UNIVERSITI TEKNOLOGI MARA

IPV6 MALICIOUS ROUTER DETECTION AND RECOVERY

AHMAD SAIFULLAH BIN AHMAD TARMIZE

Dissertation submitted in partial fulfilment of the requirements for the degree of
Master of Science in Computer Networking

Faculty of Computer and Mathematical Sciences

January 2015

ABSTRACT

The increasing number of devices in the Internet led an increasing demand of IP address for every device. IPv4 cannot solve this problem requiring IPv6 protocol to be introduced. With IPv6 protocol, it includes Neighbour Discovery Protocol (NDP) for automatic configuration IP address thus makes it easy to use compare to IPv4. Although NDP simplify the configuration process of IPv6, there are few downsides to NDP protocol which could lead network to fall for certain vulnerabilities such as Man in the Middle (MitM), Denial of Service (DoS) and also spoofing problem. One of common problem is malicious router attack which announces itself as default router in the network to run MitM. Previously, there are multiple mechanisms to encounter NDP problem such as SEcure Neighbour Discovery (SEND) and RA Guard/DHCPv6 Guard. However, this technique falls to resource exhaustion, bandwidth consumption, added overhead and expensive hardware. This paper try to design new technique of detecting malicious router attack happen in NDP and recover network from the attack the simple way.

ACKNOWLEDGEMENT

Firstly, I wish to thank God for giving me the opportunity to embark on my master and for completing this long and challenging journey successfully. My gratitude and thanks go to my supervisor Dr. Adnan Ahmad. Thank you for the support, patience and ideas in assisting me with this research project. I also would like to express my gratitude to all my colleagues and friends of the Master of Science in Computer Networking, especially Mr. Hariz Bin Naim for providing assistance and support.

My appreciation goes to the Element14 crew members who provided the facilities and assistance during project development. Special thanks to my colleagues and friends for helping me with this project.

Finally, this thesis is dedicated to my friends and my siblings for their encouragement and motivations during the period of study in UiTM Shah Alam. Last but not least to my very dear father and mother, Ahmad Tarmize bin Abdul Razak and Fadzilah binti Mohd. Din for the vision and determination to educate me. The piece of victory is dedicated to both of you. Alhamdulillah.

TABLE OF CONTENTS

Page

CONFIRMATION BY PANEL OF EXAMINERS **II**

AUTHOR DECLARATION **III**

ABSTRACT **IV**

ACKNOWLEDGEMENT **V**

TABLE OF CONTENTS **VI**

LIST OF TABLES **IX**

LIST OF FIGURES **X**

CHAPTER ONE: INTRODUCTION **1**

1.1. Research Background 1

1.2. Problem Statement 3

1.3. Research Objectives 4

1.4. Research Scope 4

1.5. Significance 5

CHAPTER TWO: LITERATURE REVIEW **6**

2.1. Introduction 6

2.2. IPv4 Overview 6

2.2.1. IPv4 Address Space Exhaustion Mitigation Technique 8

2.2.2. Network Address Translation (NAT) 9

2.2.3. Private Network Addressing 11

2.2.4. Subnetting 11

2.2.5. Named Based Virtual Hosting 12

2.3. IPv6 Overview 13

2.4. Brief Differences Between IPv4 And IPv6 Header 16

2.4.1. IPv6 Header 16

2.5. Python And Scapy 18

2.6. IPv4 And IPv6 Local Network Configuration 19

CHAPTER ONE

INTRODUCTION

1.1. RESEARCH BACKGROUND

Exhaustion of IPv4 addresses has triggered quite a concern for Internet organization around the world. The IPv4 protocol address is made up of 32 bit and it has an address space of 2^{32}. This address protocol can supports up to 4 billion hosts which seems reasonable during its inception. The IPv4 protocol design satisfies the address needed for the computer at that time (Barbhuiya, Biswas, & Nandi, 2011). Exhaustion of address space problem in IPv4 address is already expected and there are multiple efforts to address this problem. It includes the introduction of Network Address Translation (NAT) to provide way of multiple computers share same global IP address, the use of private network addressing, subnetting, and the establishment of name based virtual hosting. Although there are multiple technique to reduce the exhaustion problem, there still needs for mechanism or protocol to support the increasing number of device/gadget in the world.

IPv6 has been introduced to ensure that the huge and growing Internet map can be supported by the standard organization Internet Assigned Numbers Authority (IANA). The development work on IPv6 started in around 1998 (IETF, Internet Protocol, Version 6 (IPv6) Specification (RFC2460), 1998). IPv6 provided many benefits especially the bigger and expandable IP address which can support up to 128-bit address to support all the host address of computer. The fact that IPv6 use 128 bit address, create a possibility of addressing approximately 340 trillion trillion trillion of hosts. This means the Internet may address lots more thing or devices, which may include lamp, fan, television, refrigerator and even a window.

The advantages of IPv6 address is the auto-configuration exist inside its protocol (Narten, 1999). Auto-configuration in IPv6 protocol come in handy since it is possible to configure IP address automatically based on Neighbour Discovery