Primjena BGP protokola u virtualnim privatnim mrežama

Sudar, Ivan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA U OSIJEKU

Sveučilišni diplomski studij elektrotehnike

PRIMJENA BGP PROTOKOLA U VIRTUALNIM PRIVATNIM MREŽAMA

Diplomski rad

Ivan Sudar

Osijek, 2018. godine

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA U OSIJEKU

Sveučilišni diplomski studij elektrotehnike

PRIMJENA BGP PROTOKOLA U VIRTUALNIM PRIVATNIM MREŽAMA

Diplomski rad

Ivan Sudar

Osijek, 2018. godine

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada

Osijek, 10.09.2018.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu diplomskog rada

Ime i prezime studenta:	Ivan Sudar
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 1076, 26.09.2017.
OIB studenta:	25734077671
Mentor:	Doc.dr.sc. Višnja Križanović
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Prof.dr.sc. Drago Žagar
Član Povjerenstva:	Izv. prof. dr. sc. Krešimir Grgić
Naslov diplomskog rada:	Primjena BGP protokola u virtualnim privatnim mrežama
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	U radu je potrebno dati pregled značajki BGP (Border Gateway Protocol) usmjerivačkog protokola te analizirati primjenu BGP protokola u virtualnim privatnim mrežama (Virtual private Networks, VPN).
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	10.09.2018.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 17.09.2018.

Ime i prezime studenta:	Ivan Sudar
Studij:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 1076, 26.09.2017.
Ephorus podudaranje [%]:	3%

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena BGP protokola u virtualnim privatnim mrežama**

izrađen pod vodstvom mentora Doc.dr.sc. Višnja Križanović

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

BGP protokol (engl. *Border Gateway Protocol*) koristi se za usmjeravanje paketa između autonomnih sustava. Autonomni sustavi zahtijevaju primjenu različitih pravila usmjeravanja koja su omogućena uporabom upravo BGP-a. BGP protokol zahtjeva da svi usmjerivači budu međusobno povezani što rezultira time da sve informacije o promjenama unutar mreže brzo dolaze do svih njenih dijelova i upravo u tome je velika prednost korištenja BGP protokola. Nažalost, navedena prednost donosi sa sobom i nedostatak budući da tablice usmjeravanja znaju biti iznimno velike. Kako BGP protokol ima značajnu primjenu pri komunikaciji koja se odvija između autonomnih sustava, velik posao odrađuje upravo u VPN (engl. *Virtual Private Network*) mrežama.

VPN mreže pri komunikaciji između uređaja koriste rutu koja se naziva tunelom. Tuneli u VPN mrežama imaju zadatak zaštiti privatni promet od prisluškivanja, smetnji koje mogu uzrokovati zagušenja u isporuci, gubitak paketa te cenzure. VPN mreže su privatne mreže koje su dio javne mreže, a omogućuju povezivanje udaljenih stanica ili korisnika u jednu mrežu.

Primjena BGP protokola u VPN mrežama je zastupljena u svrhu određivanja ruta kojima će se slati paketi između autonomnih sustava koji su dio VPN-a. Osim što određuje rute između autonomnih sustava, također se koristi i unutar autonomnog sustava. Važna primjena BGP protokola je svakako ta da je promet između korisnika tuneliran, što pospješuje sigurnost prometa, a osim sigurnosti, svakako je povećana efikasnost razmjene prometa unutar VPN-a.

Rad je podijeljen u šest cjelina.

1. Uvod
2. BGP usmjerivački protokol
3. Značajke BGP protokola
4. Primjena BGP protokola u virtualnim privatnim mrežama
5. Konfiguracije praktičnog dijela
6. Zaključak

Drugo poglavlje nosi opis BPG protokola kao usmjerivačkog protokola. Definirani su opisi BGP poruka koje u radu koristi BGP protokol. Kako poruke sadrže atribute puta, definirani su i atributi

puta s osnovnim uputama o svakom atributu. Poruke i atributi puta korišteni su prilikom opisa načina rada BGP protokola, ali i prilikom izrade trećeg i četvrtog poglavlja ovog rada.

U trećem poglavlju opisane su BGP značajke, ili kako se u struci nazivaju - BGP proširenja. BGP protokol koristi dva proširenja koji uvelike pomažu prilikom odabira rute. Prvo proširenje je višeprotokolna dostupnost odredišta koje određuje koja su odredišta dostupna unutar promatranog usmjerivača. Drugo proširenje je višeprotokolna nedostupnost odredišta koje određuje nedostupnost odredišta te se takvo odredište briše iz liste ruta.

Četvrto poglavlje objašnjava primjenu BGP protokola u virtualnim privatnim mrežama. Na početku poglavlja raspisano je osnovno o virtualnim privatnim mrežama te napravljen uvod kako bi se povezala primjena BGP-a u VPN-u. Osnovna primjena BGP-a definira način distribucije ruta za virtualne privatne mreže, način prosljeđivanja definiranih ruta unutar mreže, kao i način razdvajanja VPN mreža.

U petom poglavlju definirane su dvije topologije mreže koje kroz praktični primjer omogućuju dodatnu analizu sadržaja opisanih unutar drugog, trećeg i četvrtog poglavlja. Prva topologija pokazuje kako se u osnovi koristi BGP protokol, dok druga topologija pokazuje primjenu BGP protokola unutar VPN mreža.

1.1. Zadatak

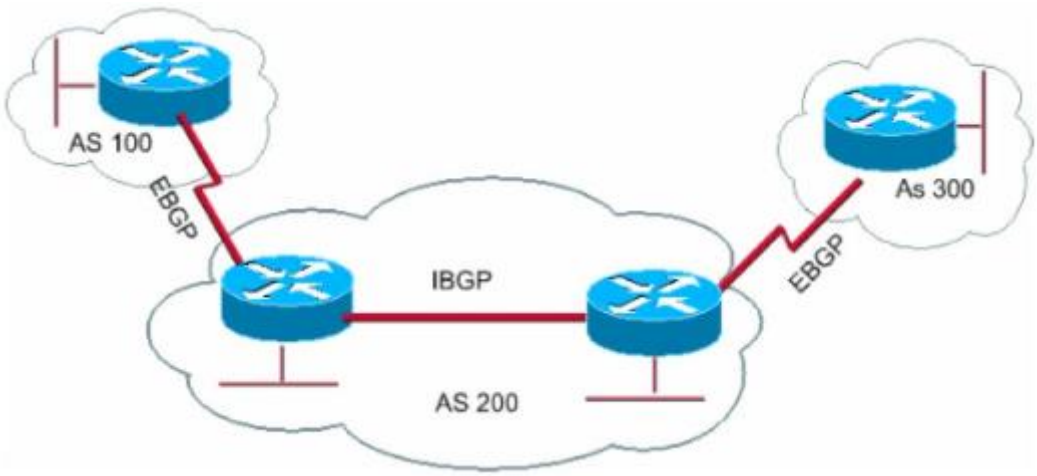
U radu je potrebno dati pregled značajki BGP (*Border Gateway Protocol*) usmjerivačkog protokola te analizirati primjenu BGP protokola u virtualnim privatnim mrežama (*Virtual private Networks*, VPN).

2. BGP USMJERIVAČKI PROTOKOL

Najvažniji protokol usmjeravanja kojim je ostvarena komunikacija između usmjerivača koji se nalaze unutar različitih autonomnih sustava je BGP protokol. Autonomnim sustavom (AS) smatra se svaki skup mreža i usmjerivača koji posjeduju zajednička pravila usmjeravanja te takvim sustavima obično upravljaju ISP (engl. *Internet Service Provider*) ili veće organizacije. AS-e razlikujemo prema pripadnom broju koji ih označava, i taj broj je jedinstven za svaki AS. Protokoli za usmjeravanje koje usmjerivači mogu koristi su neki od IGP (engl. *Interior gateway protocol*) usmjerivačkih protokola unutar AS te EGP (engl. *Exterior Gateway Protocol*) protokol usmjeravanja koji se koristi za usmjeravanje između AS-a. Na Internetu se trenutno koristi samo jedan EGP protokol, odnosno navedeni BGP protokol. Od 1994. godine na Internetu se koristi inačica četiri BGP protokola (BGPv4), koji je donio novosti poput CIDR (engl. *Classless Inter-Domain Routing*) te združivanje puteva kako bi došlo do smanjivanja veličina tablica za usmjeravanje. CIDR metoda omogućuje, temeljem mrežnog prefiksa (određenog pomoću broj bitova IP adrese koji se odnose na mrežni dio, ostatak bitova IP adrese služi za računalni dio) usmjeravanje paketa prema odredišnoj adresi. Korištenjem ove metode dolazi do uštede adresa jer se različite IP adrese mogu grupirati u njihov mrežni prefiks i paketi imaju mogućnost usmjeravanja do usmjerivača koji se nalazi unutar određene odredišne mreže. [1]

Mrežni usmjerivač ima zadatak dostaviti paket do odredišnog računala. BGP svoj rad zasniva na algoritmu vektora puta. Algoritam vektora puta ima sličnosti s algoritmom vektora udaljenosti korištenog u IGP protokolima. Razlika je u tome što BGP računa udaljenost puta prema broju AS-ova kroz koje paketi prolaze na putu do odredišnog AS-a, dok algoritam vektora udaljenosti broji usmjerivače kojima paketi prolaze. Prilagođavanjem načina usmjeravanja pojedinog AS-a moguće je promijeniti odluku o odabranom putu. Postoje dva načina rada BGP protokola: iBGP (engl. *Internal BGP*) korišten između usmjerivača koji pripadaju istom AS-u i eBGP (engl. *External BGP*) korišten između usmjerivača koji pripadaju različitim AS-ima. Na sl. 2.1. prikazane su upotrebe pojedinog načina rada BGP-a. Na slici se nalazi sustav s tri AS-a s pripadajućim BGP usmjerivačima. Tijekom rada rubni BGP usmjerivači sa susjednim BGP usmjerivačima koji se ne nalaze u istom AS-u rade u eBGP načinu rada, dok za komunikaciju sa usmjerivačima u istom AS-u koriste iBGP način rada. Ukoliko se mrežna topologija postavi na način da unutar većeg AS postoji manji AS, tada se rubni usmjerivači većeg mogu također koristiti i unutar manjeg AS-a. Važno je znati razliku između iBGP i IGP te činjenicu da se BGP protokol, prilikom načina rada u iBGP, u pravilu ne bi trebao koristiti umjesto IGP protokola koji ima funkciju usmjeravanja

paketa. Poruke BGP protokola koje se razmjenjuju istog su oblika dok se načini rada razlikuju samo u pravilima usmjeravanja. [2]



Sl. 2.1. *Način rada BGP protokola unutar te između AS-a.* [2]

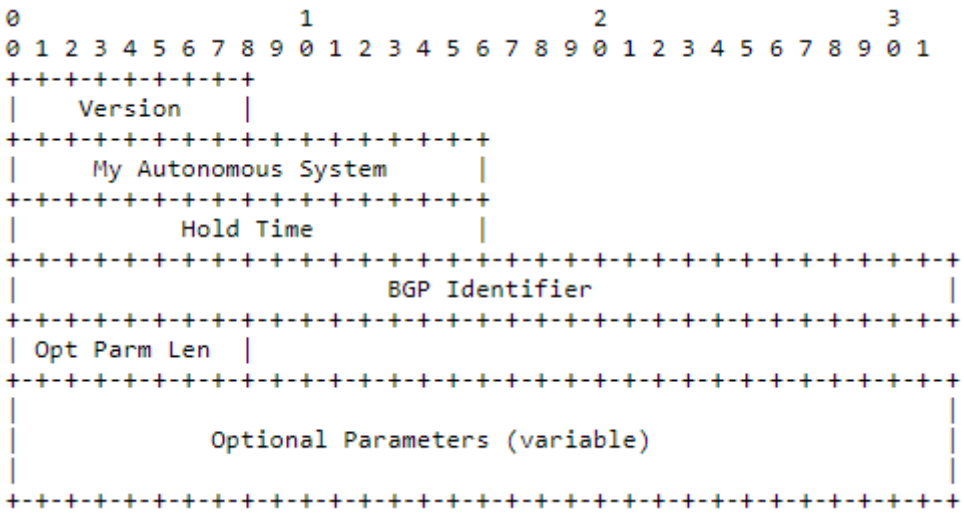
2.1. Poruke koje koristi BGP protokol

BGP protokol u komunikaciji s drugim usmjerivačima koristi četiri vrste poruka, a to su: OPEN, UPDATE, KEEPALIVE i NOTIFICATION.

Nakon što usmjerivači uspostave TCP vezu, međusobno se razmjene poruke OPEN. Poruka KEEPALIVE potvrdni je odgovor na OPEN poruku i porukom KEEPALIVE označava se da je OPEN poruka uspješno primljena. Stoga se prilikom analize mrežnog prometa može vidjeti da, nakon što se uspostavi TCP veza, oba usmjerivača razmijene po jednu OPEN i jednu KEEPALIVE poruku te se zaključuje da se porukom OPEN usmjerivači predstavljaju međusobno i pregovaraju o parametrima veze. Poruka OPEN nosi sljedeće parametre:

- *Version* – duljine jednog okteta, informacija o inačici BGP protokola.
- *My autonomus system* – duljine 2 okteta, predstavlja broj AS-a pošiljatelja poruke.
- *Hold time* – duljine 2 okteta, definira vrijeme čekanja izraženo u sekundama (maksimalan broj sekundi koje mogu proći bez primitka poruke prije nego što pošiljatelj pretpostavi da veza nije funkcionalna; zadano vrijeme čekanja tvrtke Cisco iznosi 180 sekundi).
- *BGP identifier* – predstavlja IP adresu pošiljatelja, najčešće *loopback* adresa usmjerivača.
- *Optional parameters length* – označava duljinu dodatnih parametara (*optional parameters*), ukoliko je vrijednost nula dodatni parametri ne postoje.

- *Optional parameters* – sadrži popis dodatnih parametara, npr. za autentifikaciju, višeprotokolnu podršku i osvježavanje rute. [3]



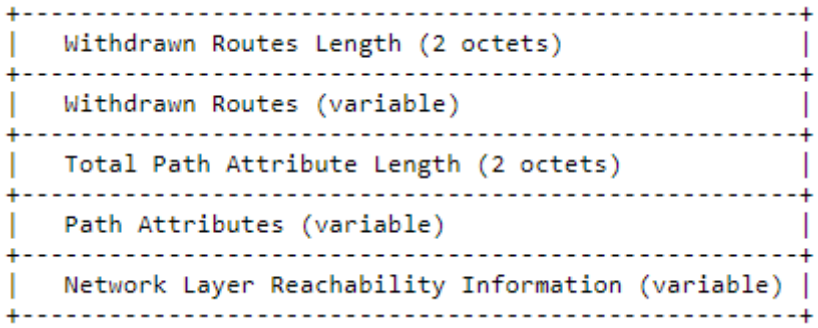
Sl. 2.2. *Polja poruke OPEN* [1]

Poruka UPDATE se koristi za prijenos podataka o usmjeravanju između BGP *peer-ova*. Informacije u poruci UPDATE tipa mogu se koristiti za izradu grafikona koji opisuje odnose različitih AS-a. Primjenom pravila za raspravu, usmjeravanje informacija unutar petlji i neke druge anomalije sustava mogu se otkriti i ukloniti iz usmjeravanja između među AS-ima. Usmjerivačima s kojima je uspostavljena TCP veza šalje se poruka UPDATE s putovima iz *Adj-RIBs-OUT* liste. Poruka tipa UPDATE također ima mogućnost objave novih puteva ili odjave starih puteva ukoliko putovi nisu aktivni, pri čemu je potrebno naglasiti da istovremeno može biti objavljena samo jedna vrsta atributa. Više atributa može biti objavljeno ukoliko se poruka šalje na više odredišta, ali pod uvjetom da taj atribut koriste sva odredišta. [1]

Polja poruke UPDATE su sljedeća:

- *Withdrawn routes length* – označava ukupnu duljinu *withdrawn routes* polja (ako je vrijednost nula, polje na koje označava nije prisutno).
- *Withdrawn routes* – sadrži popis prefiksa IP adresa ruta (sastoje se od para: duljina i prefiksa, a služe za opis odredišta koja su postala nedostupna i sklanjaju se iz usluge).
- *Total path attribute length* – označava ukupnu duljinu polja *path attributes* (ukoliko je vrijednost polja nula, polje na koje označava nije prisutno).
- *Path attributes* – opisuje značajke puta pomoću atributa puta (atributi puta obrađeni su u podpoglavlju 2.2.).

- *Network layer reachability information* – sadrži popis prefiksa IP adresa za oglašene rute [3].



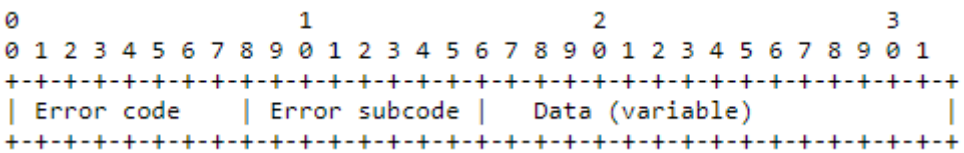
Sl. 2.3. *Polja poruke UPDATE.* [1]

Za održavanje sjednice koristi se poruka KEEPALIVE. Kako BGP ne koristi niti jednu TCP provjeru dostupnosti pojedinih *peer-ova*, KEEPALIVE poruku međusobno razmjenjuju usmjerivači kako ne bi isteklo vrijeme čekanja. Maksimalno vrijeme između dvije poruke KEEPALIVE je jedna trećina vremena koje je definirano u polju *hold time* poruke OPEN. [1] Osnovne postavke unutar Cisco uređaja definiraju da je vrijeme slanja ove poruke 60 sekundi što odgovara periodu trećine *hold time.* [3]

Poruka NOTIFICATION koristi se kada nešto pođe po zlu. Nakon što se otkrije o kojoj je pogrešci riječ zatvara se BGP veza. Razlozi slanja poruke ovog tipa mogu biti sljedeći: veza nije sinkronizirana, pogrešna duljina poruke, pogrešan BGP identifikator, nedostatak dobro poznatog atributa, i sl. [1]

Polja poruke:

- *Error code* – nose informaciju o tipu pogreške koja se dogodila.
- *Error subcode* – pruža specifične informacije o prirodi prijavljene pogreške.
- *Data* – sadrži podatke na temelju šifre pogrešaka i potvrdnih polja podkoda. Služi za dijagnosticiranje razloga za slanje poruke obavijesti. [3]



Sl. 2.4. *Polja poruke NOTIFICATION.* [1]

2.2. Primjena atributa puta

O putu, odnosno o ruti usmjeravanja paketa do odredišnog AS-a odlučuje BGP usmjerivač, a odluku usmjerivač donosi na temelju atributa puta koji se nalaze unutar poruke UPDATE. Stoga se da zaključiti da na temelju atributa puta i pomoću poruke UPDATE, usmjerivačima je omogućena primjena vlastita pravila usmjeravanja. Atributi puta mogu se podijeliti u četiri skupine:

- dobro poznati obavezni (engl. *Well-known mandatory*),
- dobro poznati neobavezni (engl. *Well-known discretionary*),
- izborni tranzitni (engl. *Optional transitive*) i
- izborni lokalni (engl. *Optional non-transitive*) atributi. [4]

Usmjerivači unutar BGP-a moraju prepoznati sve dobro poznate atribute puta. Obavezni atributi moraju biti uključeni u svaku UPDATE poruku koja u sebi sadrži polje NLRI (više o NLRI bit će navedeno u trećem poglavlju). Poznati neobavezni atributi mogu i ne moraju biti uključeni u UPDATE poruku. Nakon što BGP usmjerivač primi UPDATE poruku s nekim promjena u rutama, informacije o tome mora prenijeti svim usmjerivačima s kojima ostvaruje vezu. Uz dobro poznate atribute, svaka ruta može sadržavati jedan ili više izbornih atributa. Iako ne mora značiti da sve implementacije BGP-a održavaju izborne atribute. Ukoliko implementacija ne prepoznaje neke od izbornih atributa te se dogodi da poruka sadrži takav atribut, takav paket mora biti prihvaćen i proslijeđen do sljedećeg AS-a. Ukoliko se radi o neprepoznatom tranzitnom putu, paket se mora prenijeti dalje jer se odnosi na sve AS-ove na tom putu, i svi AS-ovi bi trebali imati mogućnost primiti takav paket. Neprepoznati lokalni atribut se također treba prenijeti u sljedeći AS jer se taj atribut odnosi na lokalni AS i iz tog razloga drugi AS-ovi nemaju potrebe razmatrati taj atribut. Za bilo kakav slučaj koji može nastati vezano uz izborne atribute, bitno je prihvatiti taj paket jer i dalje postoje dobro poznati atributi u tom paketu.

BGP protokol koristi sljedeće atribute puta: ORIGIN, AS_PATH, NEXT_HOP, MULTI_EXIT_DISC, LOCAL_PREF, ATOMIC_AGGREGATE i AGGREGATOR.

Atribut ORIGIN je dobro poznati obavezni atribut koji definira podrijetlo informacija usmjeravanja, odnosno način nastanka BGP puta. Generiran je od strane usmjerivača koji ima ulogu izvora. Drugi usmjerivači ne smiju mijenjati vrijednost ovog atributa. Atribut osim informacije o izvorišnom usmjerivaču nosi i informaciju kojom daje obavijest o primatelju poruke, odnosno o tome nalazi li se izvorni usmjerivač unutar istog AS-a kao i primatelj. Obavijesti su po

prioritetu složene sljedećim redom: IGP imaju najveći prioritet, zatim EGP su druge po prioritetu i najmanji prioritet imaju nepotpune. [4]

Atribut AS_PATH je dobro poznati obavezni atribut puta koji identificira AS-ove kroz koje su prošli podatci o usmjeravanju koji se prenose u UPDATE poruci te sve AS-ove slaže u listu koja tvori segmente puta koje paketi prolaze na putu do odredišta. [1] Svaki odsječak puta AS-a je opisan trojkom: tip, duljina i vrijednost. [5]

Pravi smisao korištenja ovaj atribut ima kada se koristi kod višestrukih puteva jer onda služi za izbjegavanje petlji, preferiranje određenog puta i zabranu usmjeravanja paketa kroz određeni AS. Atribut se koristi na način da, kada usmjerivač primi atribut ovog tipa prije nego ga proslijedi dalje, usmjerivač izmjenjuje vrijednost na način da umetne broj AS-a u kojem se nalazi na listu koja sadržava segmente puta.[4]

Atribut NEXT_HOP zadnji je dobro poznati obavezni atribut puta koji definira IP adresu usmjerivača koji će se koristit kao sljedeći skok do odredišta i naveden je u UPDATE poruci. Adresa sljedećeg skoka odabrana je tako da će odabrati najkraći dostupni put. Prilikom implementacije postavlja se ograničenje koje usmjerivaču služi da sebe ne može postaviti kao sljedeću skok na nekoj ruti. Vrijednost ovog atributa se mijenja samo u slučaju da je sljedeći usmjerivač član drugog AS-a. [4]

Atribut MULTI_EXIT_DISC je izborni lokalni atribut koji se koristi na vanjskim vezama u svrhu upravljanja između više izlaznih i ulaznih točaka na isti susjedni AS. Kako se koristi više puteva, ovaj atribut nosi informaciju u susjedni AS kojim putem će poslati pakete te se na ovaj način upravlja dolaznim prometom iz pojedinog AS-a. Ukoliko usmjerivač prilikom odabira jednog puta iz većeg broja mogućih puteva ne može na temelju ostalih atributa donijeti odluku, tada gleda koji put ima najmanju vrijednost atributa MULTI_EXIT_DISC. [1]

Atribut LOCAL_PREF je dobro poznati neobavezni atribut puta i razmjenjuje se samo između usmjerivača koji imaju iBGP vezu i iz tog razloga ovaj atribut je drugim usmjerivačima nepoznat. Takvo pravilo označava prioritet BGP usmjerivača. Ukoliko usmjerivač dobije više ruta s istog AS-a, smatra se da je put s najvišom LOCAL_PREF vrijednošću najbolji put. [4]

Atribut ATOMIC_AGGREGATE još je jedan dobro poznati neobavezni atribut puta koji ima mogućnost združivanja puteva prema odredištu. BGP uvodi pojam združivanje puteva radi smanjenja broja puteva i upravo ovim atributom puta se združuju putevi i predstavljaju kao jedan put unutar poruke UPDATE. Polje tip koje je spomenuto kod atributa AS_PATH i lista AS-a koji

čine združeni put su najčešće vrijednosti unutar atributa ATOMIC_AGGREGATE. Združivanje puteva jedino je moguće ukoliko putevi imaju iste atribute. [1]

Posljednji izborni tranzitni atribut je AGGREGATOR i povezan je s ATOMIC_AGGREGATE atributom jer AGGREGATOR atribut daje informaciju da je usmjerivač združio rutu. Ovaj atribut mora sadržavati broj AS-a i IP adresu koja mora biti jednaka BGP identifikatoru usmjerivača. [1]

2.3. Način rada BGP protokola

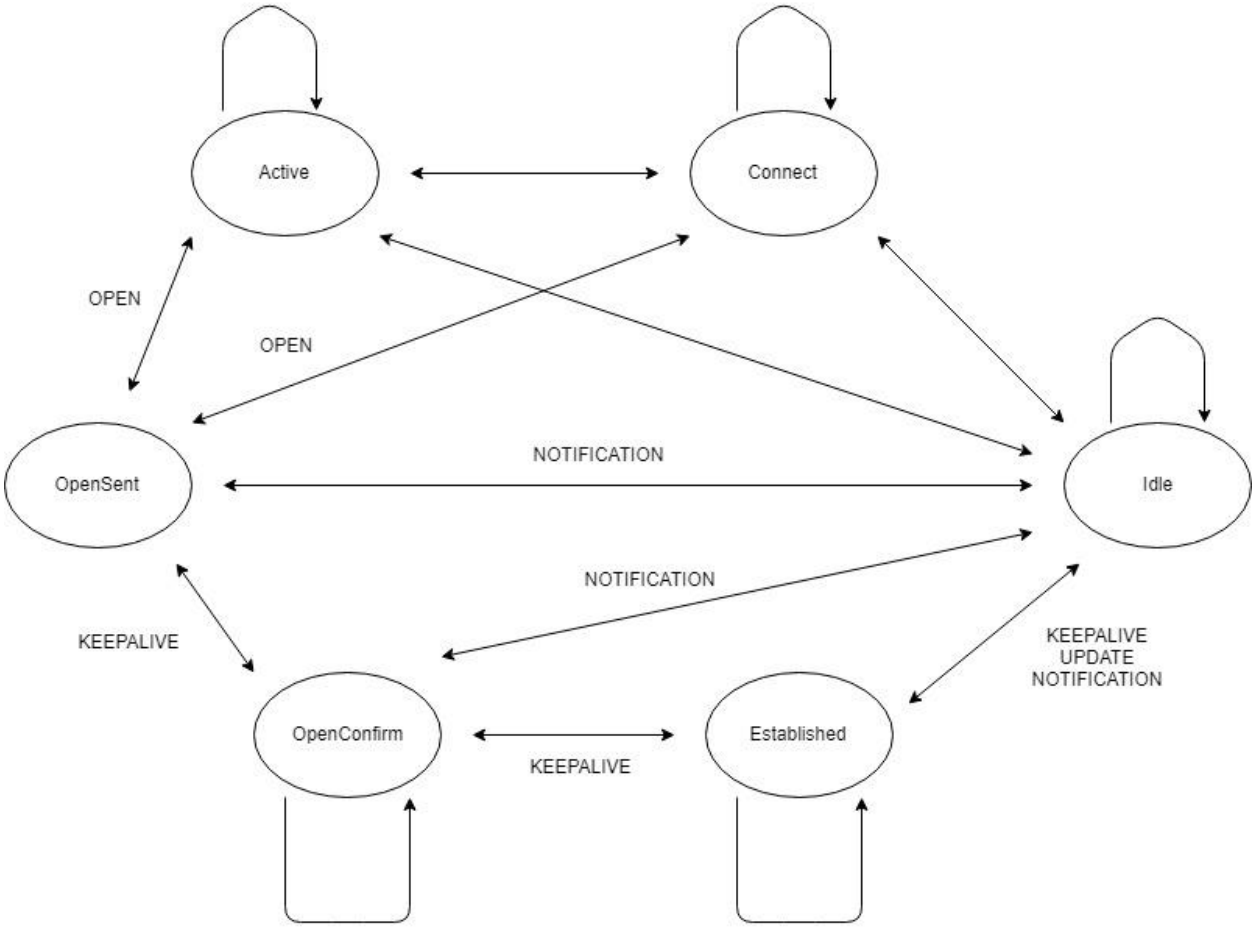
BGP protokol kao transportni protokol koristi TCP protokol. TCP protokol uspostavlja vezu između usmjerivača na priključnici 179. Konfiguracija komunikacije između usmjerivača se obavlja ručno te iz tog razloga nije potrebno definirati postupke za otkrivanje susjednih usmjerivača unutar IGP protokola. Prilikom uspostavljanja TCP veze sa svim susjednim usmjerivačima, BGP usmjerivač sa svima razmjenjuje čitave tablice usmjeravanja u kojima su upisane sve informacije o putovima NLRI (engl. *Network Layer Reachability Information*) prema odredišnoj mreži koja je dio AS-a. Spomenuto je da kako BGP put do odredišta treba proći niz AS-ova i pri tome postoji nekoliko puteva s istim odredištem te da definiranjem skupa atributa puta je omogućena primjena različitih pravila usmjeravanja. Put kojim će se usmjeravati paketi prema odredištu biraju se na temelju sljedećeg: atributa puta, dostupnosti puta, izbornih pravila o prihvaćanju paketa, lokalnih pravila o propuštanju paketa i dogovora između AS-ova. [7]

Svaki usmjerivač osim tablice usmjeravanja sadrži i bazu puteva pod nazivom RIB (engl. *BGP Routing Information Base*), na temelju baze određuju se putovi usmjeravanja paketa. Postoje tri vrste popisa baze RIB:

- ***Adj-RIBs-In*** – sprema informacije o usmjeravanju primljene od susjednih usmjerivača, a informacija je dobivena prije nego li je primijenjena bilo kakva izmjena atributa ili filtriranje rute. Za svaki susjedni usmjerivač kreira se poseban popis ovog tipa.
- ***Loc-RIB*** – sadrži rute koje je odabrao lokalni usmjerivač na temelju procesa odlučivanja (engl. *decision process*), a korištene rute prilikom odabira nalaze se u prethodno navedenom popisu *Adj-RIBs-In.*
- ***Adj-RIBs-Out*** – sadrži putove koji se šalju određenim susjednim usmjerivačima pomoću UPDATE poruke. Za svaki susjedni usmjerivač kreira se poseban popis. [1]

Rad BGP usmjerivača može se predočiti konačnim automatom sa šest stanja: *Idle, Connect, Active, OpenSent, OpenConfirm i Established.* Prikaz stanja i moguće rute između stanja najbolje

prikazuje slika Sl. 2.5. Kada BGP usmjerivač ostvari vezu sa susjednim usmjerivačem stvara se zaseban automat stanja za pojedinu vezu i gleda se stanje usmjerivača u ostvarenoj vezi.



Sl. 2.4. *BGP automat konačnih stanja* [6]

Stanje *Idle* predstavlja početno stanje BGP usmjerivača i kada je usmjerivač u ovom stanju odbijaju se dolazne BGP veze. Sustav počinje s inicijalizacijom BGP resursa nakon što se aktiviraju *ManualStart ili AutomaticStart* te se pokreće brojač *ConnectRetry* i pokušava se uspostaviti TCP veza sa susjednim usmjerivačem kako bi usmjerivač prešao u stanje *Connect.* Ukoliko se, zbog zatvorene priključnice 179 ili krive konfiguracije adrese usmjerivača ili AS-a, dogodi greška TCP veza se ne uspostavlja i usmjerivač ostaje u stanju *Idle* kroz određeni period vremena. Stanje *Connect* je predstavljeno kao stanje u kojem usmjerivač čeka da se uspostavi TCP veza sa susjedom. Uspješno postavljenom vezom šalje se poruka OPEN i usmjerivač prelazi u stanju *OpenSent.* U suprotnom, prilikom neuspješnog postavljanja veze, usmjerivač prelazi u stanje *Active* i dok je u ovom stanju usmjerivač će pokušati još jednom uspostaviti TCP vezu sa susjednim usmjerivačem. Ukoliko nakon ponovnog pokušaja dođe do uspješne uspostave dolazi do slanja OPEN poruke i prelazi u stanje *OpenState*, kao i u slučaju kada je uspješno postavljena

veza u stanu *Connect.* Neuspješno postavljanje veze nakon drugog pokušaja usmjerivač prebacuje u početno stanje *Idle.* Zbog navedenih grešaka prilikom uspostavljanja TCP veze može se dogoditi da usmjerivač prelazi samo iz stanja *Idle* u stanje *Active.* Iz stanja *Active* usmjerivač se može opet naći u stanju *Connect* ako se dogodi da istekne vrijeme brojača *ConnectRetry*, ali to označava da će usmjerivač odustati od uspostavljanja trenutne TCP veze i prelazi na uspostavljanje TCP veze sa drugim susjednim usmjerivačem. Nakon što je uspostavljena veza s drugim usmjerivačem, u stanju *OpenState* usmjerivač čeka na pouku OPEN s usmjerivača s kojim ima ostvarenu TCP vezu te provjerava ispravnost poruke. Iz trenutnog stanja usmjerivač može preći u stanje *Idle* ukoliko otkrije pogrešku u poruci OPEN te prije nego što pređe u stanje *Idle* šalje poruku NOTIFICATION i raskida TCP vezu. U suprotnom usmjerivač po uspješnom primitku poruke OPEN šalje kao potvrdni odgovor KEEPALIVE poruku. Pri tome se postavlja *hold timer* brojač i usmjerivač prelazi u *OpenConfirm* stanje. U tom stanju usmjerivač čeka na KEEPALIVE poruku od drugog usmjerivača, kojom će se potvrditi ispravan primitak OPEN poruke prvog usmjerivača. Ukoliko umjesto očekivane poruke KEEPALIVE dođe poruka NOTIFICATION, znači da je došlo do nekakve pogreške te će usmjerivač zatvoriti TCP vezi i preći u stanje *Idle*. Osim prethodno navedenog slučaja, također se može dogoditi da istekne vrijeme brojača. Nakon isteka vremena usmjerivač će postali poruku NOTIFICATION i prijeći u početno stanje *Idle.* Ipak, poželjan ishod je da usmjerivač ipak dobije KEEPALIVE poruku unutar definiranog vremena u brojaču što označava da je sve u redu s TCP vezom, a tada usmjerivač prelazi u stanje *Established.* U ovom stanju samo usmjerivači imaju mogućnost slanja UPDATE poruke te izmjenjivati vlastite tablice usmjeravanja. Iz ovog stanja uz prisutnost pogrešaka ili primitak NOTIFICATION poruke ili izostanak UPDATE ili KEEPALIVE poruka unutar definiranog vremena brojača, usmjerivač prelazi u početno stanje *Idle.* [1]

Pravila usmjeravanja za pojedini AS nalaze se u PIB (engl. *Policy Information Base*) bazi i upravo ta pravila propisuju način na donošenja odluke o odabiru puta. Kao što je već navedeno usmjerivač u svom algoritmu na temelju procesa odlučivanja, odlučuje koji je najbolji put za neko odredište pri čemu se neki od atributa uopće ne moraju koristiti prilikom donošenja odluke.

Prilikom odlučivanja usmjerivač se ipak vodi nekim osnovnim pravilima, kao što su:

- Ne uzima se u obzir put za koji nije poznat usmjerivač u sljedećem skoku.
- Vrijednost o težini koja se postavlja za pojedini usmjerivač koja nije povezana s atributima BGP protokola. Usmjerivač izabire najveću takvu vrijednost težine.
- LOCAL_PREF kao što je već navedeno gleda se najveća vrijednost.

- Najkraći put u atributu AS_PATH.
- Najmanja vrijednost ORIGIN i MULTI_EXIT_DISC.
- Prioritet imaju eBGP put u odnosu na iBGP put.
- Najmanja udaljenost do usmjerivača čije je odredište sljedeći skok.

Postoji nekolicina mogućih algoritama usmjeravanja, u nastavku je opisan jedan primjer takvog algoritma:

1. Potrebno je provjeriti dostupnost odredišnog usmjerivača u NEXT_HOP atributu.

    a. Ukoliko je usmjerivač dostupan vrši se provjera pripadnosti usmjerivača unutar odabranog AS-a.

        I. Ako usmjerivač pripada istom AS-u gleda se LOCAL_PREF atribut.

2. Ukoliko se prilikom pregleda LOCAL_PREF atributa pronađe više puteva za isto odredište, traži se onaj put koji ima najveću vrijednost atributa LOCAL_PREF.

    a. Ukoliko se dogodi da su sve vrijednosti jednake tada se gledaju drugi atributi i to najčešće AS_PATH, ORIGIN i MULIT_EXIT_DISC navedenim redoslijedom.

        I Pronalazi se put s najkraćim atributom AS_PATH.

        II Nakon toga, gleda se put s najmanjom vrijednosti u ORIGIN atributu.

        III Ako odluka još uvijek nije donesena, potrebno je pronaći put s najmanjim MULTI_EXIT_DISC atributom.

Utemeljeno na informacijama unutar popisa *Adj-RIBs-In* i lokalnih popisa *Loc-RIB* te uporabom nekog od algoritama usmjeravanja, BGP usmjerivač će odrediti za svako odredište po jedan najbolji put koji će se biti korišten za usmjeravanje paketa. [1]

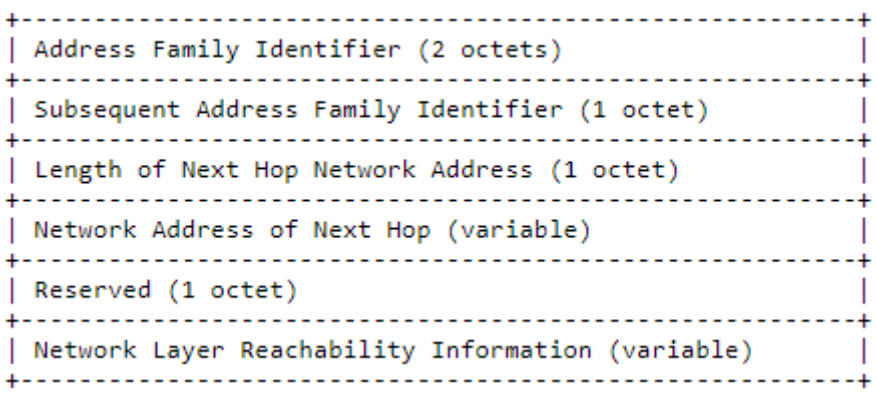
3. OSNOVNE ZNAČAJKE BGP PROTOKOLA

Specifične informacije za IPv4 protokol koje BGP prenosi su: atribut NEXT_HOP koji je izražen kao IPv4 adresa, AGGREGATOR koji sadrži IPv4 adresu i NLRI (*engl. Network Layer Reachability Information*) koji je izražen kao prefiks IPv4 adrese. Potrebno je smatrati da BGP posjeduje IPv4 adresu. Kako bi bilo moguće u BGP protokolu omogućiti podršku za usmjeravanje više mrežnih protokola potrebno je dodati dvije stvari, a to su: sposobnost povezivanja određenog mrežnog sloja pomoću NEXT_HOP informacije i sposobnost povezivanja određenog protokola mrežnog sloja s NLRI. Kako bi se prepoznali mrežni protokoli određenog mrežnog sloja uz pomoć NEXT_HOP i NLRI informacija potrebno je koristiti listu adresa koja je definirana kao IANA-AF te listu naknadnih adresa. Važno je zaključiti kako NEXT_HOP informacija jedino ima smisla u kombinaciji s informacijom o dostupnim odredištima odnosno nedostupnim odredištima. Iz tog razloga je potrebno odvojiti informacije koje nosi NEXT_HOP s dostupnim odredištima od onih informacija o nedostupnim odredištima. Kako bi se omogućilo razdvajanje informacija o odredištima, kao i pojednostavljenje podrške za višeprotokolni rad BGP protokola osmišljena su dva svojstva. [8]

Nešto više o navedenim svojstvima objašnjeno je u podpoglavljima 3.1. i 3.2.

3.1. Atribut dostupnosti odredišta

Ova ekstenzija se može koristiti u sljedeće svrhe: javljanje dostupnog puta prema svima koji odašilju informaciju i dopuštanje usmjerivaču da oglašava adresu mrežnog sloja usmjerivača koji bi trebao biti sljedeće odredište koje je navedeno u listi informacija o dostupnosti mrežnog sloja. Atribut je kodiran na sljedeći način:

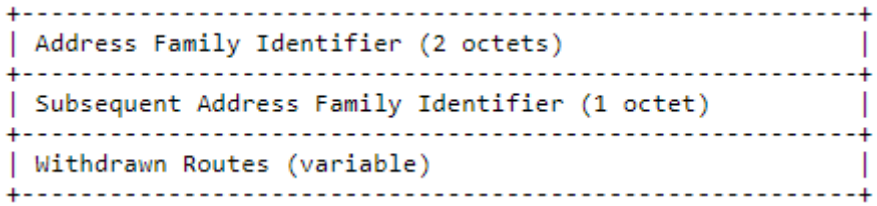


Sl. 3.1. *Kodiranje atributa puta dostupnih odredišta* [8]

Kao što je vidljivo na slici Sl. 3.1. kodiranje atributa puta dobiveno je postavljanjem informacija u navedena polja. *Address Family Identifier* (AFI) u kombinaciji sa *Subsequent Address Family Identifier* (SAFI) identificira skup protokola na mrežnom sloju u kojima se mora nalaziti adresa koju nosi sljedeći skok. Ako se sljedeći skok dopusti iz više od jednog protokola mrežnog sloja, kodiranje sljedećeg skoka mora dati način određivanja protokola mrežnog sloja. *Length of Next Hop Network Address* predstavlja duljinu *Network Address of Next Hop* koji definira polje s promjenjivom duljinom koje sadrži mrežnu adresu sljedećeg usmjerivača na putu prema odredišnom sustavu. Protokol mrežnog sloja koji je povezan s mrežnom adresom sljedećeg skoka identificiran je kombinacijom AFI i SAFI koji se prenosi u atributu puta. *Reserved* polje mora biti postavljeno na nulu i trebao bi biti zanemaren po primitku. Polje *Network Layer Reachability Information* (NLRI) s promjenjivom duljinom koje navodi NLRI za izvedive rute koje se oglašavaju u ovom atributu puta. Semantika NLRI je identificirana kombinacijom AFI i SAFI koja se prenosi u atributu puta. Kada je polje za identifikaciju SAFI postavljeno na jednu od vrijednosti, svaki NLRI je kodiran kao specifičan način NLRI kodiranja. Informacija sljedećeg skoka koja se prenosi, u atributu puta višeprotokolne dostupnost odredišta, definira adresu mrežnog sloja usmjerivača koji se mora koristiti kao sljedeći skok. Do odredišta navedenih u atributima UPDATE poruka koja u višeprotokolnoj dostupnosti odredišta nosi ORIGIN i AS_PATH atribute. UPDATE poruka koja ne nosi NLRI također ne posjeduje niti NEXT_HOP atribut. Ukoliko se dogodi da poruka sadrži NEXT_HOP atribut BGP prijemnik koji prima poruku trebao bi ignorirati ovaj atribut. UPDATE poruka ne uključuje isti prefiks adrese u više od jednog od sljedećih polja: *withdrawn routes*, polja s informacijama o dostupnosti mreže, MP_REACH_NLRI polje i MP_UNREACH_NLRI polje. Obrada poruke u tom slučaju nije definirana. [8]

3.2. Atribut nedostupnosti odredišta

Kao što i sam podnaslov govori ova ekstenzija se koristi s ciljem povlačenja neizvodivih odnosno nedostupnih ruta iz primjene. Kodiranje atributa nedostupnih odredišta ima manje polja i kodiran je na sljedeći način:



Sl. 3.2. Kodiranje atributa puta nedostupnih odredišta [8]

Prva dva polja predstavljaju istu funkciju kao što je već opisano u prethodnom podpoglavlju 3.1. Treće polje *Withdrawn Routes* predstavlja polje s promjenjivom duljinom koja navodi NLRI za rute koje su povučene iz primjene. UPDATE poruka koja sadrži MP_UNREACH_NLRI nije obavezna nositi bilo koji drugi atribut puta. [8]

4. PRIMJENA BGP PROTOKOLA U VIRTUALNIM PRIVATNIM MREŽAMA

U narednom poglavlju opisuje se način na koji pružatelj usluga može koristiti IP okosnicu za pružanje IP virtualnih privatnih mreža svojim klijentima. Koristi se *peer* model u kojem krajnji usmjerivač klijentima šalje svoje rute do usmjerivača koji je davatelj usluga. Davatelj usluga koristi BGP protokol za razmjenu ruta određenog VPN-a između usmjerivača koji su dio VPN-a. Svakoj ruti unutar BGP-a dodjeljuje se preklopni nalog višeprotokolne oznake, odnosno kada BGP distribuira VPN put također se distribuira i MPLS oznaka za tu rutu. To znači da prije nego što paket podataka upućen od strane klijenta putuje preko davatelja usluga, on je enkapsuliran u MPLS oznaku koja odgovora za rutu koja joj se najbolje podudara s odredišnom adresom poslanog paketa. Taj MPLS paket je i dalje dio tunelskog zaglavlja tako da se paket isporučuje tuneliran na odgovarajući usmjerivač. Stoga usmjerivači koji čine jezgru nemaju potrebu za poznavanjem VPN rute. Primarni cilj ovog protokola je podržati slučaj u kojem se klijentu osigurava tražena usluga pri čemu klijent može biti poduzeće ili grupa poduzeća kojem je potreban davatelj dobre virtualne privatne mreže. Klijentu je potrebna fleksibilna usluga koja neće narušiti privatnost i gubitak podataka. [9]

4.1. Virtualne privatne mreže (VPN)

VPN (*engl. Virtual Private Network*) računalna je mreža koja ima funkciju međusobnog povezivanja više mreža koristeći javnu komunikacijsku mrežu - Internet. Mreža spojena u VPN promet šiti od prisluškivanja uz primjenu tehnoloških mrežnih rješenja poput tunelskih protokola i šifriranja. VPN se može koristit prilikom spajanja različitih mreža pa je tako moguće povezati dvije IPv6 mreže preko IPv4 mreže. Povezivanje se može implementirati sklopovski ili programski, ovisno o tome koje su mogućnosti davatelja usluge na zahtjeve klijenata, a najčešće se koristi kombinacija navedenih implementacija. [10]

VPN tehnologijom potrebno je osigurati sljedeće zahtjeve:

- Upravljanje IP adresama – unutar privatne mreže dodjeljuju se klijentske adrese.
- Mehanizmi upravljanja ključevima – VPN osigurava generiranje i osvježavanje ključeva između poslužitelja i klijenata.
- Podršku za razne protokole – standardni protokoli koji su korišteni u javnim mrežama, VPN mora moći podržavati poput IP, IPX i slično. [10]

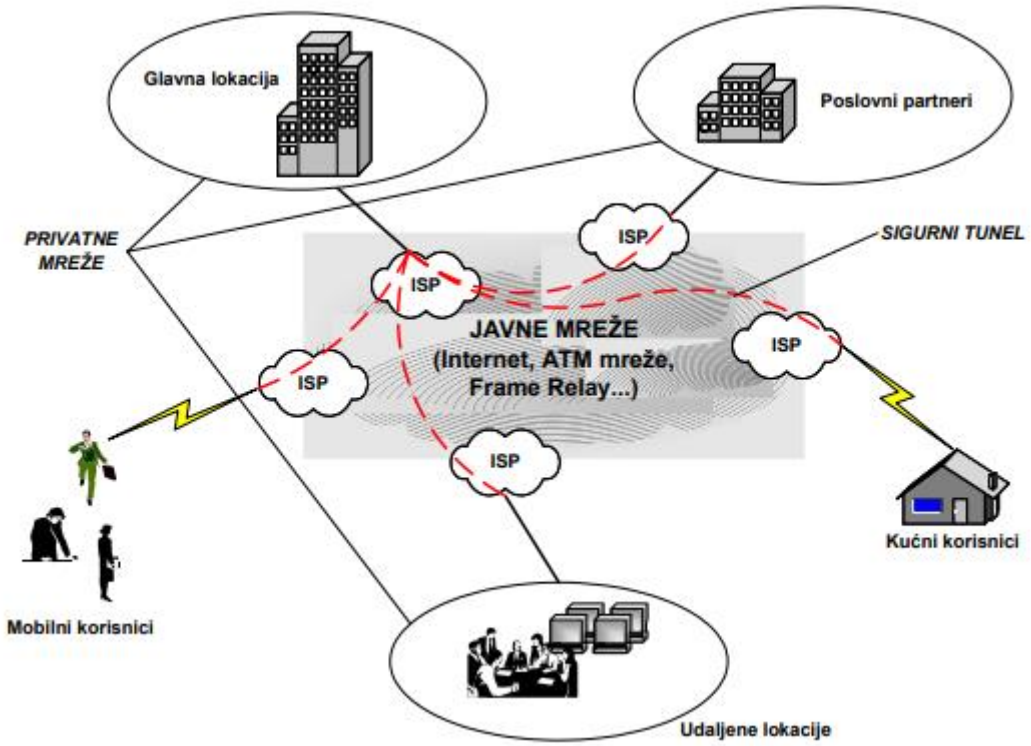
Sigurnosni zahtjev su neizostavni prilikom postavljanja VPN-a, kao što su:

- Pravo pristupa – potrebno je osigurati provjeru identiteta i dopustiti pristup samo korisnicima koji su registrirani, osim navedenog poželjno je osigurati i praćenje događaja (engl. *logging*).
- Autentifikacija i autorizacija – samo svojstvo govori da je potrebno osigurati da korisnik ima potvrđenu informaciju od izvoru primljenog prometa te provjeru korisnika koji je poslao promet u svrhu razvoja sigurnosti da je to stvarno taj korisnik za kojeg se predstavlja.
- Integritet podataka – ovaj zahtjev je osiguran uporabom MD5 algoritma koji provjerava postoje li kakve izmjene na podacima prilikom prolaska kroz mrežu.
- Povjerljivost (tajnost, kriptiranje) – zahtjev je osiguran korištenjem algoritama poput: DES, RSA, Diffie-Hellman. Navedeni algoritmi osiguravaju kriptiranje podataka te ih osim klijenta nitko ne može čitati. [10]

Osim zahtjeva koje je potrebno ispuniti, važno je spomenuti i vrste VPN mreža:

- Intranet VPN – unutar jedne organizacije korištena za povezivanje više lokacije. Prijenos podataka odvija se putem Interneta.
- Ekstranet VPN – povezivanje više različitih organizacija koje mogu biti različite tvrtke ili poslovni partneri. Također se prijenos podataka odvija putem Interneta.
- Udaljeni pristup – služi za povezivanje udaljenih korisnika na lokalnu mrežu organizacije. Povezivanje se odvija preko Interneta pomoću modemske veze. [10]

Sl. 4.1. prikazuje neke od načina korištenja VPN tehnologija. Crvenom crtkanom linijom prikazane su tunelske veze između pojedinih korisnika. Navedeni su različiti korisnici usluga kao što su: kućni korisnici, mobilni korisnici i korisnici na udaljenim lokacijama. Svaki korisnik pridružen je nekoj od privatnih mreža u kojima komuniciraju pomoću tunela te im je prijenos podataka osiguran od prisluškivanja i upadanja drugih korisnika. Osim tunelskog načina komuniciranja vidljivo je da su privatne mreže dio velike javne internetske mreže, a samo stvaranje privatnih mreža odvija se u usmjerivačima gdje se korištenjem određenih protokola stvaraju oznake kojima se upravlja između privatnih mreža.



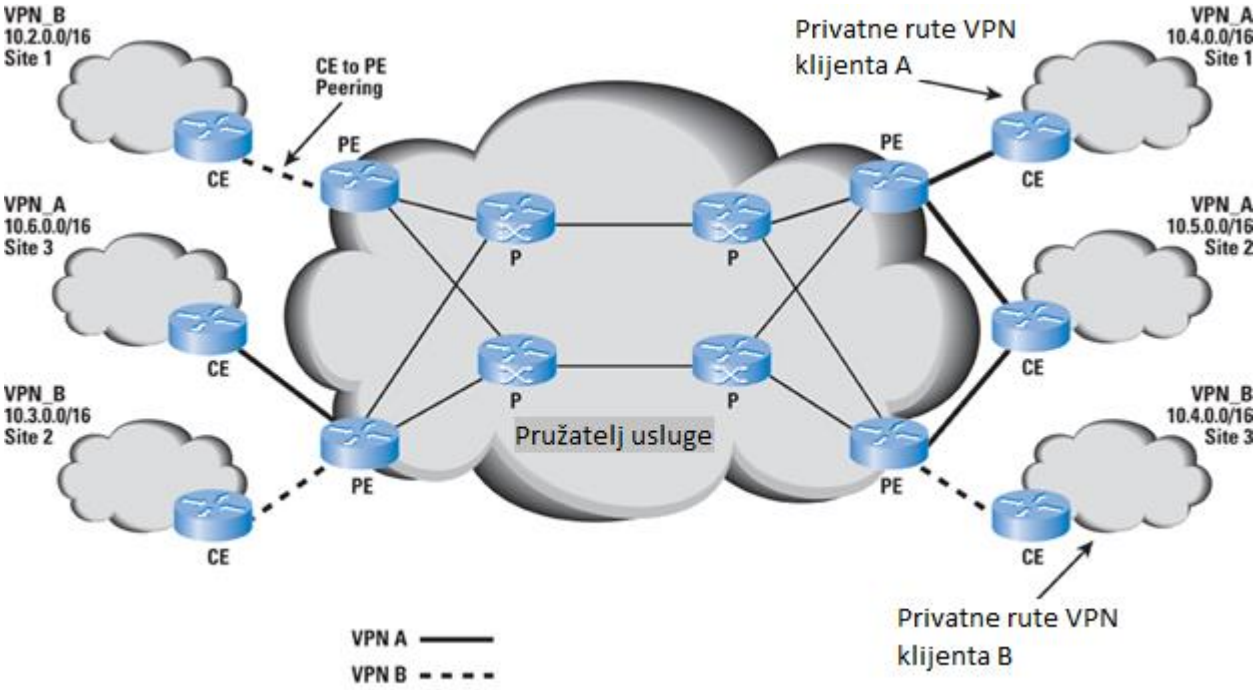
Sl. 4.1. *Prikaz korištenja VPN tehnologija.* [11]

Usmjerivači mogu biti međusobno povezani kao završni sustavi na različite načine: PPP veze, ATM *virtual circuits* (VC), *Frame Relay* VC, *ethernet* sučelje, virtualne lokalne mreže (VLAN) na *ethertnet* sučelja, GRE tunele, *Layer 2 Tunneling Protocol* (L2TP) tuneli, IPsec tuneli i slično. [11]

U daljnjoj obradi ovog rada koristit će se pojam pristupna mreža koji se općenito odnose na rješenja za pristup na usmjerivač. Pristupna mreža može biti vrsta veze koja se obično predstavlja kao podatkovna veza ili može biti neki tunel. Ono što je važno je mogućnost da dva uređaja budu mrežni sloj *peer*-a preko pristupne mreže. Svaka VPN lokacija mora sadržavat jedan ili više uređaja *Customer Edge* (CE). Svaki CE uređaj je priključen putem neke vrste pristupne mreže na jedan ili više usmjerivača *Provider Edge* (PE). Usmjerivači u *Service Providers* (SP) mreži koji ne pridaju CE uređajima poznati su kao P usmjerivači. CE uređaji mogu biti poslužitelji ili usmjerivači. U tipičnom slučaju stranica sadrži jedan ili više usmjerivača, od kojih su neki priključeni na PE usmjerivače. Usmjerivači stranica kojima se pridružuje PE usmjerivač bi tada bili CE uređaji ili CE usmjerivači. [9]

Sl.4.2. prikazuje spajanje pojedinih tipova usmjerivača na mjestima na kojima se trebaju spajati u mreži kako bi se postigao efekt BGP protokola unutar VPN mreža. Vidljivo je da usmjerivači P

tipa tvore okosnicu te se na njih povezuju usmjerivači PE tipa. PE tip kako je već navedeno tvori rubni usmjerivač na koji se povezuju CE usmjerivači koji se nalaze u autonomnim sustavima i poveznica su s okosnicom u kojoj je smješten davatelj usluge.



Sl. 4.2. *Prikaz usmjerivača unutar BGP VPN mreže.* [13]

Međutim, ne postoji ništa što bi spriječilo priključivanje usmjerivača poslužitelja izravno na PE usmjerivač. U tom slučaju poslužitelj bi bio CE uređaj. Ponekad, ono što je fizički priključeno na PE usmjerivač je preklopnik drugog sloja, pri tome treba obratiti pažnju da preklopnik drugog sloja nije CE uređaj. CE uređaji su poslužitelji i usmjerivači koji komuniciraju s PE usmjerivačem preko preklopnika drugog sloja koji je infrastrukturno transparentan. Ako infrastruktura drugog sloja pruži uslugu s više točaka, više PE uređaja može se priključiti PE usmjerivaču preko iste pristupne mreže. CE uređaji logički su dio VPN korisnika, PE i P usmjerivači su logički dio mreže SP-a. Pristupne mreže preko kojih paket putuje kada ide od CE do PE poznat je kao ulazna pristupna mreža, a PE kao paketi ulaznog PE. Pristupna mreža preko koje paketi putuju kada idu iz PE na CE poznata je kao izlazna pristupna mreža i PE kao paketi izlaznog PE. Može se reći kako je PE usmjerivač priključen na određeni VPN ako je priključen na CE uređaj koji je na mjestu tog VPN-a. Slično tomu, PE usmjerivač je priključen na određenu lokaciju ako je priključen na CE uređaj koji je na toj lokaciji. Kada je CE uređaj usmjerivač, on usmjerava *peer* PE na koji je priključen, ali nije usmjerivač *peer* CE usmjerivača na drugim mjestima. Usmjerivači na različitim mjestima neizravno međusobno razmjenjuju informacije o usmjeravanju ali na takav način da se međusobno ne trebaju poznavati. Kao posljedica toga, korisnik nema okosnicu ili virtualnu

okosnicu za upravljanje i ne mora se nositi s pitanjima vezanim za međusobno usmjeravanje. Drugim riječima, u shemi opisanoj u ovom radu, VPN ne predstavlja preklapanje na vrhu SP-a. Obzirom na upravljanje rubnim uređajima, između SP-a i njegovih klijenata održavaju se jasne administrativne granice. Korisnici nisu dužni pristupiti PE ili P usmjerivaču u svrhu upravljanja, niti je SP potreban za pristup CE uređajima u svrhu upravljanja. [9]

SP okosnica se sastoji od PE usmjerivača, kao i drugih usmjerivača, npr. P usmjerivača koji ne pripadaju CE uređajima što je prikazano na sl. 4.2.

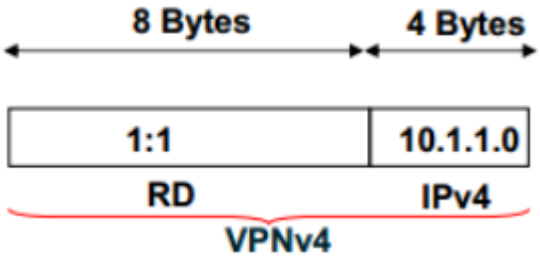
Ako bi svaki usmjerivač u okosnici SP-a morao održavati podatke o usmjeravanju za sve VPN-ove koje SP podržava, postojali bi značajni problemi vezani uz skalabilnost. Broj mjesta koji bi mogao biti podržan bio bi ograničen količinom informacija o rutama usmjeravanja koje bi se mogle pohraniti u jednom usmjerivaču. Stoga je važno da informacije o usmjeravanju određenog VPN-a trebaju biti prisutne samo u PE usmjerivačima koji se pridružuju u VPN-u. Konkretno, P usmjerivači ne moraju imati informacije usmjeravanja za bilo koji VPN. Dakle, baš kao što vlasnici VPN-a nemaju okosnicu ili virtualnu okosnicu za administraciju, SP-ovi nemaju zasebnu okosnicu ili virtualnu okosnicu za administraciju za svaki VPN. Usmjeravanje između različitih mjesta u samoj okosnici je optimalno kada se usmjeravanje odvija unutar ograničenja propisanih pravilima za formiranje VPN-ova. Optimalnost usmjeravanja ni na koji način nije ograničena umjetnom virtualnom topologijom tunela. [9]

4.2. VPN distribucija ruta korištenjem BGP protokola

Kao što je već navedeno u uvodnom dijelu ovog poglavlja VPN koristi BGP protokol za distribuciju ruta. Svakom VPN-u dopušta se vlastiti adresni prostor, što znači da odredišna adresa može označavati različite sustave u različitim VPN-ovima. Ako dvije rute imaju isti prefiks IP adrese to zapravo predstavlja rutu za različite sustave, stoga je važno osigurati da ih BGP ne tretira usporedno. U suprotnom BGP može odabrati samo jednu rutu što označava da drugi sustav neće biti dostupan. Također je bitno osigurati i POLICY koji se koristi za određivanje paketa koji se šalju na pojedinim rutama, s obzirom da postoji više ruta samo jedna se instalira unutar BGP-a te je potrebno koristiti novu listu adresa.

Značajke opisane u 3. poglavlju dopuštaju BGP-u da prenosi rute iz višestrukih adresnih obitelji. Adresne obitelji koje se mogu pojaviti unutar BGP-a su: IPv4, IPv6, L2VPN i adresna obitelj koja je u najvećem dodiru s temom diplomskog rada VPNv4. VPNv4 adresa je veličine 12 bajta od

kojih prvih 8 bajtova predstavlja tzv. *Route Distinguisher* (RD) i posljednja 4 bajta koji predstavljaju IPv4 adresu (Sl.4.3.). Ako nekoliko VPN-ova koristi isti adresni prefiks, PE ih prevodi u jedinstveni VPNv4 adresni prefiks. Takav način rada osigurava, da ako se ista adresa koristi u nekoliko različitih VPN-ova, da BGP može prenijeti nekoliko u potpunosti različitih puteva do te adrese, po jedan za svaki VPN. Budući da su adrese VPNv4 i IPv4 adrese različitih obitelji, BGP ih nikada ne tretira kao usporedive adrese.



Sl.4.3. *Prikaz adrese VPNv4 adresne obitelji.* [14]

RD je broj koji ne sadrži nikakve nerazdvojive informacije te ne identificira podrijetlo rute ili skupa VPN-ova na koje treba distribuirati put. Svrha tog broja je jedino dopustiti da stvorimo različite puteve za zajednički IPv4 prefiks adrese, ali i za stvaranje više različitih ruta za isti sustav. Kako bi put do određenog poslužitelja trebao biti različit za intranetski i ekstranetski promet stvaraju se različite VPNv4 rute koje imaju isti IPv4 dio ali različite RD brojeve. Upravo to stvaranje različitih ruta omogućuje BGP-u da instalira više različitih ruta na isti sustav i dopušta uporabu POLICY da odluči koji paketi koriste koje puteve. RD brojevi su strukturirani tako da svaki davatelj usluga može upravljati vlastitim prostorom za numeriranje, bez sukoba s RD brojevima koje je napravio bilo koji drugi davatelj usluga. RD broj se sastoji od tri polja: tip polje od 2 bajta, administratorsko polje i dodijeljeno polje brojeva. Vrijednost tipa određuje duljinu druga dva polja. Polje administratora identificira dodijeljeni broj ovlasti, a dodijeljeni broj polja sadrži broj kojim je određeno tijelo dodijeljeno u određenu svrhu. RD zapravo ima ovakvu strukturu kako bi se osiguralo da SP koji pruža uslugu VPN okosnice uvijek može stvoriti jedinstveni RD. Međutim, struktura nema smisla u BGP-u, kada BGP uspoređuje dva takva adresna prefiksa, zanemaruje strukturu u cijelosti. [9]

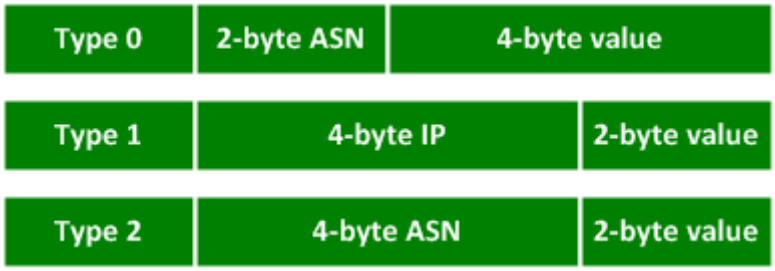
Kodiranje RD broja izvršava se na način da postoji polje tipa duljine 2 bajta i polje vrijednosti duljine 6 bajtova. Tumačenje polja vrijednosti ovisi o vrijednosti polja vrste. Postoje tri vrijednosti polja tipa, a to su: 0, 1 i 2.

Vrijednost tipa 0 podrazumijeva da polje vrijednosti svoju duljinu raspoređuje na sljedeći način: administratorsko podpolje duljine 2 bajta i dodijeljeno podpolje brojeva od 4 bajta.

Administratorsko podpolje sadržava broj autonomnog sustava (ASN). Ako je ASN iz javnog prostora, tada mora biti dodijeljen od strane odgovarajućeg tijela. Dodijeljeni broj sadrži broj prostora za numeriranje kojim upravlja institucija kojoj je dodijeljen ASN od strane odgovarajućeg tijela. [15]

Vrijednost tipa 1 podrazumijeva da polje vrijednosti svoju duljinu raspoređuje na sljedeći način: administratorsko podpolje duljine 4 bajta i dodijeljeno podpolje brojeva od 2 bajta. Administratorsko polje mora sadržavati IP adresu. Ako je IP iz javnog prostora, tada mora biti dodijeljen od strane odgovarajućeg tijela. Dodijeljeni broj sadrži broj prostora za numeriranje kojim upravlja institucija kojoj je IP adresa dodijeljena. [15]

Vrijednost tipa 2 podrazumijeva da polje vrijednosti svoju duljinu raspoređuje na sljedeći način: administratorsko podpolje duljine 4 bajta i dodijeljeno podpolje brojeva od 2 bajta. Administratorsko podpolje mora sadržavati 4 bajta ASN. Ako je ASN iz javnog prostora, tada mora biti dodijeljen od strane odgovarajućeg tijela. Dodijeljeni broj sadrži broj prostora za numeriranje kojim upravlja poduzeće kojem je dodijeljen ASN od strane odgovarajućeg tijela. [15]



Sl.4.4. *Route Distinguisher broj s pojedinim tipovima.* [16]

Nakon svega postavlja se pitanje kako kontrolirati distribuciju ruta. Ako je PE usmjerivač postavljen za određeni VPN, što znači da je priključen na određeni CE u tom VPN-u, uči neke od IP ruta VPN-a iz priloženog CE usmjerivača. Rute naučene od priključenog CE usmjerivača preko određene spojene mreže mogu se instalirati u VRF koji je povezan s tom mrežom. Upravo ono što se na taj način instalira određuje način na koji PE uči putove iz CE. Konkretno, kada PE i CE usmjeravaju protokol *peer*-a, to se određuje procesom odlučivanja protokolom usmjeravanja. Naučene rute se zatim pretvaraju u VPNv4 rute i izvoze u BGP. Ako postoji više od jedne rute na određeni adresni prefiks VPNv4, BGP odabire najbolju pomoću procesa odlučivanja u BGP-u. Taj put distribuira BGP na skup drugih PE-ova koji trebaju znati za rutu. U tim drugim PE-ovima BGP će ponovo odabrati najbolju rutu za određeni adresni prefiks VPNv4. Zatim se odabrane VPNv4 rute pretvaraju natrag u IP rute i uvoze u jedan ili više VRF. Bez obzira na to jesu li oni zapravo

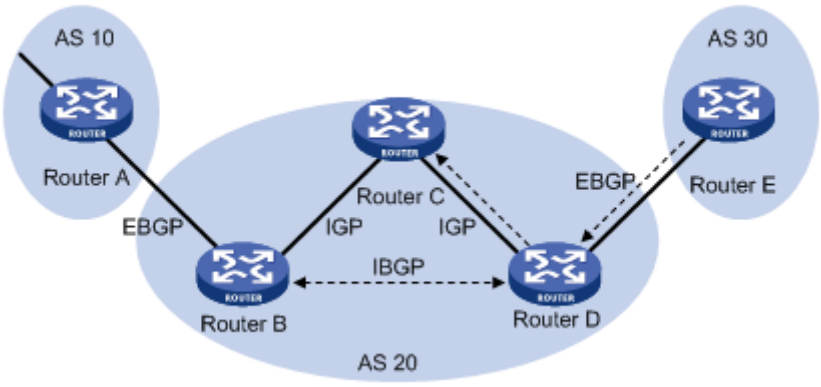
instalirani u VRF-ovima, ovisi o procesu odlučivanja i načinu usmjeravanja koji se koristi između PE i onih CE koji su povezani s predmetnim VRF-om. Konačno, svaka ruta instalirana u VRF može se distribuirati pripadajućim CE usmjerivačem. [9]

Svaki VRF je povezan s jednim ili više *Route Target* (RT) atributa. Kada je kreirana VPNv4 ruta iz IP rute koju je PE naučio iz CE onda je povezana s jednom ili više RT atributa te se prenose u BGP-u kao atributi puta. Svaka ruta koja je povezana s RT mora se distribuirati svakom PE usmjerivaču koji ima VRF povezan s odredištem rute. Kada je takva ruta primljena od strane PE usmjerivač, može se instalirati u one koji pripadaju VRF-ovima koji su povezani s RT. Atribut cilja rute može se smatrati identifikacijom skupa VRF-ova. Povezivanje određenog atributa rute s rutom omogućuje se da se ruta stavi u VRF koji se koristi za usmjeravanje prometa koji je primljen s određenih VRF-ova. Postoji skup ciljeva ruta koje PE usmjerivač pridaje putu primljenog sa stranice A, koje se mogu nazvati izvozni ciljevi. I postoji skup ciljeva ruta koje PE usmjerivač koristi kako bi utvrdio može li se ruta primljena od drugog PE usmjerivača staviti u VRF povezanu s stranicom A, a njih nazivamo uvozni ciljevi. Dva skupa su različita i ne moraju biti isti. Određena VPNv4 ruta ispunjava uvjete za instalaciju u određenom VRF-u ako postoji neki cilj rute koji je jedan od ciljeva RT i jedan od VRF-ovih uvoznim ciljeva. Funkcija koju obavlja atribut cilja rute sličan je onome koji provodi atribut BGP zajednica. Međutim, format nije adekvatan za trenutne potrebe, jer dopušta samo prostor numeriranja od 2 bajta. Poželjno je oblikovanje formata, slično onome što je opisano za RD. Tako da polje vrste definira duljinu polja administratora, a ostatak atributa je broj iz navedenog administratorskog brojčanog prostora. To se može učinit pomoću BGP proširenih zajednica. Ovdje navedeni ciljevi rute kodiraju se kao BGP *Extended Comunity Route Targets*. Oni su strukturirani slično kao i RD. Kada BGP prijemnik primi više od jedne rute na isti VPNv4 predbroj, BGP pravila za odabir rute koristi se za odabir VPNv4 rute koju je instalirao BGP. Važno je razumjeti da ruta može imati samo jedan RD, ali može imati više ciljeva. U BGP-u skalabilnost se poboljšava ako je jedan put s višestrukim atributima, za razliku od višestrukih ruta. Jedan bi mogao ukloniti atribut rute stvaranjem više ruta, odnosno korištenjem više RD-ova, ali bi skalabilna svojstva mogla oslabiti. [9]

Važno je razumjeti razliku između RD i RT. RD unutar BGP-a čini VPNv4 adresu jedinstvenu, dok RT definira koji prefiks se uvozi a koji izvozi na PE usmjerivače. [17]

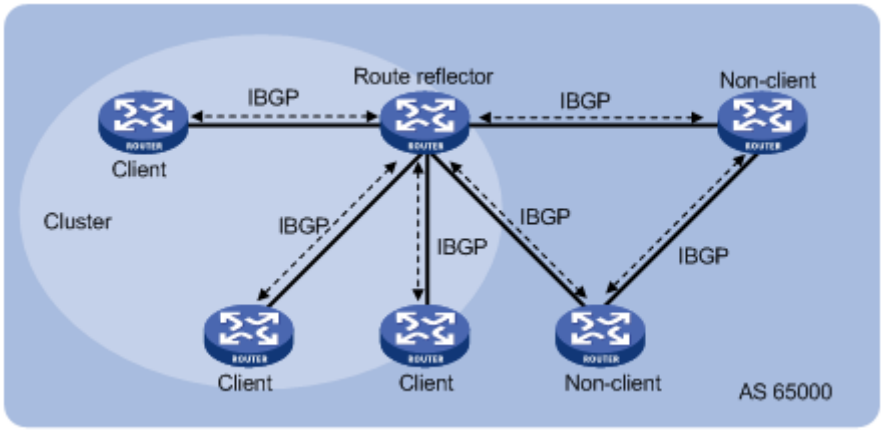
Distribucija ruta između PE-ova pomoću BGP-a opisana je unutar ovog odjeljka. Ako su dvije stranice unutar VPN-a priključene na PE koji su dio istog AS, tada PE-ovi mogu distribuirati VPNv4 rute jedni drugima putem IBGP veze između njih. Izraz IBGP u ovom slučaju se odnosi

na skup protokola i postupaka koji se koristi kada postoji BGP veza između dva BGP prijemnika u istom AS-u, a razlikuje se od EBGP koji predstavlja skup postupaka i protokola koji se koriste između dva BGP prijemnika u različitim AS (sl.4.5.).



Sl.4.5. *Razlika prilikom razmjena ruta putem IBGP i EBGP* [18]

Alternativno, svaki IBGP može imati vezu na reflektor rute (sl.4.6.). Kada PE usmjerivač distribuira VPNv4 rutu putem BGP-a, koristi svoju adresu kao BGP sljedeći skok. Ova adresa je kodirana kao VPNv4 adresa s RD tipom 0. BGP zahtjeva da adresa sljedećeg skoka bude u istoj adresnoj obitelji kao i NLRI. Dodjeljuje se i distribuira oznaka MPLS jer u osnovi PE usmjerivač ne distribuira VPNv4 rute nego VPNv4 označene rute, u praksi poznatije kao labele. Kada PE obrađuje primljeni paket koji ima labelu u vrhu stoga, PE će izbaciti paket iz stoga i obraditi ga na odgovarajući način.



Sl.4.6. *Svi usmjerivači imaju vezu sa reflektorom ruta.* [18]

Pretpostavimo da je PE dodijelio labelu L na rutu R i distribuirao mapu labela putem BGP-a. Ako je R agregat skupa ruta u VRF-u, PE će znati da paketi iz okosnica koji stignu s tom labelom moraju imati odredišne adrese unutar VRF-a. Kada PE pogleda labelu u svojoj informacijskoj bazi podataka, saznati će koji se VRF mora koristiti. Ako pak R nije agregat, tada PE pogleda labelu,

uči mrežu na kojoj je priključen za izlaz, kao i zaglavlje za enkapsulaciju paketa. U tom slučaju nema pretraživanja VRF-a. Prilikom uporabe BGP distribuiranih MPLS labela na ovaj način, pretpostavlja se da MPLS paket koji nosi takvu labelu može biti tuneliran od strane usmjerivača koji instalira odgovarajući BGP distribuirani put do usmjerivača koji je unutar BGP-a sljedeći skok na tom putu. To zahtjeva ili da između ta dva usmjerivača postoji labela koja se prebacuje između njih ili ako se između njih koristi nekad druga tehnologija tunela. Tunel može pratiti najbolji moguć put ili može slijediti put kojim se razmjenjuje promet. Između danog para usmjerivača može postojati jedan ili više takvih tunela. Ukoliko je riječ o više tunela, tada se podrazumijeva različita značajka kvalitete usluge. Sve što je važno za VPN arhitekturu je da postoj takav tunel. Kako bi se osigurala interoperabilnost među sustavima koji implementiraju ovu VPN arhitekturu pomoću MPLS labela prebacivanja puteva kao tehnologije tunela, svi takvi sustavi moraju podržaviti *Label Distribution Protocol* (LDP). LDP protokol u suštini služi za razmjenu labela. Ako tunel prati najbolji moguć put, PE pronalazi put do udaljene krajnje točke gledanjem svoje IP adrese u zadanoj tablici za prosljeđivanje. PE usmjerivač, ukoliko nije reflektor rute ili ASBR za VPN davatelja, ne smije instalirati VPNv4 rutu, osim ako nema najmanje jedan VRF s ciljem uvoza koji je identičan jednom od atributa RT na ruti. Ulazno filtriranje treba koristiti za uzorkovanje odbacivanja takvih ruta. Ako je novi cilj za uvoz kasnije dodan u jedan od VRF-ova, PE usmjerivač mora pronaći rute koje je prethodno odbacio. To se može učiniti pomoću mehanizma osvježavanja koji je opisan kao BGP-RFSH. Slično tome, ako određeni cilj za uvoz više nije prisutan u bilo kojem od VRF-ova, PE može odbaciti sve rute koje kao rezultat nemaju više od ciljanih ciljeva za uvoz VRF-a kao jedan od njegovih RT atributa. Usmjerivač koji nije priključen na bilo koji VPN i koji nije reflektor rute, nikada ne instalira nikakve VPNv4 rute. Kao rezultat tih pravila distribucije, ni jedan PE nikad ne treba održavati sve puteve za sve VPN-ove, što je važno za razmatranje skalabilnosti. [9]

Umjesto da ima kompletnu IBGP mrežu među PE-ovima, korisno je koristiti BGP reflektore ruta za poboljšanje skalabilnosti (sl. 4.6.). Dostupne su sve uobičajene tehnike korištenja reflektora ruta za poboljšanje skalabilnosti. Reflektori ruta jednini su sustavi koji trebaju imati informacije o usmjeravanju za VPN mreže na koje nisu izravno priključeni. Međutim, nema potrebe da neki reflektori za rutu zna sve VPNv4 rute za sve VPN-ove koje podržava okosnica. Reflektori ruta mogu imati dva načina dijeljena unutar skupa VPNv4 ruta:

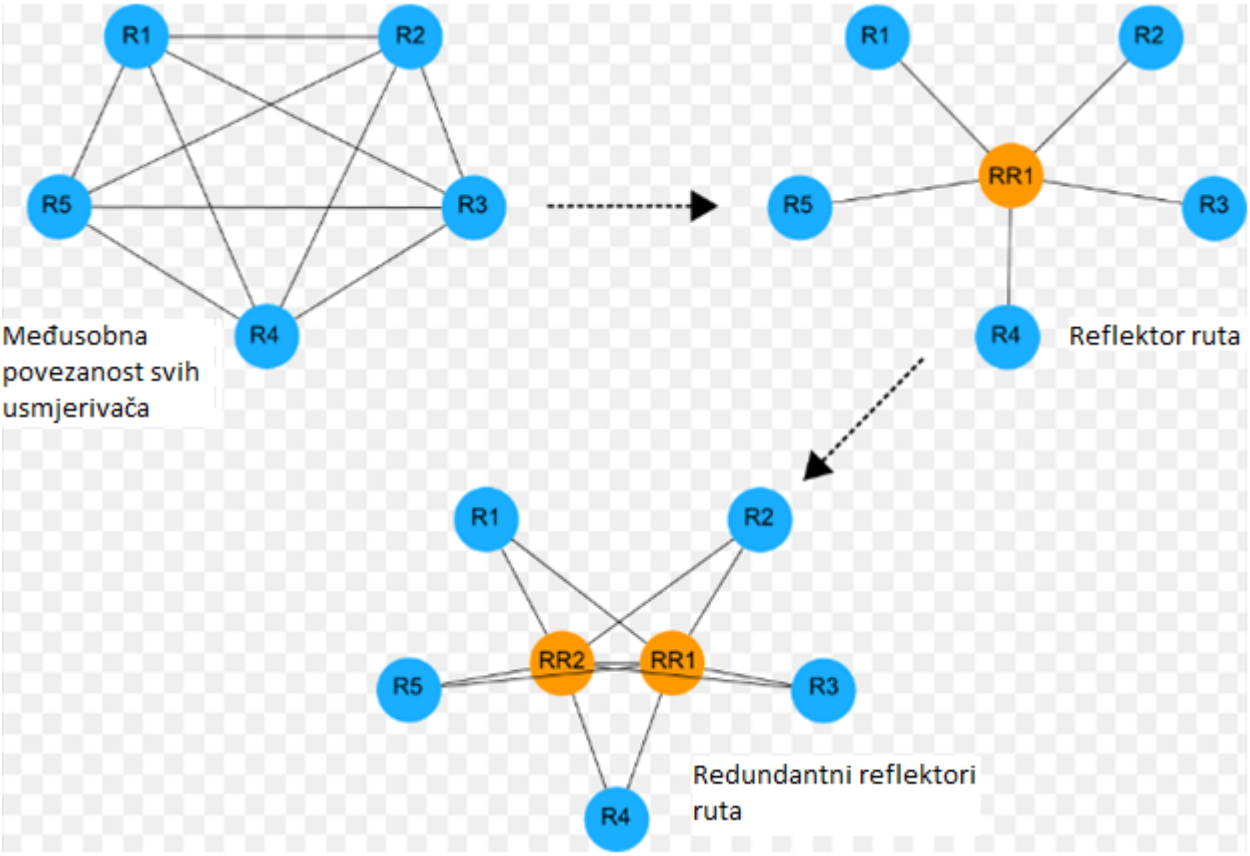
1. Svaki reflektor rute unaprijed je konfiguriran s popisom RT. Za redundantnost, može se unaprijed odrediti više od jednog reflektora ruta s istim popisom. Reflektor rute koristi unaprijed konfigurirani popis RT-a za izgradnju filtriranog ulaznog puta. Reflektor rute može koristiti

tehnike BGP-ORF za instalaciju skupa ORF-a (*Outbound Route Filters*) koji sadrže popis unaprijed konfiguriranih RT-a na svaki od njegovih *peer*-a (bez obzira je li taj *peer* drugi reflektor rute ili PE). Reflektori ruta moraju prihvatiti ORF-ove od drugih reflektora, što znači da reflektori rute trebaju oglašavati sposobnost ORF-a drugim reflektorima ruta. Davatelj usluga može izmijeniti popis unaprijed konfiguriranih RT-a na reflektoru rute. Kada se to učini, reflektor rute mijenja ORF-ove koji se instaliraju na svim svojim IBGP *peer*-ovima. Kako bi se smanjila učestalost promjena konfiguracija u reflektorima rute, svaki reflektor rute može se unaprijed odrediti blokom RT-a. Na taj način, kada je potreban novi RT za novi VPN, već postoji jedan ili više reflektora rute koji su unaprijed konfigurirani s tim RT-om. Osim ako je određeni PE klijent svih reflektora ruta, kada se novi VPN dodaju u PE, morat će postati klijent reflektora rute koji održavaju rute za taj VPN. Isto tako brisanje postojećeg VPN-a iz PE može rezultirati situacijom u kojoj PE više ne mora biti klijent nekih reflektora ruta. U oba navedena slučaja, rad pridruživanja ili brisanja nije ometan sve dok se koristi BGP-RFSH i nikada ne zahtjeva se prekine BGP veza već ju samo uspostavlja. [9]

2. Drugi način je da svaki PE bude klijent nekog podskupa Reflektora ruta. Reflektor rute nije unaprijed konfiguriran popisom RT-a i ne obavlja filtriranje rute puteva primljenih od svojih klijenata, već prihvaća sve putove primljene od svih svojih klijenata tj. PE-a. Reflektor ruta prati skup RT-a koji se prenose putovima koje prima. Kada reflektor rute primi od svog klijenta rutu s RT-om koja nije u skupu, taj RT se odmah dodaje u skup. U suprotnom slučaju, kada reflektor rute više nema rutu s određenim RT, reflektor rute započinje brisanje koje prvo odgodi najčešće za nekoliko sati, a zatim ako se ruta ne koristi tada dolazi do brisanja RT-a iz skupa. Reflektor ruta koristi skup za formiranje filtra za ulazni put koji se primjenjuje na rute primljene od drugih reflektora ruta. Reflektor ruta također može koristiti ORF-ove za instalaciju odgovarajućeg filtriranja rute na drugim reflektorima ruta. Reflektor ruta oglašava ORF sposobnost drugim reflektorima ruta kako bi se postiglo prihvaćanje ORF-ova od drugih reflektora ruta, slično kao i u prvom pristupu. Kad reflektor rute promjeni skup treba odmah promijeniti i filtriranje ulaznog puta. Osim toga, ako reflektor rute koristi ORF tada se ORF-ovi moraju promijeniti kako bi održavali promjene u skupu. Ako reflektor rute ne upotrebljava ORF u skupinu se dodaju novi RT-ovi, reflektor rute nakon što promijeni ulazno filtriranje ruta, mora izdati BGP-RFSH na druge reflektore ruta. Spomenuta odgoda od nekoliko sati omogućuje reflektoru rute da se drži na putovima s određenim RT, čak i nakon što izgubi posljednjeg klijenta s te rute. Prava smisao odgode je zaštita od ponovnog stjecanja rute ako je nestanak klijenta privremen. Također i u ovom slučaju operacije pridruživanja i brisanja nije ometan. Važno je primijetiti da ova tehnika neće

ispravno funkcionirati ukoliko neki klijent PE ima VRF s uvoznom RT koja nije ista kao i izlazna RT. [9]

U navedenim postupcima dijeljenja ruta u reflektorima ruta, PE usmjerivač koji pristaje na određeni VPN automatski otkriva druge PE koji se vežu na isti VPN. Kada se doda novi PE usmjerivač ili kada se postojeći PE usmjerivač pridruži novom VPN-u nije potrebno konfigurirati PE usmjerivače. Baš kao što ne postoji jedna PE usmjerivač koji treba znati sve VPNv4 rute podržane preko okosnice, takva distribucijska pravila osiguravaju da niti jedan reflektor ruta ne mora znati sve VPNv4 rute podržane preko okosnice. Kao rezultat toga ukupan broj takvih ruta koji se mogu podržati preko okosnice nije ograničen kapacitetom bilo kojeg uređaja, stoga se može povećavati bez ograničenja (sl.4.7.).



Sl. 4.7. *Prikaz smanjenja ruta korištenjem reflektora rute.* [12]

Višeprotokolna proširenja unutar BGP-a (BGP-MP) koriste se za kodiranje NLRI. Ako je polje AFI postavljeno na 1 i polje SAFI postavljeno na 128, tada NLRI ima značenje MPLS-labela VPNv4 adresa. Polje AFI 1 se koristi jer je protokol mrežnog sloja povezan s NLRI još uvijek IP. Vrlo važno je razumjeti da VPN arhitektura ne zahtjeva mogućnost distribucije VPNv4 adresa koje nemaju labelu. Kako bi dva BGP prijemnika mogli razmijeniti labele VPNv4 NLRI, moraju

koristiti BGP sposobnost oglašavanja, kako bi se osiguralo da su obje strane sposobne obraditi takav NLRI. Oglašavanje je načinjeno kako je navedeno u BGP-MP pomoću koda 1, s AFI 1 i SAFI 128.

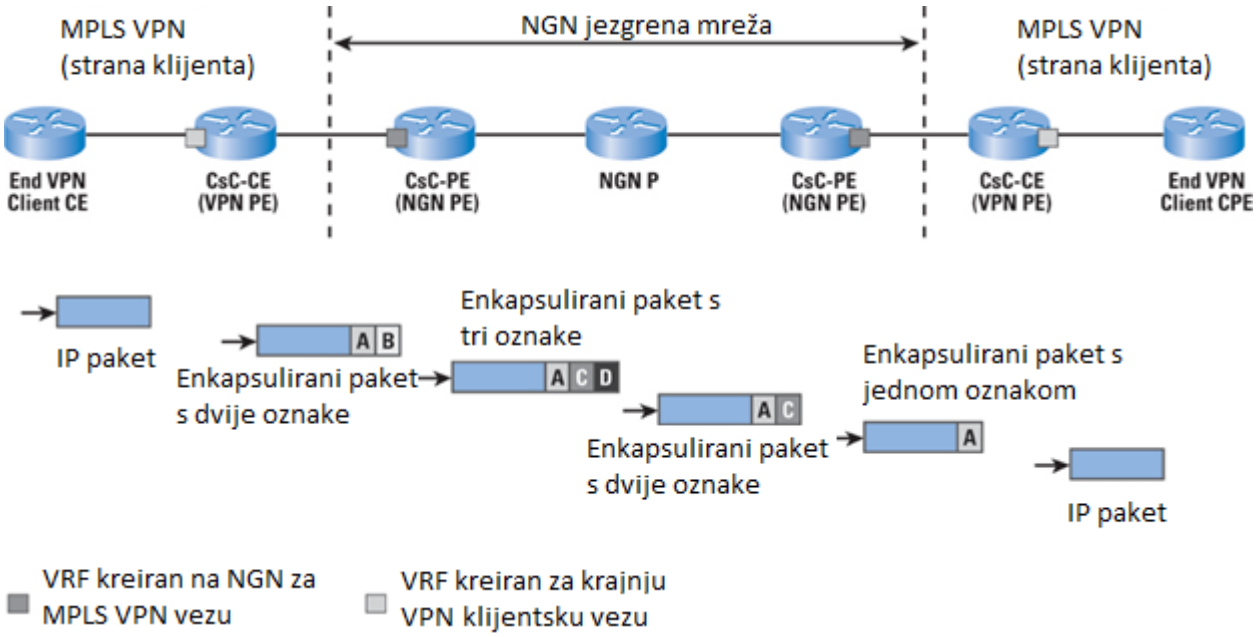
Pravilnim postavljanjem ulaznih i izlaznih ciljeva moguće je postavljanje različitih vrsta VPN-a. Pretpostavka je da se želi stvoriti potpuno zatvorena skupina korisnika odnosno skup mjesta na kojima svaki korisnik može poslati promet izravno na drugi, ali promet se ne može poslati niti primati s drugih mjesta. Zatim se svako mjesto poveže s VRF-om, odabere se RT koji će biti dodijeljen svakom VRF-u kao ulazni i izlazni cilj i RT ne može biti dodijeljen bilo kojem drugom VRF-u van ove skupine. Stoga su metode za kontrolu distribucije informacija o usmjeravanju između različitih skupova vrlo fleksibilne, što zauzvrat pruža veliko fleksibilnost pri izgradnji VPN-ova.

Moguće je distribuirati putove s jednog VRF-a na drugi, čak i ako su oba VRF-a u istom PE, iako u tom slučaju ne možemo reći da je put distribuirao BGP. Ipak, odluka o raspodjeli određenog puta s jednog VRF-a na drugi unutar jednog PE je ista odluka koja bi bila napravljena u slučaju da su VRF-ovi bili na različitim PE. Što pak znači da sve to ovisi o RT atributu koji se dodjeljuje ruti, i uvoznom cilju drugog VRF-a. [9]

4.3. Prosljeđivanje paketa između VPN stanica

U ovom dijelu rada biti će pojašnjeno kako se prosljeđuju paketi s jedne VPN stanice na drugu ako se vodi činjenicom da usmjerivači u okosnicama nemaju informacije o rutama VPN mreža. Kada PE primi IP paket iz CE uređaja, on odabire odredišni VRF u kojem će potražiti odredišnu adresu paketa. Izbor VRF-a temelji se na pridruženoj mreži paketa. Uz pretpostavku da je VRF nađen, kao rezultat pronalaska PE nauči koji je sljedeći skok primljenog paketa. Ako je sljedeći skok paketa izravno dosegnut preko VRF-a priključenog na mrežu navedenom PE-a, tada se paket šalje na mrežu za priključivanje i MPLS labele se ne stavljaju na stog labela navedenog paketa. Ako su mreže za ulaz i izlaz na istom PE, ali su povezani s različitim VRF-ovima te ruta najbolje odgovara odredišnoj adresi, u sklopu priključene mreže VRF-a je skup od nekoliko ruta u privitku izlaznog sklopa VRF-a (sl.4.8.). Stoga je potrebno potražiti odredišnu adresu paketa u izlazu VRF-a. Ako sljedeći skok paketa nije dosegnut kroz VRF priključnu mrežu, tada paket mora putovati barem jednim skokom kroz okosnicu. Paket tako ima *BGP Next Hop* i taj sljedeći skok u BGP-u će imati dodijeljenu labelu za rutu koja najbolje odgovara paketna odredišna adresa. Naziv

te labele je *VPN route label*. IP paket pretvara se u MPLS paket s labelom VPN ruta kao jedina labela na stogu. Paket se zatim mora tunelirati u *BGP Next Hop*. [13]



Sl.4.8. *Enkapsulacija IP paketa u različite oznake.* [13]

Ukoliko okosnica podržava MPLS način rada, tada dolazi do sljedećeg:

- PE usmjerivači koji redistribuiraju VPNv4 adrese trebaju umetnuti '/32' prefikse adresa u svoje IGP tablice usmjeravanja okosnice, što omogućuje MPLS. Na svakom čvoru mreže okosnice dodjeljuje se labela koja odgovara putu svakog PE usmjerivača. Kako bi se osigurala interoperabilnost između različitih implementacija, potrebno je zadržati LDP za postavljanje označenih staza preko okosnice. Također su moguće i druge metode postavljanja labela koje su načelno promjenjive.
- Ako postoje neki tuneli za prometno inženjerstvo do BGP sljedećeg skoka, i ako je jedan ili više njih dostupno za upotrebu odabranog paketa, odabire se jedan od tih tunela. Odabrani tunel bit će povezan s oznakom MPLS, tj. labelom tunela. Labela tunela potisnuta je na MPLS stog labela i paket se prosljeđuje na sljedeći skok tunela.
- U suprotnom se pojavljuju u nastavku navedene stvari. Paketi će imati IGP sljedeći skok koji je sljedeći skok duž IGP rute do BGP sljedećeg skoka. Ako su BGP sljedeći skok i IGP sljedeći skok isti, te ako se koristi ponavljanje skoka, paket se šalje u IGP sljedeći skok koji nosi samo labele VPN rute. IGP sljedeći skok će dodijeliti labelu za rutu koja najbolje odgovara adresi BGP sljedećeg skoka. Navedena labela imat će naziv

labele tunela koja će biti postavljena na vrh stoga labela navedenog paketa. Paket se zatim prosljeđuje na IGP sljedeći skok.

- MPLS će prenijeti paket preko okosnice na BGP sljedeći skok, gdje će se pregledati VPN labela. [9]

Ako okosnica ne podržava MPLS, MPLS paket koji nosi samo labelu VPN rute može biti u tunelu na BGP sljedećem skoku korištenje tehnika *MPLS-in-IP-GRE*. Kada paket izađe iz tunela, bit će na BGP sljedećem skoku, gdje će se ispitati VPN labela. Na odredištu BGP sljedećeg skok, tretman paketa ovisi o labeli VPN ruta. U mnogim slučajevima, PE će moći odrediti iz primljene labele priključnu mrežu preko koje se paket treba prenijeti na CE uređaj, osim mreže može odrediti i pravilno zaglavlje sloja s podatkovnom vezom za odredišno sučelje. U drugim slučajevima, PE može samo biti u mogućnosti utvrditi da se odredišna adresa paketa mora potražiti u određenom VRF-u prije nego što bude proslijeđena CE uređaju. Postoje i srednji slučajevi u kojim labela VPN-a može odrediti mrežu za privitak izlaznog paketa, ali treba još obaviti pretraživanje kako bi se odredilo zaglavlje podatkovne veze paketa na toj priključnoj mreži. Informacije u samom zaglavlju MPLS-a koje su povezane s informacijama o labelama mogu se koristiti za određivanje kvalitete usluge na CE sučelju. U svakom slučaju, ako paket nije imao IP labelu kada je stigao na ulaz PE, takav će biti i na izlazu sučelja. Činjenica da paketi s VPN labelama ruta su tunelirani kroz okosnicu što omogućava vođenje svih VN puteva iz P usmjerivača, te postaje ključ za osiguranje skalabilnosti sheme. Okosnica ne mora imati rute za CE, već samo za PE.

S obzirom na tunele, važno je razlikovati sljedeće specifikacije:

- Izbjegavati korištenje tunela od točke do točke (*point-to-point*), moguće je koristiti više točaka prema jednoj (*multipoint-to-point*)
- Izbjegavati eksplicitno postavljanje tunela, bilo putem signalizacije ili putem ručne konfiguracije
- Izbjegavati signalizaciju koja je specifična za tunel
- Izbjegavati da u usmjerivaču P ili PE postoji stanje specifično za tunel, osim onoga koji je potreban za održavanje informacija o usmjeravanju, i informacije o MPLS labelama.

Iako ova je specifikacija kompatibilna s korištenjem tunela *point-to-point* koja se mora eksplicitno konfigurirati te u nekim situacijama može postojati i razlog upravo korištenja takvih tunela koje bi trebali izbjegavati. Razmatranja koja su relevantna za odabir određene tehnologije tunela izvan su opsega ove specifikacije. [9]

4.4. Održavanje ispravnog razdvajanja VPN mreža

Za održavanje ispravnog razdvajanja (engl. *isolation*) jednog VPN-a od drugog, važno je da niti jedan usmjerivač u okosnici ne prihvati neprepoznatljiv paket izvan okosnice, osim ako nije siguran da su obje krajnje točke tog tunela izvan okosnice. Ako se MPLS koristi kao tehnologija tunela, to znači da usmjerivač u okosnici ne smije prihvatiti paket s labelom od bilo kojeg susjednog uređaja koji nije iz okosnice, osim ako ne zadovoljava sljedeće dva uvjeta:

1. labela na vrhu stoga je distribuirana od tog usmjerivača okosnice za taj uređaj koji nije dio okosnice, i

2. usmjerivač okosnice može utvrditi kako će uporaba te labele uzrokovati to da paket napusti okosnicu prije nego što se pregledaju labele niže u stogu i prije nego što se pregledaju IP zaglavlja.

Prvi uvjet osigurava da sve pakete s labelom dobivene od usmjerivača van okosnice imaju legitimno i ispravno dodijeljenu labelu na vrhu stoga. Drugi uvjet osigurava da usmjerivači okosnice nikada neće pogledati ispod labele koja je na vrhu. Naravno, najjednostavniji način za ispunjavanje ova dva uvjeta je samo da se okosnica ne odriče prihvaćanja paketa s labelom od uređaja koji nisu dio okosnice. Ako se MPLS ne koristi kao tehnologija za tuneliranje, potrebno je napraviti filtriranje kako bi se osiguralo da *MPLS-in-IP* ili *MPLS-in-GRE* paketu mogu biti prihvaćeni u okosnicu samo ako će IP adresa odredišta paketa uzrokovati slanje izvan okosnice. [9]

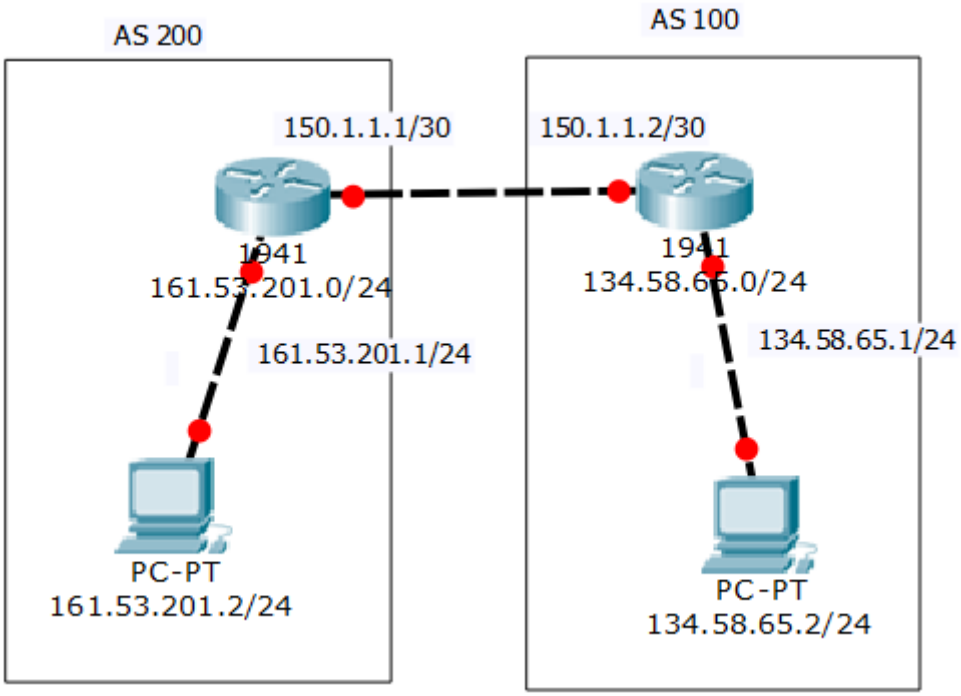
5. KONFIGURACIJE PRAKTIČNOG DIJELA

U ovom poglavlju rada prikazana su dva praktična primjera vezana uz primjenu BGP protokola. Prvi primjer prikazuje rad BGP protokola u jednostavnijoj mreži u kojoj je ostvarena komunikacija između dva računala koja se nalaze u različitim autonomnim sustavima. Drugi primjer prikazuje rad BGP protokola između dva sustava koji se nalaze u jednom VPN-u.

5.1. Konfiguracija topologije za osnovni rad BGP-a

Prema slici 5.1. sastavljena je topologija koja će prikazati osnovni rad BGP-a između dva računala u različitim autonomnim sustavima. U postavljenoj topologiji korištena su: dva računala, dva usmjerivača i *patch* kabeli. Ovim primjerom prikazan je samo jedan dio potrebne mrežne konfiguracije, a kako bi s omogućio ispravan rad BGP-a potrebno je, uz ispravno adresiranje uređaja, provesti odgovarajuću konfiguraciju uređaja u MPLS jezgrenom dijelu mreže što je primijenjeno u drugom primjeru.

Korišteni usmjerivač hAP lite TC opremljen je s snažnim procesorom brzine 650 MHZ, 32 MB radne memorije, dva lanca 2.4 GHZ bežičnog pristupa, četiri brza Ethernet porta, RouterOS L4 licencu i USB napajanje. [19]

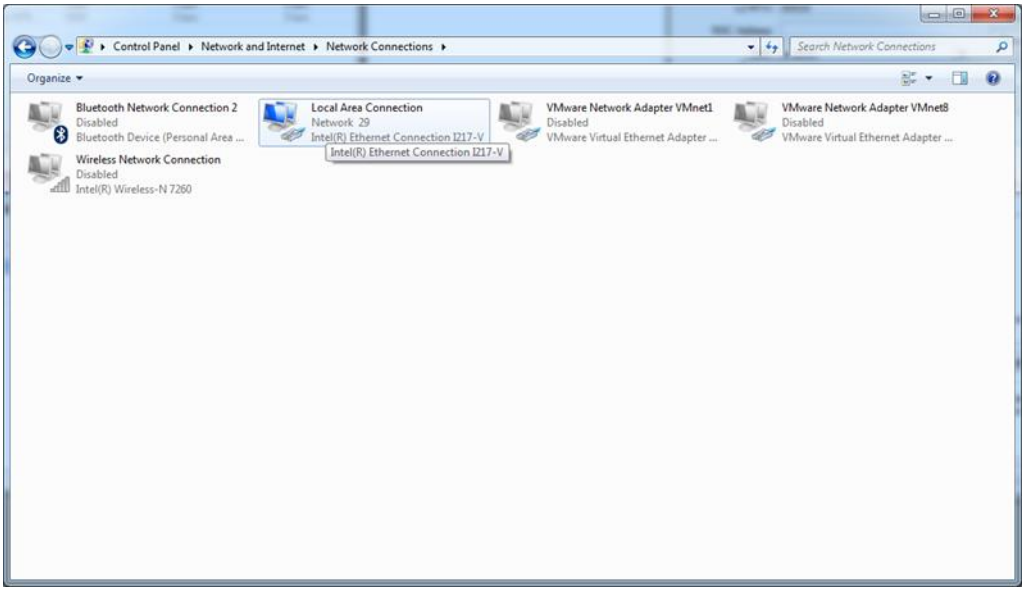


Sl. 5.1. *Mrežna topologija za prikaz rada BGP-a.*

Nakon što je sastavljena topologija, onemogućene su sve mrežne lokacije na računalima osim LAN-a i postavljene su fiksne IP adrese na računalima.

Isključivanje mrežnih sučelja odrađuje se na sljedeći način:

Control Panel -> Network and Sharing Center -> Change Adapter Settings -> desni klik na sve mrežne adaptere osim LAN *-> Disable* (sl.5.2.)

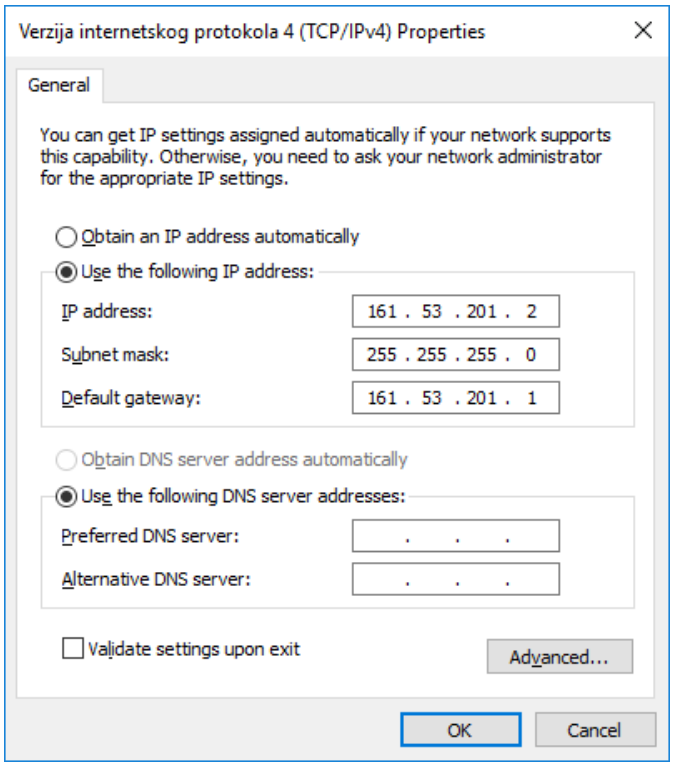


Sl. 5.2. *Isključivanje mrežnih uređaja.*

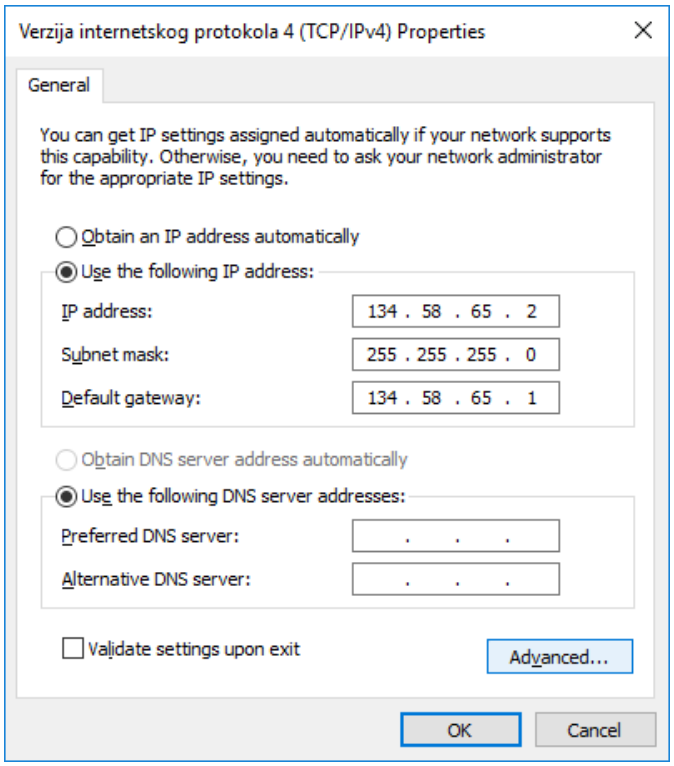
Put do postavki IP adresa je sljedeća:

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

U postavkama je potrebno ispuniti tri polja. Prvo polje *IP address* odnosi se na željenu IP adresu računala. Drugo polje *Subnet mask* predstavlja masku mreže koja označava podjelu IP adresa unutar mreže u ovom slučaju odabrana maska je 255.255.255.0 što označava CIDR prefiks /24. Prefiks /24 označava da će duljina mrežnog dijela zauzeti 24 bita, te preostalih 8 bitova je ostavljeno za računalni dio. Treće polje *Default gateway* predstavlja adresu porta na koji je računalo spojeno.



Sl. 5.3. *Postavljanje stalne IP adrese računala u prvom autonomnom sustavu.*

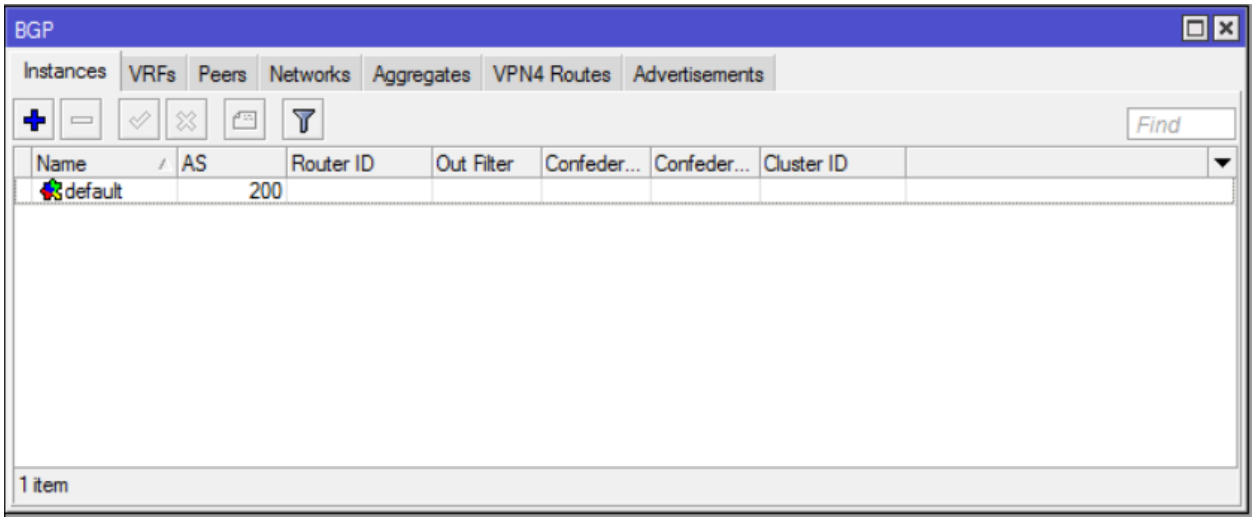


Sl. 5.4. *Postavljanje stalne IP adrese računala u drugom autonomnom sustavu.*

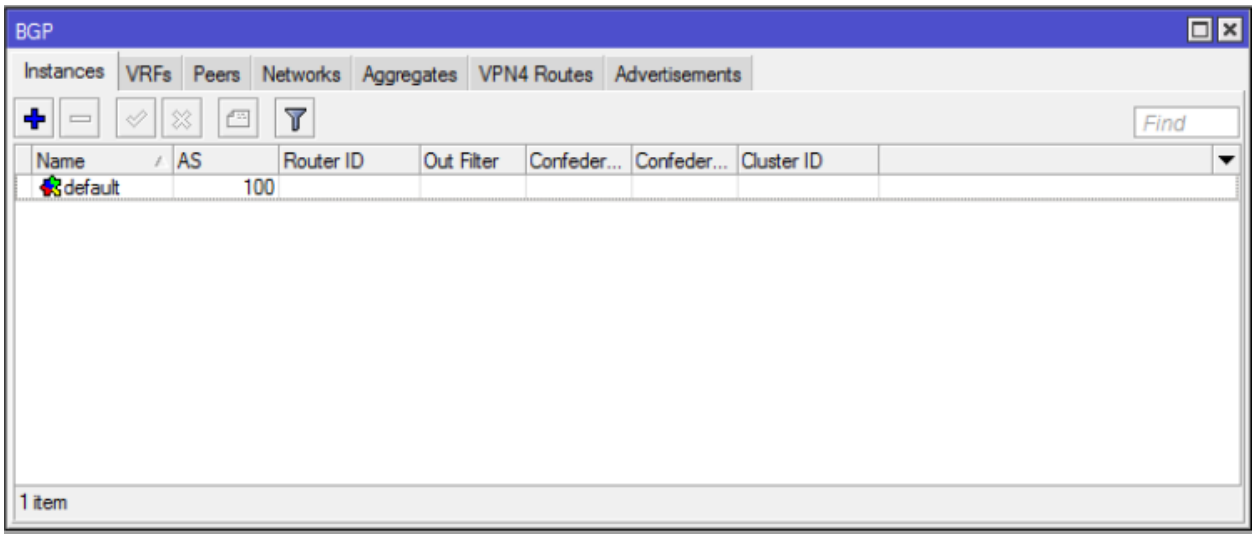
Nakon postavljanja IP adresa na svakom računalu potrebno je pokrenuti „*Winbox*“. *Winbox* je mali uslužni besplatni program koji omogućuje administriranje MikroTik usmjerivača pomoću brzog i

jednostavnog grafičkog sučelja. Nakon pokretanja programa pojavljuje se ulazno sučelje u kojem se odabire uređaj za administriranje te nakon povezivanja omogućen je niz funkcionalnosti kojima se može upravljati usmjerivačem. [20]

Nakon uspostave veze s usmjerivačem u *Winbox* sučelju potrebno je definirati autonomne sustave. (sl.5.5. i sl.5.6.). Autonomni sustav, kao što je već navedeno, predstavlja skup mreža i usmjerivača koji imaju zajednička pravila usmjeravanja.



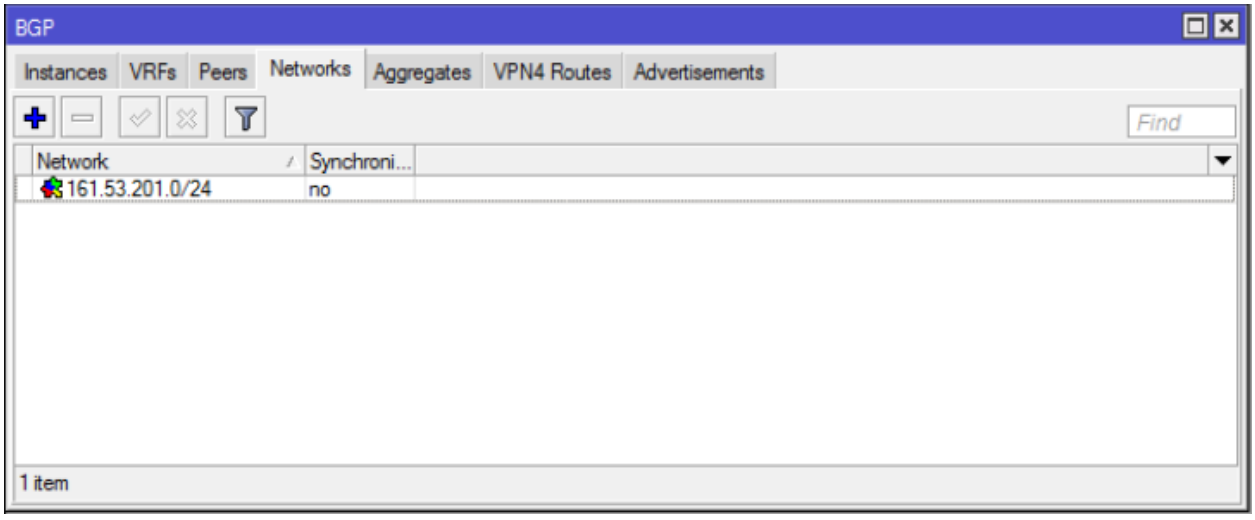
Sl. 5.5. *Autonomni sustav 200*



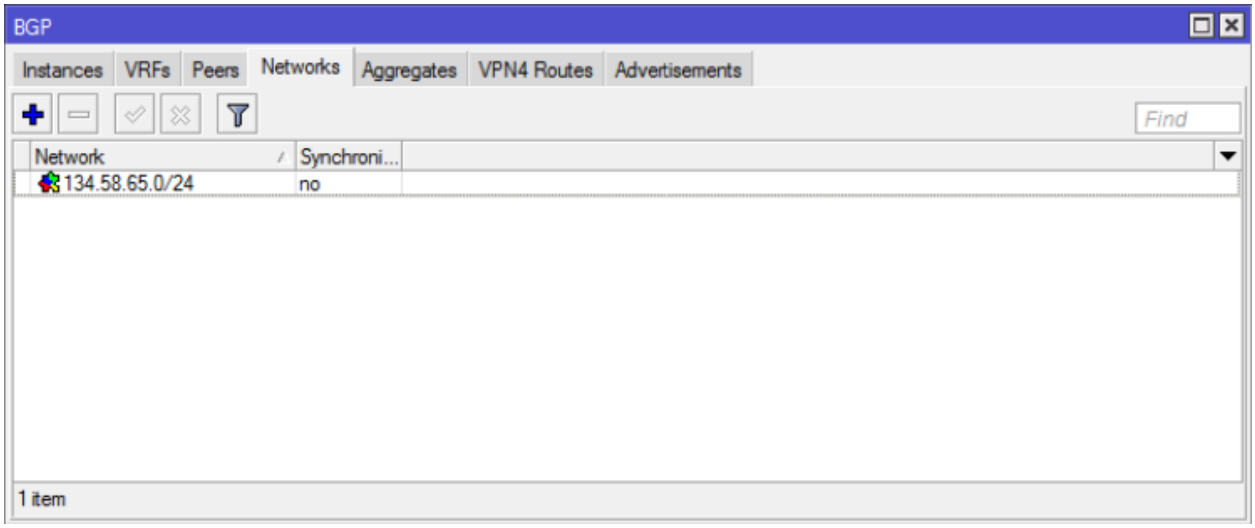
Sl. 5.6. *Autonomni sustav 100*

Sljedeći korak je postaviti mrežne adrese unutar usmjeritelja. Na sl.5.7. prikazana je adresa mreže prvog usmjerivača. Za dodjelu adrese mreže potrebno je unutar BGP prozora odabrati karticu *Networks* i zatim odabrati na ikonicu plavi plus. Nakon pritiska na OK sprema se adresa mreže

usmjerivača. Analogno tome na drugom računalu potrebno je postaviti adresu mreže drugog usmjerivača što je prikazano na sl. 5.8.



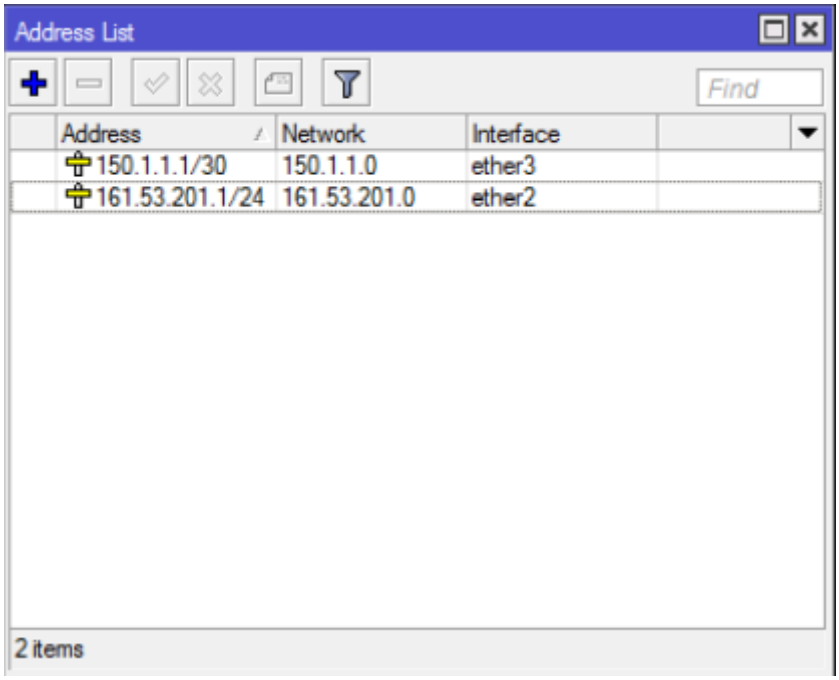
Sl. 5.7. *Mrežna adresa prvog usmjerivača*



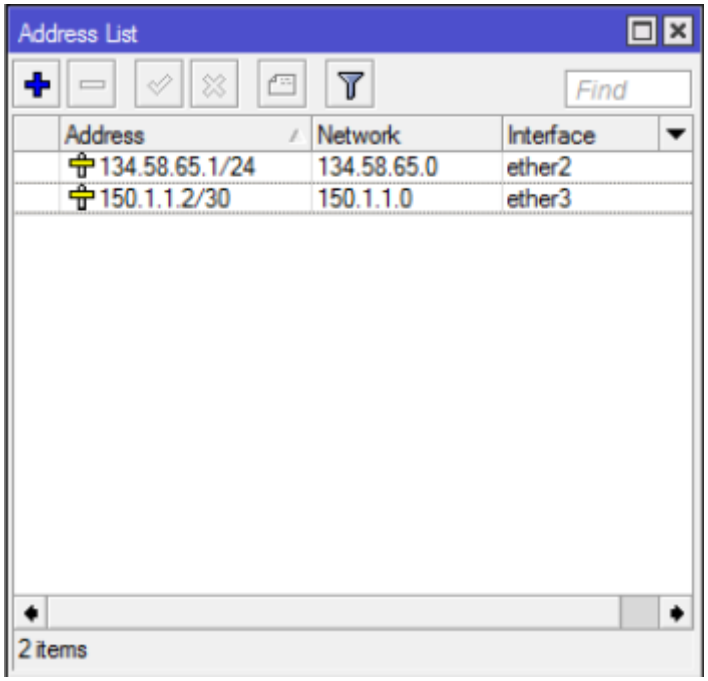
Sl. 5.8. *Mrežna adresa drugog usmjerivača*

Prije nego se nastavi s daljnjim postavljanjem BGP-a potrebno je svakako definirati adrese sučelja unutar usmjerivača. Sučelje ether2 koristi se za povezivanje usmjerivača s računalom, dok ether3 ima ulogu povezivanja samih usmjerivača. Sl.5.9. prikazuje listu adresa sučelja na prvom usmjerivaču. Vidljivo je da adresa na ether2 sučelju predstavlja *Default gateway* adresu koja je prethodno postavljena na prvom računalu (sl. 5.3.), odnosno ovo sučelje se koristi za spajanje računala s usmjerivačem. Dok adresa na ether3 portu predstavlja adresu *peer*-a na koji će drugi usmjeritelj postaviti udaljenu adresu te omogućiti povezivanje dva usmjerivača. Navedena adresa ima CIDR prefiks /30 što znači da je moguće dodijeliti samo dvije adrese unutar ove mreže, što je dovoljno za spajanje dva usmjerivača. Analogno tome, postavljene su adrese u drugom

usmjerivaču, gdje je ether2 adresa predstavlja adresu za spajanje računala, a ether3 adresa pripada mreži u kojoj će se ostvariti povezivanje ova dva usmjerivača (sl.5.10.)



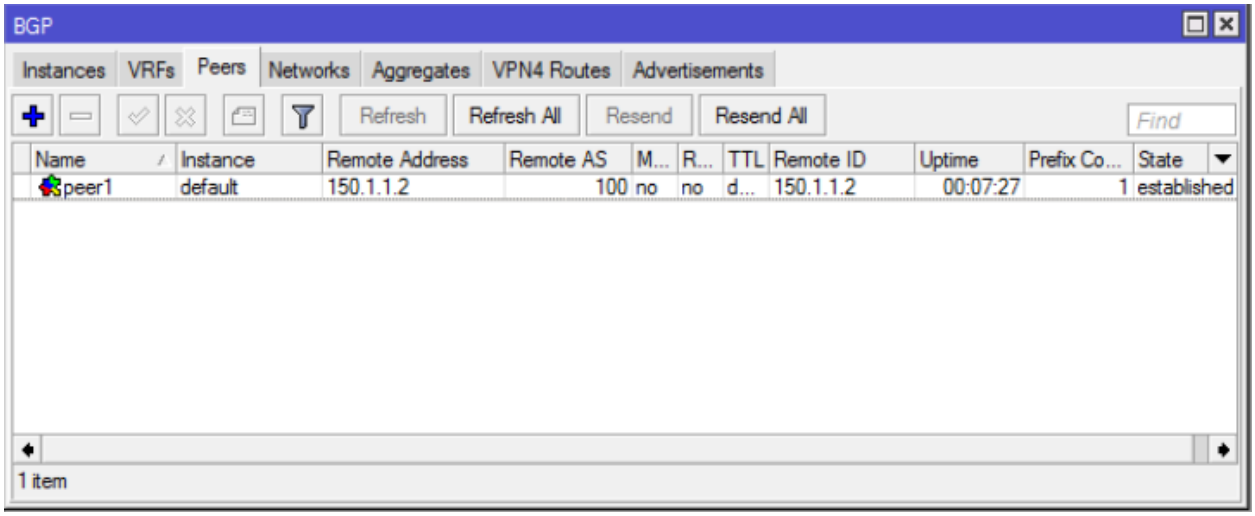
Sl. 5.9. *Adresna lista sučelja prvog usmjerivača*



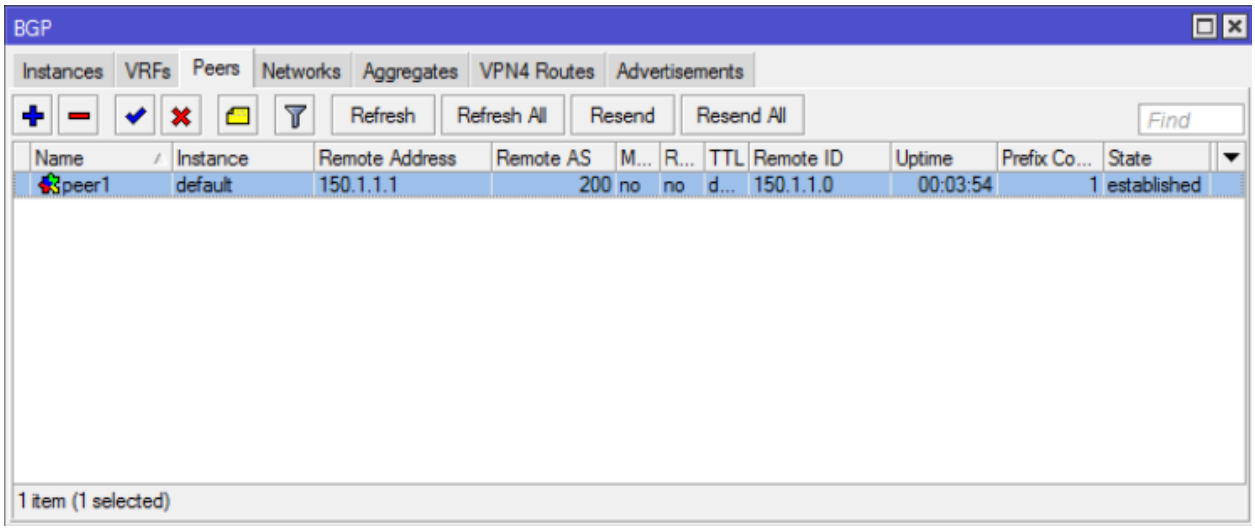
Sl. 5.10. *Adresna lista sučelja drugog usmjerivača*

Unutar BGP prozora potrebno je odabrati karticu *Peers* te unijeti *peer* za pojedini usmjerivač. *Peer* označava adresu sučelja susjednog usmjerivača na koji će biti povezan usmjerivač. Sl.5.11. prikazuje postavljanu *peer* karticu iz koje je vidljivo da *peer* na udaljenu adresu i udaljeni

autonomni sustav, postavljanje *peer*-a omogućuje spajanje na udaljeni usmjerivač preko porta *peer*-a. Analogno tome na drugom usmjerivač je također postavljen *peer* na prvi usmjerivač što je prikazano na sl.5.12.



Sl. 5.11. *Peer prvog usmjerivača*

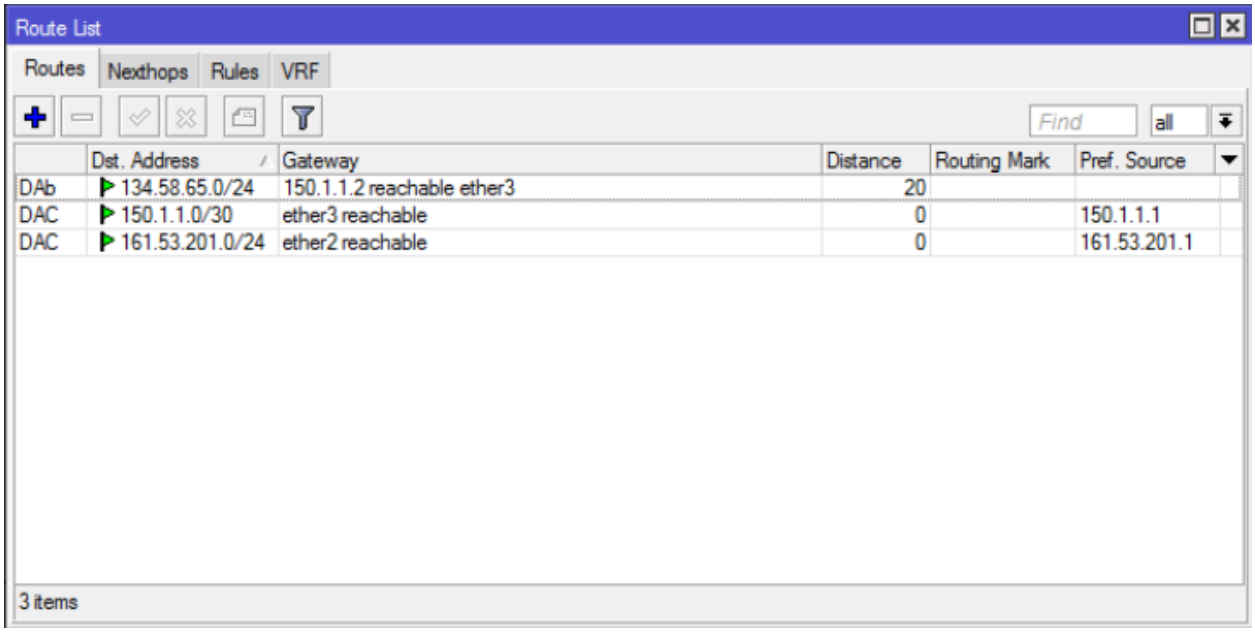


Sl. 5.12. *Peer drugog usmjerivača*

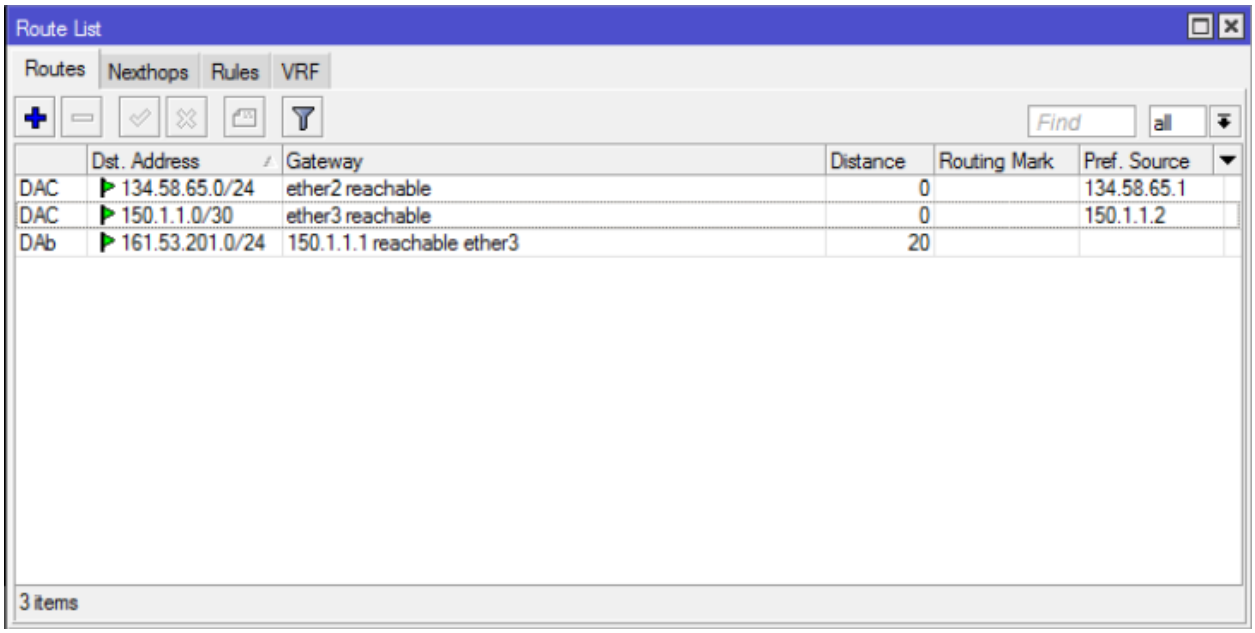
Nakon prethodno navedenog koraka uspostavljena je komunikacija te je postavljen BGP protokol između ovih autonomnih sustava. Sl.5.13. i sl.5.14 prikazuju listu ruta unutar pojedinog usmjerivača. Na sl.5.13. vidljiva su sva sučelja i adrese kojima raspolaže prvi usmjerivač.

Vidljivo je da su dostupni ether2 i ether3 sa svojim adresama te imaju zastavicu rute DAC, što označava da je ruta dinamična, aktivna i spojena (DAC= *Dynmic, Active, Connected*). Drugačiju zastavicu ima *peer* adresa kojoj je odredište adresa mreže drugog usmjerivača, zastavica ima

oznaku *DAb* što označava da je ruta dinamična, aktivna i da podržava BGP (DAb = *Dynamic*, *Active*, BGP). [21]

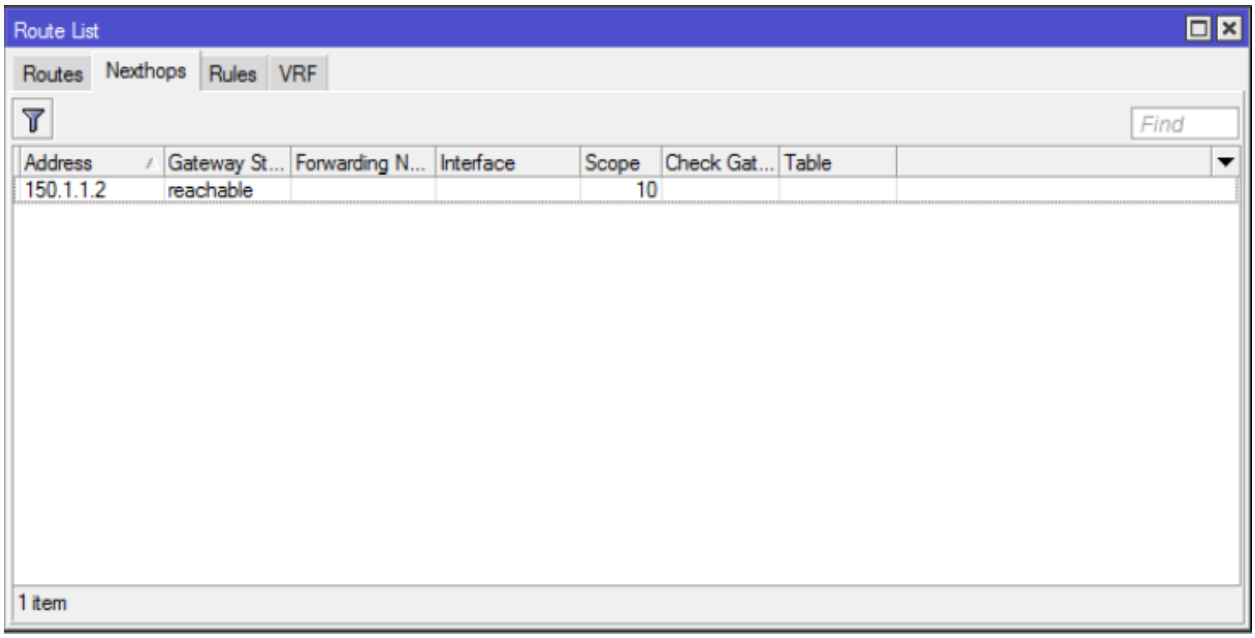


Sl. 5.13. *Lista ruta unutar prvog usmjerivača.*

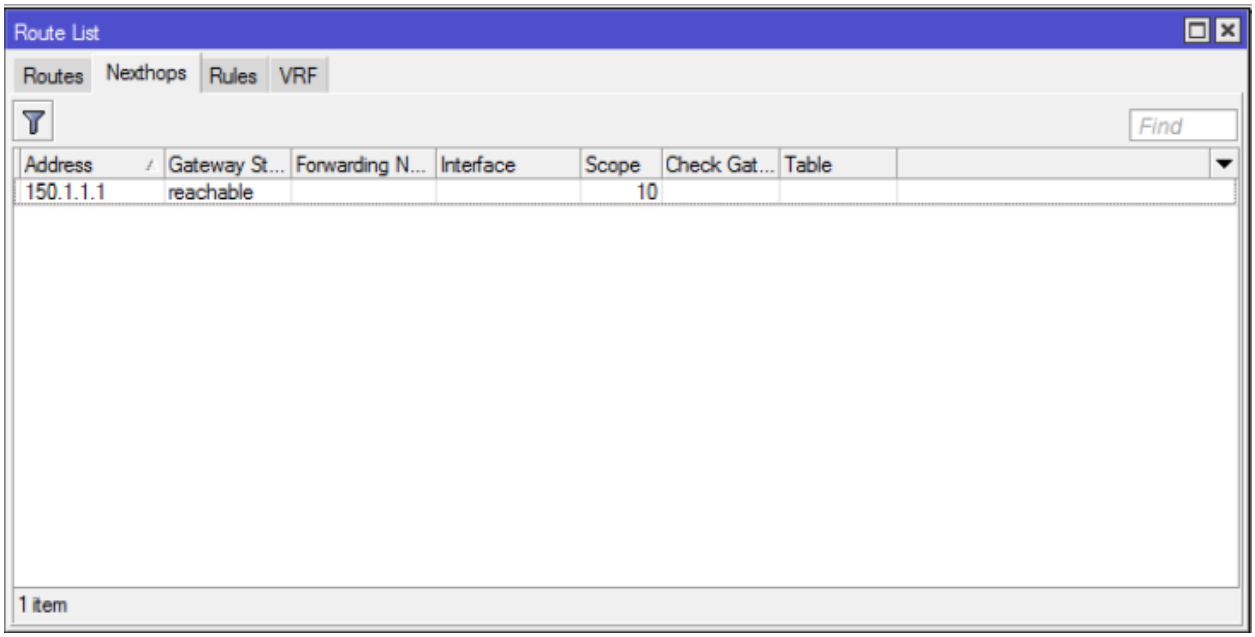


Sl. 5.14. *Lista ruta unutar drugog usmjerivača.*

Postojanje veze između usmjerivača vidljivo je i iz sljedećeg skoka pojedinog usmjerivača. Sl.5.15. prikazuje sljedeći skok usmjerivača kojemu je odredišna adresa sučelje ether3 na drugom usmjeritelju. Sl.5.16. prikazuje sljedeći skok usmjerivača kojemu je odredišna adresa sučelje ether3 na prvom usmjeritelju.

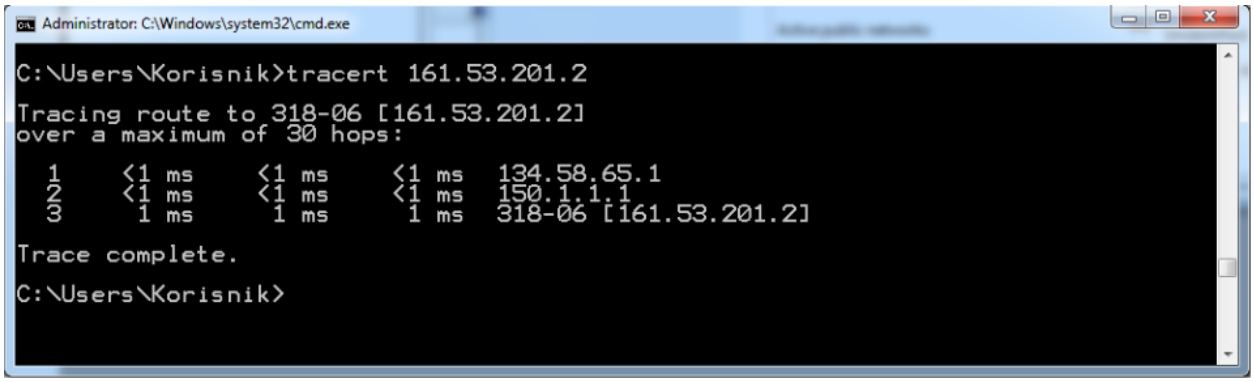


Sl. 5.15. *Sljedeći skok prvog usmjerivača.*



Sl. 5.16. *Sljedeći skok drugog usmjerivača.*

Nakon ovih dokaza o postojanju veze između usmjerivača potrebno je još prikazati dostupnost računala koji je povezan na usmjerivač autonomnog sustava. Provjera dostupnosti računala odraditi će se pomoću naredbe *tracert* <odredišna adresa>. Naredba *tracert* šalje pakete prema odredišnoj adresi te mjeri koliko je vremena potrebno da paket stigne do pojedinog dijela mreže koji se nalazi na putu do odredišne adrese.



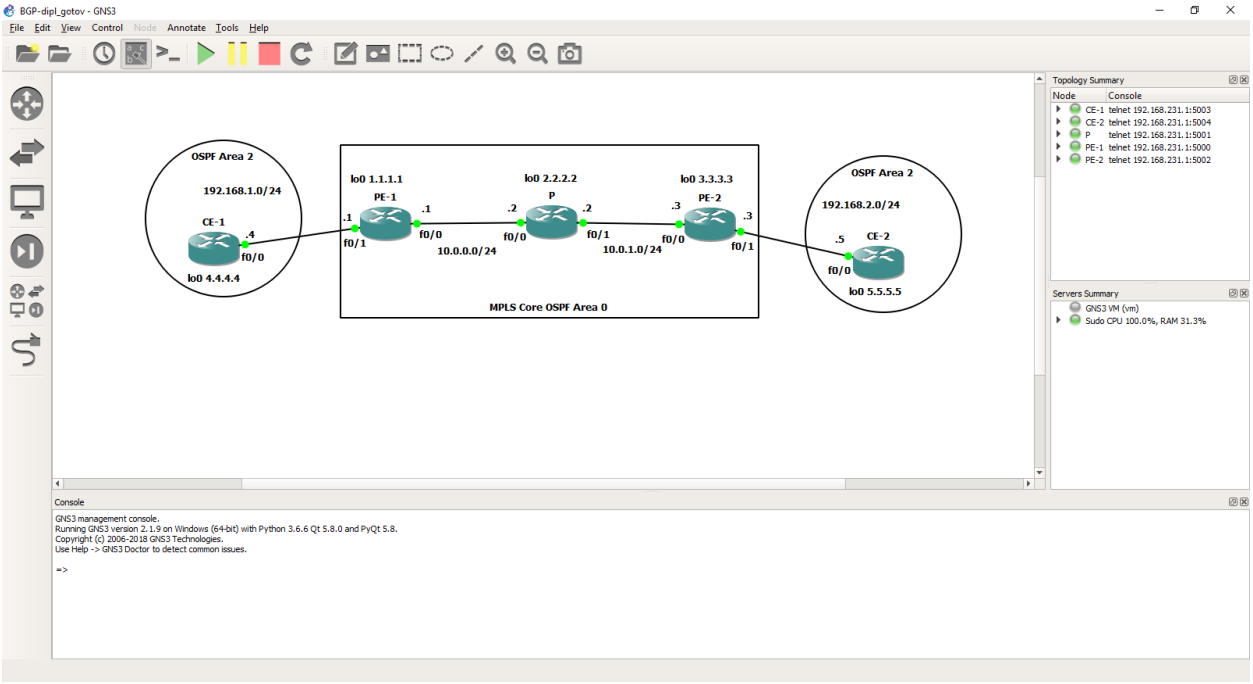
Sl. 5.17. *Odziv na naredbu tracert.*

Na Sl.5.17. vidljiva je upotreba naredbe *tracert* za odredište 161.53.201.2. što je ujedno i adresa prvog računala unutar autonomnog sustava 200. Prva linija odziva osim odredišne adrese ispisuje i ime računala za koji se provjerava dostupnost. Također je vidljivo da paket do odredišta mora proći kroz tri sučelja unutar mreže. Oznaka 1 nosi adresu sučelja ether2 na koji je povezano računalo. Oznaka 2 nosi adresu sljedećeg skoka, odnosno ulazno sučelje u prvi usmjerivač. Oznaka 3 nosi ime i adresu prvog računala za koji je provjeravana dostupnost. Kako su usmjerivači fizički spojeni jednim *patch* kabelom, potrebno vrijeme za prolazak paketa kroz sučelja je manje od jedne milisekunde.

5.2. Konfiguracija za rad BGP-a u VPN-u

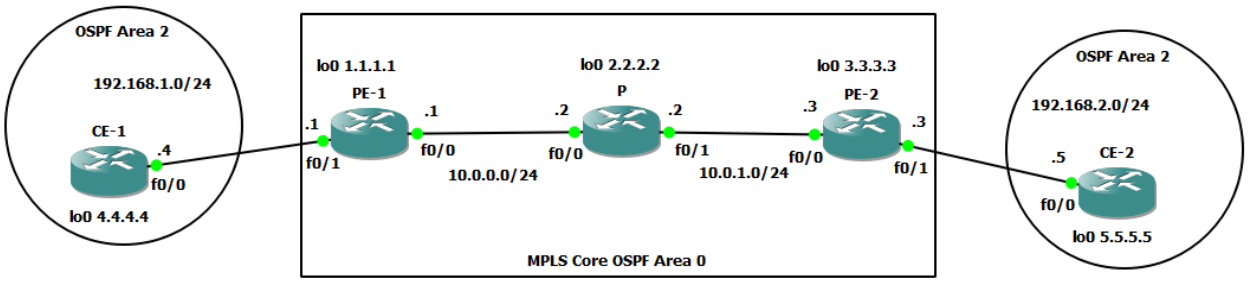
Konfiguracija topologije za prikaz BGP-a u VPN-u je složena u GNS3 simulatoru. GNS je kratica od engl. *Graphical Network Simulator* i predstavlja složeni simulator koji se od ostalih simulatora razlikuje po tome što učitava stvarni Cisco IOS umjesto da ga simulira. Bez fizičke opreme može se napraviti simulacija stvarnih mreža. GNS3 emulira usmjerivače, a radi u suradnji sa različitim alatima za virtualizaciju operacijskog sustava kako bi korisnik mogao po želji virtualizirati usmjerivač bilo koje tvrtke i koristiti ga u GNS3-u za simulaciju. Sl. 5.18.prikazuje sučelje GNS3 simulatora. S lijeve strane sučelja nalaze se ikone koje predstavljaju prečace do određenih mrežnih uređaja: usmjerivač, preklopni, terminali, sigurnosni uređaji, izbornik svih uređaja i stvaranje veza između uređaja. Gornji dio sučelja nosi osnovne alate za potrebe simulacije: pokretanje, pauziranje i zaustavljanje, ponovo pokretanje i nekolicinu grafičkih alata. Na desnoj strani nalaze se prozori koji nose informacije svih uređaja u topologiji i uređaje na kojima s može stvoriti simulacija. Donji dio sučelja prikazuje kontrolni izlaz koji javlja kontrolne greške prilikom izrade simulacija. Za rad je prije svega potrebno instalirati određeni uređaj koji će

se koristiti pri izradi simulacije te je potreban *image* uređaja za instalaciju. [22] Za potrebe ovog rada izabran je Cisco 7200 usmjerivač.



Sl. 5.18. *Sučelje programa GNS3*

Topologija potrebna za prikaz BGP prikazana je sl. 5.19. gdje je postavljena MPLS okosnica s usmjerivačima P, PE-1 i PE-2.



Sl. 5.19. *Mrežna topologija za prikaz rada BGP-a u VPN-u.*

Prije svega potrebno je postaviti MPLS okosnicu kojoj će se omogućiti rad u BGP-u. Za postavljanje okosnice potrebno je postaviti IP adrese svakog sučelja u usmjerivačima unutar okosnice. Svako sučelje ima konfiguriran i OSPF koji osigurava *loopback* vezu između PE-1 i PE-2 usmjerivača. Na Sl. 5.20. prikazana je konfiguracija IP adresa za svako sučelje koje se koristi prilikom postavljanja mrežne topologije. Konkretno za postavljanje okosnice na usmjerivaču PE-1 potrebno je konfigurirati sučelja *loopback* (lo0) i *fastEthernet* (f0/0). Konfiguriranje usmjerivača omogućeno je upotrebom naredbe *configure terminal* (*conf t*). Naredbom *interface* <oznaka

sučelja> moguće je konfigurirati pojedino sučelje. Dodavanje IP adrese omogućeno je naredbom *ip address* <adresa> <CIDR prefiks>. Za postavljanje OSPF protokola u sučelje koristi se naredba *ip ospf* <broj procesa> *area* <broj područja>

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#int
PE-1(config)#interface lo0
PE-1(config-if)#ip ad
PE-1(config-if)#ip address 1.1.1.1 255.255.255.255
PE-1(config-if)#ip ospf 1 area 0
PE-1(config-if)#ex
PE-1(config)#int
PE-1(config)#interface f0/0
PE-1(config-if)#ip add
PE-1(config-if)#ip address 10.0.0.1 255.255.255.0
PE-1(config-if)#no shut
PE-1(config-if)#no shutdown
PE-1(config-if)#ip osp
*Sep  1 23:14:55.327: %LINK-3-UPDOWN: Interface FastEthernet0/0,
o up
*Sep  1 23:14:56.327: %LINEPROTO-5-UPDOWN: Line protocol on Inte
et0/0, changed state to up
PE-1(config-if)#ip ospf 1 area 0
PE-1(config-if)#
```

Sl. 5.20. *Konfiguracija IP adresa na sučeljima na PE-1 usmjerivaču.*

Na temelju navedenih naredbi stvorena je konfiguracija na usmjerivačima P i PE-2 (sl. 5.21 i sl. 5.22.)

```
P#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P(config)#int
P(config)#interface lo0
P(config-if)#op
*Sep  1 23:16:42.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
 changed state to up
P(config-if)#ip add
P(config-if)#ip address 2.2.2.2 255.255.255.255
P(config-if)#ip ospf 1 area 0
P(config-if)#ex
P(config)#int
P(config)#interface f0/0
P(config-if)#ip add
P(config-if)#ip address 10.0.0.2 255.255.255.0
P(config-if)#no shut
P(config-if)#ip ospf 1
*Sep  1 23:19:07.119: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Sep  1 23:19:08.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
P(config-if)#ip ospf 1 area 0
P(config-if)#ex
P(config)#int f0/1
P(config-if)#ip
*Sep  1 23:19:15.699: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0
from LOADING to FULL, Loading Done
P(config-if)#ip ad
P(config-if)#ip address 10.0.1.2 255.255.255.0
P(config-if)#no shut
P(config-if)#ip osp
P(config-if)#ip ospf 1 a
*Sep  1 23:19:32.579: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Sep  1 23:19:33.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
P(config-if)#ip ospf 1 area 0
```

Sl. 5.21. *Konfiguracija IP adresa na sučeljima na P usmjerivaču.*

```
PE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-2(config)#in
PE-2(config)#interface lo0
PE-2(config-if)#
*Sep  1 23:20:52.411: %LINEPROTO-5-UPDOWN: Line protocol on In
PE-2(config-if)#ip
PE-2(config-if)#ip add
PE-2(config-if)#ip address 3.3.3.3 255.255.255.255
PE-2(config-if)#ip ospf 1 area 0
PE-2(config-if)#ex
PE-2(config)#int
PE-2(config)#interface f0/0
PE-2(config-if)#ip add
PE-2(config-if)#ip address 10.0.1.3 255.255.255.0
PE-2(config-if)#no shu
PE-2(config-if)#no shutdown
PE-2(config-if)#ip ospf 1 at
*Sep  1 23:21:39.227: %LINK-3-UPDOWN: Interface FastEthernet0/
*Sep  1 23:21:40.227: %LINEPROTO-5-UPDOWN: Line protocol on In
PE-2(config-if)#ip ospf 1 area 0
```

Sl. 5.22. *Konfiguracija IP adresa na sučeljima na PE-2 usmjerivaču.*

Uspješno postavljene IP adrese na sučeljima u usmjerivačima unutar okosnice najlakše je provjeriti naredbom *ping* na način da se s usmjerivača PE-1 pokrene naredba *ping* na *loopback* adresu PE-2 usmjerivača. (sl. 5.23.) Pokrenuta naredba prikazuje uspješan odgovor da je *loopback* adresa PE-2 usmjerivača dohvatljiva te se ispisuje informacija u uspješnosti u postotcima i minimalna, srednja i maksimalna vrijednost puta paketa.

```
PE-1#ping 3.3.3.3 source lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/143/168 ms
```

Sl. 5.23. *Naredba ping na loopback adresu PE-2 usmjerivača.*

Na vezu između usmjerivača PE-1 i P postavljeno je snimanje prometa u programskom alatu *Wireshark*. *Wireshark* alat prikazuje informacije u prijenosu paketa na toj vezi te ispisuje informacije o: rednom broju paketa, vrijeme, izvorišnoj adresi, odredišnoj adresi, protokolu koji se koristi, duljini paketa i informaciji. Odabirom bilo kojeg paketa moguće je dobiti prikaz nekih osnovnih informacija za taj paket. Na sl. 5.24. prikazan je isječak iz prometa snimljenog u *Wireshark* alatu u kojem je vidljiva razmjena paketa prilikom pokretanja naredbe *ping* sa sl. 5.23.

No.	Time	Source	Destination	Protocol	Length	Info
109	202.785801	1.1.1.1	3.3.3.3	ICMP	114	Echo (ping) request id=0x0000, seq=0/0, ttl=255 (reply in 110)
110	202.888736	3.3.3.3	1.1.1.1	ICMP	114	Echo (ping) reply id=0x0000, seq=0/0, ttl=254 (request in 109)
111	202.921715	1.1.1.1	3.3.3.3	ICMP	114	Echo (ping) request id=0x0000, seq=1/256, ttl=255 (reply in 112)
112	203.018655	3.3.3.3	1.1.1.1	ICMP	114	Echo (ping) reply id=0x0000, seq=1/256, ttl=254 (request in 111)
113	203.056632	1.1.1.1	3.3.3.3	ICMP	114	Echo (ping) request id=0x0000, seq=2/512, ttl=255 (reply in 114)
114	203.154571	3.3.3.3	1.1.1.1	ICMP	114	Echo (ping) reply id=0x0000, seq=2/512, ttl=254 (request in 113)
115	203.182554	1.1.1.1	3.3.3.3	ICMP	114	Echo (ping) request id=0x0000, seq=3/768, ttl=255 (reply in 116)
116	203.297482	3.3.3.3	1.1.1.1	ICMP	114	Echo (ping) reply id=0x0000, seq=3/768, ttl=254 (request in 115)
117	203.355447	1.1.1.1	3.3.3.3	ICMP	114	Echo (ping) request id=0x0000, seq=4/1024, ttl=255 (reply in 118)
118	203.471376	3.3.3.3	1.1.1.1	ICMP	114	Echo (ping) reply id=0x0000, seq=4/1024, ttl=254 (request in 117)

Sl. 5.24. *ICMP protokol prilikom pokretanja naredbe ping.*

Nakon postavljanja IP adresa, potrebno je konfigurirati MPLS i LDP protokole na usmjerivače okosnice. Protokoli se postavljaju na vrlo jednostavan način, potrebno je pokrenuti konfiguriranje usmjerivača, zatim pokrenuti naredbu *router ospf* <broj procesa> i naredbu *mpls ldp autoconfig* (sl. 5.25., sl. 5.26. i sl. 5.27.).

```
PE-1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#router ospf 1
PE-1(config-router)#mpls ldp at
PE-1(config-router)#mpls ldp a
PE-1(config-router)#mpls ldp autoconfig
```

Sl. 5.25. *MPLS LDP konfiguracija na usmjerivaču PE-1.*

```
P(config)#router ospf 1
P(config-router)#
P(config-router)#mpls ldp aut
P(config-router)#mpls ldp autoconfig
P(config-router)#
*Sep  1 23:25:51.763: %PARSE_RC-3-PRC_INVALID_BLOCK_PTR:
*Sep  1 23:25:51.811: %PARSE_RC-3-PRC_INVALID_BLOCK_PTR:
P(config-router)#
*Sep  1 23:25:52.287: %LDP-5-NBRCHG: LDP Neighbor 1.1.1.1:0 (1) is UP
```

Sl. 5.26. *MPLS LDP konfiguracija na usmjerivaču P.*

```
PE-2(config)#router ospf 1
PE-2(config-router)#mpls ldp a
PE-2(config-router)#mpls ldp autoconfig
PE-2(config-router)#
*Sep  1 23:26:42.871: %PARSE_RC-3-PRC_INVALID_BLOCK_PTR:
PE-2(config-router)#
*Sep  1 23:26:43.427: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (1) is UP
```

Sl. 5.27. *MPLS LDP konfiguracija na usmjerivaču PE-2.*

Prilikom pokretanja naredbi za MPLS i LDP na usmjerivačima P i PE-2 pojavljuju se poruke koje javljaju konfiguraciju LDP susjednih *loopback* adresa. Na sl. 5.28. u prvom i trećem retku vidi se poruka o postavljaju LDP susjednih *loopback* adresa te prilikom pokretanja naredbe *sh mpls interface* koja za odziv prikazuje sva sučelja u kojima je konfiguriran MPLS. Vidljivo je da sučelja f0/0 i f0/1 imaju konfiguriran LDP protokol.

```
*Sep  1 23:25:52.287: %LDP-5-NBRCHG: LDP Neighbor 1.1.1.1:0 (1) is UP
P(config-router)#
*Sep  1 23:26:43.651: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (2) is UP
P(config-router)#sh mpls int
P(config-router)#ex
P(config)#exit
P#sh
*Sep  1 23:27:59.027: %SYS-5-CONFIG_I: Configured from console by console
P#sh mpls interface
Interface              IP            Tunnel   BGP Static Operational
FastEthernet0/0        Yes (ldp)     No       No  No     Yes
FastEthernet0/1        Yes (ldp)     No       No  No     Yes
```

Sl. 5.28. *Prikaz MPLS sučelja na usmjerivaču P.*

Osim dokaza o postavljenom LDP protokolu iz sl. 5.28. dodatno se u to može uvjeriti tako da se s usmjerivača PE-1 pozove naredba *trace* na *loopback* adresu PE-2 usmjerivača. Ukoliko se u odzivu *trace* naredbe na nekoj lokaciji pojavi MPLS oznaka, LDP je uspješno postavljen (sl. 5.29).

```
PE-1#trace 3.3.3.3
Type escape sequence to abort.
Tracing the route to 3.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.0.2 [MPLS: Label 17 Exp 0] 92 msec 128 msec 56 msec
  2 10.0.1.3 128 msec 156 msec 112 msec
```

Sl. 5.29. *Trace naredba na loopback adresu PE-2 s usmjerivača PE-1.*

U okosnici u pravilno postavljeni MPLS, LDP protokoli te su sva sučelja dobro definirana. Stoga je sljedeći korak uspostaviti MP-BGP sjednicu između PE-1 i PE-2 usmjerivača. Konfiguracija se postavlja na način da se prvo pozove naredba *router bgp* <ASN>. Nakon toga potrebno je postaviti *loopback* adresu PE-2 usmjerivača za susjednu udaljenu adresu pomoću naredbe *neighbor* <ip adresa> *remote-as* <ASN> i naredbe *neighbor* <ip adresa> *update-source* <tip sučelja> koja vrača sučelje na najbliže sučelje. Nakon pozivanja navedenih naredbi potrebno je još susjednu adresu aktivirati u adresnoj obitelji VPNv4, a aktivira se naredbom *address-family vpnv4* i zatim *neighbor* <ip adresa> *activate*.

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#router bgp 1
PE-1(config-router)#nei
PE-1(config-router)#neighbor 3.3.3.3 remote
PE-1(config-router)#neighbor 3.3.3.3 remote-as 1
PE-1(config-router)#neighbor 3.3.3.3 update
PE-1(config-router)#neighbor 3.3.3.3 update-source Loopback0
PE-1(config-router)#no auto
PE-1(config-router)#no auto-summary
PE-1(config-router)#!
PE-1(config-router)#adr
PE-1(config-router)#add
PE-1(config-router)#address-family vpnv4
PE-1(config-router-af)#neig
PE-1(config-router-af)#neighbor 3.3.3.3 ac
PE-1(config-router-af)#neighbor 3.3.3.3 activate
```

Sl. 5.30. *Konfiguracija BGP-a u usmjerivaču PE-1.*

Analogno konfiguraciji na PE-1 usmjerivaču, prema istim koracima potrebno je konfigurirati BGP na PE-2 usmjerivaču (sl. 5.31.).

```
PE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-2(config)#router bgp 1
PE-2(config-router)#ne
PE-2(config-router)#nei
PE-2(config-router)#neighbor 1.1.1.1 rem
PE-2(config-router)#neighbor 1.1.1.1 remote.
PE-2(config-router)#neighbor 1.1.1.1 remote
PE-2(config-router)#neighbor 1.1.1.1 remote-as 1
PE-2(config-router)#neighbor 1.1.1.1 update
*Sep  1 23:34:37.339: %BGP-5-ADJCHANGE: neighbor 1.1.1.1 Up
PE-2(config-router)#neighbor 1.1.1.1 update
PE-2(config-router)#neighbor 1.1.1.1 update-source Loopback0
PE-2(config-router)#no
PE-2(config-router)#no u
PE-2(config-router)#no au
PE-2(config-router)#no auto-summary
PE-2(config-router)#!
PE-2(config-router)#add
PE-2(config-router)#address-family vpn
PE-2(config-router)#address-family vpnv4
PE-2(config-router-af)#nei
PE-2(config-router-af)#neighbor 1.1.1.1 acti
PE-2(config-router-af)#neighbor 1.1.1.1 activate
PE-2(config-router-af)#
*Sep  1 23:35:09.043: %BGP-5-NBR_RESET: Neighbor 1.1.1.1 reset (Capability changed)
*Sep  1 23:35:09.051: %BGP-5-ADJCHANGE: neighbor 1.1.1.1 Down Capability changed
*Sep  1 23:35:09.051: %BGP_SESSION-5-ADJCHANGE: neighbor 1.1.1.1 IPv4 Unicast topolo
on  Capability changed
PE-2(config-router-af)#
*Sep  1 23:35:10.091: %BGP-5-ADJCHANGE: neighbor 1.1.1.1 Up
```

Sl. 5.31. *Konfiguracija BGP-a u usmjerivaču PE-2.*

Nakon što je postavljen BGP na sl. 5.31. prikazane su poruke podizanja BGP sesije između rubnih usmjerivača. Kao dokaz pravilno postavljenog BGP protokola vidi se najbolje iz sl. 5.32. gdje je pokrenuta naredba *show bgp vpnv4 unicast all summary* koja ispisuje sve informacije o BGP unutar VPNv4 adresne obitelji.

```
PE-1#sh bgp vpnv4 unicast all summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4            1       6       6        1    0    0 00:01:27        0
```

Sl. 5.32. *Prikaz BGP tablice na PE-1 usmjerivaču.*

S postavljenom BGP okosnicom, okosnica je spremna za klijente. Slijedi konfiguriranje usmjerivača klijenata. Dodavanjem klijenata, klijentima je potrebno postaviti IP adrese na sučelja te ih povezati s krajnjim usmjerivačem okosnice (sl. 5.33, sl. 5.34, sl. 5.35. i sl. 5.36.).

```
CE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CE-1(config)#int
CE-1(config)#interface lo0
CE-1(config-if)#ip
*Sep  1 23:38:51.695: %LINEPROTO-5-UPDOWN: Line protocol on In
CE-1(config-if)#ip a
CE-1(config-if)#ip add
CE-1(config-if)#ip address 4.4.4.4 255.255.255.255
CE-1(config-if)#ip ospf 2 area 2
CE-1(config-if)#ex
CE-1(config)#int f0/0
CE-1(config-if)#ip add
CE-1(config-if)#ip address 192.168.1.4 255.255.255.0
CE-1(config-if)#ip ospf 2 area 2
CE-1(config-if)#no shut
```

Sl. 5.33. *Konfiguracija IP adresa na sučeljima na CE-1 usmjerivaču.*

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#int
PE-1(config)#interface f0/1
PE-1(config-if)#ip add
PE-1(config-if)#ip address 192.168.1.1 255.255.255.0
PE-1(config-if)#no shut
PE-1(config-if)#no shutdown
```

Sl. 5.34. *Postavljanje sučelja na usmjerivaču PE-1 za priključak CE-1 usmjerivača.*

```
CE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CE-2(config)#int
CE-2(config)#interface lo0
CE-2(config-if)#o
*Sep  1 23:41:26.287: %LINEPROTO-5-UPDOWN: Line protocol on In
CE-2(config-if)#ip
CE-2(config-if)#ip add
CE-2(config-if)#ip address 5.5.5.5 255.255.255.255
CE-2(config-if)#ip ospf 2 area 2
CE-2(config-if)#ex
CE-2(config)#int
CE-2(config)#interface f0/0
CE-2(config-if)#ip
CE-2(config-if)#ip add
CE-2(config-if)#ip address 192168.2.5 255.255.255.0
                           ^
% Invalid input detected at '^' marker.

CE-2(config-if)#ip address 192.168.2.5 255.255.255.0
CE-2(config-if)#ip ospf 2 area 2
CE-2(config-if)#no shut
```

Sl. 5.35. *Konfiguracija IP adresa na sučeljima na CE-2 usmjerivaču.*

```
PE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-2(config)#int f0/1
PE-2(config-if)#no shut
PE-2(config-if)#no shutdown
PE-2(config-if)#ip ad
PE-2(config-if)#ip address 19
*Sep  1 23:43:41.275: %LINK-3-UPDOWN: Interface FastEthernet0/
*Sep  1 23:43:42.275: %LINEPROTO-5-UPDOWN: Line protocol on I
PE-2(config-if)#ip address 192.168.2.3 255.255.255.0
```

Sl. 5.36. *Postavljanje sučelja na usmjerivaču PE-2 za priključak CE-2 usmjerivača.*

Nakon postavljanja usmjerivača CE-1 i CE-2 te povezivanja istih na rubne usmjerivače okosnice potrebno je postaviti VRF. Postavljani VRF s imenom FERIT, RD broj 4:4 i RT brojem 4:4 postavlja se na način prikazan sl. 5.37.

```
PE-1(config)#ip vrf FERIT
PE-1(config-vrf)#rd 4:4
PE-1(config-vrf)#route
PE-1(config-vrf)#route-ta
PE-1(config-vrf)#route-target both 4:4
```

Sl. 5.37. *Postavljanje virtualnog usmjeravanja i prosljeđivanja FERIT u PE-1 usmjerivač.*

Zatim je potrebno postaviti VRF prosljeđivanje na sučelje koje predstavlja izlaznu mrežu prema klijentu. Prosljeđivanje se postavlja na način da se ulaskom u konfiguraciju odabere sučelje naredbom *int* <ime> te naredbom *ip vrf forvarding* <naziv VRF-a>. Potvrdom prethodno navedene naredbe u konzoli se pojavljuje poruka da je IPv4 adresa izbrisana kako bi se omogućio *vrf* FERIT. Stoga je potrebno ponovo konfigurirati IP adresu sučelja f0/1 (sl. 5.38.).

```
PE-1(config)#int f0/1
PE-1(config-if)#ip vrf f
PE-1(config-if)#ip vrf forwarding FERIT
% Interface FastEthernet0/1 IPv4 disabled and address(es) removed due to enabling VRF FERIT
PE-1(config-if)#int
PE-1(config-if)#ip add
PE-1(config-if)#ip address 192.168.1.1 255.255.255.0
```

Sl. 5.38. *Postavljanje virtualnog prosljeđivanja za FERIT u PE-1 usmjerivač.*

Sl. 5.39. prikazuje konfiguraciju postavljenu na sučelju f0/1 usmjerivača PE-1, vidljivo je da sučelje ima svoju IP adresu te da je omogućeno prosljeđivanje VRF FERIT što je potvrda da je konfiguracija uspješno postavljena.

```
PE-1#show run interface f0/1
Building configuration...

Current configuration : 121 bytes
!
interface FastEthernet0/1
 ip vrf forwarding FERIT
 ip address 192.168.1.1 255.255.255.0
 speed auto
 duplex auto
end
```

Sl. 5.39. *Uspješno postavljeno virtualno prosljeđivanje za FERIT u PE-1 usmjerivač.*

Na sl. 5.40. vidi se prikaz svih IP ruta na PE-1 usmjerivaču. Pozivom naredbe *show ip route*, prvo se ispisuje legenda s kodovima koji se mogu pojaviti u ispisu ruta. Legenda je pomoć za lakše razumijevanje ruta. Uvidom u rute na usmjerivaču omogućuju provjeru povezanih adresa te je lako uočiti je li neka od ruta izostavljena uz pretpostavku da usmjerivač nema veću dostupnost ruta jer s većim brojem ruta povećava se i tablica ruta.

```
PE-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 10.0.0.2, 00:28:03, FastEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/3] via 10.0.0.2, 00:25:16, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.0.0.0/24 is directly connected, FastEthernet0/0
L        10.0.0.1/32 is directly connected, FastEthernet0/0
O        10.0.1.0/24 [110/2] via 10.0.0.2, 00:27:41, FastEthernet0/0
```

Sl. 5.40. *PE-1 usmjerivač, prikaz IP ruta.*

U naredbu *show ip route* moguće je dodati filter koji će prikazati samo željene rute. Sl. 5.41. prikazuje dodani filter na navedenu naredbu koji će omogućiti prikaz samo IP ruta za VRF FERIT. Iz priloženog se da zaključiti da fali ruta prema usmjerivaču CE-1.

```
PE-1#show ip route vrf FERIT

Routing Table: FERIT
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/1
L        192.168.1.1/32 is directly connected, FastEthernet0/1
```

Sl. 5.41. *PE-1 usmjerivač prikaz vrf FERIT ruta.*

Kako bi se dodala ruta prema usmjerivaču CE-1 potrebno je promijeniti postavke unutar izlaznog sučelja prema CE-1. Naime, trenutno je to sučelje postavljeno na *ospf 1 area 1* (sl. 5.20.) što je *ospf* unutar okosnice i potrebno je postaviti *ospf 2 area 2* što je OSPF klijenta (sl. 5.42.).

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#int
PE-1(config)#interface f0/1
PE-1(config-if)#ip ospf 2 area 2
PE-1(config-if)#
*Sep  1 23:49:25.607: %OSPF-5-ADJCHG: Process 2, Nbr 4.4.4.4 on FastEthernet0/1 from LOADING to
 FULL, Loading Done
```

Sl. 5.42. *PE-1 usmjerivač prikaz izmjena na sučelju f0/1.*

Nakon izmjene OSPF na sučelju f0/1 usmjerivača PE-1, na sl. 5.43. je vidljiva ruta prema usmjerivaču CE-1.

```
PE-1#show ip route vrf FERIT

Routing Table: FERIT
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/2] via 192.168.1.4, 00:00:54, FastEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/1
L        192.168.1.1/32 is directly connected, FastEthernet0/1
```

Sl. 5.43. *PE-1 usmjerivač, prikaz FERIT ruta nakon izmjena na sučelju f0/1.*

Analogno učinjenom između usmjerivača PE-1 i CE-1, potrebno je postaviti na isti način konfiguracije između usmjerivača PE-2 i CE-2 (sl. 5.44, sl. 5.45 i sl. 5.46.).

```
PE-2(config)#ip vrf FERIT
PE-2(config-vrf)#rd 4:4
PE-2(config-vrf)#rout
PE-2(config-vrf)#route-t
PE-2(config-vrf)#route-target both 4:4
PE-2(config-vrf)#ex
% Ambiguous command:  "ex"
PE-2(config-vrf)#exit
PE-2(config)#int
PE-2(config)#interface f0/1
PE-2(config-if)#ip vrf fo
PE-2(config-if)#ip vrf forwarding FERIT
% Interface FastEthernet0/1 IPv4 disabled and address(es) removed due to enabling VRF FERIT
PE-2(config-if)#ip add
PE-2(config-if)#ip address 192.168.2.1 255.255.255.0
```

Sl. 5.44. *PE-2 postavljanje virtualnog usmjeravanja i prosljeđivanja FERIT na sučelju f0/1.*

```
PE-2#show run interface f0/1
Building configuration...

Current configuration : 121 bytes
!
interface FastEthernet0/1
 ip vrf forwarding FERIT
 ip address 192.168.2.1 255.255.255.0
 speed auto
 duplex auto
end
```

Sl. 5.45. *Uspješno postavljeno virtualno prosljeđivanje FERIT u PE-2 usmjerivač.*

```
PE-2#show ip route vrf FERIT

Routing Table: FERIT
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      5.0.0.0/32 is subnetted, 1 subnets
O        5.5.5.5 [110/2] via 192.168.2.5, 00:00:08, FastEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, FastEthernet0/1
L        192.168.2.1/32 is directly connected, FastEthernet0/1
```

Sl. 5.46. *PE-1 usmjerivač prikaz virtualnih FERIT ruta.*

Kako bi se prikazale BGP tablice u PE-1 i PE-2 usmjerivačima potrebno je redistribuirati OSPF u MP-BGP na navedenim usmjerivačima. Redistribuciju treba napraviti na način prikazan sl. 5.47. i sl. 5.48.

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#router bgp 1
PE-1(config-router)#add
PE-1(config-router)#address-family ipv4 vrf FERIT
PE-1(config-router-af)#redi
PE-1(config-router-af)#redistribute ospf 2
```

Sl. 5.47. *PE-1 usmjerivač, redistribucija OSPF u MP-BGP.*

```
PE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-2(config)#router bgp 1
PE-2(config-router)#add
PE-2(config-router)#address-family ipv4 vrf FERIT
PE-2(config-router-af)#red
PE-2(config-router-af)#redistribute ospf 2
```

Sl. 5.48. *PE-2 usmjerivač, redistribucija OSPF u MP-BGP.*

Sl. 5.49. prikazuje BGP tablicu koja sadrži prikaz dostupnih vrf FERIT ruta koje pripadaju VPNv4 adresnoj obitelji što potvrđuje da je riječ o VPN mreži. Navedene rute prikazuju odredišne adrese klijentovih usmjerivača te koji je sljedeći skok kako bi se dosegla odredišna adresa.

```
PE-1#show ip bgp vpnv4 vrf FERIT
BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf FERIT)
 *>  4.4.4.4/32       192.168.1.4              2         32768 ?
 *>i 5.5.5.5/32       3.3.3.3                  2    100      0 ?
 *>  192.168.1.0      0.0.0.0                  0         32768 ?
 *>i 192.168.2.0      3.3.3.3                  0    100      0 ?
```

Sl. 5.49. *PE-1 usmjerivač, prikaz BGP tablice.*

Sl. 5.50. prikazuje isto što i prethodna slika samo za usmjerivač PE-2. Lako je uočiti razliku u tablicama i načine u kojima će određeni usmjerivač dostići odredišnu adresu. Konkretno za usmjerivač CE-1 koji ima *loopback* adresu 4.4.4.4 vidi se da će sljedeći skok za usmjerivač PE-1 biti sučelje f0/0 na usmjerivaču CE-1, dok će sljedeći skok za usmjerivač PE-2 biti upravo usmjerivač PE-1 koji ima *loopback* adresu 1.1.1.1 .

```
PE-2#show ip bgp vpnv4 vrf FERIT
BGP table version is 7, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf FERIT)
 *>i 4.4.4.4/32       1.1.1.1                  2    100      0 ?
 *>  5.5.5.5/32       192.168.2.5              2         32768 ?
 *>i 192.168.1.0      1.1.1.1                  0    100      0 ?
 *>  192.168.2.0      0.0.0.0                  0         32768 ?
```

Sl. 5.50. *PE-2 usmjerivač, prikaz BGP tablice.*

Kako bi se ponovo omogućila veza s kraja na kraj potrebno je u usmjerivačima PE-1 i PE-2 redistribuirati MP-BGP u OSPF. Redistribuciju treba napraviti na način prikazan sl. 5.51. i sl. 5.52.

```
PE-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-1(config)#router ospf 2
PE-1(config-router)#red
PE-1(config-router)#redistribute bgp 1 subnet
PE-1(config-router)#redistribute bgp 1 subnets
```

Sl. 5.51. *PE-1 usmjerivač, redistribucija OSPF u MP-BGP.*

```
PE-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE-2(config)#router ospf 2
PE-2(config-router)#redi
PE-2(config-router)#redistribute bgp 1 sub
PE-2(config-router)#redistribute bgp 1 subnets
```

Sl. 5.52. *PE-2 usmjerivač, redistribucija OSPF u MP-BGP.*

Sl. 5.53. i sl. 5.54. prikazuju IP rute usmjerivača CE-1 i CE-2. Svrha ovog prikaza je uvidjeti adrese koje mogu biti odredišta za navedene usmjerivače.

```
CE-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
C        4.4.4.4 is directly connected, Loopback0
      5.0.0.0/32 is subnetted, 1 subnets
O IA     5.5.5.5 [110/3] via 192.168.1.1, 00:01:00, FastEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.4/32 is directly connected, FastEthernet0/0
O IA  192.168.2.0/24 [110/2] via 192.168.1.1, 00:01:00, FastEthernet0/0
```

Sl. 5.53. *CE-1 usmjerivač, prikaz IP ruta.*

```
CE-2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/3] via 192.168.2.1, 00:00:59, FastEthernet0/0
      5.0.0.0/32 is subnetted, 1 subnets
C        5.5.5.5 is directly connected, Loopback0
O IA  192.168.1.0/24 [110/2] via 192.168.2.1, 00:00:59, FastEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, FastEthernet0/0
L        192.168.2.5/32 is directly connected, FastEthernet0/0
```

Sl. 5.54. *CE-2 usmjerivač, prikaz IP ruta.*

Uvidom u IP rute CE-1 i CE-2 usmjerivača kao dokaz validnosti ruta pozvana je naredba *ping* s CE-1 usmjerivača na *loopback* adresu CE-2 usmjerivača. Sl. 5.55. prikazuje odziv na naredbu *ping*, uspjeh je stopostotan.

```
CE-1#ping 5.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 140/233/276 ms
```

Sl. 5.55. *CE-1 usmjerivač, ping naredba na loopback adresu CE-2 usmjerivača.*

Osim naredbe *ping* zanimljivo je ispitati naredbu *trace* prema istoj adresi. Sl. 5.56. prikazuje odziv na naredbu *trace* iz koje su vidljivi svi skokovi do odredišta. 1. skok je ulazna adresa f0/1 sučelja usmjerivača PE-1. 2. skok je f0/0 sučelje usmjerivača P, u ovom skoku pojavljuje se MPLS oznaka. 3. skok je izlazna adresa f0/1 sučelja usmjerivača PE-2, i ovaj skok sadrži MPLS oznaku. 4. skok je ulazna adresa f0/0 sučelja CE-2 usmjerivača.

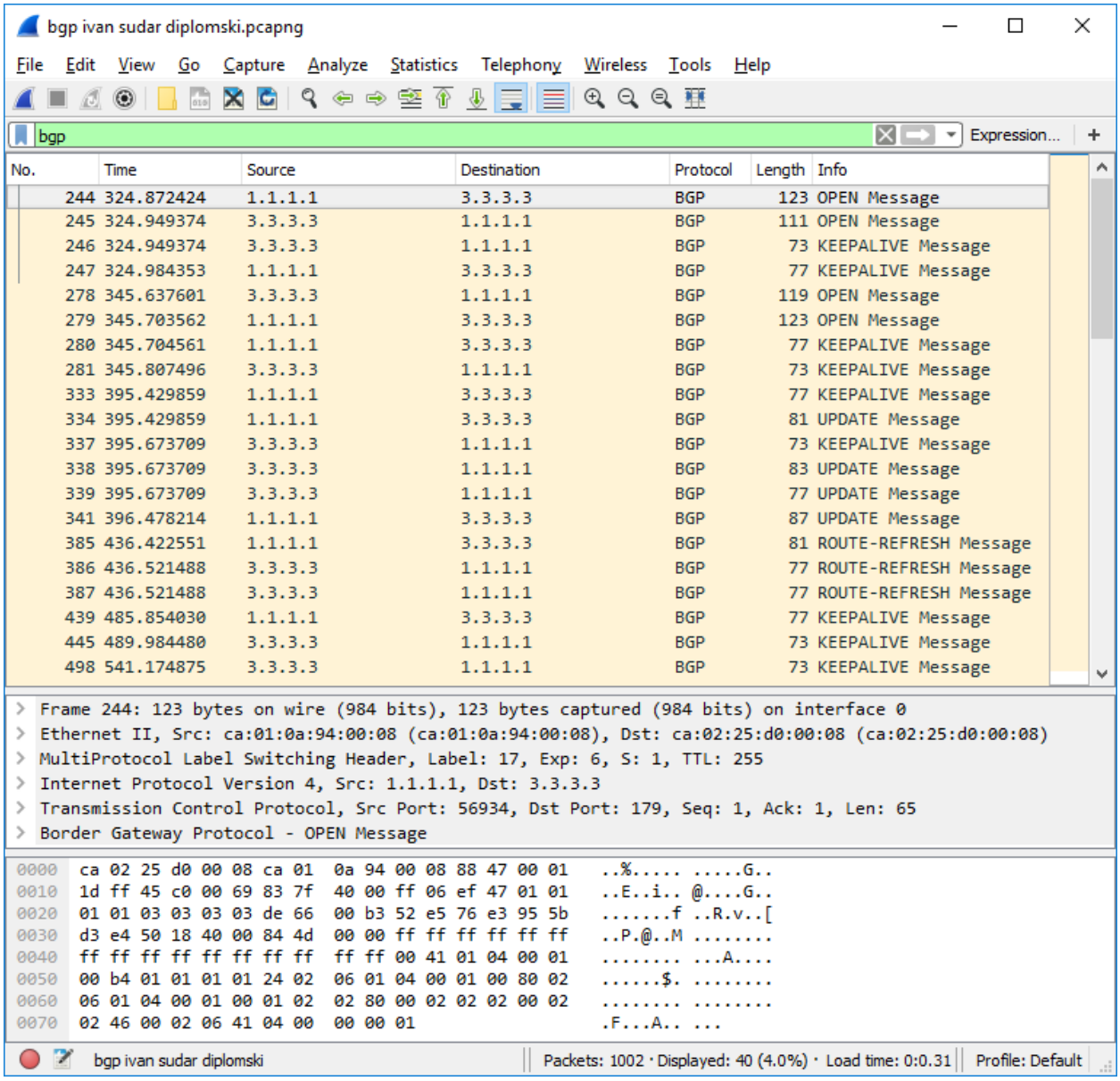
```
CE-1#trace 5.5.5.5
Type escape sequence to abort.
Tracing the route to 5.5.5.5
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 84 msec 108 msec 68 msec
  2 10.0.0.2 [MPLS: Labels 17/19 Exp 0] 216 msec 288 msec 228 msec
  3 192.168.2.1 [MPLS: Label 19 Exp 0] 172 msec 132 msec 112 msec
  4 192.168.2.5 200 msec 216 msec 176 msec
```

Sl. 5.56. *CE-1 usmjerivač, trace naredba na loopback adresu CE-2 usmjerivača.*

5.3. Analiza mrežnog prometa u kreiranoj testnoj topologiji

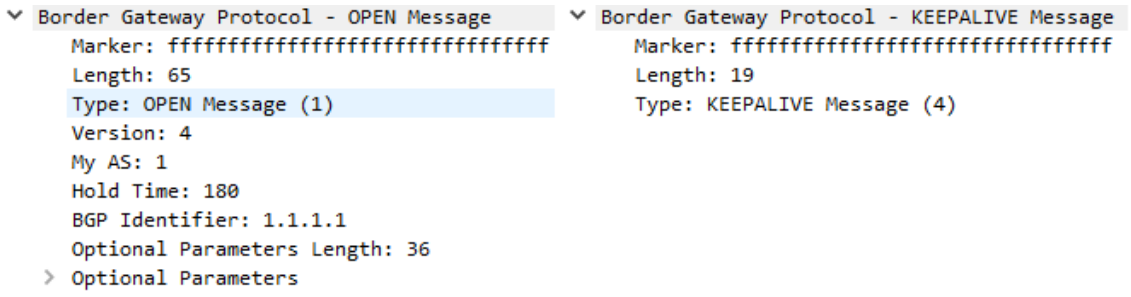
U podpoglavlju 5.2. prikazana je jedna analiza prometa u mrežnom analizatoru *Wireshark* na sl. 5.24. gdje je prikazan ICMP protokol prilikom upotrebe *ping* naredbe. Mrežni analizator prikazuje sav promet koji se odvija na određenoj vezi. Za navedenu topologiju analiza prometa postavljena je između usmjerivača PE-1 i P te se na toj vezi prikazuje sav promet koji se pojavljuje na ruti između navedenih usmjerivača. Izdvajanje određenog mrežnog prometa u *Wireskark* analizatoru omogućeno je uporabom filtera. Filter se koristi na jednostavan način i to tako da se unutar polja unese tražena vrijednost koja se želi izdvojiti. Na sl. 5.57. prikazan je izgled sučelja za vrijednost filtera *bgp*. Vidljivo je da se BGP sesija uspostavlja prvo od strane usmjerivača PE-1 prema usmjerivaču PE-2 što dokazuje da paket broj 244 poslan s izvora PE-1 usmjerivača prema odredištu PE-2 usmjerivača OPEN porukom, a paket 245 nosi odgovor na postavljanje sesije. Paketi 246 i 247 nose poruke KEEPALIVE što označava da se sesija drži otvorenom. Paket 278 nosi poruku OPEN ali ovaj puta s izvora PE-2 na odredište PE-1 što obilježava otvaranje BGP

sjednice u povratnom smjeru. Nakon što je sesija otvorena između usmjerivača razmjenjuju su poruke KEEPALIVE kojima se obnavlja BGP veza.



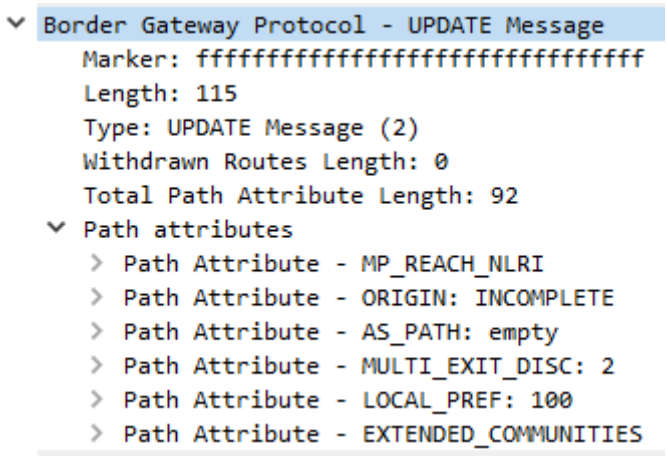
Sl. 5.57. *Wireshark mrežni analizator, BGP filter.*

Na sl. 5.58. prikazane su BGP poruke OPEN i KEEPALIVE koje potvrđuju teorijski opis u podpoglavlju 2.1. iz kojih vidimo polja definirana u teorijskom opisu da se korist u praksi. Dakle riječ je o BGP protokolu verzije 4, autonomni sustav poruke je 1, *hold time* je postavljen na 180 s što označava vrijeme između slanja dvije uzastopne KEEPALIVE poruke, BGP identifikator prikazuje adresu usmjerivača, duljina izbornih parametara je 36 okteta. Poruka KEEPALIVE nosi informacije o duljini i tipu poruke iz slike je vidljivo da je duljina 19 okteta i tip poruke je KEEPALIVE i u zagradi je ispisana verzija.



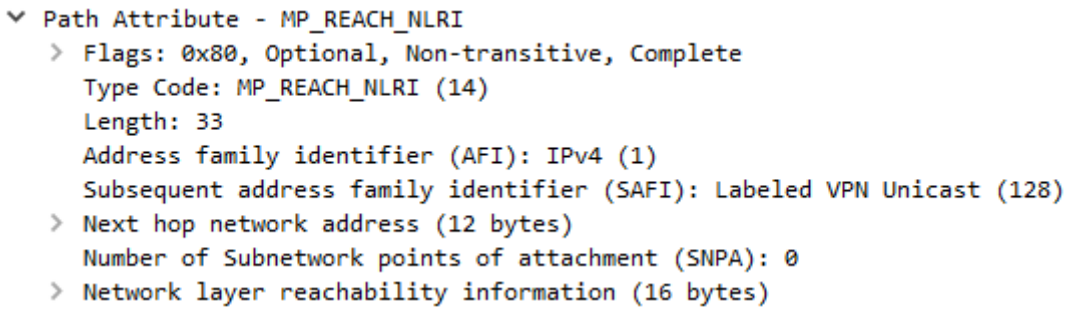
Sl. 5.58. *Wireshark mrežni analizator, BGP poruke OPEN i KEEPALIVE.*

Sl. 5.59. prikazuje zaglavlje UPDATE poruke, duljina poruke 115 okteta, duljina atributa puta je 92 okteta. Od atributa puta u ovoj poruci korišteni su sljedeći: MP_REACH_NLRI, ORIGIN: INCOMPLETE, AS_PATH: *empty*, MULTI_EXIT_DISC: 2, LOCAL_PREF: 100 i EXTENDED_COMMUNITIES.



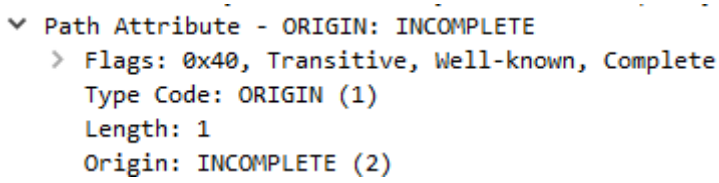
Sl. 5.59. *Wireshark mrežni analizator, BGP poruka UPDATE s pripadnim atributima puta.*

Prošireni prikaz zaglavlja navedenih atributa puta prikazanu su na: sl. 5.60. do sl. 5.65. Iz zaglavlja na sl. 5.60. prikazuje da se ovdje radi o zaglavlju BGP proširenja koje nosi informaciju o višeprotokolnoj dostupnosti odredišta opisano u podpoglavlju 3.1., a u kombinaciji AFI i SAFI polja daje informacije o skupu protokola na mrežnom sloju u kojima se mora nalaziti adresa koju nosi sljedeći skok. Duljina ovog zaglavlja iznosi 33 okteta. Bitno je uočiti da AFI polje nosi IPv4 adresnu obitelj i da SAFI polje nosi Labeled VPN Unicast adresnu obitelj što je potrebno da se dosegne odredišna adresa. Zaglavlje također nosi informaciju o mrežnoj adresi sljedećeg skoka koja zauzima 12 bajta ovog zaglavlja. NLRI polje zauzima 16 bajta ovog zaglavlja i nosi informacije o BGP prefiksu u kojem su sačuvani: RD broj i NLRI IPv4 prefiks odredišta.



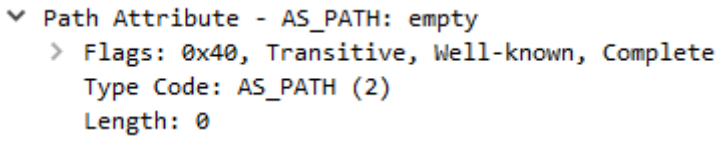
Sl. 5.60. *Wireshark mrežni analizator, MP_REACH_NLRI atribut puta.*

Sl. 5.61. prikazuje ORIGIN atribut puta, u ovom slučaju ovaj atribut ne pokazuje informacije koje su navedene u teorijskom opisu u podpoglavlju 2.2. gdje je spomenuto da u ovom atributu može naći informacija pripada li izvorni usmjerivač AS-u usmjerivača koji je primio paket. Vidimo da je ovaj atribut puta tranzitivan, dobro poznati obavezni atribut, da podrijetlo puta nije potpuno te da je duljina 1 oktet.



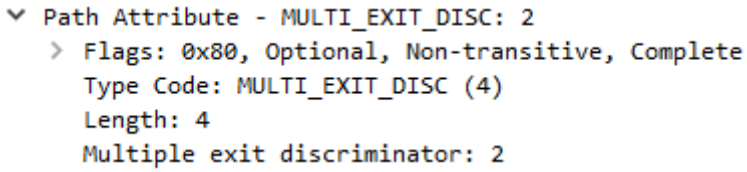
Sl. 5.61. *Wireshark mrežni analizator, ORIGIN atribut puta.*

Sl. 5.62. prikazuje AS_PATH atribut puta koji je pojašnjen u podpoglavlju 2.2., uporaba ovog atributa je za definiranje puta kao listu autonomnih sustava koje treba proći do odredišta. Iz slike je vidljivo da je ovaj atribut prazan iz razloga što je ovo manja topologija te nema potrebe za korištenjem ovog atributa, atribut ima veći značaj kod višestrukih puteva.



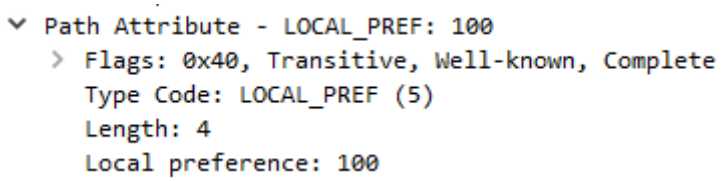
Sl. 5.62. *Wireshark mrežni analizator, AS_PATH atribut puta.*

MULTI_EXIT_DISC atribut puta je izborni lokalni atribut prikazan je na sl. 5.63., duljine 4 okteta i govori da postoje dva lokalna puta s odredišta na kojem se analizira mrežni promet.



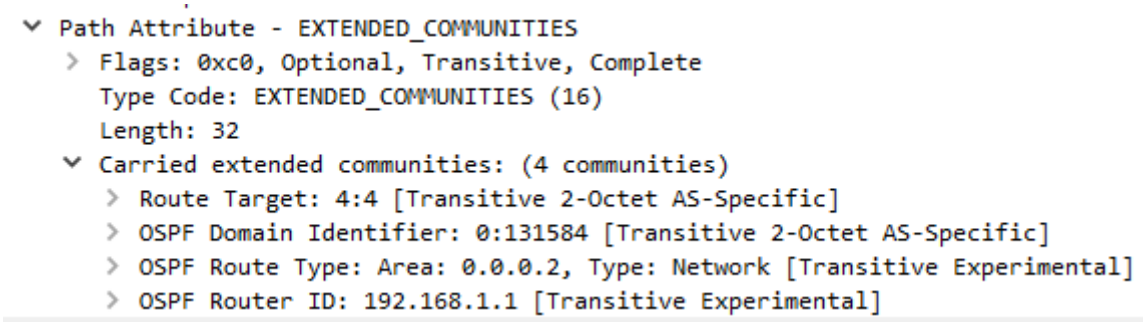
Sl. 5.63. *Wireshark mrežni analizator, MULTI_EXIT_DISC atribut puta.*

LOCAL_PREF atribut puta ima upotrebu samo onda kada postoji više izlaznih puteva iz AS-a, prikazan je na sl. 5.64., duljine 4 okteta i nosi vrijednost 100. Kada bi postojalo više izlaznih puteva odabire se put s većom vrijednosti.



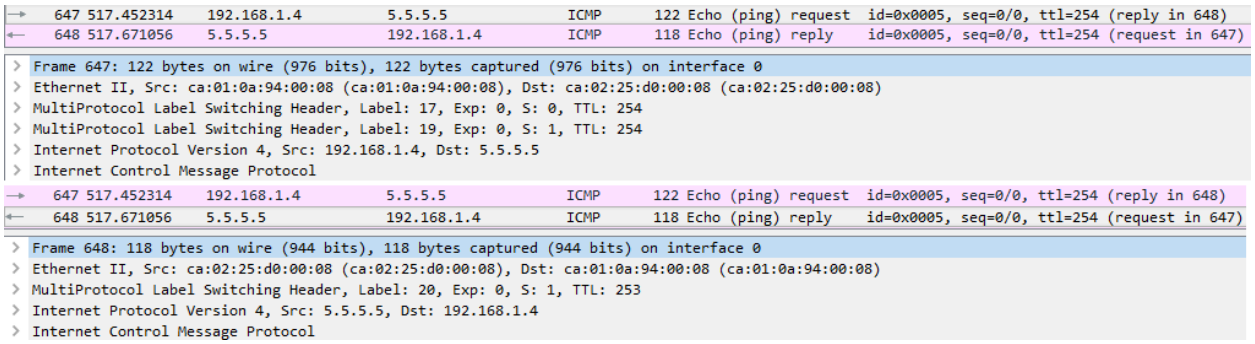
Sl. 5.64. *Wireshark mrežni analizator, LOCAL_PREF atribut puta.*

Atribut prikazan na sl. 5.65. nosi informacije o izdvojenim zajednicama, u polju Carried extended communities ispisane su 4 zajednice *(Route Target, OSPF Domain Identifier, OSPF Route Type i OSPF Router ID*)



Sl. 5.65. *Wireshark mrežni analizator, EXTENDED_COMMUNITIES atribut puta.*

Prilikom korištenja naredbe *ping* na usmjerivaču CE-1 kako bi se ispitala dostupnost usmjerivača CE-2 može se uočiti da na paket koji se šalje kao zahtjev u između Ethernet zaglavlja i IPv4 zaglavlja umetnuta dva MPLS zaglavlja od kojih jedan nosi oznaku 17, a drugi 19. Paket koji dolazi natrag kao odgovor o dostupnosti odredišta ima umetnuto samo jedno MPLS zaglavlje s oznakom 20 (sl. 5.66.). Umetanje zaglavlja potvrđuje teorijski opis razmjene oznaka prilikom slanja paketa unutar VPN mreže objašnjeno u podpoglavlju 4.3. na sl. 4.8. koja prikazuje enkapsulaciju IP paketa u različite oznake. IP paket u ovom primjeru enkapsulira u MPLS oznaku, a oznaka mu je dodijeljena za rutu koja najbolje odgovora odredišnoj adresi.



Sl. 5.66. *Wireshark mrežni analizator, prikaz enkapsulacije paketa u oznake.*

Iz analize mrežnog prometa i same analize konfiguracije u drugoj topologiji može se zaključiti kako konfiguracija BGP-a zbog velike fleksibilnosti PE usmjerivača nije toliko složena. Naravno ništa nije složeno ukoliko je korisnik upoznat s tehnologijom i sustavima mrežnih operatora, ali i sam sustav s kojim se susreće. Prilikom postavljanja topologije vidljivo je da se središnji P usmjerivač postavlja samo jednom i iz tog razloga potrebno je predvidjeti tražene kapacitete te u skladu s potrebama mreže postaviti jezgrene čvorove. Što se tiče rubnih čvorova okosnice, korisnik ima na raspolaganju stvoriti bilo koji vrstu VPN mreže. Sa stajališta jezgrene mreže nije bitno koristi li se RIP ili EIGRP jer jednom postavljena MPLS mreža unutar jezgre ne treba dodatnu konfiguraciju izvan jezgre. Stoga je na takvu jezgru lako dodati bilo koji oblik VPN-a. *Wireshark* analizom mrežnog prometa lako je uočiti ispravnu konfiguraciju i postojanje svih konfiguriranih protokola. Osim što je dokazano korištenje LDP i BGP protokola također se može primijetiti enkapsulacija IP zaglavlja u MPLS oznake.

6. ZAKLJUČAK

BGP protokol nalazi svoju primjenu i u virtualnim privatnim mrežama. Sam rad protokola zasniva se na slanju specifičnih poruka između usmjerivača. Za komunikaciju između usmjerivača potrebno je poznavati atribute puta koji protokolu pomažu odrediti rutu slanja paketa, a osim atributa potrebno je poznavati i algoritme za određivanja ruta. Poruke i atributi ruta posjeduju brojna polja unutar zaglavlja koja predstavljaju osnovne informacije. Kako bi protokol lakše mogao određivati rute potrebne su mu informacije o dostupnosti usmjerivača te su osmišljene značajke višeprotokolne dostupnosti određenih usmjerivača. Postavljanjem virtualne privatne mreže klijentu se omogućuje fleksibilnost i sigurnost pri slanju poruka između računala. BGP protokol pronalazi primjenu u VPN sustavu pri distribuciji ruta. Za distribuciju ruta potrebno je postaviti RD i RT brojeve za pojedine uređaje. RD broj je nasumični broj kojemu je osnovna uloga razlikovanje odredišta ukoliko se dogodi da više odredišta ima isti RT broj. BGP protokol ima mogućnost korištenja reflektora ruta, što omogućava skalabilnost mreže. Umjesto da svaki PE usmjerivač posjeduje adresu drugih PE usmjerivača, reflektor ruta omogućava informacije o rutama za sve PE uređaje, što svakako smanjuje listu ruta unutar usmjerivača. Prilikom prosljeđivanja paketa preko MPLS okosnice BGP omogućuje enkapsulaciju IP zaglavlja unutar drugih oznaka, najčešće je to MPLS oznaka jer unutar jezgre mreže usmjerivači za međusobnu komunikaciju razmjenjuju promet putem oznaka.

U praktični dijelu prikazane su dvije topologije mreže. Prva topologija prikazuje osnovnu uporabu BGP protokola u kojoj su prikazana dva autonomna sustava te je dokazano da je moguće izmjenjivati poruke između dva autonomna sustava pomoću BGP-a. Naredbama *ping* i *tracert* pokazano je da je moguće pristupiti s računala jednog autonomnog sustava na drugi te ispis rute kojom prolazi paket prilikom dostavljanja na odredište.

Druga topologija prikazuje uporabu BGP protokola u jednoj jednostavnijoj VPN mreži. Rad unutar GNS3 simulatora uvelike je olakšao stvaranje ovog diplomskog rada jer GNS3 koristi simulacije stvarnih uređaja te je vrlo jednostavno bilo postaviti topologiju unutar simulatora imajući na umu da nije moguće doći do nekakve pogreške unutar samog simulatora. Jedina greška koja se može dogoditi je ljudska nepažnja. Uz GNS3 simulator dolazi i mrežni analizator *Wireshark* koji omogućuje vrlo jednostavno snimanje mrežnog prometa, na način da se snimač postavi na određenu vezu unutar mreže te je prilikom snimanja omogućeno korisniku pratiti sav promet koji prolazi odabranom vezom.

Kako bi se omogućio rad BGP-a unutar VPN mreže potrebno je na uređajima prije svega pravilno postaviti IP adrese, pravilno postaviti MPLS jezgru u kojoj dva PE usmjerivača komuniciraju pomoću BGP-a, pravilno postaviti VRF koji će omogućiti rubnim usmjerivačima unutar jezgre da prosljeđuju pakete između autonomnih sustava. Analizom topologije utvrđeno je postojanje konfiguracije BGP-a unutar jezgre prilikom čega je moguće vidjeti poruke koje se razmjenjuju te atribute puta koje nosi poruka UPDATE. Daljnjom analizom potvrđena je enkapsulacija IP zaglavalja u MPLS oznake prilikom slanja paketa između PE usmjerivača između kojih je postavljen BGP.

7. LITERATURA

[1] A Border Gateway Protocol 4 (BGP-4), Dostupno na: https://tools.ietf.org/html/rfc4271 (20. lipanj 2018.)

[2] How does BGP work?, Dostupno na: https://thetechtalky.com/how-does-bgp-work (20.lipanj 2018.)

[3] BGP messages types, Dostupno na: http://ipexptobe.blogspot.com/2011/09/bgp-message-types.html (20. lipanj 2018.)

[4] BGP path atributes., Dostupno na: http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8164_mrg/content/ch15s07.html (20. lipanj 2018.)

[5] Autonomous System Confederations for BGP, Dostupno na: https://tools.ietf.org/html/rfc1965 (5. rujna 2018.)

[6] BGP Finite State Machine, Dostupno na: https://bigevilsciscoworld.wordpress.com/2010/05/14/bgp-finite-state-machine/ (5. rujna 2018.)

[7] Border Gateway Protocol: The Biggest Network Vulnerability Of All?, Dostupno na: https://www.techopedia.com/2/28494/security/border-gateway-protocol-the-biggest-network-vulnerability-of-all

(20. lipanj 2018.)

[8] Multiprotocol Extensions for BGP-4, Dostupno na: https://tools.ietf.org/html/rfc4760

(25. lipanj 2018.)

[9] BGP/MPLS IP Virtual Private Networks (VPNs), Dostupno na: https://tools.ietf.org/html/rfc4364 (25. lipanj 2018.)

[10] Virtualna privatna mreža (VPN), Dostupno na: http://mreze.layer-x.com/s060000-0.html (25. lipanj 2018)

[11] Osnovni koncepti VPN tehnologije, Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf

(10. kolovoz)

[12] Dostupno na: https://www.google.hr/search?q=router+reflector&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjnnO2AmazdAhVptIsKHfCTDLAQ_AUICigB&biw=1600&bih=773#imgrc=JZARg7o8GIa.XqM: (7. rujna 2018.)

[13] Integrating Core BGP/MPLS Networks - The Internet Protocol Journal, Volume 13, No.4, Dostupno na: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-50/134-bgp.html (10. kolovoz)

[14] MPLS VPN Components, Dostupno na: http://gponsolution.com/mpls-vpn-components-basic-knowledge.html (10. kolovoz)

[15] Route Distinguisher & its types, Dostupno na: https://sites.google.com/site/amitsciscozone/home/important-tips/mpls-wiki/route-distinguisher-its-types (20. kolovoz 2018)

[16] Route Distinguisher and Route Targets, Dostupno na: http://packetlife.net/blog/2013/jun/10/route-distinguishers-and-route-targets/ (20. kolovoz 2018)

[17] Route Distinguisher and Route Target - MPLS Tutorial. Dostupno na: https://www.rogerperkin.co.uk/ccie/mpls/route-distinguisher-vs-route-target/ (20. kolovoz 2018)

[18] 04-IP Routing Volume, Dostupno na: http://www.h3c.com.hk/Technical_Support___Documents/Technical_Documents/Security_Products/H3C_SecPath_F1000-E/Configuration/Operation_Manual/H3C_SecPath_High-End_OM(F3169_F3207)-5PW106/04/201109/725883_1285_0.htm (20. kolovoz 2018)

[19] hAP lite TC, Dostupno na: https://mikrotik.com/product/RB941-2nD-TC (25. kolovoz 2018.)

[20] Winbox, Dostupno na: https://wiki.mikrotik.com/wiki/Manual (25. kolovoz 2018.)

[21] Mikrotik RouterOS, Dostupno na: http://www.informationbeam.net/downloads/MikroTik%20RouterOS%20Online%20Training%20Class/MIKROTIK_ROS_OTC_I-BEAM_CH07.pdf (25. kolovoz 2018)

[22] GNS3, Dostupno na: https://www.gns3.com/ (1. rujna 2018)

8. POPIS KRATICA I SIMBOLA

KRATICA	ZNAČENJE
AFI	engl. Address Family Identifier
AS	engl. Autonomous System
ASN	engl. Autonomous System Number
BGP	engl. Border Gateway Protocol
CE	engl. Customer Edge
CIDR	engl. Classless Inter-Domain Routing
DES	engl. Dana Encrytpion Standard
EBGP	engl. External Border Gateway Protocol
EGP	engl. Exterior Gateway Protocol
GNS3	engl. Graphic Network Simulator
IANA-AF	engl. Internet Assigned Numbers Authority – Address Family
IBGP	engl. Internal Border Gateway Protocol
IGP	engl. Interior Gateway Protocol
IP	engl. Internet Protocol
ISP	engl. Internet Service Provider
LAN	engl. Local Area Network
LDP	engl. Label Distribution Protocol
MPLS	engl. Multiprotocol Label Switching
NLRI	engl. Network Layer Reachability Information
ORF	engl. Outbound Route Filters
P	engl. Provider
PE	engl. Provider Edge
PIB	engl. Policy Information Base

RD	engl. Route Distinguisher
RIB	engl. Routing Information Base
RSA	Tip kriptosustava, naziv iz prezimena osnivača
RT	engl. Route Target
SAFI	engl. Subsequent Address Family Identifier
SP	engl. Service Provider
TCP	engl. Transmission Control Protocol
VPN	engl. Virtual Private Network
VPNv4	engl. Virtual Private Network version 4
VRF	engl. Virtual Routing and Forwarding

9. SAŽETAK

Ključne riječi: Border Gateway Protokol, autonomni sustavi, Virtualne Privatne Mreže, protokoli, IP adrese, jezgrena mreža, MPLS, GNS3, adresne obitelji.

U radu je bilo potrebno navesti pregled značajki BGP (engl. *Border Gateway Protocol*) usmjerivačkog protokola te analizirati primjenu BGP protokola u virtualnim privatnim mrežama (VPN, engl. *Virtual Private Network*). Značajke BGP protokola su višeprotokolna proširenja koja olakšavaju rad pri definiranju dostupnosti određenih usmjerivača. Primjena BGP protokola u VPN zasniva se na distribuciji ruta. Prilikom uspostave BGP-a uspostavlja se sjednica između rubnih usmjerivača jezgrene mreže. Analizom mrežnog prometa vidljive su BGP poruke koje se razmjenjuju nakon pokrenute sjednice. Osim BGP poruka također s mogu vidjeti i BGP atributi puta što je pokazano prilikom konfiguracije topologije u GNS3 simulatoru za prikaz uporabe BGP protokola u VPN-u. Prilikom provjere dostupnosti odredišta također se može provjeriti enkapsulacija IP zaglavlja unutar MPLS oznaka. Glavni preduvjeti za postavljanje BGP unutar VPN-a su postavljanje MPLS jezgrene mreže te VRF puteva između CE usmjerivača.

10. ABSTRACT

Keywords: Border Gateway Protocol, autonomous systems, VPNs, protocols, IP address, backbone core, MPLS, GNS3, address family.

In this paper, it was necessary to review the BGP routing protocol features and analyze the application of BGP protocols in virtual private networks. BGP protocols feature multi protocols that make it easier to work on defining the availability of certain routers. The application of the BGP protocol to the VPN is located in the route distribution. When establishing a BGP, a session is established between the peripheral router cores. Analyzing network traffic shows BGP messages that are exchanged after the sessions are started. In addition to the BGP message, you can also see the BGP path attributes shown in the topology configuration in the GNS3 simulator to display the BGP protocol usage in the VPN. When checking the availability of the destination, it is also possible to check the encapsulation of the IP header within the MPLS tag. The main prerequisites for setting up BGP within the VPN are setting the MPLS core network and VRF routes between the CE routers.

11. ŽIVOTOPIS

Ivan Sudar rođen je 24. kolovoza 1994. godine u Vinkovcima. Od rođenja živi u Ivankovu, gdje je završio Osnovnu školu „August Cesarec“. Nakon osnovnoškolskog obrazovanja 2009. godine upisuje Tehničku školu Ruđera Boškovića u Vinkovcima smjer mehatronika. Nakon završenih svih razreda s odličnim uspjehom 2013. godine izravnim upisom upisuje preddiplomski studij elektrotehnike, smjer Komunikacije i informatika na Elektrotehničkom fakultetu u Osijeku koji kasnije mijenja naziv u Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku. Nakon završenog preddiplomskog studija 2016. godine upisuje diplomski studij, smjer Mrežne tehnologije.