IPv6 Observatory

Final report – January 2014

Study ref.: SMART 2011/0059

INNO TSD
COORDINATOR

University of Luxembourg

Beijing Internet Institute

CNKS Consult

European Commission

“If you can't measure it, you can't manage it.”

Peţer Drucker

The opinions expressed in this document represent the authors’ points of view which are not necessarily shared by the European Commission.

Acknowledgements

This analysis is commissioned by the European Commission, Directorate General for Communications Networks, Content and Technology (DG CONNECT) and carried out by inno TSD.

The analysis is managed by unit 4 (Experimental Platforms). Project officer from the European Commission is Mr Jorge Pereira (Jorge.Pereira@ec.europa.eu).

inno TSD would like to express its appreciation to all of the people, experts, and organisations that have participated in the study during the various meetings, survey and interviews.

Without those contributions and dedications, the findings of the study would not have been as complete as they are.

TABLE OF CONTENTS

Part A. Executive summary

1 Introduction

ICTs are expected to play a major part in driving forward the growth of the EU economy, especially in terms of GDP and employment. Following the Lisbon Agenda, the Digital agenda still recognizes ICT as a key driver of the European economy: "… is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable application". The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of Information and Communication Technologies (ICT) will have to play if Europe wants to succeed in its ambitions for 2020.

The Internet, used daily by over 50% of Europeans, is one of the core components of the Digital Agenda. The Internet network is built on the principle of exchanging packets of data from device to device. To allow the routing of packets, each device connected to the Internet has a unique address being its identifier. The Internet Protocol (IP) is about managing the format and the routing of the transmitted packets. IP addresses are not country or region specific and the addresses pool has to be managed just as any other resource does, meeting the demands of global economies.

The Internet uses mostly IP (Internet Protocol) in its fourth version (known as IPv4). IPv6 has been designed, after large consensual consultation of experts, industries and standard bodies, to be the long-term solution for replacing IPv4. IPv6 is the cornerstone of an open architecture comprising many protocols such as routing, management, transport, mobility, security etc. It is a mature technology with large- scale. With practically unlimited address space, IPv6 degrades threats on end-to-end capability due to address shortages.

Compared to the 3.7 billion of usable IPv4 addresses, the IPv6 technology provides several thousand billion available addresses per square millimeter of the planet, enough to meet the current demand of users and in the foreseeable future. IPv6 is the natural platform for scaling the expected growth of the Internet and related usages. It is also better adapted to cope with the emerging convergence of services, provide seamless interoperability and is better suited for applications dealing

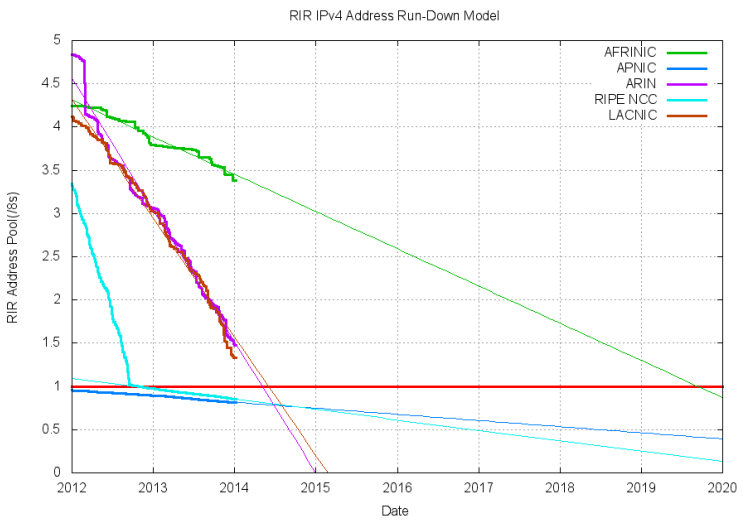

Figure 1 - RIR IPv4 Address run-down model (source http://www.pootaroo.net - 9 January 2014)

with huge amounts of data.

In its 2002 Communication on IPv6, the European Commission made the case for the early adoption of this protocol in Europe. This Communication has been successful in establishing IPv6 Task Forces, enabling IPv6 on research networks and supporting standards. Yet despite the progress made, adoption of the new protocol has remained slow.

Recognizing this, the European Commission launched a second Communication in May 2008 establishing an action plan for a rapid adoption of IPv6 in Europe, targeting 25% of users connected in IPv6 in 2010

Considering latest deployment estimates, underlined by Commissioner Neelies Kroes to be only 2% in June 2011, this deployment target has not been reached while the IANA pool exhausted on 3rd February 2011.

The issue of IPv6 adoption is still seriously tackled by the European Commission and included in its Digital Agenda for Europe 2010-2020. This agenda includes an action plan containing 100 actions covering 8 pillars. This action plan will attract much attention in the coming years and will be closely monitored through an annual plan. More especially, the Digital Agenda mentions IPv6 in two of its actions:

- **Action 89: Member States to make eGovernment services fully interoperable**
  Including the launch an innovation pilot in order to support the deployment of IPv6 by public authorities through integration of IPv6 into eGovernment services
- **Action 97: Promote the internationalization of Internet governance**
  Recognizing that the fast worldwide upgrade of Internet to IPv6 is an important priority to avoid the slow-down of Internet development and impact on economic growth.

The setup and driving of public policies requires the knowledge of the context and for that reason, the 2008 action plan launched a study aimed at monitoring the IPv6 deployment over a 2 years period. This monitoring has been ensured until 31st December 2010 and the public report has been available since February 2011. While online statistics are not longer available, **the still low level of IPv6 usage requires a pursued and enlarged effort to not only document the level of IPv6 deployment but also disseminate the situation on a regular basis toward the stakeholders. Building this European IPv6 observatory is the purpose of the IPv6 Observatory**.

2 METHODOLOGY

The IPv6 Observatory study focuses on IPv6 deployment monitoring. Thus, the work is based on 3 cycling activities running in parallel:

- Data collection: data is collected through a number of channels allowing for both quantitative and qualitative evaluation of the IPv6 deployment level. The tools available for data collection are extensive so to be adaptive to context evolutions.
- Analysis: datasets are analyzed individually and collectively. The analysis of large datasets will make use of statistical analysis and graphical representation while qualitative analysis will be based on case studies and expert's advices.
- Dissemination: dissemination is based on paper communication (leaflets, report printing) and presentations in conferences and workshops.

It is worth noting that preliminary works include the definition of indicators to monitor IPv6 deployment (see 2.2) and the development of a dedicated monitoring tool (see 2.4). Moreover, the set of indicators aims at monitoring IPv6 deployment status at every level of the Internet architecture, including for instance usage and addresses allocation, as well as competences (skilled people), compatible hardware, services and application... (Figure 4). All these indicators help to assess the overall IPv6 infrastructure readiness.

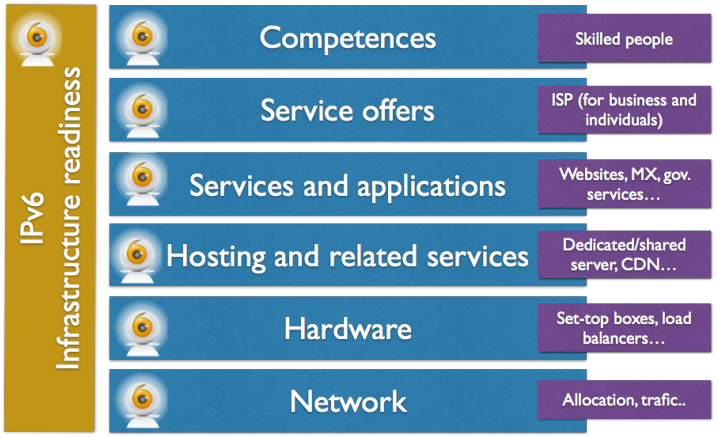

Figure 2 - Internet infrastructure layers

3 Conclusions

IPv6 is the successor of IPv4. Despite tentative by various stakeholders to develop alternative solutions to delay the deployment of IPv6, or even stay with an IPv4 Internet, IPv6 is now understood as a "next step" in the evolution of the network.

Even if we don't consider the emergence of new services and paradigms, such as the Internet of Things, IPv6 appears to be the only next step in the evolution of the Internet, and while this statement was not shared among stakeholders a few years ago, it is now the case.

As shown in the full study report, a huge amount of deployment data has been collected and analyzed during years 2012 and 2013, either on websites showing monitoring information or through the specific tool developed for the study. A survey has also been conducted in 2013 among European ISP.

Most figures are still showing a low IPv6 deployment level in all regions of the world, even if a few countries have started good initiatives, either supported to national initiatives (Czech Republic, Germany) or through the deployment of IPv6 by major ISP (e.g. ISP with a critical number of users).

However, efforts need to be pursued and progress still needs to be made in order to have IPv6 deployed on every level of the Internet architecture, plus in curricula.

In conclusion, it is important to note that begin of 2014 (January), **all actors are convinced of the need to move forward in deploying IPv6.**

And even if IPv6 deployment is still low, **progresses can be clearly seen.** Real usage remains negligible in comparison with IPv4 (and prompted by US companies) but is increasing, statistics showing **2.5% of Internet users connected in IPv6**.

On the ISP side, **IPv6 is present in core networks** but difficulties arise on the access part and the survey shown that **ISPs are internally deploying IPv6.**

With regards to curricula and training, **a pool of trained people (with IPv6 competences) exists** but progress needs to be made as IPv6 is not yet well taught in all curricula, this is an area where public authorities may have to play a role.

The table below proposes a list of main conclusions per layer studied.

Layers	Highlights
Competences	Availability of skilled staff appears to be an issue for 50% of the survey respondents (n=1000)
Usage	• 2.8% of end-users are connected in IPv6 (stats from the Observatory) • Transit IPv6 AMS-IX: 0.65%

Service offers (ISP)	• Best mark of 13.8/31 for Germany in the ranking done by the Observatory • In 2013, 18% of respondents use or plan to use CGN • gov. websites CZ 50% on AAAA, NL 40% and below 10% for the others (GEN6)
Services and applications	• AAAA/EU27: 7% • AAAA/Worldwide: 5%
Hosting and related services	*No data available.*
Hardware	Constant number of products certifications per year (~200/year) since 2008.
Network	• % IPv6 AS / Europe: 24% • % IPv6 AS / World: 17% • Average cost of an IPv4 address on relevant market places: ~10/12€

Out of these conclusions, the final report of the IPv6 Observatory provides the European Commission with **a set of recommendations to foster the deployment of IPv6 and assess impact of alternative solutions**.

4 RECOMMENDATIONS

A set of recommendations is provided on the following topics:

- IPv6 deployment monitoring
- Socio-economic impact of trends
- Training and awareness raising
- Public authorities

4.1 Monitoring IPv6 deployment

1. Continue IPv6 deployment monitoring

Objective: follow-up with IPv6 deployment observatory in order to assess progresses made over time in order to adjust public policies accordingly.

Action plan

Item	Organisation in action	Beneficiaries
1.1 Maintain this existing IPv6 indicator within the Digital Agenda Scoreboard	European Commission	IT leaders, network managers, public authorities, vendors, service providers
1.2 Develop composite indicators to cover the infrastructure readiness within Europe. As it has been seen during the IPv6 Observatory study, indicators taken individually can show significant progresses, but as soon as they are linked with other indicators, figures are not the same (example: in December 2013, 7.32% of domains (EU27) having IPv6 when looking at websites only, dropping to 0.95% when looking at domains having website, domain name and mail server IPv6.)	European Commission	IT leaders, network managers, public authorities, vendors, service providers
1.3 Extend the monitoring to the hosting and related services layer. This layer lacks of monitoring activities since information are hard to find. Since IPv6 is not a commercial argument, the majority of companies providing hosting facilities do not mention IPv6 in a highly visible zone of their website. It would therefore be recommended to monitor IPv6 offers from hosting companies and also how IPv6 is handled, e.g. with a quality of service to IPv4, or less/more.	European Commission	IT leaders, network managers, public authorities, vendors, service providers
1.4 Monitor the cost of IPv4 addresses on market places: cost of IPv4 addresses on market places will play a major role in the setting up of CGN and in the deployment of IPv6. It would also be important to monitor side effects of the IPv4 address shortage. For example, Gandi,	European Commission All	IT leaders, network managers, public authorities, vendors, service providers

a French hosting company, now offers a ~17% discount[1] to customers willing to get servers with only IPv6 (e.g. no IPv4 connectivity at all). While this is at the time of writing an isolated case, this could change to become more common.		

4.2 Socio-economical impact of trends

2. Socio-economical impact of trends		
Objective: Access impacts of the deployment of technical solution that would delay the deployment of IPv6 at the European Union level. **Action plan**		
Item	**Organisation in action**	**Beneficiaries**
2.1 Evaluate the impact of CGN on broadband access and services. CGN is a technical solution to share a single IPv4 address at the ISP level. As it has been shown in 4.1.2, services and applications can suffer when being used over a CGN.	European Commission	IT leaders, network managers, public authorities, vendors, service providers
2.2 Evaluate social impacts of CGN (new form of digital divide). Having CGN well deployed across Europe could create "two Internet", one where users would get public IP addresses and a second one, where users would get private IP addresses, with services potentially running in degraded mode. This could lead to a new form of digital divide that need to be evaluated at the EU level.	European Commission	IT leaders, public authorities, service providers
2.3 Evaluate the impact of the developing IPv4 market on existing ISP businesses and on new entrants. New companies willing to enter on the ISP market could suffer from the IPv4 addresses shortage and the low deployment of IPv6: it would be difficult for such companies to provide customers only IPv6 addresses while difficult too to obtain IPv4 addresses (at least large-enough pool). This could create a strong market distortion since a few large European ISP have enough IPv4 addresses to last a few more years.	European Commission	IT leaders, network managers, public authorities, service providers
2.4 Evaluate the impact of non-globally routable addresses. CGN-like solutions could extend the IPv4 life which could be available as a "degraded Internet" for some users. Indeed, CGN creates technical problems for advanced Internet application, as multiple levels of NAT are introduced between the end-user and the services. This would potentially create a new digital divide.	European Commission	IT leaders, network managers, public authorities, vendors, service providers

[1] http://www.gandi.net/news/en/2013-11-27/1166-ipv6-only_servers/

4.3 Training and awareness raising

3. Raising awareness and knowledge to implement seamlessly IPv6

Objective: purpose of this recommendation is to avoid any disruption in businesses within the transition phase. The target here is to raise awareness and knowledge of decision makers and network managers about obstacles hindering deployment, for example the potential security risks that would exist in case of insufficient knowledge. The European Commission facilitates raising IPv6 knowledge level cooperating with private and public stakeholders.

Action plan

Item	Organisation in action	Beneficiaries
3.1 Communicate on the need for IPv6 skilled staff. The results (final report, website) of the IPv6 Curricula study should be further promoted again as remain valid in their majority.	IPv6 Forum, IPv6 task forces, GEN6	Organisations business and human resources levels
3.2 Train network managers to use IPv6 monitoring tools. An initial set of information regarding monitoring standards and tools was provided by the 6DEPLOY project 'Network Management'[2] report which describes the different ways to retrieve management information (MIBs, IPv6 flows) and presents some IPv6 management tools and platforms.	IT services	Network managers
3.3 When selling IPv6 enabled products, warn users about the need to be IPv6 skilled for their use, even if deployment planned in an IPv4 environment. The notice should highlight risks related in running the product without needed expertise and advantages that could emerge in introducing this device in the network. This notice should target network engineers and system administrators (deploying for instance Windows 7 which is IPv6-enabled by default) and cover (at least) IPv6 security vulnerabilities, advantages and shortcomings.	Manufacturers and software providers	IT products users
3.4 Recommend ISPs to provide globally routable IP addresses. While IPv4 addresses behind CGNs might degraded services, recommending ISPs to provide globally routable addresses would help in avoiding this issue and would obviously acts in favour of the IPv6 deployment.	ISPs	Internet users

[2] « IPv6 network management », 6 deploy project, http://www.6deploy.eu/tutorials/060-6deploy_IPv6_management_v0_3.pdf

4. Make training resources available

Objective: Purpose of this recommendation is to ensure the presence of up-to-date and high quality on-line training resources and to encourage its use by training providers and beneficiaries. Developed training resources should take advantages from e–learning technology.

Action plan

Item	Organisation in action	Beneficiaries
4.1 Recommend Member States to integrate IPv6 in their college/university curriculums	Public authorities and Universities	Students
4.2 Get training content adapted to local specificities (language, industrial sectors…) and provide a set of technical tutorials ready for publication to technical magazines. While first item would be more focused on actions at a national level, the second item could be included in the dissemination plan of a project such as 6Deploy	Member states	IT practitioners Training providers
4.3 Develop hands-on remote access labs. It is underlined that IT capabilities are better acquired through on field-testing. Remote access to laboratory should be encouraged and integrated with developed e-learning courses (see action item 2.1)	NREN Academics	IT practitioners Training providers

5. Get training courses being recognised

Objective: Increasing needs for IPv6 training may lead to the development of poor quality training courses. The objective of this recommendation is to recognise a certification (academic diploma or industry certificate) scheme ensuring a minimum level acquired knowledge and training quality.

Action plan

Item	Organisation in action	Beneficiaries
5.1 Providers of certification schemes should agree on a common charter of conduct establishing a minimum level of quality.	Certification scheme providers ETSI support	Certification authorities IT practitioners Training providers
5.2 When recruiting IP practitioners who have to deal with the network layers, request certified IPv6 skills.	HR departments	Recruiting organisations
5.3 When procuring new equipment, software or services related to IP layer, follow the RIPE 554 requirements, including the request to ask for people being professionally trained in the tendering organisation[3].	Procurement departments	Equipment, software or services buyers
5.4 Select certified training courses and get your training being recognised by a diploma or a certification.	Training beneficiaries	Training providers Training beneficiaries
5.5 Get your training to be certified and propose your trainees to evaluate the acquired knowledge by passing a diploma or a certification	Training providers	Training providers Training beneficiaries

4.4 Public authorities

6. Public authorities

Objective: Ensure that member state play their role in the deployment of IPv6

Action plan

Item	**Organisation in action**	**Beneficiaries**
6.1 Ensure presence of IPv6 in public curricula	Member states governments	Students, Life long training beneficiaries
6.2 Ensure that IPv6 is required in public procurements	Member states governments, Education ministries	Vendors, public authorities
6.3 Make sure that websites at national and local levels are IPv6 enabled	Member states governments, local governments, public authorities	Public authorities, eGovernmeent services users

[3] In the RIPE 554,formulating requirements can be done in several ways: first option is based loosely on the NIST/USGv6 profile developed by the US government, second option is based on compliance with the "IPv6 Ready" program (testing and certification of the basic "core" protocols, and testing and certification of advanced IPv6 functionality), and third option is a combination of the two first options. http://www.ripe.net/ripe/docs/ripe-554

Part B. DETAILED REPORT

1 INTRODUCTION

1.1 Background and rationale

ICTs are expected to play a major part in driving forward the growth of the EU economy, especially in terms of GDP and employment. Following the Lisbon Agenda, the Digital agenda still recognizes ICT as a key driver of the European economy: "... is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable application". The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of Information and Communication Technologies (ICT) will have to play if Europe wants to succeed in its ambitions for 2020. The aim of the Europe 2020 Strategy is to exit the crisis and prepare the EU economy for the challenges of the next decade[4].

The Internet, used daily by over 50% of Europeans, is one of the core components of the Digital Agenda. Regular websites, social networks, online applications (banking, e-commerce...), all of these services are exchanging data between peers.

The Internet network is built on the principle of exchanging packets of data from device to device. To allow the routing of packets, each device connected to the Internet has a unique address being its identifier. The Internet Protocol (IP) is about managing the format and the routing of the transmitted packets. IP addresses are not country or region specific and the addresses pool has to be managed just as any other resource does, meeting the demands of global economies.

The Internet uses mostly IP (Internet Protocol) in its fourth version (known as IPv4). IPv6 has been designed, after large consensual consultation of experts, industries and standard bodies, to be the long-term solution for replacing IPv4. IPv6 is the cornerstone of an open architecture comprising many protocols such as routing, management, transport, mobility, security etc. It is a mature technology with large- scale deployments (i.e. interconnected networks worldwide like the European-wide research network GEANT), a stable corpus of standards, adopted by some leading software and hardware vendors. IPv6 compared to IPv4 offers expanded routing and addressing capabilities, simplified packet headers, embedded (versus optional in IPv4) Internet Protocol Security support and better capabilities to support auto configuration, multicasting, traffic engineering, and zero configuration networking. With practically unlimited address space, IPv6 degrades threats on end-to-end capability due to address shortages (see Figure 3).

[4] Communication from The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Region. A Digital Agenda for Europe. August 2010

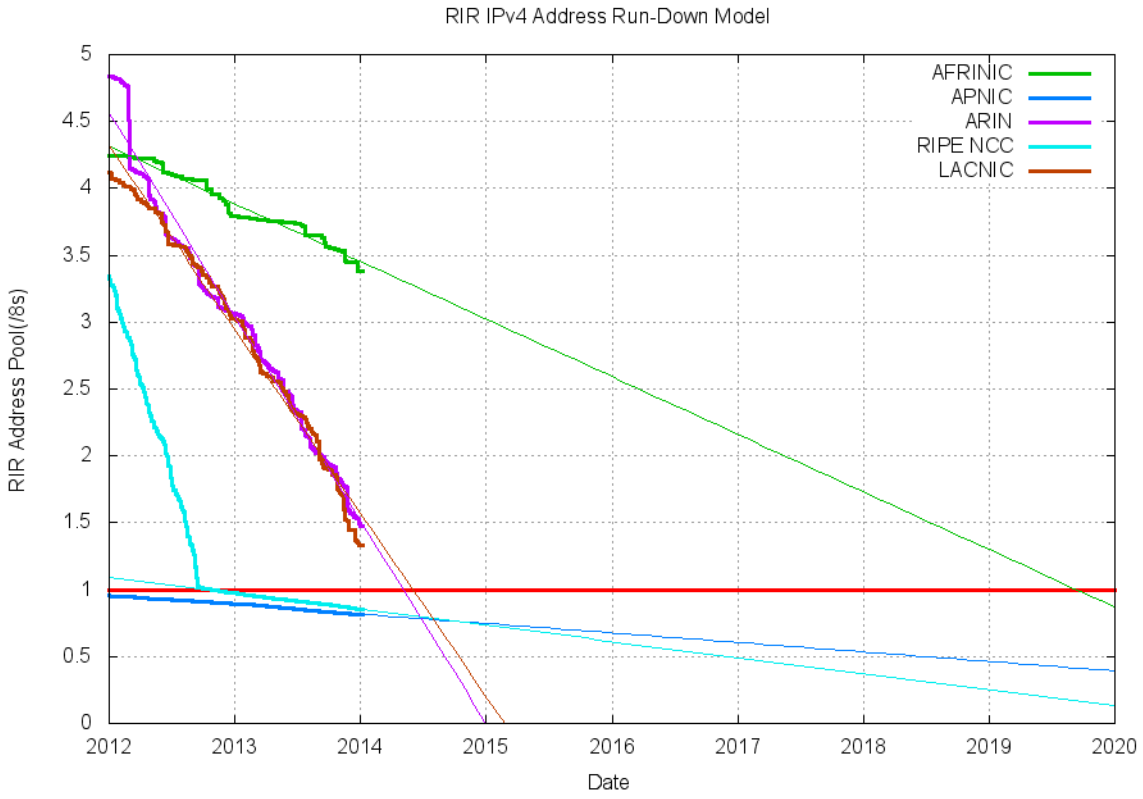

Figure 3 - RIR IPv4 Address run-down model (source http://www.pootaroo.net - 9 January 2014)

Compared to the 3.7 billion of usable IPv4 addresses, the IPv6 technology provides several thousand billion available addresses per square millimeter of the planet, enough to meet the current demand of users and in the foreseeable future. IPv6 is the natural platform for scaling the expected growth of the Internet and related usages. It is also better adapted to cope with the emerging convergence of services, provide seamless interoperability and is better suited for applications dealing with huge amounts of data.

In its 2002 Communication on IPv6, the European Commission made the case for the early adoption of this protocol in Europe. This Communication has been successful in establishing IPv6 Task Forces, enabling IPv6 on research networks and supporting standards. Following the Communication more than 30 European R&D projects related to IPv6 were financed. Europe has now a large pool of experts with experience in IPv6 deployment. Yet despite the progress made, adoption of the new protocol has remained slow.

Recognizing this, the European Commission launched a second Communication in May 2008 establishing an action plan for a rapid adoption of IPv6 in Europe. Based on the estimation than the unallocated IANA pool will be exhausted somewhere around 2011, the action plan targets that by 2010, 25% of users should be able to connect to the IPv6 Internet and to access their most important content and service providers without noticing a major difference compared to IPv4.

Considering latest deployment estimates, underlined by Commissioner Neelies Kroes to be only 2% in June 2011, this deployment target has not been reached while the IANA pool exhausted on 3rd February 2011.

The issue of IPv6 adoption is still seriously tackled by the European Commission and included in its Digital Agenda for Europe 2010-2020. This agenda includes an action plan containing 100 actions covering 8 pillars. This action plan will attract much attention in the coming years and will be closely monitored through an annual plan. More especially, the Digital Agenda mentions IPv6 in two of its actions:

- **Action 89: Member States to make eGovernment services fully interoperable**
  Including the launch an innovation pilot in order to support the deployment of IPv6 by public authorities through integration of IPv6 into eGovernment services
- **Action 97: Promote the internationalization of Internet governance**
  Recognizing that the fast worldwide upgrade of Internet to IPv6 is an important priority to avoid the slow-down of Internet development and impact on economic growth.

The set-up and driving of public policies require the knowledge of the context and for that purpose; the 2008 action plan launched a study aimed at monitoring the IPv6 deployment over a 2 years period. This monitoring has been ensured until 31st December 2010 and the public report is available since February 2011. While online statistics are not anymore available, **the still low level of IPv6 usage requires a pursued and enlarged effort to not only document the level of IPv6 deployment but also disseminate the situation on a regular basis toward the stakeholders. Building this European IPv6 observatory is the purpose of the present study**.

1.2 Objectives and approach

The European Commission is continuing its support to IPv6 deployment through its Digital Agenda and needs to maintain knowledge of the IPv6 deployment level. For that purpose, the EC calls for an enlarged follow-up of the IPv6 monitoring initiative initiated in 2008 namely to get a precise and indisputable knowledge of the IPv6 deployment level, with frequent updates and a support from the IPv6 community in its day to day action to foster IPv6 adoption.

Based on these considerations, the European Commission has entrusted inno with a study to monitor the progress of IPv6 deployment worldwide during 2012 and 2013. In that context, inno was supported by the University of Luxembourg, the Beijing Internet Institute and GNKS Consulting along with an advisory board composed of high-level IPv6 experts. Main tasks to be achieved during the study were the following:

To setup of a 2 years IPv6 observatory for:

- Gathering data from the whole EU27 and main worldwide actors with targets to monitor more than 2000 users
  - Providing analysis of the tendencies, identifying the gaps still to be filled as well as possible threats brought by the IPv6 deployment

    - Disseminating and networking, with special relationships built within the expert group with organizations such as the RIRs, ENISA, the ETSI, the IPv6 forum, national Task forces…
- To support the European Commission and to propose a set of recommendations to foster the deployment of IPv6 at the European level.

1.3 Structure of the publication

This report deals with results obtained during the study timeframe, starting with the detailed methodology used to reach the objectives.

The methodology description includes (non exhaustive list) indicators definition to monitor IPv6 deployment, existing data sources used to get data and custom tools built specifically for the study. It also provides a description of the method used to measure the IPv6 penetration in websites and presents the survey conducted during the study.

Then the third section presents IPv6 deployment trends through the use of data collected through custom tools or collected elsewhere, highlights side-effects that arise and ends with perspectives and conclusions.

Finally, the latest section focuses on recommendations for the European Commission to foster to deployment of IPv6 at the European level.

2 METHODOLOGY

Monitoring the worldwide level of IPv6 deployment means collecting, consolidating and analysing data coming from multiples sources. This part presents the methodology adopted to conduct the study to its final objectives.

2.1 Overview

The IPv6 Observatory study focuses on IPv6 deployment monitoring. Thus, the work is based on 3 cycling activities running in parallel:

- Data collection: data are collected through a number of channels allowing for both quantitative and qualitative evaluation of the IPv6 deployment level. The tools available for data collection are extensive so to be adaptive to context evolutions.
- Analysis: datasets are analyzed individually and collectively. The analysis of large dataset will make use of statistical analysis and graphical representation while qualitative analysis will be based on case studies and expert's advices.
- Dissemination: dissemination is based upon paper communication (leaflets, report printing) and presentations in conferences and workshops.

It is worth noting that preliminary works included the definition of indicators to monitor IPv6 deployment (see 2.2) and the development of a dedicated monitoring tool (see 2.4). Moreover, the set of indicators aims at monitoring IPv6 deployment status at every level of the Internet architecture, including for instance usage and addresses allocation, but also competences (skilled people), compatible hardware, services and application... (Figure 4). All these indicators help in assessing the overall IPv6 infrastructure readiness.

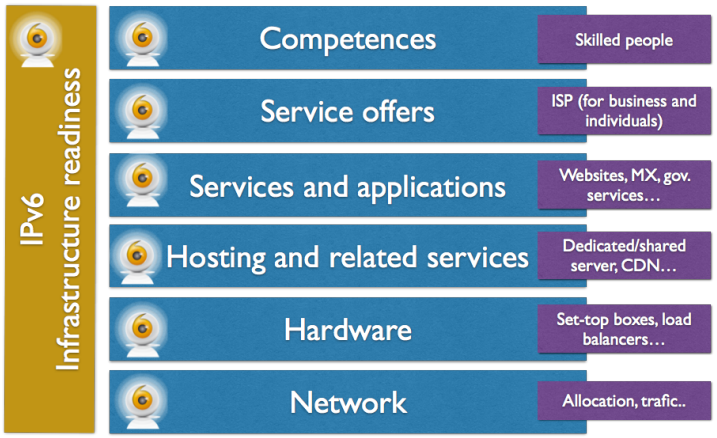

Figure 4 - Internet infrastructure layers

2.2 Indicators definition

In recent years, indicators for science and technology have witnessed an extraordinary development, mainly due to the emergence of new customers and demands, as well as by technological and methodological developments, which have opened new fields.

S&T indicators are increasingly used by policy-makers for decision-making, and especially in the last decades where the number of stakeholders involved rabidly increased together with the complexity of S&T policies and programmes. Consequently, the need for better designed indicators that could support policy-makers decisions in the context of the so-called evidence-based policies is now more purposeful than ever. As a result, the first group of indicators developed in the 1960s' based on national statistical offices collecting data on the one hand and the OECD coordinating the methodological work and producing indicators on the other hand, is no longer the unique reference. We are now able to access a wide range of both qualitative and quantitative examples of S&T indicators stemming from independent indicators producers, specialized research institutes, semi-official bodies, and large indicators projects. Moreover, there is a plethora of research teams responsible for a large number of produced indicators as well as individual Programme Impact assessments which produce indicators on an ad-hoc basis.

A set of indicators must be a tool for the measurement of an objective to achieve, a resource mobilized, an output accomplished, an effect obtained or a context variable (economic, social or environmental). An indicator provides evidence that a certain conditions exist or certain results have or have not been achieved, thus enabling decision-makers to assess progress towards the achievement of intended outputs, outcomes, impacts, and objectives. Indicators are measured, therefore, in terms of the objectives of the programme or intervention and are then used to assess its positive and negative effects in order to assess the contribution of the intervention "the IPv6 Communication" towards achieving specified targets or strengthening the process for achieving those targets and goals.

The developed indicators does not only give a measure of the IPv6 deployment level but whenever possible, puts in light correlations between the deployment level and higher level benefits expected in the 2008 IPv6 Communication, such as the support of the Digital Agenda initiative.

Below is proposed an initial set of indicators to be discussed. Data sources should be identified taking into account their sustainability, the associated IPRs and then ease of access.

	Criteria	**Indicators [Unit]**	**Data sources**	**Comments / Limits**
Infrastructure readiness	Naming service is available	Proportion of DNS root server accessible with IPv6 transport [%]	News from http://www.root-servers.org/	
		DNS Root service quality	RIPE's DNSMON tool[5]	Measurements concentrated

[5] http://dnsmon.ripe.net/dns-servmon/

		Ratio of v6/v4 average of unanswered queries Ratio of v6/v4 average response time		region. Existing API to extract measures
		Proportion of TLDs supporting IPv6 (DNS/IDN) [%]	HE site: http://bgp.he.net/ipv6-progress-report.cgi	
		TLD service quality Ratio of v6/v4 average of unanswered queries [] Ratio of v6/v4 average response time []	RIPE's DNSMON tool[6]	Measurements concentrated in RIPE NCC region. Existing API to extract measures
	IPv6 is supported at Internet Exchange Points (IXP)	Proportion of IXP supporting IPv6 [%]	Clearing House Packet	Should 'IXP' be detailed into sub-components
	IPv6 addresses are allocated	Number of IPv6 addresses allocated [addresses /year]	RIRs (public data)	
		Number of IPv6 addresses blocks allocated [number of blocks / block size /year]	RIRs (public data)	
		Size of allocated IPv6 prefixes [average size of allocated prefixes / year]	RIRs (public data)	
	Allocated IPv6 addresses are announced	Proportion of ASes that can handle IPv6 traffic [%]	Stats from global routing tables.	Caveats: No indication on native connection, Toredo, 6rd...)

[6] http://dnsmon.ripe.net/dns-servmon/

		Proportion of allocated addresses announced in BGP tables [%]		Caveats: some IPv6 blocks might be used in private networks and not advertised
		Latency between allocation and announcement [days]		
		Number of IPv6 peering agreements	Caida PeeringDB	
	IPv6 in mobile networks	IPv6 is supported in mobile operators infrastructure	Mobile operators (ISPs survey)	
	Software/Hardware is IPv6 compliant	Number of products approved by the IPv6 ready-logo program]	IPv6 Ready Logo program	Category of software/hardware (include FTP, Firewalls, DNSSEC, IPSec, Browsers,..) to be monitored is to be defined
		Proportion of network products stating compliance with IPv6 in their specification [%]		Should a panel of software/hardware for networks be defined and monitored for IPv6 readiness? Caveats: Analyse would only be based on self-declaration (product spec.). Analysis would only be conducted over a limited number of items in each category

		Proportion of business products stating compliance with IPv6 in their specification [%]		Same as above but for database, printers, VoIP phones, …
		Proportion of IPv6-enabled CPEs	RIPE survey[7], SIXXS website[8], University of New Hampshire lab[9], SamKnows[10]	
	Operating systems support IPv6 by default	Proportion of OS in used which support IPv6 by default [%]	Public market reports[11]	
	Skills availability	Number of IPv6 courses in a set of curricula's.	Stats from IPv6 Education logo program IPv6 curricula study	
	End-to-end native IPv6 connectivity	TBD	TBD	Tunnelling appears if one of the end is tunnelled. Is this assertion valid?
Service availability	ISP IPv6 offers	Proportion of ISP providing IPv6 connectivity (e.g. IPv6 offers) [%]	IPv6-enabled logo program from ISP (IPv6 forum) RIR members survey (follow-up TNO + Caida survey)	If IPv6 available, is it native or tunnelled? Mobile operators to be considered in this indicator
		Number of ISP having their website IPv6-enabled [%]	Custom tool on top-3 ISPs for 5 to 10 countries	
		Number of ISP offering (quoting) IPv6 on their website [%]	Bias evaluation through manual analysis of top-3 ISPs for 5 to 10 countries	

[7] https://labs.ripe.net/Members/marco/ipv6-cpe-survey-results-may-2011
[8] http://www.sixxs.net/wiki/Routers
[9] http://www.iol.unh.edu/services/testing/ipv6/equipment.php
[10] https://www.samknows.eu/
[11] http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

	IPv6 enabled-services (websites, mail servers, ...)	Proportion of top-500 websites for each EU27+China, USA, Japan, Canada having AAAA	v6demon tool with Alexa stats http://www.vyncke.org/ipv6status/	
		Percentage of web-sites having AAAA reachable in IPv6 (HTTP request sent on the IPv6 address) [%]	v6demon tool with Alexa stats	
		Proportion of top-500 websites for each EU27+China, USA, Japan, Canada having IPv6 MX host(s) [%]	v6demon tool with Alexa stats	
		Percentage of web-sites having MX reach-able in IPv6 (socket opened on the IPv6 address / port 25 (SMTP) [%]	v6demon tool with Alexa stats	
		Proportion of admini-stration website ready for IPv6 [%]	V6demon tool with list of 7k sites from EC	
		Proportion of univer-sity websites ready for IPv6 [%]	V6demon tool with list of university from http://www.mrp.net/IPv6_Survey.html updated with EU university list (See IPv6 Cur-ricula report)	
	Content pro-viders available in IPv6		Manual investigation	Is it meaning-ful to shortlist 50 contents providers and monitor them during the study timeframe (example: FB/Tweeter ...).
	Content distri-bution services		Stats from Alexa	

	available in IPv6 (e.g. Akamai...)			
	IPv6 Quality of Service	IPv6 requests latency compared to IPv4 [ms]	Feedback from various websites associated to the observatory and using a custom tool developed by the study team (v6demon) Plugin for web browsers	Targeted websites will be in various sectors (e.g. not only technical to avoid biased results).
	Transition mechanisms (TBD)	Repartition of used transition mechanisms	Get agreement with various IPv6-enable website' webmasters to monitor IPv6 access (providing either a custom tool or a Google Analytic add-on12).	
Usage	IPv6 traffic (at IXP, ISP and transit providers levels, app level)	Percentage of IPv6 traffic at transit providers level [%]	Stats from IXP (TBD) RIPE's Atlas tool13	
		Proportion of IPv6 native traffic versus tunnelled (6to4, Teredo, 6rd...) [%]	Stats from IXP (TBD)	
		Percentage of IPv6 usage for ISP having ISP offers [%]	ISPs Survey	
		ISPs situation and roadmaps	Continuation of ISPs monitoring survey	
		Proportion of visitors using IPv6 on websites when both IPv4 and IPv6 are available on the client and server sides (e.g. browser behaviours) [%]	Feedback from various websites associated to the observatory and using a custom tool developed by the study team (v6demon)	
		Proportion of IPv6 trafic generated by P2P applications	http://www.vyncke.org/ipv6status	
		Corporate IPv6	Stats from various tools such as MS DirectAccess	

[12] https://groups.google.com/a/googleproductforums.com/forum/#!category-topic/analytics/discuss-google-analytics-features-with-other-users/u5CZA2-33sk

[13] http://atlas.ripe.net/ (will be potentially used to monitor multiple indicators)

2.3 Existing data sources

Literature related to the IPv6 deployment already exists on the Internet. Various individuals and companies are conducted monitoring experiments (some of them have been involved in the IPv6 Observatory experts group).

In such context, it would have been useless to re-develop existing tools. Therefore, this study, beyond data collected by the team through the custom observatory tool, has built its analysis on existing data/websites. Most important websites used are listed below.

Name	URL
RIPE NCC abs	https://labs.ripe.net/
IPv6 Deployment Aggregated Status (Erick Vyncke's website)	http://www.vyncke.org/ipv6status/
Google IPv6 statistic	http://www.google.com/intl/en/ipv6/statistics/
Amsterdam IMX	https://www.ams-ix.net/technical/statistics
Akamaï IPv6 statistics	http://www.akamai.com/ipv6
APNIC Labs	http://labs.apnic.net
The IPv6 Guy	http://twitter.com/#!/theipv6guy
IPv6 to standard	http://www.ipv6-to-standard.org/
Sixxs statistics	http://www.sixxs.net/tools/grh/export/csv/
Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name system	http://www.icann.org/en/committees/security/sac018.pdf
Packet Clearing House Report on Distribution of IPv6-Enabled IXPs	https://prefix.pch.net/applications/ixpdir/summary/ipv6/
Peering database	https://www.peeringdb.com
RIPE Stats API	https://stat.ripe.net/docs/data_api
RIR statistics	• http://ftp.apnic.net/stats/afrinic/ • ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest • ftp://ftp.apnic.net/pub/stats/apnic/delegated-apnic-latest • ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest • ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest • ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest
Potaroo	http://www.potaroo.net/bgp/stats/iana/delegated-iana-latest
Distribution of IPv6-Enabled IXPs	https://prefix.pch.net/applications/ixpdir/summary/ipv6/
Cisco 6Lab	http://6lab.cisco.com/stats/
mrp.net	http://www.mrp.net/ipv6_survey/

2.4 v6DEMON

In the context of the study, a specific tool used to monitor IPv6 deployment has been developed: v6DEMON, which has its web application available at http://v6demon.ipv6observatory.eu. Its acronym stands for IP**v6 DE**ployment **MON**itor. This paragraph describes features of this tool and its technical architecture.

2.4.1 Objective of the tool

This tool aims at assessing the overall deployment of IPv6 by collecting data and providing deployment figures. It is based on a distributed architecture with servers located in different countries (France, Luxembourg and China) in order to test deployment from various locations.

Moreover, the tool is able to collect data from other monitoring tools or websites providing monitoring data.

2.4.2 Technical architecture

The table below shows what the tool monitors.

Test	Description
Websites	Checks IPv6 availability on websites from datasets (see 3.1). For each website, it tests if the website has an AAAA record.
MX servers	Checks for each domain if the mail server has an IPv6 address.
DNS servers	Checks the DNS server of each server. For each server, it tests if the server can be reached through IPv6 and if it supports DNSSEC.
HTTP latency	For each website that is available in both IPv4 and IPv6, it compares HTTP latency. See 2.6 for the full methodology.
End-users	Checks if end-users have an IPv6 connectivity, and if yes tests if requests are sent in IPv4 or IPv6 for a host having both connectivity. See for the full 2.7 methodology.
Certifications	Checks certifications issued by the IPv6 Forum (people and products).

Table 1 - Elements monitored by the v6DEMON tool

The Figure 5 shows the tool's architecture. Datasets are managed on the master server: it is the one where data are stored. Communication with other servers is done through a dedicated REST API (messages formatted in JSON are exchanged). Additional servers are mainly used for tests that need to be done from various locations: for instance, it makes sense to test HTTP latency from various places in the workd to see if it varies from one country to another one. Moreover, the architecture shows a web application: it is the frontend where tests results can

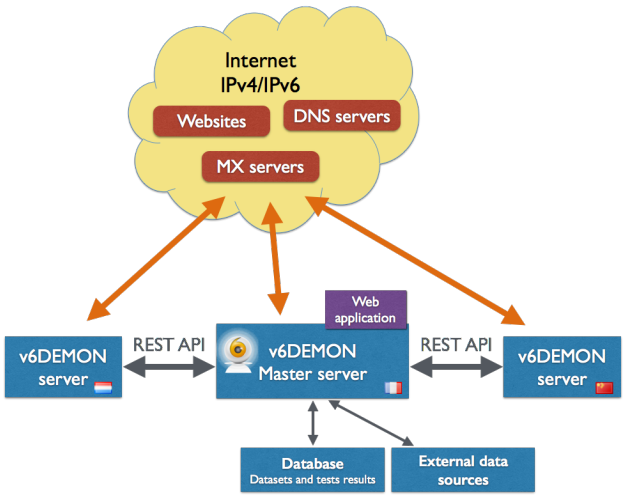

Figure 5 - v6DEMON architecture

be seen.

2.4.3 Tools and libraries used

v6DEMON is mainly powered by the following open source projects:

Name	Description	URL
Ruby	Programming language	http://ruby-lang.org/
Ruby on Rails	Web framework	http://www.rubyonrails.org
Sidekiq	Background job processing framework	http://mperham.github.com/sidekiq/
Apache HTTPd	Web server	http://httpd.apache.org/
Twitter Bootstrap	Layout framework for web projects	http://twitter.github.com/bootstrap/
Ubuntu Server	Operating system	http://www.ubuntu.com/
MySQL	Database server	http://www.mysql.com/
Redis	Database server (NoSQL)	http://redis.io/
GeoLite data by Max-Mind	Geo location API and data	http://www.maxmind.com/

Table 2 - Tools used to build v6DEMON

2.4.4 Numbers

The list below gives a few numbers from the tool (as per mid-January 2014), highlighting the number of tests performed:

- 3 134 995 websites are tested;
- Almost 1.5 billions HTTP requests have been sent;
- ~955 millions DNS requests have been sent.

2.5 Measuring IPv6 penetration in websites

A frequent measure of IPv6 penetration is done by checking in a list of web sites which have an AAAA (quad A) record in their DNS.

In comparison with the A record which provides the IPv4 address, the AAAA record provides the IPv6 address. Having a AAAA record is thus one of the prerequisites to be able to reach a web server over IPv6.

The lists of web sites to be checked are generally obtained from ranking companies such as Alexa[14], which identifies the most visited websites throughout the world. Measures are done through a toolbar installed by their users' panel. Top site ranking is then computed through an un-disclosed algorithm[15], which uses a combination of average daily visitors, page views over the past month, corrections for a number of biases and normalisation based on geographical distribution of visitors.

[14] http://www.alexa.com/ (Alexa is a company belonging to Amazon)
[15] http://www.alexa.com/help/traffic-learn-more

The list of websites from the Top 500 ranking per country as provided by Alexa[16] includes the domain name, the visitor's country, the total number of pages viewed and the number of pages viewed by visitors. These are accessible on a commercial basis.

In addition, a free list of the 1 Million top visited websites throughout the world is made available and updated daily[17]. This list only provides the domain names and the ranking.

The measurement method is then to launch for each domain name a DNS query and check whether or not an AAAA record is available. The script ran by the IPv6observatory use the following logic:

1. Domain name as provided by Alexa is tested for AAAA record
2. If no AAAA record is found in first step, a www prefix is appended in front of the domain name provided by Alexa and this new domain is tested.

The above approach raises two questions:

- How many domains should be tested to get a reliable measure of the IPv6 deployment in DNS records?
- Is the users' location provided by Alexa the one to be used to make country based analysis?

These questions are discussed below.

2.5.1 Sample size

The measurements have been made using the top 1 millions domains provided by Alexa. Each domain has been tested for the presence of AAAA record. The IPv6 penetration ratio is calculated by dividing the number of domains having the AAAA record with the total number of domains.

To evaluate the impact of the sample size, the calculated IPv6 penetration ratio is plotted against the number of domains used in the calculation (*Figure 6*). In green the domains are used in the calculation in the order they appear in the top 1 million ranking (better ranked domains are used first in the calculation) whereas in black, domains are used in a random order.

[16] http://www.alexa.com/topsites/countries
[17] http://s3.amazonaws.com/alexa-static/top-1m.csv.zip

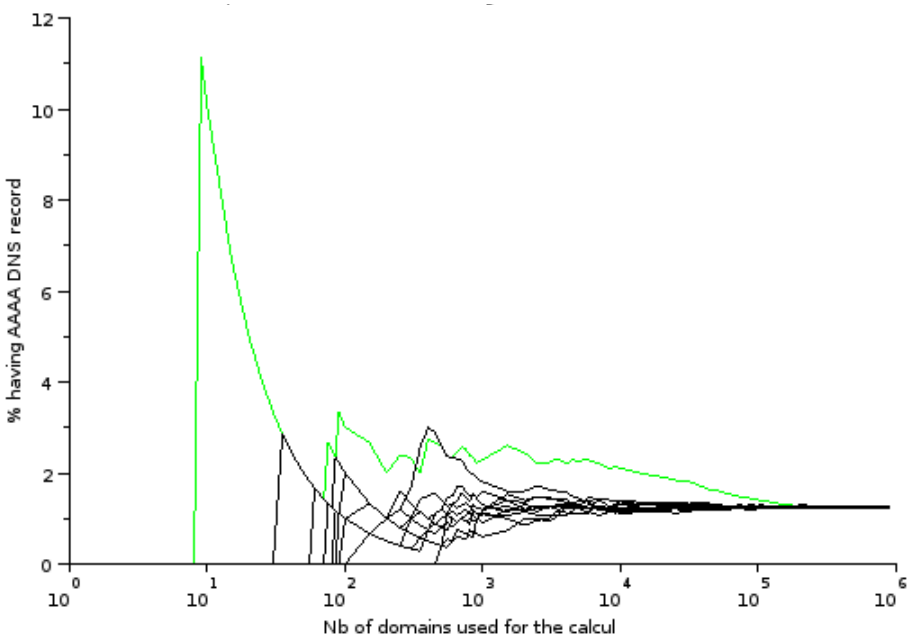

Figure 6 - Proportion of domains having an AAAA DNS record, depending on the number of tested domains (in green, domains are tested in the order they appear in the top 1Million provided by Alexa. In black, domains are used in a random order. Data from June 2012).

Figure 7 is similar to Figure 6 with a higher (300) number of generated randomly ordered domains list.

From this figure, it seems that higher ranked domains have higher IPv6 presence. This can be explained by the fact that the big players, being top ranked need to ensure their presence on the web also on IPv6, to secure their business. Nevertheless, this should be moderated as IPv6 penetration measured on 1 million domains was only 1.24% as of 16th May 2012.

This means also that **IPv6 penetration calculation done on top ranked websites will tend to over-estimate the IPv6 penetration in web domains**.

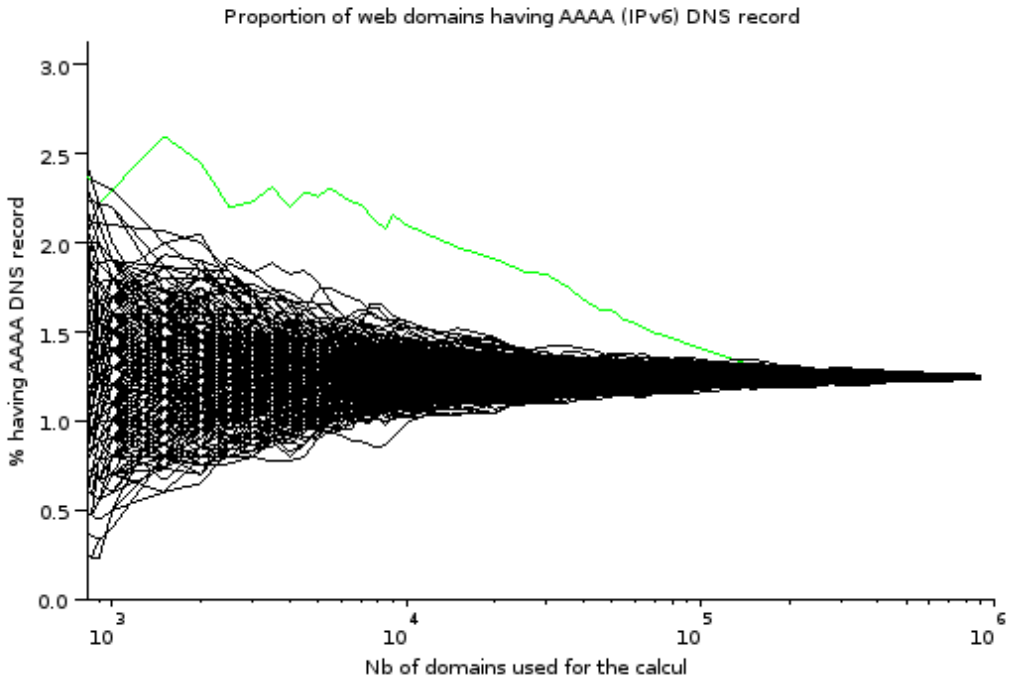

Figure 7 - Proportion of domains having a AAAA DNS record, depending on the number of tested domains (in black are shown 300 random generation of the order in which domains are tested. Data from June 2012).

Figure 8 shows the difference between the IPv6 presence (%) in DNS records calculated using the 1 million domains and the one calculated using a lower number of domains. The figure superposes the plot calculated from 300 versions ordered in a different way, to simulate different and random samplings.

The figure shows that **a minimum of 10 000 domains is necessary to estimate the ratio of domains having a AAAA record as calculated from the top 1 million domains with an error in the range [-0.5;0.5].**

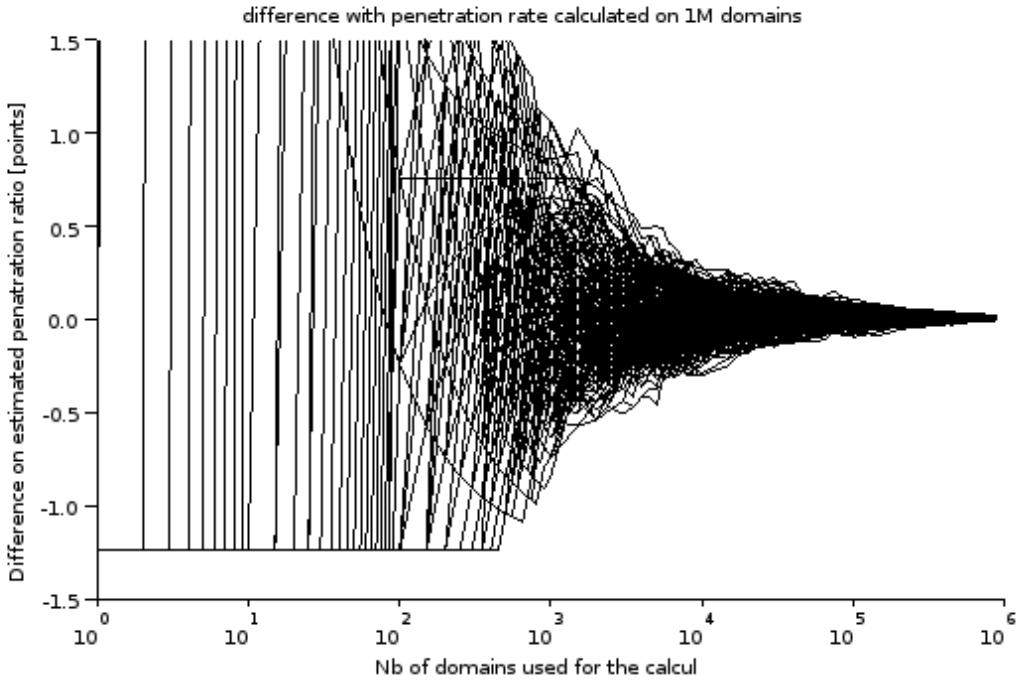

Figure 8 - Difference between the calculated IPv6 penetration in DNS record and the penetration calculated on 1 million domains, depending on the number of domains used in the calculation (300 curves plotted from randomly ordered domains list. Data from June 2012).

2.5.2 Geographical repartition

It is interesting to extract information related to IPv6 penetration on a per country basis to be able to convey messages to the governments.

As mentioned earlier, the countries referenced in the top 500 per country provided by Alexa are the countries of the domain visitors. Calculating the AAAA presence for these countries would then allow answering the question "*As a user based in this country, which proportion of my favourite websites are potentially reachable through IPv6, as having an AAAA record?*"

Alternatively, it is also of interest to look at the place where the servers are established as it would be a better indication of the country preparedness for IPv6 and would thus be a better choice to convey messages to national governments. An option is to make use of a Geo-location database such as GeoIP provided by MaxMind[18] that provides, for an IP address, the country in which the server is based.

Using the Alexa database and GeoIP services, there are roughly three ways to provide country specific data:

Option	Pro	Cons
1. The country provided	• This measure is already pro-	• It does not reflect a

[18] http://www.maxmind.com/

	by Alexa is kept and the measure is an estimate of the experience of the users established in the country	vided in many places and is easily understood.	'national readiness' but rather a country's users experience • The number of domains per country is limited to 500, implying greater uncertainty on measurement accuracy
2.	The domains listed in the top500 ranking per country are used and located by the use of the GeoIP database	• It is a reliable and sustainable source of information (paid service)	• The number of tested domains is not constant through the countries and very low in some cases
3.	All domains from the top 1 Million ranking are used and located using GeoIP database	• It provides larger number of servers per country, increasing measurement accuracy.	• It is a free resource whose sustainability is not ensured[19] • The number of tested domains is not constant through the countries

The results depending on the chosen scenario are given in the table below.

[19] https://forums.aws.amazon.com/thread.jspa?messageID=347289

Country_Name	Nb of domains	Nb of IPv6 domains	IPv6 penetration	Nb of domains	Nb of IPv6 domains from	IPv6 penetration from	Nb of domains	Nb of IPv6 domains	IPv6 penetration from 1M
Australia						GeoIP	eoIP	oIP	
Austria									
Belgium									
Bulgaria									
Canada									
China									
Cyprus									
Czech Republic									
Denmark									
Estonia									
Finland									
France									
Germany									
Greece									
Hungary									
India									
Ireland									
Italy									
Japan									
Latvia									
Lithuania									
Luxemburg									
Malta									
Poland									
Portugal									
Romania									
Slovakia									
Slovenia									
Spain									
Sweden									
The Netherlands									
United Kingdom									
United States									

Table 1 - Results per country for each proposed method (data from June 2012).

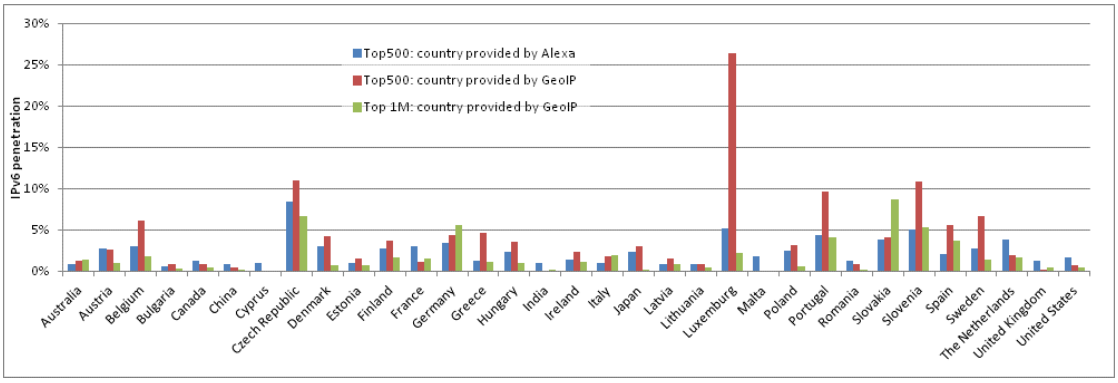

Figure 9 - Ratio of available AAAA records: comparison of the 3 methods (data from June 2012).

As shown on Figure 9, results vary a lot from one method to one another. At the exception of few countries, results confirm that evaluation made on a lower number of domains tend to over-estimate the IPv6 deployment level.

Providing countries ranking is a usual exercise in such benchmark. The top 10 European countries are provided in Table 1 - Results per country for each proposed method (Table 1 for each of the proposed method. Only 5 countries appear in all these 3 top 10: Czech Republic, Luxembourg, Portugal, Germany and Belgium.

Looking at the number of surveyed domains (Table 1) and the impact of the sample size (Figure 8) we can see for example that the first rank of Slovakia the third method is obtained with 1320 measures and has an estimated ratio of 8.6±1% while it does not appear in the 2nd method with an estimated ratio of 4(-1/+5)%

	Domain list Geolocation	*Top500 Alexa*	*Top500 GeoIP*	*Top 1Million GeoIP*
1	Czech Republic	Luxemburg	Slovakia
2	Luxemburg	Czech Republic	Czech Republic
3	Slovenia	Slovenia	Germany
4	Portugal	Portugal	Slovenia
5	Slovakia	Sweden	Portugal
6	The Netherlands	Belgium	Spain
7	Germany	Spain	Luxemburg
8	Belgium	Greece	Italy
9	Denmark	Germany	Belgium
10	France	Denmark	The Netherlands

Figure 10 - Impact of the chosen method on the top 10 European countries ranking for AAAA availability (data from June 2012).

2.5.3 Conclusion

Analysis shown in this document are based on only one sample of data provided by the Alexa ranking company so care should be taken before generalising the findings.

The analysis shows that the current proportion of websites having an AAAA record is today so low (a few %) that errors made in the measure are relatively high compared to the measured ratio. To compensate for this, there is a need to do the measure over a large number of domains. 1000 domains appear to be a minimum to get few percent's of accuracy.

Measurements made on top 500 websites thus demonstrate insufficient accuracy if analyses are made country by country and analysis made from the top 1 Million should be preferred. In any case, when comparing country scores, the number of tested servers should be looked at to evaluate overall accuracy.

Finally, there is a doubt on the sustainability of the 1M domains files as it is a free resource proposed by Alexa. Nevertheless, even if publication of the 1 Million ranking would be discontinued, the same file could still be used to run the AAAA record tests.

2.6 Measuring HTTP latency

v6DEMON (the tool developed for the study , see **Erreur ! Source du renvoi introuvable.** for more details) , monitors among other indicators the difference in latency for HTTP requests hosts offering both IPv4 and IPv6 AAAA DNS records.

This paragraph describes how measurements are done.

Results can be seen on the v6DEMON web application:

- Latest report: http://v6demon.ipv6observatory.eu/figures/web/latency/eu_27/latest
- Evolution: http://v6demon.ipv6observatory.eu/figures/latency_evolution/eu_27

2.6.1 Data collection

- A *t1* timestamp is taken when the http request is launched to the server
- A *t2* timestamp is taken the http request has been fulfilled.
- $\Delta t=t2-t1$ provides the latency
- This measure is done over both IPv4 (ΔT_4) and IPv6 (Δt_6) and is repeated every hour so to obtain N=10 measure. The averages $\Delta t4$ and $\Delta t6$ are calculated and used for the daily analysis

Note: up to 5 redirections can be taken into account in the latency estimate. When more than 5 redirections occur the test is stopped

2.6.2 Daily analysis

- Once a day, information is collected following the procedure above for all servers identified as having a AAAA record.
- Servers exhibiting either a null $\Delta t4$ or a null $\Delta t6$ measure are not taken into account.
- For each server the difference of latency is compared as: $\Delta lat\ (\%)=100\Delta t6-\Delta t4\Delta t4$
- Only values obtained in the limits of $\pm 300\%$ are kept. Others are manually investigated.

2.6.3 Produced graphics

- Ordinary density plots:
  - The number of bins is calculated as being the closest integer to $k=n$, with n being the number of servers having a retained measure and k being bounded to [5;20]
  - Average μ and standard deviation σ of the Δlat distribution are calculated. Only the values in the range $xmin=\mu-2\sigma$ to $xmax=\mu+2\sigma$ are plotted.
  - The number of values contained in the sub-range $xmin+i\cdot h;xmin+(i+1)\cdot h$ with $i\in[0\cdots n-1]$ and $h=xmax-xmink$ are then plotted at the abscissa $x=xmin+i+0.5h$

- Cumulated density plots

2.6.4 Constructing the historical plot

The historical plot is built by identifying each time a measure is taken, the percentage of servers for which the latency is lower through IPv6 than through IPv4.

Calculation is made as follow, using cumulated measurements made for each server:

1. Identify the point which as the lower latency difference
2. Select points below and above so to create a 3x2 matrix $Xi,Yi\ 1 \leq i \leq 3$
3. Calculate the regression line $y=\beta 0+\beta 1 \cdot x$ for these points.
4. The value β_0 then provides the searched valued to be used for the historical graph.

2.7 Monitoring IPv6 on the end-users side

The v6DEMON tool provides a feature that aims at monitoring the IPv6 connectivity of web clients, e.g. web browsers by providing webmasters with a Javascript code to be installer on their websites.

2.7.1 Overview

The script gives the IPv6 Observatory the possibility to monitor IPv6 deployment on the end-users side. By using a piece of Javascript code executed on web browsers, various anonymized data are collected: does the client support IPv6? If yes, which protocol is chosen when both IPv4 and IPv6 are available on the server? Through which ISP was used? ...

2.7.2 How it works

This tool uses a technique already deployed by various IPv6 monitoring tool (see 2.7.7 for references): it tries to access a remote resource using IPv4 and IPv6. Steps are described below:

1. The user visits a website;
2. The v6DEMON script is downloaded and started;
3. The script tries to access an image, through 3 distinct URLs:
    - IPv4 only URL (e.g. the FQDN -Fully Qualified Domain Name- has only an A record)
    - IPv6 only URL (e.g. the FQDN has only an AAAA record)
    - IPv4 and IPv6 (e.g. the FQDN has both an A and AAAA records)

Please note that:

- The script is run only once per day (thanks to a cookie);
- The script runs asynchronously, thus the page is not blocked during the test.

2.7.3 How to integrate it on a website

The integration on a website is straightforward: a webmaster willing to install the script needs to visit the v6DEMON tool website[20] and create an account.). Then by navigating to the "probed websites" page, he/she adds website(s) (multiple websites can be monitored). Each time a web-page is added, a piece of Javascript code is generated. This code needs to be copied and inserted on the website (see the dedicated web page[21] on the IPv6 Observatory website for the full description).

2.7.4 Retrieving statistics

Figures are available when logged in on the v6DEMON tool. Two figures have been made available to webmasters (proportion of IPv4 versus IPv6 users and IPv6 users evolution over the time).

2.7.5 Privacy

The IPv6 Observatory study does not collect any personal data: those that can be considered as private (like the IP address) are not conserved.

2.7.6 Source code

As per version 1.0, the source code is available on Github at the following address: https://gist.github.com/clarif/4984688.

2.7.7 References

This tool has been inspired by the following existing tools and documentation:

- Eric Vincke, IPv6 Deployment Aggregated Status[22]
- Google, Evaluating IPv6 adoption in the Internet[23]
- APNIC Labs, IPv6 tracker[24]

2.8 Web survey

For the fifth time since 2009, the Global IPv6 Deployment Survey has been run. This survey has been originally launched by ARIN with its members in March 2008. RIPE NCC as well as APNIC carried out this same survey in 2009. In 2010, 2011, 2012 and 2013, all RIRs participated to the survey making it truly global. The questions remain identical over years thus allowing compar-

[20] http://v6demon.ipv6observatory.eu
[21] http://www.ipv6observatory.eu/tools-webclients-monitor/
[22] http://www.vyncke.org/ipv6status/
[23] http://research.google.com/pubs/pub36240.html
[24] http://labs.apnic.net/script.shtml

ing the evolution from one year to one another. Only marginal adjustments are done to take into account the evolution of the context. The 2013 edition of the survey has been run by the IPv6 observatory. The survey is run as a web survey and is managed in a way that anonymity of respondent is preserved.

The survey, circulated as a web survey is structured into 3 parts respectively investigating the respondents' profile, their experience and their plans. The 2013 edition generated a strong response from 1515 ISPs and other organizations involved with the Regional Internet Registries, from 131 countries around the world. The general population of survey respondents has not significantly changed over the years.

The median respondent profile is a "*for-profit ISP in the RIPE NCC region that signed a registration services agreement and serves up to 10,000 customers with less than 50 personnel.*"

3 IPv6 DEPLOYMENT TRENDS

3.1 Introduction to datasets

In the context of the study, multiple dataset have been created in order to monitor IPv6 on websites. Those datasets are:

Dataset	Description	Number of web-sites	Tests periodi-city
EU27	Contains first 500 most visited websites per EU27 country (end of December, this dataset has been updated and contains now EU28 countries – e.g. with Croa-tia). Source: Alexa, http://www.alexa.com/	14 000	Every three day
UNIV	Contains websites of universi-ties[25]. Worldwide.	21 140	Every three day
EXTRA_TOP_500	Contains first 500 most visited websites for USA, Canada, China, Japan, Australia and India. Source: Alexa, http://www.alexa.com/	3 975	Every three day
GOV_EU27	Contains governmental sites from member states. Source: European Commission	4 115	Every three day
TOP_1M	Contains the TOP1Million most visited websites, worldwide. Source: Alexa, http://www.alexa.com/	1 000 000	Every week
TOP_1M_EXTENDED	Contains websites from all datasets. Source: Alexa, Euro-pean Commission, Webometrics	3 134 995	Every week

Figure 11 - Datasets description (numbers from January 2014)

3.2 Websites

Monitoring of IPv6 availabilities on websites is the most common exercise done by people will-ing to assess the level of the IPv6 deployment. Even if such measures provide relevant results, they can stand on their own and need to be completed by other indicators and provided within a consolidated view.

For this type of measure, the study team has been using datasets presented below. While this paragraph focus on AAAA records, it is worth noting that for each websites multiple things were tested such as IPv6 in the mail exchanger (MX record) or in the domain name, to name a few.

[25] Source : Webometrics, http://www.webometrics.info

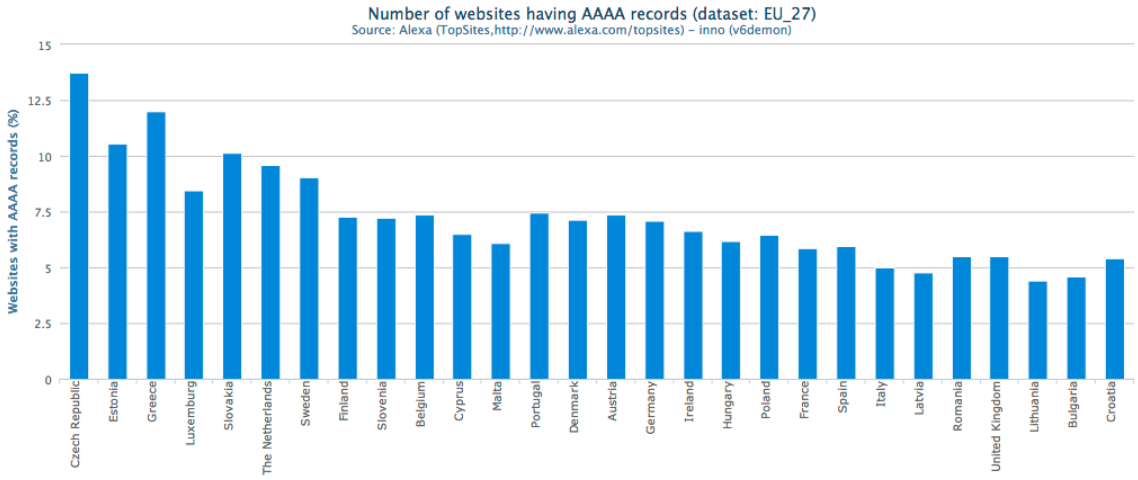

Figure 12 - % of websites having an AAAA record among TOP500 ranking (dataset: EU27)

To validate that a website supports IPv6, it is checked that its main domain name contains an AAAA record.

As shown on Figure 12, in December 2013 Czech Republic in ranked first in terms of number of websites having enabled IPv6 (13.7%) while the European average is 7.28%. This rank is essentially due to several efforts done by the Czech Government. In fact, The Czech Republic is one of the most active countries of the European Union in implementing IPv6, which has been mentioned in the Czech National Strategy as being mandatory and it is extremely urgent to deploy it. Since 2009, the Czech government adopted a resolution in 2009 that requires all ministries and other government administrations to replace it with IPv6 compatible equipment when replacing network equipment. The latest analysis that was carried out at the competent ministry has shown that all of the above mentioned institutions already meet this goal. The progression is notable here since in March 2012, most of the countries were under 4% (excepted Czech Republic, Slovenia, Luxembourg and Portugal). At the time of writing, most of the countries are over 5%.

It is also very interesting to see the evolution of this indicator over the project lifetime. While the European average was quite low in March 2012 (~2.7%), it is now around 7.28%.

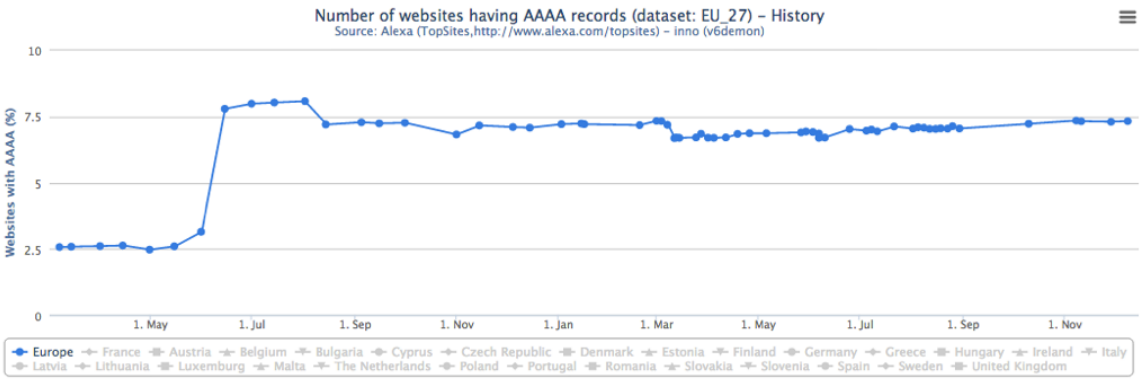

Figure 13 - % of websites having AAAA records (EU27)

The biggest positive action that helped in the uptake of IPv6 on websites (in Europe but also at the worldwide level, see Figure 14), is the World IPv6 lunch day[26] (edition 2012, organized by the Internet Society). On a specific day, websites administrators were requested to "turn on" IPv6 on their server and to let it enable after the event. As a consequence, the European average jumped from 2.6% to 7.79%.

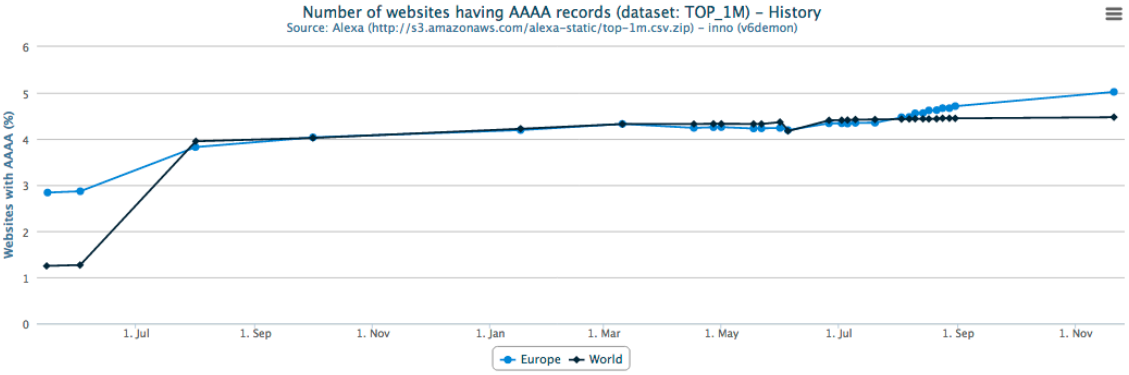

Figure 14 - % of websites having AAAA records (EU27 versus World)

Then, it is interesting to note that at some specific points in time, the average drops around ~0.5%. This happens mostly when datasets are updated. Indeed, rankings change over time so datasets are updated to contain new websites. This therefore indicates that new entrants (in the ranking) do not have AAAA record.

Moreover, in the context of the study, this indicator is used to provide data to the Digital Agenda Scoreboard maintained by the European Commission. Indeed, an IPv6 deployment indicator has been added in the Digital Agenda Score-

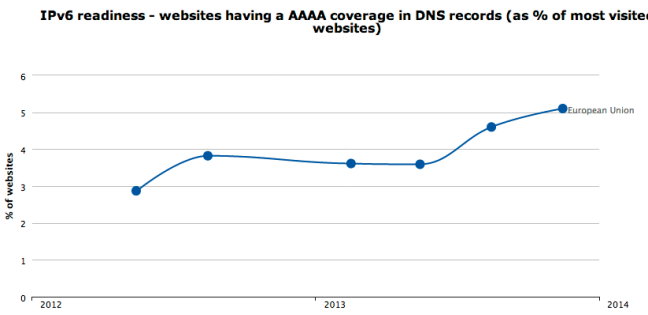

Figure 15 – IPv6 readiness (evolution) on the Digital Agenda Scoreboard

[26] http://www.worldipv6launch.org/

board[27], which assesses progress made with respect to the targets set out in the Digital Agenda. The two following figures (Figure 16 and Figure 15) show data on the Digital Agenda Scoreboard coming from the IPv6 Observatory.

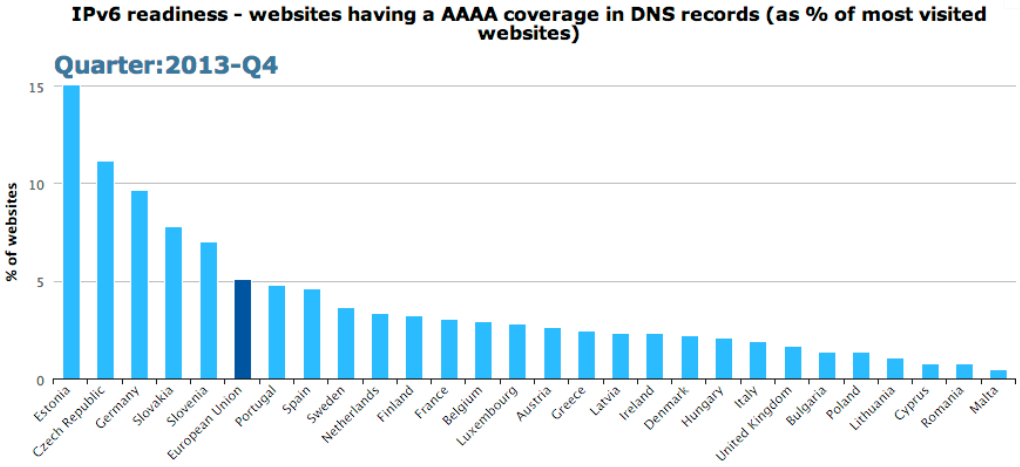

Figure 16 - IPv6 readiness on the Digital Agenda Scoreboard

Here again, the governmental actions play an important role in this ranking. Germany, for instance is successful in its implementation of the IPv6 protocol into its public and private networks. This achievement is due to some serious efforts to deploy IPv6:

- Coordination of IPv6 working group
- Proposals for the organization, address management and recommendations for technical implementation
- /32 blocks are self-administrated by Sub Local Internet Registries (Sub LIR): data centers, states, public network providers.
- Discussing technical policies (routing, security, etc.) with the community considering the special needs of public infrastructures
- Development of IPv6 profiles for ICT equipment and migration guide for government (Dual Stack for networks and applications)
- Providing an unified address concept for government
- Supporting migration to IPv4/IPv6-Dual-Stack
- Boosting IPv6 training and courses: RIPE NCC LIR Training

Thanks to data collected when checking IPv6 availability on website, a heat map has been produced and highlights parts of the world were IPv6 websites are located. Those websites have been selected out of a list of 2,7M websites, mainly coming from the TOP-1M ranking from Alexa. Among this list, 176,678 are reachable through IPv6 and have been geocoded thanks to the MaxMind's IPv6 GeoLite City[28]. Only 107 102 have been successfully geocoded and are displayed on this heat map.

[27] http://digital-agenda-data.eu/
[28] http://dev.maxmind.com/geoip/legacy/geolite/

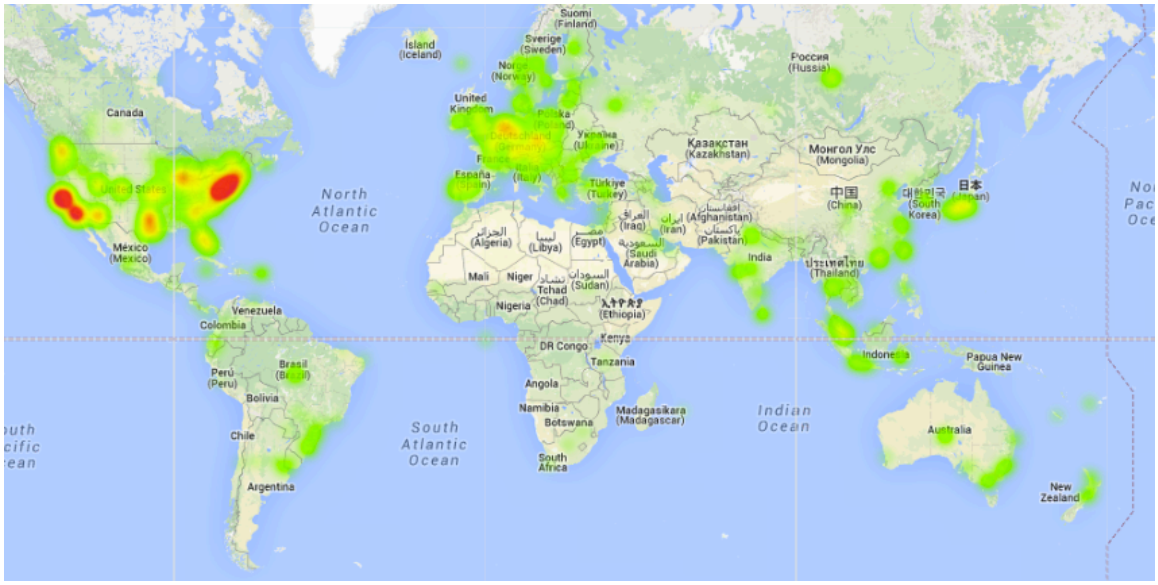

Figure 17 - Heat map for IPv6 websites[29] (source: IPv6 Observatory and Alexa for data, Google for mapping services)

3.3 Website, mail and DNS server: a consolidated indicator

Monitoring IPv6 deployment by following number of websites available though IPv6 gives a good but limited overview of the overall IPv6 deployment. Indeed, it is necessary to consolidate indicators so to provide a consolidated view.

A good example is for websites: when looking at IPv6 deployment on websites (AAAA), the European average is about 7.32% (December 2013), but when counting websites that are available in IPv6 and have an mail server (MX, mail exchanger) also available in IPv6, this average drops to 3.66%. More incredibly, this average drops to 0.95% when counting websites that are available in IPv6 with both a mail server and a DNS server available in IPv6. Worth noting that the number of websites having a mail server (even IPv4) has been checked so to avoid a bias: 96.45% (December 2013).

[29] Map generated with data from December 2013

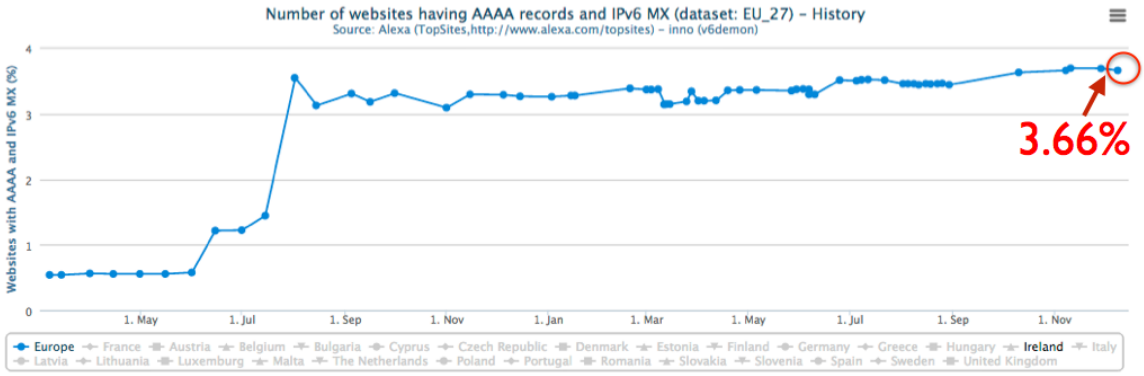

Figure 18 - % of websites with AAAA records and IPv6 MX

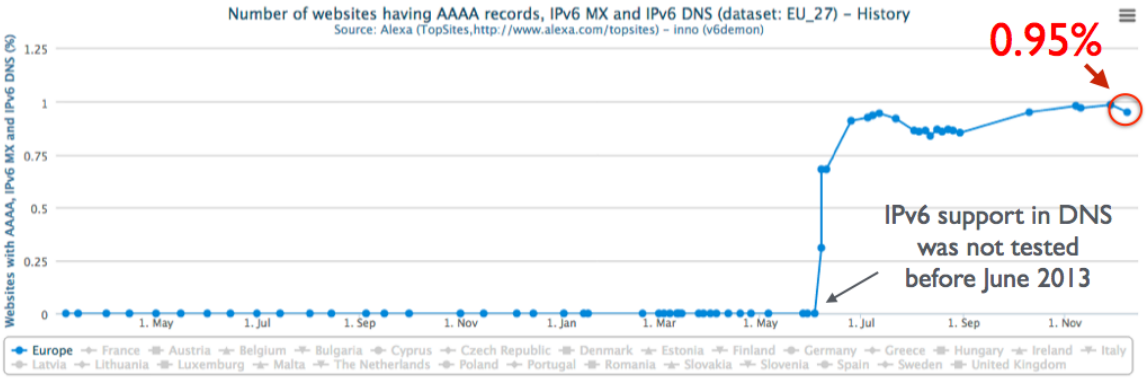

Figure 19 - % of websites with AAAA records, IPv6 MX and IPv6 DNS

3.4 Internet services providers (ISP)

3.4.1 Summary

The following report presents the findings of a benchmark of the visibility of IPv6 commercial offerings. The goal of the benchmark was to evaluate the presence and quality of IPv6 commercial offering to the general public in selected European countries. The methodology concentrated on an evaluation of publicly available information to better represent the scope of the actual deployment beyond limited pilots and the associated efforts of the ISP for providing end user technical support and a clear schedule of their deployment. The report concludes that the actual commercial deployment seems to be slowly debuting but is for now still limited.

3.4.2 Motivation and Objectives

As the inevitable IPv4 address depletion is looking increasingly close, IPv6 deployment progress and has started in recent years to reach the actual consumer market in at least some European member states.

However the scope of the deployment remains most often very limited to small pilot deployment. Actual full scale, native IPv6 connectivity by default for all customers is unfortunately something seldom seen for now for the generalist B2SME/B2C ISP market.

The availability of commercial offering by Internet Service provider is one of the metrics that was chosen to monitor the actual availability of IPv6 connectivity to end-users. The complexity of the ISP market, proposing different commercial offerings, based on different network (DSL, Cable, Fiber, Mobile), with different technological options for the deployment of IPv6 means that the "Commercial Availability" of IPv6 can seldom be treated as a "Yes" or "No" question. We have therefore chosen several criterions and a ranking methodology to evaluate the level of commercial availability of IPv6 provided by the ISP.

In this study we have also put a special emphasis on the visibility of the IPv6 connectivity offers for end-users. We consider this visibility as important as, although it is not the case currently, the availability of IPv6 offers could be a competitive argument for ISP that could accelerate the deployment. The study therefore focused on analyzing the visibility of IPv6 in the commercial offerings of ISPs for the general public. The study was therefore conducted mostly by gathering, confronting and analyzing the information publicly available on the ISP commercial offers, on the ISP websites, technical support forums, blogs and press releases.

This methodology should help us to better evaluate and communicate on the actual IPv6 availability to the end users. This ranking should be useful for concerned stakeholders, including the ISP themselves which will have a tool to evaluate their offers and the competitions'.

3.4.3 Methodology

3.4.3.1 Scope of the study

The current study present only a partial result focused on some selected countries and some selected ISP and doesn't pretend to represent the full scope of ISP commercial availability in Europe. However, the result obtained on this first sample can already be considered as representative of the global trend and provide some useful information on the visibility and availability of IPv6.

In this first step the study concentrated on 68 major operators in 12 European member states: Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Luxemburg, Netherlands, Portugal, Spain and the United Kingdom.

3.4.3.2 Overall methodology

As presented above the target of this study was to evaluate the availability of public commercial offering based on IPv6 by Internet Service Provider, and their visibility.

For each selected country, the study consisted to:

- Select several well known, visible, commercial internet service providers.
- Gather information if possible from multiple sources on the presence/absence and details of IPv6 enabled offers.
- Analyze the information gathered following several criterions

- Establish a ranking

3.4.3.3 Information gathering

Trying to evaluate the actual visibility of commercial offerings for potential end users, the study concentrated on gathering information from easily accessible, publicly visible sources. This included:

- The ISP website
- The ISP technical forum and frequent asked question section (when available)
- Press releases
- Blogs, technical information website and personal websites

For each ISP:

- When information was available we tried as much as possible to select the most recent and official information sources and to confront several sources to validate the data.
- When no information was found after a reasonable time we concluded that no public IPv6 offering was available (around 30 minutes spent on average on each ISP).

The choice of this methodology implies that the information in the report may not be 100% accurate on the actual availability of commercial offers, but it present a view of the public visibility of IPv6 for potential concerned customers looking for information.

3.4.3.4 Evaluation criterions and weighting

To evaluate accurately the availability of IPv6 commercial offering and to reflect correctly the diversity and complexity of the answers the following criterions have been selected. For each criterion we present the question, the potential answers and the point associated with each answer. The weighting of the criterion has been done to reflect the importance of the visibility / accessibility of user information and the scope of the deployment (from limited deployment to simple pilots to full scale by default choice for all users).

Criteria are detailed in Annex (see 6.4).

3.4.4 Ranking

The complete ranking is available here (link to file).

3.4.4.1 Belgium

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
edpnet	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	**16**
Belgacom	1 - Forums/Blogs	1 - Limited	1 - Yes	1 - Distinct offers	0 - No / on Request	2 - Native	**8**
Telenet	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Brutele	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Mobistar ADSL	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**
Numericable	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**

3.4.4.2 Denmark

The high number of ISP represented for Denmark is due to the availability of relevant, up to date information on a local blog: http://okey.dk/2012/06/kan-de-danske-internetudbydere-levere-ipv6-her-i-2012/

3.4.4.3 France

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Free	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	1 - New Users	1 - Tunnel	**20**
SFR	2 - Full Info/Support	1 - Limited	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	**13**
France Telecom	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Bouygues Telecom	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Numericable	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**

3.4.4.4 Germany

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Unitymedia	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	1 - New Users	2 - Native	**21**
Deutsche Telekom	1 - Forums/Blogs	1 - Limited	2 - None	2 - No Distinctions	1 - New Users	2 - Native	**15**
kabel deutschland	1 - Forums/Blogs	1 - Limited	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	**10**
QSC	1 - Forums/Blogs	1 - Limited	2 - None	1 - Distinct offers	0 - No / on Request	2 - Native	**9**

3.4.4.5 Greece

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
forthnet	2 - Full Info/Support	1 - Limited	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	**13**
OTE	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
wind gr	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Hellas on line	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**
On Telecom	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**

3.4.4.6 Ireland

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Airwire	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	16
Eircom	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	2
UPC Ireland	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	2
Digiweb	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.7 Italy

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Telecom Italia	2 - Full Info/Support	1 - Limited	2 - None	2 - No Distinctions	0 - No / on Request	2 - Native	13
Fastweb	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	1 - Tunnel	3
vodafone italy	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
wind infostrada	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
Tiscali	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.8 Luxemburg

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
P&T Luxembourg	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	1 - New Users	2 - Native	21
CEGECOM	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
TANGO	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.9 Netherlands

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Telfort	2 - Full Info/Support	2 - All but Mobile	2 - None	2 - No Distinctions	1 - New Users	1 - Tunnel	20
KPN Internet	2 - Full Info/Support	1 - Limited	2 - None	2 - No Distinctions	1 - New Users	2 - Native	18
Ziggo	1 - Forums/Blogs	1 - Limited	2 - None	1 - Distinct offers	0 - No / on Request	2 - Native	9
Tele2	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	2
edpnet	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.10 Portugal

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
vodafon.pt	2 - Full Info/Support	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	5
Zon	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	2
Sapo	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
cabovisao	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.11 Spain

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
Telefonica	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	2
Jazztel	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
Ono	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
Orange Spain	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0
Vodafone Spain	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	0

3.4.4.12 United Kingdom

ISP	User Information / Support	Availability of Commercial Offers	Additional Cost	Professional Specific Offering	By Default?	Type of Connectivity	Ranking
British Telecom	2 - Full Info/Support	1 - Limited	2 - None	2 - No Distinctions	1 - New Users	2 - Native	**18**
Sky Broadband	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Virgin Media	1 - Forums/Blogs	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**2**
Talk Talk	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**
Orange Home	0 - No	0 - None	0 - No IPv6	0 - No IPv6	0 - No / on Request	0 - No IPv6	**0**

3.4.4.13 Overall

Based on these results the following ranking can be established.

Country	Global Note	ISP Evaluated	Average Note
Germany	55	4	13,8
Netherlands	49	5	9,8
France	39	5	7,8
Luxembourg	21	3	7,0
Italy	37	6	6,2
Ireland	20	4	5,0
Belgium	28	6	4,7
United Kingdom	22	5	4,4
Greece	17	5	3,4
Denmark	38	16	2,4
Portugal	7	4	1,8
Spain	2	5	0,4

3.4.5 Conclusions

Based on the current data we can already conclude that the deployment of IPv6 commercial offers is slowly starting in 2013. As presented in previous reports, the core network is mostly ready for IPv6 deployment and ISPs are now mostly concentrating on enabling the access network. Most ISP first concentrate on limited pilots and trials before opening progressively the availability of IPv6 addresses to all their customers. Full scale native deployment is still very rare and even when available IPv6 is still rarely proposed as the standard, default option for cus-

tomers. Most ISP migrating to IPv6 prefer to only enable it for new customers, leaving the migration of legacy customers as a future topic.

However the creation of specific commercial offering based on IPv6 distinguishing between B2C and B2B customers seems to be quite rare and most often the deployment of IPv6 comes at no additional cost for the customer.

In most case (72% of the ISP evaluated in this report) at least minimal information was found available from blogs, or technical websites. However in a majority of case (54% of the ISP evaluated in this report) the information was partial and/or not coming from an official source, and this still leaves more than 27% of the European ISP evaluated in the report with no publicly available information on their plan for IPv6.

As explained before the current report doesn't pretend to be exhaustive as only a few ISP have been evaluated for some selected countries. Moreover the study concentrated on the visibility of IPv6 offering from public sources of information and therefore might not represent entirely the actual deployment efforts of some ISPs. Finally the study only represents a temporary vision of an evolving situation. The study can therefore be completed and pursued in several ways: by evaluating more ISPs in more countries, by contacting directly the ISP to verify / validate the information publicly available, and by updating the ranking regularly.

3.5 Quality of service

Measuring quality of service related to IPv6 is a complex task since IPv6 can be measured in every layer of the Internet architecture. In the context of the study, datasets used to monitor IPv6 deployment on websites have been used as a framework to test IPv6 Quality of Service (see 2.6 for the methodology): for each website which has both IPv4 and IPv6 enabled, the v6DEMON tool sends HTTP requests and compares return. Tests are done from France, Luxembourg and China.

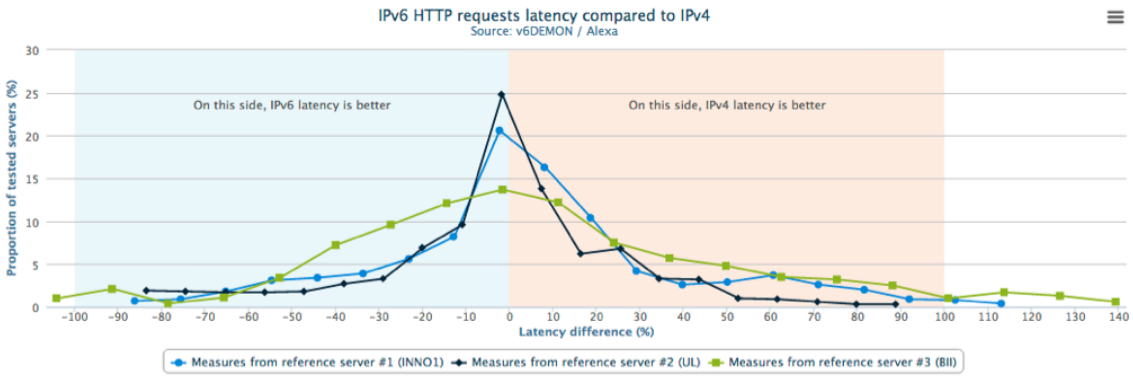

Figure 20 - HTTP requests latency compared (IPv4 versus IPv6)

The Figure 20 above that there is no real differences between both protocols and when checking the evolution of results, this behaviour is constant over time. This indicates that there are no major difference in terms of quality of services between IPv4 and IPv6. One should note that

the Figure 20 shows a very little advantage to IPv6, but this would need to be further investigated to be confirmed over time.

Moreover same conclusions can be done for both the Europe and China.

3.6 Traffic

Worldwide IPv6 traffic is still negligible as compared to IPv4. During the study, the team has monitored statistics on the website of the Amsterdam IX[30] (Exchange Point).

In January 2013, IPv6 traffic was 0.45% of the entire IP traffic. In December 2013, it represents 0.65% of the entire traffic, which is still low. However, it still represents a huge amount of data.

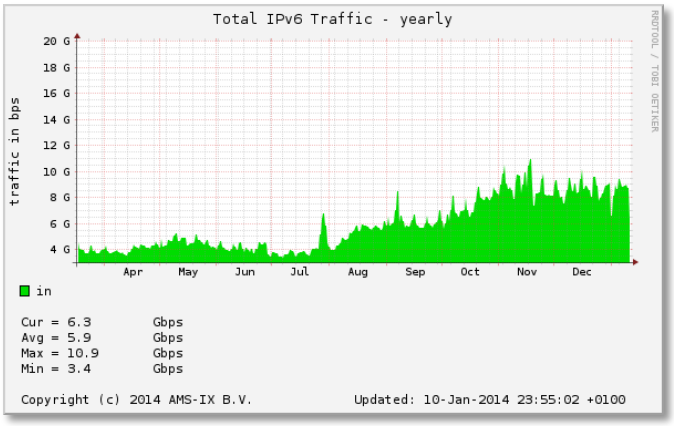

Figure 21 - IPv6 traffic at IMX (source: https://www.ams-ix.net/)

In details, numbers from December 2013 show an average IPv6 traffic of was 8.8 Gigabit/second[31]. All the full year (2013), the average for all traffic was 1.339 Terabit/second[32].

3.7 Usage

It is also very interesting to have a look at IPv6 usage: do Internet users connect to websites in IPv6? Statistics from Google[33] are showing end of December an average of 2.5% users connected in IPv6 (to access Google services). Since mid-2011, this average doubles every 9 months. Furthermore, forecasting data are showing that based on the actual progression, the percentage of users connected in IPv6 will jump to 50% in 4.5 years (following a logistic model).

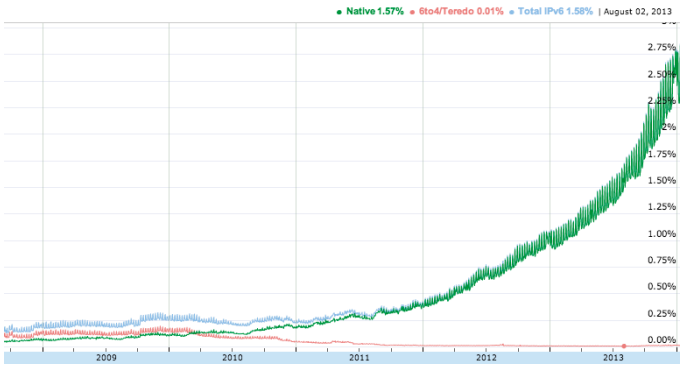

Figure 22 – IPv6 usage as seen by Google (source: Google)

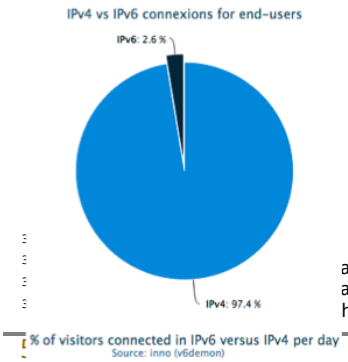

Figure 23 - IPv6 usage as seen by the IPv6 Observatory

As part of the study, a similar exercise has been done: tests have been done on Internet users to check if they had IPv6 connectivity (and if it was the case, which was the preferred protocol when accessing websites having both IPv4 and IPv6).

atistics/sflow-stats/ipv6-traffic
atistics
html

Obviously much less users have been tested, and consequently much less data has been collected. However, end of December results from the IPv6 Observatory tests were showing a 2.6% average of users connected in IPv6. The full methodology used to obtain this data is described in the section 2.7. However, it is worth noting here a little bias as most tested users where located in France or in Europe.

Usage can also be monitored on company providing Content Distribution Networks (CDN) services, such Akamaï or Amazon. A CDN is a service that allow websites operators to store their assets (for example images, videos, ...) on server that are geographically close to their customers, thus making download faster. Content stored on Akamaï servers are available in both IPv4 and IPv6, and Akamaï makes its IPv6 statistics available publicly on its website[34].

The figure below shows these statistics highlighting a constant progression of IPv6 hits (requests sent to the Akamaï service in IPv6).

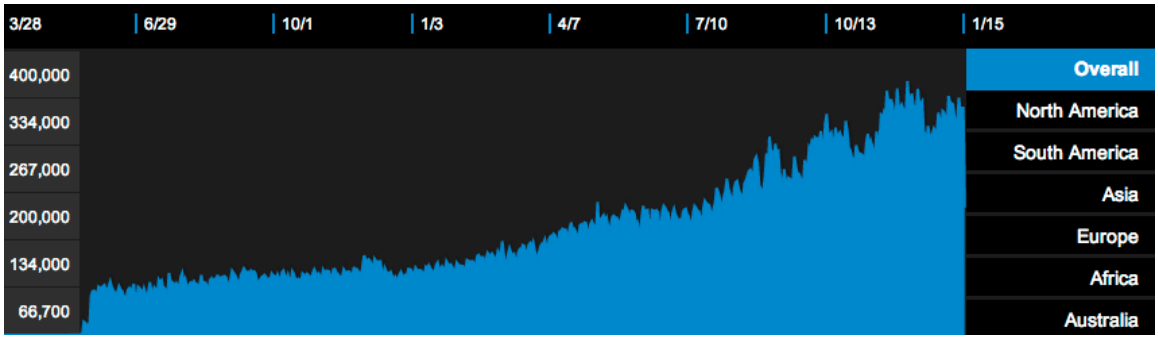

Figure 24 - IPv6 statistics from Akamaï

3.8 Addresses allocation

As an introduction, it is important to note once again that there are more connected devices that available IPv6 addresses since approximately 2006/2007. Moreover, in a recent study on Internet of Things, Cisco estimated that "there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020. It is important to note that these estimates do not take into account rapid advances in Internet or device technology; the numbers presented are based on what is known to be true today"[35]. Such conclusion amplifies the need of having IPv6 networks well deployed.

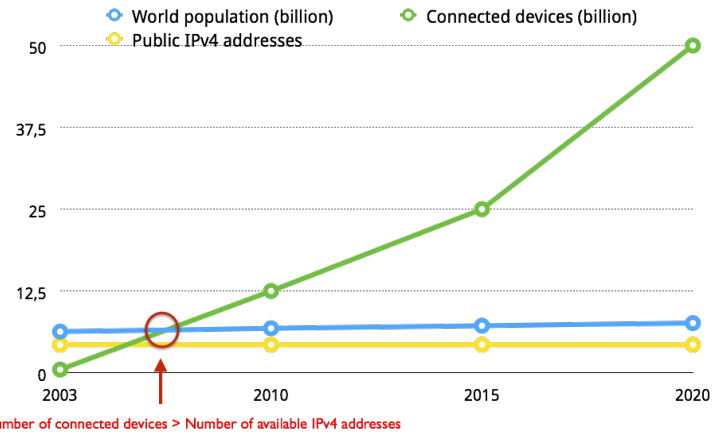

Figure 25 - IPv4 available addresses vs connected devices (source: Cisco IBSG, April 2011)

It is now interesting to compare these figures with statistics of IPv6 addresses alloca-

[34] http://www.akamai.com/ipv6
[35] Source CISCO IBSG, April 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

tion. Figure 26 shows percentage of IPv6-enabled Autonomous Systems (AS, e.g. IPv6 networks) registered in all countries (in yellow), European Union (purple) and all countries excepted European Union (blue). The positive fact is that there is a continuous increase in all region of the world with a more important progression since 2010.

It is noticeable that since 2010, the percentage of IPv6 addresses allocation starts significantly increasing. Therefore, it is interesting to evaluate the main actions and efforts that have been adapted by private and public organizations. We will take examples of each continent:

Europe

Germany and Czech Republic are two good examples, as previously explained. Another example is France:

- The French operator Free, which implemented IPv6 connectivity since 2007, has a key role in this European ranking. In 2009, Free recorded more than 310,000 IPv6 users. Orange, in other hand, has been one of the first global IPv6 providers over the VPN MPLS network since 2009.
- In September 2010, France had six providers[36] that serve their users with native IPv6 connectivity. 143 IPv6 prefixes have been allocated to France (Orange /19). There were two IPv6 exchange points operating in France (IX).
- Also, even if the impact of this action was probably limited, the Action Plan for ICT "Digital France 2012" document, which included activities for IPv6 deployment, was published in March 2009.

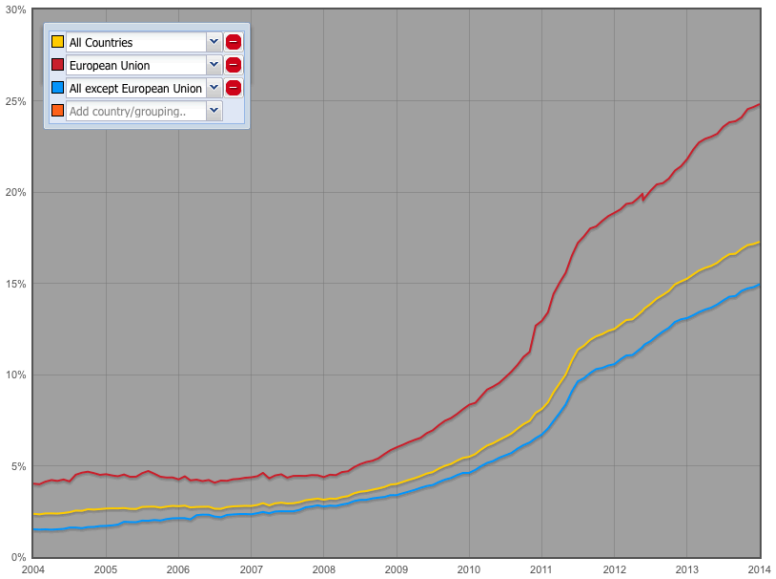

Figure 26 - IPv6 enabled networks (source RIPE, http://v6asns.ripe.net)

USA

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

[36] https://www.sixxs.net/faq/connectivity/?faq=native&country=fr

Japan

Japan is one of the most technologically advanced countries in the world. Japan adopted the "IPv6 Forum Ready" program with which they started testing device compatibility with IPv6. Based on this program and based on awarding the IPv6 Ready logos, the Japanese industry became the leading world manufacturer of IPv6 equipment.

Japan is investing between 10 and 13 million dollars annually into the IPv6 technological market. The global investment in Ipv6 market reached 1.55 milliard dollars by the end of 2010.

Korea

The Korean government intended to achieve a perfect transition to IPv6 in the public sector[37] and obtain 10 million IPv6 users by 2011. The next milestones in the action plan of the Korean government were the following:

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

[37] http://www.ipv6.com/articles/deployment/IPv6-Deployment-Status.htm

3.9 Certifications

3.9.1 IPv6 training status

Demand of ICT skills keeps growing depsite the economic crisis. While the assumed IT investment growth is around 2,2%, shortages of skills continue to increase in Europe. The figure bellow translates expectation of vacancies in e-skills from 2011 to 2015.

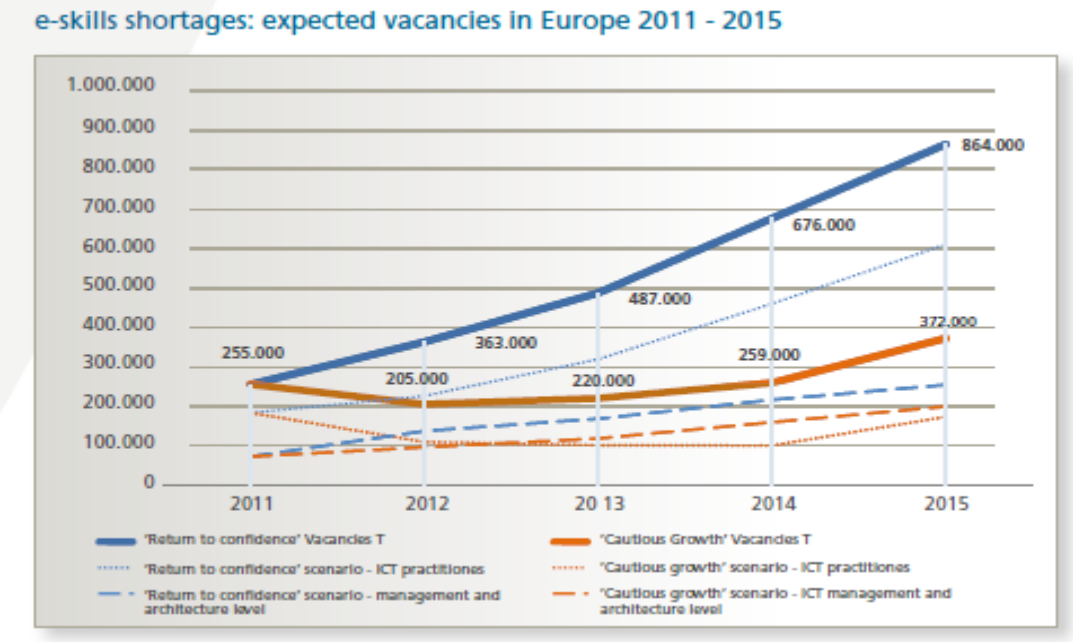

Figure 27 - e-skills shortage in Europe (source: Empirica forecast, January 2013)

Therefore, the demand for **ICT practitioners** is growing by around 3% a year, outstripping the supply. Expected vacancies by 2015 vary from **372,000 to 864,000**, and many of these will remain unfilled unless more is done to attract young people into computing degrees and to retrain unemployed people. In this context, ICT industry training and certification is clearly an element in the possible solution.

IPv6, which is a corner stone of the future Internet and ICT fields,is one of the main aspect concerned by ICT training and certifications.While CGN/ NAT and tunneling solutions are not substitute for IPv4,IPv6 is the only reliable solution to replace IPv4 and provide a huge number of IP addresses.

Given the context above,three main categories of stakeholders are identified:

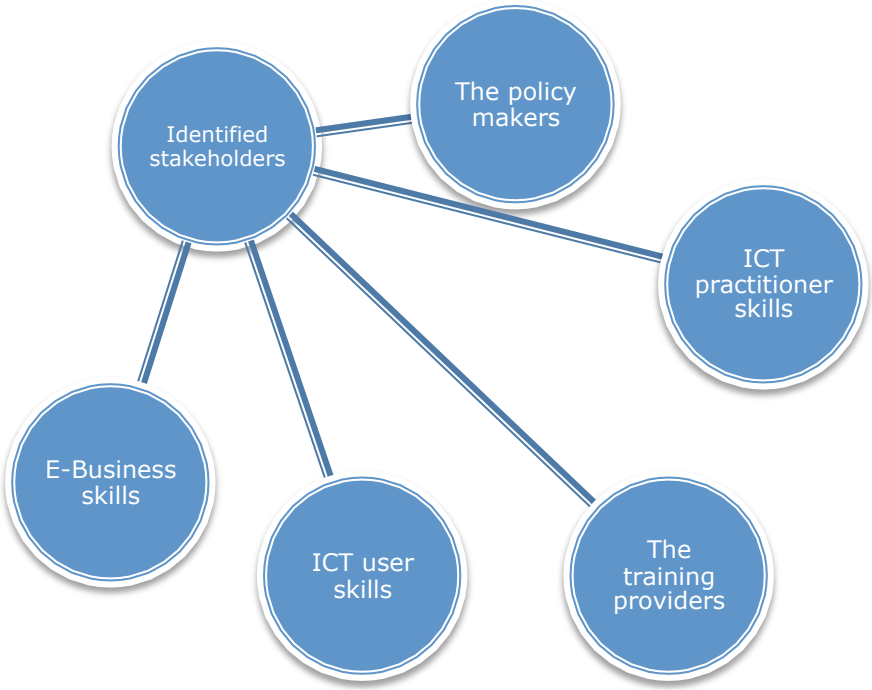

Figure 28 - Stakeholders concerned by IPv6 training

- **The policy makers** at regional national and European levels.
- **The training providers:** Any organisation or person providing training. It includes both public organisations such as universities and private organisations.*Cisco or Microsoft fall into this category.*
- **The Training beneficiaries**:There are categorises of beneficiaries according to the profile of skills needed:

ICT practitioner skills: These are the capabilities required for researching, developing,designing, strategic planning, managing, producing, consulting, marketing,selling, integrating, installing, administering, maintaining, supporting and servicing ICT systems.

ICT user skills: This category represents the capabilities required for the effective application of ICT systems and devices by the individual.

E-Business skills: These correspond to the capabilities needed to exploit opportunities provided by ICT, notably the Internet; to ensure more efficient and effective performance of different types of organisations; to explore possibilities for new ways of conducting business/administrative and organisational processes.

3.9.2 Certifications status

To monitor the certifications status, it is interesting to distinguich two kind of certification according to the targeted component:

3.9.2.1 Certification of people (IPv6 skills)

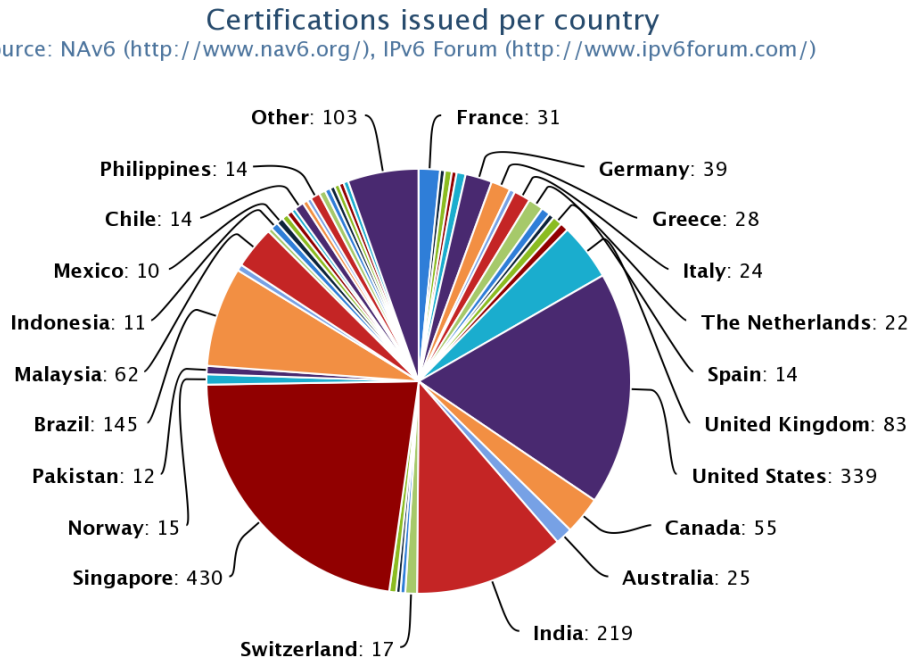

Figure 29 - Certifications issued per country

The figure illustrates the number of certifications issued per country. At the European level,the United Kingdom provides the highest number of certifications (83), followed by Germany (39) and France (31).

Asia presents more important numbers in terms of issued certifications. Singapore,provived a total of 430 certifications,which is equal to all the certifications issued in the European evaluated countries.

It is due to initiatives such as **PROGRESO,** which is offering IPv6 Forum Certified Network Engineer Courses helping companies which are still grappling with the issues surrounding the transition to IPv6. The Progreso courses trains IT managers and engineers to maintain interoperability and facilitate a smooth transition of the IP protocols across their networks. This initiative is partnering with USM (Universiti Sains Malaysia) - The National Advanced IPv6 Centre (NAV6) to offer three levels of certification to IT managers, engineers and end-users. India has also 219 issued certifications which also higher than the number issued in Europe.

On the American continent, US (339) and Brazil (145) have the highest number of certifications.

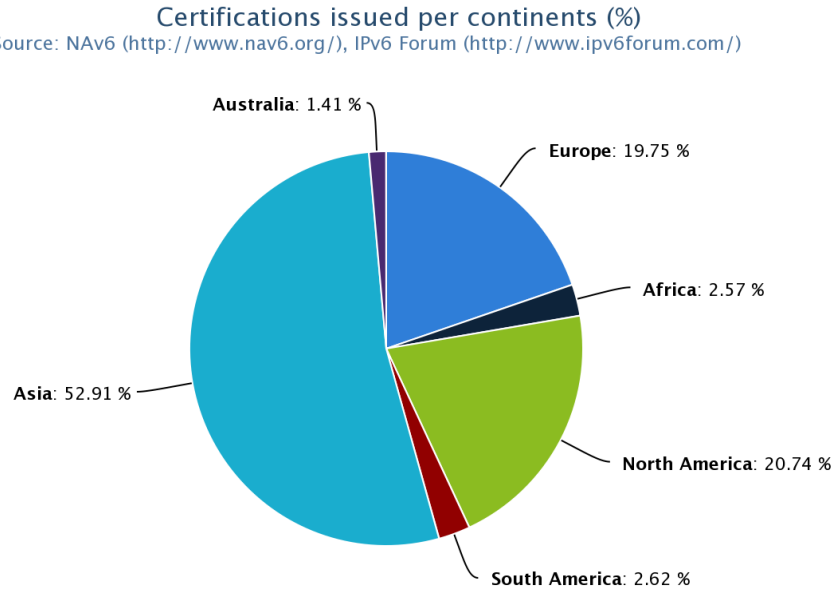

Figure 30 - Certifications issued per continent

This figure confirms what the previous one translates. In fact, Asia,leader in IPv6 adoption, reaches 52.91% of the global issued certifications which superior than the total certifications provided elsewhere (North America 20.74%,Europe 19.75%,Africa 2.57%,South America 2.62%,Australia 1.41%).

IPv6 Forum

The IPv6 Forum is a not-for-profit organization composed of leading Internet vendors, industry subject matter experts, and research & education networks. Recently, it launched a certification recognition program where training institutions it has certified will be identified by a logo. IPv6 Forum offers two levels of certification:

- Silver, for beginner and intermediate skills and topics.
- Gold, for all skills levels and advanced topics on IPv6.

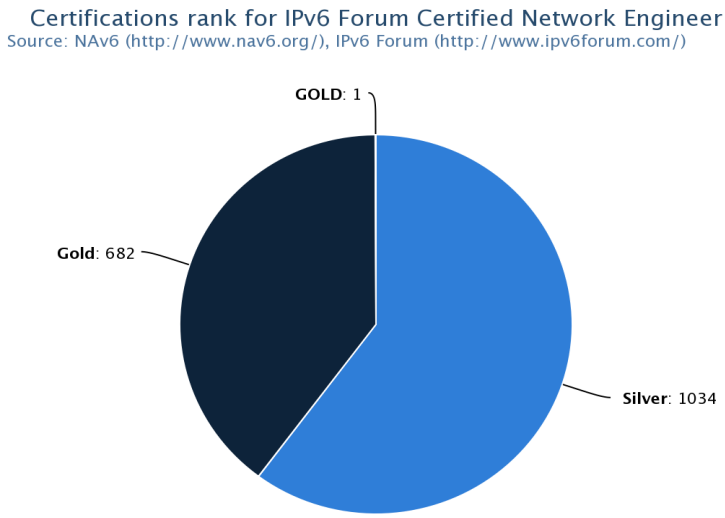

Figure 31 - Certifications rank for IPv6 Forum Certified Network Engineer

Cisco Career certifications

Cisco provides five levels of network certification: Entry, Associate, Professional, Expert and Architect, the highest level of accreditation within the Cisco Career Certification program.

- Entry which serves as starting points for individuals interested in starting a career as a networking professional.
- Associate level begins directly with CCNA (Cisco Certified Network Associate) for network installation, operations and troubleshooting or CCDA (Cisco Certified Design Associate) for network design. Think of the Associate Level as the foundation level of networking certification.
- Professional: The Professional level is an advanced level of certification that shows more expertise with networking skills. Each certification covers a different technology to meet the needs of varying job roles.
- Expert: The Cisco Certified Internetwork Expert (CCIE) certification is accepted worldwide as the most prestigious networking certification in the industry.
- Architect: Cisco Certified Architect is the highest level of accreditation achievable and recognizes the architectural expertise of network designers who can support the increasingly complex networks of global organizations and effectively translate business strategies into evolutionary technical strategies.

The Cisco training can only be commercialized by Cisco Learning Partners certified Paterners.

Hurricane Electric

Hurricane Electric runs an IPv6 certification project allowing evaluation through a quick and easy test of the basic IPV6 competencies of participants. The certification and the learning materials are free.

3.9.2.2 Certifications of the products

The figure bellow illustrates the worldwide IPv6 product certification. This kind of certification is slowly increasing. Over the past 9 years, the number of IPv6 product certification moved from 155 in January 2005 to 1664 in July 2013.

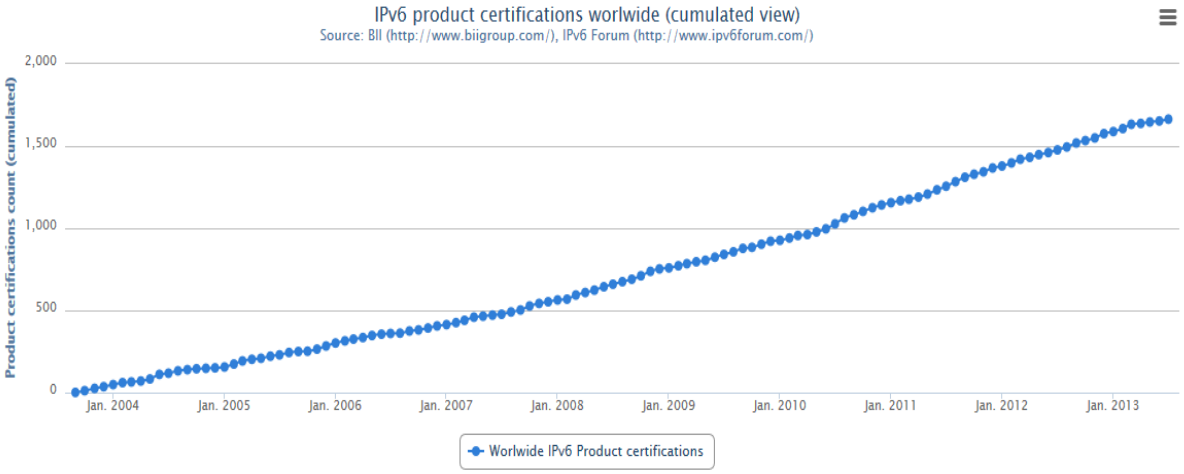

Figure 32 - Worldwide IPv6 products certifications

DoD IPv6 Product Certification in US

It is a program that mandates the Joint Interoperability Test Command (JITC) in Fort Huachuca, AZ, to test and certify IT products for IPv6 capability according to the Request For Comments (RFCs) outlined in the DoD's IPv6 Standards Profiles for IPv6 Capable Products. Once products are certified for special interoperability, they are added to the DoD's Unified Capabilities Approved Products List (UC APL) for IPv6.

DoD's IPv6 Standards

The DoD IPv6 Standards Profiles for IPv6 Capable Products (DoD IPv6 Profile) is a document that lists the six agreed upon product classes (Host, Router, Layer 3 Switch, Network Appliance, Security Device, and Advanced Server) and their corresponding standards (RFCs). It lists each standard according to its level of requirement:

- MUST: The standard is required to be implemented in the product now.
- SHOULD: The standard is optional, but recommended for implementation.
- SHOULD+: The standard is optional now, but will be required within a short period of time.

3.9.3 Other facts observed during the study

Beyond certification data on training of people and products, it has been observed that many engineers and technicians still see IPv6 as a simple address update of IPv4 and miss the potential of IPv6: this highlights the need for stronger IPv6 education of IT personal. As an example, it

is still frequent to find in programs source code variables that are not long enough to hold IPv6 addresses.

This is linked to the fact that IPv6 is not yet well taught in Universities and Engineers schools.

3.10 Web survey: IPv6 gaining momentum

Last July, 78% of all respondents to the 2013 Global IPv6 Deployment Monitoring Survey indicated to have an IPv6 presence. Only 8% of all respondents indicated still not to consider IPv6, with reasons ranging from those who feel they have plenty of IPv4 addresses available to cover their needs for the coming years, to some ISPs who have adopted a strategy of obtaining (buying) more IPv4 addresses when needed in order to serve their clients.

In addition, Carrier Grade Networks (CGN, or NAT) are mostly not introduced instead of IPv6, but along with IPv6. This is indicated by more than 70% of all respondents who introduce or use CGN.

In general, we see that the use of IPv6 is increasing in terms of the number of users getting involved, although still 35% of all responding ISPs indicate their customer base is not using IPv6, yet.

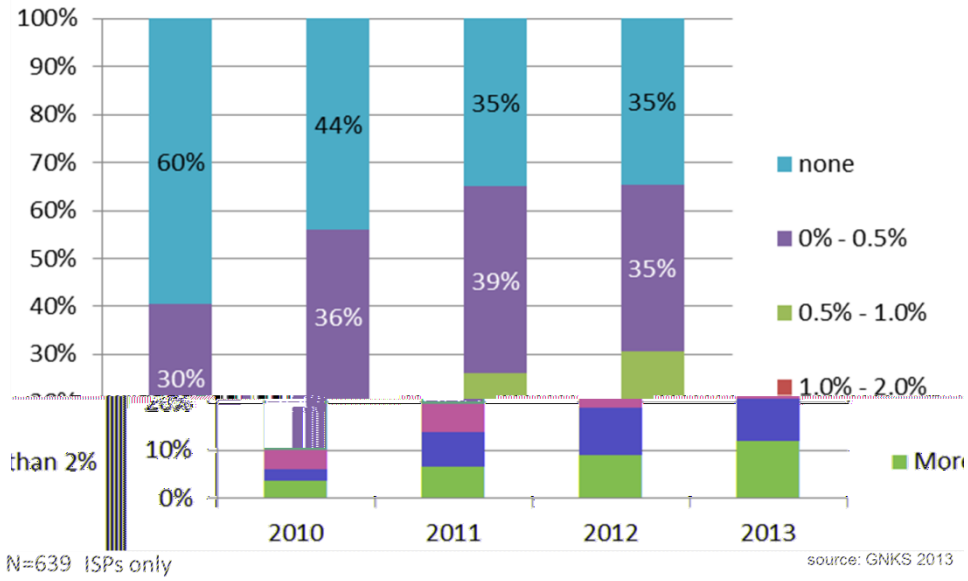

Figure 33 - What percentage of your customer base uses IPv6

At the same time, 72% of all ISPs indicate to promote, or consider promoting IPv6 to their customer base, and an additional 20% is thinking about that. From all organizations participating to the survey, only 8% does not consider to use IPv6, yet. This has not changed much since 2011. Main reason for this is that there is no perceived business need, yet. When considering the scores on "reasons not to consider adopting IPv6, yet" , it is noticeable that the reasons diminish in importance, across the board, as compared to earlier years.

In 2013 there is a further, slow but not significant, decline in respondents that indicate they don't have an IPv6 presence.

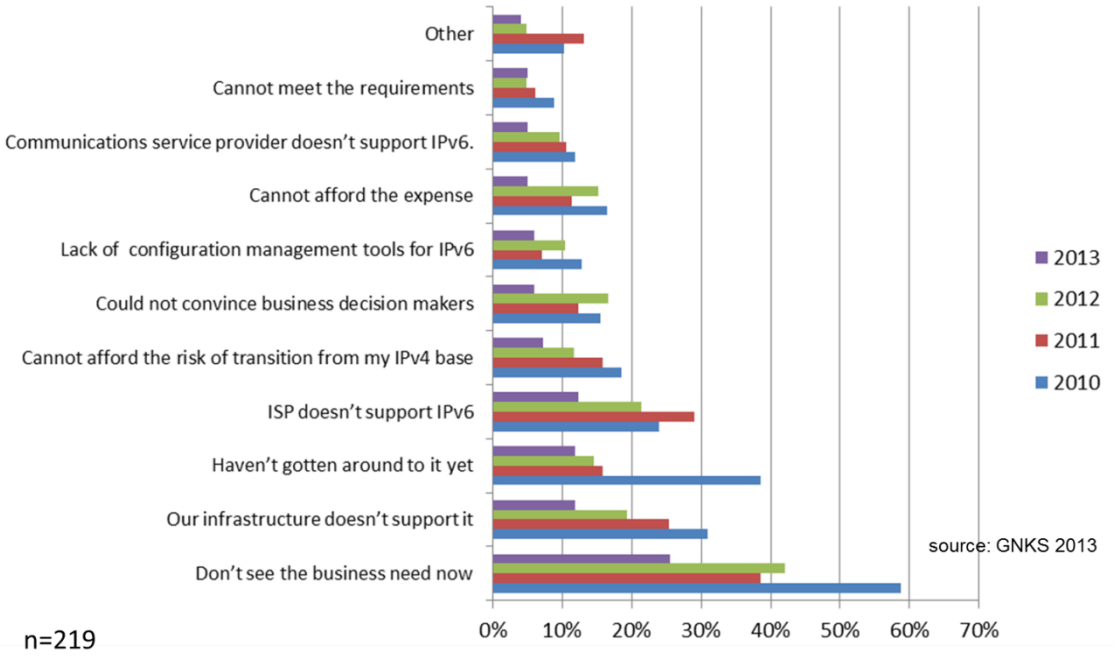

Figure 34 - If your organization hasn't considered having an IPv6 allocation/assignment, why not?

The same is true for the expected biggest challenges. Costs and being able to make a business case are still the main expected hurdles, and much less so than in earlier years. In particular, availability of knowledgeable staff has reduced significantly as perceived "biggest hurdle". From those not planning to transition to IPv6 a number indicates that they have plenty of IPv4 addresses for the time to come. Only one respondent indicates that it is not needed because of further introduction of NAT.

Does your organisation have an IPv6 Presence?	2013	2012	2011	2010
No	22%	23%	27%	36%
Yes, only within internal networks	10%	9%	19%	8%
Yes, only on the Internet	23%	20%	11%	14%
Yes, both within internal networks and on the Internet	47%	49%	43%	42%

Figure 35 - Does your organization have an IPv6 presence (n=1084)

Over the years, there is no significant shift in what the biggest perceived hurdles are. "Vendor support" continues to score highest, with consistently around 60% of all respondents indicating this as the perceived biggest hurdle. "Availability of knowledgeable staff" continues to be a hurdle according to about 50% of all respondents, and about 40% continues to indicate the "costs" and "business case" keep developments back.

When IPv6 introduction is brought in practice, the biggest problems experienced continues to be the lack of user demands (consistently above 50%) and technical problems (consistently just under 40%). The nature of implementation of IPv6 continues to be about 95% dual stack (also consistent since 2010). There is a slight increase of application of native IPv6 (was 76% in 2012, now 81%), and NAT use remains consistent at 5%.

In terms of planning, it is clear that the "horizon" for being ready is coming closer … and the increase of preparedness is slowing down as most of the respondents do now have their plans or implemented their plans, as is clear from the figure below.

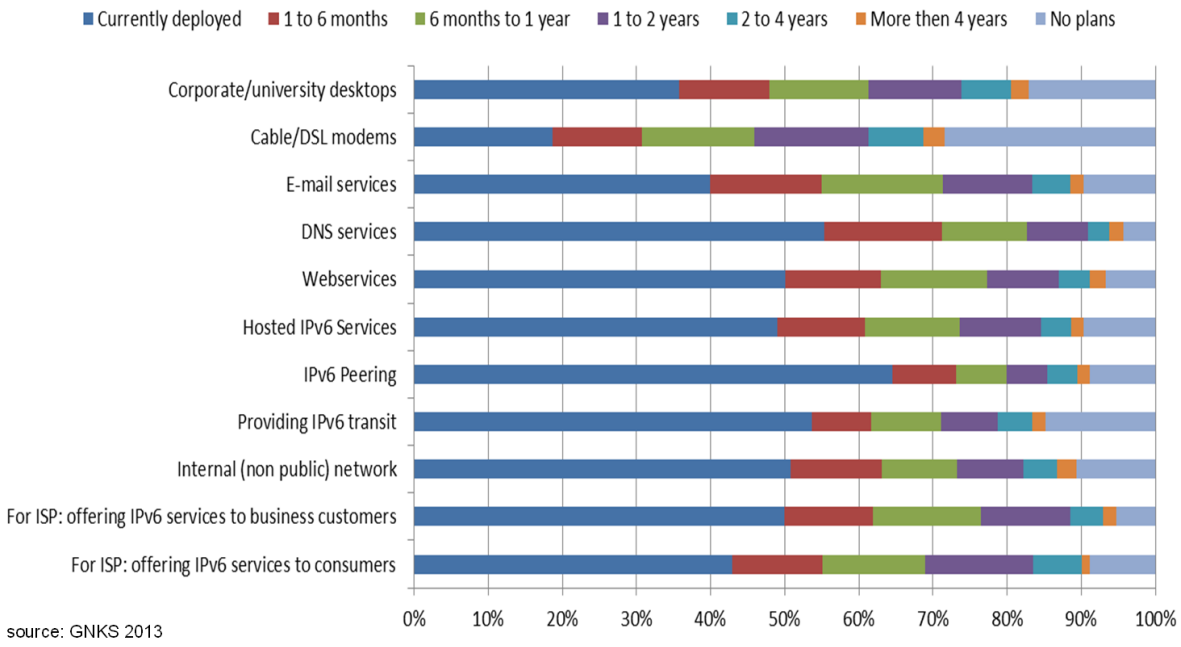

Figure 36 - Which best describes your organization's IPv6 implementation (plans)

Progress can generally be seen in the first part (currently deployed) growing, as many respondents that indicated last year to plan to move forward implementation within the year have been busy achieving this. However, it is also clear that not all respondents have been able to achieve their ambition, for instance if we look to one of the bars above in more detail and compare the responses over the last four years:

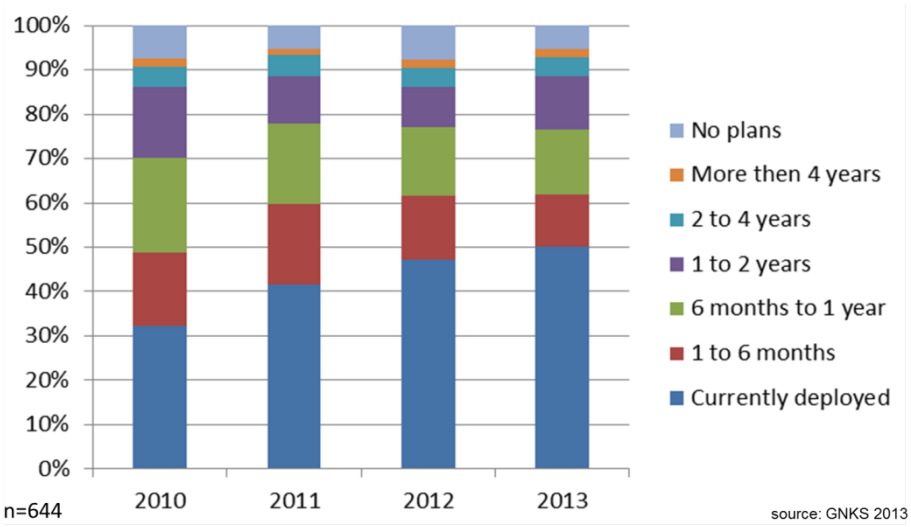

Figure 37 - IPv6 implementation plans for ISPs offering services to business customers

If the aims in 2012 would have been resulting in uptake, about 70% of all respondents should have introduced IPv6 by now. Instead, there was only 3% increase in "currently deployed".

Conclusion

Overall, it is clear that preparedness for IPv6 deployment continues to increase. More customers of ISPs use some IPv6, and with those that use IPv6 there is a slight increase in usage. However, overall usage is still insignificant as compared to IPv4 usage, as the numbers of the Amsterdam Internet Exchange still indicate that less than 1% of all traffic is IPv6.

Remarkable is that the introduction of Carrier Grade NAT is generally not used as a solution to replace IPv6. 70% of those that use or plan to introduce NAT intend to do so along with IPv6 (not instead).

Overall conclusion and recommendation:

- While a small minority is still banking on their stock of IPv4 addresses for the years to come, most recognize the importance of transitioning to IPv6. IPv6 is now more commonly used, and more users do so more frequently. However, the general levels of IPv6 traffic remain still low for now.
- As many are ready with initial preparations and are now waiting for a large scale IPv6 deployment and implementation, large scale deployment pilots would be a prudent way forward.

The 2013 Global IPv6 Survey was carried out by GNKS Consult BV. The survey was set up in 2009 with sponsorship of the European Commission, and in close collaboration with and with support from the NRO (Numbers Resource Organisation, see www.nro.net). In 2013, the survey was sponsored by the European Commission as part of the European IPv6 Observatory project, and again supported by the NRO. Full results are available from http://www.nro.net/ipv6.

3.11 IPv4 Exhaustion and IPv6 Development in APNIC region (Impacts, Statistics and Observation)

3.11.1 Introduction

In 1992 an IETF survey of IP address space exhaustion[38] sounded the alarm that our Internet faced growth-related problems, because the original IPv4 protocol with 4.3 billion addresses cannot provide enough address space for growing Internet which is now extended into everyone's home and handset. From then on, the topic of IP depletion problem never stopped and continued until Today. During the discussion, the successor of IP version 4, IP version 6 (IPv6) is coined with much larger address space in 1995. Still now everyone will safely say that the IPv6 will definitely replace IPv4 soon or later. But the real question is how soon or late the replacement will happen?

Although no one knows when IPv4 will be replaced by IPv6 in the future, we do know IPv4 address pool was exhausted in IANA level since IANA officially announced that all /8 blocks were exhausted on Feb 4th, 2011 and from then on, in most RIRs only final /8 is left and distributed via special policy. Shortage of IP address deeply affect the Internet ecosystem in many aspects. Technically the internet will be patched with lots of mid-boxes to sharing IP address or do translations which may ultimately affect the technology path of Internet and limit the Internet innovations space for our children. Commercially IPv4 exhaustion will bring cost and financial burden to economies for adding special IPv4 workarounds equipment, operation complexity as well as purchasing IPv4 address.

From that very time point, we are delighted observed that the global deployment was accelerated obviously, especially with the effort made by IETF, IPv6 forum, ISOC, RIRS, ICANN and other Internet organizations. Because not only ISPs participate in this campaign but also vendors, ICPs and Internet users make fully awareness of IPv6 as well. Many ISPs, ICPs and enterprises worldwide are planning to support dual stack in their own networks and services. According to Google's IPv6 statistics, more than 2.7% of all traffic to Google is now over IPv6 which is doubling from past year[39]. And IPv6 traffic on Verizon Wireless' network has now climbed to 40.00%[40]. Although significant growth of IPv6 traffic is observed in some pioneer companies and regions, the low IPv6 penetration worldwide indicates that IPv6 is far from fully launched. The transition to IPv6 still needs concerted effort listed as a top priority globally in the recent Montevideo Statement[41] on Oct 7th, 2013, by the leaders of Internet organizations.

There are various reasons provided by experts why transition to IPv6 is so difficult. The most commonly convincing one is because the IPv6 protocol is designed without downward-compatibility for IPv4 technically. When it comes to the difficulty of IPv6 transition, it is usually referred as to replacing the jet engines of an airplane while the plane is in flight. However, a part from on airplane. Internet is the network of networks with multi players such as ISP, ICP,

[38] P. Gross，P. Almquist, IESG Deliberations on Routing and Addressing, IETF RFC1380, November 1992
[39] Google IPv6 statistics: http://www.google.com/intl/en /ipv6/statistics.html
[40] Measurements in IPv6 Launch: http://www.worldipv6launch.org/measurements/
[41] Montevideo Statement on the Future of Internet Cooperation: http://www.icann.org/en/news/ an-nouncements/ announcement-07oct13-en.htm

IDC, end-user etc. In author's humble opinion, different from the telegram and telephone network, the multi-stockholders structure of Internet is an important model not only in the field of Internet governance but deeply affects the IPv6 deployment as well.

For a giant ecosystem, on another hand, the Internet is composed by different regions and countries with various economies and policies as well, which is also a key factor in IPv6 development. There are more than two billion Internet users around the world. Nearly half of the world's Internet users are in the Asia Pacific, which is the fastest growing region of Internet users as well as its economy. As one of the five Regional Internet Registries (RIRs), APNIC formally announced that Asia – Pacific is the first region on the world coming into the periods of lacking IPv4 (15th, April, 2011). As a typical part of global Internet, it is worthwhile to review the status of this area, the impact of IPv4 exhaustion, IPv6 development update, obstacles, typical story and some observations. Most of statistics are from results of the APNIC IPv6 Labs[42] collection.

3.11.2 IPv4 Exhaustion and Its Impact

This section introduces the situation of IPv4 exhaustion in APNIC area, the policy and impact on both commercial and technical aspects.

3.11.2.1 IPv4 Exhaustion Status

We all know that both IPv4 and IPv6 address are generally assigned in a hierarchical manner. Users are assigned IP addresses by Internet service providers (ISPs). ISPs obtain allocations of IP addresses from a local Internet registry (LIR) or National Internet Registry (NIR), or from their appropriate Regional Internet Registry (RIR). The highest level is IANA who is in charge of management and allocation of IP address to RIRs. So when it comes to IPv4 exhaustion, it does not mean there is no free IP address to keep the Internet running and growing. The context of exhaustion of IPv4 address falls into several levels according to the hierarchy of IP address allocation.

In the top level IP address is usually allocated in term of /8s when IP address is abundant. On 3rd February 2011 IANA announced it allocated its last 5 /8 blocks of IPv4 address which claimed IPv4 exhaustion in IANA level. Afterwards in succession, APNIC and RIPE NCC exhausted their free /8 address blocks respectively in 19th Apr 2011 and 14th Sep 2012. The figure 1 indicated the remaining IPv4 address in each RIRs. In APNIC particularly, there are only 81.9% of final /8 address (16,777,216 addresses) left in APNIC currently. In addition there is only little free /8 address blocks left in LACNIC, ARIN and AFRINIC which will soon run out their /8 blocks.

[42] APNIC lab: http://labs.apnic.net/index.shtml

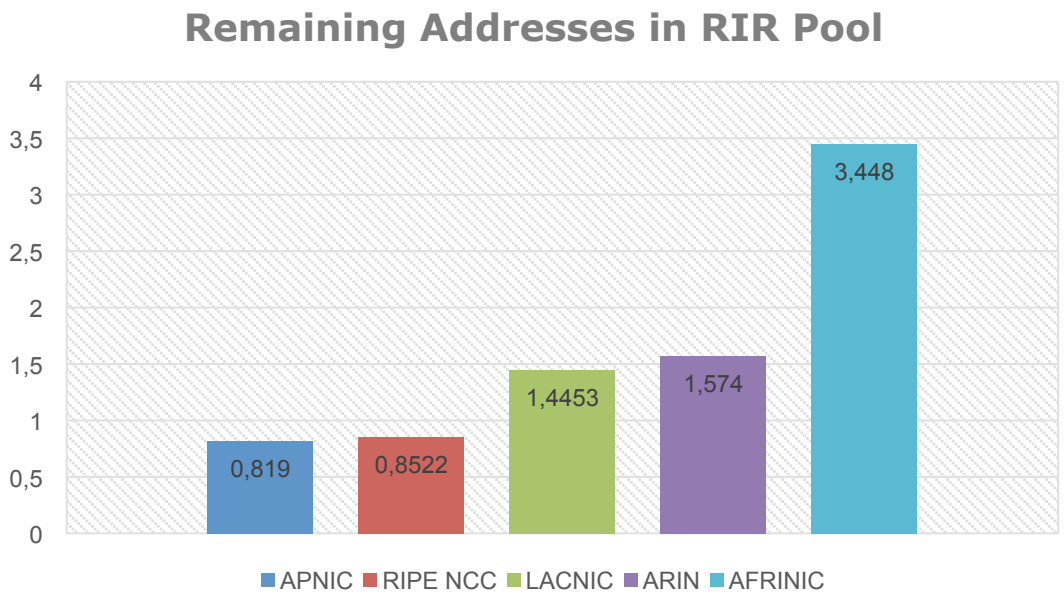

Figure 38 – Remaining addresses in RIR pool (5/12/2013)

To avoid IPv4 address pool exhausted completely in a short time, APNIC created a policy for the special distribution of APNIC's final /8 worth of addresses[43]. The policy aims to ensure that new and emerging networks can continue to receive a small amount of IPv4 for many years to come so they can connect to both IPv4 and IPv6 networks during the transition to IPv6. Under this policy, Asia Pacific organizations can each request one, and only one, small slice (a /22, or 1024 addresses) of the final /8.

It's no doubt that IPv4 scarcity is urgent problem globally especially for the economies in the Asia – Pacific region. Most people may believe that the situation will be relieved by the rise of IPv6 or dual stack. However, running both protocols in parallel does not actually reduce the demand of IPv4 numbers. Rather, it needs both IPv4 and IPv6 address until such times as a tipping point is reached, when the IPv6 traffic is overwhelming over the IPv4 so that services providers can turn off IPv4 safely. And only then, will IPv4 scarcity cease to be a problem.

The IPv4 exhaustion or scarcity problem discuss for more than 20 years and its profound influences are emerging in recent 5 years from author's observer. The lack of IPv4 address will affect network planning for economies. ISP who needs IP address to develop network and deploy new services has to turn to IPv4 workarounds like NAT and CGN which will introduce the additional CAPEX/OPEX. Content providers and specially the mobile Internet apps are affected in that their advertisements and LBS services needs the information of real IP address. In addition the operation and software development complexity will increased in dual-stack and other more complicated IPv4 and IPv6 coexistent network. Finally all cost will be accounted on the users who will pay the bill of Internet access.

[43] Use of final /8 address : http://www.apnic.net/__data/assets/text_file/0011/12422/prop-062-v002.txt

Although there are various analysis of negative effects accompanied with IPv4 exhaustion, in this report author hope to focus on two phenomenon: One is the IPv4 address transfer markets and another is IPv4 workarounds, which may inspire our thinking on the IPv6 development.

3.11.2.2 Address transfer markets

Please see 4.1.4.

3.11.2.3 IPv4 Workarounds and IPv6 Transition

Different from a marketing point of view, there are mainly two technical choices when the engineers of Internet community countering IPv4 exhaustion. One is the short term solution by prolonging the life-span of IPv4 with workarounds. For example, the Network Address Translation (NAT) is the typical example of IPv4 workarounds which is widely used when the global IPv4 address pool depletes rapidly. Shown in the option 2 of figure 2, a home gateway (CE devices) usually has a function sharing a unique IP with multiple users at the same time. It is pretty common to use the NAT function when people dial up using a cable at home or using WLAN in their office.

Another technical choice is IPv6 transition technology[44,45] to deploy IPv6 gradually with continuity of existing Internet services, Like DS-Lite, NAT64, 6rd etc. It's commonly believed that if we update our network and Internet services in to IPv6 step by step, the users and traffic will be contacted to IPv6 increasingly, then finally to the complete of transition of IPv6.

[44] Impact of Carrier-Grade NAT: http://tools.ietf.org/html/rfc7021
[45] Discussion on IETF : http://www.ietf.org/mail-archive/web/ietf/current/msg84102.html

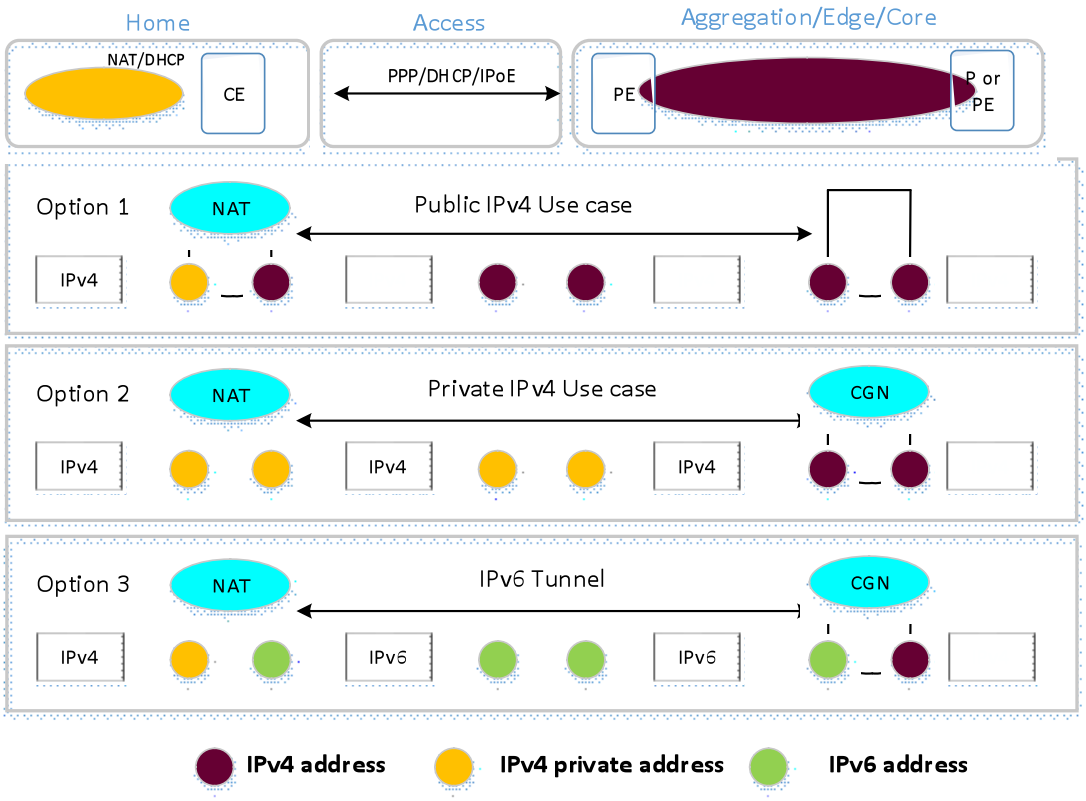

Figure 39 - NAT, CGN and IPv6

The different technical paths reflect different strategies in IPv6 deployment. The supporters of former reflects the real concern from certain group of economies entities who emphasize that there is no market needs and incentive of largely deploy IPv6. The advocates of the latter possess the believing that IPv6 is the optimal and final solution of all the problems cause by IPv4 exhaustion. The more quickly to deploy and use IPv6, the less cost will be involved avoiding the "second-upgrading" of the network.

It worth to mention here that though Carrier Grade NAT (CGN)[46] is usually presented as "IPv6 Transition Technologies" to help IPv4 exhaustion problem, in fact CGN which provides IPv4-to-IPv4 connectivity on double-NATs platforms (i.e. NAT444) are NOT transition mechanisms to IPv6. The option 2 in figure 2 is the case of CGN in which the IPv4 address sharing function is located in the high level in the network of ISP, for example the Broadband Remote Access Server (BRAS). They are still IPv4 workarounds if not involving any IPv6 deployment and dual-stack consideration.

Some times IPv4 workarounds and IPv6 transition technologies are not so separated as two distinct approaches. There are also some mechanism try to combine the two technical paths by using IPv6 tunnel (Softwire) and double-NAT together to achieve IPv4-to-IPv4 connection, such as DS-lite, Lw4over6, which are shown in the options 3 of Figure 39.

[46] D. Wing and A. Yourtchenko. Happy Eyeballs: Success with Dual-Stack Hosts. IETF RFC6555, April 2012

Technical speaking, NAT break end-to-end model of Internet which may cause serious security problem and malfunctions of some Non-NAT friendly applications. It also brings complexity of network development and management. The double-NAT CGN make this situation even worse which in addition require ISPs to afford the cost of high-performance CGN devices perform traffic aggregation, recording the state of each flow, translation, fragmentation and encapsulation/decapsulation if necessary with IPv6 tunnel. The readers who are interested in the analysis of CGN and its technical impact can turn to some article and references list in the website of APNIC[47]].

Another point observed by the author is that the communication of Internet is changed gradually because of widely users of NAT as well as the raise of NAT-friendly technology. Due to the drawback of NAT, some technologies were coined cooperating with NAT schemes, such as STUN/TURN and PCP. Multiple content severs can also share IP address by virtualization and form of server sharing technology. In addition the Web is also a NAT-friendly application which is booming increasing. Actually, the web with C/S mode become the universal services platform in today's Internet which requires only 80/443/53 port. The ability of end to end communication is given up and the innovation space of internet is limited as well.

As to IPv6 transition technology, it do provide solutions to help ISP, ICP and other operators deploy ipv6 gradually in their network, however, it is not a successful “panacea” for transition to IPv6, or say, not a smooth path at least. The history of transition study and specification can traced to as early as 1994 when the Next Generation Transition (ngtrans) WG was setup in IETF even before the IPv6 specification was fully done. Many famous IPv6 transition protocol were proposed and standardized in this work group at very early time, such as NAT-PT, SIIT, ISATAP and IPv6 Tunnel Broker.

Due to the IPv4 exhaustion at IANA and RIRs’ level, the discussion of IPv6 transition technology is warming in the past 5 years, dozens of transition technologies patching the Internet make the IPv4/IPv6 coexistent situation more complicated and costly. According to a rough counting shown in Figure 40, there are currently 14 proposals for IETF standardization in just one tunneling scenario.

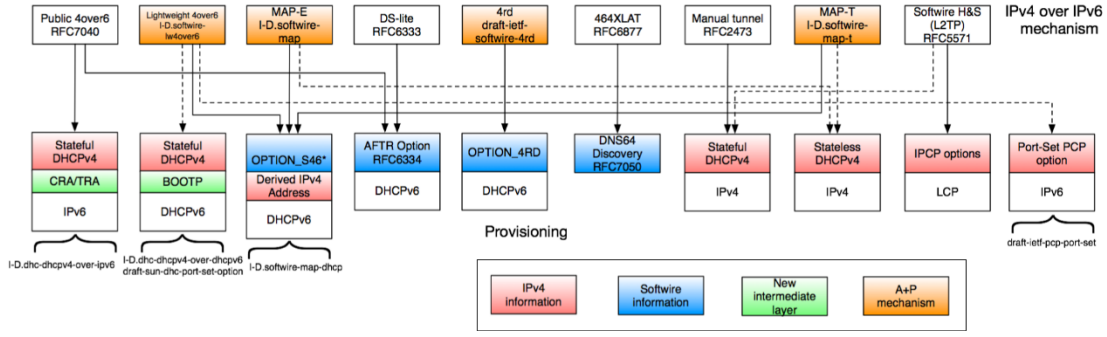

Figure 40 - IPv6 transition specification for IPv4 over IPv6

[47] APNIC IPv6 address policy : http://www.apnic.net/policy/ipv6-address-policy

So far, the straightforward dual stack is viewed as the pragmatic approach for business continuity and future growth. It is the most desirable IPv6 implementation that avoids the complexities and pitfalls of tunneling and translation, such as security, increased latency, management overhead, etc. Actually, in most cases the IPv4/IPv6 dual-stack deployment in the access network is to deploy and run NAT/CGN and IPv6 at the same time in which private IPv4 address instead of global IPv4 address is utilized in the dual stack network.

As the author mentioned, the dual stack does not alleviate the problem of IPv4 exhaustion. Moreover in some mechanisms comparing the quality of IPv4/IPv6 connection like happy eyeballs in which the dual stack approach trigger the competition of IPv4 and IPv6 at users' side which may be not in favor of IPv6 deployment in the early stage. But dual stack is still the most optimal way to deploy IPv6 support and connectivity for new subscribers directly.

3.11.3 IPv6 development in APNIC Region

The Internet is network of networks, which consists of multi stockholders including transit providers, Internet Service Providers (ISPs), access providers, content providers, content delivery networks, application providers, enterprise, governments, civil societies, and end users. IPv6 deployment affects all stakeholders, and is crucial to the continued growth and stability for the Internet, but the timing and level of IPv6 deployment will vary for each stakeholder. Therefore, when we talk about the trends and density of IPv6 deployment among these different stakeholders, for a holistic view, we should adopt a logical approach while considering related statistics.

It will be useful to divide these stockholders into categories and view the trends and density of IPv6 development in each category. 1) IPv6 address allocation by Regional Internet Registries (APNIC). 2) IPv6 adoption level in the core networks (Internet transit providers) of the Internet and Asia-Pacific countries. 3) Enterprise to enable their products and website with IPv6 in AP region. 4) Access networks that allow end users to access to IPv6 resources.

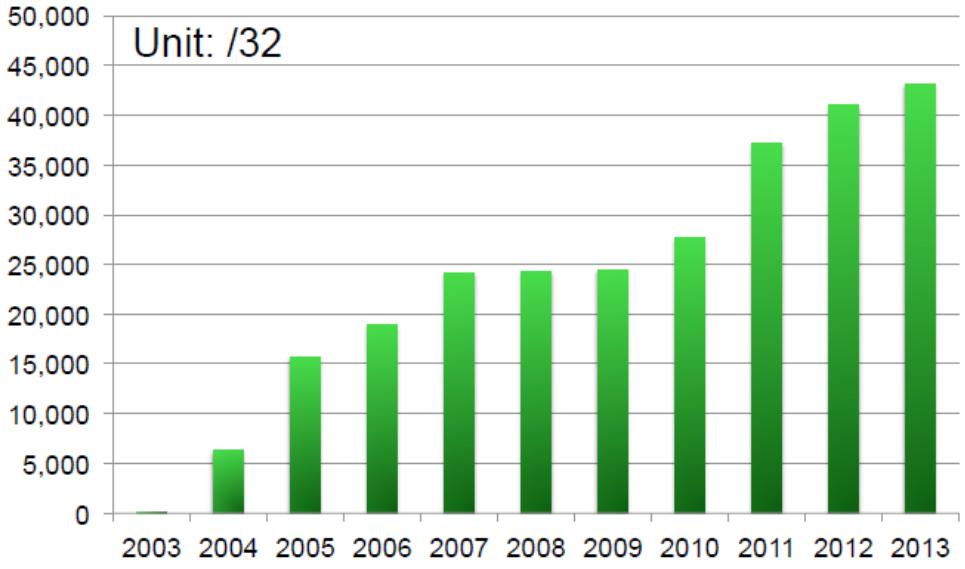

Figure 41 - IPv6 addresses allocation (cumulative), APNIC

3.11.3.1 Regional Internet Registry IPv6 address delegation

IPv6 addresses are distributed by Regional Internet Registries (RIRs) like APNIC to transit providers. In order to deploy IPv6 networks, network operators must first obtain IPv6 addresses from RIRs. Figure 3 shows cumulative IPv6 address allocations (in units of /32) over time, which are made by APNIC to its Members in the region (source: APNIC statistics). According to the IPv6 address allocation and assignment policy in APNIC, who want to apply for more IPv6 address blocks should show their plan of IPv6 deployment and assignment in next 2 years. From that point of view, the allocation of RIR at least reflect the requirement and the trends of IPv6 development in this region.

It is obvious that IPv6 address allocation increased about 35% year-on-year in 2010 to 2011 compared to the previous year with a 10% increase during 2009 – 2010, and it has maintained steady growth until now. It appears that organizations in the APNIC region that need IP addresses for business continuity took action, especially after IPv4 address exhaustion began in April 2011. IPv6 address allocation is growing steadily. APNIC will continue to encourage our community members who do not yet have IPv6 addresses to take action.

In the AP region where APNIC serves, there are 38 Countries & Regions. As there are different economies and policies environment, the IPv6 address distribution of each country in AP region differs widely. The charter (a) in Figure 42 shows the IPv6 distribution among APNIC sub-regions in which the Eastern Asia account for majority part of IPv6 address distributions. Particular, in charter (b), with active economy and Internet of this region, China, Japan and Korea consume the most of the IPv6 address currently distributed in Eastern Asia.

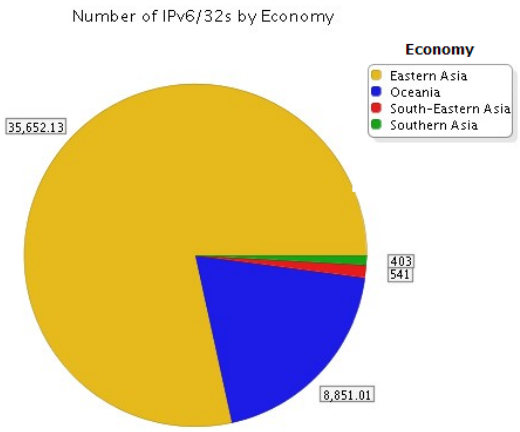

Figure 42 - APNIC sub-regions

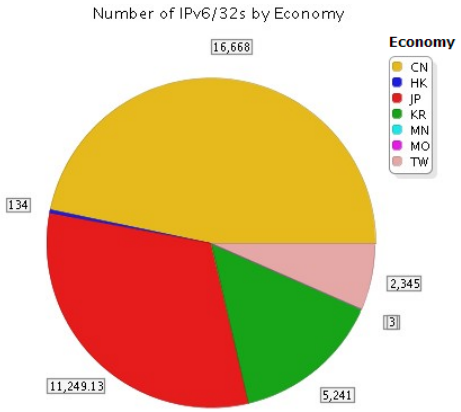

Figure 43 - Eastern Asia

3.11.3.2 IPv6 deployment among network operators

The next logical aspect to review to understand IPv6 deployment is network operators including transit providers. The chart in Figure 44 shows IPv6 prefixes announced into the Global Border Gateway Protocol (BGP) Table (Source: http://bgp.potaroo.net/stats/nro/v6/). It is important to

note that the Global BGP Table size only provides one aspect of IPv6 network growth and it is not a complete indicator of the actual growth of commercial IPv6 networks, as experimental networks can also announce IPv6 prefixes.

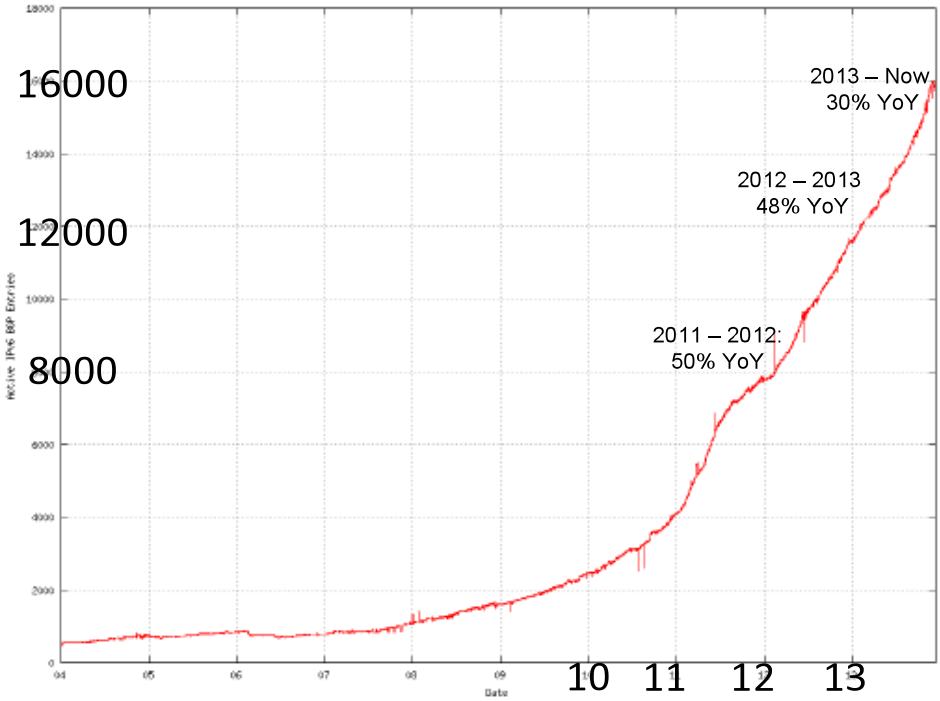

Figure 44 - IPv6 BGP table size

Although this chart is not for the APNIC region specifically, but contains a global view, there is a steady trend of increasing IPv6 prefix announcements, which amounts to around a 50% ,48%, 30% year-on-year growth rate respectively from 2011 till now, highest increase of there years in the whole. During this period, there were several major events that might have influenced IPv6 adoption, including IPv4 address exhaustion in April 2011 in the APNIC region, and two World IPv6 events – one in 2011 and the other in 2012. Such growth trends continue to be encouraging signs of increasing IPv6 deployment among transit providers, ISPs, and some content providers.

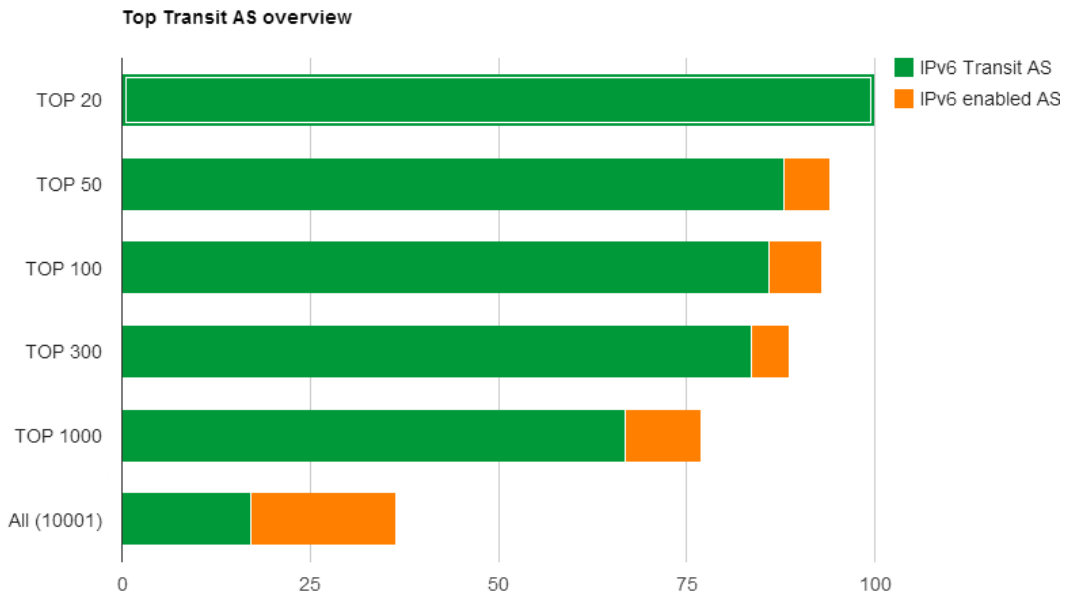

Figure 45 - IPv6 adoption in Internet core networks

The Internet is consisted of many different kinds of ISPs (AS) which are connected hierarchically by BGP protocol in Peering or Transit way. On the top (core) of such hierarchy, there are around 20 core transit providers like NTT communication and A&T and who is called Tier 1 ISPs in the world. 100 percent of them are ready for IPv6. When it go far away from top to local regional areas transit provides and stub AS, IPv6 readiness become smaller. So the enhancement of IPv6 deployment in next step will be the regional transit and stub AS.

More detailed information of IPv6 readiness of each country can be found in http://6lab.cisco.com/stats/index.php. Here is a part of IPv6 readiness of transit AS in APNIC countries which is shown in Table 3.

Country Name	IPv6 transit AS	IPv6 enabled transit AS
Japan	76.75%	90.18%
Singapore	81.96%	93.4%
Indonesia	49.88%	55.75%
South Korea	8.37%	48.88%
Thailand	76.91%	84.6%
India	77.03%	81.39%
Australia	64.14%	76.02%
New Zealand	73.0%	85.62%
Pakistan	57.63%	65.39%
China	19.08%	34.1%

Table 3 - IPv6 readiness of transit AS in APNIC

3.11.3.3 Vendors and Content providers

As the contributor and constructor of Internet, enterprises like vendors and content providers play an import role in IPv6 development globally. One reflection of IPv6 readiness in vendors and network devices is IPv6 forum IPv6 Ready Logo Program which is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and is ready to be used. Many ISPs and customers require their vendors to get IPv6 ready logo to Verify protocol implementation and validate interoperability of IPv6 products. From statistic of IPv6 Ready logo program in IPv6 Forum, up to the May of 2013, more than 1400 types of devices from vendors (including router, switch, printer etc.) got IPv6 ready logo certification. And the number grows steadily since 2003 which is shown in Figure 46.

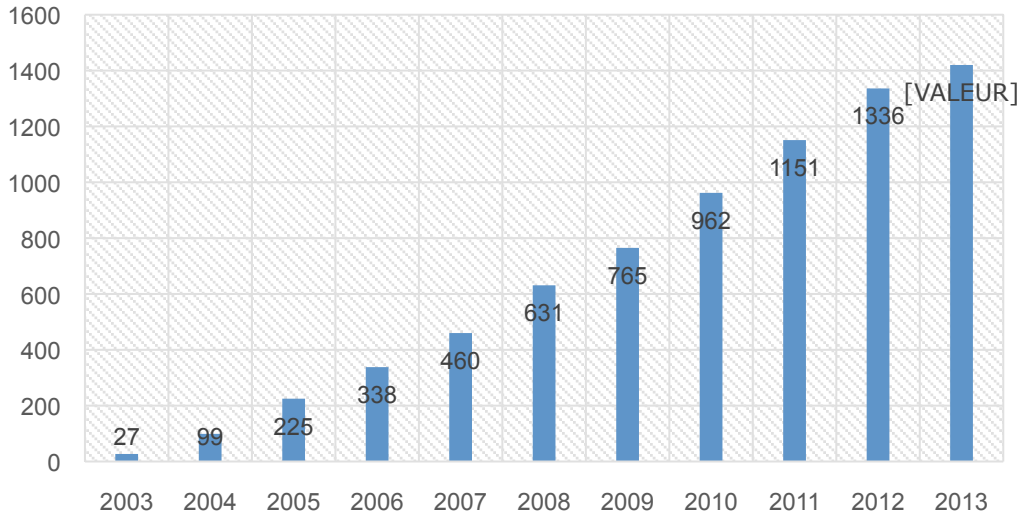

Figure 46 - The growth of IPv6 ready logo certification

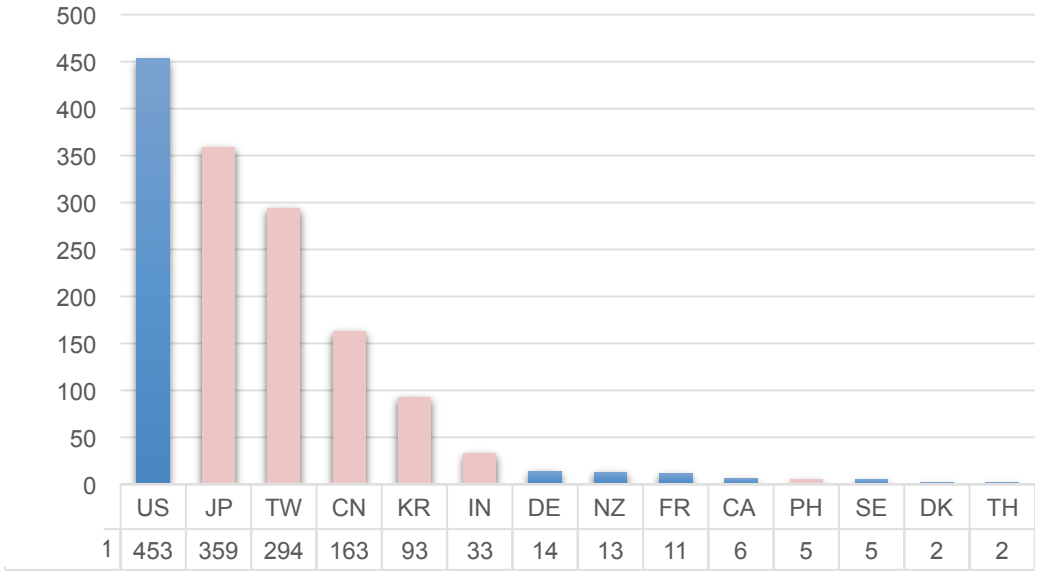

Figure 47 - The distribution of IPv6 Ready Logo certifications by regions

The Figure 47 demonstrates the distribution of IPv6 ready logo certification by countries and regions. Except US, the following 5 countries and regions (JP, TW, CN, KR, IN) are all in APNIC area, which indicates the active IPv6 development of communication manufacturing industry in this area. In another word, the growth of IPv6 certification for communication products reflects the market demand of IPv6 which is the key factor driving the commercial development of IPv6 products.

As an important factor of IPv6 development worldwide, content providers play crucial role in the process. Some ISPs hold a myth that "No content is available on IPv6, therefore there is no point in deploying IPv6 in access networks". But after IPv6 Launch more and more website now supporting IPv6. These sites include Google, Facebook, YouTube, and Yahoo! Table 4 shows the top 10 websites in Alexa list and their status in which most of them are IPv6 enabled including 3 websites (in gray line) in China from APNIC area. While this is encouraging, major local content providers also need to increase their efforts in adopting IPv6.

Website	IPv6 Enabled	Note
www.google.com	Yes	/
www.facebook.com	Yes	/
www.youtube.com	Yes	/
www.yahoo.com	Yes	/
www.baidu.com	Partially	Support in ipv6.baidu.com
www.wikipedia.org	Yes	/
www.qq.com	Yes	/
www.amazon.com	No	/
www.taobao.com	Partially	Support in ipv6.taobao.com
www.live.com	No	/

Table 4 - IPv6 readiness in top 10 websites

There is a rank of IPv6 readiness for website among countries and regions done by Eric Wink sampling top 50 website in each county, through which we can conclude the IPv6 readiness of website in APNIC region.

Country	Rank	The rate of IPv6 website
Singapore	7	20.0%
India	9	16.0%
Indonesia	12	14.0%
China Taiwan	17	12.0%
Malaysia	22	12.0%
Japan	27	10.0%
China HK	28	10.0%
Thailand	29	10.0%

Table 5 - IPv6 readiness in top 10 website (by country)

It's important to note that the IPv6 readiness of content providers in APNIC region is much crucial compared with other aspects. Because most of countries and regions in APNIC region has their own language and local customs. For example in China, local internet content and Internet applications are much preferred than global content providers which are already upgraded to IPv6. So the delay of IPv6 deployment in local Content providers of AP region may finally hind the whole IPv6 transition in this area. In the contrast other countries in RIPE NCC and ARIN region who can share the global IPv6 achievement, such as Google, YouTube, Facebook etc.

3.11.3.4 End user IPv6 readiness

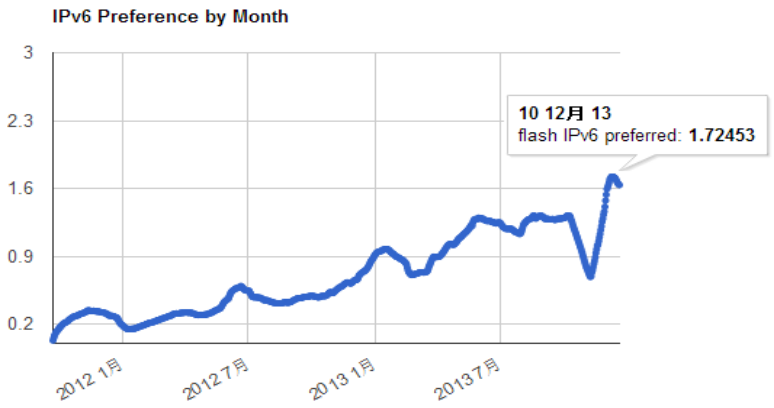

Figure 48 - IPv6 users preference of the world

Although there is no clear definition for the success of IPv6 transition, one obvious goal of IPv6 transition is that most of Internet users are capable and willing to use IPv6. So the IPv6 readiness of end users must be a key element to reflect the both global and regional progress of IPv6 development. There are usually two most referenced monitoring sites of IPv6 users. One is from Google's IPv6 monitoring site where the data is collected from its real traffic. The statistic

page indicates that more than 2.7% Google's users are using IPv6 to get Google's services. Another is from APNIC IPv6 measurement. From the global measurement of IPv6 user preference in figure 8, about 1.7% users are capable and preferred to users IPv6.

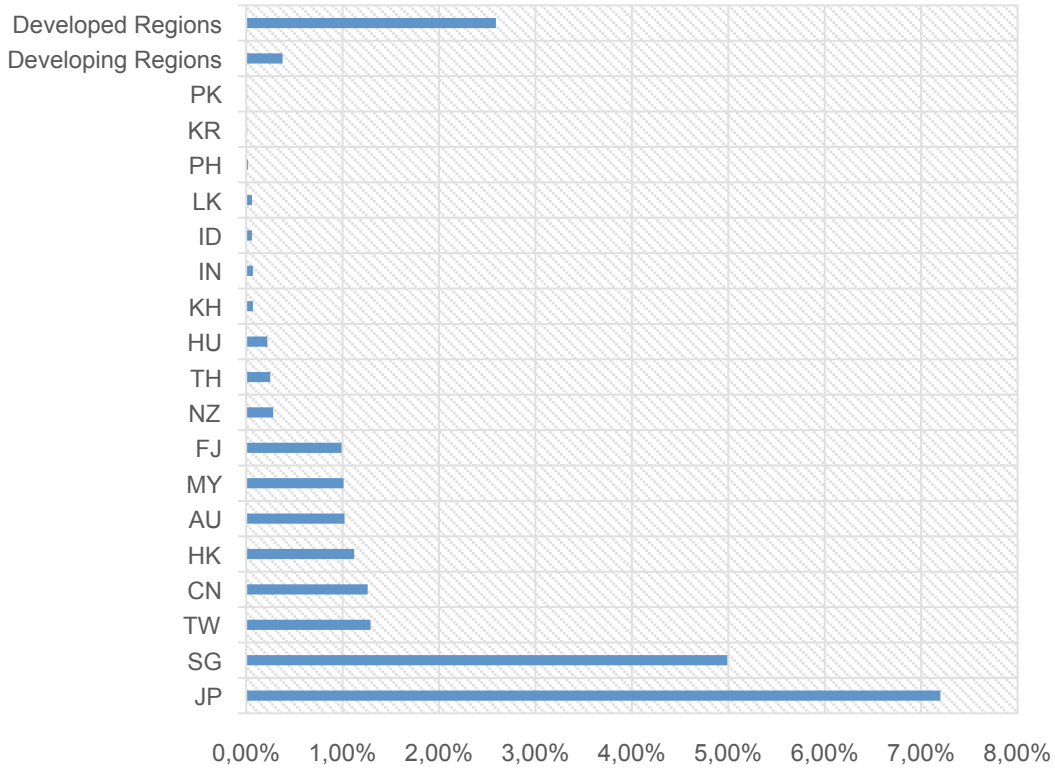

Figure 49 - IPv6 preference by economy in AP regions[48]

More specifically, Figure 49lists the IPv6 preference of economies in AP regions where the index is no less than 0.01%. An intuitive conclusion from the charter is that developed regions like Japan, Singapore, China (TW, HK and mainland), and Australia have more penetration of IPv6 users which is also attributed to their government and IPv6 encouraging policy in those area. It is worthwhile to mention that the development of IPv6 in this region is unevenly in AP area where there are still many economies in which the IPv6 readiness of end-users are under the average worldwide. It's urgent to note that much work is supposed to be done for those developing countries so that they will not loss the chance of IPv6.

3.11.4 Government's role in IPv6 development

The Last part is the government's role in IPv6 development in APNIC region. It is worth to mention that IPv6 awareness among governments' in the AP region is very high. In website (http://www.apnic.net/community/ipv6-program/ipv6-for-governments), there is a list of some useful documents on IPv6 that were issued by various governments and intergovernmental organizations, as well as news articles that explore the latest status of that economy's IPv6 poli-

[48] Source: http://labs.apnic.net/ipv6-measurement/Economies

cies. So the author will not elaborate detailed information of each economy in this report. Some of the common initiatives and actions by the government are concluded as follows:

- Developing national policies and guidelines and roadmaps to enable IPv6
- Enabling IPv6 in government networks and website, E-government for example
- Mandating for IPv6 readiness in government and ISPs' procurement for ICT goods and services for example IPv6 ready logo certification.
- Raising IPv6 awareness among key people in the government and industry
- Providing IPv6 training and education in industry and university
- Monitoring IPv6 deployment measurement and share information with industry
- Setup IPv6 conference or other national platform to share best practice worldwide
- There is a typical case study in China. We can see how Chinese government play an active role in enhancing the IPv6 development:

Due to the exhaustion of IPv4 address pool around the world, China had accelerated its IPv6 commercial deployment since 2011. Serial policies were issued by the government to promote IPv6 adoption and co-operations were enhanced between domestic institutes and international organizations such as IPv6 forum, ETSI, BBF, IETF and foreign ISPs.

For a long time, the IPv6 network constructions in China were mainly focused on education and research field. CERNET2 is built as the largest pure IPv6 network connecting more than 100 campus with over 100 thousand college students and researchers. From the end of 2011, China government issued several policies encouraging the transformation of IPv6 achievements from CERNET2 to commercial network and website in order to promote the IPv6 civil use and broader innovation. In addition, several big national projects, such as TD-LTE, IoT, Cloud Computing and Broadband China, had taken IPv6 support as a key factor in their goal.

At the beginning of 2012, Leaded by NDRC (National Development and Reform Commission) 7 departments were united to issue a document to guide and advice the development of Next Generation of Internet in China. This document identifies the roadmap and timeline of China IPv6 development: by the end of 2013, 8 million broadband users can use IPv6, while during 2014 and 2015 this number should reach 25 million. Besides the network infrastructure and IPv6 users, obviously influenced by International IPv6 Launch activity this documents paid noticeable attention on IPv6 support of Internet application and end system. More than 500 million Yuan special funding will be used to help commercial and government's website. The newly deployed Internet services, handsets and CPEs should support IPv6 as well.

As the main driving force of China IPv6 development, CNGI project has over 2 billion Yuan funding each year to promote IPv6 research and development. Recently most funding was put on IPv6 update of ISP network including Backbone, metropolitan area and access network. In addition, dozens of pilot projects were set up in petroleum, utility, transportation and security industries. These serial investments and actions of CNGI imply that Chinese Government plans to build and leverage several typical application pilot projects of IPv6 to start the huge potential IPv6 markets. In the following 2014, there are several measures taken by CNGI project to ensure effective implementation of government's policies.

- To build demonstrating City of Next Generation Internet in 16 cities like Beijing, Shanghai, Wu Han, Cheng Du, Shen Zhen, etc.
- To build third-party platform to help and test the IPv6 upgrade of network and website;
- To organize China IPv6 day in Jun 6 to demonstrate the result of China IPv6 development;
- To guide International IPv6 promotion activities such as IPv6 summit and IPv4/IPv6 transition InterOp Event.

3.11.5 Conclusion

Since Asia-Pacific was the first region on the world coming into the periods of lacking IPv4, in this report the author revisit the current situation of AP region on the impacts of IPv4 exhaustion and status of IPv6 development. Some status and impacts are general worldwide and some analysis are special for economies in AP region. Most of the data and charters are from the website of lab of APNIC. Some arguments and points are from speeches and discussion with experts of APNIC.

As the Internet is composed by multi stockholders like RIR, ISP, ICP, end users, government etc., each part may react differently facing the pressure of IPv4 exhaustion. The most direct reaction is from RIR, because there is no enough free IPv4 address space to allocate. In APNIC a special address allocation policy was issued for the final /8 block which directly affect the IPv4 address application for the member of APNIC. In APNIC a lab was setup up and dedicated to report the IPv4 address exhaustion, IPv6 measurement study and track the progress of IPv6 transition worldwide.

The economies of AP region like ISP,ICP or large enterprise who desire IPv4 address to development their network can only turn to other economies who have excess IPv4 addresses. In this report, the IPv4 address transfer market is introduced, with a public address trading case, RIRs' policies, an IGF study and different arguments on this issue. The IPv4 address transfer markets are the direct outcome of IPv4 exhaustions which challenges the transitional concept of Internet resource. In the meanwhile it indicate the fact that the Internet resource was distributed unevenly as large blocks of historical IPv4 address ware distributed before the IANA/RIR address allocation system was setup. As more and more attentions were paid on Internet Governance nowadays, the allocation and distribution of Internet resource as well as Internet operation and security must be a hot topic in IPv6 era.

Besides the commercial approach, IPv4 workarounds are preferable for many technical guys in ISPs as a short-term solution to confront IPv4 exhaustion. This report argues that some IPv6 transition technology combine IPv6 tunnel and IPv4 workarounds together which may help ISP's network move to IPv6, but the users and Content are still in IPv4. The author has a concern that The IPv4 workarounds and NAT-friendly technologies may hind the IPv6 importance and transition process. IPv4 workarounds and IPv4 itself will compete with IPv6 in a long term. The Author argues that campaigns and events are needed not only to switch IPv6 on but switch IPv4 off as well in a proper time point.

As to the status of IPv6 development in APNIC, they are divided and introduced in several logical aspects in this report: IPv6 address allocation, IPv6 readiness of network operator, vendors

and content providers and finally the IPv6 end users. From this report, it's encouraging that steady growth is observed in all kinds of indicators. More specifically, large enthusiasm of IPv6 address allocation, network upgrade and venders participation is observed, but the IPv6 readiness of the content providers and end users is still very low. It's worthwhile to note that although the average indicators are low, from the individual level of economies and AS numbers, individual operators, the indicator is quit high which demonstrates the high diversity of IPv6 development among different economies. Finally the report emphasizes the role of each government in AP region and take China as a typical case.

Internet is still developing at very high speed in a splendid way. The future Internet will connect not only people with handset but all things on this planet. In the way, there are still lots of challenges, IPv6 will definitely be the wing of Future Internet.

4 PERSPECTIVES

4.1 CGN as an alternative to IPv6?

The world is faced with the fundamental problem of IPv4 address space exhaustion. There is a huge demand for IP addresses resulting from the explosive growth of mobile devices, including smartphones, tablets, laptops and netbooks etc.

Service providers are looking for ways to extend the use of the IPv4 addresses they have during their transition to IPv6. Since IPv4 addresses are still valid and IPv6 deployment is slow, the two addressing schemes will coexist for a long time. Therefore, it is crucial to find ways to maximize the use of available IPv4 addresses. One tool of conserving IPv4 addresses is Carrier Grade NAT, or simply CGN that is sharing addresses among a large pool of addresses of Internet consumers.

4.1.1 Carrier Grade NAT Overview

Network Address Translation (NAT)[49] is positioned between a private and public IP network and uses non-global, private IP addresses and a public IP address for translation. Traditionally, NAT boxes are deployed in residential home gateways (HGWs) to translate multiple private IP addresses that are configured on multiple devices inside the home to a single public IP address that is configured and provisioned on the HGW by the service provider. Service providers deploy NAT in such a way that multiple subscribers can share a single global IP address. The service provider NAT scales to several millions of NAT translations, making it a Carrier Grade NAT (CGN).

In CGN, subscriber datagram's are modified more than once at the subscriber edge and in the carrier's access network. The IP addresses and port are mapped between external and internal values. Therefore, the subscriber's traffic uses three different source addresses as the traffic goes from the subscriber's internal network, to ISP's access network and to the global IPv4 Internet.

CGN increases the scalability of the number of NAT translations that can be supported because destination information is not stored.

The operation of CGN is show in the figure below:

[49] http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/asr1000/iadnat-cgn.html

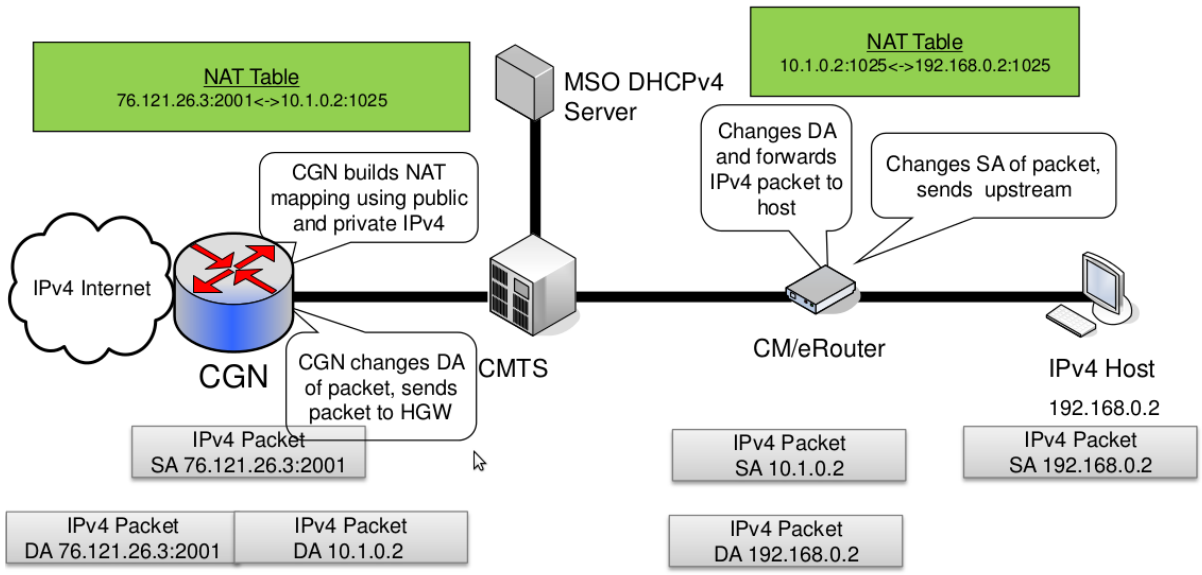

Figure 50 - CGN overview[50]

One of the features of CGN (that is supposed to be transparent to Internet consumers) is actually the source of many of the challenges of deploying CGN. In fact, when a user is simply reading emails or browsing the web, CGN is completely transparent. The complexity comes when Internet consumers use more sophisticated applications and services in terms of number of sessions required and service quality (response time, latency…): CGN becomes source of many problems.

This chapter will address implications of CGN for Internet Consumers categorized depending on the level of the impact: minimal, average or significant. Then the second one will try to approximate CGN total cost and compare it to dual stack and IPv4 buying address costs.

4.1.2 Technical impact of CGN on Internet users

4.1.2.1 Minimal impacts

Some applications usually work behind CGN, but it is interesting to know that any application can fail to work behind CGN or can face reduced performance and intermittent reliability.

Basic Internet services: Basic Internet services are expected to work behind CGN. Indeed, they represent the simplest form of Internet use including emailing, Web sites visiting… These services have common characteristics such as:

- Using few sessions
- Not requiring peer-to-peer functionality
- Using TCP or UDP at transport layer

[50] CGN ARCHITECTURE AND IMPACTS,KARTHIK SUNDARESAN

Usually applications and services that meet these criteria are likely to work in the presence of CGN.

Social networking services

A social networking service is a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services.

Most social network services are web-based and provide means for users to interact over the Internet such as e-mail and instant messaging. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.

- **Facebook**: a good example is Facebook. It is now IPv6 enabled. Therefore, in CGN presence, Facebook would not be impeded but would instead use IPv6.
- **Twitter**: Twitter is not yet available via IPv6. It turns out that Twitter does not have an especially high rate of concurrent session use. CGN presence would not be considered as a significant obstacle for Twitter.

However, Twitter apps on iOS and Android are greater consumers of sessions because they are providing live updates of search results and groups of followers. Behind CGN, Twitter might experience occasional degradation of performance due to latency of messages arrival or exhaustion of session limits.

Single player games

Single-player game usually refers to a game that can only be played by one person. The vast majority of modern console games and arcade games are designed so that they can be played by a single player.

These kinds of games apparently don't require an important number of sessions or robust network resources. Therefore, they will work behind CGN.

Notable examples of single-player games include action-adventure games such as The Legend of Zelda, platform games such as the Mario series, stealth games such as the Metal Gear series, survival horror such as Resident Evil and Silent Hill, and first-person shooter such as Doom ,Half-life.

4.1.2.2 Average impact

Advanced Internet services

Internet is providing modern websites that use advanced techniques such as AJAX (asynchronous JavaScript and Extensible Mark-up Language) to guarantee innovative consumer experience.

Web-browser's used to fetch all the elements of a web page in sequence, using just one session. Today, modern web-browsers usually fetch elements in parallel in order to improve performance and reliability.

This is the case with widely used web-browsers such as Firefox and Internet Explorer.

Some examples of the number of concurrent TCP sessions required by widely used Internet sites are shown in the table below.

Web applications	Number of concurrent sessions
Google Maps	20 to 50
Amazon	90
Youtube	90
iTunes	230 to 270

Figure 51 - Example of number of concurrent sessions per application[51]

Web Mapping Services

The popular application Google Maps is a good example. It typically requires twenty to fifty sessions and ports to function correctly. If it is not the case, it will be not completely able to display a map.

Screenshots[52] shown below illustrate Google Maps under a range of sessions.

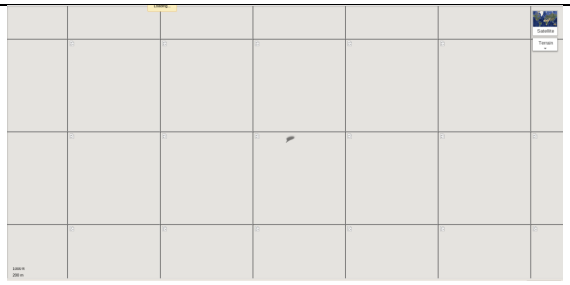

Figure 52 - Google Maps limited to 5 sessions

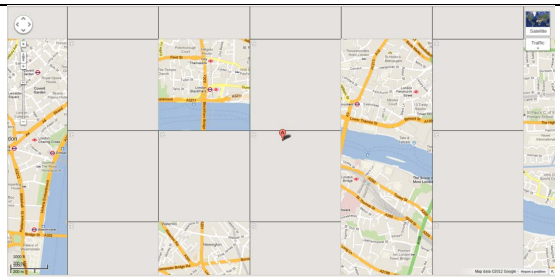

Figure 53 - Google Maps limited to 10 sessions

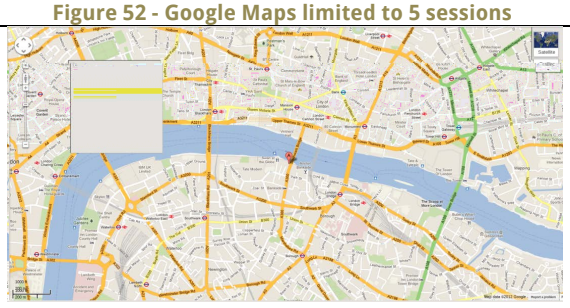

Figure 54 - Google Maps limited to 20 sessions

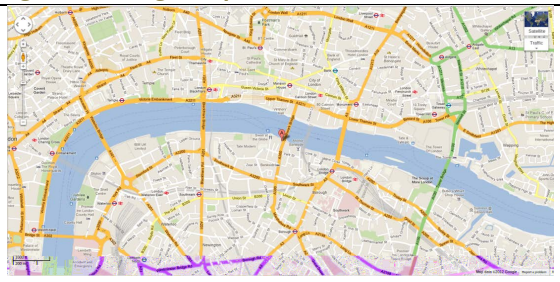

Figure 55 - Google Maps limited to 30 sessions

[51] S. Miyakawa, From IPv4 only to v4/v6 Dual Stack, IETF72 IAB Technical Plenary, Dublin, 27 July – 1 August 2008.
[52] Screenshots are provided by Erion Ltd.

Future Web applications

An application-programming interface (API) specifies how some software component should interact with each other. Here are some interesting examples of APIs :

WebSockets: WebSockets[53] is an advanced technology that makes it possible to open an interactive communication session between the user's browser and a server. With this API, it is possible to send messages to a server and receive event-driven responses without having to poll the server for a reply. Such API could experience significant impact. Indeed, this API requires an important number of sessions to facilitate communication.

ServerSentEvent: HTML5 Server-Sent Events allow a web page to get updates from a server. This was also possible before, but the web page would have to ask if any updates were available. With server-sent events, the updates come automatically. The Server-Sent Events EventSource API is standardized as part of HTML5 by the W3C.CGN impact would be significant in this case. Indeed, the API might face limitations behind of CGN.

WebRTC: WebRTC is an API definition being drafted by the World Wide Web Consortium (W3C) to enable browser-to-browser applications for voice calling, video chat, and P2P file sharing without plugins, via simple Javascript APIs. Here again,CGN might limit this APIs to function since it uses multiple sessions.

VoIP and Instant messaging services

Voice over IP services: VoIP (voice over IP) provides a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network PSTN. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

Skype: Skype allows users to communicate with peers by voice using a microphone, video by using a webcam, and instant messaging over the Internet. Skype has also become popular for its additional features, including file transfer, and videoconferencing. It is worth noting that:

- Skype is normally designed to function behind NAT44. It uses a proprietary from STUN to allow incoming connections into the subscriber's network even though they are located behind NAT.
- CGN presents a challenge for Skype[54]. It uses several ranges of different methods to traverse NAT depending on the location of the Skype clients:
    - Scenario 1: when a user is behind CGN, Skype uses connection reversal where the node behind CGN initiates the connection.
    - Scenario 2: when both users are behind CGN, Skype uses its own proprietary form of NAT traversal which is similar to STUN.

[53] https://developer.mozilla.org/en/docs/WebSockets
[54] J. Rosenberg, R. Mahy, P, Matthews & D. Wing, Session Traversal Utilities for NAT (STUN), RFC 5389, https://tools.ietf.org/html/rfc5389, 2008

    - Scenario 3: If this fail (Scenario1 and 2), Skype relays the media session via a Skype super node. It has performance implications and the service might likely degrade or even fail.
- Skype sessions from a particular user must all use the same IPv4 address for the STUN-like approach. It often breaks the STUN approach in mobile networks where sessions from the same user are not guaranteed to use the same IPv4 address.
- In fixed lines CGN environment, Skype normally works under the STUN-like approach.
- In the case of relaying the media session via Skype super node, there might be significant implications for performance and reliability in terms of latency and limited bandwidth.

Instant Messaging: Instant messaging offers real-time messaging transmission over the Internet. Short messages are typically transmitted bi-directionally between two parties, when each user chooses to complete a thought and select "send".

Chat, presence and control sessions of some Instant messaging users need to come from the same public source address. If not, the server will automatically reject them. It is the case in presence of CGN, as long as this condition is not satisfied and not guaranteed.

Take, the AOL Instant Messenger (AIM) as an example. Authentication and chat starting need two sessions. If the chat session originates from a different source address than the authentication one, the AIM server will immediately reject the chat session.

SIP clients: SIP (Session Initiation Protocol) is a signaling communication protocol, widely used for controlling multimedia communication session such as voice and video calls over Internet Protocol (IP) networks. It requires multiple connections to come from the same address. If, as an example, a SIP client is sending Real-Time transport Protocol (RTP) and Real-time control packets RTCP, each end expects that they come from the same IP address. If it is not the case, the receiving end point simply drops the packet with different address.

Geo-localization: Geo-localization is the process of approximating the location of a subscriber from his IP address. It is widely used by many applications to provide information about consumer's location. Yahoo, as an example, proposes many products using geo-localization. In the presence of CGN, Yahoo might experience significant resolution issue. The percentage of the lost resolution depends on how large is the subscriber's area that is behind CGN. These two figures[55] below illustrate CGN impact on both best and worst case scenarios.

[55] http://meetings.apnic.net/__data/assets/file/0003/38298/fesler_yahoo_2011_post_ipv6_day_20min.pptx.pdf

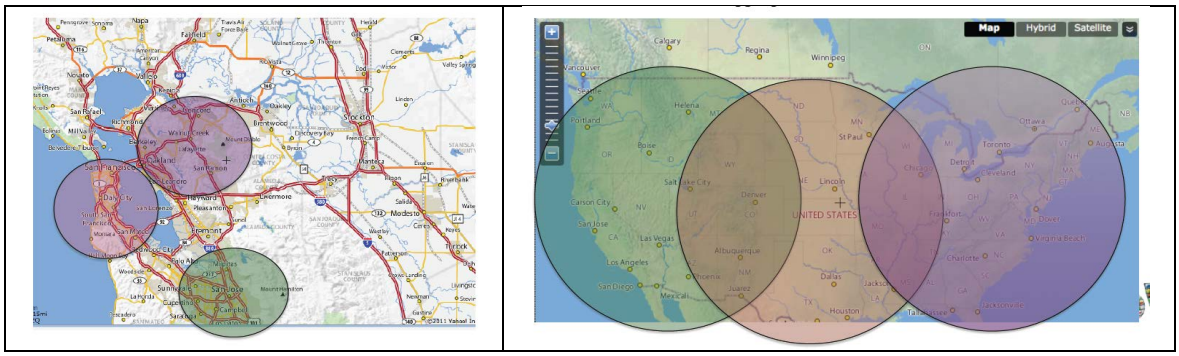

Figure 56 - CGN impacts on Yahoo geo-localization

4.1.2.3 Significant Impact

Medium libraries in the home, PVRs and other home resources:

Nowadays, many applications provide access to home networks from the public Internet resources. It requires that an external client might initiate a connection to a device in a home network. The common point between these applications is the requirement of an authentication external access to devices and the services in the residential network.

Here are some examples of this growing applications class.

- **Webcams or monitoring devices**: The user might access to the images provided by cameras in a residential network in real-time.
- **Personal Video recorders**: it allows the user to have play back recordings of TV programs (for instance).
- **Home security systems**: the user can control and supervise security alarms for instance managed by a home security system.

CGN binding addresses and port numbers is usually made on connections coming from the consumer's network. Since with these applications, it is the opposite way (external connections), it might be difficult for them to work.

Transition mechanisms

IPv6 transition mechanisms facilitate the transitioning of the Internet from its IPv4 infrastructure to the successor addressing IPv6. As their networks are not directly interoperable, these technologies are designed to permit hosts on either network to participate in networking with the opposing network.

CGNs can have a negative impact on these mechanisms when the ISP does not provide a native IPv6 service to their subscribers. Normally, without CGNs, a subscriber could use IPv6 transition

techniques such as 6to4, Teredo and Tunnel Brokers to access the global IPv6 Internet. When CGNs are deployed, they might stop functioning when they hit a CGN interface.

Tunnel brokers, for instance, require a public IPv4 address as an end-point, with CGN, it might not be possible.

P2P gaming: many tests were applied on gamers in different scenarios and here are the results:

In the case of peer-to-peer gaming between two Xbox 360 users in different home networks on the same ISP, the game could not be connected between the two users. Both users shared an outside IP address and tried to connect to the same port, causing a connection failure.

In the case where two users are in the same home network and the scenario is through a single ISP, when the Xbox tries to register with the Xbox server, the server sees that both Xboxes are coming through the same public IP address and directs the devices to connect using their internal IP addresses. So, the connection ultimately gets established directly between both Xboxes via the home gateway, rather than the Xbox server.

In the case where there are two Xbox users on two different home networks using a single ISP and the CGN is configured with only one public IPv4 address, this scenario will not work because the route between the two users cannot be determined.

However, if the CGN is configured with two public NAT IP addresses, this scenario will work because now there is a unique IP address with which to communicate. This is not an ideal solution, however, because it means that there is a one-to-one relationship between IP addresses in the public NAT and the number of Xbox users on each network.

Another problem behind CGN is latency. In peer-to-peer gaming, the user expects the responds to their movement in the game immediately. Therefore, when the delay is important, other players might get annoyed and drop the game.

One of the techniques that have been developed to reduce latency is geo-proximity. It is based on measuring nearness among players in terms of latency. The players paired together are the one who share the lowest latency.

In CGN environment, latency is increased due to the increased topological distances and a combination of CGN device latency. Connections can also break when the traffic goes via an intermediate server. It would introduce performance limitations, latency and limited bandwidth.

4.1.3 Summary of the CGN technical implications

The table below provides a summary of the technical implications of CGN for Internet users.

	IPv4	IPv4 with CGN	IPv6
Basic Internet services	Work	Likely to work behind CGN	Work

Social networking services **(Twitter)**	Work	Twitter ,works because it doesn't have a high rate of concurrent session use Twitter on iOS and Android might face some degradation of performance.	Work
Single players games	Work	Work behind CGN	Work
Advanced Internet services **(Google MAPS)** **HTML5 APIs**	Work	Require a certain number of concurrent session and if this number is reached, it might fail.	Work
VoIP services (Skype)	Work	Work if it uses NAT traversal techniques such as STUN,TURN, and sometimes an intermediate relay	Work
Instant messaging	Work	Some chat sessions might be rejected if the authentication address and the chat session address are different.	Work
Security protocols **(IPsec)**	Work	Might work for one user behind CGN's external address but not for other users.	Work
SIP clients	Work	It requires multiple connections to come from the same address. If it is not the case, the packets might be dropped	Work
Geo-localization	Work	Might experience significant resolution issue,	Work
Medium libraries in the home, PVRs and other home resources	Work	Currently likely to be impossible. In long term future may be possible if there is deployment of PCP and other techniques.	Work
Transition mechanisms	Work	Would not work without special configurations.	Not required
P2P gaming	Work	Connections can break when the traffic goes via an intermediate server. It would introduce performance limitations, latency and limited bandwidth.	Work

Figure 57 – Summary of CGN implications on Internet Users

4.1.4 Costs of CGN

A recent study[56] from Lee Howard[57] (Time Warner Cable) evaluates costs related to CGN, taking OPEX and CAPEX costs into consideration. First conclusions of the report show that CGN costs "$2 million for every 10,000 users it's used for, or $40 per user per year". This conclusion is very interested as it gives the possibility to choose between buying additional IPv4 addresses or setting up a CGN: "From $12-$40 per address, IPv4 addresses look cheaper than CGN and above $40, CGN is cheaper than each address".

[56] http://www.asgard.org/images/pricing_v1.3.docx
[57] http://rmv6tf.org/wp-content/uploads/2012/11/TCO-of-CGN1.pdf

As written in the Lee Howard's report:

Thus, until addresses reach $40 per IPv4 address, there is no reason to deploy CGN. At that point, market price increases will slow, as CGN provides an alternative. If fragmentation of address space drives operators to filter routes based on prefix length, affected address space will be less desirable. Once addresses exceed $70 per address, ISPs will give native IPv4 to fewer users; most new users will have IPv6-only, or maybe IPv6+CGN. Beyond that point, the value of addresses will stabilize or decline generally, as ISPs can realistically convert more users to IPv6-only service (or possibly IPv6 plus CGN) than their net new subscribers.

Lee Howard also mentions two options to avoid the limitations likely to happen with some applications as described above.

- The first one implies to run deep packet inspection (DPI) on customers links to identify the one in need of publicly routable addresses and the one that could make use of CGN with degradation of their services. This method is nevertheless costly and would raise issues related to the protection of private data.
- The second option is to price differently the accesses depending on either it is based on IPv4 public address or CGN. The difference in cost could be up to $70 yearly under a cost recovery principle. This would potentially create an additional digital divide.

In conclusion, the paper indicate that CGN can only be a limited option to overcome the public IPv4 addresses depletion which is expected to be used as a short term patch, to cover the period during which IPv6 services are not largely deployed, and thus require an IPv4 link to access them.

4.2 IPv4 addresses trading (e.g. IPv4 addresses market transfer)

Just one month after IANA's announcement of IPv4 exhaustion, a publicly disclosed sale of an IP address block was released which drawn much attentions and discussion widely. That is Microsoft offered to pay bankrupt Nortel $7.5 million for 666,624 legacy IPv4 addresses, $11.25 per address which is more than the going rate for to register a .com domain name at that time.

It's commonly believed that due to the extreme IPv4 scarcity, the black market of IPv4 address transfer was formed for years before the case between Microsoft and Nortel. Some experts show their warning and concern on this, because the address space is not to be considered to be property in the Internet community as a whole[58]. The distribution of IP addresses in RIRs in a somewhat socialist manner: "to each according to his needs". The applicant should show its real need and address plan to RIRs to apply a new block of address. In another word, the address is to be used not to be possessed. However, this kind of ideal socialism in Internet Governance is challenged due to a simple pure technical restrain of IP address.

[58] ARAN number resource policy manual :https://www.arin.net/policy/nrpm.html#six41

In the level of Regional Internet Registry, it's a little tricky to respond to this question: whether to keep the market black or white in RIR's level, given the fact that the market of address space is already driven by the demand of IPv4 address. If black, it will have bad impact on the ability to maintain accurate databases, such as *whois* and other LBS services. If white, RIRs should issues related policies regarding both fairness and efficiency, particularly with respect to the developing economies in this region.

Actually policies and proposals regarding IPv4 transfers in RIRs do exist. Normally the operating procedure is for the former to return addresses to the RIR governing their region, and for the latter to obtain addresses from that RIR. Table 6 summarizes the situation and links to the relevant policy documents and proposals governing IPv4 market transfers. From a study done by IGF[59], the quantity of IPv4 numbers traded exploded from only about 10,000 in 2010 to about 5 million in the first six months of 2012. The overall value of the IPv4 market, now estimated to be about $60 million in 2011 and 2012 based on an assumption of $10 per address, could increase to half a billion or even a billion US dollars if current rates of growth are extrapolated into the future.

Looking carefully into the policy changes in APNIC, the transfer policy of 2010 firstly limit the eligibility of IPv4 transfers to those who are between APNIC account holders and relating to mergers and acquisitions which can be referred as to "non-market" transfer. In the current version released in 18 February 2013, there is no such limitations and supporting Inter-RIR IPv4 transfer especially with ARIN. The policy changes in APNIC at least reflect three aspects:

RIR	Transfer policy and proposal	Data passed	Inter-RIR transfer
RIPE NCC	• http://www.ripe.net/ripe/docs/ripe-553#---transfers-of-allocations • https://www.ripe.net/ripe/policies/proposals/2012-02	12/2008	Under discussion
ARIN	https://www.arin.net/policy/nrpm.html#eight	6/2009	Yes
APNIC	• 2010 version: http://www.apnic.net/policy/proposals/prop-050 • 2013 version: http://www.apnic.net/policy/transfer-policy	2/2010	Yes
LACNIC	• http://lacnic.net/en/politicas/manual3.html • http://lacnic.net/documentos/politicas/lac-2012-08-ENv2.pdf	8/2012	Under discussion
AFRINIC	Only LR level transfer permitted: https://my.afrinic.net/help/policies/afpol-v4200407-000.htm	Not yet	Not yet

Table 6 - RIR market transfer policy

1) The IPv4 transfer market cannot be ignored due to the severe lack of IPv4. The information accuracy of address distribution in RIR has higher priority than the traditional preconception of

[59] Peng Wu, Yong Cui, Jianping Wu, Jiangchuan Liu, Chris Metz. Transition from IPv4 to IPv6: A State-of-the-Art Survey. Accepted by IEEE Communications Surveys and Tutorials, 2012

Internet address and their value. It requires RIR to record each transaction even they are profitable trading.

2) APNIC and ARIN are the only RIRs who support Inter-RIR transfer. On one hand, it is still controversial for Internet resource trading especially in developing area. On another hand, it makes high utilization IP address in that excess addresses in ARIN area can be transferred to APNIC economies in great need.

3) Since policy of IP transfer require that he minimum transfer size is a /24, the frequent transfer will impair the aggregation capability in the address space which finally deteriorate the routing table explosion problem mentioned in RFC1380, given the current active BGP entries reaches 500,000[60].

Around IPv4 transfer market there is another question: whether will IPv4 transfer market hinder or at least prolong the transition to IPv6? It is not easy to say absolute yes or not. In positive thinking, it will accelerate IPv6 deployment due to the unpredictable cost of IPv4 transfer and its delay of each transaction which may generate alternative choice for own of enterprise to adopt IPv6 solution. As far as the observatory knowledge, the allocation of free IPv4 address currently is not delegated directly to end users or specific IPv4 services. Most of them are invest in dual stack network or IPv6 transition mechanism like DS-Lite and NAT64 which finally help the transition to IPv6.

4.3 Conclusions

IPv6 is the successor of IPv4. Despite tentative by various stakeholders to develop alternative solutions to delay the deployment of IPv6, or even stay with an IPv4 Internet, IPv6 is now understood as a “next step” in the evolution of the network.

Even if we don’t consider the emergence of new services and paradigms, such as the Internet of Things, IPv6 appears to be the only next step in the evolution of the Internet, and while this statement was not shared among stakeholders a few years ago, it is now the case.

As shown earlier in this document, a huge amount of deployment data has been collected and analyzed during years 2012 and 2013, either on websites showing monitoring information or through the specific tool developed for the study. A survey has also be conducted in 2013 among European ISPs.

Most figures are showing both a still low IPv6 deployment level in all regions of the world and a rapid increase: current level is low but ramp-up has been high over the past 3 years. Few countries have started good initiatives, either supported to national initiatives (Czech Republic, Germany) or through the deployment of IPv6 by major ISP (e.g. ISP with a critical number of users) allowing them to be positioned at the forefront of the adopters.

However, efforts need to be pursued and progress still need to be made in order to have IPv6 deployed on every level of the Internet architecture. One of the key enabler remain the more generalised introduction of IPv6 in curricula.

[60] BGP report : http://bgp.potaroo.net/as6447/

In conclusion, it is important to note that begin of 2014 (January), **all actors are convinced of the need to move forward in deploying IPv6.**

And even if IPv6 deployment is still low, **progress can be clearly seen.** Real usage remains negligible in comparison with IPv4 (and prompted by US companies) but also increases, statistics showing **2.5% of Internet users connected in IPv6**.

On the ISP side, **IPv6 is present in core networks** but difficulties arise on the access part and the survey shown that **ISPs are internally deploying IPv6.**

With regards to curricula and training, **a pool of trained people (with IPv6 competences) exists** but progress need to be done on that matter as IPv6 is not yet well taught in all curricula, this is an area where public authorities may have to play a role.

Finally, IPv6 brings spill over and positive side effect. Firstly, CGN that can be seen as a solution to extend the IPv4 life (but not only) and which is a risk, ISPs continuing to provide IPv4 (private) addresses to their customers. Positive side effect arise too like the Gandi (a French hosting company) announce, now offering a ~17% discount[61] to customers willing to get servers with only IPv6 (e.g. no IPv4 connectivity at all). While this is at the time of writing an isolated case, this could change to become more common.

The table below proposes a list of main conclusion per layer studied.

Layers	Highlights
Competences	Availability of skilled staff appears to be an issue for 50% of the survey respondents (n=1000)
Usage	• 2.8% of end-users are connected in IPv6 (stats from the Observatory) • Transit IPv6 AMS-IX: 0.65%
Service offers (ISP)	• Best mark of 13.8/31 for Germany in the ranking done by the Observatory • In 2013, 18% of respondents use or plan to use CGN • gov. websites CZ 50% on AAAA, NL 40% and below 10% for the others (GEN6)
Services and applications	• AAAA/EU27: 7% • AAAA/Worldwide: 5%
Hosting and related services	*No data available.*
Hardware	Constant number of products certifications per year (~200/year) since 2008.
Network	• % IPv6 AS / Europe: 24% • % IPv6 AS / World: 17% • Average cost of an IPv4 address on relevant market places: ~10/12€

Figure 58 - Main conclusions per layer

[61] http://www.gandi.net/news/en/2013-11-27/1166-ipv6-only_servers/

5 RECOMMENDATIONS

5.1 Introduction

Conclusions of the study show that the IPv6 deployment is still low but progress can be clearly seen and that real usage remains negligible in comparison with IPv4. While this sounds positive, efforts still need to be made in order to accelerate the deployment of IPv6 and to avoid unnecessary global usage of CGNs.

Therefore, a set of recommendations is provided on the following topics:

- IPv6 deployment monitoring
- Socio-economic impact of trends
- Training and awareness raising
- Public authorities

5.2 Recommendations

5.2.1 Monitoring IPv6 deployment

7. Continue IPv6 deployment monitoring

Objective: follow-up with IPv6 deployment observatory in order to assess progresses made over time in order to adjust public policies accordingly.

Action plan

Item	Organisation in action	Beneficiaries
1.1 Maintain this existing IPv6 indicator within the Digital Agenda Scoreboard	European Commission	IT leaders, network managers, public authorities, vendors, service providers
1.2 Develop composite indicators to cover the infrastructure readiness within Europe. As it has been seen during the IPv6 Observatory study, indicators taken individually can show significant progresses, but as soon as they are linked with other indicators, figures are not the same (example: in December 2013, 7.32% of domains (EU27) having IPv6 when looking at websites only, dropping to 0.95% when looking at domains having website, domain name and mail server IPv6.)	European Commission	IT leaders, network managers, public authorities, vendors, service providers
1.3 Extend the monitoring to the hosting and related services layer. This layer lacks of monitoring activities since information are hard to find. Since IPv6 is not a commercial argument, the majority of companies providing hosting facilities do not mention IPv6 in a highly visible zone of their website. It would therefore be recommended to monitor IPv6 offers from hosting companies and also how IPv6 is handled, e.g. with a quality of service to IPv4, or less/more.	European Commission	IT leaders, network managers, public authorities, vendors, service providers

1.4 Monitor the cost of IPv4 addresses on market places: cost of IPv4 addresses on market places will play a major role in the setting up of CGN and in the deployment of IPv6. It would also be important to monitor side effects of the IPv4 address shortage. For example, Gandi, a French hosting company, now offers a ~17% discount[62] to customers willing to get servers with only IPv6 (e.g. no IPv4 connectivity at all). While this is at the time of writing an isolated case, this could change to become more common.	European Commission All	IT leaders, network managers, public authorities, vendors, service providers

5.2.2 Socio-economical impact of trends

8. Socio-economical impact of trends

Objective: Access impacts of the deployment of technical solution that would delay the deployment of IPv6 at the European Union level.

Action plan

Item	Organisation in action	Beneficiaries
2.1 Evaluate the impact of CGN on broadband access and services. CGN is a technical solution to share a single IPv4 address at the ISP level. As it has been shown in 4.1.2, services and applications can suffer when being used over a CGN.	European Commission	IT leaders, network managers, public authorities, vendors, service providers
2.2 Evaluate social impacts of CGN (new form of digital divide). Having CGN well deployed across Europe could create "two Internet", one where users would get public IP addresses and a second one, where users would get private IP addresses, with services potentially running in degraded mode. This could lead to a new form of digital divide that need to be evaluated at the EU level.	European Commission	IT leaders, public authorities, service providers
2.3 Evaluate the impact of the developing IPv4 market on existing ISP businesses and on new entrants. New companies willing to enter on the ISP market could suffer from the IPv4 addresses shortage and the low deployment of IPv6: it would be difficult for such companies to provide customers only IPv6 addresses while difficult too to obtain IPv4 addresses (at least large-enough pool). This could create a strong market distortion since a few large European ISP have enough IPv4 addresses to last a few more years.	European Commission	IT leaders, network managers, public authorities, service providers
2.4 Evaluate the impact of non-globally routable addresses. CGN-like solutions could extend the IPv4 life which could be available as a "degraded Internet" for some users. Indeed, CGN creates technical problems for advanced Internet	European Commission	IT leaders, network managers, public authorities, vendors, service providers

[62] http://www.gandi.net/news/en/2013-11-27/1166-ipv6-only_servers/

application, as multiple levels of NAT are introduced between the end-user and the services. This would potentially create a new digital divide.		

5.2.3 Training and awareness raising

9. Raising awareness and knowledge to implement seamlessly IPv6

Objective: purpose of this recommendation is to avoid any disruption in businesses within the transition phase. The target here is to raise awareness and knowledge of decision makers and network managers about obstacles hindering deployment, for example the potential security risks that would exist in case of insufficient knowledge. The European Commission facilitates raising IPv6 knowledge level cooperating with private and public stakeholders.

Action plan

Item	Organisation in action	Beneficiaries
3.1 Communicate on the need for IPv6 skilled staff. The results (final report, website) of the IPv6 Curricula study should be further promoted again as remain valid in their majority.	IPv6 Forum, IPv6 task forces, GEN6	Organisations business and human resources levels
3.2 Train network managers to use IPv6 monitoring tools. An initial set of information regarding monitoring standards and tools was provided by the 6DEPLOY project 'Network Management'[63] report which describes the different ways to retrieve management information (MIBs, IPv6 flows) and presents some IPv6 management tools and platforms.	IT services	Network managers
3.3 When selling IPv6 enabled products, warn users about the need to be IPv6 skilled for their use, even if deployment planned in an IPv4 environment. The notice should highlight risks related in running the product without needed expertise and advantages that could emerge in introducing this device in the network. This notice should target network engineers and system administrators (deploying for instance Windows 7 which is IPv6-enabled by default) and cover (at least) IPv6 security vulnerabilities, advantages and shortcomings.	Manufacturers and software providers	IT products users
3.4 Recommend ISPs to provide globally routable IP addresses. While IPv4 addresses behind CGNs might degraded services, recommending ISPs to provide globally routable addresses would help in avoiding this issue and would obviously acts in favour of the IPv6 deployment.	ISPs	Internet users

[63] « IPv6 network management », 6 deploy project, http://www.6deploy.eu/tutorials/060-6deploy_IPv6_management_v0_3.pdf

10. Make training resources available

Objective: Purpose of this recommendation is to ensure the presence of up-to-date and high quality on-line training resources and to encourage its use by training providers and beneficiaries. Developed training resources should take advantages from e–learning technology.

Action plan

Item	Organisation in action	Beneficiaries
4.1 Recommend Member States to integrate IPv6 in their college/university curriculums	Public authorities and Universities	Students
4.2 Get training content adapted to local specificities (language, industrial sectors…) and provide a set of technical tutorials ready for publication to technical magazines. While first item would be more focused on actions at a national level, the second item could be included in the dissemination plan of a project such as 6Deploy	Member states	IT practitioners Training providers
4.3 Develop hands-on remote access labs. It is underlined that IT capabilities are better acquired through on field-testing. Remote access to laboratory should be encouraged and integrated with developed e-learning courses (see action item 2.1)	NREN Academics	IT practitioners Training providers

11. Get training courses being recognised

Objective: Increasing needs for IPv6 training may lead to the development of poor quality training courses. The objective of this recommendation is to recognise a certification (academic diploma or industry certificate) scheme ensuring a minimum level acquired knowledge and training quality.

Action plan

Item	Organisation in action	Beneficiaries
5.1 Providers of certification schemes should agree on a common charter of conduct establishing a minimum level of quality.	Certification scheme providers ETSI support	Certification authorities IT practitioners Training providers
5.2 When recruiting IP practitioners who have to deal with the network layers, request certified IPv6 skills.	HR departments	Recruiting organisations
5.3 When procuring new equipment, software or services related to IP layer, follow the RIPE 554 requirements, including the request to ask for people being professionally trained in the tendering organisation[64].	Procurement departments	Equipment, software or services buyers
5.4 Select certified training courses and get your training being recognised by a diploma or a certification.	Training beneficiaries	Training providers Training beneficiaries
5.5 Get your training to be certified and propose your trainees to evaluate the acquired knowledge by passing a diploma or a certification	Training providers	Training providers Training beneficiaries

5.2.4 Public authorities

12. Public authorities

Objective: Ensure that member state play their role in the deployment of IPv6

Action plan

Item	**Organisation in action**	**Beneficiaries**
6.1 Ensure presence of IPv6 in public curricula	Member states governments	Students, Life long training beneficiaries
6.2 Ensure that IPv6 is required in public procurements	Member states governments, Education ministries	Vendors, public authorities
6.3 Make sure that websites at national and local levels are IPv6 enabled	Member states governments, local governments, public authorities	Public authorities, eGovernmeent services users

[64] In the RIPE 554,formulating requirements can be done in several ways: first option is based loosely on the NIST/USGv6 profile developed by the US government, second option is based on compliance with the "IPv6 Ready" program (testing and certification of the basic "core" protocols, and testing and certification of advanced IPv6 functionality), and third option is a combination of the two first options. http://www.ripe.net/ripe/docs/ripe-554

6 ANNEX

6.1 1st workshop report – IPv6@Gov (23-24 January 2013)

6.1.1 Summary

A workshop gathering more than 40 participants from government, academic, industry and public bodies took place on January 23-24 2013 to review the current situation for IPv6 deployment in EU member states. While figures show a tripling in availability of websites over IPv6, real usage still remains negligible in comparison with IPv6 and prompted by US companies. To compensate for the late IPv6 adoption, some ISPs are deploying large-scale NATs (also called Carrier Grade NAT (CGN)). Deployment initiatives at national and regional level reveal the need for careful planning and set-up of national IPv6 deployment roadmaps in addition to the lack of full IPv6 support for some technologies. Exchange of best practices, monitoring of the deployment, benchmarking of initiatives and increase of IPv6 engineering skills of the work force are still appraised by the present expert community.

6.1.2 Introduction

"*I came in (IPv6) five years ago [...] I thought it should be relatively straightforward since all the arguments were there [...] , in fact it was a marathon*" said Mr Per Blixt, head of Unit at European Commission in the opening of the IPv6@workshop hold on January, 23-24th in Brussels. This workshop co-organized by the IPv6 Observatory[65] and the GEN6 project[66], two initiatives funded by the European Commission, was dedicated to the policy dialogue on the IPv6 deployment in European Union Member States.

More than 40 participants from the academic, industry and public bodies attended the workshop. Sessions were organised to cover:

- Deployment situation
- National initiatives
- Regional initiatives

6.1.3 Deployment situation

Overall the deployment level of IPv6 has shown a steep increase in 2012, during the world IPv6 launch day organized by the Internet Society which saw Internet service providers (ISPs), home networking equipment manufacturers, and web companies permanently enabling IPv6 on their products and services[67].

[65] inno TSD, University of Luxembourg, "EU IPv6 observatory," 2012. [Online]. Available: http://www.ipv6observatory.eu/.
[66] GEN6, «Governments ENabled with IPv6,» [En ligne]. Available: http://www.gen6.eu.
[67] Society, Internet, "World IPv6 launch," 2012. [Online]. Available: http://www.worldipv6launch.org.

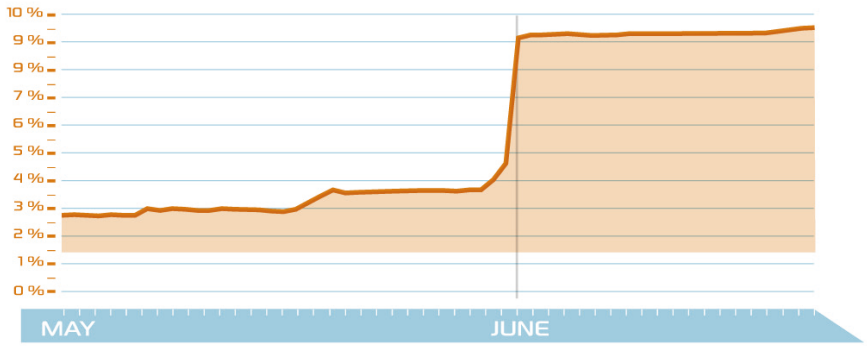

Figure 59 - Percentage of Alexa top 500 websites having a AAAA DNS record, cumulated over EU27 (13500 websites tested) (source: IPv6 Observatory)

On that day, a number of websites permanently and natively accessible on IPv6 has tripled, moving from 3% to 9% for the Alexa top500 websites in EU27 member states. Nevertheless, this positive increase in IPv6 usage has been put in perspective by several of the workshop participants:

1. First, even if the number of website accessible over IPv6 has increased to reach 4% of the top 1 million website as ranked by Alexa[68], the number of accessible website is still low compared to IPv4.
2. Looking in details at the website which enabled IPv6 shows that a major contribution to this increase has been achieved by the American giant Google, which deployed IPv6 over all its national servers (such as google.be, Google.fr, etc.), recognising the strategic interest of IPv6 presence. At the same time, European companies are noticeably less present in the list of IPv6 enabled websites.
3. The IPv6 share of bandwidth is below 1% as measured at the Amsterdam exchange point whereas only 1% of Google users connect to the search engine through IPv6[69], demonstrating a critical low level of IPv6 availability on the access network.

Two major European Internet Service Providers, Deutsche Telekom and France Telecom Orange, presented their current plans related to IPv6. In Germany, IP-based DSL connections proposed by Deutsche Telekom offer a dual stack IPv4/IPv6 since September 2012. This move has been said to be initially driven by public IPv4 addresses exhaustion but thanks to its Terastream technology (combination of cloud and networking technologies) Deutsche Telekom recognises that native IPv6 can deliver a significant experience boost for the customers and significant cost benefits for the carrier, with legacy IPv4 or MPLS delivered as a service. Part of the IPv6 addresses being used for service differentiation. Introduction of dual stack in mobile networks is planned for 2014.

From a neighboring country, Orange acknowledges IPv6 as the only perennial solution against IPv4 depletion but at the same time acknowledge that the IPv4 service continuity during the forthcoming transition period as to be ensured. Locally, the use of Carrier-Grade NAT (CGN) will thus be envisioned to rationalize the IPv4 addresses usage. CGN is recognised to strongly limit the internet user's experience as end user does not hold a global (routable) address anymore.

[68] Alexa, "The Web Information Company," [Online]. Available: http://www.alexa.com/.
[69] Google, "Gogole IPv6 statistiques," [Online]. Available: http://www.google.com/ipv6/statistics.html.

On the mobile network side, tendency is on the set-up of a single Packet Data Protocol (PDP) context to save bandwidth, leading to the probable encapsulation of IPv4 within IPv6.

Discussions following the presentations converged on the opinion that IPv6 is now well present in the core of the networks but difficulties arise on the access part of the network.

Finally, while for years the killer applications for IPv6 has been looked for, Orange now foresees that the fast development of Machine to machine (M2M) protocols will drive forward the deployment of IPv6, especially on the mobile side.

6.1.4 National initiatives

On the governmental side, several initiatives were presented. In Germany, a strong effort has been done under the impulse of the Federal Ministry of the Interior and Federal Office of Administration to coordinate the *Deutschland Online Infrastructure* (DOI) project which aims at providing a Secure electronic communication between central government, federal states, local authorities (and their representations in the EU) and the European sTESTA as well as creating and expanding a national communications infrastructure. Main efforts have been made on the definition of the addressing plan and the IPv6 profile definition. The need to exchange best practices with similar initiatives has been pointed out and as an example, recommendations from the DOI project have been published[70].

Pushed by the CZ.NIC Association and with a governmental resolution from 2009, the Czech republic demonstrates a deployment of IPv6 services in governmental institutions (national, regional and local) 3 time larger than the national average, knowing that Czech Republic is one of the most advanced EU country for IPv6 adoption[71]. The governmental progresses are monitored through a benchmark planned to be updated every 3 months. The need to develop an analysis of the impact of government policies on IPv6 deployment is underlined.

In Greece, efforts have been made within the Greek Schools network for which a dual stack backbone is fully IPv6 enabled whereas on the access side, 85% of the schools are IPv6 connected. Thanks to the support of the GEN6 project, IPv6 support is going to be included in the tender of the Greek Public Administration Network (SYZEYXIS-II).

In parallel with governmental transitions, additional constraints are brought by the development of IPv6 based cross boarder scenarios, such as public safety communication or administration communication (sTesta). Experiments are running for porting of sTesta to IPv6 as this transition has to be planned in a synchronised way among member states. Discussions also illustrated difficulties faced in the field. As an example, the cryptobox, allowing hardware based security, are still not fully compliant with IPv6.

Finally, the availability of a sufficiently skilled workforce is still questioned as a standard IPv4 knowledge is far from being enough to ensure efficient, effective and secure IPv6 deployment.

[70] Bundesministerium des Innem, "deutschland online infrastruktur ipv6 referenz handbuch," 2011. [Online]. Available: http://www.ipv6actnow.org/wp-content/uploads/2012/05/de-government-Referenzhandbuch-_EN.pdf. [Accessed February 2013].
[71] IPv6 observatory, «Measuring IPv6 penetration in websites,» 2012. [En ligne]. Available: http://www.ipv6observatory.eu/?post_type=report&p=808.

Projects such as 6Deploy[72] at the EU level initiated the development of training courses and road shows but IPv6 now needs to be urgently included in higher education curricula of member states: European IT students should know IPv4 but should think IPv6 first.

6.1.5 Regional initiatives

The regional level is the one at which many decision related to well-being of citizen are taken. A number of infrastructure and public services are set at a regional level or include a regional representation. This is visible in the European Union organisation which devotes a significant share of its budget to the EU cohesion fund acting at the regional level. It is interesting to note that the latest European strategy for regions, the Smart specialisation strategy (S3), propose pre-conditions for being eligible to EU funding which include enhancing access to and use for quality of ICT, including Digital Agenda objectives. As regions needs to develop a chapter for digital growth as part of their S3 strategy[73], IPv6 deployment should also be advocated at the regional level.

Examples of regional initiatives have been shown with applications in fields such as regional broadband deployment, datacentres set-up or smart Grid deployments. In every case, the need to carefully plan the development, starting with the set-up of a clear governance model is underlined. Then rules similar to the national level are proposed: identifying the services impacted, defining the IPv6 profiles and including IPv6 constraints in all IT tendering procedures. The need for awareness raising at regional and even local level has been raised and may have not nee sufficiently taken into consideration up to now.

This raised the interest of further monitoring the way IPv6 is deployed and the need to evaluate the socio-economic impacts of the different approaches used for IPv6 deployment.

6.1.6 Conclusions and call for actions

All actors are convinced about the need to move forward in deploying IPv6. Nevertheless, despite steep increase of IPv6 use in 2012 following the world IPv6 launch day, The real usage is still negligible compared to IPv4 and observed evolution has mostly be created by the move of few big US industries. European Internet Service Providers are slowly moving and IPv6 availability appears in roadmap but while core network is mostly ready, issues exist on the access network.

The rationale for IPv6 deployment is still here and arguments detailed in the previous EC IPv6 Communication[74] and studies[75] [76] [77] are still present in the discussions. While the depletion of the IPv4 pool is now a reality in some RIRs, new delays appear with the development of solu-

[72] 6DEPLOY-2, "IPv6 Deployment and support," [Online]. Available: http://www.6deploy.org/.
[73] European Commission, Joint Research Centre, "Guide to Research and Innovation Strategies for Smart Specialisations (RIS3)," May 2012. [Online]. Available: http://s3platform.jrc.ec.europa.eu/home.
[74] European Commission, "ADVANCING THE INTERNET - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe," 27 May 2008. [Online]. Available: http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf.
[75] inno TSD, Zaltana, «Impact of IPv6 on Vertical markets,» 2007. [En ligne]. Available: http://www.ipv6council.de/fileadmin/documents/IPv6_vertical_markets.pdf.
[76] IABG, «IPv6 security models and dual stack (IPv6/IPv4) implications,» 2010. [En ligne]. Available: http://ec.europa.eu/information_society/policy/ipv6/docs/studies/IPv6%20security%20models%20and%20implications%2030072010.pdf.
[77] Training4ipv6, «IPv6 Curricula,» 2011. [En ligne]. Available: http://www.training4ipv6.eu/images/reports/ipv6%20curricula%20final%20report-%20final%20v6.4%20no%20annex.pdf.

tions such as CGN, appearing as a short term solution for IPv4 addresses but postponing again the native IPv6 adoption while putting strong limits on the users' experience of Internet. **The socio-economic impact of IPv6 (non-)adoption, including the use of technologies such as CGN thus need to be evaluated, in light of the reality of IPv4 addresses depletion and the development of M2M and Internet of Things, avid of IP addresses.**

Practical experience of IPv6 deployments at ISP and member states level show that IPv6 knowledge is improvable and that the IPv6 technology is still not fully mainstream. **There is still a need to encourage exchange of best practices with the documentation of practical transition scenarios**. After several years of development of IPv6 national policies, **they should be benchmarked and their impact evaluated**.

The regional and local levels should not be forgotten when acting for IPv6 awareness and the RIS3 developing regional policy offer an opportunity to advocate the inclusion of IPv6 in regional IT plans.

Finally, the need for stronger education of IT personal is still required as many engineers still see IPv6 as a simple address update of IPv4 and completely miss the potential of new IPv6 capabilities. Universities and higher education school are prompted to adapt their curricula to the field reality which is now IPv6.

6.1.7 Workshop presentations

All presentations are available online on the study's website, at the following URL: http://www.ipv6observatory.eu/the-study/workshop-ipv6-gov/

6.2 2nd workshop report - IPv6 deployment: trends and perspectives (14 October 2013)

6.2.1 Summary

The IPv6 observatory organised its second public workshop during the RIPE #67 meeting that took place in Athens from 14-18 October 2013. More than 30 participants from the network services area (ISPs, RIRs, LIRs, network industry) attended the workshop, which presented the current situation and trends regarding deployment of IPv6. Observations made show deployment of IPv6 is still increasing but with overall low numbers, in the range of few percent when comparing to IPv4 situation.

An observed trend is the increasing interest for alternative technologies such as large scale Network Address Translation (NAT) which allows to address a broader customer basis by allocating private IP addresses to the end users, at the expense of reduction of final user quality of experience.

6.2.2 Introduction

The workshop organized by the IPv6 Observatory[78], an initiative funded by the European Commission, was dedicated to the analysis of the IPv6 deployment situation and its impact on the policy options for public as well as Internet authorities. The workshop was nicely co-located with parallel sessions of the RIPE #67 meeting, allowing to attract participants beyond the initially registered one. The more than 30 registered participants were mostly representing:

- Internet Service Providers (ISP)
- Regional/Local Internet Registries (RIR/LIR)
- Network industry

All given presentations are available online[79].

Figure 60 - Workshop poster

6.2.3 Deployment situation

The situation has been exposed by different presenters with converging conclusions: even if increasing, the overall deployment of IPv6 still remains negligible. The situation is here under described for the different dimensions being looked at by the IPv6 observatory

- **Network:** On the user's side, the IPv6 deployment level as measured by Google is doubling every 9 months with a current level as low as 2.25% (Figure 61) of total traffic (IPv4+IPv6). This number is representative of users access to IPv6 in countries where Google is well established (Americas, Europe) but cannot be extrapolated at the worldwide scale.

[78] inno TSD, University of Luxembourg, "EU IPv6 observatory," 2012. [Online]. Available: http://www.ipv6observatory.eu/.
[79] I. observatory, «Trends & Perspectives workshop,» 14 October 2013. [En ligne]. Available: http://www.ipv6observatory.eu/the-study/workshop-trends-and-perspectives/.

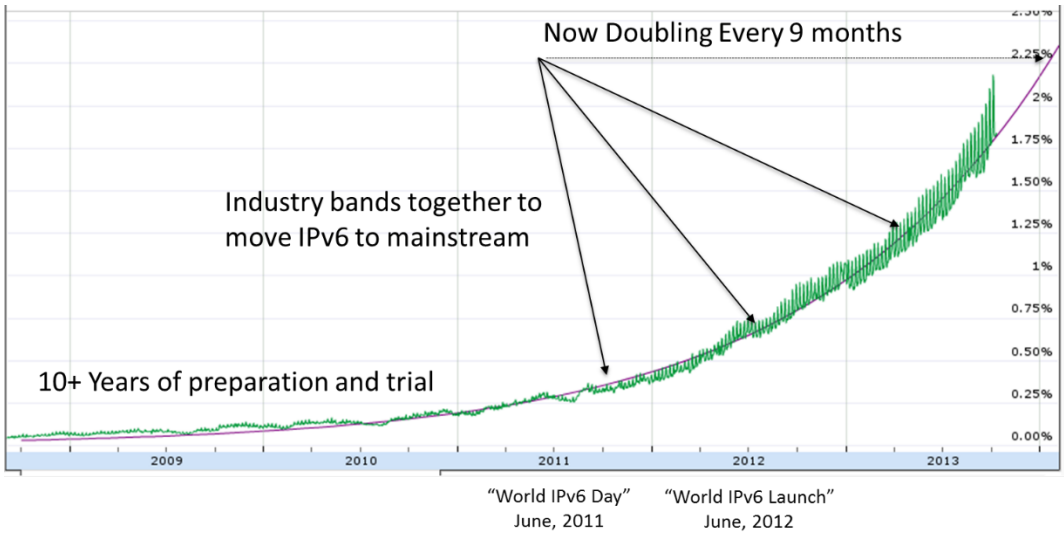

Figure 61 - Potential evolution of IPv6 usage based IPv6 deployment level as measured on requests received by Google (source Cisco).

This low level on the end users side is balanced by higher values of IPv6 penetration in the core (Figure 62) with overall 17% of networks (ASes - Autonomous Systems) announcing an IPv6 prefix in the RIPE region, reaching 24% in Europe. The historical curves shows a *take-up starting from 2008-2009*, following the European commission IPv6 call for action[80], without strict correlation demonstrated.

[80] European Commission, "ADVANCING THE INTERNET - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe," 27 May 2008. [Online]. Available: http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf.

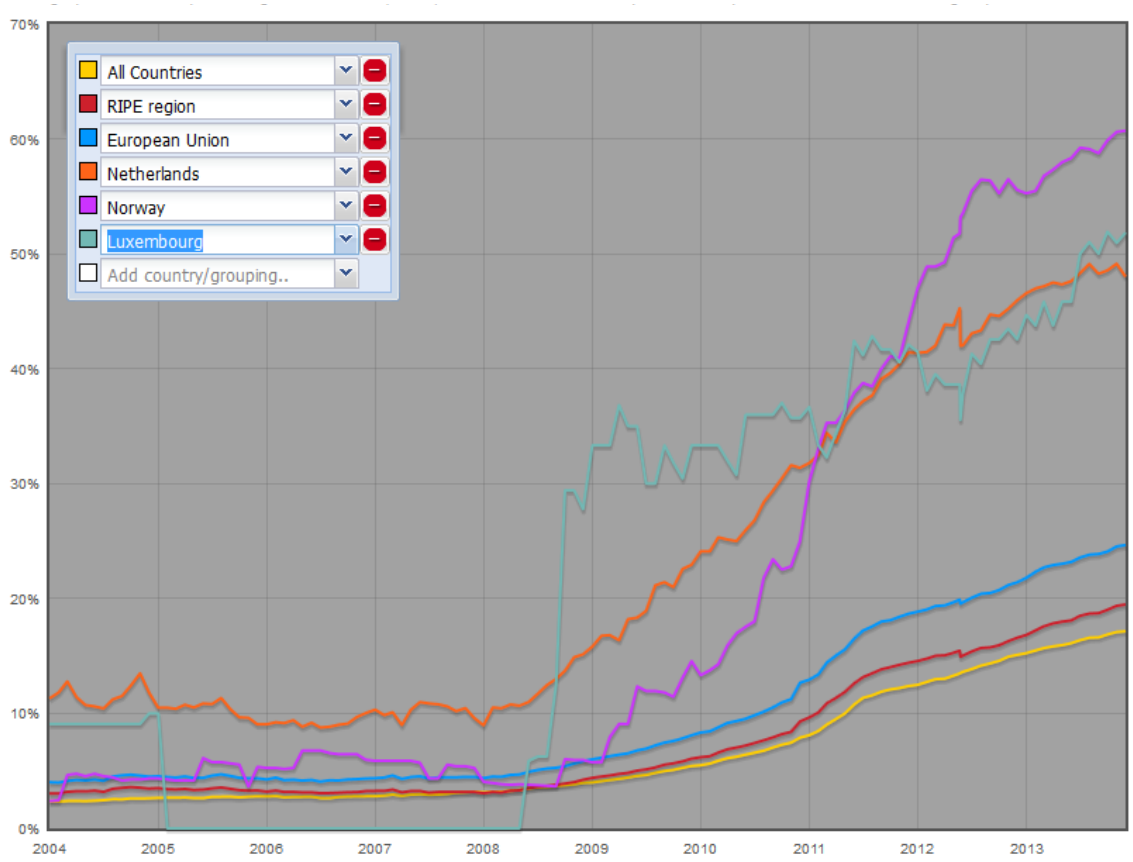

Figure 62 - Percentage of networks (ASes) that announce an IPv6 prefix for a specified list of countries or group of countries (source RIPE[81])

- **Deployed Services and applications**: logically positioned between core network and end-users, the deployed services and applications exhibit intermediate values are obtained: looking at the proportion of web domains having a AAAA record (the AAAA record maps the domain name of a website site to its IPv6 address) shows that about 5% of the websites from the top 1 million published by Alexa[82] are accessible though IPv6 (Figure 63).

[81] RIPE, «Percentage of networks (ASes) that anounce an IPv6 prefix,» [En ligne]. Available: http://v6asns.ripe.net/.
[82] Alexa, "The Web Information Company," [Online]. Available: http://www.alexa.com/.

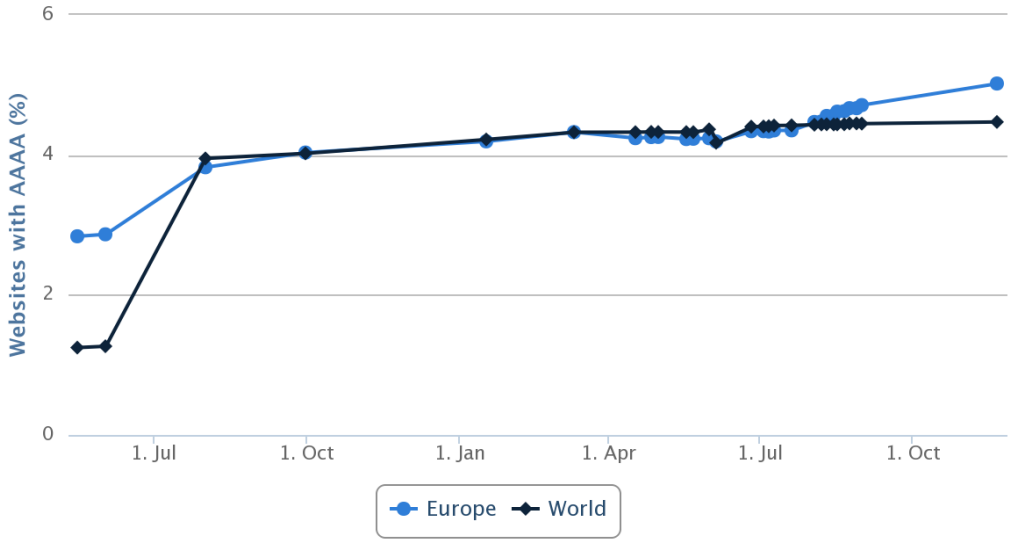

Figure 63 - Number of websites having an AAAA record (source IPv6 observatory)

Regarding the situation in public services, the gen6 project analyses the situation of public authorities' websites at both national and regional levels (Figure 64). Collected results show large discrepancies among the surveyed states. While Czech Republic and Netherlands show more than 40% of website presence on IPv6, most of the countries are well below 10%. Nevertheless, some countries such as Germany are working on the background in deploying IPv6 within the public networks. Still, no activation date has been mentioned.

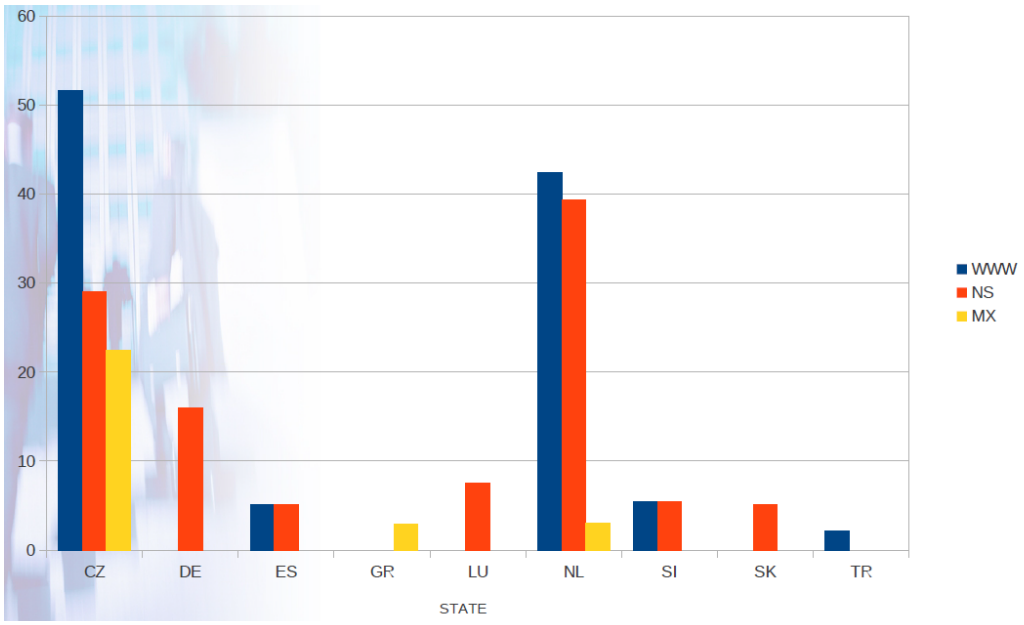

Figure 64 - IPv6 in public administration (source GEN6[83])

[83] GEN6, «IPv6 in public administration,» [En ligne]. Available: https://devpub.labs.nic.cz/ipv6-smt-new/country/

6.2.4 ISPs positioning

Finally, emphasis has been put on the analysis of the situation on the Internet Service Providers (ISP) side. Firstly 68 ISPs from 12 countries have been evaluated and the countries ranked against their proposed IPv6 offer. The study shows IPv6 in commercial offers is slowly starting and when available, comes at no additional cost. While core networks are mostly ready, operators are now concentrating on deploying the access networks.

Also, a large survey has been run by the IPv6 observatory among RIRs members. The survey collected 1515 answers from 131 regions/economies with 46% of the respondents being ISPs. While for most of the questioned topics, the situation remain stable when comparing with 2012, an emerging trend is the **increase use of CGN** (Carrier-grade NAT) which allows to overcome the public IP addresses shortage by bringing Network Address Translation (NAT) techniques closer to the core networks, **at the cost of reduced experience for the end-users**.

6.2.5 Conclusions and recommendations

Overall, the deployment of IPv6 is progressing with 17% observed in the core (number of ASes), 5% in http service (AAAA record for websites) and traffic of about 2% (Google request). While this number is still low, longitudinal analysis of the curves show a traffic doubling every 9 months and if pursued at that pace, the 25% target may be reached in the 3 years to come.

Overall already known recommendations remain valid with firstly the need to increase IPv6 skills of the workforce so engineer can better understand and rip the benefits from IPv6 while increasing efficiency of the deployment. Governmental support and awareness also still appear

Nevertheless, an observed trend is the increase usage of CGN not only in parallel of IPv6 but also as a replacement to it. While CGN may offer an easiest and faster solution to increase the customers basis by sharing public IPv4 addresses, it prevents end-users from fully benefiting of the Internet services in areas such as peer 2 peer communications, multi-players gaming, remote administration, etc.

Discussions in the room underlined **the necessity for public authorities to ensure that all citizen get globally routable IP address in order to not create an additional digital divide within the Internet.**

6.2.6 Workshop presentations

All presentations are available online on the study's website, at the following URL: http://www.ipv6observatory.eu/the-study/workshop-trends-and-perspectives/.

6.3 IPv6 Security Architecture (public report)

6.3.1 Scope

This security technology paper focuses on the fundamental security deployment issues for IPv6-enabled networks. It is not meant to define a definitive security policy for any particular environment but rather it is an attempt to enumerate all of the considerations to be accounted for when creating an appropriate security policy and architecting the IPv6 network to incorporate appropriate security measures. It is assumed that the reader is familiar with basic IPv6 operation and has a fundamental understanding of network security issues.

6.3.2 Introduction

As IPv6 networks migrate from lab environments into dependable production systems, we are presented with both the challenge of adapting our Information Assurance (IA) architecture to a new protocol and the opportunity to leverage new features to enhance network security. Native IPv6 networks will coexist with environments where IPv6 capabilities are introduced into production networks with existing IPv4-based infrastructures. While security of our current production networks must be evolved for IPv6, there are features in IPv6 and new trends in networking that should lead us to changing security paradigms. End-to-end security between hosts has had limited practicality in IPv4-based networks but is a key feature of IPv6. A return to the end-to-end network model should be architected into any dual stacked transition architecture with careful consideration for not compromising IPv4 security.

The controversy of whether host based security is better than network based security should be resolved with the understanding that a layered security approach is necessary. A combination of application, host and network-based security is required to securely conduct business on the network of networks which make up the Internet.

This white paper will enumerate the security advantages which are relevant in today's IPv6 networks and will detail the deployment considerations to effectively design and architect secure IPv6 networks.

6.3.3 Information Security Fundamentals

What does it mean to provide a secure network? Invariably, the goal is to protect electronic communication from malicious individuals and applications who are determined to spoof, corrupt, alter or destroy the data or render critical services unavailable. Protection is required by every device that is participating in networked communication and all information that is either

stored on a device or is in transit between communicating devices or is processed by the devices.

Protecting the critical devices that make up these network infrastructures and the business processes which are dependent on the network is a key concern for everyone. Too many people today are agonizingly familiar with the increasing threats of email spam, phishing scams, worms, viruses and numerous DoS attacks which impact business services and communication needs. Computer network attacks no longer target simply a single machine or even a single network. Today's attack trends are increasingly more automated and sophisticated and can result in large distributed denial-of-service attacks that broadly affect key components of information networks. Even unsuspecting users can cause a risk if unbeknownst to them their infected system begins to spread a worm or virus throughout the corporate network. Alternatively, device mis-configuration or a down-rev with respect to operating system patch levels can also create a new vulnerability that opens the network to external attack. A secure network architecture incorporates mitigation techniques which decreases the risk of both deliberate attacks or unintentional events.

6.3.3.1 Security Properties

It is critical to today's business needs that all networked devices and be accessible at all times in a reliable and secure environment. The mechanisms to provide the security regulation can take many forms, but essentially all forms pertain to the preservation of confidentiality, integrity, accountability and availability.

- Confidentiality is the property by which access to information is restricted to those who are privileged to see it. Examples of violations of confidentiality include bypassing access control rules or having the capability to read unauthorized information while it is in transit from sender to the recipient.
- Integrity can pertain to the data as well as the communicating parties. Data integrity is having trust that the information has not been altered during its transit from source to destination. Host/user integrity is having trust that the sender and / or recipient of the information is who it is supposed to be. Data integrity can be compromised when information has been corrupted, willfully or accidentally, before it is read by its intended recipient. Host/user integrity is compromised when an imposter "spoofs" a sender's identity and supplies incorrect information to a recipient.
- Accountability is synonymous with non-repudiation. Non-repudiation refers to the property that you cannot deny having done something.
- Availability is the property that the information or resources are accessible when required within a reasonable period of time. At the most fundamental level, these are the security properties that must be considered and incorporated into a sound security policy. What information is confidential? Does it need to be kept confidential while that information is accessed via the network? Does it need to be kept confidential while it is stored in a database or file? How is integrity of the data preserved? Only a comprehensive corporate risk assessment will provide the answers required to determine the protection that is warranted to any specific environment. For readers looking to supplement their existing network security policies, one of the best resources for examples and templates can be found at the following url: http://www.sans.org/resources/policies/.

6.3.3.2 Security Services

How to implement the security properties as defined by a given security policy is a different problem. Usually, there exist a variety of mechanism which needs to be considered. The following services are primarily used to implement the properties of confidentiality, integrity, accountability and availability:

- Authentication is the process of verifying the claimed identity of a device, user and/or application trying to access the resources.
- Authorization is the rights and permission granted to a user or application that enables them the access to network or computing resources.
- Access control is the means by which an authorized user has access to resources.
- Encryption is the mechanism by which information is kept confidential from unauthorized users.
- Auditing is the process that keeps track of what an authorized or unauthorized user or application is doing.

What makes the problem complex is that these services can be applied at varying levels of the TCP/IP model. Take for example the problem of wanting to provide confidentiality by encrypting a web-based financial transaction as illustrated in Figure 65.

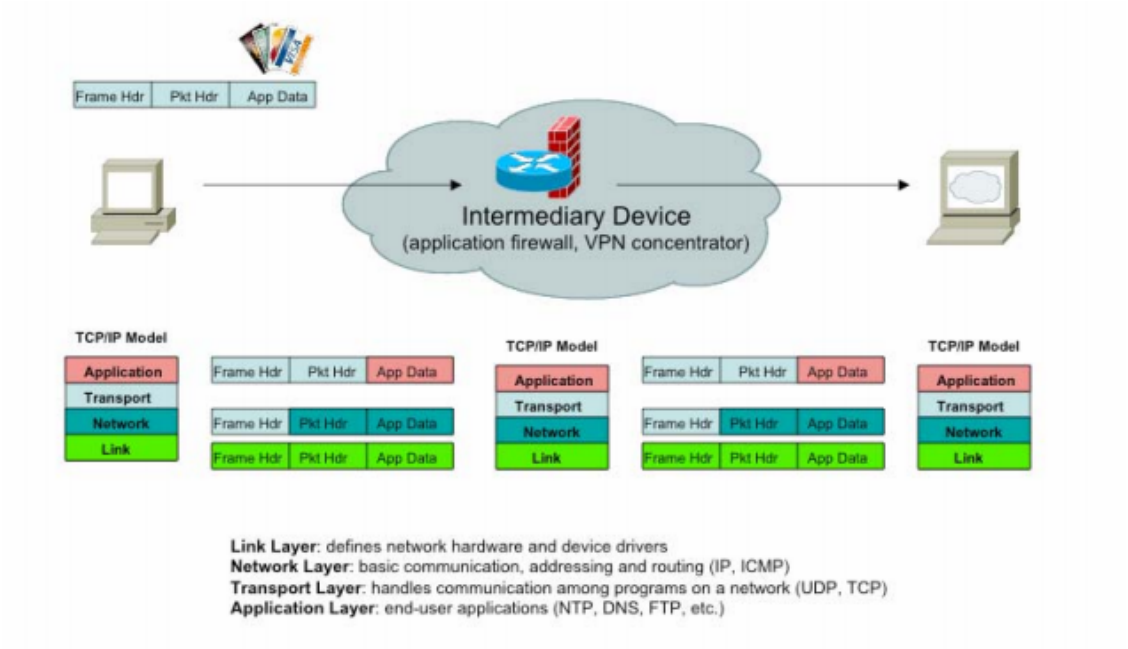

Figure 65 - TCP/IP layered security example

The encryption can be performed at either the application layer, the network layer or the link layer. Note that encryption can also be performed at the transport layer although for visual simplicity, this case was not shown in the figure. The trade-off as you go up the TCP/IP-layer stack is that you perform the security service, in this case encryption, at a greater granularity for the specific data that requires the specific service. Additionally, the security services can be pro-

vided on the end hosts that re participating in the communication or by intermediary network devices. An effective security architecture will ensure that the security services are applied in an efficient manner to avoid duplication of effort and unnecessary processing cycles.

Security services will always be required at varying layers of the TCP/IP stack due to varying policies and the need to integrate easy deployment with the appropriate granularity to offer the required security protection. When specifically dealing with the network layer, all of the security service considerations required to protect networked communication is independent of whether IPv4 or IPv6 is used for the networking layer transport.

6.3.4 Comparing IPv4 and IPv6 Security

Although any security architecture requires a layered approach, let's look at how security concerns compare and contrast in IPv4 and IPv6 environments. As pointed out in the previous section, the fundamental security properties and security services used to protect the network infrastructures and the information traversing these networks are the same in both IPv4 and IPv6 environments. A comparison of IPv4 and IPv6 threat analysis by Darrin Miller and Sean Convery shows the similarities of potential threats and mitigation techniques in both types of networks.

The paper recommends that secure IPv6 deployments should be ensured from the start and not be provided as an add-on as was done with IPv4 deployments.

It is important to recognize security enhancements that have been incorporated into the IPv6 base protocol specification (rfc2460) and the added advantage of re-introducing an end-to-end security model without some of the legacy constraints that exist in today's IPv4 networks.

The designers of the IPv6 protocol took into consideration the known security vulnerabilities affecting IPv4 networks at that time and architected a solution which would mitigate many of the risks of those known vulnerabilities. This included issues of broadcast storms, fragmentation attacks and security services such as device authentication, data integrity and confidentiality.

IPv4 networks are susceptible to varying types of fragmentations attacks. The IPv6 standard provides better fragmentation attack mitigation because it requires that:

- Fragmentation is prohibited by intermediary devices – this has a subtle advantage when it is definitively known between some communicating peers that no fragmented traffic will be used.
- Overlapping fragments are not allowed – this is implied by specifying that only the source can actually create fragmented traffic.
- Devices are required to drop reassembled packets that are less than the 1280 byte minimum MTU

Broadcast amplification was another concern in IPv4 networks. The IPv6 specification removes the concept of dedicated broadcast from the protocol and specifies specific language in RFC2463 to mitigate these types of attacks by specifying the following:

" ICPMv6 messages should not be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address or a link-layer broadcast address"

The IPv6 standard also mandates that all IPv6 capable devices support IPsec for providing authentication, integrity and confidentiality services at the network layer. Whereas the IPv4 protocol had to retrofit IPsec headers into the original IPv4 frame, IPv6 has the capability to support IPsec within the defined packet structure using extension headers.

As will be pointed out in subsequent sections of this paper, if IPv6 deployments follow the same architectures of IPv4 today, the security models will be much the same with only minor advantages.

However, IPv6 security architectures should look to take advantage of the end-to-end security model and make appropriate policy decision modifications where appropriate.

6.3.5 (Re)Introducing The End-to-End Security Model

IPv6 network architectures can easily adapt to an end-to-end security model where the end hosts have the responsibility of providing the security services necessary to protect any data traffic between them. This results in greater flexibility for creating policy-based trust domains that are based on varying parameters including node address and application, as shown in Figure 66. Each device or end-host can be a member of multiple trust domains, each subject to varying security policies.

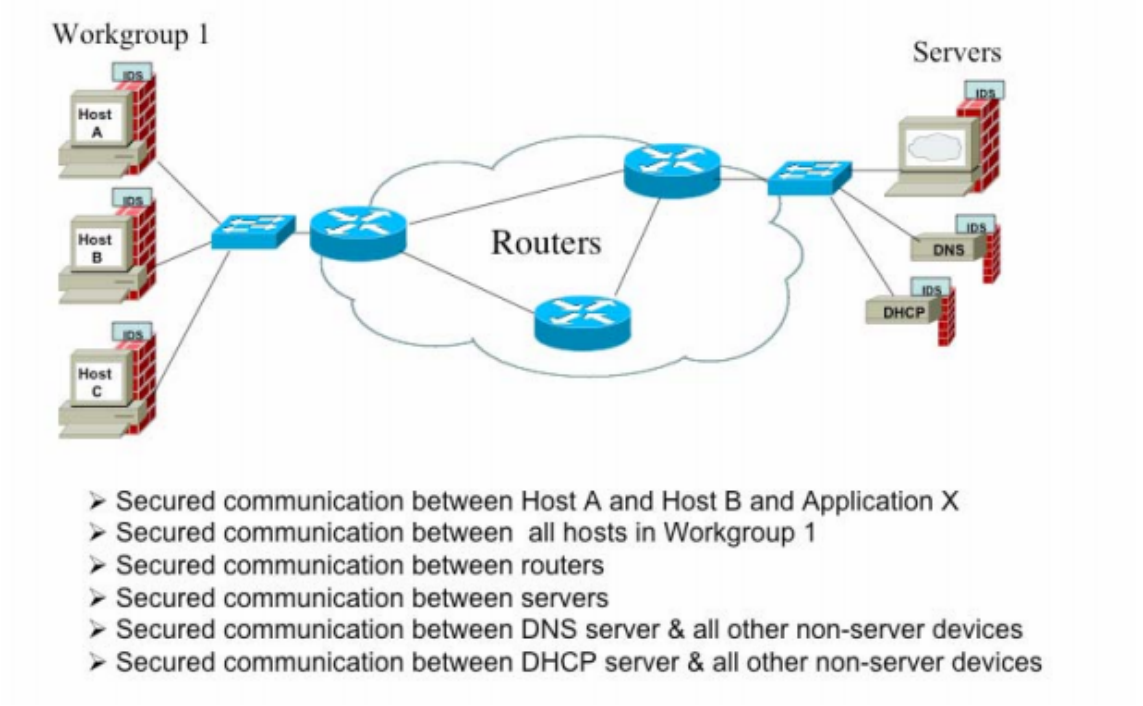

Figure 66 - End-to-end security

When any pair of end devices want to communicate securely, the devices can initiate an authenticated and confidential exchange. Note that these end devices can be end-hosts, servers or routers since the end points in an end-to-end model define the device that is either initiating or receiving the data. Most workstation or server based security implementations augment or enhance local security measures to enforce data integrity, prevent exploitation of the system, and ensure system availability. These hosts can protect themselves from unwanted traffic by providing access control (i.e. firewall) protection on the hosts such that any traffic gets inspected after it gets decrypted and before being forwarded to any upper layer processing. Auditing functions at each host log any potentially malicious activity and provide the means to audit any malicious behavior.

6.3.5.1 Hybrid End-to-End and Network Centric Security

An end-to-end security model does not mean that there will not be any security services within the network infrastructure. On the contrary, security services should be deployed in both areas to increase the defense in depth. There exist a number of hybrid scenarios which combine end-to-end and network centric security architectures when deploying IPv6. For many transition networks these hybrid solutions can provide a gradual move to native IPv6 networks while still maintaining a secure network which mitigates most of the known vulnerabilities. The tradeoff is often a decision based on performance versus management.

6.3.5.1.1 Distributed Firewalls

The most common hybrid security model will incorporate the concept of distributed firewalls. The distributed firewall model consists of managed host-based firewalls in addition to the conventional perimeter firewall model. The addition of managed host-based firewall security adds “defense in depth” to an enterprise’s security architecture and reduces reliance on a single "chokepoint" perimeter security network design. Current firewall systems typically perform all security screening through a common checkpoint. The performance of a single checkpoint approach is increasingly degraded as broadband traffic increases over time, new network protocols are added, and as end-to-end networking and encrypted tunneling become more common. With most net-centric enterprises investing in enhanced IT performance, a network-based firewall model is a definite drawback.

In future security architectures, more coordination will be established between network and host-based firewalls as illustrated in Figure 67.

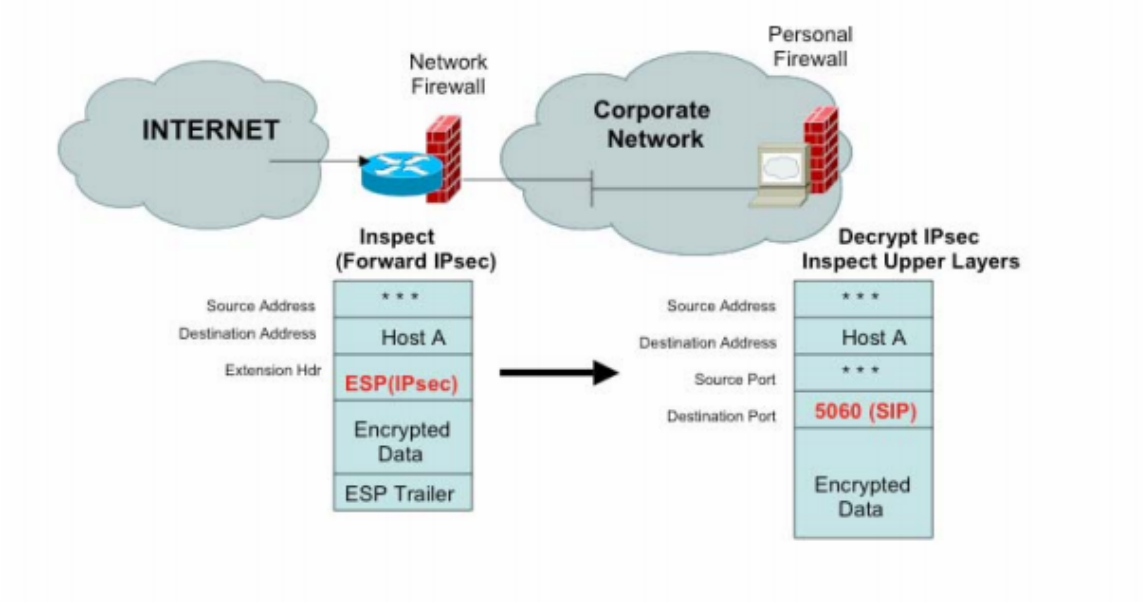

Figure 67 - Distributed firewalls

Router packet filters and stand-alone network firewalls will perform a first line screening to ensure that the packet is valid, arrives from a valid source host address and can be sent on to the destination host. At the destination, the host firewall will need to perform a more detailed packet inspection, usually incorporating some intelligent IPsec-aware function, especially if communications to the host are using encryption that prevents detailed screening at perimeter firewalls. In this case, the end-host would first decrypt the incoming packet, perform an inspection on the upper layer protocols, and if successful, send the packet on to the application process. Upon finding a security violation in the packet, a host firewall should reject the packet and report the violation to its security management system.

A distributed firewall can be used to augment a perimeter firewall or reduce the reliance on the perimeter firewall. Host-based firewalls may also be integrated into a single managed system with one or more perimeter firewalls to form a "hybrid distributed firewall" system for a managed defense in depth. A dual perimeter-firewall/distributed firewall system or a hybrid system augments the quality of perimeter defense as the internal firewalls bolster the enterprises ability to distribute, monitor, enforce IA policy and defeat attacks.

6.3.5.1.2 How IPsec Will Affect Distributed Firewall Architectures

IPsec, described in detail in the next section, is often misunderstood to be synonymous with encryption. On the contrary, IPsec does not always require that encryption be implemented or deployed to provide security services. IPsec can be used to provide the following security services:

- Data origin authentication and data integrity

• Data origin authentication, data integrity AND data confidentiality

Some security policies mandate that traffic has to be visible for signature based intrusion detection system observation or deep firewall inspection. Or sometimes the policy simply dictates that traffic has to be observable for some other reason. In those cases, end-to-end IPsec security will only provide authentication and integrity services as shown in Figure 68.

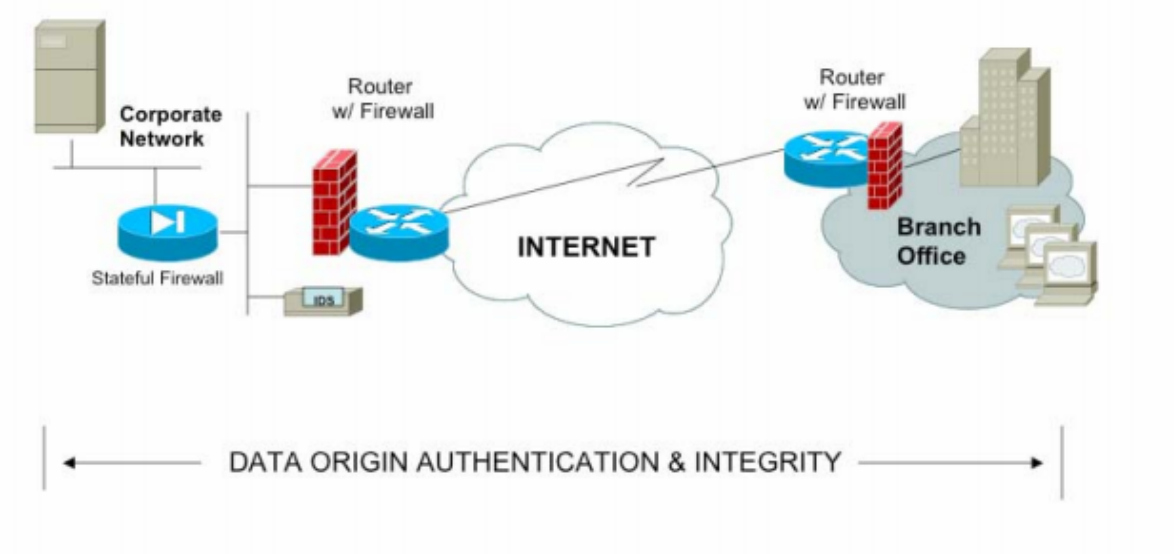

Figure 68 - End-to-End IPsec (Authentication & Integrity)

This scenario would ensure IPsec authentication and integrity protection for every data packet from the originating host to the data recipient while still keeping intact the policies which require deep packet inspection and traffic auditing via network IDS systems. If confidentiality is required but cannot impact current IDS and/or firewall filtering policies, then intermediary devices can add IPsec confidentiality protection and encrypt the traffic at allowable intermediary points.

In architectures where there is no encryption policy constraint or the policy is modified to incorporate a true end-to-end security model with confidentiality services allowed between communicating end-hosts, scenarios such as shown in Figure 69 can be deployed.

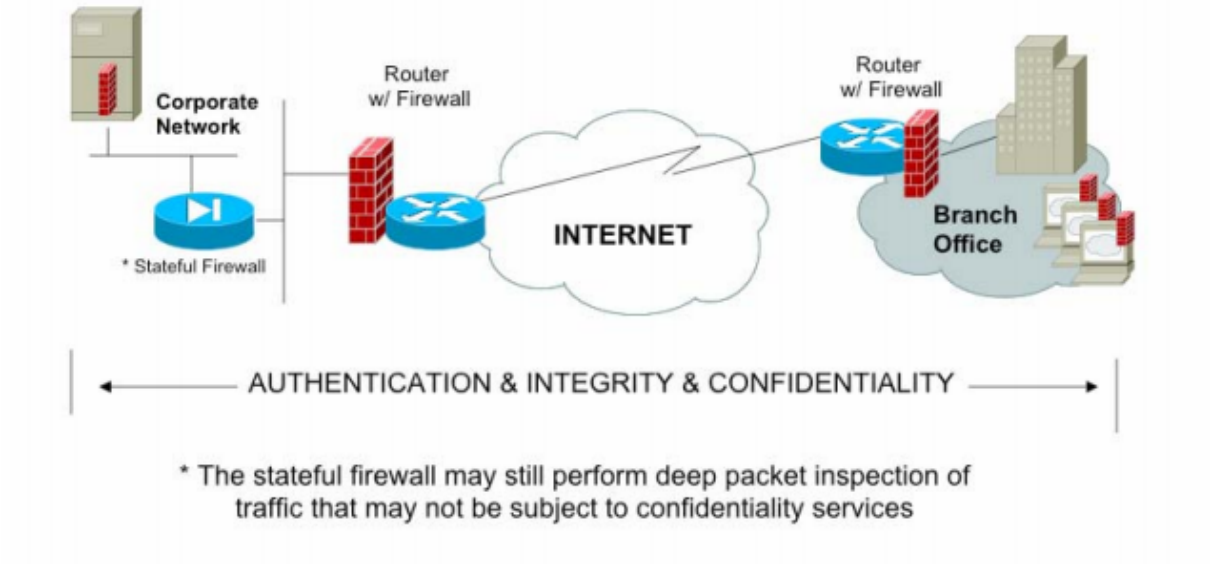

Figure 69 - End-To-End IPsec (Authentication, Integrity and Confidentiality)

Note that this scenario may still employ some network level packet inspection although it may be limited to simply IP address checking. The deployment of intelligent host-based firewall devices could be used to perform deep packet inspection at the host rather than using a network-based stateful firewall. Or, the two can be used in parallel with the deep packet inspection being performed for any traffic that does not require confidentiality services end-to-end.

A major consideration for future security policies is where to enforce confidentiality. It has often been the case that corporations do not allow for encrypted traffic across specific infrastructures due to regulatory requirements that must have the capability to have access to the data at any time.

However, if that requirement were met in some other manner, such as requiring a corporate-wide key escrow system, then perhaps the current policy of having date traverse the network unencrypted can be modified. These policy decisions will be dictated by whether it is easier for an environment to enforce more granular security at the host versus network infrastructure level. It is the flexibility of having that choice that creates the greatest advantage for future IPv6 networks. The end-to-end model can allow for more intelligent applications to take advantage of the flexible host-based security controls.

6.3.5.2 Evolving To Create A Flexible Security Architecture

As we get closer to more effectively utilizing an end-to-end security model, we will rely more heavily on distributed security with the communicating hosts providing the policy enforcement for their own communication. This has the advantage of creating specific policies for securing communications based on currently running applications rather than having a central enforcement point try and provide a single group-based policy. With distributed security it is possible to create more dynamic security policies which can vary over time based on changing trust relationships.

Distributed security endpoints consisting of host-resident firewalls, intrusion detection, security patching, and security status monitoring can be accomplished by kernel-mode processes within an operating system, These host-based security checkpoints would be managed by a central system used to distribute and monitor security policies and updates. A managed distributed host-based firewall system utilizing end-to-end IPsec can implement separate multi-level security policies with fine granularity. Using this end-to-end model it is possible to divide users and servers into various trust groups and interest communities to implement separate security rules. Applications and services that are used exclusively in one community may be blocked in other communities; this simplifies the screening rules (and exceptions) at a perimeter firewall and may prevent a breach in one network area from spilling into other network segments. If and when a breach occurs, containment of that breach is more easily managed. An additional benefit is that an, incorrectly implemented security policy in one area (or at the perimeter) does not necessarily compromise the entire system.

6.4 Evaluation criteria of the ISPs analysis

User information / Support

Question: Is there easily accessible, visible and clear information available on the IPv6 offerings and technical support?

Potential Answers:

- **No (0 point)**: No IPv6 information available on the ISP webpage and forums.
- **Forums/Blogs (2 points)**: Some/partial information available on forums, blogs or news item, but without a clear committed schedule on the IPv6 availability.
- **Full Info/Support (5 points)**: A clear IPv6 policy is presented, ideally on a dedicated page, with a deployment schedule and technical support for the already available offers.

Availability on Commercial Offers

Question: Is IPv6 available on all / some / none of the ISP commercial offers?

Potential Answers:

- **None (0 point)**: No IPv6 commercial offer available
- **Limited (2 points)**: IPv6 is available on some specific commercial offering
- **All but Mobile (5 points)**: IPv6 is available on all commercial offers except mobile internet commercial offers
- **All (10 points)**: IPv6 is available on all commercial offers.

Additional Cost

Question: Does switching to IPv6 involve an additional cost for the end user?

Potential Answers:

- **No IPv6 offer (0 point)**: No IPv6 offer.
- **Yes (1 point)**: Switching to IPv6 involves, in all or at least some case, additional cost in some way for the end user (specific offer, additional hardware...).
- **No (2 points)**: Switching to IPv6 does not involve any additional cost for the end-user.

Professional specific offering

Question: Does the ISP differentiate B2B and B2C users in his IPv6 policies?

Potential Answers:

- **No IPv6 offer (0 point)**: No IPv6 offer.
- **Distinct offers (1 point)**: The ISP offers different IPv6 policies and offers for IPv6 for B2B and B2C customers.
- **No distinctions (2 points)**: The ISP offers the same IPv6 policies for both B2B and B2C customers

Availability by default

Question: Is IPv6 available / deployed by default or on request?

Potential Answers:

- **No / on request (0 point)**: Switching to IPv6 is either not possible or involves a direct action by the end-user.
- **Default for New Users (5 points)**: New customers, of at least some commercial offers, have an IPv6 connection by default.
- **Migration complete (10 points)**: Legacy customers, on at least some commercial offers, have been migrated to IPv6.

Type of IPv6 connectivity

Question: What kind of IPv6 connectivity is available?

Potential Answers:

- **No IPv6 offer (0 point)**: No IPv6 offer.
- **Tunnel (1point)**: Any tunneling solution
- **Native (2 points)**: direct native IPv6 deployment