OECD ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Directorate for Science, Technology and Industry
Committee for Information, Computer and Communications Policy

Internet Address Space:

Economic Considerations in the Management of IPv4 and in the Deployment of IPv6

Ministerial Background Report
DSTI/ICCP(2007)20/FINAL

OECD Ministerial Meeting
on the Future of the Internet Economy

Seoul, Korea, 17-18 June 2008

Hosted by 방송통신위원회
KOREA COMMUNICATIONS COMMISSION

FOREWORD

The report provides an analysis of economic considerations associated with the transition from IPv4 to IPv6. It provides background analysis supporting the forthcoming ICCP-organised Ministerial-level meeting on “The Future of the Internet Economy”, to take place in Seoul, Korea on 17-18 June 2008.

This report was prepared by Ms. Karine Perset of the OECD’s Directorate for Science Technology and Industry. It was declassified by the ICCP Committee at its 54th Session on 5-7 March 2008. It is published under the responsibility of the Secretary-General of the OECD.

This paper has greatly benefited from the expert input of Geoff Huston from APNIC, David Conrad from the IANA, Patrick Grossetête from CISCO Systems, Bill Woodcock from Packet Clearing House, Marcelo Bagnulo Braun from the University of Madrid, Alain Durand from Comcast, and Vincent Bataille from Mulot Déclic, although interpretations, unless otherwise stated, are those of the author.

TABLE OF CONTENTS

MAIN POINTS

One of the major challenges for all stakeholders in thinking about the future of the Internet is its ability to scale to connect billions of people and devices. The objective of this report is to raise awareness among policy makers of capacity and limitations of the Internet Protocol version 4 (IPv4), to provide information on the status of readiness and deployment of the Internet Protocol version 6 (IPv6) and to demonstrate the need for all stakeholders, including governments, to play a part in IPv6 deployment.

The Internet has rapidly grown to become a fundamental infrastructure for economic and social activity around the world. The Internet Protocol (IP) specifies how communications take place between one device and another through an addressing system. The Internet technical community has successfully supported the Internet's growth by managing IPv4 Internet addresses through open and transparent policy frameworks, for all networks to have address space sufficient to meet their needs. It has also developed a new version of the Internet Protocol between 1993 and 1998, IPv6, to accommodate additional growth.

There is now an expectation among some experts that the currently used version of the Internet Protocol, IPv4, will run out of previously unallocated address space in 2010 or 2011, as only 16% of the total IPv4 address space remains unallocated in early 2008. The situation is critical for the future of the Internet economy because all new users connecting to the Internet, and all businesses that require IP addresses for their growth, will be affected by the change from the current status of ready availability of unallocated IPv4 addresses.

IPv6, on the other hand, vastly expands the available address space and can help to support the proliferation of broadband, of Internet-connected mobile phones and sensor networks, as well as the development of new types of services. Beyond additional address space, IPv6 adoption is being driven by public sector procurement mandates, by deployment of innovative products and services, by its better support for a mobile Internet, as well as by the decreased network complexity that it allows.

Today, the latest versions of new popular end systems (*e.g.* Microsoft Windows Vista/Server 2008, Apple Mac OS X, Linux, etc.) fully integrate IPv6, as do parts of the core of the Internet. However, progress in actual usage of IPv6 remains very slow to-date and considerable challenges must be overcome to achieve a successful transition. Immediate costs are associated with deployment of IPv6, whereas many benefits are longterm and depend on a critical mass of actors adopting it. A further major obstacle to IPv6 deployment is that it is not backwards compatible with IPv4: IPv6-only devices cannot communicate directly with IPv4-only devices. Instead, both protocols must be deployed, or sophisticated "tunnelling" and translation systems set-up. Experience to-date with IPv6 also suggests that IPv6 deployment requires planning and co-ordination over several years, that increased awareness of the issues is needed and that, as with all new technologies, finding skilled resources is challenging.

An intersection of economic, technical and public policy factors will determine the strategies adopted by various stakeholders who can pursue three broad paths: *i)* an even denser deployment of IPv4 Network Address Translation (NAT), whereby more devices are connected with fewer public IPv4 addresses by using private networks; *ii)* trying to obtain previously allocated but unused IPv4 addresses, and; *iii)* the deployment of IPv6. It is likely that all three of these options will be pursued by various actors in parallel, according to their business requirements. As an immediate solution, many are expected to pursue denser deployments of NAT. If Internet addressing groups were to liberalise address transfers, some actors would acquire previously allocated IPv4 addresses. Some actors will also implement IPv6. For policy makers, the most important point is that the first two strategies, which extend the life of IPv4, may be useful but are shortterm. The only sustainable solution to deliver expected economic and social opportunities for the future of the Internet economy is the deployment of IPv6.

In terms of public policy, IPv6 plays an important role in innovation and scalability of the Internet. In addition, security, interoperability and competition issues are involved with the depletion of IPv4. Transitioning to IPv6 represents a fundamental change in the Internet Protocol layer, which is necessary to foster an environment for long-term growth and competition across existing players and new entrants. In turn, such an environment is expected to enable the expanded use of the Internet and the development of new networking environments and services.

As the pool of unallocated IPv4 addresses dwindles and transition to IPv6 gathers momentum, all stakeholders should anticipate the impacts of the transition period and plan accordingly. With regard to the depletion of unallocated IPv4 address space, the most important message may be that there is no complete solution and that no option will meet all expectations. While the Internet technical community discusses optimal mechanisms to manage IPv4 address space exhaustion and IPv6 deployment and to manage routing table growth pre- and post-exhaustion, governments should encourage all stakeholders to support a smooth transition to IPv6.[1]

To create a policy environment conducive to the timely deployment of IPv6, governments should consider:

1) Working with the private sector and other stakeholders to increase education and awareness and reduce bottlenecks

IPv6 adoption is a multi-year, complex integration process that impacts all sectors of the economy. In addition, a long period of co-existence between IPv4 and IPv6 is projected during which maintaining operations and interoperability at the application level will be critical. The fact that each player is capable of addressing only part of the issue associated with the Internet-wide transition to IPv6 underscores the need for awareness raising and co-operation. Governments should aim to raise awareness and:

- Establish co-operation mechanisms for the development and implementation of high-level policy objectives to guide the transition to IPv6.

- Develop compelling and informative educational material to communicate and disseminate information on IPv6.

- Target decision-makers in awareness efforts and discussions on IPv6 deployment.

- Support registries and industry groups as they continue to develop policies and technologies to facilitate the management of IPv4 and adoption of IPv6, with a focus on:
  - Policies that safeguard security and stability.
  - Policies that give stakeholders ample opportunity to be ready and operate smoothly during the upcoming period of IPv4 unallocated address space depletion.
  - Ensuring that the deployment of IPv6 and the necessary co-existence of IPv4 and IPv6 safeguard competition, a level-playing field and are careful not to lock-in dominant positions.

- Make specific efforts to ease bottlenecks, by encouraging:
  - Operators to consider IPv6 connectivity in peering and transit agreements.
  - Greenfield deployments to contemplate IPv6 from the outset, to “future-proof” deployments.
  - Vendors and other providers of customer premises equipment to plan for and accommodate future customer needs in terms of IPv6, in recognition of consumer Internet access as the

largest current network-service growth area and the area placing the heaviest demand on IP address resources.

– Telecommunications operators to facilitate IPv6 deployment through training, equipment renewal, integrating IPv6 in hardware and software, developing new applications, conducting risk assessments.

– Software development companies to develop IP version neutral applications where possible, incorporate IPv6 capabilities into new software, and to conduct research and development on new applications that leverage IPv6 functionality.

2) Demonstrating government commitment to adoption of IPv6

As for all other stakeholders, governments need continued addresses to support growth in the public services that they provide online and more generally to meet public policy objectives associated with the continued growth of the Internet economy. They therefore have a strategic need to support transition to IPv6 by taking steps to:

- Adopt clear policy objectives that are endorsed at a high level, to guide the transition effort to IPv6.
- Plan for the adoption of IPv6 for governments' internal use and for public services, by developing a road map and planning time needed to conduct network assessment, infrastructure upgrade, and upgrade of applications, hosts, and servers.
- Set up a steering group to provide strategic guidance on achieving IPv6 implementation objectives.
- Ensure that all new programmes involving the Internet and ICT consider the relevancy of IPv6 and assess public programmes and priorities to determine how they can benefit from IPv6.
- Ensure that all relevant government security entities fully integrate the new dimension that IPv6 brings to security.
- Take pro-active initiatives to include IPv6 training efforts in life-long education cycles.

3) Pursuing international co-operation and monitoring IPv6 deployment

Awareness of the scope and scale of an issue is a key element in support of informed policy making. Benchmarking at the international level is essential to monitor the impact of various policies. With respect to IPv6, governments should:

- Engage in bilateral and multilateral co-operation at regional and global levels, to share knowledge and experience on developing policies, practices and models for coordination with private actors on IPv6 deployment.
- Consider the specific difficulties of some developing countries and assist them with capacity-building efforts to help build IPv6 infrastructure.
- Encourage the participation of all relevant stakeholders in the development of equitable public policies for IPv6 allocation.
- Encourage all relevant parties, including global and regional Internet registries, Internet exchange point operators and research organisations, to gather data to track the deployment of IPv6 in support of informed policy-making.
- Monitor IPv6 readiness, including by monitoring information on national peering points offering IPv6 connectivity, Internet Service Providers offering commercial IPv6 services, volumes of IPv6 transit, and penetration of IPv6-enabled devices in domestic markets.

INTRODUCTION

The Internet has been remarkably successful in scaling from a small community of users to a global network of networks serving more than a billion users. Over a short period it has also become a fundamental infrastructure for economies and societies around the world. Along the way, what was being interconnected expanded from one mainframe per university or company, to a one computer per person paradigm, to a multi-device environment, including greater use and all forms of access. In the future, vast numbers of objects may be connected to the Internet.

Growth in the use of the Internet has meant greater demand for Internet addresses. IP addresses combine "who", "where" and "how" roles in the Internet's architecture. Internet addresses uniquely identify devices on the network – or "endpoints" – enabling the identification of the parties to a communication transaction ("who" role).[2] In addition, addresses are used by the network to transfer data: they determine the network location of the identified endpoint ("where" role). [3] Addresses are also used to support routing decisions ("how" role). Therefore, IP addresses enable connection to the Internet, both through identification of the endpoints to a conversation and enabling the carriage of the data of the conversation through the network.[4]

Internet addressing is primarily a technical issue, but one that is influenced by economic and social factors. Increased IP infrastructure deployment, greater demand for Internet services throughout economies and societies translates into greater demand for IP addresses. Their continued and timely availability is, therefore, critical for the Internet to be able to meet the economic and social objectives all stakeholders have for this infrastructure, including in enabling public services continuity and evolution, for example, and safe guarding the continued growth of the Internet.

The Internet is currently reliant on IPv4 (Internet Protocol version 4) addresses. This is, however, a 25-year-old standard that is limited in its ability to meet future demand. The pool of unallocated IPv4 addresses available for new uses is rapidly being depleted. If current trends continue, projections expect the free pool of unallocated IPv4 address space will run out between 2010 and 2011.[5]

Foreseeing eventual depletion of IPv4 address space, as the Internet became increasingly successful, the Internet technical community took action to manage IPv4 addresses as a finite resource and plan for the future. In the 1990s, policies were introduced to tie new assignments of IP addresses to demonstrated need. A new scheme for addressing and routing, Classless Inter-Domain Routing (CIDR) was also introduced to solve the routing problem and enabled network operators to make more efficient use of address space. Moreover, a new technology called Network Address Translation (NAT) was introduced as a short-term "quick fix" solution, enabling one public address to be shared among several machines. The NAT, with its IPv4 address, provides a form of gateway to the global Internet.

Between 1993 and 1998, a new version of the Internet Protocol (IPv6) was developed to provide a vastly expanded address space for future use and transition mechanisms were planned. A decade later, abundance of IP addresses is still considered to be critical to enable business models of the future, such as widespread mobile Internet, machine-to-machine applications and other types of models based on ubiquity of the Internet.

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

The Internet’s adoption of a new addressing scheme represents a significant challenge for all stakeholders. At the time of the adoption of IPv4 there were less than 500 hosts connected to the Internet, a relatively small community of technical specialists was involved and the Internet was operating in a non-commercial environment. By 2008, over 500 *million* hosts were connected to the Internet and 1.32 billion users had Internet access.[6] The network of networks had become a fundamental infrastructure, around the world, for day-to-day economic and social activities.

Today, there is widespread agreement that the deployment of IPv6 is the best course forward, but also recognition that IPv4 will continue to be used for a long time to come. Between May and October 2007, all five regional Internet registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN), as well as national Internet registries (NIRs) made public statements emphasising the need for all those who need IP addresses to deploy IPv6 (Annex 9). Their statements recognise the critical importance of IPv6 to the future success of the Internet, urge companies to deploy it, and commit to actively promoting the adoption of IPv6 in their respective regions. Another important message of all these resolutions is renewed confidence in the Internet community and in the bottom-up, inclusive, stakeholder-driven processes in place to provide any needed policy changes.

For the successful implementation of IPv6, a transition is required which builds positive network effects or saves costs for Internet users. In other words, the use of IPv6 will increase in attractiveness for all users, as greater numbers of people use this protocol or as costs of continued deployment of IPv4 increase. The take-up in the use of IPv6 has been very slow to-date because of a lack of applications support, a lack of awareness, as well as a lack of clear benefits. Until there is market demand for the additional space and new functionality provided by IPv6, this will continue to be the case. In addition, unlike when IPv4 was initially adopted, the Internet now operates in a commercial environment, whereby a solid business case must be made to justify investment. Service providers have been understandably cautious about committing the required investment ahead of visible demand from their customers.

The nature of technology transitions is such that, prior to general adoption, there may be little or no initial incentive to shift to using a new technology. Once there is a critical mass of users, transitions often exhibit a “tipping point” at which adoption gains pace until it is widespread. In theory, a “tipping point” should occur when the marginal cost, for an Internet service provider, of implementing the next device on IPv4 becomes higher than the marginal cost of implementing the next device on IPv6. In other words, once the cost of deploying IPv4 infrastructure – determined by the cost of obtaining the addresses themselves and the cost of designing and operating networks that use fewer public addresses, by using NATs – become higher than deploying IPv6, a dynamic for IPv6 implementation should propel the industry through a dual-stack transitional phase to IPv6. The challenge lies in reaching this tipping point, which depends on a range of factors: customer demand, opportunity costs, emerging markets, the introduction of new services, incentives, regulation, as well as other factors.

The upcoming depletion of IPv4 unallocated addresses and the complexity of the transition to IPv6 has led to growing discussion in the Internet technical community about how best to manage the ongoing need for IPv4 addresses. Each of the initiatives undertaken to ensure that adequate address space is available is well founded, and raises a number of complex technical and economic issues, including some with public policy significance for the future of the Internet economy. The goal is to ensure the adoption and deployment of technically-sound solutions while maintaining the potential for new participants to access the full benefits of the global Internet.

Maintaining accurate records of address assignments is, for example, critical, for operational and security reasons. Additionally, from an economic growth perspective, IPv6 expertise is likely to be necessary to provide economies and companies with competitive advantage in the areas of technology products and services, and to benefit from ICT-enabled innovation.

Trying to achieve as much interoperability as possible between IPv4 and IPv6, for everyone to be able to continue to reach everyone else, is another priority. In the medium term, since operating dual IPv4 and IPv6 protocol stacks is required in most cases to underpin the Internet's evolution to IPv6, access to IPv4 addresses remains key for the development of new services for some time to come. A situation with anticipated scarcity of IPv4 addresses could raise competition concerns in terms of barriers to new entry and strengthening incumbent positions. Consequently, there is considerable discussion about how to manage previously allocated IPv4 space once the free pool of IPv4 addresses has been exhausted, including the ramifications of reclaim efforts and of authorised or unauthorised transfers of addresses between assignees.

A key challenge lies in ensuring that policies and practices that have been developed in the past to meet specific principles and goals such as stability, security, transparency, equity, and efficiency, are maintained or adapted to the new environment. As with any finite resource, the existence of scarcity has meant that economic issues are increasingly part of the discussion. The discussions underway are an endeavour to adapt existing policies and practices to a situation where, in the short to medium term, demand for IPv4 address space seems likely to exceed supply. A mechanism for transferring IPv4 addresses from one party to another already exists, for very specific circumstances (*e.g.* the sale of a company or a merger). For example, a modified transfer mechanism, sanctioned by the Internet community and adhering to its bottom-up consensus-driven policies and practices, could help to manage on-going demand. However, in allowing for more flexible transfers of IP address resources, safeguards to ensure adherence to long-held principles and objectives would need to be preserved or adapted to the new environment.

Technical issues are also very much to the fore in these discussions. For example, Network Address Translators (NATs), to share public IPv4 addresses between several devices, are in widespread use and are very popular with network operators. At the same time NATs are deemed to have limitations in the long term. Experts deem that NATs increase the complexity of Internet applications, therefore costs of operation, and impede some directions in innovation and the use of upper-level protocols and applications that depend upon the end-to-end functionality in the Internet. As the unallocated pool of IPv4 addresses runs out, NATs are predicted to become increasingly deployed. If this is done without simultaneously transitioning to IPv6, so as to build positive network effects, it could narrow future technical options as well as have economic and public policy implications. For example, application developers may have to build increasingly complex and costly central gateways to allow "NATed" clients to communicate with each other. This is deemed to present barriers to innovation, the development of new services and the overall performance of the Internet.

It is increasingly important that all stakeholders co-operate and make concerted efforts, based on their appropriate role and expertise, to enable the timely and smooth transition to IPv6, in most cases through a dual-stack period. All stakeholders have a role to play in the deployment of IPv6. The Internet's technical community has laid the foundation by developing the technical standards for IPv6. The technology is sufficiently mature to be introduced into production networks, although, to-date, this introduction has been on a small scale.

- The Internet technical community continues to play a critical role in evolving the IPv6 protocols and operations to meet “real-life requirements”in building awareness of the need for the transition and in helping to develop the skills base necessary for widespread deployment.
- The role of the broader Internet community’s bottom-up, consensus-based process for developing policies and practices needs to be underscored.
- The private sector, through its development of infrastructure and services, has led the development of Internet infrastructure and services from a small community of users, to a global network of networks. The implementation of IPv6 will entail continued private sector leadership.
- As large users of Internet services, governments can help to stimulate IPv6 products and services through their own procurement policies and use and through public-private partnerships in IPv6-related research and development. In terms of public policy, governments can also play a role in building the awareness of the necessity for a transition to begin in earnest.

A priority is to increase awareness of IPv6 and of its role for the future of the Internet. This can be done through public statements of support for IPv6 deployment to relevant constituencies, explaining the advantages of equipment and services that are IPv6 compliant, and highlighting the positive and negative experiences of businesses, governments and others that have implemented IPv6. A parallel priority is to increase IPv6 training and expertise, including in the area of security, since IPv6 networks introduce new opportunities and requirements compared to IPv4 networks. In addition, IPv6 deployment should be measured and progress in the roll-out monitored, by the parties best able to carry out that task.

All stakeholders should draw lessons from successes and barriers that have been identified in IPv6 implementations to-date. In general, these experiences highlight the importance of planning ahead. Planning ahead can drastically minimise costs by using natural technical refresh cycles. Experience also shows the need to adapt an organisation’s transition plan on a case-by-case basis and the need to ensure high-level decision-maker buy-in. Equipment vendors, in particular of customer premise equipment, should ensure their products are IPv6-enabled.

It is important to note that the premise of this report is that a widespread transition to IPv6 is the most likely and most desirable outcome for the future of the Internet. Experience shows, however, that the Internet will continue to change and evolve in ways that cannot be easily predicted. There are considerable challenges for the Internet community to make the transition to IPv6. In creating a dual-stack environment, IPv4 will likely be in widespread use for the next decade or more, irrespective of parallel IPv6 deployment. To make this work, NATs will have to be more extensively deployed. In turn, more NATs are likely to trigger the further development of applications and services for that environment (*e.g.* more services that use the client-server paradigm and workarounds such as in Skype).

If NAT deployments were to occur to the point where the Internet industry is both comfortable and capable of running an (IPv4) network with intense deployment of NATs, then the case for investment to support IPv6 deployment in parallel, possibly without additional customer demand, would be much more challenging. If momentum were to shift in this direction, with a demise of the "end-to-end argument", then addressing would become increasingly oriented toward mapping topology rather than to mapping identities (“who” role), with the consequence of less demand for expanded address space enabled by IPv6. In such a scenario, there would not be a global addressing scheme anymore, but increasing numbers of different types of addresses used in different scopes and domains. While the wide-scale deployment of NATs may seem the most cost-effective and near-term solution to defend against IPv4 address scarcity, it should be stressed that it is a deferral of the problem, not a sustainable solution.

The risk, in the absence of wide enough deployment of IPv6, is a partition of the Internet, whereby some regions would adopt IPv6 and others would run IPv4 with multiple layers of NAT. Such a division would impact the economic opportunities offered by the Internet with severe repercussions in terms of stifled creativity and deployment of generally accessible new services.

Scope of the report

The report reviews economic considerations associated with the transition from IPv4 to IPv6. It takes into account short to medium term considerations. The report does not aim to address all the issues surrounding the transition to IPv6, such as technical issues, even though they have economic effects.

The report notes but does not discuss long-term networking research initiatives such as the Global Environment for Networking Innovations (GENI) facility planned by the United States National Science Foundation (NSF) or the Future Internet Research and Experimentation (FIRE) initiative being undertaken by the European Commission. The paper does not address new forms of addressing and traffic routing.

The report does not discuss the impact of IPv6 on the Internet-wide routing system in any depth, although it recognises that addressing and routing on the Internet are interdependent and that there are significant economic considerations in devising solutions to scalable routing systems.

Structure of the report

- Section I provides an overview of the major initiatives that have taken place in Internet addressing to-date and the parallel development of institutions that manage Internet addressing.

- Section II briefly summarises proposals under consideration for the future management of IPv4 addresses.

- Section III provides an overview of the drivers and challenges for transitioning to IPv6 through a dual IPv4/IPv6 environment. It reviews factors that influence IPv6 adoption, drawing on available information.

- Section IV details economic and public policy considerations and recommendations to governments.

- Section V examines lessons learned from several IPv6 deployments.

I. AN OVERVIEW OF INTERNET ADDRESSING

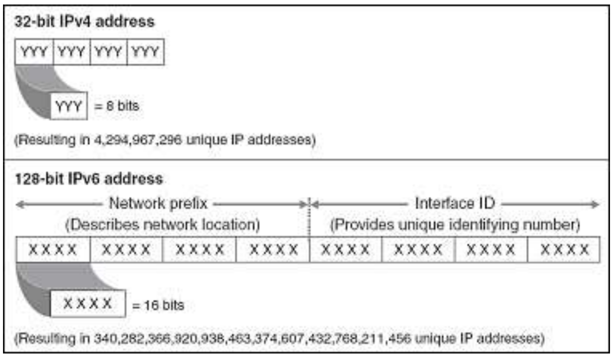
The Internet Protocol (IP) enables many different types of physical networks, such as cable TV systems, telephony systems, or wireless networks, to transport packets of data or “IP packets”. To do this, IP packets are “encapsulated” into whatever structure the underlying network uses. To connect different types of physical networks, routers “de-encapsulate” the incoming IP packets at the edge of a physical network and then re-encapsulate them to be able to forward them to the next physical network.

IP addresses play a fundamental role in the functioning of the Internet. They identify (“who” role) participating devices on the network of networks that comprises the Internet. All devices – including routers, computers, servers, printers, Internet fax machines, or IP phones – must have an IP address. IP addresses allow devices to communicate and transfer packets to each other: the Internet Protocol routes messages based on the destination IP address (“where” role). Network routers also use IP addresses to decide the way in which a packet will arrive to its destination (“how” role).

The IPv4 address space is a 32-bit address scheme, which creates an address space of theoretically 4 billion (2^{32}) possible unique addresses.[7] Since IPv4 addresses are of a fixed length, they are a finite resource and have been managed as such by the Internet community for more than a decade. Allocations of IPv4 addresses made prior to the formalisation of regional Internet address allocation bodies are known as “legacy assignments”. This class of allocation accounts for around one-third of all possible IPv4 addresses, or 1.6 billion addresses. Some portions of the IPv4 space have been reserved for special purposes such as private networks (~16 million addresses), multicast addresses (~270 million addresses) and addresses defined for “Future Use” (~270 million addresses).

IPv6, of which the core set of protocols were developed by the Internet Engineering Task Force from 1993 to 1998, has sometimes been called the Next Generation Internet Protocol or IPng. IPv6, or Internet Protocol version 6, provides a greatly expanded address range of 2^{128} possible addresses.[8] Its format, shown in Figure 1, allows for 340 billion, billion, billion, billion unique IPv6 addresses in theory.

Figure 1. Simplified Comparison of IPv4 and IPv6 Address Schemes



Source: United States Government Accountability Office (GAO).

The Internet enables communication between one IP address and another. IP addresses of a particular version can only intercommunicate directly or “natively” with IP addresses of the same version. That is, IPv4 cannot communicate directly with IPv6 and vice versa.

Routers examine the destination IP address on incoming data packets and send them on, ever-closer to the destination computer. To do this, each router must be regularly supplied with up-to-date routing tables that describe all valid destinations.[9] At the global level, individual IP addresses are combined together into prefixes. Prefixes represent a hierarchical, aggregated block of addresses for a network, for example /24.[10] The administrative entities that obtain, aggregate and announce these prefixes are autonomous systems (AS). Autonomous systems are groups of networks that operate under a single external routing policy. For example AT&T, Google, NTT and France Telecom each are an AS. Each AS has its own unique AS identifier number (for example 8228) and groups the individual prefixes that are allocated to that network.

Border Gateway Protocol (BGP) is the standard routing protocol used to exchange information about IP routing between autonomous systems. In general, each autonomous system uses BGP to announce (*i.e.*, advertise) the set of prefixes (*i.e.* aggregated IP addresses) to which it can deliver traffic. For example, the network 80.124.192.0/24 ("/24" being the prefix) being inside Autonomous System number 8228 (AS8228), means that AS8228 will announce to other providers that it can deliver any traffic destined for 80.124.192.0/24.

Overview of major initiatives in Internet addressing and routing to-date

Internet routing and addressing have been revised over the years to support the expansion in the global use of Internet, with over one billion Internet users connected in 2007 and increasingly pervasive IP‑based devices and infrastructure.

In 1972 Robert Kahn developed the concept of open-architecture networking, or "Internetting". His concept was that an open architecture would be able to connect multiple independent networks, each network itself having a different operating system and design. Such an open-architecture network required a new communication protocol which was designed in 1973-74 by Robert Kahn and Vinton Cerf and later called TCP/IP (Box 1).

Box 1. "I Survived the TCP/IP Transition"

In the early 1980s, the existing protocol (NCP) supported a very limited number of IP addresses. Such a limitation was a key motivating factor in the development of IP Version 4. The IPv4 address space is a 32-bit address scheme, providing for over 4 billion (2^{32}) possible unique addresses. The technology cutover date of all the hosts and equipment on the network was 1 January 1983 and, although less than 500 hosts made up the Internet, several years of planning and development were required in order to simultaneously convert all the machines and equipment on the network.

An excerpt from RFC801 by Jon Postel, detailing the conversion plan, reads "Because all hosts cannot be converted to TCP simultaneously, and some will implement only IP/TCP, it will be necessary to provide temporarily for communication between NCP-only hosts and TCP-only hosts. To do this certain hosts which implement both NCP and IP/TCP will be designated as relay hosts… Initially there will be many NCP-only hosts and a few TCP-only hosts, and the load on the relay hosts will be relatively light. As time goes by, and the conversion progresses, there will be more TCP capable hosts, and fewer NCP-only hosts, plus new TCP-only hosts. But, presumably most hosts that are now NCP-only will implement IP/TCP in addition to their NCP and become "dual protocol" hosts. So, while the load on the relay hosts will rise, it will not be a substantial portion of the total traffic."

Source: RFC801, ftp://ftp.isi.edu/in-notes/rfc801.txt.

The original IPv4 addressing structure was a two-level hierarchy, with 8 bits of the address identifying a host's network (network part), and the remaining 24 bits (host part), identifying the specific end system on that network, allowing for a total of 256 networks in total only.

In 1980, the addressing structure evolved from its original 8-bit/24-bit network/host part addressing to a "classful" addressing structure. The classful structure, which used the first four bits of the address to define the address "class", segmented addresses to provide three sizes of network address and allow more networks to be connected. Class "A", which mirrored the original address allocation model with 7-bit network/24-bit host, and Class "B", which provided for 14 bits of network and 16 bits of host, address spaces were very large, while class "C" (providing 21 bits of network and only 8 bits of host) was small for most networks. Class B address space, albeit too large for most networks, experienced high demand and led to the initial concerns about IPv4 address space depletion.

By the early 1990s, it was apparent that the growth in number of users along with emerging applications such as multimedia and broadband services, would put a severe strain on the capabilities of the Internet, and that its underlying protocols, in particular IPv4, would require an update.

The Internet Engineering Task Force (IETF) took on the task of finding several short-term solutions *e.g.* by introducing the "Classless" address architecture in 1993, also known as Classless Interdomain Routing (CIDR), to more efficiently use the remaining IPv4 space.[11] In the classless addressing scheme, a block of address space can have many different sizes, depending on a network's need. As an example, a small network in need of 16 addresses could obtain a /28 (pronounced "slash 28"). Addresses came to be talked about as "/n", with n indicating the number of bits that were "pre-set". For example, in a "/28", the first 28 bits of the address range are "set", while all possible variation of the last 4 bits enables the network to use 2^4 *i.e.* 16 addresses.

A new routing protocol, BGP-4, implemented support for Classless Inter-Domain Routing (or CIDR) and introduced route aggregation to decrease the size of the routing table.[12] While CIDR had to be implemented in all the routers and hosts on the Internet involved in making routing decisions, the changes needed were software-based and were backwards compatible. Therefore, the transition was fairly smooth.

Network Address Translation (NAT, RFC 2663) was devised in 1994 as another short-term solution to the lack of IPv4 address space. NAT functionality can be built into a device such as a router that sits between an upstream provider (an ISP and the public Internet) and a local network. NAT, as the name implies, translates the address used on the local network into an address used on the public network. Connection through a NAT allows a small number of public addresses to be "shared" across a much larger number of hosts using private, *i.e.* not globally unique, addresses, thereby allowing an entire group of computers and other connected devices to connect to the Internet via the NAT. As such, most devices behind NAT devices become "clients", as opposed to both clients and servers in the "end-to-end" model that characterised the early Internet (Box 2).[13]

Box 2. The "End-To-End Argument"

The Internet's original design is based on what is known as the "end-to-end argument" where the intelligence and processing power of a network reside at the outer edges while the inner network itself remains as simple as possible. The model proposed is a way to maximise the efficiency and minimise the cost of the network. The end-to-end argument explaining the relationship between the network and its end points has arguably been one of the key elements of the Internet's success. Its origins lie in a seminal paper in 1981 by Jerome Saltzer, David Reed, and David Clark.[14]

NATs are pervasive in the Internet ecosystem and are a low direct cost solution to IPv4 address space limitations. Benefits of NATs include perceived security (since by default all incoming connections are filtered), increased flexibility in changing service providers, and low usage of public IP addresses.[15]

However, NAT modifies the packet's header before it reaches its destination and thus requires intelligence and processing power within the network rather than only at the end points. Problems often associated with NATs include increasing the complexity of networks, creating asymmetry between clients and servers, complicating the provision of public services within a local network and interfering with peer-to-peer applications.[16] For example, if a computer's address is behind a NAT, it can be difficult to initiate a conversation with that computer because there is no simple way to know which computer to send the message to. Some have pointed out a primary reason NATs introduce complexity is the lack of standards to specify their "behaviour" in different scenarios. For example, standards to specify how NATs deal with peer-to-peer applications such as voice-over-IP, have not been devised. As a result, NAT implementations vary widely. Unable to predict how specific NATs will react, application designers have had to devise complex "work-arounds".[17]

As a long-term solution to the depletion of IPv4 address space, the IETF chartered a new working group named Internet Protocol – Next Generation, or IPng. In December 1993, the IETF issued a Request for Comments (RFC 1550), entitled "IP: Next Generation (IPng) White Paper Solicitation". Interested parties were invited to submit comments on specific requirements for IPng, and on factors that should be considered during the IPng selection process. The responses were grouped into a document "the Technical Criteria for Choosing IP, the Next Generation (IPng)".[18] Seventeen criteria for the new protocol were specified, including scalability, a straightforward transition plan, media independence, easy and largely distributed configuration and operation with automatic configuration of hosts and routers, multicast, network service and mobility.

In January 1995, "The Recommendation for the IP Next Generation Protocol" was published.[19] The document specified the key features of IPng, including larger addresses, enhanced routing capabilities, authentication and encryption to strengthen security, quality of service functions, and more. It also gave the IPng protocol a new name, IPv6.[20] The suite of IPv6 protocols were finalised by the IETF in 1998.[21]

Characteristics of IPv6 include, first and foremost, a widely-expanded address space. As more devices (like handheld devices, and integrated IP appliances and utilities) come to use the Internet, they require unique addresses to work optimally. Section III. Drivers and challenges of IPv6 deployment, provides further information on the characteristics of IPv6 and its adoption by businesses to-date.

The address distribution and registry function

Accompanying the evolution of the Internet, institutions were created to manage Internet resources and adapt Internet resource policies as needed. To ensure that no two networks would use the same network address in the Internet, Jon Postel, at the Information Sciences Institute (ISI) of the University of Southern California (USC), managed, until 1998, the allocation of blocks of IP addresses to networks. He also managed the allocations of blocks of IP addresses to Regional Internet Registries (RIRs), when these were formed to serve geographical regions of continental scope. The first regional Internet registry was created in 1989 for Europe and named RIPE NCC (Réseaux IP Européens-Network Coordination Centre). The APNIC (Asia Pacific Network Information Centre) was created for the Asia-Pacific region in 1993. The ARIN (American Registry for Internet Numbers) was created in 1997 for the United States, Canada and a portion of the Caribbean. The LACNIC (Latin America and Caribbean Network Information Centre) for Latin America and the Caribbean (2002). In 2005, AfriNIC became the RIR for the African region.

Allocating IP addresses to RIRs came to be known as one of the Internet Assigned Numbers Authority (IANA) functions, which ICANN has performed since 1998.[22] ICANN's Address Supporting Organisation (ASO) is the formal entity through which RIRs agree on global address policies, *i.e.* policies that require the involvement of ICANN, IANA, and all the RIRs for implementation. An Address Council was created in 1999 to communicate proposed global policies to ICANN's Board for ratification.

The Internet community uses an administrative approach to resource allocation, whereby address blocks are allocated based on demonstrated needs for addresses. IANA allocates blocks of IPv4 and IPv6 address space, and Autonomous System (AS) numbers to each RIR to meet the needs of their region.[23] The criteria, as currently agreed between the IANA and the RIRs, stipulate that IANA allocates /8 IPv4 blocks and /12 IPv6 address blocks. RIRs, in turn, allocate IP addresses to Local Internet Registries (LIRs), or to national Internet Registries (NIRs) in those countries that have them, based on demonstration of need.[24]

LIRs either "assign" address space to end-users or "allocate" address space to ISPs who, in turn, assign IP addresses to enterprises and end-users, in a manner that is consistent with regional address policies. [25]

The RIRs are membership-based organisations through which policies for address distribution are developed in an open, bottom-up and transparent manner by regional policy forums. The three primary goals of the RIR system are: *i) conservation*, to ensure efficient use of a finite resource and to avoid service instabilities due to market distortions; *ii) aggregation* (routeability), to assist in maintenance of Internet routing tables of a manageable size; and *iii) registration*, to provide a public registry documenting address space allocations and assignments, to ensure uniqueness and provide information for Internet troubleshooting. Each RIR is responsible for maintaining documentation on the allocation and use of IP space within its region and for maintaining a public database (the IP Whois) of unique allocations of these number resources, including IP space, AS number, organisation name and points of contact.[26] Importantly, addresses are not considered as property and cannot be bought or sold.

Aggregation, minimum allocations and routeability

RIRs apply a minimum size for allocations, which facilitates prefix length-based filtering for routing purposes. Furthermore, as a result of differing network sizes and different needs, prefix lengths vary by region. In general, RIRs allocate IPv4 address prefixes to Local Internet Registries (LIRs) no longer than /22 for AfriNIC and /20 for ARIN (Annex 5). In ARIN's case, if smaller allocations are needed, LIRs are expected to request address space from their upstream provider. For "provider independent" or "multi-homed" users, *i.e.* users with redundant interconnection and traffic exchange with two or more independent networks, ARIN allocates IP address prefixes no longer than /22.

In the case of IPv6, the minimum allocation size for IPv6 address space to LIRs is /32 for all five RIRs. LIRs are able to allocate IPv6 address blocks to end sites with a size between a /64 (a single subnet within the end site) and a /48 (up to 65 536 routed subnets within the end site). The choice of the allocation policies to sites within these bounds is a matter for the LIR to determine.

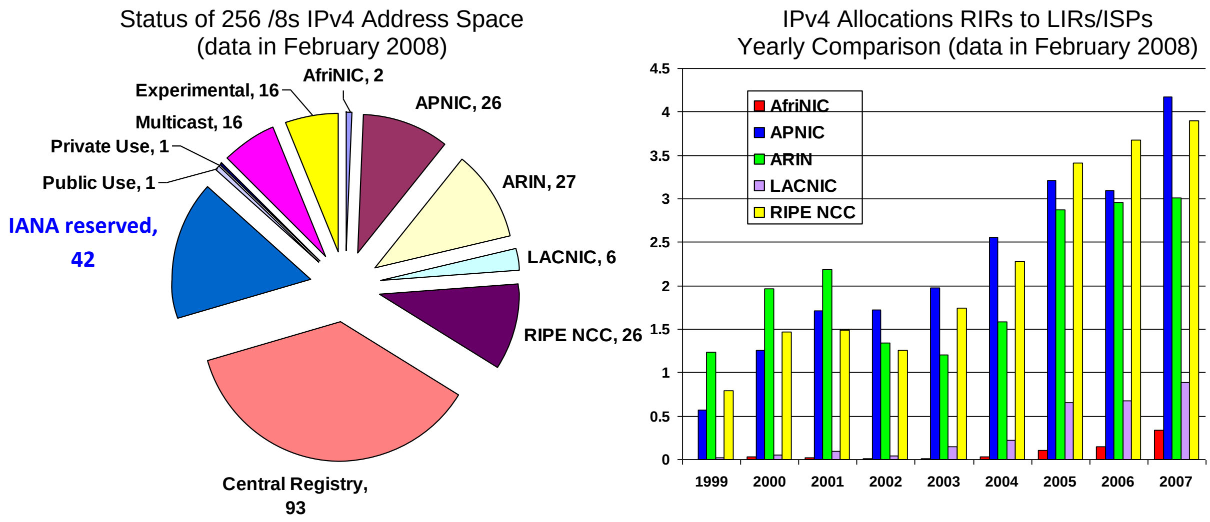
An important notion that is closely related to allocation sizes is that of address routeability. An address, as a host locator ("where"), must, for it to be useful, be recognised in routing announcements.[27] Routing announcements have to be accepted and propagated through the routing system. Yet while the practice of filtering the routes accepted from peers according to prefix length (prefix length filters) is not yet commonly applied, filtering out longer prefixes could become more commonplace to help manage increasing numbers of announcements in global routing tables.

IPv4 address depletion forecasts

Some experts project that the depletion of unallocated IPv4 address space will occur in the next two to three years, unless another method is found to extend the life of the IPv4 address space. They project that, if current allocation rates prevail, IANA will exhaust all available IPv4 space in the IANA pool by 2010 and that the RIRs will run out of large unallocated contiguous blocks of IPv4 addresses to allocate in 2011 (Figure 3). The most authoritative sources are Geoff Huston's "IPv4 Address Space Report"[28] and Tony Hain's "A Pragmatic Report on IPv4 Address Space Consumption".[29] Depending on the models used, their projections for depletion vary by a few months. There is widening awareness within the Internet community and among network operators of the upcoming depletion. There is also significant discussion of potential ways to encourage an orderly transition to an IPv6-based Internet connectivity model.

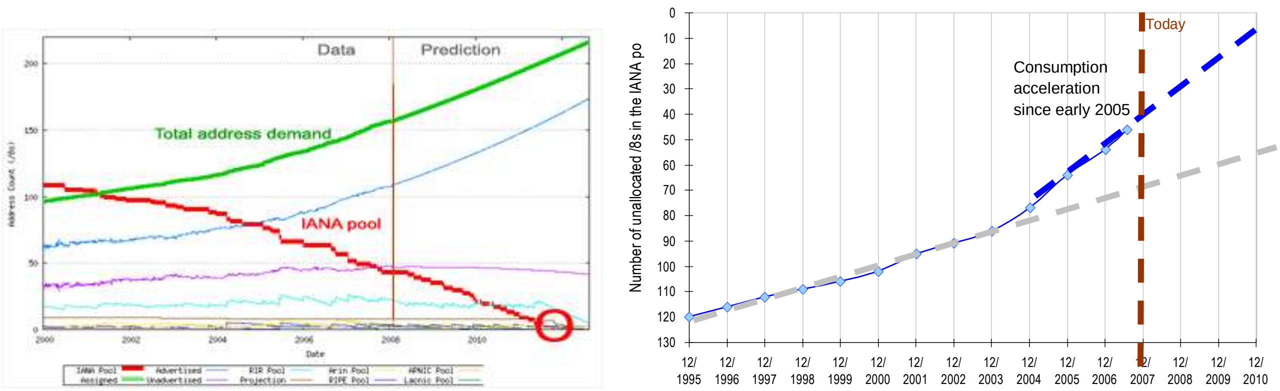
It is important to note that estimates of a depletion date assume no major technology change, policy change or "land rush" effect. However, many new policies are being proposed and a "land rush" can be expected as actors become increasingly aware of the situation. Figure 2 (left) shows the distribution of IPv4 address space in February 2008, as well as trends in growth of demand (right).

Figure 2. Distribution of IPv4 /8 allocations



Note (left): Central Registry concerns the allocations that were made before the RIR system was introduced.
Source: Number Resource Organization, January 2008.

Figure 3. Projected RIR and IANA consumption (/8s)



Source: IPv4 Address Report, Geoff Huston, 2/2/2008.

Source: Based on Telecommunications Bureau, Ministry of Internal Affairs and Communication, December 2007, Japan.

IPv6 characteristics

The IPv6 standard, established between 1993 and 1998, is a newer version of the Internet protocol. There are sound reasons for implementing IPv6. IPv6, first and foremost, offers a widely expanded address space, *i.e.* much greater volume. Experts deem that IPv6 provides other features and capabilities, including simplified assignment of addresses and configuration options for communications devices as well as more flexible addressing and Secure Neighbor Discovery. Some experts attribute additional benefits to IPv6, although many have been ported to IPv4 or are contingent on the removal of NATs, which are deeply embedded into the existing infrastructure. Such potential benefits could include more robust security at the transportation level, support of peer-to-peer applications, and better mobility support.

Dual-stack means running both IPv4 and IPv6, which enables communication with both IPv4 and IPv6 nodes.[30] Tunneling is the packaging of IPv6 data through encapsulation or address assignment so it can travel across an IPv4 network, or, less often, the packaging of IPv4 data to travel across an IPv4 network. Translation enables IPv6-only devices to communicate with IPv4-only devices through an intermediate device (*e.g.* an application layer gateway or proxy).

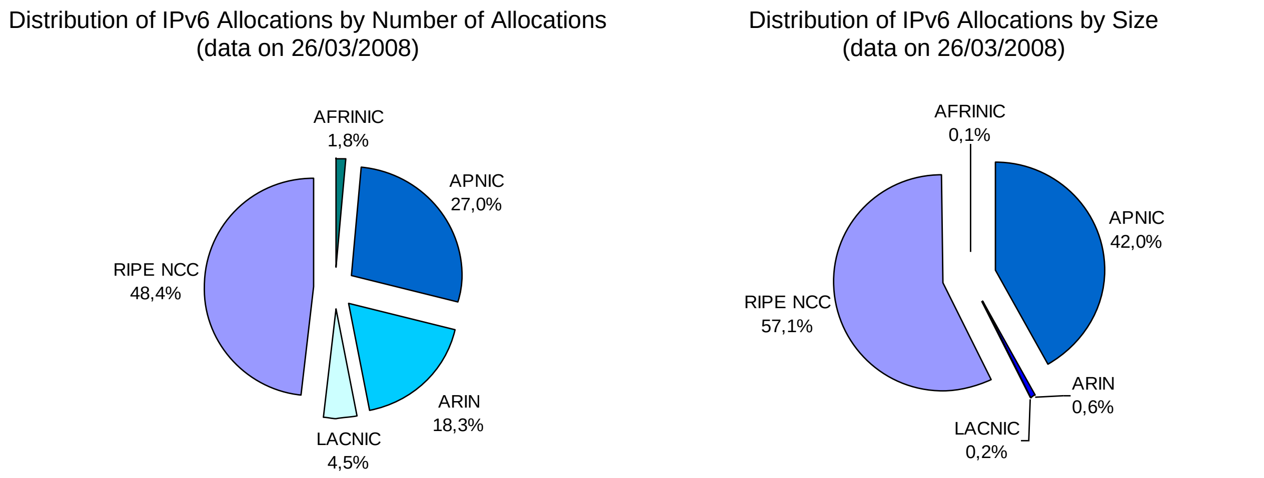
Current status of IPv6 deployment

This section examines the current status of IPv6, with respect to roll-out, technology and applications. It shows that, while support for dual-stack IPv4/IPv6 is implemented in much - but not all - available hardware and software, IPv6 is not currently used and interconnectedness is lacking. Many network operators are not rolling-out IPv6 due to insufficient demand or cost-incentive, or are just beginning to realise the need to transition to IPv6.

IPv6 address allocations

Going through the RIR's processes to obtain an IPv6 allocation is the first step in adopting IPv6. IPv6 addresses can and are being obtained and routed.[31] The number of allocated prefixes provides an indication of the number of organisations interested in implementing the IPv6 protocol (Figure 4, left). Meanwhile, the size of the allocations (Figure 4, right) is difficult to use at an aggregate level because extremely large allocations were made to some operators. The statistics shown in Figure 4 indicate that the European and Asian markets have started, or are close to starting, large-scale deployments of IPv6, while North America, Latin America and the Caribbean, and Africa, have been comparatively more interested in evaluating IPv6.

Figure 4. Distribution of IPv6 allocations by the RIRs



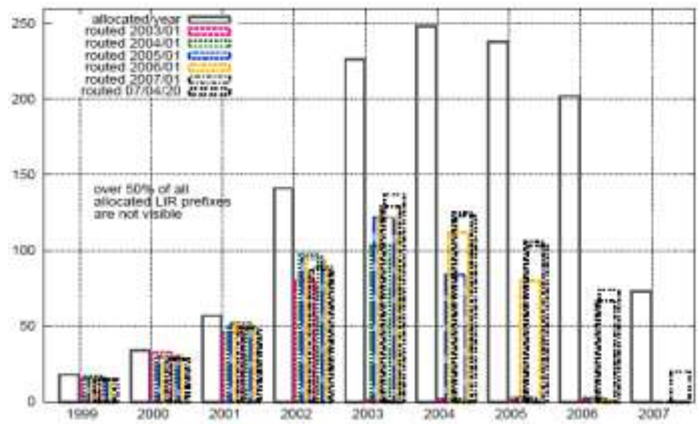
Source: http://www.ripe.net/rs/ipv6/stats/.

Routing table announcements show where IPv6 addresses are actually being used. Once an organisation has been assigned addresses (Figure 5), for these addresses to be "visible" on the Internet, routes to the address blocks used must be published in the routing tables (Figure 5, left). Germany, France, Japan, the European Union and Korea appear comparative leaders in actual use of IPv6. About 50% of all allocated IPv6 LIR prefixes are visible in the IPv6 routing table (Figure 5, right).[32] It should be pointed out, however, that volumes of IPv6 activity are extremely low: there are less than 1 000 prefixes announced in the IPv6 routing table, compared to 250 000 in the IPv4 routing table.[33] There have so far been less than 100 new IPv6 Internet routes introduced each year since its first introduction.[34] Year-on-year growth has so far been negligible.

Figure 5. Distribution of IPv6 allocations and allocated versus routed

Top 15 Countries in Terms of IPv6 Allocations

Allocated Versus Routed



Source: Have We Reached 1000 Prefixes Yet? A snapshot of the global IPv6 routing table.[35]

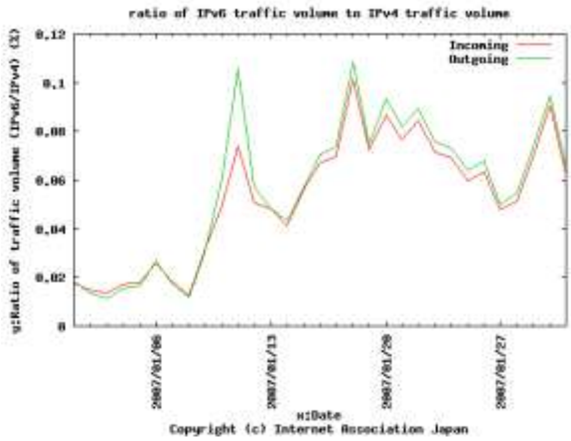
Source: OECD, 2008 (data on 26/03/2008).

Japan already has several major commercial IPv6 networks. Assignment registration information in the IP Whois database shows that the most common sizes registered are /40s and /48s. The most common prefix sizes announced are /32 and /48. IPv6 is generally assigned to end sites in fixed amounts (/48). Therefore, the number of /48 prefixes in the IP Whois databases provides an indication of the utilization of IPv6 address space by operators, since these IPv6 addresses have been assigned to end-users. This measure indicates that Japan leads in terms of actual use of IPv6 allocations, by several orders of magnitude (Figure 6, left).

Figure 6. Scale of assigned IPv6 addresses to end-users

Number of Allocated /48 Prefixes in the IP Whois Database Per Country

The Ratio of IPv6 Traffic Volume to IPv4 Traffic Volume



Source: Internet Association Japan, April 2008.[36]

IPv6/IPv4 traffic ratio

The level of IPv6 traffic is extremely low compared to IPv4 traffic. IPv6/IPv4 traffic ratio at Internet Exchanges, such as the Amsterdam Internet eXchange (AMS-IX), is at less than 0.1%. Traffic measured in Japan is similar (Figure 6, right). Early research conducted by Packet Clearing House (PCH) shows that at least 17% of Internet eXchange Points (IXPs) support IPv6 explicitly.[37] There are some indications that IPv6 traffic may actually be more significant, because much IPv6 traffic is encapsulated into IPv4 packets with a transition tunnelling scheme to be transported over an IPv4 infrastructure.[38]

There is a misconception that no global IPv6 traffic means that there is no use of IPv6. As mentioned above, current measurements may not account for "transition" IPv6 traffic which is not native IPv6 traffic, but instead is "tunneled" inside IPv4.[39] In addition, there are indications that many organisations are using IPv6 within internal networks for specific applications or to familiarise themselves with the new protocol. For example, NTT estimates that IPv6 traffic inside its network is very significant because its video-on-demand and video streaming traffic use IPv6 multicast. In another example, Comcast uses IPv6 to manage its cable modems: while the volume of IPv6 traffic is very low, this traffic is extremely important to the company.

Hardware and software

A pre-requisite to implementation of IPv6 is the availability of supporting operating systems, *i.e.* Windows Server 2008, Windows Vista or MacOS X, on top of which application and services can then be built. Many experts view widespread adoption of operating systems which support IPv6 by default, as a determining factor with the potential to trigger the deployment of IPv6 in earnest.

Most mainstream hardware and software vendors support IPv6 in their products. The level of IPv6 support in computer and device operating systems is a direct proxy for the number of computers and devices that could potentially use the new protocol as soon as IPv6 connectivity is available. All significant operating systems, DNS servers, programming languages, and routers now support IPv6 (*e.g.* BIND DNS, PowerDNS, djbdns, Linux Mobile support IPv6, Java 1.4, etc.). Most recent operating systems releases, such as Apple Mac OS X 10.x, Linux 2.6, Microsoft Windows Vista or Microsoft Windows Server 2008, have IPv6 set by default. In particular, Microsoft's Windows Vista includes a tunnelling system whereby IPv6 is enabled by default and Apple's Mac OS X has had IPv6 enabled "out of the box" for some time. These two platforms represented respectively 100 million and 30 million licences by early 2008 out of a total of 1.3 billion Internet users, *i.e.* some 10%.[40] Almost all Unix/Linux platforms and new smart phone operating systems are IPv6-ready.[41]

The major equipment vendors, including 3Com, Alcatel, Cisco Systems, Hewlett Packard, Hitachi, Juniper, Nokia, Nortel Networks, Novell, Siemens, or Sun Microsystems, all support IPv6. Several high-use public domain applications, such as Mozilla Firefox, support IPv6. The conversion of commercial applications has begun, *e.g.* with IBM Websphere Application Server 6.

Experts point out, however, that IPv6 support is not universal. For SOHO and home users, and Internet service providers, an important barrier to IPv6 uptake is the lack of suitable customer premises (CPE) devices, a market that is highly commoditised. A survey of IPv6 support in commercially available firewall equipment, noted that the level of support for static packet filtering, stateful inspection, and application layer inspection, stood at between 30% and 60% of products on the market.[42] In addition, all IPv6 implementations face the challenge of in-house software, which may need to be upgraded, adapted or replaced.[43] Lack of IPv6 support in network management applications is reported as being an issue, as in other enterprise applications that can be used via the Internet or an intranet.

Domain Name System

The inclusion of IPv6 support at all levels of the Domain Name System (DNS) is important to IPv6 adoption because it allows IPv6-enabled hosts to reach other IPv6 hosts. Most Internet applications regularly query the DNS. The DNS is a distributed registry system that "resolves" (*i.e.* translates) user-friendly host names (for example www.oecd.org) into a numeric Internet Protocol (IP) address, to locate content or applications on the Internet. Hierarchical DNS names are supported by the "dot" in the name, and structured from right to left. The data in the DNS is stored in widely distributed sets of machines known as "name servers", which are queried by "resolvers". Invisible to users, the top of the hierarchy is the "root", and the root servers that mirror this root.

The DNS uses a simple client-server model to perform a mapping between hostnames like www.oecd.org and IP addresses such as 193.51.65.71. Devices on the Internet are usually configured to send DNS queries to a resolving name server on the local network. This is typically done when the device's operating system is configured. The local resolving name server is generally configured with the addresses of the Internet's root name servers. When the local DNS server receives a query from a client (*e.g.* a web browser), it follows a chain of delegations from the root of the DNS in order to resolve the query. So for a lookup of www.oecd.org, the local resolver will first consult one of the root name servers. It will refer the resolving name server to the name servers for .org.[44] One of the .org name servers will return details of the name servers for oecd.org. When one of these is consulted, it returns the IP address of www.oecd.org to the resolving name server which then passes that answer to the clients that originally made that query. [45]

On 4 February 2008, IANA added IPv6 (AAAA) records in the "hints" file to provide the IPv6 addresses of four root servers whose operators requested this, thereby removing an important roadblock to IPv6-only Internet access. The move means that IPv6-only devices may now be able to communicate on the Internet. Back in July 2004, ICANN had added IPv6 support in the "root", to include IPv6 addresses for .KR, .JP and .FR zones. [46] Some 9% of the servers in the Internet DNS root zone are dual-stacked (84 IPv6-enabled servers in the DNS root zone compared to 1 000 IPv4-enabled DNS servers in the root zone).[47] Meanwhile, about half of the top-level (TLD) domain name servers are IPv4 and IPv6 capable. In terms of generic top-level domains (gTLDs), .com and .net for example are IPv6-enabled. About a third of country code top-level domain (ccTLD) registries (76 out of 245[48]) are IPv6-enabled. And the Measurement Factory found that in 2006 about 0.2% of the second-level zones in COM and NET were using IPv6 addresses for their name servers.[49]

II. MANAGING THE IPV4 DEPLETION

The regional Internet registries (RIRs) are considering a number of policy proposals and initiatives to manage the remaining unallocated pool of IPv4 address space and existing IPv4 assignments, and to encourage the adoption of IPv6. Policies are being prepared for the period until the depletion of previously unallocated IPv4 address space and for the post-depletion period, when all IPv4 addresses will have been allocated. The uppermost concern in these discussions is the likely continuing demand for IPv4 – fuelled by continued Internet growth and transitioning to dual-stack – even as deployment of IPv6 takes place.

The following provides a snapshot of evolving proposals and discussions (broadly summarised in Tables 2, 3 and 4). Interested parties are invited to continually check with the relevant organisations – in particular, the regional Internet registries and IANA – for the latest address distribution policies and status of discussions (Table 1). Scenarios being discussed include:

1. **Attempts to better allocate the remaining IPv4 address space**:

   – No modifications and a “wait and see” or “brick wall” approach.

   – “Reserving” one “/8” block per region, for fairness reasons and to enable some regions to save IPv4 address space to ensure, for example, dual-stack for critical information infrastructure.

   – Introducing policies to ensure that all RIRs run out at the same time so as to avoid regional distortions.

   – Rationing IPv4 space by making requirements increasingly difficult while encouraging IPv6 deployment.

2. **Attempts to better re-use allocated address space**:

   – No modifications and the possible emergence of a black or grey market for IPv4 addresses.

   – Re-using address space that was previously reserved for other purposes.

   – Reclaiming address space that is not being used.

   – Transferring IPv4 resources: discussions focus on whether to maintain a needs-based approach or, at the other extreme, to let an open market manage supply and demand.

Table 1. RIR policies for IPv4 and IPv6 address allocations and assignments

	IANA	ARIN	RIPE NCC	APNIC	LACNIC	AFRINIC
URLs	www.iana.net	www.arin.net	www.ripe.net	www.apnic.net	www.lacnic.net	www.afrinic.net

Source: RIR websites and Number Resource Organisation website.

Table 2. A sample of current policy proposals that pertain to the distribution of the remaining IPv4 address blocks

DISTRIBUTION OF THE REMAINING IPv4 ADDRESS BLOCKS			
PROPOSAL	**DESCRIPTION**	**ARGUMENTS FOR PROPOSAL**	**ARGUMENTS AGAINST PROPOSAL**
Allocation of remaining unallocated pool of IPv4[50]	Advocates an equal distribution of the remaining /8s to each RIR, once the pool reaches the threshold of 5 /8s. The proposal takes the position that each RIR community should then be able define its regional policy on how to distribute this final pool of addresses. This "global proposal" was discussed at the LACNIC X meeting in May 2007, in the APNIC 24 meeting in New Delhi in September, and in ARIN and RIPE meetings in October 2007.	Partial correction for a situation in which lower historical use of IPv4 addresses means that LACNIC and AfriNIC will have only few IPv4 addresses to go through the transition with. Reduce IANA's need to assess the relative merit of potentially competing requests. Each RIR community would define policies to allocate the final block that best match their regional situation, taking into account the relative development of IPv4 and IPv6 in their region. RIRs/NIRs, depending on the situation of their region or country, may reserve some addresses for specific constituencies in the Internet supply chain, whose "connection using dual-stack" is deemed important. For example, some RIRs might wish to create safeguards for services they consider to be "critical infrastructure".	Regional distortions because some parts of the world would reach depletion of IPv4 addresses sooner than others. LIRs could become members of different RIRs ("RIR shopping") because of remaining IPv4 resources in some regions. "Set-asides" could invite intervention by regulators. "Set-asides" may require qualitative assessments by RIRs which may in turn invite litigation.
Cooperative distribution[51]	Would establish a process for RIR-to-RIR redistribution of the tail-end of the IPv4 pool, taking effect after the IANA Reserve is exhausted.	The five RIRs would run out of IPv4 address space at approximately the same time.	No margin for safeguards by RIRs.
Rationing IPv4 address space[52]	Would institute a set of IPv4 Address Allocation "phases" that would make address allocation requirements progressively more stringent, using the amount of address space remaining unallocated by IANA as a metric. Aims to provide a smooth transition by encouraging the deployment of IPv6. Aims to encourage more efficient use of IPv4 address space through progressive supply rationing. Also introduces new requirements for requesters, such as documentation of non-private IPv4 address space used for internal infrastructure or documentation of IPv6 plans for offering connectivity and services.	At aggregate levels, documentation could provide insight on plans of LIRs in their region, drivers and barriers to adoption of IPv6, and other economic considerations. Comparable data across regions would be valuable to allow for benchmarking and measurement of progress in the adoption of IPv6. Progressively raising the requirements to obtain IPv4 space may both decrease IPv4 demand, through conservation and increased address space efficiency, and increase incentives to migrate to IPv6 by eventually making the obtaining of IPv4 space contingent on demonstrating IPv6 services and connectivity. Helps to increase awareness of the option to deploy IPv6, by compelling LIRs in need of address space to start an inventory of systems that would require adaptation to IPv6.	Commercially confidential concerns are likely to be high. Some Internet service providers that oppose increasing efficiency requirements argue that changes in the rules would favour some business models and market players. For example, some operators serve only large enterprises and it may be relatively easier for these companies to justify 100% utilisation rates. For others, like broadband providers, it may be relatively harder, since they are in a "retail" model. Assumes that significant address space is inefficiently used. The change in allocation criteria would not have much impact if assignments were already used efficiently.

Table 3. A sample of current policy proposals that pertain to increasing the IPv4 address space available for re-use

INCREASING THE IPv4 ADDRESS SPACE AVAILABLE FOR RE-USE			
PROPOSAL	**DESCRIPTION**	**ARGUMENTS FOR PROPOSAL**	**ARGUMENTS AGAINST PROPOSAL**
RECYCLING RESERVED IPV4 BLOCKS	Recycling existing assignments for other purposes. The IANA has taken the lead in identifying address space that is no longer in use, by working through the IPv4 registry data. For example, 14.0.0.0/8 is a former "Class A" that was reserved to connect X.25 networks to the Internet. Since X.25 is no longer in significant use, this space has been recovered and has been placed back into the IPv4 free pool, so 14.0.0.0/8 addresses can potentially be reassigned for other uses. [53] The Class E space, encompassing the "top" end of the address space, 240.0.0.0/4 is also a candidate that engineers have proposed to redefine as available for use, potentially in private or even public use contexts.	Contributors to the IETF are currently considering feasible re-uses for the Class E space.	Many of the currently deployed implementations of the IP protocol stack were configured to ignore traffic to or from those Class E address blocks.
RECLAIMING UNUSED IPV4 SPACE	In the early days of the Internet, large blocks of IP addresses were allocated to individual entities. It is suggested that these allocations, when these entities no longer exist or when addresses are not used or are not used efficiently, could be reclaimed by the IANA or by the RIRs and reissued. Some have advocated stronger reclamation efforts, which may not or may not be "voluntary". An important effort was for ARIN to adopt a "Legacy RSA" on 31 October 2007, for organisations and individuals in the ARIN service region, who hold legacy Internet number resources not covered by any other Registration Services Agreement with ARIN.[54]	Over the past five years, attempts to recycle legacy address space have been made, with some success. Relatively few efforts have been made to reach out to legacy holders.	Would require sizeable effort and expense, substantive negotiation (in multiple court systems around the globe) to retrieve any sizeable block. Likelihood of getting back more than a few /8 blocks is very low. Experts from the addressing groups consider that most easily recycled space has already been reclaimed Since legacy blocks were issued under terms that did not include reclamation provisions, and predate the existence of the RIRs, there is no legal framework under which to do so in the handful of countries concerned, except for legacy holders that have agreed to sign a registration services agreement (RSA).

Table 4. Policy proposals to enable IPv4 address transfers

ARGUMENTS USED FOR PROPOSAL	ARGUMENTS USED AGAINST PROPOSAL
Ongoing demand: The ongoing demand for IPv4 address space, beyond the time of unallocated address availability, may lead to a period of movement of IPv4 address blocks between address holders. **Efficiency**: Providing an incentive for unused IPv4 address space to be made available for active use, would help to satisfy residual demand for IPv4 address space during the transition to IPv6. **Security of records**: Ensuring both the accuracy and integrity of records which may otherwise be degraded without a sanctioned and transparent mechanism to transfer records. **Registration**: Avoid a black market that would drive prices up. A black market would degrade the accuracy of existing records, as changes to the registration data would not be reflected in the records. This could have ramifications for the security and stability of the Internet for many uses, such as in day-to-day internetworking or dealing with such events as denial of service attacks. There is also a broader community of users of such records, ranging from commercial geo-location services to law enforcement agencies.	**Developing countries**: Since many ISPs or other entities in developing countries came relatively late to using the Internet at a time when the RIR system was already established, their current allocations should for the most part be proportionate to demonstrated need. Developing countries may not have sufficient financial resources to purchase addresses on a market, while there could potentially be a windfall for well-resourced countries that joined the Internet early on. On the other hand, after IPv4 free pool depletion, the choice offered to all Internet users would either be IPv4 at a higher cost in a market environment or the unavailability of IPv4 addresses. In addition, the cost of IPv6-compatible equipment is currently higher than for pre-used IPv4 equipment, making less well-resourced ISPs more reliant on IPv4. A lack of IPv4 addresses, could, for example, curtail economic market entry or expansion by new 'home grown' competitors.
Hoarding: If unused address space cannot be traded, the user has no incentive to return it. However, if secondary trading is possible, this creates an incentive against hoarding, although it does not eliminate the possibility of hoarding: operators may for example wish to block the entrance of additional operators or to harm competitors.	**Speculation**: A market entails the potential for certain forms of market failures, including the possibility of speculation and price manipulation, which would be counter to existing policy goals. Proposals include safeguards aimed at preventing speculation by preventing parties to a transaction from entering into another transaction for 24 months.
Transition to IPv6: A likely increase in the price of IPv4 resources would translate into a financial compensation for those selling IPv4 addresses, helping them to bear the cost of renumbering/investing in IPv6. Allows organisations to choose the strategy that is best for them, rather than forcing a one-size-fits-all solution: some companies are likely to use IPv6 with IPv4 and NAT or a proxy to reach the remaining IPv4 Internet, while others may "pay" someone else to migrate and use their space to delay migrating until all their systems are ready.	**Transition to IPv6**: Transferring IPv4 addresses could lengthen the transition period from IPv4 to IPv6, and as a result, increase the likelihood of NAT solutions being widely implemented. **Predictability**: Some argue that introducing a market introduces confusion and removes incentives for those who implement IPv6 to return IPv4 address space.
Existing price for addresses: Transfers already take place during mergers or acquisitions. Addresses have a scarcity value and cost is transmitted to the customer. Cost of addresses will have a market value whether or not transfers are liberalised. **Pricing**: The availability of IPv6 as a free and essentially unlimited resource means that IPv4 may only have value for a limited time.	**Supply**: Some claim there will be a limited supply compared to likely high demand for IPv4 address space in the short and medium-term, driving up prices.
Competition: Fosters competition by providing a mechanism for new entrants to acquire address space. **Enforcement**: RIR's only lever, to ensure that records for transfers go through them, is whether the address space can be routed on the core of the Internet.	**Global routing table expansion**: Smaller blocks being traded would result in increased deaggregation. This could increase the cost of routing equipment to accommodate larger routing tables.[55] Policy proposals aim to control deaggregation by not permitting an entity transferring IPv4 to apply again for a specified time period.
Inter-RIR considerations: Strong arguments to consider global, or "inter-RIR" transfers rather than RIR-only, because of the regional distribution of IPv4 addresses, regional levels of demand for IPv4 addresses, and projections of demand within each region. Question of whether a global transfer domain would create inequities and imbalances in the residual IPv4 Internet that may require some other form of intervention or mediation to redress and potential policy mechanisms to mitigate such risks. To avoid abuse of an inter-RIR transfer system, necessary to increase inter-RIR co-ordination to verification policies, and possibly to direct (*i.e.* cross-regional) verification of "need" itself. Necessity to define how the "needs verification" or qualifying process will work even in an intra-regional context.	**Inter-RIR considerations**: Difficult to enforce regional membership while resources are global. Proponents of a modified transfer mechanism currently only permit transfer between account holders at the same RIR. However, entities could presumably create accounts at multiple RIRs. In addition, significant differences in levels of financial resources can exist within regions. Conflicts with RIR principle of not being involved in routing. Whether inter-RIR transfers were authorised would impact on the efficiency of a potential market.

Proposals to enable IP address transfers

The pending depletion of the free common pool of IPv4 addresses has led some in the Internet addressing community to propose modifications to the policies governing the transfer of IPv4 addresses. The question that is being debated with respect to transfers is whether greater flexibility in being able to transfer IP addresses could assist in any process of recycling previously allocated addresses. Some hold the view that significant amounts of IPv4 address space, including legacy assignments, may be transferred between parties if there are financial incentives for them to do so: address space that is allocated but unused would be moved back into potential use, albeit at a cost to the potential user.

A first proposal for IP Address transfers was introduced in the APNIC region in September 2007.[56] The proposal suggests removing restrictions on the transfer of registration of IPv4 address allocations and IPv4 portable address assignments between current APNIC account holders. The proposal argues that the ongoing demand for IPv4 address space, beyond the time of unallocated address availability, will lead to a period of movement of IPv4 address blocks between address holders. A similar proposal, entitled "Enabling methods for reallocation of IPv4 resources", was proposed and is being discussed in the RIPE region. [57] A different proposal is being discussed by ARIN.[58]

The proposals placed before each of the three RIR communities establish initial sets of "rules of the game" for address transfers and mandate that all transfers be undertaken through the local RIR. They place conditions on the transfer of the IPv4 address block, the source of the transfer (*i.e.* original assignee) and the recipient of the transfer (*i.e.* new assignee). Such ground rules include, for example, only enabling the transfer of IPv4 address blocks equal to, or larger than, a /24 prefix (16 384 addresses) between existing account holders. Further stipulations include that the source entity will be ineligible to receive any further IPv4 address allocations or assignments from the RIR for a period of 24 months after the transfer and that the RIRs will charge recipients a service fee on the transfer transaction. Holders of legacy address space are allowed to participate.

A discussion on potential supply and demand

The usefulness of enabling transfers depends on potential supply and demand. However, it is difficult to predict potential supply of IPv4 addresses, since organisations to-date have had no incentive to return unused addresses and since data on actual use of public IPv4 addresses in private networks is generally proprietary information.

Opponents of a potential liberalisation of transfer policy point to a likely high demand for IPv4 address space in the short and medium term, compared to limited supply. For example, the ISPs forming the membership of the European Telecommunications Network Operators' Association (ETNO) point to the fact that the Association's membership represents a large portion of demand for IP addresses in the RIPE region. While address demand is high, the point they stress is that sources of supply are limited in all regions except for the ARIN region: because of the Host-Density ratio utilisation requirements, address holders with an RIR membership are deemed to overall efficiently use their IPv4 allocations. Therefore, the primary source of supply is viewed by some to be the legacy, *i.e.* pre-RIR, address space allocations. For historical reasons, these allocations are located primarily within the ARIN region. Other views have also been expressed in the debate on the matter of regional variations of potential supply of addresses for unrestricted transfer.

Geoff Huston, Chief Scientist at APNIC, points out that 90% of RIR-allocated space is routed while only 40% of legacy space is routed. He uses publicly advertised address space as a proxy for consumption (and ongoing demand), because 90 to 95% of (non-recent) address space allocated since 2000 is advertised on the public Internet. By contrast, only 40% of address space allocated before 2000, *i.e.* before the RIR system, is advertised. A model developed by Huston estimates that currently allocated but unadvertised address space could support continued demand until mid 2019, *i.e.* for about 7 years after the exhaustion of the free pool of unallocated IPv4 addresses, under specific assumptions.[59] Some stress that much of the address space that is unadvertised (not publicly routed) is actually in use within inter-networks that do not exchange packets with the public Internet and therefore that it may not be available for re-allocation.

The global routing table shows whether allocated IPv4 address space is routed or not publicly routed (Annex 4). Unallocated space and space reserved for technical use can also be represented.[60] The allocations/utilisation rates shown in the figure reflect the history of IPv4 address allocation and increased efficiency measures introduced by the RIRs over time. It provides a visualisation of the sizes of routed address space, from the largest prefixes (/8) through to the smallest prefixes possible (/32).

In addition, several surveys that examine the population of "visible" IPv4 Internet hosts find that only a low percentage of advertised addresses respond, which could mean that even among routed address space, significant address space is unused. For example, one study finds that only 3.6% of allocated addresses are actually occupied by visible hosts. [61]

Possible safeguards

It is possible to envisage a number of potential constraints to address some stakeholders' concerns. The most prominent potential constraint is to continue the existing RIR policy of demonstrated need to avoid speculation with IPv4 address space. This means that only qualified applicants would be eligible to participate in the transfer of IPv4 address space. The repercussions of other qualification mechanisms, and of the absence of such forms of qualification, are also under investigation. Whether the RIRs have the means and resources to enforce such constraints, and what form they should take is a moot point. The main criteria in these considerations should be whether changes assist the Internet community to more effectively meet specific goals (the stated objective to-date has been to safeguard addresses for demonstrated need, to maintain accurate records for security and operational reasons and to minimise the load on the global routing tables) and whether they can be enforced.

If a market were to develop such that addresses were monetised, its nature and the challenges for enforcing regulation, outside of any individual national regulatory framework, would require thorough consideration. However, if Internet service providers chose to require the registration of address space within RIR databases, there could be a mechanism for RIR policy setting mechanisms to be enforced. If, however, ISPs chose to negotiate transfers of address space outside of the context of the RIR policies, those policies by definition do not apply. There may be a tipping point, perhaps dependent on the creation of an alternative "titles registry" that the ISPs can be convinced to use (Box 3).

From an economic perspective, there are strong arguments to increase the allocation efficiency of scarce resources such as IPv4 address space. For new entrants, as well as existing operators, being able to acquire IPv4 addresses that were previously allocated to other parties, seems important to maintain interoperability. Any kind of institutional arrangement should ensure efficient resource use, promote competition, and minimise interference. Political acceptability is likely to be key, considering the potential windfall gains for some actors (although such windfalls could arguably exist even without a market).

Box 3. Developing a routing PKI or "Certification of Internet resources"

Several RIRs are developing Internet resource certification frameworks in view of validating assertions of "right-to-use" of an Internet Number Resource (IP Addresses and Autonomous System Numbers). APNIC, for example, has built a Resource Certification System.[62] One potential use for this type of certification and the associated Public Key Infrastructure (PKI) is to provide a validation framework to support secure routing on the Internet and improve other aspects of securing the use of addresses within protocol transactions. Such certification by RIRs would also apply to a market for IP addresses, where a major public policy concern relates to consumer confidence.

Certificates would play three roles in a market transaction: *i)* validating that a "seller is indeed a valid seller" who has clear 'title' to the addresses that are being sold; *ii)* ensuring that the transaction of the sale cannot be repudiated or denied once completed, by either party to the sale, and; *iii)* ensuring that the buyer becomes the clear "title" holder of the addresses following the transaction and that the seller has given up rights to the address.

Each allocation or assignment made by an RIR is certified by the same RIR. Each address holder holds a private key, whose matching public key is published in the RIR-issued certificate. Anything signed by the address holder's private key can be validated through the RIR-issued certificate and the addresses bound to that certificate. In the case of using certificates to secure the routing system for example, an address holder would digitally sign a routing origination authority, giving an autonomous system address holder the authority to advertise into the routing system a routing advertisement for that address. A third party receiving the routed object could use the RIR-issued certificate to validate the signed authority and thereby check the valid advertisement of that address. Overall, adoption of security measures in the Internet's routing system that could make use of an Internet address PKI would help prevent various attacks, including denial of service, third party traffic inspection and service cloning. Such attacks on the integrity of the routing system often occur within today's Internet. But because of the distributed nature of the system and the diverse trust environment, these attacks are extremely challenging to detect, let alone prevent, without a structured trust model that number resource certification could provide.

Some express reservations and point out that such certification in the context of adoption of secure routing frameworks, expands the role of the RIRs into that of certificate issuers which, in turn, gives them a central role in the operation of the Internet's routing system.

In other respects, RIRs appear to be a logical institution to issue such certificates since what is being certified are the number resource allocation and assignment actions of the RIRs themselves, and the information provided through the certificate is the information published by the RIRs via the Whois query systems. Certificates republish this same information in a manner that is strongly secured, allowing other parties to make decisions as to the validity and authenticity of the use of an address.

The efforts to improve the security of the routing system and offer capabilities to support the integrity of the operation of a market in addresses, illustrates the adaptability and reactivity of the RIR system to evolving requirements of the address community. Governments should participate and comment as stakeholders.

With respect to modifications to the existing transfer policies, the Internet community will need to take the following into consideration:

- **The status of addresses**: IP addresses are not currently considered as property by the Internet community. The introduction of a modified transfer mechanism does not necessarily imply that this status needs to be changed if they were, for example, treated as partial use-rights rather than all-encompassing property rights.[63] Changes could also emerge in relation to concepts such as "ownership" and "leasing".
- **The geographic scope of transfers**: whether IP addresses could be transferred within RIR regions, between countries with a NIR, between RIR regions, inside countries, or between countries, and if/how policies could be enforced.
- **The technical scope of transfers**: whether the entire IPv4 address space would be transferable or just a subset, and depending on when transfers were enabled, whether the currently unassigned pool participates.
- **Pricing**: what safeguards are imposed upon transfers to help avoid IP price manipulation.

- **Participants in transfers**: whether existing RIR practices and procedures, in relation to demonstrated need, would be used to determine qualified participants or, if not, whether an open market would be compatible with achieving existing policy objectives.
- **The optimal size of address blocks and complimentary markets**: what the minimum size-transfer block should be, how a market would impact global routing table sizes, whether complimentary markets, for example a market for route entries, would be co-ordinated or who would route smaller address blocks.
- **The design, structure and convenor of a "market venue"**: what requirements and issues of market design and structure would be; price formation and price discovery, transaction and timing costs, and information and disclosure. Microstructure for financial markets can offer insights into market design. Comparisons could also draw on secondary markets for spectrum allocations and other scare resources (Annex 8). Another question may be whether the RIRs would act as the convenor of market venue for transfers and facilitate making the connection between buyer and seller in the same form as a stock exchange operator, or whether the RIRs would assume a more limited role of a "title office" as the trusted authority for number resource disposition information.

The foregoing only provides a cursory examination of some of the issues that will be considered by the Internet community. Over time, the behaviour of different actors will be highly dependent on the policies and practices adopted by the Internet community and how the valuation placed on IPv4 addresses develops and changes as positive network effects build for IPv6.

For governments, the most important message may be that any of the options available to the Internet community may only imperfectly address broader economic issues. Since after the depletion of IPv4 addresses, the IPv4 Internet will continue to function, actors who wish to connect to both IPv4 and IPv6 nodes need to have access to IPv4 addresses: consequently, mechanisms to extend the life of IPv4 or tip it towards specific uses are being thoroughly investigated. In addition, different options may have potential public policy implications, such as in the area of security, on which governments should comment as a stakeholder. All stakeholders are encouraged to contribute to address allocation mechanisms and policies, and their review, through providing input in appropriate for a, such as the regional Internet registries, as to priorities and local requirements.

III. DRIVERS AND CHALLENGES OF IPV6 DEPLOYMENT

This section investigates business drivers and challenges related to the introduction of IPv6. The vast additional address space available with IPv6 can help the Internet to support the next generation of wireless, high-bandwidth, multimedia applications as well as growth in the overall number of users. Today's IPv6 deployment drivers focus on performance approaching that of IPv4 albeit on an expanded scale, operational cost savings through simpler network models when deploying applications, and on enabling new product and service innovation. General benefits or application areas for IPv6 are listed (Table 5).

Industry is in the early stages of IPv6 production deployment, but substantial challenges remain for the adoption of IPv6 on a meaningful scale. Although the success of IPv6 will ultimately depend on the new applications that run over IPv6, a key part of the deployment of IPv6 in the short and medium-term is that of co-existing with existing IPv4 networks. Furthermore, many Internet service providers currently lack incentives to adopt IPv6. This is due to several factors such as a lack of awareness, lack of demand, expertise and capital to make investments that do not provide short-term benefits. Challenges to IPv6 deployment can be ranked in function of urgency (Annex 7).

Table 5. Several benefit/application categories

Impact Metric	Application/ Market	General Description: Examples
Cost reductions resulting from increased efficiency	NAT removal	• According to RTI International (2005), enterprise and application vendors' spending on NAT workarounds accounts for up to 30% of IT-related expenditures.
Value of remote access to existing products/services	Increased life expectancy of products	• Automobile[64] and appliance owners[65] could increase the functionality and life expectancy of their products through the use of remote monitoring and support services.
	Service costs	• Automotive and appliance owners could decrease service costs through the use of remote monitoring and support services.
Innovation in communications and online products/services	New mobile data services	• Wireless companies could sell new features through expanded network capabilities.[66] • Wireless companies need IPv6 to increase address capacity for peer-to-peer (P2P) applications.
	Online gaming	• Gaming and game console makers could see expanded functionality and thus opportunities for innovative new products.

Source: OECD (2007), adapted from IPv6 Economic Impact Assessment, RTI International for National Institute of Standards & Technology, October 2005.

DRIVERS

Scalability and demand for IP addresses

Escalating demand for IP addresses is a main driver for IPv6 adoption. Convergence and the development of ubiquitous IP networks and IP-based communications place pressure on the available IPv4 address space. The current IPv4 address space is unable to satisfy the potentially very significant increase in the number of users, or the requirements of emerging applications such as Internet-enabled wireless devices, home and industrial appliances, Internet-connected transportations, integrated telephony services, sensors networks such as RFID, IEEE 802.15.4/6LoWPAN, distributed computing or gaming. Always-on environments and the ready-to-use capability required by some consumer Internet appliances further increases the address requirements.

IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides sufficient globally unique IP addresses for a vast number of networked devices. The use of globally unique IPv6 addresses simplifies the mechanisms used for reachability of these network devices.

There may also be an increasing number of cases in which networks "outgrow" IPv4 private space, such as in the case of Comcast, a large cable operator that transitioned to IPv6 because it outgrew the largest private address space of 16.7 million addresses. It was economically critical for Comcast to transition to IPv6 in order to continue to support the growth of its network. Mobile operators, for example, could potentially consume large amounts of IP addresses.

Public procurement mandates

In some cases, aggressive IPv6 adoption curves by government bodies have provided incentives for industry, particularly those vendors supporting or interacting with the government, to work toward IPv6 adoption themselves. In many cases, public sector mandates have caused vendors to develop IPv6 solutions, which then accelerate deployment in private sector companies, because vendor software already supports specific features.

In June 2003, the United States Department of Defense (DoD) mandated the integration of IPv6 to be ready by 2008.[67] In June 2005, the United States' Office of Management Budget (OMB) set June 2008 as the deadline by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must be interfacing with this infrastructure.[68] To provide an idea of the impetus such a decision can provide to the market and vendor and operator strategies, spending on communications and network services by the US federal government will grow from USD 17.6 billion in 2007 to USD 22.4 billion by 2012.[69] The Japanese Ministry of Internet Affairs and Communications released a "*Guideline for e-Government IPv6 Systems*" in April 2007, to help central ministries plan for IPv6 adoption and promote IPv6 for e-Government systems.[70] Targets set by the Korean Ministry of Information and Communication include converting Internet equipment in public institutions to IPv6 by 2010. The Australian Government Information Management Office (AGIMO) has also released its Strategy for the Transition to IPv6 for Australian Government agencies, to last from January 2008 to December 2015. [71]

Innovative applications, including sensor networks and embedded systems

Most of the work on IPv6 to-date has focused on ensuring that what worked well with IPv4 continues to work with IPv6. But an equal level of functionality is only the first step. A key driver for IPv6 is to make possible *new* business and services on a large scale, such as networked sensors for industrial or home automation services. In addition, when new services are greenfield deployments, they do not have to interoperate with legacy IPv4 hosts and applications and can be directly deployed over native IPv6 infrastructures (or dual-stack).

Trends in the Internet include more capable consumer devices – personal digital assistants, videogame consoles, and popular audio-visual equipment, including home servers, set-top boxes, digital TV sets, networked home appliances, car navigation systems, as well as wireless sensor networks, and intelligent transport systems and servers in trains, ships and airplanes. Several features of IPv6, including its support for near unlimited numbers of potentially connected devices at any given time, combined with mobility, make the standard a logical candidate for some of these new uses. Sensor networks can also benefit from the plug-and-play capabilities of IPv6, such as address auto-configuration and anycast address support. Beyond energy management, environmental information systems, facility control and management or disaster protection (Box 4), applications in areas such as home security and health are emerging. A number of governmental authorities have actively promoted sector-specific IPv6 applications (Annex 3).

Box 4. Using IPv6 to Bridge the Physical and Virtual Worlds

Arch Rock uses IPv6 in low power wireless meshed networks of sensors.[72] The company chose Internet Protocol-based sensor networks to benefit from convergence toward the well-proven and open "Internet Protocol" (IP): IP integration helps to reliably manage sensor networks and sensor nodes using familiar Internet technologies at a dramatically lower operating cost compared to the rival proprietary options. The company uses the 6LoWPAN standard, which has scaled the IPv6 protocol down sufficiently to be useful in wireless embedded networks. The standard supports both connected and disconnected operation.[73] Other reasons for adopting IPv6 include its ease of management of two-way communications without the need for translation, its large address space to support millions of sensors, its plug and play networking capabilities, energy efficiency and simplified protocol processing as well as to support future growth and new innovations. Arch rock's sensor network solutions are rapidly deployable in many challenging environments and applications such as open fields, civil engineering structures, on mobile high-value items, factory floors, or office buildings.

With wireless sensor networks providing the ability to measure and monitor places and things that were once impossible or impractical to instrument, new applications using 6LoWPAN have demonstrated they could help:

- **Energy management**: applications using IPv6-based sensor networks allow efficient energy management with monitoring solutions for energy awareness and control in enterprise data centers, as well as with electric utility programs to influence and sometimes control electric load from subscribers. In Japan for example, the Tokyo Metropolitan Art Museum and the Tokyo Art Space have been able to reduce energy consumption by about 5%.

- **Road traffic management**: road to car communication systems with IPv6-based sensor networks offer promises to help reduce traffic jams and fuel consumption.

- **Risk detection and prevention**: IPv6-based sensor networks can be used for global monitoring and disaster management of seismic activity, volcanic eruptions or landslides and avalanches, disaster prevention, or environmental problems.

- **Industrial automation**: wireless sensor networks using Ipv6 can offer previously inaccessible insight and information. Costs are reduced because wires or heavy instruments are no longer needed. Problems can be detected early, failures or outages prevented, and new information and data can be collected to keep machinery running without direct human intervention.

- **Location and proximity:** applications developed by Arch Rock include asset tracking and monitoring, worker safety, quality of service, hazardous material management, and regulatory compliance.

Source: Arch Rock, www.archrock.com.

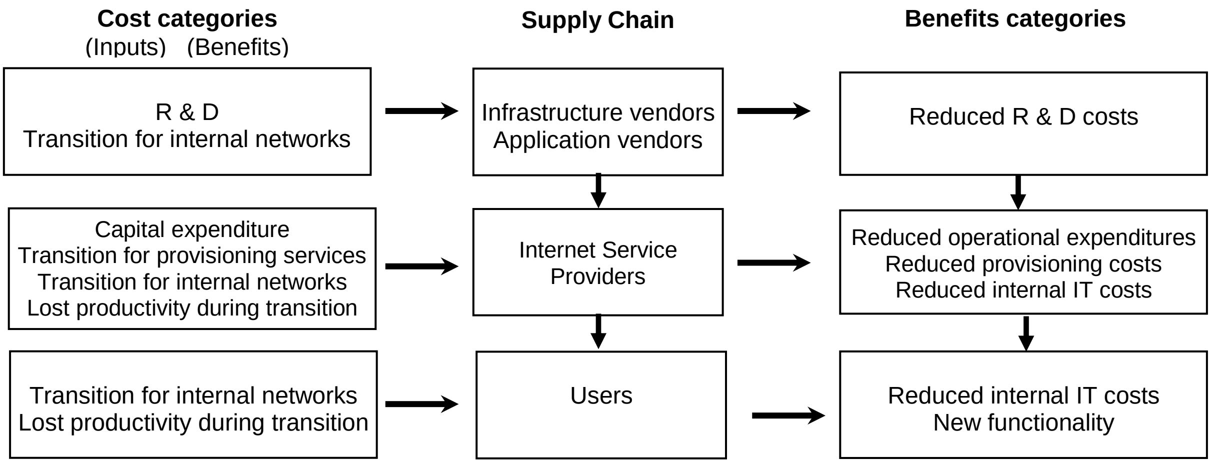
Less expensive network administration

Some network administrators deem that IPv6 simplifies some functions in network administration, through a simplified header that can improve routing efficiency, serverless autoconfiguration, easier renumbering, ready-to-use support, and multicast support with increased addresses.

Actors are likely to deploy IPv6 when the cost/benefit ratio of that deployment, given network effects, warrants it. Large address consumers, faced with non-predictable costs in obtaining resources, are likely to accelerate deployment plans for IPv6 for their internal infrastructure where possible, complemented by private use IPv4 address space, thereby freeing up the public IPv4 addresses used for internal infrastructure for use in customer assignments. In addition, it will become increasingly difficult and expensive to obtain new IPv4 address space to expand networks and the cost and complexity associated with keeping track of and managing remaining IPv4 address space will also increase. Therefore, there may be strategic benefits in avoiding opportunity costs or operational costs associated with IPv4 and increasing density of NATs.

Adoption decisions will be taken by many and various stakeholders (*e.g.* infrastructure vendors, software vendors, ISPs and users) based on the costs and benefits they see for their activity (Figure 7). As mentioned above, Internet service providers may decide to implement IPv6 in their internal networks once they consider that the benefits of reduced operational expenditures (current or projected) outweigh the capital expenditure of maintaining IPv4 and increasing NATs. It is important to note that considerations of provision of external IPv4 connectivity services and dual-stack networking remain even in such a scenario.

Figure 7. Supply chain stakeholders, costs, and benefits



Source: OECD based on RTI, IPv6 Economic Impact Assessment, National Institute of Standards & Technology, October 2005.

Better mobility support

While mobility can be supported at various levels, this document considers IP layer mobility only, which is critical because it is neither conditioned by supporting wireless radio technology nor by applications. A further distinction can be made between mobile nodes and nomadic nodes: while mobile nodes need to preserve established communications during movement, nomadic nodes only need to be able to establish new communications each time they re-connect to the network. The following considers mobile nodes.

It is projected that, in the wireless arena, very large numbers of mobile phones, personal digital assistants (PDAs), and other types of wireless devices will increasingly require Internet access in the future, and therefore, IP addressing. Some experts consider that IPv6 offers improved support for mobility. Within the IETF, a number of working groups are using IPv6 as the basis for solving protocol problems related to *handset* mobility.[74] IPv6 is also the basis for new mobility-related protocol developments, including in the areas of *ad hoc networking*.[75] Some developments target *sensor networks*.[76] In general, updating applications is an important transition issue, including applications that run on handsets to support IPv6. A number of mobile applications, in particular many mobile operating systems, support IPv6.

Mobile phone operators and manufacturers see handsets as “always-on” end points in a network. This architecture has developed into 3GPP IP Multimedia Subsystem (IMS), to be used with smartphones. As Internet-connected handsets that offer voice, data and video become the norm, operators could start to deploy IPv6 on a large scale.[77] While many smart phone operating systems support IPv6, a challenge for mobile operators is the availability of billing and authentication applications from service providers. In what follows, some of the arguments for mobile IPv6 over mobile IPv4 are described.

One reported advantage of IPv6 is that it improves timeliness of transmissions, by optimising routing.[78] However, there is an associated overhead cost, to make the mobile transmissions secure.[79] The alternative option of using IPv4 private space and NATs is considered less efficient and has its own overheads, due to cost associated with NAT transversal techniques as well as costlier management resulting from more complex architectures. Another implication of “always on” and NAT is that the handset has to send regular ‘keep alive’ messages in order to keep its IPv4 address, which drains battery capacity.

Considerations of interoperation with the IPv4 network and the concept of dual-stack support for mobility also need to be addressed. [80] The assumption made in many analyses of mobile IP support is that interoperation across IPv4 and IPv6 would be through application level gateways. The cost and complexity of these gateways needs to be considered because, while servers for Internet applications are on IPv4, they require translation.

In summary, the benefit of IPv6 is that, due to the larger address space in IPv6, public addresses can be assigned to mobile nodes, even with very many mobile nodes. In addition, Mobile IPv6 is deemed to optimise routing, by offering route optimisation between any-to-any node. Therefore, NATs, which can be expensive for mobile devices, are not needed. Considerations of interoperation with the IPv4 network also need to be taken into account. Both options carry costs.

Although there are plans to deploy MIPv6 in the future releases of 3GPP and of WiMAX, there are currently no commercial MIPv6 deployments of any significance.

As a potential indication of interest, many large IPv6 prefix assignments are to telecommunications operators. However, the policy basis under which these allocations were made – without incremental cost to requesters and without any obligation to demonstrate IPv6 deployed infrastructure – means that requesting allocations does not necessarily mean actively planning to deploy IPv6. Some of the IPv6 allocations are extremely large, such as the allocations to Telecom Italia, the Korean Education Network, Sprint, or Samsung (Table 6). As an illustration of the size of some of these prefixes, the allocation in 2006 of a /20 to Telecom Italia represented 268 435 456 (2^{28}) customers, under the assumption of each customer receiving a /48 and each customer having up to 2^{16} (65 536) local area networks.

Table 6. Sample of recent very large IPv6 allocations

PREFIX	COMPANY	DATE
2404:0e0::/28	MCI Asia Ptr, AP	(2006/05/10)
2404:180::/28	Samsung Networks, KR	(2006/08/28)
2610:080::/29	RCN Corporation, US	(2006/06/02)
2a01:110::/31	Microsoft, GB	(2006/06/01)
2a01:2000::/20	Telecom Italia, IT	(2006/05/16)
2402::/22	Korean Education Network, KR	(2006/10/20)
2600::/29	Sprint, US	(2006/12/21)
2600:800::/27	MCI / Verizon Business, US	(2007/01/08)
2401:8000::/26	NCICNET, TW	(2007/01/23)
2a01:2e0::/28	PLUSGSM, PL	(2007/03/19)
2401:6000::/20	Defence-Dcc-Mgmtconfig	(2007/08/10)
2a00:2000::/22	British Telecom, GB	(2007/08/29)

Source: RIR IP Whois databases, based on RIPE NCC presentation.

CHALLENGES

Transition and co-existence

Co-existence of the two protocols, IPv4 and IPv6, is a major challenge for IPv6 implementation, because the two protocols are not “interoperable” and it is expected that IPv4 will need to be supported alongside IPv6 for a substantial period of time. This signifies managing more than one network and maintaining interoperability with many existing IPv4 implementations during the transition. Implementing

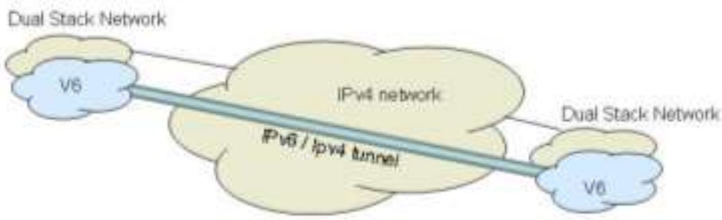
IPv6 requires careful planning, a thorough review of the network's architecture and a detailed transition plan.

Dual-stack approach

In terms of technical strategies, the dual-stack approach implies that all devices (computer, routers, cellular phones etc.) can interoperate with IPv4 devices using IPv4 packets, and also interoperate with IPv6 devices using IPv6 packets. Since the goal of most networks on the Internet is to maximise their connectivity with other networks, most IPv6 implementations today are dual-stack. Experts stress that dual-stack support is important for public-facing hosts, across the network, in the routing system, and in infrastructure services such as the domain name system, firewalls, security, and management systems, so as to enable interoperability. Edge devices (enterprise, net services, consumer etc.), for their part, can be dual-stack, IPv6-only, or IPv4, depending on configurations.

Experts also point out that the dual-stack approach is based on the idea that for as long as there is a significant level of IPv4-only networks, services and connections, new deployments will need to provide IPv4 access. The value of IPv6-only deployments would be impaired by their limited domain of connectivity. This means that in the early phases of IPv6 deployment, the IPv6 component of dual-stack hosts and network deployments will be isolated “islands” (Figure 8). Experts also stress that this implies a need for support of automated IPv6 tunnelling, in order to connect isolated IPv6 islands.

Figure 8. Dual-stack example



Source: Huston, G., “Transition to IPv6”, August 2007.[81]

A significant complication associated with dual-stack is that it assumes that parties, namely the two end host devices, have access to both IPv4 and IPv6 addresses. Internet packets need public IPv4 addresses in the destination field to be routed in the public IPv4 network, regardless of how many private addresses/ NATs are at either end. The paradox is that IPv6 is not likely to be deployed in significant volume before the free pool of unallocated IPv4 addresses is depleted. Therefore access to Internet resources may be limited for those who do not already have IPv4 addresses, as long as all servers are not widely available through IPv6.

Tunelling and other transition mechanisms

Tunnelling provides a way for the existing IPv4 routing infrastructure to remain functional, and also carry IPv6 traffic. Data is carried through an IPv4 tunnel using a process called encapsulation, in which the IPv6 packet is carried inside an IPv4 packet.

Several other transition mechanisms have been defined, and may be appropriate for some network configurations. For example, a mechanism called “6to4” allows IPv6 packets to be transmitted over an IPv4 network using automated tunnel support. The mechanism: *i)* assigns a block of IPv6 address space to any host or network that has a global IPv4 address; *ii)* encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network; and *iii)* routes traffic between 6to4 and IPv6 networks.

Box 5. "An Internet Transition Plan"

There is significant discussion within network operator groups, such as the North American Network Operators' Group (NANOG) or the South Asian Network Operators Group (SANOG), as well as within the IETF, about transitioning to IPv6. For example, one proposed "Internet transition Plan" presented as an "informational Internet draft" of July 2007 states that its goal is "to begin the discussion of Internet-wide transition plans in general". To this effect, it proposes a phased approach to transitioning to IPv6, with *i)* a preparation phase, until 2008; *ii)* a transition phase, from January 2009 to December 2010 and; *iii)* a post-transition phase, after January 2011.

The proposed plan specifies that in the first stage, which began in 2007, service providers should start offering IPv6-based Internet service to their Internet customers, via native IPv6 network service or via IPv6 transition mechanisms. It further advises that organisations in general arrange for IPv6-based Internet connectivity for any Internet-facing servers (*e.g.* web, email, and domain name servers) and should furthermore progressively provide IPv6-based Internet connectivity to internal user communities. Even though other experts believe that such a timeframe is too short and that both protocols will have to coexist for many years, the general approach proposed for the upcoming transition, is generally considered useful. Each transition plan will differ depending on the type of organisation. Some networks may in fact never need to make the transition.

While other experts believe that such a timeframe may be too fast and that both protocols will have to coexist for many years, the general approach proposed, in terms of thinking of the upcoming transition, is considered constructive. Some stress the co-ordination difficulties. Moreover, different regions are at different levels of development and have differing investment capacity, including for investment in skills building. They point out that further dialogue is needed in various forums, industries and inside firms, so as to develop better understanding of the form that collective efforts could take. For example, ISPs have stressed the need to develop a common understanding of what the basic "IPv6 service" might be, such as, for example, at a basic level, web and email support.

Source: John Curran, J., "An Internet Transition Plan", IETF Draft, August 2007.[82]

IPv6-related deployment strategies, associated costs and skills

The cost of IPv6 deployment cannot be evaluated generically, as such costs vary on a case-by-case basis according to network needs and business.[83] User cost differences are not directly related to organisational size and depend on existing organisational network infrastructure (including servers, routers, firewalls, billing systems, and standard and customised software programs); on the type of organisation (*i.e.* some types of services could be interrupted or damaged during a transition); on the future needs of an organisation's network; and on the level of security required during the transition. Furthermore, different technologies (*e.g.* cable, DSL, Ethernet and wireless) involve different IPv6 transition and co-existence scenarios.[84]

In some networks, deploying IPv6 only involves training, configuration, testing and management costs, while for others – depending on set-up, goals and strategy – the cost of software and hardware upgrades may be significant. Planning the deployment enables each organisation to determine costs and select a deployment scenario that enables IPv6 services at the lowest cost possible (Table 7).[85] Hardware and software vendors are increasingly integrating IPv6 as a standard feature in products, allowing organisations to deploy IPv6 as part of routine upgrade cycles.

For many organisations, operational costs, including staff training, and staff time to add IPv6 to management databases and documentation, are likely to constitute the majority of the cost of upgrading to IPv6. Organisations that run in-house customised software will experience additional costs to upgrade these programs to IPv6, and enterprises that have test/release processes will see a marginal additional cost for IPv6 configuration tests. A widely reported barrier to IPv6 deployment is that of expertise: education, training and awareness. There are few network engineers and computer scientists with the knowledge needed to set up and manage IPv6 networks. This is deemed to be particularly true for IPv6 security, because connectivity during the transition phase will in many cases involve tunnels, which create security vulnerabilities.

Table 7. 10 Essential Planning Steps

Step 1. Identifying how IPv6 affects operations
Step 2. Establishing goals, a critical path, and timelines
Step 3. Inventorying IT equipment and build a deployment plan
Step 4. Identifying software and services and develop an upgrade plan
Step 5. Creating an IPv6 training strategy and plan
Step 6. Developing an addressing plan and corresponding network architecture
Step 7. Obtaining an IPv6 prefix
Step 8. Developing an IPv6 threats and countermeasures security policy
Step 9. Developing an IPv6 procurement strategy and policy
Step 10. Drafting an exception strategy (systems that don't need to be modified)

Source: Planning and Accomplishing the IPv6 Integration, Cisco systems.[86]

RTI International, in a study conducted in 2005 for the US National Institute of Standards and Technology (NIST) on IPv6's economic impact, concluded that the major costs to service providers or enterprises implementing IPv6, are related to labour costs (Table 8).[87] They include staff training, product testing, network-specific management and monitoring software, testing interoperability between network components with IP capabilities, installing transition mechanisms (such as dual-stack), maintaining transition mechanisms, and ensuring high network performance.

Table 8. Distribution of IPv6-related transition costs to users

	Distribution of Total Transition Costs
Category	Internal Network Costs
Network management software (upgrade)	18%
Network testing	17.6%
Installation effort	24%
Maintaining network performance	16%
Training (sales, marketing, and technical staff)	24.4%

The percentages in this table sum to 100 percent, comprising the distribution of all costs for users to move to IPv6.

Source: RTI International, 2005.

RTI estimated that the (2005) value of costs for all stakeholder groups to transition to IPv6 in the United States would be approximately USD 25 billion, occurring mainly over the 1997 to 2025 period. The highest cost year projected was 2007, representing USD 8 billion. [88] RTI also estimated that, in the United States, users would incur most of the costs of IPv6 transition (approximately 92%), with ISPs and vendors accounting for 0.5 and 8% respectively.

Content, latency and interconnectedness

From an end user's perspective, the key issue with transitioning to IPv6 is likely to be content rather than cost. There is currently little Internet content available via IPv6 because transitioning to IPv6 is particularly challenging for content providers. Comparatively fewer IPv6 traffic exchange (peering and transit) agreements and numerous "tunnels" to carry IPv6 traffic over IPv4 infrastructures often mean IPv6 has higher latency than IPv4 (Box 6). Latency represents the amount of time it takes for a packet of data to get from one designated point to another. In a dual-stack environment, where both endpoints prefer IPv6 to IPv4 if available, IPv6 may appear to be available at both endpoints, without actually providing reachability all the way through. Thus, a user may try to browse a website, find an IPv6 address, and try to contact the IPv6 version of the site, but then experience a failed or slow connection. Content providers, with little demand and potentially downgraded performance (which most users would not realise was due to IPv6 traffic paths rather than to the content provider), consider latency to be a major obstacle to making their content and services available through IPv6.

Box 6. Measuring latency

Researchers in Portugal have compared latency with IPv4 and IPv6 from the Portuguese NREN to commercial sites and to National Research and Education Network (NRENs) in Europe, in Japan, and the United States.[89]

Results show that latency with IPv6 is generally higher than with IPv4. Results with Japanese commercial services are good, while those with the European Union, US and Russian services are not. Surprisingly, latency can actually be *improved* with IPv6, as in the case of the Irish NREN.[90] The overall conclusion of the authors' research is that global IPv6 deployment is not on track.

Source: Domingues, M., Friacas, C., "Is Global IPv6 Deployment on Track?", FCCN, October 2007.

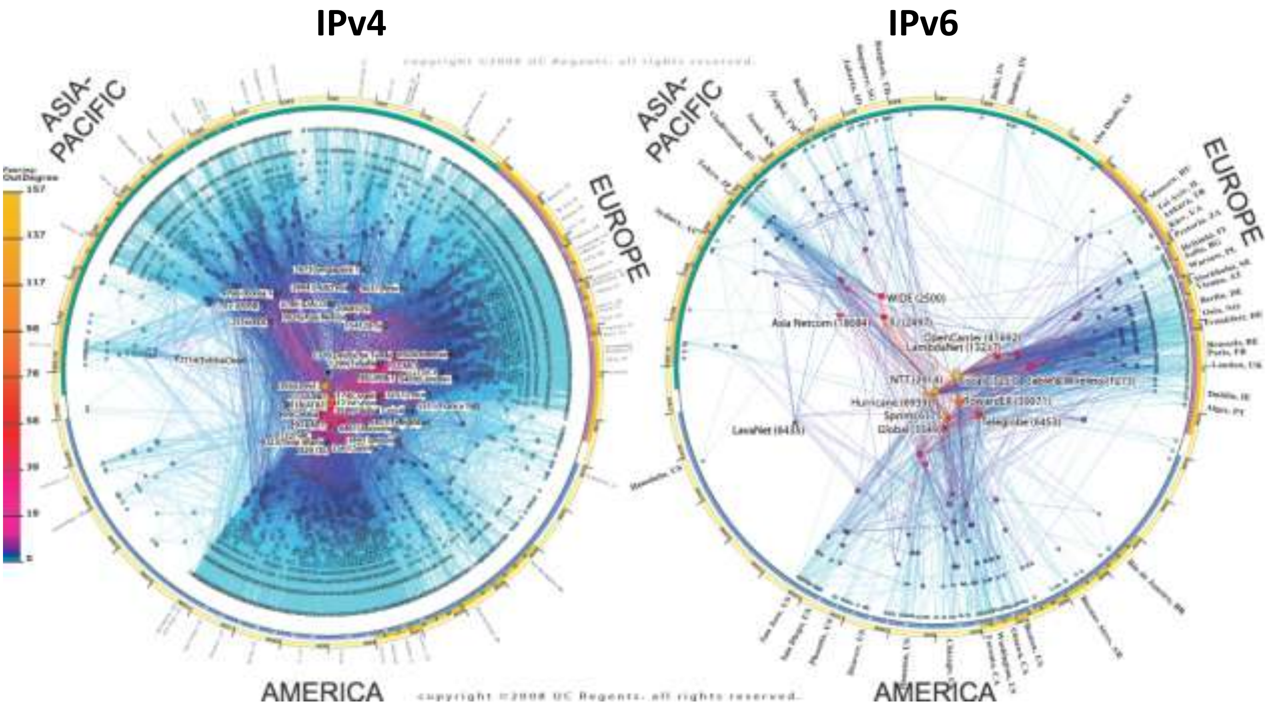
Internet traffic experts point to the low number of carriers that provide IPv6 peering and transit as a reason for latency and other issues. Lack of IPv6 peering agreements and Internet eXchange Points (IXPs) supporting IPv6 can increase latency because traffic may have to travel further to reach its destination. They deem that the latency issue with IPv6 will disappear once a critical number of service providers have enabled native IPv6, as is the case for IPv4. In the meantime, ISPs and businesses that negotiate peering and transit agreements should explicitly provide support for IPv6 traffic. There have been suggestions that public policy makers could look into subsidising IPv6 support in IXPs.

Several content providers seem to have provisioned IPv6 address space, which may signal change. For example, Google has started IPv6 deployment (see Section V. Case studies of deploying IPv6: Google) and Microsoft and Cisco Systems also each have a /32, as does Speakeasy, an ISP in the United States. YouTube has a /48 provider-independent IPv6 network assignment from ARIN, as does Tellme Networks, a provider of voice services that has recently been acquired by Microsoft. Another entity with an IPv6 assignment is Collab Network, which produces leading open source development collaboration software, enabling over 2 million geographically dispersed developers to work together on a project.

CAIDA, an association that provides tools and analyses promoting the engineering and maintenance of a robust, scalable global Internet infrastructure, has produced Internet topology maps comparing the use of IPv4 and IPv6 around the world (Figure 9). The visual representation comparing IPv4 and IPv6 is telling. The observations of IPv6 connectivity between networks (autonomous systems or "ASes") are much sparser than the IPv4 AS graph: fewer nodes and less peering richness were observed. Geographical patterns of the graphs also differ. For IPv4, the service providers with most observable connectivity are in the United States. In contrast, the operators with the richest observed IPv6 peering are NTT, headquartered in Japan, and Tiscali, headquartered in Italy. The largest cluster of high degree IPv6 AS nodes is in Europe.

The observation that Japan and Europe have the highest degree of peering in IPv6 is consistent with the registry allocations of IPv6 prefixes in these regions. It warrants noting that a relatively small number of Tier 1 providers are present in both the IPv4 and IPv6 topology maps: NTT, Global Crossing, Cable & Wireless, Tiscali, Sprint, Teleglobe and Asia Netcom.

Figure 9. IPv4/IPv6 Internet topology maps – AS-level internet graph



Source: CAIDA, observed January 2008.

Scalability of the global routing tables

Enterprises have stressed that a primary reason they were not investing in IPv6 deployment was dissatisfaction with the way IPv6 supports "provider independent" or "multi-homed" users, *i.e.* users with redundant interconnection and traffic exchange with two or more independent networks. Multi-homed users add entries corresponding to their routes to the global routing tables, which increases the size of the tables. Therefore some fear that IPv6 could exacerbate a pre-existing global routing table issue by virtue of its much larger address space, which in turn allows for a much larger scope of deployed networks, with the potential to reflect this in the size of the routing system. Simply put, the total number of routes on the Internet needs to be managed so as not to exceed the capabilities of existing equipment (*i.e.* backbone routers).[91] Technical solutions for site multihoming with IPv6 and their adoption as standards by the IETF are viewed as very important for IPv6 adoption.

Generally speaking, scalability of the routing system is seen as a major issue for the future of the Internet. Addressing and routing on the Internet are interdependent and there are significant economic considerations in devising solutions to scalable routing systems. One reason for growth in the routing table is a misalignment of economic incentives and outcomes: adding new entries or failing to aggregate existing routes may be economic or convenient for a single network operator but the cost of new entries or expansion in the routing table, however, is borne by everyone in the global routing system.[92] The issue is seen as a very high priority for the Internet in the medium-term, with further examination and discussion warranted in both the technical and economic realms.[93]

IV. ECONOMIC AND PUBLIC POLICY CONSIDERATIONS AND RECOMMENDATIONS

PUBLIC POLICY CONSIDERATIONS

Important public policy issues are associated with the smooth transition of the Internet to IPv6. These relate in part to a belief by some experts that the current IPv4-based Internet will be unable to scale to create opportunities for new connections and new services. The Internet is expected to help address challenges in areas that range from enabling new innovative services to interconnecting new types of wireless devices to support a range of economic and social objectives.

Likely scenarios, sustainability and economic growth

Governments have a special role to play in helping the transition towards IPv6 (Annex 1 presents the role of different stakeholders in the transition to IPv6 and Annex 2 provides an overview of governmental initiatives to-date). According to original plans of the Internet community, the transition of the Internet to IPv6 should have been much more advanced before the depletion of IPv4 addresses. Instead, in most countries and most companies, the transition is either just beginning, or there is still no visible activity in this area.

The three options available to networks that are growing after the depletion of previously unallocated IPv4 address space are *i)* denser deployment of NAT, *ii)* obtaining and deploying additional IPv4 infrastructure if actors gain access to previously allocated addresses, and: *iii)* IPv6 deployment (Table 9). These scenarios are not exclusive and it is likely that all three will be pursued by various actors as the depletion of previously unallocated addresses with affect actors differently (Annex 6). Experts deem that in the short term, denser NAT deployment is an inevitable response to the looming IPv4 address depletion. They also point out that as available resources diminish, actors are likely to become more efficient in the use of IPv4, particularly when there is a cost associated with obtaining address space. Therefore, operators may tend to reduce their use of public address space, most likely by making use of private address space and NAT in IPv4 and concurrent IPv6 (particularly for non-public infrastructure) wherever possible.[94] Denser NAT deployment means the associated deployment of multi-party application architectures that perform more complex operations in order to set up applications.[95] If NAT is deployed without concurrent deployment of IPv6, severe restrictions on the scalability of the Internet would appear.

It is likely that all network administrators will eventually be faced with the task of creating a plan to migrate from IPv4 to IPv6. The time at which this is done and the current infrastructure will have a significant impact on how migrations are carried out. Early adopters will require different tools and approaches than late adopters since they will have a greater need to interoperate with IPv4 networks on a large scale. Late adopters, for their part, may have the ability to more directly implement a native IPv6 infrastructure. However, experts agree that if adoption is left to the latest possible moment, this would create pressure for hurried and potentially unstable deployment of IPv6.

A number of factors – amount of IPv4 address space, speed of deployment, service offerings, and application support – will determine which transition tools are used.[96] Organisations with a large number of public IPv4 addresses will be able to use a dual-stack approach, while those with fewer addresses will need to use mechanisms for an IPv6-only internal infrastructure.[97] For organisations looking to perform testing and migrate to IPv6 only gradually, tunnelling systems may be the most appropriate mechanism.[98]

Organisations whose ISP offers native-IPv6 connectivity can use a number of tools while others will have limited options.[99] In all cases, future transition to IPv6 should be planned in today's network infrastructure and application design.

Table 9. Comparison of different scenarios to handle the exhaustion of IPv4

	USING LESS IPV4 ADDRESSES & MORE NAT	TRADING IPV4 ADDRESSES	TRANSITIONING TO IPV6
Initial impact on network configurations	• Would require additional devices and some equipment • Configurations must be reviewed	• Existing equipment can continue to be used initially • Unclear whether configurations will need to be reviewed	• Requires additional devices and some equipment would need to be updated • Network configurations must be changed entirely
Impact on users	• Difficult for users to communicate directly (*e.g.* peer-to-peer applications) • Probable interferences because people may be using the same private IPv4 address	• Need to ensure that registries have up-to-date information on usage of IPv4 blocks	• Some equipment and applications will have to be updated or modified • No limitations on use
Impact on operations	• While there is significant operational know-how, it remains unclear whether this option will work in large networks	• With mobile IPv4 addresses, the difficulty of managing addresses would continue to increase • Would require larger and more expensive routers (in some cases, requests for bigger routers cannot be supported)	• Current technicians and operational know-how are insufficient • New solutions will be needed to enable communications between IPv4 and IPv6
Costs	• Initial costs will be relatively small (however, if there is a significant increase in users, large investments may be required) • Operational costs will increase (the magnitude of which is unclear)	• Low initial costs • Potentially very significant operational costs • Significant transition costs to be able to transfer IPv4 addresses	• Initial costs will be significant • Operational costs will increase in the short term because both IPv4 and IPv6 operations will be required
Sustainability	• NAT is already in very wide use, and 170 million new IP addresses are still needed every year. • Limited because some nodes, such as servers, require unique addresses. • This option does not accommodate demand for direct end-to-end communications. • Widely considered to be a short-term solution	• Short-term measure (limited supply) • Legacy holders need to be part of a market for its viability • Signifies major change in the address management function	• Long-term solution

Source: OECD (2008), based on Telecommunications Bureau, Ministry of Internal Affairs and Communication, Japan, December 2007.

Some experts deem that business continuity and scalability of the Internet are at stake since any organisation that uses IP addresses in its growth process will be affected and since network address translation (NAT) does not scale very well.

Interoperability and competition concerns

IPv4 will not disappear; it is therefore essential that the transition strategy pursued is an integration and co-existence of IPv6 networks with IPv4. For network operators and other entities that rely on Internet numbering allocations, it will become increasingly difficult and expensive to obtain new IPv4 address space to expand their networks. A situation with anticipated scarcity of IPv4 addresses raises competition concerns in terms of barriers to new entry and strengthening incumbent positions. From a business standpoint, new or existing Internet users who need IPv4 addresses are likely to have to use private addresses with several levels of translation (NAT) and still need some quantity of public IPv4 addresses. Care must be exercised that the IPv6 transition and co-existence between IPv4 and IPv6 safeguard competition and a level playing field and do not lock in dominant positions.

As the Internet progressively becomes a dual IPv4/IPv6 network, some experts deem that ensuring *IPv6* support will be critical for retaining universal Internet connectivity. As the difficulty of obtaining IPv4 address space increases, they believe it is inevitable that some sites will only support IPv6. IPv6, therefore, will be required to ensure global connectivity. Experts stress the importance of adopting policies that will encourage IPv6 connectivity (peering and transit) among all Internet service providers.[100]

Security

Security is an important public policy objective. Maintaining network security will continue to be a challenging undertaking in both IPv4 and IPv6 contexts. In relation to IPv4 and IPv6, the following points should be highlighted:

- Legal intercept and identification are easier with IPv6 in the absence of NATs and in particular, several layers of NATs.[101]
- Because a number of new operating systems use IPv6 as a default, IPv6-enabled devices are likely to increasingly find their way into commercial and governmental networks, creating security vulnerabilities in the absence of adequate training.
- Debates concerning IPv4 versus IPv6 security often focus on different aspects of network deployment. The IPsec protocol suite works generally the same way in both IPv4 and IPv6. While IPv6 potentially facilitates deployment of end-to-end security, in practice, NATs will continue to be deployed.
- Because the IPv6 protocol is different from IPv4, it creates opportunities for new types of attacks. IPv6 products being comparatively new, they have not benefited from the recurring cycle of discovering and fixing security vulnerabilities and other bugs yet.
- In addition, the dual-stack IPv4 and IPv6 environment will require the development of new operational practices.

REQUIRED FOCUS OF PUBLIC POLICY EFFORTS

Planning for IPv6 compatible government services, and skills

Governments have an important role to play as a major consumer of IP-related products and services. As all other stakeholders, governments need continued addresses to support growth in scale and scope of the public services that they provide on line and to support the evolution of their internal networks. They therefore have a strategic need to consider adopting IPv6 to accommodate future growth in the services they offer and their operations. Japan, Korea, the United States and China are transitioning their e-government networks and services (See section III. Drivers and challenges of IPv6 deployment: Public procurement mandates). Australia and several European countries are also launching public sector transition plans. The main reasons for which Australia is planning for IPv6-compatible government services, and which are generally applicable to all governments, are summarised below (Box 7).

Beyond building IPv6 skills and applications within governmental bodies, public procurement mandates also lead to a virtuous cycle of adoption by instigating the development of skills within technology partners. Expertise takes significant time to develop and the current expertise in IPv6 of network engineers is deemed to be insufficient to meet the needs of the transition to IPv6 in many countries. Policies aimed at ensuring a sufficient skills base exists, for the implementation of IPv6, are critical.

Box 7. Why plan for the transition to IPv6 now?

There are several reasons for starting the planning process and thereby not leaving it until industry and other external pressures build and introduce additional risks and costs.

1. The risk that unplanned and uncontrolled implementation of IPv6 equipment into government networks could result in failures and loss of service delivery capability.

2. The risk that the skills shortage in the ICT arena and in particular, the IPv6 field becomes so great that the government will not be able to compete with the private sector for IPv6 skilled technical and administrative staff.

3. The opportunities for increased service delivery, particularly in the health, environment and transport industries, that IPv6 will allow with its ability to have multiple sensor/tracking devices in a variety of fields.

4. The fact that many other countries, including the United States, Japan, Korea, Australia and many European nations are all moving down this path.

5. The risk that the cost of moving to IPv6 when industry and suppliers are driving the market will be significantly greater than if the planning and transition stages are undertaken in an environment of controlled progress.

Source: Adapted from A Strategy for the Transition to IPv6 for Australian Government agencies, 'Building Capacity for Future Innovation', AGIMO, October 2007.[102]

Governments should pro-actively take initiatives to address skills shortages with IPv6 training efforts in university-level education cycles as well as ensuring lifelong education opportunities, *i.e.* include IPv6 in computer networking, software design, or security programs for the following reasons: *i)* countries' and companies' experience and knowledge of IPv6 are likely to become competitive assets in realising continued growth of the social and economic benefits enabled by the Internet since existence of IPv6 expertise among computer scientists and networking engineers is key to successful transitions; *ii)* the open market faces explicit training costs in the absence of graduates trained in IPv6. Many companies, such as Comcast or NTT Communications, have identified lack of IPv6 skills as a major challenge; and *iii)* IPv6 expertise pools will provide employment opportunities.

Awareness raising

Taking part in building awareness and helping to minimise potential barriers is an important role for governments, to complement current initiatives by private sector actors. Awareness raising of the upcoming issue has begun in all technical numbering fora, in many technical standardisation groups as well as within network operator groups. Significantly scaled-up efforts are needed to ensure that all those who depend on IP addresses, starting with Local Internet Registries, are well aware of the upcoming exhaustion of previously unallocated IPv4 addresses, its timeframe and its likely impacts. While a number of resources exist to provide information to network managers, more resources should be broad, user-friendly and comprehensive, such that they can be understood by stakeholders of the Internet economy at large: from governments through business decision makers through to more technical or operational audiences.

Government initiatives to increase awareness and prioritisation of IPv6 have included, for example, public statements and integrating IPv6 into strategic plans for the development of networks in their countries. Some countries have created agencies with the mission to promote IPv6 and facilitate its adoption by diffusing knowledge. Those agencies actively liaise with private sector parties so as to share experience and good practice, help to increase awareness of the issues and of the potential of IPv6, as well as liaise with industry on developments in the IPv6 commercial arena.

Monitoring progress

Countries and organisations should track their progress in the transition from IPv4 to IPv6. Such monitoring will enable the compilation of case-studies along with "lessons learned" to assist in transition education and best practices development. In addition, monitoring will enable comparative analyses to be carried out over time with respect to the economic drivers for the transition and to its economic impact.

Box 8. Summary of key economic considerations related to IPv6 implementation and development

ECONOMIC CONSIDERATIONS FROM INDIVIDUAL ORGANISATIONS' PERSPECTIVES:

● **Business continuity and necessary time of transition:** because implementing IPv6 takes time, planning IP addressing needs over the next few years can enable organisations to devise and implement optimal strategies to ensure continued growth and operations after IPv4 address exhaustion.

● **Cost**: Ipv6 implementation costs vary significantly in function of requirements and deployment plan (*e.g.* internal versus external, peering, transit, DNS, provision to the desktop, web services, hosted services etc.). Experts deem that in the medium or long term, IPv6 can potentially reduce operational expenditure for network administration. However, in the early stages IPv6 implementation is likely to increase capital and operational expenditures, due to:

- Internal training and skills upgrading.
- Costs of running dual-stack interoperability; and
- Potential lack of vendor and back-office tool support, increased hardware costs or upstream transit.

● **Initial presence of negative externalities**: Initially, economic actors bearing the cost of NAT may not be those who need to invest in IPv6 deployment. With time, such negative externalities should give way to (positive) network effects for those who invested, as increasing numbers of economic actors implement IPv6 and an adoption "tipping point" takes place.

● **Universal Internet connectivity:** IPv6 is projected to become critical for retaining universal Internet connectivity, which is in the interest of many organizations.

● **Scalability and demand for IP addresses**: IPv6 can provide the necessary scalability for growth of organisations, *e.g.* for mobile providers to offer always-on Internet access via mobile devices, or for service providers to benefit from more IP numbers to offer triple play services.

● **Innovative applications and services**: IPv6 enables new services which cannot be implemented with IPv4, *e.g.* remotely accessible sensor network applications / machine-to-machine communications.

● **Competitive advantage:** operational experience with IPv6 is likely to be a competitive advantage in some industries.

ECONOMIC CONSIDERATIONS FROM A PUBLIC POLICY PERSPECTIVE

● **Platform for innovation:** IPv6 provides a platform for innovation in Internet-based products and services, in particular to meet medium and long-term requirements of an increasingly mobile, wireless and ubiquitous Internet.

● **Growth and competition:** IPv6 is necessary to foster an environment capable of sustaining long-term growth of the Internet economy and competition across existing players and new entrants.

● **Competitive advantage**: IPv6 expertise is likely to be key for economies to remain competitive in the production of technology products and services.

V. CASE STUDIES OF DEPLOYING IPV6

This section of the report aims to show the rationale for a few selected IPv6 implementations. In what follows, case studies for Comcast, Bechtel Corporation, NTT Communications and Google are considered. A further source of information beyond the case studies below is the IPv6 Forum. The IPv6 Forum has actively promoted IPv6 since 1999: with chapters in 46 countries, it has conducted numerous case studies of IPv6 implementations.[103]

Several important lessons were highlighted independently by these four different organisations: planning ahead is viewed as the single most important factor in transitioning to IPv6. Challenges to transition were considered as reasonable, and costs were mainly those of labour and of training staff to develop expertise. For both NTT and Comcast, two large Internet service providers, a major benefit of IPv6 adoption is considered to be the decreased complexity of their networks and associated reduction of support costs. In all four cases, IPv6 is enabling these firms to plan new services and applications that draw on the possibility to have a locally or globally routable Internet address for any device.

Comcast

Comcast was founded in 1963, as a cable television operator, and is today the largest cable communications operator in the United States, with operations in 23 States. The growth of Comcast's customer and service base illustrates how an organisation can be constrained by insufficient IPv4 address space.

Comcast remotely manages and operates its private network, *i.e.* the cable modems, set-top boxes and voice adaptors of all its customers, with IP technology. All Comcast customer devices are identified and managed with one or more IP address. The largest block of IPv4 addresses reserved for private networks provides 16.7 million addresses theoretically.[104] Comcast was using private IPv4 space to manage the cable modems but realised in 2005 that, with new customers subscribing to its services, it was going to run out of private space.

Simple projections showed Comcast that the quantity of IP addresses that it would need in order to support its future growth in terms of subscriber base, as well as to be able to leverage potential new services, exceeded available address space. In fact, estimations were that within a few years, Comcast would have some 20 million video customers, an average of 2.5 set-top boxes per customer, and 2 IP addresses per box. This would mean that the company would be in need of some 100 million IP addresses at a minimum.

Reviewing its potential options, Comcast concluded that IPv6 was the best solution to facilitate its management of a growing network to ensure business continuity. In addition, the company considered that it would potentially be able to leverage IPv6 in its service offerings, such as its "triple play services" (Table 10), that it foresaw might grow to require several hundreds of millions of addresses.

Table 10. Triple play effect on the use of IP addresses

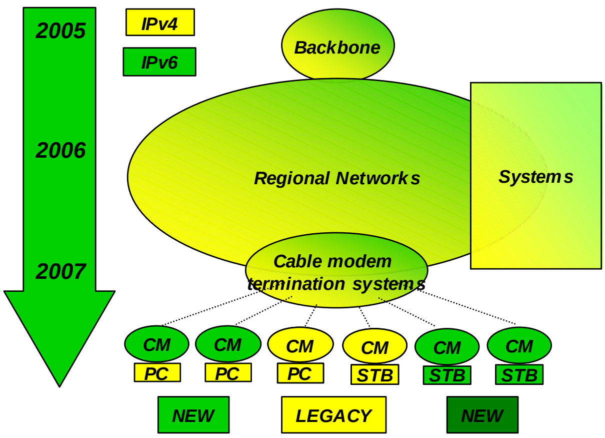
	2005 high speed data	2006+ Triple Play
Cable Modem	1 (private)	1
Home Computer / Router	1	1
Voice adaptor (embedded Multimedia Terminal Adapter)	0	1-2
Set Top Box (STB) 0 2	0	2
Total number of IP addresses (assume 2.5 STB per household)	**1-2**	**8-9**

Source: Comcast – Nanog37: Managing 100+ million IP addresses.[105]

Comcast's primary objective was to use IPv6 for the IP addresses of the cable modems and set-top boxes, with minimal disruption. To this end, dual-stack was incrementally implemented in the core networks: *i)* in the backbone (2006); *ii)* in the converged regional area network (2007) and; *iii)* in the cable modem termination system used to provide high speed data services. Challenges encountered by Comcast included the limited availability of IPv6 cable modems, IPv6 home gateways, video, and voice systems on the consumer electronic retail market. Adapting back office systems – the provisioning and monitoring systems that would have to communicate with potentially IPv6-only systems – proved to be particularly challenging.

A noteworthy aspect of the strategy is that of starting IPv6 deployment from the dual-stack core and deploying IPv6 step-by-step towards edge devices. By including IPv6 in its roadmap for new generation equipment and devices, Comcast greatly minimised transition costs. It then tested offering new services to its customers based on IPv6. Newly installed customer devices are planned to be IPv6-only, since managing dual-stack end user devices would be expensive and defeat the purpose: the edge of the network is where Comcast may have potentially several millions of devices to manage and therefore where IP addresses are needed. Dual stack for millions of devices would be complex to manage and to support, and prohibitively expensive: it would need to involve IPv6 addresses, IPv4 addresses, network address translators and various gateways etc. Comcast's strategy to deploy native IPv6 where possible and to update only those IPv4 systems that manipulate or interact with IPv6 data is pictured in Figure 10.

Figure 10. Comcast's deployment strategy



Source: Based on Comcast presentation at Nanog 37.

Training is a critical part of deploying IPv6. Internally, the company focused on diffusing IPv6 knowledge widely among its staff and at various technical levels. While the cost, operationally, of renumbering all the modems was high, it was inevitable with any of the options the company could have chosen. Knowledge was that with IPv6, renumbering would be needed only once and be able to scale to accommodate growth needs in the foreseeable future. Key lessons learned are summarised in Table 11.

While Comcast is the first known case of a service provider having run out of private address space, similar situations are likely to occur with other service providers in the near future. Other very large cable operators are already starting to investigate various options and their implications. The primary lesson from Comcast's transition to IPv6 is the importance of planning ahead. For Comcast, limited scale deployment will have taken some four years. The costs were not major, because deployment was gradual.

Table 11. Lessons learned

TO DO	TO AVOID
• Plan deployment carefully • Use IPv6 only where required • Conduct extensive training on IPv6 • Focus on the application layer rather than on the network layer • Include IPv6 in the roadmap of equipment life cycle • Deploy IPv6-only at the edges, where a dual-stack environment is non practicable for millions of devices, due to lack of IPv4 address space	• Dual stack deployment everywhere • Wait and rush

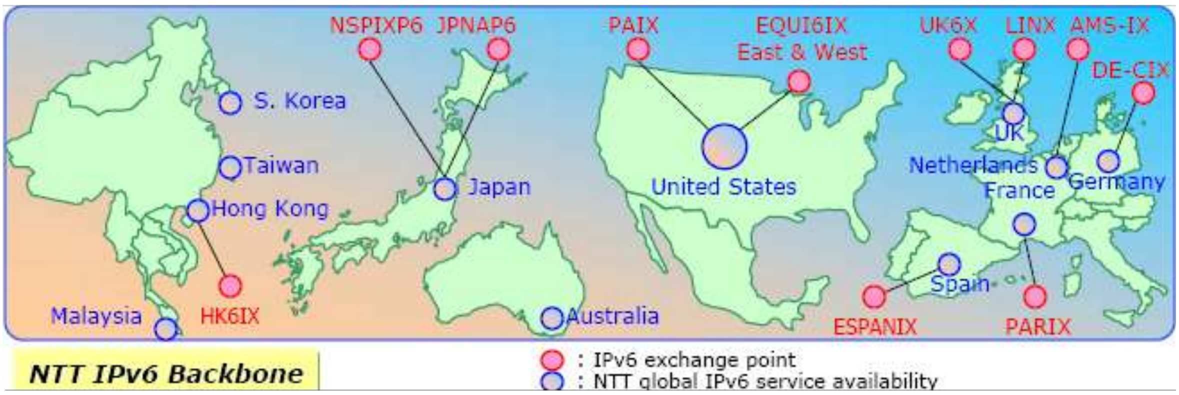
Source: Based on IPv6 Forum case study.

Another take-away message from the Comcast case is that beyond what the company has already implemented, it is now able to plan for new services to offer home networks. Comcast expects that these home networks will require smart gateways with features and services equipped to handle numerous IP devices, multiple types of links with varying characteristics (wired/wireless, different speeds, multi-cast support), as well as additional services such as home automation, network storage or video communications.

NTT Communications

NTT Communications began offering IPv6 Internet service in April 2001, leading the world in the provision of commercial IPv6 Internet connection services, both to enterprises and home users.[106] One of the largest ISPs in Japan, NTT Communications, provides several commercial IPv6 services. The company has been operating a worldwide native commercial IPv6 backbone along with an IPv6-over-IPv4 tunnel connection service since 2001 (Figure 11).

Figure 11. NTT Global IPv6 backbone and services

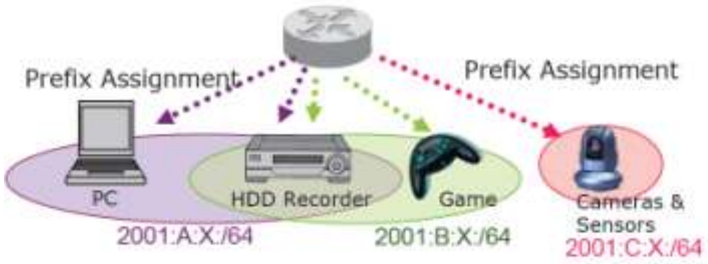


Source: NTT Communications.

Dual stack (IPv4 and IPv6) ADSL services have been offered since 2002. In addition, NTT Com has operated a dual-stack IPv6/IPv4 backbone connection since 2004. Since 2005, NTT Com has provided dual-stack Ethernet access (*e.g.* for fibre) for enterprise users. And NTT Com's 5 million residential subscribers can easily turn on IPv6 tunnel access to remotely access and control electric appliances connected to their home network (Figure 12).[107]

Applications in private IPv6 networks are where the company is seeing strong growth, compared to access to the IPv6 Internet.[108] The company says that from the time it began offering IPv6 services, users have benefited from business opportunities in using it and that IPv6 services are now profitable to the company.

Figure 12. NTT Home Network ("OCN IPv6")



Source: Asia Pacific IPv6Summit 2007, *How and Why have millions of households been already IPv6 ready?*[109]

An NTT subsidiary, NTT West, started offering IPv6 Internet Access service in 2005. The service includes an IPv6 service network, which is a private multicast-enabled network and services nearly two million customers. An observer reports that customers are generally not even aware of the fact that they are using IPv6.[110] The major reasons cited by NTT West for deploying IPv6 include ease of manageability, business continuity, as well as the multicast functionalities of IPv6 that NTT needed to provide video streaming services.

Multicast functionality – which allows for one data stream to be sent to multiple recipients, as opposed to unicast where there is one stream per recipient – is also used by NTT for new applications. An innovative service that NTT offers is its "Earthquake Flash Report System". The system reports in real time on the intensity of an earthquake and on the exact time it will take to reach a specific location, thanks to over 1 000 sensors spread out through the countryside, all connected via IPv6.[111] When the sensors detect an earthquake, they transmit the data to both government agencies and commercial utilities so appropriate action can be taken. Preventive steps can be taken in the 10 to 15 seconds before the second real earthquake wave hits people, buildings and the city/community infrastructure. This system can be developed to send a flash TV emergency news, initiate automated fire-suppression systems, to automatically stop elevators, close natural gas and petroleum pipeline valves, etc.

Bechtel Corporation

Bechtel Corporation is a large global engineering, construction, and project management company that was an early adopter of IPv6. Bechtel's pace of adoption was influenced by several drivers. First among these were the 2003 mandate of the US Department of Defense (DoD) and 2005 mandate by the United States Office of Management and Budget (OMB) which required department-wide deployment of IPv6 by 2008. Requests for proposals from the US Army and other customers started to explicitly require IPv6 products and services.[112] Another driver was that IPv6 is the default in current Windows Vista and emerging Windows Server 2008 Microsoft operating systems that are deployed in Bechtel.[113] Additionally, Bechtel views IPv6 as a significant foundation for future innovation. Bechtel is exploring opportunities to capitalise on IPv6 features to improve its project execution and operational efficiencies over time. The last driver is the broad adoption of IPv6 in industry standards as a required part of emerging products and services, for example in the standards DOCSIS 3.0 and IMS (IP Multimedia Subsystem).

In 2004, Bechtel launched a phased, enterprise-wide deployment of IPv6 spanning over eight years that was designed to develop broad awareness and competence in the new protocol across the firm. The approach has yielded growing implementations of production IPv6 services across the enterprise. The company started its deployment by sending dozens of network engineers to in-depth IPv6 training courses and created IPv6 labs that interconnected them across the Internet. Bechtel then started to integrate IPv6 into the company's existing product and service lifecycle processes, paying particular attention to turnover packages and verification processes as applications and infrastructure components moved from development through quality assurance and into production. The environment and building templates have been instrumented to provide deployment metrics and consistent IPv6 deployment look and feel. Most of the applications were not affected by adding IPv6 to the existing IPv4 network. However, the company felt that many of the carriers it solicited in the United States lagged in terms of offering adequate enterprise IPv6 communications transport to the premise.

By the end of 2006, Bechtel had enabled IPv6 on its production networks and on hundreds of computers at four of its primary sites, and created a scalable model for future deployments. The company trained all its application developers to be able to configure machines for IPv6. Bechtel has included IPv6 compatibility in its regular application-development and quality-assurance processes. By the end of 2007, Bechtel expects that over 80% of its 18 000 company-managed computers and 50% of its routers and switches will be running in a dual-stack (IPv4/IPv6) mode. All major offices are already running IPv6 on most computers and all local area network (LAN) and wide area network (WAN) connections (Figure 13).

Figure 13. Project highlights (March 2006)

Source: IPv6 Transition at Bechtel, presented by Fred Wettling, February 2007.[114]

Bechtel is interested in a range of applications using IPv6 for projects on different types of construction activities – mines, treatment plants, or power plants – across the world. The company hopes to leverage IPv6 peer discovery and peer-to-peer communications to enable the rapid deployment of project IT infrastructure as well as *ad hoc* collaboration with its partners in projects. The mobility features of IPv6 enable wireless routers in trailers at project sites to set-up "self-configuring/self-healing" networks with secure voice, data, and video.

Bechtel also sees future utility in using distributed environmental sensors to provide weather monitoring, such as on bridges, in high buildings, on large cranes, etc. In the area of communications in the field, the company wants to enable communications between employees through point-to-point and broadcast features of IPv6. Being able to track construction workers on sites for security reasons, by adding Global Positioning System (GPS) and Radio Frequency Identification (RFID) to its mobile IPv6, is also on the list of applications for Bechtel to deploy.

Google

Google provides search technologies used by millions of people every day to query online information – Web, Usenet, images, and other types of content such as videos. Google's business model relies on targeted advertising.

There are several drivers for the company to implement IPv6. Many individual engineers at Google felt that it was important for the future of the Internet and for the company to be a leader in the area. Originally a project undertaken in staff's free time, IPv6 deployment is becoming an official project. Another reason cited included the US Department of Defense and Office of Management and Budget mandates: Google wants to be able to crawl public sector IPv6 content once federal agencies are using IPv6. Google also anticipates the adoption of IPv6 in countries such as China or Japan. A last driver for the deployment of IPv6 is the company's own growth and the considerable efforts required to efficiently manage IPv4 address space while constantly adding new offices and data centers.

Google started to consult vendors in 2004 and received a "/32" IPv6 delegation from ARIN in 2005. Google then started to build out its IPv6 peering. Within the Internet technical community, Google was issued a challenge by the Chair of the IETF's IPv6 Working Group that it would have working IPv6 search functionality by November 2008, at the IETF's 73rd meeting.

There are three facets to Google's IPv6 deployment:

1. Production networking infrastructure *i.e.* peering and transit, whereby IPv6 is stretched to each data centre.
2. Corporate deployment, for all Google's internal networks and staff to be using IPv6; and
3. Deploying IPv6 in Google's software and services including gmail, search, or Google maps in production quality.

As a top web property, Google is extremely sensitive to latency, *i.e.* the amount of time it takes a packet to travel from source to destination. The lower the latency, the quicker a web page loads, so that Google puts intensive effort into measuring and improving latency. Large numbers of servers and data centers around the world provide redundancy and reduce latency to each user by ensuring that the requested data is always online. If an end user's operating system – Windows Vista for example – defaults to IPv6, delays and problems in loading web pages are more likely than with IPv4 because of IPv6's incomplete connectivity.

To ensure that service over IPv4 is not affected, Google is likely to use a separate domain name for its IPv6 service, which is not attractive from a branding perspective but ensures complete separation from IPv4-only service. Since IPv6 infrastructure must be built so that it does not affect any IPv4 traffic, separate routers and separate bandwidth are needed in some cases and some capital outlay is required.

Another challenge for Google is that in its search for minimal latency, it has been implementing very fast IPv4 Application Specific Integrated Circuits (ASIC) chips but few vendors offer similar performance in their IPv6 hardware offering yet.

Significant investments in time are needed to adapt/recode all the tools that measure IPv4 performance so that they can also measure IPv6 performance. A large portion of the infrastructure and of the computer code can be reused but most of the transition work lies in experimentation (creating, measuring etc.) and Google is developing an extensive IPv6 compliance and testing suite and monitoring tools, including IPv6 traffic monitoring, a latency map of IPv6 traffic, and tracking IPv6 adoption in web servers over time.

ACRONYMS / GLOSSARY

3G	Third generation mobile communications system
3GPP	3rd Generation Partnership Project
AfriNIC	African Region Network Information Centre
Aggregation	Aggregation refers to the distribution of public Internet addresses in a hierarchical manner, to permit the grouping of routing information and limit the number of routing entries advertised in the Internet. Aggregation is one of the main goals of Internet administration.
Allocation	Allocation refers to the range of addresses made available to a Local Internet Registry (LIR) that in turn is used by the LIR to make address space assignments to End Users or to the LIR's own network.
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
Assignment	An assignment refers to address space that a Local Internet Registry (LIR) distributes to an End User / organisation that will use the addresses to operate their specific network(s)
AS	Autonomous System - a group of IP networks operated by one or more network operators that has a single and clearly defined external routing policy
ASIC	Application Specific Integrated Circuits
ASO	ICANN’s Address Supporting Organisation
BGP	Border Gateway Protocol
ccTLD	Country Code Top-Level Domain
CERNET	China Education and Research Network
CIDR	Classless Inter-Domain Routing
CNNIC	China Internet Network Information Center
DNS	Domain Name System
DoD	US Department of Defense
DSL	Digital Subscriber Line technologies, including ADSL
Dual Stack	Concurrent service for IPv4 and IPv6 protocol stacks
End User	An entity receiving assignments of IP addresses exclusively for use in operational networks, not for reassignment to other organisations
GAC	Governmental Advisory Committee to ICANN
GENI	Global Environment for Networking Innovations
GPS	Global Positioning System
gTLDs	Generic Top-Level Domain
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
Interoperability	The ability of two devices, usually from different vendors, to work together

IP	Internet Protocol
IP Whois	Identifies the owner and the IP address of the domain
IPng	Internet Protocol – Next Generation
IPTV	IP television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPv6 capable node	Node that has an IPv6 protocol stack. In order for the stack to be usable the node must be assigned one or more IPv6 addresses
IPv6 enabled node	A node which has an IPv6 protocol stack and is assigned one or more IPv6 addresses. Both IPv6-only and IPv6/IPv4 nodes are IPv6 enabled
ISP	Internet Service Provider
ITU	International Telecommunications Union
IXPs	Internet eXchange Points
JPNIC	Japan Network Information Center
LACNIC	Latin America and Caribbean Network Information Centre
LAN	Local Area Network
LIRs	Local Internet Registry
MIPv6	Mobile IPv6
Multihomed	A network that has its own public IP address range, an AS number and a connection to two (or more) separate ISPs
NAT	Network Address Translation
NIR	National Internet registry
NIST	US National Institute of Standards and Technology
Node	Device that is connected as part of a computer network
NRO	Number Resource Organisation
OMB	United States Office of Management and Budget
Peer-to-peer	Communication model in which client devices may communicate directly, initiating the data exchange in either direction, without a server system
PI	Provider Independent
Prefix	Hierarchical, aggregated block of addresses for a network
RFC	Request for Comments
RFID	Radio Frequency Identification
RIPE NCC	Réseaux IP Européens-Network Coordination Centre
RIR	Regional Internet Registry
Routability	A block of addresses being identified as a separate entity in the routing tables and is therefore reachable in the Internet
RSA	Registration Services Agreement
SIP	Session Initiation Protocol
TLD	Top-Level Domain
UMTS	The third generation mobile communications system (see 3G)
VoIP	Voice over IP. Using an IP network to carry voice
WAN	Wide Area Network

ANNEXES

ANNEX 1: OVERVIEW OF GOVERNMENTAL INITIATIVES TO-DATE

Japan

WIDE, (Widely Integrated Distributed Environment) established in 1988 is a joint industry, government and academia research consortium that promotes the research and development of Internet technologies. Represented by Jun Murai, Vice President of Keio University and Professor of the Faculty of Environmental Information, over 100 corporations and 40 universities are currently involved in the WIDE Project. They partake in a diverse array of research and development activities concerning next generation Internet technologies.

In 2000 Japan's Prime Minister told Parliament that IPv6 was to be the core of future deployment of the Internet in the country. In January 2001, Japan was the first country to put forth a national strategy for the adoption of IPv6, e-Japan.[115] It consisted of support for academic research through the WIDE project, development of new applications, as well as tax incentives between 2001 and 2003 for organisations that deploy IPv6. Japan's investment in IPv6 is estimated at between USD 10 to USD 13 million a year. To-date, Japan is the leading country in IPv6 expertise and has the largest commercial deployments of IPv6.[116] Japan's strategy has largely been supply-driven.

The Japanese government has supported the establishment of an IPv6 Promotion Council in Japan to facilitate the resolution of issues related to development and deployment and has provided tax incentives to promote deployment. In parallel, major Japanese corporations in the communications and consumer electronics sectors are developing IPv6 networks and products. Many commercial IPv6 offerings exist in Japan.[117]

In Japan's "New IT Reform Strategy" that was released in January 2006, a time frame to become IPv6-ready was set, "as information and communications hardware is updated and replaced in the future, new equipment will as a general rule be IPv6 compatible by 2008." Each ministry and government agency continues its efforts to become IPv6-ready. [118]

In August 2007, the Japanese MIC announced in that it was convening a study group on Internet's smooth transition to IPv6 in order to study measures to facilitate the transition of domestic Internet networks to IPv6 from a technical perspective. [119]

Europe and the European Commission

European technology experts have been involved in the definition and development of IPv6 since the beginning. A RIPE WG in this area has been active since April 1994.[120] The European Commission initiated a task force in April 2001 to design an IPv6 Roadmap. The Roadmap was to serve as an update and plan of action for the development and future perspectives of IPv6. It was also to serve as a way to co-ordinate European efforts for developing, testing, and deploying IPv6.

In 2002, the European Commission issued a Communication from the Commission to the Council and the European Parliament on the "Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6"[121] stating that "a strategic concerted effort is … required that will enable the competitiveness of the European industry to be strengthened". [122] The Commission is currently examining ways to accelerate roll-out, possibly through procurement, policy and research activities, and dissemination efforts.

The European Commission (EC) dedicated some USD 216 million to several research projects (6NET, GEANT, Euro6IX, 6INIT) with the goal of instigating deployment experience, protocol expertise and new applications. The EC also brought together Universities and industry partners from around the world into various collaborative efforts.

Latin America

Latin America has also begun developing projects involving IPv6. For example, the National Autonomous University of Mexico has been conducting research to provide IPv6-enabled service to Mexico and Latin America.

United States

In June 2003, the United States Department of Defense (DoD) mandated the integration of IPv6 to be ready by 2008.[123] The Department of Defense's transition to IPv6 is a key component of its business case to be able to architect new technologies and to improve interoperability among many information and weapons systems, known as the Global Information Grid (GIG). The IPv6 component of GIG is to facilitate DOD's goal of achieving network-centric operations by exploiting these key characteristics of IPv6. The increased address space provides DOD with an opportunity to reconstitute its address space architecture to better address the future proliferation of numerous unmanned sensors and mobile assets.[124]

In June 2005, the United States' Office of Management Budget (OMB) set June 2008 as the deadline by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must be interfacing with this infrastructure.[125]

Korea

In February 2001, the Korean Ministry of Information and Communications established a plan entitled "Next Internet Infrastructure Constructing Plan by Diffusing IPv6".

In Korea, USD 81 million were invested to support several national research projects including KOREN, KREONET2, 6NGIX and TEIN (Trans Eurasia Information Network). In 2004, Korea launched its "all IPv6" development plan named IT839 and a nationwide trial service, "KOREAv6 Project".

The current targets set by the Korean Ministry of Information and Communication (MIC) to encourage the use of IPv6 include:

- Converting Internet equipment in public institutions to IPv6 by 2010.
- Securing a user base of 10 million IPv6 users by 2010, in partnership with operators and equipment vendors: a major driver is expected to come from the creation of an "IPv6-based User Created Content (UCC) portal service" to allow users to send UCC in real time through mobile terminals such as IPv6 network cameras.

- Providing commercial service, by converting the backbone equipment of the commercial telecommunications network to support IPv6 by 2010 and of the commercial telecommunications’ access network to equipment that supports IPv6 by 2013.
- Installing IPv6 equipment in every newly built telecommunications network.
- Converting the research network to IPv6 by 2008, and using the network as a test-bed for telecommunication equipment companies and Internet service providers.
- Building a co-operative relationship between the public and private sectors for the development and spread of IPv6-based application services; and
- Reviewing related rules and regulations, including the rules for IP address and domain name management, with a view to fostering the deployment of IPv6.

As of September 2007, Korea's Ministry of Information and Communication (MIC) will begin providing general users with various IPv6-based services that utilise recently spotlighted Internet technologies such as Wideband Code Division Multiple Access (WCDMA), Voice over IP (VoIP), and Ubiquitous Sensor Networks (USN).

China

The 2008 Olympics, to be held in Beijing, are planned to serve as a wide-scale IPv6 demonstration involving portable devices, intelligent transport systems (ITS), security, and 3G IPv6 mobile services.

China’s strategy for the promotion and adoption of IPv6 is based on the development of an IPv6 backbone network, China Next Generation Internet (CNGI), designed to be the core of China’s Internet infrastructure. CNGI intends to foster the development of IPv6 expertise, and of IPv6-enabled products and applications. CNGI involves many branches of the Chinese government that invested USD 170 million, private sector communication service providers with a matching investment, and academia.

CNGI is described as a nationwide demonstration platform and large-scale test bed for IPv6 SIP (Session Initiation Protocol), providing peer-to-peer communication, wireless and mobile applications, computing grid and data grid, video conference and HDTV (high definition television), environment measurement, visual surveillance, remote control of instrument and virtual reality, advanced manufacturing, remote education and digital library and remote medical treatment.

The strategy, outlined in China’s latest five-year plan, calls for the country to transition its economy from one based almost entirely on manufacturing to one that produces its own scientific and technological breakthroughs — using a new and improved version of today’s dominant innovation platform, the Internet. IPv6 is at the heart of CNGI.

ANNEX 2: ROLES OF DIFFERENT STAKEHOLDERS

Among actors that form the Internet's ecosystem, stakeholders with a particularly important role to play in the deployment of IPv6 include:

- Backbone network operators, who manage global networks.
- Internet Service Providers (ISPs) of fixed and mobile IP networks.
- Standardisation bodies, and the individuals and organisations that contribute to them.
- The IPv6 Forum and national chapters throughout the world, for the training and the sharing of best practices that they conduct.
- Regional Internet Registries that provide stewardship for IP address allocation.
- Local Internet Registries that manage IP addresses on the collection of some 26 000 autonomous systems that together form the Internet.
- ICANN, which conducts technical co-ordination for Internet parameters, including IP addresses.
- The Internet Society, which is the organisational home for the Internet Engineering Task Force and Internet Architecture Board, and itself strives to play a unique and neutral role of fostering co-ordination among the Internet constituencies including the Regional Internet Registries.
- Governments and public sector organisations that have a special role in helping to establish the enabling environment for long-term economic and social goals.
- Equipment, software and service vendors, who develop the products and services that require IPv6 support.
- Research and education networks, which have accumulated IPv6 experience and expertise.
- Domain name system operators, Internet exchange points.
- All public and private managers of IP networks, including those with experience in managing IPv6, who are willing to share best practices and lessons learned.

Successes and limitations of ongoing action

Efforts by these participants have been underway in the technical and business realms to develop solutions to a myriad of issues, to raise awareness, to find ways of measuring deployment, test and debug production solutions. For example:

- Many RFCs and websites exist to assist network managers in managing this protocol transition.
- The RIRs and individual researchers track, measure and publish data and analysis that enables others to understand portions of complex dynamics.
- The IPv6 Forum and its regional and national iterations train large numbers of engineers on IPv6.
- Governments in many countries have made important efforts to understand the stakes and invest in solutions.
- RIRs are developing a certification mechanism which could provide significant benefits to more stable and more secure network operation, and a potential transfer mechanism at a later stage.
- Network operators are making efforts to assess their future requirements and whether IPv6 can provide a cost-effective solution to help ensure business continuity.

ANNEX 3: PUBLICLY FUNDED RESEARCH AND DEVELOPMENT INITIATIVES

The first noteworthy experimental network was the 6bone Network, which ceased operation on 6 June 2006 after almost a decade. The 6bone was a worldwide network comprising many types of organisations (including academic and government organisations, hardware and software vendors, and service providers), with oversight from the IETF NGtrans (IPv6 Transition) working group within the IETF. It started out as a way to transport IPv6 packets over the existing IPv4-based Internet using a process called tunnelling, and later evolved into a network that supported IPv6 directly.

Investing in experimental networks to provide verifiable IPv6 experience helps develop experience and expertise. Cross-fertilisation between research and development and the private sector should be a priority. Technical experts with experience from R&D networks are able to train others in order to increase the skills base by orders of magnitude. Many major wide-area publicly funded research and development networks have been running IPv6 infrastructure, services, and applications over the last few years. Some examples are:

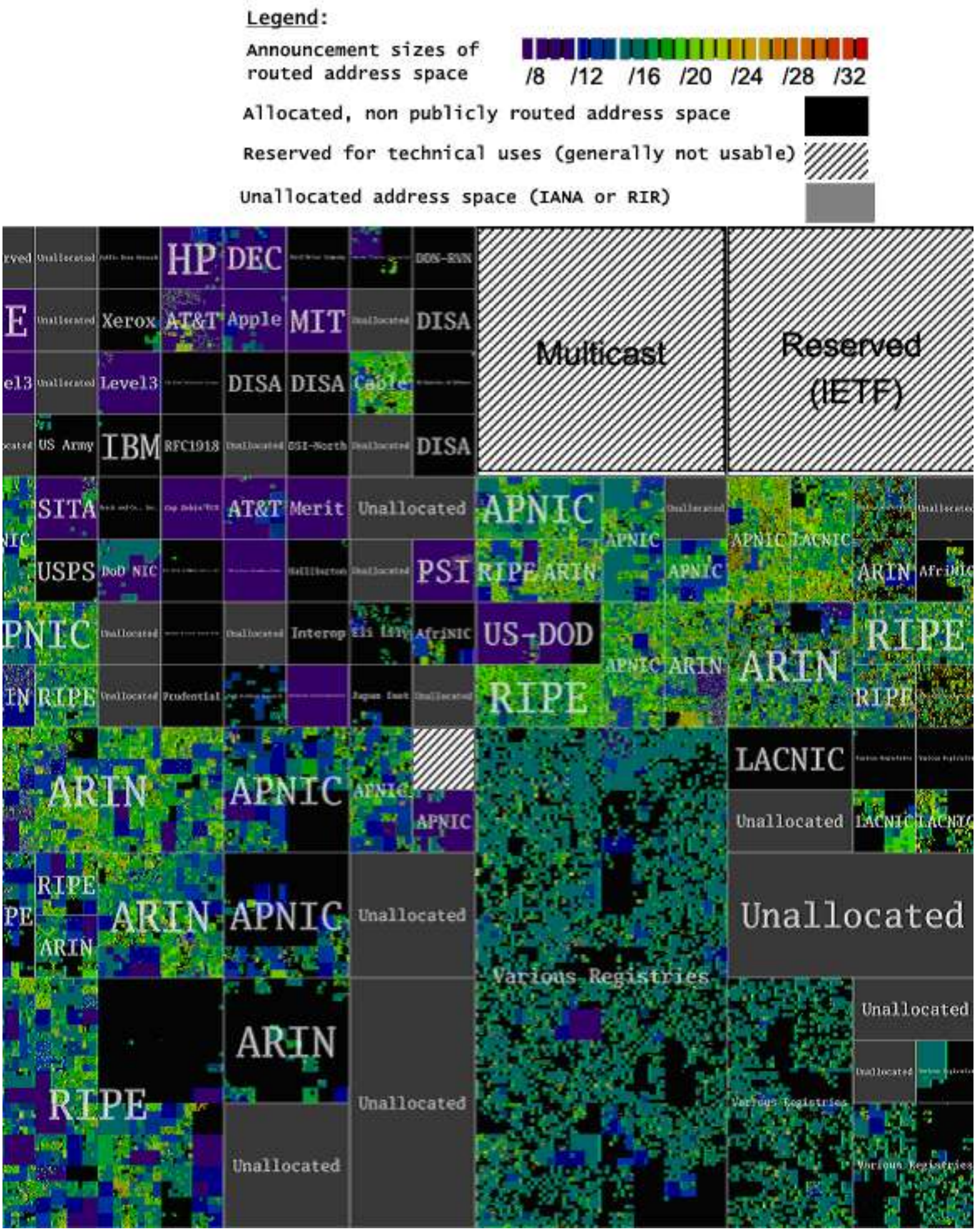
- Australian Academic and Research Network (AARNET) or Grangenet in Australia
- IPv6 Research and Education Network (6REN), Moonv6, Abilene (Internet2) in the United States
- Education and Research Network (ERNET) in India
- SURFnet in the Netherlands
- CSTNet2, China Education and Research Network (CERNET2), China Next Generation Internet (CNGI) in China
- Gigabit European Academic Network (GEANT), 6NET, 6DISS, Euro6IX and all European National Research Network (NRNs) in Europe
- JGN2 and Widely Integrated Distributed Environment (WIDE) in Japan
- Korea Research Environment Open Network 2 (KREONET2), 6NGIX and TEIN (Trans Eurasia Information Network) and the KOREAv6 Project in Korea
- RedCLARA in Latin America
- RUNet and FREEnet in Russia
- Viagenie/CANARIE in Canada
- TANET2 and TWAREN in Chinese Taipei

A number of governmental authorities have actively promoted sector-specific IPv6 applications. These include, for example:

• Applications using IPv6-based 3G mobile services and connectivity for transportation applications: trains, cars, airplanes • Peer-to-peer communication • Computing grid and data grid • Video conference and HDTV (high definition television)	• Environment measurement • Remote control of instrument and virtual reality • Advanced manufacturing • Remote education and digital library • Remote medical treatment

Many applications can use features of IPv6 to help provide economic and social benefits. The vision of the future that many stakeholders have for the Internet economy is to be an enabler of wider societal and to scale for new uses. It appears that IPv6 could provide the address space needed for many enabling applications.

ANNEX 4: "MAPPING THE IPV4 ADDRESS SPACE"



Source: Adapted from "BGP Routing Table", September 2007, The Measurement Factory, using data from the Routeviews project of the University of Oregon http://maps.measurement-factory.com/.

ANNEX 5: REGIONAL INTERNET REGISTRY POLICY DEVELOPMENT PROCESSES

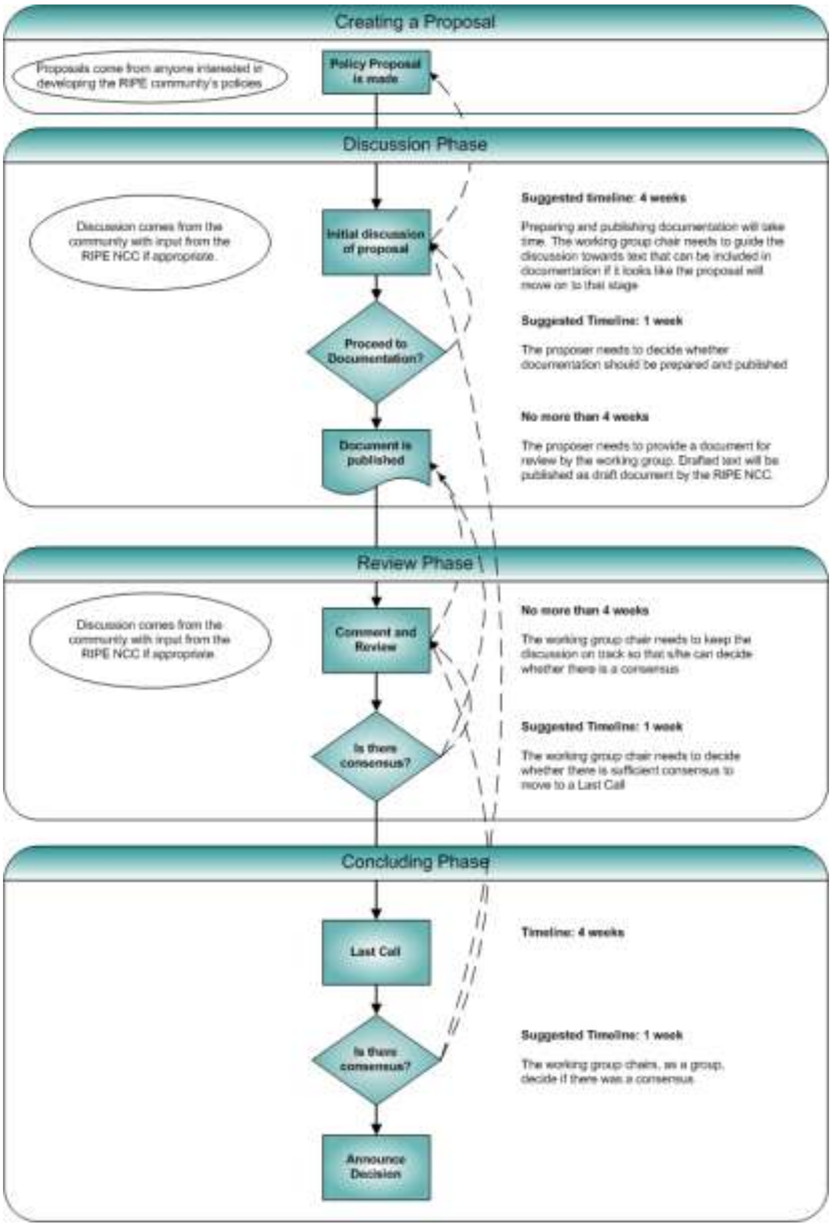
The RIRs are membership-based organisations through which Internet resource policies are developed in an open, bottom-up and transparent manner by the Internet community. In the case of ARIN for example, anyone may participate in the process and contribute to policy discussions, which often take place on public mailing lists. The ARIN Board of Trustees ratifies policies after public discussion is held, a review and recommendation by the ARIN Advisory Council is made, and there is evidence that rough consensus (*i.e.* that no parties have significant reservations), for a specific policy has been reached among the ARIN community. Addressing policy proposals are ratified, then adopted, left until the next meeting for future discussion or "rejected". [126] The other RIRs have similar processes, although each RIR's process may differ in detail. In all these respects the current RIR system is transparent, representative, flexible and effective. Figure 14 details RIPE NCC's policy development process.

Table 12. RIR policies for IPv4 and IPv6 address allocations and assignments

	Policies for IPv4 address allocation and assignment	**IPv4**	**Policies for IPv6 address allocation and assignment**	**IPv6**
IANA	www.arin.net/reference/ip_blocks.html	/8 (historical minimum /20)	www.iana.org/ipaddress/ipv6-allocation-policy-26jun02	/12 (historical minimum /23)
ARIN	ARIN's Number Resource Policy Manual (NRPM). www.arin.net/policy	/20	Ibid.	/32
RIPE NCC	www.ripe.net/docs/ipv4-policies.html	/21	Ibid.	/32
APNIC	www.apnic.net/docs/policy/add-manage-policy.html	/21	Ibid.	/32
LACNIC	http://lacnic.net/en/politicas/2002-11-asignacionip.html	/21	http://lacnic.net/en/politicas/ipv6.html	/32
AFRINIC	www.afrinic.org/docs/policies/afpol-v4200407-000.htm	/22	www.afrinic.org/docs/policies/afpol-v6200407-000.htm#5	/32

Source: RIR websites and Number Resource Organisation website.

Figure 14. A schematised view of the policy development process at RIPE NCC



Source: http://www.ripe.net/ripe/docs/pdp.html.

ANNEX 6: EFFECTS OF THE DEPLETION OF THE UNALLOCATED IPV4 ADDRESSES

TYPE OF BUSINESS / OPERATION	AFFECTED SERVICE / CONTENT	IMPACT
New Internet Service Provider	Internet connection service (New entrance)	**New entrance impossible, limitations, costs increase.**
Existing Internet Service Providers	Internet connection service	**Limits the type of available services, deteriorates quality, service is reduced.**
	Global address use service (such as permanent address service and peer-to-peer applications)	**Cannot add new subscriptions.**
	Procurement of network component equipment and lines	**Cost increase. Reduced technology selection.**
Equipment vendors	Development of new technologies and operation techniques.	**Difficult to determine investment choice technologies, cost increase.**
IP telephony	Global address use service (such as permanent address services for IP telephony). Procurement of network component equipment and lines.	**Cannot add new subscriptions, costs increase.**
Application Service Providers / Internet Data Centers	Virtual Private Network/hosting service.	**Deteriorated quality, type of services limited, reduced service.**
	Global address use service (such as Internet VPNs, dedicated hosting, access control with IP address, and Video on Demand).	**Cannot add new subscriptions.**
	Procurement of network component equipment and lines.	**Cost increase.**
End nodes and new services	New services (*e.g.* sensor networks, health and medical care, facility management, bi-directional mobility, and home appliance remote control).	**Service provision difficult, service use difficult.**
Operation staff	**Operational tasks.**	**Operation difficult, cost increase.**

Source: Based on Telecommunications Bureau, Ministry of Internal Affairs and Communication, December 2007, Japan.

ANNEX 7: PRIORITY IPV6 DEPLOYMENT CHALLENGES AS IDENTIFIED BY ATIS

"HIGH" priority challenges	Address Allocation Policies	Policy
	Site Multi-Homing	Business
	Quality of Service	Technical
	Security	Technical
	Interoperability Between IPv4 & IPv6	Technical
	Network Address Translators (NATs)	Business
	Impacts on Network Traffic & Routing	Technical
"MEDIUM" priority challenges	Impacts on Privacy/Legal Issues	Policy
	Management Tools (Dual-stack & IPv6 Networks)	Technical
	Impacts on Infrastructure Reliability	Technical
	Network Renumbering (Portability)	Business
	Peering Evolution (Impacts on Settlements)	Business
	Impacts on Access Networks	Business
"LOW" priority challenges	Separation of Locator & Identifier	Business
	Vendor Availability	Business
	Dual-Stack with Domain Name System (DNS)	Technical
	Relationships with other Numbering Systems	Technical
	Cost	Business

Source: ATIS Internet Protocol Version 6 (IPv6), Task Force Report on IPv6 Transition Challenges, July 2007.

ANNEX 8: ALLOCATION MECHANISMS FOR SCARCE RESOURCES

MECHANISM	DESCRIPTION	ADVANTAGES	DISADVANTAGES
1. First come first served	Administrative measure. Fees aimed at recovering costs of management.	- low administrative cost	- allocative inefficiency - possibility of strategic pre-emption
2. Lottery		- perceived equity	- allocative inefficiency - possibility of strategic pre-emption - does not guarantee that the winner is the one with the highest willingness to pay
3. Comparative selection "beauty contest"	The comparative selection procedure differs from auctions in that service providers are selected qualitatively (as opposed to quantitatively) in function of pre-defined "selection criteria".	- winner is firm whose business plans score best in achieving policy goals	- principal–agent setting risk of "regulatory capture" *i.e.* of the agent acting in the interest of the regulated party. - potential for asymmetric information and arbitrator must decide whether information is credible commitment to future undertakings - need to set up selection criteria - length of procedure - insufficient incentive for optimum resource utilisation - risk of bias/corruption, real or perceived. Selection is more likely to be partly subjective.
4. Auction	Assign resource to the party that is prepared to pay the most.	- rapid deployment of new services and technologies - recovery of scarcity rent that resource provides to winner - can increase the efficiency of resource use - operators can best evaluate the value of addresses for the services they provide - competitively neutral - transparent - objective (quantitative criteria) - less market distortion - allow to discover real value - well-designed auctions can maximise societal benefits of a scarce resource	- design of auction is crucial - risk of under-bidding and insolvency ("winner's curse") - necessary expertise of administrators regarding interdependencies of items auctioned to enable economies of scope - operators can be subject to "exuberant expectations" - flaws in mechanism design and rules can dissipate the benefits of using a market mechanism

ANNEX 9: INCREASED AWARENESS AND PUBLIC STATEMENTS OF SUPPORT FOR IPV6

Technical standards groups, all five regional Internet registries (RIRs), ICANN, as well as national Internet registries (NIRs) have recently made public statements emphasising the need for IPv6 deployment with renewed urgency.

On 7 May 2007, the **ARIN** Board of Trustees passed a resolution on Internet protocol numbering resource availability. The resolution *i)* advises "the Internet community that migration to IPv6 numbering resources is necessary for any applications which require ongoing availability from ARIN of contiguous IP numbering resources"; *ii)* directs ARIN staff to take any and all measures necessary to assure veracity of applications to ARIN for IPv4 numbering resources; and, *iii)* requests the ARIN Advisory Council to consider Internet Numbering Resource Policy changes advisable to encourage migration to IPv6 numbering resources where possible.[127]

In other words, ARIN was advising companies that will need public addresses in the future to support their growth to plan ahead and investigate deployment of IPv6. It also forewarned its membership and the wider business community that ARIN would carefully monitor applications for IPv4 space due to upcoming scarcity and that it would introduce policies to encourage the migration of IPv6 where possible.

Shortly thereafter, on 20 June 2007, in Montevideo, **LACNIC** announced that it was launching a regional campaign so that all the region's networks would be adapted to IPv6 by 1 January 2011. It advised companies, governments and institutions to take the necessary steps to prepare to adopt IPv6 as soon as possible.[128]

ICANN's Board passed a resolution on the deployment of IPv6 on 29 June 2007, which stated:

> "the future growth of the Internet (…) depends on the availability and timely deployment of IPv6" and that "the Board "resolves to work with the Regional Internet Registries and other stakeholders to promote education and outreach, with the goal of supporting the future growth of the Internet by encouraging the timely deployment of IPv6."

Beyond a call to real action in encouraging IPv6 deployment, the important message of the ICANN Board was that "the Board expresses its confidence in the Internet community to meet this challenge to its future prospects, and expresses its confidence in the bottom-up, inclusive, stakeholder-driven processes in place to provide any needed policy changes."[129]

On 1 July 2007, after considering the situation of the IPv4 central pool depletion and the analysis paper published by AfriNIC staff in April 2007, the **AfriNIC** Board passed a Resolution stating:

> "Noting the imminent exhaustion of the IPv4 address central pool, the AfriNIC Board resolves that efforts to draw the public's attention to the problem and potential solutions such as IPv6 be intensified, and instructs the staff to take appropriate action in this regard".[130]

In line with this resolution, the AfriNIC Board announced that they would reach out to a larger audience including the media, advise network operators in the region to make their network infrastructure IPv6 ready as soon as possible, and intensify its IPv6 awareness and training activity across the continent.

On 7 September 2007, at APNIC 24, the **APNIC** community agreed to a resolution recognising the critical importance of IPv6 for the future success of the Internet, and stating that the APNIC community would actively promote the adoption of IPv6, and focus its efforts towards comprehensive deployment of IPv6 in the Asia Pacific region. On the transition to IPv6 APNIC stated:

> "We agree that this situation requires a concerted effort by this community, working for the common good, to seek, examine and adopt responsible measures for the management of remaining IPv4 address space. We recognise that during this period, we will be learning and adapting, and that address management policies may also change to adapt to new circumstances."[131]

The APNIC resolution also reasserted support for open, bottom-up and consensus-based decision making. In addition, it stated,

> "we also call upon the leading senior and expert members of this community to provide strong leadership in the search for solutions to these issues of IPv4 address management and transition to IPv6, both within the Asia Pacific region and globally".

On 26 October 2007, the RIPE community agreed to a resolution on IPv4 Depletion and Deployment of IPv6, which included a reference to the role of governments in deployment of IPv6:

> "We recommend that service providers make their services available over IPv6. We urge those who will need significant new address resources to deploy IPv6. We encourage governments to play their part in the deployment of IPv6 and in particular to ensure that all citizens will be able to participate in the future information society. We urge that the widespread deployment of IPv6 be made a high priority by all stakeholders."[132]

On 12 November 2007, an Internet draft on an "IETF Statement on IPv4 Exhaustion and IPv6", which considered "work in progress" in IETF procedures, was submitted to the Internet standards body. In what follows, the draft's author summarises the reason for the IETF to re-iterate its support and continued commitment to IPv6:

> "IPv6 deployment is necessary to ensure the continued growth and expansion of the Internet. Deployment of IPv6 is needed to preserve the important properties of the Internet that have made it a success and enable new generations of applications and services." [133]

NOTES

1. In parallel, the technical community has to manage complex trends in routing, because of the strong interdependency between addressing and routing. To do this, the technical community is discussing solutions to enable enterprises to be independent from their Internet provider; *i.e.* supporting competition between Internet providers while mitigating its impact on routing table processing

2. An IP address is not, however, a unique identifier. While IP addresses help to identify a device that is participating in a communication, this "who" function is only valid in one location and changes based on location.

3. From a network topology context.

4. Huston, G., "Addressing as a Fundamental Part of the Internet", NSF/OECD workshop, January 2007, http://www.oecd.org/sti/ict/futureinternet2007.

5. The free pool of unallocated IPv4 address space is considered to be the IANA pool. After then, regional Internet registries will still have remaining address space to last until mid 2011 at current consumption rates. Widely consulted sources for projections are Geoff Huston's "IPv4 Address Space Report" available at http://ipv4.potaroo.net and Tony Hain's "A Pragmatic Report on IPv4 Address Space Consumption" available at http://www.tndh.net/~tony/ietf/ipv4-pool-combined-view.pdf.

6. The Internet Domain Survey, July 2007, counted 489 million hosts, http://www.isc.org/index.pl?/ops/ds/ and Internet World stats, Feb 2008, http://www.internetworldstats.com/stats.htm.

7. In reality, the number of addressable objects in an addressing plan is much lower than the "theoretical" maximum, because addressing plans are typically organised hierarchically and there is loss of efficiency at each level of a hierarchical plan. For this reason, a logarithmic "host-density ratio" or "HD-ratio" for address assignment efficiency is used rather than a linear function.

8. This number is theory – the IPv6 address architecture has already reduced this to a significantly smaller number by taking off the bottom 64 bits and using them as some form of interface identifier.

9. Or the router must have a default route to which it sends all traffic for which it doesn't have explicit instructions.

10. See page 15 for more information about the use of "/" in front of a number.

11. The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF Mission Statement is documented in RFC 3935. The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds.

12. BGP4 propagates prefix lengths along with the subnet addresses.

13. It should be noted that servers can also be behind NATs today.

14. Saltzer, J., Reed, D. and Clark, D., "End-to-end arguments in system design", 1981, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

15. Perceived security is a side effect of the statefull firewall nature implied by the use of NAT, but address translation itself does not provide any significant security benefit.

16. By for example creating strong incentives for multi-party application architectures that simulate end-to-end by using agents and clients to traverse the NAT and create a visible rendez-vous point.

17. Huston, G., “Anatomy: A Look Inside Network Address Translators”, August 2004, http://www.potaroo.net/papers/ipj/2004-v7-n3-nat/nats.pdf.

18. Partridge, C.; Kastenholz, F., “Technical Criteria for Choosing IP The Next Generation (IPng)”, Informational Internet-draft, RFC 1726, December 1994, http://www.ietf.org/rfc/rfc1726.txt.

19. Bradner, S.; Mankin, A., “The Recommendation for the IP Next Generation Protocol”, Standards Track, RFC 1752, January 1995, http://www.faqs.org/rfcs/rfc1752.html.

20. IPv6 has had a variety of names — the original IAB documents refer to IP Version 7, working on the assumption that the protocol numbers 5 and 6 were already in use in research networks. It was renamed IPng, for “next generation.”

21. http://www.itu.int/ITU-T/worksem/ipv6/200506/presentations/s1-1-carpenter.pdf.

22. To allocate means to distribute address space to Internet Registries for the purpose of subsequent distribution by them. http://www.apnic.net/mailing-lists/sig-policy/archive/2007/08/msg00027.html.

23. Initially defined in RFC 1366.

24. NIRs exist in the Asia Pacific and Latin American regions.

25. NIRs were established in the Asia Pacific and Latin American regions in the earliest days of the formation of the RIRs and are responsible for providing services within their country. APNIC NIRs operate in Korea, China, Japan, Chinese Taipei, Indonesia and Vietnam. Latin American NIRs operate in Brazil and Mexico. They are not ISPs, rather they allocate to their members (generally ISPs) within their economy following RIR policies. Organisations within those NIR economies may go to either the relevant NIR or RIR.

26. Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D., and J. Postel, “Internet Registry IP Allocation Guidelines”, Best Current Practice 12, RFC 2050, November 1996, http://www.faqs.org/rfcs/rfc2050.html.

27. It is important to note that having a global address does not mean that it is globally reachable, because there may be filtering on the routing system if the prefix is too specific. Moreover, RIRs cannot guarantee the reachability/ global routability of the addresses they assign.

28. http://www.potaroo.net/tools/ipv4/index.html.

29. http://www.tndh.net/~tony/ietf/ipv4-pool-combined-view.pdf.

30. The dual-stack approach is further detailed on page 35, Transition and co-existence.

31. The Internet Corporation for Assigned Names and Numbers (ICANN) published a Background Report on Policy for IPv6 in January 2006, updated in May 2006, reviewing the status of IPv6 policy development by the Regional Internet Registries. http://www.icann.org/announcements/ipv6-report-16may06.htm.

32. Have We Reached 1000 Prefixes Yet? A snapshot of the global IPv6 routing table, Gert D¨oring, SpaceNet AG, Munich, Germany, 8 May 2007, RIPE 54, Tallinn, Estonia, http://www.space.net/~gert/RIPE/R54-v6-table.pdf.

33. http://www.cidr-report.org/as2.0/.

34. http://www3.ietf.org/proceedings/06mar/slides/grow-0.pdf.

35. Gert D¨oring, SpaceNet AG, May 8th, 2007, RIPE 54, Tallinn, Estonia, http://www.space.net/~gert/RIPE/R54-v6-table.pdf.

36. http://v6metric.inetcore.com/en/html/st3/05.html.

37. https://prefix.pch.net/applications/ixpdir/summary/ipv6/.

38. Palet, J. and Vives, A., "6meter: Measuring Real Global IPv6 Traffic", RIPE 55, October 2007 http://www.ripe.net/ripe/meetings/ripe-55/presentations/palet-v6.pdf.

39. In a network that provides IPv6 connectivity, according to the data, IPv6 packets represent 70% of the total packets and over 90% of IPv6 traffic is tunnelled with either Teredo or 6to4 compared to just 5% of native IPv6 traffic http://www.ripe.net/ripe/meetings/ripe-55/presentations/palet-v6.pdf.

40. Operating system market share for January, 2008 http://marketshare.hitslink.com/report.aspx?qprid=8 and http://www.microsoft.com/msft/earnings/FY08/earn_rel_q2_08.mspx on 7 February 2008.

41. The IETF's "6man" working group is responsible for IPv6 protocol maintenance. The website at http://www.ipv6-to-standard.org/index.php lists vendors with IPv6-enabled products.

42. http://www.arin.net/meetings/minutes/ARIN_XX/PDF/thursday/Firewalls_Piscitello.pdf.

43. Conclusions of the Australian "IPv6 for e-business project" that took place from July 2006 to April 2007.

44. Top-level domains are the last label on the right-hand side of the domain name, such as .JP, .COM, .FR OR .ORG.

45. Top-level domains are the last label on the right-hand side of the domain name, such as .JP, .COM, .FR OR .ORG.

46. http://www.icann.org/announcements/announcement-20jul04.htm.

47. http://www.ipv6.org.au/underpin.html.

48. In April 2006 there were 245 country code top-level domains, http://www.oecd.org/dataoecd/8/18/37730629.pdf.

49. DNS Survey: August 2006, http://dns.measurement-factory.com/surveys/200608.html.

50. Prop-055-v001: Global policy for the allocation of the remaining IPv4 address space, 23 January 2008, http://www.apnic.net/policy/discussions/prop-055-v001.txt.

51. "Co-operative distribution of the end of the IPv4 free pool" by Tony Hain, Cisco Systems, http://www.apnic.net/policy/proposals/prop-052-v001.html.

52. "IPv4 soft landing proposal" by David Conrad, General Manager, IANA, http://www.apnic.net/policy/proposals/prop-056-v001.html.

53. http://www.arin.net/meetings/minutes/ARIN_XIX/ppm2_transcript.html.

54. Legacy holders who sign the "Legacy RSA" are guaranteed the same registration services as provided to organisations that sign the standard Registration Services Agreement (RSA). ARIN states that it will not reclaim unutilised address space from legacy holders who sign the RSA. It allows ARIN to accept the return or relinquishment of any address space from any existing address holder. Organisations returning addresses under this policy see their fees waived if they voluntarily return unused address space. Discussions regarding legacy space come primarily out of ARIN because most of the legacy allocations were made to organisations in the ARIN region, before the creation of the RIR system.

55. The Routing Research Group of the Internet Research Task Force (IRTF) is discussing several technical schemes that are intended primarily to help the routing system scale with growing demand for more multihomed end-user networks. Additional research is deemed necessary.

56. Huston, G., "IPv4 address transfers", proposed to APNIC on 26 July 2007, http://www.apnic.net/mailing-lists/sig-policy/archive/2007/07/msg00005.html.

57. Titley, N. and van Mook, R., "Enabling methods for reallocation of IPv4 resources", Submission Date: 23 October 2007, http://www.ripe.net/ripe/policies/proposals/2007-08.html.

58. Policy Proposal: IPv4 Transfer Policy Proposal, ARIN Advisory Committee, http://lists.arin.net/pipermail/ppml/2008-February/009978.html

59. IPv4 address report, 8 February 2008, http://www.potaroo.net/tools/ipv4/index.html

60. As seen by the Routeviews collector at the University of Oregon.

61. A study finds that only 3.6% of allocated addresses are actually occupied by visible hosts, and that occupancy is unevenly distributed, with a quarter of responsive /24 subnets less than 5% full, and only 9% of subnets more than half full. The study establishes an upper-bound on the number of servers in the Internet at 36 million servers, about 16% of the responsive addresses. Just over 100 million ping-responsive IPv4 addresses, or around 4% of advertised addresses. Heidemann, J., Pradkin, y., Govindan, R., Papadopoulos, C., Bannister, J., "Exploring Visible Internet Hosts through Census and Survey", May 2007, USC/ISI Technical Report ISI-TR-2007-640, http://www.isi.edu/~johnh/PAPERS/Heidemann07c.pdf.

62. http://www.apnic.net/meetings/24/program/amm/presentations/sanjaya-tech-area.pdf

63. "Quitclaims" by which the assignee agrees to relinquish their assignment in favour of another party.

64. The Japanese Intelligent Transport System (ITS) project and the European Car2Car consortium recommended exclusive use of IPv6 for its future Car2car applications http://www.car-to-car.org.

65. CENELEC opted for IPv6 for the smart home concept.

66. IPv6 is specified as the only IP version supported in Release 5 for IP Multimedia Subsystem (IMS). 3GPP mandated use of IPv6 for IMS (IP Multimedia Subsystems) in 2000.

67. http://www.defenselink.mil/transcripts/2003/tr20030613-0274.html.

68. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.

69. 4.9% annually, according to a recent report released by INPUT, the authority on government business. The report suggests that a key area of growth will come in the wireless market segment.

70. The guideline compares the cost structure between IPv4 and IPv6, and inventories the infrastructure and servers as well as client products used by civil servants. The guideline summarises current adoption of IPv6-enabled products in the Japanese government. It also provides a series of procedures to help each Office and Ministry in Japan plan for IPv6 adoption. http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news070402_1.html.

71. The strategy identifies three phases in a : Phase i) preparation, from January 2008 through December 2009; Phase ii) transition, from January 2010 through December 2012; and Phase iii) implementation, from January 2013 through December 2015. Department of Finance and Deregulation, A Strategy for the Transition to IPv6 for Australian Government agencies, 'Building Capacity for Future Innovation', AGIMO, October 2007, http://www.agimo.gov.au/infrastructure/ipv6.

72. Arch Rock offers low power wireless sensor nodes, routers and data and management servers based on IPv6 standards developed by the IETF 6LoWPAN Working Group for the IEEE802.15.4 low power radio standard. Arch Rock's technology provides access to the Wireless Sensor Network as well as to individual Sensor Nodes using Internet Protocol (IP) methods, services and tools.

73. 6LoWPAN22 (IPv6 over IEEE802.15.4) is a communication network based on IPv6 networking, for limited power and for low throughput requirements.

74. It should be noted that a number of other working groups are using IPv4.

75. An ad-hoc network is a local area network or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

76. E.g. mobicast or geocast.

77. Alternatively, they could deploy IPv4 private space and NATs.

78. IPv6 Mobile nodes in IPv6 are able to communicate directly with any peer, as opposed to mobile nodes in IPv4 where generally, the communication between the mobile node and its peer is routed through a fixed anchor point (the Home Agent), which makes routing sub-optimal.

79. The additional overhead cost for the direct routing with mobile nodes in IPv6 is that of a signaling overhead. Most of the signaling overhead cost is to make the transmission between the mobile node and its peer secure.

80. In this case there appears to be a need to devise more complex forms of protocol translation mechanisms that use forms of 4in6 protocol mapping, in order to allow IPv4 packets to transit across an IPv6 internal infrastructure. The issue concerns the capability of available routers to perform such packet transformations within the necessarily very high packet processing rates that such high volume networks require.

81. http://www.potaroo.net/ispcol/2007-08/dualstack.html.

82. John Curran, J., "An Internet Transition Plan", August 2007, Informational Internet-draft, http://www.ietf.org/internet-drafts/draft-jcurran-v6transitionplan-01.txt.

83. In "A Scenario-Based Review of IPv6 Transition Tools," Mackay and colleagues leverage their experience running 6Net, one of Europe's largest IPv6 research networks. They analyse the applicability of different transition tools on ISP, mobile wireless, corporate, and small–medium-business/residential networks.

84. Asadullah, S., Ahmed, A., Popoviciu, C., Savola, P., Palet, J., "ISP IPv6 Deployment Scenarios in Broadband Access Networks", Internet-Draft, Informational, RFC 4779, January 2007, http://tools.ietf.org/html/rfc4779.

85. P. Grossetête, Cisco, « 2010, année cruciale dans l'adoption de l'IPv6 », VNUnet, 21 September 2007, http://www.vnunet.fr/fr/news/2007/09/21/p-grosset-te-cisco-2010-ann-e.

86. Planning and Accomplishing the IPv6 Integration: Lessons Learned from a Global Construction and Project-Management Company, Cisco Systems, Microsoft, and Comandinformation, http://www.cisco.com/web/partners/pr67/pr41/docs/C11-439724-00_PlanningandAccomplishingtheIPv6Integration_v2.pdf.

87. The US National Institute of Standards and Technology is part of the United States Department of Commerce.

88. Measured in 2003 US dollars.

89. Domingues, M., Friacas, C., "Is Global IPv6 Deployment on Track?", Foundation for National Scientific Computing (FCCN) at the University of Lisbon, October 2007.

90. An explanation for better IPv6 results compared to IPv4 between Portugal and Ireland is a greater number of hops: IPv6 connectivity is only provided via London while IPv4 connectivity is provided in Madrid, Geneva and Paris.

91. The issue of scalable routing is being discussed within several constituencies including the Internet Architecture Board (IAB), the IETF, Internet registries, and Internet service providers. Proposed solutions range from technical means to add new layers of "indirection" at various levels of the Internet (e.g. at the end-device level, at the router level, or at the Internet service provider level), through to new addressing policies.

92. Meyer, D., Zhang, L. and Fall, K., "Report from the IAB Workshop on Routing and Addressing", Informational Internet-Draft, RFC 4984, September 2007, http://tools.ietf.org/html/rfc4984.

93. Sherbin P., “Elements of The Internet Architecture”, Informational Internet-Draft, RFC 4984, August 2007, http://www.ietf.org/internet-drafts/draft-sherbin-eia-00.txt.

94. Huston, G., “Transition to IPv6”, August 2007, http://www.potaroo.net/ispcol/2007-08/dualstack.html.

95. E.g. rendezvous mechanisms.

96. M. Mackay, C. Edwards, M. Dunmore, T. Chown, and G. Carvalho, A Scenario-Based Review of IPv6 Transition Tools, pg. 27, IEEE Computer Society, May/June 2003.

97. Such as NAT-PT or ISATAP. It is also possible to run parallel networks that run IPv6 and IPv4 and NAT.

98. E.g. ISATAP or an internal tunnel broker.

99. They will need to use a 6to4 tunnel or build IPv6-to-IPv4 tunnels to other IPv6 locations.

100. For example, Vint Cerf at the Internet Governance Forum in Rio de Janeiro.

101. Lawful Intercept for the Internet and tracing nodes and application identification by port are inhibited by NAT translation and global uniqueness of IPv6 addresses facilitates identification.

102. Department of Finance and Deregulation, A Strategy for the Transition to IPv6 for Australian Government agencies, ‘Building Capacity for Future Innovation’, AGIMO, October 2007, http://www.agimo.gov.au/infrastructure/ipv6.

103. http://www.ipv6Forum.org.

104. Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E., « Address Allocation for Private Internets”, Internet Best Current Practice, February 1996, http://www.faqs.org/rfcs/rfc1918.html.

105. http://www.6journal.org/archive/00000265/01/alain-durand.pdf.

106. http://www.v6.ntt.net/index_e.html.

107. Also called "IPv6 Dual Connection Service for Open Computer Network (OCN) Housing" that is directly linked to a high-quality area backbone connection.

108. http://www.ap-ipv6tf.org/meetings/summit2007/file/1/(3)%20JAPAN%20-%20SummitAP2007.pdf.

109. Ibid.

110. Presentation “How and Why have millions of households been already IPv6 ready?” IPv6 Deployment Status Report in Japan, Asia Pacific IPv6Summit 2007, Takashi Arano, Intec Netcore, Inc.

111. http://www.internetnews.com/infra/article.php/3722731, NTT's 'Killer' IPv6 App a Potential Lifesaver, by Sean Michael Kerner, 18 January 2008.

112. http://www.cio.com/article/print/133950.

113. IPv6 is also adequately supported in Windows XP and Windows Server 2003 to perform basic functions, including application verification.

114. http://www.afcea.org/committees/technology/techforum/ipv6/Wettling.pdf.

115. IPv6 Promotion Council: http://www.v6pc.jp/en/index.html.

116. IPv6 Services in Japan: http://www.ipv6style.jp/en/statistics/services/index.shtml.

117. http://www.ipv6style.jp/en/statistics/services/index.shtml.

118. http://www.kantei.go.jp/foreign/policy/it/ITstrategy2006.pdf (p. 35).

119. Study Group on Internet's Smooth Transition to IPv6 to Convene – August 2007, http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news070807_2.html.

120. http://www.ripe.net/ripe/maillists/archives/ipv6-wg/index.html.
121. http://www.ipv6tf.org/PublicDocuments/com2002_0096en01.pdf.
122. Ibid.
123. http://www.defenselink.mil/transcripts/2003/tr20030613-0274.html.
124. http://www.networkworld.com/research/2007/041807-better-internet-ipv6.html.
125. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.
126. http://www.nro.net/about/rir-system.html.
127. http://www.arin.net/announcements/20070521.html.
128. http://lacnic.net/ipv6/en/.
129. http://www.icann.org/minutes/resolutions-29jun07.htm.
130. Resolution [#2007.07.01] http://www.afrinic.net/news/ipv4_exhaustion.htm.
131. http://www.apnic.org/meetings/24/program/sigs/policy/transcripts.
132. http://www.ripe.net/news/community-statement.html.
133. Narten, T., "IETF Statement on IPv4 Exhaustion and IPv6", Internet draft, 12 November 2007, http://www.ietf.org/internet-drafts/draft-narten-ipv6-statement-00.txt.