International Journal of Future Generation Communication and Networking
Vol. 11, No. 1 (2018), pp.13-22
http://dx.doi.org/10.14257/ijfgcn.2018.11.1.02

# The Future of Internet: IPv6 Fulfilling the Routing Needs in Internet of Things

Fahad Samad, Asad Abbasi, Zulfiqar Ali Memon, Abdul Aziz and Abdul Rahman

*Department of Computer Science,*
*National University of Computer and Emerging Sciences (NUCES-FAST),*
*Karachi*
*{fahad.samad, k153507, zulfiqar.memon, abdulaziz and abdulrahman}@nu.edu.pk*

***Abstract***

*In recent years, the world has witnessed drastic change in modes of computing used in different application domains. The computing varies from confined biological sensing to controlling large cities using smart IoTs solutions. Consequently, footprint of devices is increasing at a higher speed. Therefore, for such huge footprint of computing devices it is of the leading importance to diminish the new challenges associated with the devices. Particularly, it demands for comprehensive and futuristic approaches for handling device identification and other related issues. Unfortunately, importance and necessity of public IP address for every device on the planet has not been understood well yet and taken for granted. However, current IPv4 solutions for device identification and management does not seem fit to address problems of this growing global IoT device space. Consequently, there is a dire need for IPv6. At its core, IPv6 is a recognized protocol established since the preceding era. IPv6 upholds the capabilities required for enhancements of network identification, management and data transfer related matters. In this connection, the fundamental objective of this study is to identify key challenges in emergence of devices with a specific and focused approach on IPv6. Moreover, the study shall provide comprehensive analytical overview of IPv4 and IPv6. Furthermore, study shall propose routing advancements required for switching from IPv4 to IPv6 along with backward compatibility.*

***Keywords****: IPv4, IPv6, Tunneling, Smart Devices, Interoperability, Security*

## 1. Introduction

The number of devices in the world is increasing radically due to technological progressions, real life application advancements and practices of numerous smart diversified machineries in almost every corner of human life (such as environmental monitoring, energy management, media, infrastructure management, medical and healthcare systems and transportation) [1][2][3]. This rapid development in applications shows that in near future there will be stable and steady stream of innovative applications and services through Internet of Things. IoT demands for thinking outside traditional computing boundaries. It stresses for small, smart and compact devices that could replace traditional computing capabilities and advancements in nano technology has made it possible to perform everyday operations by using these devices [3][4].

Moreover, it seems that these applications are just beginning of forthcoming giant industry in computing. This is result of rising technological evolution of computing devices specifically use of smart and elegant devices has become so popular nowadays that it would be very difficult to employ large-scale infrastructures without using these smart and interacting devices. Particularly, last era is abundant witness of such vagaries in

Received (August 29, 2017), Review Result (November 28, 2017), Accepted (December 1, 2017)

ISSN: 2233-7857 IJFGCN

human life's perspective. In this regard, excessive use of intelligent and elegant devices is evident as well. These devices take in sensors, surveillance devices, smart phones, actuators, laptops, RFIDs and wearables [2][7]. Today, all these technologies work stand-alone for specific applications and for some set of IoT related applications they must collaborate or share resources for distributed problem solving. In connection with all these said IoT technologies, Table 1 provides comparison of different types of IoT devices based on their attributes such as computational power, communication range, data rate, storage, battery life and data security. Table also demonstrates that IoT devices hold highest degree of heterogeneity and this heterogeneity is not only in device hardware but also in their data rates, types of data generated and communication capabilities. Although, there are numerous questions that visionaries and researchers have to work out for making such applications more efficient and reliable.

Thereby, this increase in devices also produces various challenges such as security, interoperability, privacy, integrity, data management. Another considerable challenge is unique identification and management of a globally connected network capable of sensing, communicating, information sharing and performing smart analytics for different daily life applications. Although, all these proficiencies will require public IP addresses to become reality. Unfortunately, importance and necessity of public IP address for every device on the planet has not been understood well yet and taken for granted. Moreover, it is another fact that currently used IP addressing mechanisms cannot provide IP addresses to such huge trail of devices present in the world. Since the beginning of the Internet, IPv4 has been the one & only network layer protocol working as a core address supplier. But nowadays it is facing some problems like addressing exhaustion, routing scalability and broken end-to-end property [14]. IPv4 device identification and management mechanism currently used has already been scarce. Therefore, the transition of ipv4 to ip6 has become unavoidable and predetermined. IANA (Internet Assigned Number Authority) address space of IPv4 has left no choice for the users to move to IPv6 [14]. Although, IPv4 also tried to adopt Network Address Translation (NAT) approaches to overcome address exhaustion problem by assigning one IP address to organizational network for communication on the internet. But this resulted in issues related to quality of service, security and other related problems [10]. Now, additive devices on the internet cannot get IP addresses by using IPv4. Henceforth, IPv4 is not suitable now to overcome this diverse challenge of providing public IP addresses to all devices [7].

**Table 1. Attributes IoT Devices**

| IoT | Computational Power | Communication Range | Data rate | Storage capacity | Communication | Battery Life | Data Security |
|---|---|---|---|---|---|---|---|
| Ethernet:<br>LAN IEEE 802.3<br>-cross over cable | 100 baseT1 | 100 meters | 100 Mbits/s | N/A | LAN/WAN | N/A | High |
| Laptops:<br>-Dell Inspiration i7559<br>-Lenovo G70 core i7 | 2.6GHz 300000 D MIPS@3.0 GHz | 150 m | 300000 D MIPS | 8GB 8.1 64 bits | Wifi Bluetooth | 4-8 hrs<br>-4-9 hrs | High |
| Wearables:<br>-Samsung Gear s3 | 1Ghz | 100 m | 30 to 45 mbps | 4GB | 4G LTE | 380 mAh Li-ion | Average |

 

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Smartphones:<br>-Infinite Note 3 pro<br>-Samsung galaxy J2 | 1.3Ghz<br>1.3Ghz | 130 m<br>130 m | upto 50 mbps | 16GB<br>1GB | 4G LTE, bluetooth,wifi<br>3G,bluetooth,wifi | 4500 mAh<br>2000 mAh | Average |
| Cameras:<br>-Sony DSLR-A900<br>-Canon EOS 6D | 5.0 fps<br>4.5 fps | 1.524m/s<br>1.3716m/s | 4 to 640 kbps | External | wired<br>wifi,gps | 880 shots | Low |
| RFIDs:<br>-NFC card<br>-Tags | 13.56 MHz | 15m | 106 to 424 kbit/s | Upto 8 kb | Wireless<br>Wifi | N/A | Low |
| WSN:<br>-open wireless sensor | 90 mips | upto 750 feet | upto 250 kbps | Application dependent | Wireless | Application dependent | Low |
| ZigBee:<br>Home automation | z-wave<br>90 mips | upto 750 feet | upto 250 kbps | Application dependent | Wireless<br>IEEE 802.15 | Application dependent | Low |

Nevertheless, computing world has to understand now it's the time to come out from the shelter of IPv4 and timely switch to IPv6 for better understanding and management of the futuristic network needs. At its core, IPv6 is a recognize protocol established since the preceding era. IPv6 upholds the capabilities required for enhancements of network identification, management and data transfer related matters [7]. It is the next-generation network layer protocol that is developed to overcome the problems of IPv4. It has 128-bt format that enlarges the address space & satisfies the address allocation demand. IPv6 is based on QoS which supports auto-configuration & play feature. If we talk about better mobility & security support, then it is much better than IPv4 [12]. There are numerous edge benefits that IPv6 offers over IPv4. Fundamentally, IPv6 has very higher address space as compared to IPv4 making sure that higher number of devices with their own IP addresses can be connected with internet and every attached device gets further larger pool of addresses too [8]. Moreover, it has four hundred times more addresses. This wide spread in address space is critical for the new class of IoT enabled emerging applications [7].

Further, IPv6 also provides enhanced transparent mobility provision to the devices. The support of MIPv6 in IPv6 offers improved mobility features for peer to peer and Voice over IP services [10]. Additionally, IPv6 provides simplicity, flexibility and minimized header overhead to augment the future header extensions. This simplicity helps routers to increase transmission efficiency [10]. Another important feature of IPv6 is stateless configuration which lets device to discover itself without intervention of DHCP server. Besides providing ease of management, this also reduces load of the manual device configuration and DHCP server involvement in configuration. This is done by using prefixes, Neighbor Discovery Protocol (NDP) and information stored within the router.

Furthermore, security is one of the main concerns while transmitting data over the internet. In this regard, IPv6 provides wide-ranging security features such as Stateles Address Auto Configuration, Internet Control Message Secure Neighbor Discovery, Confidentiality, encryption and authentication support as compared to IPv4. For this purpose, IP security (IPsec) has been made obligatory part of the protocol suite. Information is made secure for end to end transmission *i.e* while originated from the sending device, passing through intermediate routers and then finally delivered to the

 

destination. In order to accomplish rising data rate requirements and larger packet size support, IPv6 also provides augmentation in packet lengths by using concept of jumbogram payloads. Another leading network requirement nowadays is quality of service and IPv6 employs flow labels for this. It uses 20 bits for the identification and management of flow. Packets associated with one flow are treated similarly with some particular attributes [8][9]. With the help of this, different applications can get required quality of services accordingly. It has been believed worldwide that IPv6 is feasible and best solution for the next-generation internet. Therefore, both the transitions IPv4 & IPv6 coexists, so for solving the issues including DNS, QoS & security we need to manage the interoperability of IPv4 & IPv6 [16]. All above discussed features of IPv6 make it virtuous as compared to earlier version, but on the scale of Internet the conversion of such massive infrastructure from IPv4 to IPv6 is not an easy task to accomplish.

As far as IPv6 deployment is concerned, it's a fact that it could not get that virtuous foundational appreciation in industry but the constructive side is that some major network deployers have started or planned their services by using IPv6 in coming future. Moreover, some of the content providers have already made their websites compatible with IPv6. In this regard, governments are also scketing their plan for the active deployments of IPv6 [9]. Each of these adopters has stepped up to deploy IPv6 and the entire Internet community should applaud their efforts. But then again, still there is a lot more exertions to be put in this side. Generally speaking, there are two broad approaches for transition from IPv4 to IPv6. Either completely replace IPv4 with IPv6 or make interaction bridge between the two. Complete replacement approach seems workable for small network size but it becomes impractical because making such replacement on the scale of internet is not possible due to numerous reasons. On the other hand, alternative option is to use the mechanisms for IPv6 on top of IPv4 because it's very important to encounter the existing infrastructure with the newer one. In this case, efficient interaction methods will be obligatory for integrity and interoperability [11].

## 2. Related Work

The transition between the IPv4 (current internet) and the IPv6 (future internet) will be a long and tidy process. During this period both protocols can coexist. As a solution to this coexistence problem, different techniques for tunneling and interaction between hosts and routers is exploited. Tunneling can be used in a variety of ways and some of the mechanisms for tunneling and interactions between IPv4 and IPv6 has been discussed in the following section.

(i) Authors of [14] have focused on coexistence of both IPv4 and IPv6 protocols. Moreover, it is examined that IPv6 networks are steady and adoptable, therefore IPv6 should attain convenience of both IPv4/IPv6 networks. In this connection, authors have addressed basic problems of IPv6 protocol including heterogeneous traversing and inter-communication. Authors also introduced solutions and principles like tunneling and translation. Further, research work also provides translational and tunneling mechanisms covering aspects of technical principles, scalability and applications. This research work, divides translation mechanisms into stateless, stateful and host-side translation. Moreover, three types of tunneling mechanisms, Tunnel Mesh, Host-to-Host Tunnel and Hub and Spokes Tunnel are explored in detail.

(ii) In this research paper, authors have introduced IPv4 to IPv6 tunneling technique called DTTS (Dynamic Tunneling Transition Solution) [13] . Because IPv4 to IPv6 transition is an unavoidable procedure while deploying IPv6 network compatible with the present IPv4 version. DTTS accomplishing double stack IPv6 hubs to communicate with IPv4 hubs in IPv4 network. This solution is intricate as it needs to manage issues identified with IPv4-IPv6 interoperability. Further, DTTS transition burrowing strategy is utilized to typify an IPv4 packet in an IPv6 packet to accomplish straightforward and

 

adaptable operability. This technique is used to encapsulate an IPv4 packet in a IPv6 packet for transparent and scalable transition. DTTS has a few evident compensations such as straightforward end-to-end IP correspondence, adaptable organization, interoperability of IPv4 applications in IPv6 applications. DTTS as an IPv4 to IPv6 transition arrangement has extraordinary potential to accelerate IPv6 implementations and interoperability of DTTS on different operating systems and to include framework security to interact with other IPv4 applications in Both IPv4 and IPv6 network environments without any application proxy or gateway.

(iii) Nowadays, more and more user's interest is ever changing towards use of Voice over IP (VoIP) applications. In this context, interoperability of IP services is considerable challenge. For this purpose, this research in [10] proposes intermediary architecture for interoperable IP telephony services between IPv4 and IPv6 clients. The core study objective is to support transparent calls between the users of heterogeneous addressing mechanisms. The main components of this architecture involve SIP proxy, PSTN gateway, IPv6-IPv4 gateway, user agents and IP phones. To realize this, Session Initiation Protocol (SIP) server is utilized for registration and proxy services. Further, enhanced user authentication and telephony attributes are left for the future enhancements.

(iv) The replacement of current IPv4 with IPv6 is obligatory. But along with smooth transition, performance evaluation of this transition is also important. In this connection, authors in [15] worked in the direction of evaluating two traditional mechanisms for transition (IPv6 in IPv4 tunneling and 6 over 4). The principal objective of this work is to evaluate performance related attributes like CPU utilization, connection time, throughput and latency. These are the major factors for end to end performance measurement. For this purpose, authors have utilized test bed configurations. These configurations involved two routers and workstations and tests were conducted for very large number of packet exchanges between routers/workstations. Finally, results of the host to host encapsulation/ tunneling and router to router encapsulation/ tunneling has been presented.

(v) Transition from IPv4 to IPv6 is a tidy process. A lot of research has already been done in this direction and its backward compatibility has extensively been studied. This research work [16] is also focused with the aim of discussing constraints imposed, compatibility techniques and standardization requirements for the transition. Authors have discussed constraints such as incompatibility, incoherence, distractions, stepwise transition and IPv6 standards.

## 3. Limitations of IPv4

The Internet Protocol Version 4 (IPv4) was initially defined by IETF RFC 791 and RFC791 was published in 1981. [17] Initial architecture of IPv4 did not expect the rapid growth of internet and hence resulted in many problems, which demands that IPv4 needs to be replace soon. The main limitations of IPv4 are listed below:

(i) Scarcity of IPv4 Addresses: The IPv4 addressing scheme uses 32-bit address space. This 32-bit address space is classified to further A, B, and C classes. 32-bit address space allows 4,294,967,296 IPv4 addresses, but the previous and current IPv4 address allocation schemes limit the number of available public IPv4 addresses. Addresses which are allocated to many organizations, were not used and this created scarcity of IPv4 addresses.

(ii) Private addressing and translation: To solve the issue caused by the scarcity of IPv4, and to save public addresses, people started to use private addresses for intranets. For example, a home network can use a special reserved range of IPv4 addresses to communicate between devices in the local network. This permits internal communications to be recognized easily, but any external access requires the use of IP translation. In this context, many organizations, uses Network Address Translation scheme because private addresses cannot be routed on public IP networks. Because scarcity of IPv4 addresses,

 

many companies implemented NAT (Network Address Translation) to map multiple private IPv4 addresses to a single public IPv4 address. By using NAT (Network Address Translation) we can map many internal private IPV4 addresses to a public IPv4 address, which helped in preserving IPv4 addresses. But NAT (Network Address Translation) also have many shortfalls. NAT (Network Address Translation) do not support network layer security standards and it do not support the mapping of all upper layer protocols. In some cases, NAT also creates network problems when two companies communicate with the same private IPv4 address ranges. As more servers, clients, workstations and mobile devices which are connected to the internet also request the need for more addresses and the current measurements prove that public IPv4 address space will be exhausted soon. The scarcity of IPv4 address is a major limitation of IPv4 addressing system. In home networking, it embodies a drawback since end-to-end services are hard to configure.

(iii). IP configuration: To overcome the scarcity of IPv4, most existing IPv4 operations must be either manually configured or uses a Dynamic Host Configuration Protocol (DHCP). DHCP is a standardized network protocol used on TCP/IP networks. A DHCP server dynamically assigns an IP address and other network setup parameters to each device on a network so they can connect with other IP networks. A DHCP server can enable computers to request IP addresses and networking constraints automatically from the Internet service provider (ISP), dropping the need for a network administrator or a user to manually assign IP addresses to all network devices. A router or a domestic or residential gateway can be configured to act as a DHCP server. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned to an IP address. With dramatic increase in IP devices, there is a need for a simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure.

(iv). Security Related Issues: As RFC 791 (IPv4) was published in 1981 and the existing network security threats were not projected at that time. Internet Protocol Security (IPSec) is a protocol suit which enables network security by protecting the data being sent over the network from external attacks. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and optional. Many IPSec implementations are proprietary. Confidential communication over a public medium such as the Internet requires security services that shield the data being sent from being sniffed, viewed or modified in transportation. Even though there is a standard for IPv4 security such as IPSec, but some implementations of it are proprietary and require consumer to spend more money for license fee to use this security suit on the client site.

Table 2, represents some of the key differences between the two versions of the protocol that will be helpful in understanding them.

**Table 2. A Comparison of IPv4 and IPv6 Properties and their Differences**

| IPv4 | IPv6 |
|---|---|
| An IPv4 address consists of four bytes, which means 32 bits long. | An IPv6 addresses are 16 bytes, 128 bits long. It means more bits, more addresses. |
| Each sub area known as octet, can vary from 000 to 255. | Each byte in turns is represented as a pair of hexadecimal numbers. |
| 2 power 32, supports 4 billion addresses in total. | Total of 2 power 128 unique addresses. |
| A typical IPv4 address look like 123.123.255.255 | A typical IPv6 address looks like IE3D7:0000:0000:0000:51F4:9BC8:C0A8:6420 |

As we can observed from the address length of IPv6 that it is cable of supporting a huge amount of addresses in the global network space, make it more suitable to be

 

adopted as a standard for Internet Of Things. An address is represented in hexa numbers and is typically written as hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh. The following Figure 1, shows how these addresses are interpreted.

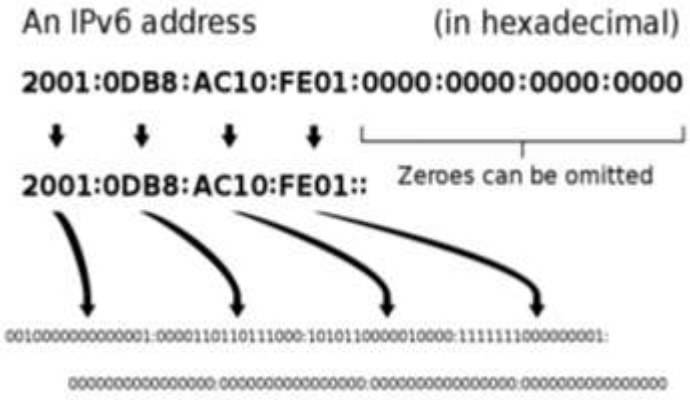


**Figure 1. An IPv6 Address Representation**

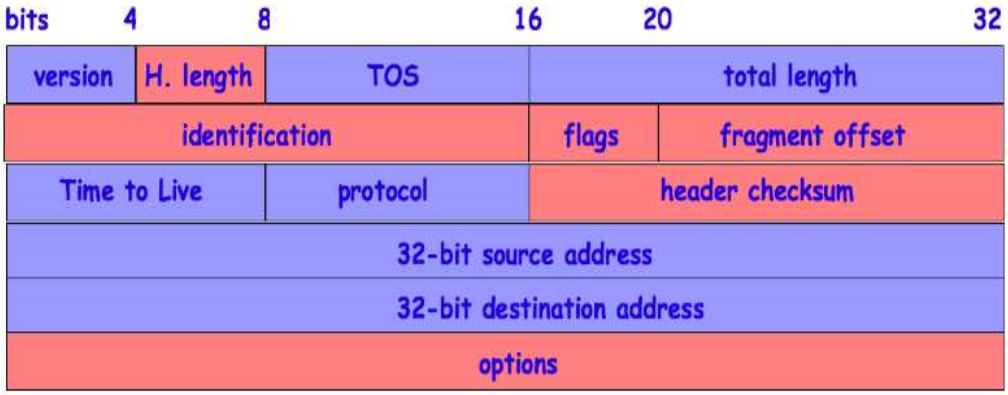


**Figure 2. An IPv4 Header Format**

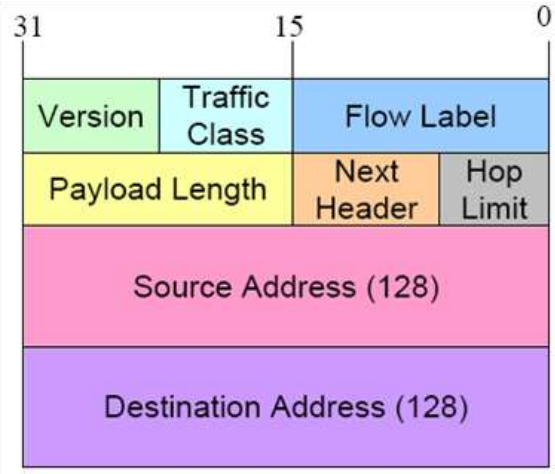


**Figure 3. An IPv6 Header Format**

## 4. Key Challenges

A lot of work has already been done towards global deployment of IPv6, but still needs sufficient effort to be put for mitigating challenges faced. In continuance of this, preceding section discusses challenges faced by IPv6 deployment. Here, it's needed to understand the key obstacles confronted in slower adoption of IPv6 on global internet scale. In this regard, Figure 1 gives details of the challenges which are primarily involve in slow adoption of IPv6 in industry. These challenges mainly involve lack of standards, costs, coordination with IPv4 and so on. The detail of the challenges is given as follows:

(i) Lack of Fixed Standardization: One of the leading challenge IPv6 acceptance is that industrial IPv6 implementations are still lacking with the De facto global standards that routing devices need to follow. These standards are very crucial and will play fundamental role for interoperability and scalability of IPv6 on global scale. Moreover, these standards will also make it easy to convince industrialists to use IPv6 enabled routing mechanisms and technologies. Though, standardizing billions of heterogeneous network devices from all parts of the world is not easy task.

(ii) Interaction of IPv4 and IPv6: Currently, IPv4 and IPv6 work stand-alone very proficiently for specific applications, but both don't collaborate for newest routing requirements and latest application or technological trends. Although, there are a few methods which are utilized for translation between IPv4 and IPv6. Some basic mechanisms are 4rd, 6rd, NAT64, DS-Lite and various tunneling mechanisms. Because switching to IPv6 is slow and iterative process, we can't disrupt network accessibility and organizational operations during that. Therefore, we need to employ unified way of interaction and address mapping between IPv4 and IPv6 enabled devices. Further, it is also required to employ new protocols for device discovery, monitoring, communication and routing that could support new-fangled needs of Content Distribution Networks, service providers, and other related network entities. This coordination and compatibility is very significant while waiting for the conversion of major part of internet to IPv6. (iii) Cost: Another leading factor in slow acceptance of IPv6 is the inevitable cost of conversion. Cost effect varies for different network players according to their different roles in internet. It is also evident that most of the existing internet infrastructure is ready for IPv6 but still it is not the case of simply reconfiguration only to make it work and start using IPv6. Undesirably, there are associative costs involved in this transition process. The major costs involve hardware cost, time, effort, human expertise, staff training and software upgradation. The unavoidable problem here is whole internet infrastructure is not equipped with hardware resources that are required for general IPv6 capabilities. Although, appropriate hardware will play vital role for IPv6 deployment. Consequently, upgradation of hardware at some extent is obligatory. Further, this hardware change will also call for change in software used. Thus, upgradation in software will also augment additional costs. Another cost related issue for organizations is training of the staff. This training is much needed that without this organizational staff will not be able to avoid problems associated to network configuration, maintenance and security related issues. Hence, to speedup industrial acceptance of IPv6, cost matrix should be worked out to provide affordability to all the stakeholders.

 

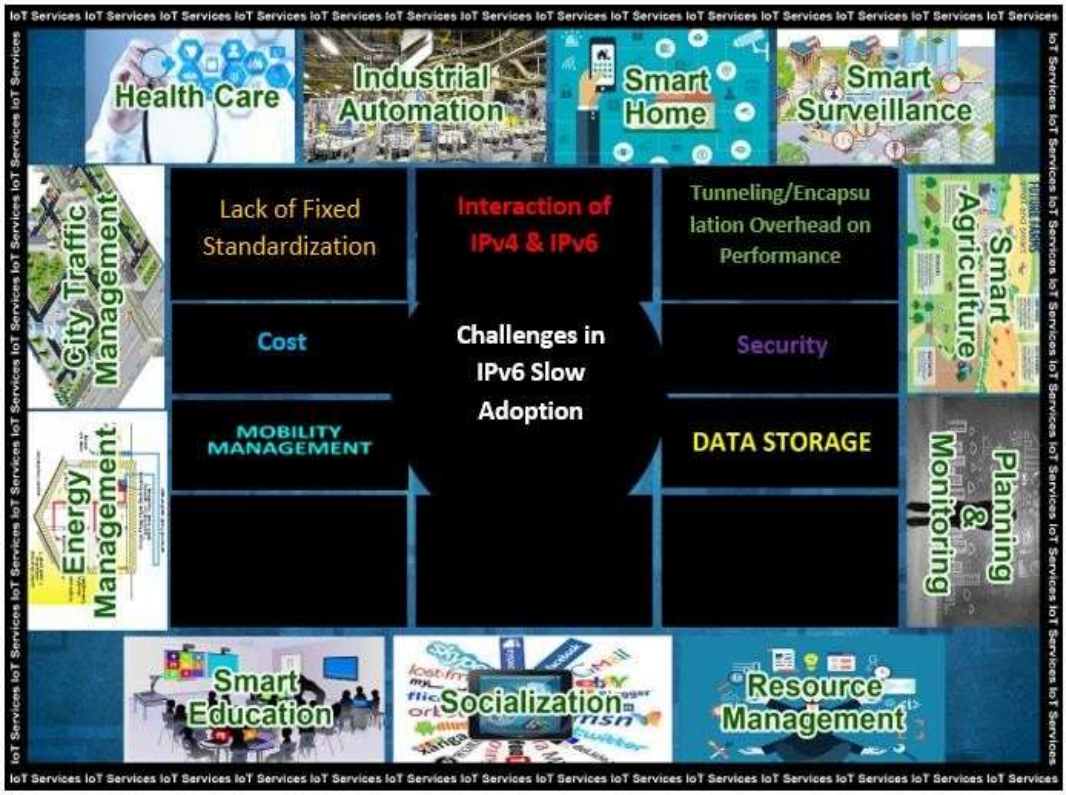


**Figure 4. Challenges in IPv6 Slow Adoption**

(iv) Security: Security concerns related to the IPv6 are very critical as well. Organizations need to train their staff for satisfying lack of IP6 security knowledge so that IPv6 practitioners should be able to handle attacks or security holes in organizations.

(v) Tunneling/Encapsulation Overhead on Performance: Another primary concern for slow IPv6 adoption is the employment of tunneling/encapsulation techniques. There are various situations where it is necessary to use encapsulation methods for the packet delivery and this encapsulation of packets adds extra overhead and effects overall system throughput. On average, this encapsulation adds 40 to 60 additive bytes in packet size and by default additive bytes means delay in the transmission.

In contrast with all discussed challenges, some other concerned challenges are related to mobility management, data storage and user trainings. Moreover, it seems very difficult to witness widespread deployment of IPv6 in industry- without confronting the above-mentioned challenges.

## 4. Conclusion and Future Directions

Importance and necessity of public IP address for every device on the planet can be achieved by using comprehensive and futuristic approaches for handling device identification, management and other related issues. IPv6 is a recognized protocol established since the preceding era and it upholds the capabilities required for enhancements of network identification problems. In this regard, this research work focuses on discussing the key obstacles confronted in slower adoption of IPv6 on the global internet scale. These challenges mainly involve lack of standards, costs, coordination with IPv4, tunneling/encapsulation overhead on performance and security issues. Further, research also elaborates tunneling mechanisms used in IPv6. It seems that research community and organizations need to take part in solving these problems for effective implementation of IPv6. Practical evaluation of IPv6 implementations and interactions and their scalability is left for the future work.

## References

[1] J. Montavont, D. Roth and T. Noël. "Mobile ipv6 in internet of things: Analysis, experimentations and optimizations", Ad Hoc Networks, vol. 14, **(2014)**, pp. 15-25.
[2] Z. Sheng, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities", IEEE Wireless Communications, vol. 20, no. 6, **(2013)**, pp. 91-98.
[3] , A.P. Castellani, "Architecture and protocols for the internet of things: A case study", Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on. IEEE, **(2010)**.
[4] A. Al-Fuqaha, "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, **(2015)**, pp. 2347-2376.
[5] M. Jung, "A transparent ipv6 multi-protocol gateway to integrate building automation systems in the internet of things", Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, **(2012)**.
[6] S. Chakravorty, "Challenges of IPv6 flow label implementation", Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, **(2008)**.
[7] A. J. Jara, L. Ladid and A. F. Gómez-Skarmeta, "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities", JoWua, vol. 4, no. 3, **(2013)**, pp. 97-118.
[8] G. Wood, "IPv6: making room for the world on the future Internet", IEEE Internet Computing, vol. 15, no. 4, **(2011)**, pp. 88-89.
[9] M. Gregr, P. Matousek and M. Sveda, "Practical IPv6 monitoring-challenges and techniques", Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on. IEEE, **(2011)**.
[10] L. Lambrinos and P. Kirstein, "Integrating voice over IP services in IPv4 and IPv6 networks", Computing in the Global Information Technology, 2007. ICCGI 2007. International Multi-Conference on. IEEE, **(2007)**.
[11] M. Bagnulo, "DNS64: DNS extensions for network address translation from IPv6 clients to IPv4 servers", **(2011)**.
[12] K. Wang, A-K. Yeo and A. L. Ananda, "DTTS: a transparent and scalable solution for IPv4 to IPv6 transition", Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on. IEEE, **(2001)**.
[13] P. Wu, "Transition from IPv4 to IPv6: A state-of-the-art survey", IEEE Communications Surveys & Tutorials, vol. 15, no. 3, **(2013)**, pp. 1407-1424.
[14] I. Raicu and S. Zeadally, "Evaluating IPv4 to IPv6 transition mechanisms", Telecommunications, 2003. ICT 2003. 10th International Conference on. vol. 2. IEEE, **(2003)**.
[15] J. Govil, "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms", Southeastcon, 2008. IEEE. IEEE, **(2008)**.
[16] R.E Gilligan and E. Nordmark, "Transition mechanisms for IPv6 hosts and routers", Transition, **(2000)**.
[17] DARPA INTERNET PROGRAM, Jon Postel (Editor), (1981) The IETF website. [online] Available: https://tools.ietf.org/html/rfc791.

 