

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Martin Štokelj

Vpeljevanje internetnega protokola IPv6 v podjetja

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

MENTOR: viš. pred. dr. Damjan Vavpotič

Ljubljana, 2011

Rezultati diplomskega dela so intelektualna lastnina Fakultete za računalništvo in Informatiko Univerze v Ljubljani. Za objavljane ali izkoriščanje rezultatov diplomskega dela je potrebno pisno soglasje Fakultete za računalništvo in informatiko ter mentorja.



Št. naloge: 00136/2011

Datum: 01.09.2011

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MARTIN ŠTOKELJ**

Naslov: **VPELJEVANJE INTERNETNEGA PROTOKOLA IPV6 V PODJETJA
IMPLEMENTATION OF INTERNET PROTOCOL IPV6 IN
ENTERPRISES**

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

V okviru diplomskega dela predstavite internetni protokol IPv6, ga primerjajte s protokolom IPv4 ter preučite različne vidike njegove vpeljave v podjetja. V prvem delu naloge predstavite tehnološke razlike med protokoloma in novosti, ki jih prinaša protokol IPv6. V drugem delu naloge se posvetite pristopom k vpeljevanju protokola IPv6 v podjetja pri čemer preučite tako tehnološke kot ekonomske vidike vpeljevanja.

Mentor:

viš. pred. dr. Damjan Vavpotič

Dekan:

prof. dr. Nikolaj Zimic

IZJAVA O AVTORSTVU

diplomskega dela

Spodaj podpisani **Martin Štokelj**,

z vpisno številko **63060336**,

sem avtor diplomskega dela z naslovom:

Vpeljevanje internetnega protokola IPv6 v podjetja

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom:

viš. pred. dr. Damjan Vavpotič

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne _____ Podpis avtorja: _____

ZAHVALA:

Posebna zahvala gre moji družini za podporo tekom študija in pri pisanju diplomskega dela.

Zahvala gre tudi mojemu mentorju viš. pred. dr. Damjanu Vavpotiču ter Janu Žoržu za strokovno pomoč in nasvete pri izvedbi diplomskega dela.

Kazalo

Povzetek	1
Abstract.....	2
1. Uvod	3
2. Kaj je IP?	4
2.1 Glava IPv4	7
2.2 Varnost v IPv4	8
2.3 Mehanizmi, ki zmanjšujejo porabo IPv4 naslovov	8
3. IPv6.....	9
3.1 Zakaj IPv6?	9
3.1.1 Pomanjkanje naslovnega prostora	9
3.1.2 Rešitev za pomanjkanje naslovnega prostora.....	10
3.2 Naslov IPv6.....	11
3.2.1 Format naslova IPv6.....	11
3.2.2 Vrste naslavljanj IPv6	12
3.2.3 Dodeljevanje naslovov IPv6.....	12
3.3 Zgradba paketa IPv6	13
3.4.1 Datagram IPv6.....	13
3.4.2 Razširitvena glava IPv6.....	15
4. Varnost v IPv6.....	16
4.1 IPsec.....	16
4.2 Kakovost storitev QoS	17
4.2.1 Prednosti QoS-a.....	18
5. IPv6 in IPv4.....	19
5.1 Primerjava	19
5.2 Združljivost med protokoloma.....	22
5.2.1 Uporaba obeh protokolov	22
5.2.2 Tunelski mehanizem IPv6 skozi IPv4.....	24
5.2.3 Translacija protokola.....	28
6. Prednosti in slabosti IPv6	30
6.1 Prednosti IPv6.....	30
6.1.1 Novosti in spremembe.....	31

6.2 Slabosti IPv6	32
7. Problem uporabe IPv6	32
7.1 Prevajanje SIIT	32
7.1.1 Prevajanje SIIT iz IPv4 v IPv6.....	32
7.1.2 SIIT prevajanje iz IPv6 v IPv4.....	33
7.2 Nadgradnja SIIT z IVI	33
8. Kako do prehoda na IPv6	33
8.1 Prehod na IPv6 v Sloveniji	34
8.1.1 Analiza obstoječega stanja uvedbe IPV6 v Sloveniji.....	35
8.1.2 Stanje uvedbe in dosegljivost slovenskih spletnih mest preko IPv6.....	36
9. Postopek uvajanja IPv6 v omrežje.....	37
9.1 Pregled lastnosti	38
9.2 Stanje standardizacije IPv6	39
9.3 Uvedba IPv6	40
9.3.1 Uvedba IPv6 v manjše podjetje.....	40
9.3.2 Koraki za prehod	42
9.3.3 Primer	42
9.4 Podpora IPv6.....	43
9.4.1 Podpora pri operacijskih sistemih	43
9.4.2 Podpora pri aplikacijah.....	44
9.5 Stroški za podjetja.....	45
10. Zaključek	48
11. Viri.....	50

Seznam uporabljenih kratic in simbolov

IP	(Internet Protocol) – internetni protokol
ISP	(Internet service provider) – ponudnik internetnih storitev
TTL	(Time to Live) – mehanizem, ki omejuje življenjsko dobo podatkov v računalniku ali omrežju
IETF	(Internet Engineering Task Force) – delovna skupina za internetno tehniko
GPS	(Global System for Mobile communications) – svetovni standard mobilnih komunikacij
GPRS	(General Packet Radio Service) – mobilna podatkovna storitev v okviru standarda GSM
UMTS	(Universal Mobile Telecommunications System) – ena ključnih tehnologij in sestavni del tretje generacije mobilnih sistemov GSM
WLAN	(Wireless LAN) – brezžično lokalno omrežje
NAT	(Network Address Translation) – proces spreminjanja IP naslova v glavah paketov.
PDA	(Personal Digital Assistant) – mobilna naprava, ki deluje kot osebni upravitelj informacij
TCP/IP	(Transmission Control Protocol) – protokol za nadzor prenosa
DNS	(Domain Name System/Service/Server) – sistem domenskih imen
IPsec	(Internet Protocol Security) – predstavlja okvir odprtih standardov, ki zagotavljajo varnost za prenos podatkov skozi omrežje
ARNES	Akadska in raziskovalna mreža Slovenije
DHCP	(Dynamic Host Configuration Protocol) – Protokol za dinamično nastavitve gostitelja
MAC address	(Media Access Control address) - Fizični naslov naprave na ravni strojne opreme
HTTP	(HyperText Transfer Protocol) – protokol za izmenjavo tekstovnih, grafičnih in drugih večpredstavnostnih vsebin na spletu
VPN	(Virtual Private Network) – mehanizem za zagotavljanje varnega prenosa podatkov po internetu
SSL	(Server Sockets Layer) – mehanizem za zagotavljanje varnosti pri prenosu podatkov, največkrat za zaščito različnih transakcij
QOS	(Quality of Service) – pojem kakovosti storitev na področju računalniških mrež in drugih telekomunikacijskih omrežjih
BIS	(Bump-In-the-Stack Mechanism) – translacijski mehanizem med IPv4 aplikacijo ter IPv6 omrežjem
SIIT	(Stateless Ip/Icmp Translation algorithm) – prevajalni algoritem
CIDR	(Classless Interdomain Routing) – metoda za dodeljevanje IP naslovov in usmerjanje paketov internetnega protokola
PAT	(Port Address Translation) – mehanizem za prevajanje zasebnih IP naslovov v zunanje IP naslove s pomočjo vrat
DHCPv6	(Dynamic Host Configuration Protocol) – boljša rešitev za dodelitev IPv6 naslovov in drugih konfiguracij kot potekajo danes z DHCP v IPv4
PDU	(Protocol Data Unit) – protokolna podatkovna enota
RFC	(Request for Comments) – dokument, ki določa tehnične vidike Interneta

Povzetek

Diplomska naloga opisuje internetna protokola IPv4 in IPv6, primerjavo med njima, mehanizme za zagotavljanje varnosti in mehanizme, ki so pripomogli k zmanjšanju porabe naslovnega prostora IPv4. Podrobno je opisan protokol IPv6, njegove prednosti, slabosti, težave pri uporabi in združljivost z obstoječim protokolom IPv4. Opisano je uvajanje protokola IPv6 v podjetja in stroški, ki lahko nastanejo v podjetju ob prehodu na protokol IPv6.

Ključne besede: IPv6, IPv4, IPsec

Abstract

The thesis describes the Internet Protocol, IPv4 and IPv6, the comparison between them, mechanisms to ensure safety and mechanisms that have contributed to reducing the consumption of IPv4 address space. It also describes in detail the IPv6 protocol, its strengths, weaknesses, problems of use and compatibility with the existing IPv4 protocol. Described the deployment of IPv6 in the businesses and the costs, which may be incurred in undertaking the transition to IPv6.

Key words: IPv6, IPv4, IPsec

1. Uvod

Naloga protokola IP je usmerjanje (ang. routing) paketov med različnimi omrežji povezanimi v internet. Naloga protokola TCP je podatkovni tok razdeliti na manjše dele (v segmente), ki jih nato med omrežji prenaša IP.

Načrtovalci protokola IP (IPv4) so za velikost naslovnega prostora predvideli 32-bitno število, kar nam teoretično omogoča, da s protokolom IP naslovimo dobre 4 milijarde naslovov. Ta omejitev je danes glavna, slabost protokola IPv4. Ker bo kmalu zmanjkalo naslovov IPv4 je prihod novega internetnega protokola neizogiben.

Statistiko naslovnega prostora IPv4 lahko opazujemo na spletnih straneh. Ena izmed njih je tudi <http://www.potaroo.net/tools/ipv4/index.html>.

Razvoj IPv6 se je tako zaradi pomanjkanja naslovov IPv4 začel že leta 1995. 128-bitni naslovni prostor protokolu IPv6 omogoča $3,4 \times 10^{38}$ razpoložljivih naslovov. IPv6 odpravlja omejitve, ki jih ni rešilo podaljševanje uporabe protokola IPv4 in uvaja veliko novosti.

Če uvajanje IPv6 ne bo močno pospešeno, bo prišlo do izjemne upočasnitve rasti interneta, ostanki IPv4 v omrežjih pa bodo povečali stroške uporabe interneta. Posledica te zamude pri uvajanju bodo večji stroški na vseh področjih internetnih storitev. Soočiti se bo potrebno tudi z upočasnitvijo inovacij v omrežjih, ki temeljijo na internetnem protokolu.

V diplomski nalogi predstavljam protokol nove generacije IPv6 ter primerjavo med protokoloma IPv4 in IPv6. Poudaril sem, kaj pomeni internetni protokol in zakaj je nov protokol pomemben. Opisujem tudi prehode na protokol IPv6, vpeljave protokola IPv6 v podjetja in stroške, ki bi pri prehodu nastali ter prednosti in slabosti, ki jih prinaša uporaba IPv6 v poslovnih informacijskih sistemih.

2. Kaj je IP?

Naslov IP je logični naslov, ki se dodeli vsem napravam, ki komunicirajo v internetnem omrežju. Podatki se v omrežja IP pošljejo v obliki blokov, ki jih imenujemo paketi ali datagrami in se prenašajo skozi vozlišča po principu preklapljanja paketov. Datagrami, poleg vseh drugih polj v glavi paketa, vsebujejo tudi izvorni naslov IP, ki sporočilo odpošilja in ciljni naslov IP, kateremu je sporočilo namenjeno. Naprave, ki usmerjajo pakete skozi računalniško omrežje, imenujemo usmerjevalniki.

Vsak računalnik oz. omrežni vmesnik ima svoj naslov IP. Ti naslovi IP so shranjeni v dvojiškem zapisu, običajno pa so prikazani desetiško oz. šestnajstiško, da jih lažje zapišemo ali preberemo. Obstajata dve vrsti naslovov IP:

IPv4, ki ima 32 bitov (primer: 208.77.188.166) in

IPv6, ki ima 128 bitov (primer: 2009:db8:0:1234:0:567:1:1).

Danes je še vedno večinoma v uporabi različica IPv4, vendar zaradi izredno hitre rasti števila uporabnikov interneta zmanjkuje naslovnega prostora. Vsak uporabnik dobi svoj naslov IP pri svojem ponudniku internetnih storitev (ISP). Ponudnik internetnih storitev pa dobi potreben razpon naslovov IP od regionalnega registra internetnih naslovov.

Glavne naloge protokola IP:

- naslavljanje in informacije za usmerjanje datagramov,
- delitev paketov transportne plasti,
- upoštevanje časa TTL z izločanjem paketov, ki so že predolgo v omrežju,
- označevanje paketov glede prioritete,
- kontrola vsote, ki se nahaja v glavi paketa.

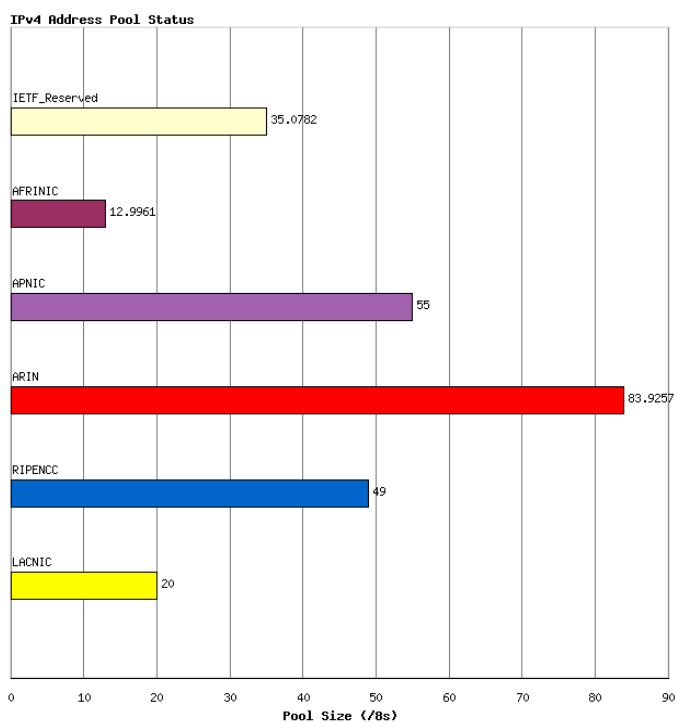
Glavni register IP naslovov vzdržuje organizacija IANA (angl. Internet Assigned Numbers Authority), ki je odgovorna za upravljanje registra naslovov IP. Izvaja tudi globalno koordinacijo korenskih strežnikov DNS in upravljanje s koreninskimi conami, ter dodeljuje druge vire, ki se nanašajo na internetni protokol.

IANA upravlja s celotnim naborom naslovov IP, vendar sama direktno ne dodeljuje blokov IP zainteresiranim končnim strankam, temveč pooblašča regionalne internetne registrarje (angl. Regional Internet Registries - RIR), ki nato naslove IP razdeljujejo med svoje člane, ki so predvsem lokalni internetni registrarji (na nivoju posamezne države) ali pa internetni ponudniki ter operaterji.

V svetovnem merilu imamo pet regionalnih internetnih registrarjev, ki pokrivajo vsak svoje področje sveta:

- AFRINIC (Afrika)
- APNIC (Azija in pacifiška regija)
- LACNIC (Latinska Amerika in Karibsko otočje)
- RIPE NCC (Evropa, srednji Vzhod in centralna Azija)
- ARIN (Severna Amerika)

Bistvenih razlik pri dodeljevanju naslovov IP med registrarji ni, saj se naslove dodeljuje praviloma na podlagi izraženih in utemeljenih potreb. Če je registrarjem začelo zmanjkovati naslovov IP, so podali zahtevek za dodatne naslove IP na organizacijo IANA.

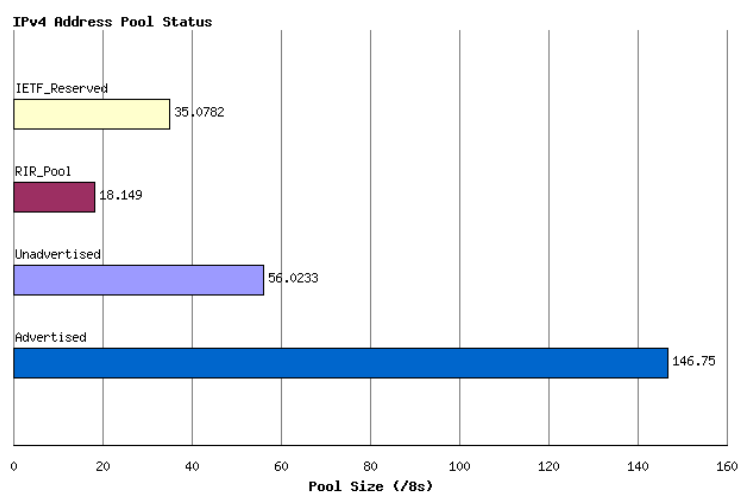


Slika 1: Stanje naslovov IPv4 po blokih (2011).

Iz slike 1 je razvidno, da je IANA vseh 256 blokov s predpono /8 že porazdelila med regionalne internetne registrarje.

Slika 2 pa prikazuje trenutne naslove IPv4, ki jih lahko razdelimo v 4 razrede:

- Dodeljeni in oglaševalni naslovi BGP.
- Nedodeljeni naslovi RIP.
- Rezervirani ali uporabljeni za eksperimentalne namene.
- Dodeljeni naslovi končnim uporabnikom, ki niso oglaševani v usmerjevalnih protokolih.



Slika 2: Razdelitev naslovov IPv4 (2011).

Pomanjkanje naslovnega prostora IPv4 ni edini razlog zaradi katerega bi morali izvesti prehod na IPv6, je pa vsekakor velik dejavnik.

2.1 Glava IPv4



Slika 3: Glava protokola IPv4.

Polja v glavi IPv4 so (Slika 3):

- Različica (angl. version): številka različice protokola IP.
- Velikost zaglavja (angl. head length): velikost glave.
- Vrsta storitve (angl. type of service): pove nam, kako naj se ravna s paketom.
- Skupna velikost (angl. total length): velikost celotnega paketa (glave in podatkovnega dela).
- Identifikacija (angl. identification): enolična vrednost vsakega paketa IP.
- Zastavice (angl. flags): nam povedo ali se lahko paket fragmentira, ali ne. Fragmentacija nam omogoča prenos paketov po različnih omrežjih, ki nimajo enako velike vrednosti MTU (največja enota prenosa).
- Odmik fragmenta (angl. fragment offset): nam omogoča fragmentacijo in ponovno sestavljanje paketa.
- Življenjska doba (angl. Time To Live): določa življenjsko dobo paketa. Na ta način preprečimo, da bi paket v neskončnosti krožil po omrežju.
- Protokol (angl. protocol): vrednost, ki pove kateremu protokolu na transportni plasti ali omrežni plasti IP, preda paket.
- Kontrolna vsota zaglavja (angl. header checksum): ciklično preverjanje redundance na glavi paketa.
- Izvorni naslov (angl. source address): 32-bitni naslov naprave, ki je poslala paket.
- Ciljni naslov (angl. destination address): 32-bitni naslov naprave, ki je naslovnik paketa.

2.2 Varnost v IPv4

Skupino protokolov TCP/IP so zasnovali za delovanje v omrežju z relativno zaupanja vrednimi uporabniki, kjer je bila omrežna infrastruktura relativno varna, informacije, ki so se prenašale, pa so bile relativno javne. Zato se takrat vključitev varnostnih funkcij, kot sta overitev uporabnikov, šifriranje in zagotavljanje celovitosti prometa neposredno v protokol IPv4, ni zdela potrebna. Ker pa se je v naslednjih desetletjih način uporabe interneta korenito spremenil in ga danes uporablja že več kot milijarda in pol ljudi, kateri niso vsi zaupanja vredni, lahko rečemo, da je IPv4 iz varnostnega vidika svoji nalogi nedorasel.

Ena izmed rešitev varnosti v IPv4 je IPsec, ki je neodvisen od aplikacij na višjem nivoju. Tunel IPsec varuje ves promet v njem ter zagotavlja overitev in šifriranje. Po drugi strani pa je IPsec obvezen del samega protokola IPv6 (več o tem v nadaljevanju).

2.3 Mehanizmi, ki zmanjšujejo porabo IPv4 naslovov

Največje povpraševanje po naslovih se je začelo že v drugi polovici devetdesetih, ko so se odpirala nova podjetja. Takrat so lahko podjetja uporabila nov nepoznan protokol (IPv6) ter veliko investirala v takrat še zelo drago in nepreverjeno opremo, ki ta protokol podpira ali pa uporabila obstoječi protokol IPv4, ki ni zahteval velikih dodatnih vložkov.

Mehanizmi:

- Vpeljava mehanizma CIDR ter zasebnih naslovov IP je omejila uporabo naslovnega prostora IPv4. Prednost, ki jo prinaša mehanizem CIDR je združevanje internetnih poti, ki omogoča, da se omrežje sestavlja iz večjega števila podomrežij, na zunaj oglašuje kot eno veliko matično omrežje.
- NAT je drugi mehanizem, ki je bistveno omejil porabo javnih naslovov IPv4. NAT-PT (angl. Network Address Translation-Port Translation), ki je običajno implementiran kot del funkcionalnosti požarne pregrade, omogoča jasno ločevanje med javnimi in zasebnimi omrežji. Naprave NAT-PT imajo na strani interneta dodeljen en ali več javnih globalnih naslovov, na strani zasebnega omrežja pa se uporablja zasebne naslove IP, ki so predpisani z internetnim standardom RFC1918.

Ko bodo vsi javni naslovi IPv4 zasedeni, bo internet deloval še naprej. Obstoječi operaterji bodo imeli možnost, da postopoma preidejo na protokol IPv6 ali pa nadaljujejo z obstoječim protokolom IPv4, pri čemer si bodo morali pomagati s translacijskimi mehanizmi.

3. IPv6

3.1 Zakaj IPv6?

Stalna rast interneta zahteva prilagajanje novim tehnologijam, ki podpirajo naraščajoče število uporabnikov, aplikacij, naprav in storitev. IPv6 je zasnovan tako, da izpolnjuje vse te zahteve. Trenutni naslovni prostor ne more izpolnjevati porasta ogromnega števila uporabnikov ali širitve interneta, kaj šele zahteve nastajajočih aplikacij, kot so osebni digitalni pomočniki (PDA), domača območja interneta (HANs), z internetom povezani avtomobili, integrirane telefonske storitve, itd. Uporaba IPv6 protokola poenostavlja mehanizme za doseganje varnosti internetnih naprav in funkcij, ki so bistvenega pomena za aplikacije in storitve in so tudi gonilna povpraševalna sila za proste IP naslove.

3.1.1 Pomanjkanje naslovnega prostora

Od leta 1981, ko je bil postavljen IPv4, se je naslovni prostor hitro polnil. Leta 2000 je bil polovično zaseden, konec 2002 pa že dvotretjinsko. Na tabeli 1 lahko vidimo razpoložljivost in zasedenost IP naslovov (po analizah spletne strani <http://www.bgpexpert.com>). V letu 2009 je bilo porabljenega približno 80% razpoložljivega IP naslovnega prostora.

Datum	Prosti naslovi v milijonih	Novo zasedeni naslovi v milijonih
01.01.2006	1468.61	
01.01.2007	1300.65	167.96
01.01.2008	1122.85	177.80
01.01.2009	925.58	197.27
01.01.2010	722.18	203.40

Tabela 1: Tabela uporabljenih in še razpoložljivih IP naslovov v letu (2010).

Zmanjševanje naslovnega prostora je prisililo veliko uporabnikov in organizacij k uporabi mehanizma NAT, ki lahko na javni naslov IP veže več zasebnih naslovov, ti pa se lahko podvajajo med zasebnimi omrežji. Kot nadgradnja mehanizma NAT se je uveljavil tudi mehanizem PAT, ki pakete iz javnega omrežja preusmeri v zasebno omrežje preko tabel, ki jih vzdržuje v času komunikacije. Uporaba teh mehanizmov je povzročila drastičen upad porabe javnih IP naslovov.

3.1.2 Rešitev za pomanjkanje naslovnega prostora

IPv6 predstavlja rešitev za problem, ki nastaja pri IPv4, kjer počasi primanjkuje prostih IP naslovov. V decembru leta 1998 je IETF določil IPv6 za naslednika IPv4 protokola.

Vedno več ljudi uporablja mobilne telefone in ročne računalnike, ki tudi pripomorejo k zmanjševanju prostih naslovov. S prihodom IPv6 protokola bo ta problem rešen, ker ta zagotavlja dovolj IP naslovov za vse večje število uporabnikov internetnih storitev.

Zahteve po novih naslovih prihajajo tudi s strani uporabniških aplikacij:

- Mobilne storitve, ki so sprva temeljile na GPRS, sedaj pa na UMTS,
- razširitev mobilnih WLAN tehnologij (802.11),
- širokopasovni dostop in stalna povezava v internet,
- elektronika in vozila, ki imajo povezavo v internet,
- avtomatika doma, ki je podprta z omrežji senzorjev.

IPv6 bo tako imel večji naslovni prostor, ki bo omejen s 128 biti in ne več z 32 biti kot IPv4. Za današnji čas pa to predstavlja zelo veliko število IP naslovov.

Sprva IPv4 protokol ni bil mišljen kot protokol za komercialno uporabo. IPv4 naslove so tudi razdelili neenakomerno. Pri tem je največji delež dobila severna Amerika, ki je dobila kar 74% vseh IP naslovov, s 17% je sledila Evropa, ostalih 9% pa je dobila Azija, zato je tudi v Aziji prehod na IPv6 protokol najbolj dinamičen.

Glavne prednosti prehoda na protokol IPv6:

- hierarhično naslavljanje,
- samodejno nastavljanje,
- multicast (naslavljanje izbrane skupine),
- podpora mobilnim komunikacijam,
- jedro IPv6 je stabilno in primerno za komercialno uporabo,
- večji naslovni prostor,
- spreminjanje javnih naslovov v privatne brez NAT,
- enostavnejša glava,
- učinkovitejše usmerjanje,
- ni broadcasta,
- mobilnost in varnost,
- vgrajena podpora varnosti (IPsecurity),
- mobilnost vgrajena v sam IPv6.

3.2 Naslov IPv6

3.2.1 Format naslova IPv6

IPv6 naslov ima naslednjo obliko:

xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx

kjer vsak xxxx predstavlja 16-biten blok, zapisan šestnajstiško.

Primer naslova:

2009:0db8:0000:0000:0000:0000:1428:57ab

Pri IPv6 naslovih velja:

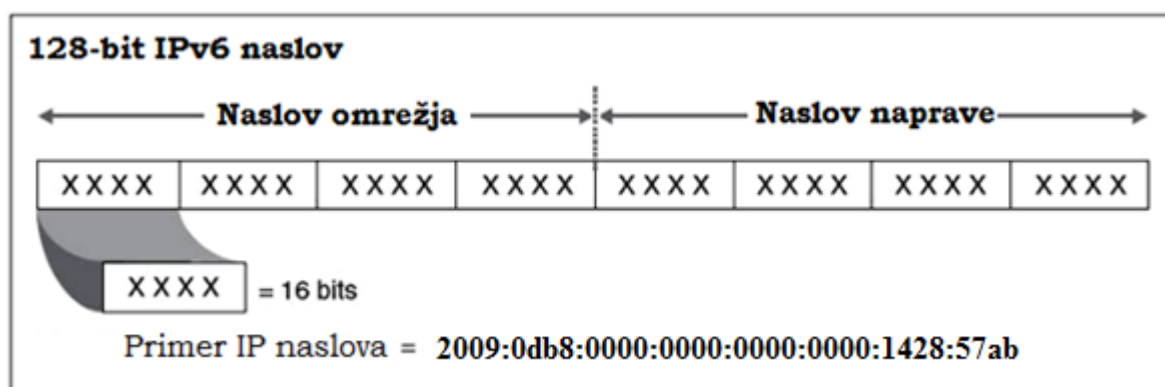
- Izpustimo lahko vse vodilne ničle blokov in tako zgornji naslov zapišemo tudi kot 2009:db8:0:0:0:0:1428:57ab.
- Sosednja ničelna polja se lahko zapiše kot :: in tako zgornji naslov zapišemo tudi kot 2009:db8::1428:57ab.
- Zaporedne bloke samih ničel lahko izpustimo le enkrat v naslovu, ker bi večkratni zapis z dvema dvopičjema onemogočil deterministično določanje naslova.
- Naslov povratne zanke, ki ga v IPv6 v celoti zapišemo z 0000:0000:0000:0000:0000:0000:0000:1 tako lahko skrajšamo v ::1.
- V protokolu IPv6 so vse vrednosti 0 in 1 dovoljene v katerem koli bloku naslova.

Sam naslov se deli na pol. Na del, ki predstavlja **naslov omrežja** in del, ki predstavlja **naslov naprave** v tem omrežju. Delitev je razvidna iz slike 4.

Primer IPv6 naslova: 2009:db8:0:0:0:0:1428:57ab

Naslov omrežja predstavlja: 2009:db8:0:0

Naslov naprave v tem omrežju pa je: 0:0:1428:57ab



Slika 4: Prikaz delitve naslova IPV6.

3.2.2 Vrste naslavljanj IPv6

IPv6 ima 3 različne vrste naslavljanj:

1. Naslov za pošiljanje na posamezen naslov (Unicast naslavljanje) - to je najpomembnejši tip naslavljanja, ki omogoča dostop do posameznih skupnih računalnikov, tiskalnikov in drugih naprav, ki so priključene v omrežje. Unicast pošlje podatek samo na en naslov (na primer: telefon). Tipi unicast naslovov:

- Globalni unicast naslovi: omogočajo možnost naslavljanja celotnega globalnega IPv6 omrežja.
- Link-local unicast naslovi: se uporabljajo za naslavljanje vmesnika znotraj določenega omrežnega segmenta – povezave.
- Site-local naslovi: tukaj lahko naslavljamo vmesnike znotraj omrežij, ki niso povezana v internet.
- Unique-local naslovi: so namenjeni usmerjanju znotraj organizacije, pri čemer so ogledi na druge organizacije enolično določeni.

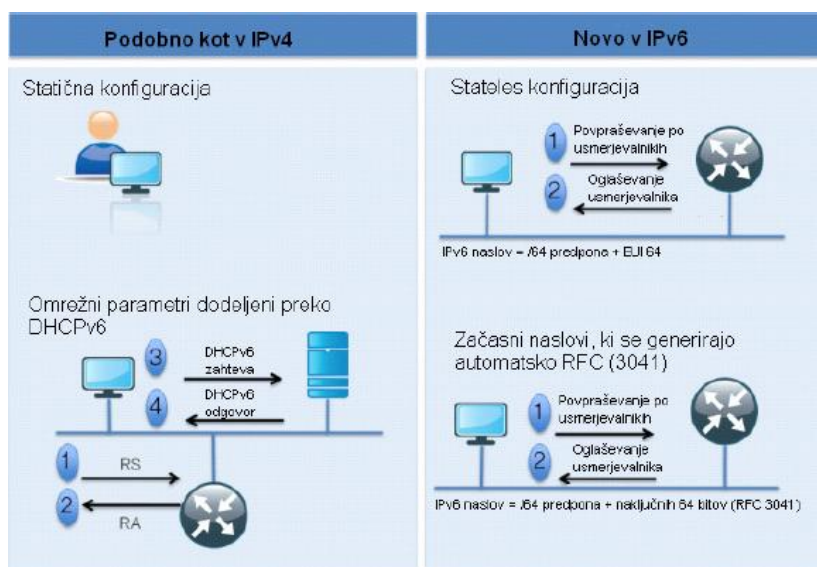
2. Naslovi za večkratno pošiljanje (Multicast naslavljanje) - zajema skupino naslovov. Pri pošiljanju paketov na multicast naslov prejme vsak vmesnik, ki pripada skupini z multicast naslovom, isti paket. Multicast se večinoma uporablja za prenos video/avdio podatkov v realnem času (videokonference/televizijske oddaje). Informacija se prenaša k določeni ciljni skupini (na primer: naročniki določenega televizijskega programa). Multicast nima ločenega naslovnega prostora, ampak je označen s predpono ff00::. Multicast naslove je s tem tudi lažje razlikovati od drugih. Multicast se pri IPv6 uporablja tudi namesto razpršenega naslavljanja (Broadcast), zato da ne pride do zasičenja vozlišč oz. mreže.

3. Naslov za poljubno razpošiljanje (Anycast naslavljanje) - Anycast se na splošno uporablja kot način za zagotavljanje visoke razpoložljivosti in izravnavo obremenitev strežnikov (na primer: DNS strežnikov). Pri anycast naslavljanju so paketi usmerjeni na najbližji strežnik v anycast skupini, kjer podatke usmerijo po najbližji oz. najboljši poti do cilja. Takšno naslavljanje se večinoma uporablja pri DNS.

3.2.3 Dodeljevanje naslovov IPv6

Dodeljevanje naslovov IPv6 je podobno kot dodeljevanje naslovov IPv4, lahko uporabimo statično nastavitve naslova ali pa dinamično z DHCPv6 (Slika 5).

Dodana pa sta tudi dva nova načina dodeljevanja naslovov, Stateless DHCP in začasni naslovi, ki se generirajo avtomatsko. Naprave, ki se želijo povezati v IPv6 omrežje samo nastavijo povezavno-lokalne naslove (angl. Link Local), ki so potrebni za komuniciranje znotraj lokalnega omrežja. Če pa želijo komunicirati z internetom, pa potrebujejo usmerjevalnik, kateri jim posreduje omrežni del IPv6 naslova.



Slika 5: Primerjava dodeljevanja IPv4 in IPv6 naslovov.

3.3 Zgradba paketa IPv6

Paket IPv6 je sestavljen iz glave, razširitvene glave in nadležne protokolne podatkovne enote PDU, kjer je lahko največja koristna vsebina dolžine 64kB. Če je ta vsebina večja, imenujemo takšne prevelike pakete tudi »jumbogrami«. Paket IPv6 vedno vsebuje glavo IPv6, ki je določene dolžine. Poleg nje ima paket lahko še več podaljšanih glav, ki so lahko različnih dolžin. Zadnja podaljšana glava označuje nadležne protokole (ICMPv6, UDP, TCP, ...), ki so vsebovani v nadležni protokolni podatkovni enoti.

Datagrami so računalniški podatki z dodanimi informacijami za krmiljenje, namenjeni prenosu med napravami v omrežju IP. Jumbogram pa je zelo velik datagram s podatki, ki so večji od 64kB (več o tem v nadaljevanju).

3.4.1 Datagram IPv6

Podrobna struktura glave paketa IPv6 je določena s standardom RFC 2460. Glava IPv6 paketa ima točno določeno dolžino 320 bitov. Če želimo to glavo dodatno razširiti, ima IPv6 vgrajeno opcijo za uporabo tako imenovane podaljšane glave.

V glavi protokola IPv6 ni več naslednjih polj iz glave IPv4 (Hagen 2006):

- dolžina glave,
- identifikacija,
- zastave,
- odmik zaradi fragmentiranja,
- preverjanje kontrolne vsote glave.

Poglejmo si sestavo glave IPv6 na sliki 6.

bytes		0								1								2								3							
	bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Verzija				Razred								Oznaka toka																			
4	32	Dolžina podatkovnega toka																Naslednja glava								Omejitev preskokov							
8	64	Naslov izvora																															
C	96																																
10	128																																
14	160																																
18	192	Naslov cilja																															
1C	224																																
20	256																																
24	288																																

Slika 6: Prikaz glave IPv6.

Naslov izvora (Source Address) – 128 bitni naslov izvora vsebuje naslov pošiljatelja.

Naslov cilja (Destination Address) – 128 bitni naslov cilja vsebuje končni naslov oz. naslov prejemnika.

Verzija (Version) – to je 4-bitno polje, ki vsebuje številko 6. Kaže na različico protokola IPv6. To polje ima enako velikost kot pri protokolu IPv4, le da IPv4 vsebuje številko 4.

Razred (Traffic Class) – to je 8-bitno prednostno polje, ki lahko v glavi IPv6 prevzame različne vrednosti. Te omogočajo razlikovanje med prioritetami paketov v usmerjevalnikih. Polje omogoča upoštevanje in doseganje QoS.

Oznaka toka (Flow Label) – 20-bitna oznaka toka v glavi IPv6 se lahko uporablja za označevanje paketov, ki pripadajo istemu toku. Ta tok se določi na strani izvora in ne sme zavzeti vrednosti 0, sicer se to smatra, da se prenos paketov ne obravnava kot tok. IPv6 usmerjevalniki morajo obravnavati pakete, ki pripadajo istemu toku. Ko usmerjevalniki sprejmejo prve pakete novega toka, jih obdelajo in shranijo rezultat, da lahko usmerjajo tudi vse druge pakete, ki pripadajo istemu toku (pakete z enakim naslovom izvora in enako oznako toka).

Dolžina podatkovnega polja (Payload Length) – 16-bitno polje določa dolžino polja s podatki. Podatkovno polje postavlja zgornjo mejo glede na največjo velikost paketa, ki je v tem primeru 64 kB.

Naslednja glava (Next Header) – 8-bitno polje opredeljuje tip glave na višji plasti v komunikacijskem skladu. To polje običajno določa prenosno plast. Dve najpogostejši vrsti naslednje glave sta glavi TCP in UDP protokolov, vendar so možni tudi drugi. To področje je podobno protokolnemu polju IPv4.

Omejitev preskokov (Hop Limit) – 8-bitna omejitev preskokov se zmanjša za ena v vsakem vozlišču, ko usmerjevalnik pošlje paket naprej. Če to polje pade na 0, se paket uniči oz. opusti. Glavna naloga tega polja je ugotovitev in opustitev paketov, ki obtičijo v kakšni zanki zaradi napake. To polje tudi postavlja zgornjo mejo glede števila omrežnih vozlišč med dvema končnima vozliščema. Na ta način je možno največ le 255 preskokov preden se podatkovni paket zavrže.

3.4.2 Razširitvena glava IPv6

Razširitvene glave sledijo osnovni glavi IPv6 in imajo lahko največjo velikost 64 bitov, hkrati pa ni nobene omejitve koliko podaljšanih glav lahko ima paket IPv6. Razširitvene glave se obdelujejo v takšnem zaporedju kot so dodane. Vsak usmerjevalnik mora tako obdelati manjše število polj v primerjavi z IPv4.

4. Varnost v IPv6

Varnost je obvezna sestavina IPv6, zato je treba varnostni model IPsec v bližnji prihodnosti podpreti. Glavni namen varnosti IP je zagotovitev kakovostne varnosti. Ta ponuja različne varnostne storitve na plasti IP in višjih plasteh. Pod te varnostne storitve štejemo: nadzor dostopa, nadzor nad izvorom podatkov, zaščito pred ponovitvami, zaupnost (šifriranje) in omejevanje prometnih tokov, ki so zaupni. Varnost IP se izvaja z uporabo avtorizacijske glave in podaljšane glave ESP.

IPv6 ima že v osnovi vključeno podporo protokolu IPsec, ki zagotavlja šifriranje in overitev na omrežni plasti ISO/OSI, kar pa ni večja izboljšava v primerjavi z IPv4, saj je IPsec danes v njem večinoma podprt. Tudi v IPv6 je konfiguracija IPseca obsežna in zapletena. V omrežju kjer nimamo NATa pa je IPsec vseeno precej lažje uporabljati.

4.1 IPsec

IPsec predstavlja okvir odprtih standardov, ki zagotavljajo varnost za prenos podatkov skozi omrežje.

Storitve IP varnosti:

- Podatkovna zaupnost: IPsec pošiljatelj lahko kriptira ali šifrira pakete, preden jih pošlje naprej po omrežju.
- Celovitost podatkov: IPsec sprejemnik lahko preveri podatke, ki jih je poslal pošiljatelj in s tem zagotovi, da se podatki niso spremenili med prenosom.
- Nadzor nad izvorom podatkov: IPsec sprejemnik lahko pregleda poslane pakete.
- Zavrnitev podvojenih podatkov: IPsec sprejemnik lahko odkrije in zavrne ponovno poslane pakete.

Z IPsec se lahko paketi pošljejo preko omrežja brez možnosti opazovanja in spreminjanja. Delovanje IPsec je pri obeh protokolih podobno, vendar ima IPv6 to prednost, da so lahko podatki šifrirani na celotni poti med virom in končnim vozliščem.

Pogosto se omenja pojem navideznega zasebnega omrežja (VPN). Pri tej vrsti omrežja gre za povezavo med dvema točkama, med katerima je vzpostavljen tunel skozi javno omrežje, ki zagotavlja varen in zanesljiv tok podatkov.

Tri glavne prednosti IPsec:

- podprti so vsi operacijski sistemi v različnih računalniških okoljih,
- rešitve VPN za zagotavljanje zaupnosti podatkov za zasebne mreže,
- standardi za različne naprave, preprostejše izvajanje.

IPsec podpira tudi naslednje funkcije:

- AH (Authentication Header), ki zagotavlja pristnost pri pošiljanju paketov. To se izvede s preverjanjem paketov s pomočjo algoritmov.
- ESP (Encapsulating Security Payload – enkapsulacija zavarovanih podatkov), ki zagotavlja šifriranje paketov.
- IPcomp (IP payload compression – podatkovna stisljivost) zagotavlja stisljivost podatkov, preden se paket kriptira.

Alternativo protokolu IPsec v kontekstu vzpostavljanja navideznega zasebnega omrežja, predstavlja protokol SSL. SSL je varnostni protokol za prenos podatkov, največkrat za zaščito http, IMAP in POP3 transakcij.

4.2 Kakovost storitev QoS

Kakovost storitev je nabor zahtev, ki morajo biti izpolnjene, ko se prenašajo podatki. Zagotavlja sposobnost upravljanja z različnimi prioritetami aplikacij, uporabnikov ali podatkov. Pri delu z večnamenskimi aplikacijami uporabniki potrebujejo in zahtevajo hitrost, zanesljivost in odzivnost.

Z mehanizmom zagotavljanja kakovostnega prenosa podatkov v omrežju rezerviramo pasovno širino za pomemben poslovni promet. Prav tako zmanjšamo zakasnitve in odstopanje prometa podatkov, izboljšamo in povečamo izkoriščenost omrežja ter administratorjem omogočimo dostop do omrežnih naprav v primeru zasedenosti omrežja. Med sejo se lahko spremlja raven učinkovitosti prenosa podatkov, hitrost in zakasnitve.

Kakovosten prenos podatkov po omrežju združuje naslednje lastnosti:

- določanje prioritet paketom,
- omejevanje,
- stiskanje paketov.

Slabost QoS je kvečjemu zahtevno uvajanje in potrebno znanje za upravljanje in odpravo napak.

4.2.1 Prednosti QoS-a

Prednosti uporabe QoS za uporabnika:

- hitra odzivnost aplikacij,
- hitrost delovanja aplikacij,
- zanesljivost komunikacij,
- zadovoljstvo uporabnikov,
- avdio in video konference.

Prednosti uporabe QoS za administratorja:

- hiter, zanesljiv in kakovosten prenos podatkov po omrežju,
- hitrejša in zanesljivejša administracija in upravljanje omrežja, tudi v primeru zasičenosti omrežja,
- omejevanje nekoristnega prometa (omejuje posamezne vrste prometa, ki ga povzročajo virusi, črvi).

Prednosti uporabe QoS za lastnika omrežja:

- boljša izkoriščenost transportnega omrežja,
- znižanje stroškov upravljanja,
- znižanje stroškov povezav.

5. IPv6 in IPv4

Primerjava med protokoloma IPv4 in IPv6 zajema temeljne lastnosti obeh protokolov, kot so velikost naslova, glava protokola, povratni naslov ... [3]. Za lažjo predstavo je primerjava prikazana tudi v tabeli 2.

5.1 Primerjava

Naslovi:

Pri IPv4 je naslov 32 biten. Naslov je sestavljen iz mrežnega in gostiteljskega dela, ki sta odvisna od razredov. Število možnih naslovov je skoraj 4,3 milijarde.

Pri IPv6 je naslov dolg 128 bitov. 64 bitov je za omrežno številko in 64 bitov za številko gostitelja. Teoretični maksimum števila uporabnih IP naslovov bo $6,0 \cdot 10^{23}$, kar je bistveno večje od števila razpoložljivih IPv4 naslovov.

Dodelitev naslovov:

IPv4 – Razdeljevanje naslovov ni bilo uravnoteženo med državami in institucijami.

IPv6 – Dodeljevanje je še na začetni stopnji. IETF je priporočil, da naj bo vsaki organizaciji dodeljena predpona podomrežja z dolžino /48.

Naslovna maska:

IPv4 – Uporablja se za delitev med omrežjem in gostiteljem.

IPv6 – Se ne uporablja.

Konfiguracija/Nastavitve:

IPv4 – Vsak na novo nameščen sistem je potrebno nastaviti za komuniciranje z drugimi sistemi. Dodeljeni morajo biti IP naslovi in poti.

IPv6 – Nastavitve so neobvezne oziroma odvisne od funkcije.

DHCP:

IPv4 – Uporablja se za samodejno pridobitev IP naslova in drugih informacij s strežnika.

IPv6 – Če administrator želi večji nadzor nad naslavljanjem, se DHCP uporablja za dodeljevanje naslovov.

ARP (Address Resolution Protocol) – protokol za razreševanje naslovov:

IPv4 – Ta protokol uporablja IPv4 za iskanje fizičnih naslovov kot je MAC.

IPv6 – Vsebuje informacije v samem IP kot del algoritmov za samodejno konfiguriranje in odkrivanje sosedov z uporabo protokola ICMPv6 (Internet Control Message Protocol). Zato ARP6 ne obstaja.

Glava IP:

IPv4 - Spremenljiva dolžina 20-60 bajtov, odvisna od IP opcij.

IPv6 - Stalna dolžina 40 bajtov. Ni možnosti IP kot pri IPv4. Glava IPv6 je enostavnejša od IPv4 glave.

Opcije glave IP:

IPv4 – Veliko možnosti za spreminjanje glave IP.

IPv6 – Oglavje IPv6 ne vsebuje možnosti, namesto tega pa so na voljo dodatna razširitvena oglavja

Povratni naslov:

IPv4 – To je vmesnik z naslovom 127.*.* (običajno 127.0.0.1), ki ga lahko uporabljamo samo za vozlišča za pošiljanje paketov samemu sebi.

IPv6 – Podobno kot pri IPv4, le da je tu 0000:0000:0000:0000:0000:0000:0001, ali ::1 (krajša različica).

FTP (File Transfer Protocol) – protokol za prenos datotek:

IPv4 – Omogoča sprejemanje in pošiljanje datotek preko omrežij.

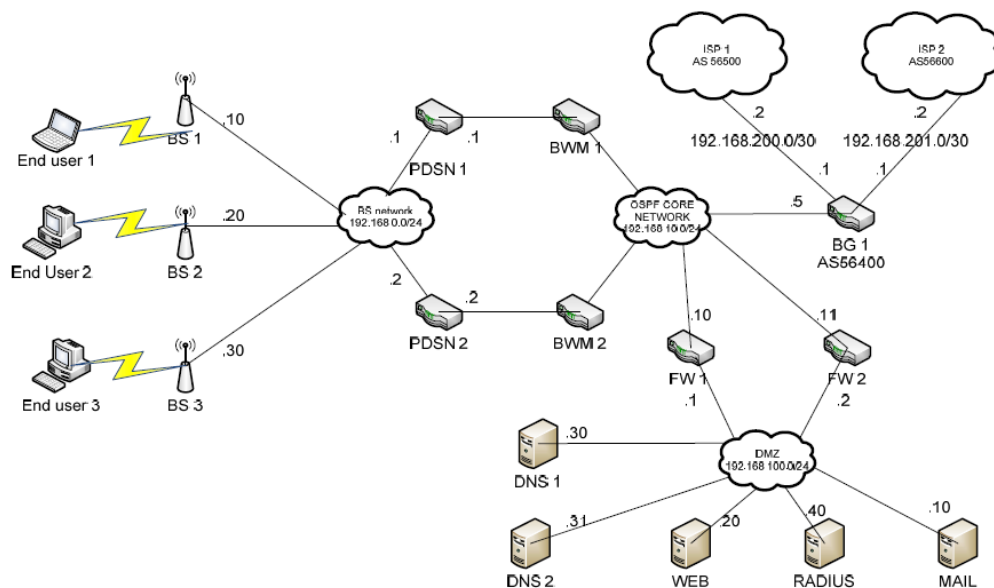
IPv6 – Nekaj FTP-jev je že dostopnih z IPv6.

Primer še ene primerjave s prikazom v tabeli 2:

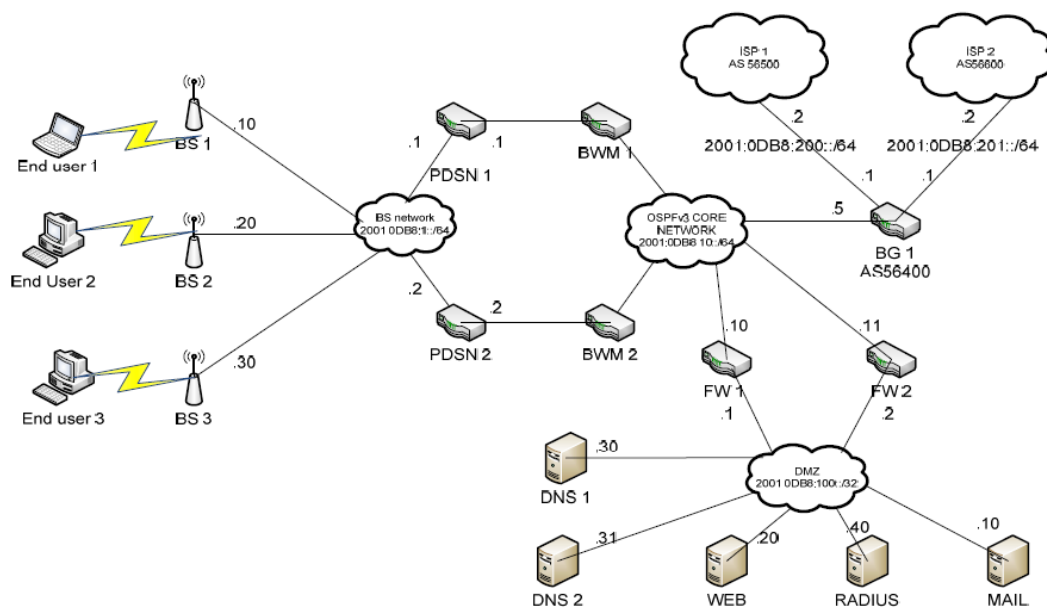
IPv4	IPv6
Uporablja 32 bitno naslavljanje	Uporablja 128 bitno naslavljanje
Podpora IPsec je izbirna	Zahteva podporo IPsec
Paketni tok nima označitve za QoS znotraj IPv4 glave	Paketni tok ima označitev za QoS znotraj glave IPv6 z uporabo polja podatkovnega pretoka
V strežniku DNS uporabljajo A zapise.	V strežniku DNS uporabljajo AAAA zapise
Konfiguracija je ročna oz. preko DHCP	Ne zahteva ročne oz. konfiguracije DHCP
Uporaba zapisov PTR v IN-ADDR.ARPA domeni DNS	Uporaba PTR zapisov v IPv6.INT domeni DNS
Fragmentacija se izvaja na strani pošiljatelja in usmerjevalnikov	Fragmentacija narejena samo na strani pošiljatelja
Ni zahtev glede velikosti paketov na povezovalnem sloju (Zmožnost 576 bajtov)	Povezovalni sloj mora podpirati 1280 bajtov velike pakete (Zmožnost 1500 bajtov)
Glava vsebuje kontrolno vsoto	Glava ne vsebuje kontrolno vsote
Glava vsebuje izbirna polja	Vsa izbirna polja so premaknjena v razširitveno glavo
Uporaba razpršenih okvirov zahtev ARP	Okviri zahtev ARP zamenjani z večponornimi sporočili za nagovarjanje sosedov
Uporaba protokola IGMP	IGMP je zamenjan z sporočili MLD
Uporaba protokola ICM odkrivanja usmerjevalnikov	Ukaz odkrivanja usmerjevalnikov z ICMPv4 zamenjan s sporočili za nagovarjanje in oglaševanje usmerjevalnikov

Tabela 2: Primerjava med IPv4 in IPv6.

Za lažje razumevanje omrežij IPv4 in IPv6 si lahko pomagamo s slikama Slika 7 in Slika 8.



Slika 7: IPv4 omrežje.



Slika 8: Omrežje IPv6.

5.2 Združljivost med protokoloma

Protokola med seboj nista združljiva oz. sta združljiva na nivoju žice. To pomeni, da si lahko delita isto fizično infrastrukturo in bivata sočasno. Obdobje prehoda do čiste IPv6 infrastrukture bo trajalo precej časa. Vsekakor pa je v tem prehodnem obdobju pomembno, ne glede na izbrano infrastrukturo, zagotoviti povezljivost omrežnih naprav in zagotoviti dostop do vsebine in storitev.

Tako so se s časom razvile tehnike za soobstoj obeh protokolov, tako imenovani tranzicijski mehanizmi (angl. transition mechanisms):

1. Uporaba obeh protokolov
 - Arhitektura dvojne plasti IP (Double IP layer)
 - Arhitektura dvojnega sklada (Dual stack)
2. Tunelski mehanizem IPv6 skozi IPv4
3. Translacija protokola

5.2.1 Uporaba obeh protokolov



Slika 9: Uporaba dvojnega sklada: razvoj IPv4 in IPv6 na isti infrastrukturi.

Dvojni sklad zagotavlja, da se ne glede na vrsto prometa vsak paket obdeluje v svojem protokolnem skladu (Slika 9). Implementiran je lahko kot del operacijskega sistema končnega uporabnika ali pa v omrežnem usmerjevalniku. Usmerjevalnik z dvojnimi skladom lahko posreduje promet IPv4 in IPv6. Nadgradnja za takšen način delovanja je lahko programska, čeprav se bodo z rastjo količine prometa začela porajati potrebe po strojni izvedbi. V primeru souporabe protokolov IPv4 in IPv6 je potrebno vzdrževati usmerjevalni tabeli za oba protokola.

Mehanizem dvojega sklada si deli vse ranljivosti, ki lahko prizadenejo izvirni IPv4 in IPv6 omrežji. Usmerjevalnik, ki uporablja dvojni sklad, lahko posreduje IPv4 in IPv6 promet. Če smo še bolj natančni, bo usmerjevalnik z vključenim dvojnimi skladom s povezavo na IPv4

usmerjevalnik posredoval samo IPv4 pakete, na povezavo z IPv6 usmerjevalnikom, pa bo posredoval samo IPv6 pakete. Zavedati se moramo, da dvojni sklad v jedru omrežja izključno omogoča komunikacijo samo med IPv4 gostitelji, ali pa samo med IPv6 gostitelji. To pomeni, da gostitelji s samo IPv4 skladom ne morejo direktno komunicirati z gostitelji, ki uporabljajo samo IPv6 in obratno.

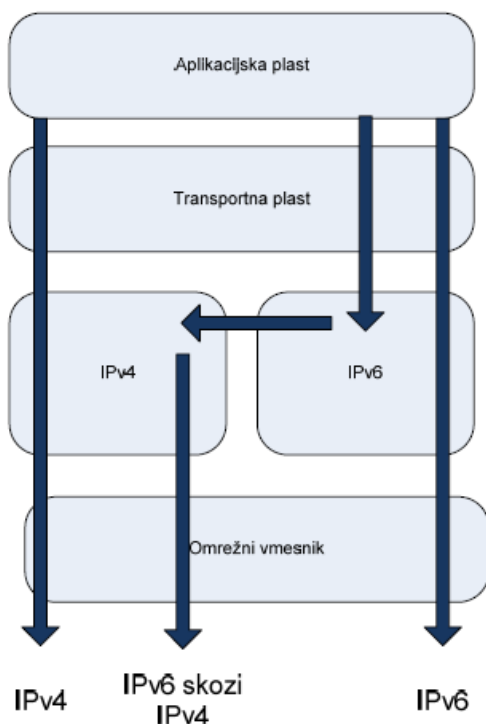
- **Arhitektura dvojne IP plasti**

Ta arhitektura vsebuje oba protokola z enkratno implementacijo protokolov na transportni plasti. Vrste paketov, ki se pojavljajo, so tipa IPv4, IPv6 ali IPv6 skozi IPv4 (Slika 10).

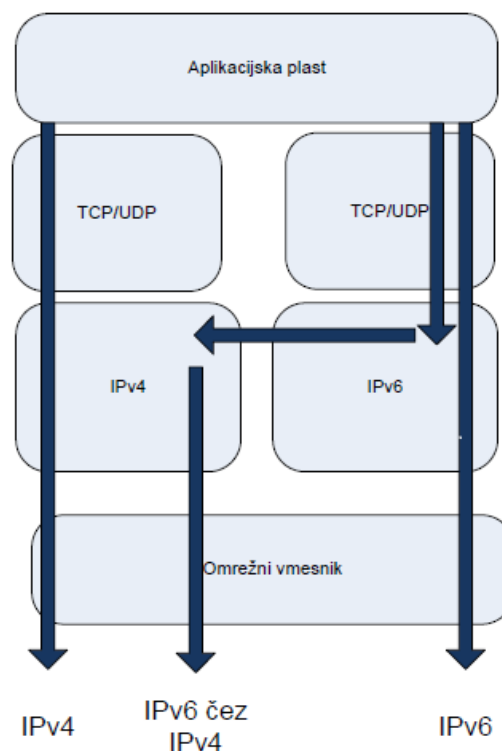
- **Arhitektura dvojnega sklada**

Podobna je arhitekturi dvojne plasti IP, pri čemer sta tu implementaciji transportne plasti ločeni. Ta arhitektura predstavlja dominantno tranzicijsko strategijo. Zagotavlja, da se glede na vrsto prometa, vsak paket obdeluje v svojem protokolnem skladu. Če končni sistem ali usmerjevalnik prejme IPv4 paket, ga bo posredoval preko protokolnega sklada IPv4, če prejme IPv6 paket, pa ga bo posredoval čez protokolni sklad IPv6 (Slika 10).

Tipi paketov pri arhitekturi dvojne IP plasti



Tipi paketov pri arhitekturi dvojnega sklada



Slika 10: Tipi paketov pri arhitekturi dvojne plasti IP ter pri arhitekturi dvojnega sklada.

5.2.2 Tunelski mehanizem IPv6 skozi IPv4

Tunel je povezana pot med dvema vozliščema in predstavlja rešitev za prenos IPv6 prometa čez obstoječo IPv4 infrastrukturo. S tem izkoristimo obstoječo IPv4 usmerjevalno topologijo in zmogljivost infrastrukture.

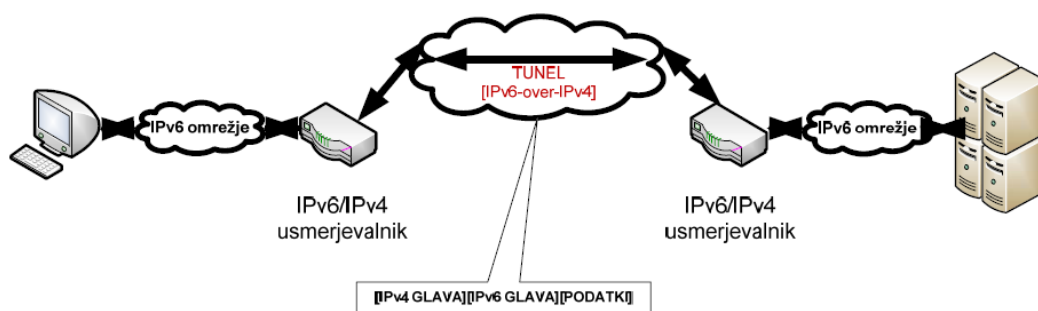
Tuneli se lahko vzpostavijo na 4 različnih relacijah.

- usmerjevalnik – usmerjevalnik,
- gostitelj – usmerjevalnik,
- gostitelj – gostitelj,
- usmerjevalnik – gostitelj.

Bistvo ideje tuneliranja je v ovijanju (angl. encapsulation). Gostitelji IPv4/IPv6 ter usmerjevalniki lahko tunelirajo datagrame IPv6 skozi usmerjevalno topologijo IPv4 z enkapsulacijo v pakete IPv4. Z drugimi besedami povedano: uporabimo pakete IPv4 kot transportni medij, v katerega vložimo pakete IPv6.

Kadar razmišljamo o uvedbi povezljivosti IPv6 preko tunelov moramo upoštevati, da tuneli lahko predstavljajo potencialno varnostno vrzel. Promet skozi njega moramo zato ustrezno nadzirati in varovati, da celotni tunel, kljub prehodu skozi množico usmerjevalnikov za robni usmerjevalnik predstavlja en sam skok in da tuneli omogočajo rekurzivno enkapsulacijo. Lahko se nam zgodi, da imamo tunel v tunelu.

Na sliki 11 lahko vidimo tunel, ki povezuje usmerjevalnika s tunelskim mehanizmom IPv6 skozi IPv4.



Slika 11: Princip tuneliranja.

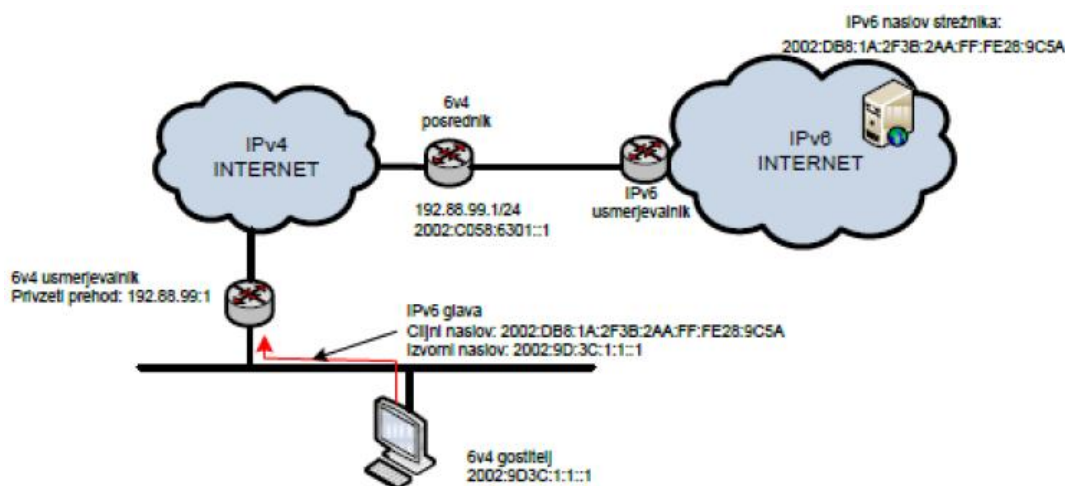
Tipi tunelov:

1. ISATAP,
2. mehanizem 6v4,
3. mehanizem 6rd,
4. mehanizem DSTM (Dual Stack),
5. Teredo,
6. Posredniški tuneli.

1. ISATAP: omogoča avtomatsko tuneliranje gostiteljem ne glede na to, ali uporabljajo zasebni ali javni naslov IPv4. Kot pri drugih tranzicijskih mehanizmih je tudi pri tem ključen način naslavljanja končnih naprav.

2. Mehanizem 6v4: se uporablja, ko se povezuje izolirana IPv6 omrežja preko avtomatično povezljivega tunela, ki je vzpostavljen skozi IPv4 omrežje (Slika 12). Mehanizem 6v4 celotno IPv4 omrežje interneta pojmuje kot povezavo, kjer je možno oddajanje samo enemu prejemniku (enoponorna povezava). Tuneliranje se samodejno izvaja na vmesniku končnega gostitelja ali usmerjevalnika, ki omogoča enkapsulacijo 6v4. Mehanizem 6v4, ki je standardiziran z RFC3056, se lahko izvaja v relacijah:

- usmerjevalnik - usmerjevalnik,
- gostitelj – usmerjevalnik,
- usmerjevalnik – gostitelj.



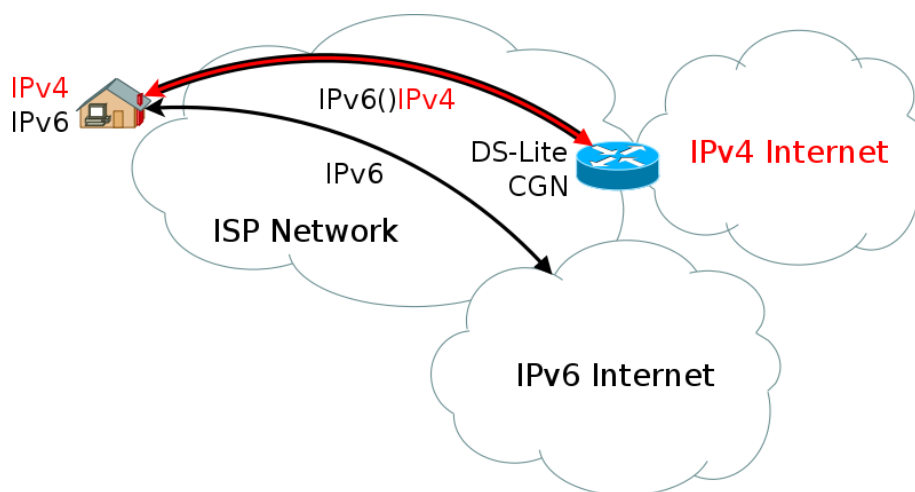
Slika 12: Komunikacija med gostiteljem 6v4 in gostiteljem IPv6.

3. Mehanizem 6rd: mehanizem 6rd (angl. Rapid Deployment) je migracijska tehnika, ki tudi omogoča povezljivost IPv6 skozi obstoječe omrežje IPv4 in ima podoben koncept kot mehanizem 6v4. Arhitektura 6rd sestoji iz:

- obstoječega IPv4 omrežja ponudnika,
- enega ali več 6rd prehodov,
- CPE usmerjevalnih prehodov (angl. Router gateway) s podporo 6rd.

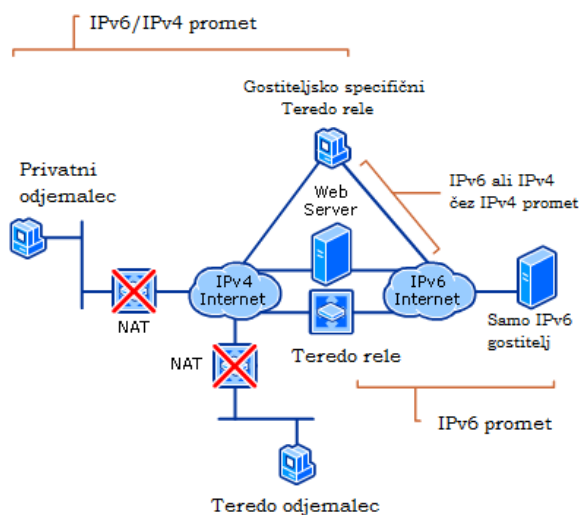
4. Mehanizem DSTM: (angl. Dual Stack Transition Mechanism) je tunelska rešitev za omrežja IPv6, kjer aplikacije še vedno uporabljajo protokol IPv4 znotraj infrastrukture IPv6. Promet IPv4 je tako tuneliran preko omrežja IPv6 samo do usmerjevalnika, ki podpira IPv6 in IPv4, ter izvaja enkapsulacijo (Slika 13).

Pri Dual stacku sta oba, usmerjevalnik in gostitelj opremljena z obema protokoloma IPv4 in IPv6. Vsako tako vozlišče imenovano vozlišče IPv4/IPv6 je nastavljeno z obema IPv4 in IPv6 naslovoma. To vozlišče lahko pošlje in sprejme datagrame, ki pripadajo kateremukoli protokolu (IPv4 ali IPv6) in lahko komunicira z vsakim vozliščem v omrežju IPv4/IPv6. To je najpreprostejši in najbolj zaželen način, da lahko hkrati obstajata IPv4 in IPv6 in je najbolj verjeten, preden bodo vsi ponudniki in uporabniki prešli na IPv6. Izziv je v uvajanju IPv6/IPv4 dual stack mreže in konfiguracije notranjega in zunanjega usmerjanja za oba protokola.



Slika 13: Prikaz Dual stack.

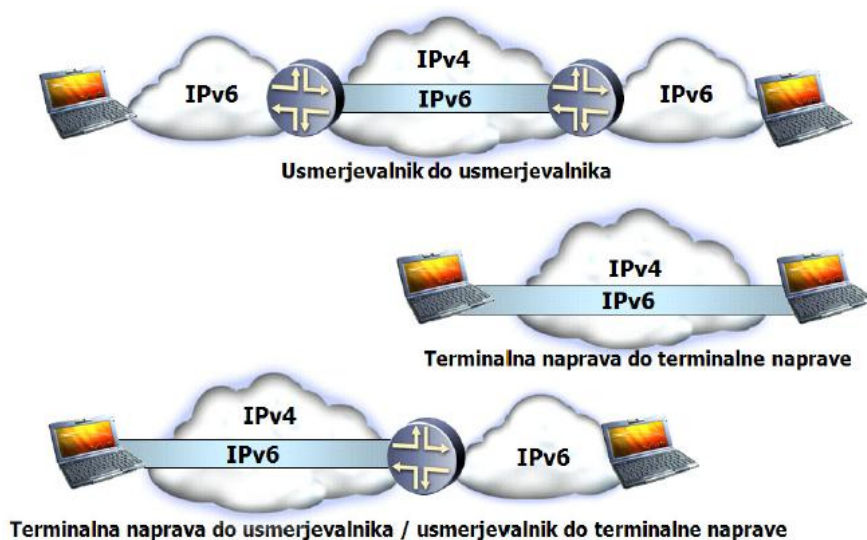
5. TEREDO: omogoča dodeljevanje naslovov in tuneliranje enoponornega prometa gostiteljem IPv6/IPv4, ki se nahajajo za napravami IPv4 NAT (Slika 14). Da se lahko vzpostavi komunikacija skozi napravo NAT, gostitelji Teredo tunelirajo ves promet IPv6 v paketih UDP, ki so oviti in poslani posrednikom Teredo. Odjemalec Teredo podpira oba protokolna sklada.



Slika 14: Povezava Teredo.

6. Posredniško tuneliranje: določa način uporabe obstoječe infrastrukture IPv4 za usmerjanje prometa IPv6. Med uvajanjem IPv6 je potrebno, da se usmerjevalna infrastruktura IPv4 zna sporazumevati s prometom IPv6. Gostitelji in usmerjevalniki, IPv4 ali IPv6, lahko tunelirajo datagrame IPv6 preko usmerjevalnikov IPv4 z enkapsulacijo paketov IPv6 v IPv4.

Tuneliranje se lahko uporablja na več načinov (Slika 15):



Slika 15: Tuneliranje IPv6.

1. Tuneliranje od usmerjevalnika do usmerjevalnika (Router-To-Router): usmerjevalniki IPv6 ali IPv4 povezani z infrastrukturo IPv4 lahko tunelirajo pakete IPv6 med seboj.

2. Tuneliranje od gostitelja do usmerjevalnika (Host-to-Router): vozlišča IPv4 ali IPv6 lahko tunelirajo pakete IPv6 preko usmerjevalnika IPv4 ali IPv6, ki je dosegljiv preko infrastrukture IPv4.

3. Tuneliranje od gostitelja do gostitelja (Host-To-Host): gostitelji IPv4 ali IPv6, ki so med seboj povezani z infrastrukturo IPv4 lahko tunelirajo pakete IPv6 med seboj. Nastali tunel med vozliščema se razteza čez celotno pot in deluje kot enoten poskok.

4. Tuneliranje od usmerjevalnika do gostitelja (Router-To-Host): usmerjevalniki IPv6 in IPv4 lahko tunelirajo pakete IPv6 do njihovega končnega gostitelja IPv6 ali IPv4.

V metodah usmerjevalnik-do-usmerjevalnika ali gostitelj-do-usmerjevalnika so paketi IPv6 tunelirani do usmerjevalnika. V metodah gostitelj-do-gostitelja in usmerjevalnik-do-gostitelja pa so paketi IPv6 tunelirani vse do konca poti. Tunelno vstopno vozlišče enkapsulira glavo IPv4 in pošlje enkapsuliran paket naprej. Izstopno vozlišče tunela sprejme enkapsuliran paket, odstrani glavo IPv4, posodobi glavo IPv6 in obdela prejet paket.

Paketi se usmerjajo po omrežju glede na informacijo, ki je zapisana v glavi tunelskega mehanizma. Tunelske mehanizme ločimo na dva tipa:

- samodejno nastavljive tunele (se vzpostavijo med dvema robnima omrežjema samodejno po potrebi),
- ročno nastavljive tunele (administrator nastavi parametre za končne robne točke tunela in tehnologije enkapsulacije).

Posredniki tunelov so organizacije, ki omogočajo končnim gostiteljem ali usmerjevalnikom z dvojnim skladom, da preko omrežja IPv4 s pomočjo vzpostavljenega tunela prejmejo povezljivost v omrežje IPv6. Spisek evropskih tunelskih posrednikov je mogoče najti na naslovu http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers#Europe.

5.2.3 Translacija protokola

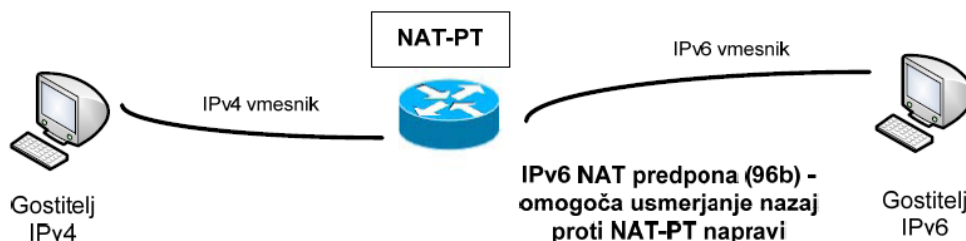
Translacija protokola deluje kot vmesni člen med svetovoma IPv4 in IPv6 (Slika 16). Ta rešitev je kompleksna, poleg tega pa ni moč zagotoviti, da se tekom translacije ohranjajo popolnoma vse informacije.



Slika 16: Uporaba translacijskega mehanizma.

Pregled translacijskih mehanizmov:

1. Mehanizem NAT-PT omogoča komunikacijo med IPv6 in IPv4 v obeh smereh. Za svojo uporabo zahteva tako tabele IPv4 kot IPv6. Glej sliko 17.



Slika 17: Koncept delovanja NAT-PT.

2. BIS (angl. Bump-In-the-Stack Mechanism)

BIS je translacijski mehanizem med aplikacijo IPv4 ter omrežjem IPv6. Promet IPv4 je preveden v IPv6 in obratno. Omogoča komunikacijo aplikacije na strani gostitelja z bodisi gostiteljem IPv4 ali IPv6 na drugi strani. Sestavljen je iz treh komponent:

- Translator
- Extension name resolver
- Address mapper

Mehanizem je uporaben v prehodnem obdobju uvajanja čistega protokola IPv6. Vedno pa bo lahko služil za programsko opremo (aplikacije), ki nikoli ne bodo nadgrajene za uporabo s protokolom IPv6.

3. TCP-UDP relay
4. SOCKS-based gateway

6. Prednosti in slabosti IPv6

IPv6 ponuja številne prednosti pred IPv4. Opisal bom nekaj najpomembnejših.

6.1 Prednosti IPv6

- Izboljšana učinkovitost pri usmerjanju paketov in ravnanju z njimi,
- podpora za samodejno konfiguracijo in Plug & Play,
- podpora za varnost,
- povečana podpora za mobilno IP in mobilne naprave,
- odpira vrata novi generaciji naprav zaradi večjega naslovnega prostora,
- rešuje problem pomanjkanja naslovov,
- omogoča veliko večje pakete podatkov,
- odprava NAT-a,
- velik prihranek pri stroških,
- povečano število naslovov za večkratno razpošiljanje, izboljšana podpora za multicast.

1. Večji naslovni prostor

To je najbolj znana značilnost IPv6. IPv6 ima naslovni prostor določen s 128 biti, kar pomeni, da ne bo »nikoli« prišlo do pomanjkanja naslovov IP. Sedanja politika, ki dodeljuje naslove, je dodelila 64 bitov naslovnega prostora za končne uporabnike in 96 bitov ali več za organizacije. Prednost v velikosti IPv6 je, da omogoča skeniranje nekaterih blokov IP, kar preprečuje zlorabe prometa.

2. Samodejna konfiguracija gostiteljev

Gostitelji IPv6 se lahko konfigurirajo samodejno, ko se priključijo na omrežje IPv6. Pri prvi povezavi v omrežje, gostitelj pošlje zahtevo za konfiguracijo parametrov. V primeru, ko se ta konfiguracija izvede pravilno, se usmerjevalnik odzove s paketom, ki vsebuje parametre konfiguracije omrežne plasti.

3. Jumbogrami

Jumbogram omogoča prenos datagramov, ki so večji od 64 kB. Hop-by-hop možnost prosi za posebno obravnavo, ki je potrebna za obdelavo teh jumbogramov.

4. Hitrejše usmerjanje

Z uporabo enostavnejših in bolj sistematičnih struktur naj bi IPv6 izboljšal učinkovitosti usmerjanja skozi vozlišča.

5. Varnost omrežne plasti

IPsec je protokol omrežne plasti za šifriranje in nadzor podatkov. Je sestavni del osnovnega protokola IPv6.

6. Mobilnost

Obstajata koncepta Domači naslov »Home address« in Skrb za naslov »Care of Address«. Protokol IPv6 omogoča mobilno vozlišče, da se lahko premaknemo iz enega omrežja v drugo, brez zamenjave naslova IPv6. Mobilno vozlišče je vedno naslovljeno na svoj privzeti domači naslov. Ko je mobilno vozlišče stran od svojega domačega naslova, so paketi še vedno lahko preusmerjeni do domačega naslova z uporabo vozlišča domačega naslova.

7. Preprostejša konfiguracija IP

IPv6 ponuja nove funkcije, ki poenostavijo nalogo konfiguriranja in upravljanja naslovov v omrežju. Na primer, samodejno nastavi vmesne naslove in privzete poti. IPv6 vzame MAC naslov naprave in omrežno predpono, ki jo ponuja usmerjevalnik in ju združi tako, da dobi unikatni naslov IPv6. Za to stvar pa ni potrebno imeti več strežnika DHCP (protokol za dinamično nastavitve gostitelja).

8. Ponovno številčenje:

Če uporabljamo IPv6, ni potrebno naslova, ki ga uporablja naprava, ponovno številčiti, kadar menjamo internetnega ponudnika. Druga polovica naslova IPv6 ostaja nespremenjena, ker je to naslov MAC mrežne kartice. Nova predpona IPv6 pa je določena s strani internetnega ponudnika.

6.1.1 Novosti in spremembe

Protokol IPv6 je obdržal večino prednosti IPv4. Spremembe so poleg daljšega naslovnega prostora, predvsem popravki napak v protokolnem skladu IPv4.

Bistvene spremembe so:

- več možnosti pri naslavljanju in usmerjanju,
- povečan naslovni prostor (iz 32 bitov na 128 bitov),
- stabilnost prenosnega načina multicast je izboljšana,
- enostavnejša zgradba in stalna dolžina glave IP,
- nekatera polja v glavi IP so ukinjena, izboljšana, oziroma prenesena v razširitvene glave,
- razširjena podpora za zagotavljanje kakovosti storitev,
- razširitve za zagotavljanje zasebnosti.

6.2 Slabosti IPv6

IPv6 nima slabosti oz. zelo malo. Največja pomanjkljivost IPv6 je, da veliko ustvarjalcev programske opreme potrebuje veliko časa pri izdelavi rešitev za IPv6. IPv4 je v uporabi že skoraj 30 let in ga vsi poznamo oz. ga uporabljamo. Pri IPv6 je to čisto drugače, ker je to nekaj povsem novega in še ni razširjen. Problem pa je tudi v ceni nadgradnje, saj moramo poleg strojne opreme nadgraditi tudi programsko opremo.

7. Problem uporabe IPv6

Precej opreme na kateri temelji delovanje interneta, se lahko nadgradi s podporo za IPv6, vendar večina ne omogoča velikih hitrosti prenosa preko tega protokola, zato bo vpeljava protokola IPv6 v internet, povezana z velikimi vlaganji v omrežja.

Nekateri uporabljajo IPv4, drugi IPv6. S tem problemom se srečujejo v IETF, kjer razmišljajo o načinih, kako se bosta sporazumevala IPv4 in IPv6. Kot vemo, ne bo mogoče istočasno nadgraditi vse opreme.

7.1 Prevajanje SIIT

Težava, s katero se IETF srečuje, je v velikih razlikah med IPv4 in IPv6. IPv4 uporablja 32-bitni naslov, medtem ko bo IPv6 uporabljal 128-bitnega. Torej, kako narediti sistem, ki bo imel le naslove IPv4 in bo lahko komuniciral s sistemom, ki bo imel samo naslove IPv6. Odgovor se skriva v prevajanju paketov. Pri IETF so našli način, kako bo to potekalo pod imenom SIIT. SIIT je algoritem, ki je potreben za sporazumevanje in komuniciranje vozlišč IPv6 z vozlišči IPv4.

7.1.1 Prevajanje SIIT iz IPv4 v IPv6

Ko prevajalec IPv4/IPv6 prejme IPv4 paket, naslovljen zunaj omrežja IPv4, ta glavo IPv4 paketa prevede v glavo IPv6 in jo potem pošlje naprej na ciljni naslov IPv6. Prvotna glava paketa IPv4 se odstrani in nadomesti jo glava IPv6. To velja za vse pakete, razen za pakete ICMP (Internet Control Message Protocol), kjer ostaneta glava transportne plasti in del podatkov nespremenjena. Ena izmed razlik med IPv4 in IPv6 je v tem, da je pri IPv6 obvezno odkrivanje poti MTU (Maximum Transmission Unit/Največja prenosna enota) medtem, ko pri IPv4 ni obvezno. Ko pošiljatelj IPv4 ne opravlja odkrivanja poti MTU, mora prevajalec zagotoviti, da paket ne presega poti MTU na strani IPv6. To naredi s skrčenjem paketa IPv4, da je paket manjši od 1280B. Tudi, ko IPv4 ne opravlja odkrivanja poti MTU, mora vedno vsebovati skrčeno glavo IPv6, ki pošiljatelju omogoča skrčevanje. To zagotavlja, da kadar so paketi skrčeni s strani pošiljatelja ali usmerjevalnika, se ti paketi na koncu poti vedno vrnejo nazaj v prvotno stanje.

7.1.2 SIIT prevajanje iz IPv6 v IPv4

Ko prevajalec IPv6 /IPv4 prejme paket IPv6, naslovljen zunaj omrežja IPv6, ta glavo paketa IPv6 prevede v glavo IPv4. Prevajalec potem pošlje naprej prevedeni paket na naslov IPv4. Prvotna glava paketa IPv6 se odstrani in nadomesti jo glava IPv4. Obstajajo tudi razlike med IPv4 in IPv6 v skrčevanju paketov. IPv6 povezava mora imeti MTU 1280B ali več. Ko je MTU 1280B ali več, lahko MTU odkriva poti od začetka do konca prevajanja. Ko največja prenosna enota (MTU) pade pod minimum 1280B, bo IPv6 pošiljatelj tvoril 1280B velike pakete, te pa bodo usmerjevalniki IPv4, po pretvorbi v IPv4, med prenosom pretvorili v manjše pakete.

7.2 Nadgradnja SIIT z IVI

IVI uporablja algoritme SIIT s spremenjenim naslovom in spremenjeno različico NAT-PT. (Prevod bi bil: prevajalec omrežnega naslova - prevajalec protokola). IVI model je bil narejen, da bi pospešil postavitve strežnikov z domenami IPv6. Omrežje IVI je sestavljeno iz dveh ali več omrežnih domen, ki sta povezani z enim ali več prehodi. Eno omrežje vodi IPv4, drugo pa IPv6. Prvo vsebuje nekaj gostiteljev, ki delujejo samo z IPv4, drugo pa vsebuje gostitelje, ki delujejo samo z IPv6. Obe omrežji pa vsebujeta uporabnike in strežnike.

8. Kako do prehoda na IPv6

Naloga prehoda na IPv6 je polna izzivov. Za prehod je potrebna visoka stopnja prilagodljivosti v programski in strojni opremi. Prehod na IPv6 zahteva, da se vsa vozlišča IPv4 znajo sporazumevati z IPv6 v času prehoda. Prav tako je tudi pomembno, da vsa tehnologija omogoča, da vozlišča IPv6 komunicirajo preko IPv4 interneta z drugimi omrežji. Obstaja več načinov prehoda na IPv6.

Prehod na IPv6 mora biti tudi dobro načrtovan in hitro izveden, ne glede na vrsto organizacije. Hitri prehod ima tudi pomanjkljivosti. Večje so možnosti za napake in okvare sistema.

Osnovni koraki spremljanja sprememb za organizacije:

- Potrebno je nadgraditi aplikacijo za podporo naslavljanju z IPv6. Nadgradnja aplikacije je lahko pogosto tudi zahtevna in lahko traja tudi več let. Za nove aplikacije je potem potrebno kupiti tudi licenco.
- Posodobitev DNS infrastrukture za ravnanje z IPv6.
- Nadgraditev in izvajanje IPv6, ki bo sposobno usmerjanja infrastrukture.
- Nadgraditev gostiteljev z združljivimi vozlišči IPv4/IPv6.
- Nadgradnja infrastrukture za usmerjanje IPv6.
- Pretvarjanje vseh vozlišč samo za IPv6.

Vsi večji proizvajalci v računalniški industriji se nagibajo k vključitvi podpore IPv6 v svoje izdelke. Nekateri Windowsi naj bi že podpirali IPv6. Windows CE.NET že popolnoma podpira IPv6. Windows strežnik 2003 je bil prvi operacijski sistem, ki ga je izdal Microsoft in podpira IPv6. Drugi operacijski sistemi oziroma proizvajalci so prav tako upoštevali prihod IPv6. Operacijski sistemi, kot so UNIX in Linux, imajo sedaj že podporo za IPv6. Vsi operacijski sistemi, ki imajo podporo IPv6, omogočajo lažje izvajanje aplikacij (več o podpori programske opreme v nadaljevanju).

8.1 Prehod na IPv6 v Sloveniji

Uvajanje IPv6 v omrežje ARNES (Akademska in raziskovalna mreža Slovenije) se je pričelo leta 2002, ko je Arnes sodeloval pri testiranju pripravljenosti in zmogljivosti omrežne opreme. Julija leta 2003 so pridobili naslovni prostor IPv6 in pričeli z uvajanjem v hrbtenično omrežje. Leta 2004 je bila povezava preko tunela IP že vzpostavljena med Fakulteto za elektrotehniko v Ljubljani ter Inštitutom Jožefa Stefana. Že leta 2005 so se pojavili tudi prvi strežniki IPv6. Vsi ti priklopi so bili realizirani preko tunelov IP. Prva neposredna povezava z IPv6 je bila vzpostavljena leta 2007, ko je omrežje Arnes z gigabitno povezavo Ethernet povežalo omrežje Metulj Univerze v Ljubljani.

Arnes se lahko pohvali tudi s strežnikom, ki meri zakasnitve, variacijo zakasnitve in izgubo paketov IP. Meritve so pokazale, da ni velikih razlik med rezultati pri uporabi protokolov IPv4 ali IPv6. V začetku leta 2008 so preko protokola IPv6 povežali tudi enega od sekundarnih strežnikov za domeno EU.

Da se je večina podjetij v Sloveniji lotila prehoda na protokol IPv6 priča podatek, da je povezavo z Arnesom vzpostavil še en ponudnik IPv6 omrežja: Tuštelekom/Voljatel. Prav tako je Inštitut Jožefa Stefana objavil naročilo za nakup strojne in programske opreme za usmerjanje prometa IPv4 in IPv6.

8.1.1 Analiza obstoječega stanja uvedbe IPV6 v Sloveniji

V tabeli 3 lahko vidimo obstoječe stanje uvedbe IPv6 protokola v nekaterih bolj znanih Slovenskih organizacijah. Stanje lahko spremljamo tudi na go6.si portalu pod sekcijo »Stanje IPv6 v Sloveniji« oziroma na naslovu <http://go6.si/stanje-ipv6-v-slo-devel/>.

Organizacija	IPv6 je implementiran	IPv6 se implementira	IPv6 je v planu	Ni podatka ali pa ni v planu
AMIS	X	X		
APEK			X	
Arne d.o.o.		X		
Arnes	X			
Astec	X			
CHS		X		
delo.si			X	
dnevnik.si				X
Domenca hosting	X	X		
gov.si			X	
Iskra Sistemi d.d		X		
Iskra Tel		X		
LTFE	X			
Mobitel	X	X		
Moj Mikro (Delo revije)			X	
najdi.si		X		
NIL	X	X		
NLB				X
POPtv				X
računalniške-novice.com				X
RTVSLO	X	X		
SiMobil			X	
SmartCom		X		
T-2		X		
Telekom Slovenije	X	X		
Telemach			X	
Tuš Telekom	X	X		
Univerza v Mariboru		X		
zavod go6	X			
ZDRZZ			X	

Tabela 3: Tabela uvajanj IPv6 v podjetja in omrežja na dan 2.11.2010.

8.1.2 Stanje uvedbe in dosegljivost slovenskih spletnih mest preko IPv6

Eric Vyncke skrbi za portal, ki preverja dosegljivost različnih servisov prek IPv6, kot je spletni strežnik, poštni strežnik ter strežnik DNS za domene iz različnih držav sveta, med drugimi tudi Slovenije.

Del stanja je prikazan na sliki 18, celotno tabelo si pa lahko ogledate na naslovu:

<http://www.vyncke.org/ipv6status/detailed.php?country=si>

Ime	Alexa	Web	Mail	DNS
 www.si whois	76/822052	FAILED	FAILED	FAILED
 poptv.si whois	77/846533	FAILED	FAILED	FAILED
 interseek.si whois	78/991618	FAILED	FAILED	ns6.interseek.si ns4.interseek.si 2001:15c0:1000:1004::1:53 2/4 2010-11-11
 nikonsvet.si whois	79/999625	FAILED	FAILED	FAILED
 akton.si whois	/	FAILED	FAILED	FAILED
 ames.eu whois	/	FAILED	FAILED	ns4.ames.eu ns8.ames.si ns9.ames.si 2001:300:14:6054:ad::1 3/5 2010-11-11
 go6.si whois	/	www.go6.si 2a02:e8::1:0:0:babe:face 2010-09-10	mail.go6.si 2a02:e8::1:0:0:babe:face 2010-09-16	ns6.pragma.si ns1.pragma.si ns6.go6.si 2a02:e8::1:0:0:babe:face 3/4 2010-11-11
 ledina.si whois	/	www.ledina.si 2001:1470:fbfe::62 2010-11-03	tito.ledina.org 2001:1470:fbfe::62 2010-11-03	ns1.ledina.si ns2.ledina.si 2001:1470:fbfe::2:53 2/2 2010-11-10
 NIL_Moz.si whois	/	FAILED	FAILED	FAILED
 pragma.si whois	/	www.pragma.si 2001:470:d422::3 2010-09-02	FAILED	carium.pragma.si ns1.ipv6.editdns.net ns1.pragma.si 2001:470:d422::3 3/4 2010-11-11
 shelastyle.net whois	/	FAILED	FAILED	FAILED
 softnet.si whois	/	FAILED	jessie.softnet.si 2a02:800::3:0:0:2 2010-07-30	FAILED
 stargate.si whois	/	FAILED	FAILED	asgard.stargate.si furling.stargate.si replicator.stargate.si prior.stargate.si 2a02:840:1:4:1008::1 4/4 2010-11-11
In total 88 hosts		5 (6%)	3 (3%)	20 (23%)

Slika 18: Dosegljivost slovenskih mest preko IPv6 (v letu 2011).

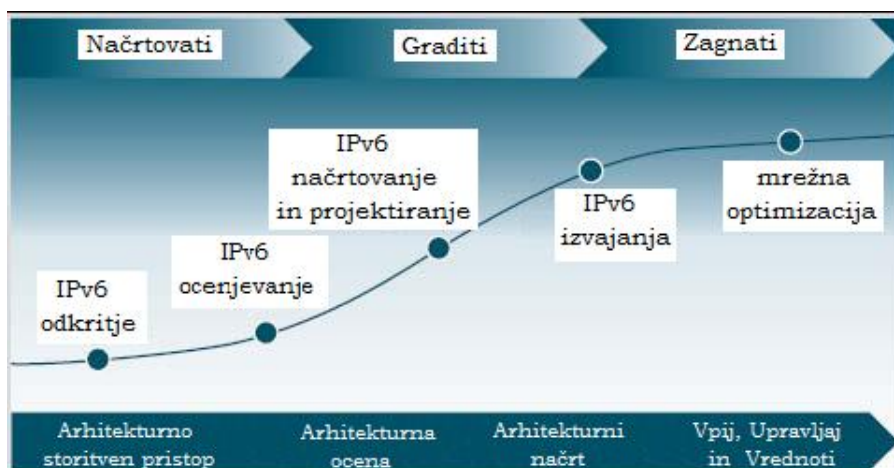
Preko protokola IPv6 je dosegljiv tudi multimedijski portal RTV Slovenija na naslovu <http://www.ipv6.rtvsllo.si> in osrednji spletni iskalnik <http://www.najdi.si> in še mnogo drugih. Stanje uvedbe statusa IPv6 lahko spremljamo na <http://go6.si>, ki aktualizira podatke. V Arnesovo omrežje IPv6 se postopno povezuje mariborska in ljubljanska univerza ter posamezne osnovne šole in tudi nekateri študentski domovi.

9. Postopek uvajanja IPv6 v omrežje

Implementacija protokola IPv6 v produkcijsko okolje zahteva določen čas, v večjih in zahtevnejših omrežjih lahko tudi več let. Takrat pa naslovov IPv4 ne bo več na razpolago.

Zato je potrebno narediti obsežno analizo, ki nam bo podala oceno tveganja, stroškov (nova oprema, izobraževanje osebja, zaposlitev novega osebja) in časa, potrebnega za prehod. Prehod se mora izvajati v korakih in vključuje potrebne spremembe za vse uporabnike, strežnike v lokalnem omrežju ali internetu, aplikacije, storitve, naprave in posamezne elemente. Narediti je potrebno analizo tehničnih in poslovnih koristi. Izvesti je treba analizo, koliko obstoječe strojne in programske opreme bo treba zamenjati ali nadgraditi, da bo sposobna učinkovito uporabljati IPv6 in IPv4. Pomembno je, da oprema, ki jo kupimo popolnoma podpira protokol in funkcionalnosti IPv6 ali pa vsaj nadgradnjo na protokol IPv6.

Izdelati je potrebno poslovni načrt, ki bo dolgoročno pokrival širjenje organizacije v prihodnje (primer načrta prikazuje slika 19). Od regionalnega oziroma lokalnega registrarja je treba dobiti naslovni blok IPv6 (IPv6 prefix) in se povezati v omrežje IPv6 (tranzit in peering). Če bomo pravilno načrtovali in predvidevali vse možne posledice, bomo imeli stroške pod nadzorom in bomo lahko minimizirali tveganje. Da končnih uporabnikov ne izgubimo, mora biti uvedba čim bolj transparentna in nezaznavna.



Slika 19: Fazni pristop k uspešnemu sprejetju protokola v vašo poslovno strategijo [18].

9.1 Pregled lastnosti

Ključni problem, s katerim se že skoraj deset let srečujemo pri uvajanju protokola IPv6 v okolja ponudnikov internetnega dostopa (ISP), so relativno omejene neposredne, ekonomske in tehnološke prednosti, ki jih prinaša njegova uporaba.

Da bi omenjene posledice za posamezne skupine uporabnikov bolje razumeli, poskusimo najprej podrobneje predstaviti prednosti, možnosti, slabosti in nevarnosti (SWOT – Strengths, Weaknesses, Opportunities, Threats), ki jih lahko ima uvedba protokola IPv6.

Prednosti:

- Bistveno večji naslovni prostor protokola IPv6 omogoča neovirano rast in razvoj števila internetnih uporabnikov, kar je ključnega pomena za ponudnike dostopa.
- Možnost zagotavljanja neposredne povezljivosti med poljubnimi vozlišči, izboljšana podpora vrednosti, zagotavljanju kakovosti storitev in mobilnosti vozlišč lahko pripomore k učinkovitejšemu delovanju multimedijskih in varnostnih aplikacij.
- Stalna dolžina glave izboljšuje učinkovitost usmerjanja. Hierarhična ureditev naslovnega prostora pa zmanjšuje velikost usmerjevalnih tabel, kar lahko v nekaterih primerih pripelje do podaljšanja funkcionalne dobe opreme.

Možnosti:

- Možnost pravičnejše razdelitve naslovnega prostora lahko pripelje do zmanjšanja informacijske nepismenosti in digitalnega razkoraka.
- Možnost pospešenega zlivanja storitev zaradi podpore mobilnosti.
- Možnost zmanjšanja stroškov razvoja aplikacij in storitev, saj bo z uporabo protokola IPv6 mogoče izvajanje nekaterih funkcionalnosti prepustiti omrežni plasti.
- Možnost razvoja povsem novih in izboljšanih aplikacij in storitev.
- Možnost uporabe omrežij M2M.

Nevarnosti:

- Lahko nastanejo visoki stroški uvedbe.
- Neustrezno izobražen kader lahko predstavlja ključno oviro pri uvajanju novega protokola IPv6.
- Prav tako lahko bistveno podaljša uvedbo in poviša stroške, hkrati pa poveča tveganje z vidika varnosti.
- Nezdržljivost posameznih implementacij protokola IPv6 lahko povzroči težave pri uvedbi.

Slabosti:

- Protokola IPv4 in IPv6 med seboj nista neposredno združljiva, kar pomeni, da je potrebno prilagoditi vso strojno in programsko opremo.
- Ker je protokol IPv4 omogočil rast interneta iz raziskovalnega v globalno omrežje in se je izkazal kot precej prilagodljiv, je bila kar nekaj časa prisotna skeptičnost glede smiselnosti njegove zamenjave.

Poleg navedenih področji, na katere vpliva uvedba protokola IPv6, ta izpostavlja tudi rešitve resnih problemov soobstoja dveh omrežij IP. Zato se je potrebno zavedati prednosti in slabosti, ki jih prinaša protokol IPv6 v primerjavi z IPv4.

9.2 Stanje standardizacije IPv6

Delovna skupina IPv6, v okviru katere je potekal razvoj osnovnih standardov za podporo delovanju internetnega protokola nove generacije, je končala z delom leta 2007. Sprejeli so preko 43 predlogov standardov in njihovih dopolnil. Navkljub temu, da je jedro specifikacij IPv6 sprejeto in stabilno, še vedno poteka razvoj dopolnilnih in razširjenih standardov IPv6 v drugih delovnih skupinah, kot so:

- IPv6 over Low power WPAN,
- IPv6 Maintenance,
- IPv6 Operations,
- Mobility EXTensions for IPv6,
- Site Multihoming by IPv6 Imediation, ...

Standardizacijski postopek IPv6 torej še ni zaključen. Posledično se proizvajalci opreme pogosto upravičeno znajdejo pred dilemo, kateri nabor standardov RFC uporabiti za katero vrsto produkta ter katere napredne funkcionalnosti implementirati. Standardizacija namreč še ni dokončana, v segmentu definicije produktov pa je večinoma nedorečena oziroma ni v pristojnosti IETF. V primeru nekaterih tipov opreme IPv6 nabor standardov, ki jih mora podpirati, ni jasno določen. Izoblikoval se bo glede na potrebe uporabnikov oziroma s soglasjem združenja proizvajalcev, operaterjev ter drugih končnih uporabnikov.

Na področju specifikacije, verifikacije ter certificiranja produktov IPv6 pionirsko delo izvajajo tri organizacije:

1. Organizacijski program »IPv6 ready«.
2. Obrambno ministrstvo združenih držav (DoD).
3. Nacionalni inštitut za standardizacijo (NIST).

9.3 Uvedba IPv6

Če želimo uvesti IPv6 moramo zaprositi na RIPE-u za dodelitev naslovnega prostora IPv6, ki nam bo omogočal oglaševanje v internet ter povezovanje z ostalimi internetnimi ponudniki. Prav tako je nujno potrebna podpora vodstvenega kadra, zaradi nakupa potrebne strojne in programske opreme. Potrebno je tudi izobraziti vse potrebne kadre v podjetju, da bodo lažje razumeli prednosti in seveda tudi slabosti uvedbe protokola IPv6.

Z uvedbo IPv6 in ukinitvijo mehanizmov NAT se odpirajo ne-slutene nove možnosti za manjša podjetja in rezidenčne uporabnike.

Frank Scalzo, CIO na podjetju Internode je za vodje informatike v podjetjih, uvedbo IPv6 skrčil in poenostavil na 5 preprostih točk, katerih se morajo držati in jih izvesti.

Pet korakov uvedbe IPv6 za vodje informatike v podjetjih [3]:

1. Pridobite dostop do storitev IPv6.
2. Določite uslužbenca, da postane strokovnjak za IPv6.
3. Zaženite pregled omrežja za morebitne težave z napravami, kot so požarni zidovi, usmerjevalniki, VPN mobilni dostop.
4. Ne pozabite na varnost. V svetu IPv6 deluje varnost drugače kot v svetu IPv4.
5. Sprejmite to, da boste delovali z »dual stack« načinom, kar nekaj časa, vendar to ne bo za vedno.

9.3.1 Uvedba IPv6 v manjše podjetje

Veliko manjših podjetij operira s svojimi lastnimi omrežji in sicer za stranko ali pa za notranjo uporabo. Obseg, do katerega je potrebno vaše omrežje nadgraditi, bo odvisen od vaših želj oziroma potreb. Da bi zagotovili, da vaše podjetje ne bo preveč oškodovano pri prehodu, morate imeti odgovore na naslednja vprašanja:

- Ali se vi in vaše IT osebe zaveda IPv6?
- Ali je vaš ponudnik internetnih storitev pripravljen zagotoviti IPv6 povezljivost?
- Je vaša omrežna oprema združljiva z IPv6 in če ni, kakšni ukrepi so potrebni, da bo združljiva z IPv6?
- Ste razmišljali o IPv6 pripravljenosti v vaši tehnološki nadgradnji?

Na podlagi teh vprašanj boste lahko načrtovali korake, ki bodo poskrbeli, da se bo podjetju nadgradnja na IPv6 zdela smiselna in jo bodo podprli.

Prvi korak je, da ocenite, kje ste v zvezi z IPv6 in če vaš ponudnik internetnih storitev morda že ponuja povezljivost IPv6. Če uporabljate strojno in programsko opremo, ki je združljiva z IPv6 potem je lahko uvedba IPv6 enostavna, kot klik na stikalo.

Bolj verjetno je, da bo uvajanje IPv6 vključevalo vsaj nekaj vložnega časa in sredstev. Naslednji seznam je vodilo, kako boste lahko nadaljevali:

- Imenovati vodjo projekta.
- Pogovoriti se s svojimi ponudniki internetnih storitev.
- Določiti omrežne komponente, ki jih bo potrebno nadgraditi ali pa celo zamenjati.
- Poskrbeti za potrebno usposabljanje za ekipo in vodjo projekta.
- Določiti stroške strojne in programske opreme.
- Izbrati dobavitelje in svetovalce.
- Narisati projektni načrt in ga začeti izvajati.

Večina podjetji se zanaša na ponudnika internetnih storitev (ISP) za povezavo z internetom. Pri uvedbi IPv6 v podjetje boste verjetno želeli vprašati svojega ponudnika internetnih storitev naslednje:

- Ali trenutno zagotavljajo povezljivost IPv6?
- Če ne, kdaj nameravajo uvesti IPv6 v omrežjih namenjenih za stranke?
- Kdaj bodo naše spletne strani vidne preko IPv6?
- Ali uporabnikom zagotavljajo IPv6 združljive modeme ali druge naprave potrebne za povezavo preko IPv6?
- Zakaj niso zagotovili informacij o IPv6 in zahtev iz naše strani?

Ko se dogovorite za načrt izvajanj z vašim ponudnikom internetnih storitev, morate upoštevati še:

1. fizično tehnologijo,
2. združljivost programske opreme,
3. izobraževanje.

1. Fizična tehnologija

Bistveni del priprave podjetja na IPv6 je, da zagotovite, da je vaša oprema združljiva z naslednjo generacijo IP-naslovov. Prvi korak je, da naredite revizijo, kateri kos opreme (usmerjevalnik, strežnik in druga strojna oprema) potrebuje nadgradnjo ali celo zamenjavo.

Vaš prodajalec strojne opreme vam mora pomagati in svetovati kako narediti potrebne spremembe. To lahko zahteva veliko časa in truda za pretvorbo vseh elementov vaše IT infrastrukture, tako da boste morda želeli razmisliti o postopnem uvajanju.

2. Združljivost programske opreme

Da bi bilo vaše celotno omrežje pripravljeno za IPv6 morate zagotoviti, da je vsa strojna in programska oprema »Dual stacked« (lahko deluje na IPv4 ali IPv6). Prepričajte se, da je izdelek združljiv s protokolom IPv6 ali pa če je na voljo nadgradnja. Veliko programske opreme, ki je na trgu ima že prevzet protokol IPv6. Če pa nadgradnja na IPv6 ni na voljo, boste morali poiskati alternativni vir programske opreme. Vsa programska oprema, ki je bila razvita v podjetju morda potrebuje predelavo.

3. Izobraževanje

Obstaja veliko možnosti usposabljanja o IPv6, tako preko interneta ali pa iz oči v oči. Če je vaša organizacija član RIPE NCC, se lahko vaši zaposleni udeležijo RIPE IPv6 usposabljanja brezplačno. Usposabljanje vsebuje informacijo o tem, kako dobiti naslove IPv6 in kako pripraviti svoj razvojni načrt. Prav tako pa obstaja tudi več dokumentov RFC, ki jih vzdržuje IETF, in vključujejo študijo primerov uvajanja IPv6 v okviru različnih poslovnih modelov.

9.3.2 Koraki za prehod

1. Potrebna je logistika in **izobraževanje** ljudi znotraj podjetja.
2. Prepričevanje vodilnih, da je vpeljava protokola IPv6 nujna.
3. Pridobiti internetni naslov IPv6 od svojega ponudnika internetnih storitev.
4. Zamenjati ali pa nadgraditi strojno opremo, da bo podpirala protokol IPv6.
5. Poleg zamenjave strojne opreme moramo poskrbeti tudi za programsko opremo, da bo delovala na protokolu IPv6.
6. Po besedah nekaterih je težnost zamenjava strojne in programske opreme le majhen procent pri prehodu na IPv6. Največjo težnost predstavlja izobraževanje.

9.3.3 Primer

Če vzamemo za primer majhno podjetje, ki ima tri računalnike povezane v usmerjevalnik svojega internetnega ponudnika, mu mora njegov internetni ponudnik priskrbeti usmerjevalnik, ki podpira protokol IPv6 in tako samo podjetje nima nobenih stroškov z strojno opremo. Podjetje mora zaprositi še svojega ponudnika internetnih storitev za IPv6 naslov in seveda **izobraziti** svoje zaposlene, da bodo znali delati s protokolom IPv6.

Poleg strojne opreme pa mora podjetje poskrbeti tudi za programsko opremo in operacijski sistem, ki bo podpiral protokol IPv6. Sedaj že večina operacijskih sistemov podpira novi protokol in pri tem ne bodo imeli težav. Pri programski opremi pa se lahko hitro pojavijo težave.

Če na primer podjetje uporablja podatkovno bazo podjetja Oracle, ne bo imelo težav saj omenjena podatkovna baza že podpira novi protokol. Če pa podjetje uporablja podatkovno bazo MySQL se lahko hitro znajde pri velikem problemu, saj podatkovna baza MySQL še ne podpira novega protokola. V takem primeru prehod na IPv6 ne bi bil smiseln za podjetje, saj bi bili stroški ob zamenjavi programske opreme preveliki. Poleg tega pa podjetje verjetno ne uporablja samo podatkovne baze omenjenih proizvajalcev, ampak tudi aplikacije za delo s podatkovnimi bazami za katere je prav tako verjetno potrebno plačilo licence. Vpeljava novega protokola v tako podjetje bi bila nespametna odločitev (vsaj dokler ne bi podatkovna baza MySQL podpirala protokola IPv6).

9.4 Podpora IPv6

9.4.1 Podpora pri operacijskih sistemih

Kot lahko vidimo na sliki 20, že velika večina operacijskih sistemov podpira protokol IPv6. Microsoft Windows je začel podpirati protokol že v verziji 6.1 oziroma z Windowsi 7. Prav tako obstaja dodatek za Windowse XP, da lahko delujejo na protokolu IPv6.

Operacijski sistem	Verzija	Ima IPv6	Nameščen ob namestitvi	DHCPv6	ND RDNS
AIX	4.3	Yes	Yes	Yes	No
Android	2.2	WiFi only ^[1]	Yes	No	No
Cisco IOS	15.0	Yes	Yes	Yes	Yes
Fedora Linux	13	Yes	Yes ^[2]	Yes ^[2]	Yes ^[2]
FreeBSD	7.1	Yes ^[3]	Yes	Addon ^[4]	No
HP-UX	11i	Yes	Yes	Yes	Yes
IBM i	7.1	Yes	Yes	Yes	No
iOS	4.1	Yes	Yes	Yes	Yes ^[7]
Mac OS X	10.6 (Snow Leopard)	Yes	Yes	No ^[4]	No ^[8]
MeeGo	1.2	No ^[13]	Yes ^[14]	No	Yes ^[15]
Microsoft Windows	6.1 (Windows 7)	Yes ^[16]	Yes	Yes ^[4]	No
Symbian OS	7.0	Yes	Yes	No	No
Ubuntu Linux	10.10 (Maverick Meerkat)	Yes	Yes	Yes	Yes
webOS	2.1.0	No	No	No	No
Windows Mobile	6.5	Yes	Yes	Lite ^[20]	No
Windows Phone 7	7.0	No	No	No	No
z/OS	V1R4.0	Yes	Yes	No ^[22]	

Slika 20: Podpora IPv6 pri operacijskih sistemih [17].

9.4.2 Podpora pri aplikacijah

Žal ni dovolj biti samo povezan preko protokola IPv6, ampak morajo tudi naše aplikacije in operacijski sistem podpirati protokol IPv6. V tabeli 4 lahko vidimo primerjavo aplikacij v zvezi z njihovo podporo protokolu IPv6. Kot vir za tabelo sem uporabil internetni naslov http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support.

Aplikacija	Kategorija	Podpora IPv6	Podpora zone ID	Prejšnja verzija ki je podpirala IPv6
Apache httpd	spletni strežnik	Da		2.0.14
ftp.exe	aplikacija	Da	Da	5.1 (XP)
Google Chrome	spletni strežnik	Da		prvotna
Internet Explorer	spletni strežnik	Da	Ne	Verzije nad 7.0
Java	programski jezik	Da	Da	Java 1.5.0
Microsoft DNS	DNS strežnik	Delno		
Mozilla Firefox	spletni brskalnik	Da	Da	1.5
MySQL	baza podatkov	Ne		
Outlook Express	poštni odjemalec	Ne		
Oracle	baza podatkov	Da		11gR1
rTorrent	BitTorrent client	Ne		
Safari	spletni brskalnik	Da	Ne	
telnet.exe	aplikacija	Da	Da	5.1 (XP)
uTorrent	BitTorrent odjemalec	Da		1.8
Windows Mail	poštni odjemalec	Da		prvotna
Wget	izmenjava datotek	Da		1.9

Tabela 4: Podpora IPv6 pri aplikacijah [17].

Kot zanimivost lahko vidimo, da podatkovna baza MySQL še ne podpira protokola IPv6, medtem ko podatkovna baza Oracle že podpira novi protokol. Če torej podjetje uporablja podatkovno bazo MySQL, bi moralo narediti veliko sprememb ob prehodu na protokol IPv6.

9.5 Stroški za podjetja

Pri prehodu na IPv6 predstavlja strošek tako strojna, kot programska oprema. Ker se menjava strojne opreme običajno izvaja že v okviru rednega vzdrževanja in nova strojna oprema že večinoma podpira IPv6, ta menjava ne bi smela predstavljati nekega nenadnega stroška ob prehodu. Podobno velja za novejšo programsko opremo, če se ta redno posodablja. S tega vidika bi še največji strošek pri prehodu na IPv6 pomenila konfiguracija obstoječih aplikacij in programov za delo z IPv6. Prav tako pa bi bilo tudi potrebno usposabljanje zaposlenih v podjetju.

Če uvajanje IPv6 ne bo močno pospešeno, bo prišlo do izjemne upočasnitve rasti interneta, ostanki IPv4 v omrežjih pa bodo povečali stroške uporabe interneta. Posledice te zamude pri uvajanju bodo večji stroški na vseh področjih internetnih storitev, soočali se bomo z upočasnitvijo inovacij v omrežjih, ki temeljijo na internetnem protokolu, počasnejša bo tudi gospodarska rast.

Pri nabavi nove strojne opreme je treba upoštevati standardne cikle zamenjave opreme, saj bo strošek menjave, ko gre za načrtovano investicijo, bistveno manjši. Pomembno je, da oprema, ki jo kupujemo danes, popolnoma podpira protokol in funkcionalnosti IPv6, ki jih bomo potrebovali v času njene življenjske dobe. IPv6 je že integriran skoraj v vseh sodobnih operacijskih sistemih, usmerjevalnikih, požarnih pregradah ... in tako se seznam naprav, združljivih z IPv6 z vsakim dnem podaljšuje.

V okviru menjave opreme večino stroškov predstavlja predvsem:

- izobraževanje osebja,
- nameščanje in konfiguriranje opreme,
- omrežno testiranje,
- ne pa sam nakup opreme, pri katerem cena ne bo bistveno višja v primerjavi z opremo, ki podpira IPv4.

Stroške zamenjave strojne in programske opreme oziroma njene nadgradnje pa je ob primernem načrtovanju mogoče vključiti v stroške rednega vzdrževanja in razvoja omrežja.

Stroški prehoda se bodo razlikovali tudi za različne uporabniške skupine.

- Pri majhnih in srednje velikih podjetjih ter končnih uporabnikih, ki ne upravljajo velikih omrežji, bo ta strošek relativno majhen in ga bo mogoče načrtovati v okviru standardne ciklične zamenjave opreme.
- V nasprotju z njimi bodo lahko imela velika podjetja in vladne agencije višje stroške, pri čemer je nihanje odvisno od obstoječe infrastrukture in operativne politike. To vključuje tudi aplikacije, ki jih bo treba spremeniti ali razviti na novo.

Stroški prehoda lahko hitro narastejo, če imamo v podjetju neizkušen in neustrezno izobražen kader, ki tako bistveno podaljša uvedbo in poviša njene stroške, hkrati pa poveča tveganje z vidika varnosti.

Veliko več pozornosti je treba, bolj kot načinu uvedbe posvetiti stroškom, saj lahko ti v primeru napačno zastavljene strategije, uvedbe in neizkušenega kadra prerastejo ocenjene okvire in resno ogrozijo poslovanje ponudnika dostopa. Ob upoštevanju rezultatov [21] raziskav ocenjujemo, da bo večina stroškov uvedbe protokola IPv6 v omrežje, tudi v Sloveniji povezana z:

- Izobraževanjem tehničnega kadra in testiranje omrežja.
- Sledili jim bodo stroški prilagoditve oziroma nadgradnje orodij za nadzor in upravljanje omrežja.
- Ter stroški zamenjave strojne in programske opreme, katere lahko vključimo v stroške rednega vzdrževanja in razvoja omrežja.

Da bi bili stroški ob prehodu čim manjši, si je potrebno pripraviti načrt. Pri pripravi načrta za prehod na novi protokol moramo določiti:

- Projektne faze ter mejnike, ki so realno dosegljivi in ki jih lahko objektivno merimo.
- Določiti je treba odgovorne osebe, ki bodo zadolžene za usmerjanje dejavnosti v posameznih institucijah, nadzor ter pripravo poročila o napredku v posamezni fazi.
- V vsaki fazi moramo preverjati, ali so načrtovane dejavnosti izvedene in ali so stroški v pričakovanih mejah.
- Če bomo pravilno načrtovali in predvidevali vse možne posledice, bomo imeli stroške pod nadzorom in bomo lahko minimizirali tveganje.

V poslovnih okoljih lahko pričakujemo, da bo največji strošek pri uvedbi protokola IPv6 povezan z izobraževanjem skrbnikov posameznih sistemov, kar še posebej velja v okoljih, v katerih velik del nalog v zvezi z vzdrževanjem opravljajo lastni omrežni in sistemski skrbniki, oziroma tam, kjer te naloge niso zaupane zunanjim izvajalcem.

Navkljub dejstvu, da sta razvoj in testiranje novega protokola prinesla kar nekaj novih stroškov, ki jih v ceno končnega izdelka ni bilo mogoče vključiti, moramo podpora za uvedbo protokola IPv6 na ravni operacijskih sistemov razumeti predvsem kot spodbudo za razvoj novih aplikacij, ki bi lahko v polni meri izkoristile prednosti protokola IPv6.

Kot smo že napisali v točki 9.3.3, bi bili stroški za majhno podjetje minimalni. Med tem ko za velika podjetja stroški hitro narastejo ob nakupu nove strojne in tudi programske opreme, če trenutna ne podpira protokola IPv6.



Slika 21: 24-portno stikalo podjetja Cisco [19].

V tabeli 5 lahko vidimo cenik strojne opreme podjetja Cisco. Tabela je sestavljena na podlagi cen iz spletne strani <http://www.mimovrste.com> iz leta 2011.

Opis naprave	Št. portov	Cena naprave (eur)
Switch Cisco SB SD2008T-EU	8	87,32
Switch Cisco Small Business SRW208-K9-G5,	8	150,11
Switch Cisco Systems Small Business SRW208G-K9-G5	8	248,95
Gigabitni Switch Cisco Small Business SRW2008	10	286,80
Switch Cisco SB SD216T-EU	16	93,02
Switch Cisco SB SR2016T-EU	16	261,04
Gigabitni Switch Cisco SLM224GT-EU	24	223,80
Switch Cisco SB SRW224G4-K9-EU	24	302,35
Switch Cisco Catalyst 2960 WS-C2960-24-S	24	627,71
Switch Cisco Cisco 2960S	24	1.633,51
Switch Cisco ESW-520-24P-K9	28	982,38
Switch Cisco SB SRW248G4-K9-EU	48	659,74
Switch Cisco SRW248G4P-K9_EU	48	1.157,50

Tabela 5: Cenik strojne opreme podjetja Cisco (2011).

Stroški strojne opreme tako rastejo glede na naše potrebe v podjetju in seveda tudi na naše zahteve po varnosti v podjetju, za katero lahko poskrbimo z različnimi napravami (primer: požarni zidovi).

Vsekakor pa ne smemo pozabiti tudi na stroške pri programski opremi. Kot smo že napisali v primeru (glej točko 9.3.3) nam lahko stroški ob prehodu na IPv6 zelo hitro narastejo, če uporabljamo na primer podatkovno bazo MySQL in programe za delo z omenjeno podatkovno bazo, katera še ne podpira protokola IPv6. Tako bi mogli zamenjati programsko opremo in tudi kupiti nove licence za delo z novo programsko opremo.

10. Zaključek

Organizacija IANA je že pred skorajšnjim izčrpanjem naslovnega prostora IPv4 in zato so potrebne druge alternative za pridobitev naslovnega prostora. Ko bo naslovov zmanjkalo, internet ne bo prenehal delovati, tudi omrežje in storitve bodo delovale še naprej. Takojšen problem pa bodo lahko imeli telekomunikacijski operaterji in internetni ponudniki, saj morda ne bodo imeli novih naslovov IPv4, ki bi jih lahko dodelili novim prosilcem. Rešitev je tako čimprejšnja uvedba protokola IPv6, saj nam ta zagotavlja dovolj veliko število naslovnega prostora.

Nadgradnje na IPv6 že potekajo, vendar bo ta prehod dolgotrajen. Mobilne naprave IP, domači igralni sistemi in ostala tehnologija se bo počasi usmerjala na IPv6. Mobilne naprave IP se povezujejo s standardom 802.11, ki se že izvaja z IPv6. Nekateri internetni ponudniki so že začeli z nadgradnjo na IPv6 (npr. Arnes).

Poslovna nadgradnja na IPv6 bo veliko vplivala tudi na podjetja, vpliv bo bolj izrazit pri večjih podjetjih. Povečali se bodo stroški programske in strojne opreme, ki bo potrebna zamenjave ali pa nadgradnje, če je to možno. Pri nadgradnji pa bo potrebno tudi usposabljanje ljudi v podjetju. Spremembe, ki jih zahteva IPv6 se ne morejo zgoditi čez noč. Po nekaterih podatkih naj bi se prehod na IPv6 v celoti izvajal do leta 2030 ali celo 2040. Čeprav se veliki koraki v smeri uvajanja novega protokola že izvajajo je verjetno, da je internet z IPv6 še desetletja stran.

Za prehod na IPv6 predstavlja strošek tako strojna, kot programska oprema. Ker se menjava strojne opreme običajno izvaja že v okviru rednega vzdrževanja in nova strojna oprema že večinoma vsa podpira IPv6, ta menjava ne bi smela predstavljati nekega nenadnega stroška ob prehodu. Podobno velja za novejšo programsko opremo, če se ta redno posodablja. S tega vidika, bi še največji strošek pri prehodu na IPv6 pomenila konfiguracija obstoječih aplikacij in programov za delo z IPv6 in pa usposabljanje zaposlenih v podjetju.

Kot zanimivost lahko še povemo, da je Kitajska že začela z razvijanjem protokola IPv9 na podlagi trenutnega protokola IPv6 [22].

Kazalo slik

Slika 1: Stanje naslovov IPv4 po blokih (2011).	5
Slika 2: Razdelitev naslovov IPv4 (2011).	6
Slika 3: Glava protokola IPv4.	7
Slika 4: Prikaz delitve naslova IPV6.	11
Slika 5: Primerjava dodeljevanja IPv4 in IPv6 naslovov.	13
Slika 6: Prikaz glave IPv6.	14
Slika 7: IPv4 omrežje.	21
Slika 8: Omrežje IPv6.	21
Slika 9: Uporaba dvojnega sklada: razvoj IPv4 in IPv6 na isti infrastrukturi.	22
Slika 10: Tipi paketov pri arhitekturi dvojne plasti IP ter pri arhitekturi dvojnega sklada.	23
Slika 11: Princip tuneliranja.	24
Slika 12: Komunikacija med gostiteljem 6v4 in gostiteljem IPv6.	25
Slika 13: Prikaz Dual stack.	26
Slika 14: Povezava Teredo.	27
Slika 15: Tuneliranje IPv6.	27
Slika 16: Uporaba translacijskega mehanizma.	28
Slika 17: Koncept delovanja NAT-PT.	29
Slika 18: Dosegljivost slovenskih mest preko IPv6 (v letu 2011).	36
Slika 19: Fazni pristop k uspešnemu sprejetju protokola v vašo poslovno strategijo [18].	37
Slika 20: Podpora IPv6 pri operacijskih sistemih [17].	43
Slika 21: 24-portno stikalo podjetja Cisco [19].	47

Kazalo tabel

Tabela 1: Tabela uporabljenih in še razpoložljivih IP naslovov v letu (2010).	9
Tabela 2: Primerjava med IPv4 in IPv6.	20
Tabela 3: Tabela uvajanj IPv6 v podjetja in omrežja na dan 2.11.2010.	35
Tabela 4: Podpora IPv6 pri aplikacijah [17].	44
Tabela 5: Cenik strojne opreme podjetja Cisco (2011).	47

11. Viri

- [1] Silvia Hagan, IPv6 Essentials, O'Reilly Media, Inc, USA, 2006.
- [2] IPv6 Network Administration, O'Reilly Associates, marec 2005.
- [3] (2011) IPv6. Dostopno na: <http://go6.si/> ter <http://en.wikipedia.org/wiki/IPv6> ter <http://www.isoc.org/educpillar/resources/ipv6.shtml> ter <http://sl.wikipedia.org/wiki/IPv6#Viri> ter <http://www-01.ibm.com/software/info/ipv6/index.jsp> ter <http://www.ipv6.org/v6-www.html>
- [4] (2011) IP protokol. Dostopno na: http://en.wikipedia.org/wiki/IP_protocol
- [5] (2011) Komunikacija med IPv6 in IPv4. Dostopno na: <http://arstechnica.com/old/content/2008/10/ietf-working-on-making-ipv6-and-ipv4-talk-to-each-other.ars>
- [6] (2011) Članek podjetja arnes, o aktivnostih IPv6. Dostopno na: <http://www.arnes.org/dokumenti/pregled-aktivnosti-2008.pdf>
- [7] (2011) Razvijanje IPv6. Dostopno na: <http://www.6net.org/book/deployment-guide.pdf>
- [8] (2011) Izivi in tveganja pri IPv6. Dostopno na: <http://www-dsg.stanford.edu/papers/triad/node24.html>
- [9] (2011) Forum o IPv6. Dostopno na: <http://www.ipv6forum.com/>
- [10] (2011) Članek o IPv6. Dostopno na: http://www.arnes.si/dokumenti/IPv6clanek/nova_generacija.htm
- [11] (2011) Knjige o IPv6. Dostopno na: <http://www.goipv6.se/ipv6books.html>
- [12] Joseph Davies, Understanding IPv6, second edition, Microsoft 2008.
- [13] (2011) Delovne skupine za IPv6. Dostopno na: <http://datatracker.ietf.org/wg/>
- [14] (2011) Statistika IPv4 in IPv6 naslovnega prostora. Dostopno na: <http://www.potaroo.net/tools/ipv4/index.html>
- [15] (2011) Teredo infrastruktura. Dostopno na: <http://technet.microsoft.com/de-de/library/dd379548%28WS.10%29.aspx>
- [16] (2011) Prehod na internetni protokol IPv6. Dostopno na: http://www.apek.si/sl/prehod_na_internetni_protokol_ipv6

- [17] (2011) IPv6 podpora aplikacijam in operacijskim sistemom. Dostopno na: http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support ter http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems
- [18] (2011) Kako naj podjetja reagirajo. Dostopno na: <http://www.ipv6actnow.org/>
- [19] (2011) Cisco strojna oprema. Dostopno na: http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/index.html
- [20] Branko Kavšek, Jernej Vičič, Izbrana poglavja iz večpredstavnosti, Univerza na Primorskem, Koper 2011
- [21] (2011) Ekonomični učinek uvedbe IPv6. Dostopno na: <http://www.rti.org/publications/abstract.cfm?pub=6578>
- [22] (2011) Kitajska izdeluje IPv9. Dostopno na: <http://www.chinatechnews.com/index.php?action=show&type=news&id=1405>
http://www.theregister.co.uk/2004/07/06/ipv9_hype_dismissed/