



**Sudan University of Science and Technology**  
**Collage of Graduate Studies**



M.Sc. Program in Electronics Engineering

## **Internet Protocol version 6 on virtual private Network provider edge routers**

**تنفيذ بروتوكول الإنترنت السادس على الموجهات الطرفية لمقدم  
خدمة الشبكة الخصوصية الافتراضية**

*A Thesis Submitted In Partial Fulfillment for the Requirements of Degree of M.Sc in  
Electronic Engineering (Computer and Network Engineering)*

**Prepared By**

**SAMAH KHATMI MOHAMED ABU AOUF**

**Supervisor**

**DR.AHMED ABDALLAH**

May 2017

## الآية

### بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قال تعالى:

( هُوَ اللَّهُ الَّذِي لَا إِلَهَ إِلَّا هُوَ عَالِمُ الْغَيْبِ وَالشَّهَادَةِ هُوَ الرَّحْمَنُ الرَّحِيمُ

(22) هُوَ اللَّهُ الَّذِي لَا إِلَهَ إِلَّا هُوَ الْمَلِكُ الْقُدُّوسُ السَّلَامُ الْمُؤْمِنُ الْمُحْيِي

الْمُتَكَبِّرُ الْمُنْتَهَى سُبْحَانَ اللَّهِ عَمَّا يُشْرِكُونَ (23) هُوَ اللَّهُ الْخَالِقُ

الْبَارِئُ الْمُصَوِّرُ لَهُ الْأَسْمَاءُ الْحُسْنَى يُسَبِّحُ لَهُ مَا فِي السَّمَاوَاتِ وَالْأَرْضِ وَهُوَ

الْعَزِيزُ الْحَكِيمُ (24))

سورة الحشر

## **DEDICATION**

To the candles which burns to light my life  
my mother and father

To the source of inspiration  
my husband

To those who have made it possible  
my teacher

To who encouraged us  
Sisters, brothers and friends

## ACKNOWLEDGEMENT

First of all I would like to give lightly appreciated thanks to **ALLAH** the greatest bidder for all the blessings that He has Also I would like to thank everyone whom helped me to design, prepare and write this project.

All thanks and respect to:

- ✚ Dr. Sami Salih who proposed this project.
- ✚ To Prf. Mhamoud who helped me to solve all the problems which facing me.
- ✚ To my friends “Asma, Arwa and Reem for the great help which they did to me.
- ✚ And special thanks for the source of inspiring and determination “my husband” who was with me in every step.

Also I would like to acknowledge and thank Eng. Ahmed Abdullah to give me the honor of being the supervisor of my thesis project which had been improved and developed by his efforts

## ***ABSTRACT***

The Internet protocols that is predominantly deployed and extensively used throughout the world. IPv6 is an IP protocol designed to replace IPv4. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits. This provides more than enough globally unique IP addresses for every network device on the planet. This research concerns with the design of IPv6 VPN Provider Edge (6VPE) over Multi Protocol Label Switching Network (MPLS) without changing network backbone. This is because existing MPLS IPv4 infrastructure needs to be migrated to MPLS IPv6 infrastructure which is very expensive. It was applied using Graphical Network Simulator (GNS3). The performance parameters like success rate and the minimum, average and maximum round – trip time, latency have been evaluated and analyzed compared with IPv4. The results obtained reveal the applicability, performance as well as usefulness in employing 6VPE in MPLS.

## المستخلص

بروتوكولات الإنترنت تم نشرها في الغالب وتستخدم على نطاق واسع في جميع أنحاء العالم. بروتوكول الإنترنت الإصدار السادس صمم لاستبدال بروتوكول الإنترنت الإصدار الرابع. ويضاعف بروتوكول الإنترنت الإصدار السادس عدد بنات عناوين الشبكة من 32 بت في بروتوكول الإنترنت الإصدار الرابع إلى 128 بت في بروتوكول الإنترنت الإصدار السادس , وهذا يوفر عناوين خاصة لبروتوكول الإنترنت لكل مستخدم للشبكة على هذا الكوكب . يهتم هذا البحث بتقديم خدمة الشبكات الافتراضية الخاصة ببروتوكول الإنترنت السادس(6) في بي إي) على تعديل البروتوكول المتعدد(أم بي أل أس) دون الحاجة لتغيير الشبكة الأساسية لأن تحويل البنية التحتية لل (أم بي أل أس) لبروتوكول الإنترنت الإصدار الرابع إلى البنية التحتية لل (أم بي أل أس) لبروتوكول الإنترنت الإصدار السادس مكلفه للغاية. وتم تطبيقه باستخدام محاكاة الشبكة الرسومية. وقد تم تقييم وتحليل معايير الأداء مثل معدل النجاح والحد الأدنى والمتوسط والأقصى لوقت الرحلة ذهابا وإيابا والتأخير والإنتاجية مقارنة مع بروتوكول بروتوكول الإنترنت الإصدار الرابع , ونتيجة لما سبق يمكننا الحصول على أداء جيد وإستفاده قصوى عند تطبيق (6 في بي إي) في ال (أم بي أل أس) .

## Table of contents

<i>الآية</i>	<i>II</i>
<b>ABSTRACT</b>	<b>V</b>
<b>List Of Tables</b>	<b>IX</b>
<b>List Of Figures</b>	<b>X</b>
<b>CHAPTER ONE</b>	<b>1</b>
<b>INTORDUCTION</b>	<b>1</b>
1.1 INTRODUCTION:	1
1.2 Problem Statement:	2
1.3 Research Objectives:	2
1.4 Proposed Solution:	2
1.5 Methodology:	3
The overall methodology used to achieve research objectives and to implement the desired solution can be summarized in the following steps:	3
1.5 Thesis Outlines:	4
<b>CHAPTER TWO</b>	<b>5</b>
<b>BACKGROUND AND LITERATURE REVIEW</b>	<b>5</b>
2.1 Background	5
2.2 PROTOCOL SPECIFICATIONS:	5
2.3 Transition Mechanisms:	8
2.3 .1 Dual Stack	8
2.3.3 Translation:	9
2.4 Multiprotocol Label Switching:	10
2.5 MPLS Header:	11

2.6 MPLS Architecture:	11
2.6.1 Label Switch Router:	12
2.6.2 Label Switched Path:	12
2.6.3 Label Distribution Protocol (LDP):	12
2.7 MPLS Label:	13
2.9 Definition of a VPN:	15
2.10 Architectural Overview of MPLS VPN:	17
2.10.2 Route Distinguisher:	18
2.10.3 Route Distinguisher Number:	18
2.10.4 Route Target:	19
2.11 Deploying IPv6 over MPLS backbone:	19
2.12 Ipv6 VPNs Provider Edge Routers over MPLS:	20
2.12.1 Functions of Routers in 6VPE:	21
2.13 Related Work:	21
<b>Research Methodology</b>	<b>24</b>
3.1 Overall Methodology:	24
The overall methodology used to achieve research objectives and to implement the desired solution can be summarized in the following steps:	24
<b>3.2 System Tool:</b>	<b>25</b>
3.2.1 Graphical Network Simulator (GNS3)	25
3.2.2 GNS3 features:	25
3.3.2 Routers (PE1, PE2, PE3, PE4):	26
3.3.3 CE Routers (CE1, CE2, CE3, CE4):	26
3.5 Configuring 6VPE:	28
3.5.1 MPLS VPN Create and Assign VRFs	28
<b>CAPTER FOURE</b>	<b>32</b>
<b>RESULTS AND DISCUSSION</b>	<b>32</b>
4.3 Performance Comparisons:	34
<b>CHAPTER FIVE</b>	<b>40</b>
<b>CONCLUSION AND RECOMMENDATION</b>	<b>40</b>
5.1 Conclusion:	40
5.1 Recommendations for Future Work:	40
<b>References</b>	<b>42</b>



<b>Appendix A</b>	<b>A</b>
<b>Appendix B</b>	<b>D</b>

## *List Of Tables*

<i>Table 1</i> Performance Comparison between IPV4 over 6VPE and tunnel...	<b>Error! Bookmark not defined.</b>
<i>Table 2</i> Table 4-2: Performance Comparison between IPV6 over 6VPE and tunnel.	<b>Error! Bookmark not defined.</b>
<i>Table 3</i> Comparison for Latency, throughput and jitter between IPV4 over 6VPE and IPV4 over tunneling mechanism:.....	<b>Error! Bookmark not defined.</b>
<i>Table 4</i> Comparison for Latency, throughput and jitter between IPV6 over 6VPE and IPV6 over tunneling mechanism .....	<b>Error! Bookmark not defined.</b>

## *List Of Figures*

Figure 1 Ipv4 Header and Ipv6 Header.....	<b>Error! Bookmark not defined.</b>
Figure 2 Dual Stack mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 3 Tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 4 Translation mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 5 Figure 2.5: LSP through an MPLS Network.....	<b>Error! Bookmark not defined.</b>
Figure 6: LSP through an MPLS Network.....	<b>Error! Bookmark not defined.</b>
Figure 7: M PLS Label [4].....	<b>Error! Bookmark not defined.</b>
Figure 8: MPLS Forwarding Mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 9: MPLS VPN with VRF.....	<b>Error! Bookmark not defined.</b>
Figure 10: MPLS VPN with VRF.....	<b>Error! Bookmark not defined.</b>
Figure 11: Detailed Explanation .....	<b>Error! Bookmark not defined.</b>
Figure 12: MPLS Interfaces.....	<b>Error! Bookmark not defined.</b>
Figure 13: LDP Neighbor.....	<b>Error! Bookmark not defined.</b>
Figure 14: VPN-A .....	<b>Error! Bookmark not defined.</b>
Figure 15: VPN-B .....	<b>Error! Bookmark not defined.</b>
Figure 16: VPNV6 .....	<b>Error! Bookmark not defined.</b>
Figure 17: Tunneling Mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 18 Figure 3-7: Tunneling Mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 19: Ping from VPN_A to VPN_A.....	<b>Error! Bookmark not defined.</b>
Figure 20 Ping from 6VPE1 to 6VPE2 .....	<b>Error! Bookmark not defined.</b>
Figure 21: IPv4 latency over 6vpe& tunneling mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 22 Figure 4-3: IPv4 latency over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 23: IPv4 latency over 6vpe& tunneling mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 24 Figure 4-4: IPv4 Throughput over 6vpe& tunneling mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 25: ipv4 jitter over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 26 Figure 4-5: ipv4 jitter over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 27 Table 4-4: Comparison for Latency, throughput and jitter between IPV6 over 6VPE and IPV6 over tunneling mechanism: .....	<b>Error! Bookmark not defined.</b>
Figure 28 Figure 4-6: IPv6 latency over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 29 Figure 4-6: IPv6 latency over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 30: IPv6 Throughput over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 31 Figure 4-7: IPv6 Throughput over 6vpe& tunneling mechanism.....	<b>Error! Bookmark not defined.</b>
Figure 32: ipv6 jitter over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>
Figure 33 Figure 4-8: ipv6 jitter over 6vpe& tunneling mechanism .....	<b>Error! Bookmark not defined.</b>

## ***ABBREVIATION***

ATM	Asynchronous Transfer Mode
BOS	Bottom Of Label Stack
BGP	border gateway protocol
CCNP	Cisco Certified Network Associate
CCNA	Cisco Certified Network professional
CE	Customer Edge
CPU	control processor unite
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
GNS3	Graphical Network Simulator
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IGP	Interior Gateway Protocol
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switch Path
LSR	Label Switch Router
MPLS	Multi Protocol Label Switching
MP-BGP	Multi protocol Border Gateway Protocol
NAT	Network Address Resolution
OPNET	Optimized Network Engineering Tool

OSPF	Open Shortest Path First
P	Provider
PE	Provider Edge
QOS	Quality of service
RD	Route distinguisher
RT	Route targets
TDM	Time Division Multiplexing
Sp	Service provider
SPF	Shortest Path First
TCP	Transmission Control Protocol
TE	Traffic Engineering
TED	Traffic Engineering Database
TTL	Time to Live
UDP	User Datagram Protocol
VPN	Virtual Private Network

# ***CHAPTER ONE***

## ***INTRODUCTION***

### **1.1 INTRODUCTION:**

Currently IP Version 4 (IPv4) delivers critical business application traffic in a so called new world of the Internet. As the evolution goes on, *IP Version 6* (IPv6) is becoming a necessary element of the network. IPv6 will enable businesses to expand their capabilities exponentially without having any limitations or restrictions. As technologies evolve and the adoption of IP enabled devices accelerates, IP will enter a new era as the protocol of choice for communications. Using globally unique IPv6 addresses increases the opportunity for service providers to create new business models and add revenue, and it increases the portfolio of services.

Multiprotocol Label Switching (MPLS) is deployed by many service providers in their IPv4 networks. (MPLS) is an IETF standard that merges layer 2 and layer 3 protocols and uses label switching in the core network, thus reduces the workload of looking the routing table overhead MPLS uses short, length-fixed, locally significant labels in the packet header between layer 2 and layer 3 header and the packets are forwarded according to label rather than by routing protocol in the core of internet Service providers (ISPs). MPLS is a good alternative option for ISPs, who want to introduce IPv6 services to their customers, but changes to their existing IPv4 infrastructure can be expensive and the

cost benefit for a small amount of IPv6 traffic does not make economic sense.

6PE is one approaches for providing IPv6 connectivity over an MPLS core network. The 6PE approach is required as an alternative to the use of standard tunnels. It provides a solution for an MPLS environment.

## **1.2 Problem Statement:**

In February 2011, all IPv4 addresses had vanished. Hence, the existing MPLS IPv4 infrastructure needs to be migrated to IPv6 infrastructure which is very expensive. Dual stack IPv4/IPv6 seems to be the appropriate solution for the migration. However, the dual stack infrastructure such as routers and gateways are rare and expensive and suffer the problems of delay and high CPU utilization resulting from using tunnel mechanism.

## **1.3 Research Objectives:**

- ❖ To implement Ipv6 over MPLS using 6VPE to enable IPv6 sites to communicate with each other over an MPLS IPv4 core network using MPLS label switched paths (LSPs).

- ❖ To analyze and evaluate the performance of data transmission over IPv4 and IPv6 over the Multiprotocol Label Switching (MPLS) backbone

## **1.4 Proposed Solution:**

6vpe is a new technology that allows IPv6 customers to communicate with each other over IPv4 MPLS Provider without any changes in the infrastructure by using 6vpe (IPv6 VPN Provider Edge) (PE)-to-PE routers . These approaches can be taken to avoid fully

upgrading the MPLS backbone, resulting in lower operational cost and acceptable performance.

This feature offers the following options to service providers.

[1] Connecting to other IPv6 networks accessible across the MPLS core.

[2] Providing access to IPv6 services and resources that service provider provides.

[3] Providing IPv6 VPN services without going for complete overhaul of existing MPLS/IPv4 core.

## **1.5 Methodology:**

The overall methodology used to achieve research objectives and to implement the desired solution can be summarized in the following steps:

1. Gathering necessary information to achieve the desired goal.
2. Design a testbed.
3. Applying the design using simulation program. GNS3 is suitable one, therefore, for the most important feature is it possible to bundle with real networks.
4. The network will be designed to simulate the following scenario:
  - ❖ Four routers act as provider router (P) in the core network (IPv4).
  - ❖ Four routers act as 6vpe (Provider Edge (PE)).
  - ❖ Four VPN routers act as customer router (Customer Edge (CE)).
5. Testing the performance of the network.
6. Drawing conclusion

## **1.5 Thesis Outlines:**

The rest of this thesis is organized as follows:

Chapter two reviews migration mechanisms to IPv6, background of MPLS, how it works, architecture, protocols used and overview of IPv6. The chapter also discusses and reviews key related work to the research problem. Chapter three discusses and explains system tools, detailed explanation of the designed testbed and implementation steps. Chapter four represents, discusses and justifies results. Finally chapter five concludes the research and puts recommendations for future researches..



# **CHAPTER TWO**

## **BACKGROUND AND LITERATURE REVIEW**

### **2.1 Background**

The great expansion of the internet, these days, creates more significant alleges. Not only the addressing of new hosts like computer, tablets, laptop, cell phone but also the technologies. This requires an improvement in the overall architecture of the Internet to support the increase number of users, application, and services that use the Internet. Internet Protocol version 6 (IPv6) came to meet the needs that enable us to get all the applications with high transparency and enable inside network environment rules. IPv6 makes important improvements to network topologies dynamically (exp. Peer to peer, client/server or mesh networks). Also, it improves most of networks functions like, notably in security, mobility, auto configuration, quality of service (QOS) and multicasting. IPv6 is proposed to provide Internet with a larger address space and better performance. [1]

### **2.2 PROTOCOL SPECIFICATIONS:**

Addressing is a key function of network layer protocols that enables data communication between hosts, regardless of whether the hosts are on the same network or on different networks. Both IPv4 and IPv6 provide hierarchical addressing for packets that carry data. IPv6

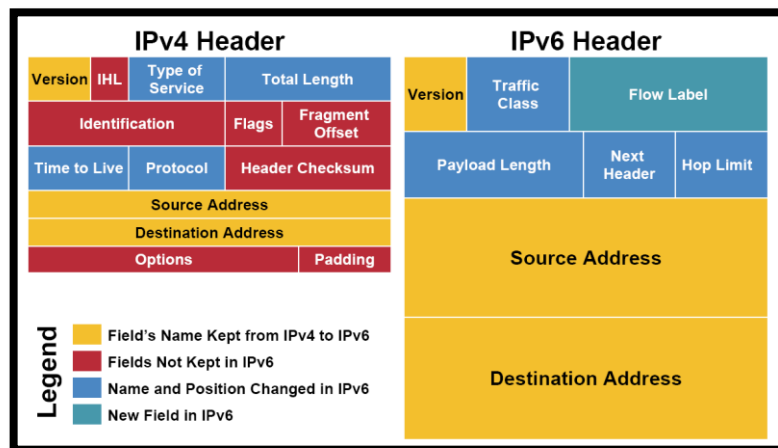
provides for 340 undecillion addresses (the number 340, followed by 36 zeroes). However, IPv6 is much more than just larger addresses; it fixes the limitations of IPv4 and includes additional enhancements.

❖ IPv4 Using the TCP/IP (Transmission Control Protocol/IP) model allowed IPv4 to become the core of the internet addressing as we know it today. In IPv4, addresses are 32-bit binary numbers and can cover 4.3 billion addresses. Some technologies have been employed to postpone the exhaustion of network numbers. The system in use today is referred to as classless addressing. The formal name is Classless Inter-Domain Routing (CIDR). However, this did not provide a long term solution and other technologies, such as NAT and DHCP (Dynamic Host Configuration Protocol) were introduced. IETF (Internet Engineering Task Force), in 1994, began its work for a successor to IPv4 which eventually became IPv6.

❖ IPv6 extends the address space from 32-bits of IPv4 to 128-bits and it supports CIDR as described above and many other features that make it an improvement over IPv4. Unfortunately, IPv6 is not backwards compatible which makes the transition more complicated. In the new IPv6 IPsec (Internet Protocol Security) was integrated, which was optional in IPv4. It is a set of Internet standards that uses cryptographic security services to provide confidentiality, authentication and data integrity. More features can be added to IPv6 due to its option field. Because of its large consumption of resources broadcast traffic is no longer available. Also, there are three modes of addressing for IPv6 packets: Unicast, Multicast and Anycast.

### 2.2.1 Header Differences:

The innovation of IPv6 lies in its header. It is two times larger than IPv4 header and it is formed of a Fixed Header and zero or more Extensions (optional headers). All the essential information for a router is kept in the fixed header. The Extension contains optional information that helps routers to understand how to handle a packet. The IPv6 header has lost some fields that were used in the IPv4 header as you can see in Fig. 1, thus saving time processing the packets. IPv6 fixed header is 40 bytes long while IPv4 is 20 bytes. The version field represents the version of internet protocol.



**Figure 2-1:IPv4 Header and Ipv6 Header**

Traffic class is divided into two parts, the most significant 6 bits are used for Type of service and the least significant two bits are used for Explicit Congestion Notification (ECN). QoS (Quality of Service) management is provided by Flow Label field which is 20 bits. The source labels the sequence to help the router identify that a particular

packet belongs to a specific flow of information. It is designed for streaming/real-time media. Payload Length is 16 bits long and is used to tell the router how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data.

The type of extension header used is detected by the Next Header field. TTL field in IPv4 header is now renamed to its exact meaning Hop Limit and Destination Address are. Source Address both 128 bits and have the same use as in IPv4 header. [2]

### **2.3 Transition Mechanisms:**

An IPv6 transition mechanism is a method to connect the hosts/networks using the same or different IP protocols under some specific IPv6 transition environment. It's the basis of IPv6 transition. The commonly used transition mechanisms can be divided into three categories: Dual stack, Translation and Tunneling.

#### **2.3 .1 Dual Stack**

Dual Stack in simple way mean Both IPv4 and IPv6 will run simultaneously on devices in the network, allowing them to coexist in the ISP network.

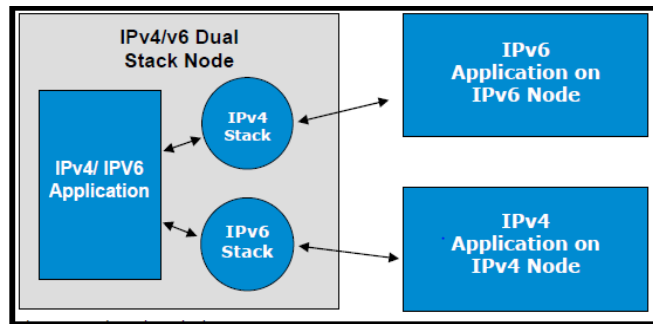


Figure 2-2: Dual Stack mechanism

### 2.3.2 Tunneling:

An IPv6 packet is encapsulated in IPv4 packet and send over an IPv4 network.

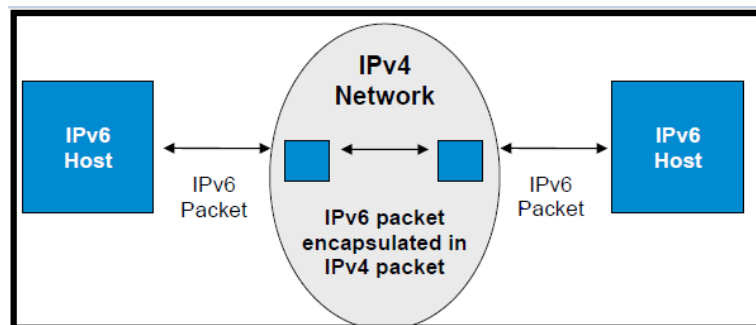


Figure 2-3: Tunneling mechanism

### 2.3.3 Translation:

A similar technique to NAT for IPv4 is used. Using NAT (Network Address Translation), the IPv6 packet is translated to IPv4 packet. [2]

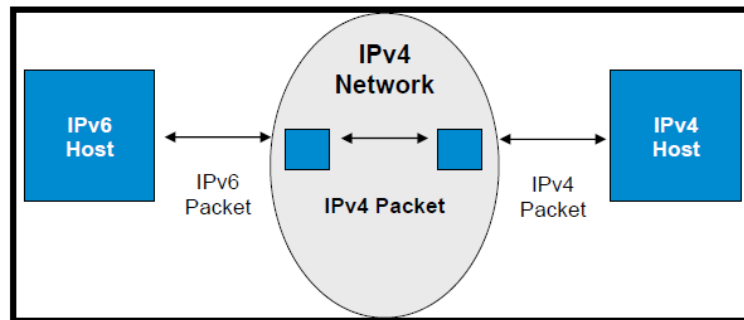


Figure 2-4: Translation mechanism

## 2.4 Multiprotocol Label Switching:

Multiprotocol Label Switching (MPLS) is deployed by many service providers in their IPv4 networks. (MPLS) is an IETF standard that merges layer 2 and layer 3 protocols and uses label switching in the core network, thus reduces the workload of looking the routing table overhead MPLS uses short, length-fixed, locally significant labels in the packet header between layer 2 and layer 3 header and the packets are forwarded according to label rather than by routing protocol in the core of network Service providers , packets are first encapsulated at the ingress router by assigning labels and then forwarded on label switched paths. At the egress router, the label is removed and the packet is delivered to the destination. MPLS is often called the Layer 2.5 technology. It enables easy construction of the explicit routes for a specific source or a service.[3]

## 2.5 MPLS Header:

A 32-bit MPLS header consists of a label field, experimental field, stack, and time to live field. The fields present in the MPLS header are shown in Figure. [4]

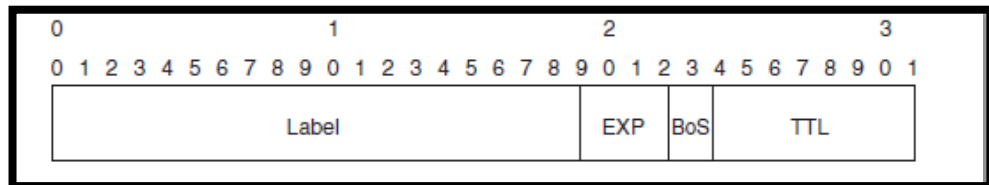


Figure 2.5: LSP through an MPLS Network

MPLS label header length is 32 bits which begins with a 20-bit Label which is used to identify the Label switched path (LSP) to which the packet belongs in the MPLS domain. The labels on the packets are established by using Forwarding equivalency class (FEC). Following the Label field there are 3 bits EXP field which is called as Traffic class field (TC field) this is used for Quality of Service (QoS) related functions. Next field is called stack field which is 1 bit field and this is used to indicate bottom of label stack. The tail consist 8-bit TTL (Time to Live) field which had similar function that of TTL field in IP header. [5]

## 2.6 MPLS Architecture:

The MPLS domain is described as “a contiguous set of nodes which operate MPLS routing and forwarding”. MPLS domain is divided into MPLS core which consists of Label Switch Routers (LSRs)

and MPLS edge which consists of Label Edge Routers (LERs). The main Terminologies of MPLS technology are explained as follows

### 2.6.1 Label Switch Router:

A label switch router (LSR) is a router that supports MPLS. It is capable of understanding MPLS labels and of receiving and transmitting a labeled packet on a data link.

### 2.6.2 Label Switched Path:

A label switched path (LSP) is a sequence of LSRs that switch a labeled packet through an MPLS network or part of an MPLS network. Basically, the LSP is the path through the MPLS network or a part of it that packets take. The first LSR of an LSP is the ingress LSR for that LSP, whereas the last LSR of the LSP is the egress LSR. All the LSRs in between the ingress and egress LSRs are the intermediate.

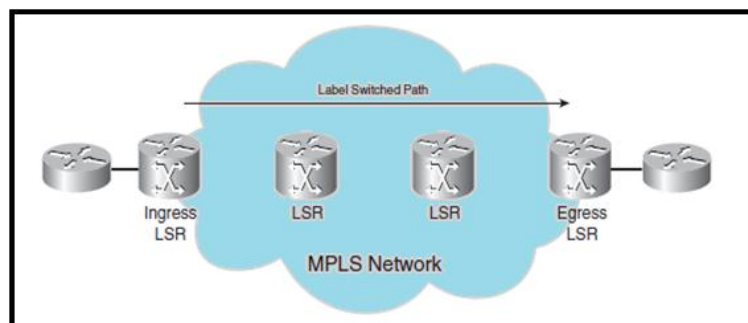


Figure 2.6: LSP through an MPLS Network

### 2.6.3 Label Distribution Protocol (LDP):

LDP is a protocol defined for distributing labels. It is the set of procedures and messages by which Label Switched Routers (LSRs) establish Label Switched Paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched



paths. These LSPs may have an endpoint at a directly attached neighbor (comparable to IP hop-by-hop forwarding), or may have an end point at a network egress node, enabling switching via all intermediary nodes [6]. LDP associates a Forwarding Equivalence Class (FEC) with each LSP it creates. The FEC associated with an LSP specifies which packets are "mapped" to that LSP. LSPs are extended through a network as each. [3]

## 2.7 MPLS Label:

MPLS label is inserted between L2 and L3 headers. The location of the MPLS label is shown in Figure2-7

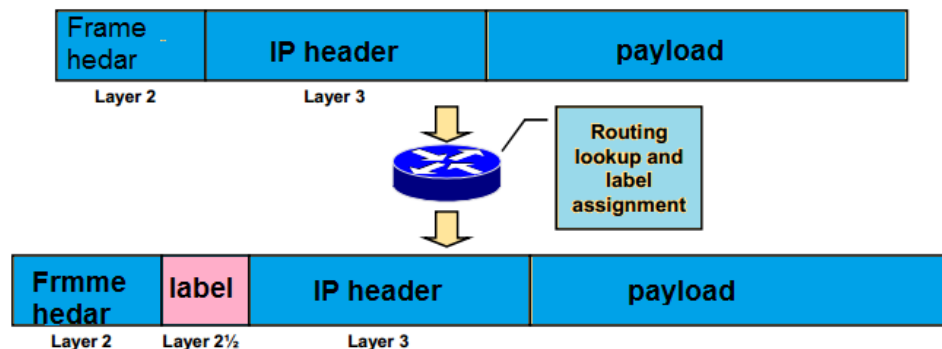


Figure 2.7: M PLS Label [4]

## 12.8 MPLS Forwarding Mechanism:

In a traditional IP forwarding has several drawbacks, routing protocols distributes L3 routing information. Every routing protocol uses destination address for forwarding and every router performs routing lookups. Forwarding decisions are independently taken by each router in the network. This forwarding criterion can be improved by using MPLS

to reduce the number of routing lookups MPLS is a forwarding mechanism which forward packets based on labels. These labels may be IP destination addresses, QoS and source address. MPLS designed support the forwarding of other protocols also. MPLS enabled routers assign labels to define paths between end points, so, only routers on the edge of the network perform a routing lookup. The routing lookup is performed by the router which first receives the packet. In figure the label 25 is given to packet. Instead of routing table lookup, core MPLS router simply looks the label and switches the packet. Then router forwards the packet by swapping the labels. On the edge of the MPLS network last router forward the packet towards its destination

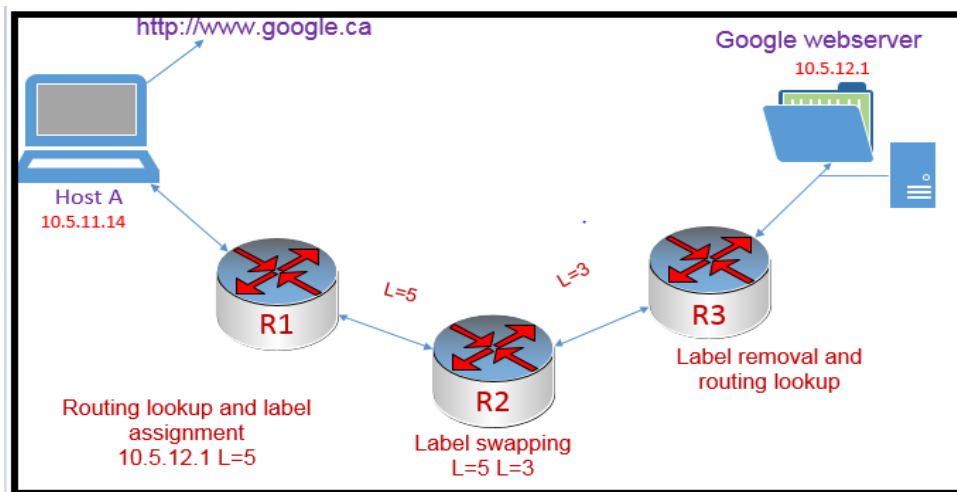


Figure2.8: MPLS Forwarding Mechanism

All routers in Figure 2.5 are configured for MPLS. Only the LER routers perform a routing lookup and assign a label. LSR routers switch packets based on simple label lookups and swap labels. In Figure 5, R1 and R3 are the edge routers while R2 is the core router. To reach web

server 10.5.12.1 from R1, R1 performs route lookup and assigns a label L=5 and forwards the packets while core router R2 performs label lookup and swaps the label to L=3 and forwards the packet. Finally, at the egress end, router R3 removes the label and performs route lookup and delivers data to the destination. [4]

## **2.9 Definition of a VPN:**

A VPN is a network that emulates a private network over a common infrastructure. The private network requires all customer sites to be able to interconnect and be completely separate from other VPNs. The VPN usually belongs to one company and has several sites interconnected across the common service provider infrastructure. Service providers can deploy two major VPN models to provide VPN services to their customers:

- Overlay VPN model
- Peer-to-peer VPN model

### **2.9.1 MPLS VPN**

Before MPLS existed, the peer-to-peer VPN model could be achieved by creating the IP routing peering between the customer and service provider routers. The VPN model also requires privateness or isolation between the different customers. You can achieve this by configuring packet filters (access lists) to control the data to and from the customer routers. Another way to achieve a form of privateness is to configure route filters to advertise routes or stop routes from being

advertised to the customer routes. Or, you can deploy both methods at the same time. Before MPLS came into being, the overlay VPN model was deployed much more commonly than the peer-to-peer VPN model. The peer-to-peer VPN model demanded a lot from provisioning because adding one customer site demanded many configuration changes at many sites. MPLS VPN is one application of MPLS that made the peer-to-peer VPN model much easier to implement. Adding or removing a customer site is now easier to configure and thus demands much less time and effort. With MPLS VPN, one customer router, called the customer edge(CE) peers at the IP Layer with at least one service provider router, called the provider router, edge(PE) router. The privateness in MPLS VPN networks is achieved by using the concept of virtual routing/forwarding (VRF) and the fact that the data is forwarded in the backbone as labeled packets. The VRFs ensure that the routing information from the different customers is kept separate, and the MPLS in the backbone ensures that the packets are forwarding based on the label information and not the information in the IP header. Figure 1-6 shows the concept of VRFs and forwarding labeled packets in the backbone of a network that is running MPLS VPN.[3]

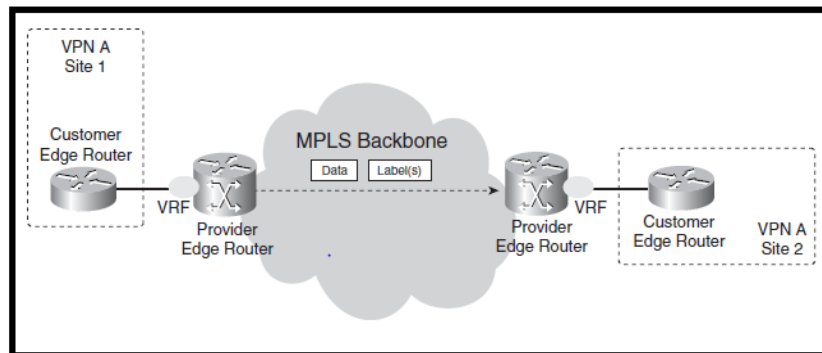


Figure 2.9: MPLS VPN with VRF

## 2.10 Architectural Overview of MPLS VPN:

To achieve MPLS VPN, you need some basic building blocks on the PE routers. These building blocks are the following: VRF, route distinguisher (RD), route targets (RT), route propagation through MP-BGP, and forwarding of labeled packets.

### 2.10.1 Virtual Routing Forwarding:

A virtual routing/forwarding (VRF) is a VPN routing and forwarding instance. It is the name for the combination of the VPN routing table, and the associated IP routing protocols on the PE router. A PE router has a VRF instance for each attached VPN. Look at Figure 2.14 to see that a PE router holds the global IP routing table, but also a VRF routing table per VPN connected to the PE. [3]

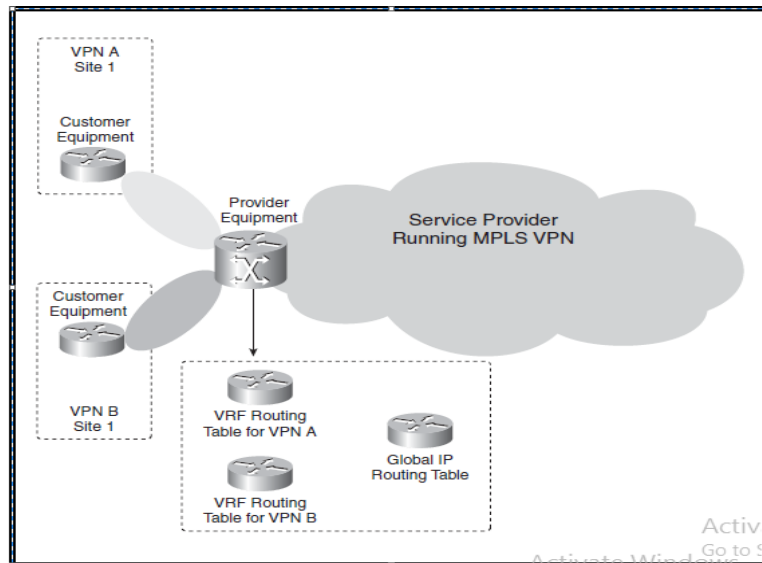


Figure 2.9: MPLS VPN with VRF

### 2.10.2 Route Distinguisher:

An important feature of MPLS VPN architecture is, support of overlapping customer address spaces, which traditional peer-to-peer VPN solution does not support. By deploying single routing protocol for all customer routes exchange between PE routers . Solution to this problem is to expand customer IP prefix which are previously using the same subnet, by using the new prefix that will make each one unique. [3]

### 2.10.3 Route Distinguisher Number:

Route distinguisher is arbitrary configurable number and users allocate numbers for selection. It just differentiates two identical IPv4 routes as two VPNv4 routes from two customers and doesn't have any technical significance. Route distinguisher is viewed as VRF identifier because of one-to-one mapping of route distinguisher and VRF in MPLS VPN implementation. RD can also serve as VPN identifier if there is

only one route distinguisher per customer. But if customer site belongs to more than one VPN it is not implemental. [6]

#### **2.10.4 Route Target:**

Route distinguisher which is pre pended to an IPv4 route is a single entity and it has no ability to show that the site belong to more than VPN.

If a router has membership in several VPNs then a set of VPN identifiers are attached to that route, so the route targets were introduce to support this requirements. [6]

#### **2.11 Deploying IPv6 over MPLS backbone:**

Interconnecting with other IPv6 service providers. Various migration strategies would include deploying IPv6 over IPv4 tunnels, deploying IPv6 using dual stack backbones. Since the networks of large Telecom Service Providers are mostly Multi Protocol Label Switching (MPLS) based therefore the IPv6 will have to be deployed over the MPLS backbones. This is also the fastest up gradation because it requires fewer backbone infrastructure upgrades and lesser configuration of core routers. It is also a very cost-effective strategy.

##### **2.11.1 Different methods for deployment of IPv6 over MPLS backbones:**

- ❖ IPv6 using tunnels on the CE (Customer edge) routers.
- ❖ IPv6 on the provider edge (PE) routers (known as 6PE.
- ❖ Adding IPv6 MPLS VPNs to 6PE (6VPE) this is also the best alternative implementation

- ❖ Native IPv6 MPLS-based backbone this is also the best alternative implementation.

#### **2.11.1.1 IPv6 Deployment Options:**

Today's popular scenario in the SP networks consists of the following:-

- ❖ Core – It is either Native IPv4 or MPLS with associated services

- ❖ Services – These are MPLS L2/L3 VPNs, QoS,.

If an ISP has to be successful in integration, all the above have to be IPv6 complaint. [7]

#### **2.12 Ipv6 VPNs Provider Edge Routers over MPLS:**

6VPE technology which is extended version of Layer 3 virtual private network technology Performance Analysis of IPv6 Transition Mechanisms over MPLS 6VPE can carry an IPv6 or IPv4 virtual private network service. 6VPE is method in which a service provider may use its packet-switched backbone to provide virtual private network services for its IPv6 customer. 6VPE supports multiple IPv6 virtual routing forwarding on provider edge(PE) routers. Multiprotocol-border gateway protocol (MBGP) is used to distribute IPv6 routes over service provider backbone and thus deal with issue of overlapping addresses, redistribution [3].



### **2.12.1 Functions of Routers in 6VPE:**

Ingress 6VPE router-data plane as the ingress 6VPE router receives an IPv6 packet, it looks for the destination address in VRF table. For the prefix learned through the remote 6VPE router, the ingress router does a lookup in the VPN-IPv6 forwarding table. The VPN-IPv6 route has an associated multi protocol label switching (MPLS) label to a MBGP next-hop and an associated L3 VPN service label. The ingress 6VPE router needs to push two MPLS labels in order to send the packets to the egress 6VPE router, where the top label is an MPLS IPv4 label used to reach the egress 6VPE router and the bottom label is an MPLS label that is advertised in MBGP by remote 6VPE for IPv6 prefixes in the VRF. Egress 6VPE router-data plane – As the core router label switch the packets to the correct egress 6VPE through the transport label, the egress 6VPE router receive label-stacked packets from the core. The egress 6VPE router the transport label, and pops the bottom IPv6 L3VPN service label and identifies the target VRF and the address family. A further L3 lookup is performed in the target VRF and the IPV6 packet is sent towards the proper customer edge router in the IPv6 domain. The egress 6VPE forwards unlabeled packets to the customer. [8]

### **2.13 Related Work:**

IPv6 transition mechanisms are widely researched. Listed below are a few of the researches that have been conducted.

IN IPv6 deployment: Real time applications and QoS aspects in this domain describe the implementation and testing of a QoS service on IPv6 networks [9].

IN Migration to Ipv6 from IPV4 by dual stack and tunneling techniques Much research has already been done on transition mechanism and porting of existing IPv4 networks and application to IPv6. Simulate three different methods in the transition from IPv4 to IPv6 (Tunneling, Dual Stack, NAT-PT) . To analysis the traffic between multiple destinations, which allows disparate IPv6 networks to communicate with each other over IPv4 network [10].

IN Analysis of IPv6 transition technologies throughput, delay, loss and other performance parameters of those different transition mechanism are compared[11, 12] .

IN Effect of Packet Delay Variation on Video-Voice over DiffServ-MPLS in IPv4-IPv6 Networks IPv6 has the least latency while comparing with the latency of IPv4 and the throughput depends upon the latency [14].

IN Analysis of IPv6 transition technologies the CPU utilization for tunnel is higher than IPv6, IPv4 and Dual- Stack because the transition technology generates more effort to encapsulate and decapsulate. The Dual-Stack found less delay , but tunnel delay is higher because the packets are not transferred directly, IPv6 has higher throughput than the other four[11].

IN Performance analysis of ipv6 transition mechanisms over mpls The results show that the Dual Stack has the best overall performance

metrics with the lowest delay, lowest jitter, and highest throughput, followed by 6PE; Native IPv6; 6to4 PE-to-PE, 6to4 CE-to-CE [13].

IN Performance analysis of ipv6 transition mechanisms over mpls 2011, 2015 uses multiple methods to provide connectivity to islands of IPv6 over MPLS as 6to4 Tunnel between Customer Edge (CE)-to-CE routers and between Provider Edge (PE)-to-PE routers. The results are then compared against 6PE, IPv6, and Dual Stack all using the MPLS backbone Traffic was generated using database access, email, File Transfer, File Print, Telnet, Video Conferencing over IP, Voice over IP, Web Browsing it was applied in all scenarios [13,12].

IN MPLS VPN using IPv4 and IPv6 protocol The advantages of MPLS VPN are so diverse i.e. it is easily, secure (since a separate VRF is maintained for each customer site) and scalable (no complete mesh between customer sites is required), so it is now the need of service provider to implement. Its ability of combining the plus points of overlay & peer to peer VPN model makes it the priority solution by ISPs to offer their services to the customers. Traffic.

# CHAPTER THREE

## *Research Methodology*

### **3.1 Overall Methodology:**

The overall methodology used to achieve research objectives and to implement the desired solution can be summarized in the following steps:

1. Gathering necessary information to achieve the desired goal.
2. Design a testbed.
3. Applying the design using simulation program. GNS3 is suitable one, therefore, for the most important feature is it possible to bundle with real networks.
4. The network will be designed to simulate the following scenario:
  - Four routers act as provider router (P) in the core network (IPv4).
  - Four routers act as 6vpe (Provider Edge (PE)).
  - Four VPN routers act as customer router (Customer Edge (CE)).
5. Testing the performance of the network.
6. Drawing conclusion

### ***3.2 System Tool:***

There is one tool used in design, Is GNS3 Graphical Network Simulator.

#### **3.2.1 Graphical Network Simulator (GNS3)**

GNS3 is a graphical network simulator that allows simulation of complex networks. GNS3 is an excellent complementary tool to real labs for network engineers, administrators and people want pass certifications such as CCNA and CCNP. It can also be used to experiment features of Cisco IOS, Juniper or to check configurations that need to be deployed later on real router [15] .

#### **3.2.2 GNS3 features:**

- ❖ Design of high quality and complex network topologies.
- ❖ Emulation of many Cisco IOS router platforms.
- ❖ Connection of the simulated network to the real world.
- ❖ Packet capture using Wire shark.

### **3.3 Testbed:**

By using GNS3 software had been designed network topology using Cisco router (7200 ,7300) series because they have feature such as availability ,quality of service and support MPLS and IPv6 Show in Figure 3-1Detailed explanation of the components for simulated network:

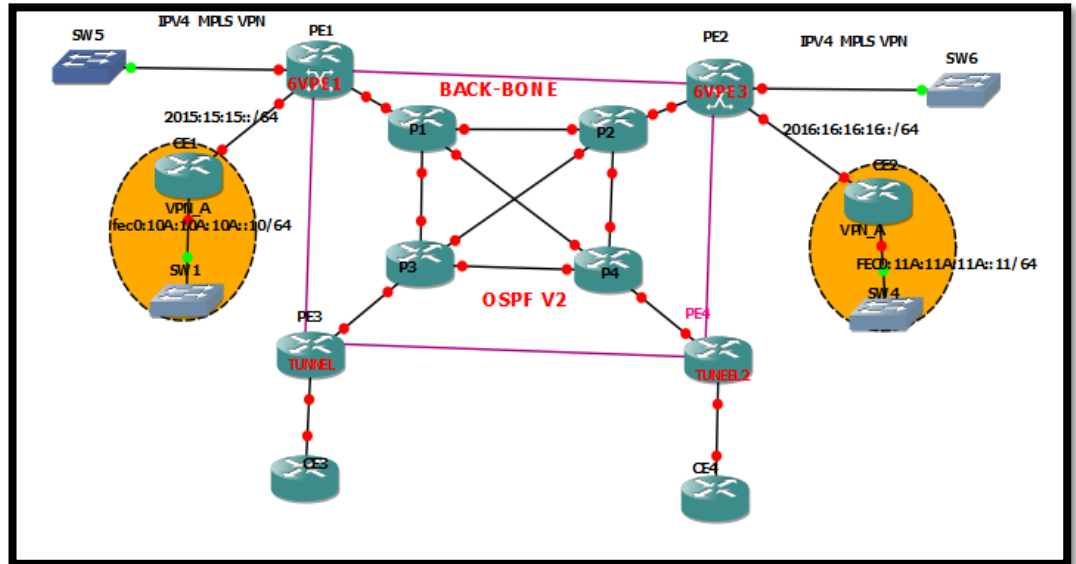


Figure 3-1: Detailed Explanation

### 3.3.1 Routers (P1, P2, P3, P4):

The core routers in the service provider network that connects to provider edge (PE) routers with IPv4 address.

### 3.3.2 Routers (PE1, PE2, PE3, PE4):

The provider edge routers in the service provider network that connects to the customer edge (CE) router with provider router.

### 3.3.3 CE Routers (CE1, CE2, CE3, CE4):

The customer is edge router a router located on the customer premises that provides an Ethernet interface between the customer LAN and provider's core network.

Perform local network using IPv6 address that connects to the provider edge router PE.

### 3.4 MPLS in Core Routers P1, P2, P3 and P4:

MPLS had been enabled on all P-P and P-PE links with the MPLS IP interface command. MPLS is *not* enabled on any CE facing interfaces; CE routers do not run MPLS, just plain IP routing. LDP is enabled automatically as the default label distribution protocol. MPL configurations see in Appendix A.

We can verify the configuration of MPLS interfaces with # show Mpls interface (Example P1 router)

```
R1#
R1#ENABLE
R1#SHOW MPLS INT
Interface          IP          Tunnel      Operational
FastEthernet0/0    Yes (ldp)   No          Yes
FastEthernet0/1    Yes (ldp)   No          Yes
FastEthernet1/0    Yes (ldp)   No          Yes
FastEthernet2/0    Yes (ldp)   No          Yes
R1#
```

Figure 3-2: MPLS Interfaces

LDP adjacencies can be verified with the command #show Mpls Ldp

```
R1#
R1#show mpls ldp neighbor
Peer LDP Ident: 192.168.2.1:0; Local LDP Ident 192.168.1.1:0
TCP connection: 192.168.2.1.29605 - 192.168.1.1.646
State: Oper; Msgs sent/rcvd: 80/80; Downstream
Up time: 00:50:35
LDP discovery sources:
FastEthernet0/0, Src IP addr: 192.168.12.2
Addresses bound to peer LDP Ident:
192.168.12.2 192.168.23.2 192.168.26.2 192.168.24.2
192.168.2.1
Peer LDP Ident: 192.168.3.1:0; Local LDP Ident 192.168.1.1:0
TCP connection: 192.168.3.1.23237 - 192.168.1.1.646
State: Oper; Msgs sent/rcvd: 81/81; Downstream
Up time: 00:50:35
LDP discovery sources:
FastEthernet2/0, Src IP addr: 192.168.13.3
Addresses bound to peer LDP Ident:
192.168.34.3 192.168.23.3 192.168.39.3 192.168.13.3
192.168.3.1
Peer LDP Ident: 192.168.4.1:0; Local LDP Ident 192.168.1.1:0
TCP connection: 192.168.4.1.55590 - 192.168.1.1.646
State: Oper; Msgs sent/rcvd: 79/80; Downstream
Up time: 00:50:31
```

Figure 3-3: LDP Neighbor

### 3.5 Configuring 6VPE:

We had Two IPv6 sites which connected through our IPv4 MPLS Core network. The connections between the PE and CE routers.

To configure 6VPE we need two step:

1-MPLS VPN Create and Assign VRFs

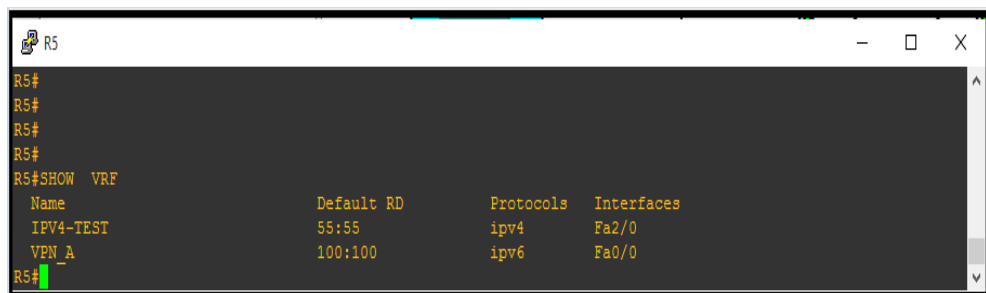
2-Configure MP-BGP between PE and CE Routers

#### 3.5.1 MPLS VPN Create and Assign VRFs

We created customer VRFs on our PE routers and assigned the customer facing interfaces to them. And assigned each VRF a route distinguisher (RD) to uniquely identify prefixes as belonging to that VRF and one or more route targets (RTs) to specify how routes should be imported to and exported from the VRF.

##### 3.5.1.1 Configured VRF VPN-A and VPN-B:

Commands configured VRF VPN-A in PE1,2 and VPN-B in PE 3,4 routers show in Appendix B.

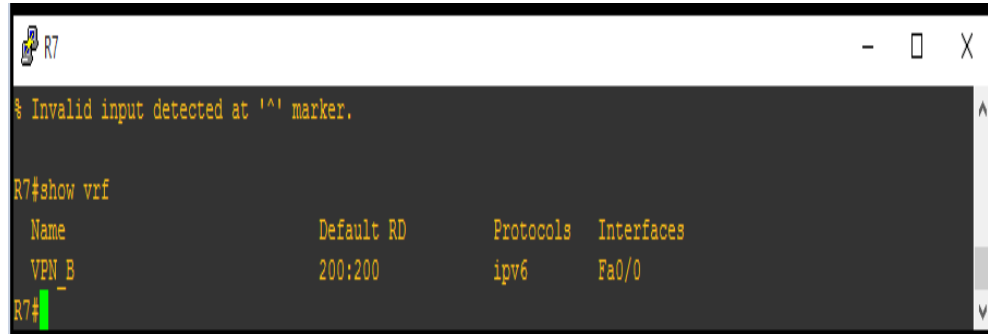


```
R5#
R5#
R5#
R5#
R5#SHOW VRF
Name                Default RD          Protocols  Interfaces
IPV4-TEST           55:55              ipv4       Fa2/0
VPN_A               100:100            ipv6       Fa0/0
R5#
```

Figure 3-4: VPN-A



## Commands configured VRF



```
R7
% Invalid input detected at '^' marker.

R7#show vrf
  Name          Default RD      Protocols  Interfaces
  ----          -
  VPN_B         200:200        ipv6      Fa0/0
R7#
```

Figure 3-5: VPN-B

### 3.5.2 Configure MP-BGP Between PE-CE:

An IGP session has been configured between each PE router and its attached CE routers to exchange routes with the customer sites.

In order to advertise VRF routes from one PE router to the other, we configured multiprotocol BGP (MP-BGP). MP-BGP is a little different from legacy BGP in that it supports multiple *address families* (e.g. IPv4 and IPv6) over a common BGP adjacency. It also supports the advertisement of VPN routes.

MP-BGP runs only on the PE routers P routers rely entirely on the provider IGP and MPLS to forward traffic through the provider network, and CE routers have no knowledge of routes outside their own VRF see in Appendix B.

Address family vpnv6 configure on 6VPE router between the 6VPE and CE router VRF see in Appendix B.

Verify that the 6VPE adjacency between PE1 and PE2 was formed successfully with the comm. and # show bgp vpnv6 unicast all summary:

```

R5#SHOW BGP VPNV6 UNICAST ALL SUMMARY
BGP router identifier 192.168.5.1, local AS number 100
BGP table version is 9, main routing table version 9
6 network entries using 1080 bytes of memory
7 path entries using 756 bytes of memory
5/3 BGP path/bestpath attribute entries using 720 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
3 BGP extended community entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2700 total bytes of memory
BGP activity 13/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2015:15:15:15::10
 4          65010    20    31      9       0     0 00:25:30    2
2016:16:16:16::11
 4          65011     0     0      1       0     0 never      Idle
2020::8      4          800    21    32      9       0     0 00:24:21    1
2020::8      4          800     0     0      1       0     0 never      Idle
192.168.6.1  4          100    19    34      9       0     0 00:24:48    2
192.168.7.1  4          100    18    35      9       0     0 00:24:41    0
192.168.9.1  4          100    21    34      9       0     0 00:24:53    1

```

Figure 3-6: VPNV6

### 3.6 Configure Tunneling Mechanism PE2, PE4 :

Commands configured Tunneling Mechanism in PE2,4 routers show in Appendix C.

```

Tunnel
interface Tunnel0
no ip address
ipv6 address 2001:DB8:2:9::1/64
tunnel source 2001:DB8:2:2::1
tunnel destination 2001:DB8:2:4::2
tunnel mode ipv6
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:2:1::2/64
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
--More--

```

Figure3-7: Tunneling Mechanism

### 3.6 Network Performance Parameters:

To evaluate the network during send any type of traffic that mention above we should define brief the network performance parameters.

The following list provides definitions for network performance that you can use when analyzing precise requirement:[16]

1- Throughput: Quantity of error-free data successfully transferred between nodes per unit of time, usually seconds.

2- Delay (latency): Time between a frame being ready for transmission from a node and delivery of the frame elsewhere in the network.

3- Delay variation (Jitter): The amount of variation in latency/response time, in milliseconds.

### 3.7 Performance metrics for 6VPN over MPLS:

$$\text{Latency} = \frac{\text{Average round trip time for packet}}{2} \text{ (ms)} \quad (1)$$

Latency is the delay from the input into a system to desired output.

$$\text{Throughput} = \frac{\text{Packet size}}{\text{Latency}} \text{ (M bits/s)} \quad (2)$$

Throughput is defined as a ratio of packet size to the latency) [17].

# CAPTER FOURE

## RESULTS AND DISCUSSION

### 4.1 Results and Discussion:

This section provides information that can use to confirm the configuration is working properly. Using ping command to verify the reachability IPV6, IPV4 through 6VPE and tunneling mechanism, and shows the round trip delay to analysis performance metrics for 6VPN over MPLS.

#### 4.2.1 Result of 6VPE Routers:

Using ping command to verify the reachability IPV6, from VPN\_A to VPN\_A through 6VPE, and shows the round trip delay when used different packet size.

```
R10#PING FEC0:11A:11A:11A::11 SIZE 64
Type escape sequence to abort.
Sending 5, 64-byte ICMP Echos to FEC0:11A:11A:11A::11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/164/204 ms
R10#PING FEC0:11A:11A:11A::11 SIZE 100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0:11A:11A:11A::11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/149/176 ms
R10#PING FEC0:11A:11A:11A::11 SIZE 400
Type escape sequence to abort.
Sending 5, 400-byte ICMP Echos to FEC0:11A:11A:11A::11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/164/280 ms
R10#PING FEC0:11A:11A:11A::11 SIZE 800
Type escape sequence to abort.
Sending 5, 800-byte ICMP Echos to FEC0:11A:11A:11A::11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/150/208 ms
R10#PING FEC0:11A:11A:11A::11 SIZE 1000
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to FEC0:11A:11A:11A::11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/143/164 ms
R10#
```

Figure 4-1: Ping from VPN\_A to VPN\_A

## 4.2.2 Result of CE5 Router:

Using ping command to verify the reach ability IPV4, from 6VPE1 to 6VPE2, and shows the round trip delay when used different packet size.

```
R5#PING VRF IPV4-TEST 177.10.10.10 SIZE 400
Type escape sequence to abort.
Sending 5, 400-byte ICMP Echos to 177.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/233/328 ms
R5#PING VRF IPV4-TEST 177.10.10.10 SIZE 100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 177.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 240/317/404 ms
R5#PING VRF IPV4-TEST 177.10.10.10 SIZE 64
Type escape sequence to abort.
Sending 5, 64-byte ICMP Echos to 177.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 196/315/444 ms
R5#
R5#PING VRF IPV4-TEST 177.10.10.10 SIZE 1000
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 177.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/215/240 ms
R5#PING VRF IPV4-TEST 177.10.10.10 SIZE 800
Type escape sequence to abort.
Sending 5, 800-byte ICMP Echos to 177.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 156/225/292 ms
```

Figure 4-2: Ping from 6VPE1to 6VPE2

### 4.3 Performance Comparisons:

Table 4-1: Performance Comparison between IPV4 over 6VPE and tunnel

Packet size(bit)	<i>Ipv4 over 6VPE Round Trip Time (ms)</i>			<i>Ipv4 over tunnel Round Trip Time (ms)</i>		
	<i>Minimum</i>	<i>Average</i>	<i>Maximum</i>	<i>Minimum</i>	<i>Average</i>	<i>Maximum</i>
<b>64</b>	<b>196</b>	<b>315</b>	<b>444</b>	<b>300</b>	<b>560</b>	<b>610</b>
<b>100</b>	<b>240</b>	<b>317</b>	<b>404</b>	<b>420</b>	<b>510</b>	<b>608</b>
<b>400</b>	<b>188</b>	<b>233</b>	<b>328</b>	<b>398</b>	<b>406</b>	<b>570</b>
<b>800</b>	<b>156</b>	<b>255</b>	<b>292</b>	<b>360</b>	<b>440</b>	<b>497</b>
<b>1000</b>	<b>192</b>	<b>215</b>	<b>240</b>	<b>400</b>	<b>432</b>	<b>495</b>

The minimum, average and maximum round –trip time have been analyzed for the transmissions through 6VPE and *tunneling mechanism*. IPv4 in 6VPE has least minimum & average round trip delay than IPv4 in *tunneling mechanism*.

Table 4-2: Performance Comparison between IPV6 over 6VPE and tunnel.

<b>Packet size(bit)</b>	<b><i>Ipv6 over tunnel Round Trip Time (ms)</i></b>			<b><i>Ipv6 over 6VPE Round Trip Time (ms)</i></b>		
	<b><i>Minimum</i></b>	<b><i>Average</i></b>	<b><i>Maximum</i></b>	<b><i>Minimum</i></b>	<b><i>Average</i></b>	<b><i>Maximum</i></b>
<b>64</b>	<b>250</b>	<b>317</b>	<b>410</b>	<b>132</b>	<b>164</b>	<b>204</b>
<b>100</b>	<b>300</b>	<b>355</b>	<b>390</b>	<b>128</b>	<b>159</b>	<b>176</b>
<b>400</b>	<b>200</b>	<b>343</b>	<b>469</b>	<b>96</b>	<b>155</b>	<b>280</b>
<b>800</b>	<b>210</b>	<b>304</b>	<b>424</b>	<b>112</b>	<b>150</b>	<b>208</b>
<b>1000</b>	<b>250</b>	<b>298</b>	<b>327</b>	<b>128</b>	<b>143</b>	<b>164</b>

The minimum, average and maximum round –trip time have been analyzed for the transmissions through 6VPE and *tunneling mechanism*. IPv6 over 6VPE has least minimum & average round trip delay than IPv6 over tunneling mechanism.

Table4-3: Comparison for Latency, throughput and jitter between IPV4 over 6VPE and IPV4 over tunneling mechanism:

Packet size(bit)	IPV4 over 6VPE			IPV4 over <i>tunneling mechanism</i>		
	<i>Latency (ms)</i>	<i>Throughput (M bits/s)</i>	<i>Jitter (ms)</i>	<i>Latency (ms)</i>	<i>Throughput (M bits/s)</i>	<i>Jitter (ms)</i>
<b>64</b>	<b>195</b>	<b>0.32</b>	<b>16.5</b>	<b>245</b>	<b>0.26</b>	<b>31.2</b>
<b>100</b>	<b>160</b>	<b>0.625</b>	<b>27</b>	<b>256</b>	<b>0.36</b>	<b>47</b>
<b>400</b>	<b>123</b>	<b>3.3</b>	<b>26.2</b>	<b>229</b>	<b>1.7</b>	<b>38</b>
<b>800</b>	<b>117</b>	<b>6.8</b>	<b>24.8</b>	<b>216</b>	<b>3.7</b>	<b>50</b>
<b>1000</b>	<b>107</b>	<b>9.3</b>	<b>20.25</b>	<b>211</b>	<b>4.7</b>	<b>45</b>

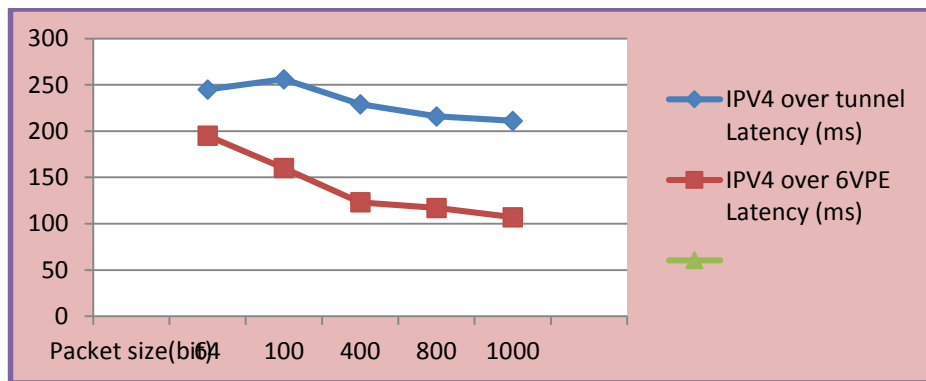


Figure 4-3: IPv4 latency over 6vpe & tunneling mechanism

IPv4 over 6VPE has the least latency while comparing with the latency of IPv4 over tunneling mechanism and the throughput depends upon the latency.



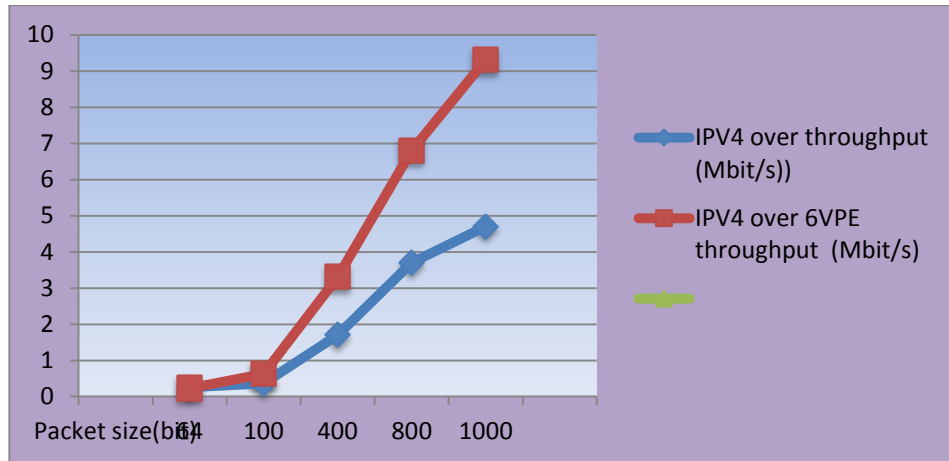


Figure 4-4: IPv4 Throughput over 6vpe& tunneling mechanism

IPv4 over 6vpe has the high Throughput while comparing with the Throughput of IPv4 over tunneling mechanism.

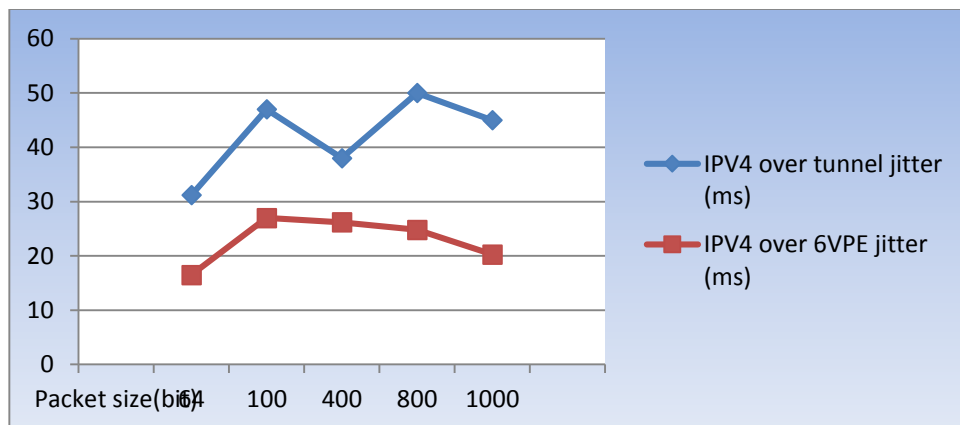


Figure 4-5: ipv4 jitter over 6vpe& tunneling mechanism

IPv6 over 6VPE has the least jitter while comparing with the jitter of IPv4 over tunneling mechanism.

Table4-4: Comparison for Latency, throughput and jitter between IPV6 over 6VPE and IPV6 over tunneling mechanism:

Packet size(bit)	IPV6 over tunneling mechanism			IPV6 over 6VPE		
	<i>Latency (ms)</i>	<i>Throughput (M bits/s)</i>	<i>Jitter (ms)</i>	<i>Latency (ms)</i>	<i>Throughput (M bits/s)</i>	<i>Jitter (ms)</i>
<b>64</b>	<b>174</b>	<b>0.36</b>	<b>20.4</b>	<b>82</b>	<b>0.8</b>	<b>7.5</b>
<b>100</b>	<b>162</b>	<b>0.61</b>	<b>35</b>	<b>78</b>	<b>1.3</b>	<b>12.2</b>
<b>400</b>	<b>168</b>	<b>2.4</b>	<b>30.7</b>	<b>77.1</b>	<b>5.2</b>	<b>15.7</b>
<b>800</b>	<b>156</b>	<b>5.1</b>	<b>16.3</b>	<b>75</b>	<b>10.6</b>	<b>5.5</b>
<b>1000</b>	<b>145.8</b>	<b>6.85</b>	<b>1.8</b>	<b>61.5</b>	<b>16.3</b>	<b>0.5</b>

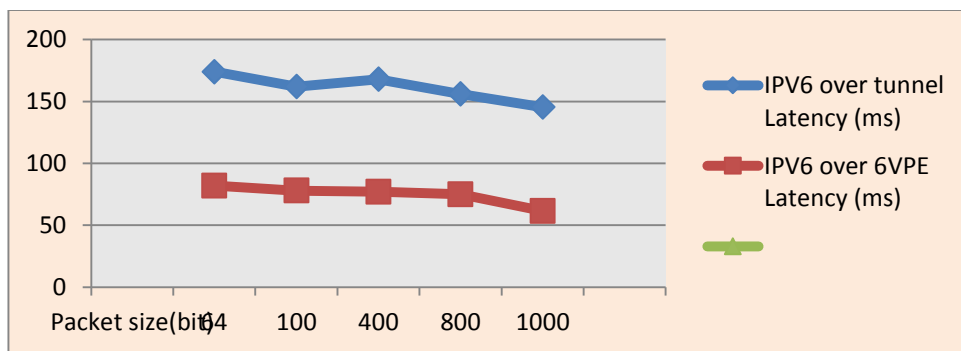


Figure 4-6: IPv6 latency over 6vpe& tunneling mechanism

IPv6 over 6VPE has the least latency while comparing with the latency of IPv6 over tunneling mechanism and the throughput depends upon the latency.

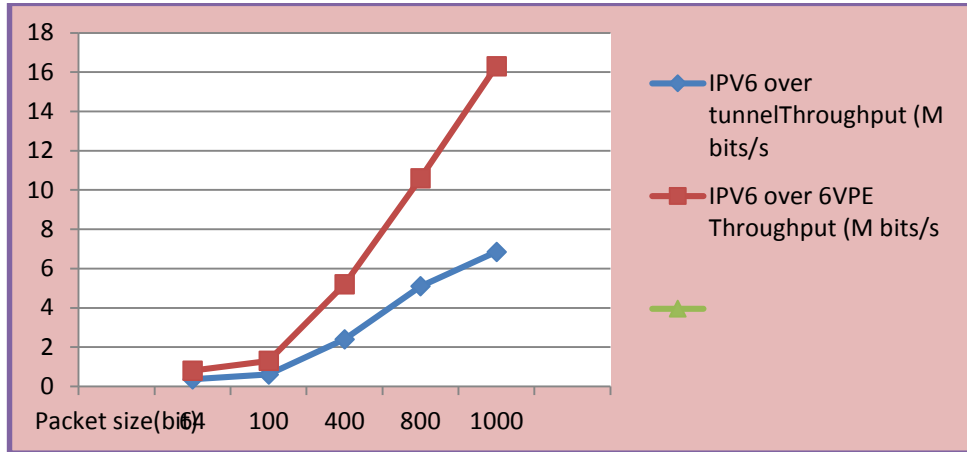


Figure 4-7: IPv6 Throughput over 6vpe& tunneling mechanism

IPv6 over 6VPE has the high Throughput while comparing with the Throughput of IPv6 over tunneling mechanism.

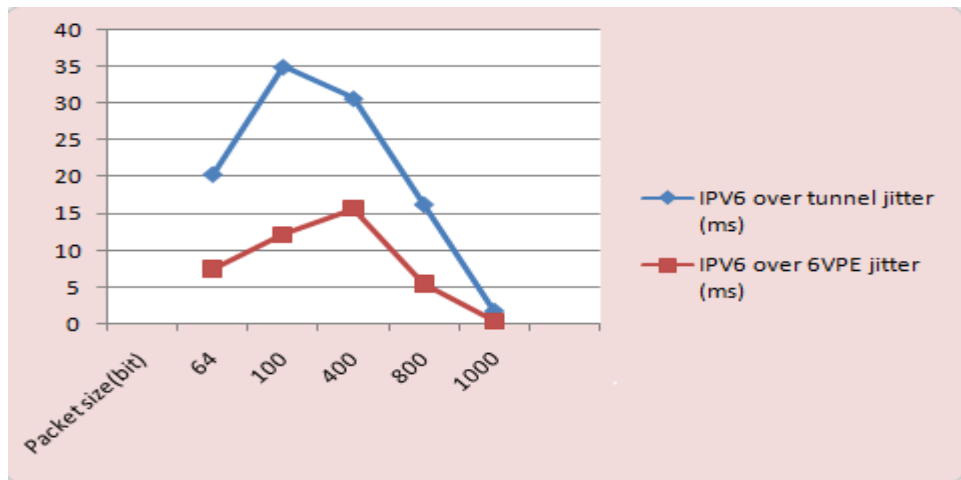


Figure 4-8: ipv6 jitter over 6vpe& tunneling mechanism

IPv6 has the least jitter while comparing with the jitter of IPv6 over tunneling mechanism.

## **CHAPTER FIVE**

### ***CONCLUSION AND RECOMMENDATION***

#### **5.1 Conclusion:**

In this research emulated 6VPE and tunneling mechanism over MPLS network on the GNS3 platform with Cisco IOS is used to evaluate 6VPE and tunneling transition mechanism' performance metrics of time trip delay, latency, jitter, and throughput.

The analyzed results show that the minimum, average and maximum round -trip time for the transmissions through 6VPE technique is less than tunneling mechanism over MPLS.

Latency, jitter and throughput for both IPv6 over 6vpe& tunneling mechanism and IPv4 over 6vpe& tunneling mechanism are calculated and analyzed. 6VPE has the least latency while comparing with the latency of tunnel and the throughput depends upon the latency

These results obtained from this analysis will be critical for those who want to implement 6VPE and are concerned about the performance of the transition mechanisms. Given the acquisition cost, schedule, risk, and technical challenges in supporting IPv6, this analysis will increase confidence about making informed decisions and choosing the appropriate.

This research mainly focuses on comparing performance of 6VPE over MPLS network and IPv4. Future work on the topic can be carried on studying performance of 6VPE over MPLS for real-time and multimedia applications such as VoIP and video.

Further can focus to compare the performance of 6VPE over MPLS with traffic engineering over MPLS.

## *References*

- [1] G. Y. A. Y. Al-Gadi, A. Amin Babiker, N. Mustafa, and M. A. Hamied, "Evaluation and Comparisons of Migration Techniques From IPv4 To IPv6 Using GNS3 Simulator," *Evaluation*, vol. 4, 2014.
- [2] D. Enache and M. Alexandru, "A STUDY OF THE TECHNOLOGY TRANSITION FROM IPv4 TO IPv6 FOR AN ISP," *Review of the Air Force Academy*, p. 117, 2016.
- [3] L. Ghein, "MPLS Fundamentals: A Comprehensive Introduction to MPLS Theory and Practice," ed: Cisco Press, Indianapolis, 2007.
- [4] S. Kathiresan, "Performance Analysis of MPLS over IP networks using CISCO IP SLAs," SIMON FRASER UNIVERSITY, 2015.
- [5] K. Jannu and R. Deekonda, "OPNET simulation of voice over MPLS With Considering Traffic Engineering," *Blekinge Institue of Technology*, vol. 15, 2010.
- [6] S. R. U. Rehman, "Investigation of different VPN Solutions," ed, 2009.
- [7] S. Aravind and G. Padmavathi, " Migration to Ipv6 From IPV4 by Dual Stack and Tunneling Techniques " *Institute of Science and Technology, Chennai, T.N., India. 6 - 8 May 2016. pp.107-111.*
- [8] A. Dumka, H. L. Mandoria, K. Dumka, and A. Anand, "MPLS VPN using IPv4 and IPv6 protocol," in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*, 2015, pp. 1051-1055

- [9] C. Bouras, A. Gkamas, D. Primpas, and K. Stamos, "IPv6 deployment: Real time applications and QoS aspects," *Computer communications*, vol. 29, pp. 1393-1401, 2006.
- [10] S. Aravind and G. Padmavathi, "Migration to Ipv6 from IPV4 by dual stack and tunneling techniques," in *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on*, 2015, pp. 107-111.
- [11] A. Albkerat and B. Issac, "Analysis of IPv6 transition technologies," *arXiv preprint arXiv:1410.2013*, 2014.
- [12] P. Grayeli, S. Sarkani, and T. Mazzuchi, "Performance analysis of ipv6 transition mechanisms over mpls," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, 2011.
- [13] P. Grayeli, S. Sarkani, and T. Mazzuchi, "Performance analysis of ipv6 transition mechanisms over mpls," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, 2015.
- [14] M. Aziz, M. S. Islam, and A. Popescu, "Effect of Packet Delay Variation on Video-Voice over DiffServ-MPLS in IPv4-IPv6 Networks," *arXiv preprint arXiv:1202.1877*, 2012.
- [15] Y. WANG and J. WANG, "Use gns3 to simulate network laboratory," *Computer Programming Skills & Maintenance*, vol. 12, p. 046, 2010.
- [16] P. Oppenheimer, *Top-down network design*: Cisco Press, 2004.

## *Appendix A*

### **Configuration Core Networks (P1, P2, P3, P4)**

```
interface Loopback0
P1 (config)# ip address 192.168.1.1 255.255.255.255
P1 (config)# interface FastEthernet0/0
P1 (config)# ip address 192.168.12.1 255.255.255.0
P1 (config)# interface FastEthernet0/1
P1 (config)# ip address 192.168.14.1 255.255.255.0
P1 (config)# interface FastEthernet1/0
P1 (config)# ip address 192.168.15.1 255.255.255.0
P1 (config)# ip ospf 1 area 0
P1 (config)# mpls ip
P1 (config)# interface FastEthernet2/0
P1 (config)# ip address 192.168.13.1 255.255.255.0
P1 (config)# router ospf 1
P1 (config)# mpls ldp autoconfig area 0
P1 (config)# network 192.168.0.0 0.0.255.255 area 0
```

```
interface Loopback0
P2 (config)# ip address 192.168.2.1 255.255.255.255
P2 (config)# interface FastEthernet0/0
P2 (config)# ip address 192.168.12.2 255.255.255.0
P2 (config)# interface FastEthernet0/1
P2 (config)# ip address 192.168.23.2 255.255.255.0
P2 (config)# interface FastEthernet1/0
P2 (config)# ip address 192.168.26.2 255.255.255.0
P2 (config)# interface FastEthernet2/0
P2 (config)# ip address 192.168.24.2 255.255.255.0
P2 (config)# router ospf 2
P2 (config)# mpls ldp autoconfig area 0
P2 (config)# network 192.168.0.0 0.0.255.255 area 0
```

```
P3 (config)# interface Loopback0
P3 (config)# ip address 192.168.3.1 255.255.255.255
P3 (config)# interface FastEthernet0/0
P3 (config)# ip address 192.168.34.3 255.255.255.0
P3 (config)# interface FastEthernet0/1
P3 (config)# ip address 192.168.23.3 255.255.255.0
P3 (config)# interface FastEthernet1/0
P3 (config)# ip address 192.168.39.3 255.255.255.0
P3 (config)# interface FastEthernet2/0
```



```
P3 (config)# ip address 192.168.13.3 255.255.255.0
P3 (config)# router ospf 1
P3 (config)# mpls ldp autoconfig area 0
P3 (config)# log-adjacency-changes
P3 (config)# network 192.168.0.0 0.0.255.255 area 0

P3 (config)# interface Loopback0
P3 (config)# ip address 192.168.4.1 255.255.255.255
P3 (config)# interface FastEthernet0/0
P3 (config)# ip address 192.168.34.4 255.255.255.0
P3 (config)# interface FastEthernet0/1
P3 (config)# ip address 192.168.14.4 255.255.255.0
P3 (config)# interface FastEthernet1/0
P3 (config)# ip address 192.168.47.4 255.255.255.0
P3 (config)# interface FastEthernet2/0
P3 (config)# ip address 192.168.24.4 255.255.255.0
P3 (config)# router ospf 1
P3 (config)# mpls ldp autoconfig area 0
P3 (config)# network 192.168.0.0 0.0.255.255 area 0
```

## *Appendix B*

### *Configuration 6VPE (PE1, PE2)*

```
PE1(config)# vrf definition VPN_A
PE1(config-vrf)# rd 100:100
PE1(config-vrf)# route-target export 100:100
PE1(config-vrf)# route-target import 100:100
PE1(config-vrf)# route-target import 300:300
PE1(config-vrf A)# address-family ipv6
PE1(config-vrf A)# exit
PE1(config-vrf A)# address-family ipv4
PE1(config-vrf A)# exit
PE1(config-vrf)# interface FastEthernet0/0
PE1(config-vrf)# vrf forwarding VPN_A
```

```
PE1(config-vrf)# ipv6 address 2015:15:15:15::5/64
PE3(config)# vrf definition VPN_B
PE3(config-vrf)# rd 100:100
PE3(config-vrf)# route-target export 200:200
PE3(config-vrf)# route-target import 200:200
PE3(config-vrf)# route-target import 300:300
PE3(config-vrf A)# address-family ipv6
PE3(config-vrf A)# exit
PE3(config-vrf A)# address-family ipv4
PE3(config-vrf A)# exit
PE3(config-vrf)# interface FastEthernet0/0
PE3(config-vrf)# vrf forwarding VPN_B
PE3(config-vrf)# IPV6 ADDRESS 2012:12:12:12::7/64
```

### *Configuration MP-BGP*

```
PE1(config)# router bgp 100
PE1(config-router)# neighbor 2020::8 remote-as 800
PE1(config-router)# neighbor 192.168.5.1 remote-as 100
PE1(config-router)# neighbor 192.168.5.1 update-source Loopback0
PE1(config-router)# neighbor 192.168.7.1 remote-as 100
PE1(config-router)# neighbor 192.168.7.1 update-source Loopback0
PE1(config-router)# neighbor 192.168.9.1 remote-as 100
```

```
PE1(config-router)# neighbor 192.168.9.1 update-source Loopback0
```

```
PE1(config-router)# address-family vpnv6  
PE1(config-router-af)# neighbor 2020::8 activate  
PE1(config-router-af)# neighbor 2020::8 send-community extended  
PE1(config-router-af)# neighbor 192.168.5.1 activate  
PE1(config-router-af)# neighbor 192.168.5.1 send-community both  
PE1(config-router-af)# neighbor 192.168.7.1 activate  
PE1(config-router-af)# neighbor 192.168.7.1 send-community both  
PE1(config-router)# neighbor 192.168.9.1 activate  
PE1(config-router-af)# neighbor 192.168.9.1 send-community  
PE1(config-router-af)# exit-address-family
```

```
address-family ipv6 vrf VPN_A  
PE1 (config-router-af)# neighbor 2015:15:15:15::10 remote as 65010  
PE1 (config-router-af)# neighbor 2015:15:15:15::10 activate  
PE1 (config-router-af)# neighbor 2016:16:16:16::11 remote-as 65011  
PE1 (config-router-af)# neighbor 2016:16:16:16::11 activate  
PE1 (config-router-af)# neighbor 2020::8 remote-as 800  
PE1 (config-router-af)# neighbor 2020::8 activate  
PE1 (config-router-af)# neighbor 2020::8 send-community extended  
PE1 (config-router-af)# exit-address-family  
PE1 (config-router)# address-family vpnv4  
PE1 (config-router-af)# neighbor 192.168.5.1 activate  
PE1 (config-router-af)# neighbor 192.168.5.1 send-community both  
(config-router-af)# neighbor 192.168.7.1 activate  
(config-router-af)# neighbor 192.168.7.1 send-community both  
(config-router-af)# neighbor 192.168.9.1 activate  
(config-router-af)# neighbor 192.168.9.1 send-community extended  
(config-router-af)# exit-address-family
```

```
(config-router)# address-family ipv4 vrf VPN_A  
(config-router-af)# neighbor 172.15.15.10 remote-as 65010  
(config-router-af)# neighbor 172.15.15.10 activate  
(config-router-af)# neighbor 172.16.16.11 remote-as 65011  
(config-router-af)# neighbor 172.16.16.11 activate  
CE1(config-if)# router bgp 65011  
CE1 (config-router)# bgp router-id 11.11.11.11  
CE1 (config-router)# neighbor 2016:16:16:16::6 remote-as 100  
CE1 (config-router)# neighbor 172.16.16.6 remote-as 100  
CE1 (config-router)# address-family ipv6
```

```
CE1 (config-router-af)# neighbor 2016:16:16:16::6 activate
CE1 (config-router-af)# exit.
```

## *Appendix C*

### *Configuration 6VPE (PE3, PE4)*

*IPv6 over IPv6 Tunnel*

*: Configuring PE3*

```
PE3(config)#ipv6 unicast-routing
PE3(config-)#ipv6 cef
PE3(config-router)#interface Tunnel0
PE3(config-router)#no ipv6 address
PE3(config-router)#ipv6 address 2001:DB8:2:9::1/64
PE3(config-router)#tunnel source 2001:DB8:2:2::1
PE3(config-router)#tunnel mode ipv6
PE3(config-router)#tunnel destination 2001:DB8:2:4::2
exit
!
PE3(config-router)#interface FastEthernet0/0
PE3(config-router)#no ipv6 address
PE3(config-router)#ipv6 address 2001:DB8:2:1::2/64
PE3(config-router)#no shutdown
PE3(config-router)#exit
!!
PE3(config-router)#interface Ethernet0/1
PE3(config-router)#no ipv6 address
PE3(config-router)#ipv6 address 2001:DB8:2:2::1/64
PE3(config-router)#no shutdown
PE3(config-router)#exit
!
```

```
PE3(config-router)#ipv6 route 2001:DB8:2:3::/64 2001:DB8:2:2::2
PE3(config-router)#ipv6 route 2001:DB8:2:4::/64 2001:DB8:2:2::2
PE3(config-router)#ipv6 route 2001:DB8:2:5::/64 Tunnel0 2001:DB8:2:9::2
```

### *Configuring PE4*

```
PE4(config-)#ipv6 unicast-routing
PE4(config-)#ipv6 cef
PE4(config-router)#IP over IPv6 Tunnels
```

```
PE4(config-router)#interface Tunnel0
PE4(config-router)#no ipv6 address
PE4(config-router)#ipv6 address 2001:DB8:2:9::2/64
PE4(config-router)#tunnel source 2001:DB8:2:4::2
PE4(config-router)#tunnel mode ipv6
PE4(config-router)#tunnel destination 2001:DB8:2:2::1
exit
```

```
!
PE4(config-router)#interface FastEthernet0/0
PE4(config-router)#no ipv6 address
PE4(config-router)#ipv6 address 2001:DB8:2:5::1/64
PE4(config-router)#no shutdown
PE4(config-router)#exit
```

```
!
PE4(config-router)#interface FastEthernet0/1
PE4(config-router)#no ipv6 address
PE4(config-router)#ipv6 address 2001:DB8:2:4::2/64
PE4(config-router)#no shutdown
PE4(config-router)#exit
```

```
!!
PE4(config-router)#ipv6 route 2001:DB8:2:2::/64 2001:DB8:2:4::1
PE4(config-router)#ipv6 route 2001:DB8:2:3::/64 2001:DB8:2:4::1
```

```
ipv6 route 2001:DB8:2:1::/64 Tunnel0 2001:DB8:2:9::1
```

*Example: Configuring CE1*

```
!
```

```
ipv6 unicast-routing
```

```
ipv6 cef
```

```
!
```

```
interface FastEthernet0/0
```

```
no ipv6 address
```

```
ipv6 address 2001:DB8:2:1::1/64
```

```
no shutdown
```

```
exit
```

```
!
```

```
ipv6 route 2001:DB8:2:5::/64 2001:DB8:2:1::2
```

```
ipv6 route 2001:DB8:2:9::/64 2001:DB8:2:1::2
```

*CE2!*

```
ipv6 unicast-routing
```

```
ipv6 cef
```

```
!
```

```
interface FastEthernet0/0
```

```
no ipv6 address
```

```
ipv6 address 2001:DB8:2:5::2/64
```

```
no shutdown
```

```
exit
```

```
!
```

```
ipv6 route 2001:DB8:2:1::/64 2001:DB8:2:5::1
```

```
ipv6 route 2001:DB8:2:9::/64 2001:DB8:2:5::1
```

```
!
```

*Example: IPv6 over IPv6 Tunnel*

*Example: Configuring Core Device 2*

```
!
```

```
ipv6 unicast-routing
```

```
ipv6 cef
!  
interface FastEthernet1/0  
no ip address  
ipv6 address 2001:DB8:2:4::1/64  
no shutdown  
exit  
!  
interface FastEthernet0/0  
no ip address  
ipv6 address 2001:DB8:2:3::2/64  
no shutdown  
exit  
!  
ipv6 route 2001:DB8:2:2::/64 2001:DB8:2:3::1
```