VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

PREHOD IZ PROTOKOLA IPv4 NA PROTOKOL IPv6

Kandidat: Boštjan Sternad

Vrsta študija: študent izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Matjaž Žuran, dipl. inž. el. (UN)

Lektorica: dr. Alenka Čuš, univ. dipl. slov.

Maribor, 2023

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Boštjan Sternad sem avtor diplomskega dela z naslovom Prehod iz protokola IPv4 na protokol IPv6a, ki sem ga napisal pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, marec 2023 Podpis študenta:

ZAHVALA

Zahvaljujem se mentorju, mag. Dušanu Brglezu, lektorici Alenki Čuš, Matjažu Žuranu, dipl. inž. el. (UN) ter svojemu prijatelju in odličnemu učitelju, Tomažu Klajdariču, za strokovno pomoč, ves vloženi trud in čas pri izdelavi diplomskega dela ter mentorstvu v šoli.
Zahvaljujem se tudi vodstvu Višje strokovne šole Academia Maribor in vsem predavateljem za posredovana znanja in organizacijo študija.

"Na svetu si, da gledaš sonce.
Na svetu si, da greš za soncem.
Na svetu si, da sam postaneš sonce
in s sveta preženeš sence."
- Tone Pavček

POVZETEK

Internet in informacijska tehnologija sta v vsakodnevnem življenju tako rekoč nenadomestljiva in sta se že skoraj čisto implementirala v naše okolje. Hiter način življenja zahteva tudi uporabo vedno hitrejših in boljših naprav, ki nam niso le v pomoč pri delu, ampak jih vse bolj uporabljamo za različne vrste nadzorovanja in kontroliranja našega bivalnega okolja. Predstavljajmo si, kako bi potekal naš vsakdan brez interneta, elektronske pošte, mobilnih telefonov, prenosnih računalnikov, tablic in podobnih pametnih naprav. Verjetno bi rekli, da je to nemogoče oziroma nepredstavljivo.

Razvoj tehnologije ima vsekakor močan vpliv na naše okolje, tako delovno kot življenjsko in tega ne moremo in tudi nočemo ustaviti. Četudi se umaknemo v manj razvito okolje brez vseh teh naprav in pripomočkov, nas slej kot prej sreča dejstvo, ko vsaj nekaj od tega potrebujemo ali si zaželimo. Ljudje smo družbena bitja in imamo zato v sebi vcepljeno to, da ne zmoremo živeti v osami, odrezani od sveta. Informacijska tehnologija pa nam ravno slednje omogoča, to povezovanje, druženje, komuniciranje.

V diplomskem delu bom prikazal prehod iz protokola IPv4 na protokol IPv6 za OŠ Miklavž na Dravskem polju. Ravno v času pandemije COVID-19, se je v vseh šolah pokazala potreba po čim boljši povezljivosti in komunikaciji preko interneta. Največji ponudniki povezovanja preko interneta že kar nekaj časa podpirajo IPv6 internetni protokol, ki je ravno zaradi svoje varnosti in stabilnosti bolj primeren kot protokol IPv4. Čeprav znotraj samega Eduroam sistema v šoli IPv6 protokol že delno uporabljamo, je v večjem delu vseeno v uporabi protokol IPv4. Največja težava, ki jo IPv4 povzroča je predvsem varnost povezovanja računovodstva preko oddaljenega namizja na strežnik z občutljivimi podatki.

Varnostno pomanjkljivost samega povezovanja zato rešujemo preko zavoda Arnes, ki preko odpiranja in zapiranja posameznih povezovalnih internetnih kanalov (ang. port) omogoča oz. onemogoča neželene vdore v lokalno šolsko omrežje. Prav protokol IPv6 s svojimi vgrajenimi mehanizmi take in podobne internetne napade preprečuje in je zato zelo smotrna izbira primernega internetnega protokola.

Ključne besede: *IP protokol, TCP/IP model, IPv4, IPv6, internetna varnost*

ABSTRACT

IPv4 to IPv6 transition

The Internet and information technology are almost irreplaceable in everyday life and have already been almost fully implemented in our environment. The fast way of life also requires the use of increasingly faster and better devices, which not only help us at work, but we increasingly use them for various types of monitoring and control of our living environment. Let's imagine how our everyday life would go without the Internet, e-mail, mobile phones, laptops, tablets, and similar smart devices. It is impossible or unimaginable.

Technology development definitely has a strong impact on our environment, both working and living, and we cannot and do not want to stop it. Even if we retreat to a less developed environment without all these devices and gadgets, sooner or later we are faced with the fact that we need or want at least some of it. Humans are social creatures; therefore, we cannot live in isolation, cut off from the world. Information technology enables us to do just that, to connect, socialize, and communicate.

In my diploma thesis, I will demonstrate the transition from the IPv4 internet protocol to the IPv6 internet protocol for Miklavž elementary school.
Precisely during the COVID-19 pandemic, the need for the best possible connectivity and communication via the internet became apparent in all schools. The largest internet connection providers have been supporting the IPv6 internet protocol for quite some time, which is more suitable than the IPv4 protocol due to its security and stability. Although the school already partially uses the IPv6 protocol within the Edoroam system itself, the IPv4 protocol is still in use for the most part. The biggest problem that IPv4 causes is above all the security of connecting accounting via a remote desktop to a server with sensitive data.

The security shortcoming of the connection itself is therefore solved through the Arnes institute, which by opening and closing individual connecting internet channels (eng. port) enables or prevents unwanted intrusions into the local school network. It is the IPv6 protocol with its built-in mechanisms that prevents such and similar internet attacks and is therefore a very sensible choice of a suitable internet protocol.

Key words: *IP protocol, TCP/IP model, IPv4, IPv6, internet security*

Vsebina

Kazalo slik

Kazalo tabel

Pojmi, kratice

ALG	Application Layer Gateway	Prehod v aplikacijskem sloju
DAD	Duplicate Address Detection	Odkrivanje podvojenih naslovov
DHCP	Dynamic Host Configuration Protocol	Protokol za dinamično konfiguriranje gostiteljskih računalnikov
DHCP-PD	DHCP-Prefix Delegation	DHCP dodeljevanje predpone
DNS	Domain Name System	Sistem domenskih imen
DNSSEC	DNS Security Extension	Varnostna razširitev za DNS
DSL	Digital Subscriber Line	Digitalni naročniški vod
EAP	Extensible Authentication Protocol	Razširljivi avtentikacijski protokol
GRE	Generic Routing Encapsulation	Generično ovijanje pri usmerjanju
HTTP	Hypertext Transfer Protocol	Protokol za prenos obogatenega besedila
IANA	Internet Assigned Numbers Authority	Uprava za dodeljevanje številk v internetu
ICMP	Internet Control Message	Protokol internetnega kontrolnega sporočila
IPv6	Internet Protocol version 6	Internetni protokol verzije 6
IPCP	IP Control Protocol	IP nadzorni protokol
IPv4	Internet Protocol version 4	Internetni protokol verzije 4
IPv6CP	IPV6 Control Protocol	IPv6 nadzorni protokol
ISTAP	Intra-Site Automatic Tunnel Addressing Protocol	Protokol za avtomatično naslavljanje tunela znotraj lokacije
IX	Internet Exchange	Internetna izmenjevalna točka
LER	Label Edge Router	Robni usmerjevalnik pri komutaciji na osnovi label
LFIB	Label Forwarding information base	Informacijska baza za posredovanje label
LIX	Ljubljana Internet Exchange	Ljubljanska točka za izmenjavo internetnega prometa

MAC	Media Access Control	Krmiljenje dostopa do medija
mDNS	Multicast DNS	Strežnik domenskih imen za oddajanje več prejemnikom hkrati
NCP	Network Control Protocol	Protokol za nadzor omrežja
NAT	Network Address Translation	Prevajanje omrežnih naslovov
RR	Resource Record	Zapis vira
SIX	Slovenian Internet Exchange	Slovenska točka za izmenjavo internetnega prometa
SLAAC	Stateless Address Autoconfiguration	Samostojna samodejna konfiguracija naslovov
SMTP	Simple Mail Transfer Protocol	Preprosti protokol posredovanja sporočil
TCP	Transmission Control Protocol	Protokol za nadzor prenosa
TCP/IP	Transmission Control Protocol/Internet Protocol	Protokol za nadzor prenosa/Internetni protokol
VLAN	Virtual LAN	Navidezno omrežje
VLSM	Variable-Length Subnet Masking	Maskiranje s spremenljivo dolžino podomrežja
RIP	Routing Information Protocol	Protokol optimalne poti med izvorom in ciljem
BGP	Border Gataway Protocol	standardizirani zunanji prehodni protokol, zasnovan za izmenjavo informacij o usmerjanju in dosegljivosti med avtonomnimi sistemi
PPPoE	Point-to-Point Protocol over Ethernet	omrežni protokol, ki olajša komunikacijo med končnimi točkami omrežja
OSPF	Open Shortest Path First	Omrežni protokol, ki poišče najkrajšo možno pot med izvorom in ciljem

BGP	Border Gateway Protocol	mejni protokol za prehode
ISP	Internet Stream Protocol	Eksperimentalni internetni protokol toka podatkov
SEND	Neighbor Discovery Protocol	Protokol odkrivanja soseda

1. Uvod

1.1 Opis področja in opredelitev problema

Internet in internetne tehnologije so v zadnjem času zelo razširjene, skoraj že infiltrirane v družbo in si zato življenja brez interneta ne moremo več predstavljati. Skorajda ni več mobilne naprave, ki ni povezana v internet. Hkrati se tudi vedno več nemobilnih in hišnih naprav povezuje v internet in nam slednji omogoča komuniciranje s takimi napravami. Vedno večji razmah interneta zato zahteva vedno boljšo povezljivost, hkrati pa boljšo in bolj natančno prepoznavnost povezanih naprav.

Prav tukaj nastopi sodobnejši protokol IPv6, ker je še vedno aktualni protokol IPv4 zmeraj bolj izčrpan. Kljub izčrpanju, se protokol IP v svoji verziji 4 ne bo takoj umaknil iz omrežja, temveč bo sobival na isti infrastrukturi z IPv6. Vsaka sodobna naprava, ali je to računalnik, mobilni telefon, tiskalnik idr. lahko komunicira preko obeh protokolov IPv4 in IPv6, odvisno od omrežja in ponudnika. Vedno več ponudnikov mobilnih storitev že omogoča povezljivost preko IPv6, česar pa uporabniki sami ne opazimo.
IPv6 in IPv4 sobivata na isti infrastrukturi, hkrati pa ni nujno, da sta povezana. Ker IPv6 omogoča daljši zapis oz. daljše naslavljanje, je prihodnost interneta vsekakor v protokolu IPv6.

1.2 Namen, cilji in osnovne trditve

Zanima nas, ali menjava iz internetnega protokola IPv4 na protokol IPv6 dejansko vpliva na okolje v katerem živimo. Če pogledamo z vidika tehnološkega napredka, potem prav gotovo ima zelo velik vpliv. Vse več naprav se povezuje v internet in vse več je tudi takih naprav, ki brez interneta praktično ne delujejo oz. niso funkcionalne. Ker novejše naprave nadomeščajo starejše, je sama poraba električne energije manjša, kar vpliva na manjši ogljični odtis za naravno okolje.

Namen diplomskega dela je prikazati, kako in zakaj se kot sistemski inženir zaposlen v nekem podjetju, instituciji, javnem zavodu sploh lotiti prehoda iz IPv4 na novejši protokol IPv6. Dejstvo je, da bo z razmahom interneta in informacijske tehnologije to nujno potrebno slej ali prej opraviti povsod, kjer bomo še hoteli uporabljati računalnike, telefone in podobne naprave povezane v internet.

Cilj diplomskega dela je ovreči ali potrditi naslednje hipoteze:

H1: Menjava iz protokola IPv4 na protokol IPv6 je neizogibna.

H2: Protokol IPv6 je hitrejši od protokola IPv4.

H3: Protokol IPv6 je varnejši od protokola IPv4.

H4: Protokol IPv6 ima več prednosti napram protokolu IPv4.

H5: Protokol IPv6 omogoča povezovanje več naprav v internetu.

H6: Omrežja IPv6 so preglednejša in hitrejša.

1.3 Predpostavke in omejitve

Omejitev, ki jo vidim pri diplomskem delu je, da na omrežju mojega delodajalca ne bo možno testiranje vseh zastavljenih nalog delovanja omrežnih naprav predvsem zaradi varnostne politike v organizaciji. Za praktični del diplomskega dela sem zato uporabil programsko orodje Cisco Packed Tracer verzije 8.0.0., ki nima omejitev glede konfiguriranja omrežij s protokolom IPv6 oz. s simulacijo prehoda iz IPv4 na IPv6.

1.4 Uporabljene raziskovalne metode

Raziskovalna metoda je kvantitativna, saj je v uvodu napovedano, kakšni so cilji raziskovanja.

Hkrati sem uporabila metodo deskripcije in komparacije. V uvodu je napovedano, kakšni so cilji raziskovanja in njihov opis. Na koncu so s testiranjem hipoteze potrjene ali ovržene.

Pri pisanju in raziskovanju sem uporabil domačo in tujo tehnično in strokovno literaturo. Literatura je primarnega in sekundarnega izvora, kot so strokovne knjige, internetni članki in osebni zapiski.

2. TCP/IP PROTOKOL

Protokol za nadzor prenosa/internetni protokol (TCP/IP) je jezik, ki ga računalnik uporablja za dostop do interneta. Sestavljen je iz nabora protokolov, zasnovanih za vzpostavitev omrežja omrežij, ki gostitelju zagotavljajo dostop do interneta. Skozi zgodovino in vedno večjo uporabo interneta, se je TCP/IP protokol nenehno spreminjal in nadgrajeval.

1.4.1 TCP

Protokol za nadzor prenosa (TCP) je omrežni komunikacijski protokol, zasnovan za pošiljanje podatkovnih paketov po internetu.

TCP je protokol transportnega sloja v sloju OSI in se uporablja za ustvarjanje povezave med oddaljenimi računalniki s prenašanjem in zagotavljanjem dostave sporočil prek podpornih omrežij in interneta.

Protokol za nadzor prenosa je eden najpogosteje uporabljenih protokolov v digitalnih omrežnih komunikacijah in je del zbirke internetnih protokolov, splošno znane kot zbirka TCP/IP. TCP predvsem zagotavlja dostavo podatkov od konca do konca med različnimi vozlišči. TCP deluje v sodelovanju z internetnim protokolom, ki določa logično lokacijo oddaljenega vozlišča, medtem ko TCP prenaša in zagotavlja, da so podatki dostavljeni na pravi cilj.

Pred prenosom podatkov TCP ustvari povezavo med izvornim in ciljnim vozliščem in jo vzdržuje, dokler komunikacija ni aktivna. TCP velike podatke razdeli na manjše pakete in tudi zagotovi, da je celovitost podatkov nedotaknjena, ko so ponovno sestavljeni v ciljnem vozlišču.

1.4.2 IP protokol

Internetni protokol je odgovoren za naslavljanje gostiteljskih vmesnikov, enkapsulacijo podatkov v podatkovne pakete (vključno z razdrobljenostjo in ponovnim sestavljanjem) ter usmerjanje podatkovnih paketov od izvornega gostiteljskega vmesnika do ciljnega gostiteljskega vmesnika prek enega ali več omrežij IP. Za te namene internetni protokol definira format paketov in zagotavlja sistem naslavljanja.

Vsak podatkovni paket ima dve komponenti: glavo in koristni tovor. Glava IP vključuje izvorni naslov IP, ciljni naslov IP in druge metapodatke, potrebne za usmerjanje in dostavo

podatkovnega paketa. Tovor so podatki, ki se prenašajo. Ta način ugnezdenja podatkovnega tovora v paketu z glavo se imenuje enkapsulacija.

Naslavljanje IP vključuje dodelitev naslovov IP in povezanih parametrov gostiteljskim vmesnikom. Naslovni prostor je razdeljen na podomrežja, ki vključujejo označevanje omrežnih predpon. Usmerjanje IP izvajajo vsi gostitelji, pa tudi usmerjevalniki, katerih glavna funkcija je prenos paketov čez meje omrežja. Usmerjevalniki med seboj komunicirajo prek posebej zasnovanih usmerjevalnih protokolov, bodisi notranjih protokolov prehodov ali zunanjih protokolov prehodov, kot je potrebno za topologijo omrežja.

1.4.3 TCP/IP

TCP/IP, Transmission Control Protocol/Internet Protocol, so torej standardni internetni komunikacijski protokoli, ki digitalnim računalnikom omogočajo komunikacijo na velike razdalje. Internet je paketno komutirano omrežje, v katerem so informacije razdeljene na majhne pakete, poslane posamično po več različnih poteh hkrati in nato ponovno sestavljene na prejemnem koncu. TCP je komponenta, ki zbira in ponovno sestavlja pakete podatkov, medtem ko je IP odgovoren za zagotavljanje, da so paketi poslani na pravi cilj. TCP/IP je bil razvit v sedemdesetih letih in leta 1983 sprejet kot standard protokola za ARPANET (predhodnik interneta).

Paket internetnih protokolov je rezultat raziskav in razvoja, ki jih je izvajala Agencija za napredne obrambne raziskovalne projekte (DARPA) v poznih šestdesetih letih prejšnjega stoletja. Po uvedbi pionirskega ARPANET-a leta 1969 je DARPA začela delati na številnih drugih tehnologijah za prenos podatkov. Leta 1972 se je Robert E. Kahn pridružil uradu za tehnologijo informacijske obdelave DARPA, kjer je delal tako na satelitskih paketnih omrežjih kot na zemeljskih radijskih paketnih omrežjih in spoznal vrednost komunikacije prek obeh. Spomladi 1973 se je Vinton Cerf, ki je pomagal pri razvoju obstoječega protokola ARPANET NCP (ang. Network Control Protocol) pridružil Kahnu pri delu na modelih medsebojnega povezovanja z odprto arhitekturo s ciljem oblikovanja naslednje generacije protokola za ARPANET. Črpali so se iz izkušenj raziskovalne skupnosti ARPANET in mednarodne delovne skupine za mreženje, ki ji je predsedoval Cerf.

Do poletja 1973 sta Kahn in Cerf izdelala temeljno preoblikovanje, v katerem so bile razlike med protokoli lokalnih omrežij skrite z uporabo skupnega medomrežnega protokola in namesto

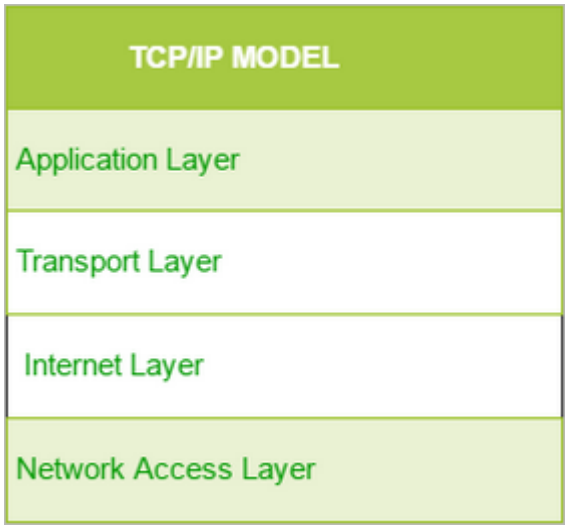
da bi bilo omrežje odgovorno za zanesljivost, kot v obstoječih protokolih ARPANET, je bila ta funkcija prenesena na gostitelje. Cerf pripisuje Hubertu Zimmermannu in Louisu Pouzinu, oblikovalcu mreže CYCLADES, pomemben vpliv na to zasnovo. Novi protokol je bil leta 1974 implementiran kot program za nadzor prenosa.

1.5 TCP/IP model

TCP/IP nam pomaga določiti, kako naj bo določen računalnik povezan z internetom in kako naj se prenašajo podatki med njima. Pomaga nam ustvariti navidezno omrežje, ko je več računalniških omrežij povezanih skupaj. Namen modela TCP/IP je omogočiti komunikacijo na velikih razdaljah.

TCP/IP je kratica za Transmission Control Protocol/Internet Protocol. Sklad TCP/IP je posebej zasnovan kot model za zagotavljanje zelo zanesljivega toka bajtov end-to-end preko nezanesljivega medmrežja oz. interneta.

TCP/IP model je sestavljen iz štirih slojev, in sicer iz aplikacijskega, transportnega, internetnega in omrežnega vmesnika. (GeeksForGeeks, 2020)



Slika 1: Plasti TCP/IP modela

Vir: (GeeksForGeeks)

1.5.1 Plast omrežnega dostopa

Ta plast ustreza kombinaciji plasti podatkovne povezave in fizične plasti modela OSI. Skrbi za naslavljanje strojne opreme in protokoli, ki so prisotni v tej plasti, omogočajo fizični prenos podatkov.

Pravkar smo obravnavali, da je ARP protokol internetnega sloja, vendar obstaja spor glede njegove deklaracije kot protokola internetnega sloja ali sloja omrežnega dostopa. Opisano je, da prebiva v plasti 3 in je enkapsuliran s protokoli plasti 2.

1.5.2 Internetna plast

Ta plast je vzporedna s funkcijami omrežne plasti OSI. Določa protokole, ki so odgovorni za logični prenos podatkov po celotnem omrežju. Glavni protokoli, ki se nahajajo na tej ravni so naslednji:

IP – pomeni internetni protokol in je odgovoren za dostavo paketov od izvornega gostitelja do ciljnega gostitelja z ogledom naslovov IP v glavah paketov. IP ima trenutno še dve različici: **IPv4** in **IPv6**. IPv4 je tisti, ki ga trenutno uporablja večina spletnih mest. Toda IPv6 raste, saj je število naslovov IPv4 v primerjavi s številom uporabnikov omejeno.

ICMP – pomeni Internet Control Message Protocol. Enkapsuliran je v podatkovne pakete IP in je odgovoren za zagotavljanje informacij gostiteljem o težavah z omrežjem.

ARP – pomeni protokol za razrešitev naslovov. Njegova naloga je najti naslov strojne opreme gostitelja iz znanega naslova IP. ARP ima več vrst: Reverse ARP, Proxy ARP, Gratuitous ARP in Inverse ARP.

1.5.3 Transportna plast

Plast je analogna transportni plasti modela OSI. Ta je odgovoren za komunikacijo end-to-end in dostavo podatkov brez napak. Aplikacije višjega sloja ščiti pred kompleksnostjo podatkov. V tej plasti sta prisotna dva glavna protokola:

Protokol za nadzor prenosa (**TCP**) – znano je, da zagotavlja zanesljivo komunikacijo brez napak med končnimi sistemi. Izvaja zaporedje in segmentacijo podatkov. Ima tudi funkcijo potrditve in nadzoruje pretok podatkov prek mehanizma za nadzor pretoka. Je zelo učinkovit

protokol, vendar ima zaradi takšnih funkcij veliko stroškov. Povečani režijski stroški vodijo do višjih stroškov.

Protokol uporabniškega podatkovnega paketa (**UDP**) – po drugi strani pa ne ponuja nobenih takih funkcij. Če naša aplikacija ne potrebuje zanesljivega transporta, je to protokol, ki je najbolj primeren, saj je zelo stroškovno učinkovit. Za razliko od TCP, ki je povezovalno usmerjen protokol, je UDP brez povezave.

1.5.4 Aplikacijska plast

Ta plast opravlja funkcije zgornjih treh plasti modela OSI: aplikacijske, predstavitvene in sejne plasti. Odgovorna je za komunikacijo med vozlišči in nadzoruje specifikacije uporabniškega vmesnika. Nekateri protokoli, ki so prisotni v tej plasti, so: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

V tej plasti so opredeljeni postopki pri komunikaciji med posameznimi uporabniškimi programi, npr. elektronska pošta, prenašanje datotek, prijava na oddaljeni računalnik, sinhronizacija komunikacije itd.

Skladno z razvojem modela OSI so se razvijale tudi aplikacije OSI, ki pa se niso širše uveljavile. Primeri so File Transfer, Access and Management (FTAM), Virtual Terminal Protocol (VTP) in SMTP (simple mail transfer protocol), ki ga uporablja večina e-poštnih programov za usmerjanje podatkov v omrežja. (Brglez, 2018)

Oglejmo si nekaj teh protokolov podrobneje:

HTTP in HTTPS – HTTP je kratica za protokol v smislu prenosa hiperteksta. Svetovni splet ga uporablja za upravljanje komunikacij med spletnimi brskalniki in strežniki. HTTPS pomeni HTTP-Secure. Je kombinacija HTTP s SSL (ang. Secure Socket Layer). Učinkovit je v primerih, ko mora brskalnik izpolniti obrazce, se prijaviti, overiti in izvesti bančne transakcije.

SSH – SSH pomeni Secure Shell. Je programska oprema za emulacijo terminalov, podobna Telnetu. Razlog, da je SSH bolj zaželen, je njegova sposobnost vzdrževanja šifrirane povezave. Vzpostavi varno sejo prek povezave TCP/IP.

NTP – NTP je kratica za Network Time Protocol. Uporablja se za sinhronizacijo ur na našem računalniku z enim standardnim časovnim virom. Zelo uporaben je v situacijah, kot so bančne transakcije. Predpostavimo naslednjo situacijo brez prisotnosti NTP. Recimo, da izvedemo transakcijo, kjer vaš računalnik odčita čas ob 14.30, medtem ko ga strežnik zabeleži ob 14.28. Strežnik se lahko celo zruši, če ni sinhroniziran.

1.6 IPv4 protokol

Internetni protokol različice 4 (IPv4) je četrta različica internetnega protokola (IP). Je eden od temeljnih protokolov medmrežnega povezovanja, ki temelji na standardih medmrežja.
Trenutno najbolj razširjena izvedba IP je IPv4, ki uporablja 32-bitni naslov. Matematično lahko 32-bitni naslov zagotovi približno štiri milijarde edinstvenih naslovov IP (232 = 4.294.967.296). Praktično število uporabnih naslovov IPv4 je mnogo nižje, saj je veliko naslovov rezerviranih za diagnostične, eksperimentalne ali multicast namene. Eksplozivna rast interneta in omrežij podjetij je hitro privedla do pomanjkanja naslova IPv4. Za ublažitev tega pojava so bile razvite različne rešitve, vključno s CIDR, NAT in zasebnim naslavljanjem. Vendar te rešitve lahko služijo le kot začasni popravki. (Balchunas, 2006)

1.6.1 Kaj je protokol IPv4

IPv4 je vrsta protokola, ki je bila predstavljena leta 1983 v ARPANET-u in je še vedno najbolj znana in uporabljena različica za prepoznavanje naprav v internetu.
Naslov IPv4 uporablja 32-bitni naslov, ki je najbolj znan tip, ki ga vidimo, ko iščemo IP. 32-bitni naslovni prostor zagotavlja skoraj 4,3 milijarde edinstvenih naslovov oz. natanko 4.294.967.296. Če bi bili vsi IPv4 naslovi statični, potem bi teoretično lahko opremili vsaj polovico svetovnega prebivalstva z IP naslovi. Vendar pa so nekateri od njih rezervirani za zasebno uporabo. Primer naslova IPv4 je 192.168.0.1.

1.6.2 Kako deluje IPv4

IPv4 je protokol omrežnega sloja (OSI-ISO sloj 3) v zbirki internetnih protokolov (znan tudi kot TCP/IP), ki se uporablja za posredovanje tokov paketov in podatkovnih paketov po omrežjih. Če poenostavimo: vsem omogoča enoten način naslavljanja (z dodeljevanjem naslovov IP napravam), kar uporabnikom v različnih omrežjih omogoča komunikacijo. In komunikacija med različnimi omrežji je navsezadnje tudi temeljno načelo interneta.
V modelu TCP/IP obstajajo štiri plasti, ki tako ali drugače ustrezajo plastem modela OSI. To so povezovalni, internetni, transportni in aplikacijski sloj (od 1 do 4). Ko so podatki poslani iz ene naprave v drugo, so enkapsulirani v različne protokole od zgoraj navzdol, tj. v aplikacijski

plasti (ki približno ustreza OSI-ISO plasti 7, 6 in 5) in jih je mogoče zaviti v protokol HTTP, nato v transport (OSI-ISO sloj 4) – v TCP, v internetnem sloju (OSI-ISO sloj 3) – v IP in nato preneseno preko Etherneta v povezovalnem sloju (ki ustreza OSI-ISO sloju 1 in 2). Ko so podatki sprejeti, se postopek obrne in sporočilo se razkrije.
Predvsem nas zanima internetna plast, kjer podatkovni paket prejme glavo IP, ki vsebuje naslov IP. Slednje omogoča, da se paket usmeri izven omrežja in prispe na cilj skozi vrsto skokov med različnimi usmerjevalniki.

Usmerjanje – routing

Unikatna značilnost katere koli naprave je njen naslov MAC, vendar naprave ne komunicirajo med omrežji tako. Zato jim je dodeljen naslov IP, ki usmerjevalniku pove, kam naj se pošlje podatkovni paket. Slednje si lahko predstavljamo kot poštno storitev: naše pismo ne gre naravnost do naslovnika; najprej se pošlje iz enega poštnega vozlišča v drugega, da se optimizira postopek dostave. Podobno se podatkovni paketi posredujejo od enega usmerjevalnika do drugega, dokler ne dosežejo pravega naslova IP.

Kako izgleda naslov IPv4

Internetni protokol, zlasti internetni protokol različice 4, določa, kako deluje naslavljanje in kako je mogoče identificirati in najti omrežne gostitelje v omrežju. Naslovi IPv4 so predstavljeni z 32-bitnimi vrednostmi, organiziranimi v štiri oktete (4 x 8), ki so običajno izraženi z decimalnimi števili s pikami, ki izgledajo takole: 172.140.150.12.

Razmeroma enostavno je prevesti decimalni naslov IPv4 v binarno obliko in obratno. Vsak oktet je sestavljen iz osmih bitov, ki jim je od leve proti desni dodeljeno določeno število: 128, 64, 32, 16, 8, 4, 2, 1. Trik je v tem, da ta števila seštejemo – začenši z najvišjimi možnimi – da pridemo do decimalne vrednosti. Ena pomeni, da številka obstaja, nič pa, da je ni. Torej za "172" bi pomenilo 128 + 32 + 8 + 4 = 172, kar v dvojiški obliki pomeni "10101100." Ker lahko štejemo hitro, je možen razpon za decimalne vrednosti od 0 do 255. (CiscoPress, Internet Routing Architectures, second edition, str. 57, 2000)

Anatomija naslova IPv4

Naslov IPv4 je pravzaprav sestavljen iz dveh delov: enega, ki identificira naše omrežje, in drugega, ki identificira gostitelja (tj. napravo) v omrežju. Ti deli niso enaki ali fiksni, zato ima naslov za določitev dolžine dela omrežja tudi »omrežno masko«. V zapisu CIDR je to številka za poševnico, ki določa, koliko bitov naslova sestavlja omrežno predpono. Na primer, 192.168.0.1/24 označuje, da ima naslov IPv4 192.168.0.1 24-bitno dolgo predpono in da omrežje, ki mu pripada, vsebuje naslove v razponu od 192.168.0.0 do 192.168.0.255 (tj. vsi imajo skupno vrednost prvih 24 bitov). Zahvaljujoč usmerjevalnim protokolom, kot so RIP, OSPF in BGP, se lahko usmerjevalniki med seboj obveščajo o omrežnih naslovih, ki so jim dodeljeni ali za katere »vedo« od drugih usmerjevalnikov, tako da se lahko podatkovni paketi posredujejo v pravo omrežje, in s tem tudi v pravo napravo.

Dinamični naslovi IP

Pri preverjanju naslova IPv4 lastne naprave bomo morda ugotovili, da ta ni vedno enak. To je zato, ker bo strežnik DHCP naši napravi dinamično dodelil naslov IP, torej ga zakupil za določen čas. Če naša naprava pravočasno ne zahteva podaljšanja zakupa DHCP, bo naslov IPv4 sproščen in dodeljen drugi napravi. Ta mehanizem je bil implementiran za ohranitev zelo omejene skupine naslovov IPv4, ki so na voljo.
Zaradi svoje arhitekture je internetni protokol različice 4 sposoben zagotoviti 2^{32} ali več kot štiri milijarde naslovov IP (4.294.967.296, če smo natančni). Če bi bili vsi statični, bi lahko samo približno polovici našega prebivalstva zagotovili napravo, opremljeno z IP. Zahvaljujoč dinamičnemu dodeljevanju smo do zadnjega desetletja lahko upravljali samo z IPv4 in ga aktivno uporabljamo skupaj z IPv6, odkar je bil prvič predstavljen. Vendar nas vseeno čaka neizogibno sprejetje IPv6 in z leti bo tega protokola vedno več.

Ali še vedno potrebujemo IPv4?

Da, zagotovo. O težavah pri uvajanju IPv6 bomo ugotavljali bolj podrobno v naslednjih poglavjih protokola, vendar je za zdaj dovolj, da smo daleč od tega, da bi v celoti prešli z internetnega protokola različice 4 na različico 6, saj gre za dolgotrajen in intenziven proces. V prihodnjih letih se bodo upravljavci omrežij morali ukvarjati z obema protokoloma, zato še ne pozabimo na IPv4.

1.6.3 Prednosti IPv4

Obstoječa infrastruktura – večina spletnih mest uporablja IPv4, tudi tista, ki podpirajo IPv6.
Enostavnost – 32-bitna decimalna številka IPv4 s pikami je veliko manjša in enostavnejša od šestnajstiških števil IPv6.
Podpora – ker večina prometa še vedno uporablja IPv4, se omrežnim operaterjem zdi IPv4 poznan. (Avsystems, 2021)

1.7 IPv6 protokol

Internetni protokol različice 6 (IPv6) je najnovejša različica internetnega protokola (IP), komunikacijskega protokola, ki zagotavlja identifikacijski in lokacijski sistem za računalnike v omrežjih in usmerja promet po internetu. IPv6 je razvila Internet Engineering Task Force (IETF) za reševanje dolgo pričakovane težave z izčrpanostjo naslovov IPv4 in naj bi IPv4 nadomestil. Decembra 1998 je IPv6 postal osnutek standarda za IETF, ki ga je nato 14. julija 2017 ta ratificiral kot internetni standard.

1.7.1 Kaj je IPv6

Naslov IPv6 uporablja 128-bitni format naslova in vključuje tako številke kot črke.
Primer naslova IPv6 je 2001:1470:F11D:0000:0000:0000:0000:8888.

1.7.2 Kako delujeIPv6

Internetni protokol različice 6 (IPv6) je najnovejša generacija internetnega protokola, ki je bil razvit za reševanje naraščajočega problema praznjenja skupine naslovov IP. Zahvaljujoč svoji strukturi lahko IPv6 sprejme 2.128 naslovov (v primerjavi z 232 ali več kot štirimi milijardami, ki so na voljo v dandanes najpogosteje uporabljeni različici IPv4). Glede na to, da nimamo niti imena za to številko, lahko domnevamo, da bi morala zagotoviti globalno potrebo po naslovih IP v bližnji prihodnosti.

1.7.3 Kako izgleda naslov IPv6

Naslovi IPv6 so sestavljeni iz 128 bitov. Zaradi doslednega in nedvoumnega zapisa so ti organizirani v osem hekstetov šestnajstiških števk, ločenih z dvopičji. Izgledajo nekako takole: fd1a:c625:de37:5b3d:0000:0000:0000:0000.

Hekstet je 16-bitni (ali štiri-grizni) blok, zapisan v šestnajstiški obliki. Šestnajstiško (ali na kratko šestnajstiško) se uporablja za zapisovanje binarnih zaporedij v bolj berljivi obliki. Eni od 16 števk od nič do devet ali od A do F dodeli vrednost štirih bitov. Male in velike črke se lahko izmenjujejo in veljajo za enakovredne.

Tabela 1: Primerjava heksadecimalne in binarne oblike zapisa

Heksadecimalni zapis	Binarni zapis
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Vir: (Lastni vir)

Hekstet "fd1a" je v dvojiški obliki predstavljen kot 1111 1101 0001 1010.

Zaradi jedrnatosti, se lahko začetne ničle v katerem koli hekstetu odstranijo; zaporedni heksteti, ki vsebujejo samo ničle, pa se izrazijo z dvojnim dvopičjem (::). Zato bo izvirni naslov videti takole: fd1a:c625:de37:5b3d:0000:0000:0000:0000.

Brez začetnih ničel bo videti takole: fd1a:c625:de37:5b3d:0:0:0:0.

In po zamenjavi zaporednih skupin ničel, kot je ta: fd1a:c625:de37:5b3d::. (Avsystem, 2021)

1.7.4 Vrste naslovov IPv6

Obstajajo tri vrste naslovov IPv6, ki se uporabljajo za različne namene:

- **unicast**, ki ustreza javnemu naslovu IPv4 in je javno usmerljiv;
- **multicast** se uporablja za komunikacijo z določenimi napravami v danem omrežju, ki »poslušajo« ta naslov;
- **anycast** je naslov, ki si ga delijo različne naprave na različnih lokacijah, od katerih bo samo najbližja prejela paket, ko bo ta poslan.

1.7.5 Zakaj moramo preklopiti na IPv6?

Čeprav je bil IPv4 prvič sprejet v osemdesetih letih prejšnjega stoletja, je bilo že v devetdesetih povsem jasno, da število razpoložljivih naslovov IP ne bo zadostovalo za rastoče potrebe interneta. Z vedno večjim sprejemanjem interneta, naraščajočim številom računalnikov, tablic, pametnih telefonov in naprav IoT (ang. Internet of Things), ki vse potrebujejo naslov IP, da so v omrežju, štiri milijarde razpoložljivih naslovov niso niti blizu tistemu, kar potrebujemo. Poleg tega je del bazena IPv4 rezerviran za zasebna omrežja, in ker je dodeljevanje naslovov IP slabo upravljano tako na globalni kot regionalni ravni, obstaja neenakomerna porazdelitev tega zelo omejenega vira po vsem svetu. IPv6 naj bi rešil težavo – vendar bo trajalo nekaj časa.

Čeprav IPv6 ponuja veliko prednosti napram IPv4, ni združljiv s prejšnjimi različicami in zato zahteva nekaj tehnoloških prilagoditev, kar pomembno vpliva na njegovo sprejetje. Lastniki omrežij – zlasti operaterji, ponudniki storitev in podjetja – morajo posodobiti svoja omrežja tako z vidika strojne kot programske opreme, da se prilagodijo naslavljanju IPv6, in ponovno usposobiti svoje osebje za upravljanje omrežja za uspešno uvedbo. Medtem ko sprejemanje raste in zdaj velja za neizogibno, še vedno ostaja veliko naprav, ki IPv6 ne podpirajo. To zahteva, da lastniki omrežja vzdržujejo programsko in strojno opremo (kot so strežniki DNS in DHCP, IPAM, prehodi in druga programska oprema za upravljanje omrežja), ki lahko hkrati podpira IPv6 in IPv4. Vložiti morajo dodatna sredstva, da ustvarijo gostitelje, ki podpirajo IPv6 in IPv4 znotraj ali zunaj svojega omrežja, da zagotovijo interoperabilnost. Slednje znatno prispeva k splošni kompleksnosti omrežnih operacij.

Po podatkih Googla, le nekaj več kot 35 % njegovih uporabnikov dostopa do njega prek naslova IPv6 – to je številka, ki je kljub temu narasla za 25 odstotnih točk od konca leta 2015. Googlovi podatki prav tako kažejo znatno nesorazmerje pri sprejemanju protokolov po vsem svetu, pri čemer veliki deleži pripadajo Ameriki, Zahodni Evropi in Južni Aziji, ki vodijo. Pričakovati gre širšo uporabo v razvitih državah v primerjavi s preostalim svetom, saj nadgradnja na splošno zahteva znatne tehnološke in finančne investicije. Hkrati pa bodo rastoče cene naslovnih blokov IPv4 in splošno pomanjkanje tega vira na trgu prisilile vse deležnike k prehodu prej ali slej.

1.7.6 Prednosti IPv6 napram IPv4

Eksponentna rast povpraševanja po internetu je povzročila pomanjkanje naslovov IPv4. Sistem naslovov IPv6 ponuja prostor za skoraj neskončno število naslovov IP. Med IPv4 in IPv6 obstaja nekaj tehničnih razlik – a povprečnemu uporabniku jih ni potrebno poznati.

IPv6 ponuja nekaj izboljšav v primerjavi z IPv4, in te so naslednje:

- Vgrajena in resnična kakovost storitve (QoS), imenovana tudi "označevanje toka".
- Vgrajena omrežna varnostna plast (IPsec).
- Nič več prevajanja omrežnih naslovov (NAT). IPv6 omogoča povezljivost od konca do konca na ravni IP.
- Boljše množično usmerjanje sporočil in je del osnovnih specifikacij v IPv6, medtem ko je to v IPv4 izbirno.
- Poenostavljene in večje glave paketov (približno dvakrat večje od IPv4).
- Poenostavljeno in učinkovitejše usmerjanje.
- Ni več prevajanja omrežnih naslovov oz. NAT (ang. Network Address Translation).
- Samodejna konfiguracija.
- Nič več navzkrižij zasebnih naslovov.
- Boljše usmerjanje omrežnih sporočil.
- Preprostejši format glave.
- Poenostavljeno, učinkovitejše usmerjanje.
- Vgrajena je podpora za preverjanje pristnosti in zasebnost.

1.7.7 QoS

Kakovost storitve (QoS) je uporaba mehanizmov ali tehnologij, ki delujejo v omrežju za nadzor prometa in zagotavljanje delovanja kritičnih aplikacij z omejeno zmogljivostjo omrežja. Organizacijam omogoča prilagajanje celotnega omrežnega prometa z dajanjem prednosti določenim visoko zmogljivim aplikacijam.

QoS se običajno uporablja za omrežja, ki prenašajo promet za sisteme, ki zahtevajo veliko virov. Običajne storitve, za katere se zahteva, vključujejo televizijo internetnega protokola (IPTV), spletne igre, pretakanje medijev, videokonference, video na zahtevo (VOD) in glas prek IP (VoIP).

Z uporabo QoS v omrežju lahko organizacije optimizirajo delovanje več aplikacij v svojem omrežju in pridobijo vpogled v bitno hitrost, zakasnitev, periode signala (ang. jitter) in hitrosti paketov svojega omrežja. Vse to zagotavlja, da lahko načrtujejo promet v svojem omrežju in spremenijo način usmerjanja paketov v internet ali druga omrežja, da se izognejo zamudi pri prenosu. Slednje prav tako zagotavlja, da organizacija doseže pričakovano kakovost storitev za aplikacije in garantira pričakovane uporabniške izkušnje.

Glede na pomen QoS je ključni cilj omogočiti omrežjem in organizacijam, da dajo prednost prometu, kar vključuje ponudbo namenske pasovne širine, nadzorovanega tresenja in nižje zakasnitve. Tehnologije, ki se uporabljajo za zagotavljanje tega, so ključnega pomena za izboljšanje delovanja poslovnih aplikacij, prostranih omrežij (WAN) in omrežij ponudnikov storitev.

1.7.8 Ipsec

Varnost internetnega protokola (IPsec) je paket varnih omrežnih protokolov, ki preverja pristnost in šifrira pakete podatkov za zagotavljanje varne šifrirane komunikacije med dvema računalnikoma prek omrežja internetnega protokola. Uporablja se v virtualnih zasebnih omrežjih (ang. Virtual Private Network – VPN).

IPsec vključuje protokole za vzpostavitev medsebojne avtentikacije med agenti na začetku seje in pogajanje o kriptografskih ključih za uporabo med sejo. IPSec lahko zaščiti pretok podatkov med parom gostiteljev (gostitelj-gostitelj), med parom varnostnih prehodov (omrežje-omrežje) ali med varnostnim prehodom in gostiteljem (omrežje-gostitelj). IPsec uporablja kriptografske varnostne storitve za zaščito komunikacij prek omrežij internetnega protokola (IP). Podpira enakovredno preverjanje pristnosti na ravni omrežja, preverjanje pristnosti izvora podatkov, celovitost podatkov, zaupnost podatkov (šifriranje) in zaščito pred predvajanjem (zaščita pred napadi ponavljanja).

Začetna zbirka IPv4 je bila razvita z malo varnostnimi določbami. Kot del izboljšave IPv4 je IPsec model OSI plasti 3 ali varnostna shema internetne plasti od konca do konca. Nasprotno, medtem ko nekateri drugi internetni varnostni sistemi v široki uporabi delujejo nad omrežno plastjo, na primer Transport Layer Security (TLS), ki deluje nad transportno plastjo, in Secure Shell (SSH), ki deluje na aplikacijski plasti, lahko IPsec samodejno zaščiti aplikacije na internetni plasti. (Bajrami, 2019)

1.7.9 Protokol ICMPv6

Internetni protokol za svoje delovanje potrebuje dodaten kontrolni kanal, ki omogoča izmenjavo meta podatkov in protokol IPv6 ni izjema.
ICMPv6 *(Internet Control Message Protocol version 6)* je nov kontrolno-nadzorni protokol, ki je osnovan na podlagi svojega predhodnika (ICMP), pri tem pa zagotavlja dodatne podporne funkcije drugim protokolom.
Protokol ICMPv6 podpira 36 kontrolnih funkcij, a naprave uporabljajo ICMPv6 sporočila večinoma za naslednje osnovne funkcije:

- sporočanje napak pri prenosu (cilj je nedosegljiv, paket je prevelik, čas je potekel ipd.),
- odkrivanje največje prenosne enote, ki se lahko prenese do končnega vozlišča (uporaba dodatnega mehanizma Path MTU Discovery),
- omrežne diagnostične funkcije, kot so PING in TRACEROUTE z uporabo ICMPv6 sporočil Echo Request in Echo Reply,
- omogočanje delovanja protokola MLD *(Multicast Listener Discovery)*, ki uporablja ICMPv6 sporočila za odkrivanje prisotnosti multicast prejemnikov in njihovih zahtev po vključevanju v določeno multicast skupino. (IPv6.si, https://ipv6.si/, 2021)

1.8 Primerjava IPv4 in IPv6

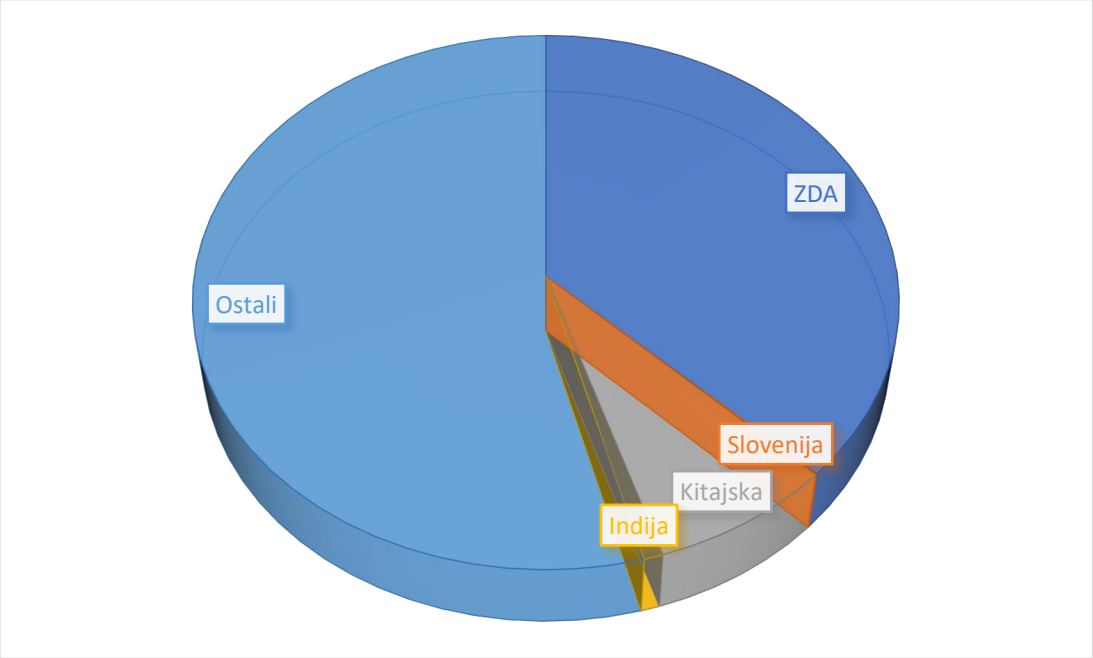
IPv4 je numerična metoda naslavljanja, medtem ko je IPv6 alfanumerična metoda naslavljanja. Binarni biti IPv4 so ločeni s piko, medtem ko so binarni biti IPv6 ločeni z dvopičjem (:). IPv4 ponuja 12 polj glave, IPv6 pa 8. To je zgolj groba primerjava, podrobnejšo si oglejmo po podpoglavjih.

1.8.1 Splošna primerjava

Dejstvo, da bo zmanjkalo IPv4 naslovov, nas je praktično že doseglo. Je pa tudi res, da vsi dodeljeni IPv4 naslovi niso v uporabi, v lasti jih imajo podjetja in organizacije, ki so si jih še pravočasno rezervirali.

Že sam podatek, da 95 % ljudi v Sloveniji ne uporablja interneta nam pove dovolj o sami neizkoriščenosti IPv4 internetnih naslovov. Razmah digitalne družbe in vse večja vključenost splošne populacije nas usmerja v uporabo interneta in internetnih aplikacij vse od javne uprave do internetnih nakupov.

Največ IPv4 naslovov imajo ZDA (1,6 milijarde); sledijo Kitajska, Indija, Slovenija ima 2,5 milijona IPv4 naslovov.



Graf 1: Količina dodeljenih IPv4 naslovov

Vir: Lastni vir

1.8.2 Tehnična primerjava

Tabela 2: Tehnična primerjava protokola IPv4 in protokola IPv6

IPv4	**IPv6**
IPv4 ima 32-bitni naslov	IPv6 ima 128-bitni naslov
IPv4 ima štiri številke, ločene s pikami	IPv6 uporablja šestnajstiška števila, ločena z dvopičjem (:)
IPv4 je v decimalni obliki	IPv6 je v šestnajstiški obliki
IPv4 podpira približno 4,29 milijarde naslovov	IPv6 podpira 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 edinstvenih naslovov
IPv4 ima glavo od 20 do 60 bajtov	IPv6 ima določeno glavo 40 bajtov
IPv4 podpira ročno konfiguracijo naslovov DHCP	IPv6 podpira samodejno konfiguracijo naslovov in preštevilčenje
Pri IPv4 fragmentacijo izvajajo predvsem pošiljatelj in usmerjevalniki za posredovanje	Pri IPv6 fragmentacijo izvede predvsem pošiljatelj
V IPv4 je na voljo polje za kontrolno vsoto	V IPv6 polje za kontrolno vsoto ni na voljo
V IPv4 identifikacija pretoka paketov ni na voljo	V IPv6 je identifikacija toka paketa na voljo in uporablja polje oznake toka v glavi
V IPv4 je največja prenosna enota (MTU) 576 bajtov	V IPv6 največja prenosna enota (MTU) znaša 1.280 bajtov
Posameznemu mrežnemu vmesniku je hkrati dodeljen samo en naslov.	Posameznemu mrežnemu vmesniku je dodeljenih več tipov naslovov hkrati (lokalni, globalni, multicast idr.)
Primer IPv4 je 192.168.1.8	Primer IPv6 je 2001:4860:4860:0000:0000:0000:0000:8888

Vir: Lastni vir

1.8.3 Prednosti in slabosti IPv4 in IPv6

Množično pošiljanje (ang. Multicasting)

Pomembna razlika med IPv4 in IPv6 je uporaba množičnega pošiljanja. To je način pošiljanja enega sporočila več prejemnikom, ki so izrazili zanimanje za njegovo prejemanje. Medtem ko je pošiljanje množičnih sporočil mogoče tudi znotraj omrežja IPv4, kjer je to izbirna funkcija, zato se oddajanje uporablja veliko pogosteje. Slednje ustvarja nepotrebne stroške, saj je oddajno sporočilo poslano vsem v omrežju brez razlikovanja, kar prisili naprave, da se z njim ukvarjajo, ne glede na to, ali je za njih pomembno ali ne. Zato zaradi učinkovitosti v IPv6 sploh ni oddajnih sporočil in je množično oddajanje osnovna specifikacija in ne izbirna funkcija.

Pv6 je hitrejši od IPv4 v omrežnih napravah, ker nima prevajanja omrežnih naslovov (ang. NAT). Raba IPv6 je boljša izbira za ljudi, ki potrebujejo visoko hitrost za svojo omrežno obdelavo.

1.9 Prehod iz IPv4 na IPv6

Glavni razlog za razvoj internetnega protokola različice 6 je bil zagotoviti zadostno število naslovov IP za prihodnjo uporabo. Kljub temu, da ponuja več kot štiri milijarde naslovov IP, se je različica internetnega protokola 4, razvita v zgodnjih osemdesetih letih, hitro izkazala za nezadostno, ko se je soočila z naraščajočo priljubljenostjo interneta. Edini način za povečanje naslovnega prostora je bila sprememba njegove strukture. Zato je naslov IPv6 dolg 128 bitov (v primerjavi z 32-imi biti pri IPv4) in uporablja šestnajstiški zapis (v nasprotju z decimalko, s pikami).

1.9.1 Kako opraviti prehod iz IPv4 na IPv6

Samodejna konfiguracija (DHCP)

Ena večjih razlik med IPv4 in IPv6 je, da slednji omogoča t. i. samodejno konfiguracijo naslova brez stanja (SLAAC). Pri IPv4 potrebujemo strežnik DHCP za samodejno dodelitev naslova IP napravi. Z IPv6 lahko naprava od usmerjevalnika pridobi omrežni ID (prvih 64 bitov) in ustvari lasten ID gostitelja (zadnjih 64 bitov), da ustvari polni naslov IPv6. Da bi usmerjevalnik to lahko opravil, naprava pošlje "naziv usmerjevalnika" (RS), ki zahteva omrežni naslov, in ga prejme od "oglasa usmerjevalnika" (RA), ki ga usmerjevalnik oglašuje tudi prek rednega eno-oddajanja.

To pomeni, da strežnika DHCP znotraj IPv6 več ne potrebujemo. Če imamo omrežje IPv4 in IPv6 z dvojnim skladom, še vedno potrebujemo strežnik DHCP za upravljanje IPv4. A četudi nimamo dvojnega sklada, potrebujemo strežnik, da napravam zagotovi vse druge možnosti DHCP. Morda bi ugotovili, da bi morali izvesti konfiguracijo »stateful« DHCPv6 (ki je zelo podobna konfiguracijskemu procesu v omrežju IPv4), če želimo bolj nadzorovano upravljanje naslovov IP. (CiscoPress, IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, 2nd Edition, 2017)

1.9.2 Načrt prehoda na IPv6

Na tej točki se lahko vprašamo, kdaj bo pomemben partner, kupec, ponudnik storitev ali opreme, naredil prehod na IPv6 in tako posredno prisilil uporabnike njegovih internetnih storitev, da mu bodo sledili. Morda bo nova, zelo pomembna aplikacija ali storitev delovala

samo na IPv6. V izogib tem scenarijem se je potrebno pripraviti in protokol IPv6 uvajati postopoma z življenjskimi cikli zamenjave opreme.

Protokol IPv6 je toliko drugačen od svojega predhodnika IPv4, da se ga ne more uvesti čez noč. Najprej ga je potrebno preučiti in nato postopoma, na sistematičen način uvesti v okolje organizacije, kar zahteva svoj čas. Ključno pri uvajanju je, da je uvedba za uporabnike transparentna in minimalno vpliva na razpoložljivost storitev, zato je potrebno najprej izdelati podroben načrt prehoda in se ga kasneje tudi držati.

Načrt prehoda na IPv6 vključuje korake, ki jih je pri uvedbi potrebno izvesti v celotnem omrežju in storitvah. Posamezne aktivnosti se lahko izvede zaporedno, druge se izvajajo vzporedno, v odvisnosti od razpoložljivega kadra in časovnih omejitev. Z vidika poslovanja je smiselno, da se prednostno izven notranjega omrežja preko IPv6 uvede tiste storitve, ki pogojujejo poslovanje podjetja (spletne strani, elektronska pošta, DNS, razne aplikacije idr.).

Načrt mora vključevati naslednje aktivnosti:

- načrtovanje prehoda (aktivnosti, število vključenih kadrov, ocena potrebnega dela, program izobraževanja),
- ocena stroškov (stroški opreme in kadra),
- izobraževanje kadra,
- inventura programske in strojne opreme,
- pridobitev IPv6 naslovnega prostora,
- pridobitev IPv6 povezljivosti,
- kreiranje IPv6 omrežne arhitekture,
- kreiranje IPv6 naslovnega načrta in usmerjanja,
- načrtovanje varnostne arhitekture glede na ocenjena varnostna tveganja,
- vzpostavitev testnega IPv6 omrežja v ločenem okolju,
- konfiguriranje omrežja in varnostnih naprav (požarne pregrade, IDS/IPS, naprave za porazdelitev bremena, VPN koncentrantorji),
- produkcijska vzpostavitev IPv6 na ravni omrežja in varnostnih naprav,
- konfiguriranje in testiranje povezav z oddaljenimi lokacijami, vključno z varnostjo (VPN),
- vzpostavitev osnovnih omrežnih storitev (DNS, DHCP, upravljanje omrežja),
- testiranje storitev in aplikacij v testnem okolju (podatkovne baze, registri, telefonija, CMS, spletni in poštni strežniki itn.),
- produkcijska vzpostavitev storitev in aplikacij na IPv6 v notranjem in zaščitenem zunanjem okolju,

- postopno aktiviranje IPv6 na delovnih postajah, tiskalnikih,
- produkcijska vzpostavitev povezav z oddaljenimi lokacijami.

Priporočljivo je, da se najprej izdela podrobna analiza trenutnega stanja strojne in programske opreme, v okviru katere se preveri združljivost obstoječe opreme z IPv6 in stopnjo implementacije nujno potrebnih funkcionalnosti. Analiza pokaže v katerih primerih bo dovolj le nadgradnja programske opreme in v katerih bo potrebno opremo delno ali v celoti zamenjati. Pomembno je, da se ob zamenjavi opreme (ob nakupu in v razpisih) zahteva, da je oprema, ki se menja v vseh potrebnih funkcijah združljiva z IPv6. V dodatno pomoč pri menjavi opreme je lahko priporočilo RIPE-554 *(Requirements for IPv6 in ICT Equipment),* ki ga je v okviru RIPE skupnosti pripravila skupina slovenskih in tujih strokovnjakov. Priporočilo je nastalo na podlagi najboljših praks in je popolnoma nevtralno kar se tiče ponudnikov strojne in programske opreme. Vsebuje seznam obveznih in opcijskih tehničnih IPv6 specifikacij ter podporo zahtevanim RFC standardom, ki jih mora podpirati različna strojna in programska oprema za delovanje v IPv6 omrežjih.
Cilj inventure oziroma podrobne analize stanja strojne opreme je, da se oceni raven pripravljenosti strojne opreme za prehod na IPv6. Ugotoviti je potrebno ali se lahko z obstoječo opremo preko protokola IPv6 izvaja vsaj podobne funkcije, kot se jih je preko IPv4, seveda če je takšna naša zahteva. Za vsak kos opreme je potrebno vedeti, katere funkcije izvaja, na kakšen način (strojno ali programsko) se funkcije izvajajo in kakšen vpliv imajo na uvedbo protokola IPv6. (IPv6.si, https://ipv6.si/, 2022)

1.9.3 Transformacija IPv6 v IPv4

Ker se sam prehod iz IPv4 na IPv6 ne bo zgodil iz danes na jutri oz. takoj, je potrebno zagotoviti hkratno delovanje naprav preko protokola IPv4 in naprav s protokolom IPv6. To nam zagotavlja translacija oz. transformacija obeh protokolov iz enega v drugega oz. iz drugega v prvega. Obstaja več načinov zagotavljanja hkratnega delovanja naprav, in sicer:

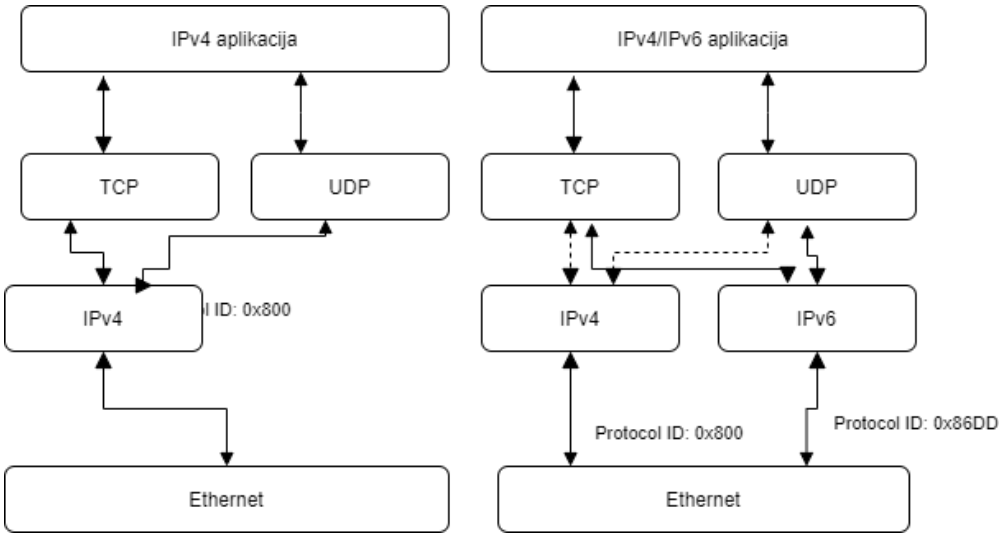
- dvojni sklad ang. Dual Stack, kjer so vse naprave opremljene tako z IPv4, kot IPv6 naslovi,
- translacija IPv6 v IPv4,
- tuneliniranje IPV4 v IPv6,
- NAT64/DNS64 translacija za mobilne naprave.

1.9.3.1 Dvojni sklad (ang. Dual Stack)

Ker se sam prehod iz IPv4 na IPv6 ne bo zgodil čez noč, bo potrebno še določeno tranzicijsko obdobje.

Ponudniki internetnih storitev so večinoma izbrali metodo prehoda naslovov IP, imenovano dvojni sklad. Rešitev z dvojnim skladom vsaki omrežni napravi, strežniku, stikalu, usmerjevalniku in požarnemu zidu v omrežju ponudnika internetnih storitev konfigurira z zmogljivostmi povezljivosti IPv4 in IPv6. Najpomembneje je, da tehnologija dvojnega sklada ponudnikom internetnih storitev omogoča hkratno obdelavo podatkovnega prometa IPv4 in IPv6.

Kaj to pomeni za uporabnika? Preprosto to, da bomo lahko še naprej brskali po internetu, ne da bi se spraševali, ali bo naša povezava prenehala delovati zaradi pretvorbe naslova IP.



Slika 2: Primerjava IPv4 in dvojnega sklada

Vir: (Lastni vir)

1.9.3.2 Translacijski mehanizmi

Dokler smo uporabljali samo klicne modemske povezave do ponudnika interneta, je bilo IPv4 naslovov dovolj, saj se je s prekinitvijo povezave sprostil tudi začasno dodeljen IPv4 naslov. S porastom širokopasovnih povezav pa internetni ponudniki in sedaj tudi mobilni operaterji prihajajo do situacije, da jim IPv4 naslovov zmanjkuje, saj širokopasovne povezave zahtevajo stalno povezljivost v internet ter stalno dodeljene IP številke.

Pomanjkanje javnih globalnih IP naslovov nam rešuje translacijski mehanizem imenovan NAPT (angl. Network Address Port Translation). Osnovni NAT mehanizem, ki izvaja samo translacijo naslovov je bil predstavljen leta 1994 z internetnim standardom RFC 1631. NAT mehanizem, ki je običajno implementiran kot del usmerjevalnika/požarne pregrade ima en zunanji vmesnik (angl. Interface), ki je naslovljen z javnim IPv4 naslovom ter eden ali več notranjih vmesnikov, ki so povezani na notranje zasebno omrežje. V notranjem omrežju uporabljamo zasebne IPv4 naslove, ki so določene z internetnim standardom RFC 1918 in se lahko podvajajo tudi v drugih zasebnih omrežjih. Z RFC 1918 določeni zasebni IP naslovi:

- 10.0.0.0/8-10.255.255.255/8;
- 172.16.0.0/12-172.31.255.255/12;
- 192.168.0.0/16-192.168.255.255/16;

se lahko uporabljajo izključno v zasebnih omrežjih ter se ne smejo pojaviti v javnem internetnem omrežju. Da tej zahtevi zadostimo, morajo biti zasebni IPv4 naslovi blokirani na robnih požarnih pregradah zasebno/javnega omrežja. (Wikipedia, 2023)

1.9.3.3 Tuneliranje IPv4 v IPv6

Tuneli so velikokrat uporabljena tehnika, predvsem kadar gre za usmerjanje prometa IPv6 pri prehodu iz IPv4. Tuneliranje IPv4 v IPv6 se nanaša na uporabo trenutnega sistema usmerjanja naslova IPv4 za prilagoditev neizogibnemu prometu IPv6. Pomaga pri učinkovitem prehodu na IPv6 z ohranjanjem skladnosti z gostitelji IPv4 in trenutno konfiguriranimi usmerjevalniki. Poleg tega lahko pospešimo postopek prenosa na IPv6 z ohranjanjem kontinuitete med infrastrukturnimi sistemi. To je bilo zato, ker ko uporabljamo IPv6, lahko uporabimo tudi omrežno infrastrukturo IPv4 za optimizacijo virov, ki so na voljo.
Za tuneliranje IPv6 preko obstoječih omrežij IPv4 so na voljo številni prehodni mehanizmi:

- ročno konfigurirano tuneliranje IPv6 preko IPv4
- tuneliranje IPv6 preko IPv4 GRE
- polavtomatsko tuneliranje
- popolnoma samodejno tuneliranje
- tuneliranje ISATAP.

Usmerjevalnik in gostiteljski strežnik IPv4 ali IPv6 lahko ustvarita podatkovni paket IPv6 prek omrežne topologije naslovov IPv4 tako, da jih uporabita v uporabnih paketih IPv4. Predvsem je mogoče doseči tuneliranje iz IPv4 v IPv6.

Usmerjevalniki IPv4 ali IPv6 so povezani s paketnimi tuneli IPv6 med napravami prek vmesnika IPv4. To pomeni, da zdaj predor pokriva vsak posamezen del poti od konca do konca paketa IPv6.

Host-to-Router: je gostiteljski tunel IPv4 ali IPv6 do vmesnega usmerjevalnika IPv4 ali IPv6, ki je v tem primeru dosegljiv prek trenutne infrastrukture IPv4. V tem primeru tunel zasede le prvi del poti od konca do konca paketa IPv6.

Host-to-Host: je dejansko povezovanje gostiteljev IPv4 ali IPv6 s paketi IPv6 tunela v omrežjih, ki uporabljajo arhitekturo IPv4. Celotna pot paketa IPv6 od konca do konca je v tem primeru zaščitena.
Router-to-Peer: usmerjevalniki IPv4 ali IPv6 tunelirajo do dejanskega ciljnega gostitelja, ne glede na to, ali je IPv6 ali IPv4. To pomeni, da predor zaseda samo zadnji del poti od konca do konca paketa IPv6.

Skladnost s široko razporejenimi strežniki in usmerjevalniki IPv4 je skrivnost gladkega prehoda IPv6. Postopek pretvorbe interneta v IPv6 je poenostavljen zaradi združljivosti IPv4 z uporabo IPv6. IPv6 povezuje izolirane lokacije IPv6 z omrežjem IPv4 prek tunela IPv4. Implementacija IPv6 prek IPv4 bo podprla ponudnike storitev in podjetja, ki so vključena v zagotavljanje storitev IPv6 od konca do konca, brez bistvenih izboljšav infrastrukture. Zmožnost povezovanja izolirane prevlade IPv6 nad obstoječo infrastrukturo in storitvami IPv4 je ena od ključnih prednosti te metode tuneliranja.

S tuneliranjem IPv6 prek IPv4 konfiguracijski podatki o zaprtem vozlišču določijo ciljni naslov tunela IPv4. Uporabljajo se lahko enosmerni ali dvosmerni tuneli. Dvosmerni tuneli služijo kot virtualne povezave od točke do točke. Čeprav platformi IPv4 in IPv6 ne moreta eksplicitno medsebojno delovati, obstajajo sheme prenosa, ki gostiteljem omogočajo povezavo s katerim koli drugim uporabnikom v kateri koli omrežni obliki.

Procesi prenosa povezujejo IPv4 z IPv6 in obema možnostma omogočijo skupno delovanje. Ker je IPv6 poseben protokol IPv4, bi lahko preklop z IPv4 na IPv6 izvajali sočasno z IPv4. Tako IPv4 kot IPv6 se lahko izvajata na istem ogrodju (dvojno zlaganje) hkrati s sistemom gostitelja in omrežja ter sta skrita. Oba protokola nimata nobene intervencije. Omrežja IPv4 bi bila sčasoma izgubljena, ko bi prešli na IPv6. (Prefixx, 2021)

1.9.3.4 NAT64/DNS64

NAT64 je mehanizem, ki gostiteljem IPv6 omogoča komunikacijo s strežniki IPv4. Strežnik NAT64 je končna točka za vsaj en naslov IPv4 in 32-bitni segment omrežja IPv6, npr. 64:ff9b::/96. Odjemalec IPv6 vdela naslov IPv4, s katerim želi komunicirati z uporabo teh

bitov, in pošlje svoje pakete na nastali naslov. Strežnik NAT64 nato ustvari preslikavo NAT med naslovoma IPv6 in IPv4, kar jima omogoči komunikacijo.

DNS64 opisuje strežnik DNS, ki na zahtevo po zapisih AAAA domene, vendar najde samo zapise A, sintetizira zapise AAAA iz zapisov A. Prvi del sintetiziranega naslova IPv6 kaže na prevajalnik IPv6/IPv4, drugi del pa vdela naslov IPv4 iz zapisa A. Zadevni prevajalnik je običajno strežnik NAT64. Standardna specifikacija DNS64 je v RFC 6147.

S tem mehanizmom prehoda gre opaziti dve težavi:

- deluje samo v primerih, ko se za iskanje naslova oddaljenega gostitelja uporablja DNS; če se uporabljajo deli naslova Ipv4 namesto imena domene, strežnik DNS64 ne bo nikoli vključen,
- ker mora strežnik DNS64 vrniti zapise, ki jih ni določil lastnik domene, preverjanje DNSSEC glede na koren ne bo uspelo v primerih, ko strežnik DNS, ki izvaja prevod, ni strežnik lastnika domene.

1.9.3.5 Varnostna primerjava

Iz vidika same varnosti omrežij, ki bazirajo na Ipv4, so omrežja Ipv6 varnejša, in sicer:
Sam prenos paketov v IPv6 bazira na IPSec varnostnem protokolu, kar pomeni, da je varnost internetnega protokola (IPSec) vključena v IPv6. To preprosto pomeni, da je komunikacija med obema končnima točkama overjena, šifrirana ali oboje prek glav razširitev.
Šifriranje IPv6: medtem ko je bilo šifriranje od konca do konca (ang. End to End) retroaktivno dodano IPv4, je bilo vgrajeno v IPv6. Šifriranje in preverjanje celovitosti, ki ju trenutno uporabljajo omrežja VPN, velja standard v Ipv6 za vse naprave in sisteme.
PPPoE je konfiguriran kot povezava od točke do točke med dvema vmesnikoma Ethernet. Kot protokol za tuneliranje se PPPoE uporablja kot učinkovita podlaga za prenos paketov IP na omrežni ravni. IP je prekrit s povezavo PPP in uporablja PPP kot navidezno klicno povezavo med točkami v omrežju. (Setra-Brumley, 2022)

1.9.4 Kaj se je zgodilo s protokolom IPv5 in ostalimi?

Na tej točki se morda sprašujemo, zakaj razpravljamo samo o IPv4 in IPv6, kot da med njima ni druge številke. Pravzaprav je to skrivnost lažje razrešiti kot odsotnost sistema Windows 9. Na neki točki je bil razvit eksperimentalni protokol, imenovan ISP (ang. Internet Stream Protocol), ki mu je bila v glavi IP dodeljena številka različice 5, čeprav ni bil na noben način oblikovan kot naslednik IPv4. Kljub temu je IPv6 moral prevzeti naslednjo razpoložljivo številko različice, da bi se izognili zmedi.

In če je IPv4 prva implementacija protokola v resničnem življenju, kaj se je zgodilo z IPv1 do 3? Pred implementacijo IPv4 se internetni protokol sploh ni uporabljal – njegove funkcije je opravljal protokol za nadzor prenosa (TCP). Zgodovina teoretičnih razprav o prejšnjih različicah protokola in o tem, zakaj ga je bilo treba ločiti od TCP, da bi ustvarili zbirko TCP/IP, je druga zgodba in jo je mogoče izslediti v dokumentih IEN (ang. Internet Experiment Note). (Lifewire, 2022)

1.10 Brezžične naprave IPv6

Internetni protokol različice 6 (IPv6) je napreden omrežni standard, ki napravam omogoča uporabo veliko večjega števila edinstvenih naslovov IP kot v starejšem standardu (IPv4). Ker se število teh naprav nenehno povečuje, nekateri ponudniki internetnih in mobilnih storitev že sedaj aktivno uporabljajo IPv6 naslavljanje mobilnih naprav, česar uporabniki sami niti ne opazijo.

1.10.1 Povečana mobilnost

Omejitve IPv4 so prisilile uvedbo posebnega protokola IP za mobilne naprave, imenovanega Mobile IP (MIP), ki uporablja trikotno usmerjanje. Zaradi omejenega nabora naslovov IPv4, je bilo nemogoče omogočiti mobilnim napravam, da obdržijo svoje naslove IP, ko se premikajo med omrežji (gostovanje), kar jim posledično onemogoča sledljivost med lokacijami. Rešitev tega je bila, da se napravi dodeli nov naslov IP, ko se premakne v novo omrežje (t. i. »obiskano omrežje«), vendar se ves promet, usmerjen v to napravo, usmeri prek njenega izvornega

omrežja (»domače omrežje«), ki je posodobljeno z novim naslovom. Čeprav je pametna rešitev, si lahko predstavljamo, da je tudi zelo neučinkovita in ustvarja veliko nepotrebnega prometa.
V nasprotju z mobilnim IPv4 je bil postopek v mobilnem IPv6 optimiziran tako, da trikotno usmerjanje ni več potrebno in se namesto tega uporablja neposredno usmerjanje. V tem scenariju, ko naprava gostuje, se domače omrežje uporablja samo za oglaševanje novega naslova IP naprave, tako da je mogoče z njo vzpostaviti neposreden stik, domačemu omrežju pa ni potrebno obravnavati vsega prometa.

1.10.2 Eduroam

Storitev Eduroam omogoča učencem in zaposlenim varen in preprost dostop do zaščitenega brezžičnega (WLAN) omrežja na bilo kateri šoli, ki omogoča Eduroam in gostovanje v omrežjih drugih institucij, vključenih v sistem Eduroam.
V omrežje Eduroam so vključene izobraževalne in raziskovalne ustanove (fakultete, inštituti, osnovne in srednje šole) v Sloveniji (http://www.eduroam.si) in tujini (http://www.eduroam.org).
Omrežje je zasnovano tako, da lahko učenci ali zaposleni dostopajo transparentno in brezplačno v katerikoli zgoraj navedeni ustanovi (doma in v tujini), in to z istim uporabniškim imenom in geslom kot v "domačem" omrežju Eduroam (npr. učitelj) dostopa v zaščiteno omrežje Eduroam drugje po Sloveniji oz. v katerokoli omrežje Eduroam v tujini. Pri tem je tako sami ustanovi kot gostujočem uporabniku zagotovljena kar največja varnost, saj je onemogočeno prisluškovanje in lažno predstavljanje.
V brezžično omrežje z imenom (SSID) Eduroam se je mogoče povezati s prenosnim računalnikom, dlančnikom, telefonom; skratka z napravo, na kateri operacijski sistem in brezžični vmesnik podpira standard 802.11a/g/n ter varnostni protokol WPA1/2/3, podjetniško (WPA1/2/3-Enterprise) in prijavni standard 802.1x z EAP-TTLS + PAP z enkripcijo podatkov AES.

Poleg tega je za brezžični dostop potrebno še veljavno uporabniško ime in geslo v matični ustanovi. Za uspešno prijavo v omrežje Eduroam potrebujemo veljavno uporabniško ime in geslo v matični organizaciji. Učenci pridobijo uporabniško ime in geslo, ki ju prejmejo po oddaji obrazca »Prijavnica za osebni dostop do omrežja Eduroam« s podpisom staršev oz. skrbnikov.

Brezžično omrežje Eduroam bazira na IPv6 protokolu, izven omrežja IPv6 pa se izvaja NAT64/DNS64 translacija. (Edoroam, 2022)

1.10.3 Internet stvari (ang. Internet of Things)

Internet stvari ali medomrežje stvari je razširitev internetnega povezovanja na in med napravami ter vsakodnevnimi predmeti. S pomočjo elektronike, internetne povezave ter senzorjev in ostale strojne opreme, lahko te naprave med seboj komunicirajo in si izmenjujejo podatke.
IPv6 zagotavlja izboljšan oddaljeni dostop in upravljanje za velike flote naprav IoT. Druga velika prednost IPv6 je njegova zelo učinkovita funkcija množičnega pošiljanja sporočil (ang. multicast), ki skorajda odpravlja potrebo po rutinskem oddajanju sporočil.
IPv6 multicast izboljša učinkovitost omrežja tako, da gostitelju omogoči prenos podatkovnega paketa do ciljne skupine sprejemnikov. Na primer, gostitelj bo morda želel poslati velik video posnetek skupini izbranih prejemnikov. Za gostitelja bi bilo dolgotrajno, če bi podatkovni paket poslal posamezno vsakemu prejemniku. Če gostitelj oddaja video posnetek po celotnem omrežju, omrežni viri niso na voljo za druga opravila. Gostitelj uporablja samo vire, ki jih potrebuje pri oddajanju podatkovnega paketa.

Usmerjevalniki uporabljajo algoritme večoddajnega tipa usmerjanja za določitev najboljše poti in pošiljanje večoddajnih podatkovnih paketov po celotnem omrežju. Usmerjevalniki serije E podpirajo številne IPv6 večoddajne protokole na virtualnih usmerjevalnikih. Vsak navidezni usmerjevalnik samodejno skrbi za interoperabilnost protokolov IPv6 multicast.
IP množično pošiljanje sporočil uporablja povratno posredovanje RPF (ang. Reverse Path Forwarding), da preveri, ali usmerjevalnik prejme večoddajni paket na pravilnem dohodnem vmesniku. Algoritem RPF usmerjevalniku omogoča, da sprejme večoddajni podatkovni paket samo na vmesniku, s katerega usmerjevalnik pošlje enostranski podatkovni paket viru večoddajnega podatkovnega paketa.

Posredovanje po povratni poti (RPF) je tehnika, ki se uporablja v sodobnih usmerjevalnikih za namene zagotavljanja posredovanja večvrstnih paketov brez zank pri večoddajnem (ang. multicast) usmerjanju in za pomoč pri preprečevanju lažnega predstavljanja IP-naslova pri unikatnem usmerjanju.

Ko usmerjevalnik prejme večoddajni podatkovni paket od vira za skupino, preveri, ali je bil paket prejet na pravilnem vmesniku RPF. Če paket ni bil prejet na pravem vmesniku, ga usmerjevalnik zavrže. Samo paketi, prejeti na pravilnem vmesniku RPF, se upoštevajo za posredovanje spodnjim sprejemnikom.

Ko delujejo v redkem načinu, usmerjevalniki izvedejo iskanje RPF, da identificirajo zgornji usmerjevalnik, od katerega zahtevajo podatke, in nato pošljejo pridružitvena sporočila za večoddajni tok samo temu usmerjevalniku.

Ko delujejo v zgoščenem načinu, usmerjevalniki, ki imajo več poti do vira večoddajnega toka, najprej prejmejo isti tok na več kot enem vmesniku. V tem primeru usmerjevalniki izvedejo iskanje RPF, da identificirajo večoddajne tokove podatkov, ki ne prispejo na najboljšo pot, in pošljejo sporočila za obrezovanje, da te tokove prekinejo.

Ni nujno, da je iskanje RPF vedno usmerjeno proti viru večoddajnega toka. Iskanje se izvede v smeri vira le, če usmerjevalnik uporablja izvorno ukoreninjeno drevo za sprejem večoddajnega toka. Če usmerjevalnik namesto tega uporablja skupno drevo, je iskanje RPF usmerjeno proti točki srečanja in ne proti viru večoddajnega toka.

1.11 Vpliv digitalne preobrazbe na okolje

Pomembno je, kako se v internet povezujemo. Čeprav morda ne vidimo in čutimo oz. nas sploh ne zanima, kako se naša naprava poveže z internetom, je vsak majhen delček energije le še ena kapljica v vedno večjem vedru, ki je internetni račun za energijo.

Izgradnja trajnostnega in energetsko učinkovitega svetovnega spleta bo zahtevala več kot le ogromne naložbe v nove tehnologije in digitalno infrastrukturo, zahtevala bo premik v tem, kako učinkovito upravljamo vire in protokole, ki jih že imamo.
Čeprav naslovi IPv4 še vedno dobro delujejo, obstaja ena velika težava: na voljo je samo 4,3 milijarde edinstvenih naslovov IPv4 in vsi so že dodeljeni. Globalna ponudba za IPv4 je izčrpana.

Kot odgovor na to je bil IPv6 ustvarjen za rešitev te grozeče težave in s svojimi neverjetnimi $3{,}4 \times 10^{38}$ edinstvenimi naslovi je IP-jev na voljo še veliko. IPv6 ima veliko prednosti, vendar ima eno pomanjkljivost. Ni ravno IPv4. IPv4 se še vedno pogosto uporablja na starejših napravah in ima v nekaterih aplikacijah prednost pred IPv6. Dejstvo je, da je precejšen del naslovov IPv4 neuporabljenih in jih imajo trenutno rezervirane nekatere največje svetovne korporacije.
Tukaj nastopi IP leasing. Zakup IP ima številne komercialne in poslovne aplikacije, zaradi katerih je priročna, trajnostna in cenovno ugodna možnost za podjetja, katerih rast je odvisna od dostopa do zadostnega števila IP naslovov. Kljub temu se zakup IPv4 lahko uporablja ne le kot orodje za priročno rast in zmanjševanje režijskih stroškov, ampak se lahko uporablja tudi za zmanjšanje spletnega vpliva podjetja na okolje.

Druga prednost IPv4 je, da v nekaterih primerih morda potrebuje manj energije za povezavo z internetom kot naprave, ki delujejo na IPv6. Leta 2017 je bila izvedena študija, ki je primerjala enake pametne telefone, ki delujejo na IPv4 oziroma IPv6. Preliminarni rezultati so razkrili, da IPv6 za delovanje potrebuje približno 5 % več energije, in čeprav se 5 % morda zdi majhna količina, če se pomnoži z milijardo ali dvema, bi ta številka lahko postala precejšnja poraba energije.

Čeprav je v zvezi s to zadevo potrebno bolj poglobljeno testiranje, dejstva kot taka močno kažejo, da bi lahko uporaba neuporabljenih IPv4 namesto IPv6 zagotovila oprijemljive rezultate, ko želimo zmanjšati stroške energije in celotno globalno porabo energije.
Trenutno sta internet in vsa tehnologija, ki mu omogoča delovanje, odgovorna za približno 3,7 % svetovnih toplogrednih plinov. Predvideva se, da se bo to število do leta 2025 podvojilo zaradi hitre rasti prebivalstva in hitre modernizacije držav v razvoju. Čeprav se tudi to v veliki shemi ne zdi velika številka, je blizu količini emisij, ki jih proizvede letalska industrija.

Brez zadostnega števila naslovov IP morajo naprave, odvisne od IPv4, intenzivno tekmovati za razpoložljive vire, kar dodatno obremeni omrežje in spodbuja idejo, da bi starejšo tehnologijo izločili iz uporabe. Ta prisilna zastarelost bi še dodatno povečala število novih naslovov IPv6, kar bi verjetno povzročilo povečanje emisij, ki bi jih povzročile naraščajoče povezave prek IPv6, kot tudi obsežna proizvodnja naprav naslednje generacije.

Več IPv4 na trgu bi uporabnikom omogočilo, da bi starejše naprave in pripomočke ohranili v uporabi in izven odlagališč nekoliko dlje, kar bi lahko, če ne zmanjšalo, vsaj ne povečalo skupnega ogljičnega odtisa interneta.
Čeprav je zmanjkalo novih naslovov IPv4, to ne pomeni, da so vsi v uporabi. Nekatera velika podjetja, ki so veliko pred pomanjkanjem pridobila IPv4, se odločijo, da bodo svoje neuporabljene naslove hranila v rezervi. Ta podjetja pogosto ne morejo prodati svojih neuporabljenih naslovov IP, saj so motivirana, da jih obdržijo v svoji lasti, da bodo na voljo in sčasoma olajšali prihodnjo rast.

Resnična težava s temi mirujočimi naslovi IPv4 je, da vsak posamezen IP še vedno potrebuje napajanje, vendar se ta moč ne uporablja za izvajanje podatkov. Ta v bistvu neuporabna skupina energetsko pomanjkljivih IP-jev bi lahko ponovno začela delovati in ustvarjati trgovino za približno enake stroške električne energije.

Zakup IP lahko odpravi te nepovratne stroške električne energije, s čimer ustvari bolj učinkovit in trajnosten internet, obenem pa zagotovi IPv4 za manjša podjetja, ki jih bolj nujno potrebujejo. IPv6 pridobiva na moči v Severni Ameriki in Evropi, vendar je še vedno zelo daleč od standarda v večjem delu preostalega sveta. Konec koncev povezava IPv4 z IPv6 ni najlažji podvig.

Stari in zanesljivi IPv4 ne bo kmalu odšel nikamor. Boj proti podnebnim spremembam in izgradnja trajnostne prihodnosti (in interneta) bosta medtem zahtevala pametno in učinkovito uporabo vseh digitalnih virov. Zakup IPv4 je preprost in učinkovit način za pozitiven vpliv na okolje brez velikega vnaprejšnjega vložka denarja, časa in dela.

Trgi zakupa IP igrajo ključno vlogo pri gradnji trajnostnega, učinkovitega in poštenega interneta, saj ponujajo okolju prijazno možnost povečanja s spremembo namena neuporabljenih virov IPv4, ki okolju prijazno podjetjem ponujajo okolju prijazna podjetja.

IPv4 že leta odlično služi digitalni pokrajini in bo z uporabo učinkovitega zakupa zdaj lahko tako uspešen tudi v zeleni prihodnosti. (TechRadar, 2021)

3. PRAKTIČNI DEL

Kot praktični primer prehoda iz IPv4 na IPv6 bom obravnaval kako opraviti tak prehod na osnovni šoli, in sicer konkretno na osnovni šoli Miklavž na Dravskem polju. V šoli se že nekaj časa pripravljamo, da bi izvedli tranzicijo, ker je zaradi Eduroam sistema po šoli prehod na IPv6 že skoraj nujno potreben oz. nujen. Arnes gradi, vzdržuje in upravlja infrastrukturo, ki povezuje univerze, inštitute, raziskovalne laboratorije, muzeje, šole, baze podatkov in digitalne knjižnice. Svojim uporabnikom nudi enake storitve kot nacionalne akademske mreže iz drugih držav, s katerimi sodeluje v projektih Evropske komisije pri testiranju, razvoju rešitev in vpeljavi novih internetnih protokolov in storitev. Opravlja tudi storitve, ki jih komercialne organizacije ne opravljajo, a so predpogoj za delovanje interneta v Sloveniji. Torej prehoda iz IPv4 na IPv6 brez pomoči Arnes-a ni.

1.12 Predstavitev praktičnega dela

Osnovna šola Miklavž na Dravskem polju obsega dve nadstropji z dodanimi tremi učilnicami v medetaži v šolskem letu 2022–2023. Dostop do interneta omogoča podjetje Telemach s svojim optičnim priklopom. Na Telemach-ov modem je priklopljen Arnes-ov Cisco 1900 usmerjevalnik, ki deluje kot most (ang. bridge) in preko katerega se filtrira ves promet iz in v internet. Na sliki 3 sta prikazani dve vrsti usmerjevalnikov, ki jih uporablja Arnes za povezovanje uporabnikov v svoje omrežje.

Slika 3: Dostopovna oprema za povezavo v internet

Vir: (Arnes)

Cisco 1900 usmerjevalnik ima le en ethernet izhod, na katerega je neposredno povezano 24-portno 1Gb stikalo brez možnosti nastavitve ločenih podomrežij znotraj obstoječega. Zaradi pomanjkanja dodeljenih IPv4 naslovov, je preko virtualnih strežnikov in nameščenega DHCP na vsakem še vsaj pet lokalnih podomrežij za računalniško učilnico, za računovodstvo in upravo, za tehnično učilnico in zbornico. Celotna šola je prav tako omrežena še z Eduroam brezžičnim hitrim internet sistemom, ki omogoča dostop do interneta in internetnih virov z uporabo AAI računa.

Prav zaradi uvedbe Eduroam-a, se pojavljajo težave s tiskanjem na mrežne tiskalnike, ki so v šoli trije, ravno dovolj za potrebe tiskanja izdelkov učiteljev in tehničnega osebja. Za računovodstvo in upravo je namenjen popolnoma ločen tiskalnik, ki v omrežju izven uprave ni viden. Tiskalniki za učitelje so v zbornici, računalniški učilnici in kabinetu računalničarja. Hkrati so to tudi mrežni skenerji in je za ta namen namenjen omrežni disk na enem izmed virtualnih strežnikov.

Slika 4: Pogled na zadnjo ploščo Cisco usmerjevalnika serije 1900

Vir: (Cisco Packed Tracer)

1.13 Podrobna predstavitev rešitve

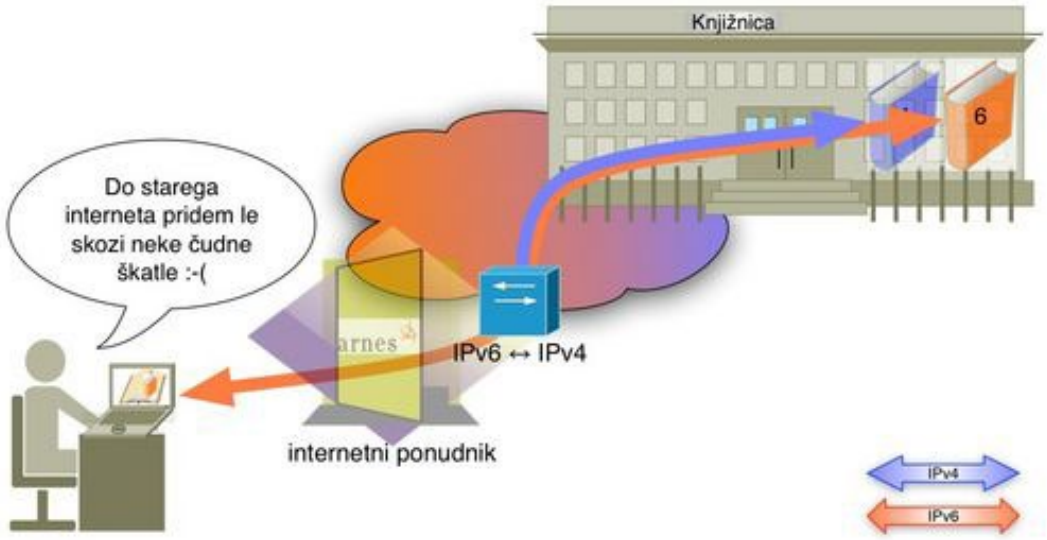
Glede na to, da kot glavni usmerjevalnik še vedno uporabljamo starejši model Cisco 1900 serije, bi bilo potrebno kot prvo zamenjati glavni usmerjevalnik za novejšega Cisco Cat3560, ki ima IPv6-podporo v osnovni različici IOS. Za to je kot skrbnik omrežja zadolžen Arnes, strošek nabave pa je na strani šole same.

V samo menjavo opreme bo potrebno zajeti tudi nova oz. novejša stikala, in to vsaj tri.

Arnes

Arnes kot akademska in raziskovalna mreža Slovenije zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture ter omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini.

Kot skrbnik omrežja, Arnes omogoča tako IPv4 kot IPv6 povezljivost, hkrati pa skrbi za translacijske mehanizme med obema protokoloma.



Slika 5: translacija IPv6 v IPV4

Vir: (Arnes)

Pri povezovanju brezžičnih naprav preko Eduroam-a v internet, pridobi vsaka izmed teh naprav IPv6 naslov. Takoj se pojavi težava, ko je potrebno komunicirati z ostalimi napravami, ki še uporabljajo IPv4 internetni protokol. Prav tako je večina internetnih strani in strežnikov konfigurirana na IPv4 protokolu. V tem primeru je najhitrejša in najboljša rešitev, da napravam, ki to omogočajo nastavimo oba IPv4 in Ipv6 statična naslova, da je taka naprava v omrežju dosegljiva preko obeh protokolov. (Arnes, 2020)

Na sliki 6 je prikazana nastavitev dvojnega sklada konfiguracije omrežnega tiskalnika HP PageWide Pro 477dw MFP, ki jih uporabljamo v šoli Miklavž na Dravskem polju.

IPv4

Ime domene	
Konfiguriral	Ročno
Naslov IP	141.255.246.13
Maska podomrežja	255.255.255.224
Privzeti prehod	141.255.246.1
DNSv4	
Konfiguriral	Ročno
Prednostni naslov DNS	
Nadomestni naslov DNS	
WINS	
Konfiguriral	Ni konfigurirano
Primarni strežnik WINS	0.0.0.0
Sekundarni strežnik WINS	0.0.0.0

IPv6

Ime domene

Naslov IP	Dolžina predpone	Konfiguriral
fe80::3a22:e2ff:fe3a:af69	64	Samodejno
2001:1470:f11d:cc:3a22:e2ff:fe3a:af69	64	Brez stanja

DNSv6	
Konfiguriral	DHCPv6
Prednostni naslov DNS	
Nadomestni naslov DNS	

Slika 6: Dual Stack nastavitev IPv4 in IPv6 na tiskalniku HP PageWide tPro 477dw

Vir: (Lastni vir)

V spodnji tabeli si oglejmo grobo oceno stroškov za menjavo neustrezne opreme prehoda iz IPv4 na IPv6.

Tabela 3: Ocena stroškov prehoda iz IPv4 na IPv6

Naziv opreme	**EM**	**MPC**
Omrežna stikala	3	960 €
Cisco usmerjevalnik	1	2.000 €

Vir: (Lastni vir)

Ostala oprema, kot so stacionarni računalniki, prenosniki in obstoječi brezžični usmerjevalniki, so za prehod iz IPv4 na IPv6 primerni.

1.14 Ugotovitve

Sam prehod iz IPv4 na IPv6 na šoli ne bi smel predstavljati večjih težav. Največjo težavo vidim predvsem v ohranitvi stanja, kakršno je sedaj in da se delni prehod na IPv6 ne bi preveč čutil v samem procesu dela na šoli. Preden se protokol IPv4 povsem umakne iz učilnic, zbornice in upravnih prostorov, bo preteklo še kar nekaj časa, je pa vsekakor to eden izmed večjih izzivov v vsakdanjih opravilih računalničarja na instituciji, kot je osnovna šola. Prehoda iz IPv4 na IPv6 se je potrebno lotiti postopoma in ni izvedljiv iz danes na jutri. Čeprav se tega lotevam zaenkrat le na papirju, se zavedam, da izvedba tega postopka ne bo enostavna in hitra, bo pa zahtevala kar nekaj časa in terjala dolgo uvajanje uporabnikov.

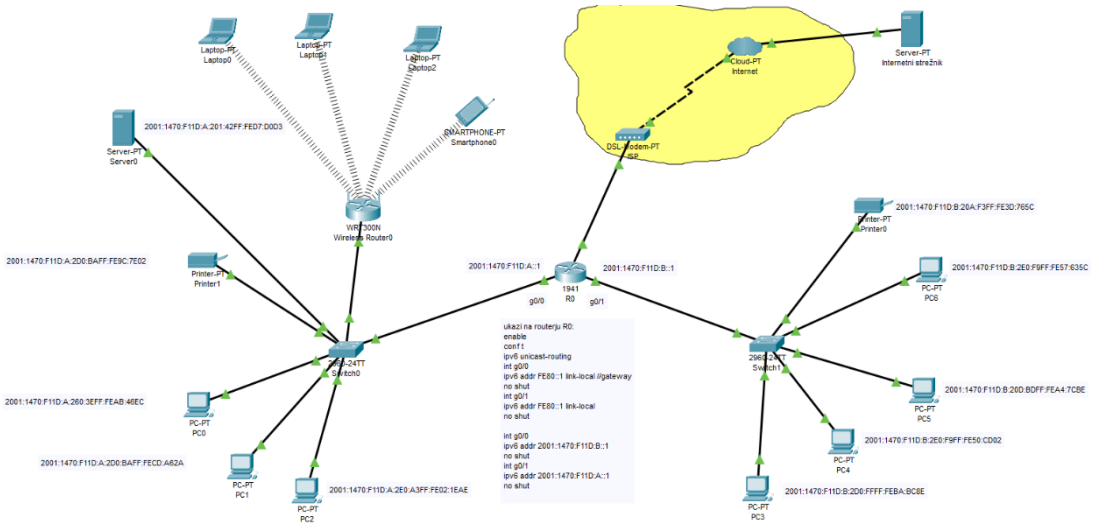
4. SIMULACIJA OMREŽJA

Simulacijo omrežja IPv6 sem pripravil s pomočjo orodja Cisco Packed Tracer, verzija 8.

Orodje Packed Tracer je orodje za vizualno simulacijo na več platformah, zasnovan s Cisco Systems, ki uporabnikom omogoča ustvarjanje omrežnih topologij in posnemanje sodobnih računalniških omrežij. Osnovna različica programa verzije 5 je na voljo brezplačno, kasneje si jo lahko nadgradimo na novejše verzije, če se registriramo in vpišemo v uporabniški vmesnik ob zagonu programa.

1.15 Topologija

Topologija omrežja je v obliki zvezde, ki je sestavljeno iz dveh podomrežij, povezanih preko skupnega usmerjevalnika tipa Cisco 1941 z vgrajeno podporo za IPv6. Računalniki obeh podomrežij so neposredno povezani v dve stikali tipa Catalyst 2960 s 24-imi mrežnimi priključki. N spodnji sliki je razviden prikaz topologije, ki sem si jo zamislil kot simulacijo prehoda iz IPv4 na IPv6.



Slika 7: Simulacija IPv6 omrežja v Cisco Packed Tracer-ju

Vir: (Lastni vir)

Tolopogijo zvezde bi bilo potrebno glede na velikost obstoječega omrežja razširiti oz. zavarovati z vsaj še enim stikalom za vsako podomrežje.

1.16 Konfiguracija omrežja

Simulacija omrežja vsebuje dve fizično ločeni podomrežji A in B, povezani preko skupnega usmerjevalnika, ki je hkrati tudi prehod za obe podomrežji in zagotavlja samodejno unikatno dodeljevanje (ang. unicast) IPv6 naslovov za vse priključene naprave od osebnih računalnikov, prenosnikov, omrežnih tiskalnikov do mobilnih naprav. Podomrežje A je na usmerjevalnik povezano preko hitrega gigabitnega priključka g0/0, na katerem je nastavljeno samodejno dodeljevanje IPv6 naslovov s predpono 2001:1470:F11D:A in se konča s povezanim lokalnim naslovom naprave.

V tabeli 2 je prikazano, kako so dejansko povezane posamezne naprave v omrežje.

Tabela 4: Povezava omrežnih naprav v Cisco Packed Tracer-ju

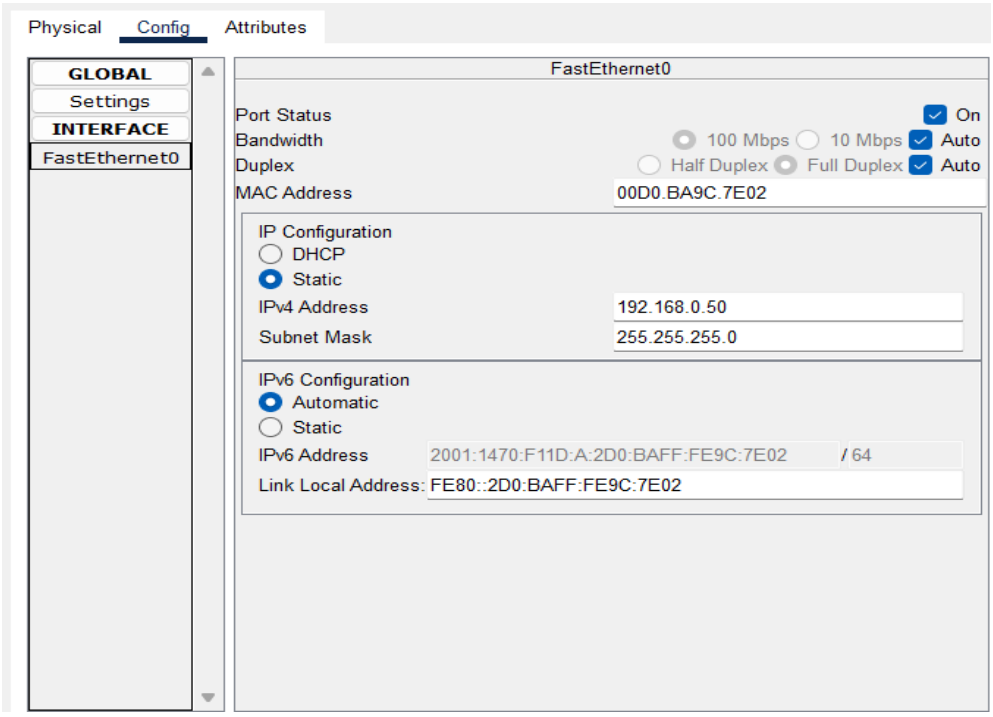
Naprava	**vmesnik**	**Naslov/predpona IPv6**	**Privzeti prehod**
usmerjevalnik R0	g0/0	2001::1470:F11D:A:1:1::1/64	FE80::1
	g0/1	2001:1470:F!1D:B:1:1::11/64	FE80::1
	console	DSL modem	NA
stikaloS0	g0/1	NA	FE80::1
	fa0/1	2001:1470:F11D:A:260:3EFF:FEAB:46EC/64	FE80::1
	fa0/2	2001:1470:F11D:A:2E0:A3FF:FE02:1EAE/64	FE80::1
	fa0/3	2001:1470:F11D:A:260:3EFF:FEAB:46EC/64	FE80::1
	fa0/4	2001:1470:F11D:A:201:42FF:FED7:D0D3/64	FE80::1

	fa0/5	2001:1470:F11D:A:2D0:BAFF:FE9C:7E02/64	FE80::1
	fa0/6	Brezžični usmerjevalnik	FE80::1
stikaloS1	g0/1	NA	FE80::1
	fa0/1	2001:1470:F11D:B:20A:F3FF:FE3D:765C/64	FE80::1
	fa0/2	NA	FE80::1
	fa0/3	2001:1470:F11D:B:2D0:FFFF:FEBA:BC8E/64	FE80::1
	fa0/4	2001:1470:F11D:B:2E0:F9FF:FE50:CD02/64	FE80::1
	fa0/5	2001:1470:F11D:B:20D:BDFF:FEA4:7CBE/64	FE80::1
	fa0/6	2001:1470:F11D:B:2E0:F9FF:FE57:635C/64	FE80::1

Vir: (Lastni vir)

Za ostale omrežne naprave, predvsem računalnike, je na stikalih še dovolj prostora, omrežje pa je zasnovano tako, da se z dodajanjem stikal razširi in tako pokrije celotno potrebo po zaključenem omrežju.

Na sliki 8 je prikazan IPv6 konfiguracijski del omrežnega tiskalnika.



Slika 8: Primer samodejne konfiguracije IPv6 naslova omrežnega tiskalnika

Vir:(Lastni vir)

IPv6 naslovi naprav v omrežju se vsi začnejo z isto IPv6 predpono in jo v našem primeru določi ponudnik internetnih storitev, to je Arnes.

Drugi – gostiteljski del IPv6 se generira s pomočjo unikatnega 48-bitnega naslova MAC omrežne kartice, v katerega se v sredino naslova vstavi šestnajstiška vrednost FF:FE.

Nastavitev samodejnega naslavljanja naprav v IPv6 omrežju je nastavljeno na samem usmerjevalniku na obeh gigabitnih priključkih usmerjevalnika.

Podomrežje A je dodatno konfigurirano kot Dual Stack, kar pomeni, da imajo vse omrežne naprave nastavljen tako IPv6, kot tudi IPv4 omrežni naslov. Podomrežje B je konfigurirano kot izključno IPv6.

Usmerjevalnik je konfiguriran kot IPv6 unicast usmerjevalnik, kar pomeni, da je omogočen dostop naprav iz omrežja A do naprav iz omrežja B in obratno. V praksi to opišemo kot možnost, da lahko uporabnik iz omrežja A tiska tako na tiskalnik iz omrežja A kot tudi na tiskalnik iz omrežja B oziroma obratno. V samem procesu dela se slednje pokaže kot zelo koristna rešitev, sploh v primeru izpadov omrežja ali naprav v omrežju.

1.17 Prikaz delovanja omrežja

Naprave omrežja A med seboj komunicirajo tako preko protokola IPv6, kot tudi protokola IPv4.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time<1ms TTL=128
Reply from 192.168.0.50: bytes=32 time<1ms TTL=128
Reply from 192.168.0.50: bytes=32 time<1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 9: Zakasnitev (ping) po IPv4 znotraj podomrežja A

Vir: (Lastni vir)

```
Pinging 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02 with 32 bytes of data:

Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=128
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=128
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=128
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=128

Ping statistics for 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Slika 10: Zakasnitev (ping) po IPv6 znotraj podomrežja A

Vir: (Lastni vir)

```
Pinging 2001:1470:f11d:B:20a:f3ff:fe3d:765c with 32 bytes of data:

Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time=1ms TTL=127

Ping statistics for 2001:1470:F11D:B:20A:F3FF:FE3D:765C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 11: Zakasnitev (ping) po IPv6 iz omrežja A v omrežje B

Vir: (Lastni vir)

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:1470:f11d:B:20a:f3ff:fe3d:765c

Pinging 2001:1470:f11d:B:20a:f3ff:fe3d:765c with 32 bytes of data:

Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=128
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time=1ms TTL=128
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=128
Reply from 2001:1470:F11D:B:20A:F3FF:FE3D:765C: bytes=32 time<1ms TTL=128

Ping statistics for 2001:1470:F11D:B:20A:F3FF:FE3D:765C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Slika 12: Zakasnitev (ping) po IPv6 znotraj omrežja B

Vir: (Lastni vir)

```
C:\>ping 2001:1470:f11d:a:2d0:baff:fe9c:7e02

Pinging 2001:1470:f11d:a:2d0:baff:fe9c:7e02 with 32 bytes of data:

Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=127
Reply from 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02: bytes=32 time<1ms TTL=127

Ping statistics for 2001:1470:F11D:A:2D0:BAFF:FE9C:7E02:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Slika 13: Zakasnitev (ping) po IPv6 iz omrežja B v omrežje A

Vir: (Lastni vir)

5. SKLEP

Vprašanje, kako in zakaj se lotiti prehoda iz internetnega protokola IPv4 na protokol IPv6, se je ravno v času Covid-19 epidemije in razcvetu interneta, internetne prodaje, skratka vsega v povezavi z internetom, verjetno večkrat kot kadar koli prej postavilo na dnevnem redu kakega sestanka znotraj večjih organizacij ali podjetij. Internet približati končnim uporabnikom, je prav zato zelo povezano z dodeljevanjem IP oz. internetnih naslovov. Za zagotavljanje boljše in učinkovitejše povezljivosti, nam bo ravno novejši in boljši protokol IPv6 omogočal povezovanje v internet za vse pametne in manj pametne naprave.

Med pisanjem diplomskega dela sem spoznal, da se sam prehod iz starejšega IPv4 na novejši IPv6 ne bo zgodil iz danes na jutri, da je IPv6 že pripravljen, da prevzame svojo vladavino nad internetom, nismo pa še popolnoma pripravljeni vsi uporabniki interneta. Načinov, kako to čim hitreje in najmanj boleče izvesti, je več in katerega kot sistemski inženir v neki organizaciji oz. podjetju izbrati, bo le stvar dogovora in stroškov menjave. Vsekakor bo potrebno v večini podjetij zamenjati določeno mrežno opremo, ki ne podpira novejšega IPv6 ali pa ga le delno podpira.

Predlog za vse, ki oklevajo, kdaj in kako pričeti s tranzicijo je, da najprej premislijo, koliko so pripravljeni investirati v napredek in omogočiti svojim zaposlenim, strankam, uporabnikom boljši in hitrejši internet, boljši in bolj varen dostop do svojih spletnih storitev, hitrejše in bolj zanesljivo povezovanje med sedežem podjetja in zunanjimi enotami in še kaj bi se našlo. Zato predlagam, da se pripravimo koliko dobro se le da, izdela se izračun stroškov in se loti prehoda mogoče ob koncu šolskega leta, v času poletnih počitnic. Napredek ne bo čakal na nas in na naše podjetje, lahko pa se zgodi, da nas bo že konec tega leta 2023 enostavno prisilil v menjavo.

H1: Menjava iz protokola IPv4 na protokol IPv6 je neizogibna. Hipoteza je potrjena, saj je za vse nove naprave v internetu že zmanjkalo IPv4 internetnih naslovov ali pa so neizkoriščeni IPv4 naslovi že rezervirani s strani organizacij in podjetij, dejansko pa niso v uporabi.
H2: Protokol IPv6 je hitrejši od protokola IPv4. Hipoteza je potrjena, že zaradi samega zapisa IPv6, ki ima štirikrat večje razširjene glave kot naslovi IPv4. Ta dodana funkcija v naslovu IPv6 pomaga zmanjšati stroške obdelave paketov in pasovne širine glave, zaradi česar je povezava veliko hitrejša. **H3: Protokol IPv6 je varnejši od protokola IPv4.**
Hipoteza je potrjena, saj je protokol IPv6 varnejši za ločevanje imen. Protokol SEND (ang. Secure Neighbor Discovery) omogoča kriptografsko potrditev identitete gostitelja ob povezavi,

kar oteži napade na podlagi poimenovanja. To ni nadomestilo za preverjanje na ravni aplikacije ali storitve, ampak nudi dodatno varnost.

H4: Protokol IPv6 ima več prednosti napram protokolu IPv4. Hipoteza je potrjena, saj že iz same definicije IPv6 protokola izhaja dejstvo, da ima protokol IPv4 manj prednosti kot IPv6.

H5: Protokol IPv6 omogoča povezovanje več naprav v internetu. Hipoteza je potrjena, saj protokol IPv6 že zaradi oblike zapisa omogoča unikatni zapis za 340 bilijonov bilijonov bilijonov internetnih naslovov. **H6: Omrežja IPv6 so preglednejša in hitrejša.** Hipoteza je delno potrjena. Z vidika preglednosti so Ipv6 naslovi težje zapomnljivi in si manj logično sledijo znotraj nekega omrežja. V unicast načinu IPv6 naslavljanja ima vsaka naprava v svojem dodeljenem IPv6 naslovu del svojega MAC naslova, kar je z vidika hitrosti in sledljivosti dobro, z vidika preglednosti pa mogoče ne preveč.

Pri IPv6 ima zaradi zadostne količine IP naslovov vsaka omrežna naprava svoj unikatni naslov, s katerim se predstavi v internetu in ni več potrebe, da so take naprave »skrite« znotraj lokalnih omrežij. Ravno zaradi teh unikatnih IP naslovov, je delovanje naprav znotraj interneta hitrejše, saj ni več potrebe po lokalnih omrežjih in DNS posredniških storitvah naslavljanja.

6. VIRI IN LITERATURA

Arnes. (2020). *http://arnes.splet.arnes.si/*. Pridobljeno iz http://arnes.splet.arnes.si/: http://arnes.splet.arnes.si/storitve/omrezne-storitve/ip-povezljivost/ipv6/vec-o-ipv6/translacijski-mehanizmi-med-ipv4-in-ipv6/

Avsystem. (2021). *https://www.avsystem.com*. Pridobljeno iz https://www.avsystem.com: https://www.avsystem.com/blog/ipv6/

Avsystems. (2021). *https://www.avsystem.com*. Pridobljeno iz https://www.avsystem.com: https://www.avsystem.com/blog/IPv4/

Bajrami, V. (september 2019). *https://www.redhat.com/sysadmin/ipv6-packets-and-ipsec*. Pridobljeno iz https://www.redhat.com/sysadmin/ipv6-packets-and-ipsec: https://www.redhat.com/sysadmin/ipv6-packets-and-ipsec

Balchunas, A. (2006). *IPv6 Addressing.*

Brglez, D. (2018). *Računalniške komunikacije in omrežja 1.*

CiscoPress. (2000). *Internet Routing Architectures, second edition, str. 57.*

CiscoPress. (2017). *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, 2nd Edition.*

Eduroam. (2022). *https://eduroam.org/*. Pridobljeno iz https://eduroam.org/: https://eduroam.org/about/connect-yourself/

GeeksForGeeks. (2020). *https://www.geeksforgeeks.org/*. Pridobljeno iz https://www.geeksforgeeks.org/: https://www.geeksforgeeks.org/tcp-ip-model/

IPv6.si. (2021). *https://ipv6.si/*. Pridobljeno iz https://ipv6.si/: https://ipv6.si/protokol-ipv6/podporni-nadzorni-protokoli/

IPv6.si. (2022). *https://ipv6.si/*. Pridobljeno iz https://ipv6.si/: https://ipv6.si/priprava-na-uvedbo-ipv6/nacrt-prehoda-na-ipv6/

Lifewire. (december 2022). *https://www.lifewire.com/*. Pridobljeno iz https://www.lifewire.com/: https://www.lifewire.com/what-happened-to-ipv5-3971327

Prefixx. (februar 2021). *https://prefixx.net/*. Pridobljeno iz https://prefixx.net/: https://prefixx.net/news/ipv4-to-ipv6-tunneling

Setra-Brumley. (april 2022). *https://www.setra.com/*. Pridobljeno iz https://www.setra.com/: https://www.setra.com/blog/ipsec-for-ipv6-is-it-more-secure-than-ipv4

TechRadar. (25. november 2021). *https://www.techradar.com*. Pridobljeno iz https://www.techradar.com: https://www.techradar.com/news/the-environmental-opportunity-of-unused-ipv4s