UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

UTJECAJ SIGURNOSTI NA FUNKCIONALNOST MPLS MREŽE ISP-A

ZAVRŠNI RAD

Mentor: prof. dr. Kemal Kačapor

Student: Edis Lokmić 58942/5666

Sarajevo, oktobar 2023

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se:

I Z J A V A O A U T E N T I Č N O S T I R A D A

Ja, Edis Lokmić, student drugog (II) ciklusa studija na Odsjeku Menadžment, Smjer Menadžment i informacione tehnologije, pod naslovom:

UTJECAJ SIGURNOSTI NA FUNKCIONALNOST MPLS MREŽE ISP-A

izjavljujem da sam završni rad izradio samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Svjestan sam činjenice da svaki oblik plagijarizma podliježe sankcijama u skladu sa relevantnim pravilima Univerziteta u Sarajevu i Ekonomskog fakulteta.

Ovom izjavom potvrđujem i da sam za potrebe arhiviranja predao elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, oktobar 2023 Edis Lokmić

SADRŽAJ

SAŽETAK

Sigurnost podataka je od ključne važnosti u vremenu kada napadi putem interneta postaju sve napredniji i sofisticiraniji. Međutim, za adekvatno funkcionisanje mreže od izuzetnog značaja su i brzina prenosa podataka kroz nju, te njena pouzdanost koja se osigurava ugovorima o nivou usluga i pruža koirsnicima garanciju da će njihovo poslovanje biti adekvatno održavano i kontinuirano. Uzimajući u vid brojne faktore, MPLS mreža se pokazala kao najbolji izbor kod mnogih provajdera internetskih usluga, te se na njoj baziraju brojni servisi, što zahtijeva adekvatno održavanje mreže i obezbjeđenje njene sigurnosti. Neki od najčešćih napada su DDoS napadi kojima će se u radu dodatno posvetiti pažnja i pokazati njihovo djelovanje na osnovu primjera iz prakse. Kroz rad će također biti predstavljene i ostale vrste napada, te alati za otkrivanje i prevenciju mrežnih napada, a objasniti će se i primjena VPN-a. Nestabilna mreža može dovesti do značajnih finansijskih gubitaka kako za korisnike, tako i za provajdere usluga, te se iz tog razloga sigurnost može posmatrati kao jedan od vitalnih parametara u poslovanju i korisnika i ISP-a.

Ključne riječi: Internet, sigurnost, MPLS, VPN, ISP, DDoS napadi

ABSTRACT

Data security has a crucial value in a time when attacks over the Internet are becoming more advanced and sophisticated. However, for adequate network functioning, speed of data transfer and its reliability based on SLA's are exceptionally important. Taking into account numerous factors, MPLS network appeared to the best choice for many internet service providers, which is why many services are based on it and that requires adequate network maintenance and ensuring its security. Some of the most common attacks are DDoS attacks which will be carefully explored in this thesis and their mode of action will be explained through an example from practice. Other types of attacks will also be explained through this thesis, as well as tools for attack detection and prevention and application of VPN's. Unstable network can lead to substantial financial losses for both customers and ISPs so because of that, security can be considered as one of the vital parameters in successful business for both customers and ISPs.

Keywords: Internet, Security, MPLS, VPN, DDoS attacks

1. Uvod

Zajednička karakteristika savremenih mreža, internet provajdera i velikih kompanija je stalno rastuća količina saobraćaja i raznih vrsta podataka koji se prenose mrežom. Integracijom usluga povećala se gustoća saobraćaja, a mrežom se prenose podaci koji se generišu na raznim uređajima poput računara, mobitela i sl., te zahtijevaju da odvijanje prenosa bude u realnom vremenu. Skalabilnost mreže predstavlja čest problem zato što je potrebno mrežu na ATM-u (eng. *Asynchronous Transfer Mode*) preslikati na IP (eng. *Internet protocol*) sloj. Savremene mreže koriste *overlay* model u kojem je IP nad ATM-om, a veze između rutera se ostvaruju *full mesh* topologijom, što ima direktan utjecaj na skalabilnost i indirektnu povezanost s problemima kvarova na mreži. Ove probleme je moguće riješiti metodama *traffic engineering*-a (TE), a alat kojim se oni rješavaju je MPLS (eng. *Multi-Protocol Label Switching*) čiji princip rada i rješavanja navedenih problema će se detaljnije opisati u ovom radu. Zahvaljujući *traffic engineering*-u omogućeno je mnogo efikasnije i efektnije korištenje resursa mreže. Upotrebom MPLS-a povećava se iskoristivost linkova i izbjegavaju zagušenja u mreži, što predstavlja glavnu prednost u odnosu na konvencionalne protokole u upotrebi. U radu će biti opisani osnovni protkoli mreže koji se danas primjenjuju, te njihove uloge i karakteristike u modernim mrežama. Jedan od glavnih problema od samog nastanka mreža je brzo rješavanje problema, grešaka i kvarova na mreži, što se također uspješno rješava saobraćajnim inženjeringom i omogućava neometan protok saobraćaja ili ograničava zastoje na minimalno *downtime* vrijeme. Protokoli u MPLS mreži su osnova njenog rada, ali i brzorastuće popularnosti koju je stekla, pa je zato značajno posvetiti im pažnju i objasniti njihove principe rada i ulogu u ovoj mreži. Sigurnost mreže vjerovatno je najprioritetnija tema kada se govori o MPLS-u, te je iz tog razloga posebno detaljno obrađena u ovom radu, uz konkretno pojašnjenje potencijalnih prijetnji mreži, te postupcima rješavanja kvarova na mreži koji bi ugrozili sigurnost podataka u njoj. Jedan od popularnijih dodataka mrežnoj sigurnosti su VPN-ovi, te će u radu biti detaljno pojašnjen princip rada MPLS VPN-a i sigurnosti koju on pruža. Dodatno, pažnja će se posvetiti upravljaju sigurnošću kod mrežnih provajdera, te opisati slučaj iz prakse o načinu rješavanja DDoS napada.

1.1. Obrazloženje teme završnog rada

MPLS stiče sve veću popularnost kao skup protokola za omogućavanje i upravljanje osnovama mreža. Mreže mogu biti usmjerene na podatke (eng. *Internet Service provider* - ISP), usmjerene na glas (mreže tradicionalnih telekomunikacijskih kompanija) ili neke od modernih mreža koje kombinuju glasovno i podatkovno usmjeravanje, a dodirna tačka ovih mreža je model koji koristi Internet protokol (IP) za prenos podataka. MPLS je tehnologija u razvoju koja olakšava nekoliko problema na Internetu, kao što su npr. performanse rutiranja, brzina i inženjering saobraćaja. MPLS pruža mehanizme u okosnicama Internet protokola za eksplicitno rutiranje korištenjem puteva s komutacijom oznaka (eng. *Label Switched Path* - LSP), enkapsuliranjem IP paketa u MPLS paket. (Alouneh & Abed, 2010)

MPLS prekriva IP mrežu kako bi omogućio rezervisanje resursa unaprijed i da rute budu predodređene, odnosno MPLS nadređuje okvir orijentisan na konekciju, putem IP mreže bez konekcije i pruža virtualne linkove ili tunele kroz mrežu, kako bi se povezali čvorovi koji se nalaze na rubovima mreže.

Razvoj svijeta podataka postavio je sve veće zahtijeve za nivoima usluga kakvi su uobičajeni na polju telefonije. Individualni korisnici imaju određena očekivanja od mreže, a među prioritetnim je da usluga bude omogućena u svakom trenutku, a nivo *bandwidth*-a u razumnom okviru. Poslovni korisnici očekuju iste usluge, s tim da oni također mogu imati i tokove podataka osjetljive na kašnjenja i poremećaje u radu mreže, te su sigurnost i dostupnost podataka vjerovatno i najznačajniji faktori pri odabiru ISP-a.

Virtualne privatne mreže (eng. *Virtual Private Network* - VPN) važna su karakteristika usluga koje ISP-ovi pružaju svojim korisnicima. VPN-ovi omogućavaju da se fizičke privatne mreže prošire tako da obuhvataju udaljene *web* lokacije povezujući ih putem Interneta. Korisnik u ovim okolnostima očekuje da će moći sačuvati svoje IP adrese i da će mu biti garantovana sigurnost njegovih podataka. MPLS pruža izvrsno rješenje za omogućavanje VPN mreže. MPLS VPN tehnologija se nedavno pojavila kroz svoje različite prednosti, posebno u smislu optimizacije performansi, kvaliteta usluge i sigurnosti. Međutim, kao i svaka tehnologija, MPLS je pod utjecajem skalabilnosti. (Bensalah, Kamoun & Baddi, 2019)

Evolucija svjetskog e-poslovanja podiže zahtjeve za pouzdanom komunikacijom. Za sigurnu komunikaciju, većina organizacije koristi tradicionalnu metodu iznajmljenih linija za povezivanje udaljenih korisnika ili ureda. Ali glavni problem sa privatnim iznajmljenim linijama je njihovo planiranje i implementacija koji nisu jeftini, a potrebno je i mnogo vremena za instalaciju i aktivaciju. Moderne organizacije žele koristiti takve tehnike komunikacije koji su relativno jeftine i pouzdanije. Ovi aspekti uvode alternativne sigurne i privatne komunikacijske mehanizme poput virtuelne privatne mreže. VPN koristi javnu mrežnu infrastrukturu kao što je Internet za slanje i primanje podataka, ali osigurava siguran put komunikacije za pouzdan prenos podataka između pošiljaoca i primaoca. (Jahan, Rahman & Saha, 2017)

Sigurnost se općenito sastoji od tri varijable koje su poznate kao sigurnosna trijada. Sigurnosna trijada se odnosi na povjerljivost, postojanost i dostupnost. (Simatimbe & Charles Lubobya, 2020a) Sigurnosni mehanizmi uključuju procese autentifikacije korisnika, enkripciju i dešifriranje podataka, te kreiranje tunela.

Potražnja za sigurnošću u mrežama podataka se povećava zbog velikih *cyber* napada i potencijalnih rizika povezanih s mrežama rasprostranjenim na udaljenim geografskim lokacijama. MPLS mreže se oslanjaju na okosnicu javne mreže koja je porozna i vrlo podložna napadima i stoga postoji potreba za pouzdanim sigurnosnim mehanizmima koji bi bili dio plana implementacije. (Simatimbe & Charles Lubobya, 2020b)

1.2. Predmet istraživanja

Zajednička karakteristika savremenih mreža, internet provajdera i velikih kompanija je stalno rastuća količina saobraćaja i raznih vrsta podataka koji se prenose mrežom. Integracijom usluga povećala se gustoća saobraćaja, a mrežom se prenose podaci koji se generišu na raznim uređajima poput računara, mobitela i sl., te zahtijevaju da odvijanje prenosa bude u realnom vremenu.

Prijetnje kontroli MPLS-a i signalnim protokolima dolaze uglavnom iz dvije vrste izvora - eksternih i internih. Eksterne prijetnje dolaze od spoljašnjih uljeza koji nisu sudionici protokola. Interne prijetnje dolaze od kompromitovanih učesnika protokola, kao što su uobičajeni MPLS čvorovi koji pripadaju domeni. S druge tačke gledišta, gore navedene prijetnje mogu nastati pasivnim ili aktivnim napadima na MPLS čvorove. Pasivni napadi su oni u kojima napadač ne

sudjeluje aktivno u obaranju mreže. Za izvođenje aktivnog napada, napadač mora biti u mogućnosti ubaciti proizvoljne pakete u mrežu. (Palmieri & Fiore, 2007a)

MPLS je lagana tehnologija tuneliranja koja se koristi u mnogim provajderima mrežnih usluga. (Daugherty & Metz, 2005) Mreže mogu biti usmjerene na podatke (ISP), usmjerene na glas (mreže tradicionalnih telekomunikacijskih kompanija) ili neke od modernih mreža koje kombinuju glasovno i podatkovno usmjeravanje, a dodirna tačka ovih mreža je model koji koristi Internet protokol za prenos podataka.

Sa razvojem računarske mrežne tehnologije i interneta, povećani su i zahtjevi za fleksibilnošću i efikasnošću, te sigurnošću u mreži, (Zou et al., 2010a) MPLS mreže obavljaju značajnu ulogu u pružanju modernih internetskih usluga i predstavljaju značajno olakšanje u upravljanju saobraćajem u odnosu na prethodna rješenja. Saobraćajnim inženjeringom se vrše brojne funkcije u MPLS mreži i osigurava sigurnost, skalabilnost i kvalitet usluge.

Obzirom da je mrežna oprema koja je uglavnom sačinjena od *router*-a i *switch*-eva okosnica interneta, od posebnog značaja je osiguranje njenog stabilnog rada i visoke dostupnosti. Vrste uobičajenih napada su: izviđački napad, napad uskraćivanjem usluge ili napad s ciljem neovlaštenog pristupa.

1.3. Ciljevi rada

U skladu sa predmetom i problemom istraživanja u završnom radu određeni su sljedeći ciljevi istraživanja:

1. Objasniti MPLS tehnologiju i njenu primjenu kod mrežnih operatera
2. Analizirati sigurnosne izazove s kojima se susreću korisnici MPLS opreme, postojeća rješenja i uspješnost rješavanja sigurnosnih problema.
3. Razmotriti mogućnosti, potencijalne izazove i ograničenja, te utjecaj sigurnosnih parametara pri odabiru MPLS opreme

1.4. Metodologija rada

Istraživanje i analiza podataka će biti bazirana na prikupljanja sekundarnih podataka. Sekundarni podaci će biti prikupljani na osnovu sveobuhvatnog pregleda relevantne stručne i naučne literature putem baza podataka kao što su Web of Science, Google Scholar, Science Direct i sl. Metoda analize će biti korištena u teorijskom dijelu rada, u svrhu pregleda postojećih praksi rješavanja sigurnosnih problema mrežnih operatera kod različitih vrsta napada i prijetnji. Metoda indukcije i dedukcije će biti korištena da se na osnovu rezultata dobivenih analiza dođe do općih zaključaka relevantnih za odgovarajući zaključak o predmetu rada. Rezultati će biti prezentirani korištenjem narativne metode prezentiranja rezultata kvalitativnih studija.

2. Pregled literature

2.1. MPLS tehnologija

MPLS stiče sve veću popularnost kao skup protokola za omogućavanje i upravljanje osnovama mreža. Mreže mogu biti usmjerene na podatke (ISP), usmjerene na glas (mreže tradicionalnih telekomunikacijskih kompanija) ili neke od modernih mreža koje kombinuju glasovno i podatkovno usmjeravanje, a dodirna tačka ovih mreža je model koji koristi IP za prenos podataka.

MPLS prekriva IP mrežu kako bi omogućio rezervisanje resursa unaprijed i da rute budu predodređene, odnosno MPLS nadređuje okvir orijentisan na konekciju putem IP mreže bez konekcije i pruža virtualne linkove ili tunele kroz mrežu, kako bi se povezali čvorovi koji se nalaze na rubovima mreže.

Jedan od glavnih zahtjeva u telefonskim mrežama je da mreža treba pokazivati veoma visoke nivoe pouzdanosti i dostupnosti, pa je tako vrlo značajno da se uvijek na vrijeme odgovara na pozive korisnika i da oni uvijek imaju pristup plaćenoj usluzi. Iz tog razloga se zastoji moraju svesti na minimum i moraju se osigurati rezervni resursi za preuzimanje kad zakaže bilo koja komponenta, kao što su link ili switch.

Razvoj svijeta podataka postavio je sve veće zahtijeve za nivoima usluga kakvi su uobičajeni na polju telefonije. Individualni korisnici imaju određena očekivanja od mreže, a među prioritetnim je da usluga bude omogućena u svakom trenutku, a nivo *bandwidth*-a u razumnom okviru.

Poslovni korisnici očekuju iste usluge, s tim da oni također mogu imati i tokove podataka osjetljive na kašnjenja i poremećaje u radu mreže.

Spajanjem glasovnih i podatkovnih mreža, naslijeđeni su i zahtjevi za uslugama njihovih kompozitnih funkcija, pa tako moderne integrisane mreže trebaju biti osigurane pomoću protokola, softvera i hardvera koji mogu garantovati visok nivo dostupnosti.

Vendori opreme obično tvrde da su ostvarili visoku dostupnost (*High Availability* - HA) kada njihov hardver postigne nivoe dostupnosti od najmanje 99,999% (pet devetki), što se može ostvariti pružanjem *backup* kopija hardvera i softvera. Kada primarna kopija zakaže, procesiranje se prebacuje na *backup* kopiju. Ovaj postupak se naziva *failover* i trebao bi rezultirati minimalnim poremećajima na području podataka.

Izgradnjom mreža opremom koja pruža visoku dostupnost, mrežni provajderi svojim korisnicima omogućavaju neophodne nivoe usluge. Međutim, oprema sama po sebi nije dovoljna, s obzirom da su mrežni linkovi skloni kvarovima, a također mogu otkazati i kompletni switchevi. Provajder mrežnih usluga također mora osigurati *backup* rute kroz mrežu, tako da podaci mogu putovati između korisničkih *web* lokacija čak i ukoliko postoji kvar na mreži u nekom trenutku.

2.1.1. Definicija i pregled primjene tehnologije

“MPLS je mehanizam visokih performansi u telekomunikacionim mrežama koji usmjerava i prenosi podatke iz jednog čvora mreže u sljedeći uz pomoć oznake (engl. *label*, naljepnice). MPLS olakšava stvaranje „virtualne veze“ između udaljenih čvorova. On može da enkapsulira pakete različitih mrežnih protokola, poput IP, ATM, SONET.

MPLS je visoko skalabilan mehanizam za prijenos podataka. U MPLS mreži, paketima podataka su dodeljene labele (oznake). Odluke o prosljeđivanju paketa se donose isključivo na osnovu sadržaja ove labele, bez potrebe da se ispita sam paket. Ovo omogućava pravljenje kola s jednog kraja na drugi kroz bilo koju vrstu transportnog medijuma, koristeći bilo koji protokol. Primarna prednost je da se eliminiše zavisnost od određene L2 tehnologije, kao što su ATM, Frame Relay, ili Eternet i eliminišu potrebu za višestrukim L2 mrežama da bi opslužile različite vrste saobraćaja. MPLS pripada porodici mreža sa komutacijom paketa. MPLS radi na sloju OSI modela za koji se

generalno smatra da se nalazi između tradicionalne definicije sloja 2 (engl. *Data Link Layer*) i sloja 3 (engl. *Network Layer*), pa se često naziva "sloj 2,5" protokol (engl. "*layer 2.5" protocol*)."('MPLS telekomunikacije (Wikipedia)', 2022)

MPLS je vrlo brzo postala ključna tehnologija za korištenje u jezgrenim mrežama, uključujući konvergirane glasovne i podatkovne mreže. MPLS nije zamjena za IP usmjeravanje, ali djeluje zajednički sa postojećim tehnologijama usmjeravanja koje pružaju veoma brzo prosljeđivanje podataka između LSR-ova (eng. *Label – Switched Router*), skupa sa rezervisanjem *bandwidth*-a za saobraćajne tokove sa različitim zahtjevima o kvaliteti usluge (eng. *Quality of Service* - QoS). MPLS unaprjeđuje usluge koje se mogu pružati putem IP mreža, postavljanjem opsega saobraćajnog inženjeringa, zagarantovanim kvalitetom usluge i virtualnim privatnim mrežama.

"MPLS uvodi, na jednostavan i fleksibilan način, novu paradigmu rutiranja, pruža niz pogodnosti za saobraćajni inženjering i značajno doprinosi poboljšanju ukupnog kvaliteta servisa. Ova relativno nova tehnologija je za kratko vrijeme zauzela značajno mjesto u praksi i postala dominantna u okosnici operatorskih i korporativnih mreža."(Stojanović & Aćimović-Raspopović, 2012)

MPLS koristi tehniku poznatu kao prebacivanje oznaka za prosljeđivanje podataka mrežom. Mala oznaka fiksnog formata stavlja se ispred svakog paketa podataka pri ulasku u MPLS mrežu. Na svakom skoku preko mreže, paket se usmjerava na osnovu vrijednosti ulaznog interfejsa i oznake, a potom šalje na izlazni interfejs s novom vrijednošću oznake.

Put koji podaci prate kroz mrežu definisan je izmjenom u vrijednostima oznake, jer se oznaka mijenja na svakom LSR-u. Budući da je mapiranje između oznaka konstantno na svakom LSR-u, put je određen početnom vrijednošću oznake, pa se takav put naziva LSP.

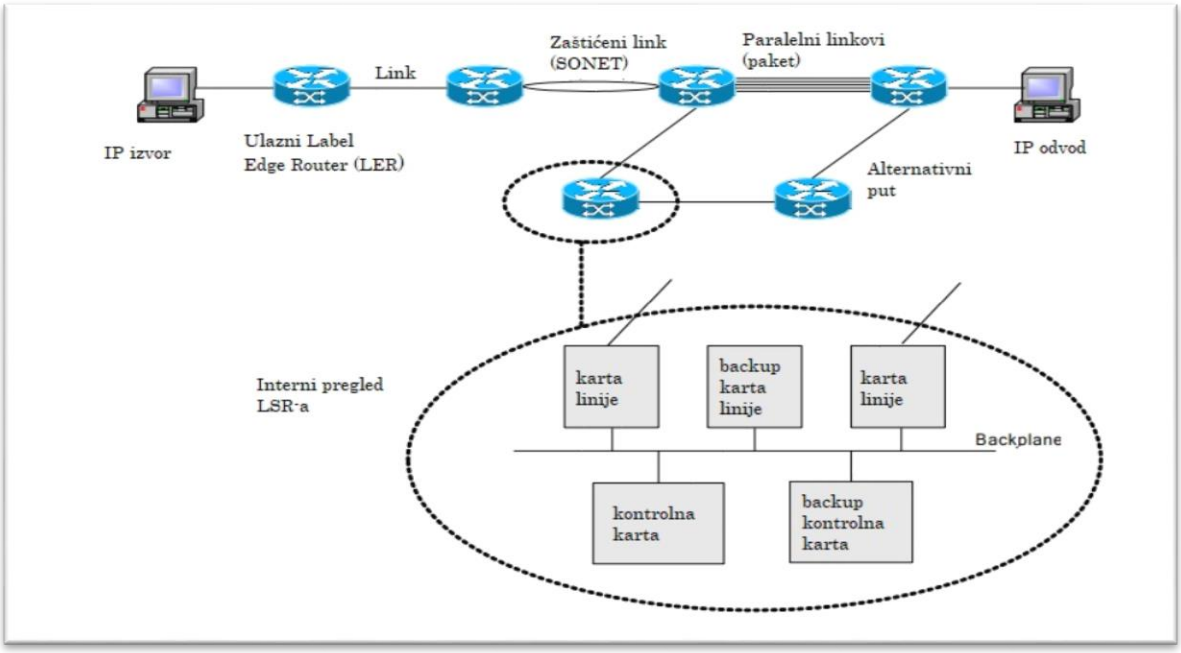
MPLS se također može primijeniti na tehnologije prebacivanja podataka koje nisu zasnovane na paketima. Put praćen podacima kroz mrežu i dalje je definisan izmjenom oznaka prebacivanja, pa se zato i dalje naziva LSP. Međutim, ove oznake bez paketa (npr. identifikatori talasne dužine ili vremenski intervali u optičkim mrežama) se koriste samo za postavljanje konekcija, poznatih kao unakrsne konekcije na LSR-ovima. Jednom kada je unakrsna konekcija uspostavljena, svi podaci se mogu usmjeriti bez pregleda, pa tako nema potrebe ni za postavljanjem vrijednosti oznake u svakom paketu. Drugačije gledano, talasna dužina ili vremenski interval su sami po sebi oznaka.

Na ulazu u MPLS mrežu, svaki paket se ispituje kako bi se utvrdilo koji LSP treba koristiti i prema tome koju oznaku mu dodijeliti. Ova odluka je lokalna stvar, ali će vjerovatno biti bazirana na osnovu faktora kao što su adresa odredišta, zahtjevi za kvalitetom usluge i trenutno stanje u mreži. Fleksibilnost je jedan od ključnih elemenata koji čine MPLS tako korisnim. Skup svih paketa koji se prosljeđuju na isti način poznat je kao FEC (eng. *Forwarding Equivalence Class*). Jedan ili više FEC-ova mogu se mapirati u jedan LSP.

2.1.2. Mrežni uređaji

Kako bi se govorilo o načinima otkrivanja, identificiranja kvarova i oporavka dijelova mreže od njih, bitno je objasniti različite komponente MPLS mreže. Nakon toga je moguće ispitati koji elementi mogu otkazati, koje greške su posljedice kvara, te kako ti kvarovi mogu biti riješeni.

Na sljedećoj slici je prikazan jednostavan primjer MPLS mreže u kojem je jedan od LSR-ova prikazan raščlanjeno, da bi se demonstrirale i njegove unutrašnje komponente.



Slika 1. Komponente MPLS mreže

Na slici su istaknuti neki od ključnih pojmova za MPLS, a njihovo objašnjenje je:

- **IP izvor** - Mjesto s kojeg se IP podaci šalju u mrežu. Obično se izvorom smatra računar, ali izvor može biti i bilo koji drugi IP uređaj kao što je npr. IP telefon. Također, izvor može da bude i *gateway* uređaj koji konvertuje između IP usluge i one koja nije zasnovana na IP-u.
- **IP Sink** – Cilj prijenosa podataka putem IP-a i ujedno partnerski uređaj IP izvora.
- **LSR** – je ključna komponenta prebacivanja u MPLS mreži. LSR je odgovoran za prosljeđivanje podataka u skladu s pravilima uspostavljenim MPLS signalnim protokolom.
- **LER** –je rubni LSR u mreži koji započinje ili završava LSP.
- **Ulazni LER** – LER koji prima IP podatke iz IP izvora, klasificira ih i ubacuje u LSP za prijenos mrežom.
- **Izlazni LER** - Partner ulaznog LER-a koji završava LSP i prosljeđuje IP podatke prema IP izvoru. Uloga uređaja može biti različita za različite LSP-ove, pa tako isti uređaj može biti LSR, ulazni LER i izlazni LER za različite LSP-ove.
- **Unakrsno povezivanje** - Pojam korišten za opis veze u hardveru između ulaznog interfejsa i oznake i izlaznog interfejsa i oznake.
- **Link** - Fizička veza između dva čvora u mreži koja može da bude električna veza ili optička vlakna.
- **Zaštićeni link** - Zaštićeni link je fizička veza s nekim ugrađenim oblikom redundancije kako prijenos podataka ne bi bio poremećen kvarom neke komponente linka. U kontrolnom panelu MPLS-a zaštićeni link se pojavljuje kao jedna tačka konekcije unutar mreže. Premda postoji mnogo šema zaštite linka, SONET je najčešće korištena šema.
- **Paralelni linkovi** - Između para čvorova u mreži može postojati više linkova. Za razliku od zaštićenih linkova, ovi pojedinačni linkovi se pojavljuju kao zasebne tačke linka unutar mreže. Njima se može upravljati kao različitim entitetima koji pružaju različite (ali paralelne) rute unutar mreže ili se njima može upravljati kao „paketom“ gdje je izbor komponentne linka dostupan samo čvorovima koji su povezani linkom.
- **Alternativni put** - je upravo to: drugačija ruta kroz mrežu za putovanje između istih tačaka do krajnjih. Paralelni linkovi pružaju najjednostavnije alternativne puteve. Komplikovaniji alternativni putevi uključuju prelazak posebnim linkovima i tranzit drugim čvorovima.

Preferirana ruta obično se izračunava koristeći algoritam Najkraći put prvo (eng. *Shortest Path First* - SPF) ili je specificirana na ulazu nakon izrade *Traffic Engineering* (TE) proračuna. Alternativne rute često mogu biti duže ili manje poželjne.

- **Kontrolna karta** - Unutrašnjosti switcheva i rutera su obično organizovane tako da je glavni procesor prisutan na kontrolnoj karti. Ova karta obično pokreće glavni softver u sistemu i odgovorna je za koordiniraciju ostalim komponenatama.
- ***Line* karta** - *Line* karte upravljaju krajevima linkova, odnosno portovima ili interfejsima. Jedna karta može imati više portova a time i opsluživati više linkova. Na jednom switchu obično ima više *line* karti. *Line* karte mogu služiti i samo u svrhu pružanja hardvera potrebnog za terminaciju linkova. *Smart line* karte također imaju i procesor koji može pokretati dio ili kompletan softver protokola koji signalizira postavljanje LSP-a na linkovima.
- **Pozadinska ploča** - Pozadinska ploča je poput LAN-a unutar switcha. Pruža povezanost između kontrolnih karti i *line* karti.
- **Backup karta** - Otpornost na greške unutar switcha se postiže postojanjem *backup* karte. One mogu biti *backup* kontrolne karte i *backup line* karte. *Backup* karta će pokrenuti sigurnosnu kopiju softvera sa primarne karte i preuzeti obradu u slučaju da dođe do greške hardvera ili softvera na primarnoj karti. Jedna *backup* karta može biti namijenjena sigurnosnom kopiranju određene primarne karte ili se može dijeliti između nekoliko primarnih karti.
- **Razdvojeni putevi** - Za dva puta kroz mrežu kaže se da su razdvojeni ako ne dijele nikakve linkove ili čvorove, osim ulaznih i izlaznih bilješki.
- **Link razdvojeni putevi** – su slični razdvojenim putevima, s tim da link razdvojeni putevi mogu dijeliti čvorove, pod uslovom da ne dijele linkove.

2.1.3. Mrežni protokoli

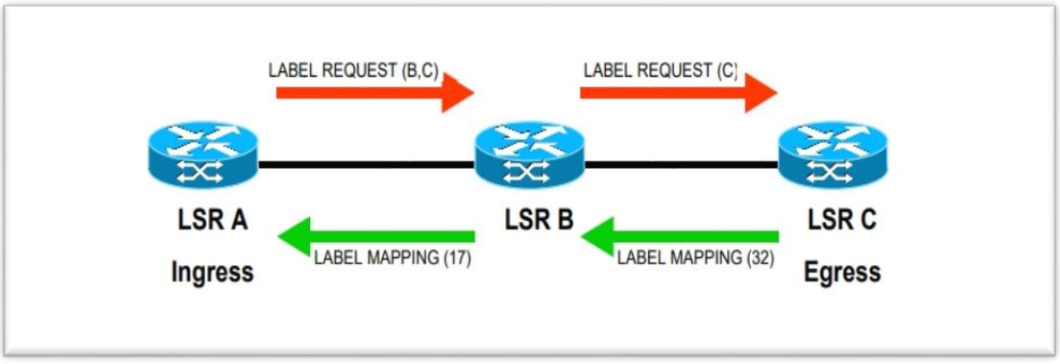
Trenutno postoje tri protokola za distribuciju oznaka koji se koriste: LDP, RSVP i BGP. Budući da su LSP-ovi postavljeni za podršku saobraćajnom inžinjeringu, svi ugovori o uslugama i VPN-ovi su konfigurisani na isti način za RSVP i CR-LDP (putem *Traffic Engineering* MIB) i oni se nazivaju *Traffic Engineering* LSP-ovi.

2.1.3.1. CR-LDP protokol

"CR-LDP (eng. *Constrained Routing Label Distribution Protocol*) je kontrolni protokol koji se koristi u nekim računarskim mrežama. Od februara 2003. godine, radna grupa IETF MPLS prestala je koristiti CR-LDP i odlučila se usredotočiti isključivo na RSVP-TE. To je ekstenzija protokola distribucije oznaka (LDP), jednog od protokola u *Multiprotocol Label Switching* arhitekturi.

CR-LDP sadrži ekstenzije za LDP kako bi proširio svoje mogućnosti poput puteva za setup izvan onoga što je dostupno protokolu usmjeravanja. Npr. LSP se može postaviti na temelju eksplicitnih ograničenja rute, ograničenja kvalitete usluge i drugih ograničenja. Rutiranje zasnovano na ograničenjima (eng. *Constraint-based Routing* - CR) je mehanizam koji se koristi za ispunjavanje zahtjeva saobraćajnog inženjeringa. Ovi zahtjevi su zadovoljeni proširenjem LDP-a za podršku usmjerenim putevima LSP-ova zasnovanih na ograničenjima (CR-LSP). Ostale upotrebe CR-LSP-a uključuju virtualne privatne mreže zasnovane na MPLS-u. CR-LDP prema strukturi paketa je gotovo isti kao i osnovni LDP, ali sadrži neke dodatne TLV-ove koji u osnovi postavljaju LSP zasnovan na ograničenjima."(Constraint-based Routing Label Distribution Protocol (Wikipedia), 2023) CR-LDP je skup ekstenzija posebno za LDP dizajniran da olakša rutiranje LSP-ova zasnovano na ograničenjima. Korištenjem TCP sesije između LSR *peers*-a šalje poruke distribucije oznaka tokom sesija. CR-LDP standardi pokušavaju omogućiti rad LDP protokola putem eksplicitnih ruta koje prenosi različite saobraćajne parametre za rezervaciju resursa kao i opcije za CR-LSP karakteristike robusnosti. (Kaur & Dinesh Kumar, 2015)

Osnovni protok za LSP setup pomoću CR-LDP-a prikazan je na slici ispod.



Slika 2. Tok postavljanja CR-LDP LSP-a

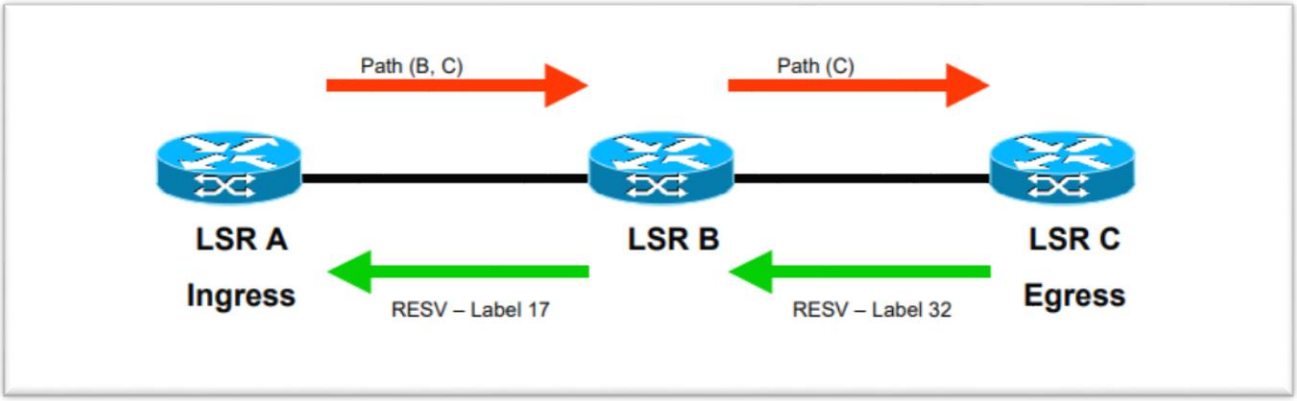
- Ulazni LSR, odnosno LSR A, utvrđuje da treba postaviti novi LSP za LSR C. Parametri saobraćaja potrebni za sesiju ili administrativne politike za mrežu omogućavaju LSR A da utvrdi da ruta za novi LSP treba ići kroz LSR B, koja možda i nije ista kao i *hop-by-hop* ruta do LSR C. LSR A gradi poruku LABEL_REQUEST s eksplicitnom rutom (B, C) i detaljima parametara saobraćaja traženim za novu rutu. LSR A rezerviše resurse potrebne za novi LSP, a zatim prosljeđuje LABEL_REQUEST na LSR B o TCP sesiji.
- LSR B prima poruku LABEL_REQUEST i utvrđuje da to nije izlaz za ovaj LSP i prosljeđuje zahtjev duž rute navedene u poruci. Zadržava resurse tražene za novi LSP, mijenja eksplicitnu rutu u LABEL_REQUEST poruci i prosljeđuje poruku na LSR C. Ako je potrebno, LSR B može smanjiti rezervaciju koju stvara za novi LSP ako su odgovarajući parametri označeni kao prilagodljivi u LABEL_REQUEST-u.
- LSR C utvrđuje da je to izlaz za ovaj novi LSP. Obavlja sve završne pregovore o resursima i vrši rezervaciju za LSP. Dodjeljuje oznaku novom LSP-u i distribuiše oznaku na LSR B u poruci LABEL_MAPPING, koja sadrži detalje o finalnim parametrima saobraćaja rezervisanim za LSP.
- LSR B prima LABEL_MAPPING i spaja ga s izvornim zahtjevom pomoću LSP ID-a sadržanog u porukama LABEL_REQUEST i LABEL_MAPPING. Završava rezervaciju, dodjeljuje oznaku za LSP, postavlja unos tablice prosljeđivanja i prosljeđuje novu oznaku na LSR A u LABEL_MAPPING poruci.
- Obrada na LSR A je slična, ali ne mora dodijeliti oznaku i proslijediti je na uzvodni LSR jer je to ulazni LSR za novi LSP.

Nakon što je CR-LSP (eng. *Constraint based Routed Label Distribution Protocol*) postavljen, njegova rezervacija *badwidth*-a će se možda morati promijeniti od strane operatera, zbog novih zahtjeva za saobraćajem koje je nosio taj CR-LSP. Karakteristika modifikacije LSP može biti podržana CR-LDP-om, upotrebom modificirane vrijednosti za zastavicu indikatora akcije u LSPID TLV (eng. *Local Service Provider ID type-length-value*). Ova funkcija ima primjenu u dinamičkom upravljanju mrežnim resursima gde se odvija saobraćaj različitih prioriteta i klasa uključenih usluga.(Kaur & Dinesh Kumar, 2015)

2.1.3.2. RSVP protokol

Za razliku od CR-LDP, RSVP-TE je najčešće korišteni signalizacijski protokol. U praksi se preferira proširivanje postojećih protokola kada god je to moguće, prvenstveno zbog napora koji je potrebno uložiti u dizajn, standardizaciju, razvoj i otklanjanje greški novih protokola. Iz tog razloga je RSVP-TE odabran kao MPLS signalizacijski protokol, a odustalo se od daljnjeg razvoja CR-LDP protokola. IETF je u okviru radnih grupa pokrenuo istraživačke aktivnosti u svrhu razvoja proširenja RSVP protokola kako bi podržao funkcionalnosti *DiffServ-aware* MPLS mreža. Protokol rezervacije resursa saobraćajnog inženjeringa (eng. *Resource Reservation Protocol – Traffic Engineering* (RSVP-TE) je odabran kao MPLS signalizacijski protokol, dok je obustavljen rad na daljnjem razvoju *Constraint based Routing Label Distribution Protocol*-a (CR-LDP). RSVP-TE predstavlja proširenje RSVP protokola koji je razvijen u okviru *Integrated Services* (*IntServ*) arhitekture"(Hodžić, n.d.)

Generički RSVP koristi razmjenu poruka za rezervisanje resursa duž mreže za IP tokove. Proširenja na RSVP-u za LSP tunele poboljšavaju generički RSVP tako da se može koristiti za distribuciju MPLS oznaka. RSVP je zasebni protokol na IP nivou. Koristi IP datagrame (ili UDP na marginama mreža) za komunikaciju između LSR *peers*-a. Ne zahtijeva održavanje TCP sesija, ali kao posljedica toga mogu se desiti gubitci kontrolnih poruka. Osnovni tok za postavljanje LSP-a pomoću RSVP-a za LSP tunele prikazan je na sljedećoj slici:



Slika 3. Tok postavljanja RSVP LSP-a

- Ulazni LSR, LSR A, utvrđuje da treba postaviti novi LSP za LSR C. Parametri saobraćaja potrebni za sesiju ili administrativne politike za mrežu omogućavaju LSR A da se utvrdi da ruta za novi LSP treba ići kroz LSR B, koja možda i nije ista kao i *hop-by-hop* ruta do LSR C. LSR A kreira poruku *Path* s eksplicitnom rutom od (B, C) i detaljima parametara saobraćaja traženim za novu rutu. LSR A onda prosljeđuje *Path* do LSR B kao IP datagram.

- LSR B prima *Path* zahtjev, utvrđuje da to nije izlaz za ovaj LSP i prosljeđuje zahtjev duž rute naznačene u zahtjevu. Mijenja eksplicitnu rutu u poruci *Path* i prosljeđuje poruku na LSR C.

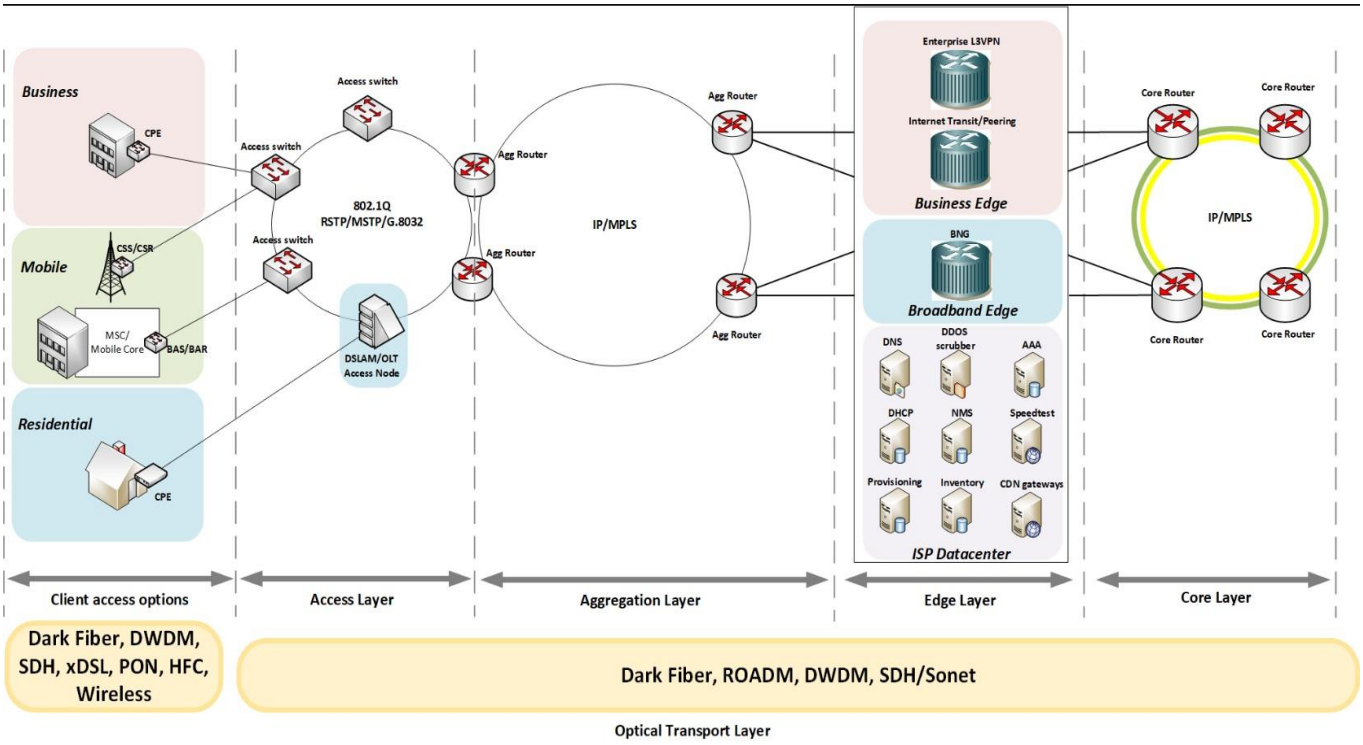
- LSR C utvrđuje da je izlaz za ovaj novi LSP, određuje iz traženih parametrira saobraćaja *bandwidth* koji treba da rezerviše i raspoređuje potrebne resurse. Potom odabire oznaku za novi LSP i distribuiše je na LSR B u *Resv* poruci, koja također sadrži i stvarne detalje rezervacije potrebne za LSP.

- LSR B prima *Resv* poruku i spaja je s izvornim zahtjevom pomoću LSP ID-a sadržanog u porukama *Path* i *Resv*. Određuje koje resurse treba rezervisati iz detalja u *Resv* poruci, dodjeljuje oznaku za LSP, postavlja tabelu prosljeđivanja, te novu oznaku prosljeđuje na LSR A u *Resv* poruci.

- Obrada na LSR A je slična, ali ne mora dodijeliti novu oznaku i proslijediti na uzvodni LSR jer je to ulazni LSR za novi LSP.

2.1.4. Arhitektura MPLS mreže za pružatelje usluga

Gotovo nijedan ISP servis ne radi bez uključivanja MPLS tehnologije, te je zbog toga i važno ubjasniti princip rada ove tehnologije kada je riječ o primjeni u ISP-ovima. Mrežna struktura ISP-a obično se sastoji od nekoliko slojeva. Najčešći slojevi koji se koriste su slojevi jezgre i agregacije koji se također pronalaze i u drugim oblastima kao što su poduzetništvo i mrežni podatkovni centri. Usluge i uređaji mogu biti različiti, ali princip agregacije linkova za brzu razmjenu podataka preko jezgre je svuda isti. Na sljedećoj slici prikazan je dijagram uobičajene strukture slojeva u jednom ISP-u, a broj slojeva može varirati u zavisnosti od veličine ISP-a i broja usluga koje pruža.



Slika 4. Uobičajena struktura slojeva u ISP-u

ISP predstavljen na gornjem dijagramu odražava ponudu modernih ISP-ova koji pružaju usluge za tri glavna tržišta:

- poslovni korisnici
- MSP mobilni backhaul
- privatni korisnici

Na tabeli ispod predstavljeni su mrežni slojevi ISP-a i njihovo pojašnjenje.

Mrežni sloj ISP-a	**Opis sloja**
Jezgreni	Brzo i pouzdano prosljeđivanje podataka. Ruteri visokih performansi instalirani u velikim POP-ovima (eng. *point of presence*). Po pravilu, topologija prstena zasnovana na dugolinijskim vezama preko optičke transportne infrastrukture. Osnovni ruteri obično pružaju nižu cijenu po portu i veću gustinu portova u zamjenu za raznolikost usluga i skaliranje. Svaki jezgreni ruter može prekinuti veze sa desetinama agregacijskih rutera. P ruter u MPLS terminologiji.
Agregacijski	Agregacija uređaja pristupnog sloja do linkova velike brzine. Velika raznolikost usluga i skaliranja. Može se instalirati na isti POP sa Core ruterom ili na manji POP. Povezan sa dva najbliža jezgrena rutera u mesh topologiji za redundantnost i balansiranje saobraćajnog opterećenja. PE ruter u MPLS terminologiji.
Rubni	Sadrži čvorove namijenjene specifičnim uslugama kao što su BNG (eng. *Broadband Network Gateway*), Mobile EPC (eng. *Evolved Packet Core*), Edge PE čvorovi za ISP DC vezu
Podatkovni centar	Aspekti kao što su potpuna vidljivost i izvještavanje o prometu, automatizacija, sigurnost, otvoreni izvor i inovacije zahtijevaju neke aplikacione servere smještene u DC-u (eng. *Data Center*). Ostale aplikacije kao što su DNS (eng. *Domain Name System*), DHCP (eng. *Dynamic Host Configuration Protocol*), AAA (eng. *Authentication, Authorization, Accounting*) moraju imati svi ISP-ovi u svom portfoliu usluga.
Pristupni	Masovno raspoređeni, jeftini pristupni uređaji. Obično u Ethernet prstenastim topologijama sa nekim protokolima za sprječavanje komutacionih petlji kao što su MSTP (eng. *Multiple Scanning Tree Protocol*) ili ERP (eng. *Ethernet Ring Protection*). OSI (eng. *The Open Systems Interconnection model*) Layer2.5 prstenovi zasnovani na MPLS-u su takođe široko rasprostranjeni. Niska raznolikost usluga, skaliranje i gustina portova za nižu cijenu.
Pristupni za korisnike	Služe za povezivanje krajnjih korisnika. Ogroman izbor tehnologija u zavisnosti od vrste usluge (Broadband, Mobile ili Business): Dark Fiber, DWDM (eng. *Dense Wavelength Division Multiplexing*), SDH (eng. *Synchronous Digital Hierarchy*), DSL (eng. *Digital subscriber line*), PON (eng. *Passive optical network*), HFC (eng. *Hybrid fiber-coaxial*), Wireless.
Optički transport	Radi na nivou 1 OSI nivoa. Gusti transport na velike udaljenosti preko postojeće infrastrukture optičkih kablova. Glavni cilj je očuvanje potrošnje vlakana što je više moguće korištenjem tehnologija optičkog multipleksiranja. Dva slučaja upotrebe: Pouzdan transport velike brzine za MPLS veze OSI Layer1 transport kao usluga. Na primjer: Ethernet privatna linija ili DCI (eng. *Data Center Interconnect*) Primjeri: Dark Fiber, DWDM, SDH, ROADM (eng. *Reconfigurable optical add-drop multiplexer*).

Tabela 1. Mrežni slojevi ISP-a

Svaki LSP ima dva servera koja se već koriste za pružanje svih usluga za pretplatnike - glavni Internet server (eng. *Master Internet Server* - MIS) i redundantni Internet server (eng. *Redundant Internet Server* - RIS).

RIS i MIS pružaju različite usluge:

- Proxy za WWW pristup
- email
- DNS
- Web hosting
- Sve ostale veze na Internet su obezbeđene preko prevođenja mrežnih adresa (eng. *Network Address Translation* - NAT).

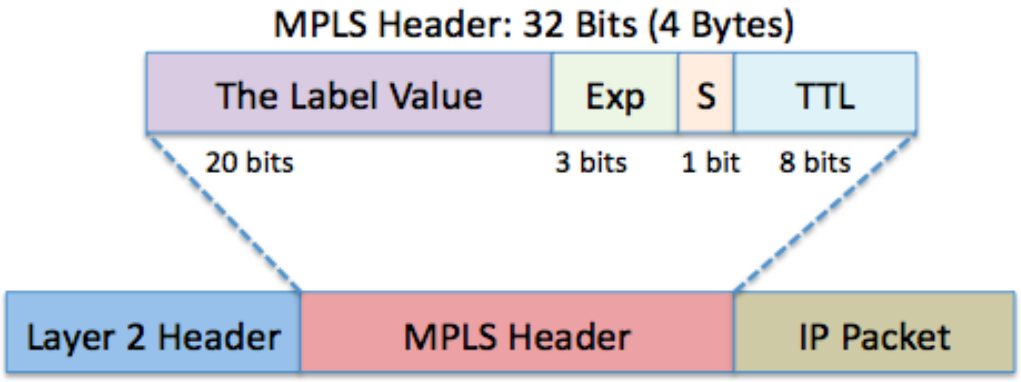
Glavni elementi MPLS mreže su:

- MPLS zaglavlje,
- LSR (eng. *Label Switched Router*),
- LSP (eng. *Label Switched Path*),
- NHLFE (eng. *The Next Hop Label Forwarding Entry*),
- ILM (eng. *Incoming Label Map*),
- FEC (eng. *Forwarding Equivalence Class*),
- LDP (eng. *Label Distribution Protocols*).

Zaglavlje MPLS ima 32 bita i umeće se iza zaglavlja podatkovnog sloja i ispred zaglavlja mrežnog sloja.

Dijelovi zaglavlja su:

- Oznaka (eng. *Label*) - polje veličine 20 bita koje opisuje putanju koju paket prolazi do odredišta,
- EXP (eng. *Experimental use*) - polje veličine 3 bita koje se koristi pri određivanju tretmana paketa,
- BoS (eng. *Bottom of Stack*) - zadnja oznaka u nizu koja se može nadovezati na drugu i veličine je jednog bita,
- TTL (eng. *Time To Live*) - polje koje opisuje životni vijek MPLS paketa.



Slika 5. MPLS zaglavlje

2.1.5. Ugovori o nivou usluge

Sigurnost podataka je od izuzetnog značaja za održavanje kontinuiteta i integriteta usluge ISP-a. Iz tog razloga postoje ugovori o nivou usluge (eng. *Service Level Agreements* – SLA) kojima se osigurava usluga koju ISP pruža svojim korisnicima i koja mora da zadovoljava određene kriterije. Mnoge upotrebe Interneta zahtijevaju pružanje određenih nivoa usluga, npr. glasovni saobraćaj zahtijeva mala kašnjenja i vrlo male varijacije kašnjenja. Video saobraćaj dodatno zahtijeva visok *bandwidth*. Korisnici sve češće traže ugovore o uslugama koji garantuju performanse i dostupnost mreže.

U prošlosti, da bi udovoljili tim zahtjevima, mrežni provajderi su morali prekomjerno osiguravati svoje fizičke mreže. MPLS nudi dobar način za izbjegavanje ovog problema dodjeljivanjem mrežnih resursa određenim tokovima, koristeći usmjeravanje LSP-a zasnovano na ograničenjima.

Najčešće kategorije SLA odnose se na kašnjenje, gubitak paketa, podrhtavanje (*jitter*) i dostupnost.

Uobičajene SLA kategorije koje se nude su:

- **Latencija -** vrijeme *ping*-a povratne veze na krugu. Naglašeni SLA za kašnjenje je obično 15% - 20% sporiji od stvarnih performansi, što omogućava pad performansi mreže mobilnog operatera bez štete. Prilikom procjene mreže, stvarna latencija se često može testirati i ugraditi u prilagođeni SLA. Neki SLA latencije se odnose na prosječno *backbone* kašnjenje za geografske regije, a ne nužno i za određene mrežne puteve.

- **Gubitak ili isporuka paketa** - ova SLA stavka je sama po sebi razumljiva. U privatnim mrežama očekivano je da gubitak paketa bude skoro nikakav. Ipak, neki operateri baziraju SLA za gubitak paketa na svojoj *backbone* mreži, a ne na *end-to-end* mreži korisnika.
- **Jitter -** SLA podrhtavanja (*jitter*) mjeri isporuku paketa u pravilnom redoslijedu. Ovo je od posebne važnosti za VoIP i video.
- **Dostupnost usluge** - Svaka mreža će imati povremenih kvarova, najčešće zbog kvara lokalne petlje. Operater treba SLA sa svojim provajderom lokalne petlje kako bi osigurao da se popravci izvršavaju brzo. Uobičajeni SLA je četiri sata za oporavak od kvara. Ali različiti operateri pokreću sat u različito vrijeme. Za upravljanu mrežu, sat bi se mogao zaustaviti kada drugi probni ping ne reaguje iz NOC-a. Neki operateri ne pokreću sat dok korisnik ne pokrene *trouble ticket*, što može biti i nekoliko sati nakon nastanka kvara, ovisno o periodu dana i globalnoj proširenosti mreže. Ova posebna mjera ima ograničenu vrijednost ako dođe do većeg broja kratkih prekida koji se ne zbrajaju u velik broj, ali ometaju poslovanje.
- **Instalacija usluge** - ovo je garancija koliko će vremena trebati za instalaciju sklopa na svakom navedenom mjestu u mreži. Mnogi operateri pripisuju nepovratnu naknadu za instalaciju koja ne zadovoljava SLA.
- **Obavijest o proaktivnom prekidu rada** – ova kategorija se nalazi samo kod nekih operatera i definiše činjenicu da će operater automatski obavijestiti korisnika o prekidu, bez potrebe da korisnik otvori *ticket*.
- **Brzi prekid rada** - mjeri brzinu prelaska s primarnog mrežnog puta do sekundarnog mrežnog puta u situaciji kvara.

2.1.6. Komparativna analiza MPLS protokola

Oba inicijalno predviđena protokola služe za distribuciju oznaka u MPLS mreži, ali se razlikuju u osnovnim karakteristikama i njihovoj svrsi.

Ključne razlike između CR-LDP i RSVP-a su pouzdanost osnovnog transportnog protokola i način vršenja rezervacije resursa, odnosno da li je ona izvršena prema naprijed ili straga. Od ovih stajališta dolaze i mnoge druge funkcionalne razlike.

"CR-LDP je formiran kako bi omogućio postavljanje LSP-a za dosljedno *end-to-end* diferenciranje usluge u MPLS mrežama. U poređenju s tim, RSVP je stvoren za podršku *soft state* rezervisanja resursa integrisanih usluga putem IP mreža. RSVP je formiran prije CR-LDP-a. CR-LDP je u smislu skalabilnosti *hard state* protokol i zbog ove karakteristike u osnovi posjeduje poboljšana svojstva skaliranja u smislu obima signalizacije saobraćaja u mreži sa povećanjem količine CR-LSP-ova. U poređenju sa RSVP-om, TCP *end-to-end* način upravljanja CR-LDP-a orjentisan na mrežu, ovisi o izlaznom i ulaznom LSR-u da upravlja LSP-om. Skalabilnost nije problem u CR-LDP-u jer je to *hard state* protokol." (Aslam & Aziz, 2008)

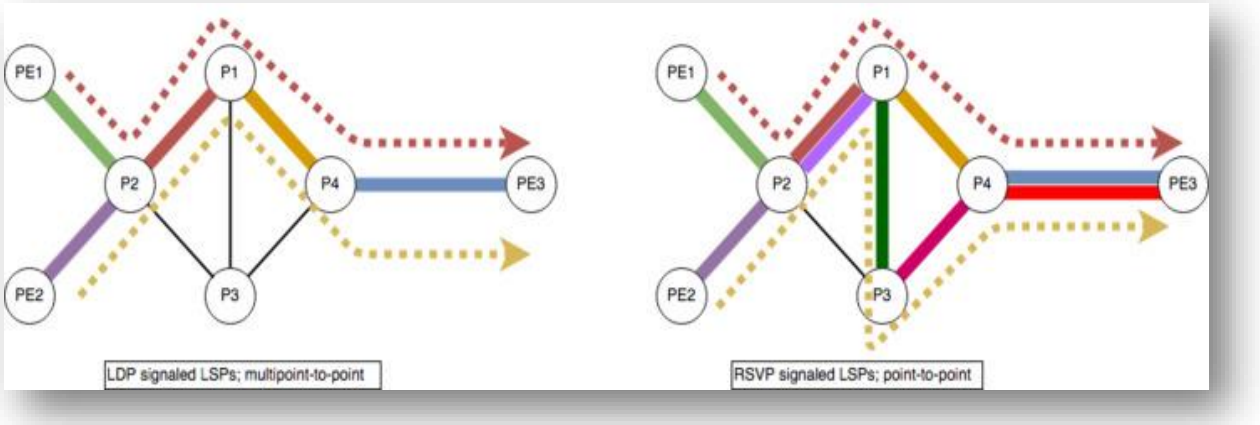
U savremenim mrežama u upotrebi su uglavnom LDP i RSVP protokoli koji su diferenciraju prema načinu rada i primjene.

Tri glavne razlike između RSVP i LDP su:

1. S LDP-om izlaz pokreće postavljanje LSP-a. Nasuprot tome, kod RSVP-a je ulaz taj koji pokreće postavljanje LSP-a.
2. S LDP-om LSP-ovi s više ulaza koriste istu oznaku da dosegnu izlaz (*multi-point-to-point* LSP). Suprotno tome, RSVP postavlja neovisne *point-to-point* LSP-ove.

LDP-om se upravlja automatski, dok RSVP zahtijeva konfiguraciju.

Slika ispod prikazuje topologije LSP-ova u LDP-u i RSVP-u.



Slika 6. Topologije LSP-ova u LDP i RSVP

2.1.7. Skalabilnost protokola

Skalabilnost protokola se razmatra u smislu mrežnih tokova koje koristi, resursa potrebnih za održavanje stanja protokola na svakom čvoru i opterećenja procesora na svakom čvoru. Sve navedeno je potrebno razmotriti u kontekstu načina korištenja MPLS-a u mreži. Ako se glavni LSP-ovi trebaju koristiti kroz mrežu za povezivanje ključnih rubnih tačaka, bit će manja potražnja na skalabilnošću pri korištenju jednog LSP-a po protoku ili postavljanju LSP-ova baziranih na topologiji usmjeravanja. Sposobnost spajanja LSP-ova također ima utjecaj na zahtjeve skalabilnosti, jer tokovi podataka mogu imati mogućnost dijeljenja dodjele resursa, a broj oznaka potrebnih u mreži je smanjen.

"Da bi se pružile operaterske usluge širokog opsega, signalni protokol trebao bi podržavati ogroman broj sesije, LSP-ova i LSR-ova i trebao bi pružiti željeni nivo performansi. Svaki signalni protokol zahtijeva više ili manje računarstva i opseg memorije LSR-a i *bandwidth* linka kako bi se njegove operacije izvodile."(Muhammad et al., 2014)

2.1.8. Rješavanje problema pri greškama LSP-ova

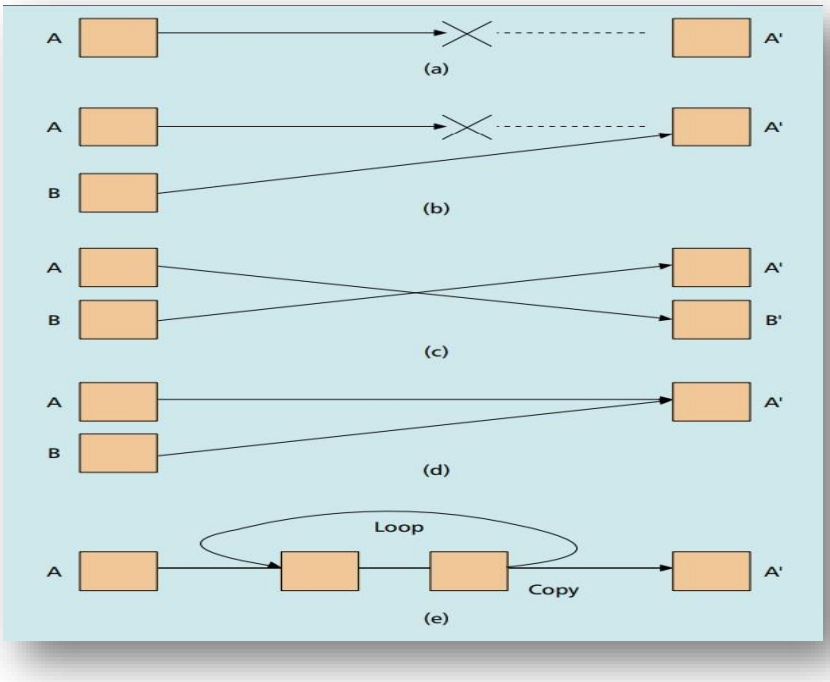
Tolerancija grešaka je važan QoS faktor za koji se smatra da treba održavati opstanak mreže. To je karakteristika sistema koji nastavlja ispravno raditi na mreži u slučaju kvara nekih njegovih dijelova.Mreže su sklone kvarovima zbog različitih razloga (npr.: nepouzdana oprema, softverske greške ili presjecanje kabla). Takve greške i kvarovi mogu utjecati na rad LSP-ova i uzrokovati gubitak paketa. U slučaju kvarova, mehanizam za balansiranje opterećenja može premjestiti pakete koji su u redu čekanja za zahvaćene LSP-ove na nepogođene LSP-ove.(Do et al., 2009)

Većina predloženih pristupa za oporavak MPLS mreže spadaju u dva modela zaštite: brza restauracija, ili unaprijed uspostavljena zaštita i preusmjeravanje, ili dinamička zaštita. U modelu brze restauracije rezervni LSP je unaprijed uspostavljen i konfigurisan, te *bandwidth* mora biti rezervisan. U modelu dinamičke zaštite rezervna kopija LSP se uspostavlja nakon kvara i shodno tome rezervacija *bandwidth*-a se ne primjenjuje sve dok ne dođe do kvara. Model dinamičke zaštite možda nije prikladan za vremenski osjetljive aplikacije zbog dugog vremena oporavka. (Alouneh & Abed, 2010)

Greške LSP-a zahtijevaju testiranje specifičnih tokova paketa, pored mehanizama otkrivanja/lokalizacije kvarova mreže, jer u mnogim slučajevima tokovi paketa mogu biti prekinuti bez greške na mreži (link/čvor). Ovo se može desiti zbog problema s tablicom rutiranja/prosljeđivanja, prekinutog vezivanje labela, zagušenje mreže ili drugih uzroka. Provjera povezanosti, kao i ping/traceroute tipovi OAM (eng. *Organization, Administration, Maintenance*) funkcija su prikladni za ovu vrstu detekcije greške. Implementacija ovih protokola može se razlikovati, ovisno o specifičnoj tehnologiji paketa. Međutim, bez obzira na tehnologiju, važno je da korišteni OAM paketi putuju isti put kao i obični paketi podataka. (Cavendish Dirceu, Hiroshi Ohta & Hari Rakotoranto, 2004)

Na sljedećoj slici prikazani su uobičajeni slučajevi kvara LSP-ova:

- Jednostavan gubitak veze
- Pogrešna veza
- Zamijenjena veza
- Pogrešno spajanje
- Petlja/nenamjerna replikacija



Slika 7. Scenariji kvara LSP: a) jednostavan gubitak veze; b) pogrešno povezivanje; c) zamijenjena veza; d) pogrešno spajanje; e) petlja/nenamjerna replikacija.

Kada je riječ o toleranciji grešaka kod MPLS tehnologije vrijeme oporavka, gubitak paketa i korištenje *bandwidth*-a su glavni parametri usluge za saobraćaj u realnom vremenu.

Tolerancija hardverskih grešaka oslanja se na hardversko otkrivanje i prijavljivanje kvarova, na dostupnost rezervne kopije hardvera i na odgovarajuće dizajniranu softversku implementaciju.

2.2. Sigurnost mreže

"Generalno govoreći, prijetnje kontroli MPLS-a i signalnim protokolima dolaze uglavnom iz dva izvora, eksterna i interna. Eksterne prijetnje dolaze od spoljašnjih uljeza koji nisu sudionici protokola. Interne prijetnje dolaze od ugroženih učesnika protokola, kao što su uobičajeni MPLS čvorovi koji pripadaju domeni. S druge tačke gledišta, gore navedene prijetnje mogu nastati pasivnim ili aktivnim napadima na MPLS čvorove. Pasivni napadi su oni u kojima napadač ne sudjeluje aktivno u obaranju mreže. Za izvođenje aktivnog napada, napadač mora biti u mogućnosti ubaciti proizvoljne pakete u mrežu." (Palmieri & Fiore, 2007b)

TCP je ranjiv na napade uskraćivanja usluge, gdje performanse TCP sesije mogu biti ozbiljno pogođene neovlaštenim pristupom mreži, što može negativno utjecati na CR-LDP.

Kod RSVP-a, autentifikacija i kontrola politike su specificirane, što dozvoljava kreatoru poruka da bude verifikovan i omogućava odbijanje neovlaštenog ili štetnog rezervisanja resursa. Slične karakteristike mogu se definisati za CR-LDP, ali priroda TCP sesije bazirane na konekciji čini ovaj zahtjev manje potrebnim.

"IETF (eng. *Internet Engineering Task Force*) je definisao dvije signalne šeme za uspostavljanje eksplicitno usmjerenih ili LSP-ova zasnovanih na ograničenjima u MPLS okruženju. Jedan se oslanja na upotrebu RSVP-a, dok se drugi pristup temelji na ekstenzijama LDP-a. Obje šeme omogućuju postavljanje eksplicitno usmjerenih LSP-ova i signalizaciju skupa parametara, kao što su ograničenja *bandwidth*-a, koja se odnose na te LSP-ove." (Palmieri & Fiore, 2007b)

MPLS mreža ima sigurnosnu prednost jer nudi VPN funkcionalnost razdvajanjem saobraćaja. Saobraćajni inženjering u MPLS-u je jedna od najčešće oglašavanih karakteristika koja pokreće

brojne pružatelje usluga i održavatelje velikih korporativnih mrežnih infrastruktura prema MPLS baziranim konfiguracijama. (Alouneh & Abed, 2010)

Glavni problemi koji utječu na sigurnost MPLS mreže su povjerljivost, dostupnost i postojanost.

- **Povjerljivost** - Kada je riječ o povjerljivost u MPLS mreži može da se govori o različitim područjima kao što su povjerljivost saobraćaja koji prolazi kroz infrastrukturu ili povjerljivost baza podataka o labelama (eng. *Label Information Base* – LIB). Razumijevanje LIB-a može dovesti do brojnih sigurnosnih problema ako LSR prihvata označene pakete od hostova izvan jezgre. Kako bi se ublažilo brute-force nabrajanje vrijednosti oznaka, bitno je osigurati da se ne prihvataju označeni paketi izvan MPLS infrastrukture. Kod oglašavanja MPLS-a obično se naglašava mogućnost pružanja VPN funkcionalnosti, ali za razliku od uobičajene VPN tehnologije, na primjer IPSec ili SSL VPN-ova, MPLS VPN-ovi ne pružaju nikakvu povjerljivost saobraćaja. MPLS mrežna arhitektura ne pruža šifriranje zaglavlja ili korisnog opterećenja. MPLS tehnologija se pojavila uglavnom kako bi omogućila velike brzine dostave paketa. Kao rezultat toga, o sigurnosnim uslovima se do nedavno nije detaljno raspravljalo sve do skorašnjih zahtjeva za sigurnošću koji su se pojavili kod većine provajdera i istraživača. Razlog zašto MPLS ne pruža mehanizama šifriranja je u vezi sa svrhom za koju je izgrađen. U konvencionalnim IP mrežama, svaki ruter u mreži ima ulogu u analizi IP-a zaglavlja paketa, za klasifikaciju i obradu svakog paketa koji prolazi kroz njega što će, naravno, dodati više troškova i kašnjenja u mreži. U MPLS mreži, samo dva rutera (ulazni i izlazni) su odgovorni za ovaj zadatak. Jezgreni ili LSR ruteri u MPLS mreži će samo proslijediti pakete bazirane na oznakama koje se prenose preko unaprijed uspostavljenog LSP-a. Upotreba enkripcije za pružanje privatnost podataka zahtijeva od osnovnih MPLS rutera analiziranje i obradu zaglavlja paketa, što će rezultirati u smanjenju performansi MPLS mreže.
- **Dostupnost** - ideja neprihvatanja oznake neovlaštenog ažuriranja protokola distribucije je također relevantna za dostupnost, budući da bi zlonamjerna upotreba mogla preusmjeriti soabraćajne tokove unutar jezgre pravljenjem lažnih ažuriranja. Takva ažuriranja treba prihvatiti samo od ovlaštenih članova u MPLS domeni.
- **Integritet** – za izgradnju mreže, MPLS se oslanja na pouzdani ulaz, a osnova su informacije o oznakama. Na osnovu ovog LIB-a, donose se odluke o prosljeđivanju. LDP

informacije i ažuriranja treba prihvatiti samo od pouzdanih izvora. To se može osigurati pomoću dva mehanizma. Prvim, LDP ažuriranja moraju biti prihvaćena samo od interfejsa na kojima se zna da se nalazi drugi LSR. Drugim riječima, LDP ažuriranja ne bi trebala biti prihvaćena od klijenata izvan MPLS jezgre. Drugo, ako se jezgrenim ruterima ne vjeruje ili se pretpostavlja da su ranjivi za napade, tada moraju biti uspostavljeni mehanizmi provjere autentičnosti kako bi se zaštitio izbor protokola distribucije oznaka unutar MPLS mreže. (Alouneh & Abed, 2010)

2.2.1. Napadi na sigurnost mreže

Prijetnje sigurnosti MPLS mreže svrstane se u dvije kategorije - struktuisane i nestuktuisane. Struktuisane prijetnje nastaju od stručnih osoba, sa odgovarajućom tehničkom opremom i značajnim poznavanjem rada mreže i njenih protokola. Kako bi se zaštitilo od ovakvih napada potrebno je naprednije znanje i takva zaštita je kompleksnija. Nestruktuisane prijetnje potiču od manje iskusnih korisnika, koji imaju za cilj pristup mrežnim resursima. Ovakvi napadi se obično izvode bez boljeg poznavanja mrežne tehnologije i putem alata dostupnih putem interneta se pokušavaju pronaći sigurnosni propusti.

Napadi se mogu svrstati u tri kategorije:

- Napadi uskraćivanjem usluge
- Napadi s ciljem neovlaštenog pristupa
- Izviđački napadi

2.2.2. Napadi uskraćivanjem usluge

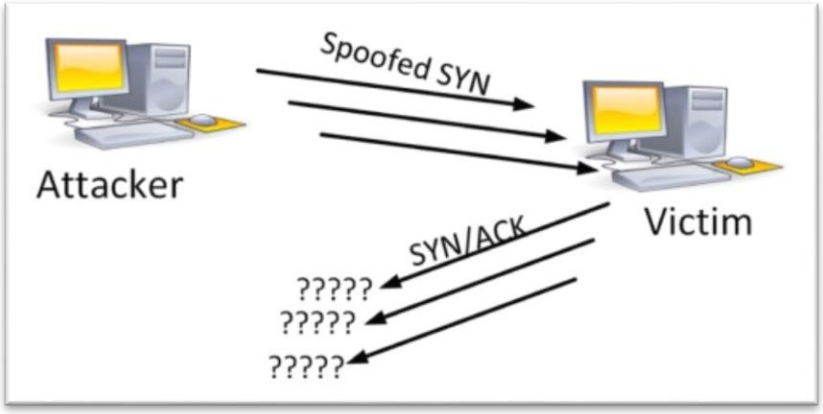
Napadi uskraćivanja usluga (eng. *Denial of Service* - DOS) su stalna opasnost za web stranice. DOS napadi su stekli veću pažnju jer mogu dovesti do ozbiljnog gubitka prihoda ako stranica bude *offline* značajnan vremenski period. Postoji mnogo vrsta napada uskraćivanjem usluga, ali dva od najčešćih su Ping of Death i TCP SYN (eng. *Transmission Control Protocol Synchronize*) Flood.

U napadu Ping of Death, *host* šalje stotine ping zahtjeva (ICMP Echo Requests - eng. *Internet Control Message Protocol*) sa velikim ili paketom nedozvoljene veličine drugom *host*-u, u pokušaju da ga izbaci van mreže ili da ga tako zadrži zauzetim odgovaranjem sa ICMP Echo

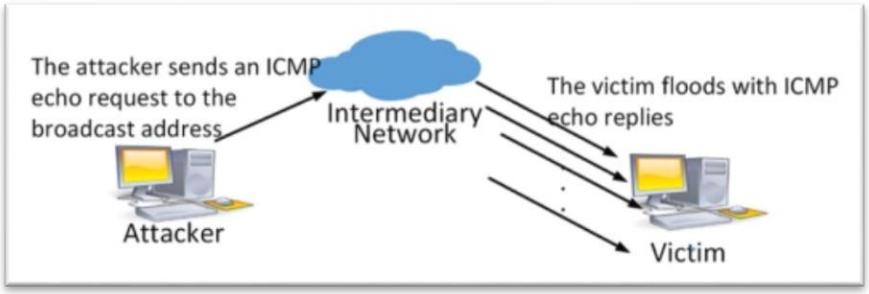
odgovare kako ne bi moga opsluživati klijente. TCP SYN Flood napad koristi prednosti standarda TCP trosmjernog rukovanja slanjem zahtjeva za povezivanje sa nevažećom povratnom adresom. (Elleithy et al., 2005)

Kako doslovno postoje stotine vrste DoS napada podijelit ćemo ih u osnovne skupine:

- Zauzimanje računalnih resursa kao što su procesor, memorija, slobodan prostor na disku i dostupna mrežna propusnost. Ova skupina je ujedno i najčešća i većina je napada fokusirana upravo na ovaj dio. U ovu skupinu spadaju i većina poznatijih DoS napada kao što su: ICMP flood, smurf napad, TCP SYN flood napad, ping smrti itd.
- Napadi s ciljem promjene konfiguracije kao što su, na primjer, stanje tablica usmjerivačkih protokola. Ovi napadi su nešto rjeđe prisutni, ali šteta koju mogu izazvati nije zanemariva, pogotovo zato što je pažnja posvećena njihovoj sigurnosti obično jako mala.
- Napadi s ciljem promjene informacija o stanju, npr. resetiranje aktivne TCP sjednice koji će dovesti do prekida mrežne komunikacije između dva mrežna uređaja.
- Ometanje fizičkih komponenti mrežnih uređaja, bilo da je riječ o različitim sučeljima ili dijelovima za procesiranje.
- Ometanje komunikacijskog medija između korisnika i poslužitelja s ciljem unošenja smetnji ili kompletnog prekida komunikacije. (Petrović, 2009)

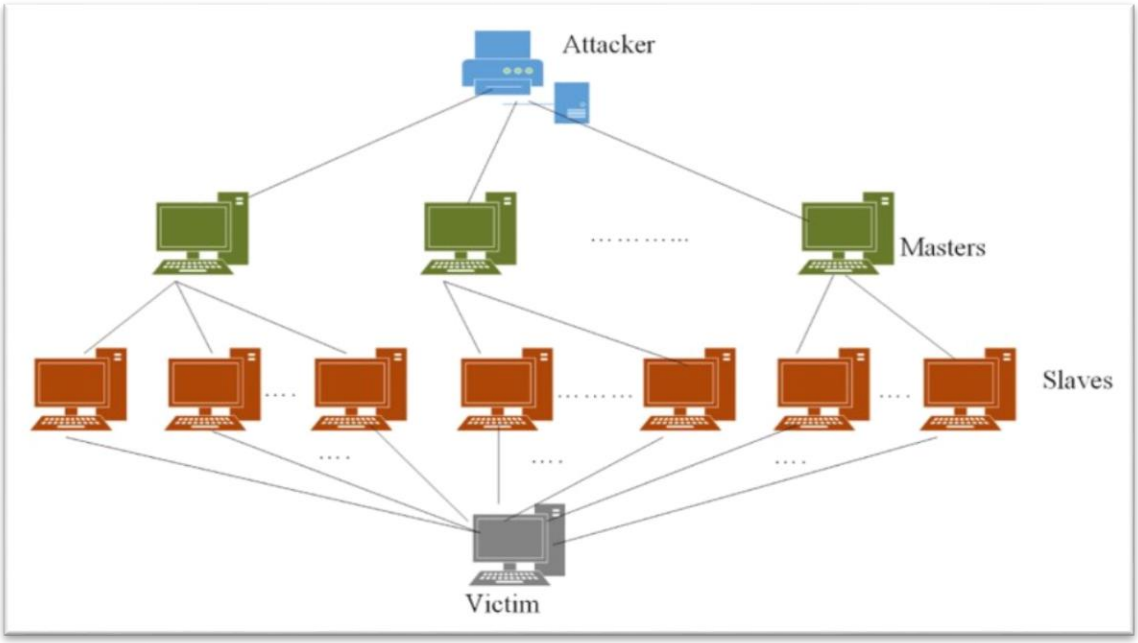


Slika 8. TCP SYN napad



Slika 9. ICMP napad

DDOS (eng. *Distributed Denial of Service*) napade je teško zaustaviti jer mogu doći sa bilo kog mjesta na svijetu. Za implementaciju DDOS-a kreira se program sličan crvu kako bi simulirao samopropagaciju na mnoge hostove na mreži. Osnovna struktura DDoS napada predstavljena je na slici 10. Sastoji se od tri različite faze i četiri različite komponente. Komponente su poznate kao napadač, višestruki kontrolori ili rukovaoci, više robova, agenata ili zombija i žrtva ili meta mašina.



Slika 10. Struktura DDoS napada

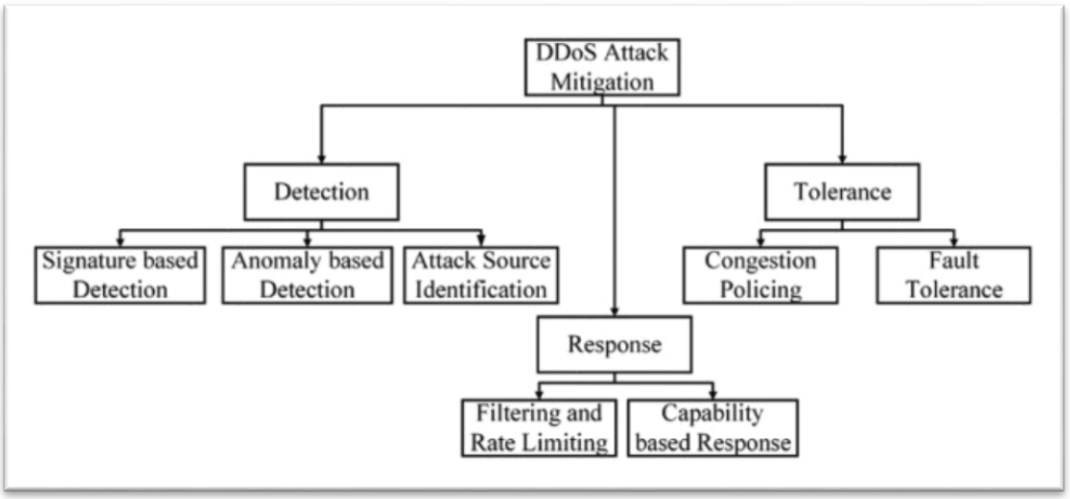
Prevencija protiv DDoS napada je najpoželjnija odbrambena tehnika za borbu protiv DDoS napada. U osnovi, DDoS napadi predstavljaju ogromnu prijetnju resursima žrtava (CPU, memorija) kao i na *bandwidth* i infrastrukturu. Prema tome, ako je napad već pokrenut i može

postati uspješan, on uzrokuje značajno kompromitiranje u sistemu žrtve. Stoga je zaštita od DDoS napada efikasnija jer osigurava prevenciju DDoS napada na saobraćaj, te upravlja velikim opterećenjima napadima, prije nego što oni uspiju rezultirati uspješnim napadom. (Mahjabin et al., 2017)

S obzirom da se DoS napadi dešavaju na različite načine, tako se i primijenjuju različiti načini odbrane od njih. Nekoliko uobičajenih načina odbrane od napada su:

- Fizičko osiguranje mrežne opreme pri njenom smještaju
- Upotreba usmjerivačkih protokola s autentifikacijom
- Upotreba sistema za detekciju napada (eng. *Intrusion Detection System* - IDS)
- Filtriranje nepoželjnih IP paketa
- Skladištenje svih logova na sigurnom centralnom mjestu

Obzirom da je prevencija prvi korak u odbrani od DDoS napada, bitno je spomenuti i ostale mogućnosti u slučaju da se napad ipak desi. Tako je mitigacija napada jedna od posebno značajnih taktika za odbranu od istih. Mitigacija DDoS-a uključuje tri različita mehanizma: mehanizme detekcije, mehanizme odgovora i mehanizme tolerancije, kao što je prikazano na sljedećoj slici.



Slika 11. Mitigacija DDoS napada

Otkrivanje napada je važan korak kod ublažavanja DDoS napada. Detekcija je vrlo jednostavna, obzirom da se performanse usluge ili sistema dramatično degradiraju kada dođe do napada. Međutim, uvijek je izazovno razlikovati zlonamjerne tokove od legitimnih tokova. U literaturi se

uglavnom spominju dvije različite tehnike za otkrivanje malicioznih tokova: detekcija zasnovana na potpisu i detekcija zasnovana na anomalijama. S druge strane, tehnike identifikacija izvora napada su također važne za identifikaciju izvora napada. (Mahjabin et al., 2017)

DOS napadi mogu biti neprimijetni tako prikriveni, lako isporučeni. Kada se kombinuju sa snagom DDoS napada, napadi uskraćivanjem usluge mogu biti zaista moćni.

2.2.3. Napadi s ciljem neovlaštenog pristupa

Još jedan od čestih napada je napad s ciljem ostvarivanja neovlaštenog pristupa. U ovom napadu zlonamjerni korisnik pokušava neovlašteno pristupiti mreži i mrežnim resursima, kao što su elektronička pošta, ftp ili udaljeni pristup putem telnet ili ssh protokola.

Da bi zlonamjerni korisnik ostvario neovlašteni pristup može koristiti više alata, uključujući i ove:

- pogađanje zaporki javno poznatih računa (npr. root, administrator, ftp, php)
- korištenje analizatora protokola da bi se dokopao zaporki koje nekriptirane putuju mrežom
- pristup datoteci s kriptiranim zaporkama, te korištenje nekih od programa za pokušaj njihove dekripcije
- socijalni inženjering (Petrović, 2009)

Ako je mrežni uređaj koji omogućava pristup MPLS mreži za korisnika ojačan u pogledu sigurnosti, onda se može dobiti neovlašteni pristup koji može pružiti detalje o povezivanju sa jezgrom infrastrukture.

Kod ove vrste napada maliciozni korisnik će obično pokušati doći do datoteke sa šiframa, a nakon toga uz pomoć nekih programa za njihovo razbijanje, pokušat će da dođe do kriptovane izvorne šifre koja se nalazi u datoteci. Kako bi došao do šifri, maliciozni korisnik može koristiti i tehniku prisluškivanja, te na taj način pristupiti šiframa koje putuju mrežom bez enkripcije. Ostali napadi s ciljem neovlaštenog pristupa uključuju iskorištavanja propusta u operativnom sistemu računara i određenih aplikacija.

Jedan od primjera je preljev spremnika, greška kojom zlonamjerni korisnik može ostvariti pristup bez prethodne provjere autentičnosti. Nakon što je uspješno provalio na jedan od mrežnih uređaja, napadač će iskoristiti taj uređaj za napad na ostale uređaje. Naravno, kada je dobio pristup, napadač

ima mogućnost promijeniti ili čak obrisati konfiguraciju s mrežnog uređaja, te tako stvoriti dodatne probleme mrežnim administratorima. (Petrović, 2009)

Socijalni inženjering je obično najlakši način za neovlašteni pristup. Njime maliciozni korisnik pokušava izmanipulirasati legitimne korisnike da mu otkriju informacije potrebne za pristup, obično se predstavljajući kao administrator. Situacija može biti i obrnuta, da maliciozni korisnik glumi legitimnog korisnika, tražeći podatke potrebne za pristup od administratora.

MPLS tehnika pruža mnoge skalabilne i fleksibilne mehanizme, npr. upotrebu MD5 algoritma za potpisivanje LDP poruka omogućava samo ruterima sa prethodno unesenim ID-om i lozinkom da uspostavljaju i održavaju sesije.

Konfigurisana šifra se ne prenosi ni u jednom trenutku sesije, što znači da potencijalni neovlašteni ruter (destruktor) nije u mogućnosti da dobije transportovane pakete. Međutim, ponekad može postojati potreba za povećanjem nivoa sigurnosti, npr. za osjetljive podatke - tada je moguće uvesti dodatne elemente, odnosno protokole iz FHRP grupe (eng. *First Hop Redundancy Protocol*), koji uključuje HSRP (eng. *Hot Standby Router Protocol*) i VRRP (eng. *Virtual Router Redundancy Protocol*). Implementacija jednog od njih omogućava redundantnost čvorova (rutera) okosne mreže, što omogućava brzu zamjenu nepodobnih elemenata odgovarajućim ruterima koji čekaju u stanju pripravnosti. (Polkowski & Laskowski, 2015)

2.2.4. Izviđački napadi

Pod izviđačke napade spadaju dvije vrste napada:

- napadi prisluškivanjem
- napadi skeniranjem

kod ovakvih napada maliciozni korisnici pokušavaju prikupiti razne podatke o mreži kao što su vrste mrežnih uređaja, topologija mreže, programi koje uređaji koriste, te njihovu konfiguraciju, a na osnovu prikupljenih informacija takvi korisnici mogu izvršiti napade s ciljem neovlaštenog pristupa ili DOS napade.

Mrežno skeniranje je najčešći napad izviđanjem. U ovom napadu maliciozni korisnik pokušava otkriti uređaje u mreži. Jedan od načina je slanje ICMP (eng. *Internet Control Message Protocol*)

ping paketa na sve IP adrese u mreži ili slanjem ICMP ping paketa na adresu razašiljanja (eng. *broadcast address*), ako to mreža podržava.

Druga vrsta napada izviđanjem je prisluškivanje. Napad prisluškivanjem uključuje presretanje i obradu paketa koji putuju od izvora prema odredištu. Napadač obično koristi neki od analizatora protokola da bi iz mrežnog prometa izdvojio podatke potrebne za daljnje napade. Najjednostavniji primjer je presretanje telnet prometa između klijenta i servera. Ovdje napadač zbog arhitekture samog protokola može vrlo lako doći do korisničkih podataka za autorizaciju. (Petrović, 2009)

2.2.5. Zaštita protokola

Sav saobraćaj u MPLS mreži mora biti isporučen sa nultim gubitkom paketa i sa malim kašnjenjem. Ovaj zahtjev je zbog bandwidth-a i sadržaja koji je osjetljiv na kašnjenje važnih aplikacija, posebno podataka o zaštiti. Mreža ne smije trpiti zbog bilo kakvog neslaganja podataka između izvora i odredišta. Ovaj problem stvara potrebu za mehanizmom zaštite i obnavljanja, što je ključno u brzom rješavanju svakog kvara. (Ridwan et al., 2020)

Sposobnost mreže da pravilno usmjeruje pakete i da se oporavi od promjene topologije uvjetovane ispadom neke od veza ovisi o mogućnosti usmjerivača da sagleda cijelu topologiju koja ga okružuje. Unutar jednog autonomnog sustava u tu svrhu koriste se unutarnji usmjerivački protokoli (IGP eng. *Interior Gateway Protocol*). Njihova osnovna namjena je otkrivanje drugih susjednih usmjerivača i razmjena informacija za usmjeravanje paketa. Unutarnji usmjerivački protokoli namijenjeni su razmjenjivanju ruta unutar jednog autonomnog sustava koji čini računalna mreža pod zajedničkom kontrolom. Sigurnost unutrašnjih usmjerivačkih protokola prilagođena je upravo toj namjeni. Ako je potrebno rute razmjenjivati s drugim autonomnim sustavom, za to postoje drugi protokoli. Oni se nazivaju EGP (eng. Exterior Gateway Protocol). (Petrović, 2009)

Kada je riječ o zaštiti protokola, važno je razlikovati zaštitu od oporavka, a razlika među njima se ogleda u vremenu signalnih poteza. Kod zaštite, putevi oporavka se pripremaju i u potpunosti signaliziraju prije nego što dođe do kvara, dok se kod oporavka putevi oporavka mogu ili prethodno planirati ili biti dinamično dodijeljeni, ali kada dođe do kvara neophodna je dodatna signalizacija kako bi se uspostavio put oporavka. Između različitih mehanizama oporavka koji su klasifikovani kao šeme zaštite, može se napraviti dalja razlika u zavisnosti od broja entiteta za oporavak koji štite određeni broj radnih entiteta.

Glavna prednost zaštite u odnosu na restauraciju je uglavnom brzo vrijeme oporavka. Međutim, tehnike restauracije mogu biti fleksibilnije te zahtijevaju manje backup prostora zbog svoje dijeljene prirode.

Za zaštitu signalnih poruka koje su eventualno modificirane od strane svakog od RSVP rutera duž putanje, mora se pretpostaviti da je svaki dolazni zahtjev autentificiran, zaštićenog integriteta i zaštićene reprodukcije. Na ovaj način se pruža zaštita od lažnih poruka ubačenih od strane neovlaštenih čvorova. Štaviše, pretpostavlja se da se svaki RSVP osvješteni ruter ponaša na očekivani način. Odlazne poruke poslane na sljedeći mrežni element primaju novu zaštitu prema RSVP sigurnosnoj obradi. (Tschofenig, 2005)

Za zaštitu u RSVP protokolu objašnjene su dvije metode. Metoda sigurnosne kopije jedan-na-jedan stvara zaobilazne LSP-ove za svaki zaštićeni LSP na svakoj potencijalnoj tački lokalnog popravka. Metoda rezervne kopije objekta stvara zaobilazni tunel za zaštitu potencijalne tačke kvara; korištenjem prednosti MPLS slaganja labela, ovaj zaobilazni tunel može zaštititi skup LSP-ova koji imaju slična ograničenja rezervne kopije. Obje metode se mogu koristiti za zaštitu linkova i čvorova tokom mrežnog kvara. Opisano ponašanje i proširenja za RSVP omogućavaju čvorovima da implementiraju bilo koju metodu, ili obje, te da interoperišu u mješovitoj mreži. (Pan, 2005)

RSVP INTEGRITY objekat je glavna komponenta RSVP sigurnosne zaštite. Ovaj objekat se koristi za obezbeđivanje integriteta i ponavljanje zaštite sadržaja signalne poruke između dva učestvujuća RSVP rutera ili između RSVP rutera i hosta. Nadalje, RSVP INTEGRITY objekat osigurava autentifikaciju porijekla podataka. Atributi objekta su:

- Flag polje
- Identifikator ključa
- Broj sekvence
- Sažetak poruke sa ključem (Tschofenig, 2005)

Razmjena ruta unutar jednog autonomnog sustava ključna je za pouzdano funkcioniranje cijele mreže. Ako bi zlonamjeran korisnik imao mogućnost manipulacije podacima koji se koriste za usmjeravanje, to bi uvelike narušilo sigurnost cijele mreže. Da bi poboljšali sigurnost unutrašnjih usmjerivačkih protokola ključno je zaštiti kanale komunikacije koji se koriste za razmjenu ruta. To se može učiniti na dva načina. Korištenjem neke vrste provjere vjerodostojnosti, te

ograničavanjem generiranja usmjerivačkih paketa na sučeljima gdje to nije potrebno, a gdje bi to potencijalni zlonamjeran korisnik mogao iskoristiti. (Petrović, 2005)

2.2.6. Sigurnost TCP/IP protokola

TCP/IP standardni su Internet komunikacijski protokoli koji omogućavaju računarima komunikaciju na velikim udaljenostima.

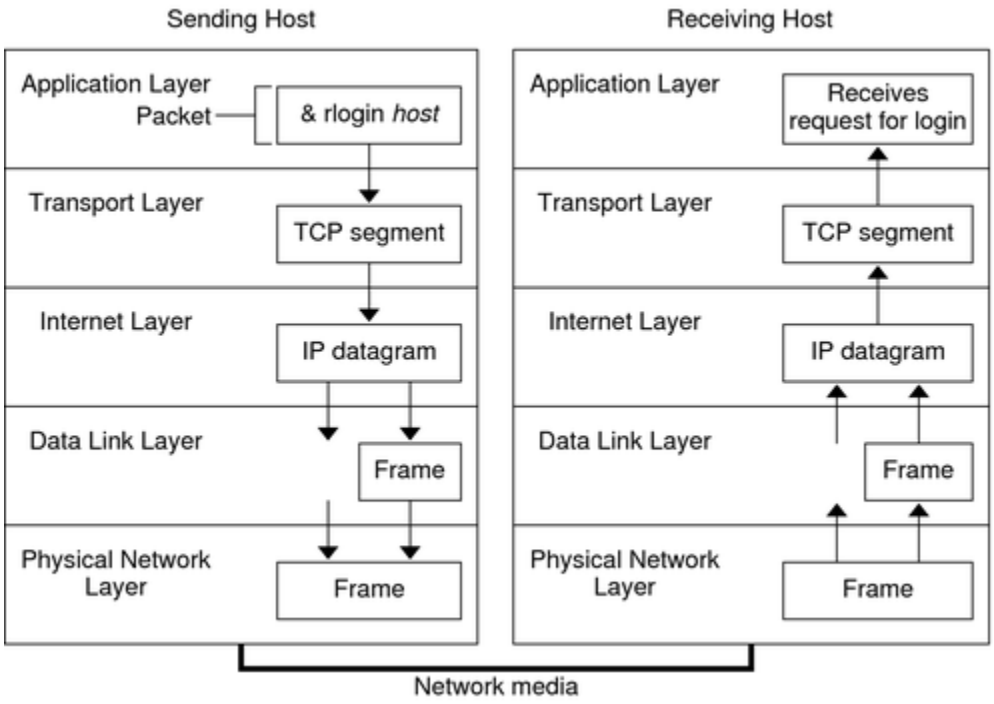
TCP/IP paket je kolekcija komunikacijskih protokola zasnovanih na mreži koji pružaju i podržavaju različite vrste usluga koje rade preko mreže. On utvrđuje, održava i prekida veze između krajnjih tačaka i pruža full-duplex end-to-end konekciju. Također formatira podatke, adrese, usmjerava mrežne pakete podataka i osigurava njihovu isporuku primaocu. Dvije glavne komponente paketa TCP/IP protokola su eng. *Transmission Control Protocol* - TCP i Internet Protokol - IP. (Saini & Pandey, 2014)

TCP/IP model se sastoji od 4 sloja:

- **Aplikacijski sloj** - najviši sloj u TCP/IP modelu, odgovoran je za rukovanje protokolima visokog nivoa, te pitanjima predstavljanja. Ovaj sloj omogućava korisniku interakciju s aplikacijom. Neki od protokola prisutnih u ovom sloju su: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.
- **Transportni sloj** - zadužen je za pouzdanost, kontrolu toka i korekciju podataka koji se šalju preko mreže. Dva protokola koja se koriste u transportnom sloju su UDP (eng. *User Datagram Protocol*) i TCP.
- **Internet sloj** – naziva se još i mrežni sloj, definiše protokole odgovorne za logički prijenos podataka preko cijele mreže. Glavni protokoli na ovom sloju su: *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Reverse Address Resolution Protocol* (RARP), *Internet Control Message Protocol* (ICMP) i *Internet Group Management Protocol* (IGMP).
- **Mrežni pristupni sloj** - sloj u TCP/IP modelu na kojem se podaci prenose i primaju preko fizičke mreže. Uređaj mrežnog interfejsa, obično linijska kartica, adapter ili port se koristi za povezivanje fizičkih žica ili vlakana s računarom kako bi mogao komunicirati sa drugim računarima. TCP/IP je dizajniran da bude nezavisan od metode pristupa mreži, formata

okvira i medija. Drugim riječima, nezavisan je od bilo koje specifične mrežne tehnologije. Na ovaj način, TCP/IP se može koristiti za povezivanje različitih tipova mreža, kao što su Ethernet, Token Ring, X.25, Frame Relay i Asinhroni način prijenosa (ATM).

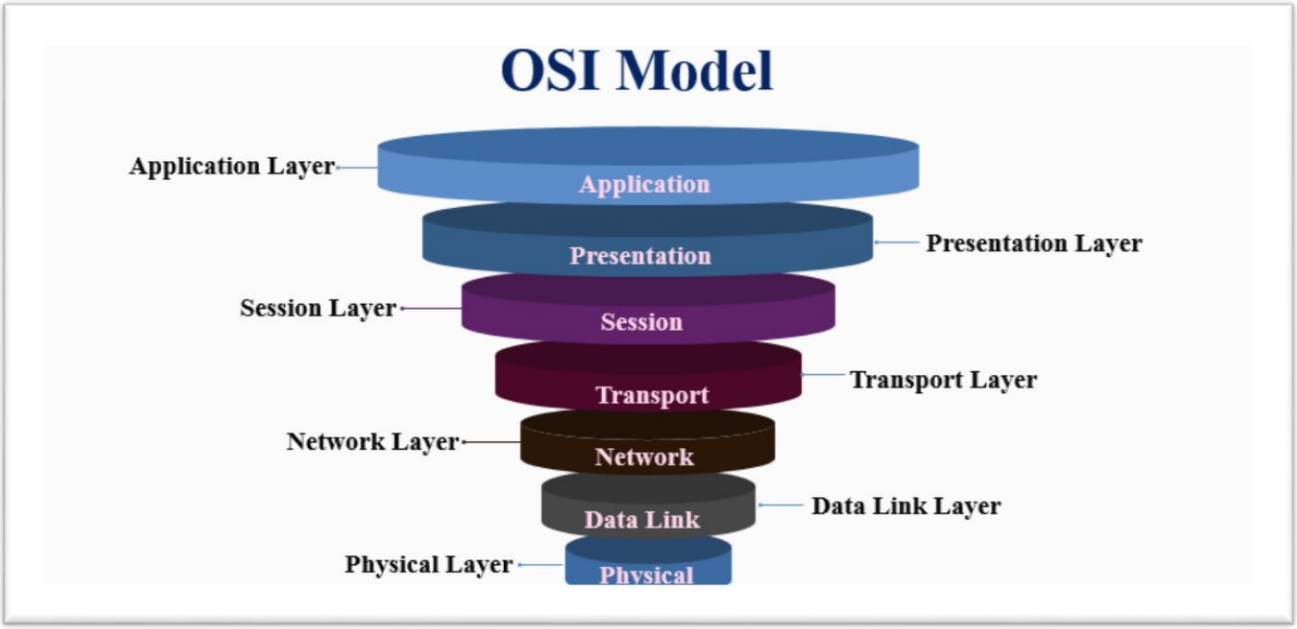
TCP/IP paket protokola je dizajniran kroz visoko strukturirani i slojeviti pristup, sa svakim slojem odgovornim za različite aspekte komunikacije. Ova hijerarhijska arhitektura, omogućava da svaki sloj pruži jedinstveni skup funkcija. Enkapsulacija podataka se postiže različitim zaglavljima između različitih slojeva kao što su IP zaglavlje, TCP zaglavlje ili zaglavlja aplikacije. Ova zaglavlja su kritična i održavaju određeni skup informacije potrebnih za funkcionalne i administrativne razloge za taj određeni sloj. (Saini & Pandey, 2014)



Slika 12. Komunikacija putem TCP/IP protokola

Međunarodna organizacija za standarde (eng. *International Organization for Standardization* - ISO) kreirala je sedmoslojni mrežni model koji se koristi za postavljanje standarda za mrežne komunikacije. Model se zove referentni model povezivanja otvorenih sistema (eng. *Open System Interconnection* - OSI). Slojevi od vrha prema dnu su: aplikacijski, prezentacijski, sjednički, prijenosni, mrežni, podatkovni i fizički sloj. Svaki sloj u OSI modelu ima svoje jasno definisane funkcije, a funkcije svakog sloja komuniciraju i stupaju u interakciju sa slojevima neposredno iznad i ispod njega, osim ukoliko sloj nema slojeve ispod ili iznad. Razlika u odnosu TCP/IP model

ogleda se u tome što se taj model ne bavi strogom hijerarhijskom enkapsulacijom i slojevima. TCP/IP prepoznaje četiri široka sloja funkcionalnosti koji su izvedeni iz operativnog opsega njihovih sadržanih protokola: opseg softverske aplikacije; transportni put od domaćina do domaćina; opseg umrežavanja; i opseg direktnih veza sa drugim čvorovima na lokalnoj mreži. ('Comparison with TCP/IP model (Wikipedia)', 2023a)



Slika 13. OSI referentni model

Svaki sloj u OSI modelu ima svoje dobro definirane funkcije, a funkcije svakog sloja komuniciraju i stupaju u interakciju sa slojevima neposredno iznad i ispod njega, osim ako sloj nema slojeve ispod ili iznad. ('OSI model (Wikipedia)', 2023c)

Glavne prijetnje TCP/IP protokolu su:

- SYN poplavljivanje
- Lažiranje IP-a
- Napad sa rednim brojem
- Otmica TCP sesije
- RST i FIN napad uskraćivanjem usluge
- Ping O' Death

Za zaštitu protokola kao prevencija od napada koriste se različite tehnike. U nastavku će biti kratko objašnjene neke od njih:

- ***Firewall***-i – Zaštitni zidovi su sistemi dizajnirani da spriječe neovlašteni pristup mreži ili iz mreže. Zaštitni zid je namjenski uređaj ili softver koji radi na sistemu koji vrši inspekciju mrežnog saobraćaja koji prolazi kroz njega i odbija ili dozvoljava prolaz na osnovu skupa pravila. Zaštitni zidovi mogu se implementirati i u hardver i softver ili kombinacijom oba.
- **Virtuelne privatne mreže** (VPN) – VPN je privatna mreža koja koristi javnu mrežu kao što je internet za povezivanje udaljenih lokacija ili korisnika zajedno. Umjesto korištenja namjenskih veza u stvarnom svijetu kao što je iznajmljena linija, VPN koristi "virtuelne" veze, rutirane kroz internet sa privatne mreže kompanije na udaljenu lokaciju. Implementira se kao dodatni logički sloj na vrhu postojeće veće mreže.
- **Autentifikacija** - autentifikacija znači provjeru identiteta korisnika koji se prijavljuje na mrežu. Autentifikacija je proces utvrđivanja da li je ta osoba zaista osoba za čiji identitet tvrdi da joj pripada. Drugim riječima autentifikacija je proces provjere identiteta korisnika.

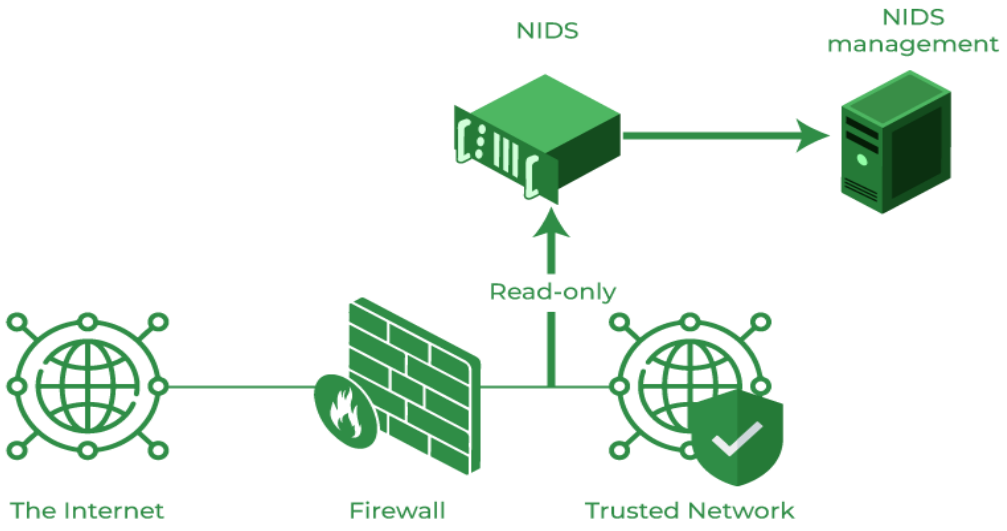
2.2.7. Sistemi za detekciju mrežnih napada

Detekcija upada se može definisati kao akt detekcije takvih aktivnosti, koje su usmjerene na kompromitovanje povjerljivosti, integriteta i raspoloživosti resursa. Preciznije, cilj detekcije upada je identifikacija entiteta koji pokušavaju da naruše postojeći sistem sigurnosnih kontrola. Praksa je pokazala da čak i detaljno filtriranje paketa, stalna inspekcija i proxy firewall mogu propustiti nedopustivo mnogo upada. Svojim dizajnom, firewall je uređaj prvenstveno namenjen za zaštitu graničnog područja jedne mreže i koji se ne bavi internim ponašanjem mreže, sistema ili korisnika. To otvara prostor za mrežne napade prema povredivim servisima, napade pomoću podataka koji su usmjereni ka aplikacijama, napade usmjerene ka hostovima (eskalacija privilegija, neautorizovani login i pristup osjetljivim datotekama i maliciozne prijetnje – virusi, trojanci i crvi). (Čisar, 2013)

Razvojem vatrozida i njihovih mogućnosti zaštita računalnih mreža pojavila se potreba za sustavom koji bi bio posvećen detaljnoj analizi mrežnog prometa i bio bi u mogućnosti predvidjeti određene vrste mrežnih napada neovisno o protokolu, aplikaciji i operacijskom sustavu koji koristi klijent ili server. U tu svrhu razvijeni su uređaji za detekciju napada (IDS, eng. *Intrusion Detection*

System) i njihove poboljšane verzije, uređaji za prevenciju napada (IPS, eng. *Intrusion Prevention system*). IDS je uređaj ili skup programa, dizajniran da bi mogao detektirati neželjene pokušaje pristupa, pokušaj onesposobljavanja ili manipulaciju računalnim sustavima, korištenjem određenih mrežnih resursa, posebno pristupa internetu. Ti pokušaji udaljenog pristupa mogu imati oblik nekih od napada, te ih IDS sustav mora razlikovati od uobičajenog mrežnog prometa. Princip rada uređaja za prevenciju napada (IPS) isti je kao i kod IDS uređaja, s tom razlikom što IPS uređaji imaju mogućnost i blokiranja potencijalnih napada. Blokiranje napada IPS može vršiti slanjem RST paketa kod TCP komunikacije ili udaljenom konfiguracijom određene mrežne opreme da bi blokirao mrežni promet s određenog izvora. (Petrović, 2005)

Metodologije otkrivanja upada klasificirane su u tri glavne kategorije: detekcija zasnovana na potpisu (eng. *Signature-based Detection* - SD), detekcija zasnovana na anomalijama (eng. *Anomaly-based Detection* - AD) i Stateful Protocol Analysis (eng. *Stateful Protocol Analysis* - SPA). Danas postoji mnogo vrsta IDS tehnologija koje se kategoriziraju u četiri klase prema tome gdje su raspoređene za inspekciju sumnjivih aktivnosti i koje događaje mogu prepoznati: IDS zasnovan na hostu (eng. *Host-based IDS* - HIDS), IDS zasnovan na mreži (eng. *Network-based IDS* - NIDS), IDS zasnovan na bežičnoj mreži (eng. *Wireless-based IDS* - WIDS), analiza ponašanja mreže (eng. *Network Behavior Analysis* - NBA) i mješoviti IDS (eng. *Mixed IDS* - MIDS). (Liao et al., 2013)



Slika 14. Osnovna konfiguracija NIDS-a

Osnovne komponente IDS sistema su: senzori, komponenta za analizu (engl. *analyzer*) i komponenta koja generiše odgovor (engl. *response*). Senzori prikupljaju podatke, odnosno događaje iz okruženja. Postoje dvije vrste senzora: senzori smješteni na računaru HIDS (engl. *Host-based IDS*) i mrežni senzori NIDS (engl. *Network IDS*).

Host-bazirani IDS se sastoji od agenta na hostu koji identifikuje upade analiziranjem poziva sistema, aplikacionih logova, promjene sistema datoteka (binarne, password datoteke, sposobnost/acl baze podataka) i druge aktivnosti i stanja hosta. Najčešći problem sa host-baziranim sistemima je to što na analizu dobijaju samo one podatke koje su aplikacije već upisale u logove.

NIDS je nezavisna platforma koja identifikuje upade ispitivanjem mrežnog saobraćaja i monitoringom višestrukih hostova. NIDS obezbjeđuje pristup mrežnom saobraćaju putem konekcije na hab, mrežni svič konfigurisan na preslikavanje porta ili mrežni pristupni port – tap (engl. *Test Access Port* – TAP). Problem kod ovih sistema predstavlja enkriptovani saobraćaj, saobraćajno preopterećenje mreže i procjena namjere neke određene akcije. (Čisar, 2013)

Maliciozni korisnici znaju da se uglavnom koriste IDS uređaji i poznaju njihove principe rada, te su s toga razvili su određene tehnike koje zaobilaze njihovu funkcionalnost. Neke od najčešće primijenjenih tehnika su:

- **Poplavljivanje** (eng. *flooding*) – generisanjem veće količine saobraćaja napadač pokušava zagušiti IDS senzor, kako bi stvarni napad prošao neprimijećeno. Ukoliko se napad ipak otkrije na osnovu zauzimanja resursa, IDS možda neće na vrijeme generisati alarm
- **Fragmentacija** - napadač dijeli maliciozne pakete na manje dijelove, što zahtijeva od IDS-a njihovo ponovo sastavljanje, na taj način opterećujući procesor. Ako je broj fragmentiranih paketa velik, IDS neće na vrijeme moći analizirati sav mrežni saobraćaj i napadi mogu proći neprimijećeni.
- **Enkripcija** – putem sigurnih sjednica napadač pokušava izvesti napad koji je obično neprimijetan za IDS.
- **Omama** (eng. *obfuscation*) – putem specijalnih znakova napadač pokušava sakriti napad. Ti znakovi mogu biti: kontrolni znakovi, heksadecimalni prikaz, unicode prikaz. IDS se bazira na obrasce te se iz tog razloga dodaju posebni znakovi u neke napade, kako bi se sistem zavarao.

Sistem za detekciju upada je ključni dio odbrambenih operacija, koji dopunjuje uobičajene statičke oblike odbrane računarske mreže. Posljednjih godina podaci o mrežnom saobraćaju su postali veći i složeniji, što dovodi do većih mogućnosti upada u mrežu. Tradicionalne metode otkrivanja upada suočavaju se s poteškoćama u obradi mrežnih podataka velike brzine i ne mogu otkriti trenutno nepoznate napade.

2.2.8. Sigurnost mrežnih uređaja

Osim uređaja za detekciju i prevenciju napada, među mrežne uređaje također spadaju i *router*-i, *switch*-evi i *firewall*-i. U cilju osiguranja tri najbitnija parametra MPLS mreže, bitno je osigurati ove uređaje, kako bi mreža bila operativna i funkcionalna u svakom trenutku, ali i kako bi protok podataka bio neometan i u skladu sa osiguranim kvalitetom usluge.

- *Router*-i su mrežni uređaji koji vrše usmjeravanje paketa prema logičkoj osnovi mrežnog sloja, te na taj način povezuju dvije ili više računarskih mreža. Arhitektura routera se sastoji od tri nivoa – upravljačkog, podatkovnog i nadzornog. Upravljački nivo se sastoji od protokola i procesa za komunikaciju između mrežnih uređaja, kako bi omogućio prijenos podataka između njih. Zaštita ovog nivoa na router-u je vrlo bitna stvar jer ona osigurava ispravan rad podatkovnog i nadzornog nivoa.
- *Switch*-evi su uređaji koji služe za spajanje više segmenata mreže u jednu cjelinu. Budući da su danas ethernet mreže skoro u potpunosti izgrađene od preklopnika (*switcheva*), koncentratore (eng. *hub)* i mostove (eng. *bridge*) rijetko gdje susrećemo. Korištenjem preklopnika u mreži, propusnost se više ne dijeli na cijelu mrežu već isključivo ovisi o brzini između dva sudionika. Korištenjem preklopnika moguće je istovremeno ostvariti više komunikacija na linijskoj brzini bez zagušenja mreže.
- *Firewall* je uređaj koji kontroliše tok podataka između različitih dijelova mreže. Tehnologija firewall-a uvelike se mijenjala tokom godina, od kada se prvi puta pojavila na tržištu početkom 90-ih godina. Prvi firewall-i bili su jednostavni uređaji za filtriranje paketa. Od tada, oni su postali sve sofisticiraniji što se tiče mogućnosti filtriranja, ali i dodajući neke nove funkcionalnosti kao što su:
- praćenje stanja veze (eng. *stateful firewall*),
- virtualne privatne mreže (VPN)

- sistemi za detekciju upada
- provjera autentičnosti konekcije
- virtualni vatrozidi

Za omogućavanje komunikacije između mrežnih uređaja kao i za obavljanje nadzora potrebno je koristiti pojedine protokole. U nastavku će biti opisani samo određeni protokoli, a to su: ICMP, TELNET, SSH i SNMP. ICMP se koristi za provjeru dostupnosti uređaja, TELNET i SSH za spajanje na usmjerivače i postavljanje potrebne konfiguracije, te SNMP za prikupljanje podataka sa mrežnih uređaja na temelju kojih će se crtati grafovi prometa i paketa. (Faletar, 2020)

- **Internet Control Message Protocol** - ICMP (engl. *Internet Control Message Protocol*) je protokol mrežnog nivoa i sastavni dio IP protokola, premda se ponaša kao protokol višeg nivoa šaljući svoje poruke putem IP protokola. ICMP protokol se uglavnom primjenjuje za osiguranje nadzora i kontrolu prenosa podataka do odredišta, jer IP protokol to ne omogućava. Putem poruka koje ICMP protokol šalje osigurava se kontrolu toka, prijava greški, pojava alternativnog puta do odredišta, kao i druge informacije namijenjene TCP/IP programskoj podršci. Ovim se ne osigurava pouzdan prijenos podataka, on se ostvaruje protokolom višeg nivoa. Poruke se šalju samo kao odgovor na poslane IP pakete, dok se on ne šalje na na poslane ICMP pakete. Ukoliko se ICMP poruka izgubi, ne generiše se nova ICMP poruka o nastaloj grešci. Mrežni uređaji, uključujući routere, koriste ICMP za slanje poruka o grešci i operativnih informacija koje upućuju na to da tražena usluga, računar ili router nisu dostupni. ICMP poruka se šalje unutar IP paketa, koji se sastoji od IP zaglavlja, ICMP zaglavlja i ICMP ostatka podataka. ICMP generiše osam različitih vrsta poruka, od kojih tri zahtijevaju odgovor. Ovaj protokol se koristi uglavnom za istraživanje i rješavanja mrežnih problema. Glavne naredbe za rješavanje mrežnih problema koje u ICMP protokolu su: „ping“ i „traceroute“. Ping je ujedno i jedan od najčešće korištenih ICMP paketa čijom primjenom se uz ispravno postavljanje potrebnih parametara može ocijeniti povezanost dva računara na internetu. Za prikupljanje statističkih podataka se također koristi naredba “ping”, tzv. „round trip“, što predstavlja vrijeme koje je potrebno da paket ode do određenog računara na internetu i nazad, broja neuspješnih odgovora itd. Druga korisna primjena ICMP protokola je u naredba “traceroute”, koja se koristi za

određivanje povezanosti dva računara na mreži, ali s tim da daje informacije i o svim računarima koji se nalaze na putu od izvora do odredišta.

- **Telnet** - Telnet je aplikacijski protokol koji korisniku omogućava komunikaciju s udaljenim uređajem. Najčešće se koristi za omogućavanje sesije korištenja interfejsa komandne linije (engl. *command-line interface* - CLI) korisniku sa jednog računara na drugom udaljenom uređaju. Mrežni administrator često koriste telnet kako bi pristupili i upravljali udaljenim uređajima. Kako bi pristupili udaljenom uređaju, oni koriste naredbu telnet, te IP adresu ili naziv uređaja (engl. *hostname*). Nakon što se uspješno spoje i pristupe udaljenom uređaju, mrežni administratori pomoću virtualnog terminala imaju mogućnost upravljanja i komuniciranja s udaljenim uređajem. Telnet koristi model telnet klijenta i telnet poslužitelja. Telnet klijent, tj. uređaj/računar koji korisnik koristi, prihvata unos tastature i šalje naredbe na telnet poslužitelj. Telnet protokol je jednostavan za korištenje, iako se više ne koristi tako često iz razloga što je nije siguran protokol, tj. upravo zbog toga što se svi podaci i naredbe šalju u obliku čistog (ne kriptiranog) teksta, pa čak i šifre, što narušava sigurnosne aspekte.
- **SSH** - SSH (engl. *Secure Shell*) protokol je nastao kao zamjena za druge, nesigurne protokole koji putem računarske mreže razmjenjuju podatke. SSH za razliku od postojećih protokola uvodi zaštitu tajnosti podataka, dok se kod drugih sličnih protokola podaci kroz mrežu šalju nekriptirani i bilo koji korisnik može ih presresti, pročitati ili čak mijenjati. SSH podatke kriptira prije slanja i dekriptira nakon prijema, čime se onemogućava njihovo otkrivanje u toku kretanja mrežom. SSH je baziran na modelu klijent/poslužitelj, što znači da se komunikacija odvija između dvije različite strane. Poslužitelj osluškuje zahtjeve na unaprijed zadanom mrežnom priključku (engl. *port*), a klijent ih po potrebi šalje poslužitelju. SSH poslužitelj osluškuje zahtjeve klijenata na TCP priključku. Uspostava komunikacije i sama komunikacija u SSH protokolu opisana je troslojnom arhitekturom: 1. Transportni sloj (engl. *Transport Layer Protocol*), 2. Autentifikacijski sloj (engl. *Authentication Protocol*), 3. Konekcijski sloj (engl. *Connection Protocol*).
- **Simple Network Management Protocol** - SNMP je protokol aplikacijskog sloja kojim se olakšava razmjena informacija o upravljanju među mrežnim uređajima, kao što su: čvorovi, routeri, switchevi i dr. SNMP je dio skupa TCP/IP protokola i administratorima omogućava udaljeni nadzor i upravljanje mrežnim performansama, pronalaženje i rješavanje mrežnih

problema te planiranje potreba za proširenjem mreže. SNMP je upravljački mrežni protokol kojim se olakšava upravljanje i nadzor kompletne mreže. Funkcionalnost i implementacija SNMP protokola je relativno jednostavna, ali ipak dovoljno fleksibilna da omogući kvalitetno upravljanje velikim brojem različitih tipova uređaja u distribuiranoj mrežnoj okolini. Do sada su se pojavile tri verzije SNMP protokola: SNMPv1, SNMPv2 i SNMPv3.

2.3. Virtualne privatne mreže

Virtualna privatna mreža (eng. *Virtual Private Network* - VPN) omogućava korisniku da proširi svoju privatnu mrežu na širu javnu mrežu na siguran način. Pružatelji internetskih usluga nude ovu uslugu osiguravajući da ulazne tačke u njihovu mrežu mogu razmjenjivati podatke samo ako su konfigusane kao da pripadaju istom VPN-u. MPLS LSP-ovi pružaju izvrstan način za pružanje ove usluge putem IP mreže.

"MPLS VPN je porodica metoda za korištenje MPLS-a u svrhu stvaranja virtualnih privatnih mreža (VPN). MPLS VPN je fleksibilna metoda za transport i usmjeravanje nekoliko vrsta mrežnog saobraćaja korištenjem MPLS *backbone*-a.

Danas postoje tri vrste MPLS VPN-ova raspoređenih u mrežama: 1. *Point-to-point* (*Pseudowire*) 2. sloj 2 (VPLS) 3. sloj 3 (VPRN)

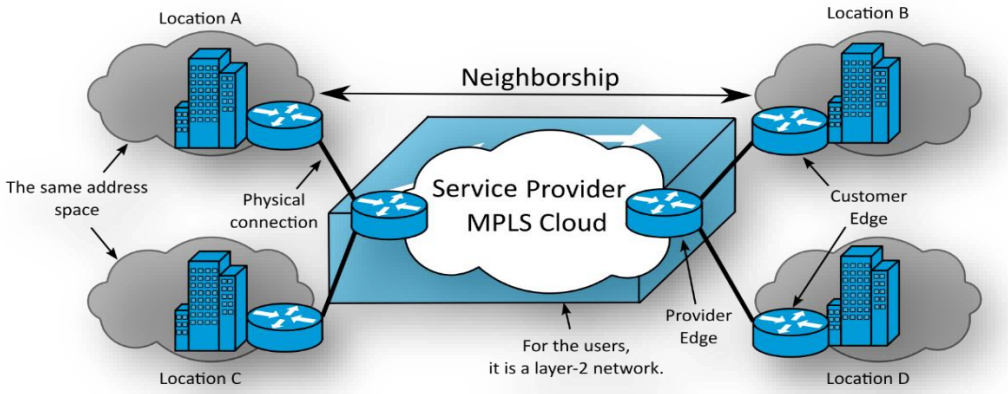
- **Point-to-point** MPLS VPN-ovi koriste VLL (eng. *Virtual leased line* - virtualne iznajmljene linije) za pružanje Layer2 *point-to-point* povezivanja između dvije web lokacije. Ethernet, TDM i ATM okviri mogu se uvrstiti u ove VLL-ove.

Primjeri kako se *point-to-point* VPN-ovi mogu koristiti uključuju:

- enkapsulaciju TDM T1 krugova spojenih na udaljene terminalne jedinice
- prosljeđivanje neusmjerenog DNP3 saobraćaja preko *backbone* mreže na SCADA glavni kontroler.

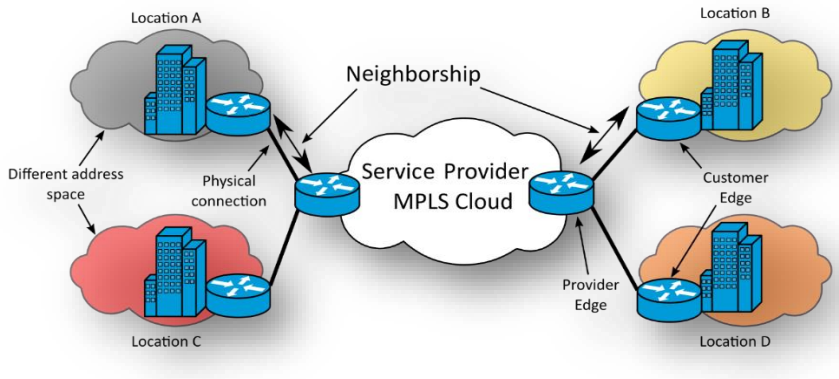
- **MPLS VPN sloja 2** ili VPLS (virtualna privatna LAN usluga) nudi uslugu u stilu „prebacivanja u oblaku". VPLS pruža mogućnost raspodjele VLAN-ova između web

lokacija. L2 VPN-ovi se obično koriste za usmjeravanje glasovnog, video i AMI saobraćaja između podstanica i lokacija podatkovnih centara.



Slika 15. MPLS VPN sloja 2

- **Sloj 3** ili VPRN (eng. *Virtual Private Routed Network* - virtualna privatna usmjerena mreža) koristi VRF sloja 3 (VPN/virtualno usmjeravanje i prosljeđivanje) za segmentiranje tabela usmjeravanja za svakog korisnika koji koristi uslugu. Korisnik se povezuje sa ruterom provajdera usluga i dvije rute razmjene, koje su smještene u tabelu usmjeravanja specifičnu za korisnika. Višestruki protokol BGP (MP-BGP) je potreban u oblaku za korištenje usluge, što povećava složenost dizajna i implementacije. L3 VPN-ovi se obično ne postavljaju na *utility* mreže zbog svoje složenosti; međutim, L3 VPN mogao bi se koristiti za usmjeravanje saobraćaja između korporacija ili lokacija podatkovnih centara.” (MPLS VPN (Wikipedia)', 2023c)



Slika 16. MPLS VPN sloja 3

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. Osnovna prednost korištenja VPN-a je značajna ušteda u odnosu na cijenu koštanja privatnih iznajmljenih linija. VPN je znatno fleksibilnija i skalabilnija mreža u odnosu na klasične privatne WAN mreže koje su bile realizirane zakupljenim vodovima. (Kraljević, 2021)

2.3.1. Virtualne privatne mreže bazirane na MPLS tehnologiji

Jedna od najvećih sposobnosti MPLS mreže je mogućnost izgradnje virtualnih privatnih mreža (VPN-ova). MPLS VPN tehnologija omogućava povezivanje pojedinih korisničkih usluga pomoću različitih tipova virtualnih privatnih mreža. MPLS VPN se može 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 dijele na VPWS (eng. *Virtual Private Wire Service*), VPLS (eng. *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 routera do PE routera, pomoću statičke rute ili BGP protokola. PE routeri sadrže virtualnu tablicu umjeravanja i prosljeđivanja podataka. Svaki PE router konfiguriše poslužitelja uz primjenu vlastite tablice. Podatci zapisani u tablicama ne dijele se unutar MPLS VPN mreže. Kada se podaci premjeste s čvora na čvor Virtual Private LAN services, pregledava se zapis u tablici usmjeravanja, dodaje se oznaka za tu lokaciju i šalje se paket na sljedeći router. 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 prenos podataka putem javnih mreža, MPLS VPN-ovi koriste izoliranu privatnu mrežu, zbog čega je potrebno šifrirati podatke koji se prosljeđuju između čvorova.

2.3.2. MPLS i VPN ahritektura mreže

MPLS omogućava ISP-ovima da ponude VPN usluge pružanjem jednostavnog, fleksibilnog i moćnog mehanizma tuneliranja. ISP može implementirati VPN obezbjeđivanjem skupa LSP-ova za pružanje povezivanja između različitih lokacija u VPN-u. Svaka VPN lokacija tada oglašava ISP-u skup prefiksa koji su dostupni unutar lokalne stranice. ISP-ov sistem rutiranja distribuiše

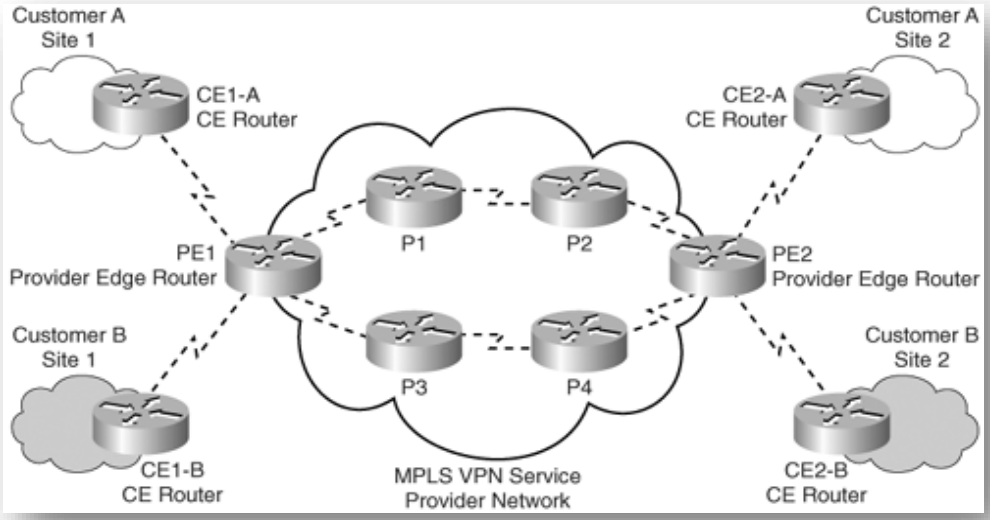
ove informacije dodavanjem oznaka u ažuriranjima protokola rutiranja ili korištenjem protokola distribucije oznaka. VPN identifikatori dozvoljavaju da jedan sistem rutiranja podržava više VPN-ova čiji se interni adresni prostori međusobno preklapaju. Na kraju, svaki ulazni LSR postavlja saobraćajne LSP-ove na osnovu kombinacije odredišne adrese paketa i informacije VPN-a o članstvu. (Lee et al., 2000)

Arhitektura MPLS VPN-a sastoji se od tri komponente: CE (eng. *Customer Edge*), PE (eng. *Provide Edge*) i P (eng. *Provide*).

- *Customer Edge (CE) ruteri*: postavljaju se na licu mjesta i obično su u vlasništvu poslovnog klijenta. Neki provajderi usluga takođe isporučuju CE opreme za malu najamninu.
- *Provider Edge (PE) ruteri*: Ovo su rubni ruteri provajdera na koje se spajaju CE ruteri. PE ruteri su uvijek u vlasništvu provajdera usluga.
- *Provajder (P) ruteri*: Ovi ruteri su uobičajeni nazivaju "tranzitni ruteri" i nalaze se u osnovi provajdera mrežnih usluga.

U MPLS VPN arhitekturi, rubni ruteri prenose informacije o rutiranju korisnika, obezbeđujući optimalno rutiranje za saobraćaj koji pripada korisniku za inter-site saobraćaj. VPN model baziran na MPLS-u također prilagođava korisnike koji koriste preklapajuće adresne prostore, za razliku od tradicionalnog peer-to-peer modela u kojem je optimalno rutiranje korisničkog saobraćaja zahtijevalo da provajder dodijeli IP adrese svakom od svojih korisnika kako bi se izbjeglo preklapanje adresnih prostora. MPLS VPN je implementacija peer-to-peer modela; MPLS VPN okosnica i korisničke stranice razmjenjuju informacije o rutiranju korisnika sloja 3, a podaci se prosljeđuju između korisničkih lokacija koristeći MPLS-omogućenu SP IP okosnicu.

Informacije o rutiranju se prosljeđuju od CE rutera do PE rutera koji koristi ili statičke rute ili usmjerivački protokol kao što je BGP (eng. *Border Gateway Protocol*). PE ruter čuva po lokaciji tabelu prosljeđivanja, također poznatu kao virtualno rutiranje i tabelu prosljeđivanja (VRF). Na PE ruteru, svaki VRF služi interfejsu ili skupu interfejsa koji pripada svakom pojedinačnom VPN-u. Svaki PE ruter je konfigurisan od strane provajdera sa sopstvenim VRF-om, što je jedinstveno. Ruteri unutar MPLS VPN-a mreže ne dijele direktno VRF informacije. (Karuna Jyothi & Reddy, 2023)



Slika 17. Mrežna arhitektura MPLS VPN-a

MPLS VPN je a fleksibilna metoda za transport i rutiranje nekoliko vrsta mrežnog saobraćaja koristeći MPLS okosnicu. MPLS VPN-ovi kombinuju snagu MPLS-a i Border Gateway Protocol-a (BGP) rutiranja. MPLS se koristi za prosljeđivanje paketa preko okosnice mrežnog provajdera, a BGP se koristi za distribuciju ruta preko okosnice.

2.3.3. Protokoli i sigurnost VPN mreže

Prijenos i obrada informacija su podijeljena na kontrolu, podatke i upravljanje tri nivoa u MPLS VPN mrežama. U kontrolnoj ravni, razmjena i obrada informacija o rutiranju je završena i uspostavljene su i održavane VPN tablice rutiranja. U podatkovnoj ravni, implementacija VPN podataka je brzo proslijeđena. Konfiguracija opreme je završena i dostavljaju se odgovarajuće informacije o upravljanju, tj. plan upravljanja. Sigurnosne prijetnje MPLS-a VPN mreže također dolaze sa ova tri nivoa.(Zou et al., 2010b)

- **Peer-Peer VPN -** Peer-Peer (P2P) VPN sistemi koji dozvoljavaju samo *peers*-ima od međusobnog povjerenja da učestvuju. Ovo se može postići korištenjem centralnog servera kao što je konekcijski hub za autentifikaciju klijenata. Alternativno, korisnici mogu razmjenjivati šifre ili kriptografske ključeve sa peers-ima da formiraju decentralizovanu mrežu. Tuneliranje je mrežna tehnologija koja omogućava enkapsulacija jednog tipa

protokola paketa unutar datagrama drugog protokola. Npr. Windows VPN linkovi mogu koristiti Point-to-Point Tunneling Protocol (PPTP) pakete za enkapsulaciju i slati privatni mrežni saobraćaj, kao što je TCP/IP saobraćaj preko javne mreže kao što je internet. VPN server se može konfigurirasi da koristi bilo kojeg Windows ili Dial-In korisnika za udaljenu autentifikaciju Usluga kao provajdera autentifikacije. Ako je Windows odabran kao provajder autentifikacije, korisnik akreditiva koje su poslali korisnici koji pokušavaju VPN veze se provjeravaju korištenjem tipičnih Windows mehanizama provjere autentičnosti i pokušaj povezivanja je ovlašten korištenjem VPN svojstva korisničkog računa klijenta i lokalne daljinske politike pristupa.

- **IPsec protokol** - (Internet Protocol Security) je standard i skup protokola koji obuhvataju mehanizme za zaštitu saobraćaja na nivou trećeg sloja OSI mrežnog modela. IPsec se često koristi za postavljanje VPN-a, a funkcioniše šifriranjem IP paketa, zajedno s autentifikacijom izvora odakle paketi dolaze. IPsec je zapravo skup protokola - AH (*Authentication Header*), ESP (*Encapsulating Security Payload*) i IKE (*Internet Key Exchange*).
- **PPTP** (eng. *Point-to-Point Tunneling Protocol*) - Mrežni protokol koji omogućava siguran prenos 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 se koristi za stvaranje i održavanje tunela unutar PPP paketa. 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
- **SSL protokol -** Transportni protokol koji je razvijen za omogućavanje sigurne i zaštićene komunikacije sugovornika preko javne mreže. Njegova prednosti je u tome što nije potrebna instalacija posebnih programa za spajanje na server, već se komunikacija odvija preko web preglednika na način da je pogodan za povremene korisnike (udaljeni zaposlenici, poslovni partneri, itd.).

Svaki protokol ima svoje prednosti i nedostatke. Za prevazilaženje slabosti i kombinovanje prednosti tradicionalnog VPN-a, MPLS VPN ima svoje karakteristike i funkcije za rješavanje niza problema, uključujući preklapanje adresa, izolaciju slanja podataka, transparentnost, fleksibilnost, visoku efikasnost i jednostavnost upravljanja. Dakle, isplativo je i sigurno rješenje za povezivanje korisnika kompanije na različitim lokacijama širom svijeta.

2.3.4. Ranjivost VPN-a

Ranjivost u MPLS-VPN znači slabosti u MPLS tehnologiji, konfiguracijama, sigurnosnoj politici ili u VPN uređajima kao što su ruteri, prekidači, serveri i zaštitni zidovi. Sigurnosna ranjivost se odnosi na propust u cyber sigurnosti u mreži koji čini sistem otvorenim za napad. Postoje različite vrste sigurnosnih propusta kao što su nedostaci u politici, maliciozni softver, slabosti protokola i ranjivosti hardvera i softvera.

VPN-ovi imaju poznate sigurnosne propuste. Kako studije pokazuju, većina implementacija VPN-a trpi ozbiljne sigurnosnih nedostatake koje maliciozni korisnici lako mogu iskoristiti za omamu, presretanje, modificiranje ili prekid saobraćaj. Neke od ovih ranjivosti su specifične za implementaciju; tj. one predstavljaju nedostatke u specifičnom protokolu implementacije uzrokovane lošim kodiranjem, nepotpunom implementacijom ili lošim izborom implementacije prema uslovima nespecificiranim u standardima. Postoje i druge, ozbiljnije ranjivosti VPN-a u osnovnim protokolima koje se ne mogu izbjeći samo dobrom implementacijom.

U nekim incidentima se može primijetiti kako sofisticirani malver napadi mogu krišom izmijeniti konfiguracije kontrolnog sistema (uključujući i VPN), te oštetiti njegove operacije. Rješenja za ove probleme su ispravne konfiguracije, redovno održavanje i validacija konfiguracije koja se može ispravno izvršiti samo ako administratori u potpunosti razumiju interne detalje protokola.

Postoje i određeni nedostaci politika upravljanja u MPLS VPN-u kao što su nedostatak kontinuiteta i nedostatak pisane politike. Slabosti protokola su one TCP/IP slabosti koje su inherentno učinile HTTP, FTP i ICMP nezaštićenim u MPLS-VPN-u. *Simple Network Management Protocol* (SNMP) i *Simple Mail Transfer Protocol* - SMTP primjeri su TCP/IP protokola koji kada su slabi, prijetnje će ih iskoristiti za napade na mrežu. (Rahimi & Zargham, 2011)

Različite vrste mrežne opreme kao što su routeri, *firewall*, switchevi predstavljaju ranjivost hardvera. Hardverske ranjivosti koje se mogu uočiti u MPLS-VPN mreži su sljedeće:

- zaštita šifrom,
- nedostatak autentifikacije,
- protokol rutiranja i
- rupe u *firewall*-u.

Mrežni uređaji, računarski hardver i mobilni uređaji imaju softver kao zajedničku stvar među njima. Ovaj softver je glavni izvor sigurnosnih problema. U MPLS-VPN-u, softver kao što je softver rutera, web pretraživači, web serveri, Linux/Windows operativni sistem može biti eksploatisan od strane napadača zbog lošeg softvera koji se izvršava preko mreže. Softverske ranjivosti se mogu posmatrati kao nedostaci u dizajnu, implementaciji ili konfiguraciji.

Primjeri tipičnih softverskih ranjivosti su prekoračenje *clipboard*-a, defekt koda ili dizajna i web problem u SQL injekciji.

Sigurnosne prijetnje ranjivosti MPLS-VPN-a javljaju se na tri različita nivoa, a to su nivoi kontrole, podataka i upravljanja. U kontrolnoj ravni, informacije o rutiranju VPN-a koje prolaze kroz P i PE rutere imaju različite napade kao što su izmjena informacija o rutiranju i uskraćivanje usluge, dok se na nivou podatkovne ravni napad obično javlja kao lažiranje IP izvorne adrese, otmica sesije protokola, u vidu trojanaca i reprodukcije legitimnog MPLS paketa itd. Ovaj napad se obično dešava između VPN Customer Edge (CE) i Provider Edge rutera. Sigurnosne prijetnje upravljačkog plana su napad na mrežne uređaje preko administrativnog interfejsa. (Ogbu, 2018)

2.4. Upravljanje sigurnošću ISP-a

Mreža je jedan od najvažnijih osnovnih resursa koje svaka veća institucija treba da ima. Danas mreže igraju veoma važnu ulogu u svakoj organizaciji. Sa široko rasprostranjenom distribuiranom implementacijom, upravljanje sigurnošću mreže postaje veoma složeno, posebno sa stanovišta ISP-a. ISP-ovi su inherentno ranjiviji jer moraju ponuditi mnoštvo javnih usluga, kako za svoje klijente, tako i u svoje ime. Efikasno upravljanje mrežom i sigurnošću treba implementirati uzimajući u obzir nedostatak bandwidth-a i dostupnost računarskih resursa na čvorovima. Upravljanje sigurnošću ima značajnu ulogu jer se sva komunikacija odvija preko nesigurnog Interneta.

2.4.1. Arhitektura

Svaki LSP ima dva servera koja se već koriste za pružanje svih usluge za pretplatnike - Glavni Internet server (eng. *Main Internet Server* - MIS) i redundantni Internet server (eng. *Redundant*

Internet Server - RIS). Sistem za otkrivanje upada u mrežu (NIDS) i sistem upravljanja konfiguracijom rade na tim serverima, te pružaju različite usluge:

- Proxy za WWW pristup
- email
- DNS
- Web hosting
- Sve ostale konekcije na Internet se obezbjeđuju putem prevođenja mrežnih adresa (eng. *Network Address Translation* - NAT), te je bitno zaštititi ove servere od napada sa Interneta i sa pretplatničke mreže.

Na osnovu glavnih arhitektonskih koncepata navedenih, prije nego što ISP-ovi osmisle mrežnu strukturu koja se sastoji od nekoliko blokova ili slojeva mreže. Najčešći od njih – slojevi jezgre ili agregacije se mogu pronaći u drugim područjima kao što su Enterprise ili Datacenter Networks.

Usluge i uređaji mogu biti različiti, ali princip agregacije linkova za brzu razmjenu podataka preko jezgre bi svuda bio isti.

2.4.2. Sistem za upravljanje konfiguracijom

U toku su brojna istraživanja u oblasti daljinskog upravljanja konfiguracijom računarskih sistema. Postoje različite vrste ovakvih sistema, a neki od njih su ManageEngine, WinRM, CFEngine itd.

Proces upravljanja konfiguracijom softvera (eng. *Software Configuration Management* - SCM) praktičari smatraju najboljim rješenjem za rukovanje promjenama u softverskim projektima. On identifikuje funkcionalne i fizičke atribute softvera u različitim vremenskim trenucima i vrši sistematsku kontrolu promjena identifikovanih atributa u cilju održavanja integriteta i praćenja softvera tokom životnog ciklusa razvoja softvera.

SCM proces dalje definira potrebu za praćenjem promjena i mogućnost da se potvrdi da konačni isporučeni softver ima sva planirana poboljšanja koja bi trebala biti uključena u izdanje. Identifikuje četiri procedure koje se moraju definisati za svaki softverski projekat kako bi se osiguralo da se implementira dobar SCM proces.

One su:

- Identifikacija konfiguracije
- Kontrola konfiguracije
- Obračun statusa konfiguracije
- Revizije konfiguracije ('Configuration Management (Wikipedia)', 2023b)

Daljinsko upravljanje konfiguracijom omogućava izvođenje promjena konfiguracije sistema kroz mrežu, bez potrebe za pristupom konzoli sistema koji se konfigurira. Tehničar također može raditi na nečijem računaru na daljinu bez potrebe da bude fizički prisutan na lokaciji. Ovo se često radi instaliranjem softvera za daljinsko upravljanje ili servisa koji omogućava komunikaciju dva povezana uređaja.

Ponekad se za ovu funkciju koriste posebni protokoli. Daljinsko upravljanje konfiguracijom može se koristiti za:

- konfiguraciju
- dijagnosticiranje problema/rješavanje problema
- upravljanje patch-evima
- praćenje

Alati za daljinsko upravljanje konfiguracijom obično upozoravaju korisnika kada neko pokušava da se poveže sa računarom. Nadalje, kako bi ograničili zlonamjernu aktivnost, korisnik ili administrator obično mogu odrediti nivo dozvole ili kontrole dodijeljene softveru. S obzirom da su hakeri koristili alate i usluge za daljinsko upravljanje konfiguracijom da bi dobili pristup računarima, dobre sigurnosne prakse su imperativ kada se koristi alat za daljinsko upravljanje konfiguracijom. Takva uslugu treba biti diskonektovana ili isključena kada se ne koristi.

2.4.3. Parametri performansi

Faktori performansi koji će najviše uticati na sisteme za upravljanje konfiguracijom su:

- **Iskorišteni *bandwidth***:

Bandwidth je mjera količine podataka koju medij može prenijeti u datom vremenskom periodu. Svaki prijenosni medij ima različit *bandwidth*.

- **Latencija**:

Latencija mreže je mjera koliko je vremena potrebno poruci da putuje s jednog uređaja na drugi preko mreže. Mreža s niskom latencijom doživljava malo kašnjenja u prijenosu, dok mreža s velikom latencijom doživljava mnogo kašnjenja. Što je više kašnjenja, duže traje prijenos podataka preko mreže.

S toga je važno minimizirati vrijeme potrebno za bilo koju kontrolnu akciju koja se pokreće. Može se raditi automatizirano ili uz pomoć operatera. U slučaju radnji uz pomoć operatera, potrebno je osigurati interfejs kako bi se operaterima olakšao posao.

- **Opterećenje na serverima na LSP-u:**

Serveri na LSP-u već pružaju razne usluge korisnicima. Svaki sistem upravljanja je dodatak koji treba da ne koristi previše raspoloživih resursa.

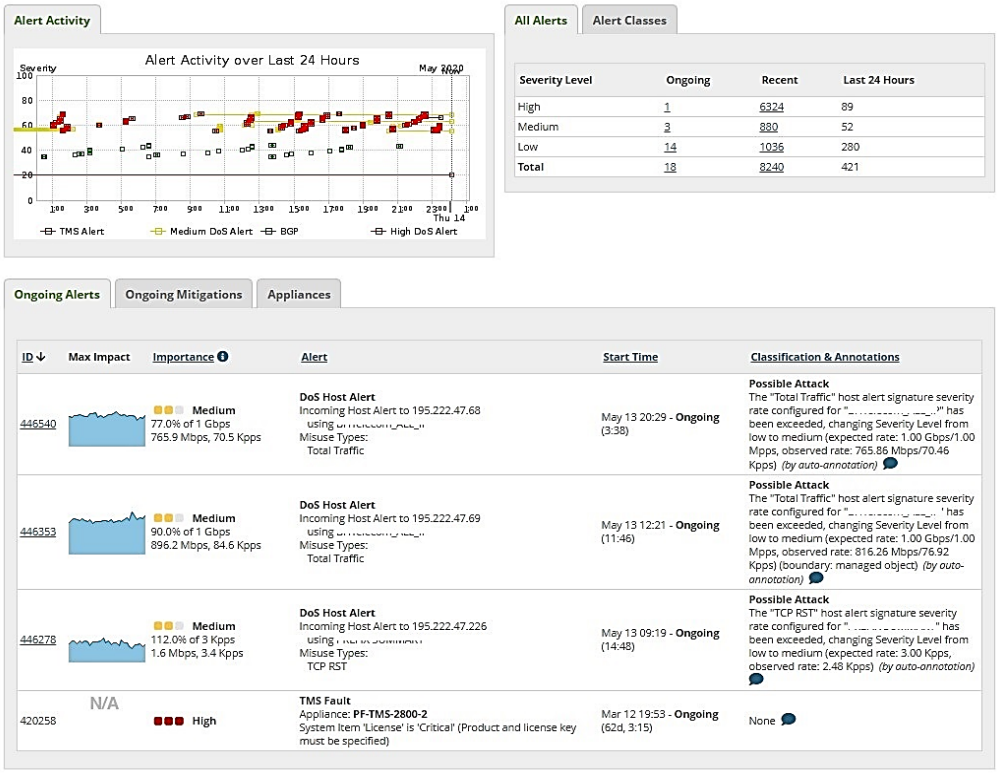
Način na koji se izvodi detekcija upada zasnovana na hostu, pravilima o NIDS-u, mehanizam izvještavanja, itd. igraju ulogu u tome koliko dobro je razvijen sistem.

2.4.4. Obavještavanje o ranjivosti i prijavljivanje incidenata

Sigurnosna ranjivost se odnosi na propust u cyber sigurnosti u mreži koji čini sistem otvorenim za napad. Postoje različite vrste sigurnosnih propusta kao što su nedostaci u politici, maliciozni softver, slabosti protokola i ranjivosti hardvera i softvera. Za nadzor sistema upravljanja sigurnošću, potrebno je koristiti standardne formate izvještavanja, kako za statističke podatke, tako i za ažuriranja u realnom vremenu. Za usklađenost sa standardima i laku integraciju sa bilo kojim NMS-om višeg nivoa, podrazumijevani format mora biti *Intrusion Detection Messages Exchang Format* (IDMEF) koji je nacrt IETF-a. Međutim, za izvještavanje u realnom vremenu, SNMP (eng. *Simple Network Management Protocol*) zamke su mnogo bolje. IDMEF je mehanizam za izvještavanje zasnovan na XML-u, pogodan za prenos statističkih informacija, dok se SNMP koristi uglavnom za upravljanje mrežnim uređajima u TCP/IP mrežama .

3. Studija slučaja DDoS napada na komponente mreže ISP-a

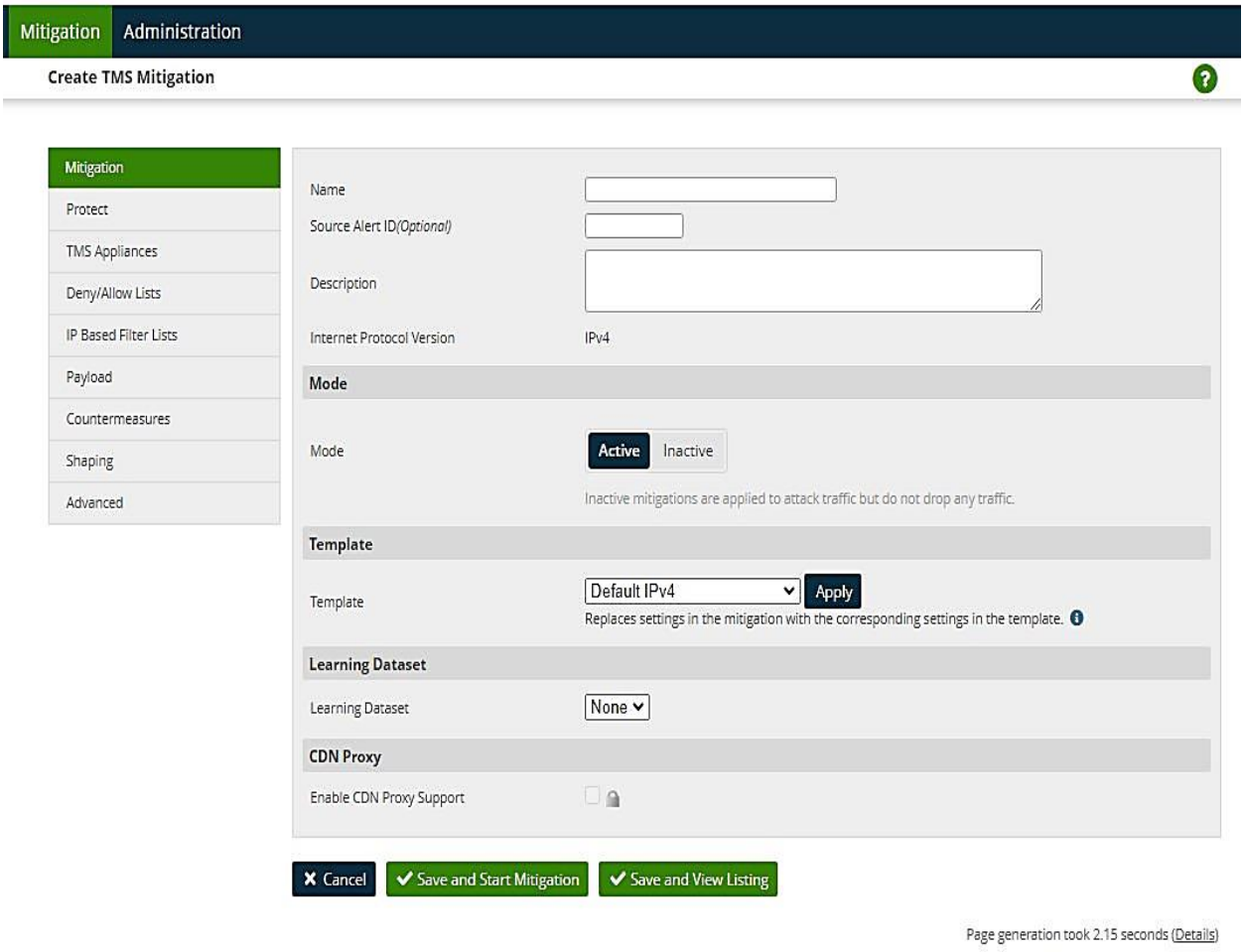
Arbor DDoS Mitigation Platform predstavlja web baziranu platformu koji se koristi kao adekvatna zaštita od DDOS napada. Kao takva postoji od 1999. godine i od tad pruža adekvatnu zaštitu od DDOS napada. Ovaj vid DDOS zaštite omogućava neometan rad internet saobraćaja, kako korisnika, tako i ostalih komponenti, te servisa koji su vezi sa IPMPLS opremom. Primjena ovakve platforme je od velikog značaja za svakog ISP-a kojem je u cilju kvalitetno pružanje usluge. Nekorištenje ovakvog vida zaštite dovodi do problema na bilo kojem nivou u mreži. Isti se manifestuje kao prekid rada internet saobraćaja ili njegovo znatno otežano odvijanje, kašnjenje, gubitak paketa i sl. Ova studija slučaja će pokazati primjenu Arbor Netscape platforme iz ličnog iskustva, te rješavnje poteškoća u toku DDoS napada. U ovom dijelu ćemo pokazati konkretan izgled, primjer i funkciju Arbor DDoS Mitigation platforme. DDoS zaštita se adekvatno odvija kroz niz predhodno postavljenih pravila (rulova), te nakon izvjesnog vremena dobivamo rezultat kao na sljedećoj slici:



Slika 18. Stanje i nivo napada u roku 24h

Slika prikazuje sumirano stanje u protekla 24h i sam uticaj na mrežu, te stanje i nivo napada koji su se odvijali u proteklom periodu. U zavisnosti od težine, napadi mogu da budu low, medium i high, što pokazuje ozbiljnost i prijetnju na određene dijelove u mreži.

Kako bismo imali takav izvještaj, potrebno je napraviti određena pravila koja dobijamo kroz određene korake u meniu:

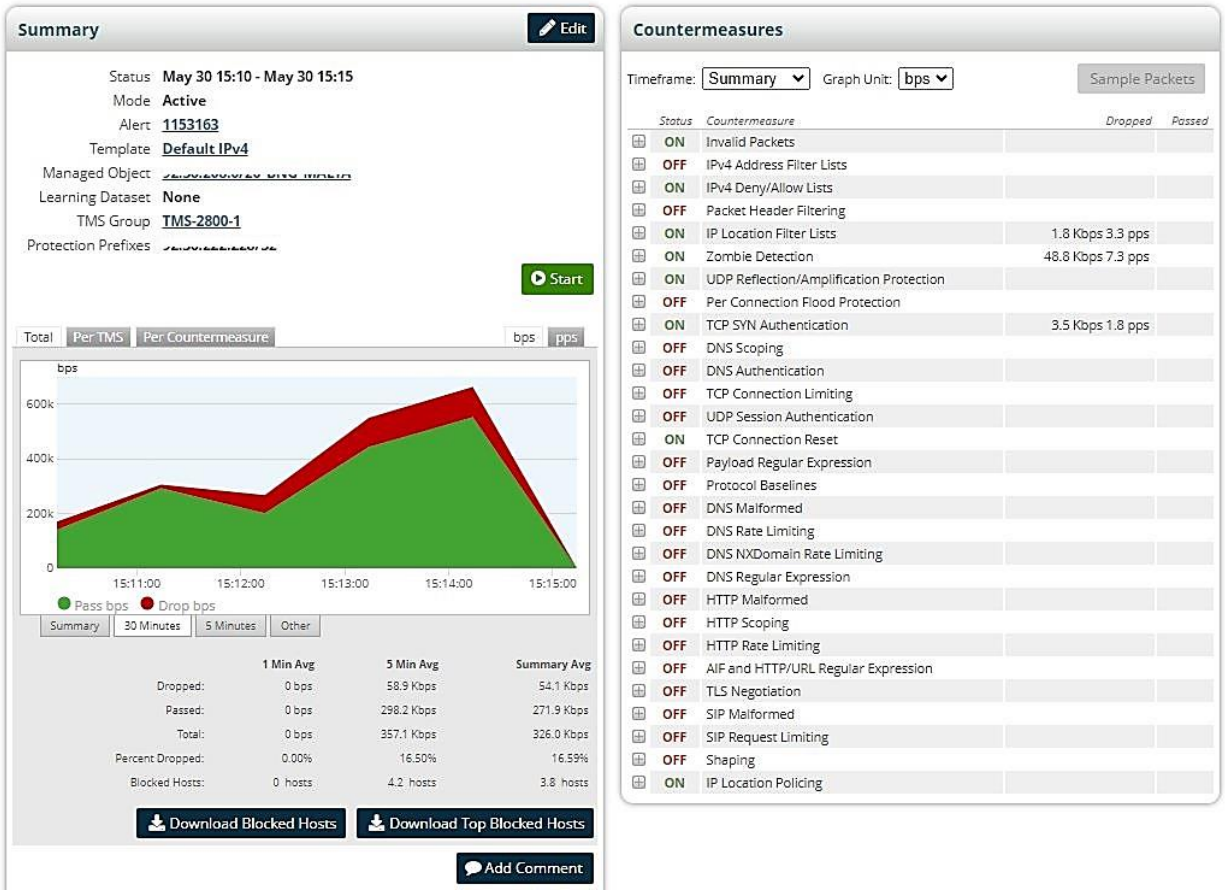


Slika 19. Kreiranje pravila za mitigaciju

Nakon setovanja pravila, imena, IP adrese i protokola, uz ostale pojedinosti, dobijamo niz podešenih oblika zašite koji se po potrebi startuju, ako se desi da sama platforma ne reaguje (predhotno podešena auto mitigacija). Takav slučaj se rijetko dešava, međutim vrlo je korisno imati spreman template koji se startuje u pravom momentu ili edituje, kako bi zaštita bila primjenjena

što je prije moguće. Na slici vidimo „save and start mitigation“, čime se zaštita aplicira na već postavljene podatke, te se spašava kao urnek. Zaduženi uposlenik za monitoring mreže i servisa mora biti na oprezu u ovakvim situacijama. Najbitnija je promtna reakcija kako bi se poslovanje nastavilo.

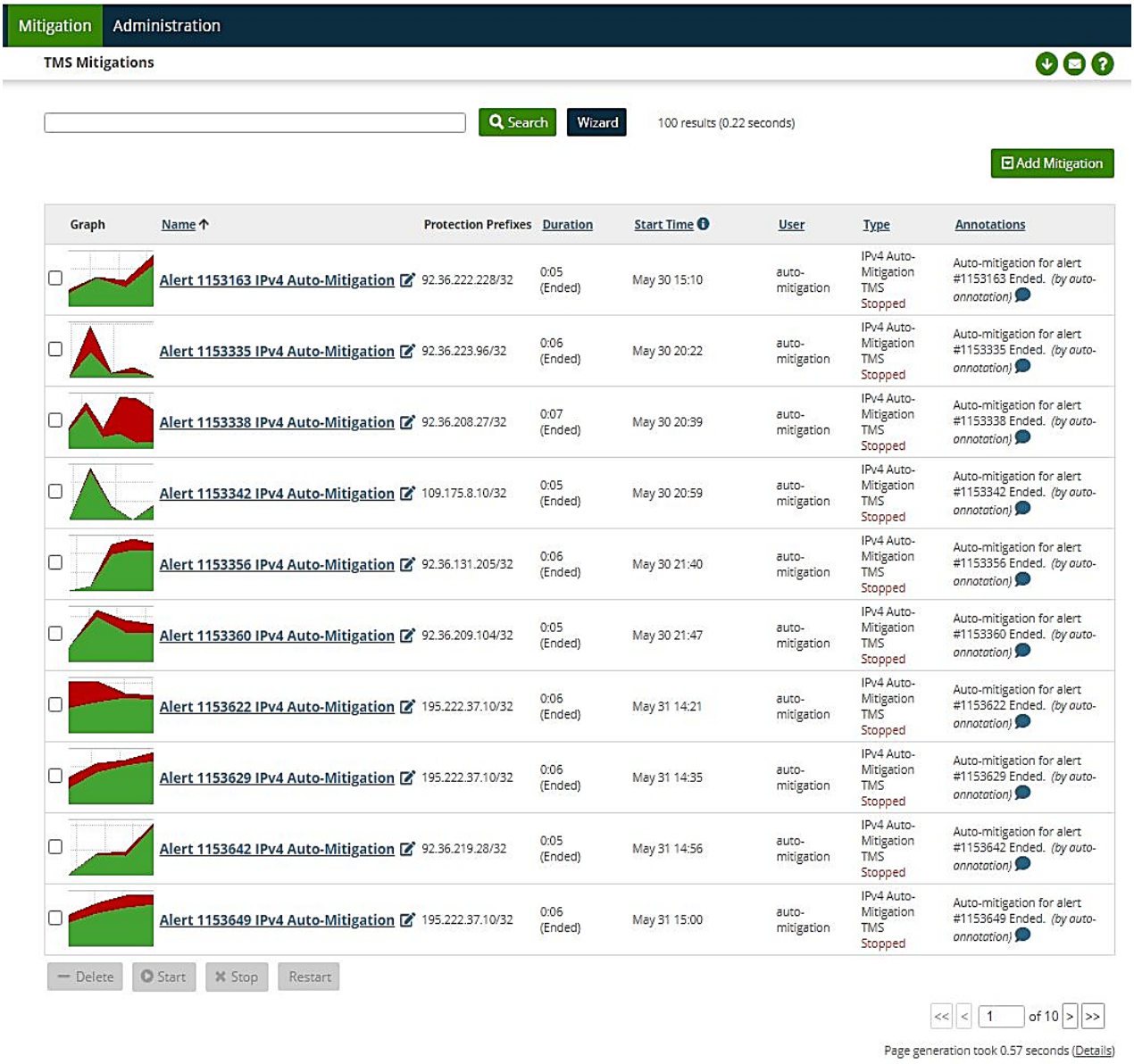
Nakon unosa dobivamo ovaj izgled:



Slika 20. Arbor template

Na slici iznad vidimo pripremljen template za napad koji se već dogodio. Kada imamo ovakav vid pripremljenog template-a dovoljno je samo kliknuti na start gdje se automatski prekida napad na određenu IP adresu.

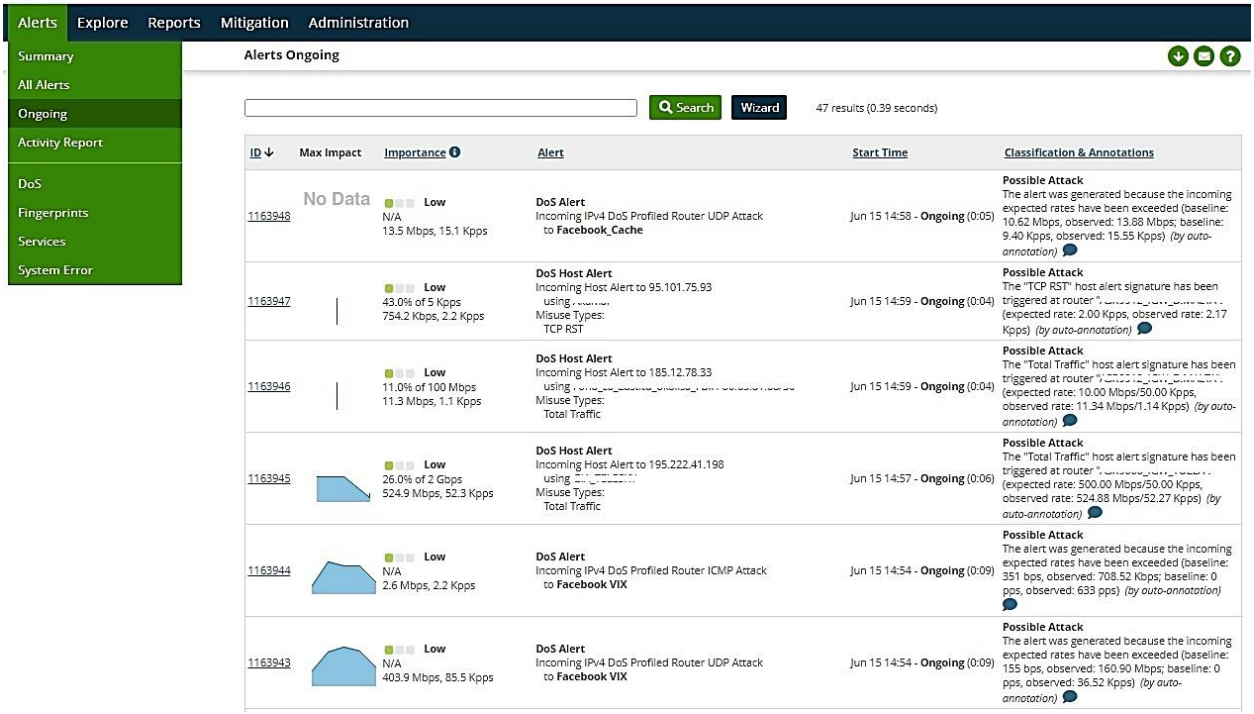
Nakon dužeg vremena korištenja, lista pripremljena za djelovanje bi izgledala kao na slici ispod:



Slika 21. Unaprijed pripremljena zaštita

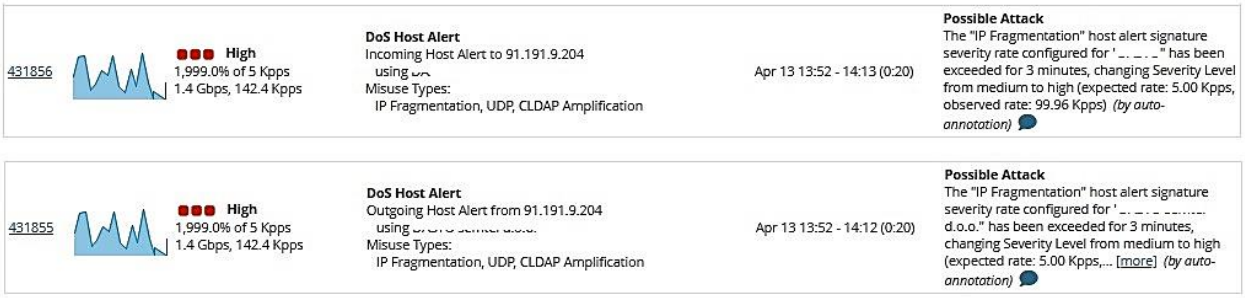
Uz monitoring IPMPLS opreme potrebno je pratiti i sam rad Arbor platforme, gdje blagovremeno možemo predvidjeti određene napade koji mogu utjecati na rad mreže i servisa. Ovaj dio se odnosi na sam pregled nivoa, kapaciteta napada na koje treba obratiti pažnju.

Taj dio možemo da vidimo na dijelu „ongoing“.



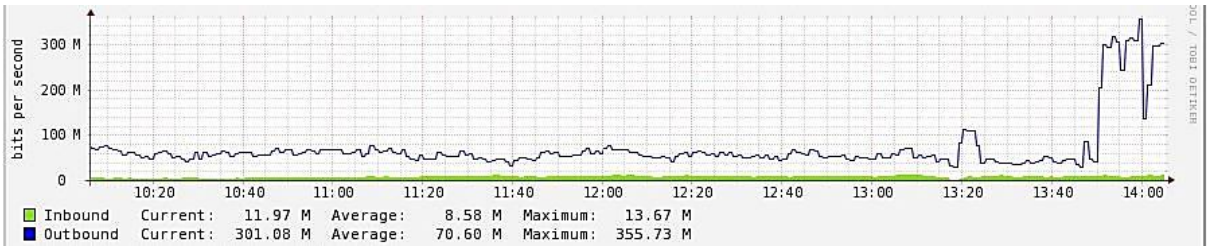
Slika 22. Prikaz „low“ napada na mrežu

Na gore prikazanoj slici vidimo određene napade koji su slabog kapaciteta pa su isti deklarisani kao „low“ što ne predstavlja opasnost za rad mreže i servisa, ali treba obratiti pažnju te preventivno djelovati (napraviti pomenuti urnek), kako bi se reakcija maksimalno ubrzala. Takva situacija je zadovoljavajuća, medjutim dešavaju se i napadi znatno većeg kapaciteta koji onesposobe rad linka u potpunosti, takav napad možemo da prikažemo na slici ispod:



Slika 23. Prikaz „high“ napada

Slika prikazuje napad od 1.4Gbps što je dovelo do prestanka rada linka iz razloga iskorištenja max kapaciteta linka, svi podatci preko se gube, link je beskoristan.



Slika 24. Praćenje rada MPLS opreme putem grafa

U ovim situacijama od velikog značaja je osoba koja prati rad MPLS opreme na gore prikazanom grafu, a uz sam monitoring koristi i Arbor platformu. Ova kombinacija omogućava brzu reakciju i otklanjanje problema na mreži ili kod targetiranog korisnika.

Kroz dugogodišnje iskustvo u monitoringu IPMPLS mreže mogu konstatovati da sigurnost igra veliku ulogu u neometanom radu mreže. Ako u nekom slučaju ne bi imali adekvatnu zaštitu kao što je Arbor platforma, to bi značilo prekid poslovanja određenog dijela ISP-a. Svaki ozbiljan ISP ima određen broj ugovora koji zahtijeva autonomnosti usluge (SLA ugovori), u nekim slučajevima i 99.9%, zavisno od ugovora. Svaki propust bi značio finansijske gubitke, kako korisniku, tako i ISP-u, te je samim tim uloga zaštite itekako vezana i za ekonomsko poslovanje ISP-a.

Gore navedenim možemo povući jednu paralelu između sigurnosti i profita. Potencijalni klijenti, koji su informisani da postoji adekvatna usluga DDoS zaštite od strane ISP-a će možda upravo to uzeti kao odlučujući faktor u izabiru usluga ISP-a. Jednostavan primjer su brokerske kuće – takav klijent jednostavno ima potrebu od 100% autonomnosti usluge, u protivnom podnosi velike finansijske gubitke u poslovanju, ako se napad desi u trenutku određenih transakcija, te kao posljedicu ima zagušenje, neupotrebljivost internet konekcije, pristup berzi se blokira, nastaje veliki problem, nezadovoljstvo, panika, gubitak novca i klijenata.

Mnoge velike kompanije ne mogu sebi priuštiti propust nekorištenja DDoS zaštite. Banke, državne institucije, vojska, avio prevoz i kontrola, jednostavno moraju imati vid zaštite kako bi zaštitili svoje poslovanje i klijente. U nekim slučajevima su i od životnog značaja. Zamislite propust kontrolora leta koji je onemogućen da koristi monitoring letova, a isti se oslanja na IP saobraćaj - to bi bilo nedopustivo

4. Zaključak

Sigurnost podataka je od ključne važnosti u vremenu kada napadi putem interneta postaju sve napredniji i sofisticiraniji. Međutim, za adekvatno funkcionisanje mreže od izuzetnog značaja su i brzina prenosa podataka kroz nju, te njena pouzdanost koja se osigurava ugovorima o nivou usluga i pruža korisnicima garanciju da će njihovo poslovanje biti adekvatno održavano i kontinuirano. Uzimajući u vid brojne faktore, MPLS mreža se pokazala kao najbolji izbor kod mnogih provajdera internetskih usluga, te se na njoj baziraju brojni servisi, što zahtijeva adekvatno održavanje mreže i obezbjeđenje njene sigurnosti. Neki od najčešćih napada su DDoS napadi kojima se u radu dodatno posvetila pažnja i pokazalo njihovo djelovanje na osnovu primjera iz prakse. Kroz rad su također predstavljene i ostale vrste napada, te alati za otkrivanje i prevenciju mrežnih napada, te je objašnjena primjena VPN-a. Nestabilna mreža može dovesti do značajnih finansijskih gubitaka kako za korisnike, tako i za provajdere usluga, te se iz tog razloga sigurnost može posmatrati kao jedan od vitalnih parametara u poslovanju i korisnika i ISP-a.

Sigurnost je također i jedan od ključnih faktora pri izboru provajdera usluga, te kao takva predstavlja temeljnu vrijednost u radu MPLS mreže. Od ključnog značaja za osiguranje visokog nivoa usluge i zadovoljavanja potreba korisnika je omogućiti neometan rad mreže, što se postiže adekvatnim izborom opreme i osiguravanja da ta oprema radi kako je namijenjeno, te da je zaštićena od brojnih vrsta napada koji potencijalno mogu usporiti ili onemogućiti njen rad. Loša sigurnost mreže bi značila i otežavanje poslovanja korisnika, te značajne finansijske gubitke, a time bi dovela i do gubitka korisnika, jer među osnovne prioritete korisnika svakako spada visoka dostupnost usluge. U vremenu kada se dešava sve više napada koji ugrožavaju integritet poslovanja, ISP koji pruža zadovoljavajuće nivoe usluge i sigurnosti podataka je imperativ.

Zajednička karakteristika savremenih mreža, internet provajdera i velikih kompanija je stalno rastuća količina saobraćaja i raznih vrsta podataka koji se prenose mrežom. Integracijom usluga povećala se gustoća saobraćaja, a mrežom se prenose podaci koji se generišu na raznim uređajima, te zahtijevaju da odvijanje prenosa bude u realnom vremenu. Upotrebom MPLS-a povećava se iskoristivost linkova i izbjegavaju zagušenja u mreži, što predstavlja glavnu prednost u odnosu na konvencionalne protokole u upotrebi. Prijetnje kontroli MPLS-a i signalnim protokolima dolaze uglavnom iz dvije vrste izvora - eksternih i internih.

Mreža je jedan od najvažnijih osnovnih resursa koje svaka veća institucija treba da ima. Danas mreže igraju veoma važnu ulogu u svakoj organizaciji. Sa široko rasprostranjenom distribuiranom implementacijom, upravljanje sigurnošću mreže postaje veoma složeno, posebno sa stanovišta ISP-a. ISP-ovi su znatno osjetljiviji jer moraju ponuditi mnoštvo javnih usluga, kako za svoje klijente, tako i u svoje ime. Mnoge velike kompanije ne mogu sebi priuštiti propust nekorištenja DDoS zaštite. Banke, državne institucije, vojska, avio prevoz i kontrola, jednostavno moraju imati vid zaštite kako bi zaštitili svoje poslovanje i klijente. Potencijalni klijenti, koji su informisani da postoji adekvatna usluga DDoS zaštite od strane ISP-a će možda upravo to uzeti kao odlučujući faktor u izabiru usluga ISP-a.

Upotrebom odgovarajućih načina nadzora opreme i njene zaštite osigurava se neometan rad mreže i omogućava kontinuiran prenos paketa putem signalnih protokola, što obezbjeđuje visoku stabilnost rada MPLS mreže i zadovoljavanje SLA ugovora, a time i zadovoljstvo korisnika i njihovo zadržavanje. Na osnovu istraživanja provedenog u ovom radu možemo zaključiti da je sigurnost jedan od odlučujućih faktora kod izbora ISP-a, te da je njena uloga od ključnog značaja za uspješno poslovanje. Kroz primjer iz ličnog iskustva prikazani su neki od alata za praćenje rada mreže, njeno održavanje, praćenje napada, organizaciju za slučajeve kada se napad desi i sl. Kao što je kroz rad objašnjeno, detekcija i prevencija napada su od najvećeg značaja, te je zato bitno imati odgovarajuće alate za praćenje stanja mreže. Uspješno spriječen napad će znatno smanjiti vrijeme potrebno za oporavak mreže, te očuvati kontinuitet rada mreže, čime se postiže veći stepen zadovoljstva korisnika usluga i bolji odnos sa istima. Na osnovu analize provedene u radu može se zaključiti da za osiguranje stabilnosti MPLS mreže i njen kontinuiran rad potrebno je posvetiti posebnu pažnju sigurnosti i adekvatnoj zaštiti mreže.

Kroz dugogodišnje iskustvo u monitoringu IPMPLS mreže mogu konstatovati da sigurnost igra veliku ulogu u neometanom radu mreže. Ako u nekom slučaju ne bi imali adekvatnu zaštitu kao što je Arbor platforma, to bi značilo prekid poslovanja određenog dijela ISP-a. Svaki ozbiljan ISP ima određen broj ugovora koji zahtijeva autonomnosti usluge (SLA ugovori), u nekim slučajevima i 99.9%, zavisno od ugovora. Svaki propust bi značio finansijske gubitke, kako korisniku, tako i ISP-u, te je samim tim uloga zaštite itekako vezana i za ekonomsko poslovanje ISP-a.

5. Reference

Alouneh, S. & Abed, S.' E. (2010) *Fault tolerance and security issues in MPLS networks 4D Entertainment Machine View project Computer Aided Diagnosis Systems to Detect Breast Cancer by Segmentation-based and Deep Learning-based Techniques using Mammogram View project Fault Tolerance and Security Issues in MPLS Networks*. 134–138. https://www.researchgate.net/publication/228850104.

Aslam, M.N. & Aziz, Y. (2008) *Traffic Engineering with Multi-Protocol Label Switching Performance Comparison with IP networks*. Master Thesis. Ronneby, Blekinge Institute of Technology. www.bth.se/tek.

Bensalah, F., Kamoun, N. El & Baddi, Y. (2019) A novel approach for improving MPLS vpn security by adopting the software defined network paradigm. In: *Procedia Computer Science*. 2019 Elsevier B.V. pp. 831–836. doi:10.1016/j.procs.2019.11.003.

Cavendish Dirceu, Hiroshi Ohta & Hari Rakotoranto (2004) Operation, Administration, and Maintenance in MPLS Networks. *IEEE Communications Magazine*.pp.91–99. http://www.hit.bme.hu/~jakab/edu/litr/MPLS_OAM/01341266.pdf.

Čisar, P. (2013) *Sistem za detekciju upada u mrežnu infrastrukturu*. https://jakov.kpu.edu.rs/bitstream/id/2634/503.pdf.

Daugherty, B. & Metz, C. (2005) *On the Wire Multiprotocol Label Switching and IP, Part I: MPLS VPNs over IP Tunnels*. www.computer.org/internet/.

Do, T. Van, Van Do, T., Papp, D., Chakka, R., Mai, X. & Truong, T. (2009) *A Performance Model of MPLS Multipath Routing with Failures and Repairs of the LSPs*. https://www.researchgate.net/publication/250058345.

Elleithy, K.M., Blagovic, D., Cheng, W.K., Sideleau, P., Et, A." & Cheng, W. (2005) Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Journal of Systemics, Cybernetics, and Informatics*.3. http://digitalcommons.sacredheart.edu/computersci_fac.

Faletar, D. (2020) *Nadzor MPLS mreže alternativnog telekomunikacijskog operatora*. Doctoral dissertation. Zagreb, Faculty of Transport and Traffic Sciences. https://urn.nsk.hr/urn:nbn:hr:119:120712.

Ghani-Ur-Rehman, Shad Muhammad, Ashraf Zia, M. Asif & Saif Rehman (2014) *Scalability Analysis Of MPLS Label Distribution Protocols RSVP*. http://vfast.org/journals/index.php/VTCS@.

Hodžić, H. (n.d.) *MPLS TE mehanizmi u IP mrežama*.

Jahan, S., Rahman, M.S. & Saha, S. (2017) Application specific tunneling protocol selection for Virtual Private Networks. In: *Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017*. 23 March 2017 Institute of Electrical and Electronics Engineers Inc. pp. 39–44. doi:10.1109/NSysS.2017.7885799.

Karuna Jyothi, K. & Reddy, B.I. (2023) *CSEIT1835225 | Study on Virtual Private Network (VPN), VPN's Protocols And Security Study on Virtual Private Network (VPN), VPN's Protocols And Security*. https://www.researchgate.net/publication/368831275.

Kaur, D. & Dinesh Kumar, E. (n.d.) Comparative Analysis of MPLS Signaling Protocols. *International Journal of Computer Science Trends and Technology*. 3.

Kraljević, M. (2021) *Virtualne privatne mreže*. Doctoral dissertation. Split, University of Split. https://urn.nsk.hr/urn:nbn:hr:228:534506.

Lee, H., Hwang, J., Kang, B. & Jun, K. (2000) *End-To-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5c92009ae41b8892ba123e22da0a0406b12a1ef7.

Liao, H.J., Richard Lin, C.H., Lin, Y.C. & Tung, K.Y. (2013) Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*.36 (1) pp.16–24. doi:10.1016/j.jnca.2012.09.004.

Mahjabin, T., Xiao, Y., Sun, G. & Jiang, W. (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*. 13 (12). doi:10.1177/1550147717741463.

Mirjana D. Stojanović & Vladanka S. Aćimović-Raspopović (2012) *Savremene IP mreže: arhitekture, tehnologije i protokoli*. first. Beograd, Akademska misao.

Ogbu, M.N.C. (2018) Security Vulnerability On Multi-Protocol Label Switching In Virtual Private Network. *International Journal of Engineering, Science and Mathematics*. 7. http://www.ijesm.co.in,.

Palmieri, F. & Fiore, U. (2007a) *Enhanced security strategies for MPLS signaling*.

Palmieri, F. & Fiore, U. (2007b) *Enhanced security strategies for MPLS signaling*.

Pan Ping, George Swallow & Atlas Alia (2005) *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. https://www.rfc-editor.org/rfc/rfc4090.html.

Petrović, K. (2009) *Ispitivanje sigurnosti mrežne opreme na uobičajene mrežne napade*. Zagreb, Fakultet elektronike i računarstva.

Polkowski, M. & Laskowski, D. (2015) Analiza Odpornosci MPLS VPN Na Narazenia Zewnetrzne. *Journal of Konbin*. 35 (1), 63–72. doi:10.1515/jok-2015-0040.

Rahimi, S. & Zargham, M. (2011) Quantitative Evaluation of Virtual Private Networks and its Implications for Communication Security in Industrial Protocols. *International Journal of Computational Intelligence Theory and Practice*.6 (1).

Ridwan, M.A., Radzi, N.A.M., Wan Ahmad, W.S.H.M., Abdullah, F., Jamaludin, M.Z. & Zakaria, M.N. (2020) Recent trends in MPLS networks: Technologies, applications and challenges. *IET Communications*.14 (2) pp.177–185. doi:10.1049/iet-com.2018.6129.

Saini, J.R. & Pandey, A. (2014) Attacks & Defense Mechanisms for TCP/ IP Based Protocols. *International Journal of Engineering Innovation & Research*.3 (1). https://www.researchgate.net/publication/260877113.

Simatimbe, C.K. & Charles Lubobya, S. (2020a) Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network. *Journal of Computer and Communications*. 8, 100–108. doi:10.4236/jcc.2020.89009.

Simatimbe, C.K. & Charles Lubobya, S. (2020b) Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network. *Journal of Computer and Communications*. 8, 100–108. doi:10.4236/jcc.2020.89009.

Tschofenig, H. & Graveman Richard (2005) *RSVP Security Properties*. https://www.rfc-editor.org/rfc/rfc4230.

Wikipedia (2023a) *Comparison with TCP/IP model*. 2023. https://en.wikipedia.org/wiki/OSI_model#Comparison_with_TCP/IP_model [Accessed: 16 April 2023].

Wikipedia (2023b) *Configuration management*. 2023. https://en.wikipedia.org/wiki/Configuration_management [Accessed: 11 May 2023].

Wikipedia (2023c) *'Constraint-based Routing Label Distribution Protocol'*. 2023. Constraint-based Routing Label Distribution Protocol [Accessed: 28 March 2023].

Wikipedia (2022) *MPLS (telekomunikacije)*. 2022. MPLS (telekomunikacije) [Accessed: 22 April 2023].

Wikipedia (2023d) *MPLS VPN*. 2023. https://en.wikipedia.org/wiki/MPLS_VPN [Accessed: 27 April 2023].

Wikipedia (2023e) *OSI model*. 2023. https://en.wikipedia.org/wiki/OSI_model [Accessed: 21 April 2023].

Zou, Y., Henan-Ligong-Daxue Jiaozuo, ISCSCT (3 2010.08.14-15 Jiaozuo) & International Symposium Computer Science and Computational Technology (3 2010.08.14-15 Jiaozuo) (2010a) *Proceedings : 14-15 Aug. 2010, Jiaozuo, China*. Academy Publ.

Zou, Y., Henan-Ligong-Daxue Jiaozuo, ISCSCT (3 2010.08.14-15 Jiaozuo) & International Symposium Computer Science and Computational Technology (3 2010.08.14-15 Jiaozuo) (2010b) *Proceedings : 14-15 Aug. 2010, Jiaozuo, China*. Academy Publ.

6. Dodaci

7. Akronimi

AAA	*Authentication, Authorization, Accounting*
AD	*Anomaly-based Detection*
AH	*Authentication Header*
ARP	*Address Resolution Protocol*
ASCII	*American Standard Code for Information Interchange*
ATM	*Asynchronous Transfer Mode*
BGP	*Border Gateway Protocol*
BNG	*Border Gateway Protocol*
BoS	*Bottom of Stack*
CE	*Customer Edge*
CR-LDP	*Constrained Routing Label Distribution Protocol*
CR-LSP	*Constraint based Routed Label Distribution Protocol*
DC	*Data Center*
DCI	*Data Center Interconnect*
DDOS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DOS	*Denial of Service*
DSL	*Digital subscriber line*
DWDM	*Dense Wavelength Division Multiplexing*
EGP	*Exterior Gateway Protocol*
EPC	*Evolved Packet Core*
ERP	*Ethernet Ring Protection*
ESP	*Encapsulating Security Payload*
EXP	*Experimental use*
FEC	*Forwarding Equivalence Class*
FHRP	*First Hop Redundancy Protocol*
HA	*High Availability*
HFC	*Hybrid fiber-coaxial*
HIDS	*Host-based IDS - HIDS*
HMAC-SHA	*Hash-based Message Authentication Code -Secure Hash Algorithm*
HSRP	*Hot Standby Router Protocol*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
IGP	*Interior Gateway Protocol*
IKE	*Internet Key Exchange*

ILM	*Incoming Label Map*
IP	*Internet Protocol*
IPS	*Intrusion Prevention system*
ISO	*International Standardization Organization*
ISP	*Internet Service Provider*
LDP	*Label Distribution Protocols*
LER	*Label Edge Router*
LIB	*Label Information Base*
LSP	*Label Switched Path*
LSPID	*Local Service Provider ID*
LSR	*Label Switched Router*
MIDS	*Mixed IDS*
MIS	*Master Internet Server*
MPLS	*Master Internet Server*
MSTP	*Multiple Scanning Tree Protocol*
NAT	*Network Address Translation*
NBA	*Network Behavior Analysis*
NHLFE	*The Next Hop Label Forwarding Entry*
NIDS	*Network-based IDS*
OAM	*Organization, Administration, Maintenance*
OSI	*The Open Systems Interconnection model*
P2P	*Peer-Peer*
PE	*Provide Edge*
PON	*Passive optical network*
POP	*point of presence*
PPTP	*Point-to-Point Tunneling Protocol*
PTP	*Point to Point*
RARP	*Reverse Address Resolution Protocol*
RIS	*Redundant Internet Server*
ROADM	*Reconfigurable optical add-drop multiplexer*
RSVP	*Resource Reservation Protocol*
SD	*Signature-based Detection*
SDH	*Synchronous Digital Hierarchy*
SHA	*Secure Hash Algorithm*
SLA	*Service Level Agreements*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SP	*Service Provider*
SPA	*Stateful Protocol Analysis*
SPF	*Shortest Path First*
SSH	*Secure Shell*

TAP	*Test Access Port*
TCP SYN	*Transmission Control Protocol Synchronize*
TE	*Traffic Engineering*
TLV	*type-length-value*
TTL	*Time To Live*
UDP	*User Datagram Protocol*
VLL	*Virtual leased line*
VPLS	*Virtual Private LAN services*
VPN	*Virtual Private Network*
VPRN	*Virtual Private Routed Network*
VPWS	*Virtual Private Wire Service*
VRRP	*Virtual Router Redundancy Protocol*
WIDS	*Wireless-based IDS*