REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO,
ZNANOST IN TEHNOLOGIJO

The Government of the Republic of Slovenia, Ministry of Higher Education, Science and Technology

Study: Transition to IPv6

(Guidelines for Deliberation on the National IPv6 Strategy)

This work was done under patronage of Go6 Institute (http://go6.si):

Translation by NIL Ltd. (http://www.nil.com)

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

Ljubljana, 10 November 2010
Updated, 16 March 2012

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

Study:Transition to IPv6 (Guidelines for Deliberation on the National IPv6 Strategy) - Ljubljana:
Ministry of Higher Education, Science and Technology, 2010

Editor: Jan Žorž
Design: Jan Žorž

Table of Contents

Foreword

Patrik Fältström[1]:

The next generation IP protocol was something that engineers in the world began working on in the early 1990's, almost 20 years ago. However, not until now have we witnessed the need, the urgency and the 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 been talking about how important IPv6 is for the Internet. And of course not only for the Internet itself but for everyone that uses the Internet.

A careful reader and those that have followed this process might ask the reasonable question of why IPv6 is so important now, when obviously the world has not collapsed before now. 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 in conjunction with how the Internet was designed. Any device connected to the Internet should be able to connect to any other device. This was rediscovered in about 2008 in the discussions around the Internet of Things. This isn't new. It is how the 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 that users cannot, when they travel, access their pictures, smoke detectors, front doors and fridges 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 anyone that comes 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 an impact on innovation and the market economy.

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

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 isn't any business rational for charging IPv6. Internet Service Providers (ISP) could extra charge any new service, which is value added for the customer, but not IPv6 as a new way of connectivity. Instead, the upgrade to include IPv6 should have happened as part of the normal upgrade cycle of the hardware and software that was made in 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, the internet of things and many other elements that would guarantee (from a technology perspective) the openness of an end-to-end principle, it unfortunately might be a deployment that happens by itself, because it 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 the Internet to coordinate and update their procurement processes.

The reason for that is that since the updating of the networks in the world does 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 by at least partially funding that deployment.

The best way of doing this is not to regulate and force deployment but is instead by ensuring that public e-services are available over both IPv4 and IPv6 and to ensure that public services are prepared to pay their upstream Internet Service Provider to get it (i.e. the best thing the public sector can do is work together). Not only among public sector entities, 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 expands on these needs that I have just briefly touched upon. There are unfortunately not many that have written texts about these problems, e.g. the lack of cooperation and the economic impact related to non-deployment of IPv6. I think the work in Slovenia is perfect. More countries should have done what Slovenia has done. However, although this document covers large ground, there is more to do. 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 roles the various parties (private as well as public sector and civil society) have in relation to 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 stated: “Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.”

Summary

Today, the Internet represents one of the most important infrastructures of modern society. It not only makes it possible for many organisations, companies and individuals to work and to educate themselves but also to survive. The Internet of today is based on the IPv4 protocol. It enables the addressing of network devices and packet switching across a network towards their target. We are facing an almost imminent exhaustion of the IPv4 address space. On 03 February 2011, Internet Assigned Numbers Authority (IANA) announced that the pool of public IPv4 Internet addresses had become depleted. Consequently Regional Internet Registries (RIRs) are left with only the addresses they have been assigned prior to this date. In the EU region, which is under the care of RIPE NCC, the IPv4 addresses shall run short in the first half of 2012. The Asia-Pacific Network Information Center (APNIC) has activated its "Last /8 address policy", which means that any organization applying for IPv4 address space to APNIC, will receive a maximum allocation of only a /22 prefix (1024 IPv4 addresses). Such allocations are too small to satisfy current growth rates, but it will assure that newcomers be able to enter the IPv4-market for a long time to come. According to some estimates, Slovenia currently has at its disposal approximately 1,700,000 IPv4 addresses. At first glance, the number seems impressive and that the number of IPv4 addresses will suffice, however, if one takes into account the trend of modern devices, which is oriented towards mobility, smart devices and smart transport, one quickly realises that there are not nearly enough IPv4 addresses for future growth and development.

The IPv4 protocol has had a successor for ten years, namely the IPv6 protocol. The IPv6 protocol is more advanced in many aspects, but its greatest advantage is its enormous address space. IPv6 is a basic communications protocol that provides, at present and in the future, addressing of smart network devices and other objects of the future Internet. Without its deployment, development and economic growth will slow down and, in the worst-case scenario, come to a halt.

The deployment of the IPv6 protocol is best with numerous problems. Vendors have been blamed, operators have been blamed, it has been said that there is no content, that applications don't support it, that the Customer Premises Equipment (CPE) is to blame. However, the biggest is the incompatibility of IPv6 with the IPv4 protocol. This means that network devices with the IPv4 protocol cannot communicate with IPv6 devices if the IPv6 protocol is not a part of the existing protocol stack. Internet Service

Providers (ISPs) do not have customers who demand IPv6, because there are almost no IPv6 websites providing content. There are no IPv6 websites, because there are no customers looking at them over IPv6. This is a classic chicken-and-egg problem. ISPs are wedged in the middle. They are being asked to make significant and costly changes to their network, without getting any increased return. In fact, some customers might not be ready for IPv6 and therefore run into technical problems. The challenge is that for a transition to be successful all those things mentioned above have to happen simultaneously.

There is also a possibility of using translation and tunnelling mechanisms with which these differences can be bridged, but these solutions are only transitional, but they additionally increase costs and create many security problems.

IPv6 is a part of the protocol stack in almost all modern operating systems, from personal computers to routers, firewalls and IDS/IPS (Intrusion Detection/Prevention Systems). The list of IPv6 compatible devices is getting longer every day. The factors hindering the deployment of IPv6 are ignorance of the issue and of the consequences of IPv4 address space exhaustion, unfamiliarity with its operation, additional operational costs related to design, deployment and maintenance of IPv6 equipment and costs for educating staff. Another problem is that it has been reported that some clients did not install IPv6 correctly. For some reason their IPv6 connectivity is broken. As a consequence they may not be able to reach a dual-stacked (IPv4 & IPv6) website at all. Therefore, some website operators might be reluctant to upgrade to IPv6, as they might loose a small fraction of their customers. If, however, they would not upgrade they do not risk loosing even this small fraction of customers. This is a vicious cycle, as many things have to work more or less simultaneously to be successful. To a lesser extent, taking into account the cyclic replacement of equipment, purchasing new or upgrading the existing equipment also represents a cost.

The analysis carried out as part of this study has shown that governments from various countries are responding differently to the imminent exhaustion of the IPv4 address space. The more economically advanced and export-oriented countries have set clear objectives with predetermined and measurable deadlines for implementing IPv6 into public, state and private communication networks. Despite the decline in economic growth, governments in some countries did not lower but actually increased the budget for investments into the ICT infrastructure that will be IPv6 based. Even the Czech Republic, which until recently was one of the less advanced countries of the former socialist block, set clear goals for deploying IPv6. With a resolution adopted in June 2009, the Czech government has set an objective of implementing IPv6 into the network of public administration by gradually replacing equipment and to also provide access to its online content over the IPv6 protocol since 31 December 2010. The Czech Republic is, besides Sweden and Portugal, one of the leading countries in the European region in terms of implementing the security extension of the DNS system (DNSSEC) with which it protects its domain names. Besides IPv6, DNSSEC or its alternatives are one of the key protocols and elements of the Internet of the future.

In the group of the 27 countries of the EU, Slovenia falls among those with average technological development of electronic communications. According to research carried out in February 2010 by the national regulator of electronic communications, APEK, some Slovenian operators are implementing IPv6 into their backbone networks at an accelerated pace and gradually also into access networks. Some of them already provide IPv6 connectivity and basic IPv6 services (DNS) to users. The Slovenian Arnes research and education network is an exception, because it has been using IPv6 in their backbone network for a number of years. IPv6 connectivity is also available at the universities of Ljubljana and Maribor, the Jožef Stefan Institute, some high schools and elementary schools, high school student residence halls and libraries.

The Slovenian government, in contrast to comparable countries, has yet to make an important step towards deploying IPv6 that would encourage all relevant stakeholders to deploy IPv6. Those stakeholders are namely the operators, service and content providers, system integrators, network equipment manufacturers, educational institutions and public and private organisations. It has yet to adopt an action plan or a strategy with which it would undertake to implement IPv6 within a certain time limit into the networks of the pubic administration, ministries or agencies. It has not pledged itself to provide its citizens access to services and websites over IPv6 within a determined time limit or to encourage IPv6 deployment in any other way.

The transition to IPv6 cannot happen overnight. Even if we were to start today, it will take years for us to compete with countries that have been successfully deploying IPv6 for years. However, we have to start somewhere and the longer we wait the more difficult it will become. The success of the transition to IPv6 depends on the cooperation of all stakeholders. IPv6 must be implemented by operators into their existing and into all new networks. The content and service providers must develop services and content that take advantage of the strengths of IPv6 or should at least at the beginning provide access to existing IPv6 services and contents. System integrators must assist public and private organisations in IPv6 deployment. Public and private educational institutions must implement IPv6 into their education programmes.

As part of this study, a range of functionalities was prepared, in cooperation with the Slovenian go6 Institute, that IPv6 compatible equipment must meet. The range of functionalities was forwarded to the European internet community in the framework of the European regional registry, RIPE NCC. The document achieved a strong technical community consensus and was published as official “Best Current Practice” document for RIPE region (RIPE-501). The approved document has the opportunity to become a recommendation of the European Commission to the member states of the European Union in deploying the IPv6 protocol.

The study was made as a response to 11 questions that must be answered in order for the country to suitably prepare for the transition to IPv6 and to correctly respond to the broader challenges we are facing - this can cover the state and public administration or the effect of the transition on citizens, industry and all other stakeholders within our society.

We hope that this document provides enough answers for deliberations regarding the national strategy of IPv6 deployment, which is urgently needed even though some are unaware of this.

Table of IPv6 Implementation into Companies and Networks as of 2 November 2010

The state of IPv6 deployment in some Slovenian companies and institutions is monitored at the go6.si portal under the section “Stanje IPv6 v Sloveniji” (State of IPv6 in Slovenia):

(Editor’s note: big “X” signs represent status in March 2012. As we can see, some progress was made.)

Organisation	IPv6 is implemented	IPv6 is being implemented	IPv6 is planned	No data or not planned
AMIS	X	X		
APEK	X	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	X	
Iskra Sistemi d.d.		X		
IskraTel		X		
LTFE	X			
Mobitel	X	X		
Moj Mikro (Delo revije)			X	

najdi.si	X	X		
NIL	X	X		
NLB				X
POPtv		X		
racunalniske-novice.com				X
RTVSLO	X	X		
SiMobil		X		
SmartCom		X		
T-2	X	X		
Telekom Slovenije	X	X		
Telemach		X		
TušTelekom	X	X		
University of Maribor		X		
zavod go6	X			
ZDRZZ			X	

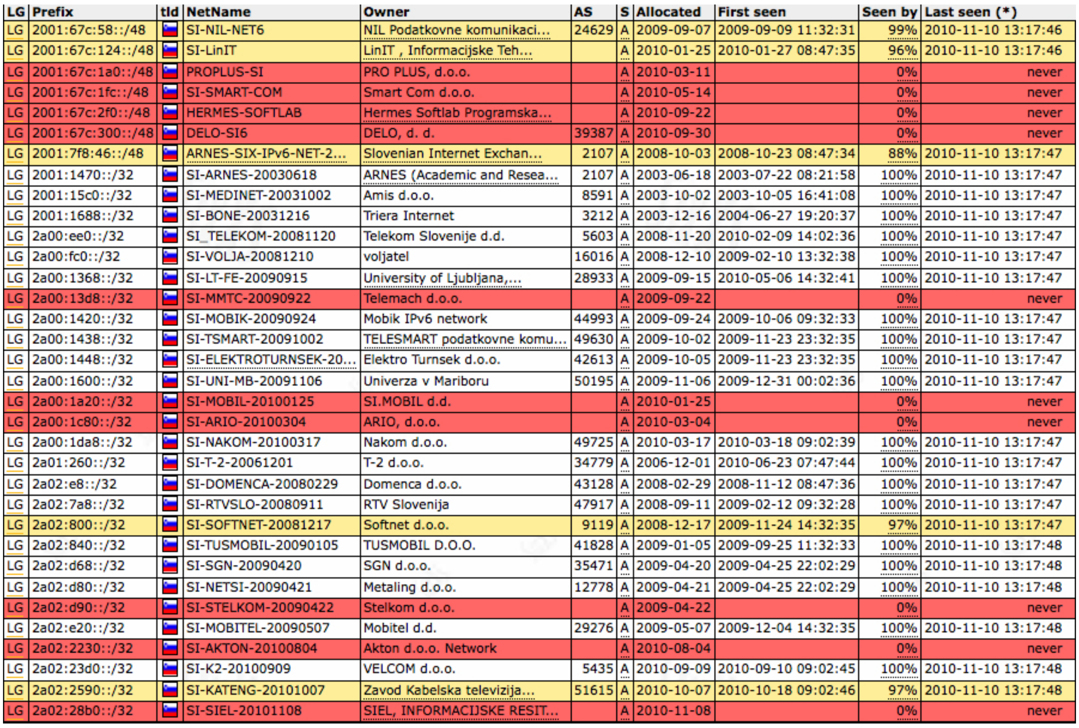
The table is listed in alphabetical order by company or organisation name.

For better understanding of the above table:

- If there is X only in “IPv6 is implemented”, then that company implemented IPv6 in all their current services
- If there is X in “IPv6 is implemented” and “IPv6 is being implemented”, that means that company fully implemented IPv6 in some services and there is still work in progress for some other services, where IPv6 is not implemented.
- If there is X in “IPv6 is being implemented” that means that IPv6 was not fully implemented in no service and there is work in progress towards that goal.

State of IPv6 Allocation in Slovenia on 2 November 2010

In this section we present IPv6 allocations at the Slovenian Local Internet Registries (LIR), which was recorded on Sixxs website on 2. November 2010. As it can be seen, 34 Slovenian AS numbers have allocated their IPv6 address. 24 of them (74.59%) correctly announce their IPv6 address in the global Internet. The allocations are arranged in alphabetical order according to address space.



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

Red colored rows indicates that IPv6 allocation was never announced on the Internet, yellow means that allocation was announced, but visibility from monitoring hosts was not 100% over time and white means that allocation was properly announced and visible from Internet all the time.

Situation in March 2012 is rather different. The database currently holds 66 IPv6 allocations, of which 21 (31.82%) did not announce it properly in the Internet. However 45 (68.18%) of the networks are currently correctly announced and visible.

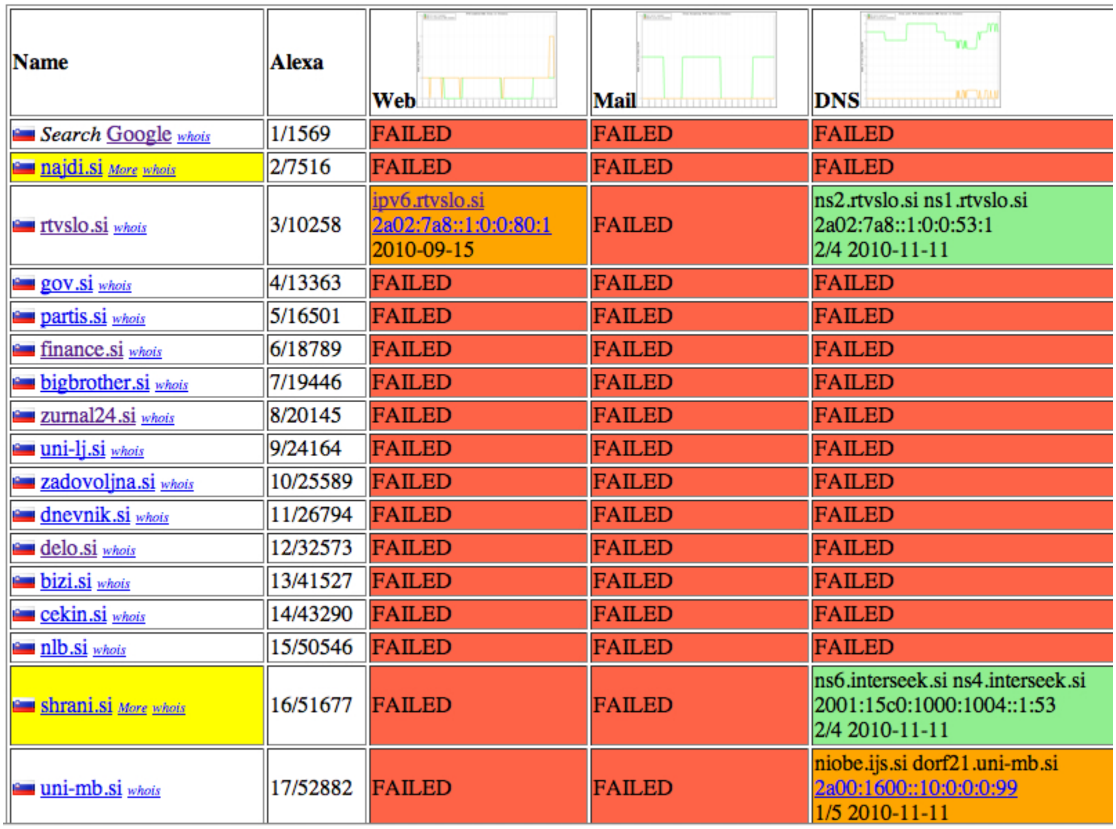
Latest status can be checked at: https://www.sixxs.net/tools/grh/dfp/all/?country=si

State of Deployment and Accessibility of Slovenian Websites over IPv6

Eric Vyncke maintains a portal that checks the accessibility of various services over IPv6 such as web servers, mail servers and DNS servers for domains from various countries of the world, including Slovenia. The list of domains is acquired from the Alexa search engine; it retrieves the most popular domains.

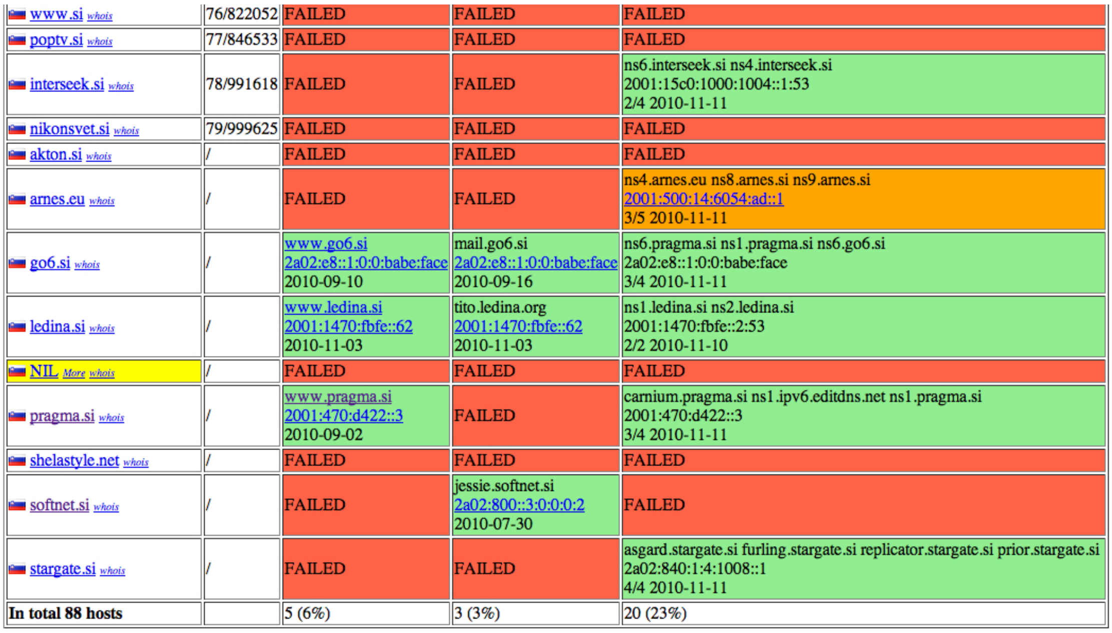
A portion of the state is shown in the picture below; the complete table is available at the address: http://www.vyncke.org/ipv6status/detailed.php?country=si

The picture below shows the status in November 2010. Meanwhile the status has changed dramatically.



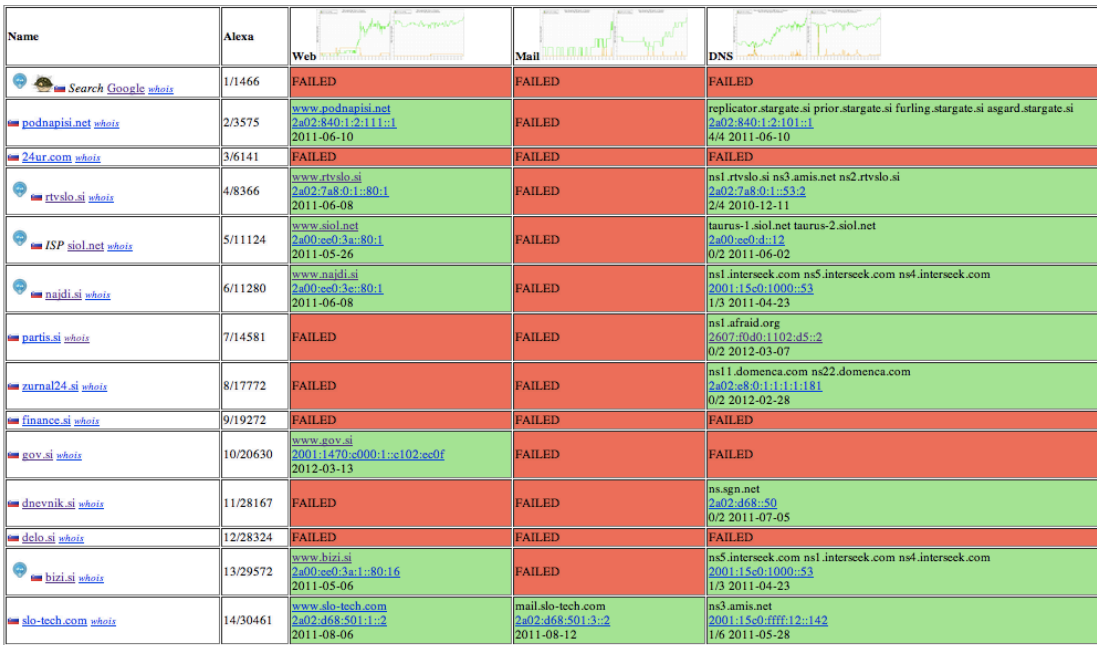
Name	Alexa	Web	Mail	DNS
Search Google whois	1/1569	FAILED	FAILED	FAILED
najdi.si More whois	2/7516	FAILED	FAILED	FAILED
rtvslo.si whois	3/10258	ipv6.rtvslo.si 2a02:7a8::1:0:0:80:1 2010-09-15	FAILED	ns2.rtvslo.si ns1.rtvslo.si 2a02:7a8::1:0:0:53:1 2/4 2010-11-11
gov.si whois	4/13363	FAILED	FAILED	FAILED
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

(a part of the table has been cut for the sake of clarity)



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%)

In March 2012 the situation is different. Many big content providers enabled IPv6 on their systems and are serving their content over both protocols, IPv4 and IPv6.



Name	Alexa	Web	Mail	DNS
Search Google whois	1/1466	FAILED	FAILED	FAILED
podnapisi.net whois	2/3575	www.podnapisi.net 2a02:840:1:2:111::1 2011-06-10	FAILED	replicator.stargate.si prior.stargate.si furling.stargate.si asgard.stargate.si 2a02:840:1:2:101::1 4/4 2011-06-10
24ur.com whois	3/6141	FAILED	FAILED	FAILED
rtvslo.si whois	4/8366	www.rtvslo.si 2a02:7a8:0:1::80:1 2011-06-08	FAILED	ns1.rtvslo.si ns3.amis.net ns2.rtvslo.si 2a02:7a8:0:1::53:2 2/4 2010-12-11
ISP siol.net whois	5/11124	www.siol.net 2a00:ee0:3a::80:1 2011-05-26	FAILED	taurus-1.siol.net taurus-2.siol.net 2a00:ee0:d::12 0/2 2011-06-02
najdi.si whois	6/11280	www.najdi.si 2a00:ee0:3e::80:1 2011-06-08	FAILED	ns1.interseek.com ns5.interseek.com ns4.interseek.com 2001:15c0:1000::53 1/3 2011-04-23
partis.si whois	7/14581	FAILED	FAILED	ns1.afraid.org 2607:f0d0:1102:d5::2 0/2 2012-03-07
zurnal24.si whois	8/17772	FAILED	FAILED	ns11.domenca.com ns22.domenca.com 2a02:e8:0:1:1:1:1:181 0/2 2012-02-28
finance.si whois	9/19272	FAILED	FAILED	FAILED
gov.si whois	10/20630	www.gov.si 2001:1470:c000:1::c102:ec0f 2012-03-13	FAILED	FAILED
dnevnik.si whois	11/28167	FAILED	FAILED	ns.sgn.net 2a02:d68::50 0/2 2011-07-05
delo.si whois	12/28324	FAILED	FAILED	FAILED
bizi.si whois	13/29572	www.bizi.si 2a00:ee0:3a:1::80:16 2011-05-06	FAILED	ns5.interseek.com ns1.interseek.com ns4.interseek.com 2001:15c0:1000::53 1/3 2011-04-23
slo-tech.com whois	14/30461	www.slo-tech.com 2a02:d68:501:1::2 2011-08-06	mail.slo-tech.com 2a02:d68:501:3::2 2011-08-12	ns3.amis.net 2001:15c0:ffff:12::142 1/6 2011-05-28

We can observe in the above picture, that out of top-6 sites 4 of them enabled IPv6, Google.si and 24ur.com will enable it on 6.6.2012

For better understanding of impact of this new picture, rtvslo.si is news portal of Slovenian national TV, siol.net is incumbent telecom news portal and najdi.si is national search engine. This means that highest traffic intense sites were enabled on IPv6. We can also see, that also Slovenian government enabled their web site on IPv6 (gov.si).

Apek: Research on Deployment and Readiness for IPv6 in Slovenia

In February 2010, the Post and Electronic Communications Agency of the Republic of Slovenia (APEK) carried out an extensive survey on the state of IPv6 deployment among Slovenian operators and providers of electronic and communications services. The analysis showed the following results regarding deployment: 41 operators responded to the questionnaire, among which five operators have more than 90% of all clients. Among them, there are many cable operators. Cable operators who have an optical-coaxial infrastructure that is entirely their own and who simultaneously provide their own services (IP) are rare.

Based on the answers received, it was determined that on average the surveyed are well aware of the issue of IPv6. Around 80% of the surveyed stated that the management is aware of the need to deploy IPv6, but only 70.7% of management supports its deployment in terms of reserving financial resources, training human resources and purchasing or updating the equipment and licenses.

Ten operators (24%) use IPv6 on their backbone network in dual-stack with IPv4; one operator has IPv6 over an IP tunnel and one over IPv4 MPLS (6PE RFC4798; v4 signalling). For now, none of the operators are using IPv6 technology over IPv6 MPLS (IPv6 routing and signalling).

Almost 20% of the operators have IPv6 in production at the access network. It is probable that the majority of these are operators that have optical fibres in their access networks, since from a technological standpoint, their equipment operates on a data link layer that is independent from the above IP protocol layer. According to the results, most operators shall not carry out the transition of the access part of the network prior to 2011.

Nine operators (22%) are already making it possible for business users to connect to IPv6. Five operators provide a native IPv6 service, four provide IPv6 over a tunnel and five provide multi-homing. Demand for IPv6 connectivity is still very low. Less then 10% of business users demanded IPv6 connectivity. The analysis shows that the majority of other operators will not provide their business users with IPv6 before the first quarter of 2011. Eleven operators are not considering connecting the business users.

The operators have started connecting residential users through DSL or FTTH technologies since 2011. Most of the problems lay in the CPE devices, which have to be replaced, because they don't fully support IPv6 functionality.

More about the analysis of IPv6 deployment in Slovenia can be found at the agency's website: www.apek.si.

Sources:
go6 Institute (2010): Table of IPv6 Deployment, available at: http://go6.si/stanje-ipv6-v-slo-devel/, visited on 2 November 2010

SixXS (2010): IPv6 Allocations Table, available at:
https://www.sixxs.net/tools/grh/dfp/all/?country=si, visited on: 2 November 2010

Apek (2010): IPv6 Deployment in Slovenia – Research,
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
List of web IPv6 servers by individual countries, http://sixy.ch/

1. Description of the Most Important Issues and the Consequences if Slovenia does not Solve them Appropriately

Is *the problem too simple to be a problem?!*
The Internet has reached a scaling limitation. And while experts might 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 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 have been 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 section points out, there are some terrifying alternatives. We start with an 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 remember, 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.

The Internet as a Critical Infrastructure of the Society

The critical infrastructure is represented by facilities, networks, services and assets of information and communication technology whose breakdown or destruction would seriously affect the health, safety and economic prosperity of citizens or the effective operation of the country.
Critical infrastructures cover numerous sectors of the economy including banking and finance, traffic and delivery, the energy industry, municipal utility services, health care, the food supply and key civil services. One of the most important, critical infrastructures is the communications infrastructure. Most of today's communications infrastructure, primarily the Internet, is based on the IPv4 protocol, which has been in use for almost 30 years. Many protocols

and mechanisms have been added to the IPv4 protocol since its creation in order to increase its usefulness and improve the security of communication. Despite improvements, its main shortcoming remains, namely a relatively small number of IPv4 addresses, with which network devices and terminals can be addressed globally, for present requirements.
The IPv4 internet protocol has had a successor for more than ten years. It is, namely, internet protocol version 6 (IPv6). Compared to IPv4, IPv6 provides additional functionalities and at the same time contains most of the functionalities that were developed in IPv4 in the form of additional protocols. It theoretically provides global addressing for more than 3.4 x 10^38 (2^128) network devices, which is its main advantage.

A Short Summary of the History of IPv4 and IPv6 Protocol Deployment

The IPv4 protocol was specified in 1981 in the RFC791 document. In 1991, the IETF (Internet Engineering Task Force) and the internet community of operators, network planners and researchers decided that IPv4 had several shortcomings, since it does not provide a large enough address space in the long term for the growth of the Internet. After long discussions and conciliations, in 1995 they issued the first IPv6 specification called IPng which was issued in RFC 1883 (IP Next Generation).

6BONE

The 6bone network was a testbed for internet protocol version 6. It was a product of the IETF IPng Project that created IPv6. It was intended to eventually replace the current Internet network layer protocols known as IPv4. 6bone began outside the official IETF framework at the March 1996 meeting and quickly became a worldwide collaborative project with informal oversight from the "NGtrans" (IPv6 Transition) working group of the IETF.

The original mission of 6bone was to establish a network for promoting the development, testing and deployment of IPv6 and used a model based on the experiences from the Mbone network, hence the name "6bone".

6bone started as a virtual network (using IPv6 over IPv4 tunnelling) operating over the IPv4-based internet with support for IPv6 traffic tunnelling and gradually added true, native connections for IPv6. Even though initially 6bone focused on testing standards and deployment, it later refocused and became a testbed for checking and developing transition and operational procedures and was no longer intended for testing the actual use of the IPv6 network.

6bone operated in the 3FFE::/16 address space.

6bone reached its peak in mid-2003. On 1 January 2004, a decision was made that 6bone had achieved its purpose and that it should be gradually closed, which took place on 6 June 2006. The 3FFE::/16 address space returned to the available allocations.

Since 1995, more than 30 RFC documents were issued that additionally define many accompanying changes, everything from how IP addresses are stored in the system and DNS applications to how datagrams are sent and routed over the data link layer (Ethernet, PPP, Token Ring, FDDI) and all other media and how the programmers call the network functions.

Because IPv4 and IPv6 are completely incompatible within the network layer, the IETF provided quite a few mechanisms for transition including tunnelling (translating IPv4 into IPv6 and vice versa) and primarily coexistence of both protocols in the dual-stack system. In this system, a network device (client, server, router, etc.) uses the IPv4 and the IPv6 protocol simultaneously.

The essential limitation of the IPv4 protocol is the size of its address space. The IPv4 address is 32-bit, meaning that it (usually recorded in the format xxx.xxx.xxx.xxx) can theoretically address four billion different devices. The number that was incomprehensible in the past has now become too small due to the increasingly rapid growth of the internet.

The key reason for the increase of address space in IPv6 was the desire to have more hierarchical routing and more effective operation of backbone networks, but unfortunately these achievements had to be abandoned due to the method of allocating IP addresses and the unresolved issue of users with redundant internet access (multihoming).

Today, IP addresses are needed by servers, communication equipment and all fixed and mobile devices and terminals that require (constant) IP connectivity. True mobility and miniaturisation of modern terminals also present key starting points for establishing a new generation of internet network, the so called Internet of Things.

Mechanisms for More Effective Use of the IPv4 Address Space

Due to slow IPv6 deployment, a series of mechanisms were developed between 1993 and 1996 that temporarily slowed the consumption of public IPv4 addresses. In 1993, the CIDR (RFC1519 – Classless Inter-Domain Routing) mechanism was developed, in 1994, the NAT (RFC1631 – The IP Network Address Translator) mechanism, in 1995, VLMS VLSM (RFC1817 – CIDR and Classful Routing) and in 1996, private address space (RFC1918 – Address Allocation for Private Internets). All the listed mechanisms and the possibility of using private address space did prolong the life cycle of the IPv4 protocol, but they devaluated the basic idea of the operation of the internet - transparent connectability of communication from one end to another.

IPv6 - Innovations and Changes

The IPv6 protocol kept the majority of advantages of IPv4; the changes are (besides the longer address space) primarily corrections of errors in the IPv4 protocol stack. The essential changes are:

- more options in addressing and routing,
- increased address space (from 32 bits to 128 bits),
- scalability of the multicast transfer method has been improved,
- simpler structure and permanent length of the IP header,
- some fields in the IP header have been removed, improved or transferred to expansion headers,
- extended support for providing quality services,
- expansion for ensuring privacy.

Other IPV6 Protocol Advantages

The shortage of IPv4 address space is not the only reason the transition to IPv6 should be carried out. In recent years, the Internet, with the content and services that it provides, opened new possibilities to all users in all areas of activity. The speed of access at fixed locations is increasing. Numerous European countries are planning to increase the access speed to at least 100Mbit/s by 2015. The number of broadband (HSPA, LTE) mobile networks shall increase, and due to great speed and short response time, they shall provide a user experience that is similar to what we have now through classic (fixed) access. The trends of internet usage such as swapping video content, high definition TV (also 3D) and education shall increase the quantity of transferred data even more. Internet services such as social networks (Facebook, Twitter, etc.) and cloud computing promote new innovations. Cloud computing is severely decreasing the obstacles in accessing the service provider market, especially for smaller and medium-sized companies. In the future, a multitude of devices, vehicles, sensors, cameras and other devices shall be able to connect to the Internet. The precondition for such a scenario is capable, high throughput and safe networks that will have to be based on modern devices and protocols that can currently be based only on the IPv6 protocol.

When planning the transition to IPv6, technical advancement is not the only driving force of the new protocol; there is also the possibility for developing new improved services and applications and new forms of connecting and exchanging information. One of the examples of usage is the expansion of the service-oriented infrastructure (SOI) for safe and effective cooperation of users with shared IT services, which is made possible through grid technology and virtualisation. Until now, service and content providing over the internet was primarily the area of larger companies – content providers with their own data centres or those hosting through servers at an ISP or server hosting provider. By deploying IPv6 and removing the NAT mechanisms, new, undreamt of possibilities are opening up for smaller companies and residential users that will be able to offer their contents that are also based on other service protocols.

Overview of IPv6 Deployment

Although the IPv6 protocol brings many improvements and advantages compared with IPv4, it has yet to experience mass commercial deployment with the exception of academic and large backbone networks. Analyses of commercial European networks have only shown growth of IPv6 traffic in the last year (Botterman 2010). IPv6 is not backwards compatible with IPv4 and IPv4 systems cannot use IPv6 services or communicate directly with IPv6 hosts (ECC-CEPT 2010). Many organisations have applications that are incompatible with IPv6, so the transition to IPv6 is conditional upon upgrading or even replacing applications or it may require using translation mechanisms (IETF 2005). Users are facing a shortage of services, applications and devices that are based on the new protocol and are at the same time the reason it is being rapidly deployed. Awareness regarding its operation and the advantages that the protocol brings is also lacking. Its implementation in the core and access network is technically and organisation-wise demanding, and it also represents additional costs for operators and internet providers. Certain devices, primarily those that ensure safety, control, load balancing and accounting, do not yet have entirely the same functionalities or effectiveness as comparable devices from the IPv4 environment. This situation is rapidly improving with an increasing demand. Many operators do not yet see the added value of the IPv6 protocol, and at the same time, there is not enough demand from users that would justify upgrading the networks. A vicious cycle, as several important events have to happen simultaneously.

The mentioned issues hinder the deployment of the IPv6 protocol. Upgrading networks to the IPv6 internet protocol is key for future development of the internet, the internet society and the internet economy. If IPv6 deployment is not significantly accelerated, there will be an extreme slow down in the growth of the internet, and the remains of IPv4 in networks will increase the costs of using the internet. The consequences of this delay in deployment shall be greater costs in all areas of internet services, we will be facing a slowdown of innovations in internet protocol based networks and economic growth will also become slower. These are the findings, among others, of the U.S Department of Commerce (2006), NTIA, NIST, OECD (2008), ITU (2008) and the Commission of the European Communities (2008).

Exhaustion of IPv4 Address Space, Forecasts and Allocation Rules

IANA already ran out of IPv4 address space early 2011. The regional registries will allocate the last acquired blocks at different times, but APNIC (Asia-Pacific Network Information Centre) is quasi-depleted since April 2011 (it runs on a special "last /8" policy). Predicted to be followed by RIPE NCC later in 2012, ARIN in 2013, and AFRINIC and LACNIC somewhere around 2014 (according to predictions performed by Geoff Huston).

For the EU region, which is under the care of RIPE NCC, this means that RIPE will no longer be able to allocate new IPv4 address space to LIR. Typically, the largest consumers of IPv4 address space are ISP. For them, this means that they can no longer connect new users. Thus, the growth and expansion of these companies would basically stop. A major, perhaps even a larger consumer of address space will be mobile (smart) phone users, which is a booming market.

It should be taken into account that an ISP (or LIR) can demand from RIPE NCC a new allocation of IPv4 address space only after using approximately 80% of their allocated addresses. The period for which an LIR can reserve and justify the use of an IP address space is systematically shrinking. From the initial two years, the time period was shortened to one year and now the period is being shortened even more every half a year as is explained below. This means that larger users of the IPv4 address space will be left without IP addresses almost simultaneously with RIRs, since they will be unable to make an address pool.

Let us examine the rule of shortening the time for reservations of the address space and the rule for allocating the last /8 block in more detail:

- during the period up to 1 January 2010, the LIR was able to justify the consumption and request allocation of IPv4 addresses for a time period of the two years,
- between 1 January and 1 July 2010, the time period was 1 year,
- between 1 July 2010 and 1 January 2011, the time period was 9 months,
- between 1 January and 1 July 2011, the time period was 6 months,
- after 1 July 2011, the time period is 3 months,
- when RIPE receives the last /8 block from IANA, each LIR will be able to acquire an address space of only /22 and no more, regardless of how big it is and what needs it has. The reasons for that are the potential future access providers, who, according to this rule, will be able to acquire /22 for quite some time after that.

This means that the majority of operators in the EU will probably remain without address pools by the end of 2012 if their growth and requirement for new IPv4 address spaces is at least approximately similar to the average growth of the internet around the world.

Countries of the world are responding in a variety of ways to the issue of the shortage of IPv4 address space and IPv6 deployment. Asian countries that have the largest increase of the penetration of broadband users in the fixed and mobile network are actively promoting and rapidly deploying the IPv6 protocol and IPv6-based services. They are aware that the IPv4 address space is insufficient for the further expansion of networks, the increase of users and the development of new applications, devices and services. The

US is also rapidly implementing IPv6 into their networks. In 2005, in an order to all their government agencies, the US government prescribed that they must upgrade their core networks to IPv6 by 2008 and to simultaneously connect their interfaces to the networks (Executive Office of the President 2005). The US National Institute for Standards and Technology (NIST) was chosen to develop the required standards that will provide a uniform system of required specifications, a certification method for all government institutions and will be obligatory when procuring IPv6 equipment (NIST 2008). The European Commission has also been actively promoting the deployment of IPv6. With the first *Communication from the Commission of the European Communities*: IPv6 Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6 (Commission of the European Communities 2002), it established the European IPv6 Task Force, outlined priority activities, made it financially possible to deploy IPv6 in research and education networks, supported the development of standards and introduced numerous workshops and trainings. In May 2008, the Commission to the European Communities issued a second *Communication:* Advancing the Internet – Action Plan for Deployment of Internet Protocol version 6 (IPv6) in Europe (Commission of the European Communities 2008) with the aim of strengthening the already implemented measures. Although progress was made, the implementation of IPv6 into European networks is still too slow, while the problem of the lack of IPv4 addresses has increased (Europe's Information Society 2010).

There are several scenarios of the consequences of the IPv4 address shortage. According to some scenarios, it is expected that the organisations that have many unused IPv4 addresses will begin returning them back to regional internet registries. The returned IPv4 addresses will become available for new allocation. This scenario is unlikely. It is unlikely that organisations would voluntarily start returning limited goods such as IPv4 address space, especially since with its short supply, its value is increasing.

Another possible scenario is that organisations will start trading with their unused IPv4 addresses. In this case, a secondary market of IPv4 addresses will be created. The problem that can occur is that there will be a great increase of records of BGP routing entries in the routing tables. Currently (March 2012), there are over 400,000 BGP entries in total, most probably due to the possibility of aggregation and suitable policy of allocating IP address blocks (IP address blocks allocated to operators are joined together). In the event of unregulated address trading, this number could significantly increase. On account of this, there is a possibility that the speed of traffic forwarding in routers could decrease or that the internet could become unstable. It can also occur that the organisations will start using the IPv4 addresses more efficiently, especially if RIRs introduce fees for the allocated IPv4 address blocks.

Market and Growth of the Internet after the Exhaustion of the IPv4 Address Space

If the IPv4 addresses run short, the internet will continue to function. The existing operators will have the option to gradually transition to the IPv6 protocol or to continue with the existing (outdated) IPv4 protocol while trying to make use of the translation mechanisms due to the shortage of public IPv4 addresses. But new operators, who will not have IPv4 address space or will be able to acquire only a little space in accordance with NRO (National Resource Organisation) rules, will face much greater difficulties when entering the market.

Slovenia has a relatively saturated internet market so there is no fear that the existing ISPs will run out of IPv4 address space in a short time. The difficulties that we see are hidden elsewhere. A new ISP that is established after the allocation of the last /8 block from RIPE will not be able to obtain more than a block of /22 IPv4 addresses, which means a maximum of 1022 IPv4 addresses. With such a quantity of public address space, the new operator can only consider allocating the private IPv4 addresses to all their users (RFC1918) and carrying out translation between private and public addresses (NAT/PAT) in the core of the network using CGN (Carrier Grade NAT) or LSN (Large Scale NAT) technology.

Why Address Translation in the Network is Considered Harmful

We know several types of translation mechanisms, and what is common to them all is that they change the content of the header of each packet that is passing through the translation device. The basic purpose of translation is primarily decreasing the number of required public IPv4 addresses. Each translation requires a certain time to process the package, and by increasing the number of sessions that run through the device, the response time of the device itself is also extended along with its complexity. Today's online applications open up to dozens of parallel sessions for each individual user (Google Maps typically opens 70 parallel connections, iTunes opens up to 300 and P2P clients more than 2000). The NAT mechanism or a device with such functionality can be used at the user level on the border between the local user network and the access provider, and it can also be installed in the core of the network in a more capable version (CGN - Carrier Grade NAT) by the access provider.

However, we must be aware that by implementing the NAT mechanism in the core of the network (CGN/LSN), the users are closed off in a "walled garden" where their transparent end to end communication, which is currently at their disposal, is limited. We also take away from them the control over the translation of addresses, which is currently carried out on an end network device (routers).

CGN technology is moving address translation into the network core, which is considered harmful and contradicts the idea of the internet – the model of simple forwarding of packages in the network core and with smart devices on the outer borders of the network (edges).

The idea of a "smart core" could bring the operator or the internet service provider into a situation where business damage could be expected, because the user could not communicate over the internet with certain private applications and protocols that were made by design and are not known and publicly accessible. If NAT (CGN) is in the core of the operator's network, communication with such applications simply does not function. Before, the users could install an Application Layer Gateway (ALG) by themselves on their own device, but now this will no longer be possible. This contradicts the primary idea of the internet – direct connectability between end points without intermediate obstacles.

Today, home NAT devices use UPnP/NAT-PMP network protocols or the technique called port-forwarding. By installing the NAT mechanism into the core, this control at the user level is completely lost, since the service provider will not allow it on the simple grounds of security.

The next difficulty that CGN devices bring is scalability. Operators are faced with the pressure of deciding between, on the one hand, aggregating the network by setting up CGN as much as possible and, on the other, the fact that aggregation represents a problem, among others, with regard to states tables. CGN also represents a single point of failure, and duplicated CGN devices will have serious problems with synchronisation of states (states tables).

However, the essential issue of translating addresses is undoubtedly the traceability of users, which is imposed by the electronic Communications Act and the European Data Retention Directive (Official Gazette of the European Union 2006). When using CGN technology, it is almost impossible to determine who the user is that hacked into the system on the other side of the world, sent spam or committed any other violation or criminal act over the internet. Theoretically, there could be more than 65,000 users hiding behind a single IPv4 address, which seriously aggravates the search for the perpetrator, especially when several users access the same server with the same IPv4 address.

Maintaining Competitiveness and Continual Growth

The essential element that will force the operators to deploy IPv6 is maintaining competitiveness and growth. The goal of an operator should be to provide the user with access to all content and services on the Internet. The services must be quality, reliable, attractive, have prices comparable to the competition and above all be secure. But nowhere is it explicitly recorded which protocol should be used for this. Some operators are already rapidly implementing IPv6 into backbone networks and are carrying out test projects in the access network. Asia, which has the largest penetration of users and the largest consumption of IPv4 addresses, has no other choice but to rapidly implement IPv6 in all parts of the network and to develop applications and services that are based on the protocol. When the competitive operators deploy IPv6 in addition to IPv4, users, services and contents will emerge which will be reachable over both protocols. Operators who will not provide access to content that will only be available over IPv6 will soon become non-competitive. With time, providing internet access through the IPv4 protocol will become increasingly complex for operators. By implementing CGN technology, the complexity of translating addresses will increase, something that has already been experienced by some mobile operators (even Slovenian) who have been using CGN for several years.

Deploying IPv6 undoubtedly simplifies the settings of end devices. According to the recommendation by IETF (RFC3177), each resident CPE device should receive its own part of the IPv6 address space and each computer their own public IPv6 address. From here on, everything is simple: from the computer/server at home, we start serving contents or services which, if the IPv6 firewall is set up correctly, is not a demanding task. The ISP's orientation towards care for the user can be a strong mechanism of coordinated and synchronised IPv6 deployment to the user, since no one wants users switching between operators and unsatisfied users besieging their help desks.

The Procedure of Implementing IPv6 into the Network

The implementation of the IPv6 protocol into a live environment requires a certain time period, in larger and more complex networks as long as several years. During this period, IPv4 addresses will cease to be available.

A detailed feasibility study must be carried out which will provide an estimation of the necessary changes, risks, costs (new equipment, education of staff, employment of new staff) and time required for the transition. The transition should be carried out in stages and include the necessary changes for all users, servers in the local network or the internet, applications, services, devices and individual elements. An analysis of technical and business benefits is also required. The transition must take into account the organisation's long-term goals that bring additional value, greater effectiveness, productivity and user satisfaction.

A thorough analysis is required to determine how many hardware and software elements need to be replaced or upgraded in order for it to effectively use IPv6 and IPv4. When creating an inventory list of the equipment, it is recommended to use a form with needed attributes that are prescribed in advance. Then, it is necessary to determine which parts of the network and services will the replacement or upgrade affect. When purchasing new hardware, the standard cycles for replacing equipment have to be taken into account, since the replacement cost will be substantially lower if the investment is planned. It is necessary that the equipment purchased today completely supports the IPv6 protocol and the functionalities, which will be required during the time of its service life. As long as there are no technical standards adopted in Slovenia or Europe which would accurately determine which equipment is compatible with IPv6 or capable of working with it and as long as there are no suitable certification bodies for this equipment that would check the equipment's compatibility (the manufacturer's technical specifications), it is recommended to use a list of equipment (UC - ACL Unified Capabilities Approved Products List) issued by the US military organisation JITC (Joint Interoperability Test Command) when making purchases. The above-mentioned list, prepared by the US NIST (National Institute of Standards and Technology), is used for purchasing by the US Department of Defence and all US federal agencies. More about this list is stated in the chapter discussing the comparison of national strategies.

A very important part is the implementation of education for network architects, system administrators and network managers, support services and other technical staff.

An address plan that will cover the future long-term expansion of the organisation and will include current and future services should be carefully prepared. An IPv6 (IPv6 prefix) address block should be acquired from the regional or local registry and a connection to the IPv6 network (transit and peering) should be made. A test-bed should be set up where the equipment and services will be tested and where it will be possible to train users and test the key functionalities in practice. The implementation into a live environment will be possible only after we determine with certainty that the test-bed is meeting all of our expectations.

When preparing the transition plan, we must determine the project stages and milestones that are realistically achievable and can be measured objectively. It is necessary to assign persons responsible who will be in charge of guiding the activities at individual institutions and of control and preparation of reports on the progress during individual stages. In each stage, it is necessary to check whether the planned activities have been carried out and whether the costs are within the expected limits. If all possible consequences are correctly planned and anticipated, the costs will be under control and it will be possible to minimise the risk. The deployment should be as transparent and undetectable for end users as possible.

The Role of the State and Public Services

The state should not and cannot afford a situation where operators emerge who, due to the shortage of IPv4 address space, provide their users solely with access over IPv6, while the internet services of the public administration are not accessible over both protocols, but only over IPv4. In the long term, the government also cannot afford to have its services accessible only over the IPv4 protocol. In this case, some of the citizens would turn into second class citizens, since they would be unable to access contents and services that were financed from public resources.

The state has a very important role in deploying IPv6. It must raise awareness by its example and encourage IPv6 deployment. Numerous governments of the world have stated in their strategies that IPv6 deployment is one of their priority tasks. Some of the first countries to start carrying out a transfer of their networks and services were the US, Germany and Japan. Awareness can be raised through public appearances by influential politicians who stress the importance of the transition to IPv6. A great encouragement for deploying IPv6 can be shown when ordering hardware and when developing or purchasing software in public tenders.

Where the state funds or co-funds the construction of (broadband) networks, it should demand that the networks and devices use IPv6 as the primary network protocol. The state should be the first to make it possible for their websites and e-services to also be accessible over IPv6 and at the same time to demand from their partners and providers to follow their example. It should assign substantial financial resources for education as part of workshops, seminars, academies, etc. It could financially support the development of new test-beds, applications and services that are based on IPv6. A large part of the economy is based on the continued stability and growth of the internet. How the further development of telecommunications will progress in Slovenia will largely be co-determined by the state. As the generator of demand and providing an example, it shall consequently in large part increase the growth and development of the country and increase the wellbeing of citizens.

As was shown by the IPv6 deployment analysis of Slovenian electronic communications operators, which was carried out by APEK in February 2010, the awareness of (at least the larger) operators regarding the necessary transition to IPv6 is very strong. But in the short term, IPv6 deployment requires costs that have to be justified. In a time of economising and lowering investments, this is much more difficult. Slovenia does not yet have much experience in the live environment; there is also not enough know-how (yet) by the suppliers of equipment and system integrators. During the transition phase, mutual operation of IPv4 and IPv6 equipment will be unavoidable. Service providers and operators are waiting on each other and watching who will first start to realise the transition and start the wheel of development. The most important thing in this phase is to unite the strength of the academic sphere, the industry, the operators and service and content providers as well as that of the state. Each one of the above mentioned must take up their role in their own area and in cooperation with all others and contribute to the development of Slovenia as a technologically advanced, secure and open country that will serve as an example to others.

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*, available at: http://www.ripe.net/ripe/docs/ripe-492.html

Phillip Smith, Alain Bidron: *Allocations from the last /8,* available at: 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), p. 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 Organisation Report Highlights Strong Growth in Both IPv4 and IPv6 Allocations,* available at: http://www.nro.net/media/nroReportHighlights.html,

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

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

U.S. Department of Commerce, NIST, NTIA (2006): *Technical and economic assessment of internet protocol version 6 (IPv6),* available at: 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*, available at: http://www.oecd.org/dataoecd/7/1/40605942.pdf

ITU (2008): *Resolution 64 – IP address allocation and encouraging the deployment of IPv6*, available at: 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*, available at: 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)*, available at: 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*, available at:
ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/mb_com_parlipv6.pdf

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

Geoff Huston, "IPv4 Address Report", available at:
http://www.potaroo.net/tools/ipv4/index.html

Official Gazette of the European Union (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*

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

2. Comparison of National Strategies and Action Plans of EU Member States Comparable to Slovenia, the Most Advanced EU Member States and Some Non-European Countries

The problem has been studied well. There are 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 costs 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 its citizens 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 a difference. It's time now to push for change.

This section looks at IPv6 deployment strategies outside Slovenia. The list does not aim in anyway to be complete and the countries that are listed here are in no particular order. Our only objective in this section is to provide some intuitive feeling about how other countries are acting. We are well aware of the fact that there are many other countries, which make a very significant effort to IPv6 deployment, which we could not list here.

France

France was one of the first countries to start deploying IPv6. In 2002, after politically favourable consideration by the French government and the Ministry of Research and New Technologies, they created the IPv6 Task Force. The team was chaired by Patric Cocquet, who was also the co-creator of the 6Wind project and Vice-President of the IPv6 forum and the Chinese IPv6 Council. In November 2003, the IPv6 Task Force issued Recommendations for a Strategic Plan for Development and Implementation of IPv6 Technologies in France. The strategic plan, which was supported and directed by the French government in cooperation with local authorities, contained specific activities that covered three target groups: public institutions and service agencies, the private sector and the third that focused on organisation and control of the progress of the strategy itself.

The role of state authorities and agencies in this strategy was their proactivity in starting and supporting IPv6 deployment. IPv6 was implemented into the national and regional communications infrastructure and into the infrastructure of public institutions and campuses. Public institutions and agencies, with the help of coordination bodies, had to specify and publish their strategies, methodology and time lines that would make it possible for their own or shared communications infrastructure to transition to IPv6.

With the strategic plan, France followed the following priority policies:

- connection of all public entities to the internet over IPv6, especially schools and universities,
- transition of all government web servers (.gouv.fr), which provide access over the IPv4 and IPv6 protocols,
- transition of existing applications and promotion of the development of new innovative applications that are based on IPv6,
- all communications equipment purchased through public tenders is able to use IPv6,
- public authorities should call upon business entities who are operating either independently or as a group (business associations, research laboratories, universities, schools and large companies) to encourage the implementation of internet technologies that are based on IPv6,
- following the example of the US, to prepare an estimate at the interdepartmental level about the new security strategy of the new generation of IP networks (the Ministry of Defence can have a leading role in approving procedures and technologies that have to be implemented).

The following activities were suggested for the private sector:

- larger companies should immediately begin designing and upgrading their computer sources and networks, which would gradually integrate IPv6. This should also include the transition of the existing and the development of new innovative applications to

IPv6. The applications should make it possible to take full advantage of the new functionalities provided by IPv6;

- telecommunications companies and manufacturers of professional and consumer electronic devices as well as developers of applications and publishers of programmes must integrate IPv6 into their products and publish the time lines of their availability;
- telecommunications operators must undertake certain time limits within which they will implement commercial IPv6 services on broadband wired (xDSL, Ethernet, cable) and wireless (WiFi) GPRS) networks;

Besides the strategic plan, the following French activities should also be emphasised:

- in 1995, the G6 group was established, a non-profit industry association which unites academic and industry partners. The area of G6 is facilitating the exchange of information, testing and experimenting in the area of IPv6 deployment in France;
- IPv6 was deployed in the French academic research network, RENATER. In 1995, the first pilot IPv6 services were implemented in the framework of cooperation with G6. Since 2002, RENATER has been providing a native backbone IPv6 network that provides access to more than 650 universities, research organisations and government agencies;
- in 2002, the international commercial native IPv6 network, Opentransitv6, was deployed (Asia, US, Europe);
- from 2001 to 2003, the national research project VTHDv6 (NExt Generation Internet2) was operating through the use of the IP/WDM technology that was co-funded by the French government and carried out by the RNRT (the research section of France Telecom). As part of the RNRT, IPv4 and IPv6 services and applications were provided among the partners of the project (transition from tunnelling to full dual-stack). VTHDv6 is defined as the first WLAN IPv6 campus (carried out in cooperation with the University of Strasbourg);
- the French internet provider Nerim was the first in Europe to provide IPv6 (2002). Since March 2003, it has been providing native IPv6 access over ADSL. Where native access is not possible, the provider provides IPv6 access over an IPv4 tunnel;

- in July 2004, the IPv6 AAAA record was enabled in the .fr TLD root domain,
- in 2005, the transition of France Telecom to IPv6 was carried out (dual-stack). In June 2005, an experimental broadband access for users was conducted. The IPv6 connectivity was provided over Teredo, Tunnel Broker and ADSLv6;
- France Telecom (the Orange telecommunications operator) has been one of the first global IPv6 providers over the VPN MPLS network since 2009;
- the second largest French internet provider, Free, made it possible for their users to access IPv6 internet (1,500,000 users) in merely five weeks (7 November - 11 December 2007) by using the 6rd (IPv6 Rapid Deployment) mechanism. They have been providing an independent IPv6 service (Telesite) since March 2008. In 2009, they recorded more than 310,000 IPv6 users;
- in March 2009, the Action Plan for ICT “Digital France 2012” document was published. It also includes activities for IPv6 deployment in France;
- in 2009, they adopted a decision that French public institutions must consistently order equipment for communications in public tenders that is compatible with IPv6.

In September 2010, France had six providers that provide their users with native IPv6 connectivity. 143 IPv6 prefixes have been allocated to France (France Telecom /19). There are two IPv6 exchange points operating in France (IX).

Sources:
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*, available at: http://www.orange-business.com/mnc/press/press_releases/2009/IPv6.html

IEEE Xplore: *Deployment and test of IPv6 services in the VTHD network*, available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1262168, visited on: 7 October 2010

Cassen, A. (2009): *IPv6@Free,* avalilable at: http://www.ripe.net/ripe/meetings/ripe-58/content/presentations/ipv6-free.pdf, visited on 8 October 2010

Nerim, available at: http://www.nerim.fr/ipv6, visited on: 8 October 2010

Austria

In Austria, the first activities in the area of IPv6 protocol research and deployment started in the research and education network ACONET (Austrian Academic Computer Network). But early IPv6 research and development was not limited merely to the academic environment. As early as 1999 to 2003, Telekom Austria cooperated in two international IPv6 projects: GCAP and Tsunami. The Austrian IPv6 Task Force was established in March 2004. The initiator for the establishment was Telekom Austria. It also included the University of Vienna, the national telecommunications and radiofusion regulator RTR (RTR-Rundfunk und Telekom Regulierungs GmbH) and other leading Austrian IT companies and research institutions. IPv6 deployment coincides with the state's national policy of accelerated development of broadband access. Five additional work groups were established as part of the IPv6 work group, whose main objective was to prepare a schedule and development of the IPv6 protocol deployment in Austria. The result of their work was a document entitled: "Austrian IPv6 Roadmap". The document contains an overview of all mechanisms for transition and surveys the possible transition stages. The document discusses the most frequent technical questions following the transition (DNS, routing, security, operating network and service tasks) and it discusses in detail the impact of IPv6 deployment on the existing access network and user network. It also lists specific recommendations for ADSL and cable access providers.

In September 2004, Austria provided IPv6 (AAAA record) in their ccTLD domain servers. In 2005, IPv6 was provided at the Vienna exchange point (VIX - Vienna Internet Exchange). According to Six Access and Internet

Number Resources Database data, there were 89 IPv6 prefixes or 8381 /32 address blocks allocated to Austria in September 2010.

Sources:
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

Germany

The Federal Republic of Germany is currently one of the leading European countries that is successfully implementing the IPv6 protocol into its public and private networks. According to Six Access data, Germany had the highest number of allocated (visible) IPv6 prefixes (221) in Europe in August 2010. On a global scale, only the US has a larger number (https://www.sixxs.net/tools/grh/dfp/all/-?country=de). It is also evident from the data on the above-mentioned website that Germany currently has as many as 10 providers (highest of all) who provide native IPv6 access to their users. Germany is also currently leading in Europe in terms of allocated IPv6 /32 address blocks. Based on statistics published on 4 October 2010 by RIPE NCC (http://www-public.int-evry.fr/~maigron/-RIR_Stats/RIPE_Allocations/IPv6/ByNb/index.html), 9927 IPv6 /32 blocks were already allocated to Germany, which is 28% of all allocated blocks. Germany is administratively divided into 16 federal states that are subdivided into administration divisions, municipalities and municipal associations. Each unit has their own public administration and authorisations prescribed to them by the constitution. The German government, as the Local Internet Registry (LIR), is a member of the European RIPE NCC registry. In 2009, the German government managed to obtain an IPv6 address space with the size of /26 from RIPE NCC, which is by far the largest compared to other European government institutions. An important fact should be mentioned that so far individual federal states and their subordinate institutions have been obtaining IPv4 address blocks independently or independent from each other. This has lead to large fragmentation of the address space. The new strategy established a principle for obtaining a large address space (/26), which will be allocated in Germany systematically depending on requirements according to a pyramid, from top to bottom.

Important driving forces in deploying IPv6 in Germany are the Office of the Federal Government for Information Technology (Die Beauftragte der Bundesregierung für Informationstechnik) and the German IPv6 Council (Deutschen IPv6 Rat).

The German IPv6 Council was established in 2007 under the authority of Prof. Christoph Meinel and Latif Ladid. Upon establishment, they outlined that their mission is to provide technical management and innovations, which will facilitate successful implementation of the IPv6 protocol into all spheres of the German network and telecommunications infrastructures. To achieve these goals, the Council created an open platform that combines various technical experts from the field of IPv6.
14 May 2009 is considered an important milestone during the time of the second German IPv6 Summit (Deutsche IPv6-Gipfel) when the Action Plan for the Deployment of IPv6 (Nationaler IPv6-Aktionsplan für Deutschland) in Germany was published. The action plan also coincides with the Broadband Strategy of the Federal Government (Breitbandstrategie der Bundesregierung) published in 2008.
The action plan, prepared by the German IPv6 Council with the coordination of the international IPv6 Forum and the European Commission, contains objectives and identifies possible gaps, opportunities and concrete measures that will facilitate the successful deployment of IPv6 in Germany. It is intended for a broad circle of stakeholders: politicians, public administration, schools and researchers, the private sector and other interested parties. The document describes necessary activities in the field of public communication, exchange of knowledge, education, research and coordination among the interested partners. It also proposes concrete measures that are regularly updated and expanded in accordance with the current state of development.

As is stated in the action plan, Germany, as the leading export-oriented country, must be aware that it must connect with other regions and simultaneously follow the advancement of technology. Here it also especially stresses the importance of China’s rapid development. If they overlook the transition to IPv6, it will unavoidably lead to a collapse of the existing development, primarily in Asia as the most advanced region. This will have an immediate (negative) impact on the German economy and exports.

Therefore, timely preparation for the upcoming demand for IPv6 services, applications and devices is a priority. With continued development, they will achieve a secure and competitive advantage on the global market. By deploying IPv6, they want to grab the opportunity and understand the transition as the start of a new generation of the internet and networks. In this context, this viewpoint should be transferred to all interested stakeholders such as: internet organisations, operators, hardware and operating systems providers, programme application providers, researchers and educational organisations and public administration at the federal, state and local level. By recognising the stakeholders, they also concretised the roles that they have in the transition to IPv6.

The German action plan pursues the objective of the European Commission, namely to ensure access to IPv6 internet and service to at least 25% of users by the end of 2010. In this context, Germany pursues the three-stage transition plan as described in RFC5211 (An Internet Transition Plan). In the first (preparation) stage of the plan, which was intended to be completed by December 2009, the internet service providers (ISPs) should start test-implementing individual IPv6 network services, and organisations connected to these networks would also provide their internet services over IPv6. In the second stage (the transition stage), from January 2010 to December 2011, the internet service providers should begin providing IPv6 and IPv4 services, and the organisations would provide their IPv6 services in the live environment. In the third stage (after the transition), which was supposed to be carried out from January 2012 onwards, the organisations should provide all internet services and connectivity over IPv6. In the transition stage, the action plan provides for a shared use of both protocols (IPv6 and IPv4).

Concrete activities of the action plan also include organising the annual German IPv6 Summit with international participants. The IPv6 Summit was also identified as a good opportunity for carrying out an international contest for selecting the most innovative IPv6 applications or ideas that help in implementing and developing IPv6. The contest that has been taking place in Germany since 2009 is sponsored by recognised sponsors from the field of research, industry and the economy. The contest, which is divided into three categories, awards the winners financial awards or/and prominently presents them in the framework of public communication.
The issuing of publications in national newspapers and popular science magazines as well as broadcasting information on the radio and television were all recognised as an important part of raising public awareness.

Germany is aware that, to achieve the objective, a general consensus and readiness for action by all involved is required at all levels of the society, primarily among economists, politicians, in public administration and among users, researchers and academics.

Politicians and the public administration have great influence in raising awareness and should speak to the public about the importance of the transition to IPv6. It is necessary to provide IPv6 access to all public government services (e-Government). In particular, the most visited websites of the government and the public administration should also be quickly accessible over IPv6. In public tenders for new content or services, IPv6 should be the obligatory protocol. The existing internet services and services that will be updated and upgraded have to provide access over IPv6. As part of the cycle of replacing equipment, it has to be ensured that the purchased hardware and software support IPv6. When forming all new projects, IPv6 should be an integral part of technical requirements. Public administration, network operators, hardware and software traders and operating systems developers must ensure the security and privacy of IT.

Research projects funded by public or European funds should take advantage of the potential of IPv6 as soon as possible. Each educational or scientific institution should also provide their websites and services over the IPv6 access. It has to be ensured as part of the innovation cycle that all hardware and software is ready for IPv6. Universities and research institutions should be a multiplier and lead to new forms of services that are based on the development of the IPv6 technology.

All providers of content, services and network operators should show determination to implement the required adjustments of the technology, which would enable a national transition to IPv6. The infrastructure for end users must be in accordance with IPv6. In particular, the most visited websites of the private sectors should be immediately accessible over the IPv6 protocol. It is necessary to research the possibilities for developing new innovative IPv6 products and solutions, especially in the field of the IT security.

In 2009, the Federal Office for Information Security (BSI – Bundesamt für Sicherheit in der Informationstechnik) issued the "Recommendation for a Secure IPv6 Network Infrastructure". The recommendation discusses security risks created by the transition to IPv6. Projects for the transition and updating of the communications infrastructure through the participation of all public institutions began the same year. The German Connected Infrastructure (DOI - Deutschland-Online Infrastruktur), which is the main communications infrastructure of the federal government, is already supporting IPv6 in full (it operates in dual-stack). Germany is also rapidly implementing IPv6 into other state communications infrastructures. Network security devices and devices for traffic encryption are being tested. A general network for federal administration (NdB – Netze des Bundes) is being designed. A distribution of the allocated address space is also in the design phase. The first IPv6 address blocks shall be allocated to federal states (DOI), including the IP services providers, and to the Ministry of Defence. An organisational concept is in the process stage. Recommendations for transition and operation, a configuration checklist and address templates are being prepared. They have started various pilot programmes such as VoIP over IPv6 (VoIP Dataport/Hamburg with 150,000 VoIP devices) and test DOI networks for transportation and services such as e-mail, DNS, network security and coding devices. A feasibility study and a study on the expenses of renewal of websites were carried out (www.cio.bund.de). Currently, the websites are in a test environment.

There are several projects being carried out or prepared that relate to IPv6 deployment (Schülting 2010). The objective of the IPv6 Profile project is to prescribe a set of necessary functionalities that the network equipment should meet in order to be compatible with IPv6. The project is being carried out by DOI and FHG, and the BMI (Federal Ministry of Interior) is partially co-financing the project. Recommendations will be prepared which will assist the administration in purchasing equipment and the effect on the public IT infrastructure will be provided.

Services are being tested in a test-bed such as: network control, mobility and multicast on IPv6. Compatibility tests and tests of interoperability are being carried out. Migration tools for online government applications (e-Government) are in preparation. A migration guide for municipalities is in preparation. In the field of IPv6 security, recommendations for a secure communication from end to end, NAT replacement and requirements for devices for network security are in preparation.

Germany has joined the deployment of IPv6 actively, systematically and with strong support from the federal government. Although they have also detected a lower demand due to the global recession, Germany has not lowered the budget for the ICT infrastructure and equipment. Their budget at the federal level for ICT equipment is EUR 500 million. In the frame of these funds, their goal is to strengthen the ICT sector and facilitate modernisation at the level of all federal administrations. They have set 360 priority goals and criteria to be achieved by 2011 with which they will improve IT security in the federal IT infrastructure and at the same time lower the impact on the environment.

Sources:
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
National IPv6 Action Plan for Germany:
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

Denmark

The Danish government, based on a proposal by the European Commission, also took over the initiative for the deployment of IPv6 in their country. It acts as an intermediate link, an intermediary between all interested stakeholders, network and service providers and users. Their Ministry of Science, Technology and Innovations prepared a strategy for IPv6 deployment for the Danish government in 2009. According to the action plan, IPv6 deployment is important both for the public as well as the private sector and must thus be carried out as a model of public and private partnership. The model of partnership strengthens these effects even further by providing a firm foundation and coordination of specific activities among stakeholders and the ministry.

Their action plan also recommends to the Danish government that it should be in charge and more decisive in investing into infrastructure, especially in the transition to IPv6. The policy of public procurement of hardware, software and network equipment should set clear requirements for the support of IPv6. The infrastructure is owned by the private sector and the development of the hardware and software market is competition based. It is essential for development that internet providers and infrastructure owners, who are usually larger telecommunications companies, are included into the transition to IPv6. Such partnership should include all actors that are influenced by the transition to IPv6: government representatives, .dk domain registries, internet providers, hardware and software providers and other interested organisations. The Ministry of Science invited the interested partners to establish a knowledge centre intended for all who are dealing with the issue of IPv6. The knowledge centre, where the above-mentioned ministry is also participating, provides the interested parties all the necessary information that relates to deployment of and transition to IPv6.

The Ministry of Science has assigned a special competent group in charge of the Danish regulator of electronic communications, NTA (Telestyrelsen – National Telecom Agency), to monitor the implementation of the transition to IPv6. According to the Danish law on internet domains [1], NTA is also responsible for the .dk domains registry.

The Danish government is aware that combining information forces is also an important part of the process, since this is the only way to ensure satisfactory and continued advancement. The government of Denmark thus perceives many combination effects that can be achieved in relation to the .dk domains registry (NTA), particularly in areas such as:

- changes to the public procurement policy,
- challenges created by the security policies during the time of transition,
- international processes and IPv6 deployment.

The target group for the joint efforts is very broad from the viewpoint of collecting the necessary information and from the viewpoint of the required professional qualifications needed for their understanding. As a priority, the action plan separates the section that is oriented towards the profession and the section that could be oriented towards citizens and to raising their awareness.

The document notes that the transfer of knowledge is important primarily on the professional market, which will use IPv6 for innovation and product development, and will also be responsible for the practical implementation of protocols in companies, internet providers, etc.

Citizens also have to be informed about the transition but to a lesser extent, because the transition shall not affect the majority. Their expectations show that the transition period will last a long time. The transition to the new protocol shall be gradual for citizens; it will take place simultaneously with the replacement of computer equipment at home. Citizens thus need information of a more general nature, particularly from the perspective of security and the increased risk of hacker attacks due to the coexistence of IPv4 and IPv6. The Danish Ministry of Science also cooperates with relevant stakeholders participating in the partnership model in such transmissions of knowledge.

The public procurement policy shall also be changed. The ministry wants to create a market as part of the public procurements with a satisfactory quantity of suitable products, of suitable prices and with IPv6 protocol support. With this approach, the new equipment shall contain all necessary functionalities and capabilities, regardless of whether a final decision on the transition to the new protocol is reached. To ensure a joint strategy and larger market size, the public procurement policy shall be coordinated with local and regional authorities that are under the auspices of the Danish government and Danish districts. The government's public procurement policy shall be coordinated so that the procurements will contain minimum requirements of IPv6 support in hardware and software and at the service level. The mentioned procurement process started at the end of 2008 when the Danish Office for Public Procurement of the Ministry of Finance submitted the first tenders for procuring network devices and components. All tenders published by the Danish regulator of electronic communications NTA, as part of the management of the .dk domains registry, also include minimum requirements according to which the registry system, including domain servers, must support IPv6. In accordance with the Communication of the Commission to the European Communities (Action Plan for the Deployment of IPv6), the indicated strategy and action plan for the period up to 2010 also includes the provision of access to government websites over IPv6.

The changes of IPv6 deployment are also being carried out in other digitalisations in Denmark. IPv6 is becoming a non-obligatory open standard. When promoting the use of IPv6 in the public sector, the current IPv6 status shall change from "useful" to "recommended". The more the market with IPv6 products evolves, the greater will be the demand for IPv6 to become an obligatory protocol in the public sector network.

The Danish government is also aware that communications networks play a decisive role in the event of possible crisis events or natural disasters. The capability of transferring information and ensuring coordination depend on the accessibility and robust and secure networks. The government thus has a special task, which ensures that electronic communications, which are vital for the society, are protected in publicly accessible networks. In relation to managing the .dk domains registry, in 2009 the Danish government imposed on the Danish regulator an issued licence that, besides general operations of the IPv4 address space, the domain registry must also provide management of the IPv6 address space.

The Danish government also expects the public network operators to reach a mutual agreement in order to prepare a prioritisation scheme for the IPv6 networks similar to the current public fixed and mobile IPv4 networks. This will provide a suitable traffic prioritisation in the event of natural disasters or other incidents. Such an agreement between operators based on a voluntary basis shall enable the transfer of vital data communications with the highest prioritisation made possible by the IPv6 protocol.

Based on the Danish time schedule for the implementation of actions, the process shall last at least two years from the first discussions to the first IPv6 deployment. The public discussions started in the third quarter of 2009. In the first quarter of 2010, detailed planning began and the first training will end at the end of the first half of 2011.

Their action plan does not contain reliable estimates of complete national expenses, which the IPv6 deployment brings. They expect that the annual costs shall remain at a relatively low level if the IPv6 implementation is carried out gradually over the course of several years and is planned in advance. They expect the transition to last at least ten years. If the transition to IPv6 is carried out gradually, it can be controlled and planned as part of the current operational schemes and schemes for updating the equipment, thus additional costs for IPv6 can become an integral part of the operating costs of each stakeholder.

Sources:

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)

Finland

One of the first pioneers of IPv6 deployment in Finland was "CSC - IT Centre of Science", which is managed by the Finnish Ministry of Education, Science and Culture. CSC manages the Funet backbone network, which provides IPv6 connectivity for Finnish research and education networks and also simultaneously connects the network into the pan-European GÉANT2 network. From 2002 to 2005, the CSC actively participated in the 6Net Project that was financed by the European Community as a pilot IPv6 project. According to surveys published last year by the Finnish Ministry of Transportation and Communications, the Finnish operators are well prepared for the transition to IPv6. Based on data from the Finnish Communication and Internet Exchange Association (FICIX), 20 to 28 members are already transferring IPv6 traffic. Despite this, only a few Finnish operators are actively promoting IPv6 routing for commercial purposes.

Currently, there is only a small number of Finnish companies that are ready for the transition to IPv6. The reason is primarily of a financial nature: changes to routers, switches, applications and data security are required. Based on a questionnaire distributed to two hundred operators in 2008 by the Finnish regulator of electronic communications, Ficora, only one operator provides users with IPv6 connectivity.

CSC is actively promoting IPv6 implementation in the framework of the Funet network. In 2009, the Finnish researcher Teemu Kiviniemi developed a protocol converter for multicast services as part of his master's thesis. With the help of the Helsinki University of Technology, the converter was successfully integrated into the Funet network. With its use, the IPv6 multicast services are now also provided to users with IPv6 connectivity.

The Finnish Ministry of Transportation and Communications would very much like to encourage the operators to prepare for IPv6 even more. They are preparing the "National Information Society" Project that will specify the schedule for IPv6 deployment. The ministry shall also encourage IPv6 deployment by informing the public regarding the possible issues of the transition. They want to establish norms with which they shall obligate the operators to include a requirement for IPv6 support when procuring equipment. The Finnish regulator Ficora is also striving for IPv6 and is encouraging its deployment. In 2009, in its 2009-2015 work strategy (Ficora 2009), it also undertook, along with its operational assignments, to actively promote the implementation of IPv6 in cooperation with Finnish communications operators. Ficora is also striving to start awarding the "IPv6

Ready" logo to all consumer communication devices that would meet the required IPv6 functionalities. Some of the operators are also in favour of this proposal, because they believe that this can be one of the possible methods for encouraging IPv6 deployment in Finland.

Sources:
CSC (2010): *Slow progress in IPv6 implementation*, available at: http://www.csc.fi/english/csc/publications/cscnews/2010/1/IPv6, visited on 1 October 2010

Finnish IPv6 Task Force: http://www.fi.ipv6tf.org/

Ficora (2009): *THE STRATEGY OF THE FINNISH COMMUNICATIONS REGULATORY AUTHORITY 2009-2015*, available at: http://www.ficora.fi/attachments/englantiav/strategy/5jyWB7NAG/DOHA_n561005_v1_Viestintaviraston_strategia_2009-2015_in_English.pdf, visited on 15 October 2010

Czech Republic

The Czech Republic is one of the most active countries of the European Union in implementing DNSSEC. According to the data from May 2010, 15% (~98,000) of Czech domains have already been signed (Filip, O., 2010). They are less successful in deploying IPv6, even though they have already implemented certain specific actions. It is evident from the statistics (CZ.NIC 2010) maintained by the Czech registrar, CZ.NIC, that in September 2010, 3.61% (25,752) of DNS servers supported the AAAA record. A year before, this value was almost 5 times lower. Even greater progress was made in regard to mail servers, as in September 2010, a 5.7-times higher growth was recorded than the year before (43,713 or 6.13% of mail servers have at least one IPv6 MX record). Noticeable progress has also been made in advertising the BGP route with the IPv6 prefix. In 2009, there were 29 autonomous ASN systems advertised over BGP; this September there are as many as 56 ASNs with the IPv6 prefix. Compared with IPv4 with 535 ASN systems registered, this is still a relatively low number. At the NIX.CZ exchange point, there are currently 99 connected organisations with IPv4 connection and 39 organisations with IPv6 connection (Petr 2010). There is less than 90Mbit/s of peering traffic compared to IPv4, of which there is more than 74Gbit/s. The number of domains that are accessible exclusively over IPv6 is also increasing. There are currently 8 of those. There are 77 IPv6 prefixes, size /32, allocated to the Czech Republic.

According to data from a representative of the Czech Ministry of Industry and Trade of Electronic Communications, Monika Kunzova, the Czech government adopted a resolution in 2009 that requires all ministries and other government administrations to replace it with IPv6 compatible equipment when replacing network equipment. By 31 December 2010, all of their websites and publicly accessible services of the e-Government must be accessible over the IPv4 and IPv6 protocols. The latest analysis that was carried out at the competent ministry has shown that all of the above mentioned institutions already meet the first condition in full, and the second is in the stage of implementation.

Sources:
Filip, O. (2010): DNSSEC.CZ, available at:
http://www.ripe.net/ripe/meetings/ripe-60/presentations/Filip-DNSSEC_in_CZ.pdf, visited on 14 October 2010

CZ.NIC (2010): *IPv6 statistics*: available at: http://labs.nic.cz/page/756/, visited on 14 October 2010

Petr, E. (2010): *IPv6 v ČR,* available at:
http://www.nic.cz/public_media/IT10/prezentace/den_2_5_Petr.pdf, visited on: 14 October 2010

United States of America

The US made a systematic decision at the government level to implement IPv6 into their government communications and information network within certain time limits. The legal basis for starting the IPv6 deployment in the networks of federal government agencies is the "Transition Planning for Internet version 6 (IPv6)" memorandum, which was issued by the OMB (Office of Management and Budget) in 2005. The OMB, which oversees and directs the work of US government agencies, prescribed that all federal agencies must start using IPv6 in their backbone networks and to connect with their interfaces into the IPv6 network by June 2008. The document specifies specific deadlines and requirements, which that must be met by government agencies by the specified date. The following activities are prescribed:

By 15 November 2005:

- assigning a person responsible for managing and coordinating the planning,
- an inventory list of all existing routers, switches and hardware firewalls (prescribed content that must be included in the list),
- an inventory list of all other devices and technologies compatible with the IP that are not included on the previous list,
- starting an analysis of the financial and operational effects and risks that are the result of the transition to IPv6 (prescribed content of the report).

By February 2006:

- in accordance with recommendations issued by the Chief Information Officers Council Architecture and Infrastructure Committee, to start a plan for the transition to IPv6 (prescribed guidelines of the required activities),
- to submit a report on the progress of making an inventory list of equipment and on the analysis of the effect of the transition to IPv6.

By 30 June 2006:

- a complete list of compatible IP equipment and technology that was not included in the first list,
- a complete analysis of financial and operational effects and risks.

By 30 June 2008:

- all agency infrastructure (backbone networks) must use IPv6 and the agencies must be connected into this infrastructure with interfaces. On this day, the agencies must report at a joint meeting on the progress that is a part of their transition strategy.

The agencies had to carry out the stated activities by June 2008 without endangering the IPv4 functionality or network security. The stated date was not obligatory for the transfer of applications, peripheral devices or other IT assets. As was reported on July 2008 at the Federal Computer Week (Mosqure 2008), the majority of agencies complied with the memorandum's obligations within the deadline.

The memorandum imposes on the agencies the need to ensure in the future that all newly purchased ICT equipment is compliant with IPv6. An IPv6 compliant product or system must be capable of accepting, processing, transferring or forwarding IPv6 packets and must be compatible with other systems and protocols in IPv4 and IPv6 modes.

The US NIST was chosen to develop the required standards that will provide a uniform system of required specifications and a certification method for all government institutions. These are obligatory for purchasing IPv6 equipment. The memorandum was followed by other important documents. Worth taking note of is a document from January 2006 issued by the US Department of Commerce in cooperation with NIST and NTIA (National Telecommunications & Information Administration). The document "Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6)" discusses the technical and economic effects that relate to IPv6 implementation including the role of the government of the US in the transition, international compatibility, security in transition, costs and benefits created by IPv6. The study finds that IPv6 creates important benefits for US business operations and for the users that will become evident only with time. The majority of internet experts and industry stakeholders in general agree that IPv6 networks will be technically better compared to current IPv4 networks. A larger address space created by IPv6 can potentially encourage many new innovative communications services and applications. Compared with IPv4, IPv6 will with time become a more useful and more adjustable mechanism for ensuring end-to-end user communication. The study also notes that rapid IPv6 implementation is hindered by numerous obstacles. Among those, there are many durable devices and applications that serve us well. Because they are only compatible with IPv4, they will have to be replaced. If we want to fully realise the potential of the communication capabilities of the IPv6 protocol, financial and human resources will also be required for the transition to IPv6.

From an economic viewpoint, the transition costs can be lowered, if the transition is planned in the framework of the standard cycle of replacing or upgrading the equipment. As part of replacing equipment, the majority of costs constitute educating staff, replacing and configuring equipment and network testing. It does not include the procurement of the equipment, as the price is not significantly higher compared to IPv4 equipment. The costs of the transition shall also differ for various user groups. In smaller and medium sized companies and end (residential) users who do not manage larger networks, the cost shall be relatively low and can be planned in the framework of the standard cycle of replacing equipment. In contrast, larger companies (corporations) and government agencies will have higher costs, where the fluctuation depends on the existing infrastructure and operational policy. This also includes applications that will have to be changed or developed anew. It also depends on how much the users will be connecting with other organisations that use IPv6. Activating IPv6 for routine use can actually occur only when a critical mass is achieved that shall be replaced with IPv6 technology. The transition shall be carried out routinely when appropriate operational and security plans and extensive training of human resources are carried out.

As they note, the greatest potential of security benefits created by the IPv6 protocol is related to the long-term development of a new security paradigm that is significantly different from the one currently established in the existing IPv4 networks. Today's networks are based on the security architecture of a parameter that is network-centric, and in future, the networks will be based on end-to-end models (host-based) that will be better at adapting to the environment. The required time and costs needed for designing and developing new security models shall be significant; however, creating new, more effective security paradigms shall benefit all current and future internet users.

Experts agree that deploying a new protocol such as IPv6 increases threats and the security vulnerability of information systems in the starting phase. Additional resources will be required that will be able to deal with the threats of a dual environment (IPv4 and IPv6). Because IPv6 is already a part of the protocol stack of much of the hardware or software equipment, it is highly likely that IPv6 will appear in operational networks without the knowledge of (uninformed) network managers and independent of the plans of organisations. Therefore, all organisations should develop the necessary plans and policies that would deal with IPv6 traffic regardless of their decision on whether and when to carry out the transition to IPv6. Even though the transition mechanisms were carefully planned for various scenarios, the operation in the dual stack mode increases the security risk.

The workgroup that prepared the above mentioned analysis has also determined that there are no major obstacles on the market that would prevent the industry from investing into IPv6 products and services, regardless of its needs or consumer demand. Therefore, there are no well-founded reasons and requirements for the US government to accelerate the

IPv6 deployment with aggressive actions against the private sector. In the near future, the private sector will have to carry out a careful analysis of their business plans for adopting IPv6. Thus, they will also face the inevitable occurrence of IPv6 traffic in the interior and exterior of the network. Taking into account the information system of the public sector, the authors of the study recommend that government agencies start analyzing the business plans for deploying IPv6 and develop suitable security plans. Because this creates certain costs, the recommendations emphasise that careful planning, development and evaluation are required, which must have precedence over specific decisions on implementing the new IPv6 technology into the operational network. The results of the presented study have namely shown that there are well-founded technical and economic risks that could be related to the lack of a suitable plan and strategy for the deployment of IPv6.

In February 2006, the Federal CIO Council Architecture and Infrastructure Committee also issued recommendations for the transition in accordance with the instructions of the memorandum to help federal agencies in transitioning to IPv6 (Federal CIO Council Architecture and Infrastructure Committee 2006). The recommendation is actually a set of three chapters that were made soon after the memorandum was published. The final document contains three chapters, including remarks by the agencies. The first chapter describes the instructions for the transition to IPv6 in companies with a business infrastructure. The second chapter discusses more technical elements that are important for the transition of the agencies. This chapter collects the best practices of the transition to IPv6. It provides information relating to the network and infrastructure, addressing, providing information, pilot deployments, testing and representations, applications, standards and education. The third chapter discusses IPv6 transition governance. It describes the management structure and individual roles and responsibilities of the participating agencies and organisations.

In 2008, NIST published the final version of the recommendations or requirements and procedures in accordance with the memorandum's requirements, based on which individual ICT equipment can obtain the status of IPv6 compliance and the label of possible coexistence with IPv4. The publication, titled "A profile for IPv6 in the U.S. Government (USG IPv6 Profile)" is a document which states the minimum operational technical requirements that must be supported by network devices such as hosts, routers and intrusion prevention systems (IDS) and firewalls. The profile was developed to assist federal agencies in their development plans,

procurements and implementation with IPv6 compliant equipment and simultaneously to ensure the compatibility and security of information systems. As stated in the introduction of the document, there is a still a lot of IPv6 equipment on the market with varying degrees of maturity and which is far from perfect. By preparing the profile, they outlined effective de facto standards of completeness and correctness that will help secure the investment for early IPv6 deployers. The profile is not just useful in the short term, but follows a strategic long-term plan of the US in deploying the IPv6 technology.
Each device that receives the mark of compatibility or capability of functioning with IPv6 must go through a strict testing and certification with accredited test laboratories and accreditation bodies that meet the ISO 17025 standard (General Requirements for the Competence of Testing and Calibration Laboratories). For this purpose, NIST prepared a document that specifies test methods and validations in detail (SP 500-273 Guidance on IPv6 Test Methods and Validation). After successful testing and certification, the manufacturer's equipment is entered on the APL list (Approved Parts List) of IPv6-compatible products (http://jitc.fhu.disa.mil/apl/ipv6.htm) that ensure compatibility with prescribed technical specifications (RFCs).

The US Department of Defence (DoD) also prepared a detailed specification of requirements and technical standards that must be met by the IPv6 capable software and hardware (DoD IPv6 Standard Profiles For IPv6 Capable Products). The document, which is regularly updated, has similar requirements to the USG IPv6 Profile. Currently the latest, fifth version was published in July 2010 and is intended for a wide range of stakeholders such as: persons competent to purchase equipment, organisations that engage in testing, defence developers and sellers of equipment. Even IPv6 capable equipment must go through strict testing, which, if it is suitably compliant, ends with the certification by the US military organisation JITC (Joint Interoperability Test Command). All communications equipment purchased and used by the US army must comply with the mentioned document and must be tested and certified by JITC. JITC carries out equipment testing and certification for all products, including the functionality of voice, data and video transmission. Currently, there is an ongoing debate between NIST and the Department of Defence regarding the testing programme, but there are no significant differences between the functional requirements. It is very likely that products that are approved by one programme are also compatible with products approved by the other (the authors of both documents cooperate with each other).

The CIO Council also prepared two additional documents for the purposes of the US government and agencies for the transition to IPv6. The first document of December 2008 (The Business Case and Roadmap for Completing IPv6 Adoption in US Government) was left in the draft phase and was replaced in May 2009 by the document “Planning Guide/Roadmap Toward IPv6 Adoption within the US Government”. The document is intended for chief information officers, network infrastructure architects and other individuals in federal agencies who are responsible for using the information technology. The purpose of the document is to deepen the understanding of the federal government's vision in deploying IPv6 and to provide all agencies with specific policies that will provide a successful adaptation of the protocol. Based on information covered in the document, the chief information officers will find it easier to recognise and develop business plans that include the use of IPv6. The document is based on the above mentioned memorandum that requires federal agencies "to be IPv6 ready". The document offers an overview of how the transition to IPv6 affects the company architecture and the planning of capital, investments and control. It gives the chief information officer practical guidelines and general milestones that can make it easier to implement IPv6 network services. It provides a description of how the transition affects the federal initiatives such as Trusted Internet Connections (TIC) and the Homeland Security Presidential Directive (HSPD). It also contains clear positioning of the IPv6 protocol as an integral framework and organisational principles for a federal next generation IT infrastructure. Although the document is primarily intended for federal agencies and their staff, the document is a good starting point for all chief information officers and technical staff in companies.

According to data by SixXS, the US has 9 providers that provide native IPv6 connectability to their users. Among the larger companies and internet providers who have already implemented IPv6 or have it in their production, we would like to emphasise the following: Comcast (the largest cable operator in the US), Google, Facebook, Verizon (an operator for business users and government institutions), NTT, AT&T, Sprint (telecommunications provider for the US government), Hurricane Electric (global internet access provider), Microsoft and many more.

The US addressed the task of deploying the IPv6 protocol at a highly professional level. The main initiator of IPv6 deployment was not the private sector but the US federal government. With the requirements in the memorandum, the government set milestones and guidelines for the

transition to IPv6 for all federal agencies. With the creation of NIST's document, “USG IPv6 Profile”, and the “IPv6 Capable Products” document that was issued by the Department of Defence, it established basic minimum technical standards of IPv6 compliance and capability that are now supported by all major ICT equipment manufacturers. With the document “Planning Guide/Roadmap Toward IPv6 Adoption within the US Government”, they established guidelines for further IPv6 development and deployment for all federal agencies and others.
The US can therefore be an example of good practices, whose guidelines and experience should also be used in Slovenia.

Sources:
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, available at: http://fcw.com/articles/2008/07/01/omb-agencies-met-ipv6-deadline.aspx, visited on 1 October 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/

Japan

Japan is one of the most technologically advanced countries in the world. The Sony Corporation, for example, announced as early as 2003 that all their products will support the IPv6 protocol after 2005 (IPv6Style, 2003). Japan, as a technological world power, came to the realisation that the process of constructing or upgrading the existing networks to IPv6 also consecutively provides the opportunity for faster development and penetration of its industry of network equipment manufacturers on the global market. Japan is one of the first Asian (or even beyond) countries that took the lead in deploying IPv6. In September 2000, Japan was the first government in the world to publish a national strategy for IPv6 deployment (Popoviciu, Grossetete 2006). It is the government's long-term strategy of broadband development in Japan called "u-Japan" (Ubiquitous Japan). With this strategy, they undertook to deploy IPv6 by 2005. At the same time, the IPv6 Promotion Council was established that represents a link between the government, the industry and research organisations and ensures that the goals set by the above mentioned u-Japan strategy are realised. Internet Initiative Japan (IIJ) was the first commercial Internet Service Provider in Japan, in 1998 they started deploying IPv6 in their network. In 1999 IIJ provided an experimental IPv6 tunnel service. With the WIDE project (Widely Integrated Distributed Environment), Japan provided academic institutions with support in developing new IPv6 applications and tax reliefs for organisations that decide to implement IPv6. The NTT Communications established the native IPv6 access to the NTT backbone network (NTT Communications 2001). In 2002, it was announced that the European IPv6 Task Force and the Japanese IPv6 Promotion Council signed a strategic alliance in deploying IPv6 (IPv6 Task Force 2002). In 2002, the major internet providers already started implementing the first IPv6 services (Kosuke 2002). NTT started providing IPv6/IPv4 access over ADSL (NTT Communications 2001). In the same year, testbeds were established by terminal providers (sensors, webcams, home devices) and service providers (internet in vehicles, trains, medicine, online games). The first test services for mobile telephony began appearing. Providers of (home) routers started providing their products (Hitachi, Fujitsu, NEC, Furakawa Electric). To raise awareness, they prepared a special showroom where they showed various intelligent home devices that offered connectivity in IPv6 (refrigerator, microwave, digital and online cameras, TV, internet terminal which combines the RFID label with Mobile IPv6 technology. In the framework of raising awareness, they started publishing special publications (IPv6 Magazine)

where experts write about new technical standards, services, products and activities from the field of IPv6. Various promotional websites were set up in order to introduce IPv6 technology and the advantages that it brings (for example http://v6start.net).
In 2008, the Task Force for IPv4 Exhaustion was established that contains 22 organisations related to the internet in one way or another. The group solves issues from the field of technology, operation and management and helps in performing trainings and workshops and raising awareness. Their goal is to ensure smooth and timely IPv6 deployment via various activities.

Japan adopted the "IPv6 Forum Ready" programme with which they started testing device compatibility with IPv6. Based on this programme and based on awarding the IPv6 Ready logos, the Japanese industry became the leading world manufacturer of IPv6 equipment.

Even though Japan started implementing IPv6 relatively early, their analyses show that it is two years behind with IPv6 deployment (Mikawa, 2010).
Japan is investing between 10 and 13 million dollars annually into the IPv6 technological market. According to the estimates of the Japanese government, this will fetch 1.55 milliard dollars by the end of 2010.

Sources:

IPv6Style (2003): Sony. In 2005, all Sony products will be IPv6-enabled, available at: http://www.ipv6style.jp/en/interviews/20030212/index.shtml, visited on 1 May 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, presentation at the Internet Governance Forum 2010, Lithuania

Popoviciu, C.P., Grossetete, P. (2006): The role of National Strategies in maintaining Competitive Edge in Information and Communication Technologies, available at
http://www.iiisci.org/journal/CV$/sci/pdfs/P563955.pdf, visited on 1 October 2010

Kosuke, I. (2002): IPv6 Deployment in Japan – the way we accomplish, available at:

http://www.eu.ipv6tf.org/PublicDocuments/v6TFII_v6PC_jp_kosuke.pdf, visited on 12 September 2010

NTT Communications (2001): Actions of NTT Communications, available at: http://www.ntt.com/ipv6_e/data/e_about_com.html, visited on 1 October 2010

IPv6 Task Force (2002): *Euro IPv6 Task Force and IPv6 Promotion Council of Japan Forge Strategic Alliance to foster IPv6 deployment world-wide*, available at: http://www.ipv6tf.org/PublicDocuments/TF-v6PCJointPressReleasev2_FINAL.pdf, visited on 15 March 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/

Matsuzaki 'maz' Yoshinobu, "IPv6 deployment at IIJ", http://www.apricot.net/apricot2009/images/PDF_files/iij-ipv6-deployment.pdf

China

China is currently one of the fastest growing countries in terms of the number of internet users. It is estimated that China had about 513 million internet users in January 2012 (Tait, 2012). In recent years, it was very productive, as it caught up with the development that lasted decades in other countries. China adopted a decision on implementing IPv6 by establishing the China Next Generation Internet (CNGI) programme. According to their estimates, the programme was successful, since it was supported by government institutions and the major telecommunications operators of backbone networks. Because a large part of internet users are mobile users, support for the Mobile IPv6 protocol was implemented into the programme at the very beginning. The main motivation of IPv6 deployment in the framework of the CNGI Project was primarily greater network effectiveness, end-to-end security and the possibility of increased cooperation with foreign governments, particularly the European Union and Japan (Tezel 2010).
Before implementing this programme, China was 10 to 20 years behind in technological development compared to other comparable countries. As part of the five year CNGI Project that was started by the Chinese government,

one of the largest commercial backbone IPv6 networks of the next generation was built. In a programme with a budget in the amount of 170 million dollars, six national backbone networks were built by 2009. Five were commercial (China Telecom, China Netcom, China Mobile, China Unicom, China Railcom) and one was academic (CERNET2). With 39 ten gigabit entry points - nodes (PoP), they connected 40 of the largest cities and more than 300 academic, industrial and government and research campuses. CERNET2, which is the backbone of CNGI, has 25 PoP nodes in twenty cities, making it currently one of the largest education and research networks that is entirely based only on the IPv6 protocol (the network has no IPv4). Within the network, equipment from various suppliers is used. For the transition, they use mechanisms such as IPv4 over IPv6 (IETF software) and IVI (IETF).

One of the largest public presentations of the results of the CNGI Project and the IPv6 infrastructure was also the implementation of the Olympic Games in Beijing in 2008. The communication infrastructure of the Olympic Games including all data links and all network broadband and mobile applications and devices that were used at the Olympics were based on IPv6 protocol. The event attracted a lot of attention, because it was an example of good practices, the first large implementation of the IPv6 production infrastructure.

In 2009, China Telecom officially announced its plans to deploy IPv6 (Digaria, 2009). In the initial phase, which will last until 2011, they will outline and establish a new platform at the business and network level that will enable operations over IPv6. Between 2012 and 2015, the first phase of commercialisation will occur. For this phase, they plan a co-existence of IPv6 and IPv4, implementation of new applications and a gradual transfer of operations to IPv6. After 2015, they expect a full commercialisation of the use of IPv6. New applications will be predominantly based on IPv6, and the networks and operations that are based on IPv4 will be gradually cancelled (by 2015).

Sources:

Cnet (2004): *China launches largest IPv6 network*, available at: http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html, visited on 10 October 2010

Reuters (2010): *China's Internet population hits 384 million*, available at: http://www.reuters.com/article/idUSTOE60E06S20100115, visited on 4 October 2010

Wikipedia: *China Next Generation Internet*, http://en.wikipedia.org/wiki/China_Next_Generation_Internet, visited on 4 October 2010

Tezel, O. (2009): *State of IPv6 in China*, available at: http://www.ipv6.org.au/09ipv6summit/talks/OrcunTezel.pdf, visited on 3 October 2010

Digaria (2009): *China Telecom Officially Announces Commercial IPv6*, available at: http://digaria.com/postings/b6f3742ce62ac02a8a63d0dd0c7b55da, visited on: 17 October 2010

Lawton, T. (2012). "15 Years of Chinese Internet Usage in 13 Pretty Graphs". *East West Connect*. CNNIC, available at: http://www.east-west-connect.com/chinese-internet-user-demographics-jan-2012, visited on: 17 March 2012

Korea

There are also many activities taking place on the Korean Peninsula. The KOREAv6 Project was composed of trial functioning of IPv6 services and testing of IPv6 equipment at the user level. Its implementation started in 2004. The goals of the project were:

- to create "IPv6 Ready" operations in companies in the public and private sector,
- to facilitate the commercialisation of IPv6 equipment,
- to encourage the raising of public awareness about IPv6.

The implementation of the project was divided into several phases:

Phase I started in 2004 and included the construction of the IPv6 network across the entire country to provide services such as VoDv6, VoIPv6, internet transition services and testing various IPv6 equipment such as routers, switches and VPN equipment;

Phase II continued the following year and included the use of IPv6 technology for some of the most important services defined in IT839, which is the IT strategy of the Korean government. The services are WiBro (Wireless Broadband) access, VoIP services, the expansion of local networks into the public sector and simultaneously the transition of the existing IPv4 web portals and applications into IPv6 portals;

Phase III was the last phase of the project that ended in 2006. It included the establishment of extensive networks for providing IPv6 services such as VoIPv6 to all users and support for IPv6 content on WiBro networks. Their desire is to encourage mass use of IPv6 internet services in the public sector.

The Korean government intends to achieve a perfect transition to IPv6 in the public sector and obtain 10 million IPv6 users by 2011. The next milestones in the action plan of the Korean government were the following:

- complete transition in backbone networks by 2010,
- a transition of ISP access networks by 2013.

The Korean action plan is being carried out successfully, but they will not succeed in achieving all the goals within the set deadlines. According to the latest announcements, the transition of backbone networks will be fully completed by the end of 2010.

Sources:
IPv6 Forum Korea, available at: http://www.ipv6.or.kr/eng/index.html, visited on 15 October 2010

IPv6.com Inc., available at: http://www.ipv6.com/articles/deployment/IPv6-Deployment-Status.htm, visited on 15 March 2012

3. Analysis of the Economic Aspect (separate for the public and private sector)

The transition to IPv6 is inevitable. However, we live still in a financially 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 the business world. It shines light on the commercial aspects of the various players. This includes not only large businesses and governments but also residential end-users.
It is hard to present a good study about the economic impact, but this section tries it's best to reflect expert-opinions. The key challenge is to clearly articulate the economic incentives for each individual company, which has to spend money on something that might appear to be only beneficial for the whole community, but not economically viable.

Implementation of any kind of novelty into an information or communication system must be economically or technologically justified. In other words, this means that the desired changes should result in lower costs of management and development of the system or its more effective, reliable and safe operation. The key issue that we have been facing for almost ten years when implementing the IPv6 protocol into the environments of the internet service providers, content providers and enterprises is the relatively limited direct economic and technological advantages that its use brings. In order to better understand the above mentioned impact on individual groups of users, we should first present in detail the strengths, weaknesses, opportunities and threats (SWOT) which the implementation of the IPv6 protocol can have while trying to shed light on the economic as well as technological aspects.

Strengths:

- the significantly larger address space of the IPv6 protocol enables unlimited growth and development of the number of internet users, which is of key importance for continued economic growth of internet providers,
- constant header length improves the effectiveness of routing, and the hierarchical arrangement of the address space decreases the size of routing tables, which in some cases results in longer periods of functioning of the equipment,
- the possibility of providing direct connectivity between optional nodes, improved support for security, ensuring quality of services and mobility of

nodes can assist in the more effective functioning of multimedia and security applications.

Opportunities:

- the possibility of developing completely new and improved applications and services (for example, those that are not client/server based),
- the possibility of lowering costs of the development of applications and services, because by using the IPv6 protocol, it will be possible to surrender the execution of some of the functionalities to the network layer (for example, it will always be possible to execute measures for providing privacy, integrity and authenticity of data by using AH and ESP protocols, which have to be supported according to RFC-4294),
- the possibility of a more equitable allotment of address space can result in a decrease of information illiteracy and the digital divide (the desires of the International Telecommunication Union (ITU) to help undeveloped countries in acquiring IPv6 address space from regional registries (RiR) could also be seen in this light),
- the possibility of accelerated fusion of services due to the support of mobility (terminal),
- the possibility of using M2M networks (e.g., sensor networks ...).

Weaknesses:

- the IPv4 and IPv6 protocols are not directly compatible, which means that all hardware and software must be adapted to the new versions of the internet protocol,
- because the IPv4 protocol enabled the growth of the Internet from a research network into a global network and has proved to be quite adjustable, the scepticism regarding the sensibility of its replacement has been present in some circles within the internet community for quite some time.

Threats:

- incompatibility of individual IPv6 protocol implementations or their lacking support for individual functionalities could cause difficulties in the protocol's deployment,
- inexperienced and unsuitably educated staff could significantly prolong the deployment and increase its costs while at the same time increasing the risk in the light of security,
- unsuitably educated and motivated staff could represent a key obstacle in implementing the IPv6 protocol,
- the risk for "early-adaptors" to invest into something that potentially does not take-off. It might appear safer from an economical standpoint to wait until a critical mass of other operators have made the move,
- and most importantly the costs of deployment, which in some cases are hard to justify to the company management.

Besides the above, IPv6 deployment represents challenges in the area of technology (ICT), sociology and business. Apart from the above mentioned areas that are affected by IPv6 deployment, it also puts forward solutions to serious issues of the co-existence of both IP networks. In implementation, the access providers must find answers to the following questions:

- *Can we still wait?*
- *Why is the IPv4 address space depleted?*
- *Why consider implementing IPv6?*
- *How should the implementation be carried out?*
- *How should the transition from IPv4 to IPv6 be carried out?*
- *Are the predictions on what will happen all there at our disposal?*
- *Why do we not have a working plan?*
- *Are the technology and the standardisation already available and mature enough?*
- *Do we have enough internet knowledge and enough human resources available?*
- *Are there any IPv6 networks already in practice available nearby?*
- *How to proceed in order to make content visible from both networks?*

The common goal is to prepare the network to offer new services. When implementing new services, at least one service must be found that will facilitate faster acceptance of the new protocol. Besides this, the access providers must do everything necessary to satisfy the needs of state authorities such as the Information Commissioner, the Competition Protection Office, the Ministry of Justice, the Ministry of Internal Affairs, the Post and Electronic Communications Agency (APEK) regulator and others. The implementation of the protocol into mobile networks should be especially underlined. We should be aware of all the strengths and weaknesses created by the IPv6 protocol compared to the IPv4 protocol.

Internet Access Providers

For many years, internet access providers were the only subject who succeeded in taking advantage of connecting individual networks with the internet. Their business models were thus at first based on a simple share for the access to the internet, while for residential users using the telephone network to access the internet meant that the price depended directly on the duration of the access and for the business user who accessed the internet over FR or ATM networks, it depended on the desired speed of access and the quantity of the transmitted data. The convergence of access networks (the use of the telephone network was soon replaced by the use of broadband access, and the fixed internet users were joined by mobile users) and complete domination of the IP protocol for transmitting all kinds of data have in recent years significantly changed the business model of the majority of access providers, so that today, besides internet access, hosting and server co-locations also often provide voice telephony and TV (the data, voice and video content is often also referred to as 3play) and many among them also play the role of a mobile operator and system integrator. The organisational structure of access providers is divided into two main elements. The first part of the organisation is the internal IT area that organisation-wise is entirely comparable to other companies of the same size; the other area is the area of communication infrastructure intended for selling services to end users and companies. The share or value of the sales-oriented infrastructure represents a majority of the joint ICT infrastructure in the companies of internet access providers. The implementation of the IPv6 protocol for access providers represents a very big challenge and there is also a big risk related to successful implementation and financial indicators. Implementation into such a company requires a project approach towards executing tasks mainly due to the risk and exceptional impact on the existing infrastructure, which represents the majority if not the only source of income for the company. Access providers must not and cannot afford to accept a wrong decision or answer the following question incorrectly: When, in what way and most importantly how to implement and commercialise the altered access to the internet?

A Motivation for Implementing the IPv6 Protocol

Because the access providers play a key role in smooth functioning of the internet, one would expect that they would start implementing IPv6 into their networks relatively early. Even though worldwide, some access providers made the first steps towards this goal relatively early (the final versions of RFC-2373 and RFC-2460, which describe addressing and the structure of packets or option headers in IPv6 protocol, were for example published in 1998, and the first access providers started connecting to the 6bone network, which was intended for early transfer of IPv6 traffic, as early as 1997), many of them were troubled for many years by, at first glance, a very simple question - why implement the IPv6 protocol into their network and start actively marketing it as such when its use is not required by their clients and it does not bring any business benefits? The internet service providers do not sell the IP protocol, but the solution that connects the user and their local network with the public internet network. For access providers, the supplementations to technical solutions for connecting users into the Internet network are an investment of certain funds into planning, implementation, testing and verification. For these earmarked funds, it is almost impossible to calculate the economic factors such as turnover of capital and return on investment. One of the main factors of the implementation is to remain competitive or to increase the competitiveness of the offer.

It seemed for quite a while that finding the answer to the above question was very similar to solving the "the chicken or the egg" dilemma, because the users of technological advantages created by the use of the IPv6 protocol are not related to economic advantages. When even the biggest sceptics realised that the change of internet protocol is a fact that cannot be avoided in any way, the access providers started seeing the above issue in a new light. Today they believe that the most suitable answer to the question is a thorough preparation for the future increase of demand or an increase of competitive advantage of the access provider, who will start implementing the IPv6 protocol and will be able to provide direct connectivity to IPv6 internet on the market for business and residence users.

But for access providers, increasing the competitive advantage is not the only economic advantage that they will have the opportunity to make use of by implementing the IPv6 protocol. Because the packet header in IPv6 protocol has a permanent length and at the same time enables a much larger address space and a more hierarchical arrangement of the address space of the individual access provider, we can expect that, due to a more efficient routing into backbone networks and the abandonment of the use of the IPv4 protocol, hardware replacement will be rarer, which will result in lowering of investment costs.

The IPv6 Implementation Method and Costs

In order to enable quality management of tasks, the access providers should create, prepare and manage the project. The vision of the project should be the following: "Setting up a new internet network and internet services before the competitor providers do, because we do not want users to turn to the competition for content." The task or the project should contain content preparation for the following areas:

- reasons for occurrence,
- vision,
- content,
- objectives (dedicated/object)
- a tactic for performing the tasks,
- a plan of implementation with a timetable (project breakdown)
- economics,
- expected business effects,
- organisation,
- control of supervision,
- links with other processes (internal and external),
- risk analysis with SWOT analysis,
- assumptions and limitations,
- methodology of measuring the performance,
- environmental aspects,

- costs and capital turnover.

Taking into account the described set of services provided by access providers to their clients today, mainly in terms of technological complexity, the method of implementing IPv6 into the access provider's network seems relatively clear. Because the operation of practically all listed services depends on the capability of the transport and exchange of IPv6 traffic with other providers, we can therefore expect that during the first stage the access providers will provide the business users with direct IPv6 connectivity, after adjusting the user equipment (CPE), they will provide it to residential users and only then will they start expanding the support for IPv6 into data centres and thus provide hosting and server co-location. Because in most cases the IP telephony and TV are private networks that are completely separate from the internet, or the link between the networks of individual operators is under strict control and at the same time the level of support for the new generation of the internet protocol on the terminal equipment is, to tell the truth, still relatively limited, the implementation of the IPv6 protocol into limited segments can be expected to arrive relatively late.

Costs deserve much more attention than the implementation method, because in the event of an incorrectly implemented deployment strategy and inexperienced staff, they can exceed the estimated limits and seriously endanger the operations of the access providers. By taking into account the results of several foreign studies (e.g. http://www.rti.org/publications/abstract.cfm?pub=6578), we estimate that the majority of costs of implementing IPv6 into the access provider's network will in Slovenia also be related to training technical staff and testing, followed by the costs of adjusting or upgrading tools for the control and management of the network and the costs of replacing hardware and software (their upgrade can be included into the costs of regular network maintenance and development if this is suitably planned). Taking into account the practice of the majority of manufacturers of hardware and software, we can determine that the use of the IPv6 protocol will not be licensed separately, so the above-mentioned costs will not contribute to the costs of the implementation. In other words, we might conclude that the operational expenditures (OPEX) will have a much larger role than capital expenditures (CAPEX) in the implementation of IPv6.

Can the implementation of IPv6 at the level of access providers result in an increase of prices of their services?
This should not be the case, because if we compare the service of an internet access provider and the service of a car repair shop, the mechanic does not increase the price per hour if he/she must purchase new tools for new vehicles. Similarly, the role of the internet access provider is to ensure to their users and clients a permanent access to the internet via their protocols and to introduce and update the quality of their services. Naturally, the operators and internet access

providers will make investments and contributions into the upgrade of the network, but such investments should already be planned and must not be an obstacle for the implementation, because every good and quality operator or internet access provider must constantly upgrade, maintain and improve their network if they want to keep up in the race with the competition or maybe even gain a competitive advantage on the market.

Implementation of the IPv6 protocol at the level of access providers also opens up an interesting issue of sharing the costs of the implementation with the content providers. If in the future, the content provider will want to lower the costs of network maintenance by completely abandoning the IPv4 protocol, they will have to carry this out in agreement with the access providers, because otherwise it could lead to a situation where users will not be able to access the desired content, because their access provider will not provide direct IPv6 connectivity to the internet.

Content and Applications Providers

The business models of content and applications providers are usually designed so that their income directly depends on the number of users. The fact that the implementation of the IPv6 protocol is just as important to them as for access providers could be easily demonstrated by taking for example a user who wants to access one of the social networks. Because the user comes from one of the developing countries where the selected access provider could not obtain a public IPv4 address for them and because due to the costs of the equipment and implementation, they do not use technologies in their network such as CGN/LSN, only an IPv6 address was allocated to the above mentioned user. However, because the two versions of the internet protocol are incompatible, and the online server through which the users access the social network is not adapted for use with the IPv6 protocol, the user is not able to use the desired application. The problem facing the content or applications provider in such an event is the narrowed target audience and consequently the income, so the decisions made by Google and Facebook are economically completely justified from this perspective.

Business Users

In business environments, the Internet today plays a key role in carrying out a series of processes - from internal communication via e-mail and systems for instant messaging and internet telephony to the transfer of data between applications for managing companies and production planning (ERP). Although quite a lot of effort has already been put into finding the economic advantage of implementing the IPv6 protocol into business networks in recent years, the results always seemed less than adequate. Even though in such environments we only rarely had to face the shortage of the available public address space and many organisations freely managed to function with only a few public addresses, the issues often occurred during the first attempts of mutual connection of two or several such environments (due to the separate management of address space, the problem of overlapping address spaces is rather common in practice). The simplification of mutual connection of business users can help improve the information support for business processes.

The possibility of direct connectivity between nodes in using the IPv6 protocol can help better integrate the telephony and systems for instant messaging and increase the frequency of their use between individual business entities. If today, we haven't trouble imagining the exchange of electronic messages between organisations without any limitations and that the costs of telephony in an individual company can be significantly decreased by using internet telephony, in practice there are still difficulties when we try similarly to establish a call between a business user in one company and a supplier or a buyer in another company.

An additional economic reason for implementing the IPv6 protocol into business networks can also be the simpler insurance of security and lowering of costs for the use of dedicated solutions, since by implementing the use of IPv6, all nodes will have to be capable of concluding IPSec sessions for which firewalls or dedicated VPN concentrators are currently in use.

Similarly to access providers, we can expect that in business environments, the highest cost in implementing the IPv6 protocol will be related to educating the administrators of individual systems, which is especially true for environments where the majority of tasks in relation to maintenance is performed by own network and system administrators or where these tasks are not entrusted to outsourcers. If there are dedicated applications that were developed for a limited number of users used in such environments and as such are not developed or maintained any more, we can expect additional costs in the implementation of the IPv6 protocol, because the termination of the use of the IPv4 protocol will have to be delayed due of that. The use of two different versions of the internet protocol usually means an increase of maintenance costs due to more complex configurations of active network components and server infrastructure.

Residential Users

The residential users represent an important source of income for practically all access providers, so the method of IPv6 protocol implementation at the level of access providers and residential users will be closely linked. Considering that according to some data, there is a local home network behind one public IP address in almost a half of the accesses, the replacement of the internet protocol version will urgently require the replacement of the devices, because due to the strict control of costs, components that would enable software upgrades are not installed. The question that arises is: who will cover the costs of the replacement?

First, let us try to shed some light on the case where the access provider provided a broadband modem to the residential user. Because this is a device that from the viewpoint of the user carries out only the functionalities of the connectivity layer (L2), the costs of replacing the equipment will be in large part borne by the user themselves, because they will have to replace the broadband router that performs the task of the network layer (L3). From the viewpoint of residential users, the more effective use of P2P applications seems the most appropriate reason for this. Things get complicated at the level of residential users in all cases where the access providers, while fighting to increase their market shares and to subscribe the users, decide to provide the possibility of using the functionalities of the network layer on devices that are their property. The costs of replacing the equipment shows itself in quite a different light in the case of using internet telephony and TV, where the operator usually provides several devices to the user or has integrated their functionalities into a single device.

When the residential user wants to use the IPv6 protocol that was provided to them by their ISP, they will have to bear the costs of replacing hardware and software that does not support IPv6. The equipment that will probably be subject to the replacements includes personal computers, telephones, televisions, refrigerators, toasters, etc., namely all the equipment that can communicate over the IP protocol.

Hardware and Software Providers

Even though hardware and software providers have been facing a similar dilemma as access and content providers for quite some time in implementing the IPv6 protocol, the developers of operating systems decided relatively early to include support for the IPv6 protocol into the operating systems (for example, at Microsoft, the support for IPv6 protocol for Windows XP was included into service pack SP1, which was published in September 2002). Despite the fact that development and testing of the new protocol created more than a few costs that could not be included into the price of the final product, the support for the use of the IPv6 protocol at the level of operating systems should be seen as an encouragement for developing new applications that could fully benefit from the advantages of the IPv6 protocol.

Similarly to the operating systems, the IPv6 protocol in applications did not have any significant impact on the market development, because individual manufacturers started including the support without payments for additional licences relatively early. If we take for example the two most commonly used web servers, open source Apache and Microsoft's IIS, then we can see that the former had its support for IPv6 protocol added in version 2.0 in April 2002 and the latter in version 6.0 in April 2003. The market shares of both applications did not change significantly due to the relatively low demand for this functionality. However, the development of new applications that could be used exclusively in relation to the IPv6 protocol progressed very slowly.

Thus from the viewpoint of operating systems and system software, the support for the use of the IPv6 protocol did not mean an increase in market share or competitive advantage. The situation is a little different with the more innovative applications that are changing the presently established models of use and are effectively utilising the advantages of the IPv6 protocol. The way this works in practice is clearly evident in terms of Microsoft's solution for remote Direct Access, which eliminates the separation between the business environment and the Internet. To the clients, it enables direct and permanent access to custom sources on the Internet while significantly simplifying their management and care for constant compliance with the required regulations and recommendations.

Thus at the level of software manufacturers, we determined that implementation of the IPv6 protocol will create an increase in competitive advantage only in the event of innovative applications. A similar situation applies to manufacturers of hardware. We believe that the segment in which the innovation will be especially prominent will be the segment of user equipment (CPE), where due to the method of apportionment of costs among access providers and residential users and the volume of production, the development and production costs are very important. Considering past experiences, we estimate that in this case an important role will also be played by open-source software.

System Integrators

For system integrators, the implementation of the IPv6 protocol primarily means a large business opportunity, because due to the rather limited experience with its use in practice, the demand for training and consultation services will increase in the next years. This means that for system integrators, mastering the new version of the internet protocol early will be of key importance, because this will be the only way to increase competitive advantage in preparing and carrying out training courses and preparing strategies of implementing the IPv6 protocol into environments of access and content providers and of business users.

Investments in obtaining knowledge and experience from the field of IPv6 can from the viewpoint of the expected future demand thus be seen as strategic investments. In order to succeed in lowering their costs, there is a series of alternative education methods already available - from carrying out internal trainings to remote education and cooperation at thematic workshops and conferences. With these, it is possible to avoid a lengthier absence of the technical staff in the event of participation at training courses. Similarly, the costs of testing and verification of individual solutions can be lowered by using tools for simulation and virtualisation.

Public Sector

(the public sector as a catalyst on the market of IPv6 equipment and services)
The fact that the motivation for deploying IPv6 cannot be exclusively economic became clear years ago when the opinion that the public sector could play a decisive role in successful deployment of the IPv6 protocol became prevalent in the internet community. The governments, ministries and other consumers of the budget from the public sector primarily used two mechanisms to facilitate its deployment.

On the one hand, the governments of some countries decided that organisations from the public sector will demand the implementation of IPv6 at the administrative level and this way increase the demand for equipment that enables its use and services related to its implementation. Probably the most known example of such a decision was the requirement of the US Office of Management and Budget (OMB) of August 2005 (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf), which required all federal agencies to implement the IPv6 protocol into backbone networks by June 2008, while no special funds for the implementation of the activities were envisaged. Similarly, China also preliminarily intervened on the market of information technology with a decision on carrying out the five year CNGI Project (China - China Next Generation Internet), the highest point of which was probably the 2008 Summer Olympics in Beijing where the IPv6 protocol was used at practically every step. The decisions by both governments undoubtedly demonstrate that they treated the deployment of the IPv6 protocol as a strategic decision for maintaining technological progressiveness.

On the other hand, some governments decided to encourage the demand for the IPv6 protocol and its use by including requirements for its support in public tenders. Although the Slovenian government has yet to adopt a similar decision, some of the more technologically advanced users are already deciding to prepare tenders in a way that primarily the hardware must enable use of the basic functionalities of the IPv6 protocol.

4. Proposals for Strengthening Slovenia's Activities on the International Scene

"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 direction 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 quickly.

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

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 difficult at all. So making a difference now is going to be less painful than the recovery process from falling behind.

This section gives an overview over current ongoing activities in Slovenia. This may also serve as some inspiration for others.

Over the last decade, Slovenia has lost its recognisability in the field of ICT. More than a decade ago, it actively cooperated in the European area, but lately larger and more important activities are hard to find. The deployment and use of the IPv6 internet protocol is a good opportunity to once again acquire a reputation and earn a larger role in the area of ICT in the European area. It is not hard to come to the conclusion that all new services of the internet of the future will use the IPv6 protocol to function. Services of the internet of the future that will only use the IPv4 protocol to function will in general be a case of bad practice, but we can still learn something from this. Let us examine the internet of the future in more detail and acquaint ourselves with the forthcoming services that will change our life. For the inhabitants of the European community, the internet of the future represents a higher quality of life, since it will provide a more effective and smart energy supply and the informatisation of the transport infrastructure that will enable less traffic jams and inform about unpredictable events and various forms of remote heath care, SOS calls and the most modern health care in the local environment.

The internet of the future will connect various devices that are used in our everyday lives, such as cars or mobile devices, with network infrastructures (e.g. with systems for managing traffic, security centres) while enabling the use of large amounts of data in real time for improving the environmental processes and new synergies among interdisciplinary economic organisations and companies.

The link between the Ministry of Higher Education, Science and Technology with public and private institutions and production and service companies in the area of implementing the IPv6 protocol would represent a strategic advantage for the Slovenian industry against foreign competition. Naturally, in the next years, the advantage will be nullified, so action has to be taken now.

The Public Agency of the Republic of Slovenia for Entrepreneurship and Foreign Investments (hereinafter referred to as JAPTI) is a key development and implementation agency for carrying out the development policy in the area of the development of entrepreneurship and competitiveness in Slovenia and for carrying out programmes for facilitating foreign direct investments and internationalisation. By cooperating with the JAPTI agency, the government can acquire the interest of foreign investors for investing into service solutions and technological devices that use the IPv6 protocol to function.

The European Commission has already published a Trans-European innovation strategy with which the European Union wants to become the leading force in the field of the Internet. With incentives in the field of the development of the Internet of the future, Europe wants to become a global superpower. The Commission wants to establish a partnership between public authorities and corporate entities in the field of ICT. For this purpose, 300 million Euros will be earmarked in the 2011-2013 period that will be available for projects, and there are already 200 million Euros available for the development of the fundamental internet technology.

On the international IPv6 scene (and in general, the internet scene), Slovenia has recently attracted attention through its activities and success with IPv6 when the RIPe-NCC laboratory published the results of the "RIPEness" analyses, which represents the readiness of a country for IPv6 according to its standards.

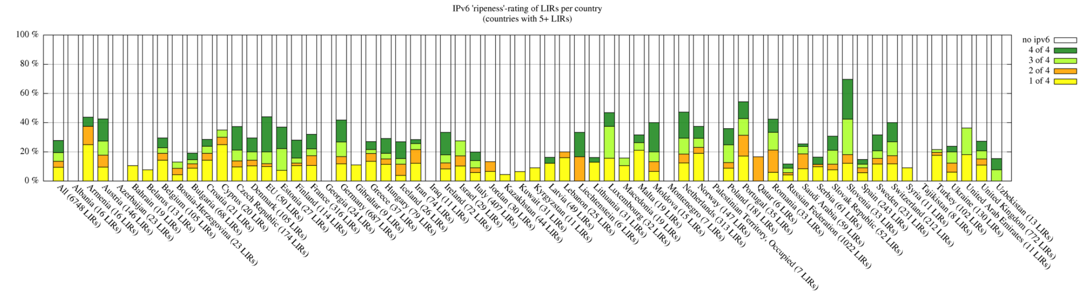


Figure 1: *"Slovenia shows the best results: 67% of LIRs in Slovenia have at least one star, while 25% have four stars! In absolute numbers, that means 8 out of their 34 LIRs have achieved four star IPv6 ripeness."*

Because this publication did not go unnoticed, go6 Institute, the Slovenian IPv6 initiative, was invited to the RIPE60 meeting in Prague to present its go6 platform and other IPv6 activities in Slovenia. The initiative was represented by Jan Žorž. This lecture lead to a great number of invitations from around the world and the go6 Institute participated with the presentation of the Slovenian IPv6 activities at the Google IPv6 Implementers Conference in Mountain View, California, at the Greek IPv6 TF in Athens and at the German IPv6 Council Meeting. They were also invited by the NRO as guests to the workshop titled "IPv6 Around the World" at the IGF event in Vilnius.

These activities of the initiative help promote Slovenia on the international scene and open up more possibilities for cooperation in various spheres, organisations and projects around the world.

An overview of current activities:

RIPE-NCC

We are cooperating with the RIPE-NCC via the presence of the go6 at all meetings, lectures and other activities of RIPE. Jan Žorž and Steffan Sander have sent a document proposal titled "Requirements for IPv6 and ICT Equipment" to the RIPE IPv6 working group, which intended scope was specifying requirements for IPv6 in ICT equipment for the purposes of formulations in public tenders. Document reached strong consensus and is now published as official Best Current Practice for RIPE region under name RIPE-501.

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

Merike Käo, Sander Steffan and Jan Žorž are currently working on RIPE-501 replacement document, aiming for acceptance as official RIPE BCP at RIPE64 meeting in Ljubljana (April 2012)

Progress and versions of new document can be followed at: http://go6.si/ripe501bis/

NRO

The NRO (Number Resource Organisation, http://www.nro.net/) has expressed a desire to further demonstrate Slovenian success in IPv6 as an example for other countries of how the implementation of the initial steps of IPv6 deployment should be handled.

IETF

IETF (the Internet Engineering Task Force) is the organisation for the standardisation of internet protocols and services. IETF Slovenia is already cooperating through the go6 Institute, which is the co-author of at least one RFC proposal.

IGF

Slovenia is actively present at meetings and forums of the IGF (Ministry of Higher Education, Science and Technology); at the most recent meeting, it was present with a lecture at one of the workshops (go6).

HGI

Telekom Slovenije, with its representative Simeon Lisec, is managing a task force for preparing technical requirements and specifications for user or home equipment as part of the HGI (Home Gateway Initiative). The HGI is an association of leading global networks and service providers and global manufacturers of home hardware and software ICT equipment. Telekom Slovenije is also currently a gold member at the go6 Institute and it thus also actively supports the work of the go6 Institute.
http://www.homegatewayinitiative.org/about/TF/IPV6/Index_IPV6.asp

BBF

The Broadband Forum is a forum for the specification of requirements for network and internet service providers. Quite a few Slovenian companies are members of the forum, but the most important and largest role it occupied by Iskratel d.o.o., who is also a member of the go6 Institute.

IPv6 Forum

Latif Ladid, the head of the European IPv6 Forum, which also has a Slovenian section operating under its auspices, is very much in favour of the Slovenian initiative and activities. It sees the initiative as an exceptional example of an enthusiastic and successful approach to implementing IPv6. The IPv6 Forum invited the go6 Institute to the expert group of the EC project for coordination of the IPv6 deployment between the EU and China.

IPv6 TF

The Slovenian IPv6 Task Force that operates under the go6 Expert Council was declared as the Slovenian section of the EU IPv6 TF, an organisation established under the auspices of the EC.

6DEPLOY

6DEPLOY is a project of the European Community, the purpose of which is to spread knowledge and educational programmes created during the 6DISS Project. By supporting local experts, several appointments can be achieved.

ISA

(Interoperability Solutions for European Public Administrations)
An ISA tender that will standardise the equipment, networks and ICT software of the EU member states on a single platform is especially relevant. The German Ministry of the Interior has signed up for creating an IPv6 profile and invited Slovenia to participate by making our document with requirements for IPv6 in ICT equipment as a basis for the EU IPv6 profile.

Proposals for Future Activities:

There are three standardisation bodies operating in the region of the European Union, ETSI, CEN and CENELEC. The ETSI (The European Telecommunications Standards Institute) standardisation body is a non-profit organisation that is in charge of telecommunication standards in Europe. The European umbrella standardisation body is CEN (Comite Europeen de Normalisation). CEN is a non-profit organisation established according to Belgian legislation. It is in charge of the joint platform for developing European standards and other documents adopted with the consent by member states. The third standardisation body is CENELEC (The European Committee for Electrotechnical Standardisation). CENELEC covers the area of electrotechnical standardisation, which also includes the services of the internet of the future. The most important services are intelligent energy and sensor networks. Both services are a part of a greater whole that recently became known as M2M (Machine to Machine). M2M covers an entire spectrum of devices that appear and will appear in mobile, wireless and fixed networks. The users of M2M networks are not people, but devices of which there are certainly at least a hundred times more than people on the planet if we consider devices that communicate with other devices under basic specifications. There is a very close connection between the IPv6 protocol and M2M networks. The IPv6 protocol is a common choice for all M2M architectures, because it supports the adequate number of public IP addresses required by the devices for communication. At the same time, we know that IPv4 public addresses are practically no longer available. Because a status of member is required to communicate with the above mentioned bodies, the ideal partner for that in Slovenia is the Slovenian Institute for Standardisation (SIST). SIST is a member of all European standardisation bodies and also has routine communication channels with these institutions. Good communication channels are urgent for carrying out certain tasks, especially when acquiring contacts and the right addresses for successful implementation.

ITU

The International Telecommunication Union (ITU) is an international organisation that prepares and confirms standards in telecommunications. It was established on 17 May 1865 in Paris as "The International Telegraph Union". Its headquarters are located in Geneva.

The organisation is divided into three sectors:

- ITU-T, the Telecommunications Sector
- ITU-R, the Radiocommunications Sector
- ITU-D, the Development Sector

IPv6 belongs under the ITU-T sector.

The ITU-T is an organisation for the development of standards (SDO) and is one of the three sectors of the International Telecommunication Union (a special agency of the United Nations). The ITU-T has a director's "Ad Hoc" group in the Telecommunication Standardisation Bureau. The bureau provided the following definition in March 2005, which was adopted in November 2005 by the ITU-T:

> The ITU-T has a long history of open standards development. However, recently some various external sources have attempted to define the term "Open Standard" in a variety of different ways. In order to avoid confusion, the ITU-T uses for its purposes the term "Open Standards" as per the following definition:
> "Open Standards" are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. "Open Standards" facilitate interoperability and data exchange among various products or services and are intended for widespread adoption.
> Other elements of "Open Standards" include, but are not limited to:
>
> - collaborative process - voluntary and market driven development (or approval) following a transparent consensus driven process that is reasonably open to all interested parties,
> - reasonably balanced - ensures that the process is not dominated by any one interest group,

- due process - includes consideration of and response to comments by interested parties,
- Intellectual property rights (IPRs) - IPRs essential to implement the standard to be licensed to all applicants on a worldwide, non discriminatory basis, either (1) for free and under other reasonable terms and conditions or (2) under reasonable terms and conditions (which may include monetary compensation). Negotiations are left to the parties concerned and are performed outside the SDO,
- quality and level of detail – sufficient to permit the development of a variety of competing implementations of interoperable products or services. Standardised interfaces are not hidden or controlled other than by the SDO promulgating the standard,
- publicly available – easily available for implementation and use at a reasonable price. Publication of the text of a standard by others is permitted only with the prior approval of the SDO,
- on-going support – maintained and supported over a long period of time.

The Open Standard is not limited to these elements.

The ITU-T, ITU-R, ISO and IEC have mutually adopted a joint patent policy [3] under the guidance of the WSC. The definition of the ITU-T Open Standard does not necessarily apply to ITU-R, ISO and IEC, because the general joint patent policy [4] does not mention "open standard" but just a "standard".

Some ITU members have voiced their concern that the IPv6 address space will be allocated to the more developed countries before it will be available to less developed countries as in the case of IPv4. Thus, they proposed that to protect the interests of underdeveloped and less developed countries, the IANA should allocate a part of the IPv6 address space to ITU. This would then be allocated at national levels, which would change the existing system of the 5 RIRs, which are currently functioning based on the geographical allocation of covering the needs for IP address space of the local internet registries (LIRs). Slovenia should express its view to the international standardisation bodies on such proposals through its representatives.
We propose the establishment of a task force that will deal with forming positions related to ITU activities in the field of the internet network.

EU Framework Programmes

The 7th Framework Programme of the European Union and the preparation of the 8th Framework Programme are also an opportunity for Slovenia as a country. Cooperation in projects in the framework of European programmes can also be supported by the government with additional incentives. It would also be very beneficial for the country's reputation to manage at least one project as part of the 8th Framework Programme. In the context of the IPv6 protocol, it is also naturally desired that such a project also uses the IPv6 protocol for its implementation. The web portal IDEAL-IST could be of great help in the coordination and logistics of the project. Additional information about the portal can be found at http://www.ideal-ist.net/.

Below is a short list of current projects that also include work in the field of the protocol as part of the 7th Framework Programme (FP7) of the European Union of 26 October 2010. There are eight projects:

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/

Proposals for strengthening Slovenia's activities on the international scene:

- inviting LIRs to cooperate and participate in RIPE task forces,
- cooperation in standardisation and preparation of RFC at IETF,
- coordinating and encouraging cooperation in FP7 and FP8 projects and thus obtaining resources from European funds for implementing, training, service development, testing and verification of IPv6 solutions,
- lobbying in the European region for acquiring resources for establishing and operating a competence IPv6 centre,
- IPv6 integration as a priority area within the guidelines of development and investments into ICT in Slovenia and Europe,

- cooperation with the JAPTI public agency in acquiring foreign investments into technologically advanced IPv6 projects,
- a more active cooperation of the Slovenian Institute of Standardisation (SIST) with the European standardisation bodies, ETSI, CEN and CENELEC, when adopting standards for the support of the services of the Internet of the future whose functioning will be based on the IPv6 protocol.

Literature and Sources:

- 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 Standardisation – CENELEC, http://www.cenelec.eu/Cenelec/Homepage.htm
- The European Committee for Standardisation (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. How to Ensure the Convergence of Individual and Partial Slovenian Integration in International Formal Activities at the National Level

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.

Like the majority of the countries of the world, Slovenia is a member of various international associations, committees, commissions and working bodies. Since it became independent, it has been actively participating in the management of the modern international community in various fields. The international activities are performed at the academic level in the form of development and research, education projects, other methods of cooperation and at the political level where the decisions for the future development of the community are formulated and adopted.

In the group of the 27 EU countries, Slovenia falls among those with average technological development of electronic communications. In the 15th report of the European Commission for 2009, Slovenia ranked just below the European average of the frequency of internet connections (COM(2010) 253 final/3). The majority of broadband connections are based on xDSL technology. However, it is significantly more successful in building optical fibre networks. The optical fibre networks in Europe represent 1.8 to 5% of all connections, but Slovenia is one of the top eight countries in the world with the largest penetration of optical fibre access to the user (FTTH Council 2010). Only South Korea, Japan, Hong Kong, Taiwan, Lithuania, Sweden and Norway are more successful. Unfortunately, the latest analyses show that the majority of constructions of optical fibre networks in Slovenia have been stopped due to the economic crisis (at least for now). The T-2 company, which according to APEK has a 60.3% market share of FTTH, is almost bankrupt because the investment is not covered with capital, and Telekom Slovenia is upgrading the optical fibre networks slowly. If the government does not take the initiative in the construction of optical fibre networks with the help of European structural funds, it will be difficult to achieve the goal of the Europe 2020 strategy (COM(2010) 2020 final (2010)).

The strategy provides that all Europeans should have broadband access to the Internet by 2013 and a speed higher than 30Mbit/s by 2020. But the investors' investments on the Slovenian telecommunication market are not the only thing that is important. What is also important is Slovenia's knowledge and experience that could be marketed better on the European market and beyond. This means that a partnership between the ICT industry and the government should be established and that we should cooperate in marketing and in the implementation of solutions abroad. The areas where we were or could have been successful should be recognised. Knowledge and experience that can be acquired during the joint project of the implementation of IPv6 in Slovenia could be marketed abroad, first in the countries of the former Yugoslavia, who at least for now are still behind Slovenia. These projects could include the training of experts, establishing pilot projects and production systems on public and private networks, the sale of ICT equipment and others. State representatives in international organisations could be very helpful in achieving this with their activity and the Chamber of Commerce and Industry of Slovenia (GZS) with its liaisons.

The problem that many countries are facing is how to provide, from a number of activities in which the government and its representatives are participating, a suitable convergence of information that will be available to all interested and authorised stakeholders. The problem is also how, in the race for survival and time, to overcome our own selfishness and private interests and to share the obtained information, experience and knowledge with others.

In 1999, the IPv6 Forum was established as a non-profit organisation based on the initiative of the IETF as the umbrella organisation that develops internet standards. Shortly after its establishment, regional and national IPv6 Task Forces and Councils and other non-profit organisations were established. A common denominator for all task forces and councils is that they combine various stakeholders: representatives of the industry, operators and internet providers, government institutions and representatives of the academic and education sphere. The majority has set out to jointly, and despite strong own interests, establish a firm initiative that will provide the necessary transition of all stakeholders to IPv6. Such cooperation can also produce greater synergistic effects than when the activities are managed by individual companies. It should be stated that important and influential individuals participated or are still participating in all the above mentioned groups in one way or another. As was stated in the German action plan, to achieve the IPv6 objective in Germany by the end of 2010, a general consensus and readiness for action is required by everybody involved at all levels of the society, including influential politicians who should recognise the opportunity of the new technology and promote it properly (IPv6 German Council, 2009).

Slovenia can also be proud of establishing a team of experts from various spheres of society that is striving with the best of their efforts to achieve the required impetus in deploying IPv6. The team that is formally registered as part of the go6 Institute is extremely successful and is highly esteemed in the international community. Because of the diversity of the participants and their expertise and innovation, many foreign observers have given them a status of an example of a good practice that should be copied.

In the last ten years, a series of conferences, symposiums and workshops were organised that promoted IPv6 deployment. A short overview of the activities shows that EU member states are competing with each other in presenting the most successful situation of their country, which demonstrates how important it is to participate at such events. Naturally, the right selection of the event and the people participating is also important. With active and successful engagement, both the lecturer and the country he/she is representing gain recognition. Successful pilot projects, together with successful promotion at international conferences, raise the country's credibility and simultaneously enable cooperation with other countries in establishing pilot projects or production systems. On 6 October 2010, the European Commission presented the Innovation Union initiative as part of the "Europe 2020" strategy with which it wants to facilitate the innovations in the European Union. The press release (IP/10/1288) lists ten key elements with which the Commission wants to facilitate the European partnerships for innovation, alleviate access to financing, reconcile the European and national policies in the field of research and expedite the investments into research in the public sector in the field of innovative products and services. In the press release, the Commission proposes the countries to reserve earmarked funds for public tenders relating to innovative products and services. For this purpose, funds in the amount of 86 billion Euros have been earmarked in structural funds for development and innovation from 2007 to 2013. These funds can be used to mobilise interested parties, the European and national bodies and the public and private sector.

By acquiring European development resources, various projects could be financed that could be used in the long-term to increase the growth and development of the Slovenian economy, create jobs and as a result ensure competitive advantage over other countries. A good example of using funds is for example obtaining the funds of the European Regional Development Fund, which are used to finance the construction of open broadband networks. The successfulness of drawing funds depends on active policy in the European region and on good communication among ministries and interested companies. Even the procedures of acquiring and drawing funds should be simplified and transparent.

The European Commission has financed several projects and pilot projects that were indirectly or directly related to the development and deployment of IPv6. The majority of these projects were financed with Framework Programs for research and technological development. According to data available to us, Slovenia has not taken advantage of the available funds enough. The reasons for this might be due to the fact that we are not recognisable enough and that our companies, due to their smallness, cannot or do not know how to compete with foreign companies and countries.

The future strategy of Slovenia should be based on a closer connection between the public and private sector. A good example of such cooperation is the establishment of the Strategic Council for the Information Society and also the activity to date of the go6 Institute. An exchange of experience and knowledge is needed and effort has to be made for a greater recognisability in the European region. Cooperation between state institutions should also be increased by forming expert interdepartmental groups that should exchange information and experience, prepare strategic plans and check the set goals several times a year. One of the priority goals should also be the renovation of the existing Broadband Networks Development Strategy (the Government of the Republic of Slovenia, 2008) and the preparation of a Strategy for Future Development of the Information Society in the next four years. Both documents should contain a commitment to include the IPv6 protocol into networks and services in accordance with the Communication from the commission to the European Communities, A Digital Agenda for Europe (the European Commission (COM(2010) 245 final/2) (2010)).

If Slovenia wants to act concertedly in the wider environment, it urgently requires a connecting and advisory body. The Connecting Advisory Body (hereinafter referred to as CAB), which could be managed by a competent ministry, should mutually connect Slovenian industry, service organisations, the academic field and RR organisations in the context of a clear vision of the future of the welfare of the Slovenian economy. The IPv6 internet protocol is an ideal opportunity that can be taken as a competitive advantage in the industry related to the manufacture of devices that use IP to communicate with the surroundings. The same competitive advantage also applies to all service activities. The CAB could achieve the best results in internet services such as e-stores, e-libraries, e-knowledge, e-energy, etc. The purpose of the CAB is by all means primarily the collection of information in one place and the forwarding of such information to the interested enquirers. The CAB should communicate with all other public organisations that operate not only in Slovenia but primarily in Europe. The CAB would also function as an advisory body for the entire state and public administration. For the public administration, the CAB would provide assistance in challenges that will appear during the deployment of the new IPv6 internet protocol. The CAB should also cooperate with a task force that could be established as part of the competent ministry of public administration. The establishment of such a task force for the preparation of the strategy for implementing IPv6 into the public administration network has been proposed in Chapter 11.

In the next decade, Europe is preparing, together with the European Commission, a strategy for the development of the internet (i2020) in the framework of the opportunities and competitiveness of the European economy with other global economic world powers. Europe wants to establish a technological balance with the US and does not want to be overtaken by Asian superpowers such as China and India in the technological advancement of the next decades. Europe is therefore financially supporting projects of the internet of the future as part of the existing 7th and 8th (2014-2020) Framework Development Programme of the European Union.

The clear message that the internet of the future should function on the internet protocol of the future is a special opportunity for CAB in Europe. Such a clear message has not been provided in Europe by any EU Member State.

We recommend that due to the range of the consensus, CAB should be linked with a credible organisation or initiative that already unites recognised experts from various environments in the field of IPv6. A close connection of experts and CAB could be another example of a good practice in Slovenia in the area of public and private partnership.

Sources:

IPv6 German Council (2009): Nationaler IPv6-Aktionsplan für Deutschland, available at: http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf, visited on 1 October 2010

Šabič, Z., Bučar, B, Roter, P., Kajnč, S. (2004): Slovenija v mednarodni skupnosti in Evropski uniji, available at: http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/seu1.pdf, visited on 19 October 2010

FTTH Council (2010): *Economies with the Highest Penetration of Fibre to the Home/Building + LAN,* available at: http://www.ftthcouncil.org/sites/default/files/2010%20Sept%20Global%20Ranking%20FTTH.pdf, visited on 19 October 2010

European Commission COM(2010) 253 final/3 (2010): Progress Report on the Single European Electronic Communications Market 2009 (15th Report) sec(2010)630, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/comm_en.pdf, visited on 29 October 2010

European Commission COM(2010) 2020 final(2010): Europe 2020 A Strategy for Smart, Sustainable and Inclusive Growth, available at: http://ec.europa.eu/eu2020/pdf/1_SL_ACT_part1_v1.pdf, visited on 29 October 2010

European Commission COM(2010) 253 final/3 (2010): "Innovation Union – Turning Ideas into Jobs, Green Growth and Social Progress", available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1288&format=PDF&aged=0&language=SL&guiLanguage=sl, visited on 29 October 2010

Government of the Republic of Slovenia (2008): Broadband Network Development Strategy in the Republic of Slovenia, available at: http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/DEK/Elektronske_komunikacije/Strategije/Strategija_BB_2008-07-10_SI.pdf

European Commission (COM(2010) 245 final./2) (2010): A Digital Agenda for Europe, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:SL:PDF, visited on: 8 November 2010

6. The Plan for Educating Own IT Staff on All Levels

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

Here at Loughborough University in the 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 is understood as natural.

Unfortunately, we are just one of a very small number of universities who teach IPv6 right from the beginning. But this is our future, it is an obligation for lectures 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. 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.

However, it should also be noted, that teaching IPv6 is not something "scary". In fact, a basic understanding is acquired very quickly. IPv6 should not be presented as the "elephant in the room" that nobody wants to see. IPv6 is in many aspects simpler than IPv4 and if we just allow students to play with it in lab-classes, we will see it is not difficult at all.

Globalisation in all areas of social and business activities, implementation of new technologies and modern communication options, changing the standard business models, opening new business opportunities, etc. are only a part of the factors that modern companies, operators, service providers, public and state administrations and other organisations in Slovenia and beyond are facing. The high process dynamic increases the need for sustainable investment into education and development of staff regardless of whether the staff is employed at a company, the public administration, an operator or other organisations. The successfulness and long-term development are directly dependent on the capacity to adapt to new conditions in the environment. Continued education of staff ensures a more successful and painless adaption to conditions and helps secure and utilise the potential of new network technologies such as the deployment of the new generation of internet protocol - IPv6.

IPv6 takes the best concepts of its predecessor (IPv4) and simultaneously introduces a number of technological innovations that open up new technical capabilities and thus business opportunities. In order to take advantage of the given potential in full, we will have to deviate from the traditional way of thinking in the technological area when designing, implementing and managing the internet systems of the new generation and also in the business area.

This chapter provides a proposal for managing the knowledge of staff in the field of IPv6 usage in business and public entities on all levels. It includes system planners, network and system administrators, developers and maintainers of portals and applications, customer services and also management.

An Overview of Education Requirements and Options

Business, development and other work processes are supported by various staff profiles (system planners, network and system administrators, developers and maintainers of web portals and applications, customer services, the management and decision-making segment, etc.). The ICT infrastructure planners and managers need special network and system knowledge and the application and service developers need special development knowledge about IPv6. In the management and decision-making segment, the technological advantages of new technologies such as IPv6 should be presented mainly from the economic and business perspective.

Various staff profiles require various approaches to education and especially the target content. Depending on prior knowledge and the field and type of work, various paths and education options must be provided to obtain the proper level of IPv6 knowledge. Education options are divided into 4 typical sets depending on the complexity, duration, level of formality and method of determining self-evaluation:

- intensive professional education and workshops,
- academic education,
- internal education in companies and organisations,
- e-education.

Intensive Professional Education and Workshops

The group of specialised professional workshops includes education carried out by industrial educational centres (NIL, ASTEC, AVTENTA, S&T, SRC, etc.) and some academic and research institutions (LTFE, Arnes, etc.). These education courses can be independent or a part of a longer educational programme that ends with tests at independent testing centres and a globally recognised certification. Example: the control of the IPv6 technology in the network and transport layer of the network is one of the prerequisites for obtaining globally recognised industrial certifications such as Cisco Certified Networking Professional (CCNP), Cisco Certified Internetworking Expert (CCIE), Juniper Networks Certified Internet Specialist (JNCIS-ER), Juniper Networks Certified Internet Expert (JNCIE-ER). Although there are other recognised certifications on the market, they are generally related to an individual hardware or software manufacturer, so in the future a lot of effort will have to be put forth to develop an independent certification of the IPv6 protocol.

Specialised professional education is intended for experienced engineers who already have an extensive general knowledge of networks systems and want to acquire new specific knowledge. There are also educational courses intended for those who are just entering the world of communication networks (for example: Cisco Certified Entry Networking Technician – CCNET, Juniper Networks Certified Internet Associate – JNCIA-ER). It is interesting that industrial professional education courses are often used as a backbone of academically oriented programmes (e.g. Cisco's network academy - see below).

Besides education that is intended primarily for users of a specific software or hardware (for example: education developed by equipment manufacturers such as Microsoft, Cisco or Juniper and which are provided by authorised and educational centres certified by the manufacturer), there are also a number of general professional IPv6 education courses on the market that are intended to provide general technological knowledge on the IPv6 protocol. Unlike education in the framework of global educational programmes (mainly in the framework of the educational architecture of individual manufacturers) where the developer of educational content provides at least a minimum global quality of education, the quality of independent courses depends primarily on the quality of the educational centre, their content developers and primarily the lecturers. In the event of selecting such an educational programme, it is wise to examine the references of the educational centre and test their quality by entering a smaller number of participants to one of their open courses.

The primary purpose of professional education is to obtain practical knowledge that is directly useful in the participants' work process. Therefore, in quality professional education a lot of time is devoted to practical work with the equipment (example: in the framework of education on the functioning of the network equipment by Cisco or Juniper, every participant has access to three or four routers or switches), which makes it possible for the participants of the course to immediately check their quality of acquired knowledge and also to rapidly gain practical experience which can then be successfully used in their everyday work. The advantage of education in an educational centre of a quality organisation which besides education also engages in other activities (consulting, construction of networks etc.) is undoubtedly the practical experience of lecturers who as part of informal interviews with the participants of the course solve many practical difficulties in the information infrastructure of the participants.

The key difference between the professional education and academic programmes (see below) is mainly the intensity of the education. Example: a subject that is discussed during the CCENT intensive course in one week takes an entire semester in an equivalent programme of Cisco network academy. Academic educational programmes are ideal for those who are only entering the world of information technology and who want to obtain a wide range of knowledge, and professional education is for those who have to acquire the knowledge needed for performing their work and tasks as soon and as effectively as possible.

The well known weakness of professional education should also be mentioned: the education itself usually does not contain a formal examination of the acquired knowledge, often due to the legal concerns of the organisations that develop such educational courses and they leave the formal examinations to specialised organisations (globally, one such organisation is for example the Pearson VUE, which has its test centres in 165 countries), because an examination passed in such an organisation is valid globally.

Due to the prevalence of knowledge about IP technology, the professional education about IPv6 is primarily intended for obtaining specific knowledge from the field of IPv6 such as: the structure of the address space, new routing protocols, new application requirements and similar.

Intensive professional workshops are appropriate for staff that have mastered the existing working process (network managers, system administrators, portal managers and maintenance personnel) and who besides basic IPv6 skills need improved knowledge supported by examples of good practice in order to implement or transition to IPv6.

Academic Education

The academic educational programmes are designed so that the participants systematically, with simultaneous work and over a longer period of time, obtain fundamental and improved knowledge about the discussed subjects. The study programme combines lectures, e-education, practical work on the equipment in laboratories, simulation environments, regular examinations, examinations of practical skills, etc. For example: in the study programme of the University of Ljubljana, in the field of Telecommunications, in order to successfully pass the examination for the subject Switching Systems and Networks, knowledge of the basics of the functioning of IPv6 is required, which the students acquire during lectures, a seminar and practical laboratory exercises. Many other universities are also introducing IPv4 and IPv6 (the "dual-stack" concept) right from the start, when talking about what an address is. It has been shown many times that students get used to the concept easily. Typically the reaction of the students is that they don't like the way an IPv6 address looks-like, but then get on with it. This is important as IPv6 is more than a decade old and should not be taught as "the new protocol" nobody (the lecturer) really don't understand. No! Dual-stack needs to be in our classrooms right from lecture one. Our next generation of network professionals need to have experience with IPv6.

The academic process includes obtaining theoretical knowledge, practical knowledge, multiple examinations and a final exam that leads to a university diploma or recognised certificates. The advantage of this approach is the great scope of the studies, because the study programme includes all areas of information and communication systems, the knowledge is strengthened over a longer period and because successful completion of the educational process results in a clearly defined level of understanding of the discussed field of topics that is also approved through suitable verified evidence of formal qualifications.

The dynamic of including new content into university study programmes represents a complex and long-running process that depends on programme boards of individual faculties or universities, therefore the level and degree of the integration of new content (e.g. educational topic from the field of IPv6) can vary among individual academic institutions. Because of the long learning process, the academic educational programmes are primarily the domain of universities and higher education institutions that carry out the programmes at various degrees of complexity. Some of the leading academic institutions that also provide content from the field of IPv6 as part of their educational ICT programme.

Leading global manufacturers of network equipment and information solutions also have their own "industrial academic education" that function according to the principle of systematic and long-term oriented educational processes. They are typically specialised and bound to products and solutions of the selected equipment manufacturers. Some of the leading programmes are:

- Cisco Networking Academy that provides a global education programme from the field of network technologies and
- Microsoft IT Academy Programme that provides an educational programme from the field of information technology.

The academic educational process is primarily intended for staff that are at the start of their career or for those who would like to improve upon it, which means that they do not have the full expanse and fundamental knowledge from the field of ICT systems yet. In this case, the IPv6 skills represent only a part of the target specialities that will be mastered during the learning process over a long period of time.

Internal Education in Companies and Organisations

Academic and intensive professional education can be improved upon through additional internal, company-specific content from the field of IPv6 that is provided by experts employed at the company or the organisation. The internal form of the transfer of knowledge is welcome because of the lecturer's integration in the culture of the organisation, their detailed knowledge of the technological situation, operation and requirements of the ICT systems and due to the improvement of the quality of internal working processes.

For example: after the employees participate in the standards education outside the organisation (e.g. intensive professional education), an internal presentation of the method of implementation and the current status of the IPv6 protocol is prepared for the participants.

In the case of some professional services such as the military and security agencies, closed network and information systems are also used, so the acquisition of new special skill based on an internal transfer of knowledge is the only possible way and thus an urgently needed process.

E-education

The model of e-education is a modern approach to learning wherever and whenever. As a rule, it is carried out separately from the place of teaching and thus requires specific techniques of planning the educational material, teaching and communication with the help of information and communication technologies and also special approaches to arranging organisational and administrative matters. It is most often used as a supplementation of the standard educational process (academic education or professional workshops), as a system for the fast distribution of content and instructions and as a system for presenting new services, products and sales - depending on the specifics and the nature of the operation of the organisation. The system provides a statistical supervision of the students, monitoring their progress and evaluating their acquired knowledge. It thus ensures good insight of the mastered content.

E-education content can also be used to prepare a group of participants for the most complex standard education (e.g. a case of good practice of using IPv6). With the introductory e-course, the participants independently acquire the minimum level of knowledge (Basics of IPv6) that is common for all participants. This method of homogenising the group makes it possible for the participants to have a relatively equal level of entry knowledge and as a part of the standard educational process to quickly focus on more complex topics, the specifics of work and practical cases.

For example: an instructor prepares an e-course with basic information on IPv6 technology. Before taking part in standard education, the participants inform themselves about the basics of IPv6 and check their comprehension with a self-evaluation test. Before the lecture, all participants already have the required minimum level of knowledge and can thus together with the instructor focus on the examples of using IPv6 in practice or in a concrete area such as for example in routing in IPv6.

A Proposal for Managing IPv6 Knowledge in Public Administration

For a successful and coordinated transition to IPv6 of all network and service ICT services supported by the public administration system, it will be necessary to additionally educate all employees who plan, build and manage the information communication systems of the public administration from service and application developers and network and system administrators to technicians at the help desk. Every profile of the professional staff that manages a certain working process will naturally require specific IPv6 knowledge.

An established educational tool "Upravna akademija MJU" (MJU Administration Academy - http://www.mju.gov.si/) for managing the knowledge of the employees in the public administration system already exists in the framework of the Ministry of Public Administration (MJU). This mechanism can be used as an established tool (e.g. IPv6 Academy in MJU) that will provide a clear and systematic increase of the level of all necessary knowledge of the employees from the area of IPv6 in the public administration of the Republic of Slovenia. We propose to implement the following in the framework of the MJU/IPv6 academy:

- **overview of needs:** an overview of the IPv6 knowledge required by individual employee profiles should be implemented,
- **systematisation of education:** a selection of educational content and their systematisation should be implemented depending on the identified needs. The educational programmes should be

systematically evaluated and arranged according to various criteria: the target group, the purpose of education, level of complexity and programme content, the required participants' previous knowledge, duration, work methods, an attestation of participation, knowledge, a diploma, a certificate,

- **determining the educational paths:** systematisation makes it possible to prepare various educational paths for specific employee profiles. Depending on the interest, knowledge and tasks of individuals, these can also be combined. Examples of general educational paths:
  - basic education for technical employees for a better understanding of IPv6,
  - specialist education for network administrators for managing advanced mechanisms such as routing, QoS, multicast and other advanced functions of the IPv6 technology,
  - education for management and decision-making for gaining a better insight into the technical area and thus strategic thinking.
- **ensuring education quality:** to successfully achieve the set goals, it has to be ensured that the education content is appropriate, that the suitable participants were sent for the education and that a quality provider of the education was selected. This is ensured with questionnaires that provide a collection of information after the completed education about the level of participants, the level of the education programme, the quality of content and lecturers, etc. The results analysis makes it possible to change and improve individual elements of the educational system if necessary,
- **attestation of participation and knowledge:** at the completion of the education, the participants receive an attestation of participation. If the participants took an examination of knowledge (oral, written, practical) that proves the minimum required level of the mastered topic, they also receive a suitable certificate or a diploma.

The presented model for managing IPv6 knowledge in public administration is sufficiently general, so that it can be used as a sample concept that can also be transferred to the state administration bodies and other public organisations.

A Proposal for Managing IPv6 Knowledge in Corporate Entities

The transition from the IPv4 technology to an IPv6 environment is an ideal example of additional education of a wide range of employees in corporate entities. Operators will have to provide additional education to the majority of their employees. In corporate entities, the additional education will be mainly limited to employees that design, create and manage the information technology (from application developers to technicians at the help desk). Naturally, every profile of professional staff requires specific knowledge:

- application developers must primarily be aware of how the IPv6 addresses affect the functioning of applications and the communication between the clients and servers,
- server managers must make sure that the servers are accessible over both the IPv4 and the IPv6 protocol and that all server software supports both protocols,
- network managers must secure the safe and effective operation of the network that will have to support both IPv4 and IPv6 for years,
- employees at the help desk must be capable of diagnosing and eliminating errors related to both protocols (and there are drastic differences between IPv4 and IPv6 in this area).

Such an expansive educational project is an ideal opportunity for implementing a system for managing knowledge and a system for e-learning into the corporate entity. Instead of ad-hoc solutions ("Let's send a couple of employees for training. I'm sure the others will somehow learn from them"), the management of the IT organisation in the company (in the case of operators, the company management itself) should launch a procedure that will:

- identify specific knowledge required by individual employee profiles,
- provide content that will offer the required specific knowledge to employees - from e-education to short workshops or professional education,
- make sure that all employees receive the required knowledge and that the level of their knowledge will be examined via a suitable procedure.

The manufacturers of information equipment and also global and regional operators have already launched these procedures and, as expected, they cover the majority of their needs with e-education, since it provides a gradual and time-effective acquisition of the required knowledge. Unfortunately, we have yet to see any such trends in Slovenia (except with some operators that are already training their network designers).

7. Attracting Operators or Access Providers

Creating incentives 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.

The key incentive that will force operators to deploy IPv6 is to maintain competitiveness and growth. We have to take into consideration what the care for the user means. The operator must provide the user with access to content and services on the Internet, but nowhere is clearly stated what protocol should be used for this. Over what protocol? It is not specified anywhere, but we can assume that it should be provided over all the possible protocols. At a certain moment, a competitor ISP will decide and implement IPv6 and thus transfer to a dual-stack network. This means that users, services and content will appear that will not be accessible over both protocols or will only be accessible over IPv6 for the sake of simplicity. Operators that will not provide access to content that is only available over IPv6 will soon become non-competitive. What then is the task of an ISP in terms of the care for their users? They can decide to take the following position: "Everything will be accessible over both protocols; I don't care", or they might decide that it would be good and beneficial to provide their users with access to content and services of the competitor ISP over both protocols, since it not possible to know when content and services will appear that will only be available in the IPv6 network.

With time, providing access to the Internet with IPv4 will become more and more complex. Even though the competitor ISP still has IPv4 addresses available, the procedure of providing the content and services of a small company or residential client will become more difficult. As a rule, they will get one IPv4 address from the ISP behind which they can conceal an entire network together with servers. It is known how to direct ports through NAT, but a lot of work is required. Those less instructed and professionally experienced users can have many difficulties with these settings. Quickly they can set it up so that nothing will work for them anymore. By implementing the CGN technology, the complexity of translating addresses will increase, which some mobile operators (even Slovenian) that have been using CGN for several years have already experienced. It is also presumed that in the future, entire access networks will be concealed behind a big NAT in the core of the network (CGN), which means that the user will no longer get a public IPv4 address but a private one, hidden to the world. Some Slovenian mobile operators have been doing this in their mobile data networks for several years.

In IPv6, everything is much easier. Deploying IPv6 undoubtedly simplifies the settings of end devices. According to the recommendations by the IETF (RFC3177), each resident CPE device should receive its own part of the IPv6 address space and each computer their own public IPv6 address. The IETF recommends to allocate (route) the /64 (or even /48) segment to every resident CPE device, which means the elimination of NAT, since every computer or device gets their own public IPv6 address. It can start providing content or services from the computer/server at home, and if the IPv6 firewall is set up correctly, this is a simple task.

Until now, service and content providing over the Internet was primarily the domain of larger companies - content providers who have their data centres or are hosting with servers at an ISP or server hosting provider. By deploying IPv6 and eliminating the NAT mechanisms, unimagined new possibilities are opening up for smaller companies and residential users where the content and services are not only ftp and http, but much more.

Thus, new content will appear that will be inaccessible to the users of ISPs who have not implemented IPv6.

The orientation of an ISP that takes care of the user can be a strong mechanism of a coordinated and timely IPv6 implementation in ISPs all the way to the user, since nobody wants their users to switch to another operator or to have the disgruntled users complaining to their help desk.

The main task of internet service providers should be the care for the user and their best possible connectivity to services and content on the Internet.

8. A Sample Model for Including Proper Specifications onto the Requirements Lists for Tenders for Procuring Communication and Computer Equipment and E-Services of the Public Administration

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

The IPv6 protocol is the latest stage in the development of the internet protocol intended for introducing the next generation of internet systems for solving the issue of IPv4 address space shortage and the improvements of some functions and capabilities. The IPv6 protocol introduces a series of innovations and advantages that are reflected in functionalities such as: a mechanism for determining MTU, an improved protocol for enquiry between neighbours, an improved QoS mechanism, a mechanism for IP parameter auto-setting, improved routing functions, improved mobility and security functions.

When using untested and narrowly used new technologies and solutions, it is important that the users are made aware, before the production stage, of the maturity of the technology or of the individual development stages that an individual solution must pass to achieve the level required for production systems in order to ensure stable performance of end production systems and to protect the investment.

The life cycle of every technology (Figure 8-1), including IPv6, can be divided into four fundamental development phases that in general follow the following sequence:

- standardisation phase,
- product development phase,
- verification phase,
- production phase.

Only after successfully completing the standardisation procedure, the development process and the verification process will the individual solution be appropriate for use in production systems.

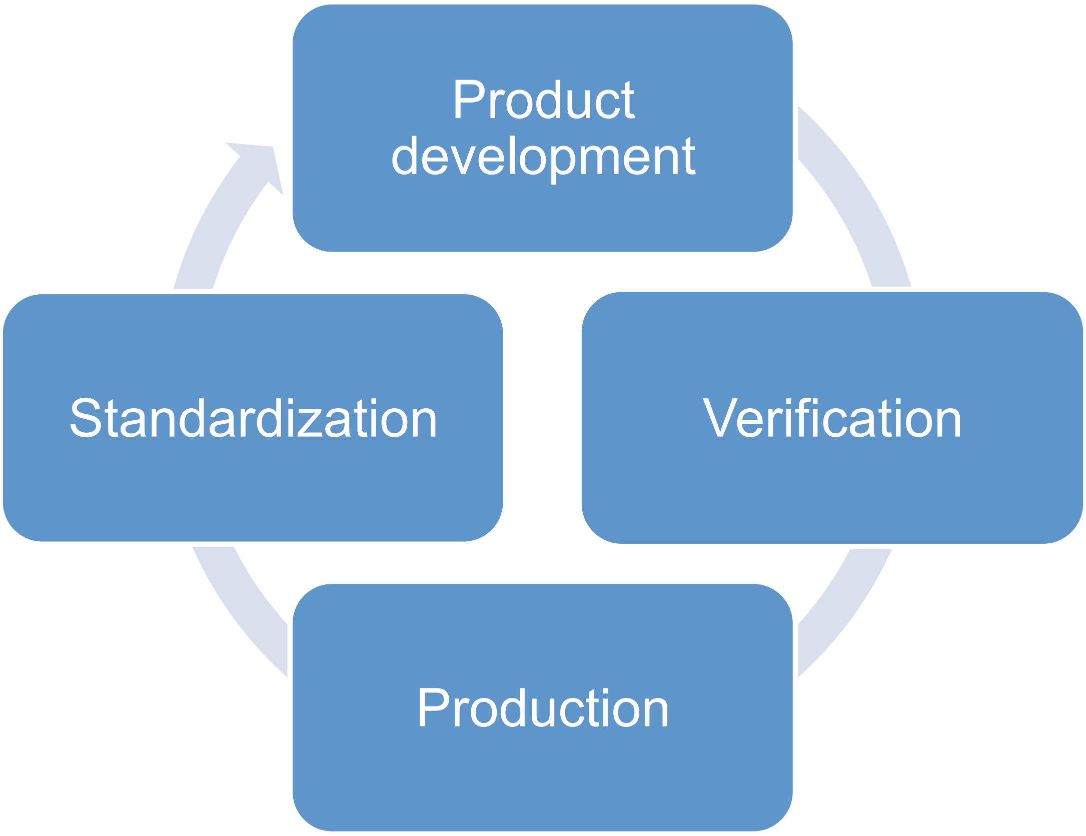


Figure 8-1. Technology life cycle.

We should be aware that a technology enters the period of maturity only after the standardisation process is completed. Thus, the product implementations become increasingly more stable and reliable, since the solutions of the manufacturers have gone through a series of verification procedures and testing that are carried out by the manufacturers themselves during the development as well as by outside independent institutions, associations and forums and also the end user in the final stage. Through pilot implementations, the solutions become sufficiently tested and reliable and thus appropriate for use in production environments.

Due to the rapid expansion of internet systems and solutions, it is hard for standardisation to keep up with the speed of product development due to the nature of the operation of standardisation procedures. Standardisation is often not provided in an appropriately short time. Consequently, the product development at the leading IP equipment manufacturers is often ahead of the standardisation. The manufacturers thus sell non-standardised or proprietary solutions on the market that are difficult to verify appropriately, but due to the demands of the market, they are nonetheless used in production systems.

The described issue represents a considerable challenge for planning, the selection of appropriate equipment and for establishing new production systems, since it often requires risky selection decisions that represent a compromise between technological modern solutions or standardised solutions that require narrowly specialised knowledge.

Chapter 8 will therefore present the standardisation process of internet systems, the analysis of the present standardisation state of IPv6, the process of the verification of IPv6 products and the final proposal for including specifications into tenders for purchasing ICT equipment of the public administration of the Republic of Slovenia.

Standardisation of Internet Protocol

The internet standardisation process is carried out by the Internet Engineering Task Force - the IETF (http://www.ietf.org/) as part of regional working groups. This organisation operates according to the principle of open community where everyone, even an individual, can participate and contribute towards the standardisation process. The standards are issued in the form of RFC specifications (Request for Comment) that define the operation of an individual protocol, a device and basic functional components of a service (e.g. BGP, MPLS, VPN). Ideals followed in the framework of their work are:

- technical excellence,
- implementation in testing of the functionality before issuing the final standard,
- clear and with consensus approved specification of standards,
- openness and fairness.

Each RFC specification goes through several phases of development and testing (maturity levels) that reflect the maturity and prevalence of an individual standard. The IETF defines three maturity levels of the protocol, solution or technology (RFC 2026):

- Proposed Standard,
- Draft Standard,
- Internet Standard.

The RFC specification can obtain the status of "internet standard" only after two equipment manufacturers have implemented all the required functionalities set out in the RFC specification and demonstrated interoperability of products, which means that a compatibility test was carried out between the two products.

Other documents marked as RFC are also created in the framework of the IETF groups but are only informative or experimental in nature. Such documents do not represent the IETF standardisation process and are not obligatory for equipment manufacturers. These include RFC specifications marked "Informational" and "Experimental". Some of the more inventive equipment manufacturers thus issue their proprietary solutions in the form of "Informational RFC" and covertly specify them as "standard" internet solutions.

The State of IPv6 Standardisation

The IPv6 Working Group (http://www.ietf.org/wg/concluded/ipv6.html), within which the development of basic standards for the support of the operation of the next generation internet protocol was carried out, ended its work in 2007. They adopted 43 proposals of standards and their amendments. Despite the fact that the core of IPv6 specifications is accepted and stable, the development of supplemental and expanded IPv6 standards is still ongoing in other working groups (http://datatracker.ietf.org/wg/) such as:

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

- Layer 3 Virtual Private Networks,
- other organisations that envisage the use of IPv6 in their systems, for example 3GPP.

The IPv6 standardisation procedure is not yet complete. Consequently, the equipment manufacturers often justifiably face the dilemma of what set of RFC standards to use for what type of products and what advanced functionalities to implement, because the standardisation has not been completed yet and in the segment of product definition is mainly undetermined or is not under the jurisdiction of IETF. In the cases of some types of equipment, the set of IPv6 standards that it must support is not clearly defined and shall be formed depending on the needs of users or with the agreement of an association of manufacturers, operators and other end users.

On the other hand, the buyers of the equipment also face the dilemma of what set of specifications and functions can be expected for an individual IPv6 product that is available on the market.

IPv6 Product Verification

The entire process of product verification, the purpose of which is to provide for stable and long-term functioning of the solution in live IPv6 environments, encompasses the following testing sets:

- conformance testing – ensures that a network element (e.g. router, server) functions in conformity with the prescribed set of standards,
- interoperability testing – ensures that equipment from various manufacturers can be successfully linked with each other,
- functional testing – determines whether the products contain all the required functionalities,
- performance testing and benchmark testing – determines the quality characteristics of the product that is subject to the verification process.

During conformance and interoperability testing, there should be no deviation among products of various manufacturers. This means that all products in the tested segment should fulfil the prescribed requirements 100%. The results of conformance and interoperability testing thus represent a minimum threshold that a product should cross in order to meet the terms of the tenders.

In the area of functional, performance and benchmark testing of solutions, the solutions by various equipment manufacturers may differ from one another. This segment shows the innovation and added value of manufacturers and thus their key competitive advantage that must represent the final criteria for the selection of equipment in tenders.

IPv6 Product Certification

Three organisations are carrying out pioneer work in the area of specification, verification and certification of IPv6 products:

- "IPv6 Ready", which represents an open global association for verification of IPv6 solutions and operates under the auspices of the IPv6 Forum,
- the Department of Defence of the Unites States of America (DoD), which prescribes verification procedures for IPv6 network equipment that will be used in the systems of the Department of Defence,
- the National Institute of Standards and Technology (NIST), which prescribes verification procedures for IPv6 network equipment intended for use in US public administration networks.

The "IPv6 Ready" Programme

Very early on in the stage of development and implementation of IPv6 technology, the IPv6 Forum established a validation process, the IPv6 Ready Logo Programme (http://www.ipv6forum.com), which is an open international association for verification of IPv6 solutions. In 2004, they developed the "Phase 1 Logo Certification" process, which tested five IPv6 product classes. With "Phase 2 and Phase 2 Logo Certification Process", the requirements for the tested products were made even stricter. "IPv6 Ready" certification encompasses only the first two sets of verification tests:

- conformance testing,
- interoperability testing.

The functional, performance and benchmark testing are not carried out in the process of "IPv6 Ready" certification. More than 891 various products have already been certified as part of the "IPv6 Ready" programme. A detailed and up-to-date list of certified equipment can be found at www.ipv6ready.org.

Today, the IPv6 Forum is still the leading international organisation in the testing and verification of procedures, but their programmes represent a certain dilemma in terms of the justifiability of certification, because the terms of the IPv6 Ready certification are not yet clearly defined.

The US Department of Defence Programme

Due to lax provisions in the segment of IPv6 products, the US Department of Defence in 2005 developed a clear and standardised definition of "IPv6 Capable" and a thorough testing programme that enables validation of IPv6 capabilities for IPv6 equipment that will be used in the networks of the US Department of Defence (http://jitc.fhu.disa.mil/apl/ipv6.html). The programme also provides documentation of requirements and a process of IPv6 product certification programme implementation. Besides these, the services of the DoD, the IPv6 Transition Office, the DoD Information Technology Standards Registry (DISR) and the Interoperability Test Command (JICT) also formed a series of three documents that encompass a model of product certification for IPv6 capability in the area of:

- conformance,
- interoperability,
- performance,
- information assurance.

The "IPv6 Capable" programme is characterised by 6 sets of IPv6 products:

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

Numerous offices and organisations of the US Department of Defence have participated in developing these documents. This way, they formed a recognised and standardised IPv6 profile of the US government that was also used as a model by the US National Institute of Standards and Technology (NIST).

The NIST Programme

In 2009, the National Institute of Standards and Technology (NIST) issued a IPv6 testing methodology, partly as a continuation of the IPv6 certification programme (http://www.antd.nist.gov/usgv6/testing.html) and the test programme of the US (USGv6 – A Profile for IPv6 in the U.S. Government), which is intended for verifying network solutions of the US public administration. The methodology is intended as a recommendation for all accredited and test laboratories for accreditation, standard reference tests, validation criteria of testing methods and feedback mechanisms for upgrading the quality and consistency of testing in the field of IPv6.

The NIST document provides a tool for testing three basic types of network nodes, categorised as "hosts", "routers" and "network protection devices", namely;

- conformance test methods – checks whether the device is in conformity with the standardised protocol specifications,
- interoperability test methods – checks the functioning of the device in a network with devices from other manufacturers over separate or connected subnetworks, while simultaneously requiring the confirmation of device interoperability with at least three or more commercial IPv6 implementations,
- network protection test methods that require the adjustability of configurations, recording, environmental security and suitable filtration of IPv6 packets.

The document additionally determines the frame for testing traceability and mechanisms for upgrading testing procedures in cooperation with users.

Testing methods include basic IPv6 functionalities, for example DHCP and IPv6 addressing, security, service quality, multicast, network management and specific connection technologies. Equipment manufacturers that are deploying IPv6 technology must also examine and test any changes that IPv6 implementation causes on other existing standards.

The "UGSv6" programme defines 3 profiles of IPv6 products:

- "Host Profile",
- "Router Profile",
- "Network Protection Device Profile".

It also additionally specifies the categories of functional requirements; "IPv6 Capabilities" that determine the following functional sets:

- "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".

Specifications of the go6 Expert Council and the go6 IPv6 Working Group

At the initiative of the wider internet community, the "go6" Expert Council and the "go6 IPv6 WG" working group, comprised of recognisable Slovenian experts from the field of internet systems, prepared a list of specifications to support the RFC standards that the IPv6 network devices that will primarily be used in networks of the public administration of the Republic of Slovenia must conform to. The recommendation divides ICT products into four sets of hardware:

- host: client or server,
- L2 switch,
- router,
- equipment for ensuring network safety (firewalls, IDS, IPS, etc.).

The specifications only provide a list of required standards, but do not prescribe detailed testing methodologies and verification procedures.

A Model of Including Specifications into ICT Tenders of the Public Administration

The analysis of the present state of IPv6 solutions standardisation and verification from the previous chapters leads to the conclusion that there is currently no clearly defined approach that could be simply adopted and directly included as a reference guide for preparing tender documentation when purchasing ICT equipment for the IPv6 of the public administration of the Republic of Slovenia.

It should also be taken into account that networks that belong under the auspices of the Republic of Slovenia are varied in size, design, openness and security and capability characteristics because they are used by public state bodies (state portals) and professional services of the government of the Republic of Slovenia (Slovenian Intelligence and Security Agency), the Ministry of Defence (Slovenian Armed Forces, Administration for Civil Protection and Disaster Relief, Intelligence and Security Service) and the Ministry of the Interior (police). The latter systems exceed the scope of this document and require an additional in-depth analysis.

Open Dilemmas

When preparing tender documentation for various target network segments of the public administration, a compromise will be needed on several levels that will not only take into account the technical requirements but also the security, economic, business, legal, formal and in some cases political consequences. Some of the dilemmas are underlined below.

What set of standards to use for which product?

The core of IPv6 standards was adopted in 2007 and represents a stable set of specifications that could be included as obligatory reference documents [1]. An open dilemma that can be solved in various ways is what set of standards to demand in a tender for an individual IPv6 product:

- a set of RFC standards prescribed for individual groups of IPv6 products by the "IPv6 Ready" programme,
- a set of RFC standards and other recommendations prescribed for IPv6 products by the programme of the US Department of Defence,
- a set of RFC standards and other recommendations prescribed for IPv6 products by the NIST verification programme,
- specifications of the go6 Expert Council and the go6 IPv6 working group.

The chosen set of standards must depend on features and requirements of the target system for which the equipment is intended, and in some cases of individual special network solutions, it will be necessary to additionally expand the presented specifications of own solutions.

Should the IPv6 Equipment be Properly Certified?

Three certification programmes have been created so far (IPv6 ready, DoD, NIST), which, however, are not entirely comparable to one another, because conceptual bases were taken into account for various target systems: the military systems (DoD), the public administration systems (NIST) and the generic system (IPv6 Ready). The programmes vary in terms of:

- the basic product definitions,
- the type and scope of verification tests,
- the methodological approach to testing,
- the reproducibility of test procedures and the method of test laboratory accreditations.

IPv6 Ready certification is the most generic approach to certification that was created at the level of open community with international consensus. The level of verification represented by the IPv6 Ready logo on a product ensures the end users that the equipment was made in accordance with standards and that interoperability was checked with one or several similar products. The certificate thus does not reflect qualitative parameters such as the functional, benchmark and performance characteristics of an individual product.

The certification programmes of the US Department of Defence, "IPv6 Capable", and NIST, "USGv6 Profile", made the verification even stricter, because, besides conformance and interoperability testing, they also require the IPv6 products to have certain functional and capability features. The US Department of Defence certification programme, "IPv6 Capable", or its individual segments could thus conditionally represent grounds for preparing terms of the tenders of the Slovenian Armed Forces (MORS), because they take into account the development guidelines of the NATO systems (net-centric warfare) that envisage the use of commercial civil products (COTS – Commercial Off the Shelf) in military communication systems (http://jitc.fhu.disa.mil/tst_time/docs/year/mar08.pdf). The "USGv6 Profile" could also be a reference concept in preparing tender specifications of the public administration of the Republic of Slovenia.

Regardless of the certification programme chosen, it should be mandatory to carry out performance and functional verification of the network equipment in a proper accredited laboratory before selecting it or including it into the production network. Besides the existing IPv6 certification programmes, the laboratory can be represented by an accredited laboratory of the manufacturer of the equipment, a supplier or buyer or the verification can also be carried out by an outside independent institution.

The "IPv6 Capable" and "USGv6 Profile" certification programmes provide an excellent reference concept and model of how state institutions should address the technical issue of implementing new technology such as IPv6 into public communications systems in a systematic and professional way.

Examples of Including Specifications into Tenders of the Public Administration

The requirements for IPv6 support can be provided in a number of ways. We have provided three examples:

1. The first is the work of the go6 Expert Council and the Slovenian IPv6 working group and provides a specification of support for RFC standards with which four groups of devices must comply.
2. The second is a specification of tests that can be carried out by manufacturers with the IPv6 Forum and its IPv6 Ready programme. The latter is divided into two stages: the first encompasses testing and certification of basic protocols, the second testing and certification of more advanced IPv6 functionalities.
3. The third option is a combination of the above options.

All three options are described in sections I, II and III.

The first, second or the third option can be used for requirements specifications, depending on the needs and required accuracy of IPv6 support.

Section I - Requirements, Categorised by Devices and Support at the Integrator (according to the proposal of the go6 IPv6 Working Groups)

The proposed text for public tenders with requirements on the suitability of ICT equipment and integration service providers for the IPv6 protocol

Text in Slovenian:
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.

Text in English for international tenders:

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.

Requirements for standards support

The ICT hardware can be roughly divided into four groups:

- host: client or server,
- L2 switch,
- router,
- equipment for ensuring network safety (firewalls, IDS, IPS etc.).

The requirements for standards support are divided into mandatory and optional. The equipment must fulfil the mandatory requirements for standards, the optional requirements provide additional points. If the hardware does not fulfil all mandatory requirements for standards support, it is considered unsuitable.

Requirements for the "host" equipment

Mandatory support:

- Basic IPv6 specification (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, and RFC2402],
- IKE version 2 (IKEv2) [RFC4306 and RFC4718],
- if support for mobile IPv6 is required, the device should support the MIPv6 [RFC3775] and "Mobile IPv6 Operation with IKEv2 and the

Revised IPsec Architecture [RFC4877]" standards in the "processing" mode,
- DNS protocol extensions for incorporating IPv6 into DNS resource records [RFC3596],
- DNS message extension mechanism [RFC2671],
- DNS message size requirements [RFC3226].

Optional support:

- corrected 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],
- Packetisation Layer Path MTU Discovery [RFC4821].

Requirements for the consumer "switch" equipment

Mandatory support:

- MLDv2 snooping (RFC4541).

Optional support (for management):

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

Requirements for the Enterprise/ISP "switch" equipment:

- Mandatory support:
- 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.

Optional support (management):

- 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.

Requirements for the "router" type equipment:

Mandatory support:

- basic IPv6 specification (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],

- if a dynamic internal gateway protocol (IGP) is required, RIPng (RFC2080), OSPF-v3 (RFC5340) or IS-IS (RFC5308) should be required. The contracting authority should specify the required protocol,
- if OSPF-v3 is required, the device should support "Authentication/ Confidentiality for OSPF-v3" (RFC4552),
- if the BGP4 protocol is required, it must be in accordance with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545,
- QoS support (RFC2474 and 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],
- if 6PE is required, the equipment should support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) [RFC4798]",
- Multicast Listener Discovery version 2 [RFC3810],
- if support for mobile IPv6 is required, the device should support the MIPv6 [RFC3775] and "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture [RFC4877]" standards in the "forwarding" mode.

Optional support:

- corrected 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, and RFC4302],
- IPSec-v2 [RFC2401, RFC2406, and RFC2402],

- IKE version 2 (IKEv2) [RFC4306 and 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,
- Packetisation Layer Path MTU Discovery [RFC4821].

Requirements for the "network security" equipment

The equipment from this section is divided into 3 subgroups:

- a firewall (FW),
- the intrusion prevention system (IPS),
- an application firewall (APFW).

Mandatory support:

- basic specification 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),
- if the BGP4 protocol is required, the equipment must be in accordance with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPs, APFW),
- if a dynamic internal routing protocol (IGP) is required, RIPng (RFC2080), OSPF-v3 (RFC5340) or IS-IS (RFC5308) should be required. The contracting authority shall specify the required protocol (FW, IPS, APFW),

- if OSPF-v3 is required, the device should support "Authentication/ Confidentiality for OSPF-v3" (RFC4552) (FW, IPS, APFW),
- support for QoS (RFC2474 and RFC3140) (FW, IPS, APFW),
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW),
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW).

Functionality and features that are supported over IPv4 should be comparable with the functionalities supported over IPv6. For example, if an intrusion prevention system is capable of operating over IPv4 in Layer 2 and Layer 3 mode, then it should also offer this functionality over IPv6. Or if a firewall is running in a cluster capable of synchronising IPv4 sessions between all members of a cluster, then this must also be possible with IPv6 sessions.

Optional support:

- corrected ICMPv6 (RFC5095),
- DHCPv6 client/server (RFC3315),
- Extended ICMP for multipart messages (RFC4884),
- SEND (RFC3971),
- SLAAC Privacy extensions (RFC4941),
- Stateless 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/Confidentiality 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),
- Packetisation Layer Path MTU Discovery [RFC4821].

Requirements for IPv6 support in software

Besides IPv4, all software should also support and communicate over IPv6 protocol. If network parameters are set up within the software (local or remote server settings), it should also have a configuration section for the IPv6 part of the protocol stack.

There should be not significant differences between the IPv4 and IPv6 functional capabilities; the user should not notice any difference between the software communication with the network over IPv4 or IPv6.

Requirements for qualifications of the provider of integration services

The service provider of the software integration into the contracting authority's network should have at least three employees that have valid equipment manufacturers' certificates on the qualification for management of the equipment. These certificates should contain general knowledge of the IPv6 protocol, network design with IPv6 protocol and ensuring security on the IPv6 protocol. If it is demonstrated during the integration and installation of the equipment that the integrator is not sufficiently qualified and capable of correctly integrating and setting up the IPv6 communication into the network, the contract shall be terminated and annulled.

The definition of correct integration, the timeframe and level of network interference during the installation of the equipment is subject to the agreement between the contracting authority and the integration services provider.

It is also recommended that the service provider of the integration of equipment into the network also has employees with broader knowledge and certificates from the field of IPv6 than provided by certificates of the equipment manufacturers. These certificates can be obtained at independent education providers that are not dependant on equipment manufacturers. The contracting authority can offer additional points for such knowledge and certificates.

The provider must sign a form on technical qualification for designing, building and integration of ICT equipment into IPv6 networks.

STATEMENT

ON TECHNICAL QUALIFICATIONS FOR DESIGNING, BUILDING AND INTEGRATION OF ICT EQUIPMENT INTO IPv6 NETWORKS

Provider______________________________________
Address____

Under criminal and material liability, we declare:

- that we have a sufficient number of employees for performing the services,
- that the employees are professionally qualified for their work - designing, building and integration of ICT equipment into IPv4 and IPv6 networks,
- that the provided service is of quality and complies with the requirements of the tender documentation.

In ____________________, on ____________________

Stamp and signature of the provider

____

Section II - Testing and Certification of Devices according to the IPv6 Forum's system entitled "IPv6 Ready"

IPv6 Forum is a European organisation and association of various IPv6 Forum chapters across countries. Among other things, they also established a fairly comprehensive system of testing and certification that is now being implemented by various laboratories around the world. In the "IPv6 Ready" database, there are currently 871 entries under phase-1 or phase-2, which is quite a sizable collection of equipment that meets at least the basic requirements of IPv6.

In order to fulfil the phase-1 requirements, over 170 tests have to be performed.
The list of all tests required for phase-1 and phase-2 (phase-1: requires only a few):
[1]

Detailed specification of the progress and requirements for testing is described in:
http://ipv6ready.org/docs/Core_Conformance_Latest.pdf

The list of certified equipment is available at:
https://www.ipv6ready.org/db/index.php/public

The proposed text for tenders in Slovenian:
»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.«

The proposed text for tenders in English:
"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 programme with a "Phase-1" logo certificate. A "Phase-2" logo certificate adds additional points (+10%) in the tender evaluation procedure."

Section III - Sharing of Both Specification Methods with Requirements

At times, certain equipment has not yet been tested for IPv6 and it would not be sensible to label it unsuitable in advance, since it might be suitable and might appropriately meet all IPv6 norms. It may just have to be tested first. In this case, the contracting authority can request an examination of the suitability of the equipment according to the IPv6 Ready method in our laboratories that are qualified and accredited for such examinations or they might simply request an IPv6 certification and, in the event that the equipment has not been tested yet, they can list the requirements for the support of RFC standards from the relevant part of Section I of this document.

The proposed text for tenders in Slovenian:
»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]

The proposed text for tenders in English:
"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 programme 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 the bidder can put the equipment to the test at one of the Slovenian laboratories that offer the IPv6Ready testing programme and enclose the testing results. If this is not possible, the equipment must comply at least with list of RFCs listed below:
[appropriate list of selected mandatory and optional RFCs from 1st option]

9. Encouraging Content Providers (Campaigns, Incentives, etc.)

This section deals again with the biggest problem: adoption and incentives for adoption. Here, we provide suggestions and ideas for companies thinking about adoption. It also highlights consequences for latecomers. While the recommendations may not fit every case, this section should be given a consideration.

The Challenges for Content Providers

As we have already described above, an increasing gap between the readiness of connectivity providers (ISP) and content providers to implement the IPv6 protocol has become evident. In some cases, mainly in environments that use open source, the transition to the IPv6 environment is almost trivial and does not interfere with the application code.

Example: an online application in PHP that is carried out in the environment of the Apache web server requires almost no corrections when transferring it into the IPv6 environment (under the condition that it does not keep numerical addresses of clients in a poorly dimensioned database). An application, written in the ASP.NET development environment on a Microsoft web server, is generally ready for the transition into the IPv6 environment.

Opposite example: an application written in the lowest programming language (for example C/C++) that directly accesses the transport or networking layer (TCP/IP) can require extensive changes and long-term testing.

So what is the problem? Smaller content providers depend on web hosting providers that in most cases have barely mastered the knowledge needed for implementing reliable hosting in the IPv4 environment and who, due to low hosting prices, have no funds needed for educating staff, upgrading hardware and software and to implement the transition. These web hosting providers will in a few years time be forced to carry out a transition into the IPv6 environment (and many of them will slowly wither away), which will not have any significant effect on agile content providers, because there are already global alternatives available (Google). From the national viewpoint, the migrations of local content abroad can naturally be problematic due to the related delays and dependence on foreign providers.

Bigger content providers (with own servers) will be losing their competitive advantage due to their delusions about the challenges of IPv6 (mainly those who use the Internet in their own business process such as for example web stores or banks), but in the long term their out-of-date information infrastructure will force them into rapid and thus poorly planned and consequently more expensive upgrades (similar to the situation when Slovenian banks, after neglecting their IT infrastructure for decades, were forced to suddenly carry out a rather expensive transition into the Eurozone).

Public Administration as a Facilitator of Implementing IPv6 Services

Due to the rules of the European Community, Slovenia has fairly limited possibilities of using direct initiatives and investments, but it can indirectly put pressure on the providers of these orders (companies in the IT sector, from programming companies to providers of network solutions) and can thus prepare them for a successful transition into the IPv6 environment. If state institutions indirectly pressure these providers to master the basics of the IPv6 environment and to adapt their applications for operation in this environment (or to simplify them so that they become independent of the network and transport layer, which is an even better solution), they will thus become ready for the moment when other content providers also feel the need to transition into the IPv6 environment.

In order to successfully put pressure on the IT sector, it is urgent that all public tenders from this field clearly require a full functioning of the new application and network equipment in the IPv6 environment or, where the above is not possible, to implement operation in the IPv6 environment as one of important factors in evaluating the offers in public tenders.

An additional encouragement for the transition into the IPv6 environment could also be provided by the technological agencies, the Ministry of Higher Education, Science and Technology and European funds. Besides encouraging other technologies in the IT environment, these institutions should also encourage the adaptation of network and application infrastructure to the IPv6 environment, especially with an emphasis on application infrastructure and migration of the existing web solution into the dual-stack environment.

Cloud Services

Cloud computing is a form of computing where self-extensible, mostly virtualised computer resources are available as a series of services over the public internet. There are several different cloud computing services:

- SaaS (Software as a service) – the service of providing software,
- IaaS (Infrastructure as a service) – the service of providing infrastructure,
- DaaS (Data as a service) – the service of providing data,
- .....

In general, the joint synonym XaaS (Anything as service) applies for all cloud services. Currently, all XaaS services in the ICT environment are seen as a hot commodity. There is a lot of talk, but such services and implementations in reality are few. The development guidelines of web services are oriented towards various cloud service architectures. Many cloud infrastructure manufacturers are still in the research and development stage. The area of developing infrastructure and cloud services is an ideal area for adapting the IPv6 internet protocol. It is unwise and cost-wise uneconomical to develop services of the future on a protocol of the past. The idea of supporting the IPv6 protocol in cloud infrastructures is by all means worthy of support and discussion and can turn into a nice example of good practice. The leading cloud service providers, Google, has an entire infrastructure already prepared for providing services over the IPv4 and IPv6 protocol, and all other competitors are actively engaged in supporting the latter. For companies that are developing cloud services, it is an opportunity and at the same time a competitive advantage, if their solutions simultaneously support both the IPv4 and the IPv6 protocol.

The Opportunities of Internet Search Engines

The issue of disinterested and self-sufficient content and service providers is prevalent around the world. IPv6 is gradually being implemented in internet access providers, but content providers are mostly still ignoring the coming changes.

The basic principle of content providers on the internet is of course profit. There are several types of content, some provide news and articles and make money by advertising, others offer their services using their own content – and that can be anything, from a travel agency that offers vacations in Greece to blacksmiths from Rome who forge nails and horseshoes. Everything ends up on the Internet sooner or later.

Similar services, content or objects are provided on the internet by their competition, which is appropriate and in the spirit of competition. Because for the past years it is hard to imagine searching the Internet without the Google search engine, a real struggle developed between content providers that prepare and adjust their content to Google’s "rules" so that they rank as high as possible in the search results. That is competition and there is nothing wrong with that. The site that will be better optimised will rank higher in the search engine in terms of certain keywords.

An entirely new business has grown from this, the SEO (Search Engine Optimisation). It is a science and knowledge of optimising websites, so that they rank as high as possible on sites with search results for individual phrases or words. Because there are always new "holes" in the optimisation, Google is constantly updating and changing the rules and algorithms according to which the content is ranked in the search results. Companies striving towards better position and profit are prepared to do more and more in order to rank better than the competitors in the Google search engine or on the website with search results.

The Google search engine requires that the content is relevant and that the user experience of the first recommended site is good. There are certain rules that must be followed.

After some time, the IPv4 addresses will start running short and we do not know what will happen then. Therefore, why should Google not take into account as one of its ranking criteria whether content is accessible from IPv4 and IPv6 networks and whether it has the A or AAAA record? Such criteria could be considered as "future-proof". The main thing would be for Google to publicly announce that sites and content that is accessible over both protocols will be ranked higher.

In that moment, a mass transition of content to IPv6 networks would occur, since no one would be willing to miss the opportunity to be better ranked than they are currently and would not want to rank lower, because this would mean that the competition is ahead of them. Content providers would probably immediately demand IPv6 connectivity to their servers and as fast as possible presence on both protocols. Another beneficial element could be added into the SEO fight - "Our content is available over both versions of the Internet".

Google might be the largest Internet search engine, but it is not the only one. We could start this initiative in Slovenia and propose our most used internet search engine, Najdi.si, to implement such criteria for ranking content on the website with search results. We presume that the search engine could add an increase from 5% to 10% on achieved points when estimating the website content, if the website were available over both networks.

Encouraging Innovation and Creativity through Competition

In order to increase the interest with programmers, network designers and content providers, Germany and Japan used mechanisms that encourage competition and creativity. They issued an invitation to a competition for the best IPv6 application – be it a programme that runs on end devices (PC, phone) or a system of applications that run on servers. Essentially, almost any more complex innovative use of IPv6 for application purposes was eligible to be entered into the competition.

In Germany, the competition was carried out as part of the IPv6 Council's meeting that took place at the Hasso-Platnner institute in Potsdam, and the main award in the amount of €10,000 went to Gert Doering for restructuring the OpenVPN mechanism so that virtual reality private networks can also support IPv6 traffic.

We recommend competent institutions in Slovenia to collect sponsorship resources and to organise a similar competition. Thus we could attract innovative individuals and recognised companies that engage in providing content on the Internet.

The Slovenian IPv6 summits are meetings co-organised by Arnes, LTF and the go6 Institute. They are organised twice a year and combine the interested public, state institutions and agencies, the industry and operators and are intended for promotion, facilitation of implementation and education in the field of IPv6. It is worth considering whether the Slovenian Ipv6 Summit might be an appropriate event for such a competition.

Enclosure 1: The proposal for internet search engines (in English), by Sander Steffann and 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 to 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 host – this host 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 minimises 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. How to Raise Awareness

What is the road map going to be? This section provides a very interesting perspective on the future and how the transition can be undertaken. In places, this section picks up old ideas on 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 and market incentives have been a focus of the whole document. Here everything is brought together.

The concern for raising awareness of IPv6 in Slovenia started in 2008 with the go6 Initiative that soon grew into the non-profit go6 Institute and made strategic connections with the Arnes and LTFE Institutions. Since then, awareness about the exhaustion of the IPv4 address space and the issue of slow implementation of IPv6 into services and networks in Slovenia has grown significantly, but we still believe that it is not high enough. Sometimes, awareness and actual actions are not completely in sync, since the human tendency is to resolve issues only after they actually affect and hurt us.

The following sections discuss this issue:

- raising awareness of access providers,
- raising awareness in business environments,
- raising awareness in state and public administration,
- raising awareness in the general public,
- past examples of raising awareness,
- proposals for raising awareness in the future.

Raising Awareness of Access Providers

The internet access providers were the first to start tackling implementation. They are the largest consumers of IP address space and will also be the first and the most affected by the shortage of IPv4 addresses. Every time they connect a new user, they have to assign a dynamic or static IP address. The same is true for connecting a business user or a user on a hired connection.

These users usually request a static IPv4 address and a set of IPv4 addresses for their internet servers and services. Native IPv6 is already being offered to business customers on hired connections by some ISPs in Slovenia. But in order to access residential users over xDSL, FTTH or cable technology, we will have to wait for IPv6 implementation into CPE devices.

In most cases, the cable operators are only reselling the internet access of existing providers.

The awareness of internet service providers is currently being raised at semi-annual Slovenian IPv6 meetings that are co-organised by the go6 Institute, Arnes and LTFE. Apek has a list of registered operators, and the IPv6 summit organisers can invite all operators to attend the event.

Raising Awareness in Business Environments

The awareness of companies and content and service providers regarding the need to transition to IPv6 has yet to reach the required level. An entire chapter in this document has already been dedicated to content providers, so this section focuses on business clients: large, medium-sized and small companies.

In many cases, the main issue of the IT staff in companies that do not directly engage in IT is lack of knowledge, since they feel there is no need to implement IPv6 into their business environment. What's more, due to preoccupation with other challenges, it can be expected based on past experience with similar turning points (the introduction of the Euro in 2000) that companies will begin solving IPv6 issues when it will already be too late. The fact that the majority of companies will not actually need IPv6 for a couple of years is also not helpful for their readiness to begin implementing IPv6 into their environment.

The companies that are not internet service providers will have to face IPv6 in three stages:

- When the internet service providers start assigning IPv6 addresses to residential users (in 1 to 2 years, in Slovenia maybe even later), most content will still be accessible over the IPv4 protocol. The IPv6 client's access to IPv4 content will become a problem of the internet service providers, who will have to solve this issue with one of the transition mechanisms (NAT64, for example).

During this stage, the majority of companies will still be unaffected by IPv6, since they primarily provide their clients with traditional web services through the HTTP or the HTTPS protocol that both operate smoothly with all transition mechanisms. The companies providing advanced services such as on-demand click-to-talk service will run into some minor issues. Unfortunately, there are not many such companies in Slovenia, because it is simpler (and cheaper) to publish a free telephone number (with the 080 prefix) on the company's web site.

Note: Business users who provide their users with secure internet access to a private network through the IPsec technology will probably have to face the IPv6 issue sooner than others, because the IPv6 client's access to the IPsec concentrator, which only supports IPv4, provides a significant challenge. Where SSL technology is used instead of IPsec, such issues will not arise. SSL technology is slowly replacing IPsec, because it is simpler to pass firewalls.

- When the majority of the more interesting content becomes accessible over IPv6, the internet service providers will stop providing access to IPv4 client content that only has IPv6 addresses (5 years or more). By then, the companies that are not already providing their content in both environments (IPv6 and IPv4) will have serious difficulties. We must be aware that the internet competition is ruthless and the web site visitors extremely impatient. If they are unable to obtain the content where they expect to find it, they will turn to alternative content and a new service provider with just a few clicks.

- In the final stage (which we will probably achieve no sooner than in the next decade), some content on the internet will be accessible only over the IPv6 protocol. By then, the business users who have yet to implement the IPv6 protocol into their business environment will find themselves facing serious difficulties. Some of them will probably try avoiding the changes by using additional tricks such as using intermediate HTTP servers (that provide IPv4 clients with access to IPv6 content over the HTTP or HTTPS protocol). Because it can be expected that at that time (also due to the deployment of the IPv6 protocol and cancellation of address translation) more and more web services will use direct communication between clients, the use of intermediate HTTP servers will also significantly limit communication options of such companies and decrease their competitiveness.

Note: Considering the fact that just a few years ago some Slovenian companies were still using the more than 30 years old SNA protocol and clients on a central IBM computer to access electronic mail, we can also expect similar behaviour (and delusions regarding the decreased competitiveness) in the future.

In contrast to the above mentioned turning points from the past (the introduction of Euro in 2000), the deployment of the IPv6 protocol faces another problem: there is no "turning date" after which the old Internet (which uses the IPv4 protocol) will stop functioning. Deploying new protocols due to a hypothetical, potential decline in future competitiveness and, above all, the deployment-related costs (work, equipment, education) (which are in no way hypothetical) will prove to be too much to handle for the management of many companies.

It is also important to mention that the majority of companies already has a network infrastructure that is at least partially ready for IPv6 deployment (it only has to be set up correctly). The majority of workstations already support IPv6 (at least those with Windows XP, Vista, Windows 7, MAx OSX or Linux operating systems), but many applications will never be mature enough to transition to the IPv6 environment – also because there are still issues of poorly documented applications, outdated development environments and lost source code.

So what actions can be taken? We should undoubtedly start with an extensive campaign of promoting the IPv6 protocol (similar to the campaign of transitioning to digital TV that is currently underway in Slovenia) that will target residential users as well as IT engineers and, above all, the management in companies. The professional association of managers should play a key role, since they generally (often also very evidently) take good care of their interests. Economic and business chambers whose purpose is to ensure the competitiveness of their members should also be included.

While increasing an interest in the IPv6 protocol and ensuring at least an initial understanding that neglecting the protocol will in the future lead to a loss of competitiveness, we must also provide easily accessible educational programmes that should serve to at least introduce the basics of the IPv6 protocol to the visitors in a few hours.

On 30 August 2010, the two-year 6Deploy Project concluded within the 7th framework research and development programme of the European Union. Its goal was to expand the basic knowledge and awareness of IPv6. Because the project proved to be an extremely successful way of delivering knowledge and raising public awareness, a decision was made to continue it (6Deploy2). We are aware that we should not interfere in the areas where Slovenian companies are commercially providing IPv6 training that in most cases are training courses provided by hardware manufacturers. Therefore, we propose to organise education under the auspices of the government according to the 6Deploy template: basic daylong workshops on innovations provided by IPv6 protocol. Participation at workshops could be free of charge for everyone and the workshops could be carried out in all Slovenian cities:

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

The financial construction and the costs for renting facilities, for food and lecturers will have to be taken care of. The government might have an interest in providing it. On the other hand, it could also be provided by companies from the industry that could use these events for the purposes of publicity, for example commercial IPv6 education providers who can offer the participants the option to continue the training in their programmes or providers of internet services who can thus acquire new clients.

There are several possibilities of financing the events. The government could finance the education of the citizens or the introductory IPv6 lectures could be sponsored by commercial providers.

The target public of these lectures could include system and network administrators in companies, heads of IT departments and other persons in charge who make decisions about technological guidelines and investments in the companies.

This way, we could raise the general public's basic awareness about the importance and innovations of IPv6 in a very short time.

The participating stakeholders can be various institutions and other entities that bring together certified 6Deploy lecturers. Additional information about the 6Deploy programme can be found at http://www.6deploy.eu/.

Raising Awareness in the State and Public Administration

Awareness should also be raised in the state and public administration, because we believe the awareness level is too low so far. This can currently not be done by making a public call, but it can be done through a simple discussion with the person responsible for projects and networks that will be subject to IPv6 deployment. For this purpose, it will be necessary to prepare special educational courses that will put a greater emphasis on requirements urgently needed for security and control of the state networks and services.

We propose an order is issued for IPv6 to be implemented into the entire network of the state and public administration and an analysis of the situation is ordered as part of the action plan. We propose that the tests of the fundamental parts of the network on IPv6 should be completed by the end of 2011, and the IPv6 protocol should be implemented into production by 2012. Online services of the e-administration could be provided in dual-stack by the end of 2011.

The competent ministry should prepare a national plan for the deployment of the new protocol for various industries and coordinate a schedule for interdisciplinary industries. The above areas should be included into the national strategy. Besides the impact of the content, publishing a strategic plan also has a very strong promotional effect. A strategic plan represents a small segment of a country's development strategy and a clear vision of the technological development of the entire country. The technological development of the entire country is an important factor in improving the competitiveness of the entire economy. If we miss the first period of publications of national strategies in Europe, the country or the competent ministry will be forced to prepare and publish a strategy under time pressure in order to maintain the present competitive level of the economy.

The current financial crisis is the right opportunity to raise the awareness of the public or the economy about what the new internet protocol provides:

- an opportunity to increase the competitiveness of the society,
- an analysis of effectiveness of the internal IT infrastructure,
- the possibility of correcting errors that occurred due to wrong decisions cause by internal and external factors.

The financial crisis is a time when the economy is ready to listen to outside ideas. The national strategy is an outside idea. With a proper unifying approach, it could be possible to link related companies with each other and create additional synergy of the Slovenian economy.

Raising the Awareness in General Public

According to unofficial information from the EU Member States that are already preparing national strategies for IPv6 deployment, the level of perception and awareness about the issue of IPv6 is in general relatively low, therefore some of them are already considering playing a more active role. At the head of these deliberations is Sweden, which recently assigned an important role to their regulator (Post-och Telestyrelsen – PTS, APEK in Slovenia). The PST has been given an important role in implementing DNSSEC; there are also ideas being entertained for the Swedish government to instruct the PTS to provide information and raise awareness about the problems and methods of deploying IPv6 in their country, which gives rise to a greater number of questions than answers.

The first message that is important here is that *EU Member States get actively involved in raising the awareness of their citizens and the industry and business world in general about the issues and traps awaiting us if IPv6 is not deployed in time*. *For this purpose, it is willing to support the role it assigned with financial resources, so that the project of raising awareness is* *carried out thoroughly and with equality, and most of all on a professional level.*

The regulator might be considered as relevant and qualified and has enough authority and reputation to raise awareness and to promote IPv6 deployment. Of course, before that, it is necessary to at least try and identify other movements, initiatives or bodies within the country that are engaged in this and determine whether they are doing their work well and fairly and maybe to also support their endeavours and work.

The stakeholders that could carry out a campaign of raising the awareness are the go6 Institute, Arnes, conference organisers (for example Telekomunikacije, Vitel, Palsit, Microsoft conference, INFOSEK, Poslovna Linux konferenca (business Linux conference), CIO conference, Informatika v javni upravi (Informatics in public administration)) and the infrastructural sector (the Chamber of Commerce and Industry of Slovenia - Združenje za informatiko in telekomunikacije (the Association of Informatics and Telecommunications)).

The Past Examples of Raising Awareness

We have been hearing for years that the IPv6 deployment should be encouraged via business opportunities and that the market will have to exert pressure so that IPv6 will be implemented into networks. But as the years go by, we are seeing that this prediction was wrong and that this wish will never come true in its entirety. Therefore, sometimes drastic measures have to be taken in raising the awareness of what can occur if we are caught unprepared for the exhaustion of the address space. The market and business will not exert any pressure for IPv6 to be implemented, because it is becoming increasingly clear that company managements only plan investments into visible results and fast profit within a single business cartel, which means that IPv6 has a long way before its time arrives. Whilst doing so, they are unaware that IPv6 deployment along with testing, technical preparations and staff education can take several years.

The business world is the hardest nut to crack when raising awareness, because managers who make decisions about the moves and investments of the company do not see the added value of the new protocol through the harsh business logic. In most cases, they also do not listen to the technical personnel in the company who are trying to make them understand why the upgrades are beneficial – the businessmen see that as expenses not as an investment.

A good mechanism of establishing a communications channel between a company's management and the technical personnel was discovered as a result of round tables at the 2nd and 3rd Slovenian IPv6 Summit in May 2010 almost by coincidence, and this mechanism or principle could be repeated more often with little cost. To the round tables (especially the round table at the 2nd Slovenian IPv6 Summit), we invited top representatives from the management of companies that in the near future will be directly involved in deploying IPv6 – representatives of internet service providers, operators, integrators, state institutions, content providers, regulators and most others. A requirement for attending the round table was an authorisation of an individual to give statements and to speak in public on behalf of their company. Because the initiator of the round tables was the Ministry of Higher Education, Science and Technology, only a few declined the invitation sent from the Ministry.

The issues at the round tables were varied. At one, we discussed the ideas that should be additionally included in the national IPv6 strategy; at another, we discussed the requirements for IPv6 functionalities in the equipment that is purchased via public tenders.

An event that is simple at first sight can have interesting background consequences. Up to that point, the company managers were mostly non-informed about the issues and the facts about IPv6, maybe because no one informed them, but even more probable is the explanation that they did not want to hear anything about it, did not find it important or did not have any time or patience to deal with it. Consequently, when making decisions in managing the company, they choose other investments and leave IPv6 implementation unaddressed. These employees have a completely false logic that someone will come to them when the time is right with a solution on a silver platter that will be cheaper, simpler and better than the one we have now. With such a low awareness of the IPv6 issue, they are surprised by an official invitation to a round table where they, together with other managers from other companies, should discuss what they expect from the national strategy, what would be good to include into it and what requirements for IPv6 functionality should be requested when purchasing the equipment. We believe that many were struck with panic and fear that their lack of knowledge and the ignorance of IPv6 as the protocol of the future, they would fall behind other participants at the round table, and mainly that they would appear unprepared in public.

What did this simple move set in motion? The managers called the technical staff to come to their office and to once again explain what IPv6 is, why the implementation is necessary, what will the company benefit from it and all else. Thus a communications channel was created between the company's management and the technical staff, and the management started listening to the technicians and the arguments about why investments into new protocols, education and allocation of their time and resources are necessary for IPv6 implementation.

APEK also additionally raised awareness about IPv6 when they sent all the operators a questionnaire about their readiness for IPv6, which the operators had to reply to under the legislation. APEK's questionnaire increased the managements' interest in the IPv6 protocol at the companies of the operators. The interest shown by APEK had an effect on the content of the operators' strategies and investment plans.

Additional Proposals for Raising Awareness on a Wider Scale in the Future

A similar tradition could be continued in the future, but at a higher level. The management that makes the decisions about the moves and investments is in most cases susceptible only to events that occur at a high business or at the state level. Our proposal for raising awareness in this field is for the Ministry of Higher Education, Science and Technology to organise a high-level round table (the Round hall in the Cankarjev dom cultural and congress centre is for example a suitable location) and invite general managers of all the largest operators, content providers, banks, insurance companies, the HKOM state network, the ZKOM health care network and other Slovenian companies for a discussion at the highest level where they can agree upon how to proceed, who will do what and, above all, when it will happen.

11. What Must the Public Administration Do to Adapt Access and Services for Citizens to the IPv6 Technology?

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

Proposals: organisation of the public administration according to the German model (LIR, de.government), acquiring the IPv4/IPv6 address space and allocation of resources within the public administration by hierarchy, a digital separation line and access to public services regardless of the way of access.

The issue of accessing the services of the public administration:
The Internet as an aggregate of interconnected networks that use the IPv protocol for routing and transfer has undoubtedly played a key role in developing the information society. If at the start of the 1990s we still primarily used telephones and faxes to exchange information in the business world, got the information on current events from the printed press and radio or TV and dealt with the state administration at municipalities or administrative units, today things are very different, because we can essentially no longer imagine a life without using e-mail or applications for instant messaging or extending our driving licence or submitting an income tax assessment without using e-administration services. If therefore we want to provide access to the above services to the widest range of users, the option of using must not be conditioned upon the selection of this or that terminal equipment, operating system or browser or a protocol that enables the routing of packets from the client to server. From this viewpoint, the implementation of IPv6 into the state administration does not differ significantly from implementation into any other content provider.

Establishing a Working Group and Preparing an Action Plan

It is probably unnecessary to emphasise that the network to which various state and quasi-government bodies in Slovenia are connected is very extensive and variegated, and the requirements of individual bodies connected to it are very varied. Implementing the IPv6 protocol into such a network is undoubtedly quite an organisational, technological and last but not least economic challenge. To better control the project implementation and above all to prevent uncontrolled growth of costs, we propose that a special working group be established that will be in charge of all activities related to implementing the IPv6 protocol into the HKOM network and suitable adaptation of e-administration services and coordination of outsourcers. Following the example of some other countries, the group should also to include representatives of the ministry that manages the HKOM network and representatives of its larger users. If the opinion of the majority of the members of the working group turns out to be that they do not have appropriate technical knowledge, renowned local and foreign experts from this field could also be included into the group. The action plan of IPv6 deployment, which should be prepared as the first in a set of operational documents, should contain accurate objectives of the implementation, deadlines and persons responsible for implementing individual tasks and an estimate of the costs of their execution.

Because the difference between implementing the IPv6 protocol into the public administration between Slovenia and some other EU Member States (e.g. France and Germany) is considerable, we also propose that the issue be included into the new strategy of the e-administration of the Republic of Slovenia, because it was not even mentioned in the strategy for the 2006-2010 period (e-uprava.gov.si/eud/e-uprava/sep2010_200406_1.doc).

Analysis of the Existing Situation

In order to enable the use of e-administration services to all internet users regardless of the internet protocol version used to access the internet, the working group should first conduct a careful analysis of the existing situation of individual information and communication systems. Hardware and software included in the analysis could for example be divided into the following groups:

- network structure – switches, content switches and routers,
- server infrastructure – mail, web, name, application and data servers, directories,
- security mechanisms – firewalls, intrusion prevention systems, VPN concentrators, SIEM systems.

During the analysis, each one should also include the following as criteria:

- a degree of support for the individual IPv6 protocol functionality (e.g. for routers, the most important being the option of static and dynamic routing, less important being the option of controlling them by using the IPv6 protocol,
- importance of individual functionality for the operation of the service as a whole (today, access to many services can for example be turned on with a simple adjustment of a web server that represents the first level of application architecture in web applications,
- an estimate of the complexity or costs for its adaptation.

Preparing the IPv6 Protocol Implementation

The key goal of the working group should without a doubt be the preparation of the strategy for implementing the IPv6 protocol into the state administration. The working group should take into account the results of the analysis of the existing situation when preparing the strategy. The strategy should clearly define the goals of implementing the IPv6 protocol into the individual segment of the network, together with deadlines and persons responsible for its implementation.
It is urgent that the strategy of implementing the IPv6 protocol into state administration, which should especially emphasise the possible pitfalls of the implementation and related risks, is in line with the national strategy and should not contain only the adaptation of applications that make the operation of e-administration possible, but should take into account all the aspects of IPv6 implementation.

Carrying Out the Education of Administrators and Verification of Solutions

Past experience with implementing the IPv6 protocol at access providers and in business environments has shown that technological as well as economic risks of the implementation can be significantly reduced by suitably educating the administrators. In order to reduce the resources needed to prepare and educate network and system administrators and architects, we propose that the possibilities of using alternative educational methods should be studied within the strategy of IPv6 protocol implementation, primarily e-educational programmes and the inclusion of the appropriate content into existing internal educational programmes.

Most applications that make it possible for the e-administration service to function have to first and foremost be reliable and ensure the safety of operation. In order to continue to ensure this after the implementation of the IPv6 protocol, we propose a verification of all the proposed solutions in a test bed, while envisaging for every test in advance what the expected results are and estimating the possible deviations in terms of the importance of every individual application. The test bed where the verification of the proposed solutions should take place should be completely separate from the live environment.

Acquiring and Allocating the Address Space

The first step in the actual implementation of the IPv6 protocol into the public administration is most likely concluding the agreement on the method of acquiring and allocating the address space. Because it is hard to imagine that the address space in the HKOM network is not already being managed in a centralised fashion, we propose to continue the existing practice in the future, because this will be the only way to avoid the increase of the costs of managing the network. During the allocation of the address space to individual countries and quasi-government bodies, it would be good to use the experience acquired in allocating the address space in the research and academic network Arnes, which the state administration uses as the internet access provider.

Gradual Implementation of the IPv6 Protocol into the Network

One of the basic criteria when selecting the appropriate method of implementing the IPv6 protocol into an individual business environment is the estimation of the effect that the change will have on the reliability and the security of operation. If, for example, we consider a backbone network whose key role is as fast and as reliable as possible transfer of traffic between individual locations, then it first has to be studied if the use of the IPv6 protocol in this case will be compatible with MPLS technology and the

OSPF and BGP protocols or if the use of the IPv6 protocol will have any consequences for its capability. Data from some network equipment manufacturers (e.g. http://www.cisco.com/web/-strategy/docs/gov/IPv6perf_wp1f.pdf) show that the bandwidths of IPv4 and IPv6 network equipment can vary significantly. On the other hand, the implementation of the IPv6 protocols into other parts of the network, the access network or DMZ segments can be problematic from the perspective of supporting hardware and the suitable secure handling of the IPv6 traffic.

However, the implementation of the IPv6 protocol into public server segments can also have a significant impact in the expert and the layman public, since this way (at least viewed from the outside) it is possible to show technological advancement and to encourage other providers to implement IPv6. One of the biggest pitfalls that individual organisations are exposed to in this way is security related. Because the servers in this case are public, the reliability of the operation of all used security mechanisms should be carefully examined before making the decision. Especially in the case of the e-administration service, we cannot afford having the security of using the IPv6 protocol being lower than when using the IPv4 protocol.

About the Authors

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

Urban Kunc is an employee of the Post and Electronic Communications Agency of the Republic of Slovenia (APEK) and is very active in the field of IPv6, both during his work and in his spare time. He prepared a survey about the implementation of IPv6 that APEK sent to the operators. He is the author of APEK's 76 page-long recommendation regarding the transition to IPv6. In general, he is very good at covering and understanding the areas related to regulations and the state in terms of IPv6 issues. Urban is also a member of the go6 Institute's Expert Council as the representative of APEK.

Ivan Pepelnjak (CCIE#1354) is employed as the head of technical advisers at NIL Data Communications (and is also a co-owner). His areas of expertise are networks and IPv6 implementation into various network environments. He has been designing and installing large data networks and writing books on advanced technologies since 1990. Ivan shares his experience and knowledge over the ioshints.info portal where he writes about IPv6; he is also a regular lecturer at Slovenian IPv meetings.

Janez Sterle is an employee of the Laboratory for Telecommunications at the Faculty of Electrical Engineering (LTFE), which is also go6 Institute's strategic partner. At his courses and educational programmes, Janez lectures about IPv6. The range of his work in IPv6 is very extensive and his primary areas of expertise are education and laboratory work/testing. Janez is also a member of the go6 Institute's Expert Council as the representative of LTFE.

Matjaž Straus Istenič is employed at Arnes, where his work and tasks are related to network maintenance and design. He is a great expert in IPv6 in a very broad sense; his primary areas of expertise are networks and the social aspect of deploying IPv6. He is the chief initiator and activist for deploying IPv6 at Arnes and is at the same time a member of the go6 Institute's Expert Council as the representative of Arnes.

Andrej Kobal is employed at Astec and has been engaged with IPv6 for a number of years. His areas of expertise in IPv6 are network and service security and the implementation of new protocols into public administration. Astec namely primarily provides administration and maintenance of HKOM, an extensive network of the Ministry of Public Administration. Besides the above, he also specialises in the field of IPv6 education; he namely lectures at Astec's IPv6 boot-camp.

Simeon Lisec is employed at Telekom Slovenije and is the head of IPv6 deployment for the entire Telekom Group. His IPv6 expertise includes the areas of ISP, standardisation, business processes, content and education providers. Simeon is an active leader of the Slovenian IPv6 working group and thus also a member of the go6 Institute's Expert Council.

Olaf Maennel is a professor at the Loughborough University, UK. Before that, he was employed at the Deutsche Telekom Lab where he was working on configuration management and network virtualization problems. His speciality is dynamic routing protocols, and network modelling. Olaf has been involved with the A+P RFC proposal that provides a mechanism for sharing the public IPv4 protocol between several user devices on the principle of port sharing. Olaf's speciality in IPv6 is a very wide view of the international development in this area. His contribution to this document was to provide an insight and a commentary to our thoughts from an outside, international standpoint. More about Olaf can be found at http://maennel.net/.

Jan Žorž - cofounder of the go6 Institute, president of the go6 Institute's Expert Council and lecturer on IPv6 issues all around the world. He is the initiator of the movement for the deployment of IPv6 in Slovenia and the head of the idea of establishing the go6 platform. He is also responsible for bringing together the state, the regulator, the industry and the civil society in joint campaigns for raising the awareness of IPv6 issues and deployment. More: http://www.pragma.si/resume/index.html.