Universiti Teknologi MARA

ENCRYPTION METHOD OF IPV6 NETWORK DISCOVERY PROTOCOLS SECURITY

Ummi Syahirah binti Mohd Daud

Thesis submitted in fulfillment of the requirements for

Bachelor of Science (Hons) Data Communications and Networking

Faculty of Computer and Mathematical Sciences

January 2019

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, praise and thanks to Allah SWT, for all the graces and blessings and also Selawat and Salam to the Prophet Rasulullah SAW, hopefully His syafa‟at will be abundant in days later.

First of all, I would like to express my highest gratitude to my supervisor, Pn Shapina bt Hj. Abdullah for her guidance, advice and support in order to complete this final year project. I appreciate every single “walk” she taught me.

Thanks also to all the lecturers in the course of Bachelor of Science (Hons) Networking & Data Communications at UiTM Shah Alam for their patience and kind advice during the process of completing the project.

Lastly, thanks you so much to all those who supporting me in any way during the completions of this proposal report by discussing, sharing or exchanging ideas and everyone who are directly or indirectly involved in writing this report.

Thank you so much.

ABSTRACT

Nowadays, there are many devices that have connection with internet and this has led to an increasing usage of IP address. IPv4 have slowly reached to an end which led to introduction of IPv6 protocol. IPv6 protocol include Neighbor Discovery Protocol (NDP) for configuration IP address that make it easier to use compare to IPv4. Even though, IPv6 have NDP but still there are few drawbacks to NDP protocol which can lead to network failure. The downside of NDP protocol can make IPv6 fall for some vulnerabilities such as Man in The Middle (MiTM), Denial of Service (DoS) and other problems. For example, a malicious router will claimed itself as a default router in network to run MiTM. Before this, there are many protocols to prevent NDP problem such as RA Guard/DHCPv6 Guard and Secure Neighbor Discovery (SEND). However, these protocol fail to protect NDP. This project is to analyse the encryption method used in IPv6 network.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background Study

Nowadays, internet has become more powerful. We tend to use internet to do our works and in our daily life. Most of things in this world now have connection with internet and have IP address. Due to this, number of available IPv4 has decreasing and almost fully use. IPv4 reduction has generated a concern for Internet organization worldwide. The IPv4 protocol address consists of 32 bit and address space of 2^{32} . This address protocol can support only up to 4 billion hosts. The IPv4 protocol design to fulfil address needed for computer only at that time (Barbhuiya, Biswas & Nandi, 2011). Reduction of address space problem in IPV4 address is acknowledged and many methods to cater this problem. One of the method are the introduction of Network Address Translation (NAT) to support way of multiple computer share same IP address, the use of private network addressing, subnetting, and the establishment of name based virtual hosting. Even there are many methods to reduce the IPv4 reduction problem, there still needs for protocol to support the requesting of IP address that getting more by days.

The IPv6 is invented to replace IPv4 in future. The invention of IPv6 to guarantee the standard organization Internet Assigned Number Authority (IANA) can fully support the growing of Internet usage. The development work on IPv6 has started around 1998 (IETF, Internet Protocol, Version 6 (IPv6) Specification (RFC2460)). IPv6 give many benefits especially the larger and extendible IP address which can support up to 128-bit address that can support all the host address of computer. The IPv6 has create a chance of addressing roughly 3.4 10^{38} of hosts. This means the Internet can address lots more thing, which include lamp, fan,