

## **IPv6 Issues and Benefits**

Dr. Yves Delphin  
Pace University  
10 Fox Run, Woodridge, NY 12789  
Email: ydelphin@pace.edu

### **ABSTRACT**

It has been almost 10 years since IPv6 was supposed to become the de facto Internet of the world. Indifference and incomprehension have prevailed. Many universities, organizations have not reached this goal yet. It is everybody's hope and wish that soon, this will happen. The benefits that it has created and will keep bringing upon the whole world are numerous. Among those, the whole advent and evolution of Internet of Things (IoT) the Web of Things (WoT) and closer to us the advent of the 5G that organization is fighting for would not be

For a long time, the protocol to access internet in the world has been thru IPv4. It still remains IPv4 even though great effort has been made to change the course of this.

possible without IPv6. Security has become tighter and more and more people are embracing the protocol. At the end of Obama administration every organization in the US should have been using it. Unfortunately this did not happen. We believe that now the time is right for IPv6 to come on board now.

### **Keywords**

IoT ( internet of everything), WoT( Web of Everything), 5G ( fifth generation), IPV4 ( internet protocl version 4, IPV6 (internet protocol version 6)

The catalyst for this change revolves around the introduction of China and India into the scene. With more than 2 billion people accessing the internet the consortium of

Internet has found it more and more difficult to keep up with the number of people involved in the concert of media. Just like the telephone gurus has changed its course by creating more number for the users, the Internet Engineering Task Force (IETF) finds itself in a difficult situation to allocate an address for each user. Although the day for the inauguration of IPv6 has come and gone, most companies find it difficult to keep pace with the gadgets using IPv6

emerging and taking place. Only the mighty few including Google, Microsoft, Cisco have been able to take advantage of the new IPv6 structure and go ahead with it. If IPv6 is the de facto standard for the new generation of computers, why are only a few companies taking full advantage of it? The answers probably lie between the issues, the implication and the benefits that IPv6 propose to establish to dismantle the reign of IPv6.

## **ISSUES WITH IPv6**

As Mr. Warfield explains it in his article “Security Implication of IPv6”, IPv6 is supposed to be the “next generation” Internet Protocol and is the designed successor of IPv4 [18]. IPv6 is available for anybody who is already using IPv4. Because of insufficient number of addresses that meet the future need of people, IPv6 comes into play. It is no longer experimental as it has been for the last several years [18]. Essentially because IPv4 limits to “future growth” constraint of 32 bit address field, technique like the Network Address Translation, IPv6 came to the scene with its overabundance of 128 bits address fields that can provide up to  $6.5 \times 10^{23}$  addresses for every square meter of the Earth surface [4].

Some of the problems that IPv6 presents come directly from IPv4 itself. That includes the renumbering of IPv4 networks which is addressed through transition mechanisms and auto configuration methods

that allow dynamic renumbering, multiple addresses and transition periods which ease the transition between the addresses prefixes [18]. Because of this inheritance, the shortcomings presented are addressed and many security enhance features will be present in IPv6. The author emphasizes that IPsec was “back ported into IPv4”. The huge amount of addresses space will “create a barrier to comprehensive vulnerability scanning”. [18]

Many intruders will evade detecting by security scanning and IDS detection through communication tunnels. [15] Trojans horse program as well as assorted malicious codes can easily evade most IPv6 unaware security and vulnerability scanning programs because the IDS must go penetrate deeper into the packet to analyze the traffic. Because of the Neighbor discovery Protocol (NDP) the hosts which are compromised will advertise the routes and forward IPv6

traffic back thru themselves for the entire network behind the firewalls. [18]

Another issue represents the mapping of the External Unique Identifier (EUI). With the auto configuration which is native to IPv6 only, mapping can be done that would reveal the network infrastructure or the connectivity through EUI mapping. The router and the serial connectivity linkage could be revealed also because the PPP end points often inherits from the system network interface. [18] Therefore, an attacker can find potentially the make and the model of a remote machine and use the information to target attacks. This is where the cryptographic algorithm comes into play to mitigate the risk by using non-predictable addresses or assigning the address by using DHCPv6. [8]

Unless certain steps are taken to mitigate the risk of attack such as to disable any IPv6 equipment, to detect and block IPv6 tunnel traffic at the network perimeter and to

include IPv6 usage policies in the organization security plan, the attacker will have an easier time since a host that has global IPv6 addresses will provide an environment that will facilitate an attack at the network level. [8]

Other issues such the Neighbor Discovery (ND) and the Stateless Address auto configuration will eventually cause IP packets to flow to unexpected states, causing denial of services. Neighbor Discovery (ND) is simply a replacement for ARP, and stateless auto-configuration which allows an IPv6 host to be configured automatically when connected to an IPv6 network. Because of the neighbor discovery, packets which are destined for a certain node can be intercepted and modified by a different node. This is being mitigated by the IPsec, AH and RFC 3756 ("RFC 3756," 2004) to secure corporate intranets, public wireless access networks and pure ad hoc network. [8]

To understand better the problems created by the introduction of IPv6 as a replacement for IPv4, it is paramount to compare both protocols and study the fundamental difference between both. Although this is not an excuse to absolve IPv4 problem, it is nevertheless an explanation to see where

### **METHODS OF CONNECTIVITY**

There exists some work around solution to connect Ipv4 to Ipv6. ISATAP, Teredo and 6to4 are tunneling solutions that will enable IPv4 hosts to connect to Ipv6 networks when the native support does not exist. [3] A description of each of them will clarify our point.

A 6to4 tunnel is a router used to generate a link from an inside IPv6 network to the rest of IPv6 world over the internet. The router will take the IPv4 address and calculate the IPv6 network prefix, by combining the 6to4 2002::/16 prefix with a 32 – bit IPv4 address of the internet –facing interface to form a /48 prefix for the IPv6 network.

IPv6 is going and the different problems, and issues it presents to the academia and the industry. We should look at the methods of connectivity, the usage statistics and the internal features of IPv6.

Generally, this technique will generate IPv6 addresses by using IPv4 addresses and will connect the IPv6 networks over 6to4 routers which will facilitate the operation.

[7]

ISATAP is an acronym for Intra-site Automatic Tunnel Addressing. It is a tunneling technique for dual stacks. It shows a remote access use case for IPv4 hosts where the IPv6 packages are encapsulated into IPv4 packets and transmitted over IPv4 networks. [3] Teredo, another transition technology which enables IPv6 capable host which do not have native IPv6 connectivity. Compared with the other technique, Teredo has the ability to perform

even behind the NAT environments. Because IPv6 is becoming more and more widespread, Microsoft which is behind the

### IPv4 AND IPv6 USAGE STATISTICS

According to Google, 7.08 % of its users access Google service via IPv6 and 7.08 %

invention of this technique has shut down this solution. [16]

of all websites support IPv6 connection. Here is an example of statistics taken as of August 21, 2015.

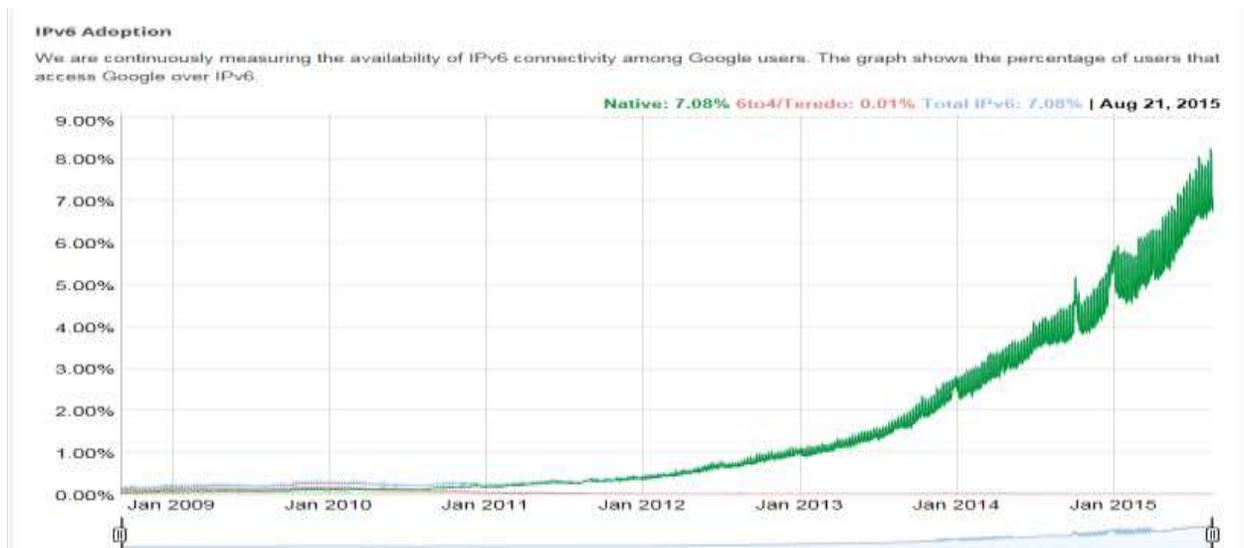


Fig. 1. IPv6 Connectivity of Google Users [3]

Looking at some of the measurements activities of activities on the global internet ("") we can see that many companies across the globe show an active presence in IPv6. Because Ipv6 is not fully adopted, the proposition is to establish a seamless transition from IPv4. To do so, tools have been implemented to fit in one of these three

categories: *tunneling* where the ipv6 packets are tunneled through an IPv4 network; *dual stack* where hosts and routers run both an IPv4 and IPv6 protocol stack; *translation* where a gateway translates IPv4. According to Carol [10] over half of the traffic in 2018 originated with non PC devices

“For example: think of monitoring the thermostat at your house during the winter so that the

temperature will automatically be set 5 degrees higher at 5:00 pm every day. By the time you get

home the house is nice and toasty! Think of a patient in a hospital whose monitoring equipment

## **BENEFITS AND IMPORTANCE OF IPv6 OVER IPv4**

There is a need for the creation of this new protocol of the Internet. The limits of IPv4 made it possible to appear on the scene. The insufficiency of IP address space, as well as the address prefix allocation and data security constitute the main reasons that propel IPv6 ahead, just like the creation of new exchange in the phone systems did for the appearance of new phone numbers. So, the benefits of IPv6 will result in a huge number of IP addresses, end to end connectivity and built-in security. [14]

will automatically notify a nurse that his or her heart rate has increased above a certain threshold.

This is the future of the Internet. Without thinking about it for very long, most people can think of

an example of M2M communication that in some way touches their lives. [10]

Many steps must be taken when a company wants to migrate from IPv4 to IPv6.

This might explain why it has been taken such a long time for many companies to follow thru.

The article in Fortinet entitled “A practical guide for beginning the Migration

IPv6 “explained the different steps needed to do so. Among them we should include the desire

to shelter IPv6 from the threats that have plagued its predecessor. Security in both protocols

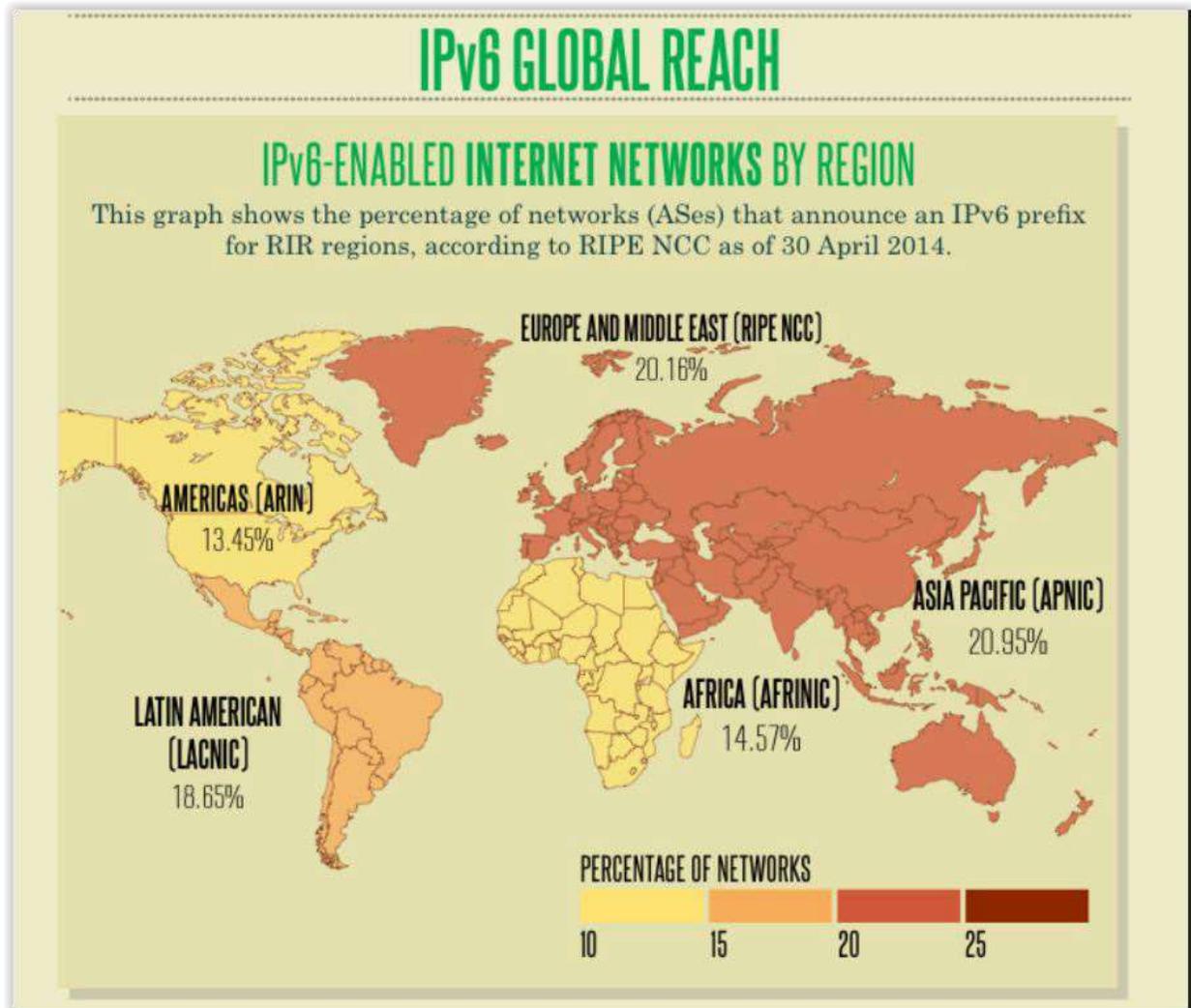
will occur gradually. [5]

We must also examine the robustness of the

IPv6 solution and the budget allocated for

that. It is no wonder that websites started to support it on June 6, 2012.

The following shows who in the world is using this protocol now:



Since the Internet is growing exponentially, a new conception has originated

Table data 8  
In the presence of what is usually called Internet of Everything (IoT)

In an article entitled “The Internet of Everything through IPv6”, Antonio Jara, Latif Ladid and Antonio Skarmeta explained that this concept is the result of the new Internet Protocol. [1]

As far as they are concerned, IPv6 offers a challenge in connectivity, reliability and mobility [1]

Application in the public sector revolves around security. Examples of vulnerabilities can affect patient health and privacy. An example would be a Denial of Service incident which could stop the monitoring of a patient critical vital sign. Another one would be the replay of an impersonation that could replay false information from a patient, informing that the patient is not in danger when in fact he/she really is. “We definitely need a security mechanism to prevent such an

attack and also decrease such an attack in the healthcare market” [1]

MIPv6 is the protocol that support IPsec in IPv6. It is used support Mobility between the mobile node and the home agent. It uses two addresses: the initial addresses of the device called the Home address and the new address in the network that is visited. This is called the care of address as the Locator. [1]

So it is a noticeable fact that IPv6 provides connectivity and reliability of equipment, guaranties security and privacy and integrity of information and user confidentiality and support the mobility since the future of the Internet present a more ubiquity and mobile internet. Anthony Skarmeta and Jara and Latif explain it well when they wrote:” Its advantages is not only limited to a universal addressing space, but also offer a stable, scalable and extensive and tested protocol for global end-to-end communication, device/service discovery,

end to send security, multicast addressing , stateless addressing and auto configuration”.

[1]

Many key challenges still exist with the introduction of IPv6. Mobility is the crucial challenge. The two fundamental phases are the movement detection “when the device is changing location and the signaling and control messages required to be aware of the changing location. To the networks and clients relative to the device in movement”. This mobility factor is based on IPv6 approach and the current internet architecture and ultimately on what is called a clean-slate trend new concept of ID/Locator split architecture which uses two values, one for the identification (ID) and the other for the location (Locator). [1]

The next step of IoT will be to connect things to the Web, thereby having the so

called Web of things which allow things and systems to interact together. IoT will be for communication, integration and interoperability. The challenge of the Web of Thing will be to build a Semantic Web of Thing (SWoT) for resources to cooperate, share, link, combine and build complex services with higher intelligence and context awareness. On a larger scale , these” challenges “can be addressed only in ideal ecosystem , since several products will develop unique features that will be out of the scope of the existing standards and each manufacturer is associated with a different standard organization”. [1] The European standard which called for an M2M (machine to machine) initiative will look into the convergence of emerging standard of the capillary and cellular networks towards an interoperable IoT ecosystem. [6]

## CONCLUSION

IPv6 benefits are countless. The major challenge we should look forward this new protocol will be security training and education, support from ISP and vendors, the congruence of the security policies in IPv4 and IPv6. There will be new vulnerabilities that we did not have to consider in the IPv4 environment. It is a new thing and the explosion of new gadgets relying on IPv6 protocol is only the tip of the iceberg that will be revealed. On

the other hand, we will have more efficient routing, more efficient packet processing, direct data flow, simplified network configuration, support for new services and a better security than its predecessor IPv4. [12] The article "Importance and Benefits of IPV6 over IPv4: A study" summarize the real reason of its existence. It is not a benchmark. It is the gold standard. "IPV6 is the future of the Internet. It is not an option but an absolute necessity". [14]

## References

- [1] Antonio, Jara, Ladid Latif and Skarmeta Antonio. "The Internet of Everything." *Antonio Jara, Latif Ladid and Antonio Skarmeta. (2013). The Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications.* 4 (2013).
- [2] "Biting the bullet: A practical Guide for Beginning the Migration to IPv6

[White Paper]." June 2011.

<[www.fortinet.com](http://www.fortinet.com)>.

- [3] Caliscan, E. *IPv6 Transition and security Threat Report.* 2014.

<[www.ccdcoe.org](http://www.ccdcoe.org)>.

- [4] Davies, J. *Introduction to IP version 6.* 24 August 2002.

<<http://www.microsoft.com/windowss2000/techinfo/howitworks/communications/nameadrmgmt/introipv6.asp>>.

- [5] "Fortinet." 2011. *A Practical Guide for Beginning the Migration to Ipv6 (WP-IPV6-R3-20116)*. <<https://doi.org/www.fortinet.com>>.
- [6] *GST,MSTF*. 2011. <<http://www.gsc16.ca/english/documents/openplenary/GSC16-PLEN-42alrl.xls>>.
- [7] Hogg, S., & Vyncke, E. *Securing the Transition Mechanism.IPV6 Security*. Indianapolis: Cisco Press, 2009.
- [8] "IPv6 Security." May 2011. <<http://www.ietf.org/rfc/rfc0791.txt>>.
- [9] Jara, A, L Latif and A Skarmeta. "The Internet of Everything." *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*. 4.3 (2013): 98-111.
- [10] Kavala, Carole. "ipv6 Are we there yet?" 2015: 8.
- [11] Metz, C. "Moving toward an IPv6 Future [Computing Magazine]." *IEEE Internet Computing* (2003): 25. <<http://computer.org/internet/>>.
- [12] *Network Computing* . 2015. <<http://www.network.computing.com>>.
- [13] "Network World Retrieved." 2013. *Biggest risks in IPv6*. <<http://www.networkworld.com>>.
- [14] Reddy, P. P. *Importance and Benefits of IPV6 over IPV4: a study*. 12 December 2012. <[www.jsrp.org](http://www.jsrp.org)>.
- [15] Spitzer, L. Oct-Dec 2002. <<http://lists.insecure.org/lists/honeypots/2002/Oct-Dec/0105.html>>.
- [16] Teredo connectivity. (). n.d. <<http://teredo.ipv6.microsoft.com>>.
- [17] *The Future is Over, World IPv6 Launch*. (). n.d. <<http://www.worldipv6launch.org/measurements>>.
- [18] Warfield, M. H. *Security Implications of IPv6*. Internet Security Systems:, 2003. Document. <[www.iss.net](http://www.iss.net)>.

([19] Biting the bullet: A practical Guide  
for Beginning the Migration to IPv6 [White  
Paper])