Barijere usvajanja IPv6 protokola

Bačac, Danijel

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Danijel Bačac

Barijere usvajanja IPv6 protokola

Završni rad

Pula, 2023 godina.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Danijel Bačac

Barijere usvajanja IPv6 protokola

Završni rad

Ime Prezime, JMBAG: Danijel Bačac, 0145029684

Studijski smjer: Informatika

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: izv. prof. dr. sc. Snježana Babić

Pula, 2023 godine

Sadržaj

1. Uvod

IPv6 predstavlja sljedeću generaciju internet protokola omogućujući više adresa i veću sigurnost u odnosu na IPv4 verziju. Iako se ova tehnologija pojavila prije nekoliko desetljeća, još uvijek nije u potpunosti implementirana na globalnoj razini. U fokusu ovog rada kao i glavni cilj je analiza višestrukih čimbenika koji koče, ometaju i usporavaju proces implementacije IPv6 tehnologije. U svrhu postizanja tog cilja, provedena je dubinska analiza tehničkih, ekonomskih i organizacijskih aspekata koji su pridonijeli usporenom prihvaćanju IPv6 tehnologije. Na taj način, rad pruža uvid u kompleksne faktore koji usporavaju sveobuhvatniju implementaciju, pomažući u boljem razumijevanju izazova s kojima se industrija suočava u ovom procesu. Koristeći interdisciplinarni pristup analizi, kombinirajući tehničke podatke s društvenim i ekonomskim kontekstom, kako bismo dobili sveobuhvatan uvid u ovaj kompleksan problem s ciljem razumijevanja glavnih prepreka koje ometaju širu i bržu integraciju u globalnu mrežnu infrastrukturu. Također istraženi su primjere iz prakse i inicijative koje su uspješno doprinijele bržem usvajanju IPv6 tehnologije, kako bi se dobila cjelovita slika o izazovima i mogućim rješenjima u vezi s implementacijom IPv6. U tom kontekstu u šestom poglavlju dodatno su razrađene migracijskih tehnologija te metodologija same migracije na novi protokol kao i načini na koje su organizacije i mrežni arhitekti nastojali prevazići ove prepreke kako bi omogućili sveobuhvatnu integraciju IPv6 u svakodnevnu upotrebu.

Nakon što je pokrenut World IPv6 Launch (2011), još uvijek smo na tek nešto više od četvrtine dostupnosti novog internetskog protokola. Ali ako to nije bilo dovoljno loše, unatoč dosta publiciteta oko nadolazećeg iscrpljenja IPv4 adresa tijekom godina, najnoviji podaci pokazuju da čak i ta neimpresivna razina rasta usporava navodi McCarthy (2018). Detaljnija analiza usvojenosti IPv6 protokola, kako na globalnoj tako i na razini Hrvatske, razrađena je u trećem poglavlju ovog rada.

Iako je to nedvojbeno sljedeća faza u evoluciji mrežnih tehnologija i predstavlja budućnost internetskog povezivanja potpuna implementacija protokola verzije 6 još je uvijek više daleka budućnost, nego bliska stvarnost. Istraživanjem trendova o upotrebi

i razvoju tehnologija koje se oslanjaju na IPv6 ključno je za procjenu dugoročne održivosti. Kroz analizu trenutnih trendova, dinamike prelaska i povezanosti dodatno je u sedmom poglavlju istražena perspektiva i budućnosti ovog protokola. Analiza budućnosti IPv6 protokola zahtjeva sagledavanje trenutnog stanja njegove implementacije i razumijevanje ključnih trendova i faktora koji oblikuju usvajanje i budućnost IPv6 protokola.

IPv6 zahtijeva značajno ulaganje i pomno planiranje kako bi postao potpuno funkcionalno rješenje. U ovom trenutku IPv6 tek polako počinje utjecati na poslovni prostor, prvenstveno zato što je cijenu i složenost implementacije IPv6 do sada bilo teško opravdati. Zbog toga su u četvrtom poglavlju dodatno analizirane prednosti koje IPv6 donosi. U drugom poglavlju obrađeni su ključni razlozi za njegovo korištenje kako bismo dobili sveobuhvatan uvid u ovu važnu tehnologiju i opravdali pa možda i potakli njegovu implementaciju. Sam prijelaz na IPv6 nije tako jednostavan. IPv6 je zapravo potpuno novi način komunikacije, i s time dolazi krivulja učenja za mrežne administratore i mrežne arhitekte.

Uvođenjem novog protokola pojavljuje se potreba za dvostrukom konfiguracijom, budući da IPv6 nije unatrag kompatibilan s IPv4. Dio rada fokusirati će se na izazove koji se javljaju prilikom implementacije IPv6 protokola u postojeću IPv4 mrežu. Isto tako, istražene su strategije migracije, dual-stack pristup i mehanizmi prevođenja između protokola. Kompatibilnost između protokola predstavlja značajan izazov, posebno tijekom tranzicijskog razdoblja. Kada je IPv6 prvi put osmišljen, nije osmišljen da funkcionira paralelno s IPv4. Dakle, ako se koristi IPv6 adresiranje unutar mreže koja se strogo temelji na IPv4, mogu se pojaviti problemi s usmjeravanjem i DNS-om (eng. Domain Name System). Uz to ne nudi sav hardver i softver istu razinu funkcionalnosti IPv6. Mrežni hardver imao je teškoća s razmjerom IPv6 adresnog prostora – što je više problem za ISP-ove i proizvođače opreme nego za normalne kućne/privatne korisnike gdje velika većina nema potrebu za implementacijom IPv6 (Conry-Murray, 2011).

Poslovni korisnici u današnjem poslovnom okruženju, također igraju važnu ulogu u usvajanju IPv6 tehnologije. Holder (2018) ističe kako otpornost poduzeća na veliku migraciju IPv6 općenito usporava usvajanje. Peto poglavlje pruža detaljan uvid u složenost problema koji koče usvajanje IPv6 tehnologije u velikim organizacijama i

poduzećima te ponuditi smjernice za prevladavanje tih izazova. Analizom različitih faktora možemo stvoriti bolje razumijevanje usvajanja IPv6 protokola u suvremenom poslovnom okruženju. Analizirane su i ključne prepreke koje su doprinijele postojećem stanju, uključujući tehničke izazove, financijske aspekte, nedostatak svijesti i edukacije te utjecaj postojeće IPv4 infrastrukture.

Uvođenje IPv6 djelom je usporeno radi prijevoda mrežnih adresa (NAT-a), koji privatne IP prevodi u javne adrese. “Ali inercija, plus činjenica da je, kao što je navedeno, raširena upotreba NAT-a spriječila IPv4 apokalipsu, sam prijelaz možda neće biti gotov do 2030. ili kasnije” (Fruhlinger,2022). Iako većina mrežnih administratora zna da je migracija neizbježna, nitko ne želi nužno biti pionir ako postoji rizik nastanka problema na vlastitoj mreži ili aplikacijama. “Poduzeća percipiraju IPv6 kao tehnologiju koja im daje upravo ono što imaju danas; Internet, ali uz povećanu cijenu i rizik” (Holder, 2018) . Iako većina korisnika razumije da IPv6 posjeduje ogroman adresni prostor, nasuprot tome, adresni prostor IPv4 protokola je izrazito ograničen i u potpunosti iscrpljen,na žalost većina ne vidi razliku između interneta temeljenog na IPv4 protokolu i interneta temeljenog na IPv6 protokolu. Iscrpljenost IPv4 adresa izravno utječe samo na podskup poduzeća. Međutim, neizravni utjecaj iscrpljenosti utječe na sve organizacije i nove tehnologije. Opseg ovog utjecaja ovisi o tome kako organizacije koriste internet i koliko je on važan za njihovo poslovanje i budući razvoj.

Kroz analizu troškova, tehničkih izazova te sigurnosnih aspekata, ovaj rad doprinosi boljem razumijevanju kompleksne dinamike koja utječe na usvajanje IPv6 tehnologije te uvid u prednosti i izazove koje donosi prijelaz na IPv6.

2. IPv6 protokol i razlozi korištenja

Nagli rast digitalne tehnologije, nadogradnja raznovrsnih konfiguracija i tehnologija u računalima, mobilnim uređajima te bežičnim uređajima doveli su do veće potražnje za IP adresama. S rastom interneta, pojavila se potreba za povezivanjem sve većeg broja ljudi i uređaja, što je dovelo do rasta problema i postavljanja zahtjeva koji su sve veći i zahtjevniji. Internet protokol verzije 6, ili kraće IPv6 predstavlja se kao zamjena za IPv4 koji se do sada smatrao temeljem suvremenog interneta. IPv6 je stvoren kao potpuno nova verzija protokola s većim adresnim prostorom kako bi prevazišao iscrpljenost IPv4 adresa i osigurao mogućnost daljnjeg rasta interneta. Ograničenja IPv4, činila su osnovu za razvoj i standardizaciju IPv6 protokola koja je definirana u RFC8200 dokumentu (Hinden, 2017).

Protokol IPv4 doveo nas je daleko, ali sa svojim ograničenim brojem adresa, prošao je svojim tijekom. Povezivanje sve većeg broja ljudi i uređaja postaje sve teže, a IPv6 je neophodan ako želimo nastaviti širenje i razvoj interneta i njegovih mogućnosti, što se istovremeno nameće kao glavni motiv za tranziciju na IPv6. Osim proširenog adresnog prostora koje pruža IPv6 otvorila se i mogućnost za ispravkom nedostataka koji su limitirali IPv4 protokol.

Rješenje se nameće u obliku nove strukture paketa i adresa koji uz povećanje broja bitova donosi i mnoga druga rješenja koja efikasno rješavaju probleme koji su vezani uz IPv4 verziju. Kroz proširenje adresnog prostora, unaprijeđeno adresiranje i optimizirane performanse, glavni fokus je usmjeren na optimizaciju usmjeravanja paketa i prilagodljivost novim zahtjevima modernog digitalnog doba. “Iako su protokolu IPv4 dodane nove tehnike sa svrhom uštede adresnog prostora: VLSM -*eng. Variable Length Subnet Mask* (Manning, 1995), CIDR - *eng. Classless Interdomain Routing* (Varadhan, 1993), privatne adrese i NAT - *eng. Network Address Translation* (Holdrege, 1999), to nije dovoljno. VLSM i CIDR povećavaju fleksibilnost dodijeljivanja IP adresa, a NAT smanjuje potrebu za javnim IP adresama. Te tehnike pomažu, ali dugoročno nisu rješenje problema.” (“Introduction to IPv6”, bez dat.). Dalje su navedeni i obrađeni ključni razlozi zbog kojih se javila potreba za IPv6 protokolom.

Nedostatak Ipv4 adresa

IPv4 je skraćenica za “Internet Protocol version 4” nastao je 1974. godine, te još uvijek prevladava internetskim prometom i prostorom. “Izvorni format za IP adrese, s 32-bitnim proširenjem dopušta definiranje internetskog adresnog prostora koji ima 4.294.967.297 mogućih IP adresa.” (Gerometta, 2010). Ta se brojka činila doista ogromnom u 1970-ima i 1980-ima godinama kada je bilo relativno malo uređaja koji su se mogli spojiti na internet. No sada, ne samo da većina ljudi ima više računala spojenih na internet, već postoje i pametni automobili, pametni televizori, pa čak i pametni hladnjaci, kojima je potrebna IP adresa za komunikaciju.

Prema Bowmanovim (2020) predviđanjima, s milijardama dodatnih novih uređaja za koje se predviđa da će se povezati s internetom u sljedećih pet godina, postalo je evidentno da velićina IPv4 adresnog prostora neće biti dovoljno velika. U 2011. godine Međunarodna organizacija za dodjelu brojeva i imena na internetu (IANA) dodjelila je posljednji raspoloživi blok IPv4 adresa svojim regionalnim organizacijama koje dalje raspodjeljuju adrese . RIPE kao Europska organizacija za dodjelu javnih adresa izvršilo je posljednju dodjelu IPv4 adresa 2020. godine i službeno je ostala bez adresa. Ostala četiri značajna registra nestala su prije nekoliko godina. Registri su organizacije koje dodijeljuju adresne blokove pružateljima internetskih usluga (ISP), dok ISP-ovi imaju skupove adresa koje oni, zauzvrat, dodijeljuju svojim klijentima.

Širokopojasne veze

Porast Dial-up i ADSL/VDSL veza povećao je drastično stopu potrošnje adresa. Svaki usmjerivač (eng. router), koji se povezuje na na Internet zahtjeva jedinstvenu IP adresu za komunikaciju.

Neefikasna upotreba adresa

Prema navodima Hoffmana (bez dat.) IPv4 adresni prostor je loše dodijeljen, sa samo 14% svih dostupnih adresa u upotrebi, a razlozi su:

- Ranih osamdesetih dodijeljeno je mnogo više adresa nego što bilo je potrebno. U početku su neke velike tvrtke tražile (i dobile) vrlo velike blokove adresa kao i neki fakulteti kojima je dodijeljeno mnogo više adresa nego što su zapravo zahtijevali ili im je bilo potrebno. (“Što je IPv6?”, bez dat.)
- Veliki pružatelji usluga koriste puno IP adresa, na primjer kabelske tvrtke, Google ili Amazon koje su registrirale velike blokove adresa iako ih ne koriste u potpunosti
- Postojanje samo tri bloka IPv4 adresa (klase A, B i C) dovodi do ograničavanja IP adresnog prostora.
- Rezervirani adresni prostori: Klasa D i E se još ne koriste

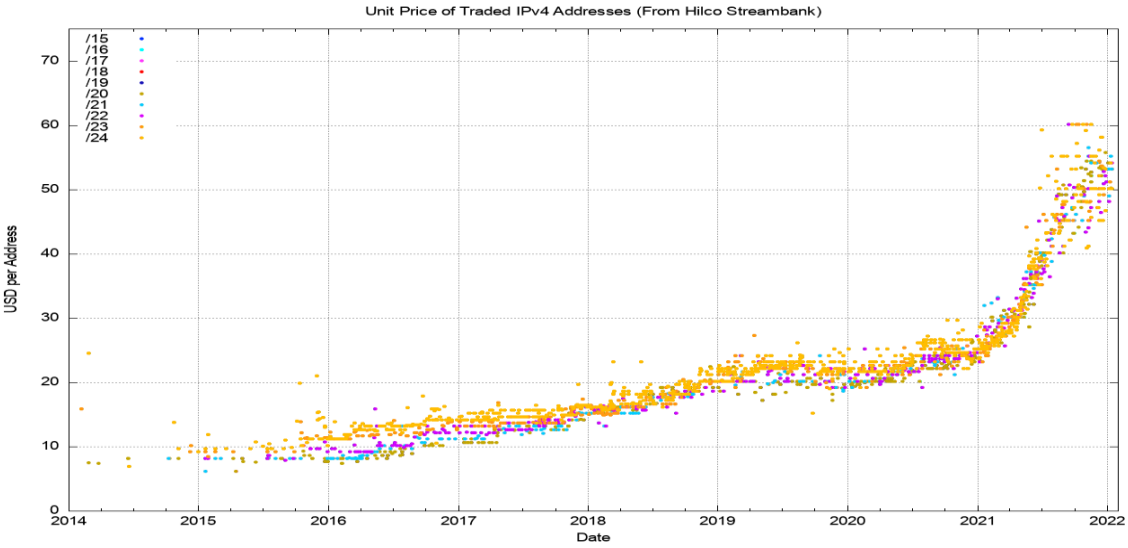
Mobilni uređaji

Kako je i mobilna tehnologija napredovala pojavilo se i povećanje zahtjeva za pristupom na internet. Razvoj mobilne telefonije jako je utjecao na potrošnju IP adresa jer svaki mobilni uređaj koji pristupa Internetu zahtjeva svoju IP adresu za daljnju komunikaciju na mreži.

Porast cijena ipv4 adressa

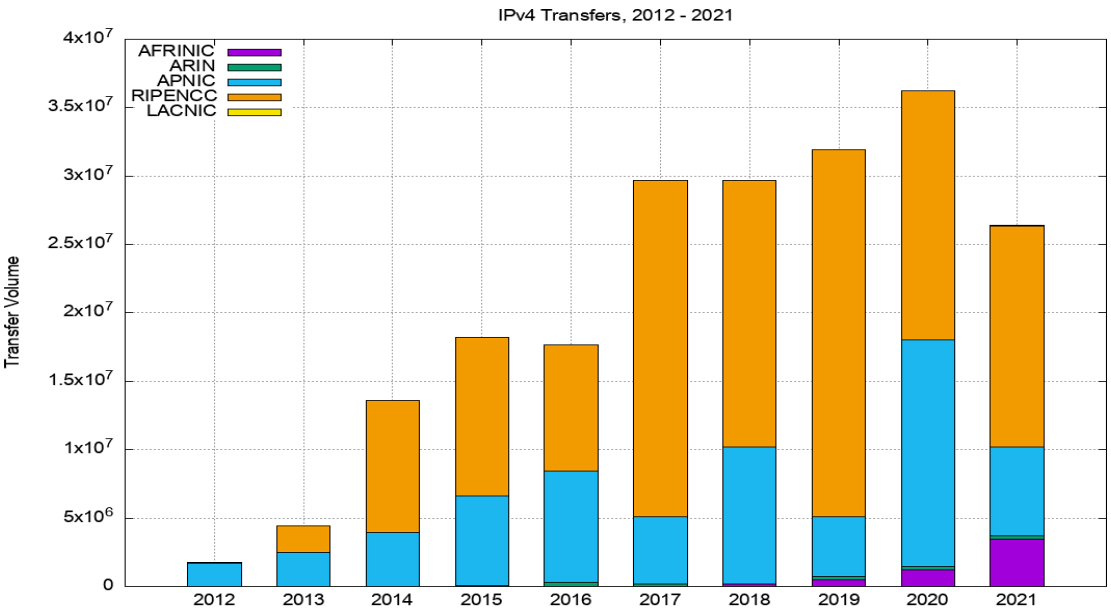
“Internet nije prestao rasti, a postoji kontinuirani priljev novih sudionika u mrežni prostor koji imaju potrebu za IPv4 adresama. Tako nastaje daljnji pritisak nad sve većom oskudicom IPv4 adresa, što se odražava u eskalaciji cijena na tržištima

prijenosa.” (Huston, 2022). Neizbježno, kako potražnja nadmašuje ponudu, a zalihe opadaju, cijene rastu. Prema analizi Hogewoning-a (2021) postoji vrlo jasan trend rasta cijena. Trenutno se cijene blokova od 256 (/24) adresa na online aukcijama prodaju od 40 do 60 dolara po adresi.



Slika 1: Porast cijena IPv4 adresa (https://ipv4.global/reports/, 2022)

Slika 1 prikazuje vremensko kretanje cijena IPv4 adresa u razdoblju između 2014. i 2022. godine. Zalihe na rabljenim IPv4 tržištima razmjene postaju sve manje i po nekim procjenama cijene za IPv4 adrese bit će još veće i do 100 USD po jednoj IPv4 adresi u bliskoj budućnosti (Huston, 2022). Novi korisnici prisiljeni su koristiti alternativno tržište IPv4 adresa tj. kupovati od preprodavača . “Na svim takvim tržištima ključna metrika je cijena robe kojom se trguje.” (Huston, 2022). Tako na slici 2 prikazano je kretanje i trgovanje IPv4 adresama u zadnjih 10 godina.



Slika 2: Trgovanje i prijenos IPv4 adresa (https://ipv4.global/reports/, 2012-2021)

“Prije ili kasnije, nedostatak IPv4 povećat će troškove sve dok ne premaše troškove implementacije IPv6. Konkurentno tržište će tada napraviti racionalan izbor i prijeći na učinkovitiji način proizvodnje i implementirati IPv6 .” (Hogewoning, 2021)

Cloud computing i povećanje prometa

Prema istraživanju Karimi (2019) očekuje se da će količina IP prometa generiranog u 2022. biti veća od prve 32 godine ukupnog internetskog prometa. Karimi (2019) dalje navodi kako dramatično povećanje prometa ima nekoliko izvora:

1. Eksplozija prometa M2M prometa (Machine-to-Machine) povezanih objekata (IoT) kao što su autonomna vozila, pametne električne mreže, industrijska automatizacija i sl. potaknut će povećanje globalnog internetskog prometa u rasponu od 3,1% do 6,4%.

2. Očekuje se da će se povećani IP promet koji generira SD-WAN (Software-defined Wide Area Network) povećati udio ukupnog IP WAN prometa s 9 % na 29 %, što se pretvara u 5,3 EB (Exabyta) IP prometa u 2022. godini
3. Povećana potražnja za Cloud computingom što zahtjeva veliko povećanje globalne serverske infrastrukture

IoT- Internet of Things

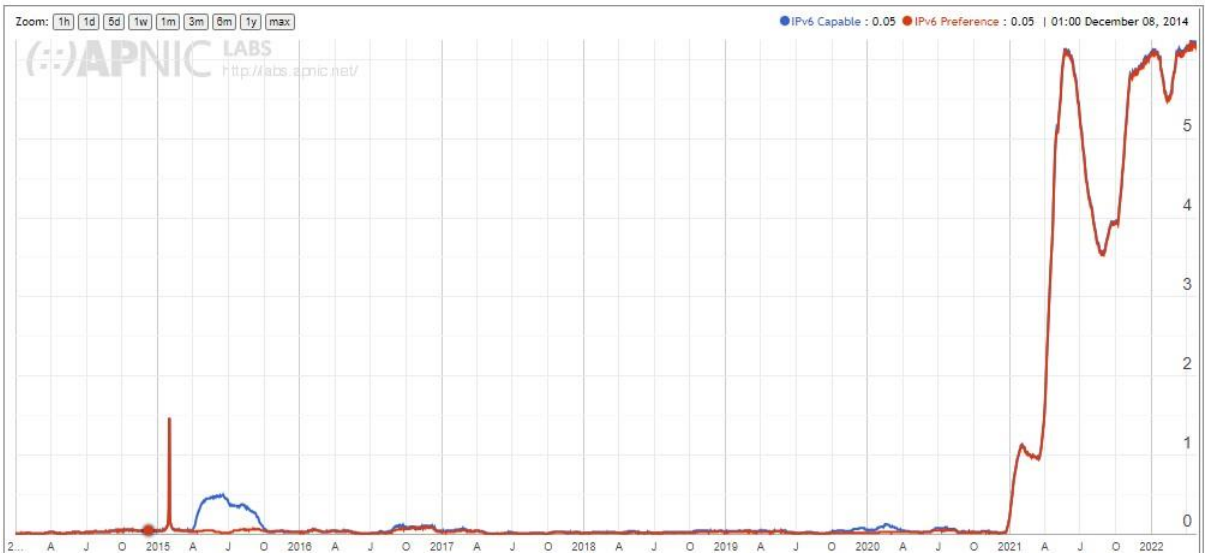
Novi se korisnici stalno priključuju mreži, prema procjeni 27.000 novih uređaja svakog sata. Predviđanja govore da će se broj IoT veza udvostručiti između 2021. i 2027. na 30 milijardi uređaja navodi Fitri (2022). IPv6 ima mogućnosti koje nedostaju IPv4, a koje ga čine povoljnim za implementaciju IoT-a. Svaka internetska krajnja točka treba numeričku IP adresu za komunikaciju s drugim uređajima. Pojava sve veće količine opreme i uređaja na mreži ukazuje na problem s ograničenim adresama IPv4 protokola. Primarna funkcija IPv6 je omogućiti stvaranje više jedinstvenih identifikatora TCP/IP adresa što omogućuje proširen adresni prostor koji podržava velike IoT mreže. To je jedan od glavnih razloga zašto je IPv6 tako važna inovacija za internet stvari. IPv6 se obično smatra ključnom tehnologijom koja omogućuje internet stvari, budući da može lako prihvatiti jako veliki broj pametnih uređaja koji se povezuju s internetom. No bez opsežnog globalnog usvajanja i uspješne implementacije IPv6 tehnologije kao primarne verzije internetskog protokola, IoT neće biti moguć ili će biti ograničen.

3. Korištenje IPv6 protokola

Prema istraživanju Hustona (2022) glavne web stranice i ISP-ovi omogućuju IPv6, a IPv6 internetsko društvo raste; međutim, ovaj rast nije tako gladak kao što je planirano. IPv6 je prvi put predstavljen 1995. Danas globalna prihvaćenost IPv6 ne doseže niti 40%. prema Googleovoj statistici usvajanja IPv6 na globalnoj razini dosegao je 34% do ožujka 2022. Statistika usvajanja IPv6 po zemljama pokazuje da Indija vodi sa 66%, dok je Njemačka na drugom mjestu s 49% usvajanja. 119 zemalja pokrenulo je implementaciju IPv6; međutim, ostali još nisu uveli IPv6 u svoje mreže ("Google collects statistics about IPv6 adoption", 2022). Postoji jasan napredak u usvajanju IPv6 u azijskim i južnoameričkim zemljama, dok afričke zemlje tek trebaju napraviti značajne iskorake. Vodeći indijski mobilni operater, na vrhu je popisa mrežnih operatera koji prihvaćaju IPv6 na globalnoj razini. U kolovozu 2021. bio je na 91,43% u prihvaćanju IPv6. Operater koji vodi usvajanje IPv6 u SAD-u, nalazi se na 6. mjestu s oko 91,21% IPv6 uvedeno u njihovu mrežu. Telekomi uvelike usvajaju IPv6, unatoč činjenici da su web poslužitelji još uvijek u ranoj fazi usvajanja IPv6. Zbog toga će IPv4 ostati neophodan resurs za krajnjeg kućnog korisnika interneta. Neke od najvećih telekomunikacijskih tvrtki u SAD-u već su uvele značajne IPv6 resurse u svoje mreže. Ovaj napredak dolazi iz puke potrebe i problema sa skalabilnosti uzrokovanih nedostatkom IPv4. Nažalost, tvrtke nailaze na probleme povezane s prevođenjem mrežnih adresa (NAT) i okruženjem s dvostrukom konfiguracijom. IPv6 sustav usmjeravanja privlači sve više pažnje operatera, a IPv6 mreža se dokazuje stabilnošću i performansama. Potrošački sektor nastavlja svoju ekspanziju IPv6 kako na glavnim tržištima Kine i Indije, tako i na brojčano manjim tržištima pa je tako na kraju 2020. oko 30% cjelokupnog web prometa bilo je preusmjereno putem IPv6 (Huston, 2022). Većina implementacije IPv6 događa u telekomunikacijskoj industriji, a mobilne mreže prednjače dok mnogi web poslužitelji još uvijek koriste IPv4. U vrijeme objave, statistika korištenja IPv6 kao elementa web-mjesta na webu pokazala je stopu usvajanja IPv6 od samo 19,4% ("Google collects statistics about IPv6 adoption", 2022).

Sa samo 5% IPv6 adresa u primjeni Hrvatska je uredno među zadnjima u Europi, uz Španjolsku, Srbiju, Albaniju i Sjevernu Makedoniju . Implementacija u

Hrvatskoj dugo je bila na niskih 0,5 % sve do prosinca 2020. kada je počeo rast što je vidljivo na slici 3.



Slika 3: IPv6 u Hrvatskoj (https://stats.labs.apnic.net/ipv6/HR, 2022)

Suočen s nedostatkom IPv4 adresa, jedan veći Hrvatski ISP počeo je testnu implementaciju IPv6 protokola . No sve dok najveći Hrvatski ISP-ovi ne počne nuditi potpune IPv6 usluge – dodijeljivanje IPv6 adresa krajnjim korisnicima, IPv6 omogućene hosting usluge itd., razina IPv6 prometa ostat će niska kao i sada (“Use of IPv6 for Croatia”, 2022).

4. Prednosti IPv6 protokola u odnosu na IPv4

IPv6 je najnovija verzija i šesta revizija internetskog protokola (IP) s 128-bitnim adresama te je ujedno i nasljednik IPv4 protokola. Standard za IPv6 objavio je IETF - Internet Engineering Task Force (1998.) koji ima 128-bitnu adresu. IPv6 koristi alfanumeričku metodu adresiranja koja se sastoji od osam grupa - a svaka grupa sadrži četiri heksadecimalne znamenke koje su međusobno odvojene dvotočkom. Takav format omogućuje veći adresni prostor i osmišljen je s ciljem za poboljšanje sigurnosti i konfiguracija. (“Što je IPv6?”, bez dat.)

IPv6 adresni prostor dovoljno je velik za buduću primjenu i zahtjeve, omogućuje 340 undecilion adresa, što bi trebalo biti dovoljno za doglednu budućnost navodi Hogewoning (2021).

Protokol je proširen na 40 okteta i pruža mogućnost za dodatnog proširenje u budućnosti bez izravnog utjecaja na temeljnu strukturu paketa. Identifikator je jedinstven unutar host dijela podmreže. Podijeljen je u osam skupina sačinjenih od šesnaest bitova gdje je svaka skupina pojedinačno razdvojena s dvotočkom. (Što je IPv6?, bez dat.)

Uspoređujući s IPv4 protokolom, IPv6 ima pojednostavljenu strukturu i format samog zaglavlja, čime se postiže jednostavnije i efikasnije usmjeravanje paketa. Ovakva jednostavnost zaglavlja direktno se reflektira na poboljšanje kvalitete usluge (QoS). Uz lakšu administraciju nudi i integriranu podršku za provjeru autentičnosti i zaštitu privatnosti u samom protokolu. (“IPv4 vs IPv6: Budućnost Internet protokola”, 2019)

U IPv6 mreži više nema potrebe za prevođenjem mrežnih adresa što uklanja mogućnost kolizija između privatnih adresnih prostora. Pojednostavljena arhitektura zaglavlja i operacije protokola znače smanjene operativnih troškova. Ugrađene sigurnosne značajke pružaju jednostavnije i efikasnije sigurnosne modele koje nedostaju u mnogim IPv4 mrežama. Iako, možda najznačajnije poboljšanje je autokonfiguracijska značajka koju podržava IPv6, jer upravo ona znači još snažniju „plug and play“ mrežnu konekciju. Autokonfiguracija uvelike olakšava rad korisnicima

te omogućuje povezivanje različitih uređaja na mrežu. (“Dostupnost IPv4 adresa smanjila se na ispod 10%”, 2010). Na slici 4 vidljiv je primjer zapisa IPv4 i IPv6 adrese.

VERSION	BITS	EXAMPLE
IPv4	32	72.75.123.123
IPv6	128	2600:1:950f:aaaa:1234:abcd:1212:abab

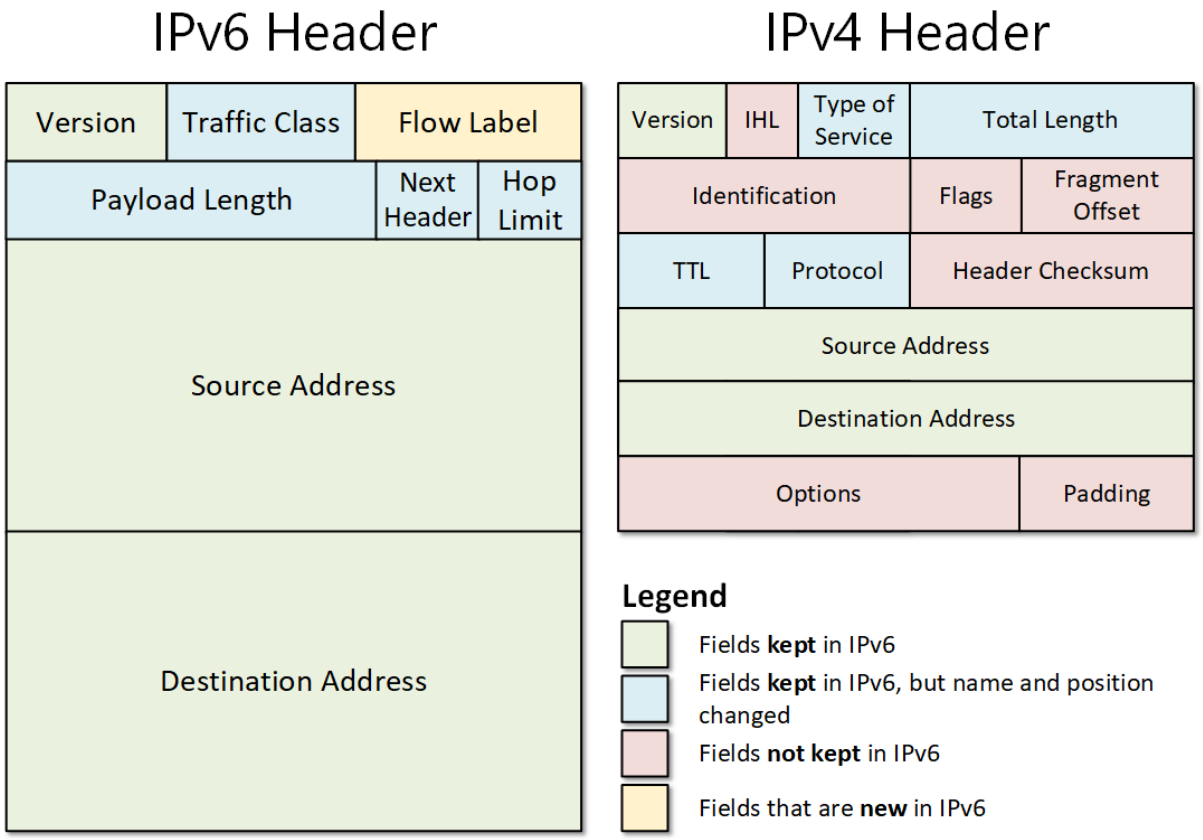
Slika 4: Primjer IPv4 i IPv6 adrese (Bowman, 2020)

Značajne prednosti IPv6 protokola su (Hinden, 2017):

- veći adresni prostor
- učinkovitija obrada pakete
- veće performanse i pruža veću podrška za prioritetnu isporuku paketa
- autokonfiguracija
- konfiguracija adresa u odsutnosti ili prisutnosti DHCP poslužitelja
- unaprijeđeno usmjeravanje paketa
- pojednostavljeno, učinkovitije usmjeravanje (routing)
- omogućava uređajima s privatnim IP adresama direktnu komunikaciju s uređajima koji posjeduju javne IP adrese
- podršku za upravljanje kvalitetom usluge (eng. Quality of Service)
- nema potreba za NAT-om (Network Address Translation)
- pokretljivost - omogućava uređajima u pokretu promijenu položaja i identifikacijsku adresu bez prekida veze
- mogućnost označavanja tokova na paketnoj razini (Flow Label)- paketi koji pripadaju istom toku mogu se označiti
- provjera autentičnosti i zaštita privatnosti unapređuju integritet i povjerljivost informacija.

4.1. Jednostavnije zaglavlje

Zaglavlje u IPv4 verziji protokola sastavljeno je od dvanaest osnovnih (slika 5) i dodatnih opcionalnih polja (Options). Osnovno dio zaglavlje zauzima dvadeset okteta dok je polje opcije varijabilne dužine. Dok kod protokola verzije 6 zaglavlje ima duljinu od četrdeset okteta i smanjen je broj polja na osam što čini procesuiranje paketa unutar usmjernika (rutera) mnogo brže.



Slika 5: Usporedba IPv4 i IPv6 zaglavlja (https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6, bez dat.)

Polja koja se nalaze u IPv6 zaglavlju (“Introduction to IPv6 “, bez dat.):

Verzija (Version) – Četverobitno polje označava verziju IP protokola.

Klasa prometa (Traffic Class) – ovo polje ima sličnu funkciju kao i u IPv4 verziji - “vrsta usluge” (eng. Type of Service). Ovo polje nam omogućuje dodjelu prioriteta prilikom isporuke paketa. Dužina polja je četiri bita što dopušta definiranje šesnaest različitih vrsta prometa.

Oznaka toka (Flow Label) – polje dužine 24 bita. Ovo polje omogućuje hijerarhijsko razvrstavanje paketa po prioritetu.

Dužina podataka (Payload Length) –označava dužinu podataka (izraženih u oktetima).

Sljedeće zaglavlje (Next Header) – je polje koje označava vrstu sljedećeg zaglavlja ili proširenja

Maksimalni broj čvorova (Hop Limit) –definira koliko skokova jedan paket može proći kroz mrežu prije nego je odbačen.

Ishodišna adresa (Source Address) – je identifikator koji označava izvorni uređaj s kojeg je paket poslan.

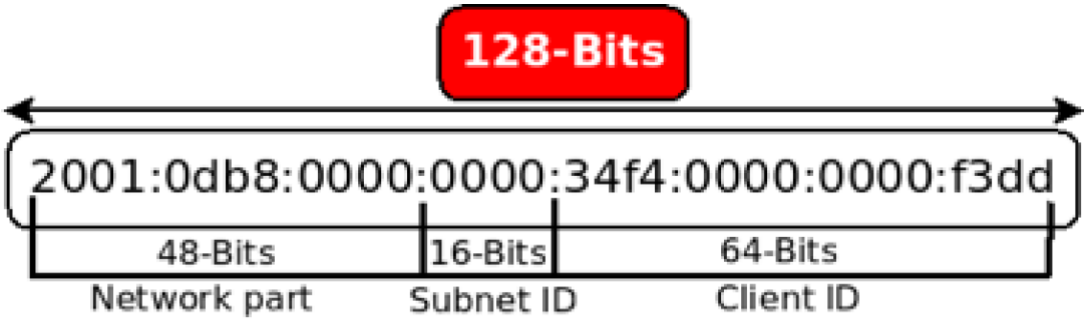
Odredišna adresa (Destination Address) – je identifikator koji označava krajnji uređaj tj. konačnog primatelja

Zaglavlje proširenja (Extensions Headers) – je dodatno fleksibilno polje koje omogućava unišenje dodatnih informacije unutar samog paketa, kao npr. fragmentacija ili enkripcija.

Uvođenje zaglavlja proširenja omogućuje implementaciju izbornih informacija u IPv6 pakete mnogo učinkovitije nego s IPv4. Budući da usmjerivači na putu isporuke paketa ne obrađuju zaglavlja proširenja IPv6, s IPv6, ona se čitaju samo na odredištu, što znači značajno poboljšanje performansi usmjerivača. (“Introduction to IPv6 “, bez dat.)

4.2. IPv6 adresiranje

Primjer osnovnog formata IPv6 adrese vidjiv je na slici 6:

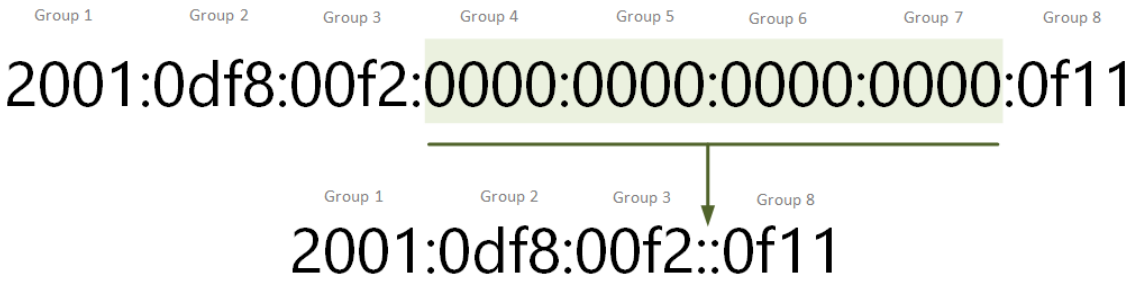


Slika 6: Primjer IPv6 adrese (https://www.redhat.com/sysadmin/what-you-need-know-about-ipv6, 2019)

Svaka IPv6 adresa (slika 6) sastoji se od 8 blokova, gdje svaki pojedinačni blok sadrži 4 heksadecimalne znamenke i razdvaja se znakom ":" (dvotočkom). Način prikaza adrese varira ovisno o kombinaciji brojeva i slova unutar adrese kako bi se pojednostavila notacija.

Pravila notacije IPv6 adrese ("Introduction to IPv6", bez dat.):

- kako bi se smanjila duljina adresa, može se izostaviti vodeće nule iz svakog bloka
- jedan ili više uzastopnih blokova koji sadrže samo nule možete zamijeniti s dvostrukom dvotočkom (::). Ovaj skraćeni oblik može se koristiti samo jednom unutar adrese, primjer notacije prikazan je na slici 7.

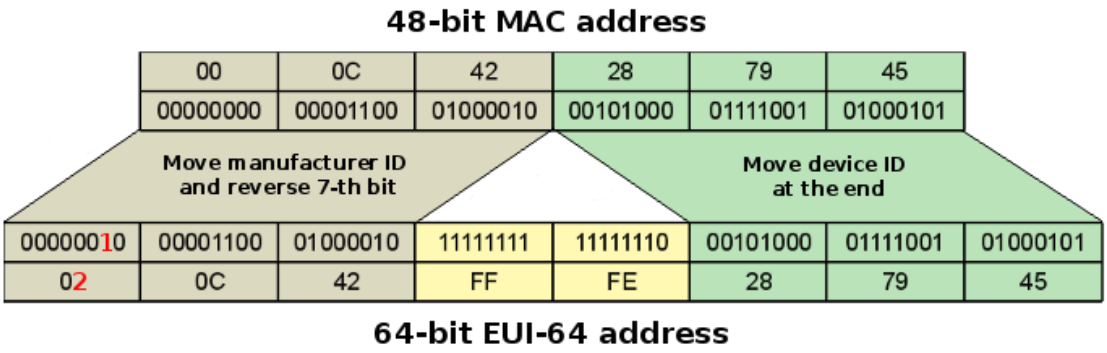


Slika 7: Primjer notacije IPv6 adrese (https://www.networkacademy.io/, bez dat)

Identifikator sučelja

Interface identifier predstavlja jedinstveni 64 bitni dio adrese koji se nalazi na kraju IP adrese, a koristi se za identifikaciju sučelja. Identifikator sučelja omogućava jedinstveno prepoznavanje i razlikovanje pojedinačnih uređaja ili sučelja unutar iste mreže. Interface Identifier omogućava mrežnim uređajima dinamičko generiranje svog identifikatora koristeći svoje fizičke adrese na podatkovnom sloju. Primjerice, u slučaju Ethernet sučelja, temelji se na MAC adresi.

Slika 8 prikazuje dinamičko stvaranje host djela IPv6 adrese na temelju MAC adrese.



Slika 8: Dinamička podjela MAC adrese (https://wiki.mikrotik.com/wiki/Manual:IPv6/Address, 2020.)

Generiranje IPv6 adrese iz MAC adrese mrežnog sučelja uključuje postupak poznat kao EUI-64 (Extended Universal Identifier) metoda. Ovaj proces zahtijeva podjelu 48-bitne MAC adrese na dva dijela, umetanjem niza FFFE između dvije polovice i postavljanje sedmog bita u prvom oktetu na 1 kako bi se označio EUI-64 format.

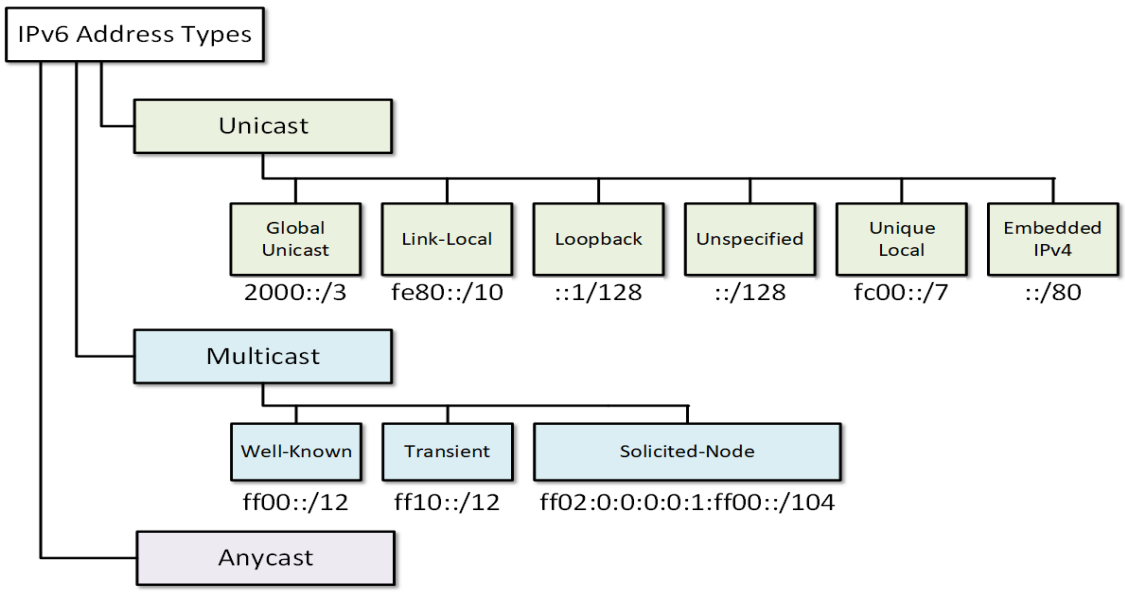
Rezultat ovog postupka čini zadnjih 64 bita IPv6 adrese, koja zajedno s prefiksom koji označava mrežu formira punu IPv6 adresu. (“Introduction to IPv6”, bez dat.)

Osnovni tipovi IPv6 adresa

Osnovni tipovi Ipv6 adresa identificiraju se po početnim brojevima adrese (“IPv6 Address Types”, bez dat.):

1. jednoodredišna adresa (unicast) – može biti lokalna i globalna, jedinstvena adresa uređaja na mreži. Omogućavaju komunikaciju između jednog pošiljatelja i jednog primatelja
2. višeodredišna adresa (multicast) – omogućavaju slanje podataka prema više primateljima istovremeno
3. najbliža zajednička adresa (anycast) - adrese koje se dodjeljuju na više sučelja unutar mreže. Paket koji je poslan na anycast adresu usmjerava se na najbliže sučelje koje ima tu adresu.

Na slici 9 grafički su prikazani osnovni tipovi IPv6 adresa.



Slika 9: Tipovi IPv6 adresa (https://www.networkacademy.io/ccna/ipv6/ipv6-address-types, bez dat.)

4.3. Dodjela IPv6 adresa

Pridruživanje IPv6 adresa uređajima moguće je na 3 načina:

- ručno
- autokonfiguracija
- pomoću DHCPv6 poslužitelja

Samostalna autokonfiguracija

U osnovi plug-and-play umrežavanje, IPv6 Stateless Address autokonfiguracija je jedna od najzanimljivijih i potencijalno najvrjednijih značajki adresiranja u IPv6. Ova značajka omogućuje uređajima na IPv6 mreži da se neovisno konfiguriraju pomoću stateless protokola. Svaki usmjernik periodično ili na zahtjev drugih uređaja oglašava 64-bitni prefiks mrežnog dijela zajedno s relevantnim mrežnim informacijama u koju je integriran.

Uređaj na mreži koji prati oglašavanje mrežnog usmjernika,kombinira dobiveni mrežni prefiks s EUI-64 formatom dijela svoje adrese koji ga jedinstveno identificira unutar mreže. Ovaj proces omogućuje autokonfiguraciju cjelokupne IPv6 adrese zajedno s ostalim nužnim mrežnim parametrima.

Dodatnim procesom poznatim kao Detekcija Duplicirane Adrese (DAD - Duplicate Address Detection) identificira se i izbjegava konflikt između adresa unutar mreže. Samostalna konfiguracija omogućava jednostavnu izmjenu mrežnih adresa. Potrebno je samo je rekonfigurirati usmjernik kako bi oglašavao novu adresu mreže. (Dooley, 2015)

DHCPv6 poslužitelj

Kako navodi Dooley (2015) Dynamic Host Configuration Protocol verzija 6 (DHCPv6) je nova verzija DHCP protokola stvoren za IPv6. DHCPv6 se može koristiti za dodijelu statičkih ili dinamičkih adresa i konfiguraciju mnogih drugih parametara. Dooley (2015) potom navodi tri načina rada DHCPv6:

- Stateful DHCPv6 je kao DHCP u IPv4. Može se koristiti za dodijelu statičkih ili dinamičkih adresa kao i opcije konfiguracije mreže.
- DHCPv6 bez stanja (stateless) ne dodijeljuje adrese. Umjesto toga za konfiguraciju se koristi SLAAC adrese i DHCPv6 koristi se samo za pružanje dodatnih opcija konfiguracije koje nisu dostupan u SLAAC-u.
- DHCPv6-PD obično koriste pružatelji usluga za delegiranje prefiksa svojim klijentima mreža.

4.4. Učinkovitije usmjeravanje

IPv6 ograničava proširenje tablica usmjeravanja i čini ih učinkovitijima dopuštajući hijerarhijsku strukturu adresiranja te uz pojednostavljeno zaglavlje koje omogućuje poboljšano usmjeravanje informacija od izvora do odredišta. Kontinuirani adresni prostor omogućuje prikupljanje adresa pod jednim prefiksom za identifikaciju na internetu čime se olakšava agregacija ruta preko interneta. Ovakav strukturirani pristup adresiranju smanjuje količinu informacija na internetu koje usmjerivači moraju održavati i pohranjivati te ubrzava usmjeravanje podataka. Osim toga, s IPv6, izvorni uređaj, a ne usmjerivač, upravlja fragmentacijom, koristeći protokol za otkrivanje maksimalne prijelazne jedinice puta (MTU) . (“6 Advantages Of IPv6 To IPv4”, bez dat.)

4.5. Više sigurnosti

Prilikom razvijanja IPv4 inačice protokola, pitanja vezana uz aspekte internetske sigurnosti nisu imala istu važnost kao što imaju u današnjem vremenu. Međutim, kod koncipiranja protokola IPv6, aspekt sigurnosti je imao ključnu ulogu. S ugrađenim fokusom na aspekte sigurnosti mnoga od sigurnosnih karakteristika koje su bile opcionalne u IPv4 verziji, inkorporirane su u IPv6 strukturu, primjerice, IPv6 automatski primjenjuje enkripciju prometa i verifikaciju cjelovitosti paketa. To pruža konvencionalnu zaštitu protoka podataka putem interneta na nivou virtualnih privatnih mreža (VPN). (“6 Advantages Of IPv6 To IPv4”, bez dat.). IP sigurnost (IPsec) , koji se obično koristi u IPv4 VPN-ovima, izvorni je dio IPv6 putem dodatnih zaglavlja paketa koja pružaju enkripciju i autentifikaciju te olakšava end-to-end enkripciju. To je skup je protokola za osiguravanje komunikacije internetskog protokola (IP) putem provjera autentičnosti pošiljatelja i pružanje zaštite integriteta plus mogućnost povjerljivost za prenesene podatke.

Specifikacija IPv6 uključuje sigurnosne značajke koje su naknadno ugrađene na IPv4. Kada se koriste ove značajke, IPv6 može biti otporniji na napade “čovjek u sredini” i ARP trovanja (protokol razlučivanja adrese). Širi skup adresa znači veću skalabilnost, ali, uz to pruža i veću sigurnost. Ovo proizlazi iz činjenice da je u okviru IPv6 sustava napadačima otežano provođenje skeniranja i identifikacija uređaja unutar mreže zbog veličine adresnog prostora.

IPv6 koristi protokol za otkrivanje sigurnog susjeda (SEND) za određivanje adresa sloja veze drugih čvorova i dostupnih usmjerivača. SEND je sigurnija implementacija koja brani od napada imenovanja poput trovanja ARP-om, na koje je IPv4 ranjiv. (Bowman, 2020)

4.6. Bolje performanse

Mehanizmi implementirani u IPv4 mrežni sloj su pojednostavljeni i poboljšani za IPv6 protokol. Ove izmjene omogućuju brže rukovanje IPv6 paketima u usporedbi s IPv4. Pojednostavljeno IPv6 zaglavlje, kontrolni zbrojevi zaglavlja, fragmentacija i

ponovno sastavljanje uklonjeni su iz IPv6 usmjerivača i sve skupa to čini IPv6 podložnijim hardverskoj obradi i utječe na brzinu obrade. (“6 Advantages Of IPv6 To IPv4”, bez dat.) Na slici 10 prikazane su razlike u brzini između IPv4 i IPv6 tehnologije koje su testirane za područje Londona.

LONDON

IPv4 x IPv6 Connection/Total Time Comparison

DOMAIN	CONNECT TIME		TOTAL TIME	
	IPv4	IPv6	IPv4	IPv6
GOOGLE	.005 sec	.005 sec	.050 sec	.051 sec
FACEBOOK	.144 sec	.145 sec	.288 sec	.291 sec
YOUTUBE	.005 sec	.005 sec	.017 sec	.019 sec
WIKIPEDIA	.011 sec	.013 sec	.018 sec	.021 sec
NETFLIX	.015 sec	.016 sec	.033 sec	.035 sec
LINKEDIN	.078 sec	.077 sec	.151 sec	.150 sec
PANDORA	.153 sec	.152 sec	.302 sec	.299 sec
CLOUDFLARE	.005 sec	.005 sec	.008 sec	.008 sec
SUCURI	.006 sec	.006 sec	.008 sec	.007 sec

Slika 10: Razlika u brzini između IPv4 i IPv6 (https://blog.sucuri.net/2016/08/ipv4-vs-ipv6-performance-comparison.html, 2016)

4.7. Kvaliteta usluge – QoS

Kvaliteta usluge je alat koji omogućuje da usmjerivač nauči dijeliti određene prioritetne pakete (VoIP, streaming usluge, video call…) različitim aplikacijama ili daje prednost pojedinim uređajima na mreži koji te aplikacije koriste. Dobra kvaliteta usluge znači, na primjer, da se računalo neće mučiti s reprodukcijom videozapisa dok istovremeno pokušava preuzeti veliku datoteku.

Kvaliteta usluge tehnički postoji u IPv4, ali zapravo ne funkcionira. Paketi se tehnički mogu dodijeliti različitim prioritetima, ali usmjerivači obično samo zanemaruju QoS zastavicu, a neki čak označavaju sve pakete kao “Najviši prioritet”, što poništava i samu svrhu takve usluge. Dok IPv6 ima u sebi ugrađeni mehanizam za upravljanje

kvalitetom usluge, koji omogućava davanje prednosti hitnim paketima, čime se postiže optimizaciji i povećana efikasnost njihove obrade. IPv6 protokol ima u samom zaglavlju paketa specijalizirana polja (“klasa prometa” i “oznaka toka”) koja su izravno odgovorna za upravljanje kvalitetom usluge. (“6 Advantages Of IPv6 To IPv4”, bez dat.)

4.8. Lakše dijeljenje datoteka

Uz IPv6, postoje dva odvojena adresna prostora za privatno adresiranje. Oni se nazivaju “lokalno na poveznici” i “lokalno na web mjestu”. Lokalna adresa veze ima puno korisnih funkcija, uključujući automatsku konfiguraciju hostinga jednostavnim upitom usmjerivača (nije potreban DHCP) i postavljanjem ad-hoc LAN-ova bez usmjerivača. To znači da možete povezati računala i dijeliti podatke bez potrebe za protokolima za dijeljenje podataka ili posebnih aplikacija (“6 Advantages Of IPv6 To IPv4”, bez dat.).

4.9. Nema NAT-a (prijevoda mrežne adrese)

Budući da nema dovoljno IPv4 adresa, veliki dio interneta se oslanja na NAT za povezivanje. NAT omogućuje sakrivanje više uređaja s privatnim IP adresama iza jedne javne IP adrese. NAT služi kao tehnologija za povećanje IPv4 adresnog prostora, ali također prisiljava svaki paket koji uđe ili izađe iz vaše mreže da se pregleda i promijeni. Za neke servise i usluge koje koriste više portova potrebna je prilagodbi da bi radile. Uz IPv6, svaki uređaj može imati svoju jedinstvenu IP adresu, što eliminira potrebu za NAT-om. IPv6 adrese ne moraju prolaziti kroz NAT što čini sam IPv6 protokol i komunikaciju bržim . (“6 Advantages Of IPv6 To IPv4”, bez dat.)

4.10. Jednostavnija fragmentacija- MTU

Različiti uređaji na mreži ili diljem interneta imaju različite dopuštene maksimalne jedinice prijenosa (MTU). Ako usmjerivač primi paket koji je prevelik za sljedeći skok, on ili ispušta ili fragmentira paket. Ispušteni paketi uzrokuju ponovni prijenos podataka, a fragmentaciji je potrebno vrijeme za ponovno sastavljanje paketa. IPv6 ne zahtijeva da mreža upravlja fragmentacijom paketa i ne dopušta mrežnim komponentama da fragmentiraju pakete, što ga u teoriji čini bržim (Bowman, 2020).

Kontrola fragmentacije IPv6 paketa događa se na IPv6 izvornom hostu, a ne na posrednom IPv6 usmjerivaču. Prije slanja paketa uređaji usklade MTU pomoću postupka koji se zove Otkrivanje jedinice maksimalnog prijenosa puta (PMTU), a za učenje veličine MTU putanje koristi se IPv6 Fragment Extension Header. Paketi se šalju dogovorenom veličinom što eliminirati potrebu da usmjerivači izvode fragmentaciju navodi Majkowski (2015).

5. Glavne barijere usvajanja IPv6 protokola

“Prijelaz na IPv6 je neizbježan, ali zašto se čini da treba toliko vremena?” (“5 reasons why the adoption of IPv6 takes so long”, 2015).

Kroz istraživanje teme završnog rada o barijerama koje koče usvajanje i implementaciju IPv6 tehnologije uočio se jasan obrazac ponavljajućih faktora. Nekoliko glavnih faktora koji direktno i najviše utječu:

- Troškovi implementacije
- Kompatibilnost između protokola
- Problemi sa naslijeđenim sustavima (Legacy System)
- Nedovoljna ili nepostojeća podrška ISP-ova
- Prisustvo prevoditelj mrežnih adresa (NAT)
- Slaba svijest među poslovni korisnici i velikim organizacijama

U nastavku detaljno je istražen i analiziran svaki od navedenih faktora.

5.1. Trošak implementacije

Troškovi prijelaza na IPv6 ovise o prirodi organizacije i poslovanja. Svi glavni (Linux,Windows,Mac OS) operativni sustavi, kao i mnoge softverske aplikacije i hardverski uređaji spremni su za IPv6, što omogućuje organizacijama da ga implementiraju kao dio rutinskih ciklusa nadogradnje.

Za mnoge organizacije operativni troškovi kao što je obuka administratora mreža/sustava, dodavanje IPv6 bazama podataka, dokumentaciji za upravljanje vjerojatno će činiti većinu troškova nadogradnje na IPv6. Organizacije koje koriste vlastiti prilagođeni softver vjerojatno će imati dodatne troškove za nadogradnju takvog softvera na IPv6, dok će oni koji imaju procese testiranja/objavljivanja novih tehnologija vidjeti marginalne dodatne troškove prilikom testne konfiguracije IPv6. Ekonomski aspect nameće se kao jedan od ključnih faktora i značajno utječe na usporenu globalnu

migraciju. Primarni izazov u implementaciji IPv6 proizlazi iz ograničenih ekonomskih dobiti koji proizlaze iz njegove implementacije.

Poslovni korisnici

Otpornost velikih poduzeća i organizacija na migraciju IPv6 općenito usporava usvajanje. “Prelazak na IPv6 uključuje različite troškove koji nisu isključivo novčani – oni također uključuju resurse kao što su vrijeme i osoblje potrebno za postizanje potpune migracije. Bit će potrebna velika količina planiranja kako bi projekt prošao što je brže moguće i na kraju sve funkcioniralo” (Kubilius, 2021) . S planiranjem dolaze i ljudski resursi koji će obavljati tu funkciju. Sa stajališta financijskih troškova, većina će biti ili nova oprema za obavljanje specifičnih IPv6 funkcija (routeri, switchevi, serveri) ili nova oprema koja do sada nije bila kompatibilna s IPv6 protokolom.

Sclafani (2021) također navodi kako postoji jedan aspekt implementacije IPv6 koji dodatno utječe na cijenu bit će na strani softvera za aplikacije koje se koriste interno ili komercijalna rješenja. To mogu biti stvari poput :

1. Trajna licenca za softver gdje je istekao ciklus održavanja :
    - podržava li IPv6
    - postoji li mogućnost ažuriranja na IPv6
    - treba li zadržati IPv4 mrežni NAT samo za takve aplikacije
    - kupnja novog softvera

2. Sustavi nadzora mogu vidjeti dodatak IPv6 kao “drugu krajnju točku”, a ne proširenje trenutne mreže. Ovisno o platformi za praćenje – implementacija IPv6 mogla bi značiti nove troškove prilikom implementacije .

U poslovanju je razborito izbjegavati nepotrebne troškove. U slučaju implementacije IPv6, nekoliko jednostavnih pravila može olakšati implementaciju IPv6 i značajno smanjiti potreban proračun. Sclafani (2021) navodi nekoliko glavnih primjera:

1. Kupnja - Potrebna je politiku kupnje koja navodi da sav kupljeni mrežni hardver, softver i usluge moraju podržavati IPv6.
2. IT Training - Obuka koja ima veze s IP umrežavanjem mora uključivati IPv6. Uključiti IPv6 kao uvjet prilikom zapošljavanja novog IT osoblja.
3. Priprema tijekom većih ili manjih projekata

Organizacije moraju razmišljati o tome kako bi se drugi IT projekti mogli koristiti za implementaciju IPv6. Na primjer, selidba ureda mogla bi biti prilika da se nova mreža napravi spremnom za IPv6, omogućenom za IPv6 ili čak samo za IPv6 (Holder, 2018). U mnogim slučajevima, organizacije će otkriti da je razina IPv6 podrške u trenutnoj infrastrukturi zapravo visoka. Bez obzira na to, prijelaz će zahtijevati određene troškove hardvera i softvera. Organizacije će trebati izraditi nove topologije mreže, pregledati postojeće koncepte, osposobiti svoje IT osoblje i možda će trebati potražiti vanjsku stručnu pomoć kako bi u potpunosti iskoristili IPv6.

Uštede povezane s IPv6 postaju sve lakše za definirati. Mreže temeljene na IPv4 postaju sve složenije. IT usluge poput VoIP-a (Voice over Internet Protocol), aplikacija za razmjenu poruka, video telekonferencija, IPTV-a (Internet Protocol television) i objedinjenih komunikacija dodaju slojeve međuopreme i složenosti. Organizacije koje se spajaju ili provode B2B (Business-to-Business) transakcije provode rješenja preklapanja NAT-a koja imaju visoke troškove upravljanja i teško ih je riješiti. Dok rastuće tržište mobilnih uređaja i mrežnih uređaja zahtijeva robusne modele pristupa koji su skupi i teški za implementaciju u IPv4 svijetu. U svim ovim slučajevima, IPv6 predstavlja čišći i isplativiji model na duge staze nego što IPv4 može pružiti. A činjenica je da je ulaganje u IPv4 ulaganje u tehnologiju na kraju svog životnog vijeka, dok je ulaganje u IPv6 ulaganje u tehnologiju budućnosti (Hagen, bez dat.).

ISP-ovi - Pružatelji internetskih usluga

Mogućnost podržavanja IPv6 zahtijeva opsežne resurse. “Internet se sastoji od milijuna routera i switcheva. Oni su u početku bili dizajnirani za rad s IPv4. Njihova

zamjena ili nadogradnja zahtijeva vrijeme i proračun. Za jezgrenu mrežu, zamjena jezgrenih usmjerivača skupim hardverom nešto je što se ne radi svakodnevno. To znači da ovaj prijelaz zahtijeva više vremena i novca" ("5 reasons why the adoption of IPv6 takes so long", 2016). "Nisu svi ISP-ovi i telekomunikacijski operateri financijski sposobni za ulaganje. Stoga se tempo razvoja uglavnom oslanja na glavne tržišne igrače. Međutim, bez malih i srednjih poduzeća u jednadžbi, industrija je na gubitku značajnog dijela organizacija koje bi mogle pomoći ubrzanju procesa implementacije IPv6" ("3 Reasons Why IPv6 Adoption Is Still Light Years Away", 2020).

Kuerbis (2019) navodi kako iscrpljenost IPv4 adresnog prostora stvara ograničenje za rast i širenje operatera. Rast IPv4 Interneta zahtijeva kupnju sve skupljih IPv4 adresa na tržištu i sve intenzivnije dijeljenje globalno preusmjerenih IPv4 adresa. Nasuprot tome, količina IPv6 adresa je obilna i besplatne su, što otvara vrata rastu. ISP-ovi su pružatelji usluga koji posreduju između korisnika i globalne internetske mreže, kao i drugih mreža. Kao takvi oni ne trguju samim IP protokolom nego pružaju korisnicima kompleksna sveobuhvatna rješenja za umrežavanje i integraciju s globalnom internetskom strukturom. S te strane pružatelji usluga suočavaju se s izazovima dodatnih tehničkih inovacija, što zahtijeva značajna kapitalna ulaganje u planiranje, implementaciju, testiranje i verifikaciju novih tehnologija. Kod ovakvih značajnih ulaganja gotovo pa i nije moguće precizno izračunati ekonomske faktore koji bi potvrdili isplativost ulaganja. Implementacija IPv6 izaziva značajne početne i tekuće troškove koji su uzrokovani nužnošću održavanja kompatibilnosti s IPv4. Zbog potrebe održavanja kompatibilnosti unatrag, implementacija IPv6 ne eliminira odmah potrebu operatera za IPv4 adresama, niti eliminira potrebu za dijeljenjem tih adresa. Ključni pokretač implementacije je operaterova objektivna procjena rasta mreže u odnosu na poslovanje i relativni trošak plana rasta koji uključuje ili implementaciju IPv6 ili onu koja ne uključuje.

Troškovi implementacije (Kuerbis, 2019):

- Početni troškovi potrebni za implementaciju IPv6 protokola - To uključuje ulaganja u infrastrukturu, kodiranje, učenje i obuku. Većina ovih troškova je jednokratna u određenom vremenskom razdoblju, iako se u većim mrežama može distribuirati na različite dijelove mreže u različitim vremenskim razdobljima.

- Trošak kompatibilnosti - To su troškovi potrebni za održavanje kompatibilnosti s IPv4 internetom. To uključuje troškove 6to4 NAT prijevoda ili infrastrukture tuneliranja, troškove pokretanja duplog protokola i troškove otkrivanja i popravljanja nekompatibilnosti uzrokovanih implementacijom IPv6.
- IPv6 nije skup ako ga dodate kao dodatni uvjet pri kupnji nove opreme. Skupo je ako trebate zamijeniti postojeću opremu samo da biste mogli implementirati IPv6.
- nema troškova stjecanja IPv6 adresa.

Za ISP-eve koji ne implementiraju IPv6 (Kuerbis, 2019) :

- Trošak stjecanja dodatnih IPv4 adresa
- Trošak proširenja IPv4 mreže korištenjem NAT uređaja

Uvođenje IPv6 protokola kod pružatelja internetskih usluga predstavlja značajan izazov. S pratećim potencijalnim izazovima dodatno dolazi i rizik povezan s uspješnom implementacijom , kao i potencijalnim učincima na prihode. Inicijativa takvog obima zahtijeva ozbiljan sveobuhvatan strateški pristup koji je nužan kako bi se smanjio rizik i potencijalnih utjecaja na postojeću infrastrukturu koja čini glavni, pa čak i dominantan, izvor prihoda za kompaniju. Ograničena sredstva ometaju proces tranzicije, ali oni koji si ne mogu priuštiti promjenu i dalje trebaju tržišno spremna rješenja za nastavak skaliranja. Kod ISP-ova povećavanje tržišne konkurentnosti i pojačavanje kompetitivnosti njihove ponude predstavljaju ključne motivirajuće faktore za implementaciju IPv6 protokola. Premda se ekonomske dobiti ne mogu lako povezati s tehničkim napretkom u korištenju IPv6 protokola, pružatelji internetskih usluga trebaju prepoznati ekonomski potencijal koja proizlazi iz konkurentske prednosti koju dolazi s uvođenje IPv6 protokola te biti spremni ponuditi povezivanje na IPv6 Internet poslovnim i rezidencijalnim korisnicima (Kuerbis, 2019).

Privatni korisnici

Krajnji privatni korisnici nemaju izravnu korist od prijelaska što može predstavljati prepreku za implementaciju IPv6. Postizanje glatkog procesa prijelaza

moglo bi potrajati dok IPv6 ne bude u potpunosti implementiran. Unutar tog vremena bit će samo IPv6 mreže i samo IPv4 mreže koje moraju međusobno komunicirati. Oprema za krajnje korisnike redovito se mijenja i većinom već podržava IPv6 protokol. Većina usmjerivači današnjice već podržava IPv6 jer gotovo svi rade na bazi Linux operativnog sustava , koji ima izvornu podršku za IPv6. No, iako ga većina kućnih usmjerivača danas podržava, on je obično onemogućen prema zadanim postavkama od strane pružatelja internetskih usluga. No i dalje će biti mnogo starih kućnih pristupnika, uređaja za ispis, starih operativnih sustava itd. koji su nekompatibilni s IPv6 protokolom. Za krajnje korisnike i rubne dijelove mreže, rješenje je vrijeme, kako navodi Mayes (2018).

5.2. Poslovni korisnici

Ovaj je sektor bio relativno konzervativan u svom pristupu novim tehnologijama i uvelike se oslanjao na privatne mrežne platforme . To je značilo da je uglavnom izoliran od tereta problema s iscrpljivanjem IPv4 adresa . Razumijevanje kompanija koje upravljaju informacijskim sustavima ili nude ICT usluge o nužnosti za tranzicijom na IPv6 protokol tek treba dostignuti neophodnu razinu. Adresni prostor obično ne predstavlja problem za poslovne korisnike, budući da većina upravlja sa samo nekoliko javnih IP adresa i organizacijske mreže uglavnom se nalaze iza NAT-a. Do komplikacija dolazi prilikom procesa integracije između dva ili više ovakvih korisnika ili vanjskih servisa. Kod organizacije koje svoje primarne aktivnosti ne temelje na informacijskim tehnologijama, ističe se ključni izazov koji se tiče IT osoblja, a to je nedovoljnog razumijevanja potrebe za uvođenjem IPv6 u svoje poslovno okruženje. Ako ne postoji jasne smjernice i podrška za ovu inicijativu, postoji realna opasnost da će kompanije odgađati tranziciju s IPv4 na IPv6. Iako je istina da većina kompanija vjerojatno neće osjetiti potrebu za punom integracijom IPv6 u svoje poslovanje u narednim godinama, ovo općenito shvaćanje dodatno usporava poticaj za pokretanjem migracijskog postupka. “Neke će organizacije nastaviti koristiti IPv4 i koristiti mehanizme poput NAT-a dok god je to moguće. Zemlje poput Indije , s velikim brojem stanovnika i rastućom tehničkom kompetencijom, gotovo sigurno neće to pokušati i izravno će prijeći na IPv6. Zapravo, možemo vidjeti da se to već događa na mjestima

poput Japana, Koreje i Kine. Te zemlje već jesu ili će tek postati velika tržišta. Organizacije koje žele biti aktivne na tim tržištima, ali ne koriste IPv6, bit će u nepovoljnijem položaju u odnosu na konkurenciju" (Reasons for IPv6, bez dat.).

5.3. Podrška ISP-ova

Pružitelji internetskih usluga (ISP) dio su procesa implementacije IPv6 tehnologije. Kako je ranije spomenuto, ISP-ovi više ne mogu korisnicima pružati javne IPv4 adrese i moraju implementirati IPv6 kako bi mogli pratiti nagli porast korisnika interneta i pružiti korisnicima potrebne IP adrese. Dawson (2021) navodi kako proces prijelaza zahtijeva nadogradnju ili promjenu infrastrukture na onu koja može podržati IPv6. ISP-ovi su glavni čimbenik koji izravno utječe na implementaciju. Moraju početi s nadogradnjom i mijenjanjem infrastrukture za podršku IPv6. Migracija na IPv6 zahtijeva mnogo više od sposobnosti prosljeđivanja IPv6 prometa na internet. Postoji dodatni trošak za svakog ISP-a koji se želi u potpunosti pretvoriti u IPv6. IPv6 nije unatrag kompatibilan s IPv4, i svaka tvrtka koja želi eksterno usmjeravati s IPv6 treba održavati dual-stack, što znači da svaka komunikacija u mreži i izvan mreže mora se usmjeravati koristeći oba protokola. To povećava troškove, ali, što je još važnije, usporava usmjeravanje prometa.

Također, nemoguće je pretvoriti kompletnu mrežu u IPv6 dok svi uređaji na mreži nisu kompatibilni s IPv6. To svake godine postaje sve manji problem, ali svaka mreža ISP-a i dalje ima korisnike i uređaje na mreži koji nisu kompatibilni s IPv6. Oni korisnici koji još uvijek koriste npr. 10 godina star WiFi usmjerivač ili pojačivač nestali bi s potpunom pretvorbom na IPv6. Ovo je jedan od primarnih razloga zašto veliki ISP-ovi i mobilni operateri nemaju 100% IPv6. Još uvijek postoji milijun ljudi koji koriste stare mobilne telefone koji se ne mogu adresirati s IPv6. Kako bi olakšali tranziciju prvo je neophodno da pružatelji internetskih usluga implementiraju IPv6, nakon čega je potrebno postupno pristupiti tranziciji kod krajnjih korisnika (Dawson, 2021).

5.4. Kompatibilnost između protokola

U svjetlu golemih razlika između formata protokola, interoperabilnost ne može postojati između IPv4 i IPv6. IPv6 protokol ima nedostatak kompatibilnosti s trenutnim IPv4 protokolom što znači da komunikacija između njih nije moguća bez dodatnih ulaganja. Prijelaz na IPv6 ne pruža jedinstveno, standardizirano rješenje za komunikaciju s uređajima i sustavima koji još uvijek koriste IPv4. “Prijelaz na novi protokol dolazi u dvije faze: prva, usvajanje dual-stack usluga, gdje se oba internetska protokola koriste istovremeno, i druga – potpuni prijelaz na IPv6. Međutim, dok se većina tržišta ne prilagodi dual-stack okruženju, prelazak samo na IPv6 nije moguć” (“3 Reasons Why IPv6 Adoption Is Still Light Years Away”, 2020).

“Nedostatak kompatibilnosti zahtijeva od operatera da istovremeno pokreću IPv4 i IPv6 u doglednoj budućnosti. To znači veće troškove održavanja, a prednosti postaju vidljive samo kada se i druge mreže prebace na IPv6. Nema izravne koristi od ranog usvajanja” (“5 reasons why the adoption of IPv6 takes so long”, 2015) . Štoviše, potrebna je nadogradnja za cijeli niz uređaja koji podržavaju značajke IPv6. Budući da IPv4 i IPv6 protokoli nisu kompatibilni, oni pokreću svoje pojedinačne sustave adresiranja i usmjeravanja. Bez dodatnih mehanizama, dvije vrste mreža ne mogu komunicirati. Ako organizacija ima dovoljno resursa za tranziciju i sposobna je održavati stabilnost svoje mreže, implementacija dual-stack usluge za oba protokola odlična je za daljnji razvoj.

“Mogle bi proći godine dok se većina tehnologije ne pokrene samo s verzijom 6, a čak i tada će većina hardvera morati imati kompatibilnost s povratnom vezom, jer će postojati stariji telefoni, prijenosna računala ili drugi uređaji koji trebaju IPv4 za povezivanje” (“3 Reasons Why IPv6 Adoption Is Still Light Years Away”, 2020).

. IPv6 protokol ima nedostatak kompatibilnosti s trenutnim IPv4 protokolom što znači da komunikacija između njih nije moguća bez dodatnih ulaganja. Prijelaz na IPv6 ne pruža jedinstveno, standardizirano rješenje za komunikaciju s uređajima i sustavima koji još uvijek koriste IPv4. “Prijelaz na novi protokol dolazi u dvije faze: prva, usvajanje dual-stack usluga, gdje se oba internetska protokola koriste istovremeno, i druga – potpuni prijelaz na IPv6. Međutim, dok se većina tržišta ne prilagodi dual-stack okruženju, prelazak samo na IPv6 nije moguć” (“3 Reasons Why IPv6 Adoption Is Still Light Years Away”, 2020).

“Nedostatak kompatibilnosti zahtijeva od operatera da istovremeno pokreću IPv4 i IPv6 u doglednoj budućnosti. To znači veće troškove održavanja, a prednosti postaju vidljive samo kada se i druge mreže prebace na IPv6. Nema izravne koristi od ranog usvajanja” (“5 reasons why the adoption of IPv6 takes so long”, 2015) . Štoviše, potrebna je nadogradnja za cijeli niz uređaja koji podržavaju značajke IPv6. Budući da IPv4 i IPv6 protokoli nisu kompatibilni, oni pokreću svoje pojedinačne sustave adresiranja i usmjeravanja. Bez dodatnih mehanizama, dvije vrste mreža ne mogu komunicirati. Ako organizacija ima dovoljno resursa za tranziciju i sposobna je održavati stabilnost svoje mreže, implementacija dual-stack usluge za oba protokola odlična je za daljnji razvoj.

“Mogle bi proći godine dok se većina tehnologije ne pokrene samo s verzijom 6, a čak i tada će većina hardvera morati imati kompatibilnost s povratnom vezom, jer će postojati stariji telefoni, prijenosna računala ili drugi uređaji koji trebaju IPv4 za povezivanje” (“3 Reasons Why IPv6 Adoption Is Still Light Years Away”, 2020).

5.5. NAT - Prevoditelj mrežnih adresa

U današnje vrijeme NAT (eng. Network address translation) uređaji nalaze se posvuda. Njihova upotreba i usvajanje u ovakvim razmjerima niu bilo planirani. Potaknut kontinuiranim rastom interneta i iscrpljivanjem IPv4 adresnog prostora, NAT tehnologija doživjela je brzi uspon. Bez NAT-a, velike korporacije s tisućama ili desecima tisuća računala progutale bi ogromne količine javnih IPv4 adresa ako bi željele komunicirati s vanjskim svijetom.

“Koncept prevođenja mrežnih adresa prvi su put opisali Kjeld Egevang i Paul Francis 1994. (RFC1631, 1994). Cilj NAT-a bio je stvoriti mehanizam koji omogućuje dijeljenje IPv4 adrese na više uređaja. Iako izvorni RFC opisuje NAT kao privremenu mjeru dok se ne nađu druga, složenija i dalekosežnija rješenja NAT još uvijek dominira internetskim prostorom i još uvijek se primjenjuje u velikoj mjeri” (The ugly side of NAT”, 2017). NAT tehnologija kao privremena mjera nikad nije standardizirana što je prisililo svakog implementatora NAT-a da donese sam lokalne odluke o njegovom korištenju i ponašanju pod određenim okolnostima. Industrija ISP-ova se okrenula korištenju NAT-

a u svojim uslugama, što im omogućava da pojedinačne IP adrese dijele na više istovremenih veza multipleksiranjem portova i korištenje vremenske podjele/dodijele (obično oko 24h).

5.6. Problemi sa naslijeđenim sustavima (Legacy System)

Sclafani (2021) definira naslijeđene sustave kao stariji sustavi. Dalje navodi kako im vjerojatno nedostaje neka značajka ili funkcionalnost trenutne tehnologije, ali još uvijek postoje jer dobro obavljaju ključnu ili važnu funkciju za organizaciju, stoga nema razloga za zamjenu. Uz IPv6 implementacije, vrijedi ponovno razmotriti kako se mreže oko naslijeđenih aplikacija mijenjaju.

Kada organizacija implementira IPv6, uređaji na mreži moraju podržavati IPv6 adrese na svom mrežnom sučelju, zajedno sa svojim postojećim IPv4 adresama. Ako uređaj ne može upotrijebiti IPv6 adresu, to će na kraju uzrokovati sukobe i probleme u nemogućnosti pronalaženja ili pravilnog komuniciranja . Moguće ga je prisiliti da koristi samo IPv4, ali kako sve više sustava sposobnih za IPv6 bude na mreži , naslijeđeni sustavi postat će sve veća odgovornost i zahtijevati mehanizme koji podržavaju IPv4 aplikacije u IPv6 mrežama i IPv6 aplikacije u IPv4 mrežama. Alternativno, možete pokrenuti dvostruku mrežu u kojoj koristite IPv4 za pristup IPv4 aplikacijama i IPv6 za pristup IPv6 aplikacijama (Sclafani, 2021). No to nije praktično rješenje i s vremenom ako se dodaje više uređaja ili aplikacija postaje teško za održavanje.

5.7. Sigurnost

Sigurnosna infrastruktura, u velikoj većini slučajeva, nije spremna. Mnogo je manje iskustva s IPv6 nego s IPv4 protokolom. Radi osiguravanja neprekidnog funkcioniranja trenutačnih usluga, primjenjuje se implementacija IPv6 koja uključuje istovremeno korištenje oba protokola. Kubilius (2021) navodi kako istovremeno upotrebljavanje obiju verzija protokola rezultira eskalacijom kompleksnosti mrežne infrastrukture. Kao rezultat toga, očekuje se da će broj potencijalnih ranjivosti biti

znatno veći. Stoga je važno da se pristupi implementaciji IPv6 protokola na pragmatičan način, počevši s procjenom trenutnog stanja same strukture mreže i konfiguracije svih mrežnih komponenti. Prije ulaska u tehničke segmente uvođenja novih funkcionalnosti vezanih uz IPv6 protokol, nužno je detaljno analizirati potencijalne prijetnje u trenutačnom sustavu te ga prilagoditi novim uvjetima. Posebna pažnja mora se posvetiti postavkama svih aktualnih zaštitnih mehanizama koji se odnose na IPv4 protokol da se repliciraju na jednak način i za IPv6 kako bi se očuvala visoka sigurnosna razina mreže.

Osim toga, paralelna primjena IPv6 i IPv4 protokola nosi sa sobom određene rizike. Unatoč brojnim poboljšanjima veza i performansi koje nudi IPv6, i dalje je prilično ranjiv navode P.Kaur i C.Kaur (2022). Sa svakim povezanim uređajem koji bi potencijalno mogao dobiti javnu IPv6 adresu umjesto privatne adrese iza NAT-a, postoji mogućnost neovlaštenog pristupa ili napada s bilo kojeg mjesta u svijetu. Rizik će biti još veći ako se svi ti uređaji spoje bežično (putem 4G/5G ili WiFi).

Prema Kubilisu (2021) glavni sigurnosni problemi kod IPv6 protokola su sljedeći :

- Dual-stacking
- IPv4/IPv6 tunneling
- Header manipulation
- Flooding
- Mobility (P.Kaur,C.Kaur, 2022)

Dual-stacking (Dvostruka konfiguracija)

Problemi s dvostrukom konfiguracijom nisu svojstveni za IPv6, već se pojavljuju u odnosu između IPv4 i IPv6. Ova dva protokola imaju svoje specifične sigurnosne probleme, koji su samo naglašeni kad se koristi dual-stacking. Pri ovakvom pristupu potrebno je da čvorovi unutar mreže podržavaju oba tipa protokola istovremeno, , što dovodi do dvostruke potrošnje snage memorijskih i procesnih kapaciteta samog hardvera što može dovesti do dupliciranja prometa paketa i smanjenje učinkovitosti mreže. Potrebno je osigurati dosljednu konfiguraciju svih mrežnih komponenata za

IPv4 i IPv6, uključujući rutere, uređaje za kontrolu pristupa, vatrozid, sustave za otkrivanje napada i druge temeljne elemente unutar mreže. U stvarnom svijetu, administratori se suočavaju s povećanim radnim opterećenjem zbog nužnosti održavanja dvostrukih postavki, što često rezultira većim brojem grešaka i potencijalno povećava ranjivost mreže. Ako dođe do neusklađene konfiguracije između protokola, potencijalno se napadačima omogućava zaobilaženje mehanizama sigurnosti korištenjem jednog od dvaju protokola. U tu svrhu, preporučena praksa u procesu mrežne konfiguracije obuhvaća isključivanje svih suvišnih funkcionalnosti s ciljem smanjenja broj potencijalnih napada (Kubilius, 2021).

IPv4/IPv6 tuneliranje

IPv4/IPv6 mehanizam tuneliranja je ranjiv. IPv6 preko IPv4 tuneliranja enkapsulira IPv6 pakete unutar IPv4 zaglavlja, što je način na koji se paketi prenose u IPv6 infrastrukturu za usmjeravanje . Međutim, usmjerivači ne provjeravaju sadržaj paketa. Nadalje, adrese IPv6 hostova i relejnih usmjerivača podložne su lažiranju paketa (spoofing). Metoda tuneliranja često se koristi usporedno s dual-stack tehnikom. Ovaj pristup ima za cilj uspostaviti komunikaciju između različitih dijelova mreže, posebno onih koji podržavaju isključivo IPv4 protokol. Krajevi tunela ili rubne točke iznimno su ranjive sa stajališta sigurnosti, budući da omogućuju zaobilaženje zaštitnih mehanizama mreže stoga su često izložene napadima. Zbog toga sav promet koji nije enkapsuliran unutar tunela treba kategorizirati kao vanjski promet te na njega primijeniti sve metode zaštite koje su u uporabi na vanjskim vezama, poput vatrozida i filtriranja, kontrole pristupa, antivirusne zaštite i druge metode zaštite navodi Kubilius (2021).

Header manipulation

Neki se napadi temelje na manipulaciji zaglavlja, a često se mogu riješiti korištenjem IP Security ili IPSec i zaglavlja proširenja. Međutim, ovo nije uvijek rješenje jer specifični čvorovi poput vatrozida mogu biti preopterećeni. Ovdje je preporuka

filtriranje prometa preko vatrozida za nepodržane servise ili servise koje se ne koriste (P.Kaur,C.Kaur, 2022).

Flooding

Zbog veličine IPv6 adrese, skeniranje cijelog segmenta je mnogo teže i traje dulje od skeniranja IPv4 adresnog prostora. Zbog toga DDoS napadi tipa Smurf mogu predstavljati problem, zbog čega je potrebno filtrirati nepotreban promet preko vatrozida (P.Kaur,C.Kaur, 2022). Prelazak na IPv6 zahtjeva sigurnosne mjere slične IPv4 mjerama, uključujući : proxy-e, vatrozid, IDS/IPS sisteme, filtere i druge sigurnosne sustave kako bi se povećala sigurnost same mreže. Potrebno je filtriranje odlaznog prometa kako bi se osiguralo da samo ovlaštene interne IP adrese napuštaju mrežu kako bi spriječili nenamjerno generiranje lažnog IP prometa na internet (Kubilius, 2021).

Mobility

Kako navode P.Kaur i C.Kaur (2022) u svom radu mobilnost je nova značajka IPv6 koja nije bila dostupna u IPv4 protokolu. Mobilnost je vrlo složena funkcija koja podiže znatnu količinu zabrinutosti kada se razmatra sigurnost. Mobilnost koristi dvije vrste adresa, pravu adresu i adresu mobitela. Prva je tipična IPv6 adresa zapisana u zaglavlju proširenja, a druga je privremena adresa zapisana u IP zaglavlju. Problem je u privremenoj adresi koja može biti podložna spoofing napadima.

5.7.1. Sigurnost na ISP strani

Mayes (2018) navodi ako ISP podržava sve funkcije IPv6, on također mora podržavati iste sigurnosne mjere koje se pružaju korisnicima IPv4. To bi trebalo

uključivati, filtriranje zlonamjerne izvorne adrese što bi za IPv6 značilo blokiranje sljedećeg:

- većina multicasta (dopušta samo ono što je potrebno za funkcioniranje veze između ISP-a i korisnika)
- jedinstvene lokalne i lokalne izvorne adrese (koje nisu globalno usmjerljive i nikada ne bi trebale biti važeća izvorna IPv6 adresa)
- dodijeljene korisnikove globalne unicast adrese (nikada ne bi smjela vrijediti kao vanjska izvorna adresa)
- druge zlonamjerne adrese koje su identificirane.

Zlonamjerno praćenje prometa, također, treba tražiti i blokirati (Mayes , 2018):

- DoS (Denial-of-Service) i DDoS (Distributed Denial-of-Service) promet
- pogrešno oblikovani paketi (poluotvorene TCP sesije, echo odgovori bez podudaranja postojećih echo zahtjeva, itd.)
- ping sweeps (ICMP sweep), skeniranje portova i drugi izviđački promet
- ostali zlonamjerni promet.

5.7.2. Sigurnost NAT-a

Neke od benefita NAT-a su i te da pruža povećanje sigurnosti privatnih mreža zadržavanjem privatnog internog adresiranja dalje od vanjske mreže. Organizacije često koriste NAT na krajnjoj točki svoje mreže, ne samo radi sigurnosti, već i radi balansiranja opterećenja prometa i otpornosti. Ova praksa je posebno naglašena u slučaju manjih ili srednjih poslovnih korisnika koji se povezuju s više internetskih pružatelja i ne pokreću BGP (Border Gateway Protocol) ili imaju svoj adresni prostor neovisan od pružatelja internetskih usluga . Čak i velike tvrtke ponekad koriste NAT kako bi olakšale korištenje više pružatelja usluga. Ukidanjem NAT-a drastično bi se povećao broj javnih IP adresa koje se usmjeravaju na internet (Holder, 2018).

5.8. Hardware i Software

Prema Martinezu (2017) proizvođači hardverskih komponenti, koji su u kontekstu IP protokola usko povezani sa softverom, ključni su akteri gdje će se inovacije posebno istaknuti kroz primjenu IPv6 protokola posebno u segmentu korisničke opreme. U praksi je potvrđeno da softveri s otvorenim izvornim kodam zauzimaju značajnu ulogu kod novih tehnologija. Gotovo svi proizvođači mrežne opreme već nekoliko godina prodaju rutere i switcheve koji su kompatibilni s IPv6. Iako većina kućnih rutera dobivena od strane IPS-a podržava IPv6 protokol i umrežavanje, na infrastrukturnoj razini mrežna oprema i pružatelji često nisu spremni za novi protokol.

Glavni problem nije nedostatak podrške za IPv6 protokol, već nedostatak podrške koju pružaju CPE dobavljači za starije (DS-Lite, lw4o6) i novije (464XLAT, MAP T/E) prijelazne mehanizme. Neki dobavljači to pružaju “na zahtjev” za velike kupce, ali mali i srednji ISP-ovi nemaju istu sposobnost kupnje, što stvara veliki problem za implementaciju. Problem s podrškom prijelaznih mehanizama je da postoji preveliki broj protokola tranzicije za koje je potrebna podrška , što odluku o usvajanju čini složenijom za ISP-ove.

U svoje platforme, proizvođači operacijskih sustava relativno rano integrirali su podršku za IPv6 protokol. Integracija direktno u operacijske sustave trebala je služiti kao poticaj daljnjem razvoju aplikacija koje mogu efikasno iskoristiti pogodnosti novog protokola No unatoč ranoj podršci operacijskih sustava nije postignut značajniji napredak. “Na primjer, dva često korištena web servera (Apache i Microsoft IIS) odavno podržavaju IPv6 (prvi od 2002. godine, a drugi od 2003. godine)” (Martinez, 2017). Međutim, napredak novijih softvera, čija je upotreba usko vezana za IPv6 protokol, odvija se izuzetno tromo. Softveri ili aplikacije mogu biti važniji od opreme i uređaja pri odabiru prijelaznog pristupa. Nadogradnje hardvera i ugrađenih operativnih sustava moguće je brže zamijeniti od prilagođenih ili gotovih aplikacija. Dobavljači hardvera radili su na podršci za IPv6 puno ranije i dulje od proizvođači softvera. Mnogi dobavljači možda neće moći ili htjeti nadograditi softver za podršku IPv6, a mnoge organizacije nemaju vlastite resurse za nadogradnju koda. Što je više naslijeđenih

aplikacija i prilagođenih aplikacija koji organizacija podržava (bilo razvijen u kući ili visoko prilagođen gotov softver) to je veći rizik da softver neće podržavati IPv6 (Martinez, 2017).

5.9. Potražnja

Prema Griniusovim (2021) istraživanjima korisnička potražnja za IPv6 protokolom je vrlo niska. Postoji potražnja korisnika za pristupom internetu neovisno o tome je li IPv4 ili IPv6. Javne internetske usluge danas su općenito dostupne putem IPv4, tako da korisnici ne percipiraju potrebu za korištenjem IPv6 . Korisnici imaju starije uređaje kao što su kamere, televizori ili igraće konzole koje prihvaćaju samo IPv4 adrese. Migriranjem na IPv6 pružatelji internetskih usluga riskiraju nelagodu klijenata čija oprema možda više neće ispravno raditi na novom protokolu.

Danas globalna prihvaćenost IPv6 ne doseže niti 40%. Prema Googleovoj statistici (“Google collects statistics about IPv6 adoption”, 2022) usvajanja IPv6 na globalnoj razini dosegao je 34% do ožujka 2022. Statistika usvajanja IPv6 po zemljama pokazuje da Indija vodi sa 66%, dok je Njemačka na drugom mjestu s 49% usvajanja. 119 zemalja pokrenulo je implementaciju IPv6; međutim, ostali još nisu uveli IPv6 u svoje mreže. Postoji jasan napredak u usvajanju IPv6 u azijskim i južnoameričkim zemljama, dok afričke zemlje tek trebaju napraviti značajne iskorake. (Grinius, 2021).

5.10. Vrijeme

Još jedan izazov za prijelaz je to što ne postoji određeni datum tranzicije. Nema zadanog datuma niti rokova za prelazak što čini potpunu implementaciju IPv6 još težom. Trenutna potreba nekima se može činiti nedovoljno hitnom. Ovo može dovesti do usporavanja investicija i prijelaza na novu tehnologiju. “Glavni razlog zašto se prelazak nije dogodio je taj što je nitko ne forsira i svijet nastavlja funkcionirati koristeći IPv4.” (Dawson, 2021).

6. Migracijske tehnologije i načini migriranja na IPv6

Prijelaz na novu verziju predstavlja značajno unapređenje te se smatra ključnom komponentom buduće mrežne infrastrukture. Međutim, usprkos brojnim prednostima, tranzicija nije gladak proces i zahtijeva sustavan pristup. S obzirom na kompleksnost internetskog ekosustava zamjena postojećeg modele adresiranja jednostavno nije ostvariva u kratkom vremenskom razdoblju. Budući da IPv6 i IPv4 nisu kompatibilni međusobno, implementaciju na IPv6 ne može se odraditi odjednom, zbog tog razloga razvijene su tehnike i mehanizmi za postizanje jednostavnijeg prijelaza. Ovi mehanizmi imaju za cilj olakšati proces implementacije kako bi započeli nesmetan prijelaz. Tijekom tranzicijskog razdoblja, nužno je je postupno implementirati IPv6 protokol i osigurati paralelnu koegzistenciju oba protokola.

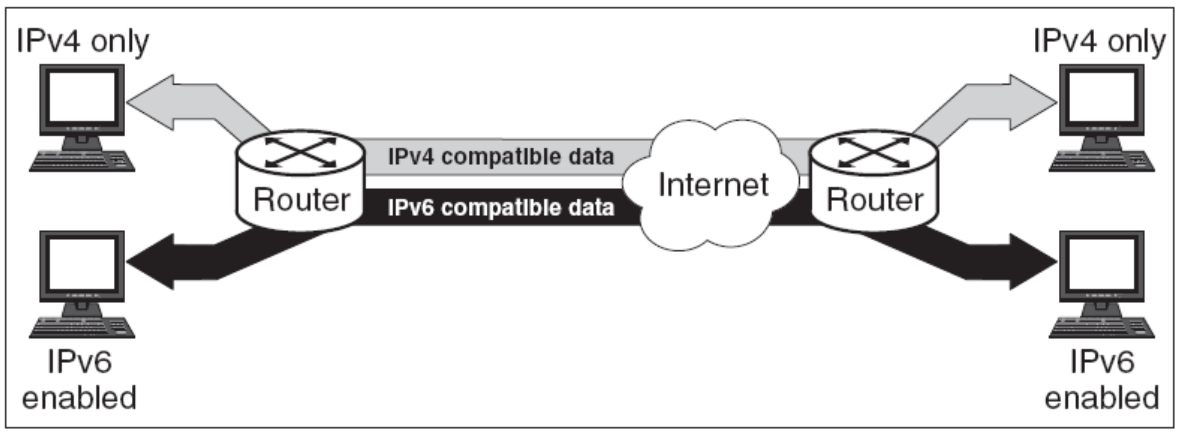
Za prijelazno razdoblje postoje 3 glavne tehnike (Wilkins, 2012):

- dvostruka konfiguracija (Dual Stack)
- tuneliranje (Tunneling)
- translacija (Translation)

6.1. Dvostruka konfiguracija

Dual-stack uređaj je bilo koji uređaj koji se spaja na internet i konfiguriran je s IPv4 i IPv6 adresom istovremeno. Kod implementacije dual stack-a ne mora se odlučivati o IPv4 ili IPv6 (“Dual-Stack Will Deliver IPv6 Connectivity”, bez dat.). Istovremeno su pokrenute obje verzije protokola i neovisni su jedan o drugome iako je IPv6 protokol preferirana metoda transporta. Izbor verzije protokola za enkapsulaciju i rutiranje paketa ovisi o ciljanoj adresi. U slučaju kada je moguće koristiti obje verzije za slanje paketa prema odredištu, prioritizira se upotreba IPv6 protokola. Kada se otkrije dolazni IPv6 promet, IPv6 umrežavanje je krajnji rezultat. Kada IPv4 promet uđe u mrežu, svaki mrežni uređaj dobiva upute da se vrati na IPv4 umrežavanje (”Prijelaz

s IPv4 na IPv6", bez dat.). Za korištenje ove metode potrebno je odvojiti više procesnih resursa na uređajima. Uređaji preferiraju IPv6 put kada je on dostupan. Barem, to vrijedi na razini operacijskog sustava, jer aplikacije mogu slijediti vlastita pravila. To vrijedi i za DNS, jer će uređaj tražiti AAAA (IPv6 DNS) zapise prije A (IPv4 DNS) zapisa. DNS igra ključnu ulogu u implementaciji IPv6. DNS poslužitelj s omogućenim IPv6 nije potreban za vraćanje AAAA zapisa. IPv6 je potreban samo u korisnom učitavanju. Osnovni transport koji se koristi za isporuku informacija uređaju još uvijek može biti IPv4 ("IPv4/IPv6 Dual Stack", 2021). Oba TCP/IP protokola su omogućena na usmjerivačima širokopojasne mreže (WAN), nakon čega slijede vatrozidi, usmjerivači podatkovnog centra i na kraju usmjerivači za pristup stolnim računalima. Prednost ovog pristupa je što ga podržavaju glavni dobavljači usluga. Nedostataka ovog pristupa je taj što mnogi naslijeđeni operativni sustavi ne podržavaju dual stack funkcionalnost. Stoga će se organizacija s naslijeđenim sustavima u svojoj postojećoj infrastrukturi morati financijski obvezati na potpuni prijelaz na novije sustave (Wilkins, 2012). Na slici 11 prikazan je primjer dvostruke konfiguracije.



Slika 11: Primjer Dual-Stack konfiguracije (https://www.cables-solutions.com/what-is-ipv4-ipv6-dual-stack-and-mpls-technique.html/ipv4-ipv6-dual-stack, 2017)

Kod implementacije Dual-Stack treba uzeti u obzir nekoliko stvari (“IPv6 Migration”, bez dat.):

- Neki mrežni uređaji imaju ograničen TCAM (Ternary content-addressable memory) prostor ; pokretanje IPv4 i IPv6 može iscrpiti ovaj prostor
- Mogu li mrežni uređaji podnijeti dodatnu propusnost
- Imaju li sigurnosni uređaji (kao što su vatrozid ili IPS) iste značajke za IPv6
- Postoje li naslijeđene aplikacije koje neće raditi s IPv6
- Postoje li neki stariji uređaji koji ne podržavaju IPv6.

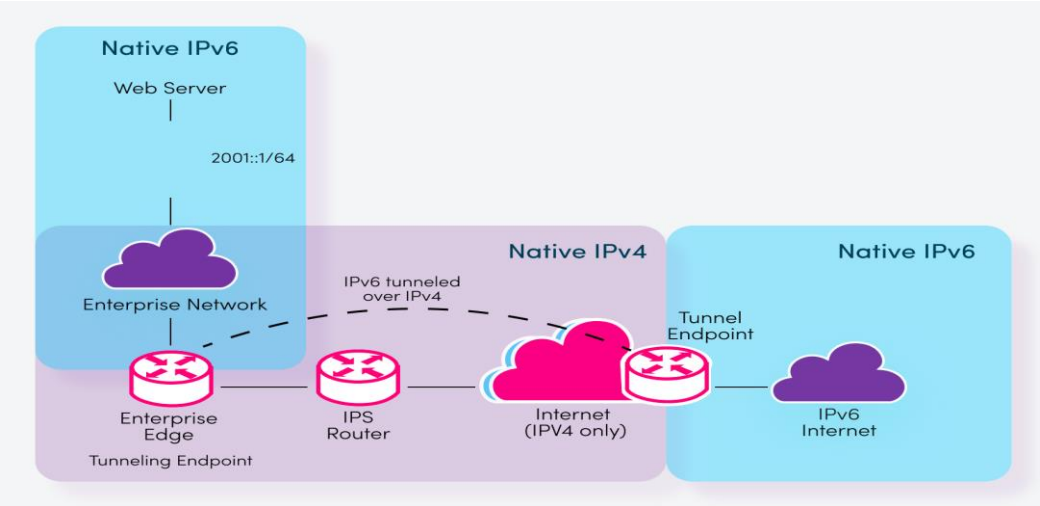
Osnovni postupak za korištenje Dual-Stack (“IPv6 Migration”, bez dat.):

1. Omogućite IPv6 usmjeravanje
2. Dodati sučeljima IPv6 adrese
3. Napravite DNS zapise

“Dvostruka konfiguracija omogućuje poslužiteljima, klijentima i aplikacijama postupak prelazak na novi protokol” (“Prijelaz s IPv4 na IPv6”, bez dat.). Gdje je moguće, prvi izbor bi trebao biti Dual-Stack. Rješenja s dvostrukom konfiguracijom često se zagovaraju kao prijelazna tehnologija za prelazak s IPv4 na IPv6. Promjene na IPv4 mreži ne utječu na promjene u IPv6 mreži. Korištenje dvostruke konfiguracije zahtijeva da svi uređaji u potpunosti podržavaju IPv6. Dvostruka konfiguracija predstavlja efikasan i jednostavan način tranzicije te se preporučuje u situacijama gdje mrežne komponente podržavaju paralelno pokretanje protokola. U situacijama gdje takva mogućnost nije ostvariva, , neophodno je primijeniti alternativne tehničke pristupe (Wilkins, 2012).

6.2. Tuneliranje (Tunneling)

Tuneliranje je proces skraćivanjem IPv6 paketa i enkapsulacije IPv6 paketa unutar IPv4 paketa i obrnuto. To omogućuje prijenos IPv6 paketa kroz postojeće IPv4 okosnice, budući da je postojeća IPv4 infrastruktura usmjeravanja potpuno nesvjesna inkapsuliranih IPv6 paketa. Na slici 12 prikazan je primjer konfiguracije tunela.



Slika 12: Primjer IPv6 tunela (“IPv6 Tunnelling”, bez dat.)

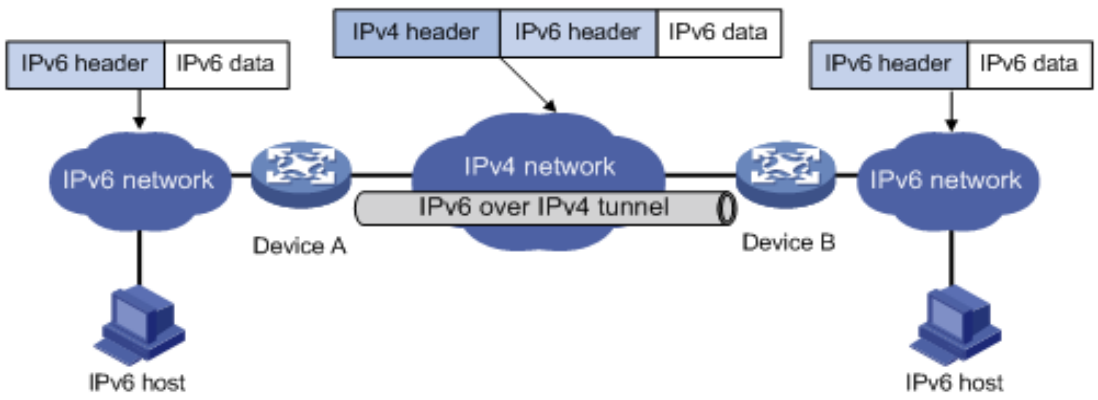
Potrebno je prethodno uspostaviti povezivanje između rutera na oba kraja tunela kako bi se omogućila komunikacija kroz tunel. Početna točka IPv4 paketa se referira na lokalni usmjerivač na početku tunela, dok se odredište odnosi na usmjerivač smješten na suprotnom kraju. Primanjem paketa odredišni usmjerivač čita posebne zastavice unutar IPv4 paketa dajući mu upute da dekapsulira IPv4 pakete i traži IPv6 pakete unutar njih te ih usmjerava dalje koristeći IPv6 adresu na IPv6 mrežu (“IPv6 Tunnelling”, bez dat.) . Postoje dvije vrste tuneliranja, a to su: statičko tuneliranje i automatsko tuneliranje. Glavna razlika između automatskog i statičkog tuneliranja je automatsko određivanje krajnje točke tunela (“Types of tunnels”, bez dat.).

Statički tuneli

U statičkom tuneliranju adresa je konfigurirana na krajnjoj točki tunela i konfiguracija je ručna. Enkapsulirajući čvor je odgovoran za pohranjivanje informacija o tuneliranju. Pohranjuje adresu krajnje točke tunela koja će biti odredišna adresa. Osim toga, pohranjuje informacije o usmjeravanju kako bi se odredilo koje pakete tunelirati (“Types of tunnels”, bez dat.).

Automatsko tuneliranje

U automatskom tuneliranju IPv6/IPv4 čvorovi mogu automatski odrediti krajnju točku tunela koja se izvlači iz IPv6 adrese. Čvorovi posjeduju mogućnost odlučivanja koji se paketi automatski tuneliraju, a koje ne (“Types of tunnels”, bez dat.). Implementacija tunela uzrokuje smanjenje maksimalne jedinice prijenosa (eng. Maximum Transmission Unit)) uslijed redukcije paketa za dvadeset okteata zbog pridodanih IPv4 zaglavlja. Osim toga korištenje tunela može dodatno kompliciratи i otežati proces prilikom dijagnosticiranja i rješavanja mrežnih problema. Automatsko tuneliranje pruža moćnost uspostave veze između kolokacija zaobilazeći potrebu konverzije tranzitne mrežne infrastrukture što je prikazano na slici 13. Tuneliranje je zadovoljavajuće kao kratkoročno sredstvo malog opsega, ali ne kao rješenje većeg opsega. Tunel zahtijeva upravljanje, a to je skupo i složeno (“Prijelaz s IPv4 na IPv6”, bez dat.).



Slika 13: Primjer tuneliranja (IPv6 over IPv4 tunneling , bez dat.)

Postoje nekoliko vrsta i načina tuneliranja (Wilkins, 2012):

- Manual
- 6RD
- ISATAP
- 6to4 tunneling
- LISP (Farinacci, 2013)
- DS-LITE (“IPv6 Dual-Stack Lite”, 2022)
- Toredo (“IPv6 tunnel technologies”, 2013)
- Tunnel Broker (Durand, 2001)

Ručno tuneliranje (Manual tunneling)

“Administrator ručno konfigurira statičke IP adrese na sučelju na početku i na kraju tunela. Uređaj ili usmjernik na svakom kraju tunela mora podržavati oba protokola.” (“Prijelaz s IPv4 na IPv6”, bez dat.) Ručno kreiran IPv6 tunel konfigurira se između dva usmjerivača od kojih svaki mora podržavati i IPv4 i IPv6. Dolazni promet koji je namijenjen mrežama s druge strane tunela enkapsuliran je na izvornom usmjerivaču i tuneliran kroz IPv4 (Conta, 1998) .

Ručni tunel je slično VPN-a konekciji sa nedostatkom enkripcije. Mogu se koristiti razni protokoli (“Prijelaz s IPv4 na IPv6”, bez dat.):

- GRE tunnel (Generic Routing Encapsulation)
- PPIP (IP preko IP) tunel
- DMVPN (GRE multipoint sa IPSec)

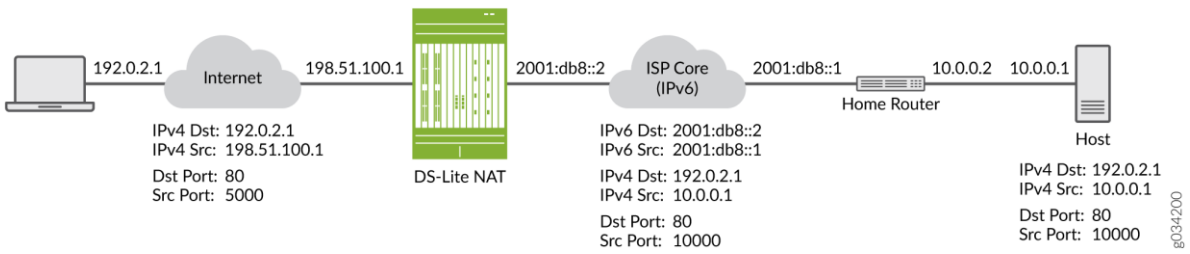
Svaka od opcija ima prednosti i nedostatke. GRE podržava multicast, dok IPIP ne. No, ima veće zaglavlje, što smanjuje MTU. GRE je dobar izbor u IS-IS (Intermediate System to Intermediate System) sizuaciji, jer može prenositi ne-IP promet. IPIP kodira IPv6 adresu u IPv4 zaglavlju.

6RD

6RD (Rapid Deployment) omogućuje brzo prenošenje IPv6 sadržaja klijentima. U ovoj se tehnici IPv4 još uvijek koristi na rubnom djelu mreže davatelju usluga. 6RD omogućuje davatelju usluga (SP) pružanje unicast IPv6 uslugu korisnicima preko svoje IPv4 mreže korištenjem enkapsulacije IPv6 u IPv4. To ograničava zahtjev za kapitalnim troškovima za davatelje usluga koji mogu podržavati IPv6 bez zamjene opreme kod krajnjeg korisnika (Townsley, 2010).

DS-LITE

IPv6 dual-stack lite (DS-Lite) je tehnologija koja pružateljima internetskih usluga omogućuje prelazak na IPv6 mrežu dok istovremeno koriste IPv4 adrese. DS-Lite omogućuje pružateljima usluga prelazak na IPv6 pristupnu mrežu bez promjene softvera ili hardvera krajnjeg korisnika. Uređaj koji pristupa internetu ostaje isti, čime se korisnicima IPv4 omogućuje nastavak pristupa IPv4 internetskom sadržaju uz minimalne smetnje u njihovim kućnim mrežama, dok korisnicima IPv6 omogućuje pristup IPv6 sadržaju (“IPv6 Dual-Stack Lite”, 2022).



Slika 14: Primjer DS-Lite NAT (IPv6 Dual-Stack Lite, 2022)

Slika 14 ilustrira DS-Lite arhitekturu koja koristi IPv6 veze između pružatelja i korisnika dok održava IPv4 (ili dual-stack) hostove u korisničkoj mreži.

LISP

LISP (*eng. Locator ID Separation Protocol*) je tehnologija preklapanja. Pokreće se na IP (trećem) mrežnom sloju . LISP koristi dvije zasebne IP adrese: adresu za identifikatore krajnjih točaka nazvanu Endpoint Identifier (EID) i adresu za označavanje lokatora usmjeravanja koja se zove Routing Locator (RLoc). Ove adrese sadržavaju informacije o IP adresama i sesijama između uređaja (Farinacci, 2013).

ISATAP

ISATAP (*eng. Intra-Site Automatic Tunnel Addressing Protocol*) koristi dual-stack čvorove koji se povezuje na IPv6 pristupnik preko IPv4 mreže. Host koristi DNS da otkrije lokaciju pristupnika. Zatim gradi tunel do pristupnika preko IPv4 mreže. Odavde, host može pristupiti IPv6 adresama. Prednost ovoga je što omogućuje kontrolu od kraja do kraja, što je dobro za sigurnost. Nedostatak je što ne podržava multicast i ne podržava NAT (Templin, 2008) .

Toredo

Prenosi IPv6 paket preko IPv4 mreže inkapsuliranjem IPv6 paketa u UDP pakete koji se usmjeravaju preko NAT uređaja na internet (Hoagland, bez dat.).

6to4 tunneling

6to4 tunneling je tehnika koja prenosi IPv6 pakete preko postojeće IPv4 infrastrukture bez potrebe za kompleksnim promjenama u mrežnoj konfiguraciji što je posebno korisno tijekom prijelaza s IPv4 na IPv6. Funkcioniranje 6to4 tuneliranja se temelji na korištenju javnih IPv4 adresa kao osnova za generiranje jedinstvenih IPv6 adresa uređaja. Za ispravno funkcioniranje ovog pristupa potrebna je podrška usmjerivača i mrežne opreme koja prepoznaje i obrađuje ovu vrstu tuneliranja (“IPv6 over IPv4 tunneling”, bez dat.).

Tunnel Broker

Tunnel broker je pružatelj usluga koji nudi IPv6 preko IPv4 mreže. Na rubnom djelu mreže koristi se uređaj s omogućenim IPv6 protokolom za izgradnju tunela do odabranog pružatelja usluga. IPv6 tunel zatim prolazi preko IPv4 podložne mreže koja preusmjerava dalje na IPv6 internet. Ovo je opcija ako trebate pristupiti IPv6 internetu, ali ne možete implementirati IPv6 na rubu svoje mreže tj. na rubnom djelu mreže nemožete dobiti javnu IPv6 adresu (Durand, 2001).

6.3. Translacija

Prethodna dva pristupa mogu biti korisni u komunikaciji između dvije izolirane IPv4 mreže ili dvije izolirane IPv6 mreže. Dok translacija omogućava komunikaciju između IPv6 i IPv4 uređaja u slučajevima u kojim oba uređaja nisu sposobna podržavati obe verzije navedenih protokola i neophodna je kada je većina mreže na IPv6 protokolu, ali neki sustavi jos uvijek koriste IPv4 npr. legacy sustavi. Translacija je u definiciji pristupni mehanizam koji omogućuje IPvX mreži da komunicirati izravno s IPvY mrežom prevodeći IPvX paket u IPvY paket kako bi se omogućila komunikacija (Novaković, bez dat.).

“Translacija je u osnovi proširenje NAT tehnike. NAT-PT (NAT-Protocol Translation) je sustav translacije koji se nalazi između IPv6 i IPv4 mreže i mapira IPv6 adrese u IPv4 i obrnuto, odnosno prevodi IPv6 pakete u IPv4 pakete i obrnuto.” (“Prijelaz s IPv4 na IPv6”, bez dat.). Translacija je koristan na rubnom djelu mreže te u situacijama gdje je potrebno povezivanju IPv6 uređaja na IPv4 internet ili IPv4 na IPv6. Tuneliranje je poželjnije od translacije kada je unutar mreže. Translacija se oslanja na dobro funkcioniranje DNS-a. Nije prikladno rješenje kada aplikacije ima tvrdo kodirane IP adrese unutar svojih postavka (Baker, 2011). U nastavku ćemo detaljnije proučiti nekoliko modela translacije u koje spadaju: NAT64, DNS64 i SLB64.

NAT64

NAT64 je mehanizam tranzicije i koegzistencije između IPv4 I IPv6 protokola. Dopušta IPv6 klijentima pokretanje komunikacije s IPv4 poslužiteljem . Također omogućuju peer-to-peer komunikaciju između IPv4 i IPv6 čvora, gdje se komunikacija može pokrenuti kada bilo koji kraj koristi postojeći NAT- traversal ili peer-to-peer komunikacijske tehnike, a pokretanje komunikacije moguće je u bilo kojem smjeru.

Neki nedostaci NAT64 su to što može razbiti HTTP zaglavlja koja koriste klijentske IP adrese . Također, NAT64 može izgledati kao DoS napad na nekim sigurnosnim uređajima zbog mnogih uslugama koje mogu kontinuirano pristupati s jedne IP adrese (“Understanding and Configuring NAT64”, 2021).

DNS64

DNS64 se može koristiti za sintetiziranje AAAA zapisa tamo gdje ne postoje. DNS64 radi zajedno s NAT64 uređajem. DNS64 omogućuje razlučivanje IPv4 adresa stvaranjem sintetiziranih IPv6 AAAA zapisa za hostove gdje AAAA zapis nije dostupan. To se postiže uparivanjem IPv6 prefiksa s IPv4 adresom dobivenom pretraživanjem A-zapisa. IPv4 adresa je umetnuta unutar posljednja 32 bita IPv6 adrese. Promet poslan na bilo koju adresu u IPv6 prefiksu zatim se usmjerava na NAT64 uređaj, koji se povezuje na mapirano IPv4 odredište u ime IPv6 klijenta i prenosi podatke između IPv4 i IPv6 veze (“About DNS64”, bez dat.).

SLB64

Balansiranje opterećenja poslužitelja (eng. Server Load Balancer) korisno je kada postavljate sučelje za IPv6 internet. SLB64 pruža IPv4 resurse IPv6 hostovima skrivanjem IPv4 adresa iza virtualne IPv6 adrese. Ovo je pomalo poput korištenja NAT64, ali se implementira na bazi aplikacije. Ovo je kratkoročno rješenje, ali je prikladno kada postoje naslijeđene aplikacije koje ne podržavaju IPv6 (Horley, 2016).

6.4. Migracija na IPv6

Budućnost interneta leži u prilagodbi novim zahtjevima sve brojnijih korisnika, a IPv6 se ističe kao evolucijski korak u daljnjem razvitku i ekspanziji internetskog prostora. U stvarnosti većina web-mjesta na kojima je omogućen IPv6 i dalje su dostupna pod IPv4 adresama i još se uvijek vežu primarno uz te adrese (“Uvodi se novi standard na internetu IPv6”, 2012). Osnovna pretpostavka je da, za u doglednoj budućnosti, organizacije će ili upravljati dvostrukim mrežama ili prihvatiti umrežavanja na druge načine. Međutim, krajnji cilj je prijelaz samo na IPv6 mrežu ili barem onu usmjerenu na IPv6. Iako većina interneta još uvijek radi na IPv4, mnoge su tvrtke i organizacije započele migraciju na IPv6. Kako međusobno nisu interoperabilni, usvajanje novog protokola zahtijevat će i obnovu ili nadogradnju postojeće hardverske i softverske infrastructure. Dobra vijest je da je IPv6 definiran prije više od 2 desetljeća te ga većina hardverskih i softverskih sustava već podržava. Postoje i neki naslijeđeni ili ugrađeni sustavi koji nikada neće prijeći i koji će i dalje morati raditi na IPv4 dok se ne mogu zamijeniti ili povući u budućnosti.

Polazna točka implementacije IPv6 je identificiranje ciljeva za budućnost – planiraju li se dodati nove lokacije, preseliti se u oblak ili implementirati više IoT uređaja. Bez potrebnog adresnog prostora to će biti sve veći problem. Što duže organizacija čeka prije migracije na IPv6, veća je vjerojatnost da će početi preklapati adresne prostore u različitim regijama, što povećava složenost upravljanja infrastrukturom i utječe na opskrbu uređaja i aplikacija. IPv6 je budućnost i u nekom trenutku nadogradnja bit će neizbježna (Avirneni, 2021). U sljedećem dijelu rada fokus je na strategije planiranja migracija na IPv6 tehnologiju za srednje i velike organizacije. Za kućne-privatne korisnike i male organizacije do 10 ljudi prelazak na IPv6 ne zahtijeva velike prenamjene niti planiranja. Prema navodima Hoffmana (2016) za to su potrebne samo tri stvari:

1. Operativni sustav kompatibilan s IPv6
2. Usmjerivač s podrškom za IPv6
3. ISP s omogućenim IPv6

Za velike organizacije i ISP-ove situacija je malo kompliciranija te zahtjeva stručan i temeljit pristup prilikom planiranja i implementacije. Fazna implementacija omogućit će organizaciji implementaciju IPv6 uz što manje ometanja trenutnog okruženje što je više moguće. Pristup u fazama smanjit će utjecaj na svakodnevne operacije. Hoffman (2016) navodi dva glavna pristupa prijelaznoj implementaciji:

- Aktivna IPv6 implementacija
- Pasivna IPv6 implementacija

Aktivna IPv6 implementacija

U aktivnom pristupu, omogućuje se dual stack (IPv4/IPv6) na opremi u kratkom roku unutar cijele mreže. Ovakav scenarij prikladan je kada je uglavnom nova oprema koja podržava i IPv4 i IPv6. Nakon što se potvrdi ispravan rad temeljne usluge i mehanizma prevođenja, IPv4 mreža se onemogućuje na svim uređajima na mreži, ostavljajući IPv6 dominantnu mrežu (Hoffman, 2016).

Pasivna IPv6 implementacija

U ovom pristupu omogućuje se IPv6 pojedinim segmentima mreže ili čvorovima u IPv4 dominantnoj mreži. Nakon što većina rubnih uređaja prijeđe na IPv6, jezgra mreže prelazi ili na dvostruku konfiguraciju ili samo na IPv6. Pasivna implementacija zahtijeva podršku i IPv4 i IPv6 promet tijekom trajanja implementacije. Ovaj pristup široko koristi IPv4/IPv6 i IPv6/IPv4 tuneliranje. Ovaj je scenarij prikladan kada postoji veliku baza starije opreme ili usluga koje ne mogu prijeći na IPv6.

Dvije glavne razlike između IPv6 aktivne i pasivne implementacije su (Hoffman, 2016):

- Aktivna implementacija IPv6 ima kraći životni ciklus od pasivne implementacije.
- Pasivna implementacija trajati će dulje i koristi mehanizme tuneliranja.

Oba scenarija implementacije pokrivena su istim planom i sve faze implementacije su iste bez obzira na pristup.

6.5. Metodologija migracije

Za uspješnu migraciju potrebno je zadovoljiti nekoliko faza (“IPv6 Migration”, bez dat.):

1. Otkrivanje
2. Analiza
3. Planiranje i dizajn
4. Provedba
5. Optimizacija mreže

1. Faza otkrivanja

Faza otkrivanja fokusira se na posao. Ovdje se identificiraju poslovni ciljevi i pokretači. Postavlja se pitanje zašto je potrebno koristiti IPv6? Kakav je utjecaj na poslovanje ako koristimo IPv6? Kakav je utjecaj ako se to ne učini?. “Poslovanje tvrtke mora se analizirati kako bi se bolje razumjele posljedice koje IPv6 može imati za poduzeće.” (Martins de Castro, bez dat.)

Za IPv6 migraciju potrebno je opravdanje u poslovnom smislu. Potrebno je uzeti i u obzir vremenski okvir , usklađenost vlade i zakona ili industrije pa tako i zemljopisnu lokaciju mjesta (“IPv6 Migration Strategy”, 2012). Svaka organizacija u svakoj industriji trebala bi pronaći način na koji im IPv6 može pomoći pri njenom poslovanju. Faza otkrivanja bavi se prikupljanjem zahtjeva i potreba. Važno je razumijeti trenutno okruženje prije implementacije IPv6. Razumijevanjem trenutnog okruženja, može se odabrati ispravan prijelazni pristup tranziciji.

Neka od potencijalnih opravdanja koje treba razmotriti uključuju (“IPv6 Migration”, bez dat.):

- Proširenje poslovanja ili klijenti zahtijevaju IPv6 podršku
- Širi li se poslovanje u zemlje u kojima je IPv4 adrese teško ili skupo nabaviti
- IPv6 je jeftiniji (po adresi) za registraciju od IPv4
- Postoje li zahtjevi za usklađivanjem u industriji
- Treba li podržavati IPv6 za rastuće tržište mobilnih uređaja i aplikacija.

Martins de Castro (bez dat.) u svom radu navodi kako su neke tvrtke već u potpunosti svjesne potrebe za migriranje na IPv6, čineći ovaj korak čak i nepotreban. Međutim, velik postotak tvrtki i organizacija u cijelom svijetu ne zna zašto moraju migrirati na IPv6 ili prednosti koje IPv6 protokol može donijeti.

2. Analiza

"Ovdje se identificiraju potencijalni problemi i zapreke koje se mogu dogoditi prilikom implementacije." ("IPv6 Migration", bez dat.). Prijelaz na IPv6 daje priliku za rješavanje problema u trenutnom okruženju. Worthen (2006) navodi kako je jedan od ključnih zadataka u početnoj fazi je provođenje opsežnog popisa IP opreme i usluge. Potrebno je saznati i imati detaljan uvid što se točno nalazi na mreži i odrediti što je već usklađeno s IPv6 ili se može nadograditi na novi protokol. Uvid nije ograničeni samo na usmjerivače i skretnice, već uključuju sigurnosne alate poput vatrozida, prijenosnih računala, pisača i sustava nadzora (Martins de Castro, bez dat.).

Nekoliko stvari koje u ovoj fazi moramo sagledati (Martins de Castro, bez dat.):

- Postoji li oprema koja nema IPv6 podršku
- Podržava li neka oprema djelomične IPv6 značajke. Na primjer, IPv6 transport može biti podržan, ali OSPFv3 nije ("IPv6 Migration", bez dat.)
- Hoće li biti potreban mehanizam prevođenja?
- Je li potrebno dodatno licenciranje za IPv6 na razini aplikacija
- Postoje li aplikacije koje koriste tvrdo kodirane IP adrese
- Razumije li tehničko osoblje IPv6 protokol
- Uskladiti planove za tranziciju IPv6 sa svojim dobavljačima ("IPv6 Migration", bez dat.).

3. Planiranje i dizajn

Cisco (2011) navodi kako je potrebno izraditi plan koji će sadržavati detaljne informacije kao što su vremenski okviri, uređaji za migraciju i prioriteti implementacije. Uz izradu plana migracije potrebno je i detaljno izraditi topologiju mreže te hijerarhijsku podjelu adresne strukture za svaki dio mreže, uzimajući u obzir regije, podatkovne centre i poslužitelje. Također moraju se razmotriti aplikacije koje trebaju podržati i definirati adresni prostor kako bi se dobro iskoristilo usmjeravanje i definicije pravila ili protokola unutar organizacije. Ako je cilj skaliranje, IPv6 će pojednostaviti usmjeravanje i znatno olakšati proces. Uređaji na mreži moraju biti sposobni podržavati IPv6 adresu i protokol, dok i dalje rade s postojećim IPv4 adresama. Ako uređaj ne može podržati IPv6 adresu, neće ga biti moguće locirati niti će biti u mogućnosti pravilno komunicirati s ostalim uređajima na mreži. Početno mjesto utječe na strategiju migracije. Dual-Stack je preporučeni pristup u većini slučajeva. Ukoliko se počne u jezgri ili od neke podružnice potrebno je tuneliranje. Razbijanje složenih situacija na manje elemente kojima je lakše upravljati i na kojima je lakše raditi olakšat će i ubrzati sam proces.

Nekoliko važnih stvari koje je po Audinu (2020) potrebno uzeti u obzir prilikom planiranja migracije:

- dobro planiranje implementacije
- nabavka IP adresa – odluka o korištenju PA (Provider Aggregatable) ili PI (Provider Independent) adresiranja
- odabir migracijske tehnologije i alata (Dual-Stack, tunel i translacija)
- odabir mjesta za početak implementacije (rubne točke, jezgra mreže ili branch office)
- potrebno je iskoristiti promjenu kako bi se postojeće strukture učvrstile i unaprijedile
- inkrementalna (agilna) metodologija dopušta sistematsko testiranje svake faze i omogućava kontrolirano povratno kretanje u slučaju pogrešaka
- dobra dokumentacija

- način dodjele adresa uređajima (DHCP, SLAAC ili ručno)
- odrediti kako rukovati postojećim IPv4 i novim IPv6 inventarom.
- planiranje vremena i resursa
- obuka osoblja.

4. Implementacija

Faza implementacije prema smjernicama Cisca (2011) uključuje sigurnu instalaciju i konfiguraciju IPv6 opreme, tunela, i mehanizma prevođenja. Faza implementacije razlikuje se ovisno o scenariju implementacije (pasivno ili aktivno). Potrebno je osigurati neprekidan rad postojećih usluga tokom implementacije, a ukoliko su prekidi neizbježni, njihovo trajanje treba minimizirati. Implementacija se razdvaja na sastavna područja koja je lakše implementirati pojedinačno i neovisno jedno o drugome i time smanjuju problem integracije, omogućavajući da se neki poslovi rade paralelno (Cisco, 2011):

1. Eksperimentalna faza- Početak migracije polazi s malom implementacijom ili testnom fazom. Potreno je testirati IPv6 konfiguraciju i pretpostavke dizajna u odnosu na postojeću opremu, testirati i procijeniti novu IPv6 opremu i započeti obuku osoblja. Nakon što se isprave sve greške može se krenuti na ostatak mreže. Ovo je učinkovita početna točka za izlaganje IPv6 operacijama bez utjecaja na poslovanje.
2. Jezgra i tuneliranje- faza koja omogućuje izvorni IPv6 transport u jezgri mreže i proširenje povezanosti s tunelima između unutarnjih ili vanjskih dijelova mreže (Podružnica), pokrećući obje verzije protokola.
3. Integracije u radnu površinu- računala, serveri i ostali uređaji te pristupni dijelovi mreže.

Faze 2 i 3 mogu se odvijati paralelno. Sve dok mrežna jezgra ne postane omogućena za IPv6, aktivnosti faze 3 mogu koristiti tunele.

1. Potpuna implementaciju IPv6- integriracija u sve aspekte mreže i puni opseg implementacije IPv6 u sva operativna područja (aplikacije,baze podataka, nadzorne sustave itd.).

5. Optimizacija mreže

"Ovo je kontinuirani proces koji zahtijeva praćenje procesa, povratnih informacija i podešavanje mreže." ("IPv6 Migration", bez dat.) Moguće je kombinirati prelazak na IPv6 s korištenjem sljedeće generacije hardverskog ili softverski definiranog DDI-a(DNS, DHCP i IPAM), koji bi im omogućio još veće performanse, mogućnosti automatizacije i napredne značajke upravljanja prometom, uključujući širenje DNS promjena u milisekundama i poboljšano, optimalno usmjeravanje. Softverski definiran DDI također ima prednost što podržava infrastrukturu koja je izvorna u oblaku (Avirneni, 2021).

6.5.1. Struktura IPv6 mreže i adresiranje

6.5.1.1. Segmentacija mreže

Većina mreža sastoji se od različitih grupa korisnika s različitim zahtjevima za pristup i zaštitu. Segmentiranjem mreže, administratori mogu ispuniti zahtjeve različitih grupa s pravilima kontrole pristupa kako bi zaštitili osjetljive web stranice, poveznice i uređaje na mreži. Cilj hijerajhiskog dizajna adresa je dati mogućnost logičnog grupiranja imovine i pojednostaviti administraciju i sigurnost. IPv6 adresni prostor je dovoljno velik da omogući različite metode organizacije adresnih blokova. Prema istraživanju Krstajić i suradnika (2019) potrebno je konfigurirati mrežne prefikse kako bi se osigurao adekvatan broj IP adresa za uređaje i čvorove unutar podmreža. Postupak segmentacije tokom faze tranzicije zahtijeva postupnu implementaciju kroz niz pojedinačnih podakcija, pri čemu se svaka IP podmreža obrađuje pojedinačno. U

sklopu ovoga postupka neophodno je izvršiti restrukturiranje i reorganizaciju IPv4 mreža i podmreža radi simplifikacije trenutačne mrežne topologije. Prije prelaska IP podmreža na dual-stack IPv4/IPv6, neophodno je provesti proces reorganizacije infrastrukture radi optimalnog usklađivanja. Ovime se postiže lakše razumijevanje i upravljanje konfiguracijama na uređajima za usmjeravanje i vatrozidima, istovremeno osiguravajući održavanje postojeće razine sigurnosti mreže.

Krstajić i suradnici (2019) u svom radu navode nekoliko važnih smjernica prilikom segmentacije mreže:

- IPv6 podmreže s čvorovima (radne stanice) moraju koristiti prefiks /64,jer zadnja 64 bita IPv6 adrese koriste se za identifikaciju interface-a.
- Access Control Lists (ACL) obično se definiraju po IP-u mreže stoga mora postojati semantička ekvivalencija između svim čvorovima u podmrežama
- Izbjegavati različite routing putanje za IPv4 i IPv6 promet.
- Koristiti isti VLAN u podmrežama za IPv4 i IPv6
- Različiti VLAN za IPv4 i IPv6 povećava složenost administracije i stvaraju komplikacije prilikom dijagnostike. Korištenje više različitih VLAN-anova za istu podmrežu stvara potrebu za dodatnim resursima pri uvođenju novih mrežnih funkcionalnosti ili servisa.
- Korištenje istih ruting protokola (npr. OSPF) za obje verzije protokola.
- Kod IPv6 rutiranja nužno je primjeniti protokol verzije koji je kompatibilan s IPv6 standardom. Potrebna je dodatna provjera pripadajućih usmjerivača da li podržavaju odgovarajuće protokole rutanja za IPv6.

6.5.1.2. Dodjela adresa

Za adresiranje IPv6 adresa su dostupni različiti mehanizmi upravljanja:

- Upravljane adresama (DHCPv6)

- Autokonfiguracija
- Manualno

DHCPv6

DHCP se široko koristi u IPv4 mrežama za dodijelu adresa. IPv6 pruža sličan mehanizam automatskog adresiranja pod nazivom DHCPv6. DHCPv6 nije isti protokol kao DHCPv4, ali pruža sličnu funkcionalnost. DHCPv6 je još uvijek osjetljiv na iste sigurnosne ranjivosti koje utječu na DHCPv4. Korištenje DHCPv6 ima sljedeće prednosti (Mrugalski I suradnici, 2018) :

- DHCPv6 može ograničiti manje raspone valjanih IPv6 adresa. Manji raspon dopušta implementaciju boljih pravila kontrole pristupa.
- DHCPv6 omogućuje lakše identificiranje klijenata na mreži za razliku od automatski konfiguriranih ili ručno konfiguriranih klijenata
- Lakše praćenje klijenata putem logova.

Autokonfiguracija

Uz automatsku konfiguraciju, računalo automatski samostalno generira IPv6 adresu. S autokonfiguracijom, generirane adrese su u širem rasponu valjanih adresa. Prednosti korištenja automatske konfiguracije uključuju (Krstajić i suradnici, 2019):

- Adrese su deterministčke
- Isti uređaj će uvijek generirati istu IP adresu.
- Administratori mogu unaprijed popuniti DNS i druge sustave za bilježenje valjanim hostovima.

Manual

Uz ručno upravljanje adresama, administratori ručno konfiguriraju svaki čvor i uređaj. Ova metoda zahtijeva više resursa od druge dvije metode opisane u ovom odjeljku. Organizacije često koriste manualno upravljanje adresama s dobro poznatim uslugama kako bi ih lakše otkrili ili njima upravljali. Upravljanje adresama u IPv6 izgleda slično metodama upravljanja adresama koje se koriste za IPv4. Nakon postavljanja IPv6, organizacije bi trebale koristiti kombinaciju metoda za upravljanje adresama. Administratori bi trebali koristiti ručno konfigurirane adrese za poslužitelje i servere. Klijentski strojevi će koristiti bilo koji DHCPv6 ili autokonfiguracija. Odluka koju metodu koristiti (DHCPv6 ili autokonfiguracija) će ovisi o tome kako administratori žele upravljati adresiranjem. Ako administratori žele upravljati svojim adresama odluka pada na DHCPv6 za upravljanje adresama. S druge strane, ako administratori žele dopustiti opremi da sama sebi dodijeli IP adresu bez dodatne mreže resursa ili administracije, odlučili bi se za autokonfiguraciju.

6.5.1.3. Serveri

Serveri trebaju biti dostupni preko IPv4 i IPv6 . Interface koji je povezan na IPv6 mrežu mora imati statičnu IP adresu (Krstajić i suradnici, 2019) :

- Dodjela statičke adrese preko DHCPv6 servera ili ručna konfiguracija servera
- Dodijeljena adresa mora biti registrirana u DNS zapis (“A” za IPv4, “AAAA” za IPv6).

6.5.1.4. Uređaji na mreži

Dodjelu IPv6 adrese treba omogućiti pomoću Stateful DHCPv6 servera što znači da onda usmjerivači i Layer 3 preklopnici trebaju biti opremljeni podrškom za IPv6 DHCP relay kako bi omogućili dodjelu IPv6 adresa u lokalnoj mreži.

- Ukoliko uređaji dobivaju dinamičke IPv4 adrese putem DHCP servera, tada bi se, s obzirom na iste parametre i postavke, trebali također konfigurirati za dobivanje IPv6 adrese putem stateful DHCPv6
- Kod manjih jednostavnijih mrežama, moguće je primijeniti SLAAC (Stateless Address Autoconfiguration) metodu u kombinaciji sa Stateless DHCPv6, kako bi se pojednostavilo upravljanje IT infrastrukturom (Krstajić i suradnici, 2019).

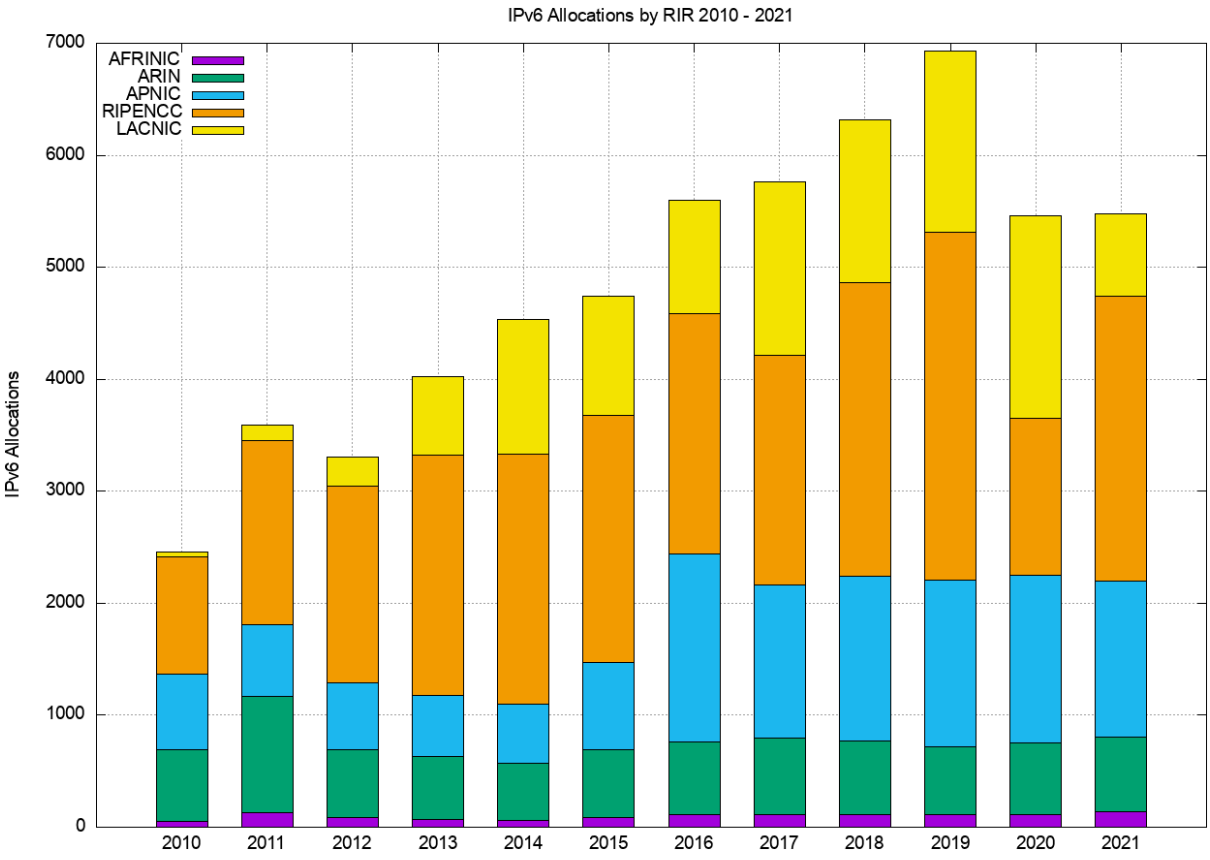
6.5.1.5. DNS

DNS je hijerarhijska distribuirana baza podataka koja prevodi nazive domena u IP adrese i jedan je od glavnih elemenata za funkcioniranje Interneta. DNS dodatno pruža zapise tipa AAAA što je namijenjeno pružanju podrške kod IPv6 protokola. DNS protokol omogućava neovisno izvršavanje upita za A i AAAA zapise, bez obzira na to je li upit primljen putem IPv4 ili IPv6 protokola. Izdvojit ćemo ključne atribute koje DNS poslužitelji namijenjeni IPv6 verziji moraju zadovoljiti (Thomson i suradnici, 2003):

- Osposobljeni DNS server za obradu i administraciju AAAA zapisa
- Izvršavati obradu zahtjeva putem IPv4 i IPv6 protokola.
- DNS server mora pružiti konzistentan odgovor bez obzira na to je li zahtjev klijenta stigao preko IPv4 ili IPv6 protokola.
- Prilagođeni u svrhu omogućavanja pravilnog izvođenja inverzne pretrage IP adresa (reverse lookup) za oba protokola
- Hostovima u dvostrukoj konfiguraciji asocirati pripadajuće adrese s identičnim nazivom
- Postojećim hostovima s A zapisom treba dodatno dodijeliti AAAA zapis.

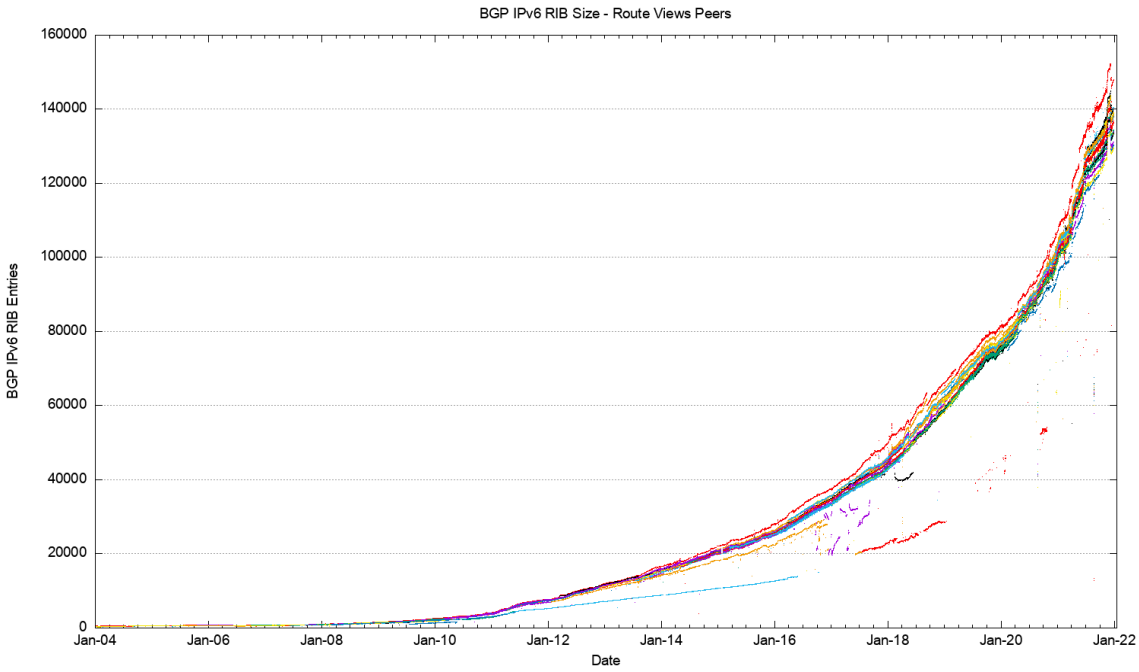
7. Budućnost IPv6 protokola i trendovi razvoja

Slika 15 prikazuje broj IPv6 adresa dodijeljenjih na godišnjoj bazi od strane RIR-ova. Prema analizi Huston-a (2022) broj dodjeljivanja je manji u odnosu na visoku točku u 2019. godini, a ovi brojevi ostali su konstantni na 5.400 izdvajanja godišnje tijekom 2020. i 2021.



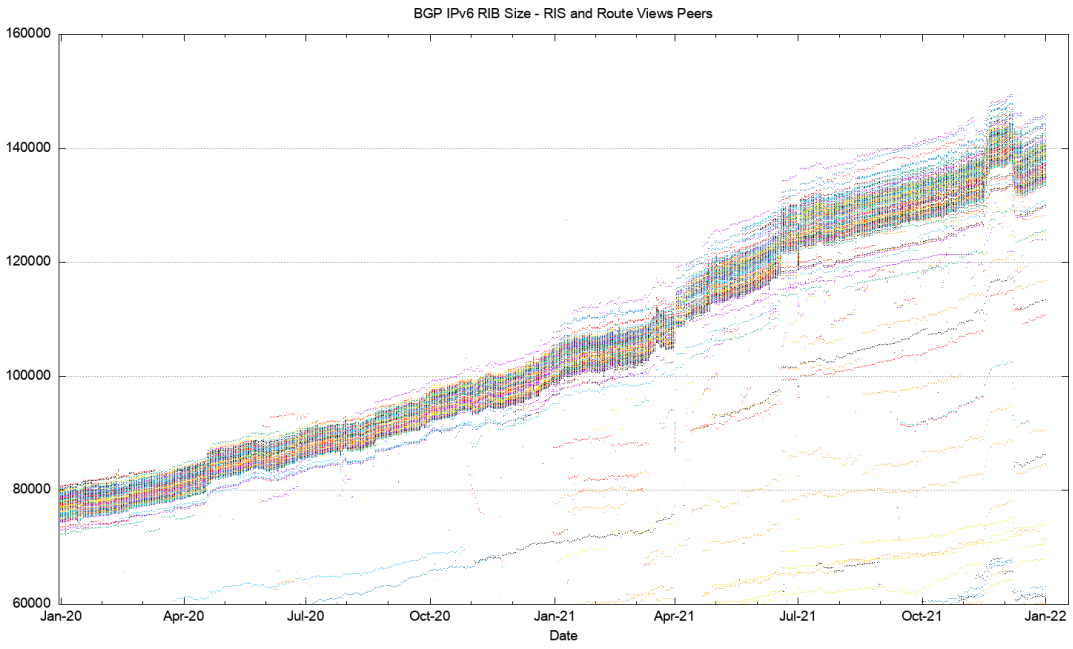
Slika 15: Distribucija IPv6 adresa po godinama (Huston, 2022)

Dugoročni trend rasta IPv6 mreže vidljiv na slici 16 očito se s vremenom povećava. Razumno prikladan za ove podatke je model eksponencijalnog rasta s faktorom udvostručenja od 24 mjeseca.



Slika 16: IPv6 usmjeravanje (https://www.ripe.net/analyse/statistics/?tags=ipv6, 2022)

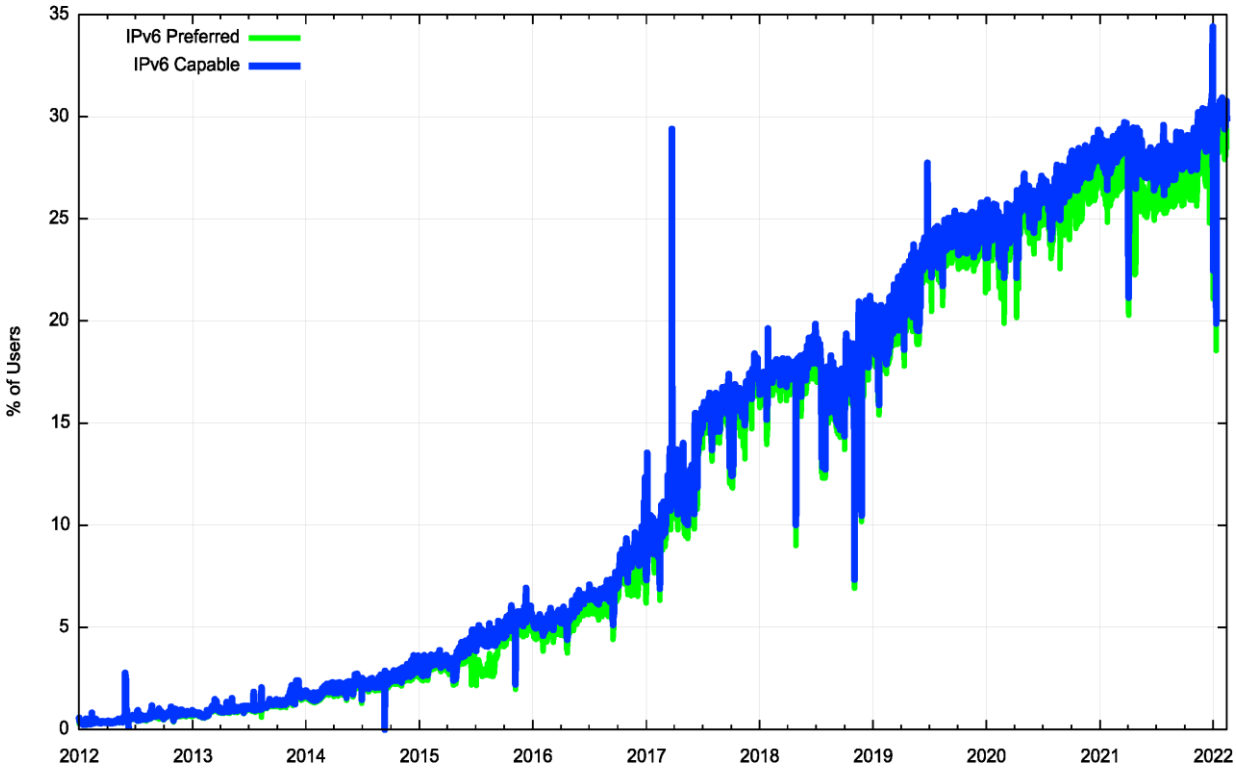
Detaljniji prikaz samo za 2021. godinu prikazan je na slici 17. Čini se da se stabilnost i performanse IPv6 sustava usmjeravanja poboljšavaju navodi Wilhelm (2022).



Slika 17: IPv6 BGP usmjeravanje za 2021. godinu (https://www.ripe.net/analyse/statistics/?tags=ipv6, 2022)

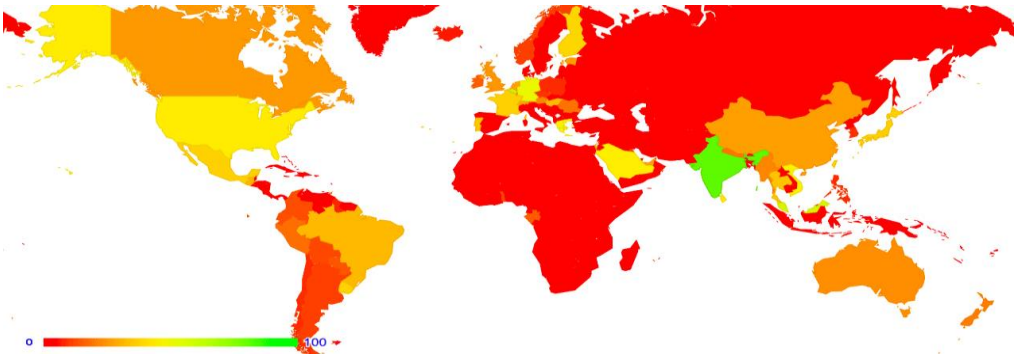
Pogledom na omjer korisnika koji pokazuju sposobnost dohvaćanja web-objekata putem IPv6 kao pokazatelja razine prihvaćenosti IPv6 na potrošačkom internetu.

Slika 18 prikazuje vremensku seriju ovog mjerenja od 2012. do početka 2022. Trenutačno je oko 31% baze korisnika interneta sposobno za IPv6, što ćini povećanje za 4% u usporedbi s prethodnih 12 mjeseci.



Slika 18: Upotreba IPv6 adresa, 2012–2022 (Huston, 2022)

Wilhelm (2022) navodi kako je očito da ovaj broj od 30% nije ravnomjerno raspoređen po Internetu, a karta mjesta gdje se IPv6 korisnici nalaze prikazana je na slici 19.



Slika 19: Globalna distribucija korisnika IPv6 protokola (https://stats.labs.apnic.net/ipv6/, 2022)

Jasno je da je usvajanje IPv6 vrlo raznoliko. Iako je u Indiji visoka stopa usvajanja (76% korisnika), postoji samo pet drugih gospodarstava u kojima je stopa usvajanja IPv6 preko 50% korisnika (Belgija, Malezija, Njemačka, Vijetnam i Grčka).

Ako promatramo implementaciju IPv6 kao postotak svake nacionalne populacije i usporedimo mjerenje na početku 2021. s onim na kraju godine, možemo dati popis gospodarstava koja imaju najveću promjenu u tom omjeru korisnika IPv6. To je prikazano na slici 20.

Rank	V6 Ratio			Users (Est.)	Name
	2021	2022	Change		
1	10%	37%	28%	9,004,547	Guatemala
2	17%	38%	21%	7,341,817	Israel
3	30%	49%	19%	32,204,986	Saudi Arabia
4	1%	15%	14%	16,308,208	Chile
5	20%	33%	13%	820,328,035	China
6	13%	26%	13%	7,081,783	Nepal
7	18%	29%	11%	8,278,192	Austria
8	19%	29%	10%	20,900,003	Myanmar
9	0%	10%	10%	2,263,165	El Salvador
10	0%	9%	9%	1,617,110	Jamaica

Slika 20: Top 10 ekonomija sa najvećim porastom upotrebe IPv6 (Huston, 2022)

Drugi način za generiranje ovog poretka je korištenje procijenjene populacije onih korisnika koji koriste IPv6 i promjene u ovom broju tijekom 2021. Što je prikazano na slici 21.

Rank	V6 Users			Users (Est.)	Name
	2021	2022	Change		
1	164,459,081	274,019,342	109,560,261	820,328,035	China
2	420,258,878	439,312,401	19,053,523	574,511,661	India
3	9,616,919	15,677,224	6,060,305	32,204,986	Saudi Arabia
4	783,660	6,587,084	5,803,424	113,054,932	Indonesia
5	34,839,061	38,584,943	3,745,882	89,811,643	Mexico
6	58,410,683	61,762,731	3,352,048	161,217,993	Brazil
7	23,995,676	26,879,572	2,883,896	53,010,341	Vietnam
8	4,140,135	6,647,417	2,507,282	34,549,112	Colombia
9	872,279	3,359,080	2,486,801	9,004,547	Guatemala

Slika 21: Top 10 ekonomija sa najvećim porastom korisnika (Huston, 2022)

Postoje još dva područja implementacije IPv6 koja treba napomenuti, ali ih je daleko teže izmjeriti.

Prvo područje je sektor poduzeća. Ovaj je sektor bio relativno konzervativan u svom pristupu novim tehnologijama i uvelike se oslanjao na privatne mrežne platforme. To je značilo da je uglavnom izoliran od tereta problema s iscrpljivanjem IPv4 adresa i da je mogao nastaviti s IPv4 programom u posljednjem desetljeću. Ovaj sektor prelazi na usluge u oblaku, ali već dugi niz godina ove poslovne usluge u oblaku mogu raditi na IPv4. Tek u posljednjih nekoliko godina vidjeli smo najave iz Microsoftovog Azurea (2016) ili Amazonovog AWS-a (2021) da njihove platforme uvode podršku za IPv6.

Drugo područje je Internet stvari (IoT). Procjene se razlikuju koliko uređaja postoji u ovoj mreži, vjerojatno zato što je to prostor koji prkosi većini konvencionalnih oblika jednostavnog brojanja, ali procjene su između 20 milijardi i 50 milijardi kada međusobno razgovaramo o broju takvih uređaja . Smatralo se da će IoT ubrzati prihvaćanje IPv6, no čini se da se to još nije dogodilo. Mnogi od ovih uređaja skrivaju se iza isprekidanog povezivanja, a do sada se čini da su IPv4 i NAT-ovi sposobni zadovoljiti zahtjeve (Huston, 2022).

Internet je ključan za kontinuirani razvoj IoT-a i drugih novih tehnologija. Jedna od ključnih grana gdje će IPv6 imati veliku ulogu u budućnosti je autoindustrija gdje će pametni automobili komunicirati s kontrolnim tornjevima, satelitima i drugim vozilima odjednom jako velikim brzinama. Uz autoindustriju IPv6 imat će utjecaja i na povećanje inovacija. S više dostupnih jedinstvenih IP adresa, tvrtke i pojedinci mogu povezati više uređaja s internetom i razviti nove aplikacije i usluge koje nisu bile moguće s IPv4. To može dovesti do povećanja inovacija, novih poslovnih prilika i gospodarskog rasta.

Uz IoT i autoindustriju, IPv6 protokol uvest će značajne promjene i razvoj u Blockchain tehnologiji. Kako navode Davies i Pagani (2022) u svom radu Blockchain tehnologija omogućuje nove mogućnosti za peer-to-peer razmjenu novčane vrijednosti i informacija. IPv6 nudi dodatne funkcionalnosti u odnosu na IPv4 podržavajući različite peer-to-peer mehanizme plaćanja i napredno upravljanje identitetom korištenjem kriptografski generiranih adresa. Ključni izazov pri projektiranju blockchain mreža visokih performansi je osigurati njihovu skalabilnost i kapacitet za podršku mnogim korisnicima i aplikacijama. Blockchain mreže obično se implementiraju na vrhu TCP/IP stoga, nudeći izbor između IPv4 i IPv6 protokola. Iako većina blockchain mreža nije

postigla značajan rast, nedavna poboljšanja u implementacijama blockchaina nude sve veće razine protoka transakcija i informacija. IPv6 protokol prikladniji je za takve mreže u pogledu privatnosti, sigurnosti i skalabilnosti.

8. Zaključak

IPv6 tehnologija predstavlja nadogradnju od IPv4 tehnologije koja je dostigla svoj maksimalni kapacitet. Implementacija IPv6 tehnologije donosi mnoga poboljšanja poput većeg broja adresa, bolje sigurnosti i kvalitetniju podršku za mobilne uređaje. Iako IPv6 predstavlja novi standard koji donosi brojne prednosti u odnosu na IPv4, implementacija ovog protokola još je uvijek ograničena i suočava se s nizom izazova koji koče njeno šire usvajanje. Analizom različitih faktora koji koče implementaciju IPv6 tehnologije jasno je vidljiva kompleksnost i višedimenzionalnost izazova s kojima se suočava proces tranzicije.

Implementacija IPv6 tehnologije u mrežama predstavlja kompleksan proces koji zahtijeva značajne investicije, promjene u procesima rada i konfiguracijama mreže, što može biti teško i vremenski zahtjevno. Trošak implementacije predstavlja značajan izazov kako i za velike organizacije tako i za manje organizacije na tržištu. Osim financijskih investicija, postoji i potreba za obukom mrežnih administratora, nabavkom novih uređaja i softverske podrške, što zahtijeva pažljivo planiranje i resurse. Ovaj financijski izazov može biti posebno ozbiljan za manje organizacije s ograničenim resursima. Trošak implementacije je jedan od ključnih faktora koji se ističe kao prepreka ka globalnom usvajanju. Iako opravdan dugoročnim prednostima koje pruža, predstavlja značajan izazov za organizacije i pružatelje internetskih usluga.

Tehničke prepreke kao što su različiti formati adresa, problemi sa starijim uređajima i potreba za prelaznim rješenjima poput NAT-a ili Dual Stack dodaju razinu složenosti. Dok NAT pruža privremeno olakšanje i određen stupanj fleksibilnosti u raspodjeli ograničenog broja IPv4 adresa, s druge strane usporava napredak prema čistoj IPv6 komunikaciji. Postoje i rizici od pogrešaka prilikom konfiguracije i održavanja IPv6 mreže, što može dovesti do problema s dostupnošću i sigurnošću mreže. Pitanje sigurnosti dodatno kompliciraju prelazak na IPv6. Iako se nova verzija IP protokola temelji na poboljšanom sigurnosnom modelu i sigurnosnim značajkama u odnosu na IPv4, rizici od novih ranjivosti i nedovoljna svijest o svim sigurnosnim aspektima mogu usporiti prihvaćanje. Zbog većeg adresnog prostora koji zahtijeva učinkovitiju zaštitu javlja se potreba za stalnim praćenjem i prilagodbom kako bi se zaštitile mreže i podaci od potencijalnih prijetnji i ranjivosti.

Kompatibilnost između protokola također je jedan od glavnih faktora. Razlike između protokola stvaraju potrebu za tranzicijskim mehanizmima mogu dovesti do usporavanja komunikacije i povećane kompleksnosti mrežnih sustava. Iako su razvijeni mehanizmi koji omogućavaju komunikaciju između dva protokola, i dalje postoji rizik od tehničkih poteškoća i usklađivanja koje mogu usporiti implementaciju.

Problemi vezani uz legacy sustave , odnosno starijim aplikacijama, sustavima i uređajima koji ne podržavaju IPv6, iako je sva manje prisutan faktor još i dalje djelom utječe na usvajanje IPv6 protokola. Mnoge organizacije još uvijek koriste starije uređaje i aplikacije koje nisu kompatibilne s IPv6. Ovaj problem zahtijeva značajno restrukturiranje , ulaganja ili zamjenu tih sustava kako bi se osigurala njihova kompatibilnost i funkcionalnost.

Važno je i napomenuti nedovoljnu podršku od strane ISP-ova (Internet Service Provider-a) koja se nameće među vodećim faktorima koji koče implementaciju. Krajnji korisnici ovise o podršci svojih ISP-ova za prijelaz na novi protokol, a nedostatak tehnološke spremnosti ili volje nekih ISP-ova korisnicima ograničava mogućnosti, što dalje usporava širu implementaciju.

Zbog svega navedenog, potrebno je raditi na smanjenju tehničkih prepreka i troškova, te informirati i educirati korisnike o prednostima IPv6 tehnologije . Sve u svemu, implementacija IPv6 tehnologije koči se zbog kombinacije nedostatka svijesti o njenoj važnosti, tehničkih,političkih i financijskih prepreka. Da bi se ova tehnologija uspješno implementirala, potrebna je snažna podrška i kontinuirano ulaganje od strane poduzeća, organizacija i država. Organizacije koje prepoznaju važnost prilagodbe i usvajanja nove tehnologije bit će bolje pripremljene za budućnost.

Unatoč ovim izazovima, implementacija IPv6 tehnologije je neophodna kako bi se osigurala budućnost interneta. IPv6 je tehnologija koja predstavlja važan korak u razvoju interneta i kako se sve više uređaja povezuje na internet, važno je da se organizacije i korisnici okrenu implementaciji IPv6 kako bi se osigurao nesmetan rad i razvoj u budućnosti. Postupna migracija, podrška ISP-ova, edukacija i prilagodba infrastrukture bit će ključni za prevladavanje prepreka i ostvarivanje potencijala koji IPv6 nudi.

Malo je vjerojatno da će IPv6 u potpunosti zamijeniti IPv4 u bliskoj budućnosti jer mnoge zemlje tek trebaju započeti proces implementacije IPv6, koji je dugotrajan i predstavlja značajne tehničke granice. Uspješna implementacija IPv6 tehnologije zahtijeva suradnju između različitih grana u IT industriji. Uzimajući u obzir sve navedene čimbenike, jasno je da prepreke u implementaciji IPv6 tehnologije nisu nepremostive, ali zahtijevaju koordinirane napore i investicije kako bi se osigurala nesmetana i sigurna tranzicija.

Još nije jasno kako će se IPv6 razvijati. Neki vjeruju da će IPv6 u potpunosti zamijeniti IPv4. Drugi vjeruju da će IPv6 postojati kao paralelni internet i dominirati IoT-om i automobilskom industrijom. Ali sigurno je da se IPv6 neće ugasiti i otići u zaborav.

Popis literature

Introduction to IPv6 (bez dat.). Preuzeto 2.3.2022. s http://etutorials.org/cert/ccnp+bsci/Part+VIII+IPv6/Chapter+20.+Introduction+to+IPv6+and+IPv6+Addressing/Foundation+Topics/

Oscar Gerometta,(2010), *Se está agotando IPv4*. Preuzeto 2.3.2022. s http://librosnetworking.blogspot.com/2010/01/se-esta-agotando-ipv4.html?*sm_au*=iVVJs4M87VFRM5ZHcGKvHK71RQ7W2

Kieren McCarthy (2018), *IPv6 growth is slowing and no one knows why.* Preuzeto 2.3.2022. s https://www.theregister.com/2018/05/21/ipv6_growth_is_slowing_and_no_one_knows_why/

Ezra Bowman (2020),*The IPv6 Apocalypse is Here: 3 Reasons to Upgrade*. Preuzeto 2.2.2022. s https://nodeployfriday.com/posts/ipv6-apocalypse/

Jason Hoffman (bez dat.), *Pros and Cons of IPv6* . Preuzeto 2.3.2022. s https://wisdomplexus.com/blogs/pros-cons-ipv6/

Što je IPv6? (bez dat.). Preuzeto 2.3.2022. s https://hr.education-wiki.com/3868670-what-is-ipv6

Geoff Huston (2022), *Another Year of the Transition to IPv6*. Preuzeto 6.3.2022. s https://circleid.com/posts/20220220-another-year-of-the-transition-to-ipv6

Marco Hogewoning (2021), *The Irrationality of Deploying IPv6*. Preuzeto 20.3.2022. s https://circleid.com/posts/20210803-the-irrationality-of-deploying-ipv6

James Karimi (2019), *If the Implementation of IPv6 Was Mandated for Tomorrow, Who Is Ready?*. Preuzeto 20.3.2022. s https://techmonitor.ai/technology/cloud/implementation-of-ipv6

Afiq Fitri (2022), *Why government action may be needed to push IPv6 adoption.* Preuzeto 20.3.2022. s https://techmonitor.ai/technology/networks/why-government-action-needed-to-push-ipv6-adoption

IPv4 vs IPv6: Budućnost Internet protokola (2019). Preuzeto 21.3.2022. s https://hr.gadget-info.com/54629-ipv4-vs-ipv6-the-future-of-internet-protocols

Dostupnost IPv4 adresa smanjila se na ispod 10% (2010). Preuzeto 23.3.2022. s https://net.hr/danas/dostupnost-ipv4-adresa-smanjila-se-na-ispod-10-99f7ba2a-b1d1-11eb-a028-0242ac15002c

IPv6 Address Types (bez dat.). Preuzeto 25.3.2022. s https://www.networkacademy.io/ccna/ipv6/ipv6-address-types

Kevin Dooley (2015), *What Every Network Admin Should Know About IPv6*. Preuzeto 25.3.2022. s https://www.auvik.com/franklyit/blog/ipv6-network-design

6 Advantages Of IPv6 To IPv4 (bez dat.). Preuzeto 26.3.2022. s https://monsterhost.com/ipv6-to-ipv4/

Marek Majkowski (2015), *Path MTU discovery in practice*. Preuzeto 26.3.2022. s https://blog.cloudflare.com/path-mtu-discovery-in-practice/

5 reasons why the adoption of IPv6 takes so long (2015). Preuzeto 6.4.2022. s https://www.excentis.com/blog/5-reasons-why-the-adoption-of-ipv6-takes-so-long/

Mindaugas Kubilius (2021), *Common Issues Concerning IPv6*. Preuzeto 6.4.2022. s https://www.ipxo.com/blog/common-ipv6-issues/

Use of IPv6 for Croatia (HR). Preuzeto 7.4.2022*. s* https://stats.labs.apnic.net/ipv6/HR

Pete Sclafani (2021), *Top 5 Concerns of Network Admins About Migrating to IPv6 in 2022.* Preuzeto 10.4.2022. s https://www.6connect.com/resources/top-5-concerns-of-network-admins-about-migrating-to-ipv6/

Drew Conry-Murray (2011), *The Reason Enterprises Aren't Deploying IPv6.* Preuzeto 10.4.2022. s https://packetpushers.net/the-reason-enterprises-arent-deploying-ipv6/

David Holder (2018), *Blockers to IPv6 Adoption.* Preuzeto 10.4.2022. s https://labs.ripe.net/author/david_holder/blockers-to-ipv6-adoption/

Silvia Hagen (bez dat.), *IPv6 Essentials, 3rd Edition.* Preuzeto 14.4.2022. s https://www.oreilly.com/library/view/ipv6-essentials-3rd/9781449335229/ch01.html

3 Reasons Why IPv6 Adoption Is Still Light Years Away (2020). Preuzeto 26.4.2022. s https://hospitalitytech.com/3-reasons-why-ipv6-adoption-still-light-years-away

Brenden Kuerbis (2019), *Economic Factors Affecting IPv6 Deployment.* Preuzeto 27.04.2022. s https://www.arin.net/blog/2019/05/02/economic-factors-affecting-ipv6-deployment/

Joseph Mayes (2018), *IPV6 Adoption: Is your ISP ready to support IPv6?*. Preuzeto 4.5.2022. s https://insights.sei.cmu.edu/blog/ipv6-adoption-is-your-isp-ready-to-support-ipv6/

Reasons for IPv6 (bez dat.). Preuzeto 7.5.2022. s http://ipv6now.com.au/primers/IPv6Reasons.php

Doug Dawson (2021), *Still Waiting for IPv6.* Preuzeto 7.5.2022. s https://circleid.com/posts/20210506-still-waiting-for-ipv6

The ugly side of NAT (2017). Preuzeto 13.5.2022. s https://www.excentis.com/blog/the-ugly-side-of-nat/

Kjeld Egevang, Paul Francis (1994), *The IP Network Address Translator (NAT)*. Preuzeto 13.5.2022. s https://datatracker.ietf.org/doc/html/rfc1631

Jordi Palet Martinez (2017), *CE vendors share their thoughts on IPv6 support.* Preuzeto 19.5.2022. s https://blog.apnic.net/2017/11/09/ce-vendors-share-thoughts-ipv6-support/

Google collects statistics about IPv6 adoption (2022). Preuzeto 24.5.2022. s https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

Vincentas Grinius (2021), *Detailed IPv6 Adoption Review.* Preuzeto 24.5.2022. s https://www.ipxo.com/blog/detailed-ipv6-adoption-review/

Josh Fruhlinger (2022), *What is IPv6, and why is adoption taking so long.* Preuzeto 27.5.2022. s https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html

Prijelaz s IPv4 na IPv6 (bez dat.). Preuzeto 4.6.2022. s http://kristinka-blazeka-blog.from.hr/?page_id=936

IPv6 Migration (bez dat.). Preuzeto 4.6.2022. s https://networkdirection.net/articles/network-theory/ipv6migration/

IPv6 Tunnelling (bez dat.). Preuzeto 4.6.2022. s https://www.catchpoint.com/benefits-of-ipv6/ipv6-tunnelling

Types of tunnels (bez dat.). Preuzeto 4.6.2022. s https://tldp.org/HOWTO/Linux+IPv6-HOWTO/ch09s01.html

"Dual-Stack" Will Deliver IPv6 Connectivity (bez dat.). Preuzeto 4.6.2022. s https://whatismyipaddress.com/dual-stack

IPv4/IPv6 Dual Stack (2021). Preuzeto 4.6.2022. s https://support.huawei.com/enterprise/en/doc/EDOC1100137941/e0e5c6c7/ipv4-ipv6-dual-stack

IPv6 over IPv4 tunneling (bez dat.). Preuzeto 7.6.2022. s https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7621r_l3-ip-svcs_cg/content/442284089.html

IPv6 Dual-Stack Lite (2022). Preuzeto 7.6.2022. s https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/security-ipv6-dual-stack-lite.html

Dr. James Hoagland (bez dat.), *The Toredo Protocol: Tunneling Past Network Security and Other Security Implications.* Preuzeto 8.6.2022. s https://www.blackhat.com/presentations/bh-usa-07/Hoagland/Whitepaper/bh-usa-07-hoagland-WP.pdf

Marijana Novaković (bez dat.), *Sretan nam 8. lipnja, Dan IPv6.* Preuzeto 15.6.2022. s https://zastita.info/hr/casopis/clanak/sretan-nam-8-lipnja-dan-ipv6,5668.html

Understanding and Configuring NAT64 (2021). Preuzeto 16.6.2022. s https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/217208-understanding-nat64-and-its-configuratio.html

About DNS64 (bez dat.). Preuzeto 16.6.2022. s https://docs.infoblox.com/space/NAG8/22251555

Ed Horley (2016), *What Tech do I need in a dual-stack adoption strategy? .* Preuzeto 20.6.2022. s https://blogs.infoblox.com/ipv6-coe/what-tech-do-i-need-in-a-dual-stack-adoption-strategy/

A. Conta (1998), *Generic Packet Tunneling in IPv6 Specification.* Preuzeto 18.6.2022. s https://datatracker.ietf.org/doc/html/rfc2473

IPv6 tunnel technologies (2013). Preuzeto 18.6.2022. s https://www.admin-magazine.com/Archive/2013/13/IPv6-tunnel-technologies

A. Durand (2001), *IPv6 Tunnel Broker.* Preuzeto 20.6.2022. s https://datatracker.ietf.org/doc/html/rfc3053

Sean Wilkins (2012), *IPv6 Transition Methods.* Preuzeto 20.6.2022. s https://petri.com/ipv6-transition/

Pedro Filipe Martins de Castro (bez dat.), *Process For IPv6 migration in large organizations*. Preuzeto 20.6.2022. s https://fenix.tecnico.ulisboa.pt

IPv6 Migration Strategy (2012). Preuzeto 20.6.2022. s https://binaryglobal.com/blog/?p=65

D. Farinacci (2013), *The Locator/ID Separation Protocol (LISP).* Preuzeto 20.6.2022. s https://datatracker.ietf.org/doc/html/rfc6830

F. Templin (2008), *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).* Preuzeto 20.6.2022. s https://datatracker.ietf.org/doc/html/rfc5214

W. Townsley (2010), *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd).* Preuzeto 20.6.2022. s https://datatracker.ietf.org/doc/html/rfc5969

Uvodi se novi standard na internetu IPv6 (2012). Preuzeto 22.6.2022. s https://net.hr/danas/danas-se-uvodi-novi-standard-na-internetu-ipv6-0e3f9204-b1d2-11eb-bf0d-0242ac150021

Srini Avirneni (2021), *Why IPv6 should be part of your digital transformation journey.* Preuzeto 22.6.2022. s https://www.thestack.technology/ipv6-digital-transformation-ns1/

Chris Hoffman (2016),*Are You Using IPv6 Yet? Should You Even Care?.* Preuzeto 22.6.2022. s https://www.howtogeek.com/175566/htg-explains-are-you-using-ipv6-yet-should-you-even-care/

Prabhjot Kaur, Charanpreet Kaur (2022), *Migration Techniques And Security Issues Of Ipv6.* International Journal of Creative Research Thoughts (IJCRT). Preuzeto 23.6.2022. s https://www.ijcrt.org/

Gary Audin (2020), *Should Enterprises Avoid or Embrace IPv6?*. Preuzeto 25.6.2022. s https://www.nojitter.com/enterprise-networking/should-enterprises-avoid-or-embrace-ipv6

Cisco (2011), *Solution Overview—Getting Started with IPv6* (2011). 5-6 preuzeto 25.6.2022. s https://www.cisco.com/site/us/en/index.html

Ben Worthen (2006), *IPv6 Is Coming Whether IT Deparments Are Ready or Not.* Preuzeto 29.6.2022. s https://www.cio.com/article/260375/internet-ipv6-is-coming-whether-it-deparments-are-ready-or-not.html

T. Mrugalski M. Siodelski A. Yourtchenko M. Richardson S. Jiang T. Lemon T. Winters (2018) *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) .* Preuzeto 2.7.2022. s https://datatracker.ietf.org/doc/html/rfc8415

S. Thomson C. Huitema V. Ksinant M. Souissi. *DNS Extensions to Support IP Version 6* (2003), Preuzeto 2.7.2022. s https://datatracker.ietf.org/doc/html/rfc3596

Božo Krstajić, Milica Pejanović-Đurišić, Zoran Veljović, Milutin Radonjić, Aleksandra Radulović (2019), *Plan migracije na protokol IPv6 u Crnoj Gori.* INSTITUT ZA RAZVOJ I ISTRAŽIVANJA U OBLASTI ZAŠTITE NA RADU, 96-99

Rene Wilhelm (2022), *IPv6 10 Years Out: An Analysis in Users, Tables, and Traffic.* Preuzeto 5.8.2022. s https://labs.ripe.net/author/wilhelm/ipv6-10-years-out-an-analysis-in-users-tables-and-traffic/

Jack Davies, Alessio Pagani (2022),*IPv4 and IPv6 for Blockchain Networks: a Comparative Analysis.* Preuzeto 20.12.2022. https://ieeexplore.ieee.org/document/10087175/references#references ::: {#refs custom-style="Bibliography"}

Popis slika