ANALYSIS OF THE LOADS AND DIFFICULTIES IN IPV4 TO IPV6 TRANSITION

MASTER THESIS

SERAP REİSOĞLU

MAY 2014

ANALYSIS OF THE LOADS AND DIFFICULTIES IN IPV4 TO IPV6 TRANSITION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ÇANKAYA UNIVERSITY

BY

SERAP REİSOĞLU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF COMPUTER ENGINEERING

MAY 2014

Title of the Thesis: **Analysis of the Loads and Difficulties in IPv4 to IPv6 Transition**

Submitted by **Serap REİSOĞLU**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Murat SARAN
Acting Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Reza ZARE HASSANPOUR
Supervisor

Examination Date : 29.05.2014

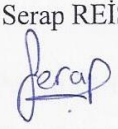
Examining Committee Members

Prof. Dr. Mehmet Reşit TOLUN	(Aksaray Univ.)	
Assist. Prof. Dr. Abdül Kadir GÖRÜR	(Çankaya Univ.)	
Assist. Prof. Dr. Reza ZARE HASSANPOUR	(Çankaya Univ.)	

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Serap REİSOĞLU

Signature : 

Date : 29.05.2014

ABSTRACT

ANALYSIS OF THE LOADS AND DIFFICULTIES IN IPV4 TO IPV6 TRANSITION

REİSOĞLU, Serap
M.Sc., Department of Computer Engineering
Supervisor: Assist. Prof. Dr. Reza ZARE HASSANPOUR

May 2014, 73 Pages

This thesis focuses on analysing of the loads and difficulties in IPv4 to IPv6. Due to the depletion of the IPv4 addresses, IPv6 transition is inevitable. Therefore all parties especially network providers, ISPs (Internet Service Providers), hardware manufacturers, software developers and goverments need to prepare itself to this transition. In this thesis obligations of all parties before and after the transition and difficulties of the transition are described in details.

At the end of research activities, it is understood that IPv6 transition will be slow about five years. After this five-year period, it is expected that there will be a further speedup of IPv6 transition and IPv6 traffic will be reach more than 50% of total traffic.

Keywords: IPv6 Transition, Loads of IPv6 Transition

ÖZ

IPV4'TEN IPV6'YA GEÇİŞİN YÜKLERİNİ VE ZORLUKLARININ ANALİZİ

REİSOĞLU, Serap
Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi: Yrd. Doç. Dr. Reza ZARE HASSANPOUR

Mayıs 2014, 73 Sayfa

Bu tezde IPv4'ten IPv6'ya geçişin yükleri ve zorlukları analiz edilmiştir. IPv4 adreslerinin tükenmesi nedeniyle IPv6 geçişi kaçınılmaz olmaktadır. Bu nedenle bütün tarafların özellikle altyapı sağlayıcılar, internet servis sağlayıcılar, donanım üreticileri, yazılım geliştirenler ve hükümetlerin kendilerini bu geçişe hazırlaması gerekmektedir. Bu tezde tüm tarafların geçiş öncesi ve sonrası yükümlülükleri ve geçişin zorlukları detaylıca anlatılmıştır.

Yapılan incelemeler neticesinde, IPv6 geçişinin yaklaşık 5 yıl süresince yavaş ilerleyeceği anlaşılmaktadır. Bu 5 yıllık sürenin ardından, IPv6 geçişinde hızlanmanın olacağı ve IPv6 trafiğinin toplam trafiğin yarısından fazlasına ulaşacağı değerlendirilmektedir.

Anahtar Kelimeler: IPv6 Geçişi, IPv6 Geçişinin Yükümlülükleri

ACKNOWLEDGMENTS

The author wishes to express her deepest gratitude to her supervisor Assist. Prof. Dr. Reza ZARE HASSANPOUR for their guidance, advice, criticism, encouragements and insight throughout the research.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

IPv4	Internet Protocol Version4
IPv6	Internet Protocol Version6
NAT	Network Address Translation
IPng	Internet Protocol Next Generation
QoS	Quality of Service
MTU	Maximum Transmission Unit
TTL	Time-to-Live
ISPs	Internet Service Providers
IPSec	Internet Protocol Security
AH	Authentication Header
ESP	Extension Header
ICMPv6	Internet Control Message Protocol Version6
ARP	Address Resolution Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
IGD	Internet Gateway Device
GRE	Generic Routing Encapsulation
DSTM	Dual-stack Transition Mechanism
TEP	Tunnel End Point
PT	Protocol Translation
CGN	Carrier Grade NAT
FIB	Forwarding Information Base
RIB	Routing Information Base
SPF	Shortest Path First
IXPs	Internet eXchange Points
OS	Operating System
HA	High Availability

VRRP	Virtual Router Redundancy Protocol
OSPF	Open Shortest Path First
ACS	Auto-Configuration Server
BGP	Border Gateway Protocol
NTP	Network Time Protocol
SLA	Service Level Agreements
ICPs	Internet Content Providers
CDN	Content Delivery Network
ICT	Information and Communication Technologies
CPE	Customer Premises Equipment
ULA	Unique Local Address
RA	Router Advertisement
DAD	Duplicate Address Detection
NUD	Neighbor Unreachability Detection
RIP	Routing Information Protocol
APIs	Application Programming Interfaces
PMTU	Path Maximum Transmission Unit
USAGI	Universal Playground for IPv6
IKE	Internet Key Exchange

CHAPTER 1

INTRODUCTION

The number of devices connected to the internet is growing incredibly day by day and Internet Protocol Version4 (IPv4) addresses are not enough for this demand. Due these IPv4 addresses running out, the Internet Protocol Version6 (IPv6) transition is inevitable. The aim of my thesis is searching the loads and difficulties in the transition to IPv6. I researched the challenges of transition and transition needs to be deal with individually. In order to gather the necessary information for my thesis I did lots of research. In addition to this research I also created a survey to find out companies opinions about the transition to IPv6. The results of this survey were very useful for my thesis.

1.1. Problem Definition and Motivation

Technology is changing everyday. Nearly sixty years ago main frames were used and number of main frames were very few. Then desktop are started to use and the numbers of the desktops were more than number of the main frames. Nearly thirty years ago mobile devices were started to use. Nowadays the number of the mobile devices are very very huge. And generally most of the them are used for connecting internet. For connecting all devices to the internet there must be enough IP addresses for these devices. Consequently, IPv4 address space are not enough for these demands. Therefore transition to IPv6 is needed because IPv6 has very huge IP address space which can meet these demands very easily.

Transition to IPv6 is needed but transition is not a easy operation. Many issues about transition must be well thought and evaluated. And transition has also costs which

are changing accourding to organizations or companies. Beside that all staff in a organization or company must be very well trained and informed. For robust and easy transition, education of staff are very important issue. Also there should be dedicated team in a company for following the all steps of the transition.

1.2. Scope of the Thesis

Task and loads of organizations for transition to IPv6 are discussed in this thesis. In addition to this, some difficulties and problems may be encountered in the transition to IPv6 are explained. But the solutions for those problems and difficulties are not mentioned in this thesis only some recommendations are given to organizations for IPv6 transition.

CHAPTER 2

OVERVIEW TO IPV6

2.1. General Information for IPv6

The number of devices with internet connections are rapidly increasing. There are a lot of computers, laptops, more than a billion mobile phones, smart phones and other wireless devices in the world which are nearly 4.3 billion in number. Each of these devices require its own IP address for internet connections. The huge growth of the number of devices has brought the need for a new protocol which has more addresses than IPv4 because of impending exhaustion of IPv4 addresses. This big demand for IP addresses speeds up the development of the large address space offered by the IPv6. If there is no a new protocol like IPv6, we need to do Network Address Translation (NAT) for providing addresses to hosts which has several problems like hiding multiple hosts behind pool of IP addresses. IPv6 contains addressing and control information to route packets for the next generation Internet. Therefore IPv6 is also named Internet Protocol next generation (IPng).

IPv6 is a new protocol for the Internet. Basic version of IPv6 was introduced in 1994. It has since seen a number of enhancements, such as the addition of mobile IPv6 specifications in 2004. IPv6 has a lot of different features and advantages according to IPv4. IPv4 and IPv6 are both used for communication within the network.

IPv6 is documented in several RFCs which are started from RFC 2460. However IPv6 is newer protocol from IPv4, both protocol will be exist at the same for the Internet in coming years [1].

2.2. IPv6 Features

IPv6 has many more features than IPv4. With these feautes IPv6 is more comprehensive than IPv4 and this way IPv6 will respond better to the future needs of ISPs, network providers, internet users and so on. These new features that come with IPv6 are listed below:

- Different header format
- Large address space
- More efficient routing
- Stateless and stateful address configuration
- Built-in security
- Improved quality of service (QoS)
- New protocol for neighboring
- Extensibility

2.2.1. Different Header Format

IPv4 header fields are shown in Figure 1. There are 13 fields in IPv4 header.

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

Figure 1 : IPv4 Header Format

Samples for IPv4 header:

45 00 00 44 ad 0b 00 00 40 11 72 72 51 c0 02 e2 51 c0 00 10

Version: 4

IHL: 5 (20 bytes)

TOS: 0x00

Total Length: 0x0044 (68 bytes)

Identificaton: 0xad0b

Flags: 0x00

Fragments: 0x00

TTL: 0x40 (64 hops)

Protocol: 0x11 (UDP)

Header Checksum: 0x7272

Source Address: 0x51c008e2 (81.192.8.226)

Destination Address: 0x51c00010 (81.192.0.16) [2]

IPv6 header fields are shown in the Figure 2. IPv6 looks like more simple than IPv4 header.

<table>
<tr><td>Version</td><td colspan="2">Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

Figure 2 :IPv6 Header Format

Samples for IPv6 header:

60 00 00 00 00 28 06 40 20 04 15 e8 16 2e 00 00 02 d0 08 ff fc c3 e8 12 20 04 15 08 19 28 17 c0 00 00 00 00 00 00 00 02

Version: 6
Traffic class: 0x00000000
Flow Label: 0x00000000
Payload Length: 40
Next Header: TCP (6)
Hop Limit: 6
Source Address: 2004:05e8:162e:0:102d:0:2d0:0:2d0:8ff:fcc3:e812
Destination Address: 2004:1508:1928:17c0::2 [3]

Some of the fields in IPv4 header have been removed from IPv6 header which are listed below:

- Header length
- Header Checksum
- Identification
- Flags
- Fragment Offset

Header length has been removed in IPv6 because it is unnecessary for a header with a fixed length.

To improve processing speed of the routers, the Header Checksum field was removed. In other words router processing becomes much faster if routers do not have to check checksums and update checksums.

Fragmentation is the process of splitting a packet into smaller pieces, in case a large packet has to be sent over a network supporting only smaller packet sizes. Fragmentation is handled by the IPv4 router. The destination host is responsible for collecting and reassembling the packets. However, in case one of the packets is missing, or there has been an error with the transmission of a packet, the packets have to be retransmitted, which makes IPv4 less efficient. In IPv6, before the transmission, there is a procedure which is named Path MTU Discovery that is used for learning the Path Maximum Transmission Unit (MTU) size by hosts; hence costs

for the routing process are reduced. If a fragmentation is needed, an extension header will be used. In contrast to IPv4 routers, IPv6 routers do not provide any fragmentation. So, the Identification, Flags, and Fragment Offset fields were removed from the IPv6 header.

Traffic Class field replaces the Type of Service field because IPv6 has a different way of handling preferences. The Time-to-Live (TTL) and the Protocol Type fields were renamed and also modified. A new field is introduced, called Flow Label. It can be used to tag packets of a specific flow to differentiate the packets at the network layer.

According to the these differences IPv6 header is simpler than IPv4 header. And it is more efficient than the IPv4 header which can be reduce header overhead.

2.2.2. Large Address Space

The size of an address in IPv6 is 128 bits destination and source addresses, which is four times larger than an address in IPv4. IPv4 uses a 32-bit address space allows for 4,294,967,296 possible addresses. IPv6 uses a 128-bit address space allows 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×1038) possible addresses. The large address space of IPv6 can provide multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization.

With a huge number of available addresses, there will be no address depletion problem and address-conservation techniques like NATs are no longer necessary. And ISPs (Internet Service Providers) will have enough IP addresses to give their all customer so that every device which need IP address can give unique IP address without any scarcity of IP addresses [4].

2.2.3. More Efficient Routing

IPv6 header size is bigger than IPv4 header size but IPv6 header is more simple than the header of the IPv4. Some fields in IPv4 which are not used frequently are moved to the extensions part of the IPv6. Therefore this simplicity, IPv6 packet processing is more efficient. And in IPv6 there is no fragmentation in router side, it is done by source device. For these reasons we can say that IPv6 has a more hierarchical and more efficient routing infrastructure according to IPv4. And we can add that backbone routers which are on the IPv6 Internet have smaller routing tables with compared to IPv4.

2.2.4. Stateless and Stateful Address Configuration

IPv6 supports both stateless address configuration and stateful address configuration to simplify configuration of hosts. Hosts configure themselves with stateless address configuration automatically.

2.2.5. Built-in Security

Internet Protocol Security (IPsec) is a mandatory component for IPv6 but in IPv4 it is optional. IPsec is implemented with the authentication header (AH) and the extension header (ESP) in IPv6. The AH provides authentication of the source and integrity. And AH can provide protection towards replayed packets optinal. Beside that ESP header provides source authentication, confidentiality, antireplay, limited traffic flow confidentiality and inner packet connectionless integrity. Beside that after using IPv6 there is no need to NATs which is not very secure and it is used generally in IPv4 networks because of the depletion of the IP addresses [5].

2.2.6. Improved Quality of Service (QoS)

There are new fields in the header of IPv6 which is used for how traffic is indentified and handled. Traffic identification provides special handling for packets that belong to a flow which is a series of packets between a destination and source and it allows routers to identify by using a Flow Label field in the IPv6 header. Thats why the traffic is identified in the IPv6 header, support for QoS can be easily obtainable even the packet payload is encrypted with IPSec. And there is a traffic class field in IPv6 which is 8-bit and used for distinguishing packets from different classes or priorities [5].

Traffic shaping, packet classification, queueing, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets features which are used for QoS are supported in IPv6 networks. With these features IPv6 is more successful about QoS than IPv4. After the number of the addresses, QoS features is one of the most important features of IPv6 with compared to IPv4.

2.2.7. New Protocol for Neighboring

In IPv6, The Neighbor Discovery protocol is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage neighboring nodes interaction. There are ICMPv4 Router Discovery, Address Resolution Protocol (ARP) and ICMPv4 Redirect messages in IPv4 instead of Neighbor Discovery in IPv6. Neighbor Discovery in IPv6 can do the work of three protocols in IPv4 with efficient unicast and multicast messages. And it provides extra good functionality [5].

2.2.8. Extensibility

By adding extension headers after the IPv6 header, IPv6 can be extended for new features. In the future this extension can be used comfortably for new goals. On the other hand in IPv4 header, there is a only 40 bytes of options area. This size is

smaller than IPv6. Because the size of IPv6, extension headers can be grow until the size of the IPv6 packet. Therefore IPv6 is more extensible then IPv4.

CHAPTER 3

IPv6 CONCEPTS

3.1. IPv6 Address Format

IPv6 address is 128 bits long (16 bytes). The format of the IPv6 address is yyyy:yyyy:yyyy:yyyy:yyyy:yyyy:yyyy:yyyy (y is a hexadecimal digit, representing with 4 bits.). The double colon (::) can be used once in the text form of an address, to designate any number of 0 bits. Leading zeros can be omitted as IPv4.

3.2. IPv6 Address Types

There are three types of addresses in IPv6. First is unicast, second is multicast and last is anycast addresses.

1- The unicast address defines a single interface. An IPv6 packet sent to a unicast address is delivered to the network interface identified by that address. There are two types of unicast addresses. First is link-local address. This address is planned for use on a single local link. The fe80::/10 prefix is used for a link-local address. Second unicast type is global address. This address is planned for use on any network. The prefix is used for a global address starts with binary 001.

2- The anycast address is assigned to a set of interfaces, usually belonging to different locations. A packet goes only to the nearest insider of the group which sent to anycast address.

3- The multicast address defines a group of interfaces, possibly at multiple locations. The ff is the prefix for multicast address. If a packet is sent to a multicast address, copy of the packet is delivered to all member of the group.

3.3. Neighbor Discovery

There are many tasks performed under neighbor discovery. Hosts and routers communicate with each other with neighbor discovery. It is used for identifying layer 2 addresses of nodes which are on the same link and finding neighboring routes that can forward packets and keeping track of reachable neighbors.

IPv6 nodes use five Internet Control Message Protocol version 6 (ICMPv6) messages to communicate with other nodes are listed below:

1- Router advertisement: These messages are sent by routers periodically or these are answer to the router solicitation. The information which is provided by router advertisements is used to create global interfaces automatically by hosts and associated routes. Other information like hop limit and maximum transmission unit are also provided by router advertisements.

2- Router solicitation: These messages are sent by host to request routers to generate router advertisements. When the host first becomes available on the network than initial router solicitation is send by host.

3- Neighbor solicitation: These messages are sent by nodes to determine neighbor link layer address or to verify a neighbor is reachable yet.

4- Neighbor advertisement: These messages are sent by nodes in response to a neighbor solicitation. Or it can be in response to as an unsolicited message to announce an address change.

5- Redirect: These messages are used for routers to inform hosts of a better first hop for a destination [6].

3.4. Stateless Address Autoconfiguration

IPv6 hosts or routers use to automatically configure IPv6 addresses with a process which is called stateless address autoconfiguration. The node builds different IPv6 addresses by combining an address prefix with either an identifier derived from the MAC address of the node or a user-specified interface identifier. The prefixes contain link-local prefix (fe80::/10) and local IPv6 routers advertised prefixes of length 64 if any exist.

The node makes duplicate address discovery for verifying matchlessness of the address before assigning this address to an interface. Firstly the node sends out a neighbor solicitation query message to the new address and waits for a response for this message. If there is no response, then the address is assumed to be unique. If there is a response for neighbor solicitation query message, it means that the address is already in use. If a node determines its temporary IPv6 address is not unique, then autoconfiguration stops and at that time interface should be configured manually[6].

3.5. Comparison of IPv6 and IPv4

IPv6 and IPv4 features are generally different from each other. There is a comparison list according the important features on Table 1.

Table 1 : Comparison of IPv6 and IPv4 [6]

Some Features	**IPv6**	**IPv4**
Address Length	128 bits	32 bits
Address Resolution Protocol (ARP)	It is not used directly. It is inside in neighbor discovery using Internet Control Message Protocol for IPv6 (ICMPv6) and stateless autoconfiguration.	It is used for discovering a physical address.
Address types	There are 3 types of address which are multicast, unicast and anycast.	There are 3 types of address which are multicast, unicast and broadcast.
Configuration	It is not mandatory in this internet protocol, it is optinal.	It is mandatory in this internet protocol.
Fragmentation	Fragmentation can be in the source node side in this protocol.	Fragmentation can be done by the sender of packets when the packet is too large for sending.
Domain Name System (DNS)	It is not supported via i5/OS in this protocol.	It is supported via i5/OS in this protocol. And It is used to get IP dynamically.
Internet Control Message Protocol (ICMP)	Is is supported in this protocol with new options.	It is supported in this protocol for communicating the network information.

Table 1 (Continue)

File Transfer Protocol (FTP)	It is not supported via i5/OS in this protocol.	It is used to communicate with files. It is supported via i5/OS in this protocol.
LAN connection	It is supported in this protocol for connecting to physical network.	It is supported in this protocol for connecting to physical network.
Loopback address	It is a virtual physical address that is used for host itself which is supported in this protocol.	It is supported in this protocol, too.
Network Address Translation (NAT)	There is no depletion of the ip addresses in the IPv6 therefore it is not supported in this protocol.	It is used for address translation. Because of the depletion of the ip addresses in IPv4 it is supported in this protocol.

3.6. Advantages of IPv6 versus IPv4

The huge growth of the Internet usage has shown its importance accourding to government, businesses, academics and all individual users in recent years. Sometimes people do not tolerate even a five minute internet outage because Internet plays an important role in many people's life. At that time IPv6 has a important role because IPv6 will greatly increase the size and range of devices connected to the Internet, the benefit of the network effect will increase accordingly. This benefit is one of the most important advantages of IPv6 over IPv4. The problems of the IPv4 are known when the stage of developing the IPv6. The major parts of the problems in IPv4 are solved by IPv6. Some problems which are solved with IPv6 are listed below:

1- Lack of Public and Private Address in IPv4: In IPv4 there is a limitation about address spaces. Therefore in IPv4, there are two different addressing types. First type is used for the enterprise networks and the other type is using for home networks.

In an enterprise network there might be public, private or both types of addresses. However, the private and public IPv4 address spaces are individual and they do not provide symmetric reachability. Symmetric reachability can be done when packet can be sent to and received from any destination. With IPv4, there is no single addressing type therefore there should be an intermediate device which can do NAT for connectivity between public and private networks.

In the home network, an Internet Gateway Device (IGD) like modem gets a single public IPv4 address and it assings private IPv4 addresses to the hosts behind of it which are on that home network. This IGD has NAT ability and it converts private addresses to public addresses and public addresses to private ones. With IPv6, there is no limitation of the ip addresses. Therefore both enterprises and homes can be assigned global address prefixes.

2- Restores End-to-End Communication Problem: For address depletion of the IPv4 sometimes NATs can be needed and can be used in IPv4. At that time there is a technical problem with NATs for applications which place reliance on listening or peer based connectivity. Because these applications need peers to discover and advertise their public IPv4 addresses and ports for communicating. On the other hand there is no depletion of address problems in IPv6 and it means that NATs are not needed in IPv6 networks. This means that end-to-end communication problem can disappear with IPv6.

3- The International Address Allocation Problem: Public address prefixes are appointed to regional Internet registries and then assign address

prefixes to other ISPs and organizations based on rightful need with IPv6 unlike the method described in IPv4. This new address allocation method comes with IPv6 which provides that address prefixes will be distributed globally based on regional connectivity needs different from the method which is used in IPv4. This new method provides a gain to the business because organizations can count on having available public IPv6 address space without the current cost of getting IPv4 public address prefixes from their ISP.

4- More Efficient Forwarding in IPv6: IPv4 has more fields to process than IPv6 and more decisions to make in forwarding packet than IPv6 therefore IPv6 is more aerodynamic and faster than IPv4. Header of the IPv6 is fixed size which is 40 bytes and allows routers to process IPv6 packets faster. In addition to that, the hierarchical addressing structure of IPv6 addresses express that the routing tables of Internet backbone routers have less routes to analyze according to IPv4. Consequently traffic can be forwarded at higher data rates in IPv6.

5- IPv6 Has Support for Security and Mobility: IPv6 has been designed to support security which is called IPsec and mobility which is called Mobile IPv6. IPv4 also supports these features but they are included in IPv4 as extensions. Therefore there are limitations in security and mobility about architectural or connectivity. These limitations might not have been present if they were known in the developing stage of the IPv4. Both security and mobility are known in the developing stage of the IPv6 therefore there can be standards defined in IPv6 according to these features. These IPv6 standards have fewer limitations about security and mobility and unlike IPv4, they are more scalable and robust to handle the current and future communication needs of the users of the Internet. The business benefit is that IPv6 can protect packets from end to end across the entire IPv6 Internet. IPsec on the IPv6 Internet is fully functional between any two endpoints.

6- IPv6 Uses Scoped Addresses and Address Selection: Unlike IPv4 addresses, IPv6 addresses have a scope which is unique and relevant. And there are two types of addresses in IPv6. First one is unique local address which is nearly equivalent to the IPv4 private address and the second is global address which is equivalent to the IPv4 public address. IPv6 router is aware of the scope of IPv6 addresses and it will never forward a packet over an interface which does not have the correct scope. But in general, IPv4 routers do not separate a public address from a private address and it will forward a privately addressed packet on the Internet [7].

These abilities of IPv6 are mentioned above can be the most important reasons for the transition to IPv6. In brief, it has very large address space, advanced security and mobility, more efficient routing and address selection mechanisms in IPv6 with compared to IPv4. The problems about restoring end-to-end communication and internal address allocation will be solved with IPv6 new features.

CHAPTER 4

TRANSITION MECHANISM TO IPv6

Transition from IPv4 to IPv6 in an instant time is not possible because the number of users and the volume of the Internet are very big. On the other hand, many businesses and organizations are becoming more and more dependent on the Internet for all their work and therefore they cannot tolerate downtime for the migration of the new IP protocol. As a result, there will not be one day on which IPv4 will be turned off and IPv6 turned on. Before the transition all the parts of the network should be checked for defining which method should be appropriate for that network. Beside that there should be very detailed transition plan. For eliminating the need to configure IPv6 hosts manually, IPv4 to IPv6 network migrating must be applied node by node with using autoconfiguration procedures. In this way, users can instantly benefit from the features of IPv6 at the same time communicating with IPv4 users [8]. There are few technologies which can be used in leery, controlled and smooth transition from IPv4 to IPv6. These transition techniques are listed below:

4.1. Tunneling Technique

Tunneling basically means that IPv6 packets are placed inside IPv4 packets, which are routed through the IPv4 routers. In other words we can say that IPv6 packet is encapsulated into IPv4 packet and it goes from source to destination where it is decapsulated and retransmitted. This technique has the ability to be used in an existing IPv4 routing infrastructure to carry IPv6 traffic. Tunneling mechanism provides a better solution where users' data can pass through a non-supported IP version.

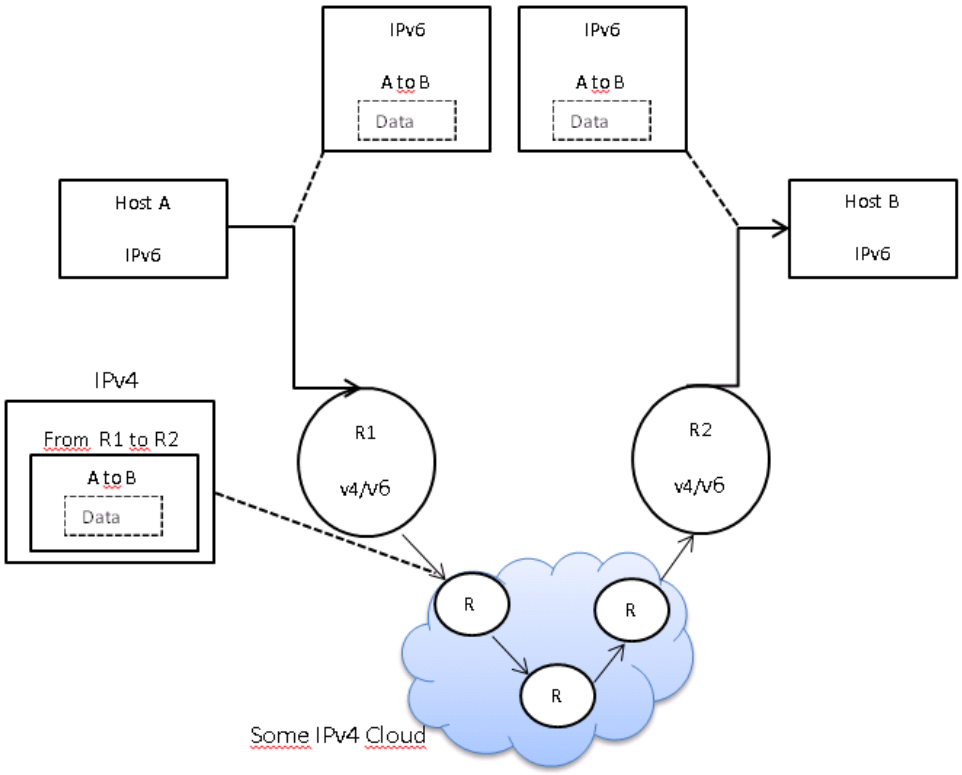


Figure 3 : Tunneling Technique

The Figure 3 is shown tunneling technique. Different tunneling methods exist in IPv6 are listed below:

1- Manual IPv6 Tunnels: Manual tunnels mean that IPv6 tunnel is configured manually between two routers that each must support both IPv6 and IPv4. A manually configured tunnel has explicitly configured IPv4 addresses for the tunnel source and destination.

2- Automatic Tunnels: Automatic tunneling refers to the routing infrastructure that automatically determines the tunnel endpoints. Automatic tunnels are configured by using IPv4 address data embedded in an IPv6 address. And destination host IPv6 address includes information about which IPv4 address the packet should be tunneled to.

3- 6to4 Tunnels: These types of tunnels allow IPv6 to be tunneled over IPv4. This method is automatically set up using the 2002::/16 IPv6

address space and designed for site-to-site and site to existing IPv6 network connectivity. IPv4 address is embedded in an IPv6 address and embedded IPv4 address allows discovery of tunnel endpoints.

4- IPv4 Compatible Tunnels: This tunneling mechanism is like to 6to4 tunneling and allows IPv6 over IPv4 tunneling. The major distinction between them is how the IPv4 address which is used by the edge device is embedded in the IPv6 address.

5- IPv6 rapid deployment: This mechanism is similar with 6to4 but it allows the implementer to use the IPv6 block that was assigned to it.

6- Generic Routing Encapsulation (GRE) IPv6 tunnels: GRE is a protocol which is used for IPv6 tunneling operations and it can be used to tunnel IPv6 over IPv4 or IPv4 over IPv6. GRE configuration is very similar with the configuration of the manual tunnels. Both the destination and source must be manually configured in GRE tunnels and each of them must support both IPv6 and IPv4.

Those who choose the tunneling technique for transition can choose one of the six tunnels are mentioned above acourding to their needs, networks and budgets. It is seen that currently 6to4 tunnels are the most deployed tunnels.

4.2. Dual-Stack Technique

The dual-stack technique or also called dual-stack transition mechanism (DSTM) is that all devices interoperate with IPv4 devices using IPv4 packets, and with IPv6 devices using IPv6 packets. In other words, the dual-stack technique is basically using IPv4 and IPv6 addresses in parallel. All connections and devices like routers, end-user devices and other infrastructure devices are dual stacked and they can communicate over both IPv4 and IPv6. This transition technique is the most

preferred technique especially according to the network providers and ISPs. Nowadays a lot of IPv6 implemantations are used dual-stack approach.

The major assumption within DSTM is that DSTM is fully transparent to applications because it can continue to work with IPv4 addresses. Also, it is transparent to the network, which carries only IPv6 packets. The other assumptions in DSTM architecture are listed below:

1- The DSTM domain is within an Intranet and it is not on the Internet.

2- The DSTM server allocates the temporary IPv4 address and different protocols like DHCPv6 can be used to assign the IPv4 address.

3- Except temporarily communication with IPv4 applications, dual stack IPv6/IPv4 nodes do not maintain IPv4 addresses.

4- DSTM uses IPv6 routing and it will keep IPv4 routing tables to a minimum. With DSTM dominant IPv6 network, DSTM will reduce the network management required for IPv4 during transition.

5- Dynamic tunneling is used to encapsulate the IPv4 packet within the IPv6 packet once IPv6 nodes have obtained IPv4 addresses. After that packet is forwarded to an IPv6 tunnel end point (TEP) DSTM border router, where the packet will be decapsulated and forwarded using IPv4. In addition to manual configuration, the IPv4 allocation mechanism, from the DSTM server, can provide the TEP IPv6 address to the DSTM client.

6- In DSTM, existing nodes and IPv4 applications do not have to be modified [9].

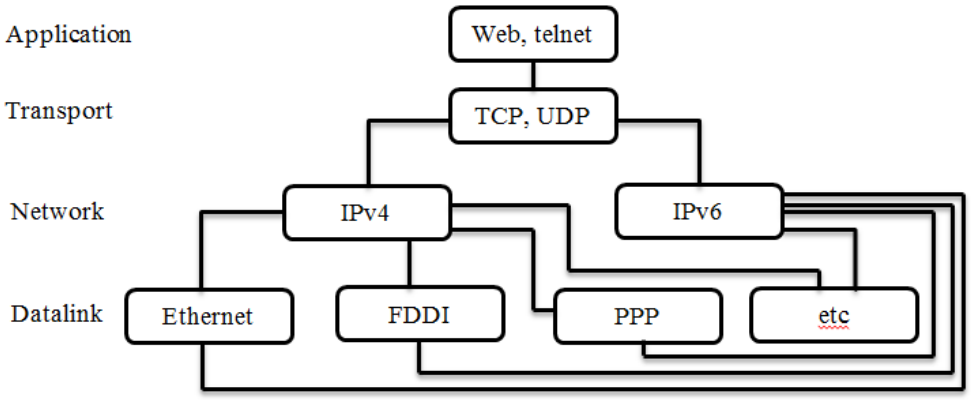


Figure 4 : Dual-Stack Technique

Figure 4 shows the basic dual-stack technique. In the dual-stack technique, subsets of both routers and hosts are upgraded for IPv6 support, in addition to IPv4. If the upgraded nodes want to communicate with IPv4-only nodes at that time they always do it by using IPv4. If the upgraded nodes want to communicate with IPv6-only nodes at that time they can do it by using IPv6.

4.3. Translation Technique

For translating IPv6 traffic to IPv4 traffic or IPv4 traffic to IPv6 traffic the translation technique is used. In this translation technique, the traffic is converted to the destination type. There is no traffic encapsulation here.

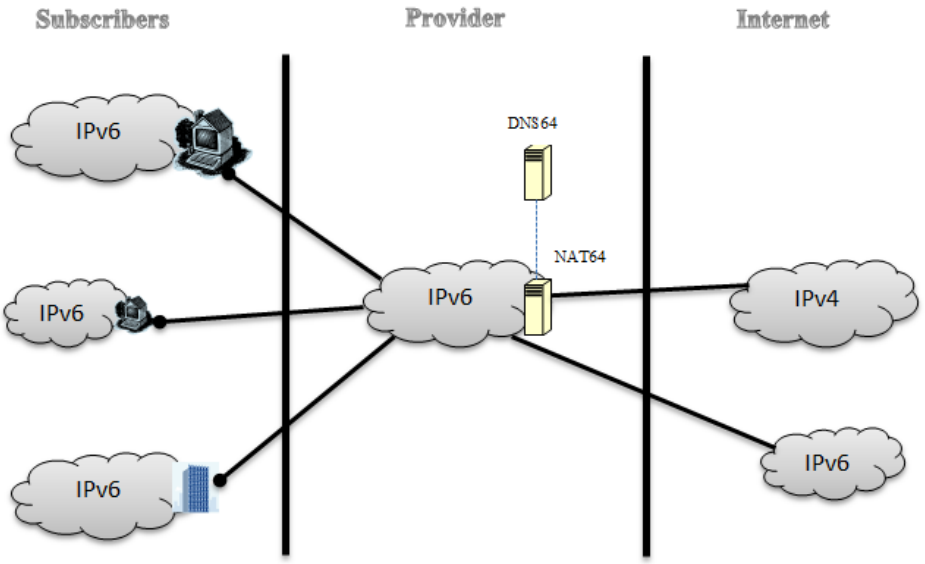


Figure 5 : Translation Technique

Figure 5 shows the basic translation technique. There are two methods that are typically used with translated IPv6 networks which are listed below:

1- NAT-PT (Protocol Translation): This technique has the ability to either dynamically or statically configure a translation of the IPv4 network address into the IPv6 network address and vice versa. It provides bi-directional connectivity between IPv4 and IPv6 networks. NAT-PT executes statefull packet translation between internal IPv6 hosts any external IPv4 hosts.

2- NAT64: This technique allows IPv6 hosts to communicate with IPv4 servers. NAT64 uses IPv4 address pool to represent IPv6 nodes. When NAT64 is deployed, both stateful and stateless options are offered [10].

4.4. 6-Bone

6-Bone is a virtual network layer on IPv4 internet for providing the routing of IPv6 packets because some routers can not control the routing of IPv6 packets correctly. In this technique, there is a virtual point-to-point tunnel for IPv6 direct connectivity.

The 6bone can provide the early policy and procedures which can be useful for the IPv6 transport [11].

CHAPTER 5

CHALLENGES AND DIFFICULTIES IN TRANSITION TO IPv6

The biggest difficulty in transition to the IPv6 protocol is that IPv6 is mostly incompatible with the IPv4 protocol. The target plan for a IPv6 network should be built in parallel with the existing IPv4-based internet. This plan requires everyone on the Internet to get a separate IPv6 address. This address will only be able to communicate with other IPv6 addresses, so each user will also still need an IPv4 address to communicate with those who do not have IPv6 addresses at that time.

5.1. Co-Existence of IPv6 and IPv4

Transition and deployment of IPv6 needs to have a long term plan and well designed coordination. Planning stage is very important. Every parts of transition should be determined and all transition step should be detailed before the deployment stage.

IPv6 protocol is not backwards compatible with IPv4 protocol. Both protocol must be deployed or there must be tunneling or translation mechanism between them. IPv4 will need to be supported beside IPv6 for a considerable part of time. This is the most difficult issue about transition to IPv6. Because co-existence of both protocol is not easy. During this co-exintence time, there will be some problems which are listed below:

1- Complexity of operation: There is a single network with two address families. At that time management will be more complex and difficult because IPv4 and IPv6 address families are in the same network. And

network operators must be more careful and precise because of this complexity.

2- Complexity of troubleshooting: Running two address families and/or tunnels is assumed to be more complex. There are a lot of device some of them support IPv4 some of them support IPv6 and some of them support both of the internet protocols. On this complex network detecting problems and solving problems are very hard issues.

3- Breaks end-to-end connectivity in IPv4: Subscribers sharing a Carrier Grade NAT (CGN) will have little to no hurdles in their communication. Several CGN will experience some application issues or subscribers separated by one.

5.2. Dual-Stack Transition Mechanism Difficulties

DSTM is a transition technique and it does not specify a protocol. DSTM uses only existing protocols. However, the features of the temporary addresses allocation methods and behavior of the server, client and border router are defined by the DSTM.

IPv6 datagram can be copied into the data field of the IPv4 datagram and convenient address mapping can be done in the dual stack transition mechanism. But some of the fields in IPv6 have no counterpart in IPv4 when the IPv6 datagram mapped into IPv4 datagram. The info in these fields will be lost. When the datagrams travel network throughly and arrive in IPv6 host, that datagram do not include all fields of the original IPv6 datagram which is sent from source [12].

Asymetric paths are not supported in DSTM. Returned IPv4 packets must enter the IPv6 cloud through the same dual-stack tunnel end point who maintains the association. Initial delay may be excessive for real time traffic.

The last difficult situation is that some implementation defined software must be ready to support DSTM. DSTM server implementation is the first software that needs to be ready. This software is required to maintain configuration information about TEPs for encapsulating IPv4 packets between IPv6 nodes. DSTM client implementation is the second needful software which is required to support the dynamic tunneling mechanisms. The last needful one is DSTM border router implementation which is required to support the decapsulation of IPv6 packets from DSTM clients [11].

5.3. Size of Routing Tables

Routing table size has been a major case for IPv6 protocol. IPv6 addresses are 4 times larger in bit width than IPv4. It means routing table size of IPv6 is bigger than IPv4. This bigger size of the routing table has negative impacts on IPv6. This size has negative effects on router memory usage and routing table lookup performance. Negative effects of the routing table growth on hardware are listed below:

- Consumes forwarding memory (Forwarding Information Base (FIB))
- Consumes routing memory (Routing Information Base (RIB))
- Affects forwarding rate (FIB lookup as a function of memory speed and size)
- Affects convergence (Shortest Path First (SPF), RIB rewrite, RIB to FIB population)

5.4. Content and Latency

According to the end user, the important issue is to reach IPv6 content. Currently there is not much Internet content available via IPv6. Content providers must focus on this subject. They should increase the IPv6 contents. But the time is very important. Content provider should have completed the preparations for the IPv6 content as soon as possible because IPv6 users are increasing day by day.

The other important issue is latency. Latency is the time needed for a packet to get from one point to another point. In dual-stack network, connection time might be slow. So content providers see latency to be a major barrier for making their content and services available through IPv6. Scarcity of IPv6 peering agreements and Internet eXchange Points (IXPs) supporting IPv6 can increase latency because traffic may have to travel further to reach its destination [13].

5.5. Cost of Transition

Transition from IPv4 to IPv6 has some costs. These costs will contain ongoing operational costs and capital investment costs. If we make the transition step by step at this time every step of transition has its own cost. There can be planning, testing and deploying steps. Total cost of transition can change according to the migration strategy and network needs. It means it will change for users, content providers, internet service providers, network providers, networks, hardware and applications are used on and so on. Costs for transition are listed below:

1- Hardware and software costs: For IPv6 hardware and software updates are needed. In special cases some hardware and software may not be updated and at that time they should be changed with the new ones. There are some steps in order to determine the needs for transition.

   a) First of all, actual network infrastructure should be evaluated for taking inventory of all hardware that cannot be upgraded to IPv6 and the result of this evaluation will result in a major capital investment.

   b) Software needs should be evaluated like hardware needs. First of all, the Operating Systems (OS) should be checked and then the particular applications should be checked. Generally most of the OSs new versions support IPv6 therefore this may not represent a big economic issue. But the applications side is different. It is quite probable that

these particular applications which are organization-wide applications do not support IPv6. Organizations will need additional costs to upgrade these applications to IPv6. It should not be forgotten that sometimes re-programming the software is cheaper than upgrading it.

2- Labor costs: Labor costs are needed for training staff and test, installations and maintainance of IPv6-capable hardware and applications. Labor costs are listed below:

a) R&D (Research and Development) costs: These include basic product design and development costs.
b) Product testing costs: These include testing product interoperability, debugging and other testing costs.
c) Network management software upgrade costs: These are labor costs allocated to network-specific management and monitoring software.
d) Network testing costs: These are costs for testing interoperability between network components with IPv6 capabilities.
e) Installation costs: These are costs for installing IPv6.
f) Staff training costs: These are costs for IPv6 trainng to staff (R&D, technical, sales and marketing staff).

3- Other costs: More security precaution is needed during the transition. And there will be future needs of an organization's network [13].

These costs given above frighten organizations about transition. Therefore some of them are looking for ways to reduce these costs or some of them are delaying the transition much as possible. Transition may be postponed, but it must be done one day.

CHAPTER 6

PROBLEMS WITH TRANSITION TO IPv6

IPv6 has much more benefits according to IPv4. Therefore every organization want to transition to IPv6. But at that time we should say that there are some problems at that transition period. Because Internet protocol change is a major change in Internet. It takes time to solve these transition problems.

6.1. Network Problems

Transition to IPv6 problems are generally for network. Some of these problems can be solved. But new problems may occur with an increase in the use of IPv6.

6.1.1. Address Architecture

IPv6 address space is larger than IPv4 address space. The IPv6 address space allows for many new use cases for address assignments to networks and customers. And IPv6 is intended to maintain a strong hierarchy. Address design of IPv6 is very different from the smaller and fragmented address design of the IPv4. Therefore, extra attention is required when designing the IPv6 network because of the great size of IPv6 address space. Operators will need a very detailed plan for IPv6 which was not needed for IPv4. This detailed plan will provide them to be more careful and make fewer mistakes.

6.1.2. Connectivity

For operators, connectivity of the customer and continuity of services is a very important subject because customers pay money for these services. When the operator begins the transition to IPv6, the network engineers who work in this operator must design a network to offer service continuity to customers. At that time operators first choice is dual-stack which is the natural approach of transition for operators. However, due to the cost for operating dual-stack network and IPv4 address depletion, operators may choose to upgrade part of their network to IPv6-only. They want to know the methodologies and guidelines about this IPv6-only upgrade.

6.1.3. High Availability

The most important requirement for networks is High Availability (HA). IPv4 is quite an old network protocol. Therefore operators have been working on IPv4 networks for many years. Througout these years, operators have gained a lot of experience of operating HA in IPv4. They have used some mature protocols like Virtual Router Redundancy Protocol (VRRP) and Open Shortest Path First (OSPF) Graceful Restart for HA. IPv6 is a new network protocol. Therefore HA in IPv6 is less known compared to IPv4. In addition, new transition methods require new HA models and operators can deploy a transition method easier if HA is supported in this method.

6.1.4. Domain Name Server (DNS) Problems

DNS operation in IPv6 is similar with DNS operation in IPv4 but there are some differences here. The most widely discussed issue in IPv6 is the usage of Reverse DNS. A lot of applications like some implementations of e-mail server rely on Reverse DNS to operate properly. That time operators must find an answer to manage Reverse DNS issue in IPv6. The list of destination addresses in a node is

collected by the DNS name resolver. Regardless of data records internet protocol, DNS queries and responses are sent by using IPv6 or IPv4 for meeting the DNS queries. So far, there does not seem to be a problem with DNS about IPv6. However, problems may arise in the following situations, for instance, if a server application does not support IPv6 yet but it works on a dual-stack hardware for other IPv6 services, and this host is listed with an AAAA record in the DNS, at that time there will be connection failure between the client and the server application. The inconsistency between DNS query result and server application's protocol version tend to cause this state [14].

6.2. CPE Problems

CPE is customer side equipment. There are two problems about CPE in transition to IPv6. First problem is updating the CPE to support IPv6. Some of the CPEs can be updated via Auto-Configuration Server (ACS) or another method but some of them can not updated at all. Customer or operators must change the CPEs which can not updated. Changing CPEs are very expensive, ISPs should think a lot about this issue before the transition.

The other problem is provisioning of the CPE because this issue is very important for operators. Operators must provide a reliable and manageable provisioning system for provisioning of IPv6 service to all their customers. In the world of IPv4, generally most customers are given a public address via DHCP or other methods. Customer CPEs manage the home network and in the home network private address space are used. Now CPE coordinates NAT mechanism because customers are accessing the internet from the home network. If the CPE can not perform the NAT mechanism the home network can not access the internet because of the private address it is using. But on the other hand with IPv6, this issue works differently. Like IPv4, CPEs are still given public IPv6 address. However, an IPv6 prefix is given to the home network and all the hosts on the home network which are behind the CPE can have public IPv6 addresses. This operating logic changes the existing CPE provisioning model.

6.3. Application Problems

Applications are part of the internet and communication. Therefore they are also affected by the change of internet protocol. During transitioning, IPv6 applications and IPv4 applications will coexist in the network for service continuity regardless to which technology or technologies an operator choose to use for transitioning. Beside that many applications are expected to be able to handle both IPv6 and IPv4 until long period of time.

In the period of transition there will be two important questions about the application side. First question is how different network transition techniques affect applications and methods. And the other, be implemented how can the development of IPv6-capable applications or protocol independent applications. Software developers work on these questions a lot because they want to be accessible both IPv4 and IPv6 users. There are four different cases that can be used for application transition:

1- IPv4 applications will exist in a dual-stack node, IPv6 is also introduced to the node, applications are not ported for IPv6 support.

2- Both IPv4 and IPv6 only applications are in a dual-stack node, that is, there are two similar applications corresponding to each protocol version. Porting has been done for IPv6 only.

3- Applications to support IPv4 and IPv6 in a dual-stack node, which is where the applications are ported in such a way, that they can support both IPv4 and IPv6. Because of this, IPv4 applications can be removed.

4- An IPv4 only node can support both IPv4 and IPv6. This way, applications are ported to support both protocol versions, but they tend to work even if IPv6 is not present.

In the long run, the first two cases are not likely to be used. Most applications ideally should work in all situations where any of the protocols are used, thus leaving out some applications behind, which are specific to IPv4 or IPv6.

The transition from IPv4 to IPv6 may not proceed seamlessly, for which the reasons are as follows:

- There is no relation between the OS and Applications regarding IPv6 support. IPv6 capable application transition on a node can be independent of protocol stacks because IPv4 and IPv6 applications are not meant to be included on a dual stack operating system. Even if IPv6 is disabled or no IPv6 connectivity, on IPv4-only nodes applications capable of IPv4 and IPv6 will have to work properly.
- It is difficult to support many versions of an application. System administrators may have various version of the same application during the transition period such as IPv4 and IPv6 only applications, or an application to support both IPv4 and IPv6. Before any DNS lookup, it is not possible to determine the IP version. Local users will face the difficulty of selecting the proper protocol version in case there exist multiple versions of an available application [15].

6.4. Network Management and Operation Problems

Management of the IPv6 network can be almost similar to management of the IPv4 network in theory. But in practice they are not similar issues. During transition, new technologies and new techniques can be introduced to the network. At that time these new technologies and new techniques will require new operation models.

Besides that, IPv6 is more complicated than IPv4 and the IPv6 addresses are unreadable. Of course this complexity brings operational difficulties with the simplest example, control of the IPv6 IP addreses in any of configuration is difficult than the control of the IPv4 IP addreses.

The other issue is before the transition to IPv6, all network management tools which are all compatible with IPv6 should be ready. Because both network -with all parts- and network management tools should be ready for giving a proper end-to-end service.

6.5. Security Considerations

IPv6 is more flexible protocol than IPv4. This flexibility brings some security problems in IPv6. Security is always important issue and must be addressed. Figure 6 is shown the survey results about IPv6 security risks which is voted by gogoNET members (a community of 95,000 network professionals).

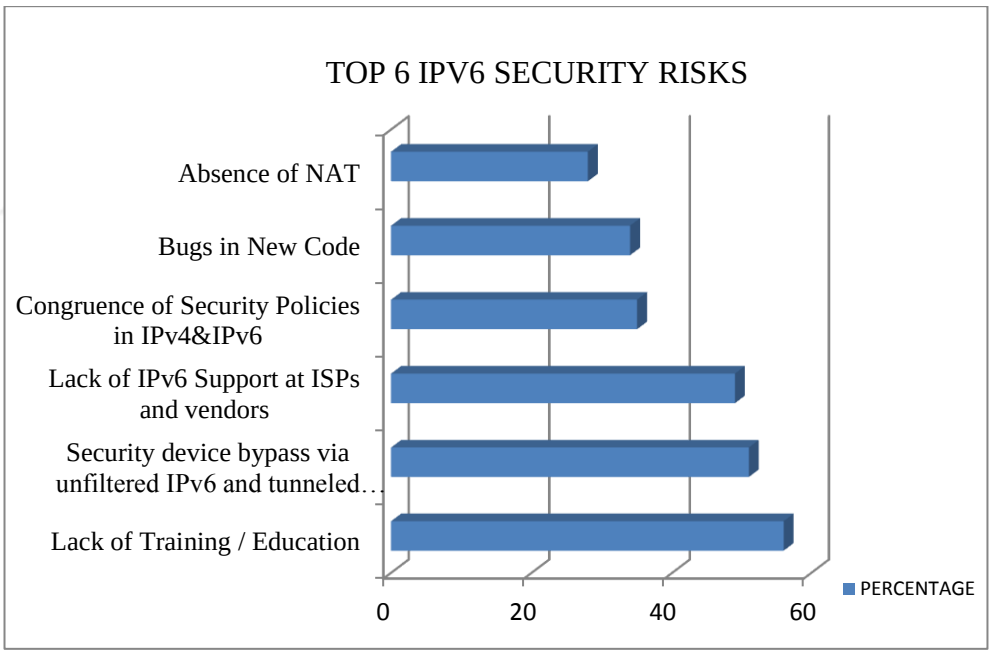


Figure 6 IPv6 Security Risks

Here are the details of the risks are listed below started from the biggest one:

1- Lack of IPv6 security training/education: The lack of IPv6 security knowledge is seen the biggest risk for gogoNET members. Companies must spend money and time for IPv6 security training, before deploying

IPv6. If they do not do it, for plugging the holes which are the risks about security they must spend more money and more time on security issues. All these show that network security is decided much more in the planning stage rather than after deployment.

2- Security device bypass via unfiltered IPv6 and tunneled traffic: There are two things are needed by security products. The first one is detecting of suspicious IPv6 packets and the second one is apply controls when they do. But in practice this is almost impossible in IPv4 let alone an environment that may have unknown tunnel or rogue traffic because there are more than 16 different tunnels and transition methods. Security products are used in today which are generally converted from IPv4 to IPv6, but sometimes their protecting capacity are not enough to match the expectation.

3- Lack of IPv6 support at ISPs and vendor: ISPs and vendors have not enough experience about IPv6 security and this lack reduces of their support capabilities. At that time testing is very important to gain experiences for coming the same level with IPv4 about security functionalities and stability. A test plan and a test network for all protocols involved must be devised to test all equipment, particularly vendors' new security technologies. Networks are different from each other and than there must be a unique test plan. Also a tunnel connected to their interface increases the complexity of security and provides a open door for attacks.

4- Congruence of security policies in IPv4 and IPv6: Lack of the current IPv6 security knowledge causes weak IPv6 security policies. The capacity of the IPv6 security policies do not need to be equal to that of their IPv4 counterparts but the capacity of the IPv6 security policies must be wider to cover new vulnerabilities that didn't need to be considered in a homogeneous IPv4 environment.

5- Bugs in new code: The new codes may be containing bugs. These bugs can be found in the code around TCP/UDP, NICS and networking software libraries that do not completely support IPv6 yet. After completely support then these bugs can be solved easily. And for cleaning any bugs in the codes doing many tests plays an important role. If there is very detailed test plan and a test network then bringing out defects can be easiy. So these defects can be removed before deployment with working on them.

6- Absence of NAT: There is no need for NAT in IPv6 therefore in IPv6 NAT is not used. It may be good to have NATs in IPv6 environments for expansion but in practise they don't provide any added security.

IPv6 and IPv4 are different protocols and therefore IPv6 security cannot be the same as IPv4 security. Policies must be extended and training must be undergone. Then measures must be taken for new threats. Network will change from simple IPv4 network to complex IPv4/IPv6 network then there will be new types of traffic and equipments that must be taken into account [16].

In addition to all risks we can say that IPv6 can not avoid all attacks which are on above the network layers like denial of service attacks, email spamming, application layer attacks or etc.

Consequently IPv6 is relatively new technology therefore it is normal to experience some security issues. After a certain period of time, the use of IPv6 will be increased and new security problems may be seen.

CHAPTER 7

TASKS AND LOADS FOR MIGRATION

7.1. Tasks and Loads of ISP

ISPs provide internet services therefore trasition to IPv6 is very important issue according to them and their task and loads are very high in this transition. ISP networks have two parts. The fist part is ISP backbone and the other is edge networks. The backbone network is in the core of the all networks and generally it is connected to every point directly or indirectly through the Border Gateway Protocol (BGP). According to the backbone network, depletion of the IPv4 address space is not a problem because the scale of the backbone network is generally limited. The number of compenents in the backbone are much less than edge networks or user sides. The highest upgrading priority in the backbone network belongs to backbone routers. On the other hand edge network is different from backbone. The edge network is like a bridge between users and backbone and it is relatively independent from the backbone and provides the infrastructure services by itself. The edge network has a aggregating feature, all along from end users to the backbone entrance. The edge network will not assign public IPv4 addresses as one wishes in the near future to the end users which are very large population because of the depletion of the IPv4 addresses. Typically, a large number of access devices, servers, routers in the current edge network cannot support IPv6 as well. This time, costly upgrades are needed to support native IPv6 for all parts of the network. All software and hardware are included in this issue. Besides, upgrading user devices and applications also need to support native IPv6 [17].

Depending on these facts, the ISP transition requirements are listed below:

1- Provisions of both IPv4 and IPv6 services: It is very important for the continuity of services for customers. Therefore ISP must guarantee that all end users can reach and be reached by both IPv6 and IPv4 internet. ISPs should take all measures on this issue to ensure this.

2- Incremental deployment and minimum upgrade: ISPs made a huge investment for the existing infrastructure. Therefore they will not want to make a new huge investment. This time incremental deployment and minimum upgrade can be chosen by ISPs which can significantly save the cost and reduce the operation burden.

After providing all requirements for transition then deployment is the next task for ISPs. The actions needed for deploying IPv6 on ISP networks are divided into 3 categories. First one is backbone transition actions, the second one is customer connection actions and the last one is network and service operation actions.

7.1.1. Backbone Transition

Backbone networks consist of core and edge routers. In the beginning of the transition, ISPs had only IPv4 networks. Now, ISPs will be running on fully dual-stacked networks. The transition steps are as follows:

- IPv4 only routers (beginning phase)
- IPv4->IPv6 tunnels (intermediate phase-1)
- IPv4->IPv6 tunnels + Dual-Stack Routers (intermediate phase-2)
- Fully Dual Stack Routers (end phase)

ISPs may follow the transition one step at a time, or directly go to the final step. Intermediate steps are not mandatory. Implementing the intermediate steps depends on the resources of the ISP and ISP's time plan about transition. If customer demand for IPv6 is low, then ISP is likely to be stuck at intermediate phase-1. But it should

not be forgotten that following the transition step by step can be a slow and costly way but it may be more reliable.

In the backbone configuration, parameters are relatively small, usually a few interface configuration and routing protocol parameters are enough for configuring backbone equipment.

After determining IPv6 topology and backbone configuration, a routing protocol choice must be made OSPFv3 or Intermediate to Intermediate (IS-IS) for IPv6. The most important decision must be made on whether to separate IPv6 and IPv4 routing trees or not. Separation requires more powerful router resources, both in memory and CPU, but it will ease the maintenance and troubleshooting of these networks individually. Single topology IS-IS can be used if dual-stack deployment is to be done in the short term. It is also preferable to transport IPv4 routing information on IPv4 links and IPv6 routing information on IPv6 links [18].

7.1.2. Customer Connection

Transition of customer networks into IPv6 are affected by several factors, business customers who runs managed networks may have some needs, end-user customers who are connected through DSL or Fiber may have different needs. In order to do the transition, a CPE, router or even a host capable of IPv6 tunneling is needed at the customers' site. The first careful stage is taken by ISP is connecting IPv6 customers to an IPv6 backbone through an IPv4 network to provide IPv6 services to its IPv4 customers. Also, some ISPs may choose to provide IPv6 service independently from the regular IPv4 service. It's up to ISP decision whether to offer IPv6 services separately or not.

When deploying small end customers' site, which usually use dynamic IPv4 address allocation, NAT traversal over IPv6 tunnel will an issue. Most CPEs will likely to assign IPv4 addresses internally and they will be doing NAT over IPv6 WAN interface. In these scenarios, Teredo running on individual hosts will solve the NAT

issue. However, other devices that are not aware of Teredo protocol, will not be able to connect. These devices will require CPEs to do the translation.

When deploying large end customers' site, deploying a dual-stack router is likely to be preferred. Tunneling should be directly done on customers' border gateways.

Customers may desire multihoming for some reasons. Multi-homing for IPv6 cannot be done if the links are selected from different ISPs. Because ISP prefixes will be different and it will not be possible to route the same packet over different prefixes. In this case, Multi-homing may be done like IPv4-style failover mechanisms.

The last issue about customer side is user authentication and access control. User authentication can be used to control who can access specific IPv6 services or who can use the IPv6 connectivity service. In IPv6, specific user authentication is not always required. For instance, a customer of the IPv4 service automatically having access to the IPv6 service. At that time IPv4 access control provides access to the IPv6 services. If a provider does not give permission to IPv4 customers automatic access to IPv6 services, at that point there must be IPv6 access control at the same time with the IPv4 access control [18].

7.1.2.1 Configuration of Customer Equipment

The customer connection networks have two parts which are CPE (Customer Premises Equipment) and PE (Provider Edge). Usually, each PE connects multiple CPE components to the backbone network infrastructure. One of the important tasks for ISPs is configuring of the customer CPEs. The configuration of CPE is difficult for the ISP, and it is even more difficult when it must be done remotely. There are two ways of configuration which are auto-configuration mechanisms and manual configuration. If ISP’s customer is a corporate customer at that time there will be a technical staff who can do configuration. But on the other hand ISP’s home users generally can not do it. And we know that in general a large majority of customers are individual home users. At that time CPE configuration is a big problem according

to ISPs. To overcome this problem ISPs are using ACS servers to configure the customer CPEs. But ACS operations and remote configuration are also difficult processes.

There are some parameters which generally need to be provided to customers automatically are the network prefix delegated by the ISP, the address of Domain Name System (DNS) and other parameters like address of the Network Time Protocol (NTP) server.

When user identification is required on the ISP's network, DHCPv6 or Radius Server may be used to provide these configurations [18].

7.1.2.2 QoS (Quality of Service)

Quality of service is really important for the transport of traffic with special requirements. According to ISPs, QoS is very important issue because the majority of customers pays attention to the quality of the services received from their ISPs. Some customer immediately change their ISPs when service quality declines. When configuring Quality of Services in IPv6, special care must be taken into account, because there are several QoS algorithms that rely of a part of the IPv4 address. For example, an IPTV service relying on IPv4 prefixed must be configured to take IPv6 prefixes into account in order to apply proper QoS parameters on the packets. If an ISP provides service with an SLA (Service Level Agreements) in IPv4 of course customers expect the same SLA in the IPv6. But in new protocol it may take time to provides same SLA [18].

7.1.3. Network and Customer Operations

Network and customer operations are the other issues for transition. All network and service operations will change according to IPv6. The network and customer operation actions are listed below:

- Set up IPv6 connection
- IPv6 device configuration
- IPv6 network management
- IPv6 monitoring
- IPv6 customer management
- IPv6 operation security

ISP should provide all these actions with an IPv6 transition. To provide all of them correctly, ISPs' operation teams should receive training about all actions before transition. Besides these, configuration and customer management tools, network management and monitoring systems should be adapted to IPv6.

7.2. Tasks and Loads of Network Operator

Network operators must find applicable transition mechanisms and make good transition plans for providing all their customers demands. Network providers jobs are a little easier than ISPs because of the association between ISPs and their end-users. Before the ISP can consider providing IPv6 service, network provider must be ready at the IPv6 level. Network provider can get ready for IPv6 by the following steps listed below:

- Controlling the all network parts (all hardware and all software) for IPv6 support and making the necessary updates.
- Preparing a very detailed transition plan. Planning stage is very important for successful transition to IPv6.
- IPv6 deployment must be done very carefully and there should be no service interruptions.
- Backbone and edge networks should be ready to IPv6 services and they must still provide IPv4 services for IPv4 demands.
- After deployment, all staff should be informed about IPv6 and there must be IPv6 training for staff, especially for the support team.

- If there are problems after deployment, they must be removed as soon as possible in order to ensure continuity of services.

7.3. Tasks and Loads of Internet Content Provider

Internet Content Providers (ICPs) must develop some methods for transition from IPv4 to IPv6. However the requirements of these methods are effected by lots of issues. These issues are mainly routing and forwarding methods in IPv4/IPv6 networks, a feasible IPv4/IPv6 address mapping method despite of the asymmetry of address spaces, scalability, upper-layer transparency and an end-to-end heterogeneous addressing method. These properties must be investigated very deeply by content providers.

There are some types for ICP and its CDN s to support IPv6. ICP can use IPv6 but its external CDNs may not. In such state its clients will use IPv4 and IPv6 only clients will have to find a transition solution. In this situation the ICP s work for supporting IPv6 will be wasted.

In another situation ICP may support IPv6 and CDN supports IPv6 for some POPs. In this scenario IPv6 – only clients could be connected to a POP supporting IPv6. Dual stack clients can be connected to a mixture of IPv4 and IPv6 POPS for different URLs according to the A and AAAA records provided. But in this situation copies of the same content may be different in IPv4 and IPv6 because of the latency in the data synchronization from the CDN. This is more apparent in the social networks. That supports dual stack.

In another type CDN can support IPv6 but ICP may not. This does not affect anything since IPv6-only users can connect via IPv6. This will not create any problem. But ICP and its support staff must be aware of it in case of future issues [17].

7.4. Tasks and Loads of Software Developer

When networks are transitioned networks from IPv4 to IPv6, it does not mean that whole transition process is complete. The general idea is hardware and network changes are the large parts of the transition to IPv6. But IPv6 will impact software as well as hardware. Software is consisting with server and desktop operating systems, email programs, web services, management softwares and security tools. IPv6 impacts all IT system parts, which means all applications must be readied for the new protocol.

Deploying IPv6 on software is important because applications will work regardless of the protocol since newly produced application supports both IPv4 and IPv6. Many big vendors like HP already offer applications working on both IPv4 and IPv6. For internally developed application it is much better to enhance the application to support IPv6.

There are two ways to enable IPv6 on applications. One way is to have separate codes for deploying IPv4 and IPv6. This approach may arise much more complexity since the race conditions and recovery mechanisms will be doubled. And it needs more resource.

Second way is to create a combined IPv4 and IPv6 logic. It guarantees the operation of the software regardless of the ip version. This second approach needs to use host names instead of specific ip addresses. The Name Resolution process will find which protocol will be used. This causes your software to operate regardless of changes on the network layer.

Everyone in the IT organization will be involved with the deployment of IPv6. Especially application developers are aware of the nuanced of creating applications that will operate over current IPv4 networks and in the near future as IPv6 is added. They should note the following issues:

1- Analyzing of Current Code for IPv6 Capability: All code should be examined in detail module by module and file by file finding such data structures. Or for this job, they can use dedicated automated software application. They can find a lot of tools on the market which are used for automated assessment of application code for IPv4/v6 calls.

2- Writing Code Backward Compatible with IPv4: Developers have to pay attention to writing codes which are backward compatible with IPv4. Writing two separate applications both support two internet protocols does not make sense. On the other hand, users of these applications should not need to be aware of which IP version is used in these applications.

3- Making Socket Connections with IPv6 and IPv4: Applications are using computers that are on dual-protocol capable network which have both IPv6 and IPv4 addresses should prefer IPv6 when possible. First of all applications should try making a connection using IPv6 then try to IPv4 if the connection of IPv6 does not exist.

Beside all above there are the cases which are described in IETF RFC 4038 Application Aspects of IPv6 Transition advice for writing dual-protocol applications to developers are listed below:

1- First Case: IPv4-only applications in a dual-stack node. IPv6 protocol is introduced in a node, but applications do not support IPv6 yet.

2- Second Case: Both IPv6-only and IPv4-only applications are in a dual-stack node. But they are ported for IPv6-only.

3- Third Case: Applications are supporting both IPv6 and IPv4 in a dual stack node and they are ported for both IPv6 and IPv4 support at the same time.

4- Fourth Case: Applications are supporting both IPv6 and IPv4 in an IPv4-only node and they are ported for both IPv4 and IPv6 support.

Generally we can say that case one and case two are not being used in the longer term. Therefore, the developers should focus on writing dual-protocol applications that can run on IPv6/IPv4 networks [19].

In summary, applications must be tested in detail. Realistically, IPv4 and IPv6 will need to coexist on networks until IPv4 is fully phased out. This is good news, because it will give you time to carefully enhance existing applications one at a time, as well as build new applications for IPv6.

7.4.1. Requirements for IPv6 Support in Software

The newly created software must support both IPv4 and IPv6. This means that the connections can be done on IPv4 only, IPv6 only or dual stack. If software has network parameters in it, it should also support configuration of IPv6 parameters. All features of the software that uses IPv4 must be used in IPv6 too and the user does not need to understand which version of the protocol is used [20].

7.5. Tasks and Loads of Hardware Manufacturers

If one day all IPv4 traffic transfers to IPv6 traffic then all requirements placed on IPv4 traffic capabilities like bandwidth, throughput and latency should also be required for IPv6 traffic. Then every piece of the networking environment like IP adresses, processes, routing, server infrastructure and customer premises will be affected by the switch to IPv6.

According to Information and Communication Technologies (ICT) hardware equipment is divided into seven functional groups:

- Host (which are server or client)
- Layer 2 switch
- Layer 3 switch / Router
- Network security equipment
- CPE (Customer Premises Equipment)
- Mobile device
- Load balancer

Each hardware group must provide some type of mandatory requirements for IPv6 support. There are a lot of mandatory requirements but for the sake of example only, some of them have been noted in this document. And there are also optional support list but it is not explained in this document either.

Each hardware group description and samples of the mandatory standards for each group are listed below.

1- Host: It is a node and part of network that sends and receives packets. Samples of mandatory requirements for Hosts about IPv6 support:

- [RFC2460] - IPv6 Basic Specification
- [RFC4443] - ICMPv6
- [RFC1981] - Path MTU Discovery
- [RFC4291] - IPv6 Addressing Architecture
- [RFC4193] - Unique Local IPv6 Unicast Addresses (ULA)
- [RFC3315] - DHCPv6 Client
- [RFC4861] - Neighbor Discovery
- [RFC3596] - DNS protocol extensions for incorporating IPv6 DNS resource records
- [RFC4862] – SLAAC
- [RFC3484] - Default Address Selection
- [RFC2671] - DNS message extension
- [RFC3226] - DNS message size requirements

2- Switch or Layer 2 Switch: It is a device that is mainly used for forwarding ethernet frames based on their attributes. Samples of mandatory requirements for Layer 2 Switch about IPv6 support:

- [RFC4541] - MLDv2 snooping
- [RFC3315] - DHCPv6 filtering
- [RFC4862] - Router Advertisement (RA) filtering
- [RFC4429] - Duplicate Address Detection (DAD) snooping and filtering
- [RFC4861] - Neighbor Unreachability Detection (NUD) filtering
- [RFC4861] - Dynamic "IPv6 Neighbor solicitation/advertisement" inspection

3- Layer 3 Switch / Router: It is a device that is mainly used for forwarding IP packets based on their attributes. Samples of mandatory requirements for Layer 3 Switch/Router about IPv6 support:

- [RFC2460] - IPv6 Basic specification
- [RFC4443] - ICMPv6
- [RFC4291] - IPv6 Addressing Architecture
- [RFC2711] - Router-Alert option
- [RFC1981] - Path MTU Discovery
- [RFC4541] - MLDv2 snooping
- [RFC3484] - Default Address Selection
- [RFC4193] - Unique Local IPv6 Unicast Addresses (ULA)
- [RFC4861] - Neighbor Discovery
- [RFC4862] - SLAAC
- [RFC3810] - Multicast Listener Discovery version 2
- [RFC5095] - Deprecation of Type 0 Routing Headers in IPv6

4- Network Security Equipment: These devices' most important job is to permit, deny and monitor traffic between interfaces in order to detect or prevent potential malevolent activity.

Samples of mandatory requirements for Network Security Equipment about IPv6 support:

- [RFC2460] - IPv6 Basic specification
- [RFC4443] - ICMPv6
- [RFC1981] - Path MTU Discovery
- [RFC4291] - IPv6 Addressing Architecture
- [RFC3484] - Default Address Selection
- [RFC4862] - SLAAC
- [RFC5095] - Deprecation of Type 0 Routing Headers in IPv6
- [RFC4213] - Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers
- [RFC2711] - Router-Alert option
- [RFC4861] - Neighbor Discovery

5- Customer Premise Equipment (CPE): It is a residential router or small office equipment that is used to connect home users with large configurations. Mandatory requirement for CPEs about IPv6 support:

- RFC6204 (Basic Requirements for IPv6 Customer Edge Routers)

6- Mobile Device: It is a node that connects to a 3GPP defined system using some 3GPP specified access technology.
Mandatory reqirements for Mobile Device about IPv6 support:

- [RFC2460] - IPv6 basic specification
- [RFC4861] - Neighbor Discovery for IPv6
- [RFC2711] - IPv6 Router Alert Option
- [RFC4862] - IPv6 Stateless Address Autoconfiguration
- [RFC4291] - IPv6 Addressing Architecture
- [RFC4443] - ICMPv6
- [RFC2472] - IPv6 over PPP
- [RFC3810] - Multicast Listener Discovery version 2

- [RFC3596] - DNS protocol extensions

7- Load Balancer: It is a networking device used for sharing loads of the network to multiple computers, servers or other resources. This ensures efficient use of resources, maximise throughput, minimise response time, and avoid overload. Mandatory requirements for Load Balancer about IPv6 support:

- [RFC2460] - IPv6 Basic specification
- [RFC4291] - IPv6 Addressing Architecture
- [RFC1981] - Path MTU Discovery
- [RFC3226] - DNS message size requirements
- [RFC2671] - DNS message extension mechanism
- [RFC3596] - DNS protocol extensions
- [RFC3484] - Default Address Selection
- [RFC4193] - Unique Local IPv6 Unicast Addresses (ULA)
- [RFC4861] - Neighbor Discovery
- [RFC4443] - ICMPv6
- [RFC5095] - Deprecation of Type 0 Routing Headers in IPv6 [20]

There are a lot of mandatory support lists for hardware. Some of them are written above. This means that hardware manufacturers have a lot to do to get ready to IPv6. Some hardware can be updated for IPv6. But some of the hardware will never support IPv6 via updates or another methods. When time for comes they will throw it in the rubbish. Beside this ISPs and other customers can wait for extra support lists which are optional from hardware manufacturers. There is a lot of hardware in the markets, thats why hardware manufacturers must satisfy requirements of technology in order to survive.

7.5.1. Hardware Vendor IPv6 Support

Around the World there are a number of IPv6 test networks deployed. However, to actually migrate to IPv6, all vendors who have network equipment need to support all IPv6 enhancements.

Two categories are important for IPv6 enhancements. Firstly supporting packet forwarding process and the other includes enhancements to support IT network infrastructure.

The first enhancement includes larger address formats, better routing protocols Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) and increased support for the routing header.

The second category of enhancements includes improvements to the DNS, Plug and Play processes, improved Application Programming Interfaces (APIs), and upgraded security.

Details about IPv6 for several leading networking vendors are listed below:

1- Apple: This open source UNIX-based operating system (after v.10.2) provide good support for IPv6 because it has advanced BSD networking and a TCP/IP stack with advanced sockets. Versions 10.2 and later of this operating system provide good support for IPv6.

2- Cisco: In the development of IPv6, Cisco has been actively involved. Their equipment provides complete support for IPv6. Their support can be observed in all their products. Furthermore, IOS 12 has details of the IPv6 features such as BGP extensions for IPv6, neighbor discovery and autoconfigured tunneling support for each platform.

3- HP: IPv6 features such as autoconfigured tunnels, advanced and basic sockets ApplicationProgramming Interfaces (APIs), IPv4/IPv6 dual stack

protocols, Path Maximum Transmission Unit (PMTU) Discovery, and OSPF are all supported by HP-UX11i.

4- IBM-Hitachi: IBM has shown support for IPv6 and has continually added IPv6 support to its products like Unix and Linux since 1997. IPv6 forwarding rates of a maximum of 26 Mbps and maximum line rates of 2.4 Gbps are provided by Hitachi GR2000 routers. Among other IPv6 features the ASIC of this system has a dual stack IPv4/IPv6 architecture and support packet filtering, IPv6 over IPv4 and IPv4 over IPv6 tunneling and OSPF.

5- Linux: IPv6 and IPsec protocols for Linux are developed by a volunteer-run open sourced collaborative effort referred to as the Universal Playground for IPv6 (USAGI).

6- Microsoft: New versions of the Windows operating system, from Windows Vista up, all have built-in IPv6 enhancements and facilitate an orderly transition from IPv4 to IPv6.

7- Nortel NETAS: Nortel Netas has been trying to provide IPv6 support since the 1990s. Newest generation of Netas Switches offers terabit performance and wire speed. They also provide IPv4 to IPv6 Tunneling, IPv6 Multicast, Neighbor Discovery and OSPF.

8- Sun Oracle: After Solaris 10 operating system, Sun Oracle offers support for important IPv6 specifications. It offers the advantage of Internet Key Exchange (IKE) which lets systems connect by using authentication and encryption and integrated IP Security (IPsec). Their systems have also dual stack tunneling features [21].

These companies are the most famous and largest hardware and software companies in the world therefore they are going ahead on IPv6 support. Almost all their new products are released to the market with IPv6 support.

7.6. Tasks and Loads of Government

Governments have an important mission to increase the awareness and encouraging the deployment of IPv6. Some governments first plan to deploy government services with IPv6. They have some precautions; agree with some of stakeholders and in some cases through test environment, support, enforce and supplyment precuations. Also governments are operating networks, providing content, developing services and applications by IPv6 awareness. However in lots of governments, not enough awareness that IPv4 sources are nearly finished and IPv6 addressing for continutiy of government services and national competitiveness.

Communications based on internet continue to be routed in the most efficient manner and to the right addresses by the seamless global addressing. This provides that government and business services continue to operate smoothly and digital economies continue to improve. But transition to IPv6 by pieces can damage government and business e-services, governments internal networks and applications. E-services are very important issue for governments to interact with the populace. For instance they use to gather information from the public or to provide information to the public or tax payments.

The continuity and stability of addressing are also needful to the evolution and functioning of the Internet and developing digital economies. Therefore governments more focus on on the importance of broadband infrastructure especially high-speed connectivity and economic competitiveness. Governments need to see IPv6 as a key economic enabler just as with broadband. If they think all of them they may be more sensitive to IPv6 transition.

There are a lots of challenges about migrating to IPv6 such as cost of migration, lack of expertise and complexities of the deployment. As the others (ISPs, hardware manufacturers and software developers, etc.) government also has responsibilities in IPv6 transition. These are the actions which should taken by governments for transition are listed below:

1- First action includes outreach and assessment. For providing these, governments have to set up multistakeholder advisory groups on IPv6. Advisory group should be include people from different sectors. The governments should do consultation with these groups from time to time. Also, governments should be also undertaking internal IPv6 assessment audits to establish the scale of the task of enabling their networks.

2- Second action is leading by example. Governments have to put agencies in charge of the issue which are endowed with sufficient authority to elicit cooperation from other agencies and departments. They should do reporting about a lot of issues which are related to transition to IPv6 especially with regard to ensuring the continuity of government services in the transition to IPv6.

3- Third action is persuasion. Once a government decides the transition to IPv6 is very important, then it becomes a matter of communications and persuasion. Governments should be declaring that IPv6 will play an important part in the future of their societies and economies can stimulate interest in IPv4 depletion and IPv6 take-up across key stakeholders. In this way stakeholders may become more willing to transition [22].

If they do not do all above actions at least all governments should provide necessary support and guidance about transition. At this point it may be beneficial to collaborate with universities.

In summary, the governments have effective roles and powers in the transition to IPv6. If they use these roles and powers on time and in the right place they can

accelerate the transition. If necessary, governments may impose certain sanctions for relevant stakeholders about transition.

CHAPTER 8

SURVEY FOR TRANSITION TO IPv6

After searching for problems and loads about transition to IPv6, I decided to conduct a survey regarding this subject. The questions in this survey gathered the opinions of companies about IPv6 transition. When selecting a company for participation in this survey, I took into account choosing different kinds of companies. These companies are network providers, ISPs, software companies, hardware manufacturers and support service companies. Therefore this survey evaluated different points of views.

The below table is a list of companies which participated in this survey:

Table 2 : Participants of the Survey

Number	Company Name	Company Category
1	Alcatel-Lucent	Hardware Manufacturer & Software Development
2	Argela	Telecom Integrator
3	BDH	Information Technology Support Services
4	Ericsson	Hardware Manufacturer & Software Development
5	Himnet	Internet Service Provider
6	Huawei	Hardware Manufacturer & Software Development
7	Kron	Software Development
8	Mynet	Internet Service Provider
9	Netaş	Hardware Manufacturer & Software Development

Table 2: (Continue)

10	Superonline	Network Provider
11	TTNet	Internet Service Provider
12	Türk Telekom	Network Provider
13	Verso	Communication Technologies
14	ZTE	Hardware Manufacturer & Software Development

Questions and percentage distribution of responses to the questions are shown on Figure 7 – Figure 27. (Only question 18 and 19 are not shown with a table because they are not selective questions. Answers of the these questions are discussed in Chapter 8.5)

8.1. How Conscious are Companies about Transition to IPv6

In the survey there are four questions to gather information about how conscious companies are about transition to IPv6. The results of these four questions answers are listed on Figure 7, 8, 9 and 10.

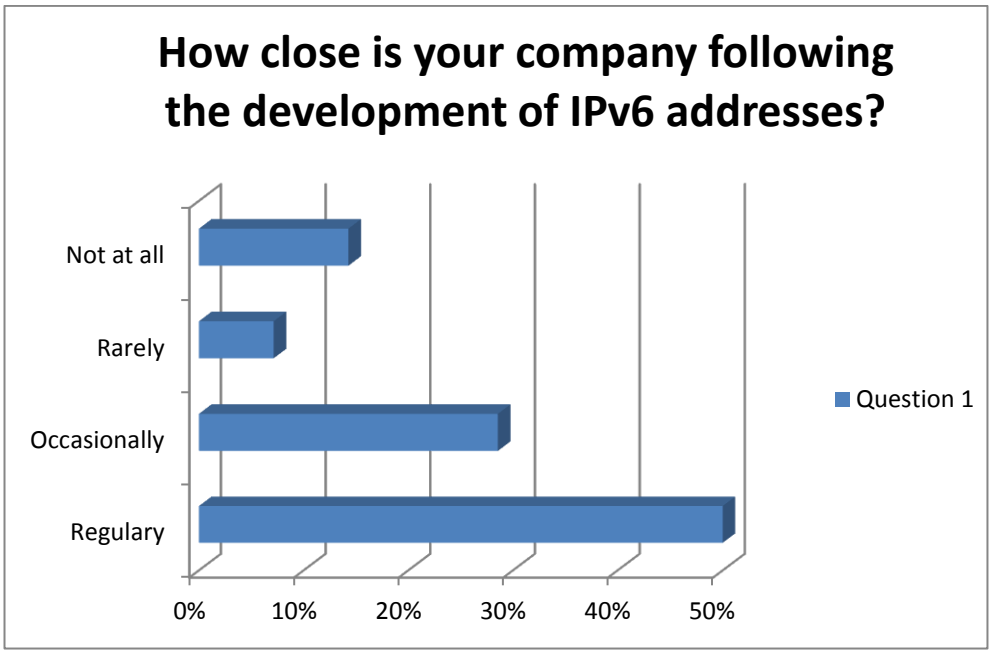


Figure 7 : Distributions of Involvement in Development

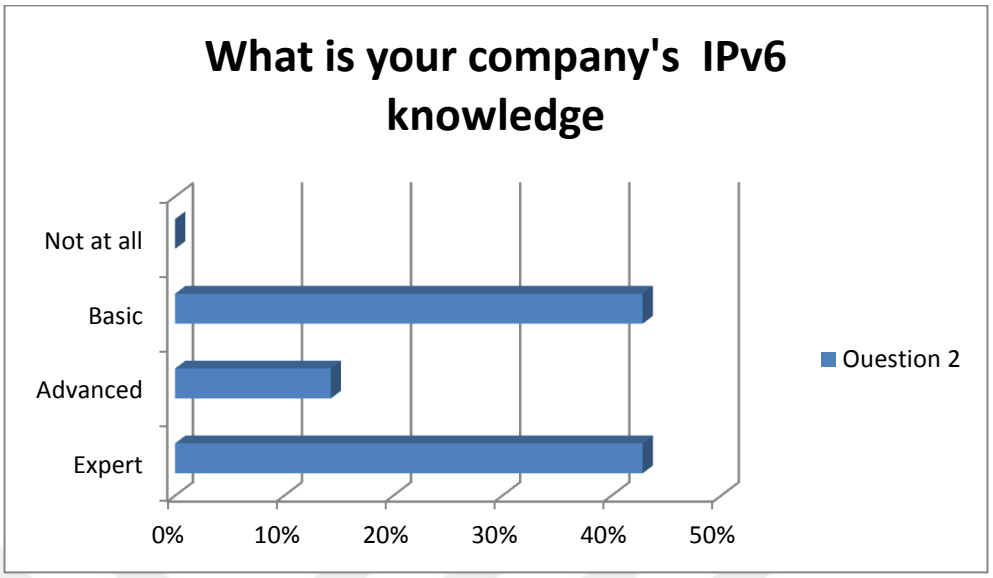


Figure 8 : Distributions of IPv6 Knowledge

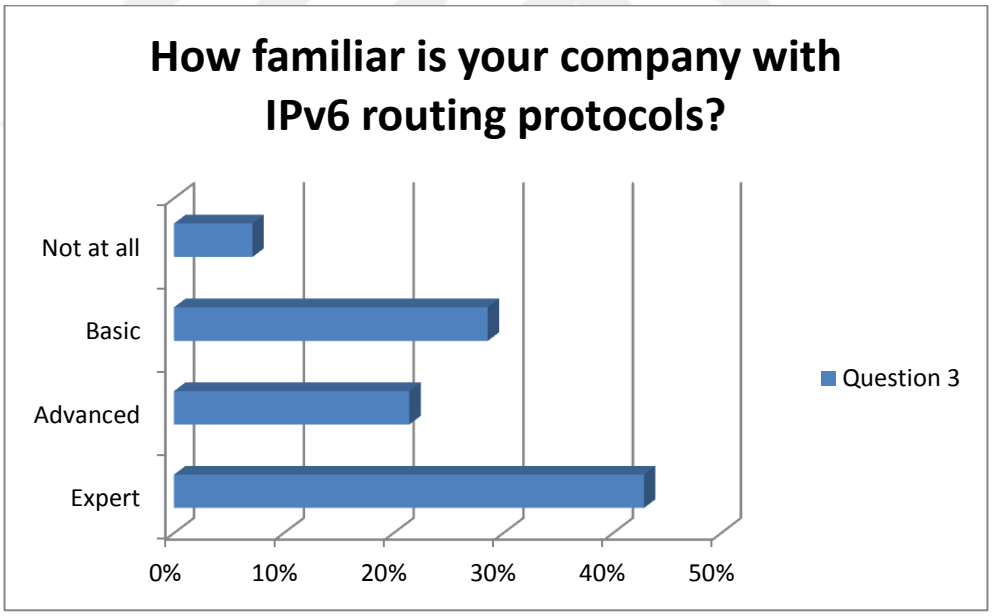


Figure 9 : Distributions of Familiarity of Routing Protocols

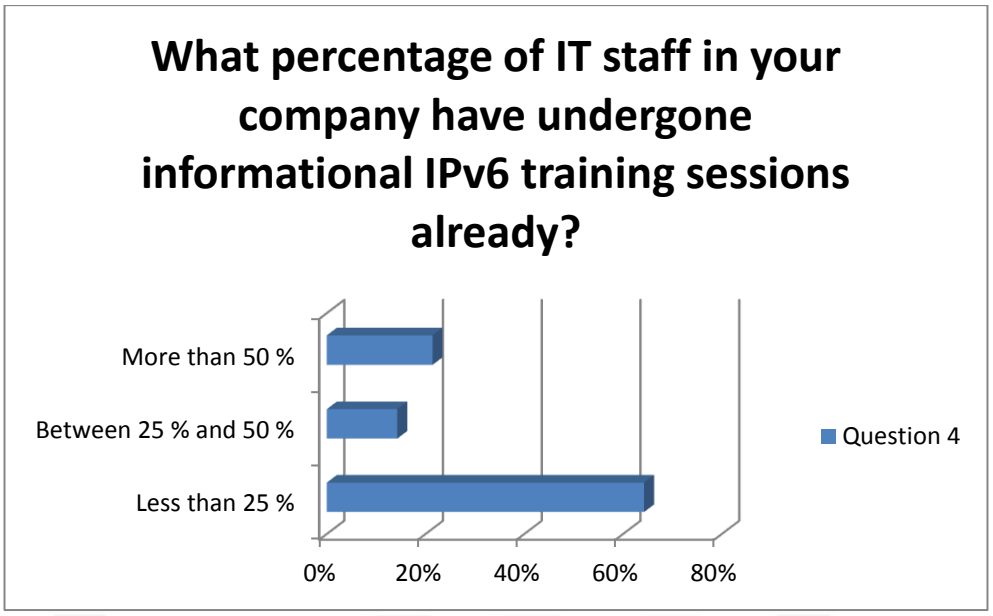


Figure 10 : Distributions of Trained IT Staff

According the results of these four questions we can say that companies that are participants of this survey generally have sufficient knowledge about IPv6. However, companies do not seem spent enough to the subject of IPv6 training. In the most of the company, less than 25% of IT staff have received training in this regard. This rate is really low. Therefore, companies should increase to give training and seminars on IPv6 to their staff. So that companies would have to increase their level of prior knowledge before IPv6 transition.

8.2. How Ready are Companies for IPv6 Transition

In the survey there are two questions to gather information about how ready companies are about transition to IPv6. The results of these two questions answers are listed on Figure 11 and 12.

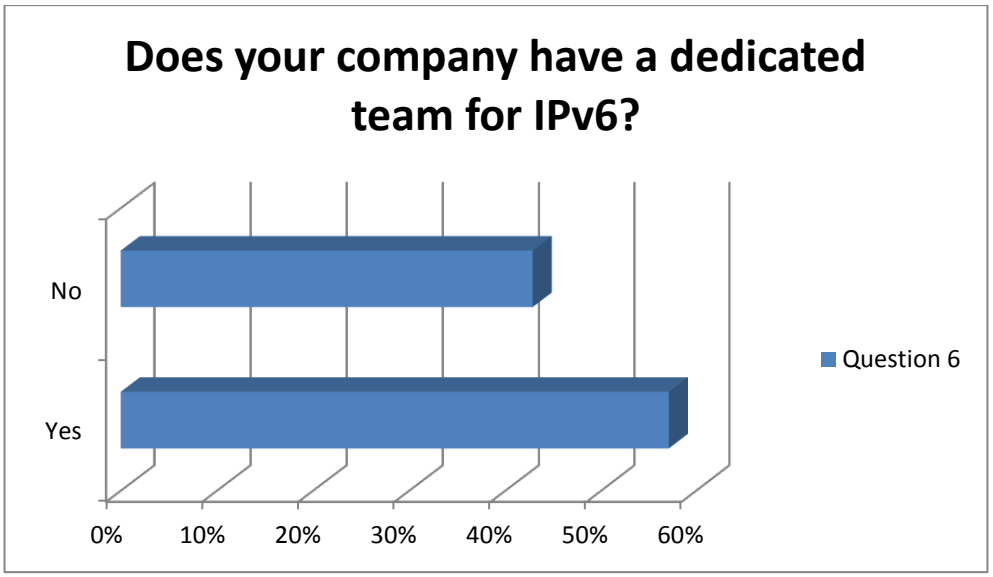


Figure 11 : Exsistence of Dedicated IPv6 Teams

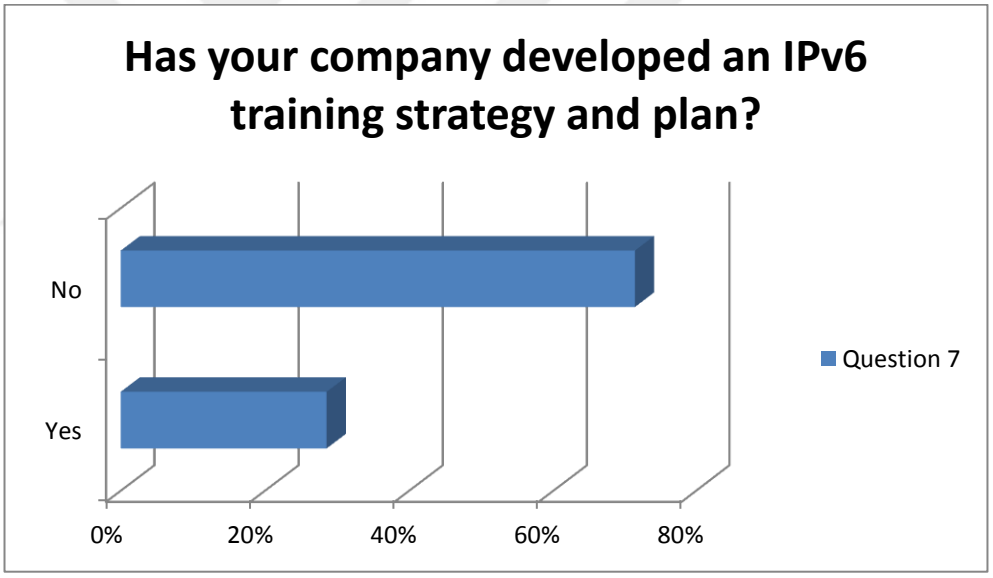


Figure 12 : Exsistence of Strategy and Plans

According to the results of question 6, we can say that most of the companies surveyed have a dedicated team for managing IPv6 activities. That's good news because it will be more healthy to separate following IPv6 activities from other work.

If we examine the answers given to question 7 we understand that mosf of the companies have no plan about IPv6 migration. We anticipate that they are not thinking of the transition to IPv6 yet.

8.3. When Companies Plan the Transition to IPv6

In the survey there are six questions to gather information about when the companies are planning the transition to IPv6. The results of these six questions answers are listed on Figure 13, 14, 15, 16, 17 and 18.

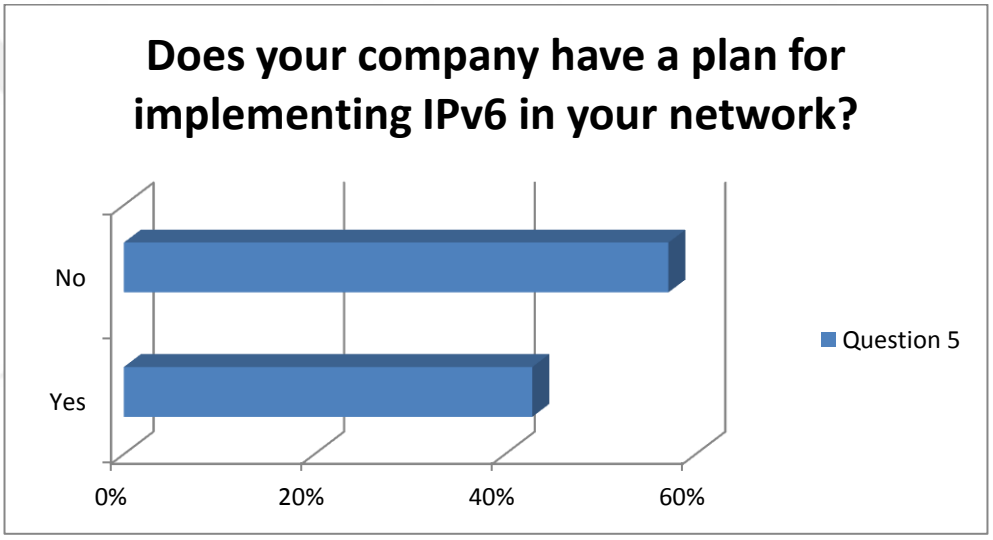


Figure 13 : Distributions of Planning to Implement IPv6

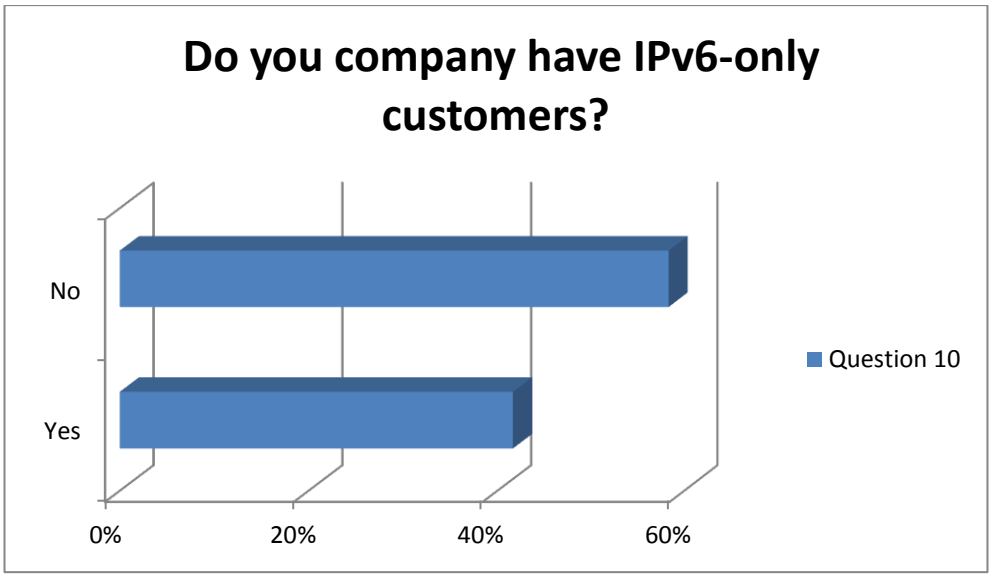


Figure 14 : Distributions of Sale IPv6 Customers

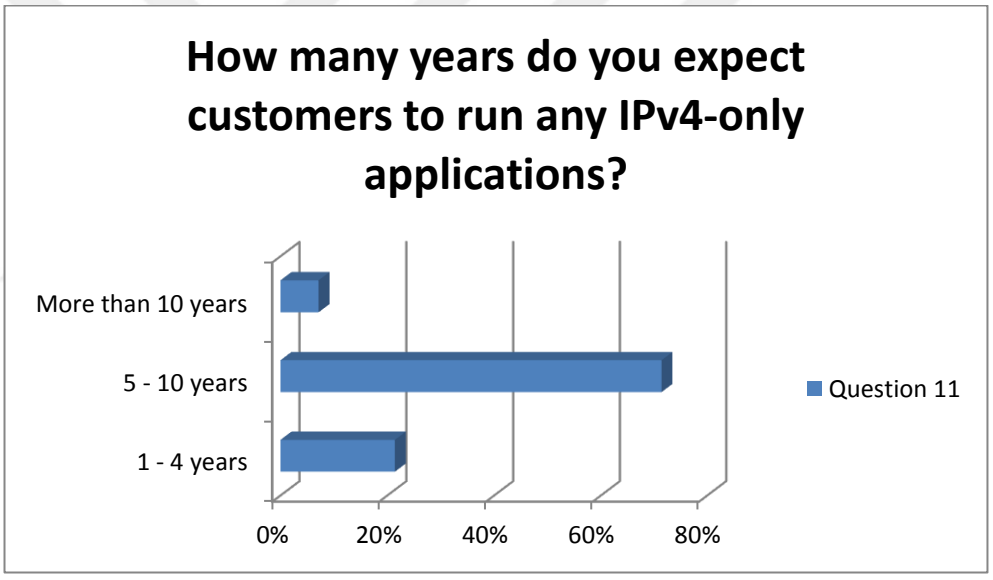


Figure 15 : Distributions of Expectation Regarding IPv4-only Applications

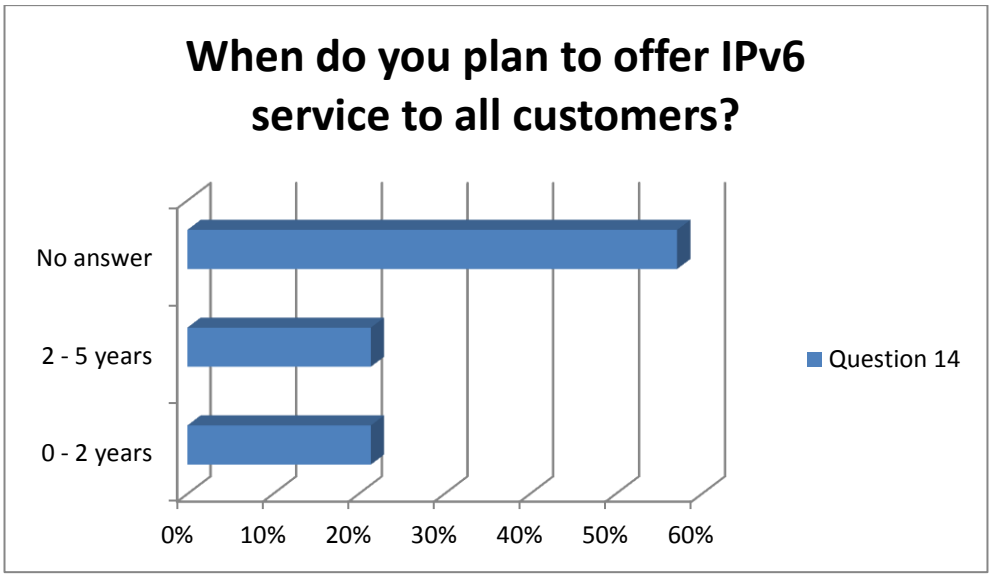


Figure 16 : Distributions of IPv6 Offer

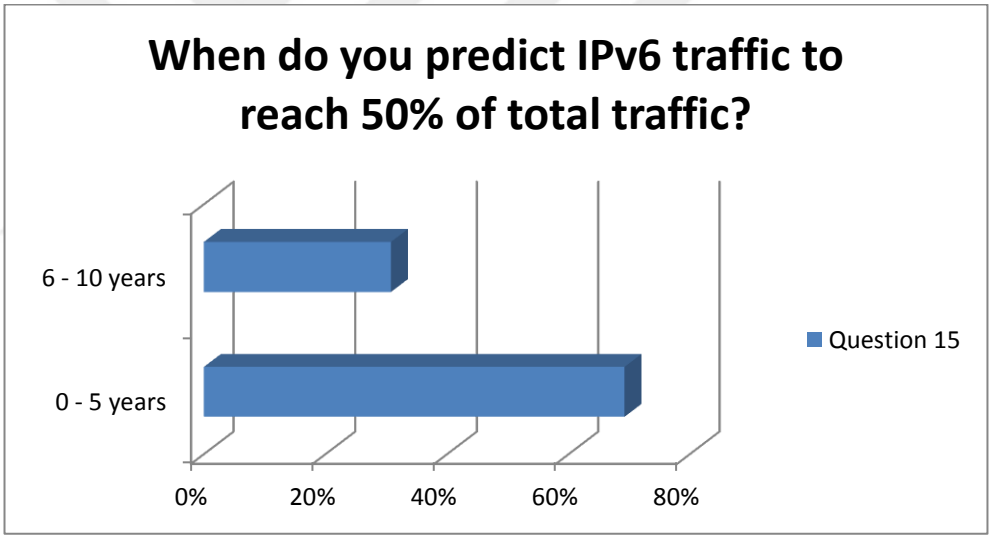


Figure 17 : Distributions of IPv6 Traffic Prediction

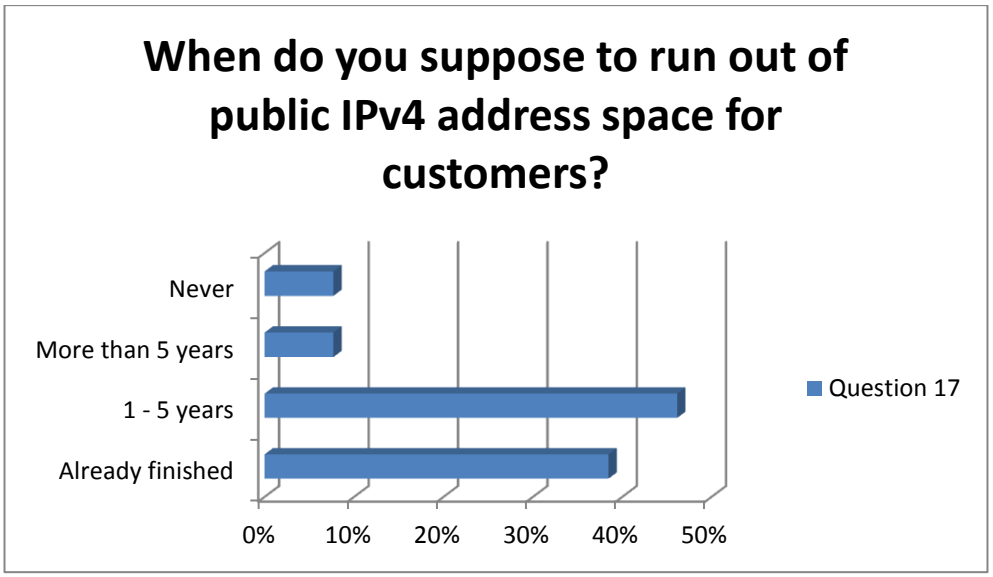


Figure 18 : Distributions of IPv4 Addresses Depletion Time

As is apparent from the answers to question 5, most of the companies do not have a time schedule for implementing IPv6 in their network. We examine that those who say yes to question 5 are generally hardware manufacturers and network providers. Network providers and hardware manufacturers are mostly large companies which are world-famous therefore they are further ahead in IPv6.

Question 10 in the survey is intended to determine whether they have IPv6-only customers. Accouring to the results we see that less than half of the companies have IPv6-only customers. In addition to that, most of the companies expect customers run IPv4-only applications nearly ten years from now, maybe even more according to the answers of question 11.

In question 14, we want to learn when do companies plan to give IPv6 service to all their customers but most of them did not reply to this question. Because this question does not appeal to every company. But if we keep aside companies which do not answer this question, according to the answers of the other companies they plan to give IPv6 service to all customers average between 0 to 5 years.

In the survey we asked them when do they predict IPv6 traffic to reach 50 % of all traffic for getting companies IPv6 traffic forecasts with question 15. Generally

answers often appeared between 0 and 5 years. In addition to this question we asked them when do they suppose to run out of IPv4 addresses in question 17. The majority of responses shown that IPv4 addresses are already finished or will finish between 1 and 5 years.

When we examine all of the answers to these five questions, the majority says that IPv4 addresses are run out of but most of them have no plan about IPv6 migration. It could be for many reasons. Maybe there is no customer demand for IPv6. Or according to network providers and ISPs, they do not need new IP blocks or they are applying NAT or a similar method in their networks for new IP address demands.

However, whether or not for the need companies should have information about IPv6 and they should prepare a transition plan. This way, they will see many benefits in the future.

8.4. Which Technologies are Companies Using for Transition to IPv6

In the survey there are five questions for learning which technologies are companies using for transition to IPv6. The results of these six questions answers are listed on Figure 19, 20, 21, 22 and 23.

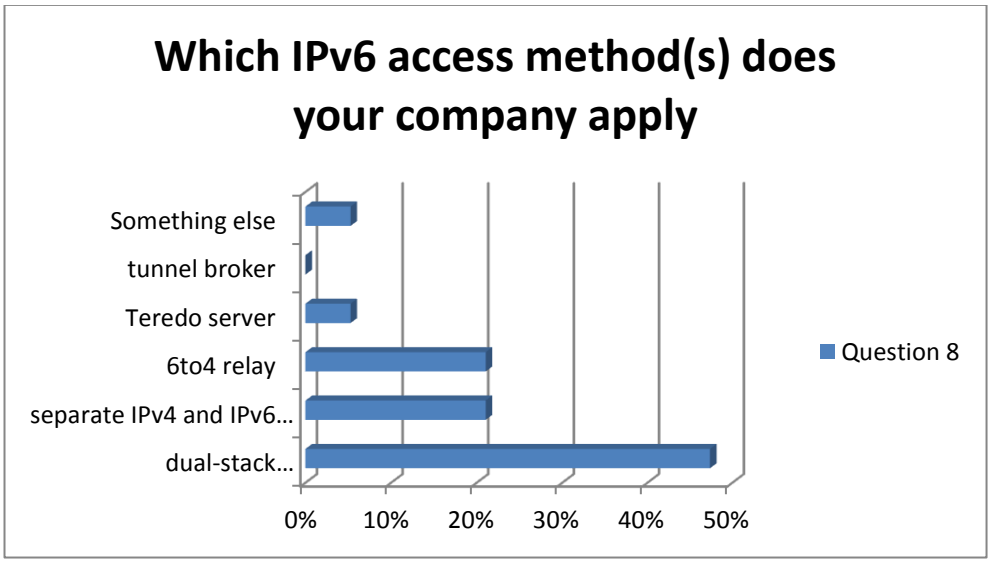


Figure 19 : Distributions of IPv6 Access Methods

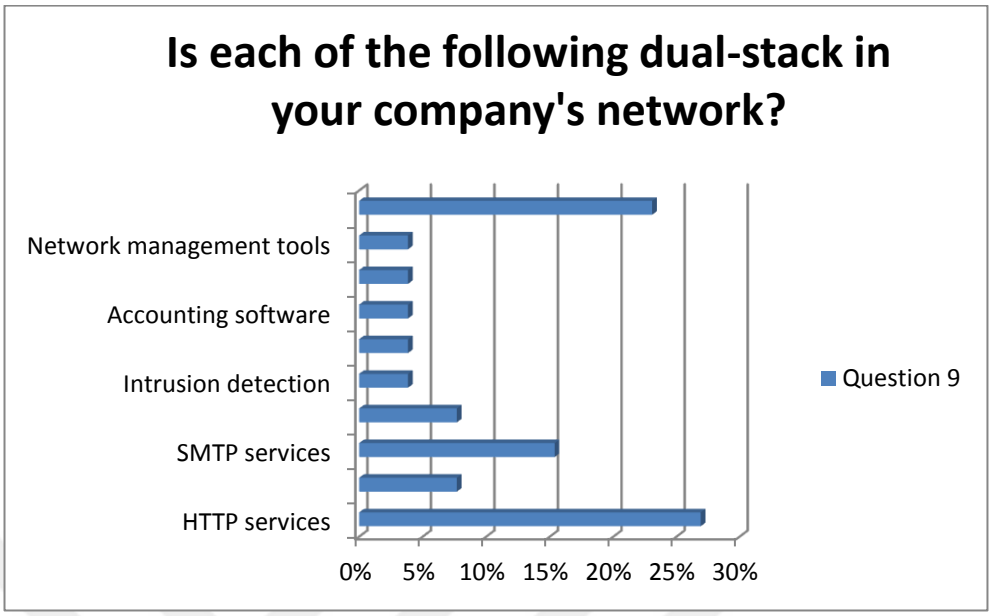


Figure 20 : Distributions of Dual-Stack Services

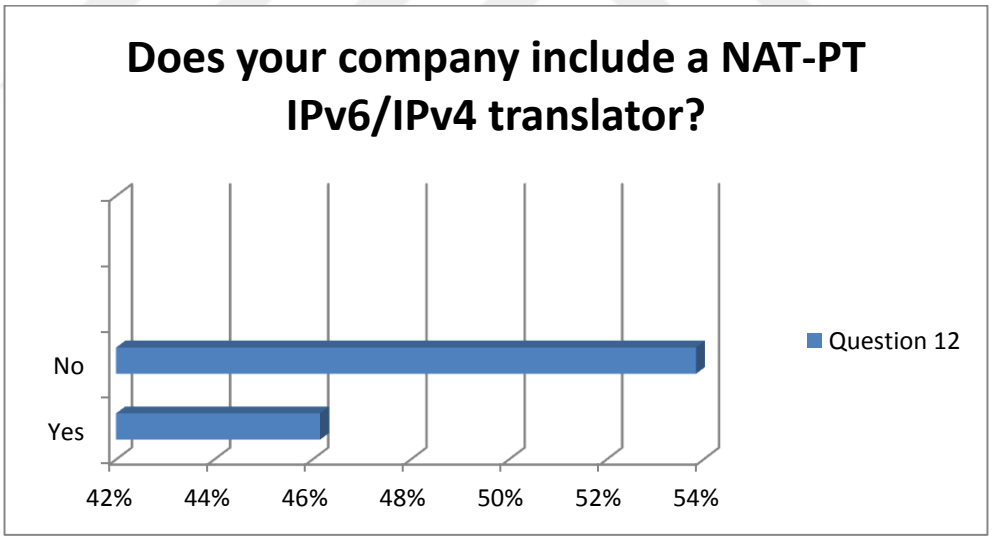


Figure 21 : Existence of NAT-PT Translators

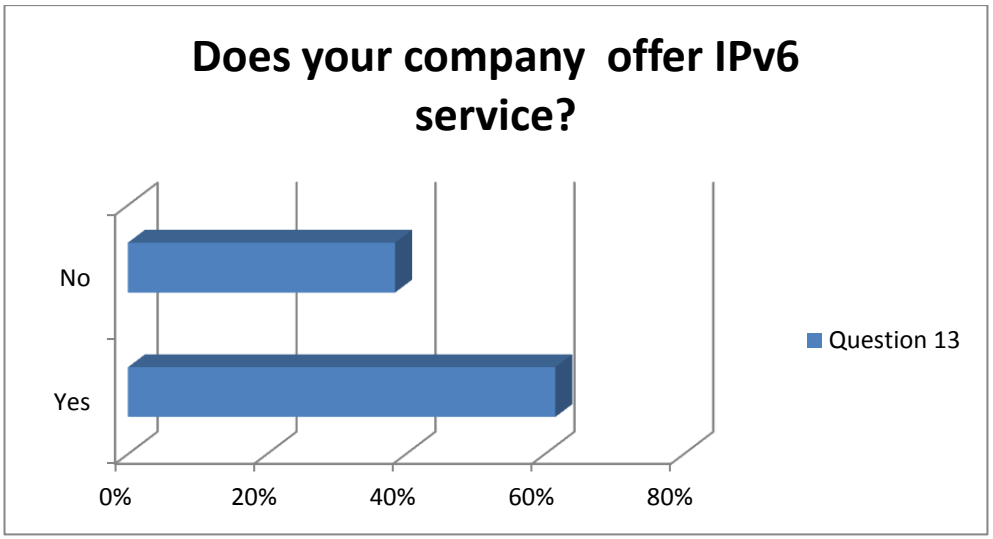


Figure 22 : Existence of IPv6 Service

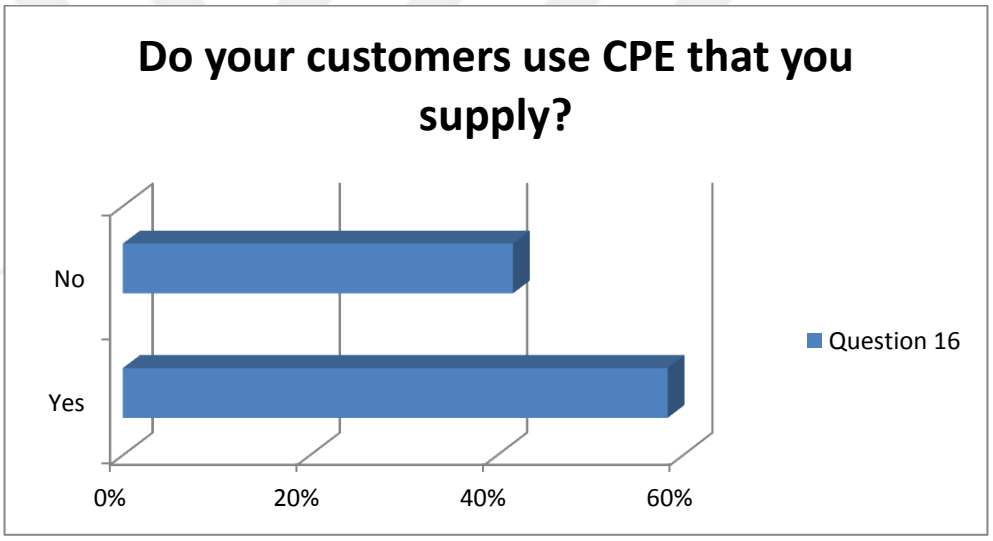


Figure 23 : Supplied Percentage of CPE Use

When we examine the answers of question 8 and 9 we see that the most common IPv6 access method is dual-stack method according to companies. Dual-stack method is espically used in HTTP (Hypertext Transfer Protocol) and SMTP (Simple Mail Transfer Protocol) services. Also the majority noted that they do not use NAT-PT IPv6/IPv4 translator with the answers of question 12.

When we look at the the answers of question 12 and 13, espically network providers and hardware manufacturers stated that they offer IPv6 as a regular service. The

other survey participants do not offer IPv6 service yet. In addition to these four problems, we want to learn if companies supply CPEs to their customers wtih question 16, most of them supply CPEs to their customers.

8.5. What are the Challenges, Problems and Costs of the Transition for Companies

In the survey there are two questions with number 18 and 19 for learning about which topics companies work on the most while planning for IPv6 migration and which topics challenged/will challenge companies the most while migrating over to IPv6. Companies often gave different answers to these two questions. According to the answers of question 18, companies mostly worked on IPv6 address planning, tunneling mechanism, NAT and security topics while planning for IPv6 migration. Besides that upgrading existing devices, NAT64, DNS64, network operations and troubleshooting of problems topics will challenge companies the most while migrating over to IPv6 according the answers of question 19.

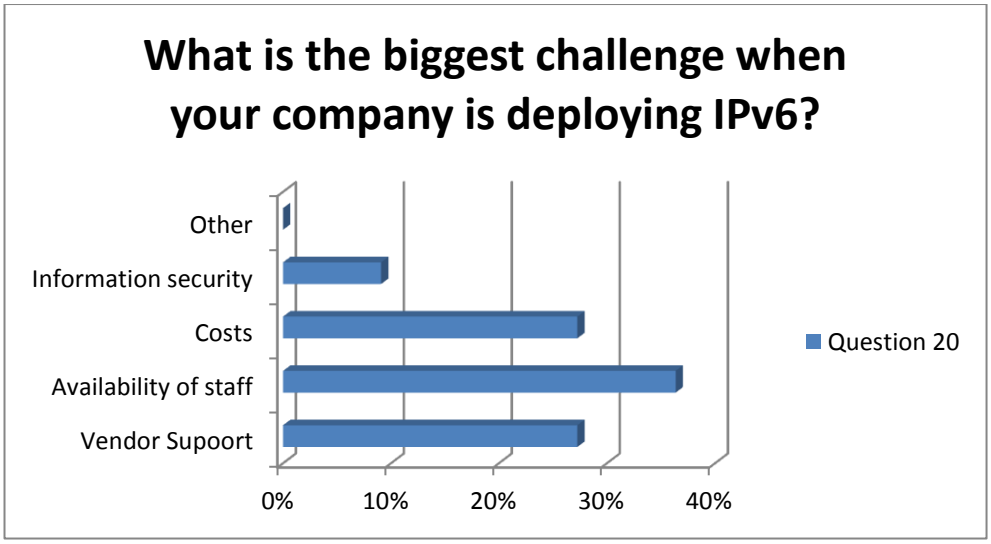


Figure 24 : Distributions of Biggest Challenge for IPv6

We asked what the biggest obstacle for companies deploying IPv6 in question 20 and the majority of them said staff availability is the biggest challenge. The other

challenges are costs and vendor support which are selected nearly 27 % by companies.

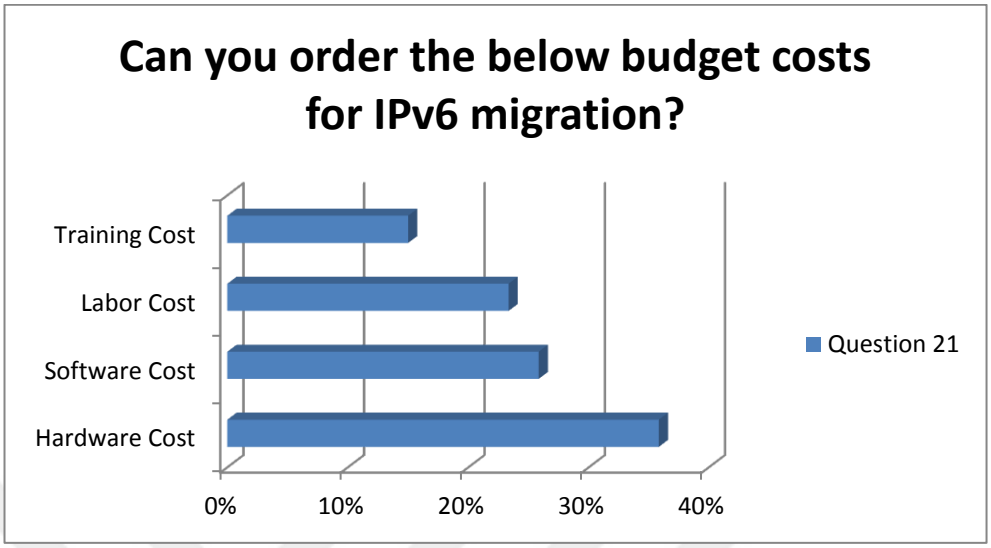


Figure 25 : Distributions of Bedget Costs

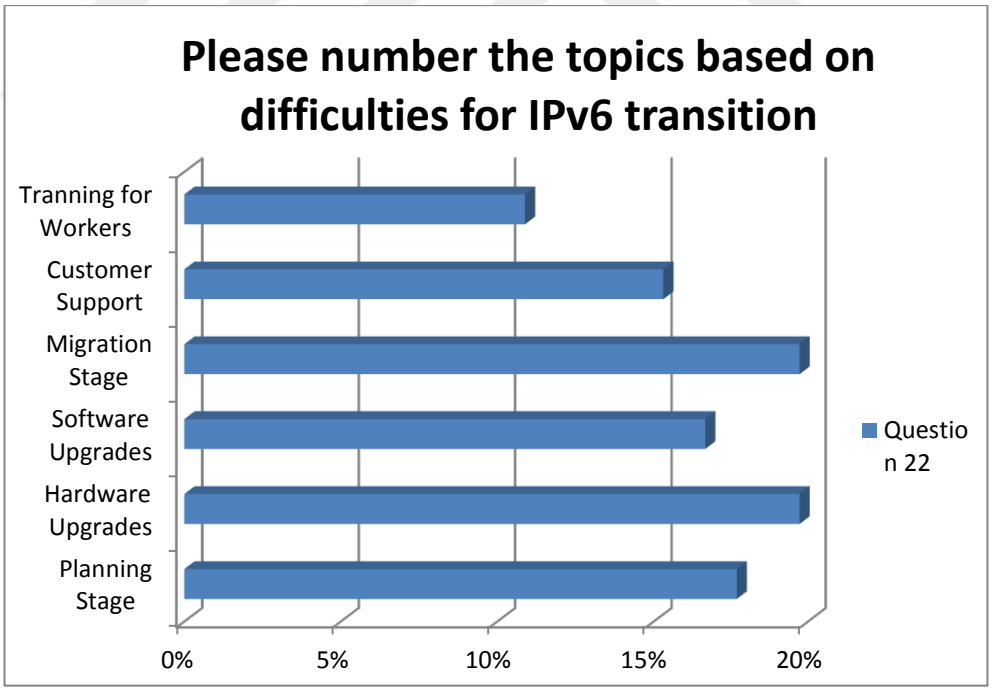


Figure 26 : Distributions of IPv6 Transition Difficulties

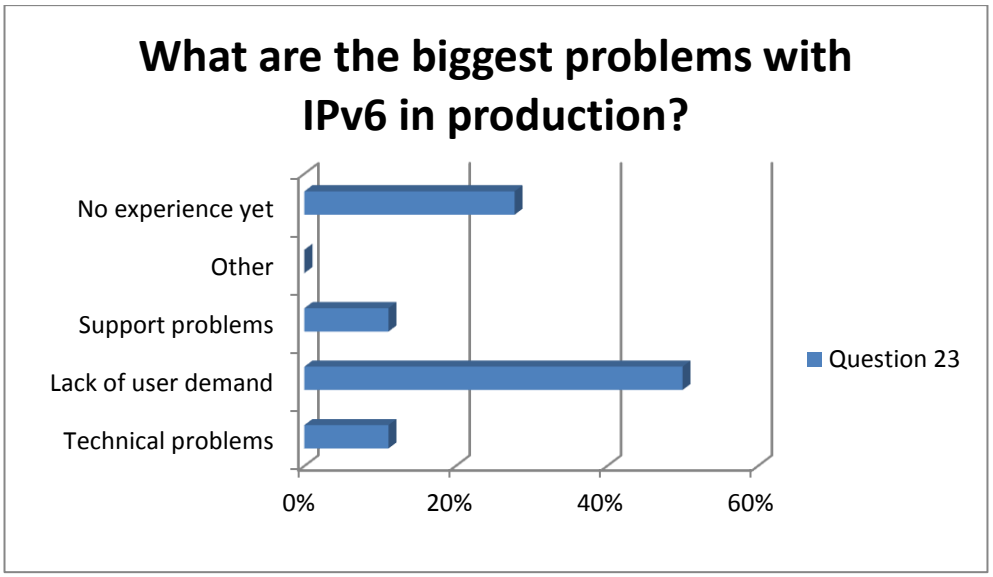


Figure 27 : Distributions of Problem Magnitudes

We wanted companies to rank the costs of IPv6 migration options and challenges of migration options in the question 21 and 22. According to the answers of question 21, ranking results from large to small in cost options are as follows: Hardware cost, software cost, labor cost and tranning cost. And according to the answers of question 22, ranking results from large to small based on difficulties are as follows: Hardware upgrades, migration stages, planning stages, software upgrades, customer support and tranning for workers. All these show that in IPv6 transition, the most important issue is hardware updates according to companies.

Finally we asked them what are the biggest problems with IPv6 production with question 23, nearly 50 % of them said lack of user demand is the biggest problem. After this option support problems and technical problems follow. However, some of the firms can not explain their biggest problems because they have no experience yet.

If we were to summarize the survey results, generally companies have enough information about IPv6. But they do not thinking of migration to IPv6 in the near future. Mainly network providers and ISPs have made preparations for the network side for IPv6 migration. Although customer-side preparations do not appear complete yet, hardware side and migration stages seem to involve the most difficulties according to companies in the transition to IPv6.

CHAPTER 9

CONCLUSION

Migration to IPv6 is not a basic process. There is no one day for changing the internet protocol IPv4 to IPv6. A lot of preparatory work has to be done before migration stage. First of all you need to have a very good knowledge about IPv6. Behind that needs should be defined for transition and there should be a very detailed transition plan and well-known dedicated team for IPv6 transition. Of course there are a lot of transition difficulties and adults. The most important challenges related to the transition are co-existence of both internet protocol, difficulties of dual-stack technique, very huge size of routing tables, network problems, application incompatibilities, CPEs which do not support IPv6, security considerations and of course cost of the transition.

My research and survey results show that there are still a lot of company which have not sufficiently knowledgeable about IPv6. Although depletion of IPv4 addresses, companies do not want to transtion to IPv6 because of its difficulties, adults and lack of customer demand. That time companies have found different solutions for their new IP requests like espically NAT.

According to all of these we can say that IPv6 transition will be slow about five years. After this five-year period, it is expected that there will be a further speedup of IPv6 transition and IPv6 traffic will be reach more than 50% of total traffic.

REFERENCES

1. **Kaushik D.,** "IPv6 - The Next Generation Internet", http://www.ipv6.com/articles/general/ipv6-the-next-generation-internet.htm (Data Download Date = 21.04.2014).

2. **Rosenberg B.,** "IP Packet Header", http://www.cs.miami.edu/~burt/learning/Csc524.092/notes/ip_example.html (Data Download Date = 17.02.2014).

3. **Network Layer Protocols,** "IPv6 Packet", http://cna.upc.edu.cn/rs/01/course/module6/6.1.4.5/6.1.4.5.html (Data Download Date = 13.03.2014).

4. **TechNet,** "IPv6 Addressing", http://technet.microsoft.com/en-us/library/cc781652(v=ws.10).aspx (Data Download Date = 19.06.2013).

5. **6WIND White Paper, (2003),** "IPv6: Features and Benefits", http://140.116.82.38/members/html/ms03/dclin/technique_paper/IPv6/IPv6%20Features%20and%20Benefiits.pdf (Data Download Date = 09.02.2014).

6. **IBM,** "Comparison of IPv4 and IPv6", http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzai2%2Frzai2compipv4ipv6.htm (Data Download Date = 02.04.2014).

7. **CommputerNetworkingNotes.com,** "Differences between IPv4 and IPv6", http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/difference-between-ipv4-ipv6.html (Data Download Date = 27.01.2014).

8. **Saklani A., Dimri S. C.,** "Technical Comparison between IPv4 & IPv6 andMigration from IPv4 to IPv6", http://www.ijsr.net/archive/v2i7/MDIwMTM2Mw==.pdf (Data Download Date = 16.03.2014).

9. **Bound J., (2005),** "Experimental RFC Proposal Internet Draft, Dual Stack IPv6 Dominant Transition Mechanism", https://tools.ietf.org/html/draft-bound-dstm-exp-03 (Data Download Date = 15.08.2013).

10. **Petri IT Knowladgebase,** "The IPv6 Transition", http://www.petri.co.il/ipv6-transition.htm. (Data Download Date = 21.10.2013)

11. **Tian J. and Li Z., (2001),** "The Next Generation Internet Protocol and Its Test", IEEE Communication Magazine, pp. 210-215.

12. **Kurose J. F., Ross K. W., (2009),** "Computer Networking: Top-Down Approach", Addison-Wesley, 5th Edition, pp. 370-373.

13. **Dr. Abuqayyas A.,** "ICT Consultant, Transition to IPv6 Drivers and Challenges", http://www.ipv6.om/gctcms/Editor/files/Transition%20to%20IPv6%20-%20Drivers%20and%20Challenges%20-%20ABUQAYYAS%20Compatibility%20Mode.pdf (Data Download Date = 12.01.2014)

14. **Minoli D., (2006),** "Voice over IPv6", Newnes, pp. 323-342.

15. **Shin M., Hong Y., Hagino J. I., Savola P., Castro Eva M., (2005),** "Application Aspects of IPv6 Transition", http://www.ietf.org/rfc/rfc4038.txt . (Data Download Date = 12.09.2013)

16. **NetworkWorld,** "Biggest Risks in IPv6 Security Today", http://www.networkworld.com/news/tech/2013/110413-ipv6-security-275583.html (Data Download Date = 12.11.2013).

17. **Wu P., Cui Y., Wu J., Liu J., Metz C.,** "Transition from IPv4 to IPv6: A State-of-the-Art Survey", http://www.cs.sfu.ca/~jcliu/Papers/IPv6.pdf (Data Download Date = 22.10.2013).

18. **Lind M., Ksinant V., Park S. D., Baudot A., Savola P., (2005),** "Scenarios and Analysis for Introducing IPv6 into ISP Networks", http://www.ietf.org/rfc/rfc4029.txt (Data Download Date = 12.09.2013).

19. **NetworkWorld,** "Top 10 Tasks for IPv6 Application Developers", http://www.networkworld.com/community/blog/top-10-tasks-ipv6-application-developers (Data Download Date = 28.07.2013).

20. **Ripe Network Cordination Centre,** "Requirements for IPv6 in ICT Equipment", http://www.ripe.net/ripe/docs/ripe-554 (Data Download Date = 16.09.2013).

21. **Kaushik D.,** "IPv6 - Hardware Vendor Support", http://ipv6.com/articles/hardware/IPv6-Vendor-Support.htm (Data Download Date = 12.08.2013).

22. **Internet Society,** "IPv6: Why and How Governments Should Be Involved", http://www.isoc.org/pubpolpillar/docs/ipv6-government-role.pdf (Data Download Date = 19.01.2014).

APPENDICES A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Reisoğlu, Serap

Date and Place of Birth: 15 July 1980, Ankara

Marital Status: Married

Phone: +90 505 581 79 53

Email: turan_serap@yahoo.com.tr

EDUCATION

Degree	Institution	Year of Graduation
B.Sc.	Çankaya Univ., Computer Engineering (Full Scholarship)	2004
High School	Seyranbağları Super High School	1998

WORK EXPERIENCE

Year	Place	Enrollment
2005- Present	Türk Telekom	Team Leader
2004 September	Çankaya Uni. Department of Computer Engineering	Research Asistant

FOREIGN LANGUAGES

Advanced English, Beginner German

HONOURS and AWARDS

1. University First Class Honors 2004
   Çankaya University

HOBBIES

Pilates, Nature Rides, Puzzle, Meeting with Friends,