Illustrating the Impediments for Widespread Deployment of IPv6

ALA HAMARSHEH and MARNIX GOOSSENS
Department of Electronics and Informatics— ETRO
Building K; Office No: 4k221, 4K220; Tel: +32 2 629 2930; Fax: +32 2 629 2883
Vrije Universiteit Brussel
Pleinlaan 2, 1050 Elsene, Brussels
BELGIUM
{ala.hamarsheh, marnix.goossens}@vub.ac.be http://www.etro.vub.ac.be

Abstract—This paper analyzes the technical and nontechnical impediments for a smooth and successful transition from IPv4 protocol to IPv6 protocol in the Internet. It tries to illustrate and defines most obstacles that hold the widespread deployment of IPv6 at both sides: end-users and Internet Service Providers (ISPs). The paper also suggests transparent, auto-configured, and cost effective solutions for both end-users and ISPs parties to allow a smooth and successful widespread deployment of IPv6.

Key-Words: - IPv6 deployment; ISP; end-user; IPv6 Transition mechanisms;

1 Introduction

Almost 15 years ago, it was decided to introduce a new version of the Internet Protocol, IP. The new version, IPv6, aimed to resolve a number of shortcomings of the current version (IPv4). The main issue at that time was IPv4 address space exhaustion, as well as the lacking of with auto-configuration, mobility, flow labeling, and security. Flow labeling and security issues with IPv4 have been addressed as far as the addresses are concerned in the meantime, and these are no longer an argument for a changeover.
Traditionally, Internet Service Providers (ISPs) obtained their IP addresses from a Local Internet Registry (LIR), a National Internet Registry (NIR), or a Regional Internet Registry (RIR). The following are the five global RIRs that administer Internet addressing [1]:

- AfriNIC: Africa Region.
- APNIC: Asia/Pacific Region.
- ARIN: North America Region.
- LACNIC: Latin America and some Caribbean islands.
- RIPENCC: Europe, Middle East, and central Asia.

Figure 1 shows the global RIRs distributed in the world.

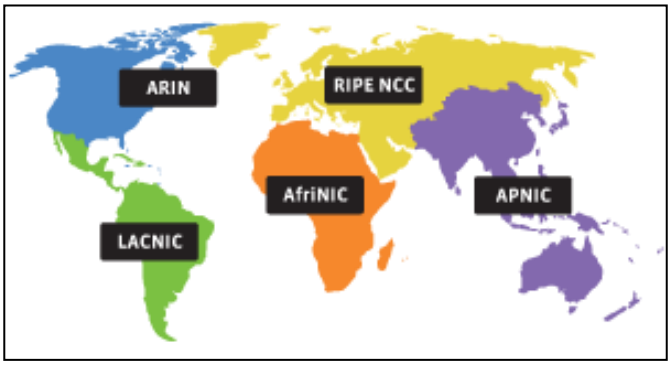


Figure 1: RIRs among the world

In February 2011, IANA allocated the last IPv4 address to RIRs. Experts predict that the RIRs will be out of addresses later in 2011 [2]

The following report is generated by Geoff [3] and shows the projected RIRs address pool exhaustion. Figure 2 illustrates the consumption of IPv4 address pools for each RIR.

- AfriNIC: May 27, 2014.
- APNIC: April 19, 2011.
- ARIN: August 2, 2014.
- LACNIC: March 12, 2014.
- RIPENCC: June 6, 2012.

ISBN: 978-1-61804-081-7

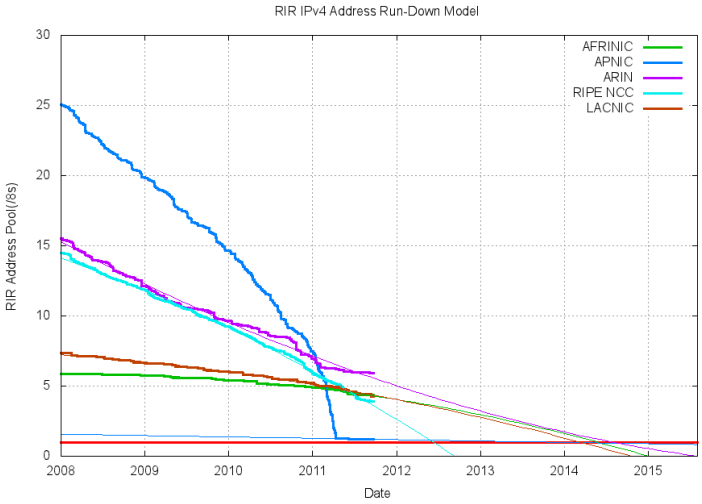


Figure 1.2: The projection of consumption of remaining RIR address pools

The Internet Engineering Task Force (IETF) has proposed a set of mechanisms (i.e. NAT [4]) to alleviate the scarcity of public IPv4 addresses. For example, NATs have been deployed to translate a public IPv4 address into a set of private IPv4 addresses.

All these solutions are makeshift measures to extend the life of the IPv4 address space. They will not ultimately overcome the scarcity of the IPv4 public address space, or many other limitations of today's communications. The intensive use of network-based devices, along with the growth of the Internet and of networking technologies, has led to the exhaustion of the IPv4 public address space.

When the IPv4 address pool is fully deployed, the current ISPs and the existing internet connected devices will continue working as they do now. However, both current and newly-launched ISPs will have increasing difficulties in obtaining new IPv4 addresses. The cost and complexity of managing the remaining IPv4 addresses will also increase.

Despite the fact that IPv6 is designed to be the successor protocol to IPv4, it is not backward-compatible with IPv4. In other words, the IPv6 protocol stack in any IPv6-only host cannot recognize IPv4 packets. And neither can the IPv4 protocol stack in any IPv4-only host cannot recognize IPv6 packets. Despite the fact that most IPv4 header fields can be mapped onto equivalent IPv6 header fields, and vice versa, the main problem comes when trying to exchange the source and destination addresses between IPv4 and IPv6 protocols.

The IETF has created a set of working groups to smooth the transition to IPv6, and has also proposed many pragmatic solutions to achieve this. These solutions can be categorized into: dual stack network (hosts and routers), tunneling, and protocol translation.

Nearly 15 years after its definition, the transition to IPv6 is still totally stuck. Only a few US organizations, including the federal government and handful commercial companies like Bechtel and Google, have deployed IPv6 across their networks [5].

At the inception of IPv6 it was – rather naively – presumed that all parties involved with the internet would be eager to make the changeover, and that the transition would happen spontaneously. It is now generally acknowledged that the human, commercial, and technical factors preventing a spontaneous transition have been underestimated. There are essentially two parties involved in the transition to IPv6: network providers and end-users. The benefits of using IPv6 are mostly for the network providers, while the end-users have only potential indirect benefits. No drive to make the changeover should be expected from the majority of end-users, as they probably have little to gain. The network providers can expect benefits, but they are dependent on the willingness of their end-users to make any changeover. The result is a kind of deadlock: no (commercial) network provider is going to force its customers to make the changeover against their will. So making the transition transparent to the end-user is one of the keys in any transition to IPv6. The average end-user are not really aware of what goes on in the network layer, and even if they are, they don't generally care.

In addition, running IPv4 and IPv6 is more expensive. So, if no users are demanding IPv6, ISPs are not going to introduce IPv6 with its added operation cost as long as IPv4 addresses are readily available. This paper tries to analyze what exactly is holding up the transition to IPv6.

2 Why it does Not Happen?

The IETF chair (Russ Housley) said "Our transition strategy was dual-stack, where we would start by adding IPv6 to the hosts and then gradually over time we would disable IPv4 and everything would go smoothly". It is characteristic of the problem that (mostly technical) people around the world are wondering and debating about "why does it not happen?" Clearly, a sound analysis of the situation, taking the "real-world" conditions into account, has never been made.

The provisioned technical measures for the transition did not have the effect of creating a

ISBN: 978-1-61804-081-7

"smooth" transition. One of the reasons identified is that these measures where only technical in nature, too abstract, only oriented towards professionals and not considerate of the average end-user, and that they did not take into account any clear business case. The Internet Society (ISOC) [6] conducted a study entitled "Organization Member IPv6 Study" [7]. This study was conducted on the operational characteristics of IPv6, and targeted to the organization's members. The study report shows that there are no concrete business drivers for IPv6. Some organizations have nevertheless begun IPv6 deployment, but these organizations have reported problems in IPv6 networks tools and applications.

From over 15 years of IPv6 transition development within IETF working groups, many proposed IPv6 development standards are deployed mainly in operational and research networks. Additionally, these standards are developed for narrow, specific and purely technical scenarios, without taking into account any business case.

The following sections discuss are the main concerns may play a vital role in the widespread deployment of IPv6.

3 End-Users

In order to achieve a smooth and transparent transition from IPv4 to IPv6, the end-users should not be technically bothered with the process of the transition to IPv6. The transition to IPv6 would have to be totally transparent to end-users in terms of:

3.1 Users' Applications

It is important to highlight that in the process of migrating to IPv6, not only the IP stack needs upgrading. The end-user's applications use IP addresses internally, and these applications need to be converted to be capable of using also the new 128-bit addresses.

Normally, IPv4 applications use IPv4 communication in order to communicate with IPv4 peers. Similarly, IPv6 applications use IPv6 communication in order to communicate with IPv6 peers. However, the IPv4/IPv6 applications can use either IPv4 or IPv6 in order to communicate with other IPv4 or IPv6 peers. IPv4/IPv6 applications are being increasingly offered by software developers. However, not all applications are IPv6 ready yet.

Apart from IP4/IPv6 applications, the other class of client-server applications (e.g. IPv4-only and IPv6-only applications) should be able to communicate with peers regardless of the current host connectivity. For example, the IPv4-only applications that are running on an IPv6-only host should be able to communicate with IPv6-only peers. Similarly, the IPv6-only applications that are running on an IPv4-only host should be able to communicate with IPv4-only peers.

It is not realistic to expect all applications to be modified to deal with the longer IPv6 addresses any time soon. Apart from the key internet applications with good support – such as web browsers and email programs – which can be expected to be IPv6 enabled, there are thousands of other applications. Some were written by small companies (which may be out of business by now), others may have been "home-made". Internet communication may only be a side issue for some applications – such as for registering and/or checking for updates – and upgrading to be IPv6 compatible is probably not a big priority for these. In general, a large proportion of applications will probably only be modified to be IPv6 compatible when IPv6 is used on a larger scale. Even then, IPv6-capable new versions of some application software may never be available, or end-users may not do the required updating of all the software on their system.

Assuming that being able to use their applications as before is a key requirement of end-users for them to be willing to change towards IPv6, and that some applications will not be modified to be IPv6-capable any time soon, it is obvious that some functionality is required that is both installed and enabled as standard on any system that has to communicate using IPv6 but potentially has to run IPv4-only applications. Additionally, in some situations, IPv6-only applications should be able to communicate on a machine with IPv4-only communication with remote hosts. IPv6-capable applications are supposed to be "agnostic" in IPv4/IPv6 support, but in some situations there are reasons to make them only IPv6-capable (e.g. for systems with limited memory and processing capability).

Figure 3: an architecture to provide cost effective dual connectivity across ISP's network

The demand that such functionality be provided on all general purpose machines is far more realistic than expecting all applications to be modified: there is only a handful of developers who implement internet communication stacks on general purpose machines, whereas there are thousands of application developers.

Thus, a generic solution is needed to allow any mixture of IPv4/IPv6-capable applications to communicate over any IPv4/IPv6 communication

with any IPv4/IPv6 application, without modifying these applications in addressing capabilities.

The authors have proposed a transparent mechanism called DAC [8] that could be installed in end-user machines and would allow applications of any mixture of capabilities (IPv4, IPv6) to communicate with each other, as long as a common communication path (over IPv4 or IPv6 or IPv4 converted along the way to IPv6 and vice versa) can be established. Similar mechanisms have been proposed by others.

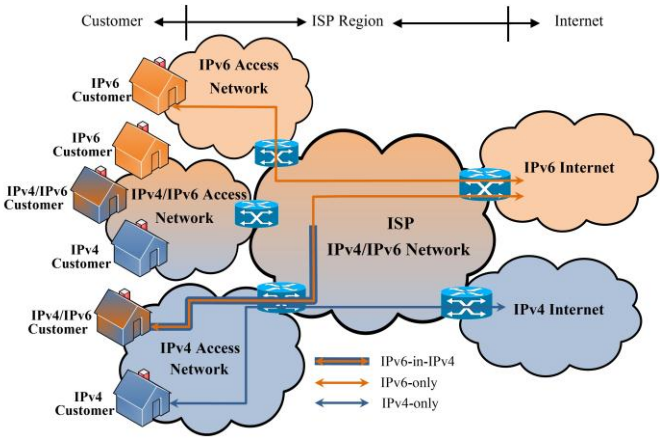


Figure 3: an architecture to provide cost effective dual connectivity across ISP's network

3.2 Host Configuration

The majority of end-users generally have limited IT or computing backgrounds and most of them have no idea about what goes on inside their computer. Generally, the end-users are not sufficiently qualified to manually configure their devices for any host-based IPv6 transition technique. Therefore, for a chance of success for any IPv6 deployment mechanism that needs some configuration at end-users' hosts, this configuration must be made completely automatic and transparent to those end-users.

3.3 Backward Compatibility

The IPv6 transition mechanisms have been introduced to overcome the problem in the development of IPv6 that it does not support real backward-compatibility with the current protocol, IPv4 [5]. At the time of developing IPv6, it was thought that the network backbone and end-user devices would operate on dual stack mode. They did not take into account that some IPv4 devices may not be upgraded to be IPv6-capable. Neither did they take into account that some IPv6-only networks may need to communicate with IPv4-only networks.

4 Service Provider Network

While about all newer general purpose computers nowadays standard support also IPv6, and upgrading the backbone networks to be IPv6 capable in addition to IPv4 is not a big issue either, there is a major problem in many non-local access networks. The access network, of which usually part is situated on the end-users' premises and that part in many cases is also owned by these end-users, are often not capable of supporting IPv6 operation. Due to end-user involvement, upgrading these access networks is not obvious. This situation prevents simply adding IPv6 communication to the existing huge IPv4 base of Internet connections, denying them the possibility to communicate with IPv6 connected server machines. And in turn making operation of IPv6 servers quite useless.

As business case, those ISPs will not start deploying IPv6 with its added operation cost as long as there are still public IPv4 addresses available. Besides, those ISPs should recognize that deploying IPv6 brings new services and business opportunities on large settings (e.g. mobile Internet).

Using tunneling of IPv6 over IPv4 to bridge the IPv6 gap over the access network is a possible solution. However, the standard tunneling solutions proposed by IETF are rather technical in nature, and almost always require some end-user manipulation and configuration, making them only suitable to the small number of end-users with the required technical knowledge. Here too, any solution would have to be standard installed and enabled, and not requiring manual configuration to be acceptable for normal end-users.

As seen in figure 3, providing IPv6 to subscribers requires changing/upgrading the old IPv4 network infrastructure. It would therefore not be in the ISPs' interest to start deploying IPv6 service alongside IPv4 into their infrastructure.

The following concerns may play a critical role in driving the ISPs to start deploying IPv6 service to their subscribers.

4.1 Proposing cost-effective solutions when providing dual connectivity (IPv4/IPv6)

In order to provide a smooth and successful transition to IPv6 on the ISP side, some transition mechanisms should be proposed in order to allow ISPs to start rapidly deploying IPv6 service to their subscribers even when these were not connected to an IPv6 network. Figure 4 shows this architecture.

ISBN: 978-1-61804-081-7

Unfortunately, all the current mechanisms that used to allow ISPs to start deploying IPv6 connectivity across their IPv4 network infrastructure require changing or upgrading the Customer Premises Equipment (CPE) and the Provider Edge Equipment (PE), which brings up the following problems:

- Despite the fact that the ISP can sometimes configure their CPEs remotely, any configuration to these CPEs will be difficult and costly. The customer connection network consists of CPEs and PEs. Normally, many CPE components are connected to one PE. The PE connects these CPEs to the backbone network infrastructure and the number of CPEs may reach thousands or more (depending on the ISP). What is even worse in many other cases is that the ISP has no control over these CPEs; hence it cannot upgrade or configure these devices remotely. In order to upgrade the CPEs, the end-users have to change or upgrade their devices themselves. As explained earlier, the majority of end-users have limited technical computing background to allow them to upgrade or change their devices. All these factors may negatively affect on the ISPs' decisions to start deploying IPv6 service into their networks.

- Customers rely on different technologies to connect to the Internet (e.g. dial-up, ISDN, ADSL, leased lines, etc.), thus changing or upgrading the ISP's network infrastructure will be quite complex and difficult across these technologies because some of them will result in changing or upgrading the end-user's devices. Furthermore, the ISPs have to setup different IPv6 transition requirements for each type of these technologies which may add additional operation cost in deploying IPv6 service to their customers.

In addition to the previous consequences, the current transition mechanisms used by the ISPs have the following limitations:

a) Tunneling is an IPv6 transition approach; it is commonly used for hosts/networks to communicate with each other by passing their packets through different IP protocol infrastructure. However, NAT boxes do not allow the tunneled packets (i.e. packets with protocol ID = 41) to traverse unless the NAT is explicitly configured by the end-user to forward these packets.

b) Firewalls in the path can block tunnels. The only solution available is to allow the administrator of the firewall to create a hole for the tunnel.

The authors have proposed transparent tunneling solutions called CHANC [9] and D6across4 [10] for this problem; some other solutions have been proposed by others too.

4.2 DNS

Due to the size of the Internet, there will be no "flag day" for the transition from IPv4 to IPv6. IPv6 protocol will slowly and gradually spread into networks and across the whole internet. Therefore there will be some IPv6-only clients wanting to initiate communications with other IPv4-only servers, and vice versa. The IETF has proposed a set of mechanisms to achieve this (e.g. SIIT [11] and stateful NAT64 [12] mechanisms). A special type of DNS server must be used in conjunction with these mechanisms, such as DNS64 [13]. The DNS64 is a mechanism for synthesizing the 'AAAA' resource records from 'A' resource records. Unfortunately, the DNS64 does not work in all heterogeneous communication scenarios. For example, it cannot synthesize an 'A' resource record from 'AAAA' resource records. This means an 'A' record cannot be resolved if the communication session is initiated from an IPv4-only client and destined to an IPv6-only server. Additionally, some functions have to be included in the DNS in order to serve newly-added transition mechanisms which current DNS types still do not support.

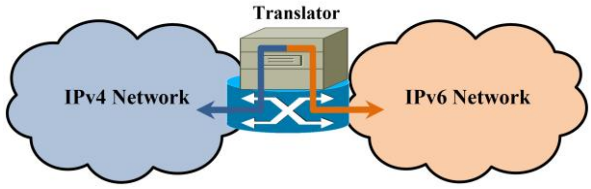
4.3 Tunneling versus Translation between two IPv4 and IPv6 Network Domains

The Internet Engineering Task Force (IETF) has proposed a set of mechanisms and specific types of addresses in order to make communication possible between nodes connected to heterogeneous (IPv6/IPv4) networks. The IETF has proposed several transition mechanisms to ensure a smooth and successful transition to IPv6. The transition mechanism is a way to facilitate the connection between hosts/networks using the same or different IP protocols. The most commonly-used transition mechanisms can be classified into three approaches: dual-stack, tunneling, and translation.

Apart from dual-stack and tunneling mechanisms, protocol translation-based mechanisms can be used to allow the communication between

ISBN: 978-1-61804-081-7

two networks deploying two different protocols. Figure 4 illustrates this scenario.



The different protocol translation-based mechanisms have many common limitations. These limitations are summarized thus:

- Some IPv4 header fields have changed meaning in the IPv6 header. This will not make translation between them straightforward.

- Translation inhibits end-to-end network security. The IP header is protected by cryptographic functions, and any translation parts of the IP header along the path will break this protection.
- Translation of both DNSSEC and end-to-end IPSec is not possible.
- Limited translator capacity (the number of simultaneous connections are limited). This may be used by denial-of-service attacks throughout exhausting the memory and address/port pool resources on the translator.
- Protocols that embed IP addresses into payloads do not get translated properly. Such protocols include DNS, FTP, SIP, RTP and ICMP. Therefore, implementing an Application Level Gateway (ALG) is required for each of these protocols.

Currently, to allow the communication between heterogeneous networks, one of the protocol translation mechanisms (e.g. SIIT, NAT64) must be used.

In order to limit the use of protocol translation-based techniques when considering the communication between two nodes connected to two different heterogeneous networks, the authors proposed new mechanisms called AIN-PT [14] and AIN-SLT [15] that may help in solving most limitation of protocol translation-based techniques .

5 Acknowledgment

This work was funded by European Union, Erasmus Mundus External Cooperation Window (EMECW) programme under project number 141085-EM-1-2008-BE-ERAMUNDUS-ECW-L02, Belgium.

6 Conclusion

The current techniques that are used to alleviate the scarcity of public IPv4 addresses all failed to overcome this problem and hence, the transition to IPv6 is the only solution. Currently, the transition to IPv6 is totally stuck and limited to few governmental organizations and handful of commercial companies.

The majority of IPv6 transition mechanisms are developed within IETF working groups. These mechanisms are narrow, specific, and customized for purely technical scenarios. The developers of these technical standard IPv6 transition mechanisms did not take into account any business case.

The key of any successful transition to IPv6 is the end-users. The IPv6 transition mechanisms have to be totally transparent to the end-users in terms to allow those end-users to use their old applications as before, provide auto-configuration when necessary, and support compatibility issues with the current standards. Additionally, providing cost-effective IPv6 deployment solutions for the ISPs' access networks would help in driving those ISPs to start deploying the IPv6 service across their access networks.

References:

[1] IANA. "Autonomous System (AS) Numbers". [Online] http://www.iana.org/assignments/as-numbers/as-numbers.xml.

[2] S., Lagerholm, "Service Provider Transition to IPv6", IPv4 ADDRESSES ARE EXHAUSTED. ARE YOU READY, Secure64 Software Corporation-white paper. [Online] http://www.secure64.com/transition_ipv6.

[3] H., Geoff ,"IPv4 Address Report. Adjunct Research Fellow at the Centre for Advanced Internet Architecture". [Online] http://www.potaroo.net/tools/ipv4/index.html.

[4] P. Srisuresh, and K. Egevang, "Traditional IP Network Address Translator (Traditional

NAT)", *Internet Engineering Task Force (IETF) RFC 3022*, 2001.

[5] Marsan, C. Duffy, "Biggest mistake for IPv6: It's not backwards compatible developers admit", Network World, [Online] http://www.networkworld.com/news/2009/032509-ipv6-mistake.html?page=1.

[6] (ISOC), The Internet Society", [Online] http://www.isoc.org.

[7] R. Phil, "Internet Society Organization Member IPv6 Study,. Reston, VA 20190, USA : Internet Society, 2009.

[8] A. Hamarsheh, M. Goossens, R. Alasem, "Decoupling Application IPv4/IPv6 Operation from the Underlying IPv4/IPv6 Communication (DAC*)", American Journal of Scientific Research*, 2011, pp. 101-121.

[9] A. Hamarsheh, M. Goossens, R. Alasem, "Configuring Hosts to Auto-detect (IPv6, IPv6-in-IPv4, or IPv4) Network Connectivity", *KSII Transactions on Internet and Information Systems*, 2011, pp. 1230-1251.

[10] A. Hamarsheh, M. Goossens, R. Alasem, "Deploying IPv6 Service Across Local IPv4 Access Networks", *10th WSEAS International Conference on TELECOMMUNICATIONS and INFORMATICS (TELE-INFO '11)*, Lanzarote, Canary Islands, Spain, The ACM Digital Library, pp. 94-100, 2011.

[11] E. Nordmark"Stateless IP/ICMP Translation Algorithm (SIIT*)", Internet Engineering Task Force (IETF) RFC 2765*, 2000.

[12] M. Bagnulo, P. Matthews, I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers" *Internet Engineering Task Force (IETF) RFC 6146*, 2011.

[13] M. Bagnulo, A. Sullivan, P. Matthews, and I. Beijnum, "DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", *Internet Engineering Task Force (IETF) RFC 6147*, 2011.

[14] A. Hamarsheh, M. Goossens, R. Alasem, "AIN-SLT: Assuring Interoperability between Heterogeneous Networks (IPv4/IPv6) Using Socket-Layer Translator", *American Journal of Scientific Research*, 2011, pp. 38-48.

[15] A. Hamarsheh, M. Goossens, A. Al-qerem, Assuring Interoperability Between Heterogeneous (IPv4/IPv6) Networks without Using Protocol Translation, Accepted for publication on *the IETE Technical Review*, "to appear in March-April 2012 issue", 2012.