Sudan University of Science and Technology
College of Engineering
Electronics Engineering Department

Implementation of IPv6 VPN Provider Edge Router

A Research Submitted In Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

Prepared By:

1. **AyaAbdallah Mohammed**
2. **LinaAbdallahAbdalrouf**
3. **Mohammed Omer Zainalabdin**
4. **RawaNaseraldinNoraldaem**

Supervised By:

Dr. Sami Hassan Omer Salih

October 2016

آيـــــة

قال تعالي:

{وَقَالَ الَّذِينَ أُوتُوا الْعِلْمَ وَيْلَكُمْ ثَوَابُ اللَّهِ خَيْرٌ لِمَنْ آمَنَ وَعَمِلَ صَالِحًا وَلَا يُلَقَّاهَا إِلَّا الصَّابِرُونَ}

{القصص الايه 40}

Dedication

This project is lovingly dedicated to our respective parents and teachers who have been our constant source of inspiration.

They have given us the drive and discipline to tackle any task with enthusiasm and determination, without their support this project would not have been made possible.

ACKNOWLEDGMENT

Firstly, everything happens with the grace of God, so we thank the almighty God for providing us an opportunity, strength and ambience to successfully accomplish this project.

Our sincere thanks are due to our supervisor Dr. Sami Hassan Omer Salih, we thank him for his continuous guidance and scientific insight during this project.

Independently on the nature of their contribution (intellectual or/and emotional), many people have pushed toward the completion of this work. To all them we are deeply and sincerely indebted.

We are extremely graceful to the celebrated authors whose research works have been freely consultant and referred in our project.

Finally, we would like to thanks all people who support our project, foremost have been our families who encouraged us to work hard and to continuous this work and colleagues for their kindness and support.

ABSTRACT

As the IPv6 has been deployed in the Internet core networks and many content providers provide service using the new protocol, various Internet Service Providers (ISPs) are lifted behind due to the high cost of migration especially for MPLS core. Therefore, the Internet Engineering Task force provides a solution to be utilized during the transition period which is 6PE. This method treats IPv6 as a label in MPLS routing and can achieve rapid deployment without any change in the core network. However the pooling of all traffic in one broadcast domain raises major security concerns to the end customers. Hence, the development of separate VPNs for each end users in 6PE was proposed in the new RFC which known as 6VPE.

In this research the 6VPE is studied and it have been evaluated in terms of performance and the level of traffic secrecy.

المستخلص

كما تم نشر بروتوكول الانترنت الاصدار السادس في الشبكة الاساسية للانترنت و توفر العديد من مقدمي المحتوي يوفرون الخدمة باستخدام بروتوكول جديد, و رفع مختلف مقدمي خدمات الانترنت وراء ذلك بسبب التكلفة العالية للهجرة خاصة لتسمية بروتوكولات الانترنت للتبديل الاساسية. و لذلك, فان فرقة عمل هندسة الانترنت توفر حل لاستخدامها خلال الفترة الأنتقالية التي هي أصدار بروتوكول الأنترنت الأصدار السادس لمزود الحافة. هذه الطريقة تعامل الانترنت بروتوكول الاصدار السادس كتسمية في تسمية بروتوكول تبديل التوجيه و يمكن تحقيق الانتشار السريع دون أي تغيير في الشبكة الاساسية و مع ذلك التجميع لكل حركة المرور في مجال بث واحد يثير مخاوف أمنية كبيرة للعملاء النهائيين. و بالتالي اقترحت تطوير شبكة خاصة افتراضية منفصلة لكل المستخدمين النهائيين في بروتوكول الانترنت الاصدار السادس مزود الحافة في استدعاء دالة النائية الجديدة المعروف باسم بروتوكول الانترنت الاصدار السادس للشبكة الافتراضية الخاصة لموفر الحافة.

في هذا البحث تم دراسة بروتوكول الانترنت الاصدار السادس للشبكة الافتراضية الخاصة لموفر الحافة وتم تقييمها من حيث الاداء و مستويات سرية المرور.

TABLE OF CONTENTS

List of Figures

List of Abbreviations

Internet Protocol	(IP)
Internet Engineering Task Force	(IETF)
Multiprotocol Label Switching	(MPLS)
IPv6 Provider Edge Router	(6PE)
Border Gateway Protocol	(BGP)
Provider Router	(P)
Intermediate System to Intermediate System	(IS_IS)
Label Distribution Protocol	(LDP)
Interior Gateway Protocol	(IGP)
Label switch path	(LSP)
Network Address Translation	(NAT)
NAT Traversal	(NAT-T)
Internet Engineering Task Force	(IETF)
Authentication Headers	(AH)
Encapsulating Security Payloads	(ESP)
Security Associations	(SA)
Internet Key Exchange	(IKE)
Kerberized Internet Negotiation of Keys	(KINK)
Dynamic Name system	(DNS)
Graphical Network Simulator	(GNS3)
Open Short Path First	(OSPF)
IP version 6	(IPv6)
IP version 4	(IPv4)
Virtual Private Network	(VPN)
Service Provider	(SP)
Internet Services Provider	(ISP)

Wide Area Network	(WAN)
Internet Protocol Security	(IPsec)
Customer Edge	(CE)
Provider Edge	(PE)
VPN Routing and Forwarding Tables	(VRF'S)
Route Distinguisher	(RD)
Route Target	(RT)
IPV6 VPN provider edge router	(6VPE)
Interior Border Gateway Protocol	(IBGP)
Transport Layer Security	(TLS)
Secure Shell	(SSH)
Forwarding Equivalence Classes	(FECs)
Routing Information Protocol	(RIP)
Label Egress Router	(LER)
Traffic Engineering	(TE)
The Internet Security Association and Key Management Protocol	(ISAKMP)
Multiprotocol Extended Border Gateway Protocol	(MP-EBGP)

CHAPTER ONE

INTORDUCTION

1. Introduction

1.1. Preface

The Internet continues to grow day by day, huge increase in number of the Internet users and new applications are emerged.So the current version of the Internet Protocol (IPv4) is slowly losing position because it is unable to satisfy the potential to the Internet growth.

The Internet Engineering Task Force (IETF) has come up with a new version of the protocol that defines the next generation IP protocol which is IPv6 (IP next generation). IPv6 provides large number of addresses will meet the growth of internet without any limitation. But due to the huge number of systems on the Internet, the transition from IPv4 to IPv6 can't be instantaneously. The transition must be smooth enough to prevent any instability in current online services especially for ISP who uses Multiprotocol Label Switching (MPLS) is there core networks[1].

A variety of deployment strategies are available for transition to IPv6. All of them are tolerating some drawbacks. This research will concentrate on two IETF RFCs 6PE and 6VPE. The former is and implementation of an automatic tunnel in MPLS core with any costly upgrades, while the latter increase the secrecy for IPv6 packet in the MPLS core by setup separate VPN for each customer [2].

However further evaluation of the performance and the security level is needed to convince customers to utilize the services during the transition period.

1.2. Problem statement

The security issues in 6PE lead to the development of 6VPE with arguing that it's provide more secrecy to the IPv6 traffic in MPLS core.

However, this method is yet to be evaluated in terms of performance and the level of secrecy.

1.3. Proposed solution

A test-bed is to be implemented to evaluate various scenarios when 6PE and 6VPE are compared.

1.4. Methodology

Prototyping methodology is used in this research to emulate the behaviours of MPLS core. The 6VPE is deployed and evaluated according to predefined KPIs.

1.5. Aims and Objectives

The methodology used to meet this research aims including these steps:

i. Gathering enough information about the environment that helps to achieve the goal.
ii. Use a GNS3 simulation programme to implement the following scenario:
    - Two routers act as provider router (P) in IPV4 core.
    - Two routers act as dual stack routers (Provider Edge (PE).
    - Four routers act as Customer Edge router (CE).
iii. Setup the IPsec, and
iv. Testing the performance of network.

1.6. Research Outlines

After this introductory chapter, Chapter Two will provide the MPLS background and an overview of IPv6. Chapter Three and Chapter Four will discuss the VPN concept when used in MPLS. The former highlight

the 6VPE operation and parameters, while the later explain the emulation test-bed features and present the results with discussion. FinallyChapter Five down the research conclusion and recommendation for future work.

CHAPTER TWO

BACKGROUND AND LITRATURE REVIEW

2. Background and Literature Review

2.1.Background

A packet of a connectionless network layer protocol travels fromone router to the next; each router makes an independent forwarding decision for that packet. That is each router analyzes the packet's header, and each router runs a network layer routing algorithm. Each router independently chooses a next hop for the packet, based on its analysis of the packet's header and the results of running the routing algorithm Choosing the next hop can there for be thought of as the composition of two functions. The first function partitions the entire set of possible packets into a set of "Forwarding Equivalence Classes (FECs)". The second maps each FEC to a next hop. All packets which belong to a particular FEC and which travel from a particular node will follow the same path (or if certain kinds of multi-path routing are in use, they will all follow one of a set of paths associated with the FEC)[3].

In conventional IP forwarding, a particular router will typically consider two packets to be in the same FEC if there is some address prefix X in that router's routing tables such that X is the "longest match" for each packet's destination address. As the packet traverses the network, each hop in turn reexamines the packet and assigns it to a FEC [4].

2.1.1. Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) was originally presented as a way of improving the forwarding speed of routers but is now emerging as a crucial standard technology that offers new capabilities for large scale IP networks. Traffic engineering, the ability of network operators to dictate the path that traffic takes through their network, and Virtual

Private Network support are examples of two key applications where MPLS is superior to any currently available IP technology [5].

MPLS is a packet labeling and forwarding technology that is highly scalable and widely used by the service providers and enterprises in their existing IPv4 backbones In MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. The FEC to which the packet is assigned is encoded as a short fixed length value known as a "label". When a packet is forwarded to its next hop, the labels sent along with it; that is, the packets are "labeled" before they are forwarded [5].

In the MPLS forwarding paradigm, once a packet is assigned to a FEC, no further header analysis is done by subsequent routers; all forwarding is driven by the labels In MPLS terminology, the packet handling nodes or routers are called Label Switched Routers (LSRs). The derivation of the term should be obvious; MPLS routers forward packets by making switching decisions based on the MPLS label. This illustrates another of the key concepts in MPLS. Conventional IP routers contain routing tables which are looked up using the IP header from a packet to decide how to forward that packet. These tables are built by IP routing protocols (e.g., RIP or OSPF) which carry around IP reach ability information in the form of IP addresses. In practice, we find that forwarding (IP header lookup) and control planes (generation of the routing tables) are tightly coupled [5].

Since MPLS forwarding is based on labels it is possible to cleanly separate the (label-based) forwarding plane from the routing protocol control plane. By separating the two, each can be modified

independently. With such a separation, we don't need to change the forwarding machinery, for example, to migrate a new routing strategy into the network [5].

MPLS forwards packets based on the Forwarding Information Base (FIB) and Label Forwarding Information Base (LFIB) tables. FIB and LFIB have all necessary label information as well as the outgoing interface and next-hop information [3].

FIB:router uses CEF to create this table. In most cases, the ingress router uses this table for incoming unlabeled packets. The router matches the destination IP address to the best prefix network it has in the FIB. It then injects a label and forwards that packet [3].

LFIB: Used by the core MPLS routers (which are not ingress and egress MPLS routers). They compare the label in the incoming packet with the label they have in their LFIB. If a match is found, the routers forward that packet based on that match. If not, the packet will be dropped. The LFIB is created by the LIB and FIB tables [3].

All routers in MPLS domain have both FIB and LFIB tables but only edge routers use FIB (ingress router uses FIB, egress router uses LFIB and FIB)[3].

LIB (Label Information Base) table holds all the labels known to the LSR and associated information that could possibly be used to forward packets. However, each LSR must choose the best label to use so FIB and LFIB contain only labels of best paths. To choose the best label, LSRs rely on the routing protocol’s decision about the best route [3].

2.1.2. Basic Concepts of MPLS:

2.1.2.1. Forwarding Equivalent class

As a forwarding technology based on classification, MPLS groups packets to be forwarded in the same manner into a class called the forwarding equivalence class (FEC). That is, packets of the same FEC are handled in the same way.

The classification of FECs is very flexible. It can be based on any combination of source address, destination address, source port, destination port, protocol type and VPN. In the traditional IP forwarding using longest match, all packets to the same destination belongs to the same FEC [2].

2.1.2.2. Label

A label is a short fixed length identifier for identifying a FEC. A FEC may correspond to multiple labels in scenarios where, for example, load sharing is required, while a label can only represent a single FEC [6].

A label is carried in the header of a packet. It does not contain any topology information and is local significant. A label is four octets, or 32 bits, in length. Figure (2-1)illustrates its format [2].

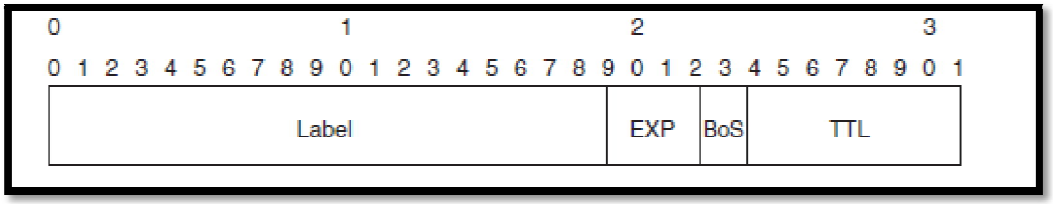

Figure (2- 1): Format of label

A label consists of four fields:

- Label: Label value of 20 bits. Used as the pointer for forwarding.
- EXP: For QoS, three bits in length.
- S: Flag for indicating whether the label is at the bottom of the label stack, one bit in length. 1 indicates that the label is at the bottom of the label stack. This field is very useful when there are multiple levels of MPLS labels.
- TTL: Time to live (TTL) for the label. Eight bits in length. This field has the same meaning as that for an IP packet.

2.1.2.3. Label Switching Router

Label switching router (LSR) is a fundamental component on an MPLS network. All LSRs support MPLS [2].

2.1.2.4. Label Switched Path

Label switched path (LSP) means the path along which a FEC travels through an MPLS network. Along an LSP, two neighboring LSRs are called upstream LSR and downstream LSR respectively in Figure (2-2),R2 is the downstream LSR of R1, while R1 is the upstream LSR of R2 [2].

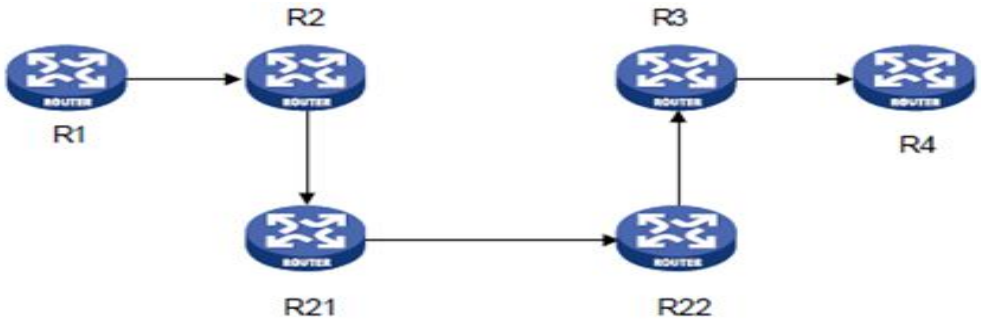

Figure (2- 2): Label switch path

2.1.2.5. Label Distribution Protocol

Label Distribution Protocol (LDP) means the protocol used by MPLS for control. An LDP has the same functions as a signaling protocol on a traditional network. It classifies FECs, distributes labels and establishes and maintains LSPs [2].

2.1.3. IPv6

IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol most Internet services use today. Every computer, mobile phone and any other device connected to the Internet needs a numerical IP address in order to communicate with other devices. The original IP address scheme, called IPv4, is running out of numbers [6].

IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4). The changes from IPv4 to IPv6 fall primarily into the following categories:

- Expanded Addressing Capabilities: IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "any cast address" is defined, used to send a packet to any one of a group of nodes [7].
- Header Format Simplification: Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing

cost of packet handling and to limit the bandwidth cost of the IPv6 header [7].

- Improved Support for Extensions and Options Changes: In the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future [7].
- Flow Labeling Capability: A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service [7].
- Authentication and Privacy Capabilities Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6 [7].

The service providers and enterprises using MPLS networks may view the integration of IPv6 services over an MPLS infrastructure as a normal evolution. The MPLS backbone provides the capability to connect islands of IPv6 with each other, either by using the existing IPv4 MPLS backbone or by partially or fully upgrading the MPLS backbones high and requires upgrading the network; transition mechanisms have been developed [2].

2.1.4. 6PE

6PE is a technology that allows IPv6 customers to communicate with each other over an IPv4 MPLS Provider without any tunnel setup, by having the customer IPv6 prefixes using a IPv4-mapped IPv6 address as next-hop inside the Provider's network and using IPv4 LSPs between the 6PEs[8].

The generic definition of a 6PE is a dual-stack IPv4 and IPv6-enabled router, with at least an IPv4 legitimate and routed address in the MPLS cloud and identified as a Forwarding Equivalence Class (FEC) with a correspondingly allocated and distributed label binding to the rest of the network.6PE is typically deployed by ISPs that have MPLS core network and (possible) supports MPLS VPN (or other) services [2].

6PE uses two labels:

- The top label is the transport label, which is assigned hop−by−hop by the Label Distribution Protocol (LDP) or by MPLS traffic engineering (TE).
- The bottom label is the label assigned by the Border Gateway Protocol (BGP) and advertised by the internal BGP (iBGP) between the Provider Edge (PE) routers.

When the 6PE was released, a main requirement was that none of the MPLS core routers (the P routers) had to be IPv6−aware. That requirement drove the need for two labels in the data plane [9].

But in the other hand 6PE has main disadvantage that customers in the network suffer from it, the disadvantage is that 6PE is like having one large single routing table. There is no differentiation of customer traffic across the core. Customers are not separated from each other as with Layer 3 MPLS-based VPNs. 6PE is more like having a big MPLS Internet service with global IPv6 routes. This technique can be used for commodity IPv6 Internet connectivity for customers. If you are using an MPLS service for Internet connectivity, you need to protect your perimeter accordingly. If you are using a 6PE service for site-to-site

connectivity, you should be filtering traffic going between sites and filtering the routes being advertised and received from the service provider. You might also want to consider using encryption between your sites as an extra measure of security [10].

The security implication of using 6PE services is that there is no inherent security built into the service [10].

2.2.Literature Review

In RFC3031 authors introduce some of the basic concepts of MPLS and describe the general approach to be used, which merges layer 2 and layer 3 protocol that uses label switching in the core network, thus reduces the workout of looking the routing table overhead. MPLS uses label which is a short, fixed length, locally significant identifier which is used to identify a FEC. The label which is put on a particular packet represents the Forwarding Equivalence Class to which that packet is assigned [11].

In RFC 3272 the author made a comparative analysis of MPLS and Non-MPLS networks and shows MPLS networks have a better performance over traditional IP networks [12].

In RFC4798 authors explained how to interconnect IPv6 islands over a Multiprotocol Label Switching (MPLS)-enabled IPv4 cloud. This approach relies on IPv6 Provider Edge routers (6PE), which are Dual Stack in order to connect to IPv6 islands and to the MPLS core, which is only required to run IPv4 MPLS. The 6PE routers exchange the IPv6 reachability information transparently over the core using the Multiprotocol Border Gateway Protocol (MP-BGP) over IPv4. In doing so, the BGP Next Hop field is used to convey the IPv4 address of the 6PE router so that dynamically established IPv4-signaled MPLS

LabelSwitched Paths (LSPs) can be used without explicit tunnel Configuration network (VPRN). The configuration and operations of the 6PE approach is somewhat simpler, since it does not involve all the VPN concepts such as Virtual Routing and Forwarding (VRFs) tables [13].
RFC4027 explain that a VRF is a per-site forwarding table. Every site to which the PE router is attached is associated with one of these tables. A particular packet's IP destination address is looked up in a particular VRF only if that packet has arrived directly from a site that is associated with that table [14].

In RFC4659 describe a method by which a Service Provider may use its packet-switched backbone to provide Virtual Private Network (VPN) services for its IPv6 customers. This method reuses, and extends where necessary, the "BGP/MPLS IP VPN" method for support of IPv6. In BGP/MPLS IP VPN, "Multiprotocol BGP" is used for distributing IPv4 VPN routes over the service provider backbone, and MPLS is used to forward IPv4 VPN packets over the backbone. Also defines an IPv6 VPN address family and describes the corresponding IPv6 VPN route distribution in "Multiprotocol BGP". PEs use "VPN Routing and Forwarding tables"(VRFs) to maintain the reachability information and forwarding information of each IPv6 VPN separately [15].

2.3.Research question

How to implement the 6VPE approach over MPLS network to provide IPV6 VPN services to customers of the network?

CHAPTER THREE

METHODOLOY

3. METHODOLOGY

3.1. Virtual Private Network (VPN):

VPN (Virtual Private Network) is a private network over the public service provider network. Customer can use this technology provided by SP (Service Provider) to connect different sites of the company and business partner around the world together seamlessly and securely, to end users the whole communication process is transparent [16].

3.1.1. Types of VPN

- Remote access VPNs**:** enables mobile users to establish a connection to an organization server by using the infrastructure provided by an ISP (Internet Services Provider) [16].
- Intranet VPNs: provides virtual circuits between organization offices over the Internet ،An IP WAN infrastructure uses IPsec to create secure traffic tunnels across the network [16].
- Extranet VPNs: are the same as intranet VPN. The only difference is the users. Extranet VPN are built for users such as customers, suppliers, or different organizations over the Internet [16].

3.1.2. Customer Edge and Provider Edge

Routers can be attached to each other, or to end systems, in a variety of different ways. We will use the term "attachment circuit" to refer generally to some such means of attaching to a router. An attachment circuit may be the sort of connection that is usually thought of as a "data

link", or it may be a tunnel of some sort; what matters is that it be possible for two devices to be network layer peers over the attachment circuit [17].

Each VPN site must contain one or more Customer Edge (CE) devices. Each CE device is attached, via some sort of attachment circuit, to one or more Provider Edge (PE) routers [17].

Routers in the SP's network that do not attach to CE devices are known as "P routers". CE devices can be hosts or routers. In a typical case, a site contains one or more routers, some of which are attached to PE routers. The site routers that attach to the PE routers would then be the CE devices or "CE routers". CE devices are logically part of a customer's VPN. PE and P routers are logically part of the SP's network [17].

3.1.3. VPN Routing and Forwarding Tables(VRF'S):

Each PE router maintains a number of separate forwarding tables. One of the forwarding tables is the "default forwarding table". The others are "VPN Routing and Forwarding tables", or "VRFs"[17].

Every PE/CE attachment circuit is associated, by configuration, with one or more VRFs. In the simplest case and most typical case, a PE/CE attachment circuit is associated with exactly one VRF. When an IP packet is received over a particular attachment circuit, its destination IP address is looked up in the associated VRF. The result of that lookup determines how to route the packet. If an IP packet arrives over an attachment circuit that is not associated with any VRF, the packet's destination address is looked up in the default forwarding table, and the packet is routed accordingly. Packets forwarded according to the default

forwarding table include packets from neighbouring P or PE routers, as well as packets from customer-facing attachment circuits that have not been associated with VRFs [17].

3.1.4. The VPN-IPv4 Address Family:

The BGP Multiprotocol Extensions [BGP-MP] allow BGP to carry routes from multiple "address families". We introduce the notion of the "VPN-IPv4 address family". A VPN-IPv4 address is a 12-byte quantity, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. If several VPNs use the same IPv4 address prefix, the PEs translate these into unique VPN-IPv4 address prefixes. This ensures that if the same address is used in several different VPNs, it is possible for BGP to carry several completely different routes to that address, one for each VPN. Since VPN-IPv4 addresses and IPv4 addresses are different address families, BGP never treats them as comparable addresses [17].

An RD is simply a number, and it does not contain any inherent information; it does not identify the origin of the route or the set of VPNs to which the route is to be distributed. The purpose of the RD is solely to allow one to create distinct routes to a common IPv4 address prefix.

The RDs are structured so that every Service Provider can administer its own "numbering space" (i.e., can make its own assignments of RDs), without conflicting with the RD assignments made by any other Service Provider [17].

3.1.5. Controlling Route Distribution:

If a PE router is attached to a particular VPN (by being attached to a particular CE in that VPN), it learns some of that VPN's IP routes from the attached CE router. Routes learned from a CE routing peer over a particular attachment circuit may be installed in the VRF associated with that attachment circuit. Exactly which routes are installed in this manner is determined by the way in which the PE learns routes from the CE [17].

In particular, when the PE and CE are routing protocol peers, this is determined by the decision process of the routing protocol; these routes are then converted to VPN-IP4 routes, and "exported" to BGP. If there is more than one route to a particular VPN-IP4 address prefix, BGP chooses the "best" one, using the BGP decision process. That route is then distributed by BGP to the set of other PEs that needs to know about it. At these other PEs, BGP will again choose the best route for a particular VPN-IP4 address prefix. Then the chosen VPN-IP4 routes are converted back into IP routes, and "imported" into one or more VRFs. Whether they are actually installed in the VRFs depends on the decision process of the routing method used between the PE and those CEs that are associated with the VRF in question. Finally, any route installed in a VRF may be distributed to the associated CE routers [17].

3.1.6. The Route Target Attribute:

Every VRF is associated with one or more Route Target (RT) attributes. When a VPN-IPv4 route is created (from an IPv4 route

that the PE has learned from a CE) by a PE router, it is associated with one or more Route Target attributes. These are carried in BGP as attributes of the route [17].

Any route associated with Route Target (RT) must be distributed to every PE router that has a VRF associated with Route Target T. When such a route is received by a PE router, it is eligible to be installed in those of the PE's VRFs that are associated with Route Target (RT) [17].

3.2.6VPE:

Cisco System's 6VPE solution smoothly introduces IPv6 VPN service in a scalable way, without any IPv6 addressing restrictions. It does not jeopardize a well-controlled service provider IPv4 backbone or any customer networks. VPN service backbone stability is a key issue for those service providers who have recently stabilized their IPv4 infrastructure. For IPv4 VPN customers, IPv6 VPN service is exactly the same as MPLS VPN for IPv4 [18].

The IPv6 MPLS VPN service model is similar to that of IPv4 MPLS VPNs. Service providers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the PE router and dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A PE-CE link can be an IPv4 link, an

IPv6 link, or a combination of an IPv4 and IPv6 link, as shown in Figure(3-1):

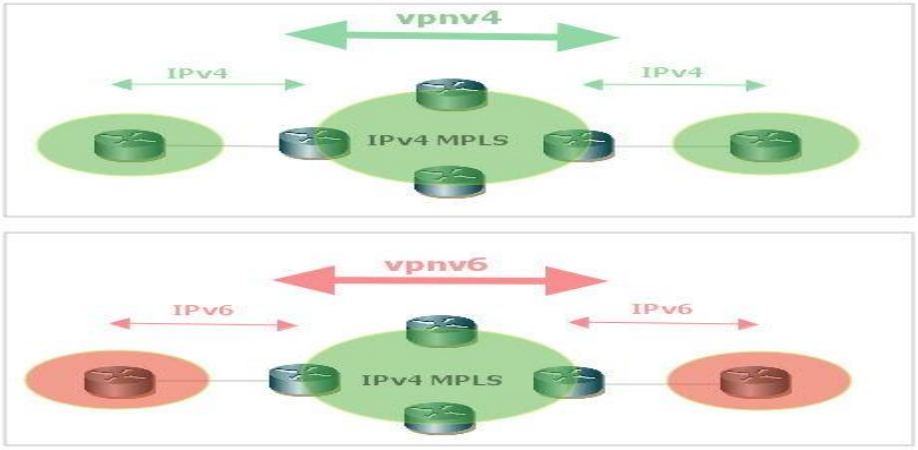

Figure (3- 1): Combination of an IPv4 and IPv6 link

IPv6 VPN service is exactly the same as MPLS VPN for IPv4. 6VPE offers the same architectural features as MPLS VPN for IPv4. It offers IPv6 VPN and uses the same components, such as:

- Multiprotocol BGP (MP-BGP) VPN addresses family.
- Route distinguishers
- VPN Routing and Forwarding (VRF) instances
- Extended community
- MP-BGP

The 6VPE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, and

switches IPv4 and IPv6 traffic using the respective fast switching CEF or distributed CEF path over the native IPv4 and IPv6 VRF interfaces (It provides logically separate routing table entries for VPN member devices). The 6VPE router exchanges reachability information with the other 6VPE routers in the MPLS domain using Multiprotocol BGP, and shares a common IPv4 routing protocol (such as OSPF or IS-IS) with the other P and PE devices in the domain. Separate routing tables are maintained for the IPv4 and IPv6 stacks. A hierarchy of MPLS labels is imposed on an incoming customer IPv6 packet at the edge LSR:

- Outer label (IGP Label) for iBGP next-hop, distributed by LDP.

- Inner label (VPN Label) for the IPv6 prefix, distributed by MP-BGP.

Incoming customer IPv6 packets at the 6VPE VRF interface are transparently forwarded inside the service provider's IPv4 core, based on MPLS labels. This eliminates the need to tunnel IPv6 packets. P routers inside the MPLS core are unaware that they are switching IPv6 labeled packets [18].

6VPE is a technology that allows IPv6 VPN customers to communicate with each other over an IPv4 MPLS Provider without any tunnel setup, by having the customer VPNv6 prefixes using a v4-mapped IPv6 address as next-hop inside the provider's network and using IPv4 LSPs between the 6VPEs[18].

In 6VPE, labels must be exchanged between the 6VPEs for their VPNv6 prefixes, which means that the VPNv6 address-family must be activated on the IPv4 iBGP session between the 6VPEs.

6VPE allows you to offer IPv6 within VRFs, and is configured in the vpnv6 address family. It's logically the same as vpnv4, except that IPv6 addresses are exchanged between vpnv6 peers, not IPv4 addresses. Send-label is needed for 6PE, as that's how the PE routers coordinate their label assignments. Send-community extended is needed for 6vPE, as that's how the PE routers coordinate their RD/VRF/RT assignments. 6VPE enables to carry IPv6 global routes over an MPLS cloud, using vpnv6 BGP address family between the PEs [19].

Also there are various approaches to control the security of a core if the VPN customer cannot or does not want to trust the service provider. IPsec from customer-controlled devices is one of them.

3.3. IPsec (Internet Protocol security)

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic

security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection [20].

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Transport Layer (TLS) and the Application layer (SSH). Hence, only IPsec protects all application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer [20].

3.3.1. Operation modes:

IPsec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

- Transport mode:

  In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be modified by network address translation, as this always invalidates the hash value. The transport and application layers are always secured by a hash, so they cannot be modified in any way, for example by translating the port numbers [20].

A means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

- Tunnel mode :

  In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).

  Tunnel mode supports NAT traversal [20].

IPsec is officially standardized by the Internet Engineering Task Force (IETF) in a series of Request for Comments documents addressing various components and extensions. It specifies the spelling of the protocol name to be IPsec [20].

3.3.2. Security architecture:

The IPsec suite is an open standard. IPsec uses the following protocols to perform various functions:

- **Authentication Headers (AH)**

  Provide connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks [20].

- **Encapsulating Security Payloads (ESP):**

Provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality [20].

- **Security Associations (SA):**

Provide the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations [20].

- **The Internet Security Association and Key Management Protocol (ISAKMP**):

Provides a framework for authentication and key exchange,[with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records[20].

ISAKMP is the negotiation protocol that allows two hosts to agree on how to build an IPsec security association. ISAKMP negotiation consists of two phases: Phase 1 and Phase 2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. IPSec then comes into play to encrypt the data using encryption algorithms and provides authentication, encryption and anti-replay services.

CHAPTER FOUR

IMPLEMNTATION AND RESULT

4. Implementation And Result

4.1.System tool:

A lot of tools were used to complete the design but the most importance tool is GNS3.

4.1.1. Graphical Network Simulator (GNS3):

GNS3 is software use for simulating different virtual devices and real devices like routers, switches etc. Gns3 uses real IOS software to simulate the different virtual devices. GNS3 is an excellent complementary tool to real labs for network engineers, administrators and people wanting to study for certifications such as Cisco CCNA, CCNP and CCIE.

4.1.2. Some Supported GNS3 Features:

- Design of high quality and complex network topologies.
- Emulation of many Cisco router platforms and PIX firewalls.
- Simulation of simple Ethernet, ATM and Frame Relay switches.
- Connection of the simulated network to the real world.
- Packet capture using Wireshark.

4.2.System implementation:

To design our network topology as showing in figure (4-1), we used Cisco (7200) series router and VPC (virtual PC) in GNS3 simulation. Cisco 7200 series router has features needed in our design such as support MPLS and IPv6.

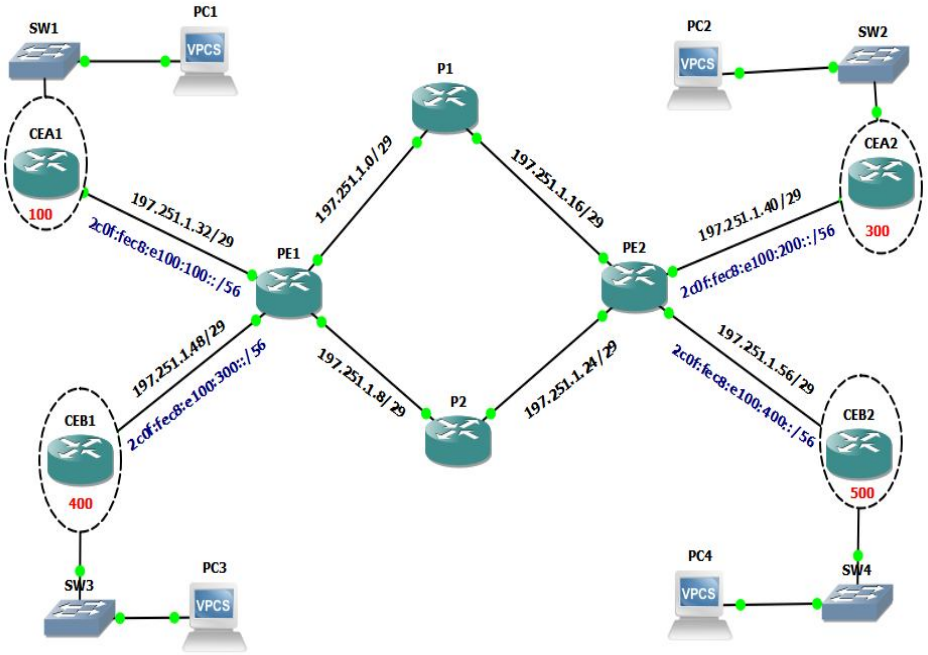

Figure (4- 1): Network Topology

4.3.Configuration:

4.3.1. Routing protocol:

After IP addresses are taken place in each router, OSPF (Open Short Path First) routing protocol was configured to connect the provider's core routers.

4.3.2. Configuring MPLS:

MPLS was configured in all P-P and P-PE links in the provider core network. Customer Edge (CE) routers do not run MPLS.

4.3.3. Configuring VRFs:

In provider edge (PE) routers, we created VRFs (virtual routing forwarding) and associated the VRFs with the customer interfaces.

To verify the configuration of VRFs:

```
PE1#sh vrf brief
  Name                             Default RD          Protocols   Interfaces
  CEA1                             200:1               ipv4,ipv6   Gi3/0
  CEB1                             200:2               ipv4,ipv6   Gi4/0
```

Figure (4- 2): VRFS table

4.3.4. MP-BGP on the PE Router:

We configured multiprotocol BGP (MP-BGP) only in PE routers to be able to advertise VRFs routes. Provider (P) routers run only OSPF routing protocol and MPLS to function as a transit router of the core network.

4.3.5. Configuring OSPF between PE-CE:

We configured OSPF (Open Short Path First) as routing protocol between CE and PE routers to advertise customer site's routes to PE routers.

4.3.6. Router distribution:

The last step to adversities customer site routes between customer sites is to redistribute OSPF processes into MP-BGP and vise-verse.

After we followed the pervious steps, end-to-end IPv4 connectivity between the CE routers within each VRF (vpnv4) is set up.

4.3.7. Configuring 6VPE:

To have end to end IPv6 connectivity between the CE routers within each VRF (VPNv6), we configured BGP between PE-CE routers.

```
PE1#SH bgp vpnv6 unicast all summary
BGP router identifier 41.67.0.5, local AS number 200
BGP table version is 13, main routing table version 13
8 network entries using 1344 bytes of memory
10 path entries using 800 bytes of memory
8/6 BGP path/bestpath attribute entries using 1056 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
6 BGP extended community entries using 208 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 3504 total bytes of memory
BGP activity 20/0 prefixes, 22/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
41.67.0.6       4          200     140     142       13    0    0 01:56:34        4
2C0F:FEC8:E100:100::2
                4          100     133     133       13    0    0 01:57:24        2
2C0F:FEC8:E100:300::2
                4          400     132     133       13    0    0 01:57:20        2
```

Figure (4- 3): VPNv6 verification

4.3.8. IPsec (Internet Protocol security):

To complete VPN we configured IPsec in CE routers.

IPSEC tunnel mode will be configured in CE routers to protect traffic of customer's site.

4.3.8.1. Configuring IPsec for IPv4 traffic:

To setup IPsec, ISAKMP needs to be configured. We can configure encryption method, hashing algorithm, diffie-hellman group and lifetime to be used in phase 1 but we prefer to use default configuration for them.

Configure IPsec **(**ISAKMP Phase 2):

To configure IPsec we need to setup the following in order:

- Create extended ACL, IPsec Transform and Crypto Map.

Then we applied crypto map to interface (interface which connect customer site to the core network).

4.3.8.2. Configuring IPsec for IPv6 traffic:

For IPv6, we don't need to setup ISAKMP phase1 again.

We assigned the key which is used in ISAKMP phase 2, Then Configuring IPv6 IPsec VTI on router. To make packets which come from customer site go through VTI (virtual tunnel internet), we used static routing.

4.4.Results and discussion:

This section shows the most relevant information that can use to verify the configuration is working properly.

4.4.1. Results for CEA1:

CEA1#Show ipv6 route

The same commands can be used to verify in CEB1, to show route for IPv4 and IPv6.

```
C   2012::/64 [0/0]
     via Tunnel0, directly connected
L   2012::1/128 [0/0]
     via Tunnel0, receive
C   2C0F:FEC8:E100:100::/56 [0/0]
     via GigabitEthernet1/0, directly connected
L   2C0F:FEC8:E100:100::2/128 [0/0]
     via GigabitEthernet1/0, receive
B   2C0F:FEC8:E100:200::/56 [20/0]
     via FE80::C801:12FF:FE50:54, GigabitEthernet1/0
C   2C0F:FEC8:E100:500::/56 [0/0]
     via GigabitEthernet2/0, directly connected
L   2C0F:FEC8:E100:500::1/128 [0/0]
     via GigabitEthernet2/0, receive
S   2C0F:FEC8:E100:600::/56 [1/0]
     via 2012::2
L   FF00::/8 [0/0]
```

Figure (4- 4): IPv6 route of router CEA1

Show crypto IPsec sa command to show IPsec security association built between CE-CE router:

```
CEA1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 2C0F:FEC8:E100:100::2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2C0F:FEC8:E100:200::2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

Figure (4- 5): IPsec of ipv6

Trace route from CE router to check which path it is used to reach their destination:

```
CEA1#traceroute 2c0f:fec8:e100:200::2

Type escape sequence to abort.
Tracing the route to 2C0F:FEC8:E100:200::2

  1 2C0F:FEC8:E100:100::1 172 msec 100 msec 188 msec
  2 ::FFFF:197.251.1.10 [MPLS: Labels 17/24 Exp 0] 732 msec 536 msec 652 msec
  3 2C0F:FEC8:E100:200::1 [AS 200] 744 msec 588 msec 608 msec
  4 2C0F:FEC8:E100:200::2 [AS 200] 768 msec 592 msec 816 msec
```

Figure (4- 6): Trace route from CE router

As showing CE router forwards packet to PE router and because of the fact that CE router doesn't have any awareness about what is happening in the core, so CE router can't see how packets forward between P routers. Also as showing PE router inject two labels before forwards packet to P routers, one of them is normal label which P router use to

forward packets and other one is VPN label which PE routers use in VPN process and P routers don't know anything about it.

4.4.2. Results of VPCs(virtual PC):

We used VPCS and assigned IPv4 and IPv6 addresses to them.

Testing end to end connectivity:

```
PC1> ping 197.251.1.74
84 bytes from 197.251.1.74 icmp_seq=1 ttl=62 time=828.048 ms
84 bytes from 197.251.1.74 icmp_seq=2 ttl=62 time=856.049 ms
84 bytes from 197.251.1.74 icmp_seq=3 ttl=62 time=841.048 ms
84 bytes from 197.251.1.74 icmp_seq=4 ttl=62 time=853.049 ms
84 bytes from 197.251.1.74 icmp_seq=5 ttl=62 time=778.044 ms
```

Figure (4- 7): Ping from pc1 to pc2

```
PC1> ping 2c0f:fec8:e100:600::2

2c0f:fec8:e100:600::2 icmp6_seq=1 ttl=60 time=917.052 ms
2c0f:fec8:e100:600::2 icmp6_seq=2 ttl=60 time=746.043 ms
2c0f:fec8:e100:600::2 icmp6_seq=3 ttl=60 time=761.043 ms
2c0f:fec8:e100:600::2 icmp6_seq=4 ttl=60 time=813.047 ms
2c0f:fec8:e100:600::2 icmp6_seq=5 ttl=60 time=819.047 ms
```

Figure (4- 8): Ping with ipv6 address from pc1 to pc2

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5. Conclusion and Recommendation

5.1. Conclusion

6VPE is used to provide VPN IPV6 service in IPv4 MPLS core. It is considered one of the best solution as it takes the advantages of operational MPLS IPV4 infrastructureand also provides many benefits to service provider :-

- IPv6 Transport with minimal operation cost and risk – While the service providers slowly move their infrastructure to support IPv6, they can use their existing IPv4 MPLS infrastructure to support IPv6.
- Address Space, Routing, and Traffic Separation BGP/MPLS allows distinct IP VPNs to use the same address space, which can also be private address space. This is achieved by adding a 64-bit Route Distinguisher (RD) to each IPv4 route, making VPN-unique addresses also unique in the MPLS core. Also by using VRF in PE routers, routing and traffic separation can be achieved.
- Hiding of the BGP/MPLS IP VPN Core Infrastructure MPLS does not reveal unnecessary information to the outside, not even to customer VPNs.
- IPSEC is used with 6VPE to provide Encryption in case that customer s don't trust service provide and MPLS does not imply any type of encryption so customer can encrypt their traffic using IPSEC in CE router.

5.2.Recommendation and future work

IPv6 Rapid Deployment (6rd) 6rd is a stateless tunneling mechanism which allows an Service Provider to rapidly deploy IPv6 in a lightweight and secure manner without requiring upgrades to existing IPv4 access network infrastructure. While there are a number of methods for carrying IPv6 over IPv4, 6rd has been particularly successful due to its stateless mode of operation which is lightweight and naturally scalable, resilient, and simple to provision. The service provided by 6rd is production quality, it "Looks smells and feels like native IPv6" to the customer and the Internet at large.

References

[1]Behrouz A. Forouzan, “DATACOMMUNICATIONS AND NETWORKING” , 2007.

[2] MPLS Basics – Cisco Support.Retrieved (October20, 2016), from https://supportforums.cisco.com/sites/default/files/mpls_basics_introduction.pdf.

[3] Rosen, Viswanathan, &Callon. (2001, January). RFC 3031 – Internet Engineering Task Force. Retrieved October 20, 2016, from https://tools.ietf.org/html/rfc3031

[4] Minoli D. (1991). *Telecommunications technology handbook*. Boston:Artech House.

[5] Cisco Active Network Abstraction Reference Guide, 3.7 ... (2014, April,29). Retrieved (October20,2016), from http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/anarefguide37/mpls.html.

[6][15]IPv6. (2011, September 23). Retrieved (October 20, 2016), from http://www.internetsociety.org/deploy360/ipv6/?gclid=cpa_gnye6c8cfqmw0wodawedtq.

[7] Deering, S. E. D. (1998, December). RFC 2460 - Internet Engineering Task Force. Retrieved October 20, 2016, from https://tools.ietf.org/html/rfc2460.

[8] Forum Topic: Best way to study for CCIE | NetworkLessons.com. Retrieved (October 20, 2016), from https://networklessons.com/topic/best-way-to-study-for-ccie/.

[9] Herrero G. (2013, April 2). 6PE model. Retrieved (October 20, 2016), from https://forums.juniper.net/t5/theroutingchurn/an-overview-of-the-6pe-model/ba-p/177313.

[10] Lawin. D. (2013, April 3). 6PE FAQ: Why Does 6PE Use Two MPLS Labels in the Data Plane? Retrieved (October 20, 2016), from http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/116061-qa-6pe-00.pdf

[11] Scott Hogg, & Eric Vyncke. (2009, January 4). IPv6 Internet Security for Your Network. Retrieved (October 20, 2016), from http://www.ciscopress.com/articles/article.asp?p=1312796&seqnum=4.

[12] A. Viswanathan , E. Rosen, & R. Callon, "Multiprotocol Label Switching Architecture ", January 2001.

[13] A. Chiu , A. Elwalid ,D. Awduche, I. Widjaja ,& X. Xiao ,"Overview and Principles of Internet Traffic Engineering" , May 2002.

[14] F. Le Faucheur, J. De Clercq,& S. Prevost ," February 2007" ,February 2007.

[15]Acreo AB , L. Andersson ,& T. Madsen , " Provider Provisioned Virtual Private Network (VPN) Terminology ",March 2005.

[16]Germaine Bacon, LizziBeduya, Jun Mitsuoka, & Betty Huang. (2012, November 19). Virtual Private Network. Retrieved October 20, 2016, from

[17] Deering, S. E. D. (1998, December). RFC 2460 - Internet Engineering Task Force. Retrieved October 20, 2016, from https://tools.ietf.org/html/rfc2460.

http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahukewifkrs9qunpahujicakhbwub7cqfggcmaa&url=http://www.csun.edu/~vcact00f/311/termprojects/700class/virtual%20private%20network.doc&usg=afqjcnhhdtr_wtyyn2eiaqmfqaeuiyaf7a&bvm=bv.136499718,d.bgs&cad=rja.[18]Ronsen &Rokhtar (2006, February). RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs). Retrieved October 20, 2016, from https://tools.ietf.org/html/rfc4364.

[18] IPv6 and 6VPE Support in MPLS VPN [Cisco IP Solution ... Retrieved (October 20, 2016), from http://www.cisco.com/en/us/products/sw/netmgtsw/ps4748/products_user_guide_chapter09186a0080935063.html.

[19] Cisco ASR 901 Series Aggregation Services Router Software ... Retrieved (October 20, 2016), from http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/configuration/guide/b_asr901-scg.html.

[20]Harkins& Carrel. (1998, November). IPsec - Wikipedia. Retrieved (October 20, 2016), from https://en.wikipedia.org/wiki/ipsec
RFC 2409.

Appendix:

Router CEA1 configuration:

```
hostname CEA1
!
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 6vpe address 197.251.1.42
crypto isakmp key 6vpe address ipv6 2C0F:FEC8:E100:200::2/56
crypto isakmp profile profile1
keyring default
!
crypto ipsec transform-set 6vpe esp-aesesp-sha-hmac
!
crypto ipsec profile profile1
set transform-set 6vpe
!
crypto map 6vpe 1 ipsec-isakmp
set peer 197.251.1.42
set transform-set 6vpe
match address 100
7!
interface Loopback0
ip address 41.67.0.1 255.255.255.255
```

```
!
interface Tunnel1
no ip address
ipv6 address 2012::1/64
ipv6 enable
tunnel source 2C0F:FEC8:E100:100::2
tunnel mode ipsec ipv6
tunnel destination 2C0F:FEC8:E100:200::2
tunnel protection ipsec profile profile1
!
interface FastEthernet0/0
!
interface GigabitEthernet1/0
ip address 197.251.1.34 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:100::2/56
crypto map 6vpe
!
interface GigabitEthernet2/0
ip address 197.251.1.65 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:500::1/56
!
router ospf 1
log-adjacency-changes
network 197.251.1.0 0.0.0.255 area 0
!
```

```
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 2C0F:FEC8:E100:100::1 remote-as 200
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family ipv6
network 2C0F:FEC8:E100:100::/56
network 2C0F:FEC8:E100:500::/56
neighbor 2C0F:FEC8:E100:100::1 activate
exit-address-family
!
access-list 100 permit ip host 197.251.1.66 host 197.251.1.74
access-list 101 permit ip any any
ipv6 route 2C0F:FEC8:E100:600::/56 2012::2
End
```

Router CEA2 configuration:

```
hostname CEA2
!
ipv6 unicast-routing
ipv6 cef
```

```
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 6vpe address 197.251.1.34
crypto isakmp key 6vpe address ipv6 2C0F:FEC8:E100:100::2/56
crypto isakmp profile profile1
keyring default
match identity address ipv6 2C0F:FEC8:E100:100::2/56
!
crypto ipsec transform-set 6vpe esp-aesesp-sha-hmac
!
crypto ipsec profile profile1
set transform-set 6vpe
!
crypto map 6vpe 1 ipsec-isakmp
set peer 197.251.1.34
set transform-set 6vpe
match address 100
!
interface Loopback0
ip address 41.67.0.2 255.255.255.255
!
interface Tunnel1
no ip address
ipv6 address 2012::2/64
ipv6 enable
tunnel source 2C0F:FEC8:E100:200::2
```

```
tunnel mode ipsec ipv6
tunnel destination 2C0F:FEC8:E100:100::2
tunnel protection ipsec profile profile1
!
interface GigabitEthernet1/0
ip address 197.251.1.42 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:200::2/56
crypto map 6vpe
!
interface GigabitEthernet2/0
ip address 197.251.1.73 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:600::1/56
!
router ospf 1
log-adjacency-changes
network 197.251.1.0 0.0.0.255 area 0
!
router bgp 300
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 2C0F:FEC8:E100:200::1 remote-as 200
!
address-family ipv4
no synchronization
no auto-summary
```

```
exit-address-family
!
address-family ipv6
network 2C0F:FEC8:E100:200::/56
network 2C0F:FEC8:E100:600::/56
neighbor 2C0F:FEC8:E100:200::1 activate
exit-address-family
!
access-list 100 permit ip host 197.251.1.74 host 197.251.1.66
access-list 101 permit ip any any
ipv6 route 2C0F:FEC8:E100:500::/56 2012::1
!
End
```

Router CEB1 configuration:

```
hostname CEB1
!
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 6vpe address 197.251.1.58
!
!
crypto ipsec transform-set 6vpe esp-aesesp-sha-hmac
```

```
!
crypto map 6vpe 1 ipsec-isakmp
set peer 197.251.1.58
set transform-set 6vpe
match address 100
!
interface Loopback0
ip address 41.67.0.3 255.255.255.255
!
interface GigabitEthernet1/0
ip address 197.251.1.50 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:300::2/56
crypto map 6vpe
!
!
interface GigabitEthernet2/0
ip address 197.251.1.81 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:700::1/56
!
router ospf 1
log-adjacency-changes
network 197.251.1.0 0.0.0.255 area 0
!
router bgp 400
no bgp default ipv4-unicast
```

```
bgp log-neighbor-changes
neighbor 2C0F:FEC8:E100:300::1 remote-as 200
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family ipv6
network 2C0F:FEC8:E100:300::/56
network 2C0F:FEC8:E100:700::/56
neighbor 2C0F:FEC8:E100:300::1 activate
exit-address-family
!
ip forward-protocol nd
!
access-list 100 permit ip host 197.251.1.82 host 197.251.1.90
access-list 101 permit ip any any
!
control-plane
!
End
```

Router CEB2 configuration:

```
hostname CEB2
!
```

```
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 6vpe address 197.251.1.50
crypto isakmp key 6vpe address ipv6 2C0F:FEC8:E100:300::2/56
crypto isakmp profile profile1
keyring default
match identity address ipv6 2C0F:FEC8:E100:300::2/56
!
crypto ipsec transform-set 6vpe esp-aesesp-sha-hmac
!
crypto ipsec profile profile1
set transform-set 6vpe
!
crypto map 6vpe 1 ipsec-isakmp
set peer 197.251.1.50
set transform-set 6vpe
match address 100
!
interface Loopback0
ip address 41.67.0.4 255.255.255.255
!
interface Tunnel1
no ip address
ipv6 address 2012::2/64
```

```
ipv6 enable
tunnel source 2C0F:FEC8:E100:400::2
tunnel mode ipsec ipv6
tunnel destination 2C0F:FEC8:E100:300::2
tunnel protection ipsec profile profile1
!
interface GigabitEthernet1/0
ip address 197.251.1.58 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:400::2/56
crypto map 6vpe
!
interface GigabitEthernet2/0
ip address 197.251.1.89 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:800::1/56
!
router ospf 1
log-adjacency-changes
network 197.251.1.0 0.0.0.255 area 0
!
router bgp 500
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 2C0F:FEC8:E100:400::1 remote-as 200
!
address-family ipv4
```

```
no synchronization
no auto-summary
exit-address-family
!
address-family ipv6
network 2C0F:FEC8:E100:400::/56
network 2C0F:FEC8:E100:800::/56
neighbor 2C0F:FEC8:E100:400::1 activate
exit-address-family
access-list 100 permit ip host 197.251.1.90 host 197.251.1.82
access-list 101 permit ip any any
ipv6 route 2C0F:FEC8:E100:700::/56 2012::1
!
End
```

Router PE1 configuration:

```
hostname PE1
!
vrf definition CEA1
rd 200:1
!
address-family ipv4
route-target export 200:1
route-target import 200:1
exit-address-family
!
address-family ipv6
route-target export 200:1
route-target import 200:1
exit-address-family
!
vrf definition CEB1
rd 200:2
!
address-family ipv4
route-target export 200:2
route-target import 200:2
exit-address-family
!
address-family ipv6
route-target export 200:2
route-target import 200:2
```

```
exit-address-family
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
ip address 41.67.0.5 255.255.255.255
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
!
interface GigabitEthernet1/0
ip address 197.251.1.1 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet2/0
ip address 197.251.1.9 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet3/0
vrf forwarding CEA1
ip address 197.251.1.33 255.255.255.248
```

```
negotiation auto
ipv6 address 2C0F:FEC8:E100:100::1/56
!
interface GigabitEthernet4/0
vrf forwarding CEB1
ip address 197.251.1.49 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:300::1/56
!
router ospf 2 vrf CEA1
log-adjacency-changes
redistribute bgp 200 subnets
network 197.251.1.33 0.0.0.0 area 0
!
router ospf 3 vrf CEB1
log-adjacency-changes
redistribute bgp 200 subnets
network 197.251.1.49 0.0.0.0 area 0
!
router ospf 1
log-adjacency-changes
network 41.67.0.5 0.0.0.0 area 0
network 197.251.1.1 0.0.0.0 area 0
network 197.251.1.9 0.0.0.0 area 0
!
router bgp 200
no synchronization
```

```
bgp log-neighbor-changes
neighbor 41.67.0.6 remote-as 200
neighbor 41.67.0.6 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 41.67.0.6 activate
neighbor 41.67.0.6 send-community extended
exit-address-family
!
address-family vpnv6
neighbor 41.67.0.6 activate
neighbor 41.67.0.6 send-community extended
exit-address-family
!
address-family ipv4 vrf CEA1
no synchronization
redistribute ospf 2 vrf CEA1
exit-address-family
!
address-family ipv6 vrf CEA1
redistribute connected
no synchronization
neighbor 2C0F:FEC8:E100:100::2 remote-as 100
neighbor 2C0F:FEC8:E100:100::2 activate
exit-address-family
!
```

```
address-family ipv4 vrf CEB1
no synchronization
redistribute ospf 3 vrf CEB1
exit-address-family
!
address-family ipv6 vrf CEB1
redistribute connected
no synchronization
neighbor 2C0F:FEC8:E100:300::2 remote-as 400
neighbor 2C0F:FEC8:E100:300::2 activate
exit-address-family
!
End
```

Router PE2 configuration:

```
hostname PE2
!
vrf definition CEA2
rd 200:1
!
address-family ipv4
route-target export 200:1
route-target import 200:1
exit-address-family
!
address-family ipv6
route-target export 200:1
route-target import 200:1
exit-address-family
!
vrf definition CEB2
rd 200:2
!
address-family ipv4
route-target export 200:2
route-target import 200:2
exit-address-family
!
address-family ipv6
route-target export 200:2
route-target import 200:2
```

```
exit-address-family
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
ip address 41.67.0.6 255.255.255.255
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface GigabitEthernet1/0
ip address 197.251.1.17 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet2/0
ip address 197.251.1.25 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet3/0
vrf forwarding CEA2
ip address 197.251.1.41 255.255.255.248
negotiation auto
```

```
ipv6 address 2C0F:FEC8:E100:200::1/56
!
interface GigabitEthernet4/0
vrf forwarding CEB2
ip address 197.251.1.57 255.255.255.248
negotiation auto
ipv6 address 2C0F:FEC8:E100:400::1/56
!
!
router ospf 2 vrf CEA2
log-adjacency-changes
redistribute bgp 200 subnets
network 197.251.1.41 0.0.0.0 area 0
!
router ospf 3 vrf CEB2
log-adjacency-changes
redistribute bgp 200 subnets
network 197.251.1.57 0.0.0.0 area 0
!
router ospf 1
log-adjacency-changes
network 41.67.0.6 0.0.0.0 area 0
network 197.251.1.17 0.0.0.0 area 0
network 197.251.1.25 0.0.0.0 area 0
!
router bgp 200
no synchronization
```

```
bgp log-neighbor-changes
neighbor 41.67.0.5 remote-as 200
neighbor 41.67.0.5 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 41.67.0.5 activate
neighbor 41.67.0.5 send-community extended
exit-address-family
!
address-family vpnv6
neighbor 41.67.0.5 activate
neighbor 41.67.0.5 send-community extended
exit-address-family
!
address-family ipv4 vrf CEA2
no synchronization
redistribute ospf 2 vrf CEA2
exit-address-family
!
address-family ipv6 vrf CEA2
redistribute connected
no synchronization
neighbor 2C0F:FEC8:E100:200::2 remote-as 300
neighbor 2C0F:FEC8:E100:200::2 activate
exit-address-family
!
```

```
address-family ipv4 vrf CEB2
no synchronization
redistribute ospf 3 vrf CEB2
exit-address-family
!
address-family ipv6 vrf CEB2
redistribute connected
no synchronization
neighbor 2C0F:FEC8:E100:400::2 remote-as 500
neighbor 2C0F:FEC8:E100:400::2 activate
exit-address-family
!
End
```

Router P1 configuration:

```
hostname P1
!
interface Loopback0
ip address 41.67.0.7 255.255.255.255
!
interface GigabitEthernet1/0
ip address 197.251.1.2 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet2/0
```

```
ip address 197.251.1.18 255.255.255.248
negotiation auto
mplsip
!
router ospf 1
log-adjacency-changes
network 41.67.0.7 0.0.0.0 area 0
network 197.251.1.2 0.0.0.0 area 0
network 197.251.1.18 0.0.0.0 area 0
!
end
```

Router P2 configuration:

```
hostname P2
!
interface Loopback0
ip address 41.67.0.8 255.255.255.255
!
interface GigabitEthernet1/0
ip address 197.251.1.10 255.255.255.248
negotiation auto
mplsip
!
interface GigabitEthernet2/0
ip address 197.251.1.26 255.255.255.248
negotiation auto
```

```
mplsip
!
router ospf 1
log-adjacency-changes
network 41.67.0.8 0.0.0.0 area 0
network 197.251.1.10 0.0.0.0 area 0
network 197.251.1.26 0.0.0.0 area 0
!
End
```