INSTITUT
za razvoj i istraživanja
u oblasti zaštite na radu

Podgorica

Broj: _____

Datum, _____

# STUDIJA
# Plan migracije na protokol IPv6 u Crnoj Gori

---

***Podgorica, januar 2019. godine***

# INSTITUT ZA RAZVOJ I ISTRAŽIVANJA U OBLASTI ZAŠTITE NA RADU

# STUDIJA

## PLAN MIGRACIJE NA PROTOKOL IPv6 U CRNOJ GORI

Investitor: Agencija za elektronske komunikacije i poštansku djelatnost

Ugovor broj: 01-1182 od 27.09.2018. god.


Projektni tim:

1. *Prof. dr Božo Krstajić,*
2. *Prof. dr Milica Pejanović-Đurišić,*
3. *Prof. dr Zoran Veljović,*
4. *Prof. dr Milutin Radonjić,*
5. *Aleksandra Radulović, Spec. App.*


**DIREKTOR,**

**mr Branimir Ćulafić**

**Projektni zadatak**

Projektni zadatak za izradu plana migracije na protokol IPv6 u Crnoj Gori definisan je Pozivom za javnu nabavku broj 0102-2296/6 od 15.06.2018. god., na stranama 7-9. Projektni zadatak obuhvata Tehničke karakteristike i specifikacije kako slijedi.

**Tehničke karakteristike i specifikacije predmeta javne nabavke**

U cilju prevazilaženja problema nedostatka Internet adresa razvijen je Internet protokol nove generacije, poznatiji kao IPv6. Prednosti novog protokola su, pored proširenja adresnog prostora, povećana efikasnost, sigurnost i mogućnost implementacija savremenih IoT rješenja. Ovaj protokol je preduslov za razvoj budućih Internet servisa i osnov za uključivanje u globalno elektronsko tržište.

Imajući u vidu porast broja korisnika elektronskih komunikacionih usluga, da elektronske komunikacione usluge operatori skoro u potpunosti baziraju na IP platformama, sljedeći logičan korak u razvoju elektronskih komunikacionih mreža i usluga je implementacija IPv6 protokola. Zbog toga je potrebno pripremiti plan migracije na protokol IPv6, u skladu sa standardima, odlukama i preporukama nadležnih evropskih i međunarodnih tijela.

| **Redni broj** | **Opis predmeta nabavke, odnosno dijela predmeta nabavke** | **Bitne karakteristike predmeta nabavke u pogledu kvaliteta, performansi i/ili dimenzija** | **Jedinica mjere** | **Količina** |
|---|---|---|---|---|
| | Usluga izrade Plana migracije na protokol IPv6 | Plan treba da u posebnim poglavljima obuhvati sljedeće:<br>**1. Razlozi/motivi implementacije IPv6- prednosti i izazovi**<br>- Karakteristike IPv4;<br>- Karakteristike IPv6;<br>- Prednosti IPv6 u odnosu na IPv4;<br>**2. Analiza postojećeg stanja implementacije IPv6 u Crnoj Gori i postojeći izazovi;**<br>- Implementacija IPv6 u mrežama javnih elektronskih komunikacionih operatora, državnim institucijama i u kompanijama na dan 31.05.2018.;<br>- Stanje dodjele IPv6 adresa u Crnoj Gori na dan 31.05.2018.;<br>- Stanje razvoja i dostupnosti Crnogorskih *website*-ova preko IPv6; | | |

| | | | | |
|---|---|---|---|---|
| 1. | | **3. Analiza potencijalnih metoda implementacije IPv6 - prednosti i nedostaci**<br>- Dvostruka konfiguracija (*Dual stack*);<br>- Tunelovanje (*Tunneling*);<br>- Translacija protokola (*Protocol translation*).<br>**4. Izazovi implementacije IPv6 koji se odnose na sigurnost i privatnost**<br>- Procjena sigurnosti i privatnosti koje se odnose na korisnike i preduzeća implementacijom IPv6;<br>- Procjena uticaja implementacije IPv6 na obaveze operatora javnih elektronskih komunikacionih mreža i usluga koje se odnose na njihove obaveze u vezi propisa o zaštiti podataka o ličnosti;<br>- Procjena uticaja implementacije IPv6 na blokiranje *website*-ova koje se odnosi na zaštitu intelektualne svojine i blokiranje koje se odnosi na zaštitu djece;<br>**5. Pregled iskustava u implementaciji IPv6 u najrazvijenim državama EU i u nekim državama iz ostatka svijeta**<br>- Napredne države EU;<br>- SAD;<br>- Napredne države Azije.<br>**6. Analiza scenarija za implementaciju IPv6 u Crnoj Gori, sa tehničkog i ekonomskog aspekta (posebno za privatni i javni sektor)**<br>- Operatori javnih elektronskih komunikacionih mreža i usluga (ISP);<br>- Provajderi sadržaja i aplikacija;<br>- Poslovni korisnici;<br>- Rezidencijalni korisnici;<br>- Provajderi hardvera i softvera;<br>- Sistem integratori; | Komplet | 1 |

| | | | | |
|---|---|---|---|---|
| | | - Državne institucije.<br>**7. Preporuke za implementaciju IPv6 u javnim ustanovama u Crnoj Gori**<br>- Metodi implementacije IPv6;<br>- Struktura mreže i adresiranje uređaja;<br>- Komponente koje se odnose na sigurnost;<br>- Upravljanje i nadzor mreže;<br>- Infrastrukturni servisi;<br>- Detaljne preporuke u obliku *Chek* - liste prilikom implementacije IPv6;<br>- Podizanje svijesti operatora javnih elektronskih komunikacionih mreža i usluga (ISP);<br>- Podizanje svijesti poslovnih korisnika;<br>- Podizanje svijesti u državnim i lokalnim institucijama;<br>- Predlozi za podizanje svijesti u budućnosti.<br>**8. Detaljan plan implementacije IPv6 u jednoj javnoj ustanovi (Ministarstvu, UCG)**<br>- Tranzicija bazičnih infrastrukturnih komponenti;<br>- Tranzicija servera i servisa;<br>- Definisanje protokola za rutiranje;<br>- Definisanje protokola za upravljanje i monitoring mreže;<br>- Mogućnosti integracije postojećih IPv4 komponenti. | | |

# Sadržaj

# 1. Predgovor

IPv6 je nova verzija IP protokola kreirana da zamijeni IPv4 verziju, čiji dizajn se nije bitno promijenio još od svog definisanja 1981. godine. Dizajn IPv4 protokola nije predvidio okolnosti koje su se pojavile ekspanzijom i popularnošću Interneta i računarsko-komunikacionih tehnologija. To se, prije svega, ogleda u nedostatku adresnog prostora, veličini tabela rutiranja, sigurnosnim izazovima, raznorodnim mrežnim čvorovima, itd. Iako nova verzija protokola rješava sve nedostatke prethodne verzije i pruža mogućnost razvoja novih servisa i potpune digitalizacije društva, proces migracije na IPv6 je spor i ne nazire se datum potpune zamjene stare verzije. No, implementacija IPv6 protokola je neminovnost koja implicira potrebu definisanja neophodnih planova i aktivnosti relevatnih subjekata na pripremi ICT infrastrukture za taj trenutak, čime će se i omogućiti potpuni nestanak IPv4 verzije u budućnosti. Zbog toga je neophodno da se na nacionalnim nivoima definišu planovi migracije na IPv6 protokol.

Za potrebe izrade Plana migracije na protokol IPv6 u Crnoj Gori, Agencija za elektronske komunikacije i poštansku djelatnost je, putem javnog tendera, angažovala Institut za razvoj i istraživanja u oblasti zaštite na radu u Podgorici. U tu svrhu su Institut za razvoj i istraživanja u oblasti zaštite na radu i Agencija za elektronske komunikacije i poštansku djelatnost sklopili ugovor dana 27.09.2018. godine. Ugovorom se Institut za razvoj i istraživanja u oblasti zaštite na radu obavezao da će izvršiti izradu Plana migracije na protokol IPv6 u Crnoj Gori, u kome će se nalaziti:

- Razlozi /motivi implementacije IPv6 - prednosti i izazovi;
- Analiza postojećeg stanja implementacije IPv6 u Crnoj Gori i postojeći izazovi;
- Analiza potencijalnih metoda implementacije IPv6 - prednosti i nedostaci;
- Izazovi implementacije IPv6 koji se odnose na sigurnost i privatnost;
- Pregled iskustava u implementaciji IPv6 u najrazvijenim državama EU i u nekim državama iz ostatka svijeta;
- Analiza scenarija za implementaciju IPv6 u Crnoj Gori, sa tehničkog i ekonomskog aspekta (posebno za privatni i javni sektor);
- Preporuke za implementaciju IPv6 u javnim ustanovama u Crnoj Gori;
- Detaljan plan implementacije IPv6 u jednoj javnoj ustanovi (Ministarstvu, UCG);

Stručni tim angažovan od strane Instituta za razvoj i istraživanja u oblasti zaštite na radu je, shodno navedenoj literaturi, analiziranim primjerima, sopstvenom višegodišnjem iskustvu i konsultacijama sa relevantnim ekspertima iz oblasti mrežnih tehnologija i Interneta predložio Plan migracije na protokol IPv6 u Crnoj Gori sa svim, Ugovorom predviđenim, elementima.

# 2. Razlozi/motivi implementacije IPv6 - prednosti i izazovi

Od početaka vezanih za potrebe komunikacije u vojno-istraživačkom okruženju, razvoj Interneta kao mreže svih mreža doveo je do kreiranja virtuelnog univerzuma koji prevazilazi fizičke, političke i socijalne granice, čime se praktično realizuje paradigma modernih komunikacija zasnovana na potpunoj globalizaciji.

Tokom proteklih decenija Internet je evoluirao iz statičkog repozitorijuma međusobno povezanih hipertekstualnih dokumenata ka dinamičnom univerzumu umreženih ljudi, mašina, stvari i aplikacija. Takav razvoj je dominantno bio uslovljen ispunjavanjem zahtijeva za povećanjem obima saobraćaja u digitalno povezanom svijetu, kao i potrebom stvaranja uslova za pružanje kvalitetnijih, sveobuhvatnijih interaktivnih servisa i aplikacija za krajnje korisnike. Trenutno se može govoriti o narednoj fazi promjena koje su omogućene prije svega punom konvergencijom tehnoloških oblasti tipa: *Big Data, Internet of Things, Blockchain, Machine Learning i Artificial Intelligence*, i koje dovode do suštinskog zaokreta i transformisanja postojećih društvenih, političkih i ekonomskih normi, kreirajući prilike i izazove: **za svakog pojedinca, na svakom mjestu i u svakom trenutku.**

U tom kontekstu, transformacija se odvija u dva ključna pravca. Prvo, telekomunikacione mreže pete generacije (5G) predstavljaju prelaz sa tradicionalnih hardverskih mreža na novu paradigmu virtuelnih mreža i mreža zasnovanih na softverski definisanom umrežavanju (*Software Defined Networking - SDN*) i virtuelizaciji mrežnih funkcija (*Network Function Virtualization - NFV*). Drugo, najveći broj aktuelnih Internet servisa podrazumijeva zamjenu tradicionalnih monolitnih klijent-server modela modularnom i distribuiranom paradigmom koja koristi potencijale *Cloud/Fog* okruženja.

Navedeni pravci ukupne digitalne transformacije omogućavaju realizaciju ambiciozne misije razvijanja nove ere umrežavanja i ostvarivanja servisa putem Interneta obezbeđujući:

1. naprednije korišćenje resursa i njihovo dijeljenje, posebno kad je u pitanju skladištenje, obrada i umrežavanje;
2. holističku mrežnu analizu, koordinaciju i optimizaciju i
3. inovativne poslovne modele i mogućnosti preduzetništva u uslovima pune sinergije sektora informacionih tehnologija i telekomunikacija, kao i segmenata mnogih drugih naučnih i stručnih disciplina.

Pri tome, upravo opisana digitalna transformacija informaciono-komunikacionog okruženja predstavlja glavni tehničko-tehnološki izazov u daljem razvoju i implementaciji koncepta Internet-baziranih mreža i njima podržanih servisa i aplikacija. U tom smislu, izazovi su i prepoznati u Strategiji razvoja informacionog društva Crne Gore do 2020, koju je Vlada Crne Gore usvojila 2016. godine, gdje je posebno naglašeno da dalja digitalna transformacija u osnovi zavisi od ispunjavanja dva ključna uslova: ostvarivanja intenzivnog razvoja širokopojasnog pristupa Internetu i poboljšanja odgovarajuće infrastrukture, kako fiksne tako i bežične [1].

Konkretno i praktično, opisani koncept digitalne transformacije u dva tehnološka pravca se svodi na stvaranje uslova za umrežavanje ogromnog broja heterogenih uređaja različitih funkcija, čime se realizuje IoT mrežna arhitektura. Cilj takvog međusobnog povezivanja svakodnevnih objekata u ekosistemu pametnih aplikacija i usluga je poboljšanje i pojednostavljenje života svakog pojedinca na globalnom nivou. U stvari, IoT se zasniva na viziji u kojoj se Internet proširuje u realni svijet koji obuhvata svakodnevne predmete. Fizički predmeti više nisu isključeni iz virtuelnog svijeta, već se mogu kontrolisati odvojeno i dobijaju ulogu fizičkih pristupnih tačaka Internet uslugama. Ovakva IoT vizija polazi od uvjerenja da će se postojeći konstantan napredak u mikroelektronici, komunikacijama i informacionoj tehnologiji nastaviti i u doglednoj budućnosti.

U pitanju je koncept koji je posebno dobio na značaju poslednjih godina sa pojavom brojnih aplikacija i servisa u različitim domenima (saobraćaj, poljoprivreda, medicina, obrazovanje…) i kojim se faktički, povezivanjem proizvoljnog broja uređaja ili njihovih klastera, realizuje globalna transformacija u pravcu naredne generacije Internet-baziranih komunikacionih mreža (*Future Internet*, *Next Generation Internet*). Prema prognozama, do 2020. godine Internet će obuhvatiti preko 30 milijardi heterogenih uređaja povezanih u okviru IoT globalnog ekosistema [IoT Lab, FP7 *European Research project on IoT and Crowdsourcing*].

I kao što se Internet, i na njemu zasnovani servisi i aplikacije, razvio do neočekivanih razmjera, tako su evoluirale i norme kojima se definiše njegovo efikasno funkcionisanje. U odnosu na početke kada se smatralo da bilo kakva forma regulative, vezane za Internet, može predstavljati barijeru u razvoju i zadržavanje pristupa karakterističnog za tradicionalne komunikacione mreže, danas postoji čitav niz međunarodnih organizacija i tijela koje su zadužene upravo za donošenje i usaglašavanje standarda i preporuka za mrežu svih mreža (*Internet Engineering Task Force* – IETF; *Internet Society* – ISOC; *International Telecommuniction Union* – ITU; *International Organization for Standardization* - ISO; *Réseaux Internet Protocol Européens* - RIPE; …).

Potreba za njihovim angažmanom je utoliko veća ako se ima u vidu navedena činjenica da savremena telekomunikaciona infrastruktura bazirana na Internetu predstavlja globalni sistem kojim se povezuju fizički i digitalni objekti, uz stvaranje mogućnosti interakcija, kako objekat-objekat, tako i onih između objekata i tradicionalnih korisnika. U najopštijem slučaju, aktuelni pravac razvoja Interneta u IoT konceptu podrazumijeva omogućavanje komunikacije za ogroman broj heterogenih korisnika i uređaja, uz podršku značajno većem obimu saobraćaja, kao i ostvarivanje odgovarajućih nivoa kvaliteta servisa i pouzdanosti, energetske i spektralne efikasnosti.

Razvoj i selekcija odgovarajućih standarda kojima se definišu elementi referentnog modela takvih mreža predstavljaju uslov njihove uspješne implementacije. U tom smislu, glavni fokus je na mrežnom nivou (*Network Layer*) OSI (*Open System Interconnection*) referentnog modela Internet-baziranih mreža gdje se specificira odgovarajući Internet protokol (IP), kojim se opisuje ukupna procedura komunikacije, tj. slanja podataka u okviru mreže.

U pitanju je ne-konektivni protokol čija je glavna karakteristika u činjenici da se ne uspostavlja kontinuirana veza između krajnjih tačaka (mrežnih čvorova) koje komuniciraju.

Poruka se enkapsulira u jedan ili više paketa, a svaki paket koji se prenosi Internet mrežom tretira se potpuno nezavisno, i ni na koji način nije povezan sa ostalim paketima koji se takođe prenose istom mrežom. Uspostavljanje adekvatnog redoslijeda u slanju djelova poruke postiže se implementacijom dodatnog protokola na višem nivou, na primjer TCP (*Transmission Control Protocol*) protokola, koji kao konektivni protokol definiše način na koji se ostvaruje očuvanje originalne poruke u uslovima mogućih gubitaka pojedinih paketa ili duplikata na prijemu. Pri tome, svakom mrežnom interfejsu (WiFi, *Ethernet*) koji pripada jednom čvoru (računar, senzor, mjerni uređaj, …) se dodjeljuje najmanje jedna IP adresa, odnosno jedinstven identifikator koji ima dvije osnovne namjene: da identifikuje mrežni čvor i da definiše njegovu lokaciju.

Razvoj komunikacionih mreža odvija se u pravcu potpunog usvajanja Internet protokola, odnosno korišćenja Internet protokola na mrežnom nivou njihove referentne arhitekture. To navodi na zaključak da je za njihovu dalju transformaciju uslovljenu 5G tehnologijom i IoT paradigmom neophodno obezbijediti potrebne resurse upravo na nivou IP mrežnog protokola.

## 2.1. IP mrežna arhitektura

U okviru Međunarodne organizacije za standarde (*International Standardization Organization* - ISO) definisan je opšti model komunikacionih sistema poznat kao OSI (*Open System Interconnection*) model. Riječ je o slojevitom modelu kojim se specificira način komunikacije između mreža, korišćenjem različitih protokola datih za svaki od sedam nivoa pojedinačno (Fizički nivo, Nivo veze, Mrežni nivo, Transportni nivo, Nivo sesije, Nivo prezentacije i Nivo aplikacije). Pri tome se svakom nivou precizno dodjeljuje tačno određeni zadatak u okviru komunikacionog sistema. Na primjer, fizički nivo definiše sve komponente fizičke prirode u komunikacionoj mreži, tj. prenosne puteve, frekvencije, kodove, modulacije itd. Mrežni nivo je odgovoran za prenos podataka od jednog mrežnog čvorišta do drugog. Pri tome, na ovom nivou se definiše postupak dodjeljivanja logičkih adresa i njihove (jedinstvene) identifikacije, kao i putanja kojom se paketi usmjeravaju kako bi stigli do odredišta.

Savremene komunikacione mreže zasnovane na Internetu koriste *Internet Protocol Suite* referentni model, koji je kombinacija niza pojedinačnih protokola za različite svrhe i potrebe. Pošto su dva glavna protokola u ovom modelu TCP (*Transmission Control Protocol*) i IP (*Internet Protocol*), obično se koristi skraćenica TCP/IP za njegovo označavanje. Za razliku od OSI referentnog modela, TCP/IP model sadrži manje nivoa, ukupno četiri (Nivo veze, Internet nivo, Transportni nivo i Nivo aplikacije).

Izostavljanje fizičkog nivoa ukazuje da je u pitanju model koji je potpuno neutralan u odnosu na prirodu umrežene opreme, i kao takav se može implementirati za komunikaciju na gotovo svim prenosnim putevima (žičnim, bežičnim). Transportni i Internet nivoi su u korespondenciji sa odgovarajućim slojevima OSI modela, dok su tri gornja nivoa OSI modela komprimovana u Nivo aplikacije TCP/IP modela.

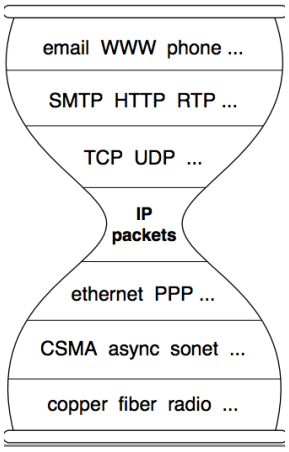
Internet protokol je jedan od glavnih protokola u okviru TCP/IP modela. Ovaj protokol odgovara mrežnom nivou OSI modela i Internet nivou TCP/IP modela i kao takav je odgovoran za identifikaciju mrežnih čvorova (*web* server, *smartphone*, *laptop*, *mail* server,

senzor, …) na osnovu njihovih logičkih adresa i za usmjeravanje podataka između njih. Suština je u mehanizmu za jedinstveno identifikovanje putem tzv. šeme IP adresiranja, pri čemu je prenos zasnovan na metodu "*best effort delivery*" koji ne pruža garancije sigurne isporuke prenošenih paketa na odredište (za taj aspekt odgovornost je na višem nivou referentnog modela).

IP (*Internet Protocol*) je veoma fleksibilan protokol, a koncepti komutacije paketa i slojevitosti protokola IP mreža omogućavaju efikasno dijeljenje i iskorišćenje mrežnih resursa. Neki od ključnih aspekata primjene IP protokola u savremenim komunikacionim mrežama heterogene prirode su: rutiranje na mrežnom nivou, prenos korisničkih podataka, kontrola mobilnosti na mrežnom ili višim nivoima, signalizacija i kontrola govornih i multimedijalnih servisa u realnom vremenu i podrška za mrežnu zaštitu i kvalitet servisa.

Takve funkcije Internet protokola, kao faktičke osnove ukupne TCP/IP arhitekture, su prvobitno bile dio TCP protokola razvijenog kao prethodnica modernog Interneta 1970-tih godina. IP protokol je formalno etabliran kao poseban protokol kada je ta rana verzija TCP-a podijeljena na TCP na 4. nivou i na IP na 3. nivou referentnog mrežnog modela. U tom smislu, ključna prekretnica je bilo objavljivanje RFC (*Request for Comments*) 791, koji je precizno definisao Internet protokol, septembra 1981 [2]. Ovaj standard, koji je bio revizija sličnog RFC 760 [3] iz prethodne godine, definisao je osnovne funkcije i karakteristike Internet protokola koji je od tada u sve većoj upotrebi. Iako je riječ o prvoj široko korišćenoj verziji Internet protokola, standardom nije označena kao verzija 1, već kao verzija 4 (v4). Razlog tome je upravo odvajanje od tri ranije verzije TCP-a, pa su radi dosljednosti nove verzije i TCP-a i IP-a nakon razdvajanja označene sa v4 [4].

U osnovi Internet dizajna izvršeno je razdvajanje infrastrukture, prenosa i aplikacija. Podaci koje kreira aplikacija moraju da prođu kroz sve slojeve referentnog modela da bi došli do odredišta. Svaki protokol aplikacionog sloja povezan je sa protokolom transportnog sloja, koji stupa u interakciju s IP-om za usmjeravanje paketa podataka. Treba imati u vidu da je, bez obzira na protokole sloja aplikacije i protokole transportnog sloja, IP jedini protokol koji se koristi za usmjeravanje paketa podataka. Kada se prenos podataka vizualizuje, poprima oblik pješčanog sata, pa se odgovarajući model naziva modelom „Internet pješčanog sata" (slika 1).

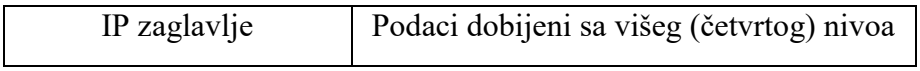



Slika 1. Model „Internet pješčanog sata" (Internet *hourglass*) [5]

Broj i mogućnosti Internet aplikacija doživjeli su još veću ekspanziju, a za očekivati je da se trend njihovog napretka i dalje nastavi. Dok se aplikacije i infrastruktura vremenom šire, prenos i dalje ostaje baziran na IP-u. Prenos je, zahvaljujući ovakvom dizajnu, jasno razdvojena i prepoznatljiva cjelina. I bez obzira koji će se protokol za prenos koristiti (verzija 4 ili verzija 6), to po pravilu neće uticati na aplikacije koje su u ovom modelu prikazane iznad, niti na infrastrukturu koja je prikazana ispod.

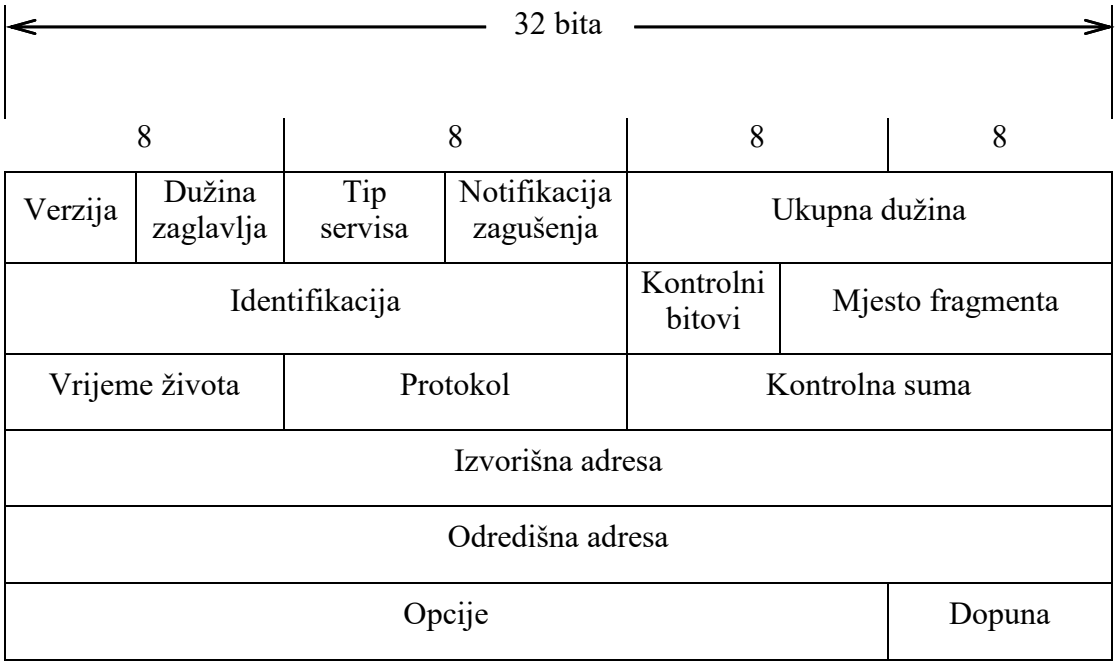
## 2.2. IPv4 protokol

Internet protokol kao protokol 3. nivoa OSI referentnog mrežnog modela uzima segmente podataka od 4. nivoa (transportnog) i dijeli ih u pakete. Tako formirani IP paketi se enkapsuliraju (pakuju) u jedinstvenu strukturu sa IP zaglavljem (slika 2), koje sadrži sve informacije potrebne za isporuku paketa odredišnom čvoru mreže (adresa početnog i odredišnog čvora, mogućnost daljeg dijeljenja u manje segmente, indikacija eventualne greške u prenosu, …).




Slika 2. IP enkapsulirani paket

IP zaglavlje (slika 3) sadrži čitav niz relevantnih informacija sa aspekta prenosa podataka, uključujući i broj verzije protokola koji je u ovom slučaju 4.




Slika 3. IP zaglavlje

Ostali prikazani elementi zaglavlja imaju sledeća značenja:

- Dužina Internet zaglavlja (IHL - *Internet Header Length*);
- Tip servisa (DSCP - *Differentiated Services Code Point*) - koristi se za označavanje prioriteta paketa, pri čemu se nivo prioriteta prikazuje cjelobrojnom vrijednošću od 0 do 7;

- Notifikacija zagušenja (ECN - *Explicit Congestion Notification*) - ukazuje na postojanje zastoja (zagušenja) na transmisionoj putanji;
- Ukupna dužina (TL - *Total Length*) - dužina ukupnog IP paketa;
- Identifikacija (I - *Identifikator*) - ako dođe do fragmentacije IP paketa tokom prenosa, svi fragmenti jednog paketa imaju isti identifikacioni broj;
- Kontrolni bitovi (F - *Flags*) - 3 kontrolna bita za indikaciju mogućnosti fragmentacije paketa. Prvi od 3 bita se koristi za fragmentaciju i defragmentaciju, drugi zabranjuje fragmentaciju ako su to zahtijevi mreže u smislu nepostojanja resursa za defragmentaciju paketa, dok je treći bit uvijek postavljen na '0';
- Mjesto fragmenta (FO - *Fragment Offset*) - za označavanje precizne pozicije fragmenta u okviru originalnog IP paketa;
- Vrijeme života (TTL - *Time To Live*) - da bi se izbjeglo beskonačno kruženje jednog paketa u mreži, TTL vrijednost definiše maksimalan broj čvorišta koji mogu procesuirati paket do njegovog odredišta (tzv. broj skokova jednog paketa). Tokom procesuiranja, svako pojedinačno čvorište (npr. ruter) ovaj broj smanjuje za jedan i u slučaju da vrijednost dostigne nulu, paket se odbacuje;
- Protokol (P - *Protocol*) - služi da mrežni nivo odredišnog čvora informiše o protokolu kome pripada paket (na primjer, za TCP ova oznaka je 6);
- Kontrolna suma zaglavlja (HC - *Header Checksum*) - ovo polje daje tzv. kontrolnu sumu zaglavlja i njegovom verifikacijom na svakom ruteru se provjerava pojava eventualnih grešaka u prenosu ili procesuiranju;
- Izvorišna adresa (SA - *Source Address*) - 32-bitna adresa čvora koji je inicirao prenos paketa;
- Odredišna adresa (DA - *Destination Address*) - 32-bitna adresa odredišnog čvora kome je upućen paket;
- Opcije (O - *Options*) - ovo polje je opciono i koristi se kad je vrijednost Dužine Internet zaglavlja (IHL) veća od 5. Može da sadrži indikacije parametara koji su dodatno specificirani od strane čvora koje je iniciralo prenos.

IPv4 podržava tri različita režima adresiranja:

1. *Unicast* - podaci se šalju samo na jedan određeni čvor, čija se adresa nalazi u DA polju IP zaglavlja;
2. *Broadcast* - paketi podataka se upućuju svim čvorovima u mreži. Saglasno tome, DA polje zaglavlja sadrži posebnu adresu (255.255.255.255);
3. *Multicast* - ovaj režim je kombinacija prethodnih. Paket podataka koji se šalje je namijenjen ne svim, već određenom broju čvorova u mreži. U takvoj situaciji, u DA polju zaglavlja daje se adresa odredišnih čvorova koja počinje sa 224.x.x.x.

U početnoj specifikaciji IPv4, IP adresa se sastojala samo od dva dijela: identifikator mreže je bio najznačajniji oktet adrese, a identifikator čvora mreže je bio ostatak adrese. Takva struktura je omogućavala maksimalno 256 mrežnih identifikatora, što se vrlo brzo pokazalo nedovoljnim. Za prevazilaženje tog ograničenja, standardom iz 1981. godine je redefinisana struktura okteta uvođenjem klasa, odnosno mogućnosti hijerarhijskog adresiranja.

Tako je specificiran IPv4 u formi koja je i danas u upotrebi. Riječ je o hijerarhijskoj adresnoj šemi sa 32-bitnom adresom u IP zaglavlju.

Pojedinačna IP adresa sadrži informaciju o mreži, njenim djelovima (podmrežama) i o čvoru (početnom ili odredišnom). Upravo takva struktura omogućava hijerahijski pristup u kome mreža može imati određeni broj podmreža, koje onda povezuju veći broj čvorova. Takva adresa može biti predstavljena u bilo kojoj notaciji koja izražava 32-bitnu cijelu vrijednost i najčešće se zapisuje u tačka-decimalnom zapisu, koji se sastoji od četiri pojedinačna okteta. Svaki od okteta sadrži po 8 bita, a vrijednost svakog bita je određena njegovom pozicijom u oktetu (standardni metod binarne konverzije u decimalnu), što je ilustrovano na slikama 4 i 5.

| 8 bita | 8 bita | 8 bita | 8 bita |
|---|---|---|---|
| Mreža | Mreža | Podmreža | Čvorište |

Slika 4. Struktura IPv4 adrese

10101100 00010000 11111110 00000001
172 . 16 . 254 . 1

Slika 5. Tačka-decimalni zapis IPv4 adrese

U cilju realizacije hijerarhijskog adresiranja putem identifikacije mreže, podmreža, i na kraju čvorišta, prvim oktetom definiše se jedna od pet klasa (A, B, C, D i E) IP adrese. Klase A, B i C se karakterišu različitim dužinama (brojem bita) kojima se identifikuje mreža, dok ostatak adrese služi za identifikaciju čvora. Na taj način, svaka od ove tri klase ima različit kapacitet u pogledu broja adresa koje se mogu dodijeliti čvorovima u mreži. Klasa D je definisana za *multicast* adresiranje, a klasa E je rezervisana uglavnom za istraživanja i eksperimente.

U principu, 32-bitna IP adresa u svakoj od IP klasa standardno sadrži informacije o čvoru i o mreži kojoj pripada, pri čemu je neophodno njihovo jasno razdvajanje. U tu svrhu svaki od rutera u mreži koristi tzv. masku podmreže (*subnet*), čime se omogućava promjena broja bitova u IP adresi koji služe za identifikaciju čvora, odnosno mreže. Tada nije moguće direktno iz IP adrese odrediti mrežnu adresu, odnosno adresu čvora, već je potrebno znati i masku podmreže, čija je dužina fiksna i iznosi takođe 32 bita.

IP adrese pojedinačnih klasa nisu fleksibilne u smislu podrške manjem broju čvorova po mreži ili većem broju mreža po klasi. Konkretno, broj mreža i broj čvorova po mreži koji se mogu adresirati u okviru pojedinačnih klasa se određuje na sledeći način:

$$\text{Broj mreža} = 2^{\text{broj bitova u adresnom polju mreže}}$$

$$\text{Broj čvorova po mreži} = 2^{\text{broj bitova u adresnom polju čvora}} - 2$$

Karakteristike pojedinačnih klasa IP adresa se mogu sistematizovati na sledeći način:

- Klasa A: Kod IP adrese klase A prvi bit prvog okteta je uvijek 0, tako da se ovaj oktet nalazi u granicama 0-127. Adrese ove klase su od 0.x.x.x do 127.x.x.x, dok je njihova maska podmreže data sa 255.0.0.0. IP opsezi 0.x.x.x i 127.x.x.x su rezervisani za

*broadcast* i *loopback* IP adrese, respektivno. Dakle, sa klasom A IP adresiranja moguće je podržati 128 mreža ($2^7$) i 16777214 čvorova ($2^{24}$-2).

- Klasa B: IP adresa ove klase ima prva dva bita prvog okteta postavljena na 10, tako da ove adrese obuhvataju opseg od 128.0.x.x do 191.255.x.x. Njihova maska podmreže je 255.255.x.x, sa mogućnošću 16384 ($2^{14}$) mrežnih adresa i 65534 ($2^{16}$-2) adresa čvorova.
- Klasa C: Prvi oktet IP adresa klase C ima prva tri bita postavljena na 110, tako da adrese ove klase počinju sa 192.0.0.x i završavaju se sa 223.255.255.x. Njihova maska podmreže je 255.255.255.x, čime je omogućeno 2097152 ($2^{21}$) mrežnih adresa i 254 ($2^8$-2) adresa čvorova.
- Klasa D: Kod klase D IP adresa prva četiri bita prvog okteta adresnog polja su 1110. Ova klasa obuhvata adrese od 224.0.0.0 do 239.255.255.255. S obzirom da je u pitanju klasa namijenjena multicast prenosu, gdje podaci nijesu namijenjeni pojedinačnom čvoru, ne postoji potreba identifikovanja njegove specifične adrese. Saglasno tome, klasa D adresa nema masku podmreže.
- Klasa E: Ova klasa IP adresa je rezervisana za potrebe istraživanja i razvoja i obuhvata adrese od 240.0.0.0 do 255.255.255.254. Kao i kod klase D, ni ovdje ne postoji potreba za maskom podmreže.

U okviru svake od navedenih klasa, postoje i rezervisane IPv4 adrese, za posebne namjene, koje se ne mogu koristiti za pristup globalnom Internetu i koje su uvedene kako bi se bolje iskoristio ukupan adresni prostor koji stoji na raspolaganju kod IPv4 protokola. U pitanju su tzv. privatne IP adrese koje se ne rutiraju, tako da ruteri automatski odbacuju pakete podataka koji ih sadrže. Skup takvih adresa po pojedinim klasama je definisan na sledeći način:

- klase A: 10.0.0.0 – 10.255.255.255,
- klasa B: 172.16.0.0 – 172.31.255.255 i
- klasa C: 192.168.0.0 – 192.168.255.255.

Konkretna klasa za IP privatnu adresu se bira u odnosu na zahtjeve i veličinu lokalne mreže u kojoj se primjenjuje, tako da se za veće mreže koristi Klasa A, dok za mreže manjih dimenzija Klasa C može biti adekvatna opcija.

Dati pregled karakteristika pojedinačnih klasa IP adresa potvrđuje ograničenja IP protokola verzije 4 kad je u pitanju veličina njegovog ukupnog adresnog prostora. Počevši od 1985. godine pravljeni su različiti pokušaji za prevazilaženje uočenog nedostatka, koji su se uglavnom zasnivali na dijeljenju Internet mreža na manje cjeline. Jedna od metoda odnosila se na korišćenje maske podmreže promjenljive dužine na nivou same klase (*Variable Length Subnet Mask* - VLSM). Takav pristup je faktički značio dijeljenje IP adrese na hijerarhijski definisane podmreže različitih veličina, što je s druge strane omogućavalo kreiranje podmreža sa različitim brojem čvorova, čime se postizalo optimalnije korišćenje ukupnog IP adresnog prostora.

Na taj način su realizovani prvi koraci vezani za izmjenu sistema klasa u IP adresiranju, u cilju odgovora na identifikovana ograničenja IPv4 protokola. Sistem klasa je zvanično zamijenjen 1993. godine objavljivanjem IETF standarda RFC 1517 [6], koji je specificirao

bezklasno međudomensko rutiranje (*Classless Inter Domain Routing* - CIDR) kao novi pristup za bolje iskorišćenje IPv4 adresnih resursa. CIDR je omogućio optimizaciju u domenu rutiranja putem korišćenja pojedinačne IP adrese i podmreže za upućivanje paketa podataka na grupu adresa. U takvim uslovima, IP adresa se sastoji od dvije grupe bitova. Prvi dio adrese je tzv. prefiks koji se koristi za identifikaciju (pod)mreže. Druga grupa bitova služi za identifikaciju čvora i određuje uređaj na mreži koji treba da primi dolazeće pakete podataka. S obzirom na činjenicu da je CIDR pristup omogućio pojednostavljenje rutiranja kroz grupisanje više mrežnih segmenata u okviru jedne IP adrese, jasno je da je na taj način postignuto i bolje iskorišćenje ukupnog adresnog prostora raspoloživog u okviru IPv4 protokola.

Još jedan pokušaj privremenog rješavanja ograničenih adresnih resursa IPv4 mreža odnosio se na implementaciju pristupa prevođenja mrežnih adresa (*Network Address Translation* - NAT). U pitanju je mapiranje jednog IP adresnog prostora u drugi, tako što se prilikom rutiranja modifikuje informacija o adresi mreže u IP zaglavlju. U najjednostavnijoj formi, obavlja se jedan-na-jedan prevod IP adresa, koji je specificiran RFC 2663 standardom [7]. Kod tog pristupa mijenjaju se samo IP adrese, kontrolna suma u zaglavlju i eventualno kontrolne sume višeg nivoa koje uključuju IP adresu. NAT je prvobitno korišćen da bi se izbjegla potreba za ponovnom identifikacijom svakog čvora u slučaju pomjeranja mreže, odnosno uvođenja komponente mobilnosti u Internet okruženje. Takođe, postignuta je i određena optimizacija upotrebe IPv4 adresnog prostora, s obzirom da je, na primjer, za identifikaciju jedne kompletne privatne mreže bila dovoljna IP adresa NAT *gateway*-a. Ipak, mapiranje IP adresa dovodi do modifikacije IP adrese u paketima, što za posljedicu ima prekid logičke Internet konekcije od kraja do kraja pa unosi dodatnu kompleksnost prilikom razvoja Internet aplikacija.

Implementacija VLSM, CIDR, NAT tehnika je pokazala određene pozitivne efekte sa aspekta prevazilažanja glavnog ograničenja IPv4 protokola. Ipak, izuzetno dinamičan razvoj Interneta i zahtjevi za adresnim prostorom su vrlo brzo pokazali da su u pitanju samo privremena rješenja koja ne daju održiv odgovor na nedostatke IPv4, koji su doveli do toga da se od februara 2011. godine i zvanično smatra da je adresni prostor u ovoj verziji Internet protokola iscrpljen.

## 2.3. IPv6 protokol

Nakon brojnih konsultacija i tehničkih diskusija, IETF je 1995. godine publikovao RFC 1883 [9] kao prvu specifikaciju Internet protokola naredne generacije: IPv6. Kasnije je ova specifikacija zamijenjena sa RFC 2460 [10] i dodatno ažurirana (RFC 8200) [11].

Dalji razvoj Interneta i konstantan rast potražnje za servisima i aplikacijama baziranim na IP mrežama, u potpunosti je opravdao takav pristup IETF-a. Sa svojim 32-bitnim formatom adresa, IPv4 može da obezbijedi maksimalno 4,3 milijarde jedinstvenih IP adresa i jasno je da, u aktuelnim uslovima implementacije IoT paradigme, ta činjenica predstavlja značajno ograničenje za dalji razvoj. Upravo zbog nedostatka IPv4 adresa u poslednjih nekoliko godina dolazi do intenzivnije implementacije IPv6, koji se smatra narednom fazom u evoluciji IP

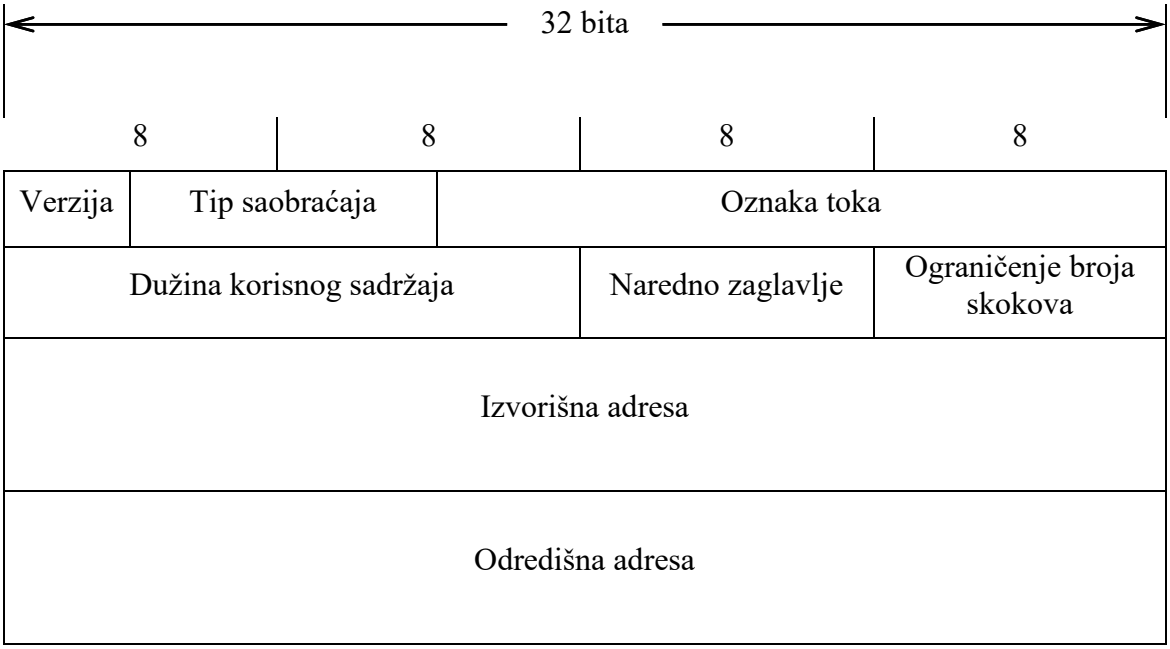
protokola[1]. Istovremeno, ukupna digitalna transformacija postavlja dodatne zahtjeve pred IP mreže: bolja podrška mobilnosti, manje kašnjenje, veća pouzdanost, poboljšana spektralna i energetska efikasnost, što dodatno ističe potrebu implementacije protokola novije generacije.

Iako IPv6 nije direktno interoperabilan sa IPv4, dizajniran je da koegzistira sa IPv4 i podrži iste Internet servise i aplikacije, tako da su trenutno u upotrebi i jedna i druga verzija. U odnosu na oko 4,3 milijarde IPv4 adresa koje su već dodijeljene na globalnom nivou, IPv6 sa svojim 128-bitnim adresnim prostorom može da podrži $3{,}4 \times 10^{38}$ jedinstvenih Internet adresa. Na taj način se rješava osnovni nedostatak IPv4, ali se istovremeno ostvaruje i čitav niz drugih prednosti koje su u skladu sa zahtijevima savremenog Internet okruženja, koje karakteriše razvoj zasnovan na IoT paradigmi u najširem smislu.

Kako je već naglašeno, glavni cilj implementacije IPv6 protokola je povećanje Internet adresnog prostora, pri čemu su osnovne izmjene u odnosu na IPv4 značajno obuhvatnije i uključuju:

- pojednostavljenje formata zaglavlja,
- povećanje adresnog prostora,
- ugrađene mehanizme zaštite,
- poboljšanu podršku za kvalitet servisa (QoS) i
- skalabilnost.

Na slici 6 je ilustrovana struktura zaglavlja IPv6 paketa. Očigledno je da je riječ o jednostavnijoj strukturi, s obzirom na manji broj specificiranih polja, nego što je to slučaj kod IPv4.




Slika 6. Struktura IPv6 zaglavlja

Značenje pojedinih polja je sledeće:

- Verzija - 4-bitna oznaka verzije protokola (6 u ovom slučaju).

[1] IPv5 je postojao samo eksperimentalno i vrlo brzo je napušten njegov dalji razvoj u toj formi

- Tip saobraćaja (TC - *Traffic Class*) - 8-bitno polje za označavanje prioriteta paketa.
- Oznaka toka (FL - *Flow Label*) - 20-bitno polje za identifikaciju toka podataka kojem određeni paket pripada.
- Dužina korisnog sadržaja (PL - *Payload Length*) - 16-bitno polje koje definiše dužinu podataka u IP paketu.
- Naredno zaglavlje (NH - *Next Header*) - 8-bitno polje za identifikaciju tipa zaglavlja koje slijedi.
- Ograničenje broja skokova (HL - *Hop Limit*) – 8-bitno polje na nivou cijelog broja, koji se umanjuje za 1 od strane svakog čvorišta koje proslijedi paket. Kad HL dostigne vrijednost nula, paket se odbacuje.
- Izvorišna adresa (SA - *Source Address*) – 128-bitna adresa čvora koji inicira prenos paketa.
- Odredišna adresa (DA - *Destination Address*) – 128-bitna adresa čvora kome je paket upućen .

Može se uočiti da su u odnosu na IPv4, u ovoj verziji zadržana samo 3 polja, a uvedeno je 5 novih. Najznačajnija promjena odnosi se na polje O (*Options*), koje se kod IPv4 eventualno može koristiti za indikaciju dodatnih parametara servisa. Kod IPv6 takve dodatne informacije se smještaju u dio paketa koji se naziva ekstenzija zaglavlja, čime se postiže fiksna dužina paketa od 40 okteta. Pri tome, ekstenzija zaglavlja se smješta između IPv6 zaglavlja i zaglavlja transportnog nivoa referentnog modela, s tim što se većina ovih ekstenzija ne obrađuje u ruterima tokom prenosa paketa. Na taj način je i ukupno procesuiranje u mreži pojednostavljeno u odnosu na IPv4.

IPv6 paket može sadržati: nula, jedan ili više ekstenzija zaglavlja, od kojih je svaka identifikovana u polju „Naredno zaglavlje“ prethodnog zaglavlja. Pri tome, svaka ekstenzija zaglavlja je dužine koja odgovara cijelom multiplu 8 okteta, kako bi se zadržala usklađenost u odnosu na zaglavlja koja slijede. IETF RFC 2460 [10] daje specifikaciju sledećih tipova ekstenzije zaglavlja paketa koje treba implementirati u svrhu pune primjene IPv6 protokola:

- zaglavlje za svaki skok (*hop-by-hop*),
- zaglavlje rutiranja,
- zaglavlje fragmenta,
- zaglavlje odredišnih opcija,
- zaglavlje autentifikacije i
- zaglavlje enkapsuliranih podataka zaštite (*Encapsulating Security Payload*).

U slučaju da paket sadrži više od jednog zaglavlja ekstenzije, standardom se preporučuje sledeći raspored: IPv6 zaglavlje, zaglavlje za svaki skok, zaglavlje odredišnih opcija, zaglavlje rutiranja, zaglavlje fragmenta, zaglavlje autentifikacije, zaglavlje enkapsuliranih podataka zaštite, zaglavlje odredišnih opcija, zaglavlje višeg sloja. Pri tome, svaki od tipova ekstenzije zaglavlja se može pojaviti samo jednom, izuzev zaglavlja odredišnih opcija koje treba da se pojavi najmanje dva puta (jednom ispred zaglavlja rutiranja i jednom ispred zaglavlja višeg sloja). Ako je zaglavlje višeg nivoa takođe IPv6 zaglavlje, onda i ono može

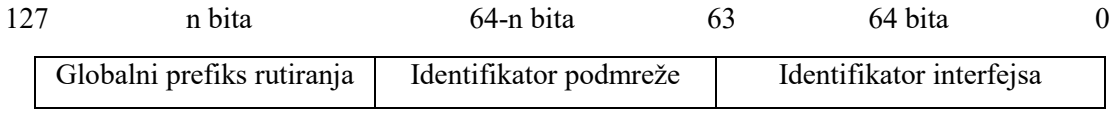
biti praćeno sopstvenim ekstenzijama zaglavlja, koja autonomno podliježu identičnom redoslijedu.

S obzirom da predstavljaju novu karakteristiku uvedenu verzijom 6, posebno su interesantna dva tipa ekstenzije zaglavlja koja se odnose na sigurnost i zaštitu podataka: zaglavlje autentifikacije i zaglavlje enkapsuliranih podataka zaštite. Imajući u vidu značaj, zaglavlje autentifikacije je specificirano posebnim standardom RFC 2402 [12] i koristi se za očuvanje autentičnosti i integriteta podataka (osiguranje od malicioznih i slučajnih izmjena podataka tokom prenosa) putem kriptografskih mehanizama i zaštitu od napada presretanjem i ponovnim slanjem paketa. Ova ekstenzija zaglavlja se specificira vrijednošću 51 u polju „Sljedeće zaglavlje“ prethodnog IP zaglavlja, pri čemu treba uočiti da se njegovom implementacijom ne ostvaruje tajnost podataka. Ukoliko postoji potreba te vrste, treba ga koristiti zajedno sa zaglavljem enkapsuliranih sigurnosnih podataka (*Encapsulating Security Payload*), koje je opisano specifikacijom RFC 2406 [13]. Ova ekstenzija zaglavlja dodatno ostvaruje tajnost podataka uključenih u IP paket, pored autentičnosti i integriteta, a identifikuje se vrijednošću 50 u polju „Sljedeće zaglavlje“ prethodnog IP zaglavlja.

Ipak, najznačajnija nova karakteristika IP protokola koja je uvedena verzijom 6, odnosi se na veličinu adresnog prostora kreiranog povećanjem dužine adresnog polja u IP zaglavlju sa 32 na 128 bitova. Segmenti tog novog adresnog polja su sledeći:

- Adresa rutiranja, koja se sastoji od dva dijela:
  - globalnog prefiksa rutiranja dodijeljenog određenoj grupi podmreža/linkova i
  - identifikatora podmreže.
- Identifikator mrežnog interfejsa.

Takva jedna uobičajena struktura, u kojoj polje „Identifikator interfejsa“ sadrži 64 bita, prikazana je na slici 7.




Slika 7. Struktura IPv6 adrese

S obzirom na dužinu ukupnog adresnog polja, predstavljanje IPv6 adrese nizom binarnih jedinica i nula nije praktično, kao ni decimalna prezentacija koja se koristi kod IPv4. Usvojeno je da se IPv6 adresa obično zapisuje kao osam grupa (blokova) od po četiri heksadecimalna broja, razdvojena sa dvije tačke. Dodatno su uvedena još dva pravila u prezentaciji IPv6 adresa: izostavljanje početnih nula, tako da se u okviru svake grupe od 16 bita između dvije dvotačke izostavljaju početne nule, kao i sukcesivne nule (što se na nivou jedne adrese može primijeniti samo jednom). Uvođenjem ovih dodatnih pravila značajno se komprimuje zapis IPv6 adrese, a time i ukupan proces obrade i programiranja na nivou mreže. Na sledećem primjeru je ilustrovan postupak pojednostavljivanja zapisa IPv6 adrese:

0010000111011010000000001101001100000000000000000010111100111011
0000001010101010000000001111111111111111000101000100111000101101O

-IPv6 adresa u binarnom zapisu-

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
-IPv6 adresa predstavljena sa 8 blokova od po 16 bita-

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
-IPv6 adresa predstavljena u heksadecimalnom zapisu-

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
-IPv6 adresa nakon izostavljanja početnih nula u blokovima-

Kad su u pitanju adresni režimi, IPv6 se razlikuje od IPv4. Pri tome, IPv6 takođe podržava različite tipove adresa, s tim što se ne mogu svi tipovi IPv6 adresa mapirati jedan na jedan sa tipovima IPv4 adresa. Nadalje, nezavisno od načina adresiranja, IPv6 adrese eksplicitno označavaju mrežne interfejse, a ne mrežne čvorove. Mrežni čvor je specificiran bilo kojom jednoznačnom (*unicast*) adresom dodijeljenom jednom od njegovih mrežnih interfejsa. Takođe, saglasno RFC 3513 [14], IPv6 ne definiše univerzalnu (*broadcast*) adresu kao što je to slučaj kod IPv4 protokola.

Dokumentom RFC 2373 [15] definiše se nekoliko tipova (režima) IPv6 adresa.

*1) Unicast* adresa je adresa dodijeljena jednom mrežnom interfejsu. Postoji više tipova IPv6 *unicast* adresa:

- Jedinstvene lokalne adrese (eng. *Unique Local address* - ULA)
- Globalna *unicast* adresa (eng. *Global unicast address* - GUA),
- *Unicast* adresa lokalnog linka (eng. *Link-local unicast address*),
- *Unicast* adresa lokalnog sajta (eng. *Site-local unicast address*),
- Specijalne IPv6 adrese
- Kompatibilne adrese

**Jedinstvena lokalna adresa**

Jedinstvene lokalne adrese su definisane u RFC 4193 dokumentu [16]. Ove adrese predstavljaju *unicast* adrese koje se mogu koristiti za internu IPv6 komunikaciju u organizaciji i globalno su jedinstvene. One su rutabilne unutar organizacije, ali se takođe mogu rutirati između lokacija koristeći tunelovanje. ULA adrese ne bi trebalo da se oglašavaju na Internetu. Ove adrese se mogu prepoznati po prefiksu fc00::/ 8 ili fd00::/8 (tabela 1). Glavna svrha ovih IPv6 adresa je lokalna komunikacija za određenu lokaciju ili između ograničenog skupa lokacija. ULA adresa koja se lokalno koristi ne treba da se mijenja u slučaju da se globalni prefiks lokacije promijeni, za razliku od GUA adrese. S druge strane, globalna komunikacija između proizvoljnih lokacija na Internetu nije moguća koristeći jedinstvene lokalne adrese. Sa softversko-tehničke tačke gledišta, ULA i GUA se mogu tretirati na isti način, tj. prilagođavanje aplikacija u vezi sa korišćenjem ULA ili GUA adresa nije potrebno.

**Globalna *unicast* adresa**

IPv6 globalna *unicast* adresa je rutabilna i dostupna iz IPv6 dijela Interneta i ekvivalentna je javnoj IPv4 adresi. Struktura globalne *unicast* adrese omogućava agregaciju prefiksa kako bi se omogućilo efikasnije rutiranje. Trenutno, globalne *unicast* adrese se dodjeljuju iz opsega

adresa koje počinju sa binarnom vrijednošću 001 (odnosno 2000::/3). Opseg 2000::/3 koristi jednu osminu ukupnog IPv6 adresnog prostora.

### *Unicast* adresa lokalnog linka (*Link-local unicast address*)

*Unicast* adresa lokalnog linka je IPv6 adresa koja se automatski konfiguriše na svakom mrežnom interfejsu, bez obzira na to da li su konfigurisane neke druge adrese. Koristi se prefiks fe80::/10 (adrese počinju sa 1111 1110 10 binarno) i identifikator interfejsa (Interface ID) koji je u EUI-64 (*Extended Unique Identifier* - 64) formatu. Ekvivalentne su IPv4 automatskim privatnim adresama (APIPA - *Automatic Private IP Addressing*) koje mogu da se automatski konfigurišu pod *Windows* operativnim sistemom koristeći opseg 169.254.0.0/16.

Ovaj tip IPv6 adresa uglavnom služi za povezivanje uređaja na lokalnom linku, bez potrebe za globalnim adresama. Na taj način uređaji mogu komunicirati bez potrebe za ruterom. Takođe *unicast* adrese lokalnog linka koriste se kod *Neighbor Discovery* protokola i procesa autokonfiguracije. Ruteri ne smiju prosleđivati pakete koji imaju ovaj tip adrese kao izvorišnu ili odredišnu adresu.

### *Unicast* adresa lokalnog sajta (*Site-local unicast address*)

Ovaj tip IPv6 adresa je ekvivalentan privatnim adresama iz IPv4 koje pripadaju poznatim opsezima 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16. Za *unicast* adrese lokalnog sajta određen je prefiks fec0::/10 (adrese počinju sa 1111 1110 11 binarno). Posle ovog prefiksa sledećih 38 bita je fiksirano na vrijednost 0, a zatim sledi 16-bitni identifikator podmreže (*Subnet* ID) i 64-bitni identifikator interfejsa (Interface ID). Privatne adrese se mogu koristiti bez potrebe za jedinstvenim prefiksom, ukoliko mreža nije povezana na Internet. Ruteri ne oglašavaju putanje i ne proslijeđuju pakete sa ovim tipom adrese van granica određenog sajta. Ukoliko kasnije bude neophodno povezivanje na Internet, dovoljno je dodijeliti globalni ruting prefiks dok se već definisana adresna šema cijelog sajta može primijeniti na ovaj prefiks.

### Specijalne IPv6 adrese

U grupu specijalnih IPv6 adresa spadaju dva tipa adresa: nedefinisane i *loopback* adrese. Nedefinisana adresa (eng. *unspecified*) označava se sa 0:0:0:0:0:0:0:0 ili samo "::". Koristi se samo u slučaju da uređaj ne posjeduje svoju IPv6 adresu. Uglavnom se koristi kao izvorišna adresa u paketima kojima uređaj pokušava da odredi jedinstvenost svoje adrese. Nikada se ne dodeljuje nekom interfejsu, niti se koristi kao odredišna adresa. Ekvivalentna je sa nedefinisanom IPv4 adresom 0.0.0.0.

*Loopback* adresa označava se kao 0:0:0:0:0:0:0:1 ili ::1. Služi za označavanje lokalnog interfejsa u IP steku, omogućavajući uređaju da šalje pakete samom sebi. Ekvivalentna je IPv4 adresi 127.0.0.1. Ne može se dodjeliti fizičkom interfejsu, a ruteri ne smiju proslijeđivati pakete sa ovim adresama.

**Kompatibilne adrese**

Zbog potrebe postepenog prelaska sa IPv4 na IPv6 i paralelnog korišćenja oba protokola, definisane su i kompatibilne adrese: IPv4 kompatibilne adrese IPv6 i IPv4 mapirane adrese IPv6.

IPv4 kompatibilna adresa IPv6 (eng. *IPv4-Compatible IPv6 address*) je tip adrese koji integriše IPv4 adresu u najnižih 32 bita IPv6 adrese, dok ostalih 96 bita IPv6 adrese ima vrijednost 0. Format IPv4 kompatibilne adrese je 0:0:0:0:0:0:w.x.y.z ili ::w.x.y.z. Svih 128 bita ove adrese predstavljaju IPv6 adresu uređaja, dok 32 najniža bita predstavljaju njegovu IPv4 adresu. Može se koristiti kod uređaja koji rade u *dual-stack* režimu, tj. podržavaju IPv4 i IPv6. Ovakvo adresiranje omogućava automatsko tunelovanje IPv6 paketa preko IPv4 infrastrukture.

- IPv4 mapirana adresa na IPv6 (eng. *IPv4-mapped IPv6 address*) je tip adrese koji takođe integriše IPv4 adresu u najnižih 32 bita IPv6 adrese. Format adrese je 0:0:0:0:0:FFFF:w.x.y.z ili ::FFFF:w.x.y.z. Koristi se za predstavljanje IPv4 uređaja IPv6 uređaju. Na *dual-stack* uređaju, IPv6 aplikacija koja šalje saobraćaj na IPv4 mapiranu adresu, poslaće IPv4 paket sa IPv4 adresom.

Na slici 8 su prikazani primjeri formata koje mogu imati navedene *unicast* adrese.

Najznačajniji bitovi IPv6 adrese se koriste za razlikovanje tipova, kao što je prikazano u tabeli 1.

| 10 bita | 54 bita | 64 bita |
|---|---|---|
| 1111111010 | 0……0 | Identifikator interfejsa |

*Unicast* adresa lokalnog linka

| 10 bita | 54 bita | 64 bita |
|---|---|---|
| 1111111011 | Identifikator podmreže | Identifikator interfejsa |

*Unicast* jedinstvena lokalna adresa

| 3 bita | 45 bita | 16 bita | 64 bita |
|---|---|---|---|
| 001 | Globalni prefiks rutiranja | Identifikator podmreže | Identifikator interfejsa |

*Unicast* globalna adresa

Slika 8. Primjeri *unicast* adresa

*Tabela 1. Tipovi IPv6 adresa*

| Tip adrese | Binarni prefiks | IPv6 zapis |
|---|---|---|
| Nedefinisana (eng. *Unspecified*) | 00…0 (128 bita) | ::/128 |
| *Loopback* adresa interfejsa | 00…1 (128 bita) | ::1/128 |
| *Multicast* adresa | 11111111 | ff00::/8 |
| Link-Local *Unicast* | 1111111010 | fe80::/10 |

| | | |
|---|---|---|
| Jedinstvene lokalne adrese (eng. *Unique Local* - ULA) | 11111100<br>11111101 | fc00::/8<br>fd00::/8 |
| Globalne unicast adrese (eng. *Global Unicast* (GUA) | Ostale IPv6 adrese | |

2.) *Multicast* – IPv6 *multicast* adrese se koriste za komunikaciju od jedne IPv6 krajnje tačke prema grupi prijemnika (grupi mrežnih interfejsa, tj. čvorova). IPv6 paketi namijenjeni određenoj *multicast* adresi se faktički dostavljaju skupu interfejsa koji pripadaju toj *multicast* grupi. Pri tome, pojedinačni mrežni interfejs može biti član više *multicast* grupa i tada mu se dodjeljuju sve IPv6 *multicast* adrese koje specificiraju te grupe.

IPv6 *multicast* adrese igraju centralnu ulogu za IPv6, pošto se mnoge funkcije protokola koje se odnose na *broadcast* u IPv4, u IPv6 implementiraju koristeći *multicast* (emitovane adrese nisu dostupne u IPv6). IPv6 *multicast* adrese počinju prefiksom FF00 ::/ 8, zatim slijede 4 bita indikatora (*flags*), 4 bita dometa i 112 bitova identifikatora grupe. Pri tome, standard RFC 4007 [17] specificira sledeće domete kod ove vrste adresa: lokalni intefejs, lokalni link, administrativno lokalni, lokacijsko lokalni, organizaciono lokalni i globalni. Jedan primjer *multicast* IPv6 adrese dat je na slici 9.

| 8 bitova | 4 bita | 4 bita | 112 bitova |
|---|---|---|---|
| 11111111 | Indikator | Domet | Identifikator grupe |

Slika 9. Primjer *multicast* IPv6 adrese

3.) *Anycast* – Ova vrsta adresa se koristi za identifikaciju grupe interfejsa, a podatke koji za odredište imaju ovu adresu IP ruteri proslijeđuju najbližem interfejsu u grupi. Dakle, ovaj tip adresiranja se koristi kod komunikacije 1:(1 od N). Trenutno se ove adrese koriste isključivo kao odredišne adrese, a dodijeljuju se IPv6 ruterima. Saglasno RFC 4291 [18] ove adrese se dodijeljuju iz adresnog prostora *unicast* adresa, pa je njihov domet određen dometom odgovarajuće *unicast* adrese.

Svaki ruter u okviru određene podmreže mora imati *anycast* adresu, koja je predefinisana i određena prefiksom podmreže za pripadajući mrežni interfejs. Adresa rutera podmreže formira se tako da se bitovi prefiksa mreže fiksiraju, a ostali bitovi adrese postave na 0. Svim mrežnim interfejsima koji su dio određene podmreže dodijeljuju se takve adrese, koje se potom koriste u komunikaciji s jednim od rutera neke udaljene podmreže. Pojedinačni interfejs i ovdje može biti dio više različitih grupa. U tom slučaju adrese svih ovih grupa su dodijeljene takvom interfejsu.

Pored navedenih, RFC 4291 [18] specificira i IPv6 adrese sa ugrađenim IPv4 adresama. Pri tome se razlikuju dva tipa takvih adresa: IPv4 kompatibilne IPv6 adrese i IPv4 mapirane IPv6 adrese. Prvi tip je zastario i više se ne koristi, tako da ga sistemi, klijenti i aplikacije više ne podržavaju.

IPv4 mapirane adrese se koriste u nekim postupcima migracije na IPv6, kada se IPv4 adrese direktno mapiraju na posebnu IPv6 adresu. Odgovarajući format ugrađivanja za IPv4

mapirane adrese je specificiran sa: 0000: 0000: 0000: 0000: 0000: ffff: <IPv4-adresa> (slika 10).

| 80 bita | 16 bita | 32 bita |
|---|---|---|
| 0000:0000:0000:0000:0000 | FFFF | IPv4 adresa |

Slika 10. Primjer IPv6 adrese sa ugrađenom IPv4 adresom

Kako je već naglašeno, jedan od glavnih motiva uvođenja IPv6 protokola je globalna digitalna transformacija koja iz dana u dan dobija na intenzitetu kroz sve značajniju implementaciju IoT infrastrukture kojom se podržavaju brojne horizontalne i vertikalne aplikacije. U tom kontekstu, upravo usvajanje plana IPv6 adresiranja, čije su osnove prethodno opisane, predstavlja strateško pitanje koje traži pravovremenu i efikasnu reakciju svih pojedinačnih relevantnih subjekata: regulatora, administracija, provajdera servisa, operatora infrastrukture, …

Upravo je to i bio razlog da 2012. godine IETF usvoji standard RFC 6540 [19], kojim se specificira obaveza podrške IPv6 protokolu od strane svih IP krajnjih tačaka. Nakon toga je, u novembru 2016. godine, IAB (*Internet Architecture Board*) usvojio formalnu preporuku da svi budući mrežni standardi budu zasnovani na IPv6, kao i da budući rad IETF-a bude usmjeren na optimizaciju i poboljšanja IPv6 protokola. Na taj način je IPv6 praktično pozicioniran kao Internet protokol budućnosti.

## 2.4. Prednosti IPv6 u odnosu na IPv4

Implementacija IPv6 protokola predstavlja ključni uslov za nastavak dinamičnog razvoja Interneta. U tom cilju, mrežni operatori, provajderi sadržaja, nosioci razvoja softvera i hardvera, regulatori i administracije, imaju ulogu nosioca odgovarajućih aktivnosti, čime obezbjeđuju uslove za efikasno poslovanje, globalno povezivanje i održivi rast Interneta i pripadajućih servisa i aplikacija.

Kako je to već naglašeno, osnovno poboljšanje koje se uvodi implementacijom IPv6 odnosi se na proširenje raspoloživog adresnog prostora koji se kod IPv4 pokazao ograničenim sa aspekta realizacije koncepta Interneta nove generacije. Tako, IPv6 povećava IP adresni prostor sa 32 na 128 bitova čime se stvaraju uslovi za podršku očekivanom rastu broja objekata koji čine osnovu IoT koncepta. Istovremeno, *multicast* adresni režim nije više opcija, već je kod IPv6 zahtjevani režim, čime se dodatno pružaju uslovi za masovnu konektivnost.

Povećanje adresnog prostora je omogućilo unapređenje nekih od IPv4 funkcija, kao i dodavanje potpuno novih funkcija u IPv6 specifikaciju. Tako je, na primjer, značajno unaprijeđena funkcija autokonfiguracije. IPv4 koristi DHCP (*Dynamic Host Configuration Protocol*) protokol za autokonfiguraciju, koji podrazumijeva da uređaj (čvor) dobija adrese interfejsa, kao i druge potrebne informacije, od DHCP servera, koji raspolaže ručno administriranom listom adresa i vodi računa o tome koje adrese su dodjeljene kom uređaju. Za razliku od IPv4, IPv6 nudi automatsku konfiguraciju uz vrlo jednostavne mehanizme konfiguracije (*plug-and-play*). Naime, zahvaljujući tome što se isporučuje kompletan IP prefiks, a ne samo adresa, uređaj ima mogućnost automatske konfiguracije sopstvene IPv6 adrese i za to mu nije potrebna asistencija servera. Koristeći tako generisanu adresu lokalnog linka, ne postoji neposredna potreba za bilo kojom drugom infrastrukturom koja bi omogućila

da taj uređaj počne da komunicira preko IPv6 na svojoj lokalnoj mreži, uključujući komunikaciju sa drugim lokalnim čvorom ili ruterom. Pri tome, ako je prisutan IPv6 ruter, svaki uređaj koji podržava IPv6 može generisati ne samo lokalnu adresu, već i globalno rutabilnu adresu i na taj način dobiti pristup globalnom Internetu. Uz opisanu mogućnost autokonfiguracije, kod IPv6 je zadržana i opcija DHCPv6, odnosno autokonfiguracije slične IPv4 DHCP.

Takođe, značajno veći adresni IPv6 prostor omogućava ponovno uspostavljanje *end-to-end* arhitekture na Internetu, koju karakteriše mogućnost direktnog komuniciranja uređaja bez potrebe za posrednikom. Naime, nedostatak IPv4 adresa je doveo do široke upotrebe privatnih adresnih prostora, koji nisu direktno dostupni sa Interneta. Sada, uređaji sa IPv6 adresama i IPv6 povezivanjem su direktno dostupni posredstvom njihove adrese i nema potrebe za formiranjem privatnih adresnih prostora koji faktički znače posrednu dostupnost. Na taj način je i značajno pojednostavljen razvoj najnovijih aplikacija koje zahtijevaju *end-to-end* komunikaciju između pojedinačnih uređaja određenih svojim IP adresama (*online* igrice za više igrača, video konferencije, *streaming*, dijeljenje datoteka, VoIP, …).

I brzina rutiranja IP paketa je povećana kod IPv6 mreža, što sa aspekta aktuelnih aplikacija i servisa, kao i realizacije IoT koncepta, predstavlja značajnu prednost. Kod IPv4 mreža paketi se prenose od jedne tačke do druge uz korišćenje mrežnih rutera. Pri tome, u skladu sa strukturom IPv4 zaglavlja, ruteri vrše obradu svakog paketa, provjeravaju kontrolnu sumu i eventualno procesuiraju adresno polje gdje su date opcije. Jasno je da se na taj način uvodi, ne samo kašnjenje u obradi, već i određeni nivo degradacije performansi ukupne mreže.

U poređenju sa IPv4, IPv6 ima mnogo jednostavniju strukturu zaglavlja paketa, koje je dizajnirano na način da minimizira vrijeme i postupke potrebne za njegovu obradu. To je postignuto pomjeranjem polja opcija i eventualno ostalih polja u ekstenziju zaglavlja, tako da se samo zaglavlje IPv6 paketa efikasnije obrađuje na ruterima. S obzirom da u takvim uslovima ne postoji potreba da ruter provjerava kontrolnu sumu, njegov softver ili hardver postaje jednostavniji uz omogućavanje brze obrade paketa, čime se smanjuje ukupno kašnjenje obrade, a time se postiže i poboljšanje performansi cijele mreže.

Postoji i čitav niz drugih razloga koji predstavljaju značajne izazove u mrežama zasnovanim na IPv4 protokolu i koji se prevazilaze upravo implementacijom IPv6.

Jedan od najvažnijih se odnosi na sigurnost i zaštitu u mrežama baziranim na Internetu. To posebno dolazi do izražaja u aktuelnim uslovima sve češće pojave DDoS (*Distributed Denial of Service*) napada, virusa i spama, pa do realnih oblika neprijateljski usmjerenih aktivnosti prema pojedincima, grupama, pa i cijelim državama. IPv4 protokol je specificiran u uslovima kada se gotovo i nije vodilo računa o potrebi zaštite podataka koji se prenose i usvojeni pristup je podrazumijevao odgovornost korisnika na osnovu evidencije o fizičkom pristupu krajnjem sistemu, za slučaj da se potreba ukaže. Neka od unapređenja koja su implementirana na nivou IPv4 protokola su bila usmjerena na obezbjeđenje određenog nivoa zaštite, korišćenjem *firewall*-a. Takođe, uveden je i IPSec protokol koji je omogućio šifriranje određenih komunikacija, ali je njegova implementacija u IPv4 ostala na nivou opcije. U cjelini, takva rješenja su se pokazala nedovoljnim sa aspekta zahtijeva novih aplikacija (elektronska trgovina, industrijski IoT, *eHealth*, …) za koje je fleksibilna *end-to-end* zaštita neophodna.

Uvođenjem obavezne podrške za sigurnost na mrežnom nivou (IPSec), IPv6 je nominalno u značajnoj prednosti u odnosu na IPv4 kod koga ne postoji mogućnost validacije adrese izvorišta, s obzirom da ruteri preusmjeravaju pakete isključivo na osnovu odredišne adrese. IPSec sadrži kriptografske protokole za podršku zaštićenom prenosu podataka i razmjenu sigurnosnih ključeva, od kojih su osnovni: AH (*Authentication Header*) protokol, koji pruža autentičnost i integritet podataka; ESP (*Encapsulating Security Payload*) protokol, koji pored autentičnosti i integriteta podataka pruža i privatnost podataka; IKE (*Internet Key Exchange*) protokol, koji omogućava početno podešavanje i pregovaranje sigurnosnih parametara između dva čvora. Obezbjeđujući *end-to-end* zaštitu preko IPSec protokola, IPv6 aplikacijama može pružiti garancije o autentičnosti i povjerljivosti razmijenjenih podataka, čime se eliminiše potreba da same aplikacije implementiraju te funkcionalnosti. Takođe, korišćenjem istih mehanizama zaštite za sve aplikacije, implementacija i administriranje funkcija zaštite postaje mnogo jednostavnije, ali umanjuje fleksibilnost sa aspekta same aplikacije.

Značajan izazov u mrežama sa tradicionalnom arhitekturom je mobilnost korisnika, odnosno intenzivno i kontinuirano povećanje penetracije mobilnog Interneta. Mobilnost korisnika uvodi određene dodatne zahtjeve kada je u pitanju postizanje kvaliteta usluge, s obzirom na to da priroda IPv4 adresa može dovesti do prekida TCP veze zbog promjene lokacije čvora i IP adrese pri kretanju. Pri tome, sa aspekta IP protokola, sam pojam mobilnosti obuhvata različite kategorije mreža i uređaja, kao na primjer: uređaje koji mogu promijeniti svoju lokaciju, ali žele zadržati postojeće veze; mreže koje pružaju mobilnost za grupu uređaja; *ad-hoc* umrežavanja kod kojih određeni uređaji ostaju povezani sa mrežom samo za kratko vrijeme trajanja komunikacione sesije. U takvim uslovima, IPv4 zahtijeva implementaciju posebnog rutera na aktuelnoj lokaciji mobilnog uređaja kako bi se obezbijedilo uspostavljanje i održavanje komunikacije. Uz to, pojavljuje se i problem filtriranja, s obzirom da ruter koristi aktuelnu adresu mobilnog uređaja kao izvorišnu adresu paketa, što može dovesti do konfuzije u daljem prihvatanju paketa od strane uređaja u mreži.

Kod IPv6 podrška za mobilnost se ostvaruje implementacijom *Mobile* IPv6 (MIPv6) protokola, koji ima ugrađenu funkciju optimizacije prenosnog puta. Dodatne funkcije, kao što su otkrivanje susjednih uređaja (*Neighbor Discovery*) i auto-konfiguracija adrese, omogućavaju mobilnim uređajima (čvorovima) da funkcionišu na bilo kojoj lokaciji bez potrebe za uključivanjem posebnog rutera. Zahvaljujući *Mobile* IPv6 protokolu osigurava se povezivanje sa transportnim slojem, čime se čvorovima omogućava da ostanu dostupni bez obzira na lokaciju u IPv6 mreži. Na taj način, održavaju se postojeće veze preko kojih mobilni čvor komunicira, bez obzira na promjene njegove lokacije i adresa.

Kvalitet servisa (QoS) i upravljanja saobraćajem takođe imaju svoja ograničenja u tradicionalnoj Internet arhitekturi, posebno kada je u pitanju garantovanje kvaliteta servisa na prioritetnoj osnovi i u realnom vremenu. Kod IPv4, polje u zaglavlju koje se odnosi na tip servisa (DSCP) ima zadatak klasifikacije paketa i definisanja vrste servisa koji se očekuje od paketa, dok se prenose u mreži. To se obično obavlja pomoću posrednih uređaja u mreži, koji klasifikuju pakete na osnovu potreba određene aplikacije. U tim okolnostima problem nastaje zbog nekompatibilnosti takvih uređaja koji imaju obavezu održavanja određenog nivoa QoS.

Kod IPv6 protokola uslovi za osiguravanje traženog nivoa QoS su značajno poboljšani uvođenjem u zaglavlje novog polja „Oznake toka“ (FL), kojim se definiše način na koji se paketi identifikuju i tretiraju od strane rutera. Time se obezbjeđuje efikasniji prenos podataka sa jednog kraja na drugi, bez mogućnosti da posredni uređaji dovedu do njihove eventualne modifikacije, odnosno narušavanja nivoa QoS. Dodatno, korišćenjem protokola tipa IntServ (*Integrated Services*) i DiffServ (*Differentiated Services*), IPv6 omogućava zahtijevani, povećani, QoS koji je neophodan za novije aplikacije, kao što su IP telefonija, video/audio, interaktivne igre ili e-trgovina. Takođe, za razliku od IPv4 koji podržava „*best effor*t“ servis, IPv6 osigurava QoS u vidu skupa servisnih zahtijeva kojima se garantuje poboljšani nivo performansi mreže za prenos. Pri tome, za mrežni saobraćaj, kvalitet se definiše parametrima tipa: gubitak podataka, kašnjenje ili propusni opseg. U cilju implementiranja oznake za QoS, kod IPv6 se koristi polje „Tipa saobraćaja“ (8 bita) u IPv6 zaglavlju, kao i navedeno 20-bitno polje „Oznake toka“.

Uz sve navedene prednosti, administriranje u IPv6 mrežama je jednostavnije. Tako, na primjer, u situacijama kada postoji potreba proširivanja postojeće mreže ili spajanja dvije različite mreže, ili kada dođe do promjene provajdera servisa, neophodno je realizovati prenumerisanje mreže, jer se dodjeljuje nova šema adresiranja. U slučaju IPv4 mreža, ukupno prenumerisanje mreže i dodeljivanje novih adresnih šema se obavlja manuelno. IPv6 pruža mogućnost automatskog prenumerisanja mreže. Dakle, za razliku od IPv4, kod IPv6 nema potrebe za manuelnim rekonfigurisanjem svakog čvora i rutera, čime se omogućava brže proširivanje mreže ili spajanje više mreža.

Imajući u vidu prethodno opisane prednosti, jasni su razlozi konstantnog rasta stepena usvajanja IPv6 protokola. Od početka implementacije, nivo zastupljenosti IPv6 se značajno povećao:

- Preko 25% svih mreža baziranih na Internetu primjenjuje IPv6 [20].
- Prema Google izvještajima, u 49 država je više od 5% saobraćaja realizovano preko IPv6 (pri čemu se taj broj stalno mijenja), dok je u 24 države taj procenat preko 15% [21].

U takvim uslovima, IPv6 je prešao iz faze inovacija i ranog usvajanja u fazu najave dominantne implementacije. Uz to, cijena IPv4 adrese je blizu projektovanog maksimuma za 2018., tako da su *cloud hosting* provajderi počeli da naplaćuju IPv4 adrese dok omogućavaju IPv6 servise bez dodatnih troškova za adresni prostor. Na taj način, IPv4 će vremenom postati nepotreban trošak i špekulativna roba, za kojom se gubi interes.

Ipak, IPv4 je u značajnom periodu uspješno implementiran na globalnom nivou, što je dokaz kvaliteta prinicipa na kojima je dizajniran. To je i razlog da su kod IPv6 prisutne brojne karakteristike koje su učinile IPv4 tako uspješnim. Ipak, uprkos činjenici da su prisutne brojne aplikacije na tržištu koje zahtijevaju IPv6, nema dileme da će IPv4 nastaviti da egzistira i dalje. Upravo to i predstavlja izazov sa aspekta izbora prave strategije za efikasnu migraciju sa IPv4 na IPv6. Generalno se može reći da je uspješan mehanizam za IPv4/IPv6 migraciju onaj koji omogućava potpunu implementaciju IPv6 protokola, dok se istovremeno postiže kompatibilnost sa već postojećim IPv4 uređajima. U takvim uslovima, IPv6 uređaji i ruteri

moraju imati mogućnost interakcije i funkcionisanja sa postojećom IPv4 mrežnom infrastrukturom.

Za ostvarivanje takvog koncepta na raspolaganju su različiti mehanizmi migracije koji omogućavaju da IPv4 i IPv6 mreže koegzistiraju u periodu koji prethodi potpunoj migraciji na IPv6. U nastavku ove Studije je dat njihov detaljan pregled i opis, na bazi čega su i formulisani predlozi koji se odnose na mogućnosti primjene u Crnoj Gori.

# 3. Analiza postojećeg stanja implementacije IPv6 protokola u Crnoj Gori i postojeći izazovi

## 3.1. Implementacija IPv6 u mrežama javnih elektronskih komunikacionih operatora, državnim institucijama i u kompanijama

U cilju analize postojećeg stanja implementacije IPv6 u Crnoj Gori, prikupljeni su podaci o trenutnom stanju implementacije i eventualnim dodjelama IPv6 adresa, dostupnosti *web* sajtova preko IPv6, kao i o eventualnim planovima implementacije IPv6 u mrežama operatora javnih elektronskih komunikacionih usluga i određenog broja kompanija koje posjeduju razvijene sopstvene informacione sisteme. Pored toga, konsultovana je i RIPE (*Réseaux IP Européens*) baza dodijeljenih IPv6 adresa za subjekte iz Crne Gore [22]. U tabeli 2 dati su podaci o dodjelama IPv6 adresa subjektima u Crnoj Gori sa odgovarajućim ASN (*Autonomous System Number*) brojevima i statusom po pitanju njihove vidljivosti.

*Tabela 2. Podaci o dodjelama IPv6 adresa subjektima u Crnoj Gori*

| **ASN** | **NAZIV** | **IPv6** | ***Status*** |
|---|---|---|---|
| AS60861 | ASREDCAT - D.O.O. Redcat | Nema | |
| AS201649 | CBCGME-AS - Centralna Banka Crne Gore | 2a03:2920::/32 | 2a03:2920::/32 nikada nije bila globalno vidljiva. |
| AS47451 | DOMEN - D.O.O."Domen" Drustvo za Proizvodnju, Promet i Usluge - Podgorica | 2001:678:408::/48 | 2001:678:408::/48 nikada nije bila globalno vidljiva. |
| AS203824 | INFOSME-AS - Info Sistemi d.o.o. | 2a0c:60c0::/29 | 2a0c:60c0::/29 nikada nije bila globalno vidljiva. |
| AS8585 | INTERNET-CG - Crnogorski Telekom a.d.Podgorica | 2a00:fe80::/29 | 2a00:fe80::/29 nikada nije bila globalno vidljiva.<br><br>2a00:fe80::/32 100% od 15.11.2012. god., 16:00:00 UTC. |
| AS62301 | IPMONT-AS - Drustvo za telekomunikacije, promet roba i usluga, export-import IPMONT d.o.o. Podgorica | 2a01:5160::/32 | 2a01:5160::/32 nikada nije bila globalno vidljiva. |
| AS202644 | MEWIRELESS - Wireless Montenegro D.O.O. | Nema | |

| | | | |
|---|---|---|---|
| AS200608 | MIXP - University of Montenegro | 2001:7f8:22::/48 | 2001:7f8:22::/48 nikada nije bila globalno vidljiva. |
| AS51629 | MKABL-AS - Telemach d.o.o. | Nema | |
| AS47881 | MNNEWS-AS - Telenor d.o.o. Podgorica | Nema | |
| AS203506 | MOD-ME - MINISTRY OF DEFENCE OF MONTENEGRO (MINISTARSTVO ODBRANE CRNE GORE) | 2a06:e340::/29 | 2a06:e340::/29 nikada nije bila globalno vidljiva. |
| AS205546 | MONTE-HOSTING - MonteHosting LTD | 2a0b:9e40::/29 | 2a0b:9e40::/29 je bila globalno vidljiva do 28.08.2017. god., 16:00:00 UTC. |
| AS43940 | MTEL-AS - Drustvo za telekomunikacije "MTEL" DOO | 2a03:7a0::/29 | 2a03:7a0::/29 100% vidljiva od 25.01.2018. god., 16:00:00 UTC. |
| AS201777 | MTEL-AS-1 - Drustvo za telekomunikacije "MTEL" DOO | Nema | |
| AS198961 | ORION-TELEKOM-MONTENEGRO - Orion Telekom Tim d.o.o.Beograd | Nema | |
| AS51924 | PORTOMONTENEGRO-AS - Adriatic Marinas d.o.o. | Nema | |
| AS29453 | TELEKOM-MPLS - Crnogorski Telekom a.d.Podgorica | Nema | |
| AS43846 | TELEMACH-AS - Telemach d.o.o. | 2a00:8700::/29 | 2a00:8700::/29 nikada nije bila globalno vidljiva. |
| | | 2a05:7b40::/29 | 2a05:7b40::/29 nikada nije bila globalno vidljiva. |
| AS15397 | TELENORMONTENEGRO - Telenor d.o.o. Podgorica | 2a01:5da0::/32 | 2a01:5da0::/32 nikada nije bila globalno vidljiva. |
| | | 2a03:16a0::/32 | 2a03:16a0::/32 nikada nije bila globalno vidljiva. |
| AS40981 | UNIVCG - University of Montenegro | 2a02:4280::/32 | 2a02:4280::/32 100% vidljiva od 14.02.2013. god.,16:00:00 UTC. |

| | | | |
|---|---|---|---|
| AS203879 | ZAPADBANKA - Zapad banka akcionarsko drustvo – Podgorica | Nema | |
| AS13213 | Drustvo Za Konsalting I Usluge, Export-Import "New Wind D.O.O." Budva | 2a04:7400::/29 | 2a04:7400::/29 nikada nije bila globalno vidljiva. |

U nastavku je, na osnovu prikupljenih podataka, dat pregled trenutnog stanja po pitanju stepena implementacije IPv6 po pojedinim subjektima u Crnoj Gori.

Crnogorski telekom je operator koji pruža javne elektronske komunikacione usluge posredstvom fiksne i mobilne telekomunikacione mreže, uključujući i distribuciju AVM (*AudioVisual Media*) sadržaja. Trenutno stanje po pitanju implementacije IPv6 u mrežama Crnogorskog telekoma može se okarakterisati na sljedeći način:

- svi uređaji u jezgru IP mreže podržavaju IPv6 funkcionalnost;
- IPv6 protokol je aktiviran u *Internet Core* mreži;
- uspostavljeno je BGP (*Border Gateway Protocol*) susjedstvo sa nadprovajderima i podprovajderima;
- na *Internet Gateway* ruterima je oglašen opseg IPv6 adresa koji je dodijeljen Crnogorskom telekomu od strane RIPE-a;
- svi PE (*Provider Edge*) ruteri u IP MPLS (*Multiprotocol Label Switching*) imaju podršku za IPv6, dok je na jednom broju PE rutera konfigurisana podrška za IPv6 protokol;
- infrastruktura u IP MPLS mreži je spremna za pružanje usluga pristupa IPv6 Internetu za poslovne korisnike, kao i aktiviranje IPv6 protokola u korisničkim VPN-ovima (*Virtual Private Network*);
- u ostalim segmentima mreže (IPTV, jezgru mobilne mreže, jezgru mreže za govorni saobraćaj) IPv6 nije aktiviran;
- oko 50% korisničke opreme ima podršku za IPv6.

Dodijeljeni opseg IPv6 adresa od strane RIPE-a Crnogorski telekom trenutno koristi za adresiranje infrastrukturnih linkova unutar jezgra Internet mreže, kao i za adresiranje linkova prema nadprovajderima i podprovajderima. Internet stranica Crnogorskog telekoma nije dostupna preko IPv6.

Crnogorski telekom radi na pripremi pristupa aplikacijama preko IPv6 protokola i na odabiru modela za uvođenje IPv6 protokola za rezidencijalne korisnike (fiksne i mobilne), kao prelaznog modela sa IPv4 na isključivo IPv6.

Za rezidencijalne fiksne korisnike razmatra se prelaz po lw4o6 (*Lightweight IPv4 over IPv6*) modelu, koji podrazumijeva obezbjeđivanje IPv6 podrške za DNS (*Domain Name System*), DHCP i RADIUS (*Remote Authentication Dial In User Service*) servise, aktivaciju IPv6 funkcionalnosti na BRAS (*Broadband Remote Access Server*) čvorištima, uz uvođenje korisničke opreme i aktiviranje funkcija za podršku IPv6 protokola.

Za rezidencijalne mobilne korisnike preferirani model je *dual-stack*. Ovaj model u slučaju mobilne mreže Crnogorskog telekoma podrazumijeva:

- obezbjeđivanje IPv6 podrške za SGSN-MME (*Serving GPRS (General Packet Radio Service) Support Node - Mobility Management Entity*), SGW/PGW/GGSN (*Serving Gateway / Packet Data Network Gateway / Gateway GPRS Support Node*) elemente, kao i za HLR/HSS (*Home Location Register / Home Subscriber Server*) elemente, a u slučaju potrebe i za biling;
- aktivaciju IPv6 funkcionalnosti na DNS i AAA (*Authentication, Authorization, and Accounting*) serverima;
- aktivaciju IPv6 podrške na segmentu RAN-UE (*Radio Access Network – User Equipment*);
- aktivaciju IPv6 podrške na IP čvorištima u jezgru mobilne mreže i u radio pristupnom dijelu mobilne mreže.

Telenor je implementirao IPv6 konektivnost isključivo kao veleprodajni (*wholesale*) servis, pri čemu IPv6 nije implementiran u PS (*Packet Switch*) jezgru mreže. Telenor Srbija, kao odgovarajući nadprovajder ima uspostavljen IPv6 *peering* na svim IPT (*IP Transit*) i IXP (*Internet Exchange Point*) čvorištima.

Telenor raspolaže sa 2x/32 IPv6 adresama alociranim u RIPE bazi (tabela 2). *Web* stranica Telenora nije dostupna preko IPv6, a trenutno ne postoji plan za implementaciju IPv6 u mreži Telenora.

MTEL, koji pored usluga mobilne telefonije pruža i usluge distribucije multimedijalnih AVM sadržaja do krajnjih korisnika, kao i usluge prenosa govora i pristupa Internetu na fiksnoj lokaciji, trenutno ima instaliranu IPv6 podršku na *upstream*-u Internet *gateway*-a ka Telekomu Srbija, kao nadprovajderu. Ovaj operator nema IPv6 korisnike, niti se u mreži interno koristi IPv6.

Telemach, kao operator koji pruža *triple play* usluge (prenos govora, pristup Internetu i distribucija AVM sadržaja), kao i manji operatori kao što su ORION, WiMAX Montenegro, TeleEye i SIOL trenutno nemaju aktiviran IPv6 ni u jednom dijelu mreže.

Kao primjer kompanije koja ima razvijen informacioni sistem sa širokom lepezom e-servisa, a nije telekomunikacioni operator, u pogledu implementacije IPv6 analiziran je sistem Crnogorske Komercijalne Banke (CKB).

Svi segmenti IT sistema CKB-a podržavaju IPv6 na IT infrastrukturnom nivou, ali se trenutno IPv6 adrese ne koriste na sistemima za internu (*Local Area Network* - LAN/*Wide Area Network* - WAN) i eksternu komunikaciju (Internet). *Web* stranica CKB, kao i ostali Internet servisi koje banka pruža trenutno su dotupni isključivo preko IPv4. Crnogorska Komercijalna Banka je više puta u ograničenim okruženjima testirala upotrebu IPv6 protokola, ali se još uvijek nije odlučila za njegovu punu implementaciju, niti trenutno ima usvojen konkretan plan migracije. Pored infrastrukturnih preduslova na mrežnom i aplikativnom nivou za korišćenje IPv6 protokola bila bi potrebna i odgovarajuća konfiguracija opreme i servisa kod Crnogorskog telekoma, kao nadprovajdera informacionog sistema CKB, uz prethodno

usaglašen i odobren plan paralelne podrške servisa banke kroz IPv4 i IPv6 protokole u prelaznom periodu.

Centar informacionog sistema Univerziteta Crne Gore (CIS UCG) ima dodijeljene IPv6 adrese od strane RIPE-a, od kojih je jedna oglašena na *border* ruteru i globalno je vidljiva.

## 3.2. Stanje dodjele IPv6 adresa i dostupnost *web* sajtova preko IPv6 protokola u Crnoj Gori

Na osnovu prethodno sprovedene analize, koja je shodno Projektnom zadatku urađena zaključno sa stanjem na dan 31.05.2018. godine, uočava se da u Crnoj Gori još uvijek niko nije u potpunosti implementirao IPv6 na mrežnom nivou. Stepen spremnosti za implementaciju ovog protokola razlikuje se od slučaja do slučaja. Takođe, ne postoji definisan jedinstven pristup procesu migracije sa IPv4 na IPv6.

Uvidom u RIPE bazu na dan 31.05.2018. godine uočava se da samo 12 subjekata u Crnoj Gori ima dodijeljen IPv6 adresni prostor, od kojih tri imaju globalno vidljive adrese. Nadalje, može se zaključiti da u Crnoj Gori ne postoji nijedna *web* stranica kojoj se pristupa posredstvom IPv6 protokola, niti je sa bilo koje od dodijeljenih IPv6 adresa iz Crne Gore registrovan pristup Google-u primjenom novog protokola.

Na osnovu svega izloženog, može se zaključiti da je pravi trenutak za definisanje jasnih smjernica i preporuka, kako bi se ovaj proces obavio na optimalan način sa odgovarajućom dinamikom, što je i cilj ove Studije.

## 3.3. Izazovi u implementaciji IPv6 u Crnoj Gori

U cilju identifikacije izazova koji se mogu očekivati u implementaciji IPv6 u Crnoj Gori neophodno je klasifikovati kategorije subjekata, sa stanovišta arhitekture njihove računarske mreže i stepena razvoja ICT infrastrukture kojom raspolažu. Te kategorije mogu biti:

- fizičko lice kao individualni korisnik,
- kućna kancelarija/mala kompanija,
- institucija/kompanija srednje veličine,
- velika institucija/kompanija,
- operator javnih elektronskih komunikacionih servisa,
- *data* centar.

Karakteristika kategorije „fizičko lice kao individualni korisnik“ ogleda se u činjenici da se Internet pristup obezbjeđuje od strane operatora javnih komunikacionih usluga. Tipično se radi o pristupu posredstvom mobilnih komunikacionih mreža, WiFi pristupnih tačaka ili pristupu Internetu posredstvom kućnog fiksnog priključka. Uobičajeno korišćeni terminali su pametni telefoni, odnosno laptop/desktop personalni računari s mrežnim pristupom. Kod ove kategorije ključni izazov za implementaciju IPv6 protokola je podrška IPv6 funkcionalnosti od strane korisničke opreme.

„Kućna kancelarija/mala kompanija“ se odnosi na fiksnu instalaciju od nekoliko klijenata s odgovarajućim *Gateway* ruterom, i pristupom Internetu posredstvom Internet provajdera.

Kod ove kategorije izazov za implementaciju IPv6 protokola je podrška IPv6 funkcionalnosti kako od strane korisničke opreme, tako i od strane odgovarajućih elemenata mrežne opreme koja je u vlasništvu imalaca ove kategorije mreža.

Kategorija „institucija/kompanija srednje veličine“ tipično se karakteriše većim brojem klijenata raspoređenih na više lokacija, od kojih neke mogu biti i udaljene, s odgovarajućim *Gateway* ruterima i internim serverima tipa DNS, DHCP i sl., i pristupom Internetu posredstvom Internet provajdera na bazi pristupnih linkova većeg kapaciteta. Ova kategorija najčešće ima javno dostupnu *web* prezentaciju i e-*mail* servis, a često ima i potrebu za pružanjem odgovarajućih *web* servisa. Kod ove kategorije, izazov za implementaciju IPv6 protokola je podrška IPv6 funcionalnosti od strane korisničke opreme, mrežne opreme i odgovarajućih privatnih i javnih servisa.

„Velika institucija/kompanija“ podrazumijeva arhitekturu i obim instalacija principski sličnu prethodnoj kategoriji samo u mnogo većem obimu u odnosu na broj klijenata, mrežnih elemenata, složenosti mrežne arhitekture i broja i kompleksnosti servisa. Izazovi su isti kao kod prethodne kategorije uz mnogo veću kompleksnost, koja pretpostavlja korišćenje WAN mreža, složenih algoritama rutiranja i inovativnih servisa.

„Operator javnih elektronskih komunikacionih servisa“ se može svrstati u prethodnu kategoriju („velika kompanija“) u tehničkom smislu, ali zbog specifičnosti osnovne djelatnosti koju obavlja i uticaja na izazove svih ostalih kategorija zaslužuje posebnu pažnju i ima dodatne izazove. Pored kompleksnih tehničkih izazova, ova kategorija se susreće i sa poslovnim, ekonomskim i strateškim izazovima koji presudno utiču na budućnost ovog subjekta, ali i na prevazilaženje izazova njihovih klijenata i povezanih subjekata.

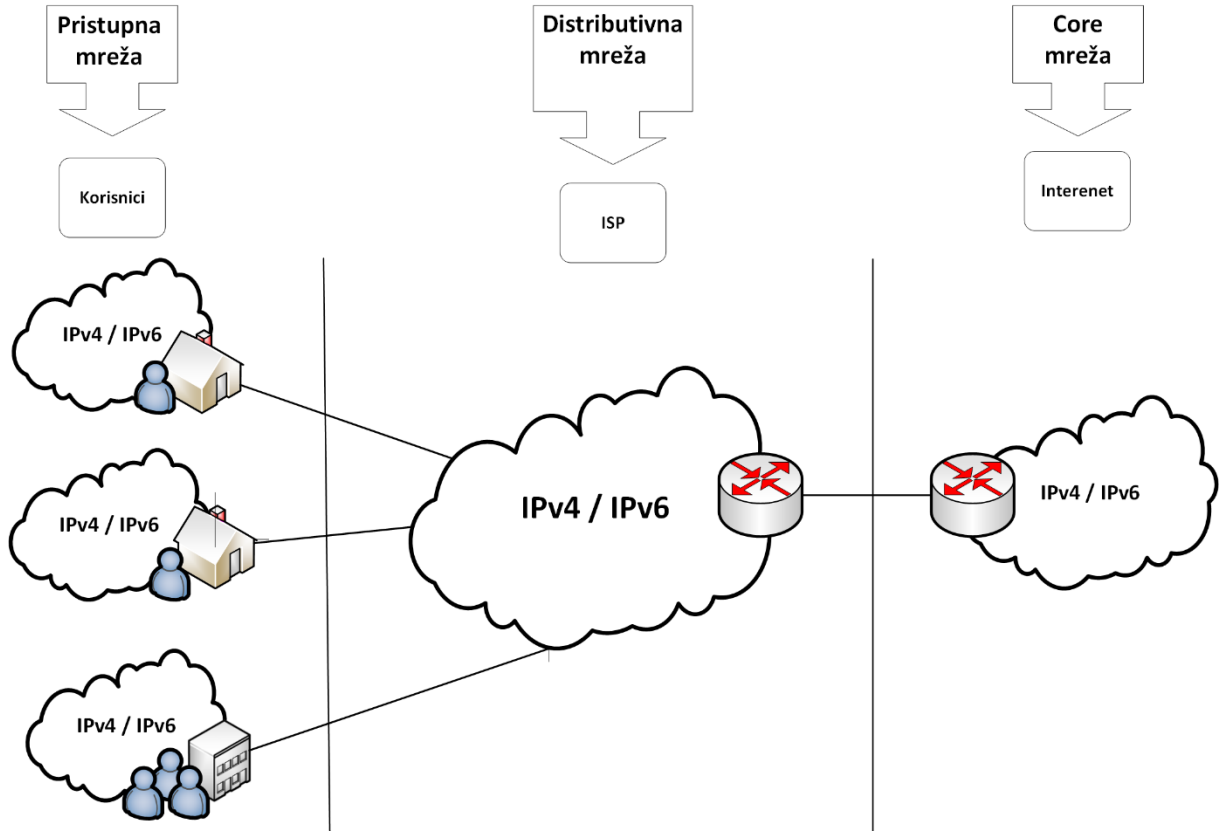
Kategorija „*data* centar“ najčešće podrazumijeva složenu računarsku i mrežnu arhitekturu u virtuelizovanom okruženju, uz kontinualne inovacije i primjenu savremenih rješenja. Karakteristika ove kategorije je i upravljanje hostovima, serverima i servisima drugih institucija/kompanija, kao i pružanje drugih naprednih IT usluga. Kod ove kategorije izazov za implementaciju IPv6 protokola je podrška IPv6 funcionalnosti mrežne opreme, odgovarajućih hostova i servera, te podrška dostupnosti svih servisa u IPv6 verziji.

Generalno govoreći, izazovi svih identifikovanih kategorija u Crnoj Gori imaju zajedničku karakteristiku, koja se ogleda u reakciji relativno stabilnog sistema sa neizbježnom infrastrukturnom promjenom koja traži angažovanje resursa neophodnih za stabilan prelazni proces. Jedini garant stabilnog prelaznog procesa na novu IP verziju je kvalitetno planiranje i projektovanje redizajniranog sistema.

# 4. Analiza potencijalnih metoda implementacije IPv6 - prednosti i nedostaci

## 4.1. Mrežna arhitektura

Internet kao mreža, posmatrana u najširem smislu, može da se podijeli na tri segmenta, kao što je prikazano na slici 11. Pristupna mreža obuhvata krajnje korisnike, distributivnu mrežu čine Internet servis provajderi (ISP), dok okosnica (*core*) mreže obuhvata ostatak Interneta. Naravno, ova podjela je logička i definiše oblasti na koje se treba fokusirati u toku procesa migracije na IPv6.




Slika 11. Model trosegmentnog dizajna mreže

## 4.2. Mehanizmi migracije sa IPv4 na IPv6

Mehanizmi migracije predstavljaju skup metoda koji omogućavaju lakši prelazak na novu verziju IP protokola, kako korisnicima Interneta, tako i ISP-ovima kao nezaobilaznim činiocima procesa razvoja Interneta i pružanja mogućnosti korišćenja naprednih rješenja.

Iako je IPv6 predstavljen 1995. (kao IETF *Proposed Standard*) [9], a 2017. prihvaćen kao Internet standard, njegova implementacija se nije odvijala očekivanom brzinom. Jedan od razloga je i u činjenici da izmjene na fizičkoj mrežnoj infrastrukturi, posebno okosnici mreže, zahtijevaju određeno vrijeme i uslove. Zato su predložene i razvijene mnoge metode i tehnike

za održavanje kontinuiranog rasta globalnog Interneta, kako bi se omogućila podrška za nove tehnologije i veći broj korisnika. U tom kontekstu se i pokazuje optimalnim pristup kojim se omogućava koegzistiranje dva IP protokola i stvara mogućnost za postepeni prelaz sa stare IPv4 na novu IPv6 verziju.

Generalno se mogu identifikovati tri mehanizma ili metoda migracije sa IPv4 na IPv6 i to:

- dvostruka konfiguracija (*dual-stack*),
- translacija i
- tunelovanje.

Svi navedeni mehanizmi imaju svoje prednosti i nose različite izazove. Mehanizmi translacije i tunelovanja se mogu realizovati sa nekoliko prihvaćenih tehnika koje su prezentovane na slici 12. U nastavku će biti ukratko opisani svaki od navedenih mehanizama sa osvrtom na pojedinačne prednosti i izazove u različitim primjenama.

| **Mehanizmi migracije** | | |
|---|---|---|
| *Dual-stack*<br>• Nativni/izvorni<br>• *Dual-stack* sa VLAN-om za IPv6 intranet | Translacija<br>• Samostalna/*statless*<br>• Nesamostalna/*stateful* | Tunelovanje<br>• ručno konfigurisani (6in4)<br>• automatski<br>• 6over4<br>• GRE<br>• 6to4<br>• AYIYA<br>• ISATAP<br>• Teredo<br>• 6rd<br>• 6a44<br>• LISP<br>• SEAL<br>• 6bed4 |

Slika 12. Mehanizmi migracije sa IPv4 na IPv6

### 4.2.1. Dvostruka konfiguracija (*Dual-stack*)

Dvostruka konfiguracija ili *dual-stack* mehanizam omogućava dualizam, tj. koegzistenciju IPv4 i IPv6 protokola kod čvorišta u računarskoj mreži. Kada su mrežne komponente i računarski sistemi, koji koriste komunikaciju baziranu na IP-u, sposobni za razmjenu podataka preko IPv4 i IPv6 paralelno, smatraju se sposobnim za primjenu *dual-stack* mehanizma. Kada će i kako računarski sistemi ili mrežni čvorovi koristiti neki od ova dva IP protokola zavisi od vrste i podešavanja krajnjih tačaka u IP komunikaciji (na primjer, klijenta i servera). Čvorovi koji ne podržavaju oba IP protokola mogu komunicirati sa *dual-stack* čvorovima, ali nemaju mogućnost izbora vrste IP komunikacije, dok *dual-stack* čvorovi biraju verziju IP protokola zavisno od potrebe i podešavanja.

*Dual-stack* čvorovi konfigurišu istovremeno i IPv4 i IPv6 protokol, koristeći neki od aktuelnih mehanizama (za IPv4 DHCP protokol, a za IPv6 konfiguracija prema RFC 2462

[23] ili DHCPv6). Obzirom da čvorovi posjeduju obje verzije IP adresa, izbor IP protokola koji će biti korišćen za slanje IP paketa zavisiće od IP adrese primaoca koju DNS server isporučuje.

Sistem domenskih imena (*Domain Name System* - DNS) se koristi za mapiranje domenskih imena u adekvatne IP adrese, bilo one IPv4 ili IPv6. Novi zapis resursa u DNS sistemu za potrebe vezivanja IPv6 adresa za domenska imena, nazvan "AAAA[2] zapis" (RFC 3596 [24]), omogućuje *dual-stack* razrješavanje domenskih imena. Shodno ovoj verziji DNS zapisa, DNS odgovor ne zavisi od IP verzije na koju je DNS upit poslat, odnosno upit (*nslookup*) može biti na IP verziji različitoj od sadržaja odgovora. Shodno konfiguraciji, DNS može da preferira neku od IP verzija, a to može da specificira i aplikacija koja traži IP adresu u zahtjevu.

Dakle, konfigurisanjem DNS servera i mrežnih uređaja (ruteri, *firewall*-i, …) Internet servis provajderi mogu svojim korisnicima da omoguće *dual-stack* kao jednu od tehnika migracije, što klijentima omogućava pristup i IPv4 i IPv6 orijentisanom Internetu.

#### 4.2.1.1. Izvorni (*native*) *dual-stack*

Izvorni *dual-stack* je potpuna primjena ("prirodna") *dual-stack*-a gdje ISP podržava *dual-stack* mehanizan u svakom segmentu svoje mreže i ne vrši razdvajanje saobraćaja po IP protokolu. U mreži u kojoj je implementiran izvorni *dual-stack* svi elementi sistema treba da podržavaju oba IP protokola. Ovaj mehanizam migracije utiče na sledeće elemente: rutere, svičeve, klijente, servere, *firewall*-e, *proxy*-ije, *gateway*-e nivoa aplikacija, infrastrukturne servise kao što je DNS, kao i operativne sisteme. Aplikacije koje preferiraju IPv4 protokol koriste IPv4 *stack*, a IPv6 aplikacije koriste IPv6 *stack*.

Za upravljanje *dual-stack* okruženjem na putanji između servisa i njegovih korisnika, IP sloj mreže (*Layer* 3) na svim uključenim komponentama mora podržavati IPv4 i IPv6 protokol nezavisno jedan od drugoga. To znači da najmanje sljedeće funkcije moraju biti dostupne za obje verzije protokola:

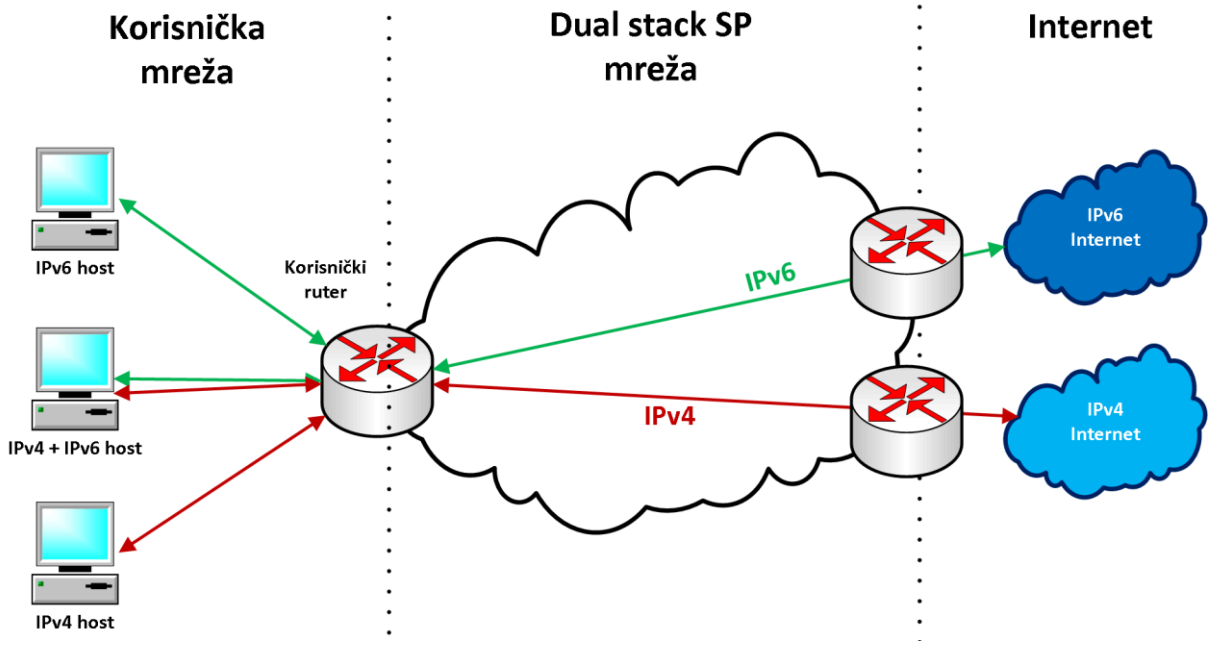
- IP adresa i distribucija IP adrese,
- prosljeđivanje IP paketa,
- IP rutiranje i povezani protokoli,
- filtriranje IP paketa (*firewall*),
- *gateway* nivoa aplikacija (*Application Layer Gateway* - ALG) i
- mogućnost postojanja IPv6-preko-IPv4 tunela koji omogućavaju IPv6 konekcije između klijenata i servera u podmrežama koje nemaju podešene IPv6 adrese.

Prelazak postojećih mreža i sistema na funkcionisanje sa *dual-stack*-om zahtijeva dobro planiran pristup kako bi se održale sve postojeće usluge i funkcionalnosti u mreži. Pored toga, redoslijed prelaska komponenti je od presudnog značaja, pošto treba pravilno odrediti zavisnost između samih komponenti. Detaljan tehnički pregled IPv4/IPv6 operacija *dual-stack* i tehnika migracije se može naći u RFC 4852 ("*IPv6 Enterprise Network Analysis IP Layer 3*") [58]. U ovom RFC-u su opisane različite početne (pre-migracione) situacije i

[2] Zapis IPv6 adrese u DNS-u (AAAA specificira IPv6 adresu)

naznačena je potreba za dobrom pripremom faznog plana za uvođenje IPv6 u IT infrastrukturu.

Na slici 13 je prikazana mreža sa nativnim *dual-stack* mehanizmom.




Slika 13. Mreža sa izvornim *dual-stack* mehanizmom

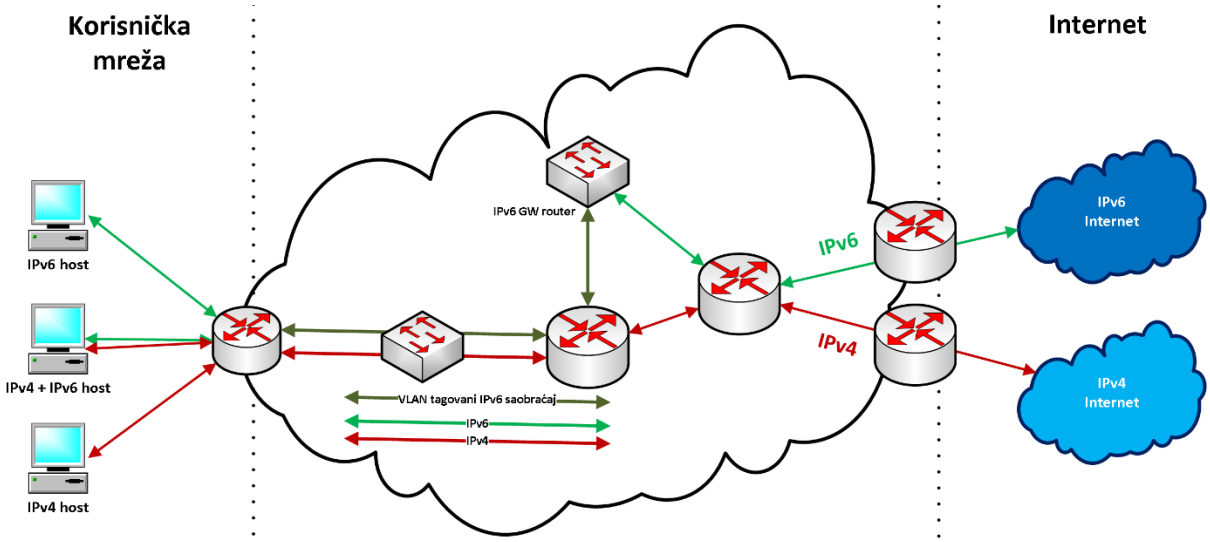
#### 4.2.1.2. *Dual-stack* sa VLAN segmentacijom saobraćaja

Korišćenjem ove tehnike *dual-stack* migracije, IPv6 prenos podataka u LAN mreži (L2 nivo) se može realizovati na odvojenim virtuelnim LAN mrežama (VLAN-ovima), nezavisno od IPv4 saobraćaja koji može koristiti postojeću infrastrukturu. Na ovaj način se omogućava prenos IPv6 saobraćaja (odvajanje) kroz mrežu *Service Provider*-a (SP) na L2 nivou, odnosno da svi ruteri ne moraju podržavati *dual-stack*. Da bi se koristila ova tehnika, uređaji na kojima se odvija ovaj saobraćaj (uglavnom L2 svičevi) moraju podržavati funkcije iz IEEE 802.1Q standarda. Tehnika je opisana u dokumentu RFC 4554 ("*Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks*") [25]. Ova tehnika je zasnovana na ideji da se IPv6 saobraćaj distribuira ka Intranetu isključivo putem Layer 2 VLAN-a. Svičevi koji podržavaju ovu tehniku i mogu se konfigurisati za implementaciju moraju obuhvatiti i transportovati IPv6 saobraćaj preko postojećih IPv4 mrežnih veza, kao što je prikazano na slici 14.

Ilustrovano rješenje bazirano na VLAN-u dovodi do različitih putanja i obrade za IPv4 i IPv6 saobraćaj između istog izvora i odredišta, što može dovesti do različitih kašnjenja u prenosu podataka. U takvim okolnostima pretraživanje mrežnih grešaka može biti izazovno u slučaju da jedna od mrežnih putanja ne radi kako treba. Ovo rješenje ne zahtjeva posredne svičeve i rutere koji podržavaju IPv6. Sa ovom tehnikom krajnji sistemi trebaju podržavati *dual-stack* i imati mogućnost podešavanja i IPv6, pored IPv4. Ovo se odnosi i na IPv6 *gateway* i sigurnosne uređaje povezane s njim, u slučaju IPv6 pristupa preko Interneta.

Ovaj tip migracije se može primijeniti u onim slučajevima gdje IPv6 treba koristiti u postojećoj IT infrastrukturi i gdje je nadogradnja mreže u nativni *dual-stack* iz nekog razloga

neizvodljiva. Ova migraciona tehnologija se ne preporučuje tamo gdje IPv4 i IPv6 mreže treba mapirati na složene VLAN-ove, tj. kada ne bi trebalo da postoje razlike u topologiji između IPv4 i IPv6 podmreža.




Slika 14. Mreža sa *dual-stack* mehanizmom i VLAN-om za IPv6 Intranet

### 4.2.2. Tunelovanje (*Tunneling*)

Kako je to već naglašeno, prelazak sa IPv4 na IPv6 infrastrukturu treba realizovati postepeno, tako da u toku implementacije IPv6 protokola, postojeća IPv4 infrastruktura može biti korišćena i za prenos IPv6 saobraćaja. Tunelovanje je takav mehanizam koji pruža mogućnost da se iskoristi postojeća IPv4 infrastruktura za prenos IPv6 saobraćaja (slika 15). Hostovi i ruteri koji imaju definisane obje vrste adresa, i IPv4 i IPv6 (u daljem tekstu IPv6/IPv4 hostovi i IPv6/IPv4 ruteri) mogu tunelovati IPv6 datagrame preko IPv4 infrastrukture tako što ih enkapsuliraju unutar IPv4 paketa. Tunelovanje može da se realizuje između dva rutera, dva hosta ili između rutera i hosta.

- Tunelovanje između dva rutera (*Router-to-Router*)

IPv6/IPv4 ruteri međusobno povezani sa IPv4 infrastrukturom tuneluju IPv6 pakete između sebe. U ovom slučaju, tunel se prostire na segment mreže između dva krajnja rutera i njime se prenose IPv6 paketi preko IPv4 mreže.

- Tunelovanje između hosta i rutera (*Host-to-Router*)

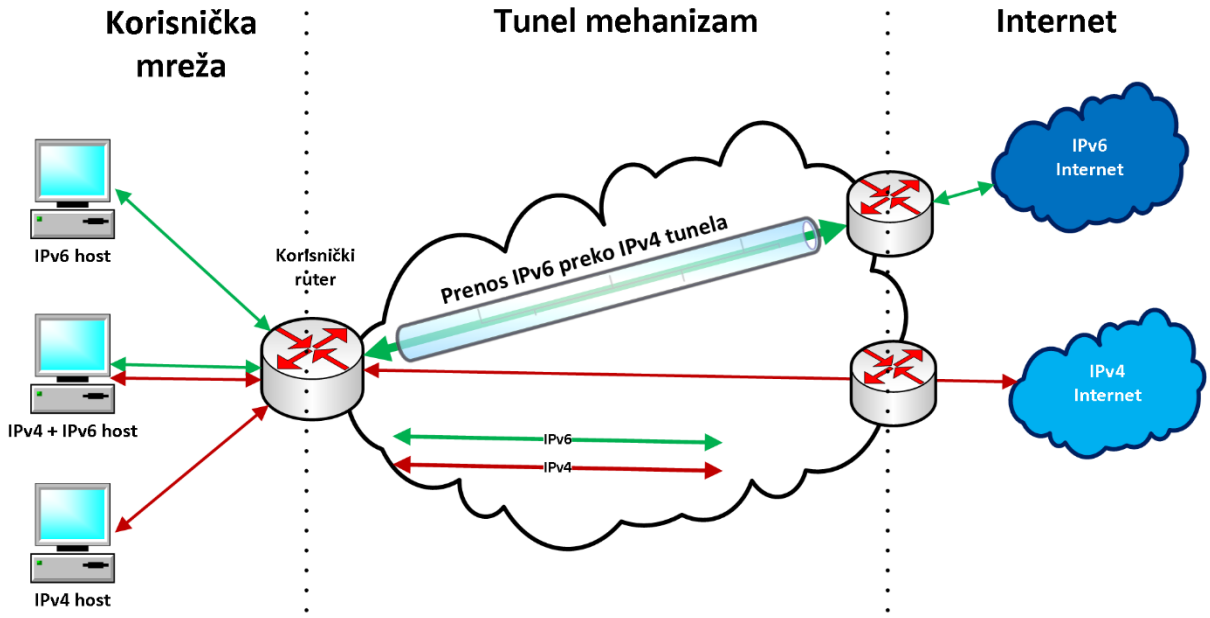
IPv6/IPv4 hostovi mogu tunelovati IPv6 pakete do posredničkog IPv6/IPv4 rutera, koji je dostupan preko IPv4 infrastrukture. Ovaj tip tunela obuhvata prvi segment putanje prilikom slanja IPv6 paketa od nekog hosta do IPv6/IPv4 rutera preko IPv4 mreže.

- Tunelovanje između dva hosta (*Host-to-Host*)

IPv6/IPv4 hostovi koji su međusobno povezani sa IPv4 infrastrukturom mogu tunelovati IPv6 pakete između sebe. U ovom slučaju, tunel se prostire kroz čitavu mrežu, od pošiljaoca do primaoca paketa.

- Tunelovanje između rutera i hosta (*Router-to-Host*)

IPv6/IPv4 ruteri mogu tunelovati IPv6 pakete do njihovog krajnjeg odredišta, tj. IPv6/IPv4 hosta. Ovaj tunel se prostire samo kroz poslednji segment mreže.




Slika 15. Mreža sa tunel mehanizmom

Tuneli se mogu konfigurisati i koristiti u svim gore navedenim slučajevima, ali najviše se u praksi koriste u slučaju *router-to-router* zbog potrebe konfigurisanja krajnjih tačaka za tunele. Osnovni elementi tunelovanja su:

- Ulazni čvor tunela (enkapsulator) enkapsulira IPv4 zaglavlje i prenosi enkapsulirani paket.
- Izlazni čvor tunela (dekapsulator) prima enkapsulirani paket, desegmentira paket ako je potrebno, uklanja IPv4 zaglavlje i obrađuje primljeni IPv6 paket.
- Informacije o stanju za svaki tunel, ako se zahtijeva da enkapsulator to sadrži, kao što je MTU (*Maximum Transmission Unit*) tunela kako bi proslijedio IPv6 pakete kroz tunel.

Prilikom konfigurisanja tunela, adresa krajnje tačke tunela određuje se u enkapsulatoru iz konfiguracionih podataka zapamćenih za svaki tunel. Koji će se paketi tunelovati određuje se na osnovu informacija o rutiranju koje sadrži enkapsulator. Ova operacija se obično vrši preko tabele rutiranja koja usmjerava pakete na osnovu odredišne adrese koristeći masku prefiksa i tehniku podudaranja. Dekapsulator provjerava pakete primljene protokolom-41 (RFC 7059 [26]) na osnovu konfiguracije tunela i dozvoljava samo pakete u kojima izvorišna IPv4 adresa odgovara adresi podešenoj na dekapsulatoru. Stoga operator mora osigurati da je konfigurisana ispravna IPv4 adresa tunela i da je ista i na enkapsulatoru i na dekapsulatoru. Protokol-41 je komunikacioni protokol koji enkapsulira IPv6 paket unutar IPv4 paketa, bez dodavanja dodatnih zaglavlja. Dodatne informacije o konfigurisanju mehanizma tunelovanja mogu se naći u trećem poglavlju „*Basic IPv6 Transition Mechanisms*“ dokumenta RFC 4213.

#### 4.2.2.1. Tehnike tunelovanja

U praksi se koristi veliki broj različitih tehnika tunelovanja, a neke su još u procesu predlaganja i testiranja. Pri tome, jedan broj tehnika je napušten od strane Internet zajednice, neke se i dalje koriste uprkos poznatim nedostacima, dok su se određene tehnike pokazale pouzdanim u procesu implementacije. Takođe, pojedine tehnike tunelovanja su dizajnirane za specijalne slučajeve, dok su druge namijenjene za univerzalniju primjenu. Postoje i dokumentovana ograničenja ovih tehnika, kao i ograničenja koja su se pojavila u procesu implementacije. U nastavku je dat pregled raspoloživih i/ili važnih tehnika tunelovanja i predlog najboljeg izbora za određene svrhe.

Aktuelne tehnike tunelovanja su:

- konfigurisani ili ručni tuneli (6in4),
- automatski tuneli,
- 6over4 (*IPv6 over IPv4 without Explicit Tunnels*),
- GRE (*Generic Routing Encapsulation*),
- 6to4 (*Connection of IPv6 Domains via IPv4 Clouds*),
- AYIYA (*Anything In Anything*),
- ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*),
- Teredo (*Tunneling IPv6 over UDP through NATs*),
- 6rd (*IPv6 Rapid Deployment*),
- 6a44 (*Native IPv6 behind NAT44 CPEs*),
- LISP (*Locator/ID Separation Protocol*),
- SEAL (*Subnetwork Encapsulation and Adaptation Layer*) i
- 6bed4 (*Peer-to-Peer IPv6 on Any Internetwork*).

Automatski tuneli, konfigurisani tuneli, 6over4, 6to4, *Intra-Site Automatic Protocol* za adresiranje tunela (ISATAP) i 6rd rješavaju slične probleme na različitim nivoima. Svi oni enkapsuliraju IPv6 pakete odmah unutar IPv4 paketa, bez dodavanja zaglavlja. Ovaj način enkapsulacije IPv6 paketa se zove "enkapsulacija protokola 41". Ime Protocol 41 je dato jer je polje "*protocol*" u IPv4 zaglavlju podešeno na vrijednost 41 da bi se naznačilo da je ono što slijedi IPv6 paket.

6to4, 6rd, ISATAP i automatsko tunelovanje generišu IPv6 adresu ili opseg IPv6 adresa zasnovane na IPv4 adresi sistema za host ili ruter koji pokreće protokol. Ovo omogućava tehnikama za tunelovanje da utvrde IPv4 odredišnu adresu iz IPv6 adrese destinacije koja se nalazi u spoljašnjem IPv4 zaglavlju, dozvoljavajući automatsko funkcionisanje bez potrebe administrativne konfiguracije krajnje tačke udaljenog tunela.

6over4 i ISATAP pružaju IPv6 konekciju između IPv6 kompatibilnih sistema unutar mreže jedne organizacije koja je inače samo IPv4 orijentisana. 6rd omogućava ISP-ovima da obezbijede IPv6 povezivanje sa svojim klijentima preko samo IPv4 infrastrukture. 6to4 direktno omogućava povezivanje sa globalnim IPv6 Internetom bez uključivanja ISP-a.

Konfigurisani tuneli takođe koriste enkapsulaciju pomoću Protokola 41, ali se oslanjaju na ručnu konfiguraciju krajnje tačke udaljenog tunela. Konfigurisani tuneli mogu se koristiti

unutar mreže organizacije, ali se obično koriste pomoću tunel-brokera za povezivanje na IPv6 Internet. GRE je sličan tunelima koji su konfigurisani, ali takođe podržava enkapsulirajuće protokole različite od IPv6.

AYIYA je sličan konfigurisanim tunelima i GRE, ali obično koristi UDP (*User Datagram Protocol*) zaglavlje za bolju kompatibilnost sa NAT-om i obično se koristi sa TIC (*Tunnel Information and Control*) protokolom za uspostavljanje tunela umjesto da se oslanja na ručnu konfiguraciju. Teredo, 6a44 i 6bed4 su slični sa 6to4, osim što su dizajnirani da rade preko NAT-a tako što će se pokrenuti preko UDP-a. Od njih, Teredo i 6bed4 pretpostavljaju da nema uključivanja ISP-a, a 6a44 pretpostavlja da je ISP uključen. 6bed4 je dizajniran za rad preko direktnih IPv4 putanja između *peer*-ova kad god je to moguće.

LISP [27] je protokol kod koga se razdvaja identitet sistema od svoje lokacije na Internetu i/ili unutrašnjoj mreži. Adrese sistema se nazivaju identifikatori krajnjih tačaka (*Endpoint Identifiers* - EID), a adrese *gateway*-ova nose naziv "ruting lokatori" (*Routing Locators* - RLOCs). Moguće je koristiti IPv6 EID sa IPv4 RLOCs i time koristiti LISP za tunelovanje IPv6 preko IPv4. LISP definiše sopstvene formate za enkapsulaciju paketa podataka i za kontrolne poruke. Svi takvi paketi se enkapsuliraju i šalju preko UDP-a. Paketi podataka koriste port 4341, a kontrolni paketi koriste port 4342.

SEAL i njene prateće tehnologije (*Virtual Enterprise Traversal* - VET, *Asymmetric Extended Route Optimization* - AERO, *Internet Routing Overlay Network* - IRON, i *Routing and Addressing in Networks with Global Enterprise Recursion* - RANGER) pružaju konfigurisan tunelski sistem za IPv6-in-IPv4 tunelovanje na podrazumijevanu vrijednost rutera, kao i automatsko otkrivanje krajnjih tačaka tunela za optimizaciju više specifičnih ruta.

Više informacija o navedenim tehnikama tunelovanja može se naći u RFC 7059 [26].

#### 4.2.2.2. Evaluacija tehnika tunelovanja

Evaluacija i poređenje gore navedenih tehnika tunelovanja vrši se na osnovu sledećih kriterijuma:

- efikasnost korišćenja IPv4 adrese,
- podržane mrežne topologije,
- robustnost,
- stanja *gateway-a* i
- performanse.

**Efikasnost korišćenja IPv4 adrese**

Iscrpljivanjem IPv4 adresnog prostora, mogućnost implementacije mehanizma tunelovanja iza NAT-a, kao i broj IPv6 pretplatnika, podmreža i broj pojedinačnih čvorova koji se mogu podržati iza jedne IPv4 adrese, postali su važni parametri za razmatranje. Ovi parametri su od manje važnosti za mehanizme tunelovanja koji pružaju IPv6 povezanost između čvorova unutar istog administrativnog domena, kao što su ISATAP ili 6over4, jer mogu koristiti privatne IPv4 adrese. Ovo važi i za 6rd tehniku, jer se ona koristi između ISP-a i *gateway*-a sa strane klijenta, kada je kod ISP-a implementiran NAT.

6to4 ne može raditi iza bilo koje vrste NAT-a. Većina drugih mehanizama zasnovanih na Protokolu 41 mogu raditi iza NAT-a, generalno gledano. U praksi ova razlika nije toliko velika, jer Protokol 41 enkapsulacija ne pruža nikakva polja koja omogućavaju NAT-u demultipleksiranje tunelovanih paketa. Posledica ovoga je da konfigurisani tuneli (kao i 6to4) nisu kompatibilni sa ISP-ima koji koriste NAT-ovanje, gdje više korisnika dijeli istu IPv4 adresu.

Teredo, 6a44, 6bed4, AYIYA, SEAL i TSP su dizajnirani za rad preko NAT-ova i koriste UDP zaglavlje, tako da jedna IPv4 adresa može biti domaćin za više tačaka IPv6 tunela. S druge strane, Teredo pruža IPv6 povezivost samo jednom hostu.

Tabela 3 prikazuje koliko IPv4 adresa zahtjeva svaki mehanizam tunelovanja i koliko IPv6 čvorova može povezati. Mehanizmi su navedeni u rastućem redoslijedu gledano po broju podržanih IPv6 čvorova po IPv4 adresi.

*Tabela 3. Tunelovani IPv6 čvorovi po IPv4 adresi*

| Mehanizam | Broj tunela po IPv4 adresi | Broj IPv6 čvorova po tunelu | Javna IPv4 adresa | NAT kompatibilnost |
|---|---|---|---|---|
| **Auto. tun.** | Jedan | jedan | obavezna | ne |
| **6to4** | Jedan | više | obavezna | ne |
| **LISP** | Jedan | više | obavezna | ne |
| **6rd** | Jedan | više | nije obavezna | ne |
| **Conf. tun.** | Jedan | više | nije obavezna | ograničena |
| **GRE** | Jedan | više | nije obavezna | ograničena |
| **Teredo** | Više | jedan | nije obavezna | da (*) |
| **6bed4** | Više | više | nije obavezna | da |
| **6a44** | Više | više | nije obavezna | da |
| **AYIYA** | Više | više | nije obavezna | da |
| **SEAL** | Više | više | nije obavezna | da |

* Iako je Teredo dizajniran za NAT kompatibilnost, on ne funkcioniše kroz sve postojeće NAT-ove.

**Podržane mrežne topologije**

Postoje dva načina korišćenja IPv6-u-IPv4 tunela za povezivanje na IPv6 Internet: pomoću tunela *point-to-point* do tunel brokera ili ISP-ovog *gateway*-a ili korišćenjem ne *broadcast*-nog višepristupnog (*Non-Broadcast Multi-Access* - NBMA) tunela i bilo kakvih javnih *gateway*-a. Prednosti modela *point-to-point* su predvidljive performanse i fleksibilnost u vezi s korišćenim IPv6 adresama. Prednost modela NBMA je u tome što saobraćaj između dva čvora ili dvije mreže koje obje koriste mehanizam, mogu direktno komunicirati bez prolaska kroz *gateway* (direktna *peer-to-peer* komunikacija). Dodatna prednost NBMA modela s javnim *gateway*-ima je automatska konfiguracija i ne uključivanje ISP-a. Nažalost, prednosti ovog NBMA javnog *anycast* modela ima svoju cijenu: oba načina povezivanja i *peer-to-peer* između korisnika i povezanost sa nativnim IPv6 Internetom mogu imati problem sa pouzdanošću i performanama.

*Anycast* mehanizam omogućava korisnicima tunela da koriste najbliže *gateway*-e za povezivanje s IPv6 Internetom jednostavnim davanjem iste adrese svakom *gateway*-u. Protokoli rutiranja zatim biraju najkraći put do *gateway*-a. Međutim, ovo ima za posljedicu da je ovaj put zauzet tuneliranim paketima i samim tim teško predvidljiv i na njega je teško uticati. Uobičajeno je za dupleks saobraćaj da se koriste različiti *gateway*-i, što dodatno otežava otkrivanje i uklanjanje grešaka.

Prednost tunela koju pruža ISP ili broker tunela je što postoji jasna odgovornost za pružanje dobre usluge sa dobro održavanim *gateway*-ima.

U tabeli 4 je dat prikaz podržanih tehnologija za različite tipove mehanizama tunelovanja.

*Tabela 4. Podržane topologije po mehanizmu tunelovanja*

| **Mehanizam** | ***Peer-to-peer*** | **Ko obezbjeđuje *gateway*** |
|---|---|---|
| **Conf. tun.** | Nema | ISP ili tunnel broker |
| **AYIYA** | Nema | ISP ili tunnel broker |
| **GRE** | Nema | N/A |
| **6a44** | U okviru određenog domena | ISP |
| **6rd** | U okviru određenog domena | ISP |
| **6over4** | Globalno | N/A |
| **ISATAP** | U okviru određenog domena | Svoja organizacija |
| **Teredo** | Globalno | Javni |
| **6to4** | Globalno | Javni ili ISP |
| **6bed4** | Globalno | Javni ili ISP ili tunnel broker |
| **Auto. tun.** | Globalno | N/A |
| **LISP** | Podesivo | ISP ili tunnel broker |
| **SEAL** | Podesivo | ISP ili tunnel broker |

**Robustnost**

Tuneli mogu prestati da funkcionišu iz tri glavna razloga:

- kada su tunelirani paketi filtrirani (obično pomoću *firewall*-a),
- kada se promijeni IPv4 adresa krajnje tačke tunela ili
- zbog problema sa NAT-om.

Ako krajnja tačka tunela dobije novu adresu, druga strana tunela treba da zna da je potrebno da šalje pakete na novu adresu. Sa mehanizmima koji izvlače IPv6 adresu iz IPv4 adrese, prethodne IPv6 adrese postaju nedostupne, a nove IPv6 adrese moraju biti tačno konfigurisane. Neki mehanizmi tunelovanja ne rade kroz NAT, ili su ograničeni kada rade kroz NAT. NAT mapiranje se obično može kreirati samo za saobraćaj od "iznutra" ka "spolja", ali ne i za saobraćaj izvan NAT-a za mrežu koja se nalazi iza NAT-a.

Mehanizmi tunela od tačke do tačke ne uspijevaju uvijek da uspostave tunel. Zato tuneli od tačke do tačke mogu podržavati protokole rutiranja, koji automatski preusmjeravaju saobraćaj oko neuspjelog tunela. Neki mehanizmi tunelovanja koriste javne *gateway*-e kako bi došli do

nativnog IPv6 Internet-a. Javni *gateway*-i mogu i ne moraju biti operativni i/ili dostupni. Takođe mogu imati ograničen učinak, zavisno od udaljenosti i upotrebe. Mehanizmi tunelovanja koji koriste modele komunikacije *broadcast* ili NBMA pristup mogu imati probleme zbog nekih kombinacija krajnjih tačaka tunela. Tabela 5 prikazuje mehanizme tunelovanja koji omogućavaju povezivanje na IPv6 Internet po redosljedu smanjenja robustnosti. Međutim, čak i manje robustni mehanizmi mogu dobro funkcionisati u odgovarajućim okruženjima.

*Tabela 5. Osjetljivost mehanizama tunelovanja na probleme*

| **Mehanizam** | **Promjena adrese krajnje tačke** | **Glavni problemi** |
|---|---|---|
| **LISP** | automatski | Nema |
| **6rd** | prekidom | Nema |
| **AYIYA** | automatski | Problem sa mapiranjem tranzitnog NAT-a |
| **Conf. + Heartbeat** | prekidom | Protokol 41 filtriranje, konkurencija za NAT mapiranje |
| **Conf. tun.** | neuspjeh | Protokol 41 filtriranje, konkurencija za NAT mapiranje, promjena adresa |
| **GRE** | neuspjeh | Protokol 41 filtriranje, promjena adrese |
| **6a44** | prekidom | NAT mapiranje prema *peer*-ovima |
| **6bed4** | prekidom | NAT mapiranje prema *peer*-ovima |
| **6to4** | prekidom | Filtriranje omogućeno, *gateway* performanse |
| **Teredo** | prekidom | NAT kompatibilnost, mapiranje prema *peer*-ovima |

**Stanje *Gateway-a***

Postoji dodatno razmatranje koje je važno operatorima *gateway*-a koji povezuju IPv6-u-IPv4 tunele sa IPv6 Internetom: koliko stanja zahtijeva mehanizam tunela.

6to4, 6rd, 6a44 i 6bed4 ne zahtijevaju ni jedno stanje: kad se enkapsuliraju IPv6 paketi unutar IPv4 paketa, IPv4 odredišna adresa je direktno sadržana u odgovarajućim bitovima IPv6 odredišne adrese. Ovo omogućava da sve moguće tunelovane destinacije budu direktno dostupne preko jednog virtuelnog interfejsa.

Teredo releji održavaju spisak *peer*-ova i namijenjeni su za servisiranje ograničenog broja čvorova. Međutim, Teredo server je samostalna komponenta *gateway*-a. Sa konfigurisanim tunelima, GRE, AYIYA i SEAL, nemaju direktnog mapirajućeg djela IPv6 odredišne adrese na IPv4 odredišnu adresu. Tipična implementacija ovih mehanizama ima virtuelni tunelski interfejs za svaki tunel. Paketi se prosleđuju na ispravan virtuelni interfejs na osnovu provjere tabele rutiranja. Tabele rutiranja mogu postati jako velike, ali i dalje ostati brze, tako da je

broj virtuelnih interfejsa ograničavajući faktor za *gateway*-e tunela. AYIYA i SixXS *Heartbeat Protocol* takođe prate dostupnost svakog tunela.

**Performanse**

Postoji više razloga zbog kojih je tunelska veza, u pogledu performansi, inferiorna u odnosu na izvornu netunelsku vezu. U suštini, problem nastaje jer tuneli dodaju jedno ili više dodatnih zaglavlja, i zbog toga povećavaju opterećenje. Međutim, za *Ethernet* paket maksimalne veličine (1500 B), dodatno IPv4 zaglavlje iznosi samo 1,3%. Postupak same enkapsulacije nije spor, ali u nekim implementacijama može biti. Veći ruteri koji prosljeđuju pakete koristeći specijalno napravljen namjenski hardver često nemaju CPU (*Central Processing Unit*) visokih performansi. Ako se enkapsulacija tunela radi na ovim uređajima koji imaju relativno spor CPU, performanse će biti gore od uobičajenog hardvera i njegovog prosljeđivanja paketa. Put koji koriste paketi u tunelima može biti duži od puta kojim se kreću paketi koji nisu u tunelima. Ovo može, ali i ne mora dovesti do smanjenja performansi.

U tabeli 6 su date tipične performanse razmatranih mehanizama tunelovanja.

*Tabela 6. Tipične performanse tunela*

| Mehanizam | Dodatni bajtovi | Povećanje putanje |
|---|---|---|
| **Conf. tun.** | 20 | Može biti veliko |
| **Auto. tun.** | 20 | Nema |
| **6over4** | 20 | Nema |
| **GRE** | 28-36 | Može biti veliko |
| **6to4** | 20 | Može biti veliko |
| **AYIYA** | 72 | Može biti veliko |
| **ISATAP** | 20 | Nema |
| **Teredo** | 28-36 | Može biti veliko |
| **6rd** | 20 | Malo |
| **6a44** | 20-28 | Malo |
| **6bed4** | 28 | Može biti veliko |
| **LISP** | 36 | Malo |
| **SEAL** | 24 - promenljivo | Malo |

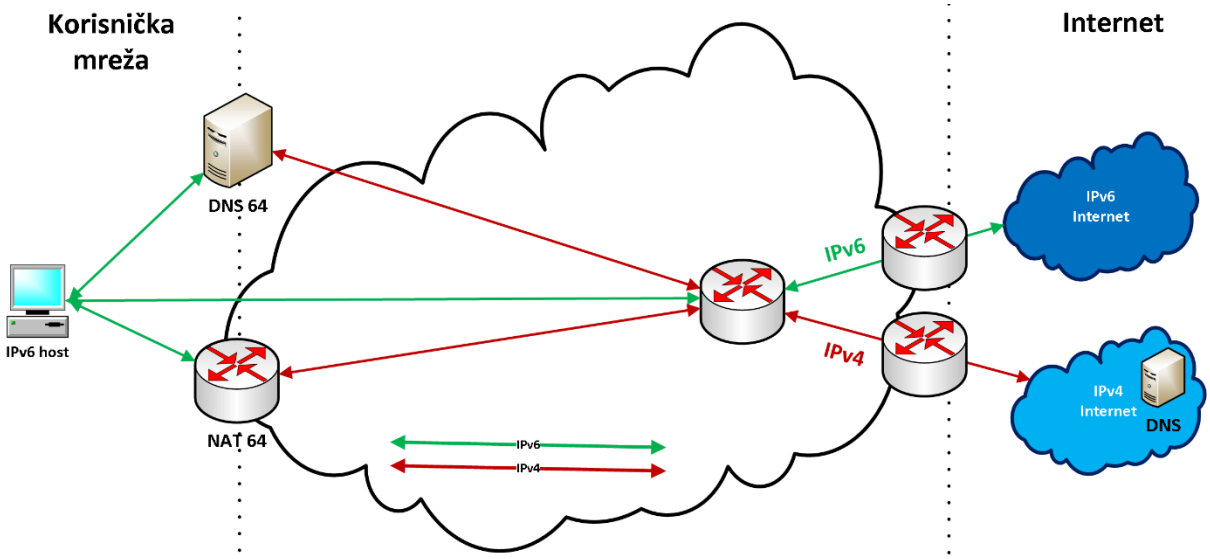
AERO, IRON i RANGER pružaju konfigurisan tunelski sistem za IPv6-in-IPv4 tunelovanje na podrazumijevanu vrijednost rutera, kao i automatsko otkrivanje krajnjih tačaka tunela za optimizaciju više specifičnih ruta.

Više informacija o navedenim tunelskim tehnikama može se naći u RFC 7059 [26].

### 4.2.3. Translacija protokola (*Protocol Translation*)

Translacija protokola omogućava korisniku mreže, bez obzira da li je u pitanju tranzitna, pristupna ili krajnja mreža, da pristupi servisima mreže i komunicira sa drugim korisnicima bez obzira na protokole koje oni koriste – naravno uz postojanje određenih granica (slika 16).

Ono što je glavna karakteristika translacionih mehanizama je pretvaranje jednog IP paketa u drugi korišćenjem nekog metoda mapiranja ili algoritma prevođenja i pamćenja informacija o tome. Ovo je dosta zahtjevan i kompleksan mehanizam koji značajno opterećuje uređaj koji vrši translaciju, a vrlo često izaziva i određene probleme kod velikog broja poznatih servisa. IPv4/IPv6 translacioni mehanizam ne treba da bude dugoročna strategija, ali može se iskoristiti kao srednjoročna strategija koja može olakšati dugoročno program migracije.




Slika 16. Mreža sa translacionim mehanizmom

**Scenariji za translaciju IPv4/IPv6**

Važno je napomenuti da izbor rješenja za translaciju i pretpostavke o mreži u kojoj se koriste utiču na rezultate. Translator za opšti slučaj može da ima brojne probleme, koje translator za određenu situaciju možda neće imati uopšte. Svi slučajevi translacije IPv4/IPv6 mogu lako da se definišu na sljedeći način: interoperacije između skupa sistema (aplikacija) koje komuniciraju koristeći samo IPv4 i skupa sistema koji komuniciraju koristeći samo IPv6.

Na osnovu plana migracije, postoje četiri vrste slučajeva translacije IPv4/IPv6:

a. Interoperacija između IPv6 mreže i IPv4 Interneta,
b. Interoperacija između IPv4 mreže i IPv6 Interneta,
c. Interoperacija između IPv6 mreže i IPv4 mreže i
d. Interoperacija između IPv6 Interneta i IPv4 Interneta.

Svaki od gore navedenih slučajeva može se podijeliti u dva scenarija, u zavisnosti od toga da li IPv6 ili IPv4 strana inicira komunikaciju, tako da postoji ukupno osam scenarija:

1. IPv6 mreža na IPv4 Internet,
2. IPv4 Internet za IPv6 mrežu,
3. IPv6 Internet na IPv4 mrežu,
4. IPv4 mreža na IPv6 Internet,
5. IPv6 mreža za IPv4 mrežu,
6. IPv4 mreža za IPv6 mrežu,
7. IPv6 Internet na IPv4 Internet i

8. IPv4 Internet na IPv6 Internet.

**Režim rada**

Po režimu rada u određenim scenarijima, predložena rješenja za translaciju IPv4/IPv6 mogu se podjeliti na dva tipa i to na nesamostalne i samostalne mehanizme translacije.

- Nesamostalni (*Stateless*) translacioni mehanizam

Ovim tipom translacionog mehanizma informacije o translaciji se prenose u samu adresu, a konfiguracija translator/prevodioca omogućava inicijalizaciju sesije i od IPv4 ka IPv6 i od IPv6 ka IPv4. Dakle, nije potrebno pamćenje parova adresa koje su translirane ili načina translacije. Ovaj mehanizam podržava transparentnost adrese od početka do kraja i ima bolju skalabilnost u poređenju sa nesamostalnim translacionim mehanizmom [29]. Samostalni mehanizmi prevođenja obično postavljaju ograničenja koje IPv6 adrese mogu biti dodijeljene IPv6 čvorovima koji žele da komuniciraju sa IPv4 odredištima koristeći algoritamsko mapiranje. Za Scenario 1 („IPv6 mreža na IPv4 Internet“), to nije ozbiljan nedostatak, pošto se politika primjene adrese može primijeniti da zadovolji ovaj zahtjev za IPv6 čvorove koji trebaju komunicirati sa IPv4 Internetom. Pored toga, ovaj mehanizam podržava Scenario 2 („IPv4 Internet na IPv6 mrežu“), što znači da serveri mogu direktno da se prebace na IPv6 bez prolaska kroz period migracije, a takođe to mogu učiniti bez rizika od gubitka povezanosti sa IPv4 Internetom.

Ovaj tip translacionog mehanizma može se koristiti za scenarije 1, 2, 5 i 6, tj. podržava „IPv6 mrežu na IPv4 Internet“, „IPv4 Internet za IPv6 mrežu“, „IPv6 mrežu za IPv4 mrežu“ i „IPv4 mrežu za IPv6 mrežu“.

Detaljne informacije o implementaciji samostalnog translacionog mehanizma mogu se naći u RFC 6144 „Framework for IPv4/IPv6 Translation“ [28], RFC 6145 „*IP/ICMP Translation Algorithm*“ [29] i RFC 6052 „*IPv6 Addressing of IPv4/IPv6 Translators*“ [31].

- Samostalni (*Stateful*) translacioni mehanizam

Ovim tipom translacionog mehanizma stanje translacije se održava između IPv4 parova adresa/port i IPv6 parova adresa/port, omogućavajući IPv6 sistemima da otvore i uspostave sesije sa IPv4 sistemima [29], [30].

Ovaj mehanizam može se koristiti za scenarije 1, 3 i 5, tj podržava „IPv6 mrežu na IPv4 Internet“, „IPv6 Internet na IPv4 mrežu“ i „IPv6 mrežu za IPv4 mrežu“.

Za Scenario 1, svaka IPv6 adresa u IPv6 mreži može da koristi nesamostalnu translaciju. Međutim, ovaj scenario obično je podržan samo ako je iniciran od strane IPv6. Osim toga, ne rezultira stabilnim adresama za IPv6 čvorove koji se mogu koristiti u DNS-u, što može izazvati probleme za protokole i aplikacije koje su osjetljive na „veoma dinamične“ adrese.

Scenario 3 se bavi serverima koji koriste privatne IPv4 adrese [33] i dostupni su na IPv6 Internetu. Ovo uključuje slučajeve servera koji se iz nekog razloga ne mogu nadograditi na IPv6 i nemaju javnu IPv4 adresu, a ipak treba da dođu do IPv6 čvorova u IPv6 Internetu. Slično ovome, i za scenario 5 može se koristiti nesamostalni mehanizam.

Detaljne informacije o implementaciji samostalnog translacionog mehanizma mogu se naći u RFC 6145 „*IP/ICMP Translation Algorithm*“ [29], RFC 6146 „*Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*“ [30] i RFC 6052 „*IPv6 Addressing of IPv4/IPv6 Translators*“ [31].

#### 4.2.3.1. Komponente translacije

Translacija kao prelazni mehanizam sadrži sledeće komponente:

- translacija adresa,
- IP i ICMP (*Internet Control Message Protocol*) translacija,
- održavanje stanja translacije,
- DNS64 i DNS46,
- ALG za druge protokole sloja aplikacija (npr. FTP (*File Transfer Protocol*)).

**Translacija/Prevod adresa**

Kada se izvrši translacija IPv6/IPv4, trebalo bi se navesti kako je pojedinačna IPv6 adresa prevedena na odgovarajuću IPv4 adresu i obrnuto, u slučajevima gde je korišćeno algoritamsko mapiranje. Ovo uključuje izbor IPv6 prefiksa i izbor metode kojom je ostatak IPv6 adrese izveden iz IPv4 adrese [31].

Za *stateless* i *stateful* translaciju, algoritamsko mapiranje tabela se koristi za prevođenje IPv6 odredišnih adresa (IPv4 pretvorene adrese) na IPv4 odredišne adrese u smjeru od IPv6 ka IPv4 i prevođenje IPv4 izvornih adresa u IPv6 izvorne adrese (IPv4 pretvorene adrese) u smjeru od IPv4 ka IPv6. Treba imati na umu da će prevođenje IPv6 izvornih adresa na IPv4 izvorne adrese u smjeru od IPv6 ka IPv4 i prevođenje IPv4 adresa odredišta u IPv6 adrese odredišta u smjeru IPv4-u-IPv6 biti drugačije za *stateless* i *stateful* translaciju.

Za *stateless* translaciju, ista algoritamska tabela mapiranja se koristi za prevođenje IPv6 izvornih adresa na IPv4 izvorne adrese u smjeru od IPv6 ka IPv4 i prevođenje IPv4 odredišne adrese na IPv6 odredišne adrese od IPv4 ka IPv6 smjeru. U ovom slučaju blokovi IPv4 adresa provajdera su mapirane u IPv6 i koriste se od strane fizičkih IPv6 čvorova. Originalni blokovi IPv4 adresa provajdera se koriste da predstavljaju fizičke IPv6 čvorove u IPv4. *Stateless* translacija podržava i IPv6 i IPv4 inicirane komunikacije.

Za *stateful* translaciju ne koristi se algoritamska tabela mapiranja, a umjesto toga koristi se tabela stanja za prevođenje IPv6 izvornih adresa u IPv4 izvorne adrese u pravcu od IPv6 ka IPv4 i prevođenje IPv4 odredišnih adresa na IPv6 odredišne adrese u smjeru od IPv4 ka IPv6. U ovom slučaju blokovi IPv4 adresa provajdera usluga se održavaju u translatoru kao IPv4 adresne grupe i dinamički su vezane za specifične IPv6 adrese. Originalni blokovi IPv4 adresa provajdera se koriste da predstavljaju IPv6 adresu u IPv4. Međutim, zbog dinamičkog vezivanja, *stateful* prevod generalno podržava samo komunikaciju koja je inicirana od IPv6.

**IP i ICMP translacija**

IPv4/IPv6 translator bazira se na *Stateless IP/ICMP Translation* (SIIT) algoritmu opisanom u RFC 2765 [32]. Algoritam vrši translaciju između IPv4 i IPv6 zaglavlja paketa (uključujući ICMP zaglavlja). IP i ICMP dokument RFC 6145 [29] govori o translaciji zaglavlja za oba

tipa *stateless* i *stateful*, ali ne pokriva održavanje stanja u *stateful* modu. U *stateless* režimu, translacija se vrši kombinacijom prenijetih informacija u adresi i informacijama konfigurisanim u translatoru. Ovo dozvoljava uspostavljanje sesije i od strane IPv4 u IPv6 i od strane IPv6 u IPv4. U *stateful* modu, stanje translacije se odvija između IPv4 adrese/transportnih portova i IPv6 adrese/transportnih portova, omogućavajući IPv6 sistemima da otvore sesije sa IPv4 sistemima. Izbor operativnog režima vrši operator koji koristi mrežu i mora se povesti računa pri izboru jer je kritičan za rad aplikacija koje ga koriste.

**Održavanje stanja translacije**

Za *stateful* translator, osim IP i ICMP translacije, posebno se mora obratiti pažnja na održavanje stanja translacije. RFC 6146 „*Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*“ opisuje mehanizam za održavanje stanja [30].

**DNS64 i DNS46**

DNS64 [34] i mogući budući dokumenti DNS46 opisuju mehanizme na osnovu kojih DNS translator treba da radi. Dizajniran je da radi na poznatom algoritmu translacije adresa definisanom u RFC 6052 „*IPv6 Addressing of IPv4/IPv6 Translators*“ [31]. Postoje najmanje dvije moguće implementacije DNS64 i DNS46:

- Statični zapisi: unos u DNS sa odgovarajućim A[3] i AAAA. Ovaj mehanizam radi za scenarije 2, 3, 5, i 6.
- Dinamički prevod statičkih zapisa: generalno gledano, zapis A se preuzima i prevodi na AAAA zapis od strane DNS64 ako i samo ako nije dostupan AAAA zapis, ili AAAA zapis se preuzima i prevodi na zapis A od DNS46 ako i samo ako ne postoji dostupan zapis A.

**ALG za druge protokole aplikacionog nivoa**

Određene aplikacije zahtijevaju posebnu podršku, kao što je, na primer, FTP. Aktivni režim FTP-a ne funkcioniše dobro u NAT-u bez dodatne podrške kao što je SOCKS [35], [36]. Preko NAT-a se obično koristi pasivni mod. Međutim, kreatori FTP-a su napravili različite i nekompatibilne implementacije pasivnog režima za IPv4 i IPv6 mreže. Stoga, da bi FTP funkcionisao između IP protokola potrebno je ili popraviti FTP, ili prevodilac mora biti napisan za aplikaciju. Druge aplikacije mogu imati slične probleme.

Kao opšte pravilo, jednostavna operativna preporuka koja može da se primjeni kod mnogih problema sa aplikacijama glasi: u svakom domenu bi trebalo da postoji server, ili jedna instanca servera, koji treba da ima interfejs u svakom domenu. Na primjer, SMTP MTA (*Mail Transfer Agent*) može biti zbunjen pronalaskom IPv6 adrese u svom HELO-u kada koristi IPv4 (ili obrnuto), ali će raditi očekivano ako ima interfejs i u IPv4 i u IPv6 domenu i ako se koristi kao most na aplikacionom nivou između njih.

Detaljnije informacije o translacionom mehanizmu mogu se naći u RFC 6144 „*Framework for IPv4/IPv6 Translation*“ [28].

[3] Zapis IPv4 adrese u DNS-u (*A specificira IPv4 adresu*)

## 4.3. Upoređenje mehanizama migracije sa IPv4 na IPv6

Uporedna analiza tri opisane migracione tehnike, na bazi sledećih njihovih funkcija: održavanje sesije preko mreže, transparentnost, kašnjenje, propusnost, skalabilnost mreže, balansiranje opterećenjem, sigurnost i troškovi, predstavljena je u tabeli 7.

*Tabela 7. Uporedna analiza tri migracione tehnike*

| **Osobine** | ***Dual-stack*** | **Translacija** | **Tunelovanje** |
|---|---|---|---|
| Održavanje veze | *End-to-End* | n/a | U okviru tunela |
| Podešavanje | Jednostavno | Kompleksno | Složeno |
| Kašnjenje | Malo | Veliko | Veoma veliko |
| Protok | Veoma veliki | Veliki (uslovno) | Mali |
| Lakoća upravljanja | Jednostavno | Komplikovano | Jednostavnije od translacije, ali komplikovanije od *dual-stack*-a |
| Skalabilnost | Veoma visoka | Veoma niska | Niska |
| *Load balancing* | Ugrađen | Potreban eksterni uređaj | Relativno kompleksno u poređenju sa *dual-stack*-om |
| *Overhead* | Mali | Veliki | Veoma veliki |
| Nivo sigurnosti | Srednji | Mali | Veliki |
| Transparentnost za korisnike | Velika | Veoma mala | Mala |

Iz tabele se jasno vidi da, po svim osobinama, *dual-stack* tehnika predstavlja najbolji izbor u procesu migracije na novi IP protokol. Pored jednostavne primjene, malog kašnjenja, lakog upravljanja, veoma visoke skalabilnosti, ugrađenih algoritama za raspodjelu opterećenja podržava i velike protoke, transparentan je za korisnike. Nedostatak *dual-stack* tehnike se ogleda u većem broju sigurnosnih ranjivosti do kojih može doći zbog dupliranja funkcionalnosti svih čvorova u mreži, dok su iste u slučaju tunelovanja limitirane na krajnje tačke tunela. Pored toga, treba imati u vidu da *dual-stack* tehnika zahtijeva čuvanje i procesuiranje veće količine informacija, što iziskuje angažovanje dodatnih hardverskih resursa na mrežnim uređajima. Mehanizam translacije je najlošiji izbor i kao takav se ne preporučuje, a primjena mu je ograničena na nužne izuzetke u ograničenom trajanju.

## 4.4. Preporuke za korišćenje tehnika migracije

Oba protokola, IPv4 i IPv6, su prisutni u razmjeni podataka na Internetu. Evidentna je ekspanzija IPv6 protokola i on će uskoro postati dominantna verzija Internet protokola, ali će i IPv4 protokol gotovo izvjesno ostati dostupan na Internetu relativno dugi vremenski period. Paralelni rad IPv4 i IPv6 protokola nije samo neizbježan, već je i koristan sa aspekta podrške klijentima koji podržavaju samo jednu verziju. Čak i kada IPv6 bude široko rasprostranjen, za očekivati je postojanje velikog broja sistema koji podržavaju samo IPv4 verziju. Zbog navedenog, neizbježno je paralelno funkcionisanje IPv4 i IPv6 protokola. U tom smislu, IPv4/IPv6 *dual-stack* tehnika je pravi izbor za budućnost.

U daljem tekstu je dat pregled tehnika koje se mogu primijeniti za korišćenje IPv6 protokola u *data* centrima i kompanijama, uz IPv4 protokol, kako bi se postiglo održivo i stabilno rješenje. Pored korišćenja *dual-stack* rješenja, preporučuje se i tunelovanje tamo gdje lokalni IPv6 pristup Internetu još nije dostupan.

Razmotrena su 3 cilja migracije:

1. pristup IPv6 Internetu,
2. IPv6 na radnom mjestu (da klijentski uređaji koriste IPv6) i
3. IPv6 za servere, servise i portale;

Prije migracije na IPv6 treba izvršiti analizu postojeće ICT infrastrukture, izvršiti procjenu spremnosti svake infrastrukturne komponente da podrži IPv6 ili nabaviti novu komponentu.

**Kompanijski pristup IPv6 Internetu**

Da bi čvorovi neke WAN mreže (kompanija, institucija, ...) ostvarili pristup IPv6 Internetu, njen granični ili pristupni WAN ruter (uređaj preko kojeg se ostvaruje Internet konekcija) mora da podrži IPv4/IPv6 *dual-stack* tehniku. Pripadajući ISP bi trebao da ponudi i IPv6 protokol uz IPv4, a idealno bi bilo da i ISP ima *dual-stack*. Treba napomenuti i preporučiti svim imaocima WAN mreža da pri kupovini novih graničnih WAN rutera povedu računa da isti obavezno podržavaju IPv4 i IPv6 protokol.

Ukoliko ISP ne podržava IPv6 protokol, pristup eksternim IPv6 mrežama (kao što je Internet) i dalje se može postići korišćenjem tehnike tunelovanja, ali je to lošiji izbor. Zbog toga bi trebalo dati prioritet *dual-stack* pristupu.

Tehnički, preporučuje se sledeća konfiguracija:

- pristupni ili granični ruter treba da podrži IPv4/IPv6 *dual-stack*;
- ovaj pristupni ruter bi trebalo da dobije IPv6 pristup od ISP-a;
- ako ISP ne pruža IPv6 pristup onda treba uspostaviti fiksni IPv6-u-IPv4 tunel između pristupnog rutera i pouzdanog *tunneling* servera u nekom *data* centru gdje se nalaze traženi podaci bazirani na IPv6 servisima. Za uspostavljanje takvog tunela treba koristiti provjereni tunel broker. Ovaj fiksni tunel se može uspostaviti i preko nekog drugog uređaja unutar mreža, a da pristupni WAN ruter može ostati sa „starim“ samo IPv4 podešavanjima i funkcijama.

Nezavisno od izbora tehnike za pristup IPv6 Internetu, IPv6 provajder mora imati podržan BGP protokol kako bi oglašavao i usmjeravao IPv6 prefikse predmetne WAN mreže na Internetu. Naravno, to podrazumijeva ispunjavanje određenih administrativnih zahtjeva i sporazuma.

Za bilo koju izabranu tehniku pristupa IPv6 Internetu, trebalo bi definisati i sporazumom precizirati nivo usluga (*Service Level Agreements* - SLA) sa provajderom, kao što bi trebalo i za IPv4 pristup.

Druge tehnike tunelovanja, kao što su 6to4 ili Teredo, ne bi trebalo koristiti zbog prethodno pomenutih nedostataka.

**Radno mjesto ili krajnji korisnici**

Da bi korisnici na radnom mjestu koristili IPv6 protokol (tj. da klijentski uređaji koriste IPv6) svi operativni sistemi, aplikacije i ICT infrastruktura (svičevi, ruteri, intranet serveri, ...) moraju podržavati IPv6 protokol. Takođe, korišćenje IPv6 protokola na radnom mjestu je nezavisno od IPv6 tehnike koja se koristi na nivou Internet pristupa, a intranet WAN pristup mora podržavati IPv6.

Preporučuje se da ICT sistemi na radnom mjestu treba da podržavaju IPv4/IPv6 *dual-stack* i da imaju pristup dvostrukoj ICT infrastrukturi.

Zbog sigurnosnih razloga, ICT sistemi na radnom mjestu ne smiju uspostavljati tunele prema IPv6 Internetu i to se mora spriječiti tehničkim sredstvima (na primjer, na *firewall*-u).

Za rad od kuće preporučuje se, pored IPv4, IPv6 podrška koja se može, na primjer, obezbijediti odvojenim IP ruterom/*gateway*-om ili VPN klijentom koji se povezuje sa kompanijskim VPN serverom.

Za pristup Internetu prenosnim računarom, pametnim telefonom ili tabletom, mobilni korisnik najčešće zavisi od toga da li provajder mobilne mreže podržava IPv6 za svoje korisnike. U slučaju nedostatka IPv6 podrške u mobilnoj mreži, mogu se koristiti tehnike migracije. Međutim, one su često nepouzdane u mobilnim IP mrežama.

**IPv6 za servere, servise i portale**

U prelaznom periodu, preporučuje se da svi javni serveri, servisi i portali podrže IPv6 pristup tako što će se nadograditi sa IPv4/IPv6 *dual-stack* podrškom. Na ovaj način može se osigurati da korisnici postepeno prelaze na IPv6 (zbog nedostatka IPv4 adresa kod svog provajdera), a pri tome kontinuirano mogu koristiti javne servise bez ikakvih tehničkih prepreka. Vjerovatno su korisnici koji putuju u inostranstvo, posebno u Aziju, mogli osjetiti nemogućnost korišćenja servisa koji su dostupni samo na IPv4 protokolu.

Zbog nedostatka IPv4 adresa, broj ISP-a koji podržavaju IPv4 samo na nivou tunelovanja ili NAT-a će se značajno povećati, a time će i kvalitet IPv4 servisa opadati.

Zbog svega navedenog preporučuje se za sve javne servere, servise i portale:

1. da moraju biti dostupni preko IPv4 i IPv6 sa istim kvalitetom usluga;
2. IPv6 pristup se može ostvariti preko odgovarajućeg ISP-a.
    - Ako ISP ne podržava IPv6 protokol, IPv6 pristup može biti obezbijeđen putem sigurne tehnike tunelovanja, koristeći granični ili lokalni ruter ili sigurni uređaj za tunelovanje.
    - SLA za IPv6 pristup treba dogovarati odvojeno od IPv4.
    - Kao prelazno rešenje za „brz“ prelazak na IPv6 za *web* servere i *web*-bazirane portale, preporučuje se upotreba HTTP (*HyperText Transfer Protocol*) tehnike obrnutog *proxy* servera. Konfiguracija postojećih *web* servera se ne mijenja, a dodatni HTTP *proxy* se podešava odvojeno od *web* servera. Softver za pokretanje obrnutog *proxy*-a je dostupan kao *open source* i može biti veoma siguran za korišćenje.

- Aplikacije za portale koje rade sa složenijim *web* tehnikama mogu zahtijevati ažuriranje konfiguracije *web* servera kako bi funkcije portala radile i preko obrnutog *proxy*-a.

Dakle, da bi javni intranet serveri, servisi i portali u budućnosti podržavati IPv6, tj. da bi im se pristupilo preko IPv6, pripadajuća ICT infrastruktura i same usluge moraju podržavati *dual-stack* tehnologiju. U slučaju da IPv6 nije dostupan u svim potrebnim internim mrežama, tada se IPv6 „ostrva“ mogu povezati pomoću IPsec VPN tunela.

# 5. Izazovi implementacije IPv6 koji se odnose na sigurnost i privatnost

Jedan od čestih navoda u stručnoj javnosti oko informaciono-komunikacionih tehnologija je da prvobitni dizajn arhitekture Interneta u potpunosti zanemaruje mehanizme zaštite. Da bi se bolje razumjelo koliko su takvi navodi opravdani, treba poći od toga da je Internet prvobitno koncipiran kao oruđe za istraživanje i razvoj računarskih mreža. Jedna od glavnih motivacija njegovog razvoja je bila dijeljenje računarskih resursa što je rezultiralo razvojem aplikacija za udaljeni pristup (telnet) i prenos datoteka, između ostalih. Rani korisnici su pretežno bili iz akademske zajednice i pristup je bio moguć sa malog broja krajnjih sistema. Kontrola pristupa Internetu se vršila putem fizičkog pristupa krajnjem sistemu, što je ujedno značilo da je odgovornost svakog korisnika u slučaju potencijalnih zloupotreba bila lako dokaziva.

Daljim razvojem Interneta i uvođenjem novijih aplikacija pojavljuju se dodatni zahtijevi, ali se prepoznaju i sigurnosne prijetnje, tako da već sredinom 80-ih godina prošlog vijeka počinje intenzivan rad na razvoju Internet mehanizama zaštite baziranih na kriptografiji. Nastavljajući otvoreni razvojni proces koji je omogućio da Internet postane široko prihvaćen, IETF dalje razvija ove mehanizme pod svojim okriljem objavljujući ih kao *Request for Comments* (RFC) dokumente sredinom 90-ih.

Dok su tehnička rješenja za zaštitu mreža i krajnjih sistema bila spremna relativno brzo nakon prepoznavanja novih zahtjeva, mnogo veći problem je bio dominantan stav u administrativnim krugovima: zašto ulagati resurse u nešto što ne donosi dobit u odnosu na postojeće stanje. Što iz radoznalosti, a što iz malicioznih namjera, uslijedile su razne vrste *cyber* napada, često od strane tinejdžera, koji su rezultirali gubicima procijenjenim i na preko milijardu američkih dolara. Neki od poznatih *cyber* napada i njihova prouzrokovana šteta su prikazani u tabeli 8.

Vremenom, administrativni krugovi su počeli da uviđaju uticaj koji *cyber* napadi mogu imati na poslovanje i na medijsku sliku institucija. Sa dodatnim resursima i motivacijom, više pažnje se počinje posvećivati zaštiti od *cyber* napada i sistemi se polako nadograđuju novim (starim) mehanizmima. Uporedo, kroz novu generaciju Internet standarda, čiji dio su i IPv6 protokoli, dizajneri Internet rješenja inkorporiraju lekcije naučene tokom 90-ih, pa se osim striktno tehničkim aspektima sve više pažnje posvećuje i lakoći korišćenja.

Upotreba nove verzije IPv6 protokola u pojedinim segmentima Interneta otvara nove izazove u oblasti sigurnosti. Prije definisanja tehničkih detalja sigurnosti komunikacionih protokola i sistemskog aspekta, za jednu instituciju je ključno napraviti model prijetnji na osnovu pređašnjeg (IPv4) iskustva kao i uporednog iskustva drugih institucija u Crnoj Gori i inostranstvu. *Koji resursi mogu biti od vrijednosti napadačima? Kompromitacija kojih resursa može narušiti i koliko sliku i povjerenje u instituciju? Da li je to web server institucije ili server na kojem se nalazi korisnička baza podataka sa osjetljivim ličnim podacima? Od*

*koje vrste napada želimo da zaštitimo resurse? Da li su u pitanju cyber napadi nezadovoljnih zaposlenih sa fizičkim pristupom osjetljivim djelovima infrastrukture, eksternog osoblja sa pristupom Internetu, propagacija malware-a širom Interneta, pažljivo ciljani cyber napadi od strane tajnih i javnih službi velikih svjetskih sila koje na raspolaganju imaju super-računare i ogromne resurse?*

Tek sa odgovorima na navedena pitanja je moguće pristupiti projektovanju zaštite konkretnog sistema i odabiru pojedinačnih mehanizama zaštite, koji su razrađeni u daljem tekstu.

*Tabela 8. Neki od medijski bolje propraćenih cyber napada od postojanja Interneta.*

| Godina | Ime | Tip napada | Meta | Procijenjena šteta | Izvor |
|---|---|---|---|---|---|
| 1988 | Morris Worm | Malware/DoS | Internet korisnici | do $96 miliona | [37], [38] |
| 1998 | Solar Sunrise | Malware | Ministarstvo odbrane SAD | neobjavljena | [39] |
| 1999 | Melissa | Malware | Internet korisnici | $80 miliona u SAD, do $1.1 milijardu širom svijeta | [40] |
| 2000 | MafiaBoy | DoS | Yahoo, Amazon, Fifa, eBay, CNN, … | $1,7 milijardi | [41] |
| 2005-2010 | Stuxnet | Malware | Nuklearna postrojenja u Iranu | neobjavljena | [42] |
| 2016 | Dyn | DDoS | DynDNS i preko 80 najvećih *web* stranica | neobjavljena | [43] |

## 5.1. Uticaj IPv6 na sigurnost mreže i korisnika

Nepisano pravilo *cyber* sigurnosti glasi da što je neki sistem kompleksniji, to postoji više potencijalnih ranjivosti i teže ga je zaštititi. Upravo iz tog razloga, jedan od glavnih ciljeva prilikom razvoja IPv6 protokola je bio pojednostavljivanje postojećih funkcionalnosti IPv4 mehanizama. U daljem tekstu je dat pregled funkcionalnosti od značaja sa aspekta sigurnosti prilikom implementacije IPv6 protokola.

### 5.1.1. IP *Security* (IPsec)

IPsec predstavlja kolekciju više protokola koji rješavaju različite aspekte zaštite komunikacije na IP nivou između dva čvorišta: autentifikaciju čvorišta i derivaciju kriptografskih ključeva kroz *Internet Key Exchange* (IKE) i IKEv2 protokole; garantovanje autentičnosti primljenih IP datagrama kroz *Authentication Header* (AH) protokol; garantovanje tajnosti i autentičnosti IP datagrama kroz *Encapsulating Security Payload* (ESP) protokol. AH i ESP protokoli se oslanjaju na kriptografski materijal koji je dobijen nakon izvršavanja IKEv2 protokola između dva čvorišta, ili pak ručno konfigurisan od strane administratora. Prva verzija IPsec protokola je razvijena 90-ih godina, pošto je IPv4 već uveliko bio u upotrebi, pa je stoga i naknadno implementiran i integrisan sa raznim implementacijama TCP/IP steka. Za razliku

od IPv4 specifikacija, IPv6 specifikacija i RFC 4301 čine IPsec protokole obaveznim dijelom bilo koje IPv6 implementacije [44].

U praksi, to znači da je IPsec podržan u svim IPv6 implementacijama koje su usaglašene sa standardom, ali ne i da je u širokoj upotrebi. Naime, praksa je pokazala da IPsec može biti prilično kompleksan za konfiguraciju od strane administratora, što je najčešće i bio izvor sigurnosnih propusta [45]. Takođe, jedan od razloga za malu upotrebu IPsec protokola je i činjenica da je u određenim konfiguracijama tehnički nemoguće postići upotrebu IPsec-a i NAT mapiranja. Na tu temu postoji više objavljenih preporuka i predloženih rješenja [46], [47]. Što se specifikacije IPsec protokola tiče, razlike između IPv4 i IPv6 verzija su minimalne pa je postojeće implementacije IPsec protokola za IPv4 lako prilagoditi IPv6 implementaciji. NIST 800-119 studija daje detaljnu analizu funkcionalnosti IPsec protokola i najbolje prakse njegove konfiguracije [45].

### 5.1.2. ICMPv6 i *Neighbor Discovery*

ICMPv6 predstavlja nezaobilazni dio IPv6 implementacije, kako sa funkcionalnog tako i sa stanovišta sigurnosti. Po IPv6 standardu, od svake link tehnologije se očekuje da je sposobna da podrži IPv6 datagrame veličine najmanje 1280 bajta. Ukoliko to nije slučaj, očekuje se da LLC (*Logical Link Control*) podnivo izvrši (de)fragmentaciju specifičnu za određeni link, tako da IPv6 implementacija o tome ne mora da vodi računa. Bitno je razlikovati ovu vrstu fragmentacije specifičnu za link od fragmentacije na IPv6 nivou, koja se može dogoditi samo na izvornom IPv6 sistemu. Jedna od funkcionalnosti ICMPv6 protokola, preporučena u IPv6 specifikaciji, je i otkrivanje MTU vrijednosti za određenu putanju u mreži, kako bi se maksimizovala efikasnost prenosa podataka korišćenjem datagrama većih od 1280 bajta. Dok sa aspekta efikasnosti korišćenje većih datagrama djeluje privlačno, bitno je napomenuti da mnoge IoT komunikacione tehnologije (IEEE 802.15.4, *Bluetooth Low Energy*, *LoRa*, *Sigfox*) podržavaju prenos značajno manjih okvira (*frame*) na nivou linka. U IETF-u postoje standardi i predlozi standarda ([48], [49]) koji definišu upotrebu ovih tehnologija za prenos IPv6 datagrama, uključujući i fragmentaciju, ali je bitno napomenuti da zbog ograničenja krajnjih sistema u tipičnim IoT aplikacijama (memorija, procesuiranje i energija), upotreba većih datagrama rezultira značajnom degradacijom performansi koja može da uzrokuje i nenamjerni *Denial of Service* napad. Stoga je takve mreže potrebno posebno zaštititi, a preporučljiva je upotreba *firewall*-a kako takav saobraćaj ne bi narušio dostupnost servisa.

Razmjena ICMPv6 poruka je neophodna za pravilno funkcionisanje IPv6 mreža. Pogrešna konfiguracija ICMPv6 parametara može dovesti do potpunog prekida dostupnosti IP servisa. Iz tog razloga, ICMPv6 poruke su veoma korisne napadačima koji imaju za cilj da prouzrokuju štetu. Napadač sa pristupom lokalnoj mreži je u mogućnosti da slanjem pažljivo generisanih ICMPv6 poruka onemogući inicijalizaciju specifičnog interfejsa, simulira prekid dostupnosti nekog od susjeda na linku, preusmjeri saobraćaj ka sebi ili drugim čvorištima u mreži u cilju prisluškivanja i slično. Da bi se zaštitili od ove vrste napada, administratorima se savjetuje pažljiva konfiguracija sigurnosnih komponenti u mreži, kao što su *firewall* ili tabele kontrole pristupa na ruterima. Detaljnije preporuke za filtriranje ICMPv6 saobraćaja putem *firewall* komponenti su date u RFC 4890 informativnom dokumentu [50]. Osim toga, ICMPv6 saobraćaj je moguće kriptografski zaštititi putem IPsec protokola.

### 5.1.3. Rutiranje

Protokoli rutiranja koji podržavaju IPv6 protokol su pretežno unaprijeđene verzije IPv4 protokola. IETF je standardizovao OSPFv3 [51] kao značajnu nadogradnju OSPF (*Open Shortest Path First*) protokola i ovaj protokol se u praksi koristi u većim mrežama. RIPng protokol [52], kao nadogradnja RIPv2 protokola, je popularan zbog lakoće konfiguracije, ali je prikladan za manje mreže. Verzija 4 BGP protokola, koji služi za povezivanje autonomnih sistema, podržava kako IPv4 tako i IPv6 protokol.

Kako protokoli rutiranja imaju jednu od ključnih uloga u funkcionisanju IP mreža, napadi na njih često imaju za posljedicu široku nedostupnost servisa. Zaštita je specifična za protokol, pa se tako RIPng i OSPFv3 oslanjaju na konfiguraciju i upotrebu IPsec protokola. Bitno je napomenuti da je u cilju zaštite protokola rutiranja mnogo bitnije obezbijediti autentičnost podataka nego njihovu poverljivost. Što se zaštite BGP protokola tiče, postoji više mehanizama na raspolaganju. Jedan od njih, GTSM (*Generalized TTL Security Mechanism*) [53], se oslanja na činjenicu da BGP ruter koji je izvor poruke, datagram šalje sa maksimalnom vrijednošću „Hop Limit“ (TTL) polja (255). Maliciozno generisani datagrami van linka koji dospiju na procesuiranje jednog BGP rutera će imati „Hop Limit“ manji od maksimalnog zbog procesuiranja u drugim ruterima na putu, pa ih je stoga lako detektovati. Bitno je napomenuti da je ovaj mehanizam moguće zaobići ukoliko ruter ima ulogu krajnjeg sistema IP tunela, gdje unutrašnje zaglavlje datagrama može ostati nepromijenjeno. Mnogo robusniji mehanizam zaštite BGP-a je korišćenje IPsec protokola između dva rutera.

### 5.1.4. DNS

DNS servis, koji mapira imena domena u IP adrese, je neizostavni dio ogromne većine aplikativnih servisa baziranih na IP protokolima. Stoga je i jedan od neophodnih koraka prilikom implementacije IPv6 protokola konfiguracija AAAA DNS zapisa vezanih za sve komponente mreže koje implementiraju IPv6. Sa aspekta sigurnosti, DNS serveri predstavljaju izuzetno vrijednu metu napadačima, kako zbog dostupnosti tako i zbog sofisticiranih napada u cilju krađe ličnih podataka, finansijskih sredstava i slično. Obzirom da je DNS aplikativni protokol, mehanizmi njegove zaštite sa implementacijom IPv6 protokola ostaju isti kao i sa IPv4 verzijom. To se prije svega odnosi na DNSSEC (*Domain Name System Security Extensions*) [54] ekstenziju koja omogućava kriptografsku zaštitu, ali i filtriranje saobraćaja putem *firewall* komponenti i tabela kontrola pristupa.

### 5.1.5. Automatska konfiguracija IPv6 adresa bez zadržavanja stanja (SLAAC) i DHCPv6

IPv6 protokol omogućava inicijalizaciju IPv6 adrese jednog interfejsa bez centralizovanog servera za dodjelu IPv6 adresa. Ova metoda je poznata kao SLAAC (*Stateless Address Autoconfiguration*). Sa tehničkog aspekta, SLAAC konfiguracija je izuzetno privlačna jer nije potrebno održavati bilo kakav centralizovani server, a konfiguracija rutera je praktično svedena na minimum. Ipak, postoji nekoliko izazova kada se SLAAC koristi u praksi. Jedan od izazova je utvrđivanje odgovornosti u slučaju zloupotreba korišćenja IP servisa, gdje je operatorima neophodno da u svakom trenutku imaju pregled aktivnih korisnika i IP adresa koje koriste. To je tehnički moguće postići na dva načina: 1) na osnovu praćenja alokacije

prefiksa podmreže dodijeljenih registrovanim pretplatnicima; 2) na osnovu pristupa ND (*Neighbor Discovery*) saobraćaju tokom SLAAC konfiguracije. U poglavlju 5.2 je dat pregled aspekata koji se tiču privatnosti adresa konfigurisanih SLAAC metodom.

Kao (nepopularna) alternativa SLAAC konfiguraciji, moguće je korišćenje DHCPv6 protokola, koji je paralela DHCP protokolu široko prihvaćenom u IPv4 mrežama. Sa jedne strane, mana konfiguracije adresa putem DHCPv6 protokola u odnosu na SLAAC je što DHCPv6 server postaje kritična tačka mreže, pa u slučaju njegovog nefunkcionisanja dolazi do prekida dostupnosti servisa. Sa druge strane, prednost korišćenja DHCPv6 se ogleda u činjenici da je teže izvesti DoS napade na pojedinačne krajnje sisteme generisanjem lažnih ND poruka iz iste lokalne mreže. Upotreba DHCPv6 protokola je uzrokovala određene kontroverze u stručnoj javnosti pod argumentom da takva implementacija IPv6 vodi ka ponovnom uvođenju NAT mehanizama. Iz tog razloga, u trenutku pisanja ove Studije, jedan od najvećih operativnih sistema za mobilne uređaje, Android, ne podržava DHCPv6 protokol već samo SLAAC mehanizam.

## 5.2. Uticaj IPv6 na privatnost korisnika i kompanija

Iako je IPv4 protokol dizajniran sa pretpostavkom da će sva čvorišta imati javne IP adrese, pod plaštom NAT mehanizma velika većina Internet korisnika i kompanija koristi dijeljene IP adrese. Ta činjenica je sa tehničkog aspekta unijela nepotrebnu kompleksnost u dizajn Internet aplikacija ali je u isto vrijeme omogućila krajnjim korisnicma (prividnu) privatnost u odnosu na korisnike sa kojima dijele IP adresu. Tačnije, identifikacija pojedinačnog krajnjeg korisnika iza NAT-a je u određenoj mjeri otežana, ali ne i onemogućena najčešće zbog njihovog ponašanja na mreži.

IPv6 omogućava dodjeljivanje javnih adresa svim čvorištima. Zavisno od konfiguracije mreže, adrese mogu biti statičke ili dinamičke. Prednost statičkih adresa je to što omogućavaju tehnički naprednim korisnicima i kompanijama održavanje sopstvene *web* infrastrukture, na primjer *web* ili *mail* servera, bez izlaganja dodatnim troškovima koji su bili neophodni za zakup dodijeljenih IPv4 adresa.

Kako je to već opisano, IPv6 adresa se sastoji od prefiksa, veličine do 64 bita, i identifikatora interfejsa koji mora biti jedinstven u podmreži, veličine 64 bita. Obije ove komponente IPv6 adrese imaju uticaj na privatnost korisnika. Prefiks podmreže kontroliše operator, dok identifikator interfejsa kontroliše krajnji korisnik (preko operativnog sistema).

Ukoliko je prefiks statički, a identifikator interfejsa dinamički, moguće je sa izvjesnošću identifikovati saobraćaj iz jedne podmreže (na primjer, jedne kompanije ili domaćinstva). Ukoliko je prefiks dinamički, a identifikator interfejsa statički, moguće je identifikovati svakog pojedinačnog korisnika u podmreži, čak i prilikom mobilnosti između mreža, pa je privatnost minimalna (nepostojeća). Maksimalna privatnost se obezbjeđuje kada se i prefiks i identifikator interfejsa generišu dinamički [55].

Identifikator interfejsa u minimalnoj konfiguraciji IPv6 protokola je adresa nivoa linka (*Media Access Control Address* - MAC) koja je generisana od strane proizvođača (EUI-64) i tipično upisana u hardveru. Ova vrsta adresa se generiše na javno dostupan način: prva 3 bajta

identifikuju proizvođača na osnovu javnog registra koji održava IEEE asocijacija [56], a ostatak adrese čini identifikator mrežne kartice i njegov format je specifičan za proizvođača. Na osnovu identifikatora mrežne kartice je takođe moguće dobiti više informacija: na primjer, hardverska serija iz koje izlazi mrežna kartica je često dostupna, a na osnovu nje i identifikatora proizvođača moguće je zaključiti verziju *firmware*-a koji je u upotrebi. Ukoliko se tokom životnog vijeka mrežne kartice ispostavi da *firmware* ima sigurnosnih ranjivosti, korišćenje IPv6 identifikatora interfejsa na osnovu ove adrese bi omogućilo lako prepoznavanje ranjivog hardvera u mreži, pa nikako nije preporučljivo.

IETF je razvio više tehničkih rješenja koja poboljšavaju privatnost, kako identifikatora interfejsa tako i korisnika. Najpoznatiji mehanizam, definisan kao RFC 4941, je *Privacy Extension for SLAAC* koji generiše identifikator interfejsa koristeći kriptografske heš funkcije i slučajne vrijednosti i periodično ga mijenja [57]. Ovaj mehanizam je implementiran u većini aktuelnih operativnih sistema i često je po *default*-u aktiviran, ali nažalost ne pruža idealnu zaštitu [45].

Kako bi poboljšao privatnost korisnika i/ili osigurao dinamičke IPv6 adrese, operator je u mogućnosti da periodično mijenja prefikse podmreža konfiguracijom rutera. Bitno je napomenuti da takve mjere imaju dodatnu vrijednost po pitanju poboljšanja privatnosti samo ako su praćene mehanizmima za zaštitu privatnosti samog identifikatora interfejsa, i time njegovih korisnika.

## 5.3. Uporedna implementacija IPv4 i IPv6: sigurnosni aspekti

Da bi se obezbijedilo nesmetano funkcionisanje postojećih servisa, projekat implementacije IPv6 najčešće podrazumijeva uporedno korišćenje obije verzije IP protokola. U takvim uslovima, uporedno korišćenje za posljedicu ima dupliranje funkcionalnosti i kompleksnosti mrežnih sistema. Samim tim, za očekivati je višestruko veći broj potencijalnih ranjivosti nego što bi bio slučaj sa izolovanom upotrebom jedne verzije IP protokola. Dodatno, svaka od najčešće korišćenih metoda uporedne implementacije IPv6 i IPv4 protokola sa sobom nosi specifične rizike.

### 5.3.1. *Dual-stack* metoda

*Dual-stack* metoda konfiguracije zahtijeva podršku oba protokola na čvorištima, pa uzrokuje dupliranu upotrebu resursa kao što su memorija i procesuiranje, a za mrežu i dupliranje kontrolnog saobraćaja i pad performansi. Konfiguracija svih komponenti mreže za IPv4 i IPv6 saobraćaj mora biti konzistentna. To uključuje rutere, liste kontrole pristupa, *firewall* komponente, sisteme za detekciju upada i slično. U praksi, administratori su izloženi povećanom obimu posla prilikom održavanja pa su i greške češće, a samim tim dolazi i do sigurnosnih ranjivosti [58] [59]. U slučaju nekonzistentne konfiguracije između IPv4 i IPv6, napadaču se ostavlja mogućnost da zaobiđe dati mehanizam zaštite korišćenjem određene verzije IP protokola. Operatorima se preporučuje i nadgledanje IPv6 i ND saobraćaja kako bi se mogao detektovati neželjeni saobraćaj i/ili maliciozni sistemi na mreži.

Dobre prakse prilikom konfiguracije mreže podrazumijevaju deaktiviranje svih nepotrebnih funkcionalnosti.

### 5.3.2. Tunelovanje

Metoda tunelovanja podrazumijeva enkapsuliranje jednog protokola (na primjer IPv6) unutar drugog (na primjer IPv4). Metoda tunelovanja se često koristi uporedo sa *dual-stack* metodom kako bi se premostili segmenti mreže koji podržavaju samo jedan protokol, najčešće IPv4. Krajnje tačke tunela su izuzetno osjetljive sa aspekta sigurnosti [45] [60], jer je preko njih moguće zaobići mehanizme zaštite ostatka mreže, pa su česta meta napadača.

Dekapsulirani saobraćaj koji dolazi iz tunela je sa aspekta sigurnosti potrebno smatrati eksternim saobraćajem i na njega aplicirati sve mehanizme zaštite koji su u upotrebi na eksternim linkovima: *firewall* i filtriranje, kontrolu pristupa, antivirus zaštita i slično. Izuzetno je bitno napomenuti da ova preporuka važi i pored moguće kriptografske zaštite saobraćaja na tunelu, na primjer putem IPsec protokola. Takva vrsta zaštite prilikom tunelovanja garantuje povjerljivost i autentičnost podataka u tranzitu između krajnjih čvorišta tunela, ali ne i izvorno porijeklo saobraćaja. U slučaju primjene IPsec protokola na tunelovani saobraćaj, neophodno je obezbijediti da gore pomenuti mehanizmi zaštite imaju pristup dešifrovanom saobraćaju.

### 5.3.3. Metoda translacije protokola

Metoda translacije protokola podrazumijeva da određena čvorišta u mreži obavljaju funkciju mapiranja jednog protokola u drugi generacijom novog zaglavlja IP datagrama. Ova metoda ima neželjeni uticaj na aplikacije zbog promijenjene vrijednosti IP polja. Takođe, upitna je prednost koju implementacija IPv6 protokola ovom metodom donosi u odnosu na IPv4 pa se sa funkcionalnog aspekta ne preporučuje. Sa aspekta sigurnosti, ova metoda onemogućava korišćenje IPsec protokola za zaštitu datagrama.

## 5.4. Uticaj IPv6 na zakonske obaveze operatora

Zakon o elektronskim komunikacijama definiše obaveze i prava operatora, kao i krajnjih korisnika prilikom pružanja usluga elektronskih komunikacija [61]. Obzirom da ovi propisi ostaju na snazi tokom planiranog perioda implementacije IPv6 protokola, važno je istaći da tehničke karakteristike ovog protokola ne mogu negativno uticati na sprovođenje i poštovanje normi ovog Zakona u pogledu obaveze operatora.

Podaci o lokaciji su u Zakonu o elektronskim komunikacijama definisani kao „podaci obrađeni u elektronskoj komunikacionoj mreži ili putem elektronske komunikacione usluge, koji ukazuju na geografski položaj terminalne opreme korisnika javne elektronske komunikacione usluge“. Nesumnjivo, javna IPv6 adresa dodijeljena korisniku ukazuje na geografski položaj ukoliko je prefiks podmreže statički. Sa druge strane, upotreba dinamičke alokacije prefiksa ne sprečava operatora u izvršavanju obaveza iz člana 181 i člana 182 koji se tiču obaveza operatora u vezi zadržavanja podataka i kategorije podataka koje treba zadržati. Sa tehničkog stanovišta, nova verzija IP protokola omogućava izvršavanje navedenih zakonskih obaveza operatora praćenjem prefiksa podmreže koji su dodijeljeni određenom pretplatniku.

### 5.4.1. *General Data Protection Regulation* (GDPR)

*General Data Protection Regulation* (GDPR) je akt na nivou Evropske unije (EU) i evropskog ekonomskog prostora, koji ima za cilj poboljšanje zaštite i privatnosti podataka svojih građana. Ovim aktom, EU je homogenizovala legislativu po pitanju privatnosti podataka na cijeloj svojoj teritoriji. Bitno je napomenuti da se ovaj akt osim operatora odnosi na sve servis provajdere koji rade sa podacima korisnika iz EU, što uključuje i provajdere potencijalno bazirane van EU.

GDPR definiše lične podatke kao bilo koju informaciju koja se može povezati sa već identifikovanom osobom, ili pak informaciju koja potencijalno može identifikovati neku osobu. Kao posledica ove definicije, IP (v4 i v6) adrese korisnika spadaju u lične podatke jer ih je moguće iskoristiti za identifikaciju [62]. Stoga su IP adrese korisnika zaštićene GDPR aktom.

Sa jedne strane, GDPR akt definiše da svi privatni podaci ne smiju biti čuvani „duže nego što je svrsishodno“ [63], a sa druge strane, Zakon o elektronskim komunikacijama u članu 181 definiše da je ovu vrstu podataka neophodno čuvati na period „ne kraći od šest mjeseci ni duži od dvije godine od dana obavljene komunikacije“ [61].

## 5.5. Procjena uticaja IPv6 na blokiranje *web* sajtova koje se odnosi na zaštitu intelektualne svojine i zaštitu djece

Potreba za efikasnijom i bržom tranzicijom na IPv6 protokol nije sporna ni u jednoj studioznoj analizi, bez obzira da li se radi o tehničkom pristupu ili o pitanjima koja se odnose na politiku vezanu za implementaciju IPv6. Veoma važna pitanja vezana za pravni aspekt korišćenja IPv6 protokola, između ostalog, su: zaštita podataka, zaštita intelektualne svojine, privatnost, blokiranje neprikladnog sadržaja i zaštita djece od zloupotrebe i nasilja na Internetu.

U početku se smatralo da će migracija sa IPv4 na IPv6 protokol narušiti postojeću ravnotežu između mogućnosti sprovođenja zakonskih procedura od strane nadležnih organa, sa jedne, i privatnosti korisnika, sa druge strane. Zabrinutost u ovom pogledu je izrazilo i savjetodavno tijelo koje je formirala EU u svrhu sprovođenja Direktive o zaštiti podataka (*Data Protection Directive*), pod nazivom *Article 29 Working Party*. Istraživanja pokazuju da je mogućnost identifikacije pojedinačnih korisnika na osnovu IP adresa uglavnom ista kod IPv4 i IPv6 okruženja, bez obzira na njihove razlike [64]. Oba protokola pružaju mogućnost za skrivanje identiteta korisnika. Kod IPv4 protokola adresni prostor je ograničen resurs i taj problem se prevazilazio translacijom adresa, što je donekle olakšavalo skrivanje pravog identiteta korisnika. Kod IPv6 protokola više nije neophodno štedjeti na adresnom prostoru, pa je moguće svakom korisniku (uređaju) dodijeliti jedinstvenu javnu adresu.

IPv6 je pružio i neke nove mogućnosti u odnosu na IPv4. Kao posljedica novih IPv6 funkcionalnosti, omogućeno je praćenje individualnog ponašanja korisnika nekog uređaja na mreži, kroz njegovu IPv6 adresu, bez obzira na način i mjesto odakle pristupa Internetu. Na taj način se donekle olakšava otkrivanje potencijalnih počinilaca krivičnih djela, ali se istovremeno otvara prostor za ugrožavanje privatnosti korisnika Interneta. Naročito se ističe mogućnost praćenja pojedinaca posredstvom njihovih mobilnih uređaja ili drugih predmeta

koji imaju mogućnost povezivanja na Internet. U tom smislu posebno je ugrožena najranjivija kategorija stanovništva, a to su djeca. Uz pomoć djeci primamljivih predmeta koji su povezani na Internet (na primjer pametne igračke), potencijalni napadač sa pristupom mrežnom saobraćaju ili provajder servisa mogu pratiti kretanje pa čak i navike djeteta i te informacije zloupotrijebiti. Stoga je potrebno preduzeti neophodne mjere, kako bi se zaštitila privatnost korisnika. Jedna od takvih tehničkih mjera je bila uvođenje tzv. *privacy extensions* u IPv6 [65]. Svi značajniji operativni sistemi današnjice podržavaju *privacy extensions*, i dok su takve mjere najčešće po *default*-u aktivirane, korisnicima se preporučuje da provjere konfiguracije operativnih sistema koje koriste. Pošto se u tom slučaju otežava upravljanje mrežom, organizacije mogu uvesti politiku kojom se korisnicima mreže nalaže deaktiviranje ovih tehnika.

Kada je u pitanju zaštita autorskih prava, u praksi EU postoje primjeri koji su uzrokovali polemike oko upotrebe tehničkih mjera za blokiranje pristupa sadržaju kojim bi se povrijedila autorska prava. Sa jedne strane potrebno je štititi autorska prava, ali je sa druge strane potrebno obezbijediti pravo na zaštitu ličnih podataka i slobodnog pristupa informacijama. Takođe, tu je i pravo Internet provajdera da nesmetano obavljaju svoj posao koji im obezbjeđuje prihode. Zato se opravdano postavlja pitanje da li je uvođenje mjere blokiranja pristupa prihvatljivo sa etičke, socijalne, političke ili ekonomske perspektive. Iskustva pokazuju da je upotreba blokiranja Interneta za pristup nezakonitom sadržaja, bez obzira na vrstu IP protokola, generalno neefikasna, često nedjelotvorna i sklona da izazove neželjene kolateralne štete korisnicima [66].

Blokiranje neprikladnog sadržaja je tehnički moguće implementirati na više načina i kombinacijom više tehnika. Svaka od tehnika ima svoja ograničenja, kako u tehničkom smislu, tako i sa aspekta važeće zakonske regulative. Među najviše korišćenim tehnikama ubrajaju se:

- *IP and Protocol-Based Blocking,*
- *Deep Packet Inspection-based blocking,*
- *URL-based blocking,*
- *Platform-based blocking* i
- *DNS-based blocking.*

Više detalja o navedenim tehnikama mogu se naći u IETF tehničkoj dokumentaciji [66].

Prilikom implementacije IPv6 protokola neophodno je osigurati da mrežne komponente koje vrše funkcije blokiranja jednako tretiraju IPv4 i IPv6 saobraćaj.

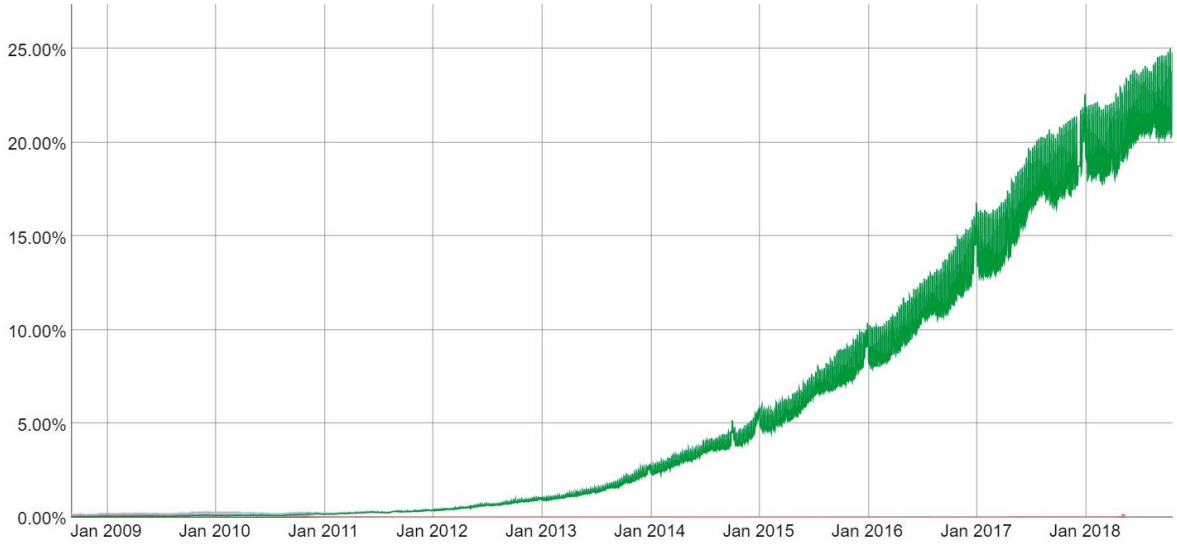
# 6. Pregled iskustava u implementaciji IPv6 u najrazvijenim državama EU i u nekim državama iz ostatka svijeta

IPv6 je u upotrebi od 1996. godine, ali je implementacija u praksi bila sporija od očekivanog. Najveći broj aplikacija i dalje funkcioniše sa starim protokolom, a i samo iskustvo korišćenja Interneta je uglavnom ostalo isto. Stoga, IPv6 nije u početku izgledao kao neophodnost. Tokom 2012. godine, veliki Internet provajderi zajedno sa proizvođačima mrežne opreme i *web* kompanijama širom svijeta pokrenuli su tzv. *World IPv6 Launch*, sa ciljem da trajno omoguće IPv6 za svoje proizvode i usluge. Od tada počinje značajan rast upotrebe IPv6 protokola. Na primjer, danas skoro 25% korisnika Google usluga koristi IPv6 [67]; skoro 50% ukupnog Internet saobraćaja iz određenih zemalja je preko IPv6; i skoro svi pretplatnici nekih većih mobilnih mreža koriste IPv6.

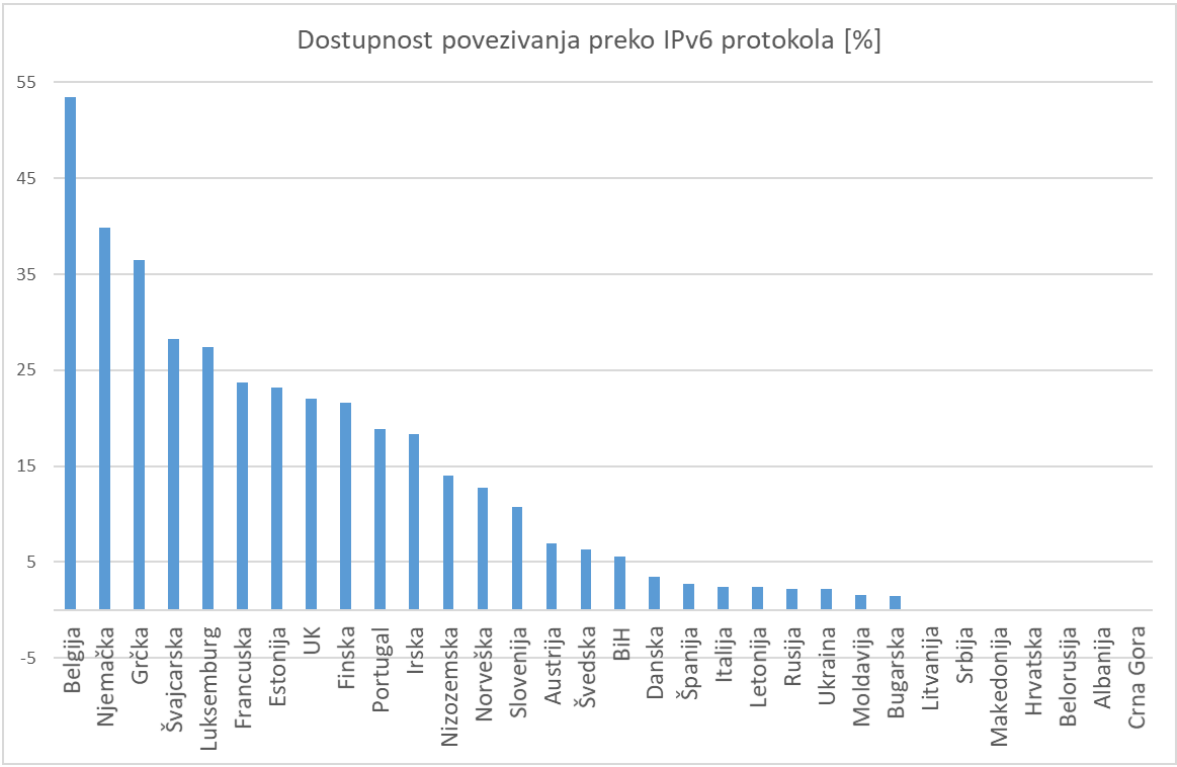
Većina današnjih operativnih sistema, uključujući i one za mobilne terminale, kao i većina mrežnih uređaja podržavaju IPv6. Međutim, postoje i neki stariji uređaji i aplikacije koje ga ne podržavaju. To je jedan od ograničavajućih faktora za potpuni prelazak na novi protokol.

Google kontinualno prikuplja statističke podatke o prihvatanju IPv6 na Internetu [67]. Na slici 17 prikazan je dijagram koji prikazuje koliki procenat korisnika je pristupio Google-ovim servisima posredstvom IPv6. Prikazani su podaci za period od početka 2009. godine do oktobra 2018. godine. Nakon početnog veoma sporog prihvatanja IPv6 protokola, od početka 2014. godine primjetan je značajan rast procentualnog učešća korisnika koji koriste IPv6 protokol. U poslednje vrijeme, procenat korisnika koji pristupaju Google-u preko IPv6 protokola kreće se u rasponu od 20% do 25%. Ukoliko se uzme u obzir da se početkom 2017. godine taj procenat kretao oko 15%, može se zaključiti da se u poslednje vrijeme IPv6 protokol značajno raširio kod Google-ovih korisnika.

Na Google-ovom sajtu [67] se mogu dobiti i ažurni podaci o dostupnosti povezivanja posredstvom IPv6 protokola za sve zemlje u svijetu. Na slici 18 prikazana je dostupnost povezivanja posredstvom IPv6 protokola izražena u procentima ukupnog Internet domena za pojedine evropske zemlje. Sa ove slike se može uočiti da je IPv6 protokol procentualno gledano najviše implementiran u Belgiji, gdje se mogućnost povezivanja preko ovog protokola kreće iznad 53%. Potom slijede Njemačka i Grčka, sa preko 30% (39,8 i 36,4, respektivno). Mogućnost povezivanja preko IPv6 protokola se kreće između 30% i 20% u Švajcarskoj, Luksemburgu, Francuskoj, Estoniji, Ujedinjenom Kraljevstvu i Finskoj. U svim ostalim evropskim zemljama procenat dostupnosti IPv6 protokola manji je od 20%. Prema podacima sa [67] jedine evropske zemlje u kojima nije moguće povezati se na Internet posredstvom IPv6 protokola su Albanija i Crna Gora. Pored toga, u nizu zemalja je dostupnost ovog protokola praktično zanemarljiva.

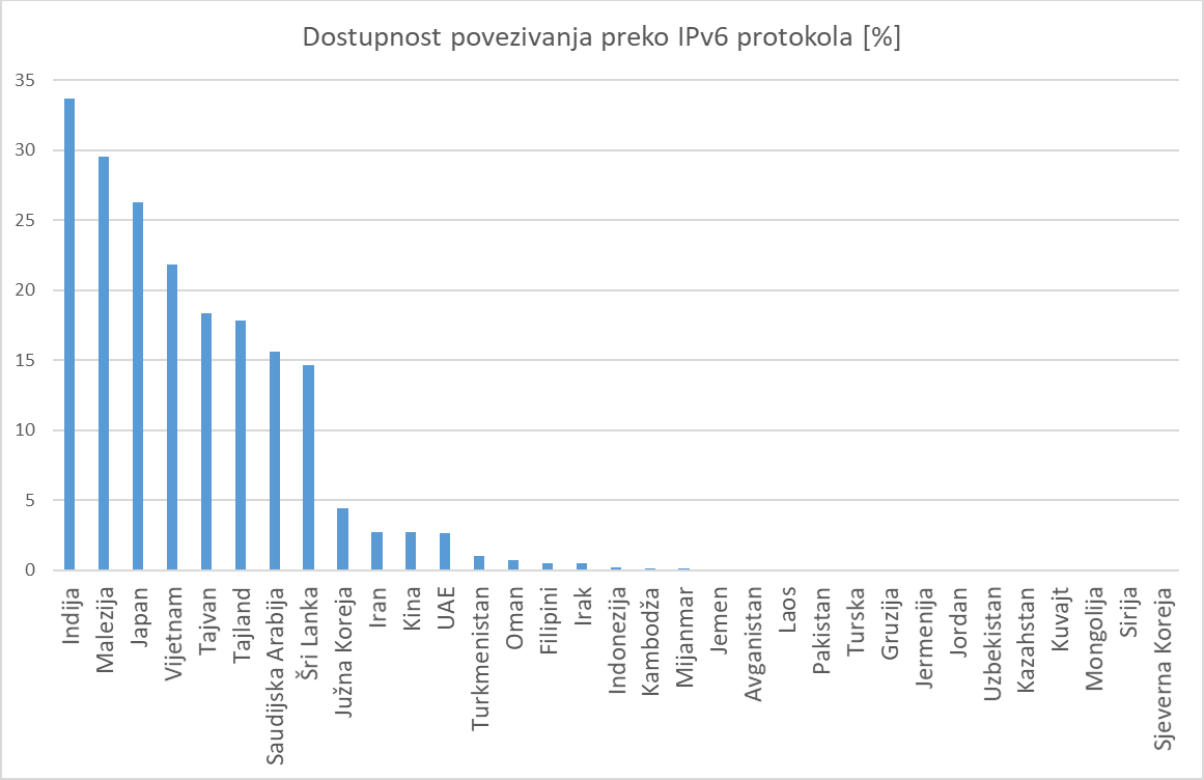



Slika 17. Procenat korisnika koji su pristupili Google-ovim servisima posredstvom IPv6 protokola [67]




Slika 18. Dostupnost povezivanja posredstvom IPv6 protokola u evropskim zemljama [67]

Na slici 19 prikazani su podaci o dostupnosti povezivanja posredstvom IPv6 protokola za pojedine azijske zemlje. Među njima prednjači Indija kod koje je IPv6 zastupljen sa 33,7%. Jedno od mogućih objašnjenja zašto baš Indija prednjači u implementaciji IPv6 protokola među azijskim zemljama leži u relativno malom broju IPv4 adresa koje ima na raspolaganju. U tom smislu, Indija je prinuđena da koristi novi adresni prostor koji nudi IPv6 protokol kad god je potrebno proširiti kapacitete za Internet saobraćaj.




Slika 19. Dostupnost povezivanja posredstvom IPv6 protokola u zemljama Azije [67]

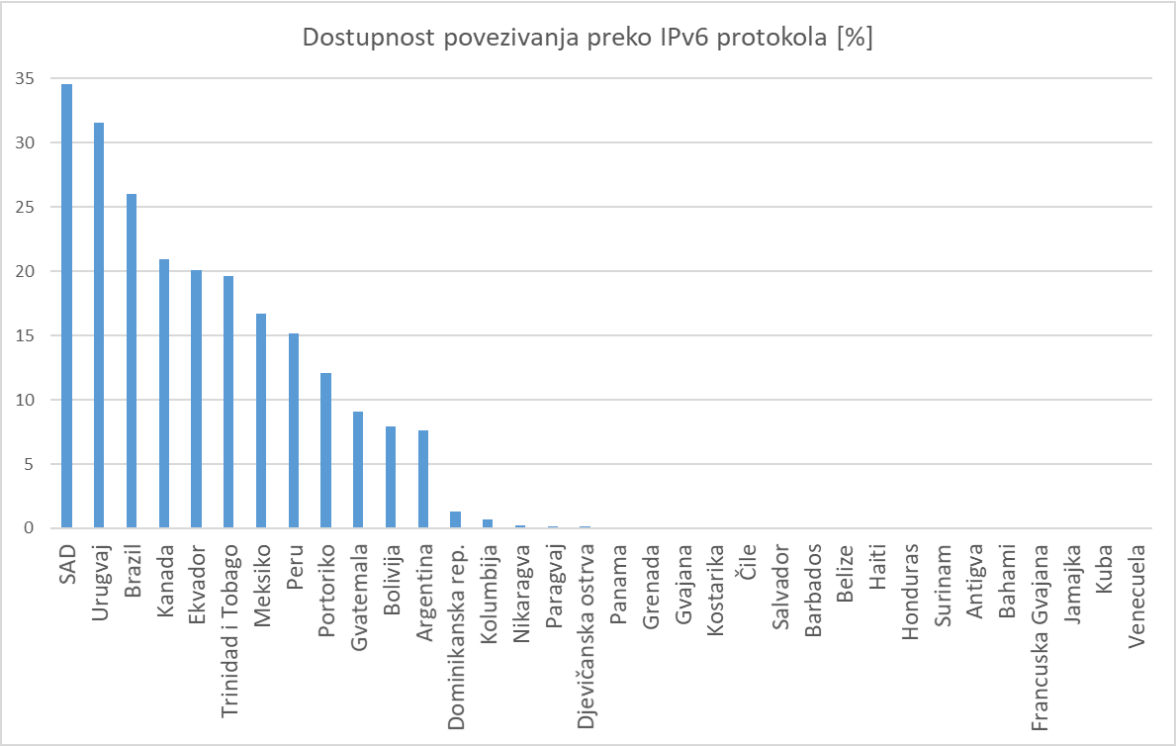
Sa druge strane, značajan dio BDP-a Indije potiče od IT industrije [64], koja je veoma oslonjena na povezanost sa Internetom. Stoga kompanije u Indiji moraju imati mogućnost povezivanja sa svojim klijentima bez obzira na to koji Internet protokol oni koriste. Takođe, Indija doživljava snažan rast pristupa Internetu posredstvom Internet kafea i operatera javnih mobilnih mreža. Da bi se zadovoljile sve ove potrebe, Indija je upućena na šire korišćenje adresnih resursa koje pruža IPv6.

Za razliku od Indije, razvijenije azijske zemlje imaju značajno veće resurse u pogledu IPv4 adresnog prostora, tako da nisu prinuđeni za tako intenzivnim korišćenjem novog protokola i njegovog adresnog prostora. Odmah iza Indije nalazi se Malezija (29,5%), a potom slijede Japan (26,2%) i Vijetnam (21,8%). Kod ostalih azijskih zemalja dostupnost povezivanja preko IPv6 protokola se kreće ispod 20%. Interesantno je da Južna Koreja, kao jedna od tehnološki jako razvijenih zemalja, ima prilično malo razvijenu IPv6 infrastrukturu (4,4%).

Najveći broj azijskih zemalja ima veoma skromne IPv6 kapacitete, koji se kreću ispod 1%: od Omana (0,7%) do Uzbekistana (0,01%). Preostale zemlje sa slike 19 (od Kazahstana do Sjeverne Koreje) uopšte nemaju mogućnost povezivanja posredstvom IPv6 protokola.

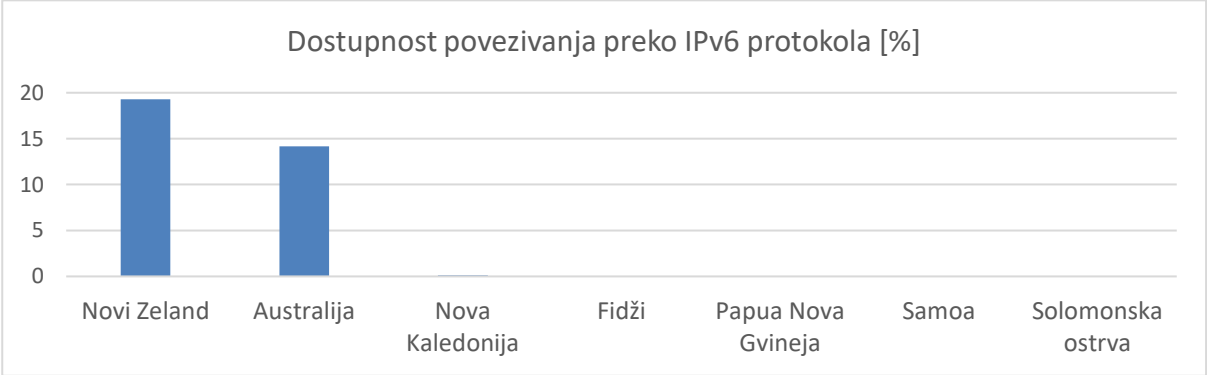
Na američkom kontinentu prednjače Sjedinjene Američke Države (SAD), sa procentom koji se kreće oko 35%. Slijede, kao što se može vidjeti sa slike 20, Urugvaj, Brazil, Kanada i Ekvador, sa 31,6%, 26%, 20,9% i 20,1%, respektivno. Ostale zemlje na američkom kontinentu imaju dostupnost IPv6 protokola ispod 20%, a kod velikog broja je dostupnost zanemarljiva. Zemlje koje su na slici 20 prikazane između Kolumbije i Surinama (uključujući i njih) imaju dostupnost IPv6 protokola manju od 1%, dok zemlje prikazane između Antigve

i Venecuele (uključujući i njih) uopšte nemaju mogućnost povezivanja na Internet posredstvom ovog protokola.




Slika 20. Dostupnost povezivanja posredstvom IPv6 protokola na američkom kontinentu [67]

Među zemljama Okeanije, po implementaciji IPv6 protokola prednjači Novi Zeland sa dostupnošću oko 19,3%, a slijede Australija sa 14,1% i Nova Kaledonija sa 0,1%. Ostale zemlje Okeanije nemaju mogućnost povezivanja na Internet preko IPv6 protokola (slika 21).

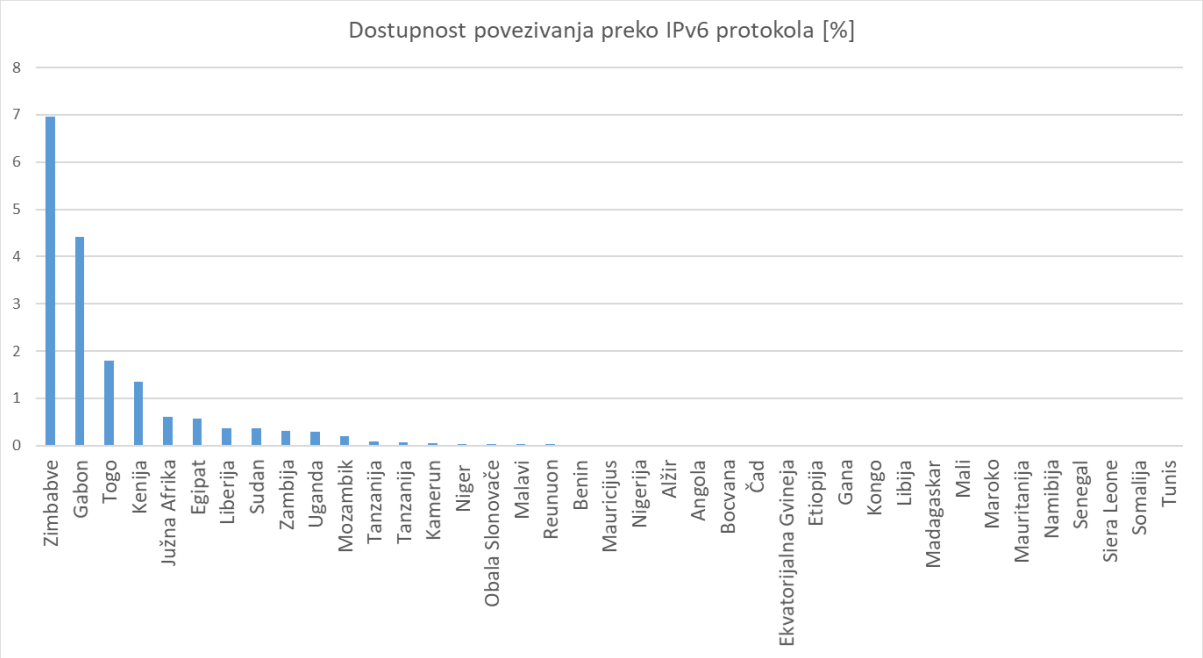



Slika 21. Dostupnost povezivanja posredstvom IPv6 protokola u zemljama Okeanije [67]

Kod afričkih zemalja je generalno implementacija IPv6 protokola na niskom nivou. Prednjači (slika 22) Zimbabve sa svega oko 7% dostupnosti IPv6 protokola, a slijede ga Gabon (4,4%), Togo (1,8%) i Kenija (1,35%). Kod svih ostalih afričkih zemalja dostupnost je manja od 1%. Zemlje koje su na slici 22 prikazane između Alžira i Tunisa (uključujući i njih) uopšte nemaju mogućnost povezivanja na Internet posredstvom IPv6 protokola.

Iz svih prikazanih podataka može se zaključiti da je implementacija IPv6 protokola na relativno niskom nivou u većini zemalja, uključujući i najrazvijenije zemlje svijeta. Razloga ima više, ali je jedan od njih svakako i nedostatak motivacije da se izvrši migracija opreme,

servisa, aplikacija i ostalih pratećih elemenata na novi protokol. To iziskuje izdvajanje ne malih materijalnih sredstava za nabavku opreme, kao i angažovanje značajnih ljudskih resursa u razvoj i konfigurisanje softverskih elemenata sistema. Značajan faktor je i vrijeme koje je potrebno za potpunu implementaciju ove migracije, kao i rizik od nefunkcionisanja sistema za vrijeme migracije i eventualnih kasnijih intervencija.




Slika 22. Dostupnost povezivanja posredstvom IPv6 protokola u zemljama Afrike [67]

Međutim, kako je to već navedeno, nedostatak IPv4 adresa, što predstavlja jedan od osnovnih hendikepa ovog protokola, je postao naročito vidljiv u svijetlu rapidnog razvoja IoT tehnologija. U tim okolnostima, prelazak na IPv6 protokol nije pitanje izbora, već je neminovnost.

## 6.1. Implementacija IPv6 protokola u najrazvijenijim državama EU

Implementacija IPv6 protokola predstavlja značajno mjesto u planovima i strategijama IT razvoja svih evropskih zemalja. Veliki broj projekata finansiran od strane Evropske komisije (EC) vezan je za IPv6 tehnologiju, podržavajući njenu implementaciju i obezbjeđujući elementarno obrazovanje u domenu IPv6. Kao primjeri takvih projekata mogu se istaći 6NET [83], 6DISS [84], Go4it [85], 6WINIT [86], EURO6IX [87] i slični. Nadalje, EU je naložila da svi istraživački projekti koje finansira EC treba da podržavaju IPv6.

Stepen implementacije IPv6 se, međutim, veoma razlikuje kod evropskih zemalja. Često dostupnost IPv6 nije u srazmjeri sa brojem IPv6 adresa koje su dodijeljene pojedinim zemljama. Ovdje će biti predstavljena neka iskustva u pripremi i implementaciji IPv6 migracije u Francuskoj i Njemačkoj, kao primjerima visokorazvijenih evropskih zemalja.

### 6.1.1. Implementacija IPv6 protokola u Francuskoj

Francuska je jedna od prvih zemalja u svijetu koja je planirala uvođenje IPv6 protokola. Još 2002. godine francuska vlada je formirala Radnu grupu sa zadatkom da se bavi planiranjem

uvođenja IPv6 u Francuskoj, pod nazivom *IPv6 Task Force France*. Ova radna grupa je u novembru 2003. godine objavila preporuke za strateško planiranje u procesu razvoja i implementacije IPv6 tehnologija u Francuskoj (*Recomendations for a Strategic Plan in the Development and Implementation of IPv6 Technologies in France*) [76]. Ove preporuke su se mogle podijeliti u tri kategorije. Prva kategorija se odnosila na javne institucije i agencije za pružanje usluga. Druga kategorija je upućena privatnom sektoru. Treća se fokusirala na zahtjeve u pogledu organizacije i kontrole strategije implementacije IPv6.

Pred državne organe, institucije i agencije u ovim preporukama je postavljen zadatak da svojim primjerom daju stimulans i podrže uvođenje IPv6 protokola. Morali su da definišu i javno objavljuju svoje strategije, metodologije i vremenske okvire za migraciju komunikacione infrastrukture na IPv6, a naročito one koja je povezana na Internet. Posebno je trebalo obratiti pažnju na dvije stvari:

- da se razmotri mogućnost uvođenja IPv6 prilikom povezivanja svih javnih subjekata sa Internetom, a prioritetno kod škola i univerziteta;
- izvršiti migraciju svih vladinih *web* servera (na domenu *gouv.fr*) na dualni IPv4 i IPv6 pristup.

Prilikom procesa nabavki, javne ustanove su obavezane da za svu opremu koja treba da bude povezana na komunikacionu infrastrukturu traže mogućnost korišćenja IPv6, kao i kasniju podršku od strane isporučioca te opreme. Ukoliko trenutno nije obezbijeđena kompatibilnost sa IPv6 za traženu opremu, isporučioc se mora obavezati na određeni vremenski okvir u kome će kompatibilnost biti obezbijeđena, kao i odgovarajuću podršku u tom smislu.

Vodeće regionalne mreže koje su povezane sa mrežom RENATER [78] treba da promovišu prelazak na IPv6 tako što će:

- ponuditi pretplatnicima pristup preko IPv4 i IPv6;
- snažno uključiti univerzitete i sve visokoškolske ustanove, kako bi obučili osoblje i sve buduće diplomce u korišćenju novih tehnologija i podstakli migraciju na IPv6 svih internih mreža u takvim institucijama;
- uvesti politiku koja podstiče eksperimentisanje novim IPv6 uslugama i kreiranje novih aplikacija.

Na taj način je došlo do uvođenja IPv6 u nacionalnu komunikacionu infrastrukturu, kao i u infrastrukturu većine javnih institucija.

Kada je u pitanju privatni sektor, predložene su sljedeće aktivnosti:

- veće kompanije treba odmah da počnu sa planiranjem nadogradnje računarskih resursa i mreža, a prilikom novih investicija treba da vode računa o kompatibilnosti sa IPv6;
- telekomunikacione kompanije, proizvođači hardvera, kao i softverske kompanije treba da integrišu IPv6 u razvoj i ponudu svojih proizvoda, te da objavljuju vremenske okvire u kojima će ovi proizvodi biti dostupni;

- operatori treba da se obavežu na određene rokove u kojima će omogućiti komercijalne usluge na bazi IPv6 protokola kod žičanih (DSL (*Digital Subscriber Line*), *Ethernet*, kablovska) i bežičnih mreža (WiFi, GPRS).

Preporuke koje se odnose na organizaciju i nadgledanje strateškog planiranja su:

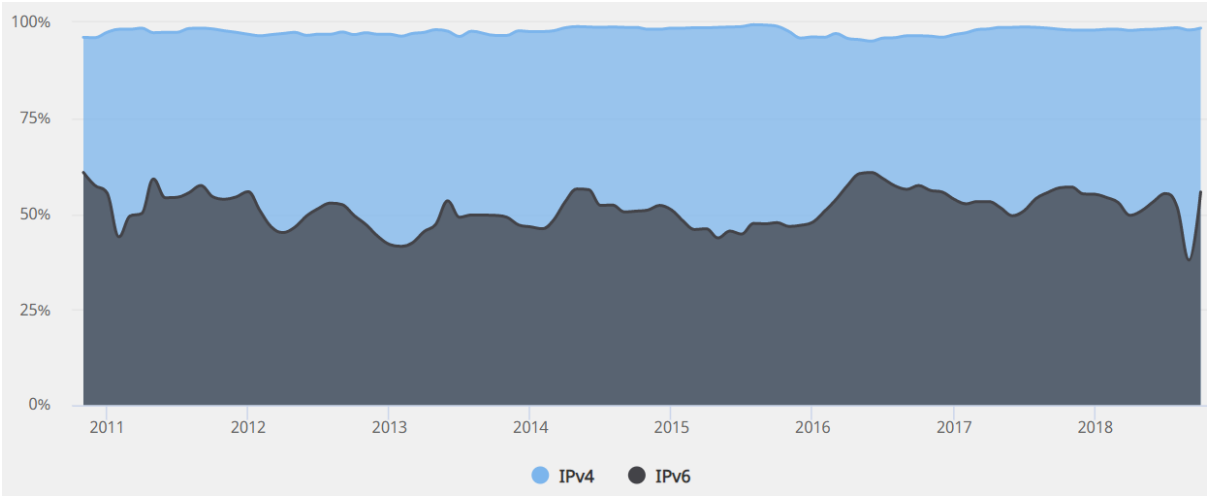
- uspostaviti strateški plan implementacije IPv6, koji vodi Ministarstvo za istraživanje i nove tehnologije;
- osnovati tijelo koje treba da bude ovlašćeno da osigura primjenu i praćenje plana, tako što će:
  - pokretati i koordinirati aktivnosti,
  - pružati informacije o testnim i operativnim implementacijama i studijama koje su aktuelne u Francuskoj, Evropi i svijetu,
  - podsticati diseminaciju i eksploataciju rezultata i primjera najboljih praksi,
  - obezbijediti koordinaciju na nivou Evrope.

Veoma važnu ulogu u uvođenju IPv6 u Francuskoj imala je mreža RENATER [78]. To je nacionalna istraživačka i edukaciona mreža, osnovana još početkom 1990. godine. Obezbjeđuje nacionalnu i međunarodnu konektivnost posredstvom pan-evropske mreže GÉANT ka više od 1000 obrazovnih i istraživačkih centara. Prve testne usluge posredstvom IPv6 uvedene su u ovu mrežu 1995. godine, a od 2002. godine RENATER realizuje okosnicu mreže baziranu na IPv6, koja je omogućila pristup za više od 650 univerziteta, istraživačkih centara i vladinih agencija.

Krajem 2001. godine završen je projekat VTHD [79], koji je takođe imao značajnu ulogu u vezi popularizacije i implementacije IPv6 u Francuskoj. Projekat je djelimično finansiran od strane francuske vlade, a partneri su bili iz akademske zajednice. Značajnu ulogu u ovom projektu je imalo i istraživačko odjeljenje *France Telecom*-a - RNRT (*Réseau National de la Recherche en Télécommunications*). Projekat je kasnije nastavljen kroz VTHDv6 projekat koji je kao rezultat omogućio IPv4 i IPv6 servise i aplikacije za učesnike u projektu [80].

Prvi komercijalni Internet provajder koji je omogućio povezivanje preko IPv6 bio je Nerim [81]. Od marta 2003. godine Nerim je omogućio direktni IPv6 pristup posredstvom ADSL-a (*Asymmetric Digital Subscriber Line*). Tamo gdje direktni pristup nije bio moguć, obezbijeđen je preko IPv4 tunela. Slijedili su ga veći operateri, a prije svih *France Telecom* (2005. godine) i *Free* (2007. godine).

Informacije o aktuelnom stanju u pogledu implementacije i korišćenja IPv6 protokola mogu se naći na Internetu. Jedna od lokacija koja na mjesečnom nivou ažurira informacije, dobijene na osnovu testiranja pomoću servisa koji provjeravaju IPv4 i IPv6 konektivnost, je http://ipv6-test.com/. Podaci o razvoju IPv6 u odnosu na IPv4 protokol, u Francuskoj, zaključno sa septembrom mjesecom 2018. godine mogu se vidjeti na slici 23. Francuski provajderi još uvijek gotovo u potpunosti podržavaju IPv4, dok je podrška IPv6 promjenljiva. U poslednjih desetak godina ta se podrška kreće između 40% i 60%, a danas se, prema [82] kreće oko 56%.




Slika 23. Podrška provajdera u Francuskoj za IPv4 i IPv6 protokol [82]

Na vrhu liste provajdera u Francuskoj koji podržavaju IPv6 nalaze se: *Orange S.A.*, *ProXad network / Free*, *Bouygues Telecom ISP Wireline*, *Ovh*, *Sfr*, *Online S.A.S.*, *Hurricane Electric LLC*, *Bouygtel-isp*, *Renater* i *Knet* [82].

### 6.1.2. Implementacija IPv6 protokola u Njemačkoj

Njemačka važi za jednu od najrazvijenijih zemalja svijeta, koja prati naučne i tehnološke trendove. Zato je naročito interesantno pogledati njihova iskustva u pogledu implementacije IPv6. Prema SixXS [88], sredinom 2010. godine Njemačka je imala najveći broj vidljivih IPv6 prefiksa među zemljama Evrope, a bila je druga u svijetu, iza SAD. Ovo je najbolji pokazatelj sa kolikim uspjehom je Njemačka krenula u proces implementacije IPv6.

Njemačka je federalna parlamentarna republika sastavljena od 16 saveznih država. Svaka od tih država ima svoju javnu administraciju, sa zaduženjima i ovlašćenjima koja su im data Ustavom. Savezna vlada igra ulogu LIR-a (*Local Internet Registry*) i kao takva je član Evropskog RIPE NCC registra. Koristeći svoju poziciju, Njemačka je u pojedinim momentima dobijala značajno više IPv6 adresa nego druge evropske zemlje. Radi efikasnosti i izbjegavanja fragmentacije, distribucija adresa se u Njemačkoj vrši na bazi podnijetih zahtjeva, sistemom piramide [89].

Veoma važan doprinos uspješnoj implementaciji IPv6 u Njemačkoj dali su Komesarijat federalne vlade za informacionu tehnologiju (*Der Beauftragte der Bundesregierung für Informationstechnik*) [90] i Njemački IPv6 savjet (*Deutschen IPv6 Rat*) [91]. IPv6 savjet je osnovan 2007. godine sa zadatkom da pruža pomoć u tehničkom i upravljačkom smislu što uspješnijoj implementaciji IPv6 u svim sferama Njemačke telekomunikacione infrastrukture. Savjet je usvojio niz dokumenata od kojih se posebno ističe *Nationaler IPv6 Aktionsplan für Deutschland* (Nacionalni akcioni plan za uvođenje IPv6 u Njemačkoj), objavljen maja 2009. godine [92]. Ovaj dokument je namijenjen najširem krugu korisnika i u njemu su navedeni ciljevi, mjere koje treba preduzeti, kao i problemi sa kojima se može suočiti tokom implementacije IPv6 u Njemačkoj.

Kako Njemačka ne bi zaostala za ostatkom svijeta, a naročito za svojim najvažnijim ekonomskim partnerima, naglašena je važnost pravovremene pripreme u susret izvjesno

nastupajućim potrebama za IPv6 opremom, servisima i aplikacijama. Svaka zainteresovana strana, a u koje se ubrajaju Internet provajderi, proizvođači hardvera i softvera, telekomunikacioni operatori, obrazovne i istraživačke institucije, kao i javna administracija, mora identifikovati svoju ulogu i značaj u procesu migracije. U ovom akcionom planu je naročito prepoznata uloga političara za uspješan proces uvođenja IPv6. Sugeriše im se da putem medija šire svijest o potrebi uvođenja IPv6. Takođe, potrebno je obavezati državne organe na upotrebu IPv6. Za početak, u tenderima za nove sadržaje, usluge, hardver i softver, na svim nivoima javne uprave, neophodno je naglasiti korišćenje IPv6. Postojeće Internet usluge treba postepeno migrirati na IPv6, u sklopu redovnih aktivnosti održavanja sistema.

Najposjećenije njemačke *web* sajtove koji pripadaju vladi i državnoj upravi u što kraćem roku treba učiniti kompatibilnim sa IPv6. Pri tome se mora osigurati sigurnost IT sistema i voditi računa o zaštiti podataka. Isto važi i za obrazovne i istraživačke institucije, koje u tom procesu mogu koristiti EU fondove kroz međunarodne projekte.

Slične preporuke su upućene i privatnom sektoru. Tu je naročit fokus stavljen na Internet provajdere koji treba da izvrše neophodna prilagođavanja za široko rasprostranjenu upotrebu IPv6 tehnologije. U standardnoj ponudi moraju imati hardver i softver koji podržava IPv6 i to bez dodatnih troškova po korisnika. I ovdje je potrebno najvažnije sajtove što prije migrirati na IPv6 i voditi računa o svim aspektima sigurnosti.

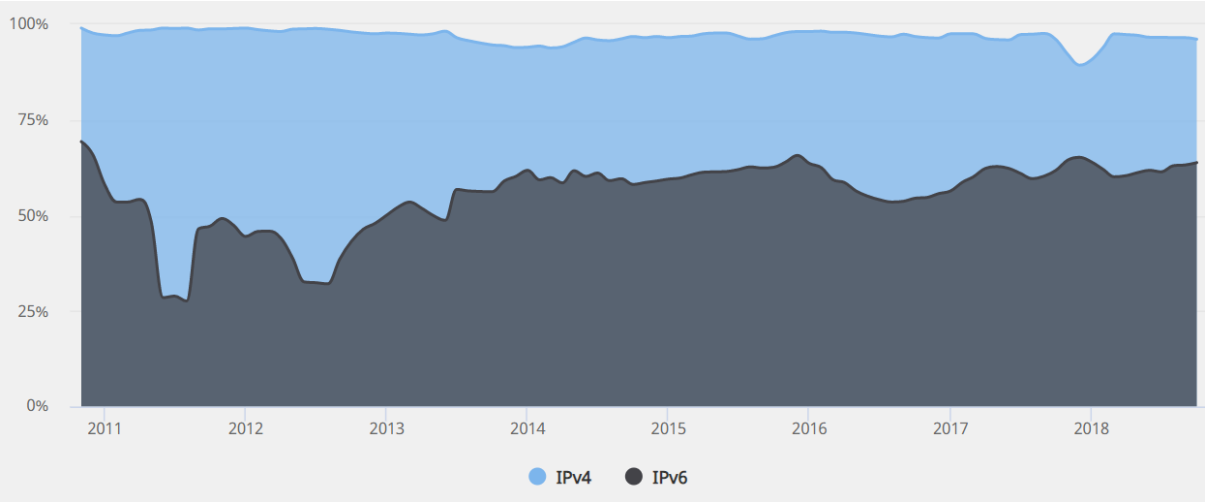
Pitanjima sigurnosti se posebno bavio Savezni biro za sigurnost u informacionim tehnologijama (*Bundesamt für Sicherheit in der Informationstechnik*), koji je usvojio dokument Vodič za sigurnu IPv6 mrežnu infrastrukturu (*Leitfaden für eine sichere IPv6-Netzwerkarchitektur*) [94]. U ovom dokumentu se sveobuhvatno tretiraju pitanja vezana za informacionu sigurnost tokom migracije na IPv6 protokol.

Njemačke naučne i istraživačke institucije organizovale su komunikacionu mrežu za svoje potrebe, koja se naziva *Deutsche Forschungsnetz* (DFN) [96]. Ona međusobno povezuje univerzitete i istraživačke institucije i integralni je dio evropske i svjetske zajednice istraživačkih i obrazovnih mreža. Pored toga, posredstvom nekoliko visokoperformantnih konekcija povezana je na globalni Internet. Okosnica DFN mreže pruža punu IPv6 podršku za sve korisnike.

Iz svega navedenog se može zaključiti da je Njemačka aktivno, sistematski i uz snažnu podršku federalne vlade pristupila uvođenju IPv6 protokola. Preduzete aktivnosti su urodile plodom i Njemačka je u decembru 2016. godine primila „*Jim Bound IPv6 Award*“ nagradu, jer se sa 24 miliona korisnika svrstala u najvećih 5 korisnika IPv6 na globalnom nivou [93]. Još jedna „*Jim Bound IPv6 Award*“ nagrada otišla je u *Deutsche Telekom*, u čijoj mreži je 10 miliona korisnika koristilo IPv6. Prema Google-ovoj statistici, Njemačka je do danas dostigla stopu prihvatanja IPv6 protokola od 40% i u stalnom je usponu [95].

Stanje razvoja IPv6 u odnosu na IPv4 protokol, u Njemačkoj, zaključno sa septembrom mjesecom 2018. godine mogu se vidjeti na slici 24. Njemački provajderi još uvijek podržavaju IPv4, mada se može primjetiti izvjestan pad ove podrške poslednjih godina. Podrška IPv6 protokolu je u početku bila jako promjenljiva, dok se u poslednje vrijeme,

prema ovim podacima, može primjetiti prilična uravnoteženost. Danas se, prema [97] podrška IPv6 kreće oko 64%.




Slika 24. Podrška provajdera u Njemačkoj za IPv4 i IPv6 protokol [97]

Prema [97], na vrhu liste provajdera u Njemačkoj koji podržavaju IPv6 nalaze se: *DTAG European region*, *Unitymedia*, *Kabeldeutschland*, *KabelBW*, *Versatel Deutschland*, *Telekom Deutschland GmbH*, *Hurricane Electric LLC*, *Hurricane Electric*, *M247 Ltd* i *DGW Network*.

## 6.2. Implementacija IPv6 protokola u Sjedinjenim Američkim Državama

U Sjedinjenim Američkim Državama (SAD) postoji veliki broj organizacija, od kojih je većina neprofitna i organizovana na dobrovoljnoj osnovi, koje se bave problemima implementacije IPv6 protokola. Među njima se ističu *The North American IPv6 Task Force* [68] i *The IPv6 Forum* [69]. Ipak, šire interesovanje za implementaciju ovog protokola nije postojalo, sve do 2003. godine [64]. Tada je pomoćnik Sekretara za odbranu SAD potpisao memorandum o usvajanju IPv6 protokola od strane Ministarstva odbrane SAD, u kojem je postavljen rok za uvođenje ovog protokola do 2008. godine. Interesovanje Ministarstva odbrane SAD za IPv6 proizašlo je iz njihove potrebe za velikim brojem IP adresa, kako bi podržali svoju viziju „umreženog bojnog polja“.

Ovaj memorandum je izazvao značajan porast interesovanja za IPv6. Mnoge firme koje su sarađivale sa Ministarstvom odbrane ili su se bavile mrežnim tehnologijama vidjele su šansu za profitom i okrenule se proizvodnji i isporuci proizvoda koji podržavaju IPv6, kao i razvoju servisa koji su zasnovani na ovom protokolu. To je dovelo do značajnog porasta broja proizvoda koji podržavaju IPv6, kao i do generalnog porasta kompetencija vezanih za IPv6.

Početkom 2004. godine, Ministarstvo trgovine SAD je objavilo Zahtjev za komentare o primjeni Internet Protokola verzije 6 [70], u kojem se navodi da je sekretar za trgovinu SAD zadužen da formira radnu grupu koja će se baviti pitanjima vezanim za implementaciju IPv6 u SAD. Ovo je takođe dalo stimulaciju za razvoj IPv6 proizvoda i usluga u SAD.

Sredinom 2005. godine stvorena je pravna osnova za pokretanje implementacije IPv6 u svim federalnim vladinim agencijama, tako što je Kancelarija za upravljanje i budžet objavila

memorandum „Planiranje migracije za Internet protokol verziju 6 (IPv6)“ [71]. Ovim dokumentom je propisano da sve savezne agencije moraju koristiti IPv6 u okosnici svoje mrežne infrastrukture, a mreže samih agencija moraju biti povezane na ovu infrastrukturu do juna 2008. godine. Takođe, predviđene su i sljedeće aktivnosti koje agencije moraju da sprovedu u tačno određenim rokovima.

Do 15. novembra 2005. godine:

- imenovati odgovorne osobe koja će voditi i koordinirati planiranje;
- napraviti spisak svih postojećih rutera, svičeva i hardverskih *firewall*-ova;
- započeti pravljenje spiska svih drugih IP uređaja i tehnologija koji nisu uključeni u prethodnu listu;
- pokrenuti analizu finansijskih i operativnih uticaja i rizika koji proizilaze iz prelaska na IPv6.

Do februara 2006:

- dostaviti završen plan prelaska na IPv6 izrađen na osnovu uputstava dobijenih od nadležnih institucija;
- dostaviti izvještaj o urađenome oko popisa opreme i analize uticaja prelaska na IPv6.

Do 30. juna 2006. godine:

- završiti popis postojeće IP opreme i tehnologija koji nisu uključeni u prvi popis;
- završiti analizu finansijskih i operativnih uticaja i rizika.

Do 30. juna 2008. godine:

- mrežna okosnica infrastrukture agencija mora da koristi IPv6 i agencije moraju biti povezane na ovu infrastrukturu.

Memorandum zahtijeva od agencija da u budućnosti osiguraju da prilikom nabavke nove ICT opreme ona bude kompatibilna sa IPv6. Uređaj ili sistem koji je kompatibilan sa IPv6 mora biti u stanju da primi, obradi i prenese ili proslijedi IPv6 pakete i da radi sa drugim sistemima i protokolima u IPv4 i IPv6 modu rada. Nacionalni institut za standarde i tehnologiju (NIST) zadužen je da napravi neophodne standarde, kako bi se osiguralo da sve državne institucije imaju jedinstven sistem tehničkih specifikacija prilikom kupovine potrebne IPv6 opreme.

Nakon memoranduma usvojeni su i drugi važni dokumenti. Među njima treba istaći studiju iz januara 2006. godine, koju je izdalo Ministarstvo trgovine u saradnji sa Nacionalnim institutom za standarde i tehnologiju i NTIA (*National Telecommunications & Information Administration*). Studija „Tehnička i ekonomska procjena Internet protokola verzije 6 (IPv6)“ [72] obrađuje tehničke i ekonomske efekte koji se odnose na uvođenje IPv6, uključujući ulogu vlade SAD u procesu migracije, međunarodnu kompatibilnost, sigurnost, troškove i benefite od uvođenja IPv6. Studija konstatuje da će IPv6 značajno koristiti američkom poslovanju i potrošačima, pri čemu će se puni efekti pokazati tek nakon izvjesnog vremena. Većina stručnjaka za Internet saglasna je da će IPv6 mreža biti tehnički bolja u odnosu na postojeće IPv4 mreže. Veći adresni prostor, koji donosi IPv6, omogućiće razvoj novih inovativnih komunikacionih usluga i aplikacija. U studiji se razmatraju i prepreke na putu

brzog prelaska na IPv6 protokol. Među njima su mnogi stariji, moćni, kvalitetni i skupi uređaji, kao i odgovarajuće aplikacije, koji još uvijek obavljaju svoje funkcije. Pošto su usklađeni samo sa IPv4 protokolom, u procesu migracije na IPv6 bi ih trebalo zamijeniti. To znači da će biti potrebna značajna finansijska sredstva i ljudski resursi u procesu migracije.

Sa ekonomske tačke gledišta, troškovi migracije se mogu smanjiti ako se na vrijeme planira unapređenje opreme. U kontekstu zamjene opreme većinu troškova čine obuka osoblja, instalacija i konfiguracija softvera i testiranje mreže, a ne sama cijena opreme koja neće biti znatno veća u odnosu na IPv4 opremu. Troškovi migracije će se razlikovati i za različite grupe korisnika. Za mala i srednja preduzeća i pojedinačne korisnike koji ne upravljaju velikim mrežama, ovaj trošak će biti relativno mali i može se planirati u kontekstu standardne periodične zamjene opreme. Sa druge strane, velike kompanije i vladine agencije moraju računati sa znatno višim troškovima, koji variraju u zavisnosti od postojeće infrastrukture i operativne politike. U obzir se moraju uzeti i aplikacije koje treba modifikovati ili razviti od početka. Takođe, proces migracije značajno zavisi od toga koliko korisnici imaju potrebu za povezivanjem sa drugim organizacijama koje koriste IPv6. Ukoliko nema urgentnih potreba i zahtjeva za prelazak na IPv6, sa migracijom se može sačekati dok ne dođe do rutinske zamjene opreme i ne obuči se dovoljan broj zaposlenih.

Jedan od najvažnijih aspekata današnje Internet komunikacije jeste sigurnost mreže i podataka koji se njome prenose. Najveći potencijal IPv6 protokola u pogledu sigurnosti može se prepoznati u dugoročnom razvoju nove sigurnosne paradigme, koja je fundamentalno drugačija od one uspostavljene u postojećim IPv4 mrežama. Iako će vrijeme i troškovi potrebni za dizajniranje i razvoj novih sigurnosnih modela biti značajni, stvaranje novih, efikasnijih paradigmi sigurnosti će donijeti benefit svim trenutnim i budućim korisnicima Interneta.

Uvođenje novog protokola, kao što je IPv6, u ranoj fazi povećava ranjivost informacionih sistema. Pošto je IPv6 protokol ugrađen u veliku količinu hardvera i softvera koji se već nalazi u upotrebi, veoma je vjerovatno da će se IPv6 pojaviti (potencijalno enkapsuliran) na operativnim mrežama nezavisno od planova organizacije i njenih mrežnih administratora. Zato je potrebno da sve organizacije definišu i implementiraju politiku prenosa IPv6 saobraćaja, bez obzira na to kada je planirana migracija na novi protokol. S obzirom da uvođenje IPv6 podrazumijeva određene troškove, u preporukama se naglašava potreba za pažljivim planiranjem, razvojem i evaluacijom, koji bi trebalo da prethode donošenju odluka o uvođenju novih tehnologija u operativnom dijelu IPv6 mreže. Rezultati gore pomenute studije pokazali su da postoje značajni tehnički i ekonomski rizici koji mogu biti povezani sa nedostatkom odgovarajućeg plana i strategije za uvođenje IPv6.

U februaru 2006. godine, *Federal Chief Information Officers Council Architecture and Infrastructure Committee*, je na osnovu ranijeg memoranduma izdao preporuke kako bi pomogao saveznim agencijama u migraciji na IPv6. Ovaj dokument se sastoji od tri poglavlja. U prvom poglavlju opisano je kako izvršiti migraciju na IPv6 kod preduzeća sa kompanijskom infrastrukturom. Drugo poglavlje bavi se tehničkim elementima, koji su važni u migraciji kod agencija. U ovom poglavlju je dat pregled najboljih praksi IPv6 migracija.

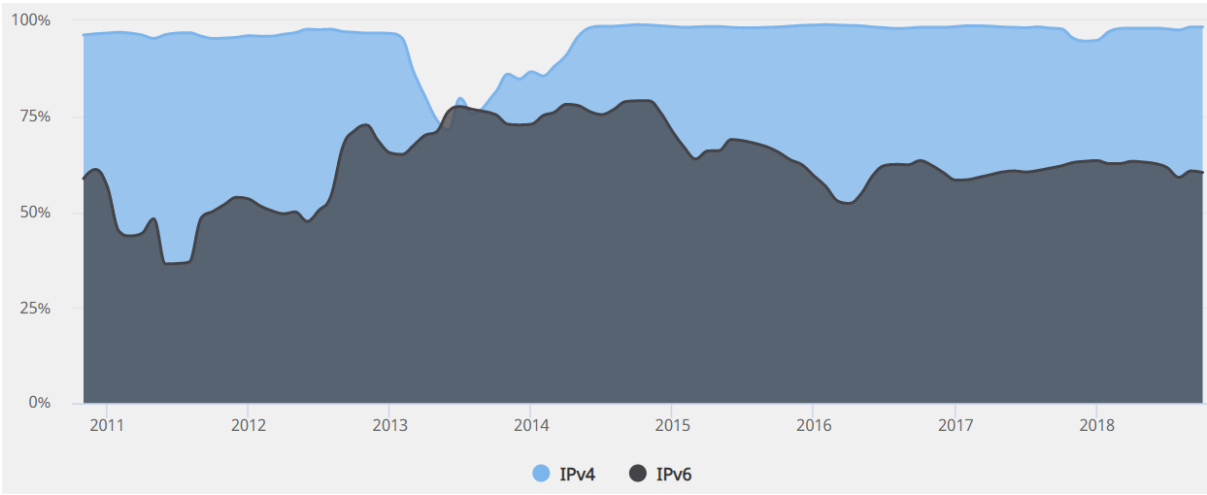
Treće poglavlje posvećeno je upravljanju IPv6 migracijom. U njemu su opisane individualne uloge i odgovornosti agencija i organizacija koje učestvuju u procesu.

U 2008. godini *National Institute of Standards and Technology (NIST)* je objavio dokument pod nazivom „*A profile for IPv6 in the U.S. Governement (USG IPv6 Profile)*“ [73], u kome su propisani minimalni operativni i tehnički uslovi koje moraju zadovoljavati mrežni uređaji, kao što su serveri, ruteri, uređaju za zaštitu mreže i slično. Ovaj dokument je napravljen da bi pomogao federalnim agencijama u njihovim razvojnim planovima, kao i prilikom nabavke i implementacije IPv6 kompatibilnog hardvera i softvera, kako bi se osigurala kompatibilnost i sigurnost informacionih sistema. Obzirom da se na taj način pomaže u zaštiti investicije u IPv6 migraciju, ovaj dokument se bavi dugoročnim strateškim planom SAD za primenu IPv6 tehnologije.

Nakon što je usvojen standard, svaki uređaj koji dobije oznaku kompatibilnosti sa IPv6 mora proći strogo ispitivanje i sertifikaciju kod akreditovanih laboratorija za testiranje koje zadovoljavaju ISO 17025 standard (Opšti zahtjevi za kompetentnost laboratorija za ispitivanje i kalibraciju). U tu svrhu NIST je pripremio dokument koji definiše metode ispitivanja i validacije: *SP 500-273 USGv6 Test Methods: General Description and Validation* [74]. Ukoliko testirana oprema uspješno prođe testiranje i sertifikaciju, uvrsti se u APL (*Approved Products List*) listu proizvoda koji su kompatibilni sa IPv6, odnosno zadovoljavaju tehničke specifikacije propisane u RFC dokumentima.

Iako su navedeni dokumenti namijenjeni prvenstveno vladinim federalnim agencijama i njihovom osoblju, oni mogu poslužiti kao dobra polazna tačka i za sve ostale koji imaju želju i namjeru da izvrše prelaz na IPv6 tehnologiju.

Aktuelni podaci o razvoju IPv6 u odnosu na IPv4 protokol, u SAD, zaključno sa septembrom mjesecom 2018. godine mogu se vidjeti na slici 25. Sa slike se može vidjeti da provajderi u SAD i dalje gotovo u potpunosti podržavaju IPv4 protokol, a da se podrška IPv6 protokolu mijenja vremenom. Najveća je bila u periodu između 2013. i 2015. godine, a danas se, prema ovom izvoru, kreće oko 60%.




Slika 25. Podrška provajdera u Sjedinjenim Američkim Državama za IPv4 i IPv6 protokol [75]

Prema [75], na vrhu liste provajdera u SAD koji podržavaju IPv6 nalaze se: *Comcast Cable Communications*, *Google LLC*, *Spectrum*, *Cellco Partnership DBA Verizon Wireless*, *Hurricane Electric LLC*, *AT&T Internet Services*, *Cox Communications Inc*., *Hurricane Electric*, *CenturyLink* i *Choopa*.

Iz svega navedenog može se zaključiti da je glavni inicijator uvođenja IPv6 u SAD bila njihova vlada. Usvajanjem Memoranduma [71] vlada je obavezala sve federalne agencije na migraciju prema IPv6. Pratećim dokumentima su definisani tehnički standardi koji moraju biti ispunjeni da bi se postigla IPv6 kompatibilnost, i to se poštuje od strane svih značajnijih proizvođača ICT opreme.

## 6.3. Implementacija IPv6 protokola u nekim zemljama Azije

Neke azijske zemlje, kao što su Japan, Tajvan, Južna Koreja, Malezija i Kina, su ranije prihvatile neophodnost prelaska na IPv6 i u tom smislu započele proces migracije prije ostalih djelova svijeta [64]. Jedan od glavnih razloga za takvu aktivnost bio je nedostatak IPv4 adresa u ovom dijelu svijeta. Kao i u mnogim drugim zemljama, migracija je podstaknuta nizom vladinih inicijativa.

Azijske zemlje su interesantne u pogledu interesovanja za IPv6 i zbog toga što se među njima nalaze i najmnogoljudnije zemlje svijeta, prije svih Kina i Indija. Obje ove zemlje imaju preko milijardu stanovnika, dok je broj IPv4 adresa koje su imale 2010. godine iznosio oko 8,8 miliona za Kinu i oko 1 milion za Indiju [100]. Sa druge strane, procenat stanovništva koji koristi Internet je kod Kine iznosio oko 34%, a kod Indije manje od 8%, za razliku od Japana kod koga se taj procenat kretao iznad 78%. To znači da se u Aziji nalazi značajno potencijalno tržište za Internet usluge i servise, a time će se javljati sve veća potreba za IP adresnim prostorom.

### 6.3.1. Implementacija IPv6 protokola u Japanu

Japan je prepoznat kao zemlja koja ne samo da prati već i diktira tehnološke trendove, naročito kod digitalnih tehnologija. To je potpuno očekivano ako se uzme u obzir da mnoge velike kompanije iz domena potrošačke elektronike imaju sjedište u Japanu. Korišćenjem IP komunikacione tehnologije mogu se značajno unaprijediti mogućnosti različitih uređaja koje proizvode Japanske kompanije. Tako je, na primjer, Sony korporacija odlučila da kod svih svojih proizvoda omogući IP komunikaciju do 2005. godine [99]. Za uspješnu podršku ovakvim uređajima i odgovarajućim servisima, neophodna je skalabilna infrastruktura, a IPv6 je pogodan da podrži takvu infrastrukturu. Proces izgradnje IPv6 infrastrukture je viđen i kao prilika za razvoj i jačanje nacionalnih proizvođača mrežnih uređaja.

Japan je bio prva zemlja koja je, 2000. godine, izradila Nacionalnu strategiju za usvajanje IPv6, pod nazivom u-Japan (*ubiquitous Japan*) [99]. U okviru ove strategije je predviđena podrška akademskoj zajednici kroz istraživanje u okviru WIDE projekta, kao i poreski podsticaji za organizacije koje razvijaju IPv6.

U-Japan strategijom, pod vođstvom Ministarstva unutrašnjih poslova i komunikacija, nastoji se postići obezbjeđivanje infrastrukture za razvoj novih aplikacija zasnovanih na novim tehnologijama u čijoj pozadini se nalazi IPv6, čime će se pristup Internetu učiniti

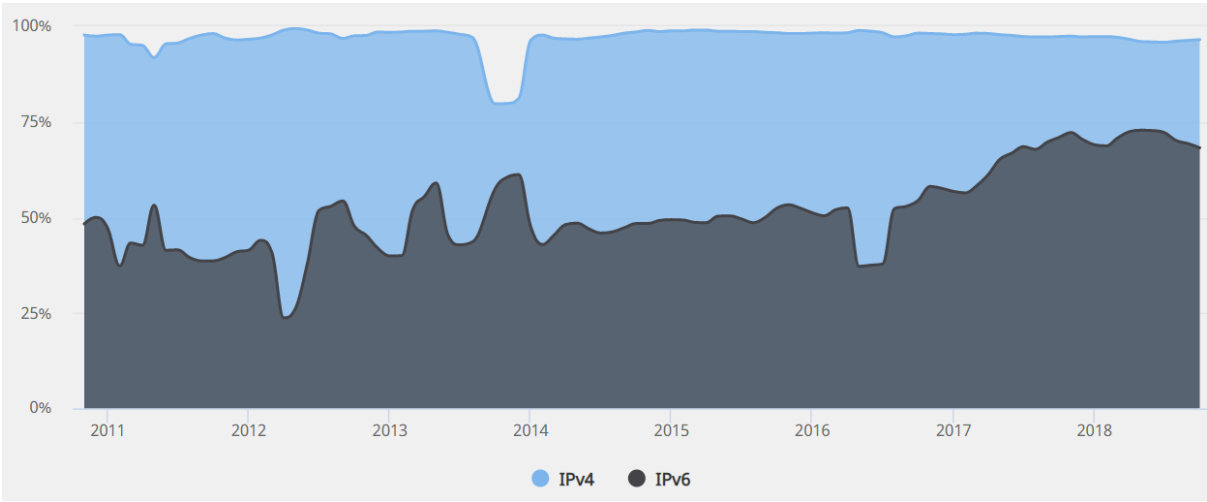
sveprisutnim. Cilj je stvoriti okruženje u kojem „svako može lako pristupiti i koristiti mrežu u bilo koje vrijeme, sa bilo kog mjesta i sa bilo kojeg uređaja“. Koristeći IPv6-bazirane tehnologije, japanski stručnjaci su razvili pionirske programe senzora zemljotresa, uređaje koji se mogu nadgledati i kontrolisati sa udaljene lokacije, te aplikacije koje pomažu da prate lokaciju djece [100].

U oktobru 2000. godine osnovan je Japanski savjet za promociju IPv6 (*IPv6 Promotion Council of Japan*) [101], koji je u početku imao 18 članova i čije su osnovne aktivnosti finansijski podržane od strane japanske vlade. Već do septembra 2002. godine, savjet je brojao 280 članova, iz različitih privrednih oblasti [102]. Savjet je postao najaktivnija i najuticajnija IPv6 organizacija u Japanu, i od vlade je imenovan za kontakt tačku prema inostranim tijelima u smislu tehničke podrške i podrške u implementaciji. Ovaj Savjet je sproveo mnoge aktivnosti tokom 2001. i 2002. godine, od kojih su najvažnije:

- program demonstracije kućnih IPv6 aparata;
- IPv6 *showroom* „Galleria v6“ u Tokiju i Osaki;
- prvi IPv6 Internet prenos koncerta uživo (decembar 2001);
- digitalni video striming srednjoškolskog bejzbol šampionata preko IPv6 DVTS (avgust 2002);
- učešće na „Global IPv6 Summit in China“;
- „IPv6 seminar“ za kompanije i pojedince, ...

Nakon prvih iskustava, Savjet je donio odluku da se težište u narednom periodu stavi na sljedeće aktivnosti: saradnju na globalnom nivou, sigurnost, sertifikaciju i širenje IPv6 aplikacija.

Stanje razvoja IPv6 u odnosu na IPv4 protokol, u Japanu, zaključno sa septembrom mjesecom 2018. godine mogu se vidjeti na slici 26. Japanski provajderi još uvijek uglavnom podržavaju IPv4, mada se ta podrška u poslednje vrijeme smanjuje. Podrška IPv6 protokolu je od 2011. do 2015. godine bila jako promjenljiva, ali se rijetko spuštala ispod 50%. Nakon toga slijedi period prilično uravnoteženog, mada blagog, rasta podrške, sa izvjesnim padom u 2016-toj godini. Danas se, prema [103] podrška IPv6 kreće oko 68%.




Slika 26. Podrška provajdera u Japanu za IPv4 i IPv6 protokol [103]

Prema [103], na vrhu liste provajdera u Japanu koji podržavaju IPv6 nalaze se: *Jpne-ip6*, *Mf-transix-e*, *Mf-transix-w*, *Ocn*, *Bbix*, *Jpne*, *Biglobe*, *Asahi*, *Japan Network Information Center*, i *Iij*.

### 6.3.2. Implementacija IPv6 protokola u Kini

Kina je jedna od zemalja sa najvećim intenzitetom ekonomskog rasta u poslednje dvije decenije. U pojedinim trenucima je čak premašivan cilj koji je postavljala kineska vlada. Na primjer, u prvom kvartalu 2005. godine je ostvaren ekonomski rast od 9,5%, što je premašilo vladino očekivanje od 8% [104]. Ova zemlja je postala i proizvođački centar, gledano u svjetskim okvirima. Međutim, smatra se da ukoliko Kina želi da zadrži trend ekonomskog rasta, osim proizvodnje se mora orijentisati i ka inovacijama. U tom smislu, informaciono-komunikacione tehnologije igraju strateški važnu ulogu. Uzimajući u obzir veliki broj Internet korisnika u Kini, jasno je da IPv6 pruža resurse za podršku gornjim zahtjevima.

Kao najmnogoljudnija zemlja svijeta Kina ima potencijalnu potrebu za velikim brojem IP adresa. Ako bi svaka osoba u Kini (oko 1,38 milijardi stanovnika) imala svoju IP adresu, samo po tom osnovu bi se potrošila skoro trećina raspoloživog IPv4 adresnog prostora (oko 4,3 milijarde adresa). Iako je poznato nastojanje kineskih vlasti da kontroliše informacije, desila se veoma brza ekspanzija Interneta kako bi se olakšao ekonomski razvoj, na kojemu režim temelji svoj legitimitet. Kineska država odigrala je naročito važnu ulogu u poslednjih nekoliko decenija kod izgradnje moderne nacionalne telekomunikacione mreže i međunarodno konkurentnih firmi. Isti pristup se može prepoznati u naporima kineske države u izgradnji kapaciteta za sledeću generaciju Internet tehnologije.

Još 2001. godine je Nacionalna komisija za razvoj i reformu podstakla kreiranje akademske mreže za Internet tehnologije sljedeće generacije, koja je bazirana na Kineskoj obrazovnoj i istraživačkoj mreži (*China Education and Research Net* - CERNET) [105]. U 2003. godini Kina je najavila Nacionalnu strategiju za promociju i usvajanje IPv6. Investirano je 170 miliona dolara kako bi se podržao nacionalni istraživački projekat pod nazivom *China Next Generation Internet* (CNGI). Najmanje 50% narudžbi komunikacione opreme u okviru CNGI projekta realizovano je preko domaćih isporučilaca opreme, što je bio jasan signal da je potrebno unaprijediti sopstveni razvoj proizvoda i aplikacija na bazi IPv6 [99]. Projekat je završen 2005. godine i bio je najveći infrastrukturni IPv6 projekat u svijetu [100].

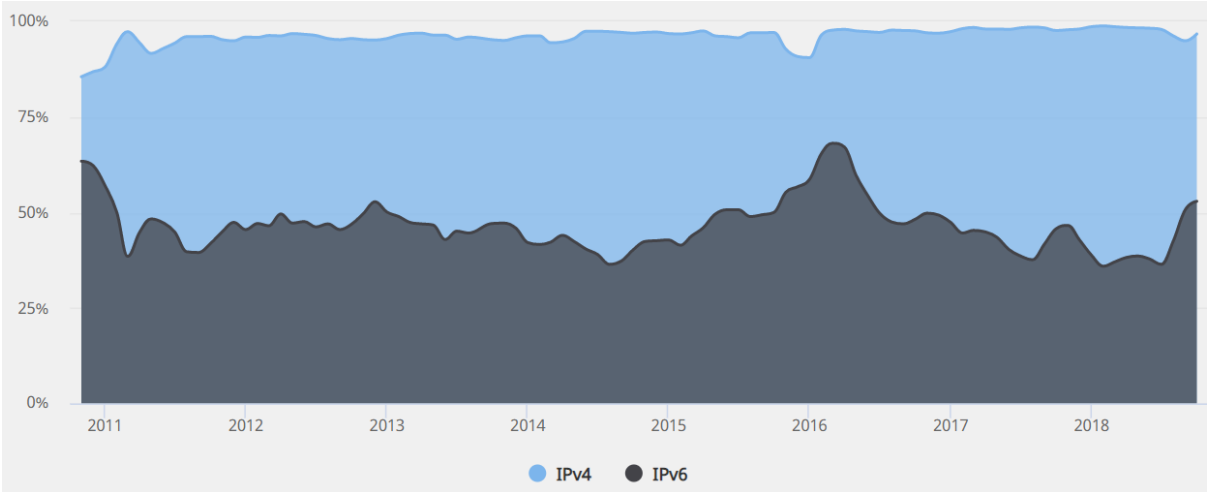
Kina je iskoristila i nekoliko svjetski popularnih i praćenih događaja koji su se odvijali na njenoj teritoriji, kako bi demonstrirala stepen svog ekonomskog i tehnološkog razvoja. Jedan od najvažnijih takvih događaja su bile Olimpijske igre u Pekingu, 2008. godine [106]. Tu je demonstrirana upotreba IPv6 u kontroli objekata i rasvjete, što je umnogome doprinijelo značajnoj uštedi energije. Takođe, taksi vozila su imala ugrađene IPv6 senzore koji su saopštavali svoju lokaciju i stanje u saobraćaju centralnoj kontrolnoj jedinici, koja je nastojala usmjeravati taksiste kako bi se izbjegle zagušene saobraćajnice.

Do kraja 2010. godine, CNGI projekat je rezultirao uspostavljanjem jedne od najvećih komercijalnih okosnica IPv6 mreže sledeće generacije. Nju su sačinjavale pet komercijalnih mreža (China Telecom, China Netcom, China Mobile, China Unicom i China Railcom) i jedna akademska mreža (CERNET2). CERNET2 je prva mreža koja je bazirana isključivo na

IPv6 protokolu, tj. unutar nje nema IPv4 adresiranja. Imala je 25 pristupnih tačaka, koje su međusobno povezane 2,5Gbps ili 10Gbps linkovima. Okosnica je pružala IPv6 servise za više od 200 pristupnih mreža različitih brzina, od 1Gbps do 10Gbps. Predstavljala je i eksperimentalnu platformu na kojoj su pokrenute mnoge zahtjevne aplikacije i testirane nove tehnologije [107].

Pošto se sa više od 700 miliona Internet korisnika 2017. godine kineska vlada suočava sa nedostatkom IPv4 adresa, napravljen je akcioni plan po kome će tokom 2018. godine 200 miliona Internet korisnika biti prebačeno na IPv6. Taj broj treba da naraste na 500 miliona do 2020. godine, a na kraju 2025. godine će sve mreže, aplikacije i krajnji uređaji, prema planu, u potpunosti podržavati IPv6 [108].

Kakvo je stanje razvoja IPv6 u odnosu na IPv4 protokol, u Kini, zaključno sa septembrom mjesecom 2018. godine može se vidjeti na slici 27. Kao i drugdje u svijetu, i u Kini se još uvijek IPv4 protokol podržava u velikom obimu, ali manje nego kod drugih posmatranih zemalja. Podrška IPv6 protokolu je jako promjenljiva i kretala se u opsegu od 38% do 68%. Nakon izvjesnog pada, u poslednje vrijeme je primjetan porast podrške IPv6 protokolu i on se, prema [109] u septembru ove godine kretao oko 53%.

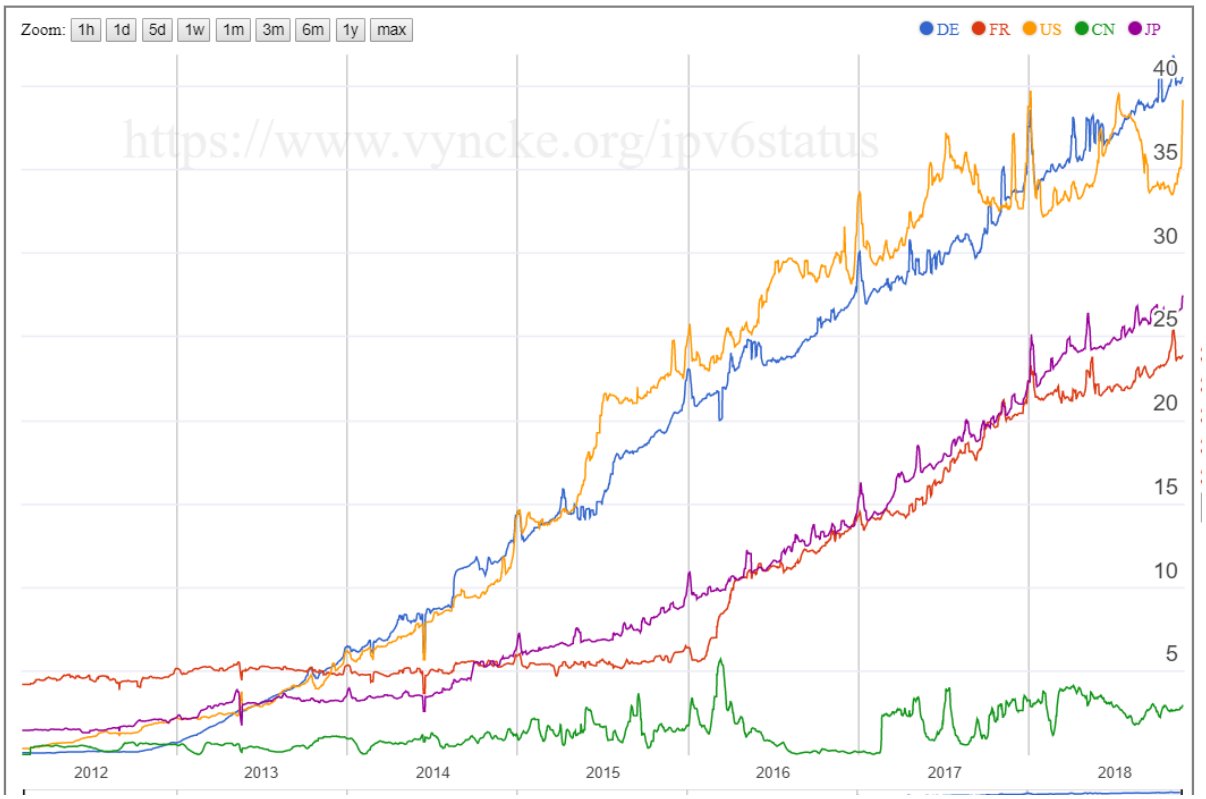



Slika 27. Podrška provajdera u Kini za IPv4 i IPv6 protokol [109]

Prema [82], na vrhu liste provajdera u Kini koji podržavaju IPv6 nalaze se: *CT Networks*, *China Unicom Network*, *China Mobile*, *China Next Generation Internet CERNET2*, *Cngi-cernet2*, *Cernet*, *Zparknet*, *Hurricane Electric LLC*, *Cernet2-tsinghua6*, i *Cstnet*.

Na kraju bi moglo biti interesantno pogledati trendove u korišćenju IPv6 protokola u posmatranim zemljama. Na slici 28 prikazani su podaci dostupni sa [98] koji pokazuju procenat upotrebe IPv6 preglednika (*Internet browser*) u pojedinim zemljama, u poslednjih sedam godina. Kod svih posmatranih zemalja, osim Kine, primjetan je rast upotrebe IPv6 preglednika. Od početka 2015. do kraja 2017. godine, najveći procenat IPv6 Internet preglednika u svom Internet saobraćaju imale su SAD. Sličan trenda rasta upotrebe IPv6 Internet preglednika primjetan je u Njemačkoj, pri čemu je njihov rast značajo ravnomjerniji i danas imaju najveći procenat. Japan i Francuska imaju prilično slične trendove i zaostaju u odnosu na SAD i Njemačku. Prilično mali procenat upotrebe IPv6 preglednika u Kini, prema podacima sa [98], može biti posljedica politike kineskih vlasti koje nastoje kontrolisati protok

informacija pa se na taj način, moguće, ograničava broj IPv6 preglednika kojima uređaji koji sakupljaju podatke za ovu statistiku imaju pristup.




Slika 28. Poređenje upotrebe preglednika koji koriste IPv6 u SAD, Francuskoj, Njemačkoj, Japanu i Kini [98]

# 7. Analiza scenarija za implementaciju IPv6 u Crnoj Gori sa tehničkog i ekonomskog aspekta (posebno za privatni i javni sektor)

Tranzicija postojeće ICT infrastrukture na *dual-stack* Internet protokol (IPv4/IPv6) je projekat sam za sebe. Takvom projektu su potrebni značajni resursi (kadrovi, budžet, vrijeme, plan, ...) i treba mu se pristupiti veoma pažljivo. Pored toga, implementacija se mora odvijati bez prekida u radu postojećih usluga, a ako su prekidi neophodni, moraju biti što kraći. U svakom slučaju, svaku kompaniju i instituciju u procesu migracije očekuju značajni tehnički izazovi.

No, migracija na IPv6 je neizbježna. Pri tome, ekonomski aspekt ove migracije je takođe od velikog značaja, kao i kakav će ukupan ekonomski uticaj imati implementacija IPv6. Koje izazove kompanije i institucije mogu da očekuju?

## 7.1. Pravila implemenacije IPv6

Implementacija migracije mora biti pažljivo planirana. Za upravljanje i promjenu složenih sistema, kao što su računarske mreže i sistemi, *data* centri i slično, primjenjuju se sljedeća dobro poznata pravila:

- dobro planiranje je polovina implementacije;
- dobra dokumentacija je druga polovina;
- oslobađanje od starih stvari ako planirate potpuno novi sistem;
- promjene treba iskoristiti za konsolidaciju i poboljšanje starih struktura;
- inkrementalni (agilni) pristup omogućava kontrolisano vraćanje u slučaju grešaka i sistematsko testiranje svakog koraka;
- migraciju „spolja ka unutra“ treba primjenjivati u odnosu na topologiju mreže;
- migraciju „odozdo prema gore“ treba primjenivati za slojeve OSI modela.

Iz ovih pravila mogu se izvesti dva preporučljiva generalna scenarija za migraciju. U svakodnevnoj upotrebi će se naći kombinacija ova dva scenarija. Kombinacijom ovih scenarija, datih tehničkih preporuka za svaki pojedinačni element ICT infrastrukture i ekonomskih aspekata, dolazi se do detaljnog plana ili scenarija migracije konkretne kompanije ili institucije. Prilikom planiranja migracije na IPv6, važno je i korisno imati precizan cilj projekta i imati na umu misiju kompanije ili institucije.

## 7.2. Faze implementacije IPv6

Implementaciju tranzicije na IPv6 protokol treba uraditi fazno, shodno navedenim pravilima, planski, uz adekvatnu pripremu i edukaciju.

Prva faza za implementaciju je pripremna faza koja je osnov planiranja. U okviru ove faze treba definisati sledeće elemente:

- ciljevi:
    - potreba IPv6 za misiju institucije ili kompanije,
    - vrstu tranzicije (puna ili djelimična),
    - vremenski rokovi i
    - potencijalni izazovi;
- infrastrukturni resursi:
    - provjera podrške IPv6 protokolu i planova zanavljanja infrastrukturnih resursa,
    - redizajn računarske mreže i uređaja,
    - servisi i njihovi funkcionalni ciklusi,
    - mrežne pristupne tačke (WAN i/ili Internet pristup, …) i
    - pružaoci usluga (ISP, javni i privatni servisi, ...);
- ugovori:
    - uključivanje kontakt informacija, uslova korišćenja, amortizacije i ugovora o nivou usluga (SLA).

Preostale faze implementacije su:

- planiranje,
- nabavka opreme i resursa,
- implementacija,
- testiranje i
- dokumentovanje.

Svaku od ovih faza treba da prati određen oblik kontinualne edukacije kadrova i korisnika kako bi bio garantovan uspjeh svih faza implementacije i postignut krajnji cilj projekta.

## 7.3. Scenariji migracije na IPv6

Postoje dva generalna scenarija migracije na IPv6 koja se baziraju na pravilima migracije, a biraju prema ciljevima projekta migracije, dinamici implementacije i raspoloživim resursima. Pored ova dva scenarija postoje i dvije vrste migracije, koje se razlikuju po obuhvatu sistema nad kojim se vrši migracija.

### 7.3.1. Scenario migracije „odozdo prema gore“

Jedan scenario implementacije IPv6 primjenom *dual-stack* tehnike u nekoj računarskoj mreži je primjena principa „odozdo prema gore“ u smislu slojeva OSI referentnog modela. Mrežne komponente, kao što su svičevi i ruteri, će biti prvo pripremljene za IPv6, dok će ostale komponente i servisi (na višim OSI slojevima) i dalje raditi samo na IPv4 protokolu. Ovo je osnova za uspostavljanje IPv6 protokola.

Migraciju treba započeti sa drugim OSI slojem (L2 svičevi), zatim mrežnim OSI slojem (L3 svičevi, ruteri, IP čvorovi), pa onda osnovnim infrastrukturnim servisima kao što su DNS, DHCP, NTP (*Network Time Protocol*), itd. Migracija se završava kada se završi migracija svih potrebnih aplikacija (L7 OSI sloj).

Alati za monitoring i upravljanje mrežom treba da podržavaju IPv6 protokol prije implementacije migracije kod drugih uređaja ili servisa. Ovo je nužno kako bi se mogli nadgledati i kontrolisati rezultati migracije ostalih djelova sistema na IPv6. Postepenom i kontrolisanom migracijom komponente sistema poprimaju IPv6 svojstva, integrišu se u sistem, testiraju i svaki korak se dokumentuje.

Prilikom uključivanja podrške IPv6 protokolu kod novih komponenti treba biti oprezan i razmotriti sve moguće konsekvence, kako na ostatak sistema tako i na samu komponentu. Na primjer, ako *firewall* još nije ispravno konfigurisan, nove komponente mogu uspostaviti komunikaciju sa spoljnim entitetima putem IPv6, iako je takva vrsta komunikacije putem IPv4 blokirana. Da bi se izbegla iznenađenja, ne treba vršiti korake u implementaciji i onda na osnovu prijavljenih grešaka ispravljati podešavanja, već izvršiti planski redizajn kompletne mreže i prilagođenje za IPv6 koncept adresa. Izrada redizajna na osnovu plana migracije, testiranje određenih rješenja (ako je potrebno može se kreirati posebno testno okruženje za kompleksne djelove sistema) i dokumentovanje podešavanja je osnov uspješne migracije.

### 7.3.2. Scenario migracije „spolja ka unutra“

Drugi scenario implementacije IPv6 primjenom *dual-stack* tehnike se koristi kad se želi obezbijediti spoljašnja vidljivost mreže na IPv6, a sama mreža još nije spremna za potpunu migraciju na IPv6. Princip ovog scenarija je implementacija migracije na IPv6, počev od graničnog rutera, kojim je predmetna mreža povezana sa „spoljašnjim okruženjem“, ka unutrašnjosti mreže, do samih čvorova.

Stoga, treba prvo implementirati *dual-stack* u segmentima mreže i kod servisa koji imaju funkcionalnu povezanost sa Internetom ili drugim WAN mrežama („spoljnjim okruženjem“). To može biti, na primjer, *web* portal, administrativni servis, interfejs baze podataka ili pristupna VPN tačka. U ovoj fazi unutrašnja ICT infrastruktura ostaje na IPv4 protokolu.

Migracija unutrašnje mreže (intraneta) se može obaviti u sledećoj fazi projekta. Ovaj pristup osigurava da svi klijenti imaju pristup uslugama nezavisno od adrese koju dobiju od svog provajdera. Razdvajanje mrežnih segmenata u kojima je izvršena migracija od ostalih se vrši putem *proxy*-a, *firewall*-a i drugim vrstama *gateway*-a i konstantno se nadziru iz sigurnosnih razloga.

Dakle, ovo je brza tehnika za omogućavanje IPv6 vidljivosti spolja bez mijenjanja cijele mreže.

### 7.3.3. Parcijalna migracija

Pored ova dva pristupa koja se razlikuju po tehničkoj paradigmi, proces migracije (po nekom od ova dva scenarija) se može izvršiti za čitav sistem ili za određene parcijalne djelove. Dakle, može se primijeniti potpuna ili parcijalna migracija sistema.

Parcijalna migracija iziskuje manje napora i vremena u poređenju sa potpunom migracijom sistema kao cjeline. Izdvojeni servisi ili djelovi mreže postanu brzo dostupni preko IPv6, a stečeno iskustvo se može koristiti u narednim projektima migracije.

Za vrijeme parcijalne migracije koristi se postojeća mreža s instaliranim *proxy* serverima. Komunikacija IPv4/IPv6 završava na *proxy*-ju, a odatle se uspostavlja nova veza sa odredišnom adresom. Ovakvo mapiranje između IPv4 i IPv6 protokola je pogodno jer je iznad transportnog sloja. Na ovaj način, uz male resurse i za kratko vrijeme, određeni servisi mogu biti dostupni za klijente koji već koriste IPv6 za pristup uslugama.

Slična procedura je korisna i kada se IPv4 segmenti mreže povezuju sa IPv6 mrežama ili kada se interno postavljaju mreže koje imaju podršku samo za IPv6 protokol, bez direktnog povezivanja sa okolnim IPv6 okruženjem.

Međutim, parcijalna migracija korišćenjem *proxy*-ja ne funkcioniše za sve vrste servisa, jer određeni protokoli ne mogu biti pokrenuti preko *proxy*-a, pa je i njena primjena ograničena. Ovo posebno važi za neke često korišćene servise kao što su VoIP i video protokoli, neke VPN konfiguracije, itd.

## 7.4. Analiza prednosti i nedostataka migracije na IPv6 sa ekonomskog aspekta i predlog scenarija

Prednosti migracije na IPv6 protokol sa tehničkog apekta su nesporne i jasno eksplicirane u literaturi i prethodnim poglavljima. Ipak, analiza prednosti i nedostataka migracije na IPv6 protokol sa ekonomskog aspekta nije uvijek jasna i nedvosmislena. Uostalom, ekonomski aspekt je presudni elemenat za relativno sporu migraciju na globalnom nivou. Dakle, analiza ovog aspekta za različite nivoe subjekata je uvijek značajan, ako ne i presudan, element same implementacije. To uključuje ne samo velike kompanije, institucije i državnu administraciju, već i rezidencijalne korisnike [110].

Konkretnije, pomenuta migracija bi trebala da ima za posljedicu smanjenje troškova održavanja i razvoja, i/ili poboljšanje sigurnosti i efikasnosti rada poslovnih sistema zasnovanih na informaciono-komunikacionim tehnologijama. Glavni problem kod implementacije IPv6 je relativno ograničen broj ekonomskih i tehnoloških prednosti koje njegova implementacija donosi. Da bi bolje razumjeli uticaj na pojedinačne grupe korisnika, prvo treba detaljno analizirati i izložiti prednosti, mane, šanse i prijetnje koje implementacija IPv6 može nositi sa sobom. Generalizovan primjer ove analize, dat u [110], može biti dobra polazna osnova za partikularne analize pojedinih subjekata.

Prednosti:

- značajno veći broj potencijalnih adresa koje pruža IPv6 protokol omogućava neograničen rast broja Internet korisnika, što je ključno za dalji ekonomski rast ISP-ova;
- konstantna dužina zaglavlja poboljšava efektivnost rutiranja, a hijerarhijski raspored adresnog prostora smanjuje veličinu tabela rutiranja, što u nekim slučajevima produžava životni vijek opreme;
- mogućnost pružanja direktne konekcije između čvorova, poboljšana podrška za sigurnost, viši kvalitet usluga i mobilnost čvorova može pomoći u efektivnijem funkcionisanju multimedijalnih aplikacija.

Šanse:

- mogućnost razvoja potpuno novih servisa i aplikacija (na primjer, onih koje nisu klijent/server orijentisane, IoT servisi, usluge sajber-fizičkih sistema, …);
- mogućnost smanjenja troškova razvoja aplikacija i servisa, pošto će u slučaju IPv6 protokola biti moguće mrežnom OSI sloju predati izvršenje nekih funkcionalnosti (na primjer, uvijek će biti moguće preduzeti mjere za pružanje privatnosti, integriteta i autentičnosti podataka korišćenjem AH i ESP protokola, koji moraju biti podržani prema RFC 4294 [111]);
- mogućnost pravičnijeg dodjeljivanja adresnog prostora može rezultirati smanjenjem stope informacione nepismenosti i digitalnog jaza (želje Međunarodne unije za telekomunikacije (ITU) da pomogne zemljama u razvoju u dobijanju IPv6 adresnog prostora od regionalnih registara (*Regional Internet Registry* - RIR) može se takođe posmatrati u ovom svijetlu);
- mogućnost ubrzanog spajanja servisa zbog podrške mobilnosti;
- mogućnost korišćenja M2M (*Machine to Machine*) komunikacione paradigme.

Mane:

- IPv4 i IPv6 protokoli nisu direktno kompatibilni, što znači da sav hardver i softver mora biti prilagođen za novu verziju Internet protokola;
- pošto je IPv4 protokol omogućio rast Interneta od istraživačke mreže do globalne mreže i pokazao se veoma prilagodljivim, već duže vrijeme je u nekim krugovima Internet zajednice prisutan skepticizam oko brzine njegove zamjene.

Prijetnje:

- nekompatibilnost pojedinačnih implementacija IPv6 protokola ili manjak njihove podrške za pojedinačne funkcionalnosti bi mogao da izazove poteškoće pri uvođenju protokola;
- neiskusno i nedovoljno edukovano osoblje bi značajno moglo da produži implementaciju i poveća troškove kao i sigurnosne rizike;
- nedovoljno edukovano i motivisano osoblje predstavlja ključnu prepreku u implementaciji protokola;
- rizik da inicijatori migracije investiraju u nešto što se potencijalno možda neće odmah isplatiti – možda je sigurnije sačekati dok kritična masa drugih operatora ne izvrši migraciju;
- troškovi razvoja, koje je u nekim slučajevima teško opravdati menadžmentu kompanije.

Osnovni cilj je pripremiti mrežu kako bi ponudila nove usluge, a pri tome zadržati postojeće, bar na istom nivou funkcionalnosti kao prije migracije. Pri implementaciji novih usluga, potrebno je naći makar jednu koja će podstaći brže uvođenje novog protokola. Implementacija protokola u mobilne mreže čini poseban izazov. Potrebno je u svakom trenutku biti svjestan svih ekonomskih prednosti i mana IPv6 naspram IPv4 protokola.

Nije jednostavno izložiti dobru studiju o ekonomskim efektima, a posebno ne sveobuhvatnu, jer svaki ekonomski subjekt treba da izvrši analizu shodno prožimanju svojih poslovnih procesa, planova i efekata sa elementima digitalizacije i samih informaciono-komunikacionih tehnologija. Svakako da ključni izazov stoji u jasnom artikulisanju ekonomskih podsticaja za svaku pojedinačnu kompaniju i istituciju, koja bi morala da uloži sredstva u nešto što se (samo) čini korisnim za društvo, ali ne i ekonomski isplativo.

## 7.5. Operatori javnih elektronskih komunikacionih mreža i usluga (ISP)

Operatori javnih elektronskih komunikacionih mreža i usluga su godinama bili jedini koji su uspjeli u monetizaciji povezivanja pojedinačnih mreža sa Internetom. Njihov poslovni model je najprije bio baziran na jednostavnom dijeljenju pristupa Internetu. Za rezidencijalne korisnike cijena je direktno zavisila od vremena trajanja pristupa, dok je za poslovne korisnike od značaja bio propusni opseg i količina razmijenjenih podataka. Konvergencija pristupnih mreža (težnja ka širokopojasnom pristupu) i potpuna dominacija IP protokola za razmjenu svih vrsta podataka su u posljednjim godinama značajno promijenili poslovni model većine ISP-ova. Danas, osim pristupa Internetu, hostinga i kolokacija servera, ISP-ovi često pružaju usluge telefonije i TV-a (podaci, audio i video sadržaj se često nazivaju *Triple play*), a mnogi od njih takođe rade kao mobilni operatori i integratori sistema.

ISP-ovi najčešće dijele svoju ICT infrastrukturu u dva glavna elementa. Prvi dio je interna, a drugi (dominantniji) dio je infrastruktura namijenjena komercijalnom pružanju usluga krajnjim korisnicima i kompanijama.

Implementacija IPv6 protokola za ISP-ove predstavlja veliki izazov, a osim toga je prisutan rizik vezan za uspješnu implementaciju i uticaj na finansijske indikatore. Takav projekat zahtijeva ozbiljan planski pristup upravo zbog rizika i uticaja vezanih za postojeću infrastrukturu, koja obezbjeđuje većinski, ako ne i kompletan, prihod kompanije. Ovi subjekti ne mogu priuštiti sebi da donesu pogrešnu odluku i nemaju jasan i precizan odgovor na pitanje: *kad, na koji način i kako implementirati i komercijalizovati migraciju na IPv6 protokol*?

**Motivacija za implementaciju IPv6 protokola**

Pošto su ovi subjekti ključni u funkcionisanju Interneta, moglo bi se očekivati da su počeli sa implementacijom IPv6 protokola, ali analiza iz poglavlja 3 pokazuje da to nije tako. Ne samo da nijedan ISP u Crnoj Gori nije započeo migraciju, nego većina i nema istu u zacrtanim planovima. Mnogi od njih su se dugi niz godina mučili sa jednostavnim pitanjem – *zašto implementirati IPv6 protokol ako klijenti to ne zahtijevaju i ne donosi benefite u pogledu poslovanja*? ISP-ovi ne prodaju IP protokol, već rješenje koje povezuje korisnike i njihove mreže sa globalnom Internet mrežom ili drugim mrežama. Za te kompanije, dodatna tehnička rješenja i inovacije zahtijevaju određene investicije u planiranje, implementaciju, testiranje i verifikaciju. Za ova uložena sredstva, skoro je nemoguće izračunati ekonomske faktore koji ukazuju na isplativost investicije.

Jedan od glavnih motivišućih faktora za implementaciju IPv6 protokola kod ISP-ova je povećavanje kompetitivnosti ponude i uvođenje novih usluga. Iako se tehnološke prednosti

korišćenja IPv6 protokola teško mogu direktno povezati sa ekonomskim prednostima, ISP-ovi moraju biti svjesni ekonomskog potencijala kompetitivne prednosti provajdera koji počnu da implementiraju IPv6 protokol i budu spremni da ponude povezivanje na IPv6 Internet za poslovne i rezidencijalne korisnike.

Ipak, kompetitivne prednosti nisu jedini aspekti IPv6 protokola koje će ISP-ovi moći da iskoriste. Pošto IPv6 protokol omogućava mnogo veći adresni prostor i hijerarhijski raspored adresa, može se očekivati da će, zbog efikasnijeg rutiranja i napuštanja IPv4 protokola, zamjena hardvera biti značajno rjeđa, što će smanjiti troškove investicija.

Glavni motiv migracije na IPv6 kod ISP-ova bi trebao biti postavljanje nove mrežne infrastrukture i servisa prije konkurencije, kako njihovi korisnici ne bi promijenili pružaoca usluga zbog pristupa IPv6 sadržaju. Veoma kompleksnu migraciju treba uraditi prema gore navedenim pravilima i scenarijima, a priprema zahtijeva analizu i planiranje u mnogim oblastima koje su dijelom ovdje navedene, a većim dijelom definisane internim pravilima samih kompanija.

Uzimajući u obzir dosadašnja iskustva i sve usluge koje ovi operatori pružaju danas, uglavnom u smislu tehnološke kompleksnosti, metod za implementaciju IPv6 protokola je prilično jasan i uobičajen: parcijalna migracija po scenariju „odozdo prema gore“. Pošto se funkcionisanje skoro svih servisa oslanja na razmjenu IP podataka sa drugim provajderima, tokom prve faze implementacije se preporučuje da ISP-ovi omoguće poslovnim korisnicima direktnu IPv6 konekciju, a nakon prilagođavanja opreme i IPv6 konekciju rezidencijalnim korisnicima. Nakon toga treba početi širenje podrške za *data* centre, usluge hostinga i ko-lokacije servera. U većini slučajeva su IP telefonija i TV usluge odvojene od Interneta, a veze između mreža pojedinačnih operatera su pod strogom kontrolom. Nadalje, nivo tehničke podrške za novi protokol za terminalne uređaje je relativno ograničen. Zbog ovoga, implementacija IPv6 protokola u ove ograničene segmente će najvjerovatnije biti završena kasnije, shodno daljim tehnološkim inovacijama i politici kompanije.

Troškovi implementacije migracije zaslužuju pažnju zato što moguće greške u implementaciji i neiskusno osoblje mogu da rezultiraju prekoračenjem predviđenih rokova i ozbiljnim ugrožavanjem funkcionisanja kompanije. Iskustva u implementaciji pokazuju da je većina troškova povezana sa edukacijom osoblja i testiranjem. Nadalje, treba imati u vidu troškove koji se odnose na prilagođavanje alata za kontrolu i upravljanje mrežom, kao i troškove neophodne za zamjenu hardvera i softvera. Konačno, iskustva pokazuju da operativni troškovi (OPEX) imaju mnogo veći udio od kapitalnih troškova (CAPEX) u implementaciji IPv6 protokola.

## 7.6. Provajderi sadržaja i aplikacija

Poslovni modeli provajdera sadržaja i aplikacija najčešće direktno zavise od broja korisnika. Činjenica da je implementacija IPv6 protokola njima jednako važna kao i ISP-ovima može se demonstrirati na primjeru korisnika koji želi pristupiti jednoj od društvenih mreža ili informativnih portala. Pošto korisnik dolazi iz jedne od zemalja u razvoju, gdje njegov ISP nije mogao da mu dodijeli IPv4 adresu, a provajder zbog dodatnih troškova ne koristi NAT tehnologije, korisniku je dodijeljena samo IPv6 adresa. Ali, kako dvije verzije protokola nisu

kompatibilne, korisnik nije u mogućnosti da koristi željenu aplikaciju. Ovakve okolnosti sužavaju broj potencijalnih korisnika, a time i prihode. Iz ovog razloga je odluka o uvođenju novog IP protokola ekonomski potpuno opravdana.

Ova vrsta usluga je malo zastupljena u Crnoj Gori, ali to ne znači da neće biti u budućnosti i da se o tome ne treba voditi računa, kada je riječ o procesu migracije.

Za ove subjekte je preporučljivo da izvrše, obzirom na njihove kapacitete u Crnoj Gori, potpunu migraciju po scenariju „spolja ka unutra".

## 7.7. Poslovni korisnici

Internet danas igra ključnu ulogu u poslovnim okruženjima: od interne komunikacije elektronskom poštom, preko servisa za razmjenu poruka i Internet telefonije do razmjene podataka između aplikacija za upravljanje kompanijom i planiranje proizvodnje (*Enterprise resource planning* - ERP). Iako poslovnim korisnicima veoma rijetko nedostaje adresnog prostora, jer većina ovih korisnika uspješno rade sa samo jednom ili par javnih adresa, problemi se pojavljuju pri povezivanju dva ili više ovakvih korisnika. Pojednostavljenje procesa povezivanja poslovnih korisnika je od velike pomoći informatičkoj podršci za poslovne procese.

Mogućnost direktnog povezivanja između čvorova pomoću IPv6 protokola može pomoći u boljoj integraciji telefonije i sistema za razmjenu poruka, kao i povećati frekvenciju njihovog korišćenja između pojedinačnih poslovnih korisnika. Iako je sada razmjena elektronskih poruka između organizacija neograničena, ipak bi korišćenje Internet telefonije značajno smanjilo troškove komunikacije unutar kompanija, kao i između poslovnih korisnika u jednoj kompaniji i klijenata ili dobavljača u drugoj kompaniji.

Još jedan ekonomski razlog za implementaciju IPv6 protokola može biti smanjivanje troškova korišćenja specijalizovanih rješenja. Na primjer, nakon implementacije IPv6, svi čvorovi će biti u mogućnosti da izvrše IPSec sesije za koje su se do sada koristili posebni VPN serveri.

Kao i kod ISP-ova, može se očekivati da će u poslovnim sredinama najveći dio troškova biti vezan za edukovanje administratora pojedinačnih sistema, što je posebno bitno za sredine gdje većinu održavanja rade sopstveni sistemski i mrežni administratori, odnosno gdje ti zadaci nijesu povjereni specijalizovanim kompanijama. Ako postoje posebne privatne aplikacije koje su razvijene za ograničen broj korisnika u toj sredini, mogu se očekivati veći troškovi, budući da će prelaženje sa IPv4 protokla zbog ovoga biti usporeno. Korišćenje dva protokola istovremeno najčešće znači više troškove održavanja zbog kompleksnijih konfiguracija komponenata mreže i infrastrukture servera koji su neophodni.

Za ove subjekte je preporučljivo da koriste parcijalnu migraciju po scenariju „spolja ka unutra".

## 7.8. Rezidencijalni korisnici

Rezidencijalni korisnici predstavljaju veoma važan izvor prihoda za praktično sve ISP-ove, pa će zbog toga proces implementacije na nivoima rezidencijalnih korisnika i ISP-ova biti usko povezani. Uzimajući u obzir da iza velikog broja javnih adresa postoji neka vrsta lokalne

mreže, migracija na IPv6 protokol će zahtijevati zamjenu uređaja za povezivanje, što svakako povećava troškove korisnika.

Ako ISP obezbjeđuje širokopojasne modeme (pristupne ili terminalne uređaje), koji funkcionišu na L2 OSI nivou, većinu troškova migracije će snositi sam korisnik, jer treba da omogući zamjenu širokopojasnog rutera (L3 OSI nivo). U slučaju da ISP, boreći se za veći dio tržišta i korisnika, koristi funkcionalnosti L3 OSI nivoa na pristupnim uređajima, troškovi zamjene pristupne opreme su manji, jer ISP obezbjeđuje pristupni uređaj koji u sebi integriše više funkcionalnosti.

Ipak, bez obzira na vrstu pristupnih uređaja, rezidencijalni korisnik pri migraciji na IPv6 protokol koji mu njegov ISP pruža mora sam da snosi troškove zamjene hardvera i softvera koji ne podržava IPv6. To najčešće uključuje lične kompjutere, telefone, televizore, itd., odnosno svu opremu koja koristi IP protokol.

Za rezidencijalne korisnike se preporučuje da izvrše potpunu migraciju po scenariju „odozdo prema gore“.

## 7.9. Provajderi hardvera i softvera

Iako se provajderi hardvera i softvera suočavaju sa istom dilemom kao i ISP-ovi i provajderi sadržaja, što se tiče uvođenja IPv6 protokola, dizajneri operativnih sistema su odlučili relativno rano da inkorporiraju IPv6 podršku u svoje sisteme. Na primjer, *Microsoft* je počeo implementaciju IPv6 podrške od *Windows* XP operativnog sistema, koji se pojavio na tržištu 2002. godine. Ova podrška IPv6 protokolu na nivou operativnih sistema je podsticaj i komparativna prednost za razvoj novih aplikacija koje mogu profitirati od prednosti IPv6 protokola.

Slično operativnim sistemima, IPv6 protokol u aplikacijama nije imao značajan uticaj na razvoj tržišta, jer su pojedinačni proizvođači implementirali podršku relativno rano. Na primjer, dva često korišćena *web* servera (*Apache* i *Microsoft IIS*) odavno podržavaju IPv6 (prvi od 2002. godine, a drugi od 2003. godine). Ipak, razvoj novih aplikacija koje se mogu koristiti isključivo u vezi sa IPv6 protokolom napreduje veoma sporo.

Situacija je malo drugačija kod inovativnih aplikacija koje mijenjaju postojeće paradigme korišćenja i efikasno koriste prednosti IPv6 protokola. Način na koji ovo funcioniše je jasno vidljiv u *Microsoft*-ovom rješenju za daljinski direktni pristup, čime se eliminiše razdvajanje između poslovnog okruženja i Interneta, kao i kod inovativnh IoT aplikacija. Klijentima ovaj sistem omogućava direktno i permanentno pristupanje za to prilagođenim izvorima na Internetu uz značajno pojednostavljenje njihovog upravljanja. Dakle, samo provajderi softvera koji nude inovativne aplikacije će implementacijom IPv6 protokola povećati svoje konkurentske prednosti.

Slična situacija važi i za proizvođače hardvera koji je, sa aspekta IP protokola, neodvojiv od softvera. Segment u kojem će inovacija biti posebno istaknuta kod korisničke opreme će iskoristiti prednosti implementacije IPv6 protokola. Dosadašnja iskustva pokazuju da će u ovom slučaju važnu ulogu odigrati i softver otvorenog koda.

Ovi subjekti će pratiti zahtjeve klijenata i direktive svojih dobavljača tako da neki poseban scenario za njih nije specificiran, a njihovi proizvodi i servisi su velikim dijelom spremni za impementaciju IPv6 protokola [112].

## 7.10. Sistem integratori

Za sistem integratore, implementacija IPv6 protokola prvenstveno znači veliku poslovnu priliku, jer će zbog prilično ograničenog iskustva sa njegovom upotrebom u praksi, potražnja za uslugama obuke i konsultacijama porasti u narednim godinama. To za sistem integratore znači da će ovladavanje novom verzijom IP protokola u ranoj fazi biti od ključnog značaja, jer će to biti jedini način da se poveća prednost u odnosu na konkurenciju u pripremi i izvođenju kurseva obuke i pripremi strategija implementacije IPv6 protokola u okruženja ISP-ova i poslovnih korisnika.

Investicije u sticanje znanja i iskustva iz oblasti IPv6 mogu se sa stanovišta očekivane dobiti i potražnje posmatrati kao strateške investicije. Da bi se smanjili troškovi, postoji niz alternativnih metoda obrazovanja koje su već dostupni: od sprovođenja internih treninga do obrazovanja na daljinu i saradnje na tematskim radnim grupama, konferencijama i simpozijumima. Konačno, troškovi testiranja i verifikacije pojedinačnih rješenja mogu se smanjiti korišćenjem alata za simulaciju i virtuelizaciju.

Ovi subjekti će pratiti zahtjeve klijenata i trendove na tržištu, te neki poseban scenario, u tehničkom smislu, za njih nije specificiran.

## 7.11. Državne institucije

Javni sektor, odnosno državne institucije i agencije treba da budu jedan od glavnih pokretača i katalizator na tržištu IPv6 opreme i usluga. Činjenica da motivacija za uvođenje IPv6 ne može biti isključivo ekonomska nameće osnov za tvrdnju da javni sektor može imati odlučujuću ulogu u uspješnom uvođenju IPv6 protokola. Vlada, ministarstva, državne institucije i agencije, državni univerzitet i drugi potrošači budžeta iz javnog sektora mogu koristiti dva, u svijetu primjenjivana, modela kako bi podstakli uvođenje IPv6.

Sa jedne strane, Vlada može na administrativnom nivou odlučiti da od svih subjekata iz javnog sektora zahtijeva implementaciju IPv6 protokola i na taj način poveća potražnju za opremom koja omogućava njegovo korišćenje i uslugama vezanim za njegovu implementaciju. Samim tim bi i svi ostali subjekti (ISP-ovi, poslovni korisnici, rezidencijalni korisnici, sistem integratori, provajderi softvera i hardvera, provajderi sadržaja i aplikacija i sistem integratori) koji imaju poslovne odnose sa javnom administracijom morali početi sa implementacijom IPv6 protokola. Takvu su odluku, na primjer, donijele SAD i Kina i na taj način nesumnjivo pokazale da su implementaciju IPv6 protokola tretirali kao stratešku odluku za održavanje tehnološke progresivnosti.

Sa druge strane, Vlada se može odlučiti da podstakne potražnju za IPv6 protokolom i njegovu upotrebu tako što će uključiti zahtjeve za njegovu podršku na javnim tenderima. Mogu i neki tehnološki napredniji korisnici, a ne samo javni sektor, početi da pripremaju tendere na takav

način da zahtijevaju hardver koji omogućava korišćenje osnovnih funkcionalnosti IPv6 protokola.

Imajući u vidu specifičnosti i rezultate poglavlja 3, ovdje možemo predložiti scenario „spolja ka unutra“ za implementaciju migracije na IPv6 protokol u javnom sektoru Crne Gore. Nakon finalizovanja ovog dokumenta i njegove javne promocije, isti treba staviti na uvid i korišćenje svim subjektima u Crnoj Gori, a dalje aktivnosti sprovoditi prema dolje navedenim koracima.

- Formirati nacionalno tijelo ili tim za migraciju na IPv6 koji će napraviti akcioni plan, koordinisati aktivnosti, promovisati i pratiti proces migracije.
- Podstaći i organizovati promociju prednosti IPv6 protokola i edukaciju o tehnikama migracije subjekata na svim nivoima javne administracije i rezidencijalnih korisnika.
- Formirati preporuke i smjernice državnim institucijama u pogledu implementacije IPv6 na administrativnom nivou.
- Formirati laboratoriju, u okviru CIS-a UCG, za testiranje koraka tranzicije na IPv6.
- Izvršiti plansku migraciju u mreži Univerziteta Crne Gore na IPv6 putem *dual-stack* tehnologije prema scenariju „spolja ka unutra“, kao pilot projekat na osnovu kojeg će se dokumentovati stečeno iskustvo i znanje koje se može primijeniti na ostale državne institucije.
- Pripremiti plan migracije za državne institucije na osnovu Projekta i dokumentovanih aktivnosti UCG-a.
- Izvršiti migraciju državnih institucija primjenom *dual-stack* tehnologije na IPv6 protokol.

Na ovaj način bi se planski i postepeno, bez narušavanja poslovnih procesa i angažovanja enormnih resursa, izvršila migracija državnih institucija na IPv6 protokol, a time bi se (vjerovatno i prije početka ove migracije) podstakli ostali subjekti da izvrše pripreme i prelazak na novi IP protokol. To bi doprinijelo razvoju novih inovativnih servisa, povećalo sigurnost komunikacija i podataka i omogućilo digitalizaciju društva u punom smislu te riječi.

# 8. Preporuke za implementaciju IPv6 u javnim ustanovama u Crnoj Gori

Imajući u vidu predloženi scenario za državne organe, korake za plansku i postepenu implementaciju IPv6 protokola, kao i tehničke preporuke iz prethodnog teksta, ovdje će biti opisane generalne preporuke za implementaciju IPv6 protokola u javnim ustanovama u Crnoj Gori. U pitanju su preporuke generalnog karaktera, u čijoj sistematizaciji su korišćeni primjeri dobre prakse u implementaciji IPv6 protokola [64] [110] [113], zasnovani na pristupu migraciji IPv4/IPv6 identičnom onom koji se predlaže za Crnu Goru. Tako koncipirane preporuke treba uzeti u obzir prilikom kreiranja akcionog plana i konkretnih projekata za neposrednu implementaciju migracije na IPv6, pri čemu je neophodna njihova dalja razrada u cilju prilagođenja konkretnom infrastrukturnom i poslovnom okruženju. Državne institucije se razlikuju po svojim zadacima, funkciji i veličini, pa zbog toga ne postoji jedinstveni postupak migracije koji odgovara svima. Kako je neophodno da procesu migracije prethodi adekvatna priprema i projekat migracije u svakom pojedinačnom slučaju, moguće je da dođe i do određenih odstupanja, na nivou detalja, od datih preporuka.

Od suštinske važnosti za javne ustanove u Crnoj Gori je da ponude svoje usluge, za početak one koje su javno dostupne, putem IPv6 protokola. Prelazak na IPv6 (*dual-stack* ili samo IPv6) treba iskoristiti i kao šansu za redizajniranje ICT infrastrukture u javnoj upravi za dugoročni period, u smislu poboljšanja performansi i sigurnosti u postojećim mrežama.

Ovo poglavlje daje preporuke za tehnički prelazak na infrastrukturu koja podržava IPv6 protokol, fokusirane na potrebe javne uprave, a usmjerene na cilj migracije na IPv4/IPv6 *dual-stack* okruženje. Kako je već naglašeno, *dual-stack* tehnika omogućava novim klijentima pristup uslugama pomoću IPv6, uz dalje funkcionisanje starih sistema sa IPv4 pristupom uslugama. Dugoročni cilj „samo IPv6“ nije u fokusu ovih preporuka.

U okviru poglavlja je dat skup kontrolnih lista koje se mogu koristiti za dokumentovanje početne situacije, za izvođenje koraka implementacije i konačno za provjeru rezultata. Preporučuje se da se prvo radi u testnom laboratorijskom okruženju da bi se, nakon sticanja praktičnog iskustva, uspješno izvela implementacija migracije na IPv6.

## 8.1. Metod implementacije IPv6

Za pripremu i planiranje IPv6 migracije, mogu se koristiti tzv. kontrolne liste. Preporučuje se detaljno analiziranje sledećih preporuka prije nego što zaista započne sama migracija.

- Prelazak IP mreže (IPv4 u *dual-stack*) treba da bude izveden u više koraka (parcijalno), po scenariju „spolja ka unutra“, počevši od WAN-pristupa (Internet ili spoljašnje mrežne veze), preko DMZ-a (*DeMilitarized Zone*), prema podmrežama zaposlenih.

    - Prvo treba omogućiti IPv6 na WAN pristupnim tačkama i to pomoću *dual-stack* tehnologije ili, ako je ISP to ne podržava, putem kriptovanog IP tunela sa fiksnom IP adresom.
    - Nakon toga, migraciju treba primijeniti na sisteme za monitoring i upravljanje.
    - Zatim, podmreže i interne servere u DMZ zoni treba migrirati jedan po jedan.
    - Kada se to uradi, DNS servisu se mora dodati podrška za IPv6 protokol, tako da se AAAA zapisi mogu tražiti od klijenata i isporučivati klijentima.
    - Konačno, nakon DNS-a mogu migrirati i klijentske podmreže i sami čvorovi.
- Ne bi trebalo koristiti mehanizme translacije IPv4/IPv6.
    - Ako je negdje neophodna translacija između IPv4 i IPv6 protokola, treba koristiti *proxy* server za tu svrhu.
- Generalna preporuka je i da se migracija LAN mreža realizuje *dual-stack* tehnikom IPv4/IPv6 (nakon migracije WAN pristupa i DMZ-a).
    - IPv4 saobraćaj i IPv6 saobraćaj treba da se prenose preko istih fizičkih i/ili virtuelnih mreža (ne treba koristiti paralelne infrastrukture). Dodatno, odvojeni VLAN-ovi se ne preporučuju jer značajno uvećavaju troškove upravljanja i održavanja;
- Ne bi trebalo koristiti VLAN označavanje (VLAN *tagging* prema IEEE 802.1q) direktno na čvorovima. Ovo posebno važi za radne stanice, a za servere se može primijeniti, ali uz analizu za svaki pojedinačni slučaj.
- Potpuni prelazak na samo IPv6 protokol u ovom trenutku i za postojeću infrastrukturu još nije preporučljiv. Naime, veliki broj i raznolikost komponenti, usluga i softvera zahtijeva vrlo velike resurse kako bi se osiguralo da svi ovi elementi mogu bezbjedno i funkcionalno koristiti samo IPv6, bez IPv4 mrežne podrške. To ne znači da pojedini djelovi sistema (na primjer VoIP infrastruktura) ne treba da imaju samo IPv6 infrastrukturu, zbog svoje specifičnosti i prednosti koje im ista daje.
- Tamo gdje se IP mreže (ili podmreže) uspostavljaju od početka, vrijedi razmisliti o pokretanju samo IPv6 protokola. Ova opcija, ako je tehnički izvodljiva, izbjegava nepotrebno uvećavanje troškova i resursa za upravljanje IPv4 mrežom.

Gore navedeni redoslijed koraka treba upotpuniti preporukama za pojedinačne infrastrukturne elemente koje su date u ovom dokumentu. Svakako, treba dodatno konsultovati literaturu, dobavljače opreme i primjere dobre prakse, kako bi obezbijedili uspješnu migraciju na novi IP protokol.

## 8.2. Struktura mreže i adresiranje uređaja

U daljem tekstu sažeto su prikazane najvažnije tehničke smjernice i preporuke za IPv6 migraciju, shodno primjeru [113], koje koriste 3 nivoa preporuka: „mora“, „treba“ i „može“.

Nivo „mora“ predstavlja opis karakteristika, konfiguraciju ili obradu koja se mora obaviti na opisani način, iz tehničkih ili administrativnih razloga. U suprotnom se ne može obezbijediti planirano ponašanje sistema. Ovaj nivo preporuka je obavezan.

Nivo „treba“ predstavlja opis karakteristika, konfiguraciju ili obradu koja se smatra sigurnom i korisnom, na osnovu tehničkog iskustva. Međutim, u zavisnosti od konkretne situacije i lokalnih zahtjeva, odstupanje od ove preporuke je dozvoljeno.

Nivo “može“ predstavlja opis karakteristika, konfiguraciju ili obradu koja je opciona. Ove preporuke nijesu obavezne.

### 8.2.1. Segmentacija mreže

Veličina IPv6 adresnog prostora omogućava strukturiranje prostora podmreža na razne načine. Prilikom segmentacije treba podesiti mrežne prefikse tako da svaka IPv6 podmreža sadrži dovoljno IP adresa za čvorove, odnosno mrežne interfejse u podmreži. Upravo segmentaciju mreže u procesu migracije treba realizovati postepeno, kao skup pod-akcija, jednu po jednu IP podmrežu, sukcesivno.

Tokom ovog procesa, IPv4 podmreže se mogu restrukturirati u svrhu pojednostavljenja postojeće mrežne strukture.

- Prvi korak može uključiti konsolidaciju opsega adresa i spajanje semantički ekvivalentnih IP podmreža.
- Restrukturiranje postojećih IPv4 podmreža je poseban korak i mora se pažljivo planirati i testirati. Planirano restrukturiranje treba da se izvrši prije bilo kakve migracije IP podmreža na *dual-stack* IPv4/IPv6.
- Ne preporučuje se restrukturiranje IPv6 podmreža bez restrukturiranja odgovarajućih IPv4 podmreža.
- IPv4 podmreže treba da budu semantički usklađene sa odgovarajućim IPv6 podmrežama. Ovo olakšava razumjevanje i održavanje pravila koja su konfigurisana za *dual-stack* na ruterima i *firewall*-ima, čime se zadržava postojeći nivo sigurnosti mreže.

Mogu se koristiti IPv6 podmreže sa više od 254 ($2^8$) čvora.

- IPv6 podmreže sa čvorovima (radnim stanicama) moraju da koriste prefiks /64, budući da se zadnja 64 bita IPv6 adrese koriste za identifikatore interfejsa.
- Svi čvorovi unutar jedne IP podmreže moraju biti semantički ekvivalentni, jer se liste kontrole pristupa (*Access Control Lists* - ACL) obično definišu po IP podmreži.
- Treba imati na umu ograničavajući tehnički faktor da je veličina tabele MAC adresa kod L2 svičeva 12.000 adresa.
- Segmentacija podmreža, ili čak čitav intranet neke institucije, može biti izostavljena ako svi čvorovi (po podmreži) imaju iste zahtjeve u pogledu zaštite. Ovo smanjuje broj podmreža, čime se pojednostavljuje upravljanje za podmreže, rutere i ACL-ove.

Isti VLAN treba da se koristi za odgovarajuće IPv4 i IPv6 podmreže.

- Odvojeni VLAN-ovi za IPv4 i IPv6 bi povećali troškove upravljanja i zakomplikovali bi pronalaženje problema, kad do njih dođe. Pored toga, korišćenje dva VLAN-a zahtjeva dodatni angažman kada se uvode nove mrežne funkcije ili usluge.

Ako je moguće, ista porodica protokola za rutiranje (npr. OSPF ili RIP) treba da se koristi i za IPv4 i za IPv6.

- Za IPv6 rutiranje mora se koristiti verzija protokola koji podržava IPv6. Ovo takođe znači da se za sve pripadajuće rutere mora provjeriti da li podržavaju odgovarajuće protokole rutiranja za IPv6.

Treba izbjegavati različite putanje za IPv4 i IPv6 saobraćaj.

### 8.2.2. Dodjela IPv6 adresa

#### Za radne stanice

Konfiguracija IPv6 adrese kod radnih stanica treba da se realizuje pomoću *Stateful* DHCPv6.

- Ako čvorovi dobijaju svoju IPv4 adresu preko DHCP-a, onda bi trebali i da dobijaju svoju IPv6 adresu preko *Stateful* DHCPv6.
- U malim, jednostavno strukturiranim podmrežama, može se koristiti SLAAC (*Stateless Address Autoconfiguration*) pristup, kako bi se pojednostavilo upravljanje IT infrastrukturom.
- SLAAC bi trebalo koristiti samo u kombinaciji sa *Stateless* DHCPv6. Ova opcija se može koristiti za distribuciju dodatnih podešavanja kao što je, na primjer, DNS server koji će koristiti čvorovi.

Ako se koristi centralni DHCP server, onda ruteri i L3 svičevi moraju podržavati IPv6 DHCP funkciju (*relay*) za distribuciju IPv6 adresa.

Ako se koristi SLAAC za generisanje IPv6 adresa, čvorovi bi trebali po *default*-u imati uključen PEX (*Privacy Extensions*).

- Čvorovi kojima je iz nekog tehničkog razloga potrebna fiksna IP adresa ne smiju koristiti PEX.

Zbog privatnosti, ne bi trebalo koristiti IPv6 adrese izvedene iz MAC adrese interfejsa (EUI-64 tip).

#### Za servere

Serveri moraju da koriste fiksnu tj. statičku IPv6 adresu na interfejsu koji je povezan na IPv6 podmrežu.

- Dodjeljivanje IPv6 adrese za servere treba da se realizuje preko DHCPv6. Drugi način je da se statička IPv6 adresa ručno konfigurirše na serveru.
- Dodijeljene IP adrese moraju biti registrovane u DNS-u (A i AAAA zapisi za IPv4 i IPv6, respektivno). AAAA zapisi za server treba da se unose samo u DNS, kada server, njegov servis i mreža već podržavaju IPv6.

Servis bi trebao da očekuje zahtjeve samo na IPv6 adresi na kojoj taj servis mora biti dostupan.

Treba izbjegavati višestruko grupisanje servera, tj. povezivanje sa više IP mreža (*Multi-homing*).

Serveri bi trebali da budu dostupni preko IPv4 i IPv6 koristeći isto ime domena.

**Za hostove generalno**

*Dual-stack* hostovi bi trebalo da imaju samo jednu aktivnu *unicast* IPv6 adresu (po interfejsu), pored *link-local* IPv6 i IPv4 adrese.

- Ova IPv6 adresa treba da bude tipa GUA ili ULA.
- Host može imati više IPv6 adresa na interfejsu (npr. jednu GUA i jednu ULA, ili dvije GUA). U ovom slučaju, sve ove IPv6 adrese moraju pripadati istoj sigurnosnoj zoni.

### 8.2.3. DNS

DNS je jedan od centralnih elemenata za funkcionisanje Interneta. Za upotrebu sa IPv6, DNS podržava tip AAAA zapisa, pored A zapisa za IPv4. DNS protokol dozvoljava upite za A i AAAA zapise nezavisno od toga da li je upit došao preko IPv4 ili IPv6 protokola.

- DNS serveri moraju biti u stanju da upravljaju AAAA zapisima, čitaju ih i isporučuju.
- DNS serveri moraju prihvatiti i odgovoriti na upite preko IPv4 kao i preko IPv6 protokola. DNS server ne može direktno zaključiti koja je IP konekcija klijenta, jer klijenti sami odlučuju koji će se IP protokol koristiti za upite ka DNS serveru.
- Hostovi koji već imaju A zapis u DNS-u moraju takođe dobiti AAAA zapis, nakon što su migrirani na IPv4/IPv6 *dual-stack*.
- *Dual-stack* hostovi navedeni u DNS-u trebaju imati svoje IPv4 i IPv6 adrese povezane s istim imenom hosta.
- DNS server mora dati isti odgovor bez obzira da li je klijentski zahtjev stigao putem IPv4 ili IPv6 protokola.
- DNS serveri moraju biti konfigurisani tako da podržavaju ispravnu IP povratnu pretragu (*reverse lookup*) za IPv4 kao i za IPv6 protokol.

## 8.3. Komponente koje se odnose na sigurnost

Pored brojnih prednosti koje donosi sa tehničkog aspekta, migracija na IPv6 protokol predstavlja izazov sa aspekta sigurnosti mreža i korisnika zbog dupliranja funkcionalnosti i povećane kompleksnosti sistema. Iz tog razloga, projektu implementacije IPv6 protokola potrebno je pristupiti krajnje pragmatično i najprije sagledati trenutno stanje arhitekture i konfiguracije mreže. Prije upuštanja u tehničke aspekte implementacije novih funkcionalnosti IPv6 protokola, neophodno je sagledati model prijetnji u trenutnom sistemu, i prilagoditi ga novonastalim okolnostima i novim resursima. Neophodno je da konfiguracija svih postojećih mehanizama zaštite IPv4 protokola bude implementirana na ekvivalentan način i za IPv6 funkcionalnosti, kako bi mreža zadržala sigurnosna svojstva. Ukoliko postojeća konfiguracija mreže ne uzima u obzir prijetnje vezane za sigurnost, preporučuje se ponovna evaluacija rizika u svijetlu savremenih trendova na Internetu.

Kvalitetna i kontinualna edukacija tehničkog osoblja na teme novih funkcionalnosti IPv6 protokola, kao i (starih) mehanizama i principa zaštite računarskih mreža, je jedan od preduslova za uspješnu implementaciju novog protokola. Prilikom odabira dodatnih softverskih i hardverskih rješenja neophodnih za realizaciju projekta, preporučuje se pažljiv

odabir vendora na osnovu reputacije, kvaliteta podrške, kao i dokazane agilnosti u reagovanju na novootkrivene ranjivosti.

Dok *firewall* komponente tradicionalno predstavljaju prvi obruč zaštite i korisne su u izolovanju segmenata i resursa mreže na osnovu prethodno definisanog modela prijetnji sistemu, bitno je napomenuti da ova vrsta zaštite ima za cilj samo da smanji „površinu mogućeg napada“ filtrirajući saobraćaj koji nije očekivan, ali ne i da izvrši autentifikaciju izvora ili provjeru autentičnosti podataka. Korisna analogija je da *firewall* zaštita „zaključava“ sporedne ulaze jednog sistema, ali ne i glavni ulaz. Stoga je neophodna zaštita bazirana na kriptografskim mehanizmima i protokolima putem koje se vrši autentifikacija izvora komunikacije, provjera autentičnosti podataka, kao i sama povjerljivost.

U daljem tekstu su rezimirane preporuke konfiguracije sigurnosnih komponenti.

**Proxy**

*Proxy* (za HTTP, HTTPS, SMTP, itd.) se koristi tamo gdje je to potrebno zbog sigurnosti, performansi (npr. keširanje podataka) i/ili zahtjeva za evidentiranjem podataka.

*Proxy* mora biti osposobljei za *dual-stack*.

Ako je konekcija sa Interneta prema nekom lokalnom hostu zabranjena, to mora biti spriječeno i za IPv6, kao i za IPv4.

***Firewall*-i / filteri paketa**

Generalno *firewall*-i i filteri paketa zahtjevaju održavanje dva nezavisna seta pravila za IPv4 i za IPv6 protokol. Ovi skupovi pravila obično nisu sinhronizovani na automatizovan način.

- IPv6 skupovi pravila moraju biti ekvivalentni postojećim IPv4 skupovima pravila.
- IPv6 skupovi pravila moraju osigurati isti nivo sigurnosti kao što osiguravaju postojeći IPv4 skupovi pravila.

No, sve više firewall-a novije generacije primjenjuju pravila ravnopravno za oba IP protokola bez obzira koju vrstu IP adrese koristi uređaj za koji se definišu pravila zaštite.

Samo namjenski tunel ruteri/*gateway*-i mogu postaviti IPv6 tunele prema Internetu.

- Zabranjene tehnike tunelovanja (na primjer 6to4 i Teredo) moraju biti blokirane pomoću rutera.

Ruteri moraju odbaciti IP datagrame sa IPv6 adresama koje su isključivo određene za internu (intranetsku) upotrebu.

Bilo koja željena dostupnost (ili nedostupnost) servera, servisa i klijenata mora biti kontrolisana listama kontrole pristupa (*Access Control Lists* - ACL).

Različita i asimetrična IPv4 i IPv6 rutiranja moraju biti spriječena.

**Sigurnosni mehanizmi kod čvorova**

IPv6 protokoli za tunelovanje i mehanizmi tunelovanja moraju biti deaktivirani na čvorovima, jer predstavljaju sigurnosni rizik.

Na čvorovima treba deaktivirati IPv6 prije početka migracije.

Čvorovi treba da koriste lokalni *firewall* („personalni *firewall*“) koji mora biti u stanju da upravlja IPv6 protokom podataka. Aktuelni operativni sistemi čvorova podržavaju *dual-stack firewall*-ove i treba provjeriti kroz primjere (za skup odabranih sistema i konfiguracija) da li instalirani skup pravila sadrži ekvivalentna pravila zaštite za IPv4 i IPv6.

Čvorovi mogu da koriste i dodatni zaštitni IPS (*Intrusion Prevention System*) sistem za sprečavanje neovlašćenog pristupa i on mora podržavati IPv6.

## 8.4. Upravljanje i nadzor mreže

Serveri i softveri koji se koriste za upravljanje (npr. *Nagios*, *Icinga*, *HP OpenView*) treba da podržavaju i IPv6 protokol.

Interfejs za upravljanje na svim mrežnim komponentama (ruterima, sviječevima i drugim uređajima) treba da bude dostupan i preko IPv6. Oni mogu migrirati na *dual-stack* nakon jezgra mreže i operativnih mreža (npr. DMZ-a i mreže klijenata).

Obratiti pažnju da migraciju servera za upravljanje treba izvršiti prije migracije komponenata kojima on upravlja.

Ako se koristi sistem za upravljanje IP adresama (*IP Address Management System* -IPAM), on mora podržavati IPv4 i IPv6 protokol.

Monitoring sistemi moraju biti provjereni u pogledu njihovih IPv6 mogućnosti, odnosno sve funkcije praćenja (pasivne i aktivne provjere) koje koriste IPv4 treba da podrže i IPv6.

**Simple Network Management Protocol (SNMP)**

SNMP agenti treba da budu dostupni preko IPv6, što zahtijeva sigurnosni tj. enkriptovani SNMP pristup koji koristi SNMPv2c i/ili SNMPv3.

U IPv6 mrežama, SNMP agenti (posebno na sviječevima i ruterima) takođe treba da podržavaju IPv6 specifične MIB-ove (*Management Information Base*) na tim uređajima.

## 8.5.Infrastrukturni servisi

### 8.5.1. E-Mail / SMTP

Da bi infrastruktura *e-mail* servisa migrirala na *dual-stack* mora se provjeriti da li sledeći elementi podržavaju IPv6 protokol:

- softver za *mail* server,
- agent za prenos *mail*-ova (MTA)
- softver za *mail* koji koriste klijenti.

Svi oni moraju podržavati IPv6.

### 8.5.2. Serveri direktorija / LDAP i AD

Serveri direktorija (npr. LDAP (*Lightweight Directory Access Protocol*) server ili *Active Directory*) neke ustanove treba da podržavaju IPv6 protokol, pod uslovom da barem jedan od njihovih klijenata radi u *dual-stack* modu.

### 8.5.3. Sinhronizacija vremena / NTP

Svi lokalni NTP serveri neke ustanove moraju biti dostupni preko IPv4 i IPv6. Vrijeme na NTP serveru može se podešavati korišćenjem tehnika kao što su prijem sa satelita ili radio-kontrolisani satovi (npr. GPS (*Global Positioning System*), DCF77) ili upitom ka spoljnjem NTP serveru. Konfiguracija klijenta je takođe moguća koristeći DHCP.

## 8.6. Detaljne preporuke u obliku kontrolne liste prilikom implementacije

U početku migracija na IPv6 protokol može izgledati jako složeno, što ne smije biti prepreka u procesu realizacije. Veoma važan korak na putu migracije je kreiranje plana, kako bi koristili benefite u vidu obezbijeđenih resursa, bolje komunikacione infrastrukture, efikasne organizacije i upravljanja procesom migracije, a što sve vodi ka održivoj Internet budućnosti. U cilju uspješne implementacije procesa migracije značajnu pomoć mogu pružiti takozvane kontrolne liste. Kontrolne liste sumiraju najvažnije korake koje treba obaviti kako bi pripremili svoju mrežu za migraciju i obavili njenu uspješnu implementaciju. Ona služi i za provjeru kako se ne bi preskočio neki značajan korak potreban za migraciju na IPv6. Za svaki segment migracije potrebno je kreirati zasebnu kontrolnu listu koja će se fokusirati na specifičnosti IPv6, kao i na izabrani metod migracije.

Kao što je već napomenuto, svaka institucija/organizacija koja treba da prođe kroz proces migracije na IPv6 ima svoje specifičnosti, pa se ne mogu napraviti univerzalne kontrolne liste koje će obuhvatiti baš svaki mogući slučaj do kojeg može doći. Ali mogu poslužiti kao vodilja koju treba slijediti. Zato ove kontrolne liste treba shvatiti kao okvirni redoslijed važnih koraka, koje treba modifikovati i dopunjavati saglasno potrebama i specifičnostima konkretne institucije/organizacije.

U daljem tekstu će biti prikazane sljedeće kontrolne liste za IPv6 migraciju:

- **Planiranje migracije** – predstavlja uvod u migraciju, utvrđuje pregled trenutnog stanja, ciljeve migracije i planiranje koraka.
- **Mrežna infrastruktura** - migracija pristupa WAN-u, podmreža i usluga mrežne infrastrukture kao što su DNS i DHCP.
- ***Web* server** - primjer za migraciju *web* servera/portala.

Projekat migracije počinje fazom planiranja u kojoj se mora evidentirati postojeća IT infrastruktura i utvrditi ciljevi migracije. Implementaciju treba započeti sa osnovnom mrežnom infrastrukturom onih djelova mreže koji su predviđeni za migraciju. Potrebno je obezbijediti IPv6 povezanost sa bar jednom WAN mrežom, a nakon toga se može izvršiti migracija servera i klijenata.

Svaka kontrolna lista, shodno iskustvima iz [113], podijeljena je u tri dijela:

- Procjena trenutnog stanja - važne informacije o zatečenom stanju.
- Koraci migracije - detalji o koracima planiranih aktivnosti.
- Validacija - testovi koji se trebaju obaviti za vrijeme i nakon migracije.

### 8.6.1. Planiranje migracije

#### 8.6.1.1. Procjena trenutnog stanja

Definisati i/ili napraviti:

- tim za migraciju koji će učestvovati u projektu (jedan od mogućih pristupa je da svaka organizaciona jedinica delegira predstavnike u ovaj tim);
- rukovodioca projekta i obaveze i odgovornosti svakog člana tima;
- cilj projekta (za koje mreže je planirana migracija);
- strategiju migracije i usaglasiti plan implementacije sa svim članovima tima;
- globalni vremenski okvir projekta u kome će biti definisana prolazna vremena za kritične aktivnosti, kao i najvažniji ciljevi i međukoraci ka tim ciljevima (na primjer *Gantt*-ovim dijagramom);
- vrstu i iznos troškova koje treba očekivati (obuhvatiti sve potencijalne tehničke i poslovne troškove);
- povezane i/ili nadređene institucije koje učestvuju u procesu migracije;
- šemu postojeće IT infrastrukture koja uključuje sve važne elemente;
- spisak usluga i mrežnih aplikacija koje organizaciona jedinica pruža trećim licima;
- spisak usluga i mrežnih aplikacija koje koriste interni korisnici posredstvom Interneta ili mrežne okosnice;
- kritične podatke i servise za koje treba napraviti rezervne kopije (*backup*) prije započinjanja procesa migracije;
- kriterijume uspjeha projekta migracije.

#### 8.6.1.2. Koraci migracije

- redoslijed migracije:
  - WAN/*gateway* ruter
  - mrežna infrastruktura
  - infrastrukturni servisi
  - IP (pod)mreže, ...
- generalne procedure za migraciju (treba razmotriti i mogućnost djelimične migracije);
- tehničke preporuke za migraciju (koje tehnike treba koristiti);
- detaljni projektni plan koji sadrži korake migracionog plana.

#### 8.6.1.3. Validacija

Obzirom da se radi o planiranju, ne može se vršiti stvarna validacija već se radi o provjeri konzistentnosti usvojenog koncepta migracije, prije nego se pristupi implementaciji. U tom smislu potrebno je odgovoriti na sljedeća pitanja:

- Da li su svi ljudi informisani o planu migracije?
- Da li je uspostavljeni vremenski plan realan/ostvarljiv?
- Da li su potrebne nove nabavke (hardver, softver)?
- Da li je osigurana podrška migracije od strane trećih lica (organizacija)?
- Da li su planirani odgovarajući testovi validacije za pokrivene usluge?

### 8.6.2. Mrežna infrastruktura

#### 8.6.2.1. Procjena trenutnog stanja

Potrebno je pribaviti i dokumentovati sljedeće podatke:

- temeljnu analizu infrastrukture u cilju pravljenja detaljnog popisa opreme koju treba migrirati;
- provajder – kontakt informacije;
- IPv4 prefiks;
- svičevi (naziv, proizvođač, model, verzija *firmware*-a, ...);
- ruter(i) (naziv, proizvođač, model, verzija *firmware*-a, ...);
- *firewall* (naziv, proizvođač, model, verzija *firmware*-a, ...);
- *proxy* (naziv, proizvođač, model, verzija *firmware*-a, ...);
- ostale mrežne i sigurnosne komponente;
    - razmotriti potrebu za unapređenjem pojedinih djelova hardvera;
    - razmotriti potrebu za virtuelizacijom pojedinih djelova infrastrukture;
- DNS (naziv, proizvođač, verzija softvera, ...);
- DHCP (naziv, proizvođač, verzija softvera, ...);
- LDAP (naziv, proizvođač, verzija softvera, ...);
- e-*mail* server (naziv, proizvođač, verzija softvera, ...);
- ostali infrastrukturni servisi;

#### 8.6.2.2. Koraci migracije

- dokumentovati dodijeljeni IPv6 prefiks;
  ako pristup Internetu ne podržava *dual-stack* potrebno je:
    - obratiti se nadležnom organu da bi dobili vlastiti IPv6 prefiks;
    - kontaktirati provajdera i utvrditi na koji način je moguće usmjeriti svoj IPv6 prefiks kroz njegovu mrežu;
    - omogućiti IPv6 protokol na svom *gateway* ruteru.
- za svaki uređaj i servis na mrežnoj infrastrukturi utvrditi da li je direktno ili indirektno pod uticajem migracije;
  ako je odgovor pozitivan, potrebno je utvrditi:
    - da li trenutna verzija uređaja/servisa podržava IPv6; ako ne podržava, neophodno je planirati nadogradnju ili zamjenu uređaja/servisa.
    - šta je i kako potrebno konfigurisati na uređaju da bi podržao IPv6;
    - kako podesiti konfiguraciju da bi se omogućila podrška za IPv6 odmah nakon restartovanja uređaja;
- utvrditi redoslijed uspostavljanja IPv6 podrške kod uređaja, IP podmreža i servisa;
- razviti odgovarajući IPv6 adresni koncept;
- prije implementacije u realnom okruženju, testirati korake migracije u laboratorijskom okruženju.

#### 8.6.2.3. Validacija

Validacija infrastrukturnih komponenti i usluga:

- da li WAN pristup (na Internet ili okosnicu mreže) radi preko IPv6?
- da li dodjela IPv6 adresa radi ispravno?

- da li su *gateway* i infrastrukturne usluge dostupne preko IPv6?
- da li su infrastrukturne usluge dostupne prema planu?

### 8.6.3. *Web* server

#### 8.6.3.1. Procjena trenutnog stanja

Dokumentovati sljedeće podatke:

- mrežni IPv4 prefiks i mrežna maska;
- IPv4 *default gateway*;
- naziv podmreže (opciono);
- VLAN *tag* (opciono);
- postojeće ACL;
- operativni sistem (tip, distribucija, kernel, ...);
- IPv4 adresa(e) *web* servera;
- DNS imena *web* servera i adresa(e) nadređenih DNS servera;
- *web* server softver (verzija, konfiguracija);
- adrese sigurnosnih komponenti (*proxy*, *firewall*, ...).

#### 8.6.3.2. Koraci migracije

- *web* server mora da ima omogućen pristup Internetu preko *dual-stack*-a; ako ga nema, prvo treba izvršiti migraciju pristupa WAN-u (Internetu);
- mora postojati adresni koncept – ako nije kreiran mora se prvo on kreirati; dodati nove vrijednosti:
  - IPv6 prefiks za IPv6 mrežu *web* servera;
  - adresa IPv6 *default gateway*-a;
  - način konfiguracije IPv6 adresa (statičke ili dinamičke);
- omogućiti *dual-stack* u okviru operativnog sistema;
- omogućiti i konfigurisati IPv6 na računaru na kome treba pokrenuti *web* server;
- definisati javnu i privatnu IPv6 adresu *web* servera;
- konfigurisati DNS tako da *web* server ima isti *hostname* i za IPv4 i za IPv6;
- konfigurisati IPv6 i *dual-stack* u *web* server aplikaciji;
- podesiti sigurnosne uređaje/aplikacije za IPv6 saobraćaj da se ponašaju analogno IPv4 saobraćaju;

#### 8.6.3.3. Validacija

- nakon podešavanja izvršenih u poglavlju 8.6.3.2 (koraci migracije) restartovati *web* server;
- provjeriti:
  - da li su predviđene IPv4 i IPv6 adrese ispravno podešene;
  - da li je moguće uspostaviti IPv4 i IPv6 konekcije sa drugim hostovima;
  - da li DNS funkcioniše prema očekivanjima;
  - da li se može pristupiti *web* sajtovima;
  - da li ostali programi rade kako treba;
- provjeriti da li se može pristupiti migriranom *web* serveru [116]:
  - iz spoljašnje mreže (sa Interneta) i iz unutrašnje mreže (intranet);
  - korišćenjem IPv4 klijenta, IPv6 klijenta i *dual-stack* klijenta;

- korišćenjem različitih *web* preglednika;
- korišćenjem različitih operativnih sistema;
- za svaki hostovani domen *web* servera;
- za pojedine važnije poddirektorijume *web* stranica;

## 8.7. Podizanje svijesti o potrebi migracije sa IPv4 na IPv6

Svijest o potrebi prelaska na IPv6 protokol, kod svih subjekata uključenih u oblast ICT-a, je od ključnog značaja za efikasno i uspješno sprovođenje i okončanje ovog procesa. Dominantan je utisak da svijest u Crnoj Gori o iscrpljenosti IPv4 adresnog prostora i evidentnom problemu sporog uvođenja IPv6 u mreže i usluge nije na potrebnom nivou. U slučaju migracije sa IPv4 na IPv6, očigledna je tendencija da se proces nepotrebno odlaže uz rizik da do njega dođe tek pošto se dese negativne posljedice. Izuzev sporadičnih prezentacija stručnjaka iz ove oblasti, na naučnim i stručnim skupovima, pitanje podizanja svijesti o potrebi implementacije IPv6 protokola u Crnoj Gori nije tretirano na organizovan način. Stoga se pokazuje neophodnim pokretanje kampanje u cilju podizanja svijesti o mogućnostima koje pruža novi Internet protokol, a samim tim i o potrebi migracije sa IPv4 na IPv6, a koja će biti usmjerena na sve najznačajnije subjekte uključene u ovaj proces: operatore javnih elektronskih komunikacionih mreža i usluga (ISP), poslovne korisnike (kompanije) i javne institucije na lokalnom i državnom nivou, ali i na ukupnu javnost.

Nacionalno regulatorno tijelo za oblast elektronskih komunikacija se može smatrati relevantnim i kvalifikovanim da radi na podizanju svijesti i promociji implementacije IPv6 protokola. Naravno, prije toga, potrebno je identifikovati i druge subjekte, inicijative ili tijela u Crnoj Gori koji mogu dati odgovarajući doprinos.

Akteri koji mogu biti uključeni u kampanju za podizanje svijesti su, pored Agencije za elektronske komunikacije i poštansku djelatnost, Ministarstvo ekonomije, Ministarstvo javne uprave, Privredna komora i Univerzitet Crne Gore.

## 8.8. Podizanje svijesti operatora javnih elektronskih komunikacionih mreža i usluga (ISP)

Kao najveći potrošači IP adresnog prostora, pružaoci usluge pristupa Internetu (IPS) će biti prvi i najviše pogođeni nedostatkom IPv4 adresa. Stoga je za očekivati da oni prvi počnu da se bave pitanjem implementacije IPv6 protokola.

Svaki put kada povežu novog korisnika, operatori moraju da dodijele dinamičku ili statičku IP adresu. Isto važi i za povezivanje poslovnih korisnika ili korisnika na iznajmljenoj pretplatničkoj liniji. Ovi korisnici obično zahtijevaju statičku IPv4 adresu i skup IPv4 adresa za svoje Internet servere i servise. Native IPv6 trenutno nema u ponudi nijedan ISP u Crnoj Gori, čak ni za poslovne korisnike na iznajmljenim linijama. Sa druge strane, za pristup rezidencijalnim korisnicima preko xDSL, FTTH ili kablovske tehnologije, mora se sačekati implementacija IPv6 u CPE (*Customer Premise Equipment*) uređajima. Uvođenjem 5G mobilnih komunikacionih mreža, pogotovo omasovljenjem IoT (*Internet of Things*), i generalno MTC (*Machine Type Communications*) uređaja, dramatično će porasti potreba za novim adresnim resursima, koju IPv4 neće biti u mogućnosti da podrži.

Generalno, operatori javnih elektronskih komunikacionih mreža i usluga su svjesni potencijalog problema, a s obzirom na to da raspolažu osobljem sa ekspertskim znanjima, podizanje svijesti o potrebi prelaska sa IPv4 na IPv6 se može realizovati na brz i jednostavan način organizovanjem okruglih stolova i stručnih skupova.

## 8.9. Podizanje svijesti poslovnih korisnika

Svijest kompanija koje posjeduju informacione sisteme ili pružaju ICT usluge o potrebi prelaska na IPv6 protokol tek treba da dostigne neophodni nivo. U mnogim slučajevima, glavni problem IT osoblja u kompanijama koje se ne bave direktno informacionim tehnologijama, je percepcija o nepostojanju potrebe za implementacijom IPv6 u njihovom poslovnom okruženju, a koja je izazvana nedovoljnim nivoom poznavanja ove oblasti. Štaviše, zbog zaokupljenosti drugim izazovima u poslovanju, u slučaju nepostojanja adekvatnog usmjeravanja i pospješivanja aktivnosti, može se očekivati da će kompanije kasno započeti rješavanje pitanja migracije sa IPv4 na IPv6. Činjenica da većini kompanija neće biti neophodna IPv6 podrška u nekoliko narednih godina, takođe nije od pomoći u iniciranju istih da započnu aktivnosti ka implementaciji IPv6 u svom okruženju.

Kompanije koje nisu pružaoci Internet usluga će najvjerovatnije proći tri faze prilagođavanja i migracije na novi IP protokol.

1. Kada Internet provajderi počnu da dodjeljuju IPv6 adrese rezidencijalnim korisnicima, većina sadržaja će i dalje biti dostupna preko IPv4 protokola. Pristup IPv6 klijenta IPv4 sadržaju će postati problem za pružaoce Internet usluga, koji će morati da ovaj problem rješavaju jednim od tranzitnih mehanizama.

Tokom ove faze, većina kompanija i dalje neće koristiti IPv6 protokola, jer one prvenstveno svojim klijentima pružaju tradicionalne *web* servise preko HTTP ili HTTPS protokola, koji rade bez problema sa svim tranzitnim mehanizmima. Kompanije koje pružaju napredne usluge, kao što je npr. usluga na zahtjev „klikni za razgovor“ (*click-to-talk*), mogu biti suočene sa manjim problemima.

Treba napomenuti da će se poslovni korisnici, koji svojim klijentima pružaju siguran pristup Internetu preko privatne mreže putem IPsec tehnologije, vjerovatno suočiti sa problemom migracije na IPv6 prije drugih, zato što pristup IPv6 klijenta IPsec koncentratoru koji podržava samo IPv4, predstavlja značajan izazov. Tamo gdje se koristi TLS/SSL tehnologija umjesto IPsec-a, takvi problemi se neće pojaviti. TLS tehnologija polako zamjenjuje IPsec, jer je jednostavnije proći odgovarajući *firewall*.

2. Kada većina interesantnijih sadržaja postane dostupna preko IPv6, provajderi Internet usluga će prestati da pružaju pristup IPv4 sadržaju klijentima koji imaju samo IPv6 adrese. Do tada, kompanije koje već ne pružaju svoj sadržaj u oba okruženja (IPv6 i IPv4) će imati ozbiljne poteškoće. Mora se voditi računa da je konkurencija nemilosrdna, a da su posjetioci *web* stranica izuzetno nestrpljivi. Ako nisu u mogućnosti da dobiju sadržaj gdje očekuju da će ga pronaći, oni će se okrenuti alternativnom sadržaju i novom pružaocu usluga, za što će im biti potrebno samo nekoliko koraka.

3. U završnoj fazi, neki sadržaji na Internetu biće dostupni samo preko IPv6 protokola. Do tada, poslovni korisnici koji tek treba da implementiraju IPv6 protokol u svoje poslovno okruženje naići će na ozbiljne poteškoće. Neki od njih će vjerovatno pokušati da izbjegnu promjene korišćenjem dodatnih mehanizama kao što je upotreba posrednih HTTP servera (koji IPv4 klijentima pružaju pristup IPv6 sadržaju preko HTTP ili HTTPS protokola). Zato što se može očekivati da će u to vrijeme (takođe zbog implementacije IPv6 protokola i otkazivanja prevođenja adresa) sve više *web* servisa koristiti direktnu komunikaciju između klijenata, upotreba posrednih HTTP servera će takođe značajno ograničiti mogućnosti komunikacije takvih kompanija i smanjiti njihovu konkurentnost.

Proces migracije sa IPv4 na IPv6 protokol prati i problem nepostojanja striktno definisanog datuma okončanja migracije i prestanka upotrebe stare verzije protokola. Primjena novih protokola zbog hipotetičkog, potencijalnog pada buduće konkurentnosti i, iznad svega, zbog troškova vezanih za implementaciju (koji ni na koji način nisu hipotetički) će od strane menadžmenta mnogih kompanija biti označena kao nepotrebna.

Takođe, važno je napomenuti da većina kompanija već ima mrežnu infrastrukturu koja je bar djelimično spremna za implementaciju IPv6, uz neophodnost ispravnog podešavanja. Većina radnih stanica podržava IPv6 protokol (barem one sa Windows XP, Vista, Windows 7, Windows 8, Windows 10, MAC OS X ili Linux operativnim sistemima), ali mnoge aplikacije nikada neće biti dovoljno zrele za prelazak na IPv6 okruženje - između ostalog i zato što još uvijek postoje slabo dokumentovane aplikacije, zastarjelo razvojno okruženje i izgubljeni izvorni kod.

Dakle, kada su u pitanju poslovni korisnici, neophodno je početi sa opsežnom kampanjom promovisanja IPv6 protokola (slično kampanji prelaska na digitalnu televiziju) koja će biti usmjerena na rezidencijalne korisnike, kao i na IT inženjere i, prije svega, na menadžment u kompanijama. Profesionalna udruženja menadžera treba da igraju ključnu ulogu, jer imaju sposobnost da dobro brinu o svojim interesima. Privredna komora, čija je uloga da osigura konkurentnost svojih članova, takođe treba da bude uključena.

Pored jačanja interesovanja za IPv6 protokol i obezbjeđivanja početnog shvatanja da će zanemarivanje problema prelaska na IPv6 protokol u budućnosti dovesti do gubitka konkurentnosti kompanije, moraju se omogućiti i lako dostupni obrazovni program i materijali, čiji cilj bi bio da zainteresovanim subjektima pruže barem osnovne informacije o IPv6 protokolu.

Finansijska konstrukcija za pokrivanje troškova edukacije može biti zaokružena na više načina. Vlada može imati interes da opredijeli odgovarajuća sredstva za ovu svrhu, pogotovo u segmentu obrazovanja građana. Sa druge strane, podršku u finansiranju promotivnih IPv6 predavanja mogu da pruže i kompanije iz industrije, koje bi koristile ove događaje u svrhu sopstvenog marketinga.

Ciljni polaznici ovih predavanja treba da uključe sistemske i mrežne administratore u kompanijama, šefove IT odjeljenja i druge odgovorne osobe koje donose odluke o tehnološkim smjernicama i investicijama u preduzećima. Obuke mogu biti realizovane od strane različitih institucija (na primjer Univerzitet Crne Gore) i drugih subjekata koji

okupljaju kvalifikovane predavače. Pri tome, kad je generalno edukacija i izgradnja kapaciteta u pitanju, fokus treba da bude na: karakteristikama IPv6 protokola; korišćenju odgovarajuće servisne arhitekture uključujući standardizovane kontrolne i signalizacione mehanizme; implementaciji IPv6 u IPv4 okruženje; upravljanju performansama; unaprijeđenju regulatornih znanja… Time će profesionalcima u kompanijama, javnim institucijama i regulatoru, biti omogućeno da savladaju napredne vještine neophodne za uspješnu IPv6 migraciju.

Na navedeni način, može se podići osnovna svijest javnosti o važnosti i inovacijama koje sa sobom donosi IPv6 protokol u relativno kratkom vremenu.

## 8.10. Podizanje svijesti javnih institucija na lokalnom i državnom nivou

Svijest o potrebi implementacije IPv6 protokola u sopstvenim informacionim sistemima treba razviti i u institucijama javne uprave na lokalnom i državnom nivou. To se može uraditi kroz organizovanje radionica sa osobama odgovornim za projekte i mreže koje će biti podvrgnute migraciji ka IPv6. U tu svrhu je potrebno pripremiti i posebne edukativne kurseve koji će staviti veći naglasak na zahtjeve koji su neophodni za obezbjeđenje sigurnosti i kontrole mreža i usluga javnih institucija.

## 8.11. Predlozi za podizanje svijesti u budućnosti

Pristup sličan prethodno elaboriranom bi se mogao primijeniti i u budućnosti, ali na višem nivou. Menadžment koji donosi odluke o strateškim potezima i investicijama, u većini slučajeva, pozitivno reaguje samo kad su u pitanju događaji koji se iniciraju sa državnog nivoa. Stoga, predlog za podizanje svijesti u ovoj oblasti je da Ministarstvo ekonomije organizuje okrugli sto na visokom nivou i pozove predstavnike najvećih operatora elektronskih komunikacionih mreža i usluga, provajdera sadržaja, banaka, osiguravajućih društava, Ministarstva javne uprave, Fonda zdravstvenog osiguranja, Privredne komore, renomiranih IT kompanija, Univerziteta Crne Gore i drugih zainteresovanih institucija i kompanija na dogovor o podjeli zaduženja i vremenskom okviru za sprovođenje aktivnosti po pitanju podizanja svijesti o značaju koordinirane i sinhronizovane migracije sa IPv4 na IPv6 u Crnoj Gori.

# 9. Detaljan plan implementacije IPv6 u Akademskoj mreži UCG

Obzirom da Akademska mreža UCG (AMUCG) sa aspekta arhitekture, složenosti sistema, servisa koji se pružaju i infrastrukture koju obuhvata, predstavlja primjer savremenog informacinog sistema, na njegovom primjeru se može realizovati pilot projekat implementacije IPv6 u jednoj javnoj ustanovi, koji bi poslužio kao model, kako za ostale javne ustanove u Crnoj Gori, tako i za veliki broj kompanija koje planiraju migraciju sa IPv4 na IPv6.

Shodno činjenicama i preporukama iznesenim u ovom dokumentu, a posebno poglavljima 7 i 8, ovdje će biti dat predlog detaljnog plana implementacije IPv6 protokola u Akademskoj mreži Univerziteta Crne Gore (AMUCG). Na osnovu zahtjeva Projektnog tima, Centar Informacionog Sistema UCG (CIS UCG) je prihvatio da AMUCG bude predmet ovog dokumenta i ustupio potrebne podatke za kreiranje predmetnog Plana. Dodatno, CIS UCG je dao i početne ciljeve, kao i nivo detalja do kojih će ići ovaj Plan. Naime, shodno svojoj poslovnoj politici i planovima razvoja, CIS UCG je izabrao infrastrukturu koju je nominovao za prvu fazu implementacije IPv6, što je u potpunosti usaglašeno i sa preporukama pripremne faze izrade plana migracije na novi IP protokol. Ovim je Projektni tim dobio relevantne ulazne podatke za planiranje i oročio detaljni plan na prvu fazu implementacije i time ostavio prostora instituciji (CIS UCG) da shodno iskustvu u ovoj fazi, a imajući u vidu date preporuke i aktuelne tehničke trendove i stanje na tržištu, nastavi implementaciju novog IP protokola.

Planiranju je pristupljeno u skladu sa preporukama, prije svega u suštinskom ali i formalnom smislu. Da bi izbjegli nepotrebna ponavljanja, detaljni plan ne sadrži već izrečene generalne preporuke, pa se isti ne može koristiti kao uputstvo za realizaciju implementacije. Poglavlja 7 i 8 treba koristiti za pripremu, planiranje i realizaciju implementacije novog IP protokola, a ovo poglavlje je dato za konkretnu instituciju koja, zbog svojih specifičnosti, ne može biti sveobuhvatni primjer. U pitanju je polazna osnova za realizaciju projekta implementacije IPv6 u AMUCG, a sa njim bi trebalo započeti intenzivniji proces migracije na novi IP protokol u Crnoj Gori.

Pripremna faza migracije sadrži definisanje ciljeva, infrastrukturnih resursa i postojećih ugovora. Obzirom da je CIS UCG već imao definisan cilj i potrebu prelaska na IPv6 (odavno iznajmljene adrese i čak globalno vidljive od 2013. godine), kao i jasno identifikovane infrastrukturne resurse i vrstu migracije, to je pripremna faza bila većinom realizovana. Kako AMUCG ima jasno definisan SLA sa Pan-evropskom akademskom mrežom GEANT, koja podržava i podstiče prelazak na novi IP protokol, kao pružaocem Internet usluga i konekcije sa ostalim autonomnim sistemima (AS), time je ovaj neophodni preduslov migracije obezbijeđen.

CIS UCG je, svjestan izazova implementacije IPv6 protokola, definisao infrastrukturne resurse za prvu fazu implementacije, a neke kritične servise ostavio za narednu fazu u kojoj će imati više iskustva i mogućnosti za njihovu migraciju. Obzirom na faznu realizaciju i

koegzistenciju dva IP protokola, ovaj agilni pristup je preporučen i ne ugrožava funkcionalnost sistema i sigurnost servisa i podataka. Ono što u pripremnoj fazi nije definisano je vremenski okvir, jer korisnik (CIS UCG) nije imao potrebu za ovim ograničenjem, ali je Projektni tim oročio prvu fazu implementacije na 6 do 10 mjeseci od trenutka izrade projekta implementacije.

Konačno, shodno analizi scenarija, za AMUCG je preporučena parcijalna migracija po scenariju „spolja ka unutra“ uz korišćenje *dual-stack* tehnike i primjenu navedenih preporuka.

U ovom poglavlju je, nakon analize postojećeg stanja AMUCG, dat detaljan plan prve faze implementacije IPv6 protokola u AMUCG.

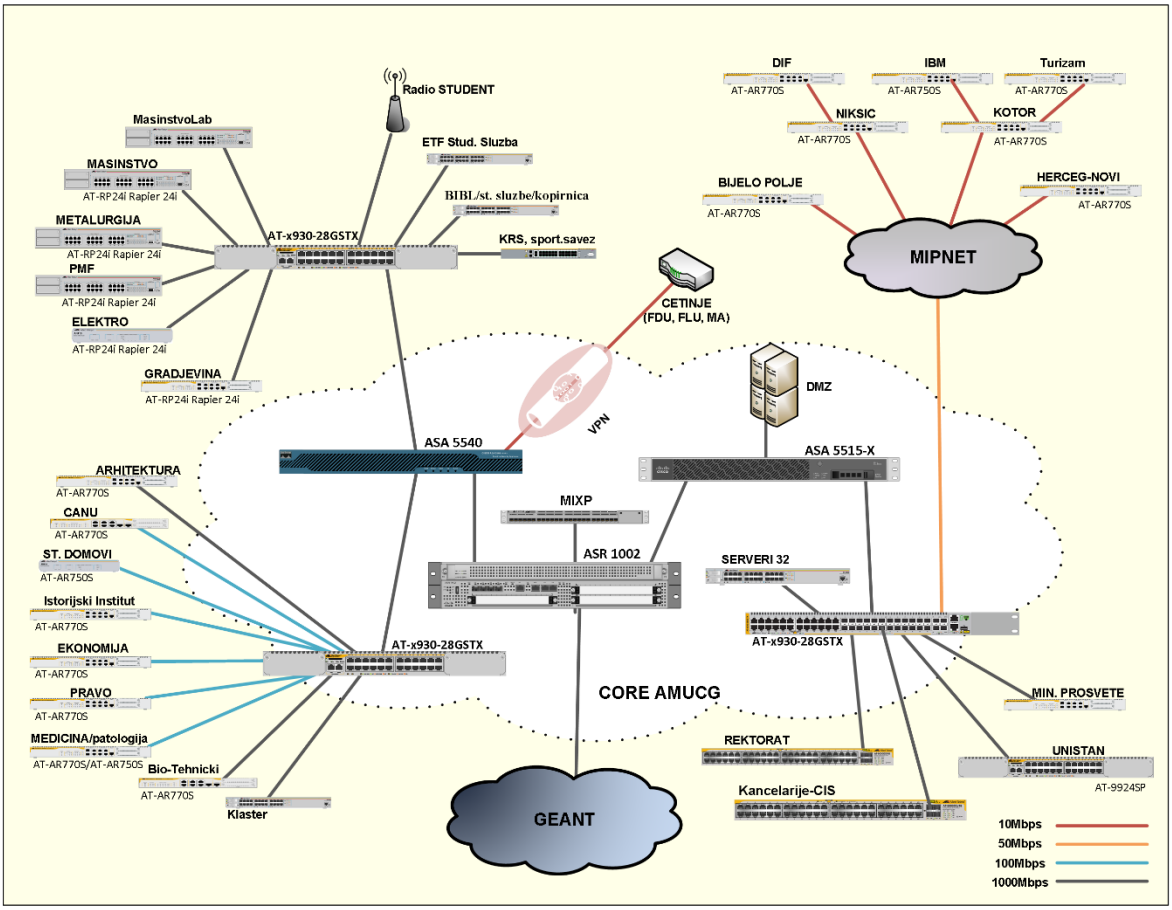
## 9.1. Analiza postojećeg stanja Akademske mreže Univerziteta Crne Gore (AMUCG)

Akademska mreža UCG (AMUCG) pruža privatne i javne servise za preko 20.000 korisnika. Na mrežu je stalno povezano preko 3000 računara koji se koriste u nastavne, naučne i administrativne svrhe. Mreža je rasprostranjena u 6 gradova (Podgorica, Nikšić, Cetinje, Kotor, Herceg Novi i Bijelo Polje), povezuje 26 lokacija i ostvarena je u topologiji višestruke zvijezde primjenom optičke infrastrukture. Pored svih univerzitetskih jedinica, na mrežu su povezani i Crnogorska akademija nauka (CANU), Ministarstvo prosvjete i studentski domovi u Podgorici i Nikšiću.

UCG nema svoju optičku infrastrukturu, osim u okviru glavnog univerzitetskog kampusa, koji obuhvata zgradu Rektorata, zgradu tehničkih fakulteta i zgradu Unistana. Zgrade tehničkih fakulteta i Unistana su povezane sa okosnicom mreže, koji se nalazi u zgradi Rektorata u CIS-ovom *data* centru, linkovima od 1Gb/s. Ostale lokacije na okosnici mreže su povezane preko MIPNet-a (*Montenegrin IP Network*) Crnogorskog telekoma, linkovima različitog kapaciteta prikazanim na slici 29.

Lokacije na Cetinju povezane su na AMUCG putem VPN-a, jer nisu direktno povezane na AMUCG preko iznajmljenih linkova, već koriste komercijalne ADSL konekcije Crnogorskog telekoma. U Kotoru su na Pomorski fakultet povezani Institut za biologiju mora i Fakultet za turizam i hotelijerstvo, linkovima Crnogorskog telekoma kapaciteta 10Mb/s. U Nikšiću je Fakultet za sport i fizičko vaspitanje povezan na isti način, linkovima Crnogorskog telekoma, kapaciteta 10Mb/s na Filozofski fakultet. Na slici 29 je prikazana topologija AMUCG na kojoj je jasno prikazana okosnica (*core*) AMUCG (3 agregaciona L3 sviča, 2 *firewall*-a, granični ruter, DMZ zona u kojoj se nalazi farma servera i pristupni linkovi), kapaciteti linkova i pristupna oprema jedinica UCG i drugih institucija povezanih na predmetnu mrežu.

U pogledu protokola rutiranja u AMUCG se koristi BGP za rutiranje saobraćaja ka GEANT-u, glavnom Internet provajderu AMUCG-a. Interno rutiranje se odvija samo preko statičkih ruta i ne koriste se protokoli rutiranja.




Slika 29. Topologija AMUCG

U tabeli 9 je dat spisak mrežne opreme u okosnici mreže AMUCG, opreme koja agregira saobraćaj od članica AMUCG i opreme koja povezuje AMUCG sa Internetom ili drugim AS. Dati su nazivi mrežnih uređaja, njihov broj, lokacija i podaci o kompatibilnosti sa novim IPv6 protokolom. Na slici 29 je dat prikaz topologije AMUCG i raspored uređaja iz tabele 9 u okviru predmetne mreže. Adresni prostor (IPv4), koji nije prikazan iz sigurnosnih razloga, bio je poznat Projektnom timu.

CIS korisnicima AMUCG nudi razne javne i privatne servise. Servisi koji su dostupni svim korisnicima AMUCG, i koje CIS UCG nominuje za prvu fazu implementacije IPv6 protokola su:

- *web* hosting,
- DNS (ac.me domen),
- MAIL hosting (ucg.ac.me domen),
- *E-learning* (Moodle LMS),
- *Educational Roaming* (*eduroam* – GEANT servis),
- Phaidra – repozitorijum,
- *Adobe connect* (*web* konferencijski sistem).

*Tabela 9. Spisak mrežne opreme CIS UCG do nivoa LAN mreža fakulteta*

| R.br. | UCG jedinica | Postojeći mrežni uređaj | Broj uređaja | IPv6 kompa-tibilan |
|---|---|---|---|---|
| 1. | Centar informacionog sistema (*core* mreže) | Allied Telesis AT-x930-28GSTX | 3 | DA |
| 2. | | Cisco ASA5540 - *firewall* | 1 | DA |
| 3. | | Cisco ASA5515-x - *firewall* | 1 | DA |
| 4. | | Cisco ASR1002 | 1 | DA |
| 5. | Arhitektonski fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 6. | Građevinski fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 7. | Metalurško-tehnološki fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 8. | Pravni fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 9. | CANU | Allied Telesis AT-AR770S | 1 | NE |
| 10. | Medicinski fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 11. | Filozofski fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 12. | Pomorski fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 13. | Biotehnički fakultet | Allied Telesis AT-AR770S | 1 | NE |
| 14. | Fakultet za fizioterapiju Igalo | Allied Telesis AT-AR770S | 1 | NE |
| 15. | Istorijski institut | Allied Telesis AT-AR770S | 1 | NE |
| 16. | Fakultet za sport i fizičko vaspitanje | Allied Telesis AT-AR770S | 1 | NE |
| 17. | Fakultet za turizam i hotelijerstvo | Allied Telesis AT-AR770S | 1 | NE |
| 18. | Elektrotehnički fakultet | Allied Telesis AT-RP24i Rapier 24i | 1 | NE |
| 19. | Prirodno-matematički fakultet | Allied Telesis AT-RP24i Rapier 24i | 1 | NE |
| 20. | Mašinski fakultet | Allied Telesis AT-RP24i Rapier 24i | 1 | NE |
| 21. | Ekonomski fakultet | Allied Telesis AT-9924SP | 1 | NE |
| 22. | Studentski domovi | Allied Telesis AT-AR750S | 1 | NE |
| 23. | Ekonomski fakultet - Bijelo Polje | Allied Telesis AT-AR750S | 1 | NE |
| 24. | Institut za biologiju mora | Allied Telesis AT-AR750S | 1 | NE |

## 9.2. Plan IPv6 adresnog prostora Univerziteta Crne Gore

UCG je 2013. godine, od nadležnog RIR-a (*Regional Internet Registry*), obezbijedio dovoljan blok IPv6 adresa za potrebe AMUCG. Jedan blok je globalno vidljiv, a drugi (namijenjen za MIXP (*Montenegro Internet eXchange Point*)) je još globalno nevidljiv.

1. **AS40981 UNIVCG** (vidljiv od 14.02.2013. godine,16:00:00 UTC)

- Inet6Num: **2a02:4280::/32**
- NetName: **ME-MREN-20110711**

- Org: **ORG-UoM41-RIPE**
- Address> **2a02:4280::0**
- Address Range Start> **2a02:4280::1**
- Address Range End> **2a02:4280:ffff:ffff:ffff:ffff:ffff:ffff**
- Mask Bits> **32**
- Usable Addresses> **$2^{96}$=79 228 162 514 264 337 593 543 950 336**

2. **AS40981 UNIVCG** (nije globalno vidljiv)

- Inet6Num: **2001:7f8:22::/48**
- NetName: **ME-MREN-20150526**
- Org: **ORG-UoM41-RIPE**
- Address> **2001:7f8:2200::0**
- Address Range Start> **2001:7f8:2200::1**
- Address Range End> **2001:7f8::22ff:ffff:ffff:ffff:ffff:ffff**
- Mask Bits> **48**
- Usable Addresses> **$2^{80}$=1 208 925 819 614 629 174 706 176**

Sa dobijenim vidljivim blokom potrebno je napraviti jedinstveni IPv6 adresni plan za UCG.

Shodno preporukama, nameću se neki generalni zaključci za ovu mrežu:

- preferirati da adresiranje u podmrežama ide sa prefiksom /64;
- adresiranje rutera, svičeva, *firewall*-a i servera treba uraditi po sledećem redoslijedu:
    - ručna konfiguracija,
    - SLAAC, pa
    - *stateless* ili *statefull* DHCPv6.

Priprema konkretnog adresnog plana zavisi od strukture i veličine mreže, uz obaveznu analizu moguće alternative. Jedan konkretni predlog adresnog IPv6 plana, u skladu sa preporukama, je da se prilikom migracije izvrši adresiranje mreže na 3 nivoa (tabela 10):

1. podmreže /48 dodijeliti institucijama i univerzitetskim jedinicama (/32→/48),
2. pojedinačne /48 podmreže na nivou jedinice/institicije podijeliti u više /64 podmreža (/48→/64),
3. dodijeliti korisničke IPv6 adrese čvorovima unutar dodijeljenih /64 mreža (/64→/128).

*Tabela 10. Predlog šeme generalnog adresnog IPv6 plana*

| IPv6 blok | I nivo | II nivo | III nivo |
|---|---|---|---|
| 2a02:4280::/32 | 2a02:4280:0100::/48<br>2a02:4280:0200::/48<br>2a02:4280:0300::/48<br>... | 2a02:4280:0100:LTBB::/64 po **L**okaciji<br>2a02:4280:0200:TLBB::/64 po **T**ipu<br>2a02:4280:0300:0012:/64 po VLAN Id-u ... | Ručna konfiguracija<br>SLAAC<br>DHCPv6 |

Predlog je da se IPv6 blokovi dodjeljuju na osnovu lokacije ili tipa (semantičke identične podmreže), a može i proizvoljno.

Ako se ova generalna šema adresnog plana primjeni na trenutni adresni i organizacioni plan UCG, jedan od mogućih predloga se nameće kao logičan.

**Adresiranje podmreža AMUCG I nivoa (/32→/48)**

- Centar informacionog sistema 2a02:4280:0100::/48
- Elektrotehnički fakultet 2a02:4280:0200::/48
- Prirodno-matematički fakultet 2a02:4280:0300::/48
- Mašinski fakultet 2a02:4280:0400::/48
- Arhitektonski fakultet 2a02:4280:0500::/48
- Građevinski fakultet 2a02:4280:0600::/48
- Metalurško-tehnološki fakultet 2a02:4280:0700::/48
- Pravni fakultet 2a02:4280:0800::/48
- Ekonomski fakultet 2a02:4280:0900::/48
- Medicinski fakultet 2a02:4280:0A00::/48
- Filozofski fakultet 2a02:4280:0B00::/48
- Pomorski fakultet 2a02:4280:0C00::/48
- Biotehnički fakultet 2a02:4280:0D00::/48
- Fakulteti (manje univ. jedinice) 2a02:4280:0E00::/48
  - za sport i fizičko vaspitanje
  - za turizam i hotelijerstvo
  - za fizioterapiju - Igalo
- Instituti 2a02:4280:0F00::/48
  - Istorijski
  - Za biologiju mora
- ...

**Adresiranje podmreža II nivoa na osnovu lokacije ili tipa podmreže (/48→/64)**

Hijerarhijska podjela na osnovu lokacije ili tipa mreže zavisi prvenstveno od strukture i veličine postojeće podmreže.

1. Adresiranje na II nivou na osnovu lokacije je pogodno za agregaciju ruta i optimizovanje tabela rutiranja. Na primjer: 2a02:4280:0100:l l l l  t t t t bbbb bbbbb:/64.
2. Adresiranje na II nivou na osnovu tipa podmreže je pogodno za efikasnije filtriranje saobraćaja, odnosno primjenu sigurnosnih pravila. Na primjer: 2a02:4280:0100:t t t t l l l l  bbbb bbbb:/64,

gdje su:

- t t t t - skup bitova dodijeljen tipu mreže,
- l l l l  - skup bitova dodijeljen lokaciji mreže i
- bbbb bbbb – skup bitova dodijeljen adresi podmreže.

*Tabela 11. Primjer adresiranja na II nivou po tipu podmreže*

| ID | Tip mreže | Lokacija | Mreža |
|---|---|---|---|
| **0** | Osnovna mrežna infrastruktura | ruteri, svičevi, *firewall*-i, *access point*, ... | 2a02:4280:0100:0000 0001 0000 0001 /64 |
| **1** | Serverska infrastruktura | DMZ | 2a02:4280:0100:0001 0001 0000 0001 /64 |
| **2** | Administrativno osoblje | Dekanat | 2a02:4280:0100:0010 0001 0000 0001 /64 |
| **3** | Rezervisano | ... | ... |
| **4** | Studijski programi i laboratorije | stud.prog.1, stud.prog.2, ..., lab1, lab2,... | 2a02:4280:0100:0100 0001 0000 0001 /64<br>2a02:4280:0100:0100 0010 0000 0001 /64<br>... |
| **5** | Studenti | učionice, WiFi, ... | 2a02:4280:0100:0101 0001 0000 0001 /64<br><br>studenski WiFi u zgradi:<br>2a02:4280:0100:0101 0111 0000 0001 /64 |
| **6** | Gosti | WiFi | 2a02:4280:0100:1111 1111 0000 0001 /64 |
| ... | ... | ... | |
| **2a02:4280:0100: L T B B ::/64** | | | |

## 9.3. Migracija bazičnih infrastrukturnih komponenti u I fazi

Shodno preporukama, potrebno je dokumentovati postojeće stanje i mogućnost podrške IPv6 protokolu na svim OSI nivoima i identifikovati sve uređaje i njihovu kompatibilnost sa IPv6 i sposobnost da rade u *dual-stack* okruženju. Za potrebe prve faze posebno treba obratiti pažnju na migraciju sledećih infrastrukturnih komponenti:

- mrežnih uređaja iz tabele 9,
- DNS servisa,
- DHCP servisa,
- sistema za upravljanje i nadzor (SSH, SNMP, NETFLOW i *Backup*/*Restore*),
- izabranih korisničkih servisa (*web*, *e-mail*, *Adobe connect*, *Moodle*, *Eduroam* i *Phaidra*).

Nakon usvajanja adresnog plana, proces implementacije bi trebao da teče prema sledećem redoslijedu:

- trening, obuka i osposobljavanje osoblja za rad i podršku novoj mreži,
- priprema fizičkih i virtuelnih servera za IPv6 (*dual-stack*),
    - *backup* servera sa mogućnošću vraćanja na ranije stanje (*rollback*),
    - adresiranje,
- priprema servisa i aplikacija za IPv6 (*dual-stack*),

    - planirati vrijeme nedostupnosti servisa (*downtime*),
- uspostavljenje IPv6 rutiranja eksterno (BGP),
    - uspostaviti BGP rute prema GEANT-u i MIXP-u tako da budu u *dual-stack*-u i da rutiranje radi na IPv4 i IPv6,
- uspostavljanje IPv6 rutiranja interno,
    - dio po dio okosnice mreže migrirati na *dual-stack*,
    - ostatak mreže migrirati na *dual-stack* po djelovima saglasno potrebama i mogućim kapitalnim troškovima,
- migracija DNS i DHCP servisa,
- prilagođavanje postojećih servisa i aplikacija za IPv6 (*dual-stack*),
    - *backup/restore* proces (fajlovi, virtuelne mašine, itd.),
- zamjena opreme i servisa koja se ne uklapa u *dual-stack* plan,
    - hostove koji su nekompatibilni sa IPv6 mijenjati po potrebi i shodno planu inoviranja i sa novijim, IPv6 kompatibilnim verzijama,
    - aplikacije sukcesivno prilagođavati, a nove treba obavezno da budu kompatibilne sa *dual-stack*-om,
- uspostavljanje nadzora i upravljanja mrežom preko IPv6.

Da bi se izbjegli mogući problemi pri migraciji, svaku navedenu stavku treba detaljno dokumentovati (pažljiva procjena trenutnog stanja i plan migracije svakog segmenta), a svaki korak migracije treba validirati u toku i/ili nakon njegove implementacije. Detalji su dati u poglavlju 8.6. Dobar plan implementacije je garancija uspjeha, ali ipak se mora pripremiti i plan oporavka i vraćanja na ranije stanje ako nešto nakon validacije ne funkcioniše kako je planirano. Svakako da se funkcionisanje sistema i potrebe korisnika ni u jednom trenutku ne smiju dovesti u pitanje.

### 9.3.1. Definisanje protokola rutiranja

Novi protokoli rutiranja (ili novije verzije postojećih protokola rutiranja) moraju biti prilagođeni za IPv6.

Obzirom da AMUCG koristi BGP protokol kao eksterni protokol rutiranja, preporučuje se nastavak korišćenja istog uz implementaciju sigurnosnih mehanizama IPsec-a, GTSM (*Generalized TTL Security Mechanism*) i MD5 (*Message Digest 5*) algoritma.

Kako AMUCG trenutno koristi statičko rutiranje umjesto internih protokola rutiranja, isto može zadržati ili preći na neki od internih protokola rutiranja koji podržavaju IPv6: RIPng (*Routing Information Protocol next generation*), OSPFv3 (*Open Shortest Path First version 3*) ili EIGRP (*Enhanced Interior Gateway Routing Protocol*). U slučaju izbora nekog od prva dva, treba koristiti i IPsec za obezbjeđenje sigurnosti razmjene podataka.

### 9.3.2. Definisanje protokola za monitoring i upravljanje mreže

AMUCG posjeduje više sistema za monitoring mreže, od *Cacti*-a, preko *Nagiosa*-a do *NetFlow* analizatora. *Cacti* je poznati *open source web* alat za monitoring mreže. *Nagios* je takođe *open-source* alat za nadgledanje mreže i servisa, obuhvatniji od *Cacti*-a. *NetFlow* je CISCO alat za analizu mrežnog saobraćaja i stanja servisa.

Sistemi za monitoring generišu velike količine podataka, a ovi podaci se eksportuju u redovnim vremenskim intervalima radi daljeg čuvanja i analize. U *dual-stack* okruženju uređaji za monitoring treba da prenose podatke preko IPv4 ili IPv6. Zapisi podataka koji predstavljaju monitoring informacije obično sadrže i informacije o IP adresi. To znači da baze podataka u *dual-stack* okruženju moraju biti u stanju da čuvaju i IPv6 i IPv4 adrese.

Obzirom da AMUCG koristi pomenuta 3 alata koji podržavaju IPv6, potrebno je provjeriti da li su instalirani potrebni *plug-in*-ovi za podršku IPv6, i ako nijesu instalirati ih. Nakon toga konfigurisati alate i unijeti IPv6 adrese resursa koji se nadgledaju.

Za upravljanje se koristi SNMP protokol (*Simple Network Management Protocol*) [117].U *dual-stack* okruženju, na upravljivim uređajima, SNMP agent treba da podržava i IPv6 i IPv4 protokol. Svakako treba provjeriti da li ti uređaji mogu pružiti putem SNMP-a informacije specifične za IPv6. Zavisno od uređaja koji se koriste, potrebno je provjeriti koji su (standardni ili specifični za proizvođača) IPv6 MIB-ovi dostupni.

## 9.4. Migracija servera i servisa

Kao što je već navedeno, CIS UCG nudi korisnicima AMUCG čitav niz raznorodnih javnih i privatnih servisa. CIS UCG je identifikovao 6 servisa koje je nominovao kao neophodne za tranziciju na novi IP protolol u prvoj fazi. Pošto su servisi *web* hosting, *E-learning* (*Moodle* LMS), *Phaidra* repozitorijum i *Adobe connect* (*web* konferencijki sistem) *web* orijentisani servisi, preporuke date za migraciju *web* servera na *dual-stack* odnosiće se i važiće za sve ove servise, odnosno servere na kojima su podignuti ovi servisi. Što se tiče servisa *Educational Roaming* (*eduroam*), on predstavlja specifični servis razvijen od strane GEANT-a i njegova migracija na *dual-stack* mora da se odradi u saradnji sa administratorima GEANT mreže. Shodno navedenom, u daljem tekstu će biti date konkretne preporuke za migraciju na *dual-stack* sledećih servera:

1. DNS,
2. DHCP,
3. *web* server i
4. *e-mail* server.

Prije početka migracije servera potrebno je napraviti dokumentaciju trenutne konfiguracije servera. Moraju biti tretirani parametri specifični za mrežu (mrežna maska i prefiks, rute, DNS unosi) i sigurnosne komponente između servera i njegovog *gateway* rutera. Pored toga, moraju se dokumentovati parametri specifični za podešavanje hostova kao što su: operativni sistem, IP adresa(e) i detalji podešavanja same aplikacije servera.

Prilikom migracije svakog servera preporučuje se, shodno poglavlju 8.6, da se izvrše sledeći koraci:

- procjena trenutne situacije,
- planiranje tehničkih koraka migracije i njihovo izvršavanje i
- validacija rezultata.

### 9.4.1. DNS server

Da bi se pripremio DNS server za migraciju na *dual-stack* potrebno je provjeriti:

- da li postojeći operativni sistem (distribucija, verzija i kernel) podržava IPv6; ako je potrebno izvršiti nadogradnju operativnog sistema u toku migracije;
- konfigurisati aplikaciju DNS servera za IPv6 protokol;
- ako neki od DNS servera radi kao virtuelni sistem, treba provjeriti da li VMware podržava IPv6.

Nakon provjere potrebno je konfigurisati DNS server tako da:

- mora biti u stanju da upravlja AAAA zapisima;
- treba da prihvati i odgovori na upite i preko IPv4 i preko IPv6 protokola;
- hostovi koji već imaju A zapis u DNS-u moraju takođe dobiti AAAA zapis;
- *dual-stack* hostovi navedeni u DNS-u trebaju imati svoje IPv4 i IPv6 adrese povezane s istim imenom hosta;
- ne odgovara bilo kojim AAAA zapisom na upite klijenata iz podmreže za koju se zna da podržava samo IPv4 protokol;
- podržava ispravnu IP povratnu pretragu (*reverse lookup*) za IPv4 kao i za IPv6 protokol.

Administrator treba da odredi pravila kojima se definiše redoslijed isporuke IPv4 i IPv6 adresa od strane DNS servera. Nakon završetka migracije potrebno je uspješno proći validaciju shodno preporukama iz 8.2.3.

### 9.4.2. DHCP server

Prije migracije, svi postojeći DHCP serveri moraju biti dokumentovani. Ovo se odnosi na IP adrese samih servera i parametre koji se šalju klijentima od strane DHCP servera. Prije početka migracije DHCP servera mora se usvojiti IPv6 adresni plan (predloženi ili modifikovani), a uključene IP podmreže moraju podržavati IPv4/IPv6 *dual-stack* operaciju.

Nakon toga, DHCP server treba migrirati na *dual-stack*. Treba instalirati noviju verziju DHCP servera koja podržava IPv6, prije konfigurisanja samog servera za IPv6. Serverski softver mora biti izabran u skladu sa korišćenim klijentima, kako bi se osigurala kompatibilnost.

Prilikom konfiguracije DHCP servera potrebno je odabrati način rada (*stateful* ili *stateless*). U slučaju korišćenja *stateful* DHCPv6, neophodno je odlučiti da li da se IP adrese dodjeljuju na osnovu klijentovog DUID-a ili iz skupa IPv6 adresa.

### 9.4.3. *Web* server

Za rad *web* servera u *dual-stack* modu, potreban je IPv6 pristup od i do ISP-a (GEANT). Pored toga, DNS pristup za traženje adrese *web* servera treba da podržava IPv6. Generalno, u momentu migracije *web* servera već bi trebalo da postoji koncept IPv6 adresa i podešen DNS.

Za postojeći operativni sistem na *web* serveru, potrebno je provjeriti:

- da li (distribucija, verzija, kernel) podržava IPv6 i ako je potrebno izvršiti nadogradnju operativnog sistema u toku migracije;
- konfigurisati aplikaciju *web* servera;
- pošto *web* server radi kao virtuelni sistem, treba provjeriti da li VMware podržava IPv6.

Nakon provjere, potrebno je odlučiti kako konfigurisati IPv6 adresu *web* servera:

- statičkom konfiguracijom na samom hostu *web* servera,
- konfiguracijom na odgovarajućem DHCPv6 serveru koji je odgovoran za podmrežu u kojem se nalazi *web* server (korišćenjem statičkog IPv6 dodeljivanja adrese na DHCP serveru).

Za uspješno DNS pronalaženje IP adrese *web* servera treba da se riješe sledeće stavke:

- eksterno ime za pristupanje *web* serveru od strane IPv6 klijenata treba da bude isto kao što se koristi za IPv4,
- interno korišćeno ime hosta za pristup *web* serveru preko IPv6 protokola treba da bude isto ime kao što se koristi za IPv4 i
- autorizovani DNS server za domen *web* servera treba da bude i sam dostupan preko IPv6, kako bi se dozvolili zahtjevi od strane klijenata na „IPv6 ostrvima“ i unutar IPv6 klijentskih mreža.

Sama aplikacija *web* servera mora biti konfigurisana shodno 8.6.3. Nakon obavljene konfiguracije potrebno je restartovati server, kako bi se utvrdilo da li su sve promjene sačuvane, aktivne i u upotrebi nakon ponovnog pokretanja sistema.

Nakon završetka migracije potrebno je uspješno proći provjere kroz pristup *web* serveru pomoću *web* preglednika (*browser*-a). Ovo podrazumijeva pristup *web* serveru sa klijenata koji imaju razne operativne sisteme, verzije IP protokola, vrste *browser*-a, lokacija u mreži i na Internetu i za sve hostovane sajtove. Pored toga, trebalo bi da se provjere performanse portala/*web* servera za slučaj upotrebe samo IPv4, samo IPv6 i *dual-stack*. Sve gore navedene testove, koji koriste mrežne alate (*ping*, *traceroute*, ...), treba obaviti tako da je korišćena IP verzija eksplicitno navedena (u komandnoj liniji), kako alat ili operativni sistem ne bi birali IP verziju sami od sebe.

### 9.4.4. *Mail* server

Serveri za elektronsku poštu uključuju POP3, IMAP, SMTP servere i agente za prenos pošte (MTA). Pošto IPv4 i IPv6 nisu direktno kompatibilni, MTA-ovi samo za IPv4 i MTA-ovi samo za IPv6 se ne mogu direktno povezati i razmjenjivati podatke.

Kao i za druge servere, treba dokumentovati korišćene funkcije i konfiguraciju *mail* servera prije samog procesa migracije. Kao i kod *web* servera, potrebno je sačuvati parametre mreže i hosta.

Redoslijed kojim se izvršavaju koraci migracije za *mail* server su isti kao kod *web* servera i dati su u 8.5.1. Za MTA je veoma važno da ispravno rade inverznu DNS rezoluciju i za IPv4

i za IPv6, jer je ova funkcija ključna za uspješnu provjeru identiteta između MTA. Sa IPv6, ovaj zahtjev je donekle smanjen, zbog novih tehnika za verifikaciju identiteta.

Tokom početnih funkcionalnih testova preporučuje se da se pažljivo prate log datoteke *mail* servera. Pored toga, korisno je pratiti dolazne i odlazne IP konekcije (posebno njihovo podešavanje), koristeći alat za monitoring mreže sa *dual-stack*-om (na primjer *wireshark* alat).

## 9.5. Mogućnosti integracije postojećih IPv4 komponenti

Predložena *dual-stack* tehnika omogućava integraciju svih komponenti koje podržavaju samo IPv4 protokol, a koje nijesu osnov same implementacije ove tehnike. Dakle, primjenom predloženih koraka migracije zadržava se postojeća funkcionalnost svih IPv4 komponenti i servisa, a omogućena je implementacija novih IPv6 komponenti i servisa.

## 9.6. Preporuka zamjene mrežne infrastrukture potrebne za tranziciju na IPv6 AMUCG sa predračunom

Analizom mrežne opreme koja se trenutno koristi u AMUCG (tabela 9) konstatovano je da je samo dio aktivne mrežne opreme koja se koristi u jezgru mreže u CIS-u UCG-a IPv6 kompatibilna. U pitanju su stavke 1, 2, 3 i 4 iz tabele 9 (granični ruter, 2 *firewall*-a i 3 agregaciona L3 sviča). Preporuka je da se postojećem graničnom ruteru *cisco* ASR1002 poveća kapacitet operativne memorije, a da postojeci L3 svičevi budu zamijenjeni ili se opredijele za neku drugu namjenu u AMUCG jer im performanse ne omogućavaju rad u *dual-stack* režimu. Umjesto njih, za agregaciju saobraćaja AMUCG se preporučuje klaster redudantnih naprednih modularnih L3 IPv6 svičeva koji su performantno sposobni da opslužuju *dual-stack* mehanizam za protoke IP saobraćaja koji se generiše u AMUCG.

Ista preporuka je i za DMZ zonu i farmu servera gdje ovaj segment jezgra mreže treba zamijeniti sa sličnim klasterom redundantnih naprednih modularnih L3 IPv6 svičeva na koje bi se povezala postojeća serverska i *storage* infrastruktura.

Za pozicije udaljenih lokacija (pristupna mreža AMUCG) se mora izvršiti kompletna zamjena komunikacionih uređaja, jer postojeći nisu IPv6 kompatibilni. Predlog je da se na ove pozicije instaliraju modularni L3 uređaji visokih performansi sa mogućnošću povezivanja na razne mrežne interfejse i većom fleksibilnošću za interkonekciju na postojeću AMUCG.

Potrebno je voditi računa da nova mrežna oprema bude kompatibilna sa postojećom.

*Tabela 12. Detaljna tehnička specifiakcija potrebne mrežne opreme*

| R.br. | Opis potrebne mrežne opreme i servisa | Jedinica mjere | Količina | Jedinična cijena EUR | Ukupna cijena EUR |
|---|---|---|---|---|---|
| 1. | Nabavka i isporuka klastera naprednih modularnih stekovanih L3, 19”, 1RU svičeva za glavno mrežno čvorište i DC-serversko čvorište jedinstvene AMUCG prema specifikaciji mrežne opreme i servisa: | komplet | 2 | 32,500.00 | 65,000.00 |

| | | | | | |
|---|---|---|---|---|---|
| | - 2 x napredni L3 modularni IPv6 stekabilni *core* svič u konfiguraciji sa minimalno sledećim interface-ima za isporuku: 12 x 10GBase-T portova, 24 x 1/10G SFP/SFP+ slot portova, 4 x 40G/100G QSFP slot portova sa dodatnim ekspanzionim mrežnim modulom koji podržava 1G, 10G, 40G i 100G kombinacije portova i redudantnim napajanjem za svičeve od minimalno 600W AC.<br>Svič zbog fleksibilnosti i modularnosti u mrežnom jezgru mora da podržava kombinaciju od 1/2.5/5/10 Gigabit *copper* portova, 1/10 Gigabit SFP+ i 40G/100G portova neophodnih za visoki kapacitet i dostupnost. Svič mora da podržava IPv4 i IPv6 *dual-stack*, IPv6 *hardware* ACLs, EPSR i G.8032 ERPS za *resilient* prstenove, OSPFv3, *Active Fiber Monitoring* (AFM) za *fiber data* i *stacking* linkove, OpenFlow v1.3 za SDN, VCStackTM2 jedinicu sa bilo kojom brzinom sa *flexi-stacking*-om, VCStack-LD za *long distance stacking*, *Energy Efficient Ethernet*, Autonomni *Management Framework* licenca za minimalno 120 mrežnih nodova. Svič mora da podržava i minimalno sledeće karakteristike: *switching fabric* od 1,9 Tbps, *forwarding rate* od 1100Mpps, podrška za 10K *jumbo frame* veličine, 4GB SDRAM i *flash* memorija, mogućnost stekovanja do 8 svičeva u jednu stek jedinicu.<br>Klaster svičeva obavezno mora imati napredne premijum licence koje podržavaju minimalno sledeće funkcionalnosti: OSPF3 (16,000 ruta), BGP43 (5,000 ruta), | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | PIMv4-SM, DM i SSM (2,000 *entries*), VLAN *double tagging* (Q-in-Q), RIPng (5,000 ruta), OSPFv3 (8,000 ruta), BGP4+ (5,000 ruta), VLAN *Translation*.<br>Uz svičeve je potrebno isporučiti i komplet *direct attach twinax* kablova za Quad SFP+ (QSFP+) po 2 komada od 1m i 2 komada od 3m. Ponuđena oprema mora da ima 5 godina hardversku garanciju i minimum 1 godinu na servise i tehničku podršku. | | | | |
| 2. | Nabavka i isporuka stekabilnog 10 gigabitnog inteligentnog visoko performantnog L3 uređaja za povezivanje udaljenih jedinca na *core* mrežu AMUCG prema specifikaciji mrežne opreme i servisa:<br>- napredni inteligentni IPv6 stekabilni L3 uredjaj, 19", 1RU u konfiguraciji sa minimalno sledećim interfejsima za isporuku: 8 x 1/2.5/5/10 Gigabit *copper* POE+ portova, 8 x 1/10G SFP/SFP+ *slot* portova, 2 x 40G/100G QSFP *slot* portova. Svič mora da podržava IPv4 i IPv6 *dual-stack*, IPv6 *hardware* ACLs, EPSR i G.8032 ERPS za *resilient* prstenove, OSPFv3, G.8032 *Ethernet Ring Protection*, *Active Fiber Monitoring* (AFM) za *fiber data* i *stacking* linkove, IEEE 802.3at *Power over Ethernet Plus* (PoE+), *Stack* funkcionalnost od minimalno 4 uređaja koristeći bilo koju brzinu portova, OpenFlow v1.3 management na uređaju preko IPv6 mreže sa SNMPv6, Telnetv6 ili SSHv6. Svič takođe mora da podržava i minimalno sledeće karakteristike: *switching fabric* od 480 Gbps, *forwarding rate* od 350Mpps, *stacking bandwidth* | komad | 25 | 4,600.00 | 115,000.00 |

| | | | | | |
|---|---|---|---|---|---|
| | 160 Gbps, *maksimum power consumption* 390W. Ponuđeni L3 uređaji obavezno moraju imati napredne premium licence koje podržavaju minimalno sledeće funkcionalnosti: BGP4 (256 ruta), RIP (256 ruta),OSPF (256 ruta), PIMv4-SM, DM i SSM, EPSR master, VLAN *double tagging* (Q-in-Q), RIPng (256 ruta), OSPFv3 (256 ruta). Ponuđeni L3 uređaj mora imati 5 godina hardversku garanciju i minimum 1 godinu na servise i tehničku podršku. | | | | |
| 3. | Sitni potrošni kablovski material i nespecificirana pasivna mrežna oprema za instalaciju i montažu aktivne opreme. | paušalno | 1 | 2,500.00 | 2,500.00 |
| 4. | Usluge redizajna postojećeg stanja AMUCG sa setovanjem i konfigurisanjem aktivne komunikacione opreme. Izrada dokumentacije izvedenog stanja nakon realizovanja migracije sa IPv4 na IPv6. | paušalno | 1 | 12,500.00 | 12,500.00 |
| | | | UKUPNO: | | 195,000.00 EUR |
| | | | PDV 21%: | | 40,950.00 EUR |
| | | | **UKUPNO SA PDV-om:** | | **235,950.00 EUR** |

Cijene date u tabeli 12 deklarisane su u cjenovnicima dobavljača opreme, što znači da bi se u procesu tenderske procedure mogle postići i niže cijene. Ako se uzme u obzir mogućnost redukcije cijene u tenderskom nadmetanju i angažovanje sopstvenih resursa za redizajniranje infrastrukture, može se očekivati da za 200.000,00 eura predmetna mreža realizuje prvu fazu implementacije, kojom bi se završilo oko 90% aktivnosti na potpunoj migraciji AMUCG. Naime, u drugoj fazi bi se zamijenila nekompatibilna aktivna mrežna infrastruktura LAN mreža članica AMUCG i preostali servisi, a to je neuporedivo lakši i manje zahtjevan dio procesa potpune migracije. Drugim riječima, nakon realizacije prve faze, predmetna mreža i institucija bi skoro završila proces migracije i omogućila da više od 20.000 korisnika ima pristup novim servisima i sadržajima preko IPv6.

Ono što u pripremnoj fazi nije definisano je vremenski okvir, jer institucija (UCG) nije imala potrebu za ovim ograničenjem, ali je Projektni tim oročio prvu fazu implementacije na 6 do 10 mjeseci od trenutka izrade projekta implementacije. Ovaj raspon procijenjenog vremena realizacije je neizbježno uzrokovan nepredvidivim procesom javne nabavke potrebne opreme. Sam proces tehničke implementacije prve faze, kada je oprema na radnoj lokaciji, se može završiti za najviše 3 mjeseca uz neophodno testiranje i validaciju.

Prezentovani plan migracije AMUCG je dobra polazna osnova za Glavni projekat migracije AMUCG na IPv6, kao i primjer kako treba pristupiti ovom procesu za državne institucije i poslovne korisnike. Korišćenje nevedenih preporuka i literature, kao i stečenih iskustava u agilnom pristupu procesu migracije, garant su uspješnosti implementacije novog protokola i otvaranja novih tehničkih i poslovnih mogućnosti za sve subjekte u Crnoj Gori.

# 10. Zaključak

Novi IP protokol, IPv6, je neminovnost i on će, prije ili kasnije, bez obzira na aktivnosti državnih institucija, kompanija, pojedinaca ili društva u cjelini biti implementiran. Upravo zbog te činjenice Crna Gora je odabrala proaktivan pristup u ovoj oblasti i u Strategiji razvoja informacionog društva Crne Gore do 2020. godine definisala prelazak na IPv6 kao jedan od strateških prioriteta. Strategija je jasno prepoznala da je ovaj protokol preduslov za razvoj budućih Internet servisa i osnov za uključivanje u globalno elektronsko tržište. U tom kontekstu, ova Studija predstavlja prvi konkretni korak u pravcu ostvarivanja strateškog ICT infrastrukturnog cilja, definisanjem planova i aktivnosti relevatnih subjekata.

Analiza stanja ICT infrastrukture pokazuje da je Crna Gora jedna od dvije države u Evropi u kojoj nije moguće ostvariti povezivanje na Internet posredstvom IPv6, s tim što postoji određeni nivo inicijative, spremnosti i razmišljanja o migraciji na novi IP protokol. No, evidentan je neplanski pristup i izostanak konkretnih aktivnosti, kao posledica uspostavljenog konformiteta ICT infrastrukture i servisa na staroj IPv4 verziji protokola. Sa druge strane, identifikuje se iskorak u uvođenju novih inovativnih ICT rješenja (IoT, M2M, senzorske mreže, smart rješenja, ...) koja će u svojoj punoj implementaciji zahtijevati upravo funkcionalnosti novog protokola. U tim okolnostima, krajnji je momenat da se pokrene nacionalna i planska akcija u cilju realizacije strateški zacrtanih ciljeva, koji će uskoro biti infrastrukturna neophodnost.

Paralelni rad IPv4 i IPv6 je neizbježan, a istovremeno i koristan sa aspekta procesa migracije i podrške klijentima koji nemaju potrebu za inovacijama ili podržavaju samo jednu verziju IP protokola. Sa tehničkog aspekta, analiza metoda tranzicije pokazuje da IPv4/IPv6 *dual-stack* tehnika predstavlja glavni izbor za tranziciju ICT infrastrukture, uz moguće parcijalne primjene ostalih tehnika koje stoje na raspolaganju (tunelovanje, translacija protokola) kada je to neophodno. U Studiji su date generalne tehničke preporuke i iskustva iz implementacije migracije sličnih sistema koje treba prilagoditi konkretnim uslovima primjene, aktuelnim i budućim tehničkim rješenjima i procedurama. Imajući u vidu dinamiku razvoja u ovoj oblasti, taj dio Studije je podložan promjenama, s tim što odgovara cilju prikaza smjernica dobre prakse koje ukazuju da je tehnički dio samog procesa u velikoj mjeri standardizovan i na nivou realizacije sličnih ICT projekata koje su subjekti ciljne grupe već implementirali na velikom broju primjera.

Novi IP protokol omogućava dodatne funkcionalnosti u odnosu na IPv4 koje se mogu iskoristiti u svrhu povećanja mogućnosti praćenja saobraćaja i korisnika na Interentu ali, sa druge strane, i ugrožavanja privatnosti korisnika. Imajući u vidu da je, s obzirom na niži nivo potencijalnih ranjivosti, zaštita sistema generalno efikasnija kod sistema koji ne uključuju kompleksna rješenja, može se zaključiti da prelazak na IPv6 protokol garantuje veću *cyber* sigurnost. No sama tranzicija na novi protokol, tj. faza dualizma dva protokola, predstavlja svojevrstan izazov sa aspekta sigurnosti mreža i korisnika zbog dupliranja funkcionalnosti i povećane kompleksnosti sistema. Upravo zato je neophodno procesu implementacije IPv6

protokola pristupiti pažljivo, sagledavajući stanje postojeće infrastrukture, estimirajući posledice uključivanja novog protokola i ostvarujući konfigurisanje sistema po principu provjere zaštite i ranjivosti sistema. Minimum koji treba realizovati je da podešavanja svih postojećih mehanizama zaštite budu implementirana na ekvivalentan način za oba protokola.

Studija pokazuje da nije samo aspekt sigurnosti razlog za neophodnošću izbora adekvatnog scenarija i izrade konkretnog i jedinstvenog plana tranzicije na novi IP protokol za bilo koji subjekat. Ekonomski aspekti, raznolikost infrastruktura i servisa, legislativni okvir, razvojni planovi, profili i navike klijenata, itd., predstavljaju neke od najvažnijih elemenata koje treba uzeti u obzir prilikom izbora adekvatnog scenarija i plana migracije. Istovremeno, TCP/IP skup protokola je zajednički imenilac u svim pojedinačnim slučajevima i jasna tehnička pravila postoje, koja u kombinaciji sa iskustvima uspješnih tranzicija, omogućavaju identifikaciju generalnih smjernica i scenarija, koji se mogu uspješno primijeniti u svakom konkretnom sistemu. U tom kontekstu, na nivou generalizovanog pristupa za izbor scenarija tranzicije, u Studiji je dat predlog izbora scenarija za relevantne grupe subjekata u Crnoj Gori.

Imajući u vidu da su državne institucije, javna preduzeća i lokalne samouprave među najvećim korisnicima ICT rješenja i resursa u Crnoj Gori, te da je migracija na IPv6 definisana kao strateški cilj na državnom nivou, bilo je neophodno izdvojeno predložiti, i posebno naglasiti, plan migracije upravo za ovu grupu subjekata. Kako kreatori Studije smatraju krucijalnim i presudnim inicijativu i aktivnosti upravo ovih institucija za sam proces tranzicije, preporučene su sledeće aktivnosti:

- formiranje nacionalnog tijela („*IPv6 task force*“) ili tima koji će napraviti akcioni plan migracije na IPv6 državnih institucija, koordinisati aktivnosti, promovisati i pratiti proces migracije. Članovi tima bi trebali biti predstavnici subjekata koji će biti nosioci procesa migracije (resornih državnih institucija, regulatora, operatora, akademske zajednice, ICT biznisa i slično);
- podsticanje i organizovanje promocije prednosti IPv6 protokola i edukacije o tehnikama migracije subjekata na svim nivoima javne administracije i rezidencijalnih korisnika;
- organizovanje i realizacija anketiranja operatora o njihovim planovima tranzicije na IPv6;
- formiranje i formalizovanje preporuka i smjernica državnim institucijama u pogledu implementacije IPv6 na administrativnom nivou;
- formiranje laboratorije, u okviru CIS-a UCG, za testiranje koraka tranzicije na IPv6;
- podsticanje planske migracije u mreži Univerziteta Crne Gore na IPv6 putem *dual-stack* tehnologije prema scenariju „spolja ka unutra“, kao pilot projekat na osnovu kojeg će se dokumentovati stečeno iskustvo i znanje koje se može primijeniti na ostale državne institucije;
- priprema plana migracije za državne institucije na osnovu Projekta i dokumentovanih aktivnosti UCG-a;
- realizacija migracije državnih institucija primjenom *dual-stack* tehnologije na IPv6 protokol.

Ovim bi se planski i postepeno, bez narušavanja poslovnih procesa i angažovanja enormnih resursa, izvršila migracija na IPv6 protokol u državnim institucijama, a time bi se podstakli ostali subjekti da izvrše pripreme i prelazak na novi IP protokol.

Studija sadrži generalne tehničke preporuke za implementaciju IPv6 protokola u javnim ustanovama u Crnoj Gori, koje treba uzeti u obzir prilikom kreiranja akcionog plana i konkretnih projekata za neposrednu implementaciju migracije na IPv6, uz njihovu razradu u cilju prilagođenja partikularnom poslovnom okruženju i infrastrukturi. Kako je neophodno da procesu migracije prethodi adekvatna priprema i projekat migracije u svakom pojedinačnom slučaju, realno je očekivati da dođe i do određenih prilagođenja, na nivou detalja, datih preporuka.

Konačno, primjenom datih preporuka na primjeru AMUCG, a na osnovu ulaznih podataka za planiranje prve faze implementacije, kreiran je i opisan plan migracije AMUCG kao polazna osnova za Glavni projekat migracije AMUCG na IPv6. Na taj način je predstavljen i konkretan primjer pristupa procesu migracije u državnim institucijama, koji je moguće primijeniti i kod drugih poslovnih korisnika.

Korišćenje preporuka datih u Studiji, literature, tehničkih standarda i stečenih iskustava u agilnom pristupu procesu migracije, predstavljaju garant uspješnosti implementacije novog Internet protokola i otvaranja novih tehničkih i poslovnih mogućnosti za sve subjekte u Crnoj Gori.

# 11. Literatura


[1] Strategija razvoja informacionog društva Crne Gore do 2020. godine. Dostupno na: http://www.cirt.me/ResourceManager/FileDownload.aspx?rId=259924&rType=2 [pristupano: novembar 2018]

[2] RFC 791 - Internet Protocol, DARPA Internet Program, Protocol Specification. Dostupno na: https://tools.ietf.org/html/rfc791 [pristupano: novembar 2018]

[3] RFC 760 - DoD standard Internet Protocol. Dostupno na: https://tools.ietf.org/html/rfc760 [pristupano: novembar 2018]

[4] Internet Engineering Task Force/RFC dokumenti: https://www.ietf.org/standards/rfcs/ [pristupano: novembar 2018]

[5] Named Data Networking: Executive Summary, https://named-data.net/project/execsummary/ [pristupano: novembar 2018]

[6] RFC 1517 - Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR). Dostupno na: https://tools.ietf.org/html/rfc1517 [pristupano: novembar 2018]

[7] RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations. Dostupno na: https://tools.ietf.org/html/rfc2663 [pristupano: novembar 2018]

[8] Agencija za elektronske komunikacije i poštansku djelatnost, „Studija o uspostavljanju nacionalne tačke razmjene Internet saobraćaja u Crnoj Gori“, Novembar 2013.

[9] RFC 1883 - Internet Protocol, Version 6 (IPv6) Specification. Dostupno na: https://tools.ietf.org/html/rfc1883 [pristupano: novembar 2018]

[10] RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. Dostupno na: https://tools.ietf.org/html/rfc2460 [pristupano: novembar 2018]

[11] RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification. Dostupno na: https://tools.ietf.org/html/rfc8200 [pristupano: novembar 2018]

[12] RFC 2402 - IP Authentication Header. Dostupno na: https://tools.ietf.org/html/rfc2402 [pristupano: novembar 2018]

[13] RFC 2406 - IP Encapsulating Security Payload (ESP). Dostupno na: https://tools.ietf.org/html/rfc2406 [pristupano: novembar 2018]

[14] RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture. Dostupno na: https://tools.ietf.org/html/rfc3513 [pristupano: novembar 2018]

[15] RFC 2373 - IP Version 6 Addressing Architecture. Dostupno na: https://tools.ietf.org/html/rfc2373 [pristupano: novembar 2018]

[16] RFC 4193 - Unique Local IPv6 Unicast Addresses. Dostupno na: https://tools.ietf.org/html/rfc4193 [pristupano: novembar 2018]

[17] RFC 4007 - IPv6 Scoped Address Architecture. Dostupno na: https://tools.ietf.org/html/rfc4007 [pristupano: novembar 2018]

[18] RFC 4291 - IP Version 6 Addressing Architecture. Dostupno na: https://tools.ietf.org/html/rfc4291 [pristupano: novembar 2018]

[19] RFC 6540 - IPv6 Support Required for All IP-Capable Nodes. Dostupno na: https://tools.ietf.org/html/rfc6540 [pristupano: novembar 2018]

[20] World IPv6 Launch – measurements. Dostupno na: https://www.worldipv6launch.org/measurements/ [pristupano: novembar 2018]

[21] Google IPv6 Statistics. Dostupno na: https://www.google.com/intl/en/ipv6/statistics.html [pristupano: novembar 2018]

[22] RIPE NCC. Dostupno na: https://stat.ripe.net/me#tabId=database [pristupano: novembar 2018]
[23] RFC 2462 - IPv6 Stateless Address Autoconfiguration. Dostupno na: https://tools.ietf.org/html/rfc2462 [pristupano: novembar 2018]
[24] RFC 3596 - DNS Extensions to Support IP Version 6. Dostupno na: https://tools.ietf.org/html/rfc3596 [pristupano: novembar 2018]
[25] RFC 4554 - Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks. Dostupno na: https://tools.ietf.org/html/rfc4554 [pristupano: novembar 2018]
[26] RFC 7059 - A Comparison of IPv6-over-IPv4 Tunnel Mechanisms. Dostupno na: https://tools.ietf.org/html/rfc7059 [pristupano: novembar 2018]
[27] RFC 6830 - The Locator/ID Separation Protocol (LISP). Dostupno na: https://tools.ietf.org/html/rfc6830 [pristupano: novembar 2018]
[28] RFC 6144 - Framework for IPv4/IPv6 Translation. Dostupno na: https://tools.ietf.org/html/rfc6144 [pristupano: novembar 2018]
[29] RFC 6145 - IP/ICMP Translation Algorithm. Dostupno na: https://tools.ietf.org/html/rfc6145 [pristupano: novembar 2018]
[30] RFC 6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Dostupno na: https://tools.ietf.org/html/rfc6146 [pristupano: novembar 2018]
[31] RFC 6052 - IPv6 Addressing of IPv4/IPv6 Translators. Dostupno na: https://tools.ietf.org/html/rfc6052 [pristupano: novembar 2018]
[32] RFC 2765 - Stateless IP/ICMP Translation Algorithm (SIIT). Dostupno na: https://tools.ietf.org/html/rfc2765 [pristupano: novembar 2018]
[33] RFC 1918 - Address Allocation for Private Internets. Dostupno na: https://tools.ietf.org/html/rfc1918 [pristupano: novembar 2018]
[34] RFC 6147 - DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. Dostupno na: https://tools.ietf.org/html/rfc6147 [pristupano: novembar 2018]
[35] RFC 1928 - SOCKS Protocol Version 5. Dostupno na: https://tools.ietf.org/html/rfc1928 [pristupano: novembar 2018]
[36] RFC 3089 - A SOCKS-based IPv6/IPv4 Gateway Mechanism. Dostupno na: https://tools.ietf.org/html/rfc3089 [pristupano: novembar 2018]
[37] Spafford, E. H. „The Internet Worm Program: An Analysis“, Purdue Technical Report CSD-TR-823, 1988. Dostupno na: https://spaf.cerias.purdue.edu/tech-reps/823.pdf [pristupano: novembar 2018]
[38] Knoblauch, M. „How One Hacker's Mistake Fashioned the Internet You Use Today“, https://mashable.com/2013/11/01/morris-worm/ [pristupano: novembar 2018]
[39] Global Security, Solar Sunrise, https://www.globalsecurity.org/military/ops/solar-sunrise.htm [pristupano: novembar 2018]
[40] The Malware Wiki, Melissa, http://malware.wikia.com/wiki/Melissa [pristupano: novembar 2018]
[41] Harris, J. K. „Ethical Perspectives in Information Security Education“, Issues in Information Systems, Vol. VII, No. 1, 2006. Dostupno na: https://web.archive.org/web/20070929144818/http:/www.iacis.org/iis/2006_iis/PDFs/Harris.pdf [pristupano: novembar 2018]
[42] Karnouskos, S. „Stuxnet Worm Impact on Industrial Cyber-Physical System Security“, IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society, 2011. Dostupno na: https://papers.duckdns.org/files/2011_IECON_stuxnet.pdf [pristupano: novembar 2018]

[43] Etherington, D. and Conger, K. „Large DDoS attacks cause outages at Twitter, Spotify, and other sites“, https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ [pristupano: novembar 2018]
[44] RFC 4301 - Security Architecture for the Internet Protocol. Dostupno na: https://tools.ietf.org/html/rfc4301 [pristupano: novembar 2018]
[45] Frankel, S., Graveman, R., Pearce, J. and Rooks, M., „Guildelines for the Secure Deployment of IPv6", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-119, 2010. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf [pristupano novembar 2018]
[46] RFC 3715 - IPsec-Network Address Translation (NAT) Compatibility Requirements. Dostupno na: https://www.ietf.org/rfc/rfc3715.txt [pristupano: novembar 2018]
[47] RFC 3947 - Negotiation of NAT-Traversal in the IKE. Dostupno na: https://tools.ietf.org/html/rfc3947 [pristupano: novembar 2018]
[48] RFC 4944 - Transmission of IPv6 Packets over IEEE 802.15.4 Networks. Dostupno na: https://tools.ietf.org/html/rfc4944 [pristupano: novembar 2018]
[49] LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP. Dostupno na: https://tools.ietf.org/html/draft-ietf-lpwan-ipv6-static-context-hc-17 [pristupano: novembar 2018]
[50] RFC 4890 - Recommendations for Filtering ICMPv6 Messages in Firewalls. Dostupno na: https://tools.ietf.org/html/rfc4890 [pristupano: novembar 2018]
[51] RFC 5340 - OSPF for IPv6. Dostupno na: https://tools.ietf.org/html/rfc5340 [pristupano: novembar 2018]
[52] RFC 2080 - RIPng for IPv6. Dostupno na: https://tools.ietf.org/html/rfc2080 [pristupano: novembar 2018]
[53] RFC 5082 - The Generalized TTL Security Mechanism (GTSM). Dostupno na: https://tools.ietf.org/html/rfc5082 [pristupano: novembar 2018]
[54] RFC 2535 - Domain Name System Security Extensions. Dostupno na: https://tools.ietf.org/html/rfc2535 [pristupano: novembar 2018]
[55] Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose, RIPE NCC, https://www.ripe.net/publications/docs/ripe-690 [pristupano: novembar 2018]
[56] IEEE OUI. Dostupno na: http://standards-oui.ieee.org/oui.txt [pristupano novembar 2018]
[57] RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Dostupno na: https://tools.ietf.org/html/rfc4941 [pristupano: novembar 2018]
[58] RFC 4852 - IPv6 Enterprise Network Analysis - IP Layer 3 Focus. Dostupno na: https://tools.ietf.org/html/rfc4852 [pristupano: novembar 2018]
[59] RFC 4942 - IPv6 Transition/Coexistence Security Considerations. Dostupno na: https://www.ietf.org/rfc/rfc4942.txt [pristupano: novembar 2018]
[60] RFC 4891 - Using IPsec to Secure IPv6-in-IPv4 Tunnels. Dostupno na: https://tools.ietf.org/html/rfc4891 [pristupano: novembar 2018]

[61] Zakon o elektronskim komunikacijama, 2013. Dostupno na: http://www.ekip.me/download/Zakon%20o%20elektronskim%20komunikacijama-40_2013.pdf [pristupano: novembar 2018]
[62] Cormack, A. „IP Addresses, Privacy and the GDPR“, https://community.jisc.ac.uk/blogs/regulatory-developments/article/ip-addresses-privacy-and-gdpr [pristupano: novembar 2018]
[63] General Data Protection Regulation (GDPR) - Principles relating to processing of personal data, https://gdpr-info.eu/art-5-gdpr/ [pristupano: novembar 2018]
[64] MC/111 Internet Protocol Version 6 Deployment Study, InterConnect Communications Ltd, Merlin House, United Kingdom, 2012. Dostupno na: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/55891/internet-protocol.pdf [pristupano: oktobar 2018]
[65] RFC 3041 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Dostupno na https://tools.ietf.org/html/rfc3041 [pristupano: novembar 2018]
[66] Internet Society Perspectives on Internet Content Blocking: An Overview. March 2017. Dostupno na: https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf [pristupano: januar 2019]
[67] Statistički podaci o usvajanju IPv6 na Internetu koje Google kontinuirano prikuplja. Dostupno na: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption [pristupano: oktobar 2018]
[68] The North American IPv6 Task Force, http://www.nav6tf.org
[69] The IPv6 Forum, http://www.ipv6forum.com
[70] Request for Comments on Deployment of Internet Protocol, Version 6, Docket No. 040107006-4006-01, 69 Fed Reg. 2890 (National Institute of Standards and Technology [NIST] and National Telecommunications and Information Administration [NTIA], Jan. 21, 2004.
[71] Transition Planning for Internet Protocol Version 6 (IPv6), Executive Office of the President, 2005. Dostupno na: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf [pristupano: oktobar 2018]
[72] Tassey, G.C., Montgomery, D.C., Lee, A. and Sloan, T., „Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)“. Dostupno na: https://www.nist.gov/publications/technical-and-economic-assessment-internet-protocol-version-6-ipv6-0 [pristupano: oktobar 2018]
[73] A profile for IPv6 in the U.S. Governement (USG IPv6 Profile), USA National Institute of Standards and Technology, 2008. Dostupno na: https://www.nist.gov/sites/default/files/documents/itl/antd/usgv6-v1.pdf [pristupano: oktobar 2018]
[74] USGv6 Test Methods: General Description and Validation, USA National Institute of Standards and Technology, 2009. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-273v2.pdf [pristupano: oktobar 2018]
[75] Statistički podaci o podršci provajdera u SAD za IPv4 i IPv6 protokol: http://ipv6-test.com/stats/country/US
[76] Recomendations for a Strategic Plan in the Development and Implementation of IPv6 Technologies in France, Task Force IPv6 France, November 2003. Dostupno na: http://www.fr.ipv6tf.org/DATA/PRESS/Recommandations%20IPv6%20TFF%20%28English%29.pdf [pristupano: oktobar 2018]

[77] Deployment and test of IPv6 services in the VTHD network, IEEE Communications Magazine, Vol. 42, No. 1, Jan. 2004. Dostupno na: https://ieeexplore.ieee.org/document/1262168?arnumber=1262168,
[78] RENATER mreža: https://www.renater.fr/?lang=en
[79] VTHD project: IPv6 deployment, ITU-T IP/Optical workshop – Chitose, ppt prezentacija, 2002. Dostupno na: www.itu.int/itudoc/itu-t/workshop/optical/s01-p01r_pp7.ppt [pristupano: novembar 2018]
[80] The European ISP case: France Telecom, Workshop on IPv6, Geneva, 2005. Dostupno na: https://www.itu.int/ITU-T/worksem/ipv6/200506/presentations/s2-2-meriem.pdf [pristupano: novembar 2018]
[81] Nerim internet provajder u Francuskoj: https://www.nerim.fr/
[82] Statistički podaci o podršci provajdera u Francuskoj za IPv4 i IPv6 protokol: http://ipv6-test.com/stats/country/FR
[83] Projekat 6NET: https://www.6net.org/, https://cordis.europa.eu/project/rcn/61113_en.html [pristupano: novembar 2018]
[84] Projekat 6DISS: https://www.6diss.org/ [pristupano: novembar 2018]
[85] Projekat Go4it: https://cordis.europa.eu/project/rcn/80143_en.html [pristupano: novembar 2018]
[86] Projekat 6WINIT: http://www.6winit.org/, https://cordis.europa.eu/project/rcn/53710_en.html [pristupano: novembar 2018]
[87] Projekat EURO6IX: https://cordis.europa.eu/project/rcn/61118_en.html [pristupano: novembar 2018]
[88] SixXS - IPv6 Deployment & Tunnel Broker: https://www.sixxs.net/ [pristupano: novembar 2018]
[89] IPv6 in Germany, Constanze Bürger, Ministry of the Interior Department, Federal IT Infrastructures and IT Security Management, 2010. Dostupno na: https://www.nro.net/wp-content/uploads/2010-burger.pdf [pristupano: novembar 2018]
[90] Komesarijat vlade Savezne Republike Njemačke za informacione tehnologije: https://www.cio.bund.de/Web/DE/Startseite/startseite_node.html
[91] Njemački IPv6 savjet: https://hpi.de/en/ipv6council/index.html
[92] Nationaler IPv6 Aktionsplan für Deutschland: https://hpi.de/fileadmin/ipv6council/documents/Nationaler_IPv6-Aktionsplan_f%C3%BCr_Deutschland_14092009.pdf [pristupano: novembar 2018]
[93] Izvještaj o godišnjem sastanku Njemačkog IPv6 savjeta, Institut Hasso-Plattner, Potsdam, 2016. Dostupno na: https://hpi.de/ipv6council/events-medien/jahressitzung-deutscher-ipv6-rat.html [pristupano: novembar 2018]
[94] Leitfaden für eine sichere IPv6-Netzwerkarchitektur, Bundesamt für Sicherheit in der Informationstechnik, 2012. Dostupno na: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf.pdf?__blob=publicationFile [pristupano: novembar 2018]
[95] Procenat pristupanja Google servisima posredstvom IPv6 preglednika u Njemačkoj: https://www.vyncke.org/ipv6status/compare.php?metric=p&countries=de [pristupano: novembar 2018]
[96] Deutsche Forschungsnetz (DFN) – komunikaciona mreža za istraživačke i naučne organizacije u Njemačkoj: https://www.dfn.de/en/
[97] Statistički podaci o podršci provajdera u Njemačkoj za IPv4 i IPv6 protokol: http://ipv6-test.com/stats/country/DE [pristupano: novembar 2018]
[98] Poređenje upotrebe preglednika koji koriste IPv6 u SAD, Francuskoj, Njemačkoj, Japanu i Kini, izraženo u procentima:

https://www.vyncke.org/ipv6status/compare.php?metric=p&countries=de,fr,us,cn,jp [pristupano: novembar 2018]
[99] Popoviciu, C.P. and Grossetete, P., „The role of National Strategies in maintaining Competitive Edge in Information and Communication Technologies“, Systemics, cybernetics and informatics, Vol. 4, No. 6, 2006. Dostupno na: http://www.iiisci.org/journal/CV$/sci/pdfs/P563955.pdf [pristupano: novembar 2018]
[100] Coleman, L., „Next Generation Internet Policy in Japan, China and India“, Asia & the Pacific Policy Studies, Vol. 1, No. 3, pp. 497–512, 2014. Dostupno na: https://onlinelibrary.wiley.com/doi/epdf/10.1002/app5.44 [pristupano: novembar 2018]
[101] Japanski savjet za promociju IPv6 (*IPv6 Promotion Council of Japan*): http://www.v6pc.jp/en/index.phtml
[102] Euro IPv6 Task Force and IPv6 Promotion Council of Japan Forge Strategic Alliance to foster IPv6 deployment world-wide, Press release. Dostupno na: http://www.ipv6tf.org/PublicDocuments/TF-v6PCJointPressReleasev2_FINAL.pdf [pristupano: novembar 2018]
[103] Statistički podaci o podršci provajdera u Japanu za IPv4 i IPv6 protokol: http://ipv6-test.com/stats/country/JP
[104] Bradsher, K., „Economic Growth in China Is Stronger Than Expected“, The New Yourk Times, April 2005. Dostupno na: https://www.nytimes.com/2005/04/21/business/worldbusiness/economic-growth-in-china-is-stronger-than-expected.html [pristupano: novembar 2018]
[105] *China Education and Research Net* – CERNET: http://www.edu.cn/english/
[106] IPv6 and the 2008 Beijing Olympics: https://www.ipv6.com/general/ipv6-and-the-2008-beijing-olympics/#Chinas_Next_Generation_Internet_CNGI [pristupano: novembar 2018]
[107] Wu, J., Wang, J.H. and Yang, J., „CNGI-CERNET2: an IPv6 Deployment in China“, ACM SIGCOMM Computer Communication Review, Vol. 41, No. 2, pp. 48-52, 2011. Dostupno na: http://www.sigcomm.org/sites/default/files/ccr/papers/2011/April/1971162-1971170.pdf [pristupano: novembar 2018]
[108] Chirgwin, R., „China plots new Great Leap Forward: to IPv6“, The Register, 2017. Dostupno na: https://www.theregister.co.uk/2017/11/27/china_plots_new_great_leap_forward_to_ipv6/ [pristupano: novembar 2018]
[109] Statistički podaci o podršci provajdera u Kini za IPv4 i IPv6 protokol: http://ipv6-test.com/stats/country/CN
[110] Kunc, U., Pepelnjak, I., Sterle, J., Straus Istenič, M., Kobal, A., Lisec, S., Maennel, O, Žorž, J., „Study: Transition to IPv6 (Guidelines for Deliberation on the National IPv6 Strategy)“, The Government of the Republic of Slovenia, Ministry of Higher Education, Science and Technology, 2010.
[111] RFC 4294 - IPv6 Node Requirements. Dostupno na: https://tools.ietf.org/html/rfc4294 [pristupano: novembar 2018]
[112] Requirements for IPv6 in ICT Equipment. Dostupno na: https://www.ripe.net/publications/docs/ripe-554 [pristupano: novembar 2018]
[113] Schmoll, C., Günther, T., Schaa Cassini, T., Tiemann, J., Bürger, C., „IPv6 Transition Guide for the Public Administration“, German Federal Office of Administration, 2013.
[114] RFC 7748 - Elliptic Curves for Security. Dostupno na: https://tools.ietf.org/html/rfc7748 [pristupano: novembar 2018]

[115] RFC 4862 - IPv6 Stateless Address Autoconfiguration. Dostupno na: https://tools.ietf.org/html/rfc4862 [pristupano: novembar 2018]

[116] NAT64check: https://www.nat64check.org/ [pristupano: januar 2019]

[117] RFC 1157 - A Simple Network Management Protocol (SNMP). Dostupno na: https://tools.ietf.org/html/rfc1157 [pristupano: novembar 2018]

# 12. Rječnik skraćenica

AAA – *Authentication, Authorization, Accounting*, autentifikacija, autorizacija i obračun

ACL – *Access Control Lists*, lista kontrole pristupa - određuje koji korisnici ili sistemski procesi imaju pristup objektima, kao i koje operacije su dozvoljene na datim objektima

ADSL – *Asymmetric Digital Subscriber Line*, tehnologija prenosa podataka preko telefonskih linija

AERO – *Asymmetric Extended Route Optimization*, podržava mobilnost modeliranjem poslovne mreže kao virtuelne veze kroz enkapsulaciju

AH – *Authentication Header* protokol

AI – *Artifical Intelligence*, vještačka inteligencija

ALG – *Application Layer Gateway*, softverska komponenta koja djeluje kao posrednik između Interneta i aplikacionog servera

AMUCG – Akademska Mreža Univerziteta Crne Gore

APIPA – *Automatic Private IP Addressing*, funkcija operativnog sistema koja omogućava računaru da sam sebi dodijeli IP adresu kada nema dostupnog DHCP servera

AS – *Autonomous System*, autonomni sistem u mrežnoj hijerarhiji

ASN – *Autonomous System Number*, jedinstveni broj koji je globalno dostupan za identifikaciju autonomnog sistema i koji omogućava tom sistemu da razmijeni informacije o spoljašnjem rutiranju sa drugim susjednim autonomnim sistemima

AVM – *AudioVisual Media*, sadržaji koji imaju i zvučnu i vizuelnu komponentu

AYIYA – *Anything In Anything*, mrežni protokol za upravljanje protokolima IP tunela između odvojenih IP mreža

BDP – Bruto Društveni Proizvod

BGP – *Border Gateway Protocol*, protokol za usmjeravanje saobraćaja između mrežnih autonomnih sistema

BRAS – *Broadband Remote Access Server*, usmjerava saobraćaj ka i od uređaja za širokopojasni daljinski pristup na mreži ISP-a

CA – *Certification Authority*, entitet koji izdaje digitalne sertifikate

CANU – Crnogorska Akademija Nauka i Umjetnosti

CERNET – *China Education and Research Net*, prva nacionalna obrazovna i istraživačka računarska mreža u Kini

CIDR – *Classless Inter Domain Routing*, bezklasno međudomensko rutiranje

CIFS – *Common Internet File System*, mrežni protokol koji se koristi za omogućavanje zajedničkog pristupa fajlovima

CIS UCG – Centar informacionog sistema Univerziteta Crne Gore

CKB – Crnogorska Komercijalna Banka

CNGI – *China Next Generation Internet*, projekat koji je inicirala kineska vlada u cilju razvoja Interneta kroz rano usvajanje IPv6

CPE – *Customer Premises Equipment*, oprema čija se fizička lokacija nalazi u prostorijama klijenta, a ne u prostorijama provajdera ili između njih

CPU – *Central Processing Unit*, centralna procesorska jedinica – procesor

DA – *Destination Address*, adresa odredišnog čvora kome je upućen paket

DDoS – *Distributed Denial of Service*, napad na računar ili sistem do koga dolazi kada više spoljnih sistema zaokupe propusni opseg ili resurse ciljanog sistema

DHCP – *Dynamic Host Configuration Protocol*, protokol koji automatski obezbjeđuje IPv4 adresu i druge srodne informacijame o konfiguraciji, kao što su maska podmreže i podrazumijevani *gateweay*

DHCPv6 – DHCP verzije 6

DMZ – *DeMilitarized Zone*, fizička ili logička podmreža koja sadrži i pruža usluge koje se odnose na spoljašnje nepouzdane mreže

DNS – *Domain Name System*, sistem Internet naziva i pripadajućih servera za prevođenje Internet adresa u imena

DNSSEC – *Domain Name System Security Extensions*, skup specifikacija IETF-a za osiguranje određenih vrsta informacija koje pruža DNS na IP mrežama

DSCP – *Differentiated Services Code Point*, 8-bitno polje (polje DS) u IP zaglavlju za klasifikaciju paketa

DSL – *Digital Subscriber Line*, tehnologija koja se koristi za prenos podataka preko telefonskih linija

DUID – *DHCP unique identifier*, koristi se od strane klijenta da dobije IP adresu od DHCPv6 servera

EC – *European Commission*, Evropska komisija

ECN – *Explicit Congestion Notification*, ekstenzija Internet protokola koja omogućava obavještavanje o zagušenju mreže bez odbacivanja paketa

EEA – *European Economic Area*, evropska ekonomska zajednica

EID – *Endpoint Identifiers*, IPv4 ili IPv6 adresa koja se koristi za identifikaciju krajnje tačke na mreži

ESP – *Encapsulating Security Payload*, protokol u okviru IPSec-a za obezbjeđivanje autentičnosti, integriteta i povjerljivosti podataka u IPv4 i IPv6 mrežama

EU – Evropska unija

EUI – *Extended Unique Identifier*, proširena jedinstveni identifikator mrežnog interfejsa

FC – *Fibre Channel*, protokol za prenos podataka velikom brzinom, prvenstveno za povezivanje skladišta računarskih podataka (*storage*) sa serverima

FCoE – *Fibre Channel over Ethernet*, mrežna tehnologija koja enkapsulira *Fibre Channel* pakete preko *Ethernet* mreža

FL – *Flow Label*, 20-bitno polje, kod zaglavlja IPv6 paketa, za identifikaciju toka podataka kojem određeni paket pripada

FO – *Fragment Offset*, polje koje specificira ofset određenog fragmenta u odnosu na početak originalnog nefragmentiranog IP datagrama

FTP – *File Transfer Protocol*, protokol koji se koristi za prenos fajlova između klijenta i servera na računarskoj mreži

GDPR – *General Data Protection Regulation*, propisi o zaštiti podataka i privatnosti za sve pojedince unutar EU i EEA

GGSN – *Gateway GPRS Support Node*, dio jezgra mreže koji povezuje GSM 3G mreže na Internet

GPRS – *General Packet Radio Service*, standard za prenos podataka na 2G i 3G GSM mreži

GPS – *Global Positioning System*, satelitski radio-navigacioni sistem koji obezbjeđuje geolokaciju i informacije o vremenu

GRE – *Generic Routing Encapsulation*, protokol za tunelovanje razvijen od strane *Cisco Sistems*-a

GTSM – *Generalized TTL Security Mechanism*, metoda zaštite prenosa Internet paketa bazirana na vrijednosti TTL (HL) polja u IP zaglavlju

GUA – *Global unicast address*, globalno jedinstvena adresa na Internetu

HBA – *Host Bus Adapter*, povezuje host sa drugim mrežnim uređajima i uređajima za skladištenje podataka

HC – *Header Checksum*, kontrolna suma zaglavlja IPv4 paketa

HELO – komanda koja se koristi kod SMTP

HL – *Hop Limit*, 8-bitno polje na nivou cijelog broja, koji se umanjuje za 1 od strane svakog čvorišta koje proslijedi paket

HLR – *Home Location Register*, baza podataka koja sadrži podatke o pretplatnicima ovlaštenim za korištenje GSM mreže

HSS – *Home Subscriber Server*, baza podataka u okviru IMS-a koja pruža podatke o pretplatnicima drugim entitetima unutar mreže

HTTP – *HyperText Transfer Protocol*, protokol koji se koristi za *web*

HTTPS – *Hyper Text Transfer Protocol Secure*, sigurni HTTP

IAB – *Internet Architecture Board*, tijelo koje nadgleda tehnički razvoj Interneta

ICMP – *Internet Control Message Protocol*, protokol podrške u paketu Internet protokola

ICT – *Information Communication Technlogy*, informaciono-komunikacione tehnologije

ID – identifikator

IEEE – *Institute of Electrical and Electronics Engineers*, profesionalna asocijacija inženjera elektrotehnike

IETF – *Internet Engineering Task Force*, profesionalna asocijacija koja se bavi standardizacijom tehničkih rješenja za unapređenje Interneta

IGP – *Interior Gateway Protocol*, protokol koji se koristi za razmjenu informacija o rutiranju između *gateway*-a

IHL – *Internet* Header *Length*, polje unutar zaglavlja IP paketa koje specificira dužinu samog zaglavlja

IKE – *Internet Key Exchange*, protokol

IoT – *Internet of Things*, Internet povezanih objekata

IP – *Internet Protocol*, Internet protokol

IP adresa – identifikator mrežnog interfejsa usklađen sa IP standardima

IPAM – *IP Address Management System*, sistem za upravljanje IP adresama

IPS – *Intrusion Prevention System*, sistem za sprečavanje neovlašćenog pristupa

IPSec – *IP Security*, skup protokola koji međusobno komuniciraju kako bi osigurali sigurnu privatnu komunikaciju preko IP mreža

IPT – *IP Transit*, servis koji omogućava saobraćaju sa druge mreže da prođe kroz mrežu provajdera

IPTV – *Internet Protocol Television*, isporuka televizijskog sadržaja preko IP mreža

IPv4 – IP adresa dužine 32 bita

IPv6 – IP adresa dužine 128 bita

ISATAP – *Intra-Site Automatic Tunnel Addressing Protocol*, IPv6 tehnika tunelovanja koja omogućava povezivanje IPv6 preko IPv4 mreže

ISO – *International Organization for Standardization*, međunarodno tijelo za uspostavljanje standarda koje čine predstavnici različitih nacionalnih organizacija za standarde

ISOC – *Internet Society*, međunarodna neprofitna organizacija koja se bavi promocijom Internet tehnologija, obrazovanjem i razvojem politika vezanih za Internet

ISP – *Internet Service Provider*, pružalac usluge pristupa Internetu

ITU – *International Telecommunication Union*, specijalizovana agencija Ujedinjenih nacija koja je odgovorna za pitanja koja se tiču informaciono-komunikacionih tehnologija

IXP – *Internet eXchange Point*, tačka razmjene Internet saobraćaja

L2, Layer2 – drugi nivo OSI modela

L3, Layer3 – treći nivo OSI modela

LAN – *Local Area Network*, lokalna računarska mreža

LIR – *Local Internet Registry*, odgovoran je za distribuciju i registraciju adresnog prostora na lokalnom nivou

LISP – *Locator/ID Separation Protocol*, protokol koji je razvila IETF LISP radna grupa

LLC – *Logical Link Control*, podsloj nivoa linka sedmoslojnog OSI modela

M2M – *Machine to Machine*, komunikacija između uređaja

MAC – *Media Access Control Address*, jedinstveni identifikator dodijeljen kontroleru mrežnog interfejsa za komunikaciju na sloju linka

MD5 – *Message Digest 5*, kriptografski heš algoritam za koji su nađene brojne ranjivosti tako da se ne smatra sigurnim

MIB – *Management Information Base*, baza podataka koja se koristi za upravljanje entitetima u komunikacionoj mreži

MIPnet – *Montenegrin IP Network*, multiservisna mreža kompanije T-Com koja omogućava IP orjentisane usluge

MIPv6 – *Mobile IPv6*, protokol razvijen kao podskup IPv6 za podršku mobilnih veza

MIXP – *Montenegro Internet eXchange Point*, crnogorska tačka razmjene Internet saobraćaja

MME – Mobility Management Entity,

MPLS – *Multiprotocol Label Switching*, tehnika rutiranja dizajnirana da ubrza i oblikuje saobraćajne tokove tako što usmjerava podatke iz jednog mrežnog čvora u sledeći na osnovu kratkih oznaka, umjesto dugih mrežnih adresa

MTA – *Mail Transfer Agent*, softver koji prenosi poruke elektronske pošte sa jednog računara na drugi koristeći SMTP

MTC – *Machine Type Communications*, komunikacija između uređaja

MTU – *Maximum Transmission Unit*, veličina najveće jedinice podatka protokola koja se može prenijeti u jednoj transakciji

NAS – *Network Attached Storage*, server za skladištenje podataka (na nivou fajlova) povezan na računarsku mrežu

NAT – *Network Address Translation*, metod preslikavanja jednog IP adresnog prostora u drugi

NBMA – *Non-Broadcast Multi-Access*, računarska mreža na koju je priključeno više hostova, ali se podaci prenose samo direktno sa jednog računara na drugi

ND – *Neighbor Discovery*, jedan iz skupa Internet protokola koji se koristi sa IPv6

NFS – *Network File System*, mrežni protokol koji se koristi za omogućavanje zajedničkog pristupa fajlovima

NFV – *Network Function Virtualization,* funkcija virtuelizacije mreže

NOC – *Network Operating Center*, nadzorno-operativni centar

NTIA – *National Telecommunications & Information Administration*, agencija Ministarstva trgovine SAD koja služi kao glavni savjetnik predsjednika u oblasti telekomunikacija

NTP – *Network Time Protocol*, mrežni protokol za sinhronizaciju satova između računarskih sistema

OSI – *Open System Interconnection*, referentni model za komunikaciju preko mreže

OSPF – *Open Shortest Path First*, protokol rutiranja u IP mrežama

OSPFv3 – *Open Shortest Path First version 3*, OSPF verzije 3

PE router– *Provider Edge*, ruter između područja jednog mrežnog provajdera i oblasti kojom upravljaju drugi mrežni provajderi

PGW – *Packet Data Network Gateway*, mrežna funkcija za 4G mobilnu mrežu

PKI – *Public Key Infrastructure*, set tehnologija koje pomažu da se zaštiti komunikacija i transakcije putem asimetrične kriptografije

PL – *Payload Length*, 16-bitno polje zaglavlja IPv6 paketa koje definiše dužinu podataka u IP paketu

PS – *Packet Switch*, svič za komutaciju paketa

QoS – *Quality of Service*, opis ili mjerenje ukupnih performansi usluge, naročito performansi koje vide korisnici mreže

RA – *Routing Advertising*, poruke koje ruteri razmjenjuju u svrhu autokonfigurisanja IPv6

RAN – *Radio Access Network*, dio telekomunikacionog sistema koji povezuje pojedinačne uređaje sa drugim djelovima mreže putem radio veza

RANGER – *Routing and Addressing in Networks with Global Enterprise Recursion*, arhitekturni okvir za skalabilno usmjeravanje i adresiranje u mrežama

RFC – *Request for Comments*, tehnički dokument objavljen od strane IETF-a, koji specificira mrežni protokol, funkciju mrežnog protokola ili bilo koju funkciju koja je povezana sa mrežnom komunikacijom

RIP – *Routing Information Protocol*, protokol koji ruteri koriste za razmjenu informacija o topologiji mreže

RIPE – *Réseaux IP Européens*, Evropski regionalni Internet registar, zadužen za dodjelu jedinstvenih IP adresa i AS brojeva u Evropi

RIPng – *Routing Information Protocol Next Generation*, RIP u IPv6 mrežama

RIR – *Regional Internet Registry*, odgovoran je za distribuciju i registraciju adresnog prostora na regionalnom nivou

SA – *Source Address*, 32-bitna adresa čvora koji je inicirao prenos paketa

SAN – *Storage Area Network*, brza specijalizovana mreža koja obezbeđuje pristup skladištu podataka na nivou bloka

SAD – Sjedinjene Američke Države

SDN – *Software Defined Networking*, pristup koji olakšava upravljanje mrežom i omogućava efikasnu programsku konfiguraciju mreže kako bi se poboljšale performanse i nadzor mreže

SEAL – *Subnetwork Encapsulation and Adaptation Layer*, tehnika tunelovanja

SGSN-MME – *Serving GPRS Support Node - Mobility Management Entity*, komponenta GPRS mreže

SGW – *Serving Gateway*, funkcija za 4G mobilnu mrežu

SIIT – *Stateless IP/ICMP Translation*, translacija između formata zaglavlja paketa u IPv6 i IPv4

SLA – *Service Level Agreement*, ugovor između provajdera usluge i krajnjeg korisnika kojim se definiše nivo usluge koji se očekuje od provajdera

SLAAC – *Stateless Address Autoconfiguration*, auto-konfiguracioni mehanizam koji ne zahtijeva ručnu konfiguraciju hostova ni dodatne servere

SMB – *Server Message Block*, mrežni protokol koji se uglavnom koristi za omogućavanje zajedničkog pristupa fajlovima

SMTP – *Simple Mail Transfer Protocol*, protokol aplikativnog nivoa koji omogućava prenos i isporuku elektronske pošte preko Interneta

SNMP – *Simple Network Management Protocol*, protokol za prikupljanje i organizovanje informacija o upravljanim uređajima na IP mrežama

SOCKS – Internet protokol koji razmjenjuje pakete između klijenta i servera preko *proxy* servera

SP – *Service Provider*, provajder usluga

SSH – *Secure Shell*, kriptografski mrežni protokol na nivou aplikacije za zaštićen pristup na daljinu mrežnim čvorovima preko neosigurane mreže

SSL – *Secure Sockets Layer*, kriptografski protokol dizajniran da obezbijedi bezbjednost komunikacije preko računarske mreže

TC – *Traffic Class*, 8-bitno polje zaglavlja IPv6 paketa za označavanje prioriteta paketa

TCP/IP – *Transmission Control Protocol* / *Internet Protocol*, model Internet arhitekture

Teredo – *Tunneling IPv6 over UDP through NATs*, tehnika tunelovanja

TIC – *Tunnel Information and Control*, protokol za tunelovanje

TL – *Total Length*, polje zaglavlja IPv4 paketa u kome se navodi dužina ukupnog IP paketa

TLS – *Transport Layer Security*, kriptografski protokol dizajniran da obezbijedi sigurnost komunikacije preko računarske mreže

TSP - *Tunnel Setup Protocol*, mrežni kontrolni protokol koji se koristi za pregovaranje parametara podešavanja IP tunela

TTL – *Time To Live*, mehanizam koji ograničava životni vijek paketa u mreži (definisan maksimalnim brojem *hop*-ova za prenos IP paketa)

UCG – Univerzitet Crne Gore

UDP – *User Datagram Protocol*, nekonektivni komunikacioni protokol koji se primarno koristi za uspostavljanje veza između aplikacija koje zahtijevaju malo kašnjenje i tolerišu gubitke paketa

UE – *User Equipment*, korisnička oprema

ULA – *Unique Local address*, IPv6 adresa u opsegu fc00::/7 (analogno IPv4 adresiranju u privatnim mrežama)

VET – *Virtual Enterprise Traversal*, apstrakcija za autokonfiguraciju i rad čvorova u poslovnim mrežama

VLAN – *Virtual Local Area Network*, virtualna lokalna mreža

VLAN ID – jedinstveni VLAN identifikator

VLSM – *Variable-Length Subnet Masking*, podjela IP adresnog prostora u hijerarhiju podmreža različitih veličina, čime se omogućava stvaranje podmreža sa različitim brojem hostova bez trošenja velikog broja adresa

VoIP – *Voice over IP*, tehnologija za omogućavanje govornih komunikacija i multimedijalnih sesija preko IP mreža

VPN – *Virtual Private Network*, virtuelna privatna mreža - mrežna tehnologija koja omogućava sigurnu mrežnu konekciju preko javne mreže

WAN – *Wide Area Network*, računarska mreža na širem području