OULU UNIVERSITY OF
APPLIED SCIENCES

Long Hoang

A STUDY OF INTERNET PROTOCOLS

Why the transition to IPv6 is so slow

A STUDY OF INTERNET PROTOCOLS

Why the transition to IPv6 is so slow

Long Hoang
Bachelor's Thesis
Spring 2019
Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Degree Programme of Information Technology

Author: Long Hoang
Title of Bachelor´s thesis: A Study of Internet Protocols
Supervisor: Kari Laitinen
Term and year of completion: Spring 2019 Number of pages: 39

The subject of the thesis came up when the author was working on the development of an IoT device.

While being a very stable and currently standard Internet protocol, the limitations of IPv4 could limit the potential of IoT devices. IPv6 with all its benefits would be the future protocol and could solve the problem of IPv4. However, the adoption of IPv6 is slow because of the cost, the incompatibility and the lack of knowledge of IPv6.

By researching about IPv6 and comparing different transition scenarios and alternative solution, the author believes that the knowledge will benefit for the author's career in the future as an Internet of Things developer, a web application developer and a Development Operations (DevOps) engineer.

Keywords: Internet, Internet Protocol, IPv4, IPv6, transition

TABLES OF CONTENTS

ABBREVIATIONS

CGN	Carrier-grade NAT
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GUA	Globally Unique Address
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol standard version 4
IPv6	Internet Protocol standard version 6
ISP	Service Provider
NAT	Network Address Translation
NCP	Network Control Program
PC	Personal Computer
PLAT	Provider-Side Translator
SLAT	Customer-Side Translator
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ULA	Unique Local Address

1 INTRODUCTION

Over the last few years, the Internet of Things (IoT) has been one of the most discussed topics. It started with the concept back to late 1990s and gained some public attentions in the middle of 2000s (Postscapes 2018, cited 1.5.2019). In 2005, the United Nations agency, International Telecommunication Union published its ITU Internet Reports about the topic (International Telecommunication Union 2005, cited 1.5.2019). The Internet of Things gained the momentum in the beginning of 2010s and has been developed heavily in these recent years. Google acquired one of the success companies in this field, Nest Labs for $3.2 billion, the second biggest deal in Google's history (Oreskovic 2014, cited 1.5.2019). People dream of the world of smart and connected daily devices. The topic also pushes the development of future technologies, voice control, artificial intelligence (AI) and self-drive car.

However, the Internet of Things will not be the next revolution without one of its cores, the Internet. The Internet has come a long way from its start. The current Internet Protocol dated back from 1981 had already showed the ages. With the goal to provide the connectivity in the simple and small network, its vision is vastly different compared to the vision of the modern world. In chapter two, the author discusses IPv4 and its problems. The Internet of Things demands a new development of the Internet. The Internet of Things needs a new Internet Protocol that has the vision of the Internet of Things. It needs to support the need of the Internet of Things and it enables the true potential of the Internet of Things. In chapter three, the author discusses IPv6 and its benefits.

Despite all benefits, the IPv6 adoption is still very slow. Although IPv6 celebrated its 20th birthday in 2016, it is still not ready for the whole world to support the rapid development of the Internet of Things. In the fourth chapter, the author discusses why the transition is so slow. Facing this question in the development of an Internet of Things device, the author researched about transition methods of IPv6. In chapter five, the author discusses the most common transition scenarios and alternative solutions.

There were some aims that the author had through the thesis. The first was to understand the Internet, IPv4 and its limits. The second one was understanding IPv6 and the benefits it brings to the technology world. The third one was to find out the answers to the question why the IPv6

transition takes so long time. The last one was the knowledge about most common transition scenarios and alternative solutions and their advantages and disadvantages. The author believes that the knowledge will benefit for the author's career in the future as an Internet of Things developer, a web application developer and a Development Operations (DevOps) engineer.

2 THE LIMITATIONS OF IPV4

2.1 Internet

The Internet is the biggest computer network. It is a global network of thousands of interconnected computer networks. Each computer network could contain many hosts, for example, personal computers (PC) or mobile phones and network devices. Those devices are connected by some data links over some media, for example physical cables or wireless communication technologies. By connecting them together, a computer network allows hosts to send, receive, share and exchange resources though the network. The resources could be information, books, sounds or even videos. The Internet allows people to share resources to everyone in the worldwide. Nobody could deny the importance of the Internet. Stephen Hawking, the famous English physicist and cosmologist, once said: “We are all now connected by the Internet, like neurons in a giant brain” (Swartz 2014, cited 1.5.2019). For the important of the Internet, according to Bill Gates, “The Internet is becoming the town square for the global village of tomorrow” (Gates 1999, 45).

War might be evil but the technology development and research that came along with that could not be denied. Many military technologies that were originally created to use in the war have then been used with civilian uses. Many of them have also changed the whole world life. The Internet is one of them. The Internet has come a long way from its origin from 1960s as a project of the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense for developing new technologies for military purposes. The term ‘Internet’ comes from the concept of the “Intergalactic Computer Network” by J. C. R. Licklider (Norman 2019, cited 1.5.2019). He described in his memo that “outlining a key part of his strategy to connect all their individual computers and time-sharing systems into a single computer network spanning the continent” in 1963. And in 1969, his idea became reality with the Advanced Research Projects Agency Network (ARPANET). At first, there were many different network methods. When people wanted to connect networks together, a standard protocol is needed so that every computer and network could talk together. In addition, because ARPANET started with a small number of computers, its host-to-host protocol Network Control Program (NCP) is not suitable for the network. This development resulted in the Transmission Control Program that was published in RFC 675 in 1974 (Cerf, Dalal & Sunshine 1974, cited 1.5.2019). Later researches led to the split of it into the

Transmission Control Protocol (TCP) and the Internet Protocol (IP) (USC Information Sciences Institute 1981, cited 1.5.2019). These protocols are still used today and known as TCP/IP or the Internet protocol suite.

2.2 Internet Protocol and Internet Model

After the Transmission Control Program was putted to use, there was discussion with the basic concept of the protocol. In 1977, Jon Postel admitted: "We are screwing up in our design of internet protocols by violating the principle of layering" (Postel 1977, cited 1.5.2019). The Transmission Control Program then was split into the Transmission Control Protocol (TCP) and the Internet Protocol (IP) in 1981. The first Internet Protocol standard was published in RFC 791 (USC Information Sciences Institute 1981, cited 1.5.2019). It is still widely used today and is known as IPv4. In the protocol specification, there is a diagram that illustrates the relationships of the Internet Protocol to other protocols (FIGURE 1).

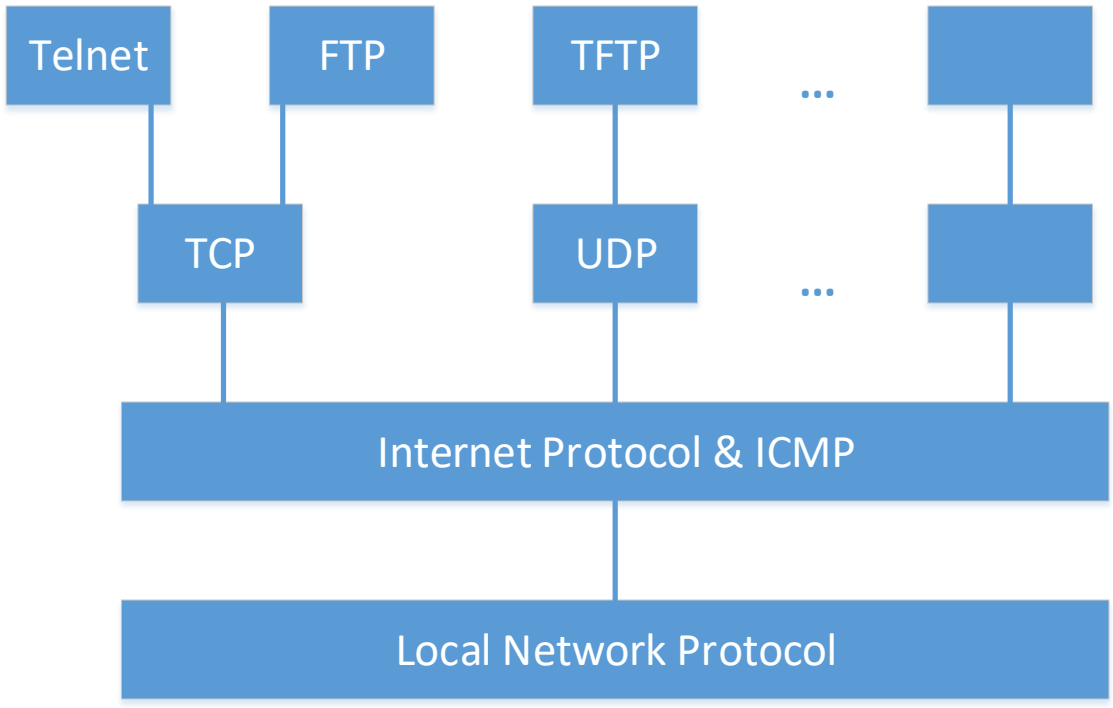

FIGURE 1. Protocol Relationships (USC Information Sciences Institute 1981, cited 1.5.2019)

This later developed into the Internet model or TCP/IP model that was defined in RFC 1122 in 1989. The TCP/IP model consists of 4 layers: Application Layer, Transport Layer, Internet Layer and Link Layer (Internet Engineering Task Force 1989, cited 1.5.2019). The Application Layer is

the top layer that contains programs and high-level protocols. They use the connection provided by lower layers and it is the layer that users interact with. In this layer, the high-level protocols are used by the programs to exchange and show information to the users. Common protocols are the Hypertext Transfer Protocol (HTTP) for websites or the File Transfer Protocol (FTP) for sending or receiving files. The Transport Layer is responsible for the host-to-host communications so that a computer could receive and understand the transmit data. It also provides the separate data channels between applications. Most commons protocols are the Transmission Control Protocol (TCP) for reliable and the User Datagram Protocol (UDP) for lower latency. The Internet Layer is responsible for the routing of the datagram, which makes sure that the data transmits across different networks through the Internet to the correct destination. The Link Layer is the lowest layer that provides the network topology and the corresponding protocols to transmit the data. There is also an Open Systems Interconnection model (OSI model) which is defined by the International Organization for Standardization (ISO). The relationship of two models is shown in FIGURE 2 with the popular protocols.

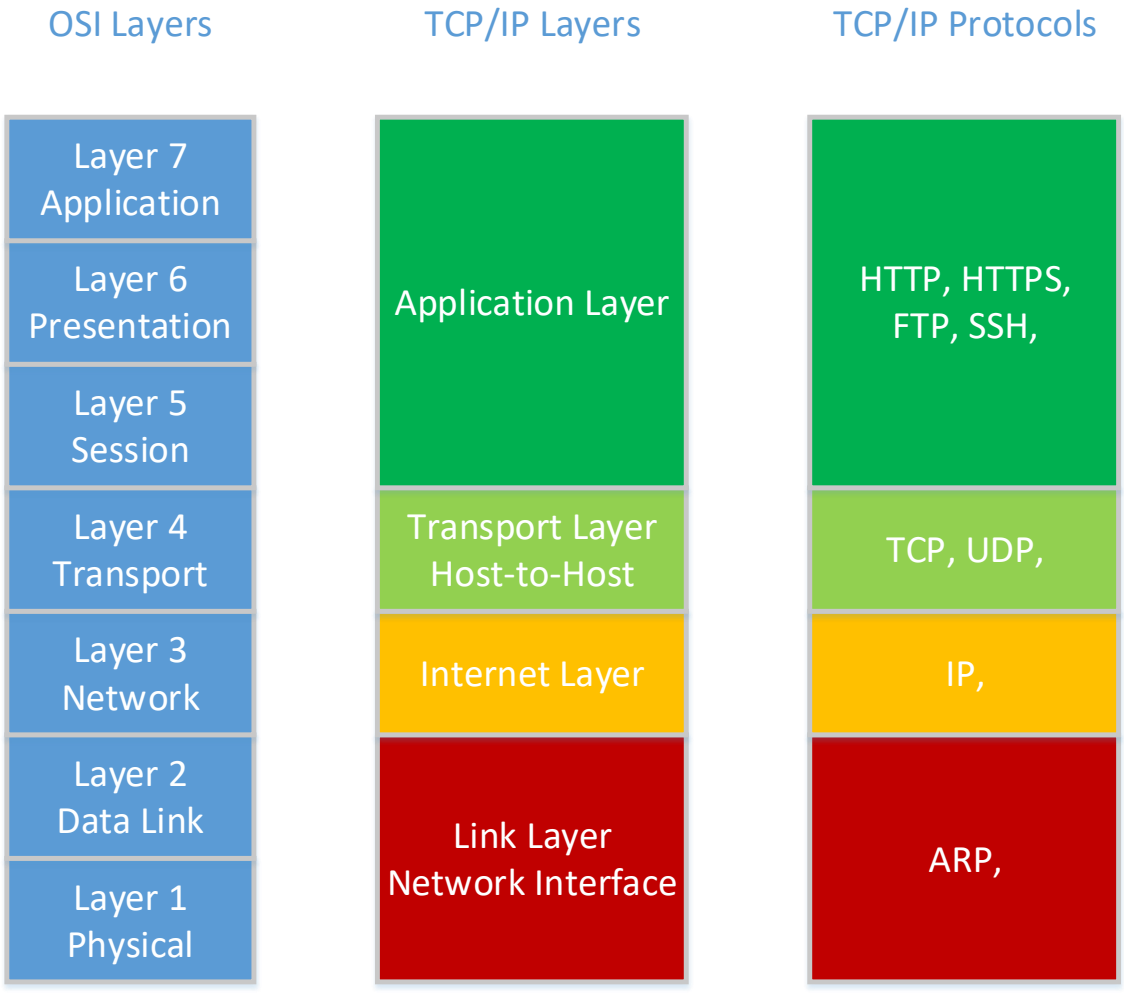

FIGURE 2. OSI layers and TCP/IP layers relationship

2.3 IPv4

The first standard of the Internet Protocol is the Internet Protocol Version 4 (IPv4), which was published in RFC 791 in 1981. It was accepted as the standard for ARPANET which later became the Internet. There was a plan to switch to TCP/IP in 1983. DARPA provided a 1-year transition from January 1982 to 1 January 1983. Every computer and network had to switch to the TCP/IP suite (Postel 1981, cited 1.5.2019). The transition plan was documented in RFC 801. The transition went smoothly, and people made the buttons said “I survived the TCP/IP transition” to celebrate the event (Powers 2014, cited 1.5.2019).

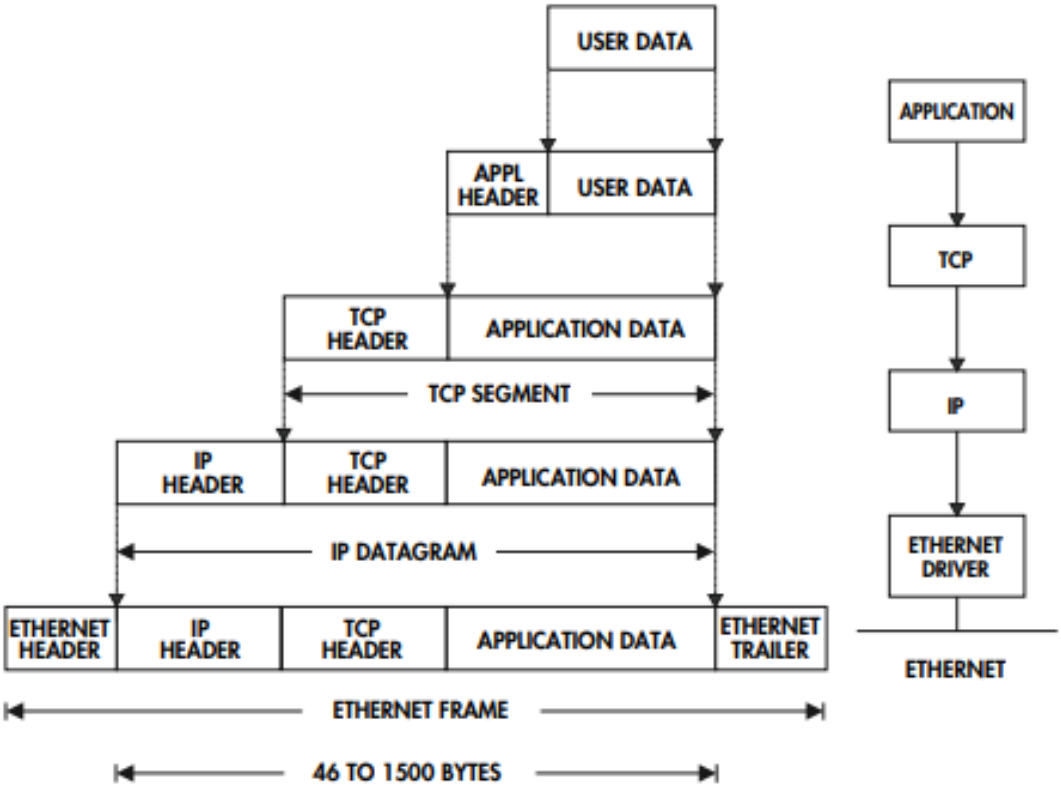

FIGURE 3. Packet payload through the network layers (Thomas 1999, 2)

The Internet Protocol defined the Ethernet frame which is how the data is transmitted. When the data is sent from the application, the corresponded protocol header is added when the packet goes down through each layer and then striped when it goes up. An example is shown in FIGURE 3. Therefore, the data payload is encapsulated in the layer 4 segment, then it is encapsulated in the layer 3 packet, and then it is encapsulated in the layer 2 frame and then passed through the physical media. With that mechanism, the frame is forwarded until it reaches the destination. To route the

packages through different networks, the packet will need to pass through devices called routers. Routers work on the layer 3 of OSI model and are called L3 devices. When the router receives the packet, it strippes the layer 2 frame to get the packet, reads the layer 3 header to find the destination IP address. Based on its router routing table, it will drop or forward the packet by encapsulating it in the layer 2 frame and send it through the outgoing network interface.

RFC 791 defined the IP header for IPv4. The source address and the destination address are both 32 bits or 4 octets (FIGURE 4). The IPv4 address is usually presented as four octets expressed as decimal numbers and separated by dot, for example, 192.0.2.1. The IP addresses are used in routing in the Internet. Each device needs to have an IP address to connect to the Internet.

<table>
<tr><td colspan="4">0</td><td colspan="4">1</td><td colspan="4">2</td><td colspan="4">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="2">Version
(4 bits)</td><td colspan="2">IHL
(4 bits)</td><td colspan="4">Type of Service
(8 bits)</td><td colspan="8">Total Length
(16 bits)</td></tr>
<tr><td colspan="4">Identification
(16 bits)</td><td colspan="2">Flags
(3bits)</td><td colspan="6">Fragment Offset
(13 bits)</td></tr>
<tr><td colspan="2">Time To Live
(8 bits)</td><td colspan="2">Protocol
(8 bits)</td><td colspan="8">Header Checksum
(16 bits)</td></tr>
<tr><td colspan="12">Source IP Address
(32 bits)</td></tr>
<tr><td colspan="12">Destination IP Address
(32 bits)</td></tr>
<tr><td colspan="8">Options</td><td colspan="4">Padding</td></tr>
</table>

FIGURE 4. IPv4 Header (USC Information Sciences Institute 1981, cited 1.5.2019)

Although IP addresses are easy to write and are used for routing the data, they are not easy to remember. It is easier to remember meaningful words than some random numbers. People started to use domain names instead. In the beginning, there was a file in the computer that mapped each domain name to its corresponding IP address. It was difficult to synchronize the file between every computer until Paul Mockapetris invented the Domain Name System (DNS) in 1983 (Mockapetris 1987, cited 1.5.2019). The DNS system contains multiple servers that when is asked about the IP address of a domain name, could reply the A record of the domain which is its IP address.

2.4 Problems of IPv4

There are some problems with IPv4 that encouraged the need to develop a new Internet Protocol. The first and biggest problem of IPv4 is that IPv4 uses 32-bit addresses. Vinton Cerf, one of the inventors of TCP/IP, when asked about what he would change if he could go back in time, replied: "I wish I had realized we'd need more than 32 bits of address space!" (Lord 2011, cited 1.5.2019). This limit the address space to only 4,294,967,296 (2^{32}) addresses or about 4.3 billion addresses. The world's population is about 7.6 billion people as of May 2018 and it still increases every year. So that there is not even enough to have one IP address per person, let alone for the servers to host the web services. The IP address space is managed by a nonprofit organization named Internet Assigned Numbers Authority (IANA). IANA then delegates the addresses to five regional Internet registries (RIR). RIR then allocates the IPv4 address blocks to the customers or smaller local Internet registry (LIR). IANA has allocated all non-reserved address blocks in 2011. As of September 2015, four out of five RIRs have exhausted all IPv4 address blocks in their free pool and the last RIR, AFRINIC which serves Africa, is expected to be exhausted in December 2019 (Huston 2019, cited 1.5.2019).

The second problem comes from the work around for the exhaustion of address space. Because of the lack of addresses, there is a method called the Network Address Translation (NAT). This method is used to map many IP addresses of a private network to one public IP address before routing in the Internet. This method reduces the need of IPv4 addresses but has some drawbacks. Because of the translation, the hosts are not actually directly connected, and it breaks the end-to-end transparency. Some protocols are then not compatible with NAT and need workarounds. NAT can also break some type of encryption and cause security issues, for example, DNS cache poisoning. Furthermore, because NAT needs to keep track of all connections which then require much resources to process the routing. Because of the exhaustion and still increasing customers, Internet Service Providers (ISP) even started to use Carrier-grade NAT (CGN), which basically adds one or more NAT layers. The connection then become double or triple NAT and these problems are significant amplified.

The last problem is the packet processing time. Because of the complex header and variable header length, much resources are needed to process packets. Furthermore, there is a header checksum in the IPv4 header. In addition, because of the fact the Time to Live (TTL) field needs to

be reduced through each hop, the check sum will need to be recalculated each time. This needs even more processing resources and reduces the effectiveness of the packet processing.

3 IPV6 AND HOW IT IS BETTER

Because of the problems with IPv4, there have been developments for a new Internet Protocol standard very early. IPv6 was specified as an Internet standard in RFC 1883 in 1995 (Deering & Hinden 1995, cited 1.5.2019). In order to avoid all the limitations and mistakes of IPv4, IPv6 was designed as an all-new Internet Protocol. There is no change to the IPv4 protocol and the IPv6 protocol will stay alongside the IPv4 protocol. Vint Cerf, when talked about IPv4, said: "I thought this was still an experiment and that, if successful, we would develop a production version. I guess IPv6 is the production version!" (Lord 2011, cited 1.5.2019).

The main advantage of IPv6 over IPv4 is its much larger address space. From 32 bits in IPv4, the address length of IPv6 is increased to 128 bits (FIGURE 6). Therefore, the address space will be 2^{128} address, equally to 3.4×10^{38} addresses or 340 trillion trillion trillion addresses. A minimum /64 prefix is recommended for a subnet or a link in IPv6. It means that each local area network could have 2^{64} or 18 million trillion addresses, more than enough for every user, IoT devices, and even for companies or institutions. In addition, the customer could still request more if the customer needs multiple subnets, for example a /56 or /48 prefix. Some people may think that a /64 prefix subnet is waste because a normal person or family would not use that many addresses. However, IPv6 was designed to make the IP address conservation irrelevant and to keep working in the future. There are still 18 million trillion /64 subnets. The large address space will eliminate the need for IP address sharing technique, for example NAT, and recover the end-to-end transparency as well as improve the processing performance.

The second advantage of IPv6 is that the packet header in IPv6 has been simplified compared to IPv4 (FIGURE 5). Some fields have been removed and the header length is fixed. These changes improve the packet processing efficiency, reduce the resources needed for processing which then improve the speed. Furthermore, the header checksum is removed, and the packet integrity is expected to be hold by upper layers which will be decided depending on the purpose of the application. This also improves the packet forwarding through each hop. Optional Extension headers are the replacement of the Options field in IPv4. Extension headers are not included in the normal IPv6 header but placed right after the IPv6 header. This change makes the IPv6 header fixed length, also called the IPv6 fixed header. The Next Header field of IPv6 fixed header will indicate the type of the first Extension header and so on. This change would make the routing of

IPv6 packets more efficient because the routing devices would only need to read and process a fixed length header. It is also simpler to do routing in hardware devices and reduce the need of a large chipset.

Another advantage of IPv6 is that it supports Stateless address autoconfiguration (SLAAC). IPv6 clients can auto configure its unique IP address without the need of a DHCP server as well as the resources for its corresponding stateful table in the routing devices. The use of /64 prefixes combined with random seed number and MAC address of the devices ensured the unique addresses between devices. The connection establishment will be faster as less steps are needed. SLAAC benefits IoT devices because of the simpler network stack. IPv6 also support multiple IP address simultaneously. Beside the normal Globally Unique Address (GUA), the device can have Unique Local Address (ULA) for routing between local networks and Link local address for the connectivity within a local network without even a router. This new addition makes it easier to troubleshoot IPv6 connection problems.

Some other advantages of IPv6 is that its design is suitable for some use cases that were not available when IPv4 was designed. For example, there are the security features as well as the mobility capabilities. IPv6 has IPsec security support built in. Combining it with the direct host-to-host connection can significantly improve the security of the network.

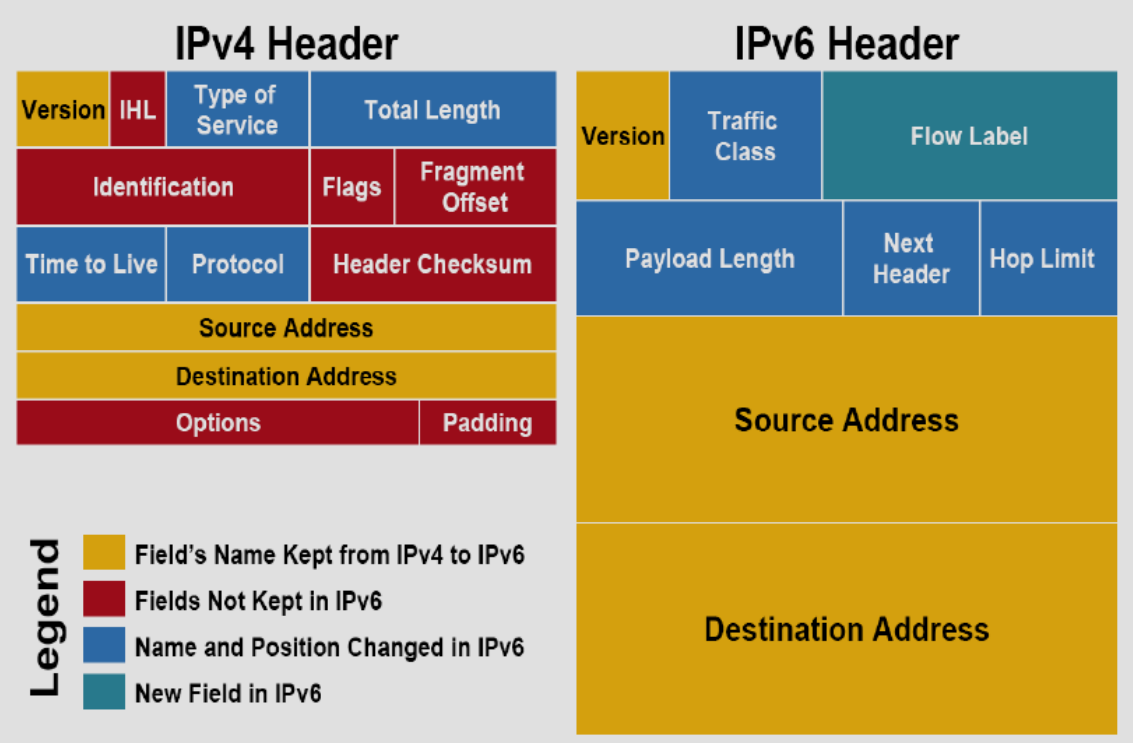

FIGURE 5. IPv4 and IPv6 header comparison (Silverman 2014, cited 1.5.2019)

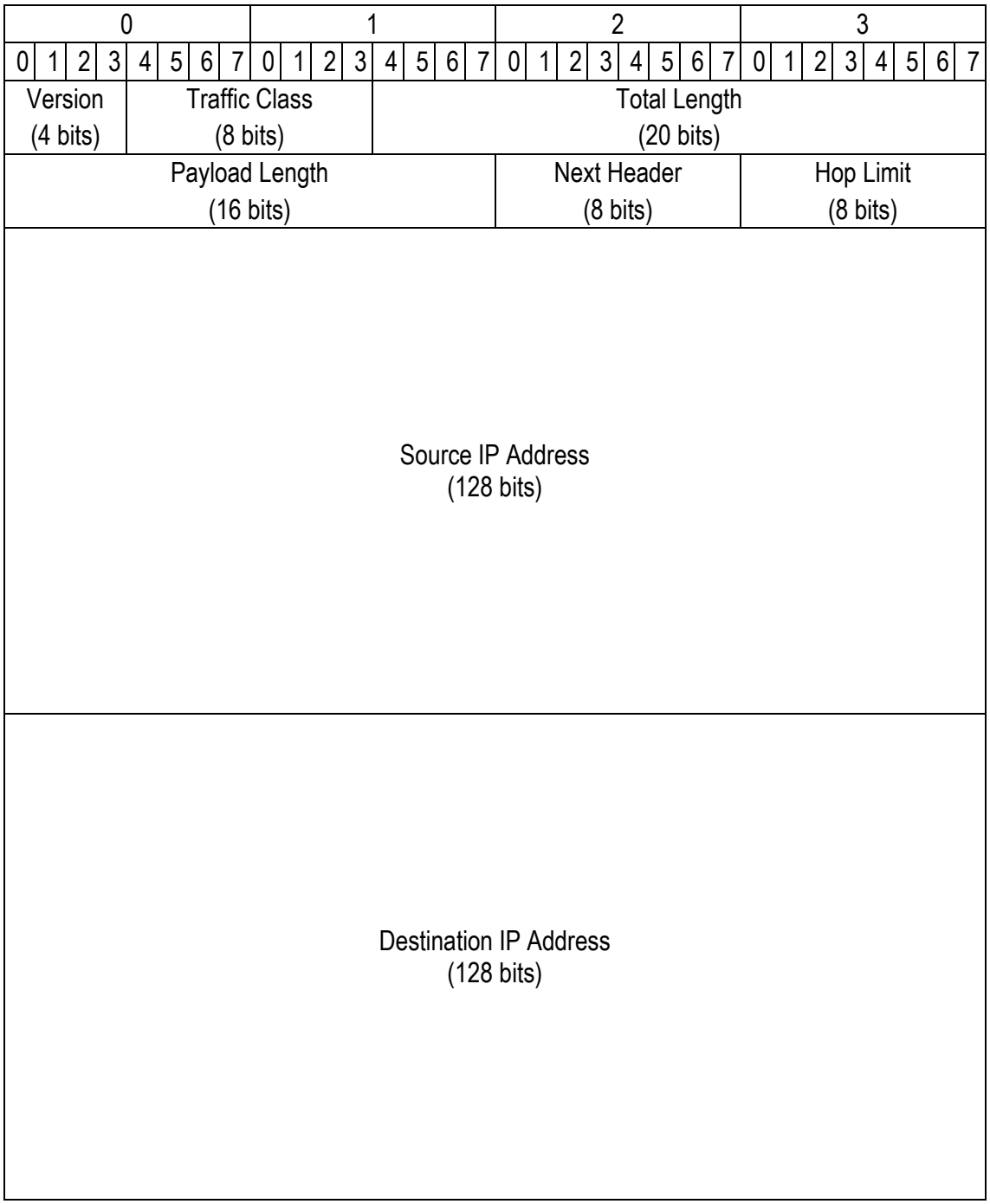

FIGURE 6. IPv6 Header (Deering & Hinden 1995, cited 1.5.2019)

4 WHY THE TRANSITION TO IPV6 IS SO SLOW

With many benefits of IPv6 and the fact that even its author thinks that IPv4 was just an experiment, IPv6 should be welcomed by the technology world and the transition would be reasonable fast. The Internet community arranged World IPv6 Day in 2011 to promote IPv6 testing and World IPv6 Launch Day in 2012 to bring IPv6 support on many websites and services. Then with the development of IoT devices, people expected that it can drive the adoption rate of IPv6. Cisco predicted that there would be 50 billion devices connected to the Internet in 2020 (Evans 2011, 3). However, the adoption of the new Internet Protocol seems very slow. When IPv6 celebrated its 20th birthday at the end of 2015, the adoption rate was only 10 percent. With some providers moving to IPv6, people said that the IPv6 adoption will follow a sine-wave shape (Hogg 2016, cited 1.5.2019), which took a very long time to reach 10 percent in 2015 but then fastened the speed to reach 50 percent in 2018 (FIGURE 7).

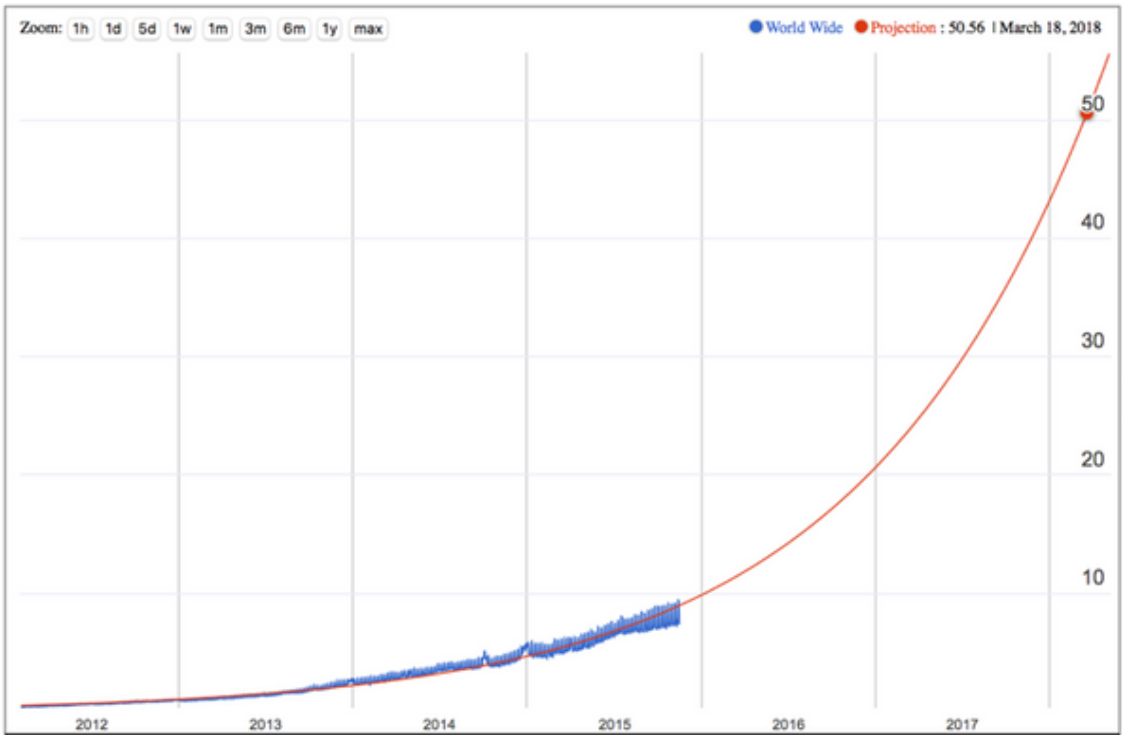

FIGURE 7. IPv6 adoption prediction in 2015, up to 50% in 2018 (Coffeen 2015, cited 1.5.2019)

As of May 2018, the adoption rate is about 20 percent and as of May 2019, the adoption rate is about 25 percent (Google 2019, cited 1.5.2019). The adoption rate is faster than earlier, but still slow. The new prediction is that people would need until 2022 for IPv6 to catch up with IPv4 at 50

percent (FIGURE 8). Center for Applied Internet Data Analysis (CAIDA) based on data from several large USA cities, predicted that this event will happen between 2022 and 2023. The adoption rate is also following a linear rather than a sine-wave shape (Hick & Polterock 2018, cited 1.5.2019).

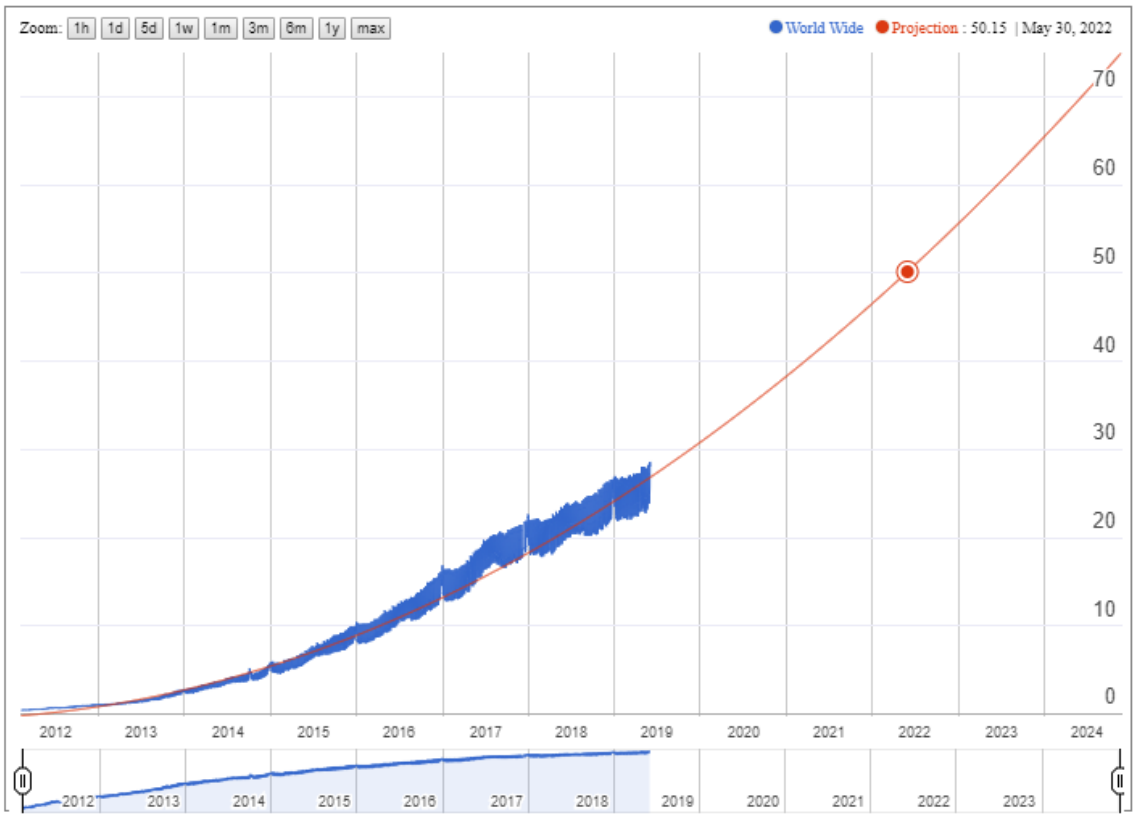

FIGURE 8. IPv6 adoption prediction in 2019, up to 50% in 2022 (Vyncke 2019, cited 1.5.2019)

The first problem of the transition is the cost of equipment. Because IPv6 is an all new protocol, every device in the routing needs to be replaced to support IPv6. This means that the service provider needs to replace or upgrade their servers. The Internet providers and data centers need to replace their routers and switches. The Internet contains millions of devices like these so replacing them will take much time and cost a lot. Then there are billions of end user devices that need to be replaced for the IPv6 to work. Therefore, the transition to IPv6 is expensive. Money could affect the decision of many companies. Normal end users could stay behind NATs, but for companies, they will need more IPv4 addresses. After ARIN runout of its IP blocks in 2015, the price of the smaller IP address blocks on the trade market significantly increased (FIGURE 9). There would be time where the cost of the transition appears to be better than to continuously buy expensive IPv4 addresses.

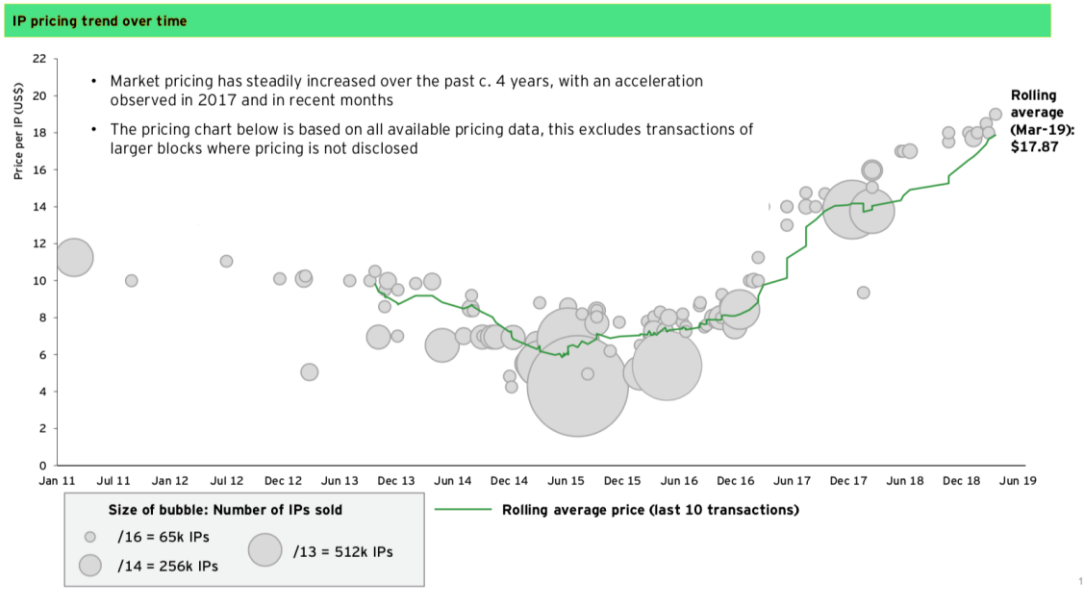

FIGURE 9. IPv4 price trends (IPv4 Market Group 2019, cited 1.5.2019)

The second problem of the transition is the widely use of NAT. Despite some drawbacks, NAT is a low-cost work around of the exhaustion of IPv4 address space. It can be slowly added when needed instead of the massive change of the IPv6 transition. Most of the service providers will stick with NAT as long as this solution still works. For end users, most people would be happy with NAT for the near future, only small percent of technology enthusiasts would complain about that.

Another problem of the transition is that there is no compatibility between IPv4 and IPv6. So that after the transition to IPv6, systems in IPv6 cannot communicate with systems that still run IPv4. It will be necessary to run both IPv4 and IPv6 side by side, which is not very attractive because IPv4 alone is still working. In order to disable IPv4, everyone needs to switch to IPv6 already, which is not very reachable compared to the transition to IPv4 in 1983. So that there is almost no advantage to adopt IPv6 early. Most companies would decide to wait for others to do that first.

The fourth problem is the knowledge about IPv6. Because there are so many huge changes between IPv4 and IPv6, the old industry will need to re-learn the new standard. The deployment process will need to change. The best practices will also need to be modified and to be studied. The newcomers could jump on the train early, but the established companies and organizations will need more time for their human resources to research, test and put IPv6 in production.

The last problem is that there is a concern about the security of IPv6, especially at its earlier implementations. One side effect of NAT is that it blocks incoming packets from outside without the outcoming requests. That effect is similar to a simple firewall. When transition to IPv6, people who are not familiar with firewall or do not have one may face security issues. While NAT is actually not a security feature, the lack of knowledge about IPv6 may cause the issue. Especially, with the rise of IoT devices, the direct connection of IPv6 may open the holes for cyber-attacks and lead to malicious devices. The earlier implementations, which are not well tested, may have bugs waiting to be exposed and fixed for the security concerns.

In conclusion, the biggest reasons of the slow adoption of IPv6 are the cost of hardware, the incompatibility of IPv6 and the lack of knowledge. While the cost of replacing old hardware could not be avoided, by researching about IPv6, there would be some solutions to work around the incompatibility of IPv6.

5 IPV6 TRANSITION SCENARIOS AND ALTERNATIVES

Understanding the differences between IPv6 and IPv4, the author wanted to explore different IPv6 transitions and alternative solutions. Because of the incompatibility between IPv6 and IPv4, there are some methods and mechanisms that have been developed to help the transition from IPv4 to IPv6. There are also some alternatives that are suggested to avoid the issues of IPv6. In this chapter, common IPv6 transition scenarios and alternatives are researched. Based on that, the author discusses the advantages and disadvantages of those solutions.

5.1 Alternative Internet Protocol

The most benefit to drive the Internet toward IPv6 is the larger address space. Because of the incompatibility between IPv6 and IPv4, people discuss the solutions that could avoid this issue but still have the benefit of larger address space.

5.1.1 IPv4.1

IPv4.1 is suggested as the extension of IPv4. IPv4 has the address space of 32 bits. IPv4.1 adds one more octets to IPv4 so the address will have a total of five octets (FIGURE 10). This will make IPv4.1 to have an address space of 2^{40}, which is more than 1 trillion addresses and 256 times larger than the address space of IPv4. To keep backward compatibility, the legacy IPv4 addresses will be translated to four lower octets of IPv4.1 and the first octet will be zero. For example, the IPv4 address 192.0.2.1 will become 0.192.0.2.1 on the IPv4.1 protocol. The developers also suggest that in the future, if the address space is not enough, people can add another octet and upgrade to IPv4.2.

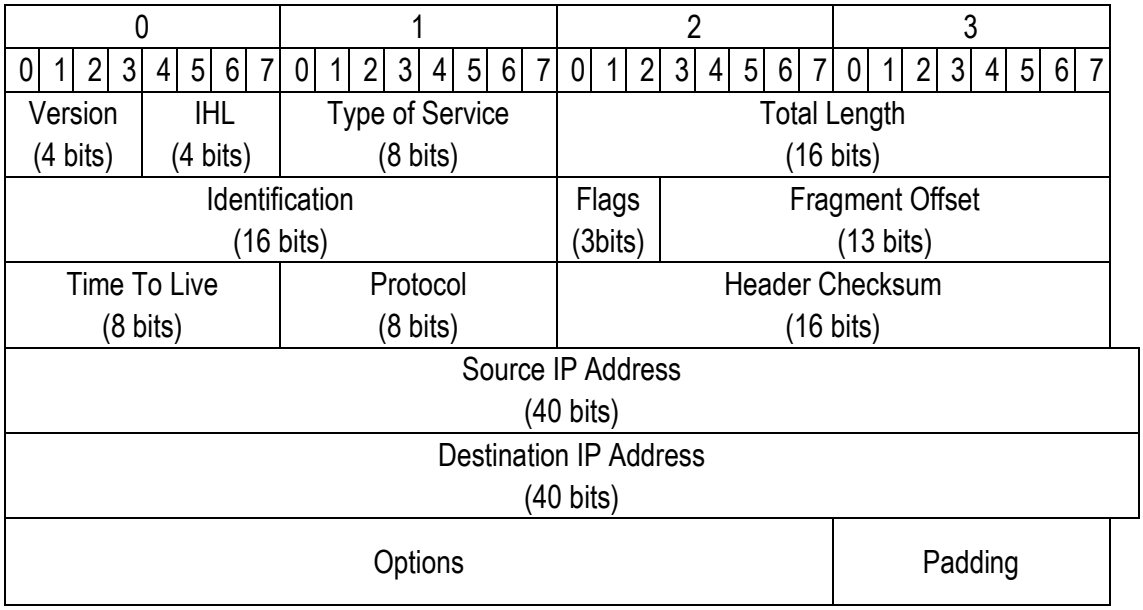

FIGURE 10. IPv4.1 Header (Stretch 2011, cited 1.5.2019)

5.1.2 IPv10

Another direction to avoid the incompatibility between IPv6 and IPv4 is a new protocol that supports both IPv4 and IPv6. IPv10 is the Internet protocol draft that follows this direction. The protocol aims to allow the communication between an IPv4 host and an IPv6 host. IPv10 keeps the same address field length as the IPv6 address, 128 bits. The idea is that the IPv10 address field can contain either an IPv4 address or an IPv6 address (FIGURE 11). When the device receives IPv10 packets, the device needs to analyze the type of address in the packet before processing or routing the packet. If the address field contains an IPv4 address, the device follows the IPv4 routing table and follows the IPv6 routing table if it detects an IPv6 address. One advantage of this protocol is that it does not add another DNS record and can process either an IPv4 A or an IPv6 AAAA record for domain names.

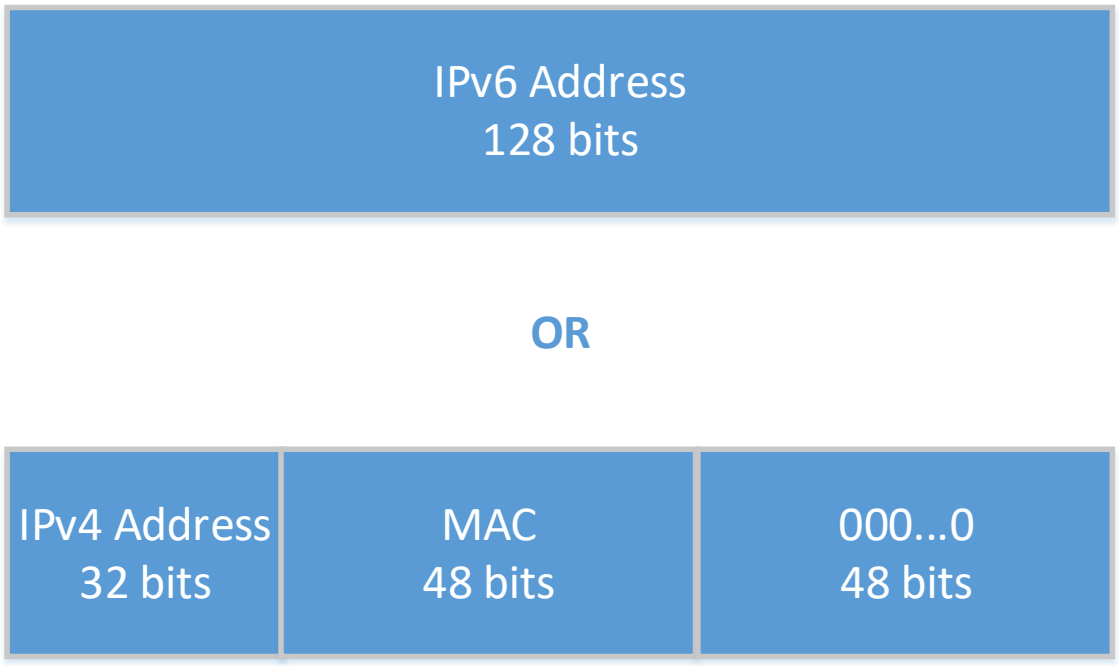

FIGURE 11. IPv10 address field (Omar 2018, cited 1.5.2019)

5.1.3 EzIP

Another suggestion is keeping the same IPv4 protocol but changing the way to allocate the IPv4 public address pool. Adaptive IPv4 Address Space or EzIP falls in this category. The developers argue that the IPv4 address exhaustion issue is the result of the allocation of the address pool because despite the reports of depleted address pool, there are unused IPv4 address blocks still being traded around. EzIP adds a reserved address block 240.0.0.0/4 and a new category of routers called Semi-Public Router. 240.0.0.0/4 is the address block that is reserved for the future use (Cotton & Vegoda 2010, cited 1.5.2019). This block is still unused despite the depletion of IPv4 address pool. Semi-Public Routers are routers that sit between Internet core routers and Internet Service Provider routers. Semi-Public Routers and Internet core routers provide the global Internet routing using the 240.0.0.0/4 address block (FIGURE 12).

The developers claimed that EzIP could expand the IPv4 address pool by 256 million (256M) times. The advantage of EzIP is because of keeping the same IPv4 packet specification, the most existing hardware will support EzIP. There are also some disadvantages of this solution. Firstly, it still keeps all other weaknesses of IPv4. Next, the EzIP solution is similar to adding another global layer of NAT. This will further the issue of direct connection between IoT devices. Finally, using the reserved

address block has a serious draw back. Most software implementations of IPv4 reject or blacklist this address block. Therefore, to deploy EzIP, many software implementations need to be updated.

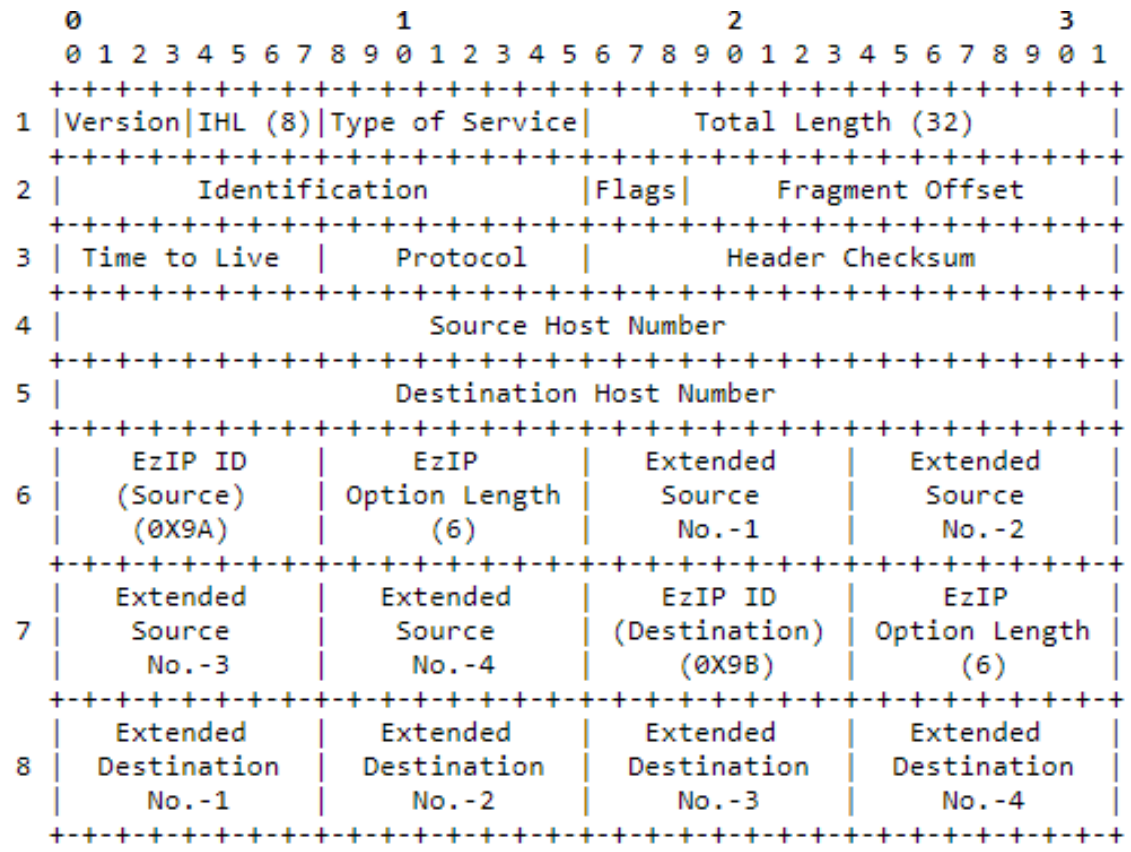

FIGURE 12. EzIP Header (Chen & Ati 2018, cited 1.5.2019)

5.1.4 Enhanced IP (EnIP)

Enhanced IP is another solution aim to expand the IPv4 address pool by adding octets to the address. Instead of modifying the address fields in the packet, it utilizes IP options 26 to store additional address bits (FIGURE 13). This allows that the Enhanced IP has the address pool of 64 bits. Enhanced IP also uses DNS AAAA records with an experimental IPv6 prefix 2001:0101 to avoid the need of a new record type and a DNS software upgrade. Enhanced IP does not require hardware upgrades but still needs software upgrades for all end hosts. All NAT devices also need to patch to support Enhanced IP. Furthermore, Enhanced IP is not compatible with multiple layers of NAT, which many ISPs have already used to work around the exhaustion of IPv4.

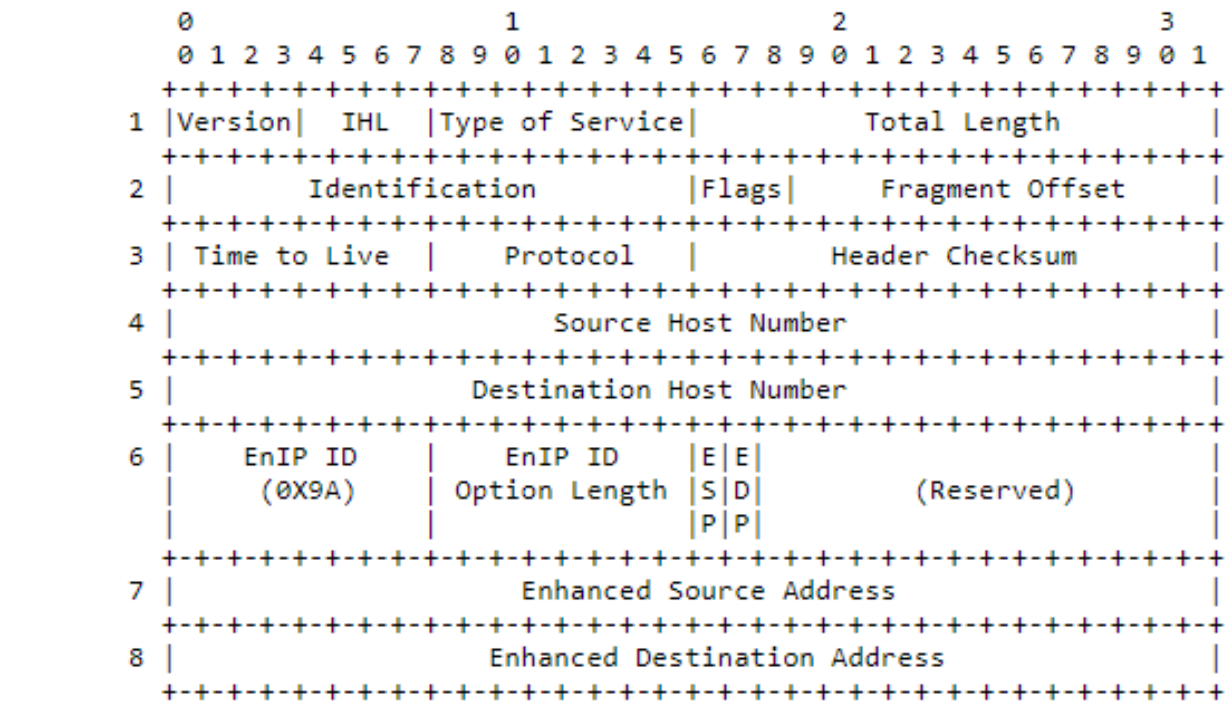

FIGURE 13. EnIP Header (Chimiak, Patton, Brown, Bezerra, Galiza & Smith 2016, cited 1.5.2019)

All of those alternative protocols try to keep their specifications close to IPv4 to avoid the compatibility issue of IPv6. They suffer from the same problems as IPv4, for example NAT layers and its consequence, direct end-to-end connections. Despite minimalizing the changes, they still need changes to Internet software or hardware layers. As some big vendors have already made changes to transition to IPv6 and other vendors are preparing, the global transition to IPv6 is inevitable. Alternative protocols are potential but not very practical at this stage of Internet.

5.2 IPv4 only network with IPv6 translation

In the early stage of IPv6 transition, the network connections will stay as IPv4 only. New service hosts will migrate to IPv6 on the IPv6 only Internet. There are some methods developed to help to provide the connectivity in this scenario.

5.2.1 6in4

6in4 is one of the oldest tunnel mechanisms. In 6in4, the IPv6 packet is packed and encapsulated as the IPv4 packet. The resulted packet is the IPv4 header followed by the IPv6 packet (FIGURE

14). Therefore, the overhead is the size of IPv4 header, which is 20 bytes (Nordmark 2005, cited 1.5.2019).

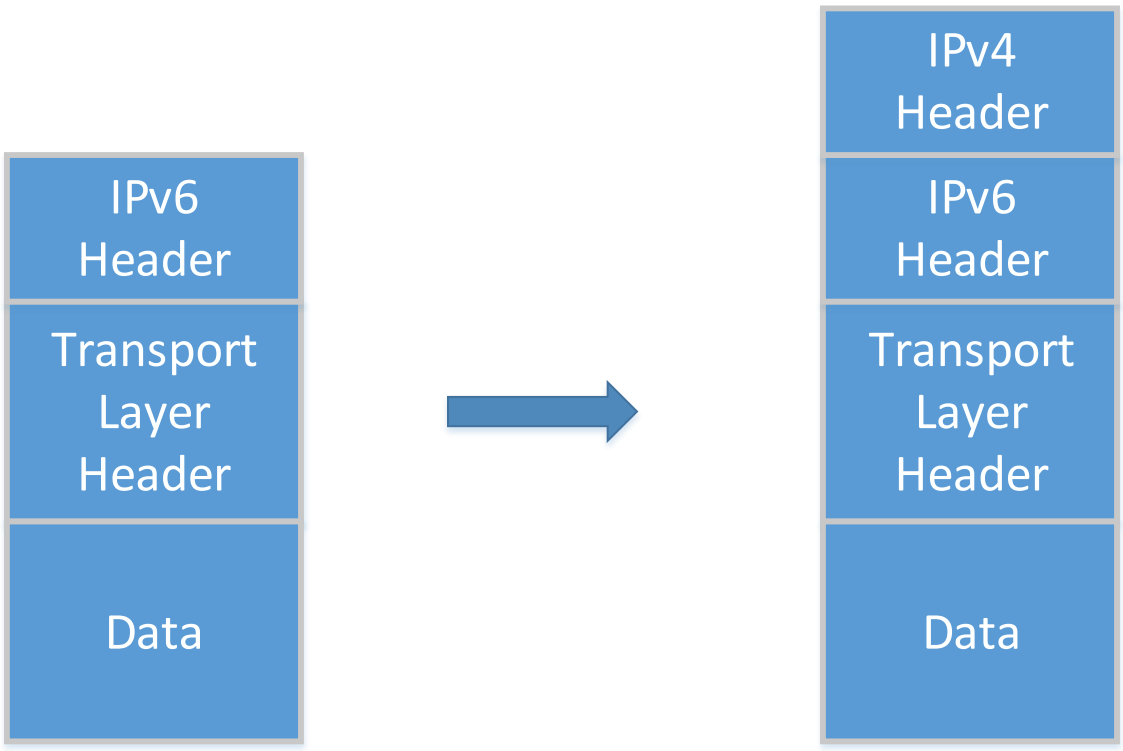

FIGURE 14. 6to4 encapsulating IPv6 in IPv4

To different from a normal IPv4 packet, the IP protocol number of the header is set to 41. The 6in4 mechanism needs an encapsulator and a decapsulator (FIGURE 15). The encapsulator is at the entry of the tunnel. It is the unit which encapsulates the packet and transmits the 6in4 packet. The encapsulator has only the IPv4 Internet connection and usually the router. The decapsulator is at the exit of the tunnel, receives the packet, strips the IPv4 header and transmits IPv6 the packet to the IPv6 only host. The decapsulator has both IPv4 and IPv6 connections and it is called tunnel broker. The 6in4 tunnel is also called the manual tunnel or the static tunnel. The reason is that the tunnel broker needs to be static and manually configured. If the public IPv4 address of the encapsulator is dynamic, the IPv4 source address in the decapsulator also needs to update dynamically to match the public IPv4 address. Therefore, the disadvantage of 6in4 tunnel is the need to be manually configured. On the other hand, because of the simplistic of protocol and the static of the tunnel broker, it is easier to debug than the more complex tunnel mechanisms.

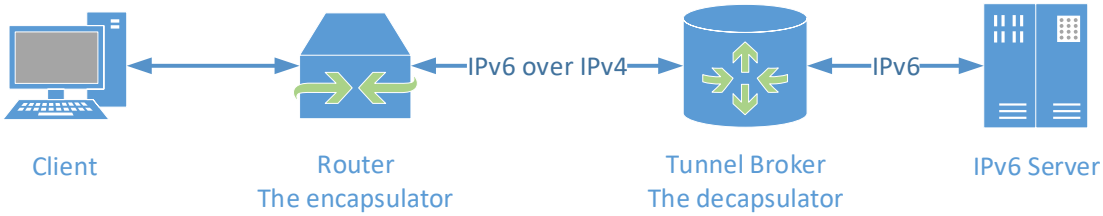

FIGURE 15. 6in4 scenario flow

5.2.2 6to4

The 6to4 tunnel is very similar to the 6in4 tunnel. The underlying mechanism is the same. The main difference is that the decapsulator is not a specific tunnel broker but a cloud of 6to4 relays (FIGURE 16). Therefore, the transmission from the encapsulator to the decapsulator is anycast. The 6to4 IPv6 prefix and address can automatically construct from the public IPv4 address and the 2002::/16 prefix. For example, if the encapsulator public IPv4 address is 192.0.2.170, then the IPv6 prefix is 2002:c000:2aa::/48 and the IPv6 address could be 2002:c000:2aa::1. The global anycast IPv4 address of the decapsulator or 6to4 relays is assigned as 192.88.99.1, so its IPv6 address is 2002:c058:6301:: (Carpenter & Moore 2001, cited 1.5.2019). The advantage of 6to4 tunnel is the automatically configuration. The disadvantage is that, because of the nature of the automatically dynamic 6to4 relay choice, there are problems with performance and high failure rates (Troan & Carpenter 2005, cited 1.5.2019). It is also difficult to debug the issue in the 6to4 tunnel.

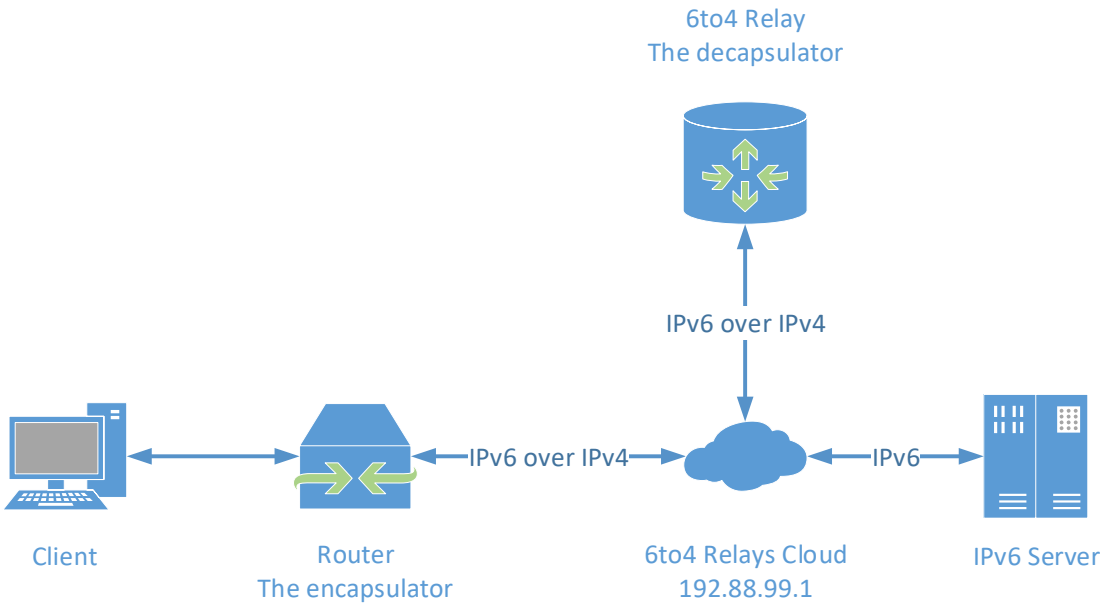

FIGURE 16. 6to4 scenario flow

5.2.3 Teredo

The problem with simple tunnel solutions is that they do not work behind NAT devices. Teredo protocol was designed to work around this problem (Huitema 2006, cited 1.5.2019). In Teredo tunnel, the encapsulator is called the Teredo client, the decapsulator is called the Teredo relay. Another new unit is added called the Teredo server (FIGURE 19). The Teredo server helps the Teredo client to config the Teredo tunnel and make the connection through the NAT layer using Teredo Bubble packets. The Teredo IPv6 packet encapsulation is also different from simple tunnel solutions. Teredo packets use the UDP protocol instead of the Protocol 41. The basic Teredo IPv6 packet encapsulation contains the IPv4 header and the UDP header followed by the IPv6 packet (FIGURE 18). The Teredo address still has 128 bits but differs from the normal IPv6 address (FIGURE 17). The advantage of the Teredo tunnel is the ability to work behind the NAT layer. Due to the complexity, the disadvantage is the high packet overhead. The overhead comes from the UDP encapsulation and the bubble technique. Therefore, the developers only recommend the Teredo tunnel after other simple tunnel solutions.

FIGURE 17. Teredo address

FIGURE 18. Teredo packet

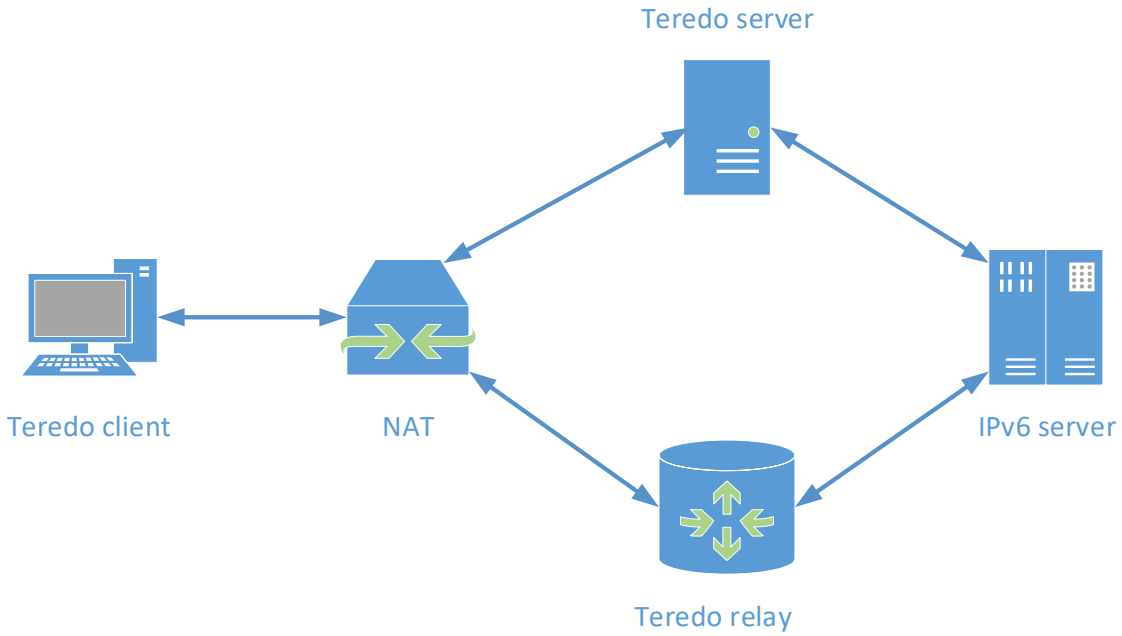

FIGURE 19. Teredo scenario flow

Tunnel protocols provide the existing IPv4 only network the ability to connect to the IPv6 only host. The disadvantage is that because of the need of the relay server, there will be some overhead issues of performance and latency compared to native IPv6. Furthermore, tunnel solutions depend on the IPv4 network and the public IPv4 address. Therefore, tunnel solutions should be used at the early stages of the IPv6 transition before moving to the IPv6 native scenarios.

5.3 IPv6 only network

In an ideal scenario, every application, every host and network would support IPv6 communications. In this scenario, moving to the IPv6 only network will remove all the issues of the IPv4 protocol and ensure all benefits of native IPv6 for all services. The problem is that the transition to IPv6 is still very slow and most of communications still in the IPv4 protocol. It is clear that, in the near future, there will not be a complete switch over to the IPv6 protocol day like the event in 1983. Therefore, there is still a need for the IPv4 translation for the IPv6 only network.

5.4 IPv6 only network with IPv4 translation

Deployment of the IPv6 only network with the IPv4 translation helps to solve the problem of the exhaustion of the IPv4 address pool, because it does not depend on an IPv4 address. It could still provide connectivity to the IPv4 only host in the transition to IPv6.

5.4.1 NAT64 and DNS64

NAT64 is a network address translation which can translate IPv6 packets to IPv4 packets and vice versa (Bagnulo, Matthews, & Beijnum 2011, cited 1.5.2019). NAT64 translates the IPv4 address to and from the IPv6 address using the algorithm defined in RFC 6052, IPv6 Addressing of IPv4/IPv6 Translators. The IPv4 address in The IPv6 address form will use the Well-Known Prefix 64:ff9b::/96 (FIGURE 20). NAT64 also keeps the mapping between the IPv4 and IPv6 address to allow the IPv6 only host communicate with the IPv4 only host.

Well-Known Prefix	IPv4 address	IPv4-Embedded IPv6 address
64:ff9b::/96	192.0.2.33	64:ff9b::192.0.2.33

FIGURE 20. IPv4-Embedded IPv6 Address using the algorithm in RFC 6052 (Bao, Huitema, Bagnulo, Boucadair & Li 2010, cited 1.5.2019)

DNS64 is a DNS server which could dynamically create and reply IPv6 AAAA records for domain names that only have IPv4 A records (Bagnulo, Sullivan, Matthews, & Beijnum 2011, cited 1.5.2019). The domain name has only IPv4 A records meaning that the host is IPv4 only. The synthesized IPv6 address is generated from the IPv4 address using the same algorithm defined in RFC 6052.

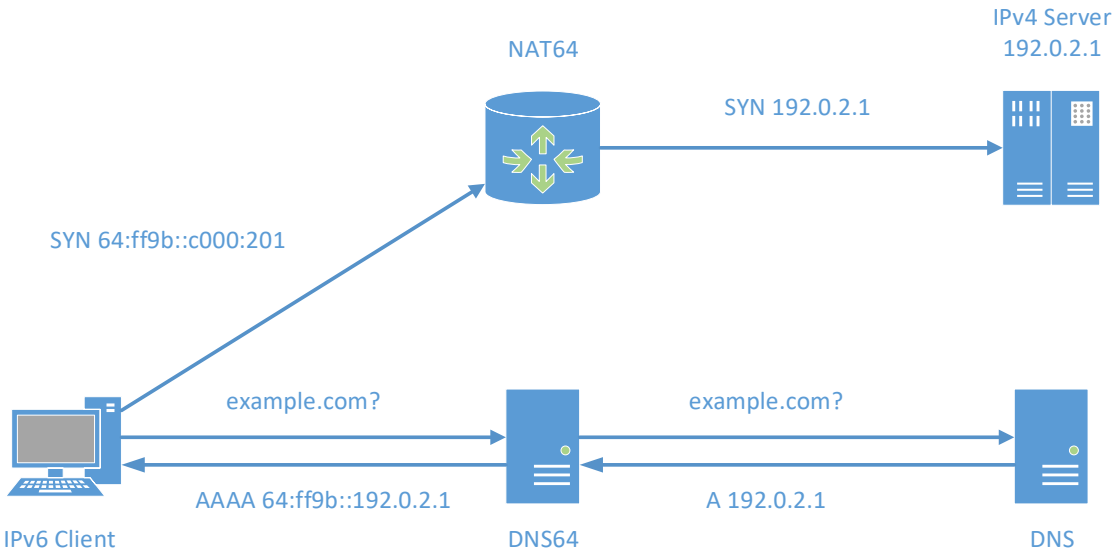

FIGURE 21. NAT64 and DNS64 scenario flow

Using both DNS64 and NAT64 together, the IPv6 only network could communicate with the IPv4 only host using domain names (Bagnulo, Matthews, & Beijnum 2011, cited 1.5.2019). An example is shown in FIGURE 21. This combination is the simple to deploy solution but still good for basic communications with the IPv4 only host. The disadvantage is that the IPv4-converted IPv6 address is generated from the domain name using DNS64. If the application uses an IPv4 literal address like 192.0.2.1, the translation will not work.

5.4.2 464XLAT

464XLAT is designed to solve the problem of using IPv4 literal addresses in the IPv4 only application. In additional to DNS64 and NAT64, called the Provider-Side Translator (PLAT), 464XLAT adds a Customer-Side Translator (SLAT) using the Stateless IP/ICMP Translation Algorithm (SIIT) mechanism (FIGURE 22). SLAT translates the IPv4 address to the IPv4-embedded IPv6 address. A packet from the IPv4 only application is translated by CLAT to an IPv6 packet for the transmission in the IPv6 only network and then translated back to the IPv4 packet by PLAT for the transmission to the IPv4 only host. The IPv4 address in the IPv6 address form will not use the Well-Known Prefix 64:ff9b::/96 but an IPv6 prefix from a prefix delegation mechanism (Mawatari, Kawashima & Byrne 2011, cited 1.5.2019).

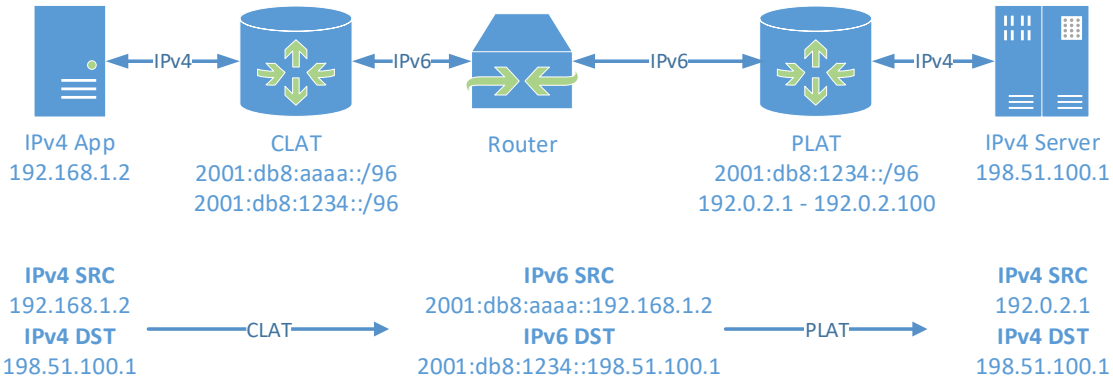

FIGURE 22. 464XLAT scenario flow

The IPv6 only network with the IPv4 translation using NAT64 combinations is the common choice for this stage of the IPv6 transition. It solves both problems of the exhaustion of the IPv4 address pool as well as the connectivity to the IPv4 only host. 464XLAT with the improvement over NAT64 and DNS64 combination is the solution for many mobile carriers to provide Internet connections. The disadvantage is that because of the network address translation, some protocol may not work correctly or has performance issues.

5.5 Dual stack

Dual stack transition scenario means to implement both IPv4 and IPv6 in the same network. Every device in the network needs to be configured for both IPv4 and IPv6 (Li, Bao, & Baker 2011, cited 1.5.2019). A packet belonging to either IPv4 or IPv6 will be route based on the corresponding routing table and network (FIGURE 23). Because both IPv4 and IPv6 are native, a dual stack solution should be the most reliable and provide the best performance. The disadvantage of dual stack is that the system administrators need to maintain two separate protocols. Because of many differences between two protocols, it doubles the work to maintain the network. It can also create confusion and misconfiguration between two protocols. Running a dual stack consumes more hardware resources. Finally, a dual stack still needs an IPv4 network and an IPv4 public address.

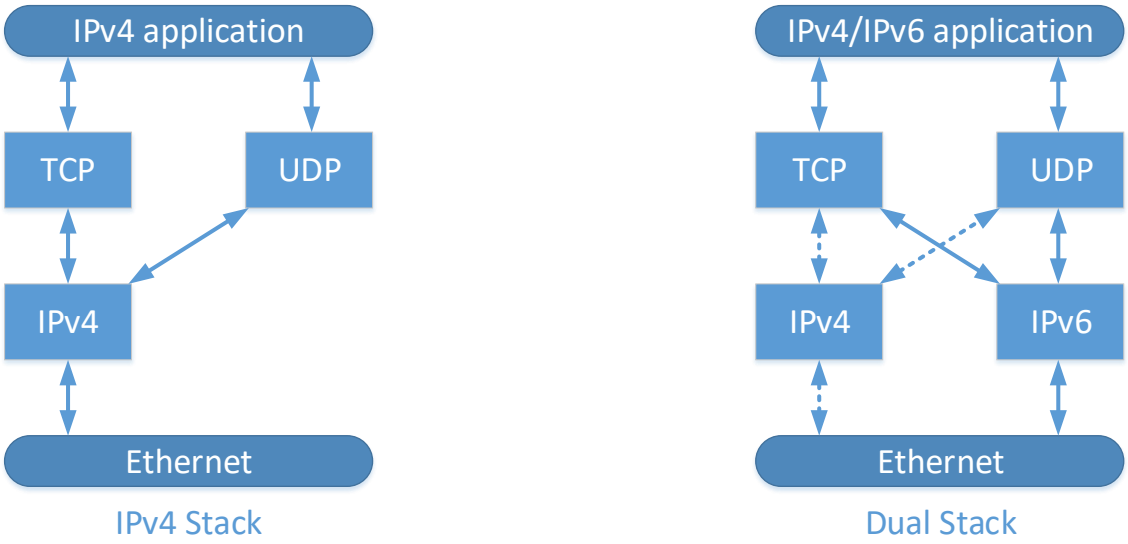

FIGURE 23. IPv4 and Dual Stack scenario comparison

6 CONCLUSIONS

The thesis topic is a real-life problem that came up when the author was working on developing an IoT device. To understand the problem, the author needed to research the structure of the Internet. Then, the author introduced the current Internet Protocol, IPv4 and discussed the problems of IPv4. After that, the author continued with details of the future Internet Protocol, IPv6 and discussed about the benefits of IPv6, which can also solve the problem with IoT devices. However, there is a phenomenon that the adoption of IPv6 is very slow. The author researched this phenomenon and found that the incompatibility between these two Internet Protocols and the lack of knowledge and confusions of IPv6 are the main reasons. In the last chapter, the author researched and compared most common IPv6 transition scenarios and alternative solutions. There are multiple scenarios between each direction of IPv6 transition and each come with its trade off. Discussing the advantages and disadvantage, the author concluded the best scenario for each phase and direction of IPv6 transition.

Through the thesis, the author has expanded the knowledge about the Internet, the current Internet network and the future Internet network. The author understands many scenarios of IPv6 networks, which will help in the IoT device development. There will be the need to test to make sure that IoT devices work in different scenarios. The new knowledge also helps the author to improve as a web developer. The web application if not design properly may have problems with the IPv6 connectivity. The deployment of websites and web applications will also move to the IPv6 environment in the near future. And as a DevOps engineer, the author could work in the new environment.

REFERENCES

Bagnulo, M., Matthews, P. & Beijnum, I. 2011. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Cited 1.5.2019, https://tools.ietf.org/html/rfc6146.

Bagnulo, M., Sullivan, A., Matthews, P. & Beijnum, I. 2011. DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. Cited 1.5.2019, https://tools.ietf.org/html/rfc6147.

Bao, C., Huitema, C., Bagnulo, M., Boucadair, M. & Li, X. 2010. IPv6 Addressing of IPv4/IPv6 Translators. Cited 1.5.2019, https://tools.ietf.org/html/rfc6052.

Carpenter, B & Moore, K. 2001. Connection of IPv6 Domains via IPv4 Clouds. Cited 1.5.2019, https://tools.ietf.org/html/rfc3056.

Cerf, V., Dalal, Y. & Sunshine , C. 1974. Specification of internet transmission control program. Cited 1.5.2019, https://tools.ietf.org/html/rfc675.

Chen, A & Ati, R. 2018. Adaptive IPv4 Address Space. Cited 1.5.2019, https://tools.ietf.org/html/draft-chen-ati-adaptive-ipv4-address-space-04.

Chimiak, W., Patton, S., Brown, J., Bezerra, J., Galiza, H. & Smith, J. 2016. IPv4 with 64 bit Address Space. Cited 1.5.2019, https://tools.ietf.org/html/draft-chimiak-enhanced-ipv4-03.

Coffeen, T. 2015. IPv4: The Future of a Legacy Protocol. Cited 1.5.2019, https://community.infoblox.com/t5/IPv6-CoE-Blog/IPv4-The-Future-of-a-Legacy-Protocol/ba-p/4779.

Cotton, M & Vegoda, L. 2010. Special Use IPv4 Addresses. Cited 1.5.2019, https://tools.ietf.org/html/rfc5735.

Deering, S. & Hinden, R. 1995. Internet Protocol, Version 6 (IPv6) Specification. Cited 1.5.2019, https://tools.ietf.org/html/rfc1883.

Evans, D. 2011. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, 3.

Gates, B. 1999. Business @ the Speed of Thought, 45.

Google 2019. IPv6 Statistics. Cited 1.5.2019, https://www.google.com/intl/en/ipv6/statistics.html.

Hick, P. & Polterock, J. 2018. IPv6 adoption as seen from an Internet backbone link. Cited 1.5.2019, https://blog.caida.org/best_available_data/2018/05/29/ipv6-adoption-as-seen-from-an-internet-backbone-link/.

Hogg, S. 2016. IPv6 is Accelerating as IPv4 is Nearing its Peak. Cited 1.5.2019, https://community.infoblox.com/t5/IPv6-CoE-Blog/IPv6-is-Accelerating-as-IPv4-is-Nearing-its-Peak/ba-p/7992.

Huitema, C. 2006. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). Cited 1.5.2019, https://tools.ietf.org/html/rfc4380.

Huston, G. 2019. IPv4 Address Report. Cited 1.5.2019, http://www.potaroo.net/tools/ipv4/index.html.

International Telecommunication Union 2005. ITU Internet Reports 2005: The Internet of Things. Cited 1.5.2019, http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.

Internet Engineering Task Force 1989. Requirements for Internet Hosts -- Communication Layers. Cited 1.5.2019, https://tools.ietf.org/html/rfc1122.

IPv4 Market Group 2019. IPv4 Price Trends. Cited 1.5.2019, http://ipv4marketgroup.com/ipv4-price-trends/.

Li, X., Bao, C. & Baker, F. 2011. IP/ICMP Translation Algorithm. Cited 1.5.2019, https://tools.ietf.org/html/rfc6145.

Lord, T. 2011. Vint Cerf Answers Your Questions About IPv6 and More. Cited 1.5.2019, https://interviews.slashdot.org/story/11/10/25/1532213/vint-cerf-answers-your-questions-about-ipv6-and-more.

Mawatari, M., Kawashima, M. & Byrne, C. 2013. 464XLAT: Combination of Stateful and Stateless Translation. Cited 1.5.2019, https://tools.ietf.org/html/rfc6877.

Mockapetris, P. 1987. Domain names - implementation and specification. Cited 1.5.2019, https://tools.ietf.org/html/rfc1035.

Nordmark, E. 2005. Basic Transition Mechanisms for IPv6 Hosts and Routers. Cited 1.5.2019, https://tools.ietf.org/html/rfc4213.

Norman, J. 2019. Licklider Describes the "Intergalactic Computer Network". Cited 1.5.2019, http://www.historyofinformation.com/detail.php?entryid=1029.

Omar, K. 2018. Internet Protocol version 10 (IPv10) Specification. Cited 1.5.2019, https://tools.ietf.org/html/draft-omar-ipv10-11.

Oreskovic, A. 2014. Google to acquire Nest for $3.2 billion in cash. Cited 1.5.2019, https://www.reuters.com/article/us-google-nest/google-to-acquire-nest-for-3-2-billion-in-cash-idUSBREA0C1HP20140113.

Postel, J. 1977. Comments on Internet Protocol and TCP. Cited 1.5.2019, https://www.ietf.org/rfc/ien/ien2.txt.

Postel, J. 1981. NCP/TCP transition plan. Cited 1.5.2019, https://tools.ietf.org/html/rfc801.

Postscapes 2018. Internet of Things (IoT) History. Cited 1.5.2019, https://www.postscapes.com/internet-of-things-history/.

Powers, J. 2014. January 1, 1983: ARPANET Switches TCP/IP. Cited 1.5.2019, https://dayintechhistory.com/dith/january-1-1983-arpanet-switches-tcpip/.

Silverman, J. 2014. What's wrong with IPv4 and Why we are moving to IPv6. Cited 1.5.2019, https://www.tecmint.com/ipv4-and-ipv6-comparison/.

Stretch, J. 2011. Alternative to IPv6 in the Works. Cited 1.5.2019, http://packetlife.net/blog/2011/apr/1/alternative-ipv6-works/.

Swartz, J. 2014. Q&A with Stephen Hawking. Cited 1.5.2019, https://eu.usatoday.com/story/tech/2014/12/02/stephen-hawking-intel-technology/18027597/.

Thomas, G. 1999. Introduction to the Internet Protocol. The Extension, 1(4), 2.

Troan, O. & Carpenter, B 2015. Deprecating the Anycast Prefix for 6to4 Relay Routers. Cited 1.5.2019, https://tools.ietf.org/html/rfc7526.

USC Information Sciences Institute 1981. Internet protocol. Cited 1.5.2019, https://tools.ietf.org/html/rfc791.

USC Information Sciences Institute 1981. Transmission control protocol. Cited 1.5.2019, https://tools.ietf.org/html/rfc793.

Vyncke, E. 2019. Projection of IPv6 %-age of IPv6-Enabled Web Browsers (courtesy Google) in World Wide. Cited 1.5.2019, https://www.vyncke.org/ipv6status/project.php?metric=p&country=ww.