PREVENTION MECHANISM AGAINST DENIAL OF SERVICE ATTACK ON DUPLICATE ADDRESS DETECTION PROCESS IN IPV6 LINK-LOCAL NETWORKS

AHMED KHALLEL IBRAHIM AL-ANI

UNIVERSITI SAINS MALAYSIA

2020

PREVENTION MECHANISM AGAINST DENIAL OF SERVICE ATTACK ON DUPLICATE ADDRESS DETECTION PROCESS IN IPV6 LINK-LOCAL NETWORKS

by

AHMED KHALLEL IBRAHIM AL-ANI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

February 2020

ACKNOWLEDGEMENT

I thank all who in one way or another contributed in the completion of this thesis. First, I give thanks to “Allah” for protection and ability to do this research.

I would like to give deep thanks to the lecturers and collegemates at the National Advanced IPv6 Center, the librarians, and other workers of the Center for their kind help during my PhD journey, without you all, I will not be able to achieve this research.

My special and heartily thanks to my research supervisor, Dr. Mohammed Anbar, and co-supervisors Dr. Selvakumar Manickam and Dr. Yu-Beng Leau. Without their assistance and dedicated involvement in every step throughout the process, this research would have never been accomplished. I would like to thank you very much for your support and understanding over these past three years.

Getting through my thesis required more than academic support, and I have many, many people to thank for listening to and, at times, having to tolerate me over the past three years. I cannot begin to express my gratitude and appreciation for their friendship. For many memorable evenings out and in, I must thank; Dr. Samar Al-Saleem, Dr. Hamza Zreaqat and Dr. Abdullah Shirari have been unwavering in their personal and professional support during the time I spent at the USM university.

Most importantly, none of this could have happened without my family. My life-coach “My Father” Prof. Khallel I. Al-Ani, I really do not have any word to explain my thankful for your assist to make me where I am now, without you Dad I am literally nothing. My lightness in this life “My Mother” who encouraged me and prayed for me throughout the time of my research. And lastly, thanks to my brothers Dr. Ayman Al-Ani and Fahad Al-Ani and my lovely three sisters. I love you all…

Lastly, I would like to express my thanks to the unknow soldier who supports me without notice. May the Almighty God richly bless all of you. I dedicate this work to all of you.

Ahmed K. Al-Ani, Penang Malaysia, 2020.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

AR	Router Access
ARP	Address Resolution Protocol
AT	Attacker Host
AT	Attacker
BC	Bandwidth Consumption
BW	Bandwidth
CGA	Cryptographically Generated Address
CPA	Certificate Path Advertisement
CPS	Certificate Path Solicitation
CPU	Central Processing Unit
CY	Cycles
DAD	Duplicate Address Detection
DAD-h	Duplicate Address Detection-hash function
DAD-match	Duplicate Address Detection – match
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
EH	Existing Host
EtR	Ending Time for Generating Message at Receiver Host
Etr	End Time for Verifing Message at Receiver Host
EtRNA	Ending Time for Generating NA Message at Receiver Host
EtRNS	Ending Time for Generating NS Message at Receiver Host
EtS	Ending Time for Generating Message at Sender Host

EtSNA	Ending Time for Generating NA Message at Sender Host
EtSNS	Ending Time for Generating NS Message at Sender Host
EUI-64	Extended Unique Identifier – 64
F	DAD times failed
FR	Frequency
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IID	Interface Identifier
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
LLC	Link-local Communication
MAC	Media Access Control
MAC	Massage Authentication Code
MG	Message
MINTM	Man in the Middle
MLD	Multicast Listener Discovery
MZ	Message Size
MZoverhead	Message Size Overhead
N	Number of DAD times

NA	Neighbor Advertisement
NC	Number of Core
NDP	Neighbor Discovery Protocol
NDPmon	Neighbor Discovery Protocol monitor
NH	New Host
NIC	Network Interface Card
NM	Number of the message
NS	Neighbor Solicitation
NUD	Neighbor Unreachability Detection
OUI	Organizationally Unique Identifier
P	Probability of Collision Attack
PT	Processing Time
PTR	Processing Time at Receiver Host
PTRNA	Processing Time for Generating NA Message at Receiver Host
PTRNS	Processing Time for Generating NS Message at Receiver Host
PTs	Processing Time at Sender Host
PTSNA	Processing Time for Generating NA Message at Sender Host
PTSNS	Processing Time for Generating NS Message at Sender Host
RA	Router Advertisement
RM	Redirect Message
RS	Router Solicitation
RSA	Rivest-Shamir-Adleman cryptosystem
SA	Security Associations
SASS	Simple Source Addressing Scheme
SAVA	Source Address Validation Architecture

SAVI	Source Address Validation Improvement
SD	Standard Deviation
SDN	Software – Defined Networking
Secure-DAD	Secure – Duplicate Address Detection
SeND	Secure Neighbor Discovery
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
SHA-3	Secure Hash Algorithm 3
SIEM	Security Information and Event Management
SLAAC	Stateless Address Auto-configuration
SNMA	Solicited Node Address Group
StR	Starting Time for Generating Message at Receiver Host
Str	Start Time for Verifing Message at Receiver Host
StRNA	Starting Time for Generating NA Message at Receiver Host
StRNS	Starting Time for Generating NS Message at Receiver Host
StS	Starting Time for Generating Message at Sender Host
StSNA	Starting Time for Generating NA Message at Sender Host
StSNS	Starting Time for Generating NS Message at Sender Host
SW	Switch
T	Time
TCP	Transmission Control Protocol
TDAD	Total of Processing Time During DAD Process
THC	The Hacker Choice
Trust-ND	Trust – Neighbor Discovery
UND	Unreachable Neighbor Detection

$\boldsymbol{PTS}$	Processing Time at Sender Host

MEKANISME PENCEGAHAN SERANGAN NAFI KHIDMAT TERHADAP PROSES PENGESANAN ALAMAT PENDUA DALAM RANGKAIAN PAUTAN-SETEMPAT IPV6

ABSTRAK

Protokol Internet versi 6 (IPv6) merupakan versi terkini IP yang bertujuan membolehkan penggunaan ratusan ribu alamat IP yang unik untuk alatan-alatan dalam rangkaian yang sama. Keunikan suatu alamat IP dapat dipastikan dengan menggunakan proses pengesanan alamat pendua (DAD), iaitu satu prosedur teras dalam rangkaian IPv6 yang memastikan alamat-alamat IP dalam pautan yang sama tidak bertindih antara satu sama lain. Oleh yang demikian, setiap nod mesti melaksanakan proses ini sebelum menyertai rangkaian IPv6. Untuk melaksanakan proses DAD, nod IPv6 menggunakan dua mesej protokol penemuan jiran (NDP), iaitu mesej *Neighbor Solicitation* (NS) dan mesej *Neighbor Advertisement* (NA), untuk berkomunikasi antara satu sama lain dalam rangkaian pautan-setempat IPv6. Walau bagaimanapun, mesej NDP mempunyai reka bentuk yang tidak selamat dan tiada mekanisma penentusahan yang menghalang nod-nod daripada memeriksa sama ada mesej-mesej tersebut datang dari sumber nod yang sah atau tidak. Oleh itu, mana-mana nod pada pautan yang sama boleh memanipulasi mesej NS atau NA dan melancarkan serangan nafi khidmat (DoS) untuk menghalang nod IPv6 yang sah daripada mengkonfigurasi alamat IPnya. Oleh yang demikian, tesis ini bertujuan memperkenalkan satu mekanisme pencegahan yang dinamai Padanan-Pengesanan Alamat Pendua (DAD-match) yang mengandungi tiga tahap, iaitu, (i) tahap penjanaan alamat IP tentatif, yang bertujuan menyembunyikan alamat IP tentatif dengan menggunakan fungsi cincangan kriptografi (*cryptographic hash function*), (ii) tahap menjamin keselamatan mesej NS dan NA, dengan tujuan menjamin keselamatan masej NS dan NA dengan menggunakan opsyen eksperimental NDP, dan (iii) tahap menghalang DoS pada DAD, yang bertujuan menghalang serangan DoS semasa proses DAD dengan mereka bentuk satu mekanisme berasas peraturan. DAD-match yang dicadangkan telah dinilai pada aspek masa pemprosesan, penggunaan lebar jalur dan kadar kejayaan menghalang serangan DoS dengan menggunakan senario-senario berbeza, dan prestasinya dibandingkan dengan mekanisme-mekanisme sedia ada, termasuk DAD-piawai, SeND, Trust-ND dan HSEC-Target-DAD. Keputusan menunjukkan DAD-match berjaya mengurangkan masa pemprosesan berbanding SeND, Trust-ND, dan HSEC-Target-DAD, masing-masing sekitar 95.5%%, 28.58% and dan 84.93%. Dalam aspek penggunaan lebar jalur, DAD-match berupaya menjimatkan penggunaan lebar jalur berbanding ketiga-tiga mekanisme di atas, masing-masing sehingga sekitar 427%, 37%, dan 595%. Semasa eksperimen dijalankan, DAD-piawai, Trust-ND dan HSEC-Target-DAD tidak berupaya menjamin keselamatan proses DAD daripada serangan DoS, manakala SeND pula terdedah kepada serangan kebanjiran. Dalam pada itu, hanya DAD-match yang membolehkan nod-nod IPv6 untuk menentusah mesej-mesej yang diterima dan menghalang serangan DoS semasa proses DAD dalam rangkaian pautan-setempat IPv6.

PREVENTION MECHANISM AGAINST DENIAL OF SERVICE ATTACK ON DUPLICATE ADDRESS DETECTION PROCESS IN IPV6 LINK-LOCAL NETWORKS

ABSTRACT

Internet Protocol version 6 (IPv6) is the most recent IP version that aims to accommodate hundreds of thousands of unique IP addresses for devices in the same link-local network. The uniqueness of an IP address can be guaranteed by performing the Duplicate Address Detection (DAD) process, a core procedure in an IPv6 network that ensures that IP addresses in the same link do not conflict with one another. Therefore, any node must undergo this process before joining an IPv6 network. To perform the DAD process, IPv6 nodes use two Neighbor Discovery Protocol (NDP) messages, namely, *Neighbor Solicitation* (NS) and *Neighbor Advertisement* (NA) messages, to communicate with one another in the same IPv6 link-local network. However, NDP messages have non-secure designs and lack any verification mechanism, thereby preventing nodes from checking whether these messages are coming from a legitimate or illegitimate node. Therefore, any node in the same link can manipulate NS or NA messages and then launch a Denial of Service (DoS) attack to prevent the legitimate IPv6 node from configuring its IP address. Thus, this thesis aims to introduce a prevention mechanism called DAD-match that comprises three stages, namely, (i) the tentative IP address generation stage, which aims to hide a tentative IP address by using a (*cryptographic hash function*), (ii) the secure NS and NA messages stage, which aims to secure NS and NA messages by using the NDP experimental option and (iii) the DoS on DAD prevention stage, which aims to prevent a DoS attack during the DAD process by designing a rule-based mechanism. The proposed DAD-match mechanism is evaluated in terms of its processing time, bandwidth consumption and DoS prevention success rate by using different scenarios, and its performance is compared with existing mechanisms, including Standard-DAD, SeND, Trust-ND and HSEC-Target-DAD. The results show that DAD-match reduces the processing time by approximately 95.5%, 28.58% and 84.93% compared with SeND, Trust-ND and HSEC-Target-DAD, respectively. In terms of bandwidth consumption, DAD-match can reduce the bandwidth consumption by approximately 427%, 37%, and 595% compared with the above three mechanisms, respectively. In terms of DoS prevention success rate, the experiments showed that Standard-DAD, Trust-ND and HSEC-Target-DAD are unable to secure the DAD process from DoS attacks, whilst SeND is vulnerable to flooding attacks. Meanwhile, DAD-match allows IPv6 nodes to verify the incoming message, discard the fake message before further processing and prevent a DoS attack during the DAD process in an IPv6 link-local network.

CHAPTER 1

INTRODUCTION

This chapter introduces the research topic and the key aspects related to the Internet Protocol version 6 (IPv6) link-local network in nine sections. Section 1.1 presents an overview of the IPv6 network and its security issues and justifies the need for improving its design. Sections 1.2 and 1.3 discuss the Denial of Service (DoS) attacks against the Duplicate Address Detection (DAD) process in an IPv6 link-local network. Sections 1.4 to 1.6 present the problem statement, research objectives and scope of the thesis, respectively. Section 1.7 discusses the contribution of this thesis, that is, to propose a prevention mechanism for securing the DAD process in an IPv6 link-local network. Section 1.8 explains the steps for securing the DAD process. Section 1.9 presents the organisation of this thesis.

1.1 Overview

The worldwide system of interconnected computer networks, known as ‘the Internet’, has invaded nearly all aspects of our daily life to the extent that this technology has become a basic need for human beings similar to water and electricity (Fontaine–Delaruelle et al., 2015; Sánchez–Valle, Abad, & Llorente–Barroso, 2017). The Internet is an assembly of private, public, academic, business and government networks with local or global scopes that are linked together by various electronic and wireless technologies in addition to optical networking techniques. The Internet also provides a massive amount of information resources and services. However, given their large number, Internet users and their devices, which are connected to one another through Internet Protocol version 4 (IPv4), have exhausted the resources of this protocol (Postel et al., 1981). The IPv4 network also faces some security issues as mentioned in previous studies (Ali, 2012; Groat et al. 2011).

To address this exhaustion problem, the Internet Assigned Numbers Authority has proposed the use of IPv6 for allocating different addresses (Deering, 1998). This new protocol is also predicted to replace IPv4 in the future. Statistics from Google reveal that the proportion of their users who have accessed their services via IPv6 has exceeded 26% of their total users in January 2019 (Figure 1.1; Google, 2019).

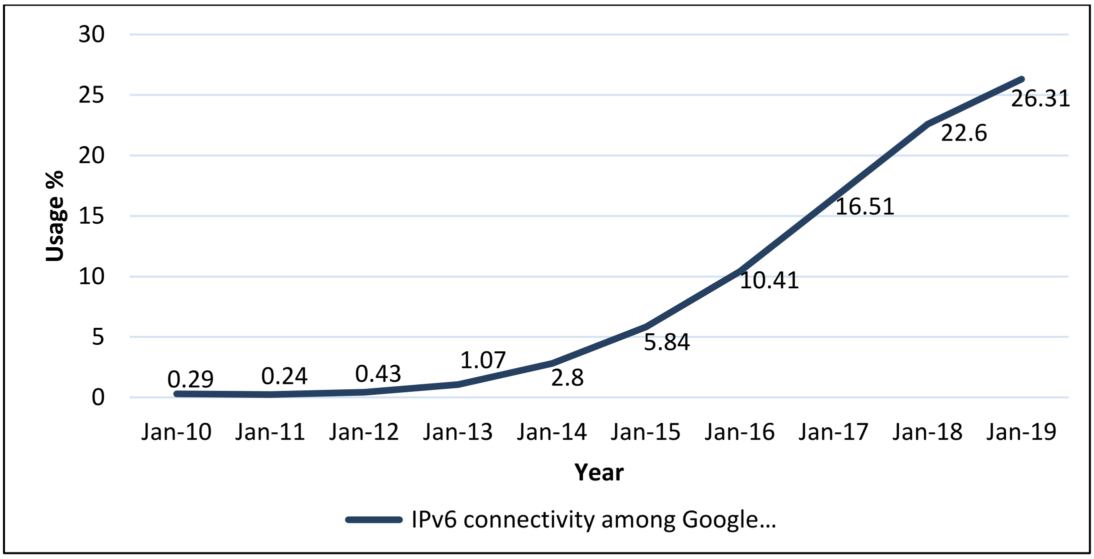

Figure 1.1 Users Accessing Google Services via IPv6 in 2019

Given the rapid exhaustion and limitations of IPv4 addresses, various organisations have started to deploy IPv6 and adopted security policies and measures to address the security issues being faced by this network (Najjar & El-Taj, 2015). IPv6 also adopts an innovative specification called Internet Protocol security (IPsec) to achieve secure connections as specified in Request For Comments (RFC) 4301 (Seo & Kent, 2005). However, the applicability of this protocol is restricted by its manual configuration. In addition, it does not support multicasting (Jankiewicz et al. 2011).

Unlike IPv4, IPv6 attempts to enhance link-local network security by introducing the novel Neighbor Discovery Protocol (NDP) as specified in RFC 4861 (Narten et al. 2007). NDP has many processes, including Neighbor Unreachability Detection (NUD) and DAD, whereas its design presumes that the Local Area Network (LAN) comprises trusted nodes. In this case, every node inside LAN is trusted by the NDP, thereby making the network vulnerable to various types of attacks.

The implementation of IPv6 makes communication systems vulnerable to different types of attacks due to a missing authentication step. Through NDP, the connected devices can generate and configure their IP addresses and communicate with more devices regardless of the authentication process adopted in the network. Furthermore, many operating systems are equipped with IPv6 by default. Therefore, LANs are prone to IPv6 attacks, including the man-in-the-middle, DoS-on-DAD, smurf and flooding attacks.

As previously mentioned, IPv6 has novel specifications and functionalities compared with IPv4; accordingly, this network faces new types of attacks in addition to those attacks it has inherited from IPv4. In addition, some types of attacks on IPv4 can be prevented by disabling the Internet Control Messages Protocol version 4 (ICMPv4). Meanwhile, the Internet Control Message Protocol version 6 (ICMPv6) (Conta & Gupta, 2006) for IPv6 plays a crucial role in the IPv6 network, and disabling such protocol will only result in the disconnectivity of the network. ICMPv6 messages also have non-secure designs, thereby allowing malicious hosts to modify these messages and perform specific types of attacks, such as a DoS attack, on a particular host.

1.2 Denial of Service Attacks

A DoS attack poses one of the most substantial threats for IPv4 and IPv6 networks (Raghavan & Dawson, 2011). Recent studies show that DoS attacks are extensive and pose a serious security threat for IPv6. Approximately 68% of the threats against IPv6 are caused by DoS attacks, with the other threats being caused by code execution, bypass, buffer overflow, port scan and privilege escalation (Ard, 2012; Elejla et al. 2016) as shown in Figure 1.2.

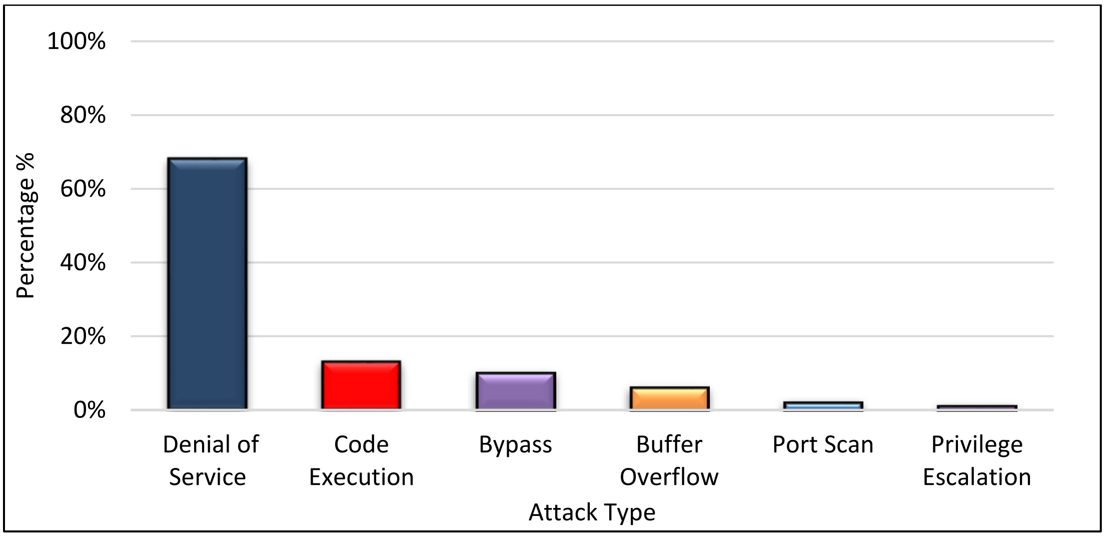

Figure 1.2 IPv6 Vulnerability Classes (Ard, 2012)

DoS attacks consume the computational resources of the target host and the network bandwidth, thereby preventing legitimate users from accessing the services provided by this host. These attacks are induced by the vulnerability of IPv6 network protocols, influence the performance of the target host and downgrade the performance of the entire network, which in turn may disable its hosts from processing massive amounts of network traffic.

Denial of Service Attacks in an IPv6 Network: DoS attacks in IPv6 networks generally take place in either the application layer or the network layer, of which the latter can be further subdivided into the gateway (router) and the local link as illustrated in Figure 1.3 (Li et al., 2011). In IPv6, the NDP considers the protocol of an IPv6 link-local network that involves several important processes, including DAD. The NDP processes in the link-layer are in charge of establishing communication amongst the hosts in the same network as specified in RFC 4861 (Narten et al., 2007).

To establish communication with its IPv6 neighbors in the same local link, an IPv6 host uses five ICMPv6 messages (Conta & Gupta, 2006). However, previous studies reveal that these messages (including five NDP messages) are exposed to DoS attacks during NDP processes, including DAD (Caicedo et al., 2009; Elejla et al., 2016; Nikander et al., 2004; Saad et al., 2013). DAD is an important process in NDP that ensures that all IPv6 nodes in the same link-local network have a unique IP address (Thomson, 2007). This process is explained in detail in Section 1.3.

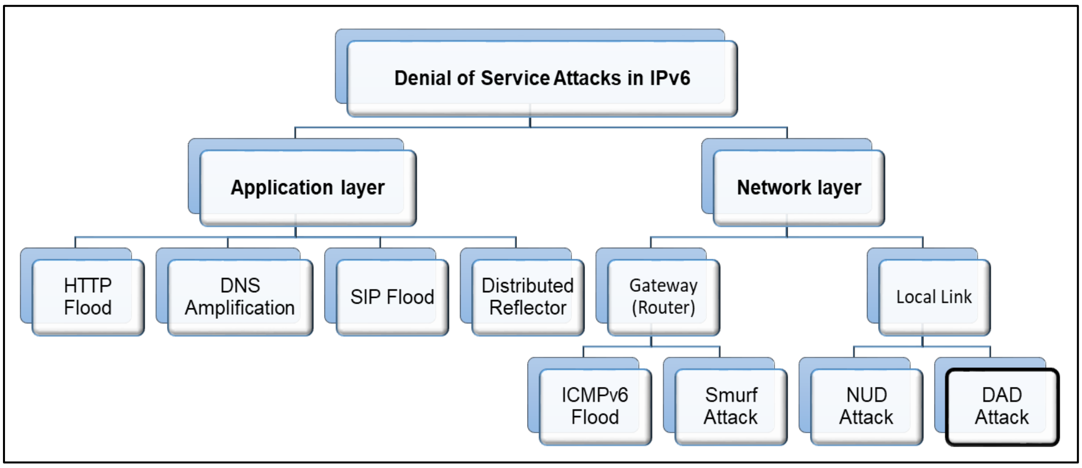

Figure 1.3 Types of Denial of Service (DoS) Attacks in IPv6 Network

Any host located in the same link can be an attacker and join/disturb any NDP process to launch a DoS attack. Given that the designs of ICMPv6 messages are generally not secure, an attacker in the same link can forge these messages and perform a DoS attack on NDP processes. An attacker may perform a DoS attack on an IPv6 network in different ways, such as by sending an extreme number of forged ICMPv6 messages to a specific host in the same link. In this scenario, the target host is unable to process these forged messages, thereby rendering this host out of service (Rafiee & Meinel, 2013; Rehman & Manickam, 2017). This type of attack is referred to as a flooding attack.

1.3 DAD Process in an IPv6 Link-Local Network and Its Security Issues

Every IPv6 host performs the DAD process before assigning IPv6 addresses to ensure that none of the hosts in the same link-local network shares the same IP address (Moore, 2006; Praptodiyono et al., 2016; Yao et al., 2010). Indeed, the IP conflict is low because of address space immensity. However, such will not be the case in the future as the number of mobile devices exponentially increase due to the emergence of novel technologies, including Internet of Things (IoT) and cloud computing (Bapat & Nimbhorkar, 2016; Li et al., 2015).

Two types of NDP messages, namely, Neighbor Solicitation (NS) and Neighbor Advertisement (NA), are used during the DAD process in an IPv6 link-local network. When the target host intends to join an IPv6 local-link or in case a host in the same link generates a new IP address as a tentative IP address, the uniqueness of this generated address needs to be verified. To this end, the target host multicasts a number of NS messages to all hosts in the same link. In case the tentative address has already been assigned by another host in the same link, an NA message should be sent by the existing host as a reply to an NS message indicating that the generated tentative IP address is not unique. Afterwards, the target host must generate a new tentative IP address and reperform the DAD process to verify the uniqueness of this generated address until NA messages are no longer received.

The DAD process presumes that all neighbor hosts in an IPv6 link-local network are reliable. Therefore, upon receiving an NA message from other hosts during the address verification process, the target host can act accordingly regardless of the validity of this message. In this scenario, a malicious host may respond to an NS message by sending a fake NA message that claims that the generated tentative IP address has already been assigned; doing so will prevent IPv6 hosts from configuring this unique IP address. Therefore, these hosts are unable to join the IPv6 network and communicate with the other hosts in the network. This type of attack is referred to as a DoS-on-DAD attack, which prevents hosts from configuring IP addresses in an IPv6 link-local network as revealed in previous studies (Ahmed et al., 2017; Al-Ani et al., 2018; Rehman & Manickam, 2017). Figure 1.4 illustrates a DoS attack on the DAD process in an IPv6 link-local network.

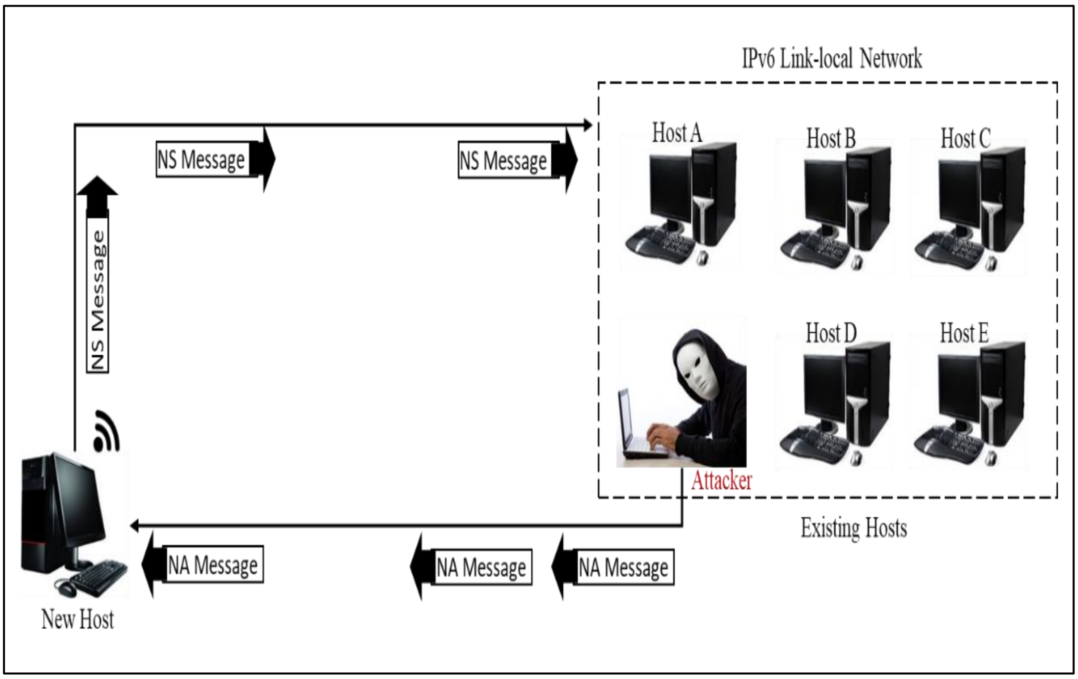

Figure 1.4 DoS Attack on DAD Process in IPv6 Link-local Network

1.4 Research Problem

To ensure the uniqueness of a tentative IP address in an IPv6 link-local network, each host performs the DAD process by using NS and NA messages (Moore, 2006; Rehman & Manickam, 2015; Yao et al., 2010). These NDP messages are not secured by default, and any attacker can benefit from such non-secure design by manipulating NS or NA messages during the DAD process. Attackers can also interrupt and negatively affect the verification process by sending forged response messages when a DAD process is being conducted by a target host. The tentative IP address represents the important information in the DAD process in an IPv6 link-local network. According to the Standard-DAD mechanism, this tentative IP address is multicast by the target host through NS messages in plaintext. Therefore, all the nodes, including the attacker, will receive NS messages. Given that the attacker can obtain the tentative IP address, he can claim that such tentative IP address is not unique by sending fake NA messages that prevent a new node from joining the IPv6 network.

Thus, Standard-DAD mechanism used in an IPv6 link-local network is vulnerable to DoS-on-DAD attacks throughout the verification process whilst the host is configuring the IP address as revealed in previous studies (Rehman & Manickam, 2017; Elejla et al., 2016; AlSa'deh & Meinel, 2012; Rafiee & Meinel, 2013). Accordingly, other mechanisms have been proposed to deal with the DoS-on-DAD attacks against the DAD process in an IPv6 link-local network. The most commonly used mechanisms include Secure Neighbor Discovery (SeND), Trust-Neighbor Discovery (Trust-ND) and Hash Secure Target Address DAD (HSEC-target-DAD). However, these mechanisms either require an extensive computation which can lead to certain types of DoS attacks such as flooding attacks, or suffer from a hash collision attack or weak security due to their design.

The SeND mechanism is introduced by the Internet Engineering Task Force (IETF) and recommended by RFC 3971 (Jari Arkko et al., 2005) to secure the NDP processes in an IPv6 link-local network. Previous studies (Praptodiyono et al., 2016; Najjar et al., 2015; Rafiee & Meinel, 2013; Rehman & Manickam, 2017) argued that SeND is inefficient due to its extensive computation requirements (which consume CPU and memory capacity), high processing time and large bandwidth consumption, all of which can lead to a DoS attack throughout the DAD process in an IPv6 link-local network.

The Trust-ND mechanism aims to address the extensive computation requirements of the SeND mechanism (Praptodiyono et al., 2016). Trust-ND utilises the SHA-1 hashing algorithm to verify the NS and NA messages throughout the DAD process (Polk et al., 2011). However, previous studies (Andreeva et al., 2015; Bhargavan & Leurent, 2016) claimed that SHA-1 is vulnerable to hash collision attacks. Moreover, given its design, Trust-ND is vulnerable to DoS attacks against the DAD process in an IPv6 link-local network.

A recent study conducted in 2018 (Ksimi et al., 2018) proposed a new mechanism called HSEC-Target-DAD that aims to secure the target address (i.e. the ‘tentative IP address’) by utilising the hybrid cryptography method of SHA-512 and RSA in verifying NS and NA messages during the DAD process. However, previous studies (Goswami et al., 2012; Mustafi et al., 2016) claimed that despite its tight security level, the RSA algorithm is very slow, particularly in key generation, thereby extending the time for generating NS and NA messages. In addition, given the size of messages, HSEC-Target-DAD consumes a high amount of bandwidth during the DAD process. Further, extracting only 64 bits of 512-bit hash values also increases the probability for a hash collision attack to occur. Therefore, the HSEC-Target-DAD mechanism is unable to secure the DAD process in an IPv6 link-local network.

Given the aforementioned disadvantages, a prevention mechanism that can secure the DAD process in an IPv6 link-local network and shows promising performance in terms of time processing, bandwidth consumption and preventing DoS attacks must be proposed. The problem statement of this research is summarised as follows:

1. The DAD process uses two types of NDP messages, namely, the NS and NA messages, which have non-secure designs. Therefore, any malicious host can manipulate these messages and send fake messages with an aim of disturbing the DAD process.

2. According to the Standard-DAD mechanism, in an IPv6 link-local network, disclosing the tentative IP address allows malicious nodes to launch DoS attacks against the DAD process.

3. The most commonly employed mechanisms, including SeND, Trust-ND and HSEC-target-DAD, suffer from extensive computations (high complexity in terms of processing time), high bandwidth consumption, hash collision or security weaknesses due to their designs. For instance, SeND and HSEC-target-DAD require high processing time and consume a large amount of bandwidth, both of which induce DoS attacks against the DAD process in an IPv6 link-local network. Meanwhile, Trust-ND and HSEC-target-DAD are prone to hash collision attacks and face security challenges that induce DoS attacks against the DAD process in an IPv6 local-link network.

1.5 Research Objectives

This thesis mainly aims to design a mechanism for preventing DoS attacks against the DAD process in an IPv6 link-local network. This goal is further broken down into the following objectives to facilitate its accomplishment:

1. To propose a cryptographic mechanism for preventing the disclosure of tentative IP addresses during the DAD process in an IPv6 link-local network.
2. To propose a mechanism for securing NS and NA messages by utilising the experimental option of NDP without jeopardising the original structure to security challenges.
3. To design a rule-based mechanism with an aim of preventing DoS attacks against the DAD process in an IPv6 link-local network.
4. To evaluate the performance of the proposed mechanism in terms of its processing time, bandwidth consumption and DoS prevention success rate.

1.6 Research Scope and Limitations

The scope of this thesis is limited to proposing a mechanism for preventing DoS attacks against the DAD process in an IPv6 link-local network as demonstrated in Table 1.1.

Table 1.1: Research Scope and Limitations

Item	Scope of Research
Environment	IPv6 Link-Local Network
Attack Type	DoS-on-DAD process
NDP Messages Types	Neighbor Solicitation (NS) and

	Neighbor Advertisements (NA)
OSI Target Layer	Network Layer
Address Auto-configuration	Stateless Address Auto-configuration
Evaluation Metrics	Processing Time, Bandwidth Consumption and DoS Prevention Success Rate.

1.7 Research Contributions

The key role and security challenges faced by the DAD process in an IPv6 link-local network were discussed in the previous sections. Previous studies have introduced various mechanisms to secure and protect this process against DoS attacks. However, these mechanisms are generally vulnerable to such attacks due to their designs as explained in detail in Section 1.4. This thesis contributes to the literature on security mechanisms by proposing a mechanism for preventing DoS attacks against the DAD process in an IPv6 link-local network by securing NS and NA messages. The other contributions of this thesis include:

i) A cryptographic mechanism for preventing the disclosure of the tentative IP address during the DAD process in an IPv6 link-local network.

ii) ii) A mechanism that secures NS and NA messages by using the experimental option of NDP without jeopardising the original structure to security challenges.

iii) A rule-based mechanism that aims to prevent DoS attacks against the DAD process in an IPv6 link-local network.

1.8 Research Steps

This section outlines the steps for undertaken in this thesis to achieve its objectives. These steps are summarised in Figure 1.5.

Step 1: Literature Review. This phase presents the background of the DAD process in an IPv6 link-local network as well as the main functions, weaknesses and challenges faced by such process. The previously proposed mechanisms that aim to prevent DoS attacks against the DAD process in an IPv6 link-local network are also reviewed.

Step 2: Analysis. In this phase, the main mechanisms for securing the DAD process in an IPv6 link-local network are analysed and discussed. The advantages and limitations of each security mechanism are also identified to provide useful insights into the current limitations and problem of this thesis and to propose the appropriate solutions.

Step 3: Design a Prevention Mechanism. The design of the proposed DAD-match prevention mechanism is presented and discussed in this phase. DAD-match selects a proper cryptographic mechanism to secure the tentative IP address during the course of the DAD process. In addition, the experiment NDP option is designed and the rule-based mechanism is modelled to prevent DoS attacks against the DAD process in an IPv6 link-local network.

Step 4: Evaluation. In this phase, an authentic case study is performed to evaluate the efficiency of the proposed mechanism. This mechanism is then compared with extant mechanisms in terms of its processing time, bandwidth consumption and effectiveness in preventing attacks against the DAD process in an IPv6 link-local network.

Step 5: Conclusion. The findings of the thesis are presented and discussed in this phase. The thesis limitations and contributions are also provided along with some suggestions for further studies.

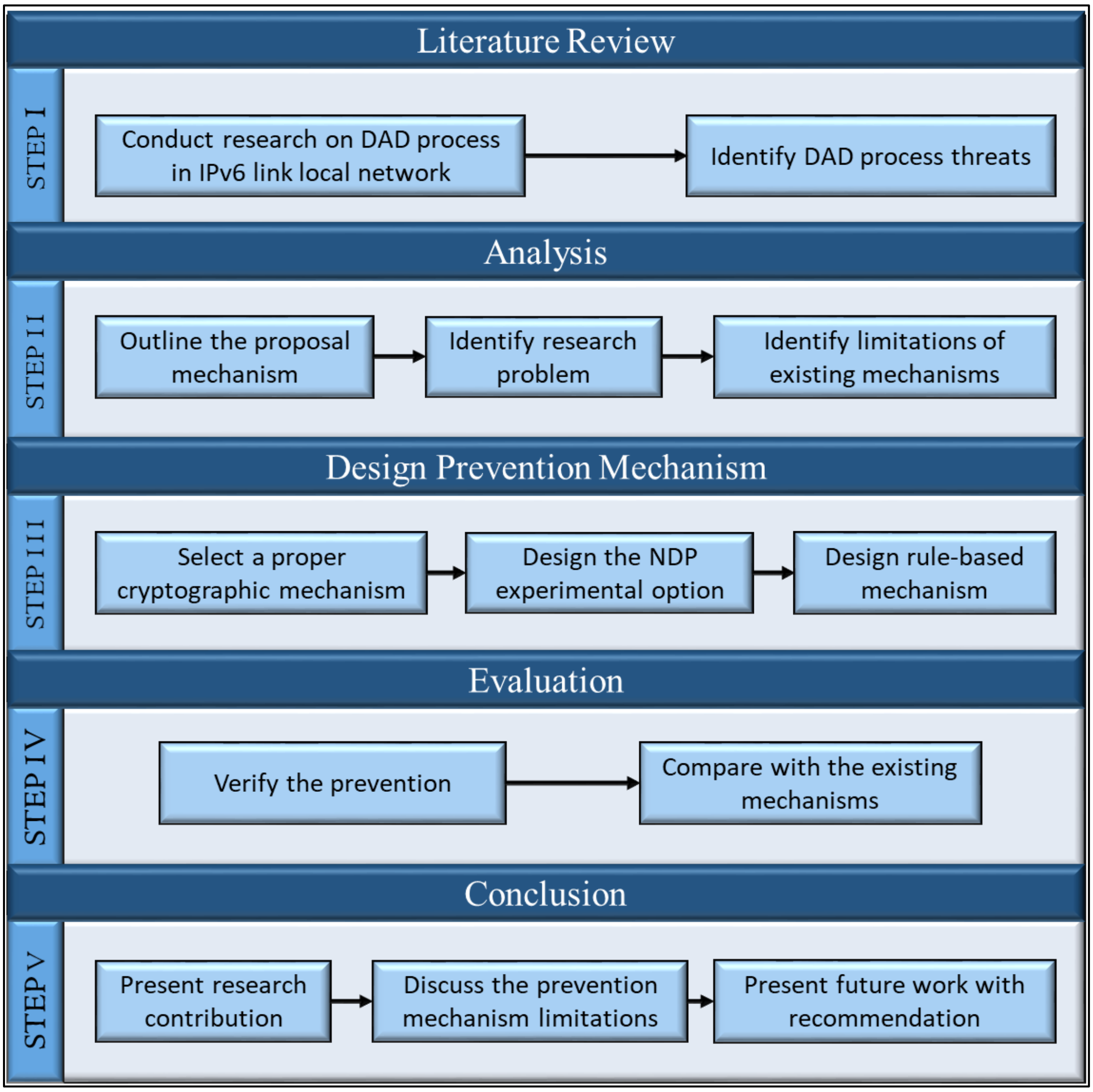
Literature Review
STEP I
Conduct research on DAD process in IPv6 link local network
Identify DAD process threats
Analysis
STEP II
Outline the proposal mechanism
Identify research problem
Identify limitations of existing mechanisms
Design Prevention Mechanism
STEP III
Select a proper cryptographic mechanism
Design the NDP experimental option
Design rule-based mechanism
Evaluation
STEP IV
Verify the prevention
Compare with the existing mechanisms
Conclusion
STEP V
Present research contribution
Discuss the prevention mechanism limitations
Present future work with recommendation

Figure 1.5 Research Steps

1.9 Thesis Organization

This thesis is divided into six chapters. The research topic is introduced in Chapter 1. The other chapters are arranged as follows:

Chapter Two critically reviews the background of the DAD process in an IPv6 link-local network. This chapter also reviews the basic concepts related to this thesis, the relevant studies and the limitations of each extant mechanism.

Chapter Three discusses the methodology of the proposed DAD-match mechanism and elaborates its requirements.

Chapter Four analyses the proposed mechanism as well as describes its structural design and implementation.

Chapter Five compares the performance of the proposed DAD-match mechanism with that of the Standard-DAD, SeND, Trust-ND and HSEC-Target-DAD mechanisms.

Chapter Six summarises the findings of this thesis and outlines its scope. The chapter also proposes some useful suggestions and recommendations for future work.

CHAPTER 2

LITERATURE REVIEW

In this chapter, Section 2.1 presents the background of the IPv6 link-local network and NDP. Section 2.2 discusses the processes and common attacks launched against NDP. Section 2.3 presents the auto-configuration of an IPv6 address, Section 2.4 introduces the concept of rule-based system. Section 2.5 presents the cryptography hash function and the secure hash standard. Section 2.6 illustrates the DAD process and its security issues, Sections 2.7 presents proposed mechanisms aim to secure the DAD process in IPv6 link-local network and 2.8 discussed the critical review on related work. Section 2.9 summarized the chapter.

2.1 Background

In a link-local network, several nodes are connected via a wired or wireless links to communicate with one another. IPv6 is implemented as a network layer protocol. Link-local communication also includes the data link layer in the form of a lower layer in accordance with the reference scheme of ISO/OSI. Many operating processes can be performed in an IPv6 link-local network, including address resolution protocol (ARP) (Plummer, 1982), router discovery (Deering, 1991) and redirect protocol (Postel et al., 1981).

The emergence of IPv6 protocol has made several evaluations on the model of link-local communication. All functions of the existing IPv4 local networks have been combined in an NDP process (Thomas et al., 2007), which allows hosts to communicate with other nodes (routers or hosts) in the same link. The functions of NDP are discussed in detail in Section 2.2.

IPv6 also aims to enhance the performance and security of the link-local network security by introducing new features, such as Internet Protocol security (IPsec). Although the original NDP design also contains IPsec as one of its features (Stockebrand, 2007; Seo & Kent, 2005), previous studies (Ahmed et al., 2017; Al-Ani et al., 2018) show that IPsec suffers from several problems, including its inability to support multicasting, its limited degree of protection (between two nodes only), high complexity and high cost. Figure 2.1 illustrates a standard communication process in a link-local network.

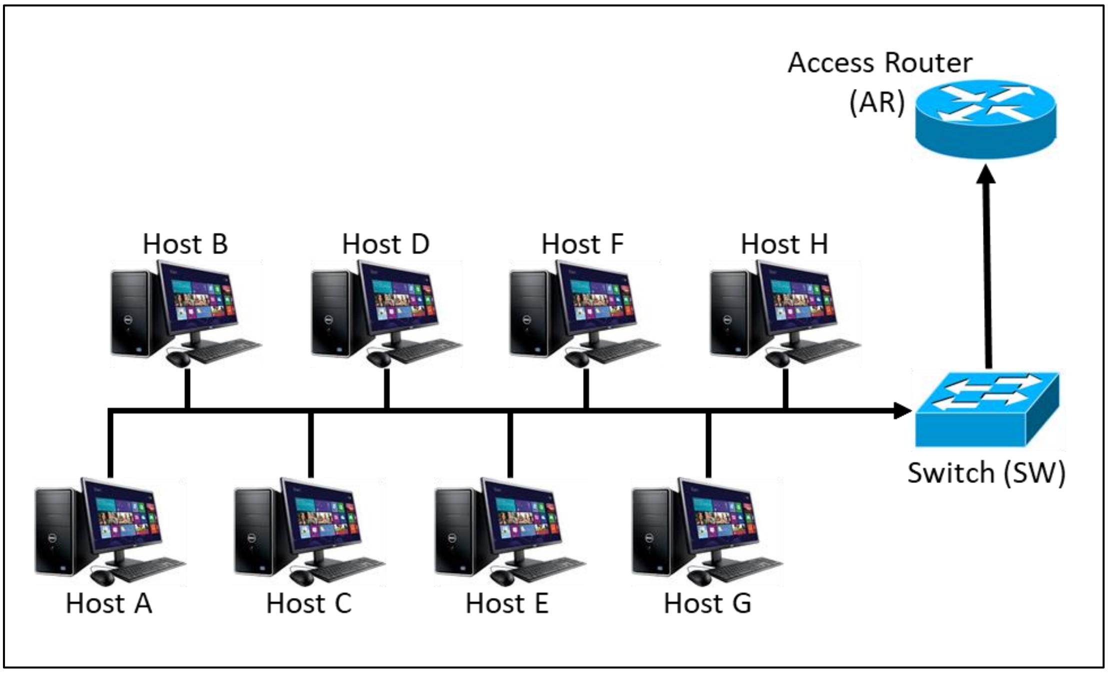

Figure 2.1 Link-Local Network

In Figure 2.1, all nodes are situated in the same link and are physically interconnected via switches. Each of these nodes can communicate with other devices without a routing protocol. Meanwhile, the edge (also called access or gateway) router connects the local network domain to an external cloud, such as the Internet. Many routers may exist in a local network (especially in a wide-scale network) and connect LANs with one another.

In a link-local network that employs ethernet as the data link layer protocol, the IPv6 node and other nodes exchange information with one another by sending a link layer frame that contacts the IPv6 packet as illustrated in Figure 2.2 (Crawford, 1998). In this figure, the frame type is x86dd, which denotes an IPv6 packet.

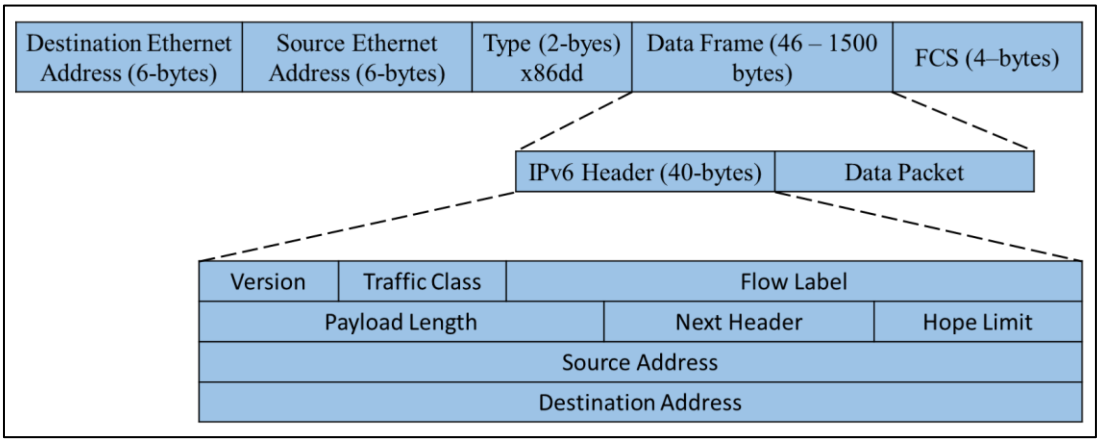

Figure 2.2 Link-Local Frame for an IPv6 Packet

IPv6 nodes use several types of addresses to communicate with one another, including the link-local IPv6 address and the global IPv6 address. These address types are discussed in detail in the following section.

Types of Addresses in an IPv6 Link-Local Network: in the Transmission Control Protocol/Internet Protocol (TCP/IP) model, nodes exchange IPv6 packets with one another. However, nodes that are connected physically to the same link-local network need to know the address of another node in order to communicate. Two types of addresses are generally used in a link-local network, namely, ethernet (also known as medium access control (MAC) or link-layer address) in the ethernet frame and the IPv6 address within the IPv6 header. The MAC address pertains to the physical address of a device and is used by an IPv6 node to communicate with a neighbor node. This address is 48 bits (6 bytes) long and comprises two parts, namely, the organisational unique identifier (OUI) and the vendor-assigned address, as illustrated in Figure 2.3.

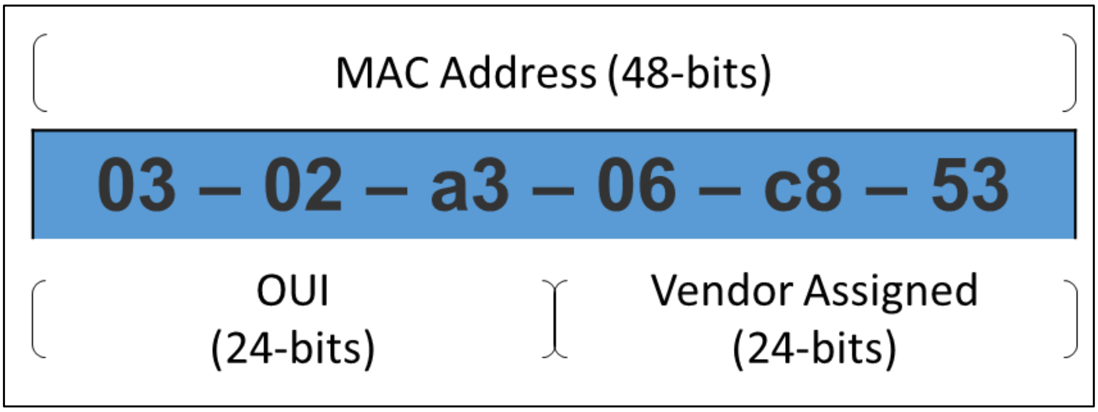

Figure 2.3 MAC Address

Figure 2.3 illustrates the MAC address of a computer (03-02-a3-06-c8-53), where 03-02-a3 represents the OUI and 06-c8-53 represents the vendor-assigned address. The OUI is administered by the Institute of Electrical and Electronics Engineers (IEEE) and is used to identify the vendor of the network adapter. The vendor-assigned portion of the MAC address is simply the alphanumeric identifier assigned by the vendor. These two parts are combined to ensure that no two network adapters will share the same MAC address.

Another address required for a node to communicate in an IPv6 link-local network is the IPv6 link-local address. Given that this link-local network has no forwarding mechanism, performing the NDP process in this network is necessary. As NDP communication uses Internet control message protocol version 6 (ICMPv6) messages that are included in the IP layer, an IPv6 link-local address is required (Hinden & Deering, 2006).

An IPv6 link-local address has a length of 128 bits and is represented as 8 colon-separated hexadecimal numbers (R. M. Hinden & Deering, 2006). The address begins with the pre-defined prefix FE80::/64. The nodes that are attached to an IPv6 network are required to automatically create an entire link-local address as part of the Stateless

Address Auto-Configuration (SLAAC) mechanism (Thomas Narten, Thomson, et al., 2007), which will be discussed in detail in Section 2.3. Nodes use the link-local address to communicate with other nodes in the same link. This type of address cannot be used to send a packet of IPv6 outside the network.

Each node needs a global IPv6 address to communicate globally over the Internet. As defined in RFC 4291 (Hinden & Deering, 2006), an IPv6 address comprises a prefix and an interface identifier and can be generated in the following ways:

- Static (Manual) IPv6 address assignment: The global IPv6 address, subnet prefix length and default gateway are manually configured and are disabled in case a dynamic host configuration protocol for IPv6 (DHCPv6) exists.
- SLAAC: The global IPv6 address can be generated by combining the host interface EUI-64 (according to the address of the host MAC on the ethernet interface) with the link prefix, which is obtained through the router advertisement (RA) messages being sent periodically by the router in the link-local network.
- DHCPv6: A centralised server of DHCPv6 is required in a LAN. DHCPv6 can be configured in the following ways as specified in RFC 3315 (Troan & Droms, 2003):
    - Stateless auto-configuration DHCPv6 mode: In this mode, SLAAC is used to obtain the IPv6 address, whilst DHCPv6 is used to obtain the other configuration options, including the domain name system and network time protocol. The DHCP server does not need to store dynamic state data on any of the individual clients.

- Stateful auto-configuration DHCPv6 mode: In this mode, DHCPv6 is used to obtain the IPv6 address and other required parameters from the DHCPv6 server.

Apart from MAC, link-local and global addresses, the IPv6 nodes join certain multicast group addresses to send out messages to a group of hosts or routers in the link and to perform certain NDP functions, including the DAD process to validate the uniqueness of an IPv6 address and the NUD process to check the reachability of another neighbor node. All routers should join an all-routers multicast group (FF02::2), which helps hosts and routers communicate with one another via Router Solicitation (RS), RA and redirect messages (RM). Alternatively, hosts in the same link an join the all-node multicast group (FF02::1) to reduce the number of receiving hosts by using a Solicited Node Multicast Address (SNMA) (FF02::1:FF/104) according to the last 24 bits of the IPv6 address (Hinden & Deering, 2006). All nodes with the same last 24 bits will join the same SNMA address.

The addresses required to establish communication in an IPv6 link-local network are listed in Table 2.1. When a host recently joins the IPv6 link-local network and does not have any address, an unspecified address (::) may be used to direct an NDP request for router information or during the DAD process to verify the IPv6 address uniqueness.

Table 2.1 Addresses Used by Nodes in an IPv6 Link-Local Network

Address Type	Purpose	Example
Link-local address (MAC)	Communicate with a neighboring node at the link layer-level.	20:AC:49:22:C1:0B (unicast) 33:33:FF:03:18:C3 (multicast)
Link-local address	Communicate with a neighboring node at the network level.	FE80::73C3:9022:12:C2BE
Global address	Communicate with an external node.	2001:db8:3c4d:15::1a2f:1a2b
All-node multicast group	Multicast an NS message.	FF02::1
All router-multicast group	Multicast an RS message.	FF02::2
Solicited node multicast address (SNMA)	Multicast an NS message for several processes, including DAD, NUD and AR.	FF02::1:FF24:1991

2.2 **Neighbor Discovery Protocol (NDP)**

NDP represents several messages and processes for establishing communication amongst nodes, routers and hosts located in the same network. The NDP replaces some protocols found in IPv4, including router discovery, ARP, ICMP and ICMP redirect. IPv6 NDP allows nodes to detect neighbors on a similar LAN and let their existence be known to their neighbors. Further, NDP has important processes, such as: DAD, NUD and AR.

In an IPv6 link-local network, all nodes can configure their addresses automatically by using SLAAC which is one of NDP functions, which will be discussed further in Section 2.3 (Narten et al., 2007), without the need for DHCPv6 (Droms et al., 2003), which is an NDP process. Using SLAAC provides the IPv6 host with some power to generate a link-local network and a global address without the need for manual intervention. Some important NDP processes in an IPv6 link-local network are summarised as follows:

- Generate an IP address by using SLAAC in case of a stateless DHCPv6.
- Check the uniqueness of the generated IP address by performing the DAD process.
- Discover a neighbor router located in the same link-local network.
- Preserve the accessibility of the neighbor nodes by performing the NUD process.
- Find the correlation between the IP and MAC addresses of neighboring nodes by performing the AR process.
- Use RM to advertise a better next-hop.

To complete an NDP process, the five ICMPv6 messages presented in Table 2.2 are used.

Table 2.2 Five NDP Messages

Message Name	Purpose
Router Solicitation (RS) Message **Type (133)**	An RS message is usually sent by the hosts when the system starts up so that an RA message is immediately received without waiting for the scheduler/timer.
Router Advertisement (RA) Message **Type (134)**	The router generates RA messages that are sent periodically or are sent in response to an RS message to let their presence known. These messages aim to send a router prefix, a maximum transit unit, a prefix and a hop limit parameters list. This message can also configure the global IP address of a host by using a stateless or stateful mechanism.
Neighbor Solicitation (NS) Message **Type (135)**	An NS message is sent by the hosts in the same local link to discover the link layer addresses of other nodes or by the DAD process to verify the uniqueness of the generated IP address.
Neighbor Advertisement (NA) Message **Type (136)**	An NA message is transmitted to change the host MAC address, to announce IP addresses or to respond to NS messages through DAD, AR or NUD processes.
Redirect Message (RM) **Type (137)**	An RM message aims to redirect the traffic between routers.