ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

THE IPV6 RESISTANCE - A SURVEY

RESHMI TR[1]*, ANUSHA K[1], SUMATHI V[2], PANDIYARAJAN K[3]

[1] School of Computing Science and Engineering, VIT University, Chennai, Tamil Nadu, India. [2]School of Electrical Engineering, VIT University, Chennai, Tamil Nadu, India, [3]Paypal India Pvt Ltd, Chennai Email: reshmi.tr@vit.ac.in

Received: 22 November 2016, Revised and Accepted: 29 March 2017

ABSTRACT

Internet Protocol Version 6 (IPv6) was developed in 1990 to overcome the shortage of IPv4 addresses. The world saw IPv6 as the next generation IP addressing and an innovative backbone for the Internet. Although more than 25 years have passed since the development of IPv6, still IPv6 is seen as new technology without drastic enhancements and has not been widely adopted. Even information technology giants fear the network transition to IPv6 backbone. This article analyses the reason for this resistance toward IPv6. A detailed study of the same has been conducted and is discussed in the paper. The discussion includes the myths and facts that have resulted to the IPv6 resistance and outlines the resolutions for IPv6 transitions.

Keywords: IPv6, Internet Protocols, Next Generation Networks.

© 2017 The Authors. Published by Innovare Academic Sciences Pvt Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4. 0/) DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19747

INTRODUCTION

Internet protocol (IP) is a set of technical rules to define how the computers communication happens over a network. There are two versions of IP, namely, IP Version 4 (IPv4) and IPv6. IPv4 is the first version of IP which is widely used, and the same accounts for most of today's internet traffic. There are about 4 billion of IPv4 addresses which are insufficient to distribute to the internet users and hence IPv6 was planned and developed. IPv6 is a new numbering system to provide a larger address pool of 2128 addresses.

To maintain the internet live for the growing internet users and to provide IP addresses for the devices, the IPv6 was proposed. According to the survey conducted by SixXS, Germany has the highest number of IPv6 peer connections (47) followed by Netherlands (39), United States (25), Switzerland and United Kingdom (17). All other countries had <10 IPv6 peers. Hence, although the IPv6 advantageous are widely discussed, the survey shows that organizations hesitate to migrate from IPv4 to IPv6.

The IP uses the datagram service to transfer data packets between the end systems. For the data communications, the IPv4 packets have the header of 20 bytes and IPv6 packets have header of 40 bytes included with the payload. The header structure of both the versions of IP is shown in Figure 1.

In IPv6 header, the fields except flow label are the same as in IPv4 but the name differs. There is an optional extension header (EH) used in IPv6 which provides more functionality compared to IPv4.

The various header fields in IPv6 are listed below:

- Ver - Version is a 4-bit number to specify the version of the IP
- Traffic class - The 8-bit mention the type of traffic and works as the same field the type of service in IPv4
- Flow label - A 20-bit field that specifies the flow type and hence the encapsulated packets are never opened by the router
- Payload length - The 16-bit integer shows the packet size of the continuing packet that follows the IPv6 header
- Next header - An 8-bit field, that. Identifies the type of header following the IPv6 header. The typical values for the next header for IPv4 and 6 are assigned by IANA
- Hop limit - An 8-bit integer is decremented by one in each node that forward the packet. At any point, if hop limit is decremented to zero the packet is discarded
- Source address - A 128 bit address field which shows the address of sender
- Destination address - A 128 bit field that shows the address of the recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is used.

The EH of IPv6 gives more information of network to the routers. The included EH in packets deteriorates the performance of the network because of added bits. So generally, the basic formats of headers are mostly used and encouraged. As per RFC 2460, there are some basic rules for the order of EH like:

i. Hop-by-hop options header
ii. Destination option header (for intermediate destinations when the routing header is present)
iii. Routing header
iv. Fragment header
v. Authentication header (AH)
vi. Encapsulating security payload header (ESP)
vii. Destination options header (for the final destination).

The security features in IPv6 are enabled using the fields in the EH. Hence, there is no need to incorporate extra security features like IP Security (IPSec)/IKE in IPv6. They are already in-build in IP Version 6 and they just need to be enabled before using it. During the proposal for IP next generation also called IPv6, it was believed to have many advantageous over IPv4. The main advantages are listed below:

- The address space is four times larger than IPv4
- It provides better network management and routing efficiency because of larger subnet space, and it can provide an efficient hierarchical route aggregation
- More encryption and authentication options can be provided with IPv6
- The IPv6 application has a plug-and-play option which can make network implementation easy
- The overall packet processing will be more efficient when compared to IPv4
- The significant advantage stated was the multicasting. It stated no organization needs a globally routable multicast group assignment
- It stated there is resource allocation support using the flow label in header format
- It stated that it has options to support mobile networks.

MYTHS: HOW FAR ARE THEY TRUE?

Today people have started asking "How IPv6" rather than "Why IPv6," but there are still some barriers which resist adoption of IPv6. A few myths are deeply rooted and it requires a thorough knowledge and practice to change over. The assumptions [5-6] are as follows.

IPv6 is just expenditure

Organizations without proper technical relevance are more concerned about the cost of deploying IPv6. It is believed that IPv4 still has large address space and by using network address translation (NAT), the IP address requirement can be resolved. The Internet society survey [6] states that IPv4 addresses are running out and there are issues caused by IPv4 NAT in global internetworking.

It is believed that IPv6 is much more complicated than IPv4

The IPv6 is far more similar to IPv4. Hence, the technical training given to the technical staff will not be substantiated by educating IPv6. The protocols such as domain name system (DNS) and Internet Control message protocol have been enhanced in IPv6, but the working of the protocols are very similar to IPv4. For example, the AAAA records of DNS in IPv6 works closely resembles the A records in IPv4. There are no complications involved in configuring and mapping the DNS records. The autoconfiguration and multicasting feature often makes IPv6 implementation much easier than IPv4.

It is believed that IPv6 deployment in an organization cannot assure redundancy, reliability, and availability to the service applications

In early 2000's, there were some allocation policies for IPv6 that states the upstream and downstream network traffic can only be through same service providers. It was believed that it can avoid the overloading in global routing table. Hence, the redundant connections were also streamlined through the same provider's stream which was taking the earlier traffic. So whenever a provider's stream goes down, it looks like IPv6 is not providing redundancy and availability. But later on in the year 2007, these allocation policies were changed and IPv6 started working with different service providers for upstream and downstream traffics.

It is believed that IPSec architecture is difficult in IPv6

IPSec works well in IPv6 due to the unavailability of NAT in IPv6 connections. There is no enhancement required for the implementation of IPSec in IPv6. The IPSec is an enhanced or optional security schema in IPv4. However, IPSec is an in-build security scheme in IPv6 using AH and ESP header fields in EH.

These are the Myths which were resulted from the inadequate knowledge of IPv6. However, there are some real facts which still acts as a barrier for the complete translation of IPv4-IPv6.

REAL FACTS AND SOLUTIONS

According to the survey conducted by Computing Technology Industry Association only 23% of the enterprises have started deploying IPv6 and most of the companies are not ready for the IPv6 migration. Some of the reasonable facts are listed below:

The top level domains still do not support IPv6

Even when end users have devices compatible with IPv6, some top domains do not support IPv6, so the users are forced to use IPv4.

The IPv6 experimental build downloads sounds dangerous

The experimental builds are generally given to enhance the usage of IPv6. These are modified source codes for the same applications. As these codes are modified and rewritten, it sounds dangerous for the end users.

Incapability for roll-back

The IPv6 when deployed completely cannot be rolled back for backward compatibility.

Introduction of non-compatible network appliances: Even certain top network vendors do not provide network appliances with IPv6 support.

Fear of commercial loss among domains

The top domains which are running in IPv6 backbones cannot serve the IPv4 request directly, so the drop in service requests increases and can result in huge commercial loss for organizations.

Service provider's incompatibility

The top ISPs and telecommunication providers still use the IPv4 backbone for cost saving and hence the end users find IPv6 not reachable.

Confusion about transition tools

Network operators and administrators choose to experiment with a few transition techniques and are still confused about what to choose.

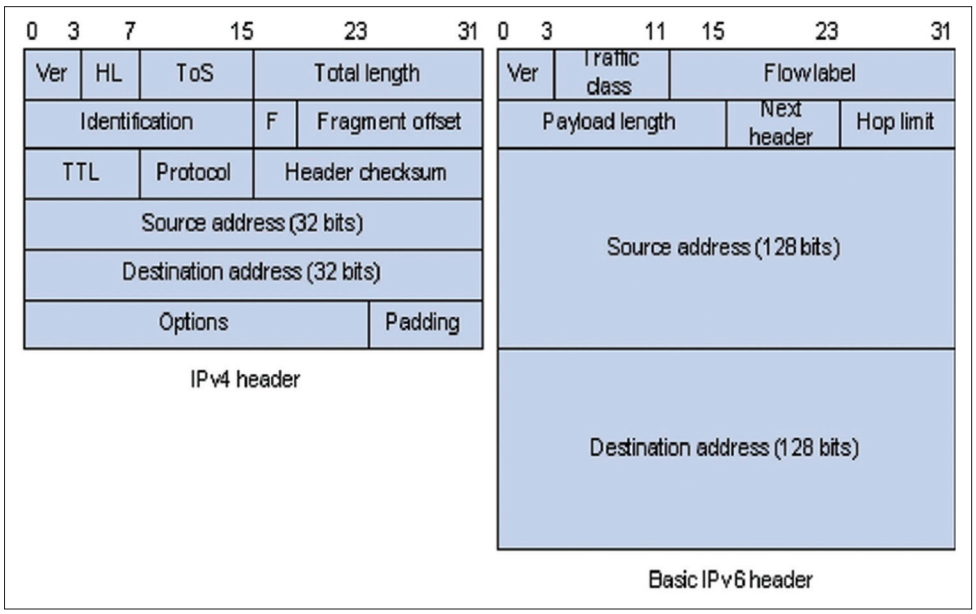

Fig. 1: IPv4 and IPv6 Headers

The IETF V6OPS workgroup is working toward providing guidance in the choice of these techniques [7] for different usage scenarios.

Unwanted publicity for transition tools
There are many IPv6 transition tools which advertise the smoother transition. The unnecessary publicity and technical jargons make the IP transition technology look complex.

Unavailability of services during transition
The shutdown duration for the deployment is another reason for the IPv6 resistance.

The reasons for the IPv6 resistance were discussed above. In spite of all the facts, there is immense need for the deployment of IPv6 due to the shortage of IPv4 addresses [8]. Only with IPv6, the innovative Internet of things can be made accessible for everyone. As a first step toward the transition, all the network equipment in the market should be IPv6 compatible. There should be a planned and simultaneous enhancement of user and provider environment to support IPv6. All the organizations are more concerned about the security of IPv6 traffic, as most of the security devices are not equipped to detect the attacks in IPv6 traffic. So if security devices which are specially meant for IPv6 are introduced, they can come out of the security fear.

Now IPv6 traffic is given the same priority like IPv4 so if there is some prioritization for IPv6 traffic in Internet; this will boost the usage of IPv6 among Commercial organizations who do prefer their traffic to be routed easily for processing. The big concern about IPv6 deployments is the unavailability of the roll-back to backward compatible technology. So if there can be any intermediate roll back technology which works well in both versions, there will encourage the organization for a switch-over.

There are many transition tools introduced for the migration to IPv6 [10], they all seem to be much technically assisted and complex. The transition is not transparent to the users. So if a user-friendly transition technology is introduced, it can be easily deployed for the usage of IPv6. There are no rules for the usage of IPv4 addresses among organizations. They just pay to the Internet Service Providers and get the IP addresses. At some point of time, all the IPv4 addresses will be exhausted and it will lead to a situation like the more the pay then the more will be the addresses provided. So to avoid this, Government should imply rules to ISPs to provide infrastructure that support IPv6 and also to limit the distribution of IPv4 addresses. All the changes cannot be happen in a day, but step by step awareness about IPv6 will make the IPv6 transition easier. Organizations should provide training to their technical resource people in IPv6 deployment and management. Even common man should be educated or made aware of the need for IPv6.

CONCLUSIONS

The reasons for the IPv6 resistances are discussed in the paper. Even though there are many myths which prevent the deployment of IPv6, there are many facts that need to be considered while deploying IPv6 in an organization. Based on the reports on allocation policies, there were changes made in the allocation stream policy of IPv6 in 2007. Likewise, the technical reporting and enhancement can make IPv6 more acceptable to the users. With the growing needs of the users and the number of devices in the Internet, IPv4 addresses are insufficient. However, IPv6 deployment is not an option but a necessity for the growing Internet.

REFERENCES

1. Kent S, Atkinson R. IP Authentication Header. RFC 2402, November; 1998.
2. Kent S, Atkinson R. IP Encapsulating Security Protocol (ESP). RFC 2406, November; 1998.
3. Hinden R, Deering S. IP Version 6 Addressing Architecture. RFC 3513, April; 2003.
4. Hinden R, Deering S. IP Version 6 (IPv6) Specification. RFC 2460, December; 1998.
5. Huston G. The myth of IPv6. Internet Protoc J 2003;6(2):23-29.
6. Huston G. IPv4: How long do we have? Internet Protoc J 2003;6(4):2-15.
7. Huston G. Transitional myths. Internet Protoc J 2011;14(1):14-21.
8. Davies J. Understanding Ipv6. Microsoft Second edition. WA, USA: Microsoft Press Redmond; 2008.
9. Myths Surrounding IPv6. Available from: http://www.ipv6now.com.au.
10. IPv6 Industry Survey Report. Available from: http://www.progreso.com.sg/training/files/IPv6-Survey-Report-2015.pdf.