osnovni prikaz jednog od rješenja vodećih vendora SD WAN sustava pomoću testnog modela četiri podružnice koje rade preko različitih pristupnih mreža na različitim sustavima SD-WAN i MPLS. Svrha rada je rezultatima prikazati prednosti SD-WAN sustava naspram MPLS-a te prikazati razliku u kašnjenju protoka paketa koje sa sobom nose različite pristupne tehnologije.

Uz mogućnost korištenja *Versa headend* uređaja, Versa networks je poznat po svojim visokim performansama i skalabilnosti. Sama segmentacija podataka daje budućim korisnicima sustava višestruki pristup sustavu, a dodatna kontrolna razina daje potpunu izolaciju unutar podružnica i odjela. Još jedna značajka koju Versu čini posebnom jest *Zero Time Provisioning* čime se drastično smanjuje vrijeme implementacije te samim time i vrijeme potrebno za upravljanje promjenama među različitim stranicama.

U uvodnom dijelu rada dan je uvod u temu, cilj, svrha i kratki opis strukture rada odnosno poglavlja obrađena u radu.

U drugom poglavlju rada dobit će se odgovor na pitanje zašto je došlo do potrebe za proširenjem postojećeg WAN sustava te koje pogodnosti nosi implementacija SD-WAN-a po pitanju QoE i QoS parametara.

U trećem poglavlju opisuje se logička i fizička arhitektura SD-WAN-a te se ukratko opisuju uloge svake.

Četvrto poglavlje daje usporedbu između WAN i SD-WAN tehnologija gledano kroz prizmu QoS zahtjeva.

Peto poglavlje prikazuje SD-WAN rješenje jednog od vodećih proizvođača na tržištu. Prikazuju se i opisuju glavni elementi Versa mrežnog rješenja. U drugoj polovici poglavlja prikazani su rezultati testa između podružnica koje imaju osiguran pristup mreži putem Versa opreme.

Šesto poglavlje rada skreće pozornost na različitosti u SD-WAN rješenjima proizvođača. Poduzeće bi trebalo na temelju svojih potreba pronaći optimalno rješenje. Opisani su izazovi s kojima se susreću poduzeća pri integraciji SD-WAN tehnologije na već postojeću infrastrukturu.

U zaključku su sintetizirane sve informacije prikupljene i obrađene tijekom izrade ovog rada.

2. ZNAČAJKE SD-WAN MREŽA

Jedan od glavnih ciljeva softverski definiranih mreža je omogućavanje mrežnim administratorima i inženjerima direktnu i brzu reakciju na promjenu poslovnih zahtjeva putem jedne centralizirane upravljačke jedinice. Softverski definirane mreže obuhvaćaju više vrsta mrežnih tehnologija koje su osmišljene kako bi se osigurala fleksibilnost mreže i kako bi se podržala virtualna infrastruktura poslužitelja koja bi zadovoljila velike potrebe propusnosti današnjih aplikacija. Svrha ovih mreža je razgraničavanje mrežnog upravljanja i prosljeđivanja, čime se omogućuje da mrežno upravljanje postane izravno programabilno i da se temeljna infrastruktura proširi.

SD-WAN (engl. *Software Defined-Wide Area Network*) mreže jedan su od modela mrežne strukture putem kojih se prvenstveno nastoje optimizirati mrežni resursi uz istodobno optimiziranje i prilagodbu mreže potrebama poslovnih korisnika, njihovim aplikacijama i prometu. SD-WAN je također i odgovor na sve zahtjevnije probleme osiguravanja QoE[1] i QoS[2] u višeuslužnim mrežama. SW-WAN mreža također podrazumijeva i operativnu strukturu koja se umnogome razlikuje od fizičkih uređaja i dosadašnjih konvencionalnih mreža jer se pomoću SDN kontrolera upravlja mrežnom arhitekturom i automatizacijom. Spomenuti SDN kontroleri pritom nisu mrežni uređaji, nego sredstva kojima je moguće iskoristiti prednosti pohrane podataka i dostupnosti suvremenih resursa računalstva. SD WAN mreže izgrađuju se na otvorenim platformama, što im omogućuje korištenje i upravljanje mrežne opreme različitih proizvođača. Razdvajanjem upravljačkih i prijenosnih slojeva umnogome se povećava fleksibilnost i ubrzava vrijeme plasiranja novih aplikacija na tržište. Vrijeme reagiranja na prekide u mreži poboljšava dostupnost i mogućnosti upravljanja mrežom, dok izrazita tendencija prema različitim mogućnostima programiranja uvelike olakšava IT organizacijama automatizaciju mrežnih funkcija smanjujući njihove operativne troškove. Mrežna infrastruktura SD WAN-a je dinamična, isplativa i prilagodljiva u razvoju, čime je izvrsna za dinamičnu prirodu velike propusnosti današnjih aplikacija. [1]

Najzastupljenija metoda umrežavanja putem središnje upravljačke jedinice danas se temelji na razdvajanju upravljačke logike na računalne resurse izvan uređaja. Spomenuti SDN kontroleri ključna su komponenta koja pruža centralizirani prikaz cjelokupne mreže i

[1] *QoE* ITU-T definira kvalitetu iskustva *(QoE)* kao "sveukupnu prihvatljivost aplikacije ili usluge, prema subjektivnoj percepciji krajnjeg korisnika". [26]
[2] *Quality of Service* predstavlja mogućnost dodjeljivanja različitih prioriteta različitim aplikacijama, korisnicima i tokovima podataka ili osiguranja određenog nivoa usluge za neki tok podataka. [27]

omogućuje mrežnim administratorima upravljanje osnovnim sustavima. Inicijalnim standardom u softverski definiranim mrežama smatra se *OpenFlow*, dok je najfrekventniji protokola u upotrebi *Southbound API* (engl. *Application Programming Interface*). *Northbound API* je s druge strane protokol čija je osnovna funkcija komunikacija s aplikacijama i pomaganje mrežnim administratorima da oblikuju i programiraju promet i implementiraju usluge po osobnim potrebama. *OpenFlow* je ujedno i prvi otvoreni standard za komunikacijski protokol koji osigurava povezivanje upravljačke razine s razinom prosljeđivanja, ali sasvim sigurno nije jedini dostupan razvojni protokol za softverski definirane mreže, [1].

OpenFlow se u dostupnoj literaturi obično spominje kao sinonim za softverski definirano umrežavanje, ali je zapravo samo jedan od elemenata čitave infrastrukture. *OpenFlow* protocol sličan je bilo kojem drugom protokolu za umrežavanje koji za cilj ima programiranje puta za podatke i zapravo je spoj klijent- server tehnologije i različitih protokola usmjeravanja. Ključne komponente ovog protokola dio su zajedničke definicije softverski definiranih mreža, a obuhvaćaju odvajanje kontrolne i podatkovne cjeline, korištenje standardiziranog protokola između kontrolera i agenta i pružanje mrežnog programiranja iz centraliziranog pogleda. *OpenFlow* je ujedno i skup protokola sačinjen od dva dijela: *Wire* protokola za uspostavu kontrolne sesije i konfiguracijskih i upravljačkih protokola za dodjeljivanje fizičkih portova određenom kontroleru i determiniranja ponašanja kod neuspjelog povezivanja s kontrolerom.

OpenFlow otvoreni je protokol temeljen na standardima koji definiraju način kojim kontrolna cjelina može biti konfigurirana i kontrolirana s centralnog mjesta. Korištenjem *OpenFlow* protokola kontroler može upravljati prosljeđivanjem paketa kroz mrežu, a protokol standardizira jedan centralni protokol koji ima mogućnost stvaranja tablice prosljeđivanja i upravljanja istima zamjenjujući sve ostale tablice prosljeđivanja.

Arhitektura *Open Flow*-a dijeli se na četiri komponente kao što su:

- *Message Layer*
- *State Machine*
- *System Interface*
- *Data Model*

Message Layer je temelj protokola sa zadaćom definiranja ispravne strukture i semantike poruka uz podržane mogućnosti konstruiranja, kopiranja, usporedbe, ispisa i

upravljanja porukama. *State Machine* definira ponašanje protokola na nižoj razini te se koristi za opisivanje radnji kao što su pregovaranje, otkrivanje sposobnosti, kontrole prometnog toka, isporuke itd. *System Interface* definira način komunikacije protokola s okolinom te spaja obavezna i moguća sučelja zajedničkom namjenom kao što su TLS[3] i TCP[4] transportni protokoli. *Data Modela* obuhvaća switcheve koji održavaju relacijski model podataka koji sadrži atribute za svaku *OpenFlow* apstrakciju, dok spomenuti atributi mogu opisivati sposobnost apstrakcije, stanje konfiguracije ili neki skup aktualnih statistika [17]. Kontroler softverski definirane mreže komunicira s *OpenFlow* kompatibilnim preklopnicima koristeći *OpenFlow* koji pokreće SSL (*Secure Sockets Layer*)[5]. Switchev-i su međusobno povezani i s krajnjim korisnicima čine izvorišta i odredišta tokova paketa. Poruke razmijenjene u *OpenFlow* protokolu dijelimo u tri glavne skupine: poruke kontrolera, asinkrone poruke, simetrične poruke.

Softverski definirana umrežavanja omogućila su veliki napredak u razvoju podatkovnih centara, što također rezultira fleksibilnijim načinom upravljanja mrežom. Pohrana informacija i računalstvo su upravo stoga značajno profitirali navedenim inovacijama u virtualizaciji i automatizaciji uz još uvijek prisutna pojedina ograničenja u mrežama.

Softverski definirana mreža također može biti povezana i s drugom tehnologijom kao što je virtualizacija mrežnih funkcija NFV (*Network Function Virtualization*), koja omogućuje virtualizaciju mrežnih funkcija temeljenih na uređajima kao što su balanseri opterećenja i akceleratori za WAN (*Wide Area Network*). Navedeno centralizirano upravljanje omogućuje softverski definiranim mrežama da učinkovito prate virtualne funkcije mreže koje omogućuje NFV. [3].

[3] TLS protokol omogućuje aplikacijama komunikaciju preko mreže na način da se spriječi prisluškivanje, izmjenu i lažiranje poruka. [22]
[4] TCP *(Transmission Control Protocol)* je dominantan, spojevni, prijenosni protokol interneta, garantira pouzdanu isporuku podataka od izvorišta do odredišta u kontroliranom redoslijedu. [23]
[5] SSL (eng. Secure Sockets Layer) protokol je standardizirana sigurnosna tehnologija za kreiranje kriptirane veze između poslužitelja i preglednika. Njome se osigurava zadržavanje privatnosti i sigurnosti svih podataka koji se razmjenjuju između sudionika komunikacije. [22]

3. ARHITEKTURA PLATFORME SD-WAN-a

Ubrzanim razvojem mrežnih aplikacija povećavaju se i zahtjevi za brzinom obrade podataka i upravljanjem paketima u mrežnim uređajima poput usmjeritelja, komutatora i ostalim sličnim uređajima. Temeljni koncept softverski definiranog upravljanja mrežom je upravo razdvajanje vertikalne mrežne infrastrukture na poseban upravljački i podatkovni sloj uz zadržavanje ostalih mogućnosti programabilnosti mreža. Središnja upravljačka jedinica softverski definiranog upravljanja je temeljna komponenta odgovorna za upravljanje uređajima pod svojom domenom. Arhitektura softverski definirane mreže se sastoji od tri sloja: aplikacijskog sloja, upravljačkog sloja i fizičkog sloja.

Upravljački sloj zadužen je za sve složene funkcije kao što su usmjeravanje, određivanje pravila i sigurnosnih provjera te se sastoji od jednog ili više poslužitelja. Softverski definirana upravljačka jedinica ili kontroler definira protok podataka na podatkovnoj razini ili fizičkom sloju. Funkcija kontrolera je također i regulacija te odobravanje i potvrđivanje da je komunikacija mrežnim resursima dopuštena. Zadaća kontrolera je i izračunavanje rute i dostavljanje informacija o propuštanju navedenog prometnog toka dužinom određene rute. Switch-evi su zaduženi za upravljanje daljnjim usmjeravanjem, dok se komunikacija između njih i kontrolera odvija se putem *OpenFlow* protokola.

U spomenutoj infrastrukturi kontroleri softverski definiranih mreža obavljaju zadaću [16]:

- definiranja mrežnih uređaja koji čine samu infrastrukturu mreže
- definiranje korisničke opreme poput stolnih ili prijenosnih računala, pametnih telefona, printera itd.
- upravljanja mrežnom topologijom te održavanjem informacija o povezanosti između mrežnih uređaja i korisničke opreme na koju su izravno povezani
- upravljanja prijenosom toka podataka, održavanjem tablica usmjeravanja kojima upravlja kontroler i obavljanjem svih potrebnih koordinacija s uređajima

Unutar infrastrukture softverski definirane mreže switch-evi obavljaju sljedeće funkcije:

- prosljeđivanje prvog paketa prijenosa na kontroler, uz dopuštanje donošenja odluke treba li se navedeni tok podataka dodati u tablicu usmjeravanja *switch-a*
- prosljeđivanje dolaznih paketa s odgovarajućih portova na temelju tablice usmjeravanja koja sadrži potencijalne informacije o prioritetima posluživanja koje određuje kontroler i
- eventualno ispuštanje paketa na određenoj ruti ukoliko je kontrolerom prethodno određeno u sigurnosne svrhe ili specifične zahtjeve za kontroliranje i upravljanje prometom.

Arhitekturu softverski definirane mreže moguće je tumačiti i definirati putem tri apstrakcijska sloja: prosljeđivanje, distribucija i specifikacije. Apstrakcijski sloj prosljeđivanja pritom je neovisan o fizičkim svojstvima mreže i odrađuje ulogu izvršavanja i podrške aplikacijski proslijeđenim zahtjevima. Distribucijski sloj čini temeljnu komponentu za rad mrežnih aplikacija uz logički centraliziranu ulogu upravljanja mrežnim uređajima i prikupljanja informacija o njihovom radu i međusobnoj povezanosti. Apstrakcijskom sloju specifikacije svojstven je način na koji mrežne aplikacije realiziraju vlastite primarne funkcije bez uplitanja u implementaciju na fizičkoj razini. Sloj specifikacije funkcionira putem virtualizacije i programskih jezika.

Velike mreže gotovo uvijek iziskuju postavljanje više od jednog kontrolera za upravljanje svim mrežnim uređajima tako da se u takvim slučajevima koriste zasebne softverski definirane domene. Razlozi za korištenje navedenih softverski definiranih domena su: privatnost, skalabilnost i dijeljena implementacija. Privatnost podrazumijeva odabir primjena različitih pravila o privatnosti na različitim domenama softverski definiranih mreža, pri čemu domena posjeduje mogućnost zadržavanja informacija o mreži unutar domene i njihovog otkrivanja entitetima izvan mreže. Skalabilnost uzima u obzir ograničenost broja uređaja kojima kontroler može uspješno upravljati te ukoliko je riječ o velikoj mreži, neophodno je implementirati više kontrolera. Transportna mreža može se sastojati od dijelova tradicionalne i novije infrastructure, prije čemu dijeljenje implementacije u više pojedinačno upravljanih domena jamči veću fleksibilnost [5].

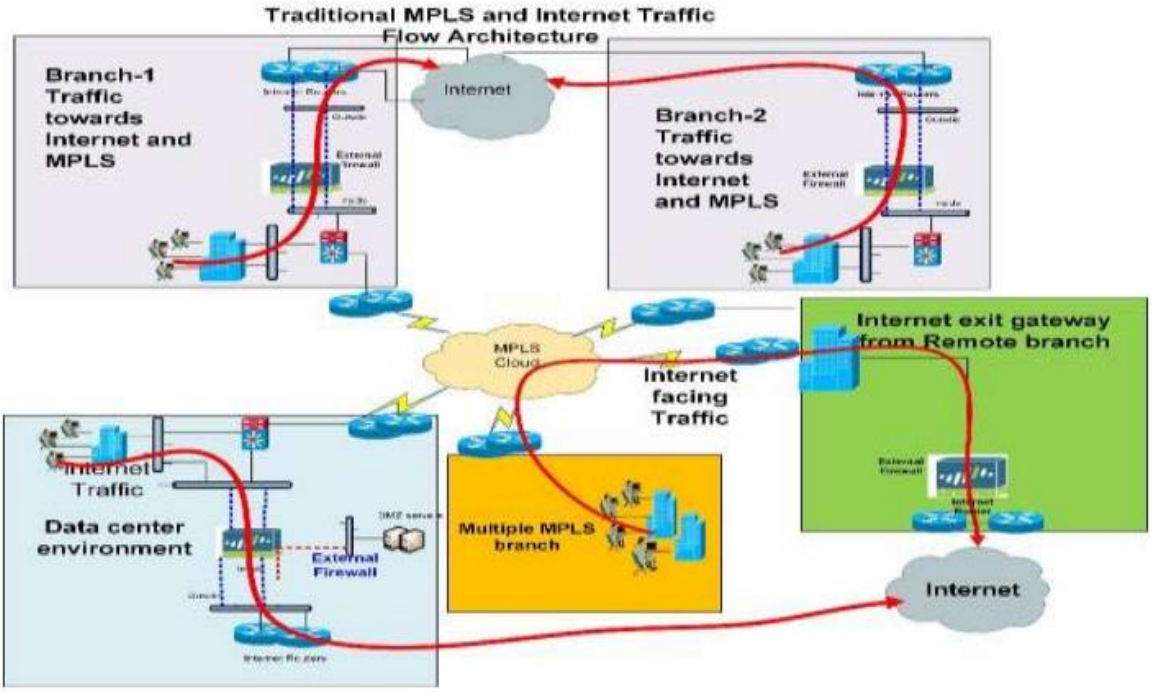
Unutar softverski definirane mreže različite domene stvaraju potrebu za komunikacijom između pojedinačnih kontrolera, što može biti omogućeno standardiziranim protokolom za razmjenu informacija usmjeravanja. SDNi (engl. *Software Defined Networking interface*) je jedan od razvojnih protokola koji je predviđen za povezivanje kontrolera domena softverski definiranih mreža, a njegove najbitnije funkcije jesu:

- postavljanje koordinata protokola od aplikacija kojima je poznat zahtjev za rutom, QoS i dogovorena pravila na razini usluge za različite SDN domene
- pružanje informacija o dostupnosti razmjene podataka između domena kako bi se pojednostavilo usmjeravanje

Odvajanje kontrolne i podatkovne cjeline predstavlja temeljno načelo softverski definirane mreže, a podrazumijeva omogućavanje određenih prednosti u odnosu na uobičajenu centraliziranu kontrolu. Kontrolna cjelina je lokalna jedinica koji se koristi za izradu ulaza tablice prosljeđivanja koje podatkovna cjelina kasnije koristi za prosljeđivanje prometa između ulaznih i izlaznih portova na uređaju. Mrežna topologija pohranjuje se pomoću skupa podataka koji se naziva RIB (*Routing Information Base*), dok FIB (*Forwarding Information Base*) predstavlja ulaze tablica prosljeđivanja te se često zrcale između kontrolne i podatkovne cjeline uređaja. Kontrolna i podatkovna cjelina su odvojene. Paketi se primaju na ulaznim portovima gdje se podatkovna cjelina nalazi. Kada je paket dostavljen kontrolnoj cjelini podatci koji se nalaze u paketu se obrađuju i rezultiraju promjenom RIB-a. Ako je primljeni paket došao od nepoznate MAC adrese, kontrolna cjelina vraća paket podatkovnoj cjelini koja prosljeđuje paket.

4. USPOREDBA TRADICIONALNIH WAN I SD WAN MREŽA

Prije same analize i isticanja prednosti SW WAN-a naspram tradicionalnih mrežnih modela neophodno je navesti i prezentirati značajke 'tradicionalnog' MPLS načina umrežavanja u svrhu usporedbe s SD-WAN modelom i njegovim specifičnim mrežnim značajkama. Prikazom slike niže daje se uvid u strujanje mrežnog prometa između podružnica koje se nalaze na različitim dijelovima MPLS-a.



Slika 1. Tradicionalni model arhitekture poduzeća [12]

Multi-Protocol Label Switching (MPLS) je tehnologija umrežavanja koja osigurava 'tradicionalni' model prosljeđivanja paketa kroz mrežu na elegantniji, efikasniji i brži način u usporedbi s nekadašnjim starijim tehnologijama poput ATM[6]-a i *Frame Relay*[7]*-a*. Ključna značajka prijenosa podataka kroz mrežu putem MPLS-a se sastoji u tome da se informacije iz zaglavlja paketa analiziraju samo jednom te se postupak usmjeravanja i prosljeđivanja paketa temelji isključivo na provjeravanju labela koji nije ništa drugo nego identifikacijska oznake

[6] ATM-mreža (prema engl. *Asynchronous Transfer Mode:* asinkroni način prijenosa), komunikacijska širokopojasna digitalna mreža u kojoj se primjenjuje asinkroni način prijenosa signala. [24]
[7] *Frame relay* je protokol za usmjeravanje okvira kroz mrežu na temelju polja IP adrese (identifikator povezivanja podatkovne veze) u okviru i za upravljanje smjerom ili virtualnim povezivanjem. [25]

paketa i koji su fiksne duljine. Vrhunac razvoja MPLS-a je postizanje poboljšanja na području propusnosti podataka i kašnjenja njihove isporuke kod usmjeravanja temeljenog na IP-u. Razvoju MPLS-a značajno je doprinijelo OSPF (engl. *Open Shortest Path First*)[8] protokol kojim su dodjeljivani paketi u mreži u kojoj se nalaze ATM komutatori odgovorni za usmjeravanje. Razvoj MPLS mreže rezultirao je spajanjem glasovnih i video aplikacija preko jedne IP mreže, zadovoljavanjem sve većih zahtjeva za IP prometom, omogućavanjem diferencijalnih razina usluga baziranih na IP-u i razvojem virtualne private mreže. MPLS tehnologijom nastojali su se izbjeći problematični nedostaci koji se pojavljuju kod tradicionalnog usmjeravanja poput velikih kašnjenja u isporuci paketa. Tehnikom zamjena labela tijekom prijenosa paketa kroz mrežu MPLS analizira zaglavlja paketa jednom, što znatno skraćuje vrijeme procesuiranja informacija u usmjerivačima u odnosu na IP tehnologiju, a značajne prednosti MPLS tehnologije su sljedeće:

- omogućava prijenos koji se bazira na okvirima i ćelijama,
- podrazumijeva integraciju MPLS mreže u već postojeće mreže
- može biti proširena u više segmenata kao što su MPLS i IP usmjerivači, QoS podrška za serijski orijentirane usluge, prometno inženjerstvo, kompatibilnost VPN (engl. *Virtual Private Network*), ATM, višeuslužni preklopnici i optički preklopnici
- MPLS integrira brzinu i performanse značajki drugog sloja sa stabilnošću i inteligencijom trećeg sloja
- nije limitiran na bilo koji posebni protocol, što omogućuje upotrebu višeslojnih tehnologija
- prilagođavanje većeg broja korisnika s MPLS tehnologijom
- podrška za beskonačno slaganje labela
- tehnikom prosljeđivanja labela omogućava se brže i jednostavnije usmjeravanje za razliku od usmjeravanja temeljenog na IP-u
- smanjuje se vrijeme obrade procesa i povećava učinkovitost

Funkcionalnost MPLS-a podijeljena ke na kontrolni i podatkovni dio, a aplikacije se razlikuju u kontrolnom dijelu, dok u dijelu prosljeđivanja koriste istu oznaku. Najvažnije MPLS aplikacije su:

[8] OSPF (*Open Shortest Path First*) usmjerivački protokol je otvoren, što znači da su njegove specifikacije javne. Definiran je RFC-om 2328 (OSPFv2). Koristi Dijkstra SPF algoritam za pronalaženje najkraćeg puta. [28]

- MPLS TE (engl. *MPLS Traffic Engineering*)
- MPLS QoS (engl. *MPLS Quality of Service*)

MPLS TE najvažnija je aplikacija MPLS-a, pri čemu MPLS prometno inženjerstvo ima veliku ulogu u implementaciji mrežnih usluga koji zahtijevaju određene garancije za kvalitetu usluge (QoS). Mreže bazirane na MPLS tehnologiji koriste TE mehanizme kako bi se smanjila zagušenja u mreži i poboljšale performanse mreže. TE podrazumijeva mogućnost promjene postojećih shema u svrhu efikasnijeg raspoređivanja prometnih tokova prema raspoloživim resursima. Svrha TE-a je smanjenje zagušenja u mreži i poboljšanje kvalitete usluge u vidu smanjenja kašnjenja tijekom dolaska paketa na odredište. Neke od glavnih funkcionalnosti MPLS TE su:

- izračunavanje puta
- optimizacija resursa
- distribucija informacija o linkovima
- TE LSP signalizacija
- MPLS prometno inženjerstvo s proširenjima za *DiffServ* arhitekturu
- protekcijska shema u slučaju ispada nekog od linkova
- tuneliranje i stavljanje labela

Podrška za QoS kod MPLS-a je povezana s klasom usluga CoS čije su osnovne funkcije:

- klasifikacija prometa i označavanje
- nadgledanje
- stavljanje u redove i nasumično odbacivanje
- raspoređivanje
- odašiljanje

Podrška za QoS kod MPLS-a je povezana s klasom usluga CoS, a osnovne funkcije QoS-a su:

- klasifikacija prometa i njegovo označavanje
- nadgledanje prometa
- sortiranje prometa u redove i nasumično odbacivanje istog
- raspoređivanje prometa
- odašiljanje prometa

Spomenuta klasifikacija u okviru QoS-a se provodi uzimajući u obzir postojanje različitih vrste aplikacija koje je na pravilan način potrebno tretirati u mreži. Presudni kriteriji za provođenje klasifikacije jesu izvorišna i odredišna adresa, tip protokola i aplikacije. Nadgledanje podrazumijeva postupak provjere poštivanja ugovora dolazećeg prometa, a odnosi se na interval i brzinu slanja. Različiti prometni tokovi slažu se u redove kako ne bi došlo do neželjenog odbacivanja prometa.

Nakon prezentacije specifičnih mogućnosti i funkcionalnosti MPLS modela i SD-WAN-a te usporedbom pojedinih značajki dolazimo do sljedećih zaključaka i sublimacije prednosti SD-WAN-a nad prijašnjim 'tradicionalnim' modelima. SD-WAN mreža je pojednostavljeni WAN model koji se odlikuje izrazito brzim raspoređivanjem i automatizacijom paketa i podataka. Jednostavnost SD WAN-a se također ocrtava u *Quality-of-Service* (QoS)-u koji se prilagođava automatiziranim poveznicama i jednostavnim, kontroliranim praćenjem kapaciteta. Softverski definirane mreže također imaju integriranu prednost skalabilne i sigurne komunikacije preko bilo kojeg prijenosa podataka koja je nije posve zastupljena i dovoljno definirana u tradicionalnim WAN tehnologijama.

Značajna pojednostavljena prednost SD WAN tehnologije je mogućnost upravljanja i orkestracije koja može biti lako i efikasno isporučena na oblaku. SD WAN model trenutačno predstavlja jedan od najučinkovitijih načina iskorištavanja punih potencijala WAN tehnologije u vidu objedinjavanja svih dostupnih WAN veza za pružanje agregiranih kapaciteta te lake distribucije usluge putem oblaka uz jednostavno *'policy-based'* umetanje. Model SD WAN-a također podrazumijeva zajamčena izvedbu aplikacije, odnosno prosljeđivanje na temelju procjene karakteristika WAN-a u stvarnom vremenu, uključujući pritom u obzir karakteristike poput kvalitete i kapaciteta link-a.

Prednost SD WAN-a je također i mogućnost dinamične reakcije na temelju poslovne politike o kriterijima izvedbe ili sigurnosti te takozvane 'aktivno-aktivne' podrške za pružanje brze reakcije na prekide unutar ili prekide rada WAN mreže tako da se tijek primjene aplikacije može nastaviti. Bitna značajka SD WAN-a je i njegova visoka razina dostupnosti, koja se odlikuje u većoj fleksibilnosti u odabiru pružatelja usluge i promjeni same usluge te brže vrijeme pružanja same usluge i automatiziranost konfiguracije iste. SD WAN također, za razliku od MPLS-a i tradicionalnih WAN-ova podrazumijeva i centralno upravljanje i olakšano rješavanje problema za složena korisnička okruženja [6].

5. PREGLED IMPLEMENTACIJE SD WAN-a NA PRIMJERU RJEŠENJA VERSA

Rješenja *Versa Networks* omogućuju davateljima usluga (ISP) i velikim poduzećima transformaciju WAN-a i mreže podružnica kako bi se postiglo stvaranje puno više prednosti u poslovanju. Versin softverski definirani mrežni pristup omogućuje neusporedivu agilnost, uštedu troškova i fleksibilnost u odnosu na tradicionalni mrežni hardver. Versa rješenja pružateljima usluga omogućuju upravljanje sljedeće generacije usluge za *virtual customer premises equipment* (vCPE)[9] i softverski definirani WAN (SD-WAN) i upravljanu sigurnost.

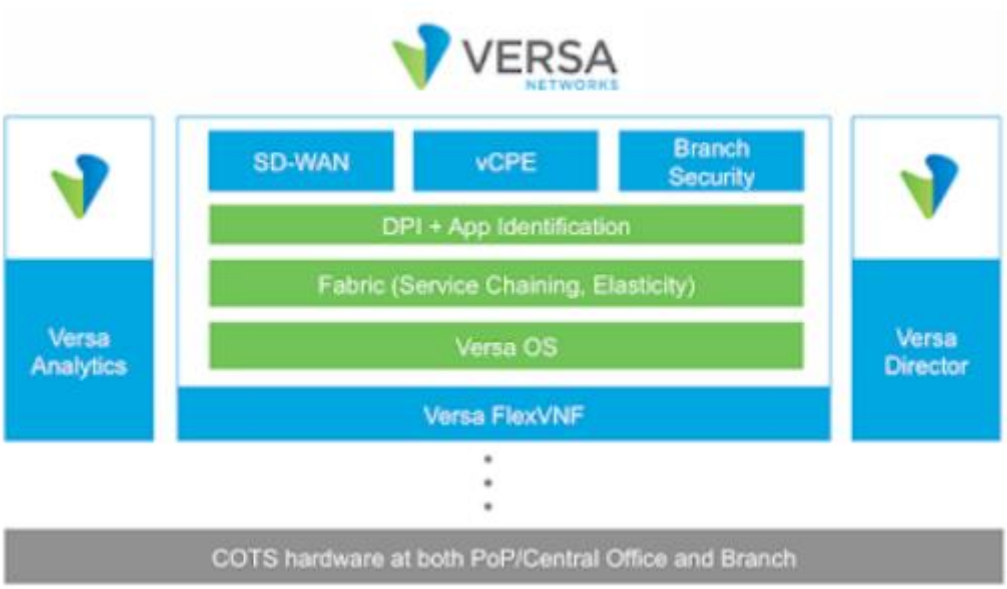
Versa SD-WAN posjeduje i vrlo fleksibilno *Versa FlexVNF* softversko rješenje koje omogućuje korisnicima da stvore široki spektar grana arhitekture iz tanke grane sa većinu virtualiziranih funkcija koje se nalaze se u točki prisutnosti (PoP)[10] ili u podatkovnom centru. *Virtual network functions* (VNFs) također čine mrežnu arhitekturu gdje su L3 - L7 mreže i sigurnosne usluge virtualizirane u softveru i odvojene od osnovnog hardvera. Koristeći takav način pristupa uključuje uvođenje novih ili nadogradnju postojećih mrežnih i sigurnosnih elemenata čime usluge postaju što brže, fleksibilnije manje složene, a pri čemu se značajno smanjuju operativni troškovi.

Versa FlexVNF uključuje najširi skup VNF-ovoj industriji – od velikog skupa mrežnih mogućnosti, uključujući SD-WAN, do širokog raspona osnovnih i naprednih sigurnosnih funkcija – što omogućuje bogatiji dizajn arhitekture upravljanih usluga i poduzeća te agilniju isporuku budući da su dizajnirani da rade zajedno. Snažno ulančavanje usluga za usluge Versa i trećih strana, uključujući uređaje, omogućuje pružateljima usluga i velikim poduzećima jednostavnu integraciju više mreža i sigurnosnih funkcija u složene upravljane usluge i arhitekture poduzeća. *Versa FlexVNF* ima ugrađen multi-tenancy koji omogućuje uslugu tisućama kupaca, pružajući fleksibilnost implementacije i ekonomija razmjera tj. opadanje jediničnih troškova. [18]

[9] Virtualni CPE učinkovito rješava nadolazeće izazove, virtualizirajući većinu CPE funkcija u mrež, ima za cilj osigurati minimalan potreban hardver na mjestu korisnika i premjestiti tradicionalne CPE funkcije na CSP (customer service provider) mrežu. [30]

[10] *Point of presence* (POP) je točka na kojoj dvije ili više različitih mreža ili komunikacijskih uređaja grade međusobno vezu. POP se uglavnom odnosi na pristupnu točku, lokaciju ili objekt koji se povezuje na i pomaže drugim uređajima da uspostave vezu s Internetom. [29]

Versa headend je grupa komponenti koje su zajedno odgovorne za rad između *headenda* i *branch* uređaja koji su dostupni preko interneta ili preko privatne mreže. Versa *headend* sastoji se od tri komponente: *Versa Director*, *Versa Analytics* i *Versa Controller* uređaja. Komponente headenda rade zajedno i upravljaju mrežom *Versa FlexVNF* uređaja koji se nalaze na branchevima i koji su povezani putem javne mreže (poput Interneta) ili privatne mreže (poput MPLS mreže) ili kroz oba. Versa headend se nalazi u podatkovnom centru.



Slika 2. Općeniti prikaz arhitekture Versa rješenje SD WAN-a [20]

Headend jedinice u ISP okruženju moraju biti podijeljene na geo-redudantne data centre, pri čemu nema strogih zahtjeva u vezi s *delay* i *jitter*, tako da bi se navedena podjela mogla učiniti. Za vrijeme konfiguracije SD-WAN, ISP je odgovoran za dodjelu *brancheva* pojedinim kontrolerima. Čitavom mrežom i sigurnošću njezinih komponenti upravlja se centralno putem platforme za upravljanje *Versa Director*.

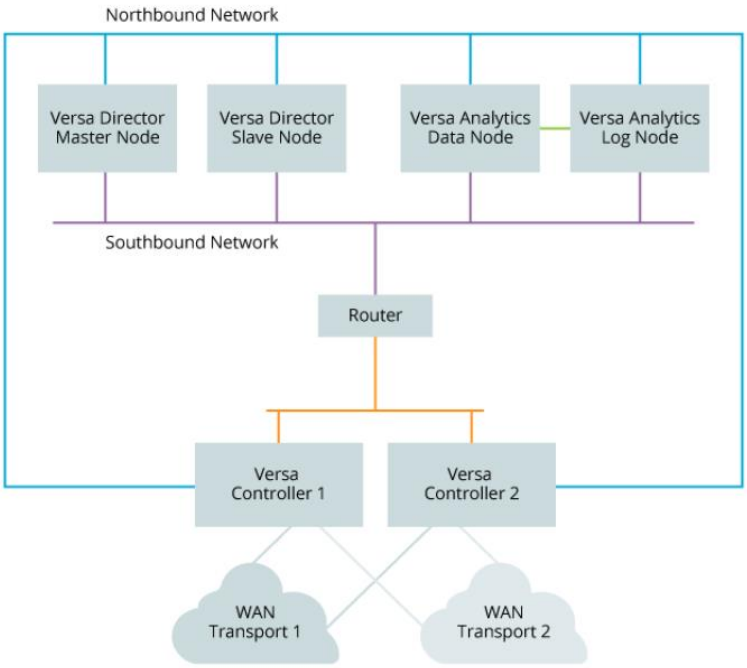
Versa Director je platforma za upravljanje rezervacijama i upravljanje koja obavlja sljedeće funkcije:

- Centralizirana single-pane-glass konfiguracija, upravljanje i nadzor *Controllera*
- Upravljanje životnim ciklusom instance *Versa FlexVNF*
- Visoka raspoloživost (HA) u modu active-standby
- *Virtual network function manager* (VNFM)
- *Zero-Touch provisioning* (ZTP) *Versa FlexVNF-ova* na branch i hub siteovima.

Značajke *Versa Director* platforme također uključuju:

- *Network overlay support* - sva *Versa FlexVNF* komunikacija odvija se pomoću *overlay*[11] mrežnog tunela koji osigurava dosljedno upravljanje u različitim WAN okruženjima.
- *Role-based access control (RBAC)* - omogućuje ograničavanje pristupa i definiranje mogućnosti *read* i *write* prava za različite vrste usera
- Nadzor uređaja – *dashboard* mogućnosti na svim uređajima, uključujući testove brzine tj. *Bandwitha*.

Versa Director također pruža pristup *Versa Analytics* prema definiranim *role-based* ulogama poput: *Interfaces Analitics Node-a*, *Northbount* za GUI and MGMT *access*, *Southbound* za komunikaciju s *Controllerom* (s CPEovima preko overlay-a) i *Directorom*, *Sync for Cluster*[12] *sync* (prikazano na slici niže).



Slika 3. Headend connectivity matrix [21]

[11] *Overlay* mrežu karakterizira virtualni sloj na vrhu fizičke mrežne infrastrukture. Nešto kao VLAN, ali obično se odnosi na složenije virtualne slojeve iz softverski definiranog umrežavanja (SDN) ili softverski definirane šire mreže (SD-WAN). [32]

[12] *Cluster* - klaster je skup računalnih resursa i konfiguracija na kojima pokreću radna opterećenja podatkovnog inženjerstva, znanosti o podacima i analize podataka. [31]

Versa Analytics je platforma dizajnirana za *Versa FlexVNF* i upravljane usluge. *Versa Analytics* pruža vidljivost na *Versa FlexVNF* uređajima. Analizirane podatke moguće je koristiti za obavljanje polaznih podataka, korelacije i predviđanja o *Versa FlexVNF* uređajima. *Versa Analytics* pruža pregled podataka u stvarnom vremenu te kroz povijest, uz mogućnost stvaranja izvješća upotrebom uzoraka, trendova, sigurnosnih događaja i alarma.

Versa controller je instanca *FlexVNF* koja osigurava *controll plane* element za sve *Versa FlexVNF* instance u mreži, uključujući *branches, hubs i gateways* (čvorove). Spomenuti kontroler obično se nalazi na centraliziranom mjestu (data centar, središnja lokacija ili javni oblak) s kojeg se povezuje na sve čvorove u mreži.

Versa Controller također je povezan s *FlexVNF-ovima* preko kontrolnih *overlay* tunela koji nose i IPsec i MP-BGP promet.

Controller rukovodi svim upravljačkim aktivnostima između udaljenih (*branch*) i glavnih (*hub*) čvorova tj. *FlexVNF* routera.

Branch routeri u *Versa Networks* rješenju pružaju networking i security funkcije objedinjene u jednu *FlexVNF* instancu koja se može primijeniti na *Versa Cloud Services Gateway* ili kao virtualni stroj (VM). Branchevi se nalaze, kao što i naziv govori, na mjestima podružnica. Povezani su međusobno i s glavnom glavom putem javne mreže (poput interneta) ili privatne mreže (poput MPLS mreže) ili oboje.

Brancheve je moguće implementirati u jednoj od sljedećih topologija:

- *Hub&Spoke*
- *Full Mash*
- *Partial mesh*.

Versa Director nudi *workflow*-e koji prikazuju konfiguraciju *brancheva* u određenoj topologiji.

U arhitekturama SD-WAN sustava gateway služi kao element za povezivanje SD-WAN domene s domenom koja ne pripada SD-WAN-u poput MPLS VPN ili IPSec VPN.

Gateway može biti prikazan i sigurnosnom uslugom za povezivanje s cloud ili SaaS aplikacijama. Primarna funkcija SD-WAN *gateway*-a je distribucija *routing* informacija između MPLS VPN i SD-WAN VPN domena kako bi se *forwardao* promet između dvije domene.

U rješenju *Versa Networks SD-WAN*, svaka *FlexVNF* instanca u mreži može se konfigurirati kao *gateway*. To znači da svaki čvor u Versa SD-WAN pruža vezu između MPLS VPN domene i SD-WAN VPN domene za prosljeđivanje podatkovnog prometa s jedne domene na drugu.

Slika 4. prikazuje glavne komponente ovisno o veličini mreža.

	Up to 2500 CPEs and 500 Tenants	**Up to 1000 CPEs and 200 Tenants**	**Up to 500 CPEs and 100 Tenants**
Director	2 single-socket servers (for HA) For each server: • 16 cores • 64 GB RAM • 512 GB SSD • 2 network ports	2 single-socket servers (for HA) For each server: • 16 cores • 64 GB RAM • 512 GB SSD • 2 network ports	2 single-socket servers (for HA) For each server: • 8 cores • 16 GB RAM • 256 GB SSD • 2 network ports
Analytics	6 single-socket servers per cluster For each server: • 16 cores • 128 GB RAM • 2 TB SSD • 2 network ports	4 single-socket servers per cluster For each server: • 16 cores • 128 GB RAM • 2 TB SSD • 2 network ports	2 single-socket servers per cluster For each server: • 16 cores • 64 GB RAM • 1 TB SSD • 2 network ports
Log Collector/ Forwarder	4 single-socket servers per cluster For each server: • 4 cores minimum • 8 GB RAM • 128 GB SSD minimum • 2 network ports	Integrated with Analytics	Integrated with Analytics

Slika 4. Minimalni hardverski zahtjevi za Versa Director, Versa Analytics i Versa Controller [19]

Multiprotocol BGP [13]promet distribuira informacije o dostupnosti za sve čvorove. *Versa Controller* distribuira BPG rute prema VPN-ovima i *tenantima*. IPsec veza između *brancheva* i Versa SD-WAN kontrolera distribuira IPsec ključeve na druge brancheve za direktnu komunikaciju među *branchevima*. Rezultat toga je da čvorovi grane moraju održavati N + 1 ključeva umjesto NxN ključeva.

[13] *Multiprotocol* proširenja za BGP, koja se ponekad nazivaju i *Multiprotocol* BGP ili *Multicast* BGP i definirana u IETF RFC 4760, proširenje su za *Border Gateway Protocol* koji omogućava paralelno distribuiranje različitih vrsta adresa. [33]

Otkrivanjem potencijalnih smetnji na *control plane* dijelu upravlja *Internet Key Exchange* (IKE) mehanizam za uklanjanje kvarova, koji se naziva *'dead peer detection'*. Sigurni IKE kanal[14] prenosi sav kontrolni promet između *branch routera* i *Versa controllera*, koji potom komunicira s *Versa Director* i *Versa Analytics* čvorovima, što bi značilo kako *Versa Director* i *Versa Analytics* imaju povezivost sa različitim CPE-ovima preko *Versa Controllera* na način da *Versa Director* šalje paket prema *overlay* adresi, koja mora biti usmjerena preko *Versa Controlera* jer on uspostavlja tunel.

5.1. Analiza mrežnih performansi SD WAN-a u *Full Mesh* topologiji – testiranje odziva

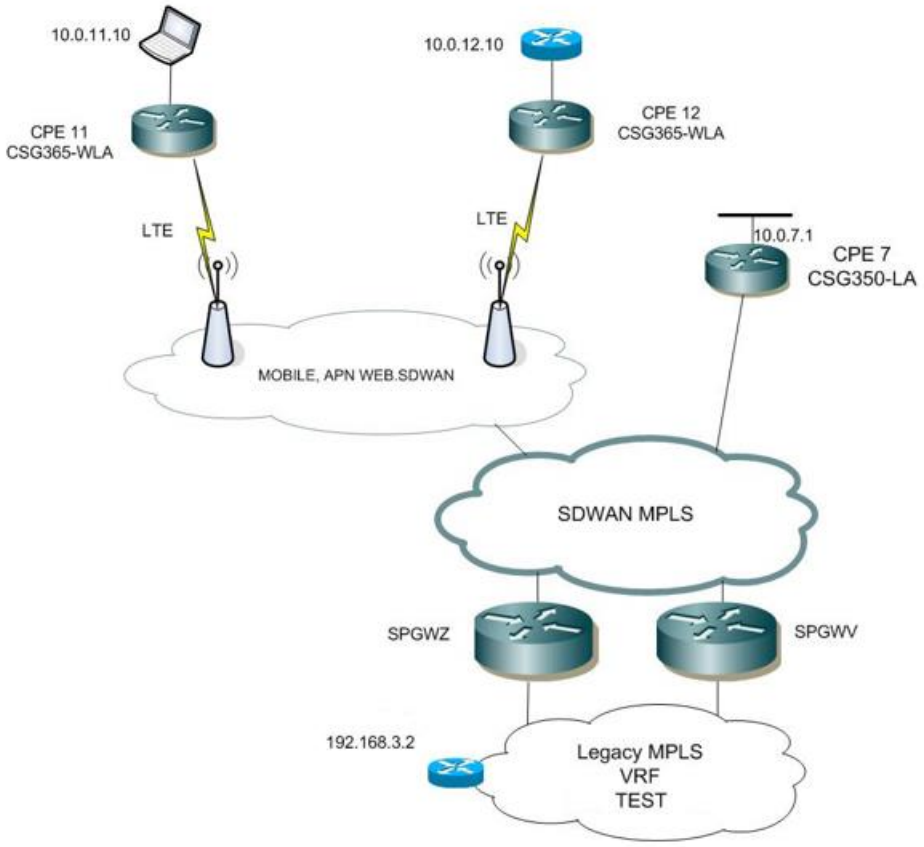
U ovom dijelu rada analiziraju se tri odvojena *brancha*:

Prvi *branch* koji ima vezu s MPLS vezom (privatna mreža) te dva brancha s LTE vezama koje prolaze kroz privatni APN.

Dvije lokacije CPE11 i CPE12 povezanesu na MPLS transport kroz privatni APN web.sdwan. Za navedene lokacije koristi se Versa CPE model CSG365-WLA.

Jedna lokacija spojena je stalnom MPLS vezom u vrf[15] SDWAN (CPE7). Ovdje se koristi CSG350-LA. Za testove prema *Legacy MPLS-u* koristiti će se udaljeni *host* u privatnom LAN-u koje se nalazi u vrfu TEST spojen preko 2 *gatewaya* (SPGWZ i SPGWV) .

[14] IKE (*Internet key exchange*) je standard protokola za upravljanje ključevima koji se koristi zajedno sa standardom *IPSec*. *IPSec* je značajka koja pruža robusnu provjeru autentičnosti i enkripciju IP paketa. [34]
[15] VRF (*virtual routing and forwarding*) je tehnologija uključena u mrežne usmjerivače internetskog protokola (IP) koja omogućuje postojanje više instanci tablice usmjeravanja na virtualnom usmjerivaču i istovremeni rad.[38]



Slika 5. Topologija testne mreže [autor]

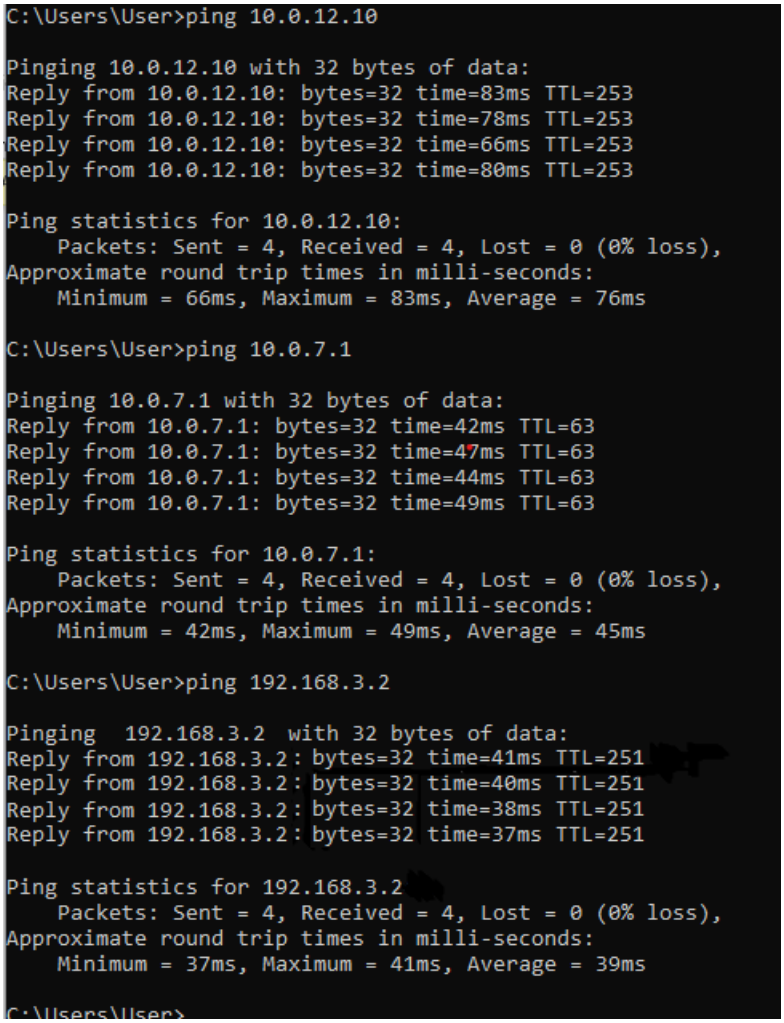
Računalo ima IP adresu 10.0.11.10 i deafult *gateway* mu je 10.10.11.1 (CPE 11).

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bd11:44dc:5a44:ac46%14
   IPv4 Address. . . . . . . . . . . : 10.0.11.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.11.1
```

Slika 6. Osnovni podaci mreže na CPE11 [autor]

Uspješno testiranje odziva prema svim lokacijama:



Slika 7. Uspješan ping prema udaljenim branchevima [autor]

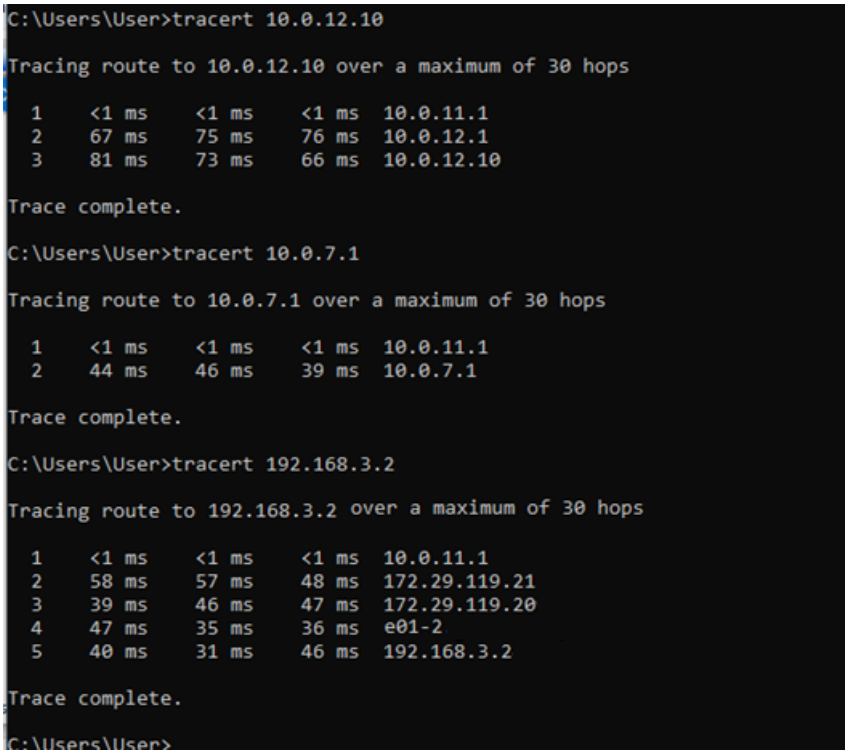
Uvidom u rezultate mjerenja odziva udaljenih lokacija vidljiva je razlika u vremenu odziva ovisno kroz koju vrstu pristupne mreže promet prolazi.

5.2. Analiza mrežnih performansi SD WAN-a u *Full Mesh* topologiji – *traceroute*

Analizirat će se *traceroute*[16] do udaljenih lokacija. Vidljivo kako su lokacije 12 i 7 samo jedan *hop* udaljene od CPE 11 s obzirom da se radi o SD WAN lokacijama koje su nam direktno dostupne zbog *Full Mesh*[17] topologije.

[16] *Traceroute* pruža kartu *hop*ova na koji podaci na internetu putuju od izvora do odredišta. [35]

[17] *Full mesh* topologija se sastoji od čvorova koji mogu imati direktne veze sa svim čvorovima u mreži (*full mesh*). [36]



Slika 8. Trace prema ostalim branchevima [autor]

Prikazani *trace*-ovi razlikuju se zato što smo prema CPE12 pratili *hopove* do *host*-a koji je spojen na LAN CPEa12, a kod 7, LAN na samom CPE7 jer nemamo *hosta* u LAN-u.

U *trace-u* prema koncentratoru na *Legacy MPLS-u* očekivano imamo više *hopova* jer moramo proći kroz SPGW. 172.29.119.21 je adresa SPGWZ koji je ujedno i primarni *gateway* tako da će promet ići očekivanim putem.

6. PROBLEMI INTEGRACIJE KOD IMPLEMENTACIJE SD-WAN TEHNOLOGIJE

Izazovi pri integraciji SD-WAN-a na postojeću infrastrukturu mogu biti raznoliki ovisno o fazi implementacije i vlastitim preferencama:

- Zabrinutost za sigurnost
- Izazov implementacije
- Izazov praćenja i korelacije
- Interoperabilnost i standardizacija
- Izazovi izvedbe

6.1. Zabrinutost za sigurnost

Sigurnosno SD-WAN rješenje dizajniralo je više proizvođača opreme (OEM) kao što su Riverbed, Cisco, VMWARE, Versa, Citrix itd.

Većina SD-WAN sigurnosnih rješenja specifična su za OEM. Postojeća tradicionalna infrastruktura već ima implementirane sigurnosne proizvode od drugih OEM-a Checkpoint, Palo Alto, Cisco itd. Postojeći promet već se prati na razini poduzeća s različitom sigurnosnom platformom. SD-WAN sigurnosna rješenja razlikuju se jedno od drugog.

Integracija sigurnosne politike i njezine organizacije s postojećim sigurnosnim sustavom i SD-WAN sigurnošću postaje velika briga za organizaciju. Nekoliko dobavljača SD-WAN-a nudi integrirana sigurnosna rješenja, pri čemu neka pružaju i osnovne značajke vatrozida.

U današnje digitalno doba poslovni svijet izložen je rastućem sigurnosnom riziku gdje je potreban firewall napredne razine *Next Gen Firewall*.

Uvođenje *gatewaya* napredne razine sigurnosti u branchu samo zbog uvođenja SD-WAN-a nije isplativo rješenje za proračun IT poduzeća, ali ignoriranje sigurnosne razine u projektiranju SD WAN-a može biti pogubna situacija za organizaciju.

Otkrivanje prijetnji i korelacije logova analize prometa od izvora do odredišta i logovi obrnutog prometa vrlo su kritično područje.

Današnja SD-WAN arhitektura nije dizajnirana da podržava tako visoku razinu napredne zaštite.

SD-WAN rješenje mora biti dizajnirano kao zaštićeni SD/WAN koji treba podržavati IPS, IDS, Firewall, AntiBot, Anti Malware, DNS otkrivanje napada i Web filtriranje. SD-WAN rješenje mora biti sposobno integrirati se s postojećim sigurnosnim alatima. [11]

6.2. Izazov implementacije

Izazov implementacije SD-WAN-a jedan je od najvećih problema. U idealnom slučaju, nastavlja se implementacija sa *Proof of Concept* (PoC) kada se u fazama poduzima mudrija implementacija. Model implementacije varira ovisno o odabranoj tehnologiji zajedno s arhitekturom. Aplikacije osjetljive na kašnjenje, propusnost i *jitter* glavna su područja koja treba razmotriti tijekom implementacije.

SD-WAN arhitektura treba biti stvorena u cilju što bolje izvedbe aplikacija. Optimiziran rad usluga vezan uz aplikacije glavni je cilj s kojim se susreće izazov implementacije. Kako bi se postigla što bolja izvedba promet se usmjerava različitim optimiziranim putevima do drugog odredišta pomoću MPLS-a i internet veza.

Tehnički izazov usmjeravanja prometa prema oblaku do oblaka temelj je usluge kao što je Office365 iz brancha potrebna je defaultna ruta za izlaz iz svake poslovnice.

U tradicionalnom modelu defaultna ruta usmjerena je prema mreži podatkovnog centra i od DC-a sav internet promet usmjerava se prema oblaku zadanom defaultnom rutom.

S obzirom na SD-WAN arhitekturu postoji potreba za izravnim izlazom iz svakog brancha što znači da je potrebna defaultna ruta iz svakog brancha prema SD-WAN uređaju.

Kada se promet usmjerava postoji potreba za vatrozidom aplikacijskog sloja za pregled prometa radi zaštite organizacije od vanjskog napada, znači da postoji potreba za integracijom aplikacije vatrozida visoke razine sa SD-WAN uređajima. [12]

Prema studiji koju je proveo PWC "*Global Crisis Survey*[13], *cyber* sigurnost postaje glavni rizik digitalnog poslovanja.

6.3. Izazov praćenja i korelacije

Praćenje toka prometa, log-ova i činjenica su konsolidirani zahtjevi za korelaciju pronalaska i identifikacije izvornog razloga prekida. Različiti OEM proizvodi stoga su rješenja integrirana u paketu s SD-WAN-om s obzirom da su praćenje log-ova i korelacija najveći izazovi u osposobljavanju te urednom funkcioniranju SD-WAN-a. [14] Osiguravajući faktor, donošenje odluka u stvarnom vremenu u pogledu odvraćanja prometa od jednog puta prema drugome suklado performansama u odgovarajućem trenutku jedna je od glavnih prednosti SD-WAN-a. Vidljivost uzorka prometa usko je vezana uz korelaciju s log-ovima.

6.4. Interoperabilnost i standardizacija

Interoperabilnost i standardizacija je teško usvojiva zadaća za koncept i rješenje kao što je SD-WAN upravo zbog nedostatka kompatibilnosti različitih vendora, što je ujedno i temeljni izazov za unifikaciju i prilagodbu SD WAN-a jedinstvenom i cjelovitom rješenju. SD-WAN kontroler i upravljačka razina za svaki OEM je prije svega zaštićeno vlasništvo pojedinog vendora. Napretkom tehnologije pokazuje se potreba za transformacijom SD-WAN tehnologije i prihvaćanje jedinstvenog upravljačkom modela iz razloga nekompatibilnosti i nemogućnosti integracije ostalih OEM SD-WAN tehnologija. Spajanje vendorskih okruženja ključno je za ostvarivanje punih potencijala SD-WAN tehnologije, dok standardizacija SD-WAN-a mora nužno biti odrađena u sinergiji industrijalizacije i standardizacijskog tijela čija je zadaća integracija i umrežavanje više tehnologija u jedanjedinstven i standardiziran model. [15]

7. ZAKLJUČAK

Pojavljivanjem novih mrežnih tehnologija dolazi i do rastuće potrebe i zahtjeva za boljom i kvalitetnijom uslugom. Konačni razvoj MPLS-a rezultirao je postizanjem poboljšanja glede propusnosti i kašnjenja paketa kod usmjeravanja temeljenom na IP-u, dok je cilj softverski definiranih mreža poput SD WAN-a omogućavanje brze i učinkovite reakcije mrežnim administratorima i inženjerima sukladno traženim promjenama poslovnih zahtjeva koji se u softverski definiranim mrežama odrađuje putem centralizirane upravljačke jedinice.

Softverski definirane mreže, za razliku od klasičnih tehnologija i prethodno spomenutog MPLS-a, obuhvaćaju više vrsta mrežnih tehnologija osmišljenih kako bi mreža bila fleksibilnija i optimizirana za podržavanje virtualne infrastrukture poslužitelja uz zadovoljavanje velike potrebe propusnosti današnjih aplikacija. Softverski definirane mreže imaju svrhu odvajanja procesa mrežnog upravljanja i prosljeđivanja, čime se osigurava izravno programiranje i upravljanje mrežom kao i tendencija da se temeljna infrastruktura proširi.

Versa Networks, lider je u sigurnosnim tehnologijama u oblaku (SASE-u). Kombinira opsežnu sigurnost, napredno umrežavanje, SD-WAN s punim značajkama, istinski *multitenancy* i sofisticiranu analitiku putem oblaka kako bi zadovoljio zahtjeve za uslugom u oblaku za mala do iznimno velikih poduzeća i pružatelja usluga. Versa pruža sigurno, skalabilno i pouzdano umrežavanje i sigurnost u cijelom poduzeću dok istovremeno povećava performanse *multi-cloud* aplikacija i dramatično smanjuje troškove.

U završnom radu napravljena je kratka komparacija u broju *hop*ova između lokacija koje su povezane direktno putem SD WAN Versa rješenja neovisno o vrsti pristupne tehnologije i udaljene lokacije koja se nalazi na MPLS *Legacyju*. Rezultati pokazuju minimalan broj *hop*ova kod lokacija direktno spojenih na Versa opremu zahvaljujući *Full Mesh* topologiji iako se broj *hop*ova povećao pri prolasku iz Versa SD-WAN MPLS-a u *Legacy* MPLS zbog prolaska kroz *Gateway* koji pretvara *routing* informacije između domena kako bi se promet mogao proslijediti. Isto tako, prikazana su variranja u odzivu prema lokacijama zbog upotrebe različitih tehnologija u pristupnoj mreži.

Višeuslužne mreže poput softverski definiranih mreža spadaju u jedan od kompleksnijih mrežnih sustava te samim time predstavljaju izazov za održavanje i upravljanje, kao što je vidljivo na primjeru Verse. Prostora za napredak i povećanje kvalitete usluge ima, iz

tog razloga, pažnju upravljanja mrežom treba usmjeriti prema tom cilju i smanjenju kompleksnosti mreže.

POPIS LITERATURE

[1] Ranjan P.: A Survey of Past Present and Future of Software Defined Networking, Hal, Tokyo, Japan, 2014.

[2] Open Network Foundation: "Software-Defined Networking: The New Norm for Networks", White Paper, 2012.

[3] What is SDN?. Preuzeto s: https://www.juniper.net/us/en/solutions/sdn/what-is-sdn/ (datum pristupanja: 01.09.2022.)

[4] Göransson P., Black C.: "Software Defined Networks - A Comprehensive Approach", Elsevier, Inc., Waltham, USA, 2014.

[5] Open Network Foundation: "SDN Architecture Overview", White Paper, ONF, Menlo Park, USA, 2014.

[6] Uppal S., Woo S., Pitt D.: "Software-Defined WAN for Dummies", John Wiley & Sons, Ltd., Chichester, West Sussex, England, 2015.

[7] Versa Networks. Preuzeto s: https://versa-networks.com/ (datum pristupanja: 4.8.2022.)

[8] Versa FlexVNF. Preuzeto s: https://www.nvc.co.jp/pdf/product/versa/Versa-FlexVNF-datasheet-final-11.5.pdf (datum pristupanja: 6.8.2022.)

[9] Versa Unveils its Vision for the SD-WAN. Preuzeto s: https://www.convergedigest.com/2015/11/versa-unveils-its-vision-for-sd-wan.html (datum pristupanja: 6.8.2022.)

[10] Versa SD-WAN – Simple, Secure and Reliable Branch to Multi-Cloud Connectivity. Preuzeto s: https://versa-networks.com/documents/solution-briefs/versa-secure-sd-wan.pdf (datum pristupanja: 6.8.2022.)

[11] N. Shah, “Do Not Underestimate the Challenge of Securing SD-WAN,” Fortinet Blog, 2019. Preuzeto s: https://www.fortinet.com/blog/business-and-technology/do-not-underestimate-thechallenge-of-securing-sd-wan.html (datum pristupanja: 6.8.2022.)

[12] BYOD Cyber Forensic Eco-System. Preuzeto s: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3713668 (datum pristupanja: 6.8.2022.)

[13] PwC's Global Crisis Survey 2019. Preuzeto s: https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html (datum pristupanja: 6.8.2022.)

[14] How to Handle Next Generation SD-WAN. Preuzeto s: https://versa-networks.com/sd-wan/tutorial.php (datum pristupanja: 6.8.2022.)

[15] MEF tackles SD-WAN interoperability with new standard**.** Preuzeto s: https://www.fiercetelecom.com/telecom/mef-tackles-sd-wan-interoperability-new-standard (datum pristupanja: 11.8.2022.)

[16] G. Lopez-Millan, R. Marin-Lopez, and F. Pereniguez-Garcia, "Towards a standard SDN-based IPsec management framework," Computer Standards & Interfaces, doi: 10.1016/j.csi.2019.103357.

[17] [17] Upravljanje protokom podataka putem MPLS-a. Preuzeto s: https://hrcak.srce.hr/file/287163 (datum pristupanja: 11.8.2022.)

[18] Versa VNFs. Preuzeto s: https://marketplace.cloud.vmware.com/services/details/versa-vnfs/?slug=true (datum pristupanja: 11.8.2022.)

[19] Headend requirements. Preuzeto s: https://bit.ly/3RQYw9F (datum pristupanja: 11.8.2022.)

[20] Općeniti prikaz arhitekture Versa rješenje SD WAN-a. Preuzeto s: https://www.convergedigest.com/2015/11/versa-unveils-its-vision-for-sd-wan.html (datum pristupanja: 10.8.2022.)

[21] Headend connectivity matrix. Preuzeto s: https://versa-networks.com/sd-wan/ (datum pristupanja: 10.8.2022.)

[22] TLS protokol CCERT-PUBDOC-2009-03-257 Preuzeto s: https://www.cert.hr/wp-content/uploads/2009/03/CCERT-PUBDOC-2009-03-257.pdf (datum pristupanja 8.9.2022)

[23] TCP protokol Preuzeto s: http://mreze.layer-x.com/s040100-0.html (datum pristupanja 8.9.2022)

[24] ATM mreža Preuzeto s: https://www.enciklopedija.hr/Natuknica.aspx?ID=4462 (datum pristupanja 8.9.2022)

[25] Frame relay Preuzeto s: https://www.ibm.com/docs/hr/i/7.1?topic=alternatives-frame-relay (datum pristupanja 8.9.2022)

[26] QoE Preuzeto s: https://www.sciencedirect.com/topics/engineering/quality-of-experience (datum pristupanja 8.9.2022)

[27] QoS Preuzeto s: https://sysportal.carnet.hr/node/505 (datum pristupanja 8.9.2022)

[28] OSPF protocol Preuzeto s: https://sysportal.carnet.hr/node/652 (datum pristupanja 8.9.2022)

[29] Point of presence (PoP) Preuzeto s: https://hr.theastrologypage.com/point-presence (datum pristupanja 8.9.2022)

[30] Virtual Cusomer Premises Equipment: a technology paradigm that promises to change the networking industry Preuzeto s: https://www.reply.com/en/topics/architecture/virtual-customer-premises-equipment (datum pristupanja 8.9.2022)

[31] Databricks Data Science & Engineering guide/Clusters Preuzeto s: https://docs.databricks.com/clusters/index.html (datum pristupanja 8.9.2022)

[32] What is SD-WAN Preuzeto s: https://www.grandmetric.com/2019/04/03/what-is-sd-wan-sdwan/ (datum pristupanja 8.9.2022)

[33] Multiprotocol BGP Preuzeto s: https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/multiprotocol-bgp.html (datum pristupanja 8.9.2022)

[34] Implementing Internet Key Exchange Security Protocol Preuzeto s: https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsbook_chapter4.html (datum pristupanja 8.9.2022)

[35] What is Traceroute: What Does it Do & How Does It Work? Preuzeto s: https://www.fortinet.com/resources/cyberglossary/traceroutes (datum pristupanja 8.9.2022)

[36] Računalne mreže: mrežne topologije Preuzeto s: https://sysportal.carnet.hr/node/379 (datum pristupanja 8.9.2022)

[37] Versa Networks Hosted and Managed Head-End Preuzeto s: https://versa-networks.com/documents/datasheets/versa-networks-hosted-and-managed-head-end.pdf (datum pristupanja 20.8.2022.)

[38] Virtual Routing and Forwarding Preuzeto s: https://www.techtarget.com/searchnetworking/definition/virtual-routing-and-forwarding-VRF (datum pristupanja 8.9.2022)

POPIS KRATICA I AKRONIMA

API (Application Programming Interface)	aplikativno programabilno sučelje
APN (Access Point Network)	mreža pristupne točke
ATM (Asynchronous Transfer Mode)	asinkroni način prijenosa
BGP (Border Gateway Protocol)	granični pristupni protocol
CPE (Customer Premises Equipment)	korisnička oprema
DC (Distribution Center)	distributivni centar
FIB (Forwarding Information Base)	protokol preusmjeravanja informacija
GUI (Graphical Unit Interface)	grafički definirano sučelje
HA (High Availability)	visoka raspoloživost
IDS (Intrusion Detection System)	sustav za otkrivanje upada
IKE (Internet Key Exchange)	internetska razmjena ključeva
IP (Internet Protocol)	internet protocol
IPS (Intrusion Prevention System)	sustav za prevenciju upada
IPsec (Internet Protocol Security)	sigurnosni internetski protocol
ISP (Internet Service Provider)	pružatelj internetskih usluga
IT (Information Technology)	informacijske tehnologije
L3 (Layer Three)	mrežni (treći) sloj
L7 (Layer Seven)	aplikativni (sedmi) sloj
LAN (Local Area Network)	lokalna mreža
LSP (Link State Packet)	paket stanja veza
MAC (Media Access Control)	kontrola pristupa mediju
MGMT (Management)	Upravljanje
MPLS (Multi-Protocol Label Switching)	višeprotokolarno prispajanje priljepnica
NFV (Network Function Virtualization)	virtualizacija mrežne funkcije
OEM (Original Equipment Manufacturer)	izvorni proizvođač opreme
OSPF (Open Shortest Path First)	„Prvo otvori najkraći put“
PoC (Proof of Concept)	provjera inovativnog koncepta
PoP (Point of Presence)	točka prisutnosti
QoE (Quality of Experience)	kvaliteta iskustva
QoS (Quality of Service)	kvaliteta usluge
RBAC (Role-Based Access Control)	kontrola pristupa putem ovlasti
RIB (Routing Information Base)	protokol usmjeravanja informacija
SDN (Software Defined Networking)	softverski definirana mreža
SD-WAN (Software Defined Wide Area Network)	softverski definirana širokopojasna mreža
SSL (Secure Sockets Layer)	sigurnosni sloj utikača
TCP (Transmission Control Protocol)	protokol kontrole transmisije
TE (Traffic Engineering)	inženjerstvo prometa
TLS (Transport layer security)	sigurnost transportnog sloja
vCPE (Virtual Customer Premises Equipment)	virtualna korisnička oprema
VM (Virtual Machine)	virtualni stroj
VNF (Virtual Networking Functions)	virtualne mrežne funkcije
VNFM (Virtual Network Function Manager)	menadžer virtualnih mrežnih funkcija

VPN (Virtual Private Network)	virtualna privatna mreža
WAN (Wide Area Network)	širokopojasna mreža
ZTP (Zero-Touch Provisioning)	automatizirano provizioniranje

POPIS SLIKA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Arhitektura i implementacija SD-WAN tehnologije na primjeru rješenja Versa, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student:

U Zagrebu, 10. rujan, 2022.

Matija Turudić