A STUDY OF THE TECHNOLOGY TRANSITION FROM IPv4 TO IPv6 FOR AN ISP

Daniel ENACHE, Marian ALEXANDRU
Transilvania University, Brașov, Romania

DOI: 10.19062/1842-9238.2016.14.1.17

Abstract: *The internet protocol IPv4 has met the demand for years, but the number of addresses, while vast, is finite. The solution to mitigate this problem was the development of the new IPv6 protocol, which extends the address space from 32-bits to 128-bits. IPv4 and IPv6 networks will interoperate during the transition period, although the two protocols structure is not compatible. This paper will shed the light on IPv4 and IPv6, look into the requirements of an ISP network and present three mechanisms that will make the transition from IPv4 to IPv6 smoother: Translation, Tunnel and Dual-Stack. Also, the implementation of Dual-Stack for an ISP and the obtained results are presented in this paper.*

Keywords: *IPv4, IPv6, ISP, Transition, Translation, Tunnel, Dual-Stack*

1. INTRODUCTION

The internet world has to go through a transition, but in this process both protocols, IPv4 and IPv6 (Internet Protocol version 6), have to connect to each other. IPv4 network has grown far more than anyone had ever imagined when the protocol was designed. As technology is developing new services and Internet-enabled devices use more mobile connectivity (2G, 3G and 4G), IPv4 is challenged with a series of problems, the most demanding one being address exhaustion. There are not enough IPs available from ISPs (Internet Service Provider) to meet the demand.

The new IPv6 protocol is needed to satisfy the needs and it features improved scalability and routing, simplified header that makes forwarding packets more efficient, end-to-end connectivity because there is no need for NAT (Network Address Translation), ease-of-configuration because it supports stateful and stateless auto-configuration, and information being stored in the start of the header is useful for a router thus resulting in higher performance routing.

The major flaw of IPv6 is that it is not compatible with IPv4, and to use the new protocol changes are required in software and every networked device. The majority of network services and applications still use IPv4, therefore it will not be replaced for a long time. So, the two network protocols will have to coexist. [1]

2. PROTOCOL SPECIFICATIONS AND THE TRANSITION MECHANISM

Addressing is a key function of network layer protocols that enables data communication between hosts, regardless of whether the hosts are on the same network or on different networks. Both IPv4 and IPv6 provide hierarchical addressing for packets that carry data. [2]

IPv6 provides for 340 undecillion addresses (the number 340, followed by 36 zeroes). However, IPv6 is much more than just larger addresses, it fixes the limitations of IPv4 and include additional enhancements. One example is Internet Control Message Protocol version 6 (ICMPv6), which includes address resolution and address auto-configuration not found in ICMP for IPv4 (ICMPv4). [3]

Mobility is another key feature of IPv6. This feature enables hosts (such as mobile phones) to roam around in different geographical area and remain connected with the same IP address. [4]

2.1 IPv4. Using the TCP/IP (Transmission Control Protocol/IP) model allowed IPv4 to become the core of the internet addressing as we know it today. In IPv4, addresses are 32-bit binary numbers and can cover 4.3 billion addresses. Some technologies have been employed to postpone the exhaustion of network numbers. The system in use today is referred to as classless addressing. The formal name is Classless Inter-Domain Routing (CIDR). However, this did not provide a long term solution and other technologies, such as NAT and DHCP (Dynamic Host Configuration Protocol) were introduced. IETF (Internet Engineering Task Force), in 1994, began its work for a successor to IPv4 which eventually became IPv6. [2]

1.2 IPv6 extends the address space from 32-bits of IPv4 to 128-bits and it supports CIDR as described above and many other features that make it an improvement over IPv4. Unfortunately, IPv6 is not backwards compatible which makes the transition more complicated. In the new IPv6 IPSec (Internet Protocol Security) was integrated, which was optional in IPv4. It is a set of Internet standards that uses cryptographic security services to provide confidentiality, authentication and data integrity. More features can be added to IPv6 due to its option field. Because of its large consumption of resources broadcast traffic is no longer available. Also, there are three modes of addressing for IPv6 packets: Unicast, Multicast and Anycast.[4]

1.3 Header differences. The innovation of IPv6 lies in its header. It is two times larger than IPv4 header and it is formed of a Fixed Header and zero or more Extensions (optional headers). All the essential information for a router is kept in the fixed header. The Extension contains optional information that helps routers to understand how to handle a packet. The IPv6 header has lost some fields that were used in the IPv4 header as you can see in Fig. 1, thus saving time processing the packets. IPv6 fixed header is 40 bytes long while IPv4 is 20 bytes. The version field represents the version of internet protocol (i.e. 0110 is version 4).

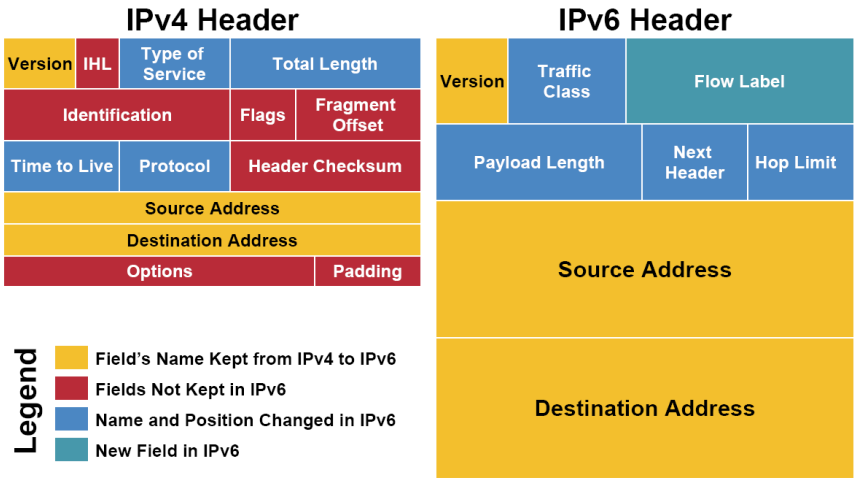

FIG. 1. IPv4 header and IPv6 header [5]

Traffic class is divided into two parts, the most significant 6 bits are used for Type of service and the least significant two bits are used for Explicit Congestion Notification (ECN). QoS (Quality of Service) management is provided by Flow Label field which is 20 bits. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. It is designed for streaming/real-time media. Payload Length is 16 bits long and is used to tell the router how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data.

The type of extension header used is detected by the Next Header field. TTL field in IPv4 header is now renamed to its exact meaning Hop Limit.

Source Address and Destination Address are both 128 bits and have the same use as in IPv4 header. [4]

2.4 Transition mechanisms. The transition from IPv4 to IPv6 is expected to take years, and in the meantime, both protocols will have to coexist and interoperate. For this to happen IETF has developed various tools that come to help the network administrator's transition to IPv6. There are three categories of migration techniques:

a) Dual Stack: Both IPv4 and IPv6 will run simultaneously on devices in the network, allowing them to coexist in the ISP network
b) Tunneling: An IPv6 packet is encapsulated in IPv4 packet and send over an IPv4 network.
c) Translation: A similar technique to NAT for IPv4 is used. Using NAT64 (Network Address Translation64), the IPv6 packet is translated to IPv4 packet.

End to end Dual Stack represents a major project for an ISP and it takes from 2 to 5 years to implement. The starting point of change is the core of the network, which is easy for most network operators, meaning a few months of work. The real problems start in the edge and access distribution layers, mostly because of the legacy equipment that does not support IPv6. Changing CPEs (Customer-premises Equipment) will most likely take years and IPv6 is needed in the meantime. As represented in Fig. 2 a server in dual configuration (IPv4 and IPv6 address) can communicate with other hosts through a dual stack router.

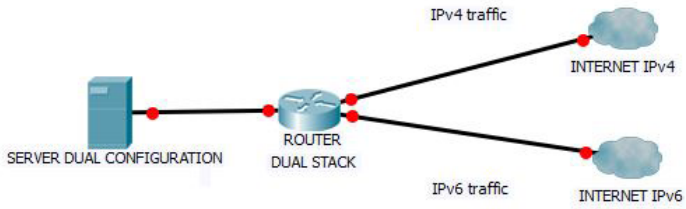

FIG. 2. Dual stack

The advantage of dual-stack is that it makes available to use devices that support only one IP protocol or both, allowing older network services to still be used. On the other hand, the costs for implementation are very high and very few organizations can change from IPv4 to IPv6.

Tunneling allows the use of IPv4 networks to carry IPv6 traffic and its basic principle of is shown in Fig. 3. This can be done either in a manual or in an automatic way. The manual configuration requires definite specification of the IPv4/IPv6 source and the tunnel IPv4/IPv6 destination. When the number of tunnels grows, administrating this technique becomes a major drawback.

FIG. 3. Tunneling

For the automatic configuration, the final destination address of the IPv4/Iv6 packets is determined using an IPv4-compatible address of the IPv6 packet, which is usually the IPv4 address prefixed with 96 bits of 0s [6]. The main advantage of using the tunneling technique is that it uses the existing infrastructure of the ISPs and it meets their standards in terms of administration and costs.

Translation is used to achieve direct communication between IPv4 and IPv6. The new protocol supports translation from IPv4 header to IPv6 format. As illustrated in Fig. 4, when an IPv4 host tries to communicate with an IPv6 server, a NAT-PT (NAT – Protocol Translation) enabled device removes the IPv4 header of the packet, adds an IPv6 header and then sends it through to the server.

When the reply comes it does the other way around.

The algorithm for all translation methods is known as Stateless IP/ICMP Translator (SIIT). For an ISP, translation is not seen as a viable solution because of NAT use with IPv4.

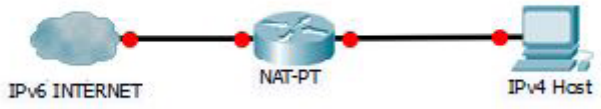

FIG. 4. NAT-PT Translation

3. IMPLEMENTATION AND ANALYSIS

For our dual-stack implementation we used the network diagram in Fig. 5. It represents real equipment from an ISP's GPON (Gigabit Passive Optical Network) based infrastructure. The end user is connected to the network through the F668 ONT (Optical Network Terminal), which supports the dual stack configuration. For IPv6 we practiced on the subnet 2a02:2f0f:5c::/48, which we divided in four /50 subnets. The subnet on our VLAN (Virtual Local Area Network) was 2a02:2f0f:5c::/50, while our IPv4 subnet was 89.33.4.0/25. Also, for the IPv6 implementation, DNS6 was provided by the higher tier ISP connection. More on the configuration of our network card can be seen in Fig. 6.

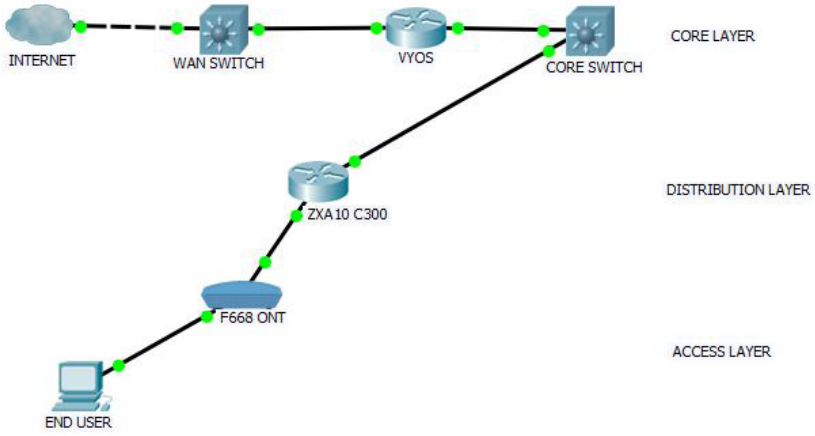

FIG. 5. Dual-Stack Network Topology

The VYOS internal router provides software-based network routing and was configured with BGP (Border Gateway Protocol) routing protocol.

Customers are aggregated by ZXA10 C300, which is an OLT (Optical Line Terminal). In our configuration we used the carrier's OLT and ONT just for transport purposes. The default gateway was directly the VYOS router, which had dual-stack configuration, and as it can be seen in the Fig. 6, we had both IPv4 and IPv6 gateways on the end device.

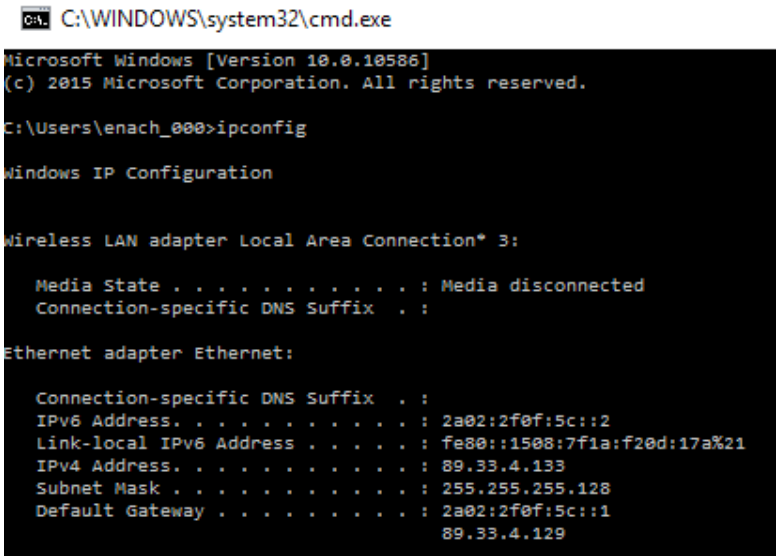

Fig 6. End User network card

Firstly, IPv6 connectivity was tested and for that purpose, we used Wireshark for network packets capture while we initiated ping to Google IPv6 public DNS server, as shown in Fig. 7.

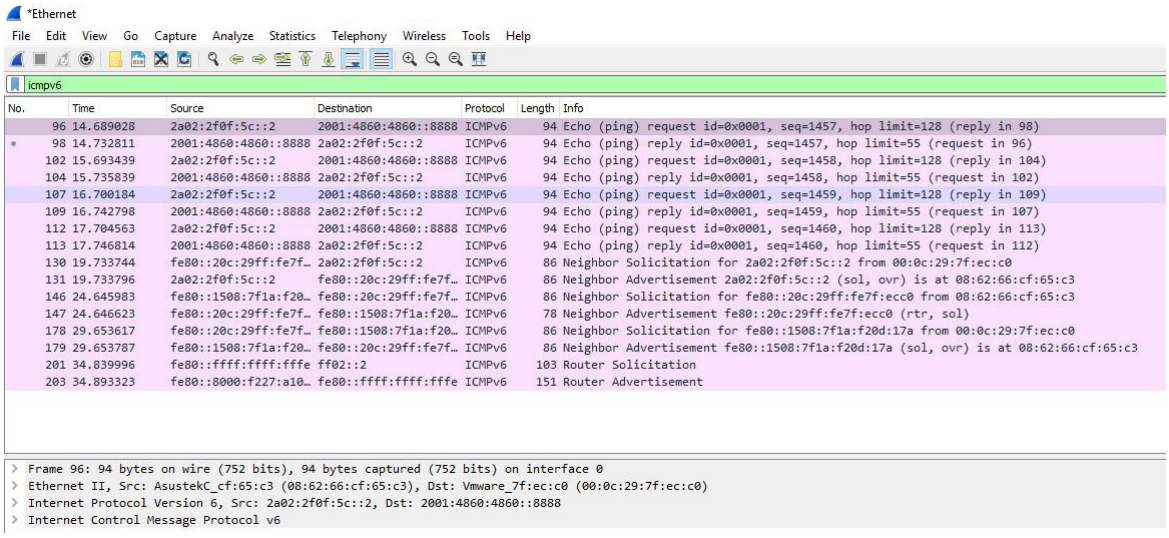

FIG. 7. Wireshark IPv6 ping capture

Afterwards consecutive pings to Google and another site which does not have IPv6 connectivity were sent to test out our dual-stack configuration. The result is illustrated in Fig. 8, where highlighted in blue are the DNS enquires and responses from the servers and on pink background the actual ping requests and reply from IPv4 site and Google for IPv6. In the info tab for DNS lookup we can see the queries of type A for IPv4 and type AAAA for IPv6, which return the IP address of the site.

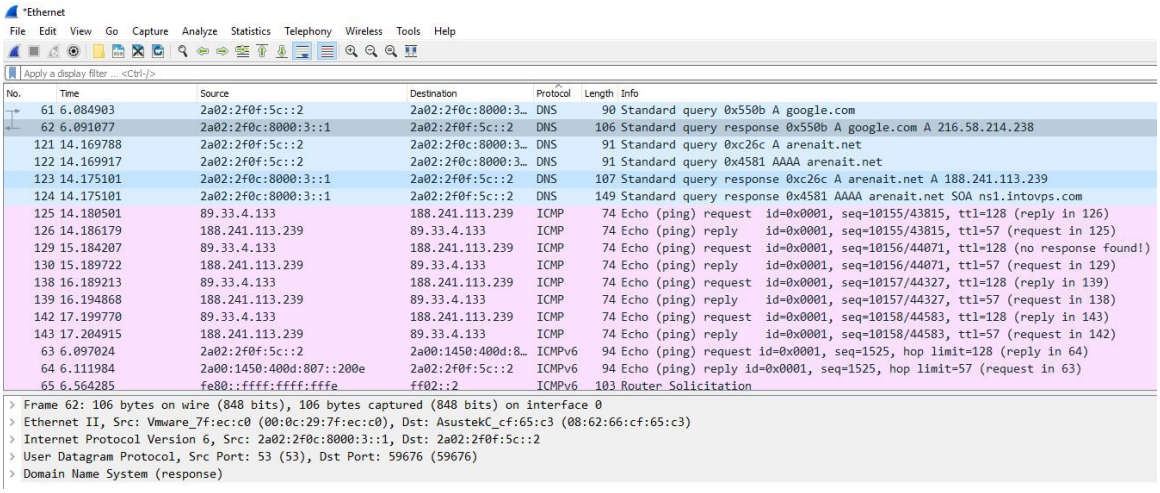

FIG. 8. Wireshark IPv4 and IPv6 ping capture

Source and destination address in Wireshark show end-to-end connectivity for both IPv4 and IPv6. As shown in the above figure we established both IPv4 and IPv6 connection using dual stack configuration on our end device and on real, ISP grade, equipment.

CONCLUSIONS

With IPv4 resources depleted, ISPs must enter the IPv6 era. Countries such as China and India are already moving forward, changing their infrastructure to support the new IP protocol. This fact determined ISPs from around the world to make the first steps towards the feature-rich IPv6, but there is still a long way to go. Given the transition mechanisms we overlooked in this study, dual stack is the viable solution for an ISP to migrate gradually to IPv6. It offers the possibility for hosts to reach content in both networks because of its ability to run the two protocols at the same time. Tunneling is not the way to go for an ISP because the protocol overhead increases the latency in the network.

Another drawback would be the administration of so many tunnels in an, already congested, service provider network. In this paper we created a sample of an ISP's network for the purpose of experimenting with IPv6 features and better understanding the steps of the migration, along with its transition mechanisms. We were able to test and debug on live equipment which gave us a better view of a real implementation when the time comes.

REFERENCES

[1] P. Wu, Y. Cui, J. Wu, J. Liu, C. Metz, *Transition from IPv4 to IPv6: A State-of-the-Art Survey,* IEEE Communications Surveys & Tutorials, Vol. 15, no. 3, pp 1407 – 1424, 2012;
[2] ***, *Cisco Certified Network Associate Routing & Switching Introduction to Networks*, Chapter 8: IP addressing, 8.0.1.1 Introduction;
[3] ***, *Cisco Certified Network Associate Routing & Switching Introduction to Networks*, Chapter 8: IP addressing, 8.2.1.1 The Need for IPv6;
[4] http://www.tutorialspoint.com/ipv6/ipv6_tutorial.pdf
[5] https://343networks.files.wordpress.com/2010/06/ipv4-ipv6-header.gif
[6] J. Hatcher, *Strategies for migrating from IPv4 to IPv6,* 2012
Available: http://datacentremanagement.com/news/view/strategies-for-migrating-from-ipv4-to-ipv6