إقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

استجابة أنظمة التشغيل للحزم الاعلانية للموجهات في بروتوكول IPV6
Operating system Response to Router Advertisement Packet in IPV6

أقر بأن ما اشتملت عليه هذه الرسالة إنما هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وإن هذه الرسالة ككل، أو أي جزء منها لم يقدم من قبل لنيل درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

DECLARATION

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification

اسم الطالب: هيثم رياض حجي عبد النبي

Student's name

التوقيع:

Signature

التاريخ: 2015/8/30

Date:

Islamic University of Gaza

Deanery of Higher Studies

Faculty of Engineering

Computer Engineering Department

Operating System Response to Router Advertisement Packet in IPv6.

استجابة أنظمة التشغيل للحزم الاعلانية للموجهات في برتوكولIPv6

Submitted by:

Saeb Reyad Abd El Nabi

Supervisor:

Prof. Mohammad Mikki

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in computer engineering

2015 - 1436

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

مكتب نائب الرئيس للبحث العلمي والدراسات العليا   هاتف داخلي 1150

Ref ...../35/ج.س.غ/ الرقم

Date 2015/08/16 التاريخ

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة شئون البحث العلمي والدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحث/ **صائب رياض صبحي عبدالنبي** لنيل درجة الماجستير في كلية ***الهندسة*** قسم **هندسة الحاسوب** وموضوعها:

استجابة أنظمة التشغيل للحزم الاعلانية للموجهات في برتوكول IPV6
Operating System Response to Router Advertisement Packet in IPv6

وبعد المناقشة التي تمت اليوم الأحد 01 ذو القعدة 1436هـ، الموافق 2015/08/16م الساعة الحادية عشرة صباحاً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

أ.د. محمد أمين مكي	مشرفاً و رئيساً	....
د. أيمن أحمد أبو سمرة	مناقشاً داخلياً	....
أ.د. سامي سليم أبو ناصر	مناقشاً خارجياً	....

وبعد المداولة أوصت اللجنة بمنح الباحث درجة الماجستير في كلية ***الهندسة*** / قسم وموضوعها: **هندسة الحاسوب**.

واللجنة إذ تمنحه هذه الدرجة فإنها توصيه بتقوى الله ولزوم طاعته وأن يسخر علمه في خدمة دينه ووطنه.

والله ولي التوفيق ،،،

نائب الرئيس لشئون البحث العلمي والدراسات العليا

أ.د. عبد الرؤوف علي المناعمة

DEDICATION

To my great father and my great mother

To my wife and my sons

To my sisters and my brothers

And to all my supported friends

ACKNOWLEDGEMENTS

My thanks to all those who generously contributed their help, this work would have never been possible

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

PC	Personal Computer
TCP/IP	Transmission Control Protocol/Internet Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
BGP	Border Gateway Protocol
OSPF	Open Shortest Path First Protocol
ICMP	Internet Control Message Protocol
RA	Router Advertisement
OS	Operating System
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
RFC	Request for Comments
IPng	Internet Protocol next generation
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
MAC	Media Access Control
ARP	Address Resolution Protocol
NDP	Neighbor Discovery Protocol
LAN	Local Area Network
OSI	Open System Interconnection

ISO	International Standard Organization
NAT	Network Address Translation
IPsec	Internet Protocol Security
QoS	Quality of Service
IESG	Internet Engineering Steering Group
ADD	Authorization Delegation Discovery
SAVI	Source Address Validation Improvement
TRDP	Trust Router Discovery Protocol
TBS	Trust Based Security
CA	Certificate Authority
RDNSS	Recursive DNS Server
EUI	Extended Unique Identifier
ND	Neighbor Discovery
LL	Link Local
DAD	Duplicate Address Detection
OUI	Organizationally Unique Identifier
SN	Solicitation Node
MLD	Multicast Listener Discovery

LIST OF APPENDICES

Abstract

With growth of internet IPv4 address will run out soon. So the need of new IP protocol is indispensable. IPv6 with 128-bit address space is developed and maintain the support of IPv4 protocols with some upgrades such as BGP, OSPF and ICMP.

ICMP protocol used for error reporting, neighbor discovering and other functions for diagnosis, ICMP version 6 has new types of packets to perform function similar to address resolution protocol ARP called Neighbor Discovery Protocol NDP.NDP is responsible for address auto configuration of nodes and neighbor discovery. It define new packets for the purposes of router solicitation, router advertisement and others discovery functions.

These RA's messages are responsible for auto configuration IP address in version 6 protocol and other information such as DNS information and Gateway. Using three flags (A, M and O) RA message can advertise the OS with proper configuration. Many question will answered at the end of research: What is the configuration for all combinations are set automatically? What will happen when all flags are set? How has the priority when two flags or more are set? What should happen if IP address and DNS information is obtained from two sources on the same link?

In this research the ambiguity of router advertisement behavior is removed. These RA messages will be set with different values. Then, discover the auto configuration IP address and DNS options for operating system response. These configurations are the aim to this research. Many public OS's compared in the research form different vendor such as Linux, Microsoft and Mac.

The main simulator is GNS3 for network topology. Hosts attached to GNS3 using VMware workstations. Wire shark is used as network analyzer packets flow.

Arabic Abstract

الملخص

بسبب النمو المتواصل لخدمة الانترنت في العالم ، لن يعد بالإمكان استيعاب اجهزة جديدة بسبب قرب نفاذ العناوين الخاصة ببرتوكول الانترنت الاصدار الرابع. لهذا اصبحت عملية تطوير برتوكول انترنت جديد مسألة مهمة جدا و عاجلة. برتوكول الانترنت الاصدار السادس هو الجيل الجديد من برتوكول الانترنت.

يدعم برتوكول الانترنت الاصدار السادس جميع ميزات البروتوكول القديم بالإضافة الى استحداث خصائص جديدة مثل برتوكول ICMP والتي تساعد في تسهيل وتسريع مرور البيانات في الموجهات حول العالم. يعتمد برتوكول ICMP في عمله بشكل اساسي على اكتشاف الاخطاء في الشبكة ، المساعدة في حل المشاكل بالإضافة الى استكشاف الاجهزة المجاورة مثل الموجهات او الحواسيب او غيرها.

يعتمد برتوكول ICMP في عمله على خاصية استكشاف الاجهزة المجاورة له من خلال برتوكول مضمن بداخله يسمى NDP. هذا البرتوكول يتطابق في عمله مع فكرة برتوكول ARP الموجود في برتوكول الانترنت الاصدار الرابع ولكن مع بعض التغييرات الجوهرية.

احدى هذه التغييرات هي استبدال برتوكول ARP ببرتوكول NDP. برتوكول ARP يعتمد على خاصية الاستعلام عن عنوان معين لجهاز معين وذلك بإرسال تعميم على جميع الاجهزة الموجودة في الشبكة. اما برتوكول NDP يعتمد على معرفة عنوان جهاز معين لجهاز معين من خلال ارسال استعلام الى مجموعة معينة تضم عدد من الاجهزة لها صفات مشتركة وليس لجميع الاجهزة الموجودة على الشبكة كما كان سابقا.

يمكن تنفيذ العملية من خلال رسالة خاصة من الموجه تسمى RA تحتوي على خصائص معينة تسمى Flag. في هذا البحث سوف نقوم بإرسال عدة رسائل RA بأنماط مختلفة لأنظمة تشغيل مختلفة وسنقوم بدراسة الردود الخاصة بهذه الانظمة على هذه الرسائل مع دراسة العلاقة بينهم من خلال العديد من البرامج المجانية استخدمت في هذا البحث لتوفير النفقات.

Chapter 1

Introduction

In 1970's, IETF workgroups were working on Internet protocol and they were firstly invented the old version of Internet Protocol. IPv0 to IPv3 were used to development of IPv4. They never used for public and they were always remained as experimental versions. [24, 27]

IP version number 5 was assigned to experimental Internet Stream Protocol, which was not referred to as IPv5 resulting to version gap [35, 45]. Table 1 shows the IP version and their use [39].

Table 1: Internet Protocol versions

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol version 4
5	ST	ST datagram mode.
6	IPv6	Internet Protocol version 6

1.1 Internet Protocol Version 4

The Internet Protocol Version 4 is defined by IETF RFC 791. IPv4 was developed in the early 1980s and widely used as public Internet Protocol. IPv4 has sat on the throne of online data transfer for over 25 years, proven that IPv4 well designed for exchange data and information over network [72, 73]. This network can be local area network used in office and home or metro area network as used in city or wide area network as used between counties. The media of transmission data in computer network consist of copper cables, radio waves or fiber optics.

Two computer connected via copper cable can be called simple computer network. Networks are built to share information and resources between different computers and devices. To connect different devices in a network, unique IP Addresses are assigned to these devices [46]. In a single collision domain; where every packet sent on the segment by one host is heard by every other host; hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host [43]. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called Internet Protocol Address IP. An IP address can't be used to transmit data within local network LAN.

1.2 IPv4 OSI Model Layers

Open System Interconnection or as known OSI Model is the international standard organization ISO well-defined model. Each layer communicates with nearest neighbor layer using various protocols defined in each one. OSI model consist of 7 conceptual layers named as it shown in figure 1 [55]:

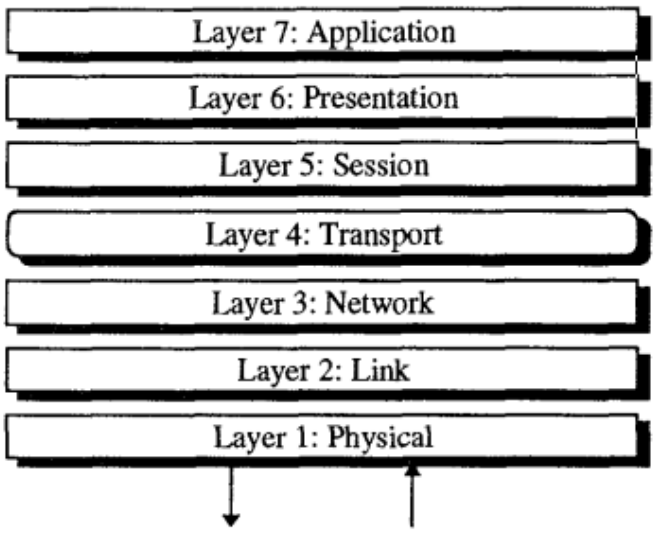


Figure 1: OSI reference model ISO 7498

1.3 IPv4 TCP/IP Model

TCP/IP is commonly used for the set of network protocols that compose the Internet Protocol. TCP/IP is the key element of Internet [26]. To interconnect your local network with other networks, you must obtain a unique IP address for your network. IP address is the device address that allows devices to transport packets from network to network via routers.

TCP/IP is containing two protocols TCP and IP. They have some differences that enable each other to work independent. IP transfers data from one device to another device on using Internet, TCP transfer data into the applications running on the devices. In contrast with the OSI model, this model of protocols contains fewer layers. Figure 2 shows the IPv4 TCP/IP layers [38]:

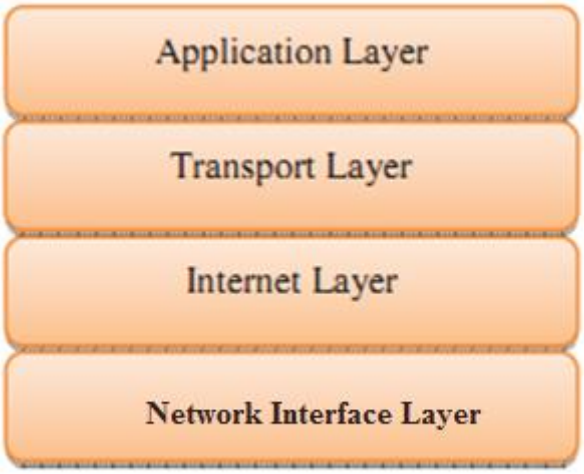


Figure 2: TCP/IP Model layers

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information [39].

IPv4 address is 32 bit wide range, which permits for 4,294,967,296 unique addresses [29, 35]. Each address is written in dotted decimal notation, where each decimal value of the four address byte is separated by “dots” or “periods”. The range of each byte is from 0 to 255 called dotted decimal notation. The first byte value of network address can’t be greater than 223, because those addresses are reserved for special use. IP address contains two parts a network part and host part [36, 37, 60].

The Internet Assigned Numbers Authority (IANA) is a department of Internet Corporation for Assigned Names and Numbers ICANN responsible for coordinating the key elements that keep the Internet running smoothly [61]. IANA Has exhausted the global IPv4 address space which leads the ISP's to transfer the technology of internet to the next level [20, 33, 42]. The transition from IPv4 protocol to IPv6 protocol presents many challenges to the internet community. Various solutions have been proposed, including dual stack, tunneling, and translation [21, 32, and 28].

1.4 IPv4 - Limitations

Initial design of IPv4 did not change since RFC 971, which was published 1981. The growth of internet created many issues, which proved IPv4 need to be changed. The main limitations of IPv4 are [62]:

Shortage of IPv4 Addresses: The IPv4 addressing system uses 32-bit address space. This 32-bit address space is further classified to usable A, B, and C classes. Many addresses are reserved, such as the research (239–254), broadcast (255), multicast (224–239), private (10, 172.16, and 192.168), and loopback addresses (127). 32-bit address space allows for 4.3 billion of IPv4 addresses. Only 3.7 billion of these addresses are actually usable. Many addresses which are allocated to many companies were not used and this created scarcity of IPv4 addresses.

Lack of Security Issues: since published in 1981 and the current network security threats were not anticipated that time. Internet Protocol Security (IPSec) is a protocol suit which enables network security by protecting the data being sent from being viewed or modified. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and optional. Many IPSec implementations are proprietary.

Address configuration related issues: Networks and also internet is expanding and many new computers and devices are using IP. The configuration of IP addresses (static or dynamic) should be simple.

Quality of Service (QoS) is available in IPv4 and it relies on the 8 bits of the IPv4 Type of Service (TOS) field and the identification of the payload. IPv4 Type of Service (TOS) field has limited functionality and payload identification (uses a TCP or UDP port) is not possible when the IPv4 datagram packet payload is encrypted.

1.5 IPv6 History and Foundation

The rapid development of internet growth justified the urgent need for the development of the Internet Protocol IPv4 to meet new challenges. This forced the Internet Engineering Task Force to develop a next generation Internet Protocol called IP version 6 [44, 63].

IPv6 was designed to be an evolutionary step from IPv4. It was not a design take over IPv4 right away. With increasing the number of new devices being connected to the internet, the need grow more address than the IPv4 able to accommodate [1, 30, 31].

First known as Next Generation Internet Protocol (IPng) [2], when it existed as a committee within Internet Engineering Task Force, now it's officially known as Internet Protocol version 6 IPv6 [22].

RFC 1752 first recommendation voice of the IPng was on what should be used to replace the current version of the Internet Protocol. This recommendation was accepted by the Internet Engineering Steering Group (IESG) and published in 1995 [63].
The current representation of IPv6 format in 128 bit long address and 16 octets long with 4 hex digit groups was found in RFC 1924 published in 1996 [64].

RIPng is routing protocol for an IPv6 internet based on protocols and algorithms currently in wide use in the IPv4 Internet. This RFC represents the minimum change to the Routing Information Protocol (RIP) published in RFC 2080 in 1997 [65].

The basic IPv6 header and the initially defined IPv6 extension headers and options specification was in RFC 2460. It also discusses packet size issues, the semantics of flow labels and traffic classes, and the effects of IPv6 on upper layer protocols [66].

RFC 3315 describe the Dynamic Host Configuration Protocol for IPv6 (DHCP) to enable DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. Also describe how DHCP provide a device with addresses assigned by a DHCP server and other configuration information, which are carried in options such as statefull and stateless auto configuration protocol.

RFC 3315 also summarizes DHCP, explaining the message exchange mechanisms and example message flows. Rather than, list of all possible client-server interactions operation [67].

The new option of prefix delegating of IPv6 mechanism using Dynamic Host Configuration Protocol was implemented in RFC 3633. This mechanism is intended for delegating a long lived prefix from a delegating router to a requesting router,

across an administrative boundary, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned [68]. This specification and optional mechanism was later updated by RFC 6603 published in 2012 [69].

The addressing architecture of the IP version 6 protocol was implemented in RFC3513 and updated by RFC4291. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, multicast addresses, loopback address, unspecified address and an IPv6 node's required addresses. Also describe the alternative representation when dealing with mixed environment of IPv4 and IPv6 addresses [70].

The privacy extensions for Stateless Address Auto configuration in IPv6 specified in RFC4941. As nodes use IPv6 stateless address auto configuration to generate addresses using a combination of locally available information and information advertised by routers.

Combining network prefixes with an interface identifier addresses are formed in IPv6. On an interface that contains an embedded IEEE Identifier, the interface identifier is typically derived from it. On other interface types, the interface identifier is generated through other means, for example, via random number generation [71].

IPv6 is developed to overcoming the problems in IPv4. One important difference between IPv4 and IPv6 is the length of their addresses [41]. Its 128-bit address format significantly enlarges the address space [25] and will satisfy the address demands for a fairly long time. It is large enough to be confidently conclude that the addresses will never run out [48].

The length of the address also makes prefix aggregation fairly flexible, and subsequently achieves global addressing and routing in a hierarchical pattern [23].

1.7 IPv6 Header vs. IPv4 Header

IPv4 address uses 32-bit address which means 2^{32} = 4.3 billion addresses, while IPv6 uses 128-bit or approximately $3.4x10^{38}$ addresses more than $7.9x10^{28}$ times as many as IPv4 [3, 24, 34, 45]. Figure 3 compares the structure of an IP address version 4 and version 6 [40].

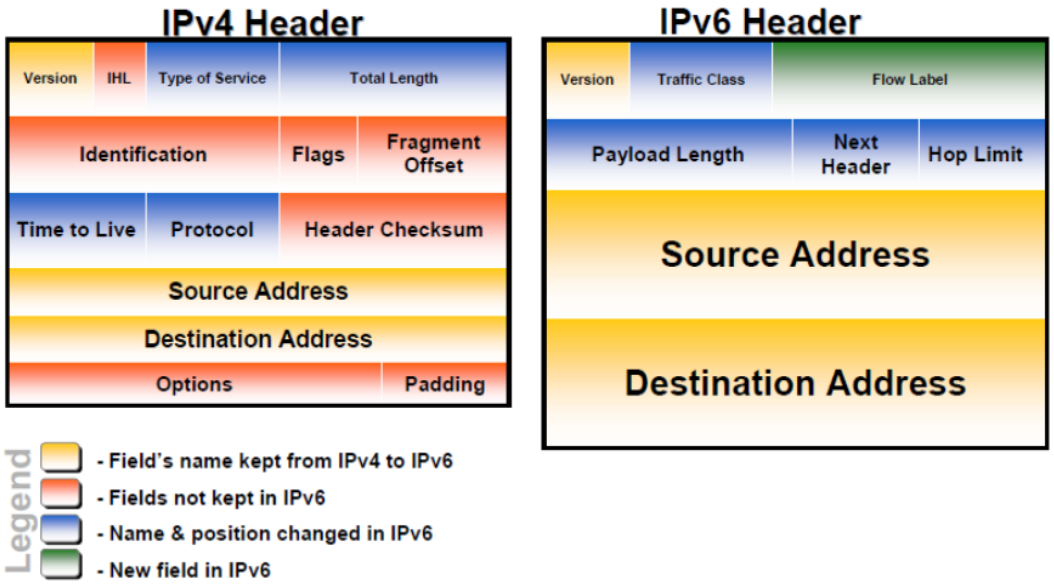


Figure 3: comparison between IP address version 4 and version 6 headers

1.8 IPv6 Features and Motivation

The main motivation of the new specification of the Internet protocol is the address space limitations. The global Internet has experienced many years of sustained exponential growth, doubling in size every nine months or faster. In 1999, on the average, a new host appeared on the Internet every two seconds [7]. However, the 32-bit address space of IPv4 is limited and, even more, unfair divided between different organizations. While network address translation technology NAT seems to be a solution for some topologies like managing multiple LANs of one corporation, it cannot handle the needs of new evolving Internet areas like for example China.

IPv6 is redesigned entirely to keep the basic functionalities of IP addressing. It offers the following features [50, 59]:

IPv6 solve the lack of Internet Protocol addresses version 4. IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy [51].
IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×10^{38} different combinations of addresses. According to an estimate, 1564 addresses can be allocated to every square meter of

this earth. With the large number of available addresses can be eliminated using address conservation techniques like NAT [52].

Although IPv6 header's is twice bigger than IPv4, IPv6 header's is simpler than IPv4 header's by moving the unnecessary options and header information to the end. The little change in header's positions makes router decisions quickly.

Every device has unique IP address and can pull through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations like Firewall, organization policies, etc.

No urgent need of DHCP server, since IPv6 supports both statefull and stateless auto configuration mode of its host devices.

An optional security services in IPv4 become a mandatory in IPv6. Cryptographic security service such as confidentiality, authentication and data integrity is implemented. Internet protocol security IPsec also becomes a part of the base protocol in IPv6 [52].

IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

IPv6 was designed to support mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

Large IP address scheme in IPv6 can configure hosts with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

Other fact, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

The Neighbour Discovery Protocol (NDP) is a protocol available in IPv6. The NDP is based on Internet Control Message Protocol Version 6 (ICMPv6) messages that manage the interaction nodes on the same link. There is no Address Resolution Protocol (ARP) for IPv6 and the role of the ARP is replaced by NDP [52].

1.9 IPv6 Address Types

IPv6 has several types of addresses as the following:

Global Unicast IPv6 addresses: Used to identify a single interface. These are standard globally unique unicast addresses (public IPv4 addresses) as in IPv4, one per host interface. Global Unicast IPv6 addresses are internet routable IPv6 addresses.

Link Local IPv6 addresses: Link Local IPv6 addresses allow communications between devices on a local link. Link Local IPv6 addresses are not routable. They are used on a subnet. Normal Link Local IPv6 address prefix is fe80::/10.

Multicast: A multicast address identifies zero or more interfaces on the same or different hosts. A multicast transmission sends packets to all interfaces that are part of a multicast group.

The group is represented by the IPv6 destination address of the packet. IPv6 multicast addresses start with FF. Following are the important IPv6 multicast addresses.

ff02::1 - All nodes on the local network segment

ff02::2 - All routers on the local network segment

Anycast: An anycast address identifies multiple interfaces. An anycast transmission sends packets to only one of the interfaces associated with the address, not to all of the interfaces. This interface is typically the closest interface, as defined by the routing protocol.

Loopback: Used by a node to send an IPv6 packet to itself. An IPv6 loopback address functions the same as an IPv4 loopback address. The IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001/128, which can be also represented as ::1

We summaries the IPv6 addresses as identified by the high-order bits of the address in Table 2.

Table 2: IPv6 address prefix identifers

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Site-local unicast	1111111011	FEC0::/10
Anycast	Multiple interfaces are assigned same IP address	
Global unicast	everything else	

1.10 Thesis Contribution

Whereas IPv4 hosts must reply on manual configuration or DHCP to provide the address of a default gateway, IPv6 hosts can automatically locate default routers on the link.

This is accomplished through the use of two ICMPv6 messages:

Router solicitation message (type 133).

Router advertisement message (type 134).

When a host joins a link, an IPv6 host multicasts a router solicitation to the all routers multicast group.

Each router active on the link responds by sending a router advertisement message (called RA message) with its address to the all nodes group.

This RA message contains three flags called A flag, M flag and O flag. These flags advertise the operating system what is the proper auto configuration can do for IP address and other network configuration such as DNS options and Gateway.

RFC's doesn't have clear behavior with public OS used in local network.

The aim of this research is to remove the ambiguity of router advertisement flags behavior with public OS by sending router advertisements message with different parameters of M, O and A flags. And answer some questions as:

What should operating systems do when IP information can be obtained from multiple sources such as router advertisements and DHCPv6 server?

Who will take the higher priority if this information is send by more than one source?

The dependency between A flag, M flag and O flag will be cleared at the end of this research.

All flags will be set with all possible values. Then, we will test the auto configuration IPv6 protocol using neighbor discovery protocol to the response of operating system for these flags.

1.11 Thesis Structure

In chapter 2, we summarize some of the related work with router advertisement message and IPv6 protocol. Despite that, there is not a lot of work in the literature examining what we aim in this research.

In chapter 3, introduce an overview of routing discovery protocols. Beginning with IPv4 discovery protocols such as ARP protocol. Answering the following questions: How APR is work? What is the ARP packet structure? What are the vulnerabilities of ARP protocol? What are ARP protocol weak points?

After that, the discovery protocol in IPv6 NDP will be introduced. NDP, which is the replacement protocol of ARP, is IPv6 protocol used to find neighbor hosts and other options. The advantages of NDP protocol over ARP protocol will be cleared. Why ARP is deprecated ?

Chapter 4 will explain in detail the simulation program and all tools used to discover the response message results.

Chapter 5 will introduce the experimental configuration results of RA message with all other public OS systems. Obtained results will be discussed in details and the relation between output results will be cleared at end of this chapter.

Finally, in chapter 6 we present thesis conclusion and recommendation for future work.

Chapter 2

Related Work

Related RFC's doesn't have clear answers with the expected behavior of operating systems configuration. Literature works in examining router advertisements messages behavior with public used operating systems are almost zero. In this chapter literature work with RA message will be summarized.

Hoffmann and Grob investigate the current state of the ICMPv6 implementation available on contemporary Operating Systems and the Router Advertising Daemon RADVD.
They suggest the following modifications that allows RA messages to be sent either as Link Local LL.

- LL multicast to the All Node address ff02::1
- LL unicast ('MAY') to individual hosts.

The propose solution has made the following adjustments in the way a RADV router acts on Router Solicitations:

- Router Advertisements sent upon a received Router Solicitation should be send to the soliciting host's LLU address.
- Router Advertisements following Router Solicitations should be send prompt without delay to the soliciting host.
- Router Advertisements sent upon Router Solicitations don't impact the timing of periodically send unsolicited advertisements.

Due to proposed changes, these functionalities can be easily realized by simple IPv6 address filters. In addition, a qualified handling of RA messages including a type3 option should include the following mechanisms:

Upon sending a Router Solicitation for prefix discovery a state flag is set which is initialized to some value, typically four times the value of the (initial) Round Trip Timer RTT. Only Router Advertisements received within that period are accept; others even targeting the node's LLU are discarded.

Per interface an upper limit for accepted link prefixes shall be imposed and perhaps may be configurable by a particular variable (accept_maxprefix = 12).

They proposed a modification of RFC4861 to balance the requirements of hosts and routers regarding Router Solicitation/Router Advertisements. These modifications

can be relatively easily incorporated into the existing IPv6 stack providing backward compatibility.

Further, the vendors of network components, in particular intelligent switches may need enhance their products to support the confinement of Router Advertisements traffic with respect to some dedicated ports [13].

Narayan and et al, conducted unbiased empirical performance comparison of IPv4 and IPv6 protocol stack on Windows operating systems. They evaluate Windows XP Professional & Server 2003 and compared results with previously studied Windows 2000. Using TCP and UDP traffic between two nodes, and throughput as the metric, found that:

For small packet sizes, performance difference between IPv4 and IPv6 is lower than theoretical value for both Windows XP and Server 2003 have throughput difference of approximately 5% evident for both TCP and UDP traffic.

For large packet sizes, IPv4 and IPv6 performance difference is higher than the theoretical value. TCP traffic on Windows Server 2003 shows a difference of 10.4% and UDP traffic on Windows XP shows 12%.

All operating systems evaluated have at the core the same Window NT kernel architecture and yet portray different throughput performance. In the absence of availability of the operating system source codes, we can only speculate reasons for differences in performance of the protocols.

Comparing Windows 2000 IPv4/IPv6 performance for both TCP and UDP protocols with the newer operating systems (Windows XP and 2003), it is observed that Windows 2000 throughput values are significantly lower than both the counterparts for smaller packet sizes.

This difference can be attributed to how efficiently an operating system handles TCP/IP packet buffer allocated by the kernel. Packet buffer is a shared memory space on a computer that holds data as it transits between devices. they have contributed to overall performance enhancement of newer Windows operating systems.

Although two operating systems may have the same kernel, network performance can be different. Comparing throughput values obtained, network throughput depends not only on traffic type and Internet Protocol version, but is also governed by the choice of the operating system [14].

Abraham and et al, used 6MoN monitoring tool that operates by listening broadcast and multicast Ethernet frames sent by active nodes on a LAN. Each IPv4 and IPv6 node has to go to neighbor discovery process before starting communication; this simple concept makes 6MoN usable with a minimal configuration on every LAN without external component.

Application installed in a dual stack host makes a DNS query before making connection to a remote host. If the DNS response contains both IPv6 and IPv4 addresses, it is common that some operating systems and network applications try to make IPv6 connection and in case of failure it fallback to IPv4.

If there is an IPv6 network connection failure, it is common to notice the network to be very slow. This is one of the most typical malfunction that users notice in presence of rogue RAs.

With the presence of rogue Router Advertisement containing a valid Router Lifetime as shown in figure 4 [49], the host configures the wrong default router. If the Router Advertisement contains a prefix option with appropriate valid and preferred lifetime having the A flag set the host auto configures the corresponding unicast address for that prefix.

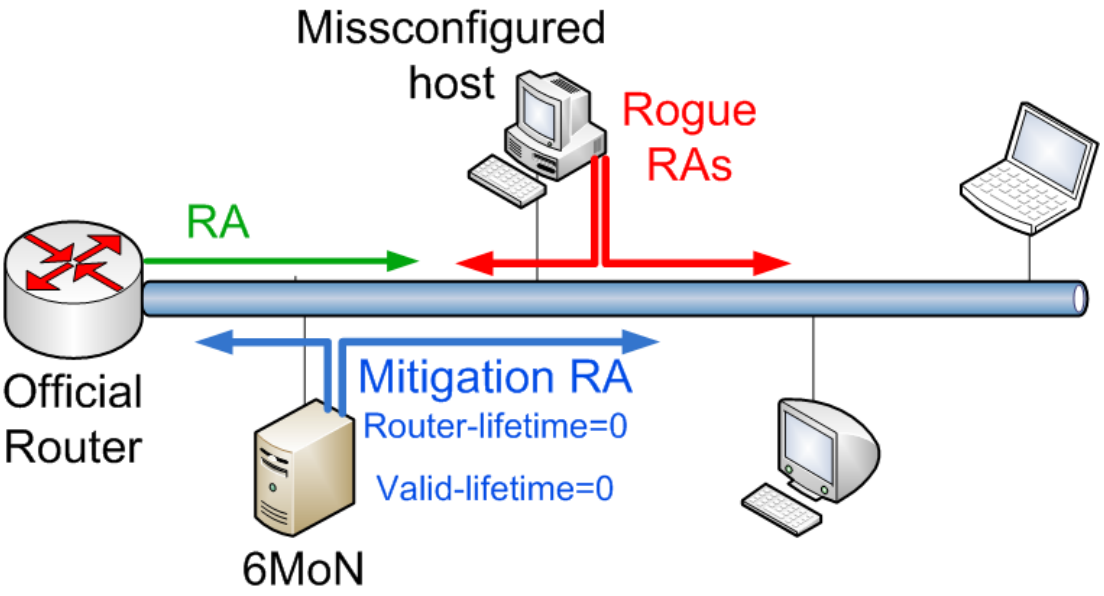


Figure 4: Rogue Router Advertisement

The policy used by hosts for selecting the default route from the default routers list depends on the implementation of the operating system. Hosts trying to access a remote site using the default router corresponding to the rogue RA may fail.

A host may also select the correct default router while using a rogue global unicast address as source address to start new connections, which may cause problems for

the returning network traffic. Only hosts using the correct network unicast addresses and the official default routers will continue to operate correctly.

In dual stack environments, it is common to have rogue Router Advertisements both on wired and wireless LANs causing operational problems for hosts on a network. In a multivendor campus network, with different networking equipment and operating systems, it is necessary to have a network monitoring tool that helps network administrators to detect and mitigate rogue router advertisements automatically [49].

Raja Kumar and et al, investigates the current router discovery mitigation methods such as Authorization Delegation Discovery ADD, Source Address Validation Improvement SAVI, Trust Router Discovery Protocol TRDP and Router Advertisement Guard. The investigation would further increase the understanding on their weakness so that it could be used to formalize a new security method for router discovery. They propose a new security mechanism based on distributed trust management called Trust Based Security (TBS) for IPv6.

The TBS trust construction uses a trust community in IPv6 LAN that distributes the trust between members in the local network, thus all nodes trusts each other without any specific Certificate Authority (CA). To do this, a mechanism to make trusted community is required.

They use a hash function algorithm to provide integrity of the NDP message including RS and RA message. Therefore, receiver could recognize the sender's message and trust them based on the trusted message.

To do this, receiver would verify the incoming message by applying the same hash algorithm used in the sender. If the integrity of the message is verified, the receiver then creates an entry on its neighbor cache for the solicitation sender.

Neighbor cache in NDP mechanism contains IP address, link layer address and reachability states. In TBS mechanism, another column in the neighbor cache table was added called trust states. This trust status would determine what trust states of neighbors that could be trusted, distrust and uncertainty.

Theoretical analysis of this mechanism shows a decrease in bandwidth consumption compared to ADD on Secure Neighbor Discovery mechanism up to 3.15 times lesser [15].

Tony Bonanno and et al, uses router advertisement message RA to design and implantation of recursive DNS server. The extension of the RA message is used via IPv6 neighbor discovery protocol, Hosts using RDNSS to resolve DNS names will increase. If the client cannot find a DNS Server in its DNS Cache, it must use other means to find DNS Servers, see figure 5[16].

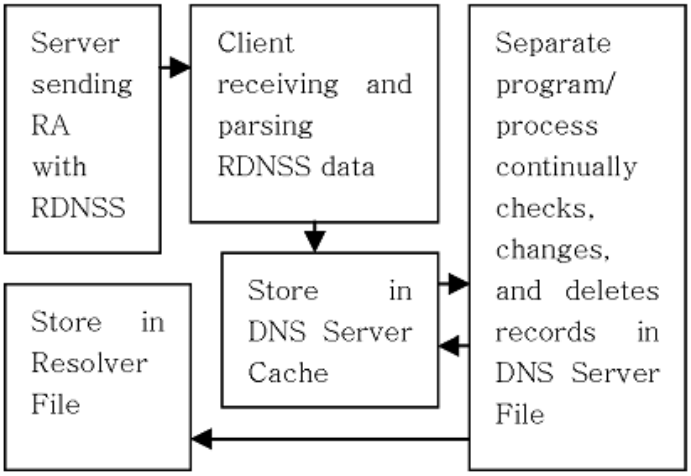


Figure 5: Process flow of recursive DNS model

The design and implementation based on Router Advertisement message have a RDNSS extension. RDNSS is a DNS mechanism which provides a recursive service to resolve DNS queries.

The procedure of this mechanism consists of these steps:

- The IPv6 host sends Router Solicitation RS message to get an RA message and its optional.
- For the RS message sent by IPv6 host, the Router sends an RA message, which contains Prefix Information option of the RDNSS for stateless address auto configuration and RDNSS options for DNS servers.
- If there is a Prefix Information option in the RA message, the IPv6 host performs stateless address auto configuration on the basis of the prefix included in the option.
- If there is an RDNSS option in RA message, the IPv6 host stores the RDNSS address in both its DNS Server Cache and Resolver File.
- If at any point Prefix Information does not exist or stateless address auto configuration does not occur, then Statefull Address Auto configuration using DHCPv6 occurs.

The design provides a functional and reliable operation of distributing RDNSS information in a local and site local network [16].

Jeong, et al. defines a new RFC for neighbor discovery ND option called RDNSS option that contains the addresses of recursive DNS servers. Existing ND transport mechanisms are used such as advertisements and solicitations.

This works in the same way that hosts learn about routers and prefixes. An IPv6 host can configure the IPv6 addresses of one or more RDNSS via RA messages periodically sent by a router or solicited by a Router Solicitation.

The RDNSS option contains one or more IPv6 addresses of recursive DNS servers. All of the addresses share the same lifetime value. If it is desirable to have different lifetime values, multiple RDNSS options can be used. Table 3 show the fields description used in Figure 6 [74]. Figure 6 show the fields options of the RDNSS.

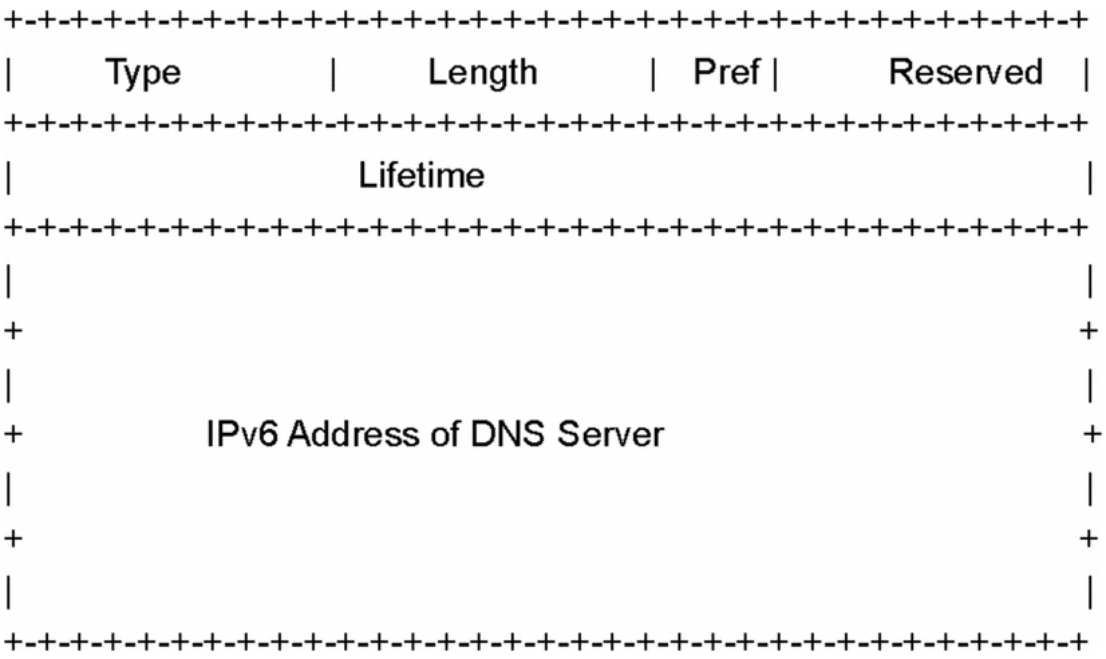


Figure 6: DNS Server Option Format

Table 3: RDNSS extension field descriptions

Field	Description
Type	Message type assigned by IANA
Length	Length of 3 X 8 octets.
Pref	A value of 15 indicates the highest preference.
Lifetime	Time to Live for a packet.
IPv6 address for DNS Server	Site local RDNSS IPv6 Address

Through the RDNSS option, along with the prefix information option based on the ND protocol, an IPv6 host can perform network configuration of its IPv6 address and RDNSS simultaneously without needing a separate message exchange for the RDNSS information.

The RA option for RDNSS can be used on any network that supports the use of ND. This approach requires RDNSS information to be configured in the routers sending the advertisements.

The configuration of RDNSS addresses in the routers can be done by manual configuration. The automatic configuration or redistribution of RDNSS information is possible by running a DHCPv6 client on the router [74].

Jeong, et al, standardizes the ND option called the RDNSS option defined in [74] that contains the addresses of recursive DNS servers. Also defines a new ND option called the DNSSL option for the Domain Search List. This is to maintain parity with the DHCPv6 options and to ensure that there is necessary functionality to determine the search domains.

The existing ND message (i.e., Router Advertisement) is used to carry this information. An IPv6 host can configure the IPv6 addresses of one or more RDNSSes via RA messages. Through the RDNSS and DNSSL options, along with the prefix information option based on the ND protocol, an IPv6 host can perform the network configuration of its IPv6 address and the DNS information simultaneously without needing DHCPv6 for the DNS configuration. The RA options for RDNSS and DNSSL can be used on any network that supports the use of ND. This approach requires the manual configuration or other automatic mechanisms (e.g., DHCPv6 or vendor proprietary configuration mechanisms) to configure the DNS information in routers sending the advertisements [75].

Chapter 3

Background of Discovery Protocols

3.1 ARP Protocol

In Ethernet network, and in order to communicate with each other, hosts should know and link the logical address (IP address) to the physical address (MAC address) [76]. The mapping between IP address and Mac address is called Address resolution ARP [53, 54].This dynamic mapping procedure is consist of two messages: ARP request and ARP replay. But this procedure is differentiate between local and remote computers.

ARP Request: It is sent by the host and contains its IP address, MAC address, the type of ARP message and the destination IP address. Then this ARP request is broadcast to all the hosts in the same LAN as the sending host. The destination MAC address field is left blank to be filled by the host with the targeted IP address [77].

ARP Reply: Upon receiving the ARP request, the host with the destination IP address fills its MAC address in the blank field previously mentioned and the operation field is set to the operation code of the ARP reply. Then, this packet is directly sent to the requesting machine (unicast), which updates its ARP cache with the requested MAC address [77].

When host tries to communicate with another local host, ARP protocol initiates an APR request. If IP establishes the request is local, the source host scans his internal memory of ARP cache for the destination host hardware address. If no entry is found, ARP protocol initiate an ARP request by asking the local hosts “which computer does this particular IP address belong to? And what it’s the hardware address? ”. The request message is broadcast over the local network. Each host receiving checks whether the requested IP address agrees with its own. If it doesn’t agree the host ignores the request. But if the message IP request matches with a host IP address, it sends an ARP replay containing its hardware address back to the source host. Then the destination host updates its ARP cache with the source host IP and the MAC address. The communication is possible as soon as the source host receives the replay.

For remote Network, the source host must find the hardware address of the default router. To do this the source host sends an ARP request containing the default router IP address. Thereupon, the default router sends an ARP replay containing its own hardware address back to the source host. Now the source host sends the data packet to the default router address. The packet contains the destination host IP address. The

router looks up this IP address in its routing table and uses routing table information to forward the packet to the destination host

ARP request by system A and ARP reply from system b step by step are shown in figure 7 [77]

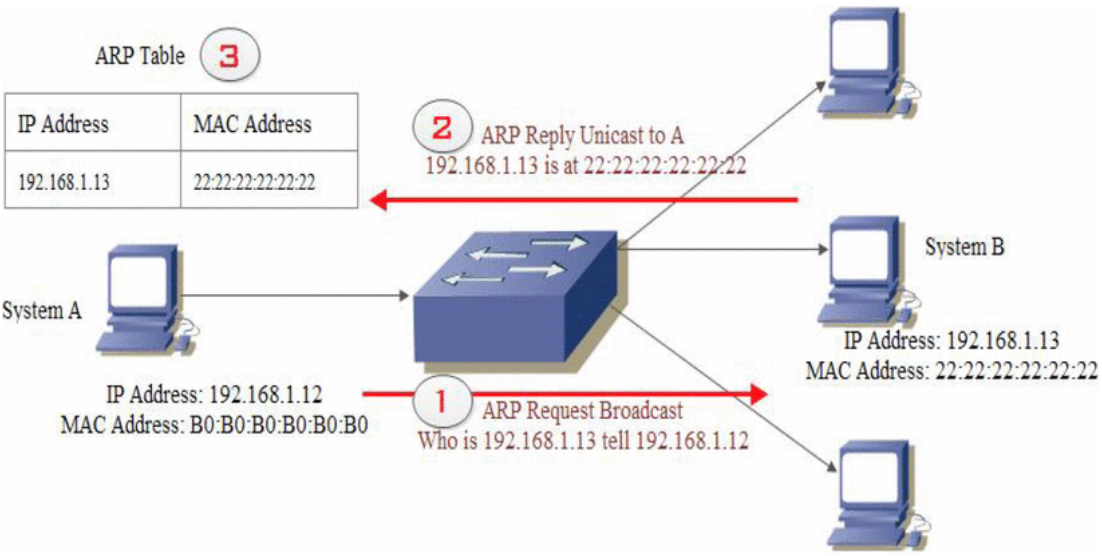


Figure 7 : ARP request and reply step by step

However, in order to reduce the number of address resolution requests, a client stores the mapped addresses for a (short) period of time in a temporary memory called the ARP cache. It has finite size and permanently deletes unused entries and evacuates unsuccessful attempts to free space in the memory by periodically flushes all the entries. Considering a host changes its MAC address, this modification can be easily detected by different hosts in the network when the cache entry is removed, and then a new ARP message is sent to affirm the new association.

Although ARP is one of the most widely used protocol in any network (e.g. IEEE 802.11 and Ethernet), it presents flaws that make it vulnerable to numerous attacks. Its weak points that are imposed by attackers can be summarized as follows [77]:

ARP does not use authentication for its requests or replies, so faked requests/replies can be easily produced.

ARP is a stateless protocol i.e. it does not retain the state of the requests, so replies can be sent without corresponding requests.

As indicated by the ARP protocol, upon receiving an ARP packet reply, a host must update its local ARP cache with the corresponding information in the source fields, without taking into consideration that the receiving node already has an entry for the source IP address in its ARP cache.

ARP specification states that the host receiving the ARP request will update its cache, even if the node already has an entry for the source IP address of the request.

ARP data frame is shown in figure 8 [78]

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware address length</td><td>Protocol length</td><td>Operation</td></tr>
<tr><td colspan="3">Sender’s hardware address(8-bit group 0~3)</td></tr>
<tr><td colspan="2">Sender’s hardware address(8-bit group 4~5)</td><td>Sender’s IP address(8-bit group 0~1)</td></tr>
<tr><td colspan="2">Sender’s IP address(8-bit group 2~3)</td><td>Receiver’s hardware address(8-bit group 0~1)</td></tr>
<tr><td colspan="3">Receiver’s hardware address(8-bit group 2~5)</td></tr>
<tr><td colspan="3">Receiver’s IP address(8-bit group 0~3)</td></tr>
</table>

Figure 8 : ARP data frame packet

3.1.1 ARP Conflict Detection

An ARP probe is an ARP request constructed with an all-zero sender IP address. The term is used in the IPv4 Address.

Conflict Detection specification. Before beginning to use an IPv4 address (whether received from manual configuration, DHCP, or some other means), a host implementing this specification must test to see if the address is already in use, by broadcasting ARP probe packets[5,6].

3.1.2 Vulnerabilities of ARP protocol

The ARP protocol security issues are mainly from its working mechanism and how the protocol stacks implement. The essence of ARP Spoofing is refreshing a host's ARP cache table, having the wrong IP address and MAC address mapping. Its vulnerability is mainly reflected in the following two aspects:

One of the vulnerabilities comes from the ARP cache. ARP cache uses dynamic updating mechanism and timely phase-out of outdated IP-MAC records, rational use of cache can improve lookup efficiency. However, this advantage has become a malicious attacker's accomplice. Though each of IP-MAC records has its own lifetime, as long as the malicious attacker has changed the record before the update, then the fake records would store in the cache, the corresponding host will be deceived during this period of time.

The other vulnerability is derived from the mechanism of requests and responses in ARP protocol. Without necessary restriction, it allows any host in the LAN to have

packets sent and received, with full trust of the packets. And the receiver does not verify the accuracy corresponding to IP and MAC in the received the packets; this is a significant vulnerability in the ARP protocol. As long as it is for the ARP reply packets from the LAN, IP-MAC address records will be updated to the local ARP cache, without any certification. It is also an important factor contributing to ARP Spoofing.

ARP weak points that are imposed by attackers can be summarized as follows [76]:

- ARP does not use authentication for its requests or replies, so faked requests/replies can be easily produced.
- ARP is a stateless protocol i.e. it does not retain the state of the requests, so replies can be sent without corresponding requests.
- As indicated by the ARP protocol, upon receiving an ARP packet reply, a host must update its local ARP cache with the corresponding information in the source fields, without taking into consideration that the receiving node already has an entry for the source IP address in its ARP cache.
- ARP specification states that the host receiving the ARP request will update its cache, even if the node already has an entry for the source IP address of the request.
- ARP spoofing (Also known as ARP cache poisoning) is a technique where an attacker sends fake ("spoofed") ARP messages onto a LAN in order to associate its MAC address with the IP address of another host (such as the default gateway), so that any traffic meant for that host is directed to the attacker instead. This attack is considered as an initiation for other attacks, such as Denial of Service (DoS), Man in the Middle (MiM) attacks

ARP protocol is deprecated in IPv6 the function of ARP is replaced in IPv6 by neighbor discovery protocol [4].

3.2 Neighbor Discovery Protocol NDP

Before exchanging information on an IP network, nodes should gather configuration information (such as IP address, network prefix, default router, etc.). IPv6 anticipated the need to configure and manage a large number of nodes by supporting stateless address auto configuration. This mechanism requires no manual configuration of hosts, minimal (if any) configuration of routers and no additional servers which make it [47].

Neighbor discovery Protocol is one of the major protocols included in IPv6.Similarly to the Address Resolution Protocol (ARP) in IPv4 networks; neighbor discovery allows the discovery of other IPv6 hosts on the link.

Neighbor discovery also includes many improvements over ARP such as router discovery, packet redirection, and maintenance of reachability information about active IPv6 neighbors, address auto configuration and duplicate address detection.

For this, neighbor discovery defines new ICMPv6 packets known as router solicitation and advertisement, neighbor solicitation and advertisement, and redirect.

Redirect messages are used by router to inform hosts of better route for packets sent to a particular destination. The purpose of neighbor solicitations and advertisements are twofold.

First, neighbor solicitations are used to resolve the link-layer address of a neighbor (similarly to ARP in IPv4). Each node registers the discovered correspondence between IPv6 and link-layer addresses in its neighbor cache.

Neighbor solicitations also serve to verify that a known neighbor is still reachable. Neighbor advertisements are sent in response to neighbor solicitation message.

Routers periodically send router advertisements to advertise their presence on the link and spread various parameters about the network connectivity.

Hosts will not wait for the next scheduled router advertisement can send router solicitation to trigger the transmission of a new router advertisement.

The reception of a router solicitation allows a host to discover the address of the router, the IPv6 prefix of the link together with the associated lifetime, and in some case the address of a DNS server.

With such information, a host is able to configure its own global IPv6 address by prepending the received IPv6 prefix to the 64 bits Extended Unique Identifier (EUI-64) of its network interface. This new address is associated to the interface as tentative. Before final association, the host has to verify its uniqueness on the link by

performing duplicate address detection. This phase consists in trying to discover hosts that already own this IPv6 address by sending neighbor solicitations.

A host already using this address replies with a neighbor advertisement. In that case, the address cannot be assigned to the interface of the original host. If there is no response after the transmission of three consecutive neighbor solicitations, the host assumes that the address is unique and can be assigned to its interface.

The major feature of IPv6 is a client auto configuration interface with neighbor discovery protocol messages through neighbor discovery; the host locates an IPv6 router on the local link and requests a site prefix. The host does the following, as part of the auto configuration process [7, 8]:

Create a link-local address for each interface, which does not require a router on the link.

Verify the uniqueness of address's on a link, which does not require a router on the link.

Determine if the global addresses should be obtained through the stateless mechanism, the statefull mechanism, or both mechanisms.

There are four types of neighbor discovery message [9]:

1. Solicited (discover from client to the Multicast group of DHCP servers).

2. Advertisement (from DHCP server to clients).

3. Request (from client to server DHCP).

4. Reply (acknowledgment from DHCP server to client).

Router solicitation message issued by a host to cause local routers to transmit information about local routing or perform stateless auto configuration [10].

Router advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host.

The information contained in these messages may be used by hosts to perform stateless auto configuration and modify its routing table defined by RFC 4861[11].

3.2.1 NDP Message Format

Static IP is better to use on critical machine such as servers, routers and printers. IPv6 gives the hosts the ability to automatically configure their own IPv6 addresses. The challenges are:

- Detect duplicate address
- Know your subnet prefix.
- Know your gateway.
- Get valid DNS service.

This can be done in IPv6 using Stateless Address Auto Configuration known as SLAAC. SLAAC is developed to achieve the following goals [56]:

Minimize the manual configuration of individual machine using unique address generation mechanism for each interface.

For communicating; link local address is used in small sites consisting of a set of machines attached to a single link should not require the presence of a DHCPv6 server or router.

Address configuration should facilitate the graceful renumbering of a site's machines. Renumbering is achieved through the leasing of addresses to interfaces and the assignment of multiple addresses to the same interface.

A large site with multiple networks and routers should not require the presence of a DHCPv6 server for address configuration. In order to generate global addresses, hosts must determine the prefixes that identify the subnets to which they attach. Routers generate periodic Router Advertisements that include options listing the set of active prefixes on a link.

A Neighbor Advertisement message is issued by a host in response to a Neighbor Solicitation or spontaneously if the IPv6 link-layer address of the host changes [12]. Table 4 shows the standard format of IPv6 router advertisement message format.

Table 4: Router advertisement message format

Name	Length	Value	Description/Notes
Type	8 bits	134	Router Advertisement
Code	8 bits	0	-
Checksum	16 bits	-	ICMPv6 checksum. Format.
Cur Hop Limit	8 bits	Variable	The hop limit to be used in the IP header when sending via this router. The value 0 = not defined for this router.
M	1 bit	-	Managed Address Configuration flag. If set indicates host should use stateful configuration (e.g. DHCPv6) for address data.
O	1 bit	-	Other Configuration flag. Indicates "other" information (such as DNS server addresses) is available using stateful configuration (e.g. DHCPv6).
Reserved	6 bits	0	Should be zero and ignored by receiver.
Router Lifetime	16 bits	-	Unsigned integer. The lifetime associated with the default router in seconds. The maximum value corresponds to 18.2 hours. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list.
Reachable Time	32 bits	-	Unsigned integer. The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).
Retrains Timer	32 bits	-	Unsigned integer. The time, in milliseconds, between retransmitted Neighbor Solicitation messages. Used by address resolution and the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).
Options	variable	-	Options format. The valid options are the Source Link-Layer, MTU and Prefix Information.

Chapter 4

Thesis approach and Methodology

In this chapter, our testing approach for virtual hosts with public used OS system is explained. Many scenarios with different flags values are implemented to find out all possible auto configurations results.

4.1 What happen when a Device Boots Up?

When a device boots up, stateless address auto configuration SLAAC will generate a link local address for this device Using Extended Unique Identifier EUI-64 mechanism.

As RFC2373 specification state, EUI allows a host to assign a unique 64-Bit IP version 6 interface identifier.

This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4.

The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific.

The 16-bit FFFE is then inserted between these two 24-bits to for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC address.

In Modified EUI-64, the seventh bit from the left needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered. If 0, the address is locally administered and if 1, the address is globally unique.

It is worth noticing that in the OUI portion, the globally unique addresses assigned by the IEEE have always been set to 0 whereas the locally created addresses have 1 configured. Therefore, when the bit is inverted, it maintains its original scope (global unique address is still global unique and vice versa) as shown in figure 9.

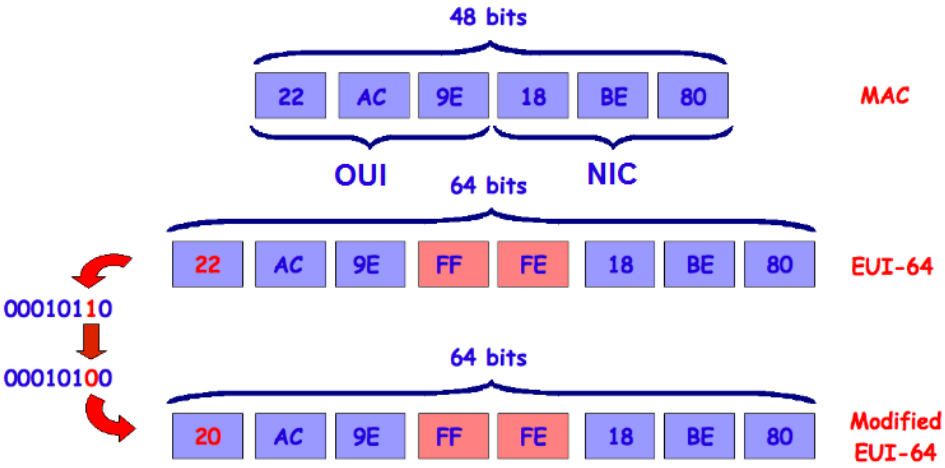


Figure 9 : EUI-64 address mechanism

After EUI address generation, the device will join solicited node SN group of its link-local address using Multicast Listener Discovery Protocol MLD report message using ICMPv6 message type 131.

This newly booted device will send router solicitation RS message to Multicast group FF02::2 (means all routers) to find its gateway and to get its global IPv6 address prefix using ICMPv6 message type 133.

If there is a router on the same link with newly booted device, router will reply to RS using router advertisement RA message ICMPv6 type 134, with destination FF02::1 means all nodes.

The device sends a neighbor solicitation to its own SN group, telling the groups about his IPv6 address using ICMPv6 type 135. This action called Duplicate Address Detection DAD.

The device repeats the joining NS groups and NS messages for each address configured on the device. The device will get the network prefix from RA message if there is no DHCPv6 server, but will communicate with the router using the router Link-local.

Some operating systems generate a temporary IPv6 addresses; those are used as security measure against tracking when using the internet.

Figure 10 shows in brief the steps when device boot up and how to find its address from neighbor router when two routers (A and B) are exits on the same link.

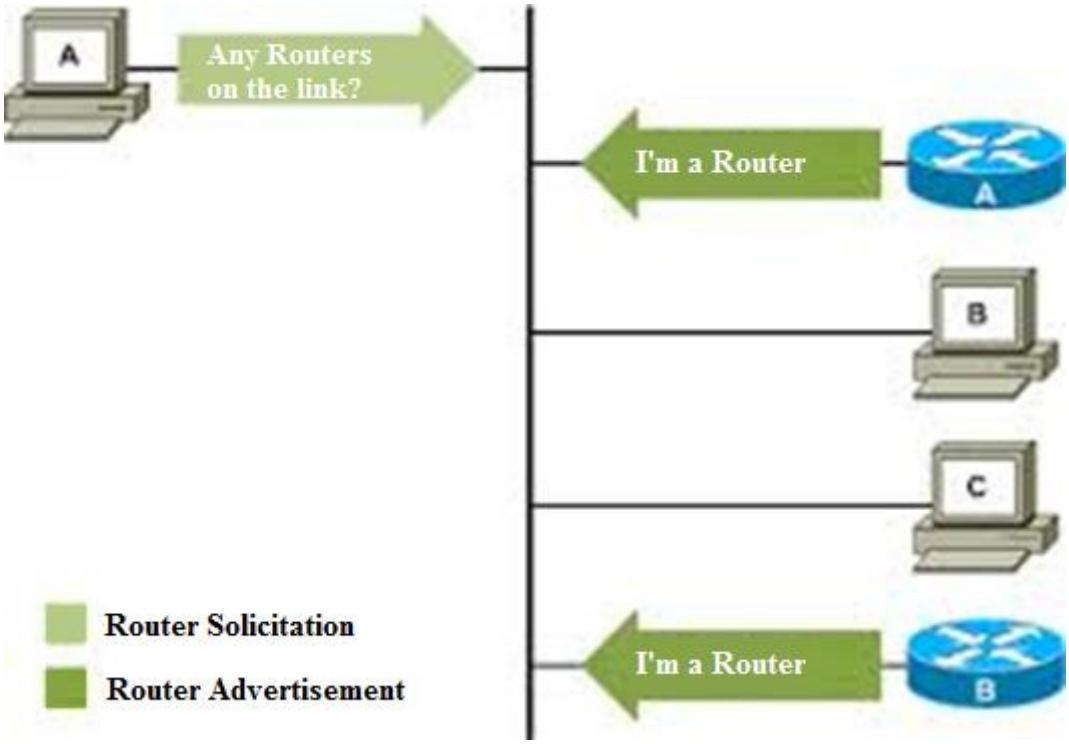


Figure 10: Router advertisements indicate paths out of the local link

IPv6 hosts are advised as for the environment options by some specific flags included in the Router Advertisement messages sent by the local router(s).

These flags are the following [11]:

- Flag M: The managed address configuration.
- Flag O: The Other configuration.
- Flag A: The autonomous address configuration flag.

Flags are having these values:
Flag M is zero by default.
Flag O is zero by default.
Flag A is one by default.

When Flag M is set, this flag indicates that IPv6 addresses are available via DHCPv6.

When Flag O is set, this indicates that other configuration information, like DNS information, is available via DHCPv6.

When Flag A is set, this indicates that the prefix can be used for SLAAC Address.

As RFC 4861 clearly states:

1. If neither M nor O flags are set, this indicates that there is no information via DHCPv6.

2. If the M flag is set, the O flag is redundant and it can be ignored

The public OS behavior with these flags is not completely specified in [75] or [11] or [56].

We can summaries the default flags behavior in Figure 11 state diagram:

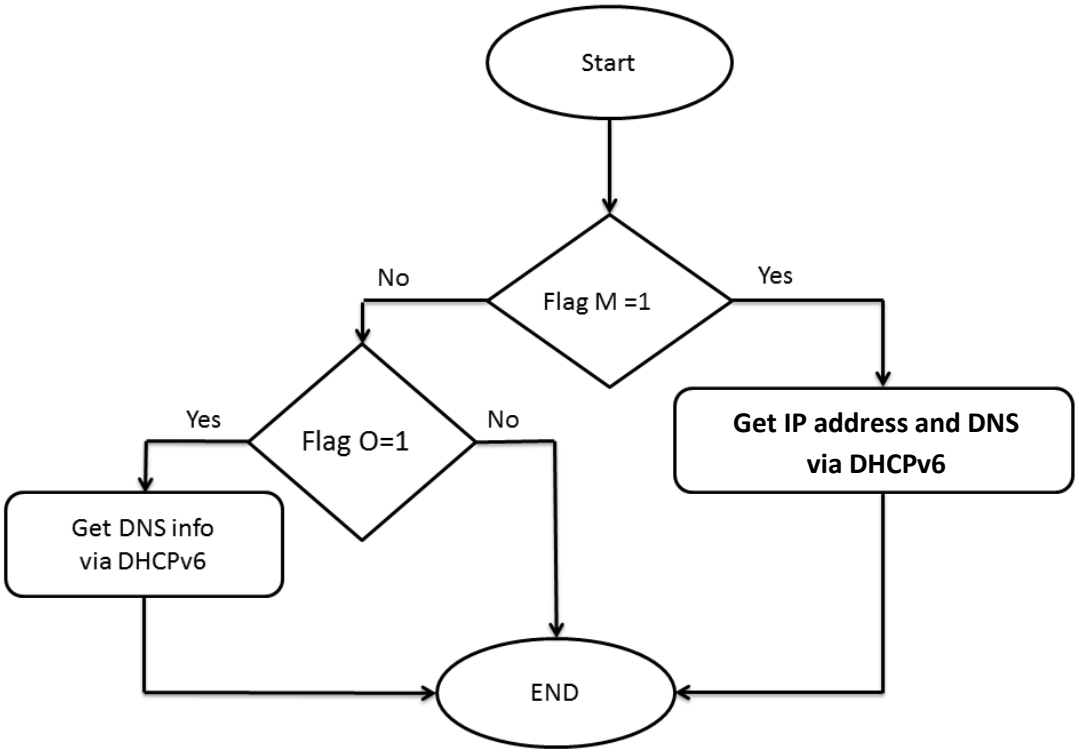


Figure 11: Flags options state diagram

4.2 Testing Methodology

A list of all scenarios with conflicting advertised parameters are created. Each case is examined to answer the following questions:

What IPv6 address host get?

What DNS are assigned to each host?

For testing purposes, all interested scenarios with different combinations of router advertisement flags parameters M, O and A are implemented.

All test scenarios are tested using one IPv6 Cisco router and DHCPv6 server on the same link and no previous configuration are set.

Our test lab consists of the following devices:

One Cisco router 3745 with Cisco IOS Software version 12.4(15)T14.

The following OS is used as virtual hosts:

Windows 7 ultimate sp1 32 bit version NT 6.1

Windows 8.1 pro 32 bit version NT 6.3

Ubuntu 14.04 LTS Trusty Tahr with kernel version 3.16

CentOS 7 with kernel version 3.10

Fedora 22 with kernel version kernel version 4.0

Mac OS-X version 10.9 Yosemite.

4.3 Methodology tools

We will use many tools for this research to simulate the network devices, routers and clients the main simulator is GNS3.

GNS3 is open source software that simulates complex networks while being as close as possible to the way real networks perform without having dedicated network hardware such as routers and switches [17].

Figure 12 shows the main window of GNS3 simulator and available devices on left sidebar.

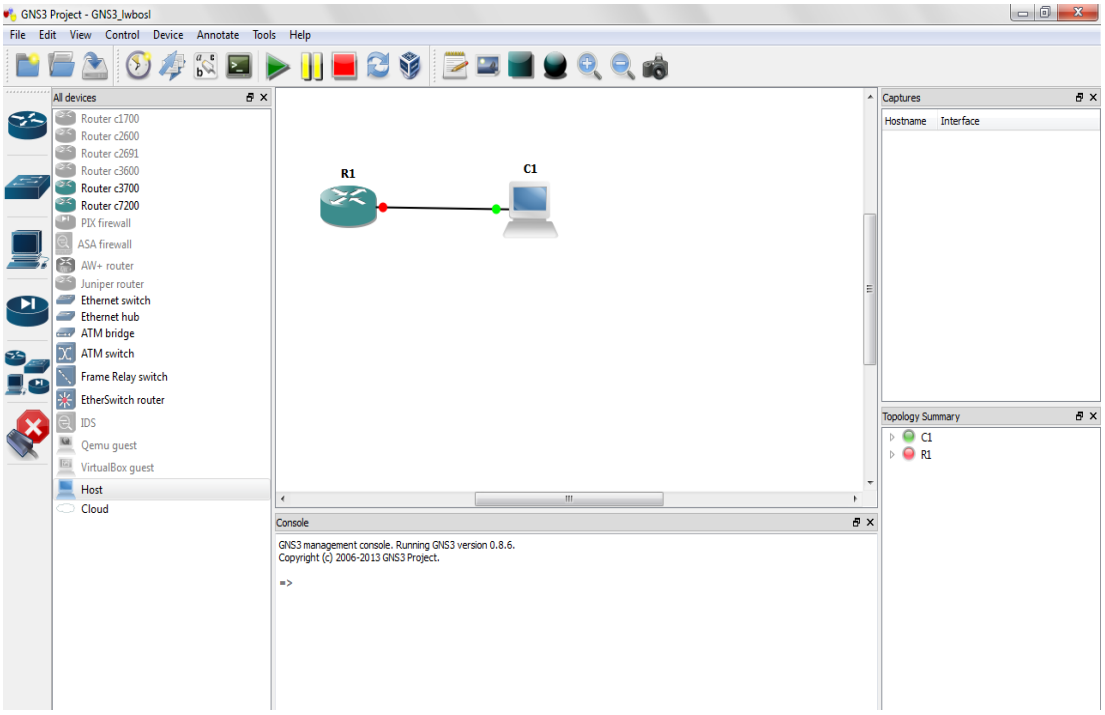


Figure 12 : GNS3 simulator main window.

Hosts can be real computers with network interface card connected to main simulation topology as shown in figure 13. But we prefer to implement hosts using virtualization mechanisms using VMware workstation software.

VMware software provides a completely virtualized set of hardware to the guest operating system [18, 58]. VMware software virtualizes the hardware for a video adapter, a network adapter, and hard disk adapters. The host provides pass-through drivers for guest USB, serial, and parallel devices.

Because of aforementioned, VMware software can customize our virtual machine hardware as needed to install and control all operating system operations on host.

Super Putty tool will be used to enter configuration mode by command line in cisco routers. Super Putty is quite possibly one of the best automation tools available in the terminal world with more than one networking device or server. Using the "Commands" feature, we can duplicate a single command on as many devices as possible in a single Super Putty window [57].

Finally, the Wire Shark tool is used as network flow analyzer. Wire Shark is open source tool used to capture the packet flow in local network [19].

4.4 Topology Implementation

For implementing our topology, one cisco router is connected with multiport switch. As shown in figure 13.

Each operating system will be installed on Virtual Machine. From computer management; Loopback network interface card is installed to connect VMware workstation machines with GNS3 routers and hosts.

Installing loopback network adapter in detailed is explained in Appendix A.

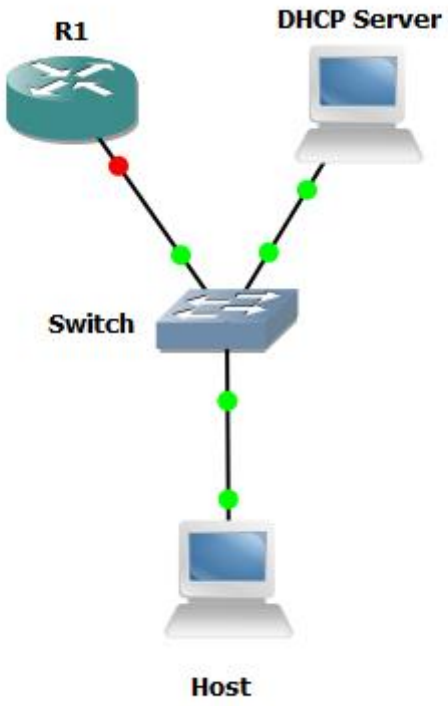


Figure 13 : The test topology implementation

We need to configure router 1 (R1) with console mode in configuration mode as explained in appendix B to communicate with hosts. After that we can start the host. Also we need to configure the Ethernet card to connecting it with virtual network adapter card with VMware host.

In the final stage, we need to capture the packets using sniffing tools to find and investigate the outgoing auto configuration packets with management flags.

Chapter 5

Experimental Results

All tested scenarios are implemented using one IPv6 Cisco router and DHCPv6 server on the same link.

We split the tests into eight cases which is the all possible combinations of router advertisement flags parameters (A, M, O).

Each case is tested with no previous configuration are set

Case 1: Flags values A=0, M=0, O=0
All hosts has no configuration at all only windows 8 has configured from DHCPv6 address and DNS.

Case 2: Flags values A=0, M=0, O=1
windows 8 has configured address and DNS from DHCPv6.

Windows 7 has configured DNS from DHCPv6.

All other hosts have no configuration at all.

Case 3: Flags values A=0, M=1, O=0
All hosts obtain address and DNS from DHCPv6 server.

Case 4: Flags values A=0, M=1, O=1
All hosts obtain address and DNS from DHCPv6 server.

Case 5: Flags values A=1, M=0, O=0
All host configured to SLAAC address

Windows 8 configured from SLAAC and DHCPv6.

Case 6: Flags values A=1, M=0, O=1
All host configured to SLAAC address and DNS information from DHCPv6 server.

Windows 8 configured from SLAAC and DHCPv6 and DNS information from DHCPv6 server.
Case 7: Flags values A=1, M=1, O=0
All hosts configured addresses to SLAAC and DHCPv6 server.

Also DNS and other information configured from DHCPv6.

Case 8: Flags values A=1, M=1, O=1
All hosts configured addresses to SLAAC and DHCPv6 server.

Also DNS and other information configured from DHCPv6.

All previous results are summarized in table 5

Table 5: RA configuration results with DHCPv6 server

Case No.	Flags Values	Item	Win7	Win8	Ubuntu	Centos	Fedora	Mac OS
1	A=0 M=0 O=0	IPv6	-	DHCPv6	-	-	-	-
		DNS	-	DHCPv6	-	-	-	-
2	A=0 M=0 O=1	IPv6	-	DHCPv6	-	-	-	-
		DNS	DHCPv6	DHCPv6	-	-	-	-
3	A=0 M=1 O=0	IPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
		DNS	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
4	A=0 M=1 O=1	IPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
		DNS	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
5	A=1 M=0 O=0	IPv6	SLAAC	Both	SLAAC	SLAAC	SLAAC	SLAAC
		DNS	-	DHCPv6	-	-	-	-
6	A=1 M=0 O=1	IPv6	SLAAC	Both	SLAAC	SLAAC	SLAAC	SLAAC
		DNS	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
7	A=1 M=1 O=0	IPv6	Both	Both	Both	Both	Both	Both
		DNS	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6
8	A=1 M=1 O=1	IPv6	Both	Both	Both	Both	Both	Both
		DNS	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6	DHCPv6

5.1 State Diagram of Results

To be familiar we represent table 5 into graphical state diagram for each operating system with similar results.

5.1.1 Windows 7 state diagram

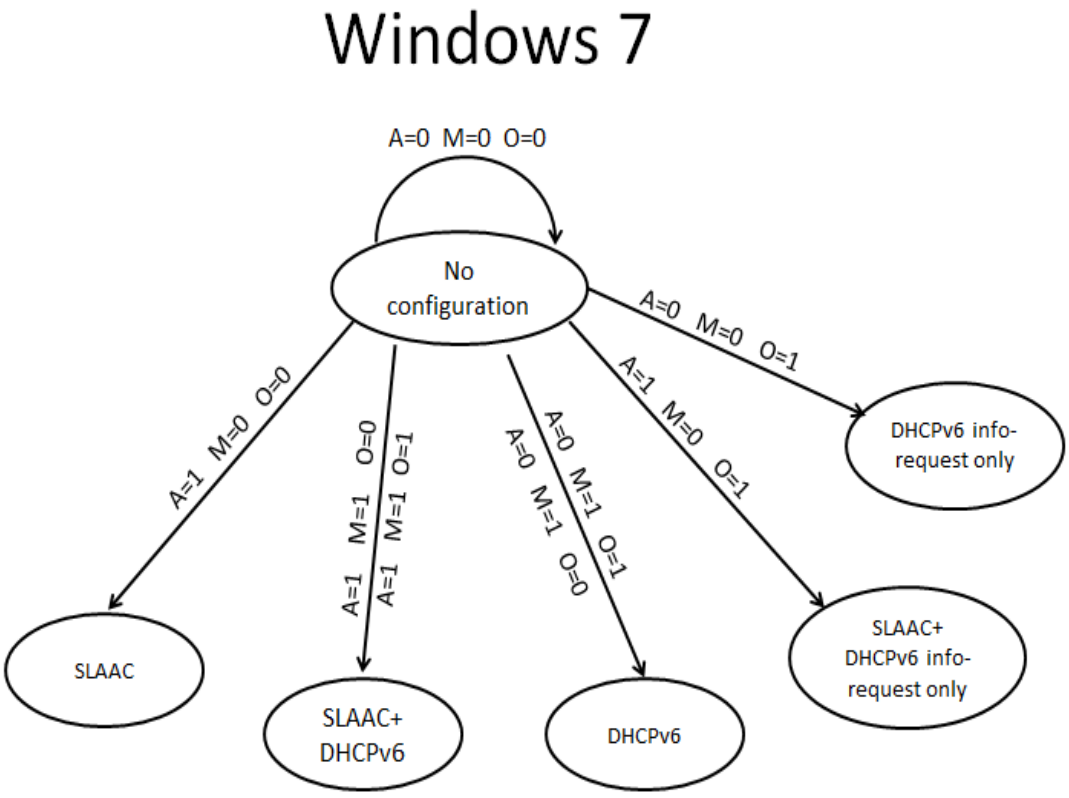


Figure 14 : Windows 7 state diagram results

Figure 14 can conclude that:

When flag M is set, then the value of O flag can be ignored as mentioned in [11].

When the value of flag M is neutral, the A flag take over the reins of configuration with SLAAC IP address (when A=1) or DHCPv6 IP address (when A=0)

Windows 7 and windows 8 doesn't use EUI-64 in SLAAC address, they generate temporary IPv6 address using a special algorithm for security reasons against tracking on internet.

5.1.2 Windows 8 state diagram

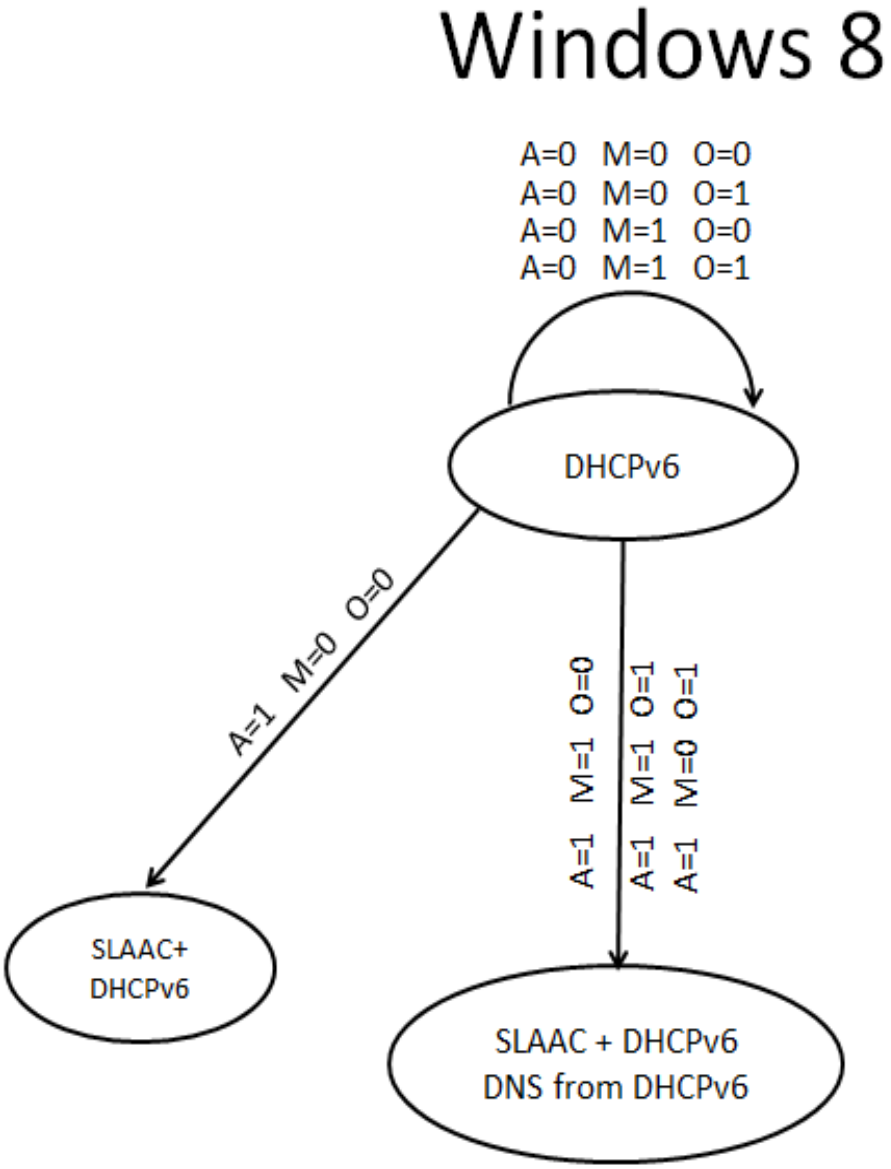


Figure 15: Windows 8 state diagram results

Figure 15 summarize windows 8 auto configuration results with each change in flag parameters.

Windows 8 gets always an IPv6 address form DHCPv6 server even with flag M is not set.

When A flag is set, the configuration of windows 8 is take two IPv6 addresses one from DHCPv6 and the other from router.

5.1.3 Linux and Mac OS state diagram

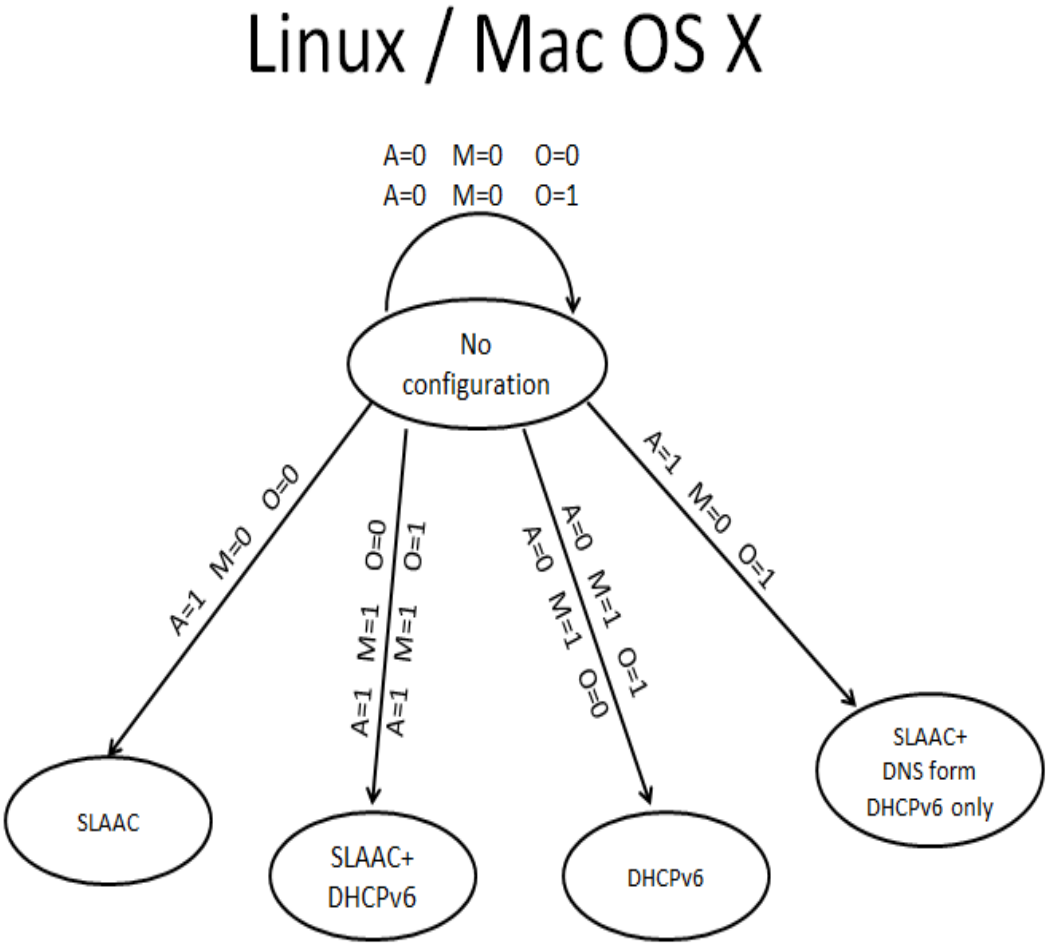


Figure 16: Mac OS and Linux OS state diagram results

Figure 16 shows the auto confirmation results that obtained from Linux OS's and Mac OS.

When flag A and M is equal to zero no confirmation at all even with O flag is set.

When A is set SLAAC IPv6 address is configured using EUI-64 mechanism.

When M flag is set the DHCPv6 options are included in OS confirmation.

5.2 Discussion of Results

In this section, the obtained results will be discussed in details. This will be useful in understanding the exact behavior between IPv6 RA message and the public OS systems related configurations. All tested scenarios are implemented using one IPv6 Cisco router and DHCPv6 server on the same link. All possible combinations of flags value are tested. Eight cases (all possible combinations of three router advertisement flags parameters) are set by command. Each case is tested with no previous configuration are set

In case 1 when all flags are not set (A=M=O= 0) this means; no prefix information option is advertised for SLAAC and don't use managed IP from DHCP server or any other information.

Fedora, MAC OS-X, CentOS, Ubuntu and windows 7 don't get any IPv6 configuration neither from RA router message or DHCPv6 server. This is compatible with RFC's default behavior.

Only Windows 8 has a contradictory behavior in dealing with the new Internet protocol. Get IP and other information from DHCPv6 server. Even that, M flag is not set. This is incompatible with RFC's behavior default behavior.

In case 2 when O flag is set and other flags are not (A=0 M=0 O=1) which means no prefix information option is advertised for SLAAC and don't use managed IP from DHCP server. Only you can use other information such as DNS from DHCP server. Linux OS and Mac OS have no configurations from any source.

Windows 8 gets an IPv6 address and other information such as DNS and gateway options from DHCPv6 server.

Windows 7 didn't have any IP. Only gets DNS information from DHCPv6 server. Windows 7 is compatible with the RFC's behavior in this case only.

Case 3 and case 4 when A is not set and M flag is set all hosts get IPv6 address and DNS information from DHCPv6 server regardless of the state of the flag O. this can prove what RFC mentioned before "M flag has higher priority than O flag. So as M flag is set, O flag can be ignored".

Case 5 when A flag is set and other flags are zeros, All hosts configured to SLAAC IP address with prefix option included in RA router message.

Only windows 8, has contradictory behavior. Its configurations get two IP's from two different sources SLAAC IP from cisco router RA message and usual IP from DHCPv6 server.

Case 6 when A flag and O flag is set and M flag in not, All host configured to SLAAC IP address and get DNS configuration from DHCPv6 RFC compatible. Windows 8 get IP address from both SLAAC and DHCP server and DNS from DHCP server.

Case 7 and Case 8 when all flags are set and O flag is interchange its value, all hosts configured addresses from both SLAAC and DHCPv6 server. Also DNS and other information configured from DHCPv6. In these cases there is no contradiction with RFC concepts at all.

Comments

From aforementioned results and all related discussion, no one can deny that Fedora, MAC OS-X, CentOS and Ubuntu have an RFC compliant behavior. Windows 7 can be compatible too with the exception.

Although Windows 7 and Windows 8.1 is same vendor provider, it presents a different behavior in simulation and results.

Windows 8 always seeks for DHCPv6 server for IP and other information in any case. It seems that they do not examine the M and O flags of the RAs in all scenarios.

For security considerations in windows 8, an attacker can install a fake DHCPv6 server and provide IP address for windows 8 clients. This vulnerability can be exploited to broadcast unauthorized information and interact with windows 8 clients.

For security reasons, Windows 7 and Windows 8 doesn’t use EUI-64 in SLAAC address generation, they generate temporary IPv6 address using a special algorithm for security reasons against tracking on internet.

5.2.1 Flags Behavior and Dependency

IPv6 hosts can configure themselves automatically for the environment options by some specific flags included in the RA messages sent by the local router(s).

These flags the managed address configuration called M flag. Other configuration flag named O flag and Autonomous address configuration flag or A flag.

This section will highlight the relationship between each flag with others. Who will take the higher priority? What flag can be ignored if other flags are set?

Back again to results in table 5 to summarize the following important facts: OS's deal with A flag as mandatory system confirmation. When A flag is set case 5,6,7 and case 8, all hosts configured its own IP to SLAAC address even when other flags are set to one or not.

M flag is mandatory for all operating systems for controlling DHCP options. When M flag is set case 3 and 4, all hosts get IP address from DHCP server. When A flag is set and M flag also set (case 7 and case 8), all host gets two IP address from two different sources router and DHCP server.

So, we can clearly say that, A and M flags are independent.

O flag has slave behavior with M flag, in case 2 when all fags are off and O flag is on all hosts ignore the O flag value.

In case 3 and 4, When M flag is set all hosts get DNS information form DHCP server and neglected the O flag value.

For summary,

A and M flags are independent.

M and O flags are dependent.

O flag value can be ignored when M flag is set.

A and O flags are dependent for each other.

Because in case 5 when A=1 and O=0 all hosts have no DNS confirmation at all. But when A=1 and O=1 (as seen in case 6) all hosts gets DNS information from DHCP server.

Chapter 6

6.1 Conclusion

The demand for Internet IP addresses is rapidly growing with large information explosion, but the current IPv4 protocol cannot meet the needs of the Internet. In order to resolve the current crisis, it badly needs to find out a new Internet protocol that adapts to the development of information society with supporting some useful old protocols.

NDP protocol is a part of ICMP protocol, used to find neighbors and query about routing information for transporting information packets. Using simulators and some other sniffing tools we can find the broadcasting messages which used to auto configure clients with new IP called link-local IP which use MAC address to generate or other random techniques.

This research intends to clear the ambiguity of new protocol. Public OS from different vendors (Microsoft, Apple and different distribution of Linux) are used. Some results are interested and other is not. Although, windows 7 and windows 8.1 are from same vendor, they have different behavior in experimental results. Linux OS distributions and Mac OS X can be considered as RFC compatible behavior.

6.2 Future work

In the near future, the studies must include Android and IOS systems because of the spread of portable devices significantly as internet users. Also the new windows 10 can be included in these studies.

References

[1] Yale University web site: http://www.yale.edu/pclt/COMM/TCPIP.HTM.

[2] Technical University of Ostrava official web site:http://www.cs.vsb.cz/ grygarek/SPS/materialy/IP_NG.html

[3] Hurricane Electric official web site: https://ipv6.he.net/

[4] J. Arkko Ericsson, C. Pignataro; "IANA Allocation Guidelines for the Address Resolution Protocol (ARP)", RFC 5494, April 2009; http://tools.ietf.org/search/rfc5494

[5] David C. Plummer, "An Ethernet Address Resolution Protocol"; RFC 826 , November 1982 ; http://tools.ietf.org/rfc/rfc826.txt

[6] Bill Croft, John Gilmore, "Bootstrap protocol (BOOTP)"; RFC 951, September 1985 ; http://tools.ietf.org/search/rfc951.

[7] Zheng Hong, Sun Nigang, and Gianfranco Ciardo; "The Analysis and Verification of IPv4/ IPv6 Protocol Conversion by Petri Nets" Fourth International Conference on Digital Home 2012.

[8] J. Arkko, Ed., J. Kempf, B. Zill and P. Nikander, "SEcure Neighbor Discovery (SEND)"; RFC 3971,March 2005; http://tools.ietf.org/html/rfc3971.

[9] official web site for cisco http://www.cisco.com/en/US/docs/switches/datacenter /sw/5_x/nx-os/unicast/configuration/guide/l3_ipv6.html

[10] ZYTRAX website, IP Network solutions http://www.zytrax.com/tech/ protocols/ipv6-formats.html

[11] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007. http://www.rfc-editor.org/info/rfc4861

[12] http://packetlife.net/blog/2008/aug/28/ipv6-neighbor-discovery/

[13] Manuel Grob, Erwin Hoffmann; "What is wrong with the IPv6 RA protocol ? Some analysis and proposed solutions", Frankfurt University of Applied Sciences, April 2012.

[14] Shaneel Narayan, Samad S. Kolahi, Yonathan Sunarto, Du D. T. Nguyen, Paul Mani; "Performance Comparison of IPv4 and IPv6 on Various Windows Operating

Systems", 11th International Conference on Computer and Information Technology (ICCIT 2008),25-27 December, 2008, Khulna, Bangladesh.

[15] Supriyanto, Raja Kumar Murugesan,Azlan Osman and Sureswaran Ramadass, "Security Mechanism for IPv6 Router Discovery based on Distributed Trust Management"; IEEE International Conference on RFID Technologies and Applications, September 2013.

[16] Tony Bonanno, HyoungJun Kim and Jungsoo Park, "Design and Implementation of Recursive DNS Server"; International conference in the communications ICACT, February 2006.

[17] GNS3 simulator official web site: http://www.gns3.net/

[18] VMware simulator official web site: http://www.vmware.com/

[19] Network protocol analyzer wire shark official website: www.wireshark.org/

[20] P.Wu, Y.Cui, J.Wu, J.Liu and C.Metz, "Transition from IPv4 to IPv6: A state-of-the-art survey", IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1407-1424, 3rd Quarter, 2013.

[21] Cui, Yong; Dong, Jiang; Wu, Peng; Wu, Jianping; Metz, Chris; Lee, Yiu L.; Durand, Alain, "Tunnel-Based IPv6 Transition," Internet Computing, IEEE , vol.17, no.2, pp.62,68, March-April 2013.

[22] IPv6Now website: www.ipv6now.com.au.

[23] S . Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 2460, December 1998, https://www.ietf.org/rfc/rfc2460.txt.

[24] Shiranzaei, Atena; Khan, Rafiqul Zaman, "Internet protocol versions A review," Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on , vol., no., pp.397,401, 11-13 March 2015.

[25] R. Elz, "A Compact Representation of IPv6 Addresses", IETF RFC 1924, April 1996, https://www.ietf.org/rfc/rfc1924.txt.

[26] Ammar Y. Korkusuz, "Introduction to IPV6 and benefits of IPV6", Bogazici University, Electrical Electronics Engineering Department, 2012.

[27] Stuart Carapola, "What Is IPv6, And What Happened To IPv1, 2, 3, and 5?", http://www.techforeverybody.com/what-is-ipv6-and-what-happened-to-ipv1-2-3-and-5/, December 2013.

[28] Amr, P.; Abdelbaki, N., "Convergence study of IPv6 tunneling techniques," Communications (COMM), 2014 10th International Conference on , vol., no., pp.1,6, 29-31 May 2014.

[29] Dr. Chris Edwards, "IPv6 - Benefits and Deployment Issues", JANET IPv6 Workshop, Lancaster University, UK, 12 February 2003.

[30] Jivika Govil; Jivesh Govil; Kaur, N.; Kaur, H., "An examination of IPv4 and IPv6 networks : Constraints and various transition mechanisms," Southeastcon, 2008. IEEE , vol., no., pp.178,185, 3-6 April 2008.

[31] WIDE project, 2006. http://www.wide.ad.jp/.

[32] Maoke Chen; Xing Li; Ang Li; Yong Cui, "Forwarding IPv4 Traffics in Pure IPv6 Backbone with Stateless Address Mapping" Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP , vol., no., pp.260,270, 3-7 April 2006.

[33] Yong Cui; Peng Wu; Mingwei Xu; Jianping Wu; Lee, Y.L.; Durand, A.; Metz, C., "4over6: network layer virtualization for IPv4-IPv6 coexistence," Network, IEEE , vol.26, no.5, pp.44,48, September-October 2012.

[34] Chakraborty, M.; Chaki, N., "An IPv6 based hierarchical address configuration scheme for smart grid," Applications and Innovations in Mobile Computing (AIMoC), 2015 , vol., no., pp.109,116, 12-14 Feb. 2015.

[35] Chandra, D.G.; Kathing, M.; Kumar, D.P., "A Comparative Study on IPv4 and IPv6," Communication Systems and Network Technologies (CSNT), 2013 International Conference on , vol., no., pp.286,289, 6-8 April 2013.

[36] Amer N. Abu Ali, Comparison study between IPV4 & IPV6,International Journal of Computer Science Issues, Vol. 9, No 1, 2012.

[37] S. Deering, R. Hinden, "Internet Protocol Version 6", IETF RFC 2460, December 1998, https://www.ietf.org/rfc/rfc2460.txt.

[38] R. E. Sheriff, "Electronics and Telecommunications Research Seminar Series: 12th Workshop Proceeedings",10 Bradford: University of Bradford. School of Engineering, Design and Technology. 182 pages. April 2013.

[39] Tutorials Point website http://www.tutorialspoint.com/ipv6/ipv6_quick _guide.htm

[40] rekrowteN Networker website : https://rekrowten.wordpress.com/2011/06/08/ ipv6-series-ipv6-datagram-part-2/

[41] Zhiwei Yan; Hwang-Cheng Wang; Yong-Jin Park; Xiaodong Lee, "Performance study of the dual-stack mobile IP protocols in the evolving mobile internet," Networks, IET , vol.4, no.1, pp.74,81, 1 2015.

[42] Suoheng Li; Yan Shao; Shoujiang Ma; Nana Xue; Shengru Li; Daoyun Hu; Zuqing Zhu, "Flexible Traffic Engineering: When OpenFlow Meets Multi-Protocol IP-Forwarding," Communications Letters, IEEE , vol.18, no.10, pp.1699,1702, Oct. 2014.

[43] D. Eastlake, "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters", IETF RFC 5342, December 2008, https://www.ietf.org/rfc/rfc5342.txt.

[44] Mohapatra, P.; Metz, C.; Yong Cui, "Layer 3 VPN Services over IPv6 Backbone Networks: Requirements, Technology, and Standardization Efforts," Communications Magazine, IEEE , vol.45, no.4, pp.32,37, April 2007.

[45] Caicedo, C.E.; Joshi, J.B.D.; Tuladhar, S.R., "IPv6 Security Challenges," Computer , vol.42, no.2, pp.36,42, Feb. 2009.

[46] Sabir, M.R.; Fahiem, M.A.; Mian, M.S., "An Overview of IPv4 to IPv6 Transition and Security Issues," Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on , vol.3, no., pp.636,639, 6-8 Jan. 2009.

[47] Montavont, J.; Cobarzan, C.; Noel, T., "Theoretical analysis of IPv6 stateless address auto configuration in Low-power and Lossy Wireless Networks," Computing & Communication Technologies - Research, Innovation, and Vision for the Future (RIVF), 2015 IEEE RIVF International Conference on , vol., no., pp.198,203, 25-28 Jan. 2015.

[48] Aun, Y.; Ramadass, S., "Dynamic assignment of Ipv6 addresses with embedded server role information for unified services and devices discovery," TENCON 2014 - 2014 IEEE Region 10 Conference, vol., no., pp.1, 7, 22-25 Oct. 2014.

[49] Abraham Gebrehiwot, Marco Sommani, Andrea De Vita, Alessandro Mancini, "6mon: Rogue Ipv6 Router Advertisement Detection and Mitigation and IPv6 Address Utilization Network Monitoring Tool", Terena Networking Conference, Reykjavík, Iceland, May 2012.

[50] Tutorials point web site: http://www.tutorialspoint.com/ipv6/ipv6_features.htm.

[51] Ling Tao; Xiao Yu Zhao; Yan Ma, "The application of proxy agent in IPv6 network management," Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on , vol.1, no., pp.209,212, 12-14 Oct. 2005.

[52] Omnisecu web site: http://www.omnisecu.com/tcpip/ipv6/ipv6-features.php.

[53] David C. Plummer, “An Ethernet Address Resolution Protocol-- or -- Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware”, RFC 826, MIT, November 1982, https://www.ietf.org/rfc/rfc826.txt.

[54] Bakhache, Bassem; Rostom, Rabiha, "Kerberos secured Address Resolution Protocol (KARP)," Digital Information and Communication Technology and its Applications (DICTAP), 2015 Fifth International Conference on , vol., no., pp.210,215, April 29 2015-May 1 2015.

[55] Loy, D.; Schmalek, R., "Thoughts about redundancy in fieldbus systems anchored in OSI Layer-4 and applied to the Lontalk Protocol on neuron based network nodes," Factory Communication Systems, 1995. WFCS '95, Proceedings., 1995 IEEE International Workshop on , vol., no., pp.21,26, 4-6 Oct 1995

[56] S. Thomson, T. Narten, T. Jinmei, “IPv6 Stateless Address Autoconfiguration”, IETF RFC 4862, September 2007; https://www.ietf.org/rfc/rfc4862.txt.

[57] Automation Nation web site: http://automation-nation.org/superputty-tutorial.

[58] Extreme Tech website: http://www.extremetech.com/computing/56702-vmware-workstation-452/2.

[59] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998 https://www.ietf.org/rfc/rfc2460.

[60] TCP/IP Network Administration, 3rd Edition, Craig Hunt, O’REILLY Media, April 2002, http://docstore.mik.ua/orelly/networking_2ndEd/tcp/ch02_02.htm

[61] IANA official site: https://www.iana.org/

[62] Jajish Thomas, Omnisecu web site: http://www.omnisecu.com/tcpip/ipv6/limitations-of-ipv4.php

[63] Bradner, S. and A. Mankin, "Recommendation for IPng", RFC 1752, January 1995. http://tools.ietf.org/html/rfc1752.

[64] Elz, R., "A compact representation of IPv6 addresses", RFC1924, April 1996, http://tools.ietf.org/search/rfc1924.

[65] G. Malkin, R. Minnear, “RIPng for IPv6”, RFC 2080, January 1997, http://tools.ietf.org/html/rfc2080.

[66] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, December 1998, http://ietf.org/rfc/rfc2460.

[67] Droms, R., Editor, Bounds, J., Volz, B., Lemon, T., Perkins, C. and M. Carney,

"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003. http://www.ietf.org/rfc/rfc3315.

[68] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003,http://tools.ietf.org/html/rfc3633.

[69] Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, May 2012. http://tools.ietf.org/html/rfc6603.

[70] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006, http://www.ietf.org/rfc/rfc4291.

[71] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Auto configuration in IPv6", RFC 4941, September 2007, http://tools.ietf.org/html/rfc4862.

[72] Han-Chieh Chao; Stuttgen, H.J.; Waddington, D.G., "IPv6: the basis for the next generation internet," Communications Magazine, IEEE , vol.42, no.1, pp.86,87, Jan 2004.

[73] Zeadally, S.; Wasseem, R.; Raicu, I., "Comparison of end-system IPv6 protocol stacks," Communications, IEE Proceedings , vol.151, no.3, pp.238,242, 25 June 2004.

[74] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli,"IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007. https://tools.ietf.org/html/rfc5006

[75] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli,"IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010. https://tools.ietf.org/html/rfc6106.

[76] David C. Plummer,“An Ethernet Address Resolution Protocol- or - Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware”, RFC 826, November, 1982, MIT.

[77] Bakhache, B.; Rostom, R., "Kerberos secured Address Resolution Protocol (KARP)," Digital Information and Communication Technology and its Applications (DICTAP), 2015 Fifth International Conference on , vol., no., pp.210,215, April 29 2015-May 1 2015.

[78] Mingji Yang; Yizhe Wang; Hui Ding, "Design of Win Pcap Based ARP Spoofing Defense System," Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2014 Fourth International Conference on , vol., no., pp.221,225, 18-20 Sept. 2014.

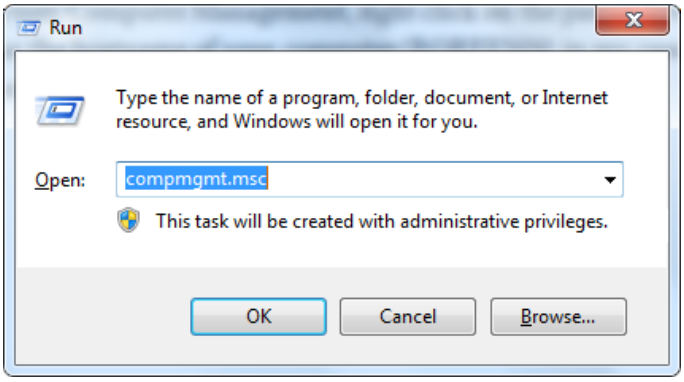
Appendix A

Creating Host to GNS3 Connection

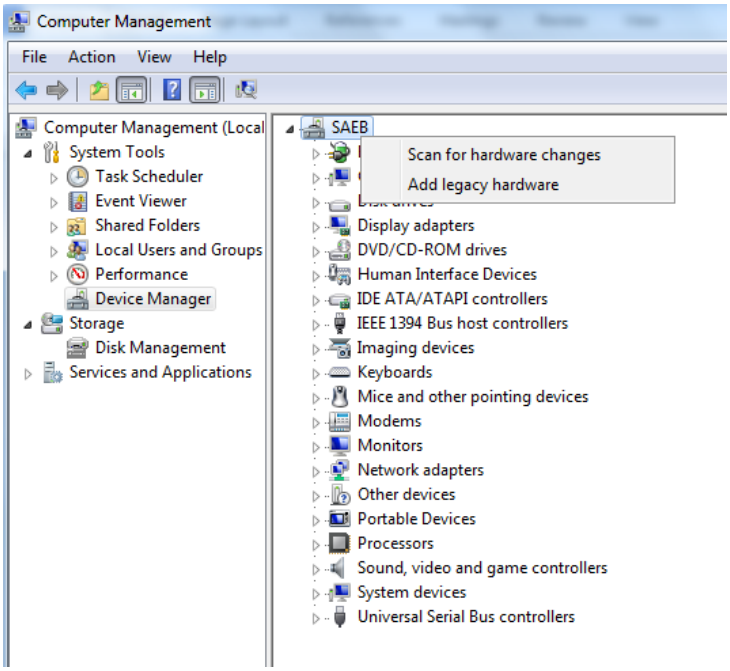
Step 1:

Installing a Loopback Network Interface

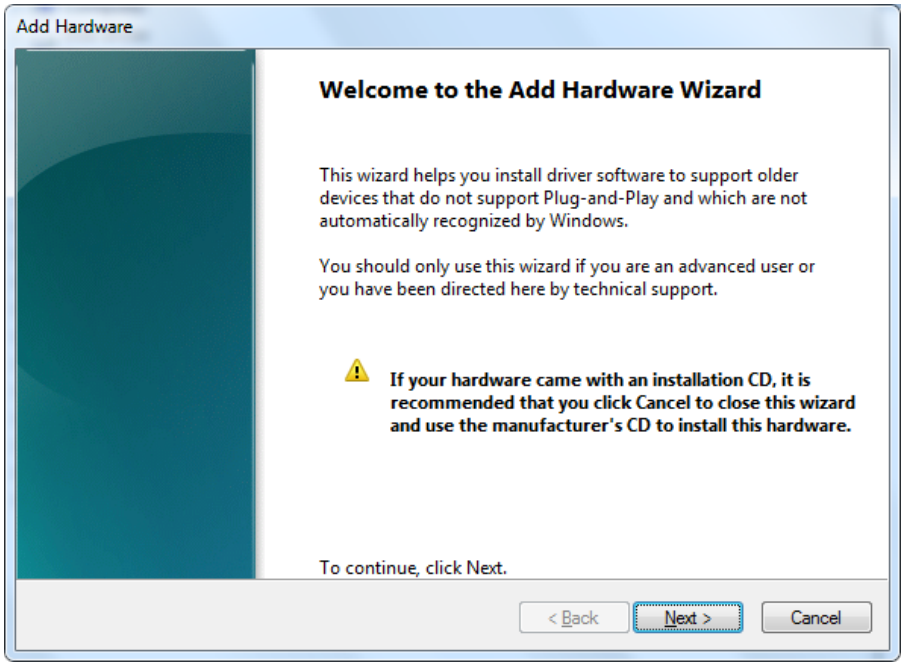
- To do this, hit windows button with R button on your keyboard to open the Run dialog.
- At the Run dialog, enter the command “compmgmt.msc” to open Computer Management.



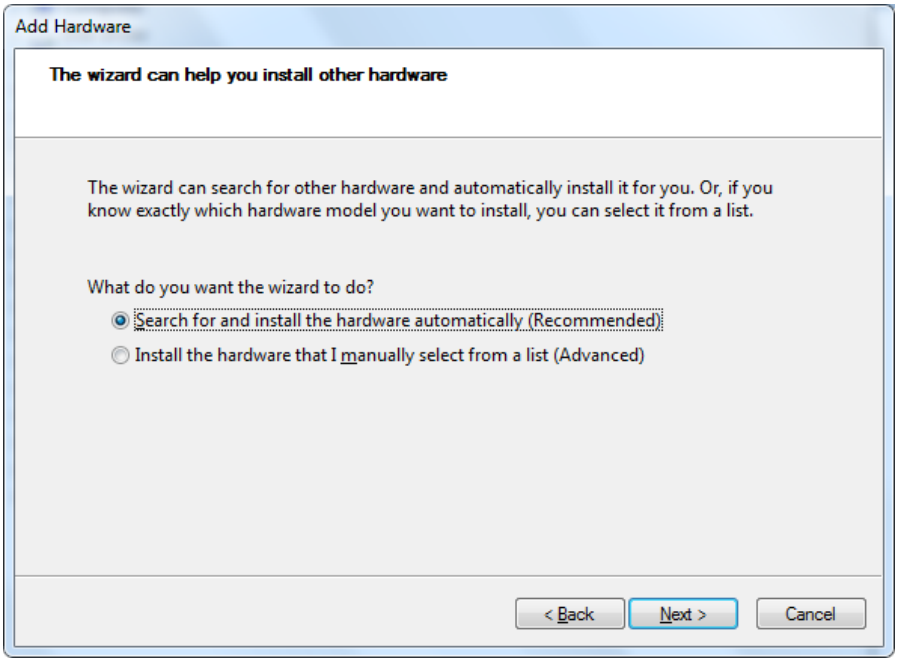
- From Computer Management, right click on the parent level item which is displayed as the hostname of your computer (SAEB in my case). From the context menu, select the option Add Legacy Hardware.



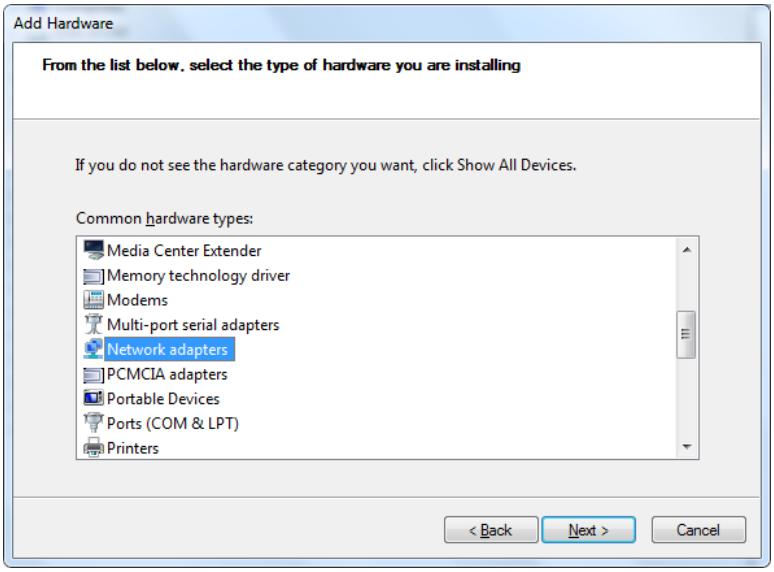
- At the Add Hardware Wizard, select Next.



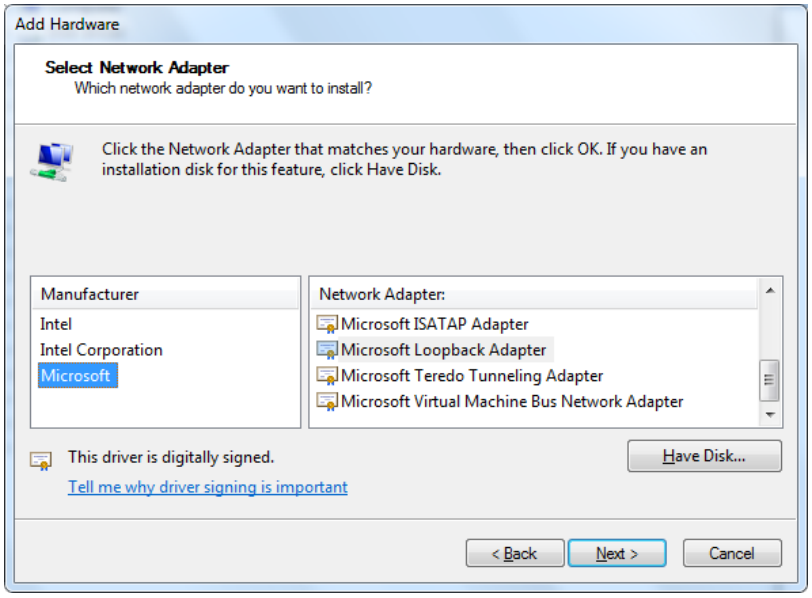
- At this point, allow the wizard to search for and install hardware automatically. Unless you have some pending hardware add or changes you will not see any new hardware detection during this stage. Once the scan for new hardware is complete, you will be given the option to press Next to manually search for the hardware. Click Next to do so.



- From the list of hardware types, select the Network adapters category, and then select Next.



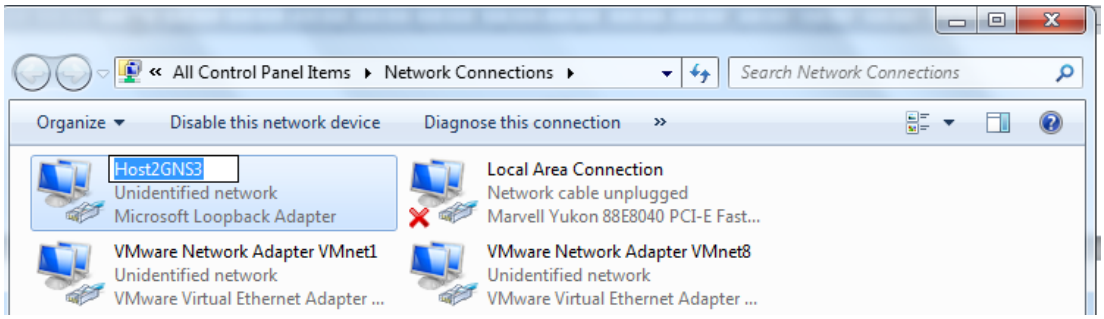
- On the next page, you will be presented with a list of available network adapters which you can add.



- Select Microsoft from the manufacturer column on the left and scroll down to select **Microsoft Loopback Adapter** from the list on the right. Once you have selected it, hit the Next button to begin installing the hardware.

Step 2: Rename your Loopback Interface to find it easily

- Open the Network Connections List you can do that from your Control Panel or from the Network and Sharing Center, or open it directly by typing “ncpa.cpl” in the run command
- On the Loopback Interface right click and chose Rename, type a new meaning full name such as HOST2GNS3 so you can easily identify it in the GNS3 program.



Step 3: Restart the computer

You need to reboot at this stage to allow dynamips to be able to detect the new adapter.

Appendix B

```
R1# configure terminal
R1 (config)# interface fastEthernet 0/0
R1 (config-if)# mac-address 0000.1111.1111
R1 (config-if)# ipv6 address fe80::1 link-local
R1 (config-if)# ipv6 address 2001:db8:111::1/64
R1 (config-if)# no shutdown
R1 (config-if)#exit
R1 (config)# ipv6 unicast-routing
```

First line is to enter configuration mode in cisco routers to do the next step setup. The second line router interface configuration mode for Fast Ethernet number 0/0. After that we made a hard code mac address for router interface 0/0 to find it easily in network analyzer program. We assign link local address because we don't need to use EUI-64 host id for simplicity trace in packet analyzer program. Global ipv6 address is assigned to the router interface 0/0 with prefix 2001:db8:111 for complete ipv6 configuration router interface.
No shutdown command is used to turn on the interface to UP state. Finally, by default cisco routers don't like to route ipv6. So we need to enable ipv6 routing protocol using ipv6 unicast-routing from global configuration mode.
When ipv6 routing protocol is enabled, router will join special multicast group called FF02::2. So if any device needs to discover information about neighbor routers, it will send discover message to known multicast group FF02::2 because any router will be joined that group automatically.

To change the A flag to value "1" use this command in interface configuration mode
R1 (config-if)# ipv6 nd prefix default no-autoconfig

To change the M flag to value "1" use this command in interface configuration mode
R1 (config-if)# ipv6 nd managed-config-flag

To change the O flag to value "1" use this command in interface configuration mode
R1 (config-if)# ipv6 nd other-config-flag

To remove either flag from router advertisement messages sent on an interface, use the "no" form of the respective command.

By default, the managed address configuration and other statefull configuration flags are not set in router advertisement messages.