Tranzicijski mehanizmi za prehod na IPv6

Tibor Djurica Potpara

Ljubljana, avgust 2011

Mentor: Matjaž Straus Istenič

Akademska in raziskovalna mreža Slovenije – Arnes

Kazalo vsebine

Predgovor

Regionalnim internetnim registrom je bil v začetku februarja 2011 dodeljen ves razpoložljiv naslovni prostor IPv4. Nove IPv4-naslove bomo lahko pridobili le iz zalog. Z izčrpanjem le-teh se bo širitev IPv4-omrežij dokončno ustavila. Soočeni bomo z dejstvom, da bo za nove omrežne sisteme in storitve možen le novi protokol – IPv6.

Ne pozabimo, da IPv4 ne bo čez noč izginil iz naših omrežij in storitev. Pripraviti se bomo morali na dolgoletno sobivanje obeh različic IP-protokola in postopno ukinitev IPv4. In prav to je bil razlog, da smo v Akademski in raziskovalni mreži Slovenije – Arnes omogočili počitniško delo gimnazijcu, ki je praktično preveril nekaj najbolj razširjenih mehanizmov za komunikacijo med IPv4 in IPv6-omrežji. Njegova naloga je bila:

- opisati osnovne tranzicijske mehanizme za prehod na IPv6,
- v laboratorijskem okolju pripraviti omrežja in računalnike (odjemalce in strežnike) tipičnih organizacij, ki so v različnih fazah prehoda na IPv6 – od organizacije, ki ima zgolj IPv4-omrežje do take, ki je IPv4 že povsem opustila in uporablja zgolj IPv6,
- praktično preveriti delovanje teh mehanizmov,
- preveriti zanesljivost in robustnost opisanih tranzicijskih mehanizmov z vidika končnega uporabnika.

Tibor Djurica Potpara je svoje delo odlično opravil. Uporabil je usmerjevalnike proizvajalcev Cisco in Juniper, med temi tudi profesionalno opremo, kot je usmerjevalnik Cisco ASR-1000, ki omogoča sodobne translacijske mehanizme (npr. NAT64) in različne vrste tuneliranja (npr. 6rd). Laboratorij je dopolnil z več navideznimi računalniki in strežniki s pestrim naborom operacijskih sistemov ter simuliranimi usmerjevalniki za domačo rabo in mala podjetja na osnovi Mikrotik RouterOS.
Prispevek je rezultat tega praktičnega dela z realno komunikacijsko in programsko opremo in v realnem omrežju. Tako je lepo dopolnilo teoretičnim razpravam in opisom tranzicijskih mehanizmov za prehod na IPv6.

Dokument so pregledali tudi člani strokovnega sveta zavoda Go6.

Mentor: Matjaž Straus Istenič, Arnes

Uvod

Navkljub vsem prizadevanjem za zmanjševanje izrabe naslovnega prostora IPv4 je neizbežno, da bo ta v bližnji prihodnosti povsem izčrpan. Edina dolgoročna rešitev je prehod na IPv6, ki ponuja dovolj velik naslovni prostor za vse projekcije prihodnje rabe. IPv6 je protokol, ki nastaja in se neprestano izboljšuje že več kot 10 let, kljub temu pa je pokritost z IPv6-internetom še zmeraj zelo nizka.

Idealni model prehoda na IPv6 bi bilo podaljšano obdobje, v katerem bi naprave na internetu podpirale tako IPv4 kot IPv6 protokolni sklad (*dual-stack*) do točke, ko bi IPv6 podpiralo dovolj naprav, da IPv4 ne bi bil več potreben. Temeljni problem je namreč, da sta IPv6 in IPv4 v osnovi nezdružljiva, kar pomeni, da naprave, ki podpirajo samo IPv4, in naprave, ki podpirajo samo IPv6, med seboj ne morejo komunicirati brez pomoči t.i. translacijskih mehanizmov.

Prehod na IPv6 je počasen iz več razlogov - veliko omrežne opreme je bilo v preteklosti nezdružljive z IPv6, kar je povzročalo velike stroške pri nadgradnji. Poleg tega je prehod na novi protokol zelo zamuden in zahteven proces, in ker je IPv4 deloval zadovoljivo dobro, IPv6 pa ni prinašal očitnih prednosti, ni bilo zadostne iniciative za prehod. Dandanes večina nove opreme podpira IPv6, prehod pa je iz možnosti postal nuja, saj se le tako lahko vzdržuje nadaljnja širitev interneta.

Ponekod po svetu, na primer v območju, ki ga pokriva APNIC, je naslovni prostor IPv4 že tako izčrpan, da je prišla v veljavo posebna politika dodeljevanja novih naslovov, skladno s katero lahko vsaka organizacija, ki potrebuje IPv4-naslove, dobi največ še blok /22 (1024 naslovov). Takšna politika bo novim organizacijam omogočila, da pridobijo naslovni prostor, hkrati pa preprečila širitev obstoječim. Nekateri ponudniki internetnih storitev so zaradi pomanjkanja IP-naslovov že prisiljeni svojim strankam dodeljevati privatne IP-naslove z dostopom do interneta prek *carrier-grade NAT* naprav, ali pa začenjajo svoje stranke priklapljati na izključno IPv6-omrežje.

V tem dokumentu so predstavljeni različni mehanizmi prehoda, ki lajšajo prehod na IPv6 ali pa omogočajo omejeno komunikacijo med napravami, ki omogočajo zgolj IPv4 ali IPv6. Za vsakega izmed predstavljenih mehanizmov sta podana primer konfiguracije omrežne opreme na Arnesovem laboratorijskem omrežju in analiza uporabnosti.

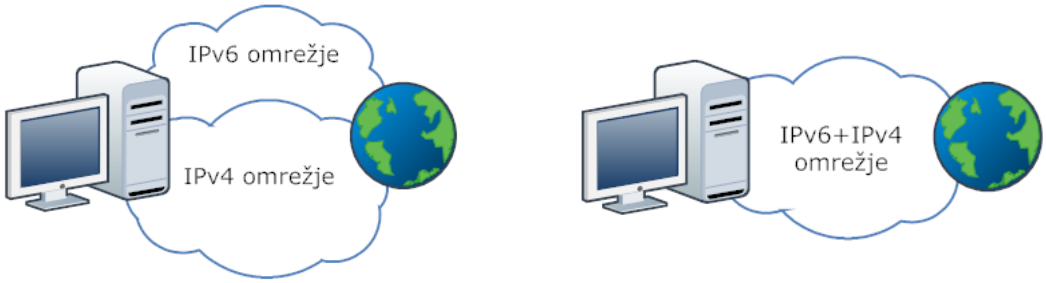
Dual-stack

V načinu *dual-stack* naprava podpira oba protokolna sklada in ima dodeljene tako IPv4 kot IPv6-naslove. Z napravami, ki podpirajo samo IPv6, komunicira prek IPv6-omrežja, z napravami, ki podpirajo samo IPv4, pa prek IPv4.

Prednosti *dual-stack* načina so, da je kompatibilen s skoraj vsemi aplikacijami. Tiste, ki ne podpirajo IPv6, preprosto uporabijo IPv4. Glede na to, da je večina višjih protokolov v skladu neodvisnih od izbire omrežnega protokola, pa je tudi nadgradnja aplikacij na IPv6 večinoma premočrtna.

Dual-stack omogoča največjo fleksibilnost in je osnova za večino preostalih mehanizmov prehoda, pri katerih naprave, ki podpirajo oba protokolna sklada, delujejo kot mejne (demarkacijske) točke med IPv6 in IPv4-omrežjem.

IPv6 lahko do končnih naprav privedemo na dva različna načina. Prvi je, da imamo dva



ločena nabora omrežne opreme, enega za IPv4 in drugega za IPv6, drugi pa, da postopoma nadgrajujemo omrežno opremo na IPv6, dokler celotno omrežje ne postane *dual-stack*. Prvi način pospeši uvedbo IPv6, vendar poveča zapletenost omrežja in stroške vzdrževanja. Pri drugem načinu je čas uvedbe daljši, vendar struktura omrežja ostane podobna, kar olajša vzdrževanje.

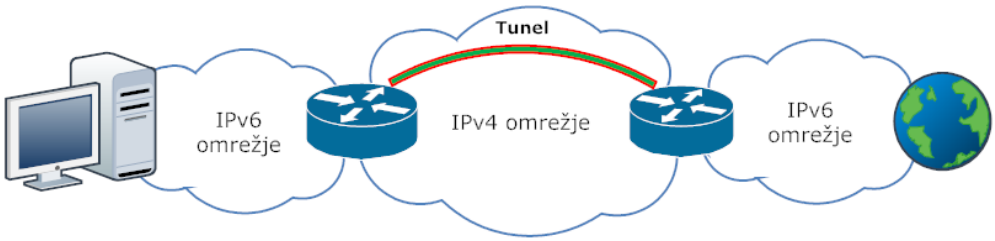
Poglavitna slabost načina *dual-stack* je, da je treba vzdrževati dve ločeni (fizični ali navidezni) omrežni infrastrukturi, za IPv6 in za IPv4. Vsaki napravi, ki je del *dual-stack* omrežja, je treba določiti vse parametre za nastavitev tako za IPv4 kot tudi za IPv6. To prinaša večje stroške vzdrževanja, zato se pričakuje, da bodo *dual-stack* omrežja začela opuščati IPv4, ko bo IPv6 dovolj razširjen.

Tranzicijski mehanizmi

Tunelski mehanizmi

Tunelski mehanizmi sami po sebi ne omogočajo neposredne komunikacije med IPv4 in IPv6-napravami, temveč omogočajo povezavo več "IPv6-otokov", ne da bi bilo treba nadgraditi celotno omrežje. Predstavljajo srednjo pot med obema načinoma prehoda na domorodni IPv6. Tunelski mehanizmi zmanjšajo potrebni čas za povezavo omrežij v IPv6-internet, poleg tega pa zmanjšajo stroške.

Ko celotno omrežje podpira IPv6, potrebe po tunelih več ni.



Osnovni princip delovanja tunelov

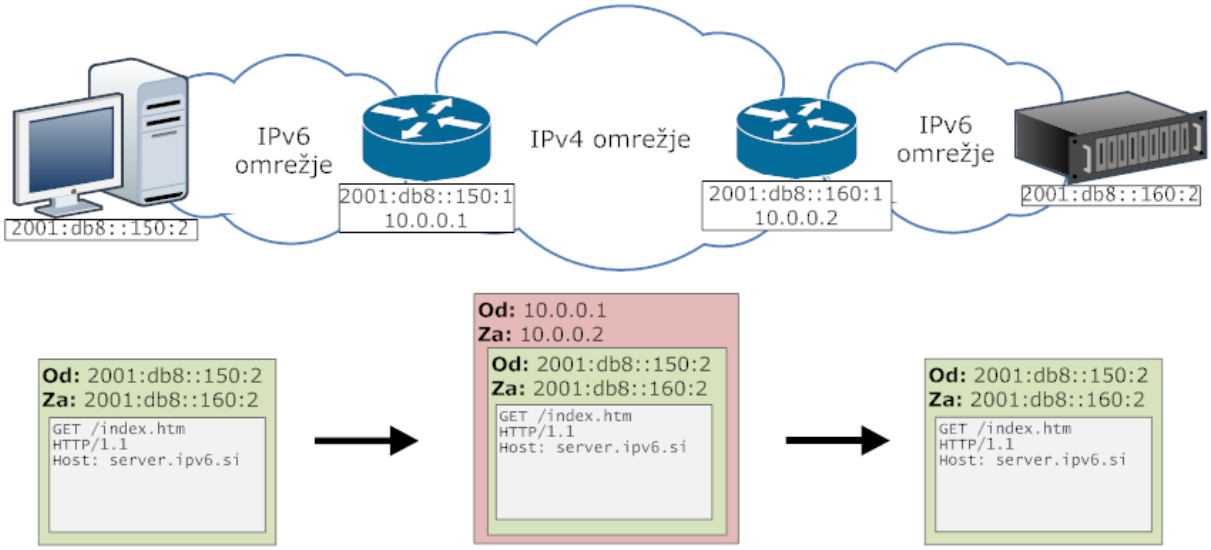
Med najbolj razširjene tunelske mehanizme štejemo:

- ročno tuneliranje (6in4),
- 6to4,
- 6rd (IPv6 Rapid Deployment) in
- Teredo.

Ročno tuneliranje (6in4)

6in4 je bil eden izmed prvih načinov tuneliranja IPv6-paketov prek IPv4-omrežja in je danes med najbolj razširjenimi, hkrati pa tudi temelj za nekatere druge tunelske mehanizme. 6in4 opisuje RFC 4213 (*"Basic Transition Mechanisms for IPv6 Hosts and Routers"*).

Glavni princip, na katerem temelji 6in4, je „enkapsulacija“ – IPv6-paket se na robu omrežja vstavi v IPv4-paket, ki nato potuje skozi IPv4-omrežje do roba omrežja naslovnika, kjer spet potuje naprej kot IPv6-paket.



Shema delovanja 6in4

Kot vidimo, morata oba usmerjevalnika, ki zaključujeta tunel, podpirati *dual-stack*, da lahko komunicirata s končnimi napravami v omrežju prek IPv6 ter med seboj prek IPv4. S stališča končne naprave je tunel neviden – obnaša se kot neposredna IPv6-povezava med usmerjevalnikoma.

6in4 ima oznako protokola 41, zato pogosto zasledimo tudi izraz **proto-41** tunel. Kot vidimo v zajemu paketa, je IPv6-paket dodan neposredno za glavo IPv4-paketa brez vmesnih višjenivojskih protokolov, kot sta TCP ali UDP. To zmanjša presežek velikosti na minimum (v 6in4 IPv6-enkapsuliran paket je le 20 bajtov večji od domorodnega IPv6 paketa) in s tem omogoči večjo učinkovitost.

```
⊞ Frame 293 (106 bytes on wire, 106 bytes captured)
⊞ Ethernet II, Src: a2:fe:68:41:8c:99 (a2:fe:68:41:8c:99), Dst: Media4_ca:e1:40 (00:10:aa:ca:e1:40)
⊟ Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 92
    Identification: 0x2db7 (11703)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
  ⊞ Header checksum: 0xf8bf [correct]
    Source: 10.0.0.1 (10.0.0.1)
    Destination: 10.0.0.2 (10.0.0.2)
⊟ Internet Protocol Version 6
  ⊞ 0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: TCP (0x06)
    Hop limit: 128
    Source: 2001:db8::150:1 (2001:db8::150:1)
    Destination: 2001:db8::160:1 (2001:db8::160:1)
⊟ Transmission Control Protocol, Src Port: 50445 (50445), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 50445 (50445)
    Destination port: http (80)
    [Stream index: 44]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 8192
  ⊞ Checksum: 0xf222 [validation disabled]
  ⊞ Options: (12 bytes)
```

Zajem 6in4-paketa

Poglavitna slabost 6in4-protokola s stališča hitrega prehoda na IPv6 je, da je treba vse tunele ročno nastaviti na obeh usmerjevalnikih ali končnih napravah, ki zaključujeta tunel. Zaradi te omejitve so bili razviti drugi mehanizmi, ki omogočajo samodejno vzpostavitev tunela, vendar kljub temu za enkapsulacijo uporabljajo protokol 41.

Zato, ker 6in4 tuneli ne delujejo vedno ob prisotnosti prehodov NAT med napravama, ki jih zaključujeta, se za povezovanje končnih naprav (npr. računalnikov, mobilnih telefonov …) v IPv6-internetu ponavadi uporabljajo drugi protokoli, kot so npr. Teredo ali AYIYA, 6in4 pa se uporablja bolj na ravni infrastrukture (npr. za povezavo celotnega domačega omrežja v IPv6-internet).

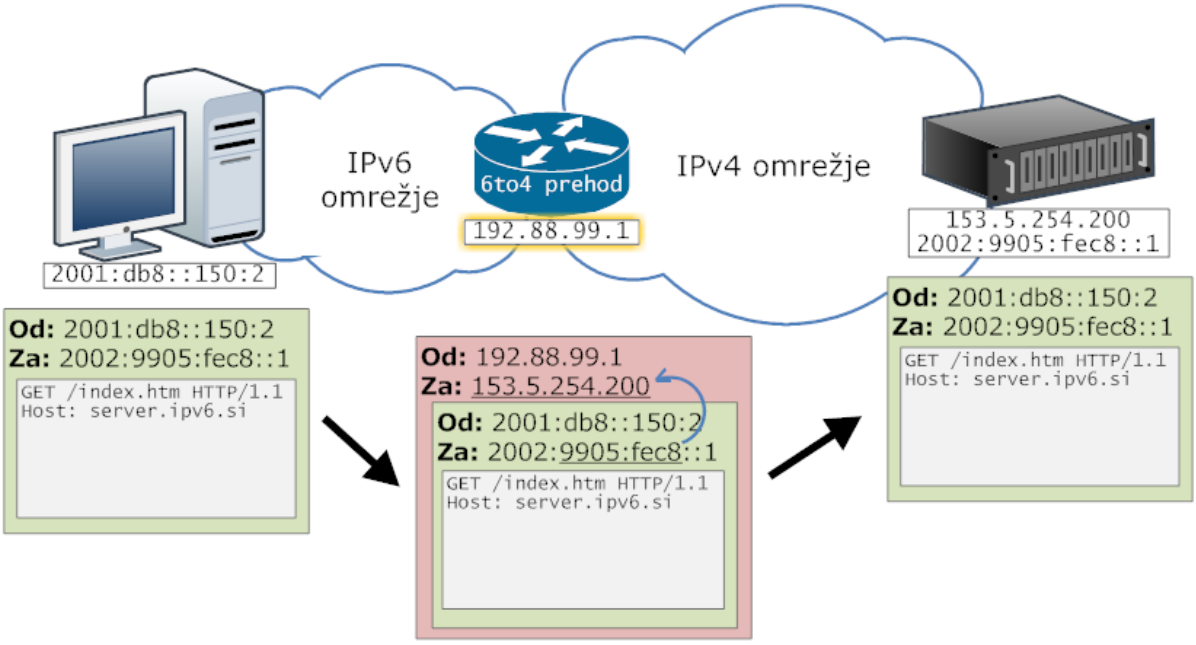
6to4

6to4 je protokol, ki omogoča vzpostavitev IPv6-povezljivosti, ne da bi bilo treba ročno nastaviti tunele. Za transportni protokol uporablja protokol 41, tunel pa se avtomatsko vzpostavi na podlagi algoritmične zveze med IPv4-naslovom in IPv6-naslovnim blokom. 6to4 opisujeta RFC 3056 ("Connection of IPv6 Domains via IPv4 Clouds") in RFC 3068 ("An Anycast Prefix for 6to4 Relay Routers").

Specifikacija 6to4 vsakemu globalno dosegljivemu IPv4-naslovu priredi IPv6-naslovni blok, tako da se prefiksu `2002` doda IPv4-naslov v šestnajstiškem zapisu, kot kaže shema:

Prefiks `2002` je dolg 16 bitov, IPv4-naslov pa 32, celotni blok ima torej prefiks /48 – to je dovolj velik blok, da vsakemu globalno dosegljivemu IPv4-naslovu pripade 65536 različnih podomrežij dolžine /64.

6to4-povezljivost omogočajo tako imenovani 6to4-prehodi. Za vzpostavitev povezave v IPv6-internet je dovolj, da nastavimo lokalne IPv6-naslove iz pripadajočega naslovnega prostora, pakete naslovljene v internet pa v 6in4-enkapsulaciji pošljemo na IPv4-naslov **192.88.99.1**. To je *anycast* naslov, zato paket vedno pride do najbližjega 6to4-prehoda, ki ga nato posreduje naprej v IPv6-internet.



Shema delovanja 6to4

V nasprotni smeri – z IPv6-interneta proti napravi, ki uporablja 6to4 – proces poteka tako, kot kaže shema. Paketi, naslovljeni na `2002::/16`, s pomočjo *anycasta* prav tako vedno pridejo na najbližji prehod. Prehod iz IPv6-naslova naslovnika samodejno ugotovi IPv4-naslov naprave ter pošlje 6in4-paket na ta ciljni naslov.

Poglavitna prednost 6to4 pred 6in4 je, da je za dostop do IPv6 interneta dovolj zgolj vklopiti 6to4 na napravah in operacijskih sistemih, ki ga omogočajo, ter nastaviti naslove na lokalni strani. Na nekaterih platformah (npr. Microsoft Windows 2008) je 6to4 po privzetih nastavitvah že omogočen, če je na katerem izmed omrežnih vmesnikov nastavljen javni IPv4-naslov.

6to4 pa ima tudi svoje slabosti. 6to4-prehode upravljajo različni internetni ponudniki, načeloma pa lahko sodeluje vsakdo. Upravitelji prehodov ne jamčijo za raven storitve, zato je 6to4 manj primeren na primer za poslovna okolja, kjer je dosegljivost storitve prek IPv6 ključnega pomena. Če se kateri izmed prehodov ne obnaša, kot bi se po specifikaciji moral, je zaradi narave anycasta težko odkriti, kje je ta problematičen prehod, saj je videti, kot da vsi paketi prihajajo z istega naslova.

6rd (IPv6 Rapid Deployment)

6rd je protokol za avtomatsko tuneliranje, ki je v osnovi zelo podoben 6to4. Avtomatska vzpostavitev tunela prav tako temelji na algoritmični zvezi med IPv6-naslovnim blokom in IPv4-naslovom, za transport pa se uporablja protokol 41. Delovanje 6rd opisuje RFC 5969 (“*IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*”).

Bistvena razlika med 6to4 in 6rd je, da se namesto znanega prefiksa `2002::/16` uporabi

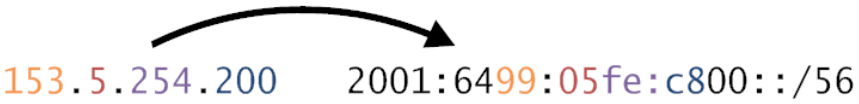
prefiks iz naslovnega prostora posameznega internetnega ponudnika, ki prav tako upravlja lastne prehode. 6rd lahko ponavadi uporabljajo le odjemalci iz ponudnikovega lastnega omrežja, ta pa lahko zagotovi kakovost storitve, saj so vsi prehodi v njegovem upravljanju.

6to4 pri svoji shemi preslikavanja naslovov uporablja velik del celotnega IPv6 naslovnega prostora, vendar s tem omogoči dodelitev /48 bloka vsakemu IPv4-naslovu, kar je dovolj za vsako omrežje, ki se nahaja za njim. Ponudnikom internetnih storitev se po drugi strani v glavnem dodeli prefiks /32. Če internetni ponudnik s prefiksom /32 za 6rd uporabi enak način preslikave kot pri 6to4, to ustreza IPv6-bloku /64 za vsak IPv4 naslov, kar pa ne zadošča vsem uporabnikom, saj blok /64 omogoča naslavljanje zgolj v enem samem lokalnem omrežju.

6rd zaradi teh okoliščin omogoča večjo fleksibilnost pri shemi preslikavanja. Pri 6rd vključen IPv4-naslov nima fiksne pozicije, prav tako pa ni treba, da se uporabi vseh 32 bitov naslova.

Manjši ponudnik, ki vsem svojim strankam dodeli naslove iz IPv4-bloka /16, lahko na primer preslika v IPv6 samo spodnjo polovico IPv4-naslova, torej spodnjih 16 bitov:

V večjih omrežjih, kjer dodeljujejo strankam naslove iz veliko različnih blokov, pa je bolj primerna pridobitev večje alokacije IPv6-naslovov (npr. /24). To omogoči preslikavo celotnega IPv4-naslovnega prostora, odjemalci pa lahko še vedno dobijo razmeroma velik IPv6-blok, npr. /56:



V praksi je zelo težko pridobiti tako velik IPv6-naslovni blok, kot v zgornjem primeru (/24), vendar v večini primerov zadošča že manjši, npr. /28, ki omogoča dodelitev IPv6-blokov /60. Stranke lahko v tem primeru naslovijo do 16 lokalnih omrežij /64. Na zadnjem srečanju skupnosti RIPE maja 2011 je bil predlagano, da se internetnim ponudnikom privzeto odobri IPv6-blok velikosti /29 namesto trenutno uveljavljenega /32. S tako alokacijo bi vsak ponudnik lahko namenil /30 za 6rd in strankam dodeljeval bloke /62.

Ravno tako kot pri 6to4 lahko ponudniki interneta prehodom v svojem omrežju nastavijo *anycast* naslove in se s tem izognejo kritični točki odpovedi ter povečajo zmogljivost.

Podobno kot 6rd deluje tudi 4rd (“*IPv4 Residual Deployment*”), kjer gre za algoritmično preslikavo IPv6-naslova v kombinacijo IPv4-naslova in razpona vrat višjenivojskih protokolov. Podobno kot DS-lite je namenjen zagotavljanju IPv4-povezljivosti prek IPv6-infrastrukture.

Translacijski mehanizmi

Tunelski mehanizmi omogočajo, da med seboj povežemo IPv6-otoke, tako da tvorimo navidezne povezave. Translacijski mehanizmi po drugi strani omogočajo neposredno komunikacijo med napravami, ki podpirajo zgolj enega izmed protokolnih skladov. Ti mehanizmi bodo še posebej pomembni v času po popolni izčrpanosti IPv4-naslovnega prostora, ko bodo organizacije in končni uporabniki lahko dobili zgolj še IPv6-povezljivost, velik del preostalega interneta pa bo še vedno uporabljal IPv4.

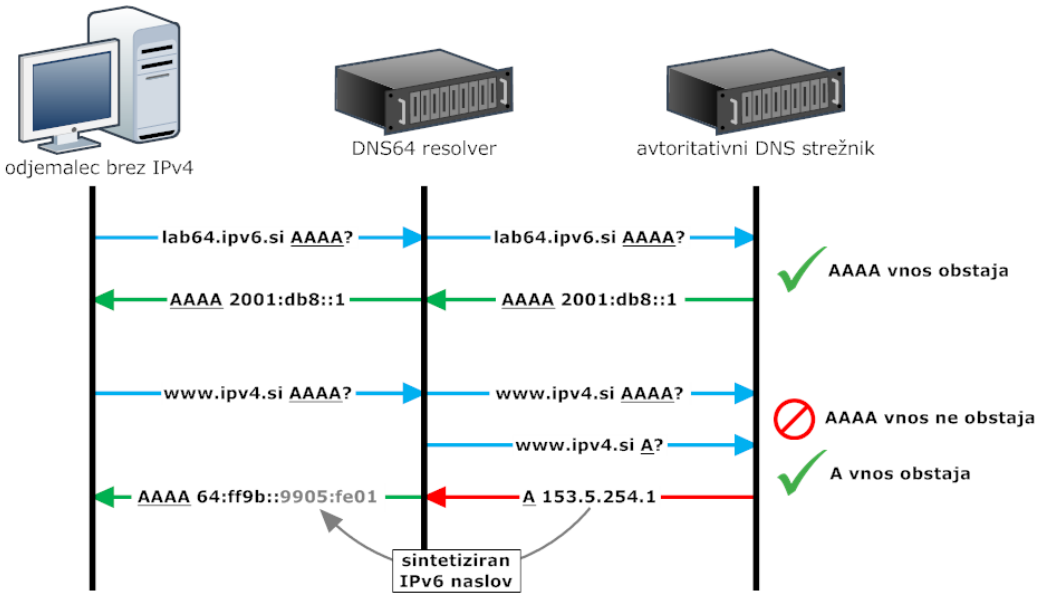
Po trenutnih projekcijah naj bi vsi regionalni registri dosegli zadnji IPv4-blok /8 do leta 2014, pri čemer je variacija med posameznimi registri velika. APNIC je to točko dosegel že aprila letos, za RIPE NCC se pričakuje, da bo zadnji /8 dosegel marca 2012, ARIN in AfriNIC do jeseni 2013, zadnji pa naj bi to točko dosegel LACNIC.

Pomembno je, da na *dual-stack* preide večina ponudnikov vsebin. Če večina spletnih strani in drugih aplikacij podpira IPv6, potem uporabniki, ki so na izključno IPv6-omrežju ne občutijo velike razlike. Kljub temu pa je v rabi še veliko podedovanih sistemov, ki so inherentno nekompatibilni z IPv6. Treba je poskrbeti, da lahko uporabniki, ki so na izključno IPv6-omrežjih, takšne storitve uporabljajo.

Translacija v drugo smer ni tako bistvenega pomena. Ko bodo ponudniki vsebin zaradi pomanjkanja naslovov začeli prehajati na izključno IPv6, bo to povečalo iniciativo odjemalcev, da posodobijo svoja omrežja. V tem primeru je lažje uporabiti mehanizme za tuneliranje, kot uporabljati zapletene translacijske sheme [1].

DNS64/NAT64

NAT64 in DNS64 sta protokola, ki omogočata odjemalcem, ki imajo zgolj IPv6-povezljivost, da komunicirajo z strežniki, ki imajo zgolj IPv4-naslov. DNS64 je opisan v RFC 6147 (*"DNS DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers"*), NAT64 pa v RFC 6144 ("Framework for IPv4/IPv6 Translation") in RFC 6147 (*"Stateful NAT Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers"*).



Shema delovanja DNS64

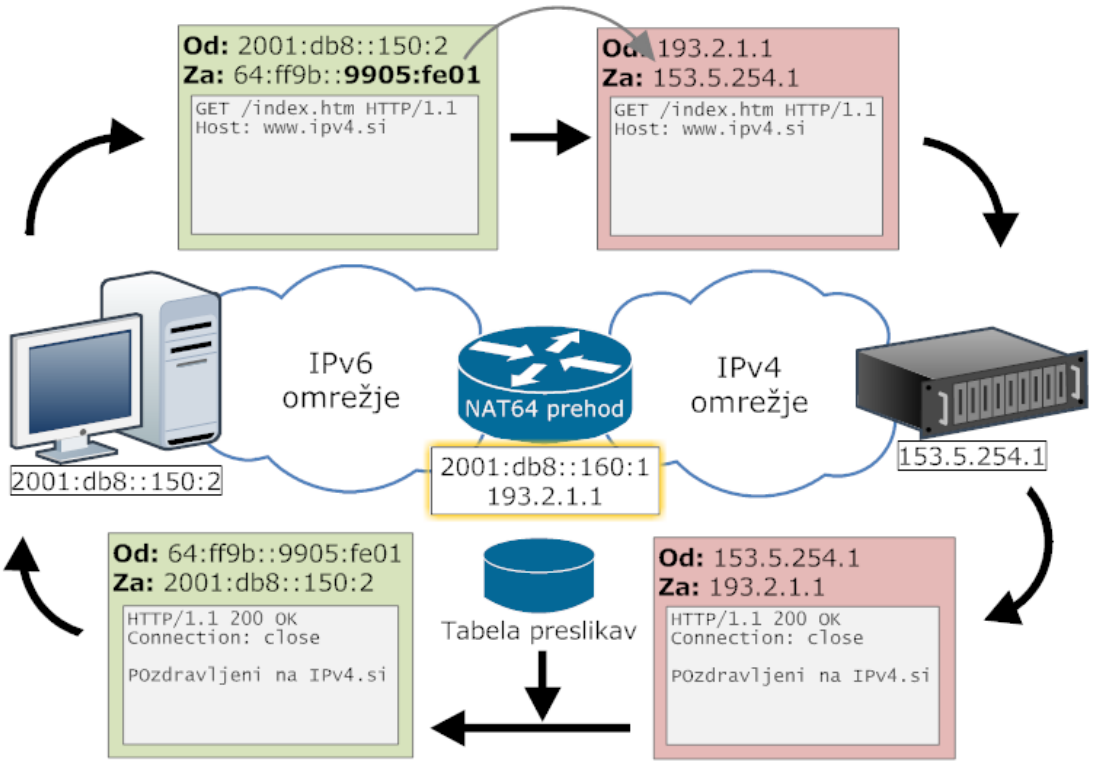
DNS64 temelji na prilagojenem imenskem strežniku – resolverju za DNS, ki je dostopen prek IPv6 in na katerega odjemalci v omrežju pošiljajo poizvedbe. Če privzamemo, da odjemalci v omrežju nimajo IPv4-povezljivosti, bodo pošiljali AAAA (IPv6-naslov) poizvedbe za razrešitev domenskih imen.

DNS64 resolver posreduje poizvedbo odjemalca avtoritativnemu domenskemu strežniku. Če avtoritativni strežnik odgovori z AAAA zapisom, ga DNS64 resolver posreduje nazaj

odjemalcu in ta se lahko poveže na strežnik prek IPv6. Če avtoritativni strežnik ne vrne AAAA zapisa, DNS64 sproži še eno poizvedbo, in sicer za A zapis (IPv4-naslov). Če dobi odgovor, sintetizira AAAA zapis za to domeno in zapis pošlje nazaj odjemalcu kot odgovor na njegovo zahtevo, v nasprotnem pa javi napako.

Sintetiziran AAAA zapis se tvori tako, da se znanemu prefiksu na koncu priključi IPv4-naslov v šestnajstiškem zapisu. Po RFC 6052 se lahko za prefiks uporabi `64:ff9b::/96` ali poljuben drug prefiks iz ponudnikove lastne alokacije.

S stališča odjemalca je strežnik, za katerega domeno je bila sprožena poizvedba, dostopen prek IPv6, saj je DNS-poizvedba vrnila AAAA zapis. Za to, da lahko odjemalec dejansko vzpostavi povezavo z omenjenim strežnikom, pa poskrbijo NAT64-prehodi na meji med IPv6 in IPv4-omrežjema. Ponudnik, ki upravlja omrežje, usmeri vse pakete, ki so namenjeni na naslove iz NAT64-prefiksa, na NAT64-prehode. Ko NAT64-prehod prejme IPv6-paket, iz njega izlušči IPv4-naslov ter ga uporabi kot ciljni naslov v novem IPv4-paketu, za izvorni naslov pa uporabi enega izmed naslovov iz svoje zaloge.



Shema delovanja NAT64

Ločimo dva tipa NAT64-prehodov:

- NAT64-prehodi brez ohranjanja stanja (angl. *stateless)* – uporabljajo statično ali algoritmično preslikavo med IPv6-naslovom odjemalca in uporabljenim izvornim IPv4-naslovom. Prednost te oblike je, da zahteva precej manj sredstev na prehodih in olajša izenačevanje obremenitve. Slabost je, da potrebuje zelo veliko IPv4-naslovov za delovanje (ponavadi 1 naslov za vsakega odjemalca), zato je uporabnost takšnih prehodov s stališča varčevanja z IPv4-naslovi omejena.
- NAT64-prehodi z ohranjanjem stanja (angl. *stateful)* – uporabljajo dinamično tabelo preslikav med naslovi in vrati višjenivojskih protokolov (recimo TCP). *Stateful* NAT64 zahteva kompleksnejšo implementacijo in poveča obremenitev na prehode, vendar omogoča delovanje z manjšim številom IPv4-naslovov (za manjša omrežja zadošča samo eden).

Poglavitna prednost NAT64/DNS64 je enostavnost konfiguracije odjemalcev. Za komunikacijo z IPv4-strežniki v veliko primerih zadostuje, da zgolj nastavimo DNS-resolver odjemalca na naslov našega DNS64-strežnika in usmerimo NAT64-prefiks na prehod.

Največja omejitev DNS64/NAT64 je zanašanje na DNS, da poskrbi za preslikavo med IPv4-naslovom in IPv6-naslovom strežnika. Aplikacije, ki uporabljajo vgrajene IP-naslove, tako ne morejo dostopati do interneta, ker DNS poizvedba ne bo nikoli oddana. Drugi problem predstavljajo aplikacije, ki so nezdružljive z IPv6, ker uporabljajo starejše programske vmesnike za povezljivost, ki ne predvidevajo IPv6-naslovov.

NAT64 prinaša tudi klasične težave, ki so povezane z uporabo NAT-prehodov in ne nujno vezane na uporabo IPv6. Aplikacije in protokoli, ki zahtevajo povezavo brez vmesnih naprav (middlebox-ov), npr. VoIP, lahko ob uporabi NAT64 delujejo moteno.

Drugi tranzicijski mehanizmi

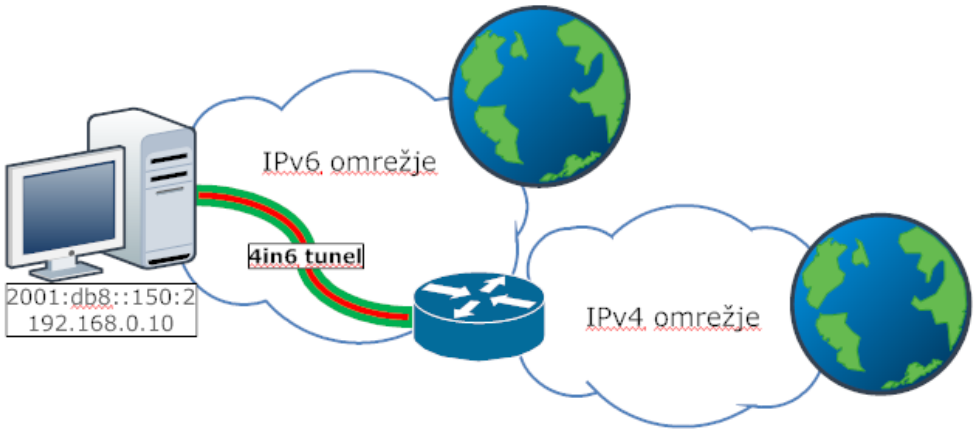
Teredo

Medtem ko se 6to4 in 6rd v glavnem uporabljata za povezavo IPv6-omrežij prek IPv4-infrastrukture, je Teredo namenjen povezavi posameznih končnih naprav v IPv6-internet. Glavna razlika med Teredom in do zdaj omenjenimi protokoli je, da Teredo uporablja UDP kot transportni protokol, kar mu omogoča povezavo skozi NAT prehode in požarne zidove. Teredo je bil razvit pri Microsoftu in kasneje standardiziran kot RFC 4380 (*"Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)"*).

Posamezne končne naprave, ki uporabljajo Teredo, dobijo IPv6-naslov iz bloka `2001:0::/32`, v naslov pa so zakodirane različne informacije, ki povedo Teredo prehodu, kam naj pošilja prejete pakete.

Teredo naj bi se uporabljal kot "last resort", torej kadar povezava v IPv6-internet ni mogoča nikakor drugače, saj je njegova zmogljivost vprašljiva.

DS-lite (Dual-stack Lite)



Shema DS-lite omrežja

DS-lite je tranzicijski mehanizem, ki podobno kot NAT64/DNS64 omogoča priklop uporabnikov v omrežje z izključno IPv6-povezljivostjo, hkrati pa omogoča dostop do delov interneta, ki še vedno uporabljajo IPv4. V nasprotju z NAT64 je DS-lite tunelski mehanizem, le da pri njem gre za enkapsulacijo IPv4-paketov v IPv6-pakete, tako imenovani *4in6 protokol*.

Končne naprave ali usmerjevalniki, ki zaključujejo tunel na strani uporabnika, dobijo dodeljene privatne IPv4-naslove, ves IPv4-promet pa pošiljajo prek tunela do NAT-prehoda, ki omogoči dostop do interneta.

DS-lite lahko primerjamo z dual-stack omrežjem, ki uporablja privatne naslove in CGN (*carrier-grade NAT*) za IPv4 ter domorodno IPv6-povezljivost, vendar DS-lite olajša vzdrževanje omrežja in zmanjša porabo IPv4-naslovov, ker omogoči da se lahko IPv4 opusti povsod razen na tistem delu, kjer se zaključujejo tuneli in izvaja NAT.

Če primerjamo DS-lite z NAT64, ima prej omenjeni bistveno prednost, da deluje z vgrajenimi IPv4-naslovi in aplikacijami nekompatibilnimi z IPv6, saj ima končna naprava omogočena oba protokolna sklada. Po drugi strani DS-lite zahteva več konfiguracije, saj je treba nastaviti tunele na napravah, ki jih zaključujejo.

Poleg omenjenih tunelskih protokolov, obstajajo tudi drugi, ki pa imajo omejeno uporabnost:

- TSP *(Tunnel Setup Protocol)* – protokol za avtomatsko konfiguracijo različnih vrst tunelov prek posrednika
- ISTAP *(Intra-Site Automatic Tunnel Addressing Protocol)* – omogoča IPv6-povezljivost med dual-stack končnimi napravami v lokalnem omrežju prek IPv4-omrežja
- 6over4 – podobno kot ISATAP, vendar temelji na IPv4-multicastu, ki ni široko podprt
- AYIYA *(Anything In Anything)* – omogoča nastavitev ročno konfiguriranih tunelov skozi NAT-prehode

Testno omrežje

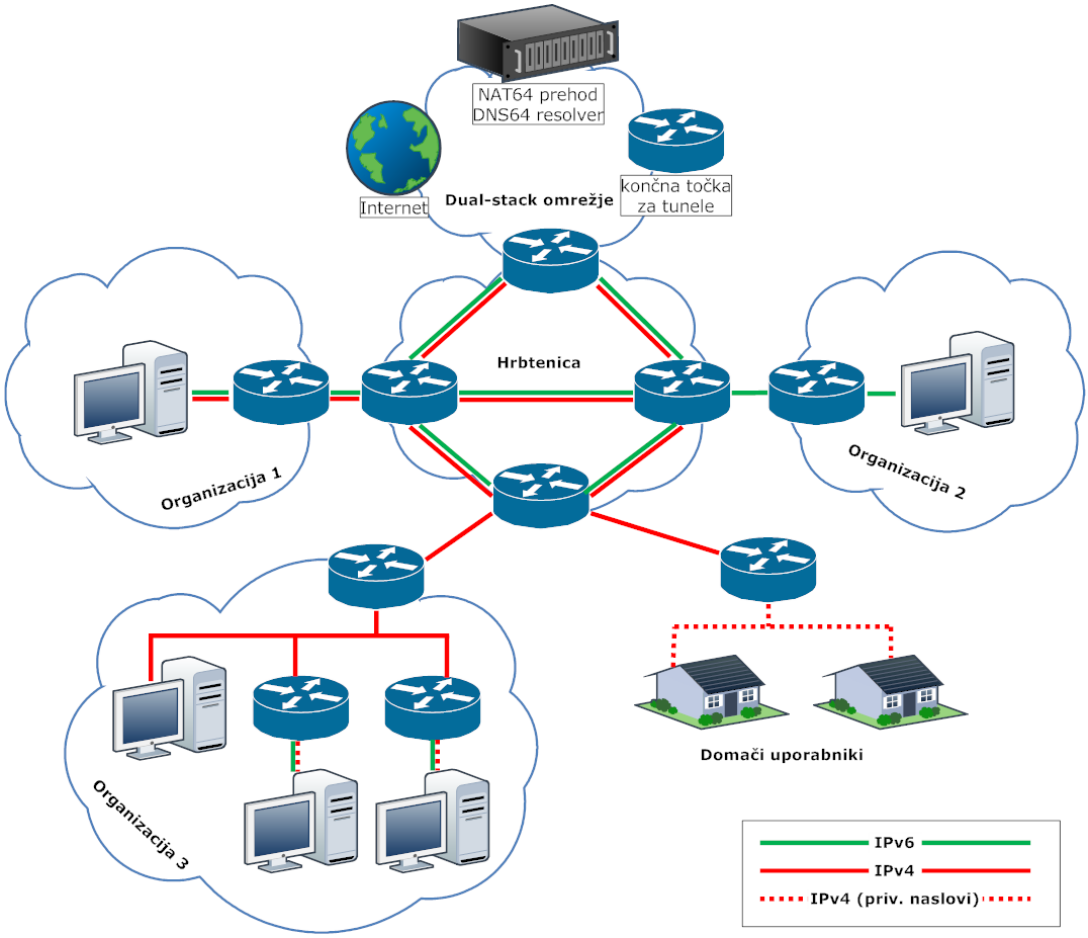
Testno omrežje za predstavitev tranzicijskih mehanizmov obsega

- hrbtenično omrežje namišljenega ISP-ja,
- lokalna omrežja treh priklopljenih organizacij in
- priklop domačih uporabnikov.

Namen omrežja je prikazati čim več različnih konfiguracij IPv4 in IPv6-povezljivosti, ki jih lahko pričakujemo v času pred in po izčrpanosti IPv4-naslovnega prostora.

Omrežje zaobjema naslednje konfiguracije:

- Dual-stack povezljivost **(Organizacija 1),**
- samo IPv6-povezljivost **(Organizacija 2)**,
  - dostop do IPv4-interneta prek NAT64/DNS64 in
  - dostop do IPv4-interneta s pomočjo DS-lite.
- samo IPv4-povezljivost **(Organizacija 3)** ter
  - IPv6-povezljivost prek statičnega tunela,
  - IPv6-povezljivost prek 6rd in
  - IPv6-povezljivost prek 6to4
- samo IPv4 z uporabo CGN **(domači uporabniki)**.
  - IPv6-povezljivost z uporabo Tereda in
  - IPv6-povezljivost z uporabo 6rd.



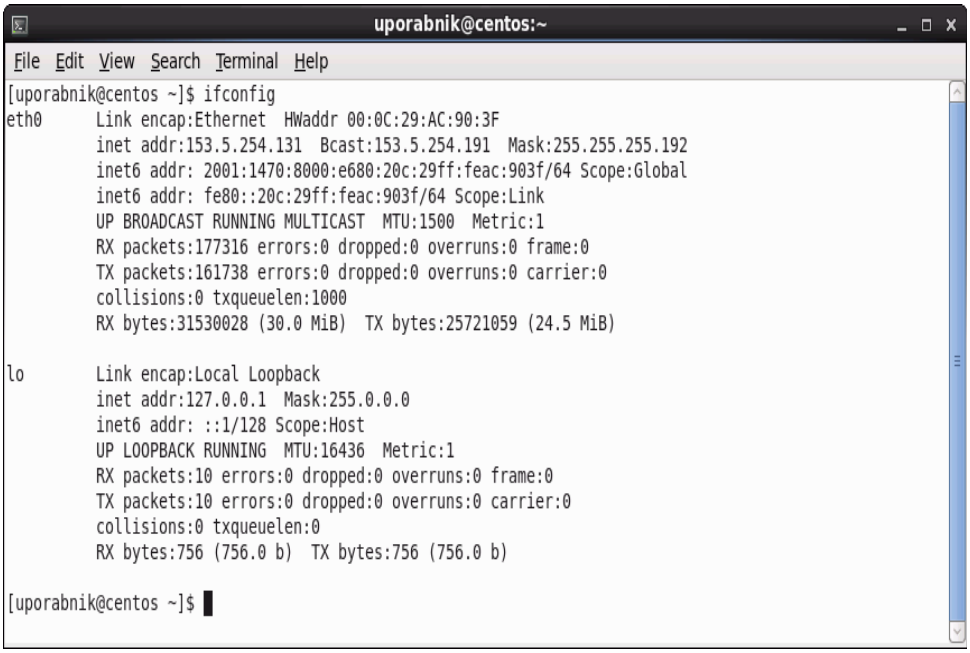
Hrbtenični del omrežja je popolnoma dual-stack, razlike pa nastopijo v dostopovnem delu in lokalnih omrežjih, kot vidimo iz sheme.

Organizacija 1

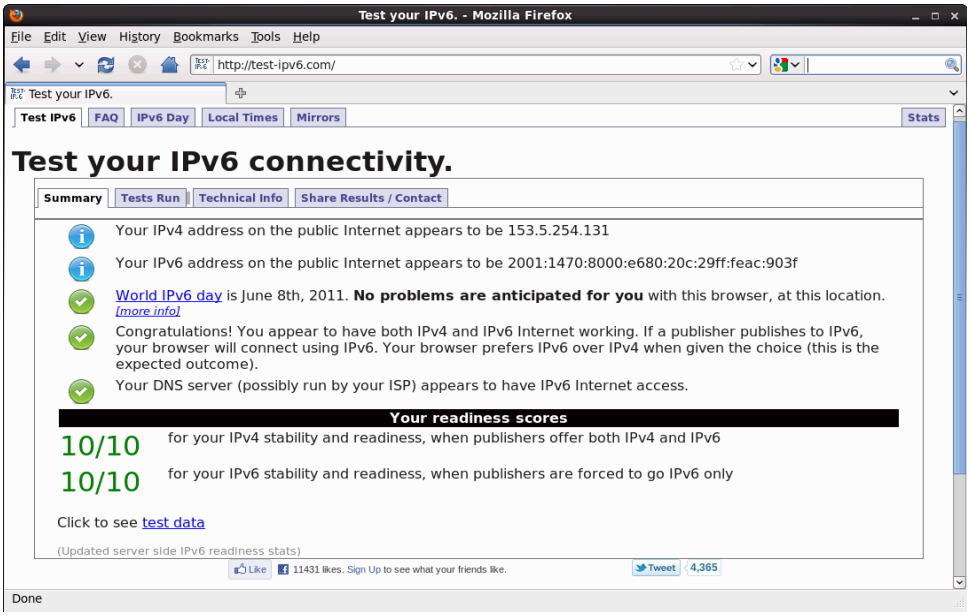
Organizacija 1 ima vzpostavljeno polno dual-stack povezljivost z javnimi IPv4 in IPv6-naslovi brez uporabe kakršnih koli tunelov. Težav pri povezavi ne pričakujemo.

Usmerjevalnik Organizacije 1 podpira DHCP in RA, zato končne naprave, ki jih priklopimo v omrežje, ne potrebujejo nobene dodatne konfiguracije.

Računalnik Organizacije 1 ima nameščen operacijski sistem **CentOS 6.0**. Ukaz `ifconfig` pokaže, da imamo nastavljena oba tipa naslovov:



IPv6-test na http://test-ipv6.com/ pokaže popolno pripravljenost na IPv6:

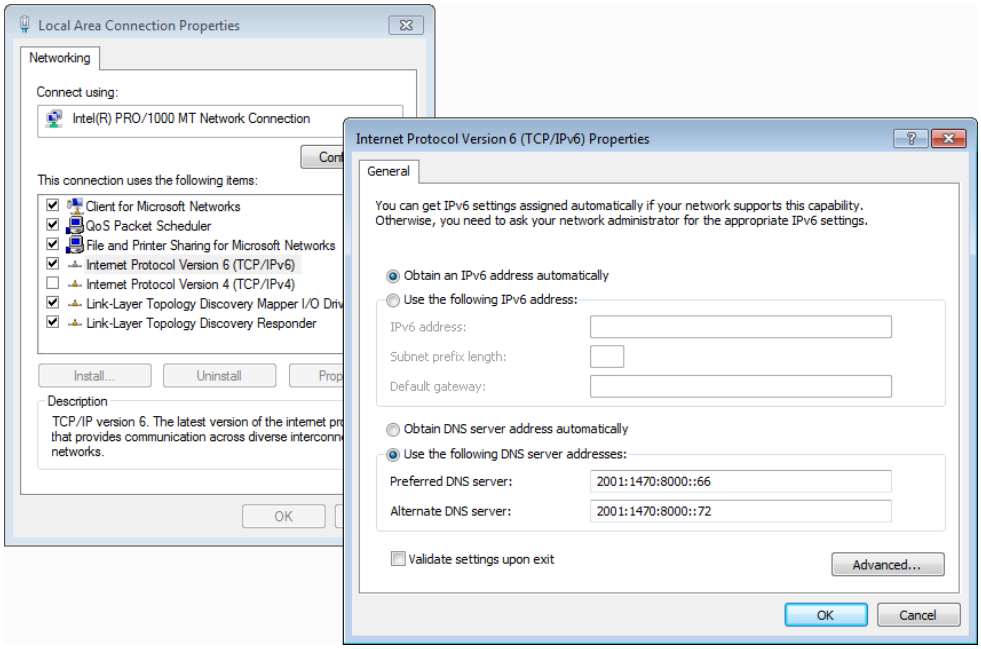


Organizacija 2

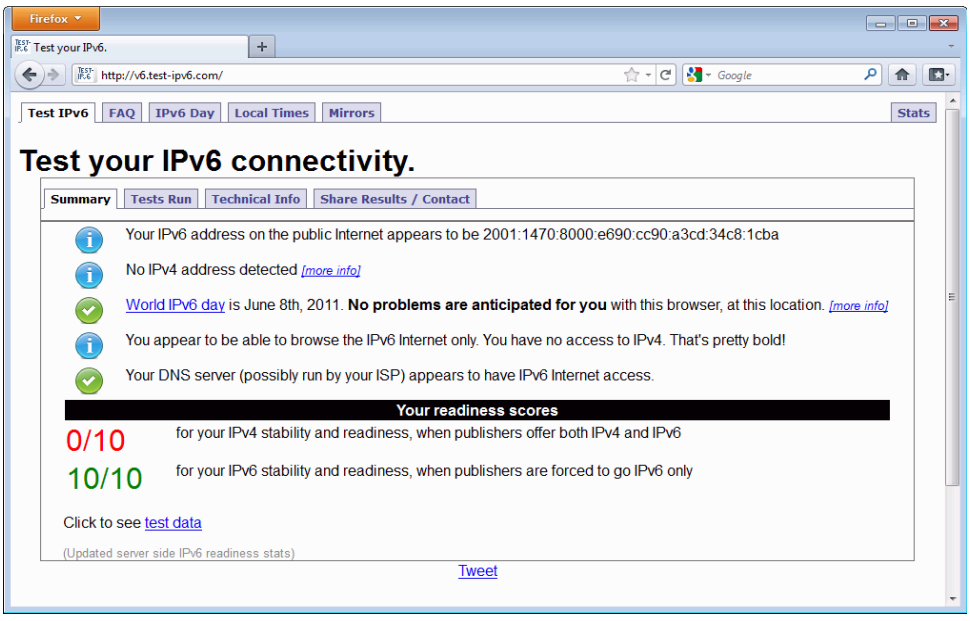
Organizacija 2 ima vzpostavljeno samo IPv6-povezljivost v internet. Ta konfiguracija predstavlja realističen scenarij v času po izčrpanosti IPv4-naslovnega prostora.

Računalnik, ki je povezan v omrežje Organizacije 2, ima nameščen operacijski sistem **Windows 7.**

Kot vidimo, je IPv4-protokolni sklad izključen, konfiguracija IPv6 pa poteka s pomočjo RA. Edina stvar, ki jo je treba nastaviti, je strežnik DNS. Poskusimo najprej z Arnesovimi strežniki DNS:

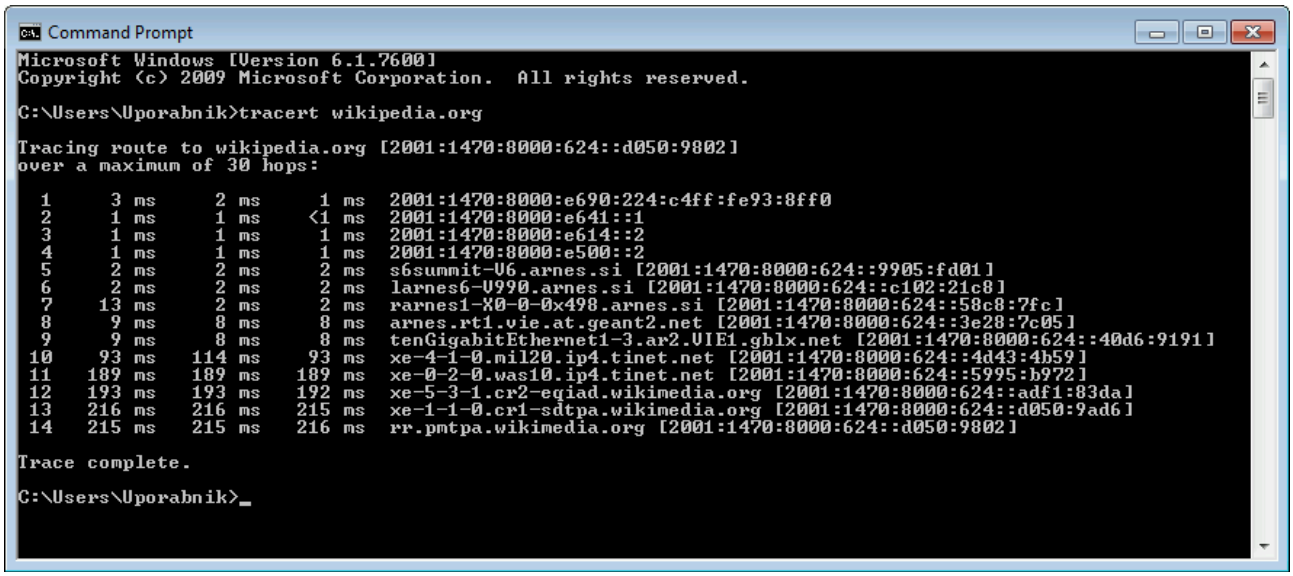


S temi nastavitvami lahko dostopamo le do peščice spletnih strani (npr. večino storitev, ki jih ponuja Google), preostale aplikacije, ki dostopajo do spleta, pa v glavnem ne delujejo. Test pokaže:



Ker želimo imeti dostop do IPv4-interneta, uporabimo NAT64-prehod/DNS64-strežnik. Postavljen je zunaj omrežja, nameščen ima operacijski sistem **Fedora 14,** uporablja pa paket **Ecdysis** in dodatno programsko kodo (*patch*) za DNS-resolver **Unbound**.
Namesto znanega prefiksa `64:ff9b::/96` se za translacijo uporablja javni naslovni blok `2001:1470:8000:624::/96`. V testnem okolju sta NAT64-prehod in strežnik DNS64 postavljena na istem računalniku na skupnem naslovu `2001:1470:8000:e500::2`. V produkcijskem okolju to ni običajno, saj sta NAT64 in DNS64 ločeni napravi.

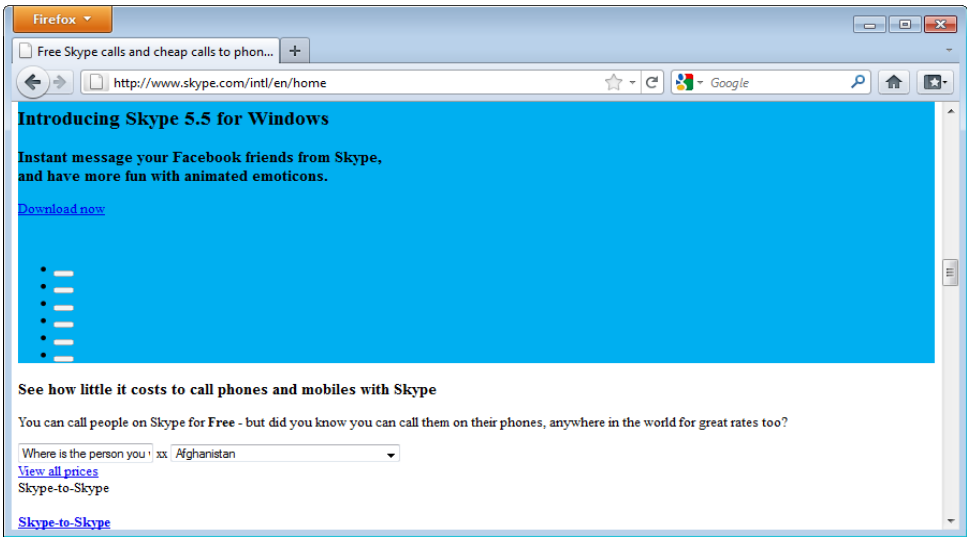
Ko nastavimo DNS-resolver na naš DNS64-strežnik, naredimo *traceroute* na *wikipedia.org*, ki je za časa pisanja dosegljiv zgolj prek IPv4:



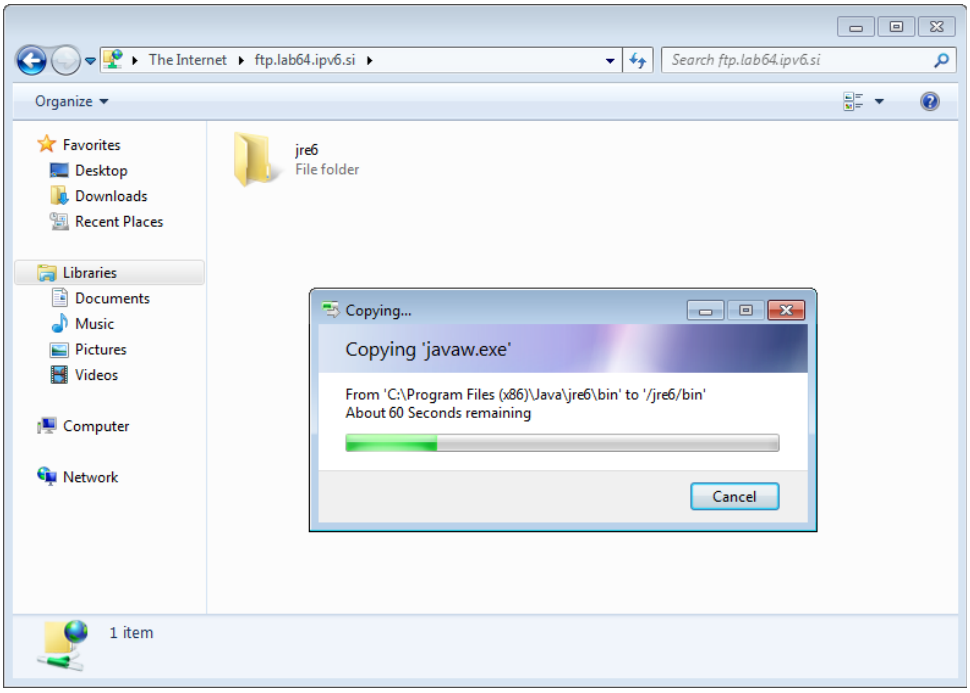
Kot vidimo, imajo od četrtega koraka naprej vsi naslovi prefiks `2001:1470:8000:624/96`, kar pomeni, da poteka translacija.

Uporaba internetnega brskalnika poteka v glavnem brez težav, kar potrdimo z obiskom spletne strani, ki de dosegljiva zgolj prek IPv4 (*IPv4 only*):

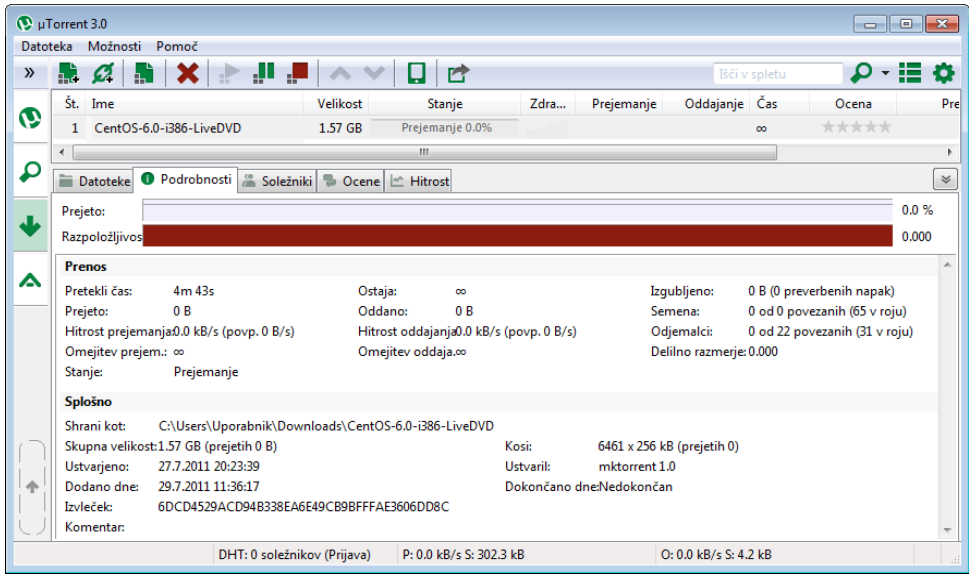
Občasno se pojavijo težave, kjer spletne strani niso prikazane v celoti. Takšne težave so najpogosteje posledica uporabe vključenih IPv4-naslovov:



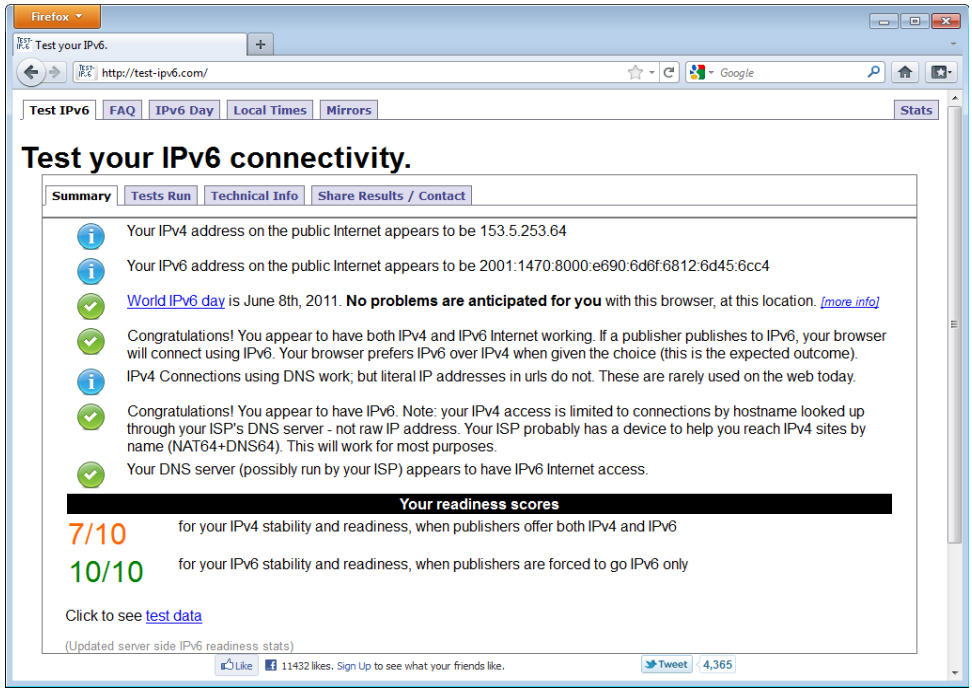
Če poskusimo FTP-povezavo na strežnik, ki ima samo IPv4-naslov, ta deluje (tako *upload* kot *download*):



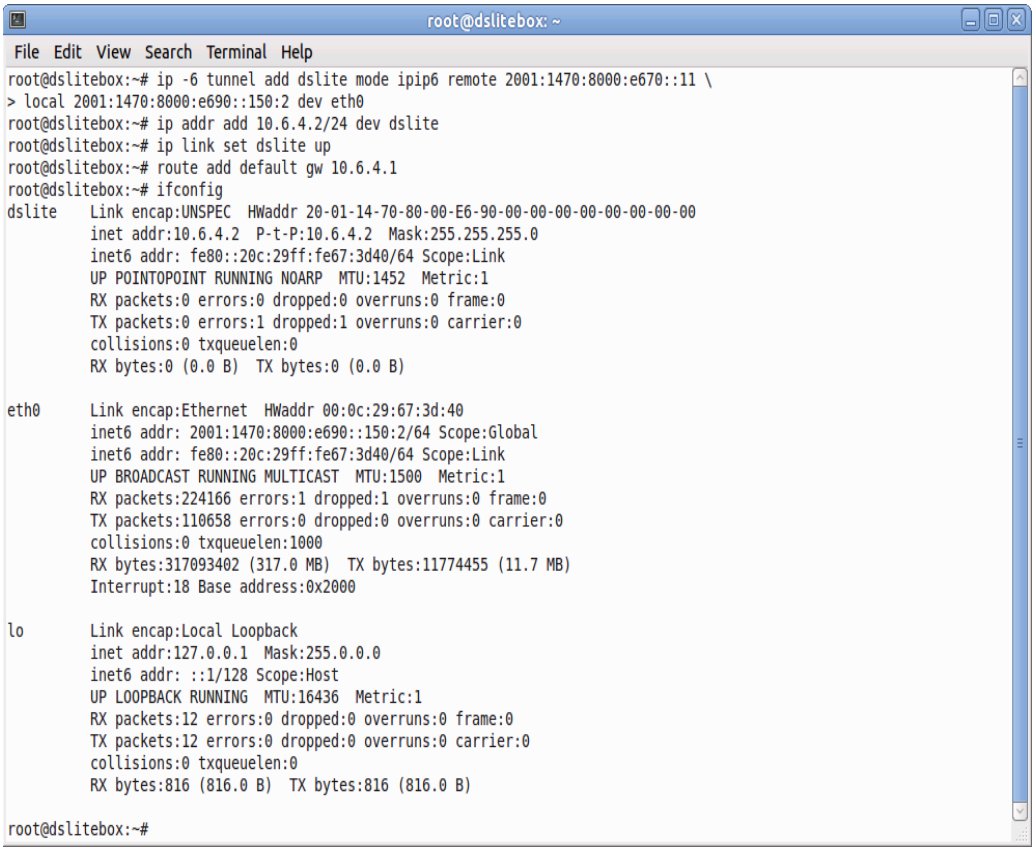
Peer-to-peer aplikacije v glavnem ne delujejo, saj protokoli predvidevajo vključene IPv4-naslove, problem pa predstavlja tudi translacija NAT:



Rezultati testa IPv6:



V omrežje Organizacije 2 postavimo še en računalnik (**Ubuntu 11.04**), kjer IPv4-povezljivost priskrbimo s pomočjo DS-Lite:



Naprava, ki na drugi strani zaključuje tunel, izvaja translacijo NAT ter s tem omogoča dostop do IPv4-interneta. Kot vidimo, lahko do IPv4-interneta s pomočjo DS-lite dostopamo tudi, ko uporabljamo eksplicitne naslove, čeprav lokalno omrežje Organizacije 2 ne podpira IPv4:

Organizacija 3

Organizacija 3 dobi od ponudnika zgolj IPv4-povezljivost. V primerjavi z organizacijami 1 in 2 ima ta nekoliko kompleksnejšo strukturo lokalnega omrežja. Sestavljajo ga računalnik, ki je povezan neposredno na njihov dostopovni usmerjevalnik, ter dve podomrežji, ki imata IPv6-povezljivost prek tunela:

- IT oddelek – dobi IPv6-povezljivost prek statično nastavljenega 6in4-tunela
- Računalniška učilnica – dobi IPv6-povezljivost prek 6rd-tunela

Tako IT oddelek kot računalniška učilnica se povezujeta v lokalno omrežje (LAN) organizacije in posredno internet prek usmerjevalnika **Mikrotik RouterOS**, ki morata biti nastavljena, da zaključujeta tunel. Računalniki za usmerjevalnikom imajo nastavljene privatne IPv4-naslove, usmerjevalnik pa skrbi za translacijoNAT.

IT oddelek

Tunel za IT oddelek ima nastavljen povezovalni segment `2001:1470:8000:e6f0::/64` (`::1` je ISP, `::2` pa organizacija). Za končne naprave na IT oddelku je uporabljen segment /64, usmerjevalnik pa izvaja RA za avtomatske nastavitve končnih naprav v lokalnem omrežju:

Konfiguracija usmerjevalnika IT oddelka:

```
/interface 6to4
add disabled=no local-address=153.5.254.200 mtu=1480 name="IPv6 tunel" \
    remote-address=153.5.253.6
/ipv6 address
add address=2001:1470:8000:e6f0::2/64 advertise=no disabled=no eui-64=no \
    interface="IPv6 tunel"
add address=2001:1470:8000:e6f1::1/64 advertise=yes disabled=no eui-64=no \
    interface="IT oddelek"
/ipv6 route
add dst-address=2000::/3 gateway=2001:1470:8000:e6f0::1
```

Računalnik IT oddelka ima nameščen operacijski sistem **Windows 7**, konfiguracijo pa dobi prek DHCP in SLAAC/RA, zato za polno povezljivost ni potrebna nobena konfiguracija.

Računalniška učilnica

Usmerjevalnik računalniške učilnice ima nastavljen IPv6-tunel prek istega ciljnega IPv4-naslova, kot IT oddelek, vendar je konfiguracija nekoliko drugačna zaradi drugačnega tipa tunela. Pri 6rd ne uporabimo povezovalnega segmenta (na tunelskem vmesniku ne definiramo nobenih naslovov), ampak zgolj usmerimo ves promet, namenjen v internet, neposredno na vmesnik.

Zunanji IP-naslov usmerjevalnika je 153.5.254.196, 6rd-prefiks v omrežju pa je `2001:1470::/32`, zato uporabimo naslovni prostor `2001:1470:9905:fec4::/64`.

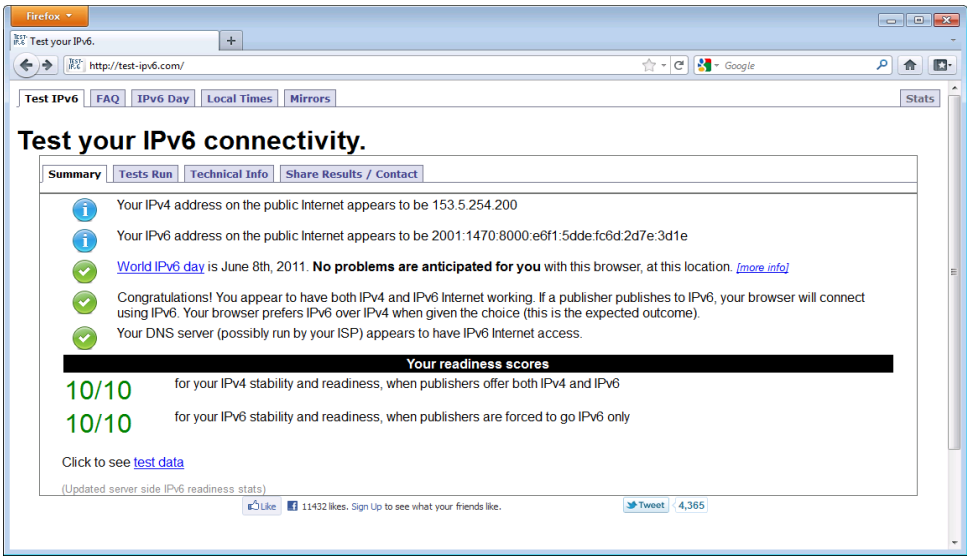
Konfiguracija usmerjevalnika računalniške učilnice:

```
/interface 6to4
add disabled=no local-address=153.5.254.196 mtu=1480 name="6rd tunel" \
    remote-address=153.5.253.6
```

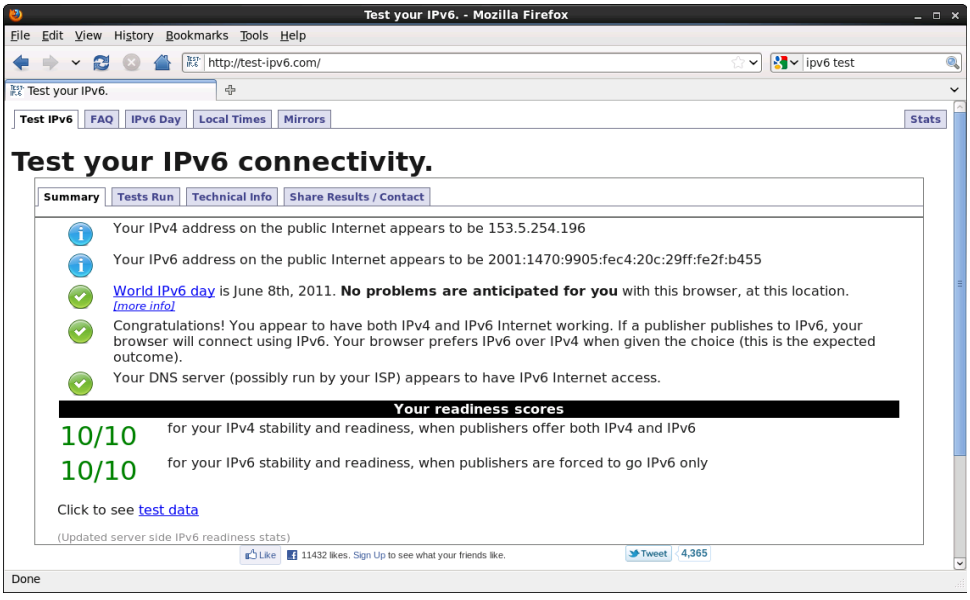
```
/ipv6 address
add address=2001:1470:9905:fec4::1/64 advertise=yes disabled=no eui-64=no \
    interface="Racunalniska ucilnica"
/ipv6 route
add dst-address=2000::/3 gateway="6rd tunel"
```

Računalnik v računalniški učilnici ima nameščen operacijski sistem **CentOS 6.0**, konfiguracijo pa dobi prek DHCP in SLAAC/RA, zato za povezljivost ni potrebna dodatna konfiguracija.

Test IPv6 za IT oddelek:



Test IPv6 za računalniško učilnico:

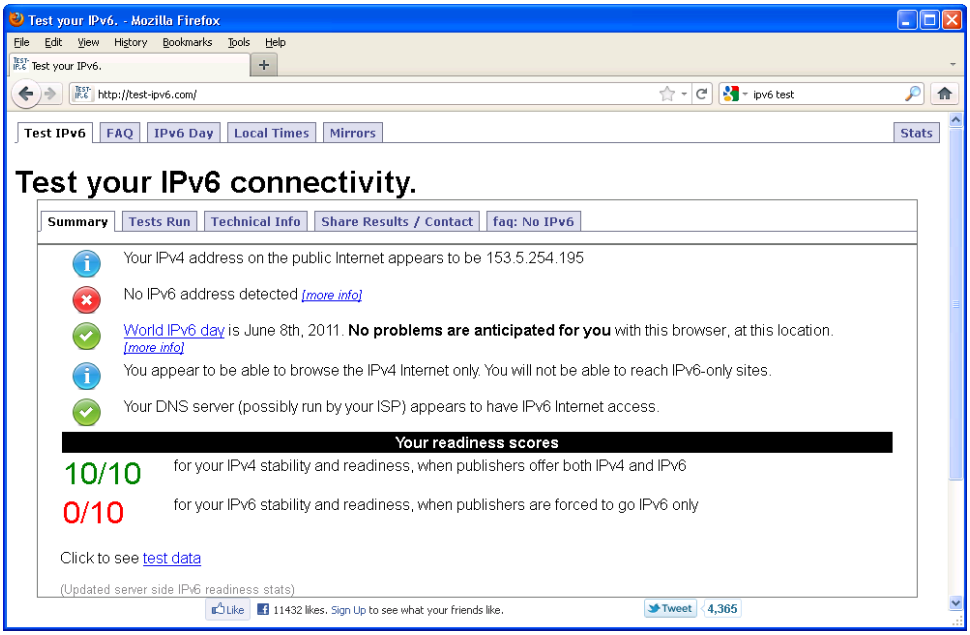


Oba testa pokažeta dober rezultat, ker je tunel navzven neviden, NAT za IPv4 pa na rezultat ne vpliva.

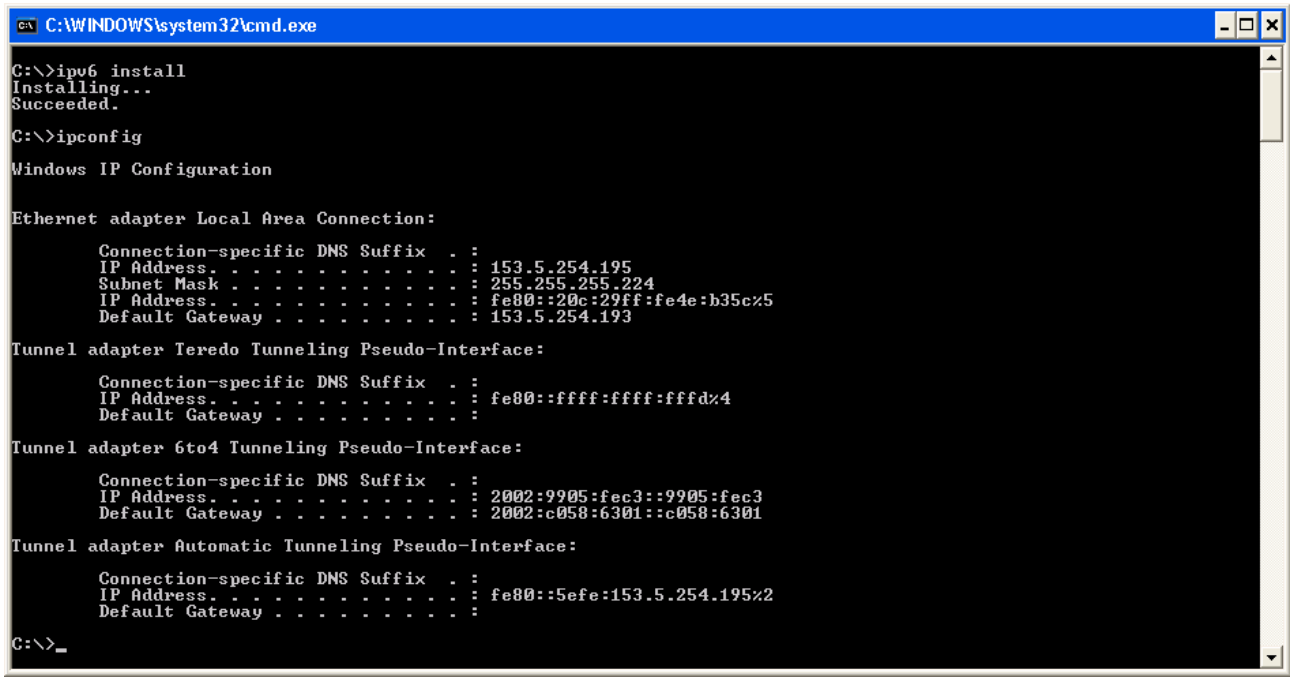
Računalnik Organizacije 3, ki je povezan neposredno na dostopovni usmerjevalnik, ima nameščen operacijski sistem **Windows XP**. Ta sistem ima javni IPv4-naslov, zato je mogoče za IPv6-dostop uporabiti 6to4. Windows XP nima polne podpore za IPv6,

protokolni sklad pa tudi ni privzeto nameščen in ga je treba namestiti.

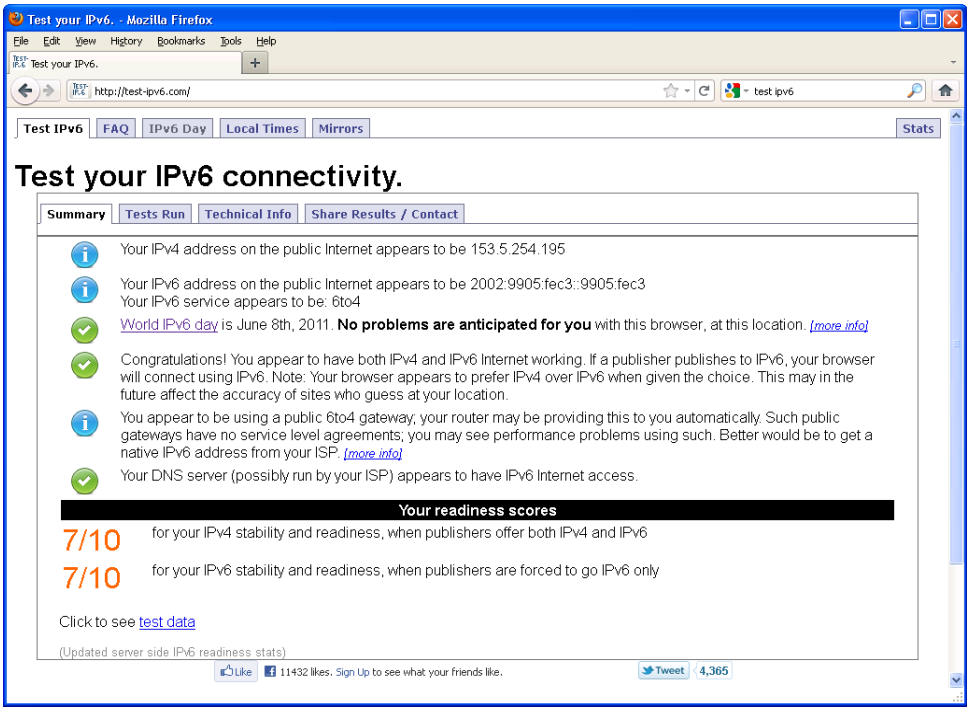
IPv6 test preden vklopimo IPv6 protokolni sklad:



IPv6-protokolni sklad namestimo z ukazom **`ipv6 install`**, Windows XP samodejno zazna, da ima nastavljen javni IP-naslov in nastavi 6to4-vmesnik:



Rezultat testa IPv6:



Dostop do IPv6-interneta je možen, kot nam pove test, vendar pa je rezultat za IPv6 zaradi manjše zanesljivosti mehanizma 6to4 nižji. Test nam pove tudi, da se brskalnik poveže prek IPv4, kadar sta na voljo oba protokola, ker uporabljamo 6to4 (sicer naj bi IPv6 imel prednost). Rezultat je nižji pri IPv4, saj lahko nekatere aplikacije dajo prednost IPv6 pri vzpostavljanju povezave, kar lahko pripelje do počasnejšega ali oteženega delovanja, kadar povezava prek tunela ni dosegljiva.

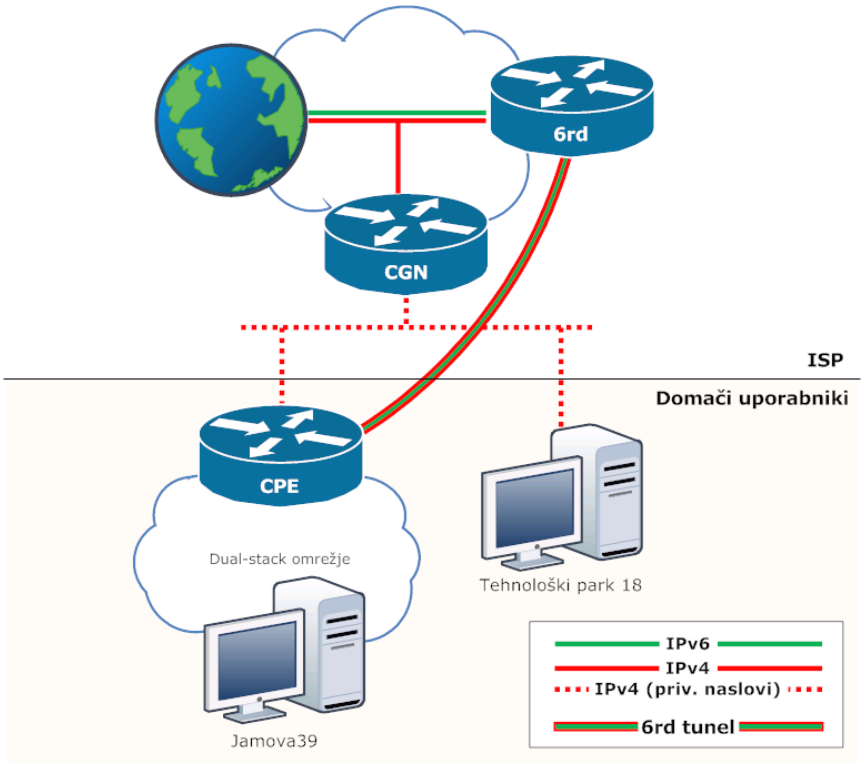
Domači uporabniki

V omrežje imamo priklopljena dva navidezna domača uporabnika – enega na Jamovi 39 in drugega na naslovu Tehnološki park 18. Glavna razlika med priklopljenimi organizacijami in domačimi uporabniki je, da slednji ne dobijo javnih IPv4-naslovov, temveč so postavljeni za *carrier-grade NAT*-prehod.

Ta konfiguracija ustreza času, ko bo zmanjkalo IPv4-naslovov, saj takrat internetni ponudniki (ISP-ji) ne bodo več mogli dodeljevati javnih naslovov svojim uporabnikom.

Končne naprave ali usmerjevalniki, ki so priključeni na omrežje, dobijo privatni IPv4-naslov iz bloka 192.168.0.0/24 od dostopovnega usmerjevalnika z mehanizmom DHCP. Če hočejo uporabniki imeti v internet povezanih več naprav, morajo izvajati še svoj lastni NAT, kar nas pripelje do položaja „dvojni NAT“, ki je lahko problematičen za zahtevnejše omrežne aplikacije.

Uporabniki, ki se za to odločijo (v našem omrežju uporabnik na Jamovi 39), lahko dobijo IPv6-povezljivost prek 6rd-tunela, ki se zaključuje na privatnih naslovih za CGN-prehodom.



Shema omrežja za domače uporabnike

Jamova 39

Uporabnik na Jamovi 39 uporablja usmerjevalnik Mikrotik RouterOS za dostop do interneta z naslednjo konfiguracijo:

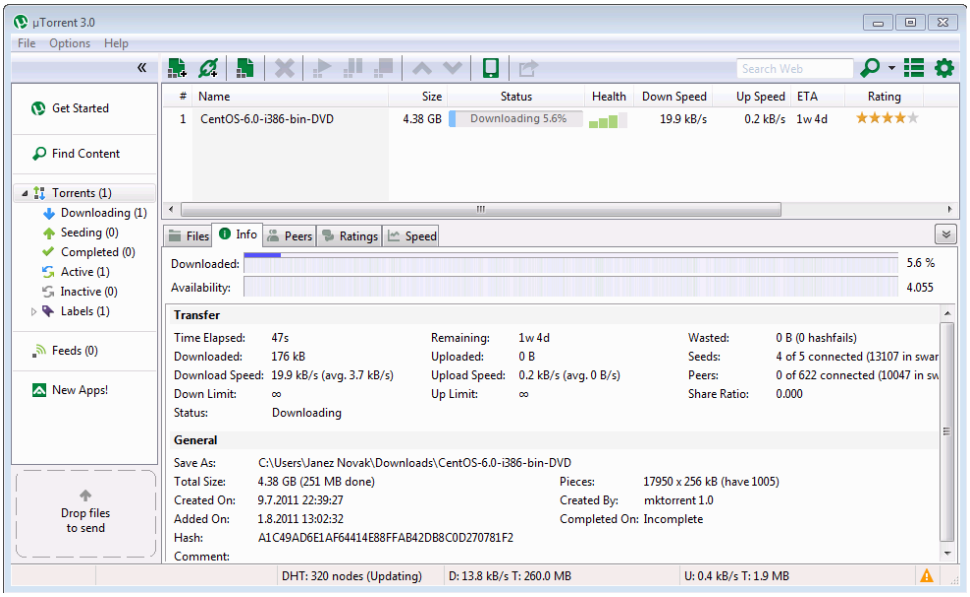
```
/interface 6to4
add disabled=no local-address=192.168.0.254 mtu=1480 name=6rd remote-address=\
    153.5.253.6
/ip pool
add name=dhcp-pool-1 ranges=10.0.0.2-10.0.0.254
/ip dhcp-server
add address-pool=dhcp-pool-1 authoritative=after-2sec-delay bootp-support=\
    static disabled=no interface=LAN lease-time=3d name=dhcp1
/ip address
add address=10.0.0.1/24 disabled=no interface=LAN network=10.0.0.0
/ip dhcp-client
add add-default-route=yes default-route-distance=1 disabled=no interface=WAN
/ip dhcp-server network
add address=10.0.0.0/24 dns-server=193.2.1.66,193.2.1.72 gateway=10.0.0.1
/ip firewall nat
add action=masquerade chain=srcnat disabled=no out-interface=WAN
/ipv6 address
add address=2001:1470:c0a8:fe::/64 advertise=yes eui-64=no interface=LAN
/ipv6 route
add dst-address=::/0 gateway=6rd
```

Opomba: čeprav ima usmerjevalnik nastavljen dinamični IPv4-naslov prek DHCP, dobi vedno isti naslov 192.168.0.254, zato da lahko statično nastavimo 6rd-prefix na `2001:1470:c0a8:fe::/64`.

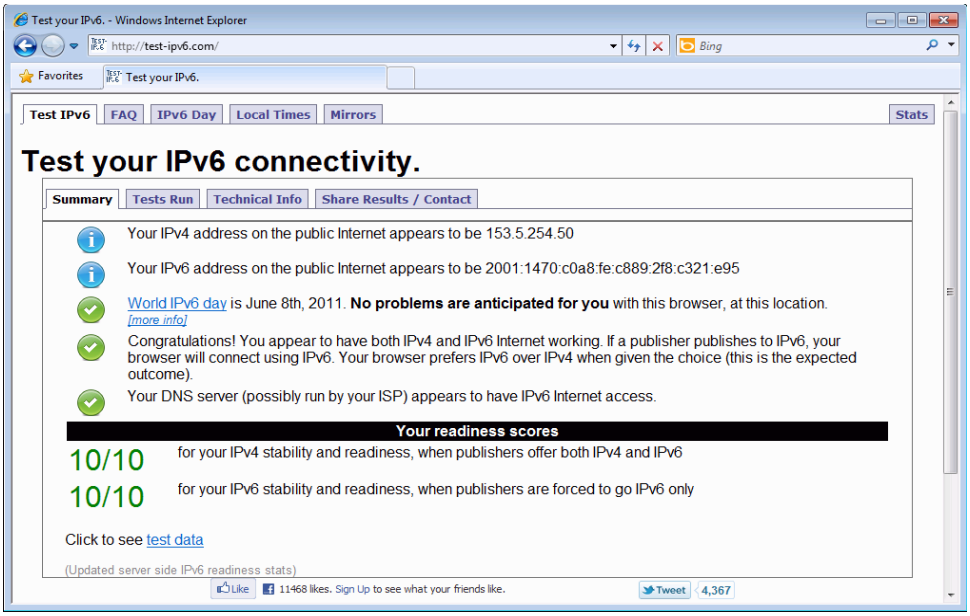
Čeprav ima 6rd-prehod podan javni naslov, ima nastavljen tunel v CGN del omrežja, zato

lahko naprave komunicirajo z njim z privatnimi naslovi in ne prihaja do translacije.

Pri večini aplikacij ne pričakujemo nobenih težav kljub dvojnemu NAT-u; do težav pride denimo pri aplikacijah, ki potrebujejo UPnP/NAT-PMP za svoje delovanje. BitTorrent na primer deluje, vendar ne moremo dobivati dohodnih povezav:

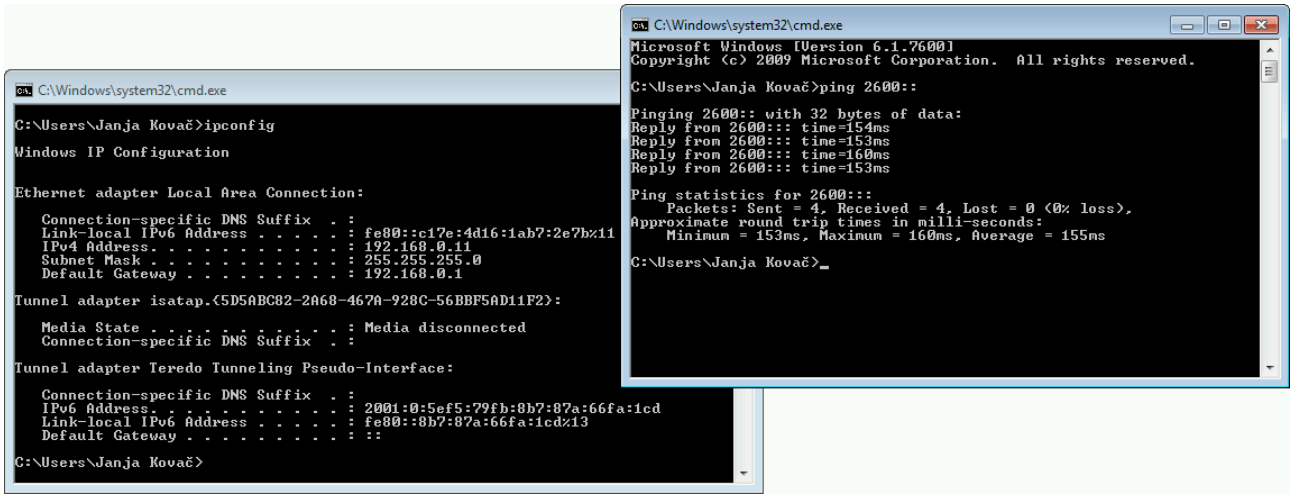


Rezultat IPv6 testa:



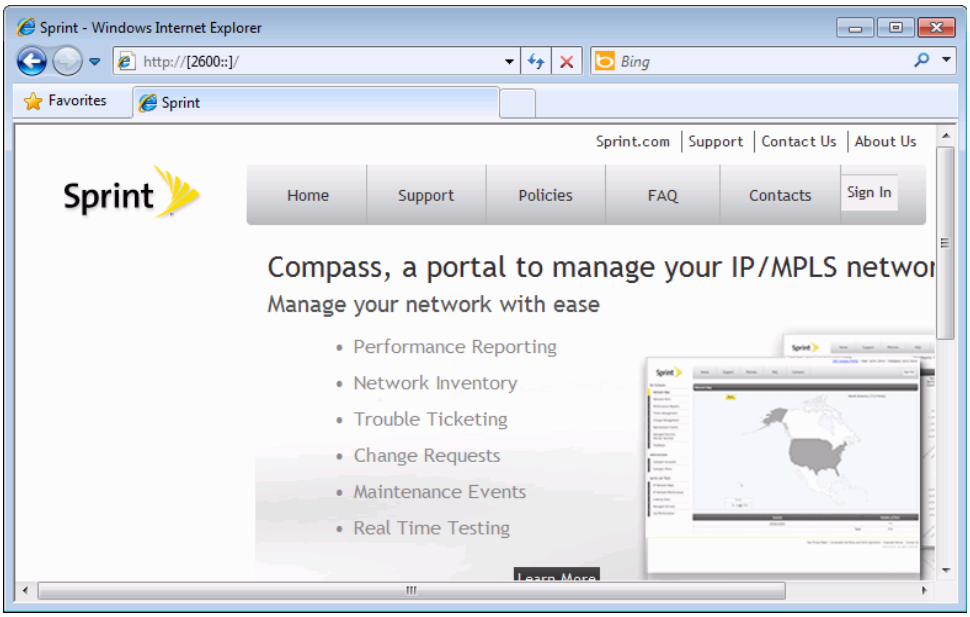
Tehnološki park 18

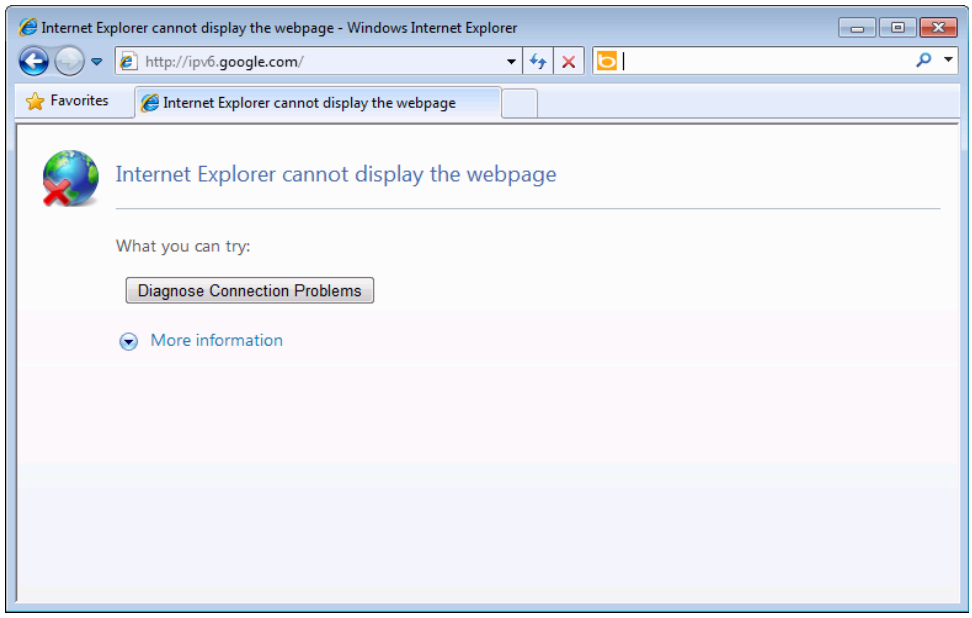
Uporabnica, ki stanuje v Tehnološkem parku, ima priključen na omrežje ISP-ja samo en PC, ki ima nameščen **Windows 7**. Uporabnica nima želje po uporabi IPv6, zato nima nastavljenega 6rd-tunela, vendar ima privzeto vklopljen Teredo.



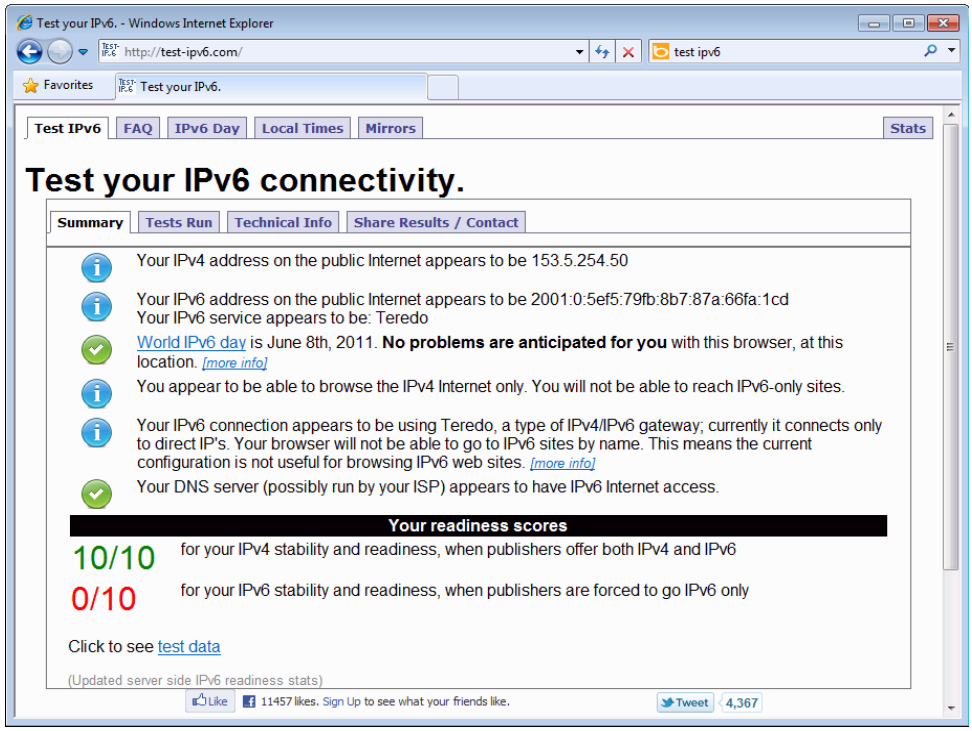
Kot vidimo, lahko uporabnica *pinga* IPv6 naslov `2600::` (www.sprint.net), čeprav je za NAT-om in ne uporablja nobenega statično nastavljenega tunela.

Teredo pa je na Windows 7 platformi privzeto zelo omejeno uporaben – ne le, da ima pri izbiri protokola IPv4 prednost, ampak povezava sploh ni možna, kadar imamo za določeno domensko ime v DNS-u podan zgolj AAAA vnos. Povezujemo se lahko samo na eksplicitno podane IPv6-naslove:



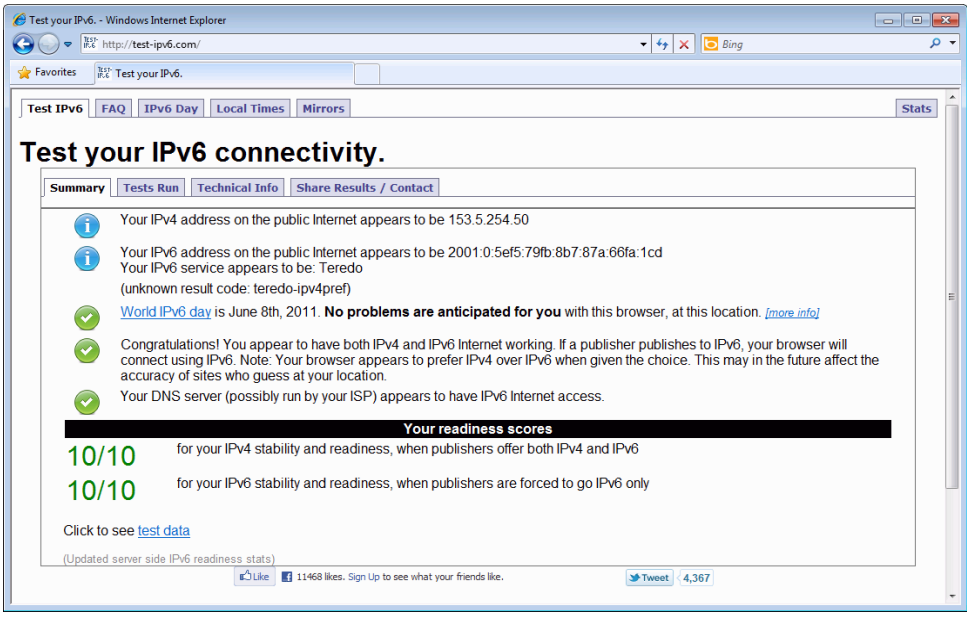


Zaradi tega dobimo na IPv6-testu slab rezultat pripravljenosti na IPv6:



Privzeto obnašanje lahko spremenimo, tako da dodamo vrednost **AddrConfigControl** = 0 (DWORD) v ključ registra `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Parameters`.

Tako dobimo zadovoljiv rezultat na testu, kljub temu pa brskalnik še zmeraj daje prednost IPv4 pred IPv6:

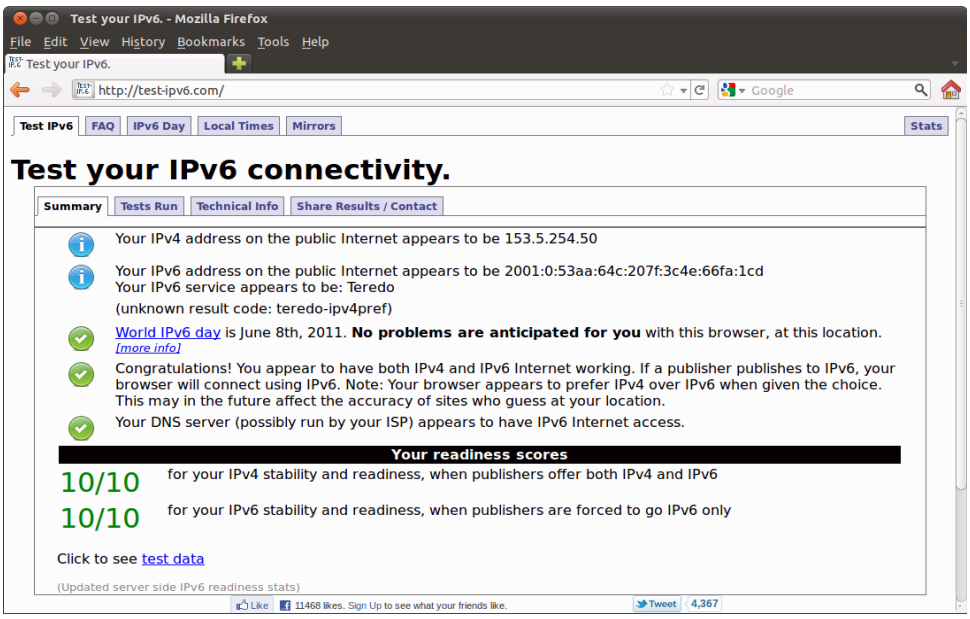


Uporabnik lahko uporablja Teredo tudi na Linux/BSD operacijskih sistemih s programskim paketom *Miredo*:

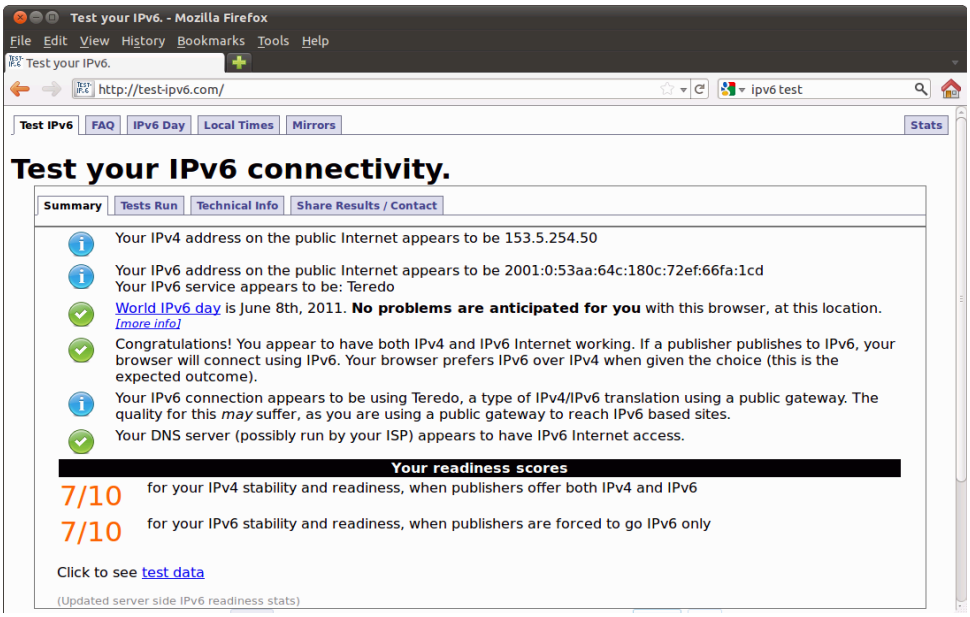
```
janja@ubuntubox: ~
File  Edit  View  Search  Terminal  Help
janja@ubuntubox:~$ sudo apt-get install miredo
[sudo] password for janja:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  miredo
0 upgraded, 1 newly installed, 0 to remove and 195 not upgraded.
Need to get 0 B/213 kB of archives.
After this operation, 504 kB of additional disk space will be used.
Selecting previously deselected package miredo.
(Reading database ... 131884 files and directories currently installed.)
Unpacking miredo (from .../miredo_1.2.3-1_i386.deb) ...
Processing triggers for ureadahead ...
Processing triggers for man-db ...
Setting up miredo (1.2.3-1) ...
 * Starting Teredo IPv6 tunneling daemon miredo                    [ OK ]
janja@ubuntubox:~$ ping6 -c 3 2600::
PING 2600::(2600::) 56 data bytes
64 bytes from 2600::: icmp_seq=1 ttl=51 time=341 ms
64 bytes from 2600::: icmp_seq=2 ttl=51 time=153 ms
64 bytes from 2600::: icmp_seq=3 ttl=51 time=153 ms

--- 2600:: ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 153.624/216.289/341.610/88.615 ms
janja@ubuntubox:~$
```

V tem primeru je po privzetih nastavitvah mogoče dostopati do strežnikov, ki imajo samo AAAA vnose, vendar je prednostni način povezave še vedno IPv4, kot kaže test:



Na Linux platformi lahko spremenimo prednostni način povezave pri 6to4 ali Teredo v datoteki `/etc/gai.conf`. Če aplikacije dajo prednost IPv6-povezavi, ko je v rabi Teredo, je rezultat:



Analiza

Cilj testiranja je bil preveriti zanesljivost in robustnost različnih tranzicijskih mehanizmov z vidika končnega uporabnika. Rezultati testiranja tranzicijskih mehanizmov, katerih namen je pospešiti prehod iz IPv4 na IPv6, so zbrani v tabeli:

Povezljivost		**Operacijski sistem**	**Izsledki**
IPv4	*IPv6*		
domorodna	domorodna	CentOS 6.0	Deluje brez kakršnih koli težav.
domorodna	brez	Windows XP	Deluje brez problemov, dostop do IPv6-strežnikov ni možen, a to trenutno ne predstavlja večjih težav, saj je večina interneta na IPv4.
domorodna	6to4	Windows XP	Deluje brez problemov - ker je prednostni način povezave IPv4, ni težav ob nedostopnosti 6to4-prehoda. Problem se lahko pojavi, če se uporabnik veliko povezuje na strežnike, ki imajo samo IPv6-povezljivost.
NAT	statični tunel 6in4	Windows 7	Deluje brez problemov, saj so aplikacije v glavnem dobro prilagojene na prisotnost NAT-prehodov. Boljša konfiguracija, kot zgolj IPv4-NAT, saj ima prednost IPv6, s čimer se izognemo NAT-prehodu ob povezavi na *dual-stack* strežnike.
NAT	6rd	Windows 7	Tako kot NAT s statičnim 6in4-tunelom, le da je olajšana nastavitev tunela.
dvojni NAT	6rd	Windows 7	Pojavljajo se problemi pri uporabi aplikacij, ki potrebujejo neposredno povezljivost, sicer deluje v glavnem nemoteno.
NAT	Teredo	Windows 7	S privzetimi nastavitvami deluje brez problemov, tudi ob morebitnem izpadu Teredo-prehoda. IPv6 je pogojno uporaben, zaradi omejitve na eksplicitno podane naslove. Če spremenimo privzete nastavitve, velja enako kot pri 6to4 – v glavnem ni problemov, ker ima IPv4 prednost. Težave lahko nastopijo ob intenzivnejši uporabi IPv6 prek Tereda. Teredo je manj primeren za postavitev strežnikov, saj lahko UDP-seja poteče in paketi ne bodo več prihajali skozi NAT-prehod, dokler se seja spet ne vzpostavi.

NAT	Teredo	Ubuntu 11.04 + Miredo	S privzetimi nastavitvami deluje brez problemov, problemi so lahko pri intenzivnejši uporabi. Če spremenimo prednostni protokol na IPv6, lahko imamo hujše težave pri dostopu do *dual-stack* strežnikov ob morebitnem izpadu ali preobremenjenosti Teredo-prehoda, zato se ta nastavitev odsvetuje.

Rezultati testiranja tranzicijskih mehanizmov, katerih namen je omogočiti IPv4-povezljivost izključno IPv6-omrežjem, so zbrani v tabeli:

Povezljivost		**Operacijski sistem**	**Izsledki**
IPv4	*IPv6*		
brez	domorodna	Windows 7	Trenutno skoraj neuporabna konfiguracija, dostop do večine spletnih strani ni mogoč, pojavljajo se hudi problemi pri uporabi drugih aplikacij.
DNS64/ NAT64	domorodna	Windows 7	Omejeno uporabna konfiguracija – dostop do spletnih strani je v glavnem mogoč, a tudi tu se lahko pojavljajo problemi. Aplikacije, ki potrebujejo zahtevnejšo internetno povezljivost, delujejo z bolj ali manj hudimi težavami ali ne delujejo.
DS-lite	domorodna	Ubuntu 11.04	V glavnem deluje brez težav, pri dostopu do IPv4 interneta se pojavljajo standardni problemi, povezani z uporabo NAT-prehodov.

Zaključek

Tranzicijski mehanizmi prinašajo lažjo pot prehoda na IPv6 kot vsesplošni *dual-stack*, zaradi zamude s prehodom na IPv6 pa so tudi neizbežni. S stališča povprečnega uporabnika interneta razlika med zanesljivostjo domorodnega dostopa do IPv6-interneta in dostopa prek tunelov ne igra velike vloge. Tunele je že zdaj relativno enostavno nastaviti, lahko pa pričakujemo da bo konfiguracija v prihodnosti še olajšana s strani proizvajalcev omrežne opreme in operacijskih sistemov.

Po drugi strani tranzicijski mehanizmi lahko prinašajo nepredvidljive težave, ki so povezane z nastavitvami MTU, požarnimi zidovi, itd. Nepazljiva uporaba tunelov lahko pripelje tudi do različnih varnostnih lukenj, ki jih je težko predvideti. Uporaba tunelov, NAT-prehodov in podobnih mehanizmov povečuje kompleksnost omrežja, to pa lahko privede do njegove zmanjšane varnosti, saj je napad možen na večih različnih točkah in na več različnih načinov. Eden izmed poglavitnih razlogov za nastanek IPv6 je namreč, da se omogoči neovirana povezava med posameznimi končnimi napravami z namenom povečanja transparentnosti omrežja in enostavnosti vzdrževanja. Zaradi teh in podobnih razlogov bi se morali tunelom izogibati, takoj ko bo to postalo možno.

Viri in literatura

Hagen S. (2006): IPv6 Essentials, Second Edition, O'Reilly Media, Sebastopol

Kunc, U. (2010): Prehod na IPv6, dosegljivo na naslovu: http://www.apek.si/datoteke/File/2010/Prehod%20na%20IPv6_2.pdf, obiskano dne 4.8.2011

Zavod go6 (2010) Študija: Prehod na IPv6 (Smernice za razmišljanje o nacionalni IPv6 strategiji), dosegljivo na naslovu: http://go6.si/docs/Studija-IPv6-MVZT.pdf, obiskano dne 4.8.2011

IETF (1998): Generic Packet Tunneling in IPv6 Specification, RFC2473, dosegljivo na naslovu: http://tools.ietf.org/html/rfc2473, obiskano dne 4.8.2011

IETF (1999): Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, RFC2529, dosegljivo na naslovu: http://tools.ietf.org/html/rfc2529, obiskano dne 4.8.2011

IETF (2001): An Anycast Prefix for 6to4 Relay Routers, RFC3068, dosegljivo na naslovu: http://tools.ietf.org/html/rfc3068, obiskano dne 4.8.2011

IETF (2001): Connection of IPv6 Domains via IPv4 Clouds, RFC3056, dosegljivo na naslovu: http://tools.ietf.org/html/rfc3056, obiskano dne 4.8.2011

IETF (2005): Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC4213, dosegljivo na naslovu: http://tools.ietf.org/html/rfc4213, obiskano dne 4.8.2011

IETF (2006): Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), RFC4380, dosegljivo na naslovu: http://tools.ietf.org/html/rfc4380, obiskano dne 4.8.2011

IETF (2007): Softwire Problem Statement, RFC4925, dosegljivo na naslovu: http://tools.ietf.org/html/rfc4925, obiskano dne 4.8.2011

IETF (2008): Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), RFC5214, dosegljivo na naslovu: http://tools.ietf.org/html/rfc5214, obiskano dne 4.8.2011

IETF (2010): IPv6 Addressing of IPv4/IPv6 Translators, RFC6052, dosegljivo na naslovu: http://tools.ietf.org/html/rfc6052, obiskano dne 4.8.2011

IETF (2010): IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification, RFC5969, dosegljivo na naslovu: http://tools.ietf.org/html/rfc5969, obiskano dne 4.8.2011

IETF (2010): IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP), RFC5572, dosegljivo na naslovu: http://tools.ietf.org/html/rfc5572, obiskano dne 4.8.2011

IETF (2010): 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-12, obiskano dne 27.7.2011

IETF (2011): DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, RFC6147, dosegljivo na naslovu: http://tools.ietf.org/html/rfc6147, obiskano dne 4.8.2011

IETF (2011): Framework for IPv4/IPv6 Translation, RFC6144, dosegljivo na naslovu: http://tools.ietf.org/html/rfc6144, obiskano dne 4.8.2011

IETF (2004): AYIYA: Anything In Anything, dosegljivo na naslovu: http://tools.ietf.org/html/draft-massar-v6ops-ayiya-02, obiskano dne: 4.8.2011

IETF (2011): Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, dosegljivo na naslovu: http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite-11, obiskano dne: 4.8.2011

Jan Žorž, Mark Townsley: 6RD and IPv6 allocation policy – prezentacija na RIPE 62 (maj 2011): dosegljivo na naslovu: http://ripe62.ripe.net/presentations/193-zorz-townsley-6rd-ripe62-may-2011.pptx, obiskano dne 20.8.2011