INTERNET PROTOCOL VERSION 6 – BENEFITS, CO-EXISTENCE MECHANISMS AND STRATEGIES FOR MIGRATION.

Delyan Genkov

Abstract: През февруари 2011 бяха раздадени последните порции от IPv4 Интернет адреси на регионалните регистратори. Повече адреси от този протокол няма да бъдат раздавани. На Интернет доставчиците и организациите се препоръчва да обмислят своя преход към новия Интернет протокол – IPv6. Това не може да стане едновременно навсякъде, затова в различни периоди двете версии ще работят съвместно.

Тази публикация има за цел да опише и сравни предимствата и недостатъците на възможните подходи за миграция, както и механизмите за съвместно съществуване на двата протокола.

Keywords: Интернет, IPv4, IPv6, миграция, съвместно съществуване

Introduction

Internet is close to one of most important changes in its history – the migration to Internet Protocol version 6 (IPv6). This process is expected to bring many benefits, most important of which is greatly increased address space. Along with these benefits, there are many visible and maybe some hidden disadvantages and inconveniences caused by this migration. One of these is the impossibility for simultaneous migration in the whole Internet. In addition not every system connected to an IP network can be migrated, without significant hardware and/or software upgrades. This is very important regarding to some embedded systems, like industrial controllers, network cameras, print servers and others, which do not have support of the newer protocol. Thus systems must be completely replaced or a special care must be given for co-existence of both protocols.

There are many types of organizations and their networks have different requirements. This paper is not a complete study of all the possibilities, instead of this it proposes some possible strategies and comparison of their use in different kinds of situations.

IPv6 benefits

1. The main reason for developing IPv6 is the exhausting IPv4 address space. That's why the addressing space is increased significantly with use of 128 bit addresses, instead of 32 bit addresses, used in IPv4. With this addressing scheme every internal network – enterprise or home will have more available addresses than the existing IPv4 Internet. There are different types of special-use IPv6 addresses, including multicast, link-local, etc., but most important is the global uncast address structure, because it will be used for access to the Internet resources. This structure is shown at figure 1. It consists of several fields: the first 23 bits represents the Registry, next 9 bits represent the ISP, and another 16 bits represent the site (organization).

Usually bigger organizations will have their 80 bits for network addressing, divided to 16 bits for subnetworks and 64 bits for the end systems.

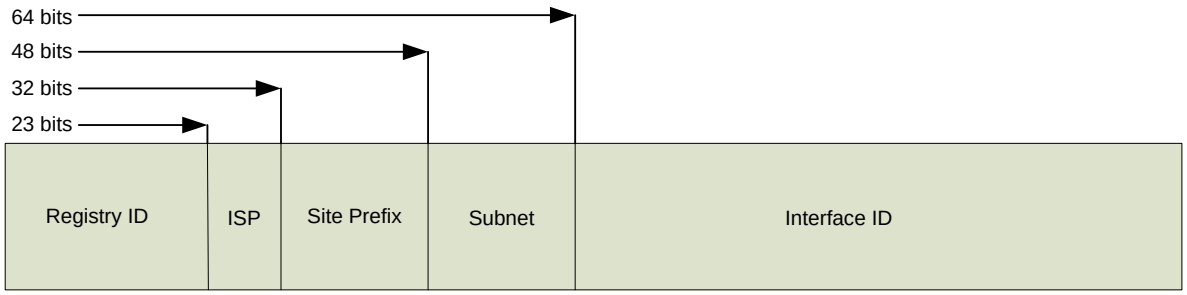

Figure 1. IPv6 global unicast address format.

2. Simplified header (1) – although source and destination addresses are four times longer than in the previous version, the header is only two times larger – 40 bytes, against 20 bytes in IPv4. There are only 8 fields in the IPv6 header, against 12 mandatory fields (and possible options) in the IPv4. Of course this means that some of the functions from IPv4 miss in IPv6. Headers comparison is shown at figure 2.

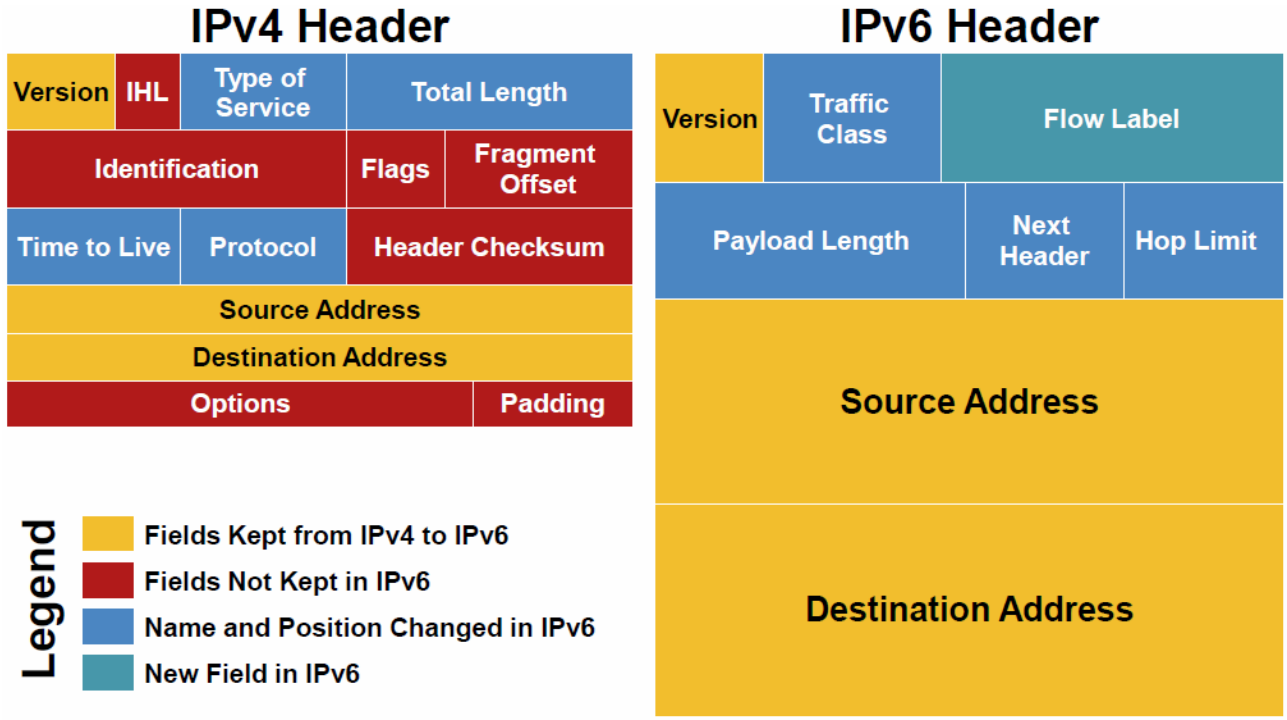

Figure 2. Headers comparison.(5)

There are no options in IPv6, that's why the header size is always the same, which means simplified buffering and processing. There is no checksum to calculate and rewrite at every router. Missing functions are implemented with additional headers.

3. Removal of broadcast transmissions – broadcast packets were one of most unnecessary traffic in IPv4 networks and in a larger network a special cares were taken for limiting unnecessary broadcasts. In IPv6 networks there is no broadcast transmission – in addition to unicasts and multicasts there are anycast packets, which will serve for service advertisement and discovery.

4. Enhanced mechanisms for automatic address configuration – except the well-known static and DHCP methods for IP address configuration, there are other possibilities for automatic address configuration, like EUI-64 for local network access and stateless autoconfiguration for Intranet/Internet access.

5. Built-in mechanisms for security – actually the widest used mechanisms for security in IPv4 – the IPSec protocol suite is originally invented and built in IPv6, and then ported for IPv4.

6. Built-in better quality of service mechanisms - the Flow Label and the Traffic Class fields in the IPv6 header may be used by a host to identify those packets for which it requests special handling by IPv6 routers, such as non-default quality of service or "real-time" service. This capability is important in order to support applications which require some degree of consistent throughput, delay, and/or jitter.

Co-existence mechanisms

1. One of the most widely described and expected to be mostly used method for co-existence is Dual-stacking. This mechanism supposes a router which supports IPv4 and IPv6 simultaneously and provides communication of IPv4 hosts to IPv4 hosts/networks only and for IPv6 hosts to IPv6 networks (4). An example of this topology is shown at figure 3.

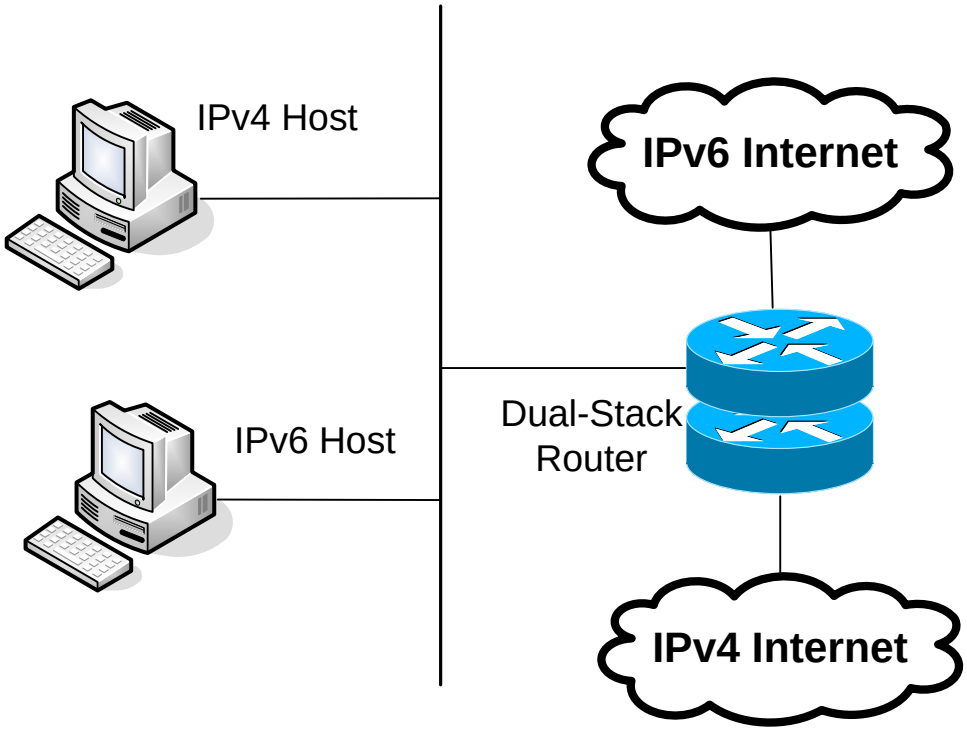

Figure 3. Dual-stacking.

Dual-stacking can be implemented not only in a router, but in an end system – client or server. An important fact is that dual-stacking can serve both protocols simultaneously, but it does not provide communication between IPv4 and IPv6 hosts and/or networks.

2. Another mechanism for providing co-existence is called tunneling. It is suitable when connecting two sites of a company using one protocol through a network or Internet using different protocol. An example of a connection between two IPv6 sites through an IPv4 Internet is shown at figure 4.

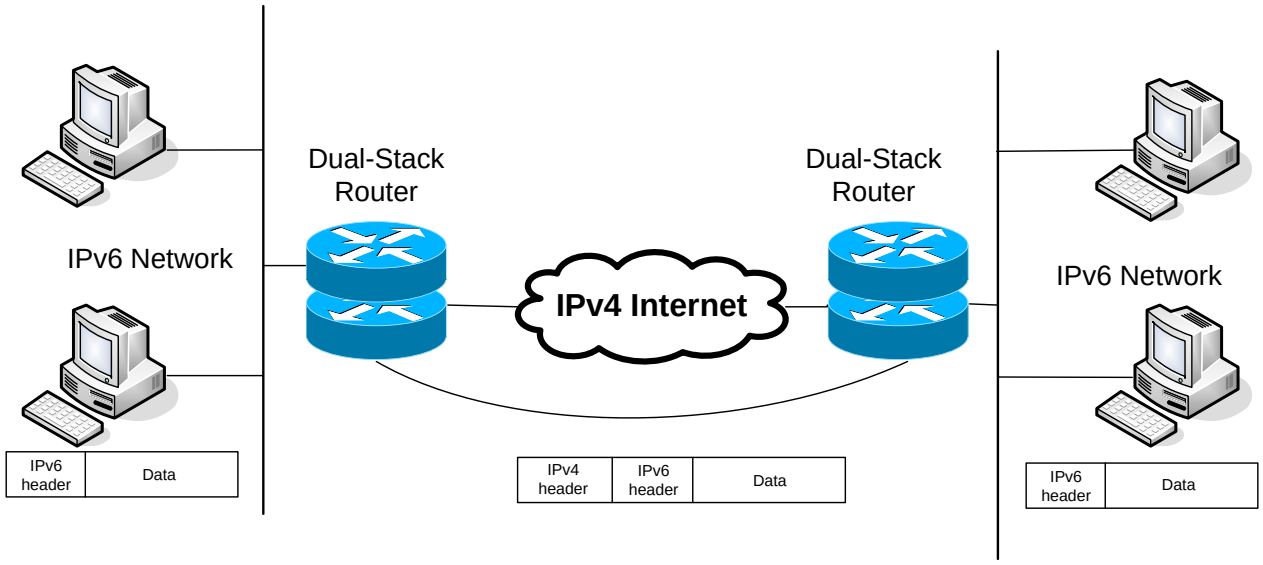

Figure 4. Tunneling.

Basically using this mechanism the packet from a network along with his header is encapsulated in other packet through adding another header for the protocol in the carrier network. When reaching the end of tunnel, receiving router strips the additional header and passes the original packet in the receiving network.

This strategy does not require different protocols in the endpoints and the carrier network, but this case is outside of the scope of this work.

The tunnel may be established between two routers, as shown on the figure, between host and a router or even between two hosts. There are different protocols for tunneling:

- static tunnel establishment – useful for all cases;
- ISATAP – a mechanism for automatic connection between dual-stack hosts in one IPv4 network/site (6);
- Teredo – provides address assignment and automatic tunneling between two dual-stack hosts in different IPv4 networks;
- 6to4 – automatic connection between host and remote IPv6 network or between two routers;
- Tunnel broker – a tunnel establishment mechanism, which uses an external host (broker) and Tunnel Setup Protocol (TSP)(3).

Every tunneling mechanism adds some extra information to the original header, thus may cause fragmentation issues and to produce poor connection performance or total lack of communication between both sides.

3. Translation mechanisms – the only option, when there are no dual-stack servers, clients or routers. It presumes some kind of change of the original information for making it understandable for the other system (5). An example for translation process is shown at figure 5.

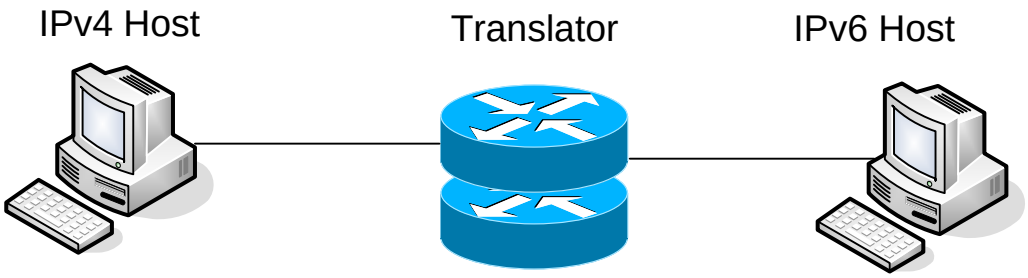

Figure 5. Translation.

There are few possible layers for translation:

- Network layer translation: Network Address Translation – Protocol Translation (NAT-PT). The translator rewrites the whole IP header and changes it according the format of the other protocol in both directions. This mechanism has been deprecated (1) but similar mechanisms are still being considered and developed, for example – NAT64.
- Transport layer: Transport Relay Translator (TRT). This mechanism is designed for use in IPv6 networks for connection to external IPv4 hosts. It relies on a DNS proxy service.
- Application layer: Application Layer Gateway (ALG). This mechanism uses an intermediate machine (proxy server) which gets the information from the IPv4 or IPv6 servers on Internet and provides it to the internal host. There are many already developed applications, like web-proxy, SMTP gateway, DNS resolver, SIP proxy, etc.

All the translation mechanisms have their drawbacks. If it is possible, they should be avoided.

Migration strategies

At first when decide to implement IPv6 protocol it must be clear whether we will create a pure IPv6 network, or will have a mixed IPv4 and IPv6 environment. It is important the size of the network and is it distributed along multiple sites, are all the sites using the same ISP, and is there IPv6 connection at all the sites.

There are too many scenarios and possible configurations. This paper will propose some guidelines for few typical companies.

1. Small office/Home office network with internal services and Internet connection.

This scenario requires migration only if the Internet Service Provider offers only IPv6 connectivity or requires connectivity to some site, which have only IPv6 address. Both reasons seem uncommon at present, but may become real in the future.

Best approach is full migration, simultaneously on every device in the network. Only if there is some device which cannot be migrated (e.g. embedded device, legacy software application and/or legacy operation system) must be implemented dual-stack on the computers that must access this device, or some kind of translation mechanism (less recommendable).

2. Single site large company with internal and external services and Internet connection.

The obvious difficulty in this case is the impossibility to migrate all the computers in a large site simultaneously, so the proposed scenario is to migrate the external services, to ensure dual-stacking compatibility for the internal servers, to migrate the internal resources until full migration, and then to remove the dual-stack support.

3. Single large office with internal and external services and small remote offices.

In this model most likely the internal and external services will be provided from servers in the central office. Also it seems impossible to migrate every remote office at the same time. That's why this model requires dual-stacking in the central office, until all the remote offices are migrated fully, or this can be accomplished with full migration of the central office and tunneling mechanism in the remote offices, until full migration.

Note that if some of the ISP's, servicing a remote office is not offering IPv6 connectivity, tunneling will be required for this remote office until migration of the ISP.

4. Large multi-site company with distributed internal and external services.

This case differs from the previous one in two main points. At first there are distributed resources (servers) at every site. At second every site will cave multiple computers, which means that host to host or host to router tunneling cannot be used, due to large number of tunnels needed. So the best approach seems to be first to enable dual-stacking on all the servers, then to migrate the central office, after that every remote site one by one, until full migration.

5. Internet Service Provider.

Because transition to IPv6 is not mandatory neither for customers, nor for Internet servers, transition in the ISP's must implement dual-stack technology in the

routers and in the servers. This must be required to support long enough, until IPv4 is depreciated (may take more than 10 – 20 years).

6. Any company with at least two simultaneous connections to different Internet Service Providers.

In this case the company must implement Multiprotocol BGP (MP-BGP4) at their border routers, connected to the ISP's. It is important to notice, that currently Internet consists of about 400000 routes. With IPv6 the address size is 4 times longer, so a border BGP router will need at least 5 times more memory to hold the full IPv4 and IPv6 tables.

Conclusions and future work

IPv6 is very close to the end customers and organizations. When it became reality, we must be prepared for it deployment without network service interruptions and miscommunications. This paper summarizes possible benefits and mechanisms for IPv6 deployment and gives some common scenarios for migration.

Future works includes detailed simulations and testing of all described and probably some new scenarios and development of a detailed guidelines for migration to the new Internet.

References

(1) Aoun, C., E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status, RFC 4966, IETF, July 2007
(2) Deering, S., R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, IETF, December 1998
(3) Durand, A., P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", RFC 3053, IETF, January 2001
(4) Gilligan, R., E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, IETF, August 2000
(5) Palúch, P., "IPv6 Technical Challenges", Academy Salute, April 2011, Bucharest
(6) Rooney, T., "IPv4-to-IPv6 Transition Strategies", BT Diamond IP, February 2007
(7) Templin, F., T. Gleeson, M. Talwar, D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 4214, IETF, October 2005

Acknowledgement

The work presented in this paper was supported within the project BG 051PO001-3.3.04/13 of the HR Development OP of the European Social Fund 2007-2013.