SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES

Performance Analysis of IPSEC over Internet Protocol version 6 Networks

تحليل اداء حزمة بروتوكول الإنترنت الأمنية في شبكات الإصدارة السادسة لبروتوكول الإنترنت

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of M.Sc. in Electronics Engineering (Computer and Network Engineering)

Prepared By:

Marwa Hashim Abdalla Mohammed

Supervisor:

Dr. Salaheldin Mohamed Ibrahim Edam

November 2018

بسم الله الرحمن الرحيم

Sudan University of Science & Technology

College of Graduate Studies

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

SUST

كلية الدراسات العليا

Approval Page

(To be completed after the college council approval)

Name of Candidate: Marwa Hashim Abdalla Mohammed

Thesis title: Performance Analysis of IPSEC over Internet Protocol version 6 network
تحليل اداء حزمه بروتوكول الانترنت الامنيه في شبكات الاصداره السادس لبروتوكول الانترنت

Degree Examined for: Master

Approved by:

1. External Examiner

Name: Dr. Elsadig Saeid Gebreel

Signature: .... Date: 5-8-2019

2. Internal Examiner

Name: Dr. Ebtihal Haider Gismalla Yousif

Signature: .... Date: 5/8/2019

3. Supervisor

Name: Dr. Salaheldin Mohamed Ibrahim Edam

Signature: .... Date: 5/8/2019

الآية

بسم الله الرحمن الرحيم

قَالَ تَعَالَىٰ:

﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوٓاْ إِذَا قِيلَ لَكُمۡ تَفَسَّحُواْ فِي ٱلۡمَجَٰلِسِ فَٱفۡسَحُواْ يَفۡسَحِ ٱللَّهُ لَكُمۡۖ وَإِذَا قِيلَ ٱنشُزُواْ
فَٱنشُزُواْ يَرۡفَعِ ٱللَّهُ ٱلَّذِينَ ءَامَنُواْ مِنكُمۡ وَٱلَّذِينَ أُوتُواْ ٱلۡعِلۡمَ دَرَجَٰتٖۚ وَٱللَّهُ بِمَا تَعۡمَلُونَ خَبِيرٞ ١١﴾

صدق الله العظيم

﴿سورة المجادلة الآية رقْم ١١﴾

DEDICATION

To my strong pillars, source of inspiration, my parents who have taught us chase our dreams. Without their love, care and support it would not have been possibleto achieve this project, yet in time. I also dedicate this work to my husband; and to everyone who has encouraged me all the way and to all lovers of science and knowledge...

God bless them all.

ACKNOWLEDGMENT

Above all, my sincere praises to the Almighty Allah for his blessings which has given me patience, strength and ability to complete this project. The assistance of my supervisor, Dr. Salaheldin Mohamed Ibrahim Edam is highly appreciated. I would like to take this opportunity to extend my sincere thanks and appreciation for the time he spent in reading this report and his positive criticism of the project and for his instructions which have directed me to complete the project in a good manner. A special thanks to my friends for their support and help in completing this work.

Abstract

IPv6 is the next generation in internet protocol. It is developed by the Internet Engineering Task Force (IETF) to provide better performance and also to provide new services in comparison to IPv4. It is intended to serve for sufficient IP address space to meet the present Internet growth. Security attacks have been common across the Internet, therefore in order to protect IPv6 networks from security attacks; IPSec has made an inbuilt component of IPv6 to ensure the integrity, authenticity and confidentiality of data transmitted across the networks. IPSec is a networking layer protocol which is used to protect the data between two devices. IPSec encrypts and authenticates the packets before sending them across the Internet. This thesis mainly focus on the effects of different attacks like spoofing and DoS attack under IPv6 networks after using IPSec as a security to test the performance of the network. Implementation of IPSec can protect the network from security threats related to confidentiality and integrity of data. However, it appears powerless against availability threats of network.

المستخلص

برتوكول الإنترنت الإصدار السادس هو بروتوكول إنترنت الجيل القادم. تم تطويره من قبل فريق مهام هندسة الإنترنت (مجموعة مهندسي شبكة الإنترنت) لتوفير أداء أفضل وأيضا لتقديم خدمات جديدة مقارنة مع برتوكول الإنترنت الإصدار الرابع. الغرض منه هو توفير مساحة عنوان بروتكول أمن الإنترنت كافية لنمو الإنترنت الحالي. لقد كانت الهجمات الأمنية شائعة عبر الإنترنت ولذلك من أجل حماية شبكات برتوكول الإنترنت الإصدار السادسمن الهجمات الأمنية ، فإن بروتكول أمن الإنترنت يتم إنشاء مكون يحمل في ثناياه عوامل برتوكول الإنترنت الإصدار السادس ويضمن سلامة البيانات التي تم نقلها عبر الشبكات وأصالتها وسريتها. بروتكول أمن الإنترنت هو بروتوكول طبقة شبكة والذي يُستخدم لحماية البيانات بين جهازين. يقوم بروتكول أمن الإنترنت بتشفير الحزم وتصديقها قبل إرسالها عبر الإنترنت. تركز هذه الرسالة بشكل أساسي على تأثيرات الهجمات المختلفة مثل الانتحال وهجوم الحرمان من الخدمة تحت شبكات برتوكول الإنترنت الإصدار السادس بعد استخدام بروتكول أمن الإنترنت للأمان ، واختبار أداء الشبكة .يؤدي تطبيق بروتوكولأمن الإنترنت إلى حماية الشبكة من التهديدات الأمنية المتعلقة بسرية وسلامة البيانات .ومع ذلك ، يبدو عاجزًا ضد تهديدات المتعلقة بإستمرارية الشبكة.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AH	Authentication Header
CIDR	Classless Inter-Domain Routing
DAD	Duplicate Address Detection
DHCPv6	Dynamic Host Configuration Protocol version 6
DOS	Denial of Serves
ESP	Encapsulating Security Payload
GER	Generic Routing Encapsulation
GNS3	Graphical Network Simulator-3
ICMPv6	Internet Control Massage Protocol version 6
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP/IPng	Internet Protocol/Internet Protocol next generation
IPSEC	Internet Protocol Security
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
MAC address	Media Access Control address
MD5	Message Digest Algorithm
NAT	Network Address Translation
NS /NA	Neighbor Solicitation/Neighbor Advertisements
RFC	Request for Comments
SHA1	Secure Hash Algorithm 1
SLAAC	Stateless Address Auto-configuration

TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network

CHAPTER ONE

INTRODUCTION

Chapter One

Introduction

1.1 Preface

IP stands for Internet Protocol. It is the method by which data is transmitted over the Internet. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internet work using the Internet protocol suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet layer of the Internet protocol suite and has the task of delivering distinguished protocol datagram (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure now referred to as Internet protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet protocol Version 6 (IPv6) is being deployed actively worldwide. IPv6 is a new version of the internetworking protocol designed to address the scalability and service shortcomings of the current standard (IPv4) [1].

The major benefit of IPv6 is that it increases the size of an IP address from 32 to 128 bits, and removes the danger of the IP address pool being exhausted within the foreseeable future. It allows each endpoint device to have its own unique IP address and to communicate directly using IPSec with other devices on the Internet [2].

Internet protocol version 6 (IPv6), was introduced not only to overcome the limitations of an existing Internet protocol version 4 (IPv4) but also be future oriented due to the rapid growth of Internet technologies. Thus, IPv6 is also known as a next generation Internet protocol. In December 1998, Internet Engineering Task Force (IETF) defined this new Internet protocol.

In addition, to provide large address space, new features were introduced in IPv6 such as; simpler header format, mobility functions, extension header, as well as address auto-configuration [3].

IPv6 cannot solve all security problems. Basically it cannot prevent attacks on layers above the network layer in the network protocol stack, Possible attacks that IPv6 cannot address include: Application layer attacks; Attacks performed at the application layer (OSI Layer 7) such as buffer overflow, viruses and malicious codes, web application attacks and so on, Brute-force attacks and password guessing attacks on authentication modules [2]; Denial of service attacks and attacks using social networking techniques such as email spamming, phishing, etc.

The term IPSec refers to a suite of protocols from the IETF providing network layer encryption and authentication for IP-based networks [4]. The objective of IPSec is to authenticate and/or encrypt all traffic at the IP level. The objective of IPSec is to provide authentication, It ensures data has been sent by an identified sender; Data Confidentiality, It provides protection to data by encrypting the information being transmitted; Data Integrity , Specifies that there are no changes while transmitting data across the networks and packets are sent to the receiver intact [5].

1.2 Problem Statement

Many security issues in IPv6 remain the same as in IPv4, but IPv6 also has new features that affect system and network security, using of IPSec for IPv6 attack is one of the security mechanism in network. However, it is seen as having a vulnerability to some network attacks which cause Problems in the network.

1.3 Proposed Solution

To implement security mechanism in small IPv6 network, it is proposed to apply the IPSec in this network as a protection strategy. IPSec for IPv6 network Site-to-Site protection using Virtual Tunnel Interface to protect the traffic against the various attacks between the two networks and to simulate this strategy by using GNS3 simulator so as to implement end to end connection.

1.4 Objectives

The main objective of this research is to providing network layer encryption and authentication for IP-based networks, the use of IPSec in IPv6 end-to-end communications achieves

i. Improve security for IPv6 Networks.
ii. Protect IPv6 networks against any attackers such as spoofing and Dos attack.
iii. Establish IPSec tunnels between security gateway devices, and provide crypto IPSec protection for traffic from internal networks when the traffic is sent across the public IPv6 Internet.
iv. Test the performance of network.

1.5 Methodology

A test bench has been implemented and configured for virtual private network technique in IPv6 network by using Graphical Network Simulator (GNS3) to simulate IPv6 network and to capture network traffic in the simulated network.

GNS3 is used for creating the topology in figure.1 to create the network involving two tunnel end points in order to make a secure connection for secure transmission of data and protected from Dos attacker.

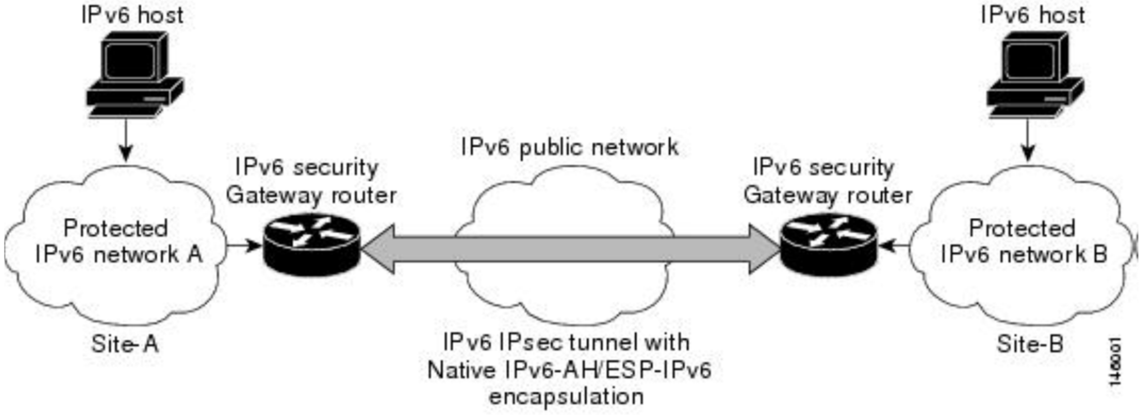

IPv6 host
IPv6 host
IPv6 public network
IPv6 security Gateway router
IPv6 security Gateway router
Protected IPv6 network A
Protected IPv6 network B
Site-A
Site-B
IPv6 IPsec tunnel with Native IPv6-AH/ESP-IPv6 encapsulation
146001

Figure 1.1: IPSec gateway

1.6 Research Outlines

In general the thesis will be divided into five chapters. Each chapter will discuss on different issues related to the project. The following are the issues discussed: **Chapter One** includes preface, states the problem, proposed solutions and methodology which used. **Chapter Two** describes the network background required to understand the proposed design and some examples of other previous solution. **Chapter Three** gives an overview of the scenarios, configurations, describes the equipments that used on it and mechanism of network. **Chapter Four** provides a step by step implementation of network design, Describes and discusses the results from each system scenario. **Chapter Five** outlines the conclusions drawn from this research and identify possible future work of this project.

CHAPTER TWO

LITERATURE REVIEW

Chapter Two

Literature Review

2.1 Background on IPv6

IP stands for Internet Protocol. It is the method by which data is transmitted over the Internet. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internet work using the Internet protocol suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet layer of the Internet protocol suite and has the task of delivering distinguished protocol datagram (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure now referred to as Internet protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet protocol Version 6 (IPv6) is being deployed actively worldwide[1].

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well-known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32-bit IP address field, and available address spaces are rapidly running out. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions parameters [2].

As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with a number of performance, ease-of-configuration, and network management issues. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 24602 (IPv6 Protocol), RFC 48613 (IPv6 Neighbour

Discovery), RFC 48624 (IPv6 Stateless Address Auto-Configuration), RFC 44435 (Internet Control Message Protocol for IPv6 (ICMPv6)), RFC 42916 (IPv6 Addressing Architecture), and RFC 43017 (Security Architecture for IP or IPSec). IPv6 is also referred as the Next Generation Internet Protocol (IPng) [2].

2.4 The IPv6 Protocol

IPv6 uses a 128-bit address. The new address space supports 2^{128} (about 3.4×1038) addresses. This expansion provides considerable flexibility in allocating addresses and routing traffic.

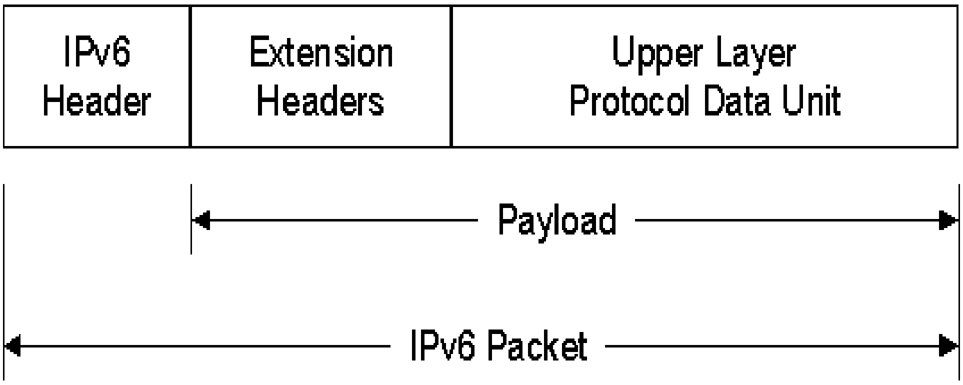
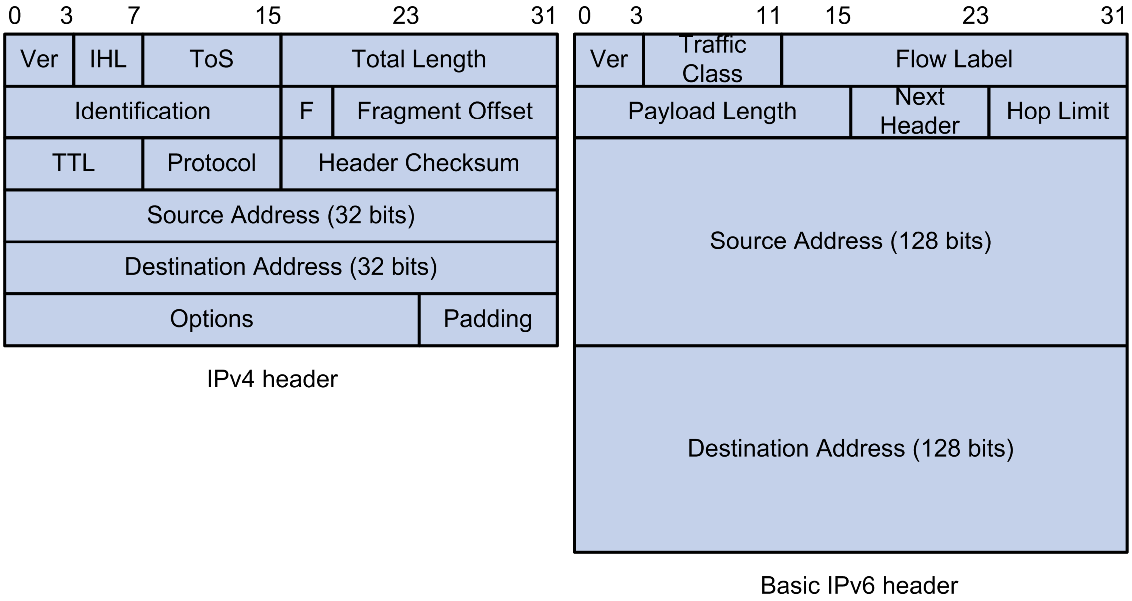


Figure 2.1: IPv6 packet.

An Internet Protocol version 6 (IPv6) data packet comprises of two main parts: the header and the payload. The first 40 bytes/octets (40x8 = 320bits) of an IPv6 packet comprise of the header that contains the following fields:



IPv4 header

Basic IPv6 header

Figure 2.2: IPv4 and IPv6 Header Fields.

The basic IPv6 protocol has a different packet header structure as compared to IPv4, as can be seen in figure 2.2, the header is simplified. The options have been restructured to follow the header and are no longer part of the header. This makes IPv6 header processing at intermediate nodes much easier. A new "flow label" field has been added to provide enhanced Quality of Service in the future. The specific benefits resulting from the new header definition are listed in the next section.

2.5 Benefits of IPv6

The new features of IPv6 result in a number of business benefits: Lower network administration costs: The auto-configuration and hierarchical addressing features of IPv6 will make networks easy to manage; Optimized for next generation networks: Getting rid of NAT re-enables the peer-to-peer model and helps in deploying new applications. E.g. communications and mobility solutions such as VoIP o Protection of company assets: Integrated IPSEC makes IPv6 inherently secure and provides for a unified security strategy for the entire network; Investment protection: The transition and translation suite of protocols helps in easy and planned migration from IPv4 and IPv6, while allowing for co-existence in the transition phase [6].

2.4 Network Notation in IPv6

The IPv6 networks are denoted by Classless Inter Domain Routing (CIDR) notation. A network or subnet using the IPv6 protocol is denoted as a contiguous group of IPv6 addresses whose size must be a power of two. The initial bits of an IPv6 address (these are identical for all hosts in a network) form the networks prefix. The size of bits in a network prefix are separated with a /. For example, 2001:cdba:9abc:5678::/64 denotes the network address 2001:cdba:9abc:5678. This network comprises of addresses rearranging from 2001: cdba:9abc:5678:: up to 2001:cdba:9abc:5678:ffff:ffff:ffff:ffff. In a similar fashion, a single host may be denoted as a network with a 128-bit prefix. In this way, IPv6 allows a network to comprise of a single host and above [1].

2.5 Comparing IPv4 and IPv6

With the rapid development and utilization of addresses in the Internet, IPv4 will be gradually substituted by IPv6. The IPv4 has been in use for over many decades and many of the related devices have been connected to the internet. But with high demand of Internet usage and due to paucity of address space and allocation mechanism some part of the world are beginning to run out of addresses [7].

Table 2.1: Comparison between IPv4 and IPv6

IPv4	IPv6
Size of header is of 20 octets.	Size of header is of 80 octets.
IHL or HLEN- Header length, gives datagram header length measures in 32-bit.	Not included.
TOS (Type of Service) - specifies how datagram is handled. It is a hint to forwarding algorithm which helps them to choose among various paths to a destination.	Replaced by Traffic Class and Flow Label. Tags the packet with a value representing a class of traffic that can be used in differentiated services.
Total length- specifies entire length of IP datagram i.e. Header + Data.	Replaced by Payload length- indicates the length of data or payload only.
ID, Flag, Fragment offset fields are used for fragmentation and reassembling of data packet at source and destination.	Not included since fragmentation is done at source node, no intermediate router is doing fragmentation so not included.
Time to Live- indicate maximum time datagram allowed to remain in network.	Replaced by Hop Limit which specifies maximum number of routers a packet traverse before it is considered invalid.
Protocol- specifies format of data area.	Replaced by Next Header.
Header Checksum- an error detecting code applied to header only not on the data. Means packet is examined at every router hop.	Removed, link layer technologies and upper layer protocol handle checksum and error control.
Source address and Destination address of 32 bits.	Source and Destination address of 128 bits

2.6 IPv6 Addressing

IPv6 addresses are 128 bits long. They are logically divided into network prefix and a host identifier. The number of bits in the network prefix is represented by a prefix length (for example, /64). The remaining bits are used for the host identifier. If you do not specify a prefix length for an IPv6 address, the default prefix length is /64 [8].

2.7 Address Configuration in IPv6

IPv6 incorporates two automatic address-configuration mechanisms: Stateless Address Auto-configuration (SLAAC) [RFC4862] and Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315]. Support for SLAAC for automatic address configuration is mandatory, while support for DHCPv6 is optional -- however, most current versions of general purpose operating systems support both. In addition to automatic address configuration, hosts, typically servers may employ manual configuration, in which all the necessary information is manually entered by the host or network administrator into configuration files at the host [9].

2.7.1 Stateless Address Auto-configuration

The basic idea behind SLAAC is that every host joining a network will send a multicast solicitation requesting network configuration information, and local routers will respond to the request providing the necessary information. SLAAC employs two different ICMPv6 message types: ICMPv6 Router Solicitation and ICMPv6 Router Advertisement messages. Router Solicitation messages are employed by hosts to query local routers for configuration information, while Router Advertisement messages are employed by local routers to convey the requested information. Router Advertisement messages convey plethoras of network configuration information, including the IPv6 prefix that should be used for configuring IPv6 addresses on the local network. For each local prefix learned from a Router Advertisement message, an IPv6 address is configured by appending a locally generated Interface Identifier (IID) to the corresponding IPv6 prefix [10].

2.7.2 Dynamic Host Configuration Protocol for IPv6

DHCPv6 can be employed as a stateful address configuration mechanism, in which a server (the DHCPv6 server) leases IPv6 addresses to IPv6 hosts. As with the IPv4 counterpart, addresses are assigned according to a configuration-defined address range and policy, with some DHCPv6 servers assigning addresses sequentially, from a specific range. In such cases, addresses tend to be predictable [9].

2.7.3 Manually Configured Addresses

In some scenarios, node addresses may be manually configured. This is typically the case for IPv6 addresses assigned to routers (since routers do not employ automatic address configuration) but also for servers (since having a stable address that does not depend on the underlying link-layer address is generally desirable) [9].

2.8 Duplicate Address Detection Process

Duplicate address detection is a mechanism ensuring that all the IPv6 hosts have unique IP addresses by verifying their uniqueness on the same link. Every host must execute DAD process before specifying an address to an interface [6]. When host(s) generate new IP addresses, after generating an interface identifier host(s) ascertain that no other neighboring host(s) already possesses that generated address on the same link to avoid the IP address conflict [7].

DAD process is being performed by sending Neighbor Solicitation (NS) messages multicast to all neighboring hosts within a same link. These NS messages carry the tentative IP address that the host(s) has generated and would like to assign as its interface identifier. If the tentative address is already assigned by any other neighboring host within a same link, then that neighboring host will send a Neighbor Advertisement (NA) in reply. Hence, new host generates a new tentative address. In next attempt, if a new host does not receive any response to its NS messages from the neighboring nodes; it indicates that the newly generated address is unique and no other neighboring host is using this address. Thus, a host can use that generated address as preferred address as an interface identifier [11].

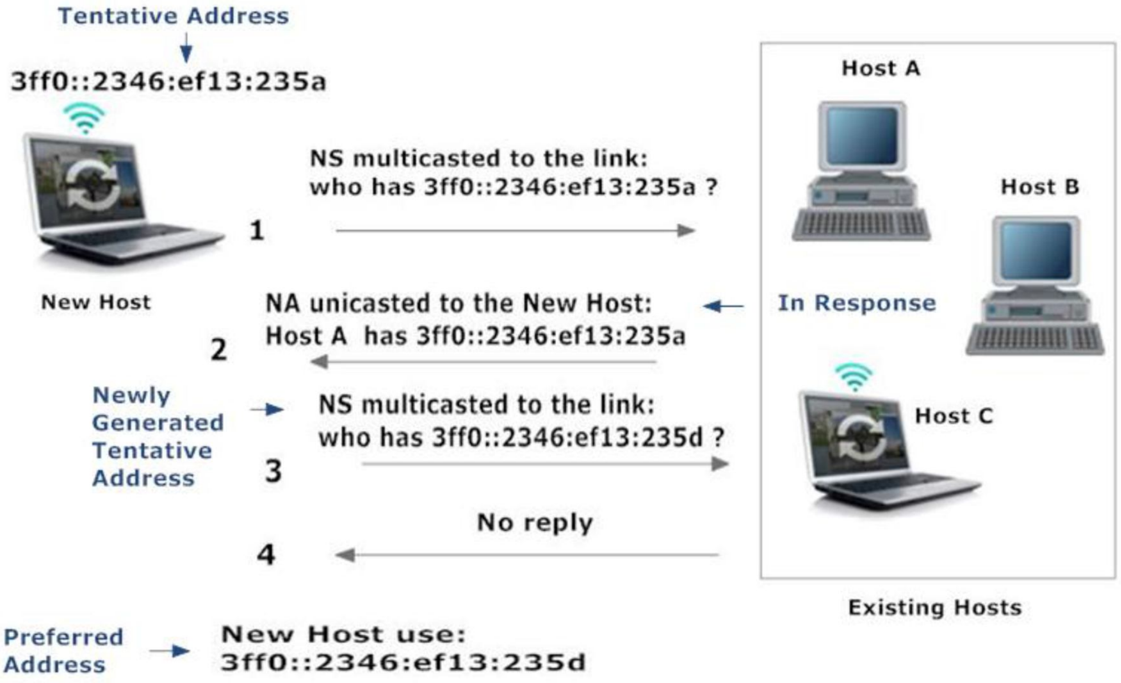

Tentative Address
3ff0::2346:ef13:235a
NS multicasted to the link:
who has 3ff0::2346:ef13:235a ?
1
New Host
NA unicasted to the New Host:
Host A has 3ff0::2346:ef13:235a
2
In Response
Host A
Host B
Host C
Newly Generated Tentative Address
NS multicasted to the link:
who has 3ff0::2346:ef13:235d ?
3
No reply
4
Existing Hosts
Preferred Address
New Host use:
3ff0::2346:ef13:235d

Figure 2.3: Example of duplicate address detection process [11].

2.9 Transition Methods

Transition methods support gradually moving from IPv4 to IPv6 without major interruptions of services and networks. It is expected that most networks will have to support both IPv4 and IPv6 in parallel for a long time because of legacy equipment and the dependency on others to completely switch to the new protocol. Transition methods can be categorized into tunneling, dual stack and protocol translation methods [1].

2.9.1 Dual Stack

Dual IP layer or Dual Stack is defined in RFC 4213 as a “technique for providing complete support for both Internet protocols—IPv4 and IPv6—in hosts and routers.” At least in part, dual stacking will occur in any transition from IPv4 to IPv6. It is further expected that dual-stacked networks will exist or a long time also after IPv4 depletion. A complete dual stack is probably the best way to avoid security issues involved with IPv4-IPv6 interaction. On the other hand, it does increase administration workload by adding complexity and literally doubling the configuration overhead. Most other transition techniques of the categories tunneling and translation require some kind of dual stacking [12].

2.9.2 Protocol Translation

Address or port translation of addresses such as via a gateway device or translation code in the TCP/IP code of the host or router and Allow IPv6 realm to access the rich contents already developed on IPv4 applications [12].

2.9.3 Tunnel

Tunneling delivers a packet as another packet's payload. Provides a general description on tunneling IPv6 over IPv4, while is a specification for tunneling other protocols over IPv6. Currently, there are a high number of different technologies tunneling IPv6 over IPv4: 6to4, IPv6 rapid deployment, 6over4, ISATAP and Teredo [13].

There are two types of tunnels: Tunnels which have to be manually configured and automatic tunnels. Configured tunnels have to be set up and managed manually by an administrator and are specified in RFC 4213 [12]. For tunneling IPv6 through an IPv4 network the protocol 41 is used and has to be enabled on the route. In case those IPv4 packets are tunneled through an IPv6 network, Generic Routing Encapsulation GRE or Multiprotocol Label Switching MPLS can be used. Configured tunnels do not scale as well as automatic tunnels because administrators have to set up and shut down tunnels manually every time when changes are necessary.

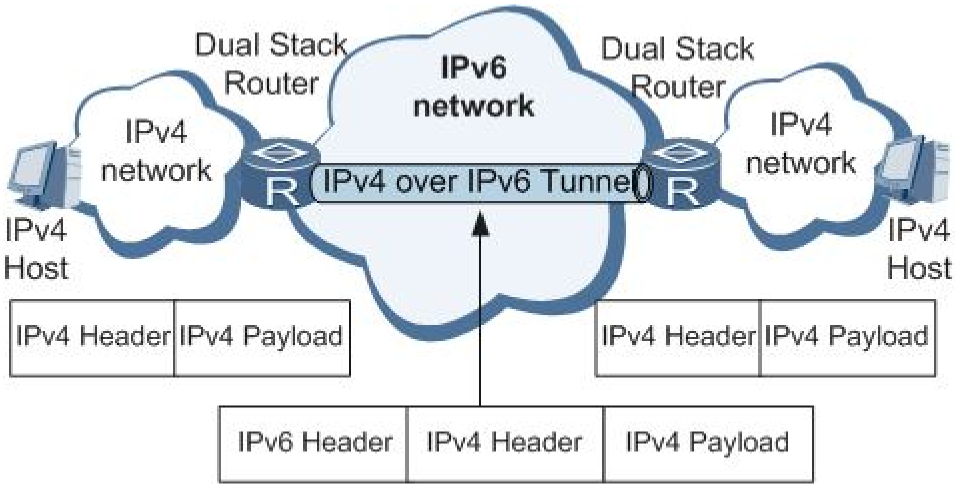


Figure 2.4: Deploying IPv6 over IPv4 Tunnels [13].

2.10 IPv4 Security Issues

Before talking about security in Pv6, we need to understand some of the best known limitations of its predecessor, IPv4. As mentioned before, IPv4 was designed with no security in mind. Because of its end-to-end model, IPv4 assumes that security should be provided by the end nodes. Today, the original Internet continues to be completely transparent and no security framework provides for resilient against threats such as: Denial of service attacks (DOS): in this kind of attack certain services are flooded with a large amount of illegitimate requests that render the targeted system unreachable by legitimate users, an example of DOS attack that results from an architectural vulnerability of IPv4 is the broadcast flooding attack or Smurf attack; Malicious code distribution: viruses and worms can use compromised hosts to infect remote systems. IPv4's small address space can facilitate malicious code distribution; Man-in-the-middle attacks: IPv4's lack of proper authentication mechanisms may facilitate men-in-the-middle attacks; Fragmentation attacks: this type of attacks exploits the way certain operating systems handle large IPv4 packets. An example of this type of attack is the ping of death attack [14].

2.11 Security Vulnerability in IPv6

The new IPv6 protocol represents a considerable advance in relation to the old IPv4. However, despite its innumerable virtues, IPv6 still continues to be by far vulnerable. We can summarize fundamental security vulnerabilities in IPv6 and present feasible countermeasures as the following:

2.11.1 Tracking the Identity of the User

Traditional interface identifiers for network adapters use a 48-bit address called an IEEE 802 address. It consists of a 24-bit company ID (also called the manufacturer ID), and a 24-bit extension ID (also called the board ID). The combination of the company ID, which is uniquely assigned to each manufacturer of network adapters, and the board ID, which is uniquely assigned to each network adapter at the time of assembly, produces a globally unique 48-bit address. This 48-bit address is also called the Media Access Control (MAC) address. For IPv6-based dial-up connections; the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto configuration. If the interface identifier is always based on the EUI-64 address (as derived from the static IEEE 802 address) as shown in figure 2.5, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet [15].

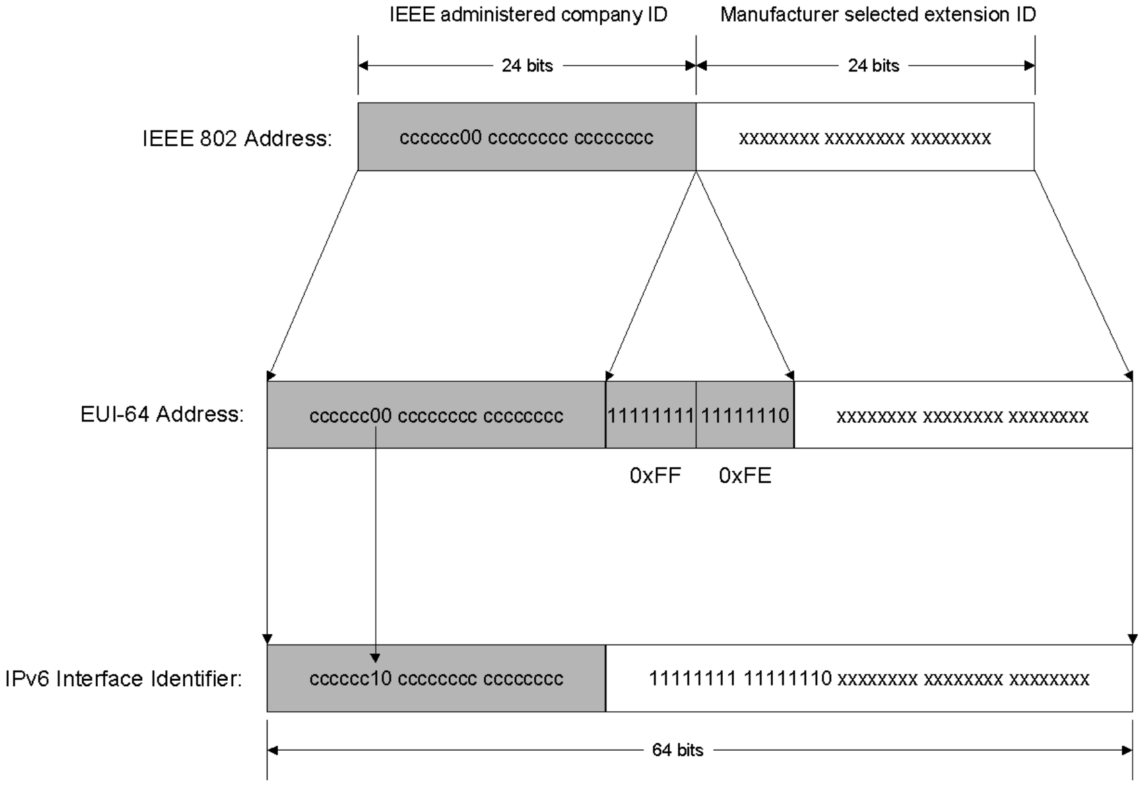

IEEE administered company ID
Manufacturer selected extension ID
24 bits
24 bits
IEEE 802 Address:
cccccc00 cccccccc cccccccc
xxxxxxxx xxxxxxxx xxxxxxxx
EUI-64 Address:
cccccc00 cccccccc cccccccc
11111111
11111110
xxxxxxxx xxxxxxxx xxxxxxxx
0xFF
0xFE
IPv6 Interface Identifier:
cccccc10 cccccccc cccccccc
11111111 11111110 xxxxxxxx xxxxxxxx xxxxxxxx
64 bits

Figure 2.5: The conversion to an IPv6 Interface Identifier [15].

2.11.2 IPv6 Address Spoofing Vulnerability

Because of IPv6 address depends on MAC address which in a sense the MAC address is a computer's true name on a LAN. A user might want to change the MAC address of a NIC for many reasons such as to get past MAC address filtering on a router; Sniffing other connections on the network.; To keep their burned in MAC address out of IDS and security logs or To pull off a denial of service attack. Therefore, many people changing their MAC address in different operating systems either manually or by software, this is privacy risk, because anyone who has your MAC address also has your IP address [15].

2.11.3 Fragmentation Security Vulnerability

Fragmentation is the process of dissecting an IP packet into smaller packets to be easily carried across a data network that cannot transmit large packets, In IPv6, fragmentation is never performed by the intermediary routers but by the end nodes themselves. So, only the end hosts are allowed to create and reassemble fragments. This process can be used by attackers to either hide their attacks or to attack a node by putting the attack into many small fragments; the attacker can try to bypass filtering or detection. Attackers can also create fragments in such a way as to exploit weaknesses in the method an end host uses to reassemble the fragments reassemble the fragments. Examples of this would be overlapping fragments, where there is an overlap in the offset and out-of-order fragments where the fragments' IDs do not match correctly with the data. Another type of fragment attack involves an attacker sending an incomplete set of fragments to force the receiving node to wait for the final fragment in the set. Fragmentation attacks can also involve nested fragments or fragments within fragments, where the IPv6 packet has multiple fragmentation headers. Fragmentation attacks are typically used by hackers with tools such as Whisker, Fragrouter, Teardrop, and Bonk [15].

2.11.4 Neighbor Discovery and Solicitation Security Consideration

In IPv4, subnets are generally small, made just large enough to cover the actual number of machines on the subnet. In contrast, the default IPv6 subnet size is a /64, a number so large it covers trillions of addresses, the overwhelming number of which will be unassigned. Consequently, simplistic implementations of Neighbor Discovery can be vulnerable to denial of service attacks whereby they attempt to perform address resolution for large numbers of unassigned addresses [15]. Such denial of service attacks can be launched intentionally (by an attacker).

2.11.5 DHCP Snooping

Dynamic Host Configuration Protocol for IPv6 (DHCPv6), enables DHCP servers to pass configuration parameters such as IPv6 network addresses and other configuration information to IPv6 nodes. DHCP plays an important role in any large network by providing robust stateful auto configuration and auto-registration of DNS Host Names. The two most common threats to DHCP clients come from malicious or mis-configured DHCP servers. A malicious DHCP server is one that is established with the intent of providing incorrect configuration information to the client. The motivation for doing so may be to mount a "man in the middle" attack instead of a valid server for services such as DNS or to cause a denial of service attack through mis-configuration of the client that causes all network communication from the client to fail [16].

2.12 Denial of service attack and its classification

Denial of service (DoS) attack is one of the major security threats to the IPv4 and IPv6 networks. In DoS attacks, a victim host(s) can be denied from the services by wasting its resources and disrupt its communication with other neighboring hosts on same link. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service. Moreover, when DoS attack is being attempted from large networks or systems then it is known as Distributed Denial of Service (DDoS) attacks [11].

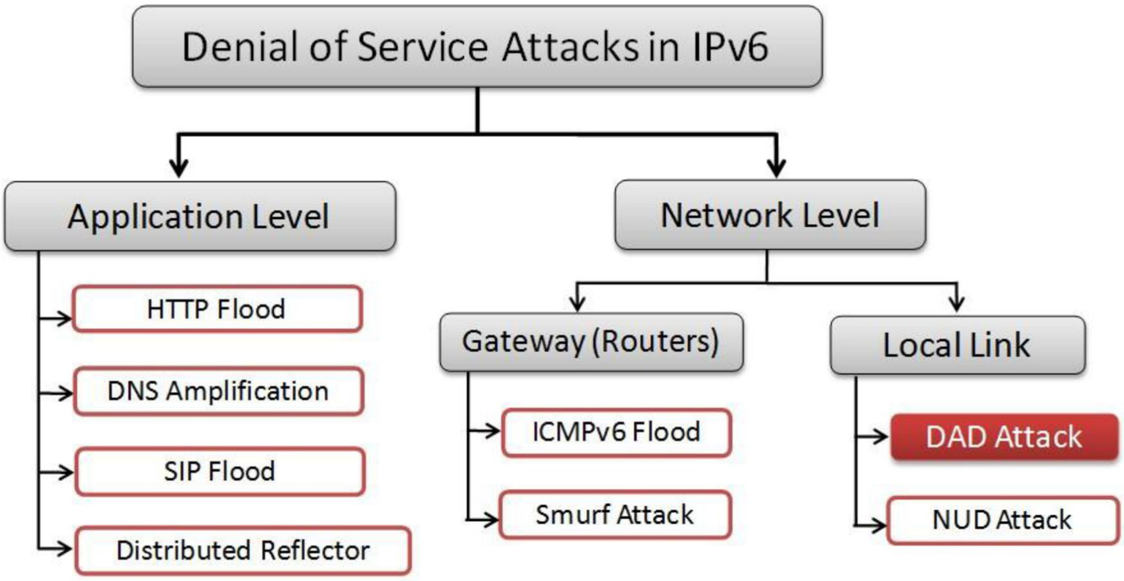


Figure 2.6: Taxonomy of DoS attacks in IPv6 network

Denial of Service (DoS) attacks in IPv6 network can be broadly classified into two main categories based on the attacked level such as; application level and network level. Further network level DoS attacks can be subdivided into gateway (router) and local link levels respectively. Figure 1 depicts the taxonomy of DoS attacks in IPv6 network.

Denial-of-service attacks are most common exploits happening on todays' internet. DoS attacks host two sub types such as Malformed Packet attacks and Packet flood attacks. The most common DoS attacks occur with flooding either bogus or undefined traffic to the targeted host. Targeted host get busy with handling this flooding, so it fails to give services for legitimate users. There exist different DoS type attacks at different layers of Open Systems Interconnection Model (OSI) model [11].

Table 2.2: DoS attack types at various OSI model

OSI Layer	DoS types
Application	Email Spams; Web DoS
Presentation	Malformed SSL requests.
Session	Telnet DoS.
Transport	SYN Floods; Smurf Attacks.
Network	ICMP/v6 Flooding; RA; NS, and etc…
Data-Link	MAC Flooding
Physical	Dummy packet Attack; Packet with more bit errors

2.13.1 ICMP Flood Attack

ICMP-Flood, as known as Ping flood, it makes use of the echo response mechanism of ICMPv6. The attacking node sends large amounts of ICMP packets to the victim with their source targeting at another IPv6 node or an invalid IPv6 address. This can waste the resources of victim and cause it to stop responding to other requests [17].

2.12.2 Denial of Service Attack on DAD Process

During the DAD operation, an attacker can disguise the victim host while attempting to verify its address uniqueness in IPv6 link local communication by using the specific address and responds to every detection message. Thus, it the victim host may be unable to configure its IP address such type of attack is known as DoS on DAD attack. During this attack an attacker can respond to every duplicate address detection attempts made by a newly joining host in IPv6 link local communication. In case an attacker claims addresses, the other host(s) on a same link will never be able to configure an IP address [11].

2.14 IPSec Overview

IPSec refers to a suite of protocols from the IETF providing network layer encryption and authentication for IP-based networks, the objective of IPSec is to authenticate and/or encrypt all traffic at the IP level. The main present-day use of IPSec is in establishing virtual private networks for connecting remote offices and users to the enterprise using the public Internet. In IPv4, widely-used NATs, but IPv6 expands address space and making NAT unnecessary. IPv6 is expected to increase the use of IPSec in end-to-end communications. With IPSec, data can be sent across a public network without observation, modification, or spoofing. IPSec functionality is similar in both IPv6 and IPv4; however, site-to-site tunnel mode only is supported in IPv6 [4].

IPSec is performed using different algorithms categorized as encryption (aes, 3des), integrity (MD5, SHA), key exchange (DIFFIE-HELLMAN) and authentication methods (pre shared certificates). These algorithms are needed for implementation in two different phases of IPSec's IKE method. Hash is used in authentication protocol and encapsulation security protocol. IPSec uses Hashed Message Authentication Codes (HMAC) and provides hashing using MD5 (Message Digest 5) and SHA 1 (Secure Hash Algorithm 1). Diffie Hellman key is used in IPSec for two systems who want to establish a secure communication and uses a shared secret key which is known only to them. The shared secret key is generated from public and private keys of both peers. AES is a symmetric key algorithm where the same key is used for encryption and decryption. AES encrypts block size of 128 bits using key size of 128, 192 or 256 bits. AES algorithm consists of steps such as SubBytes, ShiftRows, MixColumns and AddRoundKey. The first stage of the process consists of key expansion where round keys are generated using cipher key. IPSec uses AES-CBC mode (cipher block chaining mode) for providing stronger security to the data. Pre Shared key is used in IPSEC in IPv6 networks to share a secret key between two peers. This shared secret key is calculated during the phase I of IPSec's IKE phase 1 configuration. It is used to provide authentication information between two devices who wish to securely transmit information by creating a secure channel. Advantages of IPSec are packets at the network layer are encrypted and do not provide any overhead in other operations therefore it increases performance. It is scalable and can be implemented in any IP enabled networks. It provides various security mechanisms such as confidentiality, integrity checking and replay protection. Implementations of IPSec do not affect upper layers thus it ensures application transparency. Disadvantage of IPSec are that it is implemented at the end points i.e. security gateways and requires large processing power. Security is compromised if shared keys are exposed. Complexity in maintaining and deploying IPSec can lead to configuration errors due to which organization's network can lead to security risk [5].

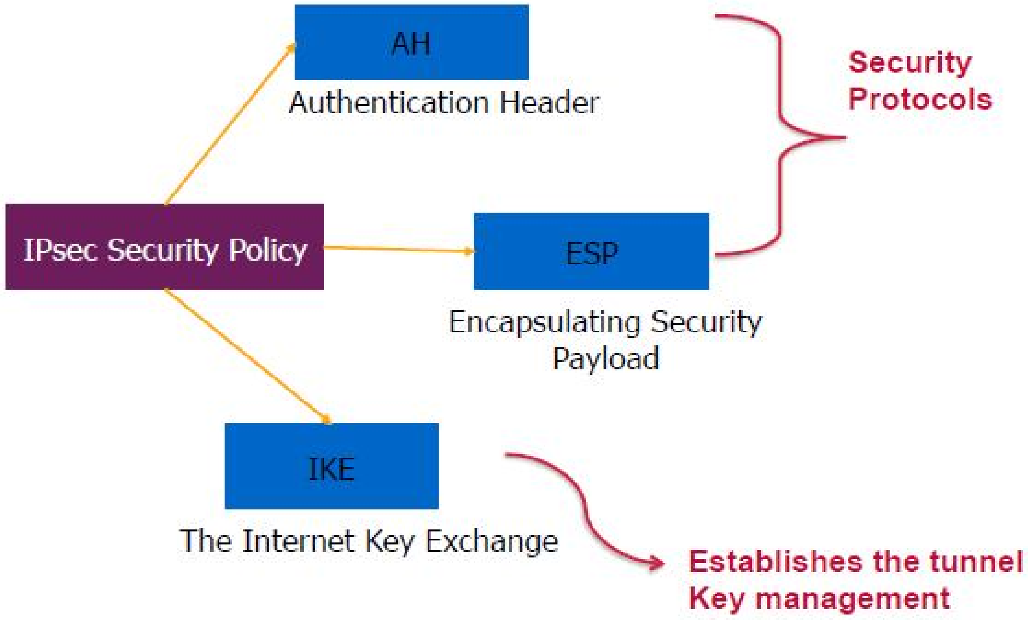


Figure 2.7: IPSec Architecture.

2.13.1 IPSec Security Features

It was designed to provide high security while transferring packets across the networks and it is the most commercial for connecting network sites. IPSec gives the network this features: Authentication which Verifies that the packet at receiver end and at source are same or not; Integrity which Ensures that the contents of the packet did not change in transit; and Confidentiality that means Conceals the message content through encryption [18].

2.13.2 IPSec Components

IPSec contains the following elements: Authentication Header (AH); Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP); AH provides authentication and integrity, which protect against data interfere, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet among the IP header and any upcoming packet contents [18].

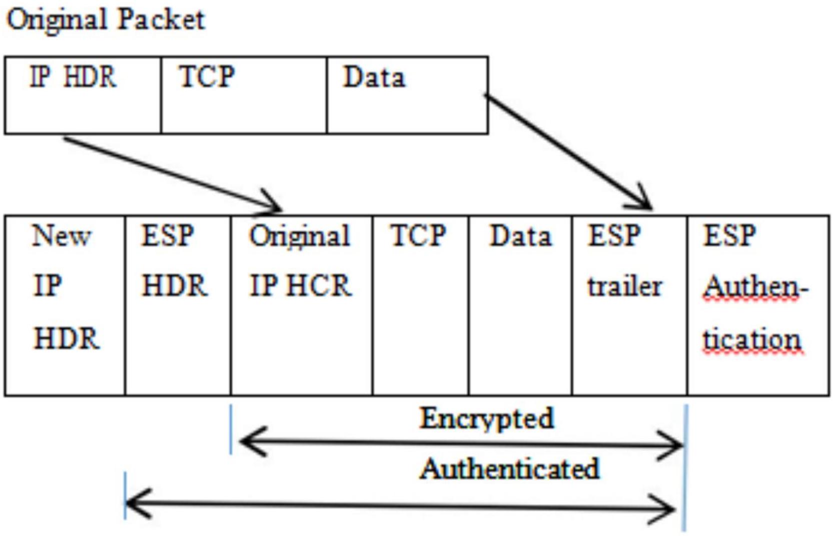


Figure 2.8: Authentication header in tunnel mode [18].

2.13.3 IPSec Modes

IPSec provides security under two modes of operation - transport mode and tunnel mode. These two modes provide security through any of the ESP or AH protocols. These protocols are meant to provide protection to upper layer. IPSec transport mode is used for a direct communication between the end points. It encapsulates or authenticates only the IP payload. The AH or ESP protocol header is inserted between the IP header and the IP payload. IPSec Tunnel mode is an encapsulation of an IP packet within an IP packet to form an IPSec packet. The payload of this IPSec packet is the original IP packet including both the original IP header and IP payload. The outer IP header is inserted to the IPSec packet to show the tunnel endpoint. This tunnel mode is used to construct a secured VPN. Tunneling helps in constructing a VPN without the intervention of ISP [19].

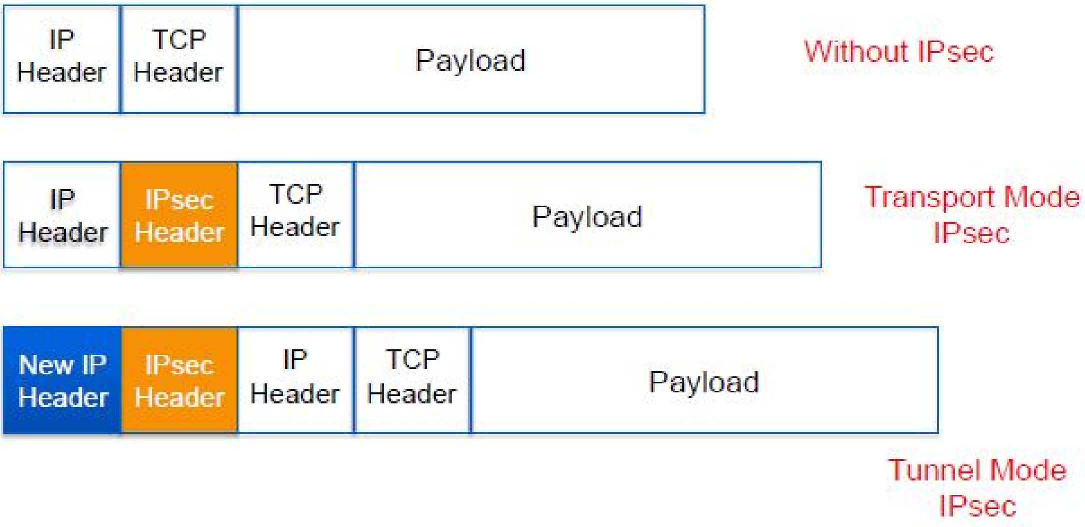


Figure 2.9: Tunnel vs. Transport mode IPSec [19].

2.14 VPN Overview

A technical solution to protect data through Internet is VPN. VPN is a virtualization concept that virtualizes the private network. It uses strong security solution for providing private communications over the public physical network. VPN is an alternative to Private Network or Private leased line connection. Private network is very much secured compared to the Internet provided VPN. But it is very expensive, requires much time and space to install and not feasible for every enterprise. A single private network will constitute only a single VPN. Large geographically dispersed network is difficult to administrate and maintain, Restoration and communication become worse during link failure. VPN is a combination of tunneling, authentication, integrity, encryption and access control [19].

2.14.1 VPN Types

In general, two different VPN types can be differentiated: Client-to-Site VPN (also known as Remote Access VPN) and Site-to-Site VPN. Remote Access VPN focuses on connecting a single client to a network. The most significant example in an enterprise environment is connecting employees from outside of the network to the enterprise network in order to access resources such as email, file or intranet servers. There are plenty of various client software tools to establish a Remote Access VPN connection. Modern operating systems have built-in functions to create VPN connections. For example, Windows can natively build VPN connections using Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). However, companies are using enterprise level solutions such as Cisco Any Connect or Palo Alto Global Protect, depending on the firewall and VPN solution that are used. These clients usually allow the VPN administrators, mostly network engineers, to configure many network parameters for the clients centrally and monitor the users [20].

However, Site-to-Site VPN is the pairing of two independent networks that want to access each other. The most significant VPN protocol for Site-to-Site VPN is IPSec and is used by every major VPN network hardware vendor. The connection has to be created between a local and a peer VPN gateway, which exchange important parameters before establishing the tunnel. Those parameters consist of encryption, hashing and key exchange details, but also the networks that are supposed to be propagated to the other side. Therefore, every gateway is sending their local IP addresses and the expected peer IP addresses. This information must match in order to establish a Security Association (SA), a tunnel [20].

2.15 Related Work

Authors in [1]: In VPN IPSec is implemented by creating a tunnel between two end users. The packet is encrypted based on the need and encrypted traffic is sent across the network with the help of a tunnel. Advantage of IPSec in VPN is that it provides end to end encryption and provides services such as authentication and encryption. It has no affect on higher layers above layer 3 i.e. network layer at which IPSec operates. IPSec can be used to protect information transmitted between two end sites and data which is used to provide authentication services needs to be protected; Stealing usernames and passwords during logging activities are vulnerable to attacks during authentication; there are several security threats at different levels such as traffic analysis, spoofing of MAC addresses, flooding attacks etc; Authors in [4]: the paper investigated the IPSec based VPN sorting out a structure and made an exchange on its related traditions. The paper highlights IPSec and its irregularity with the current IP framework and routing. Before arranging IPSec based VPN yield of a structure were a first source and target. Regardless, in the wake of arranging the solicitations of VPN, the outcome was appeared in above figures and the best way to deal with setup the VPN compose is direct and convenient, which has a nice application prospect in the remote secure transmission and shape the ensured correspondence between two branches of an association. So, it is a monetarily adroit and secure response for the association customer to relate various goals around the world together by finishing IPSEC based VPN; Authors in [11]: The purpose of this paper was to analyses the impact of DoS on DAD attack and its outcome. In pursuant to this, an IPv6 testbed has been designed and implemented to carry out the attacks on multiple OS platforms. The testbed outcome has shown that during DoS-on-DAD attack IPv6 hosts are unable to obtain IPv6 addresses due to DAD process failure. There are existing mechanisms and approaches that, to some length, address this issue but have drawbacks in terms of efficiency and complexity. Thus, a more effective security mechanism is required to secure DAD process during address auto-configuration in IPv6 link local network; Authors in [21]: This paper aim to propose a technique from existing taxonomies for the detection and analysis of synchronous and non-synchronous traffic flow with the observation of network in time-slot. Furthermore, this approach uses traffic source authentication of legitimate and malicious traffic using CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) in various ways. Hence, the proposed work is focused on traffic flow analysis of both usual and malicious traffic. In initial stage, aim of the proposed algorithm is serve the entire incoming traffic request including both genuine requests as well as illegitimate request within time-slots. So, it is necessity to reduce the DDoS attack from synchronous and non-synchronous traffic flow.

CHAPTER THREE

CONFIGURATION OF SYSTEM SCENARIOS

Chapter Three

Configuration of System Scenarios

3.1 System Tools

This section describes the system tools which are used to implement each scenario of simulation network as the follows:

3.1.1 GNS3 Simulation

GNS3 is a Graphical Network Simulator that allows emulation of complex networks. It is helpful in simulating large networks based on real CISCO IOS images and evaluates the performance of complex network scenarios. GNS3 is seen as Real time network simulation without the need for network hardware, it can be used to capture network traffic and detect any flaws in the simulated network with the help of software called wireshark.

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software, communications protocol development and education. Through various tools available in the program, Wireshark is able to capture packets by deeper understanding and statistical analysis of packets.

3.1.2 Kali Linux

Kali is just a random name, it is an Open Source operating system and a Debian-based Linux distribution aimed at advanced Penetration Testing and Security auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

Kali is a Linux-based open source system; it has built-in THC-IPv6 attacking toolkit support. Kali is used in this topology as attacker under

IPv6 network that apply VPN IPSec to test IPSec outcome with different attacks.

3.1.3 VM VirtualBox

VirtualBox is a free and open-source software, that can be installed on a number of host operating systems, including: Linux, mac-OS, Windows, Solaris, and Open-Solaris.

VirtualBox is used here to run Kali Linux operating system which is connected to IPv6 networks with GNS3 through Cloud.

3.2 System Implementation

As a supporter to IPv6 in GNS3, Cisco (7200) series router has been used to design the network topology as shown in figure 3.1.

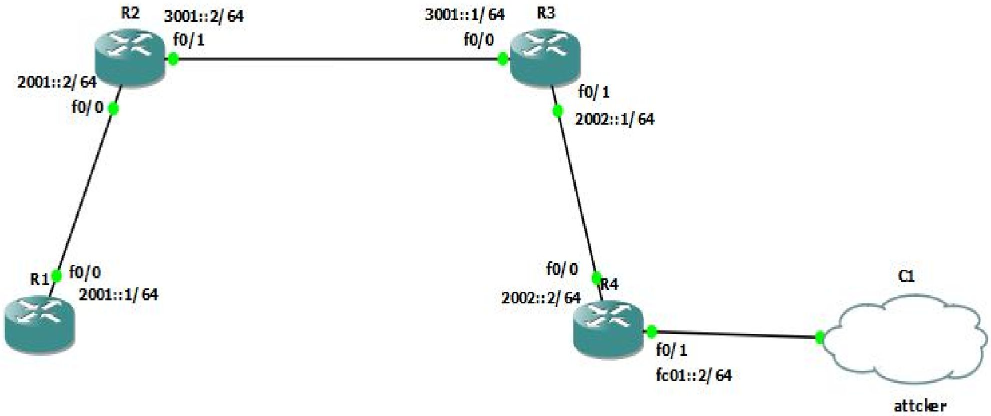


Figure 3.1: Network Topology

3.3 Configuration

In this section configuration is detailed as follows:

3.3.1 Configuration Routers

After IPv6 addresses have been assigned in each router, default routing protocol is configured to connect all routers in different networks.

3.3.2 Configuring IPSec for IPv6 Traffic

To complete site-to-site VPN configured IPSec in edge routers, then IPSEC tunnel mode will be configured in the same routers to protect traffic being tunneled over a non trusted network. VPN is implemented to protect all IPv6 traffic between two trusted networks.

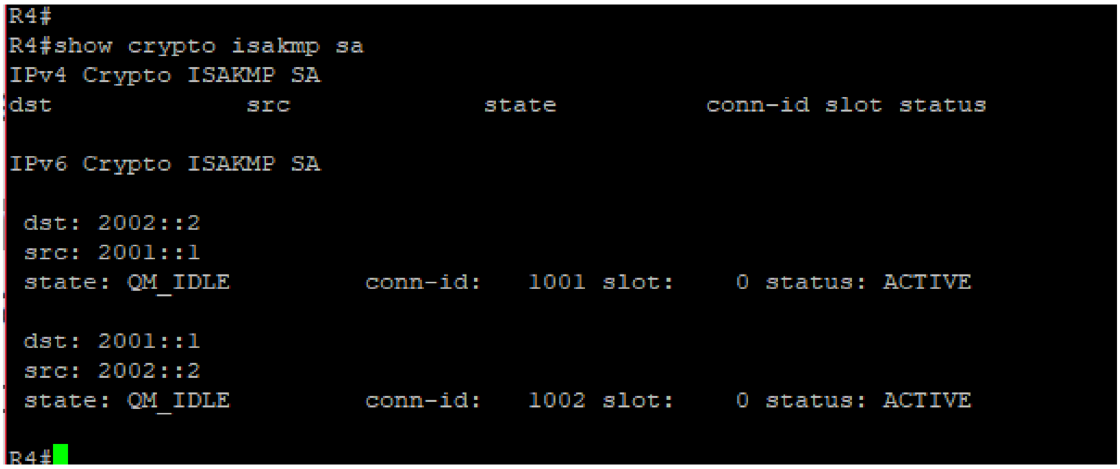
3.3.3 Site-to-Site VPN Configuration on Routers

Step 1: Configure IKE Policy and Pre-shared Key: each router must be configured with the same key, but the configuration statement should designate the address of the appropriate interface on the peer router. These keys are default ISAKMP keying. Multiple named keying can be used when the router is hosting remote client VPNs for multiple different groups of clients.

Step 2: Configure an IPSec Transform Set and IPSec Profile: Configure the same IPSec Transform Set and IPSec Profile on the routers R1 and R4.

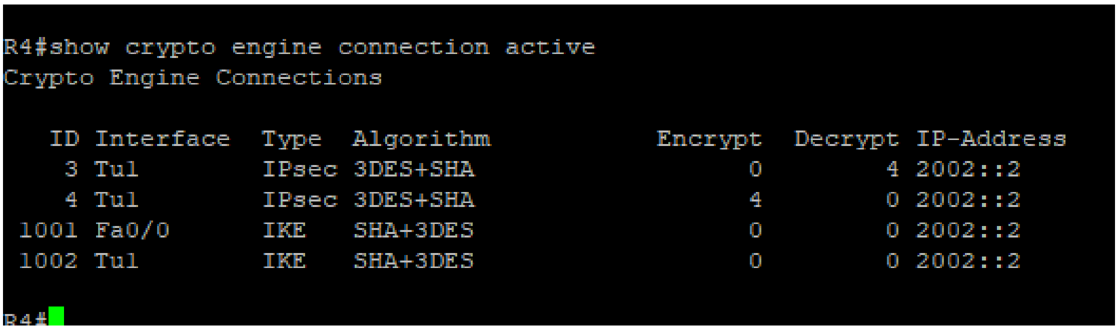
Step 3: Configure an ISAKMP Profile in IPv6: ISAKMP profile is configured in the routers R1 and R4 to ensure that configuration statement must designate the identity address of the appropriate interface on the peer router, as shown in figure 3.2 and figure 3.3.

Step 4: Configure IPSec IPv6 VTI (Virtual Tunnel Interface): Configuring IPv6 IPSec VTI on router is pretty simple as shown following figures.



```
R4#
R4#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA

 dst: 2002::2
 src: 2001::1
 state: QM_IDLE         conn-id:   1001 slot:    0 status: ACTIVE

 dst: 2001::1
 src: 2002::2
 state: QM_IDLE         conn-id:   1002 slot:    0 status: ACTIVE

R4#
```

Figure 3.2: The active ISAKMP sessions on the router



```
R4#show crypto engine connection active
Crypto Engine Connections

   ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
    3 Tu1        IPsec 3DES+SHA                  0        4 2002::2
    4 Tu1        IPsec 3DES+SHA                  4        0 2002::2
 1001 Fa0/0      IKE   SHA+3DES                  0        0 2002::2
 1002 Tu1        IKE   SHA+3DES                  0        0 2002::2

R4#
```

Figure 3.3: Configuration information for the crypto engines

3.4 Testing Scenario

By assumption, there are two scenarios in network topology to test IPSec under two different attacks:

3.4.1 Spoofing attack using Wireshark

Is a situation when a person or a program has successfully masquerades as another by falsifying data so as to gain an illegitimate advantage . As an example of this attack, the attacker will use a man-in-the-middle attack is which the attacker connects a hub to a network segment that carries the traffic the attacker wants to capture. The attacker could then use a packet-capture utility to capture traffic traveling between end systems, as shown in figure 3.4. If the captured traffic is in plain text, the attacker might be able to obtain confidential information, such as usernames and passwords. This attack can be classified as confidentiality attack.

A confidentiality attack attempts to make “confidential” data (such as personnel records, usernames, passwords, credit card numbers, and e-mails) viewable by an attacker, because an attacker often makes a copy of the data, rather than trying to manipulate the data or crash a system.

A packet-capture utility (such as Wireshark) can capture packets visible by a PC’s network interface card (NIC) by placing the NIC in promiscuous mode. Some protocols (for example, Telnet and HTTP) are sent in plain text. Therefore, an attacker can read these types of captured packets, perhaps allowing him to see confidential information.

3.4.2 Denial-of-service (DoS) using kali Linux

Denial-of-service is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. Denial-of-Service attacks can be categorized into at least two different types which include: Protocol-Based Attacks: include Smurf attacks (ICMP to a broadcast IP with a spoofed IP), Fraggle attacks (same as the Smurf, only using UDP), SYN floods, ping of deaths (oversized ICMP with the same destination and source IP and port), and many others; Application Layer Attacks are compromised of what appear to be legitimate application layer (layer 7) requests to the server but in fact they are intended to crash it.

Kali can be used as an attacker to run the DoS attack in IPv6 local link network. It has been built-in THC-IPv6 attacking toolkit support, for testing IPv6 and ICMPv6 protocol weakness as shown in figure 3.5. Therefore, In order to monitor and capture the network traffic Wireshark network analysis tool has been used to analyze the captured network traffic. Cisco routers C7200 has been used as a gateway routers for the network and Cisco Ethernet switch has been used to connect all the hosts in IPv6 link local network.

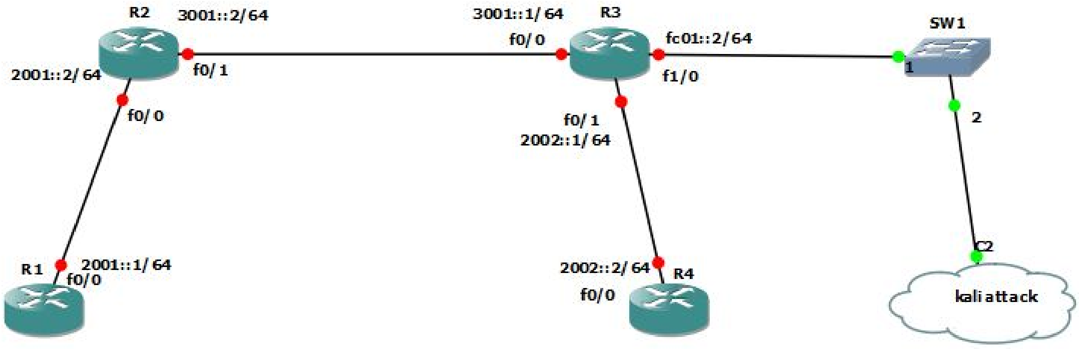
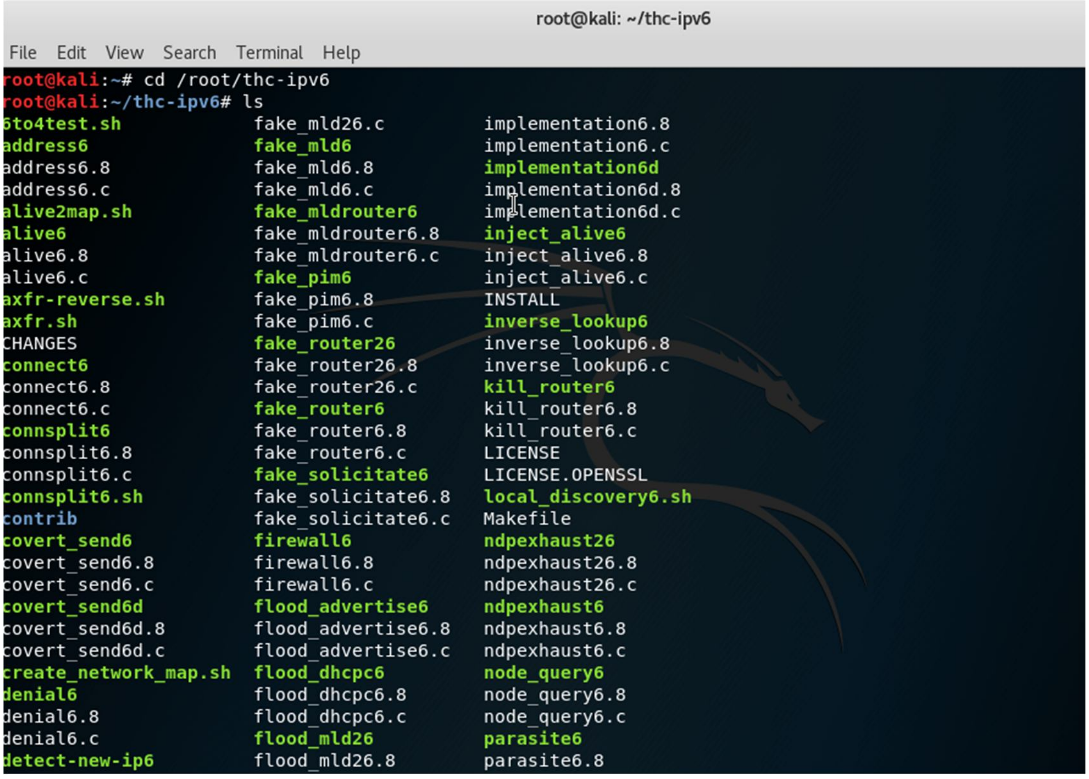


Figure 3.4: Testbed topology.



```
root@kali:~# cd /root/thc-ipv6
root@kali:~/thc-ipv6# ls
6to4test.sh             fake_mld26.c         implementation6.8
address6                fake_mld6            implementation6.c
address6.8              fake_mld6.8          implementation6d
address6.c              fake_mld6.c          implementation6d.8
alive2map.sh            fake_mldrouter6      implementation6d.c
alive6                  fake_mldrouter6.8    inject_alive6
alive6.8                fake_mldrouter6.c    inject_alive6.8
alive6.c                fake_pim6            inject_alive6.c
axfr-reverse.sh         fake_pim6.8          INSTALL
axfr.sh                 fake_pim6.c          inverse_lookup6
CHANGES                 fake_router26        inverse_lookup6.8
connect6                fake_router26.8      inverse_lookup6.c
connect6.8              fake_router26.c      kill_router6
connect6.c              fake_router6         kill_router6.8
connsplit6              fake_router6.8       kill_router6.c
connsplit6.8            fake_router6.c       LICENSE
connsplit6.c            fake_solicitate6     LICENSE.OPENSSL
connsplit6.sh           fake_solicitate6.8   local_discovery6.sh
contrib                 fake_solicitate6.c   Makefile
covert_send6            firewall6            ndpexhaust26
covert_send6.8          firewall6.8          ndpexhaust26.8
covert_send6.c          firewall6.c          ndpexhaust26.c
covert_send6d           flood_advertise6     ndpexhaust6
covert_send6d.8         flood_advertise6.8   ndpexhaust6.8
covert_send6d.c         flood_advertise6.c   ndpexhaust6.c
create_network_map.sh   flood_dhcpc6         node_query6
denial6                 flood_dhcpc6.8       node_query6.8
denial6.8               flood_dhcpc6.c       node_query6.c
denial6.c               flood_mld26          parasite6
detect-new-ip6          flood_mld26.8        parasite6.8
```

Figure 3.5: Attack toolkit for testing IPv6 weaknesses.

CHAPTER FOUR

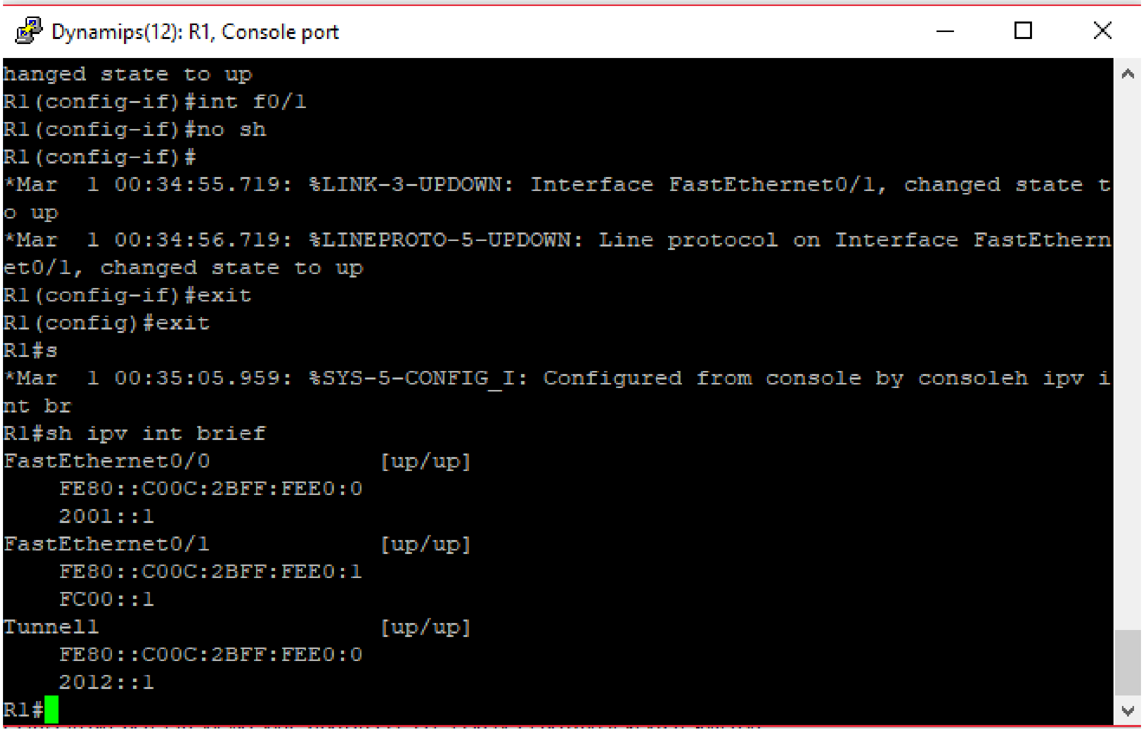
RESULTS AND DISCUSSION

Chapter Four

Result and Discussion

4.1 System Simulation

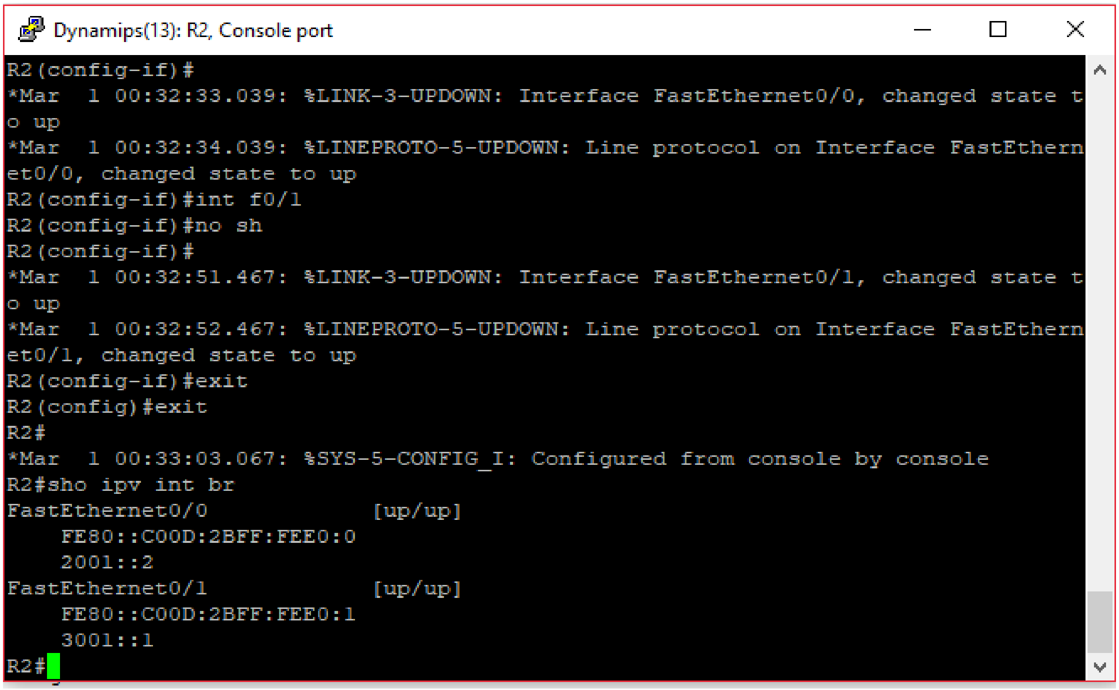
IPv6 address has been assigned to four routers: R1, R2, R3, and R4. Each router has a specific address. The default routing protocol has been applied between the routers to ensure that all packages are sent via the default route as shown in the following figures.



```
hanged state to up
R1(config-if)#int f0/1
R1(config-if)#no sh
R1(config-if)#
*Mar  1 00:34:55.719: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:34:56.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R1(config-if)#exit
R1(config)#exit
R1#s
*Mar  1 00:35:05.959: %SYS-5-CONFIG_I: Configured from console by consoleh ipv i
nt br
R1#sh ipv int brief
FastEthernet0/0            [up/up]
    FE80::C00C:2BFF:FEE0:0
    2001::1
FastEthernet0/1            [up/up]
    FE80::C00C:2BFF:FEE0:1
    FC00::1
Tunnel1                    [up/up]
    FE80::C00C:2BFF:FEE0:0
    2012::1
R1#
```

Figure 4.1: IPv6 interfaces of R1

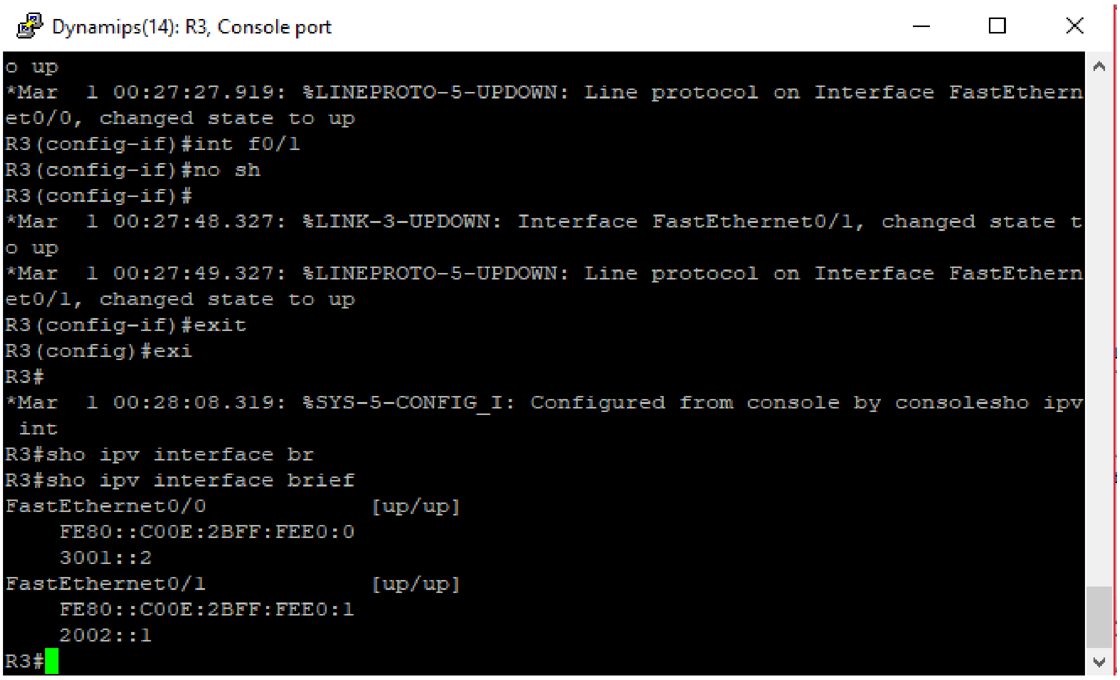
To show the IPv6 interfaces on each router, the specific command: “show ipv6 interface brief” has to be used to summarize interfaces address and tunnel address when used in the network.



```
R2(config-if)#
*Mar  1 00:32:33.039: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:32:34.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R2(config-if)#int f0/1
R2(config-if)#no sh
R2(config-if)#
*Mar  1 00:32:51.467: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:32:52.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R2(config-if)#exit
R2(config)#exit
R2#
*Mar  1 00:33:03.067: %SYS-5-CONFIG_I: Configured from console by console
R2#sho ipv int br
FastEthernet0/0            [up/up]
    FE80::C00D:2BFF:FEE0:0
    2001::2
FastEthernet0/1            [up/up]
    FE80::C00D:2BFF:FEE0:1
    3001::1
R2#
```

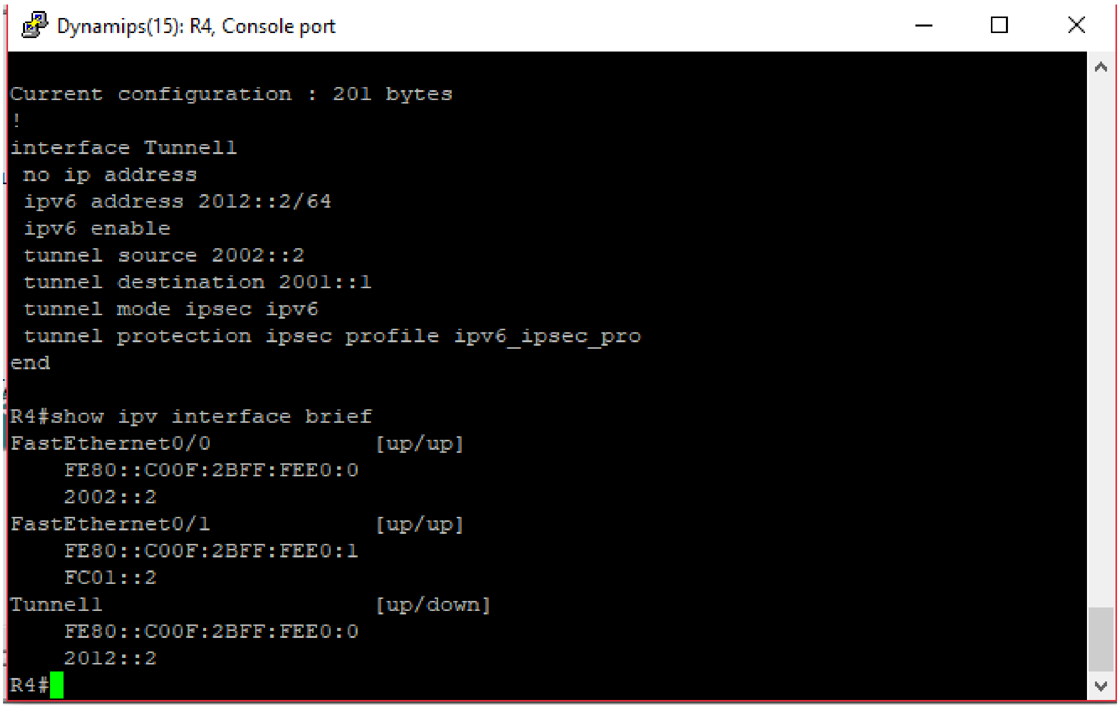
Figure 4.2: Ipv6 interfaces of R2

Figure 4.1 explains the interfaces of router R1, IPv6 and tunnel address when in the up position. The tunnel is addressed as (2012::1) IPv6 address.



```
o up
*Mar  1 00:27:27.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R3(config-if)#int f0/1
R3(config-if)#no sh
R3(config-if)#
*Mar  1 00:27:48.327: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:27:49.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R3(config-if)#exit
R3(config)#exi
R3#
*Mar  1 00:28:08.319: %SYS-5-CONFIG_I: Configured from console by consolesho ipv
 int
R3#sho ipv interface br
R3#sho ipv interface brief
FastEthernet0/0            [up/up]
    FE80::C00E:2BFF:FEE0:0
    3001::2
FastEthernet0/1            [up/up]
    FE80::C00E:2BFF:FEE0:1
    2002::1
R3#
```

Figure 4.3: Ipv6 interfaces of R3



```
Current configuration : 201 bytes
!
interface Tunnel1
 no ip address
 ipv6 address 2012::2/64
 ipv6 enable
 tunnel source 2002::2
 tunnel destination 2001::1
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipv6_ipsec_pro
end

R4#show ipv interface brief
FastEthernet0/0            [up/up]
    FE80::C00F:2BFF:FEE0:0
    2002::2
FastEthernet0/1            [up/up]
    FE80::C00F:2BFF:FEE0:1
    FC01::2
Tunnel1                    [up/down]
    FE80::C00F:2BFF:FEE0:0
    2012::2
R4#
```

Figure 4.4: Ipv6 interfaces of R4

Figures 4.3 and 4.4 show brief information about the IPv6 addresses that have been configured in routers R3 and R4, The tunnel is addressed in R4 as (2012::2) IPv6 address.

To communicate over public network IPSec-protected tunnel is set up between router R1 and router R4. Router R2 and router R3 have a global IPv6 address. However, they do not have any knowledge about the private subnets present on R1 and R4.

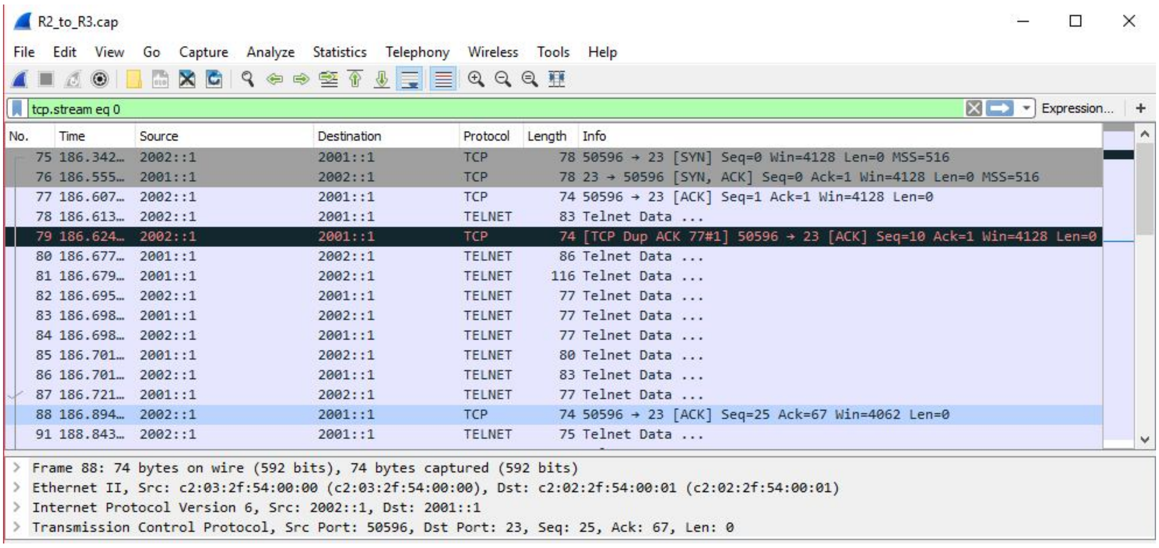
4.2 Result of First Scenario

After using the Telnet between edge routers R1 and R4 as shown in figure 4.5, implementation of man-in-the-middle is applied which represent spoofing attack.

The result is shown in the next figures in two cases; one before implementing VPN IPSec to protect the network, and the second case after implementation of security in IPv6 network.

4.2.1 Case One: Attack before IPSec

In the first case, figure 4.5 shows Telnet in wireshark as man-in-the-middle attack before implementation of IPSec.



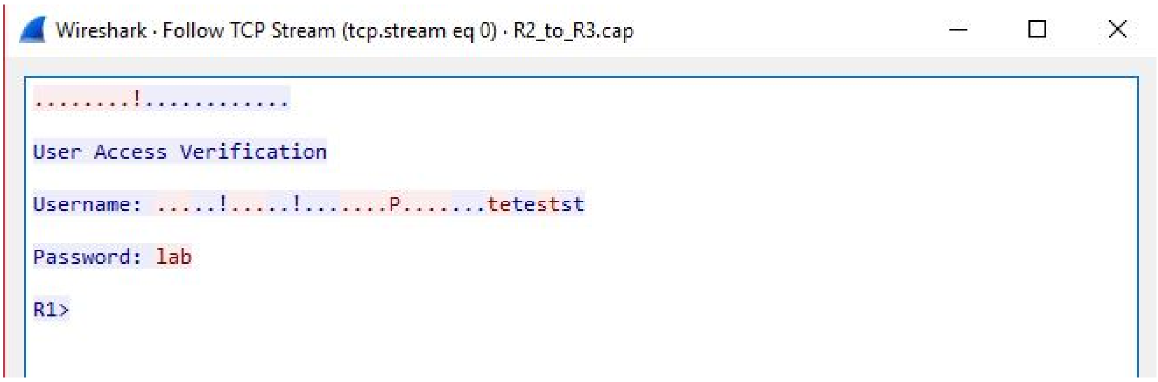
tcp.stream eq 0

```
No.  Time        Source     Destination  Protocol  Length Info
 75 186.342…   2002::1    2001::1      TCP         78 50596 → 23 [SYN] Seq=0 Win=4128 Len=0 MSS=516
 76 186.555…   2001::1    2002::1      TCP         78 23 → 50596 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=516
 77 186.607…   2002::1    2001::1      TCP         74 50596 → 23 [ACK] Seq=1 Ack=1 Win=4128 Len=0
 78 186.613…   2002::1    2001::1      TELNET      83 Telnet Data ...
 79 186.624…   2002::1    2001::1      TCP         74 [TCP Dup ACK 77#1] 50596 → 23 [ACK] Seq=10 Ack=1 Win=4128 Len=0
 80 186.677…   2001::1    2002::1      TELNET      86 Telnet Data ...
 81 186.679…   2001::1    2002::1      TELNET     116 Telnet Data ...
 82 186.695…   2002::1    2001::1      TELNET      77 Telnet Data ...
 83 186.698…   2001::1    2002::1      TELNET      77 Telnet Data ...
 84 186.698…   2002::1    2001::1      TELNET      77 Telnet Data ...
 85 186.701…   2001::1    2002::1      TELNET      80 Telnet Data ...
 86 186.701…   2002::1    2001::1      TELNET      83 Telnet Data ...
 87 186.721…   2001::1    2002::1      TELNET      77 Telnet Data ...
 88 186.894…   2002::1    2001::1      TCP         74 50596 → 23 [ACK] Seq=25 Ack=67 Win=4062 Len=0
 91 188.843…   2002::1    2001::1      TELNET      75 Telnet Data ...

> Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: c2:03:2f:54:00:00 (c2:03:2f:54:00:00), Dst: c2:02:2f:54:00:01 (c2:02:2f:54:00:01)
> Internet Protocol Version 6, Src: 2002::1, Dst: 2001::1
> Transmission Control Protocol, Src Port: 50596, Dst Port: 23, Seq: 25, Ack: 67, Len: 0
```

Figure 4.5: Man in the Middle attack before IPSec

In this case the attacker succeeded easily in detecting critical information packages (username and password) as shown in figure 4.6.

When man in the middle (MITM) attacks network using Wireshark, he can easily see TCP massages that contains user verification information between routers such as user name “test” and password “lab” during the telnet process in this network as shown in figure 4.5 above.

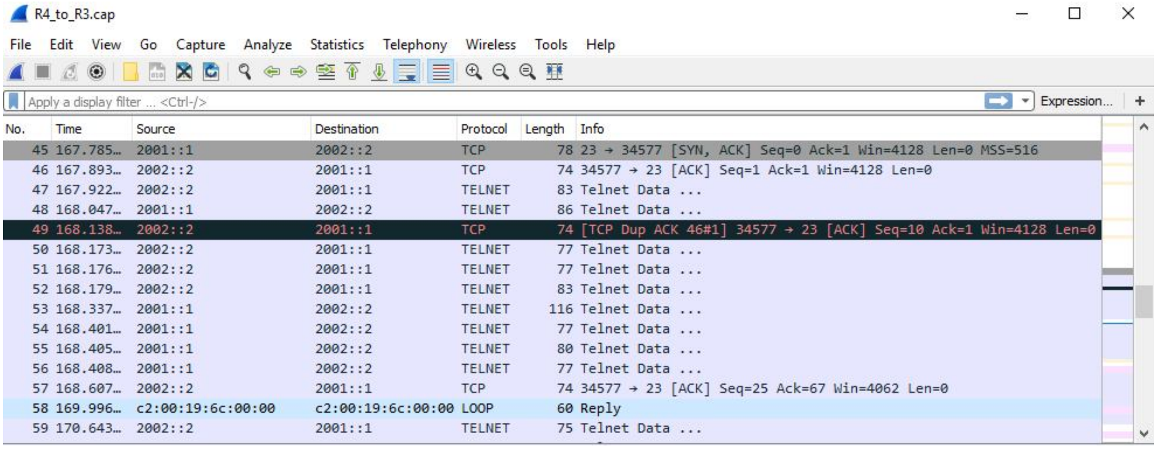

Wireshark · Follow TCP Stream (tcp.stream eq 0) · R2_to_R3.cap

```
........!...........

User Access Verification

Username: .....!.....!.......P.......teteststt

Password: lab

R1>
```

Figure 4.6: Capturing username and password before IPSec

4.2.2 Case Two: Attack after IPSec

In this case, figure 4.7 shows Telnet in wireshark as man-in-the-middle attack after implementation of IPSec in the network.

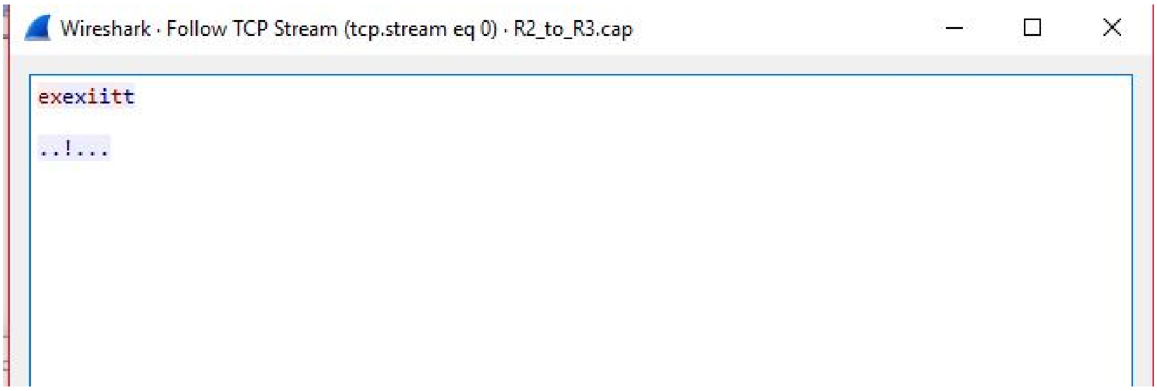


R4_to_R3.cap

No.	Time	Source	Destination	Protocol	Length	Info
45	167.785…	2001::1	2002::2	TCP	78	23 → 34577 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=516
46	167.893…	2002::2	2001::1	TCP	74	34577 → 23 [ACK] Seq=1 Ack=1 Win=4128 Len=0
47	167.922…	2002::2	2001::1	TELNET	83	Telnet Data ...
48	168.047…	2001::1	2002::2	TELNET	86	Telnet Data ...
49	168.138…	2002::2	2001::1	TCP	74	[TCP Dup ACK 46#1] 34577 → 23 [ACK] Seq=10 Ack=1 Win=4128 Len=0
50	168.173…	2002::2	2001::1	TELNET	77	Telnet Data ...
51	168.176…	2002::2	2001::1	TELNET	77	Telnet Data ...
52	168.179…	2002::2	2001::1	TELNET	83	Telnet Data ...
53	168.337…	2001::1	2002::2	TELNET	116	Telnet Data ...
54	168.401…	2001::1	2002::2	TELNET	77	Telnet Data ...
55	168.405…	2001::1	2002::2	TELNET	80	Telnet Data ...
56	168.408…	2001::1	2002::2	TELNET	77	Telnet Data ...
57	168.607…	2002::2	2001::1	TCP	74	34577 → 23 [ACK] Seq=25 Ack=67 Win=4062 Len=0
58	169.996…	c2:00:19:6c:00:00	c2:00:19:6c:00:00	LOOP	60	Reply
59	170.643…	2002::2	2001::1	TELNET	75	Telnet Data ...

Figure 4.7: Man in the Middle attack after VPN IPSec

As shown in figure 4.8 IPSec protected the packages by encapsulation and encryption traffic between routers, this enables the attacker to capture the traffic but he cannot enter into the details of the information; as such the data transmission network is secured from any modification which comes from non authorized users.



Wireshark · Follow TCP Stream (tcp.stream eq 0) · R2_to_R3.cap

```
exexiitt
..!...
```

Figure 4.8: Capturing username and password after implementation IPsec

Figure 4.8 shows the message that the MITM attacker can see instead of user data after implementing the IPsec. As such, the attacker cannot understand any information on the TCP stream.

4.3 Result of Second Scenario

By implementing the effect of DoS attack which take place by kali as attacker through IPv6 network by showing the result before and after the implementation the IPSec.

4.3.1 Package Traffic without any Attack

In this stage the packages between router R1 and router R2 as shown in figure 4.9 without any intervention on the network.

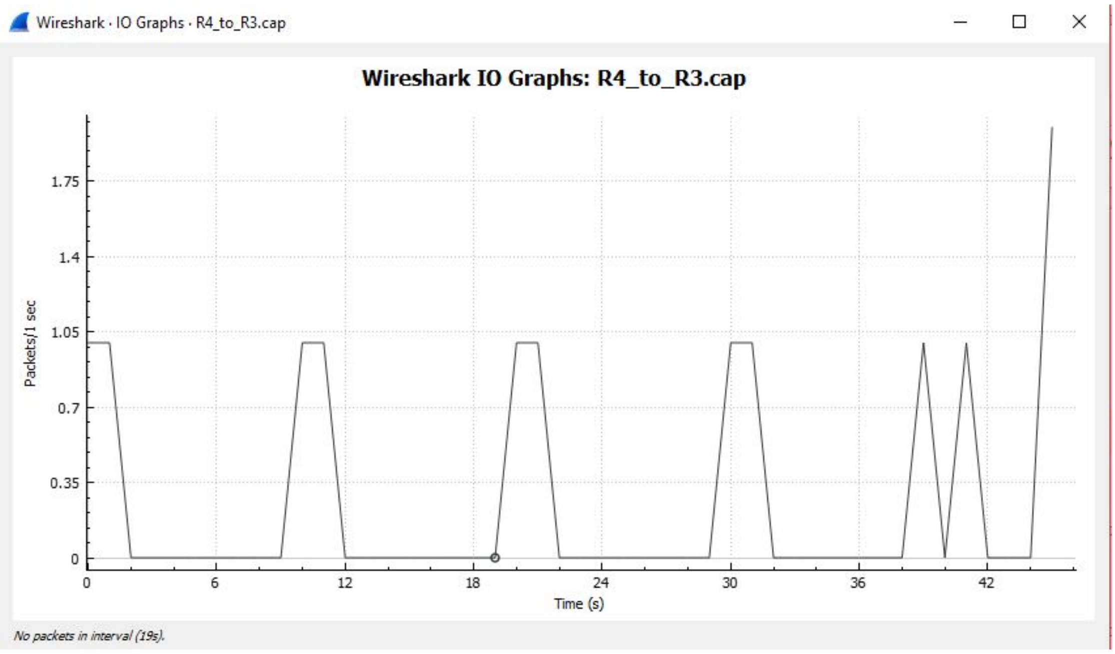
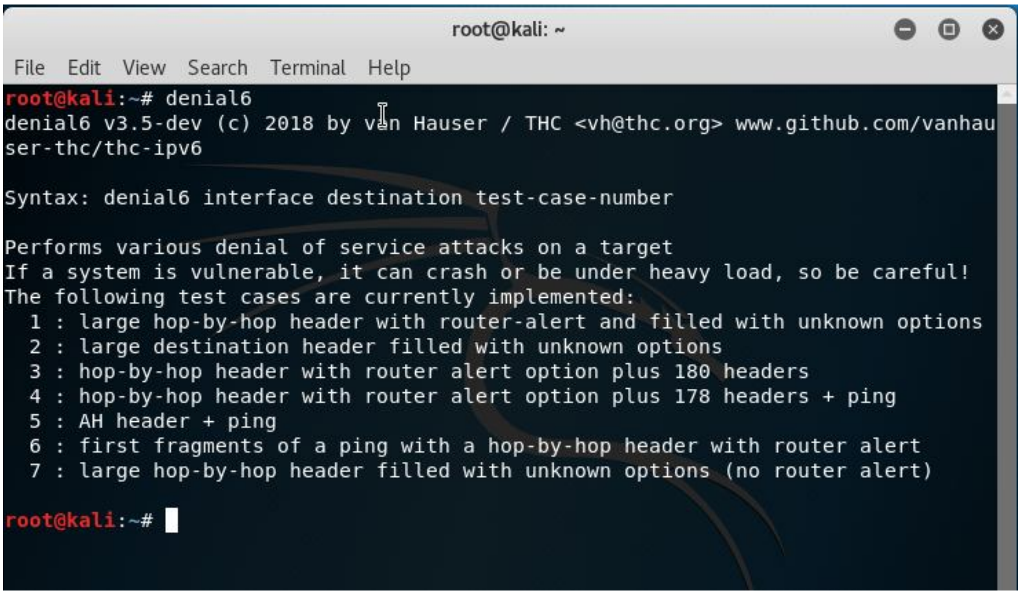

Wireshark · IO Graphs · R4_to_R3.cap
Wireshark IO Graphs: R4_to_R3.cap
Packets/1 sec
1.75
1.4
1.05
0.7
0.35
0
0
6
12
18
24
30
36
42
Time (s)
No packets in interval (19s).

Figure 4.9: Stable packages before any security or attack

By applying a network attack such as DoS attack, using Thc-IPv6 kali tools attacks to IPv6 network; such as denial6 which performs various denial of service attacks on a target as shown in figure 4.10. The DoS attack is running by thc-IPv6 tools called denial6 to the IPv6 local link network, as shown in figure 4.11.

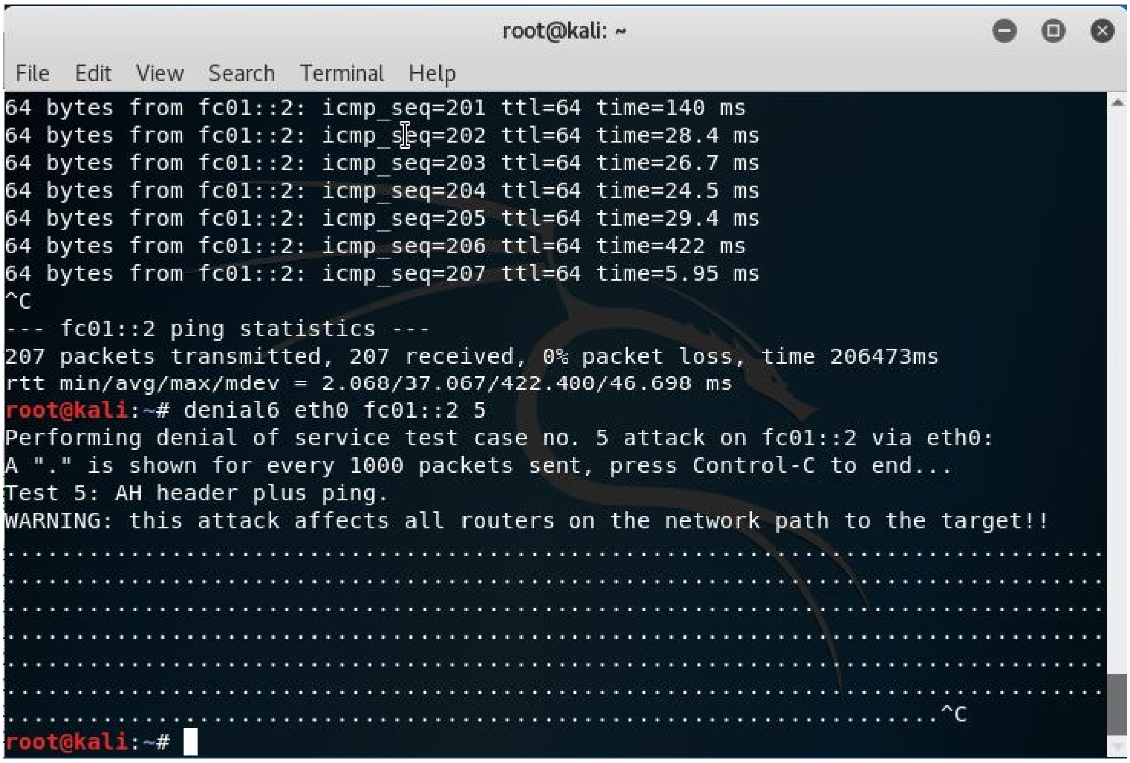
Denial6 is an option of the Dos attacks is used to attack a specific destination address. The syntax of denial6 appears with a test case number as shown in figure 4.10 to choose any various denials of serves attacks from the list of cases.

In figure 4.11 after checking the destination address by Ping results that show ICMP massages from the particular destination. Denial6 runs the DoS attack to this interface destination. The attack can affect all routers on the network path that can disable the connection on this network.



```
root@kali:~# denial6
denial6 v3.5-dev (c) 2018 by van Hauser / THC <vh@thc.org> www.github.com/vanhau
ser-thc/thc-ipv6

Syntax: denial6 interface destination test-case-number

Performs various denial of service attacks on a target
If a system is vulnerable, it can crash or be under heavy load, so be careful!
The following test cases are currently implemented:
  1 : large hop-by-hop header with router-alert and filled with unknown options
  2 : large destination header filled with unknown options
  3 : hop-by-hop header with router alert option plus 180 headers
  4 : hop-by-hop header with router alert option plus 178 headers + ping
  5 : AH header + ping
  6 : first fragments of a ping with a hop-by-hop header with router alert
  7 : large hop-by-hop header filled with unknown options (no router alert)

root@kali:~# 
```

Figure 4.10: Denial6 option for deferent DoS attacks



```
64 bytes from fc01::2: icmp_seq=201 ttl=64 time=140 ms
64 bytes from fc01::2: icmp_seq=202 ttl=64 time=28.4 ms
64 bytes from fc01::2: icmp_seq=203 ttl=64 time=26.7 ms
64 bytes from fc01::2: icmp_seq=204 ttl=64 time=24.5 ms
64 bytes from fc01::2: icmp_seq=205 ttl=64 time=29.4 ms
64 bytes from fc01::2: icmp_seq=206 ttl=64 time=422 ms
64 bytes from fc01::2: icmp_seq=207 ttl=64 time=5.95 ms
^C
--- fc01::2 ping statistics ---
207 packets transmitted, 207 received, 0% packet loss, time 206473ms
rtt min/avg/max/mdev = 2.068/37.067/422.400/46.698 ms
root@kali:~# denial6 eth0 fc01::2 5
Performing denial of service test case no. 5 attack on fc01::2 via eth0:
A "." is shown for every 1000 packets sent, press Control-C to end...
Test 5: AH header plus ping.
WARNING: this attack affects all routers on the network path to the target!!
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
....................................................................^C
root@kali:~#
```

Figure 4.11: Thc-IPv6 tools called denial6 to run the DoS attack.

4.3.2 Stage 1: Package Attacked before IPSec

Package traffic during the invaded by DoS attack before implementing VPN IPSec between routers, as showing in figure 4.12.

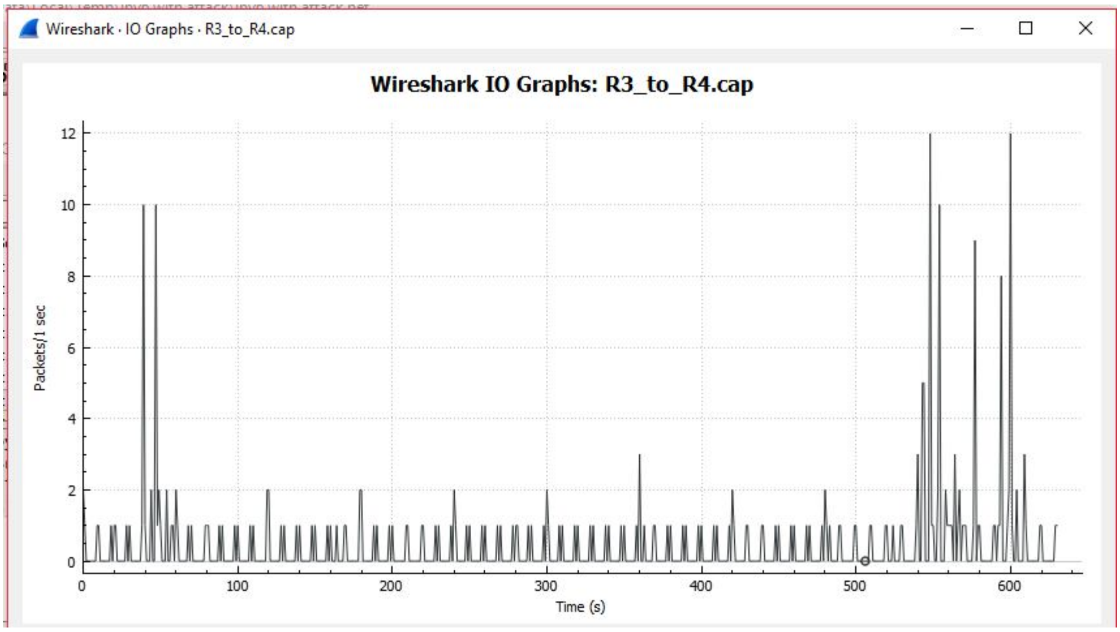


Figure 4.12: DoS attack before using IPSec

4.3.3 Stage 2: Package Attacked after IPSec

In this stage, the result of packages traffic during DoS attack after implementing VPN IPSec between routers, as shown in figure 4.13

The traffic of packages at a specific time between router R3 and R4 before and after implementing VPN IPsec does not change; that means, IPsec cannot ensure the availability of network in case of a DoS attack as shown in Figure 4.12 and figure 4.13.

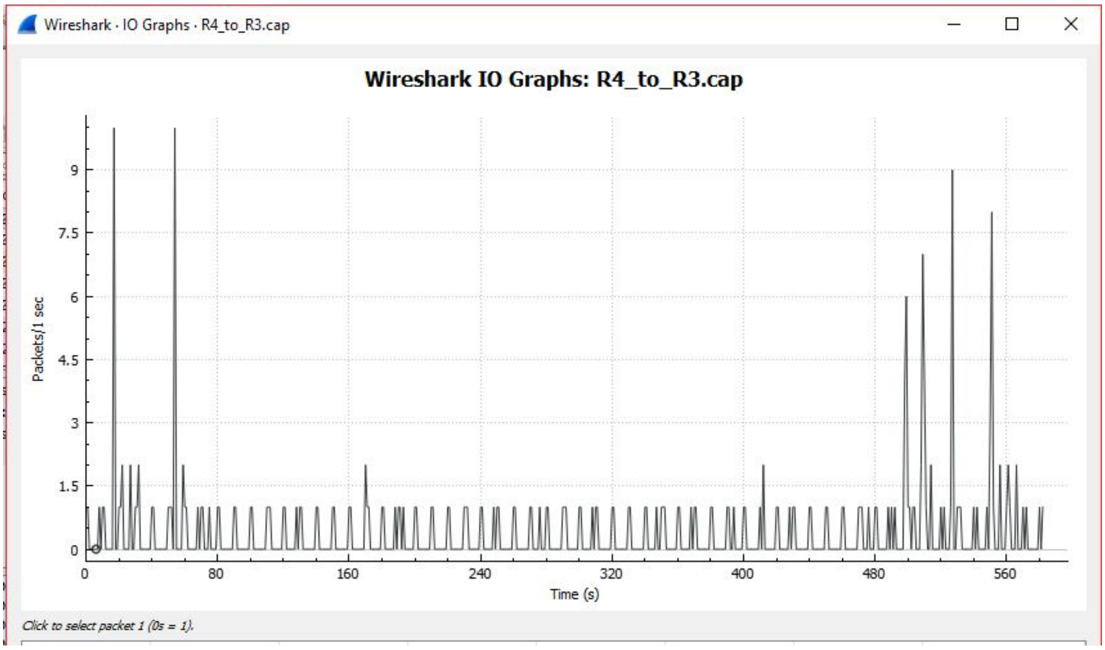

Wireshark · IO Graphs · R4_to_R3.cap
Wireshark IO Graphs: R4_to_R3.cap
Packets/1 sec
9
7.5
6
4.5
3
1.5
0
0
80
160
240
320
400
480
560
Time (s)
Click to select packet 1 (0s = 1).

Figure 4.13: DoS attack after using IPSec

4.4 Results and Discussions

By referring to the actual implementation of two scenarios of attacks against IPv6 network and the effects of the IPSec in each scenario the following is the outcome of the effectiveness and the weaknesses of IPSec under the security network.

In the first scenario: VPN IPSec achieved confidentiality and integrity, IPSec encapsulated and encrypted all package through existing IP networks from attackers who need to steal any secure information such as username or password, so IPSec here has high efficiency. In the second scenario: The non authentic packet attacks the network that comes from Kali attacker as a DoS attack. That attack might exhaust the bandwidth availability to the overlay VPN and as the result the VPN service gets affected. The IPSec here appears powerless against this type of attackers.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

Chapter Five

Conclusion and Recommendations

5.1 Conclusion

IPv6 presents both advantages as well as certain drawbacks from a security point of view; Features such as mandatory usage of IPSec come with overheads and performance issues. IPSec is designed to provide interoperable, high quality, cryptographically based security for IPv4 and IPv6; hosts can encrypt their traffic using IPSec in edge routers during transmission data. IPSec invigorates security to IPv6 by providing end to end communication security over the internet.

However, after testing the attacks effect of implementing IPSec in IPv6 network it is found that there are many threats which still remain issues in IPSec. Some of limitations of IPv6 Security are: the security protocol does not foster security to link local communication that uses Neighbor Discovery Protocol; in IPSec No traffic analysis protection for AH & ESP; No protection against all denial of service attack (DoS attacks difficult to prevent in most cases). So, it is very important to develop security mechanisms to face the huge amount of network using IPv6.

5.2 Recommendations

IPv6 Security and Internet migration is the emerging area of research today. Overall, the IPSec mechanism can’t solve all the security problems of IPv6, so a further research on the IPv6 security issues will be necessary for the performance of the network.

In future, a special attention should be put to avoid the threats arising from DoS attacks under IPv6 so as to make the network more secure. Adding some protocols or algorithms can help in avoiding these attacks.

REFERENCES

[1] Forouzan, A.B., “Data communications & networking” (sie), Tata McGraw-Hill Education, 2015.

[2] The Government of the Hong Kong Special Administrative Region,” IPv6 SECURITY”, May 2011.

[3] Atik, P. and Rick, “A Complete Guide on IPV6 Attack and Defense” 2012.

[4] Akram M. Radwan , “Using IPSec in IPv6 Security”,2016.

[5] Sharma, T. and Shiwani, S., “Statistical Results of IPSec in IPv6 Networks”, International Journal of Computer Applications 2013.

[6] ProCurve Networking , “IPv6 – The Next Generation of Networking”, 2006.

[7] Singh, R.K., Pundir, S. and Pilli, E.S., “IPv6 packet traceback: A survey”, International Journal of Computer Applications, 2016.

[8] McMillan, T., “CCNA Security Study Guide: Exam 210-260”, John Wiley & Sons, 2018.

[9] Gont, F. and Chown, T.,“Network Reconnaissance in IPv6 Networks”, 2016.

[10] Nazari, M. and Galla, L., “Denial of Service attack in IPv6 networks and counter measurements”, 2016.

[11] Rehman, S.U. and Manickam, S.,“Denial of Service Attack in IPv6 Duplicate Address Detection Process”, International Journal of Advanced Computer Science & Applications, 7, 2016.

[12] Hendriks, L., de Oliveira Schmidt, R., van Rijswijk-Deij, R. and Pras, A.,"On the potential of IPv6 open resolvers for DDoS attacks", March 2017.

[13] Johanna Ullrich, Katharina Krombholz, Heidelinde Hobel, Adrian Dabrowski and Edgar Weippl., "IPv6 Security: Attacks and Countermeasures in a Nutshell", 2015.

[14] Sotillo, S.,"IPv6 security issues", 2006.

[15] Dawood, H., "IPv6 security vulnerabilities", International Journal of Information Security Science, 1(4), pp.100-105, 2012.

[16] Chittimaneni, K., Kaeo, M. and Vyncke, E.,"Operational security considerations for IPv6 networks", 2017.

[17] Gao, J. and Chen, Y.,"Detecting DOS/DDOS Attacks Under IPv6",In Proceedings of the 2012 International Conference on Cybernetics and Informatics (pp. 847-855). Springer, New York, NY,2014.

[18] Sushma, V. and Venkateswarlu, T.," Design and Implementation of Secure Communication Between Two Branches of a Company Using IPSEC Based VPN (Virtual Private Network) Protocol", 2018.

[19] Saraswathi, S. and Yogesh, P.," Mitigating Strategy to Shield the VPN Service from DoS Attack", 2018.

[20] Schmalen, D., "Security Concept for VPN IPSec Site-to-Site Connections to Third Parties", California State University, Long Beach, 2018.

[21] Patani, N. and Patel, R.," A Mechanism for Prevention of Flooding based DDoS Attack", International Journal of Computational Intelligence Research, 2017.

[22] Gont, F. and Chown, T.," Network Reconnaissance in IPv6 Networks" 2017.

[23] Rehman, S.U. and Manickam, S., "Improved mechanism to prevent denial of service attack in IPv6 duplicate address detection process", 2017.

[24] Patani, N. and Patel, R., "A Mechanism for Prevention of Flooding based DDoS Attack", International Journal of Computational Intelligence Research, 13(1), pp.101-111, 2017.

[25] Hermann, S. and Fabian, B.,"A comparison of Internet Protocol (IPv6) security guidelines", Future Internet, 6(1), pp.1-60, 2014.

APPENDICES

APPENDIX A

Configuration of Router R1 in Gns3

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
IPv6 unicast-routing
!
multilink bundle-name authenticated
!
!
```

```
archive
 log config
  hidekeys
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key ipsecvpn address IPv6 2002::2/64
crypto isakmp profile 3des
   keyring default
   match identity address IPv6 2002::2/64
!
crypto ipsec transform-set IPv6_tran esp-3des esp-sha-hmac
!
crypto ipsec profile IPv6_ipsec_pro
 set transform-set IPv6_tran
!

interface Tunnel1
 no ip address
 IPv6 address 2012::1/64
 IPv6 enable
 tunnel source 2001::1
 tunnel destination 2002::2
 tunnel mode ipsec IPv6
 tunnel protection ipsec profile IPv6_ipsec_pro
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 IPv6 address 2001::1/64
 IPv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 IPv6 address FC00::1/64
 IPv6 enable
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
IPv6 route ::/0 2001::2
```

```
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Configuration of Router R2im Gns3

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
```

```
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
IPv6 unicast-routing
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 IPv6 address 2001::2/64
 IPv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 IPv6 address 3001::1/64
 IPv6 enable
```

```
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
IPv6 route 2002::/64 3001::2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Configuration of Router R3 in Gns3

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
IPv6 unicast-routing
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 IPv6 address 3001::2/64
 IPv6 enable
```

```
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 IPv6 address 2002::1/64
 IPv6 enable
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
IPv6 route 2001::/64 3001::1
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
End
```

Configuration of Router R4 in Gns3

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
IPv6 unicast-routing
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
```

```
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key ipsecvpn address IPv6 2001::1/64
crypto isakmp profile 3des
   keyring default
   match identity address IPv6 2001::1/64
!
crypto ipsec transform-set IPv6_tran esp-3des esp-sha-hmac
!
crypto ipsec profile IPv6_ipsec_pro
 set transform-set IPv6_tran
!
interface Tunnel1
 no ip address
 IPv6 address 2012::2/64
 IPv6 enable
 tunnel source 2002::2
 tunnel destination 2001::1
 tunnel mode ipsec IPv6
 tunnel protection ipsec profile IPv6_ipsec_pro
!
interface FastEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
 IPv6 address 2002::2/64
 IPv6 enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
!
IPv6 route ::/0 2002::1
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4

!

End
```

APPENDIX B

Installation of THC IPv6 Attack Toolkit in Kali

```
$ cd ~/src/

$ wget http://www.thc.org/releases/thc-IPv6-1.8.tar.gz

$ tar xzvf thc-IPv6-1.8.tar.gz

$ cd thc-IPv6-1.8/

$ make

$ sudo make install
```

Attack syntax:

```
kali@root# denial6 eth0 fc0::1
```