SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Lidija Belužić

PLANIRANJE MIGRACIJE S PROTOKOLA IPv4 NA IPv6

ZAVRŠNI RAD

ZAGREB, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 21. travnja 2017.

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

ZAVRŠNI ZADATAK br. 3920

Pristupnik: **Lidija Belužić (0135234102)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Planiranje migracije s protokola IPv4 na IPv6**

Opis zadatka:

Opisati karakteristike i razvoj protokola IPv4 i IPv6. Napraviti usporednu analizu protokola IPv4 i IPv6. Prikazati primjenu protokola IPv4 i IPv6 putem programskog alata Cisco Packet Tracer. Procijeniti budući razvoj protokola IPvX na temelju dostupne relevantne literature.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

doc. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

PLANIRANJE MIGRACIJE S PROTOKOLA IPv4 NA IPv6

PLANNING MIGRATION FROM IPv4 TO IPv6 PROTOCOL

Mentor: doc. dr. sc. Ivan Grgurević

Student: Lidija Belužić
JMBAG: 0135234102

Zagreb, rujan 2017.

PLANIRANJE MIGRACIJE S PROTOKOLA IPv4 NA IPv6

SAŽETAK

Internet protokol IP je internetski protokol mrežne razine koji ima osnovne funkcije adresiranja i usmjeravanja, odnosno prijenos datagrama kroz mrežu. Prilagođava se izvedbama prijenosne mreže i osigurava prijenos jedinica podataka. Postoje dvije verzije Internet protokola, a to su Internet Protokol verzije 4 i Internet Protokol verzije 6. Internet Protokol verzije 6 (IPv6) zamjenjuje Internet Protokol verzije 4 (IPv4) kao Internet standard, te je sljedeća evolucija Internet protokola. IPv6 protokol donosi nova poboljšanja koja bi trebala doprinijeti bržem i sigurnijem prijenosu podataka. Primjer primjene protokola IPv4 i IPv6 u radu je prikazan pomoću programskog alata Cisco Packet Tracer.

Ključne riječi: Internet protokol; IPv4; IPv6; mrežni sloj

SUMMARY

Internet Protocol IP is an online network protocol that has basic functions addressing and routing, or transferring data across the network. It adjusts Performs transmission networks and ensures data transfer. There are two versions of the Internet Protocol, which are Internet Protocol Version 4 and Internet Protocol Version 6. Internet Protocol Version 6 (IPv6) replaces Internet Protocol Version 4 (IPv4) as an Internet Standard and is the next evolution of the Internet Protocol. IPv6 protocol has been improved in such a way as to enable a faster and safer data transfer. Example of IPv4 and IPv6 protocol implementation is shown in the program tool Cisco Packet Tracer.

Key words: Internet Protocol; IPv4; IPv6; network layer

SADRŽAJ

1. UVOD

U mrežnoj komunikaciji podaci putuju po slojevima modela za otvoreno povezivanje sustava (engl. *Open Systems Interconnection Model* - OSI) odnosno TCP/IP (engl. *Transmission Control Protocol / Internet Protocol*) modelu koji u biti radi ono što OSI objašnjava u teoriji. Unutar tih modela mrežne komunikacije način obrade podataka određuju protokoli koji su smjernice tj. standardi. Oni se mogu definirati kao skupina pravila koja utvrđuje postupak prijenosa podataka u mreži. Referentni model po kojem se izrađuju ostali modeli je OSI referentni model te je iz njega nastao model TCP/IP koji se implementirao u telekomunikacije i postao najkorišteniji model za prijenos podataka.

Internet protokol je protokol mrežnog sloja TCP/IP složaja čija je uloga adresiranje i usmjeravanje odnosno prijenos datagrama kroz mrežu. Postoje dvije verzije Internet protokola, a to su IPv4 i IPv6.

Tema završnog rada je planiranje migracije s IPv4 na IPv6. Svrha završnog rada je prikaz značajki Internet Protokola verzije 4 i Internet Protokola verzije 6.

Cilj rada je napraviti komparativnu analizu značajki protokola te istaknuti i prikazati prednosti i nedostatke pojedine verzije protokola u funkciji migracije s IPv4 na IPv6.

Završni rad sastoji se od sedam funkcionalno povezanih dijelova ili teza:

1. Uvod,
2. Karakteristike i razvoj protokola IPv4,
3. Karakteristike i razvoj protokola IPv6,
4. Usporedna analiza protokola IPv4 i IPv6,
5. Prikaz primjene protokola IPv4 i IPv6 putem programskog alata Cisco Packet Tracer,
6. Budući razvoj protokola IPvX te
7. Zaključak.

Prvo poglavlje završnog rada je *Uvod* u kojem se iznosi predmet rada, cilj, svrha te njegova struktura.

U drugom poglavlju pod nazivom *Karakteristike i razvoj protokola IPv4***,** opisuju se klase IP adresa, karakteristike IPv4 protokola, zaglavlje IPv4 protokola te vrste adresa.

Karakteristike i razvoj protokola IPv6 prikazane su u trećem poglavlju rada gdje su opisani

tipovi adresa koje podržava protokol te su definirana polja zaglavlja IP paketa odnosno uloga informacija zapisanih u pojedinom polju zaglavlja kao i usmjeravanje kod IPv6 protokola.

Četvrto poglavlje rada je *Usporedna analiza IPv4 i IPv6 protokola*. U ovom poglavlju napravljen je usporedni prikaz IPv4 i IPv6 protokola te će se istaknuti prednosti protokola IPv6.

U petom poglavlju prikazana je primjena IPv4 i IPv6 protokola u programskom alatu Cisco Packet Tracer.

Budući razvoj protokola IPvX šesto je poglavlje rada gdje su navedene neke od budućih smjernica za daljnji razvoj IP protokola.

Sedmo poglavlje je *Zaključak* koji je donesen na temelju provedenih istraživanja/analiza i vlastitih promišljanja.

Na kraju rada se uz popis literature nalazi i popis kratica i akronima te popis slika i tablica prikazanih u tekstu rada.

2. KARAKTERISTIKE I RAZVOJ PROTOKOLA IPv4

IPv4 je internetski protokol[1] verzije 4 te je najraširenija IP protokol na najvećoj računalnoj mreži odnosno Internetu. Pojedine verzije IP protokola razlikuju se po načinu adresiranja, izgledu zaglavlja paketa, ali i brojnim drugim detaljima.

Najvažnija karakteristika IPv4 protokola je da koristi 32-bitnu IP adresu, što znači da je propisana duljina svake IP adrese u ovoj verziji protokola 32 bita [1].

IPv4 sastoji se od dva dijela:

- identifikatora mreže (engl. *Network Identifier*) i
- identifikatora krajnjeg računala (engl. *Host Identifier*).

Identifikator mreže određuje broj bita koji identificiraju mrežu u kojoj se nalazi mrežno sučelje i dodjela adrese preko ICANN (engl. *Internet Corporation for Assigned Names and Numbers*). Identifikator krajnjeg računala predstavlja ostatak bita koji služe za identifikaciju mrežnog sučelja koja je zadana s *Net* ID, dodjeljuje ih mrežni administrator i može ih dodatno podijeliti za uvođenje podmreža [2].

2.1. Zaglavlje IPv4 protokola

IPv4 verzija protokola detaljno propisuje izgled paketa, gdje su pojedina polja u zaglavlju detaljno specificirana, dok je sama duljina podataka u paketu varijabilna. Prema standardu minimalna duljina tako formiranog datagrama[2] je 20 bajtova, dok je maksimalna duljina 65535 bajtova. Slika 1 prikazuje zaglavlje IPv4 protokola te u nastavku slijedi opis polja u IPv4 paketu.

[1] **Protokol** je pravilo ili skup pravila koji su standardizirani, te omogućuju i olakšavaju komunikaciju unutar mreža.
[2] **Datagram** je nezavisan entitet koji samostalno putuje mrežom i nosi dovoljno informacija za usmjeravanje od izvorišta do odredišta [20].

Bitovi	Bitovi 0-3	4-7	8-15	16-18	19-31
0	Verzija	Duljina zaglavlja	Tip usluge	Ukupna duljina	
32	Identifikacija			*Flags*	*Fragment Offset*
64	Vrijeme života		Protokol	*checksum* zaglavlja	
96	Izvorišna adresa				
128	Odredišna adresa				
160	Opcije (0 ili više riječi)				
192	Podaci				

Slika 1. Zaglavlje IPv4 protokola [3]

Polje „Verzija“ (engl. *Version Field*) kod IPv4 zauzima četiri bita, a ima vrijednost 4, odnosno binarno 0100.

Polje „Duljina zaglavlja“ (engl. *Internet Header Length*, IHL) služi specificiranju ukupne duljine zaglavlja i označeno je s 32 bitnom riječi. Najmanja vrijednost koju ovo polje može imati je 5, kada je 5 x 32 = 160 bita = 20 bajta. Maksimalna vrijednost za 4 bitnu kombinaciju je 15 riječi, kada je 15 x 32 = 480 bita što iznosi 60 bajta [4].

Polje „Tip usluge“ (engl. *Type of Service*, TOS) je polje duljine 8 bita. Polje je osmišljeno za određivanje kvalitete usluge (engl. *Quality of Service*, QoS). Novije implementacije IPv4 protokola ovo polje mijenjaju sa 6 bitnim DSCP (engl. *Differentiated Service Code Point*) i 2 bitnim ECN (engl. *Explicit Congestion Notification*) poljem. DSCP polje određuje vrijednost QoS-a za svaki paket. ENC polje služi za dobivanje informacija o zagušenjima kroz mrežu između početka i kraja [5].

Polje „Ukupna duljina“ (engl. *Length*) služi za određivanje ukupne duljine IP paketa uključujući i podatke. Ovo polje prezentira se oktetima i u zaglavlju zauzima 16 bita.

Polje „Identifikacije“ (engl. *Identification*), zauzima 16 bita, a određeno je od strane pošiljatelja. Služi identifikaciji pojedinačnih paketa, koji su rastavljeni na fragmente od strane usmjernika[3] [4].

Polje „*Flags*“, služi za određivanje postupanja uređaja prema određenom IP paketu. Polje se sastoji od tri bita. Prvi bit uvijek ima vrijednost 0, drugi bit služi za određivanje fragmentacije (0 – paket se smije fragmentirati, 1 – paket se ne smije fragmentirati), dok treći bit prezentira lokaciju paketa u nizu fragmentiranih paketa (0 – paket se nalazi kao zadnji fragment u nizu ili paket nije fragmentiran uopće, 1 – paket nije zadnji u nizu fragmentiranih paketa i treba se očekivati dolazak više fragmentiranih paketa) [4].

Polje „*Fragment Offset*“, koristi 13 bita. Ovo polje služi određivanju konačnog uređaja gdje se trebaju nalaziti svi podaci nakon ponovnog sastavljanja. Paketi koji nisu fragmentirani i prvi paketi u nizu fragmentiranih paketa uvijek imaju vrijednost ovog polja postavljenu u 0.

Polje „Vrijeme života“ (engl. *Time to Live*, TTL) koristi se za određivanje količine vremena u kojoj je dopušteno paketu biti u mreži. Vrijeme života određeno je s 8 bita koji predstavljaju sekunde. Kako se komunikacija između uređaja izvršava za manje od 1 sekunde, ovo polje najčešće zaprima vrijednost najvećeg broja skokova od izvora do odredišta u mreži. Svaki uređaj koji zaprimi paket smanjuje vrijeme života za 1, neovisno o tome je li vrijeme slanja između 2 uređaja bilo manje od jedne sekunde. Kada polje dođe u vrijednost 0, paket se gubi.

Polje „Protokol“ (engl. *Protocol*) koristi 8 bita i služi označavanju protokola za slanje paketa. Ako polje poprimi vrijednost 0x06 (u heksadekadskom zapisu) ili 00000110 (u binarnom zapisu), koristi se TCP (engl. *Transmission Control Protocol*) protokol. Ako polje poprimi vrijednost 0x11 (u heksadekadskom zapisu) ili 00010001 (u binarnom zapisu), koristi se UDP (engl. *User Datagram Protocol*) protokol. *Internet Control Message Protocol* (ICMP[4]) predstavljen je heksadekadskim zapisom 0x01 ili binarnim zapisom 00000001 [5].

[3] **Usmjernik** je uređaj koji usmjerava podatkovne pakete kroz mrežu pomoću IP adrese i djeluje na mrežnom sloju OSI modela.
[4] **ICMP** je kontrolni protokol za otkrivanje pogrešaka u računalnim mrežama tokom komunikacije tako da se šalju tzv. ICMP paketi [21].

Polje „*Checksum*“ zauzima 16 bita. Služi kao metoda za provjeravanje i potvrđivanje da nije došlo do promjene niti jednog polja zaglavlja IP paketa. Zbog promjene polja „Vrijeme života“, polje „*Checksum*“ se ponovno računa unutar svakog uređaja u mreži.

Polja „Izvorišna“ (engl. *Source Address*) i „Odredišna“ (engl. *Destination Address*) adresa, određena s 32 bita, označavaju IP adresu izvorišnog i odredišnog uređaja.

Polje „Opcije“ (engl. *Options*) ima varijabilnu vrijednost duljine i u njemu se određuju dodatne opcije za slanje. Većina IP paketa, koji se šalju u suvremenim mrežama, nemaju ovo polje, zato što se ovo polje najčešće ne koristi [5].

Polje „Podaci“ (engl. *Data*) je polje varijabilne vrijednosti duljine. U ovom polju se spremaju podaci i protokoli vezani za slanje tih podataka, kao što su: TCP, UDP i ICMP. Ovo polje sadrži zaglavlje i podatke protokola transportnog sloja. Važno je napomenuti da svaki TCP/IP protokol dodaje svoje zaglavlje kada primi podatke od ostalih slojeva.

2.2. Tipovi adresa IPv4

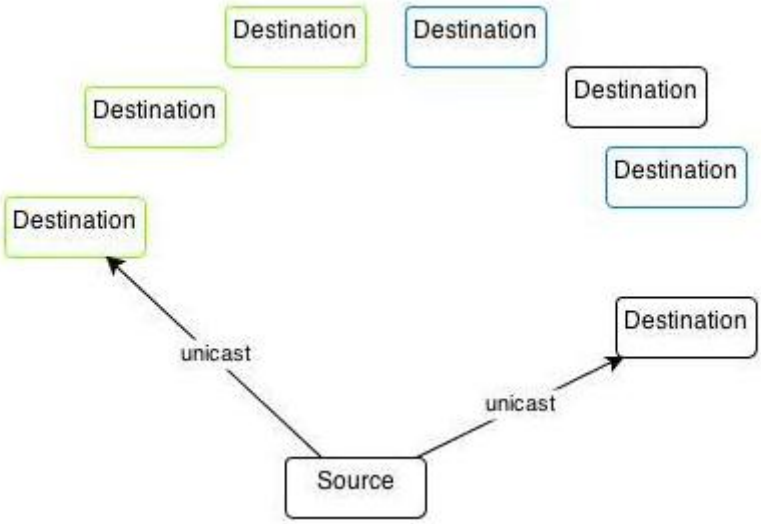
Kako bi uređaji na Internetu bili dostupni moraju imati adresu na koju će im se upućivati podaci. IP adresa može se zapisati binarno i dekadski. Decimalni zapis IP adrese je 192.168.1.1, dok je u binarnom obliku, uz odvajanje u 4 grupe po 8 bita 11000000 10101000 00000001 00000001.

S obzirom na to da je duljina 32 bita, može se izračunati maksimalni broj različitih adresa, a iznosi 4 294 967 296 adresa. Zbog povećanja broja umreženih računala, IPv4 zbog svoje limitiranosti nije više pogodan za adresiranje.

Kako bi se omogućilo komuniciranje unutar adrese Internet standard definira 3 tipa IPv4 adresa, a prema [5] to su:

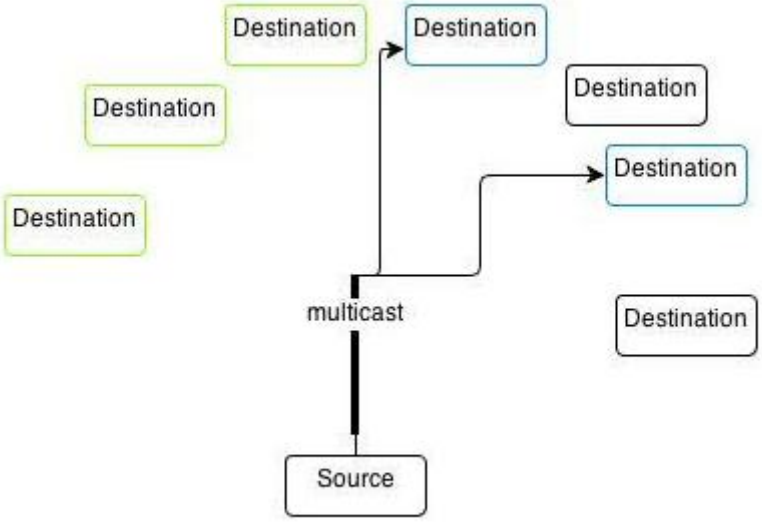
- *Unicast* – dodjeljuje se jednom mrežnom sučelju koje se nalazi na određenoj podmreži i koristi se za komuniciranje jedan na jedan.
- *Multicast* – dodjeljuje se jednom ili više mrežnim sučeljima koji se nalaze na različitim podmrežama i koriste se kada jedan korisnik komunicira prema većem broju primatelja.

- *Broadcast* - dodjeljuje se svim mrežnim sučeljima, koja se nalaze na podmreži i koristi se za komunikaciju jednog korisnika prema svima koji se nalaze u toj podmreži [6].



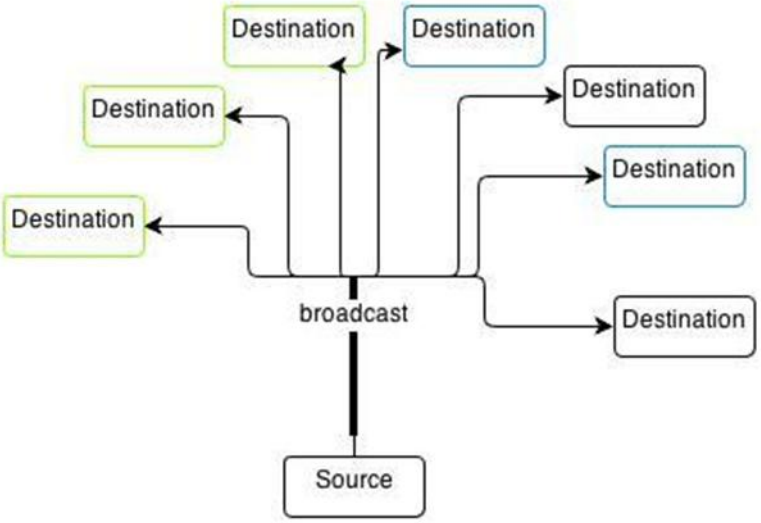
Slika 2. Komuniciranje putem unicast adrese [5]

Unicast adrese identificiraju lokaciju sučelja na mreži na isti način kao i što ulični brojevi identificiraju adresu. Da bi se locirala kućna adresa treba se znati prebivalište, isto tako i *unicast* adresa mora imati globalnu jedinstvenu mrežu i jedinstveni format. Svaka IPv4 *unicast* adresa uključuje mrežni dio (*network* ID) i računalni dio (*host* ID). Na slici 2 prikazan je način komuniciranja korištenjem unicast adresa.



Slika 3. Komuniciranje putem multicast adrese [5]

Multicast adrese se koriste za prijenos jednog paketa prema više primatelja kao što je na slici 3. Na IPv4 *multicast*u omogućen je intranet, paket je proslijeđen od strane usmjernika do podmreže, gdje se nalaze *host*-ovi koji osluškuju mrežni promet, poslan pomoću IPv4 *multicast* adrese.



Slika 4. Komuniciranje putem broadcast adrese [5]

Broadcast adresa pruža komunikaciju prema svima unutar određene podmreže. Svi paketi se obrađuju na sučeljima unutar podmreže. Postoje različite vrste *broadcast* adresa, a to su mrežni, podmrežni i ograničeni *broadcast* prikazano na slici 4.

2.3. Usmjeravanje kod IPv4 protokola

Usmjeravanje je ključna funkcija mrežnog sloja, a vrši se uz pomoć IP adrese krajnjeg odredišta koja se upisuje u zaglavlje IP datagrama. Da bi paketi stigli na odredište, moraju preći preko uređaja koji prosljeđuje podatke, a naziva se usmjernik (engl. *router*). Primarna uloga usmjernika je osigurati paketu da stigne od izvorišta do odredišta, a sekundarna da omogući da paketi idu najboljim putem [6].

IP paketi koriste najmanje jedan od dva moguća načina dostave, koji ovise o odredištu, ovisno o direktnoj povezanosti odredišta na mrežu. Ta dva načina dostave mogu biti:

- direktno ili
- indirektno dostavljane.

Direktno dostavljanje javlja se kada IP čvor (čvor koji šalje ili IP usmjerivač) prosljeđuje paket na odredište, koje je direktno povezano na mrežu. IP čvor enkapsulira[5] IP pakete u okvir za mrežni sloj, zbog fizičke adrese (MAC adrese).

Indirektno dostavljanje javlja se kada IP čvor (čvor koji šalje ili IP usmjerivač) prosljeđuje paket na drugi čvor (IP usmjerivač) zato što odredište nije direktno povezano na mrežu. IP čvor enkapsulira IP paket u okvir za mrežni sloj, zbog fizičke adrese.

Tablica usmjeravanja se kreira po *defaultu*[6] kada se TCP/IP inicijalizira te ih administrator unosi ručno ili automatski prilikom komunikacije s usmjernikom [7].

U tablici usmjeravanja spremljene su adrese IP čvorova. Tablica usmjeravanja posjeduje informacije o IP čvorovima i informacije kako doći do tih čvorova. Kada IP paket treba usmjeravati, tablica usmjeravanja se koristi za određivanje rute.

[5] **Enkapsulacija** je postupak pakiranja podataka, počinje se odvijat na uređaju koji šalje podatke odnosno izvoru informacije.
[6] **Default** – automatski postupak, odnosi se na standardnu radnju ili stanje.

U tablici usmjeravanja spremljene su adrese IP čvorova. Kada se upisuju podaci u tablicu usmjeravanja, informacije trebaju sadržavati:

- identifikator mreže,
- mrežnu masku,
- sučelje,
- *Next hop* te
- *Metric*.

Mrežna maska služi za uspoređivanje odredišne IP adrese s identifikatorom mreže.

Next hop u sebi ima spremljenu IP adresu sljedećeg čvora u mreži. Sučelje prikazuje koje mrežno sučelje se koristi za prosljeđivanje IP paketa.

U polju *Metric* se nalazi najčešći broj skokova između dva čvora kojim se označavaju troškovi rute kako bi se odabrao najbolji put do odredišta.

Za određivanje zapisa u tablici usmjeravanja za sljedeći skok, IP protokol koristi sljedeća dva koraka. U prvom koraku IP protokol provodi logičku operaciju konjunkcije (logičko „i“) između odredišne IP adrese i mrežne maske. U tom se koraku, također uspoređuje rezultat s *Network ID*-em, zbog podudaranja. U drugom koraku stvara se popis odgovarajućih ruta. Nakon stvaranja popisa odgovarajućih ruta bira se najbolja ruta. Najbolja ruta je najdirektnija ruta do odredišne IP adrese. Ako postoje dvije najbolje rute, odabire se ruta s najmanjim brojem skokova od izvora do odredišta. Krajnji rezultat u procesu određivanja ruta je jedna ruta u tablici usmjeravanja, koja propušta IP adresu sljedećeg uređaja i sučelja. Ako proces određivanja rute ne uspije, IP protokol označuje grešku prilikom usmjeravanja. Za pošiljatelja, greška o IP usmjeravanju se šalje prema protokolima višeg sloja (npr. TCP[7] ili UDP[8]). U usmjerivaču se šalje poruka o neuspjelom usmjeravanju ICMP (engl. *Destination Unreachable–Host Unreachable*) na izlazni *host* [7].

[7] **TCP** (engl. *Transmisson Control Protocol*) je protokol koji u računalnoj mreži korisniku kreira virtualnu konekciju prema drugom korisniku, tzv. spojni protokol sa mogućnošću provjere primitka poruke.
[8] **UDP** (engl. *User Datagram Protocol*) je protokol koji omogućuje slanje kratkih poruka između aplikacija na umreženim računalima, te nema mogućnost provjere primitka poruke.

3. KARAKTERISTIKE I RAZVOJ PROTOKOLA IPv6

Internet protokol verzija 6, ili kraće IPv6 je novija verzija internet protokola koja polako postaje sljedeća standardna verzija komunikacijskog protokola na Internetu. Pojedine verzije internet protokola se razlikuju po načinu adresiranja, izgledu zaglavlja paketa, ali i brojnim drugim detaljima.

Najvažnija karakteristika IPv6 je da koristi 128-bitnu IP adresu, tj. propisana duljina svake IP adrese u ovoj verziji protokola je 128 bita [8].

Podijeljena je u dva dijela:

- mrežni prefiks (engl. *network prefix*) i
- računalni prefiks (engl. *host prefix*).

Mrežni prefiks se dodjeljuje od strane institucija, a računalni prefiks se dodjeljuje ili automatski iz MAC adrese ili od mrežnog administratora. IPv6 piše se u osam grupa po četiri heksadekadske znamenke i svaka grupa odijeljena je s ":" [8].

Prema [8], uvođenjem IPv6 protokola prema zaglavlje dobiva neke nove značajke:

- novi format zaglavlja,
- veličina adresnog prostora,
- ugrađeni sigurnosni mehanizmi,
- poboljšana podrška za kvalitetu usluge te
- proširivost.

Primjer IPv6 adrese je 2001:b68:0:0:c789:0:f123. Ukoliko se u adresi ponavljaju nule tada se one mogu zamijeniti sa znakom "::" koji se može upotrijebiti samo jednom. Osim navedenog, adresa se može zapisati u obliku 2001:b68:0:a123::f123/64 i uz ovakvu mrežu na raspolaganju je 64 bita [8].

Kod adresiranja može biti više adresa bilo kojeg tipa (jednoodredišna, višeodredišna, rezervirana) na jednom fizičkom sučelju. Sva sučelja imaju *Link-local*[9] adrese i one su jedinstvene samo na razini linka. Svrha te adrese je autokonfiguracija ili trenutni pristup mreži ako nema usmjernika.

[9] ***Link-local*** – mrežna adresa za komuniciranje unutar jednog mrežnog segmenta [22].

Usmjeravanje IPv6 paketa omogućava da usmjeravanje bude na razini usmjernika nakon što *Global unicast* adrese budu konfigurirane[10] na razini lokalne mreže.

Usmjeravanje može biti:

- dinamičko – pomoću usmjerivačkih protokola ili
- statičko – pomoću statičkih ruta.

Statičke tablice usmjeravanja se učitavaju kod pokretanja operacijskog sustava i ne mijenjaju se ukoliko se ne dogodi greška. Kod statičkog usmjeravanja nije potreban dodatni softver za usmjeravanje.

Algoritam dinamičkog usmjeravanja počinje u trenutku pokretanja operacijskog sustava na isti način kao i algoritam statičkog usmjeravanja. Algoritam usmjeravanja koji koristi statičke tablice usmjeravanja i *default* rute u glavnom nije dovoljan za korištenje na većini usmjernika.

3.1. Zaglavlje IPv6 protokola

Zaglavlje IPv6 je, u osnovi, pojednostavljeno zaglavlje verzije četiri ovog protokola. Dio polja i formata je zadržan, međutim izbačena su nepotrebna, slabo korištena i zastarjela polja, a dodana su polja za bolju podršku prometa u realnom vremenu.

Dok je IPv4 zaglavlje bilo varijabilne duljine, zaglavlje IPv6 ima fiksnu duljinu od 40 okteta, od čega čak 32 okteta otpada na adrese. Osim toga, minimalno IPv6 zaglavlje ima samo sedam polja, za razliku od trinaest polja zaglavlja verzije 4. Smanjenjem broja obaveznih polja postignuta je brža obrada IPv6 paketa u usmjernicima na mreži, jer je potrebno analizirati manji broj (jednostavnijih) polja.

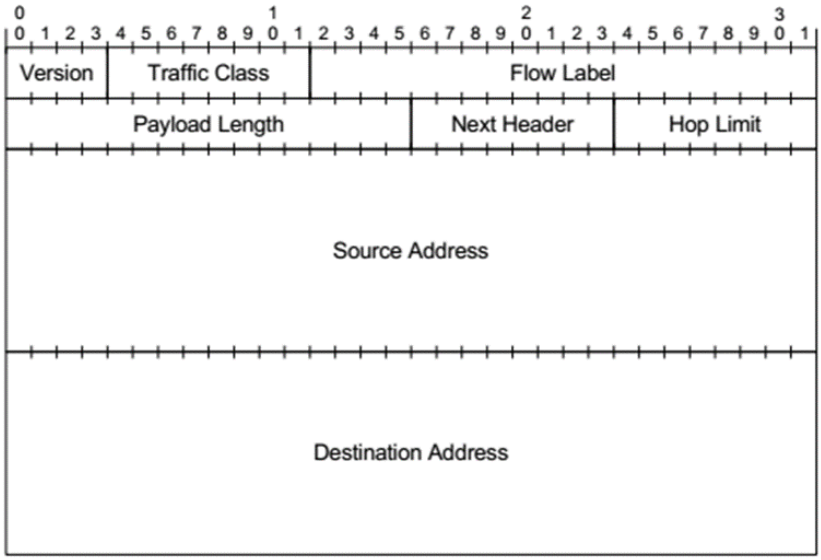
Polja IPv6 zaglavlja su:

- Version – verzija
- Traffic Class – klasa prometa
- Flow Label – tok podataka
- Payload Length – dužina podataka

[10] **Konfiguracija** je izbor računalnog hardvera konkretnog korisnika.

- Next Header – sljedeće zaglavlje
- Hop Limit – broj skokova
- Source Address – izvorišna adresa
- Destination Address – odredišna adresa

U IPv4 zaglavlju polje opcija smješteno je u osnovno IPv4 zaglavlje, i ono je varijabilne duljine, dok su kod IPv6 zaglavlja sve opcije maknute iz osnovnog zaglavlja, a uvedena su dodatna zaglavlja koja definiraju naprednije funkcije, te se nalaze nakon osnovnog zaglavlja. Ovakvim dizajnom protokola, usmjernicima u mreži ušteđeno je vrijeme obrade, jer ne troše procesorsko vrijeme na obradu polja koje se ne odnose na njih.



Slika 5. Zaglavlje protokola IPv6 [9]

Slika 5 prikazuje zaglavlje IPv6 paketa.

Zaglavlje započinje poljem *Version* te kao i kod IPv4 predstavlja verziju IP protokola. Za IPv6 u to polje mora biti upisan broj 6.

Nakon toga dolazi oznaka klase prometa te oznaka toka podataka kojemu paket pripada. Zatim dolazi oznaka duljine paketa koja sadrži duljinu polja podataka u oktetima ili bitovima. Ovo polje mora biti postavljeno na nulu. U slučaju da je potrebna veća nosivost paketa, postoji proširenje unutar IPv6 zaglavlja.

Polje *Next Header* je ekvivalentno polju *Protocol* iz IPv4 pri čemu to polje može sadržavati i oznaku opcije koja dolazi nakon zaglavlja. Ovo polje određuje protokol transportnog sloja. Dvije najčešće verzije su TCP i UDP.

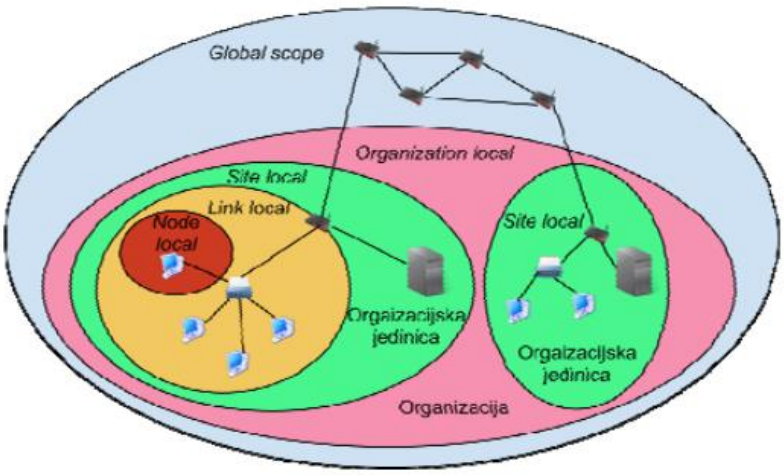
Iduće polje je *Hop Limit* koje ima ekvivalentu ulogu kao i polje TTL iz IPv4 paketa. Naime, prvotna ideja polja TTL bila je da se umanjuje za 1 svake sekunde. Međutim, u praksi se je vrijednost polja umanjivala za 1 nakon svakog usmjernika, tj. svakog skoka koji bi paket napravio. Iz tog razloga se to polje sada naziva *Hop Limit*, tj. maksimalan broj skokova koje paket može napraviti.

Na kraju dolaze *Source Address* odnosno 128-bitna adresa izvorišta i *Destination Address* odnosno 128-bitna adresa odredišta.

3.2. Tipovi adresa IPv6

IPv6 adresa se dodjeljuje mrežnom sučelju računala ili grupi takvih sučelja. Općenito, postoje 3 vrste IPv6 adresa [10]:

- jednoodredišna adresa (engl. *unicast address*),
- jednoodredišna adresa unutar skupine (engl. *anycast address*), i
- višeodredišna adresa (engl. *multicast address*).



Slika 6. Organizacija IPv6 adresa [10]

Jednoodredišne i višeodredišne adrese su vrste adresa koje se koriste i kod protokola IPv4, dok su za IPv6 karakteristične jednoodredišne adrese unutar skupine. Jednoodredišna adresa označava jedno sučelje, što znači da će paket poslan na tu adresu biti dostavljen sučelju koje je određeno tom adresom. Za označavanje grupe sučelja koriste se preostale vrste adresa, s tom razlikom da će paket poslan na jednoodredišnu adresu unutar skupine biti dostavljen "najbližem" od sučelja koja su određena tom adresom, dok će paket poslan na višeodredišnu adresu biti dostavljen svim sučeljima koja su određena tom adresom.

Postoji više vrsta jednoodredišnih adresa:

- agregabilna globalna jedinstvena adresa (engl. *Aggregatable Global Unicast Address*),
- jedinstvena adresa na lokalnoj vezi (engl. *Link-local Unicast Address*),
- jedinstvena adresa lokalne veze (engl. *Site-local Unicast Address*) i
- posebne adrese (engl. *Special Address*).

Za čvorove u Internetu najvažnija je globalna jednoodredišna adresa. Ta vrsta adrese organizirana je u tri dijela:

1. globalni prefiks usmjeravanja,
2. oznaka podmreže i
3. oznaka sučelja.

Globalni prefiks usmjeravanja predstavlja vrijednost koja označava grupu podmreža/poveznica, oznaka podmreže predstavlja oznaku podmreže/poveznice unutar te grupe podmreže/poveznica, dok je oznaka sučelja jedinstvena na podmreži na koju je sučelje priključeno. Svakom čvoru se dodjeljuje određeni broj adresa, poput lokalne adrese na razini poveznice za svako sučelje čvora, dodatnih jednoodredišnih/*anycast* adresa za sučelja čvorova, *loopback* adrese za *loopback* sučelje, različitih vrsta *multicast* adresa, itd. Usmjeritelji dodatno posjeduju još i neke vrste *anycast* adresa.

Anycast adrese su u prijevodu zajedničke adrese koriste se isključivo kao odredišne adrese, a također su dodijeljene i IPv6 usmjerivačima. Doseg zajedničkih adresa određen je dosegom odgovarajuće jednoodredišne adrese. Svaki usmjerivač unutar podmreže mora imati „najbližu" adresu koja je određena prefiksom podmreže za određeno mrežno sučelje. Zajednička adresa usmjerivača stvara se na način da se bitovi prefiksa fiksiraju, dok se ostali

bitovi postave u 0. Svim mrežnim sučeljima koji su spojeni na određenu podmrežu dodjeljuju se adrese koje se koriste u komunikaciji s jednim od usmjerivača udaljene podmreže [10].

Multicast adresiranje odnosno višeodredišno adresiranje funkcionira kao i kod IPv4 protokola. Čvorovi mogu osluškivati mrežni promet na jednoj ili više višeodredišnih adresa, mogu pristupiti višeodredišnoj grupi ili je napustiti. Ovakva se adresa ne smije koristiti kao izvorišna adresa. Ovakve adrese su jednostavne jer su prvih osam bita jedinice i zbog toga ih je jednostavno klasificirati.

Multikast adrese su:

- multikast (engl. *Multicast Address*),
- multikast adresa na zahtjev čvora (engl. *Solicited-Node Multicast Address*),

U odnosu na protokol IPv4, u IPv6 je jednostavnije pridjeliti adrese mrežnom sučelju. To se može postići korištenjem postupka autokonfiguracije adrese, pomoću kojeg računalo samostalno konfigurira parametre svog sučelja. Razlikuju se dvije vrste autokonfiguracije:

- *Stateless* autokonfiguracija - čvor koristi fizičku (engl. *Medium Access Control*, skraćeno MAC) adresu svoje mrežne kartice kao dio IPv6 adrese, i
- *Stateful* autokonfiguracija - čvor koristi protokol DHCP[11] (engl. *Dynamic Host Configuration Protocol*) verzije 6 te od DHCP-poslužitelja dobiva parametre potrebne za konfiguraciju svog mrežnog sučelja.

3.3. Usmjeravanje kod IPv6 protokola

Usmjeravanje kod IPv6 protokola je slično kao što je kod IPv4 protokola. Unos u tablice usmjeravanja nastaje ili ručno, kad ih upisuje sustavni administrator ili ih komunikacija s usmjerivačima dodaje automatski. Tablica usmjeravanja pohranjuje podatke o IPv6 mrežnim prefiksima i načinima dolazaka do njih (direktno ili indirektno) [7].

Prije korištenja tablice usmjeravanja provjerava se *cache*[12] odredišta, koji je poznat kao baza za prosljeđivanje informacija, zbog traženja potvrde o odredišnoj adresi.

[11] **DHCP** je mrežni protokol za dodjeljivanje IP adresa od strane mrežnih računala, olakšava konfiguraciju jer eliminira ručno dodjeljivanje postavki za računalnu mrežu.

Ako *cache* odredišta ne sadrži informacije o adresi, tablice usmjeravanja služe za određivanje adrese i sučelja sljedećeg čvora u mreži.

Adresa sljedećeg čvora u mreži predstavlja adresu odredišta u paketu kod direktnog dostavljanja ili adresu sljedećeg čvora (usmjerivača), kod indirektnog dostavljanja. Sučelje sljedećeg čvora u mreži identificira fizičko ili logičko sučelje koje se koristi za prosljeđivanje paketa do njegovog odredišta ili do sljedećeg usmjerivača.

Nakon što se odredi adresa i sučelje sljedećeg čvora, osvježava se *cache* odredišta. Sljedeći paketi koji se prosljeđuju u mreži za usmjeravanje koriste *cache* zapis odredišta, a ne tablicu usmjeravanja.

Zapisi u IPv6 tablicama usmjeravanja spremaju sljedeće tipove ruta:

- *Directly attached network routes,*
- *Remote network routes,*
- *Host routes* i
- *Default route* [11].

Directly attached network route je ruta za mrežne prefikse koji su direktno povezani i obično imaju 64 bitni prefiks.

Remote network route je ruta za mrežne prefikse koji nisu direktno povezani, no do njih se može doći preko ostalih usmjerivača.

Host route je ruta do određenih IPv6 adresa. Duljina prefiksa u ovom tipu rute je 128 bita.

Default route je ruta koja se koristi kada se ne može naći niti jedna od prethodno navedenih ruta. Duljina prefiksa kod *Default route* je 0.

Za određivanje svakog zapisa unutar tablice usmjeravanja, IPv6 uspoređuje bite u mrežnom prefiksu s istim bitovima odredišne IPv6 adrese. Ako svi bitovi u oba zapisa odgovaraju jedni drugima, ruta odgovara odredištu. Ako bitovi ne odgovaraju, stvara se popis odgovarajućih ruta. Odabire se ruta s najvećom duljinom prefiksa (to je ruta koja ima najveći broj bita s odredišnom IPv6 adresom). U tom slučaju ruta s najdužim zapisom je optimalna

[12] ***Cache*** se u računalnim mrežama naziva priručna memorija ili predmemorija koja služi za pohranu često upotrjebljivih podataka.

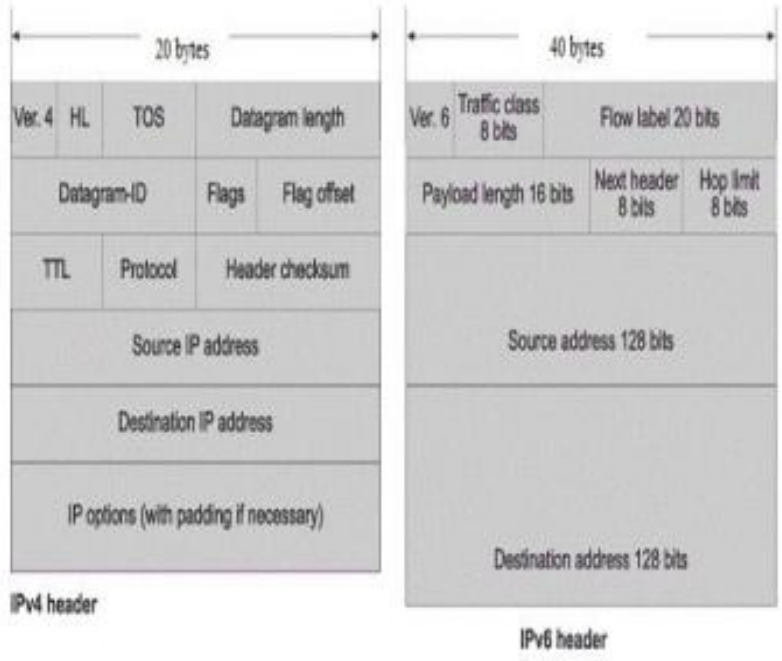
ruta do odredišta. Ako postoji više zapisa s najvećom duljinom prefiksa, za određivanje se odabire ruta s najmanjom metrikom (engl. *metric*), odnosno brojem skokova.

Krajnji rezultat u procesu određivanja rute predstavlja jedna ruta u tablici usmjeravanja. Određena ruta propušta adresu i sučelje sljedećeg uređaja u mreži. Ako proces određivanja rute ne uspije, IPv6 pretpostavlja kako je moguće doći do odredišta lokalno. Ako proces određivanja rute na usmjerivaču ne uspije IPv6 šalje pošiljatelju poruku o neuspjehu ICMPv6[13] (engl. *Destination Unreachable-No Route Found*) i odbacuje paket [12].

[13] **ICMPv6** je protokol koji se koristi za provjeru i otklanjanje poteškoća veze u komunikaciji između uređaja koji se koriste IPv6 protokolom.

4. USPOREDNA ANALIZA PROTOKOLA IPv4 I IPv6

Shvaćajući da je problem IP adresa samo vrh ledenog brijega, i da će ostali nedostaci proizašli iz ograničenja u dizajnu IPv4 tek početi uzimati svoj danak, IETF[14] (engl. *Internet Engineering Task Force)* je 1992. počeo prikupljati ideje za novi Internet Protokol, i 1995. je usvojen Internet protokol verzije 6 (IPv6) kao temelj budućeg razvoja Interneta [13].



Slika 7. Usporedba zaglavlja IPv4 i IPv6 [14]

Pri razvoju IPv6 i svih uz njega vezanih protokola IETF je smatrao ključnim zadržati i naglasiti sve dobre karakteristike IPv4, pogotovo što veću jednostavnost i otvorenost protokola, međutim striktnije definirati sučelja između različitih protokola koja će omogućiti optimalne performanse kako za krajnje korisnike, tako i za mrežnu infrastrukturu, pokušavajući na sve kompleksnije potrebe odgovoriti što jednostavnijim mehanizmima implementacije. Posebna pažnja posvećena je izradi različitih mehanizama tranzicije, kako bi se svim korisnicima što više olakšao prijelaz na novu verziju protokola, te kako bi se omogućio nesmetan "suživot" IPv4 i IPv6 na istoj mrežnoj infrastrukturi.

[14] **IETF** je međunarodna zajednica mrežnih dizajnera, operatora, dobavljača i istraživača koji se bave evolucijom internetske arhitekture i što boljim radom Interneta [23].

Tablica 1. Usporedba protokola IPv4 i IPv6

	IPv4	**IPv6**
Adresa	32-bitne adrese	128-bitne adrese
Maska adrese	Koristi se za označavanje mreže u host dijelu.	Ne koristi se.
Tipovi adresa	Unicast, multicast i broadcast adrese.	Unicast, multicast i anycast adrese.
Opcije IP zaglavlja	Opcije su raznolike i prate zaglavlje prije svakog prijenosa.	IPv6 zaglavlje nema opcija, ali ima dodatna proširenja zaglavlja.
Usmjeravanje	Paketi se prosljeđuju na temelju odredišne IP adrese. Tablica usmjeravanja se kreira po defaultu i administrator ih unosi ručno.	Usmjeravanje je slično kao i kod IPv4, ali kod ove verzije, tablica usmjeravanja nalazi se u svakom čvoru.
Format adrese	Decimalni: 192.168.1.0	Heksadecimalni: 3a00:ag90::1236

Izvor: prilagođeno prema [15]

Prema [15] bitne novosti koje donosi IPv6 mogu se sažeti u nekoliko osnovnih odrednica:

- **veći adresni prostor** - 32-bitne adrese zamjenjuju se 128-bitnim, što omogućuje praktički nepresušan broj adresa svakom zainteresiranom entitetu;
- **novi format zaglavlja** - IPv6 ima pojednostavljeno zaglavlje veličine samo 40 okteta, olakšavajući obradu paketa na čvorovima u mreži;

- **djelotvornije i slojevitije adresiranje i jednostavnije usmjeravanje** - Nove IP adrese dizajnirane su tako da podržavaju agregaciju podataka o usmjeravanju, i samim time je postignuto efikasnije i slojevitije usmjeravanje, uz znatno smanjenje veličine usmjerivačkih tablica;

- **mogućnost automatskog podešavanja mrežnih parametara na uređajima** - Osim do sada poznatih mehanizama podešavanja mrežnih postavki (statički, DHCP...), IPv6 donosi i novu metodu autokonfiguracije, specificirajući mehanizam kojim svaki uređaj može odrediti svoju lokalno vidljivu IP adresu, i od usmjerivača primiti informaciju o globalnim parametrima za usmjeravanje (javni prefiks i adresu izlaznog usmjerivača), čime se za ostvarivanje spojnosti na mrežu ne zahtijeva nikakva akcija niti od krajnjeg korisnika, niti od mrežnog administratora;

- **ugrađena podrška za sigurnost** - IPv6 ima ugrađenu podršku za sigurnosni protokol IPSec[15], čime je osigurana primjena standarda za sigurnost protoka paketa u mreži;

- **bolja podrška za osiguranje kvalitete usluge (QoS[16])** - nova polja u zaglavlju IPv6 paketa definiraju kako će se čvor ponašati prema paketu u ovisnosti o njegovom sadržaju. Ovisno o tipu prometa, usmjerivači mogu tretirati različite pakete na različit način (npr. dodjeljivati veći prioritet određenoj vrsti prometa), te osigurati zadovoljavajuću razinu usluge u okvirima mrežne infrastrukture;

- **otvoreniji poboljšanjima** - Za razliku od IPv4, IPv6 definira "osnovno" zaglavlje paketa, te omogućuje proizvoljan broj dodatnih opcionalnih polja koja prate fiksni dio zaglavlja. Na taj način vrlo je jednostavno implementirati bilo kakva proširenja protokola, kako na krajnjim točkama, tako i na usmjerivačima u IPv6 mreži.

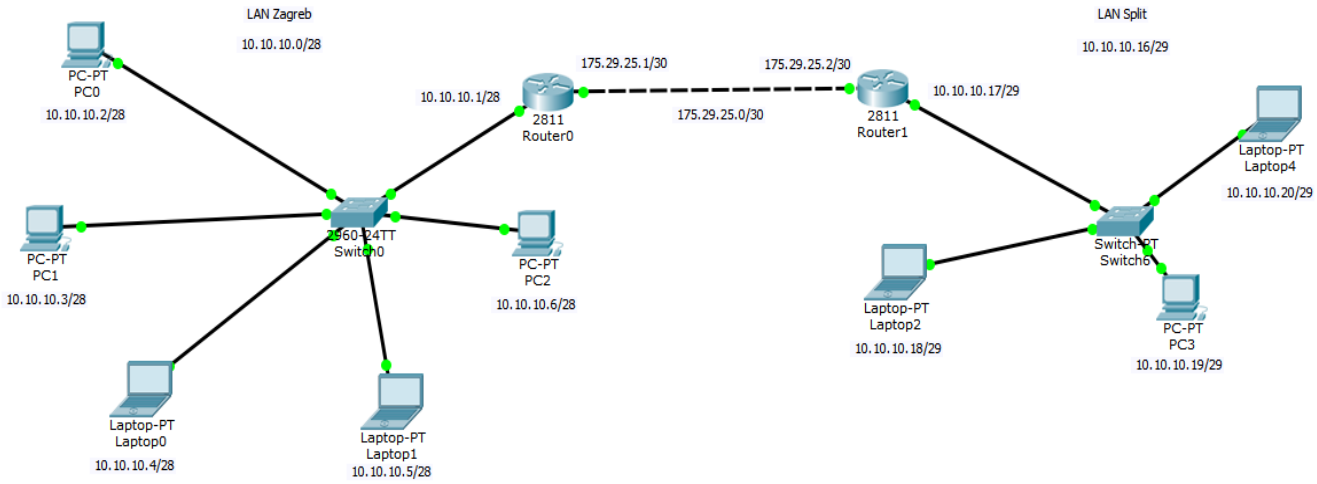
[15] **IPsec** (engl. *Internet Protocol Security*) je protokol koji pomaže pri osiguranju sigurne komunikacije putem Internet Protokola upotrebom kriptografskih sigurnosnih usluga.
[16] **QoS** (engl. *Quality of Service*) – opis i mjerenje kvalitete cjelokupne usluge u računalnim mrežama.

5. PRIKAZ PRIMJENE PROTOKOLA IPv4 I IPv6 PUTEM PROGRAMSKOG ALATA CISCO PACKET TRACER

Cisco Packet Tracer je programski alat koji omogućuje eksperimentiranje i prikazivanje simulacije, vizualizacije, procjene, te ponašanje računalnih mreža u različitim okruženjima. Nadopunjuje fizičku opremu stvaranjem mreža s neograničenim brojem uređaja pružajući praksu, otkrivanje i otklanjanje potencijalnih pogrešaka nastalih u „stvarnom okruženju“ dizajnirajući i demonstrirajući jednostavne i složene koncepte mrežnih sustava [16].

5.1. Prikaz računalne mreže primjenom IPv4 protokola

Putem programskog alata Cisco Packet Tracer-a na slici 8 prikazana je međusobna komunikacija između dviju mreža koje se služe IPv4 protokolom.

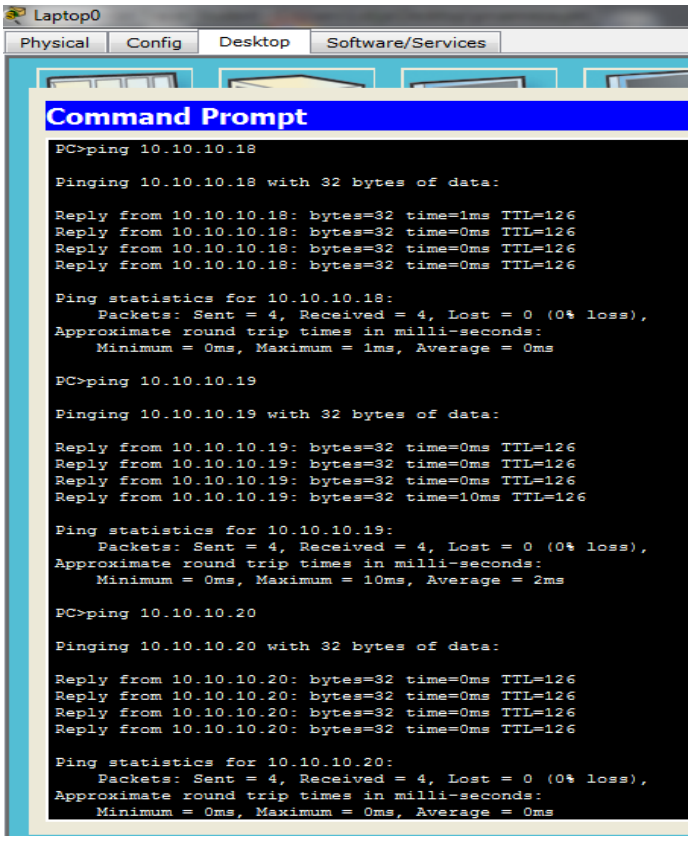


Slika 8. IPv4 mreža

Dvije LAN[17] (engl. *Local Area Network*) mreže koriste privatne adrese IPv4 protokola gdje su uređaji prvo spojeni na preklopnike[18] (engl. *switch)* modela 2960-24TT, a oni na

[17] **LAN** je mreža namijenjena je povezivanju računala i drugih uređaja na manjim udaljenostima poput ureda, kuće, zgrade i sl.
[18] **Preklopnik** je uređaj u mreži sa većim brojem mrežnih sučelja.

usmjernike (engl. *router)* 2811. Čvorovi su povezani WAN[19] (engl. *Wide Area Network*) mrežom putem javnih adresa. Adresa LAN mreže u Zagrebu je 10.10.10.0/28 (28 je oznaka mrežne maske, u ovom slučaju moguće je dotičnoj mreži pridružiti 14 korisnika), u mreži se nalazi 3 stolna računala i 2 prijenosna računala rasponom adresa 10.10.10.2-10.10.10.6/28. Svi uređaji zajedno predstavljaju zamišljeni ured tvrtke. WAN mreža označena je javnim adresama IPv4 protokola. Adresa same mreže je 175.29.25.0/30, a sučelja usmjernika iste mreže su 175.29.25.1/30 i 175.29.25.2/30. Druga LAN mreža također predstavlja ured zamišljene tvrtke sa sjedištem u Splitu. Adresa same mreže je 10.10.10.16/29, a uređaja u mreži u rasponu od 10.10.10.18-10.10.10.20/29.



Slika 9. Test mreže

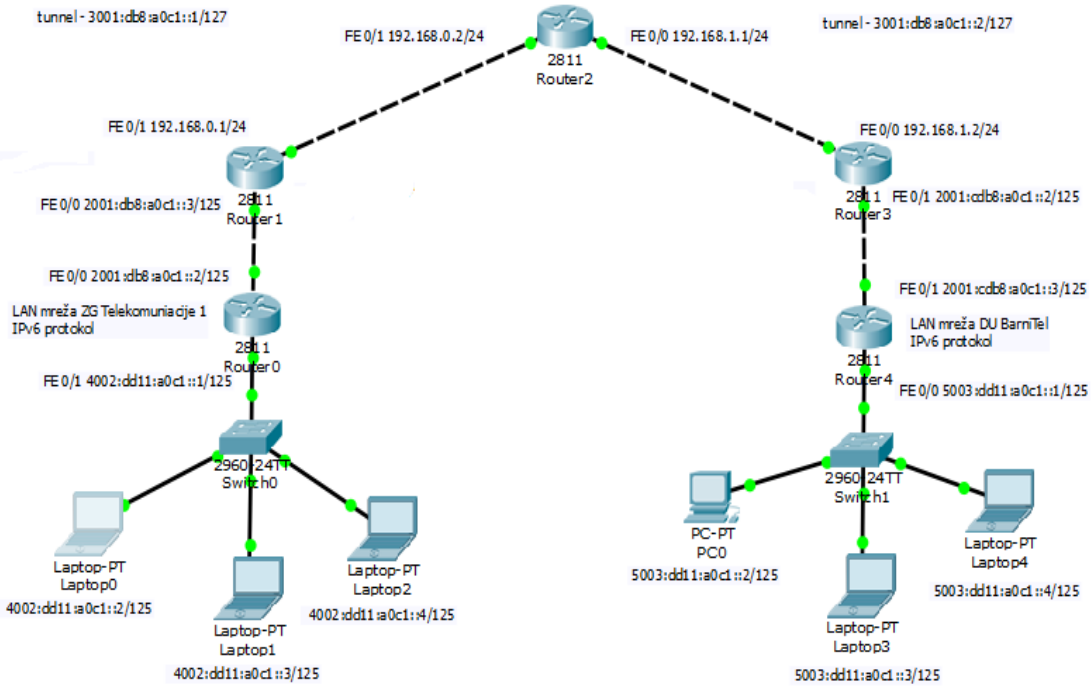
Na slici 9 prikazan je ping „test“ između uređaja u mreži. Ping-test je metoda za mjerenje minimalnog vremena potrebno za slanje najmanje moguće količine podataka i primanje odgovora na isti. Za ping-test se koriste milisekunde kao mjerne jedinice. U konkretnom ping-testu na slici poslana su 4 paketa sa uređaja iz prve LAN mreže koja se nalazi u Zagrebu na tri

[19] **WAN** je mreža koja pokriva veliku geografsku širinu kao na primjer Internet.

različita uređaja u LAN mrežu koja se nalazi u Splitu s time da paketi putuju WAN mrežom koja se nalazi između njih. Na slici je vidljivo da ni jedan od 4 paketa za vrijeme slanja u drugu mrežu na sva tri uređaja nije izgubljen.

5.2. Prikaz računalne mreže primjenom IPv4 i IPv6 protokola

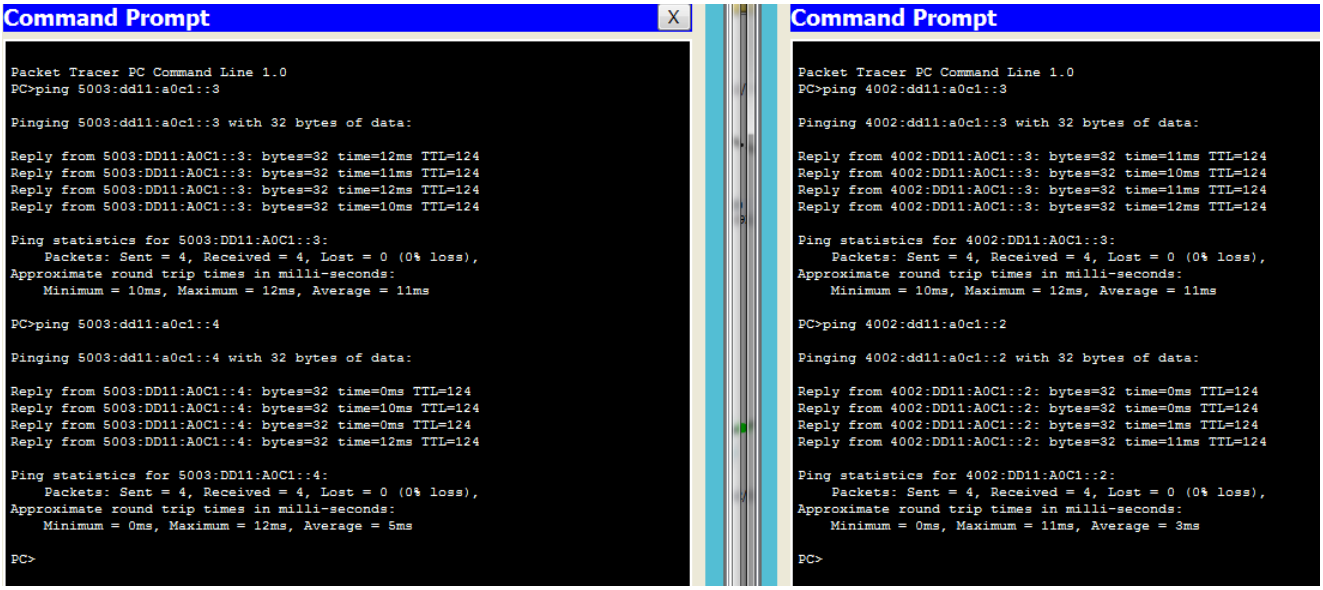
Slikom 10 prikazane su dvije zamišljene tvrtke koje razmjenjuju podatke. Te su im dodijeljene adrese IPv6 protokola.



Slika 10. IPv6 mreže putem IPv4 protokola

Na lijevoj strani je fiktivna tvrtka pod nazivom „Telekomunikacije 1“ u Zagrebu, a na desnoj „BarniTel“ u Dubrovniku. Uređajima u „Telekomunikacije 1“ mreži dodijeljene su adrese u rasponu 4002:DD11:A0C1::2/125 - 4002:DD11:A0C1::4/125, dok su za mrežu „BarniTel“ 5003:DD11:A0C1::2/125 - 5003:DD11:A0C1::4/125. Krajnje mreže koriste stolna i prijenosna računala spojena na preklopnike (engl. *switch*) 2960-24TT. U slučaju na slici komunikacija između IPv6 čvorova izvedena je putem „tunela“ u kojem su čvorovi povezani IPv4 usmjernikom. Za usmjernike u čvorovima (engl. *router)* su uzeti modeli 2811 kojima

sučelja imaju izlazne portove FastEthernet. Tunel kojim prolaze IPv6 datagrami oglašen je adresama 3001:DB8:A0C1::1/127 i 3001:DB8:A0C1::2/127. Na graničnim usmjernicima gdje se nalazi tunel između IPv6 mreža upotrijebljeni su OSPF[20] (engl. *Open Shortest Path First*) protokol u koje je potrebno unijeti pune adrese čvorišta kako bi tijekom prijenosa usmjernik mogao „prepoznati“ od kuda dolazi i kamo je paket poslan i RIP[21] 6bone protokol (engl. *Routing Information Protokol*). Da bi prijenos IPv6 paketa kroz tunel mogao prolaziti bez prepreka u graničnim usmjernicima navedene su izvorišne ili odredišne adrese i izlazna sučelja, ovisno u kojem se graničnom prijelazu događa promjena.



Slika 11. Test mreža

Putem slike 11 prikazan je protok podataka između mreža kojima su dodijeljene IPv6 adrese, dok sami podaci putuju čvorovima koji sadrže i adrese IPv4 protokola. S izvora, odnosno mreže u Zagrebu poslana su četiri paketa s jedne adrese prema odredištu u Dubrovniku. Prema priloženom se vidi da ni jedan paket prema tri različite adrese na odredištu nije izgubljen, iako su u mrežu uključeni IPv4 i IPv6 protokol.

[20] **OSPF** je usmjerivački protokol u IP mrežama koji djeluje unutar jednog autonomnog sustava. Prikuplja podatke o stanju veze s raspoloživim usmjerivačima i konstruira topologiju mreže [19].
[21] **RIP** je protokol koji usmjerava pakete na temelju vektora udaljenosti te sprječava petlje primjenom ograničenja broja skokova paketa u mreži [24].

6. BUDUĆI RAZVOJ PROTOKOLA IPvX

Shvaćajući da je problem IP adresa samo vrh ledenog brijega, i da će ostali nedostaci proizašli iz ograničenja u dizajnu IPv4 tek početi uzimati svoj danak, IETF (engl. *Internet Engineering Task Force)* je 1992. počeo prikupljati ideje za novi Internet protokol, i 1995. je usvojen Internet protokol verzije 6 (IPv6) kao temelj budućeg razvoja Interneta [13].

Već početkom '90-ih godina prošlog stoljeća bilo je jasno da će se postojeći fond IP adresa iscrpiti u skoroj budućnosti, prvenstveno zato jer je vrlo neravnomjerno raspodijeljen u četiri klase, čime se uvijek dodjeljuje puno više adresa nekoj mreži nego što je potrebno. Osim toga, maksimalni broj adresa u idealnom slučaju je 4.3 milijarde, što je već tada bilo manje od ukupne populacije svijeta. Ponukani time i novim zahtjevima od Internet-a, prvenstveno mobilnošću i kontrolom hitnosti paketa, u zimu 1992. su se pojavila četiri različita prijedloga za novi protokol:

- "CNAT" (engl. *Comprehensive Network Address Translator*),
- "IP Encaps",
- "Nimrod", i
- "Simple CLNP".

Do prosinca 1992. pojavili su se još 3 prijedloga:

- "The P Internet Protocol" (PIP),
- "The Simple Internet Protocol" (SIP) i
- "TP/IX (engl. *The next Internet*)".

Tokom 1993. stapanjem i odabirom stvorila su se dva konačna prijedloga:

- "Simple Internet Protocol Plus" (SIPP) i
- "Common Architecture for the Internet" (CATNIP).

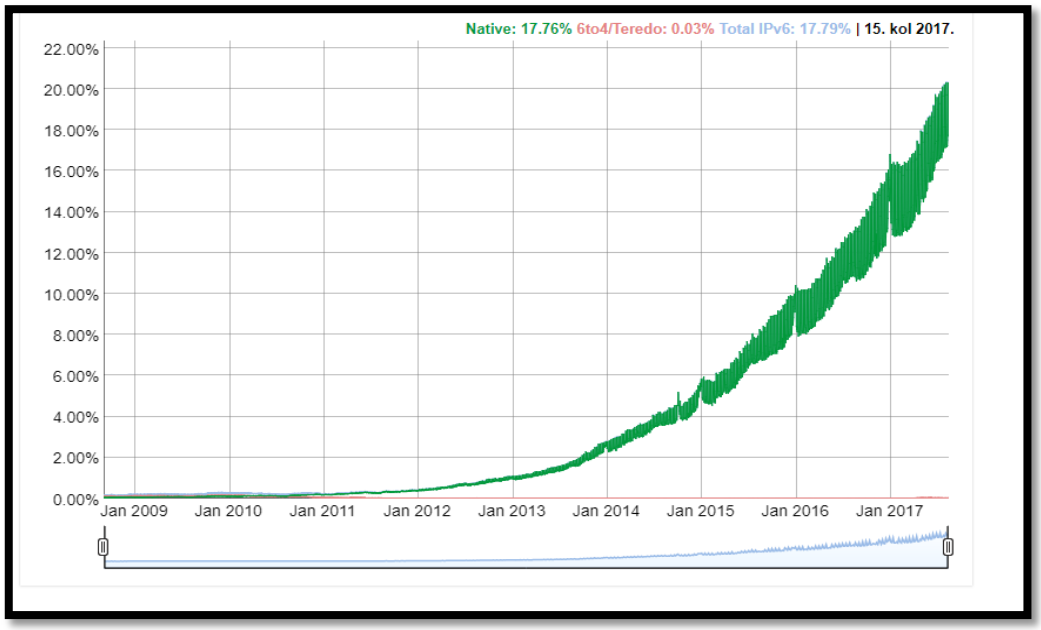
Na sastanku IETF-a (engl. *Internet Engineering Task Force*) u Torontu 25. 7. 1994. voditelji razvoja IPv6 su iznijeli prijedlog novog protokola, koji je između ostalog sadržavao:

- SIPP sa 128-bitnim adresama će biti osnova novog protokola,
- zadržat će se politika dodjele adresa, i neće biti pokušaja preraspodjele starih adresa,

- određene su nove smjernice razvoja sigurnosti i privatnosti korisnika (enkripcija, posebno zaglavlje za privatnost, Firewall...),
- načini upotrebe starih 32-bitnih adresa u novom protokolu, i upotreba starih usmjerivača sa novim adresama te
- prijelaz sa stare verzije protokola na novu mora biti posve neprimjetan krajnjem korisniku, i mora postojati mogućnost zajedničkog postojanja stare i nove verzije.

Mehanizmi prelaska na novu verziju protokola su smišljeni tako da u svakom trenutku mogu zajedno postojati obadvije verzije, te je predloženo da se prvo promijene usmjerivači (routeri) na novu verziju, a zatim postepeno i cijela lokalna mreža. Time bi krajnjem korisniku prelazak bio posve neprimjetan. Sve stare IPv4 adrese bi se nastavile koristiti na već opisan način.

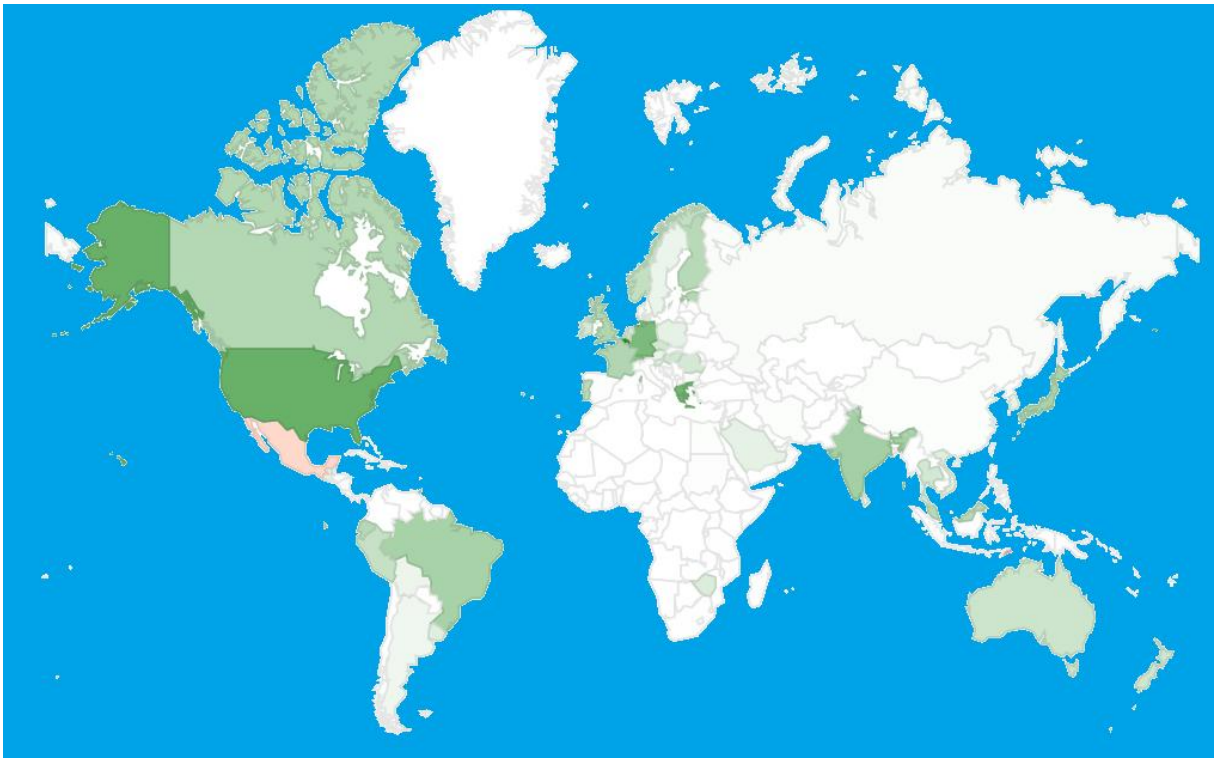
IPv6 je napravljen tako da zamijeni stari protokol bezbolno i bez pritisaka na bilo koga, ali u isto vrijeme s razumnom pretpostavkom da će zbog nedostatka adresa svi morati prijeći na njega prije ili kasnije. Sam protokol je osmišljen tako da buduće promjene budu što lakše, ali i da osigura barem deset godina prije ponovne promjene protokola.



Slika 12. Prikaz upotrebe IPv6 protokola [17]

Slikom 12 prikazana je statistika upotrebe IPv6 protokola od siječnja 2009. godine do kolovoza 2017. godine. Napravljena je od strane Google kompanije na temelju prikupljanja podataka Google korisnik koji se koriste IPv6 protokolom. Iako je protokol IPv6 usvojen

davne 1995. godine, statistika prikazuje i dalje vrlo malu upotrebu istog. U siječnju 2009. godine ukupno korištenje u svijetu iznosilo je samo 0,18 %, dok se do danas nakon 22 godine upotreba povećala, ali je i dalje vrlo malo i to od samo 18 % u cijelom svijetu.



Slika 13. Prikaz upotrebe IPv6 protokola u svijetu [17]

Na slici 9 tamno zelenom bojom prikazane su države u svijetu gdje se najviše koristi IPv6 protokol. Belgija je država koja ga je u najvećoj mjeri prihvatila sa 54 %, sljedeće su Sjedinjene Američke Države sa 36 %, Grčka 33 % i ostale. Svijetlo zelena boja označava upotrebu do 20 %, narančasta do 10 %, a bijele ispod 10 % ili ga uopće ne koriste.

6.1. Prijelaz s verzije 4 na verziju 6

Kako bi se omogućio prijelaz, najprije je potrebno omogućiti pružateljima internetskih usluga korištenje protokola verzije 6 te zatim postepeno raditi na prijelazu krajnjih korisnika. Prijelaz je moguće izvršiti na više načina. Prvi je određivanje fiksnog dana prestanka korištenja IPv4 protokola. Iako ovaj način ima smisla, u praksi je neizvediv obzirom da dio infrastrukture i dalje ne podržava IPv6. Sljedeći pristup je uporaba uređaja koji podržavaju

oba standarda. To je znatno prihvatljiviji pristup iako i on ima svojih nedostataka. Uređaji koji šalju pakete ne mogu znati je li na cijelom putu podržan IPv6, čime bi se nailaskom na IPv4 usmjernike podaci izgubili. Kako bi se doskočilo ovom problemu koriste se oba protokola, s time da se paketi prilikom napuštanja IPv6 domene, inkapsuliraju u IPv4 pakete te im se na povratku u IPv6 domenu, uklanja IPv4 zaglavlje [18].

Nakon prijelaza na verziju 6 treba ostaviti mogućnost korištenja "starog" protokola kako korisnici koji ga budu i dalje koristili ne bi bili uskraćeni za mogućnost korištenja Interneta.

6.2. Metoda prijenosa 6to4

Ova metoda omogućava prijenos IPv6 paketa preko IPv4 mreža bez konfiguracije određenih tunela. Koriste se javne IPv4 adrese pomoću kojih se stvaraju jedinstvene IPv6 adrese uređaja. Paketima se pridružuje generirana adresa te se takav IPv6 paket inkapsulira u IPv4 paket s tipom protokola.

Sve 6to4 adrese započinju s 2002::/16. Na to se nadodaje IPv4 adresa uređaja zapisana u heksadecimalnom formatu koja tvori /48 adresu. Kako su autokonfigurirane IPv6 adrese uvijek /64, do nadopune prefiksa ostaje još 16 bitova. U tom se slučaju nadodaje proizvoljna vrijednost ili jednostavno ::1. Ostatak od 64 bita je identifikator sučelja, odnosno EUI-64 adresa [18].

Kako bi ova metoda funkcionirala, potrebno je da usmjernik koji povezuje lokalnu mrežu na javnu podržava 6to4 adrese. Važno je i da usmjernik bude konfiguriran na način da njegov server za translataciju adresa propušta pakete s tipom protokola 41.

Prilikom komunikacije dva IPv6 otoka konfigurirana s 6to4 adresama preko IPv4 infrastrukture, pošiljatelj IPv6 pakete inkapsulira u IPv4 i kao takve šalje na javnu adresu odredišnog IPv6 otoka konfiguriranog s 6to4 adresom.

Odredišni usmjernik skida IPv4 omot te mu ostaje IPv6 paket koji šalje do odredišnog klijenta. Ukoliko se paket šalje na klijenta s globalno jedinstvenom IPv6 adresom, paket se na krajnjem usmjerniku konfiguriranim s 6to4 adresom, inkapsulira u IPv4 paket i šalje na rezerviranu adresu 192.88.99.1. Ta adresa predstavlja ulaz paketa s 6to4 adresama na "IPv6

Internet". Tu se uklanja IPv4 zaglavlje i paket se dalje usmjerava kao pravi IPv6 paket. Prilikom odgovora, odnosno povratka paketa na IPv4 Internet, koristi se princip komunikacije kao kod dva usmjernika konfigurirana s 6to4 adresama [18].

6.3. Metoda prijenosa Teredo

Ova vrsta tuneliranja prenosi IPv6 paket preko IPv4 mreže, ali razlikuje se od prethodno opisane metode u tome što ne zahtjeva da IPv4 adresa bude javna.

Metodom prijenosa Teredo omogućeno je korištenje i iza uređaja za translataciju adresa u lokalnim mrežama koji nisu posebno konfigurirani. Radi na principu inkapsuliranja IPv6 paketa u UDP pakete, koji mogu biti usmjeravani kroz uređaj za translataciju adresa i dalje na Internet.

Teredo tuneliranje uključuje sljedeće uređaje [19]:

- Teredo klijent – IPv4/IPv6 uređaji koji imaju adaptere i komuniciraju s drugim klijentima ili IPv6 mrežama preko Teredo štafetnih uređaja. Oni se u pravilu nalaze iza uređaja za translataciju adresa.
- Teredo server – server povezan na IPv4 i na IPv6 mrežu. Služi za konfiguraciju Teredo klijenata i inicijalizaciju prijenosa paketa u slučaju kada se klijenti nalaze iza ograničenog uređaja za translataciju adresa.
- Teredo štafetni uređaj – server povezan na IPv4 i na IPv6 mrežu. Povezuje Teredo klijente s IPv6 mrežama.

Prilikom generiranja IPv6 adresa za Teredo klijente, šalje se zahtjev za adresom prema Teredo serveru koji vraća potrebne parametre. Adresa se generira na slijedeći način [19]:

1. Teredo prefiks 2001 (32 bita)
2. IPv4 adresa Teredo servera u heksadecimalnom zapisu (32 bita)
3. Zastavice – sadrži oznaku vrste uređaja za translataciju adresa (16 bita)
4. Broj vanjskog UDP porta koji je pridružen od uređaja za translataciju adresa, a nad kojim je izvršena operacija ekskluzivno ili s heksadecimalnom vrijednošću FFFF (16 bita)

5. Vanjska IPv4 adresa uređaja za translataciju adresa nad kojom je izvršena operacija ekskluzivno ili s heksadecimalnom vrijednošću FFFF (16 bita)

Nakon što klijent iz dobivenih podataka generira IPv6 adresu, može započeti komunikaciju s ostalim Teredo klijentima i IPv6 mrežama. Ovisno o vrsti uređaja za translataciju adresa, povezivanje potpomaže Teredo server, a kada je veza uspostavljena klijenti mogu samostalno komunicirati. Time se smanjuje opterećenje servera i ubrzava komunikacija [19].

7. ZAKLJUČAK

U završnom radu razmotrene su osnovne značajke IPv4 i IPv6 protokola, te je napravljena usporedba verzija ova dva protokola. Iako se IPv4 pokazao iznimno dobrim i skalabilnim, razvoj tehnologije i drugih protokola koji u vrijeme stvaranja IPv4 protokola nisu postojali, njegovu je nadogradnju učinio nezaobilaznom. Upravo zbog toga uporaba IPv6 protokola raste svakim danom sve više, tako postotak istog trenutno u svijetu iznosi niskih 18 %, a u Hrvatskoj vrlo malo od samo 0,4 %.

Oblikovanje IPv6 zasnovano je na rješavanju nedostataka koji su tijekom godina primijećeni u radu IPv4 protokola. Unatoč tome, IPv6 donosi i određen broj novih funkcionalnosti. Jedna od njih je ugrađena podrška za osnovne elemente sigurnosne zaštite.

U završnom radu kroz poglavlje 5 napravljena je simulacija dviju mreža. Prva mreža koja je danas najviše u upotrebi pomoću Internet Protokola verzije 4, te druga gdje obje verzije Internet Protokola 4 i 6 funkcioniraju zajedno pomoću metode tuneliranja. Za prijelazno razdoblje IPv4 na IPv6 protokol moglo bi se reći da iako nije toliko jednostavno i lako, nije ni nemoguće i neophodno je.

IPv6 rješava mnoge nedostatke IPv4, kao što je broj raspoloživih adresa, dodjela adrese, njezin životni vijek, opseg i tip adrese, brzina, jednostavnost konfiguracije, mobilnost, sustav imena domene, odlomci, sučelje, IP zaglavlje, prosljeđivanje i filtriranje paketa, privatne i javne adrese, pokretanje i zaustavljanje te još mnogo važnih čimbenika.

Jednom kada se prijeđe sa starije verzije temeljnog internetskog protokola IP, tj. IPv4 na noviju verziju protokola IPv6, pitanje sigurnosti, bolje pohrane podataka i njihovog bržeg procesiranja bit će uklonjena.

Na kraju, uzimajući u obzir sve prednosti opisanog IPv6 i nedostatke zastarjelog IPv4 protokola, lako je predvidjeti njihovu buduću zamjenu na mjestu najzastupljenijeg protokola globalne računalne mreže Interneta.

LITERATURA

[1] Mrvelj, Š.: *Promet u Internet mreži*, autorizirano predavanje, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2009.

[2] Kavran, Z., Grgurević, I.: *Mrežni sloj*, autorizirano predavanje, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2015.

[3] URL: http://mreze.layer-x.com/s030101-0.html (lipanj 2017.)

[4] URL: https://www.carnet.hr/tematski/ipv6/zaglavlja.html (lipanj 2017.)

[5] URL: http://www.utilizewindows.com/the-difference-between-unicast-multicast-and broadcast-messages/ (lipanj 2017.)

[6] URL: http://www.hitechmv.com/ipv4-*unicast*-*broadcast*-and-*multicast*/ (lipanj 2017.)

[7] URL: https://www.ibm.com/support/knowledgecenter/hr/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm#rzai2compipv4ipv6__compsocketapi (srpanj 2017.)

[8] URL: http://www.vtsnis.edu.rs/specijalisticke_studije/3_kot/predmeti/sirokopojasne%20pristupne_mreze/predavanja/4_MREZNI_SLOJ.pdf (srpanj 2017.)

[9] URL: http://searchenterprisewan.techtarget.com/definition/IPv6 (srpanj 2017.)

[10] URL: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf (srpanj 2017.)

[11] URL: https://technet.microsoft.com/enus/library/dd379495%28v=ws.10%29.aspx (srpanj 2017.)

[12] URL: https://technet.microsoft.com/enus/library/cc781672(v=ws.10).aspx#w2k3tr_ipv6_how_cvln (srpanj 2017.)

[13] URL: http://tvolaric.com/preuzimanja/IPv4vsIPv6.pdf (srpanj 2017.)

[14] URL: Govil, Jivika, et al. "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms." *Southeastcon, 2008.*, IEEE, 2008.

[15]URL:https://www.hakom.hr/UserDocsImages/2017/komunikacijske_mreze_i_usluge/PuB godisnje%20-%20izvjesce-2016.pdf (srpanj 2017.)

[16] URL: http://www.filehorse.com/download-cisco-packet-tracer-32/ (kolovoz 2017.)

[17] URL: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6adoption&tab=ipv6-adoption (kolovoz 2017.)

[18] URL: Bažant, Alen; et al: Osnove arhitekture mreža, Element, Zagreb, 2004.

[19] URL: https://bib.irb.hr/datoteka/619013.Implementacija-IPv6-na-OSPF-usmjerniki-protokol.pdf (srpanj 2017.)

[20] URL: https://www.techopedia.com/definition/6766/datagram (kolovoz 2017.)

[21] URL: http://searchnetworking.techtarget.com/definition/ICMP (kolovoz 2017.)

[22] URL: https://serverfault.com/questions/118324/what-is-a-link-local-address (kolovoz 2017.)

[23] URL: https://www.ietf.org/ (kolovoz 2017.)

[24] URL: http://searchnetworking.techtarget.com/definition/Routing-Information-Protocol (kolovoz 2017.)

POPIS KRATICA I AKRONIMA

CNAT	(engl. *Comprehensive Network Address Translator*) sveobuhvatan prevoditelj mrežnih adresa
DHCP	(engl. *Dynamic Host Configuration Protocol*) konfiguracijsko dinamički protokol korisnika
DSCP	(engl. *Differentiated Service Code Point*) različita točka kvalitete usluge
ECN	(engl. *Explicit Congestion Notification*) eksplicitna obavijest zagušenja
ICANN	(engl. *Internet Corporation for Assigned Names and Numbers*) Internet korporacija za dodjeljivanje imena i broja
ICPM	(engl. *Destination Unreachable-Host Unreachable*) Internet kontrolni protokol poruka
ICPMv6	(engl. *Destination Unreachable-No Route Found*) Internet kontrolni protokol poruka
IETF	(engl. *Internet Engineering Task Force)* organizacija za razvoj i promoviranje Internetskih standarda i protokola
IHL	(engl. *Internet Header Length*) duljina Internet zaglavlja
IPv4	(engl. *Internet Protocol version 4*) internet protokol verzije 4
IPv6	(engl. *Internet Protocol version 6*) internet protokol verzije 6
LAN	(engl. *Local Area Network*) lokalna računalna mreža
OSI	(engl. *Open Systems Interconnection model*) model za međusobno povezivanje otvorenih sustava
OSPF	(engl. *Open Shortest Path First*) otvaranje prvo najkraćih staza
QoS	(engl. *Quality of Service*) kvaliteta usluge

RIP	(engl. *Routing Information Protokol*) usmjerivački protokol
TCP	(engl. *Transsmision Control Protocol*) kontrolni protokol prijenosa podataka
TCP/IP	(engl. *Transsmision Control Protocol / Internet Protocol*) kontrolni protokol prijenosa podataka Internet protokola
TOS	(engl. *Type of Service*) vrsta usluge
TTL	(engl. *Time to Live*) vrijeme života
UDP	(engl. *User Datagram Protocol*) datagram protokol korisnika
WAN	(engl. *Wide Area Network*) mreža širokog područja

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih
znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Planiranje migracije s protokola IPv4 na IPv6**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 1. 9. 2017.

Student/ica:

Lidija Belužić

(potpis)