1, 2, 3, 4 – NA IPV6!
1, 2, 3, 4 – GO IPV6!

MATJAŽ STRAUS ISTENIČ, ARNES

POVZETEK

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. V prispevku je predstavljenih nekaj bistvenih razlik med protokoloma IPv4 in IPv6 ter ključnih točk za uspešno posodobitev omrežij in storitev: pridobitev dostopa do interneta preko IPv6; izbor in izobraževanje lastnih strokovnjakov za IPv6; pregled svojega omrežja in storitev ter raziskava vpliva uvajanja IPv6; postopno uvajanje IPv6 v omrežje in posodabljanje storitev; varnost novega omrežja in storitev na IPv6; sobivanje novega protokola z IPv4.

KLJUČNE BESEDE: IPV6, PROTOKOL IP, UVAJANJE, VARNOST IP.

ABSTRACT

The last available IPv4 address space has been allocated to regional Internet registries beginning of February 2011. New IPv4 addresses will only be available from back stock. As these are exhausted, the expansion of IPv4 networks will finally stop. We will be facing the fact that only a new protocol – IPv6 – will be possible for new network systems and services.

The paper will first examine certain fundamental differences between the IPv4 and IPv6 protocols and discuss certain key points for successful modernisation of network services: Gaining an access to IPv6 service, recruitment and training of IPv6 experts, reviewing networks and services, and research into the impact of the introduction of IPv6, gradual introduction of IPv6 to the network and modernisation of services, revision of security of IPv6 networks and services, and coexistence between the new protocol and IPv4.

KEY WORDS: IPV6, IP PROTOCOL, DEPLOYMENT, IP SECURITY.

UVOD

Internetni protokol (IP) omogoča učinkovito komunikacijo preko obsežnih omrežij, v katera je povezanih izjemo veliko število naprav – pravimo, da komuniciramo preko »interneta«. Ključno je, da IP-protokol omogoča neposredno (angl. *end-to-end*) komunikacijo. Vsaka komunikacijska naprava v ta namen uporabi svoj lasten IP-naslov, brez katerega ne more neposredno komunicirati z drugimi napravami. Število različnih IP-naslovov in s tem število neposredno dosegljivih naprav v internetu je omejeno.

V začetku februarja 2011 so po svetovnih regijah razdelili zadnje IP-naslove, ki so definirani po IP-protokolu različice 4 (IPv4). Posamezne regije (Evropa, Amerika, Latinska Amerika, Afrika, Azija in Pacifik) imajo v času priprave prispevka na zalogi dovolj IPv4-naslovov za nekaj 100.000 srednje velikih lokalnih omrežij (vir 1). Z izčrpanjem le-teh bo širitev IPv4-interneta dokončno ustavljena.

Nove naprave torej potrebujejo nove naslove, ki pa jih IPv4 več ne more zagotoviti. Uporabiti bo potrebno posodobljeno različico internetnega protokola – različico 6 (IPv6). Na IPv6 lahko poenostavljeno gledamo kot na nov način oštevilčenja interneta (vir 2). Najpomembnejša lastnost IPv6 je spremenjen zapis IP-naslova, ki omogoča dovolj različnih IPv6-naslovov za vsako praktično uporabo, ki si jo danes lahko zamislimo.

V nadaljevanju si bomo ogledali nekaj bistvenih razlik med protokoloma IPv4 in IPv6. Tako bomo lažje razumeli pomembnost posameznih korakov, ki jih bomo morali opraviti med posodabljanjem omrežja in storitev na IPv6 (vir 3). IPv6 namreč ni samo spremenjen IP-naslov v praktično neomejenem naslovnem prostoru – IPv6 je drugačen in z IPv4 nezdružljiv protokol. Za uspešno uvedbo IPv6 bodo morali naši strokovnjaki za informacijsko tehnologijo pridobiti nova znanja, temeljito pregledati obstoječa omrežja in storitve ter prepoznati in obvladovati morebitne spremembe ob prehodu na nov protokol. Spoznati bodo morali nove in spremenjene lastnosti IP-protokola ter njihov vpliv na varnost omrežja.

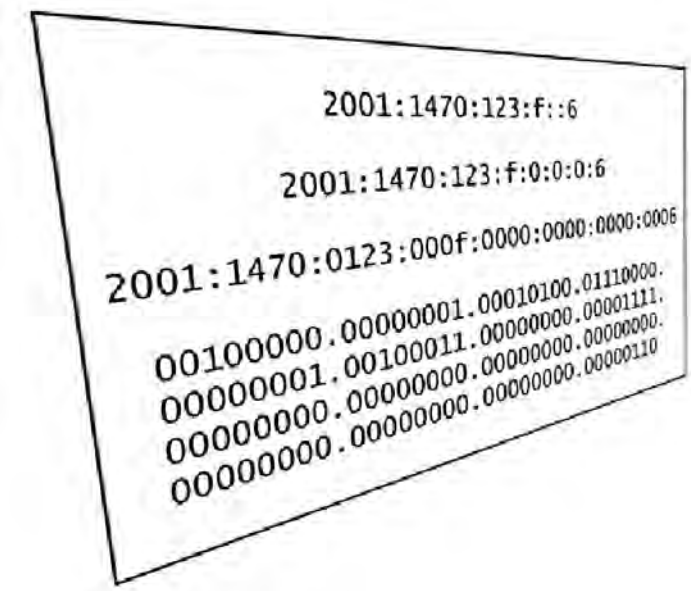
1/ IPv4-naslov je 32-bitna številka, ki jo zapišemo s štirimi decimalnimi števili med 0 in 255 ločenimi s pikami, npr. 193.2.1.66.

Ne pozabimo, da IPv4 ne bo čez noč izginil iz naših omrežij. Pripraviti se bomo morali na dolgoletno sobivanje obeh različic IP-protokola in postopno ukinitev IPv4.

O 4 IN 6
OGROMEN NASLOVNI PROSTOR

- 128-biten IPv6-naslov zapišemo s šestnajstiškimi števili, ločenimi z dvopičji, npr. 2001:1470:1:fee1::600d.
- Sisteme v lokalnem omrežju oštevilčimo s 64 biti.
- IPv6-naslovov je ogromno, dovolj za nekaj 10 milijonov lokalnih omrežij na kvadratni meter zemlje.
- Naslovni prostor IPv6 hierarhično delimo na manjše dele.

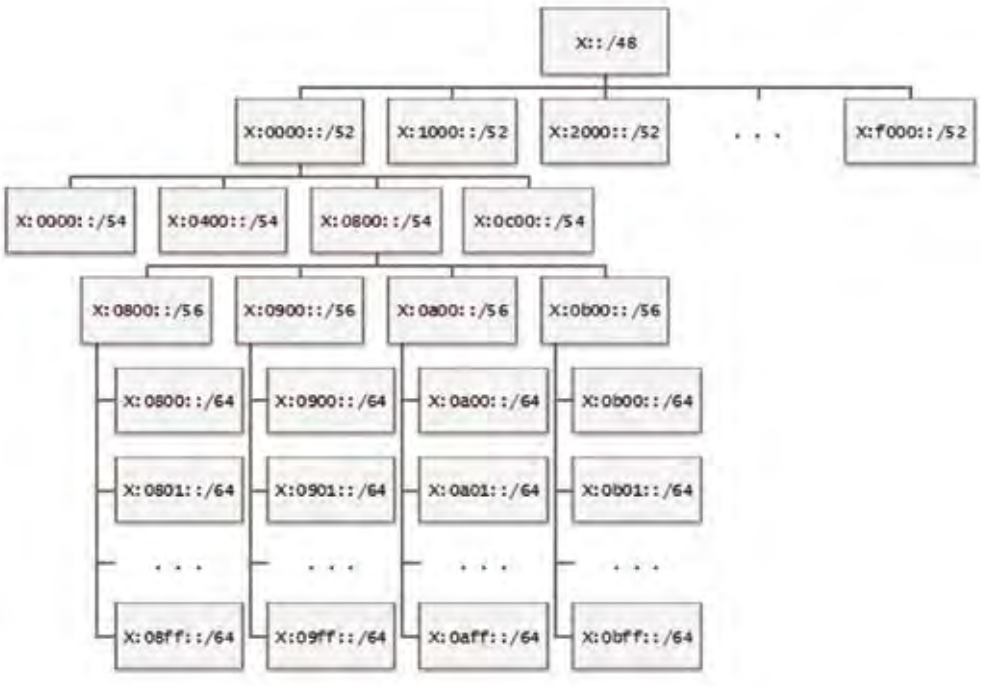
Najpomembnejša razlika med IPv4 in IPv6 je v dolžini IP-naslova, najvidnejša pa v zapisu IP-naslova. IPv6-naslov je sestavljen iz 128 bitov, združenih v osem 16-bitnih skupin[1]. Te skupine zapišemo s šestnajstiškimi števili med 0 in ffff ter jih ločimo z dvopičji. K preglednosti zapisa pripomore, če opustimo strjeno zaporedje samih ničel in ga nadomestimo z dvema dvopičjema. Prav tako lahko opustimo vodilne ničle v posameznih skupinah. Primer IPv6-naslova prikazuje Slika 1 .



Slika 1:
RAZLIČNE PREDSTAVITVE IPV6-NASLOVA.
OD ZGORAJ NAVZDOL: SKRAJŠAN – KOMPAKTEN IN PRIPOROČLJIV ZAPIS, RAZŠIRJEN ZAPIS, POLN ZAPIS BREZ OPUŠČANJA NIČEL (8 SKUPIN PO 16 BITOV), BINAREN ZAPIS (128 BITOV).

O številu vseh IPv6-naslovov pogosto govorimo v presežkih. Primerjajmo obseg 128-bitnega naslovnega prostora IPv6 z 32-bitnim naslovnim prostorom IPv4. V lokalnih omrežjih je običajno, da za številčenje posameznih IPv6-sistemov v nekem skupnem segmentu omrežja uporabimo 64 bitov. 128 bitov nam omogoča, da naslovimo sisteme v 2^{64} lokalnih omrežjih. To je ogromno število, ki si ga težko predstavljamo, zato ga raje slikovito primerjamo s številom vseh možnih IPv4-omrežij, v katerih je pribl. 250 sistemov. Teh je 2^{24}, saj od 32 bitov IPv4-naslova uporabimo 8 bitov za številčenjem posameznih sistemov. Razmerje med številoma tovrstnih IPv6- in IPv4-omrežij je ogromno, vendar bolj predstavljivo – $2^{40} \approx 10^{12} \approx 1.000.000.000.000$ (milijon milijonov). Predstavljajmo si, da bi vsa IPv4-omrežja stlačili v eno samo pšenično zrno z maso 40 mg. Za IPv6-omrežja bi potrebovali vsebnik za 40.000 ton pšenice. Ne pozabimo, da lahko v vsako od teh IPv6-omrežij »v zrnih« – zgolj teoretično, seveda – povežemo vse IP-sisteme na Zemlji, v eno od IPv4-omrežij iz naše primerjave pa le približno 250 sistemov.

Ogromen naslovni prostor nam omogoča učinkovite hierarhične načine delitve naslovov znotraj omrežij ponudnikov in uporabnikov internetnih storitev. Organizaciji z več internimi omrežji ponudnik internetnih storitev dodeli naslovni blok /48. Tak blok je dovolj velik za več kot 65.000 omrežij, zato ga v organizaciji z nekaj deset omrežji lahko brez težav razdelimo na več manjših delov enake velikosti. V IPv4-omrežjih smo bili omejeni z velikostjo posameznih delov omrežja, zato smo nekaterim namenili manj, drugim pa več IPv4-naslovov. Z IPv6 je drugače. Blok /48 razdelimo v drevesni strukturi na manjše dele, bodisi /52, /56 ali /60. Strogih pravil za tako delitev ni, priporočamo pa, da se v delitvi omejujemo na velikosti, ki so mnogokratnik števila 4. Slika 2 prikazuje primer take delitve.



Slika 2:
HIERARHIČNA DELITEV NASLOVNEGA PROSTORA /48.
PROSTOR ORGANIZACIJE JE NAJPREJ RAZDELJEN NA 16 LOKACIJ /52, POTEM PA PODROBNEJE ZA PRVO LOKACIJO, KJER SE – GLEDE NA VARNOSTNO POLITIKO – DELI V ŠTIRI DELE /54 S SKUPNO 16 PODROČJI /56. V VSAKEM OD TEH PODROČIJ JE LAHKO DO 256 PODOMREŽIJ /64.

NASLOV ZA DOLOČEN NAMEN

- Na vsakem od vmesnikov IPv6-naprave je lahko več naslovov, ki so lahko lokalni ali javni (globalni) in različnega tipa.
- IPv6-naslovi določenega tipa se uporabljajo glede na namembnost.
- Za komunikacijo v internetu uporabljamo javne naslove.
- Naslov znotraj nekega IPv6-podomrežja si naprava lahko določi sama.

Vmesnik na neki IPv6-napravi ima lahko več IPv6-naslovov[2]. Glede na način komuniciranja in namembnosti jih delimo v naslednje skupine:
eden z enim: *unicast*,
- lokalna komunikacija na skupnem segmentu: *link-local unicast*,
- lokalna komunikacija v organizaciji: *unique local unicast (ULA)*,
- globalna komunkacija na internetu (javni naslov): *global unicast*,
- komunikacija z IPv4-sistemi (v IPv6 preslikan IPv4-naslov): *IPv4-mapped*,

eden z mnogimi: *multicast*,
eden z najbližjim: *anycast*.

Naslove za komunikacijo enega sistema z mnogimi *(multicast)* poznamo že iz protokola IPv4, vendar so v IPv6 mnogo bolj sistematično definirani (vir 4, poglavja »IPv6 Addressing«, »IPv6 Multicast«). Novost v IPv6 so naslovi, ki omogočajo komunikacijo enega sistema z drugim, ki je glede na topologijo omrežja najbližje *(anycast)* in naslovi, ki so namenjeni komunikaciji na skupnem lokalnem segmentu omrežja *(link-local)*. To velja tudi za naslov privzetega prehoda do interneta (angl. *default gateway*) – tudi ta naslov je lokalnega tipa, kar je na prvi pogled nenavadno, posebno, ker v IPv4-omrežjih ni tako[3].

Za komunikacijo v IPv6-internetu uporabljamo javne naslove *(global unicast)*. Teh je za vse naprave dovolj, zato translacijski mehanizmi NAT niso potrebni[4].

V IPv6 je definiran mehanizem, ki napravam omogoča, da si same samodejno nastavijo unikaten globalni naslov. Pogosto je, da se ta naslov določi iz razširjenega naslova omrežnega vmesnika *(MAC – Media Access Control Address)* ali pa ga sistem izbere naključno.

KONTROLNA SPOROČILA ICMP

- ICMPv6 je izjemno pomemben protokol, predvsem v lokalnem omrežju.
- Previdno pri filtriranju ICMPv6-sporočil!

S sporočili ICMP kontroliramo povezljivost omrežnih naprav (npr. *ping, traceroute*), preverjamo stanje in lastnosti omrežja (npr. največjo velikost paketa, ki se lahko posreduje brez delitve – *MTU*), dosegljivost končnih sistemov ipd. Pravilno delovanje IPv4-storitev ni kritično odvisno od kontrolnih sporočil ICMP[5], kar pa nikakor ne velja za IPv6. ICMP za IPv6 (ICMPv6) je zelo pomemben – ključen protokol in veliko osnovnih mehanizmov IPv6 sloni prav na njem, npr.:
- identifikacija sosedov v omrežju,
- odkrivanje podvojenih/že uporabljenih IPv6-naslovov,
- razglašanje in iskanje usmerjevalnika,
- pridobivanje informacij za samodejno nastavitev IPv6-naslova,
- ugotavljanje največje velikosti paketa (MTU) na poti do nekega ciljnega sistema.

2/ Običajno ima vmesnik IPv6-naprave vsaj dva IPv6-naslova – lokalnega in globalnega. Nekateri operacijski sistemi že v privzeti konfiguraciji dodelijo vmesniku več globalnih naslovov.

3/ To ne pomeni, da sistem za komunikacijo preko interneta lahko uporabi lokalen naslov – ne, vedno uporabi globalnega, vendar lahko posreduje promet tudi preko lokalnega naslova privzetega prehoda.

4/ NAT ni varnostni mehanizem – za varnost skrbimo na drugačen način kot s skrivanjem za nekim javnim naslovom (filtri, požarne pregrade, zaščita na računalnikih samih).

5/ V IPv4 so zelo pomebna ICMP sporočila, ki se nanašajo na delitev paketov, npr. »destination unreachable/fragmentation needed and Don't Fragment bit set". Blokiranje takih sporočil lahko onemogoči uporabo nekaterih internetnih storitev.

Nepravilno filtriranje sporočil ICMP zato lahko povzroči nepravilno delovanje ali celo prepreči uporabo omrežnih storitev po protokolu IPv6.

6/ To je novost v NDP, na katero smo dolgo čakali. Opisuje jo RFC 6106 (IPv6 Router Advertisement Options for DNS Configuration), nov. 2010.

NA OMREŽJU ETHERNET

- Namesto ARP-a so v IPv6 vgrajeni mehanizmi ND, ki slonijo na ICMPv6.
- IPv6 omogoča samodejno določitev IP-naslova in privzetega prihoda.

Naprave si v omrežju ethernet izmenjujejo podatke v t.i. »ethernet okvirjih«. Vsak okvir je opremljen z MAC-naslovoma pošiljatelja in prejemnika. IP-sistemi morajo poznati MAC-naslov prejemnika, ki mu predajajo v ethernet okvirjen IP-paket. V IPv4 je za identifikacijo MAC-naslova, ki pripada nekemu IPv4-sistemu, skrbel poseben protokol z imenom ARP *(Address Resolution Protocol)*. V IPv6 je naloge ARP-a prevzel protokol NDP *(Neighbor Discovery Protocol)*, ki za transport podatkov uporablja ICMPv6.

NDP deluje znotraj lokalnega omrežja. Končnim sistemom omogoča, da:

- poiščejo usmerjevalnike in privzete prehode,
- izvejo IPv6-naslove podomrežij, znotraj katerih si lahko lahko sami nastavijo naslov,
- preverijo, ali je določen naslov že v u porabi *(DAD – duplicate address detection)*,
- preverijo, ali je nek drug sistem v omrežju dosegljiv,
- ugotovijo MAC-naslov nekega drugega sistema v omrežju, vključno z MAC-naslovom privzetega prehoda.

Usmerjevalniki lahko končnim sistemom s pomočjo NDP sporočijo tudi naslov imenskega strežnika DNS in privzeto ime internetne domene[6].

KAKO NA 6?

- Pridobite dostop do internetnih storitev preko IPv6. Obrnite se na svojega internega ponudnika (Arnes).
- Določite lastnega strokovnjaka za IPv6 in poskrbite za njegovo izobraževanje.
- Preglejte svoje omrežje in storitve ter raziščite vpliv uvajanja IPv6.
- Omrežje in storitve posodabljajte postopoma, začnite pri najmanj kritičnih storitvah in si pridobite izkušnje.
- Ne pozabite na varnost novega omrežja in storitev na IPv6.
- Pripravite se na sobivanje novega protokola z IPv4.

Uvajanje IPv6 je zaradi sorodnosti z IPv4 enostavnejše, kot je bilo uvajanje IP v začetkih IPv4-interneta. Otežuje ga le »kronično« pomanjkanje časa – za IPv4 smo se postopoma izobraževali vrsto let, IPv6 pa bomo morali osvojiti v letu ali dveh. Zato je toliko bolj pomembno, da se tega lotimo premišljeno. Raziskovalnim in izobraževalnim organizacijam bo pri tem v veliki meri pomagal Arnes.

KJE POMAGA ARNES?

- Registracija in delitev IPv6-naslovnega prostora.
- Svetovanje pri izboru dostopovne opreme.
- Vzpostavitev povezave z IPv6-omrežjem ARNES in nastavitve dostopovne opreme.
- Svetovanje pri posodabljanju storitev.
- Izobraževanje za IPv6.

Prehod na IPv6 se začne pri ponudniku internetnih storitev. Arnes omogoča omrežne storitve po protokolu IPv6 na vseh povezavah, kjer ima organizacija/članica ustrezno dostopovno opremo (usmerjevalnik IP-prometa) in povezavo do Arnesovega hrbteničnega omrežja. Največja ovira je prav zastarela in neprimerna dostopovna oprema, ki ne omogoča IPv6, drug problem pa so dostopovne povezave preko omrežij ponudnikov, ki na IPv6 še niso pripravljeni.

Začeli bomo s pridobitvijo IPv6-naslovnega prostora (vir 7) in razporeditvijo le-tega po lokalnih omrežjih. Arnes predlaga primerno dostopovno opremo, jo nastavi in omogoči povezavo s hrbteničnim omrežjem. Arnesovi strokovnjaki svetujejo tudi pri posodabljanju osnovnih omrežnih storitev.

KAJ NAREDI ORGANIZACIJA/ČLANICA SAMA?

Prvo in najbolj pomembno je, da organizacija izbere in čimprej izobrazi lastnega strokovnjaka, ki bo vodil prehod na IPv6. Začel bo s pregledom omrežja in omrežnih storitev in ugotovil, kaj vse je potrebno posobiti in kje lahko nastopijo potencialni problemi pri posodobitvi na IPv6. Na podlagi tega lahko v organizaciji ocenijo stroške prehoda in planirajo prehod na IPv6. Izbrati bo potrebno ustrezne dobavitelje opreme, serviserje in svetovalce oziroma preveriti, ali so obstoječi že primerno usposobljeni za IPv6.

Zavedati se moramo, da en sam strokovnjak za IPv6 v organizaciji ne bo dovolj. Izobraževanje za IPv6 bo v primernem obsegu zajelo vse osebje za informacijsko tehnologijo. Žal to ne bo poceni (vir 8).

ZA KONEC ŠE NEKAJ NASVETOV:

- Ne vklapljajte IPv6 v omrežjih, ki nimajo zanesljive IPv6-povezave. Le-ta naj bo po kvaliteti in zmogljivostih primerljiva z IPv4-povezavo.
- Povsod uporabljajte globalni (javni) IPv6-naslovni prostor.
- Naslovni prostor razdelite hierarhično.
- V lokalnih omrežjih uporabljajte naslovne bloke /64, kar omogoča nemoteno samodejno konfiguracijo sistemov (angl. *Stateless Autoconfiguration*).
- Kontrolni protokol (ICMPv6) je zelo pomemben za delovanje IPv6-omrežja in storitev! Nepravilno filtriranje prometa ICMPv6 je pogost vzrok za napake v delovanju.
- Bodite previdni pri izbiri omrežne opreme. Izberite le tako opremo, kjer se IPv4 in IPv6 promet obravnavata enako ali vsaj primerljivo (vir 5).
- Skrbite za varnost omrežja! Pri IPv4 ste bili morda navajeni skrivanja za mehanizmi NAT, sedaj pa boste na lepem uporabljali globalno dosegljive javne IPv6-naslove. Izberite primerno požarno pregrado in poskrbite za varnost omrežja neposredno na računalnikih samih.

Prepoznajte in odpravite napravilnosti, vendar ne tako, da bi na svojem računalniku preprosto izklopili IPv6 in s tem »rešili problem«.

- Poskrbite za pravočasno prenovo internetnih storitev, ki jih nudite. Novi uporabniki interneta morda ne bodo imeli več IPv4-naslovov – naj bo vaša storitev dosegljiva tudi njim.

Sodelujte in izmenjujte mnenja in izkušnje! Slovenska inicijativa za IPv6 je močna (vir 6), na Arnesu je splošen »debatni krožek« razprava@ipv6.si, IPv6 lahko preizkusite

v laboratorijih Arnesa, zavoda Go6, LTFE Univerze v Ljubljani in projekta *6deploy*, organiziramo IPv6-srečanja z delavnicami (peto bo predvidoma maja 2011) itd. Vzpodbujajte sodelavce, ki pokažejo zanimanje in zagnanost za uvajanje IPv6 v vašem okolju: izobrazite jih, dajte jim možnost dela na področju IPv6, nagradite jih – obrestovalo se vam bo!

ZAKLJUČEK

IPv6 je sprememba na bolje, korak naprej. Kot vsaka sprememba pa zahteva, da se nanjo pripravimo in se prilagodimo novemu. Zato je izobraževanje ključnega pomena za uspešno uvedbo IPv6 v naša omrežja. Pri tem vam lahko pomagajo tudi Arnesovi strokovnjaki, ki so dosegljivi na ipv6-podpora@arnes.si.

Prvi kratkoročni cilj, ki si ga lahko z Arnesom zastavimo, je, da bo spletna stran vaše organizacije dostopna po IPv6 na svetovni IPv6-dan 8.6.2011 (vir 9). Se »vidimo« na IPv6!

VIRI

(vse naštete spletne strani so bile obiskane februarja 2011)

http://en.wikipedia.org/wiki/Regional_Internet_registry, http://www.iana.org/numbers/, http://www.potaroo.net/tools/ipv4/, http://ipv6.he.net/statistics/

http://www.arnes.si/storitve/omrezne-storitve/ip-povezljivost/ipv6.html

http://www.ipv6actnow.org/info/how-to/

http://www.6deploy.eu/index.php?page=tutorials, http://en.wikipedia.org/wiki/IPv6_address

http://www.ripe.net/ripe/docs/ripe-501

http://go6.si/

http://www.arnes.si/storitve/dostop/registracija-ip.html

http://www.erion.co.uk/IPv6Training/

http://dan.ipv6.si/