Implementacija IPV6 protokola na primjeru Istarskog veleučilišta

Brnelić, Tristan

ZAVRŠNI RAD

PRIJELAZ SA IPv4 NA IPv6 PROTOKOL NA PRIMJERU „ISTARSKOG VELEUČILIŠTA“

Tristan Brnelić

Pula,rujan 2019

ZAVRŠNI RAD

PRIJELAZ SA IPv4 NA IPv6 PROTOKOL NA PRIMJERU „ISTARSKOG VELEUČILIŠTA“

Kolegij: Računalne mreže

Student: Tristan Brnelić

Mentor: pred. Kristijan Matas

Pula, rujan 2019

Izjava o samostalnosti izrade završnog rada

Izjavljujem da sam završni rad na temu „ IP Adresa“ samostalno izradio uz pomoć mentora Kristijana Matasa , koristeći navedenu stručnu literaturu i znanje stečeno tijekom studiranja. Završni rad je pisan u duhu hrvatskog jezika.

Student: Tristan Brnelić

Potpis: _____

ZAHVALA :

Zahvaljujem se mentoru Kristijanu Matasu v. predavaču na strpljenju,razumjevanju, pomoći i vodstvu u izradi ovog rada. Također želio bi se zahvaliti profesorima Politehnike Pula od kojih sam stekao puno znanja te kolegama i prijateljima koji su učinili da moj studij prođe zanimljiv i pun avantura. Veliko hvala mojim roditeljima koji su me kroz sve godine studija bodrili, bili uz mene i trudili se omogućiti mi da završim studij.

SADRŽAJ

Stranica

Popis tablica i oznaka

KRATICA	OPIS
IP	Internet protocol
IHL	Internet Header Length
TOS	Type of Service
QoS	Quality of Service
DSCP	Differentiated Service Code Point
ECN	Explicit Congestion Notification
TTL	Time to Live
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
ICANN	Internet Corporation for Assigneg Names and Numbers
RIPE NCC	RIPE Network Cordination Centere
ARIN	American Registry for Internet Numbers
LACNIC	Latin America and Caribbean Network Information Centere
AfriNIC	African Network Information Centere
APNIC	Asian-Pacific Netvork Information Centere
ISP	Internet service provider
RIR	Regionalni Internetski Registar
DHCP	Dynamic Host Protokol konfiguracije
IETF	Internet Engineering Task Force
NAT	Network Address Translation
PAT	Port Adress Translation
ESP	Encapsulating Security Payload
MAC	Medium Access Control
IV	Istarsko Veleučilište

Sažetak

U ovom radu biti će riječ o trenutno aktualnoj verziji internetskog protokola IPv4 i o novijoj IPv6. Detaljno će se opisat jedan i drugi protokol od samog načina kako funkcioniraju, od čega se sve sastoje te do načina njihove implementacije u mrežu. Nadalje, pobliže će biti objašnjene 3 najpoznatije metode koje omogućuju komunikaciju IPv4 i IPv6 protokola (dual-stack metoda,metoda tuneliranje i tranzicijska metoda). Svaka od prethodno navedenih metoda je jedinstvena prema svojem načinu funkcioniranja i komuniciranja. U današnje vrijeme s obzirom na sve veći broj uređaja koji se spajaju na Internet javila se potreba za prelaskom na noviju IPv6 verziju protokola stoga će u ovom radu bit postavljena usporedba između IPv4 i IPv6 protokola kako bi se direktno moglo vidjeti što to novija IPv6 nudi više od prijašnje IPv4.

Abstract

This labor will be about the old version of IPv4 and the newer IPv6. Both protocols will be described in detail from the way they work, what they all consist of and how they are implemented into the network. Furthermore, the 3 most famous methods that allow the communication of IPv4 and IPv6 protocols (dual-stack method, tunneling method and transition method) will be explained in more details . Each of the above methods is unique in its way of functioning and communication. Today, there is a need to upgrade to a newer IPv6 version of the protocol, so this labor will compare the IPv4 and IPv6 protocols to see directly what the newer IPv6 offers more than the previous IPv4.

1. UVOD

1.1 Opis i definicija problema

S obzirom na brzo rastući broj korisnika interneta i još brži razvoj tehnologije te uređaja koji se povezuju na internet, javlja se problem adresiranja uređaja na mreži. Dosadašnje potrebe su uspjele bit pokrivene, no broj slobodnih adresa na mreži polako se iscrpio. Usprkos raznim metodama koje su trenutno koriste da se taj problem prevlada, tendencija je da problem riješi dugoročno prelaskom sa IPv4 protokola na IPv6 koji nudi mnoga poboljšanja te ujedno i rješenje za problem nedostatka IPv4 adresa na mreži.

1.2 Cilj i svrha rada

Cilj i svrha ovog rada su dati osnovne informacije o migraciji sa IPv4 protokola na IPv6. Uz to obrađene je struktura IP adresa , tko upravlja IP adresnim prostorom, koje vrste IP adresa postoje te osnove IP protokola. Također pobliže su prikazane i uspoređene trenutno aktualna verzija IPv4 protokola te nova verzija IPv6, u kojem smjeru se razvija te koje su ključne razlike između ta dvaju protokola i na koje se načine ostvaruje komunikacija pomoću njih.

1.3 Polazna hipoteza

Prijelaz i razvoj sa IPv4 na IPv6 protokol je nužan za daljnje napredovanje internetskog sustava i zadovoljstva svih korisnika interneta te su metode prelaska lako mogu implementirani uz postojeću infrastrukturu.

1.4 Metode rada

Pri izradi pisanog dijela završnog rada korištene su sljedeće znanstveno-istraživačke metode:

- metoda analize
- metoda sinteze
- metoda deskripcije
- metoda indukcije
- metoda dedukcije

1.5 Struktura rada

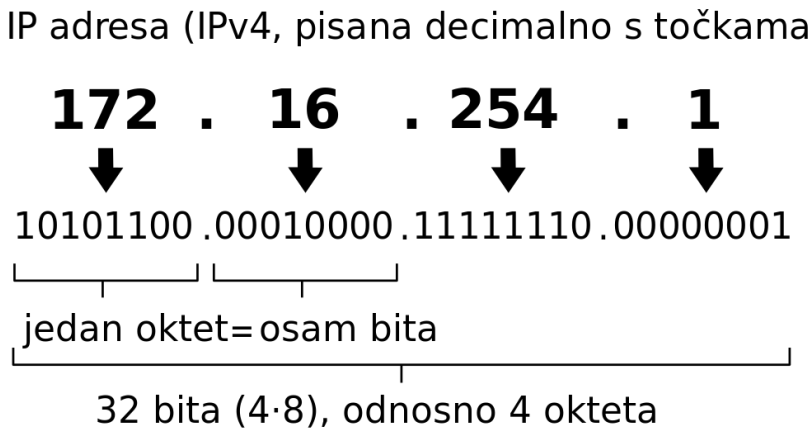
Ovaj rad sastoji se od ukupno sedam poglavlja koji su poredani redoslijedom kako bi čitatelj mogao dobiti i razumjeti sve potrebne informacije za razumijevanje problematike. Prvo poglavlje ovoga rada čini uvod u samu problematiku te se ono sastoji od definicije problema, cilja i svrhe rada, polazne hipoteze i metoda koje će biti korištene prilikom pisanja ovoga rada. U drugom poglavlju opisana je verzija četiri internet protokola što uključuje njezin izgled u binarnom zapisu, njezina obilježja, izgled hijerarhijske strukture protoka internetskih brojeva. Treće poglavlje ovoga rada razrađuje problematiku IPv4 protokola koji je već godinama dio internetske mreže te se u tom poglavlju navode postojeći problemi te se kroz primjer NAT metode dobiva mogućnost da se prethodno navedeni problemi riješe. Nadalje, četvrto poglavlje bavi se analizom nove verzije šest protokola i njezinih karakteristika. Sljedeće poglavlje ovoga rada uspoređuje IPv4 i IPv6 protokole. Činjenica je da iz tih protokola, točnije usporedbe tih protokola jasno možemo isčitati sve prednosti i mane prelaska na noviju verziju protokola. U posljednjem poglavlju prikazane su tri metode implementacije odnosno sama mogućnost korištenja oba protokola. Također, analizirati će se način paralelnog funkcioniranja protokola na mreži. Na kraju svega prethodno navedenog slijedi zaključak u kojim će se hipoteza potvrditi ili opovrgnuti.

2. KARAKTERISTIKE IPv4 PROTOKOLA

IP adresa (Internet Protocol) je jedinstveni identifikator, brojčani zapis računala ili nekog drugog uređaja koji je priključen na internetsku mrežu. Osnovni oblik IP adrese čini zapis u binarnom sustavu (0 i 1) koji se sastoji od četiri skupine po osam bita što čini ukupno zapis od 32 bita.

Radi lakšeg pamćenja, IP adrese se zapisuju u dekadskom obliku u kojem se 32-bitni broj podijeli na četiri 8-bitna broja, koji se zatim prikazuju kao četiri decimalna broja odvojena točkom kao što je prikazano na slici 1. Svaki od tih brojeva je u rasponu 0-255 što je upravo raspon brojeva koji se mogu prikazati u jednom 8-bitnom binarnom prikazu.

Slika 1.prikazuje zapis IP adrese u binarnom i dekadskom obliku

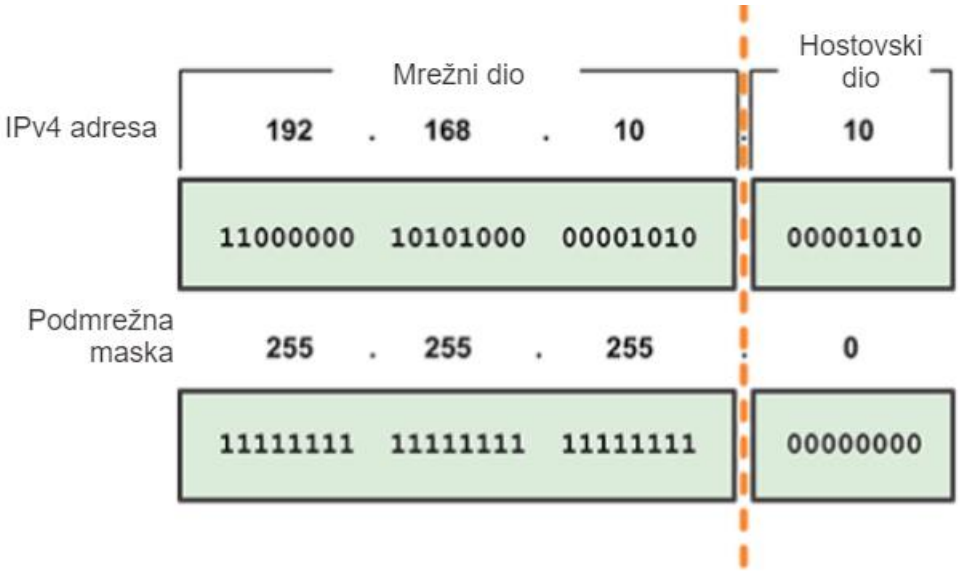


Izvor: https://www.google.com (8.5.2019)

Svakoj IP adresi dodjeljuje se podmrežna maska koja kada se koristi zajedno uz IP adresu, definira veličinu logičke podmreže. Takav sustav predstavlja fundamentalnu arhitekturu Internet mreže i omogućava podjelu u podmreže što u konačnici omogućava usmjeravanje podataka od mreže do mreže. Podmrežna maska također je duga 32 bita te označuje koji dio IP adrese je mrežni, a koji host dio (uređaj). Jedinice u maski podmreže predstavljaju mrežni dio dok nule čine dio koji se odnosi na host.

Maska podmreže tvori se stavljanjem binarne znamenke 1 na svako mjesto bita koje predstavlja mrežni dio i binarne znamenke 0 na svako mjesto bita koje predstavlja dio koji se odnosi na host. Maska podmreže zapravo ne sadrži dijelove IPv4 adrese za mrežu ili host već samo računalu govori gdje u zadanoj IPv4 adresi treba tražiti te dijelove.

Slika 2. Prikazuje podjelu IP adrese i podmrežne maske na mrežni dio i hostovski dio



Izvor: http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.1.2.1 (8.5.2019)

Slično kao IPv4 adrese, maska podmreže prikazana je u obliku dekadskog zapisa s točkama, radi lakše uporabe. Maska podmreže konfigurira se na hostu, zajedno s IPv4 adresom, te je potrebna kako bi host mogao utvrditi kojoj mreži pripada. [1]

[1]< http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.0.1.>(8.5.2019)

Slika 3. Prikazuje izled zaglavlja Ipv4 protokola

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				

Izvor: <http://mreze.layer-x.com/s030101-0.html> ,(8.5.2019)

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

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

Polje „Tip usluge“ (eng. Type of Service, TOS) je polje duljine 8 bita. Polje je osmišljeno za određivanje kvalitete usluge (eng. Quality of Service, QoS). Novije implementacije IPv4 protokola ovo polje mijenjaju sa 6 bitnim DSCP (eng. Differentiated Service Code Point) i 2 bitnim ECN (eng. 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.

Polje „Ukupna duljina“ (eng. Length) služi za određivanje ukupne duljine IP paketa uključujući i podatke. Ovo polje prezentira se oktetima i u zaglavlju zauzima 16 bita. Polje „Identifikacije“ (eng. Identification) zauzima 16 bita, a određeno je od strane pošiljatelja. Služi identifikaciji pojedinačnih paketa koji su rastavljeni na fragmente od strane usmjernika .

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) .

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“ (eng. Time to Live, TTL) koristi se za određivanje količine vremena u kojoj je paketu dopušteno 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“ (eng. 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 (eng. Transmission Control Protocol) protokol. Ako polje poprimi vrijednost 0x11 (u heksadekadskom zapisu) ili 00010001 (u binarnom zapisu) koristi se UDP (eng. User Datagram Protocol) protokol. Internet Control Message Protocol predstavljen je heksadekadskim zapisom 0x01 ili binarnim zapisom 00000001. Usmjernik je uređaj koji usmjerava podatkovne pakete kroz mrežu pomoću IP adrese i djeluje na mrežnom sloju OSI modela. ICMP je kontrolni protokol za otkrivanje pogrešaka u računalnim mrežama tokom komunikacije tako da se šalju tzv. ICMP paketi.

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

Polje „Opcije“ (eng. 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 .

Polje „Podaci“ (eng. 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] [3]

2.1 Upravljanje IP adresama

Na čelu hijerarhijske strukture dodjeljivanja i upravljanja IP adresama stoji neprofitna organizacija ICANN (Internet Corporation for Assigneg Names and Numbers).

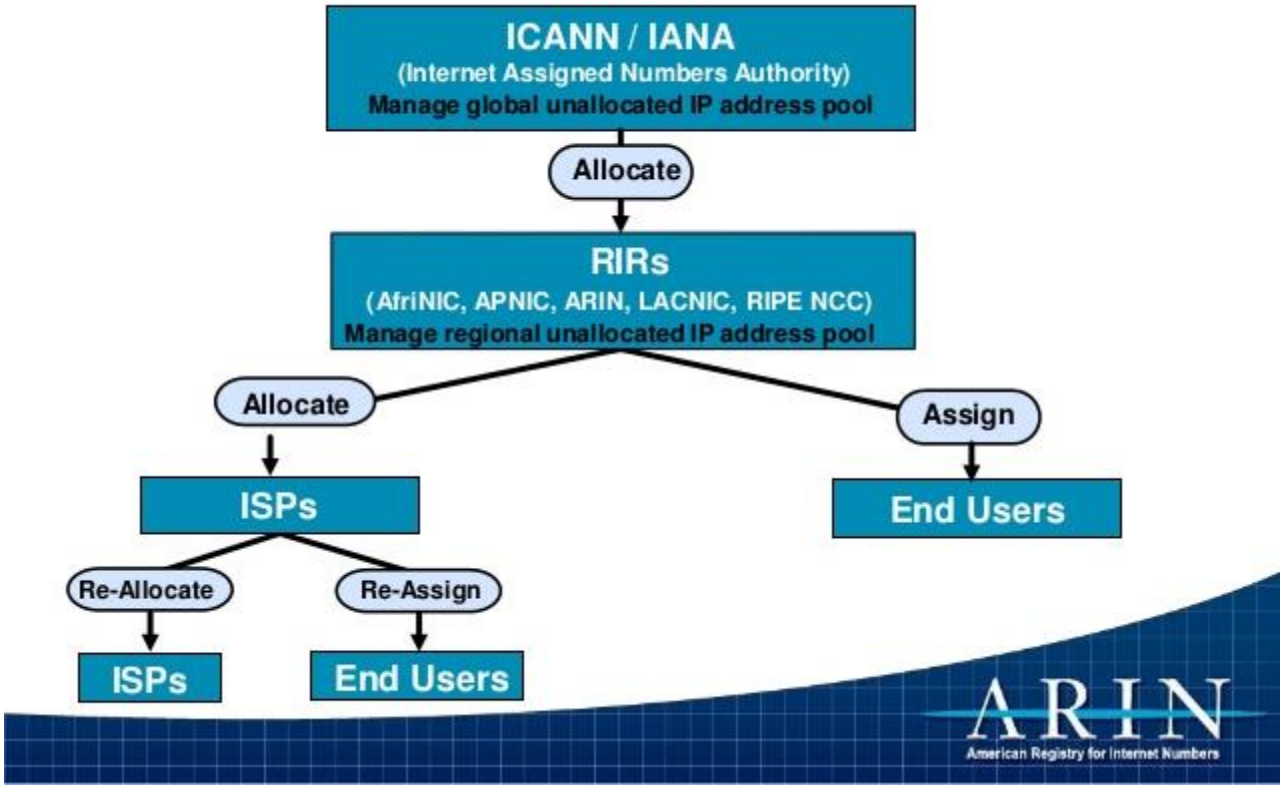
Postojanjem velike potrebe za upravljanjem IP adresama na globalnoj razini razvila su se mnoga pravila o dodjeljivanju IP adresa kojima se bave organizacije specijalizirane za taj posao. Na svijetskoj razini postoji nekoliko tih organizacija, a neke od njih su: RIPE NCC (RIPE Network Cordination Centere), ARIN (American Registry for Internet Numbers), LACNIC (Latin America and Caribbean Network Information Centere), AfriNIC (African Network Information Centere) i APNIC (Asian-Pacific Netvork Information Centere).

Slika 4. Prikazuje internetske registre prema području njihovog djelovanja.

[2] http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.0.1.1
[3] https://www.utilizewindows.com/the-difference-between-unicast-multicast-and%20broadcast-messages/

Izvor:<https://www.slideshare.net/TeamARIN/internet-operations-and-the-rirs>,(20.5.2019)

Slika 5. Prikazuje hijeraehijsku strukturu organizacija koje upravljaju IP adresama



Izvor: <https://www.slideshare.net/TeamARIN/internet-operations-and-the-rirs>,(20.5.2019)

Objašnjenje nekih izraza sa slike 4. :

- Dodjeljivanje (Allocate) - izdavanje brojevnih resursa ISP-ovima (internet service provider) za unutarnje mreže i za daljnje delegiranje kupaca
- Dodjela(Assign) - izdavanje brojevnih resursa krajnjim korisnicima samo za interne mreže

Glavna organizacija u strukturi upravljanja internetskim brojevima je ICANN. Dakle, njezina primarna funkcija je globalno upravljanje nedodjeljenim internetskim brojevima i dodjeljivanje brojeva regionalnim internetskim registrima (RIRs). Regionalni internetski registri dodjeljuju brojeve krajnjim korisnicima za internu mrežu ili dodijelit neiskorištene brojeve poslužiteljima internetskih usluga (ISP-Internet service provider). Poslužitelji internetskih usluga su tvrtke koje korisnicima nudi usluge vezane uz pristup internetu i administriranje internetskog sadržaja (eng. hosting), tj. registriranje domene, pozicija mrežnih stranica, elektroničke pošte, mrežne trgovine i sl. U Hrvatskoj postoji više davatelja internetskih usluga. U sklopu akademske zajednice djeluje neprofitna ustanova CARnet, dok na komercijalnoj osnovi usluge žičnog ili bežičnoga širokopojasnog pristupa internetu nude poduzeća Hrvatske telekomunikacije (T-Com i T-mobile), B.net, Optima Telekom, Vipnet, Tele2. Tvrtke koje se bave dodjeljivanjem i upravljanje internetskim brojevima dodjeljuju korisnicima slobodne IP adrese za usluge interneta.

2.2 Problematika IPv4 protokola

Trenutna verzija IP-a (poznata kao verzija 4 ili IPv4) nije se znatno promijenila od kada je uvedena 1981. godine. IPv4 uz TCP(Transmission Control Protocol) pokazao se kao robustan, lako implementiran protokol. Brzim prihvaćanjem i masovnim uvođenjem IPv4 protokola pojavljuju se njegovi nedostaci odnosno problemi koji nisu bili anticipirani pri njegovu dizajnu. Neki od problema koji se pojavljuju jesu :

- Eksponencijalni rast Interneta i predstojeća iscrpljenost internetskog IPv4 adresnog prostora, Iako 32-bitni adresni prostor IPv4 dopušta 4,294,967,296 adresa, iz prakse dodjele ograničavaju broj javnih IPv4 adresa na nekoliko stotina milijuna. Kao rezultat toga, javne IPv4 adrese postale su relativno oskudne, prisiljavajući mnoge korisnike i neke organizacije da koriste određene metode kojima se prevladava problem nedostatka IP adresa. Jedan od primjera je NAT – Network Address Translation, protokol kojim se mapira javna IPv4 adresa koja je vidljiva na Internetu a iza nje se koriste privatne adrese, čime se korištenjem samo jedne IP adrese, može spojiti mnogo više uređaja na Internet.
- Potreba za jednostavnijom konfiguracijom ,većina trenutnih IPv4 adresa implementacija mora biti ručno konfigurirana ili koristiti protokol za konfiguriranje adrese, kao što je Dynamic Host Protokol konfiguracije (DHCP). S više računala i uređaja koji koriste IP, postoji potreba za njima jednostavniju i automatsku konfiguraciju adresa i konfiguraciju usmjeravanja ne oslanjaju se na administraciju DHCP infrastrukture. To je veliki problem naprimjer u kampovima ili hotelim gdje imate nekoliko stotina televizija ili drugih uređaja povezanih na istu mrežu, pa kada bi se ručno upisivala svaka IP adresa trebalo bi puno vremena kojeg najčešće poslodavac želi drugačije iskoristiti.
- Zahtjev za sigurnost na internetskoj razini privatna komunikacija preko javnih medija, kao što je Internet zahtijeva kriptografske usluge koje štite podatke od mijenjanja njihovog sadržajau procesu slanja.
- Potreba za boljom podrškom za prioritetnu isporuku podataka u stvarnom vremenu[4]

Radi riješavanja ovih i drugih problema, skupina inžinjera za razvoj internetskog inžinjerstva (IETF- Internet Engineering Task Force) razvila je **a** skup protokola i standarda poznatih kao IP verzija 6 (IPv6). Ova nova verzija, ranije nazvana IPThe Sljedeća generacija (IPng), uključuje koncepte mnogih predloženih metoda za ažuriranje IPv4 protokol.

[4] Joseph Davies ,**Understanding Ipv6 third edition**, O'Reilly Media, 2012 godine str.2

2.3 NAT metoda

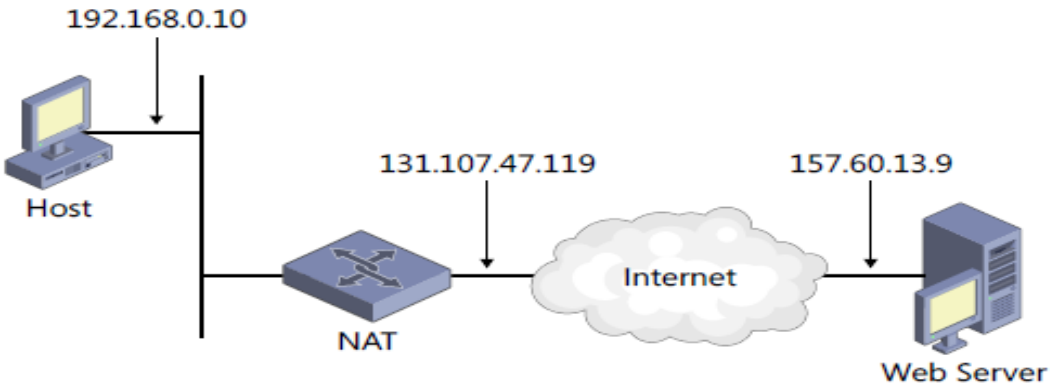
NAT (Network Address Translation) je proces promjene IP adrese koja se koristi u jednoj mreži u IP adresu koja se koristi u drugoj mreži. Jedna od mreža naziva se privatna (private) dok je druga javna (public). NAT se najčešće primjenjuje u slučaju kada jednu mrežu treba preko mrežnog prolaza spojiti s drugom mrežom kada se adrese iz unutarnje (lokalne) mreže preslikavaju na jednu ili više vanjskih (globalnih) IP adresa, a to se najčešće obavlja pomoću vatrozida (firewall-a) ili routera, postoji nekoliko vrsta: statički NAT , dinamički NAT i PAT (Port Adress Translation)[5]

Kao primjer prikazati će se jedna tvrtka koja koristi privatnu IPv4 adresu 192.168.0.0/24 za svoju intranet mrežu te joj je davatelj internetskih usluga dodijelio javnu IPv4 adresu 131.107.47.119 (ISP). NAT koji je smješten između ovih mreža mapira sve privatne adrese 192.168.0.0/24 na javnu adresu 131.107.47.119. NAT koristi dinamički odabrane TCP i UDP portove za mapiranje unutarnjih (intranet) tokova podataka na vanjske (internetske) podatkovne tokove. Privatni host dodijeljen privatnoj IPv4 adresi 192.168.0.10 za povezivanje na web poslužitelja koristi se web-preglednikom koji ima adresu 157.60.13.9, privatni host stvara IPv4 paket sa sljedećim:

- Odredišna adresa: 157.60.13.9
- Adresa izvora: 192.168.0.10
- Odredište TCP port: 80
- Izvorni TCP port: 1025

[5] **WEN Themes** , https://study-ccna.com/what -is-nat/ (21.5.2019)

Slika 6. prikazuje primjer NAT konfiguracije.



Izvor : Joseph Davies ,Understanding Ipv6 third edition, O'Reilly Media, 2012 godine str.3

Nadalje, prateći liniju kretanja podataka, podaci dolaze do NAT-a koji zatim konfigurira novu izvornu adresu i izvorni TCP port. I to izgleda ovako :

- Odredišna adresa: 157.60.13.9
- Adresa izvora: 131.107.47.119
- Odredište TCP port: 80
- Izvorni TCP port: 5000

NAT zadržava mapiranje {192.168.0.10, TCP 1025} na {131.107.47.119, TCP 5000} u lokalnoj tablici prijevoda za buduće upotrebe. Prevedeni IPv4 paket šalje se putem Interneta web poslužitelju koji prima paket i šalje odgovor nazad prema NAT-u. Kada primi poruku, paket sadrži sljedeće podatke:

- Odredišna adresa: 131.107.47.119
- Adresa izvora: 157.60.13.9
- Odredište TCP priključak: 5000
- Izvorni TCP port: 80

Zatim NAT provjerava svoju tablicu prijevoda koju je konfigurirao kada je paket poslan prvi put, prevodi odredišnu adresu prema podacima iz tablice i odredišni TCP port te prosljeđuje paket domaćinu odnosno hostu.

Za odlazne pakete iz NAT-a, izvorna IPv4 adresa (privatna adresa) mapira se na ISP-dodijeljenu adresu (javna adresa) i izvorni TCP / UDP portovi mapiraju se na različite TCP / UDP brojeve portova.

Za dolazne paketa prema NAT-u, odredišna IPv4 adresa (javna adresa) mapira se na izvornu intranetsku adresu (privatnu adresu) i odredište TCP / UDP brojevi portova vraćaju se natrag na njihove originalne TCP / UDP brojeve portova.

Naravno u stvarnoj primjeni sustav je kompliciraniji jer se komplikacije dešavaju kada postoje dva ili više hosta spojena na jedan NAT. Adresiranje i prijevod porta smanjuju performanse prosljeđivanja NAT-a zbog dodatnih operacije koje se moraju obaviti na svakom paketu. Kao rezultat, NAT se obično ne koristi u okruženjima velikih razmjera.

U ponekim slučajevima da bi izvršili izmjene IPv4 paketa potrebne su dodatne obrade pomoću softvera koji se nazivaju NAT editors (NAT uređivači),

NAT uređivači za prilagođavanje potrebni su u sljedećim situacijama:

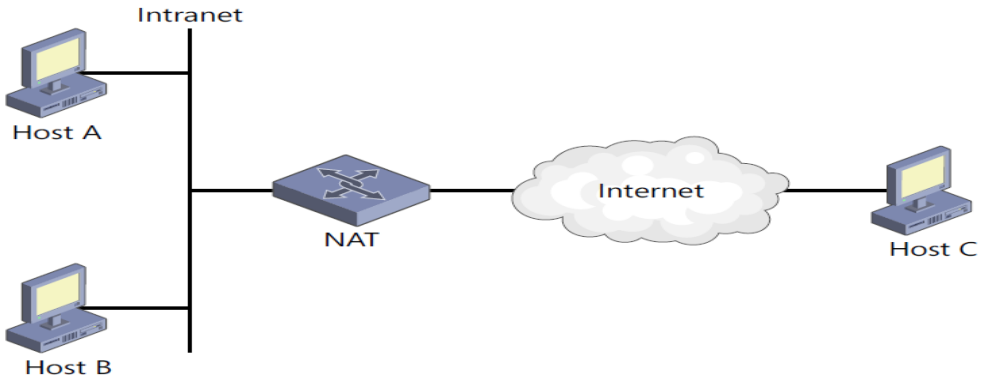
- IPv4 adresa, TCP port ili UDP port su spremljeni na drugom mjestu. Na primjer, Protokol za prijenos datoteka (FTP-File Transfer Protocol) pohranjuje točkasti decimalni prikaz IPv4 adrese u FTP zaglavlju za naredbu FTP PORT. Ako NAT ne prevede ispravno IPv4 adresu unutar FTP zaglavlja za FTP PORT naredbu i podesite TCP redne brojeve u tijeku razmjene pojavit će se problemi s povezivanjem i prijenosom podataka.
- TCP ili UDP se ne koriste za identifikaciju toka podataka. Na primjer, „tunel“ od točke do točke protokola (PPTP-Point-to-Point Tunnel Protocol) tunelirani podaci ne koriste TCP ili UDP zaglavlje. Umjesto toga, PPTP koristi Generičko zaglavlje za enkapsulaciju rute (GRE-Generic Ruting Encapsulation). Ako NAT ne prevede ispravno podatke koji se nalazi unutar GRE zaglavlja, pojavit će se problemi s povezivanjem.

NAT najbolje funkcionira kada klijent unutar NAT-a inicira komunikaciju. Gotovo svi podaci mogu preći NAT jer oba paketa zahtijevaju samo adresu ili port ili je NAT uređivač prisutan da na odgovarajući način modificira sadržaj. Ipak postoje iznimke te neki podaci ne mogu preći NAT. Ako su podaci koji zahtijevaju prijevod u šifriranom dijelu paketa, prijevod odnosno translacija nije moguća. Za podatke zaštićene s IPsec-om adresa i prijevod porta mogu poništiti integritet paketa. Za takve situacije postoje rješenja kao na primjer: IPsec NAT-Traversal (NAT-T) je noviji internetski standard koji dopušta prolaz podataka nekih tipova NAT-Traversal-a .

Dodatni problem s NAT-om je njegov učinak na aplikacije ravnopravnih korisnika. U peer-to-peer komunikaciji, hostovi mogu djelovati kao klijent ili kao poslužitelj i pokrenuti komunikaciju međusobno. Ako je peer iza NAT-a, s njim su povezane dvije adrese, jedna koja je poznata iza NAT-a (privatna adresa) i ona koja je poznata ispred NAT-a (javna adresa).

Za peer-to-peer aplikaciju koja se izvodi sa hostovima, Host A može pokrenuti sesiju s Hostom B i kod hosta C. Ali host A ne može obavijestiti host C o javnoj adresi i broju porta hosta B jer host A to ne zna. Također, Host C ne može pokrenuti sesije s hostom A ili hostom B bez postojeće unosa tablice prijevoda za prevođenje podataka koji su potrebni za ulaz u vezu sa privatnom adresom i priključkom Host-a A. Čak i sa unosom tablice, Host C možda neće moći pokrenuti sesiju s hostom A i hostom B jer su oba hosta na istoj javnoj IPv4 adresi.

Slika 7. Prikazuje primjer NAT peer-to-peer-a



Izvor: Joseph Davies ,Understanding Ipv6 third edition, O'Reilly Media, 2012 godine str.5

Da bi se riješili problemi sustava peer-to-peer ili multi-party NAT-ovi moraju biti modificirani NAT traversal tehnologijom, što rezultira dodatnom složenošću.

Kao zaključak možemo reći da je NAT učinkovita mjera kojom se omogućava produljenje trajanja IPv4 javnog adresnog prostora u smislu racionalnijeg korištenja adresa. Također NAT doprinosi sigurnosti informacijskih sustava time što su računala u privatnom dijelu dodatno zaštićena. Međutim NAT ne rješava problem s nedostatka adresa iz javnog adresnog prostora IPv4. Većini računala poslužitelja i dalje su potrebne jasne javne adrese. Iako se poslužitelj može smjestiti iza NAT-a, NAT mora biti ručno konfiguriran sa statičkim unos tablice prijevoda za prevođenje ulaznih podataka na privatnu adresu i port poslužitelja. [6]

[6] Joseph Davies ,**Understanding Ipv6 third edition**, O'Reilly Media, 2012 godine str.3-5

3. KARAKTERISTIKE IPv6 PROTOKOLA

Već 90-tih godina prema prikupljenim podacima i analizom došlo se do zaključka da IPv4 protokol ispunjava samo trenutne potrebe sa brojem adresa te da će uz određeni trend rasta biti iscrpljen. Stoga se počelo raditi na rješenju te ja razvijan novi protokol pod nazivom IPv6 koji je zapravo evolucija aktualnog IPv4 protokola.

Najznačajnija karakteristika Ipv6 jest njena veličina koja predviđa 128-bitova što omogućava adresiranje 7.9×1028. Broj adresa je toliko velik da ga je teško percipirati, no definitivno bi trebao premašiti buduće potrebe.

Format IPv6 adrese je tipa: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Neke od najvažnijih značajka protokola IPv6:

- Novi format zaglavlja
- Veliki adresni prostor
- Konfiguracija adrese bez statusa i stanja
- Bolja podrška za prioritetnu isporuku
- Ekstenzibilnost

Novi format Ipv6 zaglavlja dizajniran je za minimiziranje obrade zaglavlja. To se postiže pomicanjem nebitnih i neobveznih polja u zaglavlja proširenja koja se postavljaju nakon IPv6 zaglavlje. Pojednostavljeno zaglavlje IPv6 učinkovitije se obrađuje na ruterima. IPv4 zaglavlja i IPv6 zaglavlja nisu u potpunosti kompatibilna za direktan prijenos podataka. Host ili ruter moraju imat u sebi implementaciju oba Ipv4 i Ipv6 kako bi ih prepoznali i na pravilan način obradili zaglavlje.

Novo zadano zaglavlje IPv6 je dvostruko manje od zadanog zaglavlja IPv4 premda je broj bitova u IPv6 adresama četiri puta veći nego u IPv4 adrese.[7]

Za jednostavnu konfiguraciju hosta, IPv6 podržava oba statusa konfiguracije adrese (kao što je konfiguracija adresa u prisutnosti DHCP-a za IPv6 ili DHCPv6, poslužitelja) i konfiguracija adrese bez statusa (kao što je konfiguracija adrese i usmjeravanja u odsutnosti DHCPv6 poslužitelja). Statusnom konfiguracijom adrese hosta , hostovi na vezi automatski se konfiguriraju s IPv6

[7]Tomislav Volarić,**razlika između Ipv4 i Ipv6,** <http://tvolaric.com/preuzimanja/IPv4vsIPv6.pdf>,(29.5.2019)

adresama za link (naziva se link-local addresses) s adresama izvedenim iz prefixes-a koje odašilju lokalni routeri i lokalne podmreže i zadane rute.

Podrška za IPsec zaglavlja je zahtjev IPv6 protokola. Ovaj zahtjev osigurava riješenje temeljeno na standardima za potrebe zaštite mreže .IPsec se sastoji od dvije vrste zaglavlja, proširenja i protokola koji određuje sigurnosne postavke. Zaglavlje za provjeru autentičnosti (AH-Authentication header) osigurava integritet podataka, provjeru autentičnosti podataka, i ponovna zaštita za cijeli IPv6 paket Encapsulating Security Payload (ESP) pružaju integritet podataka, provjeru autentičnosti podataka, povjerljivost podataka i zaštitu za ponovnu reprodukciju za ESP-enkapsuliranane podatke. Protokol koji se obično koristi za ugovaranje IPsec sigurnosnih postavki za unicast komunikaciju je Internet Protokol za razmjenu ključeva (IKE).

Zahtjev za obradom IPsec zaglavlja ne čini IPv6 sigurnijim. IPv6 paketi ne moraju biti zaštićeni s IPsec, a IPsec nije zahtjev za implementaciju IPv6. Osim toga, IPv6 standardi ne zahtijevaju implementaciju za podršku bilo koje specifične metode šifriranja.

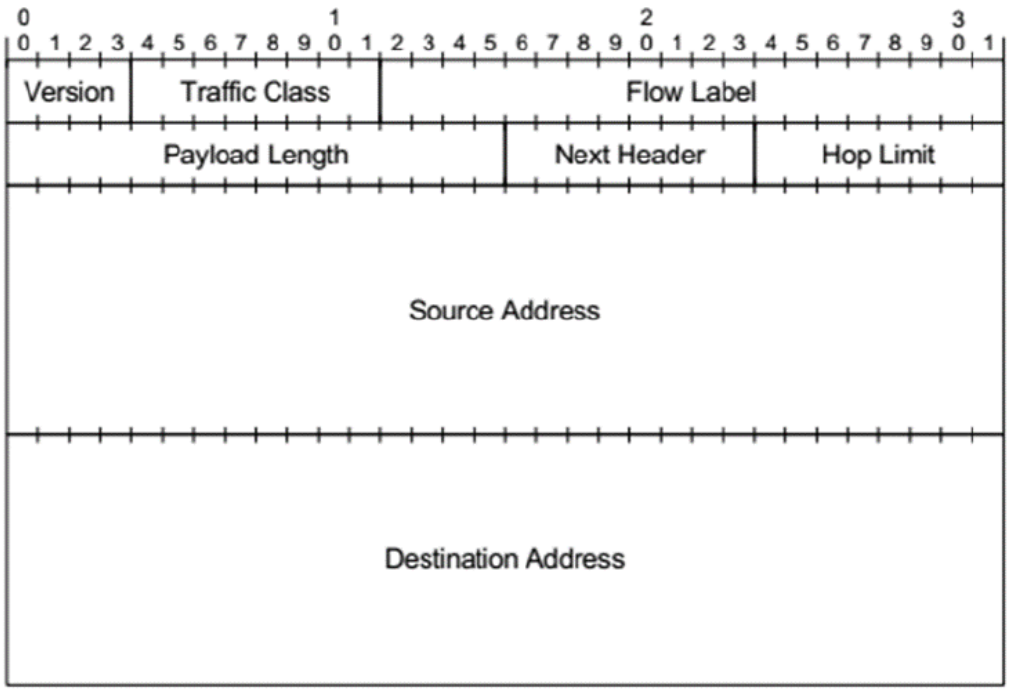
Nova polja u zaglavlju IPv6 definiraju kako se upravlja i identificira promet. Promet je klasificiran korištenjem Trafic Class polja , koji specificira DSCP vrijednost baš kao kod IPv4. Oznaka protoka koja se pojavljuje u IPv6 zaglavlje dopušta routerima da identificiraju i osiguraju posebno rukovanje za pakete koji pripadaju paketima niske važnosti (serija paketa između izvora i odredišta). Budući da je promet identificiran u zaglavlju IPv6, podrška za prioritetnu isporuku može se postići čak i kada je paketni sadržaj enkriptiran IPsec i ESP.

Protokol „Otkrivanja susjeda“ za IPv6 je niz protokola internetskih kontrolnih poruka za IPv6 (ICMPv6-Internet Control Message Protocol) poruke koje upravljaju interakcijom sa susjednim čvorovima. Otkriće „susjedstva“ zamjenjuje i proširuje kombinaciju ARP-a (Address Resolution Protocol). ICMPv4 Router Discovery i ICMPv4 Redirect poruke s učinkovitim multicastom i unicast poruke o otkrivanju susjeda odnosno drugih mreža i hostova.

Za IPv6 možemo reći da je fleksibilan zbog toga što se lako može proširiti za nove značajke dodavanjem zaglavlja proširenja nakon zaglavlja IPv6. Za razliku od opcija u IPv4 zaglavlju, koje mogu podržavati samo 40 bajta opcija, veličine IPv6 proširenja zaglavlja ograničena je samo veličinom paketa IPv6.[89]

[8] Joseph Davies ,Understanding Ipv6 third edition, O’Reilly Media, 2012 godine str.3-5

Slika 8. Prikazuje izgled zaglavlja Ipv6



Izvor : <https://searchnetworking.techtarget.com/definition/IPv6-Internet-Protocol-Version-6>, (2.6.2019)

Zaglavlje započinje poljem **verzija** (**version)** te kao i kod IPv4 predstavlja verziju IP protokola.. Nakon toga dolazi oznaka **klase prometa(traffic class)** te oznaka toka podataka kojemu paket pripada. Zatim dolazi oznaka **duljine paketa(flow label)** koja sadrži duljinu polja podataka u oktetima ili bitovima.. U slučaju da je potrebna veća nosivost paketa, postoji proširenje unutar IPv6 zaglavlja. Polje **Next Header** je jednako 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 jednaku 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.

[9] <https://www.ietf.org/>,(30.5.2019)

Postoje 3 vrste IPv6 adresa

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

Jednoodredišne i višeodredišne adrese su vrste adresa koje se koriste i kod protokola IPv4, dok su za IPv6 karakteristične jednoodredišne adrese unutar čvora. 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 tri vrste unicast adresa:

- Global unicast – javna adresa, počinje sa 2000::/3 ili 2001:
- Link local – ne prosljeđuje se van mrežnog segmenta, mora biti prisutna na svakom mrežnom adapteru. Počinje sa Fe80::/10. Ona je self-assigned, odnosno sama se konfigurira koristeći parametre MAC adrese
- Unique local – interna privatna adresa. Primjer: FD00:/8

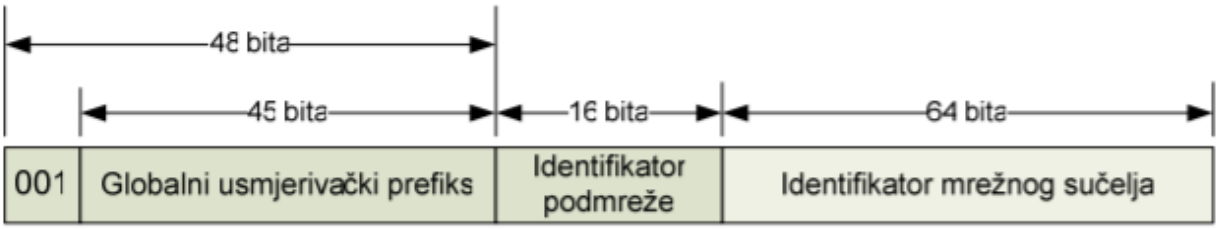
Za konfiguraciju poslužitelja koriste se global unicast adrese

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

- globalni prefiks usmjeravanja,
- oznaka podmreže i
- 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.Primjer globalne jednoodredišneadrese prikazan je na slici 9.

Slika 9. Prikazuje strukturu globalne jednoodredišne adrese



Izvor: < https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf>,(29.8.2019)

Fiksni dio postavljen na vrijednost 001 tri najznačajnija bita postavljena su na 001 pa je prefiks za globalne adrese 2000::/3. Globalni usmjerivački prefiks označava globalni usmjerivački prefiks za administrativnu domenu određene organizacije. U kombinaciji s 3-tobitnim fiksnim dijelom čini 48bitni prefiks administrativne domene.

Nakon dodjele ovakve adrese, usmjerivači na IPv6 Internetu prosljeđuju sav promet čijih se prvih 48 bita adrese poklapa s navedenim prema usmjerivačima dotične organizacije. Identifikator podmreže koristi se unutar organizacije za identifikaciju podmreže kojoj je IPv6 paket namijenjen. Veličina ovog polja je 16 bita, što omogućava ostvarivanje 65.536 podmreža ili višestruke razine hijerarhije. Identifikator mrežnog sučelja 64 bitni identifikator koji određuje mrežno sučelje odgovarajuće podmreže unutar administrativne domene organizacije kojemu je IPv6 paket namijenjen.

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 . Multicast adresiranje odnosno višeodredišno adresiranje funkcionira kao i kod IPv4 protokola. 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 DHCP11 (engl. Dynamic Host Configuration Protocol) verzije 6 te od DHCP-poslužitelja dobiva parametre potrebne za konfiguraciju svog mrežnog sučelja.[10]

[10]< https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf>,(2.6.2019)

4. USPOREDBA Ipv4 i Ipv6 PROTOKOLA.

Sljedeća tablica na temelju prikupljenih informacija biti će prikazana uspredba IPv4 i IPv6 adrese iz koje možemo zaključiti koje sve prednosti donosi upotreba Ipv6. Naglasak IETF-a kod razvoja IPv6 protokola je da se zadrži osnovna forma IPv4 uz poboljšanje svih njenih karakteristika kao što su jednostavnos i otvorenost protokola.

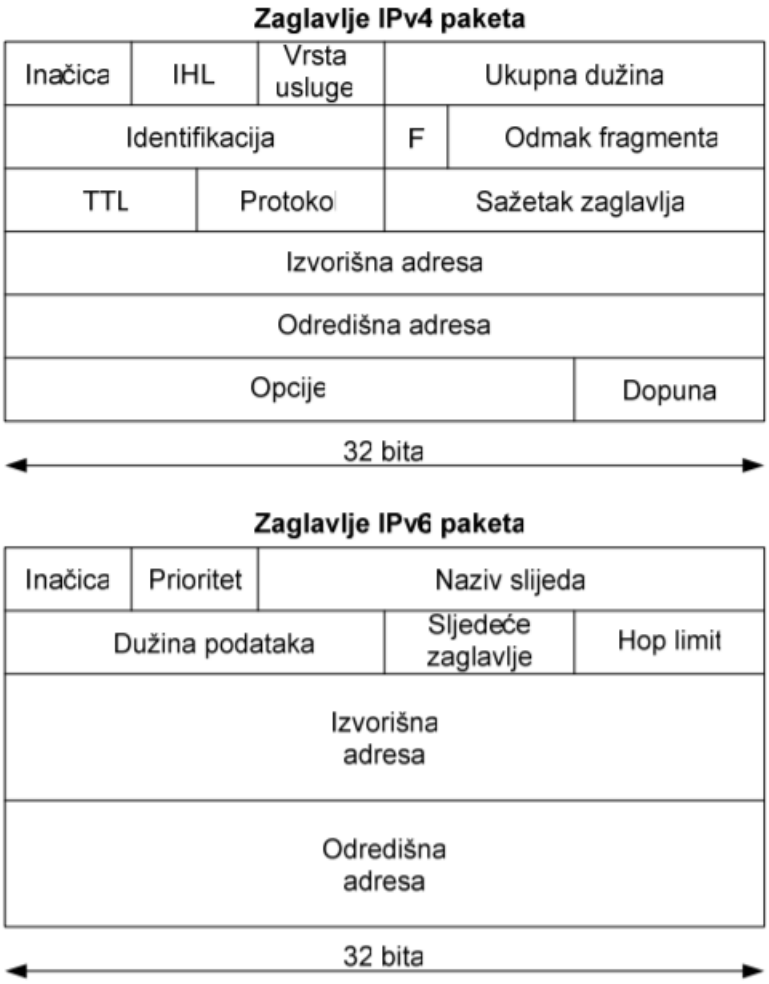
Restrikcijom definiranja sučelja između različitih protokola pružaju se bolje performanse za krajnjeg korisnika i uređeniju mrežnu infrastrukturu kako bi bilo što manje rasipanja i komplikacija. Razvojem različitih tranzicijskih metoda uvođenje IPv6 protokola ne zahtijeva gotovo nikakva dodatna ulaganja i omogućava nesmetanu upotrebu Ipv4 i Ipv6 protokola na istoj mrežnoj infrastrukturi.

Tablica 1. Prikazuje usporedbu IPv4 i IPv6 protokola.

	Ipv4	**Ipv6**
Veličina adrese	32-bitne adrese	128-bitne adrese
Tip adrese	Unicast, multicast i broadcast adrese.	Unicast, multicast i anycast adrese
Maska adrese	Koristi se za označavanje mreže u host dijelu.	Ne koristi se.
Opcije 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: Autor

Slika 10. Prikazuje usporedbu zaglalja IPv4 i IPv6 protokola.



Izvor : https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf, (2.6.2019)

Najznačajnija promjena odnosi se na polje „Opcije“. Kod IPv4 protokola polje „Opcije“ koristi se za dodavanje dodatnih informacija o raznim opcionalnim uslugama (primjerice enkripciji sadržaja paketa). Zbog navedene činjenice dužina zaglavlja IPv4 paketa nije ujednačena, već ovisi o broju korištenih opcija što znatno otežava i usporava postupak obrade i usmjeravanja paketa te nameće veće zahtjeve na sklopovlje usmjerivača. S druge strane, IPv6 protokol informacije o dodatnim uslugama pomiče u dio paketa koji se naziva ekstenzija zaglavlja (na slici 1 prikazan je samo osnovni dio zaglavlja IPv6 paketa). Na taj način, veličina zaglavlja „običnih“ IP paketa fiksirana je na 40 okteta, što znatno olakšava njihovu obradu. Druga značajna razlika IPv4 i IPv6 zaglavlja jest polje „Sažetak zaglavlja“. To je polje koje se kod IPv4 protokola koristi kod kontrole integriteta

sadržaja zaglavlja, a prilikom čijeg se izračuna koriste vrijednosti svih polja zaglavlja. Budući da „TTL“ polje u zaglavlju paketa sadrži vrijednost koja se mijenja svakim prolazom kroz usmjerivač, polje „Sažetak zaglavlja“ treba se ponovno računati na svakom koraku prolaza kroz mrežu.

Uklanjanjem tog polja, IPv6 protokol znatno umanjuje količinu posla kojeg obavljaju usmjerivači te na taj način smanjuje kašnjenje koje unose u računalnu mrežu. Integritet prenesenih podataka pritom nije ugrožen, budući da TCP sloj, koji se nalazi „iznad“ IP sloja, između ostalog provjerava integritet adresa izvorišta odnosno odredišta pa to nije potrebno izvoditi i u IP sloju. Polje „Vrsta usluge“ kod IPv4 protokola koristi se za označavanje prioriteta paketa, pri čemu se razina prioriteta prikazuje cjelobrojnom vrijednošću od 0 do 7. IPv6 protokol pruža istu funkcionalnost kroz polje koje se zove „Prioritet“. Polje „Naziv slijeda“ uvedeno je u zaglavlje IPv6 paketa radi određivanja slijeda paketa određene vrste usluge (primjerice VoIP).

Ta funkcionalnost postoji i kod IPv4 protokola, iako zahtjeva veći broj zasebnih operacija (provjera broja mrežnog priključka, odredišnih i izvorišnih adresa). Budući da se određivanje slijeda paketa pokazalo kao iznimno korisna funkcionalnost, prilikom specifikacije IPv6 protokola za tu je svrhu rezervirano posebno polje. Prilikom oblikovanja zaglavlja IPv6 paketa nastojalo se višak informacija preseliti u ekstenziju zaglavlja. Na taj je način postignuta učinkovitija obrada paketa na usmjerivačima, pogotovo u slučaju posrednih usmjerivača koji paket samo prosljeđuju. Važno je također primijetiti kako ne postoji kompatibilnost IPv4 i IPv6 zaglavlja, tako da usmjerivači koji rade u miješanim okruženjima moraju implementirati oba protokola. IPv6 paket može imati nula ili više ekstenzija zaglavlja pri čemu polje „Sljedeće zaglavlje“ definira sljedeću ekstenziju zaglavlja, s tim da posljednja ekstenzija zaglavlja na tom mjestu ukazuje na protokol višeg mrežnog sloja (npr. TCP ili UDP)[11]

[11]**CARNet**, <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf>,(2.6.2019)

5. IMPLEMENTACIJA

5.1 Prijelaz s IPv4 na IPv6 protocol

U svrhu poboljšanja internetske usluge, pružatelji internetskih usluga postepeno uvode IPv6 verziju protokola. Iako to u teoriji izgleda kao jednostavan i lagan pothvat u praksi postoje određeni problemi prilikom njegova uvođenja. Sustav se ne može implementirati odjednom jer postoje prepreke u samoj infrastrukturi mreže kao i uređaji kod krajnjih korisnika koji nemogu enkapsulirati podatke sa IPv6 protokola te dolazi do gubljenje podataka i nezadovoljstvo samih krajnjih korisnika. Stoga je preporuka da se sustav uvodit postepeno odnosno paralelno, dakle pružajući usluge i preko IPv4 i IPv6 protokola te na taj način postepeno nadograđivati samu infrakstrukturu mreže.

Jedan od načina tog načina paralelne implementacije4 jest da se se podatkovni paketi koji izlaze sa sučelja konfiguriranim IPv6 protokolom, enkapsuliraju u IPv4 pakete te im se pri povratku u IPv6 sučelje uklanja IPv4 zaglavlje. [12]

IPv6 i IPv4 će koegzistirati još dugi niz godina, a postoji širok raspon tehnika koji omogućuju suživot i omogućuju jednostavan prijelaz. Te tehnike su podijeljene u tri glavne kategorije:

- Dual-Stack tehnika dopušta da IPv4 i IPv6 koegzistiraju u istim uređajima i mrežama
- Tunneling tehnika omogućuje prijenos IPv6 prometa preko postojeće IPv4 infrastrukture
- Tranzicijska tehnika dopušta da čvorovi koji imaju samo IPv6 komuniciraju s čvorovima koji imaju samo IPv4

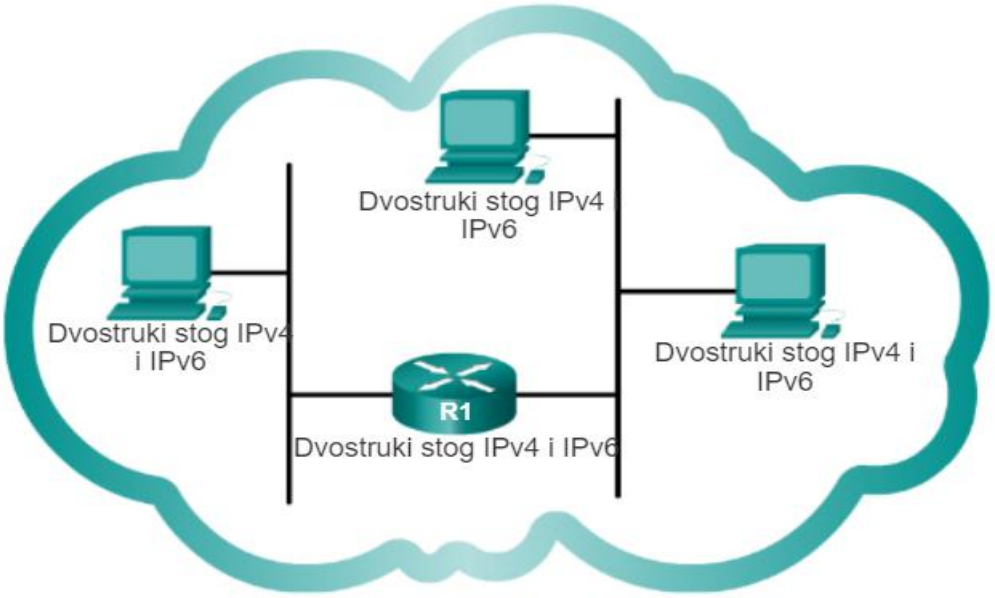
Ove tehnike senajčešće koriste u kombinaciji jedna s drugom. prijelaz na IPv6 može se obavljati korak po korak, počevši s jednim hostom ili podmrežom.

[12] Bažant, Alen; et al: **Osnove arhitekture mreža**, Element, Zagreb, 2004. Str.43

5.2 Dual –Stack metoda

Dual-stack metoda ima u potpunosti podršku za obije verzije protokola. U komunikaciji s IPv6 čvorom, takav čvor se ponaša kao čvor samo za IPv6, ali u komunikaciji s IPv4 čvorom, ponaša se kao čvor samo za IPv4. Implementacije mogu imati konfiguracijski prekidač kojim omogućite ili onemogućite jednu od mogućnosti ove metode., Tako da u svakom čvoru može se imati tri načina rada. Kada je IPv4 stack omogućen i IPv6 stack je onemogućen, čvor se ponaša kao IPv4-čvor. Kada je IPv6 stack omogućen, a stog IPv4 onemogućen, ponaša se kao IPv6 čvor. Kada su omogućeni i IPv4 i IPv6 stack , čvor može koristiti oba protokola. IPv6 / IPv4 čvor ima barem jednu adresu za svaku verziju protokola-

Slika 11. Prikazuje dual-stack tehniku prelaska sa IPv4 na IPv6



Izvor: <http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.2.1.2>(10.7.2019)

Dual-stack mrežna je infrastruktura u kojoj su i IPv4 i IPv6 prosljeđivanje omogućen na usmjerivačima (R1). Nedostatak ove tehnike je da morate izvršiti punu nadogradnju mrežnog softvera za pokretanje dva zasebna skupa protokola. Sve tablice (npr., tablice usmjeravanja) čuvaju se istovremeno s konfiguriranim protokolima usmjeravanja oba protokola. Za upravljanje mrežom, na nekim operacijskim sustavima možete još uvijek imati zasebne naredbe ovisno o protokolu (npr. ping za IPv4 i ping6 za IPv6), a potrebno je više memorije i snage procesora što je i logično pošto se svi podaci spremaju i više podataka ose obrađuje.

5.3 Tunneling (tuneliranje) metoda

Mehanizmi za tuneliranje mogu se koristiti za implementaciju IPv6 infrastrukture za prosljeđivanje dok je cjelokupna IPv4 infrastruktura još uvijek temelj i ne bi trebala ili ne može izmijeniti ili nadograditi. Tuneliranje se također naziva enkapsulacija. S enkapsulacijom, jedan protokol (u našem slučaj, IPv6) je enkapsuliran u zaglavlje drugog protokola (u našem slučaju, IPv4) i proslijeđena preko infrastrukture drugog protokola (IPv4). Proces enkapsulacija ima tri komponente:

- Inkapsulacija na ulaznoj točki tunela
- Dekapsuliranje u tunelu
- Tunel menađžment

Ukratko tuneliranje se koristi za prijenos IPv6 podatkovnog prometa takošto ga se upakira kao IPv4 paket i preko infrastrukture koja nije predviđena za podržavanje IPv6 tuneliranjem usmjeravaju se podaci.

Na primjer, ako vaš davatelj usluga i dalje koristi infrastrukturu samo za IPv4, tuneliranje vam omogućuje da imate korporativnu IPv6 mrežu i tunel kroz IPv4 mrežu vašeg ISP-a kako bi dosegli druge IPv6 hostove ili mreže. Ili možete postaviti IPv6 otoke u korporacijskoj mreži dok poveznica je još uvijek IPv4 kao što se može vidjeti na slici 8. . IPv6 paketi koji putuju s jednog IPv6 otoka na drugi moraju najprije prijeći enkapsulaciju u IPv4 pakete. Tehnike tuneliranja i enkapsulacija IPv6 paketa u IPv4 paketima definirani su u nekoliko RFC-ova, kao što su :

RFC 2473-Generički paketni tunela u IPv6 specifikaciji,

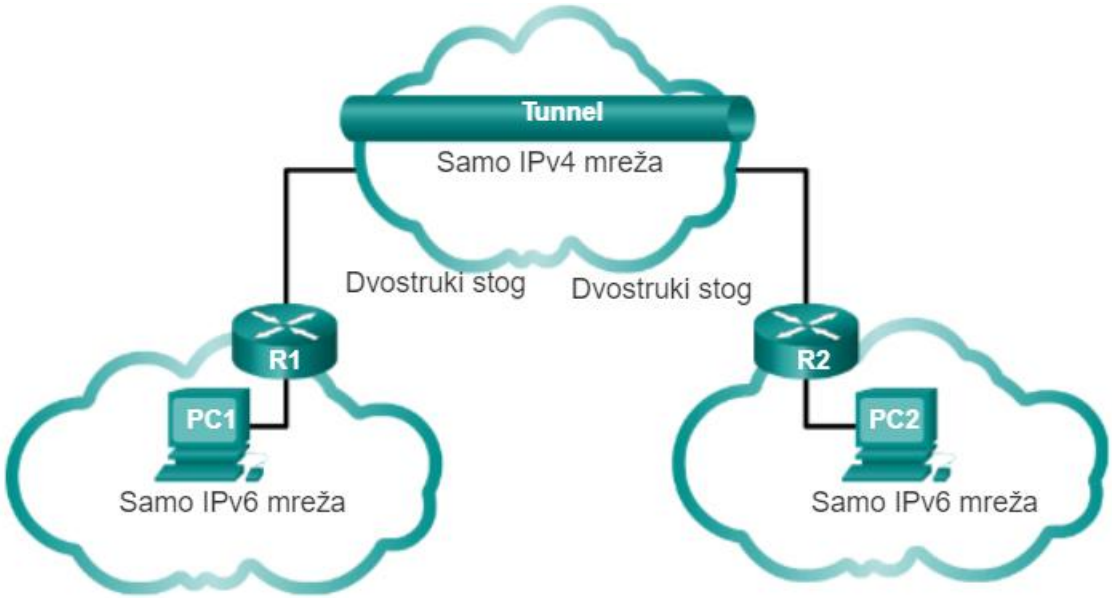
RFC 4213-Osnovni tranzicijski mehanizmi za domaćine i usmjerivače IPv6,

RFC 3056-Povezivanje IPv6 Domene putem IPv4 clouda (6 do 4)

Možemo razlikovati dvije opće vrste tuneliranja:

- **Ručno konfigurirano tuneliranje IPv6 preko IPv4:** IPv6 paketi su enkapsulirani u IPv4 pakete koji se prenose preko IPv4 usmjeravanja infrastrukture. To su tuneli od točke do točke koje je potrebno konfigurirati ručno.
- **Automatsko tuneliranje IPv6 preko IPv4:** IPv6 čvorovi mogu koristiti različite vrste adresa, kao što su 6to4 ili ISATAP adresa, za dinamičko tuneliranje IPv6 paketa preko IPv4 usmjerivačke infrastrukture.

Slika 12. Prikazuje tehniku tuneliranja iz IPv6 u IPv4



Izvor: <http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.2.1.2>,(10.7.2019)

Ručno konfigurirano tuneliranje je tuneliranje gdje su krajnja točka tunela IPv4 adrese određene konfiguracijskim informacijama na krajnjim točkama tunela. Svi Pretpostavlja se da su svi tuneli dvosmjerni. Administrativni rad za upravljanje konfiguriranim tunelima veći je nego s automatskim tunelima, ali iz sigurnosnih razloga je tako se pruža veća kontrola nad putanjom protoka podataka.. RFC 4213 raspravlja o konfiguraciji i problemima koje treba riješiti, kao što je određivanje važećih adresa krajnje točke tunela (ulazna filtriranje), kako postupati ICMPv4 ili ICMPv6 poruke, veličina MTU tunela, fragmentacija, polja zaglavlja, Otkrivanje susjeda (ND) nad tunelima i sigurnosna razmatranja.

Automatsko tuneliranje omogućuje IPv6 / IPv4 čvorovima da komuniciraju preko IPv4 infrastrukture bez potrebe za predkonfiguracijom odredišnoga tunela. U prethodnim specifikacijama adresa krajnje točke tunela određena je odredišnom adresom kompatibilnom s IPv4. RFC 4213 uklanja opis automatskog tuneliranja i IPv4-kompatibilnih adresa i odnosi se na 6to4, 6to4 ima svoj IPv6 format adrese, koji uključuje IPv4 adresu tunela krajnja točka u prefiksu i stoga omogućuje automatsko tuneliranje.

5.4 Tranzicijska metoda

Ova metoda omogućava prijenos IPv6 podataka prelp IPv4 mreže bez prethodno konfiguriranih tunela. Pomoću javnih IPv4 adresa stvaraju se unikatne IPv6 adrese uređaja. Ovaj se mehanizam naziva 6to4. Obrađuje se IPv4 mreža širokog područja kao unicast point-to-point sloj veze, a izvorne IPv6 domene komuniciraju putem 6to4 usmjerivači, koji se nazivaju i 6to4 pristupnici. U mreži 6to4 ne smiju se vršiti promjene na hostovima. Ovo je izmišljeno kao prijelazni mehanizam koji se koristi tijekom razdoblja suživota IPv4 i IPv6 a ne kao trajno rješenje. IPv6 paketi su enkapsuliran u IPv4 na pristupniku 6to4.

Potrebna je barem jedna globalna jedinstvena IPv4 unicast adresa za ovu konfiguraciju. IANA je dodijelio poseban prefiks za shema 6to4“: 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 i pomoću njih se može stvoriti još 65 536 mreža.. U tom se slučaju nadodaje proizvoljna vrijednost ili jednostavno ::1. Ostatak od 64 bita je identifikator sučelja, odnosno EUI-64 adresa.

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.

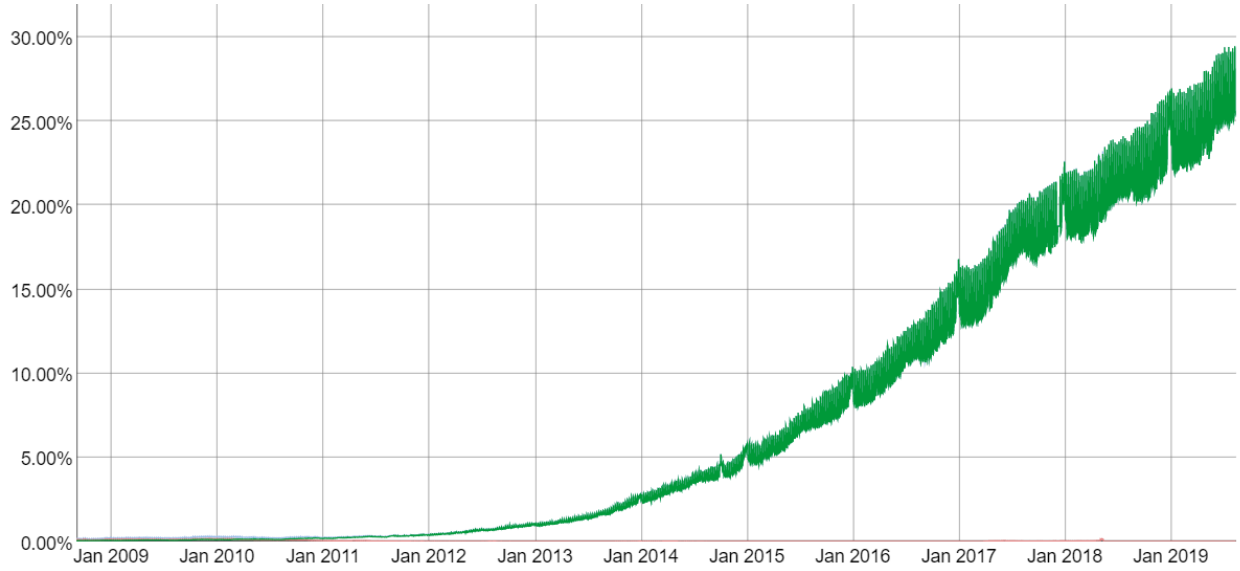
Slika 13. Prikazuje 6to4 metodu komunikacije

Izvor: >http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.2.1.2>(10.7.2019)

5.5 Statistika upotrebe i razvoja IPv6 protokola

Dana 25.7.1994 na sastanku IETF-a u Torontu tim koji je razvijao IPv6 iznjeli su predlog svog protokola te njegove specifikacije koji je i usvojen, jer zahtjeva minimalne preinake u mreži i kod korisnika da bi se mogao usvojit.

Slika 14.prikazuje upotrebu IPv6 protokola



Izvor:<https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6adoption&tab=ipv6adoption>, (8.8.2019)

Slika 14. Prikazuje graf na kojem je zelenom bojom označena upotreba IPv6 protokola u vremenu od siječnja 2009. godine do kolovoza 2019. godine. Podatke prikuplja Google od svojih korisnika na temelju koliko njih koristi IPv6 protokol. U početku IPv6 protokol nije zabilježio značajnu primjenu, od 1995. godine kada je usvojen pa do 2009.godine iz grafa se može vidjeti da je njegova globalna upotreba bila svega 0.18% u 14 godina postojanja.

Iz grafa se može zaključiti kako IPv6 protokol čini nešto manje od 30% ukupnog prometa na inernet mreži, iako kod pojedinih država taj broj je nešto veći. Belgija je država koja ga je u najvećoj mjeri prihvatila sa 54 %, sljedeće su Sjedinjene Američke Države sa 36 %, Grčka 33 % i ostale države.[13]

[13] **Internet Society,** https://www.internetsociety.org/wp-content/uploads/2018/06/2018-ISOC-Report-IPv6-Deployment.pdf,(8.8.2019)

6. IMPLEMENTACIJA NA ISTARSKOM VELEUČILIŠTU

Istarsko Veleučilište dio je mreže koja koristi IPv6 protokol u Hrvatskoj, za dodjeljivanje IPv6 protokola na području Republike Hrvatske zadužena je tvrtka CARNET. CARNET od 1993. godine upravlja nacionalnom domenom Republike Hrvatske zaduženje za upravljanje CARNET-u dodijelila je međunarodna organizacija ICANN.

Hrvatska akademska i istraživačka mreža – CARNET javna je ustanova koja djeluje u sklopu Ministarstva znanosti i obrazovanja u području informacijsko-komunikacijske tehnologije i njezine primjene u obrazovanju. Svoju povijest CARNET započinje 1991. godine kao projekt tadašnjega Ministarstva znanosti i tehnologije te postaje prvi i jedini pružatelj internetskih usluga u Hrvatskoj. Četiri godine poslije Vlada RH donosi Uredbu o osnivanju ustanove CARNET radi inoviranja obrazovnoga sustava te poticanja napretka pojedinaca i društva u cjelini s pomoću IKT-a[14]

Početkom djelovanja Politehnika Pule, sada Istarskog Veleučilišta, od CARNet je dodijeljen adresni prostor i podmreža od veličine 64 hostova.

Raspon dodijeljenih adresa je 161.53.146.192 – 161.53.146.255

Mrežna maska je 255.255.255.192 što omogućava adresiranje 62 aktivnih uređaja počevši od 161.53.146.193 do 161.53.146.254.

161.53.146.192 je adrese mreže

161.53.145.255 je broadcast adresa

Zahtjevi informacijskog sustava na Istarskom Veleučištu:

Na IV osim pristupu na Internet od strane studenata i osoblja, postavljeni su vlastiti poslužitelji koji su potrebni za rad IV.

e-mail ./197
web servis ./201
ldap – imenik za korisnike ./197
radius – protokol za autentikaciju i autorizaciju korisnika./197

[14]< https://www.carnet.hr/o-carnet-u/>,(10.8.2019)

Prva adresa koriste se za usmjerivač a to je 161.53.146.193

NAT je implementiran na adresi 161.53.146.254 na uređaju Mikrotik.

Prema zahtjevu Istarskog Veleučilišta CARNET dodjeljuje IPv6 prefiks „2001:b68:4c02::/56“ čime je za konfiguraciju moguće koristiti adrese od 2001:0b68:4c02:0000:0000:0000:0000:0000-2001:0b68:4c02:00ff:ffff:ffff:ffff:ffff i konfiguriranu u **dual-stacku s IPv4 mrezom** (161.53.146.192/26). Za potrebe ovog rada ručno su dodane IPv6 adrese na ključne servise.

Parametri IPv6 mreže:

- subnet: 2001:B68:4C02::/64
- default gateway: 2001:B68:4C02::1 (FE80::207:85FF:FE80:9DEB)

Uz postojeće IPv4 adrese dodane su IPv6 adrese koje su prikazane u tablici:

Tablica 2. Prikazuje IPv6 i IPv4 adrese te što se nalazi na njima

2001:B68:4C02::1	161.53.146.193	Gateway
2001:0B68:4C02:0000:0000:0000:0000:0010/56 2001:b68:4c02::10/56	161.53.146.254	Mikrotik .254
2001:0B68:4C02:0000:0000:0000:0000:0002/56	10.10.10.167	Test PC – interna DHCP adresa
2001:0B68:4C02:0000:0000:0000:0000:0011/56	161.53.146.197	Mail server
2001:b68:4c02::12/56	161.53.146.201	Web poslužitelj
2001:0B68:4C02:0000:0000:0000:0000:0005/56	161.53.146.195	DNS poslužitelj

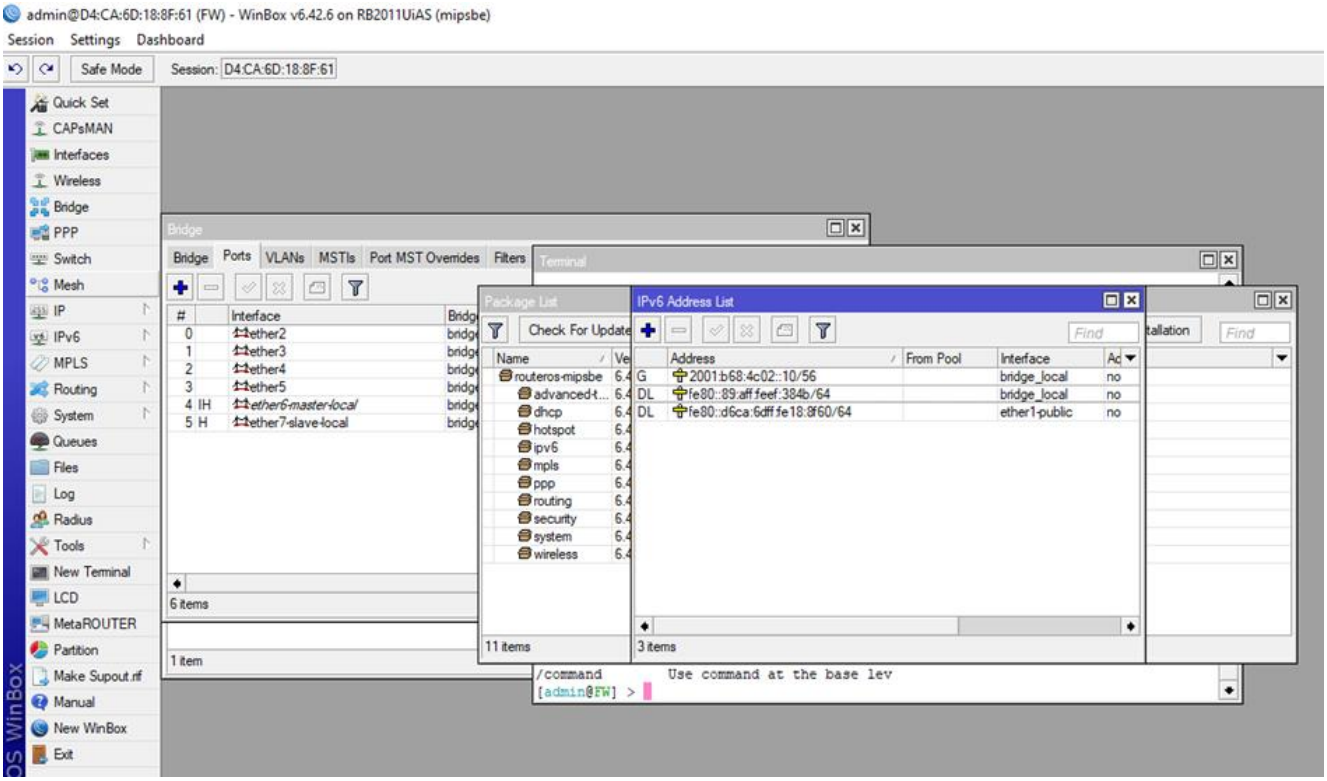
Izvor:Autor

Gateway sa IPv4 adresom 161.53.146.193 konfigurirao je mrežni operativni centar CARNeta koji su zaduženi za vanjski segment mreže. Naš interni usmjerivač i poslužitelje konfigurirali smo sami. Najprije je potrebno postaviti adrese koje će se konfigurirati. Prvo je postavljena adresa na glavni vatrozid sa adresom 161.53.146.254, a zatim su dodane pojedinačne adrese na poslužitelje

Konfiguracija vatrozida (firewall)

Glavni vatrozid je zasebni uređaj Mikrotik na kome je bilo potrebno dodati softverski paket za podršku IPv6 protokolu. Na slici 15. prikazan je Winbox alat za konfiguraciju Mikrotik uređaja nakon što je dodana IPv6 podrška te postavljena adresa 2001:b68:4c02::10/56. Uz prijašnju IPv4 161.53.146.254

Slika 15. Winbox alat za konfiguraciju Mikrotik uređaja



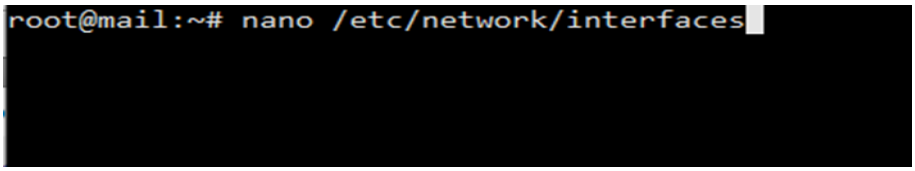
Izvor:Autor

Winbox je specijalni alat koji omogućuje administraciju MikroTik uređaja, izvorno je Win32 binarni sustav ali može se koristiti i na Linuxu i MacOs-u. zbog svoje jednostavnosti kompletne upute za korištenje mogu se naći besplatno na internetu.

Konfiguracija web poslužitelja

Konfiguracija IPv6 adrese na Linux poslužitelju napravljena je promjenom mrežne konfiguracije u /etc/network/interfaces datoteci.

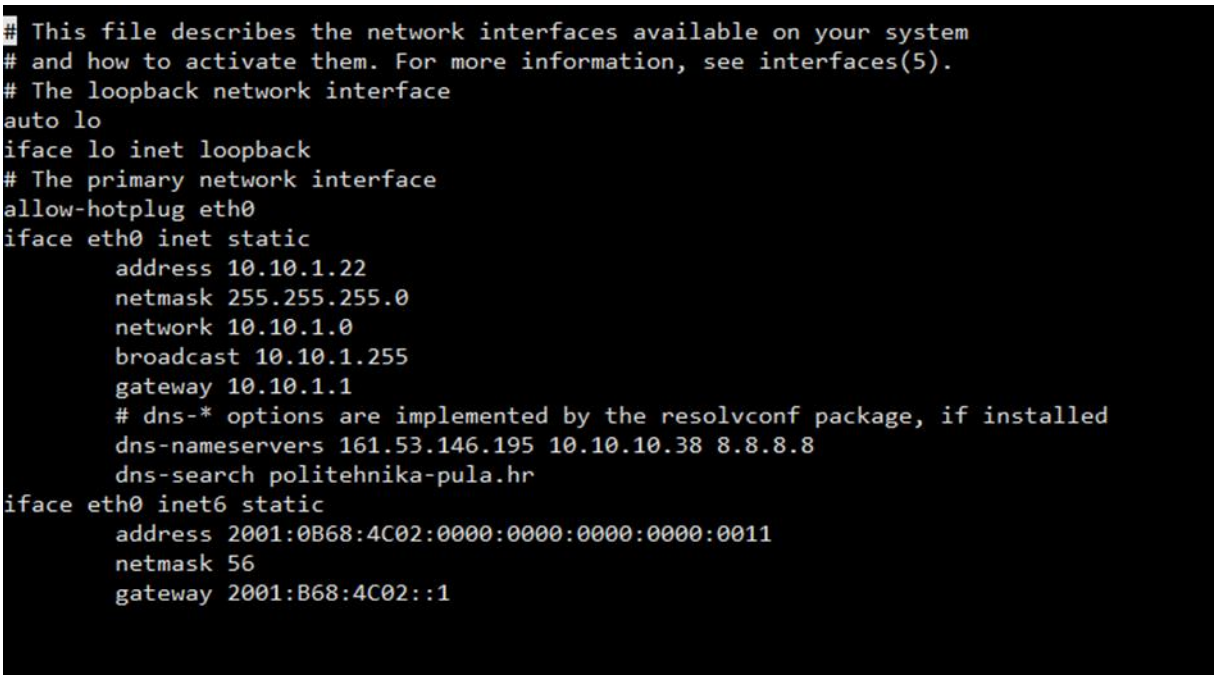
Slika 16. Prikazuje konfiguracijsku datoteku za web poslužitelja



Izvor: Autor

Postavljanjem naredbe i otvaranje same datoteke nakon dodavanje IPv6 adrese, konfiguracijska datoteka izgleda kao što je prikazano na slici 17.

Slika 17: prikazuje sadržaj datoteke za konfiguraciju web poslužitelja sa IPv6 adresom

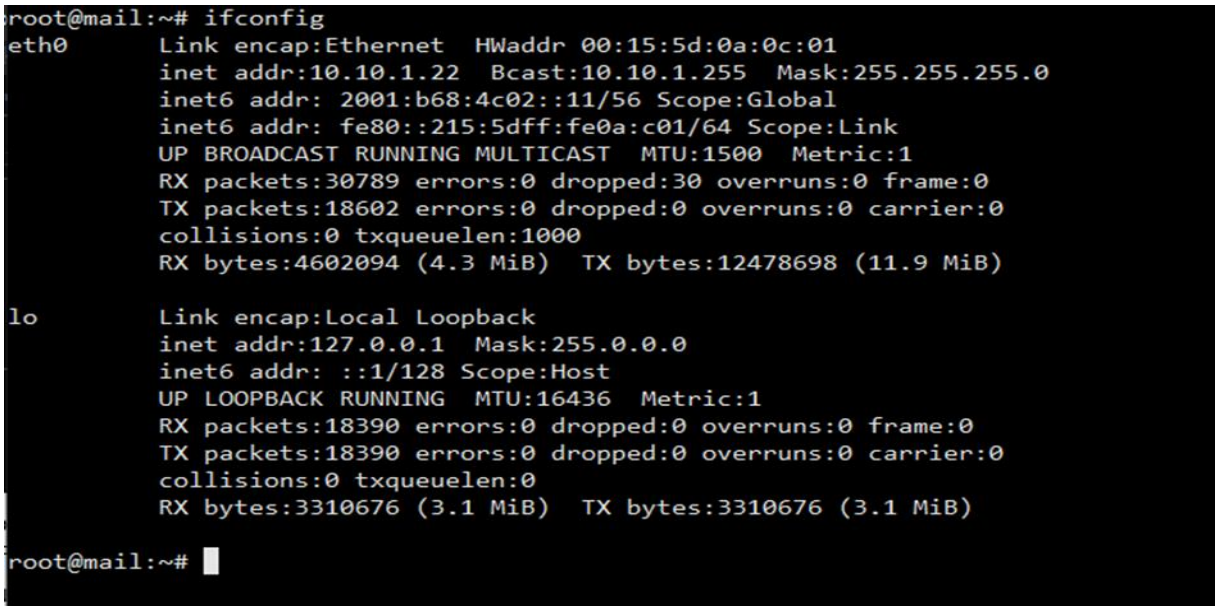


Izvor: Autor

Dosadašnjoj adresi 10.10.1.22 koja se pomoću NAT translatira na 161.53.146.197, dodana je statična IPv6 adresa 2001:0B68:4C02:0000:0000:0000:0000:0011 i usmjerivač (gateway) 2001:B68:4C02::1.

Nakon ponovnog pokretanja mrežnih servisa, adresa je uspješno konfigurirana što se vidi na slijedećoj slici 18.

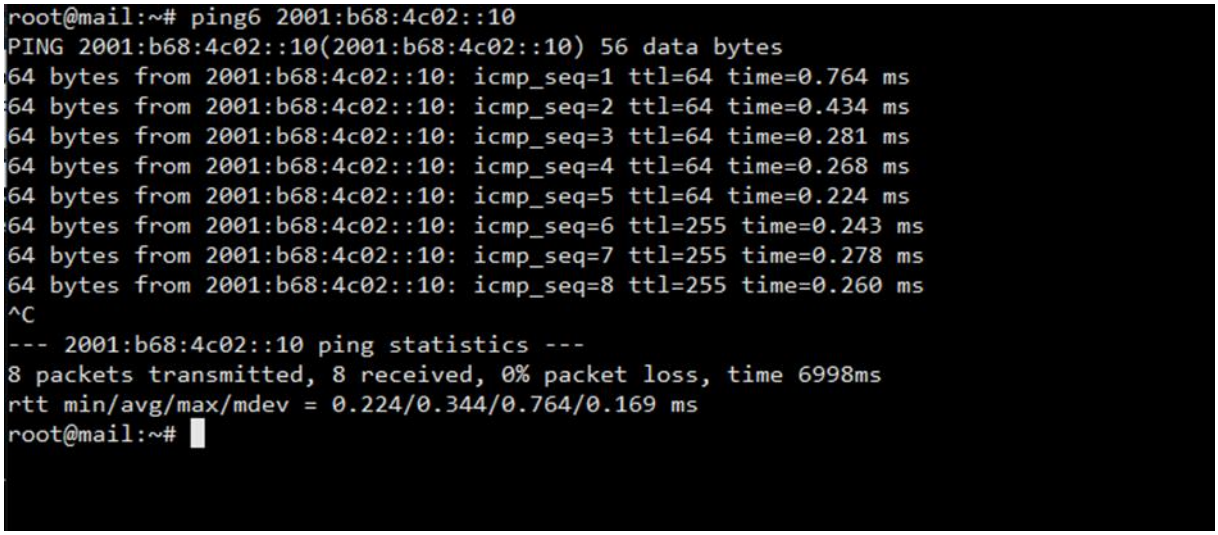
Slika 18. Prikazuje uspješno konfiguriranu adresu web poslužitelja



Izvor.Autor

U ovom koraku uspješno smo konfigurulali web poslužitelja, sada moramo provjerit dali se komunikacija ostvaruje između njega i konfigurirane IPv6 adrese.

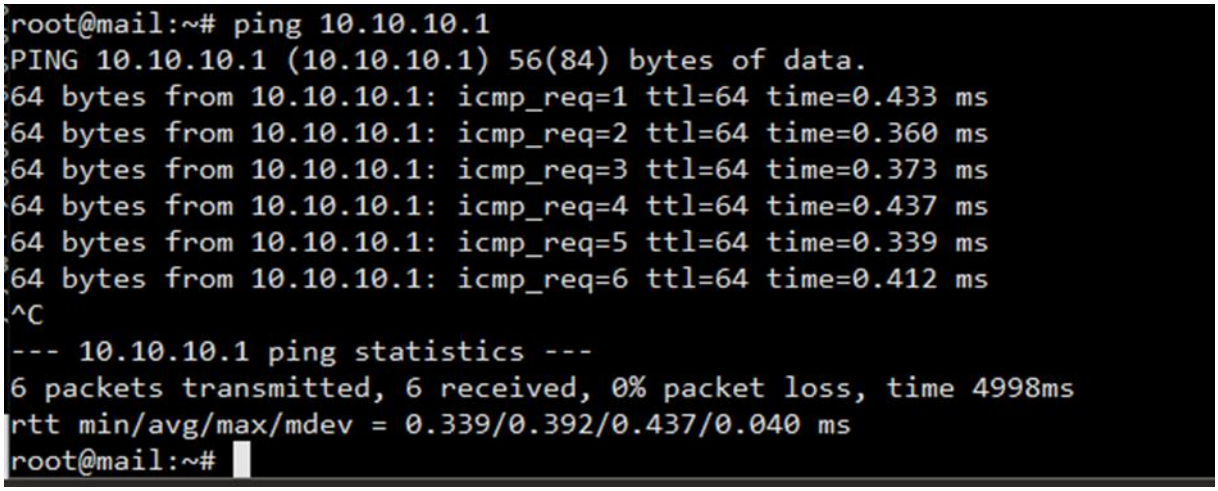
Slika 19. Prikazuje uzpješno konfiguriranje pomoću naredbe „ping6 2001:b68:4c02: :10“



Izvor: Autor

Kada smo implementirali IPv6 adresu u našeg web poslužitelja i provjerili dali ona funkcionira, treba provjerit dali smo narušili funkcioniranje IPv4 adrese. To možemo učinit kao i kod provjere za IPv6 samo umjesto IPv6 adrese upišemo IPv4 kao što je prikazano na slici 20.

Slika 20 prikazuje uspješno pinganje IPv4 adrese



Izvor:Autor

Nadalje, može se postaviti autokonfiguracija klijenata te se sva računala u ustanovi mogu adresirati pomoću IPv6 protokola, čime se otvaraju mnoge mogućnosti te povećava broj uređaja koji se mogu direktno spojiti na mrežu.

Konfiguracija DNS-a

Kako bi klijentska računala mogla u potpunosti koristiti pristup Internetu, potrebno je postaviti i DNS sustav na IPv6. Za sada se koriste CARNetovi javni DNS servisi sa adresama: 2001:b68:ff:1::3 i 2001:b68:ff:2::3. Kao i uvijek u DNS-u se dodaju dva poslužitelja radi redundancije.

Za DNS Istarskog veleučilišta koristit će se dosadašnji servis BIND na adresi 161.53.146.195 a kome će se dodijeliti IPv6 adresa 2001:0B68:4C02:0000:0000:0000:0000:0005/56.

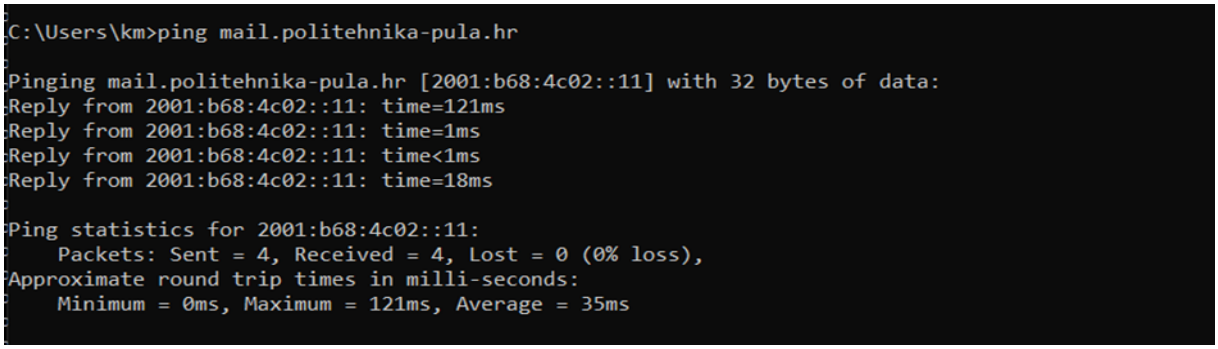
DNS zapis je ovakvog formata na primjeru mail poslužitelja:

mail.politehnika-pula.hr. IN AAAA 2001:B68:4C02::11

mail.politehnika-pula.hr. IN A 161.53.146.197

A označava IPv4 a AAAA IPv6 verziju protokola.

Na slici 21. Prikazano je uspješno pinganje kojem se klijent obraća dns-u preko IPv6 protokola



Izvor:Autor

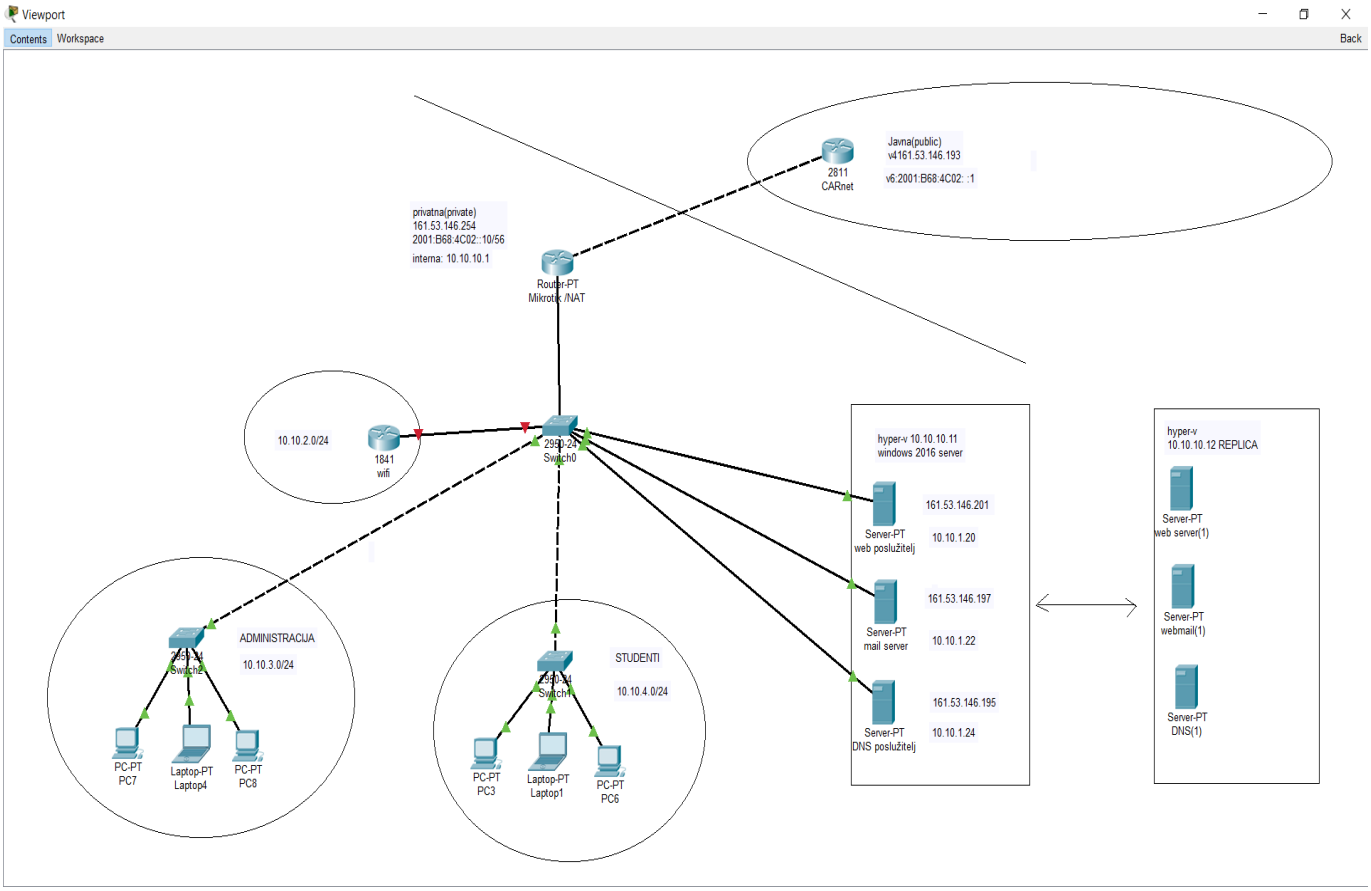
Sa slike možemo zaključiti kako su poslana 4 paketa sa ukupnom veličinom od 32 bajta, možemo isčitati njihovo vrijeme dolaska od klijenta do poslužitelja te uspješnost slanja odnosno dali siu svi paketi poslani ili su izgubljeni u prijenosu.

Umjesto dosadašnjeg protokola DHCP za raspodjelu i automatsko upravljanje IP adresama, u IPv6 domeni koristi se SLAAC -Stateless Autoconfiguration Protocol no taj dio nije obuhvaćen ovim radom

Kako bismo testirali našu mrežu, simulirali uvođenje IPv6 mreže te vizualizirali si cijeli sustav koristit ćemo program 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.[15]

Slika 22. Prikazuje simuliranje mreže na Istarskom Veleučilištu



Izvor:Autor

Kao što je prikazano na slici 22. Poslje svih konfiguracija i uvođenja IPv6 protokola u mrežu Istarskog Veleučilišta značajno smo poboljšali internetsku uslugu kao i sigurnost svih podataka koji se nalaze u internoj mreži IV-a. Svjetlo siva kosa linija označava odvajanje unutarnje i vanjske mreže odnosno interne mreže na IV i vanjske, nadalje za komunikaciju između IPv4 i IPv6 koristi se dual-stuck metoda i NAT unutar IV. Sa slike možemo vidjet kako se komunikacija ostvaruje između svih uređaja, IV kosristi virtualne servere pomoći hyper-v –a(windows server virtualization) koji ima svoj replicirajući dio kao sigurnost za sve podatke koji se nalaze i za provjeru svih podataka.

[15] <https://www.filehorse.com/download-cisco-packet-tracer-32/>,(10.8.2019)

7. ZAKLJUČAK

U ovom završnom radu opisane su osnovne značajke IPv4 i IPv6 protokola. Naročito je dana pažnja nedostacima Ipv4 protokola uslijed porasta broja korisnika Interneta.

Jedan od najvećih problema je nedovoljan broj Ipv4 adresa koji je rezultat samog dizajna Ipv4 protokola. Prikazan su rješenja

U konačnici, nova verzija protokola pod nazivom Ipv6 sa novim značajkama i poboljšanim karakterisikama u odnosu na postojeći IPv4 protokol adresiraju i rješavaju upravo te probleme. Iako Ipv6 protokol nije dovoljno raširen, potrebno je pripremiti infrastukturu za njegovo uvođenje.

Osim problematike adresiaranja, Ipv6 protokol rješava i sigurnosne probleme koji nisu bili predviđeni Ipv4 protokolom.

Ispravnim i pravovremenim planiranjem, moguće je implementirani Ipv6 protokol na postojeć infrastrukturu što smo kroz ovaj rad i pokazali.

8. LITERATURA

Knjige :

1. Joseph Davies: Understanding IPv6, Third edition, O'Reilly Media, Inc. North Sebastopol, California 2012.
2. Silvia Hagen, IPv6 Essentials, 2nd edition, O'Reilly Media, Inc. North Sebastopol, California 2006.
3. Bažant, Alen; et al: Osnove arhitekture mreža, Element, Zagreb, 2004

Internet :

1. Arin <https://www.slideshare.net/TeamARIN/internet-operations-and-the-rirs>
2. Google <https://www.google.com>
3. Politehnika Pula <http://edu.politehnika-pula.hr/racunalne_mreze/cna/course/module8/index.html#8.1.2.1>
4. Eldis Mujarić, dipl. ing. <http://mreze.layer-x.com/s030101-0.html
5. https://www.utilizewindows.com/the-difference-between-unicast-multicastand%20broadcast-messages/
6. https://study-ccna.com/what -is-nat/
7. Tomislav Volarić,razlika između Ipv4 i Ipv6, <http://tvolaric.com/preuzimanja/IPv4vsIPv6.pdf>
8. Margaret Rouse, IPv6<https://searchnetworking.techtarget.com/definition/IPv6-Internet-Protocol-Version-6>,
9. IETF< https://www.ietf.org/ >,
10. CIS <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf>
11. Internet society https://www.internetsociety.org/wp-content/uploads/2018/06/2018-ISOC-Report-IPv6-Deployment.pdf
12. CARNET https://www.carnet.hr/o-carnet-u/
13. File horse https://www.filehorse.com/download-cisco-packet-tracer-32/

9. POPIS SLIKA

10. POPIS TABLICA