

**THE UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**

**APPLYING IPv6 DYNAMIC ROUTING PROTOCOL ON A CAMPUS  
ENVIRONMENT**

**MASTER THESIS**

**Mohammed AL-Dagdoog**

**THE DEPARTMENT OF INFORMATION TECHNOLOGY**

**THE PROGRAM OF INFORMATION TECHNOLOGY**

**SEPTEMBER 2015**

**THE UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**

**APPLYING IPv6 DYNAMIC ROUTING PROTOCOL ON A CAMPUS  
ENVIRONMENT**

**MASTER THESIS**

**Mohammed AL-Dagdoog**

**1303667003**

**THE DEPARTMENT OF INFORMATION TECHNOLOGY**

**THE PROGRAM OF INFORMATION TECHNOLOGY**

**Supervisor: Assist. Prof. Dr. Shadi AL SHEHABI**

**SEPTEMBER 2015**

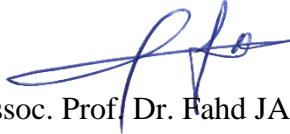
Mohammed AL-DAGDOOG, having student number 1303667003 and enrolled in the Master Program at the Institute of Science and Technology at the University of Turkish Aeronautical Association, after meeting all of the required conditions contained in the related regulations, has successfully accomplished, in front of the jury, the presentation of the thesis prepared with the title of: “APPLYING IPv6 DYNAMIC ROUTING PROTOCOL ON A CAMPUS ENVIRONMENT”.



**Supervisor:**

Assist. Prof. Dr. Shadi AL SHEHABI


The University of Turkish Aeronautical Association



**Jury Members:**

Assoc. Prof. Dr. Fahd JARAD

The University of Turkish Aeronautical Association



Assist. Prof. Dr. Abdül Kadir GÖRÜR

Çankaya University

**Thesis Defense Date:** 30.09.2015

**THE UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION**  
**INSTITUTE OF SCIENCE AND TECHNOLOGY**

I hereby declare that all the information in this study I presented as my Master's Thesis, called: APPLYING IPv6 DYNAMIC ROUTING PROTOCOL ON A CAMPUS ENVIRONMENT, has been presented in accordance with the academic rules and ethical conduct. I also declare and certify with my honor that I have fully cited and referenced all the sources I made use of in this present study.

**30.09.2015**

**Mohammed AL-DAGDOOG**

## **ACKNOWLEDGEMENTS**

Thanks to the most compassionate, gracious and merciful. May Allah's blessings and peace be upon our prophet Mohammed who protects us from the depths of darkness and leads us forth into light, and his household.

It is a pleasure to express my special thanks to my friends Samir AL-Asadi who helped me, Mohammed AL-Shimmari who inspired me and my family and other friends for their valuable support.

I would like to express my sincere gratitude to Assist. Prof. Dr. Shadi AL SHEHABI for his supervision, special guidance, suggestions, and encouragement through the development of this thesis.

**September 2015**

**Mohammed AL-DAGDOOG**

## TABLE OF CONTENTS

<b>ACKNOWLEDGMENTS.....</b>	<b>ii</b>
<b>TABLE OF CONTENTS.....</b>	<b>iii</b>
<b>LIST OF TABLES.....</b>	<b>vi</b>
<b>LIST OF FIGURES.....</b>	<b>vii</b>
<b>LIST OF ABBRIVIATION.....</b>	<b>ix</b>
<b>ABSTRACT.....</b>	<b>xi</b>
<b>ÖZ.....</b>	<b>xiii</b>
<b>CHAPTER ONE.....</b>	<b>1</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1    Background.....	1
1.2    Organization of the thesis.....	3
<b>CHAPTER TWO.....</b>	<b>5</b>
<b>2. NETWORK ADDRESSING.....</b>	<b>5</b>
2.1    OSI Model.....	5
2.1.1    Data Link Layer.....	6
2.1.2    Network Layer.....	6
2.2    The concept of two addresses.....	6
2.2.1    Layer 2 addressing (MAC).....	6
2.2.2    Layer 3 addressing (IP).....	8
2.3    The need for two addresses.....	11
2.3.1    Scenario 1.....	11
2.3.2    Scenario 2.....	12
2.4    Conclusion.....	14

<b>CHAPTER THREE.....</b>	<b>15</b>
<b>3. COMPARISON BETWEEN IPv4 AND IPv6.....</b>	<b>15</b>
3.1    IPv4 header.....	16
3.2    IPv6 header.....	18
3.3    Benefits of using IPv6 over IPv4.....	20
3.4    Unneeded fields in IPv6 header.....	21
3.5    IPv6 address format.....	21
3.6    IPv6 vs IPv4 addressing.....	23
3.7    Types of IPv6.....	23
3.7.1    Link Local.....	23
3.7.2    Unique Local.....	24
3.7.3    Global Unicast Address.....	24
3.7.4    Extended Unique Identifier EUI.....	25
3.8    IPv6 Auto-Configuration.....	25
3.9    Literature Review.....	25
3.10   IPv6 projects in Turkey.....	26
3.10.1   Design of National IPv6 Infrastructure and Transition to IPv6 Protocol.....	26
3.10.1.1   IPv6 GO CREATION.....	27
3.10.1.2   IPv6 ENABLED VIDEO- CONFERENCE SOFTWARE DEVELOPMENT.....	27
3.10.1.3   HONEYPOT DEVELOPMENT.....	27
3.10.2   Turkey’s Plan for Public Sector's Transition to IPv6...	28
3.10.3   GEN6 - Governments ENabled with IPv6.....	28
3.10   Conclusion.....	29
<b>CHAPTER FOUR.....</b>	<b>31</b>
<b>4. DYNAMIC ROUTING PROTOCOL.....</b>	<b>31</b>
4.1    OSPFv3 vs OSPFv2.....	32
4.2    LSAs.....	33
4.3    Types of routers in OSPF.....	37
4.4    Types of areas in OSPF.....	39
4.5    Conclusion about the characteristics of OSPF.....	42

<b>CHAPTER FIVE.....</b>	<b>44</b>
<b>5. THE EXPERIMENTAL WORK.....</b>	<b>44</b>
5.1    GNS3.....	46
5.2    The design of our campus network.....	46
5.2.1    The Buildings.....	47
5.2.2    The functionality of the devices.....	48
5.2.3    Physical connection and IP addressing.....	50
5.2.4    Security at Access Layer.....	51
5.2.5    The virtual network.....	52
5.3    Capturing OSPF packets.....	63
5.4    Assigning ports to VALN.....	64
5.5    Results.....	67
5.5.1    Checking routing tables.....	67
5.5.2    Packet capturing.....	69
5.5.3    Protocol tree.....	70
5.5.4    Conversation between Ankara and İzmir routers.....	70
5.5.5    Packet lengths.....	71
5.5.6    I/O Graph.....	72
<b>CHAPTER SIX.....</b>	<b>74</b>
<b>6. CONCLUSION.....</b>	<b>74</b>
6.1    Findings.....	75
6.2    Limitations.....	76
6.3    Future studies.....	76
6.4    Conclusion.....	77
<b>REFERENCES.....</b>	<b>79</b>
<b>CURRICULUM VITAE.....</b>	<b>87</b>



## LIST OF TABLES

<b>Table 3.1</b>	Comparison between IPv4 and IPv6.....	23
<b>Table 4.1</b>	LSAs.....	35
<b>Table 4.2</b>	LSAs and OSPF area types.....	42
<b>Table 5.1</b>	No. of switched for each building.....	48
<b>Table 5.2</b>	The VLAN's in Ankara campus.....	52
<b>Table 5.3</b>	The VLAN's in İzmir campus.....	53
<b>Table 5.4</b>	The VLAN's in Eskişehir campus.....	54

## LIST OF FIGURES

<b>Figure 2.1</b>	OSI Model.....	5
<b>Figure 2.2</b>	MAC address.....	7
<b>Figure 2.3</b>	ARP packet.....	8
<b>Figure 2.4</b>	IPv4 header.....	9
<b>Figure 2.5</b>	A home network.....	11
<b>Figure 2.6</b>	A request across the Internet.....	12
<b>Figure 3.1</b>	IPv4 datagram.....	17
<b>Figure 3.2</b>	IPv6 datagram.....	18
<b>Figure 3.3</b>	IPv6 base header.....	19
<b>Figure 3.4</b>	An IPv6 in binary.....	21
<b>Figure 3.5</b>	Colon to separate each segment of an IPv6.....	22
<b>Figure 3.6</b>	A binary IPv6 mapped to hex.....	22
<b>Figure 3.7</b>	General Topology of IPv6-GO.....	27
<b>Figure 4.1</b>	Areas nature of OSPF.....	37
<b>Figure 4.2.</b>	Types of routers in OSPF.....	38
<b>Figure 4.3</b>	Standard Area with LSAs.....	39
<b>Figure 4.4</b>	Stub Area with LSAs.....	40
<b>Figure 4.5</b>	Totally Stubby Area with LSAs.....	40
<b>Figure 4.6</b>	Not So Stubby Area with LSAs.....	41
<b>Figure 4.7</b>	NSSA Topological Example.....	41
<b>Figure 5.1.a</b>	Cisco campus hierarchy.....	44
<b>Figure 5.1.b</b>	Cisco campus hierarchy.....	46
<b>Figure 5.2</b>	Switch Stacking.....	49
<b>Figure 5.3</b>	Ankara campus topology.....	50
<b>Figure 5.4</b>	Show CDP neighbors command on Ankara core.....	51

<b>Figure 5.5</b>	Show VLAN command on the core switch.....	53
<b>Figure 5.6</b>	Show vtp status command on the core.....	54
<b>Figure 5.7</b>	Show vtp status command on an access switch.....	55
<b>Figure 5.8</b>	Show VLAN command on an access switch.....	55
<b>Figure 5.9</b>	Area 0.....	57
<b>Figure 5.10</b>	Area 1.....	57
<b>Figure 5.11</b>	Area 2.....	58
<b>Figure 5.12</b>	İzmir router links.....	58
<b>Figure 5.13</b>	Show IPv6 protocols command on İzmir router.....	59
<b>Figure 5.14</b>	Show IPv6 route OSPF command on Eskişehir router (R3).....	59
<b>Figure 5.15</b>	The subnet between routers.....	60
<b>Figure 5.16</b>	2001 Router-LSA on R1.....	60
<b>Figure 5.17</b>	2002 Network-LSA.....	61
<b>Figure 5.18</b>	2003 Inter-Area-Prefix-LSA.....	61
<b>Figure 5.19</b>	4005 AS-External-LSA.....	61
<b>Figure 5.20</b>	0008 Link-LSA.....	62
<b>Figure 5.21</b>	2009 Intra-Area-Prefix-LSA.....	62
<b>Figure 5.22</b>	A packet capture.....	63
<b>Figure 5.23</b>	R3 Link local address.....	64
<b>Figure 5.24</b>	LAS type 3 generated by R3.....	64
<b>Figure 5.25</b>	Adding PCs to the topology.....	65
<b>Figure 5.26</b>	IPv6 Auto-Configuration.....	65
<b>Figure 5.27</b>	IPv6 on Windows 7 host.....	66
<b>Figure 5.28</b>	Ping request on Wireshark.....	66
<b>Figure 5.29</b>	Routing table of Ankara router before OSPF.....	67
<b>Figure 5.30</b>	Routing table of Ankara router after OSPF.....	68
<b>Figure 5.31</b>	Summary of booting up all devices.....	69
<b>Figure 5.32</b>	Protocols Hierarchy used in the capture.....	70
<b>Figure 5.33</b>	Traffic between Ankara and İzmir routers.....	71
<b>Figure 5.33</b>	Packet lengths.....	72
<b>Figure 5.33</b>	I/O Graph.....	73

## LIST OF ABBRIVIATION

PC	Personal Computer
IP	Internet Protocol
NAT	Network Address Translation
CIDR	Classless Inter-Domain Routing
IETF	Internet Engineering Task Force
VoIP	Voice over IP
RFC	Request for Comments
QoS	Quality of service
IPTV	IP-based TV
OSPF	Open Shortest Path First
GNS	Graphical Network Simulator
MAC	Media Access Control
OSI	Open System Interconnection
ISO	International Standards Organization
OUI	Organizational Unique Identifier
LAN	Local Area Network
VLAN	Virtual LAN
ASIC	Application-Specific Integrated Circuit
ARP	Address Resolution Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
RIP	Routing Information Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ToS	Type of Services
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

TTL	Time To Live
IPsec	IP Security
ICMP	Internet Control Message Protocol
ULA	Unique Local address
IANA	Internet Assigned Numbers Authority
EUI	Extended Unique Identifiers
DHCP	Dynamic Host Configuration Protocol
TUBITAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (The Scientific & Technological Research Council of Turkey)
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi (Turkish Academic Network And Information Center)
BTK	Bilgi Teknolojileri ve İletişim Kurumu (Turkish Information Technologies and Communications Authority)
ICTA	Information And Communication Technologies Authority
GEN6	Governments ENabled with IPv6
EGG	eGovernment Gateway
G2G	Government to Government
G2C	Government to Citizen
PTT	Posta Telgraf Teşkilatı (The General Directories Of Post And Telegraph Organization)
SGK	Sosyal Güvenlik Kurumu (Social Security Institution)
LSA	Link State Advertisements
NBMA	Non-Broadcast Multi-Access
ABR	Area Border Router
ASBR	Autonomous System Boundary Router
DR	Designated Router
AS	Autonomous System
NSSA	Not So Stubby Area
VLSM	Variable Length Subnet Masking
CLI	Command Line Interface
STP	Shielded Twisted Pair
VTP	Virtual Trunking Protocol

## **ABSTRACT**

### **APPLYING IPv6 DYNAMIC ROUTING PROTOCOL ON A CAMPUS ENVIRONMENT**

AL-DAGDOOG, Mohammed

Master, Department of Information Technology

Thesis Supervisor: Assist. Prof. Dr. Shadi AL SHEHABI

September-2015, 78 page

As IPv4 is running out, the need for changing to IP next generation, IPv6 is obvious because the number of people and devices that connect to networks increases each and every day. Not only does IPv6 give us lots of addresses ( $3.4 \times 10^{38} =$  definitely enough), but there are many other features built into this version that make it well worth the cost, time, and effort required to migrate to it. However, the use of Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) has helped to extend the shortage of addresses, but we will run out of them, and it's going to happen within a few years.

This study aims to describe the benefits of applying IPv6 dynamic routing protocol in the campus of the university of Turkish aeronautical association. In this work a simulated network represents the campus of the university by using Graphical Network Simulator (GNS3) to deploy OSPF on three geographically separated campuses armed with IPv6. Going deep inside some packets to analyse OSPF performance over the campus by using tool of network sniffing Wireshark.

**Keywords:** Internet Protocol version 6, Dynamic Routing Protocol OSPF, Graphical Network Simulator version 3, Wireshark.

## ÖZET

### YERLEŞKE (KAMPÜS) ORTAMINDA IPv6 DİNAMİK YÖNLENDİRME PROTOKOLÜ UYGULAMASI

AL-DAGDOOG, Mohammed

Yüksek Lisans, Bilişim Teknolojileri Anabilim Dalı

Tez Danışmanı: Doç. Dr. Shadi AL SHEHABI

Eylül -2015, 78 sayfa

IPv4'ün tükenmesiyle birlikte, bir sonraki IP jenerasyonuna, IPv6'YA geçme ihtiyacı daha da belirgin hale gelmiştir; çünkü ağlara bağlanan kişi ve cihaz sayısı her geçen gün artmaktadır. IPv6 bize yalnızca bir çok adres (net olarak =  $3.4 \times 10^{38}$ ) sunmakla kalmaz aynı zamanda da kendisine yapılan masrafları, harcanan zaman ve gösterilen çabaların karşılığını veren birçok özelliğe de sahiptir. Ancak Sınıfsız Alanlar- Arası Yönlendirme (CIDR) ve Ağ Adresi Çevirisinin (NAT) kullanımı adres eksiliğinin genişlemesine yardımcı olmuş olsa da biz tüm bu adresleri birkaç yıl içerisinde tüketmiş olacağız.

Bu çalışma Türk Hava Kurumu Üniversitesi kampüsünde IPv6 dinamik yönlendirme protokolünün uygulanmasının yararlarını tanımlamayı amaçlamaktadır. Bu çalışmada, coğrafi açıdan farklı yerde bulunan IPv6 ile donatılmış üç kampüste OSPF'yi yerleştirmek amacıyla Grafik Ağ Simülatörü (GNS3) kullanılarak simüle edilmiş bir ağ, üniversite kampüsünü temsil etmektedir. Ağ yakalama aracı Wireshark kullanılarak kampüs içerisinde OSPF performansının analiz edilmesi için bazı paketler derinlemesine incelenmiştir.



**Anahtar Kelimeler:** İnternet Protokolü versiyon 6, Dinamik Yönlendirme Protokolü OSPF, Grafik Ağ Simülatörü versiyon GNS3, Wireshark.

## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.1 Background**

Undoubtedly, one of the elements of life nowadays is information technology. Computer technologies and architectures are used in all areas. PCs need to provide an infrastructure to ensure the communication with each other. The world is provided by infrastructure and companies that are providing this communication all over the Internet. Currently the standard protocol used in the Internet communication is Internet Protocol Version 4 (IPv4).

To be addressed with IPv4 by providing end to end communication between computers and similar devices, the work has continued with some improvements made in a good way as to be seamless. Internet technology on mobile devices, security systems, remote access to work in the desired systems, and electronic devices at businesses or homes are not even used in small electronic appliances. In short, both commercial and social use the Internet very often, this need has led to further growth every day. The biggest problem in the process of technological development is the limit capacity of the IPv4 address that can be used for this system. 4,294,967,296 IPv4 can't be used efficiently due to the huge growth in number of devices that use the Internet these days [2].

Rapid depletion of IPv4 has led to the start using the mechanism of the NAT and CIDR. Network Address Translation allows multiple devices to share one public IP address [4]. Classless Inter-Domain routing eliminates the concept of class from the IP address [3]. Despite these improvements, the huge increase in Internet usage, high

mobility, multimedia, strong security, end to end access, etc. have been increasing the inability to meet the demand in a good way. For these reasons, new solutions were proposed by the Internet Engineering Task Force (IETF) and other relevant institutions and organizations who are responsible for the Internet protocols. The most important study is Internet Protocol Version 6 (IPv6). The using of the Internet, mobile phone development, smart home applications, new technologies and Voice over Internet Protocol (VoIP) applications, such as anytime access, are growing faster than expected, in China and India where are billions new users in such developing countries. This growing led to lay the foundation of IPv6 in the early 1990s [5]. A new development of IP protocol working group was established in the early 1990s by the IETF, after a series of studies, in 1995 December, the first IPv6 Requests for Comments (RFC) 1883 (and others) was officially launched to announce IPv6.

The main purpose is to provide mobility between the Internet Protocol networks. IPv6 has more capabilities from on the basis of IPv4. The most basic feature that distinguishes IPv6 from IPv4 is extended with a 128-bit address space. This theoretical number of the expanded addressable nodes will provide  $2^{128}$  (340,282,366,920,938,463,463,374,607,431,768,211,456) IP addresses [6]. This huge number of IPv6's address space solves the problem of IPv4's shortage and the quick growth of different applications on the Internet.

With the currently available IPv4, the Internet address of each device in the management of IP mechanisms needs to be confirmed manually. In IPv6, this administrative burden is reduced by automatically addressing mechanism. In addition, IPv6 offers stability in commercial transactions such as scalability, availability, end-to-end access, quality of service (QoS), VoIP and IP-based TV (IPTV). IPv6 is coming with a feature of having more flexible structure according to IPv4. To compare between the two protocols, there are some changes with the structure of the headers of both v6 and v4, the major one is adding the extension to the header of IPv6. From security wise, built in IPsec is developed in IPv6, whereas in IPv4 security faces difficulty due to NAT usage [1].

IPv6 is more advanced network layer development protocol than IPv4. In Europe, Asia and especially in the United States, there are commercial interest and activity. The goal of US Department of Defense is to complete all internal communication with IPv6 transition. To do this, from October first, 2003 to 2008, the

development of IPv6 had reported that new products need to have IPv6 support. In 2005, the United States suggested the plan for the transition of all institutions to IPv6 [7].

In Turkey, December 8<sup>th</sup>, 2010 until March 31<sup>st</sup>, 2011, Prime Ministry with public institutions and organizations published that layer 3 switches, routers, security devices, Internet services provider and the software that enables the delivery of these services would make an inventory of studies on whether the IPv6 support was specified. Public institutions and organizations at the latest as of August 31<sup>st</sup>, 2012 would be supplied with IPv6 addresses and IPv6 connections. After August 31, 2012, no network hardware supports IPv6 and it was reported to be investing in software. Transition process to IPv6 in the institutions is seamlessly necessary to plan, for this, there many projects have taken place in Turkey to apply IPv6 in the institutes [8].

This work is intended to apply IPv6 to the University of Turkish aeronautical association with OSPFv3 and link the tree campuses of that university in simulated environment by using Graphical Network Simulator GNS3 since it is too difficult to work on real world campus environment. All this work is contributed to answer these questions:

With the scarcity of IPv4 address, what would happen if our campus grows up?

If we deployed IPv6, is it beneficial to work with it?

Why do we need to upgrade to IPv6?

How OSPF affects our topology?

## **1.2 Organization of the thesis**

Chapter2 includes addressing in general as well as why we need 2 addresses in the networking world, MAC (Data Link Layer address) and IP (Network layer address). Chapter3 covers IPv4 addressing and its limitations, problems and solutions represented by NAT, and IPv6 in addition to the reasons why IPv6 hasn't been used widely up to now in addition to a literature review about the works have been done regarding the field of IPv6 in a campus environment and the projects of IPv6 in Turkey. Chapter 4 discusses IPv6 routing protocol OSPFv3 that is used for the practical part of

this thesis, the reasons behind this choice, a comparison between v2 and v3 of OSPF, the benefits and how it works. Chapter 5 is about the practical side of the thesis to apply IPv6's OSPFv3 on a virtual campus of the university of Turkish aeronautical association simulated by GNS3.

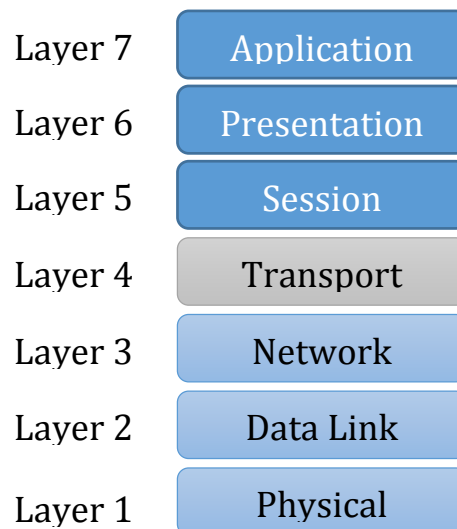
## CHAPTER TWO

### NETWORK ADDRESSING

This chapter will try to lighten the concept of addressing in the networking world, what its main purposes, the types of addressing and hierarchy, and the structure of each and every one of them. The theory behind that we need to know how the differences between IPv4 and IPv6 will affect the network and its infrastructure.

#### 2.1 OSI Model

OSI or (Open System Interconnection) is a model that developed in 1978 by the International Standards Organization (ISO) [9] to divide the communication procedure into smaller standardized steps or layers (as figure 2.1 illustrates) where every layer is responsible for a certain set of actions and functions, and each layer is communicating with the same layer at the other peer side by sending and receiving messages [10].



**Figure 2.1** OSI Model [11]

The layers start from the bottom to the top where the first three layers are the most important from a network point of view while the upper four layers are important from the users' point of view [11]. This chapter will try to focus on the second or Data Link Layer and the third or the Network layer since each one of them plays a crucial part of communication and has its own way of addressing.

### **2.1.1 Data Link Layer:**

- Uses the MAC address.
- Converts the bits to packets and packets to bits so it works as a convertor between layer 1 and the upper layers.
- Delivers the data to layer 2 as an electrical signals.
- It does framing of the packets which is dividing the packets into smaller pieces.
- It performs error checking.
- Switch and bridge are the devices of data link layer [12].

### **2.1.2 Network Layer:**

- Translates the physical address or the MAC address into logical address which is IPv4.
- Uses IP address as an addressing tool whether it is IPv4 or IPv6.
- Does the quality of service
- Chooses the route path through the routing table.
- Router and layer 3 switch are the devices of network layer [12].

## **2.2 The concept of two addresses**

There are two types of addressing in any given network which are:

### **2.2.1 Layer 2 addressing (MAC):**

Addressing at this level is based on MAC (Media Access Control) [13] address where MAC address is a globally unique value that is based on the network adapter.

MAC address is also called global address or physical address. MAC address is consist of 12 digital hexadecimal number which is 48 bits in lengths and it has two ways of writing the first one as MM:MM:MM:SS:SS:SS and the second one as MM-MM-MM-SS-SS-SS.

The first half of the MAC address represents the manufacturer of the network adapter or card and the side that regulates and gives away this unique half to all manufacturers is the Internet Standard Body.

The second half is given by the company that manufactures the card and this second half has to be unique among all the manufacture products [14]. Figure 2.2 shows the structure of the MAC address.



**Figure 2.2** MAC address [13]

The MAC addressing is used within the same Network or VLAN so devices within the same network can find and communicate with each other.

Communicating within layer two is based on MAC address called switching [15] where switching hardware based processing on the switches and it is done on a hardware called application-specific integrated circuit (ASIC) [16].

Switches or layer 2 devices read each and every frame that passes them and build a table based on the source MAC address of this frame this table has the source MAC address and the port that it reached on and by this way the switch will keep building its table until it has information about the ports that goes to all connected devices and in case there is no entry in the table for a certain device the switch will perform an operation called ARP [17] or Address Resolution Protocol where this protocol is looking for the translation between the IP address and the MAC address.

ARP will send a flood of MAC address request for the destination that the switch doesn't know its port to try finding this device, this request flood will go out of all the



switch ports except the port that the request has come from and the device with this MAC address will replay so the switch will add its MAC address and its port to the table so in the future if there is a packet destination toward this MAC address the switch will not need to perform a request flood or ARP.

ARP process can be a serious source of loops in the network where an ARP (in figure 2.3) is performed on all interfaces, the interfaces will send the ARP in their turn to the other segment so if there is cable loop in the switched network, the ARP will keep looping in the network making unexpected behaviors. This kind of loops called broadcast storm, and it can only be solved by a good planned design where there is no physical loops in the network and it also can be broken down by a layer three device, since the layer three devices separate the segment, so the flood from one segment will not be moved to the other segments [18] [19].

Hardware Type	Protocol Type	Hardware Address Length	Protocol Address Length	Option	Sender Hardware Address	Sender IP Address	Target Hardware Address	Target IP Address
---------------	---------------	-------------------------	-------------------------	--------	-------------------------	-------------------	-------------------------	-------------------

**Figure 2.3** ARP Packet

### 2.2.2 Layer 3 addressing (IP):

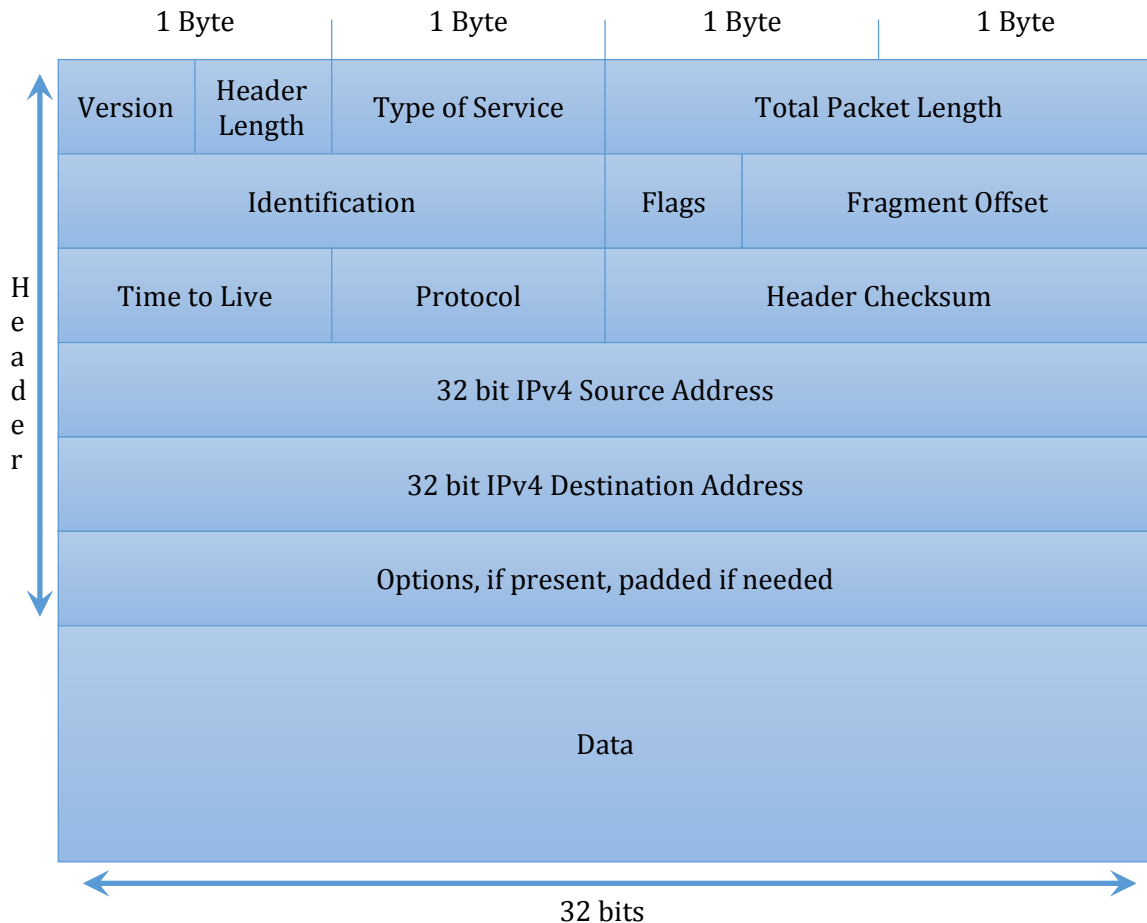
IP address is a numerical label [20] that used for each device in the network and IP addressing is working in the layer three of the network where routers and multi-layer switches function.

There are two main roles for the IP address, the first one is that it works as an identifier for the devices and hosts in the network, the other purpose of the IP address is that it works as a location separator for the segments of the network, so it has two parts, the IP address is to tell what we looking for and a subnet mask is to tell where we should look for it [21].

There are two forms of for the IP address, IPv4 and IPv6, in this chapter will try to focus more on IPv4 since we will work more closely on the IPv6 in the upcoming chapter.

The IPv4 is a 32 bits long address that is written as a form of xxx.xxx.xxx.xxx/y where x is a number between 0 and 255 since it is an 8 bits section of the IPv4

representing the network and y represents the subnet mask which is determining the size of the network so we can determine to which network this address belongs (host) [22].



**Figure 2.4** IPv4 header [21]

Unlike the layer 2 addressing (MAC address), where if the destination address is not in the table, a request flood or ARP will be generated, in IPv4 any request towards an IPv4 will be checked against the routing table.

The routing table is a table of all networks with their sizes (subnet mask) that the layer 3 device whether it is a router or a multi-layer switch can reach and know the path [16].

After a request has been delivered to the routing table asking for a path to a certain IP address, the router will match the destination IP address against its routing table and if it finds the network that the IP belongs to, it will then choose the best path toward this network (and by best path we usually mean the shortest or the least costly

path), if there are more than one match for the IP address in the routing protocol the router will choose the best match which is the network with smallest subnet mask [23].

If there is no match against the destination IP address in the routing table, the layer-three device will drop the packet declaring that it has no path toward this network [16].

There are two types of packets in the layer three or network layer of the OSI model, the first one is the data packets that are used to transport the data of the users and this type of packets come in many forms, the most famous of them is IP packets and there is also the IPX form of this packet [17].

The second type of the layer 3 packets is the route packet and this type of packet is used by the layer three devices as routers and layer three switches to build and maintain the routing protocols like EIGRP, OSPF and RIP where these routing protocols build the routing table [11].

There are many characteristics of addressing in layer 3 that layer 2 devices don't have:

- Layer 3 devices will not forward the broadcast as ARP by default which helps preventing loops and broadcast storms.
- Uses IP address instead of the MAC address [25].
- Layer three devices can manipulate the path for any giving path like changing the cost to reach it which is not possible to do in layer 2.
- Layer 3 devices can simulate the same functionality of layer 2 when needed but layer two devices cannot simulate the functionality of the layer three devices.
- Layer three devices can route Internetworking which transporting among different networks.
- Layer three devices can do quality of service which means queuing the traffic based on many criteria as the source IP address, the destination of the IP address or even the type of the application which are not possible to be done with layer two devices [24].

### 2.3 The need for two addresses

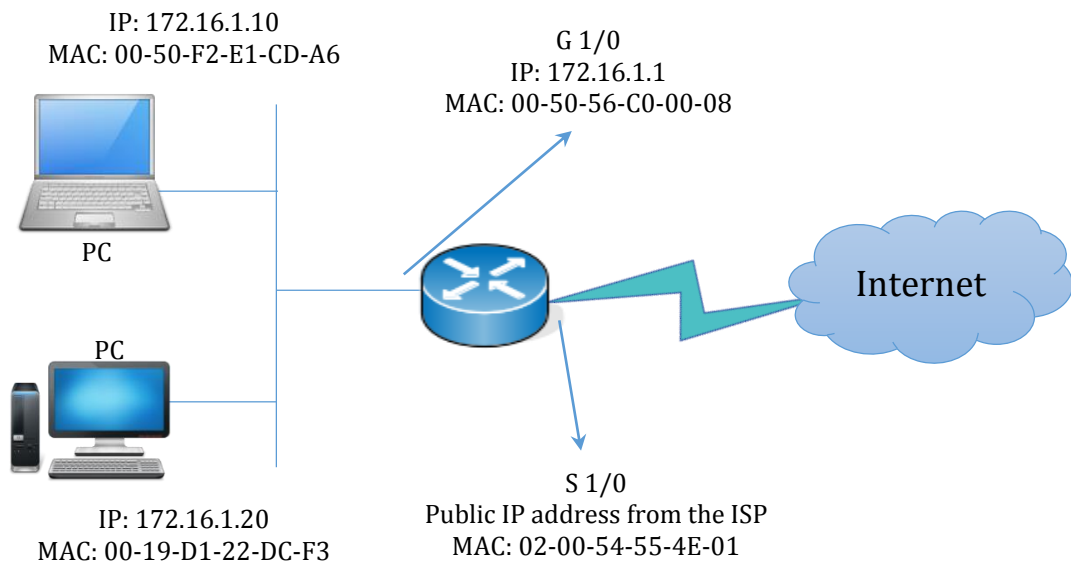
After understanding the basics of the MAC and IP addresses it is time to move on and ask: why do we have these two addresses?

At the Network layer, the logical address will be added to the packet. There are two IP addresses included in that packet which are the original source IP and the final destination IP. These IP address from start to finish will not change. As we move down to the Data Link layer where the physical address comes in, the MAC address will be added to the packet to allow local communication. When we go from end to end trying to reach our destination, we have to have two addresses one that defines locally where we go and the other defines the big picture of where we go. The MAC address from end to end will change all the time [26].

To fully understand the concept of two addresses let us assume that we have two scenarios:

#### 2.3.1 Scenario 1:

In this scenario let us say that we have a home network with two PC's each got an IP and MAC addresses and both are connected to a router running that network and connecting this home network to the Internet as shown in figure 2.4:



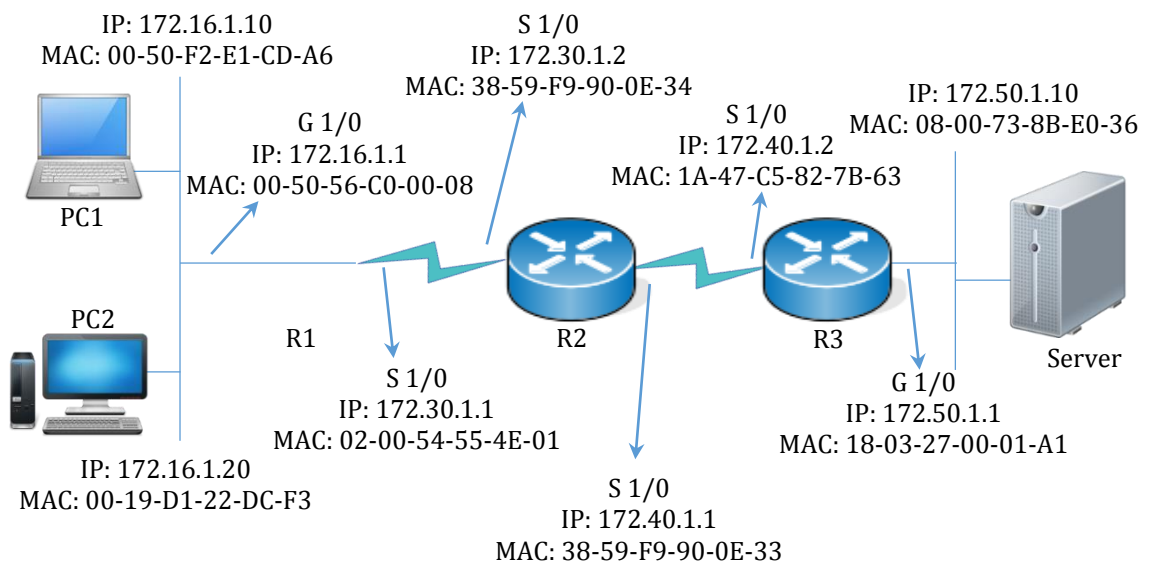
**Figure 2.5** A home network

The subnet mask of that network is 255.255.255.0, which means the first 3 bytes of the IP address represent the network and the fourth byte goes to the host. The central device of that network is the router. Its functionality is to figure out the route to the destination IP [25]. Once we leave the home network to the Internet, we will move on to a new network because the router is multiple networks. Every interface on the router represents a single network with unique IP and MAC addresses.

If host1 wants to communicate with host2, first thing it should do is comparing its IP with the IP of host2. Since they are on the same network (the same subnet mask), the PC1 will send an ARP to all devices. This ARP [13] broadcast contains the IP of PC2. Host2 will respond back to that ARP message with its MAC address. After getting the MAC, host1 will start transmitting data to that MAC address because computers communicate using only layer 2 addresses when they communicate locally [17].

### 2.3.2 Scenario 2:

It is more expanded, scenario2 has 2 PC's, 3 routers and a server as follows:



**Figure 2.6** A request across the Internet

When a host request the server which is across the Internet many routers away, the same first thing as in scenario1 will happen, the PC will compare its IP address with the IP of the server and immediately will recognize that they are on different

networks by checking the subnet mask. The PC can't use ARP to communicate with the server because ARP is a broadcast message and every device gets it, but one of the router's functionality is to stop broadcast [13].

So, the PC will ARP for the MAC address of its default gateway (R1). Default gateway is the IP address of the router that the host needs to go to when that host does not know how to get to the destination IP. After the MAC address of default gateway, the PC will send a packet including:

- Source IP address is of the host.
- Destination IP address is of the server.
- Source MAC address is of the host.
- Destination MAC address is of the default gateway (R1) [27].

The source and destination IP addresses will not change during that journey to the server, the MAC address will change frequently. When the router R1 checks the packet, it sees its MAC address and thinks that the packet is for it, but when it looks at IP address, it recognizes that the PC is trying to go through the router to reach the destination. Based on R1's routing table, it is not directly connected to the destination. R1 will send the packet to R2 putting its MAC as the source MAC address and R2's MAC as the destination MAC address without changing the source and destination IP addresses. R2 will do the same, it will forward the packet to R3 changing its MAC as the source MAC address and R3's MAC as the destination MAC address. R3 is directly connected to the destination IP address which is the server. R3 will deliver the request to that server putting its MAC as the source MAC and the server's MAC as the destination MAC address. Finally, when the server gets the packet, it will respond to the PC's request by making:

- Source IP address is of the server.
- Destination IP address is of the PC.
- Source MAC address is of the server.
- Destination MAC address is of the default gateway (R3) [27].

The same story will be repeated to the host.

## **2.4 Conclusion**

In this chapter we have discussed the network addressing in general. First, we have demonstrated the OSI model that divides the communication between two nodes into seven layers, two layers out of the total are responsible for addressing. Data Link layer is in charge of the physical addressing known as MAC address that is needed for the local communication, and Network layer that is answerable for the communication between Local Area Networks (LANs). Network layer addressing is IP. We have learned the structure of each one of the two addresses, the differences between them and why we need two addresses in the networking world because answering this question related to the main purpose of the thesis as we need both MAC and IP addresses in designing our campus.

## **CHAPTER THREE**

### **COMPARISON BETWEEN IPv4 AND IPv6**

When IPv6 first designed one of the most important things that has been taken in consideration is the compatibility between IPv4 and IPv6. Although they are not inherently compatible, but they can coexist in the same network. So there is no need to create new technologies from the ground to apply them with IPv6 for example all routing protocols that been dedicated for IPv4 had new versions where there is full support for the IPv6. Some of these protocols just updated the algorithm and way of working to fit the needs of IPv6 like OSPFv3 while other protocols' version of IPv6 has almost nothing in common of the IPv4 version except the name probably like EIGRP and RIPng [28].

There are many reasons that IPv6 is not widely deployed and accepted as:

The usage of Network Address Translation (NAT), probably one of the biggest reasons that IPv6 is not widely deployed since it allowed the using of not so big range of public IP address and some cases even on public IP address to go globally basically through making benefit of the ports so the same public IP address will be used by different users or applications to use the Internet and to differentiate the source of the request from which application or user a unique port number will be mapped with the public IP address [29].

It is not easy to fully understand the theory behind IPv6 and its application and start moving the network to it.

Financial reasons where deploying IPv6 means spending a lot of money and time updating the core network to support IPv6 that is nobody willing to do unless there is a real need for this kind of change.



So instead of deploying IPv6 widely, people and corporations start deploying it on a small scale and start merge it with IPv4 through many tunneling techniques as Teredo, ISATAP and Dual Stack.

To have a full picture of the differences between IPv4 and IPv6 we first need to understand the structure of each one of them, their header and packet format which will reflect the evolution that leads to IPv6, understanding the differences at the structure level between them will also help understanding the capabilities of each one of them and also the limitations that faced IPv4 and shaped the need for IPv6 and the applying challenges that face the spread of the IPv6.

To break down the differences between IPv4 and IPv6 we need to go first to the header of packet of each one of them since the header provides rich information about how the protocol works what its capabilities and its limits.

### **3.1 IPv4 header:**

We will start first with the IPv4 since it is the most common protocol and it bequeaths many of its characteristics to the IPv6.

The header of IPv4 packet is a 32-bit or four bytes length that makes the total available number of addressing is  $2^{32}$  which is 4294967296 addresses. Although this number seems a very huge number, but a big part of it will go to the private IP address which are the addresses that cannot be used or routed globally and it is for local or intranetworking usage only, the private IP addresses ranges are: -

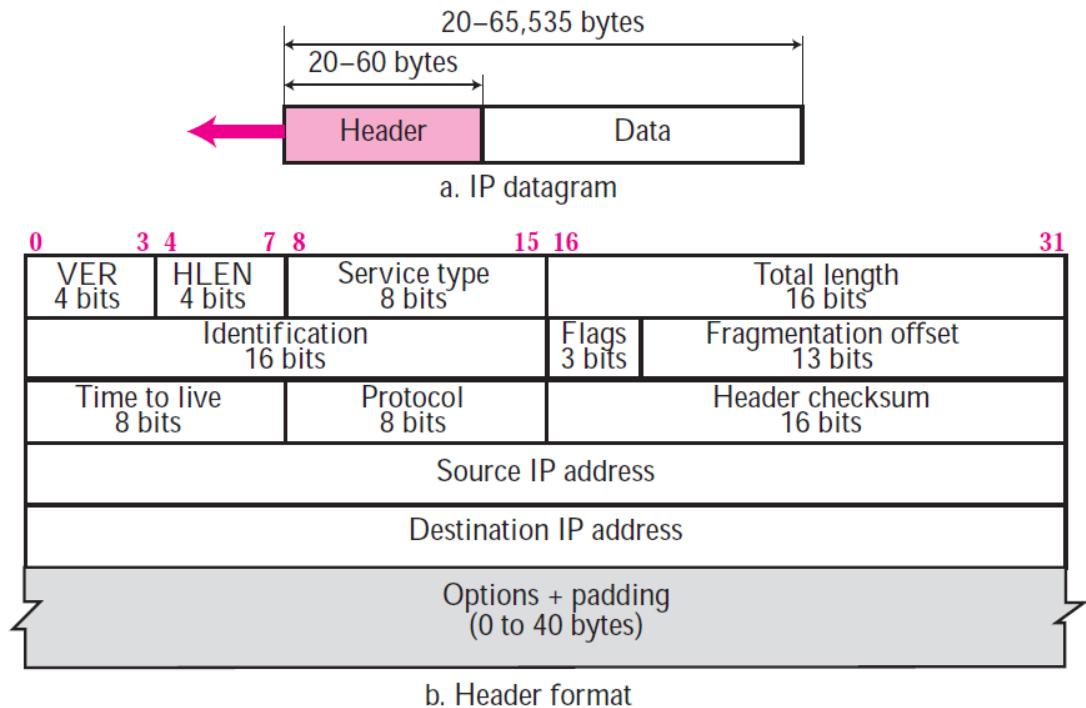
10.0.0.0/8 which has 16777216 addresses.

172.16.0.0/12 which has 1048576 addresses.

192.158.0.0/16 which has 65536 addresses.

So the total number of the private IP addresses ranges is 17891328, that makes the total number of IPv4 addresses that available for the global or routing usage is 4277075968 addresses [31].

IPv4 packet header has 14 fields from which the last one is an optional field and the other fields are mandatory [30].



**Figure 3.1** IPv4 datagram [31]

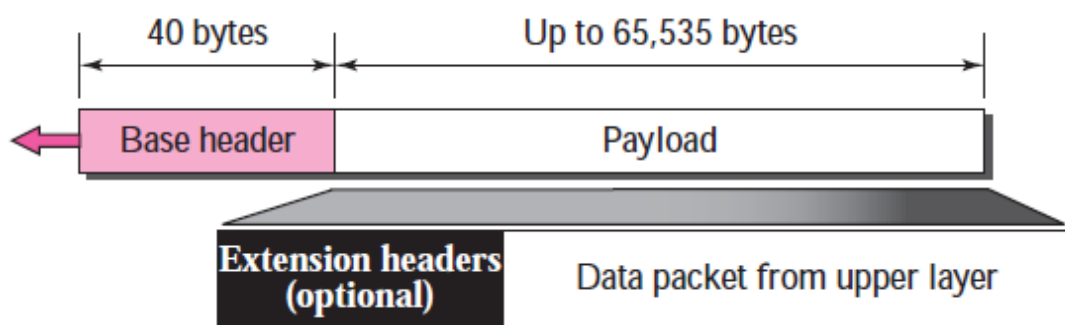
**The fields that make the IPv4 header are: -**

- Version: this is a 4 bits length field is defining the version of the IP which is IPv4 in this case [31].
- Header Length: it is a 4 bits field that refers to the end of the header and the beginning of the payload or data [31].
- Type of Services (TOS): this field determines the priority of the packet by determining the delay and reliability [32].
- Total length in bytes: it determines the length of the packet where the maximum packet size is  $2^{16}$  that is 65535 bytes.
- Identification: this two bytes field works with the fragmentation case where all fragments of the same datagram have the same identification number so the router will know that they belong to the same datagram when start assembling them again.
- Flag: this field is 3 bits wide and it works with fragmentation case where the first bit is reserved and must be 0, the second bit means do not fragment if it has been set to 1 and the last bit means more fragments on the way if it has been set to have the value of 1.

- **Fragment Offset:** this field is used for reassembly of the fragmented packet.
- **Time to Live:** is an 8 byte field that works as a loop prevention mechanism and that is why layer 3 don't have loops. The value that set by the sender is 255 and will decremented by each router that the packet goes through to be discarded when the value reaches 0.
- **Protocol:** a value that indicates the type of data that the packet carries like TCP or UDP, this field is 8 bits.
- **Header Checksum:** the function of this 2 bytes field that it looks for any errors in the header of the packet, so if there is any error found the packet will be dropped because it will represent a thread to the network.
- **Source and Destination IP Address:** these 32 bits each field determine the source IP address and the destination of the packet.
- **Options:** this field determines any extra options the header might have as time stamp and source route [31].

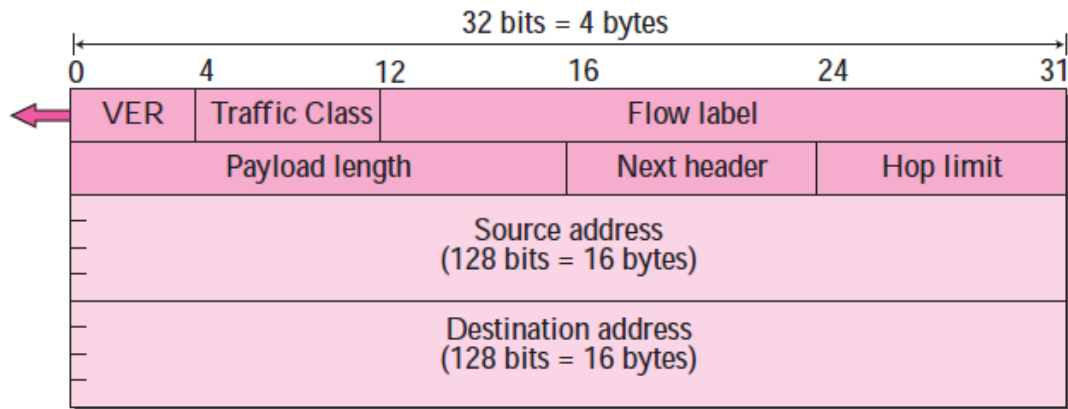
### 3.2 IPv6 header: -

The IPv6 packet consists of base header followed by the payload. The payload is composed of the optional extension headers and the data coming from the upper layer. The base header takes 40 bytes, while the extension headers and data contain up to 65,535 bytes of information [33].



**Figure 3.2** IPv6 datagram [31]

The IPv6 packet header is made of 40 bytes or 320 bits that has the bellow format:



**Figure 3.3** IPv6 base header [31]

**The fields of the IPv6 header are:**

- Version: it is a 4-bit field that has the fixed value of (0110) which represents the v6 of the IP.
- Traffic class: it is a one byte (8 bits) we can divide this field into two parts the first one that represented by the first six bits that is used for what called differentiated services or for packets classification, the remaining two bits representing a priority value that is used for congestion management [35].
- Flow Label: it is a 20-bit field that has two functions, the first function where its value is not zero to tell the switches and routers to keep the flow of the packet through the same flow or route. If there are many routes, so the packets will not reach late or be dropped. This function is important in the case of the real-time application like video streaming. The second function of the flow label that it helps detecting the spoofed packets [34].
- Payload length: it is a 16-bit two bytes field that gives information about the payload or the data that will follow the header including the extensions of the IPv6 packet. This field's value will be set to zero when there is a need to ad hop-by-hop extension making what called Jumbo Payload option.
- Next Header: 8 bits one byte length that specifies the type of the next header and it will be used usually to specify the transport or layer four information that used by the payload. If there are extensions to follow the

header this field will tell what type the next extension will be and it shares the same list of IP protocols that used to indicate the next extension with the IPv4.

- Hop Limit: 8-bits or one byte length field that replaces the time to live (TTL) and just like the way TTL works the value of this field will decreased by one every time the packet pass an intermediate device and the packet will be discarded when the value become 0.
- Source Address: 128 bits representing the sending source of IPv6.
- Destination Address: 128 bits represent the IPv6 address of the destination device or host [35].

### **3.3 Benefits of using IPv6 over IPv4**

The main reason behind the introducing of IPv6 is to fulfill the increasing need to the public IP address, where there was almost no more public IP address which leads to introducing of the Network Addressing Translation (NAT), with IPv6 there is no need to extend the range of public IP address by using the NAT since the size of the IP range has been increased from 32 bits in IPv4 to 128 bits.

More efficient when it comes to routing weather it is a static routing or through routing protocols that support IPv6 and the main reason is that routers will no longer need to fragment the packets which was making an overhead for the processing of the routers

Unlike IPv4 the Quality of Services (QoS) is built in to the IPv6 which makes a great tool to distinguish and priorities the patterns of the traffic while IPv4 has no such mechanism by default and it need to be configured which is not something easy to do.

There is a built-in Network Layer Security as IPsec which was not available in IPv4 making it a challenge to secure the network layer.

The introducing of Stateless Address Autoconfiguration where it facilitates the IP addresses assignment as an automated way which helped a lot of the complications of the IPv4 deployment.

Introducing the extensions feature into the header of IPv6 which helped improving the structure of the header with less processing and more efficiency, where there is no need to all the option fields in the header of IPv4. These headers were not used in most of cases, adding layer of complexity to the processing of the header and making the size of the IPv6 header unpredictable based on the attached options [36].

### 3.4 Unneeded fields in IPv6 header:

- Fragmentation: moving this field speeds up the processing of the IPv6 packet header since there is no need for fragmentation in the intermediate routers all the way of the traffic and the fragmentation can and will be done by the end routers that issue the packets, so only at the source and destination routers the fragmentation will take place.
- Checksum: there is no need for error checking at the network layer where IPv6 works because the transport layer which is layer four and link local which is layer two have their own error check mechanisms, beside that and because the IPv6 packet header has a Time TO Live (TTL) field the checksum should be performed in each router on the way which is a time and resourcing consuming process.
- Options: there is no place for the options in the IPv6 anymore and that helped fixing the size of the header to 40 bytes IP header, but it is still possible to add options through the extensions feature where the header will have the options in the next packet [37].

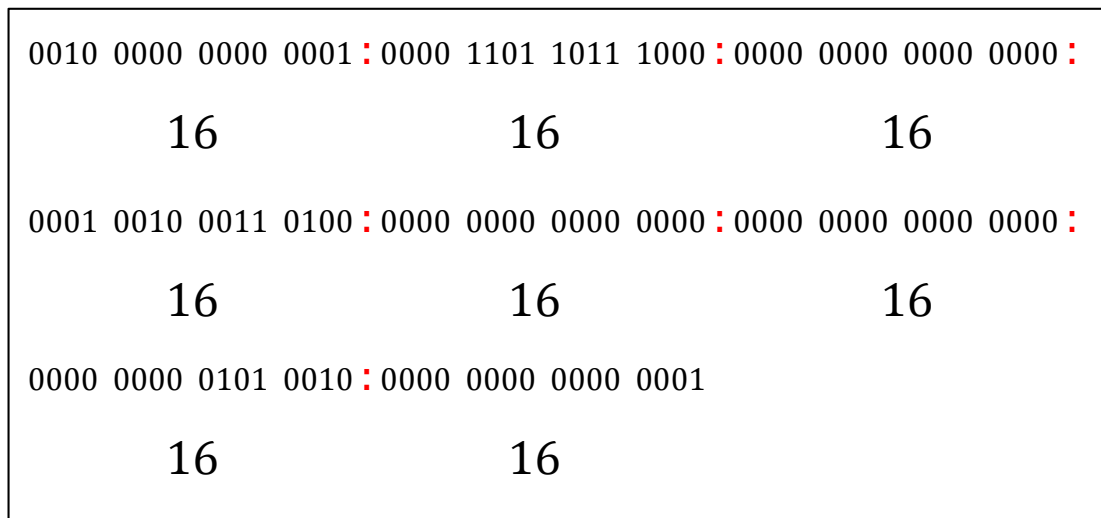
### 3.5 IPv6 address format

As IPv4, IPv6 consists of 2 parts the network and the host (host ID) differentiating between them by the subnet mask for example /64, /48 etc. IPv6 as we mentioned before is a lot longer than version 4 represented by 128 bits:

0010 0000 0000 0001 0000 1101 1011 1000 0000 0000 0000
0000 0001 0010 0011 0100 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0101 0010 0000 0000 0000 0000 0001

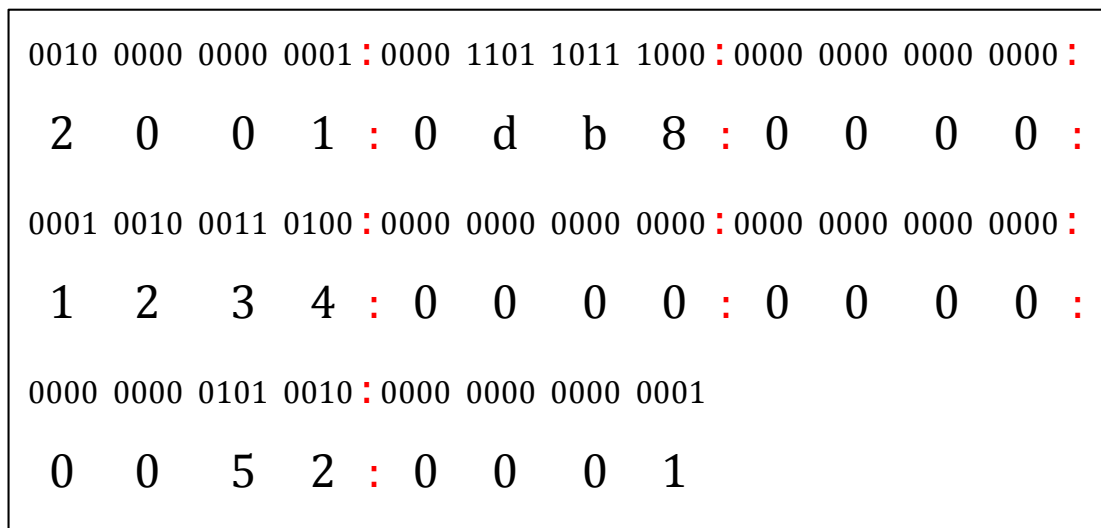
**Figure 3.4** An IPv6 in binary

IPv6 is 8 grouping of 16 bit each separated by colon:



**Figure 3.5** Colon to separate each segment of an IPv6

And represented in hexadecimal:



**Figure 3.6** A binary IPv6 mapped to hex

Where each nibble (4 bits) is represented by one hex character (0-9 and a-f or A-F are valid characters).

Shortcuts:

- Drop off the leading zeros:
  - 2001:0db8:0000:1234:0000:0000:0052:0001
  - 2001:db8:0:1234:0000:0000:52:1
- One double colon :: to represent successive groups of all zeros:

- 2001:db8:0:1234:0:0:52:1
- 2001:db8:0:1234::52:1

IPv6 is not case sensitive, which means that we write it as 2001:db8:0:1234::52:1 or 2001:DB8:0:1234::52:1 [40], [41].

### 3.6 IPv6 vs IPv4 addressing

IPv4	IPv6
Multicast address space at 224.0.0.0/4	Multicast address space at FF00::/8
Has broadcast address for all devices	No such concept in IPv6 (uses multicast groups)
Uses 0.0.0.0 as unspecified address	Uses :: as unspecified address
Uses 127.0.0.1 as loopback address	Uses ::1 as loopback address
Supports globally unique “public” addresses	Supports globally unique unicast addresses
Uses 10.0.0.0/8, 172.16.0.0/16 and 192.168.0.0/16 as “private” addresses	Uses FD00::/8 as unique local addresses

**Table 3.1** Comparison between IPv4 and IPv6

### 3.7 Types of IPv6:

#### 3.7.1 Link Local

This type of address is significant locally only the interface that it is on, so, that’s why this type of IPv6 addresses is not routable between interfaces, as well as it can be put on more than one interface at the same time and causing no overlapping since each interface will see itself as the only one with such IPv6. The format of the Link Local IP addresses range is FE80::/10. This kind of addressing is usually used by the control plane of the routers like the messages between IPv6 routing protocol and also by broadcast segments. When trying to reach a Link Local address it is so important to determine the outgoing interface since this IP might be exist on more than one interface



at the same time and reachability will be always dynamically calculated through ICMPv6.

Unlike the IPv4 which can separate its addresses into two parts the public addresses and the private address, IPv6 has many types of addressing and they can be divided down into:

### **3.7.2 Unique Local**

There was a range of IPv6 addresses that called Site Local which represented with the range of FEC0::/10 but it has been deprecated since nobody agreed about what is meant by a site or what are the boundaries of it, as a replacement the Unique Local addresses have been represented.

ULA addresses in IPv6 are the equivalent of IPv4 private address ranges, doing the same functionality and limited by the same roles so these set of addresses is not routable globally and it is used locally only.

The Unique Local scope of IPv6 addresses is a good way to start working with IPv6 even before assigning IP addresses by IANA (Internet Assigned Numbers Authority) which is responsible of managing and allocating of both IPv4 and IPv6. So after finishing the deployment of the IPv6 Unique Local we can move our network to IPv6 Global addresses by very simple steps.

### **3.7.3 Global Unicast Addresses**

This type of addresses is the equivalent of the public IP address range in IPv4 where it represents the globally unique addresses that is given away and registered by IANA and its regional offices. The range of the Global Unicast Addresses is 2000::/3 and although it is a very wide range making almost 1/8 of the whole IPv6 addresses pool, IANA gives away IPv6 with the range of 2001::/16 only. So far, there are other reserved sub-ranges within the Global Unicast Address as 2002::/16 for 6to4 tunneling.

### **3.7.4 Extended Unique Identifiers EUI**

Extended Unique Identifiers (EUIs) are 64-bit values assigned to physical interfaces. EUI has very similar nature to the MAC address as it is unique to the interface or the network card, so just like the MAC address changing the card will make a new EUI address the difference though is that the EUI can be routed globally, IPv6 uses the EUI to generate an automatic IP addressing on the shared segment, the way EUI works that the IOS will use the 48 bits MAC address as the core to create a 64 bit identifier for the host part of the IPv6 by flipping the seventh bit on the MAC address that called the Universal/Local (U/L) bit and then adding a 16 bits between the two parts of the MAC address these 16 bits are FFFE and will be right in the middle of the MAC address [38], [39].

### **3.8 IPv6 Auto-Configuration**

Although there is a DHCP version of IPv6, there is a feature called IPv6 Auto-Configuration as well that replaces a lot of the DHCP functions as it enables the host on the segment to have an automatic IPv6 address and to know the default gateway. IPv6 Auto-Configuration is using a special version of Link-Local and ICMPv6 in order to work, and just like the DHCP, this feature can be configured to be sent periodically or disabled. Auto-Configuration is disabled by default and can be enabled by using the command `no IPv6 nd suppress-ra` and the IPv6 unicast routing should be enabled also in order for Auto-Configuration feature to start [41].

### **3.9 Literature Review**

There are many works that tried to deploy IPv6 to a campus network in Turkey and we will demonstrate 3 of them as follows:

In the M.S. thesis [8], the main objective was to pass the necessary examinations of Muğla University campus network, apply IPv6 on server and reduce to a minimum the possible problems of other hardware and software by preparing the ground to smooth transition. There is a transition from IPv4 to IPv6 by assigning IPv6 to each department based on the IPv4 subnet as a first step. Full IPv6 support process of dual

stack is to Install IPv6 service. Then make a separate VLAN with an IPv6 address can also be provided to operate only with IPv6.

The author of [42] has developed (by using OPNET) a simulated environment network in order to measure the throughput of the routing performance analysis in current, transition period and finally IPv6 native networks. His major focuses include:

1. Significant differences, proposed superiorities and advantages of IPv6 to IPv4.
2. Measurement-based comparison, especially transaction mechanism, of IPv6 – IPv4 routing and IPv6 gains on a simulated test-bed environment (OPNET).

Another study about applying IPv6 on a campus environment has been done in Ege University. After close examination of the studies, the basic information about the transition to IPv6 and the transition mechanisms are given and some of the studies made about the transition to IPv6 in the world and also in Turkey are presented. In this context, the level of the current operating status for IPv6 in Ege University is also presented. In addition to the studies made, some steps to facilitate the transition to IPv6 and to optimize performance of IPv6 networks are also given in this thesis scope [43].

The difference between the three works mentioned above and our work is that we built our three campuses initially with IPv6 without any transition or adaptation to the existing IPv6 in addition to applying one of dynamic routing protocols which is OSPF to share the routing information between all campuses of the university of Turkish aeronautical associations.

### **3.10 IPv6 projects in Turkey**

#### **3.10.1 Design of National IPv6 Infrastructure and Transition to IPv6 Protocol**

TUBITAK (The Scientific & Technological Research Council of Turkey) has created this project with the coordinating of ULAKBİM and the participating of Gazi University, BTK (Turkish Information Technologies and Communications Authority) and Canakkale 18 Mart University. The main objective of the project is to draw a roadmap for the transition process to IPv6 to make suitable transition mechanism for different organization. Transition steps are planned by a timetable and solutions to transition problems in many terms such as security problems, financial analysis, technological researches, trainings, workshops and conferences.



used to establish a “honeypot network” within IPv6-GO to be used together to detect IPv6 attacks [44].

### **3.10.2 Turkey’s Plan for Public Sector's Transition to IPv6**

With the collaboration of ICTA (INFORMATION and COMMUNICATION TECHNOLOGIES AUTHORITY) and Ministry of Transportation and Communications, this project was published on 12.08.2010 by prime ministry circular. According to the project, governmental agencies must meet some predefined levels of supporting IPv6. In this context, ICTA follows the developments related to IPv6 transition in Turkey. The project has to be done in many stages:

#### **Stage 1** (January 1st, 2011 – August 31th, 2012):

Inventory analysis should be performed by governmental agencies to evaluate IPv6 support on the hardware and software. If the hardware and software do not support IPv6, the agencies should prepare a plan to renew the equipment. In addition, the annual budget should take the costs in the consideration. That agencies have to have IPv6 connections and IPv6 addresses and have to train their teams in “IPv6 Transition Training Center” which is formed by Turkish Academic and Technological Research Council of Turkey - Turkish Academic Network and Information Centre (ULAKBIM) or a “personnel licensing institute” in order to enable IPv6 services.

#### **Stage 2** (September 1st, 2012 – December 31th, 2012):

The Governmental agencies should make one of their Internet-based services IPv6- compatible as a pilot application.

#### **Stage 3** (January 1st, 2013 – August 31th, 2013):

The Governmental agencies should make all Internet-based services allowed to public access IPv6-compatible [45].

### **3.10.3 GEN6 - Governments ENabled with IPv6**

GEN6 is contributed to deploy IPv6 in the government area. The main objectives of this project are services improvement, societies strengthening, productivity and

welfare increasing, and democracy reinforcing by making EGG portal and as many as possible EGG services IPv6 enabled.

#### IPv6 Pilot in Turkey: eGovernment Services with IPv6

ULAKBIM (The Turkish Academic Network and Information Centre), TURKSAT and ICTA (Information and Communication Technologies Authority) agreed to enable IPv6 on eGovernment Gateway (EGG) of Turkey. This pilot will realize the “Stimulating IPv6 upgrades of public networks and e-Government services” goal of the specified call. Applying IPv6 will increase services offered by eGovernment Gateway (EGG) and increase public interest on this service. The proposed pilot is also in parallel with the “Turkey’s Plan for Public Sector’s Transition to IPv6”. According to the plan issued in December 2010, governmental agencies should make their all Internet based services allowed to public access IPv6 compatible until August 31st, 2013

Current status (October 2012):

Turkish e-Government Gateway has enabled IPv6 since May. Public Agency's Integration Box can run G2G and G2C Integrations. This is a hardware solution of simplifying all of the e-Government integrations. It supports IPv6. Negotiations with some institutions (PTT (The General Directories of Post and Telegraph organization), SGK (Social Security Institution) and ULAKBIM) are still in progress to have done the steps to make the connections between the institutions and TURKSAT IPv6 enabled [46].

### **3.11 Conclusion**

This chapter highlighted the differences between the two versions of IP address, explaining why IPv6 is not widely deployed and the methods that have been created to make IPv4 still alive even though it is depleted. Then we showed the structure of the two versions’ header deeply by discussing each field in the header. As well as

mentioning the advantages of IPv6 that make it a must to apply it these days due to the dramatically increasing in the devices that use the internet.

Then we have illustrated the format of IPv6 which looks the same as IPv4 when it comes to network and host parts differentiating between them by the subnet mask, how to separate between the 8 groups of 16 bit each, how to represent them and how to write IPv6 with shortcuts to make it easier to remember without mistakes. In addition, we went deep in discussing the typed of IPv6 and where and when we should use each type. Lastly, we have mentioned some works that applied IPv6 on a campus environment represented by three academic works on universities in Turkey, besides, the projects that the Turkish government has done in order to deploy IPv6.

## **CHAPTER FOUR**

### **DYNAMIC ROUTING PROTOCOL**

Before starting with OSPFv3 as the routing protocol that will be used for the practical part of this thesis, we need to explain first the reasons behind this choice.

The first reason of choosing OSPFv3 over the other routing protocols is that it is a link-state routing protocol [47], that means it is converging way faster than the other distance vector routing protocol like RIPng and EIGRPv6, this fast convergence [48] is due to the nature of this protocol where all routers in the same domain (the same area in the OSPF case) have to have the same routing database, which means each router has a full picture of its domain about all other devices within this domain, so in case of failure in any part of the domain the routers already have alternative paths through the network and there is no need for recalculations. While in distance vector routing protocol, routers learn the routing through what called learning by rumors [49], where the router knows only about his neighbor and so forth, so the router has no idea about the big picture of the network that is why distance vector as EIGRP and RIP have a loop possibility and using loop prevention mechanisms as split-horizon [50] and it is not the case with OSPF since OSPF can't suffer from loops because each router has a full map of its network.

The second reason for going with OSPFv3 over the other protocols is that it limits the advertisements within the domain by keeping them inside the area only and routers within the area don't care what is going on outside the area and need only a gateway to leave the area that we can consider the OSPF routers within that area with the other routers outside it as a distance vector way of acting.

The third reason for the OSPFv3 usage in this thesis is that it is inherited from OSPF of IPv4 which means OSPFv3 can be used with both IPv4 and IPv6 which is



not the case with the others routing protocol like RIPng and EIGRPv6 that considered totally different from their IPv4 versions and they provide no compatibility between IPv4 and IPv6 since their structure and communication algorithms are different from their IPv4 versions.

Another reason to go with OSPFv3 is that it is a standard protocol supported by all vendors unlike EIGRP which is a cisco proprietary, although cisco announced that it will standardize the EIGRP but it is still ongoing work [52].

Unlike the distance vector routing protocol that made up their decisions based on the advertisement from their neighbor as we mentioned early, OSPF uses the state of its interfaces to create a full map of the network. The information that the OSPF collects is related in one way or another to its interfaces status like the IP address on the interface that connects the neighbor, the type of the network between the two neighbors weather it is a shared segment or point-to-point network , the mask of the network and so on, all this information will be gathered up by various types of advertisement messaging, types that called link state advertisements (LSAs) [53] and these advertisement will be stored in the LSA database where the dijkstra [51] or shortest path first algorithm will use them to build an OSPF database. The OSPF database is not the same as the routing table since it has all the network paths and probabilities. Based on the database table the routing table will contain only the best path to reach each network and if there is any change in the network it will be reflected as a change on the database and finally a change on the routing table.

#### **4.1 OSPFv3 vs OSPFv2**

As we mentioned when it comes to covering the reasons behind going with OSPFv3 for this thesis that OSPFv3 is inheriting a lot of its features and way of calculation from the previous OSPFv2 that was dedicated only for IPv4 while the new OSPFv3 support both kind of addressing IPv4 and IPv6, it is covered in the RFC 5340 [52].

Unlike OSPFv3, an OSPF process needs to be created explicitly.

In OSPFv3, a routing process does not need to be explicitly created. Enabling OSPFv3 on an interface will cause a routing process, and unlike the OSPFv2 where

we can use the network command on the global configuration mode that can enable the OSPF on all interfaces that have IP addresses within the range of the network command, in OSPFv3 we need to add the interfaces one by one. In case of using the non-broadcast multi-access NBMA network in OSPFv3 we need to provide the router with the list of the neighbors manually with their router id or device id [55]. Unlike IPv4 where the interface can have only one IP address, the interface in IPv6 can have more than one IPv6 address weather with different types of addressing like one global unicast address and one link local address or even two or more global unicast addresses, the thing that with enabling OSPFv3 on the interface, the OSPF process will be enabled for all the addresses on the interface and we cannot control enabling on part of the interface addresses only. Another difference between OSPFv2 and OSPFv3 is that with OSPFv2 the interface can belong to one and only one instance while the same interface with OSPFv3 can have multiple instances of OSPFv3. The procedure of choosing the router id that will be attached to the OSPFv3 is the same that is used by OSPFv2 which is preferring the loopback interface address over any other addresses and if there is more than one loopback on the router the highest loopback IP address will be chosen, if there is no present of loopback interface on the router the highest IP address on any interface on the router will be chosen is the router id [54].

## 4.2 LSAs

Link state advertisements are the most OSPF significant feature that helps shaping the OSPF database and routing table, the LSAs come in variety of types as following:

- Router LSAs (type 1): this LSA describes the link state within the area and its cost to reach each router in the domain which is the area in this case that is why the area is the boundary of this type of LSA and cannot be sent out of the area. This LSA tells weather the router is an area border router (ABR) which is a connector between two different areas or autonomous system boundary router (ASBR) which connects an OSPF area to another routing protocol or just a normal router inside the area who has no neighbors outside its area. Type 1 LSA is used to advertise the stub networks or which is the network that has a dead end and has

only one way out. In OSPFv3, these LSAs have no address information and are network-protocol independent [56].

- Network LSAs (type 2): This LSA gives information about all routers in the area and the cost to reach one of them, it works like combining all LSA type 1 in one LSA and it is done by the designated router of the area so all routers within the area will send their LSAs type 1 to the designated router DR and the backup designated router BDR and the DR will combine them and start publishing LSA type 2 if the DR is down the BDR will take its function [57].
- Inter-area-prefix LSAs for ABRs (type 3): it is also called summary LSA. This type of LSA is advertising the networks of the area to other areas and this advertisement can be in a form of single summarized network or in a form of detailed network and it is done by the area border router (ABR) which has at least interfaces in two different areas and area 0 has to be one of them.
- Inter-area-router LSAs for ASBRs (type 4): this LSA works like a guide for how to leave an OSPF domain to another domain or routing protocol since it shows the way to reach the autonomous system border router (ASBR) which is the router that has connections to the OSPF domain and another connection outside the OSPF domain to another domain or another routing protocol so it works as a gateway for the OSPF domain. This LSA will be generated by the ABR telling the path to the ASBR so routers need to send traffic outside the OSPF domain have to choose the shortest path to the ASBR.
- Autonomous system external LSAs (type 5): this LSA type injects routes from external domains like another routing protocol into the OSPF domain and it is done by the ASBR, the networks that will be included are represented as the IP address with the length of the network, the default route will be with a 0 as its length.
- Not-so-stubby area advertisements (type 7 LSA): this special type of LSAs is used with one type of stubby networks called not-so-stubby area and its function is to inject the external routes into the area then these routes will be converted to LSA type 5.

- Link LSAs (type 8): this LSA is existed only with OSPFv3 and it works within the link-local boundaries, its function is to give away the link local address of the router to the other devices on the same segment of the network and telling them the networks that associated with this address, it also provides the options that might come with the IPv6 link local addresses.
- Intra-Area-Prefix LSAs (Type 9): A device can originate multiple intra-area-prefix LSAs for each device or transit network, each with a unique link-state ID. The link-state ID for each intra-area-prefix LSA describes its association to either the device LSA or the network LSA and contains prefixes for stub and transit networks [57].

OSPFv2 LSAs type and name	OSPFv3 LSAs type and name
1 Router	2001 Router-LSA
2 Network	2002 Network-LSA
3 Summary-Network	2003 Inter-Area-Prefix-LSA
4 Summary-ASBR	2004 Inter-Area-Router-LSA
5 AS-External	4005 AS-External-LSA
7 NSSA-External	2007 NSSA-LSA
	0008 Link-LSA
	2009 Intra-Area-Prefix-LSA

**Table 4.1** LSAs

The concept behind using the areas with OSPF provides many benefits to the network as: -

It limits the problem of large number calculations of the shortest path first (SPF), especially if the domain contains a lot of routers so any change with any router in the domain will trigger a change notification making all routers recalculating the whole SPF algorithm which can consume time and CPU recourses so the areas will limit the changes to the routers within the area boundaries only affecting none of the routers out the area.

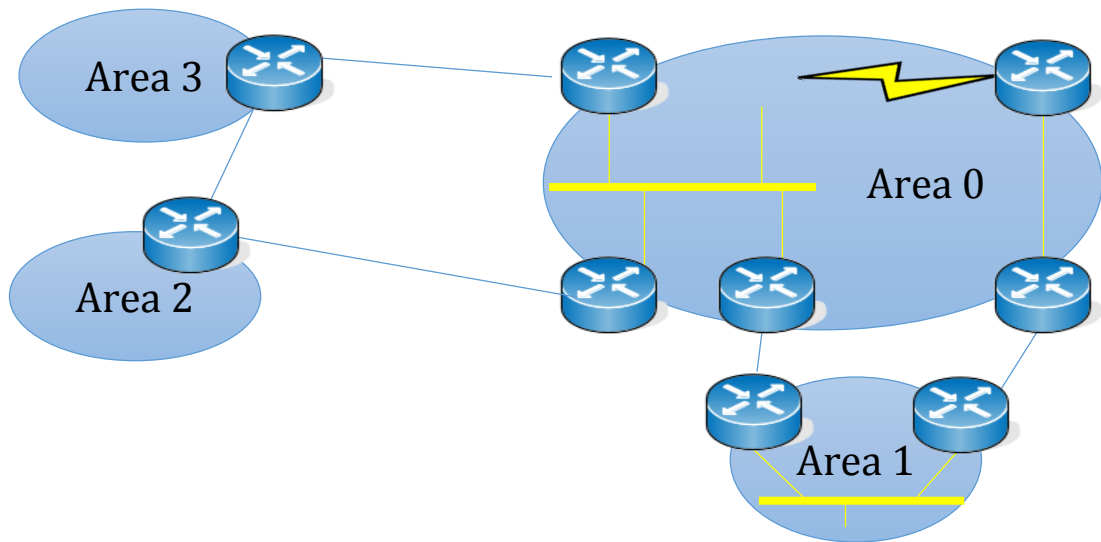
Large routing table: with one large domain and since link state routing protocol have to have a full picture of the network every routers have to maintain a very large

routing protocol where it has to have at least one entry for each other router or connection in the domain. With areas concept the routers will have a routing table only for the routers within their area and not caring about the routers and networks outside it since they have a gateway to transfer data outside the area.

Large link-state table: the same case here comparing to the routing table where all routers within the domain have to have a full database table or link state table and this table is even bigger than the routing table and it makes the pool that the routing table selects its best paths from, by applying the areas each area will have a separated and shorter version of the link state database [58].

For all the above reasons the big domains of OSPF has been divided into smaller domains that called areas yet these areas still can exchange the information among them [59].

This nature of multi-area, supported in OSPF, enhanced the hierarchical nature of the routing protocol where enlarging the routing domain is no longer a big problem since it is all done within an area that makes small part of the domain not the whole domain which helps at the end of the day to have a very controllable, customizable and efficient inter-networking. Figure 3.1 shows the concept of areas in which inter-area routing is still doable and the resources consuming processes as the link state calculation and SPF algorithm is done only within the area itself. As per the figure 3.1 if area 1 for example has some flapping links then the link state calculation will be done only in area 1 while other areas still having their way to reach area 1 and don't care what is going on inside area 1 [58].



**Figure 4.1** Areas nature of OSPF

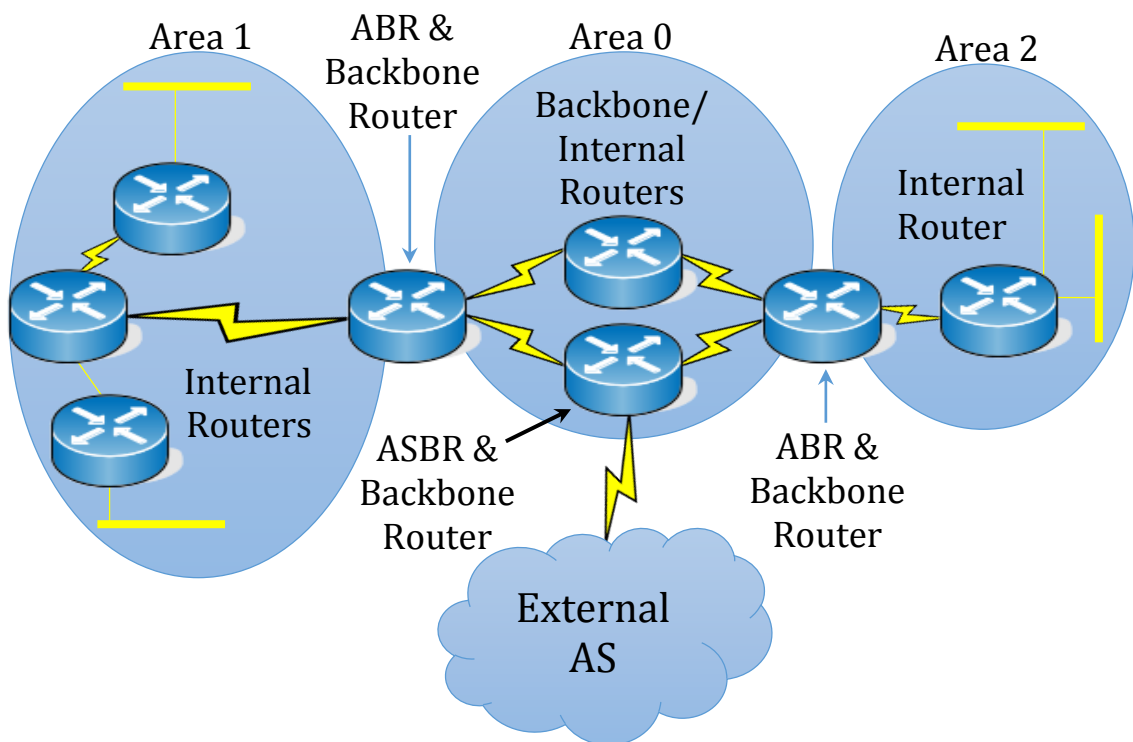
### 4.3 Types of routers in OSPF

Different types of OSPF routers as in figure 3-2 below control differently how traffic is passed to and from areas. The router types are as follows:

- Internal routers: these are the routers that have all their connections or interfaces in the same area so they share the same link state and routing table and the LSA type 1 of each one of them reach the others internal routers, and they all send their type 1 LSA to the same DR which returns issue LSA type 2 to all of them.
- Backbone routers: they are the routers that set within area 0 which is the backbone of any OSPF domain where any OSPF has to have area 0 and all other areas have to have a connection to area 0 so this area will work as a transit to all inter-routing traffic.
- Area border router (ABR): these are routers that have interfaces attached to multiple areas and at least one of these interfaces has to be in area 0. These routers have to keep a separate link state database for each area they have link into while they will have one routing table and route traffic destined to or arriving from other areas. ABR works much like a gateway for the area so any traffic destined to another area or coming from outside the area to the area has to go through the ABR. ABR can summarize the networks of the area and send them to other areas as a summarized

network or keep them separated and more detailed. An area can have one or more ABR.

- Autonomous system boundary routers (ASBR): these are routers that have at least one connection or interface into another autonomous system as another OSPF domain or another routing protocol on the other hand these routers have to have a connection inside the OSPF domain and the main function of this type of OSPF routers that they inject or what more referred to as redistributing network from outside the OSPF domain into the domain [59].



**Figure 4.2** types of routers in OSPF

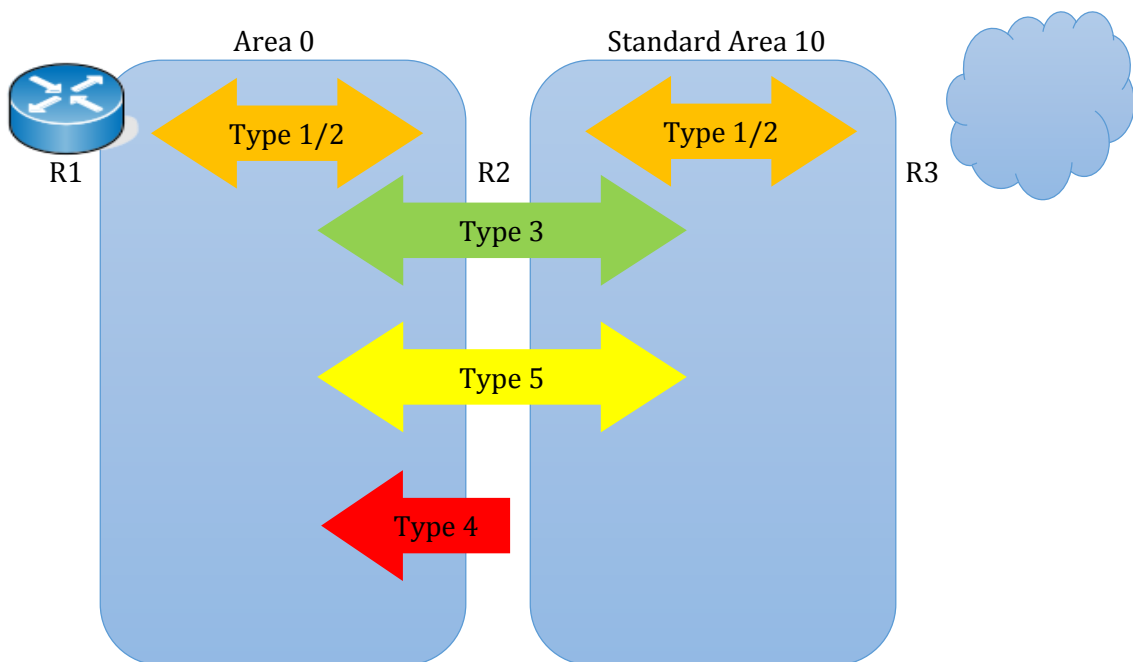
A router in OSPF can have more than one role, for example if we have a router that is connected to area 0 and to another area and at the same time connected to another autonomous system in this case this router will be considered as backbone router because it has a connection in area 0, it will also be an ABR since it has connection into two different areas and area 0 is one of them and it will also be an ASBR because it has a connection into outside of the OSPF domain which is another autonomous system. A router has a separate link-state database for each area it is connected to and

this router will have a separated link state database to each area which will share through LSA type 1 with the routers of that area only [58].

#### 4.4 Types of areas in OSPF:

The type of an area determines the type of traffic and LSAs that the area will allow and there is special characteristics for each area, the OSPF whether it was OSPFv2 or OSPFv3 has the following area types:

- Standard area: this is the normal and the most common type of areas in OSPF, this area has and allows both the intra and inter routing with all normal LSAs.

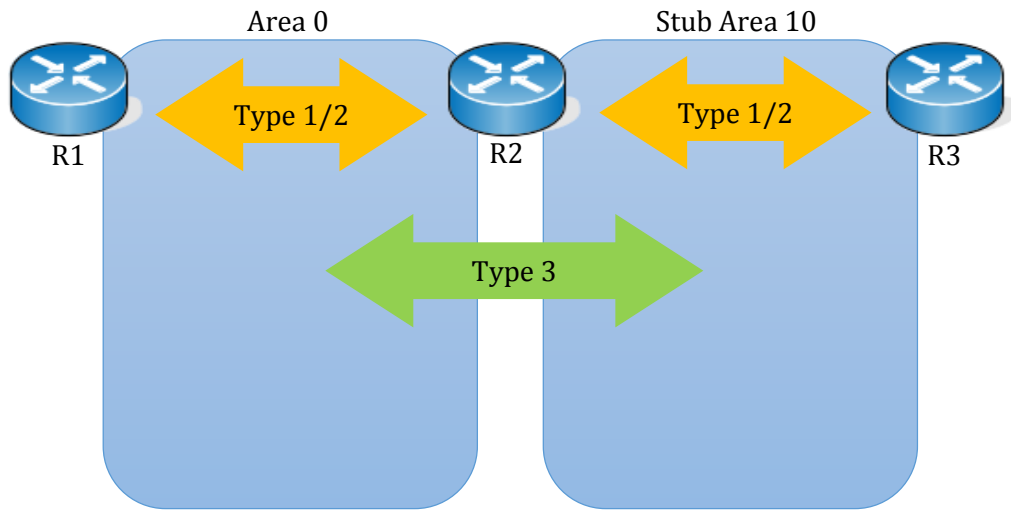


**Figure 4.3** Standard Area with LSAs

- Backbone area (transit area): in case of having a multi-area scenario the central of the domain has to be area 0 where all communications between the areas have to go through area 0 by default (although this feature can be disabled). Beside its transiting functionality area 0 can serve as any other standard area.
- Stub area: this is the area that doesn't accept any advertisement regarding network out of the OSPF domain like non OSPF routing protocols. This area has one way out to the outside that is why it only needs a default

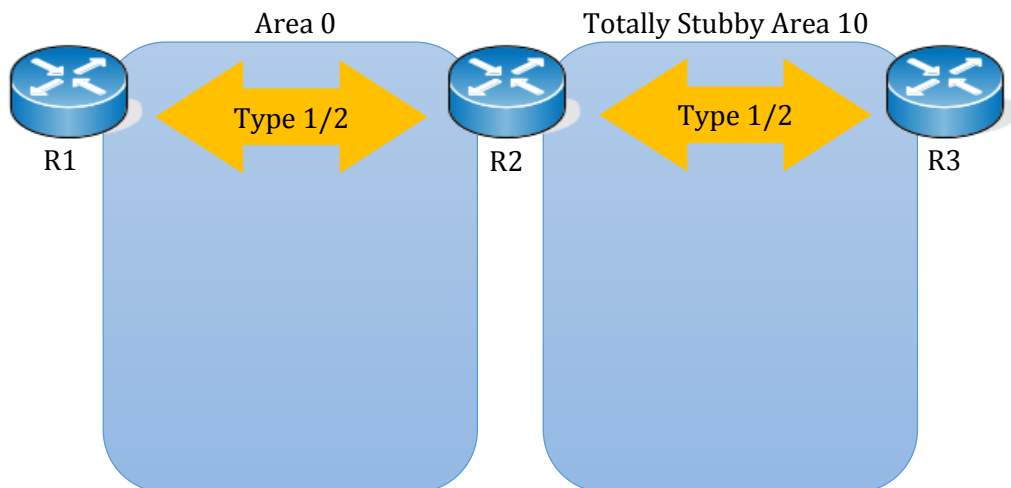


route 0.0.0.0/0 or ::/0 in the IPv6 version telling about the way out of this area.



**Figure 4.4** Stub Area with LSAs

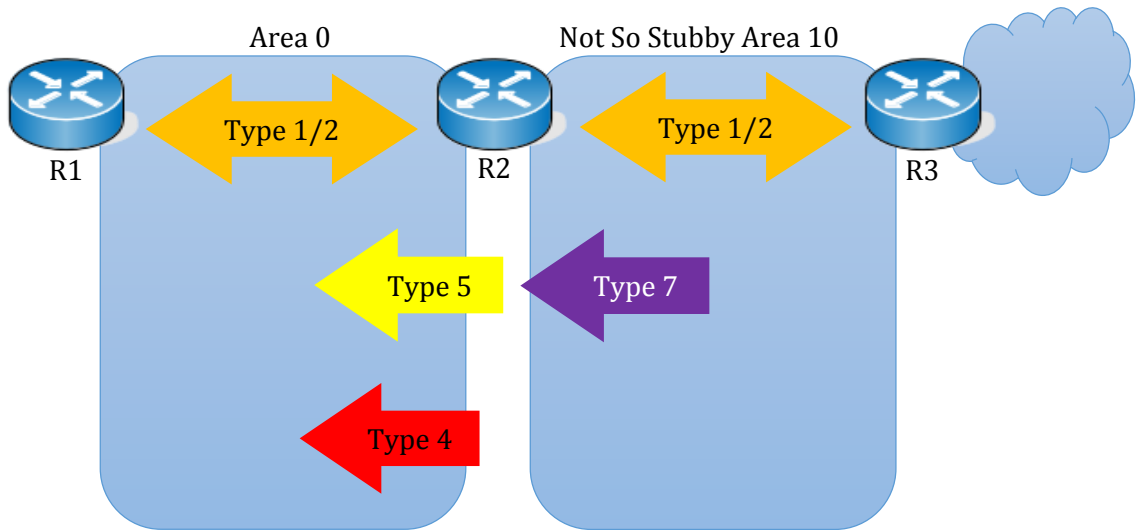
- Totally stubby area: this area type has the same characteristics of the stub area in the way that it doesn't accept any advertisement from another autonomous domain; in addition to that it doesn't accept an advertisement from another areas or LSA type 3 so the only way out of this area is through default route. This type of areas is a cisco proprietary area type and cannot be found or configured on non cisco devices.



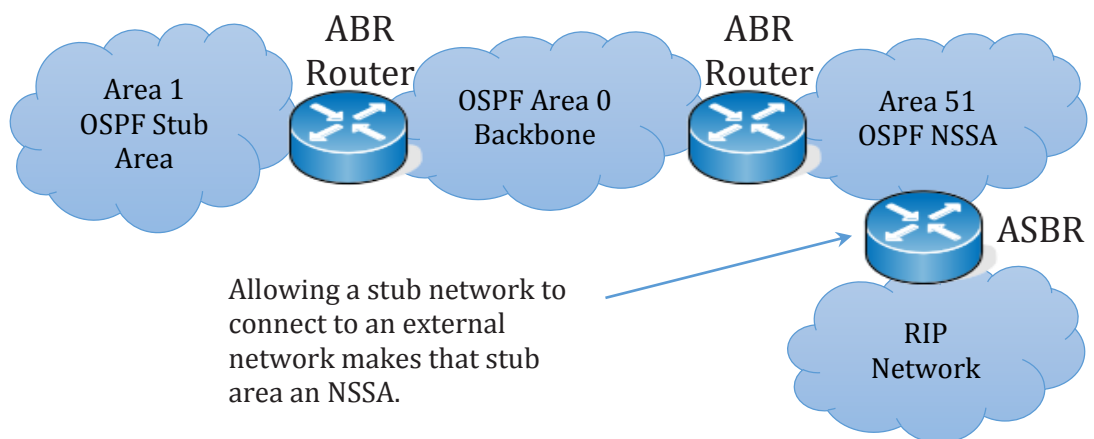
**Figure 4.5** Totally Stubby Area with LSAs

- Not-so-stubby-area—a not-so-stubby area imports a limited number of external routes. It works like the so-stubby-area but in addition it allows

the distribution of some external routes that provide inter-area connectivity as LSA type 7 and it allows the advertisement s from other areas through LSA type 3.



**Figure 4.6** Not So Stubby Area with LSAs



**Figure 3.7** NSSA Topological Example [60]

Area type	LSA1	LSA2	LSA3	LSA4	LSA5	LSA7
Backbone Area (Area 0 )	Yes	Yes	Yes	Yes	Yes	No
Standard Area	Yes	Yes	Yes	Yes	Yes	No
Stub Area	Yes	Yes	Yes	No	No	No
Totally Stubby Area	Yes	Yes	No	No	No	No
Not So Stubby Area	Yes	Yes	Yes	Yes	No	Yes

**Table 4.2** LSAs and OSPF area types

#### 4.5 Conclusion about the characteristics of OSPF

- It is a link state routing protocol which means every router has to have a full map about all the other routers in the domain.
- It uses the area concept where all the routers within the area have to be on the same page which means they all have to have the same image of the network.
- Because of its link state Nature it is faster to converge than distance vector routing protocols as EIGRP.
- It uses the bandwidth as the metric where decision is taken based on the total cost. The lower cost the better path.
- It support authentication.
- It supports VLSM.
- Doesn't require high resources of bandwidth and processing.

It is a little bit slower than the distance vector routing protocols when it comes to building the database at the beginning of its work due to its nature where every router need to know about all the routers in the domain [58].

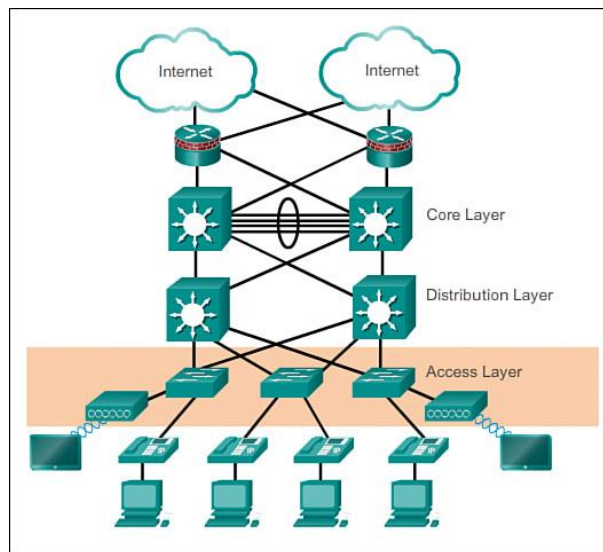
This chapter has discussed the dynamic routing protocol we used in the practical side of the thesis which is Open Shortest Path First (OSPF) to share routing information between all the devices in our simulated campus. A lot of reasons led to make the choice of OSPF over other routing protocols as we mentioned in this chapter. Technically, we started to explain the differences between two versions of OSPF, version two of IPv4 and version 3 of IPv6. Then, we showed the nature of OSPF in sharing the information using Link State Advertisement (LSA) and the types.

We also stated the types of the router in OSPF and their role in the networking environment. In addition, we explained the types of the areas that OSPF may contain and the kinds of LSAs each area may use.

## CHAPTER FIVE

### THE EXPERIMENTAL WORK

This chapter will make the capstone of the thesis, since it will grasp the information that been covered in all previous four chapters in one chapter in a practical way. Cisco usually advises of using its campus hierarchy especially in the multi-building environment, this hierarchy divides the network logically into three main layers [61]:-



**Figure 5.1.a** Cisco campus hierarchy

The Access Layer: - and this is a layer 2 switches in most of cases (also we can find a layer 3 devices belongs to this layer in the very large campuses like Google campus and AT&T), the main purpose of this layer that it makes the end-users interface into the network where they connect their devices directly either through wired or wireless type of connection [61].

Users in this layer will have no direct connection to other users and devices out of their network or VLAN scope and to be able to forward the traffic among the different VLANs and networks on the access layer traffic needs to leave the access layer to reach an upper layer three level of the network.

The Distribution Layer:- this is the layer where the layer 3 routing will usually take place so in order for two different users in two different logically separated networks or VLANs to communicate with each other their traffic need to leave the layer two access layer and reach the layer 3 distribution where the distribution layer devices usually a layer 3 switches have the inter-VLAN routing ability [62], after traffic from the access layer switches reaches the distribution layer, the distribution devices will forward the traffic toward the third layer which is the core layer [61].

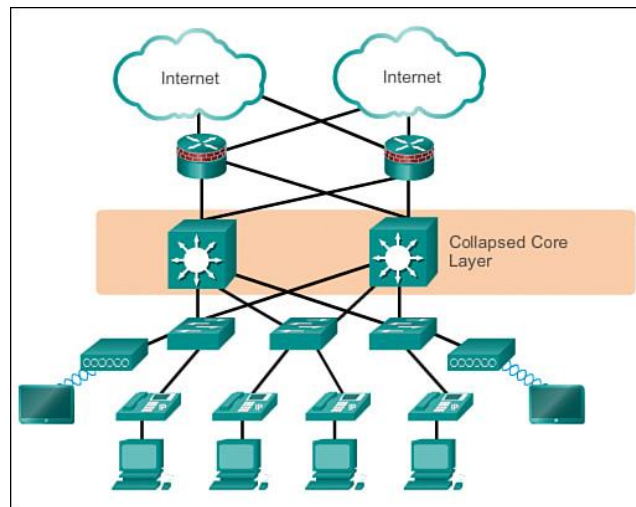
In some environment (especially the not so big campuses) we can find the distribution layer as a layer two instead of doing a layer 3 inter-VLAN routing so the whole function of this layer will be organizing and facilitating the transition of the traffic from layer 2 access layer to layer 3 core layer. In some cases there is no physical existence for this layer and can be merged into core layer which will be the case of this thesis due to the small size of the network so adding a distribution layer will only add money consumption and a complexity and providing not that much of benefit in return.

The core layer: - and this layer is the most critical layer of the network (where every environment no matter how big or small it is) should have it, because it is responsible for transforming the traffic from layer 2 (within the one network or VLAN) into inter-VLAN (between networks and VLANs), so this is the layer that will carry the traffic out of our campus and connect it to the world [61].

Devices in the core layer have to be a layer 3 devices like routers and multi-layer switches, and the heart of the core layer will be the core switch which is a layer 3 switch that will do the inter-VLAN routing and will carry the routing protocols between the different geographical sites and buildings of the campus, from a hardware point of view the core switch has to be strong enough, has a high processing capability to handle the whole campus traffic and does the processing and traffic engineering [63].

Since the campus that we are trying to simulate is relatively small, there is no crucial need for a distribution layer and we can merge it into the core layer, so we will

end up having an access layer which is a layer 2 with access switches and a layer 3 which is a core switch and Internet router.



**Figure 5.1.b** Cisco campus hierarchy

### 5.1 GNS3:

Our network environment is virtualized by using GNS3 (Graphical Network Simulator) that is an open source emulation tool in which we can create our campus network. GNS3 allows us to add different kinds of network devices, connect them together and configure the devices with Command Line Interface (CLI) that is very similar to Cisco IOS or other network vendors. In addition, GNS3 gives us the opportunity to connect our simulated topology to the Internet directly because it supports all features that exist on Cisco devices [66].

### 5.2 The Design of our Campus Network

The University of Turkish Aeronautical Association has three geographically separated campuses with the one in Ankara as the main one, the second one is in İzmir and the third campus is in Eskişehir.

The first campus we will cover is the Ankara one, since it is my campus and I have no enough information about the other campuses so we will consider them as the same when it comes design and layout.

I will try to apply Cisco campus hierarchy on the current campus with IPv6 as the layer 3 addressing carrier. To be able to grasp the final structure of the network we

need to divide it into two components the physical layout of the building and the virtual network and the mapping between them.

First of all we will start with the physical aspects of the campus:-

### **5.2.1 The Buildings: -**

The campus has many buildings but not all of them will need a wired network (as the cafeterias, the restaurant and the gym), that will leave us with five main buildings to be included in the master design: -

- Engineering building: - it consists of two floors where the first floor has two labs with 40 computers each, and a couple of administration offices so in total this floor needs around 86 ports which is 4 layer two switches to cover (as each switch has 24 ports).

The second floor is exactly the same story with 4 switches also.

- English language building: - it has two floors as the first one has classrooms with almost 90 ports to cover them which make it needs 4 switches.

The second floor has faculty offices and needs around 160 port to cover which means 7 switches to cover.

- Administration building: - it has two floors as well, the first one of them has beside a lab two classrooms and offices with around 84 port which means 4 switches to cover.

The second floor has only offices with 4 switches to cover.

- Aeronautics and Astronautics engineering building: - it has three floors that share the same layout with around 80 ports to cover each of them which means 4 switches in each floor.
- Library: - it is a one floor building with one switch to cover.

In total we will have 40 switches that will make the backbone of our access layer and each of them will have two type of connection: the first connection is the Ethernet



connection through STP (Shielded Twisted Pair) cables as CAT6 and this connection will cover the side between the access switch and the end user.

The second connection will be a single mode fiber connection, since it is the most popular form of fiber connection to connect the access layer switch from all over the campus with the core switch.

### 5.2.2 The functionality of the devices: -

The Access Layer Switches:

As we mentioned before, we need 40 access layer switches that make the interface between our core network and the end users.

These switches are doing the layer two switching which means they handling the intra-VLAN traffic and will be spread all over the campus in an equal fashion, so the places with higher people density will have more switches to provide the needed port capacity as the table shows:

Building	Floor	No. of ports	No. of switches
Engineering Building	Ground floor	86	4
Engineering Building	First floor	91	4
English Language building	Ground floor	90	4
English Language building	First floor	160	7
Administration building	Ground floor	84	4
Administration building	First floor	84	4
Aeronautics and Astronautics Engineering Building	Ground floor	80	4
Aeronautics and Astronautics Engineering Building	First floor	80	4
Aeronautics and Astronautics Engineering Building	second floor	80	4
Library building	Ground floor	3	1

**Table 5.1** No. of Switches for each Building

After designing the access layer it is always a good practice to group access layer switches in Stacking so up to four switches (connected by Stack Wise Port) will make a one logical switch. Only stackable switches can make a stack.



**Figure 5.2** Switch Stacking

The benefit of stacking the switches together can be illustrated in two points:

It is always easier to handle less number of switches, so by virtualizing the switches to 25% of the number of the physical switches (since the stack can connect up to four switches).

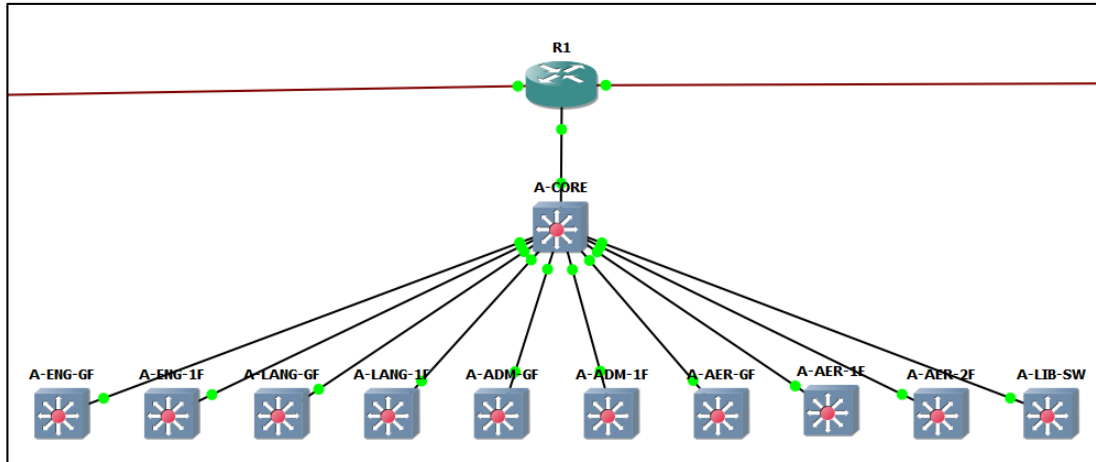
It will facilitate the connection of the switches with the core switch which is in most of the cases in another building so instead have a one uplink connection between each physical switch and the core we will need only one connection between each stack and the core, so that will reduce the between-building cabling by 75% [64].

Now the access layer switches will have, as we mentioned before, two types of connections:

Fiber optics connection between the core switch and each stack of the access layer switches, this connection will be a single-mode fiber since it is the most popular form of fiber connection and can be laid for a very long distance and can resist all the harsh environment conditions.

Ethernet connection between the access layer switches in each floor and the end users' ports, there is a critical factor to be taken in considerations that is the Ethernet cannot carry the data longer than 100 meter that is why the placing of the stack in each floor should be calculated carefully.

We will end up having the following topology representing the campus of Ankara:



**Figure 5.3** Ankara campus topology

Starting from the top down, the router R1 is to connect our campus to the ISP as well as to İzmir and Eskişehir campuses respectively. We configured it as “Router on a Stick” that enables a trunk between the router and the core switch in order to send all VLAN traffic by dividing one physical interface on the router into sub interfaces as the same number as the VLANs. This interface must be fast Ethernet or faster to be able to carry a lot of traffic comes in and out.

The core switch is connected to the router from one side, and to the access switches from the other.

Every access switch represents one floor per building.

### 5.2.3 Physical Connections and IP addressing

Each stack of switches (one virtual switch) will have a fiber connection towards the core of its campus this connection will be a trunk interface connection where this trunk will be used to carry all the VLANs information between the core switch and the access switches so the VTP will use this link to copy and modify the VLANs database from the core to all the access switches. We will use 2 modes of VTP out of 3, the core switch will be in server mode. Server VTP can create, delete, modify, and pass these changes too every switch else. While other access switches will be clients that do not

have the authority to change the database for security wise, they just receive updates from the server and apply those updates to their database.

Testing should go from the physical connectivity at layer 1 to connectivity at layer 2 and finally the layer 3 functionality. The first step of testing is whether there is or not a physical connection between the core and each and every access device in the domain, and that can be done through issuing the command `show cdp neighbors` on any device, the functionality of this command is that it is showing the devices that this device is connected to with the local interfaces that goes to the other device and the interfaces on the far end device. This command can be very handy when it comes to testing the layer 1 connectivity so if we see a neighbor on an interface that means the connection to this neighbor is working fine and the interfaces are up and working fine.

```
A-CORE#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
A-LIB-SW	Eth 3/3	157	R S	Linux Uni	Eth 0/0
A-ADM-GF	Eth 2/2	137	R S	Linux Uni	Eth 0/0
A-ENG-GF	Eth 1/2	161	R S	Linux Uni	Eth 0/0
A-AER-GF	Eth 3/0	137	R S	Linux Uni	Eth 0/0
A-LANG-1F	Eth 2/1	138	R S	Linux Uni	Eth 0/0
A-LANG-GF	Eth 2/0	138	R S	Linux Uni	Eth 0/0
A-AER-1F	Eth 3/1	137	R S	Linux Uni	Eth 0/0
A-AER-2F	Eth 3/2	159	R S	Linux Uni	Eth 0/0
A-ROUTER	Eth 0/0	149	R	7206VXR	Fas 0/0
A-ENG-1F	Eth 1/3	137	R S	Linux Uni	Eth 0/0
A-ADM-1F	Eth 2/3	159	R S	Linux Uni	Eth 0/0

**Figure 5.4** Show CDP Neighbors Command on Ankara core

#### 5.2.4 Security at Access Layer:

Since the access layer represents the interaction interface of the network with the end users it will be facing a lot of security concerns, and we need to take these concerns in a very serious way and closing all the back-doors and gaps in our network that can make a potential thread point or breaching access for our network.

Cisco switch is smart enough that if you don't set it up for security by password it is not going to allow people to Telnet into it, Telnet is the remote configuration protocol. We will lock down the privileged mode by using the command `enable secret` and put a password on the switch. Privileged mode allows us to view anything on our device such as the most important thing in terms of security which are the passwords that are set on that device, in short privileged mode is an unlimited

access mode from it we can move easily to the configuration mode which allows us to configure devices. Line vty 0 4 represents the Telnet ports and allows many people to access a specific device, in addition service password encryption encrypts every single password on the switch [27].

### 5.2.5 The virtual network:

The virtual structure of the network will consist of group of networks or VLANs that will span through the geographical boundaries and the reason of dividing them into different VLANs instead of having only one VLAN is to have more control over our network and it will be easier to manage, manipulate and traffic engineering. The reason behind VLANs is to logically segment our network into small groups of users.

The list of the VLANs in our network for Ankara campus will be as following:

VLAN NAME	VLAN NO.	IPv6 ADDRESS RANGE
Wireless VLAN	2	2001:0000:0000:0002::/64
Administration VLAN	3	2001:0000:0000:0003::/64
Labs VLAN	4	2001:0000:0000:0004::/64
Management VLAN	5	2001:0000:0000:0005::/64
Simulator VLAN	6	2001:0000:0000:0006::/64

**Table 5.2** The VLAN's in Ankara campus

Wireless VLAN: - this VLAN will be dedicated for wireless coverage and will cover all buildings that need a wireless connection. The range of the of IPv6 that will be used for this VLAN will be 2001:0000:0000:0002::/64

Administration VLAN: - will be used by the administration officers and the faculty wherever it needed. The range of the of IPv6 that will be used for this VLAN will be 2001:0000:0000:0003::/64

Labs VLAN: - this VLAN will be used by the students in the Labs that exist in three buildings. The range of the of IPv6 that will be used for this VLAN will be 2001:0000:0000:0004::/64

Management VLAN: this VLAN will be used to manage all the devices in the network including the switches and routers. The range of the IPv6 that will be used for this VLAN will be 2001:0000:0000:0005::/64

Flight Simulator VLAN: this VLAN will be dedicated to the flight simulator since it is a highly sensitive device and needs a high level of security. The range of the IPv6 that will be used for this VLAN will be 2001:0000:0000:0006::/64

After creating the VLANs on the core switch, we can see them by the command `show vlan` as follows:

```
A-CORE#show vlan
VLAN Name                Status   Ports
-----
1    default                active   Et0/1, Et0/2, Et0/3, Et1/0
                                         Et1/1
2    WIRELESS               active
3    ADMINISTRATION         active
4    LAB'S                  active
5    MANAGEMENT             active
6    SIMULATOR              active
1002 fddi-default           act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default      act/unsup
1005 trbrf-default        act/unsup

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001   1500  -       -       -     -     -       0      0
2    enet  100002   1500  -       -       -     -     -       0      0
3    enet  100003   1500  -       -       -     -     -       0      0
4    enet  100004   1500  -       -       -     -     -       0      0
5    enet  100005   1500  -       -       -     -     -       0      0
6    enet  100006   1500  -       -       -     -     -       0      0

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1002 fddi  101002   1500  -       -       -     -     -       0      0
1003 trcrf 101003   4472  1005   3276   -     -     srb     0      0
1004 fdnet 101004   1500  -       -       -     -     -       0      0
1005 trbrf 101005   4472  -       -       15    -     ibm     0      0

VLAN AREHops STEHops Backup CRF
-----
1003 7          7          off

Primary Secondary Type           Ports
-----
```

**Figure 5.5** Show VLAN command on the core switch

The list of the VLANs in our network for İzmir campus will be as following:-

VLAN NAME	VLAN NO.	IPv6 ADDRESS RANGE
Wireless VLAN	2	2001:0000:0001:0002::/64
Administration VLAN	3	2001:0000:0001:0003::/64
Labs VLAN	4	2001:0000:0001:0004::/64
Management VLAN	5	2001:0000:0001:0005::/64
Simulator VLAN	6	2001:0000:0001:0006::/64

**Table 5.3** The VLAN's in İzmir campus

The list of the VLANs in our network for Eskişehir campus will be as following:

VLAN NAME	VLAN NO.	IPv6 ADDRESS RANGE
Wireless VLAN	2	2001:0000:0002:0002::/64
Administration VLAN	3	2001:0000:0002:0003::/64
Labs VLAN	4	2001:0000:0002:0004::/64
Management VLAN	5	2001:0000:0002:0005::/64
Simulator VLAN	6	2001:0000:0002:0006::/64

**Table 5.4** The VLAN's in Eskişehir campus

These VLANs need to be created and deployed on all the 40 switches of the campus which makes it a very hard and inefficient process to deploy or update so to solve this problem we will use VTP (Virtual Trunking Protocol) [65] which allows us to choose one of our devices as a server so we create all VLANs on it then this switch will pass these VLANs through to all other switches that will be deployed as clients which means that the client switches cannot create VLANs by themselves and they only receive their database copy from the server.

The problem with the VTP deployment is that a rogue switch can be introduced to the network as a server so it can poison the VLANs database by adding or deleting VLANs, or it can introduce itself as a client to steal the VLANs database.

The solution to the above problems of VTP deployment is by adding a password protection to the VTP protocol that the server and the clients will share and any switch that has a wrong password will not be able to manipulate the database even if it belongs to the same domain. The command `show vtp status` shows us everything about the VTP:

```
A-CORE#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : THK
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : aabb.cc00.0100
Configuration last modified by 0.0.0.0 at 6-17-15 07:24:17
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision  : 6
MD5 digest              : 0x8C 0xA9 0x75 0x36 0xF1 0x49 0x7C 0x6C
                        : 0xEF 0xC0 0x63 0xE3 0xA5 0x04 0x30 0xC4
```

**Figure 5.6** Show vtp status command on the core

While the VTP on any access switch is as the following:

```

A-ENG-GF#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : THK
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : aabb.cc00.0200
Configuration last modified by 0.0.0.0 at 6-17-15 07:24:17

Feature VLAN:
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision  : 6
MD5 digest              : 0x8C 0xA9 0x75 0x36 0xF1 0x49 0x7C 0x6C
                       : 0xEF 0xC0 0x63 0xE3 0xA5 0x04 0x30 0xC4
  
```

**Figure 5.7** Show vtp status command on an access switch

We have created the VLANs on the core switch. And now we can see them on each access switch, because the VLAN Trunking Protocol passes all VLANs from the core to every access switch:

```

A-ENG-GF#show vlan
-----
VLAN Name                Status      Ports
-----
1    default                active     Et0/1, Et0/2, Et0/3, Et1/0
                                           Et1/1, Et1/2, Et1/3, Et2/0
                                           Et2/1, Et2/2, Et2/3, Et3/0
                                           Et3/1, Et3/2, Et3/3, Et4/0
                                           Et4/1, Et4/2, Et4/3, Et5/0
                                           Et5/1, Et5/2, Et5/3, Et6/0
                                           Et6/1, Et6/2, Et6/3, Et7/0
                                           Et7/1, Et7/2, Et7/3, Et8/0
                                           Et8/1, Et8/2, Et8/3, Et9/0
                                           Et9/1, Et9/2, Et9/3, Et10/0
                                           Et10/1, Et10/2, Et10/3, Et11/0
                                           Et11/1, Et11/2, Et11/3, Et12/0
                                           Et12/1, Et12/2, Et12/3, Et13/0
                                           Et13/1, Et13/2, Et13/3, Et14/0
                                           Et14/1, Et14/2, Et14/3, Et15/0
                                           Et15/1, Et15/2, Et15/3
2    WIRELESS                active
3    ADMINISTRATION          active
4    LAB's                    active
5    MANAGEMENT              active
6    SIMULATOR               active
1002 fddi-default            act/unsup
1003 trcrf-default          act/unsup
1004 fdnet-default          act/unsup
1005 trbrf-default          act/unsup
-----
VLAN Type  SAID       MTU   Parent  RingNo BridgeNo  Stp  BrdgMode  Trans1  Trans2
-----
1    enet   100001     1500  -       -       -       -       -         0       0
2    enet   100002     1500  -       -       -       -       -         0       0
3    enet   100003     1500  -       -       -       -       -         0       0
4    enet   100004     1500  -       -       -       -       -         0       0
5    enet   100005     1500  -       -       -       -       -         0       0
6    enet   100006     1500  -       -       -       -       -         0       0
1002 fddi   101002     1500  -       -       -       -       -         0       0
1003 trcrf  101003     4472  1005   3276   -       -       srb        0       0
1004 fdnet  101004     1500  -       -       -       -       ieee       0       0
1005 trbrf  101005     4472  -       -       15      -       ibm        0       0
  
```

**Figure 5.8** Show VLAN command on an access switch

We will need a Trunk port on each and every switch to share VLANs of our network between all devices, otherwise without Trunk ports we would get separate



VLANs that couldn't communicate because Trunk sends all VLANs traffic across the network.

The range of the IPv6 addresses that connect the core with the access layer switches is addressed in a way where it all start with 2001:0:0:xy::z where x always has a value of 1 referring to the core, y is the access switch number starting from 1 which is the first access switch in the network (ENG-GF) and so on until we reach the last switch which is Library-SW, z value is 1 on the core side and 2 on the access switch, for example the IPv6 of the core switch in Ankara's campus that is directly connected to the ENG-GF is 2001:0:0:11::1 (where x is 1 representing the core, y is representing the very first switch that is ENG-GF, z is 1 because it is on the core side), while the IPv6 of ENG-GF in the same campus is 2001:0:0:11::2. The above addressing is for Ankara campus only while İzmir campus range is 2001:0:1:xy::z and the values of x, y and z are the same. The third and last campus is Eskişehir with the IPv6 range of 2001:0:2:xy::z.

After all the campus connections, VLANs and addressing are done and the connectivity inside the campus been tested. The next step will be adding the connectivity among the campuses where in our case both İzmir and Eskişehir campuses will have a connection to the router of the Ankara campus so this router will work as the core of whole university with all of its campuses.

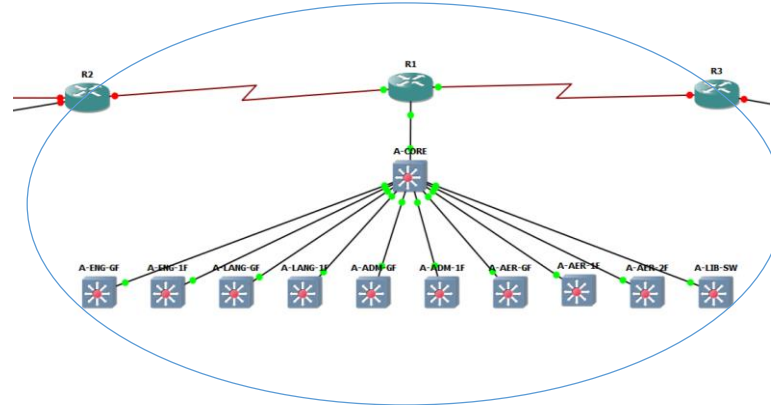
The addressing that will be used to connect the cores will be as following:

2001:0:12:12::x/64 between Ankara router (router 1) and İzmir router (router 2) where x will have the value of 1 on Ankara side and the value of 2 on the İzmir side.

2001:0:13:13::x/64 is the IPv6 address that is used between Ankara router and Eskişehir router (router 3) where x will have the value of 1 on Ankara side and the value of 2 on the Eskişehir side.

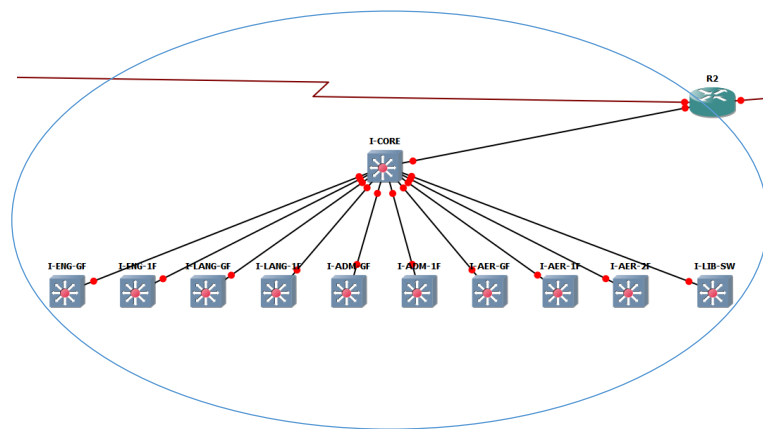
After having all the intra-campus and inter-campus networks, testing within campus network connectivity and testing the direct connectivity between the cores it is the time to deploy the OSPFv3 as our routing protocol, after having the OSPFv3 deployed we should have a full connectivity all over the three campuses and among them.

With OSPF we divided our workspace into 3 areas as OSPF uses the concept of areas. Area 0 (the backbone area) contains all devices of Ankara campus in addition to the links on İzmir and Eskişehir router that connect them to Ankara router.



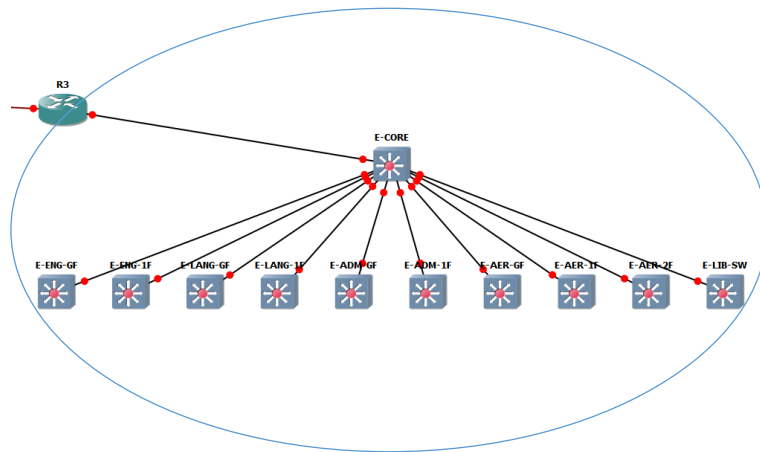
**Figure 5.9 Area0**

Area 1 has all the devices of İzmir campus except the link between İzmir router and Ankara router:



**Figure 5.10 Area1**

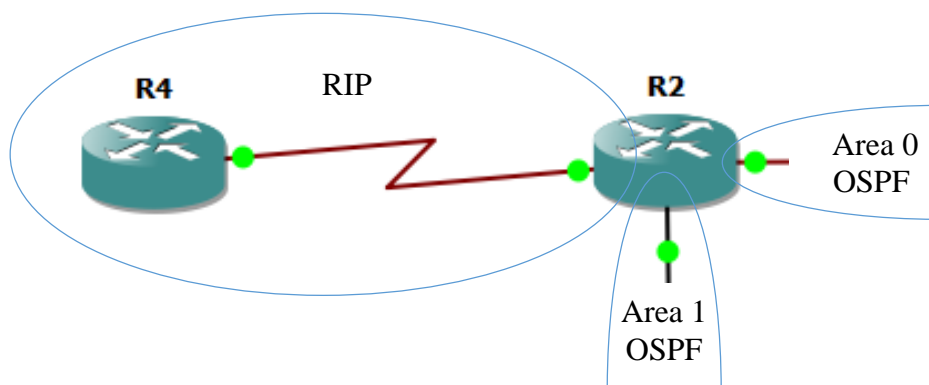
And area 2 that all Eskişehir campus devices within it note that one link of the main router of area 2 is out that area:



**Figure 5.11** Area2

After deploying OSPF all devices of the three campuses share their information between each other in a way that make all devices can reach and have connection to all. We will use some show commands to reveal facts about OSPF besides WireShark which allows us to capture, sniff, and analyze traffic packets between the connected devices.

We made İzmir router connected to different areas which are area 0 and area1 of OSPF and RIP from another side in order to see almost all the LSA types:



**Figure 5.12** İzmir router links

In this bidirectional redistribution İzmir router (R2) will take the routes from RIP and redistribute them into OSPF to see external LSA. And we will take the routes from OSPF and redistribute them into RIP in a way RIP routes can see the entire topology and we can test the connectivity. From İzmir router's view, it can run two routing protocols as shown in figure 10:

```

I-ROUTER#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Serial1/0
  Interfaces (Area 1):
    FastEthernet0/0.6
    FastEthernet0/0.5
    FastEthernet0/0.4
    FastEthernet0/0.3
    FastEthernet0/0.2
    FastEthernet0/0
  Redistribution:
    Redistributing protocol rip mo with metric 88 include-connected
IPv6 Routing Protocol is "rip mo"
  Interfaces:
    Serial1/1
  Redistribution:
    Redistributing protocol ospf 1 with metric 5 include-connected

```

**Figure 5.13** show IPv6 protocols command on İzmir router

We can see that İzmir router can run 2 routing protocols, OSPF redistributing RIP and vice versa.

So we have full connectivity across the entire network as Eskişehir router sees it:

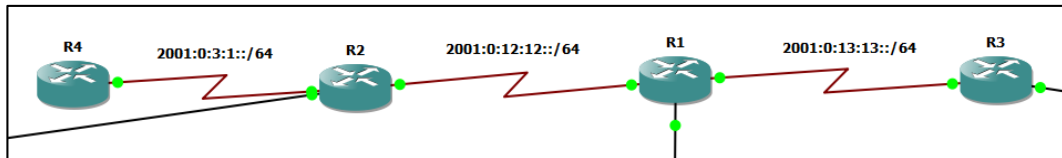
```

E-ROUTER#show ipv6 route ospf
IPv6 Routing Table - 30 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:0:0:1::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:0:2::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:0:3::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:0:4::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:0:5::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:0:6::/64 [110/65]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:1::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:2::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:3::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:4::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:5::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OI  2001:0:1:6::/64 [110/129]
     via FE80::C801:7FF:FE8C:0, Serial1/1
OE2 2001:0:3:1::/64 [110/88]
     via FE80::C801:7FF:FE8C:0, Serial1/1
O   2001:0:12:12::/64 [110/128]
     via FE80::C801:7FF:FE8C:0, Serial1/1

```

**Figure 5.14** show IPv6 route OSPF command on Eskişehir router (R3)

OE2 is external route from outside OSPF 2001:0:3:1::/64 injected it to the whole network where 2001:0:3:1::/64 is the link of İzmir router with RIP.



**Figure 5.15** the subnet between routers

OI means inter routes coming from other areas (area 0 and area 1, since Eskişehir router is within area 2).

O is intra area routes coming from devices that are inside the area the router belongs to (directly connected).

Next we will see the topology database on the main router of all (R1), in this case R1, R2 and R3 almost have the same database because they are connected to the same area (0). From R1's database we can see 6 types of LSA but let's have a look at table 4.1 first to remember them, then execute the command `show IPv6 OSPF database` to see:

```
A-ROUTER#show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0)
```

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
1.1.1.1	599	0x80000019	0	7	None
1.1.1.2	496	0x80000003	0	5	None
1.1.1.3	2097	0x80000003	0	5	None
1.1.1.4	2096	0x80000003	0	5	None
1.1.1.5	2102	0x80000002	0	5	None
1.1.1.6	2102	0x80000002	0	5	None
1.1.1.7	2102	0x80000002	0	5	None
1.1.1.8	2128	0x80000003	0	5	None
1.1.1.9	2120	0x80000004	0	5	None
1.1.1.10	2118	0x80000004	0	5	None
1.1.1.11	2125	0x80000003	0	5	None
1.1.1.12	2125	0x80000003	0	5	None
2.2.2.1	940	0x80000006	0	1	EB
3.3.3.1	767	0x80000004	0	1	B

**Figure 5.16** 2001 Router-LSA on R1

These LSAs are generated by every device within the area to advertise information about themselves and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database router`.

Net Link States (Area 0)				
ADV Router	Age	Seq#	Link ID	Rtr count
1.1.1.1	599	0x8000000D	13	2
1.1.1.1	675	0x8000000B	14	2
1.1.1.1	678	0x8000000E	15	2
1.1.1.1	678	0x8000000E	16	2
1.1.1.1	681	0x8000000D	17	2

**Figure 5.17** 2002 Network-LSA

The designated router generates then Network LSA, R1 in this area is the DR because it has the lowest router ID and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database network`.

Inter Area Prefix Link States (Area 0)				
ADV Router	Age	Seq#	Prefix	
2.2.2.1	1017	0x80000003	2001:0:1:6::/64	
2.2.2.1	1017	0x80000003	2001:0:1:5::/64	
2.2.2.1	1017	0x80000003	2001:0:1:4::/64	
2.2.2.1	1017	0x80000003	2001:0:1:3::/64	
2.2.2.1	1017	0x80000003	2001:0:1:2::/64	
2.2.2.1	1017	0x80000003	2001:0:1:1::/64	
3.3.3.1	844	0x80000003	2001:0:2:6::/64	
3.3.3.1	844	0x80000003	2001:0:2:5::/64	
3.3.3.1	844	0x80000003	2001:0:2:4::/64	
3.3.3.1	844	0x80000003	2001:0:2:3::/64	
3.3.3.1	844	0x80000003	2001:0:2:2::/64	
3.3.3.1	844	0x80000003	2001:0:2:1::/64	

**Figure 5.18** 2003 Inter-Area-Prefix-LSA

ABR are in charge of generating this type of LSA to describe the links they have inside the adjacent areas to area 0 and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database inter-area prefix`.

Type-5 AS External Link States				
ADV Router	Age	Seq#	Prefix	
2.2.2.1	50	0x80000004	2001:0:3:1::/64	

**Figure 5.19** 4005 AS-External-LSA

Izmir router R2 (router ID 2.2.2.1) tells Ankara router R1 about this external route R2 is redistributing in to OSPF and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database external`.

Link (Type-8) Link states (Area 0)				
ADV Router	Age	Seq#	Link ID	Interface
1.1.1.1	443	0x80000004	6	Se1/1
3.3.3.1	414	0x80000004	6	Se1/1
1.1.1.1	444	0x80000004	5	Se1/0
2.2.2.1	591	0x80000005	5	Se1/0
1.1.1.1	444	0x80000004	17	Fa0/0.6
1.1.1.2	169	0x80000004	24	Fa0/0.6
1.1.1.3	3764	0x80000002	72	Fa0/0.6
1.1.1.4	3764	0x80000002	72	Fa0/0.6
1.1.1.5	3764	0x80000002	72	Fa0/0.6
1.1.1.6	3765	0x80000002	72	Fa0/0.6
1.1.1.7	3765	0x80000002	72	Fa0/0.6
1.1.1.1	444	0x80000004	16	Fa0/0.5
1.1.1.2	169	0x80000004	23	Fa0/0.5
1.1.1.3	3764	0x80000002	71	Fa0/0.5
1.1.1.4	3764	0x80000002	71	Fa0/0.5
1.1.1.5	3764	0x80000002	71	Fa0/0.5
1.1.1.6	3765	0x80000002	71	Fa0/0.5
1.1.1.7	3763	0x80000002	71	Fa0/0.5
1.1.1.1	444	0x80000004	15	Fa0/0.4
1.1.1.2	169	0x80000004	22	Fa0/0.4
1.1.1.3	3764	0x80000002	70	Fa0/0.4
1.1.1.4	3764	0x80000002	70	Fa0/0.4
1.1.1.5	3764	0x80000002	70	Fa0/0.4
1.1.1.6	3765	0x80000002	70	Fa0/0.4
1.1.1.7	3764	0x80000002	70	Fa0/0.4
1.1.1.1	444	0x80000004	14	Fa0/0.3
1.1.1.2	170	0x80000004	21	Fa0/0.3
1.1.1.3	3765	0x80000002	69	Fa0/0.3
1.1.1.4	3765	0x80000002	69	Fa0/0.3
1.1.1.5	3765	0x80000002	69	Fa0/0.3
1.1.1.6	3765	0x80000002	69	Fa0/0.3
1.1.1.7	3764	0x80000002	69	Fa0/0.3
1.1.1.1	444	0x80000004	13	Fa0/0.2
1.1.1.2	170	0x80000004	20	Fa0/0.2
1.1.1.3	3765	0x80000002	68	Fa0/0.2
1.1.1.4	3765	0x80000002	68	Fa0/0.2
1.1.1.5	3765	0x80000002	68	Fa0/0.2
1.1.1.6	3765	0x80000002	68	Fa0/0.2
1.1.1.7	3765	0x80000002	68	Fa0/0.2
1.1.1.1	444	0x80000004	4	Fa0/0

**Figure 5.20** 0008 Link-LSA

R1 is not going to forward this type of LSA and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database link`.

Intra Area Prefix Link States (Area 0)					
ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
1.1.1.1	181	0x80000005	0	0x2001	0
1.1.1.1	181	0x80000003	1013	0x2002	13
1.1.1.1	181	0x80000003	1014	0x2002	14
1.1.1.1	181	0x80000003	1015	0x2002	15
1.1.1.1	182	0x80000003	1016	0x2002	16
1.1.1.1	182	0x80000003	1017	0x2002	17
2.2.2.1	592	0x80000004	0	0x2001	0
3.3.3.1	415	0x80000004	0	0x2001	0

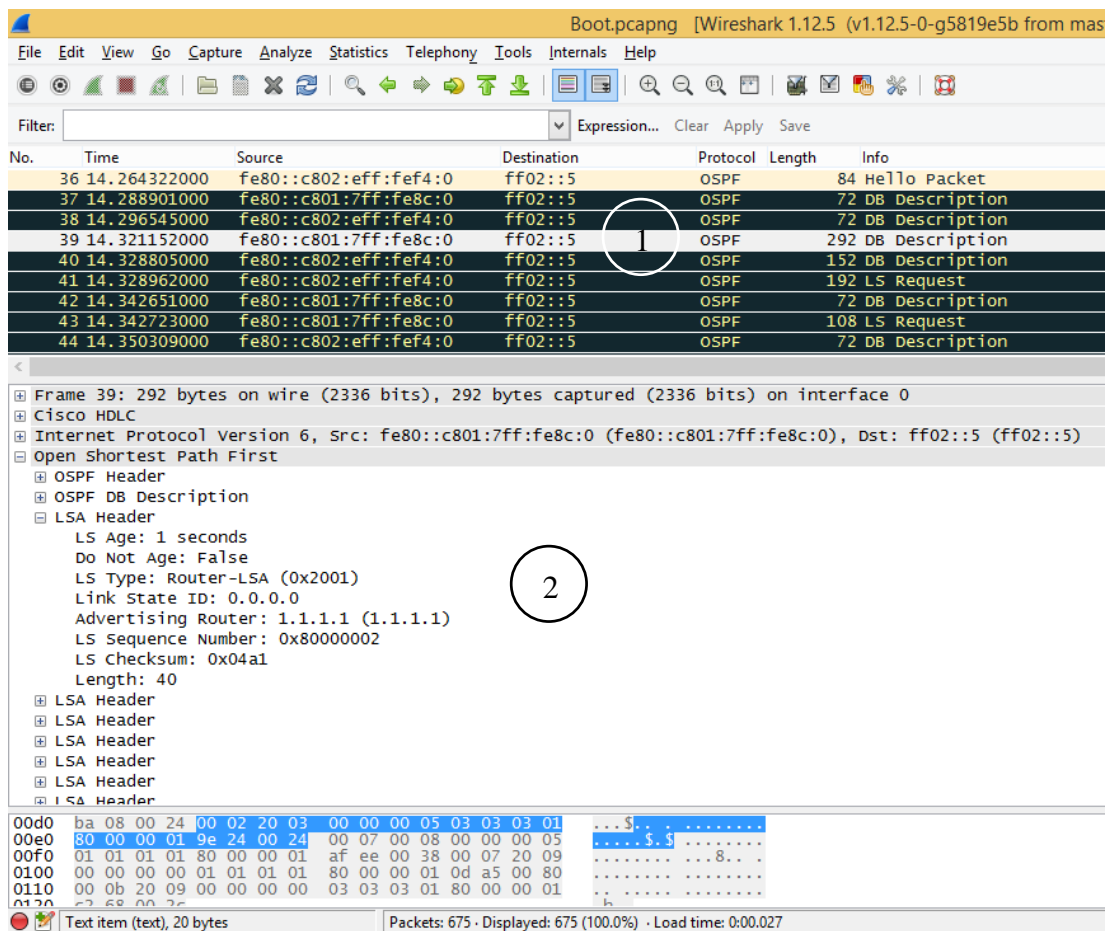
**Figure5.21** 2009 Intra-Area-Prefix-LSA

These LSAs stay in the area, they do not get forwarded outside the area and stay in the actual area where they resourced based on type 1 and 3 LSAs so that we can see

more than advertisements of R1 and we can see more details of type 1 LSA by executing the command `show IPv6 OSPF database prefix`.

### 5.3. Capturing OSPF packets

When OSPF router boots up, it has a lot of thing to do like forming adjacency with neighbors and getting copies of LSAs because every OSPF device in the area has to have the same information. We will see all these actions by putting our protocol analyzer WireShark on a link of R1 for more analyzing about OSPF behavior and then booting up all the devices.



**Figure5.22** a packet capture

If we look at packet 39 no. 1, after 14.3 seconds of booting, we see that it comes from the source: `fe80::c801:7ff:fe8c:0`, this is a link local address of R3:



```
E-ROUTER#show ipv6 interface brief
FastEthernet0/0 [up/up]
FE80::C803:9FF:FE8C:0
2001:0:2:1::1
```

**Figure 5.23** R3 link local address

Destined to all OSPF designated routers in the same link by using multicast address ff02::5. The designated router of area 0 is R1 (Ankara router) because it has the lowest router-ID 1.1.1.1. All routing protocols use layer 2 address to form neighborships as they communicate back and forth. When we look back at figure 5.21 no. 2, we see LSA type 1, R3 is telling R1 about the information it knows. We have more than one LSA within this packet:

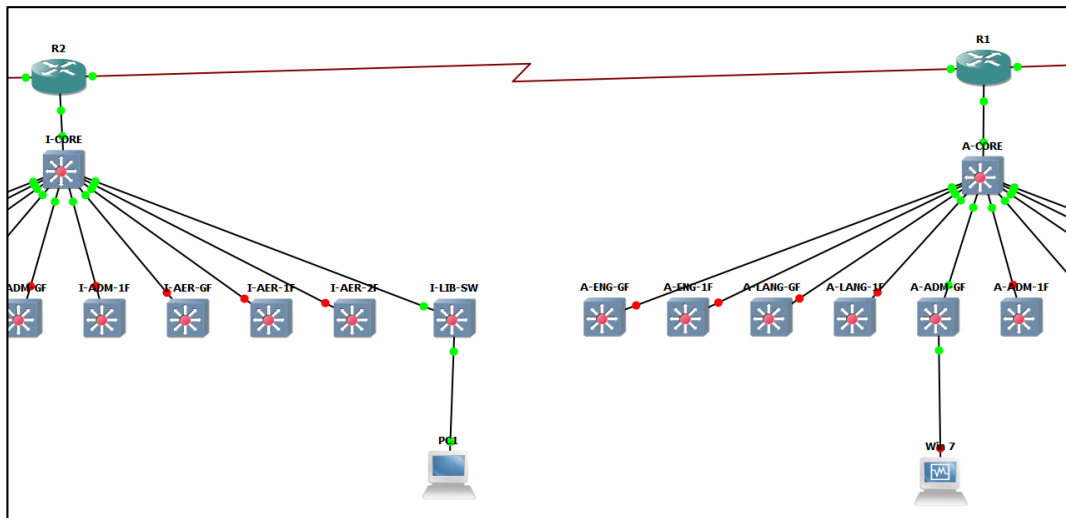
```
[-] LSA Header
  LS Age: 2 seconds
  Do Not Age: False
  LS Type: Inter-Area-Prefix-LSA (0x2003)
  Link State ID: 0.0.0.0
  Advertising Router: 3.3.3.1 (3.3.3.1)
  LS Sequence Number: 0x80000001
  LS Checksum: 0x2b97
  Length: 36
[+] LSA Header
```

**Figure 5.24** LAS type 3 generated by R3

Inter area prefix LSA is generated by Area Border Router (ABR) about summary networks it knows about.

#### 5.4 Assigning ports to VLAN

We are going to connect Windows 7 host to the Management VLAN at Ankara campus at the Administration building ground floor in order to manage our entire network. This PC will have IPv6 from the range of that VLAN 2001:0:0:5::/64, the Windows 7 PC will have 2001:0:0:5::10/64 IPv6. From another side of the campus we will use VPCS (virtual PC simulator) on GNS3 and then test the connectivity between these two PCs by using the command `ping` and running WireShark to capture the packet.



**Figure 5.25** Adding PCs to the topology

VPCS is a lightweight application that we can't assign an IP address to. It can simulate computers from a single command line interface. But it will not be on a specific VLAN because it gets IPv6 by using autoconfiguration feature of IPv6 from an access port on an access switch.

```
PC1> ip auto
GLOBAL SCOPE      : 2001:0:1:1:2050:79ff:fe66:6801/64
ROUTER LINK-LAYER : ca:02:0e:f4:00:00
```

**Figure 5.26** IPv6 Autoconfiguration

It gets this IPv4 from the range of its default gateway 2001:0:1:1::/64 and by using the method of EUI we described previously in chapter 3. Although we assigned IPv6 address to the Windows 7 PC within the range of VALN 5 but it didn't use it to ping the PC at İzmir side of the topology. It used the EUI IPv6 it made up for itself.

```

C:\Windows\system32\cmd.exe

C:\Users\Moha>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address . . . . .           : 2001:0:0:5::10
    IPv6 Address . . . . .           : 2001::5:8469:ef8d:212:2459
    Temporary IPv6 Address . . . . . : 2001::5:dd98:761e:f966:25d6 ←
    Link-local IPv6 Address . . . . . : fe80::8469:ef8d:212:2459%11
    Autoconfiguration IPv4 Address . . : 169.254.36.89
    Subnet Mask . . . . .           : 255.255.0.0
    Default Gateway . . . . .       : fe80::a8bb:ccff:fe80:600%11
                                       fe80::a8bb:ccff:fe80:100%11
                                       fe80::c801:7ff:fe8c:0%11

Tunnel adapter isatap.{E6932737-D929-41FE-BB1C-74E09B454344}:

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

Tunnel adapter Local Area Connection* 11:

```

Figure 5.27 IPv6 on Windows 7 host

And we can see the successful of that ping request using WireShark capture packet containing the source and the destination addresses:

```

*Standard input [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1299 198.648319000 aa:bb:cc:00:01:00 PVST+ 68 Conf. Root = 32768/4/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
1298 198.64831000 aa:bb:cc:00:01:00 PVST+ 68 Conf. Root = 32768/5/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
1299 198.647465000 aa:bb:cc:00:01:00 PVST+ 68 Conf. Root = 32768/6/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
1300 198.751065000 2001::5:dd98:761e:f966:25d6 2001:0:1:1:2050:79ff:fe66:6801 ICMPv6 94 Echo (ping) request id=0x0001, seq=29, hop limit=127 (reply in 13)
1301 198.843276000 2001:0:1:1:2050:79ff:fe66:6801 2001::5:dd98:761e:f966:25d6 ICMPv6 98 Echo (ping) reply id=0x0001, seq=29, hop limit=123 (request in 13)
1302 199.316853000 fe80::a8bb:ccff:fe80:600 ff02::5 OSPF 102 Hello Packet
1303 199.744137000 2001::5:dd98:761e:f966:25d6 2001:0:1:1:2050:79ff:fe66:6801 ICMPv6 94 echo (ping) request id=0x0001, seq=30, hop limit=127 (reply in 13)
1304 199.832810000 2001:0:1:1:2050:79ff:fe66:6801 2001::5:dd98:761e:f966:25d6 ICMPv6 98 Echo (ping) reply id=0x0001, seq=30, hop limit=123 (request in 13)
1305 199.854642000 fe80::a8bb:ccff:fe80:100 ff02::1 ICMPv6 122 Router Advertisement from aa:bb:cc:80:01:00
1306 199.856680000 aa:bb:cc:00:01:00 RST 68 Conf. Root = 32768/3/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001

Frame 1303: 94 bytes on wire (752 bits) captured (752 bits) on interface 0
Ethernet II, Src: aa:bb:cc:80:06:00 (aa:bb:cc:80:06:00), Dst: ca:01:07:8c:00:00 (ca:01:07:8c:00:00)
Internet Protocol Version 6, Src: 2001::5:dd98:761e:f966:25d6 (2001::5:dd98:761e:f966:25d6), Dst: 2001:0:1:1:2050:79ff:fe66:6801 (2001:0:1:1:2050:79ff:fe66:6801)
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
Payload length: 40
Next header: ICMPv6 (58)
Hop limit: 127
Source: 2001::5:dd98:761e:f966:25d6 (2001::5:dd98:761e:f966:25d6)
[Source Teredo Server IPv4: 0.0.0.5 (0.0.0.5)]
[Source Teredo Port: 35297]
[Source Teredo Client IPv4: 6.153.218.41 (6.153.218.41)]
Destination: 2001:0:1:1:2050:79ff:fe66:6801 (2001:0:1:1:2050:79ff:fe66:6801)
[Destination Teredo Server IPv4: 0.1.0.1 (0.1.0.1)]
[Destination Teredo Port: 34304]
[Destination Teredo Client IPv4: 1.153.151.254 (1.153.151.254)]
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol v6

```

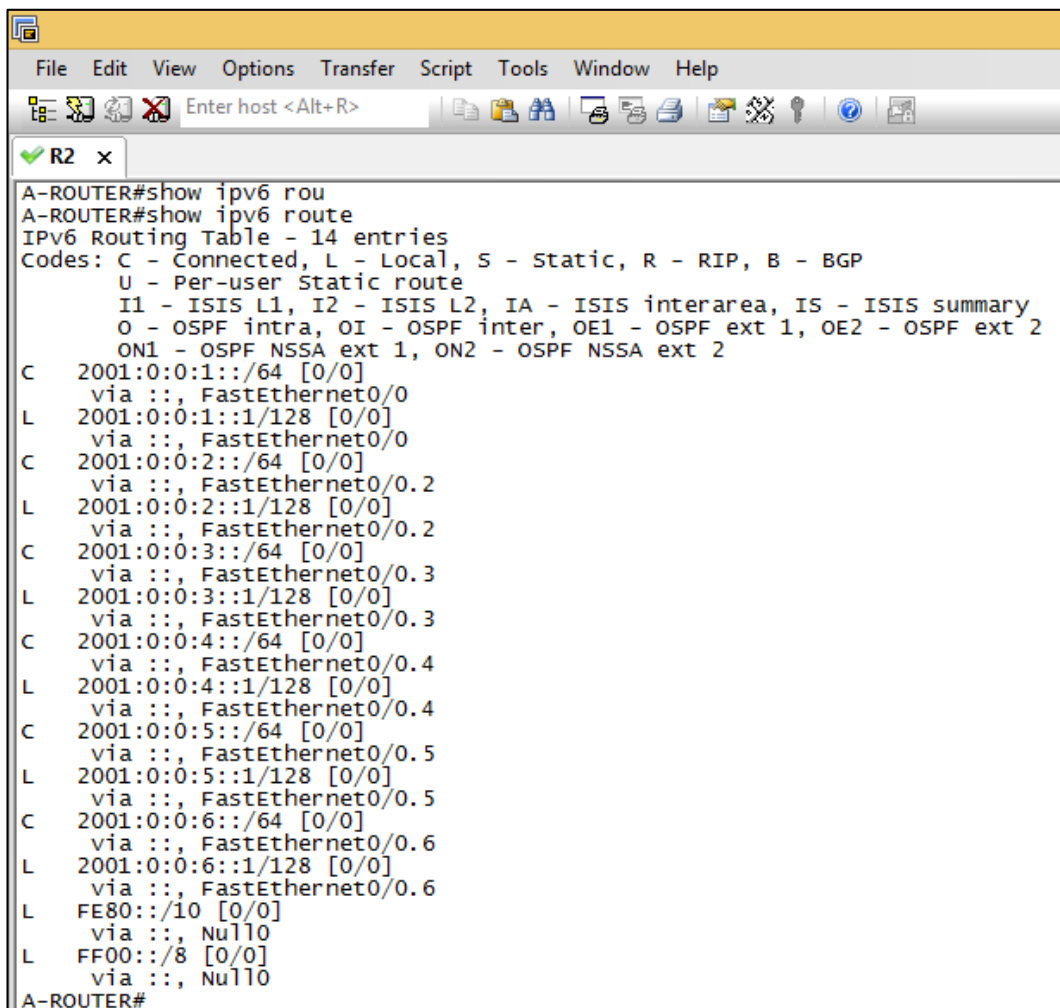
Figure 5.28 ping request on WireShark

By now all the devices can reach each other thanks to deploying OSPF on our campus and we can assign ports on access switches to supply our end users with the service. We can assign these captured ports to either to VLANs or to be access ports that serve the Internet to every one connects his/her PC to these access ports.

## 5.5 Results

### 5.5.1 Checking routing tables

Before we started to describe the statistical results of IPv6 and OSPFv3, we checked the routing table of Ankara router before we booting up all other devices. It has 14 entries that came from the 6 VLANs we created on the sub interfaces to make this router as Router on a Stick. In addition to “made up” link local address for each of our 6 VLANs, that’s 12 entries. The other remaining 2 are multicast and link-local respectively:



```
A-ROUTER#show ipv6 rou
A-ROUTER#show ipv6 route
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C    2001:0:0:1::/64 [0/0]
   via ::, FastEthernet0/0
L    2001:0:0:1::1/128 [0/0]
   via ::, FastEthernet0/0
C    2001:0:0:2::/64 [0/0]
   via ::, FastEthernet0/0.2
L    2001:0:0:2::1/128 [0/0]
   via ::, FastEthernet0/0.2
C    2001:0:0:3::/64 [0/0]
   via ::, FastEthernet0/0.3
L    2001:0:0:3::1/128 [0/0]
   via ::, FastEthernet0/0.3
C    2001:0:0:4::/64 [0/0]
   via ::, FastEthernet0/0.4
L    2001:0:0:4::1/128 [0/0]
   via ::, FastEthernet0/0.4
C    2001:0:0:5::/64 [0/0]
   via ::, FastEthernet0/0.5
L    2001:0:0:5::1/128 [0/0]
   via ::, FastEthernet0/0.5
C    2001:0:0:6::/64 [0/0]
   via ::, FastEthernet0/0.6
L    2001:0:0:6::1/128 [0/0]
   via ::, FastEthernet0/0.6
L    FE80::/10 [0/0]
   via ::, Null0
L    FF00::/8 [0/0]
   via ::, Null0
A-ROUTER#
```

**Figure 5.29** Routing table of Ankara router before OSPF

After almost 50 seconds of booting up all other devices, the routing table of Ankara router became with 31 entries, the same old 14, 12 from inter OSPF which are advertisements of VLSNs from İzmir (6 VLANs) and Eskişehir (6VLANs too), 1

external OSPF which is RIP area connected to İzmir router and 2 connections to İzmir and Eskişehir routers with their made up link local:

```

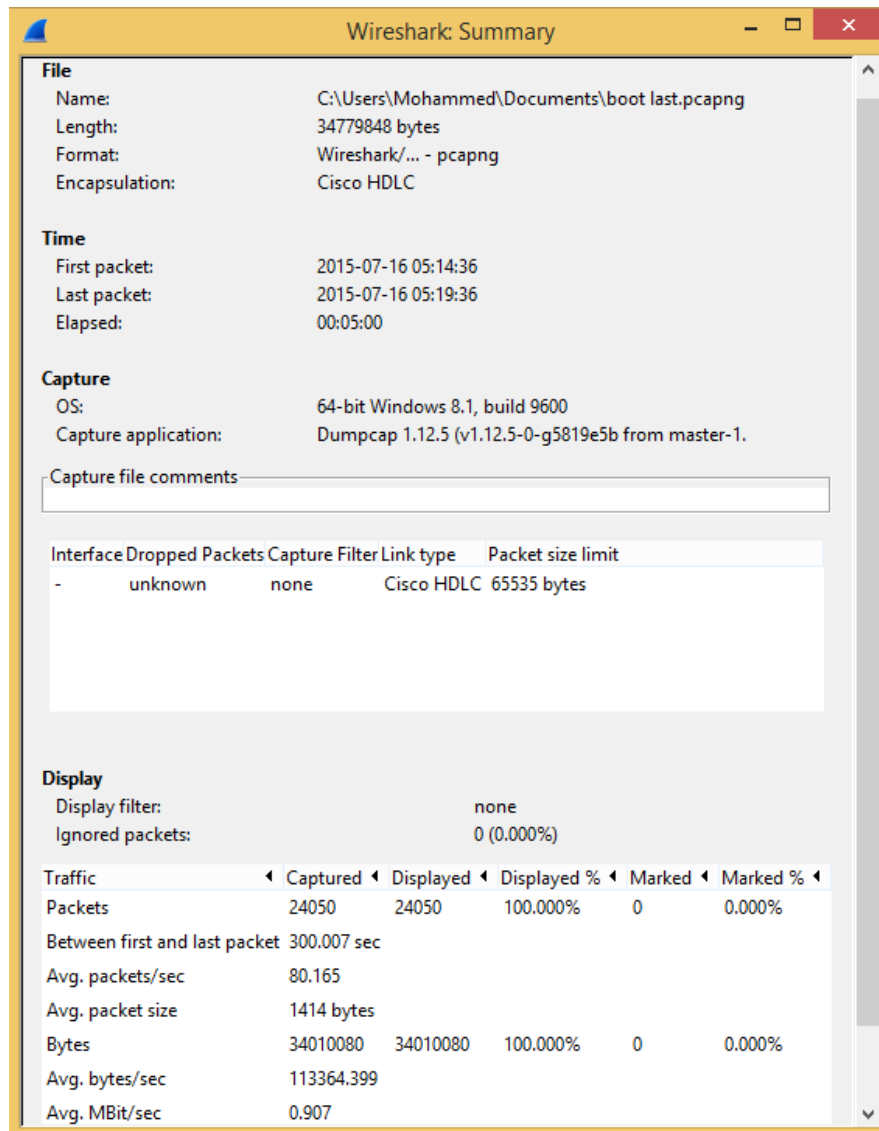
R1 x
A-ROUTER#show ipv6 route
IPv6 Routing Table - 31 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001:0:0:1::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:0:0:1:1::1/128 [0/0]
  via ::, FastEthernet0/0
C 2001:0:0:2::/64 [0/0]
  via ::, FastEthernet0/0.2
L 2001:0:0:2:1::1/128 [0/0]
  via ::, FastEthernet0/0.2
C 2001:0:0:3::/64 [0/0]
  via ::, FastEthernet0/0.3
L 2001:0:0:3:1::1/128 [0/0]
  via ::, FastEthernet0/0.3
C 2001:0:0:4::/64 [0/0]
  via ::, FastEthernet0/0.4
L 2001:0:0:4:1::1/128 [0/0]
  via ::, FastEthernet0/0.4
C 2001:0:0:5::/64 [0/0]
  via ::, FastEthernet0/0.5
L 2001:0:0:5:1::1/128 [0/0]
  via ::, FastEthernet0/0.5
C 2001:0:0:6::/64 [0/0]
  via ::, FastEthernet0/0.6
L 2001:0:0:6:1::1/128 [0/0]
  via ::, FastEthernet0/0.6
OI 2001:0:1:1::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:1:2::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:1:3::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:1:4::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:1:5::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:1:6::/64 [110/65]
  via FE80::C802:EFF:FEF4:0, Serial1/0
OI 2001:0:2:1::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OI 2001:0:2:2::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OI 2001:0:2:3::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OI 2001:0:2:4::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OI 2001:0:2:5::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OI 2001:0:2:6::/64 [110/65]
  via FE80::C803:9FF:FE8C:0, Serial1/1
OE2 2001:0:3:1::/64 [110/88]
  via FE80::C802:EFF:FEF4:0, Serial1/0
C 2001:0:12:12::/64 [0/0]
  via ::, Serial1/0
L 2001:0:12:12:1::1/128 [0/0]
  via ::, Serial1/0
C 2001:0:13:13::/64 [0/0]
  via ::, Serial1/1
L 2001:0:13:13:1::1/128 [0/0]
  via ::, Serial1/1
L FE80::/10 [0/0]

```

Figure 5.30 Routing table of Ankara router after OSPF

## 5.5.2 Packet capturing

We captured these packets at the same time we booted all the devices up. This capture was on the link between Ankara and İzmir routers by using the protocol analyzer Wireshark with High-Level Data Link Control network protocol created by Cisco Systems, Inc. for exactly 300.006708 seconds. Within that period of time we gained 24050 packets with different sizes, 34010080 bytes in total.



**Figure 5.31** Summary of booting up all devices

Average of packets per second is 80.165

Average of packet size is 1414

Average of bytes per second is 113364.399

Average of Mega bit per second is 0.907

### 5.5.3 Protocol tree

In this capture, the connection used Cisco HDLC protocol to define each frame between the devices. The smallest percentage of HDLC went to Cisco Discovery Protocol (CDP) 0.05 % with 13 packets. The second smallest portion was to Cisco Serial Line Address Resolution Protocol (SLARP) .0.25 % with 60 packets. And the biggest piece of HDLC went to IPv6 99.70 % with 23977 packets. IPv6 packets is divided between Internet Control Message Protocol (ICMPv6) 7.68 % 1846 packets, Open Shortest Path First (OSPFv3) 1.21 % with 291 packets and the Data 90.81 % with 21840 packets.

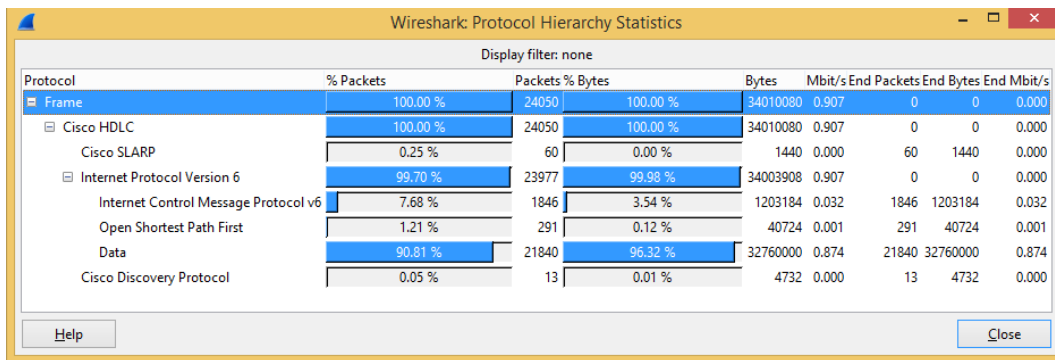


Figure 5.32 Protocols Hierarchy used in the capture

### 5.5.4 Conversation between Ankara and İzmir routers

It is the traffic between the two devices with a lot of information on tabs but just the IPv6 tab is activated because we used it to send 14 traffics from Ankara router to İzmir router and vice versa. We will take a look at two packets example. Address A: FE80::C802:EFF:FEF4 is the Extended Unique Identifier (EUI) of İzmir router. FE80::C802:EFF:FEF4 sent 89 packets (12084 bytes) to all routers that are running OSPF on the same link by using FF02::5 as address B. we can see also Rel Start with the value of 18.808146 seconds “Rel Start is the time in seconds between the start of the capture (packet #1) and the start of the conversation” while the Duration was 280.0413 seconds “Duration” is the time in seconds between the first and last packet of the conversation”. We have another FF02::5 connection from address A with the EUI of FE80::C801:7FF:FE8C which is Ankara router to all OSPF routers FF02::5. This connection was 202 packets (28640 bytes) with Rel Start of 22.133652 seconds

and Duration of 277.1956 seconds. Ankara router sent 826.56 bits per second during this connection. So we have 291 packets of FF02::5 type with 40724 bytes in total.

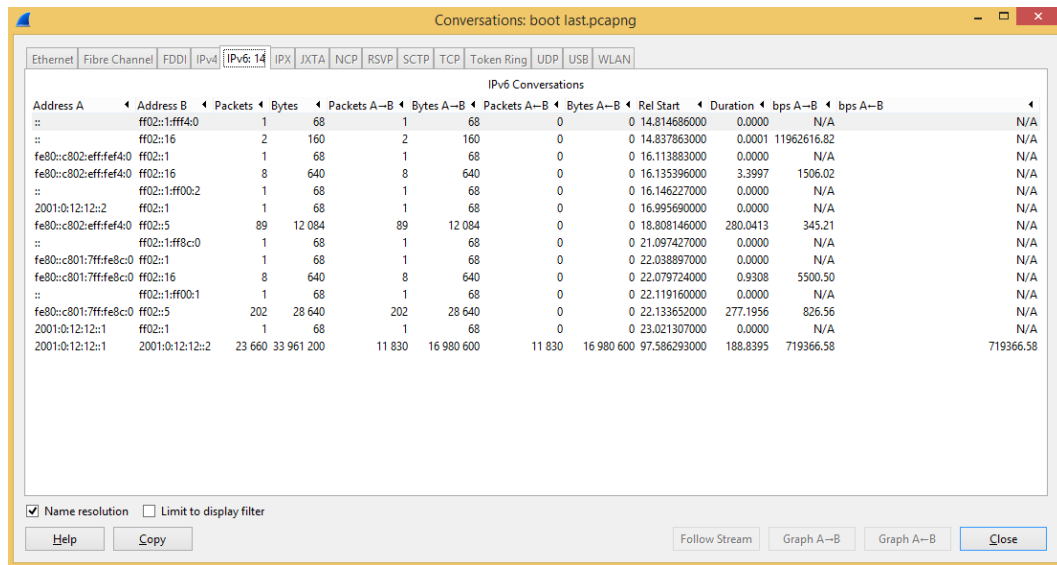


Figure 5.33 Traffic between Ankara and İzmir routers

### 5.5.5 Packet Lengths

During the connection between Ankara and İzmir routers, the two devices sent various lengths of packets to each other. We will discuss the largest ones sent, that are between 1280 – 2559 bytes. These were the maximum number of packets transmitted in that capture connection with the Count of 21840 packets and percentage 90.81 %. The maximum and minimum lengths were equal with 1500 bytes each to give us an average of 1500 bytes too. Burst Rate is the maximum number of packets sent per interval of time and Burst Start is the time when the maximum number of packets sent occurred.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	24050	2828.28	24	1500	0.0802	100%	0.4100	226.711
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	60	24.00	24	24	0.0002	0.25%	0.0100	0.000
40-79	13	69.54	68	72	0.0000	0.05%	0.0400	28.800
80-159	206	97.65	80	152	0.0007	0.86%	0.0500	22.080
160-319	91	207.52	160	300	0.0003	0.38%	0.0300	28.863
320-639	20	376.80	336	572	0.0001	0.08%	0.0300	21.024
640-1279	1820	660.00	660	660	0.0061	7.57%	0.0400	223.441
1280-2559	21840	1500.00	1500	1500	0.0728	90.81%	0.3800	226.711
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120-4294967295	0	-	-	-	0.0000	0.00%	-	-

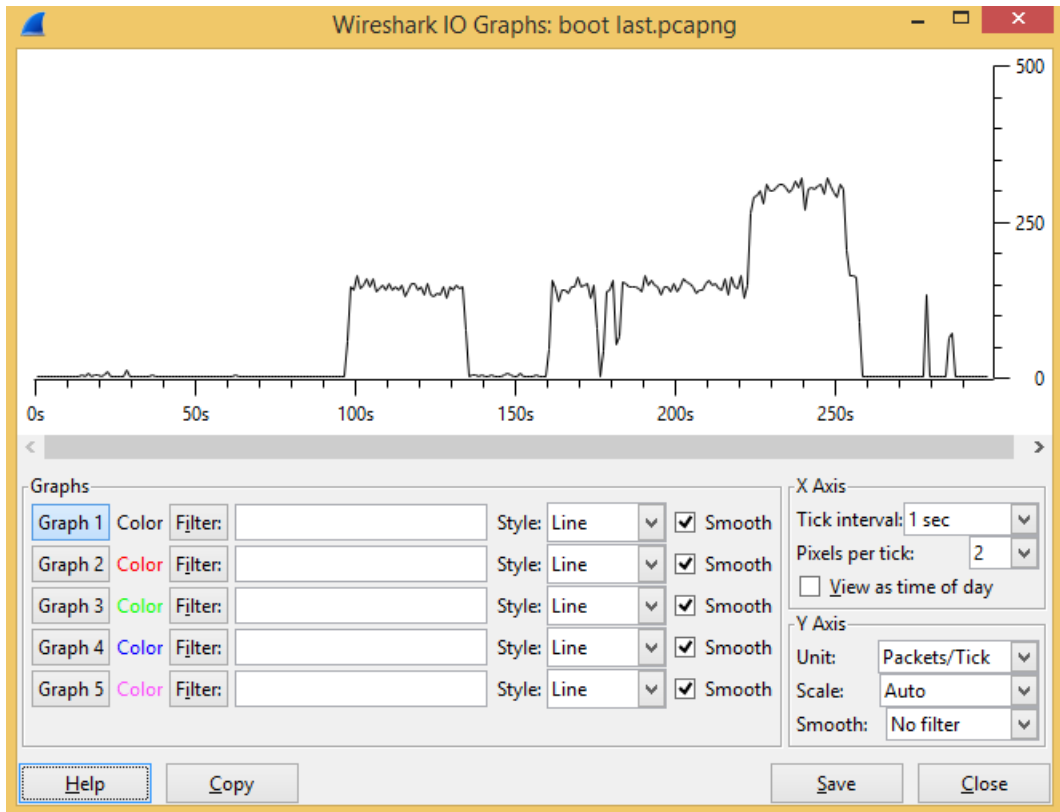
**Figure 5.34** Packet lengths

### 5.5.6 I/O Graph

This graph has two axis:

1. X Axis: consists of the following:
  - Tick interval: 1 second interval in our case.
  - Pixels per tick: we used 2 pixels per tick interval
2. Y Axis
  - Unit: in this capture the unit for the y direction was Packets/Tick.

As we can see the graph below, from time interval 0 – 96 there were small packets sending bidirectionally represented by ICMP Neighbor Solicitation and Advertisement, CDP packets and OSPF Hello Message and LSAs to complete the routing tables for all devices. Then Ankara router started to send traffic to İzmir router until second 134 with almost over 150 packets per second. However, the maximum throughput was between the period of time from 223.9 to 257 when the two devices started to send packets back and forth to each other simultaneously with more than 300 packets per second.



**Figure 5.34** I/O Graph

## CHAPTER SIX

### CONCLUSION

In this thesis we tried to build the campus of our university (University of Turkish Aeronautical Association) by following typical Cisco hierarchy, deploy IPv6 as layer 3 addressing protocol, use dynamic routing protocol for the inter and intra-campus connections, OSPFv3 as our routing protocol to apply it on the three geographically separated campuses on in a simulated environment. The significance we have acquired from applying dynamic routing protocol (OSPFv3 is our case study) is represented by getting rid of old method of routing (static routing) and automatically updating of routing table entries for the changes in network topology. The routing tables at our campus are maintained and built automatically through ongoing communication. Devices of our topology have become dynamic that use routing OSPF to facilitate the ongoing communication and dynamic updating of routing tables. At our university, we use private addressing because we have a shortage of internet addresses and we don't want to pay to assign public address to all of our computers. But, in IPv6 we have enough IP addresses to give every device an IP address in the campus for years and years to come. We don't have shortage anymore, so, this whole concept of private IP address is gone away. This has been done by using one kind of addressing which is called GLOBAL SCOPE or what people are calling the internet 2. Global scopes are addresses that are alive on the internet. Now, the good news is that our university is now able to have internet addressing for every device that is available within the campus. The study sought to answer these questions:

With the scarcity of IPv4 address, what would happen if our campus grows up?

If we deployed IPv6, is it beneficial to work with it?

Why do we need to upgrade to IPv6?

How OSPF affects our topology?

### **6.1 Findings:**

This section will synthesize the empirical findings to answer the study's two research questions:

We live in inevitably IPv4 exhaustion crisis due to the dramatically increasing of the number of devices and people that connect to networks each and every day which is not bad. IPv6 was originally created as the solution to this problem. Our university has a few buildings and faculties, so, when it grows up, we are armed ourselves with the enormous number of globally reachable IP addresses. Though, we ended up having internet address on each host (end device) as well as enough room for the future.

There are a lot of benefits we had by applying IPv6 on our campus like the reduced size of IPv6 header in comparison to IPv4 header. The IPv6 header structure has been completely overhauled, and many features that were afterthoughts and addendums in IPv4 are now included as standards in IPv6. The headers have half the fields, and they are 64 bits, which provides us high processing speed compared to IPv4. Most of the information that used to be within the IPv4 header was eliminated, and now we can choose to put it, back into the header of IPv6 in the form of optional extension headers that come right after the basic header fields. By default, IPv6 has improved included many of features as standard and mandatory. One of these new standards is IPsec which is a feature that gives end-to-end security.

It is worth the upgrade! Not only because IPv6 gives us lots of addresses ( $2^{128} =$  definitely enough), but there are tons of other features built into IPv6 that make it well worth the time, effort, and cost required to migrate to this version.

On the other side of our campus network OSPF is most popular open standard routing protocol that provides us flexibility. It initially builds up the shortest path tree using Dijkstra algorithm then advertises the routing table to the neighbors OSPF supports multiple, equal-cost routes to the same destination as well as it can work with both routed protocols. Performance analysis of OSPF is carried out to see the throughput of OSPF over a campus armed with IPv6 and how it sends its packets

throughout the entire network by checking some packet to what's inside. In this study packets from another routing protocol injected inside OSPF domain as well. With this work, the packet capture application shows us hello messages are being sent almost every 10 second by each device running OSPF making the network operates in better stable way. Update advertisements arrive with minimum time of 1 second. The packet will die after 40 seconds if it did reach the destination.

## **6.2 Limitations:**

Our emulator Graphical Network Simulator GNS3 provides the feature of connecting any simulated topology directly to the internet via network connector of the PC that runs GNS3. However, we couldn't connect our topology to the internet because we needed a public IPv4 address in order for us to make tunneling as we are running IPv6 on our simulated network and our ISP is running IPv4. So to connect between two network deploying two different routed protocol, it needs public IPv4 address.

Adding redundant core switch and main router to each single campus is vital process to make redundancy which is so critical in case of going down of one core switch makes the other one carry the traffic of the network until fixing the problem. But, redundant links need running Spanning Tree Protocol to prevent looping possibility.

It would be awesome to apply all the configuration on a real world campus by using Cisco equipment for both wired and wireless devices with better results. In addition, we can make the realistic topology running dual stack protocols.

## **6.3 Future studies:**

This work is done by using simulated environment. We can connect this topology to the internet as well as making tunnel from IPv6 to IPv4 as we surfing the internet as long as we get a public IP address.

It can be extended with redundancy and applying the configuration of STP on redundant devices in order not to have packets loops.

Upgrading our existing IP network to IPv6 in reality on real devices, Cisco or other vendors.

#### **6.4 Conclusion:**

In the light of presented findings within the limitations, we conclude that the potential impact of applying IPv6 with OSPF on our campus can give us enormous benefits in spite of the challenges the encounter deploying IPv6. Therefore, the following research questions targeted in the thesis have been approached and encouraging positive answers have been found:

With the scarcity of IPv4 address, what would happen if our campus grows up?

We found the solution to that problem by the migration to next generation of IP that provides huge number of addresses for this time and years to come.

If we deployed IPv6, is it beneficial to work with it?

IPv6 offers a lot of benefits and built in features, more efficient and scalable and less overhead.

Why do we need to upgrade to IPv6?

4.3 billion is the total available number of IPv4 addresses. We all know that we don't use most of those. We will still run out IP, and it's going to happen in a few years even though with the help of Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) to extend the inevitable of addresses.

How OSPF affects our topology?

OSPF has the ability to represent an entire network within its link-state database, which dramatically reduces the time required for convergence. OSPF allows us to take a large OSPF topology and break it down into multiple, more manageable areas (3 areas in our case study) to reduce the overhead on the devices.

We keep in that up to now most of the internet usage is via IPv4 due to CIDR and NAT, but, it is a good idea to be well prepared for the transition process to IPv6 at any time despite of the potential challenges face IPv6.

We recommend that the University of Turkish Aeronautical Association focuses on the problems expounded in our research to overcome the shortage of IPv4 and be ready to pave the road of transition to the new technologies of IPv6. In addition, we recommend that there be a focus on the enormous benefits of IPv6, thereby leading to increase the range of global addresses.

## REFERENCES

- [1] Kozierek, Charles M. 2005, “The TCP/IP guide: a comprehensive, illustrated Internet protocols reference”, No Starch Press.
  
- [2] Geoff Huston, October 2006, “Considerations on the IPv6 Host Density Metric”, RFC 4692.
  
- [3] Vince Fuller, Tony Li, August 2006, “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan”, RFC 4632.
  
- [4] Kjeld Borch Egevang, Paul Francis, May 1994, “The IP Network Address Translator (NAT)”, RFC 1631.
  
- [5] Stephen E. Deering, Robert M. Hinden, December 1998, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460.
  
- [6] Robert M. Hinden, Stephen E. Deering (Editors), December 1995, “IP Version 6 Addressing Architecture”, RFC 1884.
  
- [7] Amoss, John J., Daniel Minoli, 2007, “Handbook of IPv4 to IPv6 transition: Methodologies for institutional and corporate networks”, CRC Press.



- [8] AHMET DEMİRÖZ, June 2011, “Adaptation of IPv6 to a campus network: Mugla University case”, master thesis.
  
- [9] Toby Velte. Anthony Velte, August 2013, “Cisco a Beginner's Guide”, McGraw-Hill, 5th edition.
  
- [10] James Edwards, Richard Bramante, 2009, “Networking Self-Teaching Guide”, Wiley Publishing.
  
- [11] Behrouz A. Forouzan, 2010, “TCP/IP Protocol Suite”, McGraw-Hill, 4th edition.
  
- [12] Michael Valentine, Andrew Whitaker, 2008, “CCENT Exam Cram”, Que Publishing, 3rd edition.
  
- [13] Troy McMillan, November 29, 2011, “Cisco Networking Essentials”, John Wiley & Sons, Inc.
  
- [14] Donald E. Eastlake, September 2008, “IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters”, RFC 5342 (Draft Standard).
  
- [15] Kevin Wallace, 2012, “CompTIA Network+ N10-005 Authorized Cert Guide”, Pearson Education, Inc.
  
- [16] Jeffrey s. Beasley, Piyasat Nilkaew, 2012, “Networking Essentials”, Third Edition, Pearson Education, Inc.

- [17] Wendell Odom, 2013, “Cisco CCENT/CCNA ICND1 100-101, Official Cert Guide”, Cisco Press.
- [18] David C. Plummer, November 1982, “An Ethernet Address Resolution Protocol”, or “Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware”, RFC 826 (Draft Standard).
- [19] Stuart Cheshire, July 2008, “IPv4 Address Conflict Detection”, RFC 5227 (Draft Standard).
- [20] Emmett Dulaney, Mike Harwood, 2012, “CompTIA Network+ N10-005 Authorized Exam Cram”, Pearson Education, Inc.
- [21] Information Sciences Institute, University of Southern California, September 1981, “Internet Protocol”, RFC 791 (Draft Standard).
- [22] Darril Gibson, 2011, “Microsoft Windows Networking Essentials”, Wiley Publishing.
- [23] Jeff Doyle, Jennifer DeHaven Carroll, April 11, 2001, “Routing TCP/IP, Volume II (CCIE Professional Development)”, Cisco Press.
- [24] Anthony Sequeira, June 2013, “Interconnecting Cisco Network Devices, Part 1 (ICND1) Foundation Learning Guide”, Fourth Edition, Cisco Press, Reviewed from:  
<https://www.safaribooksonline.com/library/view/interconnecting-cisco-network/9780133410235/ch06.html>

- [25] Jerry FitzGerald, Alan Dennis, January 9, 2009, “Business Data Communications and Networking”, Wiley publishing.
  
- [26] Javvin Technologies, May 15, 2007, “Network Protocols Handbook”, 4th Edition, Javvin Press.
  
- [27] Todd Lammle, 2007, “CCNA Cisco Certified Network Associate Study Guide”, Sixth Edition, Wiley Publishing, Inc.
  
- [28] Michael Dooley, Timothy Rooney, 2013, “IPv6 Deployment and Management”, John Wiley & Sons, Inc.
  
- [29] Diane Teare, 2008, “Designing for Cisco Internetwork Solutions (DESGN), Authorized Self-Study Guide”, Second Edition, Cisco Press.
  
- [30] Information Sciences Institute, University of Southern California, September 1981, “Internet Protocol”, RFC 791 (Draft Standard).
  
- [31] Behrouz A. Forouzan, 2010, “TCP/IP Protocol Suite”, McGraw-Hill, 4th edition.
  
- [32] Kathleen Nichols, Steven Blake, Fred Baker, David L. Black, December 1998, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2474 (Draft Standard).
  
- [33] Qing Li, Tatuya Jinmei, Keiichi Shima, 2007, “IPv6 Advanced Protocols Implementation”, Elsevier Inc.

- [34] Craig Partridge, June 1995, “Using the Flow Label Field in IPv6”, RFC 1809 (Draft Standard).
- [35] J. D. Wegner, Robert Rockell, 2000, “IP Addressing and Subnetting, Including IPv6”, Syngress Media.
- [36] <http://ipv6now.com.au/primers/IPv6Reasons.php>.
- [37] Silvia Hagen, 2014, “IPv6 Essentials”, 3rd edition, O’Reilly Media, Inc.
- [38] Robert M. Hinden, Stephen E. Deering, July 1998, “IP Version 6 Addressing Architecture”, RFC 2373 (Draft Standard).
- [39] Rick Graziani, 2013, “IPv6 Fundamentals A Straightforward Approach to Understanding IPv6”, Cisco Press.
- [40] Stephen E. Deering, Robert M. Hinden, December 1998, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460 (Draft Standard).
- [41] Joseph Davies, 2012, “Understanding IPv6”, Third Edition, Microsoft Inc.
- [42] Dursun Turan Üstündağ, January 2009, “Comparative Routing Performance Analysis of IPv4 and IPv6”, Master Thesis.
- [43] Suleeman Khateeb, April 2013, “Developing Computer’s Networks by Moving from IPv4 to IPv6 and Works Done to Improve Performance in IPv6 and IPv4 Networks”, Master Thesis.

- [44] [http://www.ipv6.net.tr/index.php?option=com\\_content&view=article&id=85&Itemid=89](http://www.ipv6.net.tr/index.php?option=com_content&view=article&id=85&Itemid=89), 26/05/2015.
- [45] Tayfun Acarer, December 2010, “Recent developments regarding IPv6 in Turkey”, Information Technologies Department, ICTA.
- [46] <http://www.gen6.eu/home>, <http://www.gen6.eu/eGov-Turkey>, 26/05/2015.
- [47] Fred Baker, Rob Coltun, November 1995, “OSPF Version 2 Management Information Base”, RFC 1850.
- [48] Jeff Doyle, Jennifer DeHaven Carroll, April 11, 2001, “Routing TCP/IP, Volume II (CCIE Professional Development)”, Cisco Press.
- [49] Jeff Doyle, November 01, 2005, “OSPF and IS-IS: Choosing an IGP for Large-Scale Networks”, Addison Wesley Professional.
- [50] Cisco Systems, Inc., February 1, 2010, “Cisco Active Network Abstraction 3.7 Reference Guide”.
- [51] John Moy, April 1998, “OSPF Version 2”, RFC 2328.
- [52] Rob Coltun, Dennis Ferguson, John Moy, Acee Lindem (editor), July 2008, “OSPF for IPv6”, RFC 5340.
- [53] Cisco Systems, Inc., March 5, 2009, “Cisco IOS IPv6 Configuration Guide”, Cisco Press.

- [54] Cisco Systems, Inc., July 20, 2011, “Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x”, Cisco Press.
- [55] Yi Yang, Alvaro Retana, Abhay Roy, January 2013, “Hiding Transit-Only Networks in OSPF”, RFC 6860.
- [56] John Moy, March 1994, “Multicast Extensions to OSPF”, RFC 1584.
- [57] Cisco Systems, Inc., 2015, “IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY”, Cisco Press.
- [58] John T. Moy, 1998, “OSPF; Anatomy of an Internet Routing Protocol”, Addison-Wesley.
- [59] John Moy, April 1998, “OSPF Version 2”, RFC 2328.
- [60] Thomas M. Thomas, 2003, “OSPF Network Design Solutions”, Second Edition, Cisco Press.
- [61] Cisco Networking Academy, May 2, 2014, “Connecting Networks Companion Guide” (1st ed), Cisco Press, Retrieved from:  
<http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>
- [62] Troy McMillan, November 2011, “Cisco Networking Essentials”, John Wiley & Sons, Inc., Retrieved from:  
<https://www.safaribooksonline.com/library/view/cisco-networking-essentials/9781118097595/>

- [63] Catherine Paquet & Diane Teare, December 2005, "Campus Network Design Fundamentals", Cisco Press, Retrieved from:  
<https://www.safaribooksonline.com/library/view/campus-network-design/1587052229/>
- [64] Cisco Networking Academy, "Catalyst 3750-X and 3560-X Switch Software Configuration Guide", Cisco Press, Retrieved from:  
[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg.html)
- [65] David Hucaby, Stephen McQuerry, October 8, 2002, "Cisco Field Manual: Catalyst Switch Configuration", Cisco Press, Retrieved from:  
<http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=4>  
<http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>
- [66] "RedNectar" Chris Welsh, October 2013, "GNS3 Network Simulation Guide", Packt publishing.

## CURRICULUM VITAE

### PERSONAL INFORMATION

**Name, Surname:** Mohammed AL-DAGDOOG

**Date and Place of Birth:** 30.04.1985 / Iraq – Babel.

**Marital Status:** Single.

**Phone:** 00905380797083

**Email:** moha\_th85@yahoo.com.



### EDUCATION

**High School:** AL-Hillah Secondary School, 2003.

**Undergraduate:** Babylon University / college of Science / Department of Computer, 2008.