I. J. Computer Network and Information Security, **2020, 5, 31-45**
Published Online October 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.05.03

Analyzing the IPv6 Deployment Process in Palestine

Yazan W. Abdalaziz
Arab American University Department of Computer Science, Jenin - Palestine P.O Box 240 Jenin, 13 Zababdeh, Palestine
E-mail: yazan_d.k@hotmail.com

Ala Hamarsheh
Arab American University Department of Computer Information Technology, Jenin - Palestine P.O Box 240 Jenin, 13 Zababdeh, Palestine
E-mail: ala.hamarsheh@aaup.edu

Received: 05 May 2020; Accepted: 24 June 2020; Published: 08 October 2020

Abstract: This paper is to examine the IPv6 in Palestine and to examine where are Palestinian companies in the deployment process. Also, to examine if the infrastructure can withstand the transition to IPv6 or not. This study used quantitative research methods and collect the data through a survey from the Internet companies in Palestine as reported anonymously. Due to the lack of research related to the internet in Palestine, we saw that it is necessary to discover the internet companies and how much they achieved of the deployment process. The collected data have been analyzed and described using SPSS. The data analysis showed that one internet company representing 11% of the companies in Palestine did apply the transition process to IPv6, and the percentages have set a positive indicator for the transition process. It turns out that the other companies on their way to start deploying the IPv6.

Index Terms: IPv6, IPv6 in Palestine, IPv6 Transition Mechanisms, Internet in Palestine, Migrating to IPv6.

1. Introduction

We can imagine the number of Internet users and the speed with which they are growing. In addition, evolution and spread of mobile phones led to facilitate the process of connecting to the internet. That's mean increase of the devices and the users connecting the Internet. The most widely used protocol is IPv4 [1]. The majority of the devices and Internet users are still relaying on it to connect to the Internet. Due to the growth of the Internet and connected devices, the IPv4 address pool has been exhausted.

On 15 April 2011 the Asia-Pacific Network Information Center (APNIC) declared that it has reached the last /8 block of available IPv4 addresses [2]. Due to the consumption of the IPv4, the Internet Engineering Task Force (IETF) has proposed a new version of Internet protocol (IPv6) [3] to alleviate with the problem of IPv4 address exhaustion. The IPv6 is the most recent version of the internet protocol. It uses 128 binary bits to create a single unique address on the network [4]. It became a draft standard in December 1998 and became an internet standard on 14 July 2017 [3]. IPv4 uses 32-bit addresses which offer approximately 4.3 billion addresses, but IPv6 can provide more than 7.9×1028 times as many as IPv4.

At the time the IPv4 addresses are completely expired, the Internet Service Providers (ISPs) will not be able to face the problem with supply their customers with new IP addresses, knowing that the existing addresses are still assigned to the connected devices. The best solution is to start deploying the IPv6 and replace the IPv4 with it. However, no one can be certain that the implementation of IPv6 will be widespread without the IPv4 being depleted. The consideration of applying the transition from IPv4 to IPv6 is important now. Sum of ISPs and organizations have deployed IPv6 across their networks like the federal government in the US, and a handful of commercial companies such as Bechtel and Google [5].

So, why has it taken so long for IPv6 to be implemented?

The reasons behind the delay in implementing the IPv6 is easy to understand. First, it is too expensive. There are plenty of devices such as servers, routers, and switches which designed to work with IPv4. Upgrading or changing all this infrastructure takes a lot of efforts and it would be very expensive. The second reason is that the changing and the upgrading is the responsibility of the user as well as the providers. So, the provider would think of deploying the IPv6 as a bad investment if its clients didn't upgrade their devices or asked for this service. In addition, the biggest

beneficiary of this process is the provider doesn't gain anything from it and in most cases the users don't realize the benefit that they may gain from this process. So, no one can force all the internet users to deploy the IPv6.

The biggest mistake in developing the IPv6 is that it does not have the ability to backward compatibility with IPv4. That's mean IPv4 hosts and routers will not be able to deal with the traffic of IPv6 and vice versa. However, the IETF has proposed a set of mechanisms that support compatibility between IPv4 and IPv6 which are based on implementing IPv4 along-side with IPv6 to help smooth and fully transition to IPv6 [6]. These mechanisms can be categorized into: dual-stack network [21], tunnelling [10], and protocol translation [5].

While the internet companies and ISPs in the whole world are trying to deploy the transition to IPv6, the Palestinian companies are left unknown. In addition to the lack of research in this field particularly in Palestine, there is no sign of them trying to start the process or even offer the IPv6 to their customers. There are many solutions to this problem such as measuring the infrastructure and applying a survey on the customers or the ISPs. The best solution is to apply the survey on the ISPs because through the ISPs the authors can determine everything needed. The main limitation of this study is that if not all the ISPs agreed to reveal their information, we won't be able to get the overall picture of the internet companies in Palestine.

The purpose of this study is to measure the IPv6 in Palestine and to study the development of the IPv6 in the Palestinian companies. As well as studying the infrastructure and the extent of its readiness for IPv6 implementation. The major objectives of this study are to gain an understanding of the environment by examining the internet companies which did start the deployment process and to address the problems of which the other companies didn't start yet. Also, to drove the attention of the ISPs who didn't start the deployment process and what is the importance of them starting the process. That will be done by examining the user demand, the infrastructure, and the future plans that the Internet companies implement for the future.

This study was conducted to 7 internet companies out of 9 companies in Palestine. The companies who approved to participate in the study had to fill up a questionnaire. With the lack of quantitative researches related to this topic particularly in Palestine, this study aimed to provide a description of the data and measurements related to the Internet in Palestine and the extent of the development reached by most Palestinian companies.

The following questions is the questions that guided this research and this research intent is to answer it. (a) what customer demand and require? (b) is there an infrastructure that capable of sustaining the transition process to the IPv6 and what technologies the ISPs offered? (c) did the ISPs apply the transition to IPv6, if so, what percentage of customer demand services needed the transition to IPv6. And if they didn't apply the transition to IPv6, have they made plans for the transition process?

2. Material and Methods

With the rapid growth of internet users which has led to a shortage of the IPv4 addresses, many techniques and protocols were proposed to prolong the life expectancy of the IPv4 addresses. Also, many techniques and protocols were proposed to facilitate the transition to IPv6 and to start the process of smooth transition. In this section, we will present a literature review about the IPv4 exhaustion and best of IPv6. In Addition, the reasons that prevent the transition process to IPv6. Finally, we will provide a review of the mechanisms and techniques that help with starting a smooth transition to IPv6.

2.1. IPv4 Exhaustion

The internet service providers (ISPs) acquired their IP address from a Local Internet registry (LIR), National Internet Registry (NIR), or Regional Internet Registry (RIR). There are five RIRs specializing in supply the ISPs with the IP addresses. Each RIR operates in a specific area, dividing the world into five regions. The five RIRs are the African Network Information Center (AFRINIC), the American Registry for Internet Numbers (ARIN), the Asia Pacific Network Information Center (APNIC), the Latin America and Caribbean Network Information Center (LACNIC), the Réseaux IP Européens Network Coordination Centre (RIPE NCC), As describe in [2] the expectations of exhaustion dates of IPv4 in each RIR are:

- AFRINIC's projected exhaustion date of IPv4 addresses is late in 2019.
- APNIC's projected exhaustion date of IPv4 addresses is the middle of 2021.
- RIPE NCC's projected exhaustion date of IPv4 addresses is the middle of 2020.
- LACNIC's projected exhaustion date of IPv4 addresses is late in 2019.
- ARIN's IPv4 address pool is already exhausted.

APNIC's unassigned address pool is 3.9 million addresses marked as available. Knowing that APNIC using addresses from last/8 framework since April 2011. The remaining address pool is not all the addresses available in the RIRs. Apparently, according to the RIR's policies each RIR has reserved some addresses. For example, APNIC has 4.4 million addresses marked as reserved. See [8] for more details.

2.2. Best of IPv6

The IPv6 was designed as the successor protocol to the IPv4. IPv6 uses 128 binary bits to create a single unique address on the network to support more levels of the addressing hierarchy. One of the differences that the IPv6 overcome the IPv4 is that the IPv6 header has been facilitated to contain the necessary information that is needed. Also, working to support the extensions and options allows for more efficient forwarding, limitation with less stringent along options, and more flexibility to offer new options in the future. Also, not to forget to mention the flow labeling capabilities and the authentication capabilities [4].

There are many other Advantages that IPv6 overcomes IPv4 with. This section will present some of these advantages.

- **Address:** IPv6 is 128-bit address, which means that generate more than 7.9×1028 times as many as IPv4. So, IPv6 has more capacity to store the data than IPv4 has.
- **Address configuration**: There is no need for the configuration when using IPv6. it is automatically configured [12].
- **Packet fragmentation**: In IPv6 protocol, the routers and intermediate nodes can't fragment the packet. The packet can be fragmented by the source node. The intermediate nodes and end nodes must know how to handle the fragmented packets properly.
- **Packet header**: IPv6 header contains flow labeling field to help the source to identify packets needs a QoS handling. Also, IPv4 header contains options field up to 40 bytes, but in IPv6 protocol, the extinction headers used instead of the options field.
- **Type of addresses**: IPv6 protocol has three types of addresses. First, the unicast address. This address is to identify a single host or a single interface. The second address is the anycast address. This type of addresses is assigned to more than one single interface. When a packet sent to an anycast address, it will be delivered to the most nearly interface that the address is assigned to it. The third type is the multicast address. This type of addresses is assigned to a set of interfaces. When a packet sent to a multicast address, it will be delivered to every node that had been assigned to that address. Also, the broadcast function is provided by the multicast address in IPv6 protocol.

2.3. Reasons Prevent the IPv6 Deployment

As shown in the previous sections IPv4 and IPv6 are not backward compatible. That means the two protocols can't work with each other. IETF has proposed many mechanisms to solve this particular problem by starting the deployment of the IPv6 along-side with IPv4 until it reaches the full deployment of IPv6. We will present these mechanisms in the next section.

There are other reasons that may affect the transition process. It can be categorized into two reasons End User, and Service Provider Network [5].

A. End User

The end user is an important part of the transition process. It may not be done without user approval. To achieve the transition, there are some considerations must be taken into account. Such as host configuration and users' application. With the start of the smooth transition process, the IPv6 users will increase. With the existence of the IPv4 legacy applications, the communication process between IPv4 application and IPv6 application will form a big problem. Therefore, there are some upgrades have to be implemented so that the smooth transition is done. These upgrades must be done on the IP stack, Transmission Control Protocol TCP, and User Datagram Protocol UDP in addition to the users' legacy application so that it can communicate with the IPv6 applications. Also, the end users may not have the needed knowledge to do the needed host configuration. So, the host configuration must be done automatically and transparent to the end user [20].

There are many mechanisms were proposed to translate between IPv4 and IPv6 that support the incompatibility between the host's connectivity and the running applications. These mechanisms are Bump-In-the-Stack (BIS) [14], Bump-In-the-API (BIA) [15], Bump-In-the-Host (BIH) [16], and Decoupling Application IPv4/IPv6 Operation from the Underlying IPv4/IPv6 Communication (DACS) [23].

B. Service Provider Network

The service provider network is an important factor that directly affects the process of the transition to IPv6. The ISPs wouldn't consider the transition easily for business reasons. The transition to IPv6 needs to upgrade the infrastructure to be able to withstand the deployment of IPv6, which can be very expensive to them in the absence of the users' request to the particular service.

IETF has proposed a mechanism to start deploying IPv6 on IPv4 infrastructure to help the service providers to start the process. This mechanism is IPv6 Rapid Deployment on IPv4 Infrastructure (6rd) [24].

6rd is a mechanism by which the IPv6 packets can be transmitted over the IPv4 infrastructure. To help the ISPs to

start rapidly deploy IPv6 without the over-cost of upgrading the infrastructure. The 6rd mechanism is built over the 6to4 [13] mechanism. Like 6to4 mechanism 6rd use the stateless IPv6 in IPv4 encapsulation in order to transmit IPv6 packets over the IPv4 infrastructure. In contrast to 6to4, 6rd uses its own IPv6 prefix instead of the fixed 6to4 prefix. That's mean the ISPs can deploy their own prefix. The 6rd operational domain is restricted on the ISPs network. The tunnels are created between the 6rd gateway (ISP border relay) and the customer edge CE. See [24, 25].

There are many limitations that may prevent the ISPs from start deploying IPv6 using 6rd. These limitations are the 6rd mechanism needs upgrading and changing of the CEs, which may expense the deployment process. After the upgrading and changing process, 6rd needs configuration on the CEs. In addition to the firewall blocking of the tunneled 6rd packets and there are still few CEs that support 6rd. finally, 6rd doesn't support more than one level of DHCPv4 between the border router and the customer edge.

There are many mechanisms proposed to overcome the 6rd limitations. Such as Deploying IPv6 Service Across Local IPv4 Access Network (D6across4) [26, 27], Configuring hosts to Auto-detect (IPv6, IPv6-in-IPv4, or IPv4) network connectivity (CHANC) [28, 29], and Deploying IPv4-only Connectivity across Local IPv6-only Access Networks (D4across6) [11]. These mechanisms are not in the scope of this research.

2.4. Transition Mechanisms

In view of the current situation of the IPv4 exhaustion, the transition to IPv6 is inevitable now. On account of the big size of the internet users, the Internet Engineering Task Force (IETF) has proposed transition techniques to support a smooth transition to IPv6 because of the difficulty of deploying IPv6 on all internet users. The transition mechanisms are to simplify the connectivity between networks using the same IP address or a different one. These mechanisms can be categorized into Dual Stack network, tunneling, and protocol translation. In this section, we will present an overview of each one of these mechanisms.

A. Dual-Stack

A mechanism in which all of the nodes are both IPv4/IPv6 enabled, which mean that in every networking device, router, firewall, switch and server are configured with both IPv4 and IPv6 connectivity capabilities. That gives the ability to the IPv4/IPv6 nodes to send and receive IPv4 and IPv6 packets. Because of the ability to support both IPv4 and IPv6, the nodes must be configured with both IPv4 address to dial with IPv4 packets received, and IPv6 address to dial with IPv6 packets received. IPv4/IPv6 nodes use (DHCPv4/DHCPv6) to gain IPv4 and IPv6 addresses [7] [21].

Domain Name System (DNS) is a mechanism used to map between IP addresses and hostnames. This mechanism used in both IPv4 and IPv6 addresses. Dual stack has the ability to deal with both IPv4 and IPv6 addresses, so the nodes must have the ability to deal with IPv4 "A" records and IPv6 "AAAA" records.

The IPv4/IPv6 nodes contain resolver libraries that capable of handling "A" and "AAAA" resolutions. The applications on dual-stack have the ability to specify wither IP to use IPv4, IPv6 or both [5].

B. Tunneling

Is another approach to allow networks/hosts that use the same IP protocol and separated by a network that use another IP protocol to communicate with each other wither the network/hosts using IPv4 or IPv6. For example, tunneling IPv6 packets throw an IPv4 network. The IPv4/IPv6 hosts and routers can tunnel the IPv6 packets and carry them in the IPv4 network by encapsulating them within IPv4 packets [10, 7].

As described in [7] tunneling can be implemented in several ways:

- **Router to Router:** IPv4/IPv6 router can send and receive packets throw an IPv4 network between each other.
- **Router to Host:** IPv4/IPv6 Router can tunnel the packets to their final destination IPv4/IPv6 hosts.
- **Host to Router:** IPv4/IPv6 hosts can tunnel packets to a middle IPv4/IPv6 Router that can be reached by an IPv4 network.
- **Host to Host:** IPv4/IPv6 host that is connected to an IPv4 network can tunnel the packets to another IPv4/IPv6 host which is connected to the IPv4 network.

There are two types of tunneling: Static Tunnels and automatic tunnels.

a. Static Tunnels

Static Tunnels Tunneling technique is an encapsulation of the IPv4/IPv6 packets that have been sent throw an IPv4 network between tunnel endpoints. In static tunneling, the address configuration is manually configured at the tunnel endpoint. That's mean that the IPv6 packet which is encapsulated in an IPv4 packet and the destination address in the IPv4 header is the address of the end-point of the tunnel. In each tunnel, the encapsulating node stores the tunnel end-point. the process of determining which packets to the tunnel is done by the routing information in the encapsulating node. Also, determining the destination for this packet after it has been tunneled is done by using the prefix mask and match technique [6].

b. Automatic Tunnels

Automatic Tunnels: Unlike static tunneling, automatic tunneling is point-to-multipoint. The address configuration is automatically determined from the packet being tunneled. The tunnel endpoint address will be extracted from the destination address of the IPv6 packet. Which must be an IPv4 compatible address. The IPv4/IPv6 nodes have the ability to determine if the packet is auto-tunneled or not. That's to be done by using the IPv6 routing table using the implementation of the prefix (0:0:0:0:0:0/96). All packets that match this prefix are sent using automatic tunneling.

Types of tunneling are described at more length in [6].

C. Translation

Translation approach is a mechanism used when IPvX-only host/network trying to communicate with IPvY-only host/network. In the tunneling and dual IP layer approaches the communication was between two IPv6-only networks/hosts and the problem of transport an IPv6 packet throw an IPv4 network has been resolved. Still, the problem when an IPv4 node needs to communicate with an IPv6 node. The previous approaches will not resolve this problem. Translation mechanism allows any IP to communicate with the other IP regardless of its version. In this approach, the translation of the header is needed when an incompatibility between the current host's connectivity and the running application is found. Also, translating the header led to translating the IP address inside the header to determine the real address [5].

Translation approach can be categorized into host-based protocol and network-based protocol.

a. Host-Based

To activate the old application and make them accessible to the end-users without concern to the type of the current connectivity. host-based translators provide the connectivity between the running applications and the hosts if there is an incompatibility between the application type and the current host connectivity. the connection is between incompatible types is obtained throw translation to provide the ability to IPvX-only applications to communicate with IPvY-only applications. the changeover occurs in the application layer and the IP communication layers of incompatible types of protocols. no need for converting the address capabilities of the application.

Examples of Host-Based protocols are Bump-In-the-Stack (BIS) [14], Bump-In-the API (BIA) [15], and Bump-In-the-Host (BIH) [16].

- **Bump-In-the-Stack (BIS):** As described in [14] Dual stack hosts using bump-in-the-stack technique is an example of a network layer translator. it is inserted between the TCP/IPv4 module and network card driver module. the hosts act as translators. the inserted module translates the IPv4 to IPv6 from the data flow between the TCP/IP and the network card driver using the SIIT algorithm. also, users do not need to determine if the target hosts are IPv4 or IPv6. the assignment process of the IP address is carried out using the DNS.
- **Bump-In-the API (BIA):** Such as BIS technique Dual stack hosts using Bump-In-the-API is a technique to allow IPv4-only application that runs on dual-stack hosts to communicate with IPv6-only hosts without modifying the applications. A BIA translator is inserted between the API module and the TCP/IP module. With the BIA technique there is no need for IP header translation. It translates the IPv4 socket API functions to IPv6 socket API functions. BIA technique can be categorized into three components: function mapper, name resolver, and address mapper. See [15] for more details.
- **Bump-In-the-Host (BIH):** Dual stack host using Bump-In-the-Host [16] is the merger of the BIS technique and the BIA technique. BIA and BIS techniques can work only with dual-stack networks but, the main goal of BIH technique to allow IPv4 legacy applications to communicate with IPv6-only networks or dual IPv4/IPv6 networks by synthesizing IPv4 address from "AAAA" records. There are two implementations in BIH technique: a protocol translator which is implemented between the TCP/IPv4 module and the IPv6 stacks and an API translator which is inserted between the API module and TCP/IP module. In both implementations, IPv4 is translated to IPv6. IPv4 socket API functions translated to IPv6 API functions if the BIH is implemented in the socket API layer, and IPv4 packets will be translated to IPv6 packets using SIIT algorithm if the BIH is implemented in the network layer.

b. Network-Based

In this section, we describe mechanisms to translation between heterogonies networks such as Stateless IP/ICMP Translation (SIIT) [19], and Stateful network address translation from IPv6 clients to IPv4 servers (NAT64) [22].

- **Stateless IP/ICMP Translation (SIIT):** IP/ICMP translation algorithm is an algorithm to provide the interoperation between IPv4-only nodes and IPv6-only nodes. SIIT algorithm is the replacement for the Network Address Translation-Protocol Translation (NAT-PT). the algorithm intent to provide a full translation between IPv4 and IPv6 headers and between ICMPv4 and ICMPv6 headers. IP/ICMP translators located between the IPv4 network domain and the IPv6 network domain. the translation of the headers in the SIIT

algorithm does not contain translating of IPv4 options, or IPv6 extensions.

- **Stateful Network Address and Protocol Translation from IPv4 Clients to IPv6 Server (NAT64):** Stateful Network Address and Protocol Translation from IPv4 Clients to IPv6 Servers (NAT64) is a mechanism to allow communication between IPv6-only clients and IPv4-only servers. As in DNS64 [18], NAT64 allows peer-to-peer communication between IPv4 and IPv6 nodes. Using IP/ICMP algorithm [17], the NAT64 mechanism translates the IPv4 headers to IPv6 headers and vice versa. NAT64 is located in the ISP border network between the IPv4 network and the IPv6 network. The NAT64 is assigned an IPv6 prefix to represent the IPv4 addresses in the IPv6 networks for the translation process. In addition, Network Address Port Translation (NAPT) [9] is used to map between IPv4 and IPv6 addresses.

3. Data Analysis

The transition from IPv4 to IPv6 is important now and we have been discussed the three important factors that will affect the process of the transition. The three factors are First, the customers' demand and the customers' readiness to accept the transition process and whether the customers will accept the fact that the process may cost them extra money and did they have the knowledge about the fact that there is no benefit to them. Second, the service provider network and the network readiness for the deployment. Third, the infrastructure development and the technology which can be provided within the infrastructure [5].

The purpose of this study was to examine the transition to IPv6 in Palestine, where is Palestine in the deployment process, and examine the three factors that affect the transition directly. The ISPs companies in Palestine were part of this study as a sample of the population that the authors intent to study. Questioning the ISPs companies is helpful because through these companies the transition will be realized and the three factors can be studied and analyzed.

This section begins with an overview of the analysis of the quantitative data collected from 78% of the population which has been studied. 78% of the population is the 7 Internet companies which approved to participate in this study. The overview of the analysis will include the descriptive tables to present the answers from these companies. The result of the ISPs responses to examine each of the following research question (a) what customer demand and require? (b) is there an infrastructure that capable of sustaining the transition process to the IPv6 and what technologies the ISPs offered? (c) did the ISPs apply the transition to IPv6, if so, what percentage of customer demand services needed the transition to IPv6 and if they didn't apply the transition to IPv6, have they made plans for the transition process?

This study used Google forms to publish the survey online. The data were collected by sending emails to internet companies to fill up the survey online. Seven companies out of nine in Palestine approved to answer the survey and participate in the study. The data were analyzed using SPSS software. Descriptive Tables and frequency tables were generated using SPSS to present and discuss the data.

The next section will present a summary of the data findings as they related to the research questions.

3.1. Customers' Demands

At this part of the analysis, there are 9 questions related to the customers' demand. These questions intend to examine the customer's needs, and requirements. Each company answered the questions about their customers for us to determine the customers' demands. Also, to determine if the customers require IPv6 or not. Table 1. is the descriptive table of the first 9 questions. In these questions the respondents were given four intervals of percentage to answer with (0%-24%, 25%-49%, 50%-74%, 75%-100%). Also, the table shows the mean of the responses to each question.

As it can be observed from Table1., six participants, representing 85.7% of the responding companies, reported (75%-100%) of their private customers use one IPv4 address, and one participant, representing 14.3% of the responding companies, reported (50%-74%) of their private customers use IPv4 address. With the mean 3.86 which means that 96.5% of the private customers in Palestine use one IPv4 address.

Three participants, representing 42.9% of the responding companies, reported (0%-24%) of their corporate customers use block of IPv4 address, and one participant, representing 14.3% of the responding companies, reported (50%-74%) of their corporate customers use block of IPv4 address, and three participants, representing 42.9% of the responding companies, reported (75%-100%) of their corporate customers use bloke of IPv4 address. With the mean 2.57 which means that 64.2% of the corporate customers in Palestine use one IPv4 address.

One participant, representing 14.3% of the responding companies, reported (25%-49%) of their customers use the CPE that they supply, and four participants, representing 57.1% of the responding companies, reported (50%-74%) of their customers use the CPE that they supply, and one participant, representing 14.3% of the responding companies, reported (75%-100%) of their customers use the CPE that they supply. With the mean 3.14 which means that 73.5% of the customers in Palestine use the CPE that the ISP supply.

Five participants, representing 71.4% of the responding companies, reported (0%-24%) of their customers who require multihoming, and two participants, representing 28.6% of the responding companies, reported (25%-49%) of the customers who require multihoming. With the mean 1.29 which means that 32.2% of the customers in Palestine who require multihoming.

The fifth question asked the participant about the percentage of the corporate or private customers who request for

the IPv6. All the seven participants, representing 100% of the responding companies, reported (0%-24%) of their customers who request for the IPv6. With the mean 1.00 which means that less than 25% of the corporate or private customers in Palestine who request for the IPv6.

The sixth question asked the participant about the percentage of the customers who currently use IPv6. All the participants, representing 100% of the responding companies, reported (0%-24%) of their customers who currently use IPv6. With the mean 1.00 which means that less than 25% of the customers in Palestine who currently use IPv6.

The seventh question asked the participant about the percentage of the customers who is IPv6-only customers. All the participants, representing 100% of the responding companies, reported (0%-24%) of their customers who IPv6-only customers. With the mean 1.00 which means that less than 25% of the customers in Palestine who is IPv6-only customers.

The percentage of customers who refused to consider IPv6. Five companies, representing 71.4% of the responding companies, reported (0%-24%) of the customer who refused to consider IPv6, and one company, representing 14.3% of the responding companies, reported (25%-49%) of the customer refused to consider IPv6, and one company, representing 14.3% of the responding companies, reported (75%-100%) of the customer refused to consider IPv6. With the mean 1.57 which means that 39.2% of the customer in Palestine refused to consider IPv6.

For the next 10 years, what is the percentage of the customers who will still depend on the IPv4-only application. Two companies, representing 28.6% of the responding companies, reported (0%-24%) of the customers expected to still depend on IPv4-only applications, and two companies, representing 28.6% of the responding companies, reported (25%-49%) of the customers expected to still depend on IPv4-only applications, and Two companies, representing 28.6% of the responding companies, reported (50%-74%) of the customers expected to still depend on IPv4-only applications. and one company, representing 14.3% of the responding companies, reported (75%-100%) of the customers expected to still depend on IPv4-only applications. With the mean 1.57 which means that 39.2% of the customer in Palestine refused to consider IPv6. With the mean 2.29 which means that 57.2% of the customer in Palestine expected to still depend on IPv4-only applications.

Table 1. Customers' Demands

		0%-24%	25%-49%	50%-74%	75%-100%	Mean	Percentage
The % of the private customers who use one IPv4 address.	Count	0	0	1	6		
	% of responses	0.0%	0.0%	14.3%	85.7%	3.86	96.5%
The % of the corporate customers who use a block of IPv4 addresses.	Count	3	0	1	3		
	% of responses	42.9%	0.0%	14.3%	42.9%	2.57	64.2%
The % of the customers who use the CPE that ISPs supply.	Count	0	1	4	2		
	% of responses	0.0%	14.3%	57.1%	28.6%	3.14	78.5%
The % of customers who require multihoming.	Count	5	2	0	0		
	% of responses	71.4%	28.6%	0.0%	0.0%	1.29	32.2%
The % the of the big customers (private/corporate) who request IPv6.	Count	7	0	0	0		
	% of responses	100.0%	0.0%	0.0%	0.0%	1.00	25%
What % of the customers currently use IPv6.	Count	7	0	0	0		
	% of responses	100.0%	0.0%	0.0%	0.0%	1.00	25%
The % of the customers who is IPv6-only customer.	Count	7	0	0	0		
	% of responses	100.0%	0.0%	0.0%	0.0%	1.00	25%
The % of the customers who refused to consider IPv6.	Count	5	1	0	1		
	% of responses	71.4%	14.3%	0.0%	14.3%	1.57	39.2%
For the next 10 years, the % of the customer who will still depends on IPv4-only application.	Count	2	2	2	1		
	% of responses	28.6%	28.6%	28.6%	14.3%	2.29	57.2%

Table 2. ISPs' Infrastructure

	NO		YES	
	Count	% of responses	Count	% of responses
Companies would consider using A+P (Address-Plus-Port) or LSN (Large Scale NAT) techniques to prolong the IPv4 address space.	4	57.1%	3	42.9%
Companies supply CPE which is pure IPv6 enabled.	4	57.1%	3	42.9%
Can the equipment that the companies support be field-upgraded to support IPv6.	7	100.0%	0	0.0%
The companies that did upgrade the DNS to support "AAAA" resolutions.	3	42.9%	4	57.1%
The companies that their SMTP, POP3 and IMAP services are dual-stack, and dual-connectivity.	5	71.4%	2	28.6%
The companies that their HTTP services, including caching and webmail, are dual-stack and dual-connectivity.	5	71.4%	2	28.6%
The companies that did provide LSN (Large Scale NAT) to their customer.	2	28.6%	5	71.4%
The companies that have functions between the heterogonies networks.	5	71.4%	2	28.6%

3.2. Infrastructure Readiness

The second research question asks if there is an infrastructure capable of sustaining the transition process, and what technology the ISPs offered. The participants were asked to answer some questions related to this research question. These questions intend to examine the infrastructure and to check if the infrastructure is able to withstand the transition process. Also, to find out what are the technologies that the companies offer, and what access methods that they apply.

A. ISPs Infrastructure

Respondents answered two types of questions related to this research question. First YES/NO questions related to the first part of the research question with scale: YES = 2 and NO = 1. The next part is consisting of a few multiple-choice questions related to the second part of the research question.

To examine the research question 2, a descriptive analysis in SPSS was used to describe the answers see in Table 2.

The participants were asked if they would consider using A+P (Address Plus Port) or LSN (Large Scale NAT) to prolong the IPv4 address space. Four participants, representing 57.1% of the responding companies, answered No, they wouldn't consider A+P or LSN, and three participants, representing 42.9% of the responding companies, answered Yes, they would consider A+P or LSN.

Four participants, representing 57.1% of the responding companies, answered No, the CPE that they supply is not pure IPv6 enabled, and three participants, representing 42.9% of the responding companies, answered Yes, the CPE that they supply is pure IPv6 enabled.

The participants were asked about the equipment that they support if it can be field upgraded or not. All the seven participants, representing 100% of the responding companies, answered No, the equipment that they support can't be field upgraded.

Three participants, representing 42.9% of the responding companies, reported that they didn't upgrade the DNS to support "AAAA" resolution, and four participants, representing 57.1% of the responding companies, reported that the did upgrade the DNS to support "AAAA" resolution.

Five participants, representing 71.4% of the responding companies, reported that their SMTP, POP3, IMAP, and HTTP services, including caching and webmail, are not dual-stack and dual-connectivity. Two participants, representing 28.6% of the responding companies, reported that their SMTP, POP3, IMAP, and HTTP services, including caching and webmail, are dual-stack and dual-connectivity.

Two participants, representing 28.6% of the responding companies, reported that they didn't provide LSN to their customers, and five participants, representing 71.4% of the responding companies that they did provide LSN to their customers.

Five participants, representing 71.4% of the responding companies, reported that they don't have functions between the heterogonies networks, and tow participants, representing 28.6% of the responding companies that they have functions between heterogonies networks.

Table 2. describe that 35.7% of the companies in Palestine would consider using A+P or LSN to prolong the IPv4 address space. 35.7% of the customer in Palestine actually use the CPE that their companies supply. Less than 25% of the equipment that the companies supply can be field-upgraded. 39.2% of the companies did upgrade the DNS to support "AAAA" resolutions. 32.2% of the companies in Palestine their SMTP, POP3, IMAP, and HTTP services, including caching and webmail, are dual-stack and dual-connectivity. 42.7% of the companies in Palestine did provide

LSN to their customers. 32.2% of the companies in Palestine have functions between heterogonies networks.

B. The Provided Technologies

The second part of this research question is to examine the infrastructure and to check if the infrastructure is able to withstand the transition process, examine the technologies that they offered, and access methods that they apply.

Fig. 1. describes the access technologies that the companies offered. The participants were given five choices: Wireless Broadband, Fiber Optic, Broadband Over Powerline, Cable (Coaxial Cable), Dial-up, and ADSL. Sex participants, representing 85.7% of the responding companies, reported that they offer Wireless Broadband and Fiber Optic. Two participants, representing 28.6% of the responding companies, reported that they offer Broadband Over Powerline and Cable (Coaxial Cable). One Participant, representing 14.3% of the responding companies, reported that he offers Dial-up. And all the seven participants, representing 100% of the responding companies, reported that they offer ADSL.

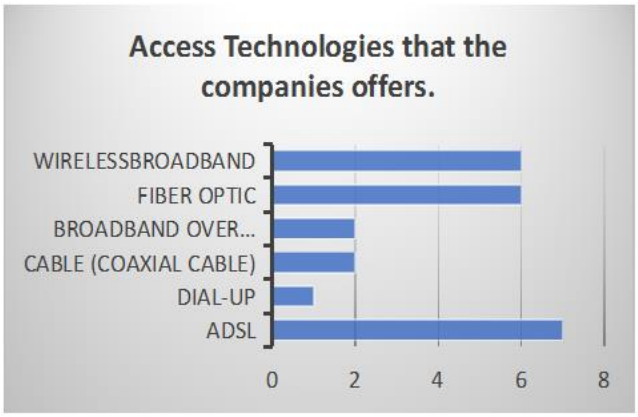

Fig.1. Access Technologies

Fig. 2. describes the IPv6 access methods that the companies apply. The participants were given sex choices: Tunnel Broker, Teredo Server, 6to4 Relay, Separate IPv4 and IPv6 Backbone, Dual-stack Routing Backbone, and nothing. Five participants, representing 71.4% of the responding companies, reported that they apply Dual-stack Routing Backbone. Two participants, representing 28.6% of the responding companies, reported that they didn't apply any IPv6 access technologies.

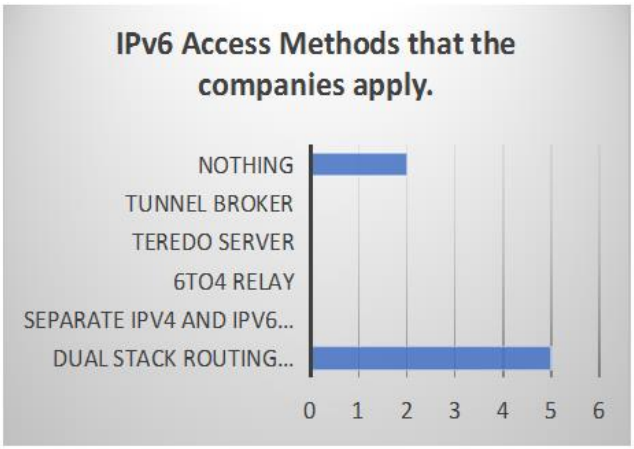

Fig.2. Access Methods

Fig. 3. describes the equipment on the companies' networks that don't support IPv6. The participants were given five choices: Switches, Servers, Firewalls, Routers, and nothing. One participant, representing 14.3% of the responding companies, reported that the switches in their network don't support IPv6. Two participants, representing 28.6% of the responding companies, reported that the servers in their network don't support IPv6. Two participants, representing 28.6% of the responding companies, reported that the routers in their network don't support IPv6. Five participants, representing 71.4% of the responding companies, reported that none of the equipment in their network don't support IPv6.

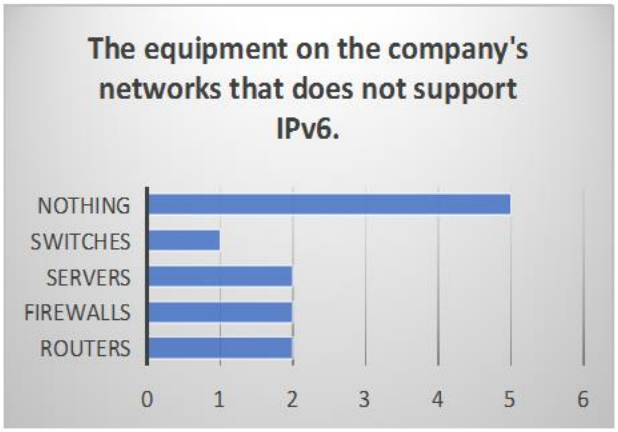

Fig.3. The Equipment that does not support IPv6

Fig. 4. describes which software in the companies is dual-stack. The participants were given seven choices: Aggregated router with upstream, Network management tools, Monitoring software, Accounting software, Address management software, Intrusion detection, and Firewalls. One participant, representing 14.3% of the responding companies, reported that Aggregated router with upstream is Dual-stack. Three participants, representing 42.9% of the responding companies, reported that Network management tools are dual-stack. Three participants, representing 42.9% of the responding companies, reported that monitoring software is dual-stack. One participant, representing 14.3% of the responding companies, reported that accounting software is dual-stack. One participant, representing 14.3% of the responding companies, reported that Address management software is dual-stack. One participant, representing 14.3% of the responding companies, reported that intrusion detection is dual-stack. sex participants, representing 85.7% of the responding companies, reported that Firewalls is dual-stack.

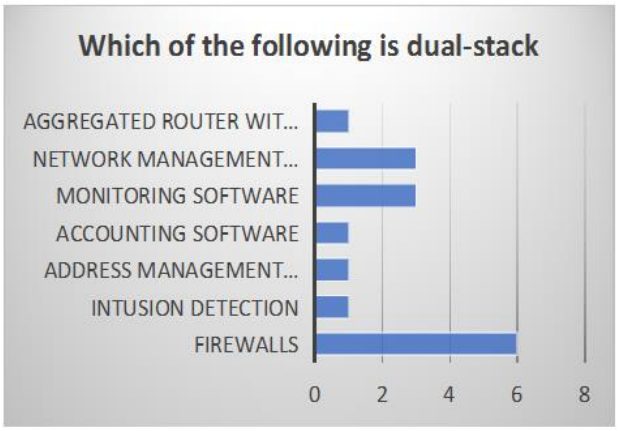

Fig.4. The Dual-Stack Software

As the previous section of the analyzes have shown that 71.4% of the companies in Palestine apply Dual-stack Routing Backbone as an access method. 42.9% of the CPE that companies supply is pure IPv6 enabled. 100% of the equipment that the companies support can be field upgraded to support IPv6. 57.1% of the companies did upgrade the DNS to support "AAAA" resolutions. 28.6% of the companies have functions between heterogeneous networks. These percentages set a positive indicator of the transition process. It turns out that the companies on their way to start deploying the IPv6.

3.3. ISPs Future Plans

At this part of the analysis, there are six questions related to the future of the ISPs companies and their plans for the future. The intend of these questions is to examine the planes that the ISPs implement for the future, and did the ISPs apply the transition to IPv6, if so, what percentage of the customers demand services needed the transition to IPv6, and if they didn't apply the transition to IPv6, have they made plans for the transition process. The respondents were given four answers with scale: Already Started = 4, 1-2 years = 3, 3-5 years = 2, more than 5 years = 1.

Table 3. is the frequency table for the first question. The respondents were asked about the time they expect to run out of all their public IPv4 addresses. Three participants, representing 42.9% of the responding companies, reported that they expect to run out of the public IPv4 address after more than five years. Two participants, representing 28.6% of the responding companies, reported that they expect to run out of the public IPv4 addresses after 2-3 years. Two

participants, representing 28.6% of the responding companies, reported that they expect to run out of the public IPv4 addresses after 1-2 years.

Table 3. When the ISPs Expect to Run Out of the Public IPV4 Addresses

When the ISPs expect to run out of all of their public IPv4 addresses				
		Frequency	Percent	Valid Percent
Valid	more than 5 years	3	42.9	42.9
	3-5 years	2	28.6	28.6
	1-2 years	2	28.6	28.6
	Total	7	100.0	100.0

Table 4. is the frequency table for the second question. The respondents were asked about the time they plan to start offering IPv6 as a regular service. One participant, representing 14.3% of the responding companies, reported that he needs more than five years to start offering IPv6 as a regular service. Three participants, representing 42.9% of the responding companies, reported that they need 3-5 years to start offering IPv6 as a regular service. Two participants, representing 28.6% of the responding companies, reported that they need 1-2 years to start offering IPv6 as a regular service. One participant, representing 14.3% of the responding companies, reported that he already started offering IPv6 as a regular service.

Table 4. When the ISPs Plan to Start Offering IPV6 as A Regular Service

When the ISPs plan to start offering IPv6 as a regular service to all of their customers				
		Frequency	Percent	Valid Percent
Valid	more than 5 years	1	14.3	14.3
	3-5 years	3	42.9	42.9
	1-2 years	2	28.6	28.6
	Already started	1	14.3	14.3
	Total	7	100.0	100.0

Table 5. is the frequency table for the third question. The respondents were asked about the time they plan to start deploying IPv6 if you didn't already start offering IPv6 as a regular service. Three participants, representing 42.9% of the responding companies, reported that they need 3-5 years to start deploying IPv6. One participant, representing 14.3% of the responding companies, reported that he needs 1-2 years to start deploying IPv6. Three participants, representing 42.9% of the responding companies, reported that they already started offering IPv6 as a regular service.

Table 5. When the ISPs Plan to Start Deploying IPV6

When the ISPs plan to start deploying IPv6				
		Frequency	Percent	Valid Percent
Valid	3-5 years	3	42.9	42.9
	1-2 years	1	14.3	14.3
	Already started	3	42.9	42.9
	Total	7	100.0	100.0

Table 6. is the frequency table for the fourth question. The respondents were asked about the time they plan to start offering IPv6 as a special or trial service to customers. Two participants, representing 28.6% of the responding companies, reported that they need 3-5 years to start offering IPv6 as special or trial service. Four participants, representing 57.1% of the responding companies, reported that they need 1-2 years to start offering IPv6 as special or trial service. One participant, representing 14.3% of the responding companies, reported that he already started offering IPv6 as a special or trial service.

Table 6. When the ISPs Plan to Start Offering IPV6 AS Trial Service

When the ISPs plan to start offering IPv6 as a special or trial service to customers				
		Frequency	Percent	Valid Percent
Valid	3-5 years	2	28.6	28.6
	1-2 years	4	57.1	57.1
	Already started	1	14.3	14.3
	Total	7	100.0	100.0

Table 7. is the frequency table for the fifth question. The respondents were asked about the time they require IPv6 to be available to all customers. Two participants, representing 28.6% of the responding companies, reported that they need more than five years to require IPv6 to be available to all customers. Two participants, representing 28.6% of the responding companies, reported that they need 3-5 years to require IPv6 to be available to all customers. Two participants, representing 28.6% of the responding companies, reported that they need 1-2 years to require IPv6 to be available to all customers. One participant, representing 14.3% of the responding companies, reported that he already started requiring IPv6 to be available to all customers.

Table 8. is the frequency table for the sixth question. The respondents were asked about the time they expect IPv6 traffic to reach 30% of total traffic. Four participants, representing 57.1% of the responding companies, reported that they expect after more than five years IPv6 traffic will reach 30% of total traffic. Two participants, representing 28.6% of the responding companies, reported that they expect after 3-5 years IPv6 traffic will reach 30% of total traffic. One participant, representing 14.3% of the responding companies, reported that he expects after 1-2 years IPv6 traffic will reach 30% of total traffic.

Table 7. When the ISPs Require IPV6 to Be Available to All Customers

When the ISPs require IPv6 service to be available to all customers				
		Frequency	Percent	Valid Percent
Valid	more than 5 years	2	28.6	28.6
	3-5 years	2	28.6	28.6
	1-2 years	2	28.6	28.6
	Already started	1	14.3	14.3
	Total	7	100.0	100.0

Table 8. When the ISPs Expect IPV6 Traffic to Reach 30% of Total Traffic

When the ISPs expect IPv6 traffic to reach 30% of total traffic				
		Frequency	Percent	Valid Percent
Valid	more than 5 years	4	57.1	57.1
	3-5 years	2	28.6	28.6
	1-2 years	1	14.3	14.3
	Total	7	100.0	100.0

4. Results

The data analysis section started with an overview to present the answers of the participants. The first research question asks about what customers demand and require. As described in the first subsection of the data analysis less than 25% of the customers in Palestine requesting IPv6. Also, less than 25% of the customers currently use IPv6 and less than 25% of the customers who are IPv6-only customers. These percentages deduce that most of the customers focus on using IPv4 or didn't even realize that there is an IPv6 they can request. Most of the customers require IPv4 addresses or a block of IPv4 addresses if the customer is a corporate customer. Also, multihoming is one of the customers' requirements. Regardless, according to the answers, 39.2% of the customers refused to consider IPv6 which means that the rest of the customers are willing to consider the transition to IPv6. That makes the transition process ISPs' responsibility.

The next research question intends to examine the infrastructure willingness to the transition process. As described in the second subsection of the data analysis, 71.4% of the respondents are actually provide their customers with Large Scale Nat (LAN) to prolong the IPv4 address space. 42.9% of the respondents provide their customers with pure IPv6 enabled CPE. Unfortunately, the equipment that the companies support can't be field upgraded to support IPv6. Also, 57.1% of the respondents did upgrade the DNS to support "AAAA" resolutions. 28.6% of the respondents their SMTP, POP3, and IMAP services and HTTP service including caching and webmail are dual-stack and dual-connectivity. In addition, 28.6% of the respondents have functions between the heterogonies networks. These percentages indicate that not all companies' infrastructures are fully ready to sustain the IPv6, but as some numbers describe that there is clear progress in some companies to until finally be able to the transition to IPv6.

The second part of the second research question was to examine the technologies that the companies provide to their customers. As indicated in the provided technology section, all the ISPs offers the ADSL access technology. Six companies offer wireless broadband and fiber optic. Two companies offer broadband over powerline and coaxial cable and one company offer dial-up. Also, five companies apply dual-stack routing backbone as an access method, which is a step to start the transition to IPv6. Five companies indicated that all their equipment support IPv6. Six companies indicated that their firewalls are dual-stack. Other software i.e. Aggregated router with upstream, Network management tools, Monitoring software, Accounting software, Address management software, and Intrusion Detection at least in one company is dual-stack.

The last research question asks if the ISPs did apply the transition to IPv6 or not. As indicated in the ISPs future plans section, 42.9% of the respondents expect to run out of the IPv4 address space in more than five years. 28.6% of the respondents expect the running out process would take from two to three years, and 28.6% of the respondents expect they will run out of IPv4 address space after one or two years. One company, which represents 14.3% of the responding companies indicates that they started to offer IPv6 as a regular service to all of the customers. The other companies indicated that they need more time to start offering IPv6. Three companies, which represents 42.9% of the responding companies, indicated that they actually started the deployment process. One company need one or two years to start deploying and three companies needs from three to five years to start with the process.

The second part of this question asks if the ISPs did apply the transition to IPv6, what percentage of the customers require services needed the transition to IPv6. As indicated in the customers' demands section, less than 25% of the customers' demands IPv6, less than 25% of the customers currently use IPv6, and less than 25% of the customers are IPv6-only customers. From these percentages, we can deduce that the customers actually don't request IPv6 or use IPv6 even though some companies are able to meet their request.

The third part of this research question asks if the ISPs didn't apply the transition to IPv6, have they made plans for the future. As indicated in the last subsection of the data analysis section, 28.6% of the respondents need one or two years to start offering IPv6 as a regular service and 42.9% of the respondents need from two to three years to start offering IPv6 as a regular service, and 14.3% of the respondents need more than five years to start offering IPv6 as a regular service. Also, 42.9% of the respondents need more than five years to start the process of deploying IPv6, 14.3% of the respondents need one or two years to start the process.

28.6% of the respondents plan to start offering IPv6 as a trial service to the customers in three to five years. 57.1% of the respondents plan to start offering the trial service in one or two years. 28.6% of the respondents plan to start providing IPv6 as a regular service in one or two years, 28.6% of the respondents plan to start providing IPv6 as a regular service in three to five years, and 28.6% of the respondents plan to start providing IPv6 as a regular service in more than five years.

These results gave us a full picture of the environment and if its capable of sustaining the IPv6 or not. As indicated the infrastructure is not fully ready to start the offering IPv6. Still the companies in progress of updating the infrastructure so that it will be able to sustain IPv6. Also, one company answered that they are capable of providing IPv6 to the customers and the other companies answered that they need more time to start providing IPv6. From these results we can expect in two or three years more companies will start the transition process.

As we discussed in the previous sections, the transition process is the responsibility of both the internet providers and the end-users. The ISPs can't force their customers to start using IPv6 knowing that it might cost them extra money. One of the problems that retard the transition process is that most of the customers require IPv4 or a block of IPv4 addresses instead of IPv6 or don't have the knowledge about IPv6 address that they can require and what are the benefits that they can get from starting the transition process.

5. Conclusion and Recommendations

To conclude, the IPv4 has been significantly exhausted in the past few years. It has reached the last /8 of available IPv4 addresses. As indicated from the LIR, NIR, and RIR the remaining address pool is subject to a significant lack of shortfall. IETF has proposed many mechanisms to prolong the life expectancy of the IPv4 address pool. These solutions will always be temporary. So, IETF has proposed mechanisms to start the deployment process of IPv6 along-side with IPv4 to achieve smooth transition at the end.

With the lack of research in this field particularly in Palestine, this study is to examine the internet companies in Palestine and what these companies have achieved in the transition process to IPv6. Also, studying the infrastructure and its willingness to the deployment of IPv6. This purpose can be achieved by applying a questionnaire on the ISPs in Palestine to examine the users' demands, the infrastructure readiness, technologies that the ISPs provides to the users, and to see if these companies have made plans for the future.

The questionnaire has been conducted on 7 companies out of 9 companies, which represent 78% of the ISPs in Palestine. The questionnaire contained three parts of questions. The first part is to examine the users' demand and requirements, and the second part intent to examine the infrastructure and the technologies that ISPs provide to the users. The last part is to detect the ISPs plans for the future and when they expect to start the deployment process.

As a result, the data analysis showed that the infrastructure is not fully willing to sustain the IPv6 deployment. Even though some companies 'infrastructure is ready to start the deployment process, and the other companies are in their way to be ready for the process. This gives us a good view of the environment. Also, the results showed that there is one company that actually did apply the transition and it's ready to start offering IPv6 as a regular service. The other companies who didn't apply the transition indicated that they plan to start deploying in the coming years. One problem that may delay the process is that the users do not require IPv6 service or any services that need the transition to IPv6.

Based on the questionnaire, we have some recommendations for farther research that can be made based on the findings of this research. This Survey was limited to internet providers in Palestine. Perhaps increasing the sample to include the users could provide for a greater collection of information across Palestine since the transition process

depends on the end-users alongside with the ISPs. Also, that might help in detecting problems this research has not revealed. Furthermore, studying other companies such as telecommunication companies and universities, to find out what benefits the transition process might have and how much these companies need it.

References

[1] J. Postel, "Internet Protocol California," USA: *Internet Engineering Task Force* RFC 791, 1981. DOI: https://doi.org/10.17487/RFC0791.

[2] G. Huston, IPv4 Address Exhaustion in APNIC. (2015). *The ISP Column*, A monthly column on things Internet. http://www.potaroo.net/ispcol/2015-08/last8.html

[3] R. Hinden, and S. Deering, "IP Version 6 Addressing Architecture," California, USA: *Internet Engineering Task Force* RFC 4291, 2006. DOI: https://doi.org/10.17487/RFC4291.

[4] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," California, USA: *Internet Engineering Task Force* RFC 8200, 2017. DOI: https://doi.org/10.17487/RFC8200.

[5] A. Hamarsheh, M. Goossens, "A Review: Breaking the Deadlocks for Transition to IPv6," *IETE Technical Review*, vol.31 no. 6, pp. 405-421, 2014. DOI: http://doi.org/10.1080/02564602.2014.950348

[6] R. Gilligan, and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," California, USA: *Internet Engineering Task Force* RFC 1933, 1996. DOI: https://doi.org/10.17487/RFC1933.

[7] E. Nordmark, and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," California, USA: *Internet Engineering Task Force* RFC 4213, 2015. DOI: https://doi.org/10.17487/RFC4213.

[8] G. Huston, "Addressing 2018," The ISP Column, A monthly column on things Internet. http://www.potaroo.net/ispcol/2019-01/addr2018.html 2019 (Accessed 2019)

[9] P. Srisuresh, and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," California, USA: *Internet Engineering Task Force* RFC 3022, 2001. DOI: https://doi.org/10.17487/RFC3022.

[10] I. Yamagata, Y. Shirasaki, A. Nakagawa, J. Yamaguchi, and H. Ashida, "NAT444," *Internet Engineering Task Force*, 2012. in Press.

[11] A. Hamarsheh, "Deploying IPv4-only Connectivity across Local IPv6-only Access Networks," IETE Technical Review, vol. 35, to be published, 2018.

[12] S. Thomson, and T. Narten, "IPv6 Stateless Address Autoconfiguration," California, USA: *Internet Engineering Task Force* RFC 2462, 1998. DOI: https://doi.org/10.17487/RFC2462.

[13] B. Carpenter, and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," California, USA: *Internet Engineering Task Force* RFC 3056, 2001. DOI: https://doi.org/10.17487/RFC3056.

[14] K. Tsuchiya, H. Higuchi, and Y. Atarashi, "Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)," California, USA: *Internet Engineering Task Force* RFC 2767, 2000. DOI: https://doi.org/10.17487/RFC2767.

[15] S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, and A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)," California, USA: *Internet Engineering Task Force* RFC 3338, 2002. DOI: https://doi.org/10.17487/RFC3338.

[16] B. Huang, H. Deng, and T. Savolainen, "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)," California, USA: *Internet Engineering Task Force* RFC 6535, 2012. DOI: https://doi.org/10.17487/RFC6535.

[17] X. Li, C. Bao, and F. Baker, "IP/ICMP Translation Algorithm," California, USA: *Internet Engineering Task Force* RFC 6145, 2011. DOI: https://doi.org/10.17487/RFC6145.

[18] M. Bagnulo, A. Sullivan, P. Matthews, and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers," California, USA: *Internet Engineering Task Force* RFC 6147, 2011. DOI: https://doi.org/10.17487/RFC6147.

[19] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)," California, USA: *Internet Engineering Task Force* RFC 2765, 2000. DOI: https://doi.org/10.17487/RFC2765.

[20] A. Hamarsheh, M. Goossens, and A. Al-Qerem, "Assuring Interoperability Between Heterogeneous (IPv4/IPv6) Networks Without using Protocol Translation," IETE Technical Review, vol. 29, no. 2, pp. 114-132, 2012.

[21] A. Durand, R. Droms, J. Woodyatt, and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion," California, USA: *Internet Engineering Task Force* RFC 6333, 2011. DOI: https://doi.org/10.17487/RFC6333.

[22] M. Bagnulo, P. Matthews, and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers," California, USA: *Internet Engineering Task Force* RFC 6146, 2011. DOI: https://doi.org/10.17487/RFC6146.

[23] A. Hamarsheh, M. Goossens, R. Alasem, "Decoupling Application IPv4/IPv6 Operation from the Underlying IPv4/IPv6 Communication (DAC)," *American Journal of Scientific Research*, Eurojournals Press, Issue 14 pp. 101-121, 2011.

[24] W. Townsley, and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) Protocol Specification," California, USA: *Internet Engineering Task Force* RFC 5969, 2010. DOI: https://doi.org/10.17487/RFC5969.

[25] R. Despres, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)," California, USA: *Internet Engineering Task Force* RFC 5569, 2010. DOI: https://doi.org/10.17487/RFC5569.

[26] Ala Hamarsheh, M. Goossens, R. Alasem, Deploying IPv6 Service Across Local IPv4 Access Networks. Presented at 10th WSEAS International Conference on TELECOMMUNICATIONS and INFORMATICS (TELE-INFO '11), pp. 94-100, Lanzarote, Canary Islands, Spain, May 27-29, 2011.

[27] Ala Hamarsheh and M. Goossens, "Exploiting Local IPv4-only Access Networks to Deliver IPv6 Service to End-users," International Journal of Computers and Communications, vol. 5, no. 3, 2011.

[28] Ala Hamarsheh, M. Goossens, and R. Alasem, "Configuring Hosts to Autodetect (IPv6, IPv6-in-IPv4, or IPv4) Network Connectivity," *KSII* Transactions on Internet and Information Systems, vol. 5, no. 7, pp. 1230-1251, 2011.

[29] Ala Hamarsheh, Yazan AbdAlaziz, Transition to IPv6 Protocol, Where We Are, 2019 International Conference on Computer and Information Sciences (ICCIS), IEEE Xplore Digital Library, 2019.

Authors' Profiles

Y. Abdalaziz is a Computer science bachelor candidate at the Faculty of Engineering and Information Technology, Arab American University - Jenin, Palestine. He interested in networking and the transition protocols to IPv6. He is working as trainer at Partners for Sustainable Development (PSD), Palestine.

Ala B. Hamarsheh is an associate professor at the Faculty of Engineering and Information Technology of the Arab American University of Jenin. Dr. Hamarsheh has obtained a PhD in engineering sciences from Vrije Universiteit Brussel (VUB)/Brussels-Belgium in 2012. He graduated in computer science at the Faculty of Science, Birzeit University, Palestine, in 2000. He obtained an MSc degree in computer science at the Kind Abdullah II School for IT, The University of Jordan, Jordan, in 2003. Dr. Hamarsheh has published numerous papers in international refereed journals and conferences.

How to cite this paper: Yazan W. Abdalaziz, Ala Hamarsheh, "Analyzing the IPv6 Deployment Process in Palestine", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.5, pp.31-45, 2020. DOI: 10.5815/ijcnis.2020.05.03

