Overview of IPv6 transition solutions and possible migration plans

Péter Bálint
Department of Telecommunications
Széchenyi István University
Győr, Hungary
Peter.Balint4@gmail.com

***Abstract*— In the 1990s it became obvious that the 32-bit address size of the IPv4 protocol would be too small in the near future, so IETF started working on an updated version of the address space with larger addresses, and the result of it was the introduction of IPv6. Unfortunately, the resulting protocol is not backward compatible with IPv4, so there was a need for additional tools to allow the transition from IPv4 to IPv6. Then IETF started introducing transition technologies for making the transition easier. The best way is still not defined. Could we find it? Or do we have to use a mixture of transition strategies and suit or change them according to the situation's requirements? In this paper, the most important IPv6 transition technologies are surveyed and their typical application situations are introduced. Two case studies are presented about the possible IPv6 transition scenario an industrial and an Internet Service Provider.**

Keywords—IPv6 transition, Mixing transition technologies, Possible Industrial and ISP migration plan, IPv6 migration design

I. INTRODUCTION

We are at the point when the Internet has outgrown the IPv4 address space. In the year 2011 the Internet Assigned Numbers Authority (IANA) delegated the last five "/8" IPv4 address blocks to the five Regional Internet Registries [1]. In the last 20 years, service providers tried to postpone the time of transition with different solutions like NAT44 or NAT444, and because of this practice the migration process went very slowly. The change comes at the depletion of the IPv4 address pool, which speeds up the process.

II. IPV6 TRANSITION TOOLS

In the history of the Internet, there was only one successful protocol change that happened in a short period of time/moment. This was in 1983, when the ARPANET was migrated from NCP to TCP/IP. This type of change is impossible today because of the very heterogeneous structure of the network and the huge amount of network devices [2].

So we could speak about a long term step-by-step process, that is to say parallel usage of IPv6 and IPv4. The process started in the 90s with very low pressure, but the depletion of IPv4 brought a big change in attitude.

The IPv6 transition includes the integration of, co-existence of and inter-operation between IPv4 and IPv6 networks and equipment and it is a very broad subject. First, we give a brief overview of the most common tools. The term 'IPv6 transition' is a bit misty: it could mean a transition or migration from IPv4-only operation to IPv6-only operation, but in practice, IPv6 deployment will be a step-by-step process. The IPv4 and IPv6 co-existence will be a medium-term strategy. The transition technologies need to handle a variety of different scenarios of IPv4 and IPv6 interworking.

There are three main classes of transition:

- Dual-stack – here network elements use both protocols and can communicate with each other using either protocol.
- Tunnels – these generally involve encapsulating IPv6 over IPv4, or IPv4 over IPv6, to allow separated protocol islands to communicate over the other protocol's paths. This requires free paths on firewalls, routers and other network elements.
- Translation – is a solution for communicating between IPv6-only and IPv4-only areas. The translation is a method of remapping one IP address space into the other and the conversion of the IP header between IPv4 and IPv6.

A. Dual-stack

Dual-stack technology is one of the most direct methods. The dual-stack protocol equips partial hosts or routers with two protocol stacks, an IPv4 and an IPv6. It can communicate with the system of IPv4, and also with the system of IPv6.

In the dual-stack case routers have to use the two independent (IPv4 and IPv6) routing protocols, and maintain two routing tables, an IPv4 and an IPv6. The IPv4 packets are forwarded according to the IPv4 routing table, and the IPv6 packets are forwarded in accordance with the IPv6 routing table. (Figure 1.)

Most of the European and international NRENs (National Research and Education Network) have deployed IPv6 dual-stack on their backbone networks. Deploying dual-stack assumes enough IPv4 addresses are

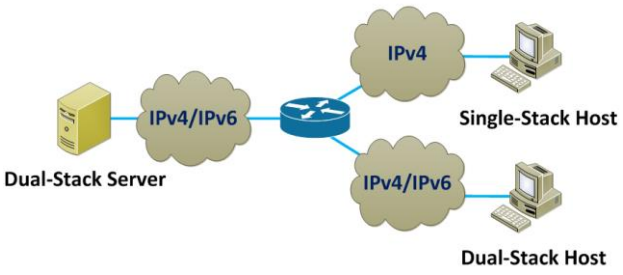

Figure 1. Dual-stack architecture.

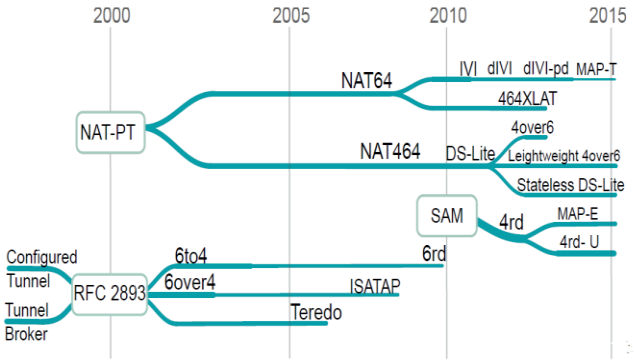

Figure 2. Evolution of IPv6 transition protocols. [4]

available, but it is also perfectly possible to deploy IPv6 with global addresses alongside IPv4 and NAT. [3] The biggest disadvantage of dual-stack networking is the complexity. All network elements, their management and monitoring systems need to support dual-stack operation. An important consideration for dual-stack is security. A good summary of IPv6 transition security issues can be found in reference 5 [5].

Before the description of translation and encapsulation technologies, we show the evolution of them in Fig. 2.

B. *Translation technologies*

We use the word "translation" when we convert the traffic between the two protocols from IPv4 to IPv6 or vice versa, that is to say transforming the headers and payload. This mechanism can be established at different layers in the protocol stack, consisting of network, transport, and application layers. The translation process can happen in the end systems or in network devices.

There are four well known types of translation:

- NAT-PT (now obsolete)
- Stateless NAT64
- Stateful NAT64
- 464XLAT

1) *NAT-PT*

NAT-PT (Figure 3.) has two types [6]. The traditional-NAT-PT allows hosts within a V6 network to access hosts in the V4 network. The traditional-NAT-PT sessions are uni-directional, supporting outbound communication from the V6 network. The other type is the Bi-directional-NAT-PT, which permits sessions in both directions, inbound

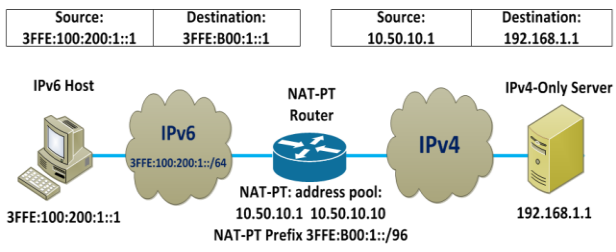

Figure 3. NAT-PT architecture

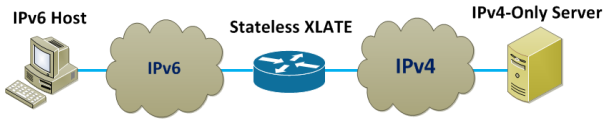

Figure 4. Stateless NAT64 architecture

and outbound. There are a lot of significant issues with NAT-PT, so NAT-PT was retired.

2) *Stateless NAT64*

The stateless NAT64 [7] architecture is shown in Fig. 4. The main features are:

- each IPv6 address is translated into a corresponding IPv4 address
- only ICMP packets and IP headers are translated

3) *Stateful NAT64*

Stateful NAT64 [8] (or "NAT64" for short), the architecture shown in Fig. 5., masks several IPv6 nodes behind a few IPv4 addresses. Its main features are:

- It is very similar to PAT (stateful NAT44)
- Individual TCP and UDP sessions + ICMP replies are translated
- Source and destination IPv6 addresses + port numbers used in lookups
- It should be used with DNS64 [9], which embeds the IPv4 address of the IPv4-only server into an IPv6 address so that it can be used by the IPv6-only client.

4) *464XLAT*

464XLAT [10] (Fig. 6.) combines the Stateful protocol translation in the core (PLAT) and stateless protocol translation at the edge (CLAT). It is a simple and scalable

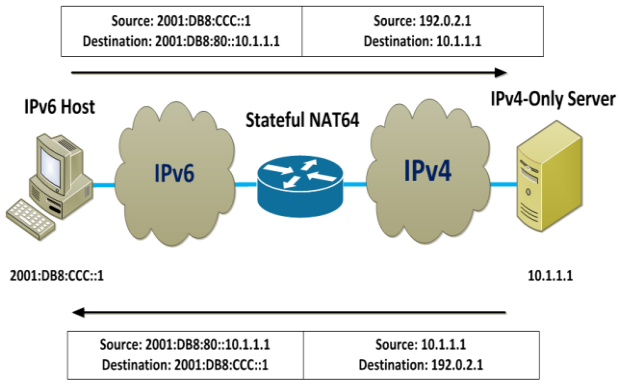

Figure 5. Stateful NAT64 architecture

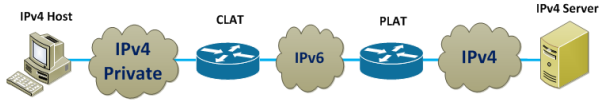

Figure 6. 464XLAT architecture

TABLE I. . COMPARISON OF STATEFUL AND STATELESS NAT64

Stateless NAT64	Stateful NAT64
1:1 translation	N:1 translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)	No requirement on the nature of IPv6 address assignment

technique to quickly deploy limited IPv4 access service to IPv6-only edge networks without encapsulation.

- PLAT is a provider-side Stateful NAT64 translator. It translates N:1 global IPv6 addresses to global IPv4 addresses, and vice versa.
- CLAT is a customer-side Stateless NAT64 translator. It translates 1:1 private IPv4 addresses to global IPv6 addresses, and vice versa.

C. Tunneling Technologies

The concept behind tunneling is not new; many people use tunneling daily. For example, many companies use IPsec or Secure Sockets Layer (SSL) tunnels to secure information when it is being transmitted over an untrusted network.
Many tunneling methods are available to support IPv4 over IPv6 or IPv6 over IPv4 tunneling. The type depends on the specific implementation details. There are two main types of tunnel: Manual tunnels and Automatic tunnels.

1) Manual tunnels

Manual tunnels are manually configured and configuration is required at both ends of the tunnel. The Administrator will always know how their tunnels are created. From a management perspective, manual tunnels are good for implementation, but from a configuration perspective they are a little bit more time consuming.

2) Automatic tunnels

Automatic means that tunnel configuration is carried out with no additional management. This method is considered as the most popular choice in the field of automatic tunneling techniques.
Types of automatic tunnels:

- 6to4 (RFC 3056)
- 6rd (RFC 5569)
- Teredo (RFC 4380)
- ISATAP (RFC4214)
- TSP (RFC 5572)

III. REAL-LIFE INDUSTRIAL EXAMPLE

We introduce a real-life migration concept based on [12]. The authors define a 3-stage process driven by several motivational factors which could be very useful in other migration scenarios as well:

- Minimize network topology change
- Simplify upgrading process
- Endpoint upgrade is independent of network change
- Protect investment on existing machine endpoints for a longer period

Stage 1 – Migrating IPv4-Only Network to Dual-Stack Network (2-3 years)

The process involves the provisioning and configuration of NAT64 gateways and DNS64 servers, including:

- Replace regular layer-3 routers and gateways with NAT64-capable devices via HW and/or SW upgrade
- Replace IPv4 DNS servers with DNS64 servers
- Install DHCPv6 servers to serve stateful DHCP requests
- Use a central NMS (Network Management System) to manage all NAT64 Gateways and DNS64 Servers and ensure consistent configuration across all systems

Stage 2 – Migrating IPv4-Only Endpoints to IPv6 (5-15 years)

- Upgrade servers, employee desktops, laptops and important IT assets to IPv6
- Upgrade Historian and other assets on the Supervisory network to IPv6
- Upgrade PLCs, Drives and other I/O devices to IPv6

Stage 3 – Migrate Dual-Stack Network to IPv6-Only Network (1-2 years)

Stage 3 begins when all the endpoints on the network support IPv6. At which point, network operators can simplify the network management and configuration by removing or disabling NAT64-related functionality and infrastructure. To ensure a smooth transition, a phased approach is also recommended:

- Selectively disable NAT64 functionality on NAT64 gateways and DNS64 servers and test drive an IPv6-only network
- Create small IPv6 pockets by replacing NAT64 gateways with regular IPv6 gateways. Merge small IPv6 pockets into bigger IPv6-only subnets
- Remove all IPv4 and NAT64 infrastructure assets
- If we would like to access IPv4 Internet, NAT64 installation is needed in LAN-IPv4 Internet edge

This migration scenario could be good for small- and medium-sized companies, but the migration is not so simple and fast for service providers, large enterprises and big companies.

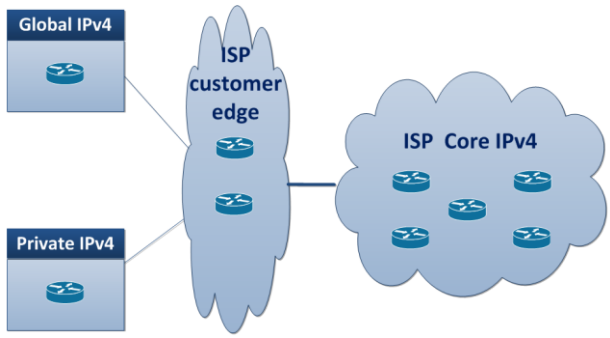

Figure 7. Only IPv4 ISP architecture

Next we will introduce a possible migration process for a service provider.

The depletion of the IPv4 address space affected strongly the service provider segment. The reasons: it makes harder the delivery of new internet services, meaning it is hard to increase the number of new customers. On the other hand, demand increases strongly because of the decreasing internet costs and the boom of IoT.

IV. Possible ISP migration plan

The ISPs have two types of customers (Fig. 7.):

1. Customer with Global IPv4 address.
2. Customer without Global IPv4 address. This type was unknown earlier. Earlier there was Global Fix and not Fix-IP-based internet service, and due to the depletion of IPv4 address space the providers introduced this type in order to delay the introduction of IPv6. This is a temporary solution with disadvantages. The target customer groups are the internet surfers and normal mobile subscribers.

According to our experiences, we defined a 3-step migration process for an ISP

Step 1. - Provide IPv6 addresses for customers

In this step, the ISP handles 4 types of traffic (Fig. 8.):

1. (yellow) IPv4 customer to IPv4 Internet: Global IPv4 only routing at customer edge, Private IPv4 NAT44 at customer edge
2. (red) IPv4 customer to IPv6 Internet: Global IPv4-only routing needed, Private IPv4 NAT44 at customer edge and stateful or stateless (the type is decided by the requested service and customer needs) NAT46 at V6 Internet edge
3. (purple) IPv6 customer to IPv4 Internet: Stateful or stateless NAT64 at customer edge (the type is decided by the requested service and customer needs)
4. (green) IPv6 customer to IPv6 Internet: Tunneling 6to4 between customer and v6 Internet edge

NAT46 was not mentioned earlier as we could find only draft RFC [11] in this topic, and at design phase we have to investigate the usage of NAT46 or other possible solutions. Nevertheless it could happen that all of the IPv6 servers will support Dual-stack, this scenario makes unnecessary the usage of NAT46. The time period of the first step is strongly influenced by new address needs and the growth of the number of customers.

Step 2. - Migration of ISP core

We can speak about 4 types of traffic too (Fig. 9.):

1. (yellow) IPv4 customer to IPv4 Internet: 4in6 Tunneling between customer and v4 Internet edge, the Private IPv4 addresses NAT44 at customer edge
2. (red) IPv4 customer (or private IPv4 customer) to IPv6 internet Stateful or stateless NAT46 at customer edge (the type is decided by the requested service and customer needs)
3. (purple) IPv6 customer to IPv4 Internet: Stateful or stateless NAT64 at v4 Internet edge (the type is decided by the requested service and customer needs)
4. (green) only routing needed

As above mentioned before using of NAT46, we have to ponder the opportunities.

Step 3. - Retire IPv4

As the last step (Fig. 10.), we migrate to an IPv6-only

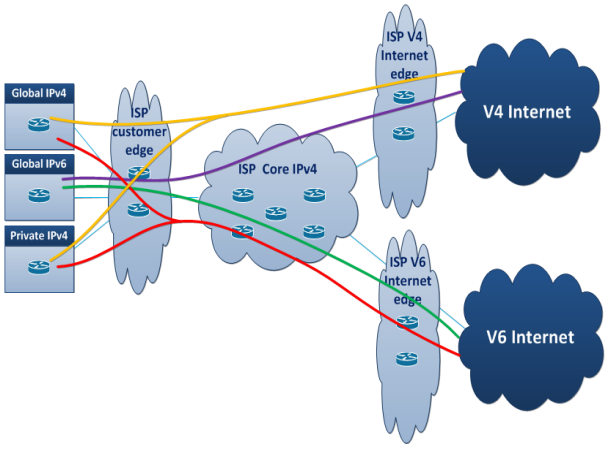

Figure 8. Step 1. architecture

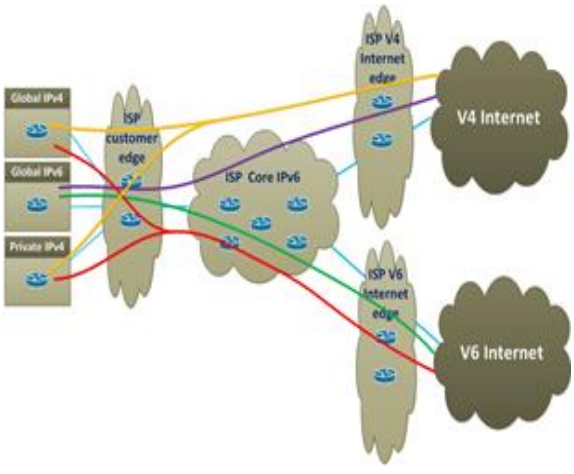

Figure 9. Step 2. architecture

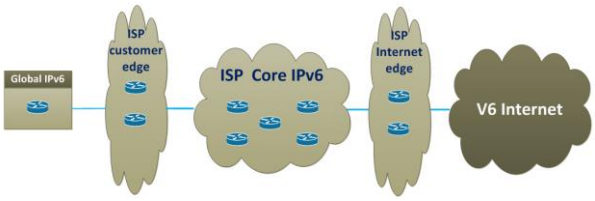

Figure 10. Step 3. architecture

network. It is not sure that the Internet will ever retire IPv4, possible never. If yes, this could be the last step.

V. THE ISP MIGRATION PROJECT

The 3 steps mentioned above define the frame of migration; the real process has many more phases. A good way is to divide every step into three different phases:

- design phase
- implementation phase
- cyclic operation phase

Design phase

The main activities in this phase:

- Traffic analysis and estimation
- Scaling the hardware and software elements according to the needs
- Design the implementation plan
- Define the threshold criterion to start the preparation for the next step

Implementation phase

We implement the new architecture and go live.

Cyclic operation phase

In the operation phase, we continously monitor and analyse the network and make changes to satisfy needs. A good example: if an increase in the number of IPv6 customers leads to the address translation capacity getting close to its limit, then we have to enhance the system capacity.

If the system reaches the threshold where the usage of the next step architecture is more efficient, then we start the design phase of the next step.

Next I investigate some usable resourse at design. We can find several publications about performance analysis and hardware resource optimatization for different solutions. For tunneling, we could use a Linux-based solution to satisfy the requirements [13].

For address translation, there are two important NAT64 solutions which offer the performance and stability to satisfy ISPs' needs, namely the PF (Packet Filter) of OpenBSD and the TAYGA+iptables under Linux [14]. As for NAT64, we have to consider the port number consumption as well: this is a crucial parameter at design [15]. For name server functionality, BIND is a good software to satisfy production network needs [16].

VI. CONCLUSION

We are at the time when we can not avoid the usage of IPv6. The lack of IPv4 addresses strongly affects the ISPs. In this paper, we introduced the different IPv6 transition solutions and two migration plans, the introduced plans could be very useful if a company or service provider start the preparation to a migration. Finally, we defined the main phases of a possible migration project and then presented some useful resources for the design phase.

REFERENCES

[1] The Number Resource Organization, "Free pool of IPv4 address space depleted" http://www.nro.net/news/ipv4-free-pool-depleted

[2] G. Lencse, S. Répás, A. Arató, *IPv6 és bevezetését támogató technológiák*, 1st. ed. Budapest: HunNet-Média Kft., 2015. DOI: 10.18660/ipv6-b1.2015.9.1

[3] T. Chown, "IPv6 Technical Guide", [Online] Available: https://community.jisc.ac.uk/system/files/487/ipv6-tech-guide-for-web.pdf

[4] M. Georgescu, *Evolution of Translation and Encapsulation Technologies*, PhD dissertation, NAIST, 2016.

[5] E. Davies, S. Krishnan, P. Savola, "IPv6 Transition/Coexistence Security Considerations", RFC 4942, DOI: 10.17487/RFC4942

[6] G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766. DOI: 10.17487/RFC2766

[7] X. Li, C. Bao, F. Baker, "IP/ICMP Translation Algorithm", RFC 6145. DOI: 10.17487/RFC6145

[8] M. Bagnulo, P. Matthews, I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146 DOI: 10.17487/RFC6146

[9] M. Bagnulo, A. Sullivan, P. Matthews, and I. Beijnum, "DNS64: DNS extensions for network address translation from IPv6 clients to IPv4 servers", IETF RFC 6147. DOI: 10.17487/rfc6147

[10] M. Mawatari, M. Kawashima, C. Byrne, 464XLAT: Combination of Stateful and Stateless Translation RFC 6877. DOI: 10.17487/RFC6877

[11] D. Liu, H. Deng, "NAT46 considerations", Expired Internet-Draft, 2010, [Online], Available: https://tools.ietf.org/html/draft-liu-behave-nat46-02

[12] X. Yang, M. Dalal, "Migrating Industrial IPv4 Network to IPv6", ODVA 2014 Industry Conference & 16th Annual Meeting 2014, March 11-13, Phoenix, Arizona, USA, [Online], Available: https://www.odva.org/Portals/0/Library/Annual_Meeting_2014/2014_ODVA_Conference_Yang%20Dalal_%20Migrating_Industrial_IPv4_Network_to_IPv6_FINAL.pdf

[13] S. Répás, V. Horváth and G. Lencse, "Stability Analysis and Performance Comparison of Five 6to4 Relay Implementations" *Infocommunications Journal*, vol 8. no. 2. pp. 1-10

[14] G. Lencse and S. Répás, "Performance Analysis and Comparison of the TAYGA and of the PF NAT64 Implementations", *Proceedings of the 36th International Conference on Telecommunications and Signal Processing (TSP 2013)*, Rome, Italy, 2013. July, 2-4. Brno University of Technology, pp. 71-76. DOI: 10.1109/TSP.2013.6613894

[15] S. Répás, T. Hajas and G. Lencse, "Port Number Consumption of the NAT64 IPv6 Transition Technology" *Proceedings of the 37th International Conference on Telecommunications and Signal Processing (TSP 2014)*, Berlin, Germany, 2014. July, 1-3. Brno University of Technology, pp. 66-72. DOI: 10.1109/TSP.2015.7296411

[16] G. Lencse, and G. Takács, "Performance Analysis of DNS64 and NAT64 Solutions" *Infocommunications Journal*, vol. IV, no. 2,. June, 2012, pp. 29-36.