UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

# POSODOBITEV INFORMACIJSKE INFRASTRUKTURE NA OSNOVI PROTOKOLA IPV6, V OMREŽJU VLADNIH ORGANOV NA PRIMERU AGENCIJE RS ZA OKOLJE

Ljubljana, junij 2016 DUŠAN REHBERGER

**IZJAVA O AVTORSTVU**

Podpisani Dušan Rehberger, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom POSODOBITEV RAČUNALNIŠKE (INFORMACIJSKE) INFRASTRUKTURE, NA OSNOVI PROTOKOLA IPV6, V OMREŽJU VLADNIH ORGANOV, NA PRIMERU AGENCIJE RS ZA OKOLJE, pripravljenega v sodelovanju s svetovalko prof. dr. Borka Džonova Jerman Blažič.

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 21.06.2016

Podpis študenta: Dušan Rehberger

# KAZALO

## KAZALO TABEL



## KAZALO SLIK

# UVOD

Sodobnega sveta si brez interneta ne moremo več predstavljati. Število uporabnikov interneta in s tem tudi velikost internetnega omrežja narašča skoraj eksponentno. Poleg klasične računalniške in omrežne opreme (osebni računalniki, strežniki, tiskalniki, usmerjevalniki…) se pojavlja vse več elektronskih naprav (mobilni terminali, video konzole…), ki bi jih želeli vključiti v internetno omrežje.

Danes se v internetnih omrežjih večinoma uporablja omrežni protokol IPv4. Glavna omejitev tega protokola je obseg njegovega naslovnega prostora - maksimalno okoli 4 milijarde gostiteljev na 16,7 milijonih omrežij. Ta prostor se zdi na prvi pogled gromozanski, vendar se zaradi eksplozivne rasti interneta v zadnjem desetletju naglo približuje svojim mejnim vrednostim. Problem premajhnega naslovnega prostora odpravlja naslednja generacija IP protokola, sprva poimenovan IPng (angl. *Internet Protocol Next Generation*). Danes ga imenujemo IP različica 6 ali na kratko IPv6, ob tem pa ne smemo enačiti IPv6 z Internet2. Internet2 je namreč ameriški konzorcij univerz, ki skrbijo za razvoj novih tehnologij in storitev, IPv6 pa je omrežni protokol, oblikovan kot naslednik dosedanjega IP protokola (IPv4). Dejansko je IPv6 ena od omrežnih tehnologij, uporabljena v Internetu2, znotraj njegovega hrbteničnega omrežja Abilene (Murphy & Malone, 2005, str. xxiii).

Ključno vprašanje je, kdaj se je potrebno začeti pripravljati na prehod na IPv6 in na kakšen način ga izvesti. Sam prehod mora biti čim bolj ugoden, tako glede stroškov kot tudi glede samega delovanja omrežja. Lahko čakamo, da uvajanje novega protokola postane nujno ali pa se na prehod pripravljamo postopoma in izkoriščamo tiste prednosti IPv6, ki jih omogoča že sedaj. Vsekakor moramo omogočiti vzajemno delovanje stare in nove infrastrukture.

Namen magistrskega dela je poglobljeno teoretično proučevanje protokola IPv6, njegovega pomena in koristi ter praktična izvedba pilotne postavitve IPv6 omrežja v delovni organizaciji, kjer sem zaposlen. Novi IP protokol bom apliciral na osnovi lastnih izkušenj in znanj, ki jih bom pridobil s proučevanjem strokovne literature. V okviru magistrskega dela želim preveriti, kakšne so možnosti pridobitve IPv6 omrežnega prostora za Agencijo RS za okolje (v nadaljevanju ARSO). Cilj pilotne postavitve IPv6 je tako testirati delovanje protokola IPv6 na obstoječi ARSO strojni opremi, z obstoječimi operacijskimi sistemi in obstoječo programsko opremo ter poiskati najbolj primerno tehnično rešitev za začasno vzajemno delovanje protokola IPv4 in IPv6. Izbrana rešitev bo morala ustrezati vsem tehničnim zahtevam in ostati znotraj meja finančnih sredstev, namenjenih Službi za analitično podporo delovnim procesom. Raziskal bom dejavnike in prepreke uvedbe novega protokola na ARSO ter predstavil, kakšna je dejanska možnost prehoda na IPv6. Tako bo ARSO bolje pripravljen, ko bo prehod zaradi potrebe po večjem omrežnem

prostoru postal neizogiben. Cilj magistrskega dela je tako poglobiti védenje o posodobitvah informacijske infrastrukture na osnovi protokola IPv6 ter združiti lastna spoznanja in znanja tujih avtorjev v zaokroženo celoto.

Pri izvedbi si bom pomagal tako s teoretičnimi kot empiričnimi metodami. Z uporabo deskriptivne metode bom zbral, uredil, ustrezno prikazal in medsebojno primerjal dobljene podatke in informacije. Pomagal si bom tudi z empiričnimi podatki in analizami. Na podlagi lastnih izkušenj in s pomočjo diskusije s strokovnjaki bom izvedel tudi pilotno postavitev IPv6 omrežja.

Magistrsko delo bom razdelil na več tematsko zaokroženih sklopov, ki skupaj tvorijo celoto. Na začetku bom predstavil zgodovino IP protokola, ki je danes nepogrešljiv del interneta. Nato bom predstavil IPv4 protokol z vsemi njegovimi prednostmi in pomanjkljivostmi ter razloge za razvoj novega IP protokola. Podrobneje bom obdelal protokol IPv6. Opisal bom strukturo in vsebino protokola ter predstavil podobnosti z IPv4 in njune medsebojne razlike. Nato bom podrobneje predstavil naslavljanje v protokolu IPv6, ki se pomembno razlikuje od naslavljanja v protokolu IPv4. Sledi opis osnovnega protokola, ki služi za izmenjavo sporočil na ravni mrežnega sloja. Za praktični del izvedbe naloge so pomembni tudi opisani mehanizmi prehoda iz starega IP naslova na novi IP. V zadnjem delu teoretičnega dela bom predstavil plan prehoda s protokola IPv4 na IPv6 na ARSO. Praktični del magistrskega dela zajema rezervacijo IPv6 naslovnega prostora pri enem od ponudnikov v Sloveniji. Sledila bo pilotna postavitev omrežja IPv6 z ustreznimi nastavitvami na usmerjevalniku in na gostiteljskih računalnikih. Uspešnost postavitve bo preverjena z obstoječimi testi, ki so običajno že del vsakega operacijskega sistema. Pilotna postavitev bo služila kot osnova za nadaljnje postopno uvajanje protokola IPv6 na celotnem ARSO omrežju.

# 1 ZGODOVINA INTERNETNE SKLADOVNICE PROTOKOLOV TCP/IP

Običajno na vsako kuverto napišemo prejemnikov naslov preden jo vržemo v poštni nabiralnik. Prav tako mora imeti tudi vsako vozlišče v internetu (usmerjevalnik ali končni sistem) enolično določen naslov. Katerikoli paket, ki potuje med dvema vozliščema mora vsebovati končni naslov, ki usmerjevalniku pove, kam tak paket poslati. Podobno, kot ima poštni servis razdeljene področne kode, morajo biti tudi internet naslovi razdeljeni. Na začetku je to potekalo na podlagi konsenza, toda že nekaj desetletij nazaj je proces postal bolj birokratski (Salus, 2000, str. 1).

Izvor vsega znanja, povezanega z internetom, je niz RFC (Requests for Comment) in IETF (Internet Engineering Task Force) osnutkov (angl. *drafts*). Obstaja okoli 2800 RFC-jev in mnogo osnutkov, toda samo nekaj ljudi pozna zgodovino in evolucijo interneta, čeprav je

poznavanje zgodovine nujno potrebno, če želimo bolje razumeti, kaj nam prinaša prihodnost. V RFC 1 (april 1969) je Steve Crocker (takrat diplomiranec, nazadnje pa podpredsednik Cybercash-a) prikazal shemo, ki je dodelila 5 bitov za naslovni prostor. To je bilo dovolj za 32 naslovov. Septembra leta 1969 je bil v laboratoriju Leonard Kleinrock's v UCLA instaliran IMP #1 (Interface Message Processor, Honeywell 516, prvi delujoč usmerjevalnik). Naslovni prostor je obsegal 6 bitov (63 naslovov, ker naslov 0 ni bil uporabljen). Leta 1972 je postalo jasno, da je to premalo. Naslovni prostor so zato povečali na 8 bitov (255 naslovov). Dejansko je ARPANET imela 63 gostiteljev že v januarju 1976. To pa je bilo že veliko glede na to, da so bili vsi naslovi vpisani v tabeli host.txt (usmerjevalna tabela), ki je morala biti posredovana vsaki lokaciji. V avgustu 1983 je bilo 213 gostiteljev, s čimer je bila dosežena meja 8-bitnega naslovnega prostora (Salus, 2000, str. 1).

Decembra 1974 sta Vinton Cerf (podpredsednik in šef Internet Evangelist pri Google Inc.) in Bob Kahn (predsednik CNRI) objavila originalno verzijo TCP protokola (Transmission Control Protocol, RFC 675). Na tej podlagi je januarja 1980 Jon Postel definiral IP (Internet protocol, RFC 760, 1980). To je povečalo naslovni prostor do 32 bitov. Toda struktura ARPANET je bila brezrazredna (angl. *classless*). Hierarhična distribuirana baza, kot jo poznamo danes, je nastala šele z Millsovim konceptom Domain Naming System (DNS, RFC 799, 1981). V praksi jo je prvi uporabil Paul Mockapetris (RFC 882 in 883, 1983). Mockapetrisovo izvedbo so poimenovali Jeeves, trenutno pa je najbolj uporabljena izvedba BIND (Berkeley Internet Name Domain), ki jo je napisal Kevin Dunlap. Tako smo dobili 32-bitni naslovni prostor in različne hierarhične razrede omrežij: A, B, C, D in E. Imamo 128 A razredov. Vsak A razred ima lahko 16.777.216 unikatnih naslovov. Obstaja še 16.384 B razredov s 65.536 naslovi. Naslovov C razreda je 2.097.192 ter okoli 268 milijonov grup razreda D. Naslovi iz razreda E niso nikoli bili na razpolago za splošno uporabo (Salus, 2000, str. 1-2).

Uporabljajoč IP shemo naslavljanja, DNS omogoča naslove za okoli 4 milijarde gostiteljev na 16,7 milijonih omrežij. To se zdi izredno velik naslovni prostor. Toda širitev interneta je bila v zadnjih letih eksplozivna. Avgusta 1990, na srečanju IETF v Vancouver-ju, so Frank Solensky, Phill Gross in Sue Hares napovedali, da bo s takšnim tempom zmanjkalo naslovnega prostora v B razredu že marca 1994. Brezrazredno usmerjanje med domenami (angl. *Classless Inter-Domain Routing* - v nadaljevanju CIDR) je z RFC 1518 in 1519 leta 1993 uvedel izboljšave pri nadgradljivosti usmerjanja kot tudi pri uporabi naslovnega prostora v medmrežju. CIDR omogoča boljše ujemanje med naslovnimi zahtevami in naslovnim razporedom. Odprava pojma omrežnih razredov omogoča razširitev področja s hierarhičnim dodeljevanjem omrežnega naslova. To se odraža v naraščanju dosega hierarhičnega usmerjanja, ki pomeni tudi izboljšanje lastnosti omrežnega usmerjevalnega sistema. CIDR predstavlja blažilo, ki omogoča nadaljnje delovanje interneta, medtem ko se njegova rast nadaljuje. Kljub temu so na IETF srečanju v Torontu julija 1994 na podlagi takratne statistike dodeljevanja IP naslovov napovedali, da bo IPv4 naslovni prostor

izčrpan nekje med leti 2005 in 2011. Z različnimi translacijskimi mehanizmi se napoved zaenkrat zamika za nekaj let v prihodnost, vendar je izčrpanje naslovov kljub temu neizbežno. Na IETF srečanju v Torontu so ustanovili posebno skupino za IPng (Internet Protocol Next Generation) ali IPv6, ki sta jo vodila Scott Bradner in Allison Mankin. Priporočila te skupine so bila objavljena v oktobru 1994 in so služila kot osnova za diskusijo na srečanju IETF decembra 1994 (Salus, 2000, str. 2-3).

IPv6 omogoča 128-bitno naslavljanje. To je velikanska številka, ki je primerljiva z ocenjenim številom molekul v vesolju. Pri uvajanju IPv6 protokola je še precej odprtih vprašanj in nejasnosti, kot je na primer prehod iz 32-bitnega naslavljanja na 128-bitno naslavljanje. Preštevilčenje bo potrebno izvesti na zelo velikem številu naslovov, ki so že v uporabi. Nekatere organizacije se bodo tega lotile zaradi učinkovitejše uporabe naslovnega prostora. Eno izmed možnosti predstavlja prevajanje omrežnega naslova (angl. *Network Addres Translation* - v nadaljevanju NAT), ki upočasni trošenje naslovnega prostora. Take organizacije imajo en zunanji naslov in mnogo privatnih naslovov (npr. omrežje 10) v internem omrežju. Glede na to bi lahko sedaj 128 bitov razdelili na 64 bitov za notranja in 64 bitov za zunanja omrežja. Kljub vsemu pa pomanjkanje prostora ni edina sila, ki nas žene k uvedbi IPv6. Naslovni prostor, ki ga omogoča IPv6 je zares gromozanski, vendar to ni vse. Veliko število ostalih funkcij bo razvitih, ko se bodo za to pokazale potrebe in sicer: bolj nadgradljiva arhitektura omrežja, zahtevana varnost in celovitost podatkov, dodatna polja za kakovost storitve (QoS), samokonfiguracija ter bolj zmogljivo usmerjanje podatkov na nivoju globalnega hrbteničnega omrežja (Salus, 2000, str. 2-3).

V nekaj naslednjih letih se bodo konvencionalni računalniki na internetu združili z različnimi napravami, kot so dlančniki, hibridni mobilni telefoni, pametne zaključene naprave z vgrajenim brskalnikom, vgrajene mrežne komponente, v širok izbor različnih naprav, od kopirnega stroja do kuhinjskih aparatov. Nekatere od teh naprav bodo zahtevale IP naslov in bodo potrošniško organizirane, npr. avtomat za kavo, pralni stroj, itd. 128-bitni naslovni prostor bo omogočal podjetjem, da razvijejo veliko novih namiznih, mobilnih in vgrajenih mrežnih naprav na stroškovno učinkovit in obvladljiv način. Nadalje IPv6 samokonfiguracija omogoča dinamično dodeljevanje naslovov, brez nepredvidenih administracijskih stroškov zaradi stalnega naraščanja potreb dodeljevanja, spreminjanja ali odvzemanja IP naslovov. Poslovne zahteve za IPv6 bodo vodene s strani aplikacij končnega uporabnika. IPv6 ima prednosti tako pri usmerjanju podatkov kot tudi direktne prednosti za aplikacije pri končnem uporabniku. Aplikacije lahko uporabljajo vgrajeno IPv6 enkripcijo in avtentikacijo, ki je bistven del IP skladovnice. Za mobilne uporabnike in organizacije predstavlja komponenta za avtomatsko konfiguracijo učinkovito dodeljevanje naslovov brez čakanja in brez stroškov, ki so povezani z ročnim dodeljevanjem naslovov. IPv6 zadeva tako končne uporabnike kot poslovne zadeve. Obdobje od leta 1981 do leta 1983 - pretvorba v DNS – je bila boleča za vse vpletene. Prehod iz IPv4 na IPv6 bo morda še bolj boleč, glavna težava pa je v velikem številu shem, ki jih bo potrebno spremeniti (Salus, 2000, 3-4).

# 2 UPORABLJENI PROTOKOLI IN TEHNOLOGIJE DANAŠNJEGA INTERNETA

## 2.1 Značilnosti in omejitve protokola IPv4

Naslovni prostor IPv4 protokola je 32-bitni. Naslov je običajno zapisan v obliki 32-bitnega števila, ki je razdeljeno na 4 oktete in med seboj ločeno s piko: a.b.c.d. Vsak a, b, c, d predstavlja decimalno številko v razponu od 0-255. Torej je naslovni prostor od 0.0.0.0 do 255.255.255.255. To pomeni, da je zgornja meja 4,294.976.296 ali okoli 4 milijarde naslovov. Ker je naslov sestavljen iz samih številk, se običajno uporablja namesto izraza IP naslov kar izraz IP številka (Murphy & Malone, 2005, str. 3). Naslovni prostor je bil sprva razdeljen na fiksne kose, imenovane razredi, ki so imeli poseben pomen. Razredi A, B in C so najbolj poznane delitve omrežnega območja. En razred A je imel 8 bitov za omrežje in 24 bitov za gostiteljski naslov, razred B je imel 16 bitov za omrežje in 16 bitov za gostiteljski naslov in razred C je imel 24 bitov za omrežni naslov (Murphy & Malone, 2005, str. 3-4). Za bolj nazorno razumevanje je v Tabeli 1 prikazan tradicionalni razpon IPv4 naslovnega prostora.

*Tabela 1: Tradicionalni razpon IPv4 naslovnega prostora*

| Razred | Območje | Maska omrežja |
|---|---|---|
| A | 0.0.0.0-127.255.255.255 | 255.0.0.0 |
| B | 128.0.0.0-191.255.255.255 | 255.255.0.0 |
| C | 192.0.0.0-223.255.255.255 | 255.255.255.0 |
| D | 224.0.0.0-239.255.255.255 | multicast |
| F | 240.0.0.0-255.255.255.255 | rezervirano |

*Vir: N. R. Murphy & D. Malone, IPv6 Network Administration, 2005, str. 4, tabela 1-1.*

V vsakem območju razreda A, B, C je določen del prostora, označen kot »privatni« naslovni prostor. Tega uporabimo takrat, ko potrebujemo IP omrežje, ni pa potrebno, da je naš IP naslov viden v internetu. Dobro poznani naslovi so 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 in 192.168.0.0-192.168.255.255. Trenutno so opisani v RFC 1918. Seveda to niso edini rezervirani naslovi. V RFC 3330 dobimo povzetek vseh rezerviranih naslovov (Murphy & Malone, 2005, str. 4).

IPv4 omogoča tudi razpršeno oddajanje. V začetku je bilo nekoliko zmede glede tega, kateri naslovi znotraj območja simbolizirajo razpršeni naslov. V praksi je sedaj tako, da vse enice v gostiteljskem delu pomenijo, da gre za naslov za razpršeno oddajanje, same ničle pa se smatrajo za omrežni naslov (Murphy & Malone, 2005, str. 4).

### 2.1.1 Brezrazredno usmerjanje med domenami

Brezrazredno usmerjanje med domenami (angl. *Classless Inter-Domain Routing* - v nadaljevanju CIDR) je ovrgel trditev, da lahko določimo velikost omrežja, če vemo, v kateri razred omrežje spada (A, B ali C). Glavna ideja je bila v tem, da se odpravi 8-bitna meja, ki med seboj ločuje mrežni in gostiteljski del naslovnega prostora. S CIDR-om meja med omrežnim in gostiteljskim delom lahko pade na katerikoli bit v naslovu; omrežje je lahko opisano s samimi ničlami. Mrežnemu naslovu sledi številka, ki pomeni število bitov, ki jih bo imel mrežni del IP naslova. Na primer, stari naslov 10.0.0.0 razreda A lahko napišemo kot 10.0.0.0/8, kjer 8 pove število bitov v omrežnem delu naslova. Razred C omrežja 192.168.1.0, ki je bil prej najmanjše možno omrežje, je sedaj lahko razdeljeno na podomrežja. Na primer, lahko je razdeljeno na 4 omrežja: 192.168.1/26, 192.168.1.64/26, 192.168.1.128/26 in 192.168.1.192/26. Številka na desni strani lahko vsebuje vrednosti od 32 (pomeni samo en gostitelj) do 0 (pomeni vsak možen gostitelj ali »ujemanje kjerkoli«). Pomembno je, da vsako pomanjšanje te številke za eno podvoji velikost ustreznega omrežja. Na primer, 10.0.0.0/23 omrežje je dvakrat tako veliko kot 10.0.0.0/24 in še vsebuje to omrežje. To pomeni, da je zbirka večih omrežij pogosto lahko predstavljena z enim CIDR blokom, namesto s točno določeno listo omrežnih kandidatov. Torej je več sosednjih omrežij lahko agregiranih v en CIDR blok, kar omogoča bolj zmogljiv opis v usmerjevalnih protokolov, dostopnih listah in podobno (Murphy & Malone, 2005, str. 4-5).

Najmanjše normalno omrežje, ki je lahko razporejeno z uporabo CIDR, je /30, ker so same ničle in same enice rezervirane, moramo pa imeti prostor za vsaj enega gostitelja. To pomeni, da omrežja, ki so med seboj povezana točka-točka (angl. *point-to-point*), običajno potrošijo 4 IPv4 naslove (Murphy & Malone, 2005, str. 5).

CIDR obravnava dve pomembni težavi, povezani z dodeljevanjem IPv4 naslovov (Murphy & Malone, 2005, str. 5):

- omogoča manjše dodeljevanje IP naslovov, s čimer je upočasnjena hitrost porabe naslovov;
- omogoča agregacijo (angl. *aggregation*), tj. združevanje več sosednjih omrežij v enotno predstavitev, zaradi česar je usmerjanje bolj zmogljivo (na hrbteničnem omrežju, kjer privzete usmerjevalne poti sploh niso možne, pa je agregacija tista, ki omogoča usmerjanje).

CIDR-u je uspelo preprečiti, da bi razreden (angl. *classful*) IPv4 počil po šivih, vendar zaradi svojega načina delovanja ni najbolj učinkovit (Murphy & Malone, 2005, str. 5).

### 2.1.2 Prevajanje omrežnega naslova

Prevajanje omrežnega naslova (angl. *Network Addres Translation* - v nadaljevanju NAT) je tehnika, ki se je pojavila kot odgovor na pomanjkanje globalnih usmerjevalnih IPv4 naslovov. Dovoljuje, da se preko posameznega IP naslova poveže veliko število gostiteljev. Običajna uporaba vključuje omrežje gostiteljev, ki uporabljajo naslov iz območja privatnih naslovov. Promet se usmerja k prehodu (angl. *gateway*) ali posredovalnemu strežniku (angl. *proxy*), s privatnim naslovom na notranji strani omrežja in s pravim IP naslovom v internet omrežju. Prehod za ves odhajajoči promet zamenja privatni IP naslov z njegovim javnim IP naslovom ter uporabi številke vrat (angl. *port*), da si zapomni privatni IP naslov, na katerega bodo lahko poslani odgovori. Za prihajajoči promet prehod poišče številko vrat v tabeli, originalen privatni IP naslov je določen in paket je poslan naprej gostitelju v privatno omrežje. Zaradi ekonomičnosti IPv4 naslovov je NAT postal dokazano zelo popularen pri domačih uporabnikih in v manjših podjetjih. NAT omogoča povezavo celotne organizacije v internet z uporabo ene cenovno ugodne klicne (angl. *dialup*) povezave (Murphy & Malone, 2005, str. 5-6).

Posamezne organizacije uporabljajo NAT kot zaščito v primeru potrebe po spreminjanju IP naslovov. Preštevilčenje omrežja je potrebno v primerih, ko se spremeni ponudnik (ISP) ali v primeru, ko organizacija uporablja svoj naslovni prostor neprimerno. Preštevilčenje v IPv4 omrežje je preprost proces, z uporabo privatnih naslovov pa je preštevilčenje še lažje. V tem primeru privatni naslovi lahko ostanejo enaki. Poleg prednosti pa ima NAT tudi nekaj pomanjkljivosti. Nedvomno je zmanjšal zahteve po IPv4 naslovih, toda določeni protokoli ne morejo delovati preko NAT brez posebnih postopkov. To so predvsem tisti, ki imajo vtisnjen naslov končne točke znotraj protokola. Eden takih protokolov je tudi FTP protokol. NAT je tudi kompleksnejši in izvaja CPU zahtevnejše operacije, v nasprotju s preprostim razpošiljanjem prometa. Rast internetnega prometa je hitrejša kot povečevanje CPU hitrosti in zato je cena izvajanja NAT pri visokih hitrostih višja kot cena hitrejših (toda »neumnejših«) usmerjevalnikov. Omrežje, ki se zanaša na NAT, bo mogoče ugotovilo, da je njegova rast omejena - ne sicer s ceno kapacitete omrežja, temveč s ceno NAT enote. Poleg tega NAT tudi ovira gostitelje na internetu pri vzpostavitvi povezave v privatno omrežje. Nekateri smatrajo to kot prednost, ker prehod lahko deluje tudi kot preprost požarni zid, spet drugi trdijo, da gre za kršitev osnovnega principa delovanja interneta, ki sloni na ideji, da mora biti vsakemu gostitelju omogočeno komunicirati z vsakim gostiteljem (angl. *end-to-end principle*; Murphy & Malone, 2005, str. 6).

### 2.1.3 Varnost

IPv4 je bil načrtovan kot omrežje relativno zaupanja vrednih uporabnikov, kjer naj bi bila omrežna infrastruktura sorazmerno varna ter informacije, ki se bodo pretakale, relativno javne, zato se takrat ni zdelo pomembno dodajati varnostnega mehanizma (avtentikacije) v

sam protokol, toda s časom se je način uporabe interneta korenito spremenil. Ogromno število uporabnikov interneta preprosto pomeni, da ni možno zaupati vsem. Omrežna infrastruktura omogoča sodelovanje med velikim številom privatnih in javnih organizacij s popolnoma različnim poslovanjem. Podatki, ki se prenašajo po internetu, so pogosto komercialno, finančno ali osebno občutljivi. Gledano z varnostne perspektive je IPv4 zelo oddaljen od varnosti (Murphy & Malone, 2005, str. 7).

Varnost poskuša zagotavljati preko aplikacijskega varnostnega nivoja (enkratna gesla, SSH, TSIG...) ali z upravljanjem s protokoli (filtriranje paketov in požarni zid). Te rešitve imajo pogosto karakteristike t.i. ad-hoc rešitev in temu primerne omejitve, npr. različne upravljalske sheme, različne nivoje varnosti, podvojene napore. SSL je najbolj uspešen kompromis, ki je bil narejen na ta način. Uporabimo ga lahko v različnih situacijah, poleg uporabe v HTTP, za katerega je bil prvotno zamišljen (Murphy & Malone, 2005, str. 7).

### 2.1.4 Sistem za domenska imena

Z varnostnega vidika je sistem za domenska imena (angl. *Domain Name System* - v nadaljevanju DNS) pri IPv4 zelo občutljiv. Večino zahtev gre preko protokola uporabniškega datagrama (angl. *User Datagram Protocol* – v nadaljevanju UDP). UDP je protokol, ki je enostaven in zelo malo obremenjuje centralno procesno enoto (angl. *Central Processing Unit* – v nadaljevanju CPU). Ima pa to slabo lastnost, da je vanj možno posegati na dokaj enostaven način. Polja protokola so v mnogo primerih lahko uganljiva. Tam kjer niso, pa se uporablja tehnika poplavljanja. Za popolnitev se uporabi dodatne pakete in eden izmed njih bi lahko zamenjal dejanski paket. DNS ima sama po sebi nekaj dodatnih zaščit, ki niso veliko vredne. Da ponaredimo odgovor na DNS zahtevo, moramo pravilno uganiti začasno številko vrat in ID povpraševanja. V primeru DNS je številke vrat pogosto enostavno določiti in nekatere DNS izvedbe proizvajajo lahko uganljive ID številke povpraševanja (Murphy & Malone, 2005, str. 7).

Če lahko potvorimo DNS odgovor, potem je možno ljudi usmeriti k napačnemu gostitelju. Če je potvorba dovolj prepričevalna, potem so lahko nekatere e-komercialne lokacije preusmerjene na kontrolirano napadalčevo internetno stran. Na ta način je zelo enostavno priti do gesel ali številk kreditnih kartic. V primeru svetovnega spleta (angl. *web*) je nekaj zaščite možne z uporabo SSL protokola, toda če se izdaja za poštni strežnik preden bi opazili, da gre pošta na napačen cilj, bi bilo že prepozno (Murphy & Malone, 2005, str. 8).

### 2.1.5 Protokol za prepoznavanje naslovov

IPv4 ethernet omrežje zahteva od mehanizma za vozlišča, da odkrije, kateri naslov na povezovalnem sloju se ujema z naslovom na sloju 3 (t.i. mrežni sloj OSI modela) oz.

povedano drugače, kako naj naprava poišče naslov povezovalnega sloja za dodeljen IP naslov na omrežju. Za veliko večino običajnih omrežij je to narejeno z uporabo protokola za prepoznavanje naslovov (angl. *Address Resolution Protocol* – v nadaljevanju ARP), ki je definiran v RFC 826 (Murphy & Malone, 2005, str. 9).

Protokol deluje na naslednji način: Gostitelji vzdržujejo tabelo naslovov povezovalnega sloja, ki se ujemajo z IPv4 naslovi. Kadar se pojavi potreba po pošiljanju paketa, gostitelj preveri to tabelo in uporabi naslov povezovalnega sloja, če je prisotna. Če ni prisotna, gostitelj razpršeno pošlje ARP zahtevo s sporočilom »Tukaj je moj IP naslov in naslov povezovalnega sloja; kdo pozna naslov povezovalnega sloja za X?« Od ciljnega gostitelja se pričakuje, da bo oblikoval odgovor in ga poslal prosilcu. Upoštevati je potrebno, da je ARP zahteva razpršeno sporočilo in vsebuje informacijo, ki je potrebna, da se v tabeli oblikuje vnos za zahtevanega gostitelja. To omogoča, da je odgovor poslan brez izdajanja nekaj nadaljnjih ARP zahtev (Murphy & Malone, 2005, str. 9).

ARP deluje zelo dobro, ima pa pomanjkljivosti glede varnosti (Murphy & Malone, 2005, str. 9):

- Ko dobimo ARP odgovor, nimamo nobene zagotovitve, da je zares prišel od pravega sistema. Vsak, ki je na istem mediju, lahko potvori odgovor, če se tako odloči. Ni enostavnega mehanizma, ki bi to preprečil. Izkušen napadalec, ki ima dostop do ključne naprave, lahko izvede DoS napad ali kako drugače onemogoči mrežni vmesnik na tej napravi. Nato lahko postavi virtualni naslov ali alias na drugi napravi in ARP bo preusmeril novo povezavo na nadomestno napravo. To tehniko pogosto imenujemo ARP zastrupljanje. Če napadalec na ta način zamenja ključne strežnike na infrastrukturi, kot so DNS ali posredovalni (angl. *proxy*) strežnik, kar je popolnoma možno, lahko začne uporabljati to oporišče za pridobivanje dodatnih avtentikacij, kot so uporabniška imena in gesla.
- Na mnogih sistemih je možno določiti mapiranje IP naslovov iz MAC naslovov, ki so vpisani v konfiguracijski datoteki. S tem smo nekoliko ublažili efekt zastrupljanja. Seveda pa je taka datoteka zelo nefleksibilna in lahko povzroča probleme, zlasti če se pozabi, da so stari MAC naslovi zapečeni na mnogih sistemih znotraj omrežja.

### 2.1.6 Razpršeno oddajanje proti večvrstnemu oddajanju

ARP je protokol razpršenega oddajanja (angl. *broadcast*). To pomeni, da gredo njegove transakcije po celem omrežju. V vsakem trenutku, ko gostitelj dobi broadcast, mora procesirati paket – celo, če paket ni namenjen temu gostitelju. To lahko povzroči ogromno količino podatkov na ploskem (angl. *flat*) ali slabo načrtovanem omrežju (Murphy & Malone, 2005, str. 10).

Večvrstno oddajanje (angl. *multicast*) je v celoti bolj smiseln način sočasne dostave podatkov več gostiteljem. Multicast omogoča, da se naslovi gostiteljev grupirajo v poseben tip omrežnega prometa, kar omogoča, da se promet pošlje samo zainteresiranim skupinam gostiteljev, ne da bi pri tem motili ostale nezainteresirane gostitelje. Žal se multicast ni nikoli zares uporabljal na omrežju IPv4, čeprav je uporaben in dobro načrtovan. Za to obstaja več različnih vzrokov (Murphy & Malone, 2005, str. 10):

- multicast ni nastavljen kot privzet;
- vzame precej časa za konfiguracijo;
- večina ciljnih aplikacij pri multicastingu vključuje sodelovanje več upravljanj.

### 2.1.7 Kakovost podatkovnega prenosa

Kakovost podatkovnega prenosa (angl. *Quality of Service* - v nadaljevanju QoS) se sklicuje na sposobnost, ki zagotavlja, da bo poslani promet pravočasno dospel na določeno mesto. Eden od prvih ukrepov, ki je zagotavljal določen nivo QoS v omrežju IPv4, je bilo polje Vrsta storitve (angl. *Type of Service*) v glavi IP. To polje je vključeno v definiciji IP v RFC 791, ki je nadalje razjasnjen v RFC 1349. V tem modelu IPv4 glava vsebuje polje, ki je nastavljeno na posebno vrednost glede na to, kakšno obdelavo želi paket od usmerjevalnika (Murphy & Malone, 2005, str. 10).

Vloženega je bilo veliko truda v boljše prileganje lastnosti. Veliko dela je bilo vloženega v načrtovanje ogrodij (angl. *frameworks*), kot sta DiffServ (RFC 2475) in IntServ (RFC 1633) ter v protokole, kot so RSVP (RFC 2205) za delo s QoS. Popolnoma nejasno pa je, kdaj bomo videli široko uporabo teh mehanizmov, saj zahtevajo veliko sodelovanja med omrežji. Nekatere raziskave so pokazale, da je cenejše zakupiti več prostora, kot pa trošiti čas in denar za opremo ter ugotavljati, kateri paket se je izgubil. Kakorkoli, dobro oblikovan mehanizem, ki bo zagotavljal QoS, bo imel nedvomno ogromno vrednost za IP uporabnike v prihodnosti (Murphy & Malone, 2005, str. 10-11).

### 2.1.8 Usmerjanje

Mirno lahko rečemo, da je internetna infrastruktura za usmerjanje omrežnega prometa presegla vsa pričakovanja in še vedno deluje zelo dobro. V vsakem lokalnem omrežju, ki je povezano z drugim omrežjem, se nahaja usmerjevalnik (angl. *router*). V splošnem lahko rečemo, da je usmerjevalnik poseben kos strojne opreme, ki posamezna omrežja povezuje med seboj. Glavna naloga usmerjevalnika je, da poveže med seboj dva ali več omrežij ter poskrbi za pravilen pretok informacij med omrežji. Na usmerjevalniku tečejo usmerjevalni protokoli, ki poskrbijo, da pretok informacij poteka zanesljivo, hitro in po najboljši možni poti (Murphy & Malone, 2005, str. 11).

### 2.1.9 Interni usmerjevalni protokoli

Routing Information Protocol (v nadaljevanju RIP) je eden izmed najbolj trpežnih usmerjevalnih protokolov. Gre za relativno star protokol, ki je bil prvotno izdelan za PUP (Xerox PARC Universal Protocol, leta 1980) in je bil uporabljen za XNS (leta 1981). Narejen je bil za uporabo v malih heterogenih omrežjih. Predstavlja klasičen usmerjevalni protokol na osnovi vektorja razdalje (angl. *distance vector*). Kot metriko za izbiro poti uporablja število skokov (angl. *hop count*). Največje število skokov je 15. Za posodabljanje uporablja razpršeno oddajanje (angl. *broadcast*) na vsakih 30 sekund. Sposoben je uravnotežiti maksimalno 6 poti. Privzeta (angl. *default*) nastavitev je 4 (Murphy & Malone, 2005, str. 11).

Sodobnejša različica RIP protokola je RIPv2. Razlike med RIPv1 in RIPv2 usmerjevalnima protokoloma prikazuje Tabela 2.

*Tabela 2: Primerjava usmerjevalnih protokolov RIPv1 in RIPv2*

| **Karakteristike** | **RIPv1** | **RIPv2** |
|---|---|---|
| Usmerjevalni protokol | razredni | brezrazredni |
| Podpira VLSM | ne | da |
| Pošilja skupno masko omrežja | ne | da |
| Naslavljanje | broadcast | multicast |
| Definiran | RFC 1058 | RFCs 1721, 1722 in 2453 |
| Podpira ročni povzetek poti | ne | da |
| Podpira avtentikacijo | ne | da |

*Vir: S. McQuerry, Interconnecting Cisco Network Devices, 2008, str. 402, tabela 5-7.*

### 2.1.10 Mejni usmerjevalni protokol

Mejni usmerjevalni protokol (angl. *Border Gateway Protocol* - v nadaljevanju BGP) je vektorski usmerjevalni protokol, zato ga ne moremo uporabljati za prenos informacij o zasedenosti omrežja (ang. *traffic engineering* – v nadaljevanju TE). BGP prenaša samo informacijo o dosegljivosti usmerjevalnikov. To pomeni, da določi pot, po kateri bomo prišli do nekega vozlišča, ne pove pa nam ničesar o zasedenosti in hitrosti linije do tega vozlišča. Za bolj funkcionalno medpodročno usmerjanje nekateri ponudniki kombinirajo BGP protokol z IGP protokoli, predvsem v kombinaciji z OSPF usmerjevalnim protokolom.

V tem primeru je BGP sistemski medavtonomni usmerjevalni protokol, ki oskrbi BGP vozlišča z informacijo o celotnem ponudnikovem omrežju. OSPF pa je IGP usmerjevalni protokol, ki teče znotraj vsakega področja in širi informacijo o sposobnostih (angl. *Link*

*State Traffic Engineering*) posamezne povezave znotraj področja skozi celotno področje. Ta kombinacija ni primerna tam, kjer je omrežje razdeljeno na zelo veliko število področij, in sicer zato, ker je tu za optimalno usmerjanje prometa potrebno zelo veliko preračunavanja, ki zahteva veliko porabo virov (CPU).

Pri uporabi BGP protokola na omrežju IPv4 se pojavlja kritičen problem - naraščanje velikosti usmerjevalnih tabel, posebno rast večdomnih sistemov in rast omrežnih lokacij. Glede na trenutni usmerjevalni model imajo končne lokacije na izbiro dvoje: lahko dobijo od dobavitelja neodvisen naslovni prostor in s tem številko novega avtonomnega sistema (AS) ali pa dobijo agregiran dobaviteljev naslovni prostor. Naslovni prostor neodvisnega ponudnika (angl. *Provider Independent* – v nadaljevanju PI) je dodeljen končnim organizacijam in se ne spremeni v primerih, ko organizacije zamenjajo ponudnika (ISP). Agregiran ponudnikov (angl. *Provider Aggregate* – v nadaljevanju PA) naslovni prostor je dobil iz skupine naslovov, ki pripadajo ponudniku (Murphy & Malone, 2005, str. 12).

Ne preseneča dejstvo, da si veliko večjih organizacij prizadeva pridobiti PI prostor. Za to imajo organizacije več motivov. Morda je najpomembnejši ta, da v primeru zamenjave ponudnika ni potrebno preštevilčenje omrežnih naslovov. Slednje tudi nekaj stane, saj predstavlja še en dodaten vnos v globalno usmerjevalno tabelo (Murphy & Malone, 2005, str. 12).

### 2.1.11 Povzetek

IPv4 ima precej pomanjkljivosti. Nekatere je mogoče zaobiti, drugih pač ne. Nove aplikacije bodo še bolj izpostavile pomanjkljivosti protokola IPv4 (Murphy & Malone, 2005, str. 13), spremembe pa bodo tako počasi neizogibne.

## 2.2 Prednosti protokola IPv4

V nadaljevanju je opisanih šest poglavitnih prednosti protokola IPv4 – preprostost, prožnost, razširljivost, fleksibilnost, samokonfiguracija in razteznost.

### 2.2.1 Preprostost

Ta prvi element je najbolj upoštevanja vreden. Preprostejša, kot je neka stvar, lažje jo je razumeti, lažje kontrolirati, hitreje deluje in enostavnejša je njena nadgradnja. Če gledamo na takšen način, potem se zdi enostavnost v zasnovi samega protokola samoumevno merilo in težko bi našli koga, ki bi lahko zagovarjal nasprotno. IPv4 je bil že ob nastanku znatno enostavnejši kot njegova konkurenca – OSI protokoli (Murphy & Malone, 2005, str. 14).

### 2.2.2 Prožnost

Ko govorimo o prožnosti, imamo v mislih dvoje (Murphy & Malone, 2005, str. 14):

- Prvič, upoštevamo običajno omrežje. V vsakem trenutku se lahko na omrežju pojavijo različni škodljivi pogoji. Ti pogoji so lahko okoljski, prirojeni ali kakšni drugi. Ne glede na to IPv4 pogosto lahko nadaljuje z delom. Kos je številnim težavam, kot so mrežno zasičenje, napake na linijah, spominske preobremenitve in drugo.
- Drugič, specifikacija za IPv4 je napisana na takšen način, da dopušča pametno skladno definicijo, ki je lahko izvršena v znanem času, z določenim številom ljudi, za omejeno količino denarja. Nimajo vsi mrežni standardi tako posrečene specifikacije. To je resničen dokaz čvrstosti IPv4, saj je v sklad vgrajen neverjeten seznam računalniške opreme, posebno v vgrajene sisteme (angl. *embedded systems*). To so majhne naprave, ki imajo komaj en kilobajt in jih je nekdo s težavo vrinil v polno IPv4 skladovnico. Težava vgradnjih sistemov je v tem, da jih v primeru pojave napak na sistemu običajno ni možno enostavno zamenjati, zato morajo biti za te sisteme specifikacije še posebej jasno podane.

### 2.2.3 Razširljivost

IPv4 ima čedalje več težav, toda internet deluje nenavadno dobro za globalno omrežje z več sto tisoč povezanimi organizacijami. Razlogi za to so delno administrativni in delno tehnični. S tehničnega vidika lahko izpostavimo distribuirano naravo DNS, CIDR naslovno arhitekturo in neodvisno strojno opremo. To so pomembne lastnosti, ki so omogočile, da je internet z uporabo IPv4 zrasel do trenutne velikosti. Ob dejstvu, da lahko IPv4 omrežje teče neodvisno od organizacije, s skupnim sodelovanjem z mejnimi omrežji, postaja problem centralne administracije ozko grlo pri širitvi omrežja. Dejansko je to rezultat tega, da je internet razdeljen v veliko različnih usmerjevalnih domen, imenovanih avtonomni sistemi (angl. *autonomous systems*). Uporaba BGP pomeni, da se vsako omrežje lahko izogne temu, da bi moralo poznati interne podrobnosti vsakega drugega omrežja (Murphy & Malone, 2005, str. 15-16).

### 2.2.4 Fleksibilnost

IPv4 je prilagodljiv, saj se zna prilagoditi problemom, ki nastajajo. CIDR je povečal donos danega dela naslovnega prostora, NAT je zmanjšal povpraševanje po naslovnem prostoru, BGP pa se je razvil za prilagajanje potreb usmerjanja omrežja (Murphy & Malone, 2005, str. 16).

### 2.2.5 Samokonfiguracija

V začetku uporabe IPv4 je bila (re)konfiguracija gostiteljev nekaj, kar je zahtevalo poseg veščega operaterja. Še v zgodnjih dneh interneta so morali končni uporabniki vnesti IP naslov in ostale konfiguracijske podrobnosti ročno. To je bilo v začetku še nekako sprejemljivo. Ko pa so se na internet priključili tehnično manj vešči ljudje, je avtomatska konfiguracija postala nujna. Rekonfiguracija gostitelja je še vedno lahko težavna v primerih, ko imamo isti naslov dalj časa in se ta potem zapiše v različne konfiguracijske datoteke, na kar pozabimo (Murphy & Malone, 2005, str. 16).

Samokonfiguracijo omogočata dva glavna protokola; DHCP za podjetja in PPP za klicne dostope. Ta dva protokola sta veliko pripomogla k dvigu uporabe interneta na raven, kot jo imamo danes. DHCP pomaga pri centraliziranju IP detajlov omrežja, kar pomeni, da končnemu uporabniku ni potrebno ročno vnesti nobenih mrežnih nastavitev. PPP in njegovi bratranci, PPPoE in PPPoA, so olajšali potrošniški ISP. Končni uporabniki morajo za delovanje ustrezne konfiguracije vpisati samo svoje uporabniško ime in geslo. Osnovni PPP servis mora konfigurirati tehnično osebje ISP-ja (Murphy & Malone, 2005, str. 16-17).

### 2.2.6 Razteznost

Takšna uporaba interneta, kot jo imamo danes, zagotovo ni bila v mislih oblikovalcev protokola IPv4. Odprta in preprosta narava IPv4 pomeni, da je možno zgraditi aplikacije, kot so oddaljeni dostop, splet in »peer-to-peer« izmenjava datotek, brez neprestanega dograjevanja. Za to je delno odgovoren OSI model, ki je bil že omenjen. Vse to govori v prid dobrega inženiringa. Enostavnost v IPv4 je zagotovo še eden izmed razlogov, zakaj so ga razširili in uporabili za nepredvidene namene. IPv4 je dovolj preprost, da ga ljudje razumejo in izvajajo. Obenem je dovolj fleksibilen in robusten, da ga lahko uporabljamo na področjih, na katerih ga sprva nismo mislili in ga je možno spreminjati brez tega, da bi karkoli poškodovali. Poleg tega ga je relativno enostavno konfigurirati celo tehnično neizobraženim ljudem (Murphy & Malone, 2005, str. 17).

# 3 NOVI PROTOKOLI IN TEHNOLOGIJE INTERNETA - STRUKTURA IN VSEBINE PROTOKOLA IPV6

## 3.1 Protokol IPv6

Podporna tehnologija vzdržuje stanje brez radikalnih sprememb v načinu vzdrževanja. Na primer, Intel in AMD vzdržujeta takšen design CPU, da deluje vse hitreje in hitreje, toda v osnovi se proizvodnja in prodaja računalnikov ni spremenila. Izboljšanje lastnosti CPU je

podporna tehnologija za računalnike, med prebojno tehnologijo (angl. *disruptive technology*) pa bi lahko uvrstili t. i. biološko računalništvo, ki sicer ne nudi bistvene ekonomske prednosti ali zmogljivosti pred mikroprocesorji (Loshin, 2004, str. 8-9). Pojavlja se vprašanje, kam uvrstiti IPv6.

### 3.1.1 Prebojna tehnologija

IPv6 je nova tehnologija, ki ne omogoča kakšne večje prednosti v primerjavi z obstoječim IPv4, zagotovo pa ima svoj skriti potencial. IPv6 omrežje je namreč tako veliko, da si to komaj predstavljamo. Slednje pomeni dosti več naslovov, kot jih omogoča IPv4 internet, ki nam trenutno še zadostuje. V prid IPv4 gre tudi dejstvo, da je precejšen delež svetovne populacije finančno prešibek, da bi si lahko omislil večje število naprav, ki bi bile priključene na internetno omrežje. Potencialna velika omrežja so postala bolj zanimiva predvsem s padanjem cen enot z vgrajenim mrežnim priključkom. V primeru, da bi vrednost mrežno pripravljenih naprav padla na nivo $100, $600 milijard je to dovolj, da bi vsak posameznik imel dostop do omrežja. Če bi padla cena na $1 na omrežno enoto, potem bi lahko povezal v mrežo vse za popolnoma razumno ceno $6 milijard. Posamezna organizacija bi lahko prevzela tako tveganje nase ali v ta namen vsaj formirala konzorcij. Okoliščine postanejo še bolj zanimive, če bi cena padla na $0.01. Povezave celotnega sveta bi v tem primeru stala samo $60 milijonov. Tako premožnih pa je več sto ali celo več tisoč posameznikov (Loshin, 2004, str. 9-10).

Raziskovalci nadaljujejo z razvojem enot, ki so poceni, dovolj močne za enostavno procesiranje in shranjevanje podatkov ter dovolj majhne, da jih lahko vgradimo v skoraj vsak izdelek ali enoto. Temu bi zagotovo lahko rekli prebojna tehnologija (Loshin, 2004, str. 11).

Največji izziv protokola IPv6, ki ga smatramo kot prebojno tehnologijo, je torej sprejetje na tržišču. Prebojna tehnologija ni vedno razpoznavna, dokler ne postane dejstvo. Eden izmed razlogov, zakaj je temu tako, je tudi ta, da je prebojna tehnologija zelo pogosto uporabljena za druge namene, kot je bilo prvotno načrtovano. To pomeni, da tehnologija, ki je razvita za en trg, pogosto uspe na docela drugem trgu. Večina prebojnih tehnologij niti ni bila razvita za obstoječi trg, kar na prvi pogled zgleda kot navadna polomija. Zanje je značilno, da so kreirale širok nov trg, zunaj nepomembnih nišnih trgov ter razdrle posel mnogih pomembnih vodilnih firm v industriji (Loshin, 2004, str. 5-6).

Podporna tehnologija za razliko od prebojne tehnologije pomaga vzdrževati status quo. Firme potrošijo milijone za raziskave in razvoj z namenom, da bi postopne izboljšave naredile izdelke mnogo bolj profitne. To počnejo na različne načine (Loshin, 2004, str. 7-8):

- Z zmanjšanjem cene izdelave. Isti proizvod je na razpolago z nespremenjeno ceno, tudi pri nižjih stroških izdelave. Tako lahko pridobimo tržni delež s pocenitvijo izdelka ali povzročimo porast dobička pri nespremenjeni ceni. Podporna tehnologija nikoli ne poceni izdelka na račun zmogljivosti izdelka, medtem ko prebojna tehnologija lahko naredi prav to. V avtomobilski industriji lahko povečamo uporabo plastike in materialov, ki so primerni za recikliranje in s tem posredno pocenijo proizvodnjo. Taka tehnologija je podporna. V primeru, ko uvedemo nov postopek, ki stane samo desetino obstoječega, pa to lahko smatramo kot prebojno tehnologijo.
- Z izboljšanjem kvalitete. Če je 50 Mhz dobro, je 100 Mhz dvakrat bolje in vredno trikrat več. Proizvajalci strojne, programske in mrežne opreme iščejo najrazličnejše načine, kako povečati zmogljivosti produkta, čeprav seveda sam dvig zmogljivosti ni vedno pomemben za kupca. (npr. proizvajalci vojaške opreme so odkrili, da izboljšanje preciznosti pri nuklearnih izstrelkih ni pomembno, po drugi strani pa je točnost izstrelkov pomembna pri konvencionalnih izstrelkih ter v civilnem svetu, kjer se GPS uporablja za pomoč pri navigaciji tudi v avtomobilskih sistemih).
- Z dodajanjem novih funkcionalnosti. Boljše programerske družbe so tem bolj uspešne, čim bolj znajo dodajati produktom dodatne funkcionalnosti ali pa zaprejo uporabnike v postopne nadgradnje. Microsoft je v tem superioren. Več kot ima funkcionalnosti, bolj je verjetno, da bo produkt zadovoljil vaše potrebe. Če bomo kupili prvo verzijo, ker zadovoljuje 80 % naših potreb, najbližji konkurent pa 75 %, bomo, ko bo prišel čas za nadgradnjo, zopet kupili isti produkt, če bo le nadaljeval z dodajanjem funkcionalnosti. Istočasno je funkcionalno bogata programska oprema bolj ranljiva v primerjavi s programsko opremo, ki podpira odprte standarde. Ti omogočajo uporabnikom, da izberejo lastne funkcionalnosti. S pridobitvijo zgodnje kontrole nad operacijskim sistemom za Intel 8086/08x86 procesorsko družino je Microsoftov operacijski sistem MS-DOS prekinil način, na kakršen je Apple vodil svoj posel.

Prebojnost ne pomeni vedno boljšega produkta glede na ostale, ki že obstajajo na trgu. IPv6 je veliko boljši protokol kot IPv4, vendar za preboj potrebuje nekaj več. Na trgu se mora pojaviti nekaj, za kar IPv4 ne bo ponudil ustrezne rešitve. Prebojna tehnologija ne spreminja samo dinamike trga s tem, ko na eni strani ustvarja nova in na drugi strani uničuje obstoječa podjetja, ampak pogosto zgradi velik, nov trg, ki zasenči obstoječega (Loshin, 2004, str. 8).

### 3.1.2 Vrednost omrežja

Prve serijske postavitve IPv6 so bile v 3G ali tretji generaciji mobilnih telefonskih sistemov v začetku leta 2003. Zgodnje napovedi o velikosti tega omrežja so predvidevale od 100 milijonov do milijarde ali več vozlišč, kar je približna velikost IPv4 omrežja. Te napovedi so se izkazale kot preveč optimistične. Kot kažejo indikacije, se bo omrežje večalo postopoma (Loshin, 2004, str. 11).

Zastavlja se nam nekaj vprašanj. Koliko brezžičnih naprav lahko uporablja ena oseba? Kje lahko v kratkem pričakujemo razvoj IPv6? Kako lahko ocenimo priložnost, ki nam jo daje IPv6? Izumitelj etherneta in glavni ustanovitelj 3Com-a Robert Metcalfe je zapisal: »Vrednost omrežja narašča s kvadratom velikosti omrežja.« Podobno kot Moore-ov zakon je tudi to praktičen zakon, ki popolnoma zadošča za ugotavljanje relativne vrednosti dveh omrežij (Loshin, 2004, str. 11).

Po nekaterih izračunih končna vrednost IPv6 omrežja predstavlja 10 milijard (10.000.000.000) IVU ali eno milijontino vrednosti obstoječega IPv4 omrežja. Kaj se bo zgodilo, ko bo 3G omrežje naraslo na 100 milijonov uporabnikov? Vrednost IPv4 in IPv6 bo po mnenju Metcalfa bolj ali manj enakovredna. Komunikacija preko IPv6 omrežja tako praktično ne prinese nobene dodane vrednosti, toda upoštevati je potrebno prihodnjo rast omrežja. IPv4 ne bo več zmogel podpirati vedno večje rasti in nadgradljivosti, razen za trenutne tipe mrežnih aplikacij (Loshin, 2004, str. 12).

### 3.1.3 Spremljanje rasti

Že od leta 1994 čedalje pogosteje govorimo o IPv6, toda redko se zastavlja vprašanje, kdaj bodo organizacije prešle na IPv6. V ospredju so diskusije o tem, kakšne so razlike med IPv4 in IPv6, kako se bo spremenila tehnologija ter kako se pripraviti na njeno instalacijo in konfiguracijo. Manj pogosta so vprašanja o konkurenčni prednosti podjetij, ki bi prej prešla na IPv6. Kupci omrežne opreme ne vidijo nujne potrebe po IPv6, proizvajalci pa postopoma spoznavajo, da morajo v svoje produkte vgraditi IPv6 podporo (Loshin, 2004, str. 13).

Kaj bo povzročilo rast IPv6? Predvidevamo lahko, da bodo organizacije prešle na IPv6 predvsem zaradi strahu pred pomanjkanjem IPv4 naslovnega prostora in zasičenjem omrežne hrbtenice ali zaradi pojava nove aplikacije, ki bi zahtevala IPv6 in bi bila komercialno zanimiva (Loshin, 2004, str. 13).

### 3.1.4 Kriza ali zgrešena investicija

Prehod z IPv4 na IPv6 internet pomeni, da IPv6 ponuja nekaj, kar z IPv4 ni mogoče. Dejstvo je, da bo IPv4 naslovnega prostora zmanjkalo. To je dovolj velik razlog za tiste, ki zaupajo v IPv6 prihodnost. Nekaj IT oddelkov je že uvedlo splošno koeksistenco med obstoječim IPv4 in novim IPv6 protokolom. IPv6 lahko deluje kot samostojen prevajalec mrežnih naslovov (NAT) ali pa zahtevamo, da vsi sistemi podpirajo tako IPv6 kot tudi IPv4 (Loshin, 2004, str. 13-14).

### 3.1.5 Ubijalske aplikacije

Človek običajno kupi tisto, kar potrebuje. Zakaj torej kupiti IPv6, če nam že IPv4 omogoča dostop do interneta in svetovnega spleta? Odgovor se skriva v t.i. ubijalskih aplikacijah (angl. *killer applications*), ki bi bile zanimive za splošno populacijo, za delovanje pa bi potrebovale IPv6 (Loshin, 2004, str.14).

Prednosti, ki nam jih prinaša IPv6, se trenutno kažejo predvsem v boljši zmogljivosti in v manjših administracijskih stroških. Kaj pa varnost? Ali bi to lahko bila potencialna ubijalska aplikacija za IPv6? Zelo težko. V IPv6 je varnost sicer zahtevana že v samem osnovnem protokolu (IPsec), vendar ima tudi IPv4 uvedeno to isto varnost kot opcijo. IPv4 je tako lahko enako varen kot IPv6, če na vseh vozliščih uvedemo IPsec podporo. Kandidat za ubijalsko aplikacijo IPv6 bi morda lahko bila samokonfiguracija. Ta je vsekakor uporabna in se izplača, vendar je zgolj to še vedno premalo, da bi pomenilo bistveno prednost IPv6. Pojaviti se bodo morale povsem nove atraktivne aplikacije, v nasprotnem primeru pa je IPv6 lahko pogubljen (Loshin, 2004, str.14-15).

### 3.1.6 Prihodnost IPv6

IPv6 se vede kot klasična prebojna tehnologija. Aplikacije, pisane za IPv6 lahko nepričakovano obrodijo sadove, kar je mogoče pričakovati kjerkoli na svetu. V Aziji se že srečujejo s pomanjkanjem IPv4 naslovnega prostora. Če bo Kitajska nadaljevala s takšnim tempom računalniškega opremljanja, bo to hud pritisk na IPv4 naslovni prostor, ki jim je dodeljen. IPv6 je lahko odločilen dejavnik, ki bo moderniziral velik del sveta (Loshin, 2004, str. 17).

Uvedba nizko stroškovnih omrežnih računalnikov bi lahko spodbudila povpraševanje v razvijajočih se delih sveta in povzročila še večjo potrebo po IP naslovnem prostoru. Prav tako skokovito narašča uporaba brezžičnih naprav, ki se povezujejo v internet in so cenovno dostopne. Morda se bo istočasno pojavilo še kaj, kar bo potrebovalo IP naslov, npr. najrazličnejši senzorji, nove oznake inventarja, pametni papir (Loshin, 2004, str. 17).

IPv6 je potrebno obravnavati kot prebojno in ne kot podporno tehnologijo. Nerazumno je pričakovati, da bodo IPv4 uporabniki nadgradili svoje omrežje za podporo IPv6 brez nekaterih očitnih prednosti, ki bi jih prinesla takšna nadgradnja. Čeprav veliko organizacij pričakuje koristi nižje cene vzdrževanja, s prehodom na IPv6 še vedno odlašajo (Loshin, 2004, str. 17-18).

## 3.2 Struktura in polja v ovojnici paketov IPv6

Struktura glave IPv6 paketa je določena v RFC 2460. Glava ima fiksno dolžino 40 bajtov. Obe polji tako za izvorne kot za ciljne naslove uporabljata 16 bajtov (128 bitov), tako da ostane za splošne informacije samo 8 bajtov. Glava IPv6 je zato veliko preprostejša in bolj vitka kot IPv4. Omogoča veliko bolj učinkovito usmerjanje in veliko večjo prilagodljivost v razširitvi protokola prihodnjim potrebam (Hagen, 2002, str. 11).

### 3.2.1 Polja v glavi IPv6

Glava IPv6 je nova in izboljšana, ker ima manjše število polj. Polje, ki vsebuje verzijo, je enako kot pri protokolu IPv4. IPv6 glava vsebuje naslednja polja (Hagen, 2002, str. 13-16):

- **Verzija** (angl. *Version*, 4 Bits) je 4-bitna vrednost. Za IPv6 je ta vrednost 6.
- **Razred prometa** (angl. *Traffic Class*, 1 Byte) je polje, ki nadomesti polje Vrsta storitve (angl. *Type od Service*) v IPv4. Omogoča obravnavo podatkov v realnem času ter vseh ostalih podatkov, ki zahtevajo posebno obravnavo. Vse te podatke pošilja vozliščem in usmerjevalnikom, ki jih uporabijo za prepoznavanje in razlikovanje med različnimi razredi ali prioritetami IPv6 paketov.
- **Označen pretok** (angl. *Flow Label*, 20 Bits) je 20-bitna vrednost, ki identificira pakete, ki pripadajo istemu toku. Vozlišče je lahko istočasno izvor več tokov. Oznaka pretoka in naslov vozlišča edinstveno določata tokove. To polje je bilo prvotno (v RFC 1883) nastavljeno na 24-bitov. Ko je bilo polje DS povečano na 8-bitov, je bila oznaka polja zmanjšana, da se je to kompenziralo.
- **Dolžina koristne vsebine** (angl. *Payload Length*, 2 Bytes) je 16-bitno polje, ki vsebuje celo število. To je enako dolžini koristnega tovora v bajtih. Z drugimi besedami, število bajtov na koncu paketa v glavi IPv6 vključuje katerikoli IPv6 podaljšek glave. To pomeni, da so IPv6 podaljški vključeni kot del koristnega prometa, z namenom izračunavanja tega polja.
- **Naslednja glava** (angl. *Next Header*, 1 Byte) pokaže, kateri protokol je uporabljen v glavi, ki sledi takoj za IPv6 paketom. Protokoli so definirani s standardno 8-bitno vrednostjo, ki je definirana in upravljana s strani IANA. Vrednost tega polja se lahko nanaša na visoke protokole, kot so TCP ali UDP ali pa označi obstoj IPv6 podaljšek glave.
- **Limita skokov** (angl. *Hop Limit*, 1 Byte). Vsakič, ko vozlišče pošlje paket naprej, zmanjša vrednost 8-bitnega polja za 1. Če je vrednost polja 0, je paket izvržen. To je drugače kakor pri IPv4, kjer polje Življenska doba (angl. Time-to-live) opravlja podobno nalogo.
- **Izvorni naslov** (angl. *Source Address*, 16 Bytes) je 128-bitni naslov vozlišča izvornega IPv6 paketa.

- **Končni naslov** (angl. *Destination Address*, 16 Bytes) je 128-bitni naslov predvidenega prejemnika IPv6 paketa. Ta naslov je lahko unicast, multicast ali anycast naslov. Če je usmerjevalni dodatek uporabljen (definira specialno smer, ki jo mora paket prečkati), je lahko končni naslov eno od teh vmesnih vozlišč namesto zadnjega končnega vozlišča.

### 3.2.2 Opcije glave IPv6

IPv4 opcije spreminjajo obliko IP glav. Paket z IPv4 opcijo ima lahko več kot 40 oktetov podatkov več v glavi kot glava brez opcij. Ta fizična razlika med običajnimi paketi in paketi, ki uporabljajo opcije, pomeni, da morajo biti opcijski paketi obravnavani na usmerjevalnikih kot specialni primeri. Usmerjevalniki so običajno optimizirani za ravnanje s standardnimi paketi. Rezultat tega je, da so datagrami z opcijo nagnjeni k počasnejšemu razdeljevanju, ker zahtevajo specialno obravnavo. Prav zato so dani na stran in se njihovo procesiranje nadaljuje takrat, ko usmerjevalnik ni zaseden z razpošiljanjem običajnih paketov (Loshin, 2004, str. 132).

IPv6 podaljšek ali opcija glave (angl. *Option Headers)* lahko drastično reducira izkoristek števila paketov, ki uporabljajo to opcijo (Loshin, 2004, str. 132).

Nove opcije glave so (Loshin, 2004, str. 133-134):

- **Skok-do-Skok opcijska glava** (angl. *Hop-by-Hop Option Header*). Ta glava se vedno pojavi takoj za glavno glavo in vsebuje opcijske podatke, ki jih mora vsako vozlišče na poti, po kateri paketi potujejo, pregledati. Doslej sta specificirani dve Hop-by-Hop opciji: Jumbo Payload Option and the Router Alert Option.
- **Možnost velikega tovora** (angl. *The Jumbo Payload Option*). Identificira koristni tovor paketov, ki so večji kot 65.535 oktav, vključno z Hop-by-Hop opcijsko glavo. Če usmerjevalnik ne more obdelati jumbograma, vrne ICMPv6 sporočilo o napaki.
- **Možnost opozorila usmerjevalnika** (angl. Router Alert Option). Uporablja se za opozarjanje usmerjevalnika na to, da je informacija znotraj IPv6 datagrama predvidena za gledanje in obdelavo na vmesnih usmerjevalnikih. To se izvede celo, če je datagram naslovljen na neko drugo vozlišče. Tak primer so kontrolni datagrami, ki vsebujejo informacijo, ki pripada protokolom za rezervacijo pasovne širine.
- **Usmerjevalna glava** (angl. *Routing Header*). Povzroči, da paket obišče posamezno vozlišče, ki je specificirano v glavi in ga na podlagi tega usmeri k njegovemu cilju. Začetni ciljni naslov IPv6 glave ni isti kot končni ciljni naslov paketa. Ko to vozlišče sprejme paket, obdela IPv6 glavo in usmerjevalno glavo ter še enkrat pošlje paket na drugi naslov iz liste v usmerjevalni glavi. Ta proces se nadaljuje, dokler paketi ne dosežejo končnega cilja.
- **Drobljenje glave** (angl. *Fragment Header*). Vsebuje vse informacije okoli IP drobcev, ki so bili prej shranjeni v poljih glavne glave IPv4. Ta podaljšek vsebuje polja za

izravnavo delčkov – več zastavic za delčke (angl. *more fragment flags*) in identifikacijsko polje (angl. *identificiation field*). To polje poda dovoljenje izvornemu vozlišču, da zdrobi pakete, ki so preveliki za MTU pot med izvorom in ciljem.

- **Ciljna opcija glave** (angl. *Destination Options Header*). Predstavlja nadomestilo za IPv4 opcijsko polje. Sedaj so edine ciljno specificirane opcije, opcije za razširitev glavo na 64 bitno mejo. Ciljna opcija glave je mišljena za prenos informacije, ki je predvidena za iskanje ciljnega vozlišča.
- **Avtentikacijska glava** (angl. *Authentication Header - AH*). Ta glava omogoča mehanizem za izračun kripto grafične kontrolne vsote (angl. checksum) na posameznih delih IPv6 glave, podaljška glav in koristne vsebine (angl. *payload*).
- **Glava za zavarovanje vsebine s šifriranjem** (angl. *Encapsulating Security Payload Header – ESP*). Ta glava je vedno zadnja, nekriptirana glava vsakega paketa. Označi preostanek šifrirane koristne vsebine in omogoča dovolj informacij pooblaščenemu ciljnemu vozlišču za dešifriranje.

### 3.2.3 Ekstra veliki paketi

IPv6 ima dodano podporo za ekstra velike pakete (angl. *jumbograms*), ki so po vsebini večji od 65.575 oktetov. JumboPayload Option (RFC 2675) omogoča pošiljanje večjih paketov. V glavi IPv6 paketa z JumboPayload opcijo je polje Payload Lenght nastavljeno na nič. RFC 2675 določa tudi UDP in TCP razširitve, ki morajo biti izvedene na gostiteljih, ki podpirajo pošiljanje ekstra velikih paketov (Loshin, 2004, str. 135).

# 4 NASLAVLJANJE V PROTOKOLU IPV6

Domnevamo, da je najbolj očitna razlika med IPv4 in IPv6 naslovni prostor. IPv4 naslovni prostor je dolg samo 32 bitov, IPv6 naslovi pa so dolžine 128 bitov (Hagen, 2006, str. 35). Obstaja tudi več razlik glede načinov uporabe teh naslovov. Po drugi strani je dolžina naslova najmanj vidna sprememba, ker bo nevidna za večino uporabnikov. Aplikacije, prenesene čez IPv6 omrežje, se morajo popolnoma zanesti na sistem domenskih imen (angl. *Domain Name System* - v nadaljevanju DNS) za pravilno povezavo IP imen gostiteljev z IPv6 naslovi in omrežji.

IPv6 naslovna arhitektura je bila prvič objavljena kot predlagan standard leta 1995 v RFC »IP Version 6 Addressing Architecture«. V prvotni obliki so bili IPv6 naslovi definirani kot 128-bitni identifikatorji za vmesnike in niz vmesnikov. IPv6 specifikacija arhitekture naslavljanja je bila od leta 1995 dvakrat posodobljena. Prvič je bilo to leta 1998 z objavo RFC 2373, »IP Version 6 Addressing Architecture« in kasneje z RFC 3513 sredi leta 2003.

## 4.1 Vrste IPv6 naslovov

Poznamo 3 vrste naslovov: unicast, multicast in anycast. Unicast naslov identificira vmesnik IPv6 vozlišča. Paket, poslan na unicast naslov, je dostavljen vmesniku, ki je identificiran s tem naslovom. Multicast naslov identificira grupo IPv6 vmesnikov. Paket, ki je poslan na ta naslov, je dostavljen vsem članom multicast grupe. Anycast naslov je dodeljen več vmesnikom (običajno na več vozliščih). Paket, ki je poslan na ta naslov, je dostavljen samo enemu izmed teh vmesnikov, običajno najbližjemu (Hagen, 2006, str. 36).

IPv6 naslovi so dodeljeni vmesniku tako kot v IPv4. To je nasprotno od OSI sistema, kjer so naslovi dodeljeni vozliščem. Zaradi tega vsak vmesnik v vozlišču potrebuje vsaj en unicast naslov. Posameznemu vmesniku je lahko dodeljeno več IPv6 naslovov različnih tipov (unicast, multicast, anycast). Vozlišče je zaradi tega lahko prepoznano s katerikolim naslovom tega vmesnika. Prav tako je možno dodeliti en sam unicast naslov več vmesnikom, da se porazdeli obremenitev (angl. *load-sharing reasons*). V tem primeru moramo preveriti, ali to podpirata tudi strojna in programska oprema (gonilniki). V IPv6 so same ničle in enice legalne vrednosti za katerokoli polje v naslovu, z izključitvijo nekaterih specialnih kombinacij, ki so odvisne od tipa naslova (npr. Subnet Router Anycast Address, RFC 2373). Tipičen IPv6 naslov vsebuje tri dele; to so globalna usmerjevalna predpona (angl. *global routing prefix*), identifikacija (ID) podomrežja (angl. *subnet ID*) in identifikacija (ID) vmesnika (angl. *interface ID*; Hagen, 2002, str. 29). Splošna oblika IPv6 naslova je prikazana v Tabeli 3.

*Tabela 3: Splošna oblika IPv6 naslova*

| **Globalna usmerjevalna predpona**<br>dolžina = n bitov | **ID podomrežja**<br>m bitov | **ID vmesnika**<br>128 – n –m bitov |
|---|---|---|
| uporabljena za identifikacijo specialnih naslovov ali naslovnega prostora dodeljenega lokaciji | uporabljen za identifikacijo povezave znotraj lokacije | uporabljen za identifikacijo vmesnika na povezavi; mora biti unikum na tej povezavi |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 29, slika 3-1.*

Globalna usmerjevalna predpona se uporablja za identifikacijo specialnega naslova, kot je multicast ali naslovnega prostora dodeljenega lokaciji. ID podomrežja se uporablja za identifikacijo povezave znotraj lokacije. (ID podomrežja se lahko nanaša tudi na predpono omrežja ali preprosto »podomrežje«). Več ID podomrežij je lahko povezanih z eno povezavo. ID vmesnika se uporablja za identifikacijo vmesnika na povezavi in mora biti edinstven na tej povezavi (Hagen, 2002, str. 29).

### 4.1.1 Zapis naslova

Zapis naslova ima svoje zakonitosti (Hagen, 2002, str. 29-30), ki so predstavljene v nadaljevanju besedila.

IPv6 naslov ima 128 bitov ali 16 bajtov. Naslov je razdeljen v osem 16-bitnih heksadecimalnih blokov, ločenih z dvopičjem.

Na primer: FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Možne so tudi nekatere okrajšave, npr. vodilne ničle v 16-bitnem bloku lahko preskočimo.

Zgornji primer bi sedaj izgledal sledeče: FE80:0:0:0:202:B3FF:FE1E:8329

Dvojno dvopičje lahko zamenja zaporedne ničle ali vodilne oz. zadnje ničle znotraj naslova. Če upoštevamo to pravilo na našem primeru, dobimo: FE80::202:B3FF:FE1E:8329

Vedeti je potrebno, da dvojno dvopičje lahko v naslovu zapišemo samo enkrat. Razlog za to pravilo je povezano z dejstvom, da računalnik vedno uporablja 128-bitno binarno predstavitev naslova - celo, če je prikazan naslov poenostavljen. Ko računalnik naleti na dvojno dvopičje, ga razširi s toliko ničlami, kot je potrebno, da dobi 128 bitov. Če bi nek naslov imel dvakrat dvojno dvopičje, računalnik ne bi vedel, koliko ničel naj dodeli vsakemu dvojnemu dvopičju.

Tako je lahko naslov CAFF:CA01:0000:0056:0000:ABCD:EF12:1234 predstavljen na sledeče načine (imamo dve možni poziciji za postavitev dvojnega dvopičja):

- CAFF:CA01:0000:0056:0000:ABCD:EF12:1234
- CAFF:CA01::56:0:ABCD:EF12:1234
- CAFF:CA01:0:56::ABCD:EF12:1234

V okolju, kjer imamo mešano IPv4 in IPv6 vozlišča, je še ena prikladna oblika IPv6 zapisa. Vrednosti IPv4 naslova so dane v štiri najnižje razporejene bite naslova. IPv4 naslov 192.168.0.2 lahko predstavimo kot x:x:x:x:x:x:192.168.0.2. Tako je lahko naslov 0:0:0:0:0:0:192.168.0.2 zapisan kot ::192.168.0.2 ali ::C0A8:2.

### 4.1.2 Anycast naslov

Anycast naslovni prostor zajema isti razpon naslovov kot agregat globalnih unicast naslovov. Vsak vmesnik mora biti konfiguriran tako, kot da ima anycast naslov. Znotraj

regije, kjer vmesnik vsebuje isti anycast naslov, mora biti vsak gostitelj objavljen kot poseben vnos v usmerjevalno tabelo. V primeru, da anycast vmesnik nima definirane regije, mora biti vsak anycast vnos (v najslabšem primeru) razposlan skozi internet. Zato je pričakovano, da podpore za tak globalni anycast naslov bodisi ne bo bodisi bo zelo omejena (Hagen, 2002, str. 39).

V RFC 2373 so definirane naslednje omejitve (Hagen, 2002, str. 39-40):

- Anycast naslov ne sme biti uporabljen kot izvorni naslov IPv6 paketa.
- Anycast naslov ne sme biti dodeljen IPv6 gostitelju. Lahko je dodeljen samo IPv6 usmerjevalniku.

Od anycast naslovov se pričakuje, da bodo identificirani množici usmerjevalnikov nudili dostop do določene usmerjevalne domene. Ena možnost je 6v4 prenos anycast naslova, ki je specificiran v RFC 3068. Druga možnost je oblikovanje vseh usmerjevalnikov znotraj omrežja organizacije s specifičnim anycast naslovom, ki nudi dostop do interneta. Kadarkoli bo paket poslan na ta anycast naslov, bo poslan na najbližji usmerjevalnik, ki omogoča dostop do interneta (Hagen, 2002, str. 40).

Zahtevan anycast naslov usmerjevalnika-podomrežja (angl. *subnet-router*) je anycast naslov, ki je definiran v RFC 2373 in prikazan v Tabeli 4.

*Tabela 4: Oblika anycast naslova usmerjevalnika podomrežja*

| **Predpona podomrežja**<br>dolžina = n bitov | **Dolžina = 128 – n bitov**<br>0000 0000… |
|---|---|
| Ta predpona identificira specifično povezavo. | Mora biti nič. |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 40, slika 3-7.*

V osnovi je naslov podoben regularnemu anycast naslovu s predpono, ki specificira podomrežje in identifikatorjem, ki ima same ničle. Paket, poslan na ta naslov, bo poslan enemu usmerjevalniku na tem podomrežju. Vsi usmerjevalniki zahtevajo podporo za anycast naslov usmerjevalnika za podomrežja, za katera imajo vmesnike (Hagen, 2002, str. 40).

RFC 2526 vsebuje več informacij glede formata anycast naslova in specificira ostale rezervirane anycast naslove podomrežja ter ID-je (Hagen, 2002, str. 40). Rezerviran anycast naslov podomrežja ima lahko enega od dveh formatov, kot prikazuje Slika 1.

*Slika 1: Splošen format anycast naslova*

<table>
<tr><td colspan="3">Za anycast naslov, ki zahteva 64 bitni vmesnik v EUI-64 formatu:</td></tr>
<tr><td>64 bitov</td><td>57 bitov</td><td>7 bitov</td></tr>
<tr><td>Predpona podomrežja</td><td>1111 1101 11 ……... 1111</td><td>Anycast ID</td></tr>
<tr><td colspan="3">Polje ID vmesnika<br><br>Za vse ostale tipe IPv6 naslova</td></tr>
<tr><td>n bitov</td><td colspan="2">121 – n bitov</td><td>7 bitov</td></tr>
<tr><td>Predpona podomrežja</td><td colspan="2">1111 1111 1111 …… 1111</td><td>Anycast ID</td></tr>
<tr><td colspan="3">Polje ID vmesnika</td></tr>
</table>

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 40, slika 3-8.*

RFC 2526 specificira, da je znotraj vsakega podomrežja, najvišjih 128 identificiranih vrednosti vmesnika rezerviranih za dodelitev anycast naslovov podomrežja. Trenutni anycast ID-ji, ki so prikazani v Tabeli 5, so rezervirani (Hagen, 2002, str. 40).

*Tabela 5: Rezervirani anycast ID*

| **Decimalno** | **Heksadecimalno** | **Opis** |
|---|---|---|
| 127 | 7F | Rezerva |
| 126 | 7E | Mobilni IPv6 anycast domači agenti |
| 0 - 125 | 00 – 7D | Rezerva |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 41, tabela 3-4.*

### 4.1.3 Multicast naslov

Multicast naslov je identifikator za grupo vozlišč, identificiranih z najvišjim bitom FF ali 1111 1111 v binarnem zapisu. Vozlišče lahko pripada več kot eni multicast grupi. Multicast obstaja v IPv4, vendar je bil redifiniran in izboljšan za IPv6 (Hagen, 2002, str. 41). Multicast naslovni format prikazuje Slika 2.

*Slika 2: Format multicast naslova*

| 1111 1111 | Zastavice | Območje | Grupni identifikator |
|---|---|---|---|
| 8 bitov | 4 biti | 4 biti | 112 bitov |

**Zastavice**: bit 0 – 3 Rezervirano, mora biti nič.
Bit 4 0 = to je dobro poznan multicast naslov.
1 = to je začasni multicast naslov.

**Območje**: Vrednosti prikazuje *Tabela 6*.

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 41, slika 3-9.*

Prvi bajt identificira naslov kot multicast naslov. Naslednji štirje biti se uporabljajo kot Zastavice. Prvi trije biti polja Zastavice morajo biti prazni; rezervirani so za prihodnjo uporabo. Zadnji bit polja Zastavice pokaže, komu je ta naslov dodeljen - bodisi je to eden od dobro poznanih multicast naslovov, dodeljenih od IANA bodisi je začasen multicast naslov. Vrednost nič za zadnji bit določa dobro poznani naslov (angl. *well-known address*); vrednost ena določa začasni naslov. Polje Območje se uporablja za omejitev področja multicast naslovov (Hagen, 2002, str. 41). Tabela 6 prikazuje možne vrednosti.

*Tabela 6: Vrednosti polja Območje*

| Vrednost | Opis |
|---|---|
| 0 | Rezervirano |
| 1 | Območje lokalnega-vmesnika |
| 2 | Območje lokalne-povezave |
| 3, 4 | Nedodeljen |
| 5 | Območje krajevne lokacije (angl. Site-local scope) |
| 6, 7 | Nedodeljen |
| 8 | Lokalno območje organizacije |
| 9, A, B, C, D | Nedodeljen |
| E | Globalno območje |
| F | Rezervirano |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 41, tabela 3-5.*

### 4.1.4 Dobro poznani multicast naslovi

Zadnjih 112 bitov nosi ID multicast grupe. RFC 2375 določa začetno dodelitev IPv6 multicast naslova, ki je permanentno dodeljen. Nekatere dodelitve so narejene za fiksno območje, druge pa so veljavne skozi vsa območja (Hagen, 2002, str. 42).

Vsi naslovi se začnejo z FF0X. Pri tem je X spremenljivka vrednosti območja. Kot primer (Hagen, 2002, str. 43) si oglejmo to, kar je opisano v RFC 2373. Tukaj je multicast grupni ID definiran za vse NTP strežnike. Multicast grupni ID je 0x101. Ta grupni ID je lahko uporabljen z različnimi območnimi vrednostmi:

FF01:0:0:0:0:0:0:101
: Vsi NTP strežniki na istem vozlišču kot pošiljatelji.

FF02:0:0:0:0:0:0:101
: Vsi NTP strežniki na isti povezavi kot pošiljatelji.

FF05:0:0:0:0:0:0:101
: Vsi NTP strežniki na isti lokaciji kot pošiljatelji.

FF0E:0:0:0:0:0:0:101
: Vsi NTP strežniki na internetu.

Začasno dodeljeni multicast naslovi so pomembni samo znotraj določenega območja. Tabela 7 prikazuje pregled naslovov, ki so dodeljena za fiksna območja. Zapis območja vrednosti v bajtih sledi multicast identifikatorju FF (prvi bajt).

*Tabela 7: Dobro poznani multicast naslovi*

| **Naslov** | **Opis** |
|---|---|
| **Območje lokalnega vmesnika** | |
| FF01:0:0:0:0:0:0:1 | Vsi naslovi vozlišč |
| FF01:0:0:0:0:0:0:2 | Vsi naslovi usmerjevalnikov |
| **Območje lokalne povezave** | |
| FF02:0:0:0:0:0:0:1 | Vsi naslovi vozlišč |
| FF02:0:0:0:0:0:0:2 | Vsi naslovi usmerjevalnikov |
| FF02:0:0:0:0:0:0:3 | Nedodeljeni |
| FF02:0:0:0:0:0:0:4 | DVMRP usmerjevalniki |
| FF02:0:0:0:0:0:0:5 | OSPFIGP |
| FF02:0:0:0:0:0:0:6 | OSPFIGP dizajnirani usmerjevalniki |
| FF02:0:0:0:0:0:0:7 | ST usmerjevalniki |
| FF02:0:0:0:0:0:0:8 | ST gostitelji |
| FF02:0:0:0:0:0:0:9 | RIP usmerjevalniki |
| FF02:0:0:0:0:0:0:A | EIGRP usmerjevalniki |
| FF02:0:0:0:0:0:0:B | Mobilni agenti |
| FF02:0:0:0:0:0:0:D | Vsi PIM usmerjevalniki |

se nadaljuje

*Tabela 7: Dobro poznani multicast naslovi (nad.)*

| **Naslov** | **Opis** |
|---|---|
| FF02:0:0:0:0:0:0:E | RSVP ograjevanje |
| FF02:0:0:0:0:0:1:1 | Ime linka |
| FF02:0:0:0:0:0:1:2 | Vsi DHCP agenti |
| FF02:0:0:0:0:0:1:FFXX:XXXX | Ponujeni vozliščni naslovi (angl. Solicited-node address) |
| **Območje krajevne lokacije** | |
| FF05:0:0:0:0:0:0:2 | Vsi naslovi usmerjevalnikov |
| FF05:0:0:0:0:0:1:3 | Vsi DHCP strežniki |
| FF05:0:0:0:0:0:1:4 | Vsi DHCP prenosi |
| FF05:0:0:0:0:0:1:1000 do FF05:0:0:0:0:0:1:13FF | Lokacija servisa |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 42, tabela 3-6.*

Multicast naslovi se naj ne bi uporabljali kot izvorni naslovi v IPv6 paketih ali se pojavljali v poljubni usmerjevalni glavi (Hagen, 2002, str. 43).

### 4.1.5 Multicast naslov povpraševanja vozlišča

Multicast naslov povpraševanja vozlišča (angl. *Solicited-Node Multicast Address*) je multicast naslov, ki ga mora vsako vozlišče priključiti za vsak unicast in anycast naslov, ki mu je dodeljen. Uporabljen je v procesu DAD (angl. *Duplicate Address Detection*). RFC 2373 specificira multicast naslov povpraševanja vozlišča. Ta naslov je nastal z jemanjem spodnje ležečih 24 bitov IPv6 naslova (zadnji del ID gostitelja) in dodajanjem teh bitov dobro poznani predponi FF02:0:0:0:0:1:FF00::/104. Na ta način je območje multicast naslova za povpraševana vozlišča od FF02:0:0:0:0:1:FF00:0000 do FF02:0:0:0:0:1:FFFF:FFFF. V primeru, da ima gostitelj MAC naslov 00-02-B3-1E-83-29 in IPv6 naslov fe80::202:b3ff:fe1e:8329, je ustrezen naslov povpraševanega vozlišča FF02::1:ff1e:8329. Če ima ta gostitelj druge IPv6 unicast ali anycast naslove, bo vsak imel ustrezen multicast naslov povpraševanega vozlišča (Hagen, 2002, str. 43-44).

### 4.1.6 Potrebni naslovi

Standard določa, da morajo biti vsakemu vozlišču za lastno identifikacijo dodeljeni naslednji naslovi (Hagen, 2002, str. 44):

- njegov naslov lokalne povezave (angl. *link-local address*) za vsak vmesnik;
- poljubno dodeljeni unicast naslovi;
- naslov povratne zanke (angl. *loopback address*);

- multicast naslov vseh vozlišč;
- multicast naslov povpraševanega vozlišča za vsak njegov dodeljeni unicast ali anycast naslov;
- multicast naslove za vse ostale grupe, ki jim gostitelj pripada.

Usmerjevalnik mora poleg zgoraj naštetega prepoznati še sledeče (Hagen, 2002, str. 44):

- anycast naslov podomrežja usmerjevalnika za vmesnike, za katere je konfiguriran, da deluje kot usmerjevalnik na vsaki povezavi;
- vse anycast naslove, za katere je bil usmerjevalnik konfiguriran;
- vse multicast naslove usmerjevalnikov;
- multicast naslove vseh ostalih grup, ki jim usmerjevalnik pripada.

## 4.2 Struktura naslovov v IPv6

Struktura glave paketa IPv6 je določena v RFC 2460. Glava ima fiksno dolžino 40 bajtov. Polje za naslov vira in polje za naslov cilja porabita vsak po 16 bajtov (128 bitov). Zato ostane za splošne informacije v glavi samo še 8 bajtov. Glava IPv6 je zato veliko vitkejša in preprostejša kot glava IPv4. To omogoča bolj učinkovito obdelavo ter večjo prilagodljivost pri razširitvi protokola za izpolnjevanje potreb v prihodnosti (Hagen, 2006, str. 17).

### 4.2.1 IPv6 predpone

Zapis predpone je specificiran v RFC 4291. Predpono zapišemo v naslednjem formatu: IPv6 naslov/dolžina predpone. Dolžina predpone določa, koliko skrajno levo sosednjih bitov IPv6 naslova obsega predpono (Hagen, 2006, str. 38). Naslednji primer (Hagen, 2006, str. 38) nam bo pokazal, kako je predpona prestavljena. Vzemimo, da imamo zapisano predpono v obliki 2E78:DA53:1200::/40. Za lažje razumevanje bomo zapis pretvorili iz heksadecimalnega v binarno vrednost, kot je prikazano v Tabeli 8.

*Tabela 8: Razlaga zapisa predpone*

| Heksadecimalni zapis | Binarni zapis | Število bitov |
|---|---|---|
| 2E 78 | 0010 1110 0111 1000 | 16 |
| DA 53 | 1101 1010 0101 0011 | 16 |
| 12 | 0001 0010 | 8 |
| | | Skupaj: 40 |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 38, tabela 3-1.*

### 4.2.2 Globalne usmerjevalne predpone

Tabela 9 prikazuje trenutno dodeljene rezervirane predpone in posebne naslove, kot so povezavno-lokalni naslovi (angl. *link-local addresses*) ali multicast naslovi. Glavni del naslovnega prostora (več kot 80 %) je še nedodeljenega.

*Tabela 9: Seznam dodeljenih predpon*

| **Dodelitev** | **Binarna predpona** | **Heksa predpona** | **Del naslovnega prostora** |
|---|---|---|---|
| Ni dodeljen | 0000 0000 | ::0/8 | 1/256 |
| Rezerviran | 0000 0001 | | 1/128 |
| Globalni unicast | 001 | 2003::/3 | 1/8 |
| Povezavno-lokalni unicast | 1111 1110 10 | FE80::/10 | 1/1024 |
| Rezerviran | 1111 1111 11 | FEC0::/10 | 1/1024 |
| Lokalni IPv6 naslov | 1111 110 | FC00::/7 | |
| Privatna administracija | 1111 1101 | FD00::/8 | |
| Multicast | 1111 1111 | FF00::/8 | 1/256 |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 39, tabela 3-2.*

Nekateri posebni naslovi se realizirajo iz rezerviranega naslovnega prostora z binarno predpono 0000 0000. Te vključujejo neznan naslov, povratne zanke in IPv6 naslove, vsebovane v IPv4 naslovih. Unicast naslovi se razlikujejo od multicast naslovov gleda na njihovo predpono. Globalen unikatni unicast naslov se začne z 001. IPv6 naslov, ki se začne z 1111 1111 (FF heksa), je vedno multicast naslov. Anycast naslovi so vzeti iz unicast naslovnega prostora, zato ne morejo biti določeni kot anycast samo na osnovi predpone. V primeru, da se dodeli unicast naslov več vmesnikom, dobimo anycast naslov. Vmesnike je potrebno konfigurirati tako, da vsi vedo, da je ta naslov anycast naslov (Hagen, 2006, str. 39-40).

## 4.3 Storitve zasebnosti in varnosti v IPv6

Varnostni protokol (angl. *IP Security Protocol* - v nadaljevanju IPsec), kot je opredeljen v RFC 2401, določa varnostno arhitekturo za internetni protokol in ne varnostne arhitekture za internet. Zagotavlja interoperabilne in odprte standarde za gradnjo varnosti v omrežnem sloju, namesto na prijavnem ali transportnem sloju. Čeprav lahko aplikacije koristijo varnost omrežne plasti, je najpomembnejša vloga, ki jo IPsec omogoča, ustvarjanje navideznih zasebnih omrežij (VPN), ki lahko varno nosijo podatke o podjetju po odprtem internetu (Loshin, 2004, str. 90).

Pogosto je uporabljen v povezavi z upravljalnimi tunelskimi protokoli, vključno z Layer 2 Tunneling Protocol-om (L2TP), The Layer 2 Forwarding (L2F) Cisco protokolom in Microsoftovim Point to Point Tunneling Protocol-om (PPTP). Protokoli za upravljanje tunela ponujajo dostop do varnostnih storitev, ne zagotavljajo pa storitve verodostojnosti ali storitve zasebnosti, zato se pogosto uporabljajo v povezavi z IPsec, ki te storitve zagotavlja (Loshin, 2004, str. 90-91).

IPsec omogoča naslednje (Loshin, 2004, str. 91):

- šifriranje (angl. *encryption*) podatkov, ki potujejo med dvema vozliščema z uporabo močnega šifrirnega algoritma javnega/zasebnega ključa;
- avtentikacijo (angl. *authentication*) podatkov in njihovega izvora z uporabo močnega avtentikacijskega mehanizma;
- nadzor nad dostopom (angl. *control over access*) do občutljivih podatkov in zasebnih omrežij;
- preverjanje celovitosti (angl. *integrity verification*) prenesenih podatkov z brezpovezavnim protokolom (IP);
- zaščito pred ponovnimi napadi (angl. *protection against replay attacks*), v katerih vsiljivec prestreže pakete med dvema vozliščema in jih ponovno pošlje po dešifriranju ali spreminjanju;
- omejitve analitičnih napadov prometa (ang. *limitation of traffic analysis attacks*), v katerih vsiljivec prestreže zaščitene podatke, analizira izvorno in ciljno informacijo, velikost in vrsto podatkov ter druge vidike podatkov, vključno z vsebino glave;
- varnost od konca do konca (angl. *end-to-end security*) za IP pakete, ki zagotavljajo jamstvo zasebnosti in integritete prenosa za uporabnike na končnih točkah vozlišča;
- varno tuneliranje (angl. secure tunneling) skozi nevarovana omrežja, kot so svetovni snternet in druga javna omrežja;
- integracijo algoritmov, protokolov in varnostne infrastrukture (angl. *integration of algorithms, protocols and security infrastructures*) v krovno varnostno arhitekturo.

Kot je definirano v RFC 2401 »Security Architecture for the Internet Protocol«, je cilj varnostne IP arhitekture zagotoviti različne varnostne storitve za promet v IP sloju, tako v IPv4 kot IPv6 okolju. To pomeni varnostne storitve, ki imajo naslednje lastnosti (Loshin, 2004, str. 91-92):

- **Interoperabilnost** (angl. *interoperability*). Predstavlja temeljni cilj v vseh internetnih protokolih. To pomeni, da vsako vozlišče, ki podpira IPsec, lahko komunicira z drugim vozliščem, ki podpira IPsec. Obstaja osnovni nabor šifrirnih algoritmov za šifriranje in preverjanje celovitosti, ki jih morajo podpirati vsa IPsec vozlišča.
- **Visoka kakovost** (angl. *high quality*). Izhodišča za varnost preko IPsec moramo postaviti dovolj visoko, da zagotavljajo primerno stopnjo dejanske varnosti. Algoritmi

in dolžine ključev, ki so ranljivi za napad, niso sprejemljivi. Na primer, podatki šifrirani s 40-bitnim šifrirnim ključem so lahko dešifrirani z metodo izčrpnega iskanja (angl. *brute-forced*) ali tako, da se preizkusi vsako kombinacijo. Zaradi tega 40-bitnih ključev ne smatramo za ključe, ki zagotavljajo visoko raven varnosti.

- **Osnovanost na šifriranju** (angl. *cryptographic basis*). Kriptografi delajo z algoritmi za šifriranje, varnostnimi zgoščevalnimi algoritmi (angl. *security hash*) in avtentikacijo. Algoritmi za šifriranje omogočajo, da se regularni podatki pretvorijo v šifropis. Tako zakodirane podatke lahko dešifrira samo subjekt z ustreznim dekodirnim ključem. Varni zgoščevalni algoritmi (angl. *secure hash algorithms*) delujejo na vseh podatkih, ne glede na velikost posameznega bloka za pripravo zaporedja bitov fiksne dolžine (angl. *hash*). Subjekt lahko potrdi celovitost podatkov tako, da na prispelih podatkih izvaja algoritem zgoščevalne funkcije. Če se prenešeni in izračunani »hash« ujemata, to pomeni, da so podatki na podlagi preverjanja poslani brez sprememb. Preverjanje pristnosti subjektov s pomočjo uporabe digitalnih podpisov je odvisna od arhitekture javnih ključev. Podatke, šifrirane z javnim ključem javno/zasebnega para ključev, lahko dešifrira samo subjekt, ki ima dostop do zasebnega ključa. Če subjekt šifrira tekstovno sporočilo s svojim zasebnim ključem, potem lahko vsak, ki ima dostop do javnega ključa, dešifrira to sporočilo in potrdi, da ima pošiljatelj dostop do tega ključa.

Računalniško varnost pooseblja trije splošni cilji (Loshin, 2004, str. 93-94):

- **Avtentikacija** (angl. *authentication*). Sposobnost zagotoviti, da so sprejeti podatki enaki poslanim in da je subjekt, ki je poslal te podatke, resnično to, za kar se izdaja.
- **Integriteta** (angl. *integrity*). Sposobnost zagotoviti, da podatki niso bili spremenjeni med potjo od izvora do cilja. Uspešno ohraniti integriteto podatkov pomeni preprečiti napadalcu, da spreminja avtentične podatke. Pomeni tudi preprečevanje prejema poškodovanih podatkov.
- **Zaupnost** (angl. *confidentiality*). Sposobnost zagotovoti prenos podatkov, ki jih lahko preberejo in uporabijo izključno določeni prejemniki. Uspešno ohranjanje zaupnosti podatkov pomeni preprečitev možnosti dostopa do zasebnih podatkov komurkoli razen predvidenemu prejemniku.

Razvoj sodobne kriptografije omogoča kombinacijo naštetih ciljev v en sklop funkcij. Te cilje je mogoče doseči s tremi povezanimi funkcijami (Loshin, 2004, str. 94):

- Digitalni podpis (angl. *digital signatures*) je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki (na primer z elektronskim dokumentom) ter je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
- Varnostna zgoščevalna funkcija (angl. *secure hashes*) digitalno povzame zaporedje podatkov z uporabo ponovljivega procesa, ki bo dal enake rezultate le v primeru, če podatki zaporedja pri preverjanju ustrezajo podatkom, ki jih je poslal pošiljatelj.

- Šifriranje (angl. *encryption*) je postopek reverzibilnega preoblikovanja berljivih podatkov, tako da postanejo neberljivi za vsakogar, ki ni imetnik ustreznega ključa za dešifriranje.

Nekatere ali vse funkcije delujejo bodisi posamično bodisi v kombinaciji v protokolih na vseh plasteh TCP/IP sklada, iz IP (skozi IPsec) do transportnega sloja (skozi TLS), skupaj z varnostnimi funkcijami, ponujenimi skozi aplikacijo. IPsec določa okvir, znotraj katerega vozlišča izpogajajo ustrezne algoritme, protokole, dolžine ključev in druge vidike varne komunikacije (Loshin, 2004, str. 95).

IP varnostna arhitektura omogoča sistemom izbrati potrebne varnostne protokole, identificira kriptografske algoritme za uporabo s temi protokoli ter si izmenjuje vse ključe, informacije ali druga gradiva, potrebna za zagotavljanje varnostnih storitev. IPsec kot protokol omrežnega sloja omogoča varnost samo na omrežnem sloju. To pomeni, da so lahko paketi zaščiteni samo od točke vstopa v IP omrežje (IP vmesnika izvornega vozlišča) do točke izstopa iz IP omrežja (IP vmesnika ciljnega vozlišča). IPsec ne more nadomestiti primernega aplikacijskega ali transportnega varnostnega mehanizma. Prav tako nas IPsec ne more zaščititi pred napadalci, ki prevzamejo nadzor nad izvornimi ali ciljnimi vozlišči oz. procesi.

## 4.4 Podrobnejša predstavitev sistema naslavljanja

V nadaljevanju sledijo podrobneje predstavljeni sistemi naslavljanja oz. različne vrste IPv6 naslovov – globalni unicast naslovi, multicast naslovi in anycast naslovi.

### 4.4.1 Globalni unicast naslovi

Globalni unicast naslovi so označeni s predpono 001. V Tabeli 10 je predstavljena struktura globalnega unicast naslova.

*Tabela 10: Struktura globalnega unicast naslova*

| | **Globalna usmerjevalna predpona** | **ID podomrežja** | **ID vmesnika** |
|---|---|---|---|
| **Število bitov** | 48 (001 + 45 bitov) | 16 | 64 |

*Vir: IETF, IP Version 6 Addressing Architecture, 2006.*

Globalna usmerjevalna predpona identificira obseg naslovov za posamezno lokacijo. Ta del naslova dodeli mednarodni register storitev in ponudnik internetnih storitev (ISP); ima

hierarhično strukturo. ID podomrežja identificira posamezno podomrežje znotraj omrežja posamezne lokacije. Ta del naslova dodeljuje lokalni skrbnik omrežja.

### 4.4.2 Multicast naslovi

Vsi multicast naslovi imajo predpono FF00::/8 ali binarno 1111 1111 (prvih 8 bitov) in jih tako lahko identificiramo. Naslednji štirje biti se uporabljajo za Zastavice, ki so definirane na sledeči način: Prvi bit v polju Zastavice mora biti 0 in je rezerviran za kasnejšo uporabo. Drugi bit pove, ali ima ta multicast naslov vdelano točko srečanja (angl. *point of randezvoues*). Točka srečanja je točka distribucije za specifičen multicast podatkovni tok v multicast omrežju (RFC 3956). Tretji bit pove, ali ima ta multicast naslov vdelano predpono informacije (angl. *prefix information*). Zadnji bit zastavice pove, ali gre bodisi za stalno dodeljen naslov, ki ga je določila organizacija IANA (bit ima vrednost 0) bodisi za začasni multicast naslov (bit ima vrednost 1; Hagen, 2006, str. 51-52). V Tabeli 11 je predstavljena struktura IPv6 multicast naslova.

*Tabela 11: Struktura IPv6 multicast naslova*

| **Struktura** | 1111 1111 | Zastavice | Področje | ID skupine |
|---|---|---|---|---|
| **Število bitov** | 8 bitov | 4 biti | 4 biti | 112 bitov |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 52, slika 3-9.*

Polje Obseg je uporabljen za omejitev obsega multicast naslova (Hagen, 2006, str. 52). Možne vrednosti so prikazane v Tabeli 12.

*Tabela 12: Vrednosti polja Področje*

| **Opis** | **Vrednost** |
|---|---|
| Rezervirano | 0 |
| Vmesnik - lokalno področje | 1 |
| Poveza - lokalno področje | 2 |
| Rezervirano | 3 |
| Upravljanje - lokalno področje | 4 |
| Nedodeljeno | 5 |
| Organizacija - lokalno področje | 8 |
| Nedodeljeno | 9, A,B,C,D |
| Globalno področje | E |
| Rezervirano | F |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 52, tabela 3-5.*

Meje področij (razen področij vmesnik-lokalno, povezava-lokalno in globalno področje) mora opredeliti in nastaviti skrbnik omrežja. Rezervirana področja se naj ne bi uporabljala (Hagen, 2006, str. 52).

### 4.4.3 Anycast naslovi

Anycast naslovi so zasnovani za zagotavljanje redundance in uravnoteženja obremenitve tam, kjer več gostiteljev ponuja enake storitve. Anycast ni bil oblikovan za IPv6. Opredeljen je bil v RFC 1546, in sicer že leta 1993 kot poskusna specifikacija za uporabo v IPv4. RFC dodeluje za anycast posebno predpono, ki omogoča prepoznavo anycast naslova. Načrtovana je bila uporaba anycast za storitve, kot so DNS in HTTP. V praksi anycast ni bil implementiran tako, kot je bilo načrtovano. Pogosto je izbrana metoda, poznana kot skupna raba unicast naslova (angl. *shared unicast address*). Po tej metodi se dodeljuje unicast naslove večjemu številu vmesnikov in ustvarja zapise v usmerjevalno tabelo. V tem primeru omrežna in transportna plast predpostavljata, da gre za enolično določen unicast naslov. Če temu ni tako, mora biti mehanizem, ki razrešuje nedvoumne naslove, vgrajen v aplikacijo. Izjeme so aplikacije, ki uporabljajo avtomatski konfiguracijski mehanizem, na primer DNS preko UDP. Korenski (angl. *root*) DNS strežniki v internetu so nastavljeni tako, da uporabljajo skupne unicast naslove. Ker ta postopek ne zahteva podpore omrežnega sloja, se lahko uporablja tudi v IPv6 (Hagen, 2006, str. 49-50).

Razvijalci IPv6 že od začetka želijo, da bi bil anycast vgrajen v omrežni sloj po RFC 1546, zato mu ni bila dodeljena nobena posebna predpona. Anycast naslovi so v istem naslovnem področju kot globalni unicast naslovi. Vsak sodelujoči vmesnik je potrebno nastaviti tako, da ima unicast naslov. V okviru regije, v kateri so vmesniki, ki vsebujejo enake anycast naslove, mora biti vsak gostitelj objavljen z ločenim vpisom v usmerjevalne tabele. V primeru, da anycast vmesnik nima določljive regije, se lahko vsak vpis anycast naslova razmnoži po celotnem internetu, kar pa ni v skladu z RFC (Hagen, 2006, str. 50).

Kadar uporabljamo anycast naslove, se moramo zavedati dejstva, da pošiljatelj nima nadzora nad tem, preko katerega vmesnika bo paket dostavljen. Ta odločitev je sprejeta na nivoju protokola usmerjanja. Ko pošiljatelj pošlje več paketov z anycast naslovom, lahko paketi prispejo na različne cilje. Primeri, ko gre za serijo zahtev in odgovorov ali ko je paket razdrobljen, znajo predstavljati problem (Hagen, 2006, str. 50). Slika 3 prikazuje obliko anycast naslova.

*Slika 3: Oblika anycast naslova usmerjevalnika podomrežja*

| Predpona omrežja<br>Dolžina = n bitov | Dolžina = 128 – n bitov<br>0000 0000... |
|---|---|
| Ta predpona označuje določeno povezavo. | Mora biti nič. |

*Vir: IETF, IP Version 6 Addressing Architecture, 2006.*

Anycast naslov pravzaprav izgleda kot običajen unicast naslov s predpono za navedbo podomrežja in identifikatorjem, nastavljenim na ničle. Paket, poslan na ta naslov, bo dodeljen enemu usmerjevalniku v tem podomrežju. Vsi usmerjevalniki morajo podpirati anycast naslov podomrežje-usmerjevalnik za tista podomrežja, v katerih imajo svoje vmesnike. RFC 2526 vsebuje več informacij o formatih anycast naslova in določa druge rezervirane anycast naslove in ID podomrežja (Hagen, 2006, str. 50).

Rezerviran anycast naslov podomrežja ima lahko eno od dveh rezerviranih oblik, kot prikazuje Slika 4. Anycast naslovi morajo imeti 64-bitni identifikator vmesnika v EUI-64 formatu.

*Slika 4: Splošna oblika anycast naslovov*

| 64 bitov | 57 bitov | 7 bitov |
|---|---|---|
| Predpona podomrežja | 1111 1101 11.....1111 | Anycast ID |
| polje ID vmesnika | | |

Za vse ostale tipe IPv6 naslovov:

| n bitov | 121 - n bitov | 7 bitov |
|---|---|---|
| Predpona podomrežja | 1111 1111 1111.....1111 | Anycast ID |
| polje ID vmesnika | | |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 51, slika 3-8.*

RFC 2526 določa, da je v vsakem podomrežju najvišja vrednost (128) identifikatorja vmesnika rezervirana za dodelitev anycast naslovov (Hagen, 2006, str. 51).

# 5 PROTOKOL ZA IZMENJAVO SPOROČIL NA RAVNI MREŽNEGA SLOJA - ICMPV6

Internetni protokol za nadzor prenosa (angl. *Internet Control Message Protocol* – v nadaljevanju ICMP), ki deluje v IPv6 in pove veliko o stanju mreže, je dobro poznan.

ICMP sporoča napake, kadar paketi niso bili primerno obdelani in pošilja informativna sporočila o statusu omrežja. Na primer, če usmerjevalnik ne more poslati paketa naprej, ker je prevelik, da bi ga poslal v drugo omrežje, vrne nazaj ICMP sporočilo izvornemu gostitelju. Izvorni gostitelj lahko uporablja to ICMP sporočilo za določitev primernejše velikosti paketa, ki ga nato ponovno pošlje. Poleg tega ICMP izvršuje tudi diagnostično funkcijo, kot dobro poznani ping, ki uporablja ICMP Echo Request in Echo Replay sporočilo za testiranje razpoložljivosti omrežja (Hagen, 2006, str. 60).

ICMPv6 je veliko bolj mogočen kot ICMPv4 in vsebuje nove funkcionalnosti, npr. funkcijo IGMP (angl. *Internet Group Management Protocol*), ki upravlja multicast članstva v grupi z IPv4 in funkcijo ARP/RARP (angl. *Address Resolution Protocol/Reverse Address Resolution Protocol*), ki se uporablja v IPv4 za mapiranje naslovov iz drugega sloja v IP naslove - in obratno. Nova je tudi funkcija odkrivanja sosedov (angl. *Neighbor Discovery* – v nadaljevanju ND). Ta uporablja ICMPv6 sporočilo za določitev naslova povezavnega sloja za sosede, ki so povezani z isto povezavo, za iskanje usmerjevalnikov, za ohranjanje sledi o tem, kateri sosedje so dostopni in za detektiranje spremembe naslovov povezavnega sloja (angl. *link-layer addresses*). ICMPv6 podpira tudi Mobile IPv6. ICMPv6 je del IPv6 in mora biti polno implementiran v vsakem IPv6 vozlišču. Definiran je v RFC 2463, ND pa je definiran v RFC 2463 (Hagen, 2006, str. 60).

## 5.1 Internetni protokol za nadzor prenosa

Poznamo dva razreda sporočil v okviru internetnega protokola za nadzor prenosa (angl. *Internet Control Message Protocol* – v nadaljevanju ICMP; Hagen, 2006, str. 60-61):

- **ICMP obvestilo o napaki** (angl. *error messages*). Obvestilo o napaki ima ničlo v zgornjem najvišjem bitu njegovega sporočila v polju Tip (angl. *Type*). Tipi ICMP obvestil o napaki so zato v razponu od 0 do 127.
- **ICMP informativno obvestilo** (angl. *informational messages*). Informativno sporočilo ima enico v zgornjem najvišjem bitu sporočila v polju Tip (angl. *Type*). Tipi ICMP informativnih obvestil so zato v razponu od 128 do 255.

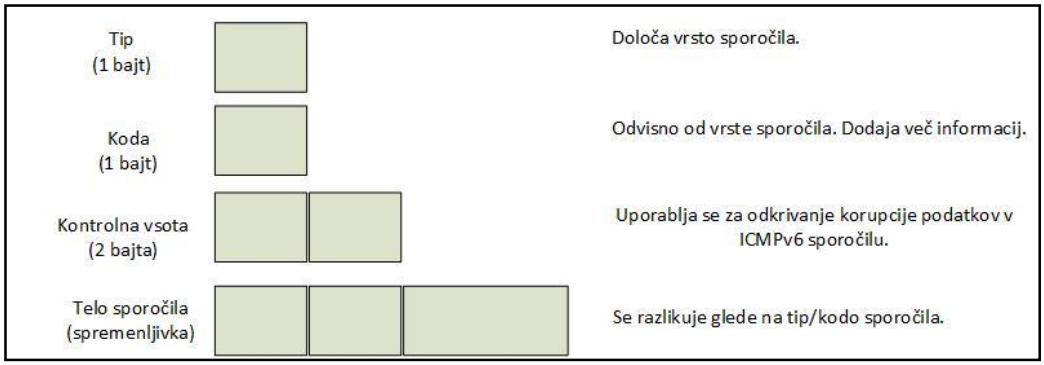
V RFC 2463 so opisani naslednji tipi sporočil (Hagen, 2006, str. 61):

- ICMP obvestilo o napaki;
  - Destination Unreahable (sporočilo tipa 1);
  - Packet Too Big (sporočilo tipa 2);
  - Time Exceeded (sporočilo tipa 3);
  - Parameter Problem (sporočilo tipa 4);
- ICMPv6 informativno obvestilo;

- Echo Reguest (sporočilo tipa 128);
- Echo Reply (sporočilo tipa 129).

Vsa ICMPv6 sporočila imajo enako splošno strukturo glave. Pri tem je dobro vedeti, da se prva tri polja za tip (angl. *type*), kodo (angl. *code*) in kontrolno vsoto (angl. *checksum*) niso spremenila od verzije ICMPv4 (Hagen, 2006, str. 61). Splošno obliko glave prikazuje Slika 5.

*Slika 5: Splošna oblika glave ICMPv6*




*Vir: S. Hagen, IPv6 Essentials, 2006, str. 62, slika 4-1.*

Splošna oblika glave je sledeča (Hagen, 2006, str. 61):

- **Tip** (angl. *Type*), 1 bajt. To polje označuje vrsto sporočila, ki določa obliko preostanka sporočila.
- **Koda** (angl. *Code*), 1 bajt. To polje je odvisno od tipa sporočila in v določenih primerih omogoča bolj podrobno sporočilo.
- **Kontrolna vsota** (angl. *Checksum*), 2 bajta. To polje se uporablja za detektiranje okvare podatkov v glavi in delih glave IPv6. Zato da izračuna kontrolno vsoto, mora vozlišče določiti izvorni in končni naslov v IPv6 glavi. Če ima vozlišče več kot en unicast naslov, obstaja za izbiro naslova več pravil. Podroben opis najdemo v RFC 2463. V izračun kontrolne vsote je vključena tudi izmišljena glava (angl. *pseudoheader*), kar je novost v ICMPv6.
- **Telo sporočila** (angl. *Message Body*), spremenljive dolžine. Telo sporočila bo vsebovalo različne podatke, odvisno od tipa in kode. V primeru sporočila o napaki bo vsebovalo kolikor je le mogoče veliko paketov, ki se sklicujejo na sporočilo za pomoč pri odpravljanju težav. Končna velikost ICMPv6 paketov naj ne bi presegla minimalnega IPv6 MTU, ki je 1280 bitov.

Tabeli 13 in 14 podajata pregled različnih tipov sporočil, poleg dodatnih kodnih informacij, ki so odvisne od tipa sporočila.

*Tabela 13: ICMPv6 sporočila o napaki in vrste kod*

| **Števila sporočila** | **Tip sporočila** | **Polje kode** |
|---|---|---|
| 1 | Destination Unreachable | 0 = ni usmeritve k cilju<br>1 = komunikacija s ciljem je administrativno prepovedana<br>2 = onstran področja izvornega naslova<br>3 = naslov je nedostopen<br>4 = port je nedostopen |
| 2 | Packet Too Big | Pošiljatelj postavi kodno polje na 0, prejemnik pa to polje ignorira. |
| 3 | Time Exceeded | 0 = prekoračen limit skokov v prehodu<br>1 = prekoračen čas ponovne sestave delčkov |
| 4 | Parameter Problem | 0 = naleteti na polje napačnih glav<br>1 = naleteti na neprepoznaven naslednji tip glave<br>2 = naleteti na neprepoznavno IPv6 opcijo |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 48, tabela 4-1.*

*Tabela 14: ICMPv6 informativno sporočilo*

| **Številka sporočila** | **Tip sporočila** | **Opis** |
|---|---|---|
| 128<br>129 | Echo Request<br>Echo Reply | RFC 2463. Oba se uporabljata za ukaz ping. |
| 130<br>131<br>132 | Multicast Listener Query<br>Multicast Listener Report<br>Multicast Listener Done | RFC 2710. Uporabljen za upravljanje multicast grupe (IPv4 uporablja za to funkcionalnost IGMP). |
| 133<br>134<br>135<br>136<br>137 | Router Solicitation<br>Router Advertisement<br>Neighbour Solicitation<br>Neighbour Advertisement<br>Redirect Message | RFC 2461. Uporabljen za odkrivanje sosedov in samokonfiguracijo. |
| 138<br>139<br>140 | Router Renumbering<br>ICMP Node Information Query<br>ICMP Node Information Response | RFC 2894 |
| 141<br>142 | Inverse ND Solicitation<br>Inverse ND Adv Message | RFC 3122<br>RFC 3122 |
| 150<br><br>151<br><br>152<br><br>153 | ICMP Home Agent Address Discovery Request Message<br>ICMP Home Agent Address Discovery Reply Message<br>ICMP Mobile Prefix Solicitation Message Format<br>ICMP Mobile Prefix Advertisement Message Format | Eksperimentalni / Osnutek – ICMPv6 sporočila za mobilni IPv6<br>Številka sporočila še ni bila dodeljena s strani IANA. |

*Vir: S. Hagen, IPv6 Essentials, 2002, str. 48-49, tabela 4-2.*

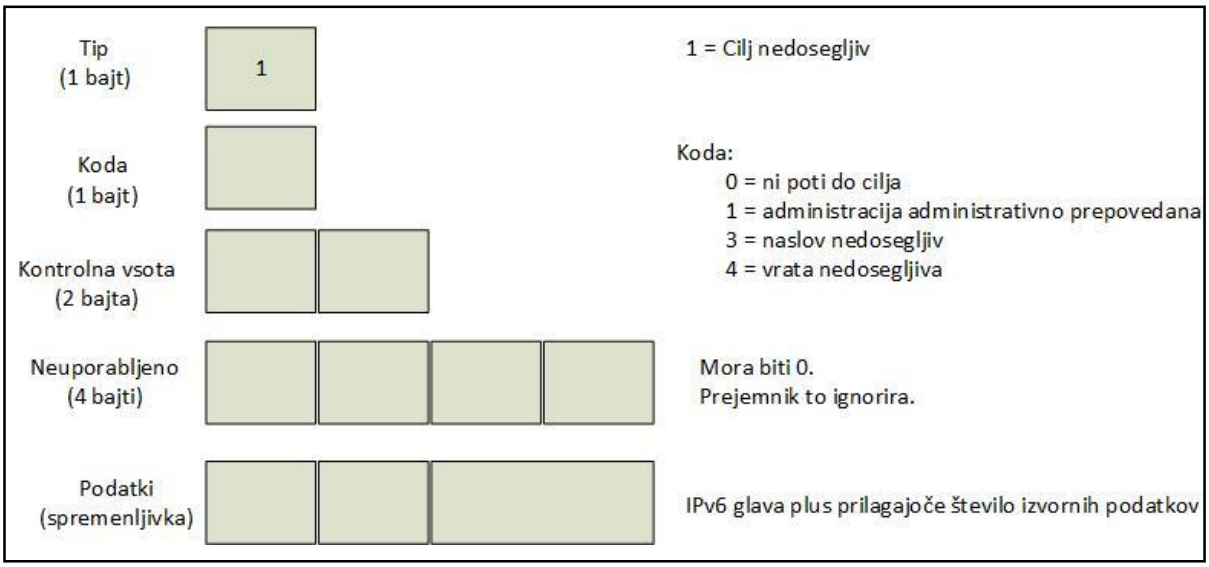
### 5.1.1 Sporočila o napaki

Vsako ICMP sporočilo ima lahko nekoliko drugačno glavo, odvisno od vrste sporočila o napaki in od informacije, ki jo prenaša (Hagen, 2006, str. 64). V nadaljevanju je podan splošen pregled strukture vsakega tipa ICMPv6 sporočila.

#### 5.1.1.1 Cilj nedosegljiv

Sporočilo Cilj nedosegljiv (angl. *Destination Unreachable*) je kreirano, kadar IP datagram ni dostavljen. Polje Tip z vrednostjo 1 identificira to sporočilo. ICMP sporočilo je poslano na izvorni naslov klicanega paketa (Hagen, 2006, str. 64).

*Slika 6: Format sporočila Destination Unreachable*




*Vir: S. Hagen, IPv6 Essentials, 2006, str. 65, slika 4-2.*

Polje Tip je nastavljeno na ena, ki je vrednost za sporočilo Cilj nedosegljiv. Kodno polje vsebuje več informacij o tem, zakaj datagram ni bil dostavljen (Hagen, 2006, str. 64).

### 5.1.2 Informativno sporočilo

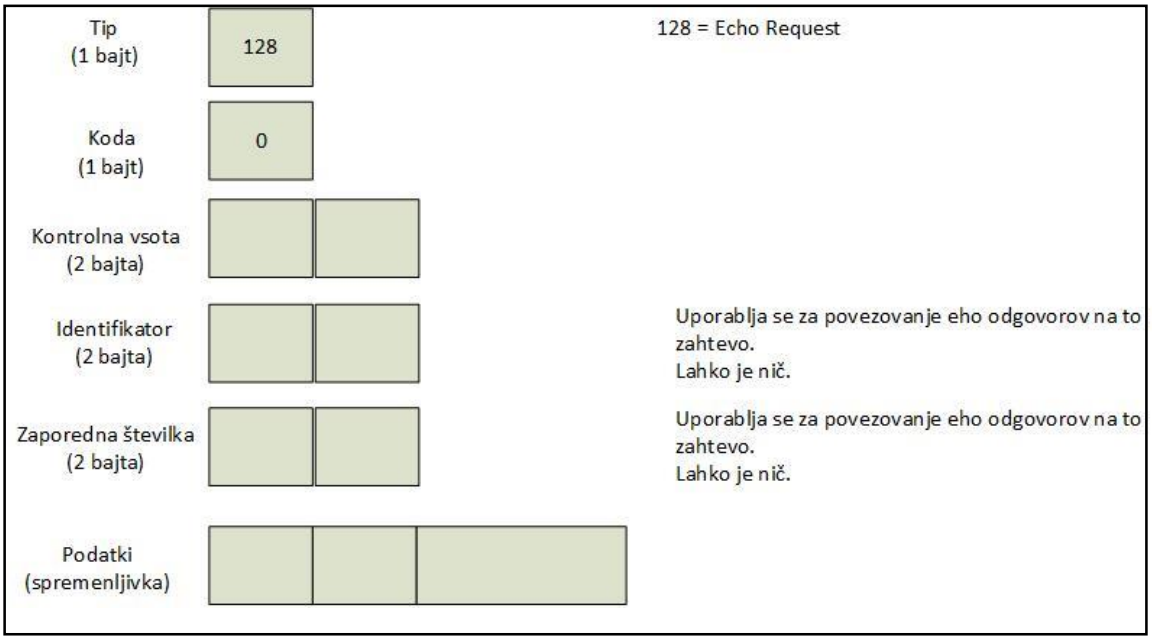
V RFC 2463 sta definirana dva tipa informativnega sporočila (angl. *Informational Messages*): sporočilo za javljanje (angl. *Echo Request Message*) in sporočilo za ponovno javljanje (angl. *Echo Reply Message*). Ostala ICMP informativna sporočila se uporabljajo za Path MTU Discovery in odkrivanje sosedov. Sporočili za javljanje in ponovno javljanje sta uporabljeni pri enem od najbolj splošno uporabljenih pomožnih programov - Packet

INternet Groper (v nadaljevanju ping). Ping je uporaben za ugotavljanje, ali je določen gostitelj na omrežju in ali je pripravljen na komunikacijo. Izvorni gostitelj tvori sporočilo za javljanje do določenega cilja, ciljni gostitelj (če je na razpolago) pa odgovori s sporočilom za ponovno javljanje (Hagen, 2006, str. 69).

#### 5.1.2.1 Sporočilo za javljanje

Format sporočila za javljanje prikazuje Slika 7.

*Slika 7: Format sporočila za javljanje*



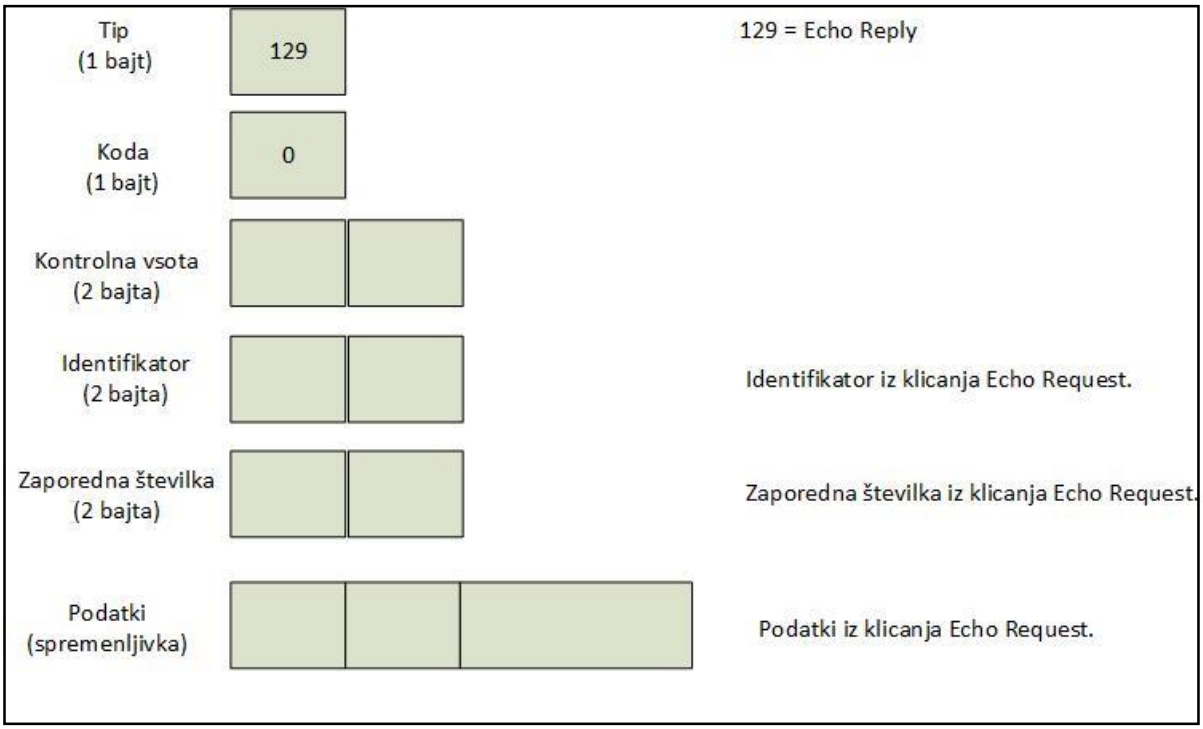

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 69, slika 4-6.*

Polje Tip je nastavljeno na vrednost 128, tj. vrednost sporočila za javljanje. Kodno polje se za to sporočilo ne uporablja, zato ima vrednost 0. Polje Identifikator in polje Zaporedna številka se uporabljata zaradi ujemanja zahtev z odgovori. Odgovor mora vedno vsebovati enako številko, kot je bila številka zahteve. Ali bosta indentifikator in zaporedna številka uporabljena in kakšne vrste okrajšanih podatkov bodo vključene v sporočilo za javljanje, je odvisno od tega, kakšen TCP/IP sklad se uporablja. Če analiziramo sledilne datoteke s sporočili za javljanje in ponovno javljanje ter če poznamo sklade, lahko z opazovanjem poljubnih podatkov določimo TCP/IP sklad pošiljatelja (Hagen, 2006, str. 69).

#### 5.1.2.2 Sporočilo za ponovno javljanje

Format sporočila za ponovno javljanje je zelo podoben formatu sporočila za javljanje in je prikazan na Sliki 8.

*Slika 8: Format sporočila za ponovno javljanje*




*Vir: S. Hagen, IPv6 Essentials, 2006, str. 70, slika 4-7.*

Polje Tip vsebuje vrednost 129 za sporočilo ponovnega javljanja. Kodno polje je neuporabljeno in nastavljeno na nič. Polje Identifikator in polje Zaporedna številka se morata ujemati s polji v zahtevi. Podatke sporočila za ponovno javljanje je potrebno preslikati v odgovor popolno in nespremenjeno. Če proces zgornjega sloja začne sporočilo za javljanje, mora odgovor skozi ta proces. Če je bilo sporočilo poslano na unicast naslov, mora imeti izvorni naslov sporočila za ponovno javljanje enak ciljni naslov kot sporočilo za javljanje. Če je sporočilo za javljanje poslano na multicast IPv6 naslov, mora biti izvorni naslov sporočila za ponovno javljanje unicast naslov vmesnika, na katerem je bilo sporočilo za javljanje sprejeto (Hagen, 2006, str. 70).

ICMPv6 sporočila za javljanje oz. ponovno javljanje so lahko avtenticirana z uporabo IPv6 avtentikacijske glave. To pomeni, da mora biti vozlišče konfigurirano tako, da ignorira neavtentikacijske ICMPv6 ping-e in omogoča zaščito proti različnim oblikam ICMPv6 napadov (Hagen, 2006, str. 70).

### 5.1.3 Pravila upravljanja procesiranja

Obstaja več pravil, ki upravljajo procesiranje ICMP (angl. *Processing Rules*) paketov. Lahko jih najdemo v RFC 2463 in so povzeti v nadaljevanju (Hagen, 2006, str. 70-71):

- Če vozlišče dobi ICMPv6 sporočilo o napaki neznanega tipa, mora to sporočilo podati zgornji plasti.
- Če vozlišče dobi ICMPv6 informacijsko sporočilo neznanega tipa, ga mora zavreči.
- Tako kot v ICMPv4 mora tudi tukaj zajeti v ICMP telo največjo možno količino sporočila o napaki. ICMP paket ne bi smel preseči minimuma IPv6 MTU.
- Če je obvestilo o napaki predano protokolu zgornje plasti, je tip protokola določen z ekstrahiranjem iz originalnega paketa (prisoten v telesu ICMPv6 sporočila o napaki). V primeru, ko tip protokola ni najden v telesu ICMPv6 sporočila (ker je prisotno preveč razširjenih glav v originalnem paketu, deli glav, ki vsebujejo tip protokola zgornjega sloja pa so obrezani), je ICMPv6 sporočilo tiho zavrnjeno.

ICMPv6 sporočilo ne sme biti poslano v naslednjih primerih (Hagen, 2006, str. 71):

- kot rezultat ICMPv6 sporočila o napaki;
- kot rezultat ICMPv6 preusmerjenega sporočila;
- kot rezultat paketa, poslanega na IPv6 multicast naslov (obstajata dve izjemi: Packet Too Big sporočilo je uporabljeno za Path MTU discovery in Parameter Problem s kodno vrednostjo 2 za neprepoznano IPv6 opcijo);
- kot rezultat paketa, poslanega kot multicast povezavnega sloja (enake izjeme kot veljajo zgoraj);
- kot rezultat pošiljanja paketa kot razpršeno oddajanje (angl. *broadcast*) povezavnega sloja (enake izjeme kot veljajo zgoraj);
- kot rezultat paketa, čigar izvorni naslov ni edinstveno identificirano enojno vozlišče; to je lahko nespecificiran IPv6 naslov, IPv6 multicast naslov ali IPv6 naslov, poznan kot anycast naslov.

Vsako IPv6 vozlišče mora implementirati funkcijo limite deležev, ki omejuje delež poslanih ICMPv6 sporočil. Konfigurirana limita je lahko časovna ali pasovno omejena. Če je ta funkcija pravilno implementirana, omogoča zaščito pred ohromitvijo strežnika (angl. *denial-of-service-attack*; Hagen, 2006, str. 71).

### 5.1.4 Funkcija odkrivanja sosedov

Odkrivanje sosedov (angl. *Neighbor Discovery* - v nadaljevanju ND) je specificirano v RFC 2461. Specifikacije v tem RFC se navezujejo na različne protokole in procese, znane

iz IPv4, ki so popravljeni in izboljšani. Prav tako so dodane nove funkcionalnosti. ND kombinira Address Resolution Protocol (ARP), ICMP Router Discovery in ICMP Redirect. Z IPv4 ni mogoče ugotoviti, ali je sosed dosegljiv, z ND protokolom pa je mehanizem za detektiranje nedosegljivosti soseda definiran. Prav tako je implementirana Duplicate IP detekcija naslova (Hagen, 2006, str. 73).

IPv6 vozlišča uporabljajo ND za naslednje namene (Hagen, 2006, str. 73):

- za določitev naslovov vozlišč druge plasti, ki so na isti povezavi;
- za najdbo sosednjih usmerjevalnikov, ki bodo posredovali njihove pakete;
- za ohranjanje sledi, kateri sosedje so dosegljivi in za detekcijo sprememb naslovov povezavnega sloja (angl. *link-layer addresses*).

Izboljšave glede na nastavitve IPv4 protokola so sledeče (Hagen, 2006, str. 74):

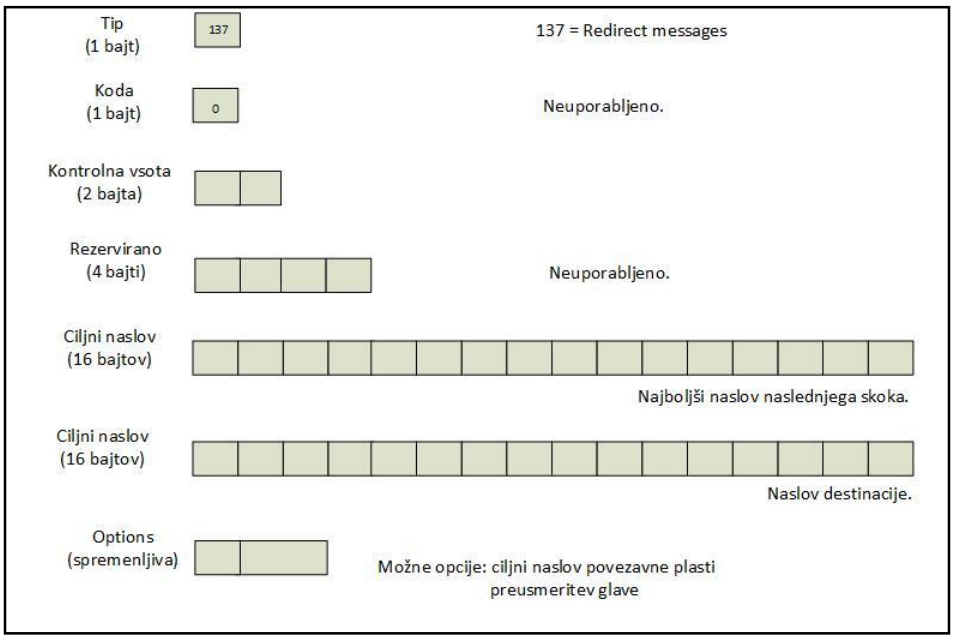
- Router Discovery je sedaj del osnovnih nastavitev protokola. Z IPv4 je moral mehanizem dobiti podatek iz usmerjevalne tabele.
- Router Advertisement paketi vsebujejo naslove povezovalnih plasti (angl. *link-layer*) za usmerjevalnik. Vozlišče ne potrebuje prejemanja Router Advertisment paketov za odpošiljanje dodatnih ARP zahtev, da bi dobil naslove povezovalnih plasti za usmerjevalnikov vmesnik. Enako velja tudi za ICMPv6 Redirect message.
- Router Advertisement paketi vsebujejo predpono povezave (tj. informacijo podomrežja). Konfiguracija maske podomrežja zato ni več potrebna. Izvede se avtomatsko preko Router Advertisement.
- Odkrivanje sosedov zagotavlja mehanizem za enostavno preštevilčenje omrežja. Nove predpone in novi naslovi so lahko uvedeni, medtem ko so stari naslovi in predpone še v uporabi, zato lahko le-te zanemarimo in odstranimo postopoma.
- Router Advertisement omogoča samostojno (angl. *stateless*) samokonfiguracijo in lahko sporoči gostitelju, kdaj naj uporabi prilagodljivo (angl. *stateful*) konfiguracijo naslova (tj. DHCP).
- Usmerjevalnik lahko oglašuje MTU za uporabo na povezavi.
- Mnogokratne predpone so lahko dodeljene eni povezavi. Že v osnovi se lahko gostitelji naučijo vse predpone iz usmerjevalnika, toda usmerjevalnik je lahko konfiguriran tako, da ne oglašuje nekaterih ali vseh predpon. V tem primeru gostitelji predpostavijo, da je neoglaševana predpona cilja oddaljena in pošljejo pakete usmerjevalniku. Usmerjevalnik lahko nato po potrebi tvori ICMP preusmeritve na sporočila.
- Detekcija nedosegljivih sosedov je del samega protokola. Trajno izboljšuje razdeljevanje paketov v primeru napake na usmerjevalniku ali na vmesniku povezave, ki je spremenila svoj povezavni naslov. Problem reši z zastarelim ARP predpomnilnikom. ND detektira padlo povezavo in izpadle usmerjevalnike ter preklopi na delujoče usmerjevalnike.

- Usmerjevalniško oglaševanje in ICMP preusmeritve uporabljajo lokalne povezavne naslove za identifikacijo usmerjevalnika. To omogoča gostiteljem, da obdržijo svoje usmerjevalniške povezave celo v primeru preštevilčenja ali uporabe novega globalnega prefiksa.
- Sporočilo odkrivanja sosedov ima vrednost limite skoka 255 in zahteve z manjšo limito skoka niso odgovorjene. To naredi ND imunega na oddaljene gostitelje, ki se poskušajo vplesti v povezavo, ker njihovi paketi zmanjšajo limito skoka, ki je na ta način ignorirana.
- Protokol odkrivanja sosedov je uporabljen za detekcijo podvojenih naslovov na povezavi.
- Standardna IP avtentikacija in varnostni mehanizem sta lahko vsebovana v odkrivanju sosedov.

### 5.1.5 Preusmerjeno sporočilo

Usmerjevalniki izvajajo ICMP preusmerjeno sporočilo (angl. *ICMP Redirect message*), da obvestijo vozlišče o boljšem prvem skoku do vozlišča na poti do danega cilja. Preusmerjeno sporočilo lahko obvesti vozlišče, da je uporabljen cilj dejansko sosed na isti povezavi in ne vozlišče oddaljenega podomrežja (Hagen, 2006, str. 79). Format ICMPv6 preusmerjenega sporočila je prikazan na Sliki 9.

*Slika 9: Format preusmerjenega sporočila*




*Vir: S. Hagen, IPv6 Essentials, 2006, str. 80, slika 4-14.*

Izvorni naslov v IP glavi mora biti naslov lokalne povezave vmesnika, iz katerega je bilo sporočilo poslano. Ciljni naslov v IP glavi je izvorni naslov iz paketa, ki je sprožil preusmerjeno sporočilo. Limita skoka je nastavljena na 225. Polje Naslov tarče (angl. *Target Address*) vsebuje naslove lokalne povezave vmesnika, ki uporablja boljši naslednji skok (angl. *better next-hop*) za dobivanje ciljnega naslova. Ciljno naslovno polje vsebuje naslove ciljev, ki so preusmerjeni, da dobimo ciljni naslov. Če sta naslova v polju Naslov tarče in v polju Ciljni naslov enaka, je cilj sosednje in ne oddaljeno vozlišče. Polje Opcija vsebuje lokalni povezavni naslov tarče (angl. *the best next-hop router*). To je izboljšava glede na verzijo IPv4, kjer mora gostitelj izvesti ločeno ARP zahtevo za določitev lokalnega povezavnega naslova naslednjega skoka usmerjevalnika (angl. *next-hop router*; Hagen, 2006, str. 80).

### 5.1.6 Samokonfiguracija

Sposobnost samokonfiguracije (angl. *autoconfiguration*) IPv6 prihrani omrežnim administratorjem ogromno dela. Oblikovan je tako, da ročna konfiguracija gostiteljev za priklop v omrežje ni potrebna. Celo večje lokacije z več omrežji in usmerjevalniki naj ne bi potrebovale DHCP strežnika za konfiguriranje gostiteljev. Sposobnost samokonfiguracije naj bi bila ključna lastnost IPv6 protokola za priključitev različnih naprav, ki uporabljajo IP naslov (TV, DVD predvajalniki, mobilni telefoni, hladilniki; Hagen, 2006, str. 87).

Samodejna samokonfiguracija (angl. *stateful autoconfiguration*) je to, kar imenujemo DHCP v IPv4 svetu. Resnično novo v IPv6 je to, da se samokonfiguracija gostiteljev izvede brez ročnega posredovanja. Nekatere konfiguracije so narejene na usmerjevalnikih, toda noben DHCP strežnik ni zahtevan za ta konfiguracijski mehanizem. Za generiranje njihovega IP naslova gostitelj uporablja kombinacijo lokalne informacije, njen MAC naslov in informacijo, pridobljeno iz usmerjevalnika. Usmerjevalniki lahko oglašujejo več predpon in gostitelji določijo informacijo od predpone iz tega oglaševanja. To omogoča preprosto preštevilčenje lokacije; spremeniti je potrebno samo predpono na usmerjevalniku – če spremenimo dobavitelja (ISP) in novi dobavitelj uporablja drugačno predpono, je potrebno usmerjevalnik prekonfigurirati tako, da oglašuje novo predpono in obdrži SLA, ki se je uporabljal s staro predpono. Vsi gostitelji, ki so povezani s tem usmerjevalnikom, se bodo sami preštevilčili skozi samokonfiguracijski mehanizem. Če tukaj ni nobenega usmerjevalnika, bo gostitelj ustvaril le lokalni povezavni naslov s predpono FE08, ki zadošča za komunikacijo vozlišč, ki so na isti povezavi (Hagen, 2006, str. 87).

Prilagodljivo (angl. *stateless autoconfiguration*) in samodejno samokonfiguracijo lahko med seboj kombiniramo, npr. gostitelj lahko uporablja prilagodljivo samokonfiguracijo za kreiranje IPv6 naslova in samodejno samokonfiguracijo za dodatne parametre. IPv6 naslov je dodeljen vozlišču za določeno življenjsko dobo. Ko življenjska doba poteče, naslov

postane neveljaven. Da zagotovimo, da je naslov edinstven na povezavi, vozlišče poganja DAD proces. DAD algoritem je definiran v RFC 2462 (Hagen, 2006, str. 87).

Kadar se vozlišče samokonfigurira, so izvedeni naslednji koraki (Hagen, 2006, str. 88):

- Lokalni povezavni naslov je generiran z uporabo lokalne povezavne predpone FE80 in dodanega indikatorja vmesnika. Ta naslov je preizkusni.
- Vozlišče združi multicast grupo vseh vozlišč (FF02::1) in povpraševano (angl. *solicited*) multicast grupo vozlišča za preizkusni naslov (iz prejšnjega koraka).
- Neighbor Solicitation sporočilo je odposlano s preskusnim naslovom kot ciljnim naslovom. IP izvorni naslov tega sporočila je naslov s samimi ničlami. IP končni naslov je multicast naslov vsiljenega vozlišča. Ta detektira, če na povezavi kakšno drugo vozlišče že uporablja ta naslov; to je DAD. Če takšno vozlišče obstaja, odgovori z Neighbor Adverisement sporočilom in samokonfiguracijski mehanizem se zaustavi. V tem primeru se zahteva ročna konfiguracija vozlišča. Če tukaj ni odgovora na Neighbor Solicitation, je varno uporabiti ta naslov. Naslov je dodeljen vmesniku in stanje naslova se spremeni v »prednosten« (angl. *preferred*). IP povezava na lokalni povezavi je sedaj vzpostavljena. Doslej je bil proces enak tako za gostitelje kot za usmerjevalnike, naslednji korak pa izvajajo samo gostitelji.
- Z namenom, da bi lahko določil, kateri usmerjevalniki so zunaj in kakšna je predpona, gostitelj pošlje Router Solicitation sporočilo vsem usmerjevalnikom multicast skupine FF02::2.
- Vsi usmerjevalniki na povezavi odgovorijo z Router Advertisement. Za vsako prepono v Router Advertisement z avtonomno konfiguracijo niza zastavic je ustvarjen naslov, ki združuje predpono in identifikator vmesnika. Ti naslovi so dodani seznamu dodeljenih naslovov za vmesnik.

Preden so dodeljeni, morajo biti vsi naslovi preverjeni z Neighbor Solicitation sporočilom (DAD). Če je naslov lokalne povezave ustvarjen skozi samokonfiguracijski mehanizem z uporabo identifikatorja vmesnika, je edinstvenost preverjena v koraku 3 in ni potrebe po njeni ponovitvi za dodatne naslove, ki uporabljajo identifikator vmesnika. Vsi ostali naslovi, ki so konfigurirani ročno ali preko prilagodljive (angl. *stateful*) konfiguracije, pa morajo biti preverjeni posamezno. Gostitelji z več naslovi (angl. *multihomed*) zato izvajajo samokonfiguracijo za vsak vmesnik posebej (Hagen, 2006, str. 88-89).

### 5.1.7 Odkrivanje največje prenosne poti

Z IPv4 lahko vsak usmerjevalnik drobi pakete, če je to potrebno. Če usmerjevalnik ne more posredovati paketa, ker je MTU naslednje povezave manjši, kot je paket, ki ga mora poslati, usmerjevalnik zdrobi paket. Razdrobi ga na kose, ki se ujemajo z najmanjšim MTU in jih odpošlje kot niz delčkov. Paket je nato ponovno sestavljen na končnem cilju.

Odvisno od načrta omrežja je lahko IPv4 paket večkrat razdrobljen na svoji poti skozi omrežje (Hagen, 2006, str. 92).

Z IPv6 usmerjevalniki ne drobijo več paketov; za to poskrbi pošiljatelj. Odkrivanje največje prenosne poti (angl. *Path MTU Discovery*) poskuša zagotoviti, da poslani paket uporablja največjo možno velikost, ki je podprta na določenem usmerjevalniku. Path MTU je najmanjša MTU povezava izmed vseh povezav od izvora do cilja. Razkritje Path MTU je opisano v RFC 1981. Proces odkrivanja deluje na sledeči način. Gostitelj domneva, da je Path MTU enak kot MTU pri prvem skoku povezave in uporabi to velikost. Če je paket prevelik za določen usmerjevalnik vzdolž poti, da bi dostavil paket naslednji povezavi, usmerjevalnik zavrže paket in pošlje nazaj ICMPv6 sporočilo - Packet Too Big. Za preklic tega, ta tip sporočila vsebuje MTU velikost naslednjega skoka povezave (angl. *next hop link*). Gostitelj sedaj uporablja MTU za pošiljanje bodočih paketov do istega cilja. Gostitelj ne bo nikoli šel pod IPv6 minimalni MTU – 1280 bitov. Proces sprejemanja Packet Too Big sporočila in reduciranje velikosti paketov se lahko zgodi več kot enkrat preden paketi dosežejo cilj. Proces odkrivanja je končan, ko paketi pridejo do končnega cilja (Hagen, 2006, str. 92-93).

Pot od danega izvora do danega cilja se lahko spreminja in zato se lahko tudi Path MTU. Manjše MTU velikosti so odkrite s prejetjem Packet Too Big sporočila. IPv6 gostitelj bo poskušal od časa do časa povečati MTU velikost, da bi bil zmožen zaznavati tudi večji Path MTU. Path MTU odkrivanje prav tako podpira multicast cilje. Če je cilj multicast, obstaja več poti, po katerih lahko kopije paketov potujejo. Vsaka izmed poti ima lahko različen Path MTU. Packet Too Big sporočilo bo ustvarjeno prav tako kot pri unicast cilju. Paketna velikost, uporabljena pri pošiljatelju, je najmanjša Path MTU v celotnem nizu ciljev (Hagen, 2006, str. 92-93).

### 5.1.8 Upravljanje multicast grup

Multicast grupni naslovi se uporabljajo kot identifikator za grupo vozlišč. Tukaj je identifikacija z najvišjim bajtom FF (angl. *high-order byte*); Hagen, 2006, str. 51).

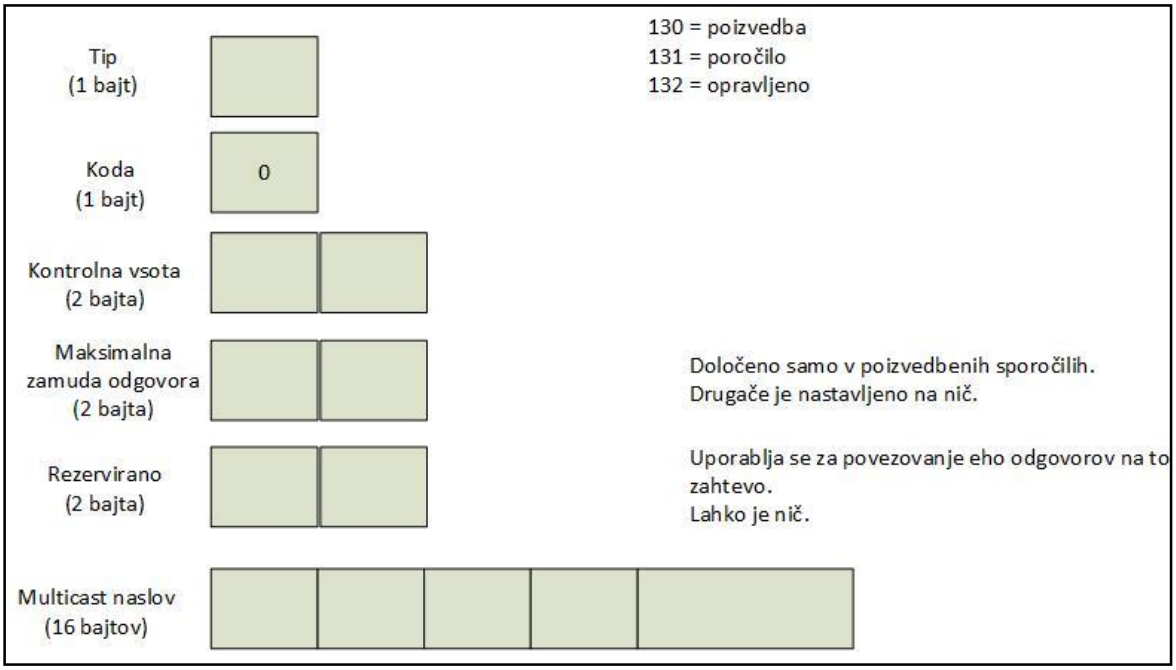
Multicast grupno upravljanje (angl. *Multicast Group Management*) v IPv4 je narejeno skozi IGMP (angl. *Internet Group Management Protocol*). IGMP verzija 2 je definirana v RFC 2236. IPv6 uporablja ICMPv6 sporočila za isto funkcionalnost; razvoj je temeljil na GMPv2 specifikacijah. Sedaj se imenuje MLD (angl. *Multicast Listener Discovery*) in je definiran v RFC 2710 (Hagen, 2006, str. 93).

Vsa MLD sporočila so poslana z izvornim IPv6 lokalnim povezavnim naslovom in mejo skoka 1, ki zagotavlja, da ostane znotraj lokalnega omrežja. Če ima paket Hop-by-Hop

Option glavo, ima Router Alert zastavico postavljeno. Tako usmerjevalnik ne bo ignoriral paketa (Hagen, 2006, str. 94).

Vsi trije tipi sporočil imajo enak format, kar je prikazano na Sliki 10.

*Slika 10: MLD format sporočila*




*Vir: S. Hagen, IPv6 Essentials, 2006, str. 95, tabela 4-19.*

Polje Tip je 130 Multicast Listener Queries, 131 za Multicast Listener Reports ali 132 za Multicast Listener Done sporočilo. Obstajata dva tipa vprašalnih sporočil. Eno je glavno vprašanje, ki se uporablja za določitev, kateri multicast grupni naslovi imajo poslušalce na povezavi. Drugi je specifično naslovno vprašanje, ki se uporablja za ugotavljanje ali so tukaj poslušalci za specifičen naslov na povezavi. Polje Maximum Response Delay je uporabljeno samo v vprašalnem sporočilu. To je maksimalno dovoljena zakasnitev (v milisekundah) v katerem mora gostitelj poslati poročilo, če ima poslušalca. V vseh ostalih sporočilih je to polje nastavljeno na nič. Multicast Address polje je nastavljeno na nič v generalnem vprašanju. V naslovno specifičnem vprašanju, vsebuje multicast grupni naslov za vprašanje. V poročanem in narejenem sporočilu, to polje vsebuje multicast grupo kateri član posluša ali grupa je zapustila. Usmerjevalniki uporabljajo MLD za odkrivanje kateri multicast naslov ima poslušalce na vsaki svoji povezavi. Za vsako pritrjeno povezavo, usmerjevalniki obdržijo seznam poslušalčevih naslovov. Glavno vprašanje je poslano na multicast naslov FF02::1 na lokalnem povezavnem območju vseh vozlišč. Katerakoli postaja, ki hoče poslati poročilo v odgovor na vprašanje, najprej zažene merilnik časa (angl. *timer*). Preden pošlje poročilo, predpostavi čas čakanja. Maksimalna zakasnitev je tista, ki je specificirana v polju Maximum Response Delay v vprašanju. Če znotraj te

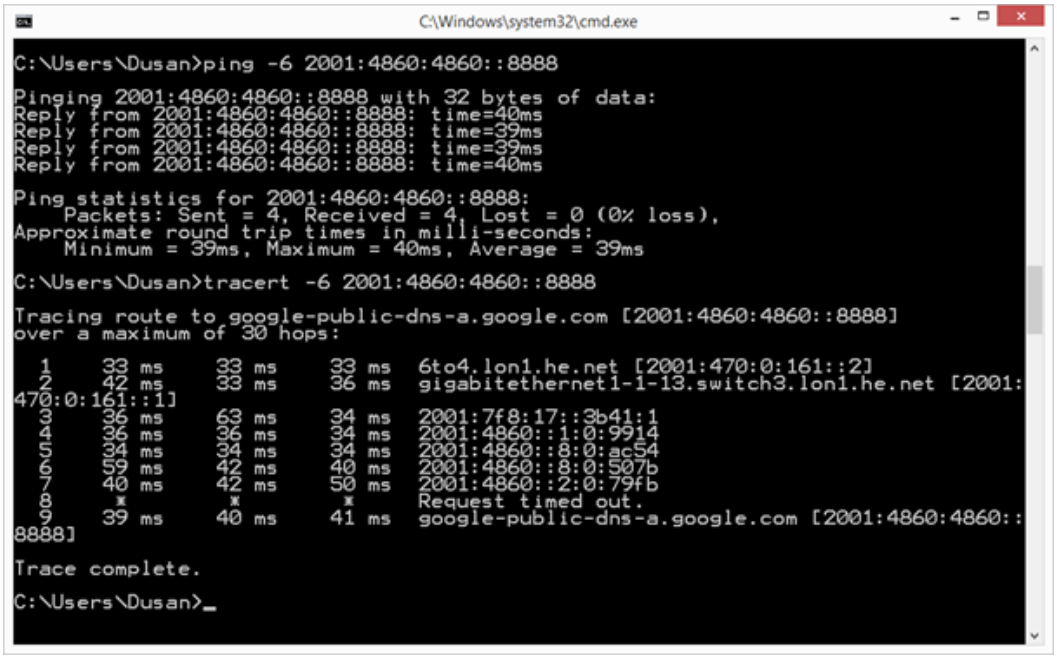
zakasnitve postaja zasledi drugo postajo, ki že pošilja poročilo, proces zaustavi (Hagen, 2006, str. 94-95).

## 5.2 Naloge in storitve IPv6 internetnega protokola za nadzor prenosa

IPv6 vozlišča uporabljajo večnamenski ICMPv6 protokol, ki podpira 36 kontrolnih funkcij, a naprave uporabljajo ICMPv6 sporočila večinoma za naslednje osnovne funkcije (Podporni in nadzorni protokoli, 2016):

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

*Slika 11: Primer ukaza PING in TRACERT (TRACEROUTE)*




Na požarnem zidu se ICMPv6 sporočil o napakah ne sme blokirati, saj ima ICMP ključno vlogo pri vzpostavitvi komunikacije. To je ravno nasprotno kot pri IPv4, kjer je ta protokol na požarnem zidu običajno onemogočen.

# 6 MEHANIZMI PREHODA OMREŽIJ IZ STAREGA V NOVI SISTEM IP

Navkljub vsem prizadevanjem za zmanjševanje izrabe naslovnega prostora IPv4, je ta skoraj povsem izčrpan. Edina dolgoročna rešitev je prehod na IPv6, ki ponuja dovolj velik naslovni prostor ($3.4 \times 10^{38}$) za vse naprave, ki jih želimo povezati v internet. IPv6 je protokol, ki je bil standardiziran že leta 1998 z RFC2460, vendar do danes ni doživel masovne vpeljave. Temeljni problem širjenja IPv6 protokola je v tem, da sta protokola IPv4 in IPv6 med seboj nezdružljiva. To pomeni, da naprave, ki podpirajo samo protokol IPv4, ne morejo neposredno komunicirati z napravami, ki podpirajo samo protokol IPv6. To težavo razrešujemo s pomočjo translacijskih in tunelskih mehanizmov, ki predstavljajo dodatne stroške.

Prehod na novi protokol zahteva dodatna znanja in sredstva za postavitev in vzdrževanje sistema, zato je odločilnega pomena motivacija uporabnikov. Ti so pogosto pomanjkljivo zavzeti za izvedbo prehoda v primeru, kadar jim ne primanjkuje naslovnega prostora, saj druge prednosti, ki jih prinaša novi protokol, niso dovolj očitne.

## 6.1 IPv4/IPv6 tehnike dvojnega protokolnega sklada

V načinu dvojnega protokolnega sklada (angl. *dual-stack*) naprava podpira oba protokolna sklada in ima dodeljene tako IPv4 kot IPv6 naslove. Z napravami, ki podpirajo samo IPv6, komunicira preko IPv6 omrežja, z napravami, ki podpirajo samo IPv4, pa preko IPv4 omrežja. Prednost načina dvojnega protokolnega sklada je v tem, da je skladen s skoraj vsemi aplikacijami. Omogoča veliko mero fleksibilnosti in je osnova za večino ostalih mehanizmov prehoda, pod pogojem, da obstaja vsaj en gostitelj z dvojnim protokolnim skladom. Po kompletni nadgradnji na IPv6, se IPv4 protokol preprosto onemogoči ali odstrani (Hagen, 2006, str. 255-256).

Glavna slabost načina dvojnega protokolnega sklada je po drugi strani v tem, da je treba na omrežni infrastrukturi vzdrževati dva ločena protokola, za IPv6 in za IPv4. To pomeni, da je potrebno na gostitelju zagotoviti večjo procesorsko moč in dodaten spomin. Vse tabele so shranjene dvakrat, za vsak protokol posebej. DNS strežnik mora razrešiti tako IPv4 kot IPv6 naslove. Vse aplikacije, ki tečejo na gostitelju, ki ima naložena oba IP protokola, morajo biti sposobne ugotoviti, ali komunikacija poteka z IPv4 ali IPv6 napravo. Vsaki napravi, ki je del takega omrežja, je treba določiti vse parametre za nastavitev - tako za IPv4 kot tudi za IPv6. Vse to prinaša večje stroške vzdrževanja. Prav tako moramo biti pozorni pri nastavitvi požarnega zidu. Postavljen mora biti tako, da varuje obe omrežji. Prav tako moramo imeti ločeno varnostno politiko in za vsak protokol svoja pravila dostopanja (Hagen, 2006, str. 256).

## 6.2 Metode in tehnike tuneliranja

Tunelski mehanizmi uporabljajo tehniko ovijanja (angl. *encapsulation*) IPv6 paketov v IPv4 pakete. Na ta način omogočajo povezavo IPv6 gostiteljev ali IPv6 omrežij skozi IPv4 omrežja. Poleg tega lahko to tehniko uporabimo za vzpostavitev posameznih IPv6 otokov znotraj omrežja, medtem ko je hrbtenica omrežja še vedno IPv4. Na takšen način lahko naredimo postopen prehod iz IPv4 omrežja v IPv6 omrežje (Hagen, 2006, str. 256).

Proces ovijanja ima tri komponente (Hagen, 2006, str. 256):

- ovijanje (angl.e*ncapsulation*) na začetni točki tunela;
- odvijanje (angl. *decapsulation*) na končni točki tunela;
- management tunela.

Tako je tuneliranje uporabno za prenos IPv6 prometa, ovitega z IPv4 paketi in poslanega preko IPv4 infrastrukture usmerjanja. Paketi so usmerjeni glede na informacijo, ki je zapisana v glavi tunelskega mehanizma (Hagen, 2006, str. 257).

Tunelske mehanizme delimo na (Hagen, 2006, str. 257):

- **Ročno konfigurirano tuneliranje IPv6 preko IPv4 protokola**. IPv6 paketi so oviti v IPv4 pakete, ki se prenesejo prek IPv4 usmerjevalne infrastrukture. To so tuneli točka-točka (angl. *point-to-point*), ki morajo biti ročno konfigurirani.
- **Samodejno tuneliranje IPv6 preko IPv4**. IPv6 vozlišča lahko uporabijo različne vrste naslovov, kot so 6v4 ali ISATAP naslovi, za dinamično tuneliranje IPv6 paketov preko IPv4 usmerjevalne infrastrukture. Povezava med robnimi omrežji se vzpostavi avtomatsko (po potrebi).

Usmerjevalniki, ki omogočajo tuneliranje, pakete pred izhodom iz izvornega omrežja ovijejo (angl. *encapsulation*) v druge pakete (v drug protokolni sklad) in jih posredujejo naprej proti drugi končni robni napravi tunela, kjer se paketi zopet odvijejo (angl. *decapsulation*) v izvorno obliko. Paketi se usmerjajo po omrežju glede na informacijo, ki je zapisana v glavi tunelskega mehanizma (Hagen, 2006, str. 258).

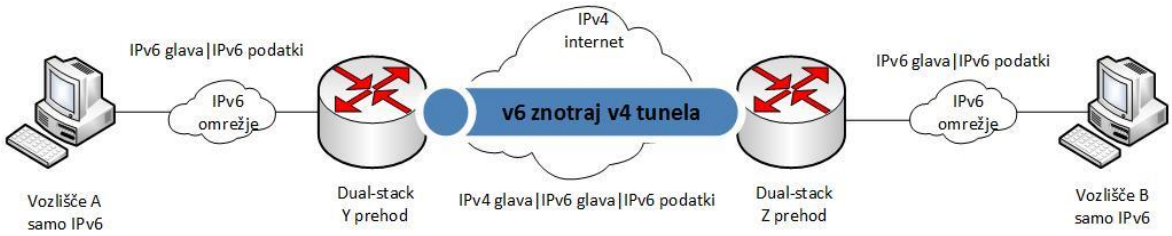
## 6.3 Ostale tehnike prehoda

V nadaljevanju so pregledno predstavljene še preostale tehnike prehoda na uporabo protokola IPv6.

### 6.3.1 Ročno tuneliranje

Statični tuneli zahtevajo, da sta usmerjevalnika z dvojnim skladom (angl. *dual-stack*) sposobna oviti in odviti IPv6 pakete v IPv4 pakete Za tunele, ki gredo skozi globalni internet velja, da mora biti vsaka končna točka tunela povezana z vsaj enim javnim IPv4 naslovom, ki ima možnost globalnega usmerjanja (Loshin, 2004, str. 327). Za bolj poglobljeno razumevanje si oglejmo primer, ki ga prikazuje Slika 12.

*Slika 12: Statično tuneliranje IPv6 skozi IPv4 infrastrukturo*




*Vir: Cisco Systems, Inc., Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S, 2014, str. 22, slika 1.*

Obe končni IPv6 vozlišči A in B sta med seboj ločeni z IPv4 omrežjem. Za izmenjavo paketov med A in B je potrebno vzpostaviti 6preko4 (angl. *6over4*) statični tunel med dvema usmerjevalnikoma dvojnega sklada, ki se nahajata na obeh koncih IPv4 omrežja. Vozlišče A lahko pošlje IPv6 pakete, namenjene vozlišču B, lokalnemu usmerjevalniku dvojnega sklada Y, ki ovije A IPv6 pakete v IPv4 pakete. Ti paketi so nato usmerjeni preko IPv4 omrežja na usmerjevalnik Z, ki z izluščenjem IPv4 glave obnovi izvirne IPv6 pakete in jih pošlje naprej na njegov prvotni IPv6 cilj, tj. vozlišče B (Loshin, 2004, str. 327).

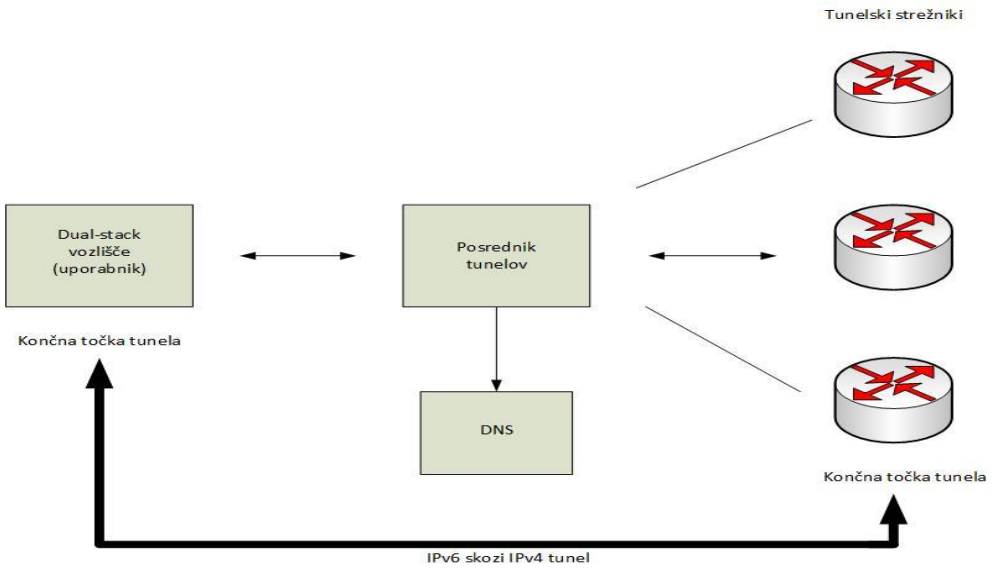
Statični tuneli so pogosto zgrajeni med usmerjevalniki, ki so pod kontrolo različnih skrbnikov omrežja. V tem primeru morajo skrbniki končnih tunelskih usmerjevalnikov izmenjati IPv4 in IPv6 informacijo o končnih tunelskih točkah ter konfigurirati svoje usmerjevalnike tako, da se bo vzpostavil statičen tunel. Statično tuneliranje je lahko pomemben mehanizem za gradnjo mostov, ki omogočajo IPv6 pretok prometa skozi IPv4 omrežje. Statični tuneli so enostavni za konfiguracijo in zahtevajo zelo malo administratorskega dela. Zahtevajo pa ločeno konfiguracijo tunela za vsak izoliran IPv6 mrežni cilj. Rezultat tega je, da niso široko uporabni. V primerih, kjer je potrebno povezati več kot le peščico IPv6 lokacij, je veliko bolj primerna metoda samodejnega tuneliranja (Loshin, 2004, str. 327-328).

### 6.3.2 Posrednik tunelov

Tunelske posrednike (angl. *Tunnel Broker*) lahko razumemo kot virtualne ponudnike, ki ponujajo povezljivost v IPv6 omrežje uporabnikom, ki že imajo IPv4 internetno povezavo. Njihovo delovanje je določeno z RFC 3053 (Hagen, 2006, str. 271).

Pri storitvi posredništva tunela se uporabnik, ki uporablja operacijski sistem z dvojnim skladom, poveže na posredovalni strežnik, kjer se registrira. Registracija se mora overiti s standardnimi postopki (npr. RADIUS). Na ta način se je mogoče izogniti nedovoljeni uporabi storitev tunela. Z registracijo uporabnik pridobi ustrezne konfiguracijske parametre, na podlagi katerih lahko vzpostavi tunel skozi IPv4 omrežje med svojo delovno postajo oz. robnim usmerjevalnikom in končno robno točko posrednika tunela. Ponudnik oz. posrednik tunela periodično preverja status tunela in tunelskega gostitelja. V primeru, da gostitelj te storitve ne uporablja, jo ponudnik lahko sprosti in ponudi drugemu uporabniku. Tunelski posredniki lahko delijo breme podatkov preko več tunelskih strežnikov. Tunelski posrednik mora biti dosegljiv z IPv4 naslovom, lahko pa ima tudi IPv6 naslov, vendar ta ni nujno potreben. Komunikacija med posredovalnim tunelom in tunelskimi strežniki lahko poteka bodisi preko IPv4 bodisi preko IPv6. Tunelski strežnik je usmerjevalnik dvojega sklada, povezan s svetovnim internetom. Odjemalec je gostitelj dvojnega sklada ali usmerjevalnik, povezan z internetom preko IPv4. Mehanizem tunelskega posredovanja (angl. *Tunnel Broker*) je namenjen manjšim in izoliranim omrežjem IPv6 in posameznim, izoliranim IPv6 gostiteljem. Deluje samo z javnimi IPv4 naslovi. Če se uporabljajo zasebni naslovi, je potrebno uporabiti drug mehanizem, npr. Teredo (Hagen, 2006, str. 272-273).

*Slika 13: Posrednik tunelov*




*Vir: RidgeRun SDK IPv6 guide, 2016, slika 4.*

### 6.3.3 Mehanizem 6v4

Mehanizem 6v4 IPv6 območjem omogoča, da lahko po IPv6 komunicirajo med seboj tudi skozi IPv4 omrežja, in sicer preko avtomatsko nastavljivega tunela. Mehanizem 6v4 celotno IPv4 omrežje interneta pojmuje kot povezavo, kjer je možno oddajanje samo enemu prejemniku. Domorodne IPv6 domene med seboj komunicirajo preko 6v4 usmerjevalnikov, imenovanih tudi 6v4 prehodi. Na samih gostiteljih ni potrebno uvesti nobenih sprememb. Ta mehanizem je mehanizem tranzicije in naj bi se uporabljal samo v obdobju soobstoja protokolov IPv4 in IPv6. Paketi IPv6 se vdelajo v IPv4 na samih prehodih 6v4. Za to konfiguracijo je potreben vsaj en unikaten globalen IPv4 unicast naslov. IANA je dodelila posebno predpono za 6v4 shemo 2002:: /16 (Hagen, 2006, str. 264-266). Podrobnosti prikazuje Slika 14.

*Slika 14: Oblika 6v4 predpone*

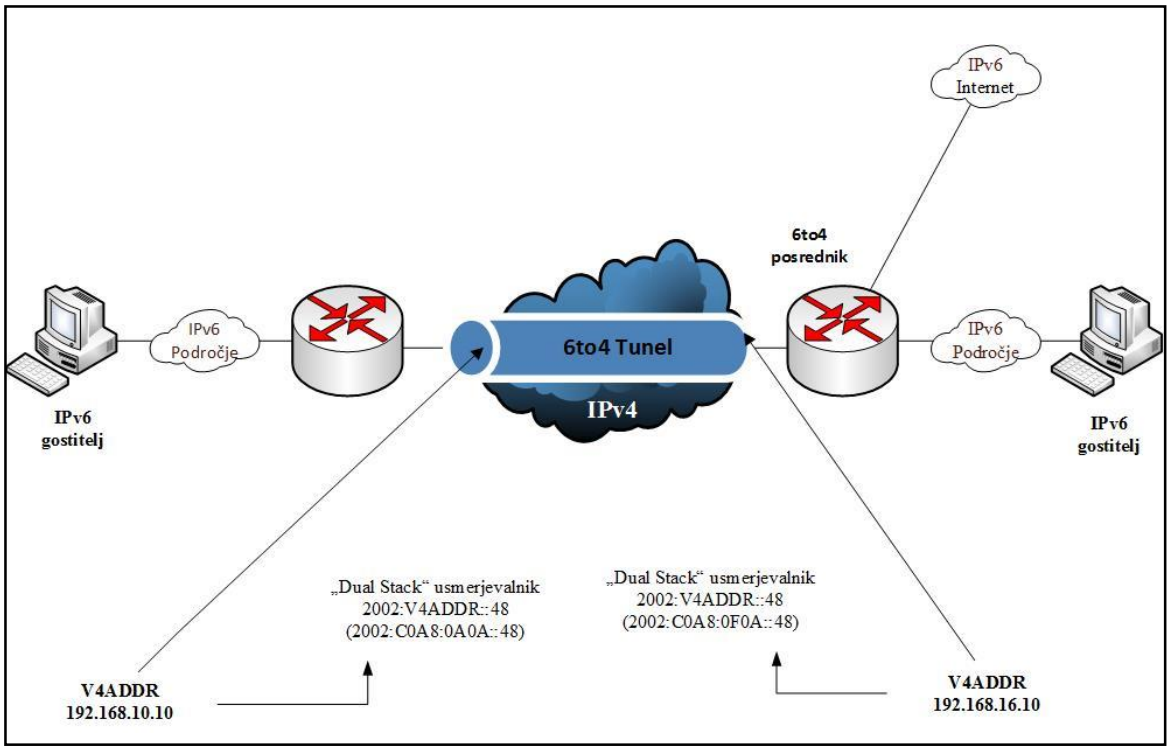
| 3biti | 13bitov | 32bitov | 16bitov | 64bitov |
|---|---|---|---|---|
| FP 001 | TLA 0x0002 | IPv4 naslov | SLA ID | ID vmesnika |
| Dolžina predpone: 48 bitov<br>Zapis: 2002:V4ADDR::/48 | | | | |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 265, slika 10-7.*

32-bitni predponi sledi IPv4 naslov prehoda v heksadecimalni vrednosti. Tako ostane 80 bitov naslovnega področja za lokalno omrežje. 16 bitov se lahko uporabi za lokalno omrežno naslavljanje, kar pomeni, da se lahko kreira 65,536 omrežij. Preostalih 64 bitov se uporabi za identifikacijo vmesnikov lokalnih vozlišč lokalnega omrežja. To pomeni, da imamo lahko 264 vozlišč na posameznem omrežju. Razširjeni naslovni prostor ima nekaj prednosti. Sedaj lahko vsak gostitelj na svojem omrežju komunicira z 6v4 gostitelji na internetu (Hagen, 2006, str. 264).

Ko vozlišče iz omrežja 6v4 želi komunicirati z vozliščem v drugem 6v4 omrežju, konfiguracija predora ni potrebna. Vstopna točka tunela prevzame IPv4 naslov izhodne točke tunela iz naslova IPv6 cilja. Za komunikacijo IPv6 vozlišča z oddaljenim IPv6 omrežjem potrebujete 6v4 posrednika - preklopni usmerjevalnik (angl. *relay router*). Posrednik je usmerjevalnik, konfiguriran za 6v4 in IPv6, ki povezuje 6v4 omrežje z izvornim (angl. *native*) IPv6 omrežjem (Hagen, 2006, str. 265).

*Slika 15: Medsebojno povezovanje 6v4 področja z izvornim IPv6 področjem*




*Vir: Transition Mechanisms (IPv6) Part 2, 2016, slika 3-8.*

### 6.3.4 Mehanizem IPv6 za hitro ukrepanje

Mehanizem IPv6 za hitro ukrepanje (angl. *Rapid Deployment* - v nadaljevanju 6rd), ki ga opredeljuje RFC5569, je migracijska tehnika, ki omogoča IPv6 povezljivost skozi obstoječe IPv4 omrežje. Mehanizem ima podoben koncept kot mehanizem 6v4, vendar predvideva določene spremembe. Mehanizem omogoča ponudniku storitev hitro uvedbo IPv6 (unicast) storitev, pri čemer lahko naročniki sočasno koristijo tako IPv6 kot IPv4 storitve (Kunc, 2010).

Arhitektura 6rd je sestavljena iz (Kunc, 2010):

- CPE usmerjevalnih prehodov (angl. *router gateway*) s podporo 6rd, ki omogočajo »softwire« ovijanje paketov IPv6 v IPv4 (izvedba poteka na strani naročnikov);
- enega ali več 6rd prehodov (lahko so nadgrajeni 6v4 posredniki), ki omogočajo zaključevanje oz. terminiranje tunelov in usmerjanje IPv6 paketov v IPv6 omrežje;
- obstoječega dostopovnega IPv4 omrežja ponudnika.

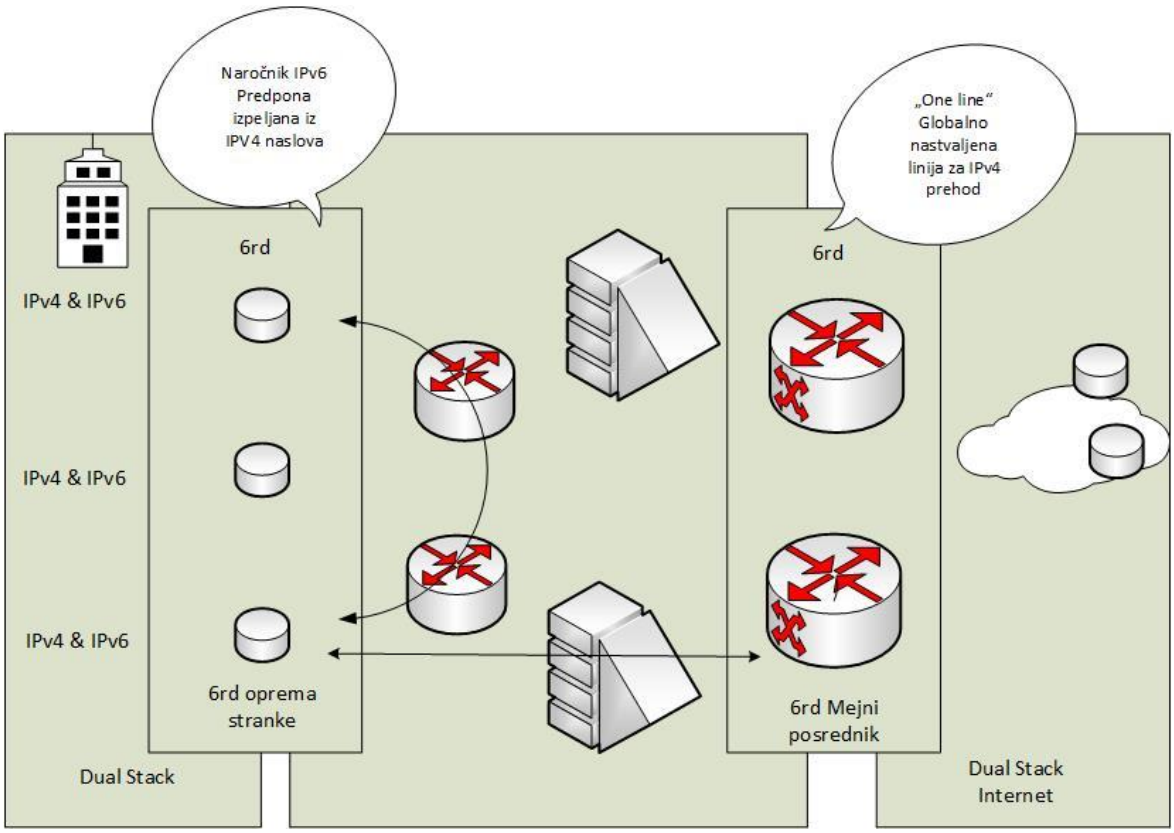
Pri 6v4 mehanizmu 6v4 gostitelj ali usmerjevalnik uporablja globalno oz. fiksno predpono, ki se začne z vrednostjo 2002::/16, pri mehanizmu 6rd pa ponudnik storitve uporablja

specifično IPv6 predpono iz svojega regionalnega internetnega registrarja. 6rd naslov CPE naprave je tako sestavljen iz (Kunc, 2010):

- ponudnikove IPv6 predpone (/26);
- unikatnega globalnega IPv4 naslova, ki je dodeljen CPE napravi;
- naslova, ki ga določajo ID podomrežja;
- ID vmesnika.

6rd mehanizem v obdobju prehoda na čisti IPv6 predstavlja za internetne ponudnike zelo obetaven način zagotavljanja IPv6 povezljivosti. V svoje omrežje ga je zelo uspešno v zgolj petih tednih implementiral francoski internetni ponudnik Free. Po podatkih naj bi imelo IPv6 povezljivost preko mehanizma 6rd tako omogočeno preko 1.500.000 Free-jevih rezidenčnih naročnikov. Vse kaže, da bo mehanizem 6rd v prvi fazi tranzicije v svoje produkcijsko omrežje vpeljal tudi Comcast, največji ameriški kabelski ponudnik internetnih storitev (Kunc, 2010). Pregled 6rd delovanja je podrobneje prikazan na Sliki 16.

*Slika 16: Pregled 6rd delovanja*




*Vir: Cisco Systems, Inc, IPv6 Rapid Deployment: Provide IPv6 Access to Customers over an IPv4-Only Network, 2011, str. 1, slika 1.*

Kot prikazuje Slika 16, usmerjevalnik BR omogoča povezljivost med usmerjevalniki CE in omrežjem IPv6 (javni ali zasebni internet). Tako usmerjevalniki CE kot usmerjevalniki BR so naprave dvojnega sklada. Naprave med temi usmerjevalniki so lahko samo IPv4. Pri usmerjevalnikih CE velja sledeče: Če se ciljni naslov paketa IPv6 ujema z lokalno nastavljeno predpono 6rd, potem se paket smatra kot del lokalne domene 6rd in je posredovan drugemu usmerjevalniku CE. V tem primeru se naslov IPv4, ki je vključen v ciljni naslov IPv6, uporablja kot ciljni naslov IPv4 tunela 6rd. Lokalni vmesnik WAN naslova IPv4 se uporabi kot izvorni naslov za tunel 6rd, ki je paket IPv6, direktno ovit v IPv4. Če se ciljni naslov IPv6 ne ujema z lokalno nastavljivo predpono 6rd ali z drugimi besedami, če paket ne pripada lokalni domeni 6rd, potem bo tuneliran usmerjevalniku BR preko tunela 6rd. V tem primeru je lokalno nastavljen BR-jev naslov IPv4 uporabljen kot ciljni naslov za oviti paket na usmerjevalniku CE (Cisco Systems, 2011).

Običajno 6rd uporabljajo le odjemalci ponudnikovega lastnega omrežja. V tem primeru ponudnik lahko zagotavlja kvaliteto storitev, saj so vsi prehodi pod njegovim upravljanjem.

### 6.3.5 Protokol samodejnega naslavljanja tunela znotraj organizacije

Protokol samodejnega naslavljanja tunela znotraj organizacije (angl. *Intra-Site Automatic Tunnel Addressing Protocol* - v nadaljevanju ISATAP) je specificiran v RFC 4214 in dopolnjen s sedanjim standardom RFC 5214. ISATAP je zasnovan za vozlišča z dvojnim skladom, ki so ločena samo z infrastrukturo IPv4. ISATAP omogoča gostiteljem avtomatsko tuneliranje z uporabo katerekoli oblike IPv4 naslova (zasebni ali javni). ISATAP uporablja identifikator tipa 0xFE za določanje naslova IPv6 z vgrajenim naslovom IPv4 (Hagen, 2006, str. 46). Oblika ISATAP naslova je prikazana na Sliki 17.

*Slika 17: Oblika ISATAP naslova*

| 64 bitov | 32 bitov | | 32 bitov |
|---|---|---|---|
| Predpona | 00 00 5E FE<br>02 00 5E FE | Naslov IPv4 | |
| 00: zasebni naslov IPv4<br>02: javni naslov IPv4<br>00 00 5E: IANA OUI<br>FE: Identificira naslov IPv6 z vgrajenim naslovom IPv4 | | | |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 46, slika 3-4.*

Prvim 64 bitom sledi oblika globalnega naslova unicast. IANA je lastnica OUI (angl. *Organizationally Unique Identifier*) 00-00-5E in določa obliko EUI-48 identifikatorja

vmesnika, dodeljenega v tem OUI. Znotraj prvih 16 bitov tip identifikatorja pokaže, ali je naslov IPv4 iz zasebnega območja (0000) ali je globalno enoličen (0200). Naslednjih 8 bitov vsebuje tip identifikatorja, ki označuje, da je to naslov IPv6 z vgrajenim naslovom IPv4. Tip identifikatorja je 0xFE. Zadnjih 32 bitov vsebuje vgrajen naslov IPv4, ki je zapisan v "pika" decimalnem zapisu ali v heksadecimalni obliki. Predpostavimo, da imamo gostitelja z naslovom IPv4 192.168.0.1, ki ima dodeljeno 64-bitno predpono 2001:DB8:510:200::/64. Naslov ISATAP za tega gostitelja je 2001:DB8:510:200:0:5EFE:192.168.0.1. Lahko uporabimo tudi heksadecimalno predstavitev naslova IPv4. V tem primeru je naslov zapisan na sledeči način: 2001:DB8:510:200:0:5EFE:C0A8:1. Povezavno-lokalni (angl. *link-local*) naslov za tega gostitelja je FE80::5EFE:192.168.0.1. (Hagen, 2006, str. 46-47).

ISATAP vmesnik oblikuje ISATAP identifikator vmesnika iz svojega IPv4 naslova in ga uporabi za kreiranje povezavno-lokalnega ISATAP naslova. Pri tem je v uporabi mehanizem za odkrivanje sosedov, določen v RFC 2461 (odkrivanje predpon in usmerjevalnikov). Z uporabo ISATAP lahko gostitelji IPv6 v IPv4 intranetu komunicirajo med seboj. Če pa želijo komunicirati z IPv6 gostitelji na internetu, kot so 6Bone gostitelji, mora biti primerno nastavljen mejni usmerjevalnik (angl. *Border Router*). To je lahko ISATAP usmerjevalnik ali 6v4 prehod (angl. *Gateway*). IPv4 naslovi znotraj področja so lahko javni, ni pa nujno. Vgrajeni so v naslov s standardno prepono in so zato edinstveni. Velikemu številu ISATAP gostiteljev se lahko dodeli samo ena ISATAP predpona. Če uvedemo IPv6 na posameznem segmentu omrežja organizacije, lahko nastavimo IPv6 vozlišče, ki ima ISATAP vmesnik, da deluje kot usmerjevalnik med izvornim IPv6 segmentom in ISATAP gostitelji v IPv4 segmentih (Hagen, 2006, str. 267).

Mehanizem ISATAP je podprt v Microsoftovih operacijskih sistemih (od Windows XP dalje) in v posameznih Linux distribucijah (od Linux-2.6.25 dalje).

### 6.3.6 Protokol Teredo

Bistvena razlika med Teredom in doslej omenjenimi protokoli je v tem, da Teredo omogoča dostop do IPv6 gostiteljev skozi eno ali več NAT plasti s tuneliranjem paketov preko UDP protokola. Specificiran je z RFC 4380 (Hagen, 2006, str. 267-268).

Številni uporabniki interneta, še posebej mnogi uporabniki doma, dostopajo do interneta skozi NAT. Uporaba NAT-a je z vidika tuneliranja IPv6 skozi IPv4 infrastrukturo vprašljiva vsaj iz dveh razlogov: (1) NAT uporabniki imajo zasebne IPv4 naslove in (2) veliko NAT naprav ima nastavljene varnostne filtre, ki blokirajo neželen promet (Hagen, 2006, str. 268).

Pri tuneliranju je IPv6 paket koristna vsebina IPv4. Mehanizem, kot je 6v4, pogosto ne deluje v takem okolju, ker zahteva splošen IPv4 naslov. 6v4 lahko deluje samo v NAT okolju, kjer sta usmerjevalnik 6v4 in NAT skupaj v eni napravi. V vseh ostalih primerih mora biti izbran drug mehanizem; eden od teh je Teredo (Hagen, 2006, str. 268). Posamezne končne naprave, ki uporabljajo Teredo, dobijo IPv6 naslov iz bloka 2001:0::/32. V naslov so zakodirane različne informacije, ki povedo Teredo prehodu, kam naj pošilja prejete pakete. Teredo je zasnovan kot zadnja translacijska tehnologijo za povezljivost z IPv6. Če že imamo izvorno IPv6, 6v4 ali ISATAP povezavo, potem gostitelj ne deluje kot Teredo odjemalec. Več kot bo nadgrajenih IPv4 robnih naprav za podporo 6v4 in bolj, ko bo razširjena IPv6 povezljivost, vse manj se bo Teredo uporabljal, dokler njegova uporabo ne bo več potrebna (Microsoft, 2007).

*Slika 18: Oblika Teredo naslova*

| 32 bitov | 32 bitov | 16 bitov | 16 bitov | 32 bitov |
|---|---|---|---|---|
| Predpona | IPv4 naslov strežnika | Zastavice | Vrata | IPv4 naslov odjemalca |
| Predpona Teredo strežnika | IPv4 naslov Teredo strežnika | Specifičen naslov in vrsta NAT-a | Mapirana UDP vrata odjemalca | IPv4 naslov odjemalca |

*Vir: S. Hagen, IPv6 Essentials, 2006, str. 270, slika 10-10.*

Teredo servisna predpona ima 32 bitov in je 2001:0000::/32. IPv4 polje strežnika je dolžine 32 bitov in vsebuje IPv4 naslov Teredo strežnika. Polje Zastavice ima 16 bitov ter določa naslov in vrsto NAT-a, ki se uporablja. 16-bitno polje za vrata (angl. *port*) vsebuje mapirana UDP vrata Teredo servisa na odjemalcu. IPv4 polje odjemalca vsebuje mapiran IPv4 naslov odjemalca. Biti v polju Vrata in polju naslova odjemalca so »zmedena«. Številka vrat je obrnjena, kakor tudi vsak bit v naslovu odjemalca (Hagen, 2006, str. 270).

## 6.4 Preslikava naslovov

Translacijske mehanizme prištevamo med tranzicijske mehanizme, ki omogočajo IPv4 in IPv6 gostiteljem, da lahko med seboj učinkovito komunicirajo.

### 6.4.1 Osnove mehanizma prevajanja omrežnih naslovov in vrat

Zaradi potrebe po ločevanju javnih in zasebnih naslovov IP je bil v omrežjih IPv4 leta 1994 pripravljen RFC 1631, ki opredeljuje mehanizem prevajanja omrežnih naslovov (angl. *Network Address Translation* - v nadaljevanju NAT). Slednji izvaja prevajanje javnih naslovov IPv4 v zasebne – in obratno. Najpogosteje je bil implementiran kot funkcionalnost usmerjevalnikov in požarnih zidov. Poleg tega poznamo tudi mehanizem prevajanja omrežnih naslovov in vrat (angl. *Network Address Port Translation* – v nadaljevanju NAPT), ki ne prevaja zgolj naslovov IP, temveč tudi številke vrat. Do njegove razširjene uporabe je prišlo zaradi pomanjkanja prostih javnih naslovov IPv4. Usmerjevalnik, ki uporablja funkcionalnost NAPT, analizira komunikacijski promet, pretakajoč preko njegovih vmesnikov, in gradi tabelo povezav oz. sej med gostitelji zasebnega in javnega omrežja. V primerih, ko zahtevo pošlje gostitelj iz javnega omrežja, si naprava NAPT v svojo tabelo zapiše izvorni naslov IPv4, vrata TCP/UDP, s katerih je prišla zahteva, sekvenčno številko TCP in njeno razliko ter časovno oznako. Nato sledi korak, v katerem se prejetemu paketu zamenja zasebni naslov IPv4 z javnim. Ob tem se zamenja tudi številka vrat in izračuna kontrolna vsota (angl. *checksum*) glave IP in TCP. Pri odzivu strežnika v javnem omrežju je postopek izveden ravno v obratnem vrstnem redu (Kunc, 2010, str. 26).

Ker ima vsaka aplikacija svoje posebnosti, obstajajo različne izvedbe prevajanja IP, TCP/UDP glav. NAT naprave morajo praviloma podpirati vsaj naslednje značilnosti prevajanja (Kunc, 2010, str. 27):

- transparentno dodeljevanje naslovov (angl. *Transparent Address Assignment*);
- statično dodeljevanje naslovov (angl. *Static Address Assignment*);
- dinamično dodeljevanje naslovov (angl. *Dynamic Address Assignment*);
- transparentno usmerjanje (angl. *Transparent Routing*);
- prevajanje ICMP paketov (angl. *ICMP Error Packet Translatio*n).

Ena izmed poglavitnih značilnosti NAPT je uporaba multipleksirane dinamične tabele. Če ga primerjamo z NAT, lahko sklepamo, da je varnejši, saj spremlja transportne identifikatorje in zunanjemu gostitelju onemogoča dostop do katerihkoli notranjih vrat (Kunc, 2010, str. 27).

### 6.4.2 Pristop prevajanja omrežnih naslovov Large Scale

V sklopu pristopa prevajanja omrežnih naslovov Large Scale (angl. *Large Scale NAT* - v nadaljevanju LSN) so predvideni trije različni koncepti prevajanj, ki imajo vsak svoje prednosti in pomanjkljivosti: NAT444, NAT464 in DSL ter NAT64. Z vidika operaterja je poleg logičnega koncepta izredno pomembna fizična umestitev funkcionalnosti v omrežje

IP. V primeru, da se ta odvije zgolj na eni točki, jo lahko pojmujemo kot eno točko odpovedi (angl. *single point of failure*), ki se ji moramo izogniti ob upoštevanju visoke razpoložljivosti omrežja in storitev (Nishitani, Yamagata & Miyakawa, 2009).

### 6.4.3 Prevajanje omrežnih naslovov 444

Prevajanje omrežnih naslovov 444 (angl. *Network Address Translation 444* - v nadaljevanju NAT444) opredeljujemo kot mrežni model, ki uporablja mrežni naslov in mehanizem NAPT s tremi podmrežnimi bloki IPv4. Prvi NAPT se izvaja na CPE, drugi pa v LSN, ki je razviden kot programski proces na robnem ali agregacijskem usmerjevalniku. Prvi blok naslovov IPv4 je zasebni – znotraj CPE, drugi se uporablja med CPE in LSN (javni ali zasebni naslovni prostor), tretji pa je globalni naslovni prostor IPv4 zunaj LSN.

Paket, ki prispe iz javnega internetnega omrežja, mora biti ustrezno usmerjen v operaterjevo omrežje IPv4, kjer ga je potrebno usmeriti na ustrezen LSN, kjer poteka prevajanje (naslov, vrata). Od tu dalje paket potuje naprej na napravo NAT končnega uporabnika. Prevajanje paketa se, odvisno od smeri prometa, izvede dvakrat, tj. na strani uporabnikov naprave NAT in na strani operaterja LSN. Ker so v vseh primerih v uporabi naslovi IPv4, govorimo o NAT444 (Kunc, 2010, str. 27).

Prednosti modela NAT444 se zrcalijo v skupku dosedanjih rešitev in v tem, da ne zahteva menjave opreme CPE pri uporabniku, prevajanja, ponovnih zapisov v DNS in dodatne fragmentacije paketov, saj ne uporablja tehnologije tuneliranja. Po drugi strani ima omenjeni model seveda tudi nekatere pomanjkljivosti. Ker ni uporabljen v širšem krogu operaterjev in ponudnikov storitev, je težko predvideti ali napovedati, koliko končnih naprav lahko obdela posamezen LSN. Prihaja lahko do podvajanja IP v omrežju, saj se isti naslovni prostor uporablja med LNS in NAT ter v končnem zasebnem omrežju uporabnika. Požarni zidovi lahko blokirajo promet, ker se po RFC 1918 zasebnih naslovov ne sme usmerjati izven zasebnega omrežja (temu se je po drugi strani mogoče izogniti, če pakete usmerjamo na zunanji vmesnik LNS). Nekatere aplikacije zahtevajo posebno obdelavo, ker je naslov IP zapisan v koristni vsebini paketa. Istočasno obstajata poti IPv4 in IPv6, kar podvoji število poti IGP znotraj LSN (Doyle, 2009).

### 6.4.4 Prevajanje omrežnih naslovov 464

Prevajanje omrežnih naslovov 464 (angl. *Network Address Translation 464* - v nadaljevanju NAT464) odpravlja težavo usmerjanja paketov med dvema ali več zasebnimi omrežji skozi isti LSN (Kunc, 2010, str. 30). Ideja tehnične rešitve spominja na prevajalni mehanizem NAPT, kjer ima po RFC 2766 omogočeno prevajanje iz IPv4 v IPv6. NAT464 uporablja protokol IPv6 med LSN in končno napravo NAT. Med notranjim zasebnim

omrežjem in napravo NAT ter med napravo LSN in javnim omrežjem pa izvaja prevajanje med obema protokoloma. Z uporabo NAT464 smo tako korak bližje uvedbi IPv6 na dostopovnem omrežju, saj se le-ta uporablja med napravo LSN in napravo NAT pri uporabniku (Kunc, 2010, str. 31).

Njegova pomanjkljivost se kaže v tem, da je omrežje med LSN in NAT poenostavljeno. V obeh točkah je potrebno prevajanje iz IPv4 v IPv6 – in obratno (Doyle, 2009). Izvajanje prevajanja med IPv6 in IPv4 je v primerjavi z NAT44 zahteven postopek. To je pravzaprav tudi eden izmed glavnih razlogov, da rešitev še ni v širši uporabi, kot na primer rešitve tipa NAT44 (Kunc, 2010, str. 32).

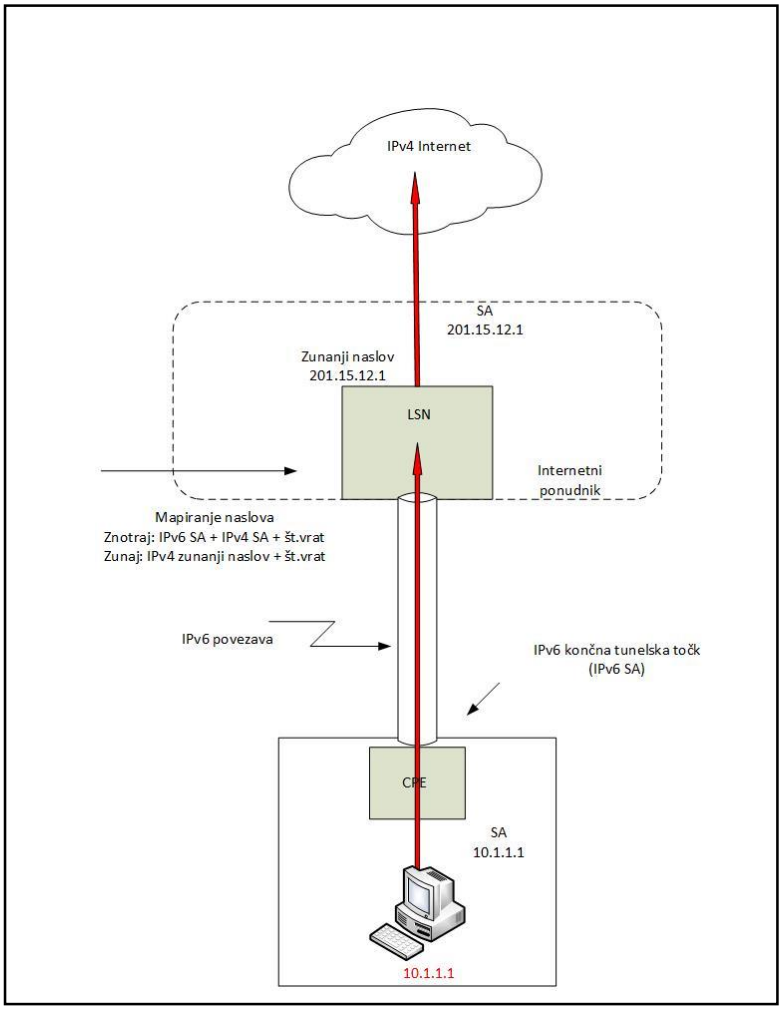
### 6.4.5 Translacijski model dvojnega sklada

Leta 2008 je Alain Durand iz podjetja Comcast predstavil translacijski model dvojnega sklada (angl. *Dual-Stack Lite* – v nadaljevanju DSL) kot internetni osnutek. Omenjeno podjetje je največji kabelski operater v ZDA, ki zagotavlja širokopasovni internet, televizijo in storitve telefonije. Ima 20 milijonov uporabnikov širokopasovnega interneta in je prav zaradi pomanjkanja naslovnega prostora IPv4 zelo motivirano za uvedbo protokola IPv6 (IETF, 2009f, po Kunc, 2010, str. 32).

DSL je učinkovitejši pristop kakor NAT464, saj koristi prednosti NAT464 in hkrati zmanjšuje njegove pomanjkljivosti. Uporablja povezave IPv6 med ponudnikom in uporabnikom, vendar ne izvaja translacije NAT64. Ko uporabniška naprava (angl. *Customer Promise Equipment* – v nadaljevanju CPE) v zasebnem omrežju pošlje paket IPv4 v internet, se omenjeni paket ovije v paket IPv6 za potrebe transporta do naprave LSN. Ta paket odvije in izvede translacijo NAT44. Tuneliranje IPv4 čez IPv6 je enostavnejši in učinkovitejši način kakor translacija, saj v tem primeru učinkovitost in redundančnost nista vprašljivi (Kunc, 2010, str. 32).

Slika 19 prikazuje arhitekturo modela DSL. IPv4 paketi so od CPE naprave do LSN naprave tunelirani skozi IPv6 tunel.

*Slika 19: Prikaz arhitekture DSL*




*Vir: J. Doyle, Understanding Dual-Stack Lite, 2009.*

Pri tej arhitekturi je potrebno namestiti dodaten element na strani naprave LSN, ki bo izvedla mapiranje med paketom IPv6, ki nosi informacijo o paketu IPv4, in uporabljenimi vrati TCP/UDP ter izhodnim paketom IPv4, ki se usmeri proti internetu. Ker je vsak prihoden paket z naslovom IPv6 na napravo LSN edinstven za vsakega uporabnika (kombinacija IPv6 izvorni naslov + IPv4 izvorni naslov + vrata TCP/UDP protokola), lahko izvajamo diferenciacijo med različnimi sejami in uporabniki. Ko naprava LSN dobi povratni paket IPv4 z interneta, iz svoje mapirne tabele prejme naslov IPv4 končnega uporabnika, zamenja številko vrat, ovije paket v IPv6 in ga posreduje v ciljno uporabnikovo omrežje. To pravzaprav pomeni, da mapiran naslov IPv6 ne razlikuje samo uporabnikovega zasebnega omrežja, temveč hkrati zagotavlja tudi referenco na končno tunelsko točko. Ker predvidevamo, da je v zasebnem uporabniškem omrežju različno število končnih računalnikov, ki uporabljajo enega ali oba protokola IP (dvojni sklad), se mora uporabnost DSL izvajati na robnem usmerjevalniku zasebnega omrežja. Če uporabnik pošlje paket IPv6, se ta transparentno usmeri na napravo LSN. Če pa robna naprava uporabniškega omrežja prejme paket IPv4, potem mora izvesti IPv4-IPv6 ovijanje

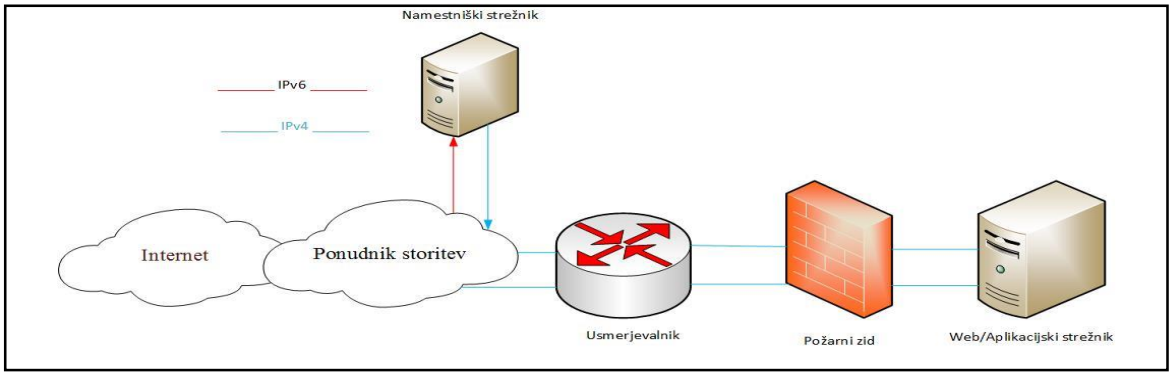
in paket posredovati naprej na LSN. Pomanjkljivost, ki je povezana z DSL, je zamenjava ali nadgradnja uporabniškega robnega usmerjevalnika (CPE), kar internetnemu ponudniku prinaša stroške. Internetni ponudniki so pogosto nenaklonjeni temu, da bi obremenjevali svoje uporabnike, poleg tega pa zamenjava opreme predstavlja finančni vložek in logistično težavo, povezano z zamenjavo in konfiguracijo naprave. Prav zaradi tega je pričakovati, da bodo internetni ponudniki, ki se bodo odločali za implementacijo DSL, tehnologijo najprej implementirali pri svojih novih uporabnikih, medtem ko se bodo pri nezahtevnih naročnikih držali amortizacijskega načrta (Kunc, 2010, str. 33).

## 6.5 Posredovalni strežnik

Ena najlažjih poti dostopa do IPv6 omrežja je uporaba obstoječe posredniške infrastrukture. Seveda je tudi v tem primeru potrebno zadostiti nekim minimalnim zahtevam. Če želimo brskati po omrežju preko IPv6, potrebujemo tako strežnik kot brskalnik, ki podpirata IPv6. Ne glede na to, kateri HTTP strežnik uporabljamo (npr. IIS ali Apache), ga moramo nastaviti tako, da je sposoben poslušati preko HTTP vrat (običajno 80). Če je to posredovalni strežnik, mu je naprej potrebno dodeliti IPv6 naslov. Nastaviti ga je potrebno tako, da deluje v načinu dvojnega sklada, saj ne želimo onemogočiti obstoječih in nadaljnjih IPv4 uporabnikov. V drugem koraku mu moramo dodeliti IPv6 privzeto smer (angl. *default route*), ki kaže na naš IPv6 usmerjevalnik. Če imamo uporabnike dvojnega sklada, bo posrednik dobil tako IPv4 kot IPv6 zahteve, ker uporabnik vpiše spletni naslov, uporaba protokola pa je odvisna od DNS.

Poleg postavitve namestniškega strežnika v organizaciji, vedno obstaja tudi možnost, da nam to storitev zagotovi naš ponudnik, kot prikazuje Slika 20. To ne zahteva nobene spremembe lokalne infrastrukture in je zelo hiter način, ki omogoča dosegljivost vsebin preko IPv6. Naslednja možnost je gostovanje našega reverznega (angl. *reverse*) posredniškega strežnika v zunanjem podatkovnem centru (angl. *external datacenter*).

*Slika 20: Namestniški strežnik nam zagotovi ponudnik (ISP)*




*Vir: S. Steffann, Making Content Available Over IPv6, 2013.*

Posredovalni strežnik se lahko uporabi v dveh primerih:

- v primeru, da imajo gostitelji v omrežju organizacije samo IPv4 in želijo dostopati do internetnih strani, ki imajo dostop samo preko IPv6;
- kadar je naša spletna stran dostopna samo preko IPv4, želeli pa bi omogočiti dostop tudi IPv6 internetnim uporabnikom.

Uporaba posredniškega strežnika ima vsaj tri prednosti:

- Ni nam potrebno spremeniti notranje infrastrukture. Vsi uporabniki lahko ostanejo na IPv4 in uporabljajo posredovalni strežnik tako kot prej.
- Lahko pridemo do spletnih strani, ki že imajo omogočen IPv6 dostop in do vsebin, ki po IPv4 niso dosegljive.
- Lahko preverimo, katere strani imajo težave z IPv6 in ali je problem samo preko spletnega naslova ali obstaja problem splošne dostopnosti.

Splošno dostopen posredovalni strežnik najdemo na naslovu http://www.ipv6proxy.net/. Uporabimo ga lahko za testiranje dostopnosti svoje spletne strani preko IPv6 naslova ali za obiskovanje drugih IPv6 spletnih mest.

# 7 PLAN PREHODA NA IPV6 V OMREŽJU AGENCIJE RS ZA OKOLJE

Agencija RS za okolje (v nadaljevanju ARSO) je organ v sestavi Ministrstva za okolje in prostor (v nadaljevanju MOP). Znotraj svojih pristojnosti opravlja strokovne, analitične in upravne naloge s področja okolja na državni ravni. Med te naloge sodi tudi spremljanje stanja in varovanje okolja ter zagotavljanje kakovostnih javnih okoljskih podatkov v skladu s predpisi. Za te namene ARSO izvaja različne upravne postopke, ki so v skladu z domačo in evropsko zakonodajo s področja okolja. Poleg tega spremlja, analizira in napoveduje naravne pojave in procese v okolju (vreme, potrese, stanje voda, kakovost zraka) ter s pravočasno in kvalitetno napovedjo le-teh zmanjšuje naravno ogroženost ljudi in njihovega premoženja. Te naloge uresničuje v okviru nacionalnih služb za meteorologijo, hidrologijo in seizmologijo (ARSO, 2016).

Za uspešno izvrševanje vseh nalog ARSO poleg dobro usposobljenega strokovnega in uradniškega kadra potrebuje tudi hitro, zanesljivo in varno omrežno infrastrukturo ter dobro usposobljene skrbnike te infrastrukture. Zato na ARSO stalno spremljamo razvoj IT in mu poskušamo slediti v okviru svojih strokovnih in finančnih zmožnosti z namenom, da ponudimo kar najboljše možne servise za opravljanje številnih dejavnosti. To zagotavljamo v okviru Službe za analitično podporo delovnim procesom in s pomočjo zunanjih sodelavcev.

Naslovnega prostora za IPv4 je v svetu že začelo primanjkovati in samo vprašanje časa je, kdaj bo uvedba IPv6 protokola postala neizogibna. To seveda ne pomeni, da bo IPv4 izginil čez noč. Najverjetneje bosta oba sistema morala teči skupaj več let, zato moramo celotno računalniško infrastrukturo temu primerno prilagoditi. Tako smo na ARSO že pred leti na mojo pobudo začeli razmišljati o prehodu na nov IP protokol, tj. IPv6. Takrat smo že imeli naprave in sisteme, ki so delno podpirali implementacijo IPv6. To so bili sistemi z Windows programsko opremo Windows XP z SP1, Windows 2003 in posamezne verzije Linux sistemov. Tudi posamezni tiskalniki so že imeli podporo za IPv6.

ARSO mora biti pripravljen na nove izzive in nove povezave. V primeru, da organizacije, s katerimi tesno sodelujemo na izmenjavi podatkov, npr. The Regional Meteorological Data Communication Network (v nadaljevanju RMDCN), preidejo na protokol IPv6, jim bomo morali slediti, zato je bolje te nove možnosti predvideti in se nanje pripraviti. Le v primeru, da bomo že imeli nekaj izkušenj z IPv6 protokolom, bomo sposobni oceniti, v kolikšem času smo zmožni tako povezavo vzpostaviti, kaj moramo narediti in koliko nas bo to stalo. O prehodu na IPv6 je potrebno misliti predvsem tedaj, ko se pripravljamo na zamenjavo strojne opreme, še bolj pa tedaj, ko nadgrajujemo ali celo naročamo novo programsko opremo. Znati moramo postaviti zahteve in preveriti delovanje programske opreme v okolju IPv6. Nespametno je namreč nakupiti novo programsko opremo, kasneje pa plačevati nadgradnjo samo zato, ker ne podpira IPv6.

Dobra lastnost prehoda na IPv6 je ta, da nadgradnjo lahko uvedemo postopoma, samo na posameznih delih omrežja ali celo pri posamezniku. Prav tako z uvedbo IPv6 na posameznih delih ne ogrožamo delovanja ostalega dela IPv4 omrežja, vseeno pa moramo biti pazljivi pri upravljanju omrežja. Varnostno politiko moramo voditi posebej za IPv4 in posebej za IPv6, saj sta to med seboj popolnoma ločena sistema. Ključno vlogo ima pri tem proces izobraževanja. V Službi za analitično podporo delovnim procesom na ARSO smo se odločili, da ustvarimo vsaj osnovne pogoje za prehod na IPv6, in sicer zakup naslovnega prostora, postavitev pilotnega omrežja in testiranje njegovega delovanja.

Pri proučevanju različnih tranzicijskih mehanizmov za prehod na IPv6 se kaže kot najbolj primeren mehanizem dvojnega sklada. Ta nam omogoča sočasno bivanje dveh, med seboj nekompatibilnih protokolov - IPv4 in IPv6. Pri uporabi tega mehanizma je dobro vedeti, da se bo obseg dela povečal, saj bomo morali upravljati dve ločeni omrežji. Prav tako je dobro vedeti, da uvedba dodatnega protokola vpliva tudi na uporabo računalniških resursov (CPU, RAM), ki pa so danes zaradi velikih zmogljivosti večinoma praktično zanemarljivi.

Večina organov v državni upravi ima dostop do interneta urejen skozi HKOM omrežje. ARSO je pri tem specifičen, saj imamo povezavo v internet urejeno preko dveh vstopnih točk:

- Arnes;

- HKOM (hitro komunikacijsko omrežje).

Akademska in raziskovalna mreža Slovenije (Arnes) je javni zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture ter omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini (Zavod Arnes, 2016).

Arnes povezava se uporablja predvsem za dostop iz ARSO do interneta in za dostop internetnih uporabnikov do storitev, ki jih nudi ARSO. HKOM povezava se uporablja predvsem za povezavo ARSO oddaljenih lokacij z ARSO internim LAN omrežjem, izmenjavo podatkov znotraj HKOM omrežja in za dostop do posameznih storitev znotraj HKOM (npr. elektronska pošta, računovodski sistem MFERAC, kadrovska evidenca, oddaljeni dostop).

Na ARSO smo v takratni Službi za informatiko leta 2006 prvič začeli razmišljati o tem, kaj bi nam lahko prinesel novi protokol IPv6, ki je bil tedaj ne samo na ARSO, ampak tudi v svetu še velika neznanka. Po premisleku smo se odločili, da bomo v skladu s pristojnostmi v okviru manjšega projekta, ki bo koordiniran s strani Službe za informatiko, postavili pilotno omrežje. Dogovorili smo se, da naredim pilotno postavitev omrežja IPv6 v okviru obstoječe infrastrukture, saj za ta namen ni bilo planiranih dodatnih finančnih sredstev. Težave so se pojavile že na samem začetku, ko sem pri popisu komunikacijske opreme ugotovil, da obstoječi izhodni usmerjevalnik in komunikacijska stikala ne podpirajo protokola IPv6. Nabava novih komunikacijski naprav še ni bila predvidena, za nadgradnjo starih pa ni bilo potrebnih finančnih sredstev, prav tako pa nadgradnja ni bila ekonomsko upravičena. S tem se je projekt postavitve pilotnega omrežja zaustavil, saj samo lokalno testiranje IPv6 protokola ni imelo pravega smisla.

Sedaj, po 10 letih, je zamisel o nadaljevanju pilotne postavitve omrežja ponovno zaživela, saj so se okoliščine v zvezi s protokolom IPv6 bistveno spremenile. Pred začetkom pilotne postavitve bom ponovno preveril ključno komunikacijsko opremo. Sledila bo inventura strojne in programske opreme za tisti del ARSO infrastrukture, kjer bi bil začetek prehoda najlažje izvedljiv. Nato bom postavil pilotno testno omrežje in preveril dostop tega omrežja tako po IPv4 kot IPv6 protokolu.

## 7.1 Hitro komunikacijsko omrežje

Hitro komunikacijsko omrežje (v nadaljevanju HKOM) je zasebno omrežje, ki je zasnovano za prenos podatkov znotraj javne in državne uprave. Komunikacija poteka med posameznimi zaključenimi celotami (ministrstva, FURS itd.), posameznimi končnimi uporabniki ter centralnim sistemom aplikativnih in podatkovnih strežnikov ter storitev (elektronska pošta, internet, klicni dostopi itd.). Omrežje je povezano s svetovnim spletom,

zato je še posebej pomembno, da deluje in je varovano ter vzdrževano po natančno določenih standardih in pravilih.

Za ARSO predstavlja HKOM eno od bolj pomembnih povezav. Preko te vstopne točke opravlja sledeče naloge in storitve:

- dostop do svojih oddaljenih lokacij (posamezni meteorološki centri, letališča…);
- dostop do ostalih organov znotraj HKOM omrežja;
- IBM Notes (elektronska pošta, SPIS, e-računi, e-nabave…);
- MFERAC;
- oddaljeni dostop (VPN, iNotes…);
- možnost dostopa do svetovnega spleta.

ARSO ima več oddaljenih lokacij, ki imajo svojo vstopno točko v HKOM omrežje. Imajo svoj IPv4 naslovni prostor, ki jim je bil dodeljen v skladu s HKOM pravili in predpisi. Pravila na omrežju in usmerjevalnikih so postavljena tako, da vsaka oddaljena lokacija deluje kot del lokalnega ARSO omrežja. Prav tako imajo dostop do svetovnega spleta preko ARSO posredovalnega strežnika.

Dostop do ostalih organov znotraj HKOM omrežja je ključnega pomena za delovanje znotraj javne uprave, saj omogoča enostavnejši in varnejši način pretoka najrazličnejših informacij. Pravila določajo, do katerih podatkov lahko dostopa vsak organ, do katerih pa dostopa po vnaprejšnjem dogovoru. Predvsem je pomembno, da je pretok informacij varen in ne potuje po celotnem internetu.

Znotraj HKOM omrežja večina izmenjave elektronskih sporočil poteka preko IBM Notes (Lotus Notes) strežnikov. Tako ima tudi ARSO svoj IBM Notes strežnik, ki poskrbi za izmenjavo elektronskih sporočil s centralnim IBM Notes strežnikom. Na IBM Notes podlagi teče več aplikacij. Ena najpomembnejših aplikacij je aplikacija za pisarniško poslovanje SPIS. Z uvedbo e-računov je postala nujna. Obstajajo še druge IBM Notes aplikacije, ki niso tako razširjene znotraj HKOM omrežja in so bolj lokalnega pomena. To so najrazličnejše verzije aplikacije za javno naročanje, študentsko delo, rezervacijo avtomobilov, vodenje projektov…

MFERAC je aplikacija, namenjena finančnemu poslovanju znotraj javne uprave. Uporabljajo jo skoraj vsi organi znotraj javne uprave - ARSO pri tem ni izjema. Zaradi sprejemanja e-računov je postala zelo tesno povezana s SPIS aplikacijo, kjer se e-računi knjižijo, potrjujejo in podpisujejo.

Oddaljeni dostop je zelo pomemben tako za skrbnike strežnikov in omrežja na ARSO kot tudi za posameznike. Preko VPN povezave praktično od kjerkoli postanemo del ARSO omrežja. Pravila določajo, ali ima posameznik poln dostop do celotnega omrežja ali samo

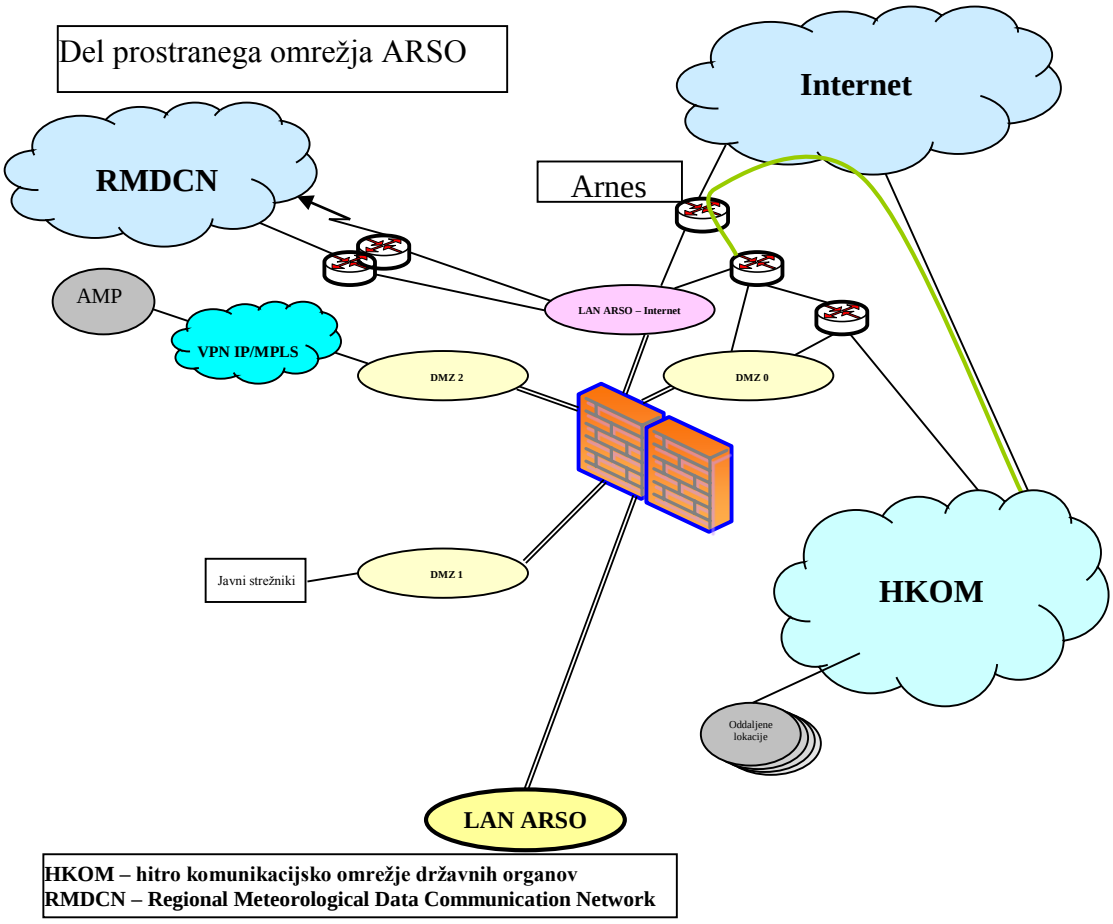
do posameznih delov. Večina uporabnikov na ta način dostopa samo do svoje elektronske pošte in lokalnih ARSO spletnih strani. V primeru, ko uporabnik potrebuje samo dostop do svoje pošte znotraj HKOM omrežja, obstajajo še drugi bolj enostavni dostopi preko iNotes, Traveler ali Blackberry storitev.

Vsak uporabnik na ARSO ima možnost dostopa do svetovnega spleta tudi preko HKOM posredniškega strežnika. Te možnosti uporabniki običajno nimajo nastavljene v svojem brskalniku, ker imajo vsi ARSO uporabniki možnost dostopa preko ARSO posredniškega strežnika, ki je povezan v internet preko dostopne točke, ki je v upravljanju Arnesa. Zaradi tako močne vpetosti v HKOM omrežje se je sprva razmišljalo o pridobitvi IPv6 naslovnega prostora s strani HKOM upravljalca, ki je sedaj Ministrstvo za javno upravo (v nadaljevanju MJU), vendar se je zelo hitro izkazalo, da smo o tem začeli razmišljati prezgodaj. Zaradi tega je ARSO, ki je že imel dodeljen javni IP naslovni prostor s strani Arnesa, pri njem zaprosil tudi za dodelitev IPv6 naslovnega prostora in ga tudi dobil.

## 7.2 Omrežna infrastruktura

Kot prikazuje Slika 21, ima ARSO zelo razvejano komunikacijsko omrežje. Imamo 5 glavnih povezav, ki med seboj komunicirajo po vnaprej določenih pravilih preko redundantnega požarnega zidu. Najpomembnejša povezava je povezava do zunanjega ARSO omrežja. Na to omrežje je priključeno privatno omrežje RMDCN ter dve povezavi za dostop do Interneta. Optimalnejša povezava poteka preko Arnes vstopne točke in druga skozi HKOM omrežje. Preko VPN MPLS in GPRS omrežja dostopamo do svojih avtomatskih merilnih postaj (AMP). Poleg tega imamo še klicne povezave za prenos podatkov iz starejših AMP postaj. Za povezavo in pravilno usmeritev podatkov skrbijo različne komunikacijske naprave, kot so omrežna stikala, usmerjevalniki in modemi. Zaradi zagotavljanja maksimalne povezljivosti in visokega nivoja varnosti uporabljamo večinoma komunikacijske naprave enega proizvajalca. Znotraj HKOM omrežja se uporablja Cisco komunikacijska oprema in tej politiki sledi tudi ARSO.

*Slika 21: Del prostranega internetnega omrežja ARSO*




*Vir: Povzeto in prirejeno po B. Hudomalj, Prostrano internetno omrežje ARSO (interno gradivo), 2015.*

Prvi pogoj za prehod na IPv6 je ta, da je naša komunikacijska oprema IPv6 podprta. Tabela 15 prikazuje seznam Cisco komunikacijske opreme glede na tip.

*Tabela 15: Cisco komunikacijska oprema*

| **Naprave po tipu** | **IPv6 Podprta verzija** | **Instalirana verzija** | **Opombe** |
|---|---|---|---|
| Cisco Catalyst 2960 Series | 12.2 | 12.2(35)SE5 | |
| Cisco Catalyst 2960 Series | 12.2 | 12.1(20)EA 1a | Potrebna nadgradnja |
| Cisco Catalyst 2960 Series | 12.2 | 12.1(20)EA 1a | Potrebna nadgradnja |
| Cisco Catalyst 3750 Series | 12.1(19)EA 1c | 12.2(50) | |
| Cisco Catalyst 3750 E-Series | 12.2 | 12.2(50) | Privzeti prehod (Arnes) |

Verzija Cisco IOS 15.3 ima že polno IPv6 podporo razen podpore za RDNSS, ki je omogočena v kasnejših verzijah 15.4(1)T in 15.3(2)S. IPv6 protokol je že privzeto naložen (angl. *default*).

Operacijski sistemi, ki ne podpirajo DHCPv6 ali ND RDNSS, ne morejo samodejno konfigurirati imenskih strežnikov (angl. *Name Servers* – v nadaljevanju NS) v IPv6 okolju. Zaradi velikega števila Cisco stikal sem glede na tip preveril samo naključno izbrana Cisco stikala. Ugotovil sem, da tudi znotraj istega tipa stikala nimajo enake verzije operacijskega sistema (odvisno od datuma nabave). Pri dejanskem prehodu na IPv6 bo temu potrebno nameniti posebno pozornost.

Iz Tabele 16 je razvidno, da vsi tiskalniki, priključeni na omrežje ARSO, podpirajo tudi IPv6 protokol, potrebno pa je preveriti, ali vsak tiskalnik podpira tudi SMTP, NTP in LDAP storitve za IPv6. Trenutno še vsi tiskalniki delujejo samo preko IPv4 protokola.

*Tabela 16: Mrežni tiskalniki*

| **Tiskalniki (po tipu)** | **IPv4/IPv6 podpora** |
|---|---|
| HP DesignJet 800C 42" | Da |
| HP LaserJet P3005 | Da |
| HP LaserJetP3015DN | Da |
| Konica Minolta C364e | Da |
| Konica Minolta C454e | Da |
| Kyocera FS-3900N | Da |
| Kyocera FS-680 | Da |
| Lexmark C950 | Da |
| Lexmark MS510dn | Da |
| Lexmark MS610dn | Da |
| Lexmark MS810dtn | Da |
| Sharp MX-3500N | Da |
| Sharp MX-4100N | Da |
| Xerox ColorQube 8570DN | Da |
| Xerox Phaser 3320 | Da |
| Xerox Phaser 3435DN | Da |
| Xerox Phaser 4510DN | Da |
| Xerox Phaser 6360DN | Da |
| Xerox Phaser 7750 | Da |
| Xerox Phaser 7760 | Da |
| Xerox Phaser 8500AN | Da |
| Xerox Phaser 8860 | Da |

## 7.3 Programska oprema

*Tabela 17: Microsoft programska oprema, uporabljena na ARSO*

| Ime izdelka | Polna IPv6 podpora | Omejena IPv6 podpora | Polna IPv4 podpora | Dodatne informacije |
|---|---|---|---|---|
| DNS Server 2008 R2 | Da | | Da | |
| DNS Server 2008 | Da | | Da | |
| DNS Server 2003 | | | Da | |
| Internet Explorer | Da | | Da | |
| Office 2013 | Da | | Da | |
| Office 2010 | Da | | Da | |
| Office 2007 | Da | | Da | |
| Office 2003 | | | Da | Microsoft podpora se je končala. |
| Office XP (2002) | | | Da | Microsoft podpora se je končala. |
| Office 2000 | | | Da | Microsoft podpora se je končala. |
| Office 97 | | | Da | Microsoft podpora se je končala. |
| Project Professional 2010 | Da | | Da | |
| Project Professional 2007 | Da | | Da | |
| SharePoint Designer 2013 | Da | | Da | |
| SharePoint Foundation 2013 | Da | | Da | |
| SQL Server 2014 | Da | | Da | |
| SQL Server 2012 | Da | | Da | |
| SQL Server 2008 R2 | Da | | Da | |
| SQL Server 2008 | Da | | Da | |
| SQL Server 2005 | Da | | Da | |
| System Center 2012 R2 | | Da | Da | |
| Web Server (IIS) | Da | | Da | |
| Windows 10 Client | Da | | Da | |
| Windows 8 Client | Da | | Da | |
| Windows 7 Client | Da | | Da | |
| Windows XP Client | Da | | Da | Microsoft podpora se je končala. |
| Windows 7 Direct Access | Da | | | Deluje preko IPv6 protokola. |
| Windows Phone 8.1 | Da | | Da | |
| Windows Server 2012 R2 | Da | | Da | |
| Windows Server 2012 | Da | | Da | |
| Windows Server 2008 R2 | Da | | Da | |
| Windows Server 2008 | Da | | Da | |
| Windows Server Update Services (WSUS) | | Da Dvojni sklad | Da | |
| Windows SharePoint Services 3.0 | Da | | Da | |
| Windows Vista Client | Da | | Da | |

*Vir: Microsoft, IPv6 Support in Microsoft Products and Services, 2015.*

Tabela 17 vsebuje popis Microsoft opreme, ki jo najpogosteje uporabljamo na ARSO.

Opomba: Microsoft za Windows XP ne daje več podatkov, ker z njihove strani ni več podprt. IPv6 je bil polno podprt že v Windows Visti in strežniku Windows 2008, s podporo IPv6 pa je nadaljeval v vseh naslednjih verzijah.

Pomembno je vedeti, da ima protokolni sklad TCP/IP od različic Windows Server 2008 in Windows Vista dalje izvedeno arhitekturo dvojne IP plasti, kar je drugače kot v prejšnjih Windows izvedbah. IPv6 lahko onemogočimo, tehnično pa ga ni mogoče odstraniti. IPv4 in IPv6 sta kombinirana v datoteki tcp.sys. Edina pot za popolno odstranitev protokola IPv6 je tako odstranitev TCP/IP (Horley, 2014).

ARSO programa »Windows DirectAccess 7« še ne uporablja. Zanimivo je dejstvo, da ta program zahteva uporabo IPv6. Tabela 18 prikazuje podporo IPv6 v Microsoftovih storitvah in produktih, uporabljanih na ARSO.

*Tabela 18: Podpora IPv6 v Microsoftovih storitvah in produktih*

| **Aplikacija** | **OS** | **Verzija** | **IPv6 Podpora** | **Opombe** |
|---|---|---|---|---|
| Google Chrome | Windows | 47+ | Da | |
| Mozilla Firefox | Windows | 46, testirana | Da | Podpira IPv6 naslov z uporabo oklepajev: [ipv6]:vrata. |
| Internet Explorer | Windows | 9+ | Da | |
| Windows raziskovalec | Windows | Testirano z Windows 7 | Da | Podpira IPv6 naslov v naslovnem polju z uporabo \\fe80--abcd-eff0.ipv6-literal.net z uporab črtice namesto dvojnih točk. |
| Microsoft Exchange Server | Windows | 2013+ | Da | Na ARSO se še ne uporablja. |
| Microsoft SQL Server | Windows | 2005+ | Da | ARSO uporablja SQL 2008+. |
| Microsoft Windows Server Update Services | Windows | 4.0 | Da | WSUS je trenutno dostopen samo preko IPv4, zato potrebujemo posredovalni strežnik ali IPv6 tranzicijske mehanizme. |
| PuTTY | Windows | 0.66+ | Da | |
| Skype for Business | Windows | vse | Delno | Podpira IPv6 omrežje tam, kjer IPv4 plast ni vezana na omrežno kartico, seveda pa odstranitev IPv4 plasti povzroči nedelovanje. |
| IBM Notes | Windows | 8.0.1 | Da | ARSO uporablja verzijo 9.0. |

se nadaljuje

*Tabela 18: Podpora IPv6 v Microsoftovih storitvah in produktih (nad.)*

| Aplikacija | OS | Verzija | IPv6 Podpora | Opombe |
|---|---|---|---|---|
| Sophos | Windows | 10.x | Da | Anti-virusni program |
| ArcServe | Windows | 10.3 | Da | GIS |
| AnyConnect | Windows | 3.1 | Da | VPN oddaljeni dostop |
| MS Office | Windows | 2007+ | Da | ARSO uporablja verzije 97+ |
| IMIS | Windows | 9.x | Da | Več na: http://www.imis.si/novice/arc9/ |
| Winscp | Windows | 5.7.6 | Da | Aplikacija za prenos podatkov. |

Vsi ključni Microsoft produkti, ki so pomembni za delovanje ARSO, so IPv6 podprti, kar pomeni, da niso ovira za prehod na IPv6. Problem predstavljajo posamezne Microsoft aplikacije, ki uporabljajo access 97, 2000 in XP. Vse te aplikacije so sicer že popisane, njihove naloge pa bodo ustrezno zajete v novem okoljskem informacijskem sistemu, ki se pripravlja. Prenova teh aplikacij je vključena v projekt prenove okoljskega informacijskega sistema.

Oracle Database 11g Release 2 podpira IPv6 naslavljanje za vse funkcije in komponente v enojnem (angl. *single-instance*) načinu. Oracle Database 12c Release 1 te funkcije razširja s tem, ko omogoča povezljivost odjemalca prek javnih omrežij do Oracle RAC z nekaj omejitvami. Te omejitve naj bi bile odstranjene v prihodnji izdaji Oraclove baze. ARSO uporablja verzijo Oracle 11g. Tabela 19 prikazuje, kateri IP odjemalci so podprti na katerem IPv4 oz. IPv6 strežniku. Razvidno je, da je edina prava rešitev strežnik z dvojnim skladom.

*Tabela 19: Oracle 11g Release 2 podpora za IPv6*

| **Samo IPv4 strežnik** | | **Strežnik z dvojnim skladom** | **Samo IPv6 strežnik** |
|---|---|---|---|
| **Samo IPv4 odjemalec** | Podprt (v4) | Podprt (v4) | *Ni podprt* |
| **Odjemalec dvojnega sklada** | Podprt (v4) | Podprt (v4, v6) | Podprt (v6) |
| **Samo IPv6 odjemalec** | *Ni podprt* | Podprt (v6) | Podprt (v6) |

*Vir: Oracle Database and IPv6 Statement of Direction, 2013, str.* 3.

VMware vSphere ESX/ESXi 4.1 podpira IPv4 in IPv6, vendar je podpora IPv6 privzeto onemogočena. IPv6 je privzeto onemogočen v ESXi 5.0 in privzeto omogočen v ESXi 5.1 in ESXi 5.5. Na ARSO se uporabljata obe verziji in imata omogočen samo IPv4 protokol.

Tabela 20 prikazuje aplikacije, ki se uporabljajo v Linux servisih in produktih. Razberemo lahko, da je večina Linux aplikacij IPv6 podprta.

*Tabela 20: Pregled podpore izbrane aplikacije IPv6 v Linux storitvah in produktih*

| Aplikacija | Verzija | IPv6 podpora | Opombe |
|---|---|---|---|
| postgresql | 9.0 | Da | PostgreSQL podpira IPv6 od verzije 8.2 |
| mysql | TBD | Ne | Razvoj je obstal na verziji 6.0 alpha |
| naptd | 0.4.2 | Da | |
| ntpd | 4.1.80-rc1 | Da | |
| ntpdate | 4.1.80-rc1 | Da | |
| mozilla | od 1.4 | Da | |
| firefox | od 1.0 | Da | |
| netscape navigator | 7.1 | Da | |
| opera | 7.20b | Da | |
| Apache HTTP Server | 2.0.43 | Da | |
| Apache HTTP Server | 1.3.27 | Ne | Priporoča se prehod na verzijo 2.0.x. |
| bind 8 | 8.4.4 | Da | |
| bind 9 | 9.2.3 | Da | |
| sendmail | 8.12.9 | Da | |
| postfix | od 2.2.0 | Da | |
| lftp | 2.6.5 | Da | |
| ftp | 0.17-35.el5 / 0.17-51.fc12 | Da | |
| smb | 3.2 | Da | Samba je odprto kodna izvedba SMB protokola |

*Vir: P. Bieringer et al., Current Status of IPv6 Support for Networking Applications, 2014.*

Tabela 21 prikazuje, katera verzija posameznega operacijskega sistema že podpira IPv6, v kateri je privzeto že naložen in katera podpira avtomatsko dodeljevanje IPv6 naslovov ter v kakšnem načinu.

*Tabela 21: Primerjava  podpore IPv6 v operacijskih sistemih*

| OS | Verzija | IPv6 podpora | Naložen | DHCPv6 | ND RDNSS | Opombe |
|---|---|---|---|---|---|---|
| AIX | 4.3 | Da | Da | Da | Ne | |
| Android | 4.2 (Jelly Bean) | Delno | Da | Ne | Ne | Ne podpira ND-RDNSS in DHCPv6. |
| Fedora | 13 | Da | Da | Da | Da | |
| FreeBSD | 9.0 | Da | Da | Dodatno | Da | |
| HP-UX | 11i | Da | Da | Da | Da | |
| IBMi | 7.1 | Da | Da | Da | Ne | |

se nadaljuje

*Tabela 21: Primerjava  podpore IPv6 v operacijskih sistemih (nad.)*

| OS | Verzija | IPv6 podpora | Naložen | DHCPv6 | ND RDNSS | Opombe |
|---|---|---|---|---|---|---|
| iOS | 4.1 | Da | Da | Da | Da | iOS podpira "stateless" DHCPv6 od verzije 4 in "stateful" DHCPv6 od 4.3.1. |
| Juniper JUNOS | 12.2 | Da | Da | Da | Ne | |
| MacOS X | 10.7 (Lion) | Da | Da | Da | Da | |
| MeeGo | 1.2 | Ne | Da | Ne | Da | |
| OpenBSD | 5.2 | Da | Da | Dodatno | Da | |
| OpenVMS | 8.3 | Da | Da | Ne | Ne | |
| Red Hat Enterprise Linux | 6 | Da | Da | Da | Da | |
| Solaris | 10 | Da | Da | Da | Ne | |
| SUSE Linux Enterprise Server | 11 | Da | Da | Da | Da | |
| Symbian | 7.0 | Da | Da | Ne | Ne | |
| Ubuntu | 11.04 to 13.10 | Da | Da | Da | Da | Podpira RDNSS dokler NetworkManager uporablja IPv6 "Avtomatske" nastavitve, sicer zahteva "rdnssd" paket. |
| webOS | 2.1.0 | Ne | Ne | Ne | Ne | |
| Windows NT in Windows 10 Mobile | 5.1 (XP) | Da | Ne | Dodatno | Ne | Windows XP uporabniki lahko uporabijo Dibbler, ki je odprto kodni sistem za implementacijo DHCPv6 |
| | 6.X, Vista,7, 8,8.1,10 | Da | Da | Da | Dodatno | rdnssd-win32 zagotavlja odprto kodno implementacijo ND RDNSS |
| Windows Mobile | 6.5 | Da | Da | Delno | Ne | Če ima OEM izrecno nenastavljen SYSGEN_TCPIP6 pre-procesorski simbol, potem nima IPv6 zmogljivosti. |
| Windows Phone | 7.5 | Ne | Ne | Ne | Ne | Podprt naj bi bil tudi Windows Phone 8. |
| | 8(.1) | Da | Da | Da | Ne | (RFC4941). |
| z/OS | V1R4.0 | Da | Da | Ne | | |
| z/VM | V5R1.0 | Da | Da | Ne | Ne | |
| z/VSE | V4R2 | Dodatno | Ne | | | Podpora od drugih ponudnikov, IP6/VSE iz Barnard Software, Inc. |

*Vir: Comparison of IPv6 support in operating systems, 2016.*

Opomba: Operacijski sistemi, ki ne podpirajo DHCPv6 ali ND RDNSS, ne morejo samodejno konfigurirati NS v IPv6 okolju. Na ARSO se kot DHCPv4 strežniki uporabljajo Windows 2012 strežniki. Za vzpostavitev DHCPv6 avtomatskega naslavljanja je potrebno te strežnike konfigurirati kot strežnike z dvojnim skladom in naložiti podporo za DHCPv6, ki je že del operacijskega sistema Windows 2012R2.

Tabela 22 prikazuje, da izmed vseh vrst operacijskih sistemov, ki tečejo na ARSO, IPv6 protokola ne podpira samo operacijski sistem Mac OS 8. Ugotovil sem, da je ta sistem naložen na stari strojni opremi, ki je v planu za zamenjavo, zato ne predstavlja resnejše ovire za prehod na IPv6. Ostali operacijski sistemi imajo podporo za IPv6, zato se jih lahko kadarkoli konfigurira kot strežnike dvojnega sklada in s tem omogoči prehod na IPv6.

*Tabela 22: Ostali operacijski sistemi na ARSO*

| **OS** | **Verzija** | **IPv6 podpora** | **IPv4 podpora** | **Opombe** |
|---|---|---|---|---|
| CentOS | 6.6 | Da | Da | |
| CentOS | 6.7 | Da | Da | |
| Debian | 7.9 | Da | Da | |
| Debian | 7.11 | Da | Da | |
| Debian | 8.5 | Da | Da | |
| Mac OS | 8 | Ne | Da | |
| openSUSE | 10.3 | Da | Da | |
| openSUSE | 11.2 | Da | Da | |
| Red Hat Enterprise Linux Server | 6.8 | Da | Da | |
| Solaris | 8 | Da | Da | |
| Solaris | 10 | Da | Da | |

Tabela 23 prikazuje dva tipa seizmoloških postaj z vidika podpore protokola IPv6.

*Tabela 23: Seizmološke postaje*

| **Komunikator** | **OS** | **IPv6 podpora** | **IPv4 podpora** | **Opombe** |
|---|---|---|---|---|
| Quanterra Q730 | 1.101 | Ne | Da | Za prenos podatkov iz »starih« postaj. |
| Quanterra Q330HRS | 1.101 | Ne | Da | Novejši model |

Komunikatorji Quanterra spadajo med najboljše komunikatorje za zajem podatkov (angl. *DataLogge*r) iz seizmoloških postaj, vendar ne podpirajo IPv6 protokola. To pomeni, da v tem delu omrežnega segmenta lahko prehod na IPv6 za nekaj časa odmislimo, še posebej, ker je to novejši model komuniktorja Quanterra.

Tabela 24 prikazuje dva tipa meteoroloških postaj z vidika podpore IPv6.

*Tabela 24: Meteorološke postaje*

| **Komunikator** | **OS** | **IPv6 podpora** | **IPv4 podpora** | **Opombe** |
|---|---|---|---|---|
| Moxxa UC-8410 | Linux 3.8.13 | Da | Da | |
| Moxxa NPort IA5150 | Lasten | Ne | Da | Za prenos podatkov iz »starih« postaj. |

Tabela 25 prikazuje dva tipa hidroloških postaj z vidik podpore IPv6.

*Tabela 25: Hidrološke postaje*

| **Komunikator** | **OS** | **IPv6 podpora** | **IPv4 podpora** | **Opombe** |
|---|---|---|---|---|
| MBIO 120 | Lasten | Ne | Da | Za prenos podatkov iz »starih« postaj. |
| Nanos G20 | Linux Debian 7.11 | Da | Da | |

Tabeli meteoroloških in hidroloških postaj prikazujeta, da komunikatorji, ki skrbijo za prenos podatkov iz starih meteoroloških in hidroloških postaj, ne podpirajo IPv6 protokola. Komunikatorji tipa Moxxa NPort IA5150 in Nanos G20 protokol IPv6 podpirajo, kar pa še ne zagotavlja, da je prehod na IPv6 v celoti izvedljiv. Pred dejanskim prehodom na IPv6 bo potrebno preveriti, ali celotna informacijska infrastruktura za zajem podatkov in prikaza teh podatkov na spletu podpira IPv6.

IBM Notes (Lotus Notes) in IBM Domino podpirata IPv6 že od verzije 7.0. Znotraj IBM Domino lahko nastavimo IPv6 podporo tudi za SMTP, POP3, IMAP, LDAP in HTTP storitve na IBM®, AIX®, Solaris® in Linux® sistemih.

ARSO ima na IBM Domino strežniku z operacijskim sistemom Windows 2008 R2 naloženo programsko opremo IBM Domino 9.0, prav tako pa vsi uporabniki uporabljajo programsko opremo IBM Notes 9.0, ki teče na Windows operacijskem sistemu (XP in višje verzije). To pomeni, da je komunikacija po IPv6 protokolu med IBM Domino strežnikom in IBM Notes odjemalci mogoča.

## 7.4 Storitve

ARSO omogoča najrazličnejše storitve tako zunanjim kot notranjim uporabnikom. Glavni sklopi storitev za zunanje odjemalce so na voljo z dostopom do ARSO spleta. Nekatere storitve so splošno dostopne, za nekatere pa so dostopi možni samo s predhodno avtentikacijo uporabnika. Dobršen del podatkov odjemalci prenesejo iz ARSO FTP strežnika. Večinoma gre za odjemalce, ki imajo z ARSO sklenjen dogovor o tem, katere podatke, na kakšen način in kako pogosto se jim jih pripravi.

Zaradi velikega števila storitev, ki jih ARSO opravlja, bom opis omejil predvsem na storitve, ki jih nudi za svoje tipične lokalne uporabnike, in sicer zato, ker je prehod na IPv6 najbolj enostavno pričeti na čim manjšem segmentu lokalnega omrežja. Glavne storitve, ki jih ARSO nudi svojim zaposlenim, so:

- antivirusna zaščita Sophos;
- dostop do podatkov v lokalnih Microsoft access bazah;
- dostop do podatkov v Oracle podatkovnih zbirkah;
- IBM Domino;
- Intranet;
- IMIS;
- oglasna deska;
- prijava v omrežje preko Microsoft aktivnega imenika (angl. *Active directory*);
- uporaba skupnih datotek (angl. *File sharing*);
- uporaba skupnih tiskalniških vrst (angl. *Print sharing*).

Antivirusna zaščita Sophos podpira delovanje v IPv6 okolju, zato sama aplikacija glede prehoda na IPv6 ni vprašljiva. Centralna instalacija antivirusnega programa je naložena na Windows 2012 R2 strežniku, ki je prav tako IPv6 podprt. Pri prehodu bo potrebno strežnik konfigurirati tako, da bo podpiral dvojni sklad, prav tako pa tudi vse odjemalce.

Podatki, ki se še nahajajo v posameznih Microsoft access bazah, večinoma uporabljajo starejše verzije programske opreme (MS Access 97, MS Access XP), ki ne podpira IPv6 protokola. Ti podatki se že sedaj postopoma selijo v Oracle bazo. Dostop do njih je še vedno omogočen preko Microsoft Access zaslonskih mask. Te maske se na novo kreirajo s pomočjo Microsoft Access 2013 aplikacije, ki pa je IPv6 podprta.

Oracle baza in strežnik, na katerem teče, sta IPv6 podprta, aplikacije, ki dostopajo do teh podatkov, pa je potrebno ločeno preveriti. Večinoma so to starejše aplikacije in verjetno niso IPv6 podprte, zato se bo potrebno na prehod tega strežnika posebno skrbno pripraviti.

Na ARSO uporabljamo IBM Notes verzijo 9. Tako strežnik (Domino) kot odjemalec podpirata IPv6. Kljub temu bo potrebno pri prehodu paziti. ARSO Notes strežnik je samo delček IBM Notes strežniške infrastrukture znotraj HKOM omrežja, zato bo moral biti prehod načrtovan in usklajen s politiko HKOM omrežja. S prehodom bo verjetno potrebno počakati vsaj toliko, da tudi HKOM postavi vsaj en centralni IBM Notes strežnik s podporo IPv6 protokola. Prav tako bo potrebno preveriti delovanje aplikacij, ki tečejo znotraj IBM Notes strežnika. Najbolj pomembna je aplikacija za pisarniško poslovanje SPIS in Appx servisi, ki omogočajo dostop do IBM Notes baz preko HTTP protokola. Aplikacije, ki so že del IBM Notes programske opreme, so IPv6 podprte. Najbolj pomembna in najbolj uporabljena je vsekakor IBM Notes elektronska pošta.

Intranet večinoma teče na strežnikih z Debian operacijskim sistemom, ki je IPv6 podprt, zato je potrebno na teh strežnikih vzpostaviti dvojni sklad, jim nastaviti ustrezne IPv6 naslove in jih vpisati v DNS tabelo, ki skrbi za pretvorbo numeričnih števil v lažje pomnljiva domenska imena.

IMIS programska oprema je sestavljena iz strežniške programske opreme in IMIS odjemalca. Strežniška programska oprema teče na operacijskem sistemu CentOS. Tako strežniški operacijski sistem kot programska oprema IMIS, ki teče na njem, sta IPv6 podprta. Na IMIS strežniku se nahaja elektronski arhiv, ki je namenjen dolgoročni hrambi vseh vrst dokumentarnega in arhivskega gradiva elektronskega ali digitaliziranega izvora preko procesa skeniranja. Proces skeniranja se izvaja na posameznih osebnih računalnikih, ki imajo naložen program IMIS/Scan. Ta poskrbi za zajem dokumentov. Vsi ostali uporabniki, ki morajo imeti le možnost vpogleda v te dokumente, imajo na svojih osebnih računalnikih naložen program IMIS/View. Programa IMIS/View in IMIS/Scan sta tesno povezana s programom SPIS, kar je pri prehodu na IPv6 potrebno upoštevati.

Oglasna deska temelji na Windows Sharepoint Foundation 2013 servisu in teče na Windows 2012 R2 strežniku. Baza SQL 2014, ki jo pri tem uporablja, teče na drugem Windows 2012 R2 strežniku. Kot smo videli v predhodni tabeli, vsi ti sistemi že nudijo IPv6 podporo. Za prehod na IPv6 jih je potrebno samo ustrezno konfigurirati.

Za uporabo skupnih datotek in tiskalniških vrst se večinoma uporabljajo Windows 2008 in Windows 2012 R2 strežniki. Ti vsi podpirajo protokol IPv6, zato prehod na samih strežnikih ni problematičen, vendar pa bo potrebno postopoma za prehod na IPv6 pripraviti tudi vse odjemalce.

Prijava v omrežje poteka preko Microsoft aktivnega imenika (angl. *Active Directory*), ki teče na Windows 2008 in Windows 2012 strežnikih. Tako strojna kot programska oprema podpirata IPv6. IPv6 protokol je na teh strežnikih že privzeto naložen, ni pa še konfiguriran, niti nima dodeljenih ustreznih naslovov. Postavitev strežnika z dvojnim skladom ne bi smela imeti negativnih posledic na delovanje strežnika. Kljub temu pa je to

strežnik, ki skrbi za prijavo na omrežje. V primeru nedelovanja aktivnega imenika prijava uporabnikov v omrežje ne bi bila možna, to pa bi pomenilo, da delo z računalnikom ne bi bilo možno. Zato moramo biti pri vsakem posegu, ki lahko vpliva na delovanje aktivnega imenika, zelo previdni in imeti vedno pripravljen obnovitveni načrt.

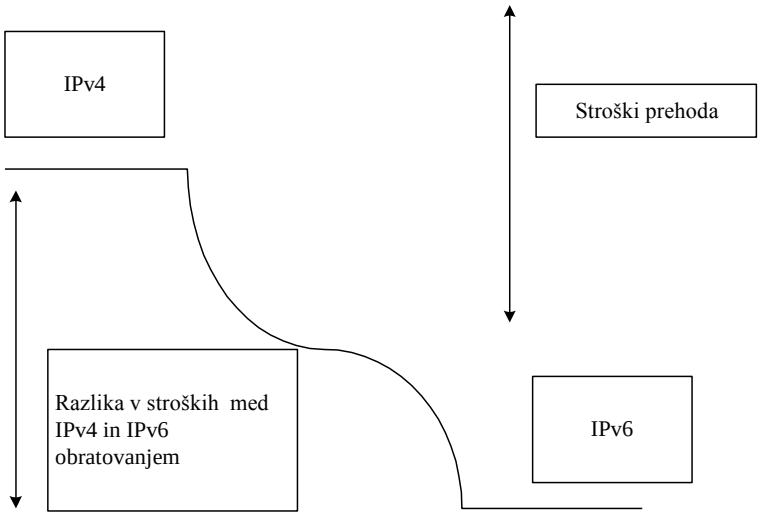
Do sedaj sem predstavil najbolj splošne storitve, ki ji ARSO nudi svojim zaposlenim. Teh storitev je še mnogo več: mednarodna izmenjava podatkov, prenos podatkov iz avtomatskih merilnih postaj (hidroloških, meteoroloških, seizmoloških…), najrazličnejši modeli za spremljanje in napovedovanje vremena, stanj voda …. Skratka, teh storitev je ogromno in pri prehodu na IPv6 bo potrebno vsak proces vsake storitve pregledati od začetka do konca in ga testirati v največji možni meri.

## 7.5 Ekonomična ocena stroškov

Uvedba IPv6 bo povzročila nekaj dodatnih stroškov, ker je to nova tehnologije, ki deluje na trenutni IPv4 omrežni infrastrukturi. Ti stroški se bodo zaradi ključnih značilnosti, ki jih ponuja IPv6, zmanjševali - predvsem na daljši rok.

Slika 22 prikazuje raziskavo organizacije North American IPv6 Task Force, ki kaže, da so stroški obratovanja IPv4 v primerjavi s stroški obratovanja IPv6 veliko višji. Prav tako bodo v obdobju prehoda na IPv6 nastali stroški prehoda zaradi uporabe mehanizmov prehoda, ki omogočajo sobivanje IPv4 in IPv6 protokola. Ta strošek vključuje strojno in programsko opremo, usposabljanje osebja in prehod na IPv6.

*Slika 22: Razlika med IPv4 in IPv6 stroški*




*Vir: A. H. Arifin, D. Abdullah, S. M. Berhan & R. Budiarto, An Economical IPv4-to-IPv6 Transition Model:A Case study for University Network, 2006, str. 171, slika 2.*

Pristop k ekonomični oceni stroškov je neposredno usmerjen k denarnim stroškom elementov v stroškovnem modelu. To velja tudi v našem primeru izgradnje IPv6 prehodnega stroškovnega modela za ARSO.

Da bi zgradili IPv6 model za neprofitno organizacijo, kot je ARSO s pristopom ekonomične ocene stroškov, moramo izpostaviti tako stroške kot tudi koristi. Obravnavali bomo vsako komponento modela gleda na pojem ekonomičnega stroška.

Naš model bo vseboval štiri komponente:

- ceno mrežne opreme;
- ceno mrežne programske opreme in operacijskih sistemov;
- ceno izobraževanja;
- nepredvidene stroške.

Strojna oprema je pomemben element. Večinoma obsega usmerjevalnik prehoda, požarni zid, mrežne vmesnike, mrežna stikala in gostitelje. Stroški strojne opreme so po ocenah Nacionalnega inštituta za standarde in tehnologijo (angl. *National Institute of Standards and Technology* - v nadaljevanju NIST) nizki ali srednji. Odvisni so od velikosti omrežja in od tega, ali je mrežno opremo potrebno zamenjati (takoj ali v rednem ciklu zamenjave) oz. ali je možna nadgradnja (Arifin, Abdullah, Berhan & Budiarto, 2006, str. 172).

Nekaj programske opreme bo potrebno nadgraditi zaradi uporabe IPv6, nekaj pa v okviru redne programske nadgradnje, ki jo je potrebno opraviti v določenem časovnem obdobju. Nadgradnja programske opreme vključuje nadgradnjo strežniške in namizne programske opreme, vključno z nadgradnjo operacijskih sistemov. Imamo programsko opremo različnih proizvajalcev, kot so Microsoft, IBM, Oracle, VMware kot tudi različne ponudnike odprtokodnih sistemov. Imamo stroške za operacijske sisteme, ki so majhni, velike stroške za specialno programsko opremo za zajem podatkov in srednje stroške za nadzor omrežja in nadgradnjo podatkovnih zbirk.

Med stroške delovne sile štejemo stroške usposabljanja, ki predstavljajo enega večjih stroškov. Stroški usposabljanja so različni glede na to, kako dobro želimo imeti usposobljene upravljalce omrežja in kako hitro sledimo spremembam strojne opreme. Prav tako je ta strošek odvisen od obstoječega znanja upravljalcev omrežja v zvezi z delovanjem usmerjevalnikov in IPv6 strežnikov. V primeru, da bo ključno osebje dovolj usposobljeno, vse dodatne izboljšave IPv6 programske opreme ne bodo bistveno vplivale na stroške izobraževanja, in sicer zato, ker bodo upravljalci omrežja že na podlagi pridobljenih znanj lahko uvedli določene mrežne zahteve in preverili, kako bodo te spremembe vplivale na varnost in interoperabilnost omrežja (Arifin, Abdullah, Berhan & Budiarto, 2006, str. 173).

Zadnja komponenta so nepredvideni stroški, ki so posledica različnih nepredvidenih nesreč in vplivajo na skupne stroške – npr. strošek, ki je nastal zaradi odprave težav v zvezi ineteoperabilnostjo ali odpravo varnostnega vdora, ki vpliva na delovanje omrežja. Ti stroški so glede na posamezno situacijo različni in so lahko majhni, srednji ali veliki (Arifin, Abdullah, Berhan & Budiarto, 2006, str. 173).

Tabela 26 prikazuje oceno stroškov prehoda na IPv6, ki je narejena na podlagi znanih stroškov na IPv4 omrežju. To nam lahko pomaga k hitrejšemu prehodu na IPv6.

*Tabela 26: ARSO stroškovni model*

| **Element** | **Opis** | **ARSO strošek** |
|---|---|---|
| **Strojna oprema** | | |
| Arnes usmerjevalnik prehoda | fiksen strošek | nizek |
| Požarni zid | fiksen strošek | nizek |
| Mrežna stikala | fiksen strošek | nizek |
| Kabli | fiksen strošek | nizek |
| | | |
| **Programska oprema** | | |
| Nadgradnja aplikacije za nadzor omrežja / upravljanje omrežja | aplikacija WhatsUp | srednji |
| Operacijski sistem (Linux) | odprto kodni sistem | nizek |
| Operacijski sistem (Windows) | fiksen strošek | |
| Nadgradnja DNS strežnikov in spletnih strežnikov (Linux) | odprto kodni sistem | nizek |
| Nadgradnja DNS strežnikov in spletnih strežnikov | fiksen strošek | nizek |
| Nadgradnja programske opreme za podatkovne zbirke | Oracle | srednji |
| Nadgradnja specialne programske opreme za področje meteorologije | zajem, kontrola, distribucija podatkov… | visok |
| Nadgradnja specialne programske opreme za področje hidrologije | zajem, kontrola, distribucija podatkov… | visok |
| Nadgradnja specialne programske opreme za področje seizmologije | zajem, kontrola, distribucija podatkov… | visok |
| | | |
| **Delovna sila** | | |
| Usposabljanje upravljavcev omrežja | 3200 € na osebo | visok |
| Običajno uporabniško usposabljanje | interno izobraževanje | nizek |
| | | |
| **Drugo** | | |
| Nepričakovana grožnja, npr. vdor | vpliva na delo in ugled ARSO | visok |

*Vir: Povzeto in prirejeno po A. H. Arifin, D. Abdullah, S. M. Berhan & R. Budiarto, An Economical IPv4-to-IPv6 Transition Model:A Case study for University Network,, 2006, str. 177, slika 3.*

Kot pri vsakem projektu bodo tudi tu začetni stroški visoki. V nadaljevanju lahko pričakujemo, da se bodo stroški zmanjševali na eni strani zaradi koristi, ki jih bo prinesla uvedba IPv6, na drugi strani pa zaradi pocenitve programske in strojne opreme, ki podpira IPv6. Ta naj bi se pocenila zaradi vse bolj množičnega prehoda organizacij iz IPv4 na IPv6. Na ARSO so celotni stroški prehoda relativno nizki. Najvišji stroški bodo nastali zaradi nadgradnje specialne programske opreme, stroškov delovne sile in nepredvidljivih stroškov. Stroški za strojno opremo so nizki, saj večji del stikal in usmerjevalnikov na ARSO že podpira IPv6, na preostalih pa bo potrebna samo programska nadgradnja strojne opreme.

# 8 PILOTNA POSTAVITEV NOVEGA OMREŽJA IPV6

ARSO potrebuje zaradi svoje narave dela, ki zahteva, da je omrežje stalno dostopno, dve vstopni točki v internet. Tako je na enem koncu priključen na državno hrbtenično omrežje HKOM, na drugem koncu pa dostopa do interneta preko Arnesa. Prav dejstvo, da že imamo IPv4 povezavo z Arnesom, nam je omogočilo, da smo pred leti lahko pri njem zaprosili še za IPv6 naslovni prostor. Z dovoljenjem takratne vodje Službe za informatiko in vednostjo generalnega direktorja ARSO sem posredoval obrazec za prijavo na Arnes. Naši prošnji so ugodili in dobili smo naslovni prostor 2001:1470:FF82::/48.

## 8.1 Prehod na novi naslovni prostor

Arnes nam je v skladu s politiko dodeljevanja IPv6 naslovov dodelil naslovni prostor s predpono /48. To pomeni, da imamo lahko 65.536 podomrežij in v vsakem podomrežju skoraj neomejeno število naslovov, zato lahko razumemo, da je izdelava načrta planiranja IPv6 naslovov zelo pomembna za strukturirano in obvladljivo uvajanje IPv6 protokola. Priporočila za dodeljevanje naslovov lahko najdemo v RFC 6177.

Planiran naslovni načrt IPv6 predvideva, da so IPv6 naslovna področja združena učinkovito in logično. To ima več prednosti:

- varnostno politiko je lažje izvajati - enostavnejša konfiguracija seznamov dostopa in požarnega zidu;
- naslovi so lažje sledljivi, ker vsebujejo informacijo o vrsti rabe in/ali lokaciji, kjer je naslov v uporabi;
- učinkovit naslov je prilagodljiv; po potrebi ga lahko razširimo, da se vključi nova vrsta uporabe ali nova lokacija;
- smotrno načrtovanje naslovov IPv6 omogoča tudi učinkovitejše upravljanje omrežja.

Tako načrtovanje na videz lahko izgleda kot razmetavanje z IPv6 naslovi, vendar temu ni

tako, saj se preglednost dodelitve naslovov bistveno poveča, predvsem pa ogromno pridobimo na učinkovitosti celotnega sistema. Tako se na primer izognemo nepotrebnemu naraščanju usmerjevalnih tabel na usmerjevalnikih.

### 8.1.1 Predlog za razdelitev naslovnega prostora

ARSO ima dodeljen IPv6 naslovni prostor: 2001:1470:FF82::/48. Prvih 48 bitov nam je dodelil ponudnik, zadnjih 64 bitov pa lahko uporabimo za porazdelitev naslovov znotraj vsakega podomrežja. Načrt IPv6 naslovov torej obsega približno 48 do 63 bitov. To pomeni, da je na voljo 16 bitov za številko podomrežja. Teh 16 bitov bom razdelil v naslednje tipe (vrste) grup:

- B: bit je prenosljiv;
- L: bit je dodeljen lokaciji;
- T: bit je dodeljen tipu (vrsti) uporabe.

Naslednji zapis prikazuje dodeljevanje bitov:

| **2001:1470:FF82** | T | T | T | T | L | L | L | L | L | L | L | L | B | B | B | B | ::/64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Vsako polje predstavlja en bit. Štiri polja skupaj predstavljajo blok (štirje biti) in s tem eno šestnajstiško številko v IPv6 naslovu. Glede na zgornji primer dobimo naslednjo naslovno strukturo: 2001:1470:FF82:TLLB::/64.

Biti od 1-4 so dodeljeni glede na tip uporabe, biti od 5-12 so dodeljeni za lokacijo in biti od 13-16 so dodeljeni za nek drug namen. Z uporabo takega načina razdelitve IPv6 naslova bosta tako uporabljen tip kot lokacija identificirana na enostaven način. Simbol (T) identificira uporabljen tip in simbol (L) identificira lokacijo.

Dodeljevanje naslovov se bo izvajalo glede na tip in lokacijo uporabe. Tip bomo uporabili za predstavljanje primarnega podomrežja, lokacijo pa za sekundarno podomrežje. Število grup določa, koliko od 16 bitov, ki so na voljo, je potrebno uporabiti pri pripravi načrtovanja IPv6 naslova. En bit lahko vsebuje dve grupi ($2^1$), 2 bita lahko vsebujeta 4 grupe ($2^2$), trije biti lahko vsebujejo 8 grup ($2^3$) itd. Podrobnejšo razdelitev prikazuje Tabela 27.

*Tabela 27: Število zahtevanih bitov za vsako možno število grup*

| Biti | Tip uporabe (grupe) |
|---|---|
| 1 | 2 |
| 2 | 3 ali 4 |
| 3 | 5 - 8 |
| 4 | 9 - 16 |
| 5 | 17- 32 |

Število grup izračunamo na naslednji način: Najprej je potrebno določiti število uporabljenih tipov znotraj ARSO in število lokacij. Vsak uporabljen tip, kot tudi vsaka lokacija, se šteje kot ena grupa. Obvezno dodamo še eno grupo za hrbtenico in ostalo infrastrukturo in še eno ali dve grupi za možnost nadaljnje širitve.

Za ustvarjanje praktičnega naslovnega prostora razdelimo naslovni prostor v bloke, ki so potenca števila 2. Nato glede na število predvidenih grup to število zaokrožimo na najbližjo potenco števila 2. Najprej je potrebno ugotoviti, kateri del 16-bitnega naslovnega prostora, ki je na voljo, se bo uporabil glede na to, koliko tipov uporabe in lokacij imamo.

Določil sem naslednje tipe uporabe, na podlagi katerih bomo dobili število grup: strežniki, zaposleni, študentje, gosti. Število tipov uporabe obsega 4 grupe, hrbtenica in ostala infrastruktura pa obsega 1 grupo. Imamo torej 5 grup, zato število grup zaokrožimo na prvo večjo potenco števila dva. Za rezultat dobimo 8 grup. Vključitev teh grup v IPv6 naslovni prostor zahteva 3 bite ($2^3 = 8$). To pomeni, da imamo 8 grup - 5 je že določenih, ostanejo pa nam še 3 grupe za nadaljnjo širitev. To bi moralo zadoščati. Predvidimo, da bi v bodoče imeli 35 lokacij (meteorološke, hidrološke, seizmološke postaje…). V primeru, da uporabimo 6 bitov, bi imeli naslovni prostor za 64 ($2^6$) lokacij, kar je več kot dovolj. Sedaj imamo dodeljenih skupaj 9 bitov za primarno in sekundarno podomrežje. Ostane nam še 7 bitov. Teh 7 bitov lahko uporabimo za kreiranje 128 ($2^7$) omrežij glede na tip uporabe na posamezni lokaciji.

Na ta način dobimo sledečo naslovno strukturo:

| **2001:1470:FF82** | T | T | T | L | L | L | L | L | L | B | B | B | B | B | B | B | ::/64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Že takoj ugotovimo, da je iz tako strukturiranega naslova nemogoče izslediti grupo. Za izboljšanje berljivosti takega naslova ga bom razdelil v grupe po 4 bite.

| **2001:1470:FF82** | T | T | T | T | L | L | L | L | L | L | L | L | B | B | B | B | ::/64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Sedaj smo dobili za tip uporabe 4 bite in za lokacijo 8 bitov. Ostanejo nam še 4 biti za kreiranje omrežij glede na tip uporabe na posamezni lokaciji.

Preverimo, če nam to zadostuje. Ne zadostuje nam v primeru, če bi imeli zahtevo, da na posamezni lokaciji potrebujemo več kot 16 ($2^4$) strežniških omrežij. V takšnem primeru lahko uporabimo dodaten manevrski prostor, ki ga ustvarimo s pomočjo dodatnega bita glede na tip uporabe.

Zapis strukture IPv6 naslova s pomočjo simbolov: 2001:1470:FF82:TLLB::/64.

Tabela 28 prikazuje, kako lahko ob primernem načrtovanju IPv6 naslovnega prostora iz naslova na enostaven način ugotovimo, kateremu tipu uporabe IPv6 naslov pripada in na kateri lokaciji se nahaja ta tip uporabnika. Pri predstavitvi grup moramo biti pozorni na to, da so prikazane v šestnajstiškem sistemu, običajno pa jih štejemo v desetiškem sistemu: 23 šestnajstiško = 35 desetiško.

*Tabela 28: Primer razdelitve IPv6 naslova po tipu uporabe in lokaciji*

| **Tip(vrsta) uporabe** | **Lokacija** | **Prenosljiv** | **Omrežje** |
|---|---|---|---|
| Infrastruktura (0) | Ni vezana na lokacijo (0) | 0 | 2001:1470:FF82:000**0**::/ 64 |
| Infrastruktura (0) | Ni vezana na lokacijo (0) | 1 | 2001:1470:FF82:000**1**::/ 64 |
| Infrastruktura (0) | Ni vezana na lokacijo (0) | 2 | 2001:1470:FF82:000**2**::/ 64 |
| Infrastruktura (0) | Lokacija 1 | 0 | 2001:1470:FF82:001**0**::/ 64 |
| Infrastruktura (0) | Lokacija 35 | 0 | 2001:1470:FF82:023**0**::/ 64 |
| Strežniki (1) | Niso vezani na lokacijo (0) | 0 | 2001:1470:FF82:100**0**::/ 64 |
| Strežniki (1) | Lokacija 1 | 12 | 2001:1470:FF82:101**C**::/ 64 |
| Strežniki (1) | Lokacija **35** | 9 | 2001:1470:FF82:1**23**9::/ 64 |
| Itd. | | | |

*Vir: SURFnet, Preparing an IPv6 Address Plan, 2013, str. 23.*

## 8.2 Usmerjevalniki in gostiteljski računalniki

Prvi pogoj za dostop do interneta po IPv6 protokolu je, da usmerjevalnik prehoda (angl. *gateway router*) podpira IPv6 protokol. V primeru, da ga ne podpira, lahko naredimo lokalno mrežo odjemalcev, ki podpirajo IPv6 protokol. Ti bodo lahko komunicirali med

seboj. Za dostop do vsebin in storitev, ki tečejo na lokalnih strežnikih, pa morajo tudi lokalni strežniki podpirati IPv6.

Tabela 29 prikazuje, katera izmed različic operacijskega sistema je že naložena na usmerjevalniku prehoda, ki je v upravljanju Arnesa.

*Tabela 29: Usmerjevalnik prehoda (Arnes)*

| Naprava | IPv6 podprta verzija | Instalirana verzija |
|---|---|---|
| Cisco Catalyst 3750 E-Series | 12.2 | 12.2(50) |

Predpogoj za pilotno postavitev je torej usmerjevalnik prehoda, ki podpira tako IPv4 kot IPv6 protokol, torej dvojni sklad. Za minimalno testiranje delovanja potrebujemo še strežnik z dvojnim skladom, odjemalca, ki podpira samo IPv4 in odjemalca s podporo samo za IPv6 protokol. Za strežnik z dvojnim skladom sem postavil Windows 2012 R2 s storitvami IIS, DNS, DHCPv6 in RDP. Za IPv4 sem uporabil že obstoječi strežnik Windows 2003, ki ima omogočen samo IPv4 protokol in prenosni računalnik Windows 10 z omogočenim IPv6 protokolom.

Pilotno postavitev okolja IPv6 sem postavil za požarni zid, na internetno (zunanjo) stran ARSO omrežja. To pomeni, da gre ves promet mimo požarnega zidu. Za tako postavitev sem se odločil iz več razlogov:

- Požarni zid ostane nedotaknjen in ni bojazni, da bi z dodatnimi pravili povzročili varnostne luknje za obstoječe ARSO IPv4 omrežje. Promet se bo preusmeril skozi požarni zid, ko bo to potrebno.
- Testiranje je lažje nadzirati. Imamo manj naprav, ki jih je potrebno konfigurirati, zato je tudi možnost napak manjša.
- Trenutno na pilotnem omrežju ni podatkov, ki bi potrebovali dodatno varovanje. Nastavljeni filtri na usmerjevalniku prehoda in postavljen požarni zid na samih gostiteljih zadoščajo za te testne namene.

Vzpostavitev IPv6 omrežja na usmerjevalniku prehoda je potekala v dveh delih. Najprej je upravljalec usmerjevalnika prehoda Arnes vzpostavil IPv6 povezavo. Uporabljene so bile privzete vrednosti usmerjevalnika prehoda. To pomeni, da je bil promet preko vseh vrat onemogočen. Potem sem upravljalcu naročil, naj omogoči IPv6 dostop za protokole HTTP, HTTPS in RDP, ki omogočajo oddaljeni dostop.

Na zunanjem delu ARSO LAN (angl. *local area network*) omrežja sem postavil Windows 2012 R2 strežnik z dvojnim skladom in z naloženimi DNS, DHCPv6, RDP in IIS storitvami. Windows 2003 Server, ki ima podporo samo za IPv4 (vključujoč storitvi DNS

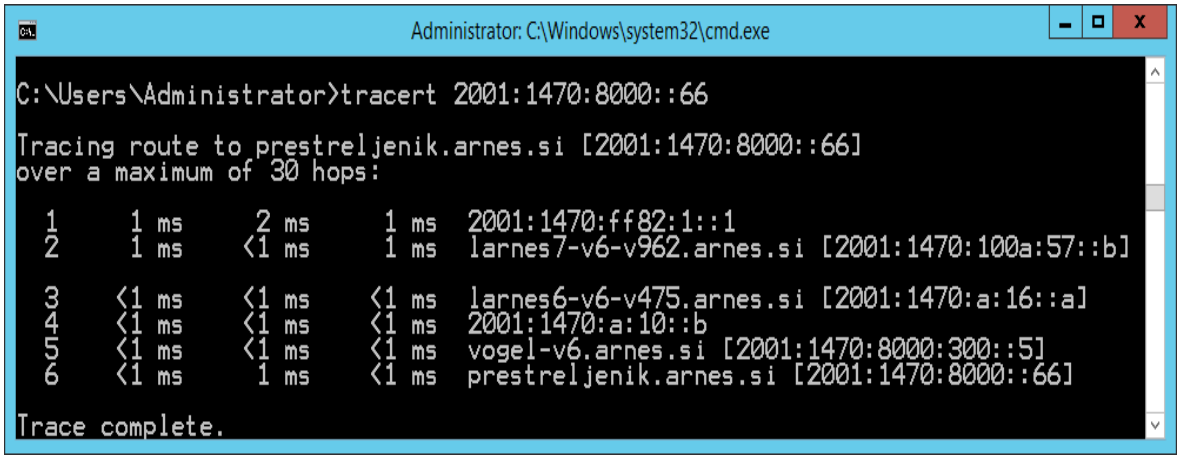
in DHCP), je bil v to omrežje že priključen. Nato sem v omrežje priključil še Windows 10 odjemalca z dvojnim skladom IPv4/IPv6. Temu odjemalcu se lahko po potrebi omogoči ali onemogoči eden ali drug IP protokol. Vse IPv6 naslove sem nastavil ročno. Avtomatsko dodelovanje naslovov IPv6 bom vzpostavil v naslednjem koraku. Najprej se moramo dogovoriti, kateri del naslovnega IPv6 področja bomo za avtomatsko naslavljanje dodelili. Pilotno omrežje se bo uporabljalo za testiranje delovanja aplikacij v okolju IPv6 in za testiranje delovanja dostopa po IPv6 protokolu iz ARSO v internet in obratno. Pilotno omrežje ponuja neizmerne možnosti za spoznavanje delovanja IPv6 protokola, in sicer brez časovnega pritiska in bojazni, da bi se kaj po nepotrebnem zapletlo.

## 8.3 Testiranje in nastavitve parametrov mreže

Glede na dobljeni IPv6 naslovni prostor s strani Arnesa sem strežniku Windows 2012 R2 dodelil IPv6 naslov 2001:1470:ff82:1:0:0:0:**230** (2001:1470:ff82:1::230). Pri tem sem poskušal ustvariti vsaj nekaj podobnosti med IPv4 in IPv6 naslovoma, zato sem nastavil v obeh naslovih enake zadnje tri številke. Njegov IPv4 naslov je 193.2.208.**230**.

Dostopnost usmerjevalnika prehoda po IPv6 protokolu sem preveril z ukazom: ping 2001:1470:ff82:1::1 in dostop do Arnes omrežja z ukazom: tracert 2001:1470:8000::66, kot kaže Slika 23.

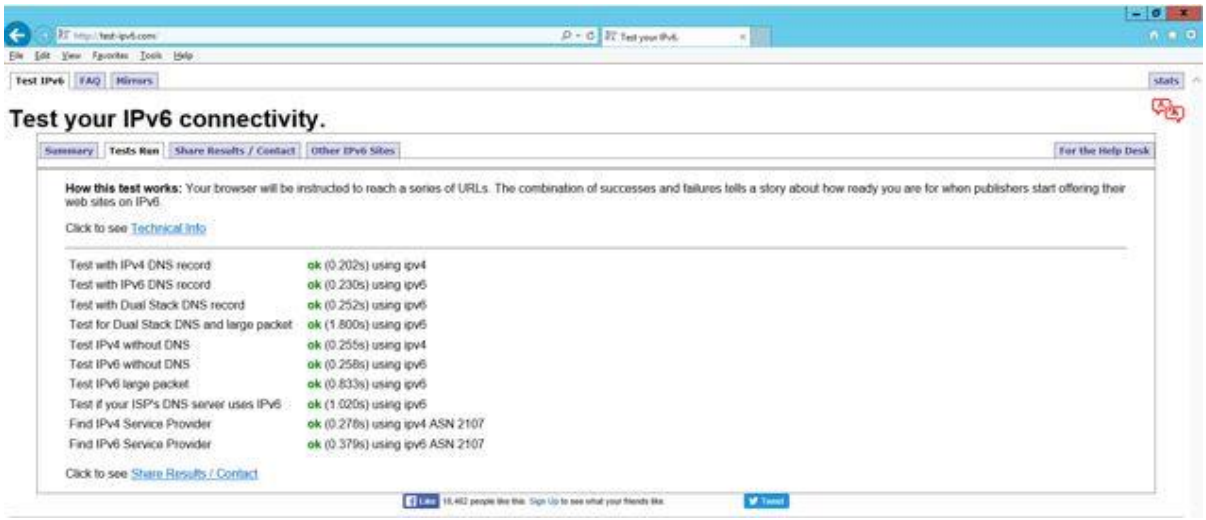
*Slika 23: Ukaz tracert do Arnes DNS strežnika*




Nato sem s pomočjo brskalnika na naslovu http://test-ipv6.com/ preveril delovanje IPv6 preko interneta.

Slika 24 nam pove, da je dostop iz pilotnega omrežja v internet možen tako po IPv4 kot po IPv6 protokolu.

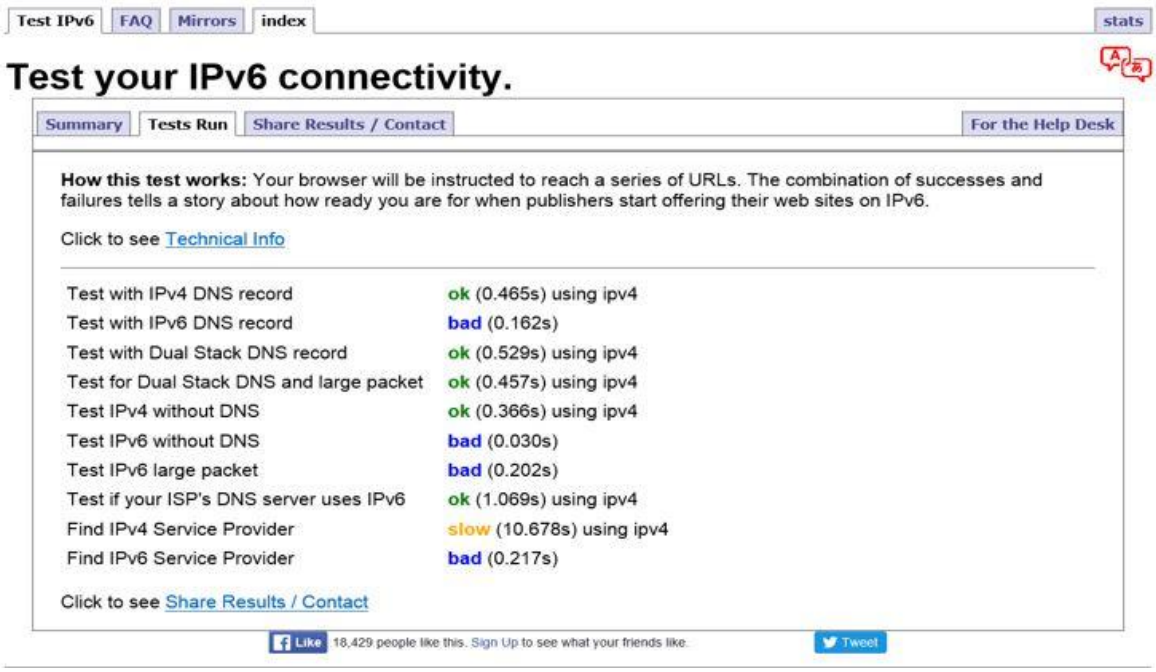
*Slika 24: Testiranje dostopa do IPv6 omrežja iz pilotnega omrežja ARSO*




*Vir: Test IPv6, 2016*

Slika 25 prikazuje, da nimamo dostopa do omrežja, ki podpira samo IPv6 protokol, kljub temu da naš usmerjevalnik prehoda to omogoča. To pa zato, ker gre ves promet preko požarnega zidu, ki smo ga pustili tako, kot je bil nastavljen za IPv4 protokol. Glede na postavljena pravila požarni zid prepušča IPv4 promet, ves IPv6 promet pa blokira.

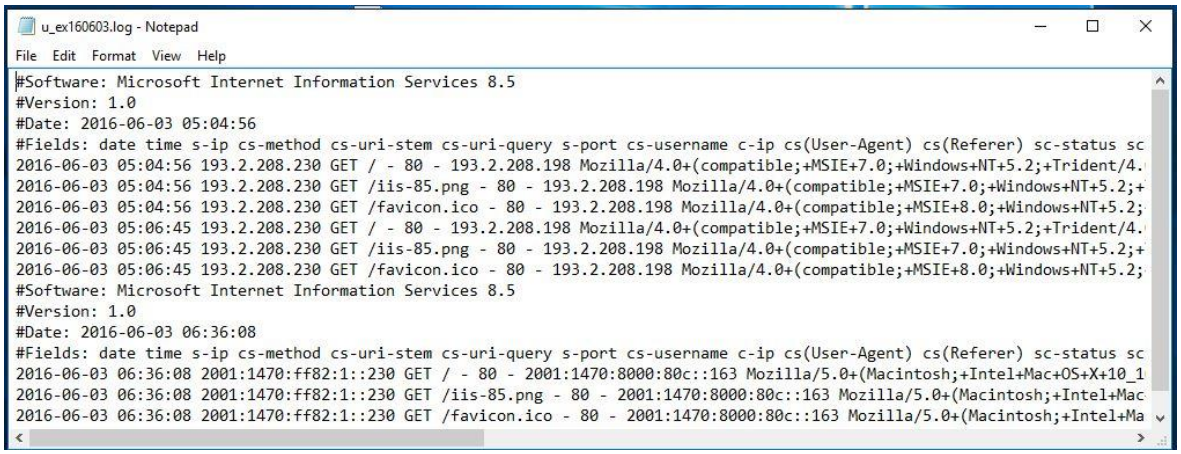
*Slika 25: Testiranje dostopa IPv6 omrežja iz intraneta ARSO preko požarnega zidu*




*Vir: Test IPv6, 2016*

Naslednji test, ki sem ga izvedel in je bil prav tako uspešen, je bil dostop do Windows 2012 R2 strežnika preko HTTP protokola. Dostop sem izvedel s pomočjo Internetnega brskalnika 11 z vpisom fizičnega naslova, ujetega med dva oglata oklepaja http://[2001:1470:ff82:1::230]. Dostope sem preveril tudi s pomočjo dnevnika, v katerega se beleži HTTP dostope do strežnika. To prikazuje Slika 26.

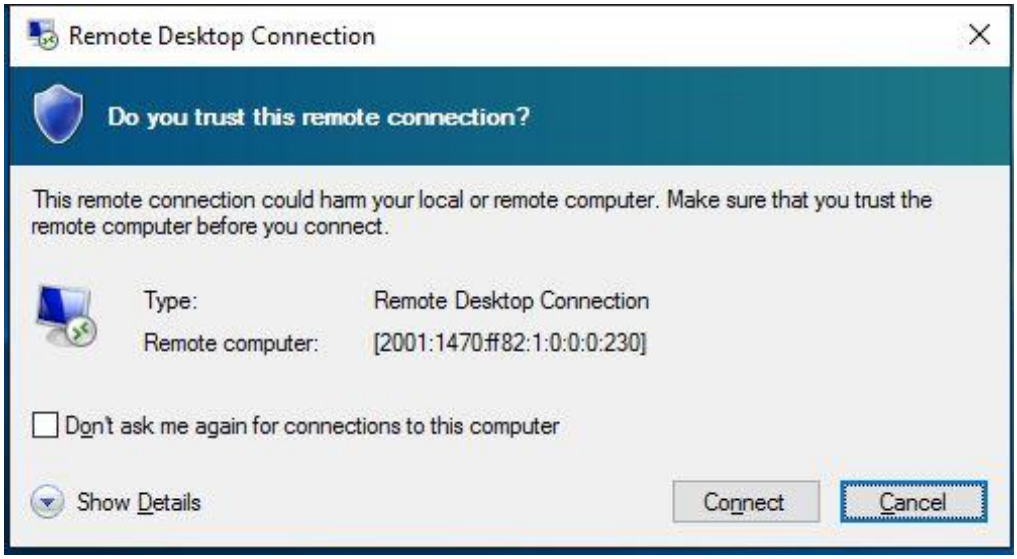
*Slika 26: Spletni dnevnik dostopov do Microsoft IIS strežnika v pilotnem omrežju*




Iz spletnega dnevnika strežnika je mogoče razbrati, da so zabeleženi tako dostopi iz IPv4 kot iz IPv6 omrežja.

Zadnji test, ki sem ga izvedel, je dostop do strežnika v pilotnem omrežju preko Microsoft RDP protokola, kot kaže Slika 27. Tudi tu je potrebno IPv6 naslov dati med dva oglata oklepaja. Do strežnika sem prišel z ukazom iz ukazne vrstice: mstsc /console /v [2001:1470:ff82:1:0:0:0:230].

*Slika 27: Oddaljeni dostop preko Microsoft RDP do IPv6 strežnika*



Dostop je bil možen šele, ko sem v požarnem zidu na samem strežniku omogočil IPv6 promet preko RDP vrat. To pomeni, da moramo biti vedno pozorni na to, da imamo dva protokola IPv4 in IPv6, kar pomeni tudi dvojno upravljanje omrežja in dvojno politiko dostopa na omrežju.

Vsi omenjeni testi so pokazali, da ARSO pilotno IPv6 omrežje deluje in pomeni dobro osnovo za nadaljnje korake pri pripravi prehoda na IPv6.

# SKLEP

Vsak dan se pojavlja več in več novih internetnih uporabnikov. Še veliko več pa je naprav, ki potrebujejo svoj IP naslov. Posledično je to privedlo do skorajšnjega izčrpanja IPv4 naslovnega prostora. Pomanjkanje IPv4 naslovov je zato postal glavni razlog za prehod na novi protokol. Vse ostale prednosti, ki jih prinaša IPv6, do sedaj niso prepričale odjemalcev k množični uporabi. V začetku pojava IPv6 so bili zadržki pri prehodu na IPv6 povezani predvsem s strojno opremo, ki še ni podpirala novega protokola in bi jo bilo zato potrebno zamenjati ali nadgraditi. Posamezni prodajalci strojne opreme, predvsem usmerjevalnikov, so za podporo IPv6 protokola zahtevali nakup programske licence. To je marsikoga odvrnilo od nadgradnje. Danes strojna oprema ne predstavlja ovire za prehod na IPv6, saj naprave že v osnovi nudijo podporo za IPv4 in IPv6. Razlog za počasen prehod na IPv6 je danes predvsem v pomanjkanju storitev in aplikacij, ki bi prinašale dodano vrednost sodobnejšemu IPv6 protokolu. Poleg tega je še vedno premalo strokovnega znanja in potrebnih finančnih sredstev za realizacijo prehoda. Razlog za oklevanju pri prehodu se skriva tudi v samem IPv4 protokolu, saj kljub strahovitemu naraščanju zahtev po novih resursih in storitvah deluje presenetljivo dobro. Tudi pomanjkanje IPv4 naslovnega prostora se dokaj uspešno rešuje. Obstajajo različni translacijski mehanizmi (NAT), ki navidezno povečujejo IPv4 naslovni prostor. Poleg tega imajo posamezni ponudniki še vedno v rezervi nekaj prostih javnih IPv4 naslovov, ki jih prodajajo ostalim ponudnikom. Vse to podaljšuje čas prehoda. Tehtnica se bo verjetno odločilno nagnila v prid IPv6 protokolu šele tedaj, ko bo dejansko popolnoma zmanjkalo IPv4 naslovnega prostora in bo cena nakupa IPv4 naslovov višja od stroškov prehoda na IPv6.

Kljub vsemu se promet IPv6 povečuje. Čeprav to pomeni le majhen delček celotnega interneta, je to obenem zelo hitro rastoč del interneta in nič ne kaže, da bi se njegova rast upočasnila. V začetku leta 2012 je IPv6 promet pomenil komaj 1 % vsega internetnega prometa, sredi leta 2015 je narasel preko 7 % in je trenutno na skoraj 10 %. Na povečanje IPv6 prometa med drugim vpliva tudi dejstvo, da so po IPv6 protokolu dostopni tudi vsi večji svetovni ponudniki vsebin (Facebook, Google, Microsoft, YouTube…). Tudi v Sloveniji se je v zadnjih letih situacija bistveno spremenila. Večina ISP ponuja možnost dostopa po obeh IP protokolih.

Kdaj se posamezna organizacija začne zavedati, da bo tudi sama morala nekaj storiti glede prehoda na IPv6, je odvisno od več dejavnikov - lahko jo k temu prisili trg, lahko njen poslovni partner, lahko se pojavi nova storitev, ki to zahteva. Veliko bolj ugodno je, da se organizacija pripravi na prehod na IPv6 še preden je to zares potrebno. V tem primeru sami določimo, na katerem delu omrežja bomo prehod opravili in s kakšnim tempom. Prav tako imamo na ta način dovolj časa, da analiziramo obstoječe stanje (popis strojne in programske opreme), se ustrezno izobrazimo in izberemo primeren trenutek prehoda. V primeru, da bi morali prehod narediti hitro in za vsako ceno, so lahko stroški prehoda zelo visoki.

Na ARSO smo se na prehod pripravili s postavitvijo pilotnega omrežja, po katerem bi se lahko zgledovale tudi preostale podobne organizacije. Postavitev pilotnega omrežja ne zahteva večjega finančnega vložka, pomeni pa pomemben doprinos na poti prehoda na IPv6. Pilotno omrežje deluje kot pravo omrežje in nam omogoča, da se seznanimo z vsemi storitvami, ki jih nudi nov protokol. Omogoča nam, da znanje, ki si ga pridobimo preko spleta in preko specializiranih izobraževanj, preverimo tudi v praksi. Naše razmišljanje o omrežju, ki je osredotočeno na IPv4, se mora prilagoditi IPv6. Preko uporabe pilotnega omrežja postane tudi zavedanje in razmišljanje o uvedbi IPv6 bolj jasno. Pomembno je, da pri vsakem vložku v informacijski sistem pomislimo, kaj to pomeni za prehod na IPv6. Ali nova naprava, aplikacija oz. storitev podpira IPv6 protokol? Izdelava aplikacije, ki podpira oba protokola, ne pomeni nujno tudi višjega finančnega vložka, vsaka nadgradnja aplikacije pa je zagotovo draga. Prav tako nam pilotno omrežje omogoča, da aplikacije, ki naj bi že podpirale delovanje v IPv6 okolju, tudi dejansko preverimo. Ključna je razdelitev naslovnega prostora. Preveriti je potrebno, v katerih primerih je smiselno ročno nastavljanje naslovov in v katerih avtomatsko. Poleg tega lahko preverimo in testiramo delovanje požarnega zidu. Postopoma odpiramo posamezna komunikacijska vrata, ki jih potrebujemo, in dostop testiramo. Izobraževanje je ključnega pomena, vendar brez možnosti uporabe v praksi izgublja na moči. Več kot se naučimo s pomočjo pilotne postavitve omrežja, manj neprijeten bo prehod za vse, tako uporabnike kot izvajalce. Ne da bi se pravzaprav zavedali, se na ta način izvaja analiza potrebnih sprememb, stroškov in časa. Izvedena analiza nas je tako obogatila z vhodnimi podatki za čimbolj eleganten in transparenten prehod.

Dobra stran prehoda je, da ga ni potrebno izvesti naenkrat. Lahko napredujemo po segmentih in sproti preverjamo, če so dani vsi potrebni pogoji za prehod (IPv6 podprta strojna, programska oprema) na posameznih delih. Priporočam, da se z delom na pilotnem omrežju nadaljuje in da se ga nadgrajuje. V testiranje naj se postopoma vključujejo storitve, ki doslej še niso bile zajete. Sočasno naj poteka izobraževanje vseh, ki so neposredno vpleteni (upravljalci omrežja, strežnikov, osebnih računalnikov, mobilnih naprav). Potek mora biti dobro koordiniran. Vsaj v prehodni fazi to pomeni za vse dodatno obremenitev. Potrebno je vzdrževati obstoječi sistem in uvajati novega, zato je pomembno, da se dela lotimo premišljeno in postopno, se sproti izobražujemo in premišljeno uvajamo

nove storitve. To prehodno obdobje bo glede na dosedanje izkušnje verjetno trajalo več let. V tem vmesnem času se bo IPv6 še naprej razvijal in postajal vse bolj razširjen, dokler se ne bo tehtnica začela nagibati v njegov prid. Že dolgo ni več vprašanje, ali naj se lotimo prehoda na IPv6, temveč le še - kdaj. ARSO je s pridobitvijo IPv6 naslova in pilotno postavitvijo omrežja že naredil prvi pomemben korak.

# LITERATURA IN VIRI


1. Arifin, A. H., Abdullah, D., Berhan, S. M, & Budiarto, R. (2006). An Economical IPv4-to-IPv6 Transition Model: A Case Study for University Network. *International Journal of Computer Science and Network Security*, *6*(11), 170-178.
2. ARSO. (2006). *Aplikacija SPIS 1.45, ARSO stalna zbirka (interno gradivo).* Ljubljana: ARSO.
3. Bieringer, P., Baraldi, F., Piunno, S., Tortonesi, M., Toselli, E., & Tumiati, D. (2014). Current Status of IPv6 Support for Networking Applications. Najdeno 22. aprila 2016 na spletnem naslovu http://www.deepspace6.net/docs/ipv6_status_page_apps.html
4. Cisco Systems. (2011). IPv6 Rapid Deployment: Provide IPv6 Access to Customers over an IPv4-Only Network. Najdeno 18. aprila 2016 na spletnem naslovu http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-665758.pdf
5. Cisco Systems. (2014). Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S. Najdeno 18. aprila 2016 na spletnem naslovu http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book.pdf
6. Comparison of IPv6 support in operating systems. Najdeno 28. junija 2016 na spletnem naslovu http://www.worldlibrary.org/articles/comparison_of_ipv6_support_in_operating_systems
7. Doyle, J. (2009). Large Scale NAT Architectures: NAT444 and NAT464. Najdeno 24. aprila 2016 na spletnem naslovu http://www.networkworld.com/article/2231905/cisco-subnet/large-scale-nat-architectures.html
8. Doyle, J. (2009). Understanding Dual-Stack Lite. Najdeno 20. aprila 2016 na spletnem naslovu http://www.networkworld.com/article/2232181/cisco-subnet/understanding-dual-stack-lite.html
9. Hagen, S. (2002). *IPv6 Essentials* (1st ed.). Beijing, China: O'Reilly Media.
10. Hagen, S. (2006). *IPv6 Essentials* (2nd ed.). Beijing, China: O'Reilly Media.
11. Horley, E. (2014). *Practical IPv6 for Windows Administrators*. New York, NY, USA: Apress.
12. Hudomalj, B. (2015). *Prostrano internetno omrežje ARSO* (interno gradivo). Ljubljana: ARSO.
13. IETF. (2006). IP Version 6 Addressing Architecture. Najdeno 30. maja 2016 na spletnem naslovu https://tools.ietf.org/html/rfc4291#section-2.5.7
14. IETF. (2006). IP Version 6 Addressing Architecture. Najdeno 30. maja 2016 na spletnem naslovu https://tools.ietf.org/html/rfc4291#section-2.6.1
15. IPv6 Support in Microsoft Products and Services. Najdeno 20. aprila 2016 na spletnem naslovu https://technet.microsoft.com/en-us/network/hh994905.aspx
16. Kunc, U. (2010). APEK - Prehod na IPv6: Razlogi in predlogi za uvedbo IPv6 v slovenska javna in zasebna komunikacijska omrežja. Najdeno 24. aprila 2016 na spletnem naslovu http://www.akos-rs.si/files/Prehod-na-IPv6-21.pdf

17. Loshin, P. (2004). *IPv6: Theory, Protocol, and Practice* (2nd ed.). San Francisco, CA, USA: Morgan Kaufmann Publishers.
18. McQuerry, S. (2008). *Interconnecting Cisco Network Devices, Part 1 (ICND1)* (1st ed.). Indianapolis, IND, US: Cisco Press.
19. Murphy, N. R., & Malone, D. (2005). *IPv6 Network Administration* (1st ed.). Beijing, China: O'Reilly Media.
20. Nishitani, T., Yamagata, I., & Miyakawa, S. (2009). Common Functions of Large Scale NAT (LSN). Najdeno 24. aprila 2016 na spletnem naslovu https://tools.ietf.org/html/draft-nishitani-cgn-02
21. O agenciji. Najdeno 3. junija 2016 na spletnem naslovu http://www.arso.gov.si/o%20agenciji/
22. Oracle Database and IPv6 Statement of Direction (2013). Najdeno 20. aprila 2016 na spletnem naslovu http://www.oracle.com/technetwork/database/enterprise-edition/oracledatabaseipv6sod-2141330.pdf
23. Podporni in nadzorni protokoli. Najdeno 29. maja 2016 na spletnem naslovu https://ipv6.si/protokol-ipv6/podporni-nadzorni-protokoli/
24. RidgeRun SDK IPv6 guide. Najdeno 18. aprila 2016 na spletnem naslovu https://developer.ridgerun.com/wiki/index.php/RidgeRun_SDK_IPv6_guide
25. Salus, P. (2000). *Big Book of IPv6 Addressing RFCs* (1st ed.). San Diego, CA, USA: Morgan Kaufmann Publishers.
26. Steffann, S. (2013). Making Content Available Over IPv6. Najdeno 20. aprila 2016 na spletnem naslovu http://www.internetsociety.org/deploy360/resources/making-content-available-over-ipv6/
27. SURFnet. (2013). Preparing an IPv6 Address Plan. Najdeno 24. aprila 2016 na spletnem naslovu http://www.ipv6forum.com/dl/presentations/IPv6-addressing-plan-howto.pdf
28. Teredo Overview. Najdeno 24. aprila 2016 na spletnem naslovu https://technet.microsoft.com/en-us/library/bb457011.aspx
29. Test IPv6. Najdeno 3. junij 2016 na spletnem naslovu http://test-ipv6.com/
30. Transition Mechanisms (IPv6) Part 2. Najdeno 18. aprila 2016 na spletnem naslovu http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-2/
31. Zavod Arnes. Najdeno 29. aprila 2016 na spletnem naslovu http://www.arnes.si/zavod-arnes/

# PRILOGE

**KAZALO PRILOG**

**PRILOGA 1: Zahtevek za pridobitev IPv6 naslovnega prostora**

REPUBLIKA SLOVENIJA
**MINISTRSTVO ZA OKOLJE IN PROSTOR**
**AGENCIJA REPUBLIKE SLOVENIJE ZA OKOLJE**
Vojkova 1b, 1001 Ljubljana p.p. 2608
tel.: 01 478 40 00 faks.: 01 478 40 52

ODPOSLANO
dne: 23 -06- 2006
Podpis: ...

ARNES
Jamova c. 39
g. MIHA DIMEC
1000 Ljubljana

Šifra: 35909-6/2006

Datum:22.06.2006

Zveza:

ZADEVA: **Zahtevek za pridobitev IPv6 naslovnega prostora**

Spoštovani,

Prosimo vas, da Agenciji RS za okolje, poleg obstoječega IPv4 naslovnega prostora, dodelite še IPv6 naslovni prostor.

Lepo vas pozdravljamo.

Dušan Rehberger

dr. Silvo Žlebir
GENERALNI DIREKTOR

Priloga:
- Zahtevek za pridobitev IPv6 naslovnega prostora (IPv6 End User Site Assignment Request Form)

SIQ ISO 9001 Q-629

CERTIFIED IQNet MANAGEMENT SYSTEM

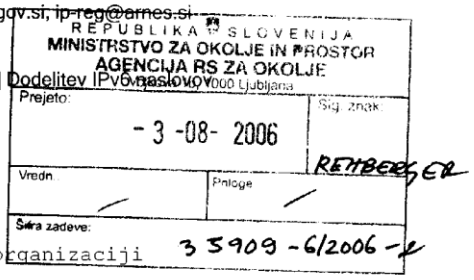
*Vir: Aplikacija SPIS 1.45, ARSO stalna zbirka (interno gradivo), 2006.*

## PRILOGA 2: Registracija IPv6 naslovnega prostora

ip-reg@arnes.si
Sent by:
mihael.dimec@arnes.si

03.08.2006 10:24

To silvo.zlebir@gov.si, barbara.hudomalj@gov.si
cc Dusan.Rehberger@gov.si, ip-reg@arnes.si
bcc
Subject [ARNES #10113353] Dodelitev IPv6 naslovov




Spostovani!

Za povezovanje v omrezje ARNES(internet), je vasi organizaciji dodeljen naslednji IP naslovni prostor:

2001:1470:FF82::/48

Obvestilu je dodana (gl. spodaj) koncna (ze registrirana) verzija obrazca, v katerem je razvidna razporeditev subnetov za dodeljeni IPv6 naslovni prostor.

Registracija IPv6 naslovnega prostora upravicencu omogoca zgolj uporabo dodeljenega prostora za dolocen cas (do prekinitve povezave na omrezje ARNES) in ne pomeni prenosa lastninske pravice.

Ko boste imeli vse (oprema, linija do omrezja ARNES ipd...) pripravljeno za vzpostavitev stalne povezave v omrezje ARNES, naj nam katera od vasih kontaktnih oseb, ki ste jih navedli v obrazcu, pise na naslov:

hw-podpora@arnes.si

da bomo uskladili datum in cas izvedbe povezave.

*Vir: Aplikacija SPIS 1.45, ARSO stalna zbirka (interno gradivo), 2006.*

**PRILOGA 3: Kratice in akronimi**

| | |
|---|---|
| **A** | |
| ADSL: | Aymetric Digital Subscriber Line |
| ARP: | Address Resolution Protocol |
| AS: | Autonomous System |
| | |
| **B** | |
| BGP: | Border Gateway Protocol |
| | |
| **C** | |
| CIDR: | Classless Inter-Domain Routing |
| CPU: | Central Processing Unit |
| CLNP: | Connectionless Network Protocol |
| CRC: | Cyclic Redundancy Check |
| | |
| **D** | |
| DARPA: | Defense Advanced Research Projects Agency |
| DECnet: | Digital Equipment Corporation net |
| DHCP: | Dynamic Host Configuration Protocol |
| DNS: | Domain Name System |
| | |
| **E** | |
| (E)IGRP: | (Enhanced) Interior Gateway Routing Protocol |
| | |
| **F** | |
| FreeBSD: | Free Berkely Software Distribution |
| FTP: | File Transfer Protocol |
| | |
| **H** | |
| HE: | Hurricane Electrics |
| HD: | Host Density |
| HKOM: | Hitro komunikacijsko omrežje znotraj državne uprave |
| HLEN: | Header Length |
| HTTP: | Hypertext Transfer Protocol |
| | |
| **I** | |
| ICANN: | Internet Corporation for Assigned Names and Numbers |
| ICMP: | Internet Control Message Protocol |
| IETF: | Internet Engineering Task Force |
| IGMP: | Internet Group Management Protocol |

| | |
|---|---|
| IIS: | Internet Information Services |
| IMAP: | Internet Message Access Protocol |
| IPng: | IP next generation |
| IPsec: | Internet Protocol security |
| IPX: | Internetwork Packet Exchange |
| ISATAP: | Intra-Site Automatic Tunnel Addressing Protocol |
| ISO/OSI: | International Organization for Standardization/Open Systems Interconnection |
| ISP: | Internet Service Provider |
| ISATAP: | Intra-Site Automatic Tunnel Addressing Protocol |
| | |
| **L** | |
| LAN: | Local Area Network |
| LDAP: | Lightweight Directory Access Protocol |
| | |
| **M** | |
| MFERAC: | Enotni računovodski sistem Ministrstva za finance |
| MTU: | Maximum Transmission Unit |
| | |
| **N** | |
| ND: | Neighbor Discovery |
| NAT: | Network Address  Translation |
| NCP: | Network Control Program |
| NS: | Name Server |
| | |
| **O** | |
| OSPF: | Open Shortest Path First |
| | |
| **P** | |
| PI: | Provider Independent |
| POP3: | Post Office Protocol |
| PPP: | Point-to-Point |
| | |
| **R** | |
| RAM: | Random Access Memory |
| RDNSS: | Recursive DNS Server |
| RFC: | Request for Comments |
| RIP: | Routing Information Protocol |
| RIR: | Regional Internet Registry |
| RMDCN: | Regional Meteorological Data Communication Network |
| RTSP: | Real time Streaming Protocol |

| | |
|---|---|
| | |
| **S** | |
| SIP: | Session Initiation Protocol |
| SMTP: | Simple Mail Transfer Protocol |
| SPIS: | SRC Pisarniški Informacijski Sistem |
| SQL: | Structured Query Language |
| SSH: | Secure Shell |
| SSL: | Secure Sockets Layer |
| | |
| **V** | |
| VPN: | Virtual Private Network |
| VPN MPLS: | Virtual Private Network  Multiprotocol Label Switching |
| | |
| **T** | |
| TB: | Tunnel Broker |
| TCP/IP: | Transmission Control Protocol/Internet protocol |
| TLS: | Transport Layer Security |
| TTL: | Time to Live |
| | |
| **U** | |
| UDP: | User Datagram Protocol |
| | |
| **V** | |
| VLSM: | Variable Length Subnet Masking |
| VPN: | Virtual Private Networks |
| | |
| **Q** | |
| QoS: | Quality of Service |