Book #2
JULY 2015

EU-China FIRE

EU-CHINA FUTURE INTERNET COMMON ACTIVITIES AND OPPORTUNITIES

IPv6
BEST PRACTICES

EU-China FIRE is a EU-funded FP7 project, lasting two years (2013-2015), to strenghten EU-China cooperation on IPv6 and Future Internet Research and Experimentation (FIRE) activities

MARTEL Consulting
SIGMAORIONIS
UNIVERSITÉ DU LUXEMBOURG
CAICT 中国信息通信研究院
Beijing internet institute 天地互连
Ruijie Networks

EU-China FIRE : IPv6 Best Practices

EU-China FIRE

Project Acronym: ECIAO
Project Full Title: EU-CHINA future Internet common Activities and Opportunities
Grant Agreement: 610418
Project Duration: 24 months (August 2013 - July 2015)

D3.1v2: IPv6 Best Practices

Deliverable Status: Final
File Name: ECIAO_D3.1v2-final.pdf
Due Date: M24
Submission Date: M24
Dissemination Level: Public
Author: UL (Latif Ladid latif.ladid@uni.lu);
BII (Davey Song @biigroup.cn), IPv6 Expert Group members

Martel GMBH
Switzerland

Easy Global Market SAS
France

Sigma Orionis SA
France

Université du Luxembourg
Luxembourg

China Academy of Telecommunication Research of Ministry of Information Industry
China

Fujian Ruijie Networks CO LTD
China

BII Group Holdings LTD
China

Table of contents

Introduction

2015 seems to be another inflection year with the ARIN announcement of its full exhaustion of the North American IPv4 address pool in July 2015. IPv6 deployment seems to pick up new steam moving forward consistently as the IPv4 address space is getting scarcer at the Telecom and ISPs levels beyond the Registries levels with some countries achieving as of July 11th more than 20% user penetration with Belgium (42.7%), USA (27%), Switzerland (26.5%) and Germany (21%) ranking at the top (http://labs.apnic.net/dists/v6dcc.html).

Over 140 million users are accessing Internet over IPv6 and are probably not aware of it. The US remains by far the biggest adopter of IPv6 by tripling its figure from 20 million users in July 2014 to some 78 million users followed by Germany, Japan and China with over 10 million users. Many IPv6 emerging countries have crossed the 1 million bar mark namely India, Brazil, Peru, Malaysia and Saudi Arabia. Some stagnant countries which are leaders in IPv4 have some catch-up to do namely Great Britain, Netherlands, Canada, Australia, Spain, Russia and Italy. Overall, Europe is still leading the IPv6 deployment making the strategic and good will case for it, re-enforced now by the US which drives everyone else in this global collaborative effort similar to what happened to IPv4 deployment in the 90s.

Many Autonomous Networks (ASN) reach more than 50% with IPv6 preferred or IPv6 capable penetration: (http://labs.apnic.net/ipv6-measurement/Economies/US/).

Worldwide IPv6 access to Google has passed 6% usage still showing the hockey-stick curve (http://www.google.com/intl/en/ipv6/statistics.html).

If this trend continues, the APNIC statistics show that we should achieve 50% IPv6 capable penetration by 2017 which would be another inflection point when the full roll-out of IPv6 becomes a strategic plumbing decision for all networks, a topic that is avoided so far due to many strategic and resource issues (lack of top awareness and management decision-making, lack of IPv6 skilled engineers and IPv6 operational and deployment best practices, very limited ISP IPv6 access deployment, and vendor push..).

The deployment of Carrier Grade NAT is in full swing making networking and the user experience more brittle than ever which could become another driver to return to simplicity in view of the emerging technologies such as SDN and NFV, which today makes a total abstraction of the IP layer, another sanity check down the road. The security and cybersecurity issues are always brushed over at this stage due mainly to the lack of IPv6 security skills. New topics are more in the limelight such as Cloud Computing, Internet of Things, SDN, NFV, Fog Computing and 5G. However, these fields are taking IP networking for granted by designing them on IPv4/NAT, building non-scalable and non-end to end solutions. The ECIAO project is driving new initiatives to garner support and create awareness and best practices on the impact of IPv6 on topics such as Cloud Computing, IoT, SDN-NFV and 5G through the ETSI IPv6 Industry Specification Group (IP6 ISG) defining best practices and deployment guidelines with use cases and success stories.

1 • IPv6 Roadmap

The Internet has shown its incredible potential as a unique economic enabler. The ability to build networks between people, groups, data, and things – the all-embracing Internet of the Future will in the next 10 years, generate a value exceeding USD 14.4 trillion, touching all sectors of the economy. A world linked together by the "Internet of Everything" will turn raw information into knowledge, creativity into practical innovation, and facts into greater relevance than ever before, providing richer experiences and a more sustainable global economy.

We are not, however, there quite yet. Currently, 99.4 per cent of physical objects that may one day be part of the "Internet of Everything" are still unconnected. Moreover, large areas of the world remain unserved or underserved by Internet connections. Meanwhile, recent technological developments in cloud computing, wireless networks, so-called "Big Data", high-performance computing, processing power, sensor miniaturisation, and many others, translate into a digital data universe that is increasing exponentially. The ability to economically extract value from this universe will offer unprecedented opportunities for welcome progress – if there is sufficient ability to connect to the growing Internet.

One of the key technologies that can enable this progress is the new Internet Protocol version 6 (IPv6). This new iteration of the IP protocol stands poised to push the boundaries of the Internet beyond what is now possible with the current version, IPv4. Moreover, IPv4 addresses are quite simply running out. IPv6 will allow users to get the most value from the "Internet of Everything", and it will enable greater connection of underserved communities and countries. Yet today, there are significant market, business, and technical challenges in making the transition from IPv4 to IPv6. The world stands poised for a great leap over those challenges and toward the possibilities of an unbounded new Internet.

This roadmap explores the transition process and suggests ways to build momentum for IPv6 around the world. **Section 1** explores some of the transition challenges, which include establishing a valuable business case and accounting for transition costs. **Sections 2 and 3** first explore the current status of IPv4 and the progress of transition to IPv6. It then seeks to break down the technical and economic factors, including costs that may be impeding transition. **Section 4** then explores how governments, standards bodies, and international organisations can help foster the conditions to promote the take-up of IPv6 technology.

Section 5 outlines the best practices of IPv6 deployment in governments and **Section 6** informs about the recently launched ETSI Industry Specification Group dealing with IPv6 integration in the key Future Internet technologies.

Section 7 outlines how the enterprise world could deploy IPv6, an area to watch carefully as we have very limited released information about enterprises that have deployed IPv6 and **Section 8** looks at the important emerging integration of 5G and IPv6. Finally, **Section 9** concludes with a summary of actions and the way forward.

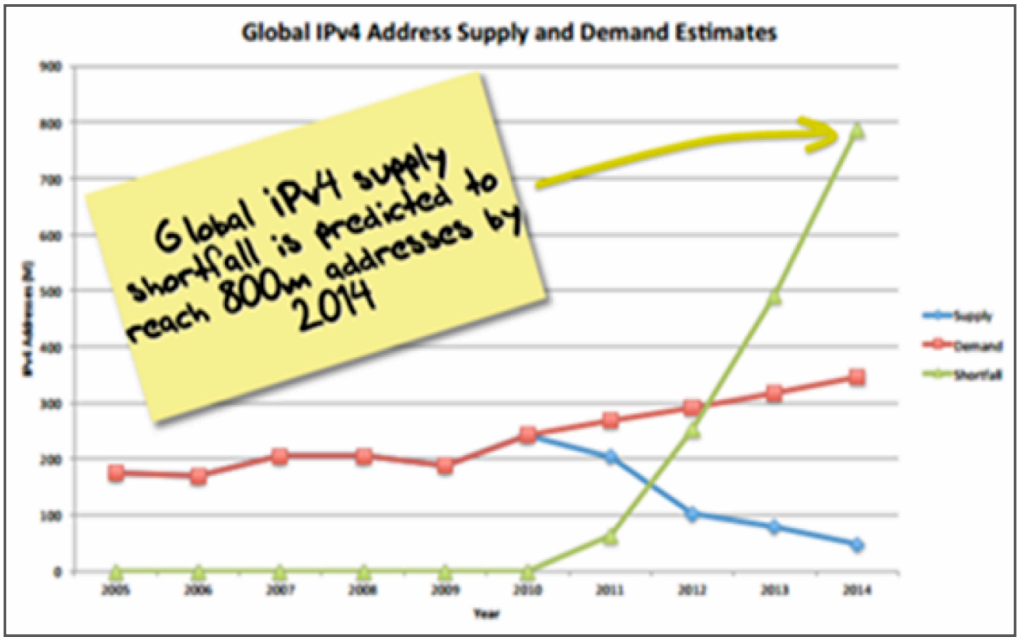


Figure 1: Coping with Demand for Internet Addresses (Source: Geoff Huston, APNIC)

Perhaps the threshold question to address in explaining the transition from IPv4 to IPv6 is "why?" make the transition to IPv6:

- The costs entailed in IPv6 adoption;
- The main roadblocks/challenges in deploying and transitioning to IPv6, such as a lack of business incentives or consumer awareness, as well as technical incompatibility and security issues;
- The existing policies, regulatory measures and guidelines developed to support the transition from IPv4 to IPv6;
- The best practices and recommendations that can encourage, facilitate and support a swifter adoption of IPv6;
- Potential innovative steps that policy-makers could take to accelerate or facilitate IPv6 deployment; and
- Measures already taken by the ITU, industry, and governments to promote awareness of the criticality of IPv6 deployment.

The following sections lay the groundwork for considering these issues by surveying the current status of IPv4 address deployment and the nascent transition to IPv6 as it stands today.

1. Status of IPv4: Preparing for the 'IPocalypse'

At full deployment, the total number of IPv4 addresses that can be used from the 32-bit address space is 3.7 billion. At the outset, then, it becomes apparent that, in a world with more than 7 billion people, the existing addressing system inevitably will be tethered by a short leash on the way to the "Internet of Everything".

Moreover, the IP address system was not originally designed to distribute addresses by country. Rather, addresses were assigned to networks as they were built (on a need-basis), giving a lion's share to the earliest networks and users. These were mostly within the U.S., which continues to have 42 per cent of IPv4 addresses. Asia now has around 20 per cent, which is far better than the 9 per cent it had back in 2000[1].

Depletion of IPv4 Address Space

The number of IPv4 addresses available from the central, global Internet Assigned Numbers Authority (IANA[2]) registry is not simply low – it has been completely depleted as of 3rd February 2011. The remaining unclaimed IPv4 addresses are now in the care of Regional Internet Registries (RIRs), which have the task of distributing them in their regions. The Internet community has predicted this address exhaustion and did not wait until the end in order to sound the bells for deployment of IPv6. This gave the Internet community, ISPs, and enterprise users alike enough time to better prepare for this transition. For example, The RIPE community established its IPv6 Working Group in 1997. At that time several industry partners, together with national research networks and other stakeholders already established a first IPv6 operational network, called 6BONE, which was used to test IPv6 implementations and gain operational experience. Several of the RIRs, including APNIC and the RIPE NCC, have also been delivering IPv6 training courses to their members for many years.

As time goes on, the depletion situation grows worse. The global IPv4 supply shortfall is predicted to reach 800 million IP addresses by 2014, according to Geoff Huston, Chief Scientist at APNIC, the Asian RIR[3]. APNIC and RIPE NCC have exhausted the addresses provided to them by IANA since 15th April 2011 and 14th September 2012, respectively. The North and South American RIR will be depleted by mid-2014. Meanwhile, the yearly demand is increasing from 300 million to 350 million annually just for the baseline ISP consumption to keep the normal growth of the Internet going. These numbers do not take into account the new needs for emerging IP-based services like the "Internet of Things," Smart GRID efforts, and Smart Cities, to name just a few.

How bad is the exhaustion situation? Well, the remaining address space among all five of the regional registries is about 5 blocks of 16 million IP addresses, which is a total of 84 million. North America has only 2.5 blocks left. It is abundantly clear that the world is facing an impending "IPocalypse", and the only solution at hand designed by the Internet Engineering Task Force (IETF[4]) over the past two decades to cater for the growth and the scalability of Internet addressing is IPv6. The big shift to IPv6 will happen by default.

Increasingly, IPv4 addresses are kept viable only by the use of a stop-gap solution: the extension of Network Address Translation (NAT) to the carrier level – a technique called Carrier Grade NAT (CGN) which is currently in deployment on a large scale. CGN is basically implementing NAT at the carrier network and will not share a single IP address per many users but rather certain ports among the same users will be shared. The Internet experience will be dramatically reduced because it will not be able to get even one global IP address to link the NAT to the Internet. The end-user will get just a certain number of ports. Applications like Google maps might need up to 250 ports; anything less than that will make the map patchy or of poor quality.

Figure 2 illustrates the exhaustion of IPv4 addresses as it plays out across the central (IANA) and regional (RIR) registries. The first (left) counter shows that the central pool has fully assigned its 256 IP blocks. The second (right) counter shows the remaining IP blocks per region at the registry level. Each block contains 16 million IP addresses. The RIR policy is that when the RIR reaches the last IP block, it will only assign 1,024 IP addresses, and only to those entities that will deploy IPv6 -- at least for now in Asia and Europe.

[1] Latif Ladid – stats from year 2000.
[2] IANA is the department of ICANN, a nonprofit private US corporation, which oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. See http://www.iana.org/about
[3] APNIC (Asia Pacific Registry www.apinic.net)
[4] IETF: http://www.ietf.org/

The Remaining IPv4 Address Space

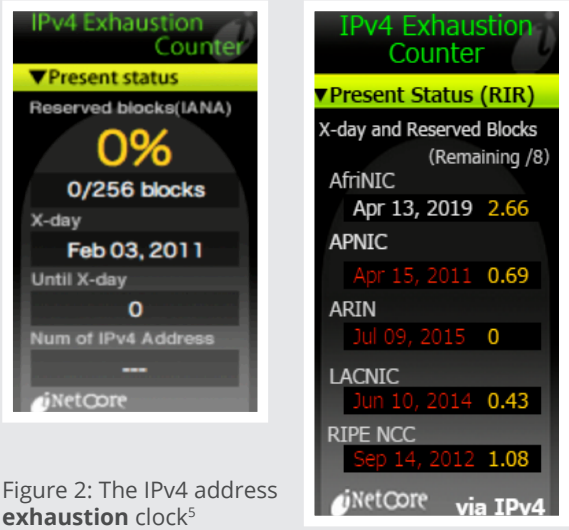


Figure 2: The IPv4 address **exhaustion** clock[5]

By linking to the website for BGP (Border Gateway Protocol)[6], one can view the number of IP addresses assigned to networks in every country of the world. The numbers are generated from information published by the RIRs (AFRINIC for Africa, APNIC for Asia, ARIN for North America, LACNIC Latin America, and the Caribbean, and RIPE NCC for Europe, Middle East and parts of Central Asia) on their FTP servers as of 6th of July 2015.

Total number of IPv4 addresses:

2^32:	4294967296	4294.97 million
Class D+E:	536870912	536.87 million
Nets 0 and 127:	33554432	33.55 million
RFC 1918:	17891328	17.89 million
Usable:	3706650624	3706.65 million

The list of the countries shows certain historical disparities in the assignment of the address space. The introduction of the registries has compensated to a certain extent in the past 20 years, helping contribute to a more balanced distribution of the IP addresses (though always on a need basis) and the promotion of balanced Internet policies through a bottom-up, community-defined consensus. Obviously, the need for 800 million IP addresses by 2014 and 2015 to sustain the growth of the Internet as a global force remains a critical issue to resolve. The only solutions are promoting IPv6 and training the community in good use of the remaining IPv4 address space during the transition period.

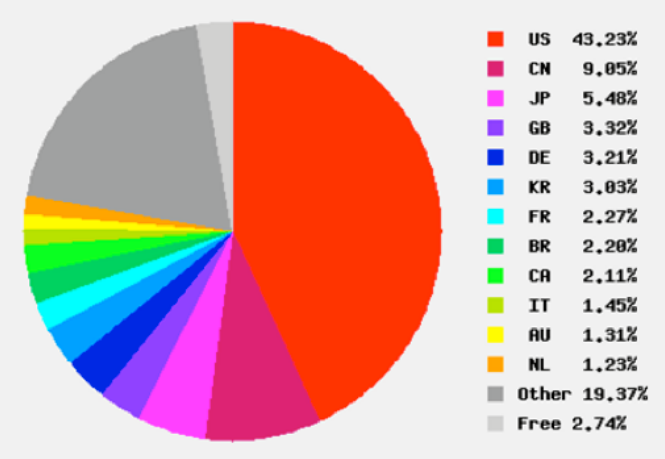


Figure 3: Distribution of IPv4 Address Space Worldwide (Source: BGP Expert)

[5] Source: Netcore: http://inetcore.com/project/ipv4ec/index_en.html
[6] BGP Expert (http://www.bgpexpert.com/addressespercountry.php)

2 • Current Deployment of IPv6

If we are in the middle of the IPocalypse, are we making any progress at deploying IPv6 addresses? Industry statistics show that, in fact, IPv6 is entering the market at a respectable pace. But will it be enough to meet the demand for Internet growth?

1. Growth of the IPv6 Connections

A chart found on the website of the Internet research organisation CAIDA[7] shows that the number of IPv6 connections is increasing constantly worldwide. Europe leads with over 50 per cent of the network connections, while there is also a strong showing in Asia, as well. A comparison of the densely connected IPv4 universe to the IPv6 world demonstrates the high IPv6 readiness of the non-US based networks and the possible balancing factor of IPv6 services in the future. Google, meanwhile, measures continuously the availability of IPv6 access among Google users. The graph in Figure 4 shows the percentage of users accessing Google via IPv6[8].

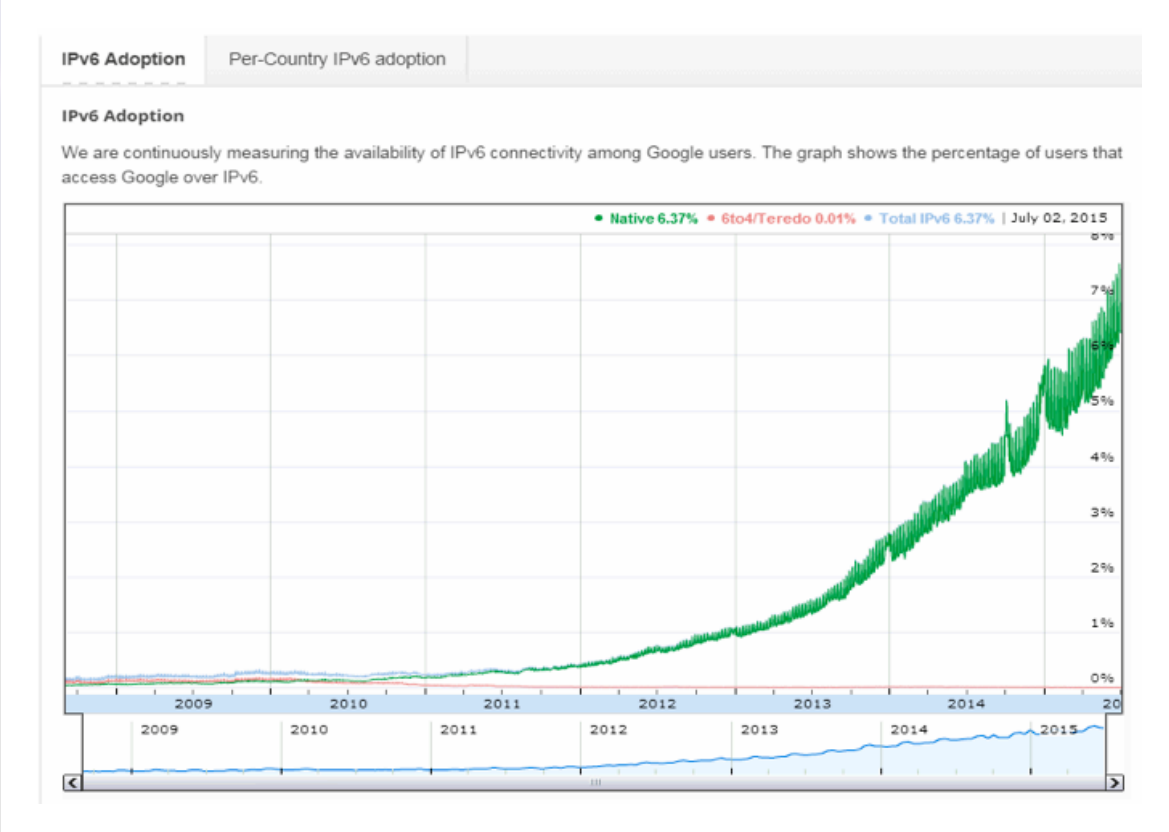


Figure 4: Google IPv6 Users[9]

[7] http://www.caida.org/research/topology/as_core_network/pics/ascore-2011-apr-ipv4v6-standalone-1600x876.png
[8] "Native" refers to equipment with IPv6 capability, in contrast with "dual stack" equipment that combines IPv6 technology with IPv4 capabilities.
[9] Source Google: http://www.google.com/ipv6/statistics.html

Google data shows that some 6.4% of the users are accessing Google over IPv6, with an exponential trend since 2012.
The following charts and analysis from Geoff Huston at APNIC show that Europe is leading the IPv6 user chart while China shows some 6.3 million users not yet reaching 1% as of June 2015.

Index	Country	Internet Users	V6 Use ratio	V6 Users (Est)	Population
1	Belgium	9201276	42.92%	3949413	11193767
2	United States of America	282614477	26.57%	75098550	325218041
3	Switzerland	7145544	26.01%	1858480	8241689
4	Germany	71167014	21.11%	15020613	82560342
5	Peru	12993754	17.58%	2283880	31160083
6	Luxembourg	510337	16.45%	83940	544070
7	Portugal	6591529	14.06%	926465	10614380
8	Norway	4886378	10.62%	518928	5143556
9	Japan	109380868	10.36%	11326591	126891959
10	Greece	6667800	10.24%	682712	11131554
11	Malaysia	20555709	9.76%	2006216	30680163
12	Czech Republic	7992399	9.59%	766455	10785964
13	Estonia	1024068	8.97%	91827	1280085
14	Romania	10748476	8.09%	869787	21583287
15	Finland	4998071	7.56%	378067	5462373
16	Singapore	4109731	7.30%	299967	5629769
17	France	54143952	6.32%	3421343	64998742
18	Ecuador	12566714	5.27%	662590	16236065
19	Austria	6897868	4.81%	331730	8558150
20	Bolivia	4355868	4.40%	191691	11027515
21	Saudi Arabia	19716043	3.98%	784734	29918123
22	Netherlands	15838065	3.96%	626591	16849006
23	Ireland	3704121	3.17%	117579	4730679
24	Bosnia and Herzegovina	2593405	2.78%	72153	3819449
25	Sweden	9190710	2.60%	239352	9694842
26	Australia	20806983	2.36%	490411	23943594
27	Brazil	110439897	2.22%	2450748	203763648
28	Hungary	7196392	1.36%	97603	9912386
29	New Zealand	3982072	1.34%	53399	4598236
30	Bhutan	232590	1.26%	2930	777896
31	Canada	33981006	1.24%	421241	35882795
32	China	668901220	0.94%	6302554	1402308638
33	Poland	24846367	0.90%	224327	38225180
34	Bulgaria	3776847	0.86%	32544	7112707
35	Russian Federation	87286773	0.73%	636876	142160869
36	India	252795481	0.73%	1838770	1283225795
37	Taiwan	18751419	0.71%	133366	23439274

Figure 5: APNIC IPv6 users by country

The IPv6 picture in Belgium is impressive, where almost one half of the users in Belgium are now IPv6 capable. Similarly, the picture in the United States appears to be radically different from that of a year ago, with almost one quarter of US users now on IPv6. Today some 30 countries now have IPv6 deployment rates in excess of 1%. The full extent of the recent moves in the United States by Comcast, Verizon, T-Mobile, AT&T, and Time Warner Cable in IPv6 are very impressive. When coupled with the efforts in Germany by Deutsche Telekom and Kabel Deutschland and KDDI in Japan then the IPv6 results in these top three IPv6 countries outnumber all the others.

Country	Internet Users	V6 Use ratio	V6 Users (Est)	Population
Americas	645043025	12.87%	83017439	991821843
Europe	528043780	5.95%	31423508	743533824
Asia	1565961282	1.46%	22903270	4388155220
Africa	297947062	0.08%	223416	1167040514
Oceania	26302864	2.01%	528687	39397499
World	3063298095	4.51%	138245886	7330037254

Figure 6: APNIC IPv6 users by Registry Continents

First, the statistics look different in 2015 as the number of worldwide Internet users has been updated from 2.3 billion users to 3.06 billion which has an impact on the percentage of IPv6 users going down from almost 9% in July 2014 to 4.5%. The massive jump in the US (23.5%) shows a 12.87 % IPv6 users in the Americas with Europe about half of that total and Asia obviously less than half of Europe. Africa is in a serious need of a better promotion and adoption strategy despite the very good work of AFRINIC's core experts however, Africa with very limited resources is the largest continent with some 54 countries.

Rank	ASN	AS Name	CC	%Total Value	Cum	% V6 Value	Cum
1	**AS7922**	**COMCAST-7922 - Comcast Cable Communications, Inc.**	**US**	**6**	**6**	**29**	**29**
2	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	4	10	0	29
3	**AS7018**	**ATT-INTERNET4 - ATT Services, Inc.**	**US**	**3**	**13**	**25**	**54**
4	AS4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	CN	3	16	0	54
5	AS4713	OCN NTT Communications Corporation	JP	2	18	0	55
6	**AS3320**	**DTAG Deutsche Telekom AG**	**DE**	**2**	**21**	**8**	**63**
7	AS701	UUNET - Verizon Business	US	2	23	0	63
8	AS3215	AS3215 Orange S.A.	FR	2	24	0	63
9	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.	US	1	26	0	63
10	**AS12322**	**PROXAD Free SAS**	**FR**	**1**	**27**	**3**	**65**
11	AS5089	NTL Virgin Media Limited	GB	1	28	0	65
12	**AS2516**	**KDDI KDDI CORPORATION**	**JP**	**1**	**29**	**6**	**71**
13	AS20115	CHARTER-NET-HKY-NC - Charter Communications	US	1	30	0	71
14	AS2856	BT-UK-AS BT Public Internet Service	GB	1	31	0	71
15	AS3269	ASN-IBSNAZ Telecom Italia S.p.a.	IT	1	32	0	71
16	AS1221	ASN-TELSTRA Telstra Pty Ltd	AU	1	33	0	72
17	**AS17676**	**GIGAINFRA Softbank BB Corp.**	**JP**	**1**	**34**	**1**	**73**
18	AS5607	BSKYB-BROADBAND-AS Sky UK Limited	GB	1	35	0	73
19	AS209	CENTURYLINK-US-LEGACY-QWEST - Qwest	US	1	35	0	73
20	AS3352	TELEFONICADEESPANA TELEFONICA DE ESPANA	ES	1	36	0	73
21	AS8151	Uninet S.A. de C.V.	MX	1	37	0	73
22	AS3209	VODANET Vodafone GmbH	DE	1	38	0	73
23	**AS20001**	**ROADRUNNER-WEST - Time Warner Cable Internet LLC**	**US**	**1**	**39**	**3**	**75**
24	AS15557	LDCOMNET Societe Francaise du Radiotelephone S.A	FR	1	39	0	76
25	AS5384	EMIRATES-INTERNET Emirates Telecommunications	AE	1	40	0	76
26	AS6128	CABLE-NET-1 - Cablevision Systems Corp.	US	1	41	0	76
27	**AS10796**	**SCRR-10796 - Time Warner Cable Internet LLC**	**US**	**1**	**41**	**1**	**77**
28	AS6830	LGI-UPC Liberty Global Operations B.V.	AT	1	42	0	77
29	AS3549	LVLT-3549 - Level 3 Communications, Inc.	US	1	43	0	77
30	**AS3303**	**SWISSCOM Swisscom (Switzerland) Ltd**	**CH**	**1**	**43**	**2**	**79**

Figure 7: Top 30 Access Providers by "network value"

Geoff Huston remarked that Figure 7 is an interesting table in a number of ways. The first is the extent of aggregation in the access business in which just 30 access providers control some 43% of the total value of the Internet's access business. The second observation is that almost one third of these access providers are actively deploying IPv6. And finally, these nine IPv6-enabled access providers (% v6 value is greater than 0 as shown in Figure 7) account for almost 80% of the total IPv6 value.

So who is deploying IPv6? The specialised technically adroit ISP enthusiasts or the largest mainstream ISPs on the Internet? Predominately, it's the latter that's now driving IPv6 deployment. And that's a new development.

For many years what we heard from the access provider sector was that they were unwilling to deploy IPv6 by themselves. They understood the network effect and were waiting to move on IPv6 when everyone else was also moving on it. They wanted to move altogether and were willing to wait until that could happen. But that was then and this is now. I would be interested to hear what today's excuse is for inaction from the same large scale access providers. Are they still waiting? If so, then whom are they using as their signal for action? If you were waiting for the world's largest ISP by value, then Comcast has already taken the decision and has almost one half of their customer base responding on IPv6 as shown in Figure 8. Similarly if you were waiting for Europe's largest ISP, then Deutsche Telkom has already embarked on its IPv6 deployment program. Overall, some 8% of the value of the Internet by this metric has now shifted to dual stack mode through their deployment of IPv6, and if just these nine IPv6-capable service providers were to fully convert their entire customer base to dual stack they would account for 16% of the total value of the Internet.

I'd like to think that the waiting is now over. I'd like to think that the balance of influence in the network is now shifting to a norm of services that embraces IPv6 in a dual stack service model. We'll keep measuring this in the coming months and keep you informed.

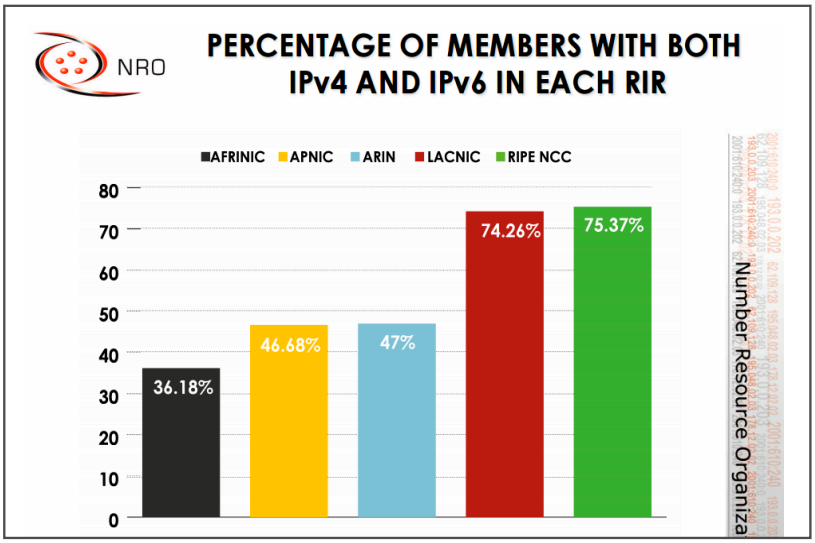
Meanwhile the reports of IPv6 deployment on a country by country basis and the level of detail of each individual network's progress with IPv6 are updated daily at http://stats.labs.apnic.net/ipv6.

The worldwide level of IPv6 adoption by ISPs reflects the fact that as of March 2015, 18,099 IPv6 prefixes have been allocated by the RIRs (Figure 9). Of those, 50% have been routed in the BGP table and 40% are alive on the routing table. This does not mean that the ISPs are offering IPv6 service. Only a few do, so far, but many have announced they are offering, or planning to offer, IPv6 service during 2015 due to the ARIN's full exhaustion of IPv4 address space.

Participating Network	ASN(s)	IPv6 deployment
Comcast	7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	34.51%
ATT	6389, 7018, 7132	52.42%
KDDI	2516	21.64%
Verizon Wireless	6167, 22394	68.73%
Time Warner Cable	7843, 10796, 11351, 11426, 11427, 12271, 20001	17.75%
Deutsche Telekom AG	3320	19.56%
T-Mobile USA	21928	46.69%
Free	12322	20.51%
Telefonica del Peru	6147	19.32%
Liberty Global	5089, 6830, 20825, 29562	5.04%
Telenet	6848	54.49%
SoftBank BB	17676	3.30%
Telekom Malaysia	4788	12.52%
Swisscom	3303	41.24%
Chubu Telecommunications	18126	42.47%
Belgacom	5432	21.72%
MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	3243	30.59%
RCS & RDS	8708	13.83%
OTE SA	6799	13.26%

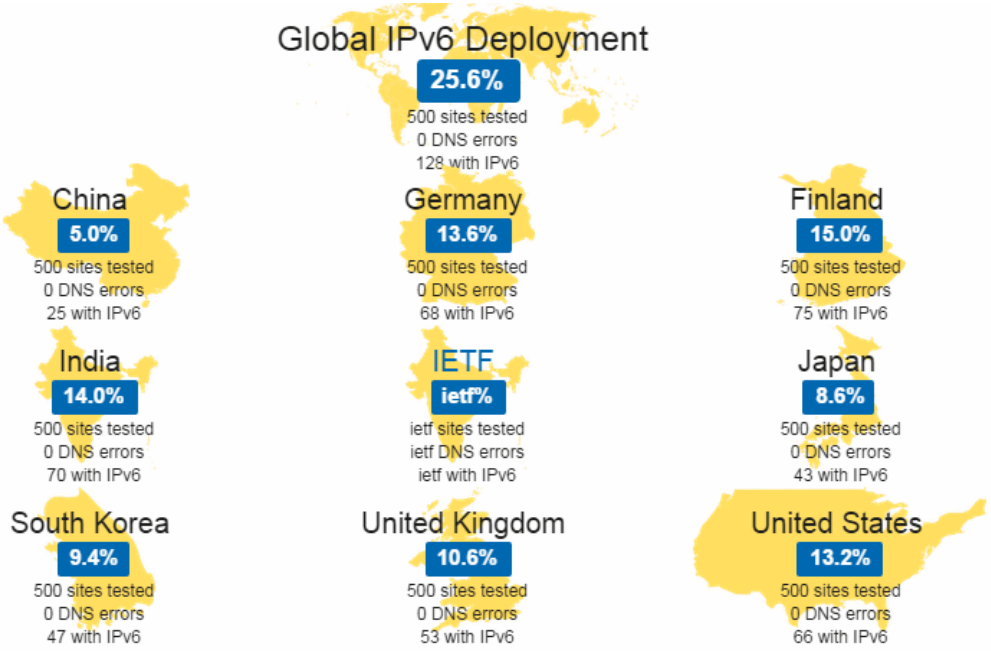
Figure 8: List of Fixed and Mobile operators showing IPv6 traffic (Source: http://www.worldipv6launch.org/measurements/)

Figure 9: IPv6 address assignment



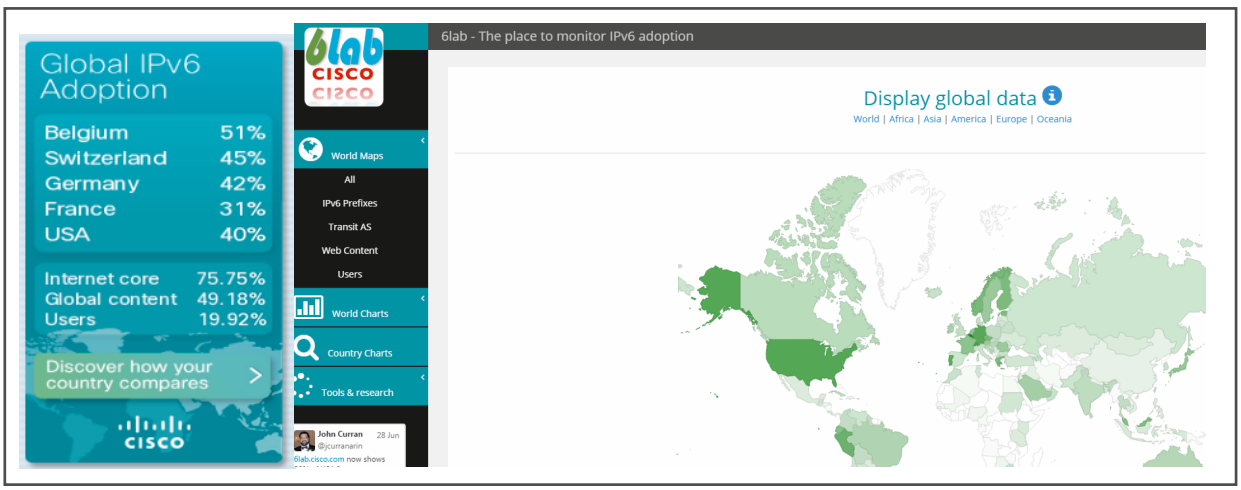
The top 500 websites have been tested for IPv6 connectivity, and 25.6% of them can be accessed by default over IPv6 (shown in Figure 10). These top 500 web sites produce 80 per cent of the world's hits and traffic; they are using IPv6 packets to send their content to the end-users accessing them via IPv6.

Figure 10: Performance Indicators: 500 Tested (Lars Eggert, IRTF Chair– IPv6 Deployment Trends – July 2015)



Cisco has calculated (Figure 11) that the global adoption of IPv6 in the Internet core backbone[10] has reached 59.16 per cent, with a global content penetration of 35.82 per cent. The user penetration, however, is growing but still very low at just 6.37 per cent. This is primarily due to the lack of IPv6 services offered by telecom and mobile operators.

Figure 11: Global IPv6 adoption (Source: Cisco: http://6lab.cisco.com/stats/)



[11] http://6lab.cisco.com/stats/

2. Worldwide Vendor Readiness

Back in 2004, the IPv6 Forum introduced a logo programme dubbed "IPv6 Ready". The goal was to create a worldwide interoperability scheme to urge vendors to accelerate adoption of IPv6 based on real, interoperable compliance testing and validation. Due to the complexity and worldwide scope of this task, a committee was formed to represent the breadth of interoperability labs from around the world: the Japanese TAHI team; the US-based UNH-IOL lab; the European-based IRISA/ETSI; the Taiwan, Republic of China TWINIC; and the Chinese BII lab. Their task was to collectively design the interoperability specifications and test scripts for worldwide execution. The adoption of this programme was an immediate success and vendors from around the world took the tests to check on their products (Figure 12).

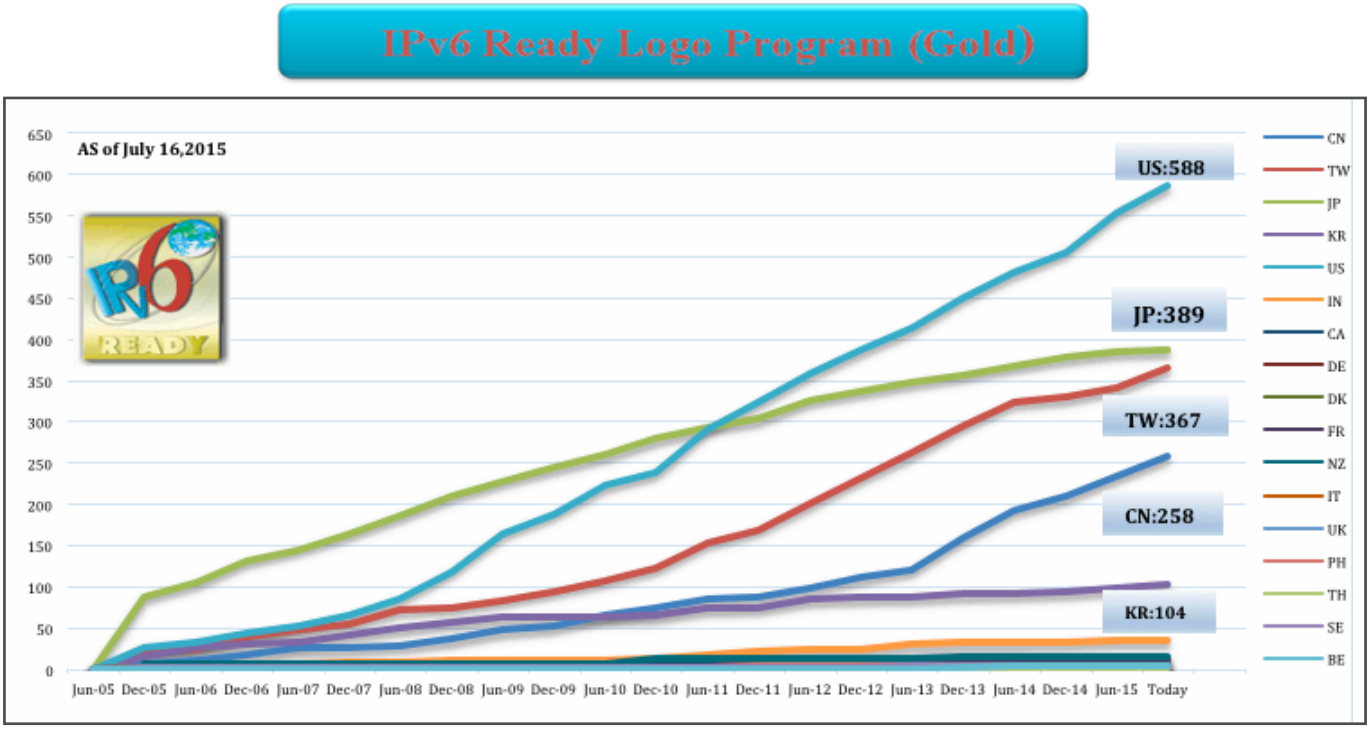


Figure 12: IPv6 Ready Logo Program (GOLD)

A large number of Asian vendors have adopted IPv6 in their routers and security solutions (IPsec). An important development to note is the entry of a large number of new vendors from China and Taiwan (Republic of China) and India, joining the large participation of U.S. and Japanese vendors. Remarkably, there is almost a non-existence of European vendors. The number of products certified as IPv6 ready is spread among vendors primarily from among the following countries:

- United States: from 233 in 2011 to 588 in July 2015
- Japan: from 122 to 389
- Taiwan, Republic of China: from 117 to 367
- China: from 67 to 258
- South Korea: from 6 to 104
- India: from 0 to 36
- Europe total: from 16 to 37

[11] http://www.ipv6forum.com/
[12] www.ipv6ready.org
[13] http://tahi.org/
[14] https://www.iol.unh.edu/services/testing/ipv6/
[15] http://www.irisa.fr/tipi/wiki/doku.php
[16] http://interop.ipv6.org.tw/
[17] http://www.biigroup.com/

Following Table 1 shows the evolution of the IPv6 Ready products by countries examined and successfully passed the tests:

M/Y-C	CN	TW	JP	KR	US	IN	CA	DE	DK	FR	NZ	IT	UK	PH	TH	SE	BE	IL	CZ	AT	AU	ES	FI	GB
Jun-05	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0						
Dec-05	7	23	89	17	28	3	1	1	1	1	8	0	0	0	0	2	0	0	0	0	0	0	0	0
Jun-06	10	26	106	28	33	4	1	2	2	1	8	0	0	1	0	2	0	0	0	1	0	0	0	0
Dec-06	17	41	133	31	44	8	2	2	2	2	8	0	0	1	0	2	0	0	0	1	0	0	0	0
Jun-07	25	49	147	33	53	8	4	2	2	2	8	0	0	1	0	2	0	0	0	1	0	0	0	0
Dec-07	26	57	166	43	66	9	4	3	2	2	8	0	0	1	0	2	0	0	0	1	0	0	0	0
Jun-08	29	73	188	51	87	9	4	3	2	2	8	0	0	1	0	2	0	0	0	1	0	0	0	0
Dec-08	36	76	212	58	120	11	4	3	2	2	8	1	0	1	1	3	0	0	0	1	0	0	0	0
Jun-09	47	85	230	64	166	11	4	3	2	3	8	1	0	1	2	3	0	0	0	1	0	0	0	0
Dec-09	52	96	246	65	190	11	4	3	2	3	8	1	0	1	2	3	0	0	0	1	0	0	0	0
Jun-10	65	109	261	65	224	13	4	3	2	3	8	1	0	1	2	3	0	0	0	1	0	0	0	0
Dec-10	73	124	281	66	240	14	4	3	2	3	13	1	1	2	2	3	0	0	0	1	0	0	0	0
Jun-11	86	155	295	75	293	19	4	4	2	3	13	1	1	3	2	3	0	0	0	1	0	0	0	0
Dec-11	88	171	305	76	326	23	6	4	2	6	13	1	1	4	2	3	0	0	0	1	0	0	0	0
Jun-12	99	202	328	86	360	25	6	7	2	6	13	1	1	4	2	3	0	0	0	1	1	0	1	0
Dec-12	111	234	339	88	388	26	6	11	2	10	13	2	1	5	2	3	0	0	0	1	1	1	1	0
Jun-13	121	263	350	89	415	31	6	13	2	10	13	2	1	5	2	4	0	0	0	1	1	1	1	0
Dec-13	160	298	359	92	453	33	6	14	2	11	16	3	2	5	2	5	1	1	0	1	1	1	1	0
Jun-14	193	326	370	93	483	33	6	14	2	11	16	3	3	5	2	5	4	1	1	1	1	1	1	1
Dec-14	209	331	380	95	508	34	6	14	2	11	16	3	3	5	2	5	4	2	2	1	1	1	1	1
Jun-15	234	343	387	99	556	36	6	14	2	11	16	3	3	5	2	5	4	2	2	1	1	1	1	1
July 15	258	367	389	104	588	36	6	14	2	11	16	3	3	5	2	5	4	3	3	1	1	1	1	1

Table 1: IPv6 Ready Products products by countries

3. Building the Business Case for IPv6 Adoption

Unfortunately, defining the business case for IPv6 has been a rather challenging task. IPv6 stands ready to revitalise the growth and use of networking and the Internet as a platform for commerce, education, entertainment, and general information sharing. However, at the end of the day, it is still seen as just communication "plumbing". The market has long looked to IPv6 to deliver the next "killer applications" when, in reality; IPv6 is just a tool, albeit a critical one, in the development of new applications and network-based services. This reality, combined with most businesses' short-term perspective on return-on-investment (ROI) and quarterly earnings, have created a reluctance to invest in upgrading Internet infrastructure to IPv6, most notably in North America and Europe.

Another impediment to IPv6 adoption has been one of the Internet IPv6 community's own making: extolling the virtues of IPv6 primarily from a technical perspective. While IPv6 offers a number of technological advancements, such as a larger address space, autoconfiguration, a more robust security model for the peer-to-peer environment, and better mobility support, these features have been offered in a technology vacuum that has not resonated with big business. Both business and government leaders are concerned about how problems are resolved, how revenue is generated, or how to build efficiencies and cost savings into their organisation. IPv6 certainly has the ability to help deliver these scenarios, but the focus of the story needs to be on the solution – not the technology that helps deliver that solution.

The Internet IPv6 community may need to motivate industry by developing appealing and compelling business-case justifications that focus on solutions built with and upon IPv6. To that end, IPv6 should be placed in context as a solutions tool and a foundation for innovation. In short, the discussion should be about IPv6 as a key to greater business or organisational success, not as a mythical quest for its own sake.

IPv6 as a Solutions Tool

Organisations utilise information technology every day to solve business problems. The adoption of networking technologies to facilitate communications, conduct financial transactions, and or exchange information has been quite successful in boosting productivity and operational efficiency. But there is growing evidence that these gains have been pushed to their limits with current technology. Ignoring for a moment the issue of impending IPv4 address exhaustion, the limited volume of addresses has short-changed technology advancements in areas like "any-casting," multicasting, or peer-to-peer exchanges. Most advanced network support features like security and quality of service which were afterthoughts are not part of the original design of IP. As a consequence, the standards bodies and industry have provided solutions that extended the capabilities of the network, but also drastically increased the complexity of the network and created additional problems.

Today, organisations are finding it increasingly more difficult to deploy new, cost-effective IT solutions that are simple to support.

As a simple example, let's examine a Business to Business (B2B) relationship between an organisation and its partners. Each organisation must participate in business processes. This requires great coordination, extra equipment, and constant management and this represents just one of hundreds of ways IPv6 can be used to solve "real world" problems that add value to the organisation AND improve return-on-investment.

IPv6 as a Foundation for Innovation

IPv6 has several advantages over its predecessor, including a larger and more diverse address space, built-in scalability, and the power to support a more robust end-to-end (i.e., without NAT) security paradigm. As such, it serves as a powerful foundation for the creation of new and improved net-centric sets of products and services. This list is by no means exhaustive, but it does highlight a number of very promising technologies for which IPv6 can provide an important boost for further expansion:

- ***Ubiquitous Communications*** – with increases in the number of mobile phone users, the expansion of Internet-related services through cellular networks, and an increasing number of connection mediums (UMTS, LTE, Wi-Fi, WiMAX, UWB, etc.), there is a need for a uniform communications protocol that supports mobility and can handle a large number of devices.
- ***Voice over Internet Protocol (VoIP)/Multimedia Services*** – VoIP has been making excellent progress from a technology-adoption perspective. A move from ITU-T Recommendation H.323 to Session Initiation Protocol (SIP) has enabled more robust VoIP implementations with a greater level of simplicity and expandability.
- ***Social Networks*** – People interact but the form in which they do this has changed drastically over the years – from written letters, to phone calls, to e-mails, to SMS and IM messages. That evolution continues today. The ability to transfer photos, conduct conversations in private Peer to Peer (P2P) transfers, display personal information on the Internet, find like-minded communities, or play interactive games requires an Internet that is flexible, supports ad-hoc connections, and can be secured. IPv6, with its auto-configuration capabilities and support for IPsec at the IP stack layer, will be a critical tool to enable this environment.
- ***Sensor Networks*** – Sensor networks are a new concept. They can be found in manufacturing equipment, heavy machinery, security systems, and heating, ventilation, and air conditioning systems. Sensors are building blocks for integrating all of those proprietary systems onto one communications network, which then must be protected through security features. IPv6 provides technical improvements to achieve this more readily.
- ***Product Tethering/Communities of Interest*** - Manufactures love to have relationships with their products once they leave the factory. But the current reality is that most consumer electronic goods producers have little, if any, interaction with the end users of their products. In a world where all things can be connected, the opportunities to monitor and troubleshoot performance, update software and market new, value-added services to existing customers are almost endless.

Making the Business Case to Vendors

A recent study released by Ericsson predicts that 50 billion devices will be connected to the Internet by 2020, dwarfing the scale and scope of the current Internet and the mobile worlds. Mobility will play a greater role in the future, as the enabler of the Internet of Things.

For its part, Cisco has recently released a study on the "Internet of Everything", making the business case for a USD 14.4 trillion market, by 2022, for networking basically everything.

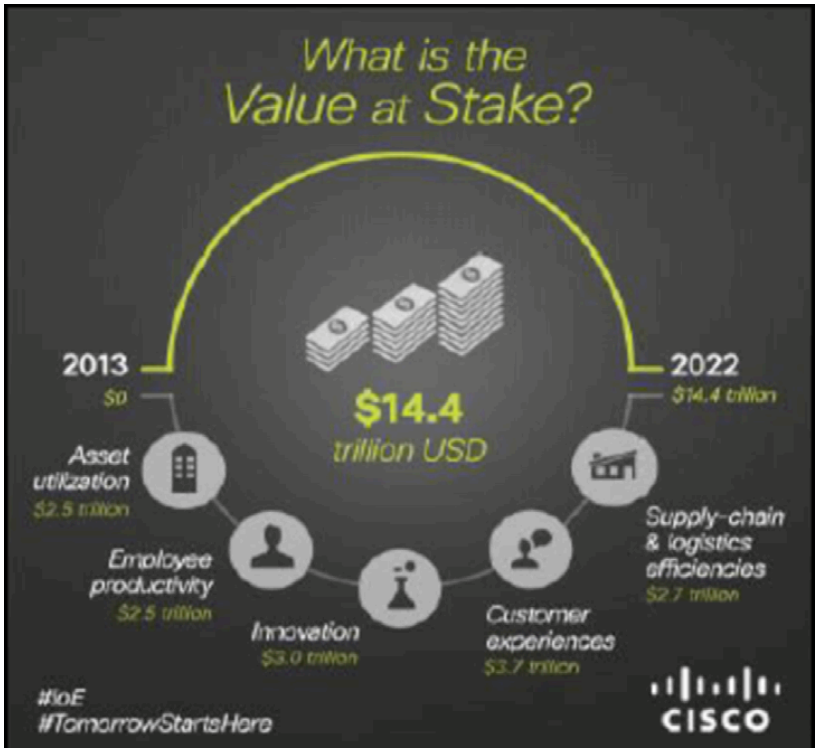


Figure 13: Cisco business case for Networking with IPv6

So the opportunity exists with IPv6 for those willing to consider the protocol as a tool for defining solutions for existing business problems, and as a platform for innovation for next-generation products and services. How, then, can industry continue the groundswell for IPv6 integration?

First, there is still a need to understand IPv6 and its features, and most importantly, how those features map to potential networking problems. Although the IPv6 Community has provided all manner of educational opportunities for industry, there remains a deficit in coordinated efforts to increase IPv6 awareness at three levels:

- Strategic planning at the corporate level,
- Improved return-on-investment (RoI), and
- Technical knowledge at a tactical level.

To achieve a measure of success, the IPv6 Community needs to follow this basic strategy:

- **Generate an interest in business solutions at the CEO/CTO level.** Stories about the virtues of auto-configuration and the power of IPsec EH should be left at the door to the boardroom. Solutions that fix business problems or build competitive advantages are more compelling. The fact that IPv6 is the glue that makes those solutions function should be icing, not the cake. Once the business solutions are "sold", IPv6 will become part of the long term strategies of these organisations.
- **Create a framework for return on investment to justify sound decision-making.** Providing executives with the framework for an ROI improvement model will expedite this process.
- **Solutions sold at the CEO/COO level will need competent engineering and architecture to deliver.** This requires formalised education and knowledge transfer, and CEO/COO level of executives needs to understand and support this process.

4. Addressing the Cost of IPv6 Transition

One of the key hurdles in formulating a business case for IPv6 adoption is the perception of costs versus benefits. The potential costs associated with deploying IPv6 consist of a mixture of hardware, software, labour, and miscellaneous costs. The transition to IPv6 is not analogous to turning on a light switch; instead, many different paths can be taken to varying levels of IPv6 deployment. Each organisation or user throughout the Internet supply chain will incur some costs to transition to IPv6, primarily in the form of labour and capital expenditures, which are required to integrate IPv6 capabilities into existing networks.

Expenditures and support activities will vary greatly across and within stakeholder groups depending on their existing infrastructure and IPv6-related needs. By and large, ISPs offering services to large groups of customers will likely incur the largest transition costs per organisation, while independent users will bear little, if any, costs.

Breaking Down the Cost Factors

Factors influencing these costs include:

- Type of Internet use or type of service being offered by each organisation;
- Transition mechanism(s) that the organisation intends to implement (e.g., tunnelling, dual-stack, translation, or a combination);
- Organisation-specific pattern of infrastructure, which comprises servers, routers, firewalls, billing systems, and standard and customised network-enabled software applications;
- Level of security required during the transition; and
- Timing of the transition.

Table 2 provides a list of relative costs that may be incurred by stakeholder group and gives a percentage breakdown by cost category.

Transition Cost Breakdown

Stakeholders	Relative Cost	HW	SW	Labor	Timing Issues	Key Factors in Bearing Costs
Hardware Vendors	Low[b]	10%	10%	80%	Currently most are providing IPv6 capabilities	Rolling in IPv6 as a standard R&D expense; international interest and future profits incentivise investments
Software Vendors	Low / Medium[c]	10%	10%	80%	Currently some are providing IPv6 capabilities	Interoperability issues could increase costs
Internet Users (large)	Medium	10%	20%	70%	Very few currently using IPv6; HW and SW will become capable as routine upgrade; enabling cost should decrease over time	Users will wait for significantly lower enablement costs or (more probably) a killer application requiring IPv6 for end-to-end functionality before enabling
Internet Users (small)	Low	30%	40%	30%	Availability and adoption schedules	With little money to spare, these users must see a clear return on investment (ROI)
Internet Service Providers (ISPs)	High[d]	15%	15%	70%	Very few offering IPv6 service; no demand currently; very high cost currently to upgrade major capabilities	ISPs see low or non-existent ROI, high costs, and high risk

Table 2: Transition cost breakdown
Source: RTI estimates based on RFC responses, discussions with industry stakeholders, and an extensive literature review.

[a] These costs are estimates based on conversations with numerous stakeholders and industry experts. Several assumptions underlie them. First, it is assumed that IPv6 is not enabled (or "turned on") or included in products and no IPv6 service is offered until it makes business sense for each stakeholder group. Hardware and software costs are one-time costs. Labour costs could continue for as long as the transition period and possibly longer.

[b] For hardware vendors producing high-volume parts that require changes to application-specific integrated circuits (ASIC), the costs could be very high and would not be offered until the market is willing to pay.

[c] Software developers of operating systems will incur a relatively low cost; however, application developers will incur greater relative costs, designated as medium.

[d] The relative cost for ISPs is particularly high if the ISP manages equipment at user sites, because premises equipment is more costly to manage and maintain.

Table 3 provides an item-by-item list of the costs to deploy IPv6 by stakeholder group. This is a relative comparison of costs and should not be interpreted as representing the actual size of each stakeholder group's cost. Furthermore, small Internet users (e.g., home and small businesses) are not captured in Table 3 because they will likely incur virtually no costs. Small Internet users will receive software upgrades (e.g., operating systems and email software) as new versions are purchased, that their IPv4-only hardware (e.g., routers and modems) will be replaced over time as part of normal upgrade expenditures, and that IPv6 will eventually be provided at no additional cost.

Item	Hardware, Software, Service Providers	ISPs	Enterprise Users
Hardware			
Replace interfacing cards	H		M
Replace routing/forwarding engine(s) [b]	M	M	
Replace chassis (if line cards will not fit)		M	M
Replace firewall		M	M
Software			
Upgrade network monitoring/management software		H	H
Upgrade operating system		M	H
Upgrade applications [c]			
Servers (Web, DNS, file transfer protocol (FTP), mail, music, video. etc.)			L
Enterprise resource planning software (e.g., PeopleSoft, Oracle, SAP, etc.)			H
Other organisation-specific, network-enabled applications			H
Labor			
R & D	M	L	
Train networking/IT employees	H	H	H
Design IPv6 transition strategy and a network vision	M	H	M/H
Implement transition:			
Install and configure any new hardware	L	H	H
Configure transition technique (e.g., tunneling, dual-stack, NAT-port address translation	M	M	M
Upgrade software (see Software section above)		L/M	L/M
Extensive test before "going live" with IPv6 services		H	H
Maintain new system		M/H	M/H
Other			
IPv6 address blocks			L
Lost employee productivity [d]			
Security intrusions [e]		H	H
Foreign activities		M	M
Interoperability issues		M/H	M/H

Table 3: Relative Costs of IPv6 Deployment by Stakeholder Group
Source: RTI estimates based on RFC responses, discussions with industry stakeholders, and a literature review.

[a] The relative designation (L = low, M = medium, and H = high) indicates the estimated level of cost to members of each stakeholder group. These costs are not incremental, but reflect differences in costs between stakeholder groups. The blank spaces indicate that a particular cost category does not affect all stakeholder groups.

[b] The "brains" of the router are commonly found on line cards.
[c] Portions of the first column, principally relating to software upgrades by hardware, software, service providers, is blank because the costs of these activities are reflected in the corresponding categories in the "Enterprise Users" column.
[d] Because of unexpected down-time during transition period.
[e] Based on unfamiliar threats.

Breaking Down the Cost Factors

This section takes a closer look at costs by breaking them down according to the various entities that may incur them.

Hardware, Software and Service Vendors

Vendors that provide products and services include: networking hardware companies, such as router and firewall manufacturers; networking software companies, including operating system and database management application developers; and service vendors, including companies that offer training, service, and support. Obviously, these companies will need to integrate IPv6 capabilities into their products and services, if they have not already done so, in order for IPv6 capabilities to be available to end users and ISPs. Once IPv6-capable products are installed in user networks and their labour forces have been trained, ISPs will be enabled to offer IPv6 service, and users will be able to purchase IPv6-enabled devices and applications. Many companies in this category are already developing, and some are even selling, IPv6-capable products and services largely because of demand outside the United States (e.g., Asia).

The majority of the costs being incurred by hardware and software developers appear to include labour-intensive research and development (R&D) and training costs. These costs, however, have not been large enough to deter most of those companies from beginning to develop IPv6 products and capabilities. R&D activity has generally been conducted in small intra-company groups dedicated to developing IPv6-capable products with, to date, limited, small-scale interoperability testing with other hardware and software makers. Based on industry experience with the early deployments of IPv4 equipment, large-scale deployment may bring to light additional interoperability issues.

ISPs

ISPs comprise two main categories: (1) companies (e.g., AOL, Earthlink, and myriad smaller companies) that provide Internet access service to corporate, governmental, non-profit, and independent Internet users and (2) companies that own and maintain the backbone hardware and software of the Internet (e.g., Verizon, Sprint, AT&T). The categories overlap because companies that own the backbone Internet infrastructure (i.e., Category 2 companies) often provide Internet access service to customers, either directly or through a subsidiary. Today, most backbone transport networks have already upgraded their major routers and routing software to accommodate IPv6. As a result, providing IPv6 connectivity to customers who do not require additional equipment, service, or support will be relatively low-cost. Consequently, this analysis focuses on those ISPs in Category 1 that have large customer service provision capabilities.

These ISPs will likely incur relatively high transition costs as they enable IPv6-capable hardware and software and work through system interoperability problems. To date, however, little demand has appeared in the United States for IPv6 services or applications. As a result, given the costs to reconfigure networks, experts and industry stakeholders agree that U.S. ISPs are currently not positioned to realise a positive return on investment from large-scale offerings of IPv6 service.

For Category 1, in order for ISPs to offer a limited amount of IPv6 service, they would need to integrate some transition mechanism(s), such as tunnelling. The costs of doing so will probably not be large. If several routers and service provisioning software are upgraded and limited testing is performed, IPv6 service could be provided to a limited number of Internet users today at minimal additional cost.

Internet Users

Costs to upgrade to IPv6 for Internet users vary greatly. Independent Internet users, including residential users and small and medium enterprises (SMEs) that do not operate servers or any major database software, will need to upgrade only networking software (e.g., operating systems), one or more small routers, and any existing firewalls to gain IPv6 capabilities. This cost will be relatively minimal if the hardware and software are acquired through routine upgrades.

Larger organisations, such as corporations, government agencies, and non-profits, will incur considerably more costs than home or small network users. The relative level of these costs, however, will depend on existing network infrastructure and administrative policies across organisations, the extent to which a specific organisation wants to operate IPv6 applications, and whether it intends to connect to other organisations using IPv6.

The magnitude of the transition costs is still uncertain because only a few test beds and universities have made large-scale transitions. According to officials at Internet2,[18] the time and effort needed to transition their backbone to IPv6 was minimal, and no significant system problems have been encountered. However, Internet2 indicated that their experimental system was implemented and maintained by leading industry experts. It is unclear what issues might arise from implementation by less-experienced staff. If normal upgrade cycles are assumed to provide IPv6 capabilities, transition costs will be limited to training and some reconfiguration.

Breaking Down the Costs by Type

Internet users, as a whole, constitute the largest stakeholder group. The robustness and diversity within this group demands a more detailed explanation of costs broken out by hardware, software, labour, and other cost categories.

Hardware Costs

Depending on individual networks and the level of IPv6 use, some hardware units can become IPv6-capable via software upgrades. However, to realise the full benefits of IPv6, most IPv4-based network hardware will need to be upgraded with IPv6 capabilities. Specifically, high-end routers, switches, memory, and firewalls all will need to be upgraded to provide the memory and processing needed to enable large scale IPv6 use within a network at an acceptable level of performance. It is generally agreed that to reduce hardware costs, all or the majority of hardware should be upgraded to have IPv6 capabilities as part of the normal upgrade cycle (generally occurring every three to five years for most routers and servers, but potentially longer for other hardware such as mainframes). At that time, IPv6 capabilities should be available and included in standard hardware versions. In the short term, replacement of some forwarding devices and software could be used to set up small-scale IPv6 networks.

Software Costs

Significant software upgrades will be necessary for IPv6 use; however, similar to hardware costs, many of these costs will be negligible if IPv6 capabilities are part of the routine requirements in periodic software upgrades. Software upgrades include server software, server and desktop operating systems, business-to-business (B2B) software, networked database software, network administration tools, and any other organisation-specific network-enabled applications. Currently, the main software costs that user organisations envision pertain to element management, network management, and operations support systems that are often network-specific and will need revised software coding to adjust for IPv6. Given the anticipated growth in IPv6-capable software, it is likely that if Internet users upgrade their commercial application software in three or four years, they will acquire IPv6 capabilities. However, they will still need to upgrade their company-specific software.

[18] Internet2 (a US Research network: http://www.internet2.edu/)

Labour Costs

According to experts, training costs are likely to be one of the most significant upgrade costs, although most view it as a one-time cost that could be spread out over several years. The magnitude of these training costs will, of course, depend on existing staff's familiarity and facility with IPv6. On a daily basis, the change in operating procedure for IPv6 will be minimal. Most network staff, however, will need some understanding of the required network infrastructure changes and how they might affect security or interoperability. The North American IPv6 Task Force[19] notes that the relative programming skills of software engineers at a particular company could substantially affect upgrade costs. A company with more skilful programmers might have to hire one additional employee, while another might need three or four, during a transition period that could last five or more years. Additionally, increased network maintenance costs following IPv6 implementation could be more pronounced, depending on the relative level of IT staff skills and technical understanding. Similarly, training costs should be minimal for large organisations with existing IPv6 expertise (e.g., universities).

Bridging the IPv6 Chasm

As stated at the beginning, the business case has been the Achilles' heel of IPv6. The focus for many businesses in the Internet and Telecom sectors is, and always has been, squarely on squeezing maximum revenues out of current infrastructure. Since IPv6 is viewed primarily as a long-term plumbing problem, many organisations and businesses are reluctant to tear open the walls, even if IPv6 represents the best investment and solution. Unlike the Year 2000 bug (Y2K), there is no 'big bang' date at which IPv4 address space will run out; thus there is no perceived urgency in transitioning to IPv6 deployment while ISPs can still take revenue from IPv4 deployment. The choice between an immediate deployment and a gradual technology refresh is fairly obvious depending on the size of the address space allocated to the region in question.

The deployment of IPv6 is a challenge that can be called the "IPv6 Chasm." While the technology is maturing, ISPs and enterprise customers are currently still stuck between the research and validation phase and full-scale deployment. The lack of IPv4 address space in Asia has accelerated the deployment in that region. Until recently, Europe and the United States had enough address space to take their time, but in the last 12 months, that has changed, and those regions have now begun to see the urgency as well.

Section 4 explores the ability of inter-governmental organisations, multi-stakeholder groups and governments to help set a policy framework to accelerate IPv6 deployment, building a potential bridge across the chasm.

[19] Nav6TF (North American IPv6 Task Force: www.nav6tf.org)

3 • Policy and Political Goodwill

Over the past decade, IPv6 has enjoyed remarkable support from governments and industry standards bodies. Government policy-makers have established plans and promoted policies to help ensure that there is sufficient awareness of the need to transition to IPv6, and regulators have played a role by establishing the frameworks for network compatibility and interconnection, among other things. Industry groups have established the technical standards for IPv6 and also have elevated the level of emphasis on implementation. All of this has helped cement the concept that IPv6 is simply not a passing technology or "trend", but truly the foundation for the next-generation Internet. The list below identifies just a few examples of how governments, including regulators, and industry bodies have helped to promote IPv6 usage:

- 3GPP[20] mandated exclusive use of IPv6 for IMS (IP Multimedia Subsystems) back in May 2000;
- Large mobile operators such as Verizon and T-Mobile have introduced IPv6 in 4G -LTE (Long Term Evolution) service;
- The United States Department of Defence mandated the integration of IPv6 in June 2003, to be ready by 2008;
- In June 2005, the U.S. White House Office of Management (OMB) set a milestone for federal agencies to use IPv6 by June 2008;
- The European Space Agency has declared its support for IPv6 in testing its networks;
- The Japanese ITS project and the European Car-2-Car consortium[21] recommended exclusive use of IPv6 for its future car2car applications;
- The Chinese government created and financially supports CNGI, an IPv6 backbone network designed to be the core of China's Internet infrastructure; and
- The European Committee for Electrotechnical Standardisation (CENELEC) has opted for IPv6 for its Smart Home concept.[22]

These represent just a few of the numerous examples in which IPv6 has garnered major support from a government body or an industry consortium. In the case of governments, aggressive IPv6 adoption curves have pushed industry, particularly those vendors supporting or interacting with the government, to work toward IPv6 adoption themselves. So, winning the political endorsement and goodwill can be a plausible and a viable route to accelerate acceptance and adoption of IPv6. This section explores the interwoven roles that can be played in promoting IPv6 adoption by:

- Inter-governmental and international non-governmental organisations,
- Standards bodies and advocacy groups, and
- Government ministers and regulators.

The role of the government in the adoption of the new Internet protocol is a continuation of the adoption of the Internet as a whole. Governments have designed Internet promotion plans in the past for e-Government, e-Commerce, and e-Health, enabling use of the Internet as a ubiquitous service platform. The broadband Internet policies promoted are the next level of extending better service to the users.

[20] 3GPP: www.3gpp.org
[21] Car 2 Car Consortium: http://www.car-to-car.org
[22] http://ar.groups.yahoo.com/group/IEEEAR-SA/message/5

1. Global IPv6 Initiatives

Intergovernmental organisations have a role to play in developing a global framework and consensus for adoption of IPv6. This section examines that role and the activities that organisations such as ITU already have undertaken to foster IPv6 adoption.

IPv6 and the Role of the ITU

The International Telecommunication Union (ITU) has taken action, in various forums, to encourage capacity-building for deployment of IPv6 and the seamless transition from IPv4 to IPv6. Recent actions include:

- **World Telecommunication Standardisation Assembly (WTSA) Resolution 64** – Revised at WTSA-12, this resolution urges continued cooperation between ITU-T and ITU-D to assist developing countries with IPv6 transition efforts, including through a website and by assisting in establishing test beds and training activities.
- **ITU Plenipotentiary Resolution 180** – Adopted in 2010 in Guadalajara, Mexico, this resolution urges efforts to facilitate the transition from IPv4 to IPv6.
- **ITU Council** – The Council established an IPv6 working group in 2009.
- **World Telecommunication Development Conference, Resolution 63** -- Adopted in Hyderabad in 2010, the resolution encourages the deployment of IPv6 in the developing countries and requests that the Telecommunication Development Bureau (BDT) develop guidelines for migration to, and deployment of IPv6. BDT also was asked to collaborate closely with relevant entities to provide human capacity-development, training, and other assistance.

Most recently, two related opinions were considered and adopted at the **World Telecommunication Policy Forum (WTPF)** held on 14th – 16th May 2013 in Geneva. Opinion 3 ("Supporting Capacity Building for the Deployment of IPv6") called for "every effort" to be made to "encourage and facilitate" the IPv6 transition. More specifically, it indicated that if remaining IPv4 addresses are exchanged among RIRs, these transfers should be based on a need for new addresses and should be equitable among all of the RIRs. Turning to sector members, Opinion 3 urged companies to deploy equipment with IPv6 capabilities as soon as possible.

Similarly, WTPF-13 Opinion 4 ("In Support of IPv6 Adoption and Transition from IPv4") urged governments to take "appropriate measures to encourage, facilitate, and support the fastest possible adoption and migration to IPv6". Meanwhile, it noted that IPv4 addresses would still be needed for some time and recommended efforts to ensure "optimal use" of those addresses. Plans and policies should be in place to accommodate new ISP market entrants that need access to IPv4 addresses at affordable prices. Both opinions took note of a trend toward marketing IPv4 addresses for trading purposes, and Opinion 4 specifically indicated that such transfers should be reported to the relevant RIRs.

Meanwhile, ITU-T's Study Group 16 conducted a transcontinental IPTV experiment over IPv6 infrastructure in February 2012. After this experiment, and upon requests from ITU membership, a global IPTV IPv6 test bed was set up among several ITU members, connecting ITU headquarters and countries such as Japan and Singapore. The purpose was to test interoperability of IPTV equipment and services, as well as other IPv6-based technologies. Another goal was to promote IPv6 capability deployment in developing countries. This test bed was updated for a second transcontinental IPTV experiment showcased in February 2013. BDT is involved in many activities related to IPv6, under PP10 Res. 180, for the adoption of IPv6. Through these and other actions, the ITU can be seen in a largely supportive role, both in expressing the policy consensus of its members and in facilitating real-world pilot projects. ITU has sought to advise governments and encourage industry to move forward with the IPv6 transition in a seamless and timely manner, but it has not attempted to mandate any particular transition pathway. This reflects the reality of the Internet addressing system as a decentralised and largely need-driven one.

The Organisation for Economic Cooperation and Development (OECD)

The OECD has been instrumental in researching and measuring the extent of deployment of IPv6 technology. In a 2010 report,[23] the OECD noted the challenge for expanding the Internet without completing the transition to IPv6. This challenge is partly technical:

> For technical reasons, IPv6 is not directly backwards compatible with IPv4 and consequently, the technical transition from IPv4 to IPv6 is complex. If a device can implement ***both*** IPv4 and IPv6 network layer stacks, the "dual-stack" transition mechanism enables the co-existence of IPv4 and IPv6. For isolated IPv6 devices to communicate with one another, IPv6 over IPv4 "tunnelling" mechanisms can be set up. Finally, for ***IPv6-only*** devices to communicate with IPv4-only devices, an intermediate device must "translate" between IPv4 and IPv6. All three mechanisms of dual-stack, tunnelling, and translation require access to some quantity of IPv4 addresses.[24]

Moreover, the OECD report, which continued a series of previous reports on IPv6, noted that "adequate adoption of IPv6 cannot yet be demonstrated by the measurements explored in this report. In particular, IPv6 is not being deployed sufficiently rapidly to intercept the estimated IPv4 exhaustion date."[25] The report issued a clarion call for greater cooperation between government and industry and for increasing government commitments to IPv6 deployment.

The Role of Standards Bodies and Multi-stakeholder Groups

While ITU has adopted a stance of promoting and encouraging IPv6 transition (and frugal use of remaining IPv4 addresses), much of the technical work to ease the transition has been addressed by standards bodies and other "multi-stakeholder" groups. As with all elements of Internet governance, these groups have been instrumental in developing and implementing the technical standards needed for open and widespread adoption of IPv6.

The Internet address space is considered to be a primary function of Internet governance in many parts of the world, especially in the North American, Asia-Pacific and European regions where Internet early adoption drove a de-centralised, technically oriented, and non-governmental approach. Because of this heritage, policy-makers in these regions often see the "multi-stakeholder model" that has typified Internet governance as the best means to rapidly engage industry and civil society in the development of technical standards. Proponents of the multi-stakeholder approach are often wary of efforts by governments and inter-governmental organisations (IGOs) to increase their influence over Internet governance, in general (including IPv4 and IPv6 transition issues).

For their part, some critics of the multi-stakeholder model argue that the existing groups have not managed to broaden access to include participation from developing countries and (to some extent) non-manufacturing interests. The result has been a global debate over how to balance the roles of multi-stakeholder groups with those of governments and IGOs. This debate likely will continue during this decade, even as the IPv6 transition continues under the current governance architecture.

Table 4 provides a representational listing of some of the major multi-stakeholder groups and standards bodies that have key roles in Internet addressing. Many of these groups are playing key roles in the IPv6 transition process, often by working with governments and IGOs. The chart notes the general type of organisation (i.e., whether its main role is to provide a forum for standards-setting, Internet governance or policy advocacy), and its role in the IPv6 transition process.

[23] See "Internet Addressing: Measuring Deployment of IPv6," OECD, April 2010 at http://www.oecd.org/internet/ieconomy/44953210.pdf
[24] Ibid, p. 6
[25] Ibid, p. 5.

Name of Organisation	Type of Organisation	IPv6 Role and Activities
Standards Bodies		
European Telecommunications Standards Institute (ETSI)	Standardisation Body	Interoperability Testing IPv6 Ready Logo Programme
The Internet Engineering Task Force (IETF)	Standards, Engineering	Sole IP designer of IPv6
Internet Governance & Advocacy Groups		
International Chamber of Commerce (ICC)	Advocacy Group	Repeated and consistent support for IPv6 transition Identified measurements of IPv6 deployment.
Internet Corporation for Assigned Names and Numbers (ICANN)/ Internet Assigned Numbers Authority (IANA)	Internet Governance	Added IPv6 addresses for 6 of the world's 13 root server networks.
Internet Governance Forum (IGF)	Advocacy, Policy Discussion	Has held workshops to address IPv6 transition issues
Internet Society (ISOC)	Advocacy, Policy Discussion	World IPv6 Day, 2011 World IPv6 Launch Day, 2012
RIPE NCC	RIR for Europe [26]	Portal IPv6 ActNow High IPv6 allocation count
ARIN	RIR for North America	Began aggressive rollout plan in 2007
APNIC	RIR for Asia	Monitors and supports IPv6 deployment in the Asia-Pacific region
AFRINIC	RIR for Africa	Offers IPv6 transition support, featuring training materials and test beds
LACNIC	RIR for Latin America and the Caribbean	Maintains a portal in 3 languages (Spanish, Portuguese, English) as a one-stop IPv6 resource
European Network and Information Security Agency (ENISA)	Advocacy, Policy Discussion	Centre of Excellence for European States on network and information security

Table 4: Standard Bodies and Multi-Stakeholder Organisations

[26] Regional Internet Registry

The Role of National Governments and Regulators

Government policy-makers and regulators have not been passive in promoting efforts to build capacity, deploy infrastructure and urge the adoption of IPv6. Regulators have had a foundational role in ensuring that regulations governing licensing, interconnection, and numbering resources are aligned with efforts to promote the transition to IPv6. Regulatory agencies have at times cited a need to maintain a "light-handed" or "light-touch" regulatory stance towards Internet addressing, emphasising the development of regulations for a competitive and affordable Internet access market that would promote demand.[27] Governments have, however, taken some specific steps to promote awareness of the need to utilise IPv6 to expand Internet resources. Key elements of governmental action have included:

- Establishing or supporting national IPv6 transition task forces (often in conjunction with multi-stakeholder groups or RIRs);
- Establishing national "roadmaps" with benchmarks and timetables for IPv6 deployment;
- Mandating that government agencies adopt IPv6 technology for their networks, websites or services;
- Promoting the use of IPv6 in government-funded educational, science and research networks; and
- Promoting overall awareness of the transition through setting up websites, hosting workshops or forums, and setting up training programmes.

As a long-time tech leader in East Asia, Japan has sought to position itself as a model for planning in this area. The Japanese Government has designed its latest program around the concept of ubiquity called "u-Japan" (Ubiquitous Japan) as the 2010 ICT Society platform. The e-government component of this plan encourages government agencies to procure IPv6-enabled devices; the infrastructure of the Japanese government has been IPv6-ready since 2007. Similarly, the Republic of Korea has unveiled its new IT sector development strategy, dubbed "IT839," seeking to build on efforts in the previous decade to embed IPv6 in e-government services and the networks of the postal service, universities, schools, the defence ministry and local governments. In some cases, governments are devoting large budget outlays to support their national roadmaps. For example, Taiwan, Republic of China, has announced a USD 1 billion budget for its "eTaiwan" programme, which entails a concerted joint effort between government and industry. The goal is to reach 6 million broadband users of IPv6 technology.

Indonesia developed a comprehensive, phased national plan and roadmap, beginning in 2006. The first phase involved generating awareness of IPv6, establishing an implementation model that included a first-stage native IPv6 network, and developing a broad-based national policy. Meanwhile, Indonesia made a commitment to participate in global efforts to shape the development of IPv6, as well as policies on Internet governance and standards activities. Additional phases called for development of further infrastructure and training to accelerate the transition process to IPv6.

Regional approaches have proved to be helpful in several parts of the world. For example, some 29 countries and territories formed the Latin American and Caribbean IPv6 Task Force (LACIPv6TH) under the auspices of LACNIC. This regional task force has held forums on IPv6 transition in more than a dozen countries around Latin America and the Caribbean, from Mexico and the Netherlands Antilles down to Brazil and Uruguay. Among other things, the task force developed an IPv6 portal to assist as data and information resources in the transition throughout the region.

[27] See, for example, the consultation paper published by the Information and Communications Technology Authority (ICTA) of Mauritius, 17 March 2011, at http://www.icta.mu/documents/Consultation_IPv6.pdf

The Arab region and Africa have also worked to share expertise on a regional basis. The Arab group formed an IPv6 Forum to spotlight individual countries' efforts:

- The United Arab Emirates has formulated an IPv6 roadmap and in March 2013 held two workshops to prepare the UAE and its Internet stakeholders for looming IPv4 depletion;
- The Egyptian Ministry of Communications and Information Technology formed a national IPv6 task force;
- The Moroccan regulator ANRT has commissioned an IPv6 study to define a roadmap and is discussing a calendar for IPv6 deployment with the country's main telecom operators;
- In Jordan, the IPv6 Forum chapter has held seminars with multiple stakeholders (including ISPs) to promote awareness and offer technical assistance;
- The Omani Telecommunications Regulatory Authority is taking the lead in promoting IPv6 transition, including by beginning to test implementation in conjunction with operators. Saudi Arabia adopted a clear strategy to move towards IPv6 in 2008 through establishing the National IPv6 Taskforce, developing awareness and capacity building plans, and starting implementation of programs aimed at raising the readiness of large enterprises to start the transition to IPv6.

The following Table 5 summarises the various countries that had a National IPv6 Regulator Policy:

National Regulators IPv6 Deployment Roadmaps

Regulator	IT Policy -- IPv6 Roadmap -- Adoption Year	Milestones	Results
India TRAI	• IPv6 Recommendation -- Year 2005	•DOT – TEC to take over 1.1.2006	• IPv6 Strategy & Roadmap published in 2010 and 2013
Europe	• Finnish Ficora – Year 2001 • Austrian RIR Year 2006 • French ARCEP Year 2002 • European BEREC	• Recommendations • In the BEREC board of Regulators 2013 Workprogramme dated December 12, 2012, the board in § 6.5 outlines an action item for IPv6 in relation to Machine to machine (M2M)	•
Saudi CITC	• IPv6 Strategy -- Year 2008 • 3 Studies: • IPv6 Readiness Assessment • IPv6 Countries Benchmark • IPv6 International bodies & Organisations	• Infrastructure Track • Awareness Track	• 14 ASNs support IPv6 • 3 ASNs have IPv6 traffice Transition Process
Oman TRA	• Oman IPv6 Strategy--Year 2010 •	• IPv6.om Web Site	• OmanTel Testing IPv6
Morocco ANRT	• IPv6 Study -- Year 2012	• ISP Readiness work	• Strategy published in 2013

Table 5: National Regulators IPv6 Deployment Roadmaps.

The RIPE NCC/MENOG[28] IPv6 Roadshow is a very good capacity building initiative to be simulated for other regions. The IPv6 Roadshow is a technical training program, developed by RIPE NCC and APNIC and organised together with the Middle East Network Operators Group (MENOG). These are 3 or 5 day technical trainings, organised throughout the Arab region with the purpose of training network engineers, who work for public sector and enterprise, to deploy and operate IPv6 based networks and services.

In Africa, the RIR and AFRINIC, has an aggressive training program that has trained some 450 engineers annually across the continent. The IPv6 address space and core network deployment has been particularly successful in South Africa, Kenya, Tanzania, Nigeria, Tunisia, and Senegal.

These efforts in developing countries largely track the efforts in the early-adopting Internet countries of Europe and North America. The United States government's Federal IPv6 task force has worked with the National Institute of Science and Technology (NIST) to make public several versions of a roadmap and recommendations, including 100 per cent enabling of public services with IPv6 and integration of IPv6 into agency Enterprise Architecture efforts, as well as capital planning and security processes. NIST has established a website to track the agencies' progress in meeting milestones. The European Commission, meanwhile, has spent more than EUR 100 million on research projects and awareness/outreach efforts, forming the European IPv6 Task Force for coordination. Individual member states have their own efforts, including:

Spain – the GEN6 programme is developing pilot projects to integrate IPv6 into government operations and cross-border services to address emergency response or EU citizens' migration issues.

Luxembourg – the Luxembourg IPv6 Council has defined a roadmap; the main telecom operator has followed through with offering IPv6 over fibre and published practical steps on implementation for other operators.

Germany – the government has obtained a sizable IPv6 prefix from the RIR to completely enable its online citizen services infrastructure with IPv6

2. Case Studies

This section contains case study examples of the approaches to IPv6 transition planned and implemented in several representative countries.

India's IPv6 Promotion Policy

The Telecom Regulations Authority of India (TRAI) has released a consultation paper on issues related to the transition from IPv4 to IPv6 in India.[29]

The Telecommunications Regulatory Authority of India's (TRAI's) recommendations on accelerating growth of Internet and Broadband served as the basis for the National Broadband Policy 2004, issued by Government. To achieve targets of this policy, the Internet and Broadband connections would require large supply of IP addresses, which may not be easily available through the present version of Internet, i.e., IPv4. The next generation Internet protocol, i.e., IPv6 is seen as one solution for this; in addition, it is claiming to provide better security, QoS, and mobility support.

In the recommendations on Broadband, the need for further analysis and discussion on transition to IPv6 was recognised due to anticipated growth of Internet and Broadband connections. Meanwhile, the Government of India has already constituted a group, called the IPv6 Implementation Group (IPIG), to speed up and facilitate the adoption of IPv6 in the country.

[28] MENOG: The Middle East Network Operators Group: https://www.facebook.com/menog.org
[29] TRA IPv6 Consultation paper: http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/IPV6.pdf

The Indian Department of Telecommunications (DoT) released the government's National IPv6 Deployment Roadmap in July 2010, updating it in 2013. The result is a set of "recommendations" (many of them are mandatory) for government entities, equipment manufacturers, content/applications providers and service providers. Government organisations are required to prepare a detailed plan for transition to dual stack IPv6 infrastructure by December 2017. All new IP-based services, including cloud computing or datacentre services, should immediately support dual stack IPv6. Public interfaces of all government services should be able to support IPv6 by no later than the 1st January 2015. Government procurements should shift to IPv6-ready equipment and networks with IPv6- supporting applications. Finally, government agencies will have to develop human resource (i.e., training) programmes to integrate IPv6 knowledge over a period of one to three years, and IPv6 skills will be included in technical course curricula at schools and technical institutes around India.

Service providers will have a role to play in the country's IPv6 transition, as well. After 1st January 2014, all new enterprise customer connections (wireless and wireline) will have to be capable of carrying IPv6 traffic, either on dual-stack or native IPv6 network infrastructure. Service providers will be urged to advise and promote the switch-over to existing customers, as well. Meanwhile, the roadmap sets aggressive timelines for retail customers. All new wireline retail connections will have to be IPv6-capable after 30th June 2014. All new GSM or CDMA wireless connections will have to meet the same deadline, and all new wireless LTE connections will have to comply a year earlier. There will also be goals for transitioning existing wireline customers, culminating in the upgrade of all customer premises equipment by the end of 2017.

The target for new website content and applications to adopt IPv6 (at least dual stack) was 30th June 2014, with even pre-existing content and apps converted by the following January. India's financial services industry (including banks and insurance companies) transitioned to IPv6 by no later than 30th June 2013. All new registrations of the ".in" national domain are IPv6 (dual stack) by the beginning of 2014, with full migration of the domain completed by the middle of that year.

On the equipment side, all mobile phones, data card dongles and other mobile terminals sold for 2.5 G (GSM/CDMA) or higher technology were sold with IPv6 capability (either dual stack or native) after 30th June 2014. And all wireline customer premises equipment sold after 1st January 2014 has met the same criteria. Finally, all public cloud computing/datacentre services have targeted adoption of IPv6 capabilities by the middle of 2014.

The Indian plan provides an example of aggressive government mandates and targets for IPv6 transition, extending across a broad swathe of the Indian Internet sector. It will be interesting to see if the strategy precipitates a "critical mass" of demand for IPv6 capability that, in turn, generates industry reaction to market solutions for the updated protocol.

Australia

Australia's IPv6 Forum Downunder,[30] in a range of activities coordinated by the IPv6 Special Interest Group of Internet Society Australia, has shifted the focus to business and implementation benefits flowing from adoption of IPv6. These activities have fostered a national discussion of IPv6 that has been accepted by the National ICT Industry Alliance.[31]

In 2005, the Forum had taken the idea of promoting a national discussion of the business and transition processes for IPv6 to the National ICT Industry Alliance[32] (NICTIA). As a result, Australia began a process of IPv6 Summits, led by consortia of the leading Australian IT trade bodies and endorsed by global IPv6 Forum. Year by year, these summits have focused on awareness, business case and transition issues.

Now there are lead IPv6 adoption sectors in Australia, including research & education, defence and government. The largest high speed education network in Australia (the Australian Academic Research Network - AARNet) began implementation with a testbed network, and has now implemented native IPv6 transports and provides IPv4 to IPv6 transition mechanisms for its member and affiliates. The Australian Department of defence announced the adoption of IPv6 in a programme that extended through 2013.

[30] www.ipv6forum.org.au, [31] www.nitcia.org.au, [32] www.nictia.org.au

More recently, the Australian Government Information Management Office (AGIMO) announced a transition strategy for the whole Australian government with a target completion date of 2015.[33] AGIMO's role in the government's implementation of IPv6 includes developing the IPv6 Transition Strategy and Work Plan documents, monitoring and reporting on agencies' progress, knowledge sharing, and monitoring international trends. There are 110 agencies, as named in Australia's Financial Management and Accountability Act (FMA Act), rolling out IPv6 capabilities, including most of the major departments (Defence, Foreign Affairs and Trade, Human Services, Finance and Deregulation, etc.). But the scope also takes in more specialised agencies such as the organ/tissue donation authority and the sports anti-doping agency.

Canada[34]

The Government of Canada (GC) IPv6 adoption strategy consists of a phased approach to progressively enable IPv6, while continuing to support IPv4. The strategy begins at the perimeter of the GC network and moves progressively toward the centre of the network. It is a business-focused approach designed to minimise cost and risk. The strategy leverages SSC's enterprise network renewal initiative and the regular equipment and software refresh cycles.

Business partners and entrepreneurs from emerging economies who, in the future, may only have IPv6 Internet service will be able to access GC websites to do business and research. Canadian citizens travelling or living abroad and non-Canadians who may have access to IPv6 networks only will be able to access GC web services for example, to access their personal income tax information through the Canada Revenue Agency or to apply for a student or work visa through Citizenship and Immigration Canada.

Canadian public servants will be able to:

- Access the GC network in Canada to perform their work duties when posted or travelling abroad in an IPv6-only region;
- Exchange electronic documents with business partners for goods crossing our borders, when these business partners are located in an IPv6-only region;
- Conduct GC business with other governments located in IPv6-only regions; and
- Access websites connected to IPv6 networks to do research.

The GC IPv6 adoption strategy comprises three phases: **Enabling Phase, Deployment Phase, and Completion Phase.**

Enabling Phase: The first phase was completed by the end of September 2013. The goal enabled federal organisations to achieve their individual plans for the adoption of IPv6. Actions achieved for this phase included:

- Developed IPv6 architecture standards and technical requirements;
- Established governance bodies to oversee adoption, including a Steering Committee and a Community of Practice;
- Created a change management strategy, including policies, training, and communications; and
- Enabled IPv6 connectivity for Internet-facing websites through a shared service.

Deployment Phase: The second phase focused on the IPv6 enablement of the principal GC externally-facing websites and was completed by the end of March 2015.

Actions implemented for this phase included:

- Enabled principal-existing GC Internet-facing websites to be accessible by IPv6 users;
- Required all new Internet-facing websites and applications put in place starting April 2015 to be IPv6-enabled; and
- Provided public servants transparent access to the public IPv6 Internet.

Completion Phase: The third phase will focus on expanding the IPv6 enablement of GC websites beyond the principal websites addressed in the Deployment Phase and, as necessary, this phase will focus on enabling IPv6 access to GC internal applications. This phase is expected to take a number of years to complete.

[33] http://www.ipv6.org.au/summit/talks/JohnHillier_AGIMO_IPv6Summit12.pdf
[34] http://www.tbs-sct.gc.ca/it-ti/ipv6/ipv603-eng.asp

Saudi Arabia

The IPv6 Task Force Forum evolved from the outcome of the IPv6 Project that was introduced by the Communications and Information Technology Commission as part of the Internet Services Development Projects undertaken by the CITC.[35] The Commission sponsored the establishment of the Task Force that convened its first meeting on July 30th, 2008. The IPv6 Strategy for Saudi Arabia identified a set of milestones to be achieved within a phased timeline via an action plan of initiatives categorised into two tracks: Infrastructure and Awareness. Meeting the milestones facilitated the deployment and further penetration of IPv6 on a nationwide basis so as to eventually realise an IPv6 ready internet infrastructure in the Kingdom of Saudi Arabia.

The milestones and action plan initiatives were based on assessments and benchmark studies performed by CITC as part of its effort to develop the Internet in Saudi Arabia. The studies assessed the IPv6 status quo and readiness of local stakeholders, extracted lessons from a comprehensive IPv6 benchmark study of eleven countries and stated the status of IPv6 in relevant international bodies and organisations. The IPv6 Strategy for Saudi Arabia objectives were a set of high level goals to be achieved for the purpose of setting up the right environment to promote the deployment of IPv6 nationwide.

The identified objectives were:

- Prepared for the IPv4 exhaustion by supporting IPv6 and ensure stability, business continuity and room for continued growth of the internet in Saudi Arabia;
- Ensured a smooth adoption of IPv6 by stakeholders so as to minimise risks;
- Raised overall IPv6 awareness nationwide by approaching stakeholders of both the public and private sectors highlighting the necessity to adopt IPv6.

The IPv6 Strategy followed a two (2) track approach that addressed Infrastructure and Awareness aspects of IPv6 adoption. It achieved tremendous progress in developing a roadmap deployment commitment for Saudi Arabia with probably the most advanced IPv6 strategy in the Arab region.[36]

CITC embarked on the "Promotion of IPv6 Deployment in the Kingdom of Saudi Arabia Project" following the first IPv6 project activities undertaken in 2008 – 2009 that resulted in the first IPv6 Strategy for Saudi Arabia as well as the establishment of the IPv6 Task Force.

While the previous IPv6 activities focused on service providers, this IPv6 project focused on adoption by enterprises. The project aims at continuing the success of the previous IPv6 activities and taking practical steps to promote the deployment of IPv6 in the Kingdom, reaching the level of implementing a set of pilot projects at selected enterprises that will provide showcases for all Internet stakeholders to emulate. The project aimed at benchmarking the status of IPv6 deployment in the Kingdom against international trends and addressing regulatory and technical aspects of the Internet ecosystem which could affect the smooth adoption and deployment of IPv6 in the Kingdom. A set of IPv6 guidelines and procedures were developed to also cover this project.

Figure 14 provides a summary of some of the objectives that the Saudi Arabian plan has met to-date.

[35] http://www.ipv6.org.sa/about
[36] http://www.ipv6.sa/strategy%20

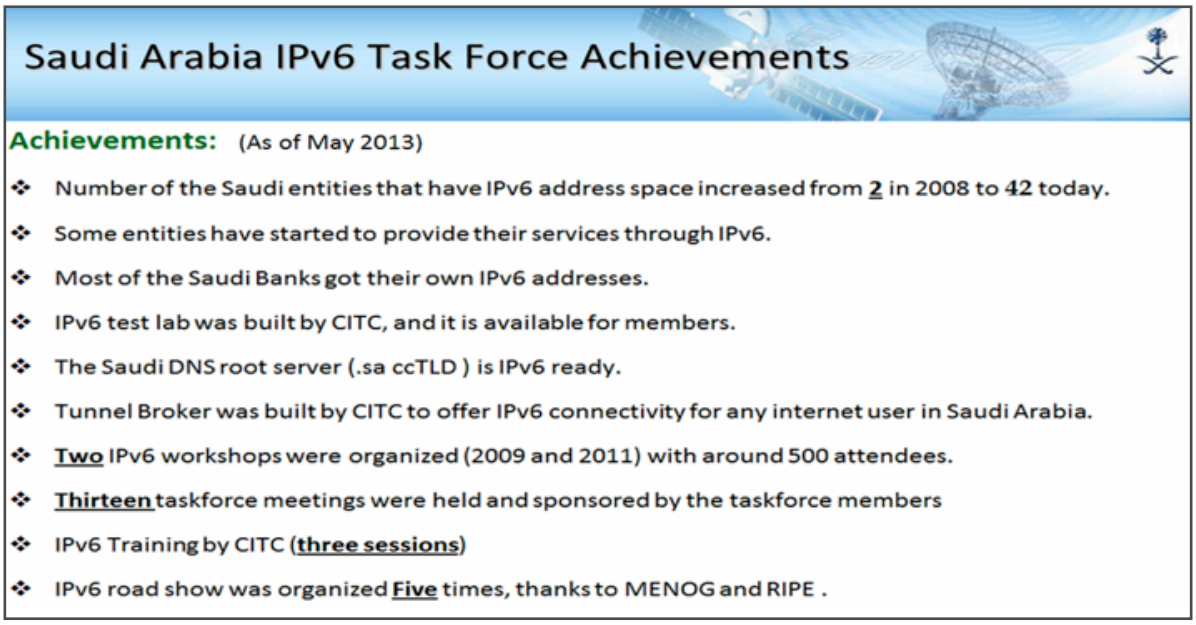


Figure 14: Saudi Arabia IPv6 Task Force Achievements

The following Table 6 summarises the various main countries that had an IPv6 Policy:

Governments IPv6 Deployment Roadmaps

Governments	IT Policy -- IPv6 Roadmap -- Adoption Year	Milestones 1	Milestones 2
United States	• IPv6 Strategy -- Year 2009 • Refreshed -- Year 2012	• Public web sites – 9.2012 • Result: 35% - May 2013	• Complete transition to IPv6 (dual stack) by December 2017
Australia	• AGIMO IPv6 Strategy – Year 2008 • Stage 1: Preparation (2008-2009) • Stage 2: Transition (2010 - 2011) Stage 3: Implementation (2012-2012)	• Tasks: • Review Procurement Policy. • Stocktake of Equipment. • Stocktake of Applications.	Government Transition to IPv6: Stage 2: Transition: Jan 2010 – Dec 2011 Implementation: Jan 2012 – Dec 2012
Canada	• IPv6 adoption strategy – Year 2012	• Enabling Phase – Sep 2013 • Deployment Phase - 2015	• Completion Phase – 201X?
India	• IPv6 Policy -- Year 2010 • Updated -- Year 2013	• Public web sites – 1.1.2015	• Complete transition to IPv6 (dual stack) by December 2017
China	• CNGI -- Year 2006 • NDRC -- Year 2012	• 8M IPv6 users by 2013	• 25M IPv6 users by 2014-5
European Commission	• i2010 • EU IPv6 Task Force Year 2001 • IPv6 Communication 2004 • IPv6 Communication 2008	• 25% IPv6 users by 2010 • Result: 1%	• Focused projects: Deployment: Gen6, EU-China-Fire, IPv6 Observatory, IoT6
Indonesia	• IPv6 Task Force -- Year 2005 • Phase 1: 2006 Dissemination, Research	• Phase 2: 2007 Development of infrastructure and Content	• Phase 3: 2008 - Development of Applications and Transition Process
Taiwan	• E-Taiwan Strategy--Year 2002 •	• Phase 1: 03-05 Promotional strategy	• Phase 2 05-07 Implementation strategy
South Korea	• IT839 Strategy-- Year 2004	• ISP Readiness	• IPv6 service
Japan	• U-Japan -- Year 2001	• ISP readiness	• IPv6 service

Table 6: Goverments IPv6 Deployment Roadmaps

3. Policy Recommendations

Despite the long-term commitment made evident by IGOs, industry/multi-stakeholder organisations and governments, all parties should consider whether the current activities and timelines are sufficient to alleviate the pressure on IPv4 addresses and spur transition to IPv6. Policy-makers and other stakeholders should consider following concrete recommendations as part of a call to action to enable IPv6 as follows:

- Create a CEO IPv6 Round Table with recognised industry leaders, focusing on industry adoption and urging the major players to include adopting IPv6 in their strategy plans. Select the target markets that are likely to be impacted first with the time-to-market in mind.
- Formulate a top-line strategic IPv6 Roadmap as a guideline.
- Increase support for the integration of IPv4 and IPv6 in fixed and mobile Broadband networks and services associated with the public sector:
  - The integration of IPv6 into e-government, e-learning and e-health services, and applications will offer users greater reliability, enhanced security and privacy, and user friendliness.
  - IPv6 future-proofing should be considered in procurements, especially considering that the life cycles of public networks are often longer than commercial counterparts.
- Establish and launch IPv6 competence centres and educational programmes on IPv6 techniques, tools, and applications, to significantly improve the quality of training on IPv6 at the professional level and create the required base of skills and knowledge.
  - A mixture of academic and commercial expertise should be drawn upon for the centres; university and academic sites may be among the early adopters and thus have key expertise.
  - A model has been created by the IPv6 Forum called the IPv6 Education Logo Program[37] which was adopted by the Cisco Learning Network.[38]
- Promote the adoption of IPv6 through awareness-raising campaigns and co-operative research activities, focusing on small and medium-size enterprises, ISPs and wireless service providers and operators.
- Organise IPv6 competition or contests similar to the German IPv6 Apps Contest[39] or the Singapore IPv6 Competition for Students.[40]
- Strengthen financial support for national and regional research networks, with a view to enhancing their integration into worldwide networks and increasing the operational experience with services and applications based on the use of IPv6.
- Provide the required incentives for development, trials and testing of native IPv6 products, tools, services and applications in economic sectors such as consumer electronics, telecommunications, IT equipment manufacturing, etc.
- Include IPv6 criteria in procurement guidelines for new equipment and applications for the public sector.
- Require universities to add IPv6 to the curricula for graduate degree programmes, in order to ensure the next generation of network engineers is IPv6 trained.
- Promote use of open source technologies for implementation of IPv6.[41]
- Support the existing national IPv6 Task Force, or create one, tasking it with:
  - The assessment of current status of IPv6 deployment, as well as with the formulation of guidelines and dissemination of best practises relating to the efficient transition towards IPv6.
  - Developing measures to align IPv6 integration schedules, favouring cohesive IPv6 deployment and ensuring that the nation can gain a competitive advantage in rolling out next-generation Internet networks and services.
  - Ensuring the active participation of national experts in the work of developing international standards, policies and specifications on IPv6-related matters, working with groups such as ETSI, 3GPP, IETF, ITU-T and the RIRs.

[37] http://www.ipv6forum.com/ipv6_education/
[38] Cisco Learning Network: https://learningnetwork.cisco.com/docs/DOC-10327
[39] German IPv6 Contest: http://www.ipv6council.de/contest2011/vertikal_menu/winners/
[40] Singapore IPv6 Contest: http://ipv6competition.com/index.html
[41] See http://www.bieringer.de/linux/IPv6

- Drawing the attention of potential IPv6 systems or application developers to funding opportunities available at a national or regional level.
- Conducting an "IPv6 Launch Day" in the country.
- Establishing collaboration arrangements and working relationships with similar initiatives being launched in other world regions, with a view toward aligning IPv6 work.

- Organise a high-level conference or summit aimed at raising IPv6 awareness, its development status and perspectives, its economic and policy dimensions, and the actions required to consolidate and harmonise international efforts.
- Encourage deployment of new security and firewall modes using IPv6, combined with the use of Public Key Infrastructure (PKI). Promote the development of secure networking applications and environments through trials, deployment, and use of IPv6 IPsec protocols.

Core IPv6 Policy Recommendations

Recommendations	IT Policy	Objectives	Impact
Top down	• CEO Round Table	• Decision-making on investment	• Priority setting for budget
IPv6 Service	• Broadband (Fixed, Optical & Mobile) • 4G – LTE (see Verizon, T-Mobile) • WiFi • Zigbee, 6LoWPAN	• Integrate IPv6 in new broadband infrastructure investment right from the beginning • Future proofing investment	• IPv6 Service readiness for broadband apps for public services • e-Gov; e-Learning; e-Health • Cloud Computing • SDN - NFV
Capacity Building	• Launch IPv6 Competence Centres, Educational Programs and Test Labs • Model: Singpaore IDA	• Build Skills & Expertise • IPv6 Skills Contest • (see Singapore iDA Program)	• High level LOCAL Skills is the cheapest transition tool as 80% of the transition cost is labour.
National Research	• Fund IPv6 Research projects • Include IPv6 in all networking projects.	• Gain higher level Skills • Add IPv6 in Higher education Curriculum	• Gain skills parity with international links
National IPv6 Task Force	• Bottom-up stakeholder Forum to define a national IPv6 Roadmap	• Consensus building PPP-based Objectives • See example of Saudi Arabia IPv6 Task Force)	• National IPv6 Strategy with key-players involvement • Promote DNSSEC

Figure 15: Core IPv6 Policy Recommendations

4 • IPv6 Deployment Best Practices for Governments[42]

1. Introduction

There is nothing more important in the contemporary world than to be a step ahead. On the contrary, regressing one step behind can cause serious problems.

The Internet and nearly all local computer networks make use of the Internet Protocol. Due to the success and the penetration of the Internet in nearly every part of modern life, the initially used Internet Protocol version 4 (IPv4) is running out of address space. In Europe, the Internet registry ran out of IPv4 address blocks in February 2012. The Internet Protocol version 6 (IPv6) was developed to counter this shortage and offers more addresses identifying endpoints.

Network providers with a growing customer base are forced to use the Internet Protocol version 6 (IPv6) to get new customers connected. Connecting ever more networked machines to the Internet ("Internet of Things") requires a huge number of additional IP addresses.

Leading content providers in the Internet world such as Facebook and Google are already running on the new IPv6 version. Some governments have already followed their success story. Not supporting IPv6 may cause connection problems and information shortage on a website to users connected from an IPv6-enabled network. When implementing IPv6, one has to remember to "think globally and act locally". No citizen is to be deprived of the convenience of an ever improving information society.

If public and private sectors introduce IPv6 in their policies, there will be no more exclusion from the future information society.

This best practice paper describes some aspects of IPv6 transition based on experiences from the national pilots of the GEN6 project: http://www.gen6-project.eu/

2. Things to consider

On the following pages, facts and observations happening around IT, services and networks are listed, however, are often being neglected, pushed to the future or even being feared. The common belief is the issue is coming from the provider or there is still enough time before it will affect my business. Whether one is an individual or belongs to the economical or government sector does not change the issue.

3. Roll out for citizens is on its way

Providers have been using IPv4 addresses for customer connections up to now. Most providers which have been in this business for many years have significant IPv4 resources available. On the other hand, competitors joining the market in the last years could not claim a huge amount of IPv4 addresses. Due to the shortage of IPv4 addresses, they were forced to think about the step towards IPv6 in their access networks. Nowadays, several providers connect new customer only with IPv6 and connections to the 'legacy' world of IPv4 are implemented by tunnelling and network address translation in IPv4 or 6to4 solutions. In both cases, expensive carrier grade gateways must be implemented. This results in increasing costs for the providers and consequently for the end users, citizens or businesses.

With IPv6-enabled server/service and access connections, one can use IPv6 without any gateway. Use of those expensive gateways can be minimised and therefore, some costly investments can be avoided.

[42] Gen6 project: Authors:
Zuzana Duračinská (CZ.NIC, Czech Republic,
Uwe Holzmann-Kaiser (FhG Fokus, Germany),
Martin Krengel (Citkomm, Germany),
Jiří Průša (CZ.NIC, Czech Republic)

4. IPv6 as a mandatory part of the operating system

IPv6 is not only promoted in the Internet but vendors regard IPv6 as central infrastructure requirement. Some vendors have declared IPv6 as a mandatory part of their operating system. Since then, there is no system test of Microsoft operating systems without IPv6 enabled. This means that pure IPv4 implementations, which are still the standard in most public administration's networks are unsupported use cases from this vendor's point of view. In practice this means several networks have been enabled with IPv6 "silently", to get vendor support or to use a specific feature. Often there is no real management for IPv6 as the management is not aware of the enabled protocol. From the safety and security point this is a high risk for the network.

5. Consumer market equipment

The number of devices per user is growing rapidly today. While a few years ago one computer per person was the norm, today with smartphones and tablets, the needs are changing. In practice, these devices are not specialised equipment for business use. Instead, the evolution is driven by personal requirements and the consumer market. The professional users in business and government need to install additional software in order to control these devices. On the network side, all these devices are IPv6 enabled, and they cannot be disabled. Consequently, there is still network equipment using IPv4 even in the local networks. In order to prevent malfunction due to usage of both protocols, proper management is in order.

6. Loss of communication

To give availability of 6to4 gateways to all customers, most of the time the number of parallel connections per customer is limited. When websites with a high information density, e.g. city map services, use many several parallel connections to speed up the transmission, some transmissions may get blocked – with an incomplete site presentation as a result on the customer side.

Websites and Internet services providing IPv6 connectivity will not be impacted by those connectivity issues, because they communicate directly with IPv6 without such gateway limitations.

7. Stagnation on eGovernment evolution

The continuous growth of electronic communication demands more connectivity and more hosts. Each node requires its own IP address. As described above, IPv4 addresses have become very limited nowadays. New large address blocks are no longer available from the regional registration authorities. Addresses can often only be acquired from someone that still has an existing claim on IPv4 addresses (but does not use all of them). This approach causes delays for new projects and businesses causing total stoppage due to unavailability of IPv4 resources.

8. Shadow market on IPv4 addresses

Up to now, IPv4 addresses have not been traded on a market – but the situation is now changing with the upcoming shortage. The implementation of further services may require the costly acquisition of IPv4 addresses, as they have become a limited asset. Each additional large project requiring additional IPv4 addresses may cause an extra growth in IPv4 address costs.

IPv6 addresses, on the other hand are available in great number via the Regional Internet Registries (RIRs). Introducing IPv6 and moving traffic to IPv6 can result in overall lowered acquisition costs for IP addresses.

9. (Re) Enabling the end to end communication

Today's local networks mostly operate with so-called "private IP addresses". Their use was not originally planned when the Internet was designed. In the public Internet only packets with public IP addresses will be routed, therefore an address translation between the address types must be established. This so called network address translation (NAT) is located at the Internet gateway of one's local network. Due to cooperation between governments, private organisations and companies sometimes multiple networks must be interconnected. Usually, at each network's edge a NAT gateway is in use. This inhibits the end to end view of the IP communication. At every point of the transmission even the network administrators only have a clear track up to the next

NAT gateway. Everything behind is hidden and hard to reach. In effect, this results in huge administration efforts in implementation and in troubleshooting of all those connection paths.

Furthermore, real-time communication profiles such as voice or video do not operate across NATs without special network appliances, causing additional costs in implementation and operation.

In IPv6, the former end to end paradigm of the Internet communication has been re-introduced. The NAT mechanism with private IP addresses is not available anymore in IPv6. Therefore, every communication is clearer and more direct which reduces administrative efforts and operational risks by increased transparency in the transport services.

10. Why removing NAT is not an issue

In marketing material for the gateway, vendors' Network Address Translation (NAT) evolved into a security feature. However, the security effects of NAT are a result of stateful ingress packet filtering and application layer gateways, features which are also available without address translation. The advertised hiding of local endpoint addresses behind a NAT firewall is a myth for many use cases, as for example the local IP address of a client can be read in every http-based browser session on the server side.

In IPv6, the strength of the public-to-private network border is in the strength of the gateway configuration with suitably customised, well deliberated rule sets, just like with IPv4 today. However, due to NAT and the absence of the address confusion, rules can be defined more clearly and therefore, with less risk of misconfiguration.

What we want to avoid?	What we want to achieve?
• Digital darkness	• Available e-services
• Broken connections	• Direct communication
• Stagnation of eGovernment services due to address shortage	• Secure network configuration
• Costs for gathering additional IPv4 resources	

Stay connected = Be IPv6 ready!!!

11. Policy background

The support of the new Internet Protocol version 6 has been implemented by some governments into their national policies. However, in the era of the global Internet, using IPv6 is not only a national, but rather a European issue. Policy support for IPv6 has been first mentioned in 2002 within the communication called "next Generation Internet – Priorities for action in migrating to the new Internet protocol IPv6". However, today's digital agenda for Europe is much more important for current decision makers and policy creators. These key European strategies encouraged, within the action 89, the member states to make eGovernment services fully interoperable while overcoming organisational, technical or semantic barriers and supporting IPv6. The need for providing electronic services via IPv4 plus IPv6 is also highlighted within the European eGovernment action Plan 2011-2015.

12. Recommendation for policy-makers

Based on analysis and long-term experiences from the GEN6 project, the following recommendations can be made in order to improve the provisioning of electronic services as well as the implementation of IPv6:

- **Involve** support for improvement of electronic services and IPv6 in strategic documents and policies.
- **Require** IPv6 support when renewing infrastructures and electronic services, preferably in the RFP (Request for Proposal) documentation.
- **Communicate** on a regular schedule with national domain registries since they are usually the ones who inform about various ways of IPv6 implementation.
- **Follow** awareness-raising and information events in order to learn about possible ways for upgrading software and hardware that need to be transformed to IPv6.
- **Maintain** permanent discussions among the experts, politicians and civil servants to exert pressure on the implementation of IPv6 and related current standards.
- **Provide** practical workshops for experts for learning and working with IPv6 and spread technical as well as organisational best common practices.

13. How to get informed?

Transition efforts exist in the public sector as well as in the private sector. In order to fulfil the European competitiveness and Innovation Framework Programme, we have to do our best to extend the European knowledge society. Transitioning to IPv6 requires learning and being familiar with best practices. Be active! Get involved! Learn and make sure you are keeping track. Information and ongoing discussions will prevent underestimation of this important issue and will help avoid possible mistakes in the future. The private and non-for-profit sector needs to be involved, too.

Figure 16: Private Sector-Public Sector

14. Best practices in government policy

In the Czech Republic, legislation made implementation of IPv6 mandatory for central government institutions. This government resolution, prepared by the Ministry of Industry and Trade in 2009 and extended in 2013, had a positive impact on IPv6 that resulted in considerable higher rank of IPv6 deployment. During the last one and half years, the IPv6 support on web-servers has increased from 36% to 57% by Ministries and from 50% to 82% by other central government institutions. Meanwhile national IPv6 average in the Czech Republic is 19.5% (January 2013) and by TOP 100 companies only 5%! The example shows that mandatory deployment of IPv6 can be an efficient tool to increase the readiness for IPv6 and that the public sector can give a positive example to private sector.

Especially in relation to the net neutrality there are interesting examples of policy implementation "General rules and recommendations for the use of data traffic management in the provision of Internet access service" which have been adopted by the Czech Telecommunication Office (CTU). According to these guidelines, "the access to the Internet" means a service enabling to connect all end user points connected via IPv4 or IPv6. This definition is related to the net neutrality and CTU clearly stated that net neutrality means also a freedom to choose an Internet protocol – IPv4 or IPv6 and the same rights are granted to IPv4 and IPv6 users.

15. Best practices in government address allocation

The routing between governmental networks over rented lines and the improvement of security by transparent routing can be significantly supported by using a homogenous IPv6 addressing space for the national government. For a central management of domestically used governmental IP addresses, each country needs a Local Internet Registry (LIR), registered with the RIPE NCC (see Figure 17). This is what has been done in Germany, and it is currently under discussion in Spain. Germany set up its central LIR called "de.government "in 2009. Upon extensive requests, the RIPE NCC allocated /26 prefix for this LIR.

Beneath the LIR de.government a set of Sub-LIRs were created to organise the IPv6 address deployment in Germany. Based on the /26 prefix, the LIR takes care of the (top level) management of the IPv6 addresses for the public administrations in Germany. A domestic address plan determines the use of the next six bits, after the /26 prefix. This way, one or more /32 prefixes are allocated to sub-LIRs as the basis for /48 site prefixes they hand out on request to their customers.

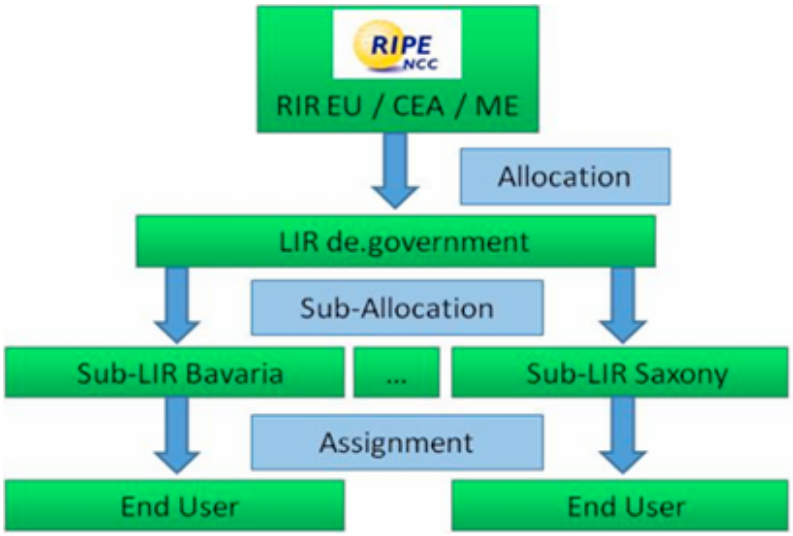


Figure 17: LIR de.goverment

16. Best practices in energy and green IT

The Greek pilot in GEN6 aims to influence the behaviour of the local school communities by raising their energy awareness. The pilot provides real-time energy efficiency services over IPv6 enabled grids to the local educational community, providing students with information on their energy consumption patterns and raising awareness among them on the energy savings that behavioural changes may bring. Through the implementation of the Greek IPv6 pilot, the deployed infrastructure has been extended and many problems that are related with the use of IPv4 for access to the smart energy meters have been solved. This extension provides a signal to European stakeholders that IPv6 technology can be an enabler for green IT.
Further reading at: http://www.gen6-project.eu/publications/booklets/

17. Best practices in emergency response systems

The aim of the advanced emergency response communications pilot or A-ERCS is to clearly demonstrate the state-of-the-art IPv6-enabled features in emergency response environments.

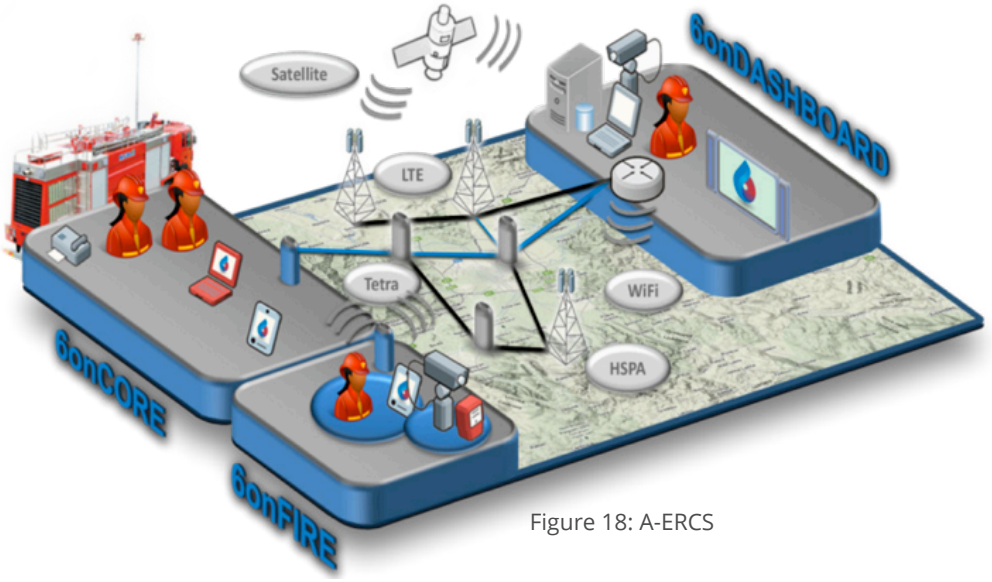


Figure 18: A-ERCS

More specifically, the A-ERCS pilot demonstrates:

- A scalable and robust overlay system for data transport and rich multimedia service built across both professional (e.g. DMR, TERA and satellite), commercial networks (e.g. UMTS/ HSPA, LTE) and ruggedized alternative commercial-of-the-shelf (cots) systems (mesh Wi-Fi and ad-hoc WiMAX).
- The ability of such a system to deliver seamless connectivity from targeted/affected areas across heterogeneous technologies and public networks, locally as well as on national and cross-border levels.
- Capabilities of the IPv6 technology to assist in deployment of automatic network planning and deployment capabilities, vital to all PPDR systems.
- IPv6 support for advanced features, such as network, node and host auto configuration, and self-organisation and self-healing characteristics.
- The ability of such a system to assure secure and QoS-enabled transmission of data, voice and multimedia-rich services system by relying upon modern professional and commercial telecommunications networks and IPv6-based technologies and features.

The A-ERCS pilot is part of 6inACTION, a broader PPDR communications and intervention management solution. Further information is available at: www.6inaction.net or refer to: http://www.gen6-project.eu/publications/booklets/.

18. Best practices in backbone transition

The Spanish IPv6 transition pilot within the GEN6 project is implemented by the Ministry of Finance and Public Administration (MINHAP) and the Ministry of Industry, Energy and Trade (MINETUR), with the collaboration of the University of Murcia. It aims to foster the IPv6-readiness of eGovernment services, with a pragmatic approach based on the following principles:

- Building upon the infrastructure already in place, making the most of the IPv6 capabilities of the existing hardware, software and networks;
- Relying on the use of shared services, increasing efficiency in the use of the existing resources, and avoiding divergence in technologies and solutions;
- Providing enough flexibility for accommodating the various transition paths of the different administrative units (IPv4 and IPv6 coexistence);
- Ensuring experience from the early adopters of IPv6 of what is shared and used by all administrations softening transition.

The pilot takes advantage of the existence of Red SARA (SARA network), operated by MINHAP, which connects all Spanish Public Administrations, as well as the shared services that Red SARA provides. Further reading: http://www.gen6-project.eu/publications/booklets/.

19. Best practices in datacentre transition

The German pilot aims to transition the Citkomm datacentre infrastructure in the municipality of Iserlohn, transitioning several applications to an IPv6-enabled dual-stack scheme. The local IPv6 infrastructure will be implemented in the "de.government" IPv6 address space and will be connected to the DOI network of German administrations.

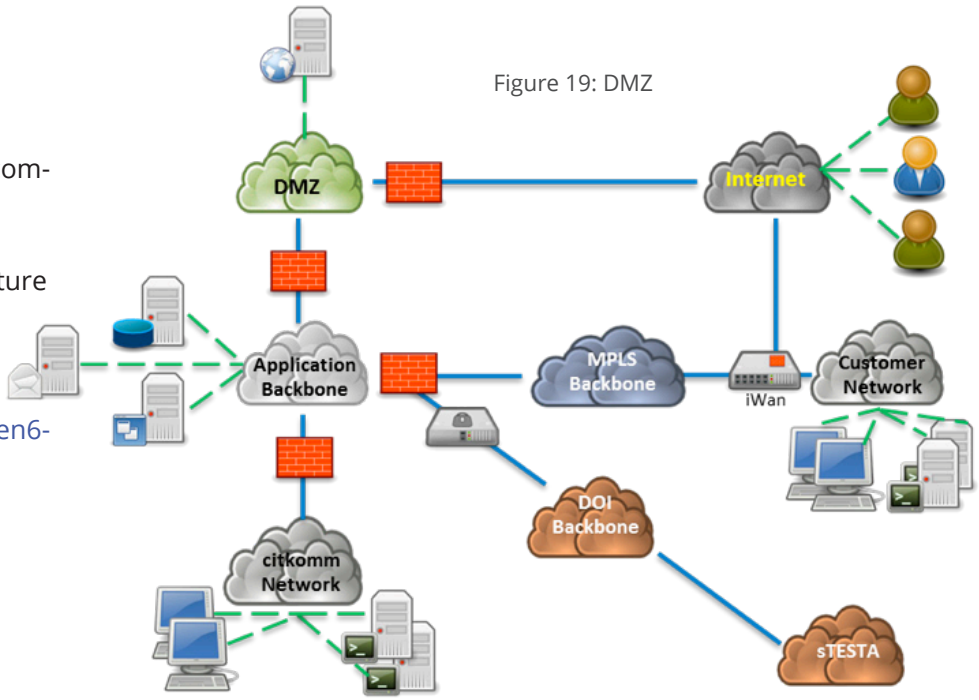
Besides the specific applications themselves, this requires the network and the local infrastructure including all clients to be IPv6 enabled as well. The work on the application backbone differentiates between the inner backbone, providing specific application services to the employees of the local government, and the outer backbone – commonly known as de-militarised zone (DMZ in Figure 19) – offering e-government services, portal applications and web presentations to the citizens.

The transition of a datacentre encompasses the following areas:

- Network Infrastructure
- Application Backbone Infrastructure
- Customer environment
- Migrating from TLS/SSL to IPsec

Further reading at: http://www.gen6-project.eu/publications/booklets/.

Figure 19: DMZ



20. Best practices in eGovernment service transition

The eGovernment Gateway (EGG) is an existing service and offers a central access to around 200 eGovernment services to more than 13 million registered users in Turkey. Around 50,000 new citizens subscribe to EGG every day. These numbers point out the public interest on this service and reveal possible wide impact of enabling IPv6 on such a service. The experience to be gained by the realisation of such a big-scale pilot project in the scope of the GEN6 project allows best practices, guidelines, methodologies and toolkits for the transition of e-Government services all around Europe. The main goal throughout the pilot was to make the EGG portal and candidate EGG services IPv6-enabled.

Further reading: http://www.gen6-project.eu/publications/booklets/.

All these pilots are showing why the transition to IPv6 is unavoidable. They can provide inspiration regarding where to start the transition, what might happen during this phase and provide information about what needs to be done and what to avoid.

5 • ETSI IPv6 Integration – Industry Specification Group

ETSI IPv6 Industry Specification Group (IP6 ISG), Sophia Antipolis, 27 April 2015

IP6 Industry Specification Group to help stakeholders adopt IPv6 and anticipate IPv4 address exhaustion.

ETSI's newly established IP6 Industry Specification Group (ISG), created to focus on better IPv6 integration and deployment and held its kickoff meeting on 22nd – 23rd April at ETSI, Sophia Antipolis, France.

IPv6 was developed to address IPv4 address exhaustion and enable new Internet services with improved end to end security. ETSI's new specification group will focus on scenarios, use cases and best practices to foster IPv6 integration and deployment in a variety of targeted communities. The first targets will be governments, enterprises, emergency and public safety organisations, Internet service providers and mobile operators, academia and education. Use of IPv6 in new technologies will also be addressed, in particular Internet of Things and Machine to Machine communications, Software Defined Networking and Network Functions Virtualisation, cloud computing and smart grids, to name a few. But overall, IP6 ISG will focus on integrating the IPv6 protocol into the next generation of mobile telecommunications, 5G systems, looking at the complete wireless network and the full spectrum of mobile wireless technologies.

At this first ISG meeting, Mr. Latif Ladid was elected as Chairman of the group. He is currently the president of the IPv6 Forum and a Research Fellow at the University of Luxembourg. Mrs. Yanick Pouffary and Mr. Patrick Wetterwald, respectively from Hewlett-Packard and Cisco Systems, were elected as Vice-Chairpersons.

"IP6 ISG was created to help guarantee the growth of the Internet and make sure that all parts of the world, including Africa, Latin America and Asia, will be connected, as we are running out of IPv4 addresses", says Luis Jorge Romero, ETSI Director General. "*Some large mobile operators have already implemented this protocol and with the arrival of the Internet of Things and the growing number of connected devices round the world, IPv6 becomes a necessity.*"

Widespread adoption of IPv6 has been slow but new Internet services are driving IPv6 deployment and if the current trend continues, we should achieve 50% penetration by 2017. IPv6 uses a 128-bit address, allowing 2128 addresses, that is more than 7.9×1028 times as many as IPv4, this much larger address space should be sufficient for the foreseeable future. IPv6 also offers many other benefits and enhanced features compared to IPv4, such as simplified processing by routers, Quality of Service, security, IP mobility, etc. But it must cope with the demand and anticipate the full expansion of Internet requirements in all parts of the world, without creating a digital divide, providing everyone and all industries with the IP addresses they need.

Participation in the IP6 Industry Specification Group is open to all ETSI members as well as organisations who are not members, subject to signing ISG Agreements. For more information on how to participate please contact ISGsupport@etsi.org.

Table 7 below outlines the work items under progress:

IP6		
IP6(15)002012	Draft	IPv6-based SDN and NFV Deployment of IPv6-based SDN and NFV
IP6(15)002010	NWI	DGS-0016 :IPv6-only App: SixChat leveraging on IRP
IP6(15)002005	NWI	DGS-0014 :IPv6 based Tactile Internet
IP6(15)001034r1	NWI	IPv6 Deployment in Privacy
IP6(15)001034	NWI	IPv6 Deployment in Privacy
IP6(15)001033	NWI	IPv6 Deployment and Security
IP6(15)001013r1	NWI	IPv6-Based 5G Mobile Wireless Internet
IP6(15)001011r1	NWI	IPv6-based SDN & NFV
IP6(15)001012r1	NWI	IPv6-based Industrial Internet leveraging on 6TiSCH technology
IP6(15)001010r1	NWI	IPv6-based Internet of Things
IP6(15)001017r1	NWI	IPv6-based Cloud Computing
IP6(15)001025r1	NWI	Generic migration steps from IPv4 to IPv6
IP6(15)001014r1	NWI	IPv6 For Governments
IP6(15)001015r1	NWI	IPv6 For Academia & Education
IP6(15)001006r1	NWI	IPv6 in Safety & Emergency Sector
IP6(15)001005r1	NWI	IPv6 in Telecom /ISPs
IP6(15)001004r1	NWI	IPv6 Deployment in the Enterprise
IP6(15)001028	Other	IPv6 IOT
IP6(15)001027	Other	Autonomic Networking with IPv6
IP6(15)001026	Other	IPv6 Service Yang Model
IP6(15)001025	NWI	Generic migration steps from IPv4 to IPv6
IP6(15)000001	Other	Slides on IPv6 for Academia and Education
IP6(15)001022r1	NWI	Security Implications of IPv6 on IPv4-only and dual-stack Infrastructures
IP6(15)001023	Other	Pascal's slides on IoT vs. IPv6
IP6(15)001022	NWI	Security Implications of IPv6 on IPv4-only and dual-stack Infrastructures
IP6(15)001017	NWI	IPv6-based Cloud Computing
IP6(15)001016	NWI	DGS-0015 : Impact of Mobile IPv6
IP6(15)001018	NWI	IPv6-based Autonomic Networking
IP6(15)001015	NWI	IPv6 For Academia & Education
IP6(15)001014	NWI	IPv6 For Governments
IP6(15)001013	NWI	IPv6-Based 5G Mobile Wireless Internet
IP6(15)001012	NWI	IPv6-based Fringe Internet & 6TiSCH
IP6(15)001011	NWI	IPv6-based SDN & NFV
IP6(15)001010	NWI	IPv6-based Internet of Things
IP6(15)001009r1	NWI	Impact of Mobile IPv6
IP6(15)001009	NWI	Impact of Mobile IPv6
IP6(15)001008r1	NWI	IPv6-based Cloud Computing
IP6(15)001008	NWI	IPv6-based Cloud Computing
IP6(15)001007	NWI	IPv6 in Security & Privacy Sector

Source: https://portal.etsi.org/tb.aspx?tbid=827&SubTB=827

Two scenarios have been selected for this Enterprise and 5G paper, mainly the enterprise sector which will be the toughest field to win as the ROI is the prime driver to mobilise new IT budgets to update the ICT infrastructure. The second scenario chosen is 5G, a Greenfield opportunity to specify IPv6 only from the outset as it is demonstrated by the deployment of 4G networks that IPv6 adds tremendous features over and beyond the IPv6 address space. These papers are still work in progress but summarises very well what needs to be addressed in the needed steps to investigate when deploying IPv6 in these networks.

6 • IPv6 Deployment in the Enterprise[43]

1. Introduction

There are many scenarios/variations to enable IPv6 within the enterprise world; however, there is no "one size fits all" answer. This document does not attempt to provide guidance for all possible networking situations. Enterprise network architects must each take the responsibility of choosing the best solution for their own case.

Let's review history; when IPv4 emerged as the standard Internet protocol in the 1980s, the address space—some four billion IP addresses—seemed more than adequate. Today it is clearly no longer the case because the world has moved from IP enabled to IP dependent. In fact, we have run out. With the growing number of users and the proliferation of smart devices and things, IPv4 address space exhaustion is a major Information and Communications Technology (ICT) issue. The current IPv4-based Internet can no longer sustain the explosive growth of ICT. Any organisation that relies on the Internet to any extent must be prepared to support IPv6. The move to IPv6 is inevitable, as the Internet is the cornerstone of our connected society. Furthermore, IPv6 offers important business and technical advantages. Among them: higher performance, enhanced mobility, automated management, built-in multicasting for multimedia applications, enhanced security, simplified administration and many more. Enterprises may be tempted to put off transitioning to IPv6 until some later date because all existing IPv4-based infrastructures will continue to work after the last IPv4 address is issued. Postponing the inevitable, however, can put an enterprise at a competitive disadvantage. As more and more customers operate in an IPv6 world, companies supporting only IPv4 risk being shut out of high-growth markets because they are unable to reach—or be reached by—these customers. The fallacy in this position is that maintaining IPv4-only communications can put enterprises at a competitive disadvantage. Seamless, pervasive connectivity is an integral part of doing business today.

2. Core principles

There are three core principles to shape IPv6 network development:

- The first principle is to maintain a standards-based approach and avoid proprietary technologies. Embracing open standards allows the use of best-of-breed products for whatever needs arise. A network build on open standards will have interoperability with the broadest base of users and partners.
- The second principle is planning. Without proper planning, the transition will be plagued with rework and missteps.
- The third principle is repeatability of the network design across the network (a standard set of requirements, and a standard solution design to meet the enterprise network requirements).

Such standardisation increases efficiency in building out the network, and also makes it easier to troubleshoot the network in each location.

[43] Author Yanick Pouffary, Vice-Chair, ETSI IP6 ISG

3. IPv6 Transition strategies in Enterprise Networks

The vast majority of devices, laptops, desktops, operating systems, switches, routers, content providers, carriers, and Internet service providers (ISPs) support native IPv6 today at no extra cost, which makes it possible to deploy a network based on IPv6. However, enterprises typically purchased and configured their network to support IPv4 traffic only. And while most equipment can be software enabled, some may need to be replaced to add support for IPv6. Furthermore, even if the capabilities to operate in a dual network configuration exist, additional planning steps, and architecture design will most likely be required. Similarly management systems and security systems that can support both environments are necessary. Enterprises must also verify that applications they use can operate correctly and are IPv6-enabled.

Because IPv4 and IPv6 will coexist for some time, a phased deployment is recommended to minimise the impact of the transition and keep costs manageable. Recognising that IPv4 and IPv6 will run parallel to each other for the foreseeable future, IETF established three standard transition mechanisms: each of these techniques has advantages and trade-offs. The optimal solution will depend on a variety of factors, including the enterprise's current environment and long-term goals. It may also encompass all three transition mechanisms. It is important to understand that one method does not fit all.

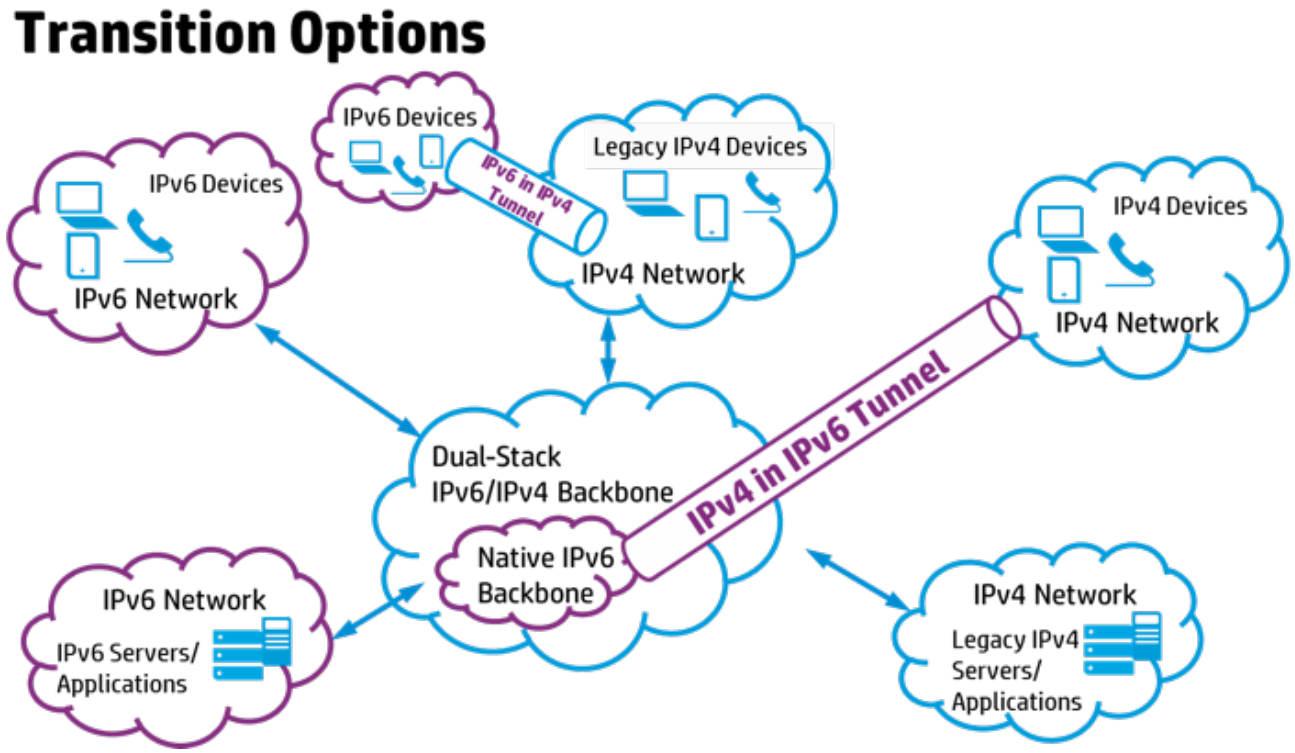


Figure 20: Transition Options

In planning the IPv6 initiative, the following three key families of mechanisms enable the transition:

- **Dual-stack** - Provides support for both protocols on the same device to allow for communications with both IPv4-only and IPv6-only nodes. This mechanism is the most versatile. A dual stack transition strategy enables a very smooth transition and will likely remain a part of the worldwide Internet infrastructure for years to come, until IPv4 is fully retired.
- **Tunnelling** - Encapsulates IPv6 packets in IPv4 headers (or vice-and-versa). Tunnelling enables the network team to create islands of IPv6 or IPv4 capabilities, and in the short term, to connect them over the existing IPv4 network. Tunnelling enables networks in transition to take advantage of IPv6 services while remaining connected to the IPv4 world.
- **Translation** - Between IPv4 and IPv6, enterprises should also implement a procurement policy to ready the network backbone so that IPv6 can be turned on without having to do a fork and replace physical hardware.

The main IPv6 transition deployment models that are being discussed are listed below:

- **IPv4 only:** Delays the introduction of IPv6 to a later date and remain an all-IPv4 network. Over the long term, it is expected that this migration strategy will lead to problems and increased costs. Due to the increase in traffic there will be an increased demand for IP addresses and the usage of NAT in the carriers' network, denoted as Carrier Grade Network Address Translation (CG-NAT). In particular, all traffic to and from the Internet will have to pass CG-NAT. Furthermore, growth in bandwidth demand can only be handled with increased CG-NAT capacity, which has a higher cost and single point of failure.
- **Coexistence of IPv4 and IPv6:** Requires the use of a dual-stack, introducing IPv6 in the network next to IPv4. Please note, however, that dual-stack networks are more complex to deploy, operate, and manage. Furthermore, this option also requires an address management solution for both IPv4 and IPv6 addresses.
- **IPv6 only:** Introduces IPv6 in the network and removes IPv4 completely. This approach can provide benefits because IPv6-only networks are simpler to deploy, operate, and manage. Moreover, an address management solution is required only for IPv6 addresses. However, the problem with this approach is that many devices, websites, and applications still only work on IPv4; therefore, moving to an IPv6-only network may lead to differences in network quality. That is why **NAT64** should be offered in addition to offering IPv6 only.

4. Preparation and Assessment Phase

- Planning
- Assessment – Network and application readiness
- Acceptance criteria
- Security Policy
- Tools Assessment
- Applications Assessment

5. Architecture

Address Plan

One of the first choices a network designer needs to make is the type of addresses to be used in the network core. Should the network use provider-independent global addresses, «private» addresses (either RFC 1918 addresses or unique-local addresses) or something else? A related choice is whether to use only link-local addresses on certain links.

- [REF IETF ID draft-ietf-v6ops-design-choices-08] PI - Globally-unique IPv4 or IPv6 addresses obtained directly from an address registry. An organisation which has such addresses is considered to have «its own» address space.
- PA - Globally-unique IPv4 or IPv6 addresses obtained from an upstream provider. Such addresses must be returned if the relationship with the upstream provider ceases.
- Private - Either RFC 1918 IPv4 addresses or unique-local IPv6 addresses [RFC4193].

Routing

- Choice of IGP & BGP.
- Choice separation of IPv4 and IPv6?
  - To what degree should IPv4 and IPv6 traffic be kept separate?
  - To what degree should IPv4 and IPv6 routing information be kept separate?
- External connectivity choices.

Security

Security must be applied to both IPv4 and IPv6. IPv6 is not so different than IPv4 since it is a connectionless network protocol using the same lower-layer service and delivering the same service to the upper layer. Therefore, the security issues and mitigation techniques are mostly identical with the same exceptions that are described further.

6. Campus and Datacentre

- Datacentre Virtualisation
- Campus Networks

7. Lessons Learned: IPv6 touches everything

What has industry learned along the way? First and foremost, that introducing IPv6 is a long journey. Dual-stack network infrastructure will likely endure for many years, for as long as IPv4-only devices remain in place. In the meantime, organisations that rely on the Internet must undertake a transition now. Remember by the time the network is asked for IPv6 for competitive purposes, it will be too late.

Another key lesson is that IPv6 is not just a network challenge. Moving to IPv6 is more than a network protocol upgrade since everything in IT is connected to the network, and the network in turn touches everything in the IT environment. It requires an across-the-board, holistic-IT approach. It touches everything from server and desktop operating systems to office productivity suites, ERP platforms, email, web services, and management software and security tools. IPv6 impacts the entire IT ecosystem.

One key aspect that is often underestimated by some IT professionals is the challenge of application IPv6 enablement. While providers of off-the-shelf software have been dealing with this challenge by writing applications to be IP version independent, home-grown applications are behind and will also need to be updated to accommodate IPv6. Application teams are going to have to add IPv6 support to their applications and test IPv6 in their applications. Enablement of IPv6 applications takes place one application at a time.

Plan ahead with partners, users - and achieving IPv6 deployment is not entirely within any single organisation's hands. Beyond internal infrastructure and applications, every organisation must plan with partners and end-users. When you transition to IPv6, you have to inventory all your content. You have to have conversations with your partners and suppliers to make sure they're ready to move forward, too.

8. Future Impact

The prospect of transitioning to IPv6 may be daunting, but everyone who relies on the Internet faces the challenge. The worst mistake is assuming the IPv6 transition can wait. Anyone who relies exclusively on IPv4 will eventually be put at a competitive disadvantage. The legacy IPv4 based Internet can no longer grow. Without deployment and support of IPv6, it is just a matter of time before networks/businesses become isolated and unable to communicate. The transition to date has been gradual but the steep curve is starting and it is critical to be prepared. For the past 30 years, the IT industry has embedded IPv4 related knowledge in all its processes, in all its infrastructure gear like network management tools, load balancers, firewalls and unfortunately, in all applications. So it will take time.

There is not a single recipe for IPv6 transformation. Each enterprise is unique and depends on its unique business goals, long-term vision, and constraints. It is critical to put in place a joint Business & IT Task Force. This will help to ensure a smooth path toward IPv6. A pragmatic roadmap for an IPv6 transition, while also developing clear business benefits that can be achieved through the transition.

9. Reference Guides

The following documents from the IETF provide guidance on strategies for adding IPv6 to a network:

- Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment (2011) - RFC6180 for general advice.
- Enterprise IPv6 Deployment Guidelines (2014) - RFC7381 and IPv6 Enterprise Network Analysis - IP Layer 3 Focus (2007) - RFC4852.
- IPv6 Unicast Address Assignment Considerations - RFC5375 for creating an IPv6 addressing plan as well as Some Design Choices for IPv6 Networks – IETF ID draft-ietf-v6ops-design-choices-08.
- Mobile Networks Considerations for IPv6 Deployment (2011) - RFC6342 for mobile network providers.
- Wireline Incremental IPv6 (2012) - RFC6782 for wireline service providers.

7 • IPv6-based 5G Mobile Wireless Internet [44]

1. Introduction

The fifth generation of mobile technology (5G) will address the demands and business contexts of 2020 and beyond. Moreover, it is expected that (1) the future European society and economy will strongly rely on 5G infrastructure, (2) its impact will go far beyond existing wireless access networks with the aim for communication services, reachable everywhere, all the time, and faster and (3) 5G technology will be adopted and deployed globally in alignment with developed and emerging markets' needs.

According to [5GPPP], several key drivers and disruptive capabilities will help the adoption and deployment of 5G globally. In particular, regarding the key drivers, 5G will ensure user experience continuity in challenging situations such as high mobility (e.g. in trains), and very dense or sparsely populated areas, and journeys covered by heterogeneous technologies. At the same time 5G will be the key enabler for the Internet of Things (IoT) by providing a platform to connect a massive number of sensors, rendering devices, and actuators with stringent energy and transmission constraints, as seen in Figure 21. In addition, new mission critical services will be deployed, requiring very high reliability, global coverage and/or very low latency, which are up to now handled by specific networks, typically public safety, will become natively supported by the 5G infrastructure.

Moreover, it is expected that 5G will integrate networking, computing and storage resources into one programmable and unified infrastructure, which will allow for an optimised and more dynamic usage of all distributed resources and the convergence of fixed, mobile and broadcast services. This unification will also enable 5G to support multi tenancy models, enabling operators and other players to collaborate in new ways.

5G will leverage on the cloud computing concepts and will stimulate paving the way for virtual pan European operators relying on nationwide infrastructures.

Another important key driver is that 5G is being designed to be a sustainable and scalable technology. This can be realised by firstly, the telecom industry which will stimulate and work towards a drastic energy consumption reduction and energy harvesting. Moreover, sustainable business models for all ICT stakeholders will be enabled by cost reductions through human task automation and hardware optimisation.

One of the most important key drivers is that 5G will create an ecosystem for technical and business innovation. This will be enabled by the fact that network services will rely more and more on software, while the creation and growth of start-ups in the sector will be encouraged. Furthermore, the 5G infrastructures will provide network solutions and involve vertical markets such as automotive, energy, food and agriculture, city management, government, healthcare, smart manufacturing, public transportation and water management.

[44] Author and Rapporteur: Georgios Karagiannis, ETSI IP6 ISG

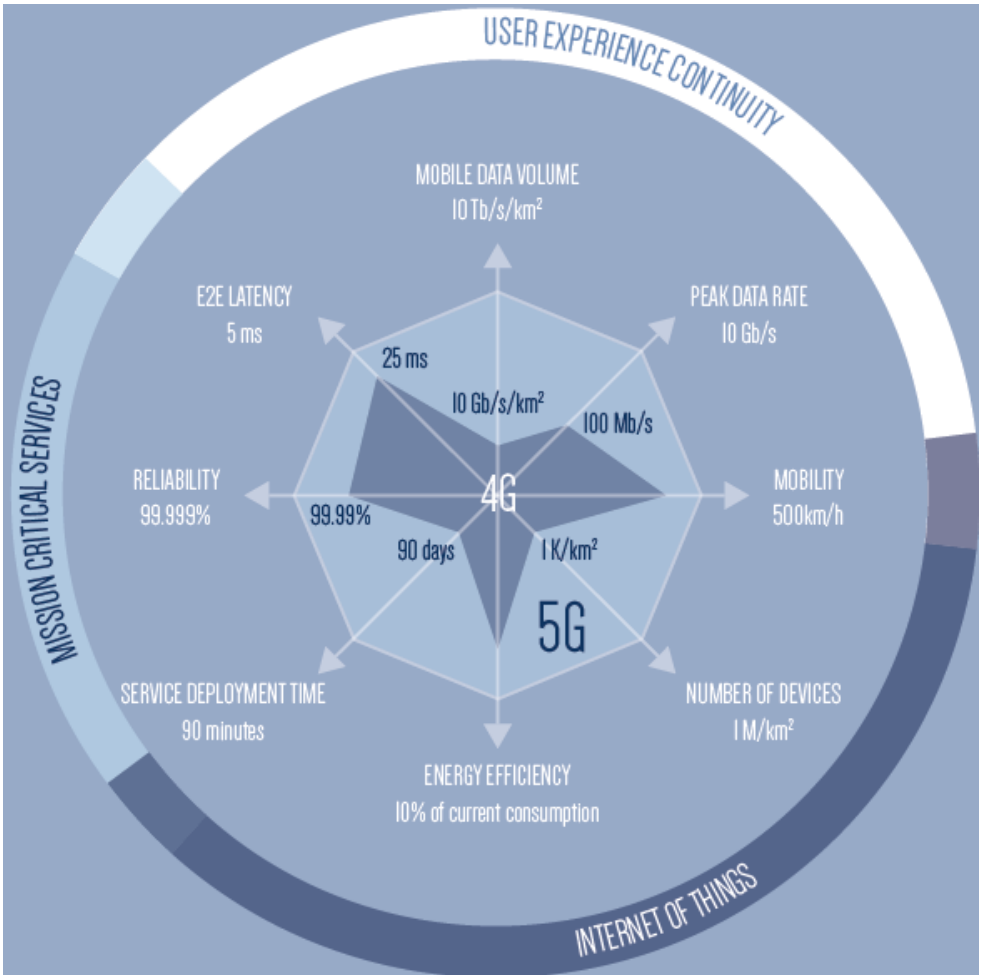


Figure 21: 5G Key drivers and disruptive capabilities, copied from (5GPPT)

Moreover, with the rapid development of the 5G network infrastructure, as well as other technology enablers such as IoT, mobile Internet, cloud computing, SDN, virtualisation, smart home and Internet of vehicles, there is a consensus between different stakeholders that the Internet demand is no longer limited to exhausting IP addresses, but extends to the end-to-end interconnection and permanently stable IP addresses as seen in Figure 22 and 23. Moreover, it has a higher requirement for the security, management, maintenance as well as the operation of the next generation Internet. One of the main challenges associated with the above statement is associated with how gradually to stop IPv4, deploy IPv6 in full scale and start using the Internet of the 21st century.

2. IPv6 Transition strategies in Mobile Networks

Currently several IPv6 migration strategies can be identified. The main IPv6 migration strategies that are being discussed by Mobile Network Operators (MNOs), see e.g. [ALU-IPv6] are listed below:

- **IPv4 only:** Delays the introduction of IPv6 to a later date and remain an all-IPv4 network. Over the long term, it is expected that this migration strategy will lead to problems and increased costs for the MNO. Due to the increase in traffic, refer to Section 8.4 5G requirements, there will be an increased demand for IP addresses and on using NAT in the carriers network, denoted as Carrier Grade Network Address Translation (CG-NAT). In particular, all traffic to and from the Internet will have to pass CG-NAT. Furthermore, growth in bandwidth demand can only be handled with increased CG-NAT capacity, which has a higher cost. This will mean that the MNO is unable to benefit from the increasing ratio of IPv6-to-IPv4 Internet traffic. This mechanism works only for DNS-based applications; IPv4-only.
- **Coexistence of IPv4 and IPv6:** Requires the use of a dual-stack, introducing IPv6 in the network next to IPv4. For a MNO, this approach is a less desirable option because dual-stack networks are more complex to deploy, operate, and manage. Furthermore, this option also requires an address management solution for both IPv4 and IPv6 addresses.
- **IPv6 only:** Introduces IPv6 in the network and removes IPv4 completely. This approach can provide benefits for a MNO, because IPv6-only networks are simpler to deploy, operate, and manage. Moreover, an address management solution is required only for IPv6 addresses. This results on the fact that there is no impact on scale, charging, and roaming because only a single bearer with a single stack is required. However, the problem with this approach is that many UE (User Equipment) devices, websites, and applications still only work on IPv4 and moving to an IPv6-only network may lead to inferior service for MNO customers, resulting in customer dissatisfaction.
- **Enhanced IPv6 only + NAT64:** In addition to offering IPv6 only, IPv4 is offered as a service over IPv6 for DNS-based applications. For the MNO, benefits from the IPv6 only strategy that there is no impact on scale, charging, and roaming as only a single bearer with a single stack is required. DNS64 (Domain Name System 64) also embeds IPv4 Internet destinations in IPv6 addresses. However, non-DNS applications are not supported and will be broken, which could result in a lower quality service for the operator's customers.
- **Enhanced IPv6 only + 464XLAT:** This strategy of IPv6 only + NAT64 solution solves at the same time, the drawback associated with the support of non-DNS applications. In particular, for IPv4-only, non-DNS applications, IPv4 packets are translated to IPv6 packets by the UE and subsequently are translated back to IPv4 packets by a central CG-NAT64, which is deployed behind the PGW (PDN Gateway).

More details will be provided in a subsequent version of this document.

3. 5G Architectures

This section briefly presents the 5G architecture proposed by [NGMN] and [5GPPP]. Further details will be provided in a subsequent version of their documents.

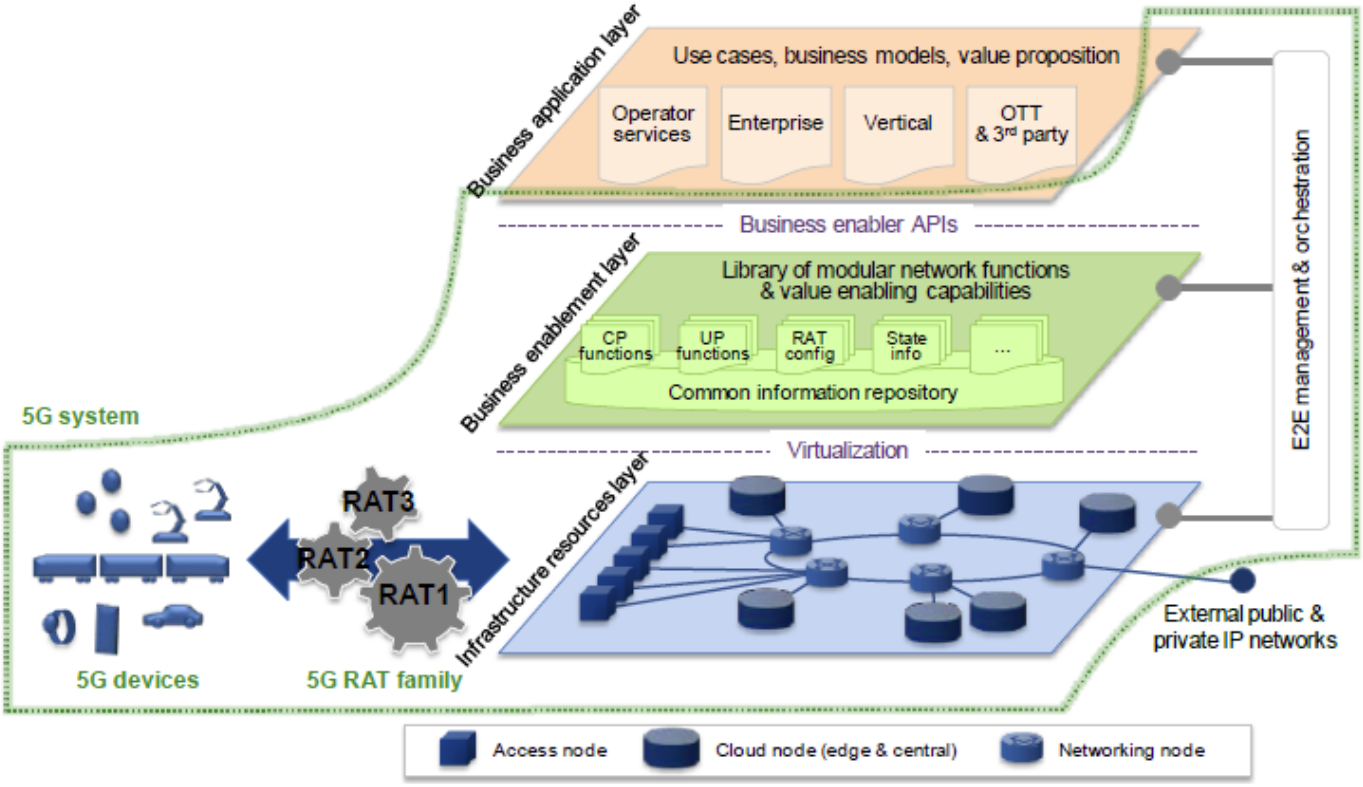


Figure 22: 5G Architecture, copied from (NGMN)

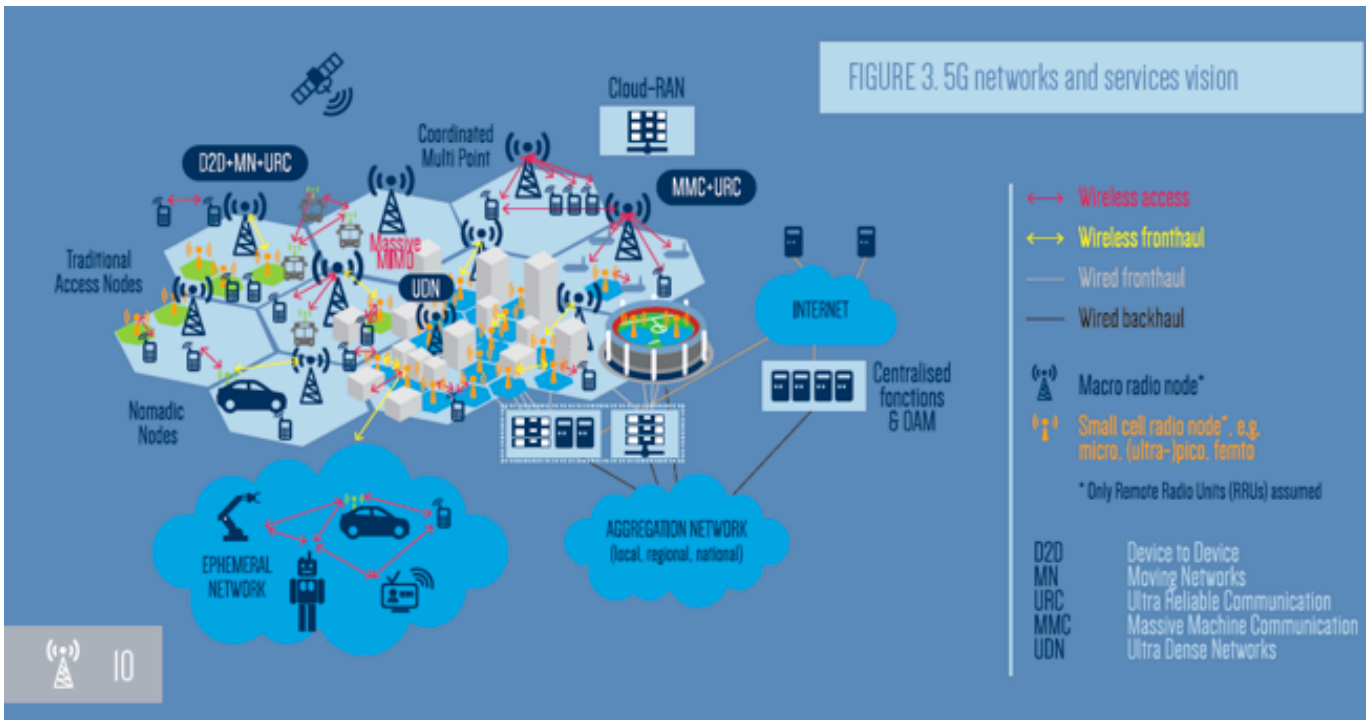


Figure 23: 5G Architecture, copied from (5GPPP)

4. 5G Key Requirements

This section is based on the 5G requirements proposed in [NGMN]. Further details will be provided in a subsequent version of that document.

The 5G requirements derived by [NGMN] are:

- **User Experience**
  - Consistent User Experience
  - User Experienced Data Rate
  - Latency
  - Mobility
  - User Experience KPIs
- **System Performance**
  - Connection Density
  - Traffic Density
  - Spectrum Efficiency
  - Coverage
  - Resource and Signalling Efficiency
  - System Performance KPIs
- **Device Requirements**
  - Operator Control Capabilities on Devices
  - Multi-Band-Multi-Mode Support in Devices
  - Device Power Efficiency
  - Resource and Signalling Efficiency
- **Enhanced Services**
  - Connectivity Transparency
  - Location
  - Security
  - Resilience and High Availability
  - Reliability
- **New Business Models**
  - Connectivity Providers
  - Partner Service Provider and XaaS Asset Provider
  - Network Sharing Model
- **Network Deployment, Operation and Management**
  - Cost Efficiency
  - Energy Efficiency
  - Ease of Innovation and Upgrade
  - Ease of Deployment
  - Flexibility and Scalability
  - Fixed-Mobile Convergence
  - Operations Awareness
  - Operation Efficiency
  - Ultra Low-cost Networks for Very Low-ARPU Areas
  - Ultra Low-Cost Networks for Very Low-ARPU MTC Services

An additional requirement is the demand of deploying and using an Internet technology that has (1) a non-exhausting IP address range and (2) is able to provide end-to-end interconnection and permanently stable IP address, and (3) which has a higher requirement for the security, management, maintenance as well as the operation of the next generation Internet.

5. Benefits of applying IPv6 in 5G

Work is ongoing to show how IPv6 will provide benefits to the solutions imposed by these requirements. In addition, the sooner a cohesive strategy for 5G and IPv6 is developed and applied among those in standardisation and research, the benefits and risks of using IPv6 in 5G will be validated. Overall, this will enable the fast deployment and success of 5G. In subsequent versions of 5GPPP documents, the conclusions and next steps associated with the objectives, the technology guidelines, the step-by-step process, the benefits, the risks, the challenges and the milestones of deploying the IPv6-based 5G Mobile Wireless Internet will be presented.

Conclusion

In a well-run relay race, the baton-holder is supposed to sprint into the exchange area, only slowing down as the second runner speeds up to grab the baton. It is a critical time, in which either runner might fail to make the exchange and drop the baton or when confusion can translate into lost time. The IPv6 transition is at perhaps a similar critical juncture. IPv4 is nearing the end of its leg, IPv6 has not yet completely cranked up to speed, and for a time, they will both be running side-by-side.

Government policy-makers, regulators, international organisations, standards bodies, stakeholder groups, companies, ISPs, and operators – all of them may be required to pass the baton to the new protocol. The complexity of the process, with its technological, economic, and political dimensions, reflects the real diversity of Internet governance as it has evolved today. Ultimately, this diversity equals strength, but it may take some time to accelerate IPv6 adoption to reach the critical impetus for Internet expansion and technology improvements. As in a relay race, the transition indicates how well the multiple participants – all of the stakeholders involved in IPv6 – can work together. Undoubtedly, the process will provide lessons and pave the way for future improvements in the field of IP addressing and Internet governance in general. For now, the race is still being run, with the expansion of the global Internet as the ultimate prize.

To understand the complexity of this transition process and how governments and multi-stakeholder groups can facilitate it, the following aspects must be considered:

- The importance of IP addressing, its distribution worldwide and its key function in a data- intensive world of online services, applications and networks that is putting strain on the availability of addresses;
- The status of IPv6 deployment and adoption trends from IPv4 to IPv6;
- The costs entailed in IPv6 adoption;
- The main roadblocks/challenges in deploying and transitioning to IPv6, such as a lack of business incentives or consumer awareness, as well as technical incompatibility and security issues;
- The existing policies, regulatory measures and guidelines developed to support the transition from IPv4 to IPv6;
- The best practices and recommendations that can encourage, facilitate and support a swifter adoption of IPv6;
- Potential innovative steps that policy-makers could take to accelerate or facilitate IPv6 deployment; and
- Measures already taken by the ITU, industry, and governments to promote awareness of the criticality of IPv6 deployment.

The deployment of IPv6 has not resonated very well with the business sectors in much the same way as IPv4 for the simple reason it was not IPv4 that was promoted by the Internet while IPv6 is an upgrade and like any upgrade it needs a real business case beyond the depletion of the IP address space.

Annexes

Annex 1: Preparing an IPv6 Address Plan

Courtesy **Sander Steffann**,
IPv6 Expert, Trainer and Consultant at Steffann
(http://www.steffann.nl/site/)

In an efficient IPv6 address plan, the IPv6 addressing ranges are grouped effectively and logically.

This has several advantages, including:

- Security policies are easier to implement, such as the configuration of access lists and firewalls.
- Addresses are easier to trace: the address contains information about the use type or location where the address is in use.
- An efficient address plan is scalable: it can be expanded, for example, to include new locations or use types.
- An efficient IPv6 address plan also enables more efficient network management.

IPv4 addresses have run out, and more and more businesses and institutions see the necessity to migrate to IPv6. As a result, they need an IPv6 address plan. An IPv6 address is 128 bits long, which means that, in theory, there are 2128 addresses available, a great deal more than the 232 (= 4.3 billion) addresses available with IPv4. To give you an idea of the volume: 2128 or 340 282 366 920 938 463 463 374 607 431 768 211 456 or 340 billion billion billion billion represents approximately the number of grains of sand on our planet. This means that an IPv6 address plan will look very different from an IPv4 address plan.

An address plan using the IPv4 system limits the options available to an organisation because there are relatively few IPv4 addresses still available. This is why the IPv4 addressing system is based on efficient address assignment. If you apply for an IPv6 address range at many Internet Service Providers, you will be assigned 280 addresses (a/ 48 prefix). This is such a huge amount that efficiency virtually ceases to be an issue. This is why it is worthwhile adopting an IPv6 address plan: a system in which you assign the IPv6 addresses to locations and/or use types.

In an efficient IPv6 address plan, the IPv6 addressing ranges are grouped effectively and logically. However, an efficient IPv6 address plan may "waste" large numbers of IPv6 addresses. In almost all cases, this is a good trade-off: seemingly wasteful practices lead to more efficiency elsewhere, for instance, by avoiding unnecessary inflation of routing tables in routers. The addresses are there; you may as well use them. This manual will show you how to prepare an effective IPv6 address plan. In making that plan, you will need to make a number of important choices. Please think carefully about these choices to ensure that the address plan will meet the requirements of your organisation. This manual will provide suggestions to help you to make the right choices.

Download the IPv6 Address Plan Document: http://www.ipv6forum.com/dl/presentations/IPv6-addressing-plan-howto.pdf

Annexes

Annex 2: IPv6 Readiness & Procurement Guidelines

Authors: **Merike Käo, Jan Žorž, Sander Steffann**
Courtesy of **Jan Žorž**,
Operational Engagement Programme Manager,
Internet Society

Abstract: To ensure the smooth and cost-efficient uptake of IPv6 across their networks, it is important that governments and large enterprises specify requirements for IPv6 compatibility when seeking tenders for Information and Communication Technology (ICT) equipment and support.

This document is intended to provide a Best Current Practice (BCP) and does not specify any standards or policy itself. It can serve as a template that can be used by governments, large enterprises and all other organisations when seeking IPv6 support in their tenders or equipment requirements and offer guidance on what specifications to ask for. It can also serve as an aid to those people or organisations interested in tendering for government or enterprise contracts.

Be aware that the standards listed here have their origin in various bodies, which operate independent of the RIPE community, and that any of these standards might be changed or become replaced with a newer version. You may also need to adjust the recommendations to your specific local needs. Some parts of this section are loosely based on the NIST/USGv6 profile developed by the US government: http://www.nist.gov/itl/antd/upload/usgv6-v1.pdf. The authors have modified these documents to make them more universally applicable. This option includes a list of RFC specification standards that must be supported, divided into eight categories of devices. This document also follows the IPv6 Node requirements document, RFC6434. This RFC is the general IETF guidance on what parts of IPv6 need to be implemented by different devices.

General information on how to use this document An IPv6 Ready Logo certificate can be required for any device. This is the easiest way for vendors providing the equipment to prove that it fulfils basic IPv6 requirements. The tender initiator shall also provide the list of required mandatory and optional RFCs in order not to exclude vendors that did not yet put their equipment under IPv6 Ready Logo testing certifications. This way public tender can't be accused of preferring any type or vendor of equipment.

1 The USGv6 specifications are currently undergoing an updated revision which is expected to be completed by early 2012. When we specify the list of required RFCs; we must list all mandatory requirements, except the entries that start with, "If [functionality] is requested..." These entries are mandatory only if the tender initiator requires certain functionality. Please note that the tender initiator should decide what functionality is required, not the equipment vendor. Certain features that are in the 'optional' section in this document might be important for your specific case and/or organisation. In such cases the tender initiator should move the requirement to the 'required' section in their tender request. How to specify requirements

As stated above, the IPv6 Ready Logo program does not cover all equipment that correctly supports IPv6; so declaring such equipment ineligible may not be desirable. This document recommends that the tender initiator specify that eligible equipment be either certified under the IPv6 Ready program or be compliant with the appropriate RFCs listed in the section below. About the IPv6 Ready Logo program: http://www.ipv6ready.org/ Also note that there exists the BOUNDv6 project whose goal is to create a permanent multi-vendor network environment connecting approved laboratories where the community can test IPv6-enabled applications and devices in meaningful test scenarios. Tender initiators are encouraged to have a look and also use the results of this project.

Download the RIPE document at https://www.ripe.net/publications/docs/ripe-554

EU-China FIRE

IPv6
BEST PRACTICES

JULY 2015

Funded by the
7th Framework Programme
of the European Union

MARTEL Consulting

SIGMAORIONIS

UNIVERSITÉ DU LUXEMBOURG

CAICT 中国信息通信研究院

Beijing internet institute 天地互连

Ruijie Networks