APEK

PREHOD NA IPv6

Razlogi in predlogi za uvedbo IPv6 v slovenska javna in zasebna komunikacijska omrežja

Pripravil:
Urban Kunc, dipl. org. manag., ing. tk.

Ljubljana, februar 2010

ZAHVALA

Zahvaljujem se doc. dr. Andreju Kosu in Janezu Sterletu iz Laboratorija za telekomunikacije na Fakulteti za elektrotehniko ter Janu Žoržu iz Zavoda go6 za koristne pripombe.

Urban Kunc

KAZALO VSEBINE

KAZALO SLIK

1 UVOD

Eden glavnih komunikacijskih protokolov, ki danes omogoča delovanje Interneta, je internetni protokol (IP). Danes najbolj razširjen in uporabljen IP protokol, ki ga uporabljamo že 25 let je označen z verzijo 4, zato ga tudi imenujemo IPv4. Drugi naprednejši protokol IP, je internetni protokol verzije 6 (IPv6), ki odpravlja ključne pomanjkljivosti, ki jih imamo sedaj z IPv4.

IPv6, ki ga tudi poimenujejo IP naslednje generacije (angl. IP Next generation protocol), je bil standardiziran že leta 1998 z RFC2460. Čeprav nam IPv6 protokol prinaša veliko izboljšav in prednosti v primerjavi z IPv4, do zadnjih nekaj let, razen v akademskih omrežjih ni doživel masovne vpeljave. Razlog je predvsem nezdružljivost z IPv4, soočamo se s pomanjkanjem novih storitev in naprav, ki bi temeljili na tem protokolu, pomanjkljivo je znanje o njegovem delovanju in njegovih prednosti, njegova vpeljava na jedrnem in dostopovnem omrežju nam lahko prinaša dodatne stroške.

Eden glavnih razlogov za vpeljavo protokola IPv6 v naša omrežja je pomanjkanje IPv4 naslovov. Ob nastanku Interneta so se načrtovalci IPv4 protokola (angl. DARPA- Defence Advanced Research Projects Agency) odločili, da bo IP naslov verzije 4 velik štiri oktete oziroma 32 bitov. Vodilo pri določanju celotne velikosti IP naslovnega prostora je bilo predvidevanje oziroma domneve o bodoči uporabi IP naslovov in razširjenosti omrežnih naprav.

Glede na to, da so bili določeni 32 bitni IPv4 naslovi, bi lahko teoretično naslavljali preko 4 milijarde različnih javno dostopnih končnih omrežnih naprav, kar je bilo za tisti čas nepredstavljiva in težko dosegljiva številka. Načrtovalci protokola pred 25 leti namreč niso računali, da bo v naslednjih letih prišlo do tako masovne uporabe Interneta in IPv4 naslovov. Dejstvo pa tudi je, da so v začetnih letih Interneta (1991-1994), nekatere organizacije predvsem v ZDA pridobile izjemno velike naslovne bloke IP številk. Kot je razvidno iz spletne strani organizacije IANA http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml so npr. IBM, XEROX, HP, DEC, Apple in MIT prejele vsaka naslovni blok razreda A (predpona /8), ki omogoča naslavljanje preko 17 milijonov naslovov. Analiza razporeditve IP naslovnega prostora pokaže, da samo 15% svetovne populacije uporablja kar 75% vsega razpoložljivega naslovnega prostora kot ga omogoča IPv4. Če bi torej še preostalih 75% populacije želelo imeti svoj IPv4 naslov, ugotovimo, da ga je glede na sedanje stanje odločno premalo.

Problem s katerim smo soočeni danes, je pomanjkanje IPv4 naslovnega prostora. Če se bo trend povpraševanja po IPv4 naslovih nadaljeval, jih bo krovni internetni organizaciji IANA zmanjkalo leta 2011, regionalnim internetnim registrarjem pa leta 2012.
Dokler bodo imeli regionalni internetni registrarji na voljo IPv4 naslovni prostor, nihče ne bo dobil zavrnjene dobro utemeljene prošnje za IPv4 naslov. Vendar zaradi povečanega povpraševanja in posledičnem izčrpanju naslovov, lahko pride do korenitih sprememb tudi na tem področju.
Ob tem ne smemo pozabiti, da se po svetu dnevno ustanavljajo novi operaterji, ki imajo na milijone novih širokopasovnih uporabnikov Interneta, pri čemer bi jih veliko želelo imeti svoj globalni unikatni IP naslov. Z enakimi ali podobnimi težavami se soočajo tudi obstoječi največji operaterji fiksnega širokopasovnega interneta in mobilne telefonije. S porastom števila (zahtevnih) naročnikov in z vse večjo ponudbo novih storitev, bodo operaterji soočeni z dejstvom, da globalnega unikatnega IPv4 naslova uporabnikom ne bodo mogli ponuditi, saj ga ne bo na razpolago. Sicer si operaterji sedaj večinoma pomagajo z napravami, ki

omogočajo translacijo IP naslovov iz javnega v privatni naslovni prostor (angl. NAT-Network Address Translation), vendar dolgoročno to ni rešitev. NAT naprave namreč onemogočajo povezljivost od konca do konca, zmanjšujejo učinkovitost pretoka podatkov in so omejitveni faktor pri razvoju novih storitev in aplikacij.

IPv6, kot rešitev navedenih težav, prinaša mnogo prednosti, pri čemer je njegova največja prednost prav naslovni prostor, ki ga zdaj primanjkuje, saj omogoča naslavljanje kar 2^{128} oziroma $3{,}4 \times 10^{38}$ končnih omrežnih naprav.

Veliko organizacij po celem svetu že nekaj let razpravlja o problemu pomanjkanja IPv4 naslovnega prostora ter kako, bi čim manj boleče in čim hitreje izvedli prehod iz IPv4 na IPv6. Vsi razpravljavci se strinjajo z ugotovitvijo, da je prehod na IPv6 nujen in edini način za nadaljnjo rast in razvoj interneta in informacijske družbe, ki temelji na široki uporabi informacijskih in komunikacijskih tehnologij.

Če uvajanje IPv6 ne bo močno pospešeno, bo prišlo do izjemne upočasnitve rasti Interneta, ostanki IPv4 v omrežjih pa bodo povečali stroške uporabe Interneta. Učinek 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 gospodarska rast.

2 RAZLOGI ZA UVEDBO IPv6

Naslavljanje v IPv4 je dvo-nivojsko. IP naslov sestavlja naslov omrežja in naslova, ki določa končno omrežno napravo. Kolikšen del predstavlja omrežni naslov in kateri del predstavlja IP naslov končne naprave določa omrežna maska oziroma predpona (angl Prefix). Arhitektura IPv4 naslavljanja je od njenega nastanka doživela število iteracij. V letih 1991-1994 je bil na podlagi specifikacije IPv4 naslovni prostor deljen na delitev 8/24, kar pomeni, da je prvih 8 bitov označeval naslov omrežja, zadnjih 24 bitov pa je identificiral končno napravo, gostitelja. Iz tega razloga, so tudi v samem začetku delili IPv4 naslove tako, da je vsaka organizacija dobila po en blok IP naslovov, ki je omogočal naslavljanje skoraj 17 milijonov omrežnih naprav. Kasneje je bil sprejet predlog, da se celotni IPv4 naslovni prostor razdeli v 5 razredov. Razredi A, B in C so bili določeni kot javni globalni (unicast) naslovi, ki pokrivajo naslovni prostor od 0.0.0.0 do 223.255.255.255. Naslovi (razred D) od 224.0.0.0 do 239.255.255.255 so bili dodeljeni za oddajanje več prejemnikov hkrati (angl. Multicast), naslovi od 240.0.0.0 do 255.255.255.254 (razred E) pa so bili rezervirani za nadaljnje raziskovanja in razvoj.

Glavni register IP naslovov vzdržuje Organizacija za dodeljevanje internetnih naslovov IANA (angl. Internet Assigned Numbers Authority). IANA, ki je sicer del javne neprofitne organizacije ICANN (angl. ICANN-Internet Corporation for Assigned Names and Numbers) ni samo odgovorna za upravljanje registra IP naslovov temveč tudi izvaja globalno koordinacijo korenskih (angl. Root) DNS strežnikov in upravljanje s korenskimi zonami ter dodeljuje druge vire, ki se nanašajo na Internetni protokol. IANA upravlja s celotnim naborom IP naslovov. IANA sama direktno ne dodeljuje IP bloke zainteresiranim končnim strankam, temveč zato pooblašča regionalne internetne registrarje (RIR-Regional Internet Registries), ki nato IP naslove 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, in sicer:

- AFRINIC (Afrika);
- APNIC (Azija in pacifiška regija);
- ARIN (severna Amerika);
- LACNIC (latinska Amerika in karibsko otočje);
- RIPE NCC (Evropa, srednji Vzhod in centralna Azija).

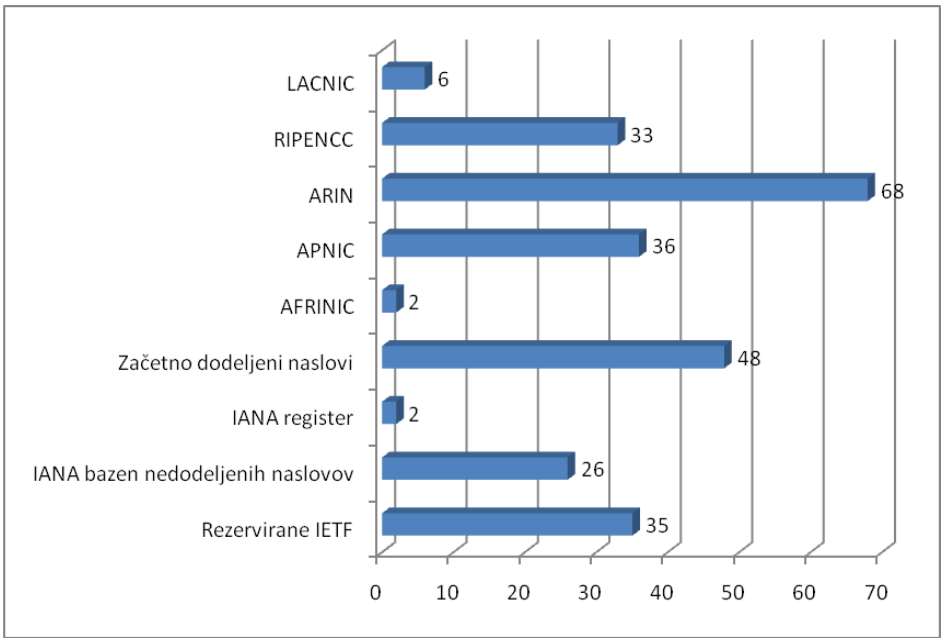
Vsak regionalni internetni registrar ima svojo politiko na podlagi katere se odloča, kako bo svoje vire (IP naslove) dodeljeval in upravljal. Bistvenih razlik pri dodeljevanju IP naslovov med registrarji ni, saj se naslove dodeljuje praviloma na podlagi izraženih utemeljenih potreb. Ko določena organizacija, ki je že član regionalnega registrarja ugotovi, da potrebuje določen IP naslovni prostor, izpolni naslovni načrt ter ga pošlje regionalnemu registrarju. V primerih, da zahtevke po IP naslovih sprejema lokalni registrar, ki je npr. internetni ponudnik, univerza ali operater, se ti zahtevki na koncu leta združijo ter kot en združen naslovni načrt pošljejo naprej v povpraševanje regionalnemu registrarju. RIR prejeti naslovni načrt podrobno pregleda ter če ugotovi, da izpolnjuje vse potrebne zahteve IP naslove dodeli organizacijam-prosilcem. V primerih, da tudi regionalnem registrarjem začne zmanjkovati IP naslovov, se po podobni proceduri zahtevek naslovi na organizacijo IANA, le-ta pa ob izpolnjevanju vseh pogojev RIR-u dodeli nov naslovni blok iz klase A. Ta procedura se lahko izvaja dokler je IP naslovov dovolj za razdeljevanje.

Internetni številski viri (angl. Internet number resources), kot so IP naslovi verzije 4 in 6 ter številke avtonomnih sistemov so po dogovoru brezplačni, saj so skupna javna dobrina. Za njih ne plačuje niti regionalni/lokalni registrar, niti končen uporabnik. Tudi storitve, ki jih IANA izvaja za regionalne registrarje, so za registrarje brezplačne. Edina finančna obremenitev, ki se pri dodeljevanju internetnih virov obračunavajo, so letne pristojbine, ki jih regionalni registrarji za opravljanje registracijskih storitev pobirajo od svojih članov. Predmet plačila je torej storitev, ne pa same IP številke. Kljub vsemu nekateri internetni ponudniki zahtevajo plačilo za dodeljene IP naslovne bloke ali pa druge dodeljene vire. Višina zneska je odvisna od internetnega ponudnika ter od zahtevanih internetnih virov.

Po trenutni (4Q 2009) IPv4 razporeditvi naslovnega prostora imamo štiri kategorije naslovov:

- Nerazporejeni IPv4 naslovi;
- Naslovi, ki so rezervirani ali uporabljeni za eksperimentalne namene;
- IPv4 naslovi, ki so bili dodeljeni še pred vzpostavitvijo regionalnih internetnih registrarjev;
- IPv4 naslovi, ki so bili dodeljeni preko regionalnih registrarjev (APNIC, RIPE NCC, ARIN, AFRINIC, LACNIC).

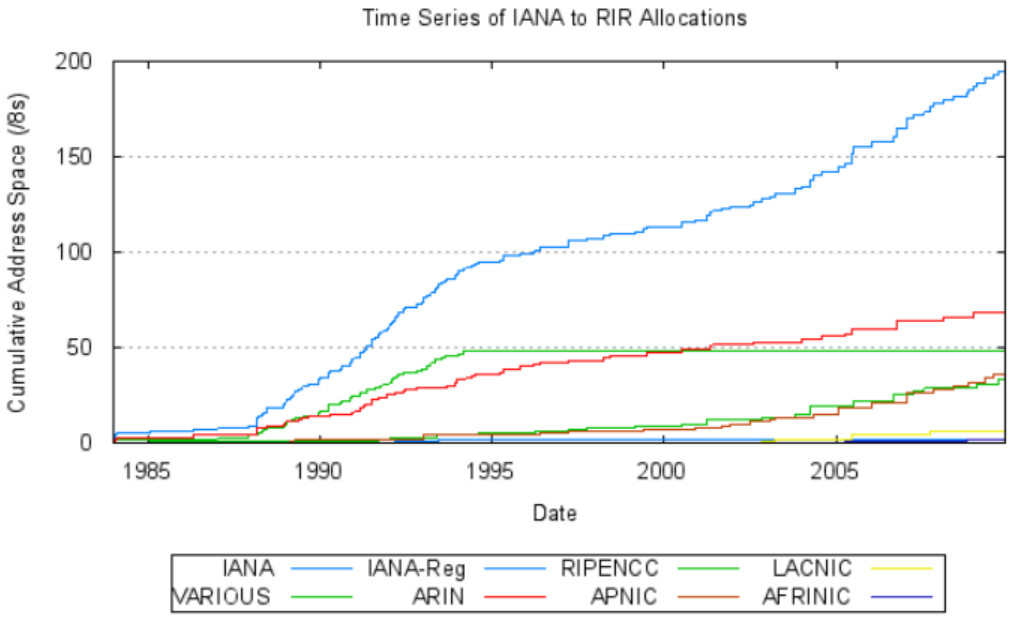
Slika 1 prikazuje trenutno stanje dodelitve IPv4 naslovnega prostora. Stanje prikazuje deleže naslovov, ki so bili dodeljeni posameznim regionalnim registrarjem, IPv4 naslovi, ki so bili dodeljeni v začetku delovanja interneta, IPv4 naslovi, ki so rezervirani za eksperimentalne namene in IPv4 naslovi, ki so še na razpolago.



Slika 1: Trenutno stanje dodeljenih IPv4 naslovov po blokih /8

Vir: http://www.potaroo.net/tools/ipv4/#r4

Iz slike 1 je razvidno, da je od vseh 256 blokov s predpono 8 ostalo nerazporejenih samo še 26 blokov. Največ blokov IPv4 naslovov je dodeljenih v severni Ameriki (začetno dodeljeni naslovi in ARIN), najmanj pa v Afriki (AFRINIC).
Na prvi pogled bi lahko trdili, da je preostalih IPv4 naslovov še dovolj, vendar trend povpraševanja po IPv4 naslovih kaže drugačno sliko.



Slika 2: Povpraševanje po IPv4 naslovih

Vir: http://www.potaroo.net/tools/ipv4/#r4

Ob upoštevanju sedanji 8% letni stopnji rasti povpraševanja po IPv4 naslovih lahko upravičeno pričakujemo, da bo organizaciji IANA IPv4 naslovov zmanjkalo v septembru 2011, posameznim RIR-rom pa v septembru 2012. Aktualno stanje preostalega IPv4 naslovnega prostora je dosegljivo na spletnem naslovu: http://www.potaroo.net/tools/ipv4/index.htm.

Pomanjkanje IPv4 naslovnega prostora pa ni edini razlog, zaradi katerega bi morali izvesti prehod na IPv6. V zadnjih letih je internet ter vsebine in storitve, ki jih omogoča, prineslo za vse uporabnike nove možnosti na vseh področjih našega delovanja. Hitrost dostopa na fiksnih lokacijah se povečuje. Številne evropske države načrtujejo hitrost dostopa vsaj na 100 Mbit/s do leta 2015. Povečalo se bo število širokopasovnih mobilnih omrežij, ki bodo uporabnikom zaradi visokih hitrosti in majhnih odzivnih časov omogočile podobno uporabniško izkušnjo, kot jo imajo sedaj preko dostopa preko klasičnega (fiksnega) dostopa. Trendi uporabe interneta, kot je izmenjava video vsebin, TV visoke ločljivosti (tudi 3D), izobraževanje, bo količino prenesenih podatkov še povečal. Internetne storitve kot so socialna omrežja (Facebook, Twitter..) in računalništvo v oblakih spodbuja k novim inovacijam. Računalništvo v oblakih močno zmanjšuje ovire pri dostopu na trg ponudnikov storitev, zlasti za mala in srednje velika podjetja. V prihodnosti se bo lahko množica naprav, vozil, senzorjev, kamer in drugih 'stvari' priključilo na internet. Predpogoj za takšen scenarij pa so le zmogljiva, visoko prepustna in varna omrežja, ki bodo morala temeljiti na sodobnejših napravah in protokolih, katere temelj je IPv6.

3 PREDNOSTI, KI JIH PRINAŠA IPv6

Glavna prednost novega IPv6 protokola je predvsem ogromen naslovni prostor, ki bo omogočal naslavljanje obstoječih naprav, kot tudi naprav, ki jih danes sploh še ni na tržišču. Protokol sam, sicer ne prinaša visoke stopnje inovacije, temveč povečuje potencialne zmožnosti obstoječih IP omrežij, obenem pa aplikacije, ki bodo narejene na podlagi IPv6 protokola, lahko pripeljejo v radikalne inovacije v različnih sektorjih industrije. IPv6 pri tem ni edina rešitev in IPv4 kot protokol lahko prevzame veliko od tega, vendar omejitev IPv4 naslovnega prostora bi lahko pripeljalo k uporabi alternativnih IP tehnologij, kar lahko posledično upočasni mrežno interoperabilnost in konvergenco medijev, kar pa je ključni faktor za rast in razvoj.

Poleg večjega naslovnega prostora, IPv6 prinaša tudi mnoge druge prednosti. Internet je bil zasnovan tako, da bi omrežne naprave neposredno komunicirale med seboj. Zaradi pomanjkanja IPv4 naslovnega prostora, so morali operaterji in ponudniki omrežne opreme iskati rešitev, kako omejiti rast porabe javnih IPv4 naslovov, ne da ta omejitev prizadela končne uporabnike. Prišlo je do uvedbe translacijskega mehanizma imenovanega NAT (angl. Network Address Translation) oz. NAT-PT (angl. NAT Port translation). NAT-PT omogoča, da ima operater na javni strani interneta samo nekaj javnih globalnih IPv4 naslovov, znotraj omrežja, kjer ima uporabnike, pa dodeljuje rezervirane privatne naslove, ki se lahko podvajajo tudi v drugih privatnih omrežjih. Tako je prišlo do umetne tehnološke ovire, ki je preprečevala nekaterim aplikacijam (npr. omrežne igre, pretočne video vsebine..), da bi normalno delovale, saj so potrebovale povezljivost od konca do konca. IPv6 nam sedaj omogoča to transparentno komunikacijsko povezavo od konca do konca, saj ne potrebuje vmesnih translacijskih mehanizmov. To dejstvo bo posledično omogočilo razvoj veliko novih produktov in storitev, ki nam bodo povečali učinkovitost, zmanjšali stroške ter olajšale življenje.

Nova funkcionalnost, ki jo prinaša IPv6 je tudi mobilnost. Ta omogoča mobilnim terminalom, da se z enim IP naslovom lahko premikajo tudi med tehnološko različnimi omrežji (WLAN hotspot, mobilno omrežje) brez prekinjanja ali izgube povezave.

Večina današnjih omrežnih naprav, ki uporabljajo IPv4 protokol IP naslov pridobi bodisi preko DHCP protokola, PPP povezave in IPCP protokola ali pa ga je potrebno nastaviti ročno. S porastom števila omrežnih naprav, ki uporabljajo IP naslov, potrebujemo enostavnejši in avtomatični način konfiguracije vseh potrebnih parametrov, ki niso odvisni od administracije DHCP infrastrukture. IPv6 nam to omogoča, saj vsebuje mehanizem (SLAAC-Stateless Address Autoconfiguration), ki omogoča na enostaven način dodelitev osnovnih mrežnih parametrov (IPv6 predpona in prehod), ki so potrebni za priključitev omrežne naprave v omrežje. To velja in bo veljalo za vse naprave, ki se lahko povezujejo v IPv6 omrežje, pa naj bodo to osebni računalniki, mobilni terminali ali pa tudi v bližnji prihodnosti inteligentni sistemi ogrevanja, razsvetljave ali navigacije.

IPv6 ima tudi poenostavljeno strukturo glave. Enostavnejša in fiksno določena dolžina IPv6 glave (40 oktetov) omogoča boljšo učinkovitost in izkoriščenost omrežja, saj omogoča hitrejše procesiranje (posredovanje) paketov v posameznih vozliščih (usmerjevalnikih). Tudi hierarhična in zgoščevalna naslovna struktura IPv6 pomeni, da bo na usmerjevalnikih in njihovih usmerjevalnih tabelah potrebno analizirati manjše število usmerjevalnih poti, kar bo omogočalo hitrejše posredovanje paketov in večjo učinkovitost omrežja.

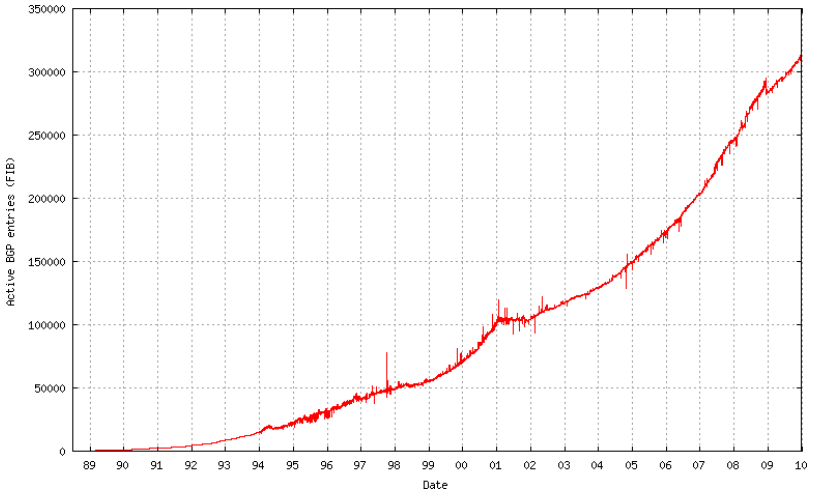
IPv6 povečuje tudi varnost komunikacije med dvema napravama, saj je varnostni protokol IPsec, ki zagotavlja avtentičnost, celovitost in zaupnost komunikacije za razliko od IPv4 že sestavni del protokola. IPv6 s svojo strukturo omogoča tudi enostavnejši način zagotavljanja kvalitete storitve (QoS), skozi celotno pot potovanja paketov. V IPv4 omrežju se paketi tipično posredujejo v najboljšem možnem načinu (Best effort), kar pomeni, da v primeru zasičenja omrežja, lahko prihaja do zakasnitev in drugih anomalij, kar je kritično za časovno odvisne aplikacije (npr. pretočne video, avdio vsebine). V vsakem IPv6 paketu imamo sedaj dva polja (Traffic Class, Flow label) s katerima lahko določamo, kako se posamezni paket obravnava skozi omrežje. Še posebej od polja Oznaka pretoka (angl. Flow label), v glavi paketa se pričakuje, da bo skozi celotno pot potovanja posameznega paketa poenostavil način prepoznavanja in klasifikacije prometa. Za npr. pretočne avdio in video vsebine bomo tako lahko definirali večjo prioriteto prenosa in enako obravnavanje skozi celotno pot paketov skozi omrežje.

3.1 Mehanizmi, ki podaljšujejo življenjsko dobo IPv4 naslovov

Dejstvo, da bo IPv4 naslovov zmanjkalo, so ugotovili že zelo zgodaj, saj je bilo očitno, da je zaradi hitre rasti Interneta povpraševanje po IPv4 naslovih večje, kot ga je na razpolago. Največje povpraševanje po naslovih se je začelo že v drugi polovici devetdesetih, ko je prišlo do množičnega ustanavljanja .com podjetij. Novo ustanovljena podjetja so bila pred dilemo, uporabiti nov nepoznan protokol (IPv6) ter veliko investirati v takrat še drago in nepreverjeno opremo, ki ta protokol podpira, ali pa uporabiti obstoječi IPv4 protokol, ki ni zahteval dodatnih velikih vložkov tako v opremo kot v znanje upravljavcev omrežij. Večina se je odločila za preverjen in dobro poznan IPv4 protokol, ki ga je bilo možno hitro implementirati in ki je hitro povrnil začetne vstopne stroške (ROI).

Drugo zelo pomembno dejstvo, ki je upočasnilo vpeljavo IPv6 protokola v poslovna okolja ter obenem omejilo uporabo IPv4 naslovnega prostora je vpeljava mehanizma CIDR (angl. Classless Interdomain Routing) in NAT-PT (angl. Network Address Translation - Port Translation) ter zasebnih IP naslovov.
Mehanizem CIDR, ki temelji na VLSM (angl. Variable-Length Subnet Masking) je bil predstavljen leta 1993 z internetnim standardoma RFC1518 in RFC1519, v letu 2006 pa je bil še dopolnjen s standardom RFC4632. Glavna funkcionalnost, ki jo omogoča mehanizem CIDR je dodatna pomoč pri prehitrem izčrpanju preostalega IPv4 naslovnega prostora. Paketi, ki potujejo skozi usmerjevalnike se usmerjajo na podlagi ciljnega naslova (omrežja), ki je zapisan v glavi IP paketa. Vsak usmerjevalnik s pomočjo usmerjevalnih protokolov vodi eno ali več tabel, v katere se zapisujejo informacije, preko katerih vmesnikov je dostopno določeno omrežje. Dokler so se razdeljevali samo IP naslovni bloki razreda A in B je bilo teh zapisov v usmerjevalnih tabelah malo, saj oba razreda predstavljata majhno število omrežij in veliko končnih gostiteljev. Po drugi strani pa razreda A in B predstavljata kar 75% vsega razpoložljivega IPv4 naslovnega prostora, pri čemer imamo manj kot 17.000 organizacij na svetu, ki so številčno tako velike, da bi potrebovale tako velik naslovni blok, kot je razred A ali B. Ko pa je začelo blokov A in B razreda zmanjkovati, so začeli podeljevati naslovne bloke iz razreda C, ki omogočajo kreiranje skoraj 17 milijonov različnih omrežij, vendar z največ 254 končnimi napravami, ki so direktno dosegljivi tudi iz Interneta. CIDR poskuša izpolnjevati zahteve organizacij po IP naslovih tako, da zagotavlja organizaciji samo toliko IP naslovov, kot jih dejansko potrebuje. Če npr. organizacija potrebuje 1980 IP naslovov, se ji ne dodeli razred B, ki omogoča 16.382 končnih naprav, temveč si ji dodeli 8 nepretrganih blokov omrežij razreda C, kjer vsak blok omogoča naslavljanje 254 končnih naprav (8x256=2048). Ker internetni BGP usmerjevalniki v svojih usmerjevalnih (BGP) tabelah hranijo in vzdržujejo podatke o dosegljivosti vseh avtonomnih sistemih (angl.- AS Autonomous systems), se s

povečanjem števila omrežij (predvsem iz razreda C) tudi bistveno poveča velikost usmerjevalne tabele posameznega BGP usmerjevalnika. Slika 3 prikazuje porast zapisov v BGP tabeli. Iz tabele je tudi razviden preskok v številu zapisov v času porasta .com podjetij v letih 1999 do 2002.



Slika 3: Porast zapisov (FIB) v BGP tabelah od 1994 do danes

Vir: http://bgp.potaroo.net/as1221/bgp-active.html

Posledica porasta števila zapisov v BGP tabelah bi lahko bila, da bi manj zmogljivi usmerjevalniki odpovedali, saj ne bi uspeli hitro in učinkovito obdelati enormno število zapisov Internetnih usmerjevalnih poti. Po drugi strani pa je za BGP usmerjevalni protokol značilno, da ob nedosegljivosti posameznega vozlišča, potrebuje za razliko od drugih usmerjevalnih protokolov bistveno več časa za konvergenco vseh (posodobljenih) zapisov BGP usmerjevalne tabele.
Prednost, ki jo prinaša tudi mehanizem CIDR ob podpori posodobljenega BGPv4 usmerjevalnega protokola (RFC 4271) je tudi združevanje internetnih poti (angl. Route aggregation), ki omogoča, da se omrežje sestavljeno iz večjega števila (blokov) podomrežij na zunaj oglašuje kot eno veliko 'super' omrežje. Na ta način se tudi zmanjša število zapisov v BGP usmerjevalnih tabelah, kar poveča učinkovitost delovanja usmerjevalnika oz. zmanjša čas potrebne konvergence vseh zapisov.

NAT je drugi mehanizem, ki je bistveno omejil porabo javnih IPv4 naslovov. NAT-PT, ki je običajno implementiran kot del funkcionalnosti požarne pregrade, omogoča jasno ločevanje med javnimi in zasebnimi omrežji. NAT-PT naprave imajo na strani interneta dodeljen eden ali več javnih globalnih naslovov, na strani zasebnega omrežja pa se uporablja zasebne IP naslove, ki so predpisani z internetnim standardom RFC1918. Ta mehanizem omogoča, da imamo na strani zasebnega omrežja ogromno število gostiteljev z zasebnimi IP naslovi, ki se na strani javnega interneta predstavljajo s samo enim ali manjšim številom javnih IPv4 naslovov. Čeprav mehanizem bistveno zmanjšuje porabo javnih IPv4 naslovov, prinaša tudi mnogo slabih strani. Njegove slabost je predvsem, da preprečuje povezljivost od konca do konca, nekatere aplikacije in igre preko teh naprav ne delujejo, problematične so za avdio ali video pretočne vsebine. Ker se za posameznim javnim IP naslovom lahko skriva na tisoče uporabnikov, je tudi zelo težko določiti katera naprava, je uporabljala javni IP naslov v določenem trenutku.

V tem trenutku je zelo težko natančno napovedati, kako se bo nadaljevalo povpraševanje po IPv4 naslovih in kakšne bodo posledice pomanjkanja in nezmožnost pridobitve novih IPv4 naslovov. Veliko je odvisno od razvitosti posamezne države ter od števila širokopasovnih uporabnikov interneta. Velik porast povpraševanja po IP naslovih lahko pričakujemo predvsem v državah, kjer se širokopasovni internet šele razvija. Večina evropskih držav vključno s Slovenijo imajo dobro razvit trg širokopasovnega fiksnega dostopa, zato se ne pričakuje, da bo na tem segmentu prišlo do bistvenih sprememb v trendu povpraševanja po IP naslovih. Je pa že opaziti trend, da so zelo hitro povečuje število uporabnikov, ki stalno uporabljajo širokopasovne podatkovne storitve tudi na mobilnih terminalih. Med najbolj obetajoče storitve na mobilnih terminalih bi lahko izpostavili uporabo socialnih omrežij, storitev prisotnosti, lokacijska informacija, P2P aplikacije, dostop do spletnih vsebin. Te in podobne storitve bodo v bližnji prihodnosti bistveno spremenile (povečale) povpraševanje po IP naslovih.

Obstaja več scenarijev, ki bodo posledica pomanjkanja IPv4 naslovov. Nekateri scenariji predvidevajo, da bodo tiste organizacije, ki imajo veliko neizkoriščenih IPv4 naslovov, naslove začele vračati nazaj regionalnim internetnim registrarjem. Vrnjeni IPv4 naslovi bodo na razpolago za ponovno dodelitev. Ta scenarij je malo verjeten. Možen scenarij je tudi, da bodo organizacije začele trgovati s svojimi neuporabljenimi IPv4 naslovi. V tem primeru se bo vzpostavil sekundarni trg IPv4 naslovov. Lahko pa se tudi zgodi, da bodo organizacije začele IPv4 naslove uporabljati učinkovitejše, še posebej, če bodo RIR-i uvedli pristojbine za dodeljene IPv4 naslovne bloke.

V kolikor bo IPv4 naslovov zmanjkalo bo Internet deloval še naprej. Obstoječi operaterji bodo imeli možnost, da postopoma preidejo na IPv6 protokol ali pa nadaljujejo z obstoječim (zastarelim) IPv4 protokolom, pri čemer si bodo morali zaradi pomanjkanja javnih IPv4 naslovov pomagati s translacijskimi mehanizmi.
Vsi novi operaterji, internetni ponudniki, ponudniki vsebin in storitev ter organizacije, ki se bodo želele povezati v globalni internet in IPv4 naslovov ne bodo dobile, bodo morale zaprositi za IPv6 naslove in se povezati v Internet preko IPv6 protokola.

4 STRUKTURA OMREŽIJ

Infrastrukturo Interneta sestavlja množica med seboj povezanih žičnih in brezžičnih omrežij. Ključne elemente in enitete Interneta lahko v grobem delimo na:

- hrbtenično-jedrno omrežje, ki ga zagotavlja večje število relativno zelo velikih med seboj povezanih operaterjev internetnega transporta. Ponudniki internetnega transporta, ki v povprečju prenesejo enakovredno količino podatkovnega prometa si med seboj izmenjujejo komunikacijski promet brezplačno, njihove medsebojne povezave (angl. Peering) pa so določene z dogovorom o nivoju storitev (SLA). Ponudniki internetnega transporta imajo svojo lastno zmogljivo hrbtenično infrastrukturo, ki je sestavljena predvsem iz optičnih vlaken ter pripadajoče aktivne opreme;
- ponudniki internetnih storitev (ISP -Internet Service Provider), ki zagotavljajo storitev dostopa do interneta svojim poslovnim in rezidenčnim uporabnikom. Ponudniki internetnih storitev, si preko skupnih internetnih izmenjevalnih točk (angl. IX-Internet Exchange) med seboj izmenjujejo komunikacijski promet obenem pa so povezani še na enega ali več ponudnikov internetnega transporta, ki jim omogočajo globalno povezljivost v internet. Ponudniki internetnih storitev imajo lahko svojo lastno

dostopovno infrastrukturo ali jo najamejo v okviru storitve dostopa z bitnim tokom pri operaterju s pomembno tržno močjo;

- širokopasovno žično in brezžično dostopovno in agregacijsko omrežje ter pripadajoča aktivna oprema;
- omrežja poslovnih in rezidenčnih uporabnikov;
- sistem strežnikov domenskih imen (DNS), ki predstavljajo distribuirano hierarhično bazo, ki omogoča in zagotavlja prevajanje domenskih imen v IP naslove;
- poštni strežniki, ki omogočajo shranjevanje in prenos elektronske pošte;
- spletni in podatkovni strežniki, ki omogočajo shranjevanje in predstavitev spletnih in drugih vsebin na Internetu;
- strežniki, ki omogočajo shranjevanje medijske vsebine in njeno distribucijo na zahtevo;
- strežniki, ki omogočajo in zagotavljajo prenos govornih storitev (VoIP) in storitev navzočnosti (angl. Instant Messaging) preko IP protokola;
- druge Internetne storitve.

5 MIGRACIJSKE TEHNIKE

Vpeljava novega komunikacijskega protokola, ki povrh vsega ni združljiv s starim ni enostaven postopek, zato tudi prehod iz verzije IPv4 v verzijo IPv6 ni nobena izjema. Vpeljava novega komunikacijskega protokola v omrežje kot je IPv6 lahko tudi pomeni nadgradnjo ali zamenjavo opreme na vseh vozliščih znotraj posameznega omrežja. Sama izvedba migracije je lahko različna glede na elemente omrežja, ki jih ima posamezni operater ter tehnologije in protokolov, ki jih uporablja. Če npr. operater že v svojem jedrnem omrežju uporablja IP/MPLS, je morda tudi razumna odločitev, da migracijska strategija temelji na že obstoječi IP/MPLS tehnologiji. Migracija je lahko na jedrnem omrežju drugačna od strategije, ki jo bomo uporabili na agregacijskem ali dostopovnem omrežju. Razlike so lahko tudi med samimi ponudniki dostopovnega omrežja. Vpeljava novega protokola tudi posledično povzroči, da je potrebno izvesti veliko testiranja interoperabilnosti z drugimi protokoli in napravami, ki ta protokol uporabljajo. Če je to lahko obvladljivo v majhnih okoljih z majhnim številom omrežnih naprav, predstavlja to velik organizacijski in tehnični zalogaj v okoljih, ki ima na tisoče uporabnikov in naprav. Z vidika interneta, ki združuje na milijone naprav in milijone uporabnikov, ki so odvisni od internetnih storitev, je prehod iz IPv4 na čisti IPv6 podvig, ki ga ni mogoče opraviti čez noč. Nekateri pesimisti celo napovedujejo, da bi ta prehod preko vmesnih faz trajal lahko celo dvajset let ali več.

Ker je torej za pričakovati, da bomo čisti IPv6 imeli šele po daljšem časovnem obdobju, je skoraj edina rešitev v vmesnem času sobivanje obeh protokolov. Razvijalci IPv6 protokola so v internetnem standardu RFC 1752 (The Recommendation for the IP Next Generation Protocol) zapisali naslednje kriterije prehoda (IETF, 1995):

- Obstoječi IPv4 gostitelji so lahko nadgrajeni kadarkoli, neodvisno od nadgradnje ostalih gostiteljev ali usmerjevalnikov
- Novi gostitelji, ki uporabljajo IPv6, se lahko v omrežje dodajo kadarkoli, neodvisno od ostalih gostiteljev ali infrastrukture usmerjanja,
- Obstoječi IPv4 gostitelji, ki imajo nameščen IPv6, lahko uporabljajo obstoječe IPv4 naslove in ne potrebujejo novih naslovov,

- Potrebne so manjše priprave, če želimo nadgraditi obstoječe IPv4 vozlišča na IPv6 ali če želimo namestiti nova IPv6 vozlišča.

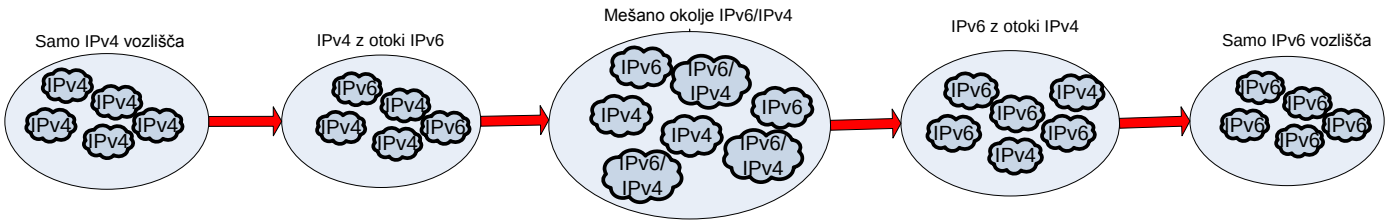
Ker protokola IPv6 in IPv4 nista med seboj združljiva, IPv4 in IPv6 usmerjevalna infrastruktura potrebuje mehanizem, ki bo omogočal brezprekinitveno sobivanje obeh protokolov.

Internetni standard RFC 4213 iz leta 2005 (Basic Transition Mechanisms for IPv6 Hosts and Routers) določa naslednje vozliščne tipe:

- Samo IPv4 vozlišča so gostitelji in usmerjevalniki, ki uporabljajo samo IPv4 verzijo protokola. Ta vozlišča ne razumejo IPv6 protokol. Večina starejših računalnikov, strežnikov in druga omrežna oprema, kot so mrežni tiskalniki in usmerjevalniki so IPv4 vozlišča,
- Vozlišča IPv6/IPv4 so gostitelji ali usmerjevalniki, ki imajo implementiran IPv6 in IPv4 protokol,
- Samo IPv6 vozlišča so gostitelji ali usmerjevalniki, ki imajo implementiran le IPv6 protokol in uporabljajo le IPv6 naslove. Ta vozlišča lahko direktno komunicirajo le z IPv6 vozlišči in IPv6 omogočenimi aplikacijami in ne razumejo IPv4 protokola,
- Vozlišča IPv6 so gostitelji in usmerjevalniki, ki imajo implementiran IPv6 sklad ter lahko pošiljajo in sprejemajo IPv6 pakete. IPv6 vozlišča so lahko samo IPv6 vozlišče ali IPv6/IPv4 vozlišče,
- Vozlišča IPv4 so gostitelji in usmerjevalniki, ki imajo implementiran IPv4 sklad ter lahko pošiljajo in sprejemajo IPv4 pakete. IPv4 vozlišča so lahko samo IPv4 vozlišče ali IPv6/IPv4 vozlišče.

Da se lahko vzpostavi sobivanje obeh protokolov, morajo IPv4 in IPv6 vozlišča uporabljati IPv4, IPv6 infrastrukturo ali infrastrukturo, ki omogoča (so)uporabo kombinacijo obeh protokolov.

Pravi prehod ali izpolnjen končni cilj je uresničen šele takrat, ko se vsa IPv4 vozlišča preoblikujejo v vozlišča, ki uporabljajo samo in izključno IPv6 sklad. V vmesnem obdobju moramo torej stremeti k cilju, da imamo v omrežju čim več omrežnih naprav (IPv6/IPv4 vozlišča), ki podpirajo oba protokola. Slika 4 nam prikazuje faze prehoda iz IPv4 na IPv6.



Slika 4: Faze prehoda iz IPv4 na IPv6

Ker imamo na razpolago velik nabor migracijskih tehnik, ni enostavna odločitev za posameznega operaterja/internetnega ponudnika, katero strategijo izbrati, ki bo za njega najbolj optimalna. V prehodnem obdobju sobivanja obeh protokolov, je tako zelo verjetno, da

bomo imeli samo IPv4 vozlišča, samo IPv6 vozlišča ali pa vozlišča, ki hkrati podpirajo oba protokola (Dual stack). Kakor dolgo med seboj povezani gostitelji uporabljajo isti IP protokol, je komunikacija med njimi mogoča. Če gostitelji uporabljajo isti IP protokol, ne pa tudi usmerjevalniki, ki prenašajo pakete med njimi, se mora uporabiti tunelske mehanizme. Če gostitelji uporabljajo različne verzije IP protokola, potrebujemo med njimi translacijski mehanizem, ki bo zagotavljal povezljivost med obema protokoloma.

Da lahko omogočimo uporabo obstoječo IPv4 infrastrukture ter obenem pripravimo podlago za čisto IPv6 infrastrukturo so najbolj znane naslednje migracijske tehnike, ki zagotavljajo povezljivost med končnimi sistemi in omrežji, ki uporabljajo različen IP protokol:

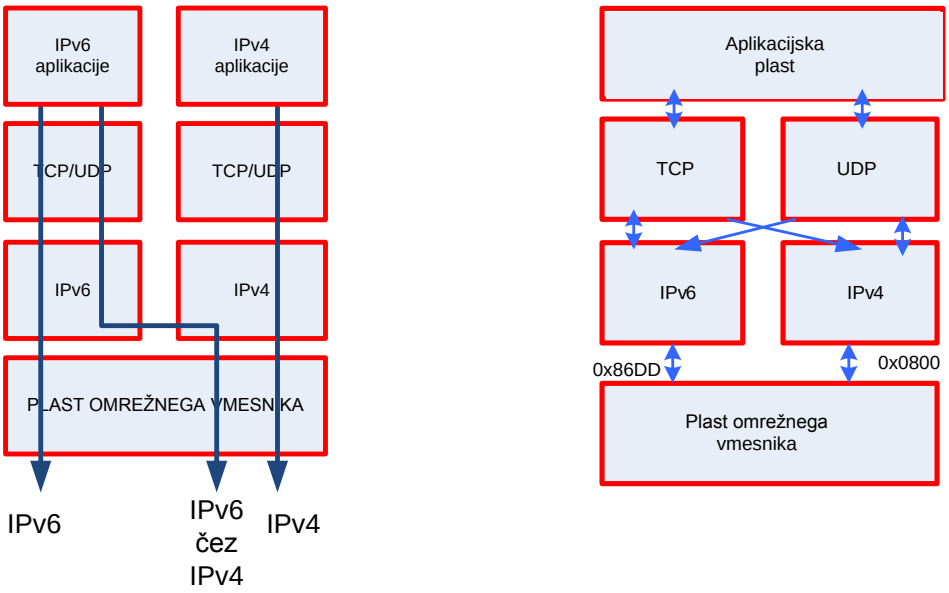
- Souporaba obeh protokolov IPv6 in IPv4 (Dual stack),
- Tunelski mehanizmi,
- Translacijski mehanizmi.

5.1 Dvojni sklad (Dual stack)

Obdobje prehoda od sedanje IPv4 infrastrukture do končne čiste IPv6 infrastrukture bo trajalo precej časa. Čeprav se prehod izvaja v korakih, je potrebno ne glede na uporabljeno infrastrukturo (IPv4, IPv6, IPv6/IPv4) in druge uporabljene komunikacijske protokole zagotoviti povezljivost omrežnih naprav, uporabnikom pa omogočiti uporabo storitev z enako ali boljšo uporabniško izkušnjo ne glede na to, na kakšni infrastrukturi so postavljeni ali katere protokole uporabljajo. Kljub temu bodo lahko nekatere Internetne storitve dostopne le preko IPv4 ali samo preko IPv6 protokola. Iz tega razloga morajo končni sistemi in usmerjevalniki, ki usmerjajo promet med omrežji sposobni obdelovati oba protokolna sklada IPv4 in IPv6. To nam omogoča t.i. arhitektura dvojnega sklada (Dual Stack), ki 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 IPv4 protokolnega sklada, če prejme IPv6 paket ga bo posredoval čez IPv6 protokolni sklad. Razlikovati moramo med dvojnim skladom, ki ga uporabljajo usmerjevalniki in dvojni sklad, ki je implementiran v operacijskih sistemih gostiteljev.

Usmerjevalnik, ki uporablja dvojni sklad, lahko posreduje IPv4 in IPv6 promet. Če smo še bolj natančni, bo usmerjevalnik z vključenim dvojnim skladom s povezavo na IPv4 usmerjevalnik posredoval samo IPv4 pakete, na povezavo z IPv6 usmerjevalnikom, pa bo posredoval samo IPv6 pakete. Poleg tega, lahko usmerjevalnik z dvojnim skladom deluje kot vhodna ali izhodna točka tunela, ki povezuje med seboj sicer nekompatibilna (IPv6 oz. IPv4) omrežja.

Tudi končni sistemi, ki imajo dvojni sklad implementiran kot del operacijskega sistema, enako kot usmerjevalniki ločeno glede na vrsto prometa obdelujejo datagrame v svojem protokolnem skladu. Glavna razlika med usmerjevalniki je v tem, da imajo poleg omrežne in trasportne plasti ločeno tudi aplikacijsko plast. Aplikacije lahko izbirajo svoj protokolni sklad. Če imamo IPv4 aplikacije bodo te uporabile IPv4 sklad, IPv6 aplikacije pa bodo uporabile IPv6 sklad. Odločitev o izbiri ustreznega protokolnega sklada je avtomatična in je v primeru prihajajočega okvirja izbira protokola odvisna od vrednosti, ki je zapisana v 16 bitnem polju Ethertype, ki opredeljuje vrsto omrežnega protokola, ki je ovit (angl. Encapsulation) v koristnem delu tovora sloja podatkovne povezovalne plasti. Slika 5 prikazuje arhitekturo dvojnega sklada.



Slika 5: Arhitektura dvojnega sklada

Zavedati se moramo, da dvojni sklad v jedru omrežja izključno omogoča komunikacijo samo med IPv4 gostitelji, kot tudi samo med IPv6 gostitelji. To pomeni, da gostitelji s samo IPv4 skladom ne morejo direktno komunicirati z gostitelji, ki uporabljajo samo IPv6 in obratno.
Ker so ukazi vtičnika za vsak IP protokol med seboj različni, morajo starejše aplikacije, ki so bile razvite za IPv4 protokol nadgrajene na IPv6. To pomeni, da v primerih, ko aplikacijska plast uporablja IP naslov v svoji koristni vsebini (npr. FTP-File Transfer Protocol, SIP-Session Initiation Protocol ali H.323) potem se mora pripadajoča aplikacija nadgraditi, če želimo da bo uspešno obravnavala IPv6 naslove.
Z vidika operacijskih sistemov je teh problemov manj, saj večina sodobnejših operacijskih sistemov Microsoft Windows Vista, Windows Server 2008, Windows 7 ter večina distribucij Linuxa, Mac OS X, BSD, Solaris, HP-UX, AIX, Symbian 7 (Nokia) že omogočajo delovanje v dvojnem skladu. Pri operacijskem sistemu Windows XP in Windows Server 2003, IPv6 protokolni sklad privzeto ni nameščen, zato ga moramo namestiti posebej. Navedeno velja tudi za starejše Linux sisteme.

V kolikor imamo usmerjevalnike, ki že podpirajo dvojni sklad, je smiselno to funkcionalnost izkoristiti, še posebej, ker je tudi z IPv6 potrebno pridobiti nekaj praktičnih izkušenj. V kolikor pa moramo za IPv6 funkcionalnost nadgraditi usmerjevalnike ali celo kupiti nove, lahko to predstavlja za večje organizacije ali operaterje nemajhen strošek. V začetni instalacijski fazi, uporaba dvojnega sklada na usmerjevalnikih predstavlja strošek v opremi (CAPEX) kot strošek v zagotavljanju varnosti, upravljanju in vzdrževanju te opreme (OPEX). V Sloveniji zaradi majhnega števila implementacij podatka o stroških še nimamo, vendar je za pričakovati, da bodo operativni stroški (OPEX) zaradi uporabe dvojnega sklada lahko večji v primerjavi s stroški upravljanja in vzdrževanja samostojnega IPv4 sklada. Operaterji bodo zato dolgoročno že zaradi zmanjševanja stroškov stremeli k čim prejšnji uvedbi čistega IPv6 omrežja.

5.2 Tunelski mehanizmi

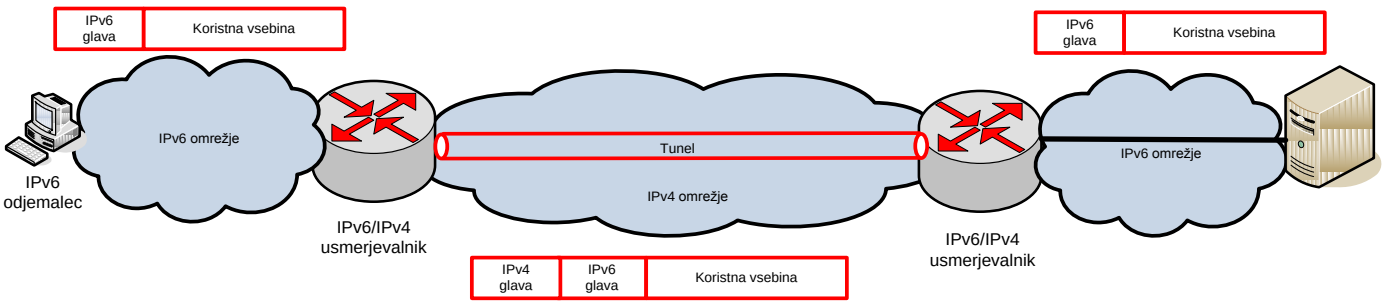
Tuneli so velikokrat uporabljena tehnika, kadar moramo en transportni protokol oviti kot koristno vsebino drugega protokola. Velikokrat so razlogi pri tem lahko v nezdružljivosti med prenosnim in končnimi omrežji, ali zaradi zahteve po povečani varnosti vsebine prometa. Tunelske mehanizme lahko koristno izkoristimo tako, da preko tunela poleg IPv4 od zanesljivega ponudnika pripeljemo v omrežje tudi IPv6.

Kadar razmišljamo o uvedbi IPv6 povezljivosti preko tunelov, moramo upoštevati vsaj še naslednje:

- tuneli lahko predstavljajo potencialno varnostno vrzel, zato moramo promet skozi njega ustrezno nadzirati in varovati,
- zavedati se tudi moramo, da celotni tunel, čeprav promet prehaja skozi množico usmerjevalnikov, za robni usmerjevalnik predstavlja en sam skok (angl. Hop),
- tuneli omogočajo rekurzivno ovijanje, kar nam omogoča, da imamo lahko tunel v tunelu,
- kadar uporabljamo tunelske mehanizme moramo tudi ustrezno nastaviti največjo prenosno enoto (angl. MTU-Maximum Transfer Unit).

V omrežjih IPv4 so prilagajanje na velikost največje prenosne enote (MTU) določale vmesne naprave (usmerjevalniki), pri IPv6 pa so gostitelji tisti, ki odkrivajo in prilagajajo velikost največje prenosne enote (MTU Discovery) skozi celotno pot paketa. Če pride do napake pri prenosu podatkov skozi tunel, morajo biti ICMP (angl. Internet Control Message Protocol) nadzorna sporočila o napakah ustrezno prevedena med obema protokoloma.

Usmerjevalniki, ki omogočajo tuneliranje, pakete pred izhodom iz izvornega omrežja ovijejo (angl. Encapsulation) v druge pakete (v drug protokolni sklad) ter 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. Osnovni princip tuneliranja nam prikazuje slika 6.



Slika 6: Tuneliranje

Tunelske mehanizme lahko ločimo na:

- samodejno nastavljive tunele, ki se vzpostavijo med dvema robnima omrežjema samodejno po potrebi. IPv4 naslov tunelske končne točke je določen z IPv4 naslovom, ki je vsebovan v (IPv4 kompatibilnem) ciljnem naslovu IPv6 paketa.

Značilni predstavniki avtomatsko nastavljivih tunelov so 6to4, ISATAP, posredniški tuneli (angl. Tunnel Broker).

- ročno nastavljive tunele, kjer administrator ročno nastavi parametre za končne robne točke tunela in tehnologijo ovijanja. IPv4 naslov tunelske končne točke je določen s parametri, ki jih poda usmerjevalnik, ki izvaja ovijanje paketov. Značilni predstavniki ročno nastavljivih tunelov so IP v IP, GRE (angl. Generic Routing Encapsulation), IP/MPLS (IP Multiprotocol Label Switching)

Samodejno nastavljivi tuneli (6-4, ISATAP, storitev Tunnel Broker) so zelo uporabni v začetni fazi prehoda na IPv6, saj omogočajo, da na cenovno dostopen način dobimo povezljivost v IPv6 omrežja, ki ga lahko izkoristimo za testiranje in učenje ali priklop manjših skupin uporabnikov.

5.2.1 Posrednik tunelov (Tunnel Broker)

Posredniki tunelov so organizacije, ki omogočajo končnim gostiteljem ali usmerjevalnikom z dvojnim skladom, da preko IPv4 omrežja s pomočjo vzpostavljenega tunela prejmemo povezljivost v IPv6 omrežje. V Sloveniji lahko končni uporabniki dobijo tunelsko IPv6 povezljivost preko tunelske vhodne točke, ki jo omogoča Laboratorij za telekomunikacije (http://www.ltfe.org/ltfefour6/), ki deluje v okviru Fakultete za elektrotehniko in računalništvo, Univerze v Ljubljani. Obstaja še množica drugih posrednikov, kot so npr.: SixXS, Tunnel Broker (Hurricane Electric) in drugi. Spisek evropskih tunelskih posrednikov je mogoče najti na naslovu: http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers#Europe.
Pri storitvi posredništva tunela, se uporabnik, ki uporablja operacijski sistem z dvojnim skladom poveže na posredniški strežnik, kjer se registrira. Z registracijo pridobi ustrezne konfiguracijske parametre, na podlagi katerih lahko vzpostavi tunel skozi IPv4 omrežje med svojo delovno postajo oz. robnim usmerjevalnikom ter končno robno točko posrednika tunela. Ponudnik oz. posrednik tunela periodično preverja status tunela in tunelskega gostitelja ter, če gostitelj storitve ne uporablja, jo sprosti in ter ponudi drugemu uporabniku. Samodejni tuneli so za posrednika tunela praviloma enostavnejši in cenejši kot ročno nastavljivi tuneli.

5.2.2 Mehanizem 6v4

Mehanizem 6v4 (angl. 6to4) se lahko uporabi, kadar želimo povezati izolirana IPv6 omrežja preko avtomatično vzpostavljenega tunela, ki je vzpostavljen skozi IPv4 omrežje. Mehanizem je enostaven in je podprt v večini operacijskih sistemov (Windows, Linux, BSD), vključno s PC kompatibilnimi aparati (angl. PC compatible appliances). Mehanizem 6v4 celotno IPv4 omrežje interneta pojmuje kot povezavo, kjer je možno oddajanje samo enemu prejemniku (angl. Unicast). Mehanizem 6v4, ki je standardiziran z RFC3056 se lahko izvaja v relacijah:

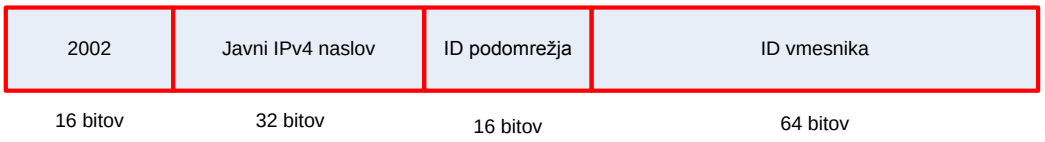
- usmerjevalnik-usmerjevalnik
- gostitelj – usmerjevalnik
- usmerjevalnik-gostitelj

Omenjeni standard tudi predpisuje samostojen naslovni format IPv6 naslova, ki je sestavljen iz štirih blokov, v katerem so vrednosti zapisane v šestnajstiški obliki:

- prvo 16 bitno polje prestavlja naslovni prostor, ki definira mehanizem 6v4. Sestavljen je iz formata 2002::/16, ki predstavlja rezerviran naslov za naslavljanje 6v4,
- drugo 32 bitno polje predstavlja dodeljeni javni globalni IPv4 naslov, ki je dodeljen s strani Internetnega ponudnika,

- tretje 16 bitno polje predstavlja ID podomrežja, ki je nastavljeno znotraj organizacije
- 64 bitno polje, ki identificira končno vozlišče (strojni naslov komunikacijskega vmesnika) na podomrežju organizacije.

Slika 7 predstavlja strukturo 6v4 naslovnega polja.



Slika 7: Struktura 6v4 naslovnega polja

Tuneliranje 6v4 se samodejno izvaja na vmesniku končnega gostitelja ali usmerjevalnika, ki omogoča ovijanje 6v4. Ime vmesnika je odvisno od nastavitev računalnika, praviloma pa so vmesniki, ki izvajajo tuneliranje označeni z zvezdico (*). V primeru, da je to Windows operacijski sistem, je ta vmesnik imenovan *Local Area Connection* * 6 (Davies, 2006). Vmesnik, ki izvaja tuneliranje 6v4 pojmuje IPv4 Internet kot samostojni (single) povezovalni sloj oziroma povezavo, podobno, kot ga predstavlja Ethernet. V primeru tunelske povezave 6v4, je v podatkovnem povezovalnem sloju uporabljen način ovijanja paketov IPv4.
Velikokrat je tudi napačno razumevanje principa 6v4, da za komuniciranje z IPv6 omrežji oz. strežniki v internetu potrebujemo IPv6 povezljivost ali 48 bitno naslovno predpono (angl. Prefix), ki jo pridobimo od svojega internetnega ponudnika. Čeprav je to zaželeno, ta pogoj ni nujen. Mehanizem 6v4 nam omogoča, da:

- ustvarimo in uporabljamo javno globalno IPv6 predpono omrežja, ki temelji na dodeljenem IPv4 naslovu v obliki: 2002:IPv4_naslov::/48
- se povezujemo na svoj že vzpostavljen del IPv6 (pod)omrežja skupaj z tuneliranjem IPv6 prometa čez IPv4 internet
- se povezujemo in koristimo IPv6 vire, ki so povezani samo v IPv6 internet.

Vmesniki, ki izvajajo 6v4 ovijanje, uporabljajo svojo lastni 6v4 IP naslov, ki predstavlja izvorni IPv6 naslov. Tunelski 6v4 vmesnik določa ciljni IPv4 naslov, ki ga prebere iz ovitega IPv4 naslova (drugi in tretji blok ciljnega IPv6 naslova).
Internetni standard RFC3056 določa štiri komponente, ki so del implementacije 6v4. To so:

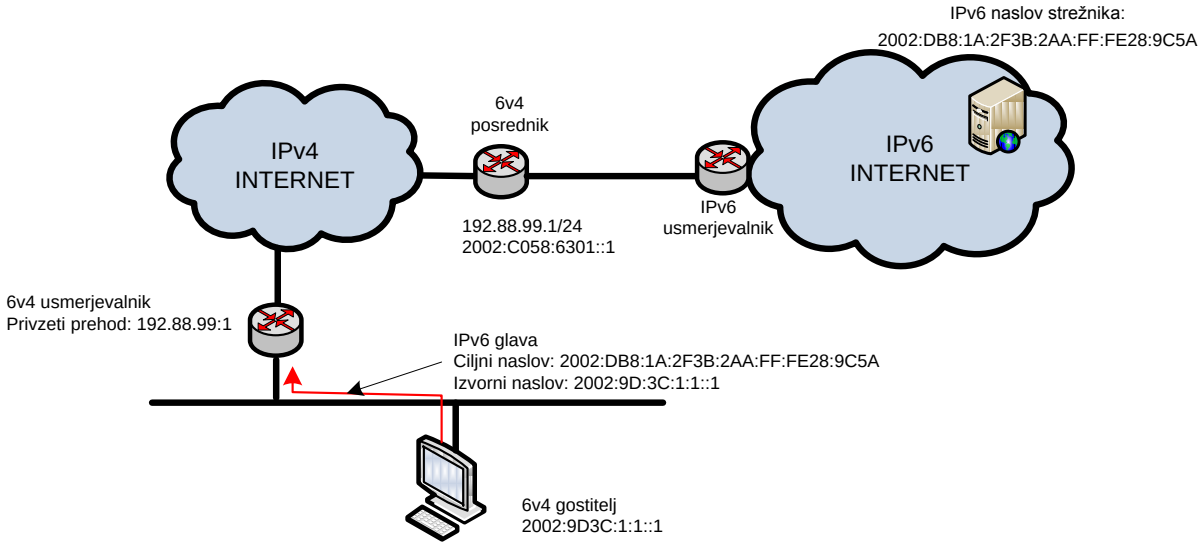
- 6v4 gostitelj, ki predstavlja računalnik, ki je konfiguriran vsaj z enim 6v4 naslovom (2002::/16 predpono). 6v4 gostitelji, ne potrebujejo nobene dodatne podpore ali ročne konfiguracije parametrov, saj vse potrebne podatke samodejno dobijo od usmerjevalnika s funkcionalnostjo 6v4 ali DHCPv6 strežnika. 6v4 gostitelji nimajo tunelskega vmesnika, niti ne izvajajo tuneliranja,
- 6v4 usmerjevalnik. Usmerjevalnik uporablja 6v4 tunelski vmesnik, ki omogoča posredovanje 6v4 naslovljenega prometa med 6v4 gostitelji znotraj posamezne lokacije ali pa med drugimi 6v4 usmerjevalniki. Omogoča tudi posredovanje prometa med napravami, ki so v funkciji 6v4 gostitelja/usmerjevalnika ali 6v4 posrednika (angl. Relay).
- gostitelj/usmerjevalnik 6v4. Je IPv6/IPv4 gostitelj, ki uporablja 6v4 tunelski vmesnik s katerim izmenjuje 6v4 naslovljen promet z drugimi 6v4 gostitelji/usmerjevalniki, 6v4 usmerjevalniki ali 6v4 posredniki čez IPv4 internet. Za razliko od 6v4 usmerjevalnikov,

6v4 gostitelj/usmerjevalnik ne posreduje prometa drugim 6v4 gostiteljem. Primer 6v4 gostitelja/usmerjevalnika je npr. gostitelj z Windows Vista operacijskim sistemom, ki je direktno povezan v IPv4 internet z dodeljenim IPv4 javnim naslovom.

- 6v4 posrednik (angl. Relay). 6v4 posredniki so bili vzpostavljeni z namenom, da izvajajo posredništvo med IPv4 Internetom in IPv6 Internetom. 6v4 posrednik je usmerjevalnik, ki posreduje 6v4 naslovljen promet med 6v4 usmerjevalniki in 6v4 gostitelji/usmerjevalniki, ki so povezani v IPv4 internet in gostitelji, ki so povezani samo v IPv6 omrežje. Paketi, ki prihajajo iz IPv6 Interneta in so naslovljeni na 6v4 usmerjevalnike ali 6v4 gostitelje, morajo biti poslani preko 6v4 posrednika s pomočjo običajnega IPv6 usmerjanja. RFC3056 določa, da morajo 6v4 posredniki oglaševati samo 2002::/16 omrežje, ne pa tudi podomrežje. S tem preprečimo, da bi z IPv4 potmi onesnaževali usmerjevalne tabele IPv6 usmerjevalnikov.

V kolikor 6v4 usmerjevalnik ali gostitelj želi komunicirati z 6v4 usmerjevalnikom ali gostiteljem, se ta povezava vzpostavi preko IPv4 interneta. V primeru, da želi 6v4 usmerjevalnik ali gostitelj komunicirati z gostiteljem, ki se nahaja v IPv6 omrežju, se ta komunikacije vedno vzpostavi preko 6v4 posrednika, ki nato posreduje promet proti IPv6 internetu. V obratni smeri, ko 6v4 posrednik prejme promet Iz IPv6 Interneta in je ta naslovljen v 6v4 omrežja, pakete ovije v IPv4 pakete ter jih posreduje ustreznemu 6v4 usmerjevalniku ali gostitelju.

Slika 8 prikazuje promet vzpostavitve komunikacije med 6v4 gostiteljem ter strežnikom, ki se nahaja v IPv6 Internetu.



Slika 8: Komunikacija med 6v4 gostiteljem in IPv6 gostiteljem

5.2.3 Mehanizem 6rd

Mehanizem 6rd (angl. Rapid Deployment), ki ga opredeljuje RFC5569 je migracijska tehnika, ki tudi omogoča IPv6 povezljivost skozi obstoječe IPv4 omrežje. Mehanizem ima podoben koncept kot mehanizem 6v4 (angl. 6to4) le da vključuje določene spremembe. Mehanizem

omogoča ponudniku storitev hitro uvedbo IPv6 (unicast) storitev pri čemer naročniki lahko uporabljajo IPv6 in IPv4 storitve sočasno.
Arhitektura 6rd se sestoji z:

- CPE usmerjevalnih prehodov (angl. Router gateway) s podporo 6rd, ki omogočajo 'softwire' ovijanje paketov IPv6 v IPv4, ki se izvaja na strani naročnikov
- Enega ali več 6rd prehodov (lahko so nadgrajeni 6to4 posredniki), ki omogočajo zaključevanje (terminiranje) tunelov in usmerjanje IPv6 paketov v IPv6 omrežje
- Obstoječo dostopovno IPv4 omrežje ponudnika

Pri mehanizmu 6v4, 6v4 gostitelj ali usmerjevalnik uporablja globalno (fiksno) predpono, ki se začne z vrednostjo 2002::/16. Pri mehanizmu 6rd pa ponudnik storitve uporablja specifično IPv6 predpono, ki jo pridobi od svojega regionalnega internetnega registrarja. 6rd naslov CPE naprave je tako sestavljen iz:

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

6rd mehanizem v času tranzicije na čisti IPv6 predstavlja za internetne ponudnike zelo obetajoč način zagotavljanja IPv6 povezljivosti. 6rd je v svoje omrežje zelo uspešno in to v kratkih petih tednih implementiral francoski internetni ponudnik Free. Po podatkih[1], naj bi IPv6 povezljivost prek mehanizma 6rd imelo omogočeno prek 1.500.000 Free-jevih rezidenčnih naročnikov. Zadnje novice (januar 2010) pa tudi kažejo, da bo mehanizem 6rd v prvi fazi tranzicije vpeljal v svoje produkcijsko omrežje tudi Comcast, največji ameriški kabelski ponudnik internetnih storitev.

5.2.4 ISATAP

ISATAP (angl. Intra-Site Automatic Tunnel Addressing Protocol) je še en mehanizem, ki omogoča avtomatsko tuneliranje IPv6 paketov skozi IPv4 omrežje. ISATAP je bil v predstavljen v internetnem osnutku RFC4214, kasneje pa je bil dopolnjen s sedanjim Internetnim standardom RFC 5214. 6v4 mehanizem zagotavlja povezljivost v IPv6 internet tako IPv6 kot tudi IPv4/IPv6 gostiteljem. ISATAP pa omogoča avtomatsko tuneliranje gostiteljem ne glede na to, ali uporabljajo zasebni ali javni IPv4 naslov. Tako, kot tudi pri drugih tranzicijskih mehanizmih, je tudi pri ISATAP ključno način naslavljanja končnih naprav.

ISATAP naslov je lahko:

- IPv6 globalni usmerjevalni unicast naslov (kadar se promet usmerja proti IPv6 internetu)
- IPv6 povezavno-lokalni (kadar se promet izmenjuje med direktno povezanimi gostitelji ali usmerjevalniki)
- IPv4 naslov (kadar se povezuje z IP4 gostitelji)

Ko komuniciramo direktno s sosedom v lokalnem omrežju, njegov ID vmesnika povezavno-lokalni (angl. Link-local) naslov avtomatsko naznanja tunelsko končno točko. ISATAP

[1] RFC5569: http://tools.ietf.org/html/rfc5569

pojmuje IPv4 infrastrukturo kot podatkovni povezavni sloj (angl. Data Link Layer) virtualnega nerazpršenega večdostopovnega omrežja (angl. NBMA - Nonbroadcast multiple-access network), ki ne omogoča razpršenega oddajanja (angl. Broadcast) ali oddajanje več gostiteljem hkrati (angl. Multicast). NBMA je omrežje direktno povezanih računalnikov in naprav, kjer se komunikacija med njimi izmenjuje preko navideznih povezav (angl. Virtual circuit). Primer takšnih omrežij so ATM, blokovno posredovanje (angl. Frame Relay) ali X.25. Ker ISATAP pojmuje IPv4 omrežje kot NBMA, ne uporablja značilne funkcionalnosti IPv6 protokola, to je odkrivanje sosedov ali usmerjevalnikov (Neighbor/Router discovery). Običajno se v IPv6 okoljih v ta namen uporablja funkcionalnosti protokola ICMPv6. Naslov povezavnega sloja (Link Layer address), ki je povezan z IPv6 naslovom je mogoče razbrati v zadnjih 32 bitih IPv6 naslova, zato mehanizma za odkrivanje sosedov ne potrebujemo. Ker ISATAP tudi ne omogoča naslavljanja več oddajnikom hkrati, nam to preprečuje uporabo funkcionalnosti avtomatskega odkrivanje usmerjevalnikov (angl. Router solicitation). Za pridobitev informacije o razpoložljivih usmerjevalnikih imamo na razpolago tri načine:

- usmerjevalnike vpišemo ročno v 'Host' tabelo gostitelja (potencialna lista usmerjevalnikov),
- jih oglašujemo s pomočjo protokola DHCP,
- IP naslovi in pripadajoče popolno kvalificirano domensko ime (FQDN) so zapisani v DNS strežniku (npr. isatap.router.com).

Ko gostitelj enkrat pridobi IPv4 naslove vseh potencialnih usmerjevalnikov, lahko vsakemu na njegov IP naslov direktno pošlje povpraševanje (angl. Router solicitation). Pri tem lahko gostitelj koristi pridobljen usmerjevalnikov povezavno-lokalni IP naslov ali pa tunelira svoje povpraševanje v IPv4. Na podlagi odgovora usmerjevalnika, lahko gostitelj kreira svoj IPv6 globalni naslov, ki temelji na oglaševani predponi (usmerjevalnika) in ISTAP ID-ju vmesnika (0000: 5EFE+IPv4 naslov).
ISTAP mehanizem je podprt v protokolnem skladu Microsoft Windows XP, Vista, Windows 7, Windows Mobile in v nekaterih distribucijah Linuxa.

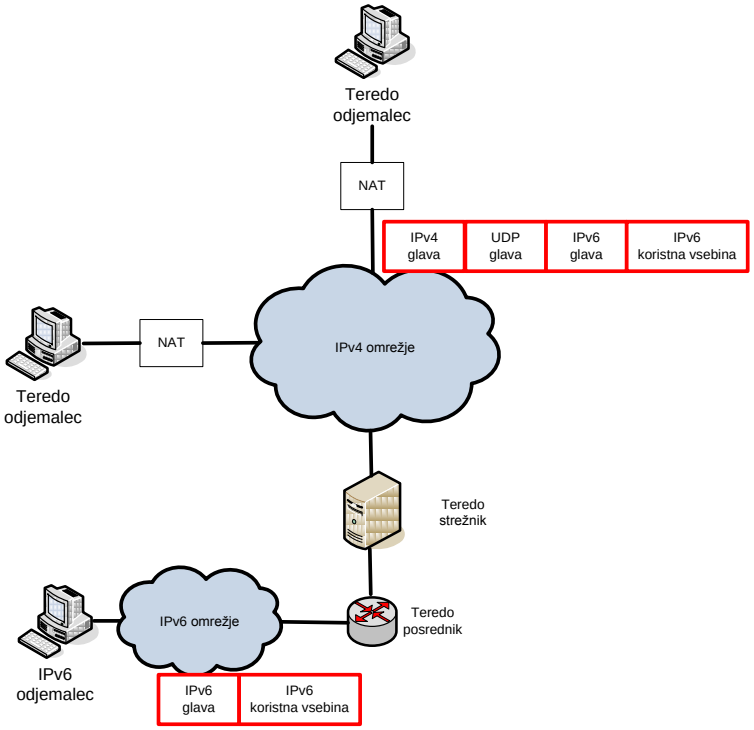
5.2.5 Teredo

Teredo, ki je opisan z internetnim standardom RFC4380 je še en IPv6 tranzicijski mehanizem, ki omogoča dodeljevanje naslovov in tuneliranje unicast prometa IPv6/IPv4 gostiteljem, ki se nahajajo za IPv4 NAT napravami. Gostitelji v primeru mehanizma Teredo lahko uporabljajo zasebne IP naslove, ki so definirani v RFC1918. Da lahko vzpostavimo komunikacijo skozi NAT napravo, Teredo gostitelji tunelirajo ves IPv6 promet v UDP paketih, ki so oviti in poslani Teredo posrednikom. Pri tem tudi izkoriščamo specifiko večine NAT naprav, da transparentno prepuščajo UDP pakete, katera koristna vsebina sta glava in vsebina IPv6 paketa.
Tehnika Teredo se sestoji iz treh osnovnih komponent:

- Teredo odjemalca
- Teredo strežnika
- Teredo posrednika (angl. Relay)

Teredo odjemalec, ki podpira oba IP protokolna sklada (IPv4 in IPv6) prejme od Teredo strežnika IPv6 predpono (angl. Prefix) ter obenem deluje kot vstopna/izstopna točka tunela. Teredo strežnik posluša prihajajoči promet na UDP vratih 3544 ter ga posreduje naprej proti Teredo posredniku. Teredo posredniki so IPv4/IPv6 mejni usmerjevalniki, ki posredujejo IPv4 UDP promet med Teredo strežniki in čistimi IPv6 odjemalci, ki se nahajajo v IPv6 internetu

in, ki komunicirajo preko IPv6 prometa. Posredniki delujejo kot tunelska končna točka za IPv6 pakete, ki so tunelirani čez UDP IPv4. Teredo posredniki poleg tega oglašujejo dosegljivost Teredo storitev v IPv6 omrežje obenem pa so zmožni komunicirati tudi z drugimi tranzicijskimi mehanizmi, kot je npr. 6v4. Teredo strežnik kot tudi posrednik sta običajno locirana na isti lokaciji.



Slika 9: Infrastruktura Teredo

Specifično za Teredo je tudi njegova naslovna struktura. Slika 10 predstavlja naslovno strukturo paketov Teredo.

32 bitov	32 bitov	16 bitov	16 bitov	32 bitov
Teredo predpona	IPv4 naslov Teredo strežnika	Zastavice	Mapirana odjemalčeva UDP vrata	Mapiran odjemalčev IPv4 naslov

Slika 10: Teredo naslovna struktura paketa

Teredo IPv6 naslovna struktura zaradi vstavljene IPv6 usmerjevalne predpone predstavlja sicer neučinkovit način rabe IPv6 naslovnega prostora. Razlog temu je, da mora Teredo posrednik oglaševati dostopnost Teredo storitev preostalemu delu IPv6 interneta. 32 bitna Teredo predpona je skupna vsem Teredo strežnikom, tako, da mora Teredo posrednik oglaševati v IPv6 Internet IPv6 predpono, ki se mora ujemati najmanj z Teredo predpono in IPv4 naslovom Teredo strežnika. To pomeni, da se mora usmerjevalna predpona za vsak različen Teredo strežnik injicirati v IPv6 Internet. V teoriji lahko to pomeni injiciranje usmerjevalne predpone v IPv6 Internet za vsako IPv4 lokacijo, ki se skriva za NAT napravo. Če nimamo niti IPv6 povezljivosti niti nimamo skupnega prostora za 6v4 usmerjevalnik in NAT, se zaradi navedenega Teredo storitev uporabi le kot zadnjo možnost. Zaradi njegove

kompleksnosti je tudi vprašljivo njegovo delovanje v okoljih, ki so postavljeni za NAT napravami, saj obstaja veliko variacij NAT-a, ki niso nujno kompatibilne z Teredo mehanizmom. (6net Consortium, 2005).
Predstavljeni avtomatski tunelski mehanizmi nam morajo biti le prehodna stopnja, kajti na daljši rok mora biti naš cilj čisti IPv6, ki ga moramo dobiti od zanesljivega internetnega ponudnika tranzita.

5.3 Translacijski mehanizmi

5.3.1 Osnove NAT(PT) mehanizma

Dokler smo uporabljali samo klicne modemske povezave do ponudnika interneta, je bilo IPv4 naslovov dovolj, saj se je s prekinitvijo povezave sprostil tudi začasno dodeljen IPv4 naslov. S porastom širokopasovnih povezav pa internetni ponudniki in sedaj tudi mobilni operaterji prihajajo do situacije, da jim IPv4 naslovov zmanjkuje, saj širokopasovne povezave zahtevajo stalno povezljivost v internet ter stalno dodeljene IP številke.
Pomanjkanje javnih globalnih IP naslovov nam rešuje translacijski mehanizem imenovan NAPT (angl. Network Address Port Translation). Osnovni NAT mehanizem, ki izvaja samo translacijo naslovov je bil predstavljen leta 1994 z internetnim standardom RFC 1631. NAT mehanizem, ki je običajno implementiran kot del usmerjevalnika/požarne pregrade ima en zunanji vmesnik (angl. Interface), ki je naslovljen z javnim IPv4 naslovom ter eden ali več notranjih vmesnikov, ki so povezani na notranje zasebno omrežje. V notranjem omrežju uporabljamo zasebne IPv4 naslove, ki so določene z internetnim standardom RFC 1918 in se lahko podvajajo tudi v drugih zasebnih omrežjih. Z RFC 1918 določeni zasebni IP naslovi (10.0.0.0/8-10.255.255.255/8; 172.16.0.0/12-172.31.255.255/12; 192.168.0.0/16-192.168.255.255/16) se lahko uporabljajo izključno v zasebnih omrežjih ter se ne smejo pojaviti v javnem internetnem omrežju. Da tej zahtevi zadostimo morajo biti zasebni IPv4 naslovi blokirani na robnih požarnih pregradah zasebno/javnega omrežja.

Vsaka vzpostavljena komunikacija med računalnikom v zasebnem omrežju ter računalnikom v javnem internetu predstavlja TCP/UDP sejo, ki unikatno identificira n-terko (angl. Tuple), ki jo sestavlja izvorni IP naslov, izvorna TCP/UDP vrata, ciljni javni IP naslov in ciljna TCP/UDP vrata. Sporočila ICMP protokola, ki so integralni del IP protokola ter služijo za javljanje napak v komunikaciji, so identificirane kot n-terka: izvorni IP naslov, ID ICMP poizvedbe in ciljni IP naslov. Vse druge seje so okarakterizirane kot n-terka izvornega IP naslova, ciljnega IP naslova in vrsta IP protokola.
Osnovna naloga usmerjevalnika, ki uporablja NAT mehanizem je, da prevaja IP naslove iz enega naslovnega področja v drugega, pri čemer je usmerjanje paketov transparentno za obe končni točki. NAPT za razliko od osnovnega NAT mehanizma, ne prevaja samo IP naslove, temveč tudi številke vrat (portov).
Usmerjevalnik z NAPT funkcionalnostjo analizira komunikacijski promet, ki potuje skozi njega ter pri tem gradi tabelo povezav (sej) med računalniki zasebnega omrežja in računalniki javnega omrežja.
Ko pride zahteva za vzpostavitev komunikacije s strani gostitelja v notranjem omrežju z zunanjim internetnim virom (npr. spletnim strežnikom), si NAT-PT naprava v svojo tabelo zapiše izvorni IPv4 naslov, TCP/UDP vrata s katerega je prišla zahteva, sekvenčno TCP številko ter njeno razliko ter časovno oznako (IETF, 1994). V naslednjem koraku NAT v prejetem paketu zamenja zasebni IPv4 naslov z javnim, zamenja številko vrat ter ponovno izračuna kontrolno vsoto (angl. Checksum) IP in TCP glave. Namreč, če želimo spreminjati IP naslov (iz zasebnega v javnega), mora usmerjevalnik poleg tabele povezav ponovno tudi izračunati kontrolno vsoto IP in TCP glave ter popravljeno vrednost vstaviti v nov paket. Pri

odzivu strežnika na zahtevo, NAT izvede obratni postopek: zamenja javni naslov v privatnega, zamenja številko vrat, izračuna kontrolno vsoto, popravi sekvenčno številko ter paket usmeri računalniku v zasebno omrežje. Strežnik v javnem omrežju notranjih naslovov ne pozna, saj komunicira samo z NAT napravo, ki ima javni IP naslov, ki je dodeljena (statično ali preko DHCP strežnika) s strani internetnega ponudnika (ISP), ki zasebnemu omrežju zagotavlja povezljivost v Internet.

Poznamo več izvedb prevajanja IP, TCP/UDP glav, ki so uporabni pri različnih aplikacijah. Ker ima vsaka aplikacija svoje specifike, morajo praviloma NAT naprave podpirati vsaj naslednje karakteristike prevajanja (RFC2663):

- Transparentno dodeljevanje naslovov (angl. Transparent Address assignment),
  - Statično dodeljevanje naslovov (angl. Static Address assignment),
  - Dinamično dodeljevanje naslovov (angl. Dynamic Address assignment),
- Transparentno usmerjenje (angl. Transparent routing),
- Prevajanje ICMP paketov (angl. ICMP error packet translation).

Pri transparentnem dodeljevanju naslovov NAT vzpostavi relacijo (angl. Bind) med zasebnimi naslovi in javnimi ter obratno, pri čemer omogoča transparentno usmerjanje datagramov, ki prehajajo med obema naslovnima področjema. Pri povezovanju IP naslovov (zasebni, javni) lahko v nekaterih primerih naprednejši NAT mehanizem upošteva tudi t.i. transportne identifikatorje, kot so številka TCP/UDP vrat in ICMP identifikatorjev poizvedb (angl. Queery identifiers). Mehanizem, ki omogoča tudi prevajanje transportnih identifikatorjev, je bil predstavljen leta 1999 z internetnim osnutkom RFC 2663. Omenjeni translacijski mehanizem so poimenovali Network Address Port Translation (NAPT), v literaturi zasledimo tudi imena kot so Port Address Translation (PAT) ali maskiranje (angl. Masquerading).
Pri statičnem dodeljevanju imamo direktno mapiranje en IP naslov iz zasebnega omrežja v en javni IP naslov, ki velja samo za čas NAT operacije. Pri dinamičnem dodeljevanju se nabor dodeljenih javnih IP naslovov dinamično dodeljujejo omrežju zasebnih naprav. Ko se posamezna seja zaključi, je porabljen javni IP naslov razpoložljiv za druge računalnike iz zasebnega omrežja.
Pri transparentnem usmerjanju je NAT usmerjevalnik nameščen na robu med dvema različnima IP naslovnima shemama in prevaja IP naslove v glavi IP paketa, tako, da so paketi pravilno usmerjeni v pravo omrežje. Ker ima NAT naprava povezave z večjim številom naslovnih področij (angl. Realm), mora pravilno prenašati informacije o omrežjih (npr. usmerjevalne protokole) iz ene naslovne sheme (področja) v drugo. V nasprotnem je oglaševanje usmerjevalnih informacij nesprejemljivo.
Če med dvema naslovnima področjema uporabljamo NAT napravo, moramo tudi transparentno spreminjati tudi ICMP pakete, ki nosijo informacije in obvestila o uspešnosti/neuspešnosti komunikacije (npr. ciljni naslov je nedosegljiv, čas je potekel, problemi parametrov). Spremembe v ICMP paketih vključujejo tudi spremembe originalnega IP paketa in njegove koristne vsebine (ICMP), ki nosi informacije o napakah.

Značilno za NAPT mehanizem je, da uporablja multipleksirano dinamično tabelo. Zaradi prevajanja transportnih identifikatorjev lahko večje število računalnikov v zasebnem omrežju uporablja za izhod proti javnemu omrežju samo en IP naslov. Zaradi prevajanja transportnih identifikatorjev imamo lahko na usmerjevalniku na zunanjem vmesniku samo en javni IP naslov, ob translaciji pa računalniki iz notranjega (zasebnega) omrežja poleg zamenjanega IP naslova (zasebni v javni IPv4) dinamično dobijo dodeljeno tudi številko TCP/UDP vrat, s katero se računalnik predstavlja v globalnem internetu.
NAPT je v primerjavi z NAT bistveno bolj varen, saj zaradi spreminjanja transportnih identifikatorjev blokira dostop do katerihkoli notranjih vrat (portov) s strani zunanjega

gostitelja, kar je bila ključna pomanjkljivost mehanizma NAT. Praviloma vsi sodobni usmerjevalniki, ki izvajajo omenjeno translacijo uporabljajo mehanizem NAPT, vendar bomo izraz NAT v nadaljevanju obdržali, saj se je v svetu najbolj uveljavil.

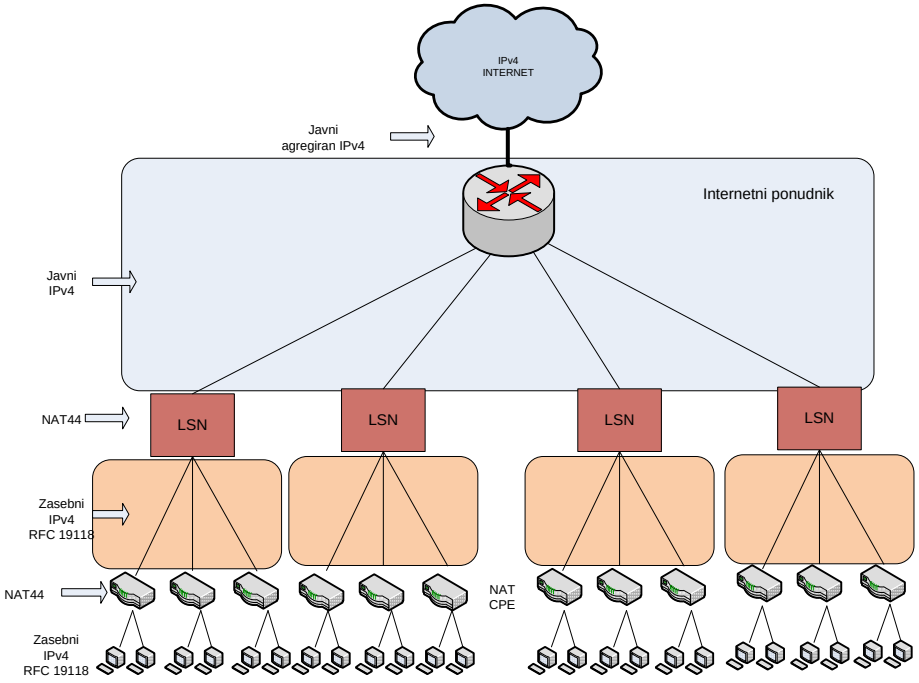
5.3.2 Large scale NAT (LSN)

V maju 2009 je bil s strani organizacije IETF objavljen internetni osnutek, imenovan Large Scale NAT (LSN). LSN, ki ga v literaturi zasledimo tudi pod imenom Carrier Grade NAT (CGN) ali Address Family Transition Routers (AFTR), podobno kot NAT izvaja translacijo IP naslovov ter TCP/UDP vrat, le da je ta naprava za razliko od NAT naprav, ki so nameščene pri končnih (rezidenčnih, poslovnih) uporabnikih, nameščena pri internetnemu ponudniku. Gre torej za izredno kompleksno in zmogljivo napravo, ki mora sočasno beležiti na tisoče hkratnih sej in izvajati translacijo med notranjim in javnim internet omrežjem. IETF predlog LSN mehanizma predvideva tri različne koncepte translacije (IETF, 2009a):

- NAT 444
- DS-Lite (NAT 464)
- NAT 64

5.3.3 NAT 444

Slika 11 prikazuje konceptualni primer translacije z mehanizmom NAT444.



Slika 11: NAT444

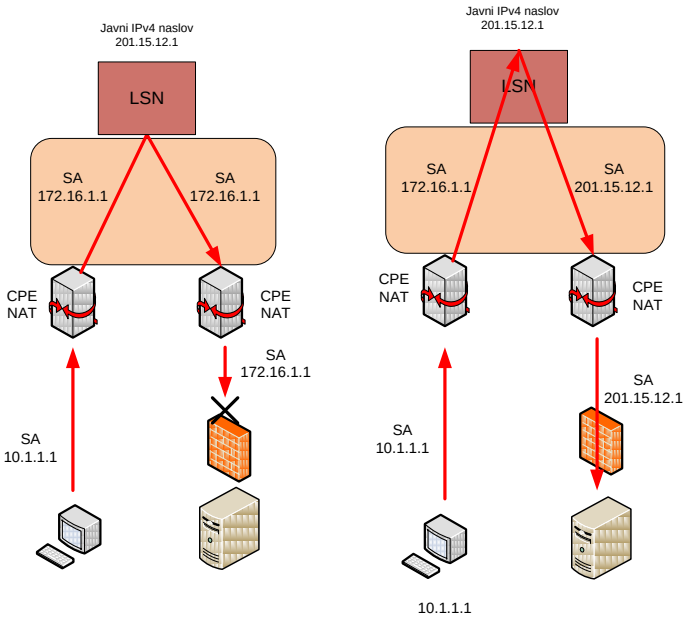
Internetni ponudnik ima s strani regionalnega ali lokalnega internetnega registrarja običajno rezerviran blok IPv4 javnih naslovov, ki jih dodeljuje naprej svojim (rezidenčnim, poslovnim) uporabnikom, strežnikom in usmerjevalnikom. Ponudnikov celotni dodeljeni nabor IPv4 naslovov se s pomočjo mehanizma imenovanega CIDR (angl. Classless Inter-Domain Routing) preko robnega usmerjevalnika proti zunanjemu internetu oglašuje in usmerja kot

ena agregirana usmerjevalna pot. Internetni ponudnik dodeljene javne IPv4 naslove nastavi na zunanje vmesnike LSN naprav v svojem omrežju. Med notranjimi vmesniki LSN naprav in zunanjimi vmesniki NAT naprav (rezidenčnih, poslovnih) uporabnikov se uporablja privatno omrežje, običajno iz bloka 17.16.0.0/12, znotraj omrežja uporabnika, pa se uporablja drug privatni naslovni prostor, tipično blok iz razreda A (10.0.0.0/8).
Ko uporabnik pošlje paket v javno omrežje, se njegov zasebni IP naslov (npr. 10.1.1.1/8) in številka vrat na NAT napravi preslika v drug IP naslov, ki je v drugem bloku in v drugo številko TCP/UDP vrat (npr. zasebni razred B, z IP številko 172.16.1.1/12). Ko paket prejme naprava LSN, se zopet izvede translacija IP naslova in vrat, tokrat v javni IP naslov, ki je dodeljen internetnemu ponudniku. Paket, ki kot odgovor iz javnega interneta pride na ponudnikov usmerjevalnik, se usmeri na LSN napravo (ki zopet izvede translacijo (IP naslova in vrat), ta pa jo posreduje naprej uporabnikovi NAT napravi, ki zopet izvede ustrezno translacijo. Usmerjanje paketov iz interneta proti uporabnikovem notranjem omrežju je odvisna vsaj od dveh stvari:

- seja, ki se začne na strani uporabnikovega omrežja mora imeti na strani NAT naprave uporabnika in na na strani LSN naprave pravilno mapiranje IP naslovov in vrat
- ter usmerjevalna pot gledano s strani javnega interneta mora biti unikatno identificirana.

Paket, ki prispe iz javnega interneta mora biti torej pravilno usmerjen na IPv4 (agregacijske) naslove, ki jih ima dodeljen internetni ponudnik. Ko je paket enkrat v omrežju ponudnika, se mora paket usmeriti na pravilen LSN (kar je običajno programski proces na robnem oziroma agregacijskem usmerjevalniku), kjer se izvede ustrezna translacija (naslovov, vrat) ter paket naprej posreduje na NAT napravo končnega uporabnika, kjer se je začela komunikacija. Translacija se v odvisnosti od smeri prometa (proti internetu ali proti uporabniku) za vsak paket izvede dvakrat: na strani uporabnikove NAT naprave in na strani LSN naprave internetnega ponudnika. Ker se v vseh primerih uporablja IPv4 naslove (javne, privatne) govorimo o NAT444. Opisan pristop je atraktiven, saj na strani NAT naprav končnih uporabnikov ni potrebe po zamenjavi opreme, saj je za napravo vseeno ali je na zunanjem vmesniku javni ali zasebni IPv4 naslov.
Ima pa opisan pristop tudi negativno konotacijo. Ena od pomanjkljivosti opisane arhitekture in LSN rešitev nasploh je razširljivost. Za vsakega internetnega ponudnika omrežje končnega uporabnika lahko predstavlja ogromno število naprav, ki se povezujejo na svojo NAT napravo. Vsaka od teh končnih naprav lahko proizvaja množico sej. Ker NAT444 obstaja šele zelo kratek čas, je izredno težko napovedati koliko omrežij in koliko končnih uporabnikov lahko posamezni LSN sočasno obdela, ne da bi prihajalo do zastojev ali prekinjanja povezav.
Drugi problem, ki ga ta rešitev prinaša, je tudi nastavljanje zasebnih IPv4 naslovov. Če omrežje ni pravilno konfigurirano, lahko prihaja do podvajanja IP naslovov. Lahko se namreč zgodi, da internetni ponudnik med LSN in NAT napravo uporablja enak naslovni blok, kot se ga uporablja v končnem zasebnem omrežju uporabnika. V tem primeru bodo vsi paketi izgubljeni. Zagotavljanje, da bo uporabnik uporabljal blok IP naslovov, ki ni v konfliktu s ponudnikovim lahko povzroča velike administrativne težave.
Problem, ki se tudi izpostavlja z NAT444 arhitekturo je tudi usmerjanje prometa med dvema ali več omrežji, ki sta povezani na isto LSN napravo. Ko npr. želi uporabnik iz enega zasebnega omrežja poslati paket drugemu uporabniku, ki je v drugem omrežju in ki je povezan v isto LSN napravo bodo požarne pregrade paket blokirale, saj se po omenjenem pravilu (RFC 1918) zasebnih naslovov ne sme usmerjati izven zasebnega omrežja. Da se izognemo temu problemu se morajo paketi najprej usmeriti na zunanji vmesnik LSN naprave, kjer paket dobi javni naslov ter nato zopet usmeriti nazaj v drugo zasebno omrežje. V kolikor je teh primerov veliko, kaj kmalu lahko pridemo do situacije, da porabimo ves razpoložljivi javni IPv4 naslovni prostor, ne da bi promet odšel v javni internet.

Slika 12 nam prikazuje situacijo, kjer zaradi nastavljenega pravila požarna pregrada blokira vhodni promet iz IP rezerviranih naslovov.

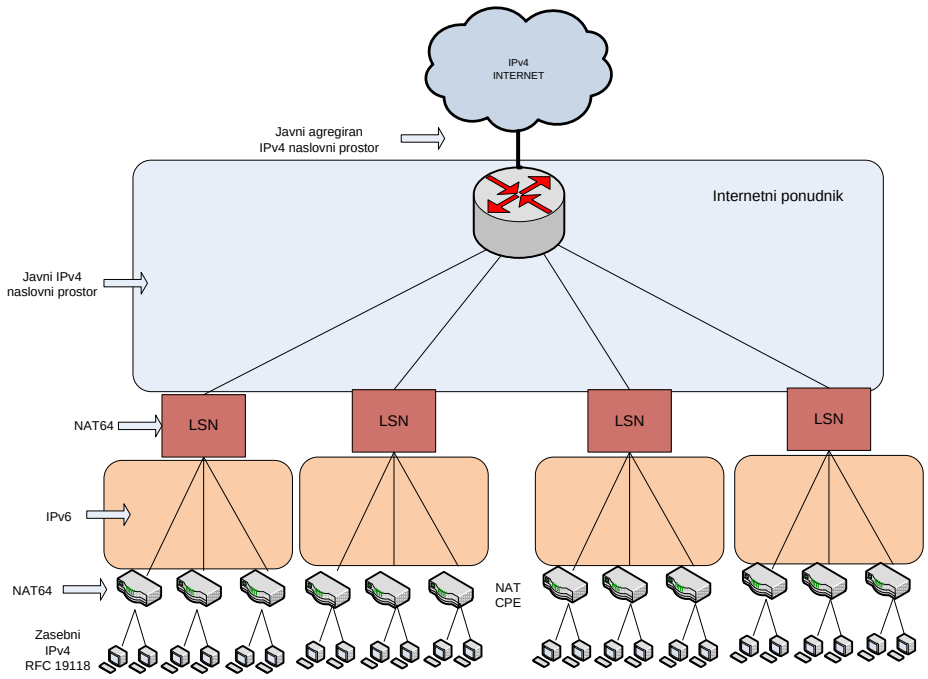


Slika 12: Blokiranje RFC 1918 naslovov

Predlagana rešitev k temu problemu je tudi, da bil se del preostalih javnih IPv4 naslovov rezerviralo kot skupna raba, ki se lahko uporablja na posamezni LSN napravi (podobno kot so rezervirani zasebni naslovi v RFC 1918), internetni ponudnik pa jih nato dinamično dodeljuje posameznim sejam glede na zahteve, ki prihajajo iz notranjih omrežij. To je trenutno le predlagana rešitev (IETF, 2009d), saj ni bil rezerviran še noben blok naslovov iz naslovne sheme IPv4.

5.3.4 NAT 464

Rešitev za problem usmerjanja paketov med dvema ali več zasebnimi omrežji skozi isto LSN napravo nam ponuja arhitektura NAT464, ki je prikazana na sliki 13.



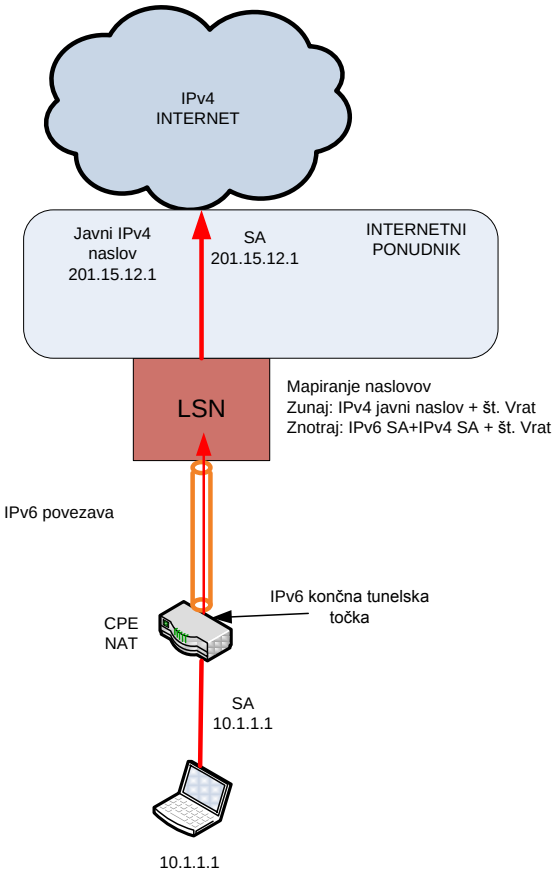
Slika 13: NAT464

Ideja ni nova, saj je bil podoben translacijski mehanizem NAT-PT (angl. NAT-Protocol Translation), ki omogoča prevajanje naslovov iz IPv4 v IPv6 predstavljen že leta 2000 v RFC 2766, vendar zaradi določenih njegovih pomanjkljivosti ni bil sprejet. NAT64 mehanizem, ki je njegov naslednik omogoča podobno funkcionalnost, prevajanje IPv6 v IPv4 in obratno, vendar je bistveno bolj izpopolnjen (IETF, 2009c). DNS64, ki mehanizmu NAT64 pri translaciji pomaga, sintetizira iz A zapisa v DNS strežniku, AAAA zapis. Oba mehanizma tako omogočata, da odjemalec, ki uporablja izključno IPv6 protokol lahko vzpostavi komunikacijo z IPv4 strežniki ter tudi omogoča, da se vzpostavi direktna komunikacija med čistim IPv6 in IPv4 odjemalcem. Omenjena translacija se izvaja s pomočjo translacijskega algoritma, ki omogoča translacijo IP/ICMP glav (IETF, 2009b). NAT64 in DNS64 je po mnenju njegovih razvijalcev enostavno implementirati, saj ni potrebnih sprememb ne na IPv6 odjemalcih, ne na IPv4 strežnikih. Za osnovno funkcionalnost, moramo NAT64 funkcijo implementirati le v napravi, ki povezuje oba (čista) omrežja (IPv6 in IPv4), vključno z implementacijo DNS64 funkcionalnosti na DNS strežniku, ki je nameščen v IPv6 omrežju. V arhitekturi NAT464 se torej uporablja omenjeni translacijski mehanizem.
NAT464 uporablja med LSN napravo in končno NAT napravo uporabnikov (samo) protokol IPv6, med notranjim zasebnim omrežjem in NAT napravo ter med LSN napravo in javnim omrežjem pa izvaja translacijo med obema protokoloma. IPv4 paketi, ki prihajajo iz zasebnega omrežja uporabnikov se na NAT napravi prevedejo (translirajo) v IPv6 pakete. Ti se nato usmerijo do LSN naprave, ki izvede translacijo iz IPv6 na javno dodeljen IPv4 naslov. Pri tem ni možnosti, da bi prišlo do konfliktov med IPv6 naslovi na zunanji strani NAT naprav in IPv4 naslovi na notranji, zasebni strani omrežja. Ker je med LSN napravo in NAT napravo uporabnikov že čisti IPv6 protokol, smo že tudi bližje končni migraciji, to je neoporečnim (čistim) IPv6 omrežju. Predlagana rešitev pa ima v tem trenutku tudi slabe strani. Kjer NAT464 poenostavlja vmesno cono med LSN in NAT, sta pri tem najbolj problematična tako LSN in NAT naprava sama, saj morata izvajati prevajanje iz IPv4 v IPv6 in obratno. Trenutno je na trgu zelo malo NAT64 naprav, poleg tega pa za to internetne ponudnike predstavlja

nemajhen strošek. Prevajanje med dvema različnima naslovoma (IPv6 in IPv4) je v primerjavi z translacijo NAT44 izredno kompleksen in zamuden postopek, kar je tudi razlog, da se ni tako razširil kot rešitve tipa NAT44. NAT64 se bo vsekakor še izpopolnjeval, vendar ni za pričakovati, da bo tako učinkovit kot NAT44.

5.3.5 Dual Stack Lite

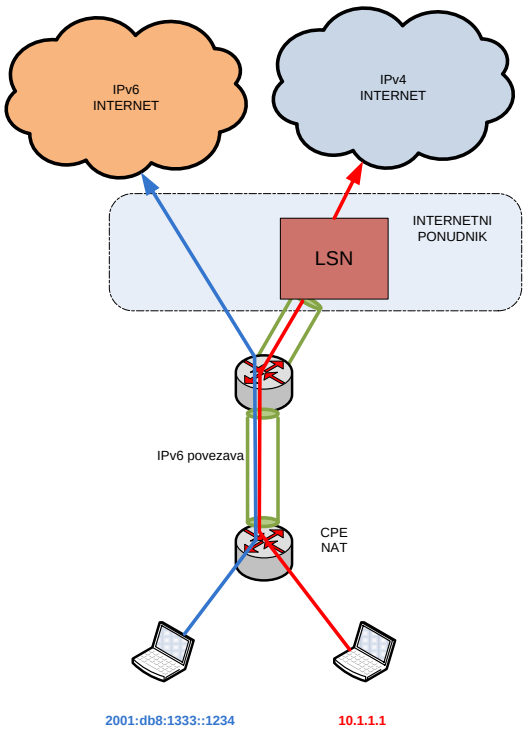
Dual Stack Lite model je leta 2008 kot internetni osnutek predstavil Alain Durand iz podjetja Comcast. Comcast je sicer največji kabelski operater v ZDA, ki zagotavlja širokopasovni internet, televizijo in storitve telefonije tako za rezidenčne kot poslovne uporabnike. Kot operater z 20 milijoni uporabnikov širokopasovnega interneta ima zaradi pomanjkanja IPv4 naslovnega prostora zato velik interes za uvedbo IPv6 protokola. Trenutni osnutek je v veljavi do aprila 2010 (IETF, 2009f). Dual-Stack Lite je bistveno boljši pristop kot NAT464, saj izkorišča prednosti NAT464 in obenem zmanjšuje njegove probleme. Dual Stack-Lite uporablja IPv6 povezave med ponudnikom in uporabnikom, toda ne izvaja NAT64 translacije. Ko uporabniška naprava (CPE-Customer Promise Equipment) v zasebnem omrežju pošlje IPv4 paket v internet, se ta paket za potrebe transporta do LSN naprave ovije v IPv6 paket, LSN naprava paket dekapsulira in izvede translacijo NAT44. Tuneliranje IPv4 čez IPv6 je enostavnejši in učinkovitejši način kot translacija, saj ni vprašljiva učinkovitost in redundačnost, kar je bil problem pri mehanizmu NAT464. Slika 14 nam prikazuje arhitekturo Dual Stack Lite, kjer so IPv4 paketi od CPE naprave do LSN naprave tunelirani skozi IPv6 tunel.



Slika 14: Dual-Stack Lite

Pri tej arhitekturi moramo dodati dodaten element na strani LSN naprave, ki bo izvajala mapiranje med IPv6 paketom, ki nosi informacijo o IPv4 paketu in uporabljenimi TCP/UDP vrati ter izhodnim IPv4 paketu, ki se usmeri proti internetu. Ker je vsak prihajajoč paket z IPv6 naslovom na LSN napravo unikaten za vsakega uporabnika (kombinacija IPv6 izvorni naslov+IPv4 izvorni naslov+vrata TCP/UDP protokola) lahko učinkovito izvajamo diferenciacijo med različnimi sejami in uporabniki. Ko LSN naprava iz Interneta dobi povratni IPv4 paket, pogleda v svojo mapirno tabelo, kjer dobi IPv4 naslov končnega uporabnika, zamenja številko vrat, ovije paket v IPv6 ter ga posreduje v ciljno uporabnikovo omrežje. Z drugimi besedami, mapiran IPv6 naslov, ne razlikuje samo uporabnikovo zasebno omrežje, temveč tudi zagotavlja referenco na končno tunelsko točko.
Ker predpostavljamo, da je v zasebnem uporabniškem omrežju različno število končnih računalnikov, ki uporabljajo eden ali oba IP protokola (dvojni sklad), se mora DS Lite funkcionalnost izvajati na robnem usmerjevalniku zasebnega omrežja. Če uporabnik pošlje IPv6 paket, se paket transparentno usmeri na LSN napravo, v kolikor pa robna naprava uporabniškega omrežja prejme IPv4 paket, potem mora izvesti IPv4-IPv6 ovijanje ter paket posredovati naprej na LSN. Slabost, ki jo prinaša DS Lite, je zamenjava ali nadgradnja uporabniškega robnega usmerjevalnika (CPE), kar prinaša določene stroške internetnemu ponudniku. Internetni ponudniki so velikokrat nenaklonjeni temu, da bi nadlegovali svoje uporabnike, poleg tega zamenjava opreme predstavlja strošek in logističen problem (zamenjava in konfiguracija naprave). Iz tega razloga je tudi za pričakovati, da v kolikor se bodo internetni ponudniki odločali za implementacijo DS Lite tehnologijo, jo bodo verjetno najprej implementirali pri svojih novih uporabnikih, obstoječi CPE-ji, pri nezahtevnih naročnikih pa se bodo zamenjevali v skladu z amortizacijskem načrtom.

Drug Dual Stack Lite model, kot ga prikazuje slika 15 ne vpeljuje DS Lite funkcionalnost na strani robnih naprav zasebnih omrežij, temveč na strani končnih individualnih naprav.



Slika 15: Dual-Stack Lite z uporabo dveh protokolov

Ta naprava uporablja oba protokola (IPv6 in IPv4), tako, da lahko pošilja in sprejema IPv6 in IPv4 promet. Ta model je primeren tako za uporabnike, ki so z Internetom direktno povezani samo z enim namiznim računalnikom, igralno konzolo ali prenosnikom kot tudi ima velik potencial za mobilni širokopasovni Internet. Tudi mobilni operaterji širokopasovnega Interneta, predvsem z vpeljavo naslednika HSPA tehnologije, LTE (angl. Long Term Evolution) bodo za svoje pametne mobilne terminale, ki bodo uporabljali IPv6 protokol potrebovali povezljivost na IPv4 omrežja, kjer se bo še nahajala spletna vsebina in storitve.

5.3.6 A+P Addressing and forwarding

Mehanizem A+P je še en primer internetnega osnutka, ki je nastal kot posledica pomanjkanja IPv4 naslovnega polja in počasnega uveljavljanja IPv6 protokola. Trenutno je A+P že dobil strateško dovolj močno pozicijo, da bo mogoče v okviru organizacije IETF organizirana samostojna delovna skupina. Predlagatelj A+P mehanizma je Randy Bush, kot soavtor na delu, ki obravnava signalizacijo pa sodeluje tudi slovenski strokovnjak Jan Žorž, ki je tudi eden od ustanoviteljev slovenskega Zavoda go6, ki je slovenska iniciativa za prehod na IPv6. A+P je v določenih elementih podoben mehanizmu DS Lite, saj so razlike bolj kot ne v mestu NAT-a in dodeljevanja vrat.

Osnovna ideja A+P mehanizma je, da omogoča souporabo IPv4 naslovov, na način, da se določeni biti, ki opredeljujejo številko vrat v TCP/UDP glavi protokola, dodajo obstoječemu IPv4 naslovu kot podaljšek (Address+Port; A+P), pri čemer se aplikacijam zmanjša nabor možnih vrat, ki jih lahko naslavljajo. Predlagana rešitev tako omogoča dodeljevanje enakih IPv4 naslovov različnim napravam, pri čemer vsaka aplikacija, ki teče na napravi lahko uporablja (odpira) samo omejeni nabor vrat (portov) za komuniciranje z drugo napravo. TCP ali UDP glava transportnega protokola poleg ostalih polj vsebuje tudi 16 bitno polje, ki opredeljuje izvorna in ciljna vrata (angl. Source/Destination Port) preko katerih lahko dve napravi (aplikaciji) komunicirata. Z obstoječim TCP/UDP protokolom lahko tako naslavljamo 2^{16} oziroma 65535 komunikacijskih vrat. Številke vrat so razdeljene na tri območja (IANA, 2009):

- številke vrat od 0 do 1023 so t.i. dobra znana vrata (angl. Well Known Ports), ki se jih lahko uporablja izključno za sistemske procese ali programske ukaze s strani privilegiranih uporabnikov,
- številke vrat od 1024 do 49151 so t.i. registrirana vrata, ki jih na večini operacijskih sistemov lahko uporabljajo običajni uporabniški procesi ali programi, ki jih poganjajo navadni (nepriviligirani) uporabniki,
- številke vrat od 49152 do 65535 so t.i. dinamična vrata ali zasebna vrata, ki jih lahko uporabljajo katerekoli javno določene aplikacije.

Prednost podaljšanega naslavljanja (A+P) je ohranjanje komunikacije od konca do konca (angl. End-to-end), za razliko od NAT naprav, ki to komunikacijo prekinjajo. Avtorji A+P zagovarjajo tezo, da je bil Internet zasnovan za komunikacijo od konca do konca z hitrim posredovanjem paketov po jedru omrežja in pametnimi robnimi napravami brez vmesnih translacijskih mehanizmov, ki bi preoblikovali vsebino paketov. Z implementacijo različnih oblik NAT naprav se v omrežje dodaja dodatna kompleksnost, ki omejuje, upočasnjuje in spreminja komunikacijo med končnimi točkami. Današnje NAT naprave, ki vse bolj delujejo kot prehod v aplikacijskem sloju (angl. Application Layer Gateway) po mnenju avtorjev ne bodo delovale z CGN/LSN napravami internetnega ponudnika. CGN pristop velikih NAT translatorjev na strani internetnega ponudnika dodaja pregrado, nad katero ima nadzor samo internetni ponudnik, ne pa tudi uporabnik. Vprašljiva je tudi uporaba novih aplikacij, ki so

nameščene in uporabljene na strani uporabnikov, saj so lahko na strani CGN naprav blokirane. CGN naprave lahko tudi postanejo kritična točka odpovedi, obenem pa je tudi vprašljiva njihova razširljivost.

6 Infrastrukturne spremembe ob prehodu na IPv6

IPv6 je končni cilj in obenem tudi potencialna rešitev na pomanjkanje IPv4 naslovnega prostora. Glavna motivacija operaterjev in ponudnikov internetnih storitev mora biti zagotovitev in omogočanje IPv6 povezljivosti in storitev. Kljub vsemu bodo operaterji in ISP-ji motivirani tudi z ostalimi prednostmi, ki jih prinaša IPv6. To je predvsem večji javni naslovni prostor, ki ga bodo sedaj lahko ponudili tudi končnim uporabnikom, nižji operativni stroški, ki jih prinašajo čista IPv6 omrežja, mobilnost, povezljivost od konca do konca, večja varnost, številne nove aplikacije, večja kvaliteta storitev ali število drugih prednosti za katere bi bil IPv6 rešitev. Spremembe se bodo pojavile tudi v tehnologiji, ki je danes še zelo redka ali pa je šele v razvojni fazi. Pričakujemo lahko porast IP terminalov, ki bodo komunicirale s svojim lastnim unikatnim globalnim IP (IPv6) naslovom. Terminali bodo imeli povezljivost z brezžičnimi omrežji (še posebej z WLAN), omogočali bodo hiter prenos podatkov in hiter dostop do Internetnih storitev. Zaradi povezljivosti od konca do konca, bomo imeli še večjo izbiro aplikacij tipa vsak z vsakim (P2P), ki bodo temeljile na IP-ju (telefonija, video konference, storitve na zahtevo). Uspešnost razvoja novih aplikacij, ki bodo prinašale dodano vrednost poslovnim in rezidenčnim uporabnikom je tako v veliki meri pogojeno s ponudbo hitrega širokopasovnega IPv6 dostopa. V vsakem primeru bo moral vsak operater in ISP posodobiti svoje omrežje z IPv6 povezljivostjo, ne da bi prekinil povezljivosti in storitve, ki so vezane na IPv4. Scenarij prehoda mora torej upoštevati koeksistenco obeh protokolov. Ponudniki Interneta bodo morali imeti mehanizem, ki bo omogočal transparenten prehod uporabnikov z uporabe IPv4 aplikacij na IPv6 aplikacije in kapacitete, ki bo omogočale razvoj novih aplikacij, novih terminalov in pripadajočih sprotnih (angl. Online) storitev.

Prvo kar se lahko vprašamo je: "Kateri problem bi radi rešili z uvedbo IPv6?" Je to pomanjkanje naslovnega prostora. Kaj moramo torej storiti, da lahko uvedemo IPv6 v svoja omrežja?

Naj naštejemo samo nekaj vprašanj, na katera moramo najprej dobiti odgovore:

- Koliko obstoječe strojne in programske opreme ter storitev moramo zamenjati ali nadgraditi, da bo omogočena podpora za IPv6?
- Na katere dele našega sistema bo IPv6 še vplival?
- Ali potrebujemo kakšno dodatno strojno ali programsko opremo, ki bo potrebna samo za IPv6 podporo?
- Kdo od ponudnikov internetnega tranzita, 'peering' partnerjev ali ponudnikov internetnih storitev nam trenutno omogoča tudi IPv6 povezljivost. Kakšen dogovor o nivoju storitev lahko dosežemo ter za kakšno ceno? Ali moramo s IPv6 povezljivostjo spremeniti, nadgraditi ali na novo vzpostaviti pogodbe?
- Kakšno je tveganje in koliko časa potrebujemo za izvedbo?
- Kakšno je naše trenutno znanje in usposobljenost naših inženirjev in drugega osebja?

Da dobimo ustrezne podatke, moramo izvesti študijo izvedljivosti, ki nam bo podala oceno potrebnih sprememb, tveganja, stroškov in potrebnega časa za izvedbo tranzicije. Šele, ko je študija narejena in imamo vse potrebne informacije, se lahko odločamo kateri scenarij prehoda je za naše razmere najugodnejši. Študija mora vsebovati vse potrebne projektne faze ter mejnike, kjer bomo preverjali, če so posamezne faze izvedene ter ali so pravilno izvedene in ali so stroški v pričakovanih mejah. Če bomo pravilno načrtovali ter predvidevali

vse možne posledice, imamo pod nadzorom stroške, tveganje pa minimiziramo. Uvedba mora biti čim bolj transparentna in neboleča za končne uporabnike. V kolikor bomo morali menjati opremo, moramo natančno preveriti ali izbrani ponudniki izpolnjujejo vse naše zahteve, ali je oprema skladna s standardi, kompatibilna z opremo drugih ponudnikov ter, ali jo je možno nadgraditi z bodočimi novimi funkcionalnostmi. Potrebno je narediti načrt aktivnosti potrebnega izobraževanja za omrežne arhitekte, omrežne administratorje in management.

Pomemben del projekta, je priprava celovitega popisa strojne in programske opreme ter storitev na katere bi lahko prehod na IPv6 vplival.

Popis mora med drugim vključevati stanje:

- Usmerjevalnikov in L3 stikal (usmerjevalniki in L3 stikala morajo znati procesirati oba tipa glav IPv4 in IPv6),
- Varnostnih sistemov (požarne pregrade, proxy strežniki, IDS/IPS sistemi). Varnostni sistemi morajo prepoznati in ustrezno pravilno prepuščati/blokirati obe vrsti prometa (IPv4 in IPv6) ter ostale protokole,
- DNS (DNS mora biti konfiguriran da posluša in odgovarja na IPv6 naslove in domenska imena),
- DHCP (DHCPv6 strežnik mora vozliščem in gostiteljem nadzorovano dodeljevati vse mrežne parametre in druge informacije),
- Operacijskih sistemov (operacijski sistemi morajo delovati na obeh skladih IPv4 in IPv6),
- Podpornih sistemov za nadzor in obračunavanje (OSS/BSS - AAA mora podpirati IPv6, zakonito prestrezanje…)
- Podpornih sistemov za nadzor in upravljanje omrežja,
- Strežnikov, ki zagotavljajo storitve,
- Aplikacij in storitev (aplikacije in storitve morajo biti neodvisne od uporabljene verzije IP protokola),
- Programske knjižnice (knjižnice mora uporabljati kompatibilne IPv6 sistemske klice)
- Naprav končnih uporabnikov (STB, RG usmerjevalniki, VoIP terminali).

Internetni ponudniki in operaterji morajo posebno posvetiti tudi IT sistemom, ki omogočajo nadzor omrežja, oskrbovanje, obračunavanje, administracijo in vzdrževanje. Omenjeni sistemi, sicer velikokrat niso predmet obravnave v okviru prehoda na IPv6, vendar so nujno potrebni za zagotavljanja brezhibnega delovanja omrežja. Pri nakupu nove strojne ali programske opreme mora biti tudi zavedanje, da mora oprema podpirati tako IPv4 kot IPv6 protokolni sklad (IPv6 Ready[2]).

6.1 Hrbtenična omrežja

Kako bomo IPv6 uvedli in na katerih delih omrežja, je odvisno od izbrane metodologije. Oba največja proizvajalca mrežne opreme tako Juniper kot Cisco priporočata svojim strankam, da

[2] Ameriški NIST ima objavljen popis zahtev, ki jih izpolnjujejo IPv6 sposobni izdelki (IPv6 Capable Products): http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_product_profile_v4.pdf

se IPv6 protokol uvede najprej v jedru omrežja, šele nato pa v agregacijskem in dostopovnem omrežju.
Hrbteničnо ali jedrno omrežje sestavljajo: visoko zmogljivi in inteligentni robni usmerjevalniki (angl. PE-Provider Edge), ki povezujejo dostopovno/agregacijsko omrežje z jedrom omrežja, sami jedrni usmerjevalniki, ki povezujejo robne PE usmerjevalnike ter vročilne točke, kjer se izvaja avtorizacija/avtentikacija uporabnikov ter ponuja storitve (IPTV, VoIP, DNS..). Del hrbteničnega omrežja so tudi mejni (angl. Border) usmerjevalniki s katerimi se posamezni operater povezuje z drugimi internetnim ponudniki (angl. Peering) ter ponudniki tranzita (angl. Upstream providers). Povezljivost z drugimi operaterji in ponudniki interneta (angl. Peering) se izvaja preko internetnih izmenjevalnih točk (angl. Internet Exchange Points-IX), ki povezujejo različne avtonomne sisteme in usmerjevalne BGP poti. V Sloveniji imamo dve taki točki, in sicer: SIX (angl. Slovenian Internet Exchange) ter LIX (angl. Ljubljana Internet Exchange). SIX, ki je pod upravljanjem Arnesa na podlagi dogovora vsem svojim članom omogoča 10Gbit/s medoperaterske povezave in brezplačno izmenjavo tako IPv4, kot tudi IPv6 lokalnega prometa.
Ker so jedrni usmerjevalniki običajno najzmogljivejši in najsodobnejši del omrežja, je na njih najlaže uvesti IPv6. Ker gre za relativno manjše število naprav so operativni stroški izvedbe implementacije IPv6 v primerjavi z drugimi deli omrežja najmanjši.
Obstaja več različnih pristopov, ki omogočajo vpeljavo IPv6 preko jedrnega omrežja operaterja. V literaturi zasledimo naslednje pristope uvedbe IPv6 v hrbteničnem omrežju:

- Tuneliranje (IPv6 čez IPv4, L2 tuneli čez IPv4),
- postopna nadgradnja vseh jedrnih usmerjevalnikov na dvojni sklad (angl. Dual Stack),
- paralelno IPv6 omrežje z IPv6 usmerjevalniki,
- IPv6 čez MPLS,
- IPv6 jedrno omrežje.

6.1.1 Tuneliranje

Najlažji in najhitrejši način uvedbe IPv6 v hrbteničnem delu omrežja je uporaba tehnike tuneliranja IPv6 prometa čez obstoječe IPv4 omrežje. Pri tem izkoriščamo obstoječo IPv4 omrežno usmerjevalno topologijo in zmogljivosti usmerjevalnikov. Z večanjem IPv6 prometa, moramo tunelske mehanizme nadomestiti bodisi z dvojnim skladom, vzpostavitvijo paralelnega omrežja, bodisi, če imamo možnost, uporabimo obstoječe IP/MPLS omrežje.

6.1.2 Dvojni sklad

Z večanjem IPv6 prometa, moramo obstoječe usmerjevalnike postopoma nadgraditi tudi z IPv6 protokolnim skladom (angl. Dual stack). Nadgradnja na IPv6 je lahko v začetku izvedena samo programsko, vendar na daljši rok, še posebej s povečanjem IPv6 prometa, je strojni način procesiranja prometa obvezujoč. Odločiti se tudi moramo, kateri usmerjevalni protokol je za naše omrežje najbolj primeren in kakšno usmerjevalno politiko bomo imeli. V arhitekturi dvojnega sklada, mora usmerjevalnik vzdrževati obe usmerjevalni tabeli, eno za IPv4 in drugo za IPv6 promet. Pomembno vprašanje, ki se pri tem poraja je, ali naj vzdržujemo ločena usmerjevalna procesa za vsak IP protokol (IPv4 in IPv6). Ločena procesa nam povečujeta režijo, toda zagotavljata večjo prožnost in stabilnost med IPv4 in IPv6. V kolikor uporabljamo usmerjevalna protokola OSPF in IS-IS, imamo na razpolago naslednje možnosti[3]:

[3] 6NET: http://www.6net.org/publications/deliverables/D4.6.1.pdf

- OSFPv2 za IPv4, IS-IS za IPv6,
- OSPFv2 za IPv4, OSPFv3 za IPv6,
- IS-IS za IPv4, OSPFv3 za IPv6,
- IS-IS za oba protokola IPv4 in IPv6 (isti proces),
- IS-IS z ločenimi procesi (vsak proces ima svojo instanco –podatkovno bazo za vsak protokol).

Pri Geant največjem evropskem raziskovalnem omrežju, katerega član je tudi slovenski Arnes, so se leta 2002, ko so izvajali prehod na IPv6 odločili, da bodo obstoječi usmerjevalni protokol OSPFv2 popolnoma odstranili z omrežja ter ga nadomestili s protokolom IS-IS. Prednost, ki so jo navedli v primerjavi z OSPFv3 (naslednik OSPFv2 protokola), da ima IS-IS samo eno bazo za katerikoli tip IP protokola, je nevtralen glede na tip omrežnih naslovov, ki jih mora usmerjati, je fleksibilen, v primerjavi z OSPF podpira večje število usmerjevalnikov na posameznem področju (angl. Area), dobavitelji pa na tem protokolu prvo uvedejo zadnje novosti in naprednejše funkcije. IS-IS se hitreje prilagodi, da podpira IPv6, medtem, ko OSPF zahteva temeljito preučitev vseh možnih vplivov.

Prehod na dvojni sklad v hrbteničnem omrežju bi moral vključevati naslednje korake:

- z namenom pridobitve izkušenj delovanja IPv6, moramo kreirati in vzpostaviti testno omrežje s tuneliranimi IPv4 povezavami,
- v testnem okolju vrednotimo verzije programske opreme usmerjevalnikov. Poskušamo ugotoviti, katera verzija je stabilna in dovolj robustna, da se jo lahko uporabi tudi v produkcijskem IPv4/IPv6 omrežju. Spremljati moramo vpliv IPv6 na delovanje obstoječih IPv4 storitev,
- če je okolje stabilno, začnemo s postopno nadgradnjo usmerjevalnikov na dvojni sklad (IPv4/IPv6). Običajno se omrežna topologija ne spreminja (ostane enaka kot pri IPv4), čeprav je lahko prehod na IPv6 tudi razlog (vzrok), da omrežje načrtujemo sedaj bolj optimalno,
- če imamo probleme (npr. programski hrošči v OS usmerjevalnika, ki vplivajo na produkcijske storitve) jih poskušamo poiskati, izolirati od ostalega okolja ter odpraviti oziroma v najslabšem primeru preiti nazaj na IPv4.

Prednost delovanja dvojnega sklada nam omogoča, da imamo omrežje, ki je enotno, tako za IPv4 kot za IPv6. Ker so jedrni usmerjevalniki praviloma najsodobnejši del omrežja, praviloma vsi podpirajo IPv6 protokolni sklad, zato ni potrebe po nakupu novih. Ni pa seveda to pravilo. Pri tem tudi nimamo potrebe po vzdrževanju potencialnega kompleksnega prekrivnega omrežja. Vendar, če imamo enotno omrežje, nam to po drugi strani (še posebej v primeru programskih hroščev) lahko vpliva tudi na delovanje obstoječih IPv4 storitev, kar se nam v primeru ločenega omrežja ne more zgoditi. V kolikor tudi nimamo zmogljivih sodobnih usmerjevalnikov (npr. IPv4 usmerjevalnik obdeluje strojno, IPv6 programsko), se lahko to kaže v slabši učinkovitosti/prepustnosti omrežja. V tem primeru so lahko začetna paralelna testna omrežja zanesljivejša, vendar vsaj v začetku tudi dražja izbira.

6.1.3 Paralelno IPv4 in IPv6 omrežje

Ena od alternativ, je tudi vzpostavitev paralelne IPv6 infrastrukture, kar je primer nemškega 6WiN hrbteničnega omrežja[4]. Paralelna infrastruktura lahko vključuje čisto ločene povezave, ali samo ločeno tuneliranje prometa čez obstoječe IPv4 povezave. Izbira med dvojnim skladom in paralelno infrastrukturo je pogojena z veliko kompromisi. Odločitev je pogojena s

[4] 6WiN: http://www.6win.de/

ceno strojne opreme, različno zmogljivostjo, omrežje je bodisi ločeno, bodisi skupno, razlike so v upravljanju. Končni cilj je vsekakor omrežje s samo IPv6 prometom, saj poenostavlja upravljanje in zmanjšuje stroške. V kolikor pa operater že uporablja omrežje, ki temelji na MPLS, lahko IPv6 promet peljemo tudi čez tako omrežje.

6.1.4 IP/MPLS

IP/MPLS (angl. IP Multiprotocol Label Switching) je zmogljiv komunikacijski mehanizem, ki omogoča prenos podatkov med različnimi omrežji. MPLS omogoča ponudnikom internetnih storitev prožno orodje, ki zagotavlja in podpira različne vrste storitve, zagotavlja kvaliteto storitev, aplikacij ter omogoča prometni inženiring. Zgodovinsko gledano se je MPLS razvil kot odgovor na IP/ATM integracijo, ki omogoča ločljivost posredovalnih funkcij od funkcije usmerjanja (IP glava) ter omogoča podporo različnim protokolom brez sprememb v funkciji posredovanja. Združuje najboljše lastnosti preklapljanja in usmerjanja obenem pa v nepovezavno usmerjen princip omrežja vpeljujejo povezavno usmerjenost. V klasičnem okolju usmerjanja se paketi posredujejo skozi različna omrežja s pomočjo različnih usmerjevalnih protokolov. Pri MPLS arhitekturi se paketi na MPLS usmerjevalnikih preklapljajo na podlagi algoritma zamenjave MPLS label. Če tehnologija povezavnega ali fizičnega sloja podpira labele (npr. ATM ali blokovno posredovanje) se MPLS labela ovije na mesto originalne labele. Če pa tehnologija povezavnega sloja ne podpira labele (npr. Ethernet) pa se MPLS glava vrine med glavo protokola povezavnega/fizičnega sloja in glavo IP protokola. Labela je kratek identifikator s fiksno dolžino in identificira ekvivalentni posredovalni razred (FEC), predstavlja pa skupino paketov, ki jih MPLS omrežje obravnava na enak način (Kos, Bešter, 2001). Arhitekturo MPLS omrežja sestavljajo robni LER (angl. Label Edge Router) usmerjevalniki, ki prispelim paketom na podlagi klasifikacije dodajo labele, izhodnim paketom pa labele odvzemajo ter jih posredujejo naprej proti ciljnemu omrežju na podlagi klasičnega usmerjanja (BGP, OSPF, IS-IS). Hrbtenični LSR (angl. Label Switching Router) oziroma P (angl. Provider) usmerjevalniki imajo samo nalogo, da glede na LFIB (angl. Label Forwarding information base) bazo, labele zamenjujejo, celotni paket pa brez dodatnega analiziranja posredujejo naprej naslednjemu MPLS usmerjevalniku.

V kolikor že imamo vzpostavljeno jedrno MPLS omrežje je priporočljivo, da MPLS infrastrukturo uporabimo tudi za prenos IPv6. Generalno gledano, obstaja kar nekaj načinov za prenos IPv6 prometa s pomočjo uporabe MPLS arhitekture. Našteli smo že našteli nekaj tunelskih mehanizmov, ki so transparentni za MPLS. Poleg tega obstaja še nekaj tranzicijskih mehanizmov, ki delno modificirajo obstoječe MPLS infrastrukturo. Idealen pristop z uporabo MPLS tehnologije je uvedba IPv6 usmerjanja in posredovanja in/ali uporaba signalizacije IPv6 LSP (angl. Label Switch Protocol) protokola v vsakem LSR (angl. Label Switch Router) usmerjevalniku. Drugi pristop uporablja MP-BGP tuneliranje s pomočjo katerega se IPv6 paketi usmerjajo čez IPv4 MPLS jedrno omrežje. In končno operaterji lahko tudi izvajajo tuneliranje v drugem sloju čez obstoječo MPLS infrastrukturo.

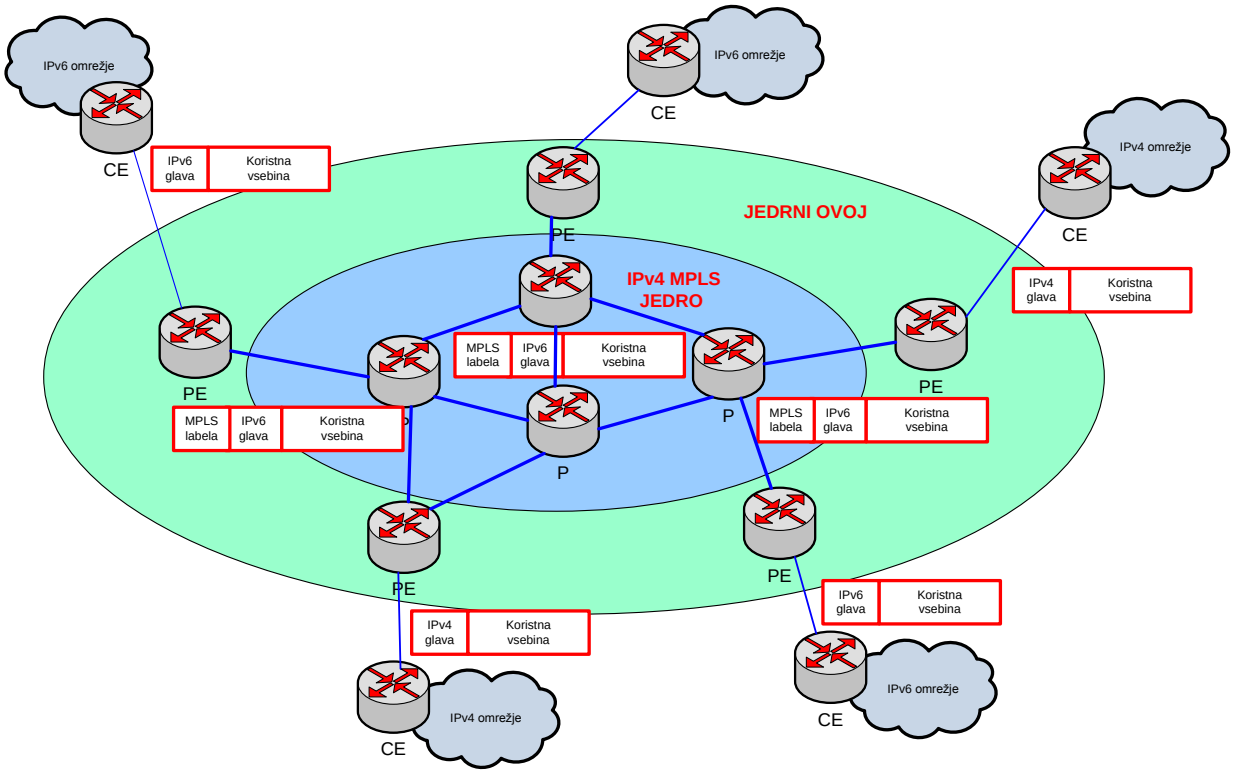
6.1.4.1 IPv6 čez IPv6/MPLS

IPv6 čez infrastrukturo omrežja MPLS pomeni, da vsi MPLS usmerjevalniki uporabljajo IPv6 kot osnovni IP protokol, MPLS pa se uporablja kot odločitveni posredovalni mehanizem. Da omogočimo prenos IPv6 prometa čez MPLS omrežje mora operater nadgraditi obstoječe jedrne LSR (P) usmerjevalnike z IPv6 podporo (IPv6 usmerjanje, IPv6 LDP v jedru). Jedrna infrastruktura zahteva polno nadgradnjo na IPv6 nadzorno ravnino. Nadgradnja zahteva dvoje: prvič, usmerjevalniki potrebujejo omrežne vmesnike, ki so sposobni obdelovati IPv6 protokolni sklad in drugič, MPLS z distribucijo label (uporaba LDP protokola) mora znati

prepoznavati in obdelovati IPv6 128 bitne naslove. Trenutno so redki primeri, ki uporabljajo IPv6 čez IPv6 MPLS.

6.1.4.2 IPv6 čez IPv4/MPLS

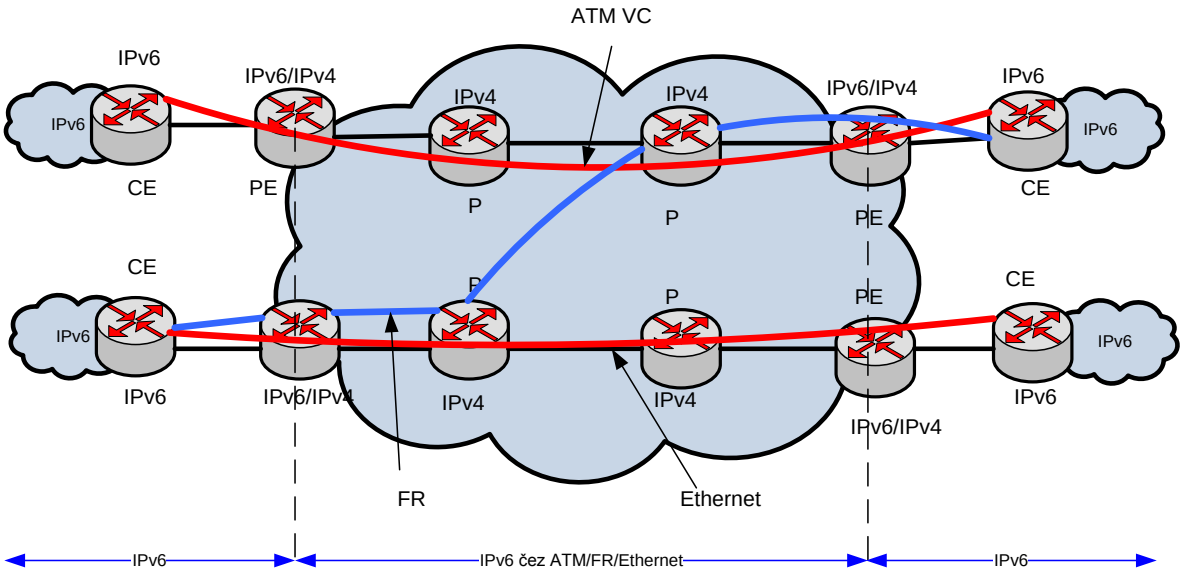
IPv6 čez IPv4 MPLS omogoča, da IPv6 domene komunicirajo med seboj preko obstoječe MPLS IPv4 hrbtenice. Prednost pri tem je, da ni potrebe po posodobitvi ali zamenjavi strojne ali programske opreme ali same konfiguracije jedrnega dela omrežja, niti ne vplivamo na prenos obstoječega IPv4 prometa. Pri tem pristopu moramo nadgraditi samo robne PE (angl. Provider Edge) MPLS usmerjevalnike, ki so povezani z IPv6 domenami. V kolikor imamo vzpostavljeno navidezna zasebna omrežja in izvajamo prometni inženiring lahko tudi IPv6 domene kombiniramo v VPN omrežja ali ekstranete. Z uporabo MP-BGP (angl. Multiprotocol-Border Gateway Protocol) tuneliranja, lahko LSR usmerjevalniki z uporabo BGPv4 čez IPv4 prenašajo IPv6 predpone. Pri tej arhitekturi MPLS omrežje vsebuje klasične (IPv4) P usmerjevalnike (angl. Provider routers), ki imajo nalogo samo preklapljati MPLS pakete, ne pa tudi analizirati IP glave. Na robu omrežja pa imamo posodobljene MPLS usmerjevalnike (PE usmerjevalnike), ki analizirajo IP glave, celoten paket pa označijo z MPLS labelo ter ga usmerijo naprej proti jedrnem P usmerjevalniku. Operaterjevi naročniki se povezujejo proti robnim LER usmerjevalniki s svojimi obstoječimi (Dual stack) IPv4/IPv6 oz. IPv6 robnimi usmerjevalniki (angl. CE-Custumer Edge). Med CE in PE usmerjevalniki se promet izmenjuje s pomočjo klasičnih usmerjevalnih protokolov (npr. OSPFv3, IS-ISv6, BGP, statično usmerjanje..). Slika 16 prikazuje IPv6 povezljivost preko IPv4/MPLS.



Slika 16: IPv6 čez IPv4/MPLS

6.1.4.3 Tuneliranje L2 čez MPLS

Z uporabo MPLS lahko prenašamo različne omrežne protokole. V večini primerov je to prenos IP paketov. Kljub vsemu, pa lahko preko MPLS omrežja prenašamo tudi L2 (Ethernet, ATM, blokovno posredovanje) promet. Robni PE usmerjevalniki morajo L2 okvirje oviti v MPLS ter jih posredovati naprej skozi MPLS hrbtenico (P usmerjevalnike). Izhodni PE usmerjevalniki MPLS domene odstranjujejo MPLS labele ter razvite okvirje na vrhu prvega (fizičnega) sloja (npr. z uporabo optičnega multipleksiranja) posredujejo naprej proti ciljnemu omrežju. Ta rešitev ne zahteva sprememb v IPv4 MPLS jedru, nadgrajeni na IPv6 pa morajo biti robni usmerjevalniki (IPv6 čez ATM/FR/Ethernet). Slika 17 prikazuje L2 tuneliranje čez MPLS omrežje.



Slika 17: L2 tuneliranje čez IPv4 MPLS

6.2 Dostopovna omrežja

Dostopovno omrežje omogoča širokopasovni dostop do IP storitev in agregacijo prometa. Promet naročnikov se prenaša do ponudnika storitev preko sloja podatkovne povezave (drugi OSI nivo) ali preko omrežnega nivoja (tretji OSI nivo). Če ima ponudnik dostopa omrežje, ki temelji samo na sloju podatkovne povezave, v omrežju nimamo usmerjanja. Dostopovno omrežje se v tem primeru preko robnega usmerjevalnika (angl. Edge Router) združuje (agregira) v redundantno, elastično in skalabilno hrbtenično omrežje, ki temelji na drugem nivoju. Hrbtenično omrežje je lahko zgrajeno iz različnih transportnih tehnologij kot so: Ethernet, ATM, MPLS in podobno. Ta tip omrežja je lahko transparentno za protokole tretjega nivoja, vendar mora zagotavljati ustrezno filtriranje in nadziranje IPv6 prometa, ki je pogojeno na informacijah drugega nivoja (npr. IPv6 Ethernet tip protokola-0x86DD, IPv6 Multicast specifični MAC naslovi-33:33:xx:xx:xx:xx).
Če dostopovno omrežje ponudnika temelji na tretjem (omrežnem) nivoju, se lahko (broadcast) domene drugega nivoja zaključujejo na robnem usmerjevalniku, od tam pa se promet usmerja proti omrežju ponudnika storitve. Dostopovni usmerjevalniki združujejo naročniški promet in ga usmerjajo preko hrbtenice tretjega nivoja do robnih usmerjevalnikov ponudnika storitev. V tem primeru uvedba IPv6 storitev bistveno vpliva na elemente omrežja.

V Sloveniji imamo trenutno tri tipe fizične dostopovne infrastrukture: omrežje bakrenih paric z uporabo DSL tehnologije, optično-kabelsko omrežje (angl. HFC-Hybrid fiber coaxial) in optično dostopovno omrežje (angl. FTTH-Fiber-to-the-home). Vsako od naštetih dostopovnih omrežij uporablja različno opremo, tako na strani (rezidenčnega/poslovnega) naročnika, kot na strani operaterja, ponudnika IP storitev.

6.2.1 Dostopovno omrežje bakrenih paric

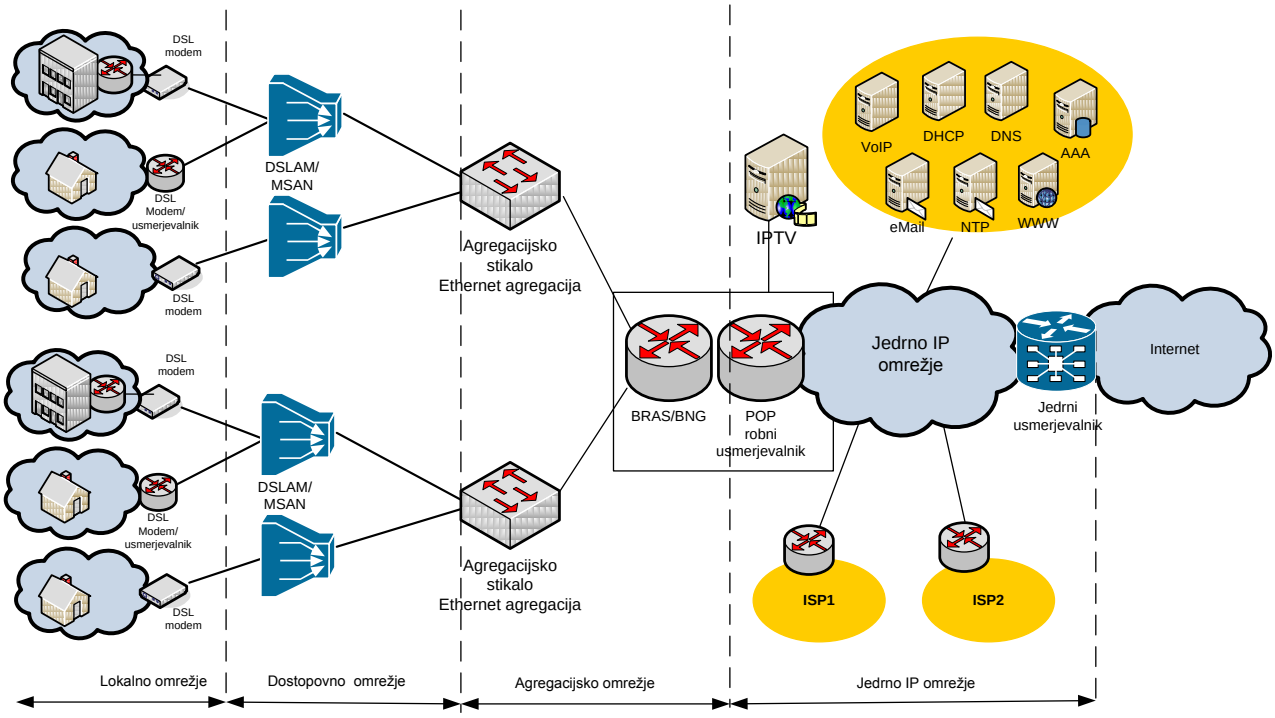
V dostopovnem omrežju, ki uporablja kot prenosni medij bakrene parice, se za dostop do internetnih storitev uporablja tehnologija, ki temelji na digitalnem naročniškem vodu (angl. DSL- Digital Subscriber Line). V Sloveniji tehnologija DSL omogoča končnemu uporabniku storitve kot so: stalni širokopasovni dostop do Interneta, uporabo govora preko IP protokola (VoIP), video na zahtevo (VoD), televizijo preko IP protokola (IPTV) ter druge internetne storitve.
Poznamo družino sorodnih DSL tehnologij, ki se med seboj razlikujejo v modulaciji, kodiranju, uporabljenem frekvenčnem spektru, v različni prenosni hitrosti ter še nekaterih drugih specifičnih parametrih. V Sloveniji sta najbolj razširjeni DSL tehnologiji ADSL in VDSL ter njune nadgradnje (ADSL2, ADSL2plus, VDSL2). VDSL2 je kompatibilen tudi za nazaj z tehnologijami ADSL in ADSL2 in ADSL2plus. Za obe tehnologiji je značilna različna prenosna hitrost (VDSL omogoča hitrejši prenos, ADSL počasnejši), uporabljeni pasovni širini (VDSL2 30 MHz; ADSL2plus 2,2 MHz) ter največji možni razdalji delovanja (ADSL2 max.~5 km, VDSL2 max. ~1,2 km). Tehnologija ADSL2 je pogojena z asimetričnostjo hitrostjo prenosa (večja hitrost proti uporabniku – 24 Mbit/s in manjša proti omrežju 2,2 Mbit/s), VDSL(2) tehnologija pa omogoča tudi simetrično hitrost način prenosa (VDSL2: 100/100 Mbit/s).

Gradniki dostopovnega DSL omrežja poleg bakrenih paric sestavljajo:

- naročniški xDSL modemi (CPE-Customer Premises Equipment)
- dostopovna vozlišča (MSAN/DSLAM)
- agregacijska stikala,
- širokopasovni oddaljeni strežniki - BRAS (angl. BRAS-Broadband Remote Server)[5],
- zmogljivi inteligentni (robni) usmerjevalniki.

Ostali ključni elementi omrežja, ki jih imamo tudi v drugih dostopovnih omrežjih (HFC, FTTH) so še: strežniki za avtentikacijo, avtorizacijo in obračunavanje (RADIUS, Diameter), DNS in DHCP strežniki ter strežniki, ki zagotavljajo storitve (VoIP, IPTV,VoD…).
Slika 18 prikazuje konceptualno shemo jedrnega in DSL dostopovnega omrežja.

[5] V literaturi se srečamo tudi z izrazom širokopasovni omrežni prehod (angl. BNG-Broadband Network Gateway) ali širokopasovni storitveni usmerjevalnik (angl. BSR-Broadband Service Router)



Slika 18: Konceptualna shema jedrnega in dostopovnega omrežja

Naročniška oprema (CPE-Customer Premises Equipment) je lahko samo modem, ki deluje v funkciji enostavnega mostu (angl. Bridge) ali pa omogoča tudi naprednejše (usmerjevalne) funkcije (CPE usmerjevalnik). V primeru, da deluje kot most med naročniškim lokalnim omrežjem (LAN) in DSL prostranim (WAN) omrežjem je xDSL modem v celoti transparenten za IP promet, ki je lahko IPv4 ali IPv6. V poslovnih okoljih je praviloma poleg CPE naprave še eden ali več usmerjevalnikov in oprema, ki zagotavlja nadzor prometa, zaščito proti vdorom in druge naprednejše funkcije. Če imamo IPv6 povezljivost, morajo naprave znati obdelovati tudi IPv6 promet. V manjših okoljih so lahko naprednejše funkcije vgrajene tudi v eni sami napravi. Med njimi bi izpostavili: prevajanje IPv4 naslovov/vrat (NAT, PAT), delovanje na obeh protokolnih skladih (IPv4/IPv6), izvajanje translacije naslovov (6to4,..), tuneliranje (IPsec, L2TP VPN), vsebuje napredne translacijske mehanizme, omogoča filtriranje in nadzor prometa, vsebuje dodatne vmesnike (USB in optični vmesnik). Tovrstne zahteve so praviloma v domeni poslovnih okolij, vendar se navedene funkcionalnosti v obliki hibrida modem/usmerjevalnik vedno bolj širijo tudi k rezidenčnim uporabnikom.

Dostopovna vozlišča (DSLAM/MSAN) zaključujejo (terminirajo) dostopovne fizične vode in izvajajo agregacijo prometa do agregacijskih stikal oz. BRAS. MSAN (angl. Multi-Service Access Node) je sicer strokovni termin za zmogljivo dostopovno vozlišče, ki uporabnikom zagotavlja storitve prenosa multimedije, podatkov in govora preko različnih vmesnikov (DSL, optika, Wimax, POTS). Dostopovna vozlišča se obnašajo kot zmogljivo inteligentno Ethernet stikalo, zagotavljajo naprednejše funkcionalnosti protokolnega vzajemnega delovanja (Interworking), združujejo VLAN oznake. Omogočati morajo replikacijo multicast prometa (IGMP (IPv4), MLD (IPv6) vohljanje (angl. Snooping)), izvajajo MAC filtriranje, identifikacijo naročnikov in izolacijo prometa. V kolikor transport med CPE in dostopovnim vozliščem temelji na ATM, morajo biti vozlišča sposobna izvajati vzajemno delovanje med naročniškim

ATM nivojem in Ethernet nivojem na izhodu proti BRAS. Dostopovna vozlišča so transparentna za IPv6 promet.
Agregacijska stikala združujejo promet iz vseh dostopovnih vozlišč. Omogočati morajo multicast promet in visoko razpoložljivost (večdomnost). Sposobna morajo biti premoščati VLAN označevanje (IEEE 802.1ad), izvajati izolacijo uporabnikov. Ker delujejo na drugem nivoju (razen za IP multicast) so transparentna za IPv6 promet.

Širokopasovni oddaljeni dostopovni strežniki (BRAS) so točka, kjer se združuje (in terminira) promet vseh naročnikov. Omogočajo tuneliranje, agregacijo (IP, Ethernet, PPP) med dostopovnim omrežjem in ponudnikom jedrnega omrežja (Network Service Provider) ali ponudnikom storitev (ASP-Application Service Provider). Poleg agregacije lahko omogočajo naprednejše funkcionalnosti, kot so: centralni nadzor in upravljanje, naprednejše IP usmerjanje, zagotavljanje QoS, DHCP posredovanje (angl. Relay), naprednejše upravljanje prometa. Lahko so fizično nameščeni v regionalnem omrežju operaterja, ki omogoča veleprodajno storitev širokopasovnega omrežja ali v omrežju ponudnika storitev. Ker imajo nekatere aplikacije specifične zahteve (oddajanje v multicast načinu) in veliko porabo pasovne širine (npr. video), jih je smiselno zaradi optimizacije prometa obravnavati ločeno od ostalih storitev. V takih okoljih imamo lahko ločene BRAS strežnike, ki so prvenstveno izključno namenjeni za optimizacijo video prometa. Ker BRAS strežnik deluje tudi v funkciji usmerjevalnika mora podpirati oba protokolna sklada (IPv6/IPv4). Funkcionalnosti BRAS in robnega usmerjevalnika so lahko združene v eni napravi.

Robni usmerjevalnik (angl. Edge Router) predstavlja glavno robno vozlišče med dostopovnim/agregacijskem omrežjem in hrbteničnim omrežjem. Predstavlja vozlišče, kamor se povezujejo alternativni operaterji in internetni ponudniki storitev. V hrbteničnem omrežju, ki temelji na MPLS, robni usmerjevalnik predstavlja vstopno točko v MPLS omrežje. Robni usmerjevalnik mora podpirati oba IP protokolna sklada. Lahko tudi omogoča vse funkcionalnosti, ki so bile navedene za BRAS.

Avtentikacija, avtorizacija in obračunavanje naročnikov (AAA - Authentication, Authorization, and Accounting) je lahko centralizirana storitev na enem strežniku ali pa je storitev porazdeljena na več strežnikih. Če želimo vpeljati IPv6 mora IPv6 atribute podpirati tudi oprema, ki izvaja AAA. RFC3162[6] in RFC4818[7] opisujeta različne RADIUS atribute, ki se lahko uporabijo pri uvedbi IPv6 v širokopasovnem omrežju. CPE naprava v fazi avtentikacije s pomočjo avtentikacijskega protokola CHAP (angl. Challenge Handshake Authentication Protocol) ali EAP (angl. Extensible Authentication Protocol) prenese svojo zahtevo na BRAS strežnik. BRAS strežnik zahtevo po prijavi (uporabniško ime in geslo) posreduje RADIUS strežniku, ki izvede avtorizacijo obenem pa tudi opredeli in preveri parametre kot so: storitve do katerih je uporabnik upravičen (Internet, IPTV, VoIP, VoD), njihova kakovost, hitrost prenosa (navzgor/navzdol), obračunavanje ipd. RADIUS vrne parametre BRAS strežniku, ta pa jih posreduje CPE napravi. RADIUS strežnik je lahko en sam in upravlja naročnike tako iz IPv6 kot iz IPv4 omrežij ali pa imamo dva ločena AAA strežnika, eden za IPv4 in drugi za IPv6. Če uporabljamo dva ločena RADIUS strežnika, je sicer povečana kompleksnost upravljanja, vendar nam lahko olajša vpeljavo novih IPv6 storitev (ni nam potrebno spreminjati obstoječe RADIUSv4 konfiguracije). Uporaba AAA funkcionalnosti je podobna tudi v drugih dostopovnih omrežjih (HFC, FTTH).

[6] RFC3162: Radius and IPv6
[7] RFC4818: RADIUS Delegated-IPv6-Prefix Attribute

IPv6 naslovi in drugi omrežni parametri se CPE napravam oz. gostiteljem dodeljujejo s pomočjo DHCPv6 protokola[8]. Uporaba DHCPv6 zahteva, da imamo zagotovljen IPv6 transport. DHCPv6 pozna dva mehanizma s katerimi lahko odjemalci nastavijo svoje mrežne parametre. To je 'Stateful' način konfiguracije, kjer odjemalci dobijo vse potrebne parametre z vsemi stanji in 'Stateless, kjer odjemalci od DHCPv6 strežnika dobijo samo IPv6 predpono in privzeti prehod. Odjemalec mora znati uporabljati oba stanja. Ker DHCPv6 v načinu 'Stateful' vzdržuje podatkovno tabelo s stanji odjemalcev potrebujemo strežniško komponento oziroma poseben strežnik. Podatkovna baza vsebuje podatke o vseh dodeljenih IPv6 naslovih in gostiteljih, ki te naslove uporabljajo. Strežnik DHCPv6 zagotavlja, da odjemalec (gostitelj) dobi enega ali več IPv6 naslovov, lahko dobi dodatno konfiguracijsko informacijo (IP naslove DNS strežnikov, čas obstojnosti IP naslova), eno ali več IPv6 predpon ali vse našteto. V načinu DHCPv6 'Stateful' BRAS deluje v funkciji DHCPv6 posrednika (DHCP Relay agent), ki DHCPv6 sporočila Solicit odjemalcev posreduje DHCPv6 strežniku, ki je drugje v omrežju. Tudi pri tem načinu je uporabniški profil shranjen v RADIUS strežniku, ki s svojimi atributi oskrbuje BRAS strežnik. Prednost pri tem je tudi povečana varnost, saj DHCP posredniški agent skriva IP naslov AAA strežnika, po drugi strani pa razbremeni BRAS strežnik.

IPv6 naslove pa se lahko dodelujejo tudi v 'Stateless' načinu, kjer ne potrebujemo posebnega strežnika in kjer si odjemalci sami popolnoma neodvisno od centralne avtoritete konfigurirajo svoj IPv6 naslov. Če uporabljamo protokol SLAAC (RFC2462), ki je akronim za avto konfiguracijo naslovov brez stanj (angl. Stateless address autoconfiguration) se BRAS usmerjevalnik oglašuje z Routing Advertisment (RA) sporočili, ki odjemalcem (CPE usmerjevalnikom) pošilja mrežno IPv6 predpono (IPv6 Prefix) in privzeti prehod. CPE mora omogočati in mora biti konfiguriran tako, da posluša oglasna sporočila usmerjevalnika (Router Advertisement). Ker lahko v omrežju pride tudi do podvajanja IPv6 naslovov pri tem sodeluje še Neighbor Discovery protokol s funkcijo DAD (angl. Duplicate Address Detection), ki preprečuje konflikte s preostalimi IPv6 vozlišči (zaznava podvojene IPv6 naslove). Javni globalni IPv6 naslov se na mrežnem vmesniku CPE naprave s pomočjo prejetih parametrov nastavi sam s pomočjo avto-konfiguracijskega mehanizma (angl. Stateless Autoconfiguration). Mrežno IPv6 predpono prejme od usmerjevalnika, zadnjih 64 bitov, pa po postopku, ki ga določa standard IEEE EUI-64 (64-bit Extended Unique identifier) generira sam iz svojega mrežnega vmesnika. Mehanizem SLAAC omogoča gostiteljem povezavo v omrežje, nastavitev IPv6 naslova ter takojšnjo vzpostavitev komunikacije z drugimi vozlišči, ne da bi se registriral in overil v lokalnem omrežju. Ta način pa ima tudi varnostne pomanjkljivosti. Uporaba mehanizma SLAAC in zaznavanje podvojenih naslovov (DAD-Duplicate Address Detection) odpira tudi možnosti napada zavrnitve storitve. (angl. Denial of Service). V omrežju npr. lahko katerikoli vozlišče odgovori (namerno ali nenamerno) na povpraševanje (Neighbor Solicitation) gostitelja po IPv6 naslovu. Zaradi varnosti je zato priporočljivo, da se na lokalnem nivoju (Link-Local) med napravami za avtentikacijo usmerjevalnikov uporabi varnostno razširitev NDP (Neighbor Discovery Protocol) protokola, protokol SEND (angl. SEcure Neighbor Discovery)[9]. SLAAC je zelo enostaven način, kako lahko vozliščem zagotovimo njihove IPv6 naslove. V koliko usmerjevalnika v omrežju ni, si lahko gostitelj generira le lokalni-povezavni (Link-Local) IPv6 naslov, s katerim lahko komunicira z ostalimi odjemalci, ki so povezani na isto povezavo. Žal 'Stateless' način gostiteljem ne zagotovi IP naslova DNS strežnika. V tem primeru se mora gostitelj povezati na DHCPv6 strežnik, ki deluje v načinu 'Statefull'. Opisan način naslavljanja odjemalcem se lahko izvaja enako ali podobno tudi pri dostopovnem HFC in FFTH omrežju.

[8] DHCPv6 opredeljujejo trije standardi: RFC3315 (DHCP for IPv6), RFC3633 (IPv6 Prefix Options for Dynamic Host Configuration Protocol DHCP version 6) in RFC 3736 (Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6).
[9] RFC3971: SEND-http://tools.ietf.org/html/rfc3971

Med xDSL modemom in BRAS strežnikom se je v preteklosti največ uporabljala prenosna tehnologija ATM (angl. Asynchronous Transfer Mode), ki pa jo danes že v večini izpodriva Ethernet. Ethernet za razliko od ATM omogoča hitrejše prenosne hitrosti, omogoča kvaliteto storitev (QoS), enostavnejše upravljanje, omogoča multicast in redundanco na učinkovitejši način kot ATM. Standardni virtualizacijski mehanizem, ki ga uporablja Ethernet je VLAN (Virtual LAN) označevanje (angl. Virtual LAN tagging)[10]. VLAN omogoča, da omrežje, ki temelji na Ethernetu segmentiramo na logične skupine[11]. VLAN označevanje prometa (Ethernet okvirjev) se izvaja na uporabniški CPE napravi, zaključuje (terminira) pa se na tronivojski napravi (BRAS ali robni usmerjevalnik). Vmesna dostopovna vozlišča (MSAN, DSLAM) in agregacijska stikala morajo pri tem transparentno preslikavati VLAN promet. V širokopasovnih omrežjih se največkrat uporabljajo naslednji VLAN modeli:

- naročniški VLAN (C-VLAN), ki ga tudi imenujejo 1:1 model, kjer je ima vsak naročnik svoj VLAN logični kanal. V tem logičnem kanalu, ki je izoliran od prometa ostalih naročnikov se vse IP storitve (VoD, IPTV, VoIP, Internet..) pošiljajo v načinu unicast (oddajanje samo enemu prejemniku),
- storitveni VLAN (S-VLAN) - vsaka IP storitev se prenaša v svojem VLAN logičnem kanalu. Ta model imenujejo N:1 model, ker si večje število naročnikov deli isti VLAN,
- hibridni VLAN. Hibridni model izkorišča vse prednosti naročniškega in storitvenega VLAN modela. Naročnik ima namenski C-VLAN za potrebe storitev, ki so optimizirane za unicast način prenosa prometa (VoIP, Internet, VoD) ter storitveni VLAN, pri prometu, ki je optimiziran za multicast način prenosa (IPTV).

Z VLAN označevanjem prometa lahko tudi vsaki IP storitvi dodelimo svoj razred storitve (angl. Class of Service), kar nam omogoča izvajanje prioritizacije prometa ali ga uporabimo za vzpostavitev navideznih zasebnih omrežij na drugem nivoju (L2 VPN). Na podlagi IEEE 802.1ad terminologije ločujemo zunanje VLAN označevanje (S-TAG oz. S-VLAN), ki se uporablja na V vmesniku med dostopovnim vozliščem in BRAS, ter notranje VLAN označevanje (C-TAG oz. C-VLAN), ki se uporablja na U vmesniku med dostopovnim vozliščem in rezidenčnim usmerjevalnikom (CPE)[12].
VLAN oznake pa lahko tudi nalagamo v sklad dveh plasti (VLAN stacking)[13]. Označevanje okvirjev v dveh plasteh nam omogoča, da VLAN notranje identifikatorje uporabljamo za razlikovanje med naročniki, zunanje VLAN identifikatorje pa uporabimo za razlikovanje med različnimi ponudniki storitev, kar je še posebej uporabno na veleprodajnem trgu.
Vzpostavitev in zagotavljanje povezljivosti z naročniki se sestoji iz več faz:

- Avtentikacija uporabnika - ko je povezava vzpostavljena, se mora pred dostopom v omrežje preveriti identiteta uporabnika (avtentikacija)
- Dodelitev IP naslova – ko je uporabnik avtenticiran, se mora CPE napravi dodeliti IP naslov
- Nadzor dostopa - omrežje mora avtorizirati kateri omrežni viri (storitve) so dostopne uporabniku ter v kakšni kvaliteti in hitrosti (hitrost dostopa navzgor/navzdol, QoS).
- Kontrola povezave – vsaka seja mora biti nadzorovana, da zagotovimo, da je naročnik še vedno povezan v omrežje

Danes najbolj razširjena protokola, ki zagotavljata zgoraj naštete funkcije sta PPPoE in IPoE (IP over Ethernet). IPoE se velikokrat navezuje tudi na DHCP (angl. Dynamic Host

[10] VLAN označevanje Ethernet prometa opredeljuje standard IEEE 802.1Q, ki ga sedaj izboljšuje IEEE 802.1ad
[11] Juniper Networks (2009): VLAN design for IPTV/Multiplay
[12] Broadband Forum. Tehnični dokument TR-101: http://www.broadband-forum.org/technical/download/TR-101.pdf
[13] IEEE 802.1Q-Q

Configuration Protokocol), saj ta protokol izvaja ključno vlogo pri vzpostavitvi IPoE povezljivosti. PPP seje so osnovane na storitvenem modelu, DHCP pa je bolj primeren za storitve, ki so stalno na razpolago (Always-on-services). Oba našteta protokola imata svoje prednosti in slabosti.

PPP protokol (angl. Point-to-Point Protocol) je dominanten sejni nadzorni protokol, ki se je najprej uporabljal pri vzpostavljanju klicnih povezav (angl. Dial-up), nato pa se je razvil tudi za uporabo v DSL omrežjih. Ker so prva dostopovna DSL omrežja temeljila na ATM prenosni tehnologiji, so PPP nadgradili na PPPoA (PPP over ATM), ko pa je ATM začel izpodrivati Ethernet so PPP nadgradili na PPPoE (PPP over Ethernet). PPPoE je tudi še danes v Sloveniji najbolj razširjen sejni vzpostavitveni in nadzorni protokol, ki se uporablja med naročniškim xDSL modemom in usmerjevalnikom. PPPoE proces vzpostavitve povezave gre čez več faz, ki vključuje vzpostavitev seje točka-točka in določitve enoličnega identifikatorja seje, vzpostavitev povezavne zveze s pomočjo protokola LCP (Link Control Protocol), pogajanja o dodatnih parametrih zveze (kompresija in avtentikacijska metoda), avtentikacija uporabnika (PAP, CHAP ali EAP) in dodelitev IP naslova s pomočjo IPCP (angl. IP Control Protocol) (IPv4) ali IPv6CP (IPv6) protokola. Če imamo vzpostavljeni dve seji IPCP in IPv6CP, kar je primer vozlišča z dvojnim skladom, lahko obe seji delujeta paralelno, čez eno PPP povezavo. Razlikovanje med IPv4 in IPv6 prometom se izvaja s pomočjo zapisa v protokolnem polju, ki ga vsebuje PPP glava (0x0021 za IPv4 in 0x0057 za IPv6). Glavna razlika med IPCP in IPv6CP je ta, da IPCP protokol omogoča, da odjemalec v fazi dodeljevanja naslovov v celoti dobi vse potrebne mrežne parametre, pri IPv6CP pa odjemalec dobi le povezavno-lokalni naslov (angl. Link-Local). Če želimo odjemalcu dodeliti še javni IPv6 globalni naslov, potrebujemo mehanizem SLAAC (angl. Stateless Address Autoconfiguration) ali pa DHCPv6 (RFC3315). Preverjanje ali je PPP seja vzpostavljena in delujoča, se periodično nadzira z 'Keep-alive' paketi, kar protokolu PPPoE daje še posebno prednost. Dodatno lahko naprednejši nadzor izvajamo tudi s pomočjo PPP LQM (Link Quality Monitoring) protokola[14]. Dodatni element omrežja je RADIUS strežnik. V fazi avtentikacije BRAS usmerjevalnik posreduje zahtevo po prijavi RADIUS strežniku, RADIUS pa poleg verifikacije uporabnika vrne tudi informacije, ki opredeljuje parametre kot so: storitve (Internet, IPTV, VoIP, VoD) do katerih je uporabnik upravičen, njihova kakovost in hitrost prenosa (navzgor/navzdol). Ker se pri PPPoE proces avtentikacije uporabnika izvede še predno omrežje dodeli IP naslov, nam to omogoča, da BNG ali samostojni DHCP strežnik dodeli IP naslov, ki je pogojen z naročeno storitvijo. To je zelo pomembno v omrežjih, kjer je širokopasovni dostop (z bitnim tokom) veleprodajna storitev in kjer lahko vsak naročnik izbere različnega ponudnika za izbrano vrsto IP storitve (npr. imamo več ponudnikov Interneta, ki uporabljajo omrežje glavnega operaterja). Iz tega razloga je PPP še vedno dominanten mehanizem, ki omogoča operaterjem omrežij, da ponudijo svoje storitve in omrežje v najem drugim operaterjem na veleprodajnem trgu.

PPP pa ima tudi slabosti. Ethernet okvir se zaradi dodatnih 8 oktetov (PPP glava + PPPoE glava) poveča, kar ima za posledico potrebo po kompleksnejšem procesiranju okvirjev v primerjavi z IPoE. Druga slaba stran pa je, da PPP ne zagotavlja učinkovite podpore Multicast prometu. IPTV je IP aplikacija, ki je pogojena prav z multicast prenosom TV vsebin več uporabnikom hkrati, obenem pa multicast prenos učinkovito izrablja pasovno širino agregacijskega dela omrežja. Če uporabljamo PPPoE, se seje zaključujejo na robnem usmerjevalniku, ne glede na to, ali uporabljamo unicast ali multicast prenos. Če imamo tri uporabnike, ki uporabljajo IP storitev IPTV (npr. gledajo isti TV program) potem moramo imeti od robnega usmerjevalnika do dostopovnega vozlišča (DSLAM, MSAN) vzpostavljene tri med seboj neodvisne unikatne seje, kjer vsaka prenaša isti tok podatkov na eni fizični

[14] PPP Link Quality Monitoring- RFC1989: http://tools.ietf.org/html/rfc1989

povezavi. Pri velikem številu uporabnikov storitve IPTV z načinom ovijanja PPPoE bistveno bolj (po nepotrebnem) zapolnimo razpoložljivo pasovno širino agregacijskega dela omrežja.

Broadband Forum, pravni naslednik DSL Foruma zaradi navedenih slabosti PPPoE priporoča tudi uporabo IPoE oz. DHCP. IPoE, ki ne potrebuje PPP ovijanja zagotavlja veliko funkcionalnosti PPPoE protokola, obenem pa za razliko od PPPoE omogoča bistveno boljšo izrabo pasovne širine agregacijskega dela omrežja za potrebe multicast prometa. IPoE kot druga alternativa temelji na DHCP protokolu, ki je bil razvit predvsem za dodeljevanje IP konfiguracijskih parametrov gostiteljem, ki se nahajajo na lokalnem omrežju v eni broadcast domeni. Iz tega razloga DHCP protokol v prvotni izvedbi ne podpira procesa vzpostavitve povezave, avtentikacijo uporabnikov ali nadzor nad delovanjem povezave. DHCP razširitve in drugi protokoli (EAP-Extensible Authentication Protocol) so sedaj kombinirani z DHCP, da zagotavljajo podobne funkcionalnosti kot PPPoE. IPoE ne vzpostavlja seje med končnimi točkami, zato pri tem nimamo unikatne stalne identifikacije uporabnika, kot pri PPPoE. IPoE tudi nima procedure za overjanje uporabnika, kot je npr. CHAP ali EAP. Omrežje zato za dodelitev naročenih storitev uporablja informacijo o fizični priključitvi uporabnika na dostopovno vozlišče (vozliščna številka, reža, port vmesnika) ali uporablja informacijo, ki je osnovana na Ethernet VLAN/ATM VC identifikaciji preko katere je bila sprožena DHCP zahteva za dodelitev omrežnih virov. IPoE ta pristop zagovarja, da ni potrebe po ločeni prijavi uporabnika, saj je uporabnik s širokopasovno povezavo vseskozi prijavljen in obenem povezan na isti fizični port dostopovnega vozlišča. Ker pa zadnji trendi še posebej pri širokopasovnem dostopu preko WiFi vročih točk ali mobilnem Wimax-a ne omejujejo uporabnika, da se prijavlja iz ene same lokacije, v tem primeru nimamo mehanizma, ki bi unikatno identificiral uporabnika in način njegove povezljivosti v omrežje. Ta pristop tudi onemogoča uporabnikom, da bi dinamično prestopali med različnimi ponudniki storitev. Z uporabo procesa prijave naročnik lahko dostopa do katerekoli domene. V odgovor lahko omrežje dodeli naročniku IP naslov v odvisnosti od uporabljene prijavne domene (uporabnik123@domena.si). V primeru IPoE je IP naslov dodeljen še preden lahko omrežje preveri do katerih storitev je uporabnik upravičen. Rešitev za tovrstne težave je uporaba avtentikacijskega mehanizma IEEE 802.1x preko LAN (angl. EAPoL-Extensible Authentication Protocol). Mehanizem 802.1x se uporablja tako v brezžičnih omrežjih kot v omrežjih točka-točka, vendar trenutno še veliko naprav nima implementiranega DHCP odjemalca, ki bi protokol EAPoL podpiral. Drugi izziv, ki ga prinaša DHCP je doba obstojnosti dodeljenega IP naslova. Vsak IP naslov, ki ga dodeli DHCP strežnik ima omejeni čas trajanja. Ko ta čas preteče, mora odjemalec ponovno zaprositi za nov IP naslov. Ker DHCP sproži RADIUS povezavo, se to ponavlja vsakokrat, kot zakupna doba IP naslova preteče. To je lahko še posebej problematično v situacijah, ko pride do izpada omrežja, saj ob ponovni vzpostavitvi omrežja lahko DHCP strežnik dobi veliko simultanih zahtev odjemalcev po pridobitvi novega IP naslova. IPoE je lahko tudi problematičen pri operaterjih, ki zagotavljajo širokopasovni dostop v okviru veleprodajne storitve[15]. Ker IPoE ne identificira posamezne seje, je težko dinamično slediti kam je namenjen posamezni paket, ki prihaja od ponudnika storitev. Alternativni operaterji morajo zato zahtevati svoj unikatno VLAN identifikacijo (VLAN po uporabniku) ali pa jim mora biti dodeljen nabor IP naslovov, na podlagi katerih jih je mogoče med seboj ločevati. Pri implementaciji IPv6 moramo za razliko od PPP protokola uporabiti samostojni VLAN identifikator za posamezni IP protokol.

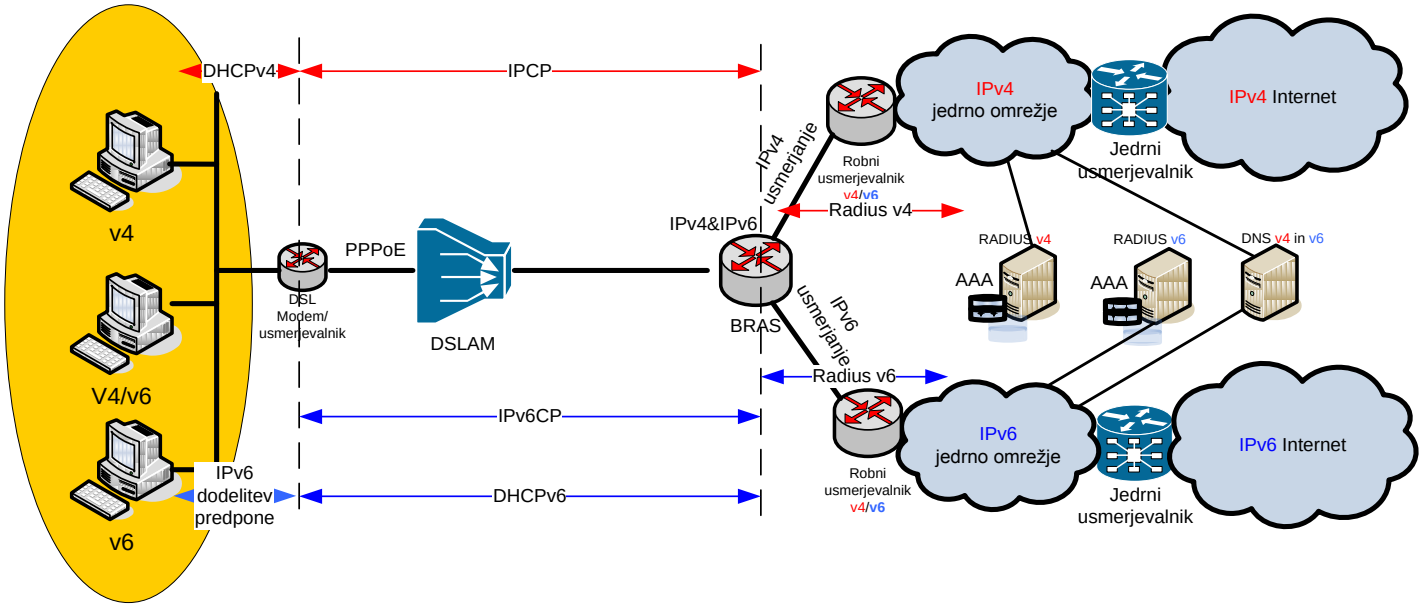
Broadband Forum je v tehničnem dokumentu TR-025 opredelil dva storitvena modela širokopasovnega omrežja, ki pomembno vplivata na vpeljavo IPv6 (upravljanje naročnikov, usmerjanje, dodeljevanje IP naslovov). Oba modela temeljita na drugonivojskem protokolu točka-točka (PPP). To sta:

[15] Juniper Networks (2008): Using PPPoE and IPoE in Ethernet Broadband Networks: http://www.juniper.net/solutions/literature/white_papers/200187.pdf

- PPP Terminated Aggregation (PTA) in
- L2TP Access Aggregation (LAA)

PTA model uporabljajo operaterji, ki ponujajo omrežni dostop in IP storitve v maloprodaji, LAA model pa se uporablja, kadar omrežje in IP storitve operater omogoča na veleprodajnem trgu.

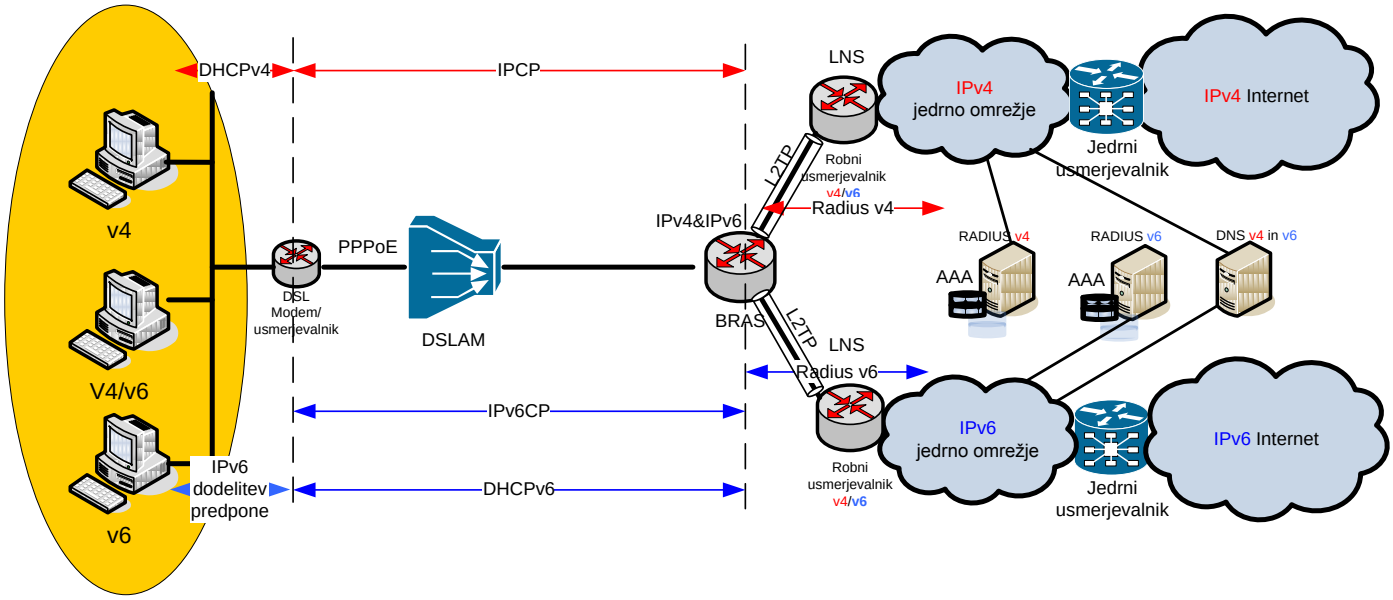
Pri PTA modelu so PPP seje odprte med vsakim naročnikom in BRAS strežnikom. BRAS seje avtorizira, naročnika overi (opravilo lahko izvaja tudi samostojni AAA strežnik), dodeljuje IP naslove (npr. s pomočjo mehanizma DHCP-PD (angl. DHCP-Prefix Delegation)) in seje zaključuje (terminira). Nadaljnji promet med BRAS in robnim usmerjevalnikom poteka preko IP usmerjanja. DNS informacije se zagotavljajo preko Statefull (RFC3315) in Stateless (RFC3736) DHCPv6. Ker BRAS strežnik pri tem scenariju izvaja usmerjanje, mora biti nadgrajen na IPv6. Ker BRAS PPP seje zaključuje, mora podpirati tudi protokol IPv6CP. Zaradi prehoda na IPv6 se mora nadgradnja na IPv6 izvesti tudi pri: končnem gostitelju, naročniškem CPE usmerjevalniku (če je prisoten), BRAS strežniku in robnemu usmerjevalniku. Tako BRAS strežnik kot robni usmerjevalnik, morata imeti podporo za IPv6 usmerjanje (OSPFv3 (RFC2740) ali IS-IS (RFC5308)). Z vidika usmerjanja, za CPE napravo naslednji skok (next-hop) in privzeta pot (angl. Default route) predstavlja BRAS strežnik.
Slika 19 prikazuje PTA model omrežja.



Slika 19: PTA model omrežja
Vir: Cocquet, P: IPv6 on DSL: The Best Way to Develop Always-On Services

Kadar uporabljamo LAA model, PPPoE povezavo in mrežne parametre gostitelja (CPE usmerjevalnika) nadzoruje ponudnik omrežja. Pri tej rešitvi, se vzpostavita dve seji, PPPv4 in PPPv6. Prva seja se vzpostavi med CPE usmerjevalnikom in BRAS preko PPPoE, druga seja (PPPv4+PPPv6), pa se vzpostavi s pomočjo L2TP (Layer 2 Tunneling Protocol) protokola med BRAS in agregacijsko točko L2TP omrežnega strežnika (LNS-L2TP Network Server) ponudnika omrežja. L2 povezava lahko temelji na podlagi VLAN navideznih kanalov, ATM permanentnih navideznih kanalov (ATM PVC), navideznih tokokrogov v blokovnem posredovanju (Frame Relay VC) ali druge splošne tehnike ovijanja. BRAS v tem primeru deluje kot L2 dostopovni koncentrator

(LAC - L2 Access Concentrator), ki ima nalogo vzpostavitve L2TP tunela. Ko je tunel vzpostavljen, se ves promet preko L2TP posreduje naprej robnemu usmerjevalniku ponudnika omrežja. V tem primeru se avtentikacija, avtorizacija in naročniška konfiguracija ne izvaja na BRAS strežniku (katerega lahko upravlja ponudnik dostopa), temveč to opravlja ponudnik omrežja, običajno preko RADIUS(v6) strežnika. L2TP tunel, ki je vzpostavljen med L2TP koncentratorjem in LNS strežnikom je lahko IPv4 ali IPv6. Če temelji povezava na L2TP preko IPv4, lahko ta del omrežja ostane nespremenjen, ne glede na to, da ponudnik omogoča naročnikom IPv6 povezljivost. Nadgradnja na IPv6 pa se mora v tem primeru izvesti pri gostitelju, oz. CPE usmerjevalniku in robnemu usmerjevalniku (LNS strežniku). V kolikor pa imamo L2TP tunel preko IPv6, mora biti na IPv6 nadgrajen tudi BRAS oz. LAC koncentrator. Naročniški profil za avtorizacijo in avtentikacijo se lahko nahaja na robnem usmerjevalniku ali pa na AAA strežniku. Ker v tem modelu zaključevanje sej izvaja robni usmerjevalnik (LNS), je tudi njegova naloga, da gostiteljem oz. CPE usmerjevalnikom s pomočjo DHCP-PD (DHCP - Prefix Delegation). zagotavlja IPv6 naslove, v odvisnosti od profila naročnika. Pri dodeljevanju IP naslovov, moramo pri tem izpostaviti pomembno razliko med IPv4 in IPv6. Pri vpeljavi IPv4 je naročnik dobil IP naslov iz bazena naslovov v odvisnosti od tega, na katerem robnem usmerjevalniku se je njegova seja zaključila. V primeru uvedbe IPv6 pa lahko naročnik obdrži in uporablja vseskozi isti IPv6 naslov ne glede na to, na katerem robnem usmerjevalniku, se je v danem trenutku njegova seja zaključila. DNS informacije se enako kot pri PTA modelu zagotavljajo preko Statefull (RFC3315) in Stateless (RFC3736) DHCPv6.
Slika 20 prikazuje LAA model omrežja.



Slika 20: LAA model omrežja
Vir: Cocquet, P: IPv6 on DSL: The Best Way to Develop Always-On Services

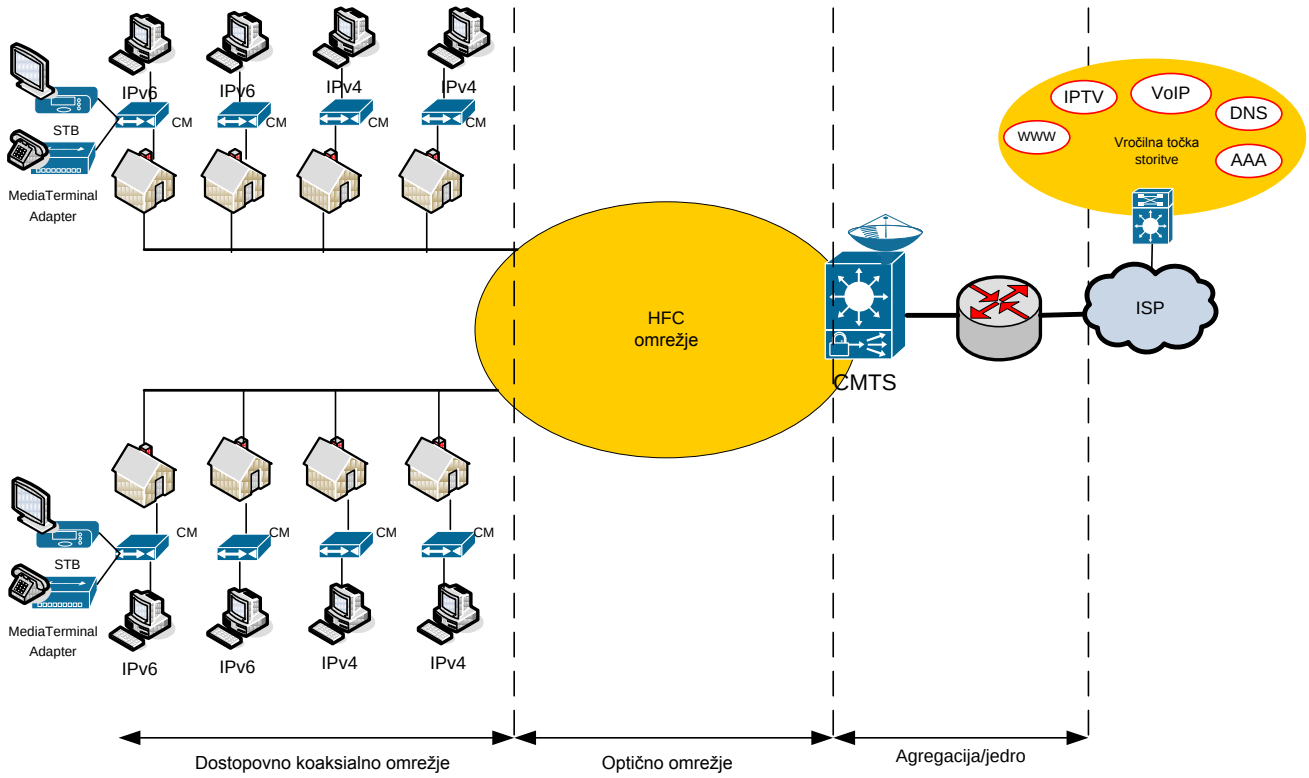
V primeru zagotavljanja multicast storitev, kot je npr. IPTV, ki potrebuje veliko pasovne širine, pa ima LAA model tudi slabe strani. Ker se seje zaključujejo na robnemu usmerjevalniku (ER-Edge Router), in ne na BRAS strežniku kot pri PTA modelu, lahko pridemo v situacijo, da je del omrežja med BRAS in ER po nepotrebnem preobremenjen zaradi kopij istega podatkovnega toka, ki vsebuje posamezni IPTV program. Rešitev temu je arhitektura, kjer se replikacija IPTV podatkovnega toka izvaja čim bližje naročniku, to je na BRAS strežniku. PPP seje se glede na IP storitev (IPv4 ali IPv6) pri tem hibridnem modelu zaključujejo na

različnih omrežnih napravah. PPP seje obstoječih IPv4 storitev uvedenih v LAA modelu, se zaključujejo na robnemu usmerjevalniku, PPP seje na novo vzpostavljenih IPv6 storitev, uvedenih v PTA modelu, pa se zaključujejo na BRAS strežniku.

6.2.2 Dostopovna optično-kabelska omrežja

Koaksialna kabelska omrežja, kot predhodnica današnjih hibridnih optično-kabelskih omrežij so bila primarno razvita, za enosmerni prenos analognih TV in radijskih signalov v arhitekturi točka več točk. Zgrajena so bila iz koaksialnih vodnikov, ki imajo, tehnološko gledano velik potencial, saj zaradi svoje zasnove omogočajo prenos električnih signalov na zelo širokem frekvenčnem območju. Če današnja najbolj zmogljiva xDSL tehnologija (VDSL2), na bakrenih paricah že zmore koristiti skoraj 30MHz frekvenčni pas, na koaksialnem vodniku lahko danes izrabljamo več ko tri krat večji frekvenčni pas (do 1 GHz) in to na bistveno daljših razdaljah, kot ga omogočajo bakrene parice. Z uvedbo interneta, je prišlo do velikih sprememb tudi v kabelskem omrežju. Če so kabelski operaterji želeli naročnike obdržati, so morali posodobiti opremo in infrastrukturne vode, poleg kvalitetnejše in številčnejše ponudbe radijskih in televizijskih programov pa so morali ponuditi še širokopasovni dostop do Interneta in VoIP, kateri storitvi zahtevata dvosmerno komunikacijo. Nove storitve, kot sta Internet in VoIP je leta 1997 omogočil nov mednarodni standard imenovan DOCSIS (angl. Data Over Cable Service Interface Specification), ki določa potrebne tehnične parametre za nadgradnjo klasičnega kabelskega omrežja in njegovih elementov z dvosmernim podatkovnim prenosom. Ker je bil DOCSIS primarno razvit za ZDA (CableLabs), kjer uporabljajo NTSC standard za razširjanje analognega TV signala, ki potrebuje manjši frekvenčni pas (6MHz), kot PAL (8MHz), ki se ga uporablja v Evropi, je standard doživel delne popravke, ki so bili objavljeni pod imenom EuroDOCSIS (8MHz pasovna širina kanala, različna frekvenčna razdelitev pasov proti/od uporabnika). DOCSIS se je nadgrajeval, sprva na verzijo 1.1 (april 1999) (podpora za zagotavljanje kvalitete storitev in izboljšana varnost), v decembru 2001 je dobil verzijo 2.0 (povečana pasovna širina v smeri navzgor, izboljšana modulacija in korekcija napak, za sodostop uporablja mehanizem CDMA, prej TDMA). Zadnja specifikacija DOCSIS 3.0 objavljena leta 2006 pa prinaša veliko novosti v primerjavi s predhodnimi verzijami. Nova specifikacija omogoča povečano prepustnost v obeh smereh, kar so dosegli s pomočjo tehnike logične vezave kanalov (angl. Channel bonding). Vezava kanalov je tehnika delitve bremena, ki omogoča kombiniranje večjega števila kanalov v skupni podatkovni tok. DOCSIS 3.0 specificira vezavo kanalov v smeri proti uporabniku (lahko združuje 4-8 kanalov), kot v smeri od uporabnika (lahko združuje 4 kanale). V smeri proti uporabniku, lahko podatkovni tok posameznega DOCSIS kanala širine 8 MHz prenaša v idealnih pogojih 50 Mbit/s koristne vsebine, v smeri od uporabnika pa 27 Mbit/s. Če kanale združujemo v podatkovni tok s pomočjo vezave kanalov, lahko v idealnih pogojih in izbrani najboljši modulacijski shemi proti uporabniku prenašamo 400 Mbit/s, od uporabnika pa 108Mbit/s koristne vsebine. Ker kabelska omrežja temeljijo na sodostopu, se navedeno podatkovno hitrost delijo uporabniki, ki so povezani v isto razdelilno vejo. Nova specifikacija tudi omogoča učinkovitejšo izrabo frekvenčnega spektra. Od uporabnika do glavne razdelilne postaje je sedaj namenjen frekvenčni pas od 5 do 65 MHz, proti uporabniku pa frekvenčni pas od 108 MHz do celo 1GHz. DOCSIS 3.0 omogoča tudi naprednejše šifriranje (uporaba šifrirnega algoritma AES) ter ima polno podporo za IPv6 (naslavljanje, IPv6 Multicast, IGMPv3, MLDv2, IPv6CP, IPv6 Neighbor Discovery..). Na infrastrukturi je s prihodom standarda DOCSIS prišlo do zamenjave primarnega koaksialnega omrežja (lokalne hrbtenice) z optičnimi elementi in optičnimi vlakni, na sekundarnem delu omrežja pa so starejše koaksialne kable zamenjevali z novejšimi, ki imajo bistveno boljše karakteristike (manjše dušenje pri visokih frekvencah). Zaradi potrebe po povratnem kanalu so se morali zamenjati tudi vsi ojačevalniki in pasivni elementi (odcepniki, delilniki), ki sedaj omogočajo

dvostransko komunikacijo. Velike tehnološke spremembe so se zgodile tudi na glavni sprejemni postaji pri operaterju in na kabelskem modemu (CM-Cable modem) pri naročniku. Naročniki so povezani v kabelsko omrežje preko kabelskega modema, ki predstavlja L2 napravo, ki je transparentna za IP promet (IPv4 ali IPv6). DOCSIS standard za kabelski modem določa tako fizični nivo (frekvence, modulacijo), kot tudi dostopovni MAC (angl. Media Access Control) nivo. MAC določa karakteristike prenosa (RF vmesnik) proti glavni sprejemni postaji iz nazaj, ureja sodostop do prenosnega medija in podeljuje zahtevano pasovno širino. Le-ta je v povratni smeri sorazmerna zmogljivosti povratnega kanala in obratno sorazmerna številu aktivnih uporabnikov. Več kot je aktivnih uporabnikov, z nižjo prenosno hitrostjo lahko deluje posamezen uporabnik. Modemi se povezujejo na glavno sprejemno postajo – CMTS (angl. CMTS - Cable Modem Termination System), ki je eden glavnih elementov omrežja. CMTS ima podobne funkcionalnosti kot jih zagotavlja DSLAM v DSL sistemih. Lahko je transparenten za IP promet (deluje kot most) ali pa izvaja tudi IP usmerjanje. Na eni strani je z Ethernet vmesnikom povezan IP omrežje, na drugi strani proti HFC omrežju in uporabnikom pa je povezan z optičnim vlaknom oziroma RF vmesnikom. Slika 21 prikazuje konceptualno shemo HFC omrežja.



Slika 21: Glavni elementi hibridnega optično-koaksialnega omrežja

Način uvajanja IPv6 v kabelskih sistemih je podobno, kot pri ostalih dostopovnih sistemih. IPv6 najprej uvedemo na primarnem hrbteničnem sistemu, nato na CMTS napravah in nazadnje na kabelskih modemih. Kabelski sistemi lahko delujejo v CMTS mostičnem (angl. Bridged) načinu ali pa delujejo v načinu IP usmerjanja. V mostičnem načinu, tako kabelski modem kot CMTS transparentno posreduje ves podatkovni promet. Promet od/do naročnika se preko kabelskega omrežja posreduje do robnega usmerjevalnika, kjer se nato preko omrežja internetnega ponudnika usmeri na Internet. Kabelski modem kot CMTS pri tem

omogočata L3 funkcionalnost samo za potrebe upravljanja. IPv6 se lahko vpelje v mostičnem kabelskem omrežju uvede bodisi preko tunela ali bodisi direktno. Nadgradnja na IPv6 se mora izvesti pri gostitelju, 'domačem' usmerjevalniku (če obstaja) in robnemu usmerjevalniku. CMTS kot kabelski modem (za potrebe upravljanja) morata omogočati prenos multicast in unicast IPv6 paketov, ki prihajajo od robnega usmerjevalnika do gostiteljev in obratno. V primeru uporabe IPv6 multicast aplikacij (npr. IPTV), morata kabelski modem in CMTS podpirati tudi protokole IGMPv4, MLDv2 in MLD snooping. IPv6 naslavljanje izvaja DHCPv6 strežnik oziroma robni usmerjevalnik, gostitelji oz. 'domači' usmerjevalnik, pa morajo biti sposobni poslušati in sprejeti DHCPv6 sporočila oz. oglaševalske (angl. Router Advertisement) pakete (Network Discovery protokol). V tem primeru si s pomočjo Stateless auto-configuration mehanizma sam nastavi zadnjih 64 bitov IPv6 naslova (EUI-64-64 bit Extended Unique Identifier). Če se uporablja v omrežju DHCPv6 strežnik, mora tako CMTS kot kabelski modem transparentno premostiti njegove pakete.
V primeru, da ima naročnik poleg kabelskega modema še 'domači' usmerjevalnik je ta preko statične privzete poti (angl. Default static route) povezan z robnim usmerjevalnikom. Praviloma v domačem okolju ne potrebuje funkcionalnosti usmerjanja. Podpirati mora IPv6 in nastavitev mrežnih parametrov, ki jih preko Network Discovery protokola (Router Advertisement paketov) prejme od robnega usmerjevalnika. Za predpone, ki so manjše od /64 (tipično /48[16]), se uporablja protokol DHCP-PD (DHCP-Prefix Delegation). Domači usmerjevalnik s pomočjo RA paketov naprej razdeljuje IP naslove gostiteljem v notranjem omrežju. Za gostitelje je v tem primeru naslednji skok 'domači' usmerjevalnik, za usmerjevalnik pa je naslednji skok robni usmerjevalnik. 'Domači' usmerjevalnik mora znati poslušati in sprejeti (Network Discovery protokol) oglaševalske pakete robnega usmerjevalnika ter tudi posredovati IPv6 multicast in unicast promet. V primeru, da gre za komunikacijo med gostitelji, ki niso povezani na isti kabelski modem, gre komunikacija vedno preko CMTS glavne sprejemne postaje. Kabelski modem podpira samo en IP protokolni sklad (IPv4 sklad za IPv4 promet ali IPv6 sklad za IPv6 promet), ne pa oba.

V usmerjevalnem HFC omrežju, se IP promet med naročnikom in CMTS posreduje na podlagi IP naslavljanja (IP izvorni in ciljni naslov). Kabelski modem pri tem za IP promet še vedno deluje v premostitvenem (L2) načinu, L3 funkcionalnost modema se uporablja samo za potrebe upravljanja. Za gostitelje (računalnike), naslednji skok (angl. Next hop) predstavlja robni usmerjevalnik (angl. Edge Router). CMTS v tem okolju deluje kot L3 usmerjevalnik in lahko vključuje tudi funkcionalnosti robnega usmerjevalnika. Če želimo gostiteljem v HFC omrežju omogočiti IPv6 povezljivost, imamo možnost prenosa IPv6 prometa preko IPv4 tunela ali direktno z uporabo IPv6. Če uporabimo IPv6 povezljivost, je predpogoj, da tako kabelski modem kot CMTS podpirata DOCSIS 3.0 standard (DOCSIS 1.0 in 2.0 ne podpirata Neighbor Discovery protokola). DOCSIS 1.0 in 2.0 omogočata IPv6 povezljivost le, če uporabimo tunelske mehanizme. CMTS in robni usmerjevalnik RFC4779[17] v HFC omrežju, ki deluje na podlagi usmerjanja definira 5 možnih načinov uvedbe IPv6:

- IPv4 kabelsko (HFC) omrežje

  V tem scenariju, kabelsko omrežje kot tudi kabelski modem in CMTS ne zamenjujemo saj transparentno premoščajo IPv4 promet. Nadgradnja na dvojni sklad se mora izvesti edino na gostitelju ter robnemu usmerjevalniku. Ker so v omrežju najmanjše spremembe, je za kabelskega operaterja to najlažji in najcenejši način, da omogoči IPv6 storitve. Promet med gostiteljem in robnim usmerjevalnikom poteka preko avtomatskega ali ročno nastavljivega IPv6 v IPv4 tunelskega mehanizma. Če mora robni usmerjevalnik

[16] RFC3177: IAB/IESG Recommendations on IPv6 Address Allocations to Sites
[17] RFC4779: ISP IPv6 Deployment Scenarios in Broadband Access Networks

zaključevati veliko tunelov je priporočljivo, da se zaradi avtomatizacije, uporablja avtomatsko tuneliranje. V kolikor se preko tunela prenašajo tudi storitve, ki temeljijo na multicast prenosu, moramo uporabiti ročno nastavljive tunele. Začetek tunela predstavlja gostitelj, robni usmerjevalnik tunel zaključuje, vmesne naprave (kabelski modem in CMTS) pa transparentno premoščajo IPv4 promet.

- IPv4 kabelsko (HFC) omrežje, usmerjevalni prehod (angl. Gateway Router) na strani naročnika

Če ima naročnik poleg kabelskega modema še usmerjevalni prehod, se mora nadgradnja na dvojni sklad izvesti na usmerjevalnem prehodu, gostitelju in robnemu usmerjevalniku. Ostali del omrežja in opreme ostaja nespremenjen. Kabelski operater ima lahko v tej arhitekturi naročnike, ki imajo še vedno samo IPv4 povezljivost in naročnike, ki jim z zamenjavo (nadgradnjo) usmerjevalnega prehoda omogoči IPv6 povezljivost. Usmerjevalni prehod mora znati na poslušati in sprejeti oglaševalske pakete (Router Advertisement) robnega usmerjevalnika ter si obenem nastaviti svoj mrežni vmesnik z IPv6 naslovom. Dobljeno IPv6 predpono mora oglaševati gostiteljem v notranjem omrežju. Če se naslavljanje izvaja s pomočjo DHCPv6, robni usmerjevalnik deluje kot DHCP posredniški agent ter DHCPv6 sporočila posreduje med usmerjevalnim prehodom in DHCPv6 strežnikom. Tako, kot v prejšnjem primeru, se tudi pri tej zasnovi vzpostavi tunel, pri čemer začetek tunela ni gostitelj temveč usmerjevalni prehod. Tunelsko končno točko predstavlja robni usmerjevalnik. Ker je omrežje še vedno IPv4, usmerjevalni prehod še vedno preko DHCP protokola dobi svoj IPv4 naslov.

- Kabelsko (HFC) omrežje z dvojnim skladom, kabelski modem in CMTS podpirata IPv6

Pri tem scenariju, CMTS nadgradimo na dvojni sklad. Zmogljivi CMTS lahko omogoča funkcionalnosti usmerjevalnika. Kabelski modem kot L2 naprava mora premoščati IPv6 promet. Pogoj: kabelski modem in CMTS morata biti skladna z DOCSIS 3.0 specifikacijo (omogočata prenos multicast in unicast IPv6 promet).

- Kabelsko (HFC) omrežje z dvojnim skladom, IPv6 podpira CMTS in samostojni usmerjevalni prehod

Če ima naročnik poleg modema še usmerjevalni prehod, mora imeti polno podporo za IPv6. Usmerjevalni prehod posreduje IPv4 in IPv6 promet. Če se uporablja za IPv6 povezljivost tunelski mehanizem (npr. 6to4), mora usmerjevalnik to podpirati. Za usmerjevalni prehod predstavlja naslednji skok CMTS (če deluje v funkciji L3 naprave) ali robni usmerjevalnik. CMTS je tako, kot v prejšnjem primeru nadgrajen na dvojni sklad ter lahko vsebuje funkcionalnosti robnega usmerjevalnika. Kabelski modem kot CMTS tako, kot v prejšnjem primeru, morata biti skladna z 3.0 DOCSIS specifikacijo.

- Kabelsko (HFC) omrežje z dvojnim skladom, IPv6 podpira CMTS ter kabelski modem in usmerjevalni prehod, ki sta združena v eni napravi

V tem scenariju kabelski modem vključuje funkcionalnosti usmerjevalnega prehoda, zato mora imeti naprava podporo za dvojni sklad in IPv6 multicast in unicast promet. CMTS je nadgrajen na dvojni sklad. Oprema pri naročniku, kot pri operaterju mora imeti polno podporo za DOCSIS 3.0.

V kabelskih omrežjih poleg naštetih možnosti, lahko tako kot pri DSL dostopovnem omrežju, IPv6 povezljivost omogočimo tudi z uporabo L2 tuneliranja preko VPN (L2VPN). V tem primeru CPE naprava naročnika (usmerjevalni prehod), Ethernet okvirje v katerem je IPv6 glava in koristna vsebina ovije v DOCSIS okvirje ter jih preko kabelskega omrežja prenese

do CTMS. CMTS DOCSIS okvirje, ki pridejo od posameznega kabelskega modema odstrani, ter jih na podlagi MAC naslova kabelskega modema mapira v ustrezni VLAN ter pošlje naprej proti IPv6 usmerjevalniku, kjer se izvaja združevanje (agregacija) prometa in IPv6 usmerjanje. CMTS pri tem vodi interno bazo mapiranja kabelski modem-VLAN. Na podlagi VLAN oznak, se IPv6 promet naročnikov lahko združuje v enotno logično omrežje VPN. Vsa politika usmerjanja med VLAN logičnimi kanali (med kabelskimi modemi) se izvaja na usmerjevalniku. Ker se za prenos IPv6 prometa uporablja L2VPN tuneliranje, se v tem scenariju mora izvesti nadgradnja na dvojni sklad le pri gostitelju in usmerjevalnem prehodu. Kabelski modem in CMTS lahko ostaneta IPv4 napravi. Naslavljanje usmerjevalnih prehodov s IPv6 predpono se lahko izvaja bodisi preko avto konfiguracijskega mehanizma SLAAC (angl. Stateless Address Auto-Configuration) z uporabo Neighbor Discovery (Router Advertisment) protokola bodisi preko DHCPv6 strežnika (DHCP Prefix Delegation). Izbira naslavljanja je lahko pogojena tudi z vgrajenimi funkcionalnostmi prehoda (usmerjevalnik mora podpirati DHCPv6 'Stateful' in 'Stateless' način).

Pri načrtovanju kabelskega omrežja za zagotavljanje IPv6 storitev je potrebno poleg že naštetih sprememb, posebno skrb posvetiti tudi zagotavljanju kvalitete storitve (QoS), varnosti in upravljanju naročnikov, modemov in drugih naprav. Ker se v kabelskih omrežjih ne zagotavlja samo Internet, je potrebno na IPv6 vzpostaviti tudi opremo, ki zagotavlja storitev IPTV (Televizijski komunikator - STB) ter govorne storitve – VoIP (zamenjava medijskega terminalnega adapterja in VoIP terminala).

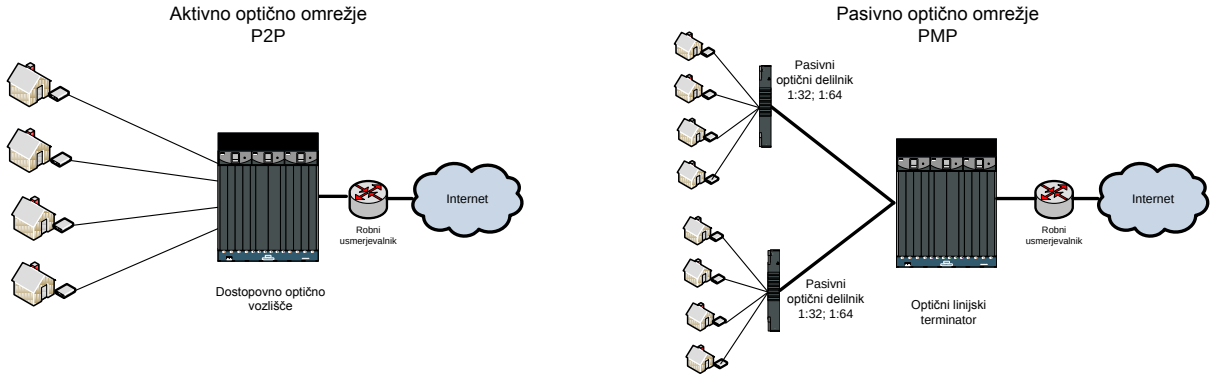
Arhitektura hibridno optičnega-koaksialnega omrežja (angl. HFC-Hybrid Fiber Coax) je kombinacija optike, ki predstavlja hrbtenico omrežja in koaksialnega vodnika, ki se uporablja v zadnjih nekaj sto metrih na stranskih in odcepnih vejah pred priklopom naročnika. Tako, kot pri DSL tehnologiji, je tudi pri hibridno optično-koaksialnih omrežjih trend, da se optika in pripadajoča oprema čim bolj približa uporabnikom.

6.2.3 Optična dostopovna omrežja

Medtem, ko DOCISIS 3.0 kot kombinacija optičnega in kabelskega dostopovnega omrežja omogoča kabelskim operaterjem s pomočjo združevanja kanalov bistveno povečanje podatkovnega prenosa, po najbolj optimističnih napovedi ne more doseči niti 15% zmogljivosti, kot jo omogoča čisto optično dostopovno omrežje. Z združevanjem kanalov, lahko sicer povečamo podatkovno hitrost, vendar gre ta hitrost na račun manjšega števila TV kanalov, ki jih lahko na ta način prenašamo skozi HFC omrežje. Poleg tega optično omrežje za razliko z HFC omogoča simetrični prenos podatkov. Optično omrežje lahko sicer v idealnih pogojih primerjamo z VDSL2 tehnologijo, vendar primerjava zdrži le na zelo kratkih razdaljah.

Optično dostopovno omrežje se sestoji iz optičnega dostopovnega vozlišča (optičnih stikal), optičnega delilnika in CPE naprav (optičnih modemov). Osnovni povezovalni medij med napravami je enorodovno optično vlakno. Vlakno je med uporabniškim optičnim modemom in optičnim dostopovnim vozliščem lahko eno samo, ali pa imamo dva ali več vlaken. V primeru, da za povezavo uporabljamo eno samo vlakno, z različno valovno dolžino ločujemo promet proti uporabniku in od uporabnika, v primeru, da pa imamo dva vlakna, lahko eno vlakno uporabljamo za promet proti naročniku in drugo za promet proti omrežju. V primeru, da imamo dva vlakna obstaja tudi druga možnost, kar je primer rešitve družbe Telekom Slovenije. Eno vlakno se uporablja za dvostranski prenos podatkovnega prometa (Internet, VoIP..), drugo pa se uporablja za enosmerni prenos (proti naročniku) analognega RF TV signala.

V optičnih dostopovnih omrežjih srečamo dve najbolj pogosti topologiji omrežja: točka-točka (P2P-Point-to-Point) in točka-več točk (P2MP-Point-to-Multipoint). Optična omrežja so lahko aktivna (vsebujejo aktivne elemente-optične ojačevalnike) ali pa pasivna. P2MP arhitektura lahko uporablja tehnologijo Ehernet PON (EPON-Ethernet Passive Optical Network), Gigabit PON (GPON) ali Gigabit Ethernet PON (GEPON). Slika 22 prikazuje koncept aktivnega in pasivnega optičnega omrežja.



Slika 22: Aktivno in pasivno optično omrežje

Pri topologiji točka-točka (P2P) ima vsak naročnik optični omrežni terminator –optični modem (ONT-Optical Network Terminator), ki ga lahko dopolnjuje usmerjevalnik/stikalo ali so vse funkcionalnosti združene v eni sami napravi (CPE-Customer Premises Equipment). Na CPE je priklopljeno optično vlakno, ki se zaključuje v prostorih operaterja na optičnem delilniku oz. optičnem vozlišču (angl. Access Node oz. MSAN - Multiservice Access Node). Ker ima pri topologiji P2P vsak naročnik do vozlišča samostojno optično vlakno, lahko v celoti razpolaga s pasovno širino, ki jo omogoča vlakno in aktivna oprema. Za podatke od vozlišča do uporabnika se uporablja valovna dolžina 1490 nm, ki jo modulira zmogljiv laser, za podatke od uporabnika do vozlišča pa se uporablja enostavna laser dioda (FP laser dioda), ki modulira z valovno dolžino 1310nm. Cenejša laser dioda poceni izdelavo modema, obenem pa operaterju zniža stroške (CAPEX). V kolikor se na istem vlaknu prenaša še video, se uporablja valovna dolžina 1550nm, ki je modulirana z laserjem in ojačana z ojačevalnikom EDFA (angl. EDFA- Erbium-Doped Fiber Amplifier).

Pri topologiji točka-več točk (P2MP), se posamezno vlakno, ki je povezano na enoto optičnega linijskega terminatorja (OLT-Optical Line Termination Unit) na strani operaterja najprej pripelje do vmesnega vozlišča (pasivnega optičnega delilnika). Signal se na delilniku deli na 32, 64 ali več optičnih vlaken, ki so potegnjeni naprej do naročniških optičnih omrežnih enot (ONU-Optical Network Unit). Ker si pri topologiji P2MP več naročnikov deli isti medij (optično vlakno) se informacija v smeri od omrežja proti naročniku prenaša v načinu broadcast (razpršeno) in z delitvijo pasovne širine, od uporabnika proti omrežju pa se za sodostop do medija uporablja časovno multipleksiranje (TDMA-Time Division Multiplex Access). Ker pa TDM način sodostopa ne omogoča potratnih multimedijskih storitev, kot je IP TV ali VoD v HD ločljivosti, se sedaj TDM-PON nadgrajuje na WDM-PON (WDM-PON Wavelength Divison Multiplexing) tehnologijo. WDM-PON za sodostop namesto časovnega multipleksiranja uporablja sodostop z razvrščanjem valovnih dolžin, kar bistveno bolje izkorišča pasovno širino optičnega vlakna.

Obe predstavljeni topologiji imata svoje prednosti in slabosti. Z vidika stroškov je P2P topologija vsekakor dražja rešitev, saj zahteva bistveno več vlaganja v infrastrukturo optičnih vlaken. Po drugi strani pa prinaša bistveni boljši izkoristek pasovne širine, kot ga omogoča topologija PMP, saj ni potrebe po delitvi pasovne širine.

Ker celotno optično dostopovno omrežje predstavlja le fizični nivo OSI modela in način prenosa podatkov, nima direktnega vpliva na implementacijo IPv6. Opisane naprave optičnega dostopovnega omrežja (OLT, ONU oz. ONT) morajo transparentno premoščati IPv6 unicast in multicast promet. Posodobitve pa se morajo izvesti v domačem omrežju (gostitelj mora podpirati dvojni sklad, domači usmerjevalnik mora podpirati IPv6) in na drugih segmentih operaterjevega omrežja (BRAS, robni usmerjevalnik, storitve: DNS, DHCP, AAA, VOIP, IPTV…). Vse naštete naprave morajo v celoti podpirati IPv6.

6.3 IPv6 in prevedba imen

Če smo si lahko veliko IPv4 naslovov in pripadajočih domenskih imen še nekako zapomnili, si IPv6 naslovov zaradi njihove 128 bitne dolžine zapisa zapomniti ne bomo mogli, ali pa bo to vsaj zelo težko. Iz tega razloga je podpora za prevedbo domenskih imen in IPv6 naslovov kritični del infrastrukture ter predpogoj za uspešno uvedbo IPv6. Poznamo dva ključna protokola, ki nam danes omogočata prevedbo IPv6 naslovov in domenskih imen. To sta DNS in LLMNR.

6.3.1 DNS

Eno najpomembnejših vlog pri prehodu iz IPv4 na IPv6 ima sistem domenskih imen (angl. DNS - Domain Name System), ki pretvarja domenska imena v IP naslove in obratno. DNS strežniki predstavljajo porazdeljeno hierarhično podatkovno bazo, ki vsebuje IP naslove vseh registriranih domenskih strežnikov ter njihova pripadajoča domenska imena. Govorimo o porazdeljeni in hierarhični bazi, ker so podatki o posameznih domenah strukturirani po nivojih ter ker posamezen strežnik vsebuje le del podatkov, preostale potrebne podatke pa pridobi s pomočjo poizvedb pri drugih DNS strežnikih.
Hierarhijo DNS strežnikov sestavljajo vrhnji, korenski (ang. Root) DNS strežniki, domene vrhnjega sloja (angl. TLD-Top Level Domain) ter domene drugega nivoja (angl. Second level domain) in pod domenski (angl. Sub domain) DNS strežniki. Administrativno vsak nivo ali vozlišče v hierarhiji predstavlja ločnico, ki je pod upravljanjem posamezne avtoritete določenega imenskega prostora. Administrativne ločnice ali deli domenskega imena predstavljajo samostojno DNS cono. DNS cona lahko vsebuje samo eno domeno ali združuje več domen in pod domen, v odvisnosti od strukture in administrativne avtoritete, ki je poverjena s strani upravljavca. Korenski strežniki, ki so najvišje v hierarhiji predstavljajo eno DNS cono, ki se imenuje korenska cona (angl. Root zone). Korenska cona je pod administrativnim upravljanjem organizacije IANA. IANA kot glavni upravljavec DNS korenske cone s predpisano politiko in procedurami določa, kdo je odgovoren in upravlja s posamezno domeno vrhnjega sloja (TLD). Korensko cono sestavlja 13 logičnih korenskih strežnikov, ki so poimenovani s črkami od A do M in, ki so porazdeljeni kot gruča (angl. Cluster) preko 150 fizičnih strežnikov. Ker so korenski strežniki najbolj kritični del interneta in ker so prvi korak pri prevedbi domenskih imen v IP naslove, so postavljeni v strogo varovanih okoljih na različnih lokacijah sveta. Uspešne DNS poizvedbe se zaradi učinkovitosti sicer shranjujejo v lokalni medpomnilnik (angl. cache) vsakega DNS strežnika, vendar v kolikor dalj časa (odvisno od nastavljene vrednosti TTL) nimamo povezljivosti z vsaj enim korenskim

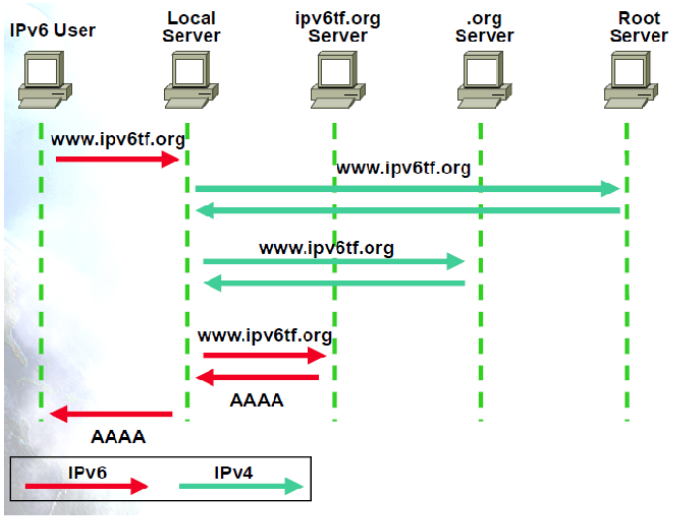
strežnikom, potem ne moremo dostopati tudi ostalih domen oz. dostop do interneta bi bil onemogočen.
Korenski imenski strežniki (angl. NS-Name Server) vsebujejo spisek NS zapisov imenskih strežnikov za domene vrhnjega sloja (TLD) ter A ali AAAA IP naslovne povezovalne (angl. glue) zapise, ki kažejo na te imenske strežnike. Povezovalne zapise oz. IP naslove potrebujemo, če želimo določiti imenske strežnike posamezne domene na konkretna določena imena gostiteljev, ki so pod okriljem domene same. Npr., če želimo določiti imenska strežnika (ns1.example.com in ns2.example.com), da sta odgovorna za domeno example.com potem moramo zagotoviti tudi povezovalni zapis, to sta IP naslova obeh omenjenih strežnikov (ns1.example.com in ns2.example.com). Če za imenske strežnike teh povezovalnih zapisov (IP naslovov) nimamo določenih, potem poizvedbe za konkretno domensko ime ne bodo uspešne.

Trenutno (4Q 2009) je pri organizaciji IANA registriranih 280 TLD strežnikov, ki jih sestavlja 21 splošnih gTLD strežnikov, ki opredeljujejo generične domene (.com, .org, .biz) ter 259 ccTLD strežnikov, ki opredeljujejo kode posameznih držav (angl. ccTLD-Country code TLD). V Slovenski .Si TLD domeni je trenutno (4Q 2009) registriranih 73.950 drugo nivojskih domen[18]. Vsak TLD strežnik mora imeti v svoji bazi vpisane t.i. avtoritativne imenske strežnike, ki so odgovorni, da dajejo odgovore za posamezno domeno. Imenski strežniki morajo biti v DNS bazi zapisani s polnim kvalificiranim domenskim imenom (angl. FQDN-Fullly Qualified Domain Name), ki vključuje ime strežnika, ime domene ter ime domene vrhnjega sloja (TLD), npr. ns1.example.com. Sintaksa FQDN zapisa določa, da so domene med seboj ločene s piko ".". Za posamezno domeno mora obstajati primarni DNS strežnik in vsaj en sekundarni DNS strežnik.
Veliko TLD strežnikov pokriva tako generične kode kot kodo svoje države. Ti strežniki skupaj z drugo nivojskimi strežniki, ki hierarhično spadajo pod TLD strežniki so praktično najbolj pomemben in najbolj obremenjen del sistema DNS.

Podatki v posameznem DNS strežniku so organizirani v t.i. virih zapisov (angl. RR-Resource Record). Vsako domensko ime ima eno ali več virov zapisov, ki se nanašajo na različne tipe podatkov, kot so: SOA, NS, A, AAAA, MX, CNAME, HINFO, TXT. Npr. RR zapis A (angl. Address) zapis vsebuje IPv4 naslov, AAAA RR zapis vsebuje IPv6 naslov, MX (angl. Mail exchange) RR zapis opredeljuje IP naslov poštnega strežnika, ki je zadolžen za sprejem in oddajanje e-pošte za posamezno domeno.

Če želimo uporabljati IPv6 omrežja in naprave z IPv6 povezljivostjo, je zato predpogoj, da DNS strežniki vsebujejo tudi IPv6 zapise naslovov (AAAA) ter, da sprejemajo in odgovarjajo na poizvedbe preko IPv6 protokola.
Slika 23 nam prikazuje primer poizvedbe za IPv6 naslov v sistemu DNS.

[18] Vir: http://www.ipdn.tw/DomainNameResources/ccTLDDNRegistrationObservedStudy52Country



Slika 23: Poizvedba za IPv6 naslov v DNS

Vir: 6Deploy
(http://www.6deploy.org/workshops/kenya_20080617/IPv6%20Applications%20&%20DNS%20IPv6.pdf)

Ustrezne IPv6 zapise lahko v DNS strežnik vpišemo ne glede na to, ali DNS strežnik uporablja IPv6 protokolni sklad ali samo IPv4 sklad. Predpogoj za to je seveda kompatibilnost programske opreme DNS strežnika z internetnim osnutkom RFC 3596, ki predpisuje potrebne DNS razširitve za uporabo protokola IPv6. Glavne dopolnitve z razširitvijo so predvsem nov tip zapis vira, ki lahko sedaj shrani tudi IPv6 naslove (AAAA Record type), predpisuje nov podatkovni format AAAA (AAAA Data format), omogočil je spremembe pri poizvedbah tipa AAAA (AAAA Query), nov je tekstualni format AAAA zapisa (Textual format of AAAA record) ter nova domena IP6.ARPA (IP6.ARPA domain) (IETF, 2003).
V DNS-u AAAA zapis vira vsebuje 128 bitni IPv6 naslov, ki je shranjen v polju RDATA. Četverček AAAA (Quad A) izhaja iz dejstva, da so 128-bitni IPv6 naslovi 4x daljši kot 32-bitni IPv4 naslovi. Omenjeni RFC 3596 predpisuje tudi potrebne spremembe na obstoječih tipih poizvedb, ki jih potrebujemo pri procesiranju poizvedb imenskih imen, lokacij storitev (angl. SRV-Location of services) in zapisih za poštne strežnike (MX) tako, da sedaj podpirajo tako AAAA zapis za IPv6 naslove kot A zapis za IPv4 naslove.

Če želimo npr. izvedeti IPv6 naslov določenega strežnika, mora programski servis-tolmač (angl. Resolver) izvesti AAAA poizvedbo (ang. Lookup) v DNS bazi (polje Question Type vsebuje vrednost 0x1C ali poizvedbo tipa Any polje Question Type vsebuje vrednost 0xFF). Poizvedba tipa Any se uporablja, kadar imamo v DNS bazi več domenskih imen, ki se sklicuje na IPv6 naslov (npr. spletni strežniki). Za obratne poizvedbe (domensko ime iz IPv6 naslova) je v razširitvi sedaj vzpostavljeno polje IPv6.ARPA, ki se imenuje tudi poizvedba z kazalnikom (ang. Pointer queries). Če bi izvajali poizvedbo domenskega imena iz IPv6 naslova 2001:1470:0:47::1, bi nam zapis s kazalnikom (ang. PTR-Pointer record), podal vrednost, ki je obratna vrednost IPv6 naslova (brez okrajšav):
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.4.0.0.0.0.0.0.0.7.4.1.1.0.0.2.IP6.ARPA (vir:
http://www.hscripts.com/tools/HDNT/rdns-lookup.php)

AAAA zapis DNS bazi ima naslednjo strukturo (Straus, 2009):

Name	IN	AAAA	*Address*
lizum2-v6.arnes.si	IN	AAAA	2001:1470:0:47::1

Slika 24 predstavlja primer zapisov v DNS strežniku za domeno rhadamanthe.

```
Example: In zone file rennes.enst-bretagne.fr
@           IN          SOA         rsm.rennes.enst-bretagne.fr. fradin.rennes.enst-bretagne.fr.
                        (2005040201 ;serial
                        86400       ;refresh
                        3600        ;retry
                        3600000     ;expire}

                        IN          NS          rsm
                        IN          NS          univers.enst-bretagne.fr.
[...]
ipv6        IN          NS          rhadamanthe.ipv6
            IN          NS          ns3.nic.fr.
            IN          NS          rsm
;
rhadamanthe.ipv6                    IN          A           192.108.119.134
                                    IN          AAAA        2001:660:7301:1::1
[...]
```

Slika 24: Zapisi v DNS strežniku

Vir: 6Deploy (http://www.6deploy.org/tutorials/090-6deploy_ipv6-dns_v0_2.pdf)

Iz slike je razvidno, da potrebujemo IPv4 (A 192.108.119.134) povezovalni zapis (angl. Glue record), če želimo rhadamanthe doseči preko IPv4 transporta in IPv6 (AAAA 2001:660:7301:1::1) povezovalni zapis če želimo rhadamanthe doseči preko IPv6 transporta.

Vsakemu DNS strežniku se mora ob instalaciji naložiti spisek vseh 13 korenskih DNS imenskih strežnikov s pripadajočimi naslovi IPv4 in IPv6 naslovi. Spisek strežnikov je v DNS strežniku shranjen v datoteki root.hints, dosegljiv pa je tudi preko FTP naslova: ftp://ftp.internic.net/domain/named.root. Kot je razvidno iz spiska na omenjenem naslovu (4Q 2009) lahko ugotovimo, da trenutno le 7 od 13 korenskih strežnikov vsebuje zapis vira (angl. RR - Resource Record) za AAAA (IPv6) zapis, kar pomeni, da so ti strežniki dosegljivi tudi preko IPv6 transporta. Čeprav ima večina drugih DNS korenskih strežnikov tudi IPv6 naslov, jih je težko objaviti v korenski coni. Omejitev je predvsem tehnične narave, saj obstaja omejitev pri kreiranju DNS odgovorov. DNS sporočila, ki vsebujejo poizvedbe in odgovore nanje, se namreč večinoma pošiljajo s pomočjo UDP protokola. RFC 1035 (IETF, 1987) omejuje velikost UDP DNS sporočil na 512 bytov, pri čemer ne šteje IP in UDP glav. V primeru, da je sporočilo daljše od navedene omejitve, se ga del odreže, v glavi DNS sporočila pa se polje Truncation Flag postavi na vrednost 1. V tem primeru se mora DNS sporočilo poslati s pomočjo TCP protokola, ki pa je počasnejši in povečuje režijo, vendar ni omejen z dolžino paketa. Problem rezanja UDP DNS sporočila je v tem, da protokol odreže del, ki vsebuje povezovalne (glue) zapise IP naslovov imenskih strežnikov posamezne domene. Izpustitev povezovalnih zapisov je posebno kritično, kadar poizvedbe delamo k korenski coni. Omejitev 512 bytov pri prenosu UDP DNS paketov rešuje mehanizem EDSNS0 (angl. Extension Mechanisms for DNS), ki je opisan v internetnem standardu RFC

2671. Razširitveni mehanizem mora biti implementiran tako na strani imenskih strežnikov, kot na strani tolmačev (resolverjev).
EDSN0 je sicer tudi ključni element pri uvedbi varnostne razširitve DNS sistema - DNSSEC (angl. DNS Security Extension).
Ker EDSN0 razširitev ni bila še implementirana na vseh strežnikih, je posledica temu, da trenutno (4Q 2009) samo 64% (fizičnih) korenskih DNS strežnikov lahko obdeluje poizvedbe in odgovore preko IPv6 protokola.

Čeprav je DNS strežnik eden od najpomembnejših entitet pri prehodu na IPv6, je praviloma najenostavnejši del migracije. Če želimo, da IPv6 deluje tudi v vrhnjih TLD avtoritativnih strežnikih morajo biti na imenskih strežnikih izpolnjeni naslednji pogoji[19]:

- imeti mora IPv6 naslov in čisto (angl. native) povezljivost na IPv6 omrežje iz katerega je tudi dosegljiv,
- v korenski coni (angl. root zone) mora imeti AAAA zapis svojega povezovalnega (glue) IPv6 naslova,
- na poizvedbe mora biti sposoben odgovarjati tudi z AAAA IPv6 zapisom.

V novembru 2009 ima že 80% (224) TLD imenskih strežnikov tudi IPv6 naslov[19]. Pri tem ima 64,6% (181) od vseh 280 TLD strežnikov tudi svoj IPv6 povezovalni naslov zapisan tudi že v korenski coni. Med njimi je tudi ARNES (Akademsko in raziskovalna mreža Slovenije), ki upravlja s slovensko vrhnjo domeno, kodo .si TLD. Arnes ima čisto IPv6 povezljivost na pan evropsko omrežje GEANT, obenem pa je že v svojih mehanizmih za avtomatsko preverjanje DNS-ov pri vpisu ali spremembi domenskih strežnikov že omogočil IPv6 zapise. Tudi njegovi imenski strežniki imajo v korenski coni že zaveden IPv6 zapis AAAA. Če v formo za spremembo ali vpis DNS strežnikov na svoji domeni vnesemo imena strežnikov s pripadajočimi IPv6 naslovi, bo skripta Arnesovega DNS strežnika za preverjanje veljavnosti in pravilne konfiguracije DNS zone našla tudi AAAA zapise, s tem pa tudi IPv6 naslove in jih pravilno vnesla v svoj DNS strežnik .si TLD.

6.3.2 mDNS

Pretvorbo domenskih imen in IPv6 naslovov, pa nam omogoča tudi nov protokol mDNS (angl. multicast DNS) oziroma LLMNR (RFC 4795), ki se uporablja takrat, ko DNS strežnika v lokalnem omrežju ni. Protokol LLMNR (angl. LLMNR- Link-Local Multicast Name Resolution) nam omogoča pretvorbo tako za IPv4 kot za IPv6 odjemalce v lokalnem omrežju. Z uporabo protokola LLMNR si odjemalci med seboj izmenjajo enostavna poizvedovalna sporočila in njihove odgovore nanj, ne da bi bil v omrežju postavljen DNS strežnik ali pa, da bi računalniki imeli nastavljeno DNS konfiguracijo. IPv4 odjemalci za pretvorbo imen v lokalnem podomrežju uporabljajo protokol NetBIOS over TCP/IP (NetBT). IPv4 odjemalci z razpršenim (ang. Broadcast) NetBIOS sporočilom izvedejo poizvedbo v podomrežju. Računalnik oziroma vozlišče, ki ima iskani naslov v poizvedbi, se odzove ter pošlje svoj IPv4 naslov. Vendar NetBIOS deluje samo v okolju IPv4 omrežja. V kolikor je NetBIOS v sistemu izklopljen, mora računalnik uporabljati DNS strežnik, ali pa je potrebno parametre (IP naslove in pripadajoče domenska imena) vpisati v datoteko Hosts.
Primer uporabe LLMNR protokola je npr. začasno vzpostavljeno ad hoc (neposredna povezava dveh računalnikov) podomrežje WLAN uporabnikov (IEEE 802.11). Uporabniki v takem omrežju lahko z uporabo protokola LLMNR med seboj pretvarjajo domenska imena in IPv6 naslove, ne da bi bil potreben v omrežju DNS strežnik. LLMNR sporočila uporabljajo

[19] Vir: http://bgp.he.net/ipv6-progress-report.cgi

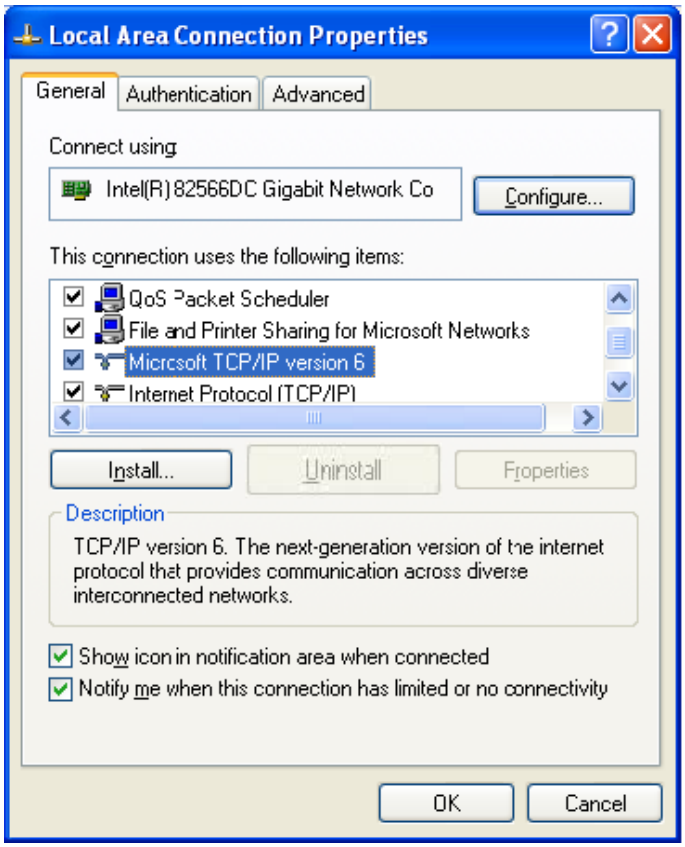
podoben format, kot se ga uporablja pri DNS sporočilih, razlika je le v uporabljenih vratih (zahteva in odziv nanjo uporablja vrata 5355), kjer se odziva posamezen odjemalec. Vsi IPv6 računalniki, ki uporabljajo LLMNR protokol poslušajo na mrežnem nivoju IPv6 multicast naslov FF02::1:3, njihove mrežne (Ethernet) kartice, na drugem nivoju (OSI) pa poslušajo Ethernet okvirje, ki vsebujejo ciljni multicast naslov 33-33-00-01-00-03.

6.4 Podpora IPv6 v operacijskih sistemih

Eden bistvenih elementov, ki nam omogoča uporabo IPv6 protokolnega sklada so operacijski sistemi. Večina sodobnih operacijskih sistemov v celoti podpira vse potrebne funkcionalnosti IPv6 protokola.

6.4.1 Microsoft Windows

Microsoft je z IPv6 uvedel z operacijskim sistemom Windows XP z vključenim servisnim popravkom 1. Ta vključuje tudi druge IPv6 funkcionalnosti, kot je podpora za vtičnike (angl. Socket), Internet Explorer in orodja, kot so Ping (Ping6.exe) in Traceroute (tracert6.exe). IPv6 tudi podpirata Windows 2000 (potrebujemo SP1-Microsoft IPv6 Technology Preview) in Windows Server 2003. Ker IPv6 privzeto pri navedenih sistemih ni nameščen, ga je potrebno namestiti posebej. Namestitev se lahko izvede s pomočjo ukazne vrstice (v ukazno vrstico vpišemo ukaz '*IPv6 install*') ali pa s pomočjo grafičnega vmesnika (GUI), kjer se dodajo mrežne komponente za posamezni mrežni vmesnik (Install/Add protocol/ Microsoft TCP/IP version 6).



Slika 25: Windows XP namestitev podpore za IPv6

V Windows XP, Windows 2000 in Windows Server 2003 manjka podpora za DHCPv6 odjemalca, kar se lahko rešuje s pomočjo dodatne programske opreme, kot je npr. Dibbler[20]. Manjka tudi podpora za PPPv6, IPv6 Mobility ter IPv6 souporaba datotek in tiskalnikov (File and print sharing). Popolno podporo IPv6 z vsemi potrebnimi funkcionalnostmi, vključno s požarno pregrado in zagotavljanjem zasebnosti zagotavljajo šele Microsoft Vista, Windows Server 2008 in Windows 7. Navedeni sistemi imajo IPv6 protokolni sklad že privzeto nameščen in aktiviran. Omogočajo tudi uporabo protokola DHCPv6 (Stateless in Stateful), PPPv6 preko PPPoE ter vzpostavitev tunelov 6to4, Teredo ter ISATAP. Podpora IPv6 Stateful filtriranju prometa je omogočeno šele od Windows XP SP2 naprej. IPv6 podporo ima tudi operacijski sistem Windows CE od verzije 4.2 naprej.

6.4.2 BSD

Eden prvih pionirjev na področju implementacije IPv6 v svojem protokolnem skladu je operacijski sistem BSD (angl. BSD-Berkley Software Design). BSD ima veliko izpeljank kot so: OpenBSD, FreeBSD, NetBSD. Vse naštete izpeljanke BSD sistema v svojem jedru (KAME) v celoti podpirajo IPv6. Trenutno so vsi BSD sistemi kompatibilni z drugimi sistemi prav zaradi široke razširjenosti KAME protokolnega sklada. FreeBSD za filtriranje IPv6 prometa uporablja tri paketne filtre (pf, ipf in ipfw), ki v celoti podpirajo IPv6.

6.4.3 Linux

Tudi Linux je imel podoben projekt, kot BSD, ki se imenuje USAGI (angl. UniverSAl playGround for Ipv6). Iniciativa je prvo izhajala iz ideje KAME, kasneje pa so Linux distribucije začele z razvojem lastnega protokolnega sklada USAGI, ki je v uporabi še danes. Projekt USAGI ni samo omejen na IPv6 funkcionalnosti, ki se izvajajo v jedru operacijskega sistema, temveč razvijajo tudi aplikacije, ki temeljijo na IPv6. Podpora za IPv6 filtriranje prometa je vgrajena v samem jedru od verzije 2.6.20 dalje (netfilter/IP6tables).

6.4.4 MAC OS

Operacijski sistem MAC OS je z IPv6 podporo začel z MAC OS X (10). IPv6 funkcionalnost je implementirana v jedru KAME, ki izhaja iz FreeBSD. IPv6 je nameščen privzeto tudi v novejših sistemih, kot sta Leopard (MAC OS Xv10.5) in Snow Leopard (MAC OS Xv10.6). MAC OS X zna pridobiti omrežne IPv6 parametre iz SLAAC protokola (Router Advertisment), nima pa še uradne podpore za DHCPv6. MAC OS X ima podporo za IPv6 filtriranje, saj uporablja FreeBSD paketno filtriranje z upoštevanjem vseh stanj (ipfw Stateful filtering).

6.4.5 Solaris

Prva konkretna podpora IPv6 protokolnemu skladu v operacijskem sistemu Solaris Unix je bila narejena z verzijo 8. Zadnja verzija Solaris 10 ima sedaj polno podporo IPv6 v katero so vključene tudi dodatne funkcionalnosti in pomožni protokoli (DHCPv6 odjemalec, PPPv6, tunelski mehanizmi 6to4). Solaris ima od verzije 10 polno podporo IPv6 filtriranju prometa (TCP in UDP Stateful filtriranje).

6.4.6 Cisco Systems

Cisco IOS (Internet Operating System) je primarni operacijski sistem Cisco Systems usmerjevalnikov, LAN stikal in drugih omrežnih infrastrukturnih komponent. Cisco je zelo

[20] Dibbler: http://klub.com.pl/dhcpv6/

aktiven pri implementaciji IPv6 arhitekture znotraj IETF standardizacijskih naporov po uvedbi IPv6. Je tudi eden od ustanovnih članov IPv6 Foruma. Cisco je uvedel večino IPv6 tranzicijskih mehanizmov (dvojni sklad, tuneliranje, translacija), kot del svojih IPv6 rešitev.
Svoj načrt uvedbe IPv6 v svojem operacijskem sistemu IOS je prvič napovedal v letu 2000, leta 2001 pa je IPv6 že bil implementiran v prvi komercialni izdaji (IOS 12.2T). Z verzijo IOS 12.0S je bil IPv6 uveden v jedrni infrastrukturi. Danes večina Cisco usmerjevalnikov in druge mrežne opreme tako na strani ponudnikov omrežja, poslovnih uporabnikov in naprav za širokopasovni dostop z ustrezno verzijo IOS v celoti podpira vse funkcionalnosti IPv6. Več konkretnih informacij je dosegljivih na spletnih straneh Cisco System: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

6.4.7 Juniper Networks

Juniper Networks je poleg Cisco Networks eden glavnih dobavitelj jedrnih (T-serija) in robnih usmerjevalnikov (M-serija) v omrežjih operaterjev in ponudnikov dostopa do Interneta. Operacijski sistem, ki poganja Juniper usmerjevalnike je JUNOS, ki temelji na odprtokodnem operacijskem sistemu FreeBSD. IPv6 je polno podprt od verzije 5.1 (November 2001) naprej. V nekaterih vmesnih verzijah JUNOS-a so se kazale tendence proizvajalca po zaračunavanju dodatne licence za IPv6 modulu, a na srečo v zadnjih verzijah tega ni več. IPv6 je sedaj del sistema, ki ne zahteva doplačila. Obe seriji usmerjevalnikov (M in T) imata strojno podporo obdelave in posredovanje IPv6 prometa.

6.5 IPv6 migracija na spletnih in poštnih strežnikih

Pomemben del migracije na IPv6 so poleg storitve domenskih imen (DNS) tudi storitve, ki jih omogočajo spletni, poštni in drugi strežniki, ki omogočajo internetne storitve. Te morajo zagotavljati svoje storitve tudi uporabnikom, ki do njih dostopajo samo preko IPv6 protokola (IPv6 otoki). Raziskava, ki je zajela 206.741.990 spletnih strani, ki jo je v januarju 2010 objavilo podjetje Netcraft[21], kaže na to, da daleč največ spletnih strežnikov uporablja programsko opremo - aplikacijo Apache. Uporablja jo kar 111 milijonov strežnikov oziroma kar 53% vseh spletnih strežnikov. Apache je podprt za množico operacijskih sistemov, kar je verjetno tudi delni razlog njegove velike razširjenosti. Apache je omogočal IPv6 podporo že v letu 2000 z verzijo 1.3.11 na katero smo morali namestiti popravek: (ftp://ftp.kame.net/pub/kame/misc/apache-1.3.11-v6-20000204a.diff.gz). Od verzije 2.0 pa je Apache IPv6 polno kompatibilen, tako da lahko sprejema in odgovarja na zahteve, ki prihajajo preko IPv4 ali IPv6. Predpogoj je seveda, da je spletni strežnik povezan (tudi) v IPv6 omrežje (uporablja oba protokolna sklada).

Pol manjše število spletnih strežnikov (49 milijonov strežnikov oz. 24%) pa ima nameščeno programsko opremo Microsoft Internet Information Services (IIS). Microsoft IIS je nabor Internetnih storitev (programskih modulov), ki so del operacijskega sistema Microsoft Windows. IIS zagotavlja storitve kot so FTP (angl. File Transfer Protocol), FTPS (FTP čez SSL), SMTP (angl. Simple Mail Transfer Protocol), NNTP (angl. Network News Transfer Protocol) in HTTP/HTTPS (angl. Hypertext Transfer Protocol). IPv6 podporo je Microsoftov IIS dobil z verzijo 6.0 (Windows Server 2003). IIS 6.0 zagotavlja IPv4 in IPv6 spletne storitve (HTTP in HTTPS strežnik) ne omogoča pa IPv6 FTP, SMTP in NNTP storitev. FTP in FTPS servisa sta IPv6 podporo dobila z IIS 7.0.
SMTP storitev pošiljanja pošte s podporo IPv6 je dobil Microsoft Exchange od verzije 2007 SP1 naprej. Poleg Microsoft Exchange 2007 SP1 storitev pošiljanja pošte (SMTP) preko

[21] Netcraft: http://news.netcraft.com/archives/2010/01/07/january_2010_web_server_survey.html

IPv6 omogočajo med drugim še: Sendmail (od verzije 8.10), Postfix (od verzije 2.2) in Exim (od verzije 4.30), Lotus Domino (od verzije 7.0).

6.6 IPv6 v lokalnih omrežjih

Večina današnjih uporabnikov se v širokopasovni Internet povezuje bodisi preko xDSL, kabelskega ali optičnega modema. Kot omenjeno, so modemi L2 naprave, ki transparentno prenašajo IPv4 ali IPv6 promet. V primeru, da je uporabnik z računalnikom direktno povezan na modem ter ima vzpostavljeno IPv6 preko IPv4 povezave bodisi z uporabo tranzicijskih mehanizmov (ISATAP, Teredo, Tunnel Broker, 6to4..) ali pa IPv6 povezljivost ponuja ponudnik dostopa, se vse seje vzpostavljajo na gostiteljskem IPv6/IPv4 računalniku. V prvem primeru mora gostiteljski operacijski sistem podpirati tranzicijske mehanizme, v drugem primeru pa mora imeti vgrajenega odjemalca PPPoE s podporo PPP čez IPv6 (IPv6CP). Ker bo vsaj v začetni fazi prehoda na IPv6 še vedno obstajala povezljivost preko IPv4, mora odjemalec podpirati tudi simultani prenos IPv4 in IPv6 prometa čez eno PPP povezavo. Ker je eden glavnih motivacijskih faktorjev za vpeljavo IPv6 tudi avto-konfiguracijski mehanizem za nastavitev globalnega in lokalnega IPv6 naslova, mora gostiteljski operacijski sistem podpirati bodisi IPv6 Stateless Address Autoconfiguration (SLAAC-RFC4862), bodisi Stateful DHCPv6 (RFC3315).

Drugi zelo pogosti primer povezljivosti uporabnika v širokopasovni Internet pa je preko L3 naprave, ki je usmerjevalni rezidenčni prehod (angl. RG-Residential Gateway). V tem primeru je prehod tista naprava, ki vzpostavlja PPP seje z robnim BNG (angl. Broadband Network Gateway) usmerjevalnikom. Trenutno le redki rezidenčni usmerjevalniki polno podpirajo IPv6 in druge pripadajoče protokole in tranzicijske mehanizme. Ker je spisek potrebnih funkcionalnosti, ki bi jih moral IPv6 rezidenčni usmerjevalnik podpirati zelo dolg in ker so določeni dokumenti šele v nastajanju (Broadband Forum, IETF), priporočamo ogled vsaj naslednjih dokumentov:

- Broadband Forum: TR-124i2 (Functional Requirments for Broadband Residential Gateway Devices)
- Broadband Forum: PD-192 (Residential Gateway (RG) IPv6 Requirements)
- IETF: Basic Requirements for IPv6 Customer Edge Routers
- Microsoft: IPv6 Support in Home Routers
- NIST: USGv6 Profile version1

7 ZAKLJUČEK

Veliko število uporabnikov interneta in posledično pomanjkanje IPv4 naslovnega prostora je snovalce interneta privedla do zasnove novega protokola, internetnega protokola verzija 6 – IPv6. Glavne prednosti IPv6 protokola pred IPv4 je večji naslovni prostor, večja podpora mobilnosti, omogoča učinkovitejši prenos telekomunikacijskega prometa, samodejno konfiguracijo mrežnih parametrov, transparentno komunikacijo od konca do konca, vsebuje varnostne mehanizme in mehanizme za nadzor kvalitete storitev ter še bi lahko naštevali. Protokol je standardiziran že več kot deset let, vendar še ne dosega masovne uporabe. Razlog je predvsem v pomanjkanju storitev, aplikacij in končnih naprav, ki bi dvigovale dodano vrednost sodobnejšemu IPv6 protokolu. Trenutno tudi še primanjkuje potrebnega strokovnega znanja, njegova vpeljava v omrežja pa zahteva finančna sredstva.

Kljub vsemu IPv6 že več let uspešno uporabljajo v raziskovalno-akademskih okoljih in drugih velikih omrežjih (6bone, CERNET2, Renater, GEANT2, FreeNET, Google, Hurricane Electric, Euro6IX, 6NET, 6WiN…). Trenutna gonilna sila in uporabniki IPv6 protokola so predvsem akademska okolja in Azija, ki zaradi skokovitega tehnološkega napredka že čuti pomanjkanje naslovnega prostora protokola IPv4. Njihove izkušnje kažejo, da je dobro vnaprejšnje načrtovanje in postopno uvajanje in vsaj v začetni fazi sobivanje obeh protokolov (IPv4 in IPv6) ključ do uspeha.

V Evropi je vzpostavljeno veliko iniciativ in raziskovalnih projektov z namenom predstavitve IPv6 ter želje po njegovi čimprejšnji vpeljavi v produkcijska okolja operaterjev, ponudnikov storitev, vsebin in drugih okolij. IPv6 spodbuja k razvoju bolj inovativnih internetnih aplikacij, zlasti tistih, ki v omrežja združujejo ogromna števila majhnih, enostavnih naprav. Napovedujejo, da bo IPv6 izboljšal upravljanje energije za cestno razsvetljavo in varčnih inteligentnih stavb, prek interneta bi lahko poceni in zanesljivo povezali daljinske senzorje v običajnih gospodinjskih aparatih, velike priložnosti se kažejo v avtomobilski industriji, obrambnem in varnostnem sektorju. To bi hkrati pomenilo spodbudo in priložnost za podjetja, da še naprej razvijajo inovacije in tako ustvarjajo naslednjo generacijo internetnih aplikacij, storitev in naprav.

Evropska komisija si je leta 2008 v Akcijskem načrtu za uvedbo IPv6 v Evropi zadala za cilj, da bo vsaj 25% evropskih uporabnikov imelo do leta 2010 možnost priklopa v internet prek IPv6 in tako imelo dostop do zanje najpomembnejših ponudnikov vsebin in storitev, ne da bi občutili razliko v primerjavi z IPv4. Komisija poziva ponudnike vsebin in storitev, da zagotovijo dostopnost svoje ponudbe tudi preko IPv6 dostopa, zainteresirane strani iz panoge, ki zdaj uporabljajo tehnologijo IP v okviru svoje temeljne dejavnosti, pa da premislijo o tem, da bi IPv6 uporabljale kot svojo glavno platformo za razvijanje aplikacij in naprav (senzorji, kamere..). Komisija spodbuja države članice EU, da omogočijo IPv6 dostop tudi do spletnih strani javnega sektorja in storitev e-uprave. Komisija ugotavlja, da so lahko javna naročila učinkovit način za pospešitev prehoda na IPv6 (vlada ZDA je npr. vsem svojim zveznim vladnim agencijam naročila, da prenesejo svoja osrednja hrbtenična omrežja na IPv6 do sredine leta 2008). Komisija spodbuja države članice, naj pripravijo svoja omrežja na IPv6 in pri obnavljanju pogodb za zunanje mrežne storitve zagotovijo, da te vsebujejo tudi določbe za povezljivost za IPv6 ter da vsa dobavljena oprema podpira IPv6.

Slovenija z vidika številčnosti projektov in konkretnih implementacij IPv6 zaostaja v primerjavi z drugimi evropskimi državami. Leta 2008 je bil ustanovljen IPv6 Task Force Slovenia, v juniju leta 2009 pa je bil ustanovljen Zavod go6. Žal vsaj po naših podatkih IPv6 Task Force

Slovenia ni izvajal vidnejših aktivnosti, zato pa je toliko bolj dejaven Zavod go6[22], ki združuje člane iz akademsko-raziskovalnega okolja, predstavnike državnih institucij, ponudnikov dostopa, internetnih storitev in multimedije, industrije in sistemskih integratorjev. Zavod go6 je neprofitne narave in vzdržuje odprto člansko platformo za pretok IPv6 znanja in storitev. Trenutno skupaj s strateškima partnerjema ARNES in LTFE predstavlja glavno iniciativo za prehod na IPv6 v Sloveniji.

Prve zametke implementacije IPv6 v Sloveniji smo zasledili leta 2002, ko je ekipa strokovnjakov ARNES-a (Akademskega in izobraževalnega omrežja Slovenije), DANTE-ja (upravljavci pan-evropskega akademskega omrežja GÉANT, ki povezuje nacionalna akademska omrežja) in RedIRIS-a (špansko akademsko in izobraževalno omrežje) postavila nov rekord v hitrosti prenosa podatkov s protokolom IPv6. Po podatkih s katerimi sedaj razpolagamo, ima Arnes danes že v celoti vzpostavljeno jedrno omrežje, ki temelji na dvojnem skladu. V omrežje IPv6 Arnesa se postopoma povezujejo ljubljanske in mariborske fakultete ter posamezne osnovne in srednje šole. Povezljivost v IPv6 omrežje Arnesa imajo tudi nekateri študentski domovi.

IPv6 je uveden (januar 2010) v omrežju operaterjev Amis, TušTelekom in TušMobil, pri Telekomu Slovenije so v fazi njegove implementacije. IPv6 se uvaja pri sistemskih integratorjih, kot so NIL, Astec, CHS in Iskratel[23]. Preko IPv6 protokola je dosegljiv multimedijski portal RTV Slovenije in osrednji slovenski spletni iskalnik Najdi.si. IPv6 protokol je že omogočen na virtualnih strežnikih Domenca.si, ki zagotavljajo spletno gostovanje organizacijam, podjetjem in posameznikom.

V Sloveniji je trenutno IPv6 prometa še zelo malo, vendar pričakujemo, da se bo z večanjem ponudbe internetnih storitev, ki bodo delovale na IPv6 protokolu, promet bistveno povečal. IPv4 protokol se bo še nekaj časa uporabljal, zato moramo zagotoviti, da bodo IPv4 storitve in vsebine še vedno nemoteno na voljo končnim uporabnikom.

Prehod na IPv6 vključuje vse akterje naše družbe. Razvijalci IPv6 protokola so že naredili glavnino svojega dela. Njihovo delo se sedaj usmerja v razvoj novih protokolov in mehanizmov temelječih na IPv6, ki bodo prinesli nove funkcionalnosti, zmožnosti in še večjo varnost komunikacij.
Tudi akademsko-raziskovalna sfera je za skupnost naredila veliko. IPv6 so implementirali v svoja jedrna omrežja, sedaj mora IPv6 implementirati po vseh inštitutih, univerzah, srednjih in osnovnih šolah. Na novem protokolu preizkušajo nove storitve in funkcionalnosti (npr. IPv6 Multicast, senzorska omrežja), ki se bodo kasneje selila tudi v poslovna in rezidenčna okolja.
Velika teža prehoda na IPv6 je vsekakor na operaterjih omrežij. Ti morajo vsem svojim uporabnikom zagotoviti zanesljivo, hitro, varno in na IPv6 posodobljeno infrastrukturo. Na jedrnem delu omrežja bo zaradi manjšega števila opreme migracija relativno enostavna, zato pa je toliko več energije in finančnih sredstev potrebnih na dostopovnem delu in sistemih za podporo omrežij. Še posebej širokopasovna dostopovna omrežja so lahko pri uvajanju IPv6 potencialno ozko grlo, ki bi lahko zavirala razvoj uvajanja IPv6.
Veliko dela čaka tudi industrijo in razvijalce opreme. IPv6 je sicer že polno podprt v vseh novejših zmogljivih usmerjevalnikih in stikalih, veliko pomanjkanja pa se čuti na trgu (usmerjevalniki, modemi, TV komunikatorji, terminalski medijski vmesniki…), ki pokriva segment rezidenčnih uporabnikov. Razlog temu se deloma skriva v pomanjkanju ustreznih specifikacij, deloma zaradi slabega povpraševanja na trgu. Tudi na področju upravljanja,

[22] Zavod go6: http://ipv6.go6.si/
[23] Vir: Zavod go6

oskrbovanja (OSS/BSS) in varnosti (IDS/IPS, požarne pregrade) bo potrebno še veliko postoriti.
Svojo vlogo pri prehodu na IPv6 morajo odigrati tudi ponudnikih vsebin in storitev. Tudi ti morajo zagotoviti, da bodo njihove vsebine in storitve enakovredno dostopne tako za IPv6 kot za IPv4 uporabnike. Uporabnikov ne zanima, na kakšni platformi deluje ponudnik dostopa, vsebine in storitev in kakšne protokole uporablja. Zanje je pomembno zgolj to, da so internetne vsebine in storitve ne glede na uporabljeno platformo dosegljive vedno, hitro in povsod.
Pomemben akter v tej zgodbi je tudi poslovni sektor, ki bo moral zahtevati od svojega ponudnika dostopa IPv6 povezljivost ter začeti s posodabljanjem vseh svojih strežnikov in spletnih vsebin in storitev, da bodo dosegljive tudi IPv6 uporabnikom.
Posodobitev na IPv6 se bo morala izvesti tudi v vseh lokalnih omrežjih. Izvesti bo potrebno podrobno analizo potrebnih sprememb, tveganja, stroškov in potrebnega časa za uvedbo IPv6. Analiza nam bo podala potrebne vhodne podatke, ki bodo omogočili čim bolj gladek, transparenten in neboleč prehod na IPv6.
V veliko pomoč pri tranziciji so tudi sistemski integratorji. Njihova vloga je predvsem pomoč vsem zainteresiranim v obliki izobraževanj in strokovne podpore pri implementaciji IPv6.
Zelo pomemben, morda celo ključen člen v tej zgodbi je država s svojo lastno mrežno infrastrukturo, spletnimi vsebinami in storitvami, ki jih omogoča sebi ter svojim državljanom. Država lahko stori veliko z ozaveščanjem in spodbujanjem vseh ostalih akterjev po čimprejšnji uvedbi IPv6. Je lahko velik generator in stimulator povpraševanja po novi IPv6 opremi in novih storitvah, ki bi izkoriščale prednosti IPv6 protokola. Svojo strategijo širokopasovnih omrežij lahko usmeri v izgradnjo novih naprednejših in varnejših omrežij, ki bodo izključno temeljile na protokolu nove generacije IPv6. Lahko sofinancira raziskovalne projekte, izgradnjo testnih omrežij, razvoj novih storitev in funkcionalnosti, lahko sofinancira izobraževanja v okviru delavnic, seminarjev in predavanj.
In končno tudi civilna družba, vključno z organizacijami in končnimi uporabniki lahko s povpraševanjem po IPv6 povezljivosti in storitvah pri svojih ponudnikih internetnih storitev spodbudi konkurenčnost ter s tem dvig kakovosti in ponudbo novih storitev.

V vseh okoljih moramo stremeti k temu, da se bo povečalo število implementacij omrežij, naprav, storitev in vsebin, ki bodo temeljile na IPv6 protokolu. S tem bomo zagotovili nove možnosti in priložnosti za inovacije na področju storitev, aplikacij in naprav ter obenem povečali konkurenčno prednost evropskega (in slovenskega) gospodarstva na svetovnih trgih.

8 LITERATURA IN VIRI

Ahmed, A., Asadullah, S. (2009): *Deploying IPv6 in Broadband Access Networks*, John Willey&Sons, Hoboken, New Jersey

Broadband Forum (2006a): *TR-101 Migration to Ethernet Based DSL aggregation*, dosegljivo na naslovu: http://www.broadband-forum.org/technical/download/TR-101.pdf, obiskano dne 30.12.2009

Broadband Forum (2006b): *TR-124 Functional Requirements for Broadband Residential Gateway Devices*, dosegljivo na naslovu: http://www.broadband-forum.org/technical/download/TR-124.pdf, obiskano dne 30.12.2009

Broadband Forum (2009): *PD-192 Residential Gateway (RG) IPv6 Requirments (updates fo TR-124)*, dosegljivo na naslovu: https://datatracker.ietf.org/documents/LIAISON/file667.pdf, obiskano dne 30.12.2009

Bush, R. (2009): The A+P Approach to the IPv4 Address Shortage draft-ymbk-aplus-05, dosegljivo na naslovu: http://ipv6.go6.si/wp-content/uploads/2009/10/draft-ymbk-aplusp-05.txt, obiskano dne 27.10.2009

Cisco: *Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS,* dosegljivo na naslovu: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosip_an.pdf, obiskano dne 9.11.2009

Cisco (2009): *Cisco Carrier-Grade IPv6 (CGv6) Solution Delivering on the future of the Internet*, dosegljivo na naslovu: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-558744-00.pdf, obiskano dne 22.12.2009

Cocquet, P. (2004): *IPv6 on DSL: The Best Way to Develop Always-On Services*, dosegljivo na naslovu: http://www.ipv6.eu/admin/bildbank/uploads/Documents/Positionpapers/IPv6_over_DSL__Patrick_Cocquet.doc, obiskano dne: 6.1.2010

COMMISSION OF THE EUROPEAN COMMUNITIES (2008): *Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe*, dosegljivo na naslovu: http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf, obiskano dne: 21.10.2009

ECC-CEPT (2009): *Preparing for IPv6, draft ECC report 144,* dosegljivo na: http://www.cept.org/4E2CDDBF-A9CF-4927-B6BF-471CA95A4384?frames=no&, obiskano dne 20.12.2009

DARPA INTERNET PROGRAM (1981): *Internet protocol Protocol specification,* dosegljivo na spletnem naslovu: ftp://ftp.rfc-editor.org/in-notes/rfc791.txt, obiskano dne 27.10.2009

Davies, J. (2008): *Understanding IPv6,* Microsoft Press., Redmon Washington

Doyle, J. (2009): *Large Scale NAT Arhitectures*, dosegljivo na naslovu: http://www.networkworld.com/community/node/45776, obiskano dne 15.11.2009

Doyle, J. (2009): *Understanding Dual-Stack Lite*, dosegljivo na naslovu: http://www.networkworld.com/community/node/46600, obiskano dne 15.11.2009

Durand, A. (2009): *Dual-stack lite broadband deployments post IPv4 exhaustion draft-ietf-softwire-dual-stack-lite-01*, IETF, Internet draft, dosegljivo na naslovu: http://www.ietf.org/id/draft-ietf-softwire-dual-stack-lite-01.txt, obiskano dne 25.10.2009

Ericsson (2001): *The benefits of IPv6 for the Mobile Internet,* dosegljivo na naslovu: http://www.ipv6-tf.com.pt/documentos/geral/ericsson/Benefits%20of%20IPv6%20for%20Mobile%20Internet.pdf, obiskano dne 25.10.2009

European IPv6 Task Force (2006): *Deliverable D3.1.2 National Task-Forces Report,* dosegljivo na naslovu: http://www.ipv6.eu/admin/bildbank/uploads/Documents/Deliverables/ipv6tf-sc_pu_d3_1_2_v3.3.pdf , obiskano dne 20.10.2009

Grossetete, P., Popoviciu,C.P., Wettling, F. (2008): Global IPv6 Strategies from BussinessAnalysis to Operational Planning, Cisco Press 800 East 96th Street, USA

Hagen, S. (2006): *IPv6 Essential,* O'Reilley Media Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472

IETF (1987): *Domain Names-Implementation and specification,* RFC1035*,* dosegljivo na naslovu*:* http://tools.ietf.org/html/rfc1035, obiskano dne 29.11.2009

IETF (1994): *The IP Network Address Translator* (NAT), RFC1631*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc1631, obiskan dne 14.11.2009

IETF (1995): *The Recommendation for the IP Next Generation Protocol,* RFC1752, dosegljivo na naslovu: http://tools.ietf.org/html/rfc1752, obiskano dne 21.11.2009

IETF (1996): *Address Allocation for Private Internets,* RFC1918*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc1918, obiskano dne 13.11.2009

IETF (1997a): *Basic Socket Interface Extensions for IPv*6, RFC2133, dosegljivo na naslovu:http://tools.ietf.org/html/rfc2131, obiskano dne 30.11.2009

IETF (1997b): *Routing Aspects Of IPv6 Transition,* RFC2185, dosegljivo na naslovu: http://tools.ietf.org/html/rfc2185, obiskano dne 27.10.2009

IETF (1998): *Advanced Socket API for IPv6,* RFC2292*, dosegljivo na naslovu:* http://tools.ietf.org/html/rfc2292, obiskano dne 30.11.2009

IETF (1999): *Extension Mechanisms for DNS* (EDNS0), RFC2671*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc2671, obiskano dne 28.11.2009

IETF (2001a): *Connection of IPv6 Domains via IPv4 Clouds*, RFC3056*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3056, obiskano dne 12.12.2009

IETF (2001b): *An Anycast Prefix for 6to4 Relay Routers*, RFC3068*,* dosegljivo na naslovu:http://tools.ietf.org/html/rfc3068, obiskano dne 15.12.2009

IETF (2001c): *Radius and IPv6*, RFC3162*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3162, obiskano dne: 22.1.2010

IETF (2003a): *DNS Extensions to Support IP Version 6*, RFC3596*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3596, obiskano dne 28.11.2009

IETF (2003b): *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC3315*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3315, obiskano dne 28.11.2009

IETF (2003c): *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*, RFC3633*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3633, obiskano dne 28.11.2009

IETF (2004): *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*, RFC3736*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc3736, obiskano dne 28.11.2009

IETF (2005a): *Scenarios and Analysis for Introducing IPv6 into ISP Networks,* RFC4029*,* dosegljivo na http://tools.ietf.org/html/rfc4029, obiskano dne 12.11.2009

IETF (2005b): *SEcure Neighbour Discovery (SEND),* RFC3971, dosegljivo na naslovu: http://tools.ietf.org/html/rfc3971#section-3, obiskano dne 27.10.2009

IETF (2007a): - *ISP IPv6 Deployment Scenarios in Broadband Access Networks,* RFC4779, dosegljivo na naslovu: http://tools.ietf.org/html/rfc4779, obiskano dne 4.1.2010

IETF (2007b): *RADIUS Delegated-IPv6-Prefix Attribute*, RFC4818*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc4818, obiskano dne 4.1.2010

IETF (2008a): *NAT Port Mapping Protocol (NAT-PT)*, dosegljivo na naslovu: http://tools.ietf.org/html/draft-cheshire-nat-pmp-03, obiskano dne: 15.11.2009

IETF (2008b): *A Comparison of Proposals to Replace NAT-PT*, dosegljivo na: http://tools.ietf.org/html/draft-wing-nat-pt-replacement-comparison-02#section-3.2.4, obiskano dne 18.11.2009

IETF (2008c): *Intra-site Automatic Tunnel Addressing Protocol (ISATAP)*, RFC5214*,* dosegljivo na naslovu: http://tools.ietf.org/html/rfc5214, obiskano dne 16.12.2009

IANA (2009): *Port numbers*, dosegljivo na naslovu: http://www.iana.org/assignments/port-numbers, obiskano dne: 15.11.2009

IETF (2009a): *Common Functions of Large Scale NAT* (LSN, draft-nishitani-cgn-02, dosegljivo na naslovu: http://www.ietf.org/id/draft-nishitani-cgn-02.txt, obiskano dne 13.11.2009

IETF (2009b): *IP/ICMP Translation Algorithm*, dosegljivo na naslovu: http://tools.ietf.org/html/draft-ietf-behave-v6v4-xlate-03, obiskano dne 15.11.2009

IETF (2009c): *NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers,* dosegljivo na naslovu: http://tools.ietf.org/html/draft-ietf-behave-v6v4-xlate-stateful-02, obiskano dne 15.11.2009

IETF (2009d): *ISP Shared Address*, dosegljivo na naslovu: http://tools.ietf.org/html/draft-shirasaki-isp-shared-addr-03, obiskano dne 15.11.2009

IETF (2009e): *PET-based framework for IPv4/IPv6* coexistence, Internet draft, dosegljivo na naslovu: http://tools.ietf.org/html/draft-cui-softwire-pet-framework-00, obiskano dne 4.11.2009

IETF (2009f): *Dual-stack lite broadband deployments post IPv4 exhaustion*, dosegljivo na naslovu: http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite-02, obiskano dne: 15.11.2009
IETF (2009g): *Basic Requirements for IPv6 Customer Edge Routers* (draft-ietf-v6ops-ipv6-cpe-router-04), dosegljivo na naslovu: http://tools.ietf.org/html/draft-ietf-v6ops-ipv6-cpe-router-04, obiskano dne: 21.1.2010

Inno group&Zaltana (2007): *Impact of IPv6 on vertikal markets*, study commissioned by European Commission, dosegljivo na naslovu: http://www.ipv6council.de/fileadmin/documents/IPv6_vertical_markets.pdf , obiskano dne: 25.10.2009

IPv6 Task Force Austria (2005): *Austrian IPv6 Roadmap*, dosegljivo na naslovu: http://www.ipv6taskforce.at/kolloquium2/pdf/IPv6_Roadmap_full.pdf, obiskano dne 17.11.2009

IPv6 Task Force, U.S. Department of Commerce, NIST, NTIA (2006): *Tehnical and economic assessment of internet protokol version 6 (IPv6),* dosegljivo na naslovu: http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/IPv6final.pdf*, obiskano dne:* 30.10.2009

Juniper Networks (2008): *Using PPPoE and IPoE in Ethernet Broadband Networks*, dosegljivo na naslovu: http://www.juniper.net/solutions/literature/white_papers/200187.pdf, obiskano dne 2.1.2010

Juniper Networks (2009): *VLAN design for IPTV/Multipley networks*, dosegljivo na naslovu: http://www.juniper.net/us/en/local/pdf/whitepapers/2000186-en.pdfm, obiskano dne 2.1.2010

Kos, A., Bešter, J. (2001): *Evolucija hrbteničnih IP-omrežij v smeri MPLS*, dosegljivo na naslovu: http://ev.fe.uni-lj.si/4-2001/kos.pdf, obiskano dne 20.12.2009

Komisija Evropskih skupnosti (2009): *Javno-zasebno partnerstvo za internet prihodnosti*, dosegljivo na naslovu: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0479:FIN:SL:DOC, obiskano dne 12.11.2009

Kumer, J. (2007): *BGP/MPLS VPN v IPv6*, diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

LACNIC: *ISPs: IPv6 in 3 steps*, dosegljivo na: http://portalipv6.lacnic.net/en/ipv6/ipv6/isps/isps-ipv6-3-steps, obiskano dne 16.11.2009

Loshin, P. (2004): *IPv6 Theory, Protocol and Practice*, Morgan Kaufmann Publishers is an Imprint of Elsevier, 500 Sansome Street, Suite 400, San Francisco, CA 94111

MIcrosoft (2005): *IPv6 Support in Home Routers*, dosegljivo na naslovu: http://www.microsoft.com/whdc/device/network/IPv6_IGD.mspx, obiskano dne 15.12.2009

Minoli, D., Kounos, J. (2009): *Security in an IPv6 Environment,* CRC Press, Auerbach Publications, Taylor&Francis Group, New York

NIST (2008): *A Profile for IPv6 in the U.S. Government – Version 1.0*, dosegljivo na naslovu: http://www.antd.nist.gov/usgv6/usgv6-v1.pdf, obiskano dne 25.1.2010

Oblak, A. (2008): *Prehod na IPv6 za potrebe telekomunikacijskih podjetij,* diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

OECD (2007): *Economic Consideration in the Management of IPv4 and in the Deployment of IPv6*, dosegljivo na naslovu: http://www.oecd.org/dataoecd/7/1/40605942.pdf, obiskano dne: 15.1.2010

RFC-REF: *History and Problem Description,* dosegljivo na spletnem naslovu: http://rfc-ref.org/RFC-TEXTS/4632/chapter2.html, obiskano dne 24.10.2009

Smith, P. (2009): *Cisco - IPv6 Technical & Service Considerations*, dosegljivo na naslovu: http://www.pacnog.org/pacnog5/meeting/ipv6intro.pdf, obiskano dne 18.11.2009

Straus, M. (2009): *Poenostavimo delitev naslovnega prostora v hrbteničnih omrežjih,* dosegljivo na naslovu: http://ipv6.go6.si/wp-content/uploads/2009/10/IPv6summit2_Matjaz-Straus-poenostavimo-delitev.pdf, obiskano dne 8.1.2009

Uze, J.M. (2009): *How to transition: Mechanism and Methodologies for Smart IPv6 Implementation,* dosegljivo na naslovu: https://www.linx.net/files/meetings/2009-ipv6/Linx-IPv6-HowtoTransition-jmuze-130309.pdf, obiskano dne 16.11.2009

6net (2005): *An IPv6 Deployment Guide*, dosegljivo na naslovu: http://www.6net.org/book/deployment-guide.pdf, obiskano dne 17.11.2009

9 SEZNAM UPORABLJENIH KRATIC

Kratica	Angleški pomen	Slovenski pomen
ALG	Application Layer Gateway	Prehod v aplikacijskem sloju
AS	Autonomous system	Avtonomni sistem
ATM	Asynchronous Transfer Mode	Asinhroni prenosni način
BRAS	Broadband Remote Access Server	Strežnik za širokopasovni oddaljeni dostop
ccTLD	Country Code Top Level Domain	Deželne kode TLD
CE	Custumer Edge	Robna naprava stranke
CHAP	Challenge Handshake Authentication Protocol	Avtentikacijski protokol z usklajevanjem zahtev za geslo
CIDR	Classless Interdomain Routing	Brezrazredno meddomensko usmerjenje
CMTS	Cable Modem Termination System	Zaključitev kabelskega omrežja
CoS	Class of Service	Razred storitve
CPE	Customer Premises Equipment	Oprema pri stranki
DAD	Duplicate Address Detection	Odkrivanje podvojenih naslovov
DHCP	Dynamic Host Configuration Protokocol	Protokol za dinamično konfiguriranje gostiteljskih računalnikov
DHCP-PD	DHCP-Prefix Delegation	DHCP dodeljevanje predpone
DNS	Domain Name System	Sistem domenskih imen
DNSSEC	DNS Security Extension	Varnostna razširitev za DNS
DOCSIS	Data Over Cable Service Interface Specification	Specifikacija vmesnika za prenos podatkov prek kabelskih omrežij
DoS	Denial of Service	Tajitev storitve
DSL	Digital Subscriber Line	Digitalni naročniški vod
EAP	Extensible Authentication Protocol	Razširljivi avtentikacijski protokol
EAPoL	Extensible Authentication Protocol over LAN	Razširljivi overilni protokol v omrežju LAN
EDSNS0	Extension Mechanisms for DNS	Razširitveni mehanizem za DNS
FQDN	Fully Qualified Domain Name	Popolno kvalificirano domensko ime
FR	Frame Relay	Blokovno posredovanje
FTP	File Transfer Protocol	Protokol za prenos datotek
FTPS	FTP Secure (FTP-SSL)	Varni FTP
FTTH	Fiber-to-the-home	Optično vlakno do hiše
GRE	Generic Routing Encapsulation	Generično ovijanje pri usmerjanju
HFC	Hybrid fiber coaxial	Hibridni prenos prek optičnih in koaksialnih kablov
HTTP	Hypertext Transfer Protocol	Protokol za prenos hiperteksta
IANA	Internet Assigned Numbers Authority	Uprava za dodeljevanje številk v internetu
ICMP	Internet Control Message	Protokol internetnega kontrolnega

	Protocol	sporočila
IPv6	Internet Protocol version 6	Internetni protokol verzije 6
IPCP	IP Control Protocol	IP nadzorni protokol
IPv4	Internet Protocol version 4	Internetni protokol verzije 4
IPv6CP	IPV6 Control Protocol	IPv6 nadzorni protokol
ISTAP	Intra-Site Automatic Tunnel Addressing Protocol	Protokol za avtomatično naslavljanje tunela znotraj lokacije
IX	Internet Exchange	Internetna izmenjevalna točka
LER	Label Edge Router	Robni usmerjevalnik pri komutaciji na osnovi label
LFIB	Label Forwarding information base	Informacijska baza za posredovanje label
LIX	Ljubljana Internet Exchange	Ljubljanska točka za izmenjavo internetnega prometa
LLMNR	Link-Local Multicast Name Resolution	Povezavno-lokalna pretvorba imena pri oddajanju več prejemnikom hkrati
LSP	Label Switch Path	Z labelami komutirana pot
LSR	Label Switching Router	Usmerjevalnik z labelnim stikalom
LTE	Long Term Evolution	Evolucija na daljši rok
MAC	Media Access Control	Krmiljenje dostopa do medija
mDNS	Multicast DNS	Strežnik domenskih imen za oddajanje več prejemnikom hkrati
MLD	Multicast listener discovery	Iskanje za multicast prometom
MP-BGP	Multiprotocol-Border Gateway Protocol	Večprotokolni mejni protokol
MPLS	Multiprotocol Label Switching	Večprotokolna komutacija z zamenjavo label
MSAN	Multi-Service Access Node	Večstoritveno dostopovno vozlišče
MTU	Maximum Transfer Unit	Maksimalna prenosna enota
MX	Mail exchange	Izmenjava pošte
NA	Neighbor advertisement	Oglaševanje soseda
NAPT	Network Address Port Translation	Prevajanje omrežnih naslovov in portov
NAT	Network Address Translation	Prevajanje omrežnih naslovov
NBMA	Nonbroadcast multiple-access network	Omrežje z nerazpršeno oddajo in brez sodostopa
ND	Neighbor Discovery	Iskanje soseda
NNTP	Network News Transfer Protocol	Protokol za prenos omrežnih novic
NS	Name Server	Imenski strežnik
PE	Provider Edge	Robna naprava ponudnika
PPP	Point-to-Point Protocol	Protokol točka-točka
RA	Router Advertisment	Oglaševanje usmerjevalnika
RADIUS	Remote Authentication Dial in User Service	Komutirana uporabniška storitev z oddaljeno overitvijo
RG	Residental Gateway	Rezidenčni prehod
RR	Resource Record	Zapis vira
SEND	SEcure Neighbor Discovery	Varno iskanje sosedov
SIX	Slovenian Internet Exchange	Slovenska točka za izmenjavo

		internetnega prometa
SLAAC	Stateless Address Autoconfiguration	Samostojna samodejna konfiguracija naslovov
SMTP	Simple Mail Transfer Protocol	Preprosti protokol posredovanja sporočil
TLD	Top Level Domain	Domene vrhnjega sloja
VC	Virtual Circuit	Navidezna povezava
VLAN	Virtual LAN	Navidezni LAN
VLSM	Variable-Length Subnet Masking	Maskiranje s spremenljivo dolžino podomrežja