REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OBSTACLES AND REASONS THAT PREVENT TRANSITION TO IPV6

AHMED A. RADIF AL-KHAFAJI

M.Sc. THESIS
DEPARTMENT OF COMPUTER ENGINEERING
PROGRAM OF COMPUTER ENGINEERING

ADVISER
PROF. DR. HASAN HÜSEYİN BALIK

İSTANBUL, 2018

REPUBLIC OF TURKEY

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OBSTACLES AND REASONS THAT PREVENT TRANSITION TO IPV6

A thesis submitted by Ahmed A. Radif AL-KHAFAJI in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE** is approved by the committee on 08.11.2018 in Department of Industrial Engineering, Systems Engineering Program.

Thesis Adviser

Prof. Dr. Hasan Hüseyin BALIK

Yıldız Technical University

Approved By the Examining Committee

Prof. Dr. Hasan Hüseyin BALIK

Yıldız Technical University _____

Assoc. Prof. Dr.Sırma YAVUZ , Member

Yildiz Technical University _____

Assoc. Prof. Dr. Metin ZONTUL, Member

Istanbul Arel University _____

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my supervisor assistant Prof. Dr.Hasan Hüseyin BALIK to supervision and scientific advice that helped me to build this thesis.

Thanks go also to jury members for their suggestions and comments.

Finally , I would like to thank everyone who helped me and supported me on my trip to get a master's degree .

November, 2018

Ahmed A. RADIF AL-KHAFAJI

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ATU	Attitude Towards Usage
ARPANET	Advanced Research Projects Agency Network
AH	Authentication Header
BGP	Exterior Gateway Protocol
CIDP	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
ESP	Encapsulating Security Payload
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
IPv4	Internet Protocol Version Four
IPv6	Internet Protocol Version Six
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IPsec	Internet Protocol Security
ICV	Integrity Check Value
IU	Intention of Use
IETF	Internet Engineering Task Force
IPPM	IP Performance Measurements
ICANN	Internet Corporation for Assigned Names and Numbers
IKE	Internet Key Exchange
LAN	Local Area Network
MLD	Multicast Listener Discovery
NFS	Network File System
NAT	Network Address Translation
PU	Perceived usefulness
PE	Perceived of Use
PU	Perceived Usefulness
PEOU	Perceived Ease of Use
QoS	Quality of Service

RIP	Routing Information Protocol
RIRs	Regional Internet Registries
RFID	Radio Frequency Identification
SME	Subject Matter Experts
SA	Security Association
SPSS	Statistical Package for the Social Sciences
TWAMP	Two-Way Active Measurement Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UB	Usage Behaviour
WLAN	Wireless Local Area Network
WAN	Wide Area Network

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

OBSTACLES AND REASONS THAT PREVENT TRANSITION TO IPV6

Ahmed A. RADIF AL-KHAFAJI

Department Of Computer Engineering
M.Sc. Thesis

Adviser: Prof. Dr.Hasan Hüseyin BALIK

The evolution of internet technology has played an ineviTablerole in changing the façade of the world, specifically in terms of improved communication, enhanced organisational processes, etc. However, this whole credit goes to standard internet protocol suite (TCP/IP) that supports millions of internet devices. Since 50 years, internet-based activities were supported by IPv4, but due to increasing number of smartphones and internet driven devices, IPv4 would not be able to fulfil the demands of its consumers in the upcoming years. Considering the scenario, IPv6 has been introduced to act as a viable solution to the depletion of addresses that is expected to be encountered in the near future. However, there are certain factors that are hindering the transition of IPv4 to IPv6. The present research study has been conducted to analyse the factors that are hindering the adoption of IPv6. In this account, survey questionnaire has been conducted with 153 IT experts, working in Iraqi companies. The findings have revealed that lack of leadership support, perceived ease of use, need of skilled employees, and increased cost are the main factors that are restricting the organisation to shift from IPv4 to IPv6.

Key words: Internet Protocol , Ipv4 , Ipv6

ÖZET

IPV6'YE GEÇİŞİ ÖNLEYEN ENGELLER VE NEDENLER

Ahmed A. RADIF AL-KHAFAJI

Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Tez Danışmanı : Prof. Dr.Hasan Hüseyin BALIK

İnternet teknolojisinin gelişmesi, özellikle gelişmiş iletişim, gelişmiş organizasyonel süreçler vb. bakımından dünyanın çehresini değiştirmede kaçınılmaz bir rol oynamıştır. Ancak burada en büyük rolü milyonlarca kullanıcıyı destekleyen standart internet protokolü paketi (TCP / IP) üstlenmektedir. 50 yıldan beri internet temelli işlemler IPv4 tarafından desteklenmektedir; fakat akıllı telefonların ve internet kullanan cihazlarının kullanımının artmasıyla birlikte, IPv4 önümüzdeki yıllarda kullanıcıların istek ve ihtiyaçlarını karşılayamamaya başlayacaktır.Bu olasılık göz önünde bulundurulduğunda, IPv4'ün yerine, IPv6 gelecek yıllarda karşılaşılması beklenen adreslerin tükenmesi sorununa karşı uygulanabilecek bir çözüm olarak düşünülebilir. Ancak IPv4'ten IPv6'ya geçişi engelleyen bazı etkenler vardır. Bu çalışmada IPv6'nın uygulamasını engelleyen söz konusu etkenler ele alınmıştır. Çalışma için bir anket oluşturulmuş, hazırlanan bu anket çeşitli Irak şirketlerinde çalışan 153 bilişim uzmanı tarafından cevaplanmıştır. Anketin sonucuna göre, liderlik desteğindeki eksiklik, fark edilen kullanım kolaylığı, yetişmiş eleman eksikliği ve yüksek maliyet, IPv4'ten IPv6'ya geçişi engelleyen en önemli etkenlerdir.

Anahtar Kelimeler: İnternet Protokolü, Ipv4, Ipv6

CHAPTER 1
INTRODUCTION

The chapter incorporates the detailed analysis of the introductory elements that contributed to the successful completion of this thesis. In this account, the background information has been provided in the chapter to establish the foundation of about IPv4 and IPv6. Some of the other sections of the introduction include a problem statement, aim and objectives, adopted the methodological approach, research scope, and the entire structure of the thesis.

1.1 Literature Review

The internet technology has been recognised as the global system of interconnected computer networks that make use of standard internet protocol suite (TCP/IP). This protocol suite plays an ineviTablerole in connecting billions of computing devices, across the globe. In short, internet technology has commendably contributed in the evolution and tremendous growth of the digital devices and their application in approximately all aspects of life. It has been established from the analysis of the study of Shah[1], that since its advent the operations of the internet became dependent on IPv4 (Internet Protocol Version 4). IPv4 is the fourth version of IP that is famous for efficiently routing traffic on the internet. IPv4 is nothing more than the connectionless protocol that works on packet-switched networks. IPv4 had served the internet world for the period of fifty years and it is also the fact that the internet, based on IPv4 has made considerable success during the period of last twenty years. However, because of the

insufficiency of the unallocated IPv4 addresses, this protocol was not able to fulfil the changing needs of the ever expanding internet. In other words, it can be affirmed that the exponential growth in the number of technological systems and devices had resulted in the exhaustion of IPv4. Some of the researchers have claimed that the scale of IPv4 internet has become far bigger than it was expected at the time of its designing. The situation had resulted in causing series of issues to IPv4 that include broken end-to-end property, scalability of routing, and address exhaustion Shah[1]. IANA (Internet Assigned Numbers Authority) had started facing the issue of IPv4 address pool exhaustion. At that time, it was predicted that in next three years all 'Regional Internet Registries' (RIRs) will completely utilise their address space (specifically the one that belong to IPv4). In the year 2011, February ICANN (Internet Corporation for Assigned Names and Numbers) had given out the last block of the IPv4 address. In short, it is expected the address space of IPv4 will be completely depleted. Though, SPs (service providers) have resorted to a number of mechanisms, for instance, multi-layers of NAT (Network Address Translation). The main objective of such initiatives is to reuse and save the address blocks from exhaustion. However, the more appropriate approach to handle this issue was to move from IPv4 to IPv6. According to Sharma and Singla[2], IPv6 which is also referred as IPng is the most viable solution to the depletion of IPv4 address space. In other words, IPv6 has been designed and presented as the next-generation network layer protocol that would efficiently overcome the issues in IPv4. IPv6 possess the address space of 128 bit and authorises around 340 undecillion addresses Sharma and Singla[2]. It shows that IPv6 would definitely fulfil address needs of continually increasing network devices. Besides that, the address length of IPv6 also plays a significant role in making the prefix aggregation fairly flexible; thereby, successively achieving global routing and addressing in a hierarchical pattern. Thereby,

it can be asserted that IPv6 is the feasible, mature, and the most viable solution for the next-generation internet that is demanding increasing IP addresses.

1.2 Objective of the Thesis

The aim of the present research is to examine the reasons that are involved in the existence of IPv4, despite the development of IPv6. In order to successfully accomplish this research aim, following objectives have been formulated.

- To examine the functions and characteristics of IPv4.
- To analysis the functions and characteristics of IPv6.
- To understand the need of transition from IPv4 to IPv6.
- To recognise the security threats that are posed to IPv4 and IPv6.
- To assess the factors that are hindering the adoption or assimilation of IPv6.
- To deploy TAM (Technology Acceptance Model) for determining the adoption of IPv6 in Iraq.

To make recommendations to the IT experts of Iraq to ensure a smooth transition from IPv4 to IPv6.

1.3 Hypothesis

Hypothesis plays an imperative role in the successful accomplishment of the research objectives. Therefore, it is considered as one of the greatest responsibilities of the researcher to make cautious decisions while selecting the methodology of the research Bernard and Bernard[6]. While taking these aspects into consideration, the present research has adopted mixed research approach. In this account, primary quantitative data was collected by conducting survey questionnaire with the IT experts, working in Iraqi organisations. It is significant to bring into the notice that the survey questionnaire was developed on the basis of the constructs of TAM (Technology Acceptance Model) the model has been designed to show how users come to accept and use a technology.

The theoretical basis is built on the premise that when users are presented with a new technology, three major factors influence their decision on how and when they will use it. The first determinant is its PU (Perceived Usefulness), the second is the PEOU (Perceived Ease Of Use), while the third determinant is user ATU (Attitude Towards Usage). According to Davis perceived usefulness (PU) is the degree to which a user believes that using a particular system would enhance his or her job performance.The survey questionnaire was conducted with 153 IT professionals, working in Iraq. Besides that, secondary sources (literature review) were also used to establish more cohesive understanding of the core concepts, related to the research work. The combination of the primary and secondary data has played an ineviTablerole in the successful accomplishment of the research objectives. The quantitative data was analysed by using SPSS(Statistical Package for the Social Sciences) software, it is for editing and analyzing all sorts of data. These data may come from basically any source: scientific research, a customer database, Google Analytics or even the server log files of a website. SPSS can open all file formats that are commonly used for structured data.

1.4 Problem Statement

IPv6 with its enhanced features, in terms of new addressing schemes and improved IP packet headers, had gained considerable recognition in the networking and technology-driven organisations. Regardless of these benefits, the adoption of IPv6 is still in its infancy and the majority of the organisations prefer to continue on IPv4. According to Durdağı and Buldu[3], the adoption of IPv6 is slowed down because of facing numerous obstacles. First of all, there is not any financial driver for the organisations that could motivate them to move towards IPv6. Moreover, it is also observed that IPv4 address space exhaustion has been advertised for several years that have resulted in leading the industry towards developing such technologies that could help them in extending the

use of IPv4 address. In this regard, one of the most popular technologies includes NAT (Network Address Translation). This feature ultimately limits the communication amid IPv6 and IPv4 networks. In particular, an independent and parallel network has been developed by IPv6 that exist with IPv4. In such circumstances, if the IPv4 network supports the communication activities of IPv6 then it will have to ensure dedicated routing and addressing for IPv6 while upgrading its network devices. Interestingly, the IPv6-accessible contents and IPv6-driven application are still in minimum number and the majority of the network applications, services, and resources are compatible to IPv4. This scenario shows that IPv4 networks are expected to last for the longer periods of time and it would take several years to completely move towards IPv6 from IPv4. When the adoption of IPv6 was assessed in the global context, it was observed that Belgium has been ranked as the global leader in the adoption of IPv6 with 46.4% connections. However, some of the countries have considerably low adoption rate of IPv6, including Singapore (3.5 per cent), Israel (2.9 per cent), Austria (3.0 per cent), South Korea (2.2 per cent), Oman (0.1 per cent), Bosnia / Herzegovina (2.9 per cent), Denmark (1.2 per cent), China (0.3 per cent), Tanzania (0.2 per cent), Zambia (0.1 per cent), and Iraq (0.0 per cent) Akamai[4]. The biggest issue that is hindering the complete transition from IPv4 to IPv4 is the limited knowledge of the executive and technical experts regarding IPv6 and its associated functions. It is a fact that the security solutions that are currently being used for the mitigation of the IPv4 security issues are not sufficient for the threats that are posed to IPv6. However, hackers have developed such malicious codes and techniques that have IPv6 specific features. It is established that the malicious codes and security vulnerabilities can be easily identified during the phases of penetrating testing; however, security experts usually avoid carrying out these activities as they are time-consuming Çalışkan[5]. It is also found that the limited awareness, lack of

comprehensive penetration testing practices, and the unwillingness of the organisations to invest in employee training and infrastructure, lack of compatibility amid IPv4 and IPv6, etc. are the core factors that are hindering the transition to IPv4 to IPv6.

1.5 Research Scope

There are the clear evidences that the address spaces in IPv4 will be completely depleted in the upcoming years. This aspect has also been acknowledged by concerned entities that are responsible for the provision of IP address allocation. Moreover, it has also been notified that the negligent behaviour towards the transition from IPv4 to IPv6 would result in putting the organisations and internet users in a devastating situation. Therefore, it is essential to adequately understand the need of moving towards IPv6, while assessing the measures that could help in the smooth transition from IPv4 to IPv6. The present research work is expected to significantly contribute to the presently existent literature regarding IPv4 and IPv6 transition and would commendably highlight the aspects that are responsible for the existence and widespread use of IPv4, despite IPv6 development.

1.6 Thesis Structure

The structure of the thesis is as follows:

Chapter 1: The chapter entails the introductory elements that played a critical role in the planning phase of the research. The main features of the chapter include background, problem statement, research aim and objectives, methodological approach, and research scope.

Chapter 2: The chapter incorporates the review of the diverse literature, related to the exhaustion of IPv4 and limited adoption of IPv6 and the reasons behind low adoption rates. The chapter has greatly contributed in establishing the theoretical foundation of

the present research work.

Chapter 3: The chapter demonstrates the methodological approaches that have been adopted by the researcher to accomplish the research aim and objectives. Some of the prominent constructs of the chapter include research approach, design, data sources, data collection techniques, sampling strategy, data analysis techniques, and description of variables.

Chapter 4: The chapter includes the findings that were drawn from the data, collected from survey questionnaire.

Chapter 5: This is the last chapter of the thesis that encapsulates the concluding remarks, on the basis of the collected evidence. The chapter also provides some recommendations that could be helpful in accelerating the adoption of IPv6.

CHAPTER 2
GENERAL INFORMATION

2.1 Introduction

The section reviews literature related to internet version protocol 4 and 6 so as to recognise the reasons for widespread use of IPv4, despite the emergence of IPv6. According to Bilski[7], the evolution of internet from IPv4 to IPv6 is one of the biggest transformations that is quite complex in nature and consumers extensive resources (financial and human resources). It is expected that this transformation is going to bring considerable changes in the internet services, i.e., in terms of data security, network performance, and economy. Most importantly, IPv6 would offer huge address space that would address the continually increasing need of address spaces, due to rising internet-driven devices. However, it is observed that the majority of the IT experts still prefer to continue their operations of IPv4, instead of switching towards IPv6. It is found that the increased need for resources, security issues related to IPv6 transition and deployment phase, lack of support etc. are the core factors that are hindering the adoption of IPv6. For establishing a cohesive understanding of these aspects, diverse related studies have been reviewed in this section. Specifically, the section incorporates the review of literature related to internet protocols functions and characteristics. The chapter also includes the in- depth analysis of IPv4 and IPv6 in terms of their address representation, packet header, features, and benefits. The transition from IPv4 to IPv6 is also discussed in the section, on the basis of diverse literature and studies. The security threats,

associated with IPv4 and IPv6 are also assessed in the section, along with the detailed comparison of both of these internet protocols. Factors that are hindering the transition to IPv4 to IPv6 are also incorporated in the section.

2.2 Internet Protocols and its Functions

Mason and Mahindra[40], have demonstrated IP(Internet Protocol) as the one that is present in the network layer. The main function that is carried out by this protocol is to transmit data from the source host to the destination host. It is important to note that a unique number is assigned to each host that eradicates the risk of duplication or any other related issue. In short, the IP is nothing more than the network-layered protocol that incorporates source control information as well as the addressing information that ultimately leads the packets to be routed. Aluko et al.[8], had stated that internet has played an ineviTablerole in making the entire world, a global village, specifically by connecting billions of devices. It is important to note that the correct, secured, and meaningful connection between these devices is established through distinctive IPs. Therefore, it can be affirmed that the overall performance and functions of the internet are based on IP. For this reason, internet protocols have become the most famous non-proprietary (open system) protocol suite. Abdullahi and Mahadevan[9], had stated that IP is the protocol that facilitates communication activities, across the internet. The primary task of the protocol is to deliver datagrams, belonging from different protocols to the specific destination. These operations are based on the packet encapsulation, security techniques, specific addressing formats and other related capabilities of the internet protocol. According to Kozierok[10], IP is nothing more than the collection of protocols that are solely aimed at facilitating communication amid the networks. Aluko et al.[8], had highlighted some of the functions of internet protocols that include addressing, indirect delivery/routing, fragmentation and reassembly, and data

encapsulation and formatting/packaging. The main function of IP is associated with the host addressing that enable the datagrams to be delivered to the correct device, regardless of the presence of the arbitrarily large networks. While describing the data encapsulation and formatting/packaging function of IP, Aluko et al.[8], had suggested that it receives data from transport layer protocol TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) . Afterward, this data is encapsulated into the IP datagram before the commencement of formal transmission. Another function that is carried out by IP is the reassembly and fragmentation. In this account, the IP datagrams are transferred to the data link layer so as to pass the information towards the local network. However, when the IP datagram has to be delivered to the destination which is on the similar local network, it is usually done by the help of network's underlying WAN(Wide Area Network) / WLAN(Wireless Local Area Network) / LAN(Local Area Network) protocol. This practice is usually termed as direct delivery. Aluko et al.[8] , had stated that this activity is usually carried out with the help of some other protocols that mainly include the TCP/IP routing/gateway protocols and ICMP(Internet Control Message Protocol), such as BGP(Exterior Gateway Protocol) and RIP(Routing Information Protocol).

2.3 Internet Protocol Version 4

Bons and Weigand[11] , had referred to the definition of RFC 791 and regarded IPv4 as the first protocol version that was deployed on ARPANET(Advanced Research Projects Agency Network). After some time, ARPANET had become the internet. This internet protocol version had 32 bits address space that means it offered the space of 4, 294, 967, 296 addresses. Abdullahi and Mahadevan[9], had stated that the main objective of developing IPv4 was to ensure network interconnectivity. The operations of IPv4 are based on two-level hierarchy that mainly includes host part and network part. As far as

the function of both of these parts is concerned, it is found that host is responsible for carrying out the data packets to the final destination. On the other hand, network part has the responsibility of finding network's location, specifically where the host is connected. In this way, the functions of data transmission are performed on IPv4. While highlighting the operational significance of IPv4, Shah and Parvez[24], had stated that it is a fourth internet version and is among the first protocol's version that has widely been deployed in advanced TCP/IP. The protocol is supporting million and billion of networking devices because of having strong capability of delivering datagrams to the correct destination networks, without harming the integrity of the information. On the basis of this mechanism, the internet based on this protocol version (i.e., version 4) had made commendable success during the period of last twenty years. Bi and Leng[12], had highlighted that because of the unavailability of empty address spaces, this protocol cannot fulfil the needs of continually expanding devices that are driven by the internet. Hanumanthappa[13], had also presented the same idea by claiming that the unexpected explosion of internet-based devices has played a major role in the exhaustion of IPv4 address space that was based on only 32 bits. According to Ahmed[30], the exhaustion of IPv4 address space is apparent since the 1980s. Though a number of measures like CIDR addressing, etc. have been made to control the situation but the consumption of IPv4 addresses has reached to the alarming situation. Primarily, it is found that the increased utilisation of the cable modems, ADSL modems, increased usage of internet, increasing mobile devices, and growing internet users have significantly contributed to the depletion of IPv4 address spaces.

2.3.1 Limitations of IPv4

According to Hanumanthappa and Manjaiah[14], there were some serious problems that resulted in the development of next-generation internet protocol, i.e., IPv6. In particular, the biggest issue is associated with the unavailability of unique addresses to be allocated on to the devices. Some of the other issues of IPv4 that have been demonstrated by Johansson[16], include increasing the size of the routing tables, inefficient packet sizes, and inflexibility of the fixed length headers for new functions. Aluko et al.[8], had also highlighted some limitations of IPv4 that are mainly related to addressing configuration and service quality, security, and scarcity of addresses. However, Shah[1], had claimed that the exhaustion of IP address is the prominent issue in IPv4. Though, the structure of IPv4 is based on 32-bit address spaces, which has the capacity of offering approximately 4.3 billion unique addresses. Nonetheless, the rapid technological advancements and increased adoption of networking devices had resulted in an unexpected situation. In particular, the dramatic increase in internet users had caused scarcity of unique IP addresses and it is expected that in the upcoming years it would result in the complete exhaustion of address space. Besides the dramatic increase in networking devices, it is also found that IANA (Internet Assigned Numbers Authority) has registered a large number of IP addresses for special or local uses. This feature has also resulted in the exhaustion of address spaces in IPv4. Another limitation of IPv4, as highlighted by Hanumanthappa and Manjaiah[14], Aluko et al.[8], Shah[1], is related to large-sized routing tables. Since each network needs to have separate and unique routing Tableentry so if any network includes more hosts than the specific class it results in the need of moving up to the subsequent class or having two IP addresses of the similar class. It is important to note that besides the growing routing tables and inefficient allocation of addresses, the process of routing is also complex in IPv4.

Abdullahi and Mahadevan[9], had stated that another prominent aspect that could be considered as the biggest limitation of IPv4 is security. In the contemporary era, organisations have become cautious about the security of their confidential information. However, in IPv4, security is optional, which is regarded as the biggest limitation of this protocol version. Tavakoli and Swanson[15], had affirmed that during the development of IPv4 the only motive of the inventors was to develop such protocol that could facilitate communication. The security feature (i.e., IPSec, authentication) was added into this protocol, after a long time of its development. It shows that security is not built-in on the IPv4 infrastructure. Apart from it, QoS (Quality of Service) is another prominent factor that is deployed and considered as a type of service field that is usually present in its header. Shah[1], has suggested that besides security, large sized routing tables, and exhaustion of address spaces, there are some other features that are required in IPv4. These include the accommodation of plug and play or auto-configuration capabilities as well as the improved capabilities of multicasting. Tavakoli and Swanson[15], had stated that configuration of the address is impossible to be managed in IPv4. There are mainly two methods that are often used for the allocation of IP addresses. These include the utilisation of DHCP(Dynamic Host Configuration Protocol) server, which needs additional cost. On the other hand, the second method is to allocate unique IP to each user and ask them to specifically use those addresses to their devices. This procedure is found to be tough for the users. Tavakoli and Swanson[15], have stated that mobility-related issues are also associated with IPv4. In particular, IPv4 requires the nodes to make use of different addresses for different networks. Such practices result in affecting the network performance because of sudden connection drops that are due to frequent switching of networks.

2.4 Internet Protocol Version 6

Tavakoli and Swanson[15], have established that after observing the limitations of IPv4, IPv6 was developed. IPv6 is an acronym of internet protocol version 6 as is recognised as a next generation internet protocol. According to Shah and Parvez[24], IP next generation (Ipng) is the expected to serve the networking needs of the virtual world. Similar to IPv4, this internet protocol also offers end-to-end transmission of datagrams, across numerous IP networks. One of the characteristics of IPv6 is that it is based on 126-bit address space that would remarkably contribute in fulfilling the increasing need of address space. In other words, it can be affirmed that IPv6 would allow a number of users and devices on the internet to use the unique address. It would also increase flexibility in the allocation of addresses while increasing the routing efficiencies. Most importantly, it would completely eradicate the need of NAT (Network Address Translation) that was used for alleviating the exhaustion of IPv4 address space. According to Abdullahi and Mahadevan (2010), it is anticipated that IPv6 would take over the current position of IPv4, after its complete exhaustion. It is due to the fact that it posses a number of exclusive features including higher scalability of the network, improved flexibility, etc. IPv6 also facilitates the process of end-to-end communication without having the need of utilising other features, like NAT, etc. Shah[1], had also established that IPv6 is specifically developed for the resolution of IPv4 issues. Some additional features have been added in the pre-existing architecture to retain the advantageous elements of IPv4; thereby, achieving higher operational efficiencies. It is established that the applications, based on IPv6 posses the capability of providing improved performance and higher efficiency, in terms of latency and bandwidth Bi and Leng[12]. Johansson[16], had presented the same idea by claiming that IPv6 is an improved version of IPv4 and this enhancement is beyond the address spaces. IPv6

makes use of multicast and unicast addresses, similar to IPv4; however, it also utilises any-cast address. This can be considered as one of the greatest features that guarantee timely availability of the network. This feature ultimately eradicates the need of using extra protocols for the management of virtual addresses. Besides that, Johansson[16], had also highlighted that as compared to IPv4 the next generation internet protocol version is less complex and offers efficient and more improved routing capabilities to the network. While demonstrating the objective of developing IPv6, Aluko et al.[8], had contended that the dramatic internet growth and increased networking devices have played a substantial role in creating the need for expanding address spaces on IPs. IPv6 utilises 128-bit addresses that would provide address space of approximately 3.4x1038 addresses; thereby, it is expected that it would adequately satisfy the networking needs of the internet-driven world. Bons and Weigand[11], had claimed that IPv6 has not just resolved the issue of address space, but it has also played a remarkable role in restoring end-to-end internet transparency. The greatest feature that IPv6 is expected to offer to the companies is the enforcement of regional and geographic addressing. This feature would help the companies in having common prefixes on the basis of their geographical locations as well as their network providers. In short, IPv6 would resolve the current issues of the organisations by ensuring terminal mobility, automatic router and terminal configuration, end-to-end and highly protected accessibility for P2P applications, and unlimited addressing space. Abdullahi and Mahadevan[9], had also stated that strong security and mobility mechanisms are the prominent features of IPv6. IPv6 has built-in IPsec facilities, unlike IPv4, that protects the network from unintended security risks and vulnerabilities. According to Aluko et al.[8], IPv6 has integrated IPsec that is based on cryptographic security techniques. These techniques robustly secure the integrity, authenticity, and confidentiality of the network. Besides that, Abdullahi and

Mahadevan[9], had underlined another feature that makes IPv6 better than IPv4, i.e., the simplicity of the header. This feature plays an imperative role in improving the flow of traffic, i.e., no checksums and broadcasting are needed for determining traffic flows; thereby, resulting in better forwarding and performance of the network, at scalable rates.

2.4.1 Benefits of IPv6 over IPv4

According to Ahmed[30], along with considerably huge address space, internet service providers will be able to easily allocate the addresses to the users. It is a fact that NAT is helping the service providers in coping with the issues, related to address space exhaustion, but it is not effective for several internet applications like DNS(Domain Name System), NFS(Network File System), group conferencing, etc. IPv6 removes the need of NAT while providing improved services to the internet users in terms of higher flexibility, reliability, and strong connectivity. Yadav and Kaul[17], had also categorised the benefits of IPv6 into three types, i.e., no need for broadcasting features, strong security, and increased mobility. AbuAli and Aliudos[18], have stated that IPv6 is one of the greatest initiatives towards re-establishing end-to-end traffic and transparency across the internet. Shah and Parvez[24], had presented an idea that IPv6 plays an indispensable role in minimising the total time that is required for the management and configuration of the systems. The exclusive features of IPv6 support auto-configuration that result in the creation of unique and secured IP addresses, specifically through the combination of provided prefix and LAN MAC address; thereby, reducing the need of DHCP. Babatunde and Al-Debagy[19], had outlined some of the benefits of IPv6 including improved support for mobile computing and networking devices, expansion of multicast addresses, providing plug-and-play features, auto-configuration, strong security that is based on IPSec, reduced dependency over NAT (network address translation), hierarchical architecture of the network.

2.5 Security Threats posed to IPv4

It has already been discussed that IPv4 does not contain any built-in security mechanism. This feature ultimately exposes this protocol version to malicious security attacks. Durdağı and Buldu[20], have claimed that sniffing attacks are the most common attacks that are encountered by IPv4. In sniffing attacks, the hackers steal the confidential information of the users that are being transmitted over the network. In this situation, if the confidential and private information is transferred in the form of a plaintext protocol, it results in devastatingly impacting the integrity of the information due to sniffing attacks. Some of the other security attacks that are introduced to IPv4 networks are flooding attacks, application layer attacks, man-in-the-middle attacks, etc. Durdağı and Buldu[20]. However, Wieringa and Visser[21], had stated that worms, Trojans, and viruses are the prominent attacks that devastatingly affect the security of IPv4. According to Minoli and Kouns (2016), worms, Trojans, and viruses, once entered into a network, have the capability of spreading themselves across different hosts. Viruses and worms are usually transferred from one host to another or from one computer to another in the form of a file. However, Trojans is quite different from both of these types of attacks and seems to be like useful software, but damages the entire system. Luntovsky and Spillner[22], had stated that reconnaissance and port scanning are other security threats that are posed to IPv4. In this security attack, the attacker scans the host for getting an access to the available UDP and TCP. In this way, open ports are accessed to introduce a security attack to the specific host. Wieringa and Visser[21], had regarded DoS (Denial Of Service) attacks, fragmentation attacks, and MITM (Man-in-the-middle) attacks as the most malicious and dangerous security threats to IPv4. It shows that due to the absence of any built-in security framework, IPv4 is vulnerable to malicious security attacks.

2.6 Security Threats posed to IPv6

Despite having built-in security mechanism (i.e., IPSec) IPv6 is vulnerable to the security threats. According to Durdağı and Buldu[20], reconnaissance attacks severely threatens the security of IPv6. In this attack, the hacker collects important information from the network of the victim and uses it for performing malicious activities. It is found that reconnaissance attack is performed by using different active methods, like passive data mining techniques and scanning techniques. However, Sotillo[23], had contended that IPv6 is also prone to encounter dual-stack related issues. IPv6-IPv4 dual stacks would surely result in increasing the risks and vulnerabilities related to the security of the network, mainly due to the similar infrastructures of IPv4 and IPv6. As per the specification of IPv6 protocol, all related nodes should have the ability to process the routing headers. However, routing headers can also be utilised to avert access control initiatives on the basis of destination addresses. It is found that such behaviour usually results in the occurrence of security-related incidents. It is possible that the intruder tries to transmit packets of data to the publically accessible addressing along with the forbidden address, contained in a routing header. Such practices result in leading the host (that is publically accessible) to transfer the data packet to the destination; thereby, result in DoS attacks or spoofing attacks. Khudhair and Mohammed[42], had supported the idea by presenting the elaboration of the security attacks that are often encountered by IPv6. The issues that were explained by the researcher included firewall evasion by fragmentation, header manipulation, smurf attack (broadcast amplification attack), host initialisation attack, and reconnaissance attack. The prevalence of these attacks in IPv6 was also acknowledged by a number of researchers including Ullrich, and Weippl[25], Durdağı and Buldu[20], Choudhary[26], Sabir and Mian[27], Dawood[28], Hovav and Schuff[29].

2.7 Comparing Internet Protocol Version 4 with Internet Protocol Version 6

According Hanumanthappa and Manjaiah[14], IPv4 and IPv6 possess similar basic framework; however, they are different in several perspectives. In the context of addressing, Tavakoli and Swanson[15], had established that the most prominent difference that is present in IPv4 and IPv6 is associated with their addresses. The address of IPv4 is based on 32 bits; on the other hand, IPv6 possess 128 bits. It is also important to note that in IPv6, the total number of bits is equally divided among the host address and network address. It means that 64 bits are allocated for host address and 64 bits are allocated for the network address. Contrary to IPv4, IPv6 offers clear routing and addressing mechanisms. Babatunde and Al-Debagy[19], had highlighted another difference amid IPv4 and IPv6, which is related to hierarchical addressing. According to the researcher, IPv4 makes use of three addresses, i.e., multi cast, broad case, and unicast addresses. In contrast, IPv6 also uses three types of addresses, but are different from IPv4, i.e., multicast, unicast, and any-cast address. It shows that the only difference amid both of this protocol version is the introduction of any-cast address, which facilitates multiple nodes to be assigned the similar any-cast address. The application of the any-cast address is found in the creation of mirror websites that could be accessed at any geographical location, by using the similar any-cast address. According to Ahmed (2006), in IPv4 the fragmentation is carried out by both the sending host as well as by the routers. Contrarily, in IPv6 it is only performed by the sending host and not by the routers. Apart from that, in the context of security, Ahmed (2006) had outlined that in IPv4 IPSec is optional. On the other hand, in the case of IPv6, it is mandatorily required for the protection of the network from security-related incidents. The brief yet insightful comparison of IPv4 and IPv6 is provided in the below-provided Table 2.1.

Table 2.1 IPv4 and IPv6 Comparison Tavakoli and Swanson[15]

Internet Protocol Version 4	Internet Protocol Version 6
Destination and source addresses are 4 bytes (32 bits) in length.	Destination and source addresses are 16 bytes (128 bits) in length.
Mandatory to be configured through DHCP or manually.	No requirement or DHCP or
Options are included in the header.	IPv6 extension headers are there to receive optional data.
The checksum is included in the header.	No checksum is included in the header.
IPSec (security) is not mandatory.	IPSec (security) is not optional.
Broadcast addresses are utilized for the sake of transferring traffic to the nodes that are present on a subnet.	IPv6 does not include any broadcast address.
The local subnet group membership is used for the management of IGMP(Internet Group Management Protocol).	The replacement of IGMP is performed with MLD(Multicast Listener Discovery) messages.

2.8 Factors Hindering the Transition from IPv4 to IPv6

Babatunde and Al-Debagy[19] , had established that the migration or transition from IPv4 to IPv6 has been initiated, but the adoption rate is found to be too slow. A number of factors are involved in the slow adoption of IPv6 that mainly include infrastructure issues, financial issues, tunnelling issues, and security issues. Babatunde and Al-Debagy[19], had stated that IPv6 adoption is greatly hindered due to the infrastructure issues. A number of technologies and protocols are needed to be redesigned for the sake of supporting IPv6. These include TCP/IP, ARP, BGP, RIP, OSPF, and DHCP. On the other hand, Dey and Shilpa[31], had identified tunnelling issues are the ones that are hindering IPv6 adoption. The researcher has stated that without any transformation in applications, the next generation internet protocol can be utilised in a pre-existing

network, by using tunnelling techniques. It would act as a medium between IPv6 and IPv4. However, tunnelling is a time-consuming process and it has extremely minimal throughput. Babatunde and Al-Debagy[19], had recognised the need of additional financial resources as the limiting factor of IPv6 adoption. According to the researcher, the transition from IPv4 to IPv6 needs the companies and enterprises to invest their capital cost in the account of routers, switches, employee training etc. that restricts them to switch from IPv4 to IPv6. The vague and unclear security mechanism of IPv6, due to limited testing, is also restricting the companies to move from IPv4. Kaur[32], had claimed that the lack of required experiences and skills are limiting the organisations to assimilate and adopt IPv6. Grossetete and Wettling[33], have presented an idea that there is a limited availability of IPV6 SME(Subject Matter Experts). Hovav and Schuff[34], had also supported the idea by claiming that the lack of IPv6 skilled employees may restrict the organisation towards fully assimilating and adopting IPv6. Dell[35], has presented an idea that the wrong perception of the organisations towards IPv6 is also delayed IPv6 adoption. Some of the organisations perceive that IPv6 is immature and instable. Bons and Weigand[11], have also stated in this regard that perceived immaturity of IPv6 is the biggest hurdle in its adoption as most of the organisations consider this technology as the biggest risk to their security. Dell and Liu[36], have mentioned that the prominent barrier in IPv6 adoption is the reluctance of the organisations towards becoming an early adopter. Organisations usually find it better to learn from the experience of other organisations so as to save them from potential risks. White and Cook[39], have stated that cost is the biggest barrier to the assimilation and adoption of IPv6. Organisations tend to avoid the cost that is required for bringing additional hardware, employee training, etc. Grossetete and Wettling[33], have claimed that any investment that is related to IPv6 is considered as cost and

organisations prefer to avoid this cost. Another factor that is responsible for the limited adoption of IPv6 has been presented by White and Cook[39], i.e., underestimating the power of IPv6. In other words, some companies do not consider IPv6 as the strong and resilient business champion, as compared to other tools and systems. Such perceptions ultimately result in slow-paced adoption of IPv6 and leading the businesses to continue their operations on IPv4. Kaur[32], has affirmed that cultural differences also act a barrier to digital infrastructure adoption. Organisations, belonging from specific cultures or countries tend to delay or avoid the adoption of IPv6 because of having the low inclination and knowledge about digital technologies. Bons, E. and Weigand, H., (2011) [11] , have presented an idea that complexity of IPv6 and size of the organisation act as a barrier in IPv6 assimilation. It is found that large-sized companies usually avoid adopting IPv6, as they have to replace a greater number of equipment and applications during the adoption process. On the other hand, small sized organisations usually avoid its adoption because of having minimal financial resources. Gallaher and Rowe[38], had also emphasized that the size of the organisation act as a barrier in the decision of an organisation to assimilate IPv6. On the other hand, Kaur[32], had identified that lack of support from senior level management and decision makers also limit IPv6 adoption in organisations. White and Cook[39], had indicated that the over reliance of organisations on workaround technologies is the biggest factors that are hindering IPv6 adoption. These technologies were initially developed for the sake of handling the scarcity of IPv4 addresses; however, despite the development of IPv6, organisations are still relying on it. Some of the prominent technologies include CIDP(Classless Inter-Domain Routing), DHCP(Dynamic Host Configuration Protocol), and NAT. The analysis of all of these evidences has revealed that IPv6 transition must be carried out gradually so as to cause minimal disturbance to the existing networks. Moreover, organisations also need to be

vigilant and cautious during the planning phase, as it requires huge investment and efforts Mason and Mahindra[40], Khudhair and Mohammed[42].

2.9 IPv4 vs. IPv6 Support in Iraq

It is found that limited researches have been conducted in the perspective of IPv6 adoption in Iraq. The study of Khudhair and Mohammed[42], has shown that the majority of the Iraqi infrastructure, including institutions, companies, and universities are using IPv4 protocol and the users are least interested in assimilating IPv6. Findings, collected from IPv6-test (2017) have revealed that 100 per cent of the hosts in Iraq are supporting IPv4 and IPv6 is negligibly growing in a country. The low adoption and support of IPv6 in Iraq is also evident from the below-mentioned Figure 2.1 .

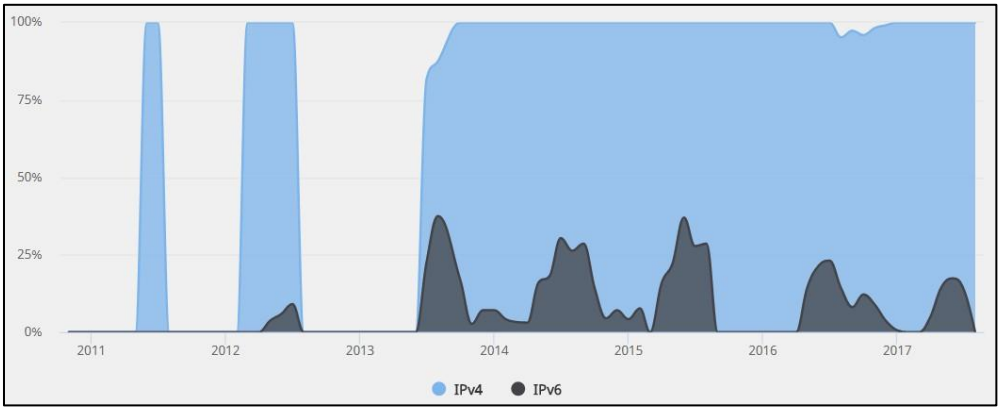

Figure 2.1 IPv4 vs. IPv6 Adoption in Iraq (IPv6-test, 2017)

When the factors behind the low adoption of IPv6 were analysed it was revealed that one of the greatest factors is associated with the limited awareness and management capabilities of the organisations. It is established that cautious handling of the operations is needed during the transition to IPv4 to IPv6 Çalışkan[5]. For instance, tunnelling operations, dual stack management efforts, IPv6 address mapping (i.e., through AAAA DNS records) are the core activities that are needed to be performed in a careful and vigilant manner so as to ensure organisational security. All of these aspects demand the organisations invest capitals, in the account of creating transition

plans, hiring and training employees, and successfully implementing the transition plans. Most importantly, bringing awareness among organisations, focusing on employee training and skill development, and top management support are essential for ensuring successful IPv6 transition in Iraq, Kaur[32].

2.10 Chapter Summary

The chapter has reviewed a number of related articles and studies so as to present a comprehensive knowledge about IPv4 and IPv6. In this account, the chapter has discussed and analysed both of these protocol version, while assessing their functions. In addition to this, the associated security threats and detailed comparison of IPv4 and IPv6 are also included in the chapter. The chapter has also shed light on the factors that are hindering the adoption of IPv6, causing a slow transition from IPv4 to IPv6. The current situation of IPv6 adoption in Iraq has also been briefly described, specifically due to the limited availability of relevant literature.

CHAPTER 3

IP SECURITY AND PERFORMANCE MEASUREMENT IPSEC ISSUE

3.1 Major Functions of IPSEC Protocols

IPsec (Internet Protocol Security) is considered a standard protocol for maintaining the security of networks in this era, with the implementation of cryptography. It provides safeguard against denial of service attacks and is implemented on most of the operating systems. IPsec is used to defend the flow of data between communicating hosts, between communicating gateways like firewalls, routers etc. or between a host and a gateway Dhall and Rani[43]. IPsec works on the basis of three major functionalities, i.e. authentication, confidentiality and key management. The authentication feature ensures that the received packet is sent by the source mentioned in the header of the packet and not from unwanted senders and it also ensures that the packet has not undergone any kind of alteration. Confidentiality feature of the protocol applies encryption on the message and therefore enables secrecy of the message and lastly it provides the decryption mechanism for the previously applied encryption, Stallings[44], IPsec can be implemented on the host end, at the gateway end, or even on both ends. At the host-end, the implementation of IPsec is implemented with the operating system at the network layer, and secondly, it can be implemented in between network layer and data link layer, which is called “Bump in the Shack” implementation. On the router’s end, IPsec is implemented to secure a packet over any network, and it has two types of implementation as well. Firstly, it has the native implementation, which is implemented

on the router's software and the "Bump in the wire" implementation, which is executed on the device connected to the physical interface of the gateway router, Stallings[44]. Every procedure of IPsec is used extensively, and its ability to secure communication is the main reason for its adoption in the companies, worldwide. IPsec protocol is implemented on the IP layer by defining suiTablealgorithms for the data transfer services, and different cryptographic keys are installed on the algorithm. Therefore, two protocols are used for enabling security on the networks; a protocol for authentication implemented on the header of the protocol i.e. AH(Authentication Header) and a collective authentication and encryption protocol designed in the format of the data packet known as ESP(Encapsulating Security Payload), Malik and Sya[45]. Authentication header is algorithm dependent because it works depending on the algorithm of choice, and the choice depends on the level of security that is required by the network. AH (Authentication Header) can be implemented alone if the only authentication of the packet is allowed, but for adding encryption to the packet, ESP is implemented. ESP enables limited traffic flow confidentiality and is also algorithm-dependent like AH (Authentication Header), Malik and Sya[45]. Both of these protocols when implemented support transport mode, which provides safeguarding on the upper layer, i.e. it mostly deals with end-to-end communication and tunnel mode, which provides protection on the entire data packet. The tunnel mode provides a separate packet outside the original data packet, with a different IP header as well. During the tunnel mode, the routers between source and destination are unable to determine the original data packet or even the header, Malik and Sya[45]. In addition to the above-mentioned algorithms, IPsec is also provided with encryption keys to the implemented algorithms, by the IKE (Internet Key Exchange), Malik and Sya[45].

3.2 Important Security Fields in IPv6

IPv6 was initially introduced to eliminate the shortage of IP addresses in the IPv4 networks, but it was preferred over IPv4 because of having better internetworking abilities. IPv6 has a built-in IPsec protocol just like IPv4, with authentication, confidentiality, and key management features that are included in it; however, IPsec protocols are optional in IPv4 while they are mandatory in the IPv6 scheme, which makes the system even more secured . Hovav and Popoviciu[37]. IPv6 provides an increase in address space, which makes the scanning of port difficult for the infiltrator. The number of bits in its address is 128 bits, a lot more than that if IPv4 addresses which are estimated to be scanned in about 10 hours; therefore, the duration for scanning IPv6 is longer. As mentioned beforehand, IPv6 is also based on IPsec protocol; therefore, it follows the functionalities of authentication, confidentiality, and key exchange mechanism. The AH (Authentication Header) of IPv6 is designed in a flexible manner, i.e. it does authentication and checks the integrity of those fields of the packet, which do not change during the transition. The AH (Authentication Header) also provides non-compulsory protection for countering replay attacks, which also ensures that the packet is not delayed Sotillo[23]. The Figure 3.1 below illustrates how the authentication header of IPv6 is designed theoretically (IBM, 2012, p. 16).

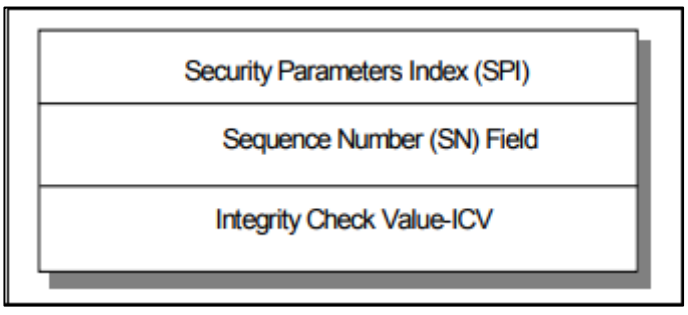

Figure 3.1 Specification of Authentication Header of IPv6

The SPI is a 32-bit value, which is used by the receiver to identify the incoming traffic to the SA(Security Association) of the IPsec protocol. Secondly, the sequence number part consists of a 32-bit value, which is similar to a counter for counting the number of each packet, sent or received. Initially, the counter is set to 0, of both sender and receiver, when the security association is established. Lastly, ICV(Integrity Check Value) is designed to protect the packet from altering by allowing the receiver to detect if there is any modification in the packet (IBM, 2012, pp. 16- 17). The AH (Authentication Header) ensures the integrity and authentication of the packets by using algorithms in end-to-end data communication, Sharma[46]. Another security feature of IPv6 network is the implementation of ESP, which is mandatory in the IPsec protocol. The packet consists of Security Parameters Index and Sequence Number, which are similar to authentication header. Following these, is the Payload data field, which provides a structure depending upon the choice of the encryption algorithm. Payload data has a variable length value and it consists of data from the original packet. The next segment consists of padding field, which consists of the value of the next header and also its length, and integrity check value completes the structure of ESP (see Figure 3.2). All data that follows this protocol is encrypted, and the next header must be relatively similar to the ESP header (IBM, 2012, p.18). The ESP further enhances the integrity and confidentiality and it also ensures authentication of origin data, anti-replay and integrity of the inner packet, and providing confidentiality to limited traffic flow, Sharma[46] .

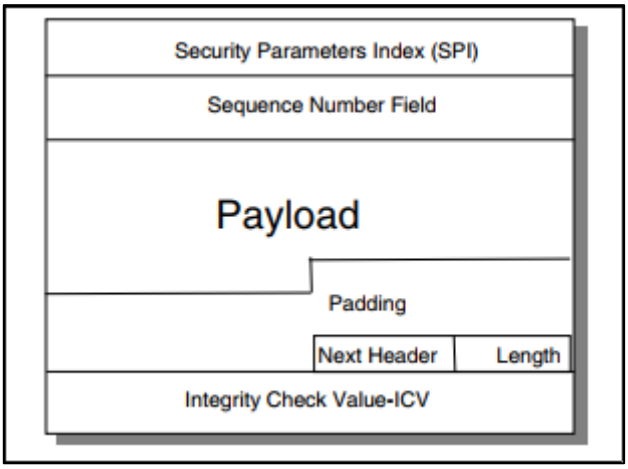

Figure 3.2 Specification of ESP Header of IPv6

3.3 Security Advantages of IPv6 over IPv4

Security advantage of IPv6 over IPv4 can be discussed with the fact that IPsec was not installed primarily in the design, but was developed as an additional feature. In IPv6 networks, IPsec protocol is embedded and is also made mandatory. IPv6 networks maintain simplicity and provide greater security assurance than IPv4 networks, Sharma[46]. IP security is implemented on layer 3 present in the OSI model, and with open standard protocols to provide security for datagram transmission. This method provides encryption and authentication to the packets during data communication, while providing data confidentiality and data integrity, Sharma[46]. The main purpose of introducing IPv6, apart from the increase in a number of addresses was the lack of data protection provided in IPv4. However, apart from a few changes in IPv6, it is still very familiar to IPv4 with respect to basic transmission mechanisms and above-layer protocols mostly unchanged, Sameeha[47]. In IPv4, the infiltrator has many ways to collect information, since the reconnaissance mechanism of IPv4 is vulnerable. The infiltrator can do ping sweeps by determining the addresses of the organisation, because the number of addresses in IPv4 configuration is limited. Furthermore, the hacker can execute the scanning of the ports to identify reachable or active systems and then use these active ports to determine the versions of operating systems and various

applications running on the host and manipulate them. However, in IPv6 the number of addresses is much more than IPv4, which creates a type of barrier to identify the active ports Ullrich, and Weippl[25]. The most common issue of IPv4 networks were the spoofing attacks of layer 3 and layer 4, which occurred on a daily basis. Ipv4 networks had difficulties to track denial of service attacks, spams, and worms, due to the sheer bulk of their occurrences. Layer 3 spoofing is difficult for the infiltrator because of the complications in guessing what the return traffic holds, therefore it is not used in interactive attacks. However, layer 4 spoofing is used interactively to change the destination of where the traffic actually came from. Some filtering mechanisms are discussed in various researches, but they are not generally implemented because they require extensive usage, Sameeha[47]. However, IPv6 networks are allocated in a way that filters can be applied on different points in the network. This allows internet service providers to guarantee that at least their own customers are not spoofing externally.

3.4 IP Performance Measurements

3.4.1 Related work of IP Performance Measurements

Performance measurement can be defined as the observation of the network technology, in terms of observing its application or its services. Performance measurement is a statistical estimation of the process and it determines the behaviour of the system White and Cook[39]. The performance of any IP network largely depends upon the QoS (Quality of Service) of the data traffic between networks. The key purpose of the quality of service is to make sure that the traffic moves along smoothly along its bandwidth. Internet service providers give their customers guarantee of steady end-to-end connection in the networks. For this purpose, high measurements of performance for quality aspects have become a definite requirement Grossetete and Wettling[33]. It is considered as a necessary

feature with the initiation of various wireless networks and smartphones. Cell phone networks are also executing performance measurements provided by the Internet service providers, for the measurement of Service quality of the networks, such as availability, latency, delivery etc. Soumyalatha and Kounte[49]. Measuring the performance of quality is a very challenging implementation due to the diverse nature of present networks and different types of flow of data. For this purpose, IETF(Internet Engineering Task Force) has assigned a working group, the IPPM(IP Performance Measurements), who has defined a certain standard for measuring the quality metrics of the system. The performance standards of the system consist of the reliability, performance, and quality of the delivery of data on transport protocol applications, Soumyalatha and Kounte[49]. The performance standards for measuring the service quality of networks considered are Bandwidth, delay and packet loss. The service providers give assurance regarding the quality of their networks by providing them with these standards, Kocak and Zaim[48]. For measuring the performance of IP networks, three protocols are usually used commonly, i.e. PING protocol, OWAMP protocol and TWAMP protocol. PING protocol is supported by almost all of the systems of ICMP networks for measuring the quality of packet delivery, Kocak and Zaim[48]. Ping is usually implemented for determining the connectivity of the host and the round-trip time to the connected host. Ping is widely used in networks but, its execution is bad practice for calculating delays because ICMP packets are limitedly rated in routers, Bäckström[50]. ICMP packets consist of the sequence number and the round-trip time is calculated by addition of time information to the sent and received packets. The protocol can be termed as limited because the incoming packets can be rejected or not sent, Soumyalatha

and Kounte[49]. The one-way active measurement protocol (OWAMP) examines one-way traffic by measuring delay and loss of packets in the traffic. The OWAMP protocol can be further divided into two subprotocols i.e., OWAMP-control and OWAMP-test. The control protocol can be used for setting up test sessions and gather results for the performance measurements of the one-way traffic, while the test protocol initiates the test packets which are used between the measurement nodes. The IIPM highly recommends implementation of both of these protocols together for the performance measurement. The research suggests that the wide-scale implementation of the OWAMP servers should be made a norm because the hosts are clock synchronized to NTP and GPS, David[51] .The TWAMP(Two-Way Active Measurement Protocol) supports layer 3 network protocols of the OSI model and it is used to measure the performance of any two devices Wieringa and Visser[21]. The quality of performance of the two-way traffic is measured at two TWAMP-supported endpoint. Its architecture is somewhat similar to OWAMP model and it adds the features of two-way and round-trip measurements. Similarly, like OWAMP, TWAMP also consists of two subprotocols, i.e. TWAMP-control and TWAMP-test. And the functionalities are similar as well, with TWAMP-control starts and stops test sessions and TWAMP-test initiates the exchange of test packets between the measurement nodes, Kocak and Zaim[48]. The research consists of an evaluation conducted between the devices to check the performance of the traffic between two nodes. During the evaluation, it was recorded that device A sends TWAMP test packet to device B and the device B responds back with the test-packets with a delay of 50 ms, and the topology of the test network is illustrated below, Kocak and Zaim[48].

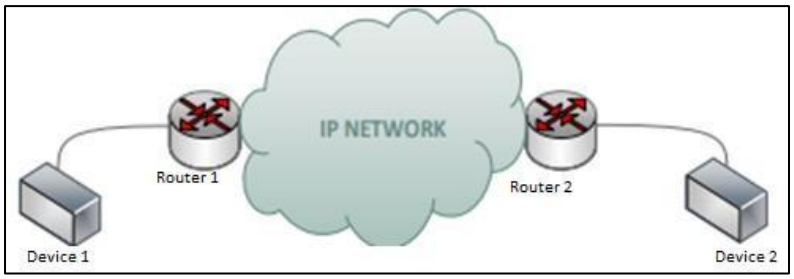

Figure 3.3 Test Topology of TWAMP Network

CHAPTER 4
ANALYSIS OF RESULTS

The chapter incorporates the analysis of the results that have been collected by conducting a survey with 153 IT professionals, working in Iraqi firms. As mentioned questionnaire was developed on the basis of the constructs of TAM (technology acceptance model) The Technology Acceptance Model, David[51] , has been applied in various information technology and information system areas . Researchers have identified specific areas where the model has been adopted. Moon and Kin used the model to explain the users' acceptance of World- Wide-Web in an educational context; Lin et al. in Chen and Chen et al. used the model in clarifying e-stock users' behavioral intention, Chen and Chen et al. adopted the model while investigating automotive telematics users' intention while Stern et al. used the model in their studies on consumers' acceptance of online auctions. Other researchers, Serenko et al. used the model to assess user acceptance of interface agents in daily work applications whereas Muller-Seitz et al. used the same model to determine customer acceptance of RFID(Radio Frequency Identification). Almasri arguments that TAM is an accepTablemodel and has been employed in many information technology and information system areas such as e-learning, World-Wide-Web, online auctions, Radio Frequency Identification (RFID), e-portfolio systems, wireless LAN, E-government, Ecommerce, internet banking, and mobile learning. In this regard therefore, TAM is a model that can inform technology designers on the impact of the system to the user's

behavior. Alharbi and Steve supports that TAM has been adopted and tested as a useful framework in the field of information science and Learning Management Systems. Many others scholars such as Seyal et al. also attests that TAM is a sufficiently influential research model, whose tools have provided statistically reliable results. The survey consisted of diverse open-ended questions (developed on the Likert scale) to identify the factors that are hindering the adoption of IPv6 in Iraq. Diverse statistical techniques have been used to analyse the collected data, including descriptive, reliability crosstab, regression, and correlation analysis.

4.1 Demographics Analysis

As mentioned in the previous section, the survey was conducted on 153 IT professionals. The Tableabove discusses the age group of participants that answered the questions over the Google forms about the adoption of IPv6 over IPv4. The majority of the professionals belonged to the age between the years of 18 and 25, having a percentage of 54.9 per cent. The next largest frequency of the age group belonged to the professionals between the age group of 25 and 45, covered about a percentage of 39.9 per cent. The remaining two frequencies belonged to the professionals belonging to the age groups of 45 or more and professionals who belonged to the age of under 18, with a frequency percentage of 3.3 per cent and 2.0 per cent, respectively (see Table 4.1 and Figure 4.1).

Table 4.1 Age group

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	18 - 25	84	54.9	54.9	54.9
	25 - 45	61	39.9	39.9	94.8
	45 or more	5	3.3	3.3	98.0
	Under 18	3	2.0	2.0	100.0
	Total	153	100.0	100.0	

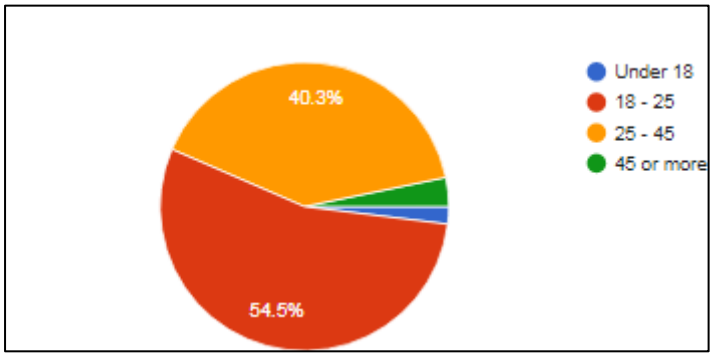

Figure 4.1 Age Group of Participants

For the sake of gaining diverse opinion about the factors that impact the transition of IPv4 to IPv6, the survey was conducted with 153 IT professionals. Among the respondents, 14.4 per cent were done with a bachelor degree. On the other hand, 41.2 per cent of the participants had done a higher diploma. The candidates having diploma covered about 24.8 per cent of the total audience. The professionals having Bachelors and Master's degree covered about 14.4 per cent of the total audience having a similar frequency. The audience consisted of 4 Ph.D. holders that made 2.6 per cent (see Table 4.2 and Figure 4.2).

Table 4.2 Education Level

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid		2	1.3	1.3	1.3
	Bachelor	22	14.4	14.4	15.7
	Diploma	38	24.8	24.8	40.5
	Higher Diploma	63	41.2	41.2	81.7
	Masters	22	14.4	14.4	96.1
	PHD	4	2.6	2.6	98.7
	uneducated	2	1.3	1.3	100.0
	Total	153	100.0	100.0	

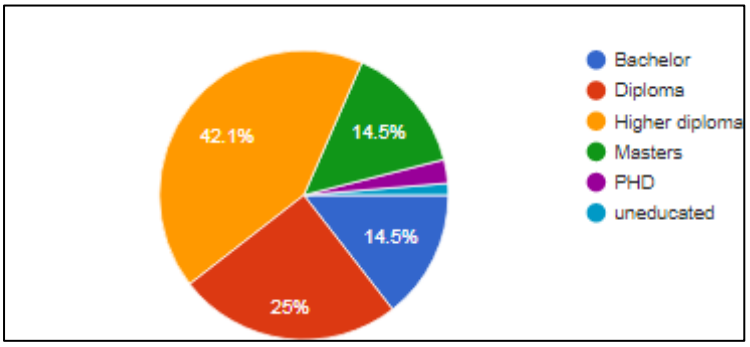

Figure 4.2 Education Level of Participants

The survey was conducted by IT professionals having different level of professional experiences. 47.7 per cent of the professionals had the experience of 3-5 years. The respondents who had less than 1 year of experience covered the second largest frequency covering about 19 per cent of the total respondents. The professionals having experience of more than 1 year and less than 3 years covered about 15 per cent of the total participants. The percentage of participants having experience between 5 to 10 years was 9.8 per cent. The minimum number of percentages belonged to the participants having more than 10 years of experience and no experience at all with 5.9 per cent and 0.7 per cent respectively (see Figure 4.3 and 4.4).

Table 4.3 Experience in Field

	Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	3	2.0	2.0	2.0
Less than 1 year	29	19.0	19.0	20.9
More than 1 year and less than 3 years	23	15.0	15.0	35.9
More than 10 years	9	5.9	5.9	41.8
More than 3 years and less than 5 years	73	47.7	47.7	89.5
More than 5 year and less than 10 years	15	9.8	9.8	99.3
No Experience in higher Education	1	.7	.7	100.0
Total	153	100.0	100.0	

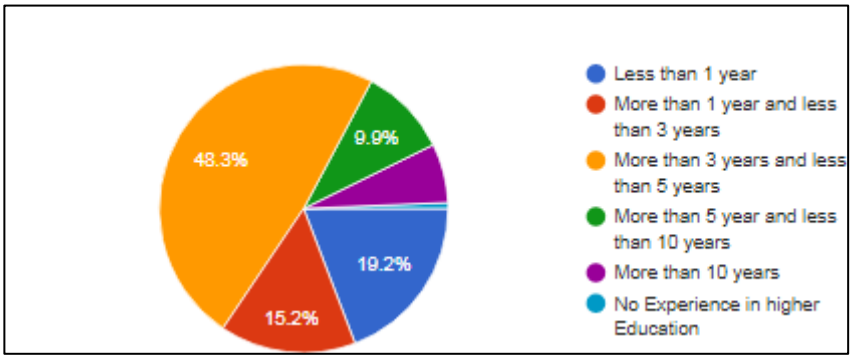

Figure 4.3 Experience in Field of Participants

The IT professionals involved in the survey consisted of people belonging to both genders. The male professionals covered about 71.9 per cent of the total number of participants, while female professionals covered about 28.1 per cent of the participants (see Table 4.4, Figure 4.4).

Table 4.4 Gender

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Female	43	28.1	28.1	28.1
	Male	110	71.9	71.9	100.0
	Total	153	100.0	100.0	

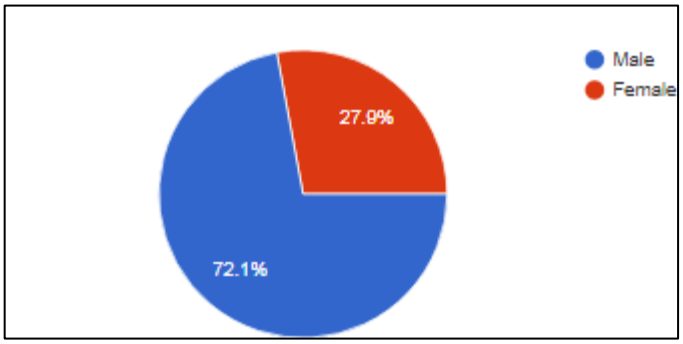

Figure 4.4 Gender

The respondents were basically IT professionals and since the survey was regarding IPv4 and IPv6, the researcher also needed to know the level experiences each individual had with the IPv4 and IPv6. The largest percentage of respondents belonged to the professionals who had 1 to 3 years of experience covering 52.9 per cent of the total participants. The participants having less than year experience with both of these technologies covered about 23.5 per cent while those who had 3 to 5 years of experience covered about 11.1 per cent of the total number of participants. The remaining participants consisted of individuals who never used a management system which covered about 6.5 per cent and the individuals having more than 5 years of experiences covered the minimum percentage of respondents of 3.3 per cent (see Table 4.5 and Figure 4.5).

Table 4.5 Experience with IP v4 and IP v6

	Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	4	2.6	2.6	2.6
1-3 years	81	52.9	52.9	55.6
3-5 years	17	11.1	11.1	66.7
Have not used a System Management System	10	6.5	6.5	73.2
Less than a year	36	23.5	23.5	96.7
More than 5 years	5	3.3	3.3	100.0
Total	153	100.0	100.0	

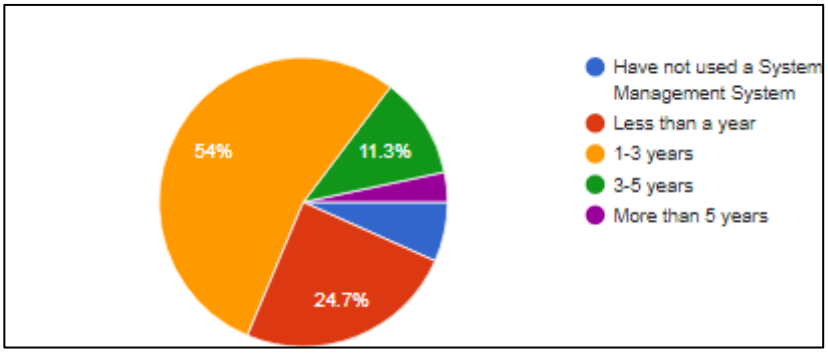

Figure 4.5 Experience of Participants

4.2 Descriptive Analysis

The respondents were asked whether the conversion from IPv4 to IPv6 can be time consuming and can affect the operations of the organization. According to a research, it was suggested that the transition can be a time-consuming process and can affect daily operations Çalışkan[5]. However, the respondents had varying responses with the highest amount of people disagreeing to the prospect with a percentage of about 39.9 per cent and 18.3 per cent of the respondents strongly disagreed to it. The next percentage of the respondents was 27.5 who had neutral views on the issue. While 7.8 per cent and 6.5 per cent agreed and strongly agreed that the conversion process will take time and eventually causing delay in the operations of the organisation (results are shown in Table 4.6, Figure 4.6).

Table 4.6 IPv4-IPv6 conversion is the time-taking process that ultimately affects the operations of the firms.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	28	18.3	18.3	18.3
	Disagree	61	39.9	39.9	58.2
	Neutral	42	27.5	27.5	85.6
	Agree	12	7.8	7.8	93.5
	Strongly Agree	10	6.5	6.5	100.0
	Total	153	100.0	100.0	

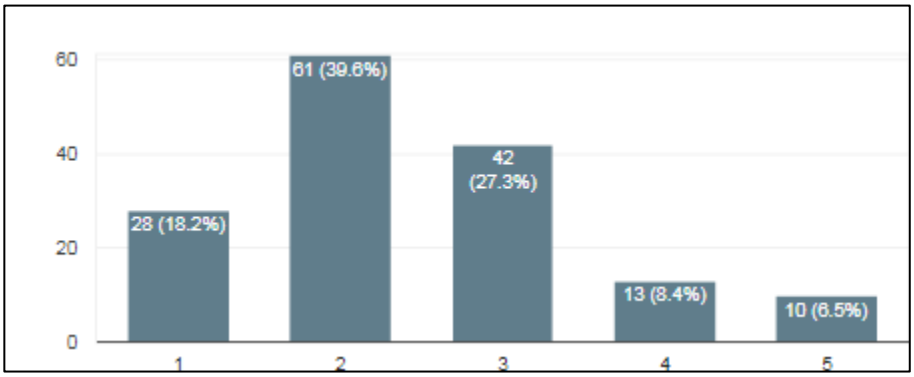

Figure 4.6 IPv4-IPv6 Conversion is the Time-taking Process

Organisations perceive IPv6 as an immature and unsTableas compared to IPv4 that ultimately hinders its adoption. When it was asked by the respondents, 19 per cent of them had shown strong agreement. The number of candidates having neutral response were around had the percentage of 29.4, while 13.1 per cent and 3.3 per cent of the total respondents agreed and strongly disagreed that IPv6 systems were immature to be executed. It shows that the perception of organisations towards the reliability of IPv6 is restricting its adoption in Iraq (see Table 4.7 and Figure 4.7).

Table 4.7 Since IPv6 is relatively new technology, it is quite immature and unsTableas compared to IPv4.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	29	19.0	19.1	19.1
	Disagree	53	34.6	34.9	53.9
	Neutral	45	29.4	29.6	83.6
	Agree	20	13.1	13.2	96.7
	Strongly Agree	5	3.3	3.3	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
	Total	153	100.0		

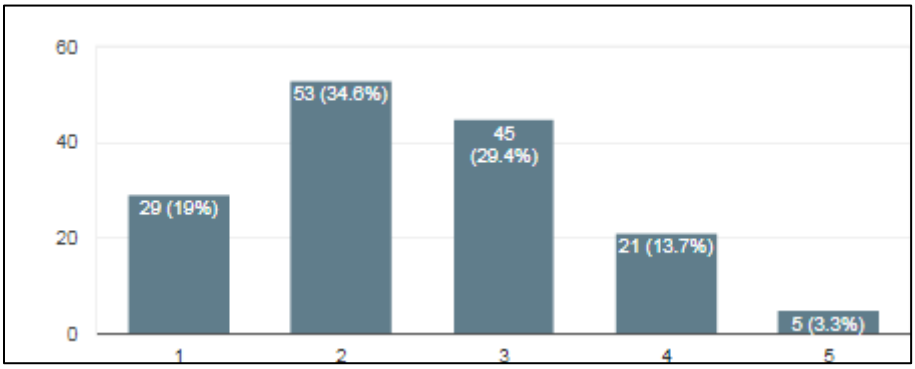

Figure 4.7 Immaturity and Instability of IPv6

When the respondents were asked if IPv6 systems had vague and unclear security mechanism and it is the reason for the hindrance its adoption, the majority of the respondents gave neutral perspective. Around 20.3 and 29.4 per cent of the respondents strongly disagreed to this prospect. Furthermore, around 12.4 per cent of the respondents agreed to this issue with the remaining 3.3 per cent of the respondents strongly agreed to the statement. It shows that Iraqi experts perceive IPv6 as the secured protocol, as compared to IPv4. These findings contradict the analysed literature. The results are shown in Table 4.8 and Figure 4.8.

Table 4.8 Vague and unclear security mechanism of IPv6 is also the biggest factor that is limiting the adoption of this internet protocol version

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	31	20.3	20.3	20.3
	Disagree	45	29.4	29.4	49.7
	Neutral	53	34.6	34.6	84.3
	Agree	19	12.4	12.4	96.7
	Strongly Agree	5	3.3	3.3	100.0
	Total	153	100.0	100.0	

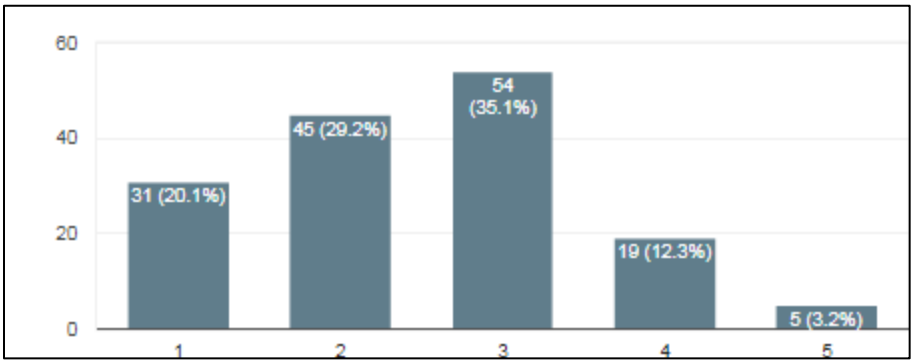

Figure 4.8 Vague and unclear security mechanism of IPv6 as a Limiting Factor

Reconnaissance attack was another main issue in the IPv4 systems, with the research conducted by Luntovsky and Spillner[22], which says that the reconnaissance and port scanning are the security threats that surround IPv4 systems. It was asked by the respondents, if it is the reason for the delay in IPv6 adoption, a large number of respondents having a percentage 44 per cent disagreed to the issue, while 13.7 per cent strongly disagreed to it. Around 35.3 per cent of participants had neutral answers and 13.7 per cent of the respondents agreed to the prospect. Only 7.8 per cent of the total respondents strongly agreed to the issue (see Table 4.9 and Figure 4.9).

Table 4.9 Though IPv6 has built-in IPsec mechanism, but the risk of reconnaissance attacks limits the organisations to adopt this version of internet protocol.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	21	13.7	13.8	13.8
	Disagree	44	28.8	28.9	42.8
	Neutral	54	35.3	35.5	78.3
	Agree	21	13.7	13.8	92.1
	Strongly Agree	12	7.8	7.9	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
Total		153	100.0		

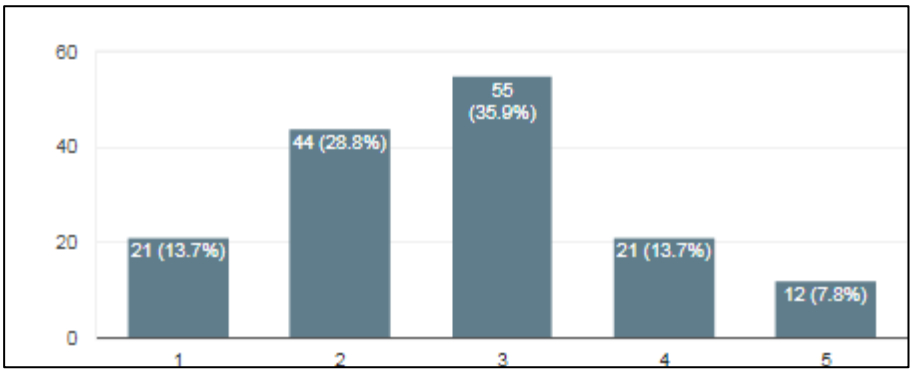

Figure 4.9 IPv6 and Reconnaissance Attacks

Transition from IPv4 to IPv6 consists of many operations such as tunnelling operations, IPv6 address mapping and efforts for dual stack management. These activities require many efforts and excessive amount of vigilance as suggested by Kaur[32], hence, they were asked whether the transition is worth the hassle or, they should just stick to IPv4. Majority of the responses were against the proposition, where 38.6 per cent disagreed to it and 21.6 strongly disagreed to it. The percentage of neutral responses was recorded 24.8 per cent, while 8.5 and 6.5 per cent respondents agreed and strongly agreed to the issue.

Table 4.10 Dual stack management efforts, tunnelling operations, and IPv6 address mapping are the prominent activities that need excessive vigilance during the transition from IPv4 to IPv6. Despite handling these hassles, it is better to continue using IPv4.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	33	21.6	21.6	21.6
	Disagree	59	38.6	38.6	60.1
	Neutral	38	24.8	24.8	85.0
	Agree	13	8.5	8.5	93.5
	Strongly Agree	10	6.5	6.5	100.0
	Total	153	100.0	100.0	

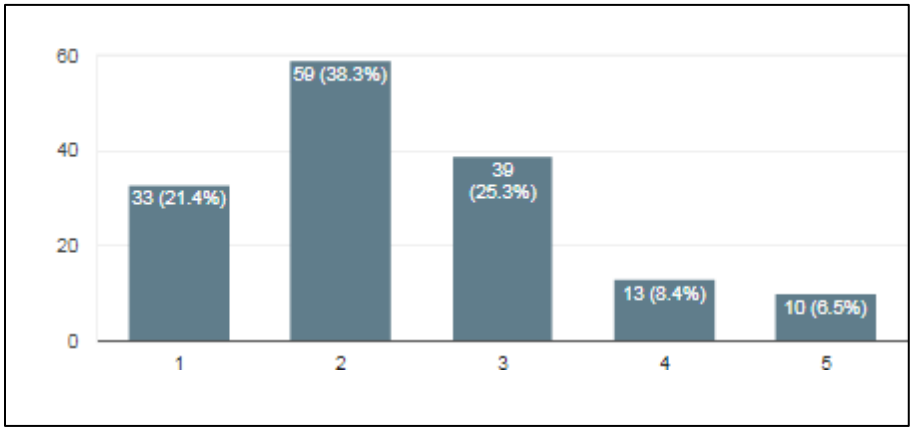

Figure 4.10 Excessive Vigilance Requirement

Among the different processes which are required for the transition from IPv4 to IPv6 systems, tunnelling is a time-consuming, but a necessary process. Tunnelling issues are also one of the reasons for the lack of IPv6 adoption in organizations. The respondents were asked whether they should use this process for transition or just stay with present IPv4 systems. The respondents had varying responses with 12.4 per cent and 34.6 per cent strongly disagreeing and disagreeing to the problem, while 38.6 per cent responded neutrally. 7.8 and 6.5 per cent shown agreement and strong agreement towards the statement.

Table 4.11 Tunnelling is a time-consuming process that limits the organisations to adopt IPv6 and continue their operations on IPv4.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	19	12.4	12.4	12.4
	Disagree	53	34.6	34.6	47.1
	Neutral	59	38.6	38.6	85.6
	Agree	12	7.8	7.8	93.5
	Strongly Agree	10	6.5	6.5	100.0
	Total	153	100.0	100.0	

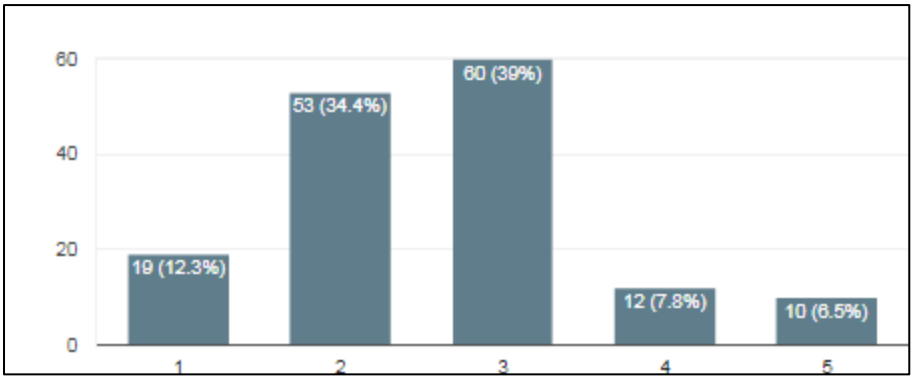

Figure 4.11 Tunnelling is a Time-Consuming Process

The advantages of IPv6 were vast and extensive as compared to IPv4, but its operations are difficult as compared to those of IPv4. In response to the statement 19.6 per cent of the respondents had shown strong disagreement. On the other hand, 7.8 per cent were strongly agreed. These findings are aligned with the ones, presented in the research of Çalışkan[5], that shows established that cautious handling of the operations is needed during the transition to IPv4 to IPv6. The issue was addressed with professionals with the majority of the responses against it, with a percentage of about 19.6 per cent and 27.5 per cent disagreeing and strongly disagreeing with it. However, 13.7 of the responses agreed to the prospect, while 7.8 per cent strongly agreed to it. 30.1 per cent of the total respondents stayed neutral on the issue (see Table 4.12 and Figure 4.12).

Table 4.12 IPv6 operations are not as simple as that of IPv4.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	30	19.6	19.9	19.9
	Disagree	42	27.5	27.8	47.7
	Neutral	46	30.1	30.5	78.1
	Agree	21	13.7	13.9	92.1
	Strongly Agree	12	7.8	7.9	100.0
	Total	151	98.7	100.0	
Missing	System	2	1.3		
Total		153	100.0		

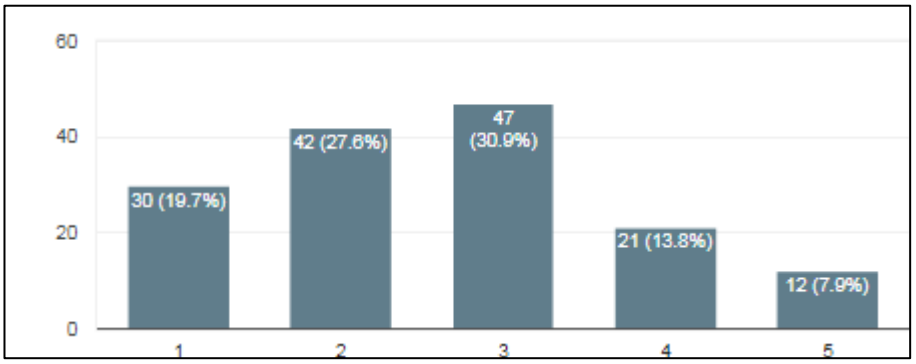

Figure 4.12 Complexity of IPv6 Operations

The operations of IPv6 are far more complex than IPv4 operations, therefore the IT personnel need to improve their skills on IPv4 operations so they can adapt quickly to the new technology, and this was asked to participants as well. The question was respond was raised because of the research conducted by Dey and Shilpa[31], who stated that the lack of skills of IPv6 technology limits the organizations in adopting the technology. Opposing to the research, around 17.6 per cent of the total participants strongly disagreed to the issue while 11.1 per cent strongly agreed to it. Around 32 per cent of the total respondents gave neutral responses, while 24.8 per cent and 13.7 per cent disagreed and agreed to the issue (see Table 4.13 and Figure 4.13).

Table 4.13 IT staff handling day-to-day operations on IPv4 is expected to improve and enhance their expertise and skills so as to easily handle the technical and quite complex operations of IPv6.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	27	17.6	17.8	17.8
	Disagree	38	24.8	25.0	42.8
	Neutral	49	32.0	32.2	75.0
	Agree	21	13.7	13.8	88.8
	Strongly Agree	17	11.1	11.2	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
	Total	153	100.0		

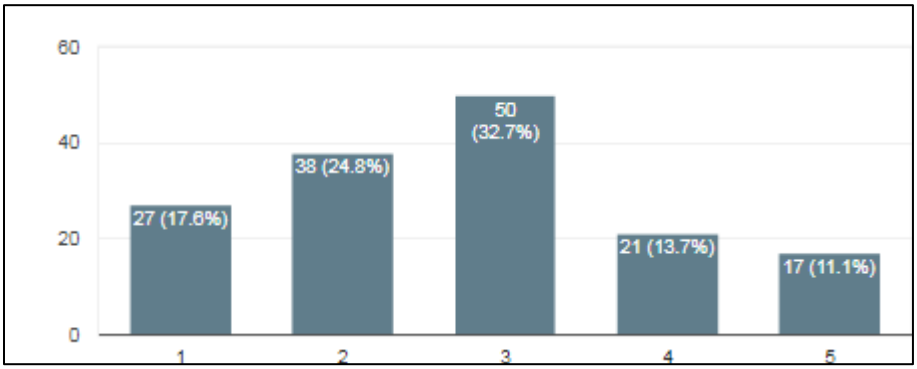

Figure 4.13 Requirement of High Skills and Expertise

Table 4.14 NAT, DHCP (dynamic host configuration protocol), and CIDP (classless inter- domain routing) are the good options, instead of completely shifting the operations to IPv6.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	25	16.3	16.4	16.4
	Disagree	52	34.0	34.2	50.7
	Neutral	42	27.5	27.6	78.3
	Agree	24	15.7	15.8	94.1
	Strongly Agree	9	5.9	5.9	100.0
	Total	152	99.3	100.0	
Missing	System	1	0.7		
	Total	153	100.0		

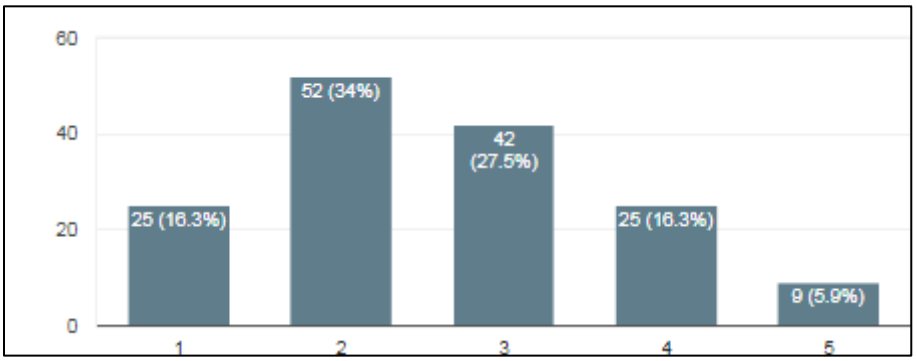

Figure 4.14 Bar chart of the above-mentioned responses

Shifting completely to IPv6 can be stopped by implementing NAT, DHCP and CIDP protocols to the IPv4 systems to improve the performances. These technologies are being adopted by organizations to improve the performances of IPv4 without the time-consuming aspect of the transition to IPv6, Mason and Mahindra[40], Che and Lewis[41]. The responses consisted of 34 per cent of the respondents disagreeing to the issue and 16.3 per cent strongly disagreeing to it. However, those who supported this issue consisted of 5.9 per cent strongly agreeing to it while 15.7 per cent agreed to it. The number of neutral respondents was around 27.5 per cent, which shows that a maximum number of respondents perceived that IPv6 does not require high cost, which is quite opposite to the literature findings.

Table 4.15 Transition from IPv4 to IPv6 requires high cost, specifically for the installation of switches, routers, etc. so it is better to continue operations on IPv4.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	32	20.9	21.1	21.1
	Disagree	50	32.7	32.9	53.9
	Neutral	42	27.5	27.6	81.6
	Agree	20	13.1	13.2	94.7
	Strongly Agree	8	5.2	5.3	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
Total		153	100.0		

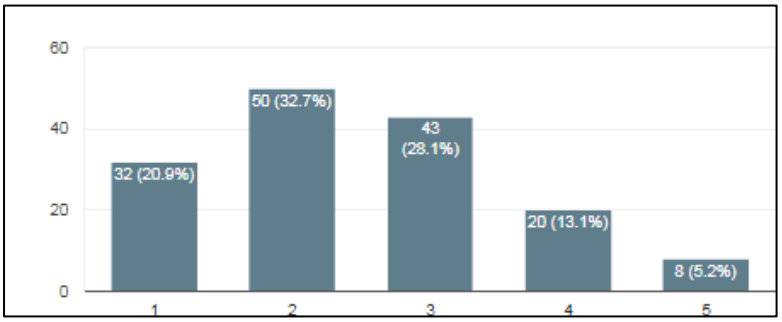

Figure 4.15 High Cost Required for IPv6

The transition from IPv4 to IPv6 is cost consuming especially with the installation IPv6 supported switches, routers, and other devices. Hovav and Popoviciu[37], suggested that cost is the biggest factor that hinders IPv6 transition. In contrast to the research, the question was asked to just avoid the cost bearing transition and continue operating on IPv4. Around 21.1 per cent and 32.0 per cent of the respondents strongly disagreed and disagreed to this outlook. Furthermore, there were supporters as well with around 13.1 per cent agreeing and 5.2 per cent of strongly agreeing to it, with 27.5 per cent of the respondents delivering neutral answers (see Table 4.16 and Figure 4.16).

Table 4.16 Lack of support from senior management is also limiting the adoption of IPv6.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	24	15.7	16.0	16.0
	Disagree	31	20.3	20.7	36.7
	Neutral	60	39.2	40.0	76.7
	Agree	24	15.7	16.0	92.7
	Strongly Agree	11	7.2	7.3	100.0
	Total	150	98.0	100.0	
Missing	System	3	2.0		
Total		153	100.0		

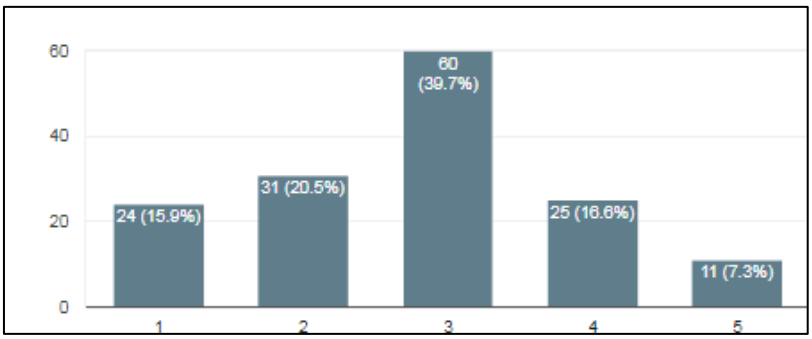

Figure 4.16 Lack of Support from Senior Management

The research suggested that there is always lack of support that when adopting new technologies. According to Kaur[32], senior management creates greater obstacles to the adoption of the IPv6 over IPv4. The respondents were asked about the reason, and around 39.2 per cent of the participants gave neutral responses while 15.7 per cent and 20.3 per cent of the respondents respectively strongly disagreed and disagreed with it. The responses go against the research, because of the disagreement factor involved. 15.7 per cent and 7.2 per cent of the total respondents shown agreement and strong.

Table 4.17 Lack of IPv6 skilled employees is restricting the organisations towards adopting this new internet protocol.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	26	17.0	17.1	17.1
	Disagree	36	23.5	23.7	40.8
	Neutral	53	34.6	34.9	75.7
	Agree	22	14.4	14.5	90.1
	Strongly Agree	15	9.8	9.9	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
Total		153	100.0		

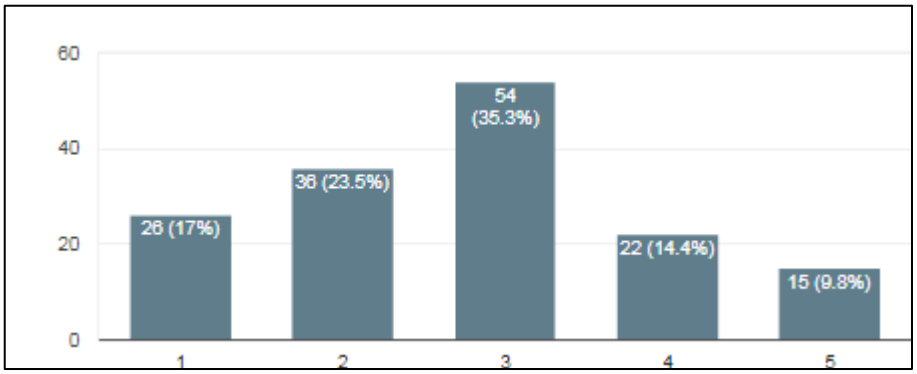

Figure 4.17 Lack of IPv6 Skilled Employees

Since IPv6 is a highly complex technology, necessary skills are required to operate it in an organizational structure. Hovav and Schuff[34], also suggested that skills of the employees are also a source of a major hindrance in adopting IPv6 technology and restrict them to IPv4 systems. The following prospect was asked in the survey, and the number of neutral respondents was around 34.6 per cent. Furthermore, around 14.4 and 9.8 per cent of the respondents moved towards agreement and strong agreement. However, the majority of the respondents were at disagreement with 17.0 per cent and 23.5 per cent giving disagreement and strongly disagreement responses.

Table 4.18 Organisations find it difficult to redesign technologies and protocols, like TCP/IP, ARP, BGP, RIP, OSPF, and DHCP. It ultimately restricts them to adopt IPv6.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	20	13.1	13.2	13.2
	Disagree	55	35.9	36.2	49.3
	Neutral	50	32.7	32.9	82.2
	Agree	19	12.4	12.5	94.7
	Strongly Agree	8	5.2	5.3	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
	Total	153	100.0		

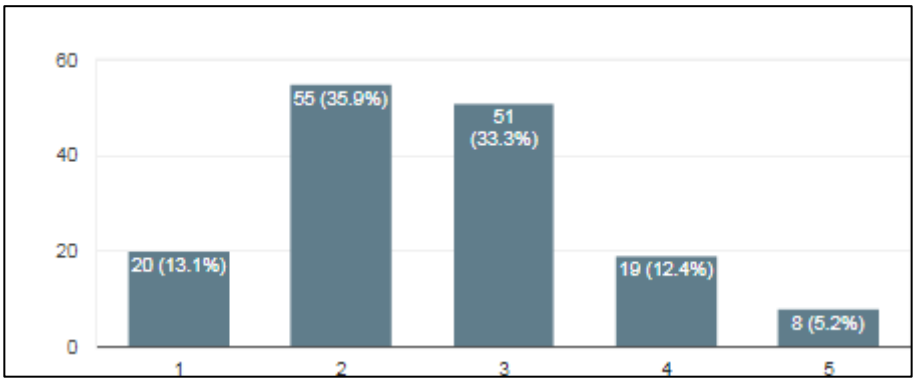

Figure 4.18 Organisations Finding Difficulty in Redesigning Technologies

IPv6 is a relatively new technology and it consists of new protocols and processes for implementing it. Babatunde and Al-Debagy[19], suggest that protocols such as TCP/IP, ARP, BGP etc. are needed to be redesigned which is one of the reasons that IPv6 is not implemented by many organizations. The respondents had opposing answers, with 35.9 per cent of the audience disagreed to the reason, and 13.1 per cent strongly disagreed with it. While 12.4 per cent of the respondents agreed to it; however, 32.7 per cent of the respondents stayed neutral to this. Furthermore, around 12.4 per cent of respondents agreed to it, while a minimum percentage of 5.2 per cent of respondents strongly agreed

to it.

Table 4.19 Organisations, belonging from specific cultures or countries tend to delay the adoption of IPv6, specifically the ones having the low inclination and knowledge about digital technologies.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	22	14.4	14.5	14.5
	Disagree	50	32.7	32.9	47.4
	Neutral	48	31.4	31.6	78.9
	Agree	17	11.1	11.2	90.1
	Strongly Agree	15	9.8	9.9	100.0
	Total	152	99.3	100.0	
Missing	System	1	.7		
Total		153	100.0		

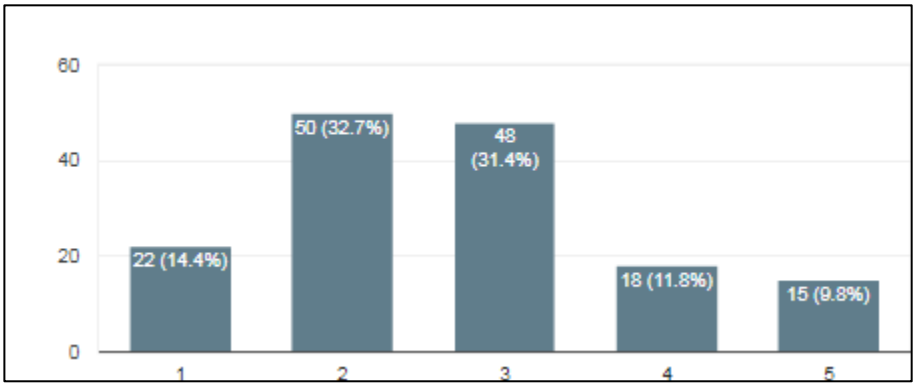

Figure 4.19 Cultural Aspects Hindering IPv6

Different cultures play an important role in any kind of organizational change, and Kaur[32], affirmed that the adoption of a digital change in organizational structure is largely affected by cultural indifference. Therefore, the question was asked whether the adoption is hindered by cultural indifference, and the responses largely contradict the relevant research with the respondents strongly disagreeing by 14.4 per cent and disagreeing to it by 32.7 per cent. On the other hand, the respondents also gave neutral answers to the prospect with the percentage of 31.4 per cent. The positive responses to the query were also made with respondents agreeing and strongly agreeing with 11.1 per

cent and 9.8 per cent respectively.

Table 4.20 It is better for the organisations, not to be an early adopter of IPv6.It is better to learn from the experience of other organisations.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	18	11.8	11.8	11.8
	Disagree	41	26.8	26.8	38.6
	Neutral	63	41.2	41.2	79.7
	Agree	16	10.5	10.5	90.2
	Strongly Agree	15	9.8	9.8	100.0
	Total	153	100.0	100.0	

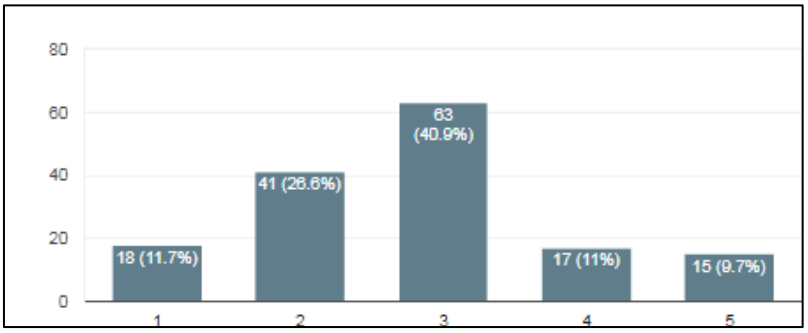

Figure 4.20 Early Adoption of IPv6

When adopting a new technological practice, it is necessary to evaluate the previous experiences and not be an early adopter as suggested by Dell and Liu[36]. The research suggests that organizations prefer learning for other organization's experience which also helps them to avoid potential risks. The responses oppose the relevant research and on asking the prospect, the respondents provided neutral answers with the probability of 41.2 per cent, while the 11.8 per cent and 26.8 per cent of the respondents strongly disagreed and merely disagreed to the prospect. However, around 10.5 per cent agreed to the issue and around 9.8 per cent strongly agreed to it. The acquired results are contradicting the findings, collected from the extensive literature. When adopting new

technology, the cost is a very important factor for any organization, and . Hovav and Popoviciu[37], suggests that one of the biggest barriers in adopting IPv6 is the cost that comes with training the individuals for IPv6 systems and therefore it is avoided by the many organizations. The survey discussed this issue, and the majority of the respondents gave neutral responses to the issue with a probability of 40.5 per cent. On the other hand, the around 11.1 per cent of the respondents strongly disagreed to it with 8.5 per cent of the respondents strongly agreeing to it. The responses also consist of 28.1 per cent of disagreement and 11.8 per cent of agreement about the relevant issue (see Table 4.21, Figure 4.21).

Table 4.21 It is better to save the cost, required for the training of the employees and continue operations on IPv4, instead of investing large amounts and switching to IPv6.

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Valid	Strongly Disagree	17	11.1	11.1	11.1
	Disagree	43	28.1	28.1	39.2
	Neutral	62	40.5	40.5	79.7
	Agree	18	11.8	11.8	91.5
	Strongly Agree	13	8.5	8.5	100.0
	Total	153	100.0	100.0	

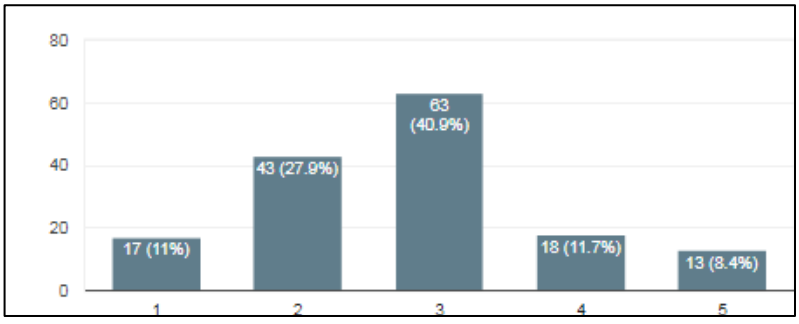

Figure 4.21 Cost Saving by Limited Investment on IPv4

The below Table (Table 4.22) is a comparison demographics chart between the educational qualification of the participants and their experience in the field of IPv6 technologies. The majority of the participants holding bachelor's degree had less than a year of experience in the field, while the there was a single participant who had experience between 3 to 5 years and two of them had 1 to 3 years of experience in the field. However, there were 6 individuals who did not even used system management system. On the other hand, the diploma holders who had 1 to 3 years of experience were 17 and 12 of them had experiences of less than 1 year. While 1 individual each had experience between 3 to 5 years and more than 5 years, while 4 of the diploma holders never even used management systems. There were vast numbers of higher diploma holders with a frequency of 63, with 49 of them ranging having 1 to 3 years of experience and 9 of them having 3 to 5 years of experience in the field of IPv6. 5 of them had experiences of less than a year with no individual who was not experienced with management systems. All master graduates were experienced some way with 11 of them having experiences of 1 to 3 years and 4 individuals each having experiences with 3 to 5 years and less than a year. There were 3 participants who also had more than 5 years of experiences. The candidates who were doctorate consisted of 2 of them having experiences between 1 to 3 years and 3 to 5 years, while 1 each uneducated personnel had experiences of 1 to 3 years and 3 to 5 years. The results have shown that individuals, having Master's Degree have higher exposure to IPv6.

Table 4.22 Education with Experience

Education Level	Experience with IP v4 and IP v6						
		1-3 years	3-5 years	Have not used a System Management System	Less than a year	More than 5 years	Total
	0	0	0	0	2	0	2
Bachelor	1	2	1	6	12	0	22
Diploma	3	17	1	4	12	1	38
Higher Diploma	0	49	9	0	5	0	63
Masters	0	11	4	0	4	3	22
PHD	0	2	2	0	0	0	4
Uneducated	0	0	0	0	1	1	2
Total	4	81	17	10	36	5	153

Second comparison Table (Table 4.23) is between the educational qualification and the age group their frequency belongs to among the participants. The participants of who had bachelor's degree mostly were between the age of 18-25 with 11 number of participants, 7 belonged between the age of 25-45 while 2 each were aged 45 or more or were under 18 years of age. The diploma holders were mostly between the age of 18 -25 and 25 – 45 comprising of 19 and 18 participants respectively, while one of them was under 18. The majority of the participants (40) who had higher diploma were between the age 18 – 25 and 22 of them belonged to the age 22 – 45, however only one participant was above the age of 45. 13 participants having master's degree were aged between 18 – 25 years and 9 of them were between the ages of 25-45 year. The doctorate degree holders were divided into 2 categories, where 3 of them were aged between 25-45 years; 1 of the participant was above 45 years. The two uneducated participants lie between the age of 25-45 and above 45.

Table 4.23 Education Level * Age group Crosstabulation

	Age group				Total
	18 - 25	25 – 45	45 or more	Under 18	
Education Level	1	1	0	0	2
Bachelor	11	7	2	2	22
Diploma	19	18	0	1	38
Higher diploma	40	22	1	0	63
Masters	13	9	0	0	22
PHD	0	3	1	0	4
uneducated	0	1	1	0	2
Total	84	61	5	3	153

4.3 Reliability Testing

Table 4.24 is a reliability analysis of the perceived usefulness factor that was introduced in the research. The reliability analysis has been conducted for all of the factors, involved in perceived usefulness with all other variables. For the perceived usefulness, the factor the Cronbach's alpha had a value of 0.673, which rounds off to 0.7. The value shows that the reliability of the four items, incorporated in a questionnaire.

Table 4.24 Reliability Statistics

Cronbach's Alpha	N of Items
.673	4

Table 4.25 consists of the reliability analysis of the factors involved in the perceived ease-of-use of the research. The reliability analysis showed the value of Cronbach's Alpha which is 0.768 for the consistency of 4 items involved in perceived ease-of-use. The Cronbach's alpha shows that the reliability of the four items is validated.

Table 4.25 Reliability Statistics

Cronbach's Alpha	N of Items
.768	4

The presented Table 4.26 is the reliability statistics of the conditions which fulfils the purpose of intention of use. The reliability analysis provided the value of Cronbach's Alpha, 0.715 for determining the consistency of the potential 4 items. The consistency was found reliable with the consistency value it delivered.

Table 4.26 Reliability Statistics

Cronbach's Alpha	N of Items
.715	4

Table 4.27 provided the reliability analysis of the usage behaviour by analysing their factors with the Cronbach's alpha value. The reliability statistics provided a Cronbach's value of 0.75, for the consistency of four items. The value proved that the items are highly reliable and highly consistent.

Table 4.27 Reliability Statistics

Cronbach's Alpha	N of Items
.750	4

4.4 Correlation Analysis

Table 4.28 Correlations

		PU	PE	IU	UB
PU	Pearson Correlation	1	.550**	.544**	.471**
	Sig. (2-tailed)		.000	.000	.000
	N	153	153	152	153
PE	Pearson Correlation	.550**	1	.476**	.466**
	Sig. (2-tailed)	.000		.000	.000
	N	153	153	152	153
IU	Pearson Correlation	.544**	.476**	1	.397**
	Sig. (2-tailed)	.000	.000		.000
	N	152	152	152	152
UB	Pearson Correlation	.471**	.466**	.397**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	153	153	152	153

**. Correlation is significant at the 0.01 level (2-tailed).

The correlation analysis provides the evaluation of an independent and dependent variable. There were four factors that were analysed in the research. Primarily, it was examined if they are correlated with one another having, and providing the identification of strong, moderate and weak relationship. The value was generated with the p-value of 0.01 (2- tailed) which showed the significance of each relationship, which was illustrated by two steric. The findings of the correlation analysis portrayed that the PU(Perceived usefulness) with PE(Perceived ease-of-use) and IU(Intention of use) had a strong relationship with the value above 0.5, while its relationship with UB(Usage Behaviour) was a moderate one with value lying between 0.4 and 0.5. Furthermore, the

relationship of between PE and IU had a moderate value while its relationship with UB was weak because of the value lying below 0.4. Moreover, the relationship between IU and UB was weak, with the value lying below0.4, while its relationship with others was moderate. It shows that the relationship between the dependent and independent variables is significant and positive.

4.5 Regression Analysis

The regression analysis is implemented in order to evaluate the impact of the independent variable with the dependent entity. The dependent variables in the Tables (4.29- 4.31) below are IU while independent variables are the other entities involved, i.e. PU and PE in the analysis. The regression was done on the basis of the significant value of 0.000, which clearly states that the independent variable has significant impact largely on the dependent one.

Table 4.29 Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.584[a]	.341	.332	.68393

a. Predictors: (Constant), PE, PU

Table 4.30 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	36.029	2	18.014	38.512	.000[b]
	Residual	69.696	149	.468		
	Total	105.724	151			

a. Dependent Variable: IU
b. Predictors: (Constant), PE, PU

Table 4.31 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.903	.208		4.351	.000
	PU	.444	.087	.405	5.087	.000
	PE	.244	.077	.254	3.188	.002

a. Dependent Variable: IU

The next regression analysis is executed by using UB as the dependent variable, whereas, IU and constant were defined as the dependent variable. The regression analysis also showed significant relationship between the dependent and independent variables.

Table 4.32 Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.397[a]	.158	.152	.75885

a. Predictors: (Constant), IU

Table 4.33 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	16.207	1	16.207	28.143	.000[b]
	Residual	86.379	150	.576		
	Total	102.586	151			

a. Dependent Variable: UB
b. Predictors: (Constant), IU

Table 4.34 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.676	.206		8.154	.000
	IU	.392	.074	.397	5.305	.000

a. Dependent Variable: UB

CHAPTER 5
RESULTS AND DISCUSSION

5.1 Conclusion

In this contemporary era, internet technology is considered as a global system for interconnected computing networks. This system accelerates the use of internet protocol suite (IP/TCP) which plays a commendable role in connecting several computing devices all over the world. In short, emerging internet technology has inevitably contributed to outstanding growth and evolution of digital devices in almost all the facets of life. IPv4 is known as the fourth version of internet protocol suite which is famous for routing internet traffic efficiently. It is a connectionless protocol and its application is based on packet-switched networks. IPv4 is serving the world of internet for fifty years. One cannot deny the fact that it has made ineviTablesuccess and growth in past twenty years. However, it was observed that this protocol was ineligible to handle the changing needs of the emerging internet. In 2011, IANA (Internet Assigned Numbers Authority) started facing exhaustion issue of IPv4 address pool. Moreover, it was anticipated in 2011 that all RIRs (Regional Internet Registries) will utilise the address space completely. The last IPv4 address block was given out by ICANN (Internet Corporation for Assigned Names and Numbers) in February 2011. In other words, it was anticipated that IPv4 capacity for internet address will be consumed completely. However, service providers considered a number of different mechanisms such as multi- layers network address translation (NAT). The main goal of this

mechanism is to save the address block from being depleted. In this regard, the most relevant approach to the exhaustion issue of address block was to switch to IPv6 from IPv4. In consideration of IPv4 ineligibilities, IPv6 gained ineviTablerecognition in the computing sectors and technology-oriented organisations. This is due to the enhanced features of IPv6 in terms of modified IP packets headers and addressing schemes. Irrespective of all these benefits, IPv6 adoption is still not approved fully by corporate world as many organisations prefer using IPv4 instead of IPv6. The reason behind this preference lies in the fact that IPv6 lacks in backward compatibility with previous protocol i.e. IpV4. This fact eventually limits the communication between IPv4 and IPv6 networks. The biggest issue, hindering the transition from IPv4 to IPv6 direct towards technical expertise to effectively manage IPv6 functions, limited knowledge, etc. Moreover, security is another issue as the security system currently used by IPv4 is not capable enough the security concerns of IPv6. Hackers have developed different malicious techniques and codes that cover the features of IPv6. It is acknowledged that security vulnerabilities and malicious codes can be identified easily during the testing phase. However, security experts avoid those activities as they consume a lot of time. Compatibility issues, the unwillingness of corporate sector for investing in infrastructure and employee training, lack of appropriate testing practices, and limited knowledge are the hindering factors that hamper the transition to IPv6 from IPv4. In this regard, the aim of this research study is to identify the features that pressurise people to stick to IPv4, irrespective of the IPv6 development. In order to establish a cohesive understanding of the factors, hindering Ipv4 to Ipv6 transition, following objectives were formulated in the research. The objectives were: To examine the functions and characteristics of IPv4; To analysis the functions and characteristics of IPv6; To understand the need for a transition from IPv4 to IPv6; To recognise the security threats

that are posed to IPv4 and IPv6; To assess the factors that are hindering the adoption or assimilation of IPv6; To deploy TAM (technology acceptance model) for determining the adoption of IPv6 in Iraq; To make recommendations to the IT experts of Iraq to ensure a smooth transition from IPv4 to IPv6. For the sake of ensuring the successful acquisition of research aim and objectives, quantitative research method was adopted. The survey was conducted with 153 IT professionals that work in Iraqi corporate sector. Other than this, literature was also reviewed as a secondary source to develop an understanding of concepts regarding present research work. The blended data source including primary and data source played a crucial role in the successful achievement of above-mentioned objectives. The acquired findings have revealed that transition or migration to IPv6 from IPv4 has been started; however, the adoption rate is way too slow due to a number of different factors that are hampering the entire transition process. The factors hindering the adoption of IPv6 direct towards security issues, tunnelling issues, financial issues, and infrastructure issues. In this regard, a number of protocols and technologies are required to support the adoption of IPv6. The most needed technologies are DHCP, OSPF, RIP, BGP, ARP, and IP/TCP. On the other hand, the paper revealed tunnelling issues as the major issues in the transition of IPv6. It was observed by the literature discussed in the paper that modified internet protocols in the pre-existing network can be utilised easily with the help of tunnelling technique without a transformation in the applications. However, the process of tunnelling consumes a lot of time its throughput is limited which makes the process unattractive to acquire. In addition to it, the paper also revealed the fact that additional financial resources are required for the purpose of transition which is another hindering factor. According to the discussed literature, the transition to IPv6 from IPv4 needs the enterprises and companies to invest the capital cost for employee training, switches, and

routers that are causing difficulty for them to switch to IPv6 from IPv4. In addition to it, it was highlighted by the paper that the limited testing practices lead towards lack of information, unclear, and vague security mechanism which is considered as another factor that restricts the corporate sector and enterprises to switch to IPv6 from IPv4. While discussing hindering factors, the paper discussed a number of reasons that hamper the adoption of IPv6 in which the biggest issue direct towards over-reliance of corporate world on workaround technologies.

5.2 Future Work

The size of the organisations and the complexity of IPv6 is something which cannot be denied in the transition of IPv4 to IPv6. In recognition of this, it was observed that large company avoid switching to IPv6. This is due to the fact that during the transition, they will have to replace a large number of applications and equipment. On the other hand, the small companies, due to the lack of financial resources and funding avoid IPv6 assimilation. In other words, Cost is said to be the biggest hindering factor in the adoption and assimilation of IPv6. In addition to the issues of IPv6 adoption, the reluctance of organisation is another factor that restricts them from adopting IPv6 as they want to learn from the experience of other companies who have switched to IPv6 in order to avoid associated risks and challenges. Additionally, perceived security threats and immaturity of IPv6 is another hurdle in the way of transition of IPv4 as the mutual thought of many organisation direct towards the fact that this technology is a threat to the security; thereby, making it unattractive to adopt. The wrong perceptions of the organisations, regarding IPv6 is also counted as an obstacle for IPv6 as some of the companies criticise that it is an unsTableand immature technology. Considering skills and capabilities, lack of skilled employees and expertise of IPv6 is also restricting the firms to go for IPv6 as it would be difficult for them to manage its technical operation.

As many organisations are not willing to adopt this technology, there are no positive experiences which can encourage the firms to adopt it. Considering the perspective of Iraqi corporate sector, limited management capabilities and technological awareness are the main factors that hamper the adoption of IPv6. It is acknowledged that cautious handling of this technology is required while adopting IPv6. In this regard, the organisations need to invest for the sake of successful implementation of IPv6, employee training, recruitment of skilled individuals, and development of transition plans. Most importantly, management support, skill development, and employee training are the prominent factors that are needed the most in the entire transition process of IPv6 in Iraq.

REFERENCES

[1] Shah, H., (2013). Comparing TCP-IPv4/TCP-IPv6 Network Performance. University of Missouri-Columbia.

[2] Sharma, P. and Singla, R. M. (2016). "A Detail Comparative Review on IPv4/IPv6 Dual Stack Co-existence Techniques". International Journal of Innovative Research in Computer and Communication Engineering.

[3] Durdağı, E. and Buldu, A., (2010). "IPV4/IPV6 security and threat comparisons", Procedia- Social and Behavioral Sciences, 2: 5285-5291.

[4] Akamai (2017) IPv6Adoption Visualisation Akamai. Retrieved from, https://www.akamai.com/uk/en/about/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp.

[5] Çalışkan, E., (2014). "IPv6 transition and security threat report. NATO CCD COE, Tallinn.

[6] Bernard, H.R. and Bernard, H.R., (2012). Social research methods: Qualitative and quantitative approaches, Sage.

[7] Bilski, T., (2011). "From IPv4 to IPv6–data security in the transition phase". In Proc. 7th Int. Conf. Netw. Serv, ICNS (2011) : 66-72.

[8] Aluko, T.S., Olusanya, O.J., Oloyede, O.E. and Ebisin, A.F., (2014). "Comparative Analysis between Internet Protocol Version 4 & 6 (IPv4 and IPv6)". International Journal of Scientific & Engineering Research, 10:278-291.

[9] Abdullahi, G. A. and Mahadevan, V. (2010). Why is IPv4 still in Existence?. School of Information Science, Computer and Electrical Engineering Halmstad University, http://www.div portal.se/smash/get/diva2:380776/FULLTEXT01.pdf, 10 Nov 2018.

[10] Kozierok, C.M., (2005). The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. No Starch Press.

[11] Bons, E. and Weigand, H., (2011). IPv6: "Drivers and Barriers for Adopting.

Department of Information Management", Tilburg University.

[12] Bi, J., Wu, J. and Leng, X., (2007). "IPv4/IPv6 transition technologies and univer6 architecture. International Journal of Computer Science and Network Security", 7(1) : 232-243.

[13] Hanumanthappa, J., (2009). "IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model": A Case Study for University of Mysore Network. arXiv preprint arXiv, 0908-0548.

[14] Hanumanthappa, J. and Manjaiah, D.H., (2008). "A Study on Comparison and Contrast between IPv6 and IPv4 Feature Sets".

[15] Tavakoli Momtaz, M. and Swanson, M., (2015). "IPv4 to IPv6 Transition and Security".

[16] Johansson, E., (2016). "Evaluation of prerequisites for an IPv4 to IPv6 transition".

[17] Yadav, A., Abad, P., Shah, H. and Kaul, A., (2012). "IPv6 protocol adoption in the US: Why is it so slow?". Capstone paper, University of Colorado, May, 4.

[18] AbuAli, A.N., Shayeb, I.G., Batiha, K. and Aliudos, H.Y., (2010). "The Benefits of Using Internet Protocol Version 6(IPV6)". International Review on Computers and Software, 5(6) : 583-587.

[19] Babatunde, O. and Al-Debagy, O., (2014). "A comparative review of internet protocol version 4 (ipv4) and internet protocol version 6 (ipv6)". arXiv preprint arXiv, 1407-2717.

[20] Durdağı, E. and Buldu, A., (2010). "IPV4/IPV6 security and threat comparisons. Procedia- Social and Behavioral Sciences", 2(2),: 5285-5291.

[21] Wieringa, F., de Laat, C. and Visser, M.R., (2012). "IPV6 risks and vulnerabilities Project Report".

[22] Luntovskyy, A. and Spillner, J., (2017). "Security in Distributed Systems. In Architectural Transformations in Network Services and Distributed Systems" Springer Fachmedien Wiesbaden, 247-308.

[23] Sotillo, S., (2006). "Ipv6 security issues. Scanning".

[24] Shah, J. and Parvez, J., (2015). "Security Issues in Next Generation IP and Migration Networks". IOSR Journal of Computer Engineering, 17(1), : 13-18.

[25] Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A. and Weippl, E.R., (2014), August. "IPv6 Security: Attacks and Countermeasures in a Nutshell". In WOOT.

[26] Choudhary, A.R., (2009), November. "In-depth analysis of IPv6 security posture". In Collaborative Computing: Networking, Applications and Worksharing,

(2009). CollaborateCom , 5th International Conference 254.

[27] Sabir, M.R., Fahiem, M.A. and Mian, M.S., (2009). "An overview of IPv4 to IPv6 transition and security issues", In Communications and Mobile Computing, 3 – 5 Oct 2006, Baghdad.

[28] Dawood, H., (2012). "IPv6 security vulnerabilities". International Journal of Information Security Science, 1(4) : 100-105.

[29] Hovav, A. and Schuff, D., (2005). "Global Diffusion of the Internet V-The Changing Dynamic of the Internet: Early and Late Adopters of the IPv6 Standard". Communications of the Association for Information Systems, 15(1) : 14-14.

[30] Ahmed, M.M., (2006). "A Comperative Study on the Performance of IPv4 and IPv6". Independent University, Bangladesh.

[31] Dey, S. and Shilpa, N. (2011). "Issues in IPv4 to IPv6 Migration", International Journal of Computer Applications in Engineering Sciences (IJCAES,. 1 (1).

[32] Kaur, A., (2015). How is digital infrastructure adopted and assimilated?, The IPv6 story,Ph.D Thesis, Auckland University of Technology, Basrah.

[33] Grossetete, P., Popoviciu, C.P. and Wettling, F., (2004). Global IPv6 strategies: from business analysis to operational planning. Cisco Press.

[34] Hovav, A. and Schuff, D., (2005). "Global Diffusion of the Internet V-The Changing Dynamic of the Internet" : Early and Late Adopters of the IPv6 Standard. Communications of the Association for Information Systems, 15(1) : 14.

[35] Dell, P., (2010). "Two economic perspectives on the IPv6 transition". info, 12(4) : 3-14.

[36] Dell, P., Kwong, C. and Liu, Y., (2008). "Some reflections on IPv6 adoption in Australia". info, 10(3) : 3-9.

[37] Hovav, A. and Popoviciu, C., (2009). "Adoption leadership and early planners": Comcast's IP upgrade strategy, Communications of the ACM, 52(7): 143-146.

[38] Gallaher, M.P. and Rowe, B.R., (2006). "The costs and benefits of transferring technology infrastructures underlying complex standards: the case of IPv6". The Journal of Technology Transfer, 31(5), : 519-544.

[39] White, G.L., Shah, J.R. and Cook, J.R., (2005). Internet Technology in (2010): "The Issue of IPv6 Adoption in the USA". Journal of International Technology and Information Management, 14(3) : 5.

[40] Mason, A. and Mahindra, T., (2011). "Report for IDA: IPv6 Adoption Guide for Singapore". Minoli, D. and Kouns, J., (2016). Security in an IPv6 environment.

CRC Press. Oki, E., Rojas-Cessa, R. and Vogt, C., (2012). Advanced internet protocols, services, and applications. John Wiley & Sons.

[41] Che, X. and Lewis, D., (2010). "Ipv6: current deployment and migration status". International Journal of Research and Reviews in Computer Science (IJRRCS), 1(2): 22-29.

[42] Khudhair, H. E. and Mohammed, J. I.(2017). "A Prototype and Roadmap for Transition to IPv6 with Performance Evaluation". Research Journal of Applied Sciences, Engineering and Technology, 14(8): 299-309.

[43] Dhall, H., Dhall, D., Batra, S. and Rani, P., (2012), January. Implementation of IPSec protocol. "In Advanced Computing & Communication Technologies" (ACCT), Second International Conference, 176.

[44] Stallings, W., (2011). "Cryptography and network security: principles and practices". Pearson Education India.

[45] Malik, R. and Syal, R., (2010). "Performance analysis of IP security VPN". International Journal of Computer Applications, 8(4) : 6.

[46] Sharma, G., (2014). "Implementation of IPv6". Rovaniemi University Of Applied Sciences School Of Technology, 19 : 31-32.

[47] Sameeha, M.A.A., (2012). "Look at IPV6 Security advantages over IPV4". Network and Complex Systems, ISSN, : 34-35.

[48] Kocak, C. and Zaim, K., (2017), "Performance measurement of IP networks using Two- Way Active Measurement Protocol". In Information Technology (ICIT), 8th International Conference, 249.

[49] Soumyalatha, N., Ambhati, R.K. and Kounte, M.R., (2013), August. Performance evaluation of ip wireless networks using two-way active measurement protocol. "In Advances in Computing, Communications and Informatics" (ICACCI), International Conference, 1896.

[50] Bäckström, I., (2009). "Performance measurement of IP networks using the two-way active measurement protocol". Skolan för datavetenskap och kommunikation, Kungliga Tekniska högskolan.

[51] The Technology Acceptance Model (TAM) and its "Application to the Utilization of Mobile Learning Technologies" . David Gitumu Mugo1*, Kageni Njagi2, Bernard Chemwei2 and Jared Ochwagi Motanya1. British Journal of Mathematics & Computer Science 20(4): 1-8, (2017); Article no.BJMCS.29015. ISSN: 2231-0851.

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname : Ahmed A. Radif AL-KHAFAJI

Date of birth and place : 11.07.1982 , Iraq

Foreign Languages : English , Turkish

E-mail : aradeef14@gmail.com

EDUCATION

Degree	Department	University	Date of Graduation
Master			
Undergraduate	Computer Sciences	Almansoor University College	2006
High School	Secondary education	Central Preparatory School	2001

PUBLISHMENTS

Papers

1. Alkhafajı, A. R. and Balık, H. H. (2018). “A Comparative study in Ipv4 and Ipv6”, ISSN : 2320-5407.