IPv6, A Passport For The Future Internet

Executive summary

After a historical review situating the exhaustion of the IPv4 address space, this paper underlines the real issues involved in this phenomenon and in the inevitable transition from IPv4 to IPv6. It then briefly highlights the contributions of IPv6, recalls the roles of the various Internet stakeholders and describes the communication models for which IPv6 integration should be prioritized. A set of illustrative but non-limitative examples of transition mechanisms are given in order to show IPv6 integration in practice within various technical contexts. Finally, this paper makes operational recommendations to support the deployment of IPv6 and launches an appeal for stakeholders to seize – immediately – the opportunities provided by IPv6, in order to make the "The Future Internet" an open field for innovation.

1 Background

The Internet was invented in the early 1970s in the United States and grew quite slowly until the late 1980s. The advent of the Web in the early 1990s, especially as a tool for business presence on the Internet, led to the massive deployment of millions of new network nodes and therefore to its huge success. The exponential growth in demand for IP addresses (unique numbers to ensure the identification and location of network equipment) made the Internet a victim of its own success... such that the first prediction of the "end of the Internet" was published in 1994!

Immediately, emergency measures were enacted and applied individually or jointly to "stop the haemorrhage." These measures included the exceptional allocation of "Class B"[1], address blocks, the reuse of Class C blocks[2], then the abolition of classes in the allocation and routing mechanisms of IP prefixes (CIDR, *Classless Internet Domain Routing*[3]). Later additions included the "development" of a private address space ([RFC 1918][4]), [RFC 1918]), the use of "proxies" or Network Address Translators (NAT[5]) to communicate with the outside.

In parallel to the application of these emergency measures, however, in 1993 the Internet Engineering Task Force (IETF) began the research work in order to prepare for the succession to IPv4, the limits of which by now had been demonstrated.

2 Specification for the new version of IP (v6)

The new version of the IP protocol that was to be developed required the following main objectives: extend the IP address space, correct the defects of IPv4 standard and improve its performance as much as possible, anticipate future needs, and promote innovation by simplifying the implementation of functional extensions to the protocol.

These objectives were constrained, however, in that they had to retain the principles that made IPv4 such a success: "end-to-end communication", "robustness", and "best effort".

3 What's new with IPv6?

Readers who wish to know in detail what IPv6 brings and how this new version works may refer to "IPv6, Theory and Practice"[6].

First of all, IPv6 provides a much larger address space than IPv4, with the transition from 32-bit coding of IPv4 addresses (4.3 billion addresses) to 128-bit coding of IPv6 addresses (3.4 10^{38}, or 340 billion, billion, billion, billion addresses). As a result, IPv6 is seen as an "enabler", capable of stretching our imagination. It is also an opportunity to restore the "end to end" communication model, one of the foundations of IPv4 that was shaken by the massive influx of NATs.

In addition, IPv6 provides a new form of auto-configuration, known as "stateless" for hosts. For a host, this mechanism consists in automatically building a local address for it to communicate with its neighbours, and then to build a global IPv6 address on the basis of the information announced by a local router on the network link. The stateless au-configuration mode is in addition to the existing "stateful" auto-configuration mode, covered by the Dynamic Host Configuration Protocol (DHCP).

Finally, IPv6 enables better integration of multicasting and better support for functional extensions, by encapsulating them in dedicated optional headers, such as those for security or mobility.

[1] The concept of class was deprecated upon CIDR arrival. A class B block has 2^{16} addresses, equivalent in number today to one /16.
[2] A class C block contains 2^8 addresses, equivalent in number to a /24.
[3] http://fr.wikipedia.org/wiki/Adresse_IP#Agr.C3.A9gation_des_adresses
[4] http://www.ietf.org/rfc/rfc1918.txt
[5] http://fr.wikipedia.org/wiki/Network_address_translation
[6] http://livre.g6.asso.fr/ (online in French) or http://www.getipv6.info/index.php/Book_Reviews websites.

4 What "exhaustion of IPv4 space" means, and what lies behind it?

In 2003, Geoff Huston (Chief Scientist, APNIC) forecast the lifetime of the IPv4 address space (*IPv4 Address Lifetime*) : **http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-IPv4-lifetime.pdf**
The message understood by his audience (mostly Regional Internet Registries [RIR]) was that if no major surprise occurred (change in model, China going digital, etc.) there would still be IPv4 addresses available up until 2030 - 2037 (see slides 49-51 of the presentation above). It was reassuring for the RIRs who were already trying to handle the shortage of IPs but were not very enthusiastic about the idea of pushing for the adoption of IPv6 at that time. The sigh of relief was audible... No need to rush onto IPv6, and so they could make haste slowly by consuming the remaining pool of addresses.

The surprise of the RIRs was all the greater when the same G. Huston informed them in 2007 that the exhaustion would occur much earlier than anticipated! The new forecasts gave 2010 and 2012 as the years when the Internet Assigned Numbers Authority (IANA) IPv4 pool and that of the RIRs would be depleted, respectively: **http://www.ripe.net/ripe/meetings/ripe-55/presentations/huston-ipv4.pdf** (see slides 12-15, 37, 38).

Now hear this: there's no time to lose! Panic stations on board the RIR... Quick, somebody do something... and all Randy Bush did was rub salt into the wound with his "doom and gloom" presentation: **http://rip.psg.com/~randy/071022.v6-op-reality.pdf**

Since that date, the automatic daily update by G. Huston has become a benchmark worldwide in forecasting: **http://www.potaroo.net/tools/ipv4/index.html**

On 3 February 2011 the IANA IPv4 pool was exhausted[7], an announcement during an ICANN-NRO-IAB-ISOC press conference[8].

The next deadline will be the depletion of the IPv4 pool at each RIR. This will depend on the rate of consumption at each RIR, but it is foreseeable that exhaustion will occur as of year-end 2011 or early in 2012 at the latest.

So what are the real issues involved in the depletion of IPv4 addresses, which still seems to surprise some quarters, to the point of creating a climate of panic? What will happen after the exhaustion? Who will be affected, and what will have to be done so that the Internet continues to operate in an acceptable manner?

Each of these questions deserves a detailed reply, but here are some general outlines of an answer.

For most Internet players, it will still be possible to (out)live IPv4 for a variable period, of up to several years, even after the depletion of the IANA + RIR pools. This is because those who have already stocked up with IPv4 addresses can ration their management (i.e. manage the shortage): the "grey market"[9] of IPv4 addresses is another option, certainly not one to be recommended, but one that is predictable, and finally some will put up with having multiple "layers" of NATs, as they have already done for several years.

None of these solutions, however, will do any more than postpone the problem, because the cost and complexity of deploying new services in IPv4 and the maintenance of the existing services increases significantly (due to the increase in v4private-v4public network translation, to the resurgence in v4-in-v6 and v6-in-v4 tunnelling / encapsulation at the level of both the backbones and the network access). In addition, those who have not taken the time to practice and master these techniques may face serious problems of stability in their network infrastructure and services.

Finally, it is worth noting that as network players deploy IPv6, anyone who stands in their way will run the risk of being excluded (loss of market / economic competitiveness). In short, simply being satisfied with IPv4 will become a genuine obstacle to innovation, such that the digital divide will only get bigger (as eventually will the bill).

[7] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
[8] http://www.nro.net/news/ipv4-free-pool-depleted
[9] It is called a "grey market" and not a "black market" in that it is possible to know the players in sales transactions of IPv4 prefixes, but not the amount of the transactions.

5 The integration of IPv6: how, who and where?

The integration of IPv6 is a gradual, collective initiative, for which all the players in the network are responsible, each according to their own roles and tasks. There will be no D-day for a sharp 'switchover' to IPv6. Before deciding how this should be carried out, the following questions have to be asked: what is to be done, by whom, and where?

Let us start with what everyone should do on their own computer, i.e. upgrade / update the operating system and network applications they use, to make them compatible with IPv6. For most operating systems and typical network applications, there is almost nothing else to do, since the recent versions handle IPv6 properly.

Users managing their own local area network (individuals, businesses, campus, etc.) must integrate IPv6 in their routers and subscribe to a connectivity service provided by an IPv6 ISP (preferably their usual IPv4 ISP if they have an IPv6 plan, or provided by someone else).

ISPs / operators in turn must integrate IPv6 in their routers within the access network & backbone, in their border routers (transit/peering), as well as in their other network systems such as firewalls and load balancers.

Furthermore, hosting services (web, DNS, etc.) must integrate IPv6 in their dedicated or shared network equipment and services.

However, unless you are an administrator of a large network, in general you will not have to handle all of these issues at once. In other words, you can usually take care of your business and ask the other players later to take charge of theirs, especially when you do not depend on them for yours! Even if you do manage a large network with multiple responsibilities, there is no point in doing everything at the same time, but gradually after a serious task of prioritisation and planning.

For further information about the role of each player, the following website may come in extremely useful to readers:
http://www.ripe.net/v4exhaustion/

6 IPv6 integration: communication models, classification

Communication model

IP communication requires the vertical and horizontal cooperation of all the underlying or intermediate components in the network. The following communication model[10] can be used to identify the types of communication that deserve special attention and require practical mechanisms of transition. What connects to what and how?

1. An IPv4 system connects to an IPv4 system across an IPv4 network;
2. An IPv6 system connects to an IPv6 system across an IPv6 network;
3. An IPv4 system connects to an IPv4 system across an IPv6 network;
4. An IPv6 system connects to an IPv6 system across an IPv4 network;
5. An IPv4 system connects to an IPv6 system;
6. An IPv6 system connects to an IPv4 system;

An analysis of the complexity and of the requirements shows that 1 & 2 are trivial, that 3 & 4 are less easy but involve no major obstacles, and 5 & 6 are more complex and that to date we have no satisfactory global solution to the problem.

[10] This model is based on the scenarios described in the document produced by the "Behave" Working Group of the IETF
http://tools.ietf.org/html/draft-ietf-behave-v6v4-framework

Classification of transition techniques

For 1 & 2, the **IPv4-IPv6 dual stack** technique today is the most practical, as long as IPv4 addresses are available. V6-v6 or v4-v4 communication.

In cases 3 & 4 which require crossing a different network family, there are several techniques based on **manual** (configured) or **automatic** tunnels For example, an IPv6 in IPv4 tunnel consists in encapsulating an IPv6 packet in an IPv4 packet and routing the IPv4 packet thus obtained by all the IPv4 routers on the path to the destination, until the tunnel end-point ("dual stack" router), which will decapsulate the IPv6 packet and will forward it to the IPv6 final destination

Cases 5 & 6 represent coexistence scenarios between existing IPv4-only networks and new IPv6-only networks. The techniques often applied in these cases are different forms of translation at the IP level or application proxies ("Application Level Gateways"). Note that the type 5 above has been considered low priority for the time being, the priority having been set for access to the IPv4 world (still dominant) from IPv6 systems (still minority).

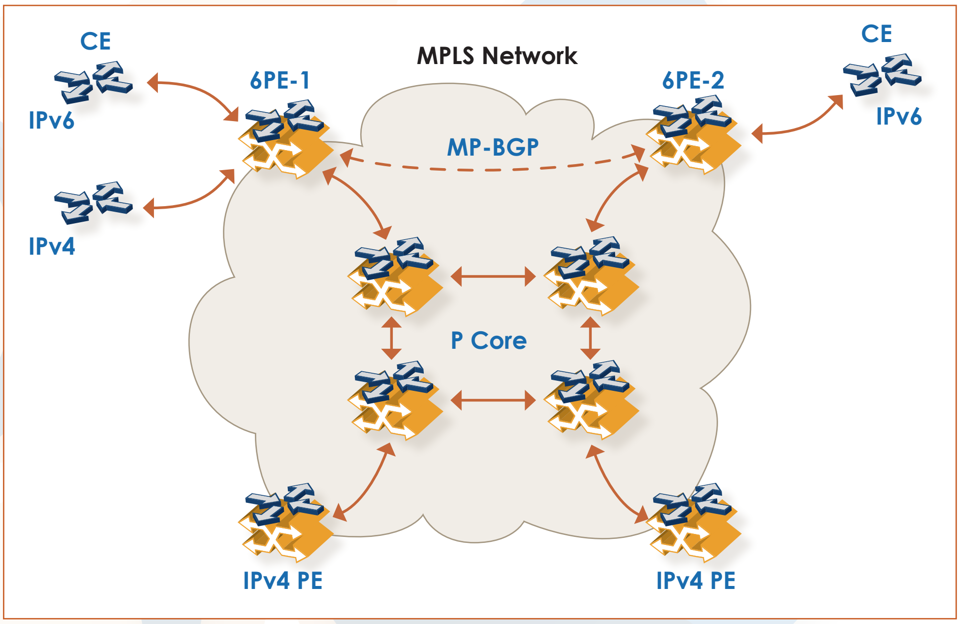
7 A few examples of transition mechanisms

It is very difficult to provide a comprehensive or detailed description of all the transition mechanisms that have been proposed so far. We shall content ourselves with a few examples that illustrate the classes of techniques mentioned above. These techniques should not be viewed as recipes to be systematically applied, but rather as tools available for network players to select according to their individual needs, wishes, and constraints.

6PE / MPLS tunnels in an operator's core network

Operators that already have a Multi-Protocol Label Switching type (MPLS) core network can use tunnels called 6PE , as specified in [RFC 4798][11]. More specifically, this involves establishing "BGP peerings" between IPv6-enabled border routers, without modifying the core routers, thereby solving problem 4 in the model above. This technique has the advantage of being flexible, gradually scalable, and inexpensive

The following figure illustrates 6PE mechanism:



11 *Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE),* http://www.ietf.org/rfc/rfc4798.txt

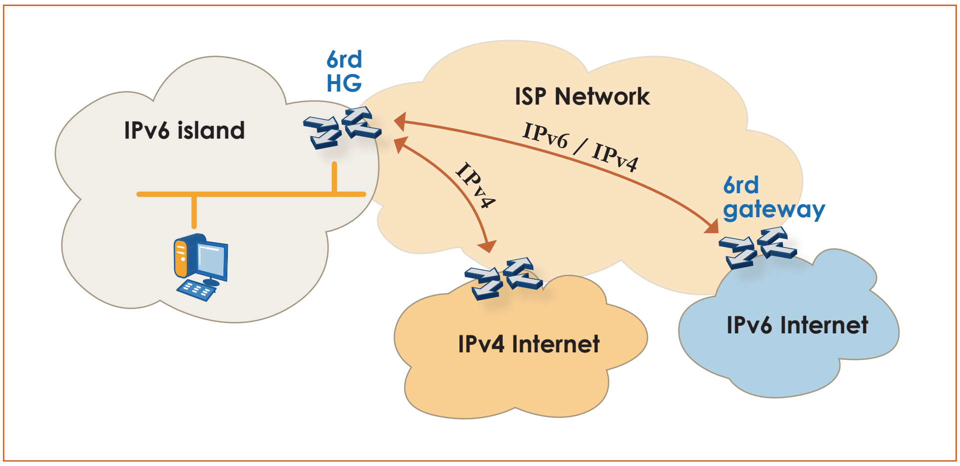
6rd ("Rapid Deployment") tunnels, a better way than 6to4 to connect a customer site!

This is a solution derived from 6to4 ([RFC 3056][12]), specified in [RFC 5569][13] for information, and then in [RFC 5969][14] in an attempt to standardise the mechanism. This solution addresses problem 4 in the communication model above.

The principle is relatively simple: the ISP provides IPv6 connectivity to its subscribers with minimal impact on its access network, reusing the good properties of 6to4. This is possible because the IPv6 prefix of the subscriber is partly derived from the IPv4 address that has been assigned to it (no specific addressing plan to deploy) and the ISP can incrementally size its access network by gradually rolling out Anycast[15] relays. The latter are responsible for decapsulating and then routing the subscribers' IPv6 packets. That way, the 6to4 security / performance issues referred to by [RFC 3964][16] are largely avoided.

This solution was deployed for the first time in 2007 by Free, a French ISP, and has since then attracted growing interest from other ISPs, either on a trial basis or for deployment in production[17].

The following figure illustrates 6rd mechanism:



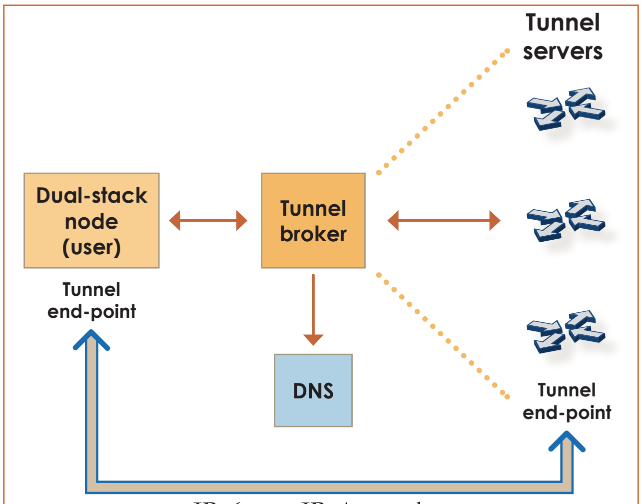
Site / terminal connectivity: the Tunnel Broker

These techniques are slightly different from each other, but are all based on the "Tunnel Broker" concept described in [RFC 3053][18]. This solution addresses problem 4 in the communication model above.

As its name suggests, the "broker" provides an interface for exchanges between clients wishing to connect their machine or site to the IPv6 Internet and an IPv6 connectivity provider via negotiated, dedicated tunnels (IPv6 in IPv4). Via this intermediate interface (typically a web interface), the clients specify their wishes regarding the allocation of IPv6 address(es) (either a single address, or "prefix/length" depending on the policy of the tunnel supplier) and provide additional information, including their IPv4 address (for the tunnel), operating system, etc. The "Broker" forwards the information collected to the tunnel provider on the one hand, and secondly, provides the clients with the proposed parameters to connect (chosen address or IPv6 prefix, start script according to the operating system, etc.). The client and tunnel server each activate their tunnel end-point and that is all.

[12] http://www.ietf.org/rfc/rfc3056.txt
[13] *IPv6 Rapid Deployment on IPv4 infrastructures (6rd),* Rémi Després http://www.ietf.org/rfc/rfc5569.txt
[14] http://www.ietf.org/rfc/rfc5969.txt
[15] http://fr.wikipedia.org/wiki/Anycast
[16] http://www.ietf.org/rfc/rfc3964.txt
[17] http://en.wikipedia.org/wiki/IPv6_rapid_deployment
[18] http://www.ietf.org/rfc/rfc3053.txt
More recently, the Tunnel Setup Protocol (TSP), which had been designed many years ago, was published in [RFC 5572] http://www.ietf.org/rfc/rfc5572.txt ("EXPERIMENTAL").

The following figure illustrates generic "Tunnel Broker" mechanisms:



IPv6 over IPv4 tunnel

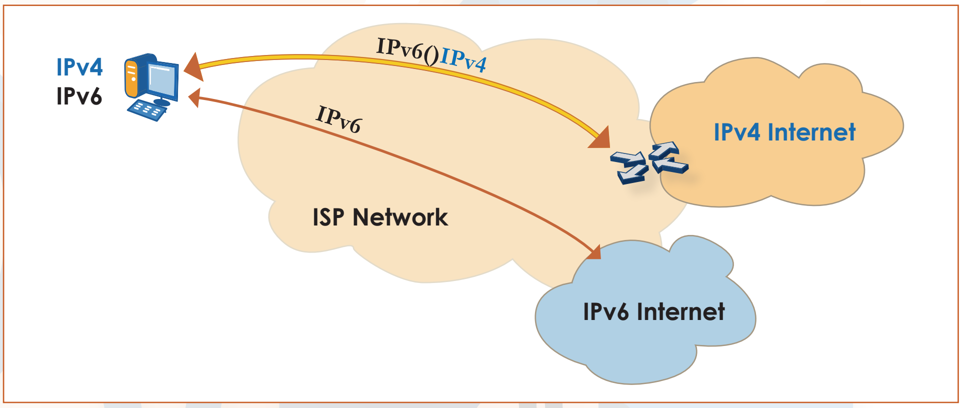
There are several tunnel providers in various parts of the world. The following three are among those known worldwide: gogo6/Freenet6[19], Hurricane Electric[20] and SixXS[21]. The following page provides further information and details on the features provided by the various solutions: http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers

DS Lite: subscriber access to IPv4 and IPv6 without IPv4 public address

This technique was developed by the "Softwires" IETF working group[22] in anticipation of the exhaustion of IPv4 address space. It is specified in the document (work in progress) *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*[23].

DS-Lite prévoit un boîtier NAT associé à plusieurs abonnés, hébergé par le FAI, le *Carrier Grade NAT* (CGN)[24]. Subscribers get from their ISP an IPv6 prefix and an IPv4 private address. The CGN ensures the translation between the private IPv4 on the subscriber side and the public IPv4 on the ISP side (core network). In addition, IPv4 traffic from the subscriber is transported over IPv6. That way, instead of a double-NAT scenario, the IPv4 packets (private source address) are "tunnelled" in IPv6 packets to the CGN. The latter keeps the context based on the IPv6 public address of the subscriber.

The following figure illustrates the DS-Lite mechanism:



This technique has been implemented by the ISC under the name AFTR[25], adopted by Comcast (www.networkworld.com/news/2010/031810-comcast-isc-ipv6-tool.html) Industrial deployment is also scheduled with FT-Orange (France).

[19] http://gogonet.gogo6.com/
[20] http://tunnelbroker.net/
[21] http://www.sixxs.net/
[22] http://datatracker.ietf.org/wg/softwire/
[23] http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite
[24] http://en.wikipedia.org/wiki/Carrier_Grade_NAT
[25] http://www.isc.org/software/aftr

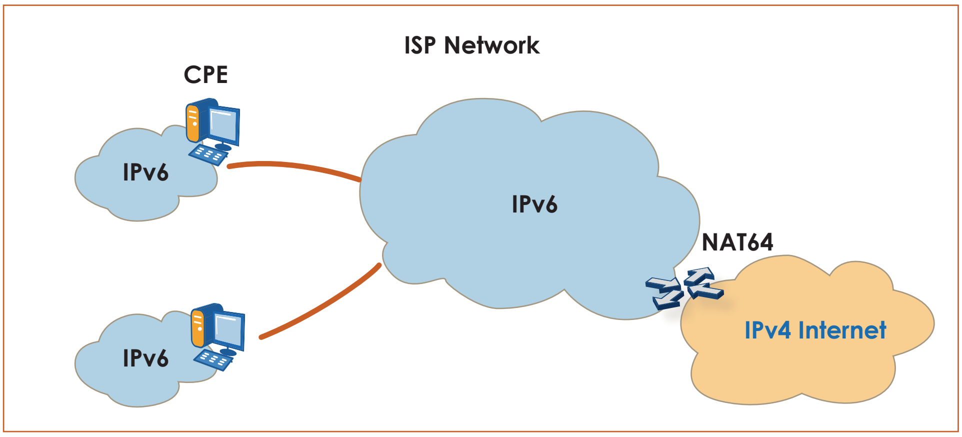
"NAT64 + DNS64" for coexistence: enabling IPv6 equipment to connect to an IPv4 one

This technique is the work of the "behave" IETF working group[26]. It addresses issue 6 identified in the model above.

While the "Dual-Stack" was supposed to be massively deployed for a smooth v4-v6 transition before the exhaustion of the IPv4 address space, it did not work as expected. Very little deployment has been registered so far and the days of the IPv4 space are counted. It is therefore difficult to circumvent v4-v6 translation if one wants to continue to access existing "IPv4-only" services.

The principles, framework, and key constraints in applying this technique are described in the following IETF documents: [RFC 6144] *Framework for IPv4/IPv6 Translation*[27].

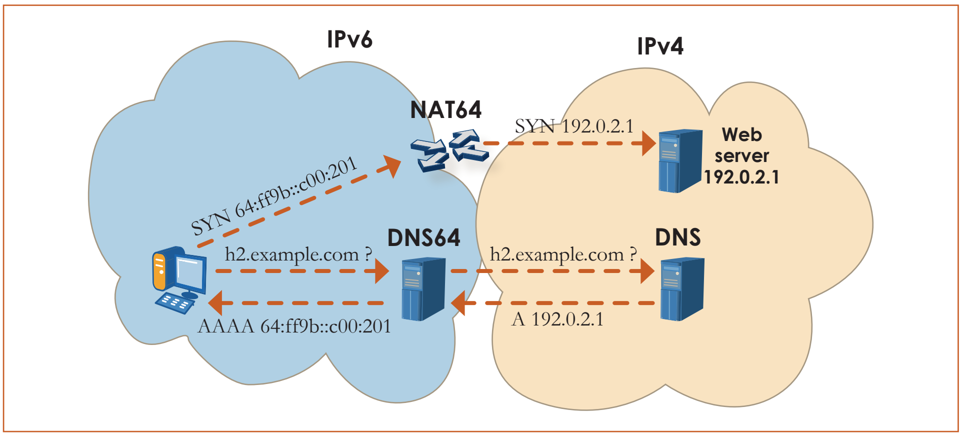
The following figure illustrates the framework:



The translation mechanisms are specified in three separate IETF documents:

- [RFC 6145] *IP/ICMP Translation Algorithm*[28]: a stateless translation mechanism;
- [RFC 6146] *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*[29]: an effective replacement for NAT-PT (deprecated by [RFC 4966][30], because of the issues and risks involved);
- [RFC 6147] *DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*[31]: a mechanism for synthesizing IPv6 DNS records (AAAA) from DNS IPv4 records (A) thus allowing "IPv6-only" equipment to initiate communication with "IPv4-only" equipment, through the NAT64 box.

The following figure illustrates NAT64/DNS64 mechanisms:



The Canadian company Viagénie offers an implementation of NAT64/DNS64[32], which it has experimented during recent IETF meetings. For further information, readers may refer to the following presentation : http://www.slideshare.net/IOSHints/nat64-and-dns64-in-30-minutes

26 http://datatracker.ietf.org/wg/behave/

27 http://www.ietf.org/rfc/rfc6144.txt See also a summary of this RFC in French: http://www.bortzmeyer.org/6144.html

28 http://www.ietf.org/rfc/rfc6145.txt See also a summary of this RFC in French: http://www.bortzmeyer.org/6145.html

29 http://www.ietf.org/rfc/rfc6146.txt See also a summary of this RFC in French: http://www.bortzmeyer.org/6146.html

30 http://www.ietf.org/rfc/rfc4966.txt

31 http://www.ietf.org/rfc/rfc6147.txt See also a summary of this RFC in French: http://www.bortzmeyer.org/6147.html

32 http://ecdysis.viagenie.ca/

8 A few practical recommendations for IPv6 integration

At the risk of breaking down open doors, it is useful to recall that **native IPv6 everywhere** is the **only viable solution**. Since, however, this ultimate goal cannot be achieved in overnight, the following practical recommendations are given to support the gradual transition:

- Consolidate IPv6 in the infrastructure wherever possible, and without delay;
- Ensure the "dual-stack" wherever possible (for smooth integration of IPv6 in production);
- Secure / check the reliability of the IPv6 networks and services as and when they are deployed. This NIST document may be of great help in doing so: *Guidelines for the Secure Deployment of IPv6*[33];
- Think of the IPv6-IPv4 functional parity in deployment, but also of parity in terms of performance, such as load / speed, resilience, response time, etc.

Another obvious factor that is worth recalling, if only to reassure those who are slow to adopt IPv6, is that the complexity of deploying IPv6 decreases, and therefore so does its cost.

This is because the natural refresh cycles of network equipment and software mean it is possible to have IPv6 without even asking in most cases, and often with no additional financial cost . Care should therefore be taken not to buy solutions despite their attractive price when they are already or will shortly become obsolete, even if it is certain that the deployment of IPv6 will only occur several months later: the amortisation of these investments usually covers several years (3-5 years)! In this regard, for those wishing to acquire network hardware / software solutions, the requirements in terms of IPv6 compatibility can be formulated using the following document: http://ripe.net/docs/ripe-501.html.

As with any new technology, IPv6 requires a major investment in training. Students, engineers, trainers, and network instructors will need to be trained at some point. Training is now considered the largest cost item in the gradual integration of IPv6.

Finally, those who are convinced of the need to deploy IPv6, who have already begun the task but who are still anxious about the operational impact of the transition to IPv6 on their services in production, even partially, could seize –if time still permits - the "IPv6 Day"[35], opportunity on 8 June 2011. It involves a global experiment designed to provide the content of your website in dual stack (IPv4 and IPv6) for 24 hours[36]. A huge turnout for the event will help diagnose the largest possible number of operational issues and resolve them collectively in a timely manner, thereby promoting a more sustained deployment of IPv6. Organisations that already have IPv6 in production in their network services, such as AFNIC, which has been ready since 2003[37], can also participate. In addition, even if it not for the same objectives (test), those who are experienced in IPv6 are invited to show their support for those who are starting, and help them in their transition from IPv4 to IPv6.

9 Seize the IPv6 opportunity – now!

IP resources are abundant once again with the arrival of IPv6. As a result, fairness in access to resources on the global level has been restored[38].

From this point of view, thanks to IPv6, innovation is encouraged and the digital economy stimulated. It is without doubt the most important and the most tangible benefit of IPv6, the search for a "killer application" having proved to be vain.

While for some technologies, there is a battle for the essential resources, with IPv6, it is a different story. Since IPv6 addresses are abundant, the battle is more in terms of the mastery of IPv6 technology itself and the timely availability of innovative products and services that depend on it.

33 http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
34 A few years ago, certain hardware and software vendors offered IPv6 for a price, in order to buy the license or specific cards that went with it. Others proposed IPv6 "at no additional cost", but in fact an outlay was required, in order to obtain the additional memory needed to manage IPv6.
35 http://isoc.org/wp/worldipv6day/how-to-join/
36 http://test-ipv6.com/ipv6day.html
37 http://www.afnic.fr/actu/nouvelles/118/communique-de-presse-nbsp-ipv6-entierement-integre-dans-le-systeme-de-production-de-l-afnic-des-le-1er-octobre-2003
38 This is far from being the case for IPv4, given the background to its adoption and deployment.

10 Useful references

Portals:

- http://www.g6.asso.fr/
- http://www.ipv6actnow.org/ (RIPE)
- http://www.getipv6.info/ (ARIN Wiki documentation)
- http://www.ipv6forum.com/
- http://www.sixxs.net/

Books, blogs, reports, articles:

- The G6 blog: http://g6.asso.fr/blog
- Book *IPv6, Théorie et pratique* (in French) of the G6 (Gisèle Cizault :-)): http://livre.g6.asso.fr/
- *Yet another technical blog* : http://blog.ioshints.info/search/label/IPv6
- OECD report with deployment measurements: http://www.oecd.org/sti/ict/ipv6
- http://www.circleid.com/posts/ip_address_exhaustion_in_12_easy_questions/
- http://www.circleid.com/posts/ipv6_and_transitional_myths/
- http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303870A1.pdf
- Dossier ZDnet sur IPv6 : http://www.zdnet.fr/dossier/ipv6.htm

Feature article written by Mohsen Soussi, AFNIC R&D Manager

Read all of our issue papers:
http://www.afnic.fr/actu/presse/liens-utiles_en

web www.afnic.fr - afnic@afnic.fr