SVEUČILIŠTE ALGEBRA

Sistemsko inženjerstvo

INDIVIDUALNI PROJEKTNI ZADATAK

SIP – Mrežni dio

Marin Krešić

Zagreb, 04.06.2026.

Sadržaj

1. Uvod

Suvremeno poslovanje distribuiranih organizacija zahtijeva pouzdanu mrežnu infrastrukturu koja omogućuje neometanu komunikaciju između geografski udaljenih lokacija. Tvrtka ASI ltd. posluje na četiri lokacije: tri podružnice u Ljubuškom, Grudama i Čapljini te podatkovni centar u Zagrebu. Potrebno je mrežno rješenje koje osigurava povezanost svih lokacija, pristup internetu i otpornost na ispade pojedinih mrežnih segmenata.

Cilj ovog projektnog zadatka je projektiranje i implementacija cjelovite mrežne infrastrukture za tvrtku ASI ltd. u mrežnom simulatoru GNS3 korištenjem Cisco IOS usmjernika. Zadatak obuhvaća konfiguraciju svih mrežnih usluga potrebnih za svakodnevno poslovanje, od automatskog dodjeljivanja IP adresa putem DHCP-a i pristupa internetu uz NAT, do naprednih tehnologija poput MPLS L3 VPN-a kao primarne komunikacije između podružnica, GRE tunela zaštićenih IPSec enkripcijom kao rezervnog puta te HSRP protokola za redundanciju pristupa internetu u podatkovnom centru.

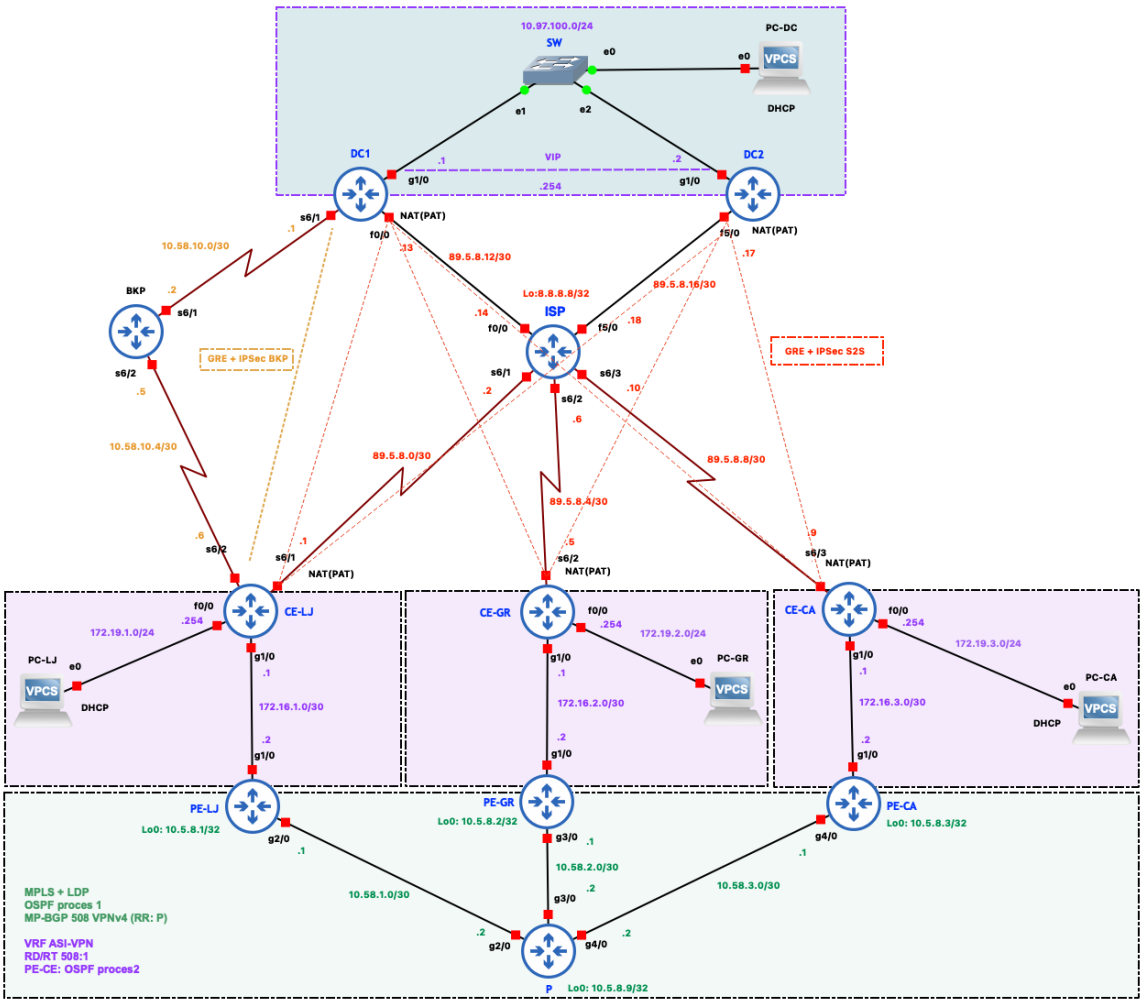
Poseban naglasak stavljen je na otpornost mreže na ispade. Implementiran je višerazinski mehanizam failovera koji osigurava komunikaciju čak i u slučaju otkaza pojedinih linkova ili cijelih segmenata mreže. Redoslijed failovera strogo je definiran: MPLS kao primarni put, GRE+IPSec VPN tuneli kao prvi rezervni put te dedicirani backup link kao krajnje rješenje.

Osim bazne implementacije, zadatak uključuje tri migracijska scenarija koji demonstriraju prijelaz s jedne tehnologije na drugu uz minimalni prekid u radu mreže: migraciju protokola usmjeravanja s EIGRP-a na OSPF na PE-CE segmentu, migraciju sa statičkog na dinamičko usmjeravanje kroz S2S tunele te migraciju sa S2S IPSec tunela na DMVPN Dual-Hub rješenje faze 3.

2. Topologija mreže i adresni plan

2.1. Opis topologije

Mrežna topologija tvrtke ASI ltd. sastoji se od četiri lokacije povezane putem ISP-a (engl. Internet Service Provider) i MPLS provider mreže. Na slici 2.1 prikazana je cjelokupna topologija implementirana u GNS3 simulatoru.

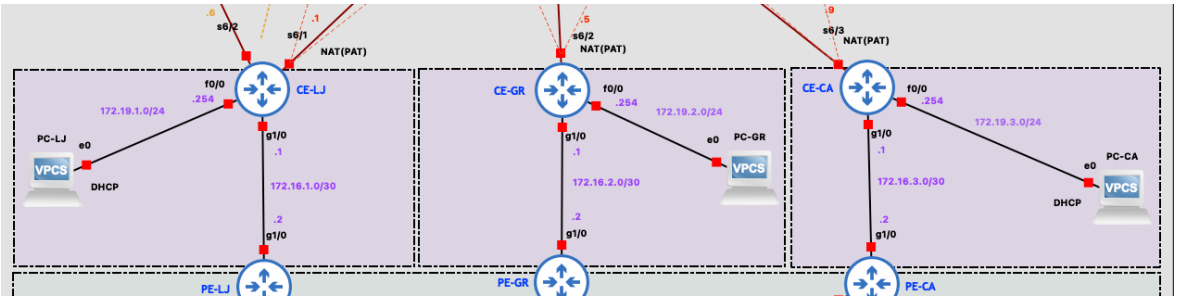


Slika 2.1 Topologija mreže tvrtke ASI Ltd.

Topologija se može podijeliti na tri logička segmenta:

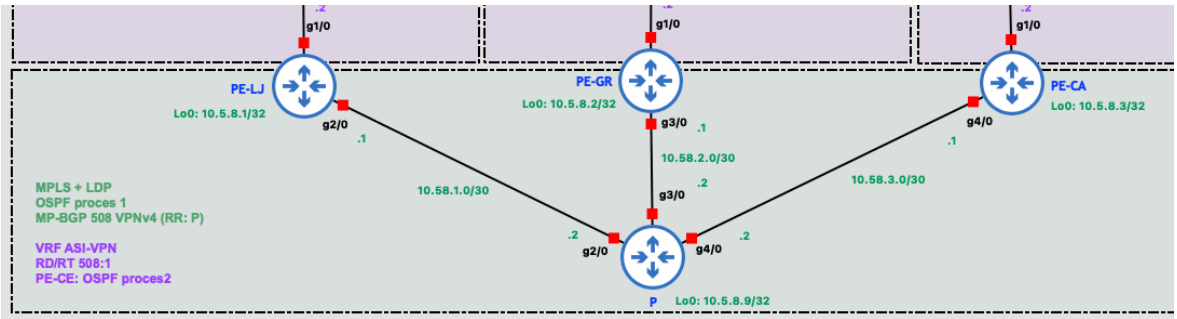
Korisnički segment (podružnice) obuhvaća tri lokacije: Ljubuški (CE-LJ), Grude (CE-GR) i Čapljinu (CE-CA). Svaka podružnica ima CE (engl. Customer Edge) usmjernik koji povezuje lokalnu mrežu (LAN) s ostatkom infrastrukture. Na LAN strani svaki CE

usmjernik služi kao DHCP poslužitelj i default gateway za korisničke uređaje. Na WAN strani svaki CE ima tri veze: serial link prema ISP-u za pristup internetu, GigabitEthernet link prema PE usmjerniku za MPLS pristup te GRE+IPSec tunele preko interneta prema podatkovnom centru. CE-LJ dodatno ima serial vezu prema BKP usmjerniku koja služi kao krajnji rezervni put prema podatkovnom centru.



Slika 2.2 Topologija mreže tvrtke ASI Ltd. – korisnički segment

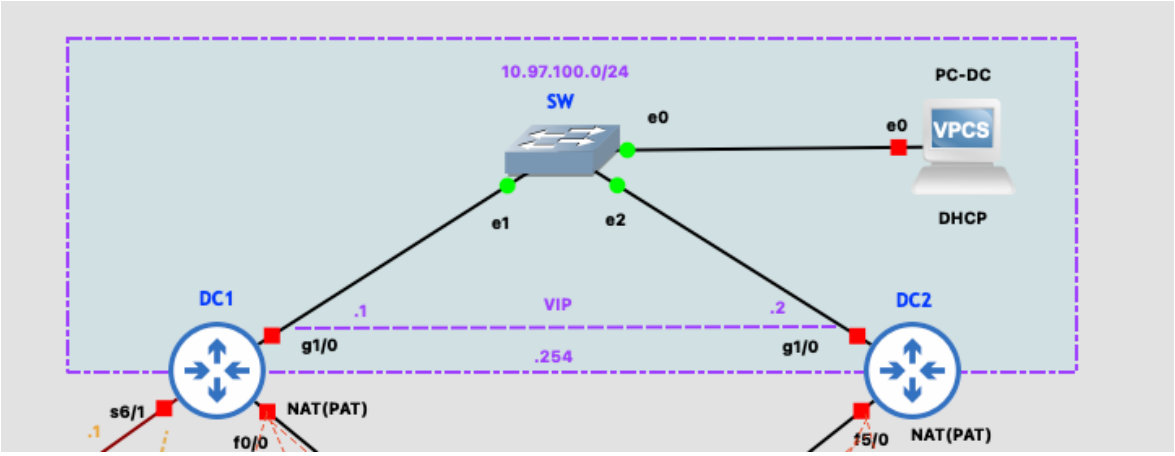
Provider segment (MPLS core) čini jezgru mreže i sastoji se od tri PE (engl. Provider Edge) usmjernika (PE-LJ, PE-GR, PE-CA) i jednog P (engl. Provider) usmjernika u topologiji zvijezde. P usmjernik je središnja točka, svaki PE je spojen na P. Na ovom segmentu radi OSPF, MPLS s LDP-om (engl. Label Distribution Protocol) za label switching te MP-BGP (engl. Multiprotocol BGP) s VPNv4 address-family za razmjenu VPN ruta. P usmjernik ima ulogu BGP route-reflectora čime se izbjegava potreba za full-mesh BGP sesijama između PE usmjernika.



Slika 2.3 Topologija mreže tvrtke ASI Ltd. – Provider segment

Podatkovni centar (DC) nalazi se u Zagrebu i sastoji se od dva usmjernika, DC1 (primarni gateway) i DC2 (rezervni gateway), spojenih na zajednički LAN segment (10.97.100.0/24) putem Ethernet preklopnika (SW). DC1 i DC2 koriste HSRP (engl. Hot Standby Router Protocol) s virtualnom IP adresom 10.97.100.254 kao gateway za uređaje na DC LAN-u. Oba DC usmjernika imaju internet pristup putem zasebnih serial linkova prema ISP-u te

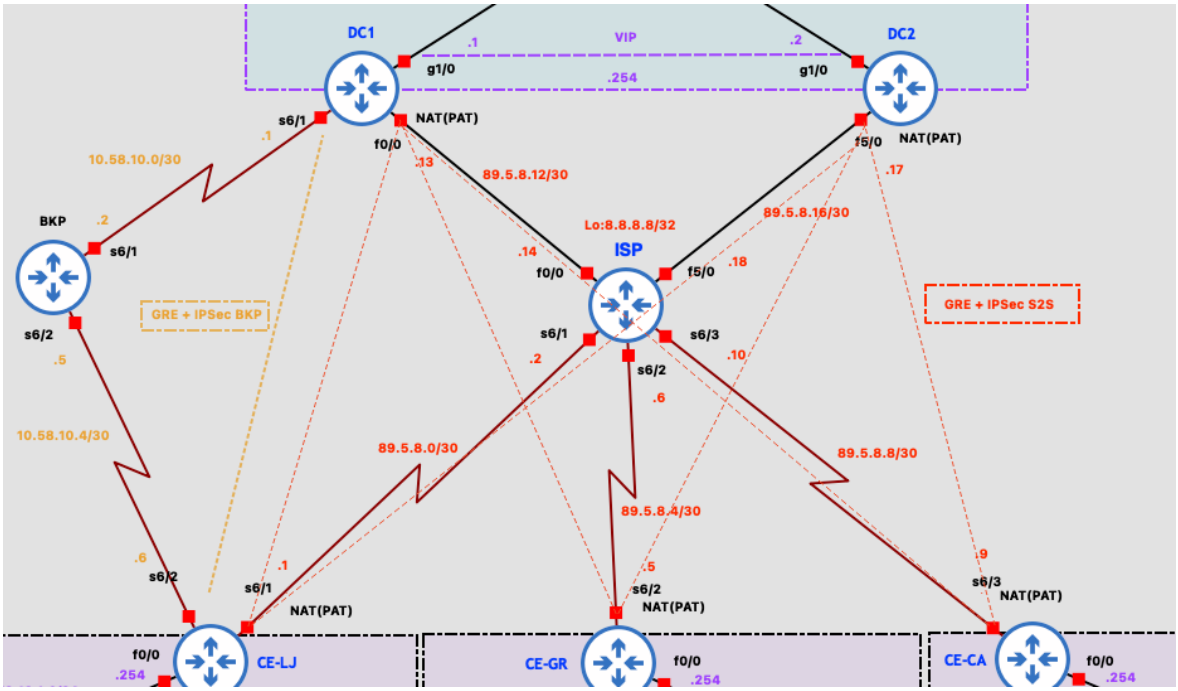
GRE+IPSec tunele prema svim podružnicama. DC1 dodatno ima serial vezu prema BKP usmjerniku za scenarij potpunog pada DC internet pristupa.



Slika 2.4 Topologija mreže tvrtke ASI Ltd. – DC segment

ISP usmjernik simulira pružatelja internetskih usluga. Spojen je na sve CE usmjernike i oba DC usmjernika putem serial linkova. Na Loopback0 sučelju ima adresu 8.8.8.8/32 koja služi za testiranje internet povezanosti (simulira javni DNS poslužitelj).

BKP usmjernik služi isključivo kao relay između CE-LJ i DC1 za scenarij kad CE-LJ izgubi i ISP i MPLS vezu. Spojen je serial linkom na DC1 (s6/1) i na CE-LJ (s6/2).



Slika 2.5 Topologija mreže tvrtke ASI Ltd. – ISP i BKP usmjernici

2.2. Adresni plan

Adresni plan izveden je iz datuma rođenja autora: **05.08.1997.** Način izvođenja pojedinih adresnih blokova prikazan je u nastavku.

2.2.1. Način generiranja adresa

- Privatne LAN adrese podružnica: 172.19.X.0/24 — broj 19 izveden iz godine (19.97), X = redni broj podružnice (1, 2, 3)
- Javni WAN adresni prostor: 89.5.8.0/24 — dan (05) i mjesec (08) iz datuma rođenja
- MPLS core linkovi: 10.58.X.0/30 — spoj dana i mjeseca (5+8=58), X = redni broj linka
- MPLS Loopback adrese: 10.5.8.X/32 — dan i mjesec iz datuma rođenja
- DC LAN: 10.97.100.0/24 — godina rođenja (97)
- BGP ASN: 508 — dan i mjesec (05.08.) bez točke
- EIGRP AS: 197 — zadnje tri znamenke godine (1997)
- VRF Route Distinguisher i Route Target: 508:1 — BGP ASN + redni broj VPN-a
- GRE tunelske adrese: 10.10.X0.0/30 — tuneli prema DC1, 10.10.X0+10.0/30 — tuneli prema DC2 (X = redni broj podružnice)

2.2.2. Adresne tablice

Tablica 2.1 LAN mreže

Lokacija	Podmreža	Gateway	DHCP
Ljubuški (LJ)	172.19.1.0/24	172.19.1.254	.1-.239
Grude (GR)	172.19.2.0/24	172.19.2.254	.1-.239
Čapljina (CA)	172.19.3.0/24	172.19.3.254	.1-.239
DC - Zagreb	10.97.100.0/24	10.97.100.254 (VIP)	statički

Tablica 2.2 Javne WAN veze (prema ISP-u)

Veza	Podmreža	CE/DC sučelje	CE/DC IP	ISP sučelje	ISP IP

CE-LJ – ISP	89.5.8.0/30	S6/1	.1	S6/1	.2
CE-GR – ISP	89.5.8.4/30	S6/2	.5	S6/2	.6
CE-CA - ISP	89.5.8.8/30	S6/3	.9	S6/3	.10
DC1 – ISP	89.5.8.12/30	F0/0	.13	F0/0	.14
DC2 – ISP	89.5.8.16/30	F5/0	.17	F5/0	.18

Tablica 2.3 MPLS core linkovi

Veza	Podmreža	Usmjernik A	Usmjernik B
PE-LJ - P	10.58.1.0/30	PE-LJ g2/0 (.1)	P g2/0 (.2)
PE-GR - P	10.58.2.0/30	PE-GR g3/0 (.1)	P g3/0 (.2)
PE-CA - P	10.58.3.0/30	PE-CA g4/0 (.1)	P g4/0 (.2)

Tablica 2.4 MPLS Loopback adrese

Usmjernik	Loopback0
PE-LJ - P	10.5.8.1/32
PE-GR - P	10.5.8.2/32
PE-CA - P	10.5.8.3/32
P	10.5.8.9/32

Tablica 2.5 PE-CE veze (VRF)

Veza	Podmreža	CE (g1/0)	PE (g1/0)
CE-LJ — PE-LJ	172.16.1.0/30	.1	.2
CE-GR — PE-GR	172.16.2.0/30	.1	.2
CE-CA — PE-CA	172.16.3.0/30	.1	.2

Tablica 2.6 GRE+IPSec tuneli prema DC1 (primarni hub)

Tunel	Podmreža	Strana DC1	Strana podružnice

CE-LJ — DC1 (Tunel10)	10.10.10.0/30	.1	.2
CE-GR — DC1 (Tunel20)	10.10.20.0/30	.1	.2
CE-CA — DC1 (Tunel30)	10.10.30.0/30	.1	.2

Tablica 2.7 GRE+IPSec tuneli prema DC2 (rezervni hub)

Tunel	Podmreža	Strana DC2	Strana podružnice
CE-LJ — DC2 (Tunel40)	10.10.40.0/30	.1	.2
CE-GR — DC2 (Tunel50)	10.10.50.0/30	.1	.2
CE-CA — DC2 (Tunel60)	10.10.60.0/30	.1	.2

Tablica 2.8 Backup link (DC1- BKP – CE-LJ)

Veza	Podmreža	Strana A	Strana B
DC1 (s6/1) — BKP (s6/1)	10.58.10.0/30	DC1 .1	BKP .2
BKP (s6/2) — CE-LJ (s6/2)	10.58.10.4/30	BKP .5	CE-LJ .6

Tablica 2.9 VRF i BGP parametri

Parametar	Vrijednost
VRF ime	ASI-VPN
Route Distinguisher (RD)	508:1
Route Target (import/export)	508:1
BGP ASN (provider)	508
EIGRP ASN (PE-CE)	197

3. Bazna konfiguracija mrežnih usluga

Ovo poglavlje opisuje implementaciju baznih mrežnih usluga koje čine osnovu poslovanja tvrtke ASI ltd. Redoslijed izlaganja prati logiku izgradnje mreže od usluga najbližih krajnjem korisniku (DHCP i pristup internetu putem NAT-a), preko primarne komunikacije među podružnicama (MPLS L3 VPN), do sekundarnog komunikacijskog puta (GRE tuneli sa IPSec enkripcijom) te zaštite mreže od neovlaštenog pristupa s interneta (access liste).

3.1. DHCP poslužitelj na podružnicama

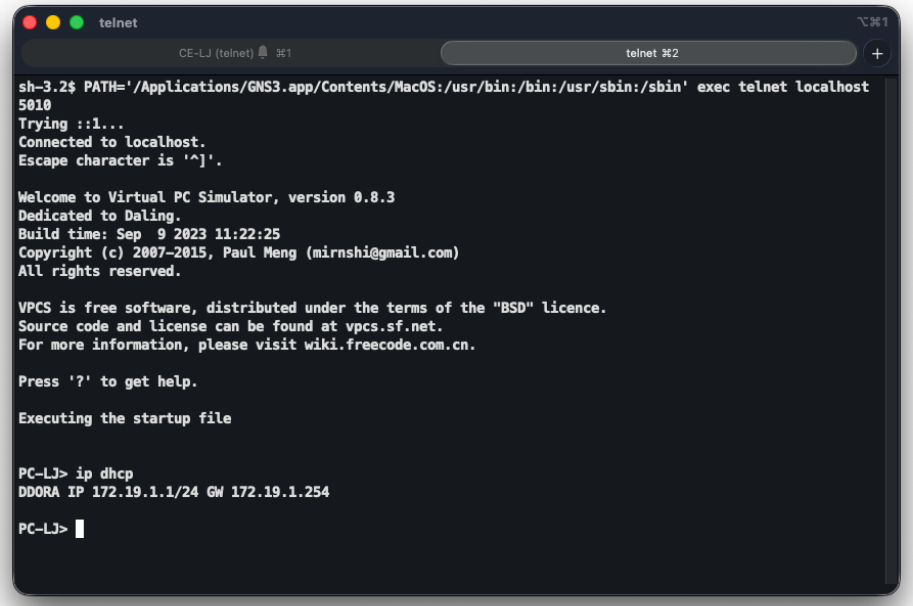
Kako bi korisnička računala u svakoj podružnici automatski dobivala mrežnu konfiguraciju, na svakom CE usmjerniku konfiguriran je DHCP (engl. Dynamic Host Configuration Protocol) poslužitelj. Time se izbjegava ručno postavljanje IP adresa na svakom uređaju te se osigurava dosljednost mrežnih postavki unutar lokalne mreže. Primjer na CE-LJ:

```
ip dhcp excluded-address 172.19.1.240 172.19.1.255
ip dhcp pool LAN-LJ
 network 172.19.1.0 255.255.255.0
 default-router 172.19.1.254
 dns-server 8.8.8.8
```

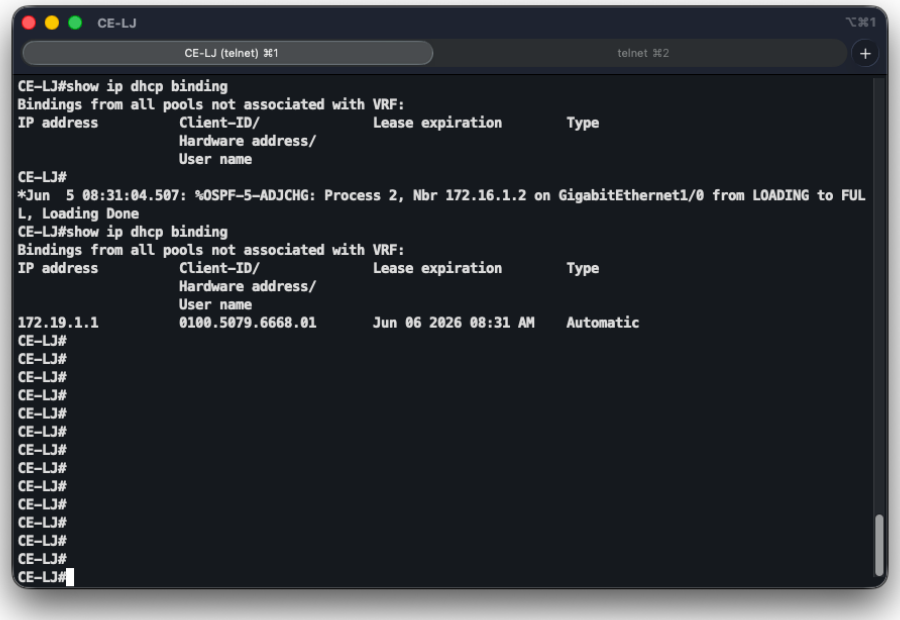
Naredbom `ip dhcp excluded-address` iz raspona za automatsko dodjeljivanje isključuju se gornje adrese (.240 do .255) koje su rezervirane za mrežnu opremu, prije svega za adresu default gatewaya (.254). Bez ovog isključenja postojala bi opasnost da poslužitelj dodijeli adresu gatewaya korisničkom računalu, što bi izazvalo sukob adresa. Naredba `network` definira podmrežu iz koje se dijele adrese, čime računala dobivaju adrese u rasponu od .1 do .239. Parametrom `default-router` računalima se zadaje adresa default gatewaya, a to je FastEthernet0/0 sučelje CE usmjernika preko kojeg sav promet izvan lokalne mreže napušta podružnicu. Naposljetku, `dns-server` zadaje poslužitelj za razrješavanje imena; u simulaciji se koristi javni Googleov poslužitelj 8.8.8.8 koji ujedno odgovara Loopback0 adresi ISP usmjernika pa služi i za provjeru internetske povezanosti.

Ispravnost rada provjerava se na korisničkom PC (VPCS u simulatoru GNS3) naredbom `ip dhcp`, nakon čega računalo dobiva adresu iz očekivanog raspona. Na CE usmjerniku

naredba `show ip dhcp binding` prikazuje popis dodijeljenih adresa zajedno s pripadajućim MAC adresama uređaja.



Slika 3.1 Dodijeljene DHCP adrese na podružnici Ljubuški



Slika 3.2 Dobivena adresa DHCP-om na klijentu

3.2. NAT i pristup internetu

Kako podružnice u lokalnim mrežama koriste privatne adrese koje nisu rutabilne na javnom internetu, na svakom CE usmjerniku konfiguriran je NAT (engl. Network Address Translation) u izvedbi PAT (engl. Port Address Translation, poznat i kao *overload*). Time svi uređaji jedne podružnice pristupaju internetu tako da dijele jednu javnu IP adresu konfiguriranu na WAN sučelju CE usmjernika.

Preduvjet za rad NAT-a bila je konfiguracija ISP usmjernika. Na njemu je postavljena Loopback0 adresa 8.8.8.8 koja simulira internet i javni DNS, te su konfigurirana serijska sučelja prema svim CE usmjernicima i podatkovnom centru s adresama prema adresnom planu. Primjer na CE-LJ:

```
interface FastEthernet0/0
 ip nat inside
interface Serial6/1
 ip nat outside
!
ip nat inside source list 1 interface Serial6/1 overload
access-list 1 permit 172.19.1.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 89.5.8.2
```

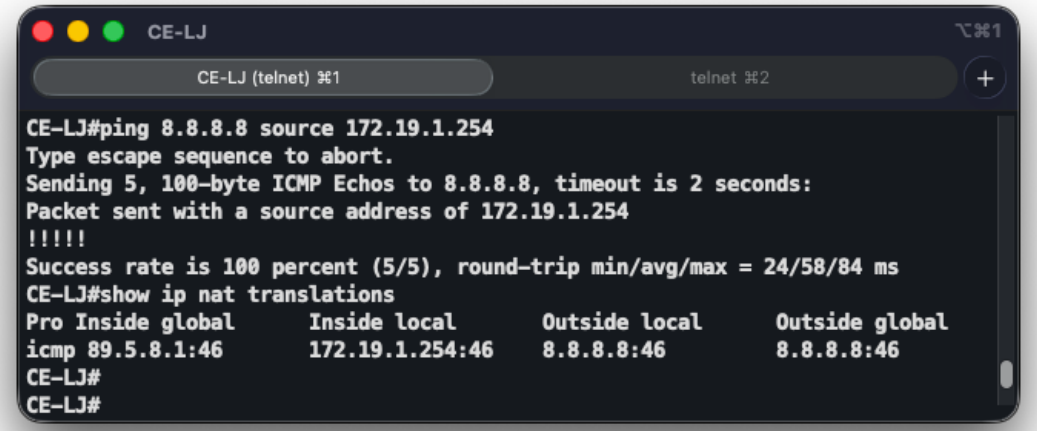
Sučelje prema lokalnoj mreži označava se kao *inside*, a sučelje prema ISP-u kao *outside*, čime se definira smjer prevođenja adresa. Ključna je naredba `ip nat inside source list 1 interface Serial6/1 overload` koja propisuje da se izvorišne adrese prometa koji zadovoljava pristupnu listu 1 prevode u adresu WAN sučelja (89.5.8.1), pri čemu parametar `overload` omogućuje da više uređaja istovremeno dijeli istu javnu adresu razlikujući se po brojevima portova. Pristupna lista `access-list 1 permit 172.19.1.0 0.0.0.255` određuje koje izvorišne adrese podliježu prevođenju. Default ruta `ip route 0.0.0.0 0.0.0.0 89.5.8.2` usmjerava sav promet bez specifičnije rute prema ISP usmjerniku.

Tablica 3.1 Raspodjela javnih adresa po podružnicama

Podružnica	Inside (LAN)	Outside (WAN)	Javna IP	Next-hop (ISP)

Ljubuški	Fa0/0	Se6/1	89.5.8.1	89.5.8.2
Grude	Fa0/0	Se6/2	89.5.8.5	89.5.8.6
Čapljina	Fa0/0	Se6/3	89.5.8.9	89.5.8.10

Rad NAT-a provjerava se naredbom `ping 8.8.8.8 source 172.19.1.254` na CE usmjerniku, koja prisilno koristi privatnu LAN adresu kao izvorište i time aktivira prevođenje, te naredbom `ping 8.8.8.8` s korisničkog računala koja provjerava cijeli lanac od računala preko gatewaya i NAT-a do ISP-a. Naredba `show ip nat translations` prikazuje aktivne translacije u obliku para izvorišna adresa i port naspram prevedene adrese i porta, a `show ip nat statistics` ukupne pokazatelje rada.



Slika 3.3 NAT/PAT prijevod na CE-LJ

3.3. MPLS L3 VPN

Primarna komunikacija među podružnicama ostvarena je tehnologijom MPLS L3 VPN (engl. Multiprotocol Label Switching Layer 3 Virtual Private Network). Ovo rješenje omogućuje da sve tri podružnice međusobno komuniciraju preko provider mreže koristeći privatne adrese, a da pritom provider usmjernik (P) uopće ne poznaje adresni prostor klijenta. MPLS L3 VPN gradi se u četiri sloja, pri čemu svaki sloj ovisi o prethodnome.

3.3.1. OSPF na jezgri (underlay)

Prvi sloj čini protokol OSPF (engl. Open Shortest Path First) koji omogućuje međusobnu dostupnost svih usmjernika jezgre putem njihovih Loopback adresa. Ovo je temelj bez kojeg ne mogu raditi ni razmjena MPLS oznaka ni BGP sesije.

```
router ospf 1
 router-id 10.5.8.9
 network 10.5.8.9 0.0.0.0 area 0
 network 10.58.1.0 0.0.0.3 area 0
 network 10.58.2.0 0.0.0.3 area 0
 network 10.58.3.0 0.0.0.3 area 0
```

Koristi se jedinstvena zona (area 0) jer je topologija jednostavna. Radi se je o zvijezdi s P usmjernikom u središtu. Oglašavaju se isključivo linkovi jezgre i Loopback adrese, dok se PE-CE linkovi izostavljaju jer pripadaju virtualnoj routing tablici klijenta (VRF). Identifikator usmjernika (`router-id`) eksplicitno se postavlja na Loopback adresu radi stabilnosti i lakšeg popravka kvarova.

3.3.2. MPLS i LDP

Drugi sloj uključuje označavanje paketa (engl. label switching) te protokol LDP (engl. Label Distribution Protocol) za razmjenu oznaka među usmjernicima. Na svakom sučelju jezgre dodaje se naredba `mpls ip`, a identifikator LDP-a vezuje se uz Loopback sučelje:

```
interface GigabitEthernet2/0
 mpls ip
!
mpls ldp router-id Loopback0 force
```

Uključivanjem MPLS-a usmjernici jezgre prosljeđuju pakete na temelju oznake umjesto pregledom cjelokupnog IP zaglavlja, što ubrzava prosljeđivanje i, što je još važnije, omogućuje izolaciju VPN prometa — P usmjernik ne mora poznavati privatne adrese klijenata. Parametar `force` nalaže da LDP odmah koristi adresu Loopback sučelja, koje je stabilno jer nikada ne ispada.

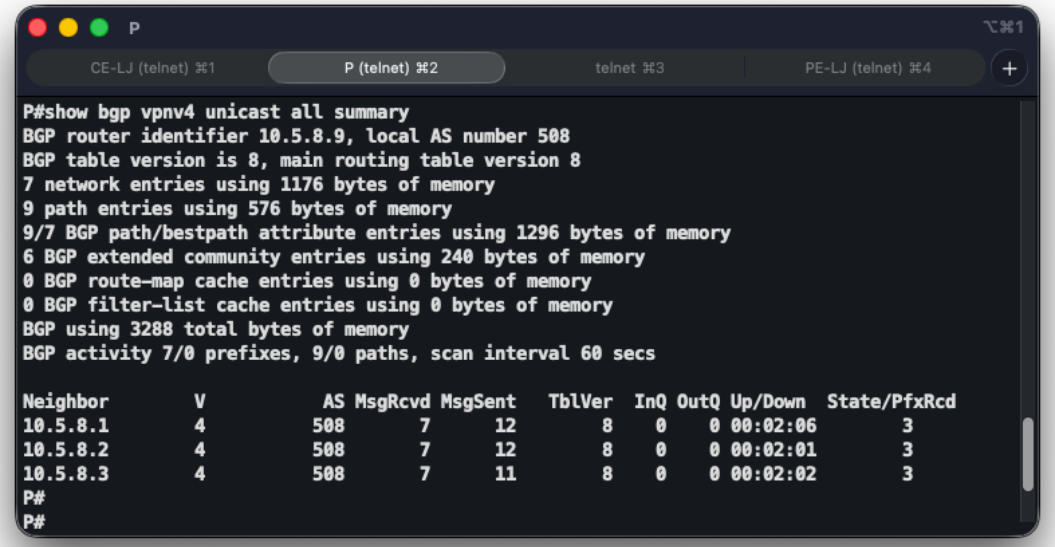
3.3.3. MP-BGP s VPNv4 address-family

Treći sloj čini MP-BGP (engl. Multiprotocol Border Gateway Protocol) s VPNv4 address-family koji prenosi VPN rute među PE usmjernicima. P usmjernik ima ulogu route-

reflectora, čime se izbjegava potreba za potpuno povezanim (engl. full-mesh) skupom BGP sesija. Konfiguracija na P usmjerniku i na karakterističnom PE usmjerniku glasi:

```
router bgp 508
 no bgp default ipv4-unicast
 neighbor 10.5.8.1 remote-as 508
 neighbor 10.5.8.1 update-source Loopback0
 address-family vpnv4
  neighbor 10.5.8.1 activate
  neighbor 10.5.8.1 route-reflector-client
!
router bgp 508
 no bgp default ipv4-unicast
 neighbor 10.5.8.9 remote-as 508
 neighbor 10.5.8.9 update-source Loopback0
 address-family vpnv4
  neighbor 10.5.8.9 activate
  neighbor 10.5.8.9 send-community both
 address-family ipv4 vrf ASI-VPN
  redistribute eigrp 197
```

Naredbom `no bgp default ipv4-unicast` isključuje se obični IPv4 BGP jer se koristi isključivo VPNv4 address-family. Sesije se uspostavljaju preko Loopback adresa (`update-source Loopback0`) koje su dostupne iz svih smjerova zahvaljujući OSPF-u. Postavljanje P usmjernika kao route-reflectora (`route-reflector-client`) smanjuje broj potrebnih sesija s šest na tri. Naredba `send-community both` osigurava prijenos proširenih atributa zajednice koji nose Route Target, a `redistribute eigrp 197` ubacuje rute naučene od CE usmjernika u BGP kako bi ih ostali PE usmjernici mogli naučiti. Korišteni autonomni sustav 508 izveden je iz datuma rođenja autora.



Slika 3.4 MP-BGP VPNv4 susjedstva na P

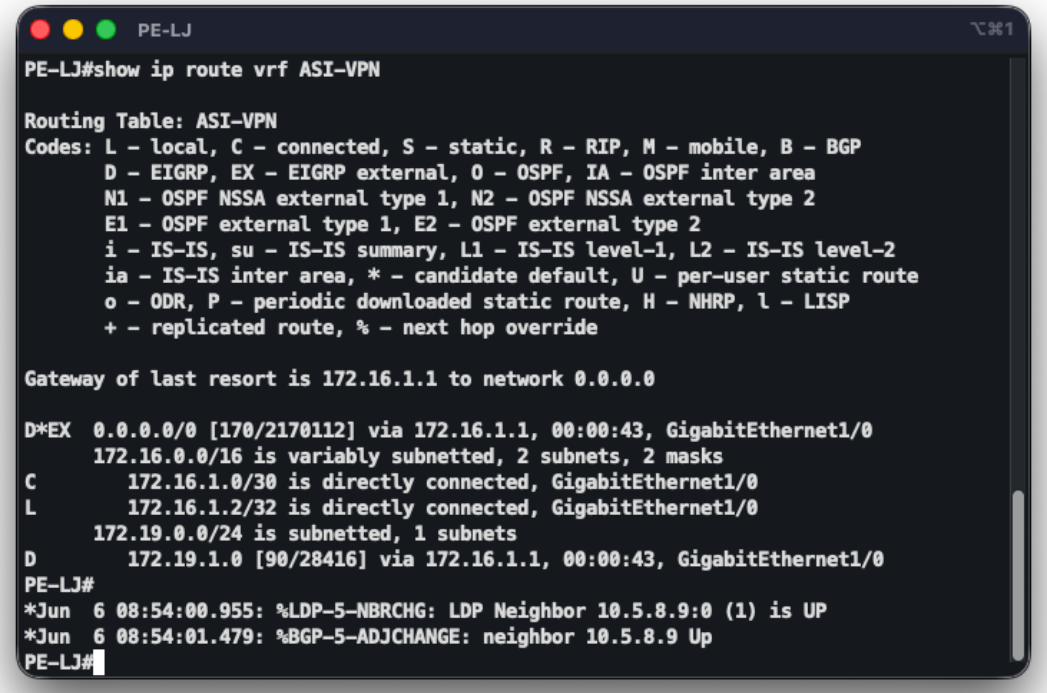
3.3.4. VRF i EIGRP na PE-CE segment

Četvrti sloj uvodi virtualnu routing tablicu (VRF, engl. Virtual Routing and Forwarding) na PE usmjernicima te protokol EIGRP (engl. Enhanced Interior Gateway Routing Protocol) kao protokol usmjeravanja između PE i CE usmjernika:

```
ip vrf ASI-VPN
 rd 508:1
 route-target export 508:1
 route-target import 508:1
!
interface GigabitEthernet1/0
 ip vrf forwarding ASI-VPN
 ip address 172.16.1.2 255.255.255.252
!
router eigrp 197
 address-family ipv4 vrf ASI-VPN
  network 172.16.1.0 0.0.0.3
  redistribute bgp 508 metric 1500 100 255 1 1500
  autonomous-system 197
  no auto-summary
!
```

```
router eigrp 197
 network 172.19.1.0 0.0.0.255
 network 172.16.1.0 0.0.0.3
 no auto-summary
```

VRF stvara zasebnu routing tablicu za klijenta ASI, čime se rute klijenta ne miješaju s rutama providera ni drugih klijenata. Route Distinguisher (`rd 508:1`) čini rute globalno jedinstvenima, dok Route Target (`route-target export/import 508:1`) određuje koje rute VRF izvozi u BGP i uvozi iz njega; budući da svi PE usmjernici koriste isti Route Target, sve podružnice međusobno razmjenjuju rute. Važno je napomenuti da naredba `ip vrf forwarding` briše prethodno postavljenu IP adresu sa sučelja pa ju je nužno ponovno konfigurirati. Naredba `redistribute bgp 508` s eksplicitno zadanom metrikom prenosi rute drugih podružnica iz BGP-a u EIGRP kako bi ih CE usmjernik mogao naučiti, jer BGP ne posjeduje EIGRP metriku. Korišteni EIGRP autonomni sustav 197 također je izveden iz datuma rođenja autora.

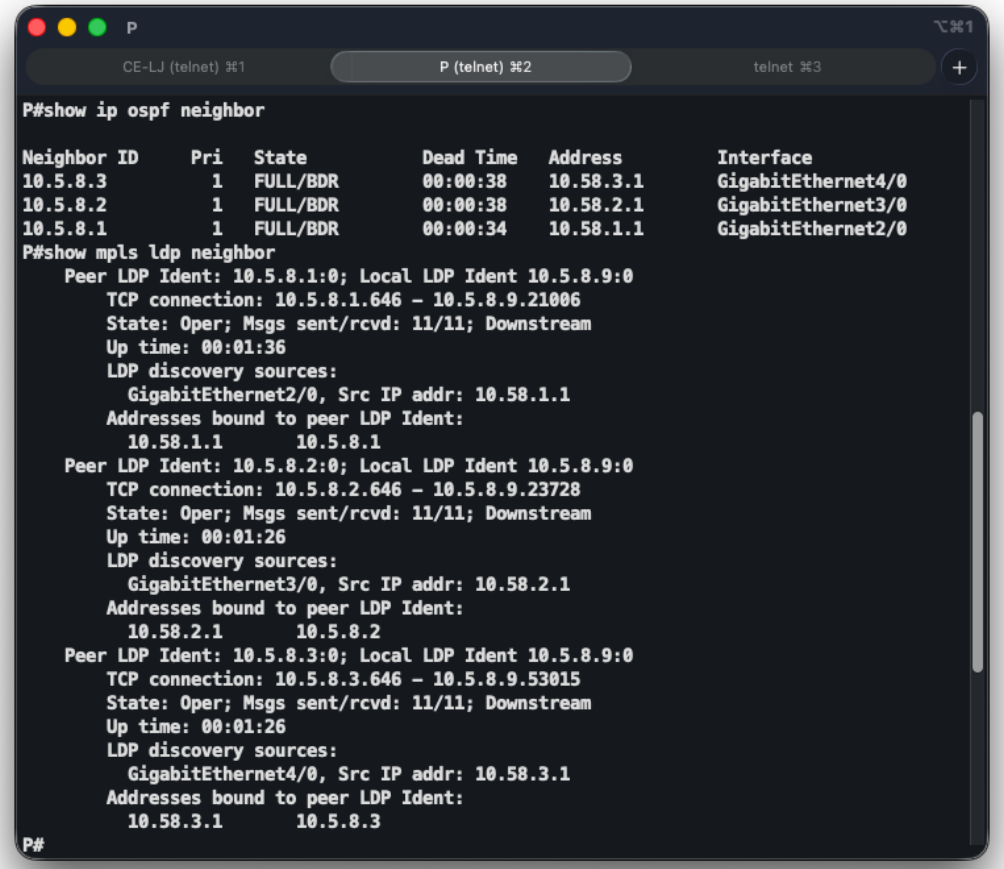


Slika 3.5 VRF tablica ASI-VPN (B i D rute)

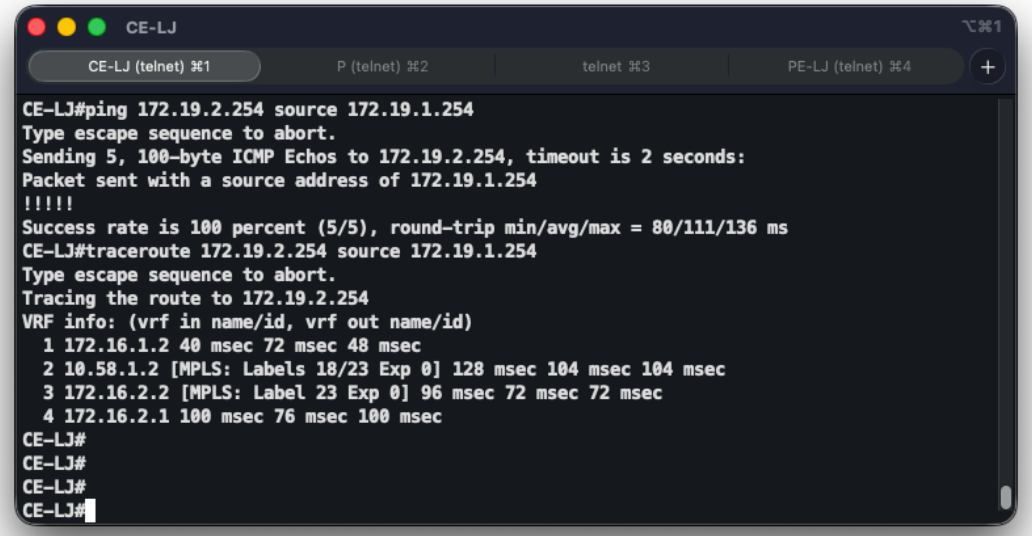
3.3.5. Tijek paketa i provjera

Pri komunikaciji iz Ljubuškog prema Grudama paket s računala podružnice najprije dolazi do CE-LJ usmjernika koji ga, prema EIGRP ruti, prosljeđuje na PE-LJ. PE-LJ na temelju VRF tablice i BGP-a utvrđuje da odredište leži iza PE-GR usmjernika te paketu dodaje dvije MPLS oznake. Vanjsku oznaku za prijenos do PE-GR i unutarnju za identifikaciju VPN-a. P usmjernik pregledava samo vanjsku oznaku, zamjenjuje je i prosljeđuje paket. PE-GR potom uklanja oznake, na temelju VRF tablice i EIGRP-a prosljeđuje paket do CE-GR te konačno do odredišnog računala.

Ispravnost rada MPLS L3 VPN-a provjerava se nizom naredbi: `show ip ospf neighbor` na P usmjerniku mora prikazati tri susjeda u stanju FULL; `show mpls ldp neighbor` tri LDP susjeda u stanju Oper; `show bgp vpnv4 unicast all summary` tri BGP susjeda s primljenim prefiksima; a `show ip route vrf ASI-VPN` na PE usmjerniku rute označene kao B (BGP) i D (EIGRP) za sve podružnice. Krajnja provjera povezanosti izvodi se naredbom `ping 172.19.2.254 source 172.19.1.254`, dok naredba `traceroute` prikazuje put kroz MPLS jezgru s pripadajućim oznakama.



Slika 3.6 OSPF i LDP susjedstva na P



Slika 3.7 End-to-end provjera kroz MPLS L3 VPN (CE-LJ – CE-GR)

3.4. GRE tuneli zaštićeni IPSec enkripcijom

Kao rezervni komunikacijski put, za slučaj ispada MPLS-a, konfigurirani su GRE (engl. Generic Routing Encapsulation) tuneli preko interneta između svake podružnice i oba usmjernika podatkovnog centra, zaštićeni IPSec enkripcijom. Svaka podružnica raspolaže dvama tunelima: jednim prema DC1 kao primarnom čvorištu i jednim prema DC2 kao rezervnom čvorištu.

Tablica 3.2 GRE tuneli

Tunel	Izvor	Odredište	Podmreža
Tunnel10	CE-LJ (89.5.8.1)	DC1 (89.5.8.13)	10.10.10.0/30
Tunnel20	CE-GR (89.5.8.5)	DC1 (89.5.8.13)	10.10.20.0/30
Tunnel30	CE-CA (89.5.8.9)	DC1 (89.5.8.13)	10.10.30.0/30
Tunnel40	CE-LJ (89.5.8.1)	DC2 (89.5.8.17)	10.10.40.0/30
Tunnel50	CE-GR (89.5.8.5)	DC2 (89.5.8.17)	10.10.50.0/30
Tunnel60	CE-CA (89.5.8.9)	DC2 (89.5.8.17)	10.10.60.0/30

Konfiguracija GRE tunela na primjeru veze CE-LJ prema DC1 glasi:

```
interface Tunnel10
 description GRE to DC1
 ip address 10.10.10.2 255.255.255.252
 tunnel source Serial6/1
 tunnel destination 89.5.8.13
 tunnel protection ipsec profile ASI-IPSEC
```

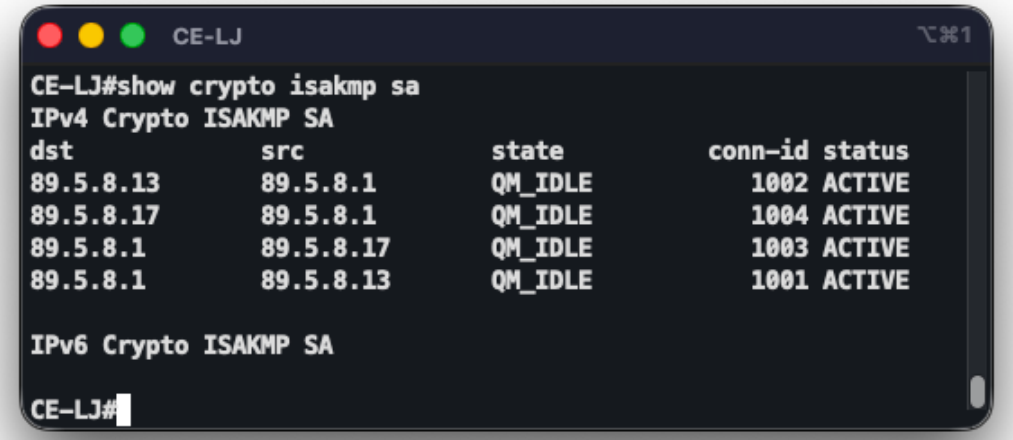
GRE enkapsulira promet u novi IP paket i tako stvara virtualni tunel kroz internet, no sam po sebi ne pruža zaštitu sadržaja. Izvorište tunela vezano je uz WAN sučelje (javnu adresu), a odredište je javna adresa DC1 usmjernika — ISP vidi samo vanjsko IP zaglavlje, ne i sadržaj tunela. Naredba `tunnel protection ipsec profile ASI-IPSEC` automatski šifrira sav

promet koji prolazi tunelom prema definiranom IPSec profilu. Konfiguracija IPSeca u dvije faze:

```
crypto isakmp policy 10
 encryption aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400
!
crypto isakmp key ASI-VPN-KEY address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ASI-TS esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile ASI-IPSEC
 set transform-set ASI-TS
```

ISAKMP politika (Faza 1) određuje način međusobne autentikacije usmjernika i dogovora ključeva: koristi se AES enkripcija s 256-bitnim ključem, SHA-256 za provjeru integriteta, autentikacija unaprijed dijeljenim ključem (engl. pre-shared key) te Diffie-Hellman grupa 14 (2048-bitna) za sigurnu razmjenu ključeva, uz obnavljanje svaka 24 sata. Transform-set (Faza 2) određuje zaštitu stvarnog korisničkog prometa primjenom ESP-a s AES-256 enkripcijom i SHA-256 provjerom integriteta. Koristi se transportni način rada (engl. transport mode) jer je u kombinaciji s GRE-om učinkovitiji od tunelskog načina, budući da GRE već dodaje vlastito zaglavlje. IPSec profil povezuje transform-set sa sučeljem tunela; ovaj pristup pomoću `tunnel protection` moderniji je i pregledniji od klasičnih crypto mapa.

Ispravnost tunela provjerava se naredbom `show crypto isakmp sa`, pri čemu stanje QM_IDLE označava uspješno uspostavljenu sesiju Faze 1, te `show crypto ipsec sa` čiji brojači šifriranih i dešifriranih paketa potvrđuju da se promet stvarno enkriptira. Naredba `show interfaces tunnel 10` prikazuje status tunela, a `ping 10.10.10.1 source 10.10.10.2` potvrđuje prohodnost GRE veze.



Slika 3.8 ISAKMP/IPSec asocijacije na GRE tunelima

3.5. Access liste na internetskim sučeljima

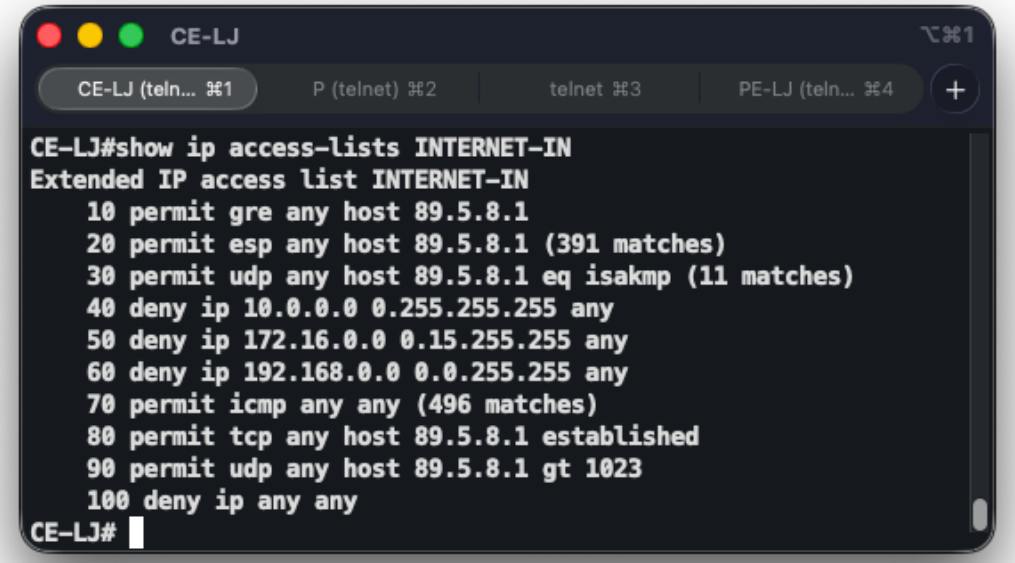
Kako bi se mreža zaštitila od neovlaštenog pristupa s interneta, na svakom usmjerniku s internetskim sučeljem konfigurirana je proširena pristupna lista (engl. extended access list) pod nazivom INTERNET-IN, primijenjena na ulazni promet. Pristupna lista propušta legitiman promet — protokole VPN-a, ICMP poruke i povratni promet — dok blokira sve ostalo. Konfiguracija access lista na CE-LJ:

```
ip access-list extended INTERNET-IN
 permit gre any host 89.5.8.1
 permit esp any host 89.5.8.1
 permit udp any host 89.5.8.1 eq 500
deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
permit icmp any any
permit tcp any host 89.5.8.1 established
 permit udp any host 89.5.8.1 gt 1023
deny ip any any
!
interface Serial6/1
 ip access-group INTERNET-IN in
```

Prva skupina pravila propušta protokole nužne za rad VPN tunela: GRE (protokol 47), ESP (protokol 50) koji nosi šifrirani sadržaj te ISAKMP na UDP portu 500 za razmjenu ključeva. Slijede pravila za zaštitu od lažiranja adresa (engl. anti-spoofing) koja odbacuju pakete pristigle s interneta s privatnim izvorišnim adresama prema RFC 1918, jer takve adrese ne mogu legitimno postojati na javnom internetu. Pravilo `permit icmp any any` dopušta dijagnostički promet. Dva pravila za povratni promet: `permit tcp ... established`, koje propušta samo pakete već uspostavljenih TCP veza, te `permit udp ... gt 1023`, koje propušta UDP odgovore na visokim portovima koje koristi PAT. Ta dva pravila se nalaze samo na podružnicama jer usmjernici datacentra ne obavljaju NAT. Eksplicitno pravilo `deny ip any any` na kraju iako se podrazumijeva dodano je radi preglednosti i lakšeg praćenja broja hitova po pravilu.

Na usmjernicima podatkovnog centra primijenjena je ista lista bez pravila za NAT povratni promet, prilagođenih javnih adresa (89.5.8.13 za DC1, 89.5.8.17 za DC2).

Ispravnost pristupnih lista provjerava se naredbom `show ip access-lists INTERNET-IN` koja uz svako pravilo prikazuje broj pogodaka, što potvrđuje da promet zaista prolazi kroz očekivana pravila. Provjerava se i da nakon primjene liste i dalje rade pristup internetu (`ping 8.8.8.8 source <LAN-IP>`) te komunikacija kroz MPLS i GRE tunele.



Slika 3.9 ACL Internet-IN na CE-LJ

4. Mehanizmi redundancije i failovera

Osim povezanosti, ključni zahtjev projekta je i otpornost mreže na ispade. Ovo poglavlje opisuje tri mehanizma redundancije koji zajedno osiguravaju neprekidan rad mreže i u uvjetima otkaza pojedinih linkova ili cijelih segmenata: automatski failover primarne komunikacije među podružnicama s MPLS-a na GRE+IPSec tunele, redundanciju pristupa internetu u podatkovnom centru putem HSRP-a i IP SLA praćenja te višerazinski failover internetskog pristupa podružnica.

4.1. Failover među podružnicama (MPLS – GRE+IPSec)

Primarni put komunikacije među podružnicama je MPLS L3 VPN, no za slučaj njegova ispada implementiran je automatski prijelaz na GRE+IPSec tunele opisane u poglavlju 3.4. Mehanizam se temelji na plutajućim statičkim rutama (engl. floating static routes) kojima je namjerno povišena administrativna udaljenost (engl. administrative distance, AD) tako da stupaju na snagu tek kad nestane bolji put.

Konfiguracija na usmjerniku CE-LJ glasi:

```
ip route 172.19.2.0 255.255.255.0 10.10.10.1 200
ip route 172.19.3.0 255.255.255.0 10.10.10.1 200
ip route 10.97.100.0 255.255.255.0 10.10.10.1 200
ip route 172.19.2.0 255.255.255.0 10.10.40.1 210
ip route 172.19.3.0 255.255.255.0 10.10.40.1 210
ip route 10.97.100.0 255.255.255.0 10.10.40.1 210
```

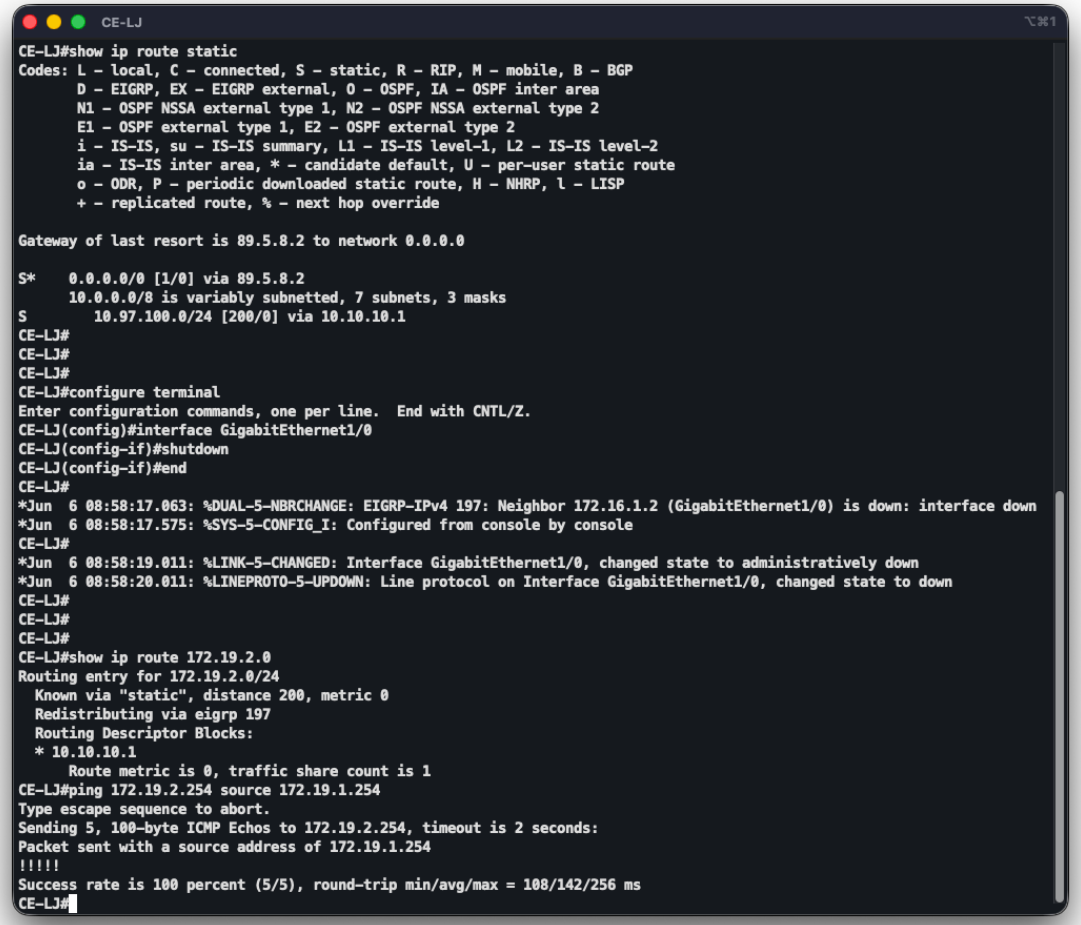
Uobičajena statička ruta ima administrativnu udaljenost 1, ali ovdje su rutama dane vrijednosti 200 (preko tunela prema DC1) i 210 (preko tunela prema DC2). Budući da EIGRP preko MPLS-a ima administrativnu udaljenost 90, on uvijek ima prednost dok je dostupan. Tek kad MPLS ispadne i EIGRP izgubi susjeda, ruta s udaljenosti 90 nestaje iz tablice usmjeravanja te na njezino mjesto dolazi plutajuća ruta s udaljenošću 200. Promet počinje teći kroz GRE tunel prema DC1. Ako ni taj put nije dostupan, aktivira se ruta s udaljenošću 210 preko DC2. Rute su definirane za sve mreže do kojih se normalno dolazi preko MPLS-a, tj ostale dvije podružnice i LAN podatkovnog centra.

Time je uspostavljen strogo definiran redoslijed failovera:

a. Prioritet 1: MPLS (EIGRP, AD 90) — PE link aktivan, EIGRP susjed uspostavljen.
b. Prioritet 2: GRE preko DC1 (AD 200) — MPLS pao, tunel prema DC1 aktivan.
c. Prioritet 3: GRE preko DC2 (AD 210) — MPLS i DC1 pali, tunel prema DC2 aktivan.

Na usmjernicima podatkovnog centra, koji ne sudjeluju u MPLS-u, konfigurirane su obične statičke rute prema podružnicama kroz pripadajuće tunele.

Ispravnost mehanizma potvrđena je testiranjem 12. travnja 2026. U normalnom stanju naredba `show ip route 172.19.2.0` prikazuje EIGRP rutu s udaljenošću 90 preko PE-LJ, a `traceroute` otkriva MPLS oznake na putu kroz P usmjernik. Nakon gašenja sučelja prema MPLS jezgri (`shutdown` na GigabitEthernet1/0) EIGRP susjed se gubi i ruta prelazi na plutajuću statičku rutu s udaljenošću 200 kroz GRE tunel, pri čemu ping kroz tunel uspijeva u svih pet pokušaja. Ponovnim podizanjem sučelja (`no sh`) EIGRP se obnavlja i ruta se vraća na primarni put.



Slika 4.1 Failover MPLS - GRE+IPSec

4.2. Redudancija internet pristupa u podatkovnom centru (HSRP + IP SLA)

Podatkovni centar ima dva usmjernika (DC1 i DC2) od kojih svaki ima vlastiti internet link. Kako bi uređaji na DC LAN-u (10.97.100.0/24) imali otporan pristup internetu, na oba usmjernika konfiguriran je protokol HSRP (engl. Hot Standby Router Protocol) s jednom virtualnom IP adresom (VIP) 10.97.100.254 koju uređaji koriste kao default gateway. DC1 je primarni (aktivni) gateway, dok DC2 automatski preuzima ulogu ako DC1 izgubi internet link. Stanje internet linka prati se mehanizmom IP SLA (engl. Service Level Agreement). Konfiguracija IP SLA na DC1:

```
interface GigabitEthernet1/0
 ip nat inside
interface FastEthernet0/0
```

```
 ip nat outside
ip nat inside source list 10 interface FastEthernet0/0
overload
access-list 10 permit 10.97.100.0 0.0.0.255
!
ip sla 1
 icmp-echo 89.5.8.14
 frequency 5
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 reachability
!
interface GigabitEthernet1/0
 standby 1 ip 10.97.100.254
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 20
```

Na rezervnom usmjerniku DC2 konfiguracija je ista, sa nižim početnim prioritetom (100) i IP SLA praćenjem svojeg ISP linka:

```
interface GigabitEthernet1/0
 ip nat inside
interface FastEthernet5/0
 ip nat outside
ip nat inside source list 10 interface FastEthernet5/0
overload
access-list 10 permit 10.97.100.0 0.0.0.255
ip sla 2
 icmp-echo 89.5.8.18
 frequency 5
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 reachability
interface GigabitEthernet1/0
 standby 1 ip 10.97.100.254
 standby 1 priority 100
 standby 1 preempt
 standby 1 track 2 decrement 20
```

Virtualna IP adresa (`standby 1 ip 10.97.100.254`) zajednička je objema usmjernicima i predstavlja stabilan default gateway. Pri promjeni aktivnog usmjernika adresa se ne mijenja pa uređaji na LAN-u ne moraju ništa rekonfigurirati. DC1 ima viši prioritet (110) od DC2 (100) pa je u normalnim uvjetima aktivan. Naredba `preempt` osigurava da se usmjernik s

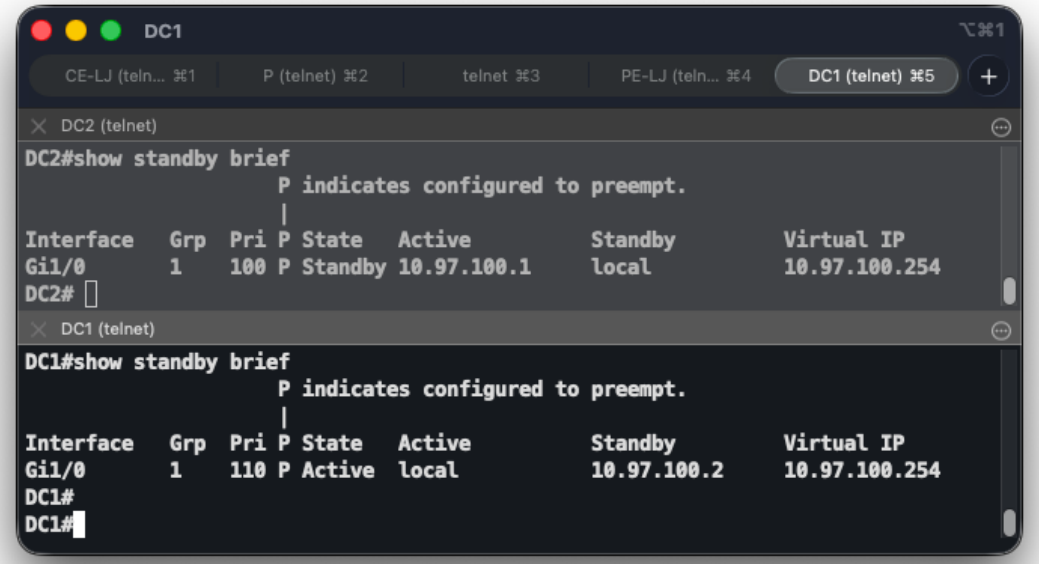
višim prioritetom nakon oporavka automatski vrati u aktivnu ulogu. Ključ mehanizma je naredba `standby 1 track 1 decrement 20`: ako objekt praćenja (track 1) padne jer ISP link postane nedostupan, prioritet DC1 smanjuje se za 20 (sa 110 na 90), čime postaje niži od DC2 (100) i DC2 preuzima ulogu aktivnog usmjernika.

IP SLA aktivno provjerava dostupnost ISP susjeda slanjem ICMP upita svakih pet sekundi. Ovaj pristup pouzdaniji je od praćenja stanja sučelja jer sučelje može ostati fizički podignuto i kad je ISP nedostupan. Objekt `track 1 ip sla 1 reachability` poprima stanje "Up" dok upiti dobivaju odgovor, odnosno "Down" kad odgovora nema a HSRP nadzire upravo to stanje. NAT u izvedbi PAT konfiguriran je na oba usmjernika kako bi promet s DC LAN-a mogao izaći na internet.

Scenarij rada je: u normalnom stanju DC1 je aktivan i sav promet ide preko njega; kad ISP link DC1 ispadne, IP SLA bilježi istek vremena, objekt praćenja pada, prioritet DC1 spušta se na 90 i DC2 (100) preuzima ulogu aktivnog usmjernika; nakon oporavka ISP linka DC1 vraća prioritet na 110 i zahvaljujući naredbi `preempt` ponovno postaje aktivan.

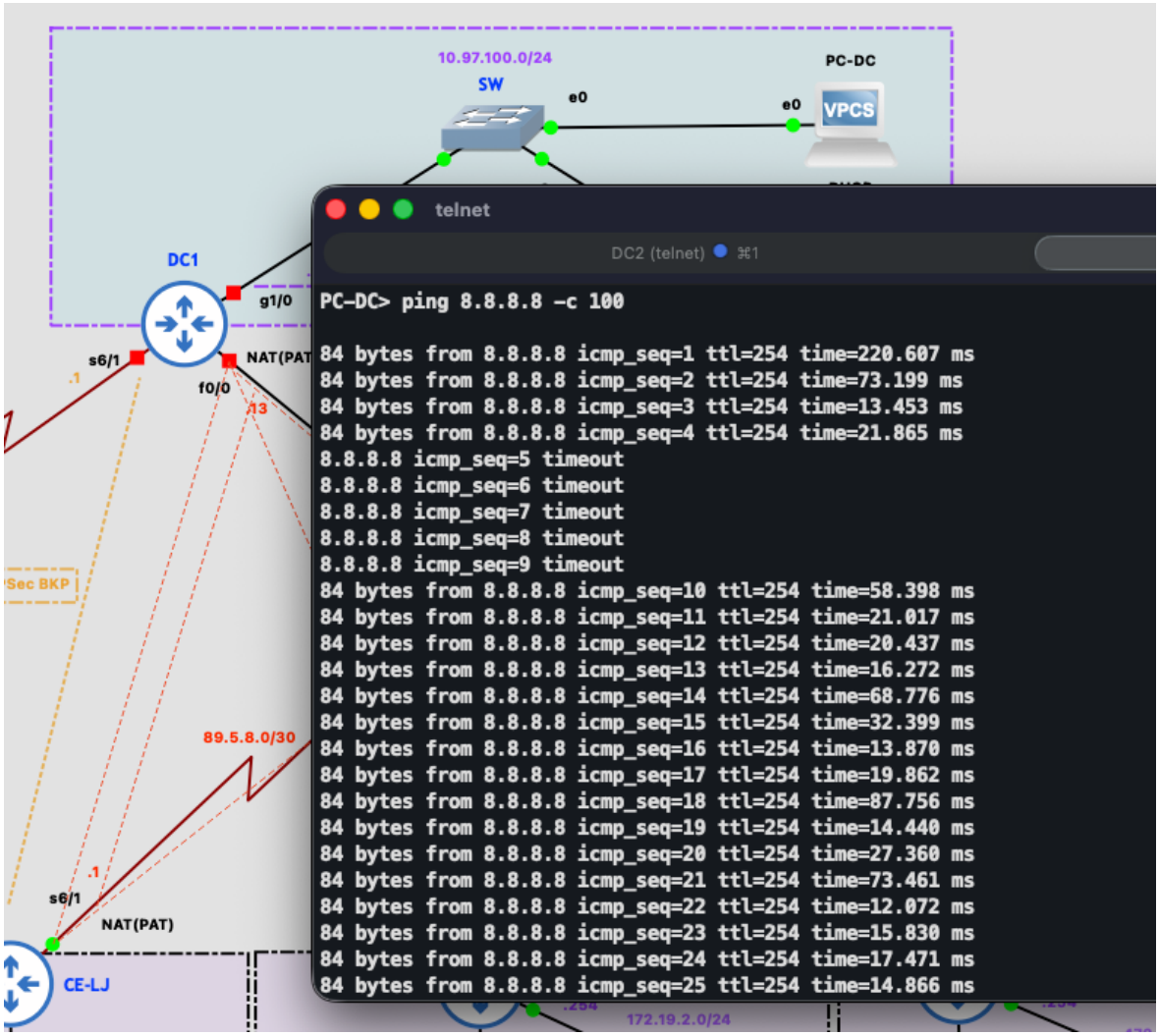
Poseban slučaj jest istovremeni pad oba internetska linka. Tada i DC2 zbog vlastitog praćenja spušta prioritet (sa 100 na 80), dok je DC1 na 90 pa DC1 ponovno postaje aktivan i zadržava virtualnu adresu. To je namjerno, jedino DC1 ima rezervnu vezu (backup link, poglavlje 4.4) prema podružnicama pa virtualna adresa mora ostati na njemu kako bi promet s DC LAN-a prema podružnicama imao povratni put. Da DC2 nema vlastiti decrement, virtualna bi adresa pri padu samo DC1-ovog linka ispravno prešla na DC2, ali bi pri padu *oba* linka ostala na DC2 koji nema rezervni put i povratni promet prema podružnicama bi se gubio. Vrijednosti decrementa odabrane su tako da u svim kombinacijama prevlada ispravan usmjernik: oba linka rade = DC1 (110); pao samo DC1 = DC2 (100 naspram 90); pao samo DC2 = DC1 (110 naspram 80); pala oba = DC1 (90 naspram 80).

Testiranjem je potvrđeno da uređaj na DC LAN-u pristupa internetu preko virtualne adrese s uspjehom. Nakon gašenja internetskog sučelja DC1, IP SLA bilježi istek vremena, objekt praćenja pada, prioritet se spušta na 90 i DC2 preuzima aktivnu ulogu pri čemu internetski pristup ostaje neprekinut. Ponovnim podizanjem sučelja DC1 se zbog mehanizma preempt vraća u aktivnu ulogu. Stanje se prati naredbama `show standby brief`, `show track 1` i `show ip sla summary`.



Slika 4.2 HSRP uloge: DC1 aktivan, DC2 u pripravnosti

Osim ispada samog ISP linka, zasebno je testiran i otkaz cijelog DC1 uređaja, budući da zadatak zahtijeva failover u oba slučaja. Riječ je o dva različita mehanizma detekcije: pad ISP linka otkriva IP SLA praćenje (DC1 ostaje aktivan u HSRP grupi, ali sa smanjenim prioritetom), dok potpuni otkaz uređaja otkriva sam HSRP izostankom hello poruka, nakon čega DC2 po isteku hold vremena (10 sekundi uz zadane HSRP timere) preuzima aktivnu ulogu i virtualnu adresu. Test je proveden potpunim gašenjem DC1 virtualnog stroja u GNS3 uz kontinuirani ping s računala na DC LAN-u prema 8.8.8.8: tijekom HSRP konvergencije izgubljeno je pet paketa, nakon čega je promet nastavio teći kroz DC2 bez ikakve ručne intervencije. Naredba `show standby brief` na DC2 prikazuje stanje Active uz nepoznat (unknown) standby uređaj, čime je potvrđeno da je DC2 jedini preostali gateway. Ponovnim uključivanjem DC1 uređaj se nakon podizanja HSRP procesa zahvaljujući mehanizmu preempt automatski vratio u aktivnu ulogu, a DC2 u pripravnost.



Slika 4.3 Otkaz cijelog DC1 uređaja – HSRP preuzimanje na DC2 uz gubitak pet ICMP paketa

4.3. Failover internet pristupa podružnica

Kad podružnica izgubi izravni ISP link, internet promet se automatski preusmjerava drugim putem. Implementiran je mehanizam s tri razine: izravni ISP link kao primarni put, prolaz kroz MPLS jezgru do unaprijed definirane backup podružnice kao prvi rezervni put te isključivo za CE-LJ prolaz kroz backup link i podatkovni centar kao krajnje rješenje.

Na CE usmjernicima, na primjeru CE-GR, default ruta vezana je uz IP SLA praćenje, a propagacija default rute kroz MPLS ostvarena je redistribucijom u EIGRP:

```
ip sla 1
 icmp-echo 89.5.8.6
 frequency 5
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 reachability
```

```
ip route 0.0.0.0 0.0.0.0 89.5.8.6 track 1

ip prefix-list DEFAULT-ONLY seq 5 permit 0.0.0.0/0
route-map REDISTRIBUTE-DEFAULT permit 10
 match ip address prefix-list DEFAULT-ONLY
router eigrp 197
 redistribute static route-map REDISTRIBUTE-DEFAULT
```

Default ruta prema ISP-u vezana je uz objekt praćenja (`ip route ... track 1`) pa se povlači iz tablice usmjeravanja čim ISP postane nedostupan, čime se izbjegava slanje prometa u "crnu rupu". Redistribucija u EIGRP putem rutne mape i prefiksne liste `DEFAULT-ONLY` osigurava da se u EIGRP ubaci isključivo default ruta, a ne i ostale statičke rute (poput plutajućih ruta za GRE failover). Svaka podružnica tako oglašava svoju default rutu kroz MPLS, a ostale je primaju kao EIGRP external rutu s administrativnom udaljenošću 170. Dok podružnica ima ispravan ISP link, lokalna statička ruta (AD 1) ima prednost; kad ISP padne, ona nestaje i preuzima ju EIGRP default ruta kroz MPLS prema podružnici koja još ima internet.

Da bi promet jedne podružnice mogao izaći na internet kroz NAT druge podružnice, na PE usmjernicima dodana je naredba `default-information originate` a pristupna lista NAT-a na CE usmjernicima proširena je podmrežama ostalih podružnica:

```
router bgp 508
 address-family ipv4 vrf ASI-VPN
  redistribute eigrp 197
  default-information originate
access-list 1 permit 172.19.1.0 0.0.0.255
access-list 1 permit 172.19.2.0 0.0.0.255
access-list 1 permit 172.19.3.0 0.0.0.255
access-list 1 permit 10.97.100.0 0.0.0.255
interface GigabitEthernet1/0
 ip nat inside
```

BGP po zadanim postavkama ne propagira default rutu pa naredba `default-information originate` to eksplicitno omogućuje čime default ruta prolazi kroz MPLS jezgru. Označavanjem PE linka (GigabitEthernet1/0) kao NAT *inside* sučelja omogućuje se prevođenje prometa koji preko MPLS-a stiže od druge podružnice, a extended access lista osigurava da NAT prepoznaje i te podmreže.

Zadatak zahtijeva da backup odnosi budu jednoznačno definirani, tj. za svaku lokaciju mora biti unaprijed određeno preko koje lokacije izlazi na internet kad izgubi vlastiti ISP link. Sama redistribucija default rute to ne jamči: route-reflector među jednakim default rutama svih podružnica bira jednu najbolju prema vlastitim BGP kriterijima (u pravilu najniži router-id) i samo nju reflektira ostalima, pa bi izbor backup lokacije bio posljedica slučajnosti topologije, a ne projektne odluke. Backup odnosi stoga su eksplicitno definirani kružnom shemom:

Tablica 4.1 Backup odnosi internetskog pristupa podružnica

Lokacija	Backup lokacija	Community (vlastiti / backup)
Ljubuški (CE-LJ)	Grude (CE-GR)	508:10 / 508:20
Grude (CE-GR)	Čapljina (CE-CA)	508:20 / 508:30
Čapljina (CE-CA)	Ljubuški (CE-LJ)	508:30 / 508:10

Determinizam je ostvaren u dva koraka. Prvo, svakom PE usmjerniku dodijeljen je jedinstveni Route Distinguisher (PE-LJ 508:1, PE-GR 508:2, PE-CA 508:3) uz nepromijenjen Route Target 508:1 na svim stranama. Time tri default rute postaju tri različita VPNv4 prefiksa pa ih route-reflector sve reflektira umjesto da bira jednu najbolju, čime svaki PE raspolaže potpunim skupom kandidata; riječ je o standardnoj praksi za višestruko povezane VPN lokacije (engl. unique RD per PE). Drugo, svaki PE pri redistribuciji u BGP označava vlastitu default rutu standardnim BGP community atributom koji identificira lokaciju (508:10 Ljubuški, 508:20 Grude, 508:30 Čapljina, dakle redni broj podružnice pomnožen s 10, u skladu s adresnim planom), a ulazna rutna mapa na VPNv4 sesiji podiže BGP local-preference sa zadanih 100 na 200 isključivo default ruti koja nosi community definirane backup lokacije. Izravno uspoređivanje BGP next-hopa u ulaznoj rutnoj mapi nije korišteno jer ga korišteni IOS na ulaznoj BGP strani ne podržava (poruka "nexthop match not supported"), dok je označavanje community atributima podržano i ujedno čitljivije. Budući da se standardni community atributi ne prenose automatski, na route-reflectoru i PE usmjernicima dodana je naredba send-community both. Konfiguracija na PE-LJ (vlastita oznaka 508:10; backup za Ljubuški su Grude pa se preferira community 508:20):

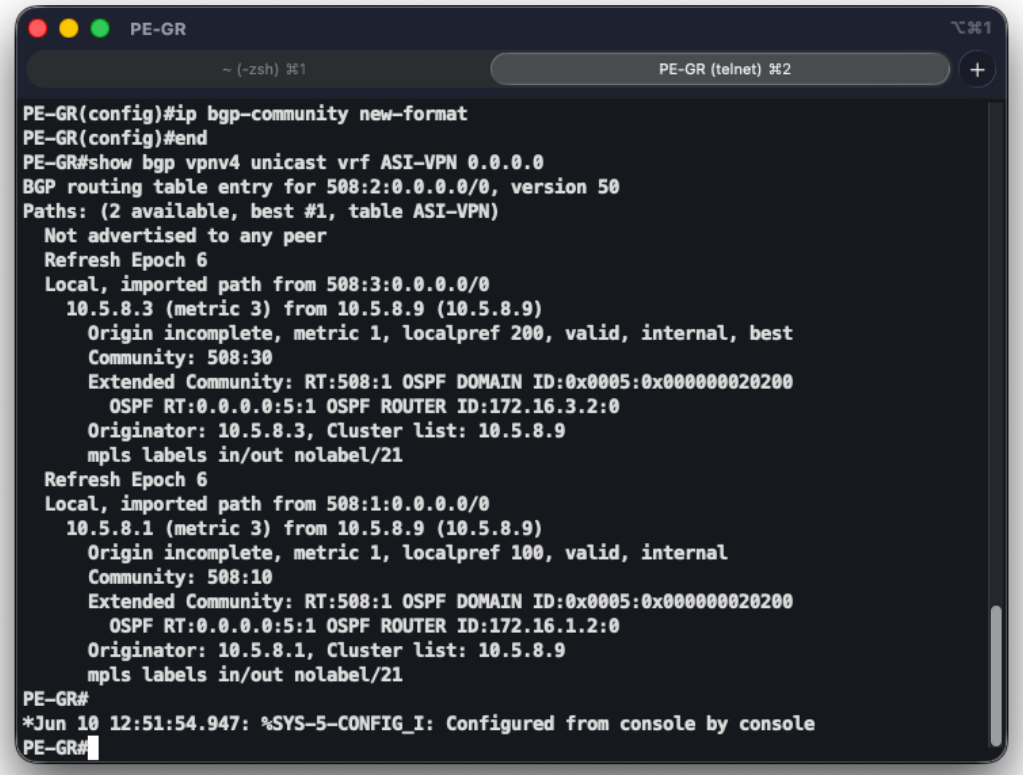
```
ip vrf ASI-VPN
 rd 508:1
!
```

```
ip prefix-list DEFAULT-ONLY seq 5 permit 0.0.0.0/0
!
route-map TAG-DEFAULT permit 10
 match ip address prefix-list DEFAULT-ONLY
 set community 508:10
route-map TAG-DEFAULT permit 20
!
ip community-list standard BACKUP-SITE permit 508:20
!
route-map BACKUP-INTERNET permit 10
 match ip address prefix-list DEFAULT-ONLY
 match community BACKUP-SITE
 set local-preference 200
route-map BACKUP-INTERNET permit 20
!
router bgp 508
 address-family ipv4 vrf ASI-VPN
  redistribute ospf 2 match internal external 1 external 2
route-map TAG-DEFAULT
  default-information originate
 address-family vpnv4
  neighbor 10.5.8.9 send-community both
  neighbor 10.5.8.9 route-map BACKUP-INTERNET in
```

Rutna mapa TAG-DEFAULT pri redistribuciji označava isključivo default rutu (prva stavka), dok sve ostale rute prolaze neoznačene (druga stavka). Ulazna rutna mapa BACKUP-INTERNET podiže local-preference samo presjeku dvaju uvjeta, prefiksu 0.0.0.0/0 s community oznakom backup lokacije, a sve ostale rute propušta nepromijenjene. Bitno je uočiti međudjelovanje s lokalno generiranom default rutom: ona nosi Cisco weight 32768 koji se u BGP izboru vrednuje prije local-preference, pa dok podružnica ima vlastiti ISP link njezin promet izlazi lokalno, bez obilaska. Tek kad CE zbog IP SLA praćenja povuče svoju default rutu, lokalni kandidat nestaje i local-preference 200 deterministički odabire definiranu backup lokaciju. Mehanizam se pritom kontrolirano degradira: izgubi li internet i backup lokacija, preostaje ruta treće lokacije s local-preference 100 pa mreža ostaje funkcionalna. Na PE-GR community lista BACKUP-SITE propušta 508:30 (Čapljina), a na PE-CA 508:10 (Ljubuški), uz odgovarajuću vlastitu oznaku u rutnoj mapi TAG-DEFAULT. Kako cijeli mehanizam djeluje na BGP VPNv4 razini, neovisan je o PE-CE protokolu usmjeravanja pa ostaje nepromijenjen i nakon migracije s EIGRP-a na OSPF (poglavlje 5.1).

Promjena Route Distinguishera prazni VRF tablicu (na korištenom IOS-u zahtijeva brisanje i ponovno kreiranje VRF-a) pa je provedena kao najavljeni zahvat, jedan PE usmjernik u trenutku, uz provjeru konvergencije prije prelaska na sljedeći.

Ispravnost je provjerena naredbom `show bgp vpnv4 unicast vrf ASI-VPN 0.0.0.0`, koja na svakom PE usmjerniku prikazuje sva tri kandidata za default rutu: lokalno generiranu rutu (weight 32768, best u normalnom stanju) te dvije reflektirane rute, od kojih ona s community oznakom backup lokacije nosi local-preference 200. Radi čitljivijeg prikaza community atributa u obliku 508:X umjesto decimalnog broja, na PE usmjernicima uključena je naredba `ip bgp-community new-format`. Gašenjem ISP linka na CE-GR promet podružnice Grude izašao je na internet kroz NAT na CE-CA, što je potvrđeno next-hopom 10.5.8.3 u naredbi `show ip route vrf ASI-VPN 0.0.0.0` na PE-GR te naredbom traceroute prema 8.8.8.8 s korisničkog računala, dakle točno prema definiranom mapiranju, a ne kroz proizvoljnu lokaciju. Dodatnim gašenjem ISP linka i na CE-CA promet je preuzela posljednja preostala lokacija (Ljubuški), čime je potvrđena i kontrolirana degradacija mehanizma.



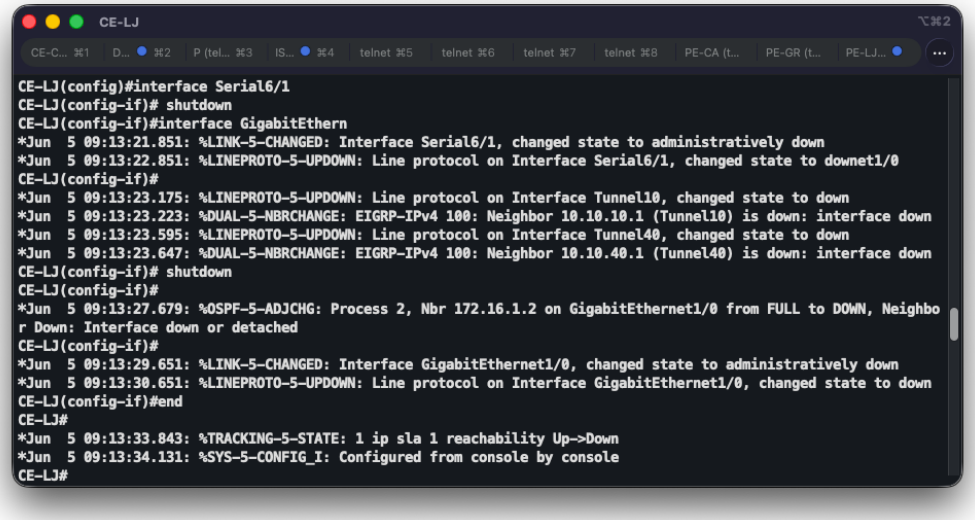
Slika 4.4 Deterministički odabir backup lokacije – BGP kandidati za default rutu na PE-GR

Za krajnji slučaj, kad CE-LJ izgubi i ISP i MPLS, internet promet izlazi kroz backup vezu prema podatkovnom centru. Ta backup veza je S2S GRE+IPSec tunel (`Tunnel100`) između CE-LJ i DC1, koji fizički putuje dediciranim serijskim linkovima kroz BKP usmjernik. Tunel je neovisan o internetu pa ostaje dostupan i kad zakaže ISP pristup na bilo kojoj strani, a BKP prosljeđuje isključivo enkapsulirani (GRE/ESP) promet između krajnjih točaka tunela:

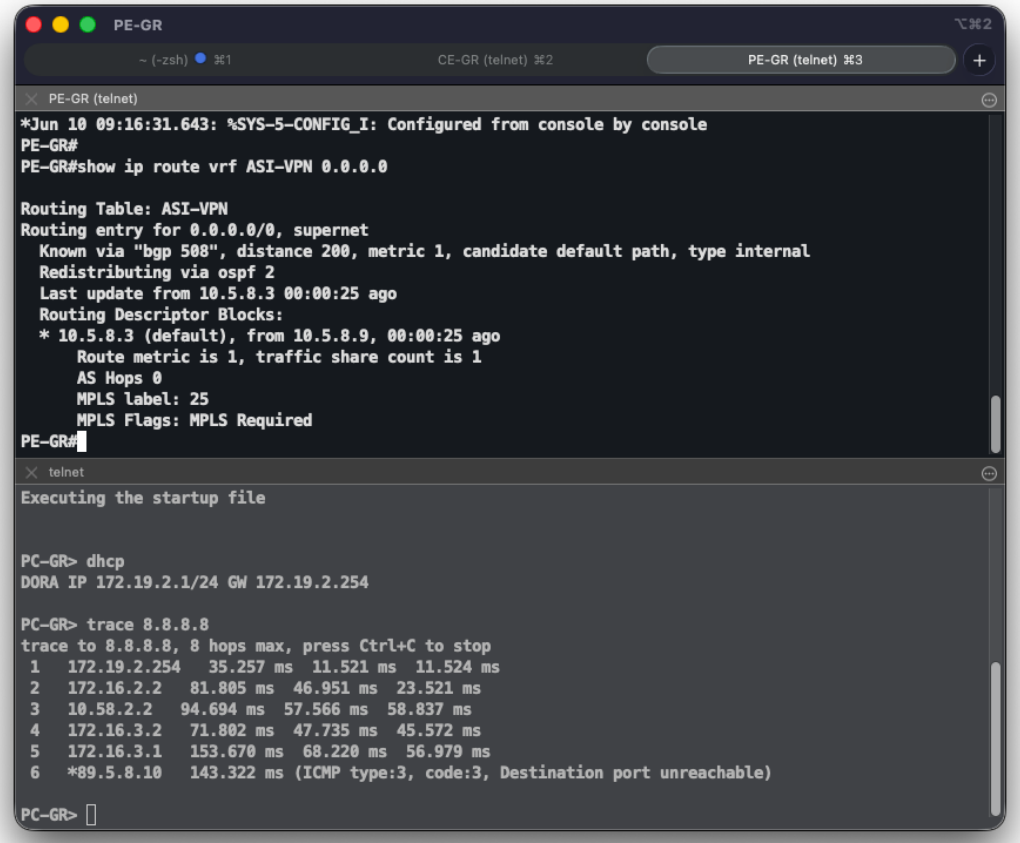
```
crypto ipsec profile ASI-IPSEC-BKP
 set transform-set ASI-TS
interface Tunnel100
 ip address 10.58.100.2 255.255.255.252
 tunnel source Serial6/2
 tunnel destination 10.58.10.1
 tunnel protection ipsec profile ASI-IPSEC-BKP
ip route 10.58.10.0 255.255.255.252 10.58.10.5
ip route 0.0.0.0 0.0.0.0 10.58.100.1 210
interface Tunnel100
 ip address 10.58.100.1 255.255.255.252
 ip nat inside
 tunnel source Serial6/1
 tunnel destination 10.58.10.6
 tunnel protection ipsec profile ASI-IPSEC-BKP
ip route 10.58.10.4 255.255.255.252 10.58.10.2
ip route 172.19.1.0 255.255.255.0 10.58.100.2 215
```

Za backup tunel namjerno je definiran zaseban IPSec profil (`ASI-IPSEC-BKP`): glavni profil `ASI-IPSEC` na DMVPN tunelima koristi `shared` zaštitu vezanu uz sučelje prema internetu, pa se isti profil ne može dijeliti s tunelom koji izlazi kroz drugačiji izvor (serijsko sučelje prema BKP-u). Budući da je tunel točka-na-točku (`tunnel destination`), zaštita ne treba `shared`. Ključna je underlay ruta `ip route 10.58.10.0/30 ... 10.58.10.5`: bez nje bi se odredište tunela (`10.58.10.1`) razrješavalo kroz zadanu rutu koja vodi natrag u sam tunel, čime bi nastala rekurzivna petlja. Na CE-LJ plutajuća default ruta (AD 210) sada usmjerava internet promet u kriptirani tunel umjesto u goli serijski link; promet izlazi na internet tek nakon NAT-a na DC1, koji backup tunel označava kao NAT *inside* sučelje. Ova ruta preuzima promet tek kad nema ni izravnog ISP-a (AD 1) ni EIGRP default rute kroz MPLS (AD 170).

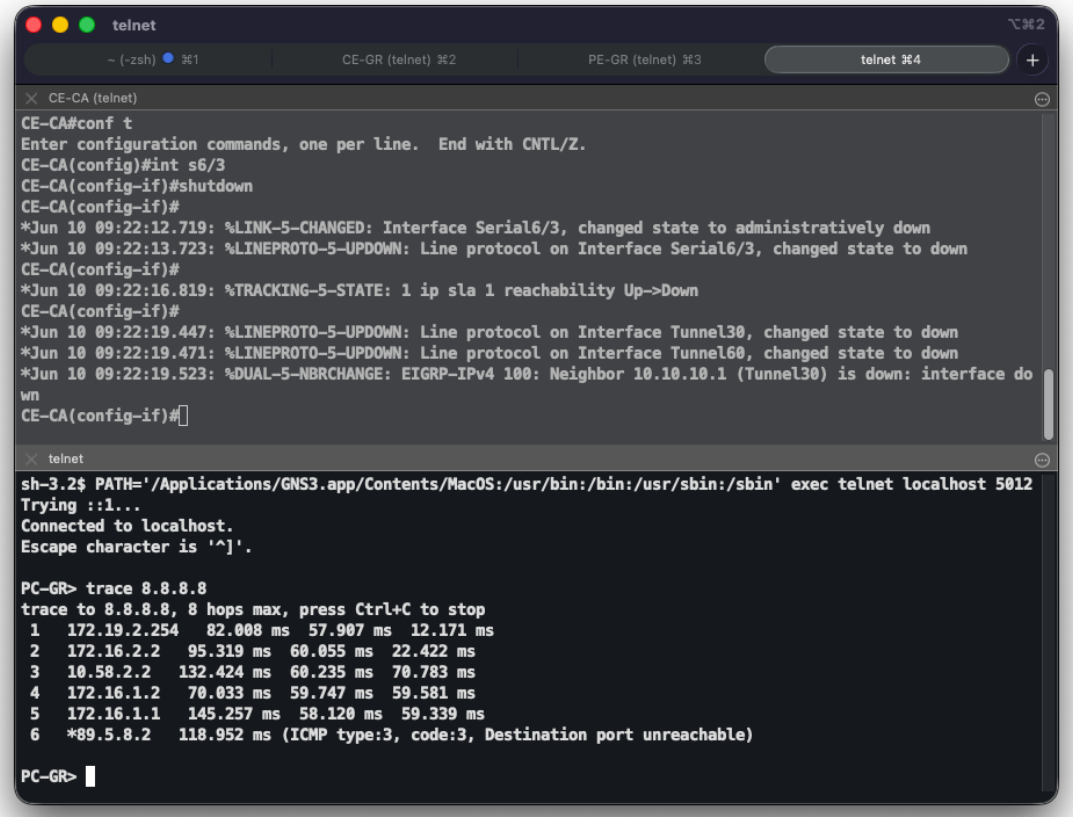
Ispravnost je potvrđena testiranjem: na CE-LJ su ugašeni i ISP i MPLS link, default ruta prešla je na `Tunnel100` (AD 210), a internetski pristup ostvaren je kroz kriptirani tunel i NAT na DC1 (deset od deset upita s LAN adrese). Da je promet stvarno enkriptiran, potvrđuju brojači naredbe `show crypto ipsec sa` (`#pkts encaps/encrypt` i `#pkts decaps/decrypt` rastu za GRE protokol). Za failover internetskog pristupa preko MPLS-a (priorit 2) dodatno je provjereno gašenje ISP linka na CE-GR: praćenje je palo, statička default ruta nestala, a promet je preuzela EIGRP default ruta kroz MPLS (pet od pet upita uspješno). Stanja se prate naredbama `show track`, `show ip route 0.0.0.0`, `show crypto ipsec sa` te provjerom internetskog pristupa naredbom `ping 8.8.8.8 source *ip*`.



Slika 4.5 Internet failover podružnice – primarna ruta (normalno stanje)



Slika 4.6 Pad ISP linka na CE-GR – default ruta i promet kroz definiranu backup lokaciju (Čapljina)



Slika 4.7 Degradacija – pad ISP linka i na backup lokaciji, izlaz kroz Ljubuški (CE-LJ)

4.4. Backup komunikacija podružnica s DC pri potpunom padu DC interneta

Poseban scenarij jest kad istovremeno otkažu ISP linkovi i na DC1 i na DC2. Tada oba kriptirana tunela podružnica prema podatkovnom centru (koja putuju preko interneta) padaju, pa podružnice uobičajenim putem gube vezu s DC LAN-om (10.97.100.0/24). Sve tri podružnice i u tom slučaju nastavljaju komunicirati s podatkovnim centrom, i to kroz backup vezu jedne podružnice, CE-LJ. Backup GRE+IPSec tunel (`Tunnel100`) opisan prethodno je idealan za to jer putuje dedicated serijskim linkovima i ne ovisi o internetu.

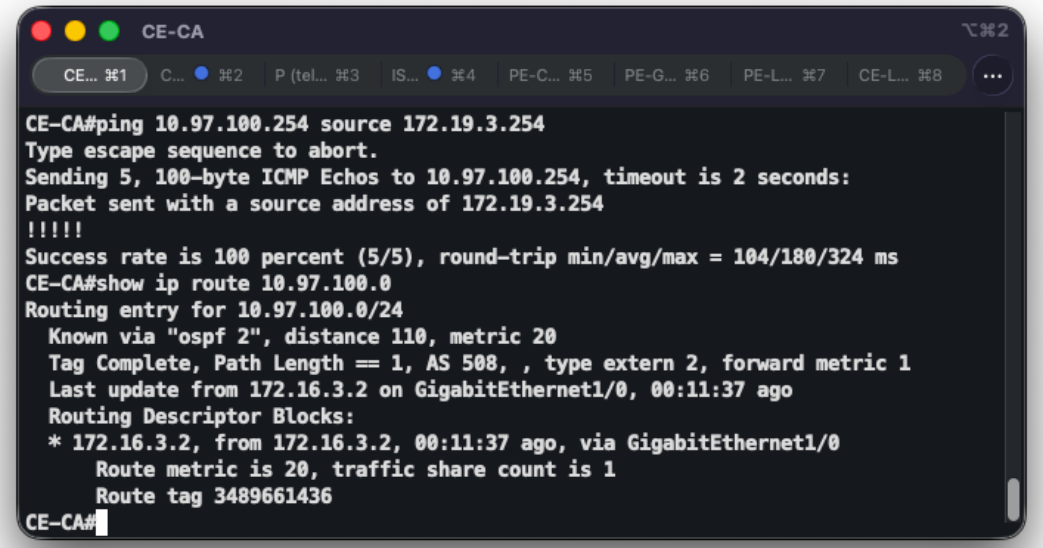
Da bi i CE-GR i CE-CA mogli iskoristiti taj put, CE-LJ uvjetno oglašava DC LAN u MPLS jezgru:

```
ip route 10.97.100.0 255.255.255.0 10.58.100.1 215
ip prefix-list DC-LAN seq 5 permit 10.97.100.0/24
route-map REDIST-DC-BKP permit 10
 match ip address prefix-list DC-LAN
```

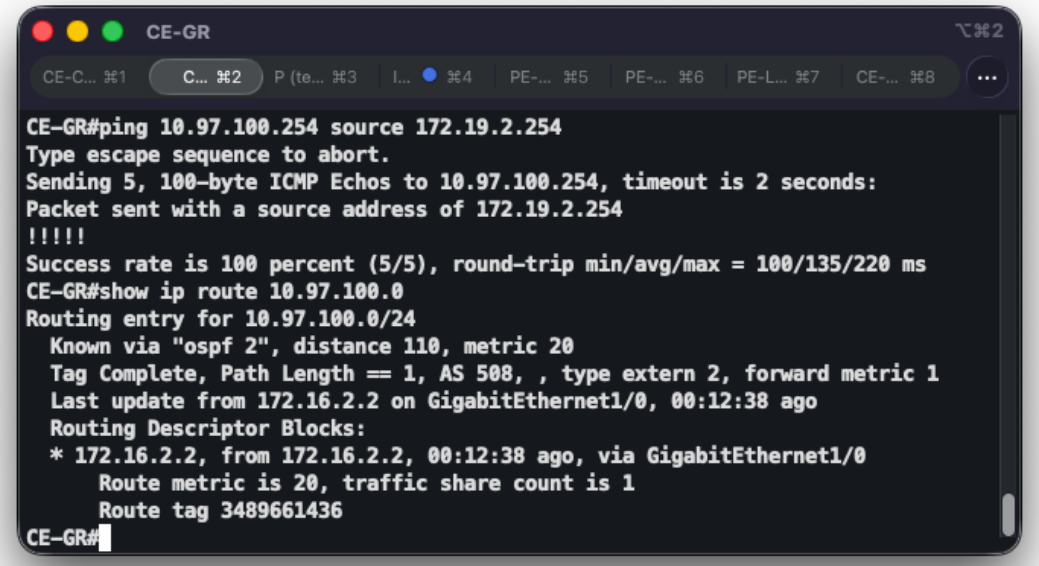
```
router eigrp 197
 redistribute static route-map REDIST-DC-BKP
ip route 172.19.1.0 255.255.255.0 10.58.100.2 215
ip route 172.19.2.0 255.255.255.0 10.58.100.2 215
ip route 172.19.3.0 255.255.255.0 10.58.100.2 215
```

Mehanizam se oslanja na svojstvo plutajuće statičke rute: ruta do DC LAN-a kroz backup tunel ima visoku administrativnu udaljenost (215) pa se u tablicu usmjeravanja instalira tek kad nestane bolji, primarni put prema DC-u (izravni tunel niže AD). Kako redistribucija u protokol usmjeravanja uzima samo rute koje su *stvarno* prisutne u tablici, DC LAN se u MPLS oglašava samo dok je primarni put nedostupan, dakle upravo onda kad oba DC ISP-a padnu. PE usmjernici tu rutu redistribuiraju u BGP VPNv4, pa je CE-GR i CE-CA primaju kroz MPLS i promet prema DC-u šalju do CE-LJ, koji ga dalje provodi kroz kriptirani backup tunel do DC1; povratne rute na DC1 (AD 215) vraćaju promet istim putem. Čim se internet u DC-u oporavi i primarni se put vrati, plutajuća ruta nestaje iz tablice, redistribucija prestaje i podružnice se automatski vraćaju na izravne tunele bez ručne intervencije. Time je izbjegnuto trajno usmjeravanje cjelokupnog DC prometa kroz bottleneck backup link, a istovremeno je zadovoljen uvjet da backup veza nosi isključivo statičke rute (bez dinamičkih protokola na samom tunelu). U baznom stanju redistribucija ide u EIGRP 197 kao PE-CE protokol; nakon prve migracije (poglavlje 5.1) isti se uvjet preslikava u `redistribute static ... router ospf 2`.

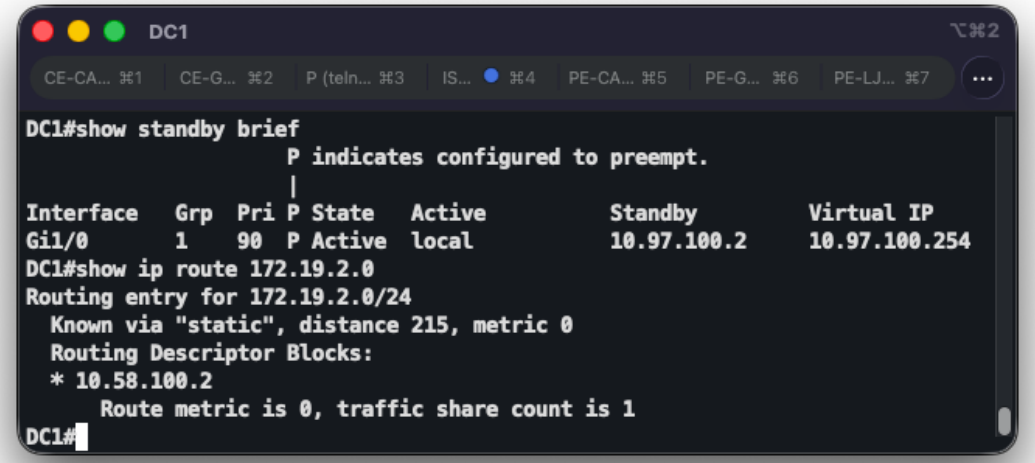
Ispravnost je potvrđena na integriranoj topologiji: gašenjem oba DC ISP linka oba tunela podružnica prema DC-u su pala, CE-LJ plutajuća ruta do DC LAN-a se aktivirala i redistribuirala u MPLS, a CE-GR i CE-CA dosegnule su DC LAN kroz backup tunel (pet od pet upita s LAN adrese za obje podružnice). Promet kroz `Tunnel100` pritom je kriptiran. Ponovnim podizanjem DC ISP linkova podružnice su se automatski vratile na izravne tunele (ruta do DC LAN-a ponovno preko dinamičkog protokola), čime je potvrđeno da backup put ne narušava primarni redoslijed.



Slika 4.8 Backup DC - oba ISP-a u kvaru, stanje prije



Slika 4.9 Backup DC - aktivacija rezervne rute



Slika 4.10 Backup DC - promet kroz backup link

5. Migracija mrežne arhitekture

Napravljene su tri migracije kojima se postojeća arhitektura postupno modernizira bez prekida usluge. Svaka je migracija dokumentirana zasebnim migracijskim planom koji obuhvaća analizu početnog stanja, definiciju ciljnog stanja, točan operativni slijed koraka, procjenu rizika i plan povrata, nakon čega slijedi opis izvedbe s podatkom o pogođenom dijelu topologije, trajanju prekida i potvrdi stabilnosti.

Sve tri migracije provedene su nad živom već konfiguriranom mrežom, a zajednička im je metoda istovremenog rada starog i novog mehanizma (engl. *ship-in-the-night*): novi protokol ili enkapsulacija pušta se paralelno uz postojeći, provjerava se njegova ispravnost dok stara konfiguracija još nosi promet, i tek se tada izvodi cutover uz mjerenje gubitka. Prije svake migracije izrađena je sigurnosna kopija GNS3 projekta (*Export portable project*), čime je omogućen povrat na prethodno stanje u slučaju pogreške.

5.1. Migracija 1 – prijelaz s EIGRP na OSPF na PE-CE segment

5.1.1. Analiza početnog stanja

Na segmentu između edge usmjernika davatelja (PE) i korisnika (CE) kao protokol usmjeravanja unutar VRF-a `ASI-VPN` koristi se EIGRP (autonomni sustav 197). EIGRP rute redistribuiraju se u MP-BGP koji ih prenosi kroz MPLS jezgru, a zadana ruta prema internetu propagira se redistribucijom statičke rute. Sva komunikacija među podružnicama i internetski failover kroz MPLS u tom trenutku ovise o ispravnom radu EIGRP-a na tri PE-CE para.

5.1.2. Ciljno stanje

EIGRP na PE-CE segmentu zamijenjen je protokolom OSPF (proces 2), uz zadržanu redistribuciju u MP-BGP. Rute podružnica trebaju se u tablicama usmjeravanja pojaviti kao OSPF međupodručne rute (oznaka `O IA`, administrativna udaljenost 110), tablica EIGRP susjeda mora biti prazna na svim uređajima, a mehanizam internetskog failovera kroz MPLS mora i dalje raditi neizmijenjeno.

5.1.3. Redoslijed koraka

1. Konfiguracija OSPF-a paralelno uz EIGRP na svim CE usmjernicima (`router ospf 2`) i PE usmjernicima (`router ospf 2 vrf ASI-VPN`); EIGRP i dalje nosi promet.
2. Provjera potpune susjednosti naredbom `show ip ospf neighbor` — sva tri PE-CE para moraju biti u stanju FULL.
3. Dodavanje redistribucije OSPF-a u MP-BGP uz zadržanu EIGRP redistribuciju (oba izvora privremeno koegzistiraju).
4. *Cutover*: uklanjanje EIGRP-a — redistribucije iz BGP-a te procesa `router eigrp 197` na CE i PE usmjernicima — uz kontinuirano mjerenje gubitka paketa.
5. Čišćenje zaostataka i pohrana konfiguracije.

```
router ospf 2
 router-id 172.16.1.1
 network 172.16.1.0 0.0.0.3 area 0
 network 172.19.1.0 0.0.0.255 area 0
 default-information originate
router ospf 2 vrf ASI-VPN
 router-id 172.16.1.2
 network 172.16.1.0 0.0.0.3 area 0
 redistribute bgp 508 subnets
 default-information originate
router bgp 508
 address-family ipv4 vrf ASI-VPN
  redistribute ospf 2 match internal external 1 external 2
  default-information originate
```

Ključna razlika u odnosu na EIGRP odnosi se na propagaciju default rute. Pod EIGRP-om se ruta `0.0.0.0/0` propagirala redistribucijom statičke rute, no OSPF ne preuzima zadanu rutu iz redistribucije statičkih ruta, već ju je potrebno izričito proizvesti naredbom `default-information originate`, i to na obje strane: na CE usmjerniku kako bi se lokalni izlaz na internet ubacio u OSPF, i na PE usmjerniku unutar VRF-a kako bi zadana ruta prošla od jezgre prema podružnici.

5.1.4. Procjena rizika i rollback

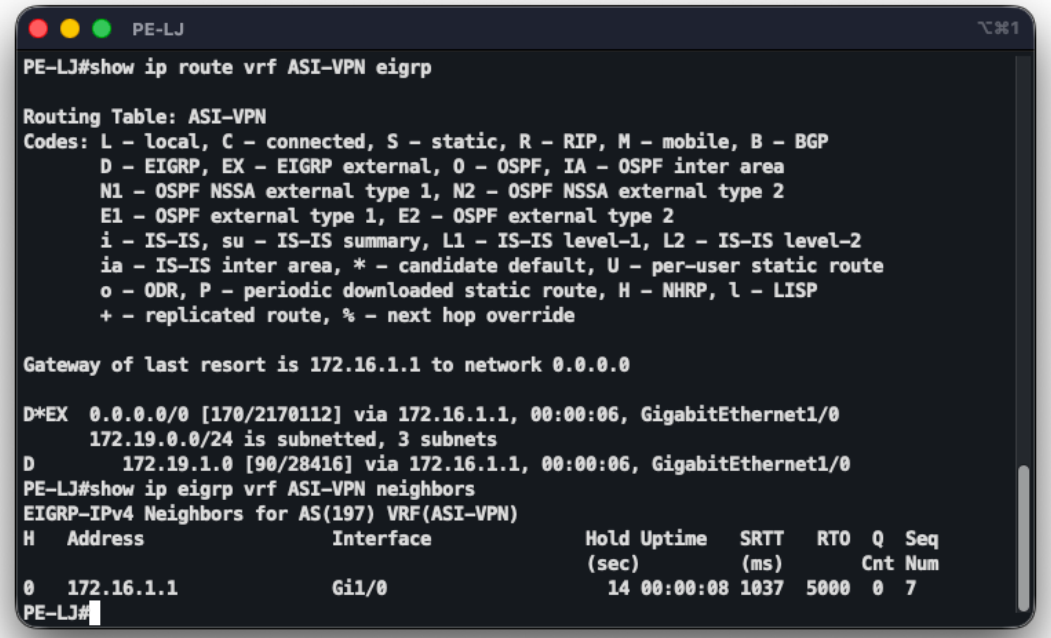
Glavni je rizik nastanak "crne rupe" tijekom *cutovera* ako bi se EIGRP uklonio prije nego što OSPF postigne potpunu susjednost; umanjen je paralelnim radom obaju protokola i

izričitom provjerom stanja FULL prije uklanjanja EIGRP-a. Drugi je rizik gubitak zadane rute, jer OSPF za razliku od EIGRP-a ne preuzima zadanu rutu iz redistribucije statičkih ruta. Izostanak naredbe `default-information originate` na bilo kojoj strani prekinuo bi internetski failover kroz MPLS (simptom: nestanak prefiksa `0.0.0.0/0` iz BGP VPNv4 tablice). Rizik je umanjen dodavanjem te naredbe na obje strane i provjerom failovera prije i poslije migracije. Treći je rizik prekoračenje dopuštena dva izgubljena paketa, ublažen kratkim *cutoverom* nakon potvrđene konvergencije OSPF-a.

U slučaju neuspjeha predviđena su dva sloja povrata. Brzi povrat tijekom rada: budući da EIGRP ostaje aktivan sve do *cutovera*, ponovno uvođenje EIGRP redistribucije i uklanjanje OSPF konfiguracije vraća prethodno stanje bez gašenja uređaja. Potpuni povrat: učitavanje sigurnosne kopije `SIP-backup-pred-migraciju-1b.gns3project`, koja čuva stanje neposredno prije migracije.

5.1.5. Izvedba i rezultati

Pogođeni dio topologije bila su tri PE-CE para i pripadne podružnice. Prekid je mjeren kontinuiranim pingom s računala PC-LJ prema podmreži druge podružnice tijekom *cutovera*: zabilježen je gubitak od samo jednog paketa od pedeset, čime je zadovoljen zahtjev od najviše dva izgubljena paketa. Stabilnost je potvrđena na više načina: sva tri PE-CE para pokazivala su stabilnu potpunu susjednost kroz uzastopne provjere, tablica EIGRP susjeda bila je prazna na svim uređajima, rute podružnica pojavile su se kao `O IA`, a ponovno su uspješno provjereni i internetski failover i komunikacija s kraja na kraj. Pri čišćenju su uklonjeni prazan proces `router eigrp 197` zaostao na PE usmjernicima te gola redistribucija statičkih ruta na CE usmjernicima.



Slika 5.1 Rezultat migracije 1

5.2. Migracija 2 – prijelaz sa static na EIGRP na DC tunelima

5.2.1. Analiza početnog stanja

Promet između podružnica i podatkovnog centra prolazi kroz GRE+IPSec tunele po kojima idu plutajuće statičke rute. Statika je ručno održavana, ne otkriva sama pad tunela (oslanja se na zaobilazni mehanizam IP SLA praćenja na DC1) i ne nudi automatsku zalihost između primarnog (DC1) i rezervnog (DC2) odredišta osim kroz specifično posložene administrativne udaljenosti.

5.2.2. Ciljno stanje

Statičke rute na tunelima zamijenjene su dinamičkim usmjeravanjem protokolom EIGRP (autonomni sustav 100) kao *overlay* protokolom: DC1 postaje primarni *hub*, DC2 rezervni, a podružnice *spoke* Time se priprema upravljačka ravnina za treću migraciju jer DMVPN koristi isti *overlay*. Pritom propisani redoslijed failovera (MPLS-VPN-backup) mora ostati

nenarušen: promet među podružnicama i dalje preferira MPLS, a EIGRP preko tunela služi kao rezervni put.

5.2.3. Redoslijed koraka

1. Konfiguracija EIGRP-a (AS 100) paralelno uz postojeću statiku na koncentratorima i krakovima; statika i dalje nosi promet.
2. Provjera uspostave susjedstva i topologije naredbama `show ip eigrp neighbors` i `show ip route`.
3. Podizanje administrativne udaljenosti EIGRP-a na krakovima naredbom `distance eigrp 200 210` te podešavanje metrike (`delay`) za preferenciju DC1.
4. *Cutover*: uklanjanje plutajućih statičkih ruta uz mjerenje gubitka.
5. Uklanjanje zaobilaznog mehanizma IP SLA praćenja pada tunela na DC1 (EIGRP ga zamjenjuje) i pohrana konfiguracije.

```
router eigrp 100
 network 10.10.10.0 0.0.0.3
 network 10.10.40.0 0.0.0.3
 network 172.19.1.0 0.0.0.255
 passive-interface FastEthernet0/0
 distance eigrp 200 210
 no auto-summary
interface Tunnel10
 delay 1000
interface Tunnel40
 delay 2000
interface Tunnel10
 no ip split-horizon eigrp 100
```

Podmreža podatkovnog centra, koja nema konkurenciju na MPLS-u, koristi EIGRP rutu (administrativna udaljenost 200), dok podmreže drugih podružnica i dalje preferiraju MPLS (`O IA`, udaljenost 110). Naredba `no ip split-horizon eigrp 100` na tunelima hub-a nužna je da bi hub ponovno oglasio rute jednog spoke-a ostalima.

5.2.4. Procjena rizika i rollback

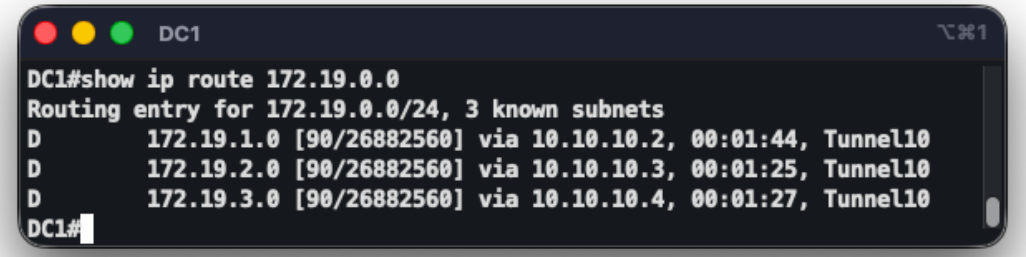
Najveći je rizik narušavanje redoslijeda failovera: interna EIGRP ruta ima administrativnu udaljenost 90, nižu od OSPF-ove (110), pa bi uz zadane postavke EIGRP preuzeo promet

među podružnicama s MPLS-a. Rizik je uklonjen podizanjem udaljenosti na spoke-ovima naredbom `distance eigrp 200 210`. Drugi je rizik prekid komunikacije među podružnicama zbog isključivanja svojstva *next-hop-self*: na klasičnim točka-na-točku GRE tunelima hub bi rutu jedne podružnice oglasio sa sljedećim skokom druge podružnice, čija je adresa u drugom tunelskom subnetu i nedostupna. Rizik je izbjegnut zadržavanjem tog svojstva u zadanom stanju i odgodom njegova isključivanja za treću migraciju (mGRE). Treći je rizik pogrešan izbor hub-a ili rutne petlje, ublažen metrikom (`delay`) i naredbom `no ip split-horizon`.

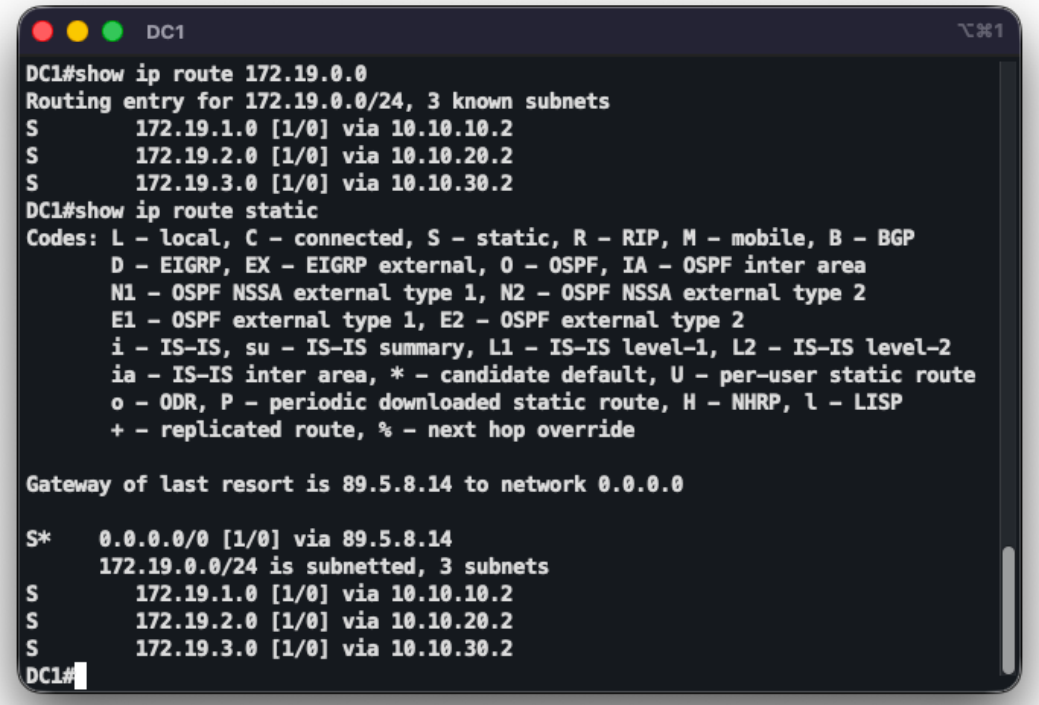
Brzi povrat: statičke rute zadržavaju se sve do *cutovera*, pa njihovo ponovno uvođenje uz uklanjanje EIGRP procesa vraća prethodno stanje bez prekida. Potpuni povrat: učitavanje sigurnosne kopije `SIP-backup-pred-migraciju-2.gns3project` (stanje nakon prve migracije).

5.2.5. Izvedba i rezultati

Pogođeni dio topologije bili su tuneli između podružnica i podatkovnog centra. Prekida praktički nije bilo. Pri *cutoveru* nije izgubljen nijedan paket (60 od 60 uspješnih upita), budući da je EIGRP ruta već imala isti sljedeći skok prema DC1 kao i uklonjena statika. Stabilnost je potvrđena dvama testovima otpornosti. U prvom je ugašen MPLS link radi provjere prebacivanja prometa među podružnicama na *overlay*; uočeno je da konvergencija ovisi o povlačenju prefiksa iz BGP VPNv4 tablice (oko 30 sekundi), a ne o samom EIGRP-u, jer podružnica privremeno zadržava staru MPLS rutu prema ugašenom susjedu. U drugom je testu ugašen tunel prema DC1: promet podatkovnog centra prešao je na DC2 bez gubitka paketa (45 od 45), a po oporavku tunela vratio se na DC1 zahvaljujući boljoj metrici.



Slika 5.2 Migracija 2 - DC1 statička ruta (prije)



Slika 5.3 Migracija 2 - DC1 EIGRP ruta (poslije)

5.3. Migracija 3 – prijelaz s P2P IPSec tunela na DMVPN Dual-hub Phase 3

5.3.1. Analiza početnog stanja

Između podružnica i podatkovnog centra postoji šest zasebnih P2P GRE+IPSec tunela. Svaka podružnica ima poseban tunel prema DC1 i prema DC2 sa statički definiranim odredištem. Takav pristup ne razmjenjuje promet izravno među podružnicama (sav promet prolazi kroz hub) i slabo se skalira jer svaki novi par lokacija zahtijeva ručno definiran tunel. Preko tunela već radi EIGRP *overlay* uveden u prethodnoj migraciji.

5.3.2. Ciljno stanje

Šest P2P tunela zamjenjuje se tehnologijom DMVPN u izvedbi Dual-Hub Dual-Cloud Phase 3: uvodi se multipoint GRE (mGRE) uz protokol NHRP, pri čemu DC1 i DC2 postaju poslužitelji sljedećeg skoka (NHS) za po jedan oblak, a podružnice se na njih dinamički

registriraju. Cilj uključuje izravnu komunikaciju među podružnicama (treća faza DMVPN-a) bez prolaska kroz hub, uz očuvan šifrirani prijenos i nepromijenjen redoslijed failovera. Adresni plan i EIGRP *overlay* ostaju isti, pa je migracija u biti čista zamjena enkapsulacije.

5.3.3. Redoslijed koraka

Migracija je izvedena namjenskom skriptom za automatizaciju (`migracija_3b.py`), koja konfiguracijske naredbe šalje na konzole uređaja kroz GNS3:

1. Faza 1 — konverzija rezervnog oblaka (DC2 kao hub), dok primarni oblak (DC1) i MPLS ostaju netaknuti. Hub se konfigurira prvi, zatim spoke.
2. Provjera oblaka 2: registracije NHRP spoke, EIGRP susjedstva i šifriranog prometa.
3. Faza 2 — konverzija primarnog oblaka (DC1 kao hub), uz već uspostavljen rezervni oblak kao zaštitu.
4. Provjera oblaka 1.
5. Provjera treće faze (izravni tunel među podružnicama) i pohrana konfiguracije na svim uređajima.

```
interface Tunnel10
 ip address 10.10.10.1 255.255.255.0
 ip nhrp authentication ASI-NHRP
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 no ip split-horizon eigrp 100
 no ip next-hop-self eigrp 100
 no tunnel destination
 tunnel mode gre multipoint
 tunnel key 1
interface Tunnel10
 ip address 10.10.10.2 255.255.255.0
 ip nhrp authentication ASI-NHRP
 ip nhrp network-id 1
 ip nhrp map 10.10.10.1 89.5.8.13
 ip nhrp map multicast 89.5.8.13
```

```
ip nhrp nhs 10.10.10.1
ip nhrp shortcut
delay 1000
no tunnel destination
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile ASI-IPSEC shared
```

Sada je, za razliku od prethodne migracije, primijenjeno isključivanje svojstva *next-hop-self* na hub-ovima. Uz mGRE i NHRP to više ne razbija komunikaciju među podružnicama, nego upravo omogućuje treću fazu DMVPN-a: krak u tablici usmjeravanja vidi stvarnu tunelsku adresu drugog spoke kao sljedeći skok, pa po primitku NHRP preusmjerenja od hub može izgraditi izravni tunel.

5.3.4. Procjena rizika i rollback

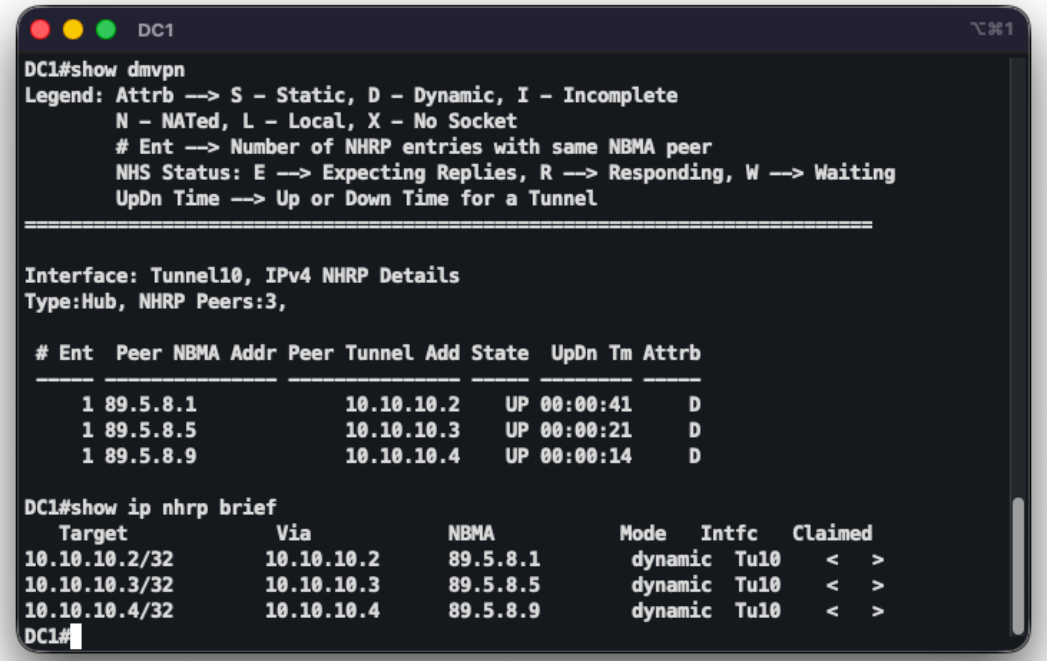
Najozbiljniji je rizik istovremeni gubitak povezanosti prema podatkovnom centru ako bi konverzija pošla po zlu na oba oblaka odjednom; umanjen je izvedbom oblak po oblak, počevši od rezervnog oblaka, tako da je u svakom trenutku barem jedan oblak i MPLS operativan. Drugi je rizik izostanak šifriranja: budući da oba tunela jednog kraka dijele isti izvor, IPSec zaštita mora biti označena kao dijeljena (`shared`), no dodavanje te oznake preko zatečenog kriptografskog stanja ne biva prihvaćeno pa bi hub primao nešifrirani promet. Rizik je uklonjen ispravnim redoslijedom, uklanjanjem zaštite s oba tunela (čime se ISAKMP resetira) pa ponovnim dodavanjem s oznakom `shared` koji skripta izvodi automatski. Treći je rizik pad emulacije usmjernika u simulatoru: brisanje tunelskog sučelja s kriptografskom i NHRP konfiguracijom (`no interface Tunnel`) ruši GNS3 emulaciju serije 7200, pa se nebitni izvorni tuneli na hub-ovima ne brišu nego samo administrativno gase (`shutdown`).

Zbog izvedbe oblak po oblak, neuspjeh na jednom oblaku ostavlja drugi oblak i MPLS netaknutima kao radni put, što omogućuje povrat samo zahvaćenog oblaka na prethodnu konfiguraciju. Potpuni povrat: učitavanje sigurnosne kopije `SIP-backup-pred-migraciju-3.gns3project` (stanje nakon druge migracije). Nakon uspješno dovršene i provjerene migracije izrađena je i kopija završnog stanja.

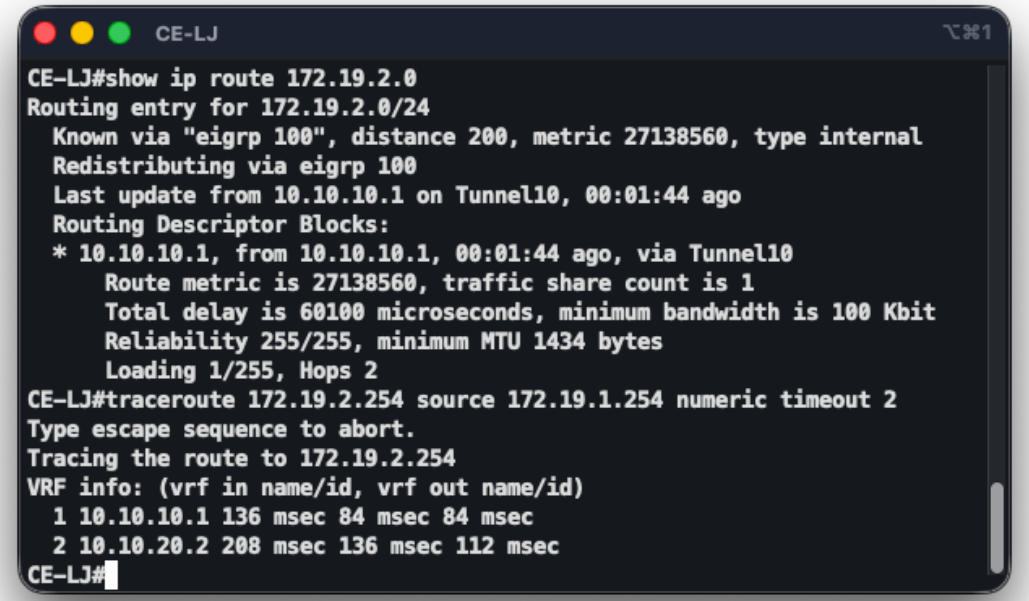
5.3.5. Izvedba i rezultati

Pogođeni dio topologije bili su tuneli između podružnica i oba hub-a; tijekom konverzije svakog oblaka prekid je bio ograničen na taj oblak, dok je drugi oblak (i MPLS) nosio promet, pa stvarni prekid usluge nije nastupio. Stabilnost je potvrđena dijagnostikom: oba hub-a prikazivala su po tri registrirana NHRP spoke-a u stanju UP, EIGRP susjedstva bila su potpuna, a na strani spoke-a postojale su dvije aktivne ISAKMP asocijacije (prema DC1 i DC2) s rastućim brojačima šifriranih i dešifriranih paketa, čime je potvrđen šifrirani prijenos kroz oba oblaka. Propisani redoslijed failovera ostao je očuvan: promet među podružnicama i dalje preferira MPLS (`O IA`, udaljenost 110).

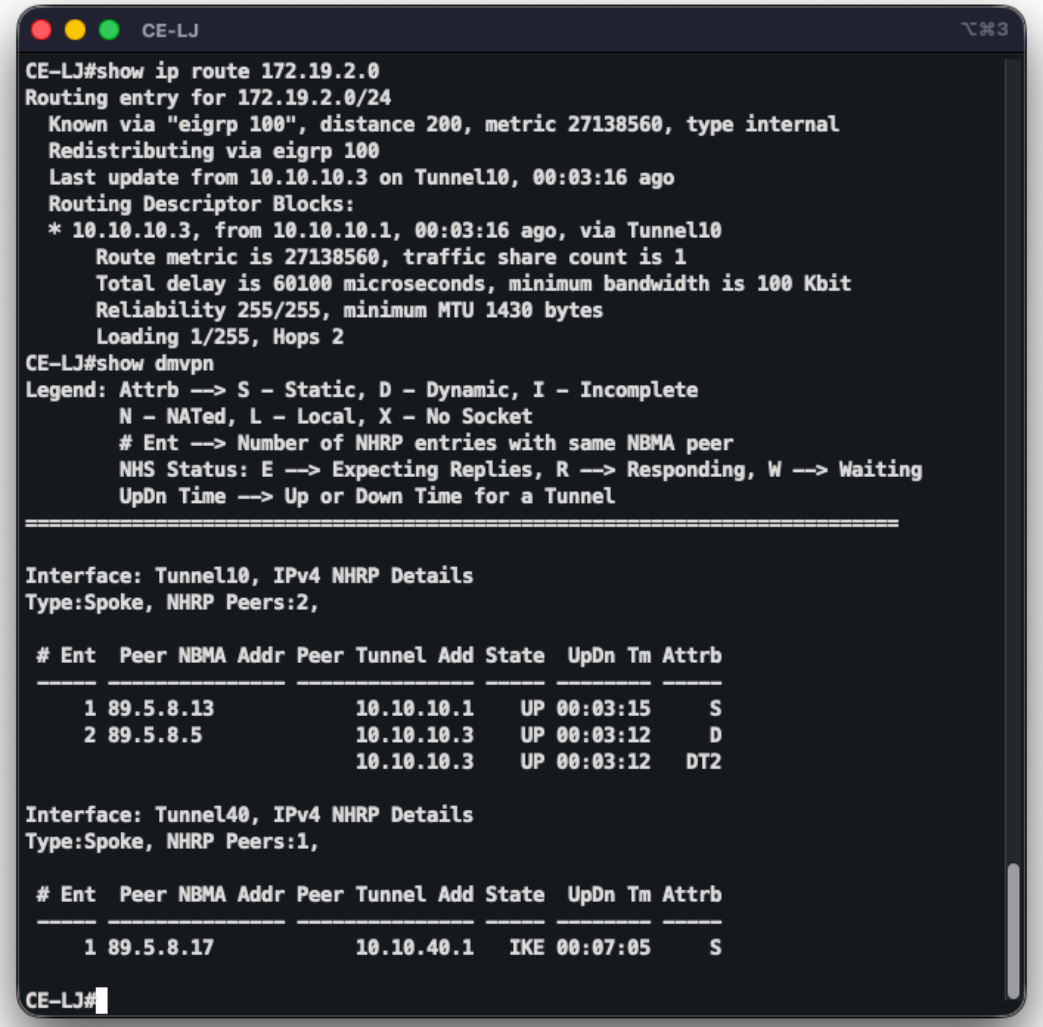
Posebno je provjerena treća faza DMVPN-a, odnosno izravna komunikacija među podružnicama. Privremenim gašenjem MPLS sučelja na CE-LJ promet prema podmreži druge podružnice prebačen je na *overlay*, pri čemu je ruta pokazivala stvarnu tunelsku adresu drugog spoke-a kao sljedeći skok. Prvi niz upita izgubljen je tijekom NHRP rezolucije i uspostave IPSec asocijacije za novi tunel, dok je drugi niz prošao u cijelosti (dvadeset od dvadeset upita uspješno). Naredba `show dmvpn` potvrdila je uspostavu izravnog dinamičkog tunela između CE-LJ i CE-GR, čime promet ide izravno s spoke na spoke umjesto kroz hub. Po vraćanju MPLS sučelja ruta se vratila na MPLS, potvrđujući da je strogi redoslijed failovera funkcionalan.



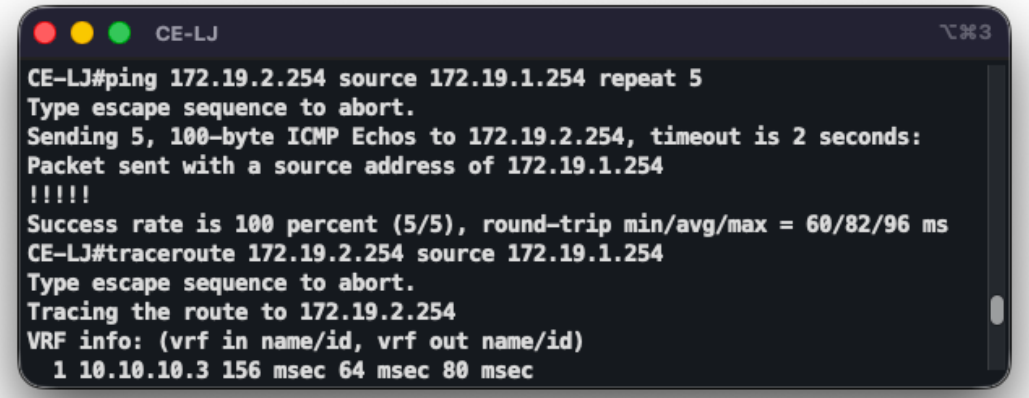
Slika 5.4 Migracija 3 - DMVPN na DC1



Slika 5.5 Prije DMVPN - promet kroz hub (2 skoka)



Slika 5.6 DMVPN phase 3 - ruta sa spoke next-hopom



Slika 5.7 DMVPN phase 3 - ping + traceroute (1 skok)

Zaključak

U okviru ovog projektnog zadatka projektirana je i implementirana cjelovita mrežna infrastruktura za tvrtku ASI ltd. u simulatoru GNS3, od bazne povezanosti i pristupa internetu do naprednih tehnologija usmjeravanja, enkripcije i otpornosti na ispade. Svi zahtjevi zadatka uspješno su ostvareni: automatsko dodjeljivanje adresa putem DHCP-a, pristup internetu uz NAT, MPLS L3 VPN kao primarni put komunikacije među podružnicama, GRE tuneli zaštićeni IPSec enkripcijom, redundancija internetskog pristupa u podatkovnom centru putem HSRP-a i IP SLA praćenja te višerazinski mehanizam failovera. Funkcionalnost svakog segmenta potvrđena je dijagnostičkim naredbama i testovima povezanosti, a otpornost ciljanim simulacijama ispada pojedinih linkova i segmenata.

Središnja projektna odluka je strogi redoslijed failovera u kojem MPLS ima prednost pred VPN tunelima, a backup link služi kao krajnje rješenje. Provučena je kroz cijelu implementaciju i očuvana pri svakoj kasnijoj promjeni. Upravo je to ograničenje oblikovalo niz tehničkih izbora, ponajprije podešavanje administrativnih udaljenosti pri uvođenju EIGRP-a kao *overlay* protokola, kako dinamičko usmjeravanje preko tunela ne bi preuzelo promet s primarnoga MPLS puta.

Tri provedene migracije pokazale su da se postojeća, živa mreža može modernizirati bez osjetnog prekida usluge primjenom metode istovremenog rada starog i novog mehanizma uz mjerenje gubitka pri prebacivanju. Prijelaz s EIGRP-a na OSPF izveden je uz gubitak od svega jednog paketa, prijelaz sa statičkog na dinamičko usmjeravanje preko tunela bez ijednog izgubljenog paketa, a prijelaz na DMVPN Dual-Hub fazu 3 uz dokazanu izravnu komunikaciju među podružnicama. Pritom se pokazalo koliko su za uspjeh ključni naizgled sitni detalji: izričito proizvođenje zadane rute pri promjeni protokola, pravilan redoslijed primjene dijeljene IPSec zaštite na tunelima koji dijele izvor te svjesnost o ograničenjima samog simulatora. Posljednja migracija dodatno je automatizirana namjenskom skriptom, čime je smanjena mogućnost pogreške pri ručnom unosu i ubrzano ponavljanje konfiguracijskih koraka.

Popis kratica

ACL	*Access Control List*	pristupna lista
AD	*Administrative Distance*	administrativna udaljenost
AES	*Advanced Encryption Standard*	napredni standard šifriranja
AS	Autonomous System	autonomni sustav
BDR	Backup Designated Router	rezervni određeni usmjernik
BGP	Border Gateway Protocol	protokol rubnog pristupnika
BKP	Backup	pričuvni link / usmjernik
CE	Customer Edge	rubni usmjernik korisnika
DC	Data Center	podatkovni centar
DH	Diffie-Hellman	algoritam za razmjenu ključeva
DHCP	Dynamic Host Configuration Protocol	protokol za dinamičko dodjeljivanje dresa
DMVPN		Dynamic Multipoint VPN dinamički višetočkovni VPN
DR	Designated Router	određeni usmjernik
DUAL	Diffusing Update Algorithm	algoritam difuzijskog ažuriranja
EIGRP	Enhanced Interior Gateway Routing Protocol	poboljšani protokol unutarnjeg usmjeravanja
ESP	Encapsulating Security Payload	sigurnosno enkapsuliranje korisnog tereta
GNS3	Graphical Network Simulator 3	grafički mrežni simulator
GRE	Generic Routing Encapsulation	generička enkapsulacija usmjeravanja
HSRP	Hot Standby Router Protocol	protokol pripravnog usmjernika
ICMP	Internet Control Message Protocol	internetski protokol kontrolnih poruka
IKE	Internet Key Exchange	internetska razmjena ključeva
IOS	Internetwork Operating System	međumrežni operacijski sustav
IP	Internet Protocol	internetski protokol
IP SLA	IP Service Level Agreement	sporazum o razini usluge
IPSec	Internet Protocol Security	sigurnost internetskog protokola
ISAKMP	Internet Security Association and Key Management Protocol	protokol za upravljanje sigurnosnim asocijacijama i ključevima
ISP	Internet Service Provider	davatelj internetskih usluga
LAN	Local Area Network	lokalna mreža

LDP	Label Distribution Protocol	protokol za raspodjelu labela
L3 VPN	Layer 3 VPN	virtualna privatna mreža trećeg sloja
mGRE	multipoint GRE	višetočkovni GRE
MP-BGP	Multiprotocol BGP	višeprotokolni BGP
MPLS	Multiprotocol Label Switching	višeprotokolno prospajanje po labelama
NAT	Network Address Translation	prevođenje mrežnih adresa
NBMA	Non-Broadcast Multiple Access	višepristupna mreža bez emitiranja
NHRP	Next Hop Resolution Protocol	protokol za razlučivanje sljedećeg skoka
NHS	Next Hop Server	poslužitelj sljedećeg skoka
OSPF	Open Shortest Path First	protokol najkraćeg puta
P	Provider	jezgreni usmjernik davatelja
PAT	Port Address Translation	prevođenje adresa s portovima
PE	Provider Edge	rubni usmjernik davatelja
PSK	Pre-Shared Key	unaprijed dijeljeni ključ
QM	Quick Mode	brzi način rada
QoS	Quality of Service	kvaliteta usluge
RD	Route Distinguisher	razlikovnik ruta
RT	Route Target	ciljna oznaka ruta
SD-WAN	Software-Defined Wide Area Network	programski definirana mreža širokog područja
SHA	Secure Hash Algorithm	sigurni algoritam sažimanja
SNMP	Simple Network Management Protocol	jednostavni protokol upravljanja mrežom
SYSLOG	System Logging	sustav zapisivanja događaja
TCP	Transmission Control Protocol	protokol kontrole prijenosa
VIP	Virtual IP	virtualna IP adresa
VPCS	Virtual PC Simulator	simulator virtualnih računala
VPN	Virtual Private Network	virtualna privatna mreža
VPNv4	VPN IPv4 Address Family	VPN IPv4 adresna obitelj
VRF	Virtual Routing and Forwarding	virtualno usmjeravanje i prosljeđivanje
WAN	Wide Area Network	mreža širokog područja