# VIRTUALNE PRIVATNE MREŽE

**Kraljević, Marko**

**Undergraduate thesis / Završni rad**

**2021**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Split / Sveučilište u Splitu**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:228:534506

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-03-28**

*Repository / Repozitorij:*

Repository of University Department of Professional Studies

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

**SVEUČILIŠTE U SPLITU**

**SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE**

Preddiplomski stručni studij Elektronika

**MARKO KRALJEVIĆ**

# Z A V R Š N I  R A D

# VIRTUALNE PRIVATNE MREŽE

Split, rujan 2021.

# SVEUČILIŠTE U SPLITU

## SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Elektronika


**Predmet:** Širokopojasne mreže

# Z A V R Š N I  R A D


**Kandidat:** Marko Kraljević


**Naslov rada:** Virtualne privatne mreže


**Mentor:** Toni Jončić

**Komentor:** Toni Jončić



Split, rujan 2021.

# Sadržaj

Sadržaj ..... i
1. UVOD ..... 2
2. OPĆENITO O VIRTUALNOJ PRIVATNOJ MREŽI ..... 3
2.1. PREDNOSTI VPN-a: ..... 4
2.2. VRSTE VPN-a ..... 5
2.3. TUNELIRANJE ..... 7
3. VPN PROTOKOLI ..... 8
3.1. IPSEC ..... 8
3.1.1. Authentification Header (AH) ..... 10
3.1.2. Encapsulated Security Payload (ESP) ..... 11
3.1.3. IKE (*Internal Key Exchange*) ..... 12
3.2. PPTP *(The Point-to-Point Tunneling Protocol*) ..... 14
3.3. L2F (*Layer 2 Forwarding*) ..... 15
3.4. L2TP (*Layer 2 Tuneling Protocol*) ..... 15
3.5. SSL protokol ..... 16
3.6. SSL i TLS protokoli ..... 17
4. VPN mreže temeljene na MPLS tehnologiji ..... 18
4.1. Osnovni elementi MPLS mreže ..... 19
4.1.1. MPLS ZAGLAVLJE ..... 19
4.1.2. USMJERIVAČI ..... 20
4.1.3. The Next Hop Label Forwarding Entry (NHLFE) ..... 21
4.1.4. Incoming Label Map (ILM) ..... 21
4.1.5. Fowarding Equivalence Class (FEC) ..... 21
4.1.6. Label Distribution Protocol (LDP) ..... 21
5. MPLS VPM ..... 23
5.1. MPLS VPN TREĆEG SLOJA (L3) ..... 24
5.2. USPOREDBA ..... 27
6. BUDUĆI RAZVOJ VPN MREŽA ..... 28
7. ZAKLJUČAK ..... 29
LITERATURA ..... 30
POPIS SLIKA ..... 32

## Sažetak

### Virtualne privatne mreže

Cilj ovoga završnog rada je objasniti što su virtualne privatne mreža (VPN )i za što se koriste. Kroz ovaj rad je opisano općenito o virtualnim privatnim mrežama, vrste virtualni mreža, te njihove prednosti. Također su opisani i objašnjeni protokoli koji se koriste u virtualnim privatnim mrežama, te VPN mreže temeljene na MPLS tehnologiji.



**Ključne riječi**: VPN, tuneliranje, IPSEC,PPTP,L2F,L2TP,SSL,TLS,MPLS, MPLS VPN



## Summary

### Virtual private networks

The aim of this final paper is to explain what virtual private networks (VPNs) are and what they are used for. Through this work is described in general about virtual private networks, types of virtual networks and their benefits.. Also described are explained and protocols that are used in virtual private networks and VPNs based on MPLS technology.



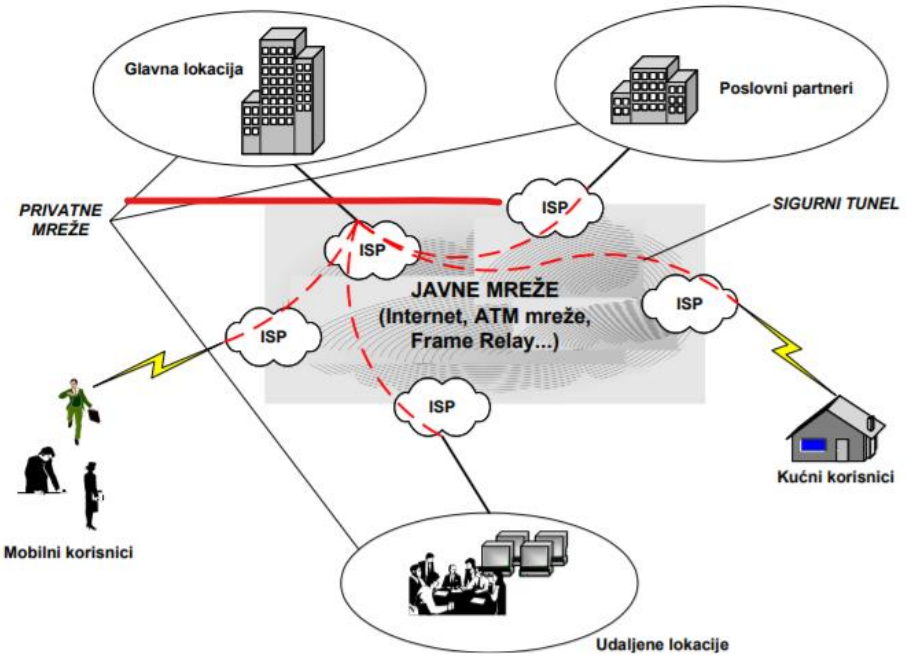
**Keywords**: VPN, tunneling, IPSEC, PPTP, L2F, L2TP, SSL, TLS, MPLS, MPLS VPN

# 1. UVOD

Što je VPN? VPN (*engl. Virtual Private Network*) je skraćeno ime od virtualne privatne mreže. To je privatna računalna mreža koja omogućuje povezivanje računala ili privatnih mreža u sigurnu javnu ili privatnu mrežu. Osigurava privatnost i sigurnost prijenosa podataka putem Interneta (javne mreže) korištenjem protokola tuneliranja i sigurnosnih procedura.

VPN -ovi u osnovi proširuju privatnu mrežu na javnu mrežu, što bi trebalo omogućiti korisniku da sigurno šalje i prima podatke putem interneta.

Za razliku od privatnih mreža koje koriste iznajmljene linije za slanje podataka, virtualna privatna mreža preko javne mreže stvara sigurni kanal između dvije krajnje tačke

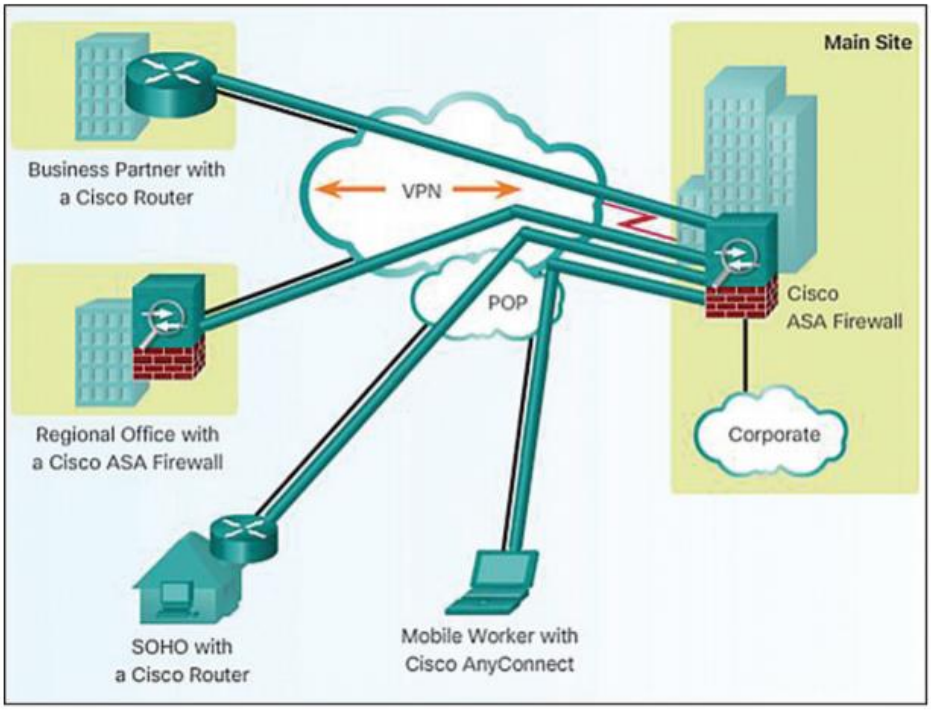



Slika 1.1 Mogućnost korištenja VPN tehnologije [1]

# 2. OPĆENITO O VIRTUALNOJ PRIVATNOJ MREŽI

VPN ili virtualna privatna mreža je mreža koja koristi javnu mrežu (obično internet) za povezivanje udaljenih web stranica ili korisnika. VPN koristi "virtualne" veze usmjerene putem Interneta od privatne mreže tvrtke ili VPN usluge treće strane do udaljenog web mjesta ili osobe [2].

VNP tehnologija omogućuje krajnjim korisnicima sigurnost od prisluškivanja i upadanja drugih korisnika pomoću tunelski protokola i šifriranje. Danas je internet pristupačniji nego ikad prije, a time je i omogućeno da se internetske usluge nastavljaju razvijati brže i pouzdanije usluge. VPN tehnologiju koriste mnoge velike i male kompanije kako bi proširili i osigurali svoju mrežu te osigurali pristup podacima preko sigurnosnog kanala do povjerljivih podataka.



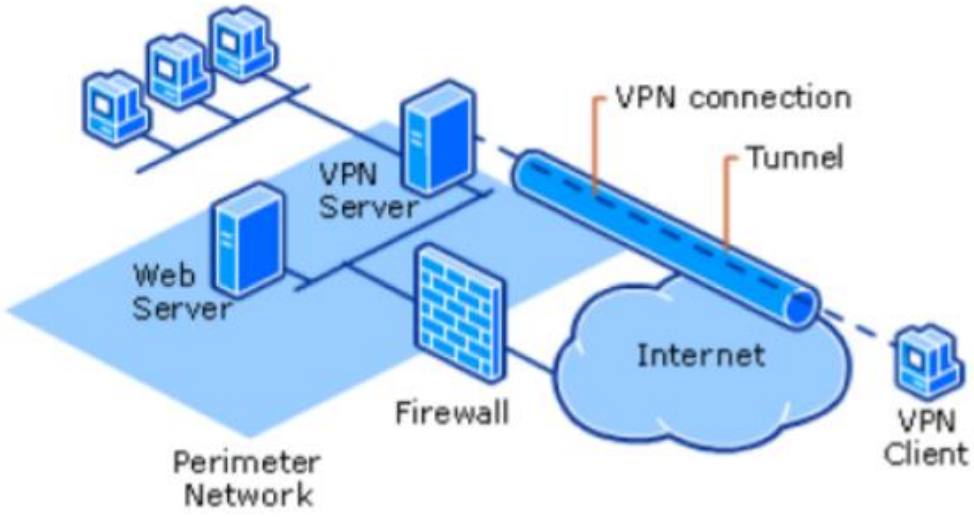

Slika 2.1 VPN tuneli putem Interneta [3]

Na slici (slika 1) možemo vidjeti kako pojedine organizacije koriste VPN usluge kako bi stvorile privatne mrežne tunele koristeći Internet usluge. Ovim tunelom omogućeno je spajanje korisnika na udaljenim lokacijama kako bi pristupili resursima tvrtke .

Osnovne sastavnice VPN-a, bez kojih komunikacija nije ostvarena a to su :

- privatna mreža
- VPN pristupnik (*engl. Gateway*)
- uređaji (vatrozid,usmjerenik,VPN koncetrator)
- Podrška za upravljanje tunelima

Ako jedna od ovih sastavnica nedostaje ne može biti moguć prijenos podataka.




Slika 2.2 Sastavnice VPN-a [4]

## 2.1. PREDNOSTI VPN-a:

Osnovna prednost korištenja VPN-a je značajna ušteda u odnosu na cijenu koštanja privatnih iznajmljenih linija. Niska cijena izgradnje mreže u odnosu na klasične privatne mreže.VPN je znatno fleksibilnija i skalabilnija mreža u odnosu na klasične privatne WAN mreže koje su bile realizirane zakupljenim vodovima.

Omogućavaju vrlo brzo i jeftino povećanje broja udaljenih ureda, međunarodnih lokacija, mobilnih korisnika u roamingu i sl.

Značajno manji troškovi i napori u održavanju vlastite mreže (veći dio poslova održavanja odvija u okviru mreže davatelja usluga)

Davatelji usluga korištenjem prometnog inženjerstva jamče korisnicima razinu usluge koja se definira u ugovoru o razini usluge SLA (*Service Lavel Agreement*).

Svako VPN rješenje mora osigurati slijedeće:

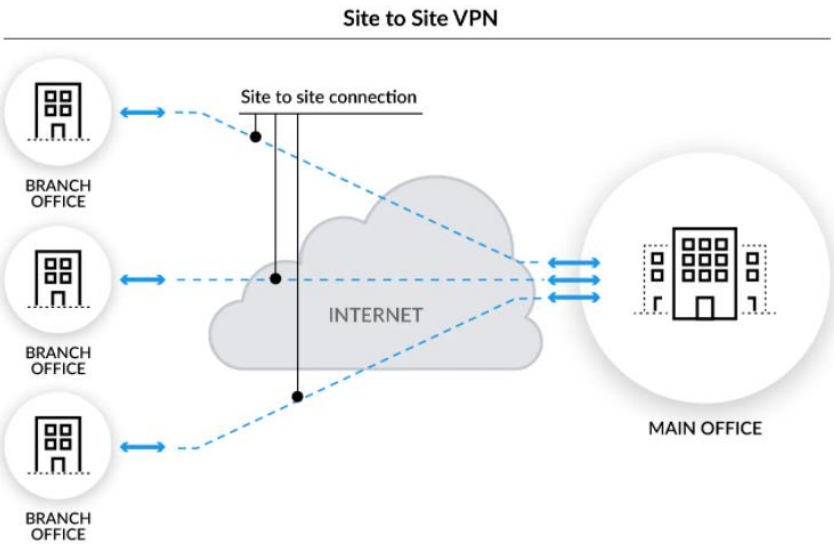
- Šifriranje-podatci koji se prenose preko javne mreže(Internet) moraju biti šifrirani da njihov sadržaj ne bi bio dostupan neovlaštenim korisnicima
- Upravljanje ključevima-VPN sadrži ključeve nužne za šifriranje podataka
- Upravljanje adresama-VPN je zadužen za prosljeđivanje adresa unutar privatne mreže
- Podrška za protokol-VPN mora podržavati protokole koji se koriste u javnim mrežama
- Identificiranje korisnika-VPN mora osigurati provjeru identiteta korisnika i ograničiti pristup samo ovlaštenim korisnicima

## 2.2. VRSTE VPN-a

### *SITE-TO-SITE VPN*

Virtualna privatna mreža "site-to-site" (VPN) je veza između dvije ili više mreža, poput korporativne mreže i mreže poslovnice. Mnoge organizacije koriste VPN-ove s web-mjesta na mjesto kako bi iskoristile internetsku vezu za privatni promet kao alternativu korištenju privatnih MPLS sklopova.

VPN-ove s web-mjesta na mjesto često koriste tvrtke s više ureda na različitim geografskim lokacijama koje trebaju stalno pristupati i koristiti korporativnu mrežu. Pomoću VPN-a web-mjesta tvrtka može sigurno povezati svoju korporativnu mrežu sa svojim udaljenim uredima kako bi komunicirala i dijelila resurse s njima kao jedinstvenom mrežom.

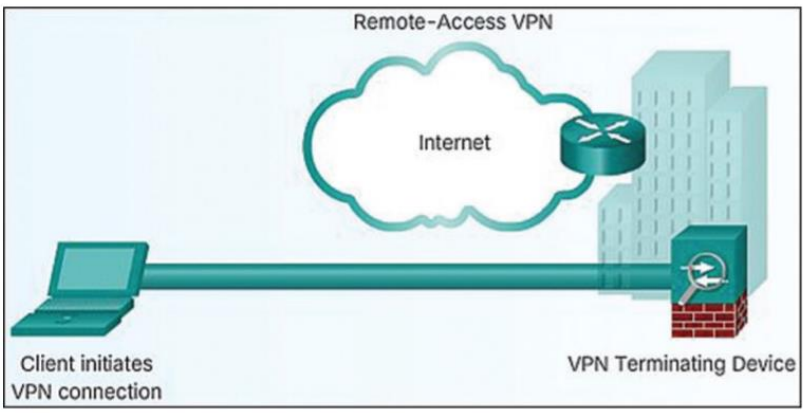



Slika 2.3. Primjer site to site VPN [5]

***REMOTE-ACCESS* VPN**

Virtualna privatna mreža s udaljenim pristupom (VPN) omogućuje korisnicima koji rade na daljinu siguran pristup i korištenje aplikacija i podataka koji se nalaze u korporacijskom podatkovnom centru i sjedištu te šifriraju sav promet koji korisnici šalju i primaju.

VPN za daljinski pristup to čini stvaranjem tunela između mreže organizacije i udaljenog korisnika koji je "gotovo privatan", iako je korisnik možda na javnoj lokaciji. To je zato što je promet šifriran, što ga čini nerazumljivim za svakog prisluškivača. Udaljeni korisnici mogu sigurno pristupiti i koristiti mrežu svoje organizacije na isti način na koji bi to učinili da su fizički u uredu. S VPN -om za daljinski pristup podaci se mogu prenositi bez potrebe organizacije da brine o tome da li će se komunikacija presresti ili ometati [6].




Slika 2.4. Remote-access VPN [7]

## 2.3. TUNELIRANJE

Većina VPN -ova oslanja se na tuneliranje za stvaranje privatne mreže koja seže preko Interneta. Tuneliranje je postupak stavljanja cijelog paketa u drugi paket prije nego što se transportira putem interneta. Taj vanjski paket štiti sadržaj od pogleda javnosti i osigurava da se paket kreće unutar virtualnog tunela.

Ta slojevitost paketa naziva se enkapsulacija. Računala ili drugi mrežni uređaji na oba kraja tunela, nazvani tunelska sučelja, mogu enkapsulirati odlazne pakete i ponovno otvoriti dolazne pakete.

Svrha protokola tuneliranja je dodati sloj sigurnosti koji štiti svaki paket na njegovom putovanju internetom. Paket putuje s istim transportnim protokolom koji bi koristio bez tunela. Protokol tuneliranja koji se koristi za enkapsulaciju dodaje sloj sigurnosti za zaštitu paketa na njegovom putovanju internetom.

Neki od protokola za tuneliranje su: PPTP, L2F, L2TP i GRE, a zbog niske razine sigurnosti često se koriste zajedno sa IPsec-om.

# 3. VPN PROTOKOLI

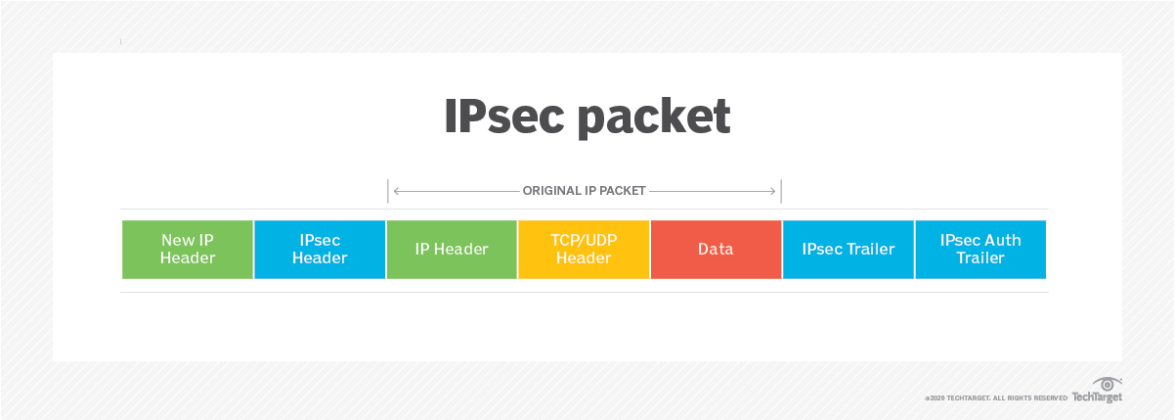
## 3.1. IPSEC

IPsec protokol (*Internet Protocol Security*) je standard i skup protokola koji obuhvaćaju mehanizme za zaštitu prometa na razini trećeg sloja OSI mrežnog modela.

IPsec se često koristi za postavljanje VPN -a, a funkcionira šifriranjem IP paketa, zajedno s autentifikacijom izvora odakle paketi dolaze. IPsec nije jedan protokol, već skup protokola a to su AH (*Authentication Header*) , ESP(*Encapsulating Security Payload* ) i IKE (*Internet Key Exchange*).

IPsec veze uključuju sljedeće korake:

Razmjena ključeva: ključevi su potrebni za šifriranje. Ključ je niz nasumičnih znakova koji se mogu koristiti za "zaključavanje" (šifriranje) i "otključavanje" (dešifriranje) poruka. IPsec postavlja ključeve s razmjenom ključeva između povezanih uređaja, tako da svaki uređaj može dešifrirati poruke drugog uređaja.




Slika 3.1. IPsec paket [8]

Zaglavlja i nadopuna (*Trailer*) paketa: Svi podaci koji se šalju putem mreže razlažu se na manje dijelove koji se zovu paketi. Paketi sadrže korisni teret ili stvarne podatke koji se šalju, te zaglavlja ili podatke o tim podacima tako da računala koja primaju pakete znaju što s njima učiniti. IPsec dodaje nekoliko zaglavlja paketima podataka koji sadrže podatke za provjeru autentičnosti i šifriranje. IPsec također dodaje nadopuna (*Trailer*), koje idu nakon korisnog opterećenja svakog paketa umjesto prije.

Autentifikacija: IPsec omogućuje provjeru autentičnosti za svaki paket, poput žiga autentičnosti na kolekcijskoj stavci. To osigurava da paketi dolaze iz pouzdanog izvora, a ne od napadača.

Šifriranje: IPsec šifrira korisni teret unutar svakog paketa i IP zaglavlja svakog paketa (osim ako se umjesto načina tunela koristi način prijevoza - vidi dolje). Time se podaci koji se šalju putem Ipsec-a čuvaju sigurnima i privatnima.

Prijenos: Šifrirani IPsec paketi putuju preko jedne ili više mreža do odredišta pomoću transportnog protokola. U ovoj se fazi IPsec promet razlikuje od običnog IP prometa po tome što najčešće koristi UDP *(User Datagram Protocol*) kao svoj transportni protokol, a ne TCP. TCP (*Transmission Control Protocol*) postavlja namjenske veze između uređaja i osigurava da stižu svi paketi. UDP, protokol korisničkog datagrama, ne postavlja te namjenske veze. IPsec koristi UDP jer to omogućuje IPsec paketima prolaz kroz vatrozide.

Dešifriranje: Na drugom kraju komunikacije paketi se dešifriraju, a aplikacije (npr. Preglednik) sada mogu koristiti isporučene podatke.

Kroz rad IPSec koristi sljedeće protokole i standarde:

- Diffie-Hellman metodu za razmjenu ključeva - glavni ključ koji se koristi za generiranje regularnih ključeva se ne prenosi istim medijem kao i ostali podaci za spajanje
- DES ili 3DES standard za šifriranje podataka - enkripcijski podatkovni standard
- HMAC - kombinirano orijentirana autentifikacija koda
- Digitalna uvjerenja izdana od strane odgovarajućeg autoriteta

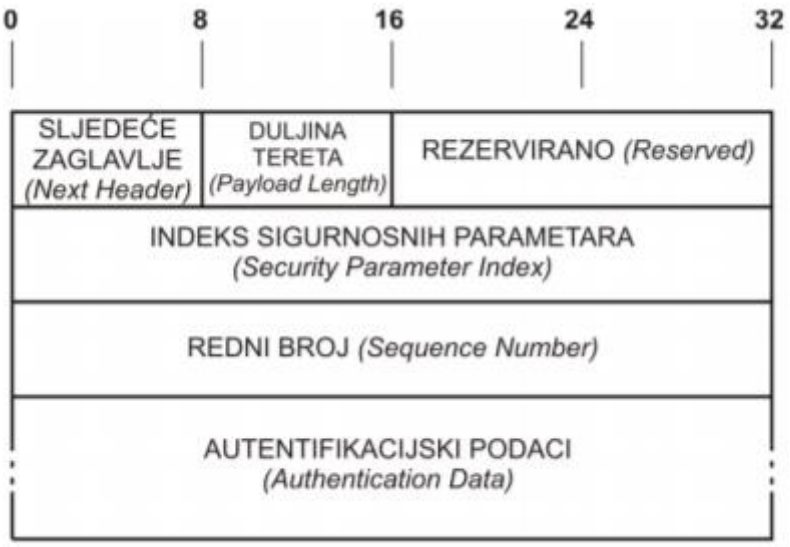
IPSec protokol podržava dva načina rada i to prijenos podataka i IPSec tuneliranje podataka. Kod prijenosnog načina rad šifrira se samo podatkovni dio IP paketa, dok zaglavlja ostaju u originalnom obliku. To znači da potencijalni napadač može vidjeti adrese od računala s kojeg paketi dolazi i na koji odlaze. Prednost ovog načina rada je to što se svakom paketu dodaje samo nekoliko okteta. Ovaj način rada namijenjen je kada se komunicira direktno između dva računala (sa vlastitom IP adresom), što znači da na taj način ne mogu komunicirati računala koja su spojena na Internet preko usmjerivača ili sličnog uređaja.

IPSec tuneliranje je poseban način tuneliranja prometa koji implementira dodatnu zaštitu na način da obje strane (klijent i poslužitelj) konfiguriraju IPSec mod kod tuneliranja prometa.

Kod prijenosa prometa koriste se dogovoreni mehanizmi za enkapsulaciju i šifriranje gdje se za razliku od metode prijenosa podataka enkriptiraju kompletni IP paketi što omogućava siguran prijenos neovisno da li se koristi javna ili privatna mreža

### 3.1.1. Authentification Header (AH)

Zaglavlje provjere autentičnosti (AH) uglavnom je protokol i koristi se za provjeru autentičnosti. Osim toga koristi se kao i za zaštitu od napada ponavljanjem slanja paketa. Protokol za provjeru autentičnosti mora se postaviti između IP zaglavlja i bilo kojeg drugog sloja sigurnosnog protokola poput TCP -a, UDP -a. U Slučaju da koristimo više zaglavlja , AH zaglavlje uvijek mora biti postavljeno iza svih zaglavlja koja se procesiraju na svakom čvoru (usmjerivaču) preko kojih paket prolazi, a ispred svih zaglavlja koja se procesiraju samo na odredišnom čvoru.




Slika 3.2 AH zaglavlje [9]

Zaglavlje za provjeru autentičnosti sastoji se od :

- Sljedeće zaglavlje (Next Header) –S maksimalnom duljinom od 8 bita ,te identificira protokol zaglavlja koje slijedi
- Duljina tereta (Payload Length) – sastoji se od 8 bite, te pokazuje ukupnu duljinu AH zaglavlja

- Indeks sigurnosnih parametara (SPI, Security Parameter Index) – 32-bitno polje čija je vrijednost proizvoljna
- Rezervirano (Reserved) –polje rezervirano za buduću uporabu,sastoji se od 16 bita
- Redni broj (Sequence Number) – 32-bitna vrijednost koja predstavlja brojač. Služi za sprečavanje napada ponovljenim slanjem paketa
- Autentifikacijski podaci (Authentication Data) – polje se sastoji od n 32-bitnih jedinica, predstavlja najvažniji dio AH zaglavlja. Ovo polje sadrži ICV vrijednost (*engl. Integrity Check Value*) vrijednost za provjeru integriteta .

### 3.1.2. Encapsulated Security Payload (ESP)

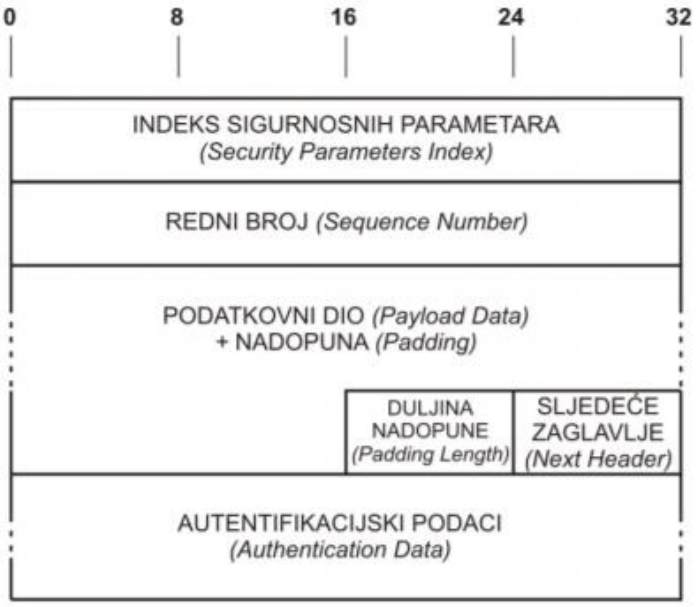
Encapsulating Security Payload (ESP) protokol osigurava povjerljivost podataka. Protokol koristi vlastito zaglavlje koje umeće iza IP zaglavlja. Svrha ESP zaglavlja (Encapsulating Security Payload) jest omogućiti mrežnim čvorovima slanje i prijem paketa čiji je podatkovni dio enkriptiran (šifriran) . Razlika između ESP i protokola AHje da ESP osigurava šifriranje.

ESP zaglavlje omogućava nekoliko različitih usluga a neke se preklapaju s uslugama AH

zaglavlja:

- Povjerljivost podatkovnog paketa (postignuta zahvaljujući enkripciji)
- Utvrđivanje autentičnosti porijekla podataka
- Zaštita od napada ponavljajućim paketima (zahvaljujući mehanizmu brojača, kao kod AH zaglavlja)
- Ograničena povjerljivost podatkovnog toka (uporabom sigurnosnih gateway-a)

Iako se može koristiti i samostalno ,uglavnom ESP zaglavlja koristimo zajedno s AH zaglavljem. ESP zaglavlje dolazi iza svih zaglavlja koja se moraju procesirati između izvora i odredišta (budući da je sav sadržaj iza ESP zaglavlja enkriptiran).



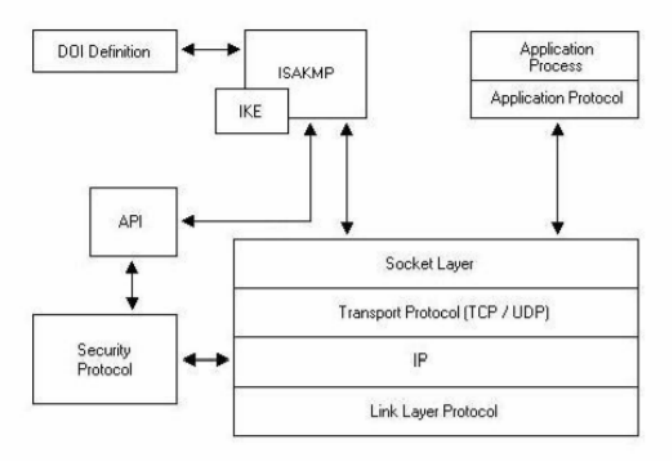

Slika 3.3 ESP zaglavlje [10]

ESP može funkcionirati na dva načina, a može biti određen pomoću metode IPSec u cilju prepoznavanja računala ili usmjerivača. U transportnom načinu, ESP zaglavlje slijedi IP zaglavlje originalnog IP datograma. Ako datogram već ima IPSec zaglavlje, tada ESP zaglavlje ide prije njega.

Transportni način ne šifrira IP zaglavlje, što može otkriti adresne informacije potencijalnom napadaču dok se datogrami prenose. Transportni način zahtijeva manje opterećenje pri obradi od tunelskog načina, ali ne omogućuje toliku sigurnost. Tunelski način kreira novo IP zaglavlje i koristi ga kao krajnje vanjsko IP zaglavlje datograma, koje slijedi ESP zaglavlje.

### 3.1.3. IKE (*Internal Key Exchange*)

IKE protokol obavlja obostranu autentifikaciju korisnika te uspostavlja SA (Security Association) vezu. Pomoću uspostave SA veze podrazumijeva izračunavanje keying materijala te dogovaranje oko skupa algoritama i parametara koji će štititi SA. Protokol radi tako da inicijator veze (eng. initiator) nudi parametre kako bi zaštitili SA. Ako ih druga strana prihvati (eng. responder) ostvaruje se SA veza.




Slika 3.4 prikaz IKE protokola [11]

U IPSec-u se mogu koristiti razni algoritmi šifriranja, ključevi različite duljine i drugo, stoga je potreban dogovor između pošiljatelja i primatelja o standardima koje će koristiti. Za to je zadužen DOI (Domain of Interpretation), čija je velika prednost to što mjere sigurnosti ne zahtijevaju promijene u određenim računalima korisnika. DOI se koristi u tuneliranju i u transportnom modu koji osigurava sigurnu vezu između dvije krajnje točke, budući da smanjuje teret IP-a, dok u sustavu tunela smanjuje cijeli IP paket kako bi se realizirala sigurna virtualna vezapošitalj i primatelj moraju dogovoriti




Slika 3.5. IPsec struktura [12]

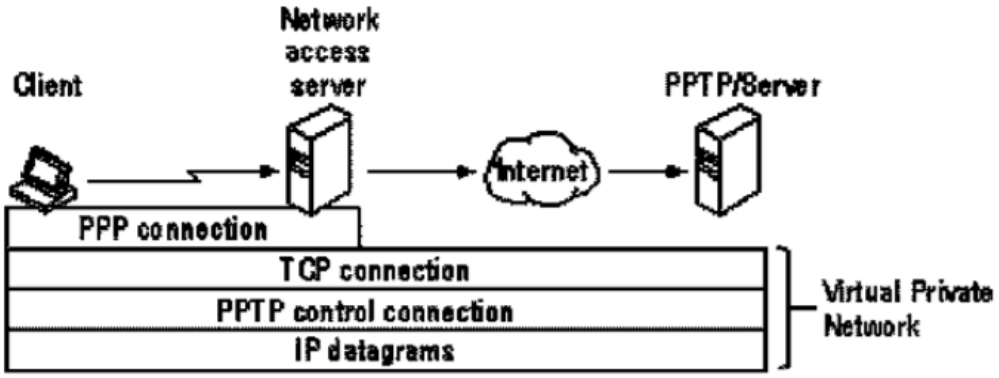
IPSec struktura sastoji se od tri glavne komponente. To su AH (*Authentication Header*) i ESP (*Encapsulated*) protokoli te upravljanje ključevima. Autentifikacijska zaglavlja se

koristi za autentifikaciju i integritet te nema mogućnosti šifriranja podataka. ESP pruža iste mogućnosti kao i AH ali ima i mogućnost šifriranja. Sigurni ključ za upravljanje koriste samo pošiljatelj i primatelj. Ukoliko su podatci autentificirani, primatelj može biti siguran da je podatak uspješno stigao te se nije promjenio.

U IPSec-u se mogu koristiti razni algoritmi pa se pošiljatelj i primatelj moju dogovoriti koje će koristiti. Za to je zadužen DOI (*Domain of Interpretation*) koji osigurava sigurnu vezu za prijenos op pošiljatelja do primatelja.

### 3.2. PPTP *(The Point-to-Point Tunneling Protocol*)

Mrežni protokol koji omogućava siguran prijenos podataka na privatnu mrežu preko javne mreže poput Interneta ili neke druge mreže koja se temelji na TCP/IP protokolu zove se PPTP protokol. TCP protokol koristi se za stvaranje i održavanje tunela unutar PPP paketa [13].




Slika 3.6. PPTP protokol [14]

PPTP također osigurava autentifikaciju te metode za šifriranje i kompresiju podataka. Autentifikacija se ostvaruje korištenjem protokola MSCHAP4 , MS-CHAPv2, a enkripcija pomoću RC-4 i MPPE algoritma. Kada PPTP poslužitelj primi paket s javne mreže, potom ga šalje do odredišnog računala privatnom mrežom. Na slici prikazan je VPN s PPTP poslužiteljem na privatnom LAN-u. Na ovaj način tuneliranje predstavlja proces slanja paketa na računalo u privatnoj mreži usmjeravajući ih preko neke druge mreže, npr. Interneta. Drugi mrežni usmjerivači ne mogu pristupiti računalu koje je u privatnoj mreži.

Tuneliranje omogućuje mreži za usmjeravanje prijenos paketa na računalo, kao što je PPTP poslužitelj, koji je povezan s mrežom usmjeravanja i privatnom mrežom. PPTP klijent i PPTP poslužitelj koriste tuneliranje za sigurno usmjeravanje paketa na računalo u privatnoj mreži korištenjem usmjerivača.koji znaju samo adresu posredničkog poslužitelja privatne mreže.

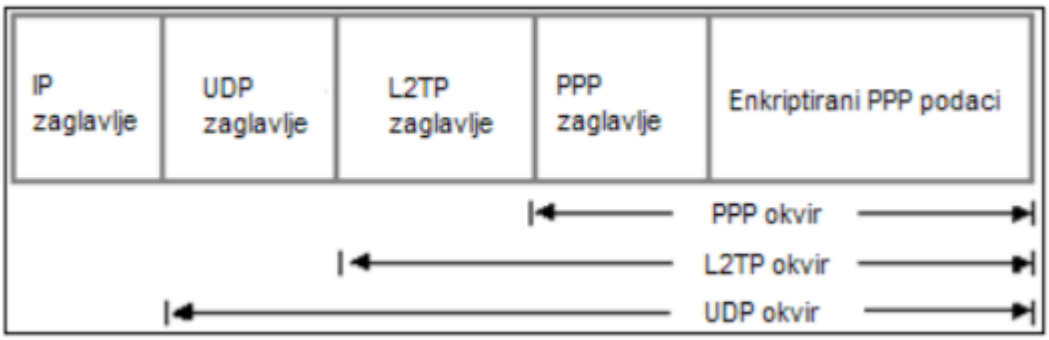
PPTP koristi 40, 56 ili 128 bitnu enkripciju, ali je čitav proces oslabljen upotrebom korisničkih zaporki za generiranje sjedničkih ključeva te je podložan napadima. Dugi ključevi generirani na potpuno slučajan način predstavljaju jedinu zaštitu od takvih napada.

### 3.3. L2F (*Layer 2 Forwarding*)

Layer 2 Forwarding (L2F) je protokol za tuneliranje razvijen od tvrtke Cisco, a sličan je PPTP protokolu. Onovna funkcija je osigurati mehanizam tuneliranja za okvire prijenosnog sloja ili protokole viših slojeva. Preko WAN spojeva se prenose enkapsulirani paketi do L2F poslužitelja,gdje se obavlja enkapsulacija i prosljeđivanje u mrežu. Cisco i Microsoft su odlučili sspojiti svoja dva protokola u jedan, pod nazivom *Layer 2 Tunneling Protocol* (L2TP), a o kojem će više biti rečeno u narednoj podcjelini .

### 3.4. L2TP (*Layer 2 Tuneling Protocol*)

L2TP radi na drugom mrežnom sloju. Razvili su ga Microsoft i CISCO kao kombinaciju PPTP i L2F protokola. L2TP je mrežni protokol koji enkapsulira PPP okvire za slanje preko IP-a, X.25, Frame Relay-a ili ATM mreža. Kada protokol koristi IP za slanje paketa, L2TP se može koristiti za tuneliranje kroz Internet. L2TP koristi UDP i nizove L2TP poruka za održavanje tunela preko IP mreža. Moguće je stvaranje više tunela između istih krajnjih točaka. L2TP koristi dvije vrste poruka kontrolne i podatkovne poruke. Kontrolne poruke se koriste prilikom uspostave i održavanja tunela. Definiraju pouzdani kontrolni kanal unutar L2TP koji garantira dostavu. Podatkovne poruke koristimo za enkapsulaciju PPP okvira koji se prenose tunelom. Ukoliko dođe do gubljena paketa podatkovne poruke se ponovo šalju.




Slika 3.7 Prijenos podataka pomoću L2TP protokola [15]

Prijenos podataka ostvaren je na način da se osnovnom paketu dodaje L2TP zaglavlje te se na njega dodaje UDP zaglavlje. Paket se enkapsulira dodavanjem IP zaglavlja koje sadrži IP adrese klijenta i poslužitelja.

### 3.5. SSL protokol

Transportni protokol koji je razvijen kako bi se omogućila sigurna i zaštićena komunikacija sugovornika preko javne mreže naziva se SSL protokol. Njegova prednosti je ta što nije potrebna instalacija posebnih programa za spajanje na poslužitelj već se komunikacija odvija preko web preglednika na način da je pogodan za povremene korisnike ( udaljeni djelatnici, poslovni partneri, itd.). Ovo je najšire korišteni kriptografski protokol kojeg je 1999. naslijedio TLS. Osnova protokola je ostala ista. Osigurava privatnost podataka i njihovu cjelovitost. Enkripcija se provodi pomoću algoritama simetričnog ključa pri čemu obje strane moraju posjedovati isti tajni ključ. To onemogućuje interpretaciju podataka trećim stranama koje nemaju ključ, čak niti u slučajevima kada oni te podatke mogu čitati. TLS se sastoji od dva sloja - sloja rukovanja i sloja zapisa. Sloj rukovanja je zadužen za međusobnu autentikaciju servera i klijenta, te dogovor o ključu i enkripciji koja će biti korištena. Ta interakcija se odvija prije izmjene bilo kakvih podataka . Sloj zapisa se bavi sigurnošću podataka koristeći poznate podatke iz sloja rukovanja. On enkriptira i dekriptira podatke, osigurava cjelovitost (integritet) podataka, te ih štiti od neovlaštenog čitanja. Danas ovi protokoli, a pretežito TLS, imaju široku primjenu u području sigurnog prijenosa podataka, sigurnom pristupu web stranicama i sl. Tako je protokol HTTPS, koji je poznatiji kao sigurna verzija HTTP protokola, zapravo kombinacija protokola HTTP i SSL/TLS. Za uspostavu zaštićenog prijenosa podataka ovaj protokol zahtijeva minimalno identifikaciju poslužitelja.

Nakon što je identifikacija obavljena, klijent i poslužitelj mogu krenuti sa razmjenom kriptiranih poruka štiteći tako podatke od prisluškivanja i neovlaštenih izmjena. Za svoj rad SSL koristi dva protokola. Jedan je SSL *handshake* koji omogućuje klijentu i poslužitelju međusobnu identifikaciju. Identitet strana koje sudjeluju u komunikaciji osigurava se primjenom digitalnog potpisa i javnih ključeva. Koriste se algoritmi RSA i DSS. Kada SSL klijent i SSL poslužitelj prvi puta započnu komunikaciju, dogovaraju se o inačici protokola, algoritmu za kompresiju i odabiru algoritama za simetrično kriptiranje nakon čega mogu započeti s razmjenom podataka. Još jedna prednost korištenja SSL algoritma leži u činjenici kako je veza pouzdana jer se provjerava integritet datoteka ili poruke prilikom prijenosa između pošiljatelja i primatelja. U tu se svrhu koriste algoritmi SHA i MD5 . Drugi protokol je SSL Record, a zadužen je za kriptiranje i prijenos poruka. Radi na principu da primanja podataka od aplikacijskog sloja u blokovima proizvoljnih duljina. Same podatke ne interpretira, već ih fragmentira u blokove fiksne dužine (veličine 214 bajtova ili manje), koje zaštiti i šalje sugovorniku, gdje se odvija obrnuti proces. Na taj način više klijentskih poruka može biti spojeno u jedan fragment ili jedna poruka podijeljena u više fragmenata. Isti se podaci zatim komprimiraju i zaštićuju korištenjem algoritama za simetrično kriptiranje – DES i RC4. Tako se, u odnosu na asimetrične ključeve, postiže veća brzina rada, iako ona nije toliko bitna kada se poslužuje jedan korisnički zahtjev, međutim, ukoliko se radi o velikom broju zahtjeva koji se poslužuju paralelno, bolje je koristiti simetrični sustav .

### 3.6. SSL i TLS protokoli

Ova dva protokola funkcioniraju zajedno kao jedan protokol, a oba se upotrebljavaju za postavljanje VPN veze. Kod ove VPN veze mrežni preglednik igra ulogu klijenta, a korisnički pristup je ograničen isključivo na određen aplikacije umjesto cijele mreže. SSL i TLS protokol se koristi najviše za stranice s e-trgovinama i pružatelje usluga. SSL i TSL VPN pruža vam sigurnu sesiju od mrežnog preglednika na vašem PC-u pa do aplikacijskog poslužitelja. To je zato što se preglednici s lakoćom prebacuju na SSL i za to ne zahtijevaju praktički nikakve postupke od strane korisnika. Mrežni preglednici dolaze integrirani sa SSL-om i TSL-om. SSL veze na početku URL adrese uvijek imaju “https” umjesto uobičajenog “http” [16].

# 4. VPN mreže temeljene na MPLS tehnologiji

MPLS (*Multi-Protocol Label Switching*) je protokol koji se koristi za prijenosi usmjeravanje podataka na temelju kratkih labela umjesto dugih mrežnih adresa. Labele su zapravo kratke identifikacijske oznake paketa. Labele predstavljaju virtualni put između izvora i odredišta, odnosno rutu kojom se paket treba kretati. MPLS protokol se nalazi između podatkovnog i mrežnog sloja u OSI modelu. MPLS se može koristiti za prijenos bilo koje vrste podataka. MPLS svojom tehnologijom može nadopuniti nedostatke koje je pojavljuju kod tradicionalnog prijenosa podataka. Korištenjem labela podatci se prenose brže nego kod tradicionalnog prijenose jer MPLS usmjerivači analiziraju zaglavlje paketa jedom dok se kod tradicionalnog provodi na svakom koraku. MPLS omogućuje osiguranje kvalitete usluga prema krajnjim korisnicima uz maksimalno iskorištavanje mrežni resursa.

Sredinom 90-tih godina kao kombinacija IP i ATM tehnologije došlo je do razvoja MPLS mreže. IP i ATM tehnologije koristile su OSPF protokol kojim su dodjeljivali pakete u mreži u kojoj se nalaze ATM komutatori odgovorni za daljnje usmjeravanje paketa.

Ciljevi MPLS mreže bili su:

- povećanje efikasnosti uz smanjenje cijene
- spajanje videa, govora i aplikacija preko jedne IP mreže
- virtualne privatne mreže
- mogućnost primjene IP mreža u smislu zadovoljavanja sve većih zahtjeva za IP prometom

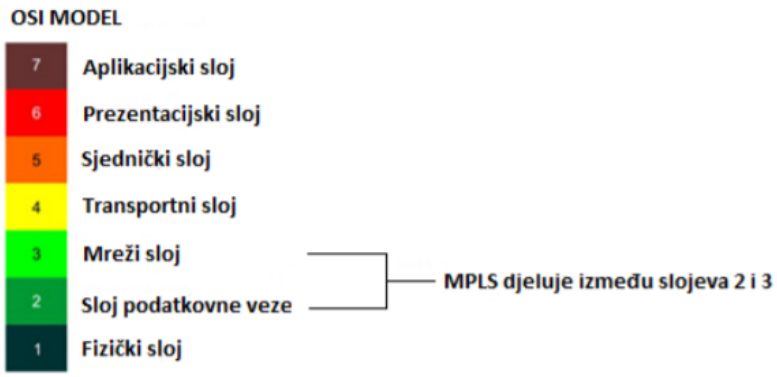
MPLS metodom žele se izbjeći svi nedostatci koji se pojavljuju kod tradicionalnog usmjeravanja. Prilikom prijenosa paketa preko labela (virtualni put) kroz mrežu, MPLS analizira zaglavlje paketa jednom za razliku od tradicionalni tehnologija. Pomoću LRS (*Label Switch Router*) usmjerivača koji obavljaju pregled i zamjenjuju oznake omogućeno je znatno brže i pouzdanije usmjeravanje. Tehnologije poput MPLS-a imaju mnogobojne prednosti u odnosu na druge opcije usmjeravanja podataka u mreži.

Neke od prednosti su:

- smanjuje se vrijeme obrade procesa i povećava učinkovitost
- sposobnost mreže da prilagodi veći broj korisnika s MPLS tehnologijom
- podrška za beskonačno slaganje labela

- sposobnost izgradnje MPLS mreže u već postojeće mreže
- tehnikom prosljeđivanja labela omogućava se brže i jednostavnije usmjeravanje

Budući da se MPLS protokol nalazi između mrežnog i podatkovnog sloja OSI modela, omogućuje prosljeđivanje paketa podatkovnom sloju i mogućnost proširivanja mrežnog sloja. Pomoću ove karakteristike MPLS predstavlja nadogradnju mrežnog i podatkovnog sloja pa je on protokol „2.5“ sloja.

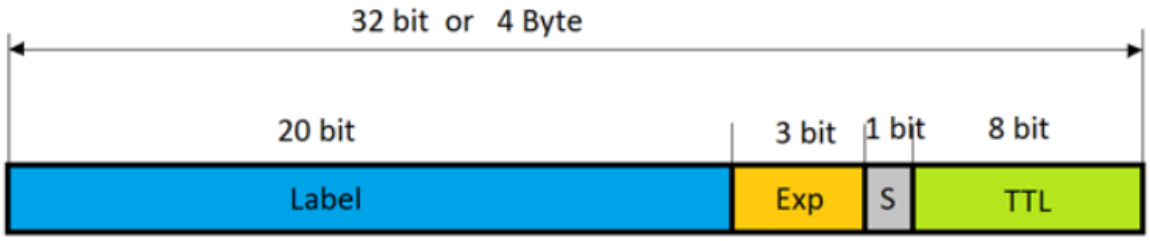



Slika 4.1. MPLS u OSI modelu [17]

## 4.1. Osnovni elementi MPLS mreže

### 4.1.1. MPLS ZAGLAVLJE

Zaglavlje se sastoji od 32 bita koje je podjeljeno na 4 različita polja. Ovo zaglavlje naziva se i umetnutim zaglavljem zbog toga što se umeće između zaglavlja podatkovnog i mrežnog sloja.




Slika 4.2. MPLS zaglavlje [18]

Dijelovi zaglavlja su:

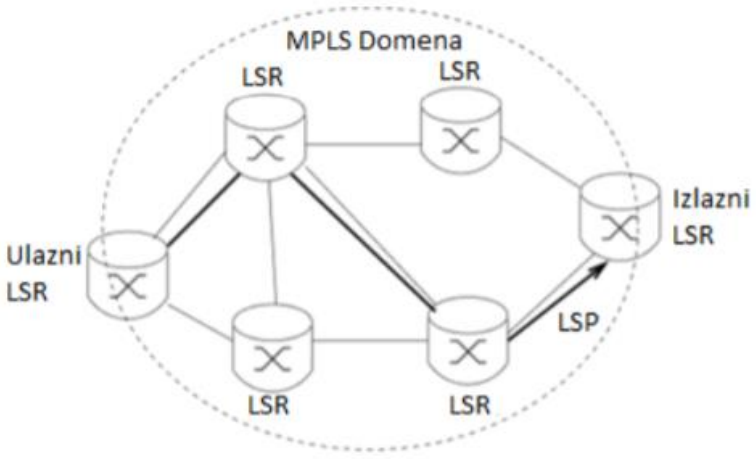
- Labela (oznaka)-polje veličine 20 bita, označava broj oznake te se njime prosljeđuju MPLS paketi
- EXP (*Experimental)*-polje veličine 3 bita koji usmjerivači koriste kako bi odlučili gdje će se u redu čekanja postaviti paket
- BoS (*Bottom of Stack*)-polje veličine 1 bit i predstavlja zadnju oznaku prije IP paketa.
- TTL (*Time To Live*)-polje koje opisuje životni vijek MPLS paketa

### 4.1.2. USMJERIVAČI

MPLS protokol koristi dvije vrste usmjerivača a to su:

LSR (*Label Switched Router*) usmjerivači i LER (*Label Edge Router*) rubni usmjerivači. LSR je usmjerivač koji spada u fizički dio mreže koji podržava tehnologiju MPLS. Kompatibilan je s MPLS-om u pogledu primanja i transmisije označenih paketa na podatkovnom sloju. LSR usmjerivači mogu brzo usmjeravati podatkovne pakete bez potrebe za provjerom tablica usmjeravanja. Postoje tri različite vrste LSR-a, diferencirane prema lokaciji i položaju na LSP putu paketa a to su:

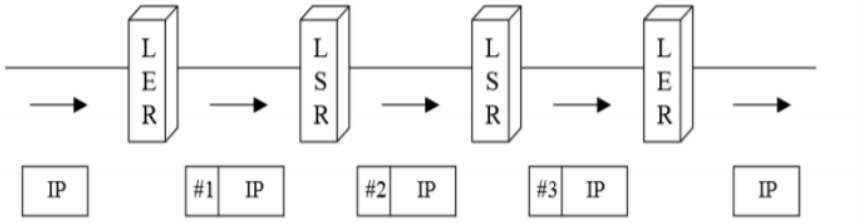
- ulazni LSR-rubi LSR prima paket i dodaje mu oznaku te ga šalje u MPLS domenu
- tranzitni LSR-nalazi se usred LSp-a,prebacuje MPLS pakete na sljedeći put u LSP-u
- izlazni LSR-LSR koji prima pakete i uklanja oznaku i isporučuje dalje




Slika 4.3 MPLS model prosljeđivanja [19]

Kod ulaznog LSR-a, oznake se stavljaju na neoznačene pakete, a kod izlaznog LSR-a te oznake se uklanja. LSP (*Label Swithed Path*) sadrži niz povezanih LSR-ova koji

predstavljaju putanju u MPLS mreži kojom putuju označeni paketi jedne veze. Prvi LSR na LSP putu je ulazni LSR, dok je posljednji LSR na LSP putu izlazni LSR. Paket na ulaznim i izlaznim usmjerivačima dobiva oznaku pri čemu može putovati LSR-ovima kroz mrežu. Na rubnom izlaznom usmjerivaču ta oznaka se ponovno skida i paket nastavlja svojim putem.




Slika 4.4 Prolazak paketa kroz LSP [20]

### 4.1.3. The Next Hop Label Forwarding Entry (NHLFE)

NHLFE se koristi pri prenošenju označenog paketa mrežom. Sadrži informacije o slijedećem skoku paketa. Svaka oznaka dolazećeg paketa može biti povezana sa određenom NHLFE. U slučaju da se prometni tok podjeli na različite puteve postoji mogućnost za više NHLFE za jednu oznaku.

### 4.1.4. Incoming Label Map (ILM)

ILM predstavlja mapu dolaznih oznaka, poznata i kao **tablica prosljeđivanja labela**. Opisuje mapiranje između labele dolazećeg paketa i skupa NHLFE. ILM se može usporediti s tablicom usmjeravanja kod konvencijalnog IP usmjernika.

### 4.1.5. Fowarding Equivalence Class (FEC)

FEC predstavlja grupu paketa koji se prosljeđuju istom putanjom. Svi paketi koji pripadaju istom FEC-u imaju iste oznake, ali svi paketi koji imaju iste oznake ne moraju pripadati istom FEC-u, jer im se EXP oznake mogu razlikovati. Usmjerivač koji odlučuje kojoj klasi pripada koji FEC je ulazni LSR koji klasificira i dodaje oznaku paketu.

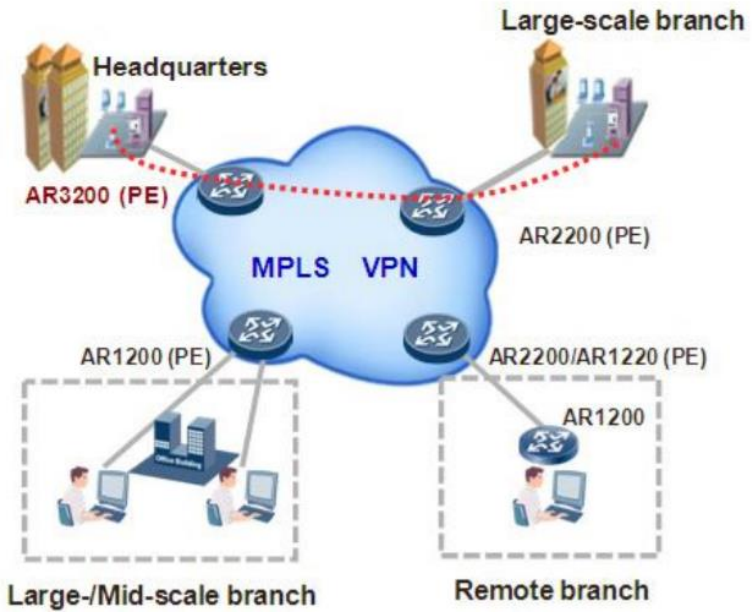
### 4.1.6. Label Distribution Protocol (LDP)

LDP koristi se u procesu postavljanja puta. LSR obavještava putem LDP-a drugi LSR o napravljenoj poveznici oznake/FEC-a. Takvi LSR-ov se nazivaju *label distribution peers* .

Povezivanje oznaka može biti napravljeno na dva načina. U prvom LSR zahtijeva od susjednog LSR povezivanje za posebni FEC, dok u drugom silazni LSR povezuje bez potražnje od susjednog LSR kao u prvom modelu. MPLS dopušta tri LDP kao što su: LDP, CR-LDP i RVSP-TE.

# 5. MPLS VPM

Jedna od najvećih sposobnosti MPLS mreže je mogućnost izgradnje virtualnih privatnih mreža (VPN-ova). MPLS VPN tehnologija omogućuje povezivanje pojedinih korisničkih usluga pomoću različitih tipova virtualni privatnih mreža. Na slici možemo vidjeti povezivanje korisnika putem virtualnih privatnih mreža koje su realizirane kroz MPLS mrežu.

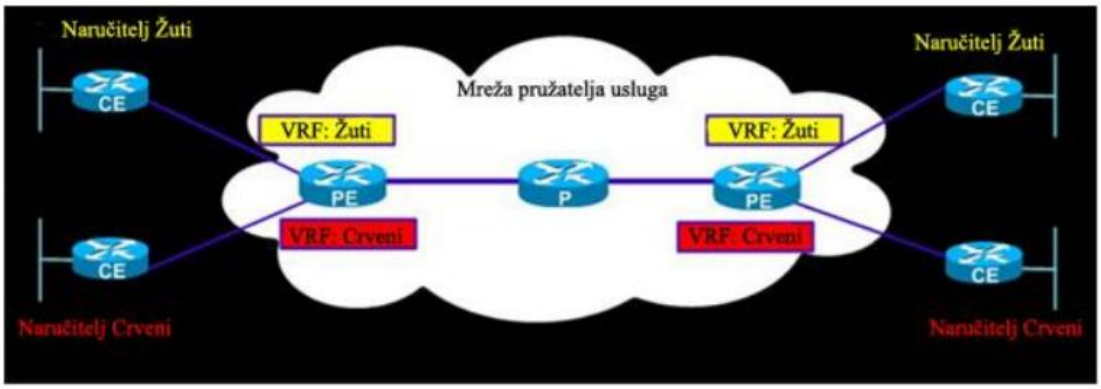



Slika 5.1MPLS VPN [21]

MPLS VPN možemo podijeliti na VPN L3 trećeg sloja (*Layer 3*) i VPN L2 drugog sloja (*Layer 2*). L3 VPN-ovi mogu biti MPLS L3VPN i *Virtual Router*, dok se L2 VPN se dijele na VPWS (*Virtual Private WireService*), VPLS (*Virtual Private LAN services*), Ethernet , PTP( *Point to Point*). MPLS VPN koristi karakteristike MPLS-a i BGP protokola. MPLS se koristi za prosljeđivanje paketa preko mreže, dok se BGP koristi za određivanje ruta preko jezgre mreže.

Informacije se prosljeđuju od CE usmjerivača do PE usmjerivača pomoću statičke rute ili BGP protokola. PE usmjerivači sadrži virtualnu tablicu umjeravanja i prosljeđivanja podataka. Svaki PE usmjerivač konfigurira poslužitelja uz primjenu vlastite tablice. Podatci zapisani u tablicama ne dijele se unutar MPLS VPN mreže.

Na slici je prikazana mreža u kojoj su virtualne tablice jedinstvene za svaki VPN povezan sa PE usmjerivačem.




Slika 5.2Mrežni dijagram MPLS VPN [22]

MPLS VPN usluge koriste se kao rješenje s više točaka. Kada se podaci premjeste s čvora na čvor , pregledava se zapis u tablici usmjeravanja, dodaje se oznaka za tu lokaciju i šalje se paket na sljedeći usmjerivač. Ovaj pristup smanjuje kašnjenje paketa pri prijenosu podataka između lokacija, ali i zahtjeva da sve udaljene lokacije budu povezane s MPLS mrežom. Jednostavnost implementacije i visoke performanse osnovne su prednosti MPLS VPN-a pred drugim rješenjima. Za razliku od tradicionalnih VPN-ova, koji koriste za prijenos podataka putem javnih mreža, MPLS VPN-ovi koriste izoliranu privatnu mrežu, zbog čega je potrebno šifrirati podatke koji se prosljeđuju između čvorova.

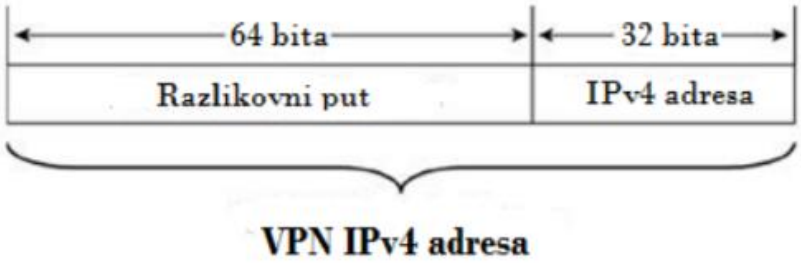
## 5.1. MPLS VPN TREĆEG SLOJA (L3)

MPLS L3 VPN karakterizira složenija konfiguracija i primjena mrežnih tehnologija i protokola, u odnosu na druge vrste MPLS VPN-ova. VPN-ovi MPLS Layer 3 koriste model ravnopravnih računala koji koristi BGP protokol za distribuciju informacija vezanih za VPN. Osim BGP protokola koristi se i tzv. MP-BGP više protokolni BGP.

MPLS L3 VPN sastoji se od sljedećih elemenata:

- Oznaka (*Label*) – oznaka duljine (32 bita) koja se dodaje svakom paketu koji ulazi u MPLS mrežu. Koriste ga MPLS mreže za promjena oznaka;
- MP-BGP – protokol kojeg koriste PE uređaji za rute korisnika na odgovarajuće PE uređaje preko MPLS jezgrine mreže.
- PE usmjerivač – rubni usmjerivač u mreži, uređaj na kojem se postavlja i uklanja oznaka;
- P usmjerivač – jezgreni usmjerivač, a nalazi se u mreži pružatelja usluge;

- CE usmjerivač – rubni usmjerivač smješten unutar korisnika ,koji je povezan s PE usmjerivačem;
- IP tablica usmjeravanja - tablica usmjeravanja koja sadrži putove pružatelja usluga koji nisu uključeni u VRF tablicu. Korisnici trebaju ovu tablicu da bi se mogli međusobno povezati, dok je VRF tablica potrebna za pristup korisničkim uređajima u nekoj VPN (virtualnoj privatnoj mreži);
- Virtualna tablica za usmjeravanje i prosljeđivanje (VRF) – razlikuje rute za različite korisnike, kao i rute korisnika od ruta pružatelja usluga na PE uređaju. VRF sastoji se od jedne ili više tablica usmjeravanja, sučelja koja koriste tablicu ,te pravila koja određuju što se događa u tablici za prosljeđivanje. Budući da je svaki primjerak konfiguriran za određenu virtualnu privatnu mrežu, svaka virtualna privatna mreža ima zasebne tablice - i pravila koja upravljaju njezinim radom
- Oznaka rute (RD) – služi za jednoznačno određivanje korisnika. Koristi se za kreiranje VPNv4 adrese veličine 96 bita. Omogućuje korisnicima da imaju iste adrese na svojim CE usmjerivačima.

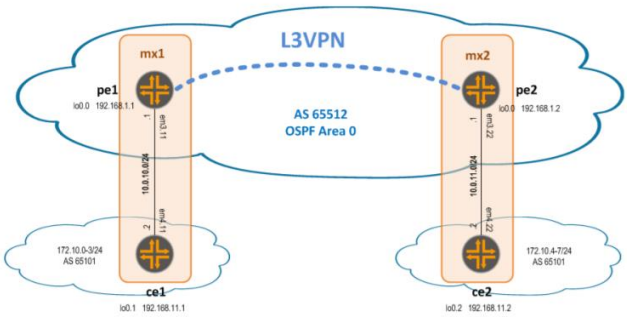



Slika 5.3 VPN IPv4

VPN-IPv4 ruta – sastoji od 96-bitne sekvence sastavljene od 64-bitne RD (*Route Distinguisher*) oznake predane 32-bitnoj IPv4 adresi. Treći sloj omogućuje povezivanje korisničkih CE usmjerivača sa mrežnim PE usmjerivačima. PE usmjerivači raspoređuju informacije o usmjeravanju svim CE usmjerivačima koji se nalaze istoj virtualnoj privatnoj mreži. Svaka virtualna privatna mreža ima vlastitu tablicu usmjeravanja koja je koordinirana s tablicama usmjeravanja CE i PE usmjerivača. CE i PE usmjerivači imaju različite VRF tablice. Svaki CE usmjerivač ima samo jednu VRF tablicu, dok se PE usmjerivač može se povezati s više CE usmjerivača. PE usmjerivač ima opću IP usmjerivačku tablicu i VRF tablicu za svaki priključeni CE usmjerivač. PE usmjerivač zna koja se VRF tablica treba koristiti za pakete koji dolaze s udaljenih virtualnih privatnih mrežnih stranica, jer svaka

VRF tablica ima jedan ili više zajedničkih atributa. Zajednički atributi prepoznaju put kao pripadnost određenoj zbirci usmjerivača.

PE usmjerivač koristi RD za ispravljanje puteva u svoje VRF tablice. Pomoću BGP protokola definiraju se pravila za usmjeravanje i način razmjene podataka. Ta pravila moraju biti ispravno konfigurirana na temelju topologije mreže. PE usmjerivač koristi IPv4 rute proslijeđene od CE usmjerivača i primljene od PE usmjerivača kao VPN-IPv4 rute. Kada ulazni PE usmjerivač prima rute izravno povezanog CE usmjerivača, ulazni PE usmjerivač provjerava primljenu rutu prema VRF pravilima za taj VPN. To jest, ulazni PE usmjerivač odlučuje koji udaljeni PE usmjerivači trebaju znati o oglašenim rutama.




Slika 5.4 L3VPN usmjerivač [21]

Na slici je prikazan jedan veliki L3VPN usmjerivač. Korisniči CE usmjerivači različito su konfigurirani u odnosu na PE usmjerivače. Dva udaljena CE usmjerivača imaju iste mrežne adrese. Takvu mrežu nazivamo virtualnom privatnom usmjerivačkom mrežom (VPRN). Svaka VPRN sastoji se od korisnički stanica koje su povezanih s PE usmjerivačima. Svaki povezani PE usmjerivač čuva posebnu tablicu za prosljeđivanje IP adresa za svaki VPRN.

## 5.2. USPOREDBA

U tablici je prikazana usporedba MPLS-a i VPN-a.

5.1. Tablica usporedbe MPLS i VPN

| **Osnova za usporedbu** | **MPLS** | **VPN** |
|---|---|---|
| Šifriranje | Nije obavezno | Zapošljava šifriranje |
| Tehnika | Više točaka | Od točke do točke i više točaka |
| Funkcije završene | Sloj 2 i sloj 3 OSI | Svi OSI slojevi |
| Trošak | Visoko | Niska |
| Konfiguracija i upravljanje | Izvršio davatelj usluga | Kupci su odgovorni za konfiguriranje i omogućavanje postavljanja VPN-a. |
| Podjelu prometa i usmjeravanja kontrolira | Davatelj usluga | Kupac |
| Pouzdanost | Pouzdaniji zbog QoS-a. | Pouzdan za promet osjetljiv na kašnjenje. |
| Usluge u oblaku | Dostupno u ograničenom smislu. | Dostupan je širok spektar usluga. |
| Postavljanje prometnih prioriteta | Vjerojatno | Nije moguće |

# 6. BUDUĆI RAZVOJ VPN MREŽA

VPN je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko distribuirane ili javne mrežne infrastrukture. Ona podrazumijeva korištenje određenih sigurnosnih i upravljačkih pravila unutar lokalnih mreža. VPN veze mogu se uspostaviti preko različitih komunikacijskih kanala kao što su internet, komunikacijske infrastrukture davatelja internetskih usluga i drugi. Vrlo je bitno kako virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točaka.

Osnovna zadaća tehnologije je kreiranje sigurnog komunikacijskog kanala između privatnih mreža putem javne mreže. Prilikom komunikacije, podaci iz lokalne mreže prolaze kroz gateway uređaj koji ima ulogu zaštite komunikacijskog medija. Isti postupak se primjenjuje kada podaci dolaze u lokalnu mrežu, također prolaze kroz gateway uređaj. Na taj se način štite tako odaslani podaci automatskim šifriranjem prilikom slanja podataka između dviju udaljenih privatnih mreža i enkapsuliranjem u IP pakete, te automatskim dešifriranjem paketa na drugom kraju komunikacijskog kanala.

Uspjeh virtualnih privatnih mreža u budućnosti ovisi uglavnom o razvoju tehnologije. Njihova najveća vrijednost krije se u potencijalnom smanjenju troškova poduzeća.

Uslijed razvoja i pada cijena mrežne opreme koja se koristi za potrebe Interneta, virtualne privatne mreže se posljednjih godina sve više koriste kao alternativno rješenje. Ističu se svakako i kao najjeftinija metoda. Prednosti virtualnih privatnih mreža ogledaju se u:

- fleksibilnosti mreže (moguće je u kratkom roku povezati nove adrese što nije moguće kada se koriste iznajmljene linije);
- kod VPN-a se plaćaju (samo) znatno niži troškovi za spajanje preko Interneta;
- manjem trošku za nabavu i održavanje opreme koja se koristi

Prednosti koje proizlaze iz uporabe virtualnih privatnih mreža neograničene, što je vidljivo kroz razvoj novih mrežnih usluga i dostupnost novih mrežnih tehnologija. Pogodnosti za virtualnu privatnu mrežu ne treba podcjenjivati, upravo iz razloga što uključuju brzinu, fleksibilnost, privatnosti i financijske pogodnosti.

# 7. ZAKLJUČAK

Na kraju rada možemo zaključiti da VPN osigurava siguran prijenos podataka do krajnjih korisnika. Virtualne privatne mreže funkcioniraju na način da se stvori privatni tunel kroz Internet do korisnikovog odredišta. Budući da je Internet danas pristupačniji nego prije, VPN tehnologija se sve više koristi. VPN iz dana u dan privlači mnoga velika i mala poduzeća kojima je cilj ojačati svoje umrežavanje te smanjiti troškove. U današnje vrijeme najviše se koriste MPLS VPN, IPSec VPN te SSL VPN usluge.

MPLS VPN je tehnički najbolji, ali i najskuplji način uspostave VPN mreža. Pruža nam apsolutnu sigurnost i izdvojenost korporacijskog prometa od ostalog prometa javnom mrežom. Pruža nam garantirani QoS (*Quality of service*) što je jako bitno kada to zahtijevaju osjetljive aplikacije koje neka korporacija koristi u svome radu. Skup je jer moramo na svakoj lokaciji imati skupu opremu (CE usmjerivače),te trebamo imati kvalitetne veze od svake lokacije do ulaza u MPLS mrežu (PE usmjerivač), te zbog toga što moramo sklopiti ugovor sa ISP i plaćati naknadu za održavanje VPN mreže.

IPSec VPN je jeftiniji jer ne moramo plaćati naknadu ISP-u za održavanje VPN-a.Osigurava nam apsolutnu povjerljivost i autentifikaciju, ali ne garantira QoS jer su paketi kriptirani pa transportna mreža ne vidi klasu prometa. Ukoliko imamo više lokacija može doći do velikih kašnjenja.

SSL VPN – najjeftiniji je i najjednostavniji način za uspostavu VPN komunikacije, ali i najnepraktičniji obzirom da nije dizajniran da povezuje mreže, već je prvenstveno dizajniran da povezuje pojedinačna računala sa web SSL serverom kroz kojeg se na siguran način može pristupiti pojedinim uslugama. U praksi, ovakav način pristupa korporacijskoj mreži koristiti će mobilni djelatnici ali sa ograničenim mogućnostima.

# LITERATURA


[1] »cis.hr,« 31. Kolovoz 2021.. [Mrežno]. Available: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf.

[2] wikipedia. [Mrežno]. Available: https://en.wikipedia.org/wiki/Virtual_private_network. [Pokušaj pristupa 30. Kolovoz 2021.].

[3] D. Ž. D. M. I. Ćulumović, Spajanje dviju kompanija u VPN, Zagreb, 2016.

[4] S. Posavac, »Razvitak i tehnološke značajke virtualnih privatnih mreža,« Zagreb, 2019..

[5] »Paloalto,« [Mrežno]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn. [Pokušaj pristupa 31. Kolovoz 2021.].

[6] hofstuffworks. [Mrežno]. Available: https://computer.howstuffworks.com/vpn.htm#pt2. [Pokušaj pristupa 30. Kolovoz 2021.].

[7] D. Ž. I. M. Davor Ćulumović, »SPAJANJE DVIJU KOMPANIJA U VPN,« *POLYTECHNIC & DESIGN,* 2016..

[8] »TechTarget,« [Mrežno]. Available: https://searchnetworking.techtarget.com/definition/anti-replay-protocol. [Pokušaj pristupa 31. Kolovoz 2021.].

[9] »wiki,« [Mrežno]. Available: https://security.foi.hr/wiki/index.php/VPN_pomo%C4%87u:_L2TP/IPSEC-a.html. [Pokušaj pristupa 1. Rujan 2021].

[10] »wiki,« [Mrežno]. Available: https://security.foi.hr/wiki/index.php/VPN_pomo%C4%87u:_L2TP/IPSEC-a.html. [Pokušaj pristupa 1. Rujan 2021].

[11] G. Živković, »Sustavi za praćenje i vođenje procesa,« Zagreb, 2006.

[12] D. Hofman, »SIGURNOST U VIRTUALNIM PRIVATNIM MREŽAMA,« Zagreb, 2005..

[13] netmotionsoftware. [Mrežno]. Available: https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols. [Pokušaj pristupa 31. Kolovoz 2021.].

[14] »Virtual Private Networks (VPN),« [Mrežno]. Available: http://www.umsl.edu/~siegelj/information_theory/projects/Law/pptp.html. [Pokušaj pristupa 1. Rujan 2021.].

[15] cis.hr. [Mrežno]. Available: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-11-246.pdf. [Pokušaj pristupa 2. Rujan 2021.].

[16] vpnmentor. [Mrežno]. Available: https://hr.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/#section-7. [Pokušaj pristupa 31. Kolovoz 2021.].

[17] S. Pavin, »Kako izgledaju podaci koji putuju tunelom od modemskog (PPP) korisnika može se vidjeti u donjoj tablici. Sličan izgled imaju i podaci kod PPTP tuneliranja.,« Osijek, 2018..

[18] »Wikipedia,« [Mrežno]. Available: https://sr.wikipedia.org/wiki/MPLS_(telekomunikacije). [Pokušaj pristupa 30. Kolovoz 2021.].

[19] R. Susitaival, Adaptive Traffic Engineering in MPLS and, 2004..

[20] M. R. José Ruela. [Mrežno]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.589.6130&rep=rep1&type=pdf. [Pokušaj pristupa 1. Rujan 2021].

[21] M. Vlajčić, »Simulacija MPLS VPN mreţe primjenom programske,« Zagreb, 2016..

[22] fiervall.cx. [Mrežno]. Available: https://www.firewall.cx/networking-topics/wan-technologies/821-mpls-ip-vpn-security.html. [Pokušaj pristupa 2. Rujan 2021.].

# POPIS SLIKA I TABLICA

Slika 1.1 Mogućnost korištenja VPN tehnologije [1] ..... 2
Slika 2.1 VPN tuneli putem Interneta [3] ..... 3
Slika 2.2 Sastavnice VPN-a [4] ..... 4
Slika 2.3. Primjer site to site VPN [5] ..... 6
Slika 2.4. Remote-access VPN [7] ..... 6
Slika 3.1. IPsec paket [8] ..... 8
Slika 3.2 AH zaglavlje [9] ..... 10
Slika 3.3 ESP zaglavlje [10] ..... 12
Slika 3.4 prikaz IKE protokola [11] ..... 13
Slika 3.5. IPsec struktura [12] ..... 13
Slika 3.6. PPTP protokol [14] ..... 14
Slika 3.7 Prijenos podataka pomoću L2TP protokola [15] ..... 16
Slika 4.1. MPLS u OSI modelu [17] ..... 19
Slika 4.2. MPLS zaglavlje [18] ..... 19
Slika 4.3 MPLS model prosljeđivanja [19] ..... 20
Slika 4.4 Prolazak paketa kroz LSP [20] ..... 21
Slika 5.1MPLS VPN [21] ..... 23
Slika 5.2Mrežni dijagram MPLS VPN [22] ..... 24
Slika 5.3 VPN IPv4 ..... 25
Slika 5.4 L3VPN usmjerivač [21] ..... 26

Tablica 5.1. Tablica usporedbe MPLS i VPN ..... 27