IPv6-only Network Design and Deployment at IITH

Sharu Radhakrishnan

A Thesis Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of Technology

Department of Computer Science Engineering

June 2014

Declaration

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.

(Signature)

(Sharu Radhakrishnan)

CS12M1009

(Roll No.)

Approval Sheet

This Thesis entitled IPv6-only Network Design and Deployment at IITH by Sharu Radhakrishnan is approved for the degree of Master of Technology from IIT Hyderabad

(P. Rajalakshmi) Examiner
Dept. of Electrical Engineering
IITH

(T. Bheemarjuna Reddy) Examiner
Dept. of Computer Science and Engineering
IITH

(Dr. Kotaro Kataoka) Adviser
Dept. of Computer Science and Engineering
IITH

(Dr. Naveen Sivadasan) Chairman
Dept. of Computer Science and Engineering
IITH

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my advisor Dr. Kotaro Kataoka for his valuable guidance, constant encouragement, motivation, enthusiasm amd immense knowledge. Many individuals contributed in many different ways in completion of this thesis. I am deeply grateful for their support, and thankful for the unique chances they offered me. Finally, I thank my family for supporting me throughout all my studies at the institute.

I would like to make a special mention of the excellent facility provided by my institute, IIT Hyderabad.

.

Abstract

The aim of thesis is for deploying an IPv6 only daily base enterprise network in IITH and making it fully functional for the daily use and address some of the key current challenges.

The motivation for deploying IPv6 only network in the campus is due to the depletion of IPv4 address space. The IPv4 address space is only 32 bits, therefore has 2^{32} addresses whereas IPv6 addresses are represented by 128 bits thereby its address space consists of 2^{128} addresses which is quite enough to address all the particles in the world with an IP address.
Because of this scarcity of IPv4 addresses, many public organizations implemented NAT (Network Address Translation) to map private IPv4 addresses to a single public IPv4 addresses. So like this way NAT helped in dealing with the problem of IPv4 address scarcity. But NAT has got many disadvantages such as NAT adds complexities and it has basic disconnectivity problem with IPv6 only enabled devices. Also NAT has many security issues such as it is not compatible with IPSec protocol. Morover NAT was meant to be just a temporary solution for IPv4 exhaustion.
So came the IPv6 address which contains enough IPv6 addresses to address all the devices. But the problem is both IPv4 and IPv6 are not compatible and during initial phase of IPv6 deployment IPv4 and IPv6 coexist together.So there has to be some mechanism to translate IPv4 to IPv6 and vice versa.

In order to achieve this we applied a translation technology NAT64 which translates IPv6 address into IPv4 and vice versa. The need for translation technology is because of the fact that many of the service providers hav still not moved into IPv6.
So an IPv6 only network was set up in IITH campus using a NAT64 translator through which the IPv6 only clients connected to the IPv4 internet outside. But it was observed that some of the applications such as skype, instant messaging and VoIP applications were not working. This was because their APIs didnt support IPv6 or they carried IPv4 literals. In order to address this issue, a proxy server was set up and a tunnel was created and passed all IPv4 traffic for the not applications which didnt support IPv6 through that. But this is just a temporary solution.But there is lot of testing to be carried out for security purposes since there are many security issues which are to be addressed. Chapter 4 gives a detailed discussion on the general experiences with the network, the progress and some issues to be addressed.

Contents

Chapter 1

Introduction

1.1 Background

IPv4 has been the network layer protocol which routes most of the traffic in internet. It is 32-bit address. Now because of the fast rate of incease in number of internet enabled devices, it has come to a stage where 32 bit IPv4 address is not enough to assign to each and every device in the internet. IANA has already exhausted all the public IPv4 address pool in 2011.But IPv6 address has much longer address space of 128 bit. Therefore unlike IPv4 address which has only 2^{32} IP addresses, IPv6 has 2^{128} global IP addresses available which are more than enough to address every particle in the world.

Although we need IPv6 to address all the internet enabled devices in the internet now, IPv6 is not backward compatible with IPv4 protocol. But majority of the contents in internet still exists in IPv4. Therefore we cant take out IPv4 all of a sudden and IPv6 has to coexist with IPv4 protocol in parallel for some time. But this will lead to some issues with DNS, QoS, Security etc under this dual stack approach since IPv6 is not backward compatible with IPv4. Therefore there has to be some mechanism for both to communicate which leads to the need for transition technologies.

1.2 Specification : IPv4 vs IPv6

1.2.1 Addressing

The most important and obvious difference between IPv4 and IPv6 address is the space they occupy for addressing. IPv4 address is 32 bits long whereas IPv6 protocol is 128 bits long. Therefore with IPv4 address we will be able to address 2^{32} hosts whereas with IPv6 address we will be able to address 2^{128} hosts.

Three types of IPv6 address are there : Unicast address, Multicast address and Anycast Address.

As you can notice here that the broadcast address which existed in IPv4 protocol is now replaced with Multicast address in IPv6. A typical unicast IPv6 address consists of a 64 bit prefix and a 64 bit interface identifier. Therefore there are enough (2^{64}) public IPv6 addresses available

to address each and every hosts within a subnet and different subnets. This eliminates the need for NAT.Elimination of NAT brings end-to-end transparency in IPv6 only network.

Another benefit of addressing is that renumbering has now become much easier with RA(Router Advertisement) and SLAAC (Stateless Address Autoconfiguration). Also the long sized address format of IPv6 makes it easier for embedding IPv4 address in them.

1.2.2 IPv6 Improvements over IPv4 protocol

IPv6 protocol header is much more simplified than IPv4 protocol header.That is there is an "Optional Extension" field in IPv6 header. All the insignificant field which existed in IPv4 header is now moved to this Optional Extension header field in IPv6.
Also now the fragmentation in IPv6 is no more carried out by the router. Instead it is carried out by the end hosts. Because of these two improvements in IPv6 network now the processing on router is much simplified.

Now the next next improvement of IPv6 over IPv4 is the introduction of certain new protocols in IPv6 such as SLAAC protocol and making IPSec protocol mandatory requirement in IPv6. IPSec protocol accounts for network layer security and SLAAC(Stateless Address Autoconfiguration) protocol accounts for autoconfiguration of the IP addresses in the host interfaces without the need for a DHCP.

1.3 Transition Technologies

As the IPv4 and IPv6 have many protocol differences, they have inter-operability issue. Therefore the ISPs inorder to support a IPv6 should support a separate network in parallel to IPv4.
When the end host is configured as dual stack, normally they send DNS requests for both IPv4 and IPv6 address of destination parallelly.But dual stack is made inorder to move the network into IPv6 only and hence if the host gets back both IPv4 nd IPv6 address, then it will prefer IPv6 over IPv4.

Since IPv4 and IPv6 are not compatible, they hav individual addressing and routng system. Therefore without any additional mechanism, IPv4 and IPv6 wont be able to communicate with each other. But in real world scenario, both IPv4 and IPv6 will be coexisting, and different network operators and ISPs should be able to move to choose either IPv4 and IPv6 to comunicate. According to [3] there can be many scenarios depending on this which will be :
IPv6 network to IPv4 network
IPv4 network to IPv6 network
IPv6 network to IPv4 internet
IPv4 network to IPv6 internet
IPv6 internet to IPv4 network
IPv4 internet to IPv6 network
IPv6 internet to IPv4 internet
IPv4 internet to IPv6 internet
Therefore in such scenarios where two diferent networks having different protocols, they should be

able to communicate with each other.For this we have to enforce some artificial "inter-operability" mechanism which are known as transition mechnisms.

The transition mechanisms are broadly classified into three categories :

a. Dual Stack
b. Tunneling
c. Translation

1.3.1 Dual Stack Approach

In Dual Stack transition technology the devices support both IPv4 and IPv6 protocol. So the devices will be now able to communicate with both IPv4 and IPv6 protocol.
The advantage of dual stack approach is that now since device supports both protocol whenever communication over one particular protocol fails, it can always try for communication services with its other protocol. But the problem is still not solved. The shifting to IPv6 protocol was due to the reason that IPv4 addresses were getting deleted. Now in dual stack approach, it still demands all the internet enabled devices to have IPv4 addresses along with the IPv6 addresses and this does not solve the problem of IPv4 address depletion. Also some intelligence should be encorporated in the applications running in the end systems to choose which protocol to use for the communication.

1.3.2 Tunneling

Tunneling can be applied to only certain scenarios.The scenarios are if two IPv6 only devices want to communicate over an IPv4 network or viceversa.
The advantage of tunneling is that new network protocol is deployed without affecting the previous network implementation setup. But it has got certain disadvantages like tunneling cannot be applied to situations where an IPv6 only host wants to directly communicate with an IPv4 only host.

1.3.3 Translation Technology

IPv4/IPv6 translation technology is used for enabling direct communication between the IPv4 and IPv6 devices. Translation technology solves the disadvantages for both dual stack and tunneling approach by including a dual stack node only on the gateways located on the edge of the network where the translation is performed.

The basic principle of translation technology is semantic conversion of the protocol. That is if a packet IPvX is destined to an IPvY network, it the translating gateway will convert the IPvX packet to IPvY and if a packet IPvY is destined to an IPvX network, then that IPvY packet will be translated to IPvX.

Two types of translation technologies are there :

a. Stateless Translation
b. Statefull translation

1.4 Generic Issues

IPv4 and IPv6 are not directly compatible so programs and systems designed to one standard cannot communicate with those designed to the other. Therefore if one node supports only IPv4 and another supports only IPv6, then direct communication is not possible. During initial stage both IPv4 and IPv6 coexist.So most of the devices will be in dual stack. But some of the devices will not yet be upgraded to support IPV6. But keeping dual stack nodes in the internet wont solve the problem because IPV4 address depletion still happens since even now all nodes require IPv4 address. So we use translation technology which translates IPv4 address to IPv6 address and vice versa. But even using the translator there are many generic issues existing as following:

a. Bugs in some part of the code :

There are issues classified under bugs.For instance some operating system facilities support IPv6 but have annoying problems only uncovered in IPv6-only network.

b. Lack of IPv6 Support

Many applications from minor (some UNIX commands like arp) to major applications such as Skype still dont support IPv6.
For an application to be working in IPv6, they should be accessible to necessary APIs. IPv6 is supported by almost all commonly used APIs. Skype socket API doesnt support IPv6 because of which Skype doesnt work in IPv6 only environment.

c. Protocol and content (IPv4 Address Literal) Problem

Some of the protocols contain IP address in them.So when these protocols passes through a translator, it leads to many problems. For example some of the instant messengers wont work due to this. Also some part of the web pages refers to IPv4 address literals which are plain IP addresses rather than a domain name. This also leads to some part of the internet being inaccessible. This is because when these web pages with IPv4 literals are accessed by an IPv6 only network, the IPv4 literals embedded in html code may break the web pages. This happens because the DNS64 cannot synthesize the AAAA queries for the literals since they are not queried in DNS.
So many applications which make use of IPv4 literals fails when trying to access using IPv6.

d. Instant Messaging and VoIP Applications

This is the most important drawback of IPv6 only networks. In order for an application to be able to access internet via IPv6, it should be accessible to the necessary APIs. Many of the APIs support IPv6 but there are sertain languages like perl which doesnt support IPv6.
The most important out of these is that the skype wont work in IPv6. This drawback pulls many users from migrating into IPv6 only networking.

Out of the above mentioned issues we addressed solutions for problems (b) Lack of IPv6 support and (c) Issues with IPv4 address literals. But the sulotions are just a temporary solution.More research needed to be applied in this area.

1.5 Research Overview

This thesis deals with the deployment of an IPv6 only network. NAT64, an IPv4/v6 translation mechanism is used in order to achieve interoperability between IPv4 and IPv6 protocols. Therefore scenario addressed: **An IPv6 only network connected to internet through NAT64.**

In the current internet environment, the transition from IPv4 to IPv6 has become very critical and urgent. Due to the very high and ever increasing usage of IP enabled devices in the network environment, IPv4 having just 32bit address space is getting depleted which urged the need for IPv6 deployment which is of 128 bit address. IANA has already exhausted all the IPv4 addresses which push forward the deployment of IPv6.

During the initial stage of IPv6 deployment there will exist a stage when both IPv4 and IPv6 networks will coexist. Therefore it is indispensable to enable communication between the two heterogeneous networks while maintaining the availability of both even though IPv4 and IPv6 are incompatible. Many transition techniques were proposed years ago, even though many of them failed.

Here the difference between network and internet is Internet is a huge Network of Networks Out of the 8 different scenarios mentioned in section 1.3, we are considering the most important in the present environment and the scenario of our interest is : IPv6 network to IPv4 internet. That is deploying and implementing an IPv6 only network in the campus and making it access both IPv4 and IPv6 parts of the internet.

Therefore an IPv6 only network was setup in the campus allowing some of the clients in the institute to access over the internet through this network. But the network due to lack of proper testing had many security issues which are not addressed properly. Also othe network was tested against many applications and it was found out that many instant messaging and VoIP applications are not working details of which are explained in chapter 4.

Chapter 2

Related Work

2.1 NAT-PT

NAT-PT [2] used a combination of address translation scheme and protocol translation scheme in-order for the end nodes in v6 to communicate with end nodes in v4 and vice versa.

The NAT in NAT-PT [2] is similar to the basic IPv4 NAT. A basic IPv4 NAT translates one IPv4 address into another IPv4 address.The difference in NAT-PT and an IPv4 NAT is that the NAT in NAT-PT refers to the tranlsation of an IPv4 address into IPv6 and vice versa.

Application Level Gateway (ALG) [2] is an application specific agent that allows a V6 node to communicate with a V4 node and vice versa. Some applications carry network addresses in payloads. NAT-PT is unaware about the application and does not inspect the payload. ALG could work in conjunction with NAT-PT to provide support for many such applications.

However NATPT raised many issues.One of them is if you want NAT-PT to perform DNS mappings in the forwarding path, it has to see all IPv4 and all IPv6 traffic. NAT-PT must inspect all the traffic, not just the traffic that needs to be translated.That is in order to perform DNS-,apping NAT-PT, instead of inspecting only those packets which are destined to IPv4 address, it also inspects native IPv6 traffic. But whereas in case of NAT64, the native IPv4 traffic and native IPv6 traffiv never traverses the NAT64 translator.
So NAT-PT was declared no longer useful for IPv6 deployment and therefore later was replaced by NAT64.

2.2 464XLAT

464XLAT [3] is a combination of statefull and stateless translation. It is used to provide IPv4 services over IPv6 network.
As some of the applications are not yet supporting IPv6 services, this technology considers this situation and thus provides limited IPv4 connectivity by combining statefull translation at the core and stateless translation at the edge.

464XLAT does not require a DNS64 because the IPv6 nodes will just send native IPv4 packet and the address therefore can be resolved using an IPv4 only DNS server. This packet can then be translated into an IPv6 packet using a translator in the customer side(CLAT) passed through IPv6 network and translated back into IPv4 packet by a translator in the provider side(PLAT).But wherever only single translation is needed 464XLAT should be able to provide just that single translation.

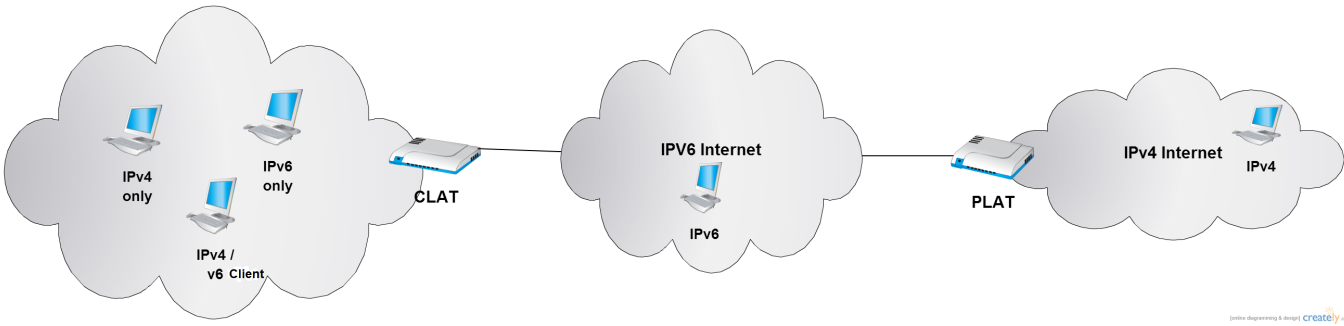

Figure 2.1: 464XLAT translation mechanism

PLAT(Provider-side translator)

It uses stateful translator technology which translates N:1 global IPv6 addresses to global IPv4 addresses and vice versa.

CLAT(Customer-side translator)

It uses stateless translation technology which algorithmically translates 1:1 private IPv4 addresses to global IPv6 addresses. The CLAT [3] can be implemented either in a router which can be a home router or a wireless 3GPP router or it can be applied to an end node such as a wireless mobile phone. But even if the CLAT functionality is implemented in an end node, it should perform all the gateway functionalities such as routing and packet forwarding, being a DHCP server and DNS proxy for the end clients etc.
CLAT uses different IPv6 prefixes on the CLAT side and on the PLAT [3] side therefore it does not require that the IPv6 prefixes of the IPv4-translatable IPv6 address and IPv4-convertable IPv6 address should be same.
Therefore it does not enable communication between a IPv4 node and a node in IPv6 internet.

IPv6 prefix handling

The CLAT [3] needs to be aware about two prefixes.One is the prefix which it uses for the translation mechanism. The other IPv6 prefix is the PLAT-side prefix which PLAT uses for the translation.
The PLAT-side prefix is used as the destination by the CLAT.

Traffic handling scenarios

The below table 2.2 describes the traffic handling scenarios of 464XLAT. So it is a client server model in which is the client is IPv6 only and server is IPv6 only, it is native IPv6 traffic and there

is no need of any translation. If the client is IPv6 and the server is IPv4 then there is translation occuring in the provider side gateway (PLAT) only. If both the client and the server are IPv4, then the traffic is treated as 464XLAT traffic , that is now the translation occurs both in the customer side(CLAT) and the provider side(PLAT).

server	client	Traffic treatment	Tranlsation location
IPv6	IPv6	end-to-end IPv6	None
IPv4	IPv6	Stateful Translation	PLAT
IPv4	IPv4	464XLAT	PLAT/CLAT

2.3 6RD Tunnel

6RD [4] is a mechnism to deploy IPv6 access to the IPv6 only clients which are served by ISP which supports only IPv4 infrastructure. Therefore it is a tunneling mechanism. Means it encapsulates the IPv6 packets originated from the IPv6 client inside an IPv4 header and then transports the packet through the IPv4 only supported ISP network to a destination IPv6 server.

The figure below shows 6RD tunneling mechanism

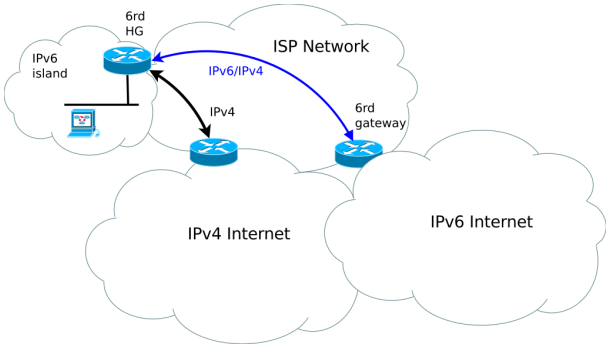

Figure 2.2: 6rd tunneling mechanism

It is derived from 6to4, a preexisting mechanism to transfer IPv6 packets over the IPv4 network, with the significant change that it operates entirely within the end-user's ISP's network, thus avoiding the major architectural problems inherent in the original design of 6to4.

2.4 ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) [4] is another tunnel mechanism for IPv6 hosts to communicate with each other across IPv4 networks.
An ISATAP host uses a link-local IPv6 address which has the fixed prefix of fe80::5efe/96 followed by the 32-bit IPv4 address of the host. The data plane procedure follows typical stateless manner. During the transmission of the encapsulated IPv6 packet through the IPv4 network, the IPv4 source and destination address which it gets is extracted from the IPv6 source and destination addresses. The control plane complexity of ISATAP is much higher than 6RD [4].

Chapter 3

Campus-wide Deployment IPv6-only Networking

This research proposes to deploy IPv6 only daily base network in IITH as a commodity infrastructure and addressing some of the key issues.

This research deploys IPv6 only network in parallel to the already existing IPv4 only network to move certain number of hosts from IPv4 to native IPv6.The other part of network was left unaffected considering the users who did not want to opt-in for IPv6 and also for those devices which supported only IPv4.So a small IPv6 only wifi network was created so that the IPv6 only clients may access the internet by connecting to an access point "IPv6-Only". But the underlying infrastructure was having only IPv4 connectivity. So the IPv6 only client cannot access internet(both IPv4 and IPv6).

Currently IITH has two ISPs, BSNL and NKN as shown in Figure 3.2 out of which NKN supports IPv6 connectivity. So IPv6 was enabled in the core routers and gateways CN, A2 and C2. Then the IPv6 only clients were able to access the sites having IPv6 address also (mostly the google sites). But in order to access IPv4 part of the internet, this was not enough. So a NAT64 translator was configured in the router connecting IPv6 only network to the internet inorder for the IPv6 only clients to access IPv4 parts of the internet.Figure 3.1 shows NAT64 translator in a gateway which connected the IPv6 only network to the outside IPv4 network in the institute intranet.
Currently some of the applications are not functioning in the IPv6 only clients such as the various instant messaging and VoIP applications. But these are because these applications do not support IPv6.

3.1 NAT64

NAT64 [4] is designed to be used when the communications are initiated by IPv6 hosts. Two types of NAT64 are there: stateless and stateful. We use stateless NAT64(tayga) so that the NAT64 translator doesnt have to maintain the IPv4-IPv6 mapping states now for each and every translation which can increase the memory usage. NAT64 mechanism is to allow IPv6 clients to communicate with IPv4 servers. The NAT64 server situates in the gateway connecting the IPv6 only network segment of 32-bits which will be the IPv6 network prefix used for allocating the IPv6 address for the

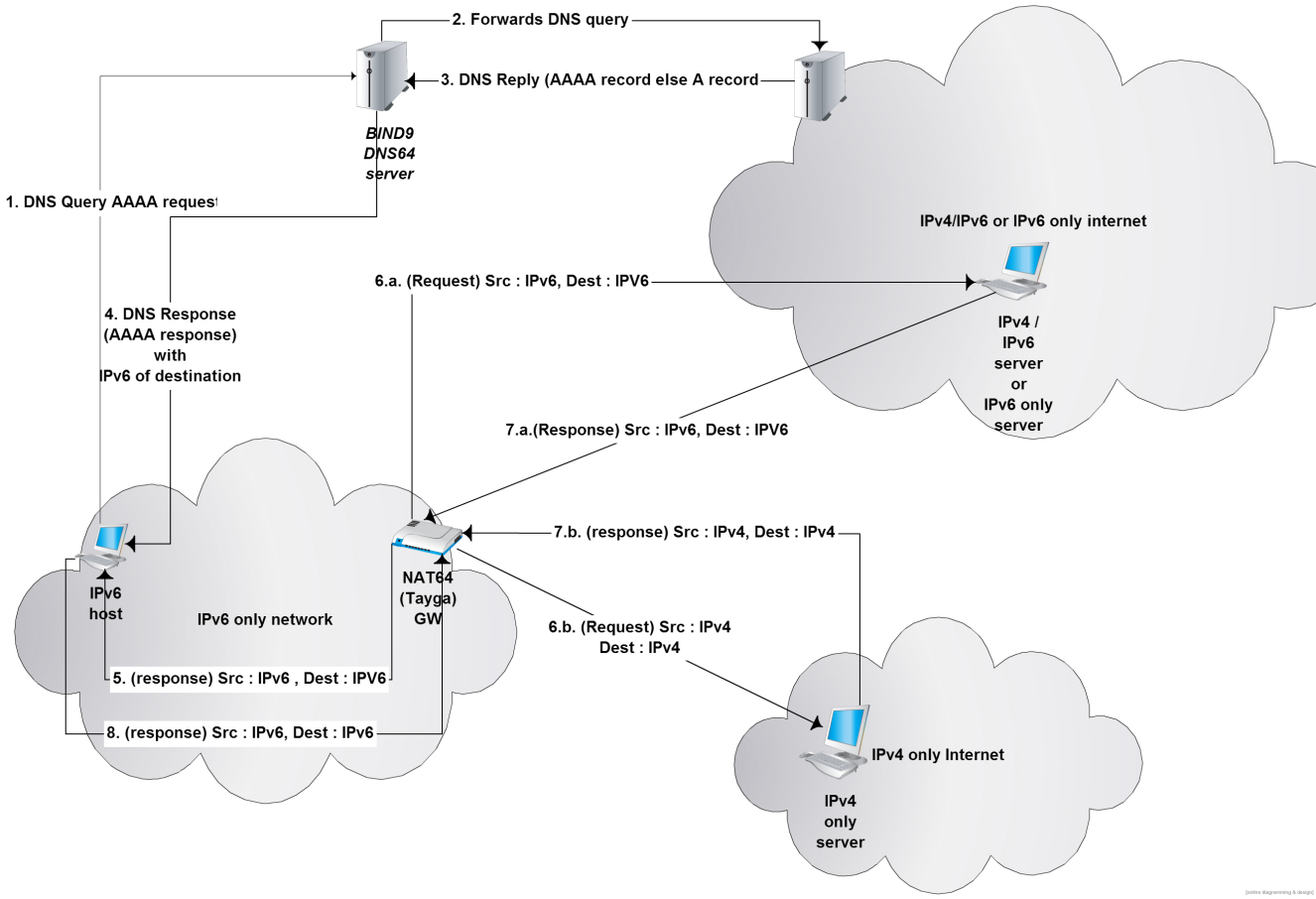

Figure 3.1: IPv6 only client connected to IPv4 and IPv6 part of the internet using NAT64

IPv6 only hosts and the outside internet. There that NAT64 gateway (router) will be a dual stack host whose one interface will be having IPv6 address and the other interface having IPv4 and IPv6 address.

The IPv6 client embeds the IPv4 address it wishes to communicate with using these bits, and sends its packets to the resulting address. The NAT64 server then creates a NAT-mapping between the IPv6 and the IPv4 address, allowing them to communicate.

3.2 DNS64

DNS64 is a DNS server that when querried for a domain's AAAA records and if finds only an A record, synthesizes the AAAA records from the A records. The first part of the synthesized IPv6 address points to an IPv6/IPv4 translator and the second part embeds the IPv4 address from the A record.

The DNS64 maintains an IPv6 address prefix which will be the same prefix which the NAT64 uses for the transltion.

Procedure 1 to 4 in Figure 3.1 shows how DNS64 serves an IPv6 only host.DNS64 when queried for an AAAA record, checks if the AAAA record is found in it.If it doesnt have will forward the query

to a real DNS server(can be any public DNS server) for the AAAA record and if found,then it will get back AAAA reply from the real DNS server then will respond back to the client with the AAAA record(IPv6 destination address), else if not found, it will query real DNS server for A record, get the A reply from the real DNS server and prepend the IPv4 address in A record with the prefix to get the AAAA record and reply back to the IPv6 client with the AAAA record (IPv4-convertable IPv6 address).

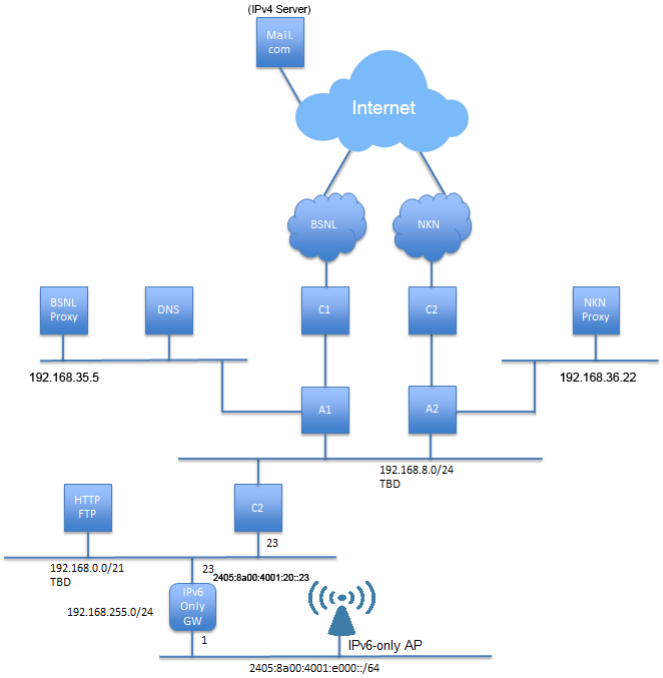

Figure 3.2: IITH network diagram

The NAT64 software used, TAYGA only handles translation between IPv4 and IPv6 and does not cover connectivity between the IPv6-enabled sites and IPv6 servers on the internet.
Conceptually, the IPv6 Internet is a separate global network from the IPv4 Internet. So the institution needed to establish an upstream link to the Internet which operates in parallel to the existing IPv4 upstream link in order to get connectivity to IPv6 enabled sites. So the IPv6 service was enabled in the institution servers and core routers as shown in Figure 3.2 by the upstream provider, NKN which supports IPv6 natively.
The DNS64 software used was bind9 which was configured as a DNS local cache.

The hosts in the institute environment have a heterogeneous hardware with PCs, laptops and routers running linux, Mac OS and Microsoft Windows. And the common uses of the network include web browsing, email, Voice over IP (VoIP) applications, Secure Shell (SSH), instant messaging, gaming, streaming.

3.3 IPv6 only Implementation

The IPv6-only network was provided as a parallel network on the side of the already existing dual stack network. A separate wireless network bridged to this existing IPv4/v6 dual stack backbone was created as the new IPv6 only network. We introduced IPv6-only gateway as NAT64 router as well as DnS64 server. The following table 3.3 shows the router specification.

OS	Ubuntu 12.04.3
NAT64	Tayga 0.9.2
DNS64	Bind 9.8.1-P1
CPU	Intel Core i7
RAM	11.7 GiB
NIC	Realtek RTL8111/8168B PCIe ethernet controller

Table 3.1: Router Specification

The router was located on the edge of the IPv6 only network which was connected to the existing IPv4/v6 dual stack network. The router was configured to act as a NAT64 router by installing tayga 0.9.2 and configuring it. DNS64 was configured on the same router by installing bind9 on the same machine and configuring it as a local cache.

No IPv4 routing or DHCP was made in this network. Radvd was installed in the NAT64 router so that it sends the router advertisements (RAs) from which the IPv6 only hosts learns the IPv6 prefix and can automatically configure the IPv6 addresses for them using SLAAC (Stateless Address Autoconfiguration) [4] protocol.

This new IPv6 only network needed a /64 prefix to be advertised by the router for the addressing of IPv6 only clients and an additional /64 prefix for the NAT64 device to represent the IPv4 destinations in the IPv6 only network.

The NAT64 devices have dual stack conectivity and their DNS64 function can use both IPv4 and IPv6 when requesting information from DNS. Therefore if the destination host has both A and AAAA record, then the host in the IPv6 only network will contact the destination over IPv6. Therefore IPv6 services were enabled in the core routers and servers in the institute intranet. And the destinations with only A record will be given a synthesized AAAA record which will be used for communication.

Appendix .2 gives the router configuration and the tayga configuration. A quick startup script tunnat.sh was created in order to create the tunnel interface and set the routing rules to the NAT64 interface and also to set the firewall rules.

Chapter 4

Deployment Progress in IITH

With the help of a monitoring server cacti in institute and wireshark, and many packet dumps it was ensured that the IPv6 network deployed in the campus is working properly.

There are some issues still existing in the network such as some of the applications still dont work with IPv6 in the scenario of IPv6 network to IPv4 internet. But this has got nothing to do with the NAT64 translator.So either the application side developers have to ensure for this that they use appropriate APIs and support IPv6 or we may introduce further mechanisms to resolve such issues.

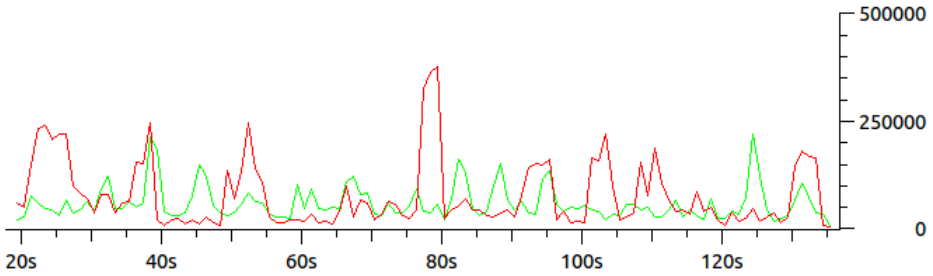

Figure 4.1: Graph showing both IPv4 and IPv6 traffic in bits per second in the outgoing interface of NAT64 router

In the figure 4.1 the red color shows the IPv6 traffic and the green color shows the IPv4 traffic.X-axis indicates the time in seconds and the Y-axis gives the bits.

4.1 General Experiences

The network was tested on linux (Ubuntu), Mac OS and windows 7, raspberrian operating system. There were not any practical differences in the browsing (http and https) experience between IPv4 and IPv6 only. Also many applications such as email, chats, instant messaging, videos, media streaming, some operating system services such as apt-get in Ubuntu worked well.

But different operating systems behaved differently under the ipv6 only environment. For example in the windows system, it was not getting the correct default gateway and the DNS64 address using RAs (Router Advertisements) whereas in the Linux and MacOS operating systems it did.

Aliases were added to the DNS64 device to allow it to receive packets on the well-known DNS

server addresses that Windows operating systems use (fec0:0:0:ffff::1, fec0:0:0:ffff::2, and fec0:0:0:ffff::3). Therefore we had to manually configure the appropriate DNS64 IP and the default gateway IP in the windows operating system in order to support IPv6 only networking which will become difficult for end the users. So DHCPv6 server was installed on the NAT64 router in order for the windows clients to get the DNS64 address by default.

Also in windows the windows update installing the updates worked but downloading the new updates was not working.

4.1.1 Lack of IPv6 Support

Many applications from minor (some UNIX commands) to major applications such as Skype still dont support IPv6.
For an application to be working in IPv6, they should be accessible to necessary APIs. IPv6 is supported by almost all commonly used APIs. Skype socket API doesnt support IPv6 because of which Skype doesnt work in IPv6 only environment[1] .

4.1.2 Issues with IPv4 address literals

IPv4 address literals (contents on some web pages which refer to plain IP addresses rather than host and domain names) are inaccessible by an IPv6 only network. When accessed by an IPv6 only network, the IPv4 literals embedded in html code may break the web pages. This happens because the DNS64 cannot synthesize the AAAA queries for the literals since they are not queried in DNS. So many applications which make use of IPv4 literals fails when trying to access using IPv6.

4.1.3 Instant Messaging and VoIP Applications

Many applications were tested in IPv6 networking the details of which is shown in Appendix A .1. It was observed that many instant messaging and VoIP applications failed to work in IPv6 only enviornment.

4.1.4 Comparison of NAT64 with other methods

Here the web access with NAT64 was compared with the web access through IPv4 only and native IPv6. Fot this purpose we used wget to go through the top 300 web sites being listed in a text file in linux machine.
Separate tests were conducted with IPv4 only network, IPv6 only network with NAT64. The tests were repeated to find the average failure.

While accessing the web using IPv4 only network it showed some error rate.Now this error rate can be either because it failed to load a web page page itself or some contents such as image in that web page was not loaded properly. But the access through wget is different from the access through a normal browser. Some web sites refuse to give contents to the wget. This can be the cause of the error rate which occured.

Now while accessing the web using IPv6 only network without any translator as expected it showed a very high, more than 90 percent error rate.This is because most of the contents in internet doesnt support IPv6.

While accessing the web using IPv6 only network using NAT64, it showed an error rate of approximately 0.99 percent. This error rate can be mostly due to IPv4 address literals.

4.2 Security Issues

IPv6 deployment is growing in the internet society now. For these deployments to be successful it is important for the network to be secure and reliable and Qos(quality of service) must rival IPv4 infrastructure. To understand the IPv6 security issues, we need to have a clear understanding on how secure IPv6 is compared to IPv4.
Network users expect some similarity between IPv4 and IPv6 functionality. Simiarily network administrators also expect that there is a high degree of security in both IPv4 and IPv6 networks.

Therefore the secure mechanisms we use in IPv6 is similar to that of the security mechanisms we use in case of IPv4 networks which includes :

a. firewalls in the end systems to make them secure

b. Standalone firewalls for deep packet inspection

c. Employing packet filters in routers and switches to remove suspicios packets

d. Intra-subnet security mechanisms(DHCP snooping allowing the DHCP outgoing packets to pass through only a specific port).

Above the network layer, all the functionalities remain same in both IPv4 and IPv6 [7] . For example, TCP and UDP havnt changed and they run over IPv6 in same way as it was in IPv4. But between the network and the transport layer there are many differences in the fuunctionalities amd implementation between IPv4 and IPv6. For example in IPv6 protocol header, there is an extra extension header making the layer 4 inspection in IPv6 more complex. Because of this extension header it reduces the performance of the devices which have packet filtering implemented in them which increases the probability of security threat in IPv6. But also IPsec is mandatory in IPv6 whereas not in IPv4 making IPv4 more prone to security threats.

Therefore most of the security difference between the IPv4 and IPv6 are mainly because of the implementation difference between IPv4 and IPv6. Some of the common security threats in IPv6 which needed to be taken care of are :

a. The end systems and the network devices protocol stacks hav not been thorougly tested as their IPv4 counterparts which makes them prone to the attack from hackers. Therefore as iPV6 deployment progresses over a wider range we can expect many flaws in the security due to this.

b. Lack of exposure to IPv6 enviornments to the network and security engineers can account for many occasional security challenges.

c. Unintentional connectivity to the protected parts of internet can happen through IPv6-over-IPv4 tunnels and hence can expose their internal or closed resources to the outside world. If there is no proper firewall and security mechanisms in the end host implemented in such a scenrio this can lead to many security flaws.

d. Most impotanty the IPv6 implementations from the networking vendors still lack some first hop security features needed to make IPv6 as secure as IPv4.First hop security deals with the security issues associated with the local links(Layer 2).Traditional layer two security differs between IPV4 and IPv6 due to the difference in the functionalities in layer 2 in IPv4 and IPv6.
Many first-hop attacks are available to attckers.Some of the threats to the IPv6 first-hop security are:

Router Discovery Related Concerns

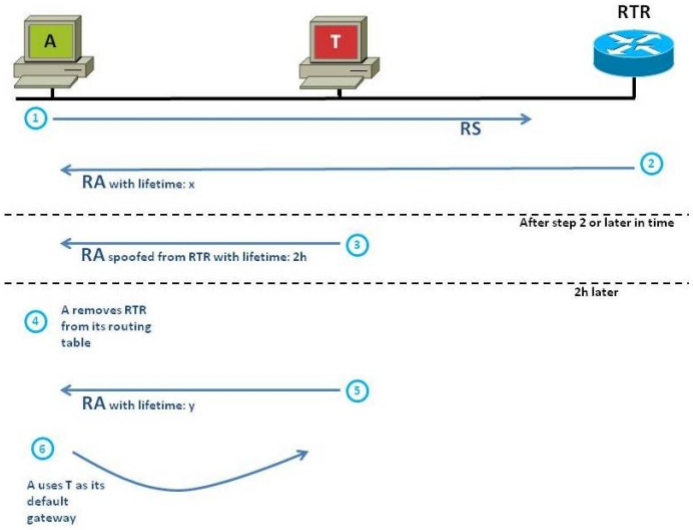

Figure 4.2: Attack against IPv6 router discovery [7]

IPv6 Neighbor Discovery uses ICMPv6 messages[7]. In order to find the router in its link, an IPv6 only node will send a Router Solicitation ICMPv6 message for the information of the routers in its link.
Therefore in this scenario an IPv6 host A sends ICMPv6 Router Solicitation message on its link to find the routers. A legitimate router R then replies back with a ICMPv6 Router Advertisement message with a lifetime of x and lets A know that R is the router in the link.

As shown in the above Figure 4.2, T is the intruder. A will first send router solicitation message. Then the router R will reply back with the router advertisement message with a lifetime of x units. Then the host A will add R as its default router in its routing table entry with a lifetime of x. Now the intruder will somehow try to install itself in the link as shown in Figure 4.2 and will spoof a Router Advertisement message as the router R to the host A with a lifetime of 2 hours for exxample

as shown in the figure. If the remaining time is less than 2 hours it will just ignore or else after 2 hours the host will wait for next 2 hours and then remove router R from its default router entry. Now intruder T is free to insert itself as the default router in the routing table entry of host A. So the intruder T now sends Router Advertisement and if T succeeds to become the deafult router of A, now T can listen to all traffic from the host A and launch man-in-the-middle attack.

Neighbor-Discovery Related Concerns

a. Attack against IPv6 auto configuration

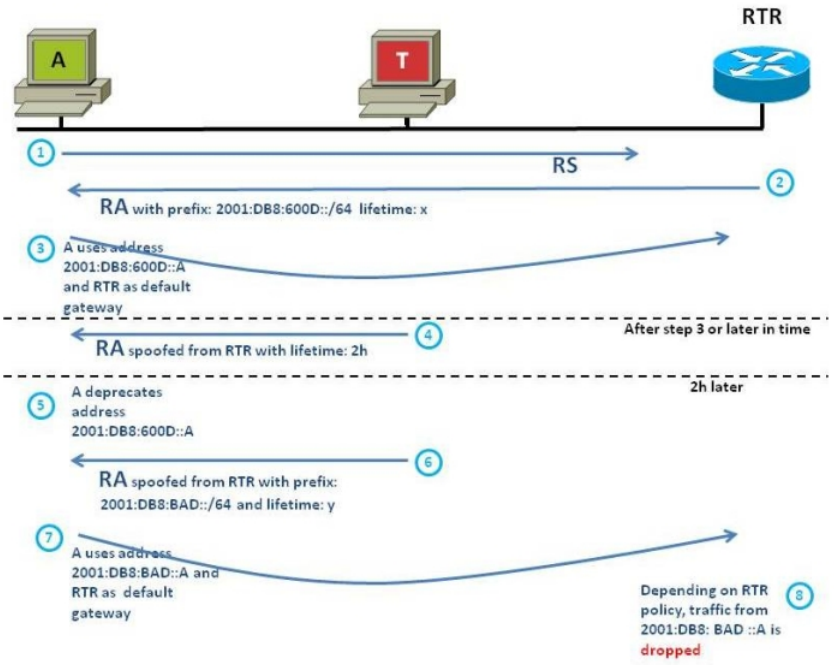

Figure 4.3: Attack against IPv6 auto configuration[7]

The Figure 4.3 shows an attack against IPv6 autoconfiguration. Here the host A wil first send RS message to find the router in its link. Then router R will reply back with RS message with a IPv6 prefix with lifetime x. Then router R will be entered in the host A's routing table entry as default router for a period of x and will autoconfigure its IP address based on the IPv6 provided by this router. Now if malicious host T succeeds to install itself in the link between the host and the legitimate router, it will send another RA message with a new IPv6 prefix with a lifetime of 2 hours for example. Now if the remaining time is less than 2 hours, the host A will ignore the new prefix and wait for the remaining time. Else the router will remove the legitimate router from its routing table entry and make the intruder T as its default router and change its IP address based on the new prefix provided by the intruder. Now if the host A tries to connect to the internet, legitimate router R may deny the new IP address from traversing around the network.
Therefore if IPv6 address autoconfiguration is used and if first-hop security is not employed , T can potentially blackhole hosts in the loal link.

b. Attack against IPv6 address resolution

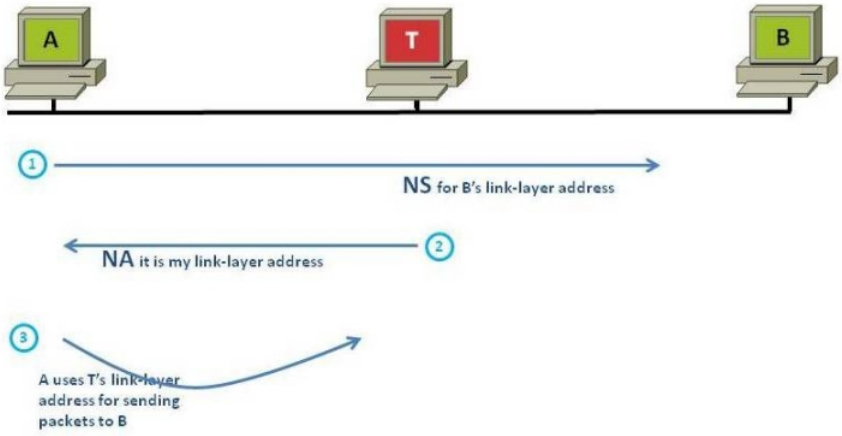

Figure 4.4: Attack against IPv6 address resolution[7]

The Figure 4.4 shows attack against IPv6 address resolution. In IPv4 ARP does the job of address resolution. But in IPv6 networking, ICMPv6 does that job.
So if a host A wants to send a packet to host B which is on its local link, then host A needs to know the MAC address of host B to set layer 2 frames destination MAC. So the host A will send a ICMPv6 neighbor solicitation (NS) message requesting link layer address of host B. Then the host B wil reply back host A with ICMPv6 Neighbor Advertisement (NA) which contains its MAC address. Now the host A will make a neighbor cashe entry for host B which maps host B's MAC address to IP address.
Now if an intruder T manages to install itself in the link between then, it can impersonate host B which inturn interscepting all packets destined for host B from A.

c. Attack against DAD

Duplicate Address Detection (DAD) is a protocol that lets an endhost interface verify the uniqueness of its IP address. If a host A wants to perform DAD, it will send a ICMPv6 NS message for its IPV6 address it wants to claim. If no other hosts reply back with a NA message, then it can make sure that no other hosts have that IP address and hence can assign that address to itself.

Figure 4.5 shows attack against DAD where host A performs DAD by sending out a ICMPv6 NS message.Then if a intruder T installs itself in tht link, it can continously send the NA message for whatever NS message the host A sends claiming that it possesses that IP address.Thereby denying the host A to assign an IP address it itself.This is a denial-of service attack.

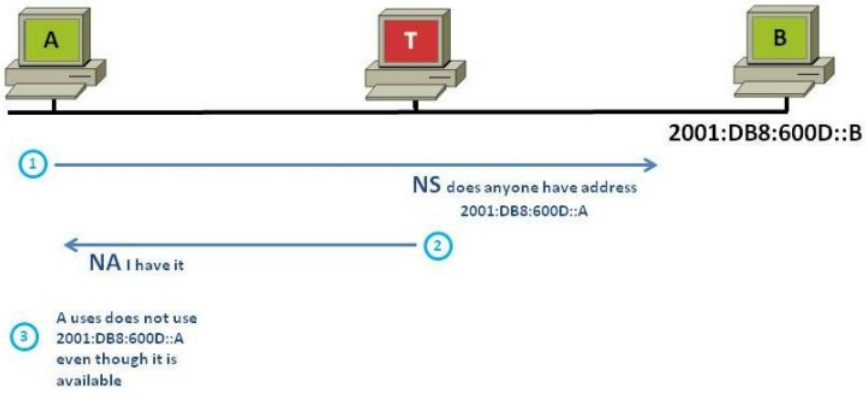

Figure 4.5: Attack against Duplicate Address Detection[7]

DHCPv6 Concerns

As the DHCP assigns IP address in IPv4 enviornment, in IPv6 networkinng there is DHCPv6 which is a statefull protocol for address assignment.DHCPv6 is also compatible with stateless addressing.That is it can just provide the configuration information to hosts and does not provide address assignment.It will do address assignment to only those hosts which requests for it. Just like in the case of IPv4 DHCP, DHCPv6 is also prone to attacks.Therefore if a malicious user is able to install a malicious DHCPv6 server in the local link, it can send out the configuration information and bad address assignments.
This DHCP protection is very important both in IPv4 and IPv6.

4.3 Solutions for non-functional Applications and IPv4 address literals

4.3.1 Using a Proxy Server [1]

Configure the end systems to use the proxy for those applications and web pages which doesnt work on IPv6.
Proposed Solutions:

SSH tunneling

Set up a dynamic tunnel in the local system through 192.168.0.23 via SSH. This will create a SOCKSv5 proxy on the local system listening on a specified port (say 1080). Configure the required applications running on the local machine to use the SOCKS proxy 127.0.0.1:1080 (No Authentication)

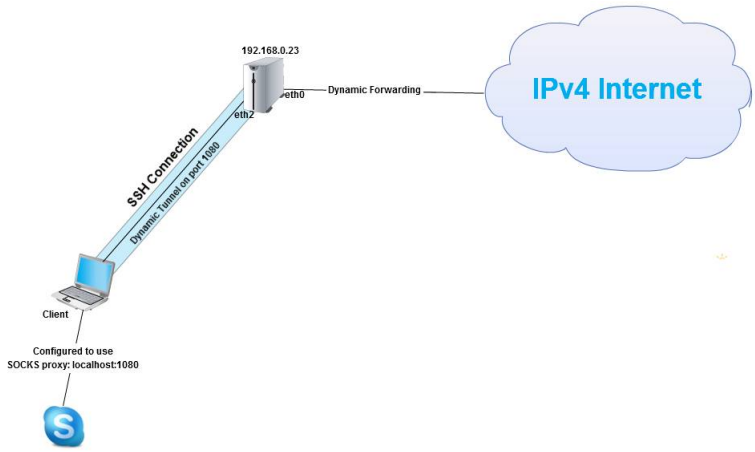

Figure 4.6: Dynamic tunneling

Local Port forwarding over SSH:

Set up a local tunnel(static tunneling) to one of the institute proxies (say 192.168.36.22:3128) through 192.168.0.23 over SSH. The local machine then listens on a specified port (like 3128) and forwards all incoming requests to the institute proxy through the SSH connection with 192.168.0.23 Configure the required applications running on the local machine to use the HTTPS proxy 127.0.0.1:3128 (Additional Authentication info should also be supplied)

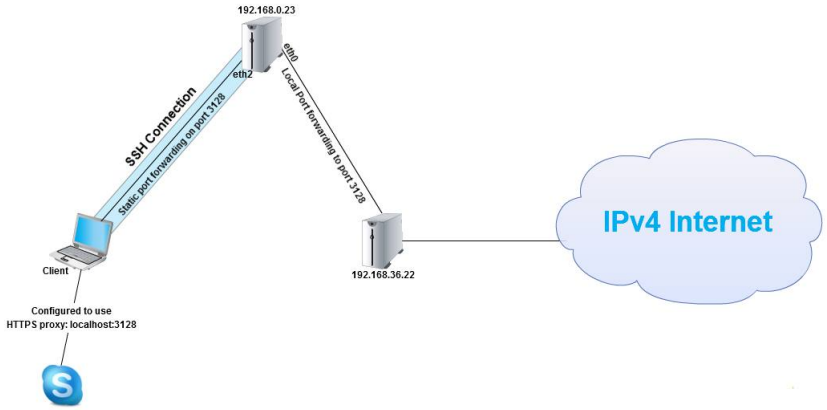

Figure 4.7: Static tunneling

Disadvantage of using proxy as the solution

The disadvantage of using this proxy as a solution for applications which wont work with IPv6 is that, we have to manually configure each and every end systems in which the IPv4 only supporting applications are running. The solution to this problem is either upgrading IPv4 only sites to support IPv6 also.

4.3.2 WebRTC

WebRTC is an open source project which enables real time communication capability in web browsers using a javascript API.
As from the observations, it was seen that the browsers worked well in the IPv6 network just as they worked in IPv4. So for the applications like skype which doesnt support IPv6, there is always an option for using WebRTC based applications for real time communication.

4.3.3 Clean up web pages from IPv4 literals

IPv4 address literals seems to be fairly rarely encountered atleast so that they would be rarely noticed in a regular web surfing.
Reports [1] shows that the total IPv4 literals in the internet will come to less than 1 percent, which is soo less. But then also we cant make a clear decision on this wether to ignore those web contents with IPv4 address literals because it also depends on the importants of the contents in them.

4.4 Solutions for First-Hop Security Issues

Cisco has implemented RA guard feature to protect router advertisement and there is implementation of SEND(Secure Neighbor Discovery) protocol which provides cryptographic measures ensuring more security. But these all are complex methods when compared to ARP inspection and DHCP(Dynamic Host Configuration Protocol) snooping in IPv4 world.

As a solution for this first-hop security we can apply either AP isolation for the man-in-the-middle attacks or configure static neighbor cache entries for security issues rising from neighbour discovery.

Chapter 5

Conclusion and Future Work

The conclusion of the thesis is that, a fully functional IPv6 only network deployed in the campus and is available for daily use. The network was tested with several applications and we observed that :
a. There was not much difference in the browsing experience between IPv6 only network and an IPv4 only network.
b. Some of the applications mainly the VoIP and instant messaging applications like skype, google talk etc dont work in IPv6 only network. But this problem was solved using a proxy. Also for the applications like skype we have another alternative WebRTC based applications for real time communication in IPv6 only network.

We also did the comparison of browsing experience(using wget) of IPv6 only network with NAT64 and without NAT64 and IPv4 only network and observed that the error rate increases in following order : IPv4 < IPv6(with NAT64) < IPv6(without NAT64)

We also examined certain security issues specifically the first hop security issues in IPv6 and summarized some possible solutions.

As future work, the network coverage of IPv6 only network should be extended in the IITH campus.And apply the security issues suggested in section 4.4 to the IPv6 only network. Also more security testings have to done in the IPv6 network to take care of the security attacks mentioned in section 4.2.

References

[1] J. Arkko, A. Keranen, "Experiences from an IPv6-Only Network draft-arkko-ipv6-only-experience-05" , IETF, February 7 2012.

[2] G. Tsirtsis, P. Srisuresh "Network Address Translation - Protocol Translation (NAT-PT)" RFC 2766, February 2000.

[3] M. Mawatari, M. Kawashima, C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation" , RFC 6877,IETF, April 2013.

[4] Peng Wu, Yong Cui, Jianping Wu, Jiangchuan Liu, and Chris Metz, "Transition from IPv4 to IPv6: A State-of-the-Art Survey " , IEEE Communication Surveys and Tutorials, VOL. 15, NO. 3, 2013.

[5] Deka Ganesh Chandra, Margaret Kathing, Das Prashanta Kumar " A Comparative Study on IPv4 and IPv6 " , International Conference on Communication Systems and Network Technologies, 2013.

[6] Enis Hodzic, Sasa Mrdovic, " IPv4/IPv6 Transition Using DNS64/NAT64: Deployment Issues " , IX International Symposium on Telecommunications (BIHTEL), Sarajevo, Bosnia and Herzegovina, 2012.

[7] Cisco, " IPv6 First-Hop Security Concerns "

.1 Appendix A

App Name	Description	Functionality	Test Notes
Google Talk	Broken	communication	chat works , but video call fails to connect
Google+	Broken	social	updated status and uploads, but no video hangouts. Says it times out while connecting
Gmail	Works	communication	Sent mails, chat works
IP Track	Broken	utilility	does not show ipv6
Skype	Broken	communication	cannot sign in
Youtube	Works	video	search and played videos
Thunderbird	Broken	communication	cannot log in
Twitter	Works	social	login, viewed tweets, posted pictures
Facebook	Works	social	login. Viewed news feed , chat , posted pictures
WhatsApp	Works	communication	send and received messages
Watch ESPN	Broken	video	Watched video
Google Navigation	Works	Maps	Used gps to map a route
ABC News	Works	news	loads news stories, plays videos
Amazon	Works	shopping	signed in, added item to cart
Amazon Kindle	Works	shopping	signed in, downloaded free kindle reading app and book
Amazon Market	Works	shopping	downloaded market, signed in
Amazon MP3	Works	shopping	played a sample
Angry Birds	Works	Game	played game
Antivirus Free	Works	utility	scanned files, loads ads
Bing	Works	search	search, maps, news
Calendar	Works	utilility	syncs with google
Camera	Works	utilility	Shares with facebook and google
Chrome	Works	web browser	loadedcpages
CNN	Works	news	loaded news
DailyHoroscope	Works	news	loaded horoscope
Dropbox	Works	cloud	uploaded photo and shared document
ebay	Works	shopping	load items and added to cart
ESPN Scorecenter	works	news	loads scores and news
Facebook for Android	Works	Social	Updates, Photos, messages
Facebook Messanger	Works	Social	messages
File Manager	Works	utilility	loads ads, shows system status
Firefox	Works	browser	loads web pages
Flash	Works	Video	played video
Flipkart	Works	shopping	Search items, selected and added to cart
Flickr	Works	photos	logged into account, uploaded photo
Fruit Ninja Free	Works	Game	loaded ads
Go Weather	Works	weather	checked weather
Google Books	Works	shopping	displays text
Google Docs	Works	cloud	load and edit docs
Google Drive	Works	file sharing	load and edit docs and added document
Google Earth	Works	map	loads places
Google Finance	Works	Finance	loads stocks and news updates
Google Maps	Works	maps	loads maps, does directions
Google Search	Works	utilility	Did searches
Google shopper	works	shopping	searched for items
Google Translate	Works	utility	translated language

Google Videos	Works	video	Watched video
Linkedin	Works	social	logged in
Myntra	Works	shopping	searched for items
opera mini	Works	browser	loads web pages
opera mobile	Works	browser	loads web pages
Paypal	Works	finance	login
Real Player	works	music	played music
redbox	works	video	loaded movie info
Yatra	Works	travel	Searched for hotels and flights
Yahoo	Works	news	loads news and portal info
Yahoo Answers	Works	utility	logged in, answered question
Yahoo Mail	Works	communication	loads mail
Yahoo Music	Works	music	loaded songs
Yahoo News	Works	news	loaded articles
Yahoo Search	Works	search	did voice search
Yahoo Weather	Works	weather	shows weather

.2 Appendix B

Router Configuration :

auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.0.23
netmask 255.255.248.0
network 192.168.0.0
gateway 192.168.0.100
iface eth0 inet6 static
address 2405:8a00:4001:20::23
netmask 64
gateway 2405:8a00:4001:20::1

auto eth2
iface eth2 inet6 static
address 2405:8a00:4001:e000::1
netmask 64

Tayga 0.9.0 configuration :

tun-device nat64
ipv4-addr 192.168.255.1

prefix 2405:8a00:4001:e001::/96
dynamic-pool 192.168.255.0/24

Tunnat.sh startup script configuration

route add 192.168.255.0/24 dev nat64
ip route add 2405:8a00:4001:e001::/96 dev nat64
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o nat64 -m state –state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i nat64 -o eth0 -j ACCEPT
tayga
/etc/init.d/bind9 start