Vlada Republike Slovenije, Ministrstvo za visoko šolstvo, znanost in tehnologijo

Študija: Prehod na IPv6

(Smernice za razmišljanje o nacionalni IPv6 strategiji)

Avtorji: Urban Kunc, Ivan Pepelnjak, Janez Sterle, Matjaž Straus Istenič, Andrej Kobal, Simeon Lisec, Olaf Maennel, Jan Žorž

Ljubljana, 10.11.2010

KUNC, Urban; PEPELNJAK, Ivan; STERLE, Janez; STRAUS Istenič, Matjaž; KOBAL, Andrej; LISEC, Simeon; MAENNEL, Olaf; ŽORŽ, Jan

Študija: Prehod na IPv6 (Smernice za razmišljanje o nacionalni IPv6 strategiji) – Ljubljana : Ministrstvo za visoko šolstvo, znanost in tehnologijo, 2010

Urednik: Jan Žorž
Oblikovanje: Jan Žorž

Kazalo

Predgovor [1](Foreword)

Patrik Fältström[2]*:*

The next generation IP protocol was something that engineers in the world started working on in the early 1990's, almost 20 years ago. But not until now we see the need, the urgency and actual deployment of what we call IPv6. It was of course not called IPv6 from the beginning, but for more than ten years, people have talked about how important IPv6 is for the Internet. And of course not only for the Internet but for everyone that uses the Internet.

A careful reader and people that have followed this process might ask the reasonable question why IPv6 is so important now, when obviously the world has not collapsed earlier. The answer is of course that we see two things happening, or rather, one thing is happening and one is not.

Let us start with what is happening. People are designing more and more services that are client-server only. Not peer-to-peer as in the way Internet was designed. Any device connected to the Internet should be able to connect to any other device. Something discovered again around 2008 in the discussions around Internet of Things. This isn't new. That is how Internet has always worked.

If those end-to-end connections do not exist, you can implement proxies, address translation devices etc. But that also implies users cannot, when they travel, access their pictures and smoke detectors, front door and fridge at home. It would be impossible to create a new service in your garage, as no one can access the service. This is of course a bad scenario, as innovation is built upon the idea that any one that come up with something themselves should be able to choose who their potential customers are. Not a third party that has to open up or configure a proxy so that the customer and provider can reach each other. The proxy implies control, and any control mechanism has impact on innovation and market economy.

What is not happening, is the deployment of IPv6. We see some deployment here and there, but not much. The problem with the lack of deployment is that there is no direct business model for IPv6. Not enough parties can charge extra for IPv6. For them it is important that their favourite service works, and it does as long as we have IPv4 addresses. There is a slim chance (if any) for (for example) a service provider to charge more for including IPv6 in the Internet access they sell. Instead, the upgrade to include

1 Zaradi ohranitve avtentičnosti je predgovor nespremenjen in v angleškem jeziku.

2 *Patrik Fältström is employed by Cisco, co-chair of the cooperation working group at RIPE and adviser to the Swedish IT Minister.*

IPv6 should have happened as part of the normal upgrade cycle of the hardware and software that was made the last 10 years. Just like we changed from diagonal to radial tires without having to change the cars.

Now, when we really need IPv6 for innovation, internet of things and many other things that guarantee (from technology perspective) the openness of and end-to-end principle, it unfortunately might be a deployment that happens by itself, because that is an extra cost. But the cost can be minimised if coordination is happening, and specifically public services have a responsibility as a user of Internet to coordinate and update their procurement processes.

The reason for that is that as the update of the networks in the world do imply an investment, and because governments and public services want to see IPv6 deployed due to innovation and market economy reasons, the public sector can and possibly should help with at least partially fund that deployment.

The best way of doing that is not to regulate and force deployment, but instead by ensuring public e-services are available over both IPv4 and IPv6, and to ensure that public services are prepared in paying their upstream Internet Service Provider for getting it. I.e. the best thing public sector can do is to work together. Not only among public sector, but in a multi stakeholder fashion. Include providers of services in the building of the plan for IPv6 deployment, and then include IPv6 and IPv4 as necessary components in the communication network to be used for the next couple of years.

This document is expanding on these needs that I just briefly have touched upon. There are unfortunately not many that have written texts about these problems. The lack of cooperation, the economical impact on non-deployment of IPv6, and I think the work in Slovenia is perfect. More countries should have done what Slovenia has done. But although this document is covering large grounds, there are more things to do. And I am looking forward to further studies in Slovenia and elsewhere that explain why the end-to-end model is so important, why IPv6 is a key ingredient in a working Internet model, and specifically what the roles the various parties (private as well as public sector and civil society) have regarding deployment of an Internet that helps the country to grow and become more competitive and efficient.

A big thanks to Jan Žorž and other friends in Slovenia for this work, and I am looking forward to the continuation of the studies. Or as Winston Churchill said: »Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.«

Povzetek

Internet danes predstavlja eno najpomembnejših infrastruktur sodobne družbe. Marsikateri organizaciji, podjetju ali posamezniku ne omogoča le dela ali izobraževanja, temveč tudi preživetje. Današnji internet temelji na protokolu IPv4. Ta omogoča naslavljanje omrežnih naprav in usmerjanje paketov skozi omrežje do cilja. Smo pred skorajšnjim izčrpanjem naslovnega prostora IPv4. Krovni mednarodni organizaciji IANA, ki razdeljuje naslove IP, jih bo po sedanjem trendu povpraševanja zmanjkalo ob koncu letošnjega leta ali v začetku leta 2011. V regiji EU, za katero skrbi RIPE NCC, bo naslovov IPv4 zmanjkalo nekje v prvi polovici leta 2012. Slovenija po nekaterih ocenah danes razpolaga s približno 1.700.000 naslovi IPv4. Na prvi pogled se zdi številka impresivna in da imamo naslovov IPv4 dovolj, če pogledamo trend današnjih naprav, ki gre v smeri mobilnosti, pametnih naprav in pametnega transporta, pa kaj hitro ugotovimo, da naslovov IPv4 še zdaleč ni dovolj za prihodnjo rast in razvoj.

Protokol IPv4 ima že deset let svojega naslednika, to je protokol IPv6. IPv6 je v mnogih ozirih naprednejši od IPv4, vendar njegovo največjo prednost predstavlja ogromen naslovni prostor. IPv6 je temeljni komunikacijski protokol, ki že zdaj in bo tudi v prihodnje omogočal naslavljanje pametnih omrežnih naprav in stvari interneta prihodnosti. Brez njegove uvedbe se bosta razvoj in gospodarska rast upočasnila, v skrajnem primeru pa tudi ustavila.

Uvedbo protokola IPv6 pestijo številne težave. Še največjo predstavlja nezdružljivost protokola IPv6 s protokolom IPv4. To pomeni, da se omrežne naprave s protokolom IPv4 ne morejo sporazumevati z napravami IPv6, če protokol IPv6 ni del obstoječega protokolnega sklada. Obstaja tudi možnost uporabe translacijskih in tunelskih mehanizmov, s katerimi lahko premostimo razlike, vendar so to le rešitve prehodnega značaja, ki dodatno povečujejo stroške in odpirajo mnoge varnostne probleme.

IPv6 je del protokolnega sklada v skoraj vseh sodobnih operacijskih sistemih, od osebnih računalnikov do usmerjevalnikov, požarnih pregrad in sistemov IDS/IPS. Seznam naprav, združljivih z IPv6, se z vsakim dnem podaljšuje. Zaviralni dejavnik pri uvajanju IPv6 so nezavedanje problema in posledic izčrpanja naslovnega prostora IPv4, nepoznavanje njegovega delovanja, dodatni operativni stroški načrtovanja, implementacije in vzdrževanja opreme IPv6 ter stroški za izobraževanje osebja. V manjši meri, ob upoštevanju ciklične menjave opreme, predstavlja stroške tudi nakup nove ali nadgradnja obstoječe opreme.

Analiza, ki je bila opravljena v okviru študije, je pokazala, da se vlade različnih držav različno odzivajo na skorajšnje izčrpanje naslovnega prostora IPv4. Gospodarsko naprednejše in izvozno naravnane države so si postavile jasne cilje z vnaprej določenimi in merljivimi roki uvedbe protokola IPv6 v javna, državna in zasebna komunikacijska omrežja. Nekatere vlade držav navkljub upadanju gospodarske rasti niso zmanjšale, temveč so celo povečale proračun za investicije v infrastrukturo IKT, ki bo temeljila na IPv6. Celo Češka, ki je še nedavno tega predstavljala manj napredno državo bivšega socialističnega tabora, si je postavila jasne cilje za uvedbo IPv6. Z resolucijo, sprejeto junija 2009, si je češka vlada postavila za cilj, da bo postopno z menjavo opreme IPv6

uvedla v omrežje javne administracije, do 31. decembra 2010 pa omogočila dostop do svojih spletnih vsebin tudi prek protokola IPv6. V evropskem prostoru je poleg Švedske in Portugalske ena od vodilnih držav pri uvedbi varnostne razširitve sistema DNS (DNSSEC), s katerim omogoča zaščito svojih domenskih imen. DNSSEC oziroma njegove alternative je poleg IPv6 eden ključnih protokolov in elementov interneta prihodnosti.

Slovenija se v skupini sedemindvajseterice držav EU uvršča v povprečje v tehnološki razvitosti elektronskih komunikacij. Po raziskavi, ki jo je opravil nacionalni regulator elektronskih komunikacij APEK februarja 2010, nekateri slovenski operaterji pospešeno uvajajo IPv6 v svoja hrbtenična, postopno pa tudi v dostopovna omrežja. Nekateri od njih poslovnim uporabnikom že ponujajo povezljivost IPv6 in osnovne storitve IPv6 (DNS). Pri tem je slovensko raziskovalno-izobraževalno omrežje Arnes izjema, saj IPv6 že vrsto let uporablja v hrbteničnem omrežju. Povezljivost IPv6 imajo tudi ljubljanska in mariborska univerza, Institut Jožef Stefan, nekatere srednje in osnovne šole, dijaški in študentski domovi ter knjižnice.

Slovenska vlada za razliko od nam primerljivih držav vsaj za zdaj pri uvedbi IPv6 ni naredila pomembnega koraka, ki bi spodbudil vse relevantne deležnike k uvedbi IPv6. To so operaterji, ponudniki storitev in vsebin, sistemski integratorji, proizvajalci omrežne opreme, izobraževalne institucije ter javne in zasebne organizacije. Ni sprejela nobenega akcijskega načrta ali strategije, s katerim bi se zavezala, da bo v določenem roku IPv6 uvedla v omrežje javne administracije, ministrstev ali agencij. Ni se zavezala, da bo v določenem roku omogočila svojim državljanom dostop do storitev in spletnih strani prek IPv6, ali da bi na tak ali drugačen način spodbujala uvedbo IPv6.

Prehod na IPv6 se ne more zgoditi čez noč. Tudi če uvedbo začnemo danes, bo trajalo leta, da bomo lahko konkurenčni državam, ki že več let pred nami pospešeno uvajajo IPv6. Uspešnost prehoda na IPv6 je pogojena s sodelovanjem vseh deležnikov. IPv6 morajo uvesti operaterji v svoja obstoječa in vsa nova omrežja. Ponudniki vsebin in storitev morajo razviti storitve in vsebine, ki bi izkoriščale prednosti IPv6, oziroma morajo za začetek vsaj omogočiti dostop do obstoječih storitev in vsebin IPv6. Sistemski integratorji morajo biti v pomoč javnim in zasebnim organizacijam pri uvajanju IPv6. Javne in zasebne Izobraževalne inštitucije morajo IPv6 uvesti v svoje programe izobraževanja.

V okviru te študije je bil ob sodelovanju slovenskega Zavoda go6 pripravljen nabor funkcionalnosti, ki jih mora izpolnjevati z IPv6 združljiva oprema. Nabor funkcionalnosti je bil posredovan evropski internetni skupnosti v okviru evropskega regionalnega registrarja RIPE NCC. Dokument je ob manjših popravkih dosegel konsenz, ki se bo še potrdil na prihajajočem srečanju RIPE sredi novembra 2010 v Rimu. Sprejeti dokument ima možnosti, da postane priporočilo Evropske komisije članicam Evropske unije pri uvedbi protokola IPv6.

Študija je bila izdelana kot odgovor na 11 vprašanj, na katere potrebujemo odgovore, da bi se država lahko primerno pripravila na prehod na IPv6 in se pravilno odzvala na širše izzive, ki so še pred nami – pa naj to zajema državno in javno upravo ali vpliv prehoda na državljane, industrijo in vse druge deležnike naše družbe.

Upamo, da bo ta dokument dal dovolj odgovorov za razmišljanja o nacionalni strategiji uvedbe IPv6, ki jo zares potrebujemo, čeprav se tega nekateri še ne zavedajo.

Analiza obstoječega stanja uvedbe IPv6 v Sloveniji

Tabela uvajanj IPv6 v podjetja in omrežja na dan 2.11.2010

Stanje uvedbe IPv6 v nekaterih slovenskih podjetjih in ustanovah se spremlja na go6.si portalu pod sekcijo “Stanje IPv6 v Sloveniji”:

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

Tabela je urejena po abecedi glede na ime podjetja oziroma organizacije.

Stanje alokacij IPv6 v Sloveniji 2. 11. 2010

LG	Prefix	tld	NetName	Owner	AS	S	Allocated	First seen	Seen by	Last seen (*)
LG	2001:67c:58::/48		SI-NIL-NET6	NIL Podatkovne komunikaci...	24629	A	2009-09-07	2009-09-09 11:32:31	99%	2010-11-10 13:17:46
LG	2001:67c:124::/48		SI-LinIT	LinIT , Informacijske Teh...		A	2010-01-25	2010-01-27 08:47:35	96%	2010-11-10 13:17:46
LG	2001:67c:1a0::/48		PROPLUS-SI	PRO PLUS, d.o.o.		A	2010-03-11		0%	never
LG	2001:67c:1fc::/48		SI-SMART-COM	Smart Com d.o.o.		A	2010-05-14		0%	never
LG	2001:67c:2f0::/48		HERMES-SOFTLAB	Hermes Softlab Programska...		A	2010-09-22		0%	never
LG	2001:67c:300::/48		DELO-SI6	DELO, d. d.	39387	A	2010-09-30		0%	never
LG	2001:7f8:46::/48		ARNES-SIX-IPv6-NET-2...	Slovenian Internet Exchan...	2107	A	2008-10-03	2008-10-23 08:47:34	88%	2010-11-10 13:17:47
LG	2001:1470::/32		SI-ARNES-20030618	ARNES (Academic and Resea...	2107	A	2003-06-18	2003-07-22 08:21:58	100%	2010-11-10 13:17:47
LG	2001:15c0::/32		SI-MEDINET-20031002	Amis d.o.o.	8591	A	2003-10-02	2003-10-05 16:41:08	100%	2010-11-10 13:17:47
LG	2001:1688::/32		SI-BONE-20031216	Triera Internet	3212	A	2003-12-16	2004-06-27 19:20:37	100%	2010-11-10 13:17:47
LG	2a00:ee0::/32		SI_TELEKOM-20081120	Telekom Slovenije d.d.	5603	A	2008-11-20	2010-02-09 14:02:36	100%	2010-11-10 13:17:47
LG	2a00:fc0::/32		SI-VOLJA-20081210	voljatel	16016	A	2008-12-10	2009-02-10 13:32:38	100%	2010-11-10 13:17:47
LG	2a00:1368::/32		SI-LT-FE-20090915	University of Ljubljana,...	28933	A	2009-09-15	2010-05-06 14:32:41	100%	2010-11-10 13:17:47
LG	2a00:13d8::/32		SI-MMTC-20090922	Telemach d.o.o.		A	2009-09-22		0%	never
LG	2a00:1420::/32		SI-MOBIK-20090924	Mobik IPv6 network	44993	A	2009-09-24	2009-10-06 09:32:33	100%	2010-11-10 13:17:47
LG	2a00:1438::/32		SI-TSMART-20091002	TELESMART podatkovne komu...	49630	A	2009-10-02	2009-11-23 23:32:35	100%	2010-11-10 13:17:47
LG	2a00:1448::/32		SI-ELEKTROTURNSEK-20...	Elektro Turnsek d.o.o.	42613	A	2009-10-05	2009-11-23 23:32:35	100%	2010-11-10 13:17:47
LG	2a00:1600::/32		SI-UNI-MB-20091106	Univerza v Mariboru	50195	A	2009-11-06	2009-12-31 00:02:36	100%	2010-11-10 13:17:47
LG	2a00:1a20::/32		SI-MOBIL-20100125	SI.MOBIL d.d.		A	2010-01-25		0%	never
LG	2a00:1c80::/32		SI-ARIO-20100304	ARIO, d.o.o.		A	2010-03-04		0%	never
LG	2a00:1da8::/32		SI-NAKOM-20100317	Nakom d.o.o.	49725	A	2010-03-17	2010-03-18 09:02:39	100%	2010-11-10 13:17:47
LG	2a01:260::/32		SI-T-2-20061201	T-2 d.o.o.	34779	A	2006-12-01	2010-06-23 07:47:44	100%	2010-11-10 13:17:47
LG	2a02:e8::/32		SI-DOMENCA-20080229	Domenca d.o.o.	43128	A	2008-02-29	2008-11-12 08:47:36	100%	2010-11-10 13:17:47
LG	2a02:7a8::/32		SI-RTVSLO-20080911	RTV Slovenija	47917	A	2008-09-11	2009-02-12 09:32:28	100%	2010-11-10 13:17:47
LG	2a02:800::/32		SI-SOFTNET-20081217	Softnet d.o.o.	9119	A	2008-12-17	2009-11-24 14:32:35	97%	2010-11-10 13:17:47
LG	2a02:840::/32		SI-TUSMOBIL-20090105	TUSMOBIL D.O.O.	41828	A	2009-01-05	2009-09-25 11:32:33	100%	2010-11-10 13:17:48
LG	2a02:d68::/32		SI-SGN-20090420	SGN d.o.o.	35471	A	2009-04-20	2009-04-25 22:02:29	100%	2010-11-10 13:17:48
LG	2a02:d80::/32		SI-NETSI-20090421	Metaling d.o.o.	12778	A	2009-04-21	2009-04-25 22:02:29	100%	2010-11-10 13:17:48
LG	2a02:d90::/32		SI-STELKOM-20090422	Stelkom d.o.o.		A	2009-04-22		0%	never
LG	2a02:e20::/32		SI-MOBITEL-20090507	Mobitel d.d.	29276	A	2009-05-07	2009-12-04 14:32:35	100%	2010-11-10 13:17:48
LG	2a02:2230::/32		SI-AKTON-20100804	Akton d.o.o. Network		A	2010-08-04		0%	never
LG	2a02:23d0::/32		SI-K2-20100909	VELCOM d.o.o.	5435	A	2010-09-09	2010-09-10 09:02:45	100%	2010-11-10 13:17:48
LG	2a02:2590::/32		SI-KATENG-20101007	Zavod Kabelska televizija...	51615	A	2010-10-07	2010-10-18 09:02:46	97%	2010-11-10 13:17:48
LG	2a02:28b0::/32		SI-SIEL-20101108	SIEL, INFORMACIJSKE RESIT...		A	2010-11-08		0%	never

Trenutno imamo v Sloveniji 34 alokacij naslovnega prostora IPv6, od katerih je 24 pravilno oglaševanih v globalni IPv6 internet (74,59 %)

Alokacije so razvrščene abecedno po naslovnem prostoru.

Stanje uvedbe in dosegljivost slovenskih spletnih mest preko IPv6

Eric Vyncke skrbi za portal, ki preverja dosegljivost različnih servisov prek IPv6, kot je spletni strežnik, poštni strežnik ter strežniki DNS za domene iz različnih držav sveta, med drugimi tudi Slovenije. Sezname domen pridobi iz iskalnika Alexa, vzame pa najpopularnejše domene.

Del stanja je prikazan na spodnji sliki, celotno tabelo si pa lahko ogledate na naslovu: http://www.vyncke.org/ipv6status/detailed.php?country=si

Name	Alexa	Web	Mail	DNS
Search Google whois	1/1569	FAILED	FAILED	FAILED
najdi.si *More* whois	2/7516	FAILED	FAILED	FAILED
rtvslo.si whois	3/10258	ipv6.rtvslo.si 2a02:7a8::1:0:0:80:1 2010-09-15	FAILED	ns2.rtvslo.si ns1.rtvslo.si 2a02:7a8::1:0:0:53:1 2/4 2010-11-11
gov.si whois	4/13363	FAILED	FAILED	FAILED
partis.si whois	5/16501	FAILED	FAILED	FAILED
finance.si whois	6/18789	FAILED	FAILED	FAILED
bigbrother.si whois	7/19446	FAILED	FAILED	FAILED
zurnal24.si whois	8/20145	FAILED	FAILED	FAILED
uni-lj.si whois	9/24164	FAILED	FAILED	FAILED
zadovoljna.si whois	10/25589	FAILED	FAILED	FAILED
dnevnik.si whois	11/26794	FAILED	FAILED	FAILED
delo.si whois	12/32573	FAILED	FAILED	FAILED
bizi.si whois	13/41527	FAILED	FAILED	FAILED
cekin.si whois	14/43290	FAILED	FAILED	FAILED
nlb.si whois	15/50546	FAILED	FAILED	FAILED
shrani.si *More* whois	16/51677	FAILED	FAILED	ns6.interseek.si ns4.interseek.si 2001:15c0:1000:1004::1:53 2/4 2010-11-11
uni-mb.si whois	17/52882	FAILED	FAILED	niobe.ijs.si dorf21.uni-mb.si 2a00:1600::10:0:0:0:99 1/5 2010-11-11

(del tabele izrezan zaradi preglednosti)

www.si whois	76/822052	FAILED	FAILED	FAILED
poptv.si whois	77/846533	FAILED	FAILED	FAILED
interseek.si whois	78/991618	FAILED	FAILED	ns6.interseek.si ns4.interseek.si 2001:15c0:1000:1004::1:53 2/4 2010-11-11
nikonsvet.si whois	79/999625	FAILED	FAILED	FAILED
akton.si whois	/	FAILED	FAILED	FAILED
arnes.eu whois	/	FAILED	FAILED	ns4.arnes.eu ns8.arnes.si ns9.arnes.si 2001:500:14:6054:ad::1 3/5 2010-11-11
go6.si whois	/	www.go6.si 2a02:e8::1:0:0:babe:face 2010-09-10	mail.go6.si 2a02:e8::1:0:0:babe:face 2010-09-16	ns6.pragma.si ns1.pragma.si ns6.go6.si 2a02:e8::1:0:0:babe:face 3/4 2010-11-11
ledina.si whois	/	www.ledina.si 2001:1470:fbfe::62 2010-11-03	tito.ledina.org 2001:1470:fbfe::62 2010-11-03	ns1.ledina.si ns2.ledina.si 2001:1470:fbfe::2:53 2/2 2010-11-10
NIL *More* whois	/	FAILED	FAILED	FAILED
pragma.si whois	/	www.pragma.si 2001:470:d422::3 2010-09-02	FAILED	carnium.pragma.si ns1.ipv6.editdns.net ns1.pragma.si 2001:470:d422::3 3/4 2010-11-11
shelastyle.net whois	/	FAILED	FAILED	FAILED
softnet.si whois	/	FAILED	jessie.softnet.si 2a02:800::3:0:0:0:2 2010-07-30	FAILED
stargate.si whois	/	FAILED	FAILED	asgard.stargate.si furling.stargate.si replicator.stargate.si prior.stargate.si 2a02:840:1:4:1008::1 4/4 2010-11-11
In total 88 hosts		5 (6%)	3 (3%)	20 (23%)

Apek: Raziskava uvedbe in pripravljenosti na IPv6 v Sloveniji

Agencija za pošto in elektronske komunikacije Republike Slovenije (APEK) je v februarju 2010 izvedla obširno raziskavo o stanju uvedbe IPv6 pri slovenskih operaterjih in ponudnikih telekomunikacijskih storitev.

Analiza je pokazala naslednje rezultate uvajanja: na vprašalnik se je odzvalo 41 operaterjev, pri čemer ima pet operaterjev več kot 90 % vseh naročnikov. Med njimi je veliko kabelskih operaterjev. Redki kabelski operaterji imajo v celoti lastno optično-koaksialno infrastrukturo in obenem še razpolagajo z lastnimi storitvami (IP).

Iz prejetih odgovorov je bilo ugotovljeno, da anketirani v povprečju dobro poznavajo problematiko IPv6. Dobrih 80 % anketiranih je navedlo, da je vodstvo seznanjeno s potrebo po vpeljavi IPv6, vendar le 70,7 % vodstva podpira njegovo vpeljavo v smislu rezervacije finančnih sredstev, šolanja kadra, nakupa oziroma posodobitve opreme in licenc.

Deset operaterjev uporablja na hrbteničnem omrežju IPv6 v dvojnem skladu z IPv4, eden ima IPv6 prek IP tunela in eden prek IPv4 MPLS (6PE RFC4798; v4 signalizacija). Tehnologije IPv6 prek IPv6 MPLS (IPv6 usmerjanje in signalizacija) doslej ne uporablja še noben operater.

IPv6 je v produkciji na dostopovnem omrežju pri skoraj 20 % operaterjev. Predvidevamo, da gre večinoma za operaterje, ki imajo v dostopovnem omrežju optična vlakna, saj s tehnološkega vidika njihova oprema deluje na sloju podatkovne povezave, ki je neodvisna od zgoraj ležečega protokola IP. Kot izkazujejo rezultati, bo večina operaterjev prehod na dostopovnem delu omrežja izvedla šele v letu 2011 ali pozneje.

Devet operaterjev že omogoča priklop poslovnih uporabnikov na IPv6. Pet operaterjev omogoča domorodno storitev IPv6, štirje omogočajo IPv6 prek tunela, pet jih omogoča večdomnost (multi-homing). Pri petih operaterjih le 10 % poslovnih uporabnikov IPv6 dejansko tudi že uporablja. To nakazuje, da je povpraševanje po povezljivosti IPv6 še zelo majhno. Iz analize je razvidno, da bo večina ostalih operaterjev poslovnim uporabnikov IPv6 omogočila šele v prvem četrtletju leta 2011. Enajst operaterjev ne razmišlja o priklopu poslovnih uporabnikov.

Rezidenčne uporabnike na tehnologijah DSL ali FTTH naj bi operaterji začeli priklapljati v drugi četrtini leta 2011.

Več o analizi uvajanja IPv6 v Sloveniji na spletnih straneh agencije www.apek.si.

Viri:
Zavod go6 (2010): Tabela uvajanja IPv6, dosegljivo na: http://go6.si/stanje-ipv6-v-slo-devel/, obiskano dne 2.11.2010

SixXS (2010): Tabela alokacij IPv6, dosegljivo na: https://www.sixxs.net/tools/grh/dfp/all/?country=si, obiskano dne: 2.11.2010

Apek (2010): Uvajanje IPv6 v Sloveniji – raziskava, http://www.apek.si/datoteke/File/2010/sporocila-za-javnost/Uvajanje%20IPv6_v%20Sloveniji_april_2010.pdf

Urban Kunc, IPv6 v Sloveniji in Evropi, VITEL zbornik
Seznam spletnih strežnikov IPv6 po posameznih državah, http://sixy.ch/

1. Opis najpomembnejših problemov ter posledice, če se Slovenija ne loti ustreznega reševanja

Olaf Maennel[3]:

The problem is too simple to be a problem?!
The Internet has reached a scaling limitation. And while experts would have predicted a collapse of the routing protocols, or a failure in congestion control mechanisms, the first 'real failure' of the Internet, that we are going to observe soon, is a very simple one: we are out of new addresses. No more "names" for the growing number of users. Who would have thought of that?

Isn't this a trivial problem? Any sane man or woman would answer: "but why don't we just increase the address space then?". This is exactly what people are preaching for more than a decade now. It's a simple problem, and there is a simple solution: IPv6. The protocol has been created, implemented, and is supported by most modern operating systems. The only problem: it is just not being used.

What if we continue not using it? As this document points out very nicely, there are some terrifying alternatives. I mainly agree with what is said in this section, it's a very good overview of the benefits of IPv6 and some of the horrors that we might face, if we chose to ignore the problem for much longer.

And always recall, IPv6 is not "a fancy new thing", it has been around for a long time, and should be turned on now. This section also addresses some of the challenges if we turn it on and balances this with the problems we face, if we don't turn it on.

Internet kot kritična infrastruktura družbe

Kritično infrastrukturo predstavljajo obrati, omrežja, storitve in premoženja informacijske komunikacijske tehnologije, katerih okvara ali uničenje bi resno vplivala na zdravje, varnost ali gospodarsko blaginjo državljanov, ali pa na učinkovito delovanje države.

Kritične infrastrukture zajemajo številne sektorje gospodarstva, tudi bančništvo in finance, promet in dostavo, energetiko, komunalne storitve, zdravstvo, oskrbo s hrano ter ključne državne službe. Ena od najpomembnejših, tudi kritičnih infrastruktur je komunikacijska infrastruktura. Večina današnje komunikacijske infrastrukture, predvsem pa internet, temelji na protokolu IPv4, ki se uporablja že skoraj 30 let. Protokolu IPv4 so od njegovega nastanka do danes dodali mnogo protokolov in mehanizmov, da bi povečali njegovo

3 **Olaf Maennel**, redni profesor na Loughborough University, UK., ima zelo širok pogled nad mednarodnim dogajanjem na področju IPv6. Njegov prispevek k študiji bo pogled in komentar na naša razmišljanja iz zunanjega, mednarodnega stališča. Njegove misli smo zapisali v izvirniku na začetku posameznih poglavij.

uporabnost in izboljšali varnost komunikacije. Kljub izboljšavam ni odpravljena glavna pomanjkljivost, to je za današnje potrebe relativno majhno število naslovov IPv4, s katerimi lahko globalno naslavljamo omrežne naprave in terminale.

Internetni protokol IPv4 ima svojega naslednika že več kakor deset let. To je internetni protokol v različici 6 (IPv6). IPv6 v primerjavi z IPv4 omogoča dodatne funkcionalnosti, hkrati pa vsebuje večino funkcionalnosti, ki so bile pri IPv4 razvite v obliki dodatnih protokolov. Teoretično omogoča globalno naslavljanje več kakor 3,4 x 10^38 (2^128) omrežnih naprav, kar je njegova največja prednost.

Kratek povzetek zgodovine uvajanje protokola IPv4 in IPv6

IPv4 protokol je bil specificiran leta 1981 v dokumentu RFC791. Leta 1991 se je IETF (Internet Engineering Task Force) in internetna skupnost operaterjev, načrtovalcev omrežij in raziskovalcev odločila, da ima IPv4 pomanjkljivosti, saj dolgoročno ne zagotavlja dovolj velikega naslovnega prostora za rast interneta. Po dolgih razpravah in usklajevanjih so leta 1995 izdali prvo specifikacijo IPv6, imenovano IPng (IP Next Generation)[1].

6BONE

Omrežje 6bone je bilo testno okolje za internetni protokol različice 6. Bilo je produkt projekta IETF IPng, ki je ustvaril protokol IPv6. Ta naj bi sčasoma nadomestil sedanje internetne protokole omrežne plasti, znane kot IPv4. 6bone se je začel zunaj uradnega okvira IETF na srečanju marca 1996 in hitro je postal svetovni partnerski projekt z neformalnim nadzorom IETF, delovne skupine »NGtrans» (IPv6 Transition).

Prvotno poslanstvo 6bone je bilo vzpostaviti mrežo za pospeševanje razvoja, testiranja ter uvajanje IPv6 in je uporabljal model, ki temelji na izkušnjah iz omrežja Mbone, od tod tudi ime »6bone«.

6bone je začel kot navidezno resnično omrežje (z uporabo IPv6 čez tuneliranja IPv4), ki je deloval na osnovi interneta IPv4 s podporo za tuneliranje prometa IPv6, sčasoma pa so dodajali tudi prave, domorodne povezave za IPv6. Čeprav je bil na začetku pri 6bonu poudarek na testiranju standardov in implementacije, se je pozneje osredotočil in tudi postal testno okolje za preverjanje in razvijanje postopkov prehoda in operativnih postopkov, ni bil pa več namenjen testiranju dejanske uporabe omrežja IPv6.

6bone je deloval v naslovnem prostoru 3FFE::/16.

Svoj vrhunec je 6bone dosegel sredi leta 2003. 1. januarja 2004 so se odločili, da je 6bone dosegel svoj namen in da ga je treba počasi zapreti, kar se je zgodilo 6. junija 2006. Naslovni prostor 3FFE::/16 se je vrnil med razpoložljive alokacije.

IPv6 je zasnovan tako, da odpravlja ključne pomanjkljivosti IPv4, v grobem pa lahko spremembe razdelimo na 6 glavnih področij:

1. velik naslovni prostor,
2. hierarhično naslavljanje in usmerjanje (Addressing and routing),
3. varnostne razširitve,
4. odpravlja prevajanje omrežnih naslovov (NAT),
5. samodejna konfiguracija omrežnih elementov,
6. podpora za mobilnost.

Od leta 1995 je bilo objavljenih čez 30 dokumentov RFC, ki dodatno opredeljujejo veliko spremljajočih sprememb, od tega, kako so naslovi IP shranjeni v sistemu in aplikacijah DNS, do tega, kako so "datagrami" poslani in usmerjani čez plast podatkovne povezave (Ethernet, PPP, Token Ring, FDDI) in vse druge medije, ter tega, kako programerji kličejo omrežne funkcije.

Ker sta IPv4 in IPv6 v omrežni plasti popolnoma nezdružljiva, je IETF predvidel kar nekaj mehanizmov za prehod, od tuneliranja (prenos paketov IPv6 po omrežju IPv4 in nasprotno) do translacije (prevajanje IPv4 v IPv6 in nasprotno) ter predvsem soobstajanja obeh protokolov v sistemu dual-stack. V tem sistemu omrežna naprava (odjemalec, strežnik, usmerjevalnik ...) sočasno uporablja protokola IPv4 in IPv6.
Bistvena omejitev protokola IPv4 je velikost naslovnega prostora. Naslov IPv4 je 32-biten, kar pomeni, da lahko z naslovom IPv4 (navadno zapisan v obliki xxx.xxx.xxx.xxx) teoretično naslovimo štiri milijarde različnih naprav. V tistih časih nepojmljiva številka je zdaj zaradi vedno hitrejše rasti interneta postala premajhna.
Ključni razlog za tolikšno povečanje naslovnega prostora v IPv6 je bila želja po bolj hierarhičnem usmerjanju in učinkovitejšem delovanju hrbteničnih omrežij, a smo se omenjenim pridobitvam zaradi načina dodeljevanja naslovov IP in nerešenega vprašanja uporabnikov z redundantnimi internetnimi dostopi (multihoming) morali žal kmalu odpovedati.

Dandanes naslove IP potrebujejo strežniki, komunikacijska oprema ter vse fiksne in mobilne naprave ter terminali, ki potrebujejo (stalno) povezljivost IP. Prav mobilnost in miniaturizacija sodobnih terminalov predstavljata tudi ključni izhodišči za vzpostavitev nove generacije internetnega omrežja, tako imenovani »internet stvari« (Internet of Things).

Mehanizmi za učinkovitejšo rabo naslovnega prostora IPv4

Zaradi počasnega uvajanja IPv6 so med leti 1993 in 1996 razvili vrsto mehanizmov, ki so začasno upočasnili porabo javnih naslovov IPv4. Leta 1993 so razvili mehanizem CIDR (RFC1519 – Classless Inter-Domain Routing). Leta 1994 je bil razvit mehanizem NAT

(RFC1631 – The IP Network Address Translator), leta 1995 mehanizem VLSM (RFC1817 – CIDR and Classful Routing) ter nato leta 1996 še zasebni naslovni prostor (RFC1918 – Address Allocation for Private Internets). Vsi našteti mehanizmi in možnost uporabe zasebnega naslovnega prostora so sicer podaljšali življenjsko dobo protokolu IPv4, vendar so razvrednotili osnovno idejo delovanja interneta – transparentno povezljivost komunikacije od enega do drugega konca.

IPv6 – novosti in spremembe

Protokol IPv6 je obdržal večino prednosti IPv4; spremembe so (poleg daljšega naslovnega prostora) predvsem popravki napak v protokolnem skladu IPv4. Bistvene spremembe so:

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

Druge prednosti protokola IPv6

Pomanjkanje naslovnega prostora IPv4 pa ni edini razlog, zaradi katerega bi morali izvesti prehod na IPv6. V zadnjih letih je internet z vsebinami in storitvami, ki jih omogoča, prinesel vsem uporabnikom nove možnosti na vseh področjih delovanja. Hitrost dostopa na fiksnih lokacijah se povečuje. Številne evropske države načrtujejo, da bodo povečale hitrost dostopa vsaj na 100 Mbit/s do leta 2015. Povečalo se bo število širokopasovnih (HSPA, LTE) mobilnih omrežij, ki bodo uporabnikom zaradi velikih hitrosti in kratkih odzivnih časov omogočile podobno uporabniško izkušnjo, kot jo imajo zdaj s klasičnim (fiksnim) dostopom. Trendi uporabe interneta, kot so izmenjava video vsebin, TV visoke ločljivosti (tudi 3D), izobraževanje, bodo količino prenesenih podatkov še povečali. Internetne storitve, kot so socialna omrežja (Facebook, Twitter ...) in računalništvo v oblakih, spodbujajo nove inovacije. Računalništvo v oblakih močno zmanjšuje ovire pri dostopu na trg ponudnikov storitev, zlasti za mala in srednje velika podjetja. V prihodnosti se bo lahko v internet priključila množica naprav, vozil, senzorjev, kamer in drugega. Predpogoj za takšen scenarij pa so le zmogljiva, visoko prepustna in varna omrežja, ki bodo morala temeljiti na sodobnejših napravah in protokolih, katerih temelj je trenutno le protokol IPv6.

Pri načrtovanju prehoda na IPv6 pa ni gonilna sila samo tehnična naprednost novega protokola, temveč tudi možnost za razvoj novih izboljšanih storitev, aplikacij, ter novih oblik

povezovanja in izmenjave informacij. Kot primer uporabe bi lahko navedli razmah storitveno usmerjene infrastrukture (SOI – Service Oriented Infrastructure) za varno in učinkovito sodelovanje uporabnikov z deljenimi storitvami IT, ki jo omogoča grid tehnologija in virtualizacija. Doslej je bilo ponujanje storitev in vsebin prek interneta večinoma domena večjih podjetij – ponudnikov vsebin z lastnimi podatkovnimi centri, ali ki gostujejo s strežniki pri kakšnem ISP-ju ali ponudniku strežniškega gostovanja. Z uvedbo IPv6 in ukinitvijo mehanizmov NAT se odpirajo na slutene nove možnosti za manjša podjetja in rezidenčne uporabnike, ki bodo lahko svoje vsebine ponudili tudi na podlagi drugih storitvenih protokolov.

Pregled uvajanja IPv6

Četudi nam protokol IPv6 prinaša veliko izboljšav in prednosti v primerjavi z IPv4, razen v akademskih in velikih hrbteničnih omrežjih še ni doživel množične komercialne vpeljave. Analize v komercialnih evropskih omrežjih kažejo porast prometa IPv6 šele v zadnjem letu dni (Botterman 2010). IPv6 ni nazaj združljiv z IPv4 in sistemi IPv4 ne morejo uporabljati storitev IPv6 ali komunicirati neposredno z gostitelji IPv6 (ECC-CEPT 2010). Mnoge organizacije imajo aplikacije, ki niso združljive z IPv6, zato je prehod na IPv6 pogojen z nadgradnjo ali celo zamenjavo aplikacij, ali pa zahteva uporabo translacijskih mehanizmov (IETF 2005). Uporabniki se soočajo s pomanjkanjem storitev, aplikacij in naprav, ki bi temeljile na novem protokolu in bi bile hkrati razlog za njegovo pospešeno uvedbo. Pomanjkljivo je tudi znanje o njegovem delovanju in o prednostih, ki jih prinaša protokol. Njegova vpeljava na jedrnem in dostopovnem omrežju je tehnično in organizacijsko zahtevna, poleg tega pa operaterjem in internetnim ponudnikom predstavlja dodatne stroške. Določene naprave, predvsem tiste, ki zagotavljajo varnost, nadzor, izenačevanje prometa (Load balancing) in obračunavanje, še nimajo povsem enakovrednih funkcionalnosti ali učinkovitosti, kot jih imajo primerljive naprave iz okolja IPv4. Takšno stanje se pospešeno popravlja z vse večjim povpraševanjem. Mnogi operaterji še ne vidijo dodane vrednosti protokola IPv6, hkrati pa ni dovolj velikega povpraševanja uporabnikov, zaradi katerih bi izvedli nadgradnjo omrežij.

Naštete težave zavirajo uvedbo protokola IPv6. Nadgradnja omrežij na internetni protokol IPv6 pa je ključna za nadaljnji razvoj interneta, internetne družbe in internetnega gospodarstva. Če uvajanje IPv6 ne bo močno pospešeno, bo prišlo do izjemne upočasnitve rasti interneta, ostanki IPv4 v omrežjih pa bodo povečali stroške uporabe interneta. Posledice te zamude pri uvajanju bodo večji stroški na vseh področjih internetnih storitev, soočali se bomo z upočasnitvijo inovacij v omrežjih, ki temeljijo na internetnem protokolu, počasnejša bo gospodarska rast. To ugotavljajo med drugim pri ameriškemu Ministrstvu za trgovino (U.S. Department of Commerce 2006), NTIA, NIST, OECD-ju (OECD 2008), ITU-ju (ITU 2008) in pri Evropski komisiji (Commission of the European Communities 2008).

Izčrpanje IPv4 naslovnega prostora, napovedi in pravila razdeljevanja

Po nekaterih napovedih naj bi organizaciji IANA, ki skrbi za celoten nabor naslovov IPv4, teh zmanjkalo že konec tega leta ali v začetku leta 2011, ko bodo zadnjih 5 naslovnih blokov /8 razdelili regionalnim registrom – vsakemu svojega. Regionalni registri bodo zadnje dobljene bloke razdelili v različnem času, a pričakuje se, da bo prvi brez IPv4 naslovnega prostora ostal APNIC (Asia Pacific regija) predvidoma novembra 2011.

V regiji EU, za katero skrbi RIPE NCC, bomo zelo verjetno ostali brez novih naslovnih prostorov nekje v prvi polovici 2012, kar pomeni, da RIPE ne bo več mogel dodeljevati novega naslovnega prostora IPv4 lokalnim internetnim registrom (LIR). Tipično so največji porabniki naslovnega prostora IPv4 ponudniki dostopa do interneta (ISP). Zanje to pomeni, da ne morejo več priključevati novih uporabnikov. S tem se rast in širjenje teh podjetij praktično ustavi. Veliki, če ne celo večji porabniki naslovnega prostora pa bodo postali uporabniki mobilnih (pametnih) telefonov, ki se vse več povezujejo v internet.

Razumeti moramo, da ISP (oziroma LIR) lahko zahteva od RIPE NCC novo alokacijo naslovnega prostora IPv4, šele ko porabi približno 80% svojih dodeljenih naslovov. Obdobje, za katero lahko LIR rezervira in upraviči porabo naslovnega prostora IP, se sistematično zmanjšuje. S prvotnih dveh let smo časovno razdobje zmanjšali na eno leto, zdaj pa se vsake pol leta razdobje še skrajšuje, kot je navedeno v spodnji razlagi. To pomeni, da bodo veliki porabniki naslovnega prostora IPv4 ostali brez naslovov IP skoraj sočasno z RIR-i, saj si ne bodo mogli narediti zaloge naslovov.

Poglejmo si podrobneje pravilo skrajševanja časa za rezervacije naslovnega prostora in pravilo razdelitve zadnjega bloka /8:

- do 1. 1. 2010 je bil čas, za katerega je LIR lahko opravičil oziroma utemeljil porabo in zahteval dodelitev naslovov IPv4 za naslednji dve leti,
- med 1. 1. 2010 in 1. 7. 2010 je bil ta čas 1 leto,
- med 1. 7. 2010 in 1. 1. 2011 je ta čas 9 mesecev,
- med 1. 1. 2011 in 1. 7. 2011 bo ta čas 6 mesecev,
- po 1. 7. 2011 bo ta čas 3 mesece,
- ko RIPE od IANA dobi zadnji blok /8, bo iz njega vsak LIR lahko dobil naslovni prostor samo /22 in nič več, ne glede na to, kako velik je in kakšne potrebe ima. Razlogi za to so morebitni prihodnji novi ponudniki dostopa, ki bodo po tem pravilu lahko dobili /22 še kar nekaj časa.

To pomeni, da bo večina operaterjev v EU verjetno ostala brez zalog do konca leta 2012, seveda če je njihova rast in potreba po novih naslovnih prostorih IPv4 vsaj približno podobna povprečni rasti interneta po svetu.

Države sveta se različno odzivajo na problem pomanjkanja naslovnega prostora IPv4 in uvajanje protokola IPv6. Azijske države, ki imajo največji porast penetracije širokopasovnih uporabnikov v fiksnem in mobilnem omrežju, aktivno promovirajo in pospešeno uvajajo protokol IPv6 ter storitve, ki temeljijo na IPv6. Zavedajo se, da jim naslovni prostor IPv4 še zdaleč ne zadošča za nadaljnjo širitev omrežij, porast uporabnikov, razvoj novih aplikacij, naprav in storitev. Tudi ZDA pospešeno uvajajo IPv6 v svoja omrežja. Leta 2005 je vlada ZDA z odlokom predpisala vsem svojim vladnim agencijam, da morajo do junija 2008 nadgraditi svoja jedrna omrežja na IPv6 in se obenem povezati s svojim vmesniki na ta omrežja (Executive Office of the President 2005). Ameriški Nacionalni inštitut za standarde in tehnologijo (NIST – The National Institute for Standards and Technology) je bil izbran, da razvije potrebne standarde, ki bodo za vse vladne institucije zagotovili poenoten sistem potrebnih specifikacij in način certificiranja, ki bodo zavezujoče pri nabavi opreme IPv6 (NIST 2008). Tudi Evropska komisija zadnjih deset let aktivno promovira uvajanje IPv6. S prvim *Sporočilom Evropske komisije: IPv6 internet prihodnje generacije – prioritete za ukrepanje in migracija na nov internetni protokol IPv6* (Commission of the European Communities 2002) je vzpostavila evropski IPv6 Task Force, začrtala prednostne dejavnosti, finančno omogočila uvedbo IPv6 v raziskovalno-izobraževalnih omrežjih, podprla razvoj standardov ter vpeljala številne delavnice in usposabljanja. Maja 2008 je Evropska komisija izdala še drugo *Sporočilo*: *Nadaljnji razvoj interneta – Akcijski načrt za uvedbo internetnega protokola različice 6 (IPv6) v Evropi* (Commission of the European Communities 2008), s katerim je želela, da se že sprejeti ukrepi še podkrepijo. Čeprav je bil napredek narejen, je uvajanje IPv6 v evropska omrežja še vedno prepočasno, medtem ko se je problem s pomanjkanjem naslovov IPv4 še povečal (Europe's Information Society 2010).

Obstaja več scenarijev, ki bodo posledica pomanjkanja naslovov IPv4. Nekateri scenariji predvidevajo, da bodo tiste organizacije, ki imajo veliko neizkoriščenih naslovov IPv4, te začele vračati nazaj regionalnim internetnim registrarjem. Vrnjeni naslovi IPv4 bodo na razpolago za vnovično dodelitev. Ta scenarij je malo verjeten. Malo verjetno je, da bi organizacije prostovoljno začele vračati omejeno dobrino, kot je naslovni prostor IPv4, še posebej zato, ker jim z njihovim pomanjkanjem ekonomska vrednost raste.

Možen scenarij je tudi, da bodo organizacije začele trgovati s svojimi neuporabljenimi naslovi IPv4. V tem primeru se bo vzpostavil sekundarni trg naslovov IPv4. Problem, ki lahko pri tem nastane, je, da bo prišlo do velikega povečanja zapisov BGP usmerjevalnih poti v usmerjevalnih tabelah. Vseh poti BGP je trenutno (november 2010) čez 330.000, predvsem zaradi zmožnosti agregacije in ustrezne politike dodeljevanja naslovnih blokov IP (operaterjem dodeljeni bloki naslovov IP so si med seboj stični). Ta številka bi se lahko ob ne reguliranem trgovanju z naslovi bistveno povečala. Zaradi tega lahko pride do

degradacije hitrosti posredovanja prometa v usmerjevalnikih oziroma do nestabilnosti interneta.

Lahko pa se tudi zgodi, da bodo organizacije začele naslove IPv4 uporabljati učinkoviteje, še posebej, če bodo RIR-i uvedli pristojbine za dodeljene naslovne bloke IPv4.

Tržišče in rast interneta po izčrpanju naslovnega prostora IPv4

Če bo naslovov IPv4 zmanjkalo, bo internet deloval še naprej. Obstoječi operaterji bodo imeli možnost, da postopoma preidejo na protokol IPv6 ali nadaljujejo z obstoječim (zastarelim) protokolom IPv4, pri čemer si bodo morali zaradi pomanjkanja javnih naslovov IPv4 pomagati s translacijskimi mehanizmi. Z veliko večjimi težavami pa se bodo pri vstopu na trg srečali novi operaterji, ki naslovnega prostora IPv4 ne bodo imeli ali ga bodo v skladu s pravili NRO (National Resource Organisation) lahko dobili zelo malo.

Slovenija ima dokaj zasičen internetni trg, zato se ni treba bati, da bi obstoječim ISP-jem zmanjkalo naslovnega prostora IPv4 v zelo kratkem času. Problemi, ki jih vidimo, se skrivajo drugje. Nov ISP, ki bo nastal po dodelitvi zadnjega bloka /8 od RIPE, ne bo mogel dobiti več kot blok /22 naslovov IPv4, kar pomeni največ 1022 naslovov IPv4. S takšno količino javnega naslovnega prostora lahko nov operater začne razmišljati samo o tem, da bo vsem svojim uporabnikom dodelil zasebne naslove IPv4 (RFC1918) ter v jedru omrežja izvajal prevajanje med zasebnimi in javnimi naslovi (NAT/PAT) s tehnologijo CGN (Carrier Grade NAT) ali LSN (Large Scale NAT).

Zakaj je prevajanje naslovov v omrežju škodljivo

Poznamo več vrst translacijskih mehanizmov, vsem pa je skupno, da spreminjajo vsebino glave vsakega paketa, ki prehaja skozi translacijsko napravo. Osnovni namen translacije je predvsem v zmanjševanju potrebnih javnih naslovov IPv4. Za vsako translacijo je potreben določen čas obdelave paketa, z večanjem števila sej, ki poteka skozi napravo, pa se podaljšuje tudi čas odzivnosti same naprave, kot se povečuje njegova kompleksnost. Današnje spletne aplikacije za posameznega uporabnika odpirajo več deset vzporednih sej (Google Maps tipično odpre 70 vzporednih povezav, iTunes jih odpre tudi do 300, odjemalci P2P pa tudi več kot 2000). Mehanizem NAT ali napravo s to funkcionalnostjo lahko uporabimo pri uporabniku na meji med lokalnim uporabniškim omrežjem in ponudnikom dostopa, lahko pa ga v zmogljivejši različici (CGN – Carrier Grade NAT) namesti tudi ponudnik dostopa v samem jedru omrežja.

Moramo pa se zavedati, da z uvedbo mehanizma NAT v jedru omrežja (CGN/LSN) zapremo uporabnike v »Walled garden«, kjer jim omejimo transparentno komunikacijo od konca do konca, ki jo imajo sedaj na voljo. Odvzamemo jim tudi ves nadzor nad prevajanjem naslovov, ki se sedaj izvaja na končni omrežni napravi (usmerjevalniku).

Tehnologija CGN premika prevajanje naslovov v jedro omrežja, kar je slabo in v nasprotju z idejo interneta – modelom preprostega posredovanja paketov v jedru omrežja in s pametnimi napravami čim bolj na zunanjih mejah omrežja.

Ideja »pametnega jedra« lahko pripelje operaterja oziroma ponudnika dostopa do interneta v situacijo, ko je mogoče pričakovati poslovno škodo, ker uporabnik ni mogel komunicirati po internetu z določenimi zasebnimi aplikacijami in protokoli, ki so bili narejeni namensko ter niso znani in javno dosegljivi. Če je NAT (CGN) v jedru operaterjevega omrežja, komunikacija s takšnimi aplikacijami preprosto ne deluje več. Prej si je uporabnik namestil aplikacijski prehod (ALG-Application Layer Gateway) pri sebi na svoji napravi, po novem pa tega ni več možno narediti, saj NAT v jedru omrežja dodatnih aplikacijskih prehodov ne podpira, oziroma ga ni mogoče preprosto in hitro prirediti za nove aplikacije in protokole. To pa je v nasprotju s primarno idejo interneta – neposredno povezljivostjo med končnimi točkami brez vmesnih ovir.

Dandanes domače naprave NAT uporabljajo omrežne protokole UPnP/NAT-PMP ali tehniko, ki se imenuje »port-forwarding«. S postavitvijo mehanizma NAT v jedro se ta nadzor pri uporabniku popolnoma izgubi, saj ga ponudnik storitev ne bo dovolil že iz varnostnih razlogov.

Naslednja težava, ki jo prinašajo naprave CGN, je skalabilnost. Operaterji se soočajo s pritiski odločanja med tem, ali bodo s postavitvijo CGN agregirali omrežje, kolikor je to le mogoče, po drugi strani pa množična agregacija pomeni problem, če ne drugačnega, s tabelami stanj. CGN predstavlja tudi kritično mesto odpovedi (single point of failure) in podvojene naprave CGN bodo imele velike probleme s sinhronizacijo stanj (states tables).
Bistven problem prevajanja naslovov pa je nedvomno sledljivost uporabnikov, ki jo nalagata Zakon o elektronskih komunikacijah ter evropska Direktiva o hrambi prometnih podatkov (Uradni list Evropske unije 2006). Ob uporabi tehnologije CGN je skorajda nemogoče ugotoviti, kdo je uporabnik, ki je vdrl v sistem na drugem koncu sveta, poslal nezaželeno pošto ali naredil kakšen drug prekršek ali kriminalno dejanje v internetu. Za enim naslovom IPv4 se teoretično lahko skriva več kakor 65.000 uporabnikov, kar hudo oteži iskanje kršitelja, še zlasti kadar več uporabnikov z istega javnega naslova IPv4 dostopa do istega strežnika.

Ohranjanje konkurenčnosti in kontinuirane rasti

Bistveni element, ki bo operaterje prisilil k uvedbi IPv6, je ohranjanje konkurenčnosti in rasti. Operater mora uporabniku zagotoviti dostop do vsebin in storitev v internetu. Storitve morajo biti kakovostne, zanesljive, privlačne, cene primerljive s konkurenco, predvsem pa varne. Nikjer pa ni eksplicitno zapisano, kateri protokol naj se za to uporabi. Napredni operaterji že pospešeno uvajajo IPv6 v hrbtenična omrežja in delajo testne projekte v

dostopovnem omrežju. Azijski del sveta, ki ima največjo penetracijo uporabnikov in največjo porabo naslovov IPv4, nima druge izbire, kot da že pospešeno uvaja IPv6 v vseh delih omrežja ter razvija aplikacije in storitve, ki temeljijo na tem protokolu. Ko bodo konkurenčni operaterji poleg IPv4 uvedli še IPv6, se bodo pojavili uporabniki, storitve in vsebine, ki bodo lahko dosegljivi po obeh protokolih. Operaterji, ki svojim uporabnikom ne bodo omogočili dostopa do vsebin, ki bodo dostopne le prek IPv6, bodo kmalu postali nekonkurenčni. Operaterjem bo zagotavljanje dostopa do interneta s protokolom IPv4 sčasoma postalo vse preveč zapleteno. Z uvajanjem tehnologije CGN se bo kompleksnost prevajanja naslovov še povečevala, kar so že občutili nekateri mobilni operaterji (tudi slovenski), ki CGN uporabljajo že več let.

Uvajanje IPv6 nedvomno poenostavi nastavitve končnih naprav. Po priporočilu IETF (RFC3177) dobi vsaka rezidenčna naprava CPE svoj del naslovnega prostora IPv6, vsak računalnik pa svoj lastni javni naslov IPv6. Od tu dalje je vse preprosto: iz računalnika/strežnika doma začnemo streči vsebine ali storitve, kar ob pravilni nastavitvi požarnega zidu IPv6 ni zapleteno opravilo. Usmeritev ISP-ja v skrb za uporabnika zna biti močan mehanizem koordinirane in časovno usklajene uvedbe IPv6 vse do uporabnika, saj si nihče ne želi ne prebega uporabnikov med operaterji in ne nezadovoljnih uporabnikov, ki oblegajo center za telefonsko pomoč.

Postopek uvajanja IPv6 v omrežje

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

Treba je izvesti natančno študijo izvedljivosti, ki nam bo podala oceno potrebnih sprememb, tveganja, stroškov (nova oprema, izobraževanje osebja, zaposlitev novega osebja) in časa, potrebnega za prehod. Prehod se mora izvajati v korakih in vključuje potrebne spremembe za vse uporabnike, strežnike v lokalnem omrežju ali internetu, aplikacije, storitve, naprave in posamezne elemente. Narediti je treba analizo tehničnih in poslovnih koristi. Prehod mora upoštevati dolgoročne cilje organizacije, ki prinašajo dodano vrednost, večjo učinkovitost in produktivnost ter zadovoljstvo uporabnikov.

Izvesti je treba temeljito analizo, koliko obstoječe strojne in programske opreme bo treba zamenjati ali nadgraditi, da bo sposobna učinkovito uporabljati IPv6 in IPv4. Pri popisu opreme je priporočena uporaba vnaprej predpisanega obrazca z zahtevanimi atributi. Nato je treba ugotoviti, na katere dele omrežja in storitev bosta zamenjava oziroma nadgradnja še vplivali. Pri nabavi nove strojne opreme je treba upoštevati standardne cikle zamenjave opreme, saj bo strošek menjave, kadar gre za načrtovano investicijo, bistveno manjši. Pomembno je, da oprema, ki jo kupujemo danes, popolnoma podpira protokol in

funkcionalnosti IPv6, ki jih bomo potrebovali v času njene življenjske dobe. Dokler v Sloveniji ali Evropi ni sprejetih tehničnih standardov, ki bi natančno opredeljevali, katera oprema je skladna z IPv6 oziroma sposobna za delo z njim, in dokler za to opremo ne bo ustreznih certifikacijskih organov, ki bi skladnost opreme (tehnične navedbe proizvajalcev) preverjali, se priporoča, da se pri nabavi uporablja seznam (UC – ACL Unified Capabilities Approved Products List) opreme, ki ga objavlja ameriška vojaška organizacija JITC (Joint Interoperability Test Command). Omenjeni seznam, ki ga je naredil ameriški NIST (National Institute of Standards and Technology), pri nabavi opreme uporabljajo ameriško Ministrstvo za obrambo in vse ameriške zvezne agencije. Več o tem seznamu je zapisano v poglavju, ki govori o primerjavi nacionalnih strategij.

Zelo pomemben del je izvedba izobraževanja za omrežne arhitekte, sistemske skrbnike in upravljavce omrežij, podporne službe in drug tehnični kader.Skrbno je treba izdelati naslovni načrt, ki bo dolgoročno pokrival širjenje organizacije v prihodnje, in ki bo vključeval sedanje in prihodnje storitve. Od regionalnega oziroma lokalnega registrarja je treba dobiti naslovni blok IPv6 (IPv6 prefiks) in se povezati v omrežje IPv6 (tranzit in peering). Postaviti je treba testno okolje, v katerem se bo preizkusila oprema, storitve, v katerem bo mogoče izobraziti uporabnike ter preizkusiti ključne funkcionalnosti v praksi. Šele ko bomo zagotovo ugotovili, da testno okolje izpolnjuje vsa naša pričakovanja, bomo lahko implementacijo v produkcijsko okolje.

Pri pripravi načrta prehoda moramo določiti projektne faze ter mejnike, ki so realno dosegljivi in ki jih lahko objektivno merimo. Določiti je treba odgovorne osebe, ki bodo zadolžene za usmerjanje dejavnosti v posameznih institucijah, nadzor ter pripravo poročila o napredku v posamezni fazi. V vsaki fazi moramo preverjati, ali so načrtovane dejavnosti izvedene in ali so stroški v pričakovanih mejah. Če bomo pravilno načrtovali in predvidevali vse možne posledice, bomo imeli stroške pod nadzorom in bomo lahko minimizirali tveganje. Uvedba mora biti za končne uporabnike čim bolj transparentna in nezaznavna.

Vloga države in javne storitve

Država si ne sme in ne more privoščiti, da bi se pojavili operaterji, ki bi zaradi pomanjkanja naslovnega prostora IPv4 ponujali uporabnikom samo dostop prek IPv6, internetne storitve javne uprave pa ne bi bile dostopne po obeh protokolih, ampak samo po IPv4. Država si dolgoročno ne sme privoščiti niti tega, da bi imela svoje storitve dostopne samo prek protokola IPv4. V tem primeru bi nekatere državljane spremenili v drugorazredne, saj ne bi mogli dostopati do vsebin in storitev, ki so bile financirane iz javnih sredstev.

Država ima zelo pomembno vlogo pri uvajanju IPv6. S svojim vzorom mora dvigovati ozaveščenost in spodbujati uvedbo IPv6. Številne vlade držav po svetu so v svojih strategijah zapisale, da je uvedba IPv6 ena od njihovih prioritetnih nalog. Med prvimi so

začele izvajati prenos svojih omrežij in storitev ZDA, Nemčija, Japonska ... Ozaveščenost se lahko dviguje z javnimi nastopi vplivnih politikov, ki poudarjajo pomembnost prehoda na IPv6. Velika spodbuda uvajanju IPv6 se lahko izkaže pri naročanju strojne opreme in pri razvoju ali nakupu programske opreme v javnih naročilih. Kjer financira ali sofinancira gradnjo (širokopasovnih) omrežij, bi morala zahtevati, da omrežja in naprave uporabljajo IPv6 kot primarni omrežni protokol. Država bi morala med prvimi omogočiti, da so njihove spletne strani in e-storitve dosegljive tudi prek IPv6, obenem pa zahtevati od svojih partnerjev in izvajalcev, da sledijo njenemu zgledu. Namenjati bi morala znatna finančna sredstva za izobraževanje v okviru delavnic, seminarjev, akademij in podobno. Finančno lahko podpre razvoj novih testnih okolij, aplikacij in storitev, ki bi temeljile na IPv6. Velik del gospodarstva temelji na kontinuirani stabilnosti in rasti interneta. Kako bo potekal nadaljnji razvoj telekomunikacij, v Sloveniji v veliki meri soodloča tudi država. Kot generator povpraševanja in dajanja zgleda posledično v veliki meri pospešuje rast in razvoj države ter povečuje blaginjo državljanov.

Kot je pokazala analiza o uvajanju IPv6 med slovenskimi operaterji elektronskih komunikacij, ki jo je opravil APEK v februarju 2010, je zavedanje (vsaj večjih) operaterjev po potrebnem prehodu na IPv6 zelo močno. Vendar uvedba IPv6 zahteva na kratek rok stroške, ki jih je treba upravičiti. V času varčevanja in zmanjševanja investicij je to še težje. Veliko izkušenj iz produkcijskega okolja Slovenija še nima, prav tako (še) ni dovolj strokovnega znanja s strani dobaviteljev opreme in sistemskih integratorjev. V prehodni fazi bomo neizogibno potrebovali vzajemno delovanje opreme IPv4 in IPv6. Ponudniki storitev in operaterji čakajo drug drugega in opazujejo, kdo bo začel prehod uresničevati in obrnil krog razvoja. V tej fazi je najpomembnejše, da se združijo moči med akademsko sfero, industrijo, operaterji ter ponudniki storitev in vsebin, pa tudi državo. Vsak od naštetih mora na svojem področju in v sodelovanju z vsemi prevzeti svojo vlogo in prispevati k razvoju Slovenije kot tehnološko napredne, varne in odprte države, ki bo zgled tudi drugim.

Randy Bush, Brett Carr, Daniel Karrenberg, Niall O'Reilly, Ondrej Sury, Nigel Titley, Filiz Yilmaz, Ingrid Wijte: *IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region*, dosegljivo na: http://www.ripe.net/ripe/docs/ripe-492.html

Phillip Smith, Alain Bidron: *Allocations from the last /8,* dosegljivo na: http://www.ripe.net/ripe/policies/proposals/2010-02.html

Sterle, J. Koršič, L. Volk, M., Kos, A. (2010): *IPv6 in Internet prihodnosti, Zbornik referatov: Prehod na IPv6. 24. delavnica o telekomunikacijah VITEL (Robnik, A., Sterle, J., Žorž, J. Straus, M., Kunc, U., Šoštarič, D), str. 8-14. Elektrotehniška zveza Slovenije: Ljubljana*

Botterman, M. (2010): *Draft Survey of IPv6 Deployment in 2010, http://www.ripe.net/ripe/meetings/ripe-60/presentations/Botterman-Update_on_IPv6_deployment_monitoring.pdf*

NRO (2010): *Number Resource Organization Report Highlights Strong Growth in Both IPv4 and IPv6 Allocations,* dosegljivo na naslovu: http://www.nro.net/media/nroReportHighlights.html,

ECC-CEPT (2010): *Preparing for IPv6, ECC Report 144,* dosegljivo na: http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP144.PDF

IETF(2005): *Application Aspects of IPv6 Transition, RFC4038*, dosegljivo na naslovu: http://tools.ietf.org/html/rfc4038

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

OECD (2008): *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

ITU (2008): *Resolution 64 – IP address allocation and encouraging the deployment of IPv6*, dosegljivo na naslovu: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.64-2008-PDF-E.pdf

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

Executive Office of the President, Office of Management of Budget (2005): *Transition Planning for Internet Protocol Version 6 (IPv6)*, dosegljivo na naslovu: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

COMMISSION OF THE EUROPEAN COMMUNITIES (2002): *Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6*, dosegljivo na naslovu: ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/mb_com_parlipv6.pdf

Europe's Information Society (2010): *Piloting IPv6 upgrade for Europe*, dosegljivo na naslovu: http://ec.europa.eu/information_society/policy/ipv6/events/march2009/IPV6%20TAKE%20UP%20IN%20EU%20Public%20autorities%20%20(2).doc

Uradni list Evropske unije (2006): *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in*

connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[1] RFC1883: Internet Protocol, Version 6 (IPv6) Specification
6BONE: http://en.wikipedia.org/wiki/6bone

2. Primerjava nacionalnih strategij in akcijskih načrtov nam primerljivih držav članic EU, najnaprednejših držav članic EU in nekaterih neevropskih držav

The problem has been studied well. There is just no incentives for players to deploy IPv6. Deploying IPv6 implies an increased hassle for end-users. And end-users just want to use the Internet, and not have to do a Ph.D. in networking first. The next set of players are website operators: why should they take-up the hassle to move to IPv6, if there are no "eye-balls" looking at their IPv6 version of the website. And finally there are Internet Service Providers, who face increased cost and potential issues by changing their network infrastructure. Why bother, if no customer is going to pay extra for it?

The problem of address space shortage, however, is still real! It does not go away just because there are no incentives to individual players. It has been understood that this is often the job of a government, if it's citizen are facing a crisis that they can't resolve on their own accord.

This section looks at other countries and governments and discusses what they have done or are planning to do to tackle the problem. It is amazing how some simple things can make an impact. It's time now to push for this change.

Francija

Ena od prvih držav, v kateri so se lotili uvedbe IPv6, je bila Francija. Leta 2002 je ob politični naklonjenosti francoske vlade in Ministrstva za raziskave in nove tehnologije ustanovila IPv6 Task Force. Skupini je predsedoval Patric Cocquet, ki je bil med drugim tudi soustanovitelj projekta 6Wind, podpredsednik IPv6 Foruma in kitajskega IPv6 Sveta. IPv6 Task Force je v novembru 2003 izdal priporočila za pripravo strateškega načrta, ki bi pomagal pri razvoju in uvajanju tehnologije IPv6 v Franciji (Recommendations for a Strategic Plan in the Developmentand Implementation of IPv6 Technologies in France). Strateški načrt, ki ga je podprla in usmerjala francoska vlada v sodelovanju z lokalnimi oblastmi, je vseboval konkretne dejavnosti, ki so pokrivale tri ciljne skupine: javne institucije in storitvene agencije, zasebni sektor in tretjo, ki se je osredotočala na organizacijo in nadzor poteka same strategije.

Vloga državnih organov in agencij v tej strategiji je bila v njihovi prodejavnosti pri zagonu in podpori uvajanja IPv6. IPv6 je bil uveden v nacionalni in regionalni komunikacijski infrastrukturi ter v infrastrukturi javnih institucij in kampusov. Javne institucije in agencije so morale ob pomoči koordinacijskih teles opredeliti ter objaviti svoje strategije, metodologijo ter časovne okvirje, ki bi njihovi lastni ali so uporabljeni komunikacijski infrastrukturi omogočili prehod na IPv6.

Francija je s strateškim načrtom sledila naslednjim prioritetnim usmeritvam:

- povezava vseh javnih entitet v internet po IPv6, še posebej šol in univerz,
- prehod vseh državnih spletnih strežnikov (.gouv.fr), ki bi omogočali dostop prek protokola IPv4 in IPv6,
- prehod obstoječih in promocija razvoja novih inovativnih aplikacij, ki bi temeljile na IPv6,
- vsa komunikacijska oprema, kupljena prek javnih naročil, lahko uporablja IPv6,
- javni organi bi morali pozvati gospodarske subjekte, ki delujejo bodisi samostojno bodisi kot skupina (poslovna združenja, raziskovalni laboratoriji, univerze, šole in velike družbe), k spodbujanju uvajanja internetnih tehnologij, ki temeljijo na IPv6,
- po vzoru ZDA na medresorski ravni pripraviti presojo o novi varnostni strategiji nove generacije omrežij IP (Ministrstvo za obrambo ima lahko pri tem vodilno vlogo pri potrjevanju procedur in tehnologij, ki jih je treba uvesti).

Za zasebni sektor so bile predlagane naslednje dejavnosti:

- večje družbe bi morale takoj začeti z načrtovanjem in nadgrajevanjem svojih računalniških virov in omrežij, ki bi postopno integrirale IPv6. To bi moralo vključevati tudi prenos obstoječih ter razvoj novih inovativnih aplikacij na IPv6. Te bi morale omogočati polno izkoriščanje novih funkcionalnosti, ki jih omogoča IPv6;
- telekomunikacijska podjetja ter izdelovalci profesionalnih in potrošniških elektronskih izdelkov, pa tudi razvijalci aplikacij in založniki programov morajo IPv6 integrirati v svoje izdelke ter objaviti časovni okvir njihove razpoložljivosti;
- operaterji telekomunikacij se morajo zavezati določenim časovnim okvirjem, v katerih bodo na hitrih žičnih (xDSL, Ethernet, kabel) in brezžičnih (WiFi, GPRS) omrežjih uvedli komercialne storitve IPv6;

Poleg strateškega načrta bi izpostavili še naslednje francoske dejavnosti:

- leta 1995 je bila ustanovljena skupina G6, neprofitno industrijsko združenje, ki združuje akademske in industrijske partnerje. Področje dela G6 je pospeševanje

izmenjave informacij, testiranje in eksperimentiranje s področja uvajanja IPv6 v Franciji;

- IPv6 je bil uveden v francoskem akademskem raziskovalnem omrežju RENATER. V okviru sodelovanja z G6 se leta 1995 uvedejo prve pilotske storitve IPv6. Od leta 2002 naprej RENATER omogoča domorodno hrbtenično omrežje IPv6, ki omogoča dostop več kakor 650 univerzam, raziskovalnim organizacijam in vladnim agencijam;
- leta 2002 je bilo uvedeno mednarodno komercialno domorodno omrežje IPv6 OpenTransitv6 (Azija, ZDA, Evropa);
- od leta 2001 do 2003 je potekal nacionalni raziskovalni projekt VTHDv6 (Next-generation Internet2) z uporabo tehnologije IP/WDM, ki ga je sofinancirala francoska vlada, izvajal pa RNRT (raziskovalni del France Telecom). V okviru RNRT so se med partnerji projekta omogočale storitve in aplikacije IPv4 in IPv6 (prehod iz tuneliranja v polni dvojni sklad). VTHDv6 je opredeljen kot prvi evropski WLAN IPv6 kampus (izveden v sodelovanju z Univerzo v Strasbourgu);
- francoski internetni ponudnik Nerim je prvi, ki je omogočil IPv6 v Evropi (2002). Od marca 2003 omogoča domorodni dostop IPv6 prek ADSL. Kjer domorodni dostop ni mogoč, ponudnik omogoča dostop IPv6 prek tunela IPv4;
- julija 2004 je omogočen zapis IPv6 AAAA v korenski domeni .fr TLD,
- leta 2005 je potekal prehod France Telecom na IPv6 (dvojni sklad). V juniju 2005 je bil izveden eksperimentalni širokopasovni dostop za uporabnike. Povezljivost IPv6 je omogočena prek Teredo, Tunnel Broker in ADSLv6;
- France Telecom (telekomunikacijski operater Orange) je od leta 2009 eden prvih globalnih ponudnikov IPv6 prek omrežja VPN MPLS;
- drugi največji francoski internetni ponudnik Free je v slabih petih tednih (7. november – 11. december 2007) z uporabo mehanizma 6rd (IPv6 Rapid Deployment) svojim uporabnikom omogočil dostop do interneta IPv6 (1.500.000 uporabnikov). Od marca 2008 dalje so ponudili samostojno storitev IPv6 (Telesite). V letu 2009 so zabeležili več kakor 310.000 uporabnikov IPv6;
- marca 2009 je bil objavljen dokument Action Plan for ICT »Digital France 2012«, ki vključuje tudi dejavnosti za uvedbo IPv6 v Franciji;
- v letu 2009 so sprejeli sklep, da morajo francoske javne institucije pri javnih naročilih komunikacijske opreme dosledno naročati opremo, ki je združljiva z IPv6.

Francija ima trenutno (septembra 2010) šest ponudnikov, ki svojim uporabnikom zagotavlja domorodno povezljivost IPv6. Francija ima dodeljenih 143 predpon IPv6 (France Telecom /19). V Franciji delujeta dve izmenjevalni točki IPv6 (IX).

Viri:

IPv6 Task Force France (2003): *Recommendations for a Strategic Plan in the Development and Implementations of IPv6*, http://www.fr.ipv6tf.org/DATA/PRESS/Recommandations%20IPv6%20TFF%20%28English%29.pdf

SixXS: http://www.sixxs.net/faq/connectivity/?faq=native&country=fr

Orange (2009): *Orange Business Services: first global service provider to offer IPv6 on the managed IP VPN global market*, dosegljivo na: http://www.orange-business.com/mnc/press/press_releases/2009/IPv6.html

IEEE Xplore: *Deployment and test of IPv6 services in the VTHD network*, dosegljivo na: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1262168, obiskano dne: 7.10.2010

Cassen, A. (2009): *IPv6@Free,* dosegljivo na naslovu: http://www.ripe.net/ripe/meetings/ripe-58/content/presentations/ipv6-free.pdf, obiskano dne 8.10.2010

Nerim, dosegljivo na: http://www.nerim.fr/ipv6, obiskano dne: 8.10.2010

Avstrija

V Avstriji so se prve dejavnosti s področja raziskav in uvajanja protokola IPv6 začele v raziskovalno-izobraževalnem omrežju ACONET (Austrian Academic Computer Network). Zgodnejša raziskovanja in razvoj IPv6 pa niso bila omejena samo na akademsko okolje. Telekom Austria je že v letih 1999 do 2003 sodeloval v dveh mednarodnih projektih IPv6: GCAP in Tsunami. Avstrijski IPv6 Task Force je bil ustanovljen marca leta 2004. Pobudnik za ustanovitev je bil Telekom Austria. Združuje še Univerzo na Dunaju, nacionalnega regulatorja telekomunikacij in radiodifuzije RTR (RTR-Rundfunk und Telekom Regulierungs GmbH) ter druga vodilna podjetja IT in raziskovalne institucije Avstrije. Uvedba IPv6 sovpada z nacionalno politiko države po pospešenem razvoju širokopasovnega dostopa. V okviru delovne skupine IPv6 je bilo ustanovljenih pet dodatnih delovnih skupin, katerih glavni cilj je bil pripraviti časovni načrt in razvoj uvedbe protokola IPv6 v Avstriji. Rezultat njihovega dela je bil dokument z naslovom: »Austrian IPv6 Roadmap«. Dokument vsebuje pregled vseh mehanizmov za prehod, popisane so možne faze prehoda. Dokument obravnava najpogostejša tehnična vprašanja, ki sledijo prehodu (DNS, usmerjanje, varnost, operativno omrežne in storitvene naloge), podrobneje je obravnavan vpliv uvedbe IPv6 na obstoječe dostopovno omrežje ter omrežje uporabnikov. Popisana so specifična priporočila za ponudnike ADSL in kabelskega dostopa.

Septembra 2004 je Avstrija IPv6 (AAAA zapis) omogočila v svojih ccTLD domenskih strežnikih. V letu 2005 je bil IPv6 omogočen na dunajski izmenjevalni točki (VIX – Vienna

Internet Exchange). Po podatkih Six Access in Internet Number Resource Database ima Avstrija v septembru 2010 dodeljenih 89 predpon IPv6 oziroma 8381 naslovnih blokov /32.

Viri:
Österreichische IPv6 Taskforce (2004): *Einleitung zur österreichischen IPv6 Task force*, http://www.ipv6taskforce.at/dokumente/040708/IPv6TF-Plenary-Intro-20040708.pdf
IPv6 Task Force Austria (2005): *Austrian IPv6 Roadmap*, (http://www.ipv6taskforce.at/dokumente/050929/roadmap-fullversion.pdf)

SixXS: https://www.sixxs.net/tools/grh/dfp/all/?country=at

Nemčija

Zvezna republika Nemčija je trenutno ena od vodilnih evropskih držav, ki v svojih javnih in zasebnih omrežjih pospešeno uvaja protokol IPv6. Po podatkih Six Access ima Nemčija v Evropi v avgustu 2010 registrirano največje število dodeljenih (vidnih) predpon IPv6 (221). V svetovnem merilu ima večje število le še ZDA (https://www.sixxs.net/tools/grh/dfp/all/-?country=de). Iz podatkov omenjene spletne strani je tudi razvidno, da ima Nemčija trenutno kar 10 ponudnikov (največ od vseh), ki svojim uporabnikom omogočajo domorodni dostop IPv6. Nemčija v Evropi trenutno vodi tudi po dodeljenih naslovnih blokih IPv6 /32. Na podlagi statistike, objavljene 4. 10. 2010, ki jo objavlja RIPE NCC (http://www-public.int-evry.fr/~maigron/-RIR_Stats/RIPE_Allocations/IPv6/ByNb/index.html), so Nemčiji dodelili že 9927 blokov IPv6 /32, kar predstavlja kar 28 % vseh dodeljenih blokov.

Nemčija je upravno razdeljena na 16 zveznih dežel, ki se dodatno delijo na upravne divizije, občine in občinske zveze. Vsaka enota ima lastno javno administracijo in pooblastila, ki so jim predpisani z ustavo. Nemška vlada kot lokalni internetni registrar (LIR) je član evropskega registrarja RIPE NCC. Nemška vlada si je leta 2009 pri RIPE NCC izborila naslovni prostor IPv6 velikosti /26, kar je daleč največ v primerjavi z drugimi evropskimi vladnimi institucijami. Pri tem moramo izpostaviti pomembno dejstvo. Doslej so posamezne zvezne dežele in njihove podrejene institucije samostojno in neodvisno ena od druge od RIPE NCC dobivale naslovne bloke IPv4. To je pripeljalo do velike razdrobljenosti naslovnega prostora. Nova strategija je začrtala princip, da se pridobi velik naslovni prostor (/26), ki se bo v državi sistematično in glede na potrebe razdelil po piramidi od vrha do dna.

Pomembna gonilna sila pri uvajanju IPv6 v Nemčiji je Zvezni vladni urad za informacijsko tehnologijo (Die Beauftragte der Bundesregierung für Informationstechnik) in Nemški IPv6 Svet (Deutschen IPv6 Rat).

Nemški IPv6 Svet je bil ustanovljen leta 2007 pod vodstvom prof. Chistopha Meinela in Latifa Ladida. Ob ustanovitvi so si začrtali, da bo njihovo poslanstvo zagotavljanje tehničnega vodstva in inovacij, ki bo omogočilo uspešno uvedbo protokola IPv6 v vse sfere nemške omrežne in telekomunikacijske infrastrukture. Za dosego teh ciljev je Svet vzpostavil odprto platformo, ki združuje različne tehnične strokovnjake s področja IPv6.
Za pomemben mejnik se šteje 14. maj 2009 v času drugega nemškega vrha IPv6 (Deutsche IPv6-Gipfel), ko je bil objavljen Akcijski načrt za uvedbo IPv6 v Nemčiji (Nationaler IPv6-Aktionsplan für Deutschland). Akcijski načrt se tudi sovpada z leta 2008 objavljeno Širokopasovno strategijo zvezne vlade (Breitbandstrategie der Bundesregierung).

Akcijski načrt, ki ga je pripravil nemški IPv6 Council s koordinacijo mednarodnega IPv6 Foruma in Evropske komisije, vsebuje cilje ter identificira morebitne vrzeli, priložnosti in konkretne ukrepe, ki bodo omogočili uspešno uvedbo IPv6 v Nemčiji. Namenjen je širokemu krogu deležnikom: politikom, javni administraciji, šolstvu in raziskovalcem, zasebnemu sektorju in drugim zainteresiranim. Dokument opisuje potrebne dejavnosti na področju javnega obveščanja, izmenjave znanja, izobraževanja, raziskovanja in koordinacije med vsemi zainteresiranimi partnerji. Predlaga tudi konkretne ukrepe, ki se redno posodabljajo in razširjajo v skladu s trenutnim stanjem razvoja.

Kot je zapisano v akcijskem načrtu, se mora Nemčija kot vodilna izvozno naravnana država zavedati, da se mora povezovati z drugimi regijami in obenem slediti napredku tehnologije. Pri tem še posebej izpostavlja hitro razvijajočo se Kitajsko. Če bodo prehod na IPv6 prezrli, bo neizogibno prišlo do razpada obstoječega razvoja predvsem v Aziji kot najnaprednejši regiji. To bo imelo takojšen (negativni) učinek na ekonomijo in izvoz Nemčije. Prioritetna je zato pravočasna priprava na prihajajoče povpraševanje po IPv6 storitvah, aplikacijah in napravah. S kontinuiranim razvojem bodo dosegli varno in konkurenčno prednost na globalnem trgu. Z uvedbo IPv6 želijo zagrabiti priložnost in razumeti prehod kot začetek nove generacije interneta in omrežij. V tem kontekstu bi to stališče moralo prispeti do vseh zainteresiranih deležnikov, kot so: internetne organizacije, operaterji, ponudniki strojne opreme in operacijskih sistemov, ponudniki programskih aplikacij, raziskovalci in izobraževalne organizacije ter javna administracija na zvezni, državni in lokalni ravni. S prepoznavo deležnikov so tudi natančno konkretizirali njihove vloge, ki jih imajo pri prehodu na IPv6.

Nemški akcijski načrt sledi cilju Evropske komisije, da se do konca leta 2010 zagotovi vsaj 25 % uporabnikov dostop do interneta in storitev IPv6. V tem kontekstu Nemčija sledi trifaznemu načrtu za prehod, kot je opisan v RFC5211 (An Internet Transition Plan). V prvi (pripravljalni) fazi tega načrta, ki naj bi bil končan do decembra 2009, naj bi internetni ponudniki (ISP-ji) začeli testno uvajati posamezne omrežne storitve IPv6, organizacije, povezane v ta omrežja pa bi svoje internetne storitve omogočale tudi prek IPv6. V drugi

fazi (fazi prehoda) od januarja 2010 do decembra 2011 bi internetni ponudniki začeli svojim uporabnikom produkcijsko ponujati storitve IPv6 in IPv4, organizacije pa bi svoje storitve IPv6 ponujale v produkcijskem okolju. V tretji fazi (fazi po prehodu), ki naj bi potekala od januarja 2012 naprej, pa bi organizacije zagotavljale vse internetne storitve in povezljivost prek IPv6. Akcijski načrt v fazi prehoda predvideva souporabo obeh protokolov (IPv6 in IPv4).

Konkretne dejavnosti akcijskega načrta vključujejo tudi organizacijo vsakoletnega nemškega IPv6 Summita z mednarodnimi udeleženci. IPv6 Summit je bil prepoznan tudi kot dobra priložnost za izvedbo mednarodnega tekmovanja za izbor najbolj inovativnih aplikacij ali idej IPv6, ki pomagajo pri uveljavljanju in razvoju IPv6. Tekmovanje, ki poteka v Nemčiji od leta 2009, sponzorirajo s priznanimi sponzorji s področja raziskav, industrije in gospodarstva. Tekmovanje, ki je razdeljeno na tri kategorije, podeljuje prvo udeleženim finančne nagrade ali/in jim omogoča izpostavljeno predstavitev v okviru javnega obveščanja.Kot pomemben del osveščanja javnosti so priznali tudi izdajo publikacij v nacionalnih časopisih, popularnih znanstvenih revijah, obveščanje na radiu in televiziji.

Nemčija se zaveda, da je za dosego cilja potreben splošen konsenz in pripravljenost k delovanju vseh vpletenih na vseh ravneh družbe, predvsem pa med ekonomisti, politiki, v javni administraciji, med uporabniki, raziskovalci in akademiki.

Veliko moč pri osveščanju imajo politiki in javna administracija, ki bi morala spregovoriti javnosti o pomembnosti prehoda na IPv6. Omogočiti je treba dostop IPv6 do vseh javnih vladnih storitev (e-Government). Še posebej najbolj obiskane spletne strani vlade in javne uprave bi morale biti hitro dostopne tudi prek IPv6. Pri javnem naročanju novih vsebin ali storitev bi moral biti IPv6 obvezujoč uporabljen protokol. Obstoječe internetne storitve in storitve, ki se bodo posodabljale in nadgrajevale, morajo omogočiti dostop prek IPv6. Kot del cikla menjave opreme je treba zagotoviti, da bo nabavljena strojna in programska oprema podpirala IPv6. Pri oblikovanju vseh novih projektov mora biti IPv6 sestavni del tehničnih zahtev. Javna administracija, operaterji omrežij, prodajalci strojne in programske opreme ter razvijalci operacijskih sistemov morajo zagotoviti varnost in zasebnost IT.

Raziskovalni projekti, ki so financirani z javnimi ali evropskimi sredstvi, bi morali čim prej izkoristiti potencial, ki ga ima IPv6. Vsaka izobraževalna ali znanstvena institucija bi morala svoje spletne strani in storitve ponuditi tudi prek dostopa IPv6. Kot del inovacijskega cikla je treba zagotoviti, da je vsa strojna in programska oprema pripravljena na IPv6. Univerze in raziskovalne institucije bi morale biti multiplikator in voditi v nove oblike storitev, ki temeljijo na razvoju tehnologije IPv6.

Vsi ponudniki vsebin, storitev in operaterji omrežij bi morali izkazati pripravljenost, da izvedejo potrebne prilagoditve tehnologije, ki bi omogočile nacionalni prehod na IPv6. Infrastruktura za končne uporabnike bi morala biti skladna z IPv6. Še posebej najbolj

obiskane spletne strani zasebnega sektorja morajo biti takoj dostopne tudi prek protokola IPv6. Raziskati je treba možnosti za razvoj novih inovativnih izdelkov in rešitev IPv6, še posebej na področju varnosti IT.

Zvezni urad za informacijsko varnost (BSI – Bundesamt für Sicherheit in der Informationstechnik) je v letu 2009 izdal »Priporočilo za varno omrežno infrastrukturo IPv6«. V priporočilu so obravnavana varnostna tveganja, ki jih prinaša prehod na IPv6. V istem letu so se začeli projekti prehoda in posodobitve komunikacijske infrastrukture, pri katerih so sodelovale skoraj vse javne institucije. Nemška povezana infrastruktura (DOI – Deutschland-Online Infrastruktur), ki je glavna komunikacijska infrastruktura zvezne vlade, že popolnoma podpira IPv6 (deluje v dvojnem skladu). Nemčija pospešeno uvaja IPv6 tudi v drugi državni komunikacijski infrastrukturi. Testno preverjajo omrežne varnostne naprave ter naprave za šifriranje prometa. V načrtovanju je splošno omrežje za zvezno administracijo (NdB – Netze des Bundes). V fazi načrtovanja je razporeditev dodeljenega naslovnega prostora. Prve naslovne bloke IPv6 bodo dodelili zveznim državam (DOI), vključno s ponudniki storitev IT, in Ministrstvu za obrambo. V fazi procesa je organizacijski koncept. V pripravi so priporočila za prehod in operativno delovanje, konfiguracijski kontrolni seznam in naslovne predloge. Začeli so z različni pilotskimi programi, kot je VoIP prek IPv6 (VoIP Dataport/Hamburg s 150.000 napravami VoIP), testnimi omrežji DOI za transport in storitve, kot so elektronska pošta, DNS, omrežna varnost in kodirne naprave. Opravljena je bila študija izvedljivosti in stroškov prenove spletnih strani (www.cio.bund.de). Trenutno so spletne strani v testnem okolju.

V izvajanju ali pripravi je več projektov, ki se nanašajo na uvedbo IPv6 (Schülting 2010). Cilj projekta IPv6 Profile je predpisati nabor potrebnih funkcionalnosti, ki jih mora izpolnjevati omrežna oprema, da bo skladna z IPv6. Projekt izvajajo DOI in FHG, BMI (Zvezno ministrstvo za notranje zadeve) pa delno sofinancira projekt. Pripravljena bodo priporočila, ki bodo v pomoč administraciji pri nakupu opreme, in podan bo vpliv na javno infrastrukturo IT.

V testnem okolju se preizkušajo storitve, kot so: nadzor omrežja, mobilnost, multicast na IPv6. Izvajajo se testi združljivostiin testi medsebojnega obratovanja. V pripravi so migracijska orodja za spletne vladne aplikacije (e-Government). V pripravi je migracijski vodnik za občine. Na področju varnosti IPv6 se pripravljajo priporočila za varno komunikacijo od konca do konca, zamenjava NAT in zahteve za naprave za omrežno varnost.

Nemčija je aktivno, sistematično in z močno podporo zvezne vlade pristopila k uvedbi IPv6. Čeprav je tudi pri njih čutiti zmanjševanje povpraševanja zaradi globalne recesije, kljub vsemu ni zmanjšala proračuna za infrastrukturo in opremo IKT. Njihov proračun na zvezni ravni za opremo IKT je celih 500 milijonov evrov. V okviru teh sredstev je njihov cilj

okrepiti sektor IKT in pospešiti posodabljanje na ravni vseh zveznih administracij. Do leta 2011 so si zastavili 360 prioritetnih ciljev in meril, s katerimi bodo na zvezni infrastrukturi IT izboljšali varnost IT ter obenem zmanjšali vpliv na okolje.

Viri:

Bundesministerium fur Wirtschaft und Technologie (2009): *Darmstadt Declaration, The Third National IT Summit: Shaping the Digital Future in Germany*: http://www.bioin.or.kr/upload.do?cmd=download&seq=8719&bid=policy

IPv6 German Council (2009): http://www.ipv6council.de
Nacionalni IPv6 akcijski načrt za Nemčijo:
http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf

Bürger, C. (2009): *IPv6 in Germany*,
http://www.ripe.net/ripe/meetings/ripe-59/presentations/buerger-german-govt-v6-update.pdf

Schülting, H.W. (2010): *Status of IPv6 in Germany*,
http://ec.europa.eu/information_society/policy/ipv6/events/april2010/germany.ppt

Danska

Tudi danska vlada je po predlogu Evropske komisije v svoji državi prevzela pobudo pri uvajanju IPv6. Je v vlogi vmesnega člena, posrednika med vsemi zainteresiranimi deležniki, ponudniki omrežij, storitev in uporabniki. Njihovo Ministrstvo za znanost, tehnologijo in inovacije je leta 2009 za dansko vlado pripravilo strategijo uvajanja IPv6. Iz akcijskega načrta izhaja, da je uvajanje IPv6 pomembno tako za javni kot za zasebni sektor, zato se mora izvajati kot model javno-zasebnega partnerstva. Model partnerstva z zagotavljanjem dobrega temelja in koordiniranjem specifičnih dejavnosti med deležniki in omenjenim ministrstvom še krepi te učinke.

Tudi njihov akcijski načrt predlaga danski vladi, da bi morala biti vodilna in odločnejša pri vlaganjih v infrastrukturo, še posebej pri prehodu na IPv6. V politiki javnega naročanja strojne, programske in omrežne opreme bi morala postaviti jasne zahteve po podpori IPv6. Infrastruktura je v lasti zasebnega sektorja in razvoj strojne in programske opreme in omrežij temelji na osnovi trga in konkurence. Za razvoj je ključno, da se v prehod na IPv6 vključijo internetni ponudniki in lastniki infrastrukture, tipično velika telekomunikacijska podjetja. Tovrstno partnerstvo bi moralo vključevati vse akterje, na katere vpliva prehod na IPv6: predstavnike vlade, registrarja domen .dk, internetne ponudnike, dobavitelje strojne in programske opreme ter druge zainteresirane organizacije. Ministrstvo za znanost je zainteresirane partnerje povabilo, da se vzpostavi center znanja, namenjen vsem, ki se ukvarjajo s problematiko IPv6. Center znanja, v katerem sodeluje tudi omenjeno ministrstvo, omogoča zainteresiranim vse potrebne informacije, ki se nanašajo na uvajanje in prehod na IPv6.

Ministrstvo za znanost je zadolžilo posebno pristojno skupino pod vodstvom danskega regulatorja elektronskih komunikacij NTA (Telestyrelsen – National Telecom Agency) da nadzira izvajanje prehoda na IPv6. NTA je tudi po danskem Zakonu o internetnih domenah[1] odgovoren za register domen .dk.

Danska vlada se zaveda, da je pomemben del tega procesa tudi združitev informacijskih moči, saj le na ta način lahko zagotovi zadovoljiv in kontinuiran napredek. Vlada Danske tako vidi veliko sinergijskih učinkov, ki jih lahko doseže v povezavi z registrarjem domen .dk (NTA), še posebno na področjih, kot so:

- spremembe politike javnega naročanja,
- izzivi, ki jih prinašajo varnostne politike v času prehoda,
- mednarodni procesi in uvajanje IPv6.

Ciljna skupina za skupna prizadevanja je zelo široka z vidika zbiranja potrebnih informacij in z vidika potrebnih strokovnih kvalifikacij, potrebnih za njihovo razumevanje. Akcijski

načrt prednostno ločuje del, ki je usmerjen v stroko, in del, ki bi bil usmerjen k občanom in njihovem osveščanju.

V dokumentu ugotavljajo, da je prenos znanja predvsem pomemben na profesionalnem trgu, ki bo na eni strani uporabljal IPv6 za inovacije in razvoj izdelkov, ter za drugi segment, ki bo odgovoren za praktično implementacijo protokolov v podjetjih, pri internetnih ponudnikih in podobno.

Tudi državljane je treba seznaniti s prehodom, vendar v manjšem obsegu, kajti na večino prehod ne vpliva. Njihova pričakovanja kažejo, da bo prehodno obdobje dolgo. Prehod na nov protokol bo za državljane postopen, potekal bo sočasno z zamenjavo domače računalniške opreme. Državljani zato potrebujejo informacije bolj na splošni ravni, še posebej z vidika varnosti in povečanega tveganja napadov hekerjev zaradi sobivanja IPv4 in IPv6. Tudi pri tovrstnih dejavnostih posredovanja znanja sodeluje dansko Ministrstvo za znanost v sodelovanju z relevantnimi deležniki, vključenimi v model družabništva.

Spremenjena bo tudi politika javnega naročanja. Ministrstvo želi v okviru javnih naročil ustvariti trg z zadostno količino primernih izdelkov s primernimi cenami in podporo protokolu IPv6. S tem pristopom bo nova oprema vsebovala vse potrebne funkcionalnosti in zmogljivosti, ne glede na to, kdaj bo prišlo do končne odločitve o prehodu na nov protokol. Za zagotovitev skupne strategije in večjega tržnega obsega bo politika javnega naročanja koordinirana z lokalnimi in regionalnimi oblastmi, ki so pod okriljem danske vlade in danskih okrožij. Vladna politika javnega naročanja bo usklajena tako, da bodo naročila vsebovala minimalne zahteve po podpori IPv6 pri strojni in programski opremi ter na ravni storitev. Navedeni proces naročanja se je začel že konec leta 2008, ko je danski Urad za javna naročila Ministrstva za finance za vlado oddal prve razpise za nakup omrežnih naprav in komponent. Tudi vsi razpisi, ki jih objavlja danski regulator elektronskih komunikacij NTA v okviru upravljanja registra domen .dk, vključuje minimalne zahteve, pod katerimi mora sistem registra, vključno z domenskimi strežniki, podpirati IPv6. V skladu s Sporočilom Evropske Komisije (Akcijski načrt za uvedbo IPv6), navedena strategija in akcijski načrt do leta 2010 vključuje tudi zagotovitev dostopa vladnih spletnih strani prek IPv6.

Spremembe z uvajanjem IPv6 se izvajajo tudi pri preostali digitalizaciji Danske. IPv6 postaja obvezujoč odprti standard. Pri promociji uporabe IPv6 v javnem sektorju se bo sedanji status IPv6 iz »uporaben« spremenil v »priporočljiv«. Zrelejši kot bo trg z izdelki IPv6, večja bo zahteva po tem, da IPv6 postane obvezujoč protokol v omrežju javnega sektorja.

Danska vlada se tudi zaveda, da komunikacijska omrežja igrajo odločilno vlogo v primeru morebitnih kriznih dogodkih ali naravnih nesreč. Zmožnost prenosa informacij in

zagotavljanje koordinacije sta odvisno od dostopnosti ter od robustnih in varnih omrežij. Zato ima vlada posebno nalogo, ki zagotavlja, da so elektronske komunikacije, ki so življenjskega pomena za družbo, zaščitene v javno dostopnih omrežjih. V povezavi z upravljanjem registrom domen .dk je danska vlada danskemu regulatorju z izdano licenco že leta 2009 predpisala, da mora register domen poleg splošnih operacij naslovnega prostora IPv4 omogočati tudi upravljanje naslovnega prostora IPv6.

Danska vlada predvideva tudi, da se bodo operaterji javnih omrežij med seboj dogovorili, da bodo podobno kakor za sedanja javna fiksna in mobilna omrežja IPv4 tudi za omrežja IPv6 pripravili prioritizacijsko shemo. Ta bo v primeru naravnih nesreč ali drugih izrednih dogodkov omogočila ustrezno prioritizacijo prometa. Tovrstni med operaterski dogovor, ki temelji na prostovoljni bazi, bo omogočal prenos vitalnih podatkovnih komunikacij v najvišji prioritizaciji, kot jo lahko omogoča protokol IPv6.

Iz danskega časovnega načrta izvajanja dejanj izhaja, da bo proces od prvih razprav do prvega uvajanja IPv6 trajal najmanj dve leti. Z javnimi razpravami so začeli v tretji četrtini leta 2009, v prvi četrtini leta 2010 so začeli podrobno načrtovanje, prva uvajanja pa naj bi se zaključila konec prve polovice leta 2011.

Njihov akcijski načrt ne vključuje zanesljivih ocen celotnih nacionalnih stroškov, ki jih prinaša uvedba IPv6. Pričakujejo, da bodo letni stroški ostali na relativno nizki ravni, če so bo uvajanje IPv6 izvajalo postopoma skozi več let ob predhodnem načrtovanju. Pričakujejo, da bo prehod trajal vsaj deset let. Če bo prehod na IPv6 potekal postopoma, se lahko nadzoruje in načrtuje v okviru tekočih operativnih shem in shem posodabljanj opreme, zato lahko dodatni stroški za IPv6 postanejo integralni del operativnih stroškov posameznega deležnika.

Viri:
HØRINGSUDKAST (2009): Handlingsplan for implementering af IPv6 (http://di.dk/SiteCollectionDocuments/Foreningssites/itek.di.dk/Downloadboks/IPv6%20Handlingsplan_final.pdf)

HØRINGSUDKAST (2009): Statens strategi for overgang til IPv6 (https://www.borger.dk/Lovgivning/Hoeringsportalen/dl.aspx?hpid=19673)

Finska

Eden prvih pionirjev uvajanja IPv6 na Finskem je bil »CSC – IT Center of Science«, ki je pod upravljanjem finskega Ministrstva za izobraževanje, znanost in kulturo (Ministry of Education, Science and Culture). CSC upravlja hrbtenično omrežje Funet, ki omogoča povezljivost IPv6 za finska raziskovalna in izobraževalna omrežja, obenem pa tudi povezuje omrežje v panevropsko izobraževalno omrežje GÉANT2. CSC je v letih od 2002 do 2005 aktivno sodeloval pri projektu 6Net, ki ga je kot pilotski projekt IPv6 financirala Evropska skupnost. Kot kažejo raziskave, ki jih je lansko leto objavilo finsko Ministrstvo za transport in komunikacije, so finski operaterji dobro pripravljeni na prehod na IPv6. Na podlagi podatkov finskega združenja za izmenjavo internetnega prometa FICIX (Finnish Communication and Internet Exchange Association) od 10 od 28 članov že prenaša promet IPv6. Kljub vsemu le nekaj finskih operaterjev aktivno promovira usmerjanje IPv6 za komercialne namene.

Trenutno je le malo finskih podjetij, ki so pripravljena na prehod na IPv6. Razlog je predvsem finančne narave: potrebne so spremembe na usmerjevalnikih, stikalih, v aplikacijah in pri podatkovni varnosti. Na podlagi vprašalnika, ki ga je leta 2008 razposlal finski regulator elektronskih komunikacij Ficora dvestotim operaterjem, le en operater uporabnikom omogoča povezljivost IPv6.

CSC v okviru omrežja Funet aktivno promovira implementacijo IPv6. V letu 2009 je finski raziskovalec Teemu Kiviniemi v okviru magistrskega dela razvil pretvornik protokola za storitve multicast. Pretvornik je bil ob pomoči helsinške Univerze za tehnologije uspešno vgrajen v omrežje Funet. Z njegovo uporabo so storitve IPv6 multicast zdaj omogočene tudi uporabnikom s povezljivostjo IPv6.

Finsko Ministrstvo za transport in komunikacije bi zelo rado spodbudilo operaterje, da se še bolj pripravijo na IPv6. Pripravljajo projekt »National Information Society«, v katerem bo opredeljen časovni načrt uvedbe IPv6. Ministrstvo bo spodbujalo uvedbo IPv6 tudi tako, da bodo seznanili javnost z možnimi problemi prehoda. Vzpostaviti želijo norme, s katerimi bodo obvezali operaterje, da bodo vključili zahtevo po podpori IPv6 pri nabavi opreme. Tudi finski regulator Ficora se zavzema za IPv6 in spodbuja njegovo uvajanje. Leta 2009 je v svoji strategiji dela 2009–2015 (Ficora 2009) med operativne naloge tudi zapisal, da bo v sodelovanju s finskimi komunikacijskimi operaterji aktivno promoviral vpeljavo IPv6. Ficora se zavzema tudi za to, da bi začeli podeljevati logotip »IPv6 Ready« vsem potrošniškim komunikacijskim napravam, ki bi izpolnjevale potrebne funkcionalnosti IPv6. Temu predlogu so naklonjeni tudi nekateri operaterji, saj menijo, da je to lahko eden od možnih načinov spodbude za uvedbo IPv6 na Finskem.

Viri:

CSC (2010): *Slow progress in IPv6 implementation*, dosegljivo na: http://www.csc.fi/english/csc/publications/cscnews/2010/1/IPv6, obiskano dne 1.10.2010
Finnish IPv6 Task Force: http://www.fi.ipv6tf.org/

Ficora (2009): *THE STRATEGY OF THE FINNISH COMMUNICATIONS REGULATORY AUTHORITY 2009-2015*, dosegljivo na: http://www.ficora.fi/attachments/englantiav/strategy/5jyWB7NAG/DOHA_n561005_v1_Viestintaviraston_strategia_2009-2015_in_English.pdf, obiskano dne 15.10.2010

Češka

Češka je ena od najbolj aktivnih držav Evropske unije pri uvajanju DNSSEC. Po podatkih iz maja 2010 je že 15 % (~98.000) čeških domen podpisanih (Filip, O. (2010)). Manj uspeha imajo z uvajanjem IPv6, čeprav so že izvedli določene konkretne korake. Iz statistike (CZ.NIC 2010), ki jo vodi češki registrar CZ.NIC, lahko razberemo, da je v septembru 2010 3,61 % (25.752) strežnikov DNS, ki podpirajo zapis AAAA. Leto prej je bila ta vrednost skoraj 5-krat manjša. Še večji napredek je bil dosežen pri poštnih strežnikih, saj v septembru 2010 beležijo 5,7-krat večjo rast v primerjavi z letom poprej (43.713 ali 6,13 % poštnih strežnikov ima najmanj en zapis IPv6 MX). Opazen napredek je bil narejen tudi pri oglaševanju poti BGP s predpono IPv6. V letu 2009 je bilo prek BGP oglaševanih 29 avtonomnih sistemov ASN, v letošnjem septembru pa imajo že 56 ASN-jev s predpono IPv6. V primerjavi z IPv4, ki ima registriranih 535 sistemov ASN, je to še vedno zelo malo. Na izmenjevalni točki NIX.CZ je trenutno povezanih 99 organizacij s povezavo IPv4 ter 39 organizacij s povezavo IPv6 (Petr 2010). IPv6 peering prometa je manj kakor 90 Mbit/s v primerjavi z IPv4, ki ga je več kot 74 G bit/s. Povečuje se tudi število domen, ki so dosegljive izključno prek IPv6. Teh je trenutno 8. Češka ima dodeljenih 77 predpon IPv6 velikosti /32.

Po podatkih predstavnice češkega ministrstva za industrijo in trgovino elektronskih komunikacij, Monike Kunzove, je v juniju 2009 češka vlada sprejela resolucijo, ki zahteva od vseh ministrstev in drugih vladnih administracij, da morajo ob menjavi omrežne opreme to zamenjati z opremo, ki je združljiva z IPv6. Do 31. decembra 2010 morajo biti vse njihove spletne strani in javno dostopne storitve e-Government dostopne prek protokolov IPv4 in IPv6. Ob zadnji analizi, ki so jo opravili na pristojnem ministrstvu, se je pokazalo, da vse navedene institucije v celoti že izpolnjujejo prvi pogoj, drugi pa je v fazi izvajanja.

Viri:
Filip, O. (2010): DNSSEC.CZ, dosegljivo na: http://www.ripe.net/ripe/meetings/ripe-60/presentations/Filip-DNSSEC_in_CZ.pdf, obiskano dne 14.10.2010

CZ.NIC (2010): *IPv6 statistics*: dosegljivo na: http://labs.nic.cz/page/756/, obiskano dne 14.10.2010

Petr, E. (2010): *IPv6 v ČR,* dosegljivo na: http://www.nic.cz/public_media/IT10/prezentace/den_2_5_Petr.pdf, obiskano dne: 14.10.2010

Združene države Amerike

ZDA so se sistematično in na vladni ravni odločile, da bodo v določenih časovnih rokih uvedle IPv6 v svoje vladno komunikacijsko-informacijsko omrežje. Pravna podlaga za začetek uvajanja IPv6 v omrežjih zveznih vladnih agencij je memorandum »Transition Planning for Internet version 6 (IPv6)«, ki ga je leta 2005 izdal OMB (Office of Management and Budget). OMB, ki nadzoruje in usmerja delo vladnih agencij ZDA, je predpisal, da morajo vse zvezne agencije do junija 2008 v svojih hrbteničnih omrežjih začeti uporabljati IPv6 in se tudi s svojimi vmesniki povezati v omrežje IPv6. Listina opredeljuje konkretne časovne roke in zahteve, ki jih morajo zvezne vladne agencije izpolniti do navedenega datuma. Predpisane so bile naslednje dejavnosti:
Do 15. novembra 2005:

- določitev odgovorne osebe, ki bo vodila in koordinirala načrtovanje,
- popis vseh obstoječih usmerjevalnikov, stikal in strojnih požarnih pregrad (predpisana vsebina, ki jo mora zajemati popis),
- popis vseh drugih naprav in tehnologij skladnih z IP, ki niso bile zajete v prejšnjem popisu,
- začeti analizo finančnih in operativnih vplivov ter tveganj, ki so posledica prehoda na IPv6 (predpisana vsebina poročila).

Do februarja 2006:

- v skladu s priporočili, ki jih je izdal CIO Svet za arhitekturo in odbor za infrastrukturo (Chief Information Officers Council Architecture and Infrastructure Committee), začeti načrt prehoda na IPv6 (predpisane smernice potrebnih dejavnosti),
- predložiti poročilo o napredku pri popisu opreme in analizi vpliva prehoda na IPv6.

Do 30. junija 2006:

- celoten popis skladne opreme in tehnologije IP, ki ni bila zajeta v prvem popisu,
- celotna analiza finančnih in operativnih vplivov in tveganj.ž

Do 30. junija 2008:

- vsa infrastruktura agencij (hrbtenična omrežja) mora uporabljati IPv6 in agencije morajo biti z vmesniki povezane v to infrastrukturo. Agencije morajo na ta dan na skupnem sestanku poročati o napredku, ki je del njihove strategije prehoda.

Agencije so morale do junija 2008 izvesti najmanj navedene dejavnosti, pri čemer niso smele biti ogrožene funkcionalnosti ali omrežna varnost IPv4. Navedeni datum ni bil obvezujoč za prenos aplikacij, perifernih naprav ali drugih dobrin IT. Kot so poročali julija 2008 pri Federal Compur Week (Mosqure 2008), je večina agencij v roku izpolnila obveznosti memoranduma.

Memorandum agencijam nalaga, da morajo v prihodnje zagotoviti, da je vsa novo kupljena oprema IKT skladna z IPv6. Z IPv6 skladni izdelek ali sistem morata biti sposobna sprejeti, obdelati ali prenesti ali posredovati pakete IPv6 in morata biti združljiva z drugimi sistemi in protokoli v načinih IPv4 in IPv6.

Ameriški nacionalni inštitut za standarde in tehnologijo (NIST – The National Institute for Standards and Technology) je bil izbran, da razvije potrebne standarde, ki bodo zagotovili za vse vladne institucije poenoten sistem potrebnih specifikacij in način certificiranja. Ti so pri nabavi opreme IPv6 zavezujoči.
Memorandumu so sledili še drugi pomembni dokumenti. Med njimi bi izpostavili dokument iz januarja 2006, ki ga je izdalo ameriško Ministrstvo za trgovino (U.S. Department of Commerce) v sodelovanju z NIST in NTIA (National Telecommunications & Information Administration). Dokument »Tehnical and Economic Assessment of Internet Protocol, Version 6 (IPv6)« obravnava tehnične in ekonomske vplive, ki se nanašajo na uvajanje IPv6, vključno z vlogo vlade ZDA pri prehodu, mednarodno združljivostjo, varnostjo v prehodu, stroški in koristmi, ki jih prinaša IPv6. Študija ugotavlja, da IPv6 prinaša ameriškemu poslovanju in potrošnikom pomembne koristi, ki pa se bodo pokazale šele čez čas. Večina internetnih strokovnjakov in deležnikov industrije v splošnem soglaša, da bodo omrežja IPv6 tehnično boljša v primerjavi s sedanjimi omrežji IPv4. Večji naslovni prostor, ki ga prinaša IPv6, bo potencialno spodbudil veliko novih inovativnih komunikacijskih storitev in aplikacij. Čez čas bo IPv6 v primerjavi z IPv4 postal bolj uporaben in bolj prilagodljiv mehanizem za zagotavljanje uporabniške komunikacije od konca do konca. V študiji nadalje ugotavljajo, da hitro uvedbo IPv6 preprečujejo številne ovire. Med njimi je veliko trpežnih naprav in aplikacij, ki nam dobro služijo. Ker so skladne samo z IPv4, bi jih bilo treba zamenjati. Če želimo polno uresničiti potencial, ki ga prinašajo komunikacijske zmožnosti protokola IPv6, bo poleg tega treba imeti za prehod na IPv6 finančna sredstva in človeške vire.

Z ekonomskega vidika so lahko stroški prehoda nižji, če ga načrtujemo v okviru standardnega cikla menjave ali nadgradnje opreme. V okviru menjave opreme večino stroškov predstavlja predvsem izobraževanje osebja, nameščanje in konfiguriranje

opreme, omrežno testiranje, ne pa sam nakup opreme, pri katerem cena ne bo bistveno višja v primerjavi z opremo IPv4. Stroški prehoda se bodo razlikovali tudi za različne uporabniške skupine. Pri majhnih in srednje velikih podjetjih ter končnih (rezidenčnih) uporabnikih, ki ne upravljajo velikih omrežij, bo ta strošek relativno majhen in ga bo mogoče načrtovati v okviru standardne ciklične zamenjave opreme. V nasprotju z njimi bodo lahko imela velika podjetja (korporacije) in vladne agencije višje stroške, pri čemer je nihanje odvisno od obstoječe infrastrukture in operativne politike. To vključuje tudi aplikacije, ki jih bo treba spremeniti ali razviti na novo. Odvisno je tudi od tega, koliko se bodo uporabniki povezovali z drugimi organizacijami, ki uporabljajo IPv6. Aktiviranje IPv6 za rutinsko uporabo se lahko dejansko pojavi šele, ko bo dosežena kritična masa, ki bo zamenjana s tehnologijo IPv6. Rutinsko se bo prehod izvajal tudi, ko bodo izvedeni primerni operativni in varnostni načrti ter izdatna šolanja kadra.

Kot ugotavljajo, je največji potencial varnostnih koristi, ki jih prinaša protokol IPv6, povezan z dolgoročnim razvojem nove varnostne paradigme, ki je bistveno drugačna od zdaj uveljavljene v obstoječih omrežjih IPv4. Današnja omrežja temeljijo na varnostni arhitekturi perimetra, ki je osredotočen na omrežje (network centric), v prihodnje pa bodo omrežja temeljila na modelih od konca do konca (host-based), ki se bodo bolje prilagajali okolju. Potrebni čas in stroški, ki bodo potrebni za snovanje in razvoj novih varnostnih modelov, bodo precejšnji, vendar pa bo ustvarjanje novih, učinkovitejših varnostnih paradigm, v korist vsem trenutnim in prihodnjim internetnim uporabnikom.

Strokovnjaki se strinjajo, da uvedba novega protokola, kakršen je IPv6, v začetni fazi povečuje grožnje in varnostno ranljivost informacijskih sistemov. Potrebni bodo dodatni viri, ki se bodo lahko ukvarjali z grožnjami dvojnega okolja (IPv4 in IPv6). Ker je IPv6 že del protokolnega sklada marsikatere strojne ali programske opreme, je zelo verjetno, da se bo IPv6 pojavil v operativnih omrežjih brez vednosti (nepoučenih) upraviteljev omrežja in neodvisno od načrtov organizacij. Zato bi morale vse organizacije razviti potrebne varnostne načrte in politike, ki bi se ukvarjale s prometom IPv6 ne glede na njihovo odločitev, ali in kdaj bodo izvedle prehod na IPv6. Čeprav so bili mehanizmi prehoda skrbno načrtovani za različne scenarije, delovanje v načinu dvojnega sklada povečuje varnostno tveganje.

Delovna skupina, ki je pripravljala omenjeno analizo, je ugotovila tudi, da na trgu ni večjih ovir, ki bi industriji preprečevale vlaganje v izdelke in storitve IPv6, in to ne glede na njene potrebe ali potrošniško povpraševanje. Zato ni utemeljenih razlogov in potreb, da bi ameriška vlada z agresivnimi ukrepi proti zasebnemu sektorju pospešila uvedbo IPv6. Zasebni sektor bo moral v bližnji prihodnosti izvesti skrbno analizo svojih poslovnih načrtov za posvojitev IPv6. S tem se bodo soočili tudi z neizogibnim pojavom prometa IPv6 v notranjem in zunanjem delu omrežja. Ob upoštevanju informacijskega sistema javnega sektorja avtorji študije priporočajo, da vladne agencije začnejo analizirati poslovne načrte za uvedbo IPv6 ter da razvijejo ustrezne varnostne načrte. Ker to prinaša določene

stroške, priporočila poudarjajo, da je potrebno skrbno načrtovanje, razvijanje in vrednotenje, ki mora imeti prednost pred specifičnimi odločitvami o uvedbi nove tehnologije IPv6 v operativno omrežje. Rezultati predstavljene študije so namreč pokazali, da obstajajo tehtna tehnična in ekonomska tveganja, ki so lahko povezana s pomanjkanjem ustreznega načrta in strategije uvedbe IPv6.

V februarju 2006 je zvezni CIO Council in odbor za infrastrukturo v pomoč zveznim agencijam pri prehodu na IPv6 v skladu z navodili memoranduma izdal še priporočila za prehod (Federal CIO Council Architecture and Infrastructure Commite 2006). Gre pravzaprav za skupek treh poglavij, ki so nastala kmalu po objavi memoranduma. Končni dokument vsebuje tri poglavja, vključno s pripombami agencij. Prvo poglavje opisuje navodila za prehod IPv6 v podjetjih s podjetniško infrastrukturo. Drugo poglavje obravnava bolj tehnične elemente, ki so pomembni pri prehodu agencij. V tem poglavju so zbrane najboljše prakse prehoda na IPv6. Podane so informacije, ki se nanašajo na omrežje in infrastrukturo, naslavljanje, zagotavljanje informacij, pilotske postavitve, testiranje in predstavitve, aplikacije, standarde in izobraževanje. Tretje poglavje govori o upravljanju IPv6 prehoda. Opisuje strukturo menedžmenta in posamezne vloge ter odgovornosti udeleženih agencij in organizacij.

Leta 2008 je NIST v skladu z zahtevami memoranduma objavil končno različico priporočil oziroma zahtev in postopkov, na podlagi katerih lahko posamezna oprema IKT dobi status skladnost z IPv6 ter oznako možnega sobivanja z IPv4. Publikacija z naslovom »A profile for IPv6 in the U.S. Governement (USG IPv6 Profile)« je dokument, v katerem so navedene minimalne operativne tehnične zahteve, ki jih morajo podpirati omrežne naprave, kot so gostitelji, usmerjevalniki, sistemi za preprečevanja vdorov (IDS) in požarne pregrade. Profil je bil razvit v pomoč zveznim agencijam pri njihovih načrtih razvoja, nabavi in implementiranju z IPv6 skladne opreme in obenem zato, da zagotovi združljivost in varnost informacijskih sistemov. Kot je bilo v dokumentu uvodoma navedeno, je trenutno na trgu še vedno množica opreme IPv6, ki je na različni zrelostni ravni in daleč od popolnosti. S pripravo profila so začrtali učinkovite de facto standarde popolnosti in pravilnosti, ki bo pomagal zavarovati naložbo zgodnjim uvajalcem IPv6. Profil ni samo uporaben na krajši rok, temveč zasleduje strateški dolgoročni načrt ZDA pri uvajanju tehnologije IPv6.

Vsaka naprava, ki dobi oznako združljivosti oziroma sposobnosti delovanja z IPv6, mora prestati strogo testiranje in certificiranje pri akreditiranih testnih laboratorijih in akreditacijskih telesih, ki izpolnjujejo standard ISO 17025 (General Requirements for the Competence of Testing and Calibration Laboratories). V ta namen je NIST pripravil dokument, ki natančno določa testne metode in način validacije (SP 500-273 Guidance on IPv6 Test Methods and Validation). Po uspešnem testiranju in certificiranju se oprema izdelovalcev vpiše v seznam APL (Approved Parts List) z IPv6 združljivih izdelkov

(http://jitc.fhu.disa.mil/apl/ipv6.htm), ki zagotavljajo združljivost s predpisanimi tehničnimi specifikacijami (RFC-ji).

Tudi ameriško Ministrstvo za obrambo (DoD – Department of Defence) je pripravilo podrobno specifikacijo zahtev in tehničnih standardov, ki jo mora izpolnjevati za IPv6 sposobna (IPv6 Capable) programska in strojna oprema (DoD IPv6 Standard Profiles For IPv6 Capable Products). Dokument, ki se redno posodablja, ima podobne zahteve kakor USG IPv6 Profile. Trenutno zadnja, peta različica je bila izdana julija 2010 in je namenjena širokemu krogu deležnikov, kot so: pristojni za nabavo opreme, organizacije, ki se ukvarjajo s testiranjem, obrambni razvijalci in prodajalci opreme. Tudi za IPv6 sposobna oprema mora prestati strogi testiranje, ki se v primeru ustrezne skladnosti zaključi s certifikacijo ameriške vojaške organizacije JITC (Joint Interoperability Test Command). Vsa komunikacijska oprema, ki jo nabavlja in uporablja ameriška vojska, mora biti skladna z omenjenim dokumentom in jo mora testirati in certificirati JITC. JITC opravlja testiranja in certificiranja opreme za vse izdelke vključno s funkcionalnostjo prenosa govora, podatkov in videa. Trenutno še poteka razprava med NIST in Ministrstvom za obrambo v zvezi s programom testiranja, vendar ni bistvenih razlik med funkcionalnimi zahtevami. Zelo verjetno je, da so izdelki, ki jih odobri en program, združljivi z izdelki, ki jih odobri drugi (pisci obeh dokumentov med seboj sodelujejo).

Svet Informacijskih direktorjev (CIO Council) je za potrebe ameriške vlade in agencij za prehod na IPv6 pripravil še dva dokumenta. Prvi dokument iz decembra 2008 (The Business Case and Roadmap for Completing IPv6 Adoption in US Government) je ostal v fazi osnutka in ga je nadomestil maja 2009 izdani dokument Planning Guide/Roadmap Toward IPv6 Adoption within the US Government. Dokument je namenjen direktorjem informatike, arhitektom omrežne infrastrukture in drugim posameznikom v zveznih agencijah, ki so odgovorni za uporabljanje informacijske tehnologije. Namen dokumenta je bilo poglobiti razumevanje vizije zvezne vlade pri uvedbi IPv6 in zagotoviti vsem agencijam specifične usmeritve, ki bodo omogočile uspešno prilagoditev tega protokola. Na podlagi informacij, zajetih v tem dokumentu, bodo direktorji informatike lažje prepoznali in razvili poslovne načrte, ki vključujejo uporabo IPv6. Dokument temelji na že omenjenem memorandumu, ki zahteva, da so zvezne agencije »v stanju uporabe IPv6« (*to be IPv6 State*). Dokument podaja pregled, kako prehod na IPv6 vpliva na arhitekturo podjetij ter na načrtovanje kapitala, investicij in nadzor. Direktorjem daje praktične usmeritve in splošne mejnike, ki jim lahko olajšajo uvedbo omrežnih storitev IPv6. Poda opis, kako prehod vpliva na zvezne pobude, kot so Varne internetne povezave (TIC – Trusted Internet Connections) in Predsedniška direktiva o domovinski varnosti (HSPD – Homeland Security Presidental Directive). Vsebuje tudi jasno umeščanje protokola IPv6 kot integralnega okvirja in organizacijske principe za zvezno infrastrukturo IT naslednje generacije. Čeprav je dokument namenjen predvsem zveznim agencijam in njihovemu osebju, je dokument dobro izhodišče za vse direktorje informatike in tehnično osebje v podjetjih.

ZDA imajo po podatkih SixXS 9 ponudnikov, ki omogočajo domorodno povezljivost IPv6 za svoje uporabnike. Med večjimi podjetji in internetnimi ponudniki, ki so IPv6 že uvedli ali ga imajo skoraj v produkciji, bi izpostavili: Comcast (največji kabelski operater v ZDA), Google, Verizon (operater za poslovne uporabnike in vladne institucije), AT&T, Sprint (telekomunikacijski ponudnik vlade ZDA), Hurricane Electric (globalni internetni ponudnik dostopa), Microsoft in še bi lahko naštevali.

ZDA so se lotili uvedbe protokola IPv6 na visoki profesionalni ravni. Glavni pobudnik uvajanja IPv6 ni bil zasebni sektor, temveč zvezna ameriška vlada. Z zahtevami v memorandumu je vlada postavila vsem zveznim agencijam mejnike in smernice za prehod na IPv6. Z nastankom NIST-ovega dokumenta USG IPv6 Profile ter dokumenta IPv6 Capable Products, ki ga je izdalo Ministrstvo za obrambo, je postavila temeljne minimalne tehnične standarde skladnosti in sposobnosti IPv6, ki se jih zdaj držijo vsi glavni izdelovalci opreme IKT. Z dokumentom Planning Guide/Roadmap Toward IPv6 Adoption within the US Government so postavili vsem zveznim agencijam in tudi drugim smernice za prihodnji razvoj in uvajanje IPv6.

ZDA so zato lahko primer dobre prakse, katerih smernice in izkušnje bi morali uporabiti tudi pri nas v Sloveniji.

Viri:

Executive Office of the President (2005): Transition Planning for Internet Protocol Version 6 (IPv6), http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf

U.S. Department of Commerce, NIST, NTIA (2006): Tehnical and Economic Assessment of Internet Protocol, Version 6 (IPv6): http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/IPv6final.pdf

Federal CIO Council Architecture and Infrastructure Commite (2006): IPv6 Transition Guidance, http://www.cio.gov/Documents/IPv6_Transition_Guidance.doc

Mosqure, M. (2008): OMB: Agencies met IPv6 deadline, dosegljivo na: http://fcw.com/articles/2008/07/01/omb-agencies-met-ipv6-deadline.aspx, obiskano dne 1.10.2010

NIST (2008): A profile for IPv6 in the U.S.Governement – Version 1: http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

Department of Defence (2010): IPv6 Standard Profiles For IPv6 Capable Products, http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf

CIO Council (2008): The Business Case and Roadmap for Completing IPv6 Adoption in US Government, http://osrin.net/docs/DRAFT_Business_Case_&_Roadmap_for_Completing_IPv6_Adoption_in_USG_12242008.pdf

CIO Council (2009*)*: Planning Guide/Roadmap Toward IPv6 Adoption within the US Government, http://www.ipv6council.de/fileadmin/documents/Planning_GuideRoadmap_Toward_IPv6_Adoptionin_USG_May_2009_final1.pdf

Network world (2010): http://www.networkworld.com/news/2010/040610-verizon-ipv6.html

IPv6 (Sprint&IPv6): http://www.networkworld.com/news/2010/040610-verizon-ipv6.html

AT&T and IPv6: http://www.corp.att.com/gov/solution/network_services/data_nw/ipv6/

Verizon: http://www.verizonbusiness.com/fi/products/internet/ipv6/

Japonska

Japonska je tehnološko ena najbolj razvitih držav sveta. Korporacija Sony je npr. že leta 2003 oznanila, da bodo vsi njeni izdelki po letu 2005 podpirali protokol IPv6 (IPv6Style, 2003). Japonska kot tehnološka velesila je prišla do spoznanja, da proces gradnje ali nadgradnje obstoječih omrežij na IPv6, posledično prinaša tudi priložnost za hitrejši razvoj in uveljavitev njene industrije izdelovalcev omrežne opreme na globalnem trgu. Japonska je ena od prvih azijskih (če ne celo širše) držav, ki so prevzele vodstvo pri uvajanju IPv6. Septembra 2000 je Japonska kot prva vlada na svetu objavila nacionalno strategijo uvedbe IPv6 (Popoviciu, Grossetete, 2006). Gre za vladno dolgoročno strategijo širokopasovnega razvoja na Japonskem, imenovano »u-Japan« (Ubiquitous Japan). S strategijo so se zavezali, da bodo IPv6 uvedli do leta 2005. Sočasno je bil vzpostavljen IPv6 Promotion Council, ki predstavlja vezni člen med vlado, industrijo in raziskovalnimi organizacijami in skrbi za uresničitev ciljev, zastavljenih z omenjeno strategijo u-Japan. S projektom WIDE (Widely Integrated Distributed Environment) so akademskim institucijam zagotovili podporo pri razvoju novih aplikacij IPv6, organizacijam, ki so bodo odločale za uvedbo IPv6, pa so namenili davčne olajšave. V istem letu je podjetje NTT Communications vzpostavilo prvi komercialni domorodni dostop IPv6 do hrbteničnega omrežja NTT (NTT Communications 2001). Leta 2002 so objavili, da sta evropski IPv6 Task Force in japonski IPv6 Promotion Council podpisala strateško zavezništvo pri uvajanju IPv6 (IPv6 Task Force 2002). V letu 2002 so večji internetni ponudniki že začeli s prvimi storitvami IPv6 (Kosuke 2002). NTT je začek ponujati dostop IPv6/IPv4 prek ADSL (NTT Communications 2001). V istem letu so testna okolja začeli vzpostavljati ponudniki

terminalov (senzorji, spletne kamere, domače naprave) in ponudniki storitev (internet v vozilih, vlakih, medicina, spletne igre). Začele so se pojavljati že prve testne storitve za mobilno telefonijo. Ponudniki (domačih) usmerjevalnikov so začeli ponujati svoje izdelke (Hitachi, Fujitsu, NEC, Furakawa Electric). Zaradi osveščanja so pripravili poseben razstavni prostor, na katerem so razstavljali različne inteligentne domače naprave, ki so omogočale povezljivost v IPv6 (hladilnik, mikrovalovna pečica, digitalne in spletne kamere, TV, internetni terminal, ki kombinira oznako RFID in tehnologijo Mobile IPv6). V okviru ozaveščanja so začeli izdajati posebne publikacije (IPv6 Magazine), v katerih strokovnjaki pišejo o novih tehničnih standardih, storitvah, izdelkih in dejavnostih s področja IPv6. Vzpostavljene so bile različne spletne strani, namenjene promoviranju, na katerih so predstavljene tehnologija IPv6 in prednosti, ki jih prinaša (npr. http://v6start.net).

Leta 2008 je bila vzpostavljena skupina Task Force for IPv4 Exhaustion, v katero je vključenih 22 organizacij, ki so tako ali drugače povezane z internetom. Skupina rešuje probleme s področja tehnologije, obratovanja in upravljanja, pomaga pri izvajanju izobraževanj in delavnic ter osveščanju. Njihov cilj je z različnimi dejavnostmi zagotoviti gladko in pravočasno uvedbo IPv6.

Japonska je sprejela tudi program »IPv6 Forum Ready«, s katerim so začeli testirati združljivost naprav z IPv6. Na podlagi tega programa in podeljevanja logotipov IPv6 Ready je japonska industrija postala vodilna svetovna proizvajalka opreme IPv6.

Čeprav je Japonska relativno zgodaj začela z uvajanjem IPv6, njihove analize kažejo, da z uvajanjem IPv6 zamuja za od eno do dve leti (Mikawa, 2010).
Japonska vlaga v tehnološki trg IPv6 od 10 do 13 milijonov dolarjev letno. Kot ocenjuje japonska vlada, ji bo to do konca leta 2010 prineslo celih 1,55 milijarde dolarjev.

Viri:
IPv6Style (2003): Sony In 2005, all Sony products will be IPv6-enabled, dosegljivo na: http://www.ipv6style.jp/en/interviews/20030212/index.shtml, obiskano dne 1.5.2010

Report. Study Group on Internet's. Smooth Transition to IPv6: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/080617_1.pdf

Mikawa, S. (2010): Capacity building for IPv6, predstavitev na Internet Governance Forumu 2010, Litva

Popoviciu, C.P., Grossetete, P. (2006): The role of National Strategies in maintaining Competitive Edge in Information and Communication Technologies, dosegljivo na http://www.iiisci.org/journal/CV$/sci/pdfs/P563955.pdf, obiskano dne 1.10.2010

Kosuke, I. (2002): IPv6 Deployment in Japan – the way we accomplish, dosegljivo na: http://www.eu.ipv6tf.org/PublicDocuments/v6TFII_v6PC_jp_kosuke.pdf, obiskano dne 12.9.2010

NTT Communications (2001): Actions of NTT Communications, dosegljivo na: http://www.ntt.com/ipv6_e/data/e_about_com.html, obiskano dne 1.10.2010

IPv6 Task Force (2002): *Euro IPv6 Task Force and IPv6 Promotion Council of Japan Forge Strategic Alliance to foster IPv6 deployment world-wide*, dosegljivo na: http://www.ipv6tf.org/PublicDocuments/TF-v6PCJointPressReleasev2_FINAL.pdf, obiskano dne 15.3.2010

IPv6 Council: http://www.v6pc.jp/en/index.phtml
Live E! project: http://www.live-e.org
IPv6-FIX: http://v6fix.net/

InternetCAR Project: http://www.sfc.wide.ad.jp/InternetCAR/

Kitajska

Kitajska je trenutno ena od najhitreje rastočih držav po rasti števila internetnih uporabnikov. Kot je poročal Reuters v začetku leta 2010, naj bi Kitajska imela do konca leta 2010 384 milijonov internetnih uporabnikov. V zadnjih letih je bila zelo produktivna, saj je dohitela razvoj, ki je pri nekaterih drugih državah trajal desetletja. Kitajska je sprejela odločitev o uvedbi IPv6 z vzpostavitvijo programa China Next Generation Internet (CNGI). Kot ocenjujejo, je bil program uspešen, ker so ga podprle vladne institucije in glavni telekomunikacijski operaterji hrbteničnih omrežij. Ker velik delež internetnih uporabnikov predstavljajo mobilni uporabniki, so že na začetku projekta umestili v program podporo protokolu Mobile IPv6. Glavna motivacija uvedbe IPv6 v okviru projekta CNGI je bila predvsem večja učinkovitost omrežja, varnost od konca do konca ter možnost povečanega sodelovanja s tujimi vladami, predvsem z Evropsko unijo in Japonsko (Tezel 2010).

Pred uvedbo tega programa je Kitajska pri tehnološkem razvoju komunikacijske infrastrukture za od 10 do 20 let zaostajala v primerjavi z drugimi primerljivimi državami. V okviru petletnega CNGI projekta, ki ga je sprožila kitajska vlada, je bilo zgrajeno eno od največjih komercialnih hrbteničnih omrežij IPv6 naslednje generacije. V programu s proračunom, visokim 170 milijonov dolarjev, je bilo do leta 2009 zgrajenih šest nacionalnih hrbteničnih omrežij. Pet komercialnih (China Telecom, China Netcom, China Mobile, China Unicom, China Railcom) in eno akademsko (CERNET2). Z 39 deset gigabitnimi vstopnimi točkami – vozlišči (PoP) so povezali 40 največjih mest in več kakor 300 akademskih, industrijskih in vladno-razvojnih kampusov. CERNET2, ki predstavlja hrbtenico CNGI, je s 25 vozlišči PoP v dvajsetih mestih trenutno eno največjih izobraževalno-raziskovalnih

omrežij, ki v celoti temelji samo na protokolu IPv6 (v omrežju nimajo IPv4). V omrežju uporabljajo opremo različnih dobaviteljev. Pri prehodu si pomagajo z mehanizmi, kot so IPv4 over IPv6 (IETF softwire) in IVI (IETF).

Ena od večjih javnih predstavitev rezultatov projekta CNGI in infrastrukture IPv6 je bila tudi izvedba olimpijskih iger v Pekingu leta 2008. Komunikacijska infrastruktura olimpijskih iger z vsemi podatkovnimi povezavami, pa tudi vse omrežne širokopasovne in mobilne aplikacije in naprave, ki so bile uporabljene na olimpijadi, so temeljile na protokolu IPv6. Dogodek je bil zelo odmeven, saj je bil primer dobre prakse, prve velike implementacije produkcijske infrastrukture IPv6.

Leta 2009 je Telecom China uradno objavil svoje načrte za uvedbo IPv6 (Digaria, 2009). V začetni fazi, ki bo potekala do leta 2011, bodo začrtali in vzpostavili novo platformo na poslovni in omrežni ravni, ki bo omogočala poslovanje prek IPv6. V letih 2012-2015 bo prišlo do prve faze komercializacije. V tej fazi načrtujejo sobivanje IPv6 in IPv4, uvedbo novih aplikacij ter postopen prenos poslovanja na IPv6. Po letu 2015 pričakujejo popolno komercializacijo uporabe IPv6. Nove aplikacije bodo temeljile pretežno na IPv6, omrežja in poslovanje, ki temeljijo na IPv4, pa bodo postopno ukinili (do leta 2015).

Viri:
Cnet (2004): *China launches largest IPv6 network*, dosegljivo na: http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html, obiskano dne 10.10.2010

Reuters (2010):*China Internet population hits 384 million*, dosegljivo na: http://www.reuters.com/article/idUSTOE60E06S20100115, obiskano dne 4.10.2010

Wikipedia: *China Next Generation Internet*, http://en.wikipedia.org/wiki/China_Next_Generation_Internet, obiskano dne 4.10.2010

Tezel, O. (2009): *State of IPv6 in China*, dosegljivo na: http://www.ipv6.org.au/09ipv6summit/talks/OrcunTezel.pdf, obiskano dne 3.10.2010

Digaria (2009): *China Telecom Officially Announce Commercial IPv6*, dosegljivo na: http://digaria.com/postings/b6f3742ce62ac02a8a63d0dd0c7b55da, obiskano dne: 17.10.2010

Koreja

Veliko dejavnosti poteka tudi na korejskem polotoku. Projekt KOREAv6 so sestavljala poskusna delovanja storitev IPv6 in preizkušanja opreme IPv6 pri uporabnikih. Začeli so ga izvajati leta 2004. Cilji projekta so bili:

- ustvariti poslovanje »IPv6 Ready» v podjetjih v javnem in zasebnem sektorju,
- pospešiti komercializacijo opreme IPv6,
- spodbuditi ozaveščanje javnosti o IPv6.

Izvajanje projekta so razdelili na več faz:

I. faza se je začela 2004 in je zajemala gradnjo omrežja IPv6 po vsej državi za ponujanje storitev, kot so VoDv6, VoIPv6, storitve internetnih prehodov in preizkušanje različne opreme IPv6, kot so usmerjevalniki, stikala, oprema VPN;

II. faza se je nadaljevala naslednje leto in je zajemala uporabo tehnologije IPv6 za nekaj najpomembnejših storitev, določenih v IT839, ki je strategija IT korejske vlade. Storitve so internetni dostop WiBro (Wireless Broadband), storitve VoIP in širitev lokalnih omrežij v javni sektor ter hkratni prehod obstoječih spletnih portalov in aplikacij IPv4 v portale IPv6;

III. faza je bila zadnja faza projekta, ki se je zaključil leta 2006. Zajemala je vzpostavitev obsežnih omrežij za omogočanje storitev IPv6, kot je na primer VoIPv6 vsem uporabnikom, in podporo vsebinam IPv6 na omrežjih WiBro. Spodbuditi želijo množično uporabo internetnih storitev IPv6 v javnem sektorju.

Korejska vlada namerava doseči popoln prehod na IPv6 v javnem sektorju in doseči 10 milijonov uporabnikov IPv6 do leta 2011. Naslednja mejnika v akcijskem načrtu korejske vlade sta bila:

- popoln prehod v hrbteničnih omrežja do leta 2010,
- prehod dostopovnih omrežij ISP do leta 2013.

Korejski akcijski načrt teče uspešno, vendar jim vseh ciljev v zadanih časovnih terminih ne bo uspelo doseči. Po zadnjih javnih objavah bodo prehod hrbteničnih omrežij v celoti dokončali do konca leta 2010.

Viri:
IPv6 Forum Korea, dosegljivo na: http://www.ipv6.or.kr/eng/index.html, obiskano dne 15.10.2010

IPv6.com Inc., dosegljivo na: http://www.ipv6.com/articles/deployment/IPv6-Deployment-Status.htm, obiskano dne 11.10.2010

3. Analiza ekonomske dimenzije (ločeno za javni in zasebni sektor)

The transition to IPv6 is inevitable. However, we live still in a finically oriented world. It is absolutely crucial to understand what the economic impact of IPv6 will be. What challenges are companies facing?

Section 3 provides a solid analysis of advantages, disadvantages and opportunities of IPv6 in a business world. It shines light on the commercial aspects of the various players. This includes not only large businesses and governments, but also the residential end-users.
It is hard to present a good study about the economic impact, but this section is written by experts and I my understanding does not differ very much from what is being said. Every company, however, is different and so the analysis has to remain at a somewhat high-level.

Uvedba kakršnekoli novosti v informacijski oziroma komunikacijski sistem mora biti ekonomsko oziroma tehnološko upravičena. Z drugimi besedami to pomeni, da morajo želene spremembe prinesti nižje stroške upravljanja in razvoja sistema oziroma njegovo učinkovitejše, zanesljivejše in varnejše delovanje. Ključni problem, s katerim se že skoraj deset let srečujemo pri uvajanju protokola IPv6 v okolja ponudnikov internetnega dostopa (Internet Service Provider), ponudnikov vsebin (Content providers) in poslovna okolja (Enterprises), so relativno omejene neposredne ekonomske in tehnološke prednosti, ki jih prinaša njegova uporaba. Da pa bi omenjene posledice za posamezne skupine uporabnikov bolje razumeli, poskusimo najprej podrobneje predstaviti prednosti, priložnosti, slabosti in nevarnosti (SWOT – Strengths, Weaknesses, Opportunities, Threats), ki jih lahko ima uvedba protokola IPv6, pri tem pa poskusimo poleg tehnoloških vidikov osvetliti tudi ekonomske.

Prednosti:

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

Priložnosti:

- možnost razvoja povsem novih in izboljšanih aplikacij in storitev (na primer takšnih, ki ne bodo slonele na modelu odjemalec/strežnik),
- možnost zmanjšanja stroškov razvoja aplikacij in storitev, saj bo z uporabo protokola IPv6 mogoče izvajanje nekaterih funkcionalnosti prepustiti omrežni

plasti (na primer skrb za zagotavljanje zasebnosti, celovitosti in istovetnosti podatkov bo mogoče vselej izvesti z uporabo protokolov AH in ESP, za katere podporo zahteva RFC-4294),

- možnost pravičnejše razdelitve naslovnega prostora lahko pripelje do zmanjšanja informacijske nepismenosti in digitalnega razkoraka (v tej luči gre mogoče razumeti tudi želje mednarodne zveze za telekomunikacije ITU, da bi nerazvitim državam pomagala pri pridobivanju IPv6 naslovnega prostora od regionalnih registrov (RiR)),
- možnost pospešenega zlivanja storitev zaradi podpore mobilnosti (terminalski),
- možnost uporabe omrežij M2M (na primer senzorskih omrežij ...).

Slabosti:

- protokola IPv4 in IPv6 med seboj nista neposredno združljiva, kar pomeni, da je treba uporabi nove različice internetnega protokola prilagoditi vso strojno in programsko opremo.
- ker je protokol IPv4 omogočil rast interneta iz raziskovalnega v globalno omrežje in se je izkazal kot precej prilagodljiv, je bila v nekaterih krogih znotraj internetne skupnosti kar nekaj časa prisotna skeptičnost glede smiselnosti njegove zamenjave.

Nevarnosti:

- nezdružljivost posameznih implementacij protokola IPv6 oziroma njihova pomanjkljiva podpora za posamezne funkcionalnosti lahko povzroči težave pri uvedbi,
- neizkušen in neustrezno izobražen kader lahko bistveno podaljša uvedbo in poviša njene stroške, hkrati pa poveča tveganje z vidika varnosti,
- neustrezno izobražen in motiviran kader lahko predstavlja ključno oviro pri uvajanju protokola IPv6,
- visoki stroški uvedbe, ki jih je v nekaterih primerih težko opravičiti z ekonomskega vidika.

Poleg tega uvedba IPv6 predstavlja izzive na področjih tehnologije (IKT) in sociologije in poslovanja. Poleg navedenih področij, na katere vpliva uvedba protokola IPv6, ta izpostavlja tudi rešitve resnih problemov soobstoja dveh omrežij IP. Pri uvedbi morajo ponudniki dostopa poiskati odgovore na naslednja vprašanja:

- *Ali lahko še čakamo?*
- *Zakaj bomo v roku dveh let izčrpali naslovni prostor IPv4 (do 2012)?*
- *Zakaj razmišljati o uvedbi IPv6?*
- *Kako bi morala uvedba potekati?*
- *Kako bi moral potekati prehod z IPv4 na IPv6?*
- *Ali imamo na razpolago le predvidevanja, kaj se bo dogajalo?*
- *Zakaj nimamo delujočega načrta?*

- *Ali je tehnologija in standardizacija že na razpolago in dovolj zrela?*
- *Imamo dovolj internega znanja in dovolj človeških virov na razpolago?*
- *Imamo v bližji okolici že omrežje IPv6 v praksi?*
- *Kako ravnati, da bo vsebina vidna iz obeh omrežij?*

Skupni cilj je priprava omrežja za ponujanje novih storitev. Pri uvajanju novih storitev je treba poiskati vsaj eno storitev, ki bo promocijsko pripomogla k hitrejšemu sprejetju novega protokola. Poleg tega morajo ponudniki dostopa narediti vse potrebno za zadovoljitev potreb državnih organov, kot so Informacijski pooblaščenc, Urad za varstvo konkurence, Ministrstvo za pravosodstvo, Ministrstvo za notranje zadeve, regulator APEK-a in drugi. Posebej bo treba poudariti uvedbo protokola v mobilna omrežja. Treba se je zavedati prednosti in slabosti, ki jih prinaša protokol IPv6 v primerjavi s protokolom IPv4.

Ponudniki dostopa do interneta

Ponudniki dostopa so bili dolga leta praktično edini subjekt, ki je uspel povezovanje posameznih omrežij v internet izkoristiti v komercialne namene. Njihovi poslovni modeli so tako sprva temeljili na preprostem zaračunavanju dostopa do interneta, pri čemer je za rezidenčne uporabnike, ki so za dostop navadno uporabljali telefonska omrežja, to pomenilo, da je bila cena neposredno odvisna od časa trajanja dostopa, pri poslovnih, ki so se v internet povezovali prek omrežij FR ali ATM pa tudi od želene hitrosti dostopa in količine prenesenih podatkov. Konvergenca dostopovnih omrežij po eni strani (uporabo telefonskega omrežja je kmalu nadomestila uporaba širokopasovnega dostopa, stacionarnim uporabnikom pa so se začeli pridruževati še mobilni) in popolna prevlada protokola IP za prenos najrazličnejših vrst podatkov sta v zadnjih letih precej spremenila poslovni model večine ponudnikov dostopa, tako da danes poleg dostopa do interneta, gostovanja in kolokacije strežnikov pogosto ponujajo tudi govorno telefonijo in televizijo (podatkovnim, govornim in videovsebinam pogosto pravimo tudi 3play), marsikateri med njimi pa igrajo tudi vlogo mobilnega operaterja in sistemskega integratorja. Organizacijska struktura ponudnikov dostopa je razdeljena na dve poglavitni področji. Prvi del organizacije je notranje področje IT, ki je po organiziranosti povsem primerljivo z drugimi podjetji enake velikosti, drugo področje pa je področje komunikacijske infrastrukture, namenjene prodaji storitev končnim uporabnikom in podjetjem. Delež ali vrednost infrastrukture, namenjene prodaji, predstavlja večinski del skupne infrastrukture IKT v podjetjih ponudnikov dostopa v internet. Uvedba protokola IPv6 za ponudnike dostopa pomeni zelo velik izziv, veliko pa je tudi tveganje uspešne uvedbe in finančnih kazalcev. Uvedba v takšno podjetje potrebuje projektni pristop k izvršitvi nalog predvsem zaradi tveganja in izjemnega vpliva na obstoječo infrastrukturo, ki predstavlja večinski, če ne celo edinega vira prihodkov podjetja. Ponudniki dostopa si preprosto ne smejo in morejo privoščiti, da bi sprejeli napačno odločitev ali napačno odgovorili na vprašanje: Kdaj, na kakšen način in predvsem kako uvesti in komercializirati spremenjen dostop do interneta?

Motivacija za uvedbo protokola IPv6

Ker igrajo ponudniki dostopa pri nemotenem delovanju interneta kot celote ključno vlogo, bi pričakovali, da se bodo uvedbe IPv6 v svoja omrežja lotili relativno zgodaj. Čeprav so v svetovnem merilu nekateri ponudniki dostopa prve korake v tej smeri res naredili že relativno zgodaj (končni različici RFC-2373 in RFC-2460, ki opisujeta naslavljanje in zgradbo paketov oziroma opcijskih glav pri protokolu IPv6, sta bili na primer objavljeni leta 1998, prvi ponudniki dostopa pa so se začeli v omrežje 6bone, ki je bilo namenjeno zgodnji izmenjavi prometa IPv6, povezovati že leta 1997), je mnoge med njimi dolga leta mučilo na prvi pogled relativno preprosto vprašanje – zakaj v svoje omrežje uvesti protokol IPv6 in ga kot takega začeti aktivno tržiti, ko pa njegove uporabe stranke ne zahtevajo oziroma ta še ne prinaša poslovnih koristi? Ponudniki dostopa do interneta ne prodajajo protokola IP, temveč rešitev, ki uporabnika in njegovo krajevno omrežje poveže z javnim internetnim omrežjem. Dopolnitve tehničnih rešitev povezovanja uporabnikov v internetno omrežje za ponudnika dostopa pomeni vlaganje določenih sredstev v načrtovanje, implementiranje, testiranje in verificiranje. Za ta namenska sredstva je skoraj nemogoče izračunati ekonomske dejavnike, kot sta obrat kapitala in povrnitev investicije. Eden glavnih dejavnikov uvedbe je ostati konkurenčen ali povečati konkurenčnost ponudbe.

Iskanje odgovora na omenjeno vprašanje se je precej časa zdelo podobno reševanju problema »kokoš ali jajce«, saj uporabniki tehnoloških prednosti, ki jih prinaša uporaba protokola IPv6, niso znali povezati z ekonomskimi. Ko so še največji skeptiki uvideli, da je sprememba internetnega protokola dejstvo, ki se mu na noben način ne bo mogoče izogniti, so tudi ponudniki dostopa začeli na omenjeni problem gledati drugače. Danes tako verjamejo, da je najustreznejši odgovor na omenjeno vprašanje temeljita priprava na prihodnje povečanje povpraševanja oziroma povečanje konkurenčne prednosti ponudnika dostopa, ki se bo lotil zgodnje uvedbe protokola IPv6 in bo na trgu lahko kot prvi ponudil neposredno povezljivost do interneta IPv6 za poslovne in rezidenčne uporabnike.

Povečanje konkurenčne prednosti pa za ponudnike dostopa še zdaleč ni edina ekonomska prednost, ki jo bodo imeli možnost izkoristiti z uvedbo protokola IPv6. Ker ima namreč glava paketa pri protokolu IPv6 stalno dolžino, hkrati pa omogoča bistveno večji naslovni prostor in precej bolj hierarhično ureditev naslovnega prostora posameznega ponudnika dostopa, lahko pričakujemo, da bo zaradi učinkovitejšega usmerjanja v hrbteničnih omrežjih in opuščanja uporabe protokola IPv4 potrebna redkejša zamenjava strojne opreme, kar bo lahko pripeljalo do zmanjšanja investicijskih stroškov.

Način in stroški uvedbe IPv6

Za dobro vodenje nalog so pri ponudnikih dostopa zaželeni kreiranje, priprava in vodenje projekta. Vizija projekta bi se morala glasiti »Postavitev novega internetnega omrežja in internetnih storitev pred konkurenčnimi ponudniki, ker ne želimo, da gredo uporabniki iskat vsebino h konkurenci.« Naloga oziroma projekt bi morala vsebovati vsebinsko pripravo naslednjih področij:

- vzroki za nastanek,
- vizija,
- vsebina,
- cilji (namenski/objektni),
- taktiko izvedbe nalog,
- plan izvajanja z časovnico (projektna razčlenitev),
- ekonomiko,
- pričakovane poslovne učinke,
- organiziranost,
- kontrolo nadzora,
- povezave z drugimi procesi (notranji in zunanji),
- analiza tveganja z analizo SWOT,
- predpostavke in omejitve,
- metodologijo merjenja uspešnosti,
- okoljske vidike,
- stroške in obrat kapitala.

Glede na opisano množico storitev, ki jih ponudniki dostopa danes ponujajo svojim strankam, predvsem pa glede na tehnološko zahtevnost, se zdi način uvedbe protokola IPv6 v omrežje ponudnika dostopa relativno jasen. Ker je namreč od sposobnosti transporta in izmenjave IPv6 prometa z drugimi ponudniki dostopa odvisno delovanje praktično vseh naštetih storitev, lahko torej pričakujemo, da bodo ponudniki dostopa v prvi fazi poslovnim uporabnikom ponujali neposredno povezljivost IPv6, po prilagoditvi uporabniške opreme (CPE) jo bodo ponudili rezidenčnim uporabnikom, šele pozneje pa bodo začeli podporo za IPv6 širiti v podatkovne centre in na ta način omogočili gostovanje in kolokacijo strežnikov. Ker gre v večini primerov telefonije IP in televizije za zasebna omrežja, ki so popolnoma ločena od interneta, oziroma je povezava med omrežji posameznih operaterjev strogo nadzorovana, hkrati pa je trenutna raven podpore internetnemu protokolu nove generacije na terminalni opremi resnici na ljubo še vedno precej omejena, lahko uvedbo protokola IPv6 v omenjene segmente pričakujemo relativno pozno.

Veliko več pozornosti je bolj kot načinu uvedbe treba posvetiti stroškom, saj lahko ti v primeru napačno zastavljene strategije uvedbe in neizkušenega kadra prerasejo ocenjene

okvire in resno ogrozijo poslovanje ponudnika dostopa. Ob upoštevanju rezultatov nekaterih tujih raziskav (na primer http://www.rti.org/publications/abstract.cfm?pub=6578) ocenjujemo, da bo večina stroškov uvedbe protokola IPv6 v omrežje ponudnika dostopa tudi v slovenskem okolju povezana z izobraževanjem tehničnega kadra in testiranjem, sledili jim bodo stroški prilagoditve oziroma nadgradnje orodij za nadzor in upravljanje omrežja, stroške zamenjave strojne in programske opreme oziroma njene nadgradnje pa je ob primernem načrtovanju mogoče vključiti v stroške rednega vzdrževanja in razvoja omrežja. Glede na prakso večine proizvajalcev strojne in programske opreme namreč lahko sklenemo, da se uporaba protokola IPv6 ne bo licencirala ločeno, tako da omenjeni stroški ne bodo prispevali k stroškom implementacije. Če povedano poskusimo zapisati še drugače, lahko sklenemo, da bodo pri uvajanju protokola IPv6 veliko večjo vlogo kot investicijski stroški (CAPEX) igrali operativni stroški (OPEX).

Ali lahko uvedba IPv6 na strani ponudnikov dostopa pripelje do povišanja cen njihovih storitev? Naj ne bi, saj če primerjamo storitev ponudnika dostopa do interneta in storitev mehanične delavnice, mehanik ne poviša cene ure, če mora za nova vozila nabaviti novo orodje – prav tako je naloga ponudnika dostopa do interneta, da svojim uporabnikom in strankam vedno zagotavlja dostop do interneta prek vseh protokolov ter vpeljuje in nadgrajuje kakovost svojih storitev. Seveda bo pri operaterjih in ponudnikih dostopa do interneta prišlo do investicij in vložkov v nadgradnjo omrežja, a take investicije morajo biti že načrtovane in ne smejo biti ovira pri uvedbi, saj mora vsak dober in kakovosten operater oziroma ponudnik dostopa do interneta nenehno nadgrajevati, vzdrževati in izboljševati svoje omrežje, če hoče vzdržati v konkurenčni tekmi, ali pa morda celo pridobiti konkurenčno prednost na trgu.

Uvajanje protokola IPv6 pri ponudnikih dostopa navsezadnje odpira tudi zanimivo vprašanje delitve stroškov uvedbe s ponudniki vsebin. Če bodo namreč v prihodnosti ponudniki vsebin želeli znižati stroške vzdrževanja omrežja s popolno opustitvijo protokola IPv4, bodo to morali narediti v soglasju s ponudniki dostopa, saj se v nasprotnem primeru kaj lahko zgodi, da uporabniki do želenih vsebin ne bodo mogli dostopati, saj neposredne povezljivosti IPv6 do interneta njihov ponudnik dostopa ne bo zagotavljal.

Ponudniki vsebin in aplikacij

Poslovni modeli ponudnikov vsebin in aplikacij so navadno zasnovani tako, da so prihodki neposredno odvisni od števila uporabnikov. Da je uvedba protokola IPv6 zanje vsaj tako pomembna kakor za ponudnike dostopa, si zlahka predstavljamo, če kot primer vzamemo uporabnika, ki želi dostopati do socialnih omrežij. Ker gre za uporabnika v razvijajoči se državi, kjer izbrani ponudnik dostopa zanj ni uspel pridobiti javnega naslova IPv4, prav tako pa zaradi stroškov opreme in implementacije v svojem omrežju ne uporablja tehnologij, kot sta LSN ali CGN, je bil omenjenemu uporabniku dodeljen le naslov IPv6.

Ker pa različici internetnega protokola med seboj nista združljivi, spletni strežnik, prek katerega uporabniki dostopajo do socialnega omrežja, pa ni bil prilagojen za uporabo s protokolom IPv6, uporabnik želene aplikacije ne more uporabljati. Težava, s katero se v takšnem primeru kaj lahko sreča ponudnik vsebin oziroma aplikacij, je zmanjšanje ciljne publike in posledično prihodkov, tako da so zgodnje odločitve Googla in Facebooka s tega vidika ekonomsko povsem upravičene.

Poslovni uporabniki

Internet igra danes v poslovnih okoljih ključno vlogo pri izvajanju vrste procesov – od medsebojne komunikacije po elektronski pošti in sistemih za neposredno sporočanje ter internetni telefoniji do prenosa podatkov med aplikacijami za vodenje podjetij in načrtovanje proizvodnje (ERP). Čeprav je bilo iskanju ekonomskih prednosti uvedbe protokola IPv6 v poslovna omrežja v preteklih letih posvečenega že kar nekaj truda, so se rezultati vselej zdeli vse prej kot ustrezni. Če so se namreč v takšnih okoljih le redko srečevali s pomanjkanjem razpoložljivega javnega naslovnega prostora in so mnoge organizacije brez težav shajale le z nekaj javnimi naslovi, so se težave pogosto pojavile že ob prvih poskusih medsebojnih povezav dveh ali več takih okolij (zaradi ločenega upravljanja naslovnega prostora je namreč v praksi težava s prekrivanjem naslovnih prostorov precej pogosta). Prav poenostavitev medsebojnega povezovanja poslovnih uporabnikov pa lahko pripomore k izboljšani informacijski podpori poslovnim procesom.

Možnost stalne neposredne povezljivosti med vozlišči pri uporabi protokola IPv6 lahko pripelje do boljše integracije internetne telefonije in sistemov za trenutno sporočanje ter njihovi pogostejši uporabi med posameznimi poslovnimi subjekti. Če si namreč danes brez težav predstavljamo, da si je elektronska sporočila mogoče med organizacijami izmenjevati brez kakršnihkoli omejitev in da je mogoče stroške telefonije v posameznem podjetju bistveno zmanjšati z uporabo internetne telefonije, imamo v praksi še vedno težave, ko želimo na enak način vzpostaviti klic med poslovnim uporabnikom v enem podjetju in dobaviteljem ali kupcem v drugem.

Dodatni ekonomski razlog za uvedbo protokola IPv6 v poslovna omrežja je lahko tudi preprostejše zagotavljanje varnosti in znižanje stroškov za uporabo namenskih rešitev, saj bodo morala biti z uveljavitvijo uporabe protokola IPv6 vsa vozlišča sposobna zaključevati seje IPSec, za kar se trenutno uporabljajo požarne pregrade ali namenski koncentratorji VPN.

Podobno kakor velja za ponudnike dostopa, lahko tudi v poslovnih okoljih pričakujemo, da bo največji strošek pri uvedbi protokola IPv6 povezan z izobraževanjem skrbnikov posameznih sistemov, kar še posebej velja v okoljih, v katerih velik del nalog v zvezi z vzdrževanjem opravljajo lastni omrežni in sistemski skrbniki, oziroma tam, kjer te naloge

niso zaupane zunanjim izvajalcem. Če se v takih okoljih uporabljajo namenske aplikacije, ki so bile razvite za omejeno število uporabnikov, in se kot take morda sploh ne razvijajo oziroma vzdržujejo več, lahko pričakujemo pri uvedbi protokola IPv6 dodatne stroške, saj bo treba ukinitev uporabe protokola IPv4 zaradi tega zamakniti. Uporaba dveh različic internetnega protokola namreč navadno pomeni povečanje stroškov vzdrževanja zaradi kompleksnejših konfiguracij aktivnih omrežnih gradnikov in strežniške infrastrukture.

Rezidenčni uporabniki

Rezidenčni uporabniki predstavljajo za praktično vse ponudnike dostopa do interneta pomemben vir prihodkov, tako da bosta načina uvedbe protokola IPv6 pri ponudnikih dostopa in rezidenčnih uporabnikih med seboj tesno povezana. Glede na to, da se po nekaterih podatkih že pri skoraj polovici dostopov rezidenčnih uporabnikov za enim javnim naslovom IP skriva domače krajevno omrežje, bo zamenjava različice internetnega protokola nujno zahtevala zamenjavo omenjenih naprav, saj se zaradi strogega nadzora stroškov vanje ne vgrajujejo komponente, ki bi omogočale programske nadgradnje. Vprašanje, ki se ob tem ponuja kar samo od sebe, je, kdo bo pokril stroške omenjene zamenjave?

Poskusimo najprej malce podrobneje osvetliti primer, v katerem je ponudnik dostopa rezidenčnemu uporabniku namenil širokopasovni modem. Ker gre za napravo, ki s stališča uporabnika izvaja le funkcionalnosti povezavne plasti (L2), bo stroške zamenjave opreme v veliki meri nosil uporabnik sam, saj bo moral zamenjati širokopasovni usmerjevalnik, ki opravlja naloge omrežne plasti (L3). Učinkovitejša uporaba aplikacij P2P se zdi s stališča rezidenčnih uporabnikov najprimernejši razlog zanjo. Stvari se v primeru rezidenčnih uporabnikov zapletejo v vseh primerih, ko se ponudniki dostopa v boju za povečanje tržnih deležev in vezavo uporabnikov odločijo ponuditi možnost uporabe funkcionalnosti omrežne plasti na napravah, ki so v njihovi lasti. V precej drugačni luči pa se razdelitev stroškov zamenjave opreme pokaže v primeru uporabe internetne telefonije in televizije, ko je operater uporabniku navadno namenil več naprav, oziroma je njihove funkcionalnosti integriral v eno samo.

Če bo rezidenčni uporabnik hotel uporabljati protokol IPv6, katerega mu bo omogočil ISP, bo moral nositi stroške zamenjave strojne in programske opreme, ki ne podpira IPv6. Oprema, ki bo verjetno podvržena spremembam, lahko rangira od osebnega računalnika, telefona, televizije, hladilnika, opekača za kruh itd., skratka vsa oprema, ki zna komunicirati prek protokola IP.

Ponudniki strojne in programske opreme

Čeprav so se ponudniki strojne in programske opreme pri uvajanju protokola IPv6 precej časa srečevali s podobno dilemo kot ponudniki dostopa in vsebin, so se predvsem razvijalci operacijskih sistemov že relativno zgodaj odločili vključiti podporo za protokol IPv6 v same operacijske sisteme (pri Microsoftu so na primer pri operacijskem sistemu Windows XP podporo za protokol IPv6 vključili v servisni paket SP1, ki je bil izdan septembra 2002). Navkljub dejstvu, da sta razvoj in testiranje novega protokola prinesla kar nekaj novih stroškov, ki jih v ceno končnega izdelka ni bilo mogoče vključiti, moramo podporo za uporabo protokola IPv6 na ravni operacijskih sistemov razumeti predvsem kot spodbudo za razvoj novih aplikacij, ki bi lahko v polni meri izkoristile prednosti protokola IPv6.

Podobno kakor pri operacijskih sistemih tudi pri aplikacijah protokol IPv6 ni bistveno vplival na dogajanje na trgu, saj so posamezni proizvajalci podporo zanj začeli vključevati brez plačila dodatnih licenc že relativno zgodaj. Če kot primer vzamemo dva danes najpogosteje uporabljena spletna strežnika – odprtokodnega Apache in Microsoftovega IIS, potem lahko zapišemo, da je bila pri prvemu podpora za protokol IPv6 dodana v različici 2.0 aprila 2002, pri drugem pa pri različici 6.0 aprila 2003. Tržni deleži obeh aplikacij se zaradi relativno majhnega povpraševanja po omenjeni funkcionalnosti niso pretirano spremenili. Nove aplikacije, ki bi jih bilo mogoče uporabljati izključno v povezavi s protokolom IPv6, pa so se razvijale izjemno počasi.

S stališča operacijskih sistemov in sistemske programske opreme torej podpora za uporabo protokola IPv6 ni pomenila povečanja tržnega deleža ali konkurenčne prednosti. Malce drugačne so stvari pri inovativnejših aplikacijah, ki spreminjajo dosedanje uveljavljene modele uporabe in dejansko izkoriščajo prednosti protokola IPv6. Kako je to videti v praksi, verjetno zelo nazorno kaže Microsoftova rešitev za oddaljeni dostop Direct Access, ki odpravlja ločitev med poslovnim okoljem in internetom. Odjemalcem omogoča neposredni in stalni dostop do poljubnih virov v njem, hkrati pa močno poenostavlja njihovo upravljanje in skrbi za stalno skladnost z zahtevanimi predpisi in priporočili.

Pri proizvajalcih programske opreme smo torej ugotovili, da bo uvedba protokola IPv6 prinesla povečanje konkurenčne prednosti le v primeru inovativnih aplikacij. Podobno velja tudi za proizvajalce strojne opreme. Segment, v katerem bo omenjena inovativnost prišla še posebej do izraza, je po našem mnenju segment uporabniške opreme (CPE), kjer so zaradi načina porazdelitve stroškov med ponudnikom dostopa in rezidenčnim uporabnikom ter obsega proizvodnje zelo pomembni stroški razvoja in proizvodni stroški. Glede na pretekle izkušnje ocenjujemo, da bo tudi v tem primeru pomembno vlogo odigrala odprtokodna programska oprema.

Sistemski integratorji

Uvedba protokola IPv6 pomeni za sistemske integratorje predvsem veliko poslovno priložnost, saj bo zaradi precej omejenih izkušenj z njegovo uporabo v praksi v prihodnjih letih povpraševanje po izobraževalnih in svetovalnih storitvah naraščalo. To pomeni, da je za sistemske integratorje ključnega pomena zgodnja osvojitev nove različice internetnega protokola, saj bodo le na ta način lahko povečali konkurenčno prednost pri pripravi in izvedbi izobraževalnih tečajev, pripravi strategij uvedbe protokola IPv6 v okolja ponudnikov dostopa in vsebin ter poslovnih uporabnikov.

Investicije v pridobivanje znanja in izkušenj s področja protokola IPv6 lahko torej z vidika pričakovanega prihodnjega povpraševanja obravnavamo kot strateške. Da bi njihove stroške uspeli znižati, imamo danes na voljo celo vrsto alternativnih izobraževalnih metod – od izvedbe notranjih izobraževanj do izobraževanja na daljavo in sodelovanja na tematskih delavnicah in konferencah. S temi se lahko izognemo daljšim odsotnostim tehničnega kadra v primeru udeležbe na izobraževalnih tečajih. Podobno lahko stroške za testiranje in verifikacijo posameznih rešitev zmanjšamo z uporabo orodij za simulacijo in virtualizacijo.

Javni sektor

(javni sektor kot katalizator na trgu IPv6 opreme in storitev)
Da motivacija za uvedbo protokola IPv6 ne more biti izključno ekonomska, je postalo jasno že pred leti, ko je v internetni skupnosti prevladalo mnenje, da lahko javni sektor odigra odločilno vlogo pri pospešenem uvajanju protokola IPv6. Vlade, ministrstva in drugi proračunski porabniki iz javnega sektorja so za pospešitev njegovega uvajanja uporabili predvsem dva mehanizma.

Po eni strani so se vlade nekaterih držav odločile, da bodo od organizacij iz javnega sektorja na administrativni ravni zahtevale uvedbo protokola IPv6 ter na ta način povečale povpraševanje po opremi, ki njegovo uporabo omogoča, in storitvah, povezanih z njegovo uvedbo. Verjetno najbolj znan primer takšne odločitve je bila zahteva ameriškega proračunskega urada (OMB – Office of Management and Budget) iz avgusta leta 2005 (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf), ki je od vseh zveznih agencij zahtevala uvedbo protokola IPv6 v hrbtenična omrežja do junija 2008, pri čemer posebna sredstva za izvedbo omenjenih aktivnosti niso bila predvidena. Podobno je predhodno tudi kitajska vlada posegla na trg informacijskih tehnologij z odločitvijo o izvedbi petletnega projekta internet naslednje generacije (CNGI – China Next Generation Internet), katerega vrhunec so verjetno bile poletne olimpijske igre leta 2008 v Beijingu, na katerih so protokol IPv6 uporabljali na praktično vsakem koraku. Odločitvi obeh vlad brez dvoma kažeta na to, da sta uvedbo protokola IPv6 obravnavali kot strateško odločitev za ohranjanje tehnološke naprednosti.

Po drugi strani so se nekatere vlade odločile za spodbujanje povpraševanja po protokolu IPv6 in njegove uporabe z vključevanjem zahtev za njegovo podporo v javne razpise. Čeprav slovenska vlada podobne odločitve še ni sprejela, se nekateri tehnološko naprednejši uporabniki že odločajo za pripravo razpisov na tak način, da mora predvsem strojna oprema omogočati uporabo osnovnih funkcionalnosti protokola IPv6.

4. Predlogi za okrepitev dejavnosti Slovenije na mednarodni sceni

"A low hanging fruit for the future of Slovenia?"
Up to this point the document should have convinced the reader that IPv6 is something of importance for the future of the Internet.
Whatever way the evolution of the Internet will take, there have to be some significant changes.
Those who get ready now, will benefit in the future and those who wait will lag behind very soon.

There are many efforts at the moment ongoing in Slovenia, supporting this wave will make a difference for the future of the country.

And personally, I consider preparing for IPv6 as a "low hanging fruit".
There are so many incentives, the technology is ready for deployment, and overall it is not that hard. So making a difference now, is going to be less painful than the recovery process from falling behind.

This section gives very useful references of current ongoing activities.

Slovenija je v zadnjem desetletju izgubila prepoznavnost na področju IKT. Pred desetletjem je aktivno sodelovala v evropskem prostoru, v zadnjem času pa ni zaslediti večjih in pomembnejših dejavnosti. Uvedba in uporaba internetnega protokola IPv6 je lepa priložnost, da si spet pridobi večji ugled in večjo vlogo na področju IKT v evropskem prostoru. Ni težko priti do ugotovitve, da bodo vse nove storitve interneta prihodnosti uporabljale protokol IPv6 za svoje delovanje. Storitve interneta prihodnosti, ki bodo za svoje delovanje uporabljale le protokol IPv4, bodo v večji meri primeri slabe prakse, seveda pa se pri tem lahko tudi nekaj naučimo. Pa si podrobneje oglejmo internet prihodnosti in se seznanimo s storitvami, ki prihajajo in bodo spremenile naše življenje. Internet prihodnosti predstavlja za prebivalce evropske skupnosti kakovostnejše življenje, saj nam bo omogočil učinkovitejšo in pametno oskrbo z energijo, informatiziranje transportne infrastrukture bo omogočilo manj zastojev na cestah in obveščanje pred nepredvidljivimi dogodki, ter različne oblike zdravljenja na daljavo, klicev SOS in najsodobnejše zdravljenje v domačem okolju.

Internet prihodnosti bo povezal različne naprave, ki jih uporabljamo pri vsakodnevnem življenju, kot so avtomobili ali mobilne naprave, z omrežnimi infrastrukturami (npr. s sistemi za upravljanje prometa, varnostnimi centri), pri čemer je mogoče veliko podatkov uporabiti v realnem času za izboljšanje okoljskih procesov in novih sinergij med interdiscliplinarnimi gospodarskimi organizacijami in podjetji.

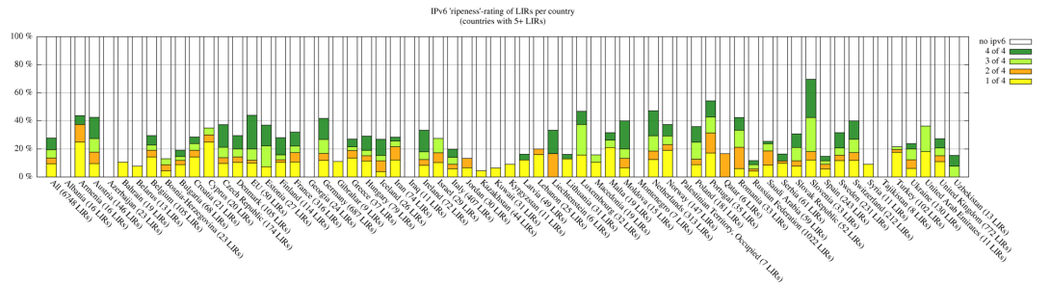
Povezava ministrstva za znanost, visoko šolstvo in tehnologije z javnimi in zasebnimi zavodi ter proizvodnimi in storitvenimi podjetji na področju uvedbe protokola IPv6 bi za

slovensko industrijo pomenila strateško prednost pred tujo konkurenco. Seveda se bo v prihodnjih letih ta prednost izničila, zato tega je treba ukrepati danes.

Javna agencija Republike Slovenije za podjetništvo in tuje investicije (v nadaljevanju JAPTI) je ključna razvojno-implementacijska agencija za izvajanje razvojne politike na področju razvoja podjetništva in konkurenčnosti v Sloveniji ter za izvajanje programov spodbujanja tujih neposrednih investicij in internacionalizacije. Država lahko s sodelovanjem z agencijo JAPTI pridobi zanimanje tujih investitorjev za investiranje v storitvene rešitve in tehnološke naprave, ki za svoje delovanje uporabljajo protokol IPv6.

Evropska komisija je že objavila vseevropsko inovacijsko strategijo za internet, s katero želi evropska zveza postati vodilna sila na internetnem področju. Evropa želi s spodbudami na področju razvoja interneta prihodnosti postati svetovna velesila. Komisija želi vzpostaviti partnerstvo med javnimi organi in gospodarskimi družbami na področju IKT. V ta namen bo v obdobju 2011-2013 predvidenih 300 milijonov evrov, ki bodo na voljo za projekte, za razvoj temeljne internetne tehnologije pa je že zdaj na voljo 200 milijonov evrov podpore.

Slovenija je na mednarodni (in na splošno internetni) sceni IPv6 zadnje čase vzbudila pozornost s svojimi dejavnostmi in uspehi z IPv6, ko je RIPE-NCC laboratorij objavil rezultate »RIPEness« analiz, kar pomeni pripravljenost države na IPv6 po njihovih merilih.



Slika 1: *»Slovenia shows the best results: 67% of LIRs in Slovenia have at least one star, while 25% have four stars! In absolute numbers that means 8 out of their 34 LIRs have achieved four star IPv6 ripeness.«*

Ker ta objava ni ostala neopažena, je bil Zavod go6, slovenska iniciativa IPv6 povabljen, da na srečanju RIPE60 v Pragi predstavi platformo go6 in druge dejavnosti IPv6 v Sloveniji, kjer je go6 zastopal Jan Žorž. To predavanje je sprožilo plaz povabil za ponovitve širom po svetu in iniciativa go6 se je pojavila s predstavitvijo slovenskih dejavnosti IPv6 na Google IPv6 Implementors conference v Mountain View v Kaliforniji, na grškem IPv6 TF v Atenah, na nemškem IPv6 council meetingu, kot goste jih je povabil NRO na delavnico z naslovom »IPv6 around the world« na dogodku IGF v Vilniusu, in še marsikje.

Te dejavnosti omenjene iniciative potegnejo s sabo promocijo Slovenije na mednarodni sceni in nam odpirajo več možnosti za sodelovanje v različnih sferah, organizacijah in projektih po svetu.

Pregled trenutnih dejavnosti:

RIPE-NCC

Z RIPE-NCC sodelujemo skozi prisotnost Go6 na vseh srečanjih, predavanjih in drugih dejavnostih RIPE. Jan Žorž in Steffann Sander sta v delovno skupino RIPE IPv6 poslala predlog dokumenta z naslovom »Requirements for IPv6 in ICT equipment«, kjer se išče široki konsenz na ravni EU za specifikacijo zahtev za IPv6 v opremi IKT za potrebe formulacij v razpisih.
http://www.ripe.net/ripe/draft-documents/ipv6-ict-requirements.html

NRO

NRO (Number Resource Organisation, http://www.nro.net/) je izkazal željo po večjem izkazovanju slovenskih uspehov na IPv6 kot zgled za druge države, kako se je treba vesti pri izvajanju začetnih korakov uvedbe IPv6.

IETF

IETF je organizacija za standardizacijo internetnih protokolov in storitev. Pri IETF Slovenija že sodeluje tudi skozi zavod Go6, ki je soavtor pri vsaj enem predlogu RFC.

IGF

Slovenija je aktivno prisotna na srečanjih in forumih IGF (MVZT), na zadnjem tudi s predavanjem na eni od delavnic (go6).

HGI

Telekom Slovenije s svojim predstavnikom Simeonom Liscem vodi delovno skupino za pripravo tehničnih zahtev in specifikacij za uporabniško oziroma domačo opremo v sklopu delovanja iniciative HGI, Home gateway Initiative. Iniciativa HGI je združenje vodilni svetovnih ponudnikov omrežja in storitev ter svetovnih proizvajalcev domače strojne in programske opreme IKT. Telekom Slovenije je trenutno tudi zlati član v zavodu go6, s tem pa tudi aktivno podpira delo zavoda go6.
http://www.homegatewayinitiative.org/about/TF/IPV6/Index_IPV6.asp

BBF

Broadband forum je forum za specifikacijo zahtev za ponudnike omrežja in internetnih storitev. Kar nekaj slovenskih podjetij je članov foruma, vsekakor ima najpomembnejšo in največjo vlogo podjetje Iskratel d.o.o. Iskratel d.o.o. je tudi član zavoda Go6.

IPv6 Forum

Latif Ladid, vodja evropskega foruma IPv6, pod okriljem katerega deluje tudi slovenski odsek, je zelo naklonjen slovenski pobudi in dejavnostim. Pobudo vidi kot izreden primer entuziastičnega in uspešnega pristopa k uvedbi IPv6. Forum IPv6 je povabil zavod Go6 v ekspertno skupino projekta EC za koordinacijo uvedbe IPv6 med EU in Kitajsko.

IPv6 TF

Slovenska delovna skupina IPv6, ki deluje pod okriljem strokovnega sveta go6, je bila razglašena za slovenski odsek EU IPv6 TF, organizacije, ustanovljene pod okriljem EC.

6DEPLOY

6DEPLOY je projekt evropske skupnosti, katerega namen je širjenje znanja in izobraževanj, ki so nastali v projektu 6DISS. S podporo lokalnih strokovnjakov lahko dosežemo nekaj imenovanj.

ISA

(Interoperability Solutions for European Public Administrations)

Aktualen je razpis ISA, v katerem se bodo standardizirala oprema, omrežja in programska oprema IKT držav članic EU na enotno platformo. Nemško notranje ministrstvo se je prijavilo za izdelavo profila IPv6, k sodelovanju pa vabijo Slovenijo, da bo naš dokument z zahtevami po IPv6 pri opremi IKT vzeli kot osnovo za EU profil IPv6.

Predlogi za prihodnje dejavnosti:

Na področju Evropske unije delujejo tri standardizacijska telesa ETSI, CEN in CENELEC. Standardizacijsko telo ETSI (The European Telecommunications Standards Institute) je neprofitna organizacija, ki skrbi za telekomunikacijske standarde v Evropi. Evropsko krovno standardizacijsko telo je CEN (Comite Europeen de Normalisation). CEN je neprofitna organizacija, ustanovljena po belgijski zakonodaji. CEN skrbi za skupno platformo za razvoj evropskih standardov in drugih dokumentov, sprejetih s soglasjem držav članic. Tretje standardizacijsko telo je CENELEC (The European Committee for Electrotechnical Standardization). Cenelec pokriva področje elektrotehniške standardizacije, med katere sodijo tudi storitve interneta prihodnosti. Najpomembnejši storitvi sta pametna energija in senzorska omrežja. Obe storitvi sta del večje celote, katere se je v zadnjem času prijel sinonim M2M (Machine to Machine). M2M pokriva celotni spekter naprav, ki se pojavljajo in bodo pojavljala v mobilnih, brezžičnih in fiksnih omrežjih. Uporabniki omrežij M2M niso ljudje, ampak naprave, za katere zagotovo vemo, da jih je na planetu vsaj stokrat več, kot je ljudi, pri tem, da štejemo naprave, ki imajo komuniciranje z drugimi napravami v osnovnih specifikacijah. Obstaja zelo tesna povezava med protokolom IPv6 in omrežji M2M. Protokol IPv6 je naravna izbira za vse arhitekture M2M, ker ta podpira zadostno število javnih naslovov IP, ki jih naprave potrebujejo za komuniciranje. Hkrati vemo, da javnih naslovov IPv4 praktično ni več na razpolago. Kar za lažjo komunikacijo z omenjenimi telesi potrebujete status člana, je v slovenskem prostoru idealen partner Slovenski inštitut za standardizacijo (SIST). SIST je član vseh evropskih standardizacijskih teles, poleg tega pa ima tudi utečene komunikacijske kanale s temi institucijami. Dobri komunikacijski kanali so nujni za izpeljavo določenih nalog predvsem pri pridobivanju kontaktov in pravih naslovov za uspešno izvedbo.

ITU

Mednarodna telekomunikacijska zveza (International telecommunication union; kratica **ITU**) je mednarodna organizacija, ki sestavlja in potrjuje standarde v telekomunikacijah. Ustanovljena je bila 17. maja leta 1865 v Parizu kot »International Telegraph Union». Njen sedež je v Ženevi.

Organizacija je razdeljena še na tri dele:

- ITU-T Sektor za telekomunikacije (Telecommunications Sector)
- ITU-R Sektor za radiokomunikacije (Radiocommunications Sector)
- ITU-D Sektor za razvoj (Development Sector)

IPv6 sodi pod sektor ITU-T.

ITU-T je organizacija za razvoj standardov (ORS), ki je del treh sektorjev mednarodne telekomunikacijske unije (posebna agencija Združenih narodov). ITU-T ima direktorsko skupino »Ad Hoc« v telekomunikacijskem standardizacijskem biroju. Tam so marca leta 2005 proizvedli naslednjo definicijo, ki jo je novembra 2005 v celoti sprejela ITU-T za svojo:

> ITU-T ima dolgo zgodovino razvoja odprtih standardov. Vendar so pred kratkim različni zunanji viri poskušali definirati »odprti standard» na različne načine. Da bi se izognili zmedi, je uporabil ITU-T svojo definicijo za termin odprti standard:
> »Odprti standardi« so standardi, dostopni splošni javnosti, razviti (ali odobreni) in vzdrževani s procesi sodelovanja in konsenza. »Odprti standardi« proizvajajo interoperabilnost in izmenjavo podatkov med različnimi produkti ali storitvami in so namenjeni za uporabo v splošno razširjeni javnosti.
> Drugi elementi »odprtega standarda«:
>
> - proces sodelovanja – razvoj (ali odobritev), ki temelji na prostovoljstvu in trgu, kateremu sledi transparenten konsenz, odprt za vse prisotne stranke,
> - razumno uravnotežen – zagotavlja, da v procesu razvoja ni nobena interesna skupina dominantna,
> - za proces – vsebuje upoštevanje in odziv na komentarje vseh vključenih strank,
> - lastništvo intelektualnih pravic (IPR) – skrbi za to, da je standard vključen v licenco vseh kandidatov po vsem svetu, na nediskriminatorni ravni, ali brezplačno in pod drugimi razumnimi pogoji ali pod razumnimi pogoji, ki zahtevajo plačilo. Pogajanja so prepuščena vsem strankam zunaj ORS,
> - kakovost in stopnja podrobnosti – mora biti zadostna, da dovoljuje razvoj raznovrstnih implikacij interoperativnih produktov ali storitev. Standardizirani

vmesniki niso skriti ali kontrolirani drugače kakor s strani SDO, ko odobri standard,
- dostopnost javnosti – mora biti lahko dostopen za izvedbo in uporabo, po razumni ceni. Publikacija besedila standarda je dosegljiva samo po preventivni odobritvi ORS,
- tekoča podpora – podpora mora biti vzdrževana skozi daljše časovno obdobje.

Vendar pa odprti standard ni omejen na te elemente.

ITU-T, ITU-R, ISO in IEC so vzajemno sklenile skupno patentno politiko [3] pod taktirko WSC. Definicija odprtega standarda ITU-T ne velja nujno tudi za ITU-R, ISO in IEC, ker splošna skupna patentna politika [4] ne omenja »odprtega standarda« ampak samo »standard«.

Nekatere članice ITU so izrazile zaskrbljenost, da bo IPv6 naslovni prostor razdeljen med razvitejše države, preden bi do njega lahko prišle manj razvite države, kot se je to zgodilo z IPv4. Zato so predlagale, da morala za zaščito interesov nerazvitih in manj razvitih držav IANA alocirati del naslovnega prostora IPv6 ITU-ju. Tega bi delili na nacionalnih ravneh in s tem spremenili obstoječi sistem 5 RIR-ov, ki zdaj dobro deluje na podlagi geografske razdelitve pokrivanja potreb po naslovnem prostoru IP lokalnih internetnih registrov (LIR). Slovenija mora prek svojih zastopnikov v mednarodnih standardizacijskih telesih izraziti stališče o tovrstnih predlogih.

Predlagamo ustanovitev delovne skupine, ki se bo ukvarjala z oblikovanjem stališč v povezavi z dejavnostmi ITU na področju internetnega omrežja.

Okvirni programi EU

Sedmi okvirni program evropske unije in priprava osmega okvirnega programa sta priložnost tudi za Slovenijo kot državo. Sodelovanje pri projektih v okviru evropskih programov lahko podpre tudi država z dodatnimi spodbudami. Zelo dobro za ugled države pa bi bilo tudi vodenje vsaj enega projekta v okviru osmega okvirnega programa. Seveda je v kontekstu protokola IPv6 zaželeno, da je to projekt, ki za izvedbo uporablja protokol IPv6. V veliko pomoč pri koordinaciji in logistiki projekta je lahko spletni portal IDEAL-IST. Več o portalu lahko preberete na spletnem naslovu http://www.ideal-ist.net/.

V nadaljevanju sledi kratek seznam tekočih projektov, ki vključujejo tudi delo na področju protokola v sklopu sedmega okvirnega programa (FP7) evropske unije s 26. oktobra 2010. Gre za osem projektov:

1. 6DEPLOY-2
Title: ***IPv6*** Deployment Support

Research area: INFRA-2010-2.3.3 Research Infrastructures
Project start date: [2010-09-01]

2. EFIPSANS
Title: Exposing the features in IP version six protocols that can be exploited/extended for the purposes of designing/building autonomic networks and services
Research area: ICT-2007.1.1 The network of the future
Project start date: [2008-01-01]

3. 6DEPLOY
Title: ***IPv6*** Deployment Support
Research area: INFRA-2007-3.3 Studies, conferences and coordination actions supporting policy development, including international cooperation, for e-Infrastructures
Project start date: [2008-03-01]

4. HOBNET
Title: Holistic Platform Design for Smart Buildings of the Future Internet
Research area: ICT-2009.1.6 Future Internet experimental facility and experimentally driven research
Project start date: [2010-06-01]

5. NOBEL
Title: Neighbourhood Oriented Brokerage ELectricity and monitoring system
Project start date: [2010-02-01]

6. FIEMSER
Title: Friendly Intelligent Energy Management System for Existing Residential Buildings
Project start date: [2010-02-01]

7. 6CHOICE
Title: India-Europe cooperation to promote ***IPv6*** adoption
Research area: INFRA-2007-3.3 Studies, conferences and coordination actions supporting policy development, including international cooperation, for e-Infrastructures
Project start date: [2008-03-01]

8. GEONET
Title: Geo-addressing and geo-routing for vehicular communications
Research area: ICT-2007.6.1 ICT for Intelligent Vehicles and Mobility Services
Project start date: [2008-02-01]
Project web site: http://www.geonet-project.eu/

Predlogi za okrepitev dejavnosti Slovenije na mednarodni sceni:

- pozivanje LIR-ov k sodelovanju in udeleževanju v delovnih skupinah RIPE,
- sodelovanje pri standardizaciji in pripravi RFC na IETF,
- koordiniranje in spodbujanje sodelovanja pri projektih FP7 in FP8 in s tem pridobivanje sredstev iz evropskih skladov za uvajanje, izobraževanje, razvoj storitev, testiranje in verifikacijo rešitev IPv6,
- lobiranje v evropskem prostoru za pridobitev sredstev za ustanovitev in delovanje kompetenčnega centra IPv6,
- vključevanje IPv6 kot prioritetnega področja v okviru smernic razvoja in investicij v IKT v slovenskem in evropskem prostoru,
- sodelovanje z javno agencijo JAPTI pri pridobivanju tujih investicij v tehnološko napredne projekte s področja IPv6,
- aktivnejše sodelovanje slovenskega inštituta za standardizacijo (SIST) z evropskimi standardizacijskimi telesi ETSI, CEN in CENELEC pri sprejemanju standardov za podporo storitvam interneta prihodnosti, katerih delovanje bo temeljilo na protokolu IPv6.
-

Literatura in viri:

- RIPE-NCC Labs, http://labs.ripe.net/Members/becha/content-ipv6-ripeness/
- EC FP7: http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&QZ_WEBSRCH=IPv6
- Javna agencije Republike Slovenije za podjetništvo in tuje investicije – JAPTI, http://www.japti.si/
- SIST- Slovenski inštitut za standardizacijo; http://www.sist.si/slo/g1/g1.htm
- European Committee for Electrotechnical Standardization – CENELEC, http://www.cenelec.eu/Cenelec/Homepage.htm
- The European Committee for Standardization (CEN), http://www.cen.eu/cen/pages/default.aspx
- The European Telecommunications Standards Institute (ETSI), http://www.etsi.org/WebSite/homepage.aspx
- ISA, http://ec.europa.eu/isa/
- http://sl.wikipedia.org/wiki/Mednarodna_telekomunikacijska_zveza
- http://sl.wikipedia.org/wiki/Odprti_standard#ITU-T_definicija

5. Kako zagotoviti konvergenco individualnih in parcialnih slovenskih vključenosti v mednarodnih formalnih dejavnostih na državni ravni

Despite the economic downturn there are motivated people pushing very hard for the right thing. This section follows up on the last one and describes how local initiatives have already formed.

Slovenija je tako kot večina držav sveta vključena v različna mednarodna združenja, odbore, komisije in delovna telesa. Odkar je samostojna, se aktivno vključuje v upravljanje sodobne mednarodne skupnosti na različnih področjih. Mednarodne dejavnosti potekajo na akademski ravni v obliki razvojno-raziskovalnih in izobraževalnih projektov ter drugih načinov sodelovanja, pa tudi na politični ravni, kjer se oblikujejo in sprejemajo odločitve prihodnjega razvoja skupnosti.

Slovenija se med skupino sedemindvajseterice držav EU po tehnološki razvitosti elektronskih komunikacij uvršča v povprečje. V 15. poročilu Evropske komisije za leto 2009 je Slovenija po gostoti internetnih priključkov malo pod evropskim povprečjem (COM(2010) 253 konč./3). Večina širokopasovnih priključkov temelji na tehnologiji xDSL. Zato pa je bistveno uspešnejša pri gradnji optičnih omrežij. Če optična omrežja v Evropi predstavljajo od 1,8 do 5 % vseh priključkov, se Slovenija uvršča med prvih osem držav sveta z največjo penetracijo optičnega dostopa do uporabnika (FTTH Council 2010). Med uspešnejše sodijo le države, kot so Južna Koreja, Japonska, Hong Kong, Tajvan, Litva, Švedska in Norveška. Žal zadnje analize kažejo, da se je večina gradenj optičnih omrežij v Sloveniji zaradi gospodarske krize (vsaj za zdaj) ustavila. Podjetje T-2, ki ima po podatkih APEK-a 60,3% tržni delež FTTH, je zaradi kapitalske nepokritosti investicije skorajda pred stečajem, Telekom Slovenije pa optična omrežja dograjuje počasi. Če ne bo država ob pomoči evropskih strukturnih skladov prevzela pobude pri gradnji optičnih omrežij, bomo težko dosegli cilj strategije Evropa 2020 (COM(2010) 2020 konč.(2010)). Strategija predvideva, da bi morali imeti vsi Evropejci do leta 2013 širokopasovni dostop do interneta, do leta 2020 pa celo hitrost, ki je večja od 30 Mbit/s. Pomembne pa niso samo investicije vlagateljev na slovenskem telekomunikacijskem trgu, temveč tudi slovensko znanje in izkušnje, ki bi ga lahko še bolj tržili na evropskem trgu in širše. To pomeni, da je treba vzpostaviti partnersko sodelovanje industrije IKT in države ter sodelovati pri trženju in uvajanju rešitev v tujini. Treba bo prepoznati, kje smo bili ali bi lahko bili uspešni. Znanje in izkušnje, ki jih lahko pridobimo pri skupnem projektu uvedbe IPv6 v Sloveniji, lahko tržimo tudi v tujini, najprej v državah bivše Jugoslavije, ki vsaj za zdaj še zaostajajo za Slovenijo. Ti projekti bi lahko vključevali izobraževanje strokovnjakov, vzpostavljanje pilotskih projektov in produkcijskih sistemov na javnih in zasebnih omrežjih, prodajo opreme IKT in še bi lahko naštevali. Pri tem lahko veliko pomagajo državni predstavniki v mednarodnih organizacijah s svojo dejavnostjo in Gospodarska zbornica Slovenije (GZS) s svojimi povezavami.

Problem, s katerim se srečuje marsikatera država, je, kako iz množice dejavnosti, v katerih so udeleženi država in njeni predstavniki, zagotoviti ustrezno konvergenco informacij, ki bodo razpoložljive vsem zainteresiranim in pooblaščenim deležnikom. Problem je tudi, kako v dirki za preživetje in v časa preseči lastno sebičnost in zasebne interese ter pridobljene informacije, izkušnje in znanja deliti z drugimi.

Leta 1999 je bil na pobudo IETF kot krovne organizacije, ki razvija internetne standarde, kot neprofitna organizacija ustanovljen IPv6 Forum. Kmalu po njegovi ustanovitvi so po njenem zgledu začeli ustanavljati regionalne in nacionalne Delovne skupine IPv6 in Svete IPv6 (IPv6 Task Force; IPv6 Council) ter druge podobne neprofitne organizacije. Vsem ustanovljenim delovnim skupinam in svetom je skupno, da združujejo različne deležnike: predstavnike industrije, operaterje in internetne ponudnike, vladne institucije in predstavnike akademsko-izobraževalne sfere. Večina si je postavila za cilj, da s skupnimi močmi in navkljub morda močnim lastnim interesom vzpostavijo trdno iniciativo, ki bo omogočila potreben prehod vseh relevantnih deležnikov na IPv6. Tovrstno sodelovanje lahko prinaša tudi večje sinergijske učinke, kakor če bi dejavnosti vodila posamezna podjetja. Pri tem je treba poudariti, da so v omenjenih skupinah praviloma povsod tako ali drugače sodelovali in še sodelujejo pomembni in vplivni posamezniki. Kot so zapisali v nemškem akcijskem načrtu, je za dosego cilja IPv6 v Nemčiji do konca leta 2010 potreben splošen konsenz in pripravljenost k delovanju vseh vpletenih na vseh ravneh družbe, vključno z vplivnimi politiki, ki morajo prepoznati priložnost nove tehnologije in jo na pravi način promovirati (IPv6 German Council, 2009).

Tudi Slovenija se lahko pohvali, da je vzpostavila ekipo strokovnjakov iz različnih sfer družbe, ki se trudi po najboljših močeh doseči potreben zagon pri uvajanju IPv6. Ekipa, ki je formalno registrirana v okviru Zavoda go6, je izjemno uspešna in uživa velik ugled v mednarodni skupnosti. Mnogi tuji opazovalci ji zaradi raznolikosti sodelujočih, strokovnosti in inovativnosti priznavajo status primera dobre prakse, ki ga je vredno posnemati.
V zadnjih desetih letih je bila organizirana vrsta konferenc, simpozijev in delavnic, s katerimi se je promovirala uvedba IPv6. Kratek pregled dejavnosti kaže na to, da države članice EU kar tekmujejo med seboj, katera bo predstavila uspešnejše stanje svoje države, kar kaže na to, kako pomembno je aktivno sodelovanje na tovrstnih dogodkih. Seveda je pri tem pomembna tudi izbira pravega dogodka in oseb, ki se jih udeležujejo. Z aktivnim in uspešnim udejstvovanjem postaneta prepoznavna predavatelj in država, ki jo zastopa. Uspešni pilotski projekti, podkrepljeni z uspešno promocijo na mednarodni konferenci, državi dvigujejo kredibilnost, obenem pa omogočajo sodelovanje z drugimi državami pri postavitvi pilotskih projektov ali produkcijskih sistemov. Šestega oktobra 2010 je Evropska komisija v okviru strategije »Evropa 2020« predstavila Pobudo o Uniji inovacij, s katero želi pospešiti inovacije v Evropski uniji. V sporočilu za javnost (IP/10/1288) je navedenih deset ključnih elementov, s katerimi želi Komisija pospešiti evropska

partnerstva za inovacije, olajšati dostope do financiranja, uskladiti evropske in nacionalne politike na področju raziskav ter pospešiti vlaganja v raziskave v javnem sektorju na področju inovativnih proizvodov in storitvah. Komisija v sporočilu predlaga, naj države rezervirajo namenska sredstva za javne razpise v zvezi z inovativnimi proizvodi in storitvami. V ta namen so v strukturnih skladih za razvoj in inovacije v letih 2007–13 namenjena sredstva v višini 86 milijard evrov. S temi sredstvi se lahko mobilizirajo zainteresirane strani, evropski in nacionalni organi, javni in zasebni sektor.
S pridobivanjem evropskih razvojnih sredstev bi lahko financirali različne projekte, s katerimi lahko dolgoročno povečamo rast in razvoj slovenskega gospodarstva, ustvarjamo delovna mesta in posledično zagotovimo konkurenčno prednost pred drugimi državami. Dober primer koriščenja sredstev je npr. pridobitev sredstev Evropskega sklada za regionalni razvoj (ESSR), s katerimi se financira gradnja odprtih širokopasovnih omrežij. Uspešnost črpanja sredstev pa je pogojena z aktivno politiko v evropskem prostoru ter z dobro komunikacijo med ministrstvi in zainteresiranimi podjetji. Tudi postopki pridobivanja in črpanja sredstev bi morali biti poenostavljeni in transparentni.

Evropska komisija je financirala več projektov in pilotov, ki so se posredno ali neposredno dotikali razvoja in uvajanja IPv6. Večina teh projektov je bila financirana z Okvirnimi programi za raziskave in tehnološki razvoj (Framework Programme). Po nam znanih podatkih je Slovenija le malo izkoristila razpoložljiva sredstva. Razlogi za to se morda skrivajo tudi v dejstvu, da smo premalo prepoznavni ter da naša podjetja zaradi majhnosti ne zmorejo ali ne znajo konkurirati večjim tujim podjetjem in državam.

Prihodnja strategija Slovenije bi morala temeljiti na tesnejšem povezovanju med javnim in zasebnim sektorjem. Dober primer tovrstnega sodelovanja je nastanek Strateškega sveta za informacijsko družbo, pa tudi dosedanje delovanje Zavoda go6. Treba bo izmenjevati izkušnje in znanja ter se truditi za večjo prepoznavnost v evropskem prostoru. Treba bi bilo povečati sodelovanje med državnimi institucijami z oblikovanjem strokovnih medresorskih skupin, ki bi večkrat letno izmenjavale informacije in izkušnje, pripravljale strateške načrte ter preverjale zastavljene cilje. Eden od prioritetnih ciljev bi morala biti tudi prenova obstoječe Strategije razvoja širokopasovnih omrežij (Vlada Republike Slovenije, 2008) ter priprava Strategije za prihodnji razvoj informacijske družbe v naslednjih štirih letih. Oba dokumenta bi morala vsebovati zavezo po vključitvi protokola IPv6 v omrežja in storitve v skladu s Sporočilom Evropske komisije o Evropski digitalni agendi (Evropska komisija (COM(2010) 245 konč./2) (2010).

Če Slovenija želi usklajeno delovati v širšem okolju, nujno potrebuje povezovalno in svetovalno telo. Povezovalno Svetovalno telo (v nadaljevanju PStelo), ki bi ga vodilo pristojno ministrstvo, naj bi povezovalo slovensko industrijo, storitvene organizacije, akademsko področje in organizacije RR v kontekstu jasne vizije prihodnosti dobrobiti za slovensko gospodarstvo. Internetni protokol IPv6 je ena od idealnih priložnosti, kjer se

lahko v industriji, vezani na proizvodnjo naprav, ki uporabljajo IP za komuniciranje z okolico, izkoristi kot konkurenčna prednost. Enaka konkurenčna prednost velja tudi za vse storitvene dejavnosti. Največje rezultate pa bi PStelo doseglo pri internetnih storitvah, kot so e-trgovine, e-knjižnice, e-znanje, e-energija ipd. Namen PStelesa je v prvi meri vsekakor zbiranje informacij na enem mestu in njihovo posredovanje zainteresiranim povpraševalcem. PStelo bi moralo komunicirati z vsemi drugimi javnimi organizacijami, ki delujejo ne le v slovenskem, temveč predvsem v evropskem prostoru. PStelo bi delovalo tudi kot svetovalno telo za celotno državno in javno upravo. Za javno upravo bi PStelo izvajalo pomoč pri izzivih, ki se bodo pojavili ob uvajanju novega internetnega protokola IPv6. PStelo sodeluje z delovno skupino, ki je lahko ustanovljena v okviru pristojnega ministrstva za javno upravo. V poglavju 11 je predlagana ustanovitev te delovne skupine za pripravo strategije za uvedbo IPv6 v omrežje javne uprave.

V naslednjem desetletju Evropa skupaj z Evropsko komisijo pripravlja strategijo razvoja interneta (i2020) v kontekstu priložnost in konkurenčnosti evropskega gospodarstva z drugimi svetovnimi gospodarskimi velesilami. Evropa želi vzpostaviti tehnološko ravnovesje z ZDA in ne želi, da bi jo azijske velesile, kot sta Kitajska in Indija, prehitele v tehnološkem napredku v naslednjih desetletjih. Zato Evropa tudi finančno podpira projekte interneta prihodnosti v okviru obstoječega sedmega in osmega (2014-2020) Okvirnega razvojnega programa Evropske unije.

Posebna priložnost za PStelo v evropskem prostoru pa je jasno sporočilo, da mora internet prihodnosti delovati na internetnem protokolu prihodnosti. Takšnega jasnega sporočila v Evropi ni še podala nobena članica EU ali katerakoli druga država v evropskem prostoru.

Predlagamo, da se zaradi širine konsenza PStelo poveže s kredibilno organizacijo ali pobudo, ki združuje že uveljavljene strokovnjake iz različnih okolij na področju IPv6. Tesna povezava strokovnjakov in PStelesa je lahko še en primer dobre prakse v Sloveniji na področju javno zasebnega partnerstva.

Viri:

IPv6 German Council (2009): Nationaler IPv6-Aktionsplan für Deutschland, dosegljivo na: http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf, obiskano dne 1.10.2010

Šabič, Z., Bučar, B, Roter, P., Kajnč, S. (2004): Slovenija v mednarodni skupnosti in Evropski uniji, dosegljivo na: http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/seu1.pdf, obiskano dne: 19.10.2010

FTTH Council (2010): *Economies with the Highest Penetration of Fibre to the Home/Building + LAN,* dosegljivo na:

http://www.ftthcouncil.org/sites/default/files/2010%20Sept%20Global%20Ranking%20FTTH.pdf, obiskano dne 19.10.2010

Evropska komisija COM(2010) 253 konč./3 (2010): Poročilo o napredku na enotnem evropskem trgu elektronskih komunikacij za leto 2009 (15. poročilo) sec(2010)630, dosegljivo na: http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/comm_sl.pdf, obiskano dne 29.10.2010

Evropska komisija COM(2010) 2020 konč.(2010): Evropa 2020 Strategija za pametno, trajnostnjo in vključujočo rast, dosegljivo na: http://ec.europa.eu/eu2020/pdf/1_SL_ACT_part1_v1.pdf, obiskano dne 29.10.2010

Evropska komisija COM(2010) 253 konč./3 (2010): »Unija inovacij – spremeniti ideje v delovna mesta, zeleno rast in socialni napredek«, dosegljivo na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1288&format=PDF&aged=0&language=SL&guiLanguage=sl, obiskano dne 29.10.2010

Vlada Republike Slovenije (2008): Strategija razvoja širokopasovnih omrežij v Republiki Sloveniji, dosegljivo na: http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/DEK/Elektronske_komunikacije/Strategije/Strategija_BB_2008-07-10_SI.pdf

Evropska komisija (COM(2010) 245 konč./2) (2010): Evropska digitalna agenda, dosegljivo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:SL:PDF, obiskano dne: 8.11.2010

6. Načrt izobraževanja lastnega IT kadra na vseh ravneh

Let's face it: One of the significant problems in the IPv6 deployment is education. There is just not sufficient appropriate training in IPv6 technology. It is often not part of classes, so that learners get appropriate exposure to it.

Here at Loughborough University in UK we are teaching IPv6 and IPv4 in parallel. Students get exposed to the new address format right from the beginning and thus will not be "scared". The difference will be understood come natural.

Unfortunately, we are just one of a very few number of universities who teach IPv6 right from the beginning. But this is our future, it is an obligation for us to teach the next generation how to live in the future - not the past.

I would even postulate that if IPv6 would have been in the curriculum of network classes and lab courses for the last decade or so, then there would be no need for this document today. Thus, this section addresses a very relevant problem. If we want to experience a successful transition period, then we have to pay attention to teaching and training.

Globalizacija na vseh področjih družbenega in poslovnega delovanja, uvajanje novih tehnologij in sodobnih komunikacijskih možnosti, spreminjanje ustaljenih poslovnih modelov, odpiranje novih poslovnih priložnosti itd. predstavljajo le del dejavnikov, s katerimi se danes srečujejo sodobna podjetja, operaterji, ponudniki storitev, javna in državna uprava ter druge organizacije v slovenskem in širšem prostoru. Velika dinamika procesov povečuje potrebo po trajnostnem vlaganju v izobraževanje in razvoj kadrov ne glede na to, ali so slednji zaposleni v podjetju, javni upravi, operaterju ali drugih organizacijah. Uspešnost in dolgotrajen razvoj sta neposredno odvisna od sposobnosti prilagajanja novim razmeram v okolju. Kontinuirano usposabljanje kadrov zagotavlja uspešnejše in neboleče prilagajanje razmeram ter pomaga zavarovati in izkoristiti potencial novih omrežnih tehnologij, kot jo npr. predstavlja vpeljevanje nove generacije internetnega protokola – IPv6.

IPv6 povzema najboljše koncepte svojega predhodnika (IPv4), hkrati pa vpeljuje vrsto tehnoloških novosti, ki odpirajo nove tehnične zmožnosti in posledično poslovne priložnosti. Da bomo lahko v polni meri izkoristili dani potencial, bo potreben odklon od tradicionalnega načina razmišljanja na tehnološkem področju pri načrtovanju, vpeljevanju in upravljanju internetnih sistemov nove generacije, pa tudi na poslovnem področju.

To poglavje tako podaja predlog upravljanja znanja kadrov s področja uporabe IPv6 v poslovnih in javnih subjektih na vseh ravneh. Zajema načrtovalce sistemov, omrežne in

sistemske skrbnike, razvijalce in vzdrževalce portalov ter aplikacij, službe za podporo uporabnikom, pa tudi vodstvo.

Pregled potreb in možnosti izobraževanja

Poslovni, razvojni in drugi delovni procesi so podprti z različnimi profili kadra (načrtovalci sistemov, omrežni in sistemski skrbniki, razvijalci in vzdrževalci spletnih portalov ter aplikacij, službe za podporo uporabnikom, segment vodstva in odločanja, itd.). Načrtovalci in upravljavci infrastrukture IKT potrebujejo posebna omrežna in sistemska znanja, razvijalci aplikacij in storitev pa potrebujejo posebna razvojna znanja o IPv6. V segmentu vodstva in odločanja pa morajo biti tehnološke prednosti nove tehnologije, kakršna je IPv6, predstavljene predvsem z ekonomskega in poslovnega vidika.

Različni profili kadrov potrebujejo različne pristope k izobraževanju in posebno ciljno vsebino. Glede na predznanje, področje in tip dela morajo biti za pridobivanje ustrezne ravni znanja IPv6 predvidene različne poti in izobraževalne možnosti. Izobraževalne možnosti lahko glede na zahtevnost, trajanje, stopnjo formalnosti in način ugotavljanja refleksije, razdelimo v 5 tipičnih sklopov:

- intenzivna strokovna izobraževanja in delavnice,
- akademska izobraževanja,
- interna izobraževanja v podjetjih in organizacijah,
- e-izobraževanja.

Intenzivna strokovna izobraževanja in delavnice

V skupino specializiranih strokovnih delavnic sodijo izobraževanja, ki jih izvajajo industrijski izobraževalni centri (NIL, ASTEC, AVTENTA, S&T, SRC itd.) in nekatere akademske in raziskovalne institucije (LTFE, Arnes itd.). Ta izobraževanja so lahko samostojna ali pa so del daljšega izobraževalnega programa, ki se sklene s testiranjem v neodvisnih testnih centrih in svetovno priznano certifikacijo. Primer: obvladovanje tehnologije IPv6 v omrežnem in transportnem sloju omrežja je eden od predpogojev za pridobitev svetovno priznanih industrijskih certifikacij, kot so Cisco Certified Networking Professional (CCNP), Cisco Certified Internetworking Expert (CCIE), Juniper Networks Certified Internet Specialist (JNCIS-ER), Juniper Networks Certified Internet Expert (JNCIE-ER). Čeprav je na trgu uveljavljenih še nekaj podobnih certifikacij, so praviloma vezane na posameznega proizvajalca strojne oziroma programske opreme, tako da bo v prihodnje treba v razvoj neodvisne certifikacije za protokol IPv6 vložiti še veliko truda.

Specializirana strokovna izobraževanja so namenjena izkušenim inženirjem, ki že imajo široko splošno znanje o omrežnih sistemih in želijo pridobiti nova specifična znanja. Obstajajo tudi izobraževanja, ki so namenjena tistim, ki šele vstopajo v svet

komunikacijskih omrežij (na primer: Cisco Certified Entry Networking Technician – CCNET, Juniper Networks Certified Internet Associate – JNCIA-ER). Zanimivo je, da so industrijska strokovna izobraževanja marsikdaj uporabljena kot hrbtenica akademsko-usmerjenih programov (na primer Ciscova omrežna akademija – glej spodaj).

Poleg izobraževanj, ki so namenjena predvsem uporabnikom specifične programske ali strojne opreme (primer: izobraževanja, ki so jih razvili proizvajalci opreme, kot so Microsoft, Cisco ali Juniper, in ki jih ponujajo pooblaščeni in s strani proizvajalca certificirani izobraževalni centri), obstaja na trgu tudi vrsta splošnih strokovnih izobraževanj za IPv6, ki naj bi udeležencem zagotovila splošno tehnološko znanje o protokolu IPv6. Za razliko od izobraževanj v okviru globalnih izobraževalnih programov (večinoma v okviru izobraževalne arhitekture posameznih proizvajalcev), v katerih razvijalec izobraževalnih vsebin zagotavlja vsaj minimalno globalno kakovost izobraževanja, je kakovost neodvisnih tečajev odvisna predvsem od kakovosti izobraževalnega centra, njegovih razvijalcev vsebin in predvsem predavateljev. V primeru izbora takšnega izobraževalnega programa je zato smiselno preveriti reference izobraževalnega centra in preizkusiti njegovo kakovost z udeležbo manjšega števila udeležencev na enem od odprtih tečajev.

Strokovna izobraževanja so namenjena predvsem pridobivanju praktičnih znanj, ki so neposredno uporabna v delovnem procesu udeležencev. Pri kakovostnih strokovnih izobraževanjih je zato velik del časa namenjen praktičnemu delu z opremo (primer: v okviru izobraževanja o delovanju omrežne opreme proizvajalcev Cisco ali Juniper ima vsak udeleženec dostop do treh ali štirih usmerjevalnikov ali stikal), kar omogoča udeležencem izobraževanja takojšnje preverjanje kakovosti pridobljenega znanja, pa tudi hitro pridobivanje praktičnih izkušenj, ki jih lahko nato uspešno uporabijo pri svojem vsakodnevnem delu. Prednost izobraževanja v izobraževalnem centru kakovostne organizacije, ki se poleg izobraževanja ukvarja še z drugimi dejavnostmi (svetovanje, gradnja omrežij ...), pa so nedvomno tudi praktične izkušnje predavateljev, ki lahko v okviru neformalnih pogovorov z udeleženci tečaja rešijo marsikateri praktičen problem v informacijski infrastrukturi udeležencev.

Bistvena razlika med strokovnimi izobraževanji in akademskimi programi (glej spodaj) je predvsem intenzivnost izobraževanja. Primer: tematika, ki je v intenzivnem tečaju CCENT obdelana v enem tednu, traja v enakovrednem programu Ciscove omrežne akademije ves semester. Akademski izobraževalni programi so zato idealni za tiste, ki šele vstopajo v svet informacijske tehnologije in si želijo pridobiti širok nabor različnih znanj, strokovna izobraževanja pa so namenjena tistim, ki morajo znanje, potrebno za opravljanje svojih del in nalog, pridobiti čim prej in čim bolj učinkovito.

Vsekakor pa velja omeniti tudi znano slabost strokovnega izobraževanja: samo izobraževanje navadno ne vsebuje formalnega preverjanja pridobljenega znanja, marsikdaj zaradi pravnih pomislekov organizacij, ki razvijajo takšna izobraževanja, in ki

formalno preverjanje znanja raje prepustijo specializiranim organizacijam (v svetovnem merilu je takšna organizacija na primer Pearson VUE, ki ima testne centre v 165 državah), saj ima izpit, opravljen v takšni organizaciji, globalno veljavnost.

Zaradi razširjenosti znanja o tehnologiji IP so strokovna izobraževanja s področij IPv6 namenjena predvsem pridobivanju specifičnih znanj s področja IPv6, kot so: struktura naslovnega prostora, novi usmerjevalni protokoli, nove aplikacijske zahteve in podobno.

Intenzivne strokovne delavnice so primerne za kadre, ki suvereno obvladujejo obstoječi delovni proces (upravljavci omrežja, sistemski skrbniki, upravljavci in vzdrževalci portalov), za vpeljavo oziroma prehod na IPv6 pa potrebujejo poleg osnovnih veščin IPv6 še poglobljena znanja, ki so podkrepljena s primeri dobrih praks.

Akademska izobraževanja

Akademski izobraževalni programi so zasnovani tako, da udeleženci sistematično, s sprotnim delom in skozi daljše časovno obdobje pridobivajo temeljna in poglobljena znanja o obravnavanih vsebinah. Študijski program združuje predavanja, e-izobraževanja, praktično delo na opremi v laboratorijih, simulacijsko okolje, redna preverjanja znanja, preverjanje praktičnih veščin itd. Primer: v študijskem programu UNI-LJ FE, smer Telekomunikacije, so za uspešno upravljanje izpita pri predmetu Komutacijski sistemi in omrežja potrebna znanja iz osnov delovanja IPv6, ki jih študentje pridobijo med predavanji, seminarjem in praktičnimi vajami v laboratoriju.

Akademski proces vključuje pridobivanje teoretičnega znanja, praktičnega znanja, večkratno preverjanje znanja in zaključni izpit, kar vodi v pridobitev univerzitetne diplome oziroma priznanih certifikatov. Prednost pristopa je velika širina, saj študijski program zajema vsa področja informacijskih in komunikacijskih sistemov, utrjevanje znanja skozi daljše časovno obdobje, ter da se uspešen zaključek izobraževalnega procesa izkazuje z jasno določeno stopnjo razumevanja obravnavanega tematskega področja, ki je potrjen tudi z ustreznim verificiranim dokazilom.

Dinamika vključevanja novih vsebin v univerzitetne študijske programe predstavlja kompleksen in dolgotrajen proces, ki je odvisen od programskih odborov posameznih fakultet oziroma univerz, zato je raven in stopnja integracije nove vsebine (npr. izobraževalne tematike s področja IPv6) med posameznimi akademskimi inštitucijami lahko različna. Zaradi dolgotrajnosti učnega procesa so akademski izobraževalni programi primarno v domeni univerz in visokošolskih izobraževalnih ustanov, ki jih izvajajo na različnih stopnjah zahtevnosti. Med vodilne akademske institucije, ki v okviru izobraževalnega programa IKT podajajo tudi vsebine s področja IPv6, sodijo:

- UNI-LJ, Fakulteta za elektrotehniko – program Telekomunikacije,

- UNI-LJ, Fakulteta za računalništvo – program Računalništvo in informatika,
- UNI-MB, Fakulteta za elektrotehniko računalništvo in informatiko – program Telekomunikacije.

Vodilni globalni proizvajalci omrežne opreme in informacijskih rešitev imajo tudi lastna »industrijska akademska izobraževanja«, ki delujejo po principu sistematičnega in v daljše časovno obdobje usmerjenega izobraževalnega procesa. Tipično so specializirana in vezana na produkte in rešitve izbranih proizvajalcev opreme. Med vodilne programe sodijo:

- Omrežna akademija Cisco (Cisco Networking Academy), ki predstavlja globalni izobraževalni program s področja omrežnih tehnologij ter
- Microsoft IT akademija (IT Academy Program), ki predstavlja izobraževalni program s področja informacijskih tehnologij.

Akademski izobraževalni proces je primarno namenjen kadrom na začetku poklicne poti ali tistim, ki bi jo radi nadgradili, tako da še nimajo širine in temeljnih znanj s področja sistemov IKT. V tem primeru veščine IPv6 predstavljajo le del ciljnih specialnosti, ki bodo osvojene v učnem procesu v daljšem časovnem obdobju.

Interna izobraževanja v podjetjih in organizacijah

Akademska in intenzivna strokovna izobraževanja se lahko nadgrajujejo z dodatnimi internimi, podjetju specifičnimi vsebinami s področja IPv6, ki jih izvajajo strokovnjaki zaposleni v podjetju oziroma organizaciji. Interna oblika prenosa znanja je zaželena zaradi predavateljeve vpetosti v kulturo organizacije, podrobnega poznavanja stanja tehnoloških razmer, delovanja in potreb sistemov IKT ter zaradi izboljšanja kakovosti internih delovnih procesov.

Primer: po udeležbi zaposlenih na klasičnem izobraževanju zunaj organizacije (npr. intenzivno strokovno izobraževanje) se za udeležence delavnice pripravi interna predstavitev načina uvedbe in trenutnega stanja protokola IPv6.

V primeru nekaterih profesionalnih služb, kot so npr. vojska in varnostne agencije, se uporabljajo tudi omrežni in informacijski sistemi zaprtega tipa, zato je pridobivanje novih posebnih veščin na osnovi internega prenosa znanja edini možen način in tako nujno potreben proces.

E-izobraževanja

Model e-izobraževanja omogoča sodoben pristop učenja kjer koli in kadar koli. Praviloma se izvaja ločeno od mesta poučevanja in zato zahteva specifične tehnike načrtovanja

izobraževalnih gradiv, poučevanja ter komunikacije s pomočjo informacijskih in komunikacijskih tehnologij, pa tudi posebne pristope k ureditvi organizacijskih in administrativnih zadev. Največkrat se uporablja kot dopolnitev klasičnega izobraževalnega procesa (akademska izobraževanja ali strokovne delavnice), kot sistem za hitro distribucijo vsebin in navodil ter kot sistem za predstavitev novih storitev, produktov in prodajo – odvisno od specifike in narave delovanja organizacije. Sistem omogoča statistični nadzor nad učečimi, sledenje napredka in preverjanje pridobljenega znanja ter tako zagotavlja dober vpogled nad osvojenimi vsebinami.

E-izobraževalne vsebine se lahko uporabljajo tudi za pripravo skupine udeležencev na zahtevnejše klasično izobraževanje (npr. Primer dobre prakse uporabe IPv6). Z uvodnim e-tečajem udeleženci samostojno pridobijo minimalno raven znanja (Osnove IPv6), ki je skupen vsem udeležencem. Slednji način homogenizacije skupine omogoča, da imajo udeleženci razmeroma enako raven vstopnega predznanja in se v okviru klasičnega izobraževalnega procesa razmeroma hitro lahko osredotoči na zahtevnejše tematike, specifiko dela in praktične primere.

Primer: inštruktor pripravi e-tečaj z osnovnimi informacijami o tehnologiji IPv6. Pred udeležbo na klasičnem izobraževanju se udeleženci sami seznanijo z osnovami IPv6 in preverijo razumevanje s samoevalvacijskim testom. Pred samim pričetkom predavanja imajo vsi udeleženci že zahtevani minimalno raven predznanja in se z inštruktorjem lahko takoj osredotočijo na primere uporabe IPv6 v praksi oziroma na konkretnem področju, kot je npr. usmerjanje v IPv6.

Predlog upravljanja znanja IPv6 v javni upravi

Za uspešen in usklajen prehod na IPv6 vseh omrežnih in storitvenih servisov IKT, ki jih podpira sistem javne uprave, bo treba dodatno izobraziti vse zaposlene, ki načrtujejo, gradijo in upravljajo informacijsko komunikacijske sisteme javne uprave, od razvijalcev storitev in aplikacij ter omrežnih in sistemskih administratorjev do tehnikov v službi za pomoč uporabnikom. Vsak profil strokovnega kadra, ki obvladuje določen delovni proces, bo seveda potreboval specifična znanja o IPv6.

V okviru ministrstva za javno upravo (MJU), že obstaja utečeno izobraževalno ogrodje »Upravna akademija MJU« (http://www.mju.gov.si/) za upravljanje znanja zaposlenih v sistemu javne uprave. Ta mehanizem se lahko uporabi kot utečeno ogrodje (npr. IPv6 Akademija v MJU), ki bo zagotavljal pregleden in sistematičen dvig ravni vseh potrebnih znanj zaposlenih s področja IPv6 v javni upravi RS. Predlagamo, da se v okviru akademije MJU/IPv6 izvedejo:

- **pregled potreb:** izvede se pregled potrebnih znanj IPv6, ki jih potrebujejo posamezni profili zaposlenih,

- **sistematizacija izobraževanj:** glede na identificirane potrebe se izvede izbor izobraževalnih vsebin in njihova sistematizacija. Izobraževalni programi se sistematično ovrednotijo in uredijo po različnih merilih: ciljna skupina, namen izobraževanja, raven zahtevnosti in vsebina programa, potrebno predznanje udeležencev, trajanje, metode dela, potrdilo o udeležbi, znanju, diploma, certifikat,
- **določitev izobraževalnih poti:** sistematizacija omogoča, da se za specifične profile zaposlenih pripravi različne izobraževalne poti. Ti se lahko glede na interes, znanje in delovne naloge posameznikov med seboj tudi združujejo. Primeri splošnih izobraževalnih poti:
    - osnovno izobraževanje za tehnične sodelavce za boljše razumevanje področja IPv6.
    - specialno izobraževanje za omrežne administratorje za obvladovanje naprednih mehanizmov, kot so usmerjanje, QoS, multicast in druge napredne funkcije tehnologije IPv6,
    - izobraževanje za vodstvo in odločanje za pridobivanje boljšega vpogleda v tehnično področje in s tem strateško razmišljanje.
- **zagotavljanje kakovosti izobraževanj:** za uspešno doseganje zastavljenih ciljev je treba zagotoviti, da je izobraževalna vsebina ustrezna, da so bili na izobraževanje poslani pravi udeleženci ter da je bil izbran kakovosten izvajalec. To zagotavljamo z anketami, ki nam po končanem izobraževanju omogočajo zbiranje informacij o ravni udeležencev, ravni izobraževalnega programa, kakovosti vsebin in predavateljev itd. Analiza rezultatov nam omogoča, da po potrebi spremenimo ter izboljšamo posamezne komponente izobraževalnega sistema,
- **potrdila o udeležbi in znanju:** udeležencem se ob zaključku izobraževanja podeli potrdilo o udeležbi. Če udeleženci opravljali tudi preverjanje znanja (ustno, pisno, praktično), ki dokazuje minimalno zahtevano raven osvojene tematike, se jim podeli tudi ustrezen certifikat oziroma diploma.

Predstavljen model za upravljanja znanja IPv6 v javni upravi je dovolj splošen, da se lahko uporabi kot vzorčen koncept, ki se prenese tudi na organe državne uprave ter druge organizacije javnega značaja.

Predlog upravljanja znanja IPv6 v gospodarskih družbah

Prehod s tehnologije IPv4 v okolje IPv6 je idealen primer dodatnega izobraževanja široke palete zaposlenih v gospodarski družbi. Operaterji bodo morali dodatno izobraziti večino svojih zaposlenih, v gospodarskih družbah pa bo dodatno izobraževanje omejeno predvsem na zaposlene, ki načrtujejo, gradijo in upravljajo informacijsko tehnologijo (od razvijalcev aplikacij do tehnikov v službi za pomoč uporabnikom). Seveda potrebuje vsak profil strokovnih kadrov specifična znanja:

- razvijalci aplikacij se morajo zavedati predvsem tega, kako naslovi IPv6 vplivajo na delovanje aplikacij in komunikacijo med odjemalci in strežniki,
- upravljavci strežnikov morajo poskrbeti, da so strežniki dostopni s protokolom IPv4 in s protokolom IPv6 ter da vsa programska oprema strežnikov podpira oba protokola,
- upravljavci omrežja morajo zagotoviti varno in učinkovito delovanje omrežja, ki bo moralo še leta podpirati IPv4 in IPv6,
- delavci v službi za pomoč uporabnikom morajo biti sposobni diagnosticirati in odpravljati napake, ki so povezane z obema protokoloma (in ravno na tem področju obstajajo med IPv4 in IPv6 drastične razlike).

Tako obsežen izobraževalni projekt je idealna priložnost za uvajanje sistema za obvladovanje znanja in sistema za e-učenje v gospodarsko družbo. Namesto ad-hoc rešitev (pošljimo nekaj zaposlenih na izobraževanje, drugi pa se bodo že nekako naučili od njih) bi moralo vodstvo organizacije IT v gospodarski družbi (v primeru operaterjev pa kar uprava podjetja) sprožiti postopek, ki bo:

- identificiral specifična znanja, ki jih potrebujejo posamezni profili zaposlenih.
- zagotovil vsebine, ki bodo zaposlenim ponujale zahtevana specifična znanja – od e-izobraževanja do kratkih delavnic ali strokovnih izobraževanj,
- zagotovil, da bodo vsi zaposleni dobili zahtevana znanja in da bo raven njihovega znanja tudi preverjena z ustreznim postopkom.

Proizvajalci informacijske opreme, pa tudi globalni in regionalni operaterji, so te postopke že sprožili in, kot je bilo pričakovati, večino svojih potreb pokrivajo z e-izobraževanjem, saj to omogoča postopno in časovno učinkovito pridobivanje potrebnih znanj. Žal v Sloveniji podobnih trendov (razen pri nekaterih operaterjih, ki že ustrezno usposabljajo svoje načrtovalce omrežij) še nismo zaznali.

7. Pritegovanje operaterjev oziroma ponudnikov dostopa

Creating incentive and attracting operators and providers is important for the future of Slovenia and the rest of the world. This section reflects upon competitiveness and how to create this incentive.

Bistveni element, ki bo operaterje prisilil k uvajanju IPv6, je ohranjanje konkurenčnosti. Razmisliti moramo, kaj pomeni skrb za uporabnika. Operater mora uporabniku zagotoviti dostop do vsebin in storitev v internetu, nikjer pa ni eksplicitno zapisano, kateri protokol naj za to uporabi. Po kakšnem protokolu? To ni nikjer specificirano, ampak predvideva se lahko, da po vseh možnih. V nekem trenutku se bo konkurenčen ISP odločil in uvedel IPv6 ter s tem prešel na dual-stack omrežje. To pomeni, da se bodo pojavili uporabniki, storitve

in vsebine, ki bodo lahko dosegljivi po obeh protokolih ali zaradi enostavnosti samo po IPv6. Operaterji, ki svojim uporabnikom ne bodo omogočili dostopa do vsebin, ki bodo dostopne le po IPv6, bodo kmalu postali nekonkurenčni. Kaj je torej naloga ISP-ja v smislu skrbi za svoje uporabnike? Lahko se odloči za stališče »saj bo vse dostopno po obeh protokolih, kaj mi to mar«, ali pa ugotovi, da bi bilo lepo in koristno svojim uporabnikom omogočiti dostop do vsebin in storitev pri konkurenčnem ISP-ju prek obeh protokolov, saj ni mogoče vedeti, kdaj se bodo pojavile vsebine in storitve, ki bodo na voljo samo v omrežju IPv6.

Zagotavljanje dostopa v internet s protokolom IPv4 bo sčasoma postalo vse bolj kompleksno. Čeprav ima konkurenčni ISP še na voljo naslove IPv4, postaja postopek ponujanja vsebin in storitev majhnega podjetja ali rezidenta vedno težja. Praviloma dobi od ISP-ja en naslov IPv4, za katerega skrije celotno zasebno omrežje s strežniki vred. Kako usmeriti vrata skozi NAT, je znano, a je s tem veliko dela. Manj poučeni in strokovno podkovani uporabniki imajo s temi nastavitvami nemalo problemov. Kaj hitro zadeve postavijo tako, da jim ne deluje nič več. Z uvajanjem tehnologije CGN se bo kompleksnost prevajanja naslovov še povečevala, kar so že občutili nekateri mobilni operaterji (tudi slovenski), ki CGN uporabljajo že več let. Predvideva se celo, da se bodo v prihodnosti celotna dostopovna omrežja skrivala za velikim NAT-om v jedru omrežja (CGN), kar pomeni, da uporabnik ne bo več dobil javnega naslova IPv4, ampak zasebnega, skritega pred svetom. Nekateri mobilni operaterji pri nas to že nekaj let izvajajo v svojih mobilnih podatkovnih omrežjih.

Pri IPv6 je vse precej lažje. Uvajanje IPv6 nedvomno poenostavi nastavitve končnih naprav. Po priporočili IETF dobi vsaka rezidenčna CPE naprava svoj del naslovnega prostora IPv6, vsak računalnik pa svoj javni naslovI Pv6. IETF priporočila so alociranje (routed) /64 (ali celo /48) segmenta vsaki rezidenčni napravi CPE, kar pomeni odpravo NAT-a, saj vsak računalnik oziroma naprava dobi svoj javni naslov IPv6. iz računalnika/strežnika doma lahko začne streči vsebine ali storitve in ob pravilni nastavitvi požarnega zidu IPv6 je to dokaj preprosto opravilo.

Doslej je bilo ponujanje storitev in vsebin prek interneta večinoma domena večjih podjetij – ponudnikov vsebin, ki imajo svoje podatkovne centre ali gostujejo s strežniki pri kakšnem ISP-ju ali ponudniku strežniškega gostovanja. Z uvedbo IPv6 in ukinitvijo mehanizmov NAT se odpirajo neslutene nove možnosti za manjša podjetja in rezidenčne uporabnike, kjer vsebina in storitve niso samo ftp in http, ampak še marsikaj drugega.
Pojavile se bodo torej vsebine, do katerih uporabniki ISP-jev, ki ne bodo uvedli IPv6, ne bodo mogli dostopati.

Ravno usmeritev ISP-ja, ki skrbi za uporabnika, zna biti močan mehanizem koordinirane in časovno usklajene uvedbe IPv6 pri ISP-jih vse do uporabnika, saj nihče noče prebega

uporabnikov med operaterji ali nezadovoljnih uporabnikov na svojem centru za telefonsko pomoč.

Glavna naloga ponudnikov dostopa do interneta bi morala biti skrb za uporabnika in njegovo najboljšo možno povezljivost do storitev in vsebin v internetu.

8. Vzorčni model za vključevanje ustreznih specifikacij v sezname zahtev pri razpisih za nabavo komunikacijske in računalniške opreme ter e-storitve javne uprave

Ensuring quality is critical. Especially, for governments giving out recommendations and directions. Therefore I appreciate very much initiatives such as "IPv6 Ready". This section lists all the relevant standards and explains what it takes to get ready for IPv6. It is a really valuable section with all the right details.

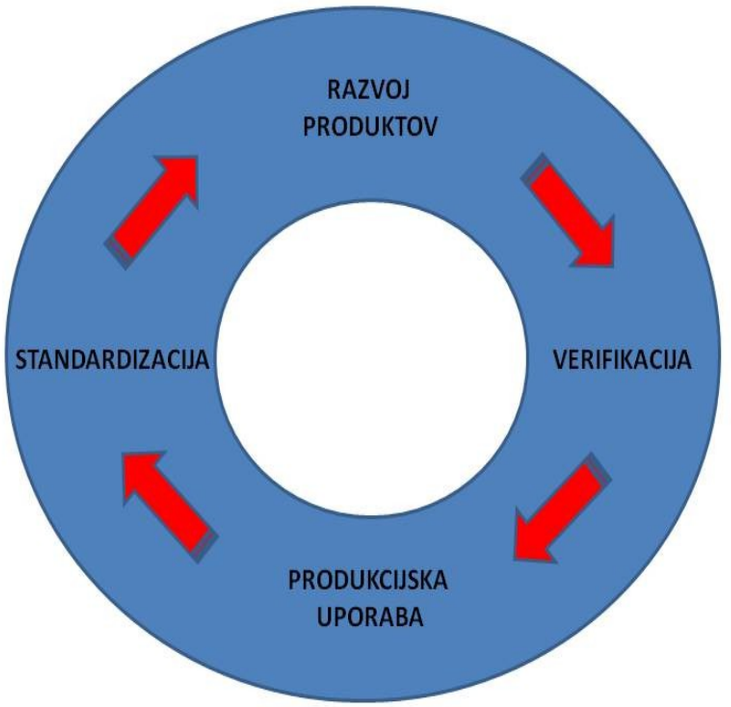
Protokol IPv6 predstavlja najnovejšo stopnjo razvoja internetnega protokola, namenjen vzpostavljanju naslednje generacije internetnih sistemov za razrešitev problema pomanjkanja naslovnega prostora IPv4 ter izboljšave nekaterih funkcij in zmogljivosti. Protokol IPv6 vpeljuje vrsto novosti in prednosti, ki se odražajo v funkcionalnostih, kot so: mehanizem za določitev MTU, izboljšan protokol za poizvedbe med sosedi, izboljšan mehanizem QoS, mehanizem za samonastavitev parametrov IP, izboljšane usmerjevalne funkcije, izboljšana mobilnost in varnostne funkcije.

Pri novih tehnologijah in rešitvah, ki so še nepreizkušene in se širše še ne uporabljajo, je zaradi stabilnosti delovanja končnih produkcijskih sistemov ter zaščite investicije pomembno, da se uporabniki pred produkcijsko uporabo zavedajo stopnje zrelosti tehnologije oziroma posameznih razvojnih faz, ki jih mora posamezna rešitev prestati, da doseže stopnjo, ki se zahteva za produkcijske sisteme.

Življenjski krog vsake tehnologije (Slika 8-1), tudi IPv6, lahko delimo v štiri temeljne razvojne faze, ki si praviloma sledijo v naslednjem zaporedju:

- faza standardizacije,
- faza razvoja produktov,
- faza verifikacije,
- produkcijska uporaba.

Šele po uspešnem zaključku standardizacijskega postopka, razvoja ter verifikacijskega procesa je posamezna rešitev primerna za uporabo v produkcijskih sistemih.



Slika 8-1. Življenjski krog tehnologij

Zavedati se je treba, da tehnologija lahko preide v zrelo obdobje, šele ko je standardizacijski proces zaključen. Implementacije produktov s tem postajajo čedalje bolj stabilne in zanesljive, saj so rešitve proizvajalcev prestale vrsto verifikacijskih procedur in testiranj, ki jih izvajajo tako proizvajalci sami med razvojem kot zunanje neodvisne institucije, združenja ter forumi, v končni fazi pa tudi končni uporabniki. Skozi pilotne implementacije postanejo rešitve dovolj preizkušene in zanesljive ter s tem primerne za uporabo v produkcijskih okoljih.

Zaradi hitre širitve internetnih sistemov in rešitev standardizacija zaradi narave delovanja standardizacijskih postopkov težko sledi hitrosti razvoja produktov. Standardiziranost večinoma ni zagotovljena v ustrezno kratkem času. Posledično razvoj produktov pri vodilnih proizvajalcih opreme IP velikokrat prehiteva standardizacijo. Proizvajalci na trgu tako prodajajo nestandardizirane oziroma lastniške rešitve, ki jih je težko ustrezno verificirati, vendar se zaradi potreb trga vseeno uporabljajo v produkcijskih sistemih.

Opisana problematika predstavlja precejšen izziv pri načrtovanju, izboru ustrezne opreme ter vzpostavljanju novih produkcijskih sistemov, saj pogosto zahteva tvegane odločitve pri izboru, ki predstavljajo kompromis med tehnološko sodobnimi ali standardiziranimi rešitvami, za kar pa so potrebna ozko specializirana znanja.

V poglavju 8 bo tako predstavljen proces standardizacije internetnih sistemov, analiza trenutnega stanja standardizacije, v katerem je IPv6, proces verifikacije produktov IPv6 ter končen predlog vključevanja specifikacij v razpise za nakup opreme IKT javne uprave Republike Slovenije.

Standardizacija internetnega protokola

Internetni standardizacijski proces se izvaja v organizaciji Internet Engineering Task Force – IETF (http://www.ietf.org/) v okviru področnih delovnih skupin (Working Groups). Organizacija deluje po principu odprte skupnosti, kjer se lahko vsakdo, tudi posameznik, udeleži in prispeva k standardizacijskem procesu. Standardi se izdajajo v obliki specifikacij RFC (Request for Comment), ki določajo delovanje posameznega protokola, naprave, osnovnih funkcionalnih gradnikov storitve (npr. BGP, MPLS, VPN). Ideali, ki jih zasledujejo v okviru svojega dela, so:

- tehnična odličnost,
- implementacija in testiranje funkcionalnosti pred izdajo končnega standarda,
- jasna in s konsenzom sprejeta specifikacija standardov,
- odprtost in pravičnost.

Vsaka specifikacija RFC prestane več faz razvoja ter testiranj (maturity levels), ki odražajo zrelost in razširjenost posameznega standarda. IETF definira tri stopnje zrelosti protokola, rešitve oziroma tehnologije (RFC 2026):

- predlagani standard (Proposed Standard),
- osnutek standarda (Draft Standard),
- internetni standard (Internet Standard).

Specifikacija RFC lahko pridobi status »internetnega standarda« šele, ko sta dva proizvajalca opreme implementirala vse zahtevane funkcionalnosti, določene v specifikaciji RFC, ter izkazala medsebojno delovanje produktov, kar pomeni, da je bilo med produktoma izvedeno združljivostno testiranje (interoperability testing).

V okviru delovnih skupin IETF nastajajo tudi dokumenti, označeni z RFC, ki pa so informativnega oziroma eksperimentalnega značaja. Slednji ne predstavljajo standardizacijskega procesa IETF in za proizvajalce opreme niso obvezujoči. Mednje sodijo specifikacije RFC, označene z oznako »Informational« ter »Experimental«. Nekateri

bolj iznajdljivi proizvajalci opreme tako objavijo v obliki »Informational RFC« svoje lastniške (proprietary) rešitve in jih prikrito navajajo kot »standardne« internetne rešitve.

Stanje standardizacije IPv6

Delovna skupina IPv6 (http://www.ietf.org/wg/concluded/ipv6.html), v okviru katere je potekal razvoj osnovnih standardov za podporo delovanju internetnega protokola nove generacije, je končala z delom leta 2007. Sprejeli so prek 43 predlogov standardov in njihovih dopolnil. Navkljub temu, da je jedro specifikacij IPv6 sprejeto in stabilno, še vedno poteka razvoj dopolnilnih in razširjenih standardov IPv6 v drugih delovnih skupinah (http://datatracker.ietf.org/wg/), kot so:

- IPv6 over Low power WPAN,
- IPv6 Maintenance,
- Mobility EXTensions for IPv6,
- Site Multihoming by IPv6 Intermediation,
- IPv6 Operations,
- Layer 3 Virtual Private Networks,
- ter drugih organizacijah, ki predvidevajo uporabo IPv6 v svojih sistemih, npr. 3GPP.

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

Po drugi strani pa so kupci opreme pred dilemo, kateri nabor specifikacij in funkcij lahko pričakujejo pri posameznem produktu IPv6, ki je na trgu na voljo.

Verifikacija produktov IPv6

Celovit proces verifikacije opreme, katerega namen je zagotoviti stabilno in dolgoročno delovanje rešitev v produkcijskih okoljih IPv6, zajema naslednje sklope testiranj:

- skladnostno testiranje (conformance testing) – zagotavlja, da omrežni element (npr. usmerjevalnik, strežnik) deluje v skladu s predpisanim naborom standardov,
- združljivostno testiranje (interoperability testing) – zagotavlja, da se oprema različnih proizvajalcev lahko uspešno medsebojno povezuje,

- funkcionalno testiranje (functional testing) – ugotavlja, ali so v produktu zajete vse zahtevane funkcionalnosti,
- zmogljivostno (performance testing) in primerjalno testiranje (benchmark testing) – ugotavlja kvalitativne lastnosti verifikacijskemu procesu podvrženega produkta.

V sklopu skladnostnih in združljivostnih testov med produkti različnih proizvajalcev ne sme prihajati do odstopanj. Kar pomeni, da morajo vsi produkti v testiranem segmentu 100% izpolnjevati predpisane zahteve. Rezultati skladnostnih in združljivostnih testiranj, tako predstavljajo minimalni prag, katerega mora produkt izpolnjevati, da še ustreza razpisnim pogojem.

Na področju funkcionalnega, zmogljivostnega in primerjalnega testiranja rešitev pa se rešitve različnih proizvajalcev opreme med seboj lahko razlikujejo. Na tem segmentu se pokaže inovativnost in dodana vrednost proizvajalcev ter s tem njihova ključna konkurenčna prednost, ki mora predstavljati končno merilo za izbor opreme pri razpisih.

Certifikacija produktov IPv6

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

- program »IPv6 ready«, ki predstavlja odprto svetovno združenje za verifikacijo rešitev IPv6 in deluje pod okriljem IPv6 Foruma,
- obrambno ministrstvo združenih držav (DoD), ki določa verifikacijske procedure za omrežno opremo IPv6, ki se bo uporabljala v sistemih njihovega obrambnega ministrstva,
- nacionalni inštitut za standardizacijo (NIST), ki določa verifikacijske postopke za omrežno opremo IPv6, namenjeno za uporabo v omrežjih javne uprave ZDA.

Program »IPv6 Ready«

IPv6 Forum je že v zelo zgodnji stopnji razvoja in uveljavljanja tehnologije IPv6 vzpostavil validacijski proces IPv6 Ready Logo Program (http://www.ipv6forum.com), ki predstavlja odprto mednarodno združenje za verifikacijo rešitev IPv6. Tako so leta 2004 razvili proces »Phase 1 Logo certification«, ki je testiral pet razredov produktov IPv6. S programom »Phase 2 in Phase 3 logo certification proces« pa so zahteve za testirane produkte še dodatno zaostrili. Certifikacija IPv6 Ready zajema samo prva dva sklopa verifikacijskih testov:

- skladnostno testiranje (conformance testing),
- združljivostno testiranje (interoperability testing).

Funkcionalna, zmogljivostna in primerjalna testiranja se v procesu »IPv6 Ready« certifikacije ne izvajajo. V okviru programa IPv6 Ready je bilo certificiranih že prek 891 različnih produktov. Natančen in ažuriran seznam certificirane opreme je na spletni strani www.ipv6ready.org.

Danes IPv6 Forum še vedno predstavlja vodilno mednarodno organizacijo v postopkih testiranja in verifikacije, vendar pa njihovi programi predstavljajo določeno dilemo glede upravičenosti certifikacije, saj pogoji certificiranja IPv6 Ready niso povsem jasno določeni.

Program obrambnega ministrstva ZDA

Zaradi ohlapnih določil v segmentu produktov IPv6 je leta 2005 obrambno ministrstvo ZDA razvilo jasno in standardizirano definicijo »IPv6 Capable« ter temeljit testni program, ki omogoča validacijo zmogljivosti IPv6 za opremo IPv6, ki se bo uporabljala v omrežjih Obrambnega ministrstva ZDA (http://jitc.fhu.disa.mil/apl/ipv6.html). Program podaja tudi dokumentacijo zahtev in proces implementacije programa za certifikacijo produktov IPv6. Poleg tega so službe DoD IPv6 Transition Office, DoD Information Technology Standards Registry (DISR) in Interoperability Test Command (JITC) oblikovale še serijo treh dokumentov, ki zajemajo model certifikacije produktov za IPv6 zmogljivosti na področju:

- skladnosti (conformance),
- združljivosti (interoperability),
- zmogljivosti (performance),
- zagotavljanja informacijske varnosti (Information Assurance).

Program »IPv6 capable« opredeljuje 6 sklopov produktov IPv6:

- »Host«,
- »Network Appliance or Simple Server«,
- »Advanced Server«,
- »Router«,
- »Layer-3 Switch«,
- »Information Assurance Device«.

Pri razvoju teh dokumentov so sodelovali številni uradi in organizacije obrambnega ministrstva ZDA. S tem so oblikovali priznan in standardiziran profil IPv6 vlade ZDA, kot vzor pa ga je prevzel tudi Nacionalni inštitut za standardizacijo ZDA (NIST).

Program inštituta NIST

National Institute of Standards and Technology (NIST) je leta 2009 izdal metodologijo testiranja IPv6 (http://www.antd.nist.gov/usgv6/testing.html) deloma kot nadaljevanje programa certifikacije IPv6 in testnega programa vlade ZDA (USGv6 – A Profile for IPv6 in the U.S. Government), ki je namenjen za verifikacijo omrežnih rešitev javne uprave ZDA. Metodologija je namenjena kot priporočilo vsem akreditiranim in testnim laboratorijem za akreditacijo, standardne referenčne teste, merila validacije testnih metod in povratne mehanizme za nadgrajevanje kakovosti in konsistence testiranj na področju IPv6.

Dokument NIST podaja ogrodje za testiranje treh osnovnih tipov omrežnih vozlišč, kategoriziranih kot »hosts, »routers« in »network protection devices«, in sicer:

- metodo za skladnostno testiranje (Conformance Test methods) – preverja, ali je naprava skladna s standardiziranimi specifikacijami protokola,
- metodo za združljivostno testiranje (Interoperability Test methods) – preverja delovanje naprave v omrežju z napravami drugih proizvajalcev prek ločenih ali povezanih podomrežij, pri čemer je zahtevana potrditev interoperabilnosti naprave z najmanj tremi ali več komercialnimi implementacijami IPv6,
- metodo za testiranje omrežne zaščite (Network Protection Test methods), ki zahteva nastavljivost konfiguracij, beleženje, okoljsko varnost in ustrezno filtriranje paketov IPv6.

Dokument dodatno določa ogrodje za sledljivost testiranj in mehanizme za nadgrajevanje testnih postopkov v sodelovanju z uporabniki.

Testne metode zajemajo osnovne funkcionalnosti IPv6, npr. naslavljanje DHCP in IPv6, varnost, kakovost storitev, multicast, upravljanje omrežja in specifične tehnologije povezav. Proizvajalci opreme, ki implementirajo tehnologijo IPv6, morajo poleg tega preučiti in testirati tudi vsakršne spremembe, ki jih implementacija IPv6 povzroči na drugih obstoječih standardih.

V programu »UGSv6« so definirani 3 profili produktov IPv6:

- »Host Profile«,
- »Router Profile«,
- »Network Protection Device Profile«.

Dodatno pa specificira tudi kategorije funkcionalnih zahtev »IPv6 Capabilities«, ki določajo naslednje funkcionalne sklope:

- »IPv6 Basic«,
- »Routing Protocols«,
- »Quality of Service«,

- »Transition Mechanisms«,
- »Link Specific Capabilities«,
- »Addressing«,
- »IP Security«,
- »Network Management«,
- »Multicast«,
- »Mobility«,
- »Application Requirements«,
- »Network Protection Device Requirements«.

Specifikacije strokovnega sveta go6 ter delovne skupine go6 IPv6

Strokovni svet »go6« in delovna skupina »go6 IPv6 WG«, ki jo sestavljajo vidni slovenski strokovnjaki s področja internetnih sistemov, sta na pobudo širše internetne skupnosti pripravila seznam specifikacij podpore standardom RFC, s katerimi morajo biti skladne omrežne naprave IPv6, ki se bodo primarno uporabljale v omrežjih javne uprave Republike Slovenije. V priporočilu so produkti IKT razdeljeni v štiri sklope strojne opreme:

- gostitelj: odjemalec ali strežnik (host),
- stikalo L2 (L2 switch),
- usmerjevalnik (router),
- oprema za zagotavljanje omrežne varnosti (požarni zidovi, IDS, IPS ...).

Specifikacije podajajo samo seznam potrebnih standardov, podrobnih testnih metodologij in verifikacijskih procedur pa ne določajo.

Vzorčni model vključevanja specifikacij v razpise IKT javne uprave

Iz analize trenutnega stanja standardizacije ter verifikacije rešitev IPv6, ki sta bili narejeni v predhodnih poglavjih, lahko zaključimo, da še ne obstaja jasno določen pristop, ki bi ga lahko preprosto povzeli in neposredno vključili kot referenčno vodilo za pripravo razpisne dokumentacije pri nakupu opreme IKT za IPv6 javne uprave RS.

Pri problematiki bo treba tudi upoštevati, da se omrežja, ki sodijo pod okrilje Republike Slovenije, med seboj razlikujejo po velikosti, namembnosti, odprtosti ter varnostnih in zmogljivostnih karakteristikah, saj jih uporabljajo državni organi javnega značaja (državni portali) in profesionalne službe vlade Republike Slovenije (SOVA), ministrstva za obrambo (SV, URSZR, OVS) ter ministrstva za notranje zadeve (policija). Slednji sistemi presegajo obseg pričujočega dokumenta in potrebujejo dodatno poglobljeno analizo.

Odprte dileme

Pri pripravi razpise dokumentacije za različne ciljne omrežne segmente javne uprave bo potreben kompromis na več ravneh, ki ne bo upošteval samo tehničnih zahtev, ampak tudi varnostne, ekonomske, gospodarske, pravno formalne, v nekaterih primerih pa tudi politične posledice. Nekatere dileme so izpostavljene v nadaljevanju dokumenta.

Kateri sklop standardov uporabiti in za katere produkte?
Jedro standardov IPv6 je bilo sprejeto leta 2007 in predstavlja stabilen sklop specifikacij, ki se jih lahko vključi kot obvezujoče referenčne dokumente[1]. Odprta dilema, ki se jo lahko rešuje na različne načine, je, kateri nabor standardov zahtevati v razpisu za posamezen produkt IPv6:

- nabor standardov RFC, ki jih za posamezne skupine IPv6 produktov določa program »IPv6 Ready«,
- nabor standardov RFC in drugih priporočil, ki jih za produkte IPv6 določa program obrambnega ministrstva ZDA,
- nabor standardov RFC in drugih priporočil, ki jih za produkte IPv6 določa verifikacijski program NIST,
- specifikacije strokovnega sveta go6 ter delovne skupine go6 IPv6.

Izbran nabor standardov mora biti odvisen od značilnosti in zahtev ciljnega sistema, za katerega je oprema namenjena, v nekaterih primerih pa bo treba za posamezne posebne omrežne rešitve predstavljene specifikacije dodatno razširiti z lastnimi.

Ali mora biti oprema IPv6 ustrezno certificirana?
Do danes so se izoblikovali trije certifikacijski programi (IPv6 ready, DoD, NIST), ki pa med seboj niso popolnoma primerljivi, saj so bila upoštevana konceptualna izhodišča za različne ciljne sisteme: vojaški sistemi (DoD), sistemi javne uprave (NIST), generičen (IPv6 Ready). Programi se med seboj razlikujejo po:

- izhodiščnih definicijah produktov,
- vrsti in obsegu verifikacijskih testov,
- metodološkemu pristopu k izvajanju testov,
- ponovljivosti testnih procedur ter načinu akreditacije testnih laboratorijev.

Certifikacija IPv6 Ready predstavlja najbolj generičen pristop certifikacije, ki je bil narejen na ravni odprte skupnosti z mednarodnim konsenzom. Stopnja verifikacije, ki jo predstavlja logotip IPv6 Ready na produktu, končnim uporabnikom zagotavlja, da je oprema izdelana skladno s standardi ter da je preverjeno združljivostno delovanje z enim ali več sorodnih produktov. Certifikat torej ne odraža kvalitativnih parametrov, kot so funkcionalne, primerjalne ter zmogljivostne lastnosti, posameznega produkta.

Certifikacijska programa Obrambnega ministrstva ZDA »IPv6 capable« ter inštituta NIST »USGv6 profile« sta zahtevnost verifikacije še dodatno zaostrila, saj se poleg skladnostnega in združljivostnega preverjanja od produktov IPv6 zahtevajo tudi določene funkcionalne in zmogljivostne karakteristike. Certifikacijski program Obrambnega ministrstva ZDA »IPv6 capable« ozirom njegovi posamezni segmenti bi lahko tako pogojno predstavljal izhodišča za pripravo razpisnih pogojev Slovenske vojske (MORS), saj upoštevajo tudi smernice razvoja sistemov NATO (net-centric warfare), kjer je predvidena uporaba komercialnih civilnih produktov (COTS – Commercial Off the Shelf) v vojaških komunikacijskih sistemih (http://jitc.fhu.disa.mil/tst_time/docs/year/mar08.pdf). Prav tako pa bi lahko bil »USGv6 profil« referenčen koncept pri pripravi razpisih specifikacij javne uprave Republike Slovenije.

Ne glede na izbrani program certifikacije je treba omrežno opremo pred izborom oziroma vključitvijo v produkcijsko omrežje OBVEZNO zmogljivostno in funkcionalno verificirati v ustreznem akreditiranem laboratoriju. Slednjega lahko poleg obstoječih certifikacijskih programov IPv6 predstavlja akreditiran laboratorij proizvajalca opreme, dobavitelja, kupca ali pa verifikacijo izvede zunanja neodvisna ustanova.

Certifikacijska programa »IPv6 capable« in »USGv6 profile« podajata odličen referenčni koncept in zgled, kako se morajo ustanove državnega značaja na sistematičen in profesionalen način lotiti tehnične problematike uvajanja nove tehnologije, kot je npr. IPv6, v javne komunikacijske sisteme.

Primeri vključevanja specifikacij v razpise javne uprave

Zahteve po podpori IPv6 se lahko podajo na več načinov. Obdelali bomo tri primere:

1. Prvi je delo go6 strokovnega sveta ter slovenske IPv6 delovne skupine in poda specifikacijo podpore standardom RFC, s katerimi morajo biti skladne naprave, razdeljene na štiri skupine naprav.
2. Drugi je specifikacija testov, ki jih lahko opravijo proizvajalci s Forumom IPv6 in njegovim programom IPv6 Ready. Ta se deli na dve fazi, prva zajema testiranje in certifikacijo osnovnih protokolov, druga pa testiranje in certifikacijo naprednejših funkcionalnosti IPv6.
3. Tretja možnost je pa mešanica zgoraj opisanih možnosti.

Vse tri možnosti so opisane v sekcijah I., II. in III.

Pri specifikaciji zahtev lahko uporabimo prvo, drugo ali tretjo možnost, odvisno od potreb in zahtevane natančnosti podpore IPv6.

Sekcija I. – Zahteve, razdeljene na naprave in podporo pri integratorju (po predlogu IPv6 delovne skupine go6)

Predlog besedila za javne razpise z zahtevami o ustreznosti opreme IKT in ponudnikov storitve integracije za protokol IPv6
Vsa strojna oprema IKT mora podpirati protokola IPv4 in IPv6, pri čemer mora biti zagotovljena podobna zmogljivost delovanja na obeh protokolih, pri tem, da razlika v zmogljivosti ne bi smela biti večja kot ...% za vhodne, izhodne in/ali prehodne tokove podatkov ter pri prenos in obdelavi paketov med obema protokoloma.

(Opomba za naročnika: Za opremo razreda »high-end« priporočamo, da se navede maksimalna razlika 15 %. Za opremo razreda »enterprise« priporočamo največ 30 %. Za opremo razreda »consumer« priporočamo največ 40 %...)

Vsa programska oprema, ki po svoji naravi komunicira prek protokola IP, mora podpirati oba protokola (IPv4 in IPv6), pri čemer ne sme biti opazne razlike za uporabnika.

Angleška verzija besedila za mednarodne razpise:

All ICT hardware must support both the IPv4 and IPv6 protocols. Similar performance must be provided for both protocols. There should not be more than ...% difference in input, output and/or throughput data-flow performance, transmission and processing of packets between the two protocols.

(Notes for tender initiators: For high-end devices, we recommend to state a maximum difference of 15%. For enterprise grade devices, we recommend a maximum of 30%. For consumer grade devices, we recommend a maximum of 40%.)

Any software that communicates via the IP protocol must support both protocol versions (IPv4 and IPv6). The difference must not be noticeable to users.

Zahteve za podporo standardom

Strojna oprema IKT se v grobem lahko razdeli na štiri skupine:

- gostitelj: odjemalec ali strežnik (host),
- stikalo L2 (L2 switch),
- usmerjevalnik (router),
- oprema za zagotavljanje omrežne varnosti (požarni zidovi, IDS, IPS ...).

Zahteve za podporo standardom se delijo na nujne in opcijske. Oprema mora zadostiti nujnim zahtevam po standardih, opcijske zahteve pa prinašajo dodatne točke. Če strojna

oprema ne zadosti vsem nujnim zahtevam po podpori standardom, se upošteva kot neprimerna.

Zahteve za tip opreme »gostitelj»

Nujna podpora:

- osnovna specifikacija IPv6 (RFC2460),
- Basic IPv6 Addressing Architecture [RFC4291],
- Default Address Selection [RFC3484],
- ICMPv6 (RFC4443),
- DHCPv6 client (RFC3315),
- SLAAC (RFC4862),
- Path MTU discovery (RFC1981),
- neighbour discovery (RFC4861),
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213],
- Ipsec-v2 [RFC2401, RFC2406, in RFC2402],
- IKE version 2 (IKEv2) [RFC4306 in RFC4718],
- če je zahtevana podpora za mobilni IPv6, mora naprava v načinu »procesiranje« podpirati standarda MIPv6 [RFC3775] in »Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture [RFC4877]«,
- DNS protocol extensions for incorporating IPv6 into DNS resource records [RFC3596],
- DNS message extension mechanism [RFC2671],
- DNS message size requirements [RFC3226].

Opcijska podpora:

- popravljen ICMPv6 (RFC5095),
- Extended ICMP for multipart messages (RFC4884),
- SEND (RFC3971),
- SLAAC Privacy extensions (RFC4941),
- Stateless DHCPv6 (RFC3736),
- DS (Traffic class) (RFC2474 in RFC3140),
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193],
- Cryptographically Generated Addresses [RFC3972],
- Ipsec-v3 [RFC4310, RFC4303, in RFC4302],
- SNMP protocol [RFC3411],
- SNMP capabilities [RFC3412, RFC3413, RFC3414],
- Multicast Listener Discovery version 2 [RFC3810],
- Packetization Layer Path MTU Discovery [RFC4821].

Zahteve za tip opreme »stikalo» razreda »consumer«

Nujna podpora:

- MLDv2 snooping (RFC4541).

Opcijska podpora (za upravljanje):

- osnovna specifikacija IPv6 (RFC2460),
- basic IPv6 Addressing Architecture [RFC4291],
- Default Address Selection [RFC3484],
- ICMPv6 (RFC4443),
- SLAAC (RFC4862),
- SNMP protocol [RFC3411],
- SNMP capabilities [RFC3412, RFC3413, RFC3414].

Zahteve za tip opreme »stikalo» razreda »Enterprise/ISP«:

- Nujna podpora:
- MLDv2 snooping [RFC4541],
- DHCPv6 snooping [RFC3315],
- Router Advertisement (RA) filtering [RFC2462, RFC5006],
- Dynamic »IPv6 neighbour solicitation/advertisement» inspection [RFC2461],
- Neighbour Unreachability Detection [NUD, RFC2461] filtering,
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering.

Opcijska podpora (menedžment):

- IPv6 Basic specification [RFC2460],
- IPv6 Addressing Architecture basic [RFC4291],
- Default Address Selection [RFC3484],
- ICMPv6 [RFC4443],
- SLAAC [RFC4862],
- SNMP protocol [RFC3411],
- SNMP capabilities [RFC3412, RFC3413, RFC3414],
- IPv6 Routing Header [RFC2460, Next Header value 43] snooping,
- UPNP filtering.

Zahteve za tip opreme »usmerjevalnik«:

Nujna podpora:

- osnovna specifikacija IPv6 (RFC2460),
- basic IPv6 Addressing Architecture [RFC4291],
- Default Address Selection [RFC3484],
- ICMPv6 (RFC4443),
- SLAAC (RFC4862),
- MLDv2 snooping [RFC4541],
- Router-alert option (RFC2711),
- Path MTU discovery (RFC1981),
- Neighbour discovery (RFC4861),
- Classless Inter-domain routing [RFC4632],
- če obstaja zahteva po dinamičnem notranjem usmerjevalnem protokolu (IGP), se zahteva RIPng (RFC2080), OSPF-v3 (RFC5340) ali IS-IS (RFC5308). Naročnik specificira zahtevani protokol,
- Če je zahtevan OSPF-v3, mora naprava podpirati »Authentication/ Confidetiality for OSPF-v3« (RFC4552),
- če obstaja zahteva po protokolu BGP4, mora oprema ustrezati RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 in RFC2545,
- podpora za QoS (RFC2474 in RFC3140),
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213].
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891],
- Generic Packet Tunneling in IPv6 [RFC2473],
- če obstaja zahteva po 6PE, mora oprema podpirati »Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) [RFC4798]«,
- Multicast Listener Discovery version 2 [RFC3810],
- če je zahtevana podpora za mobilni IPv6, mora naprava v načinu »forwarding« podpirati standarda MIPv6 [RFC3775] in »Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture [RFC4877]«.

Opcijska podpora:

- popravljen ICMPv6 (RFC5095),
- DHCPv6 client/server (RFC3315),
- Extended ICMP for multipart messages (RFC4884),
- SEND (RFC3971),
- SLAAC Privacy extensions (RFC4941),
- Stateless DHCPv6 (RFC3736),
- DHCPv6 PD (RFC3633),
- [RFC2918] Route Refresh Capabilities for BGP-4,
- [RFC4360] BGP Extended Communities Attribute,
- (QOS) Assured Forwarding [RFC2597],
- (QOS) Expedited Forwarding [RFC3246],
- Generic Routing Encapsulation [RFC2784],
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193],
- Cryptographically Generated Addresses [RFC3972],
- ProSafe-v3 [RFC4310, RFC4303, in RFC4302],
- IPSec-v2 [RFC2401, RFC2406, in RFC2402],
- IKE version 2 (IKEv2) [RFC4306 in RFC4718],
- SNMP protocol [RFC3411],
- SNMP capabilities [RFC3412, RFC3413, RFC3414],
- SNMP MIBS for IP [RFC4293], Forwarding [RFC4292], IPsec [RFC4807], and DiffServ [RFC3289],
- DNS protocol extensions for incorporating IPv6 into DNS resource records [RFC3596],
- DNS message extension mechanism [RFC2671],
- DNS message size requirements [RFC3226],
- 127-bit IPv6 Prefixes on Inter-Router Links:
    - http://tools.ietf.org/html/draft-kohno-ipv6-prefixlen-p2p-01,
- Packetization Layer Path MTU Discovery [RFC4821].

Zahteve za tip opreme »omrežna varnost»

Oprema v tej sekciji se deli na 3 podskupine:

- požarni zid (oznaka FW),
- naprava za preprečevanje vdorov (oznaka IPS),
- aplikativni požarni zid (oznaka APFW).

Nujna podpora:

- osnovna specifikacija IPv6 (RFC2460) (FW, IPS, APFW),
- basic IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW),
- Default Address Selection [RFC3484] (FW, IPS, APFW),
- ICMPv6 (RFC4443) (FW, IPS, APFW),
- SLAAC (RFC4862) (FW, IPS),
- Router-alert option (RFC2711) (FW, IPS),
- Path MTU discovery (RFC1981) (FW, IPS, APWF),
- Neighbour discovery (RFC4861) (FW, IPS, APFW),
- če obstaja zahteva po protokolu BGP4, mora oprema ustrezati RFC4271, RFC1772, RFC4760 in RFC2545 (FW, IPS, APFW),
- če obstaja zahteva po dinamičnem notranjem usmerjevalnem protokolu (IGP), se zahteva RIPng (RFC2080), OSPF-v3 (RFC5340) ali IS-IS (RFC5308). Naročnik specificira zahtevani protokol (FW, IPS, APFW),
- če je zahtevan OSPF-v3, mora naprava podpirati »Authentication/ Confidetiality for OSPF-v3» (RFC4552) (FW, IPS, APFW),
- podpora za QoS (RFC2474 in RFC3140) (FW, APFW),
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW),
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW).

Funkcionalnosti, ki jih naprava omogoča pri protokolu IPv4, morajo biti primerljive s funkcionalnostmi pri protokolu IPv6 (če je, na primer, sistem za preprečevanje vdorov sposoben pri protokolu IPv4 delovati v načinu L2 in L3, naj to velja tudi za promet IPv6. Če je, na primer, požarna pregrada pri delovanju v gruči sposobna seje IPv4 sinhronizirati med vsemi člani gruče, potem naj to velja tudi za promet IPv6).

Opcijska podpora:

- popravljen ICMPv6 (RFC5095),
- DHCPv6 client/server (RFC3315),
- Extended ICMP for multipart messages (RFC4884),
- SEND (RFC3971),
- SLAAC Privacy extensions (RFC4941),
- Stateles DHCPv6 (RFC3736),
- DHCPv6 PD (RFC3633),
- [RFC1997] BGP Communities Attribute,
- [RFC3392] Capabilities Advertisement with BGP-4,
- (QOS) Assured Forwarding [RFC2597],
- (QOS) Expedited Forwarding [RFC3246].
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193],
- Cryptographically Generated Addresses [RFC3972],
- Ipsec-v3 [RFC4310, RFC4303, in RFC4302],

- OSPF-v3 (RFC5340),
- Authentication/Confidetiality for OSPF-v3 (RFC4552),
- Generic Packet Tunneling in IPv6 [RFC2473,
- Ipsec-v2 [RFC2401, RFC2406, in RFC2402],
- IKE version 2 (IKEv2) [RFC4306 in RFC4718],
- SNMP protocol [RFC3411],
- SNMP capabilities [RFC3412, RFC3413, RFC3414].
- DNS protocol extensions for incorporating IPv6 into DNS resource records [RFC3596],
- DNS message extension mechanism [RFC2671],
- DNS message size requirements [RFC3226],
- Using IPSec to Secure IPv6-in-IPv4 Tunnels [RFC4891],
- Multicast Listener Discovery version 2 [RFC3810],
- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode),
- Packetization Layer Path MTU Discovery [RFC4821].

Zahteve po podpori IPv6 v programski opremi

Vsa programska oprema mora poleg protokola IPv4 podpirati tudi protokol IPv6 in biti sposobna komunicirati prek njega. Če se znotraj programske opreme nastavljajo omrežni parametri (lokalne ali nastavitve oddaljenih strežnikov), mora programska oprema imeti tudi konfiguracijski del za IPv6 del protokolnega sklada.

Funkcionalne sposobnosti se ne smejo bistveno razlikovati med IPv4 in IPv6, uporabnik ne sme opaziti razlike med komunikacijo programske opreme z omrežjem po IPv4 ali IPv6.

Zahteve po usposobljenosti ponudnika storitev integracije

Ponudnik storitev integracije opreme v omrežje naročnika mora imeti vsaj tri zaposlene, ki imajo veljavne certifikate proizvajalcev opreme o usposobljenosti upravljanja s prodano opremo. Ti certifikati morajo vsebovati splošno poznavanje protokola IPv6, načrtovanje omrežij s protokolom IPv6 ter zagotavljanje varnosti na protokolu IPv6. Če se pri integraciji in nameščanju opreme izkaže, da integrator ni dovolj usposobljen in sposoben opreme pravilno integrirati v omrežje in vzpostaviti normalne komunikacije IPv6, se pogodba razdre in postane nična.

Definicija pravilne integracije, časovni okviri ter stopnja motenja omrežja med nameščanjem opreme so stvar dogovora med naročnikom in ponudnikom storitve integracije.

Priporočljivo je tudi, da ima ponudnik storitev integracije opreme v omrežje v podjetju tudi zaposlene, ki imajo širše znanje in certifikate iz IPv6, kot ga ponujajo certifikati proizvajalcev opreme. Ti certifikati so lahko pridobljeni pri neodvisnih ponudnikih izobraževanj, ki niso vezani na proizvajalce opreme. Za takšna znanja in certifikate lahko naročnik v razpisu ponudi dodatne točke.

Ponudnik mora podpisati obrazec o tehnični usposobljenosti za načrtovanje, gradnjo in integracijo opreme IKT v omrežja IPv6.

I Z J A V A

O TEHNIČNI USPOSOBLJENOSTI ZA NAČRTOVANJE, GRADNJO IN INTEGRACIJO OPREME IKT V OMREŽJA IPv6

Ponudnik_____
Naslov_____

Izjavljamo pod kazensko in materialno odgovornostjo:

- da imamo zaposlenih zadostno število ljudi za opravljanje storitev,
- da so zaposleni strokovno usposobljeni za svoje delo – načrtovanje, gradnjo in integracijo opreme IKT v omrežja IPv4 in IPv6,
- da je ponujena storitev kakovostna in ustreza zahtevam iz razpisne dokumentacije.

V _____, dne_____

Žig in podpis ponudnika

Sekcija II. – Testiranje in certifikacija naprav po sistemu IPv6 Foruma z naslovom »IPv6 ready«

IPv6 Forum je evropska organizacija in združenje različnih poglavij IPv6 Foruma po državah. Med drugim so sestavili tudi dokaj obsežen sistem testiranja in certifikacije opreme, ki ga zdaj izvajajo različni laboratoriji po svetu. Trenutno je v bazi »IPv6 ready«

pod phase-1 ali phase-2 že 871 vpisov, kar pomeni kar obsežno zbirko opreme, ki ustreza vsaj osnovnim zahtevam IPv6.

Da bi zadostili zahtevam phase-1, je treba opraviti nekaj čez 170 testov.
Seznam vseh testov, ki so potrebni za fazo 1 in fazo 2 (za fazo 1 so potrebni samo nekateri):
[1]

Natančna specifikacija poteka in zahtev testiranj je opisana v:
http://ipv6ready.org/docs/Core_Conformance_Latest.pdf

Seznam certificirane opreme najdemo na:
https://www.ipv6ready.org/db/index.php/public

Predlagano besedilo za razpise:
»Oprema IKT, ki podpira in komunicira prek protokola IPv4, mora podpirati tudi protokol IPv6 in mora biti prek njega sposobna normalno komunicirati v omrežju z drugimi napravami IPv6. Podpora osnovnim protokolom IPv6 mora biti preverjena in certificirana v programu IPv6 Ready, v katerem mora pridobiti vsaj logotip certifikacije »Phase-1« oziroma »IPv6Ready Silver logo«. Certifikacija »Phase-2« ali »IPv6Ready Gold logo« opremi prinese dodatnih 10 % točk pri končnem ocenjevanju.«

Predlagano besedilo za razpise v angleškem jeziku:
»ICT equipment that supports and communicates over the IPv4 protocol must also support the IPv6 protocol and must be able to communicate with other devices over IPv6. Basic IPv6 support must (should) be verified and certified by the IPv6ready program with a »Phase-1« logo certificate. A »Phase-2« logo certificate adds additional points (+10%) in the tender evaluation procedure.«

Sekcija III. – Souporaba obeh načinov specifikacij z zahtevami

Včasih se zgodi, da oprema še ni bila podvržena testiranju IPv6 Ready in za takšno opremo ne bi bilo smotrno, da se a priori označi kot neprimerno, saj je mogoče čisto primerna in ustrezno izpolnjuje vse normative IPv6, le testirali je še niso. V takšnem primeru lahko naročnik zahteva preverjanje ustreznosti opreme po metodi IPv6 Ready v naših laboratorijih, ki so usposobljeni in akreditirani za takšna preverjanja, ali pa preprosto zahteva certifikacijo IPv6 Ready in v primeru, da oprema še ni bila podvržena tovrstnemu testiranju, navede zahteve po podpori standardov RFC iz ustreznega dela I. sekcije tega dokumenta.

Predlagano besedilo za razpise:

»Oprema IKT, ki podpira in komunicira prek protokola IPv4, mora podpirati tudi protokol IPv6 in mora biti prek njega tudi sposobna normalno komunicirati v omrežju z drugimi napravami IPv6. Podpora osnovnim protokolom IPv6 mora biti preverjena in certificirana v programu IPv6 Ready, v katerem mora pridobiti vsaj logotip certifikacije »Phase-1« oziroma »IPv6Ready Silver logo«. »Phase-2« oziroma certifikacija »IPv6 Ready Gold logo« prinese opremi dodatnih 10 % točk pri končnem ocenjevanju. Če oprema, ki je predmet tega razpisa, še ni bila podvržena testiranju programa IPv6 Ready, lahko ponudnik opremo preizkusi v enem od slovenskih laboratorijev, ki ponujajo testiranje po programu IPv6 Ready in predloži rezultate testiranja. Če to ni mogoče, se ustreznost opreme ocenjuje po podpori standardov v spodnji tabeli:

[tabela nujne in opcijske podpore za ustrezen tip opreme]

Predlagano besedilo za razpise v angleškem jeziku:

»ICT equipment that supports and communicates over the IPv4 protocol must also support the IPv6 protocol and must be able to communicate with other devices over IPv6. Basic IPv6 support can be verified and certified by the IPv6ready program with a »Phase-1« logo certificate. A »Phase-2« logo certificate adds additional points (+10%) in the tender evaluation procedure. If the equipment has not been put through the IPv6Ready testing procedure then bidder can put the equipment to test in one of Slovenian laboratories, which offer IPv6Ready testing program and enclose the testing results. If this is not possible, equipment must comply at least with list of RFCs listed below:

[appropriate list of selected mandatory and optional RFCs from 1st option]

9. Animiranje ponudnikov vsebin (akcije, spodbude ...)

This section deals again with the biggest problem: adoption and incentives for adoption. Here experts provide some useful ideas and insights for companies thinking about adoption. It also highlights consequences for late comers. It is always useful to listen to experts and while the recommendations may not fit every case, the document is written by absolute experts in the area and is worth a consideration.

Izzivi ponudnikov vsebin

Kot smo že opisali, je v zadnjem času opaziti vse večji razkorak med pripravljenostjo ponudnikov povezljivosti (ISP) in ponudnikov vsebin (content providers) na uvajanje protokola IPv6. V nekaterih primerih, predvsem v okoljih, ki uporabljajo odprto kodo, je prehod v okolje IPv6 skorajda trivialen in ne posega v aplikacijsko kodo.

Primer: spletna aplikacija v jeziku PHP in izvajana v okolju spletnega strežnika Apache, ob prehodu v okolje IPv6 skorajda ne zahteva popravkov (če le ne hrani numeričnih naslovov odjemalcev v slabo dimenzionirani bazi podatkov). Tudi aplikacija, napisana v razvojnem okolju ASP.NET na Microsoftovem spletnem strežniku, je načelno pripravljena za prehod v okolje IPv6.

Nasprotni primer: Aplikacija, napisana v nižjem programskem jeziku (npr. C/C++), ki neposredno dostopa do transportnega ali omrežnega sloja (TCP/IP), lahko potrebuje obširne spremembe in dolgotrajno testiranje.

Kje je torej problem? Majhni ponudniki vsebin so odvisni od ponudnikov spletnega gostovanja (web hosting), ki so v mnogih primerih komajda osvojili znanja, potrebna za izvedbo zanesljivega gostovanja v okolju IPv4 in ki zaradi nizkih cen gostovanja nimajo sredstev, potrebnih za izobraževanje kadrov, nadgradnjo strojne in programske opreme in izvedbo prehoda. Ti ponudniki spletnega gostovanja bodo v nekaj letih prisiljeni opraviti prehod v okolje IPv6 (marsikateri od njih pa bo počasi odmrl), kar pa agilnih ponudnikov vsebin ne bo prav hudo prizadelo, saj že danes obstaja nekaj globalnih alternativ (Google). Seveda so lahko z nacionalnega stališča problematične selitve lokalnih vsebin v tujino, s tem povezane zakasnitve in odvisnost od tujih ponudnikov.

Večji ponudniki vsebin (z lastnimi strežniki) bodo zaradi zatiskanja oči pred izzivi IPv6 izgubljali konkurenčni položaj (predvsem tisti, ki v veliki meri uporabljajo internet v svojem poslovnem procesu, kot so na primer spletne trgovine ali banke), dolgoročno pa jih bo zastarelost njihove informacijske infrastrukture prisilila v hitre ter zato slabše planirane in posledično dražje nadgradnje (podobno, kakor so bile slovenske banke po desetletjih

zanemarjanja lastne infrastrukture IT prisiljene naenkrat izvesti precej drag prehod v evroobmočje).

Javna uprava kot pospeševalnik uvajanja storitev IPv6

Slovenija ima zaradi pravil Evropske skupnosti precej omejene možnosti neposrednih spodbud in investicij, seveda pa lahko posredno (skozi sistem javnih naročil) pritiska na izvajalce teh naročil (podjetja v sektorju IT, od programerskih hiš do ponudnikov omrežnih rešitev) in jih tako pripravi na uspešen prehod v okolje IPv6. S posredno prisilo državnih institucij bodo ti izvajalci osvojili osnove okolja IPv6, prilagodili svoje aplikacije delu v tem okolju (ali pa jih poenostavili do te mere, da bodo postale neodvisne od omrežnega in transportnega sloja, kar je še boljša rešitev) in tako postali pripravljeni za trenutek, ko bodo tudi drugi ponudniki vsebin začutili potrebo po prehodu v okolje IPv6.

Za uspešno izvajanje pritiska na sektor IT je nujno, da vsi javni razpisi s tega področja nedvoumno zahtevajo polno delovanje nove aplikacijske in omrežne opreme v okolju IPv6, oziroma, kjer to ni mogoče, uvedejo delovanje v okolju IPv6 kot enega od pomembnih faktorjev pri vrednotenju ponudb na javnih razpisih.

Dodatno spodbujanje prehoda v okolje IPv6 lahko opravijo tudi razpisi Tehnološke agencije, Ministrstva za visoko šolstvo, znanost in tehnologijo in evropskih skladov. Te institucije bi morale poleg spodbujanja drugih tehnologij v okolju IT spodbujati tudi prilagajanje omrežne in aplikacijske infrastrukture okolju IPv6, morda še zlasti s poudarkom na aplikacijski infrastrukturi in migraciji obstoječih spletnih rešitev v okolje dual-stack.

Storitve v oblaku

Računalništvo v oblaku je oblika računalništva, pri katerem so samorazširljivi, večinoma virtualizirani računalniški viri na voljo kot vrsta storitev prek javnega interneta. Poznamo nekaj različnih računalniških storitev v oblaku:

- SaaS (Software as a service) – storitev ponujanja programske opreme,
- IaaS (Infrastructure as a service) – storitev ponujanja infrastrukture,
- DaaS (Desktop as a service) – storitev ponujanja računalniškega namizja,
- .....

Na splošno za vse storitve iz oblaka velja skupen sinonim XaaS (Anything as a Service). Trenutno vse rešitve XaaS v okolju IKT veljajo za vroče žemljice. Veliko se govori, a takšnih storitev in implementacij v realnem okolju je bolj malo. Smernice razvoja spletnih storitev se gibljejo k različnim arhitekturam storitev v oblaku. Veliko proizvajalcev infrastrukture v oblaku je še vedno v raziskovalno-razvojnem stanju. Področje razvoja infrastrukture in storitev v oblaku je idealno področje za adaptacijo internetnega protokola

IPv6. Nespametno in stroškovno neekonomično je razvijati storitve prihodnosti na protokolu preteklosti. Ideja podpore protokola IPv6 v infrastukturah oblaka je vsekakor vredna podpore in diskusije in lahko postane lep primer dobre prakse. Vodilni ponudnik storitev v oblaku podjetje Google ima celotno infrastrukturo že pripravljeno za ponujanje storitev na protokolih IPv4 in IPv6, vsi drugi konkurenčni ponudniki pa se aktivno ukvarjajo s podporo slednjemu. Za podjetja, ki razvijajo storitve v oblaku, je priložnost in hkrati tudi konkurenčna prednost, če bodo njihove rešitve hkrati podpirale protokola IPv4 in IPv6.

Priložnosti internetnih iskalnikov

S težavo nezainteresiranih in samozadostnih ponudnikov vsebin in storitev se soočamo širom po svetu, IPv6 se počasi začenja uvajati pri ponudnikih dostopa do interneta, ponudniki vsebin pa še vedno večinoma ignorirajo prihajajoče spremembe.

Osnovno načelo ponudnikov vsebin na internetu je tipično zaslužek. Imamo več tipov vsebin, nekateri ponujajo novice in članke ter služijo z oglaševanjem, drugi pa v svojih vsebinah na spletu ponujajo svoje storitve – in to je dejansko lahko karkoli, od potovalne turistične agencije, ki ponuja počitnice v Grčiji, pa vse do kovaških mojstrov iz Krope, ki kujejo žeblje in podkve. Vse se prej ali slej znajde na internetu.

Podobne storitve, vsebine ali predmete na internetu ponuja tudi njihova konkurenca, kar je edino pravilno in v skladu z duhom konkurenčnosti. Ker si iskanja po internetu zadnja leta ne predstavljamo brez iskalnika Google, se je na tem področju razvila prava vojna med ponudniki vsebin, kdo bo po Googlovih »pravilih« pripravil in priredil svoje vsebine na tak način, da bodo v rezultatih iskanja čim višje. Temu se reče konkurenčni boj in prav je tako. Tista stran, ki bo bolje optimizirana, bo v iskalniku kotirala višje za določene ključne besede.

Iz tega se je razvil čisto nov posel, SEO (Search Engine Optimisation). To je veda in znanje o optimizaciji spletnih strani, da se uvrščajo čim višje na strani z iskalnimi zadetki za določene želene iskalne fraze ali besede. Ker se vedno najdejo nove »luknje« v optimizaciji, Google vedno znova posodablja in spreminja pravila in algoritme, po katerih se vsebine razvrščajo v rezultatih iskanja. Podjetja, ki stremijo po boljši poziciji in zaslužku, pa so pripravljena narediti vedno več, da bi bila pred tekmeci v iskalniku Google, oziroma na strani z iskalnimi rezultati.

Zahteve iskalnika Google so, da so vsebine relevantne, da je uporabniška izkušnja strani, ki jih predlaga prve, dobra. Zato obstajajo določena pravila, katerih se moramo držati.

Čez nekaj časa bo začelo zmanjkovati naslovov IPv4 in ne vemo, kaj se bo takrat dogajalo. Zakaj torej Google ne bi kot enega od meril za razvrščanje upošteval tudi, ali je vsebina dostopna iz omrežij IPv4 in IPv6, če ima zapis A in AAAA? To merilo bi lahko

upoštevali kot »future-proof«. Poglavitno bi bilo, da bi Google to javno oznanil, da bodo višje uvrščene strani in vsebine, do katerih se dostopa prek obeh protokolov.

V tem trenutku se zgodi plaz prehoda vsebin na omrežja IPv6, saj nihče noče zamuditi priložnosti, da bi bil bolje uvrščen, kakor je zdaj, nikakor pa slabše, saj to pomeni, da jih je konkurenca prehitela. Ponudniki vsebin bi verjetno takoj zahtevali povezljivost IPv6 do njihovih strežnikov, predvsem pa čim hitrejšo dejansko pojavnost na obeh protokolih. V vojno SEO lahko dodamo še en koristen element – vsebino ponujamo v obeh internetih.

Google je res največji internetni iskalnik, ni pa edini. S to spodbudo lahko začnemo že pri nas in predlagamo našemu najbolj uporabljanemu internetnemu iskalniku Najdi.si, da uvede takšno merilo pri razvrščanju vsebin na strani z iskanimi zadetki. Predvideva se lahko, da bi od 5 % do 10 % dodatka na dosežene točke pri ocenjevanju vsebine strani iskalnik lahko dodal, če je dosegljiva iz obeh omrežij.

Spodbujanje inovativnosti in kreativnosti z nagradnimi natečaji

Nemčija in Japonska sta za povečevanje interesa pri programerjih, snovalcih omrežij in ponudnikih vsebin posegli k mehanizmom, ki spodbujajo tekmovalnost in kreativnost – razpisali so natečaj za najboljšo aplikacijo IPv6 – pa naj bo to program, ki teče na končnih napravah (PC, telefon) ali pa sistem aplikacij, ki teče na strežnikih. V bistvu se je za nagrado lahko potegovala skoraj vsaka inovativna kompleksnejša uporaba IPv6 v aplikativne namene.

V Nemčiji je bil natečaj izveden v okviru srečanja IPv6 Council, ki je potekalo na inštitutu Hasso-Platnner v mestu Potsdam, glavno nagrado 10.000 evrov je pa odnesel Gert Doering s predelavo mehanizma OpenVPN za podporo navidezno-resničnim zasebnim omrežjem tudi za promet IPv6.

Pristojnim institucijam predlagamo, da se tudi pri nas zbere sponzorska sredstva in priredi podoben natečaj. S tem bi v veliki meri pritegnili inovativne posameznike in uveljavljena podjetja, ki se ukvarjajo s ponujanjem vsebin na internetu.

Slovenski IPv6 summiti so srečanja v soorganizaciji Arnesa, LTFE in Zavoda Go6. Organizirana so dvakrat letno in združujejo zainteresirano javnost, državne ustanove in agencije, industrijo ter operaterje, namenjena pa so promociji, pospeševanju uvedbe in izobraževanju na področju IPv6. Razmisliti bi bilo vredno, ali je mogoče Slo IPv6 summit primeren dogodek, da se v njegovem okviru izpelje takšen natečaj.

Priloga 1: Predlog za internetne iskalnike (v angleškem jeziku), avtorja: Sander Steffann in Jan Žorž:

Abstract
Deployment and adoption of IPv6 is slow at this point in time. This can be a risk for future growth of the internet. One of the observed obstacles is that content providers are waiting for IPv6 viewers, and viewers are waiting for IPv6 content. We propose a slight change the search engine scoring algorithms to stimulate content providers to make their content accessible over IPv6.

Proposed change
We propose that search engines check whether a website is available over both IPv4 and IPv6. Having the same content available over both lower level protocols is the situation that will give the IPv4 to IPv6 transition the largest chance of succeeding. The way to determine if a website has 'good' IPv4 and IPv6 support is an implementation detail of the search engine.

Websites that are available over both protocols should then get some kind of bonus when compared to websites available over only IPv4 or IPv6. One possible idea is to use this as a tiebreaker when two pages get the same score based on the original scoring algorithm. Another possibility is to give the website a 5% bonus in the scoring algorithm. This choice is an implementation detail of the search engine.

The search engine operator should then make it publicly known that IPv6 support will have a positive impact on the search engine scoring algorithm.

Pros
This will stimulate website owners to make their websites available over IPv6, which benefits the whole internet community. For cases where the website owner makes use of services from a separate website hoster – this hoster will also be stimulated to support IPv6. It will also send a signal that the search engine operator sees IPv6 support as being important for the future of the internet. Improving the future internet is also in the best interest of the search engine operator itself, as their business is based on the content available on the internet.

Cons
This proposal changes the scoring algorithm of the search engine, which is a very important part of the quality that the search engine provides. Using IPv6 support only as a tiebreaker or as a small component in this algorithm minimizes the impact. Another con can be that the public will see the search engine operator as pushing a technology instead of focusing on returning the search results that are 'best' for the end user. A counter argument to this can be that making content available over IPv6 is in the long term in the users' best interest.

10. Kako poskrbeti za dvig ozaveščenosti

What is the road map going to be? This section provides an very interesting perspective on the future and how the transition can be undertaken. At places this section picks up old ideas how the fathers and mothers of IPv6 thought a transition may happen. This has not turned out to be the case, and only the future will show how accurate this road map could predict the future. Nevertheless, this section is a detailed discourse into strategies that might make a difference. Awareness of the problem is certainly the first step, market incentives have been a focus of the whole document, and here the experts bring everything together.

Za dvig ozaveščenosti o IPv6 v Sloveniji je leta 2008 začela skrbeti pobuda go6, ki je kmalu prerasla v neprofitni zavod go6 in se strateško povezala z ustanovama Arnes in LTFE. Od takrat se je ozaveščenost o izčrpanju naslovnega prostora IPv4 in problematiki prepočasnega uvajanja IPv6 v storitve in omrežja zelo dvignila na slovenski ravni, a še vedno menimo, da to ni dovolj. Ozaveščenost in realna dejanja včasih niso čisto usklajena, saj je dokazano človeško nagnjenje, da bomo za probleme poskrbeli takrat, ko nas bodo zadeli in zaboleli.

Problematiko obravnavamo v naslednjih sklopih:

- Dvigovanje ozaveščenosti pri ponudnikih dostopa
- Dvigovanje ozaveščenosti v poslovnih okoljih
- Dvigovanje ozaveščenosti v državni in javni upravi
- Dvigovanje ozaveščenosti v širši javnosti
- Primeri ozaveščanja v preteklosti
- Predlogi za dvigovanje ozaveščenosti v prihodnosti

Dvigovanje ozaveščenosti pri ponudnikih dostopa

Najhitreje so se uvedbe lotili ponudniki dostopa do interneta. Ti so največji porabniki IP naslovnega prostora, obenem pa jih bo pomanjkanje naslovov IPv4 najbolj in najprej prizadelo. Vsakič, ko priklopijo novega uporabnika, mu morajo dodeliti dinamični ali statični naslov IP. Prav tako je s priklopom poslovnega uporabnika ali uporabnika na najeti povezavi – ti tipično za povezavo zahtevajo statičen naslov IPv4 in nabor naslovov IPv4 za svoje internetne strežnike in storitve. Nekateri ISP-ji v Sloveniji že ponujajo domorodni IPv6 poslovnim strankam na najetih povezavah, za dostop do rezidenčnih uporabnikov prek xDSL, FTTH ali kabelskih tehnologij pa bo treba počakati na uvedbo IPv6 v naprave CPE.

Kabelski operaterji v veliki večini primerov samo preprodajajo dostop do interneta obstoječih ponudnikov.

Ozaveščenost ponudnikov dostopa do interneta se trenutno že dviguje na polletnih slovenskih srečanjih IPv6 v so organizaciji Zavoda go6, Arnesa in LTFE. Apek ima seznam registriranih operaterjev, organizatorji summitov IPv6 pa lahko povabijo na dogodek vse operaterje.

Dvigovanje ozaveščenosti v poslovnih okoljih

Do potrebnega zavedanja prehoda na IPv6 še ni prišlo v podjetjih in pri ponudnikih vsebin in storitev. O ponudnikih vsebin je v tem dokumentu napisano celo poglavje, zato bi se osredotočili na poslovne stranke, velika, srednja in mala podjetja.

V velikem številu primerov kadra IT iz podjetij, ki niso neposredno povezana z IT, je problem pomanjkanje znanja, saj ne čutijo potrebe po uvedbi IPv6 v svoja poslovna okolja. Še več, zaradi preobremenjenosti z drugimi izzivi je glede na izkušnje s podobnimi prelomnimi dogodki v preteklosti (leto 2000, uvedba evra) pričakovati, da se bodo ta podjetja lotila problemov IPv6 takrat, ko bo že skoraj prepozno. Tudi dejstvo, da večina teh podjetij IPv6 realno še nekaj let ne bo potrebovalo, ne vpliva pozitivno na njihovo pripravljenost na začetek uvajanja IPv6 v njihovo okolje.

Podjetja, ki niso ponudniki dostopa do interneta, se bodo z IPv6 srečala v treh korakih:

- Ko bodo ponudniki dostopa do interneta začeli dodeljevati rezidenčnim uporabnikom naslove Pv6 (1-2 leti, v Sloveniji morda še pozneje), bo večina vsebine še vedno dostopne predvsem prek protokola IPv4. Dostop odjemalcev IPv6 do vsebin IPv4 bo takrat predvsem problem ponudnikov dostopa do interneta, ki bodo morali ta problem reševati z enim od tranzicijskih mehanizmov (na primer NAT64).

  V tej fazi večina podjetij še ne bo občutila vpliva IPv6, saj večinoma svojim strankam ponujajo le klasične spletne storitve s protokolom HTTP ali HTTPS, oba protokola pa brez težav delujeta z vsemi tranzicijskimi mehanizmi. Manjše težave bodo imela le tista podjetja, ki strankam ponujajo napredne storitve, kot je govor-čez-internet na zahtevo (click-to-talk). Takšnih podjetij v Sloveniji žal ni veliko; še vedno je veliko preprosteje (in ceneje) objaviti brezplačno telefonsko številko (s predpono 080) na spletnih straneh podjetja.

  Opomba: Tisti poslovni uporabniki, ki omogočajo svojim zaposlenim prek interneta varen dostop v zasebno omrežje s tehnologijo IPsec, se bodo s problematiko IPv6 verjetno srečali prej kakor drugi, saj je dostop odjemalca IPv6 do koncentratorja IPsec, ki podpira samo IPv4, precejšen tehnični izziv. Če namesto tehnologije IPsec

uporabimo tehnologijo SSL, teh težav ni več. Tehnologija SSL počasi izpodriva tehnologijo IPsec tudi zaradi preprostejšega prehajanja požarnih pregrad.

- Ko bo večina zanimive vsebine dostopne tudi s protokolom IPv6, bodo ponudniki dostopa do interneta prenehali zagotavljati dostop do vsebin IPv4 odjemalcem, ki imajo samo naslove IPv6 (5 let ali več). Takrat bodo tista podjetja, ki svojih vsebin še ne bodo ponujala v obeh okoljih (IPv6 in IPv4) imela resne težave. Zavedati se moramo, da je internetna konkurenca neusmiljena, obiskovalci spletnih strani pa neverjetno neučakani – če vsebine ne bodo dobili tam, kjer jo pričakujejo, bodo z nekaj kliki našli alternativnega ponudnika vsebin ali storitev.

- V zadnji fazi (ki jo bomo verjetno dosegli šele v naslednjem desetletju), bodo nekatere vsebine na internetu dostopne le s protokolom IPv6. Takrat bodo tisti poslovni uporabniki, ki še ne bodo uvedli protokola IPv6 v svoje poslovno okolje, naleteli na hude probleme. Nekateri od njih se bodo verjetno poskušali izogniti spremembam z dodatnimi triki, kot je uporaba posredniških strežnikov HTTP (ki omogočajo odjemalcem IPv4 dostop do vsebin IPv6 s protokolom HTTP ali HTTPS). Ker lahko pričakujemo, da bo v tem času (tudi zaradi uvajanja protokola IPv6 in ukinjanja prevajanja naslovov) vse več spletnih storitev uporabljalo neposredno komunikacijo med odjemalci, bo tudi uporaba posredniških strežnikov HTTP močno omejevala komunikacijske možnosti takšnih podjetij in zmanjševala njihovo konkurenčnost.

  Opomba: Glede na to, da so pred nekaj leti nekatera slovenska podjetja za dostop do elektronske pošte še vedno uporabljala več kot 30 let star protokol SNA in odjemalce na centralnem računalniku IBM, lahko podobno vedenje (in zatiskanje oči pred zmanjševanjem konkurenčnosti) pričakujemo tudi v prihodnje.

V nasprotju z že omenjenimi preteklimi prelomnimi dogodki (leto 2000, uvedba evra) ima uvajanje protokola IPv6 še eno težavo: ni »prelomnega datuma«, po katerem bi stari internet (ki uporablja protokol IPv4) prenehal delovati. Uvajanje novih protokolov zaradi hipotetičnega potencialnega zmanjševanja prihodnje konkurenčnosti in predvsem s tem uvajanjem povezani (prav nič hipotetični) stroški (delo, oprema, izobraževanje) bo za vodstvo marsikaterega podjetja prevelik zalogaj.

Omenimo še, da je v večini podjetij omrežna infrastruktura vsaj delno pripravljena na uvajanje IPv6 (treba jo je le pravilno nastaviti), prav tako IPv6 podpira večina delovnih postaj (vsaj tiste z operacijskimi sistemi Windows XP, Vista, Windows 7, Mac OSX all Linux), marsikatera aplikacija pa nikoli ne bo zrela za prehod v okolje IPv6 – tudi zaradi tega, ker se še vedno srečujemo s problemi slabo dokumentiranih aplikacij, zastarelih razvojnih okolij in izgubljene izvorne kode.

Kaj lahko torej storimo? Nedvomno je treba začeti s široko zastavljeno akcijo propagiranja protokola IPv6 (tako kot se ravno v tem času odvija akcija prehoda na digitalno televizijo), ki bo namenjena tako rezidenčnim uporabnikom kot tudi inženirjem v okolju IT, še predvsem pa vodilnim delavcem v podjetjih. Tu morajo pomembno vlogo odigrati stanovska združenja vodilnih delavcev, ki navadno precej dobro (in včasih zelo vidno) skrbijo za njihove interese, pa tudi gospodarske in obrtno-podjetniške zbornice, ki naj bi skrbele za konkurenčnost svojih članov.

Ob vzbujanju zanimanja za protokol IPv6 in vsaj začetnega razumevanja, da pomeni zanemarjanje tega protokola v prihodnosti izgubo konkurenčnosti, moramo zagotoviti lahko dostopno izobraževanje, ki naj obiskovalcem v nekaj urah predstavi vsaj osnove protokola IPv6.

V okviru sedmega okvirnega razvojno-raziskovalnega programa Evropske unije se je 31. avgusta 2010 zaključil dvoletni projekt 6Deploy. Cilj projekta 6Deploy je bilo širjenje osnovnih znanj in zavedanj na področju IPv6. Ker se je projekt izkazal kot izjemno uspešen način predajanja znanja in osveščanje javnosti, je bila sprejeta odločitev, da se projekt nadaljuje (6Deploy2). Zavedamo se, da ne smemo posegati na področja, kjer slovenska podjetja komercialno ponujajo izobraževanje o IPv6, v večini primerov so to izobraževanja ponudnikov strojne opreme – zato predlagamo, da se pod okriljem države organizira izobraževanje po predlogi 6Deploy, osnovne celodnevne delavnice o novostih, ki jih prinaša protokol IPv6, udeležba na delavnicah je za vsakogar brezplačna, izvedlo bi se pa delavnice v različnih večjih slovenskih mestih:

- Ljubljana,
- Koper,
- Nova Gorica,
- Novo Mesto,
- Celje,
- Maribor,
- Kranj,
- Murska Sobotal
- Krško,
- Velenje.

Poskrbeti bo treba za finančno konstrukcijo ter pokrivanje stroškov najema prostorov, hrane in predavateljev. Za to bi lahko bila zainteresirana država, po drugem scenariju so pa to lahko podjetja iz industrije, katerim so takšni dogodki lahko reklama, na primer ponudniki komercialnih izobraževanj IPv6, ki na dogodku udeležencem ponudijo nadaljevanje usposabljanja v njihovih programih, ali pa ponudniki storitev na internetu, ki s tem lahko privabijo k sebi nove stranke.

Možnosti financiranja je več, lahko država financira izobraževanje državljanov ali pa komercialni ponudniki izobraževanj sponzorirajo ta uvodna predavanja IPv6.

Ciljna publika tako zastavljenih predavanj lahko zajema tako sistemske in mrežne skrbnike v podjetjih, vodje oddelkov IT in druge odgovorne, ki odločajo o tehnoloških smernicah in investicijah v podjetjih.

Na takšen način lahko v zelo kratkem času dvignemo osnovno zavedanje širših množic o pomenu in novostih v IPv6.

Deležniki, ki pri tem lahko sodelujejo, so lahko različne institucije in druge entitete, ki združujejo certificirane predavatelje 6Deploy. Več o programu 6Deploy lahko preberete na http://www.6deploy.eu/.

Dvigovanje ozaveščenosti v državni in javni upravi

Dvig ozaveščenosti bo treba izvesti tudi v državni in javni upravi, saj menimo, da je bila stopnja zavedanja doslej premajhna. Tega trenutno ne moremo storiti z javnim pozivom, ampak preprosto s pogovorom z odgovornimi za projekte in omrežja, ki bodo podvržena vpeljavi IPv6. Za te potrebe bo treba pripraviti posebna izobraževanja, ki bodo imela večji poudarek na zahtevah, nujno potrebnih za varnost in kontrolo nad državnimi omrežji in storitvami.

Predlagamo, da se v okviru akcijskega načrta zapove uvedba IPv6 v celotno omrežje državne in javne uprave ter naroči analiza stanja. Predlagamo, da se s testiranji osnovnih delov omrežja na IPv6 zaključi do konca leta 2011, do leta 2012 pa se uvede protokol IPv6 v produkcijo. Spletne servise e-uprave se lahko omogoči na dvojnem skladu do konca leta 2011.

Pristojno ministrstvo mora pripraviti nacionalni plan uvajanja novega protokola za različne gospodarske panoge in koordinirati časovnico interdiscliplinarnih gospodarskih panog med seboj. Omenjena področja je treba zapisati v nacionalni strategiji. Objava strateškega načrta ima poleg vsebinskega tudi zelo močan promocijski učinek. Strateški načrt podaja kratek izsek razvojne strategije države in jasno vizijo tehnološkega razvoja celotne države. Tehnološki razvoj celotne države je pomemben dejavnik pri izboljšanju konkurenčnosti celotnega gospodarstva. Če zamudimo prvo obdobje objav nacionalnih strategij v Evropi, bo država oz. pristojno ministrstvo prisiljeno pod časovnim pritiskom pripraviti in objaviti strategijo, če želimo ohraniti sedanjo konkurenčno stopnjo gospodarstva.

Priložnost, ki nam jo ponuja sedanja finančna kriza, je prava priložnost za ozaveščanje javnosti, torej gospodarstva, da novi internetni protokol ponuja:

- priložnost za povečanje konkurenčnosti družbe,
- analizo učinkovitosti notranje arhitekture IT,
- možnost popraviti napake, ki so nastale zaradi napačnih odločitev, ki so jih povzročili notranji ali zunanji dejavniki.

Finančna kriza je čas, ko je gospodarstvo pripravljeno prisluhniti zunanjim idejam. Nacionalna strategija je zunanja ideja. S pravilnim povezovalnim pristopom je po našem mnenju mogoče povezati sorodna podjetja med seboj in ustvariti dodatno sinergijo slovenskega gospodarstva.

Dvigovanje ozaveščenosti v širši javnosti

Po neuradnih informacijah iz držav članic EU, ki že pripravljajo nacionalne strategije uvedbe protokola IPv6, je nivo zavesti in ozaveščenosti o problematiki IPv6 povečini relativno majhna, zato nekatere že razmišljajo o bolj aktivni vlogi. V teh razmišljanjih prednjači Švedska, zadnje čase daje veliko vlogo regulatorju (Post-och Telestyrelsen – PTS, pri nas APEK). PTS je dobil veliko vlogo pri vpeljavi DNSSEC, prav tako pa se porajajo ideje, da bi švedska vlada zakonsko naložila PTS izvajanje in dvigovanje ozaveščenosti o problemih in načinih vpeljave IPv6 v njihovi državi, kar sproža več vprašanj, kot ponudi odgovorov.

Prvo sporočilo, ki je tu pomembno, je, da je *država članica EU aktivno pristopila k dvigu zavesti in ozaveščanja svojih državljanov, industrije in poslovnega sveta na splošno ter o problemih in pasteh, ki nas čakajo, če IPv6 ne bomo uvedli pravočasno. V te namene je pripravljena dano nalogo podpreti s finančnimi sredstvi, da bo lahko projekt ozaveščanja potekal korenito, transparentno in enakopravno, predvsem pa na profesionalnem nivoju.*

O regulatorju morda lahko razmišljamo kot relevantnem in usposobljenem, ki ima dovolj avtoritete in po drugi strani ugleda, da dviguje ozaveščenost in promovira uvedbo IPv6. Seveda je treba pred tem vsaj poskusiti identificirati znotraj države druga gibanja, pobude ali telesa, ki to počnejo, ugotoviti ali to počnejo dobro in nepristransko ter jih morda tudi podpreti pri njihovih prizadevanjih in delu.

Deležniki, ki tu lahko opravljajo dvigovanje ozaveščenosti, so Zavod Go6, Arnes, prireditelji konferenc (npr. Telekomunikacije, Vitel, Palsit, Microsoft konferenca, INFOSEK, Poslovna Linux konferenca, konferenca CIO, Informatika v javni upravi), infrastrukturni sektor (GZS-Združenje za informatiko in telekomunikacije).

Primeri ozaveščanja v preteklosti

Leta in leta že poslušamo, kako je treba uvedbo IPv6 spodbujat iz poslovnih priložnosti, kako bo trg moral poskrbeti za pritiske pri uvedbi IPv6 v omrežja … A bolj ko leta minevajo, bolj ugotavljamo, da je bila takšna napoved napačna in se ta želja nikoli ne bo čisto zares uresničila. Zato so potrebni včasih že kar drastični ukrepi pri poskusih ozaveščanja, kaj se

nam lahko zgodi, če nas bo izčrpanje naslovnega prostora ujelo nepripravljene. Trg in posel nam ne bo prinesel pritiskov za uvajanje IPv6, saj se vedno bolj kaže dejstvo, da vodstva podjetij planirajo investicije v vidne učinke in hitre zaslužke znotraj enega poslovnega kvartala, kar pomeni da IPv6 še dolgo ne bo prišel na vrsto. Pri tem se pa ne zavedajo, da traja uvedba IPv6 z vsem testiranjem, tehničnimi pripravami in izobraževanjem kadra lahko tudi več let.

Poslovni svet je najtrši oreh pri ozaveščanju, saj managerji, ki odločajo o potezah in investicijah podjetja skozi trdo poslovno logiko ne vidijo dodane vrednosti novega protokola – v veliki večini primerov pa tudi ne poslušajo tehničnega osebja podjetja, ki jim poizkuša dopovedati, zakaj so posodobitve dobre – poslovnež jih vidi kot strošek in ne kot investicijo.

Dober mehanizem za vzpostavljanje komunikacijskega kanala med vodstvom podjetja in tehničnim osebjem smo kot posledico organizacije okroglih miz na summitu 2. in 3. Slo IPv6 maja 2010 odkrili skoraj čisto po naključju in ta mehanizem oziroma princip je možno z malo stroški pogosteje ponavljati. Na okrogle mize (predvsem na okroglo mizo 2. Slo IPv6 summita) smo povabili visoke predstavnike iz vodstev podjetij, ki bodo v bližnji prihodnosti neposredno vpletena v vpeljavo IPv6 – predstavnike ponudnikov dostopa do interneta, operaterjev, integratorjev, državnih institucij, ponudnikov vsebin, regulatorja in večine preostalih. Zahteva za nastop na okrogli mizi je bilo pooblastilo posameznika, da v javnosti lahko daje izjave in govori v imenu podjetja, iz katerega prihaja. Ker je bil pobudnik okroglih miz MVZT, se redki niso odzvali vabilu, ki je prišlo iz naslova MVZT.

Vprašanja na okroglih mizah so bila različna, na eni smo se pogovarjali o idejah, katere bi morali dodatno zajeti v nacionalni strategiji IPv6, drugič smo pa razpravljali o zahtevah po funkcionalnostih IPv6 v opremi, ki se kupuje z razpisi.

Na prvi pogled preprost dogodek ima lahko zanimive posledice v ozadju. Vodilni delavci podjetja do tega trenutka večinoma niso bili seznanjeni s problematiko in dejstvi o IPv6, morda, ker jih o tem nihče ni poučil, še verjetnejša razlaga je, da o tem niso hoteli nič slišati, se jim ni zdelo pomembno ali pa niso imeli časa in potrpljenja, da bi se s tem ubadali. Posledica je, da se pri odločanju vodenja podjetja odločajo za druge investicije in uvedbo IPv6 puščajo ob strani. Med tem kadrom je kronično razširjeno napačno razmišljanje, da bo ob pravem času že nekdo prišel in prinesel rešitev na zlatem pladnju, ki bo cenejša, preprostejša in boljša, kot jih imamo sedaj. V takšnem stanju poznavanja problematike IPv6 jih preseneti uradno vabilo na okroglo mizo, kjer bodo z drugimi vodilnimi delavci drugih podjetij razpravljali, kaj pričakujejo od nacionalne strategije, kaj bi bilo fino vključiti vanjo ter kakšne zahteve po funkcionalnostih IPv6 naj bi bile zahtevane pri nakupu opreme. Verjamemo, da je marsikoga zajela panika in strah pred tem, da morda s svojim neznanjem in nepoznavanjem IPv6 kot protokola prihodnosti ne bi na

okrogli mizi zaostajal za ostalimi sogovorniki, predvsem pa, da se v javnosti ne bi pojavil nepripravljen.

Kaj je ta preprosta poteza v veliki večini primerov sprožila? Vodilni delavci so poklicali k sebi tehnični kader v podjetju, ki jim je moral spet na dolgo in široko razložiti, kaj je IPv6, zakaj je uvedba nujna, kaj bo od tega podjetje imelo in še vse ostalo - ustvaril se je torej komunikacijski kanal med vodstvom podjetja in tehničnim kadrom, vodstvo podjetja je začelo poslušati tehniko in njihove argumente, zakaj je potrebno vlaganje v nove protokole, izobraževanje ter alokacija njihovega časa in resursov za uvedbo IPv6.

Dodaten dvig ozaveščanja o IPv6 je izvedel Apek, ko je vsem operaterjem poslal vprašalnik o pripravljenosti na IPv6, na katerega so po zakonski dolžnosti operaterji morali odgovoriti. Apekov vprašalnik je povečal zanimanje o protokolu IPv6 vodstvenega kadra v operaterskih podjetjih. Zanimanje Apeka je vsebinsko vplivalo na vsebino operaterskih strategij oziroma investicijskih planov.

Dodatni predlogi za dvigovanje ozaveščenosti širšega obsega v prihodnosti

V prihodnosti bi lahko nadaljevali podobno tradicijo, vendar na še višji ravni. Vodilni kader, ki se odloča o potezah in investicijah, je dojemljiv v večini primerov samo za dogodke, ki se zgodijo na visoki poslovni ali pa na državni ravni. Naš predlog za dvig ozaveščenosti na tem področju je, da MVZT organizira okroglo mizo na visoki ravni, okrogla dvorana v Cankarjevem domu je recimo primerna lokacija, in povabi k pogovoru direktorje vseh največjih operaterjev, ponudnikov vsebin, bank, zavarovalnic, državnega omrežja HKOM, zdravstvenega omrežja ZKOM in ostalih velikih slovenskih podjetij ter predlaga, da se na najvišji ravni zmenijo, kako in kaj naprej, kdo bo kaj naredil in predvsem kdaj.

11. Kaj mora storiti javna uprava za prilagajanje dostopa in storitev za državljane na tehnologiji IPv6

This is the "future work" section. After understanding the proposed road-map, this section clearly outlines what needs to be done next.

Predlogi: Organizacija javne uprave po nemškem modelu (LIR, de.government) pridobitev naslovnega prostora IPv4/IPv6 in razdeljevanje sredstev znotraj javne uprave po hierarhiji, digitalna ločnica in dostop do javnih storitev ne glede na način dostopa.

Problem dostopa do storitev javne uprave: Internet kot skupek med seboj povezanih omrežij, ki za usmerjanje in prenos paketov uporabljajo protokol IP, je brez dvoma odigral ključno vlogo pri razvoju informacijske družbe. Če smo namreč še v začetku devetdesetih let za izmenjavo podatkov v poslovnem svetu večinoma uporabljali telefone in telefakse, informacije o aktualnih dogodkih pridobivali iz tiskanih medijev in radia oziroma s televizije, poslovanje z državno upravo pa opravljali na občinah oziroma upravnih enotah, so danes stvari precej drugačne, saj si na primer življenja brez uporabe elektronske pošte ali aplikacij za trenutno sporočanje, podaljšanja veljavnosti prometnega dovoljenja ali oddaje dohodninske napovedi brez uporabe storitev e-uprave praktično ne znamo več predstavljati. Če torej želimo dostop do omenjenih storitev zagotoviti kar najširšemu krogu uporabnikov, možnosti uporabe ne smemo pogojevati z izbiro te ali one terminalne opreme, operacijskega sistema ali brskalnika in nenazadnje protokola, ki omogoča usmerjanje paketov od odjemalca do strežnika. S tega vidika se torej uvedba protokola IPv6 v državno upravo ne razlikuje bistveno od uvedbe pri katerem koli drugem ponudniku vsebin.

Ustanovitev delovne skupine in priprava akcijskega načrta

Kot verjetno ni treba posebej izpostavljati, je omrežje, v katero so v Sloveniji povezani različni državni in paradržavni organi, zelo obsežno in raznoliko, potrebe posameznih organov, ki so vanj povezani, pa se med seboj precej razlikujejo. Uvedba protokola IPv6 v takšno omrežje je brez dvoma precejšen organizacijski, tehnološki in navsezadnje tudi ekonomski zalogaj. Da bi izvajanje projekta lahko bolje nadzorovali, predvsem pa preprečili nenadzorovano rast stroškov, predlagamo ustanovitev posebne delovne skupine, ki bo zadolžena za vodenje vseh aktivnosti, povezanih z uvedbo protokola IPv6 v omrežje HKOM in ustrezno prilagoditvijo storitev e-uprave ter koordinacijo zunanjih izvajalcev. V omenjeno skupino naj bodo po zgledu nekaterih drugih držav vključeni tako predstavniki ministrstva, ki upravlja omrežje HKOM in predstavniki večjih uporabnikov omenjenega omrežja. Če bo med člani delovne skupine prevladalo mnenje, da sami ne razpolagajo z ustreznimi tehničnimi znanji, je mogoče vanjo vključiti tudi priznane domače in tuje

strokovnjake s tega področja. Akcijski načrt uvedbe protokola IPv6, ki naj bi nastal kot prvi v sklopu operativnih dokumentov, naj vsebuje natančne cilje uvedbe, roke in odgovorne za izvedbo posameznih nalog ter oceno stroškov njihove izvedbe.

Ker je razlika v ujvajanju protokola IPv6 v državno upravo med Slovenijo in nekaterih drugih državah EU (na primer Franciji in Nemčiji) precejšnja, predlagamo tudi, da se omenjena tematika vključi v novo strategijo e-uprave Republike Slovenije, saj v strategiji za obdobje 2006–2010 ni bila omenjena (e-uprava.gov.si/eud/e-uprava/sep2010_200406_1.doc).

Analiza obstoječega stanja

Da bi torej lahko uporabo storitev e-uprave omogočili vsem internetnim uporabnikom ne glede na različico internetnega protokola, ki jo uporabljajo za dostop do interneta, bi delovni skupini najprej svetovali izvedbo skrbne analize obstoječega stanja posameznih informacijskih in komunikacijskih sistemov. Strojno in programsko opremo, vključeno v omenjeno analizo, bi na primer lahko razdeliti v naslednje skupine:

- omrežna infrastruktura – stikala, vsebinska stikala in usmerjevalniki,
- strežniška infrastruktura – poštni, spletni, imenski, aplikacijski in podatkovni strežniki, imeniki,
- varnostni mehanizmi – požarne pregrade, sistemi za preprečevanje vdorov, koncentratorji VPN, sistemi SIEM.

Pri vsaki od njih pa je treba kot merila pri analizi vključiti:

- stopnjo podpore posamezni funkcionalnosti protokola IPv6 (za usmerjevalnike je na primer najpomembnejša možnost statičnega in dinamičnega usmerjanja, manj pomembna pa je možnost njihovega upravljanja z uporabo protokola IPv6),
- pomembnost posamezne funkcionalnosti za delovanje storitve kot celote (dostop do marsikatere storitve se danes na primer lahko vključi s preprosto prilagoditvijo spletnega strežnika, ki pri spletnih aplikacijah predstavlja prvi nivo aplikacijske arhitekture),
- in oceno zahtevnosti oziroma stroškov za njeno prilagoditev.

Priprava strategije uvedbe protokola IPv6

Ključni cilj delovne skupine bi brez dvoma morala biti priprava strategije za uvedbo protokola IPv6 v državno upravo. V omenjeni strategiji, pri pripravi katere bi delovna skupina morala upoštevati rezultate analize obstoječega stanja, bi morali biti jasno določeni cilji uvedbe protokola IPv6 v posamezni segment omrežja skupaj z roki in odgovornimi za njihovo izvedbo.
Strategija uvedbe protokola IPv6 v državno upravo, ki bi morala posebej izpostaviti morebitne pasti uvedbe in s tem povezana tveganja, bi nujno morala biti usklajena z nacionalno strategijo in ne bi smela obsegati zgolj prilagoditve aplikacij, ki omogočajo delovanje storitev e-uprave, pač pa bi morala obravnavati vse vidike uvedbe protokola IPv6.

Izvedba izobraževanja skrbnikov in verifikacija rešitev

Pretekle izkušnje z uvajanjem protokola IPv6 pri ponudnikih dostopa in v poslovnih okoljih so pokazale, da je mogoče tako tehnološko kot tudi ekonomsko tveganje pri uvedbi močno zmanjšati z ustreznim izobraževanem skrbnikov. Da bi sredstva, potrebna za pripravo in izvedbo izobraževanj omrežnih in sistemskih skrbnikov ter arhitektov zmanjšali, predlagamo, da se v strategiji uvedbe protokola IPv6 preučijo možnosti uporabe alternativnih izobraževalnih metod, predvsem e-izobraževanja in vključitve ustreznih vsebin v obstoječa interna izobraževanja.

Pri večini aplikacij, ki omogočajo delovanje storitev e-uprave, sta na prvo mesto postavljeni zanesljivost in varnost delovanja. Da bi ju lahko zagotavljali tudi po uvedbi protokola IPv6, predlagamo verifikacijo vseh predlaganih rešitev v testnem okolju, pri čemer bi se za vsakega od testov vnaprej predvidelo, kakšni so pričakovani rezultati, morebitna odstopanja pa ocenilo glede na pomembnost posamezne aplikacije. Testno okolje, v katerem se bo izvajala verifikacija predlaganih rešitev, naj bo popolnoma ločeno od produkcijskega okolja.

Pridobitev in razdelitev naslovnega prostora

Prvi korak pri dejanski uvedbi protokola IPv6 v javno upravo verjetno predstavlja sprejetje dogovora o načinu pridobitve in razdelitve naslovnega prostora. Ker si težko predstavljamo, da se naslovni prostor v omrežju HKOM že danes ne upravlja centralizirano, predlagamo ohranitev obstoječe prakse tudi v prihodnje, saj se bo le na ta način mogoče izogniti povečanju stroškov upravljanja omrežja. Pri razdelitvi naslovnega prostora posameznim državnim in paradržavnim organom bi kazalo uporabiti izkušnje, ki so bile pridobljene pri razdelitvi naslovnega prostora v raziskovalnem in akademskem omrežju Arnes, katerega državna uprava uporablja kot ponudnika dostopa do spleta.

Postopna uvedba protokola IPv6 v omrežje

Eno od osnovnih meril pri izbiri ustreznega načina uvedbe protokola IPv6 v posamezno poslovno okolje je ocena vpliva, ki ga ima sprememba na zanesljivost in varnost delovanja. Če na primer vzamemo hrbtenično omrežje, katerega ključna naloga je karseda hiter in zanesljiv transport prometa med posameznimi lokacijami, potem moramo najprej proučiti, ali je uporaba protokola IPv6 v konkretnem primeru združljiva s tehnologijo MPLS in protokoloma OSPF in BGP, oziroma, ali bo uporaba protokola IPv6 imela kakršnekoli posledice na njeno zmogljivost. Podatki nekaterih proizvajalcev omrežne opreme (na primer http://www.cisco.com/web/-strategy/docs/gov/IPv6perf_wp1f.pdf) namreč kažejo, da se prepustnost omrežne opreme za promet IPv4 in IPv6 lahko močno razlikujeta. Po drugi strani pa je lahko uvedba protokola IPv6 v druge dele omrežja, dostopovno omrežje ali segmente DMZ problematična z vidika podpore strojni opremi in ustreznim varnostnim obravnavanjem prometa IPv6.

Po drugi strani pa lahko ima uvedba protokola IPv6 v javne strežniške segmente precejšen odmev v strokovni in laični javnosti, saj je na ta način (vsaj navzven) mogoče pokazati tehnološko naprednost in spodbuditi k uvedbi tudi druge ponudnike vsebin. Ena večjih pasti, ki jim je posamezna organizacija na ta način lahko izpostavljena, pa je povezana z varnostjo. Ker gre v tem primeru za javne strežnike, je treba pred omenjeno odločitvijo skrbno pretehtati zanesljivost delovanja vseh uporabljenih varnostnih mehanizmov, saj si še posebej v primeru storitev e-uprave na noben način ne moremo privoščiti, da bi bila varnost pri uporabi protokola IPv6 manjša kakor pri uporabi protokola IPv4.

O avtorjih

- Urban Kunc
- Ivan Pepelnjak
- Janez Sterle
- Matjaž Straus Istenič
- Andrej Kobal
- Simeon Lisec
- Olaf Maennel
- Jan Žorž

Urban Kunc je zaposlen na Agenciji za Pošto in Elektronske komunikacije Republike Slovenije (Apek), zelo aktiven na področju IPv6 v službi in prostem času. Pripravil je anketo o vpeljavi IPv6, ki jo je Apek poslal vsem operaterjem. Je avtor 76 strani dolgega Apekovega priporočila o prehodu na IPv6 in na splošno zelo dobro pokriva ter razume področje regulacije in države napram problematiki IPv6. Urban je tudi član Strokovnega Sveta zavoda go6 kot predstavnik Apek-a.

Ivan Pepelnjak (CCIE#1354) je zaposlen kot vodja tehničnih svetovalcev v podjetju NIL Data Communications (hkrati je tudi solastnik podjetja). Njegovo področje ter ekspertiza so omrežja in uvajanje IPv6 v različna omrežna okolja. Od leta 1990 načrtuje in postavlja velika podatkovna omrežja ter piše knjige o naprednih tehnologijah. Ivan deli svoje izkušnje in znanje preko portala ioshints.info, kjer veliko piše o IPv6, in je reden predavatelj na slovenskih IPv-srečanjih.

Janez Sterle je zaposlen v Laboratoriju za Telekomunikacije na Fakulteti za Elektrotehniko (LTFE), ki je tudi strateški partner Zavoda go6. Janez predava o IPv6 na svojih tečajih in izobraževanjih. Njegovo področje dela na IPv6 je zelo široko, izstopa pa izobraževalni ter laboratorijski/testni del. Janez je tudi član Strokovnega Sveta Zavoda go6 kot predstavnik LTFE.

Matjaž Straus Istenič je zaposlen na Arnesu, kjer opravlja dela in naloge vzdrževanja in načrtovanja omrežja. Je velik poznavalec IPv6 v zelo širokem smislu, poudarjena znanja pa so omrežja ter socialni vidik uvajanja IPv6. Je glavni pobudnik ter aktivist za vpeljavo IPv6 na Arnesu, hkrati pa tudi član Strokovnega Sveta Zavoda go6 kot predstavnik Arnesa.

Andrej Kobal je zaposlen v podjetju Astec, z IPv6 se ukvarja že veliko let. Njegova specialnost na IPv6 so varnost omrežij in servisov ter vpeljava novih protokolov v javno upravo, saj Astec večinoma skrbi in vzdržuje HKOM, prostrano omrežje MJU. Poleg omenjenega se je odlično odrezal tudi v IPv6 izobraževalnih sferah, saj predava na Astecovem IPv6 boot-campu.

Simeon Lisec je zaposlen pri Telekomu Slovenije, je vodja uvedbe IPv6 za celotno Telekom skupino. Njegove IPv6 specialnosti segajo na področja ISP, standardizacije, poslovnih procesov, ponudnikov vsebin in izobraževanja. Simeon je aktivni vodja slovenske IPv6 delovne skupine in zaradi tega tudi član Strokovnega Sveta Zavoda go6.

Olaf Maennel je redni profesor na Loughborough University, UK. Pred tem je bil zaposlen na Deutche Telekom Lab, kjer je razvijal nove metode usmerjanja v omrežjih, specialnost so mu dinamični routing protokoli. Z Olafom sodelujemo na predlogu RFC-ja A+P, ki ponuja mehanizem za deljenje javnega IPv4 protokola med več uporabniškimi napravami na principu deljenja vrat. Olafova posebnost pri IPv6 je zelo širok pogled nad mednarodnim dogajanjem na tem področju, njegov prispevek bo pogled in komentar na naša razmišljanja v dokumentu iz zunanjega, mednarodnega stališča. Več o Olafu na http://maennel.net/.

Jan Žorž – soustanovitelj Zavoda go6, predsednik Strokovnega Sveta Zavoda go6 in predavatelj o IPv6 tematikah po svetu. Iniciator gibanja za uvedbo IPv6 v Sloveniji in idejni vodja nastanka go6 platforme ter povezovanja države, regulatorja, industrije in civilne družbe v skupne akcije za dvig ozaveščenosti o problematiki in uvedbi IPv6. Več: http://www.pragma.si/resume/index.html.