



VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Zelalem Temesgen Weldeselasie

Layer 3 Multiprotocol Label Switching Virtual Private Network

Technology and Communication

2014

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Zelalem Temesgen Weldeselasie
Title	Layer 3 Multiprotocol Label Switching Virtual Private Network
Year	2014
Language	English
Pages	47 + 7 Appendices
Name of Supervisor	Chao Gao (DR.Tech.)

Layer 3 Multi-protocol Label Switching Virtual Private Networks (L3 MPLS VPNs) is becoming a key technology of Service Providers' Services for corporations who desire to use remote connectivity. It is getting more popularity by customers for its significant advantages over the prior VPN technologies such as Frame relay and ATM.

The main purpose of this thesis project was to develop an understanding of L3 MPLS VPNs in theory and practice. It is targeting to explain the technology briefly and demonstrate how it works to prepare a learning material for Data Network Services course given at VAMK, University of Applied Sciences.

The practical part of this project took place in the Technobothnia Research Center using Cisco technology. Four Cisco 2801 routers, laboratory computers and Ethernet and serial media links were used to build the network and accomplish connectivity. There are also software tools used such as HyperTerminal to configure the routers and WireShark packet analyzer to examine the communication protocols used for connectivity.

Keywords Layer 3, MPLS, VPN

FOREWORD

This thesis is written as a completion for Degree program in Information Technology for Vaasan ammattikorkeakoulu, University of Applied Sciences.

I would like to forward gratitude to my supervisor Dr. Chao Gao for his guiding, understanding and patience he presented during my thesis writing experience.

Special thanks for Matti Puska who made my thesis journey interesting and easier to finish. I really appreciate his kindness and support.

May, 2014

Vaasa

Zelalem T. Weldeselasi

CONTENTS

ABSTRACT

1	INTRODUCTION	11
2	MULTIPROTOCOL LABEL SWITCHING	12
	2.1 Technology Background of MPLS	12
	2.2 Why MPLS?.....	15
	2.3 MPLS Operation	16
	2.4 Value Added Services	17
	2.5 MPLS Label and Label Stack	18
	2.6 Label Distribution and Label Distribution Protocol	20
3	L3 MPLS VPN	24
	3.1 Overview of VPNs	24
	3.2 Classification of VPN	26
	3.3 Introduction to L3 MPLS VPN	26
	3.4 Advantages and Disadvantages	28
	3.5 Routing Issue	29
4	IMPLEMENTATION.....	31
	4.1 Requirements	31
	4.2 Topology and Address	34
	4.3 Configuration	36
	4.4 Test Result.....	38
5	ANALYSIS	40
6	CONCLUSION.....	46
	REFERENCES	47
	APPENDICES	48

ABBREVIATIONS

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AtoM	Any Transport over MPLS
BGP	Boarder Gateway Protocol
BoS	Bottom of Stack
C	Customer Router
CE	Customer Edge Router
CPU	Central Processing Unit
DRAM	Dynamic Random-Access Memory
EIGRP	Enhanced Interior Gateway Routing Protocol
EXP	Experimental
FEC	Forwarding Equivalence Class
FRR	Fast ReRouting
GMPLS	Generalized Multiprotocol Label Switching
GP	Gateway Protocol
GRE	General Routing Encapsulation
IDB	Interface Descriptor Block
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol

IOS	Internetwork Operating System
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LDP	Layer Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LSP	Label Switching Protocol
LSR	Label Switching Router
MIS	Management Information System
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
OSI	Open Systems Interconnection model

OSPF	Open Shortest Path First
P	Provider Router
P2P	Peer-to-Peer
PE	Provider Edge Router
PIM	Protocol Independent Multicasting
POS	Packet over SONET/SDH
PPP	Point-to-Point Protocol
QoS	Quality of Service
RD	Routing Distinguisher
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RD	Route Distinguisher
RT	Route Target
SP	Service Provider
TCP	Transmission Control Protocol
TE	Traffic Engineering
TFTP	Trivial File Transfer Protocol
TTL	Time-To-Live
UDP	User Datagram Protocol

VAN	Value Added Network
WAN	Wide Area Network
VoIP	Voice over Internet Protocol
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPNv4	Virtual Private Network with IP Version 4
VRF	Virtual Routing and Forwarding

LIST OF FIGURES

Figure 1. MPLS Principle.....	13
Figure 2. Value added Services	17
Figure 3. 32 bit MPLS label.....	18
Figure 4. LDP session establishment/2/	22
Figure 5. Classification of Virtual Private Networks /9/.....	26
Figure 6. VPNv4 routing	30
Figure 7. Tftpd32 preparation	32
Figure 8. IOS copying from TFTP server	33
Figure 9. Topology	35
Figure 10. Routers end to end connection demonstrated by ping and trace route	39
Figure 11. WireShark screenshot for MPLS packet header	40
Figure 12. WireShark screenshot for LDP Hello	41
Figure 13. WireShark screenshot for LDP KeepAlive Messages	42
Figure 14. WireShark screenshot for BGP KeepAlive Message.....	43

LIST OF TABLES

Table 1. Reserved label values /7/	19
Table 2. Advantages and Disadvantages of L3 MPLS VPNs /10/	28
Table 3. Address table	35
Table 4. BGP header description	44

LIST OF APPENDICES

- Appendix 1.** Provider Edge (PE) router configuration
- Appendix 2.** Customer Edge (CE) router configuration
- Appendix 3.** CE1 routing protocol verification
- Appendix 5.** PE1 routing protocol verification
- Appendix 6.** PE1 VRF routing verification
- Appendix 7.** PE1 BGP verification
- Appendix 8.** PE1 LDP neighbor

1 INTRODUCTION

We are living in the era of technology where information gets closer to us than ever. Accessing and acquiring services from the Internet and different sources become simple to use distantly from anywhere. Employers are offering flexibility of working condition for their employees to carry out their tasks from their home or from any other part of the world as if they were physically connected to the corporation's network. On the other hand Service Providers are competing with each other to deliver the best of their services to succeed in the market.

A number of various technologies have been deployed to achieve a fast, reliable and secured connection for transferring data, voice and video over the Internet. Network utility producers release their newer versions all the time to cop up with customers' demand. L3 MPLS VPN is becoming more preferable to customers due to its several advantages over the other technologies which are still in use today.

This thesis explains briefly the background and scope of the L3 MPLS VPN technology and illustrates a network scenario to demonstrate and examine the protocols used for communication.

The structure of the thesis is arranged by dividing the topic in to seven chapters. Chapter 2 will explain the background, advantages and applicability of MPLS in deep. Chapter 3 will describe the VPN technology and security subjects. Chapter 4 introduces the L3 MPLS VPN technology and its routing issues. The practical part which has been performed in the laboratory will be described in Chapter 5 and the test analysis will be explained in the next chapter. Chapter 7 will give conclusion about this thesis.

2 MULTIPROTOCOL LABEL SWITCHING

2.1 Technology Background of MPLS

Comparing to other Wide Area Network (WAN) protocols for data networking, such as ATM and Frame Relay Service, Multi-Protocol Label Switching (MPLS) promises a number of new competences and control features for service providers. MPLS is an Internet Engineering Task Force (IETF) proposal that eliminates the desires of dependency on a particular OSI model data link layer technology. It becomes a competent technology due to less overhead requirement which provides connection oriented services for variable length frames. It expands the functionality of an IP-based network infrastructure by adding flexibility for the restrictions. MPLS packets can run on other Layer 2 technologies such as ATM, Frame Relay, PPP, POS and Ethernet, in the same manner as these Layer 2 technologies can run on MPLS network /4/.

MPLS is normally used by Service Providers, however large scale corporations also build their own private MPLS network. The popularity of this technology is attracting customers as a result of its lower price and scalability which makes it superior regarding network routing size, routing performance, link bandwidth utilization and services.

In case of traditional network layer packet forwarding like IP forwarding, packet travels from one router to the next by each routers independent forwarding decision /1/. The main approach of MPLS is adding connection oriented operation to the IP network to avoid complex lookups (longest prefix matching) in the routing table which creates a bottleneck in high performance routers. Routers which support MPLS are called Label Switching Routers (LSR). In the ordinary IP routing, every router examines the packet's IP header and runs a network layer routing algorithm. Unlike these, MPLS computes a path and makes routing decision at the source router by assigning short fixed length known as "label" and the intermediate LSR reads the label and switches the packet according to their local Label Forwarding Information Base (LFIB) /2/. LFIB is a label switching skim built by

LSRs after exchanging MPLS label information between them. In short MPLS switches packets instead of routing packets for delivery of IP services.

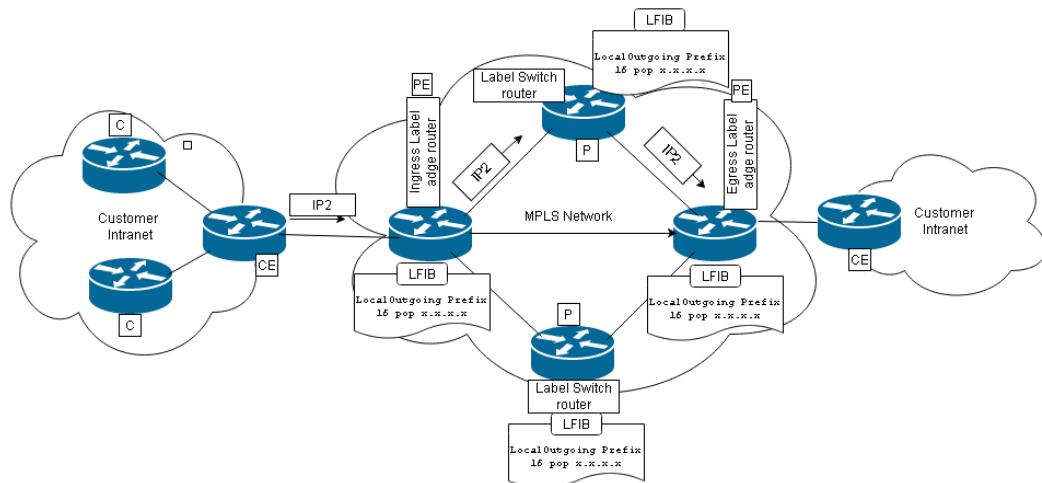


Figure 1. MPLS Principle

Figure 1 shows a general structure of MPLS network and how it works. The MPLS routers can be clarified as:

- **P (Provider Routers):** Also called Core or Intermediate LSRs or Transit routers, are the backbone routers which perform the label switching. They execute the switching by manipulating the packet label to forward it to the correct data link.
- **PE (Provider Edge router):** Also known as Label Edge Router (LER). This router is facing the customer router featuring termination in multiple services like; Internet, L3 VPN, L2 VPN, VPLS.
- **C (Customer Routers):** This router is used by the customer network
- **CE (Customer Edge router):** Is the router which peers at L3 provider edge to converses directly with it.

The provider router P is connected to the CE router through the PE router with a single physical interface for each customer. Through the customer internal network, C routers and a suitable Gateway Protocol (GP) will be used for the distribution. This will be advertised to the PE via the CE router.

The PE router serves as **ingress** and **egress** router depending on the direction of data flow. There are also other types of LSRs from where the path has been established to forward the packet through the network.

- **Ingress Label Edge Router:** represents the packet source side of the PE router. It makes the routing decision by adding (pushing) label on the top of the represented IPv4 network address.
- **Egress Label Edge Router:** On the other hand the egress PE router removes (pops) the label and routes the packet to the access network.
- **Penultimate router:** This router is located next to the last hop in the MPLS network. It performs the egress LER operation which is removing the label before sending the packet in to the customer network.

Label Switched Paths (LSPs) are the sequence of labels which are unidirectional paths through one or more LSRs at one level of hierarchy followed by packets in a particular Forwarding Equivalence Class (FEC) and they are determined by LSRs. FEC is a collection of an IP packet which needs a common transport treatment. The IP packet received by the ingress LSR will be observed to pick the FEC depending on the unicast IP address and by using several layers information. Generally LSPs are made for point to point connection; however, lately there are new approaches introduced specifically for multicasting purposes so-called point to multi-point and hub & spoke multipoint. Incoming LSPs with similar destination address and transport treatment but different labels can be merged in to a single LSP due to saving label space, efficiency of LFIB lookups and speeding up the restoration under error circumstances.

Label Information Base (LIB) is a database created by the routing and label information exchange between LER and LSR and the LIB is kept in control plane. It consists of FEC information (like destination network prefix), local label (which is advertised to neighbor LSRs) and next-hop label received from neighbor. On the other hand the LFIB in the data plane is used for forwarding decision which is built by the LERs and LSRs according to the information in the routing table, the

ARP table and the label distribution in the MPLS routers. It has the information of FEC, input and output labels, output interface and next hop IP address. Technically, the LFIB is a subset of LIB which contains only those local labels that are currently being used for forwarding.

2.2 Why MPLS?

Customers who are building a high-speed IP core can enable a single infrastructure which is efficient to support a multitude of applications in a secured manner to minimize the cost of establishing a simplified network. MPLS is desirable technology to fulfill the need of high-speed communication. Adding MPLS to a network can be capable of bringing several advantages related to economical solutions, scalability, bandwidth management and simplified networking /3/. These advantages are explained briefly below.

Economic solutions by using a single network infrastructure:

The great advantage of MPLS is the first provider edge router from the source side which will label the packet based on the their destination address or other preconfigured standards and switch all the traffics over a common infrastructure which makes MPLS a method of switching multiple protocols in a single network /5/.

Scalability:

With conventional IP packet forwarding, any topology change such as subnet ID change or location change is linked to all devices within the routing domain and this process always involves a period of convergence due to routers relying on the IP header information. Adding label on the top of IP packets will provide communication to other devices through the distribution of new label to implement a mechanism with low convergence for the change in the topology.

Bandwidth management:

MPLS provides unequal load balancing network protection and faster restoration. It also offers a guaranteed bandwidth solutions, in which customers can provide voice and data services with point-to-point guarantees with a predictable delivery at a various network conditions to address the traditional IP networking limitations.

2.3 MPLS Operation

The basic idea of MPLS is to separate the path finding and bulk frame switching operations by routing only once at the LER which marks the packet to a common destination with a label. LSRs assign these labels to routing table entries and distribute the label values with other LSRs using Layer Distributing Protocols (LDP), Resource Reservation Protocol (RSVP) or a modified routing protocol [2].

In Figure 1, the customer edge routers (acting as a default gateway of the subnet) forward IP packets to the LER. The LER will insert a label to this IP packet according to its destination IP address. This label is used by all the LSRs in the MPLS network (enclosed by the cloud). Eventually the labelled IP packet reaches the destination LER which removes the label and forwards it to the destination network.

In an MPLS network, routers can use normal (such as RIP, EIGRP and OSPF) or extended (for example LDP and Resource Reservation Protocol with Traffic Engineering (RSVP-TE)) routing protocols to build topology database. When a packet is received by the provider edge router in the core from a local customer network router (non-MPLS network), the PE router in this case the ingress will study the packet, determine a path and add a label to forward in to the provider core. In the MPLS core network, it will be the intermediate LSRs responsibility to forward the packet according to the label attached to it until the destination PE router which is the egress router. Finally, this egress LSR removes the MPLS label and forwards the packet in to the customer network with an appropriate Layer 2 header. In this process the ingress router isolates the routes of different customers to logical VRF instances and builds a routing table for each of instances at the entry point.

The customer inside local network can use any private addresses and it is possible that different VPNs can have overlapping private IP addresses. The uniqueness of address is needed only between each customer. This intranet can use static routing or any suitable Interior Gateway Protocol (IGP) like RIP, EIGRP or OSPF.

2.4 Value Added Services

Additional services can be deployed on the top MPLS network whether the customer wishes to migrate the previous protocol or add the facility over the preceding network.

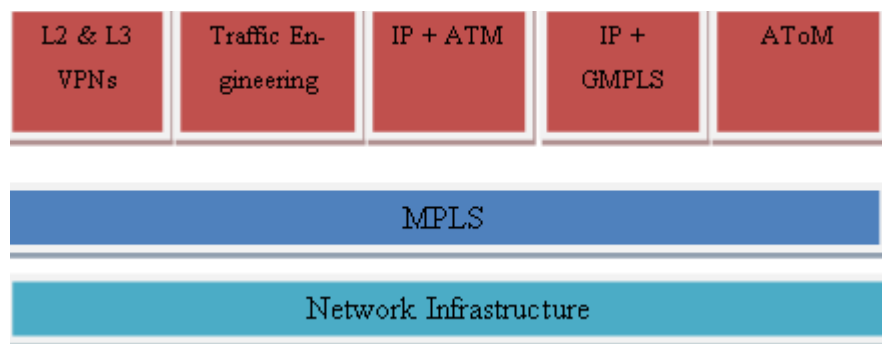


Figure 2.Value added Services

Figure 2 shows further technologies and protocols that can be added over MPLS network, these are explained below:

- **L2 and L3 VPNs:**

MPLS Virtual Private Network separate traffic of different VPNs using Virtual Routing and Forwarding (VRF) instances and Multiprotocol BGP attributes [2]. It adds flexibility for the network traffic to transport packets on the MPLS backbone network.

- **Traffic Engineering (TE):**

Traffic Engineering controls the packet flow to optimize network and offer differentiated services. Implementing TE over MPLS network will deliver a consistently spreading of traffic and utilization of all available links. The other advantage of TE is that the possibility of Fast ReRouting (FRR), which permits labeled packets

to be rerouted when the link becomes unavailable or down within less than 50 ms, which is faster than standards used today /5/.

- **GMPLS:**

Generalized MPLS is enhancement for MPLS to provide multiple types of switching, i.e. the addition of support for EDM, lambda and fiber (port) switching /6/.

- **Quality of Service (QoS):**

MPLS with QoS, VPNs can be guaranteed with hard QoS by providing multiple classes of services /3/.

- **AToM**

Any Transport over MPLS (AToM) is a feature that any Layer 2 frame is carried across the MPLS. This allows service providers to facilitate customers to transport Layer 2 packets over MPLS backbone, just like any other IP networks with their existing data link layer network.

2.5 MPLS Label and Label Stack

MPLS is sometimes called Layer 2.5 technology because the label is added between the Layer 2 Data Link Layer frame header and the Layer 3 Network Layer packet header. This label acknowledged as an MPLS shim.

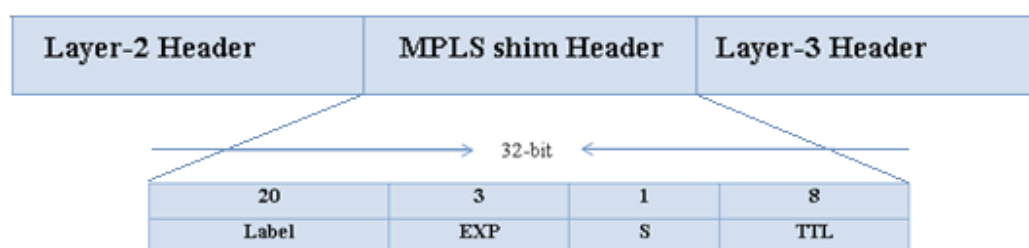


Figure 3. 32 bit MPLS label

In Figure 3, the 32 bit MPLS label has four units, each having different bit values and functions due to the routing process. The first 20-bits are specifies the **label**. The next 3-bits are **Experimental (EXP)** bits used for traffic class field to provide QoS capabilities by using the bits set in the MPLS label. The 1-bit on third section is the **Bottom of Stack** flag. Normally it has set to 0 unless this is the last label in

the case of multiple labels usage. The last 8-bits are the **Time-To-Live (TTL)** field. This TTL behaves in the same manner as IP header TTL that it decreases the value by one in each hop to prevent routing loop by setting the TTL limit and discard the packet when the value reaches zero. The ingress LER copies the coming IP packet of TTL value in to the TTL field of the shim label and by the exit; the egress router also copies the shim label TTL value back to the TTL on the Layer packet header.

Table 1. Reserved label values /7/

Label	Description	Remark
0	IPv4 explicit NULL label	Only legal at the bottom of the label stack indicating that the label stack needs to be popped and forwarded based on IPv4 header.
1	Router alert label	Legal anywhere but not at the stack bottom
2	IPv6 explicit NULL label	Only legal at the bottom of the label stack indicating that the label stack needs to be popped and forwarded based on IPv6 header.
3	Implicit NULL label	Assigned and distributed by the LSR though, may not appear on the encapsulation.
4-15	Reserved	N/A

Table 1 illustrates the reserved values of 20-bit label and their appearance in the header. In fact the value of the label varies between 0 to $20^{20} - 1$ or 1,048,575 which gives additional information needed to forward the packet.

There are three procedures when forwarding a packet through an MPLS network. When the ingress router inserts this label to the packet, it is called *pushing*. The second one is called *swapping*; this is when the intermediate routers change the label throughout the network. During swapping, if an unlabeled packet arrives in the LSR, it will examine the network layer header (IP header) to learn the packet's FEC to forward to the next hop. Finally, the egress router or sometimes the Penultimate router will remove the shim label and send it to the IP network, this procedure is known as *popping*.

It is possible to use tunneling over another MPLS network to build interconnection between private MPLS clouds, MPLS Virtual Private Network (VPNs), or hierarchical Traffic Engineering [5]. In this case label stacking is used to route the packet through the MPLS network by packing the labels in to a stack. The first and the last labels are called *top label* and *bottom label* respectively. Between these two labels there can be unlimited number of labels packed. In the stack, only the bottom label has value of "1" for BoS because it is the last label.

2.6 Label Distribution and Label Distribution Protocol

In the process of MPLS packet delivery, here it goes the steps of label creation, LSP selection and finally the label distribution. The LERs and LSRs build their internal LFIB table to illustrate the incoming labeled packets followed by the LER commencement to create a label with a special MPLS control message containing the FEC information for mainly the destination IP address subnet. There are three basic methods used for label creation: *Topology-based* (the method uses ordinary routing protocol information to determine a need for an FEC to LSP mapping), *Request-based* (based on Resource Reservation Protocol 'RSVP' resource request) and *Traffic-based* (the method builds the mapping and the path, after receiving the first packet of the FEC).

Layer Switched Path (LSP) is a mechanism of selecting a path via LSRs by learning their neighbors using LDP hello procedure. MPLS offers two methods for LSP selection: The first one is *Hop-by-Hop routing* in a similar manner to the traditional IP routing where every LSRs select their next hop independently based on

the local routing table information. The second option is based on the *Explicit routing*. This routing is defined via the ingress router by the network administrator configuration or through routing protocol configuration which triggers a dynamic routing explicit path. In the explicit routing the hop can be either *strict* or *loose*. Strict hops are referred as the directly connected hops in the path and loose hops are the remotely connected ones /8/.

LDP is a set of procedures that LERs and LSRs exchange information concerning label distribution and FEC binding made by each of the routers to build a complete topology of the network which guarantees the reachability of each node. LSR binds label to the IPv4 prefix and the local and remote bindings will be stored in a table known as Label Information Base (LIB). Binding has a great advantage of synchronizing label distribution and routing to eliminate the need of other protocols configured in the LSR.

The four steps of LDP message exchange are:

1) Peer discovery: A peer is a pair of LSRs which are connected directly or indirectly to exchange label information. Therefore, in this stage LSRs multicast their presence for all neighbors in the subnet to establish an LDP peer relationship through periodic *Hello* messages. These messages use unreliable UDP transport over port 646. If two LSRs are label distribution peers by receiving the LDP Hello, it indicates that there exists *Hello adjacency* between them. Listing 1 shows an example of LDP discovery between PE1 (IP address 7.7.7.7) and PE2 (IP address 2.2.2.2).

<pre>PE1#show mpls ldp discovery Local LDP Identifier: 2.2.2.2:0 Discovery Sources: Interfaces: FastEthernet0/0 (ldp): xmit/recv LDP Id: 7.7.7.7:0</pre>	<pre>PE2#show mpls ldp discovery Local LDP Identifier: 7.7.7.7:0 Discovery Sources: Interfaces: FastEthernet0/0 (ldp): xmit/recv LDP Id: 2.2.2.2:0</pre>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

Listing 1. LDP Discovery

2) **Session establishment:** In this stage the LSR establishes a TCP connection with standard three-way handshake. The connection setup is between active and passive parties where the active is the LSR with the higher IP address which starts the session establishment by sending the LDP initialization as displayed on Figure 4. On the other hand, the passive party will reply “LDP KeepAlive” for acceptance or “session reject” or “error notification” message for rejection the LDP initialization.

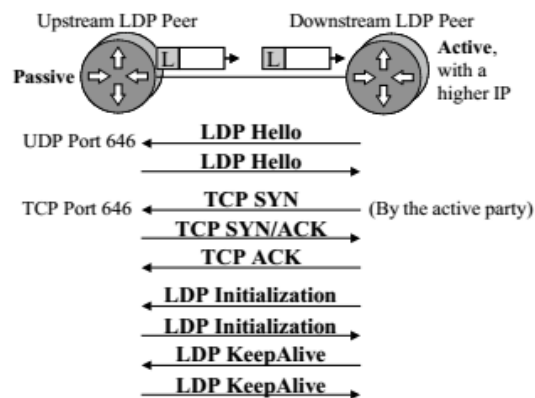


Figure 4. LDP session establishment/2/

3) **Session maintenance:** The session establishment will be retained active with a periodic hello messages. If one of the peer is unsuccessful to receive the Hellos in a given hold time, then the LDP session will be terminated due to the failure of peer.

4) **Label distribution:** LDP address message is exchanged between LERs and LSRs to build the LSP known as label distribution. The sender and receiver routers will use the LDP addresses to maintain their mapping and identify next hop address.

The label is advertised to all LSRs by the ingress LER regardless of the upstream or downstream of destination within one LSP. The ingress router will push one or more labels and the intermediate LSRs will swap the packet by changing the top level of the label value and forward it until the end of the MPLS network where the egress router rips off the label. The label value can be exchanged using: LDP, RSVP or routing protocols, Traffic Engineering and resource reservation, Border

Gateway Protocol (BGP) for inner VPN labels or Protocol Independent Multicasting (PIM) for multicasting.

3 L3 MPLS VPN

3.1 Overview of VPNs

Virtual Private Network (VPN) is developed to use the public telecommunication infrastructure like the Internet, privately and securely within different sites or groups which are allowed to access remotely as one private network. It allows branch sites to use resources and send data across the public network just as they are physically connected to the company network. In early days, information exchange was made using dial-up modems or through leased lines by mail, telephone or fax. These techniques had so many downsides related to the low flexibility, speed, security and performance for branch and teleworkers to exchange information. High price of communication establishment was also the other disadvantage of these technologies each node needed to be connected physically by cables.

In the mid-1990s companies were demanding a better way of connection to exchange their data securely due to the drawbacks mentioned above. This has led to the development of VPN using the Internet which is highly secured and cheap. To explain the name VPN, it is *virtual* because there is no real physical connection between sites or nodes; it operates using special software provided for VPNs. It is *private* because only authorized users are allowed to use the network. VPN can be deployed within shared backbone network infrastructures using a layer-2 ATM or frame relay, IP or An MPLS networks.

VPN allows employees to connect to the corporate network or other companies regardless of their location to use the resources and communicate with each other. Companies can choose how they can establish their VPN, either by Management Information Systems (MIS) department solutions where the company itself takes the responsibility to buy, install and maintain VPN infrastructure or they can choose Value Added Network (VAN) solutions, which means paying an outsourced company to provide all the telecommunication infrastructure solution/ 9/.

There are two kinds of VPN usages, intranet and extranet. The intranet is the local network in the corporation where the employees use the VPN inside the company which is not visible to the outside Internet users. This helps to keep the network safe from malicious users outside the company. On the other hand the remote network of a corporation that uses the IP network connectivity to allow remote employees to use the VPN is called extranet. Even though it is called extranet, it performs as an intranet through the Internet. This is because the actual server is protected by a firewall to control the access between intranet and Internet by clarifying the users in a way of authentication. Any node that desires to connect to this network needs to use a correct username and password or an IP address.

A tunnel is a method which is used in VPN to provide a way of transporting packets through the public network. The tunneling mechanism can be created based on the protocols used in the network like IP-header, MPLS label, General Routing Encapsulation (GRE) field, etc. It can be generated either statically or dynamically according to the VPN establishment configuration.

In VPN usage security is the main issue since it is using the public network privately. The main goals of securing the VPN are based on the privacy, reliability and availability matters. By privacy we mean that the data transfer must be confidential for those users who are only authorized for the facility. The communication also must be aware of reliability of the data which has been sent and received between hosts and data transferring must be available when it is needed. Software, hardware, ISPs and some security polices will be involved to achieve these goals listed above. Mostly username and password are required to authorize users and encryptions to encrypt data. If all the machines in the VPN are using the same encryption key, it is called symmetric encryption and if they use different keys for public and private, then it is called asymmetric encryption.

3.2 Classification of VPN

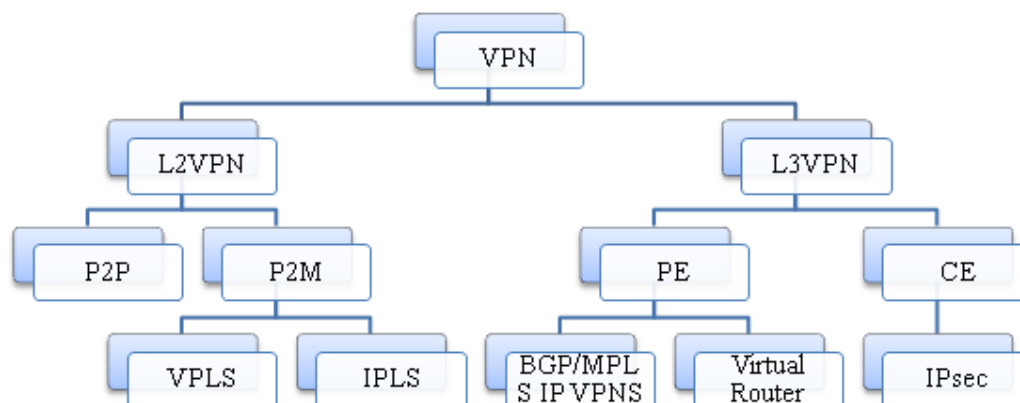


Figure 5.Classification of Virtual Private Networks /9/

Figure 5 illustrates the different types of VPNs through Layer 2 and Layer 3. In L2 VPNs, only non-IP protocols are taken in to account and Provider network is not responsible for distributing router information to the VPN sites. Since L3 VPN passes through the network layer, all the packets must be encapsulated with an IP header and the Provider will take the responsibility of routing information distribution. IPsec is a network layer security protocol which is used widely to protect the connection from malicious and attackers.

3.3 Introduction to L3 MPLS VPN

L3 MPLS VPN is a service offered by the service providers which delivers IP connectivity between customer businesses to outsource their services to diverse locations. These networks necessitate the corporations to peer with SP at the network Layer level which makes it different than the overlay VPNs we are using today, such as ATM and Frame relay. The connectivity and data transferring is implemented by each customer's VRF (Virtual Routing/Forwarding) tables.

In addition to the normal MPLS terminologies mentioned in the first chapter, there are some extra links and used for the L3 MPLS VPN connection. These are:

Backdoor connectivity is the link which connects the customer routers outside the MPLS VPN cloud where the customer routers use the same Interior Gateway

Protocol. This is an optional link which will be used as a backup in case the service provider does not offer an external leased line which is integrated to the VRF.

MP-BGP is shortened from Multi-Protocol Border Gateway Protocol which supports IPv4 and IPv6. It is an extension protocol for BGP which runs between the PE routers to exchange VPNv4 labels learned from the customer sites over an MPLS network.

Route Distinguisher (RD): The ingress LER makes routing decision by adding (pushing) 64-bit (8 byte) RD to the presented IPv4 network address resulting in a 96-bit of address called VPNv4 address. The RD selection should consider that the VPNv4 must be unique even in the case of private IP address redundancy.

Route Target (RT): besides the RD, RT is also used to determine the VPNv4 that should be installed in the VRF /10/. It is also a 64-bit number. The RT is inserted to the VRF for controlling the import and export of routes among other VRF's.

VPNv4 is a 96-bit address formed by the combination of the RD and IPv4 which passes in the MP-BGP.

Virtual Routing and Forwarding (VRF): The VRF identifies if the IP address of the customer who is attached to the PE router is a member of the VPN. It contains information of an IP routing table and with the corresponding interfaces and a set of rules and routing protocol parameters which are pointed out in the routing table.

In the basic L3 MPLS VPNs network topology, the providers connect customers through the PE routers using single physical interface with a subnet for each customer on their CE routers. The customers can use C routers for their local network to establish a LAN. The PE router selects the best path by the ingress router within the correct VRF table and labels the packets with suitable MPLS label. The P routers in the core will forward the packets by changing the label value based on their local LFIB table and by the exit the egress router will remove the label and deliver the packet to the local customer network with original IP to be forwarded to the destination.

3.4 Advantages and Disadvantages

L3 MPLS VPNs have numerous substantial advantages for service providers and their customer corporations. The advantages and the drawback of this technology are explained in Table 2.

Table 2. Advantages and Disadvantages of L3 MPLS VPNs /10/

Advantages	Disadvantages
Scalability of network size: The L3 MPLS VPN offers extremely scalable VPN architecture for customers to expand their sites in to thousands of locations.	They only transport IPv4 traffics, non-IP protocols need a way of tunneling which requires a mechanism called Generic Routing Encapsulation (GRE) on the customer routers to transport the packets though the provider network.
Scalability of routing: Unlike the ATM and Frame relay, L3 MPLS VPNs routing will have less demand on the customer or customer edge routers which will consume less CPU and Interface Descriptor Block (IDB).	Service Provider dependency: The network is dependent on the SP regards to the Layer 3 features, even if the technology allows some exceptional features such as IP Multicast; the SP may not offer this service.
Scalability of bandwidth: The connectivity is not limited by the connection media type, it is depends on the SP infrastructure for PE-CE.	Possible difficulties in integration—The difficulty of integration from Layer 2 to Layer 3 peering varies greatly depending on the SP offering. For example, EIGRP as a PE-CE protocol is ideal for customers already running EIGRP as their IGP. However, if the SP does not offer this service, integration with a different routing protocol, such as eBGP, might require design changes and training of network staff.
Less cost: Comparing with other similar purpose networking solutions, MPLS offers less expensive utility because of network farm out responsibility and lower service cost. (typically 10-40 percent lower)	
Intelligent QoS—The SP can now provide L3 QoS, which allows more intelligence in the SP core compared to L2 QoS.	

<p>Any-to-any connectivity—By peering with the SP at Layer 3, each site (after it is terminated into the SP cloud) can be configured with IP route reachability to all other customer sites. This allows any-to-any connectivity and offers more efficient routing compared to ensuring connectivity between spokes in a traditional hub-and-spoke topology. This is an important advantage where there is a growing trend toward distributed applications and VoIP.</p>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

3.5 Routing Issue

Routers in the customer network including the customer edge routers can use any routing protocols provided. Whether a static or any other dynamic routing protocols like RIP, EIGRP, OSPF or IS-IS is used, it can be redistributed in the provider routers using BGP. The customer network can use any private address provided by RFC 1918 without getting concerned about the uniqueness of subnets of different VPNs.

The CE and PE routers will be associated with the correct VRF to facilitate the MPLS network break the IP address of customers and add label on the top of it. Neither CE and C routers in the customer network need to be configured with any special features, the PE router VRF configuration will automatically initiate the peering between the PE-CE routers. The PE routers will study the IP prefixes of the remote customer network and advertise them to the CE routers which are peered with the same VRF.

The PE routers will be configured with different VRF instances for each CE router interfaces. These VRF instances form a virtual router with separate routing and forwarding tables, separate import and export rules, routing protocols and IGP peers. Extra care must be taken when giving a VRF instance identifier names since they are case sensitive. The VRF accepts routing update from the customer

network routers and alter an RD in front of the IPv4 address to advertise VPNv4 for the MPLS network.

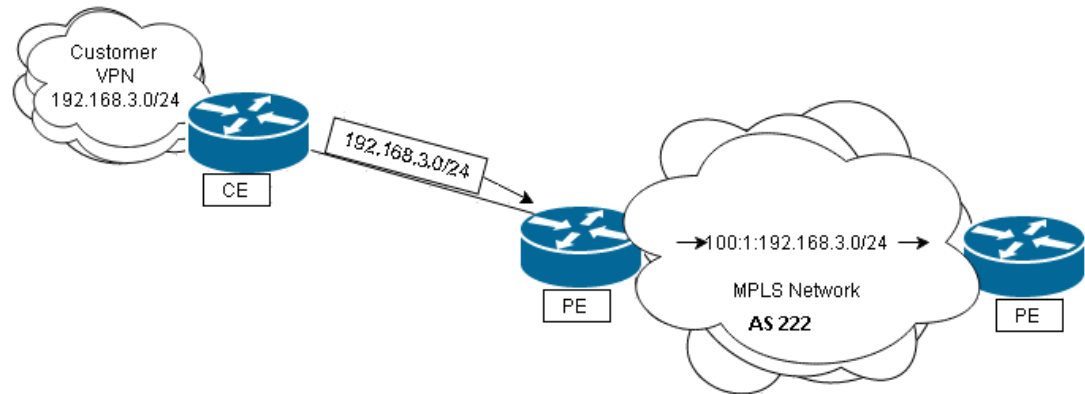


Figure 6. VPNv4 routing

Figure 6 shows the VPNv4 routing in the PE routers when using Autonomous Number in the RD. The PE router adds the RD (100:1) on the given IPv4 prefix (192.168.3.0/24) which came from the customer network and injects the VPNv4 (100:1:192.168.3.0/24) it to the MPLS network.

4 IMPLEMENTATION

4.1 Requirements

Before starting the connection and configuration to make the test, the routers must achieve the minimum hardware and software requirements to support MPLS Virtual Private Networks. These prerequisites are:

- Router which can support MPLS
- IOS which can perform MPLS VPN
- At least 192 MB DRAM and 64 MB Flash to support the IOS

According to the Cisco router memory specification for 2800 series, the routers comes with default onboard memory of 128 MB and can be raised up to maximum of 384 MB. Therefore I upgraded the memory by adding 64 MB of DRAM to meet the minimum requirement. The next step was installing the IOS to the router using TFTP server. I used “c2801-advipservicesk9-mz.124-24.T6.bin” IOS which is compatible with Cisco 2801 router to provide MPLS service.

Tftpd32 is used as TFTP server on the computer. Tftpd32 is a free, open source application which can serve as TFTP and clients servers. Download the installer from the website http://tftpd32.jounin.net/tftpd32_download.html and install it on the computer. Open the Tftpd32 application and select the setting button from the bottom of the window to configure it as a server. Uncheck all the boxes except the TFTP server and press OK to confirm. Then select the Browse button on the right side and the ‘Browse for folder’ small window will pop up. Choose the folder where the IOS is saved and continue. Figure 7 shows the screenshots of both processes.

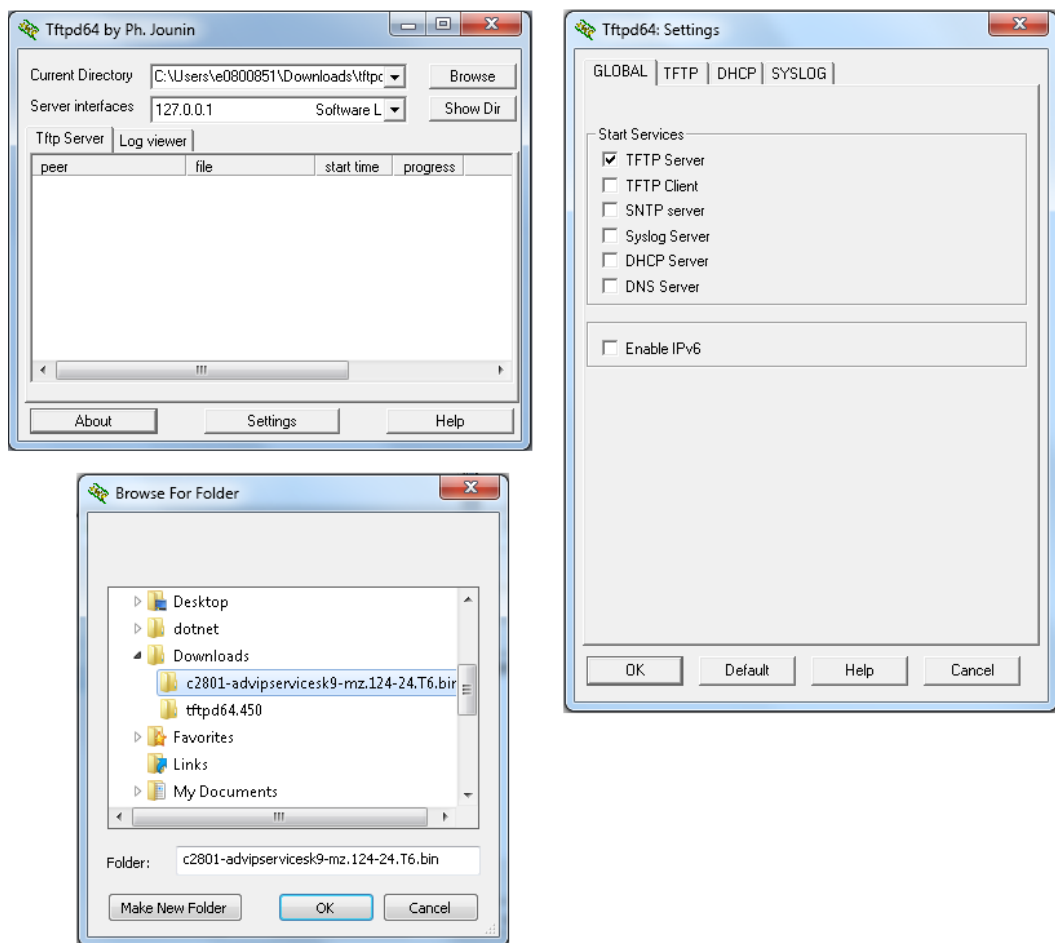


Figure 7. Tftpd32 preparation

Enter “Router#copy tftp flash” command on the router to copy the operating system from the TFTP server to the router’s flash memory. Some portion of the commands and installation process are listed on the following Listing 2.

```
[Output omitted]
Router#copy tftp flash
Address or name of remote host []? 192.168.69.194
Source filename []?
opening  tftp://255.255.255.255/cisconet.cfg  (Timed out)c2801-advipservicesk9-
mz.124-24.T6.bin
Destination filename [c2801-advipservicesk9-mz.124-24.T6.bin]?
Accessing tftp://192.168.69.194/c2801-advipservicesk9-mz.124-24.T6.bin...
Loading c2801-advipservicesk9-mz.124-24.T6.bin from 192.168.69.194 (via FastEther-
net0/0): !
[Output omitted]
```

Listing 2. IOS installation process on the router

In Listing 1, the address 192.168.69.194 is the IPv4 address of the computer in which the TFTP server is installed to facilitate connection with the router. And on the next line where it asks for the source filename, the right file is copied and pasted as it is from where it has saved in the TFTP server. After the router and server are connected and the router can access the file, it will request for destination filename. If “Enter” is pressed, the router automatically saves the IOS by the filename saved in the TFTP server. It is always suggested to remain with the original IOS filename to recognize which version it is for later use and update. Finally the router will start loading the IOS from the server stating the IP address and the router interface connected to it for file transfer.

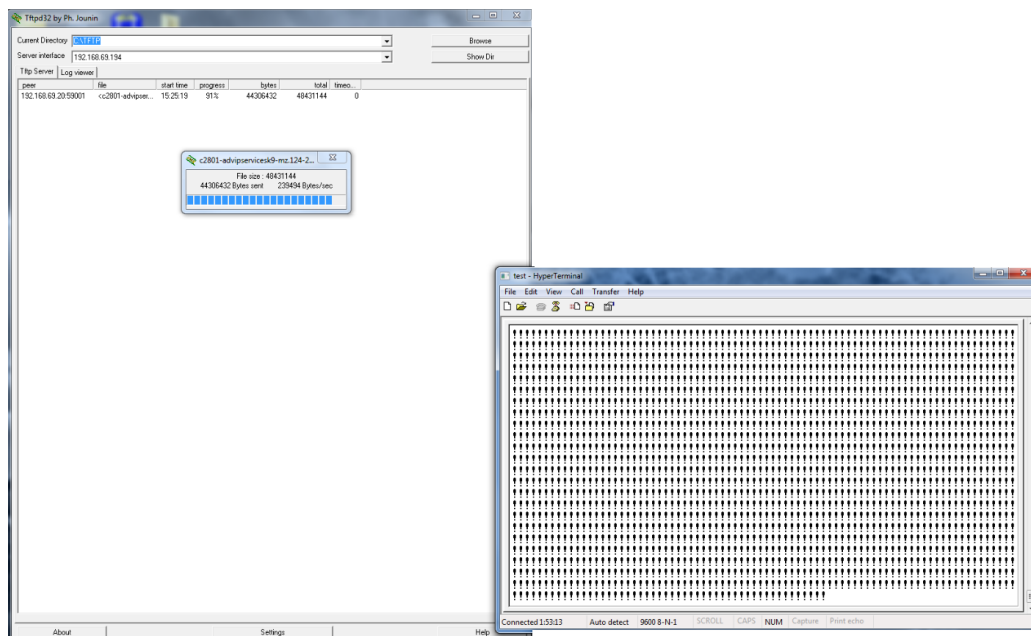


Figure 8. IOS copying from TFTP server

The screenshots on Figure 8 demonstrates the router copying the IOS from the TFTP server installed on the computer within the same subnet of the router.

It is always important to check the prerequisites step by step before starting any configuration or installation. There was one problem occurred during installing the routers, after the IOS was installed, the system could not boot the IOS from the flash memory because there was not enough space in the DRAM. Therefore, it

engaged with a non-stop attempt of booting. Some portion of the output looks like as follows in Listing 3:

```
[Output omitted]

Cisco IOS Software, 2801 Software (C2801-ADVIPSERVICESK9-M), Version 12.4(24)T6,
RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2011 by Cisco Systems, Inc.

Compiled Tue 23-Aug-11 02:02 by prod_rel_team

SYSTEM INIT: INSUFFICIENT MEMORY TO BOOT THE IMAGE!

%Software-forced reload

[Output omitted]
```

Listing 3. Router boot failure message due to the insufficient memory.

After realizing it was the memory problem, I upgraded the memory to the appropriate size which is stated above on the requirement.

4.2 Topology and Address

The network topology diagram I used to make the connection can be seen in figure 9.

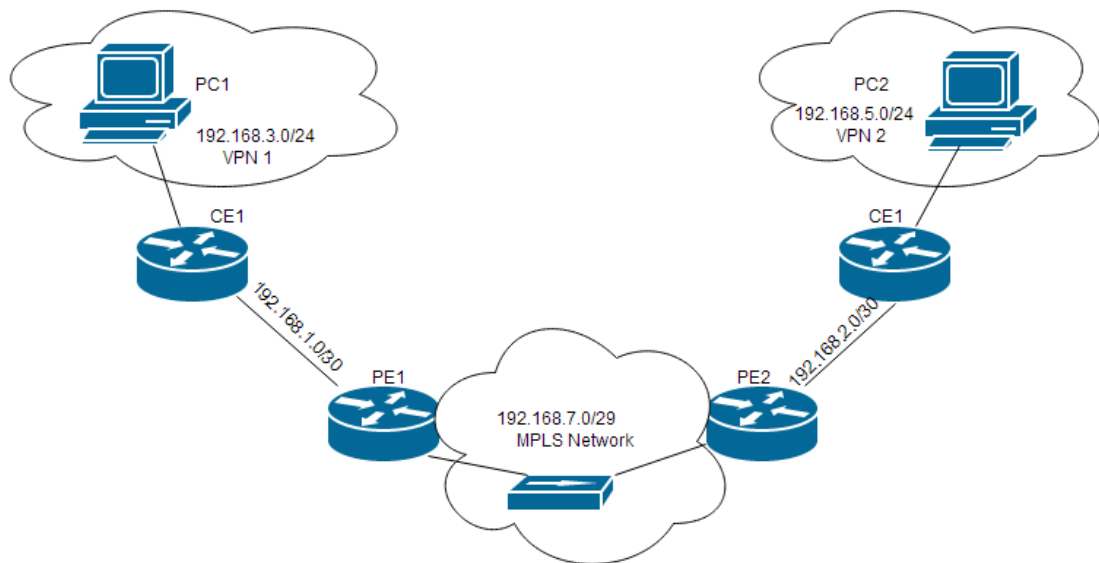


Figure 9. Topology

There are four routers used, two PE routers which perform the MPLS VPN service and two CE routers for the local network in the VPN. I used a hub in between the PE routers and extend the network to a PC in order to capture the MPLS packets. Since the hub I used was 10Base-T, I had to change the routers interface speed to 10MB/S and the duplex feature from full to half.

The interface address of the routers and computers and their subnets are specified in Table 3.

Table 3. Address table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	Fa 0	192.168.3.50	255.255.255.0	192.168.3.1
PC2	Fa 0	192.168.5.50	255.255.255.0	192.168.5.1
PE1	S0/1/0	192.168.1.1	255.255.255.252	N/A
	Fa 0/0	192.168.7.1	255.255.255.248	N/A
	Lo 0	2.2.2.2	255.255.255.255	N/A

PE2	S0/1/0	192.168.2.1	255.255.255.252	N/A
	Fa 0/0	192.168.7.2	255.255.255.248	N/A
	Lo 0	7.7.7.7	255.255.255.255	N/A
CE1	S0/1/0	192.168.1.2	255.255.255.252	N/A
	Fa 0/0	192.168.3.1	255.255.255.0	N/A
CE2	S0/1/0	192.168.2.2	255.255.255.252	N/A
	Fa 0/0	192.168.5.1	255.255.255.0	N/A

4.3 Configuration

The customer routers can be configured with any IP routing protocol like RIP, EIGRP or OSPF. For my project I used RIPv2 for routing in the local customer network and CE-PE. The PE routers which perform the label switching must be configured with MPLS and some other BGP and routing protocols. The configuration procedure will be explained step by step as follow:

1. Create the VRF with a name, I used "test" in this project

```
PE1(config)#vrf definition test
```

2. Specify the routing distinguisher (RD)

```
PE1(config)#rd 100:1
```

3. Change in to the IPv4 configuration mode for VRF

```
PE1(config)#address-family ipv4
```

4. Specify the routing target export and import policies

```
PE1(config)#ipvrf test
```

```
PE1(config-vrf)#route-target export 100:1
```

```
PE1(config-vrf)#route-target import 100:1
```

```
PE1(config-vrf)#exit
```

5. Enable the MPLS and Cisco Express Forwarding (CEF). CEF is a technology used by Cisco in layer 3 core networks to improve the performance of the network.

```
PE1(config)#mplsip
```

```
PE1(config)#ipcef
```

6. Setup and loop back interface

```
PE1(config)#interface loopback 0
```

```
PE1(config-if)#ip address 2.2.2.2 255.255.255.255
```

```
PE1(config-if)#exit
```

7. Enable the interfaces; this process is the normal enabling of the interfaces which are going to be used with a proper IP addresses, subnet and "no shutdown" command to wake the link up.

8. After the interfaces are configured, those ones which are exposed to the MPLS networks should be defined with MPLS protocols to allow the service.

```
PE1(config)#mplsip
```

```
PE1(config)#mpls label protocol ldp
```

9. Configure routing protocol for the MPLS network. It is possible to apply any routing protocol on the top label switching network. As a result I used OSPF and included the loopback address in the neighboring networks.

```
PE1(config)#router ospf 1
```

```
PE1(config-router)#network 2.2.2.2 0.0.0.0 area 0
```

```
PE1(config-router)#network 192.168.7.0 0.0.0.7 ar-  
ea 0
```

```
PE1(config-router)#network 192.168.1.0 0.0.0.3 ar-  
ea 0
```

```
PE1(config-router)#exit
```

10. Configure IBGP between PE routers. In this example the 7.7.7.7 is IP address used in the PE 2 for loopback 0 and 27 is the autonomous system number.

```
PE1(config)#router bgp 27
```

```
PE1(config-router)#neighbor 7.7.7.7 remote-as 27
```

```
PE1(config-router)#neighbor 7.7.7.7 update-source  
loopback0
```

Then tell BGP to export the routes from VRF to MP-BGP by redistributing them in to BGP. In this case since we used RIP for the customer network as a routing protocol, we redistributed it in to the BGP.

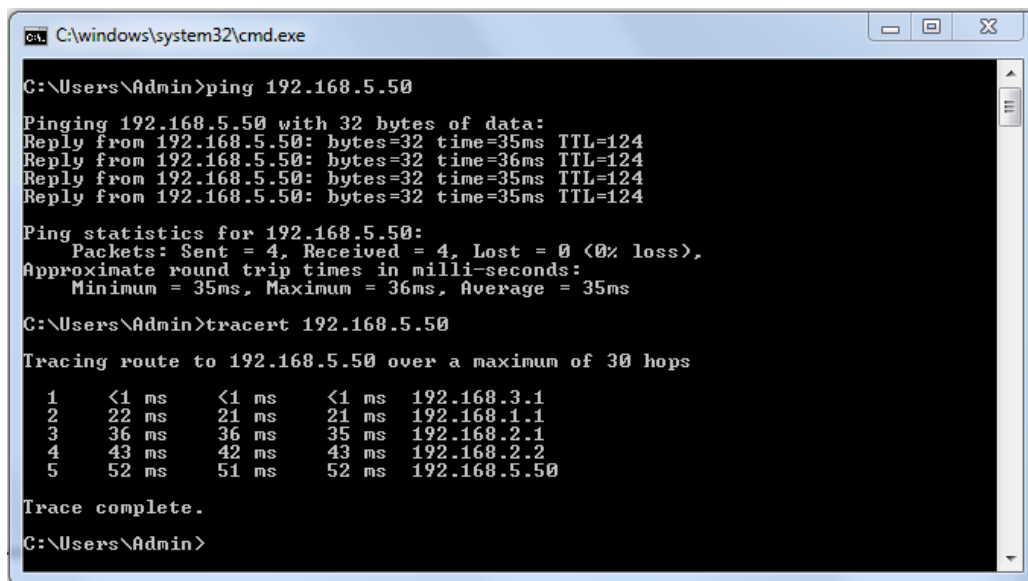
```
PE1(config-router)#address-family ipv4 vrf test  
PE1(config-router-af)#redistribute rip  
PE1(config-router)#exit
```

Finally before leaving the BGP, Configure VPNv4 capability between PE1 and PE2

```
PE1(config-router)#address-family vpnv4  
PE1(config-router-af)#neighbor 7.7.7.7 activate  
PE1(config-router-af)#neighbor 7.7.7.7 send-  
community both  
PE1(config-router-af)#end
```

4.4 Test Result

After the configuration is completed, I used the “ping” and “tracert” administration utilities to test the reachability of hosts from one end to the other.



```
C:\windows\system32\cmd.exe

C:\Users\Admin>ping 192.168.5.50

Pinging 192.168.5.50 with 32 bytes of data:
Reply from 192.168.5.50: bytes=32 time=35ms TTL=124
Reply from 192.168.5.50: bytes=32 time=36ms TTL=124
Reply from 192.168.5.50: bytes=32 time=35ms TTL=124
Reply from 192.168.5.50: bytes=32 time=35ms TTL=124

Ping statistics for 192.168.5.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 36ms, Average = 35ms

C:\Users\Admin>tracert 192.168.5.50

Tracing route to 192.168.5.50 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    192.168.3.1
  1  22 ms    21 ms    21 ms    192.168.1.1
  2  36 ms    36 ms    35 ms    192.168.2.1
  3  43 ms    42 ms    43 ms    192.168.2.2
  4  52 ms    51 ms    52 ms    192.168.5.50

Trace complete.

C:\Users\Admin>
```

Figure 10. Routers end to end connection demonstrated by ping and trace route

Figure 10 shows the screen shot taken from the “ping” and “tracert” result received from the hosts. The packet forwarding order has taken place according to the topology exhibited in Figure 7.

5 ANALYSIS

I used WireShark network analyzer to observe the forwarded packets through the MPLS network. The MPLS packet header can be studied from Figure 11.

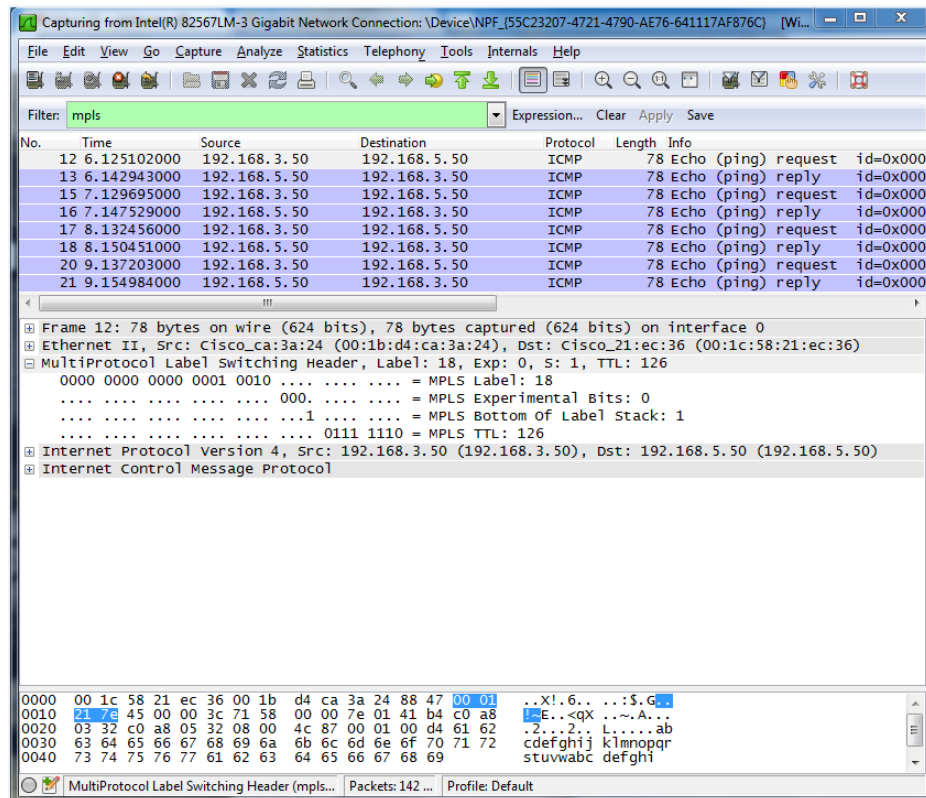


Figure 11. WireShark screenshot for MPLS packet header

The MPLS packet header lays between the Ethernet and IP protocols as it is showed in Figure 11. The packet has label 18 with an experimental bit set to 0. It is possible to have various MPLS headers to be stacked in the packet header, and the third part of the header which denoted by later “S” tells which MPLS header has showed up in the stack. Since I only have a single header for this packet, it displays “1”. The last portion states the life of the packet in the route as TTL.

Periodic Hello messages are used in the basic LDP discovery and if it has received by the other router, then it indicates Hello adjacency has been established. These messages are connectionless UDPs sent and received on port 646. Hello messages

include the common Hello Parameters which lists the limitation and Hold Time for receiving the Hellos.

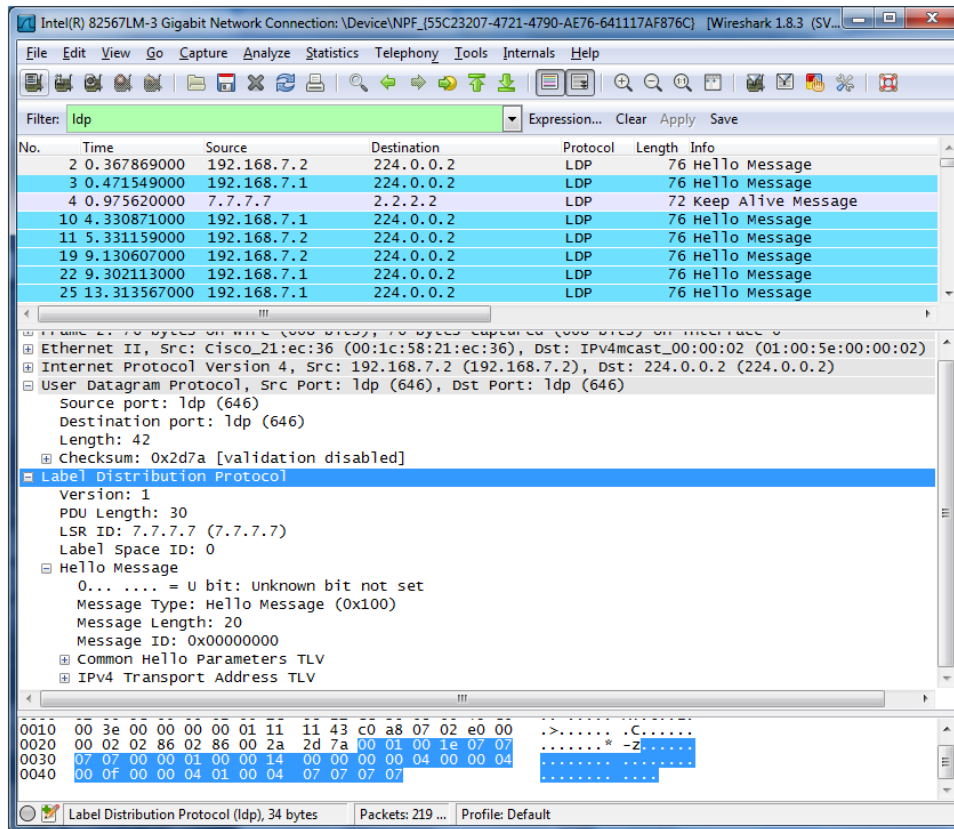


Figure 12. WireShark screenshot for LDP Hello

Figure 12 shows the LDP Hello message sent to multicast address (240.0.0.2) to all routers in the subnet. Even though there is only one router in this subnet, the sender will keep on multicasting the LDP Hello messages in the subnet for basic discovery. This label discovery protocol uses Type-Length-Value (TLV) encoding rules for all common parameters such as FEC, Label, Address list, Hop count, Path vector and Status.

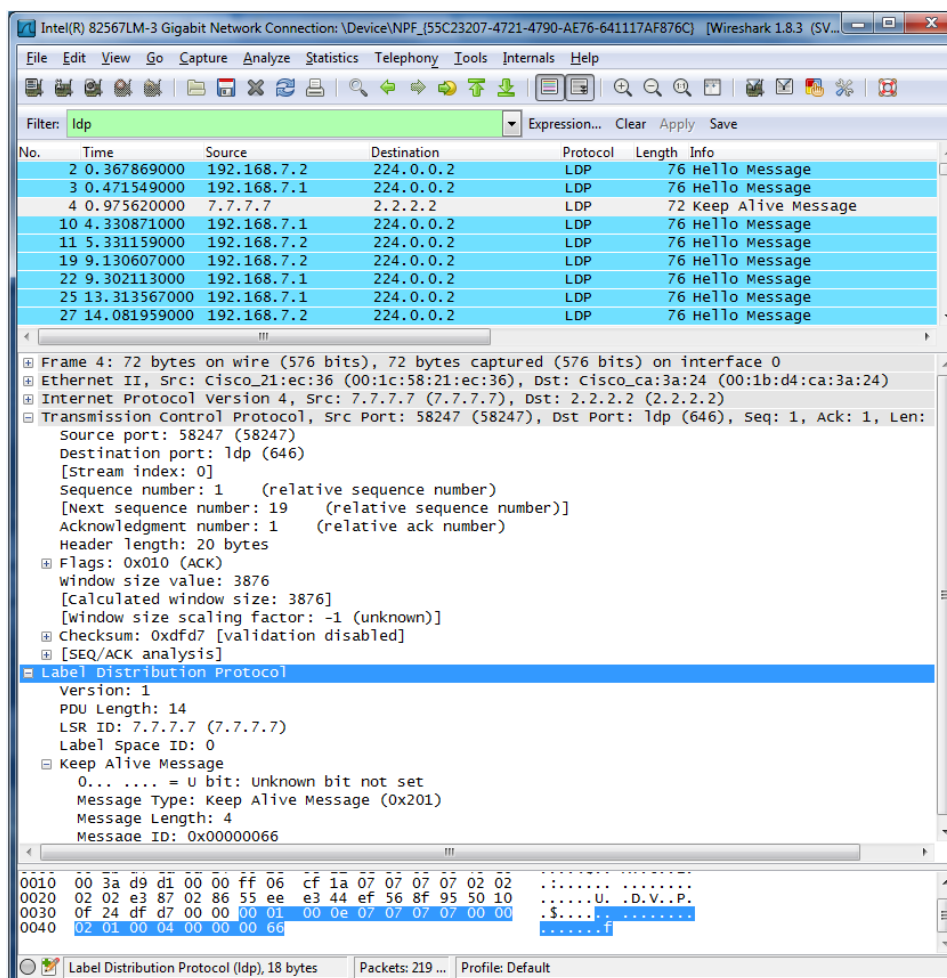


Figure 13. WireShark screenshot for LDP KeepAlive Messages

Figure 13 shows the LDP KeepAlive message from the PE1 Loopback 0 interface 7.7.7.7 (which is stated as LSR ID on the figure) to PE2 Loopback 0 address 2.2.2.2. The Hello adjacency is established by the routers when the receiver LSR accepts the initialization message sent from the other neighboring LSR. Then the receiver LSR will check if the parameters proposed in the message are acceptable. If they are, LSR replies with an initialization message of its own to propose the parameters it wishes to use and a KeepAlive message to signal acceptance of PE1's parameters /8/. If the adjacency has not been accepted, the PE2 would send **Session Reject** or **Error Notification** message instead of KeepAlive message.

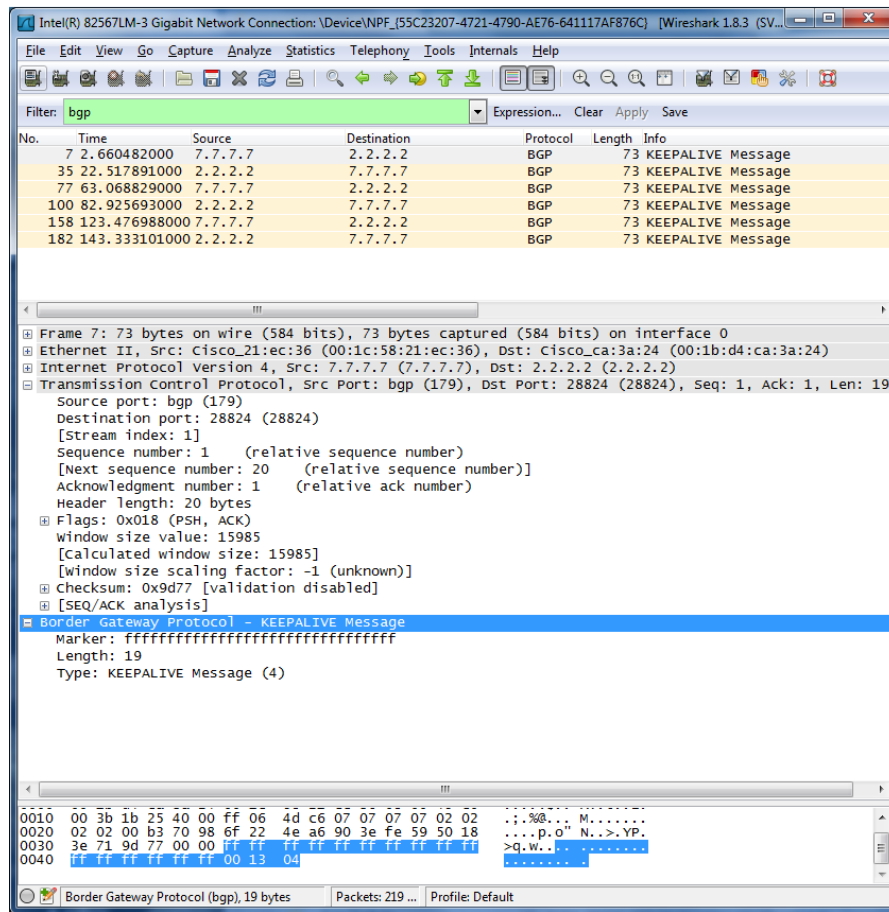


Figure 14. WireShark screenshot for BGP KeepAlive Message

The BGP KeepAlive message is exchanged periodically between peers to ensure that the connection is alive, often not to cause the Hold Timer to expire. The BGP message consists of only the message header and has a length of 19 octet /11/. In Figure 14, the WireShark captures the BGP KeepAlive exchange between PE1 and PE2 they made every other time by turn. The header consists 3 segments which are explained in Table 4:

Table 4. BGP header description

Type	Length in octet	Value in Hex	Description
Marker	16	All 'f's	Synchronizes with all ones
Length	2	00 13	The "Length" field tells the length of the BGP header which is 19.
Type	1	04	States that IPv4 has been used.

The marker in the header synchronizes the message with value of all binary "1" in the field, if the value comes other than this, it will generate error occurrence message. Errors can also be identified if the header comes with greater or less than 19 on the length field.

The LIB is the MPLS table where all the labels are kept in and "show mpls ldp binding" command displays the table. Listing 4 shows the LIB table.

```

PE1#show mpls ldp bindings

  lib entry: 2.2.2.2/32, rev 2

    local binding: label: imp-null

    remote binding: lsr: 7.7.7.7:0, label: 17

  lib entry: 7.7.7.7/32, rev 9

    local binding: label: 16

    remote binding: lsr: 7.7.7.7:0, label: imp-null

  lib entry: 192.168.7.0/29, rev 7

    local binding: label: imp-null

    remote binding: lsr: 7.7.7.7:0, label: imp-null

```

Listing 4. The LIB table

LIFB is also MPLS table that routers uses to make decision where to forward the packets using their labels. The command to display the LIFB is "show mpls forwarding-table" and the listing 5 will illustrates the table.

```
PE1#show mpls forwarding-table
```

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
16	Pop Label	7.7.7.7/32	0		Fa0/0	192.168.7.2
17	No Label	192.168.1.0/30 [V]	0		Se0/1/0	point2point
18	No Label	192.168.3.0/24 [V]	0		Se0/1/0	point2point

Listing 5. LFIB

6 CONCLUSION

The main goal of the thesis was to determine the importance of applying L3 MPLS VPNs to a traditional IPv4 network to demonstrate the advantages of the technology over the current similar services on the market. In this investigation, the aim focused on assessing the routing traffic intensely by developing a good understanding of the most important protocols which facilitate communication. As a result, I have achieved the objectives of the thesis both by studying the principles and illustrating the theory by implementing actual demonstration for further detailed studies.

Multiple protocols headers were captured in the MPLS service by using a hub in between the PE routers. Hence, I reduced the speed of the router interfaces to 10MB/S to match the with the hub capacity. For this reason the round trip for the ping became slower which contradicts with one of the benefits of the technology.

During working on the project, I have learned a lot about mainly the different natures of MPLS protocols, VPN types and security concerns and the behaviors of OSI network layers on IP routing. Though there were some limitations on the procedure, such as fewer number of routers available than the study required, I could succeed to reach the goals and equipped a way for further research corresponding MPLS TE, MPLS QoS and many more as a project for students in the future.

REFERENCES

- /1/ Rosen E., A. Viswanathan, R. Callon 2001, RFC 3031: Multiprotocol Label Switching Architecture. Accessed 28.02.2014. (<http://www.ietf.org/rfc/rfc3031.txt>)
- /2/ Puska, Matti 2010, Multiprotocol Label Switching Accessed, Metropolia University of Applied Sciences. Accessed 04.03.2014.
- /3/ What is MPLS? Accessed 12.04.2014. <http://www.mplstutorial.com/mpls-tutorial-what-mpls-multi-protocol-label-switching>
- /4/ Cisco systems, Inc. 2004, Introduction to MPLS. Accessed 13.04.2014. https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/3294-102-1-9011/cdcont_0900aecd8031205f.pdf
- /5/ De Ghien Luc, 2006, MPLS Fundamentals Accessed date 13.04.2014.
- /6/ E. Mannie, ED. 2004, RFC 3945: Generalized Multi-Protocol Label Switching (GMPLS). Accessed 17.04.2014. (<http://tools.ietf.org/html/rfc3945>)
- /7/ E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li Procket Networks, A. Conta 2001, RFC 3032: Multiprotocol Label Stack Encoding. Accessed 18.04.2014 (<http://www.rfc-editor.org/rfc/rfc3032.txt>)
- /8/ L. Andersson, Ed. Acreo AB, I. Minei Ed., B. Thomas Ed. 2007, RFC 5036: LDP Specification Accessed 20.04.2014. (<http://tools.ietf.org/html/rfc5036>)
- /9/ L. Andersson, T. Madsen 2005, RFC 4026: Provider Provisioned Virtual Private Networks (VPN) Terminology Accessed 22.04.2014. (<http://tools.ietf.org/html/rfc4026>)
- /10/ Cisco Systems, Inc. 2006, Layer 3 MPLS VPN Enterprise Consumer Guide Version 2 Accessed 25.03.2014. (http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html)
- /11/ Y. Rekhter, T. Li, S. Hares 2006, RFC 4271 (A Border Gateway Protocol 5 (BGP-4)), Accessed 25.03.2014. (<http://tools.ietf.org/html/rfc4271>)

APPENDICES

PE1 Running configuration

Building configuration...

```
Current configuration : 1878 bytes
!
version 12.4
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
vrf definition test
rd 100:1
!
address-family ipv4
route-target export 100:1
route-target import 100:1
exit-address-family
!
logging message-counter syslog
!
noaaa new-model
dot11 syslog
ip source-route
!
ipcef
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
archive
logconfig
hidekeys
!
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
```

```
interface FastEthernet0/0
ip address 192.168.7.1 255.255.255.248
duplex auto
speed auto
mplsip
!
interface FastEthernet0/1
noip address
duplex auto
speed auto
!
interface Serial0/1/0
vrf forwarding test
ip address 192.168.1.1 255.255.255.252
clock rate 64000
!
interface Serial0/1/1
noip address
shutdown
clock rate 125000
!
routerospf 1
log-adjacency-changes
redistributebgp 27
network 2.2.2.2 0.0.0.0 area 0
network 192.168.7.0 0.0.0.7 area 0
!
router rip
version 2
!
address-family ipv4 vrf test
redistributebgp 27 metric 2
network 192.168.1.0
no auto-summary
exit-address-family
!
routerbgp 27
bgp log-neighbor-changes
neighbor 7.7.7.7 remote-as 27
neighbor 7.7.7.7 update-source Loopback0
!
address-family ipv4
neighbor 7.7.7.7 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 7.7.7.7 activate
```

```
neighbor 7.7.7.7 send-community extended
exit-address-family
!
address-family ipv4 vrf test
redistribute rip
no synchronization
exit-address-family
!
ip forward-protocol nd
noip http server
noip http secure-server
!
control-plane
!
line con 0
line aux 0
linevty 0 4
login
!
scheduler allocate 20000 1000
end
```

CE1 Configuration

Building configuration...

```
Current configuration : 1192 bytes
!
version 12.4
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
!
hostname CE1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
noaaa new-model
dot11 syslog
ip source-route
!
ipcef
no ipv6 cef
```

```
!  
multilink bundle-name authenticated  
!  
voice-card 0  
!  
archive  
logconfig  
hidekeys  
!  
interface Loopback0  
ip address 3.3.3.3 255.255.255.255  
!  
interface FastEthernet0/0  
ip address 192.168.3.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
noip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.1.2 255.255.255.252  
!  
interface Serial0/1/1  
noip address  
shutdown  
clock rate 125000  
!  
router rip  
version 2  
network 192.168.1.0  
network 192.168.3.0  
no auto-summary  
!  
ip forward-protocol nd  
ip route 0.0.0.0 0.0.0.0 192.168.69.0  
ip route 0.0.0.0 0.0.0.0 192.168.69.254  
ip route 0.0.0.0 0.0.0.0 192.168.69.79  
noip http server  
noip http secure-server  
!  
control-plane  
!  
line con 0  
line aux 0  
linevty 0 4
```

```
login
!
scheduler allocate 20000 1000
end
```

CE1 routing protocol verification

```
CE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
   o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback0
R    192.168.5.0/24 [120/2] via 192.168.1.1, 00:00:00, Serial0/1/0
    192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/1/0
    192.168.2.0/30 is subnetted, 1 subnets
R       192.168.2.0 [120/2] via 192.168.1.1, 00:00:00, Serial0/1/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

PE1 routing protocol verification

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
   o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
    7.0.0.0/32 is subnetted, 1 subnets
O       7.7.7.7 [110/2] via 192.168.7.2, 01:23:01, FastEthernet0/0
    192.168.7.0/29 is subnetted, 1 subnets
C       192.168.7.0 is directly connected, FastEthernet0/0
```

PE1 vrf routing verification

```
PE1#show ip route vrf test
```

```
Routing Table: test
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
   o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
B    192.168.5.0/24 [200/1] via 7.7.7.7, 00:43:14
```

```
     192.168.1.0/30 is subnetted, 1 subnets
```

```
C        192.168.1.0 is directly connected, Serial0/1/0
```

```
     192.168.2.0/30 is subnetted, 1 subnets
```

```
B        192.168.2.0 [200/0] via 7.7.7.7, 01:19:59
```

```
R    192.168.3.0/24 [120/1] via 192.168.1.2, 00:00:04, Serial0/1/0
```

PE1 BGP verification

```
PE1#show ip bgp all
```

```
For address family: IPv4 Unicast
```

```
BGP table version is 11, local router ID is 2.2.2.2
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
r>i7.7.7.7/32	7.7.7.7	0	100	0	?
r>i192.168.7.0/29	7.7.7.7	0	100	0	?

```
For address family: VPNv4 Unicast
```

```
BGP table version is 14, local router ID is 2.2.2.2
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 100:1 (default for vrf test)					

```
*> 192.168.1.0/30 0.0.0.0 0 32768 ?
*>i192.168.2.0/30 7.7.7.7 0 100 0 ?
*> 192.168.3.0 192.168.1.2 1 32768 ?
*>i192.168.5.0 7.7.7.7 1 100 0 ?
```

PE1 LDP neighbor

```
PE1#show mpls ldp neighbor all fa0/0
Peer LDP Ident: 7.7.7.7:0; Local LDP Ident 2.2.2.2:0
TCP connection: 7.7.7.7.58735 - 2.2.2.2.646
State: Oper; Msgs sent/rcvd: 77/76; Downstream
Up time: 01:01:07
LDP discovery sources:
FastEthernet0/0, Src IP addr: 192.168.7.2
Addresses bound to peer LDP Ident:
7.7.7.7 192.168.7.2
```