Application Aware Multicasting in VPLS Networks

Allan Rwamo Kweli

This thesis is submitted in partial fulfillment of the academic requirements for the degree of

Masters of Science in Electrical Engineering

in the Faculty of Engineering and The Built Environment

University of Cape Town

December 2012

As the candidate's supervisor, I have approved this dissertation for submission.

Name: Doctor Alexandru Murgu

Signed: _____

Date: _____

Declaration

I hereby declare that: (1) the above thesis is my own unaided work, both in conception and execution, and that apart from the normal guidance of my supervisor, I have received no assistance apart from that stated below; (2) except as stated below, neither the substance or any part of the thesis has been submitted in the past, or is being, or is to be submitted for a degree in the University or any other University.

I am now presenting the thesis for examination for the Degree of MSc in Electrical Engineering. I also grant the University free license to reproduce the above thesis in whole or in part, for the purpose of research.

Allan Rwamo Kweli — 4th December 2012

Name — Date

DEDICATION

This thesis is dedicated to my parents David and Odette Musemakweli and my siblings Angelo, Adrian and Grace Kweli.

It is also dedicated to my late grandma Mrs. Norah Mitali.

ACKNOWLEDGEMENTS

I first of all thank my supervisor Dr. Alexandru Murgu for his willingness to supervise my work and the continuous support he offered me during the course of this thesis research. Thank you for your time and invaluable time and advice.

I would also like to thank members of the CRG group as well as my friends and family for your continuous support. I am also very thankful to the following individuals Cecilia A.M.N, Mark M.N, Derrick M.N Veronica S.N and Charles K.D.N for your time, sacrifices and relentless support; I'm forever in your debt.

I thank the Lord for His continuous mercy and health and may he continue blessing you all.

Abstract

Enterprise customer demand for business class Ethernet service offerings, over the years, has steadily increased. More so, the demand for high throughput coupled with efficient utilization of the available bandwidth. This has driven service providers to seek more reliable means of delivering services to their customers. As businesses expand both financially and geographically service providers have deployed Wide Area Networks (WANs) to deliver Ethernet services to their customers. However the deployment of such networks raises issues related to the cost and scalability of the network deployment. Furthermore the efficiency, in relation to resource utilization, of the network is a major concern to both the SP and the client. Ethernet services provided by a Virtual Private LAN Service (VPLS) network provide scalability, resilience and efficient utilization of the existing network resources.

The objectives of this thesis are to investigate how VPLS can offer on-demand business class Ethernet services while being consistent with the core network organization. Furthermore this research aims to develop efficient bandwidth utilization in a Point-to-Multipoint VPLS network using Multiprotocol Label Switching (MPLS) as a transport protocol. MPLS is a Layer 2.5 transport protocol that encapsulates and labels frames from their sources to their destinations. MPLS uses labels to identify the frame destination and in so doing reduces the overall bandwidth when IP headers are used. MPLS facilitates the deployment of VPLS networks, thus VPLS relies on MPLS as its transport protocol. VPLS networks offer emulated Ethernet services, are scalable and are not restricted by geographical dispersion of the customer sites. VPLS networks over MPLS also offer efficient utilization of the networks' bandwidth through mechanisms such as multicast awareness, auto-bandwidth allocation, signaling and auto-discovery.

From the mentioned mechanisms, this thesis aims at setting up a VPLS network in a virtualized environment. The reason being, it is cost effective and line with archiving cost efficiency. In the VPLS network, the preferred signaling protocol is Label Distribution Protocol (LDP) as it is essential in the establishment of the MPLS backbone network. The VPLS pseudowires are dynamically created using the Border Gateway Protocol (BGP) protocol. The BPG protocol also ensures scalability, using *route-reflect* routers in the network. The auto-discovery of peering nodes in the VPLS network is achieved using the BGP protocol. Multicast

awareness is achieved by configuring separate VPLS instances. Therefore the traffic is not flooded into the network but rather forwarded to members belonging to the same VPLS instance so the existing bandwidth is efficiently utilized. By using MPLS traffic engineered (MPLS-TE)tunnels; the auto-bandwidth mechanism is implemented. Auto-bandwidth control over the MPLS-TE tunnels ensures improved utilization of the available tunnel bandwidth.

As mentioned before, the VPLS network is in a virtualized environment. The network routers are based on the Mikrotik routerOS. The routerOS is a standalone operating system based on the Linux v2.6 kernel. The customer sites created have server and client machines, all of which have been virtualized.

List of Figures

List of Tables

List of Abbreviations

AC	Attachment Circuit; this is a virtual circuit that attaches a CE router to a PE router
AMS-IX	Amsterdam Internet exchange
AS	Autonomous Systems; is a collection of network elements under the control of one entity
ATM	Asynchronous Transfer Mode; this is an ITU-T standard
AToM	Any Transport over MPLS; is a transport technology of L2 traffic over IP or MPLS backbone networks
BGP	Border Gateway Protocol; is a protocol used for core routing in a network
CE	Customer Edge router; is a router at the customer site connected to a PE router
CSPF	Constrained Shortest Path First
FEC	Forward Equivalent Class; describes a set of packets that are bound to the same MPLS label
FIB	Forward Information Base; is a forwarding table used to match input interfaces to forwarded traffic
IETF	Internet Engineering Task Force; develops and promotes internet standards
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2VPN	Layer 2 Virtual Private Network; is a VPN network that uses MPLS labels to transport data
LAN	Local Area Network; is a network that interconnects computers on a small scale e.g. homes
LDP	Label Distribution Protocol; is a protocol that MPLS enabled routers use to exchange label mapping information
LER	Label Edge Router; this is router that operates on the edge of an MPLS network
LFIB	Label Forwarding Information Base; consists of MPLS label entries
LSR	Label Switching Router; is a router that makes up part of the MPLS core network
MP2MP	Multipoint-to-Multipoint; is a type of network element connection
MPLS	Multiprotocol Label Switching; is a mechanism based on forwarding data packets encapsulated in labels
MPLS-TE	Multiprotocol Label Switching-Traffic Engineered; this extends the core capability of an MPLS network
OSPF	Open Shortest Path First; is a link-state routing protocol
P	Provider node; is a router at the core of the MPLS network
P2MP	Point-to-Multipoint; is a type of network element connection
P2P	Point-to-Point; is a type of network element connection
PC	Personal Computer

PE	Provider Edge node; is a router that interfaces between the MPLS Provider node and the Customer Edge node.
PSN	Packet Switched Network
PW	Pseudowire; this is an emulated point-to-point connection
QoS	Quality of Service; is a network performance metric
SP	Service Provider
TLS	Transparent LAN Service; is a service that remotely links Ethernet networks
VC	Virtual Circuit; this is a communication path between network element points
VLAN	Virtual Local Area Network
VLL	Virtual Leased Lines; are a way of providing Ethernet –based point to point connectivity over an IP/MPLS network
VM	Virtual Machine; is a software implementation of a physical machine
VPLS	Virtual Private LAN Service; this is a way of providing Ethernet-based multipoint connectivity over an IP/MPLS network
VPN	Virtual Private Network; this technology offers a secure network over a public network
VPRN	Virtual Private Routed Networks; these emulate dedicated IP-based routed networks between the customer sites
WAN	Wide Area Network; this is a network that spans a large geographical area

Table of Contents

Chapter 1 Introduction

1.1 Virtual Private LAN Service Networks

Virtual Private Networks (VPNs) based on dedicated leased lines were introduced in the early 1980s. By the early 1990s, these leased lines were replaced by Frame Relay technology to deliver the VPNs. Having used Frame relay for some time the emergence of Multiprotocol Label Switching, in the late 1990s, gave rise to new types of VPNs. The following types of VPNs that were based on the MPLS technology include [**1**]:

- Layer 3 multipoint (MP) VPNs or IP based VPNs which are commonly known as Virtual Private Routed Networks (VPRN)
- Layer 2 point-to-point (P2P) VPNs that are based on Virtual Leased Lines (VLL) or Pseudowires (PW)
- Layer 2 multipoint (MP) VPNs which are also known as Virtual Private LAN Services (VPLS).

The multipoint VPNs offer a distinct single point to multiple point type of connectivity. These multipoint connections are abbreviated as P2MP. P2MP VPN connections must overcome traditional telecommunications burdens such as high setup costs, scalability and connecting geographically dispersed client sites [**2**].

The use of Ethernet switched networks allows the reliable and efficient transfer of large volumes of data over a P2MP network [**3**]. However to achieve such reliability and efficiency of the network the traditional burdens, previously presented, must be overcome. This in turn ensures the provision of high performance business class type Ethernet to the SPs clients over a Wide Area Network (WAN) [**2**].

Figure 1.1 is a global representation of VPNs based on MPLS technology. MPLS is discussed in the subsequent sections.

Figure 1.1: Global VPN IP/MPLS business network[4**]**

Figure 1.1 further illustrates the growth and expansion of VPNs that are located in major cities as of 2011 [**4**]. Companies that deploy P2MP connectivity with VPN capability to their clients include Cisco, Mikrotik, Juniper and the Amsterdam Internet Exchange (AMS-IX).

The evolution of information technology has led to the rise of larger traffic volumes being exchanged over public domains.Service providers are therefore tasked with demands for more dexterous and cost effective measures to manage the available network resourcesthey offer to their clients both private and corporate for example bandwidth.

Companies, which offer services, such as financial institutions and manufacturing plants require an exchange of information based on their different sectors. For example a multinational financial institution will have large databases of client information, global market trading transactions and these large volumes can be requested on demand by different offices around the world, as shown in Figure 1.2. Therefore the secure transfer of bulky information/data over the financial institution's SP network is vital for all involved parties.

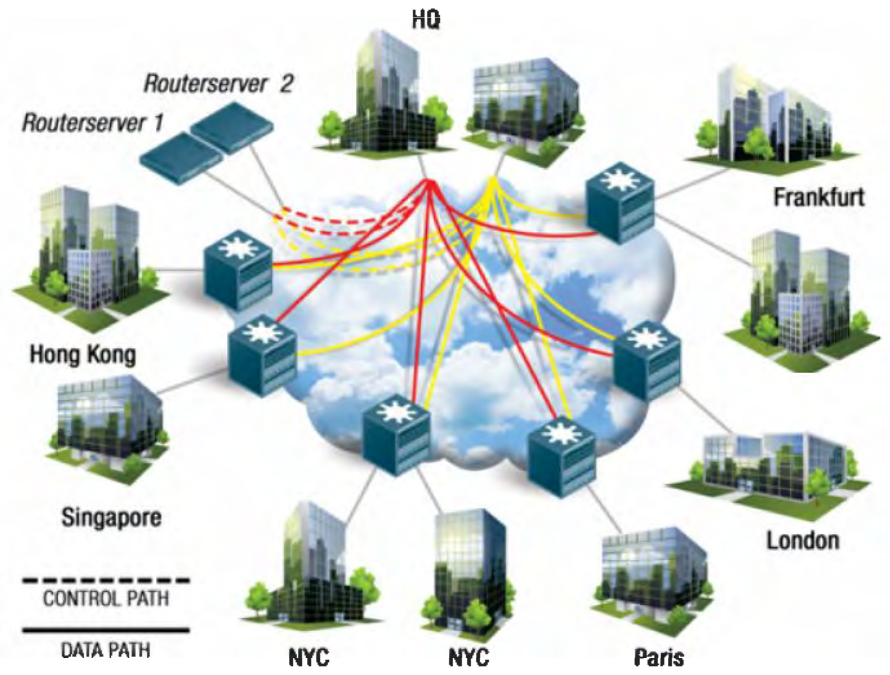

Figure 1.2:Enterprise Community of Interest Networks (CoINs) [5]

.

In Figure 1.2 above, an example of a multinational company is shown as an enterprise community sharing a common network also known as a Community of Interest Network (CoIN). An enterprise community is one that is based on common goals such as economic opportunity or community welfare.

The National Health Service (NHS) in the United Kingdom uses CoINs to meet demands for increased bandwidth to sites, control user end support and increase front line services to its various outlets [**6**].

As the number of customers requesting to manage their own private networks increases, SPs must meet these demands. Furthermore, the networks that are being setup by the SPs must be resilient, scalable and offer multi-services in order to ensure network predictability and that performance parameters are not compromised. As illustrated in Figure 1.2, connectivity services offered by SPs must not be constrained by the geographic separation of the sites.

Customers that have an exchange of information flowing or being exchanged across an Ethernet network enjoy benefits that come with using the IEEE 802.3 technology [**2**]such as:

- Easy setup and operational requirements
- Larger volume of data transfer
- Access to both Layer 3 VPN and Layer 2 MP2MP VPN services

With such benefits, the onus is on the SP to provide customers with high performance networks that ensure quality of service delivery. Ethernet service type delivery is essential and for the purpose of this research, it is important to note that it can be used to deliver L3VPN and point-to-multipointand L2VPN services [**2**].

As companies expand both financially and geographically, they request Ethernet services over MAN and WAN connections. Even though it is possible to deliver multipoint L2VPN services, it becomes increasingly difficult for the SP to guarantee connectivity over wider areas. Through the use of technologies such as IEEE 802.1q, tunneling can deliver multipoint Ethernet L2VPN service using large scale Ethernet switches. However this is not technically feasible when the enterprise sites are vastly separated, for example if one site is in Tokyo and the other in New York [**7**].

Therefore, in order to overcome the connectivity limitation brought about by geographic separation the Internet Engineering Task Force (IETF) developed mechanisms such as Internet Protocol (IP) and Multiprotocol Label Switching (MPLS).Through these mechanisms Ethernet services can be delivered to prospective clients[**2**].

To offer multipoint Ethernet connectivity to enterprise sites using transparent Ethernet segments, also known as Transparent LAN Services, Virtual Private LAN Service networks were introduced. Under VPLS multiple sites are connected through virtual Ethernet bridges using MPLS pseudowires [**2**]. MPLS as a forwarding mechanism and pseudowires (PWs) are further discussed in the subsequent chapters. Virtual Private LAN Service (VPLS) meets the demands of both the clients and service providers while being consistent with core organization of the network.

Virtual Private LAN Service (VPLS) is a Layer 2 Virtual Private Network technology that uses Multiprotocol Label Switching (MPLS) as its transport protocol to deliver Ethernet services over a Service Provider network [**8**]. This enables clients/customers multipoint access/connectivity over geographically distant areas. The multipoint nature of VPLS reduces transmission delay through directly connecting its associated clients to each other, contrast to point-to-point which makes the use of a hub to connect users[**2**].

The growth of enterprise clients switching to VPLS networks has prompted service providers to offer management solutions.Vendors offer solutions such as[**9**]:

- Cisco IP Solution Center
- Alcatel-Lucent Service Aware Manager (SAM)
- HP Service Activator Solution for VPN Services (HPSA-VPN)
- IBM Tivoli Network Manager

The consolidation of enterprise network traffic, regardless of geographical dispersion, is vital to the service provider to attract clients. Figure 1.3 illustrates the AMS-IX client base in which it uses VPLS/MPLS to interconnect customer sites that are geographically separated.

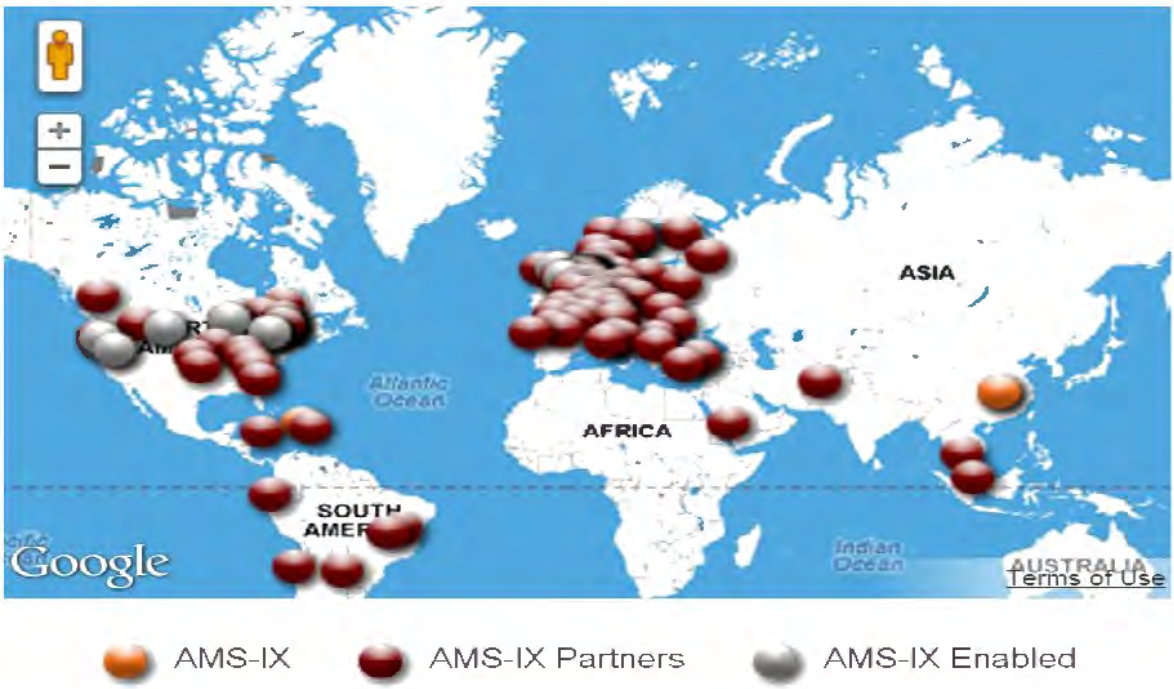

Figure 1.3: Amsterdam Internet Exchange (AMS-IX) Global Client Map [10**].**

VPLS offers an attractive business growth model to the SP as it is cost effective in terms of overall resource allocation and distribution. VPLS as a service delivery technology is not constrained by geographical separation of its subscribing clients, as illustrated in Figure 1.3, therefore both the SPs and enterprise clients would largely benefit by deploying it for service delivery.

VPLS also known as Transparent LAN Service (TLS) emulates a multipoint-to-multipoint (MP2MP) Local Area Network (LAN) connection over dispersed areas by bridging its domains over an MPLS network [**11**]. Through the emulation of a LAN connection using VPLS SPs are able to offer their clients high data throughput, synonymous with Layer 2 connections within the network. The created remote LAN segment customer sites behave as a single LAN via VPLS MP2MP interconnectivity [**12**].

As a Layer 2 VPN, VPLS enables SPs to offer L2 connectivity to their clients and not get involved in the management of routing or Layer 3 design protocols of the client [**13**]. This is an advantage for SPs offering L2 connection to clients that want to privately manage their own networks and also requiring multipoint connectivity across multiple WAN sites.

Not only does VPLS offer business class Ethernet connectivity, like WAN to its enterprise clients, it also guarantees a solution to multicasting. VPLS provides a mechanism in which multicast traffic can be transported using MPLS label switched paths (LSPs). The high data rates synonymous with Ethernet connections can be archived in a VPLS network using "Selective trees" and ingress replication of the data across network nodes, thus rendering VPLS multicast aware [**14**]. Multicast services available to clients is a significant advantage to the SP in that the network is not flooded with traffic packets to unknown destinations thereby improving bandwidth utilization within the network [**15**].

1.2 Problem Definition

VPLS relies on MPLS as its transport protocol; however MPLS relies on label distribution protocol (LDP) to set up the LSPs in which the pseudowires connecting different client sites are embedded. LDP is used for signaling purposes in the MPLS network but is not suitable in relation to peer discovery of network nodes [**15**]. Border Gateway Protocol (BGP) is not as

suitable for signaling but is the preferred mechanism for discovery of peering nodes in a network [**16**]. Both LDP and BGP can be used in the setup of VPLS networks, there is a need to understand which techniques will provide a scalable and resilient network using the signaling and discovery merits of either protocol. Therefore, based on the signaling mechanisms required in the setup of a VPLS network, this research aims to identify what combination of signaling and discovery protocols offer an efficient utilization of the available network resources.

Virtual Private LAN Service (VPLS) networks as multipoint architectures allow service providers to offer the Plug and Play option to the network. This is vital as it has low maintenance costs and a high bandwidth throughput. Through VPLS, SPs can deploy Traffic Engineering (TE) mechanisms in their networks to offer better services to their customers by improving quality of service (QoS) parameters for example delay and jitter [**17**]. Other performance metrics to be considered in the VPLS setup include [**18**]:

- Auto-discovery of the topology
- Signaling
- Pseudowire creation

As previously mentioned, VPLS is able to provide multicast services and this makes it attractive to multicast-service based entities. Multicast services such as IP TV are on the rise and it is essential for client routers to handle large volumes of multicast traffic.Thus it is important for VPLS networks supporting such services to function efficiently.

The Layer 2 nature of VPLS renders it transparent to routing protocols and offers dedicated connection to its clients participating in the same VPLS instance through pseudowires over an MPLS backbone network [**11**]. Client sites belonging to the same VPLS instance will appear as though they are connected to a single LAN. However, this is very different to the way these sites were once set up. Enterprise Ethernet LAN sites were originally connected expensively using multiple Layer 2 Ethernet switches [**19**]. With the introduction of VPLS, enterprise market drivers such as MPLS Traffic Engineered (MPLS-TE) transport tunnels offer multiservice delivery and efficient bandwidth utilization through the invocation of auto-bandwidth allocation schemes within the network.

Even though there are Internet Service Providers that offer VPLS connectivity to their client networks, a combination of mechanisms in order to effectively and efficiently utilize/establish VPLS networks is recommended. This thesis proposes/formulates research objectives aimed at ensuring the VPLS networks are scalable and offer Ethernet service to enterprise customers.

1.3 Research Objectives

In the development of the research objectives, the following key research questions are defined:

- What Signaling and Auto-discovery protocols can be used by network routers belonging to the same virtual service instance?
- How does multicast resource awareness improve network resource handling?
- How can Auto-bandwidth management be archived in a multicast aware VPLS network?

Under the stated key research questions, research objectives are considered for the accomplishment of the development and appraisal of the research project. The following techniques are implemented in order to achieve the objective of efficient bandwidth utilization within a VPLS network over an MPLS backbone network:

- Implement a Signaling and Auto-discovery mechanisms.
- Instrument Multicast optimization through ingress replication of forwarded packets.
- Implement Auto-bandwidth allocation and management of traffic within the network.

1.4 Research Scope and Limitations

This thesis explains the importance of VPLS from the viewpoint of both the customer and the service provider. It also formulates the problems in a key research question method to which key research objectives and technical solutions address the paused questions.

In the implementation of signaling and auto-discovery mechanisms of a VPLS network, only Label Distribution Protocol and Border Gateway Protocol will be used. This proposed solution is meant to illustrate the merits of using both protocols in the establishment of a VPLS network.

Having established a VPLS network with dynamically created pseudowires, this research focuses on the multicast awareness aspect of the VPLS network by transferring bulky data to sites belonging to different multicast sessions.

This research then focuses on the auto-bandwidth allocation scheme within traffic engineered tunnels. From the proposed mechanisms, this research illustrates the techniques for efficient bandwidth utilization in a multicast aware VPLS network.

1.5 Research Contribution

The contribution of this research is the practical approach in which a virtualized environment is used to setup and establish a Multicast aware Virtual Private LAN Service network. This VPLS network is based on LDP signaling, BGP peer auto-discovery mechanisms and an auto-bandwidth allocation scheme. Having a virtualized network serves both the SP and the client in regards to resource sharing thus reducing on the cost incurred while setting up a physical infrastructure.

1.6 Thesis Outline

The remainder of this thesis is structured as follows:

- Chapter 2 presents background information on Multiprotocol Label Switching and Virtual Private LAN Service networks. This chapter further discusses the features and advantages of using VPLS over an MPLS backbone network. It also discusses the advantages of using auto-bandwidth adjustment in the MPLS-TE tunnels.
- Chapter 3 defines the methodology adopted to implement a functional multicast aware VPLS network. This chapter begins by defining parameters and tools that are involved in the setup of the test bed. The VPLS test bed is planned, designed and then developed in this section. In this chapter tools like VMWare and Mikrotik routerOS v5.2 are introduced as facilitators to the realization of a VPLS network. It then proceeds into defining the planning of the test bed answering how resources are to be shared and the functionality of the different protocols to be used.
- Chapter 4 describes how the defined methodology in chapter 3 is implemented. In this chapter, the setup of a VPLS network is described beginning form how the test bed is

built up until how different protocols interact between network nodes to finally realize a functioning VPLS multicast network with an auto-bandwidth allocation scheme.

- Chapter 5 presents evaluation results based on the implemented strategy as discussed in chapter 4 through the use of Wireshark as a monitoring tool. This chapter further discusses and justifies the advantages of the VPLS network through predefined performance metrics in chapter 1.
- Chapter 6 concludes the research by presenting a set conclusions based on how well the research objectives have been answered as defined in chapter 1. This chapter then discusses recommendations for future research in the field of multicast awareness in VPLS networks.

Chapter 2 Background and Literature Review

2.1 Introduction

In this chapter the fundamentals of Multiprotocol Label Switching (MPLS), Virtual Private LAN Service (VPLS) networks and Multicasting are presented in order to familiarize the reader with the informational background of the mentioned protocols (MPLS, VPLS and Multicasting).

This chapter firstly, discusses MPLS as a transport protocol and its adaptation to VPLS networks. It then presents VPLS as a method of transparently bridging Ethernet segments between client sites. The requirements of archiving a bridged Ethernet connection between different client sites using VPLS are also presented. This chapter also provides an overview on multicasting and finally discusses how to enable multicast awareness in a VPLS network.

2.2 Multiprotocol Label Switching Protocol (MPLS)

Multiprotocol Label Switching is a mechanism in which routers add a label in front of a packet (instead of a packet header) so that other routers within the network know how to act upon the packet based on the assigned label[**20**]. The label attached to the packet is a short, fixed length, local identifier used to identify a Forward Equivalent Class, representing the FEC to which the packet is assigned [**21**].

The use of MPLS to establish virtual end-to-end connections is a driving force in its adaptation by Service Providers across networks. Previously SPs relied on manually configuring ATM VCs attached to ATM switches in which packets were forwarded based on predefined mappings thus leading to suboptimal routing. MPLS offers dynamic mapping of virtual circuits thereby improving the routing of packets within the network. MPLS further provides Layer 2 services that had previously relied only on separate networks [**22**].

MPLS, through combining L2 switching and L3 routing technologies, offers a flexible network with increased performance, stability quality of service and traffic engineering with VPLS capability [**23**]. Figure 2.1 below illustrates how a service provider connects customer A and B using an MPLS backbone network. The features/network elements are discussed in greater lengths in the sections to follow.

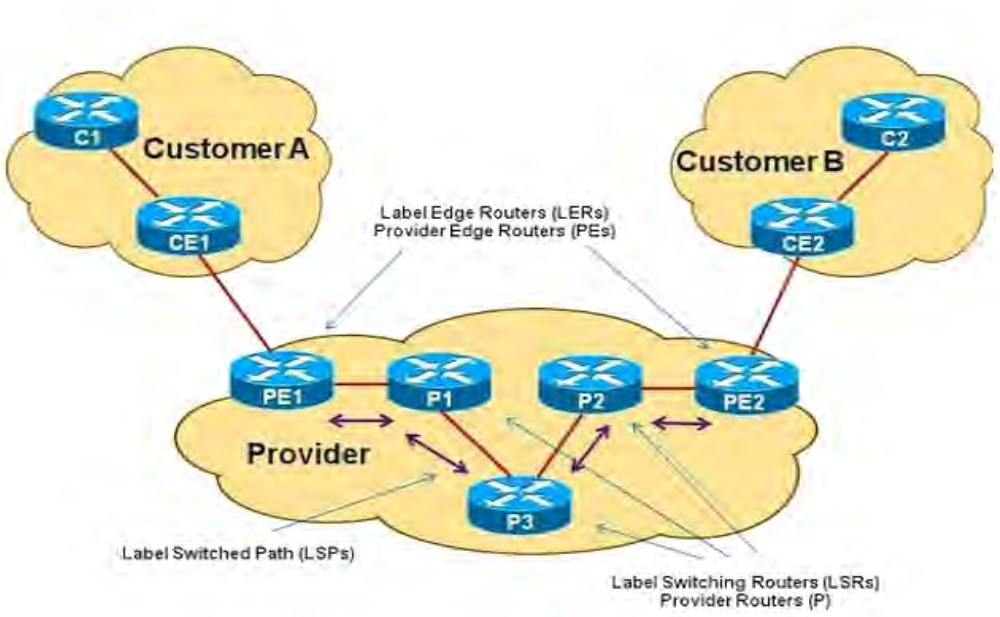

Figure 2.1: MPLS Network [24**]**

Network service providers (SPs) strive to ensure certain attributes within the network core are optimally utilized for example maximum link bandwidth, reserved/unreserved bandwidth with priority levels and traffic engineering metrics [**20**].

MPLS provides SPs with efficient utilization of their networks' resources for example bandwidth and routing optimization. Through the resource utilization techniques, MPLS is advantageous within networks for example the Traffic Engineering (TE) properties enable single or multiple paths attributes to be configured to suit the different classes of traffic traversing the network thus improving the Quality of Service (QoS) and bandwidth utilization [**23**].

As mentioned, MPLS offers traffic engineering (TE) through which traffic within the network is routed from the ingress routers to the egress routers. The MPLS-TE network routing process ensures performance optimization through providing low latency and loss rates thus efficiently utilizing network resources [**25**].

Through MPLS-TE, using MPLS as the backbone enables SPs to replicate and expand upon the networks' traffic engineering capabilities of L2 ATM and Frame Relay networks. MPLS enables traffic engineering within the network by making use of features traditionallyreserved for Layer 2 and Layer 3, thus MPLS is an integration of Layer 2 and Layer 3.

Through MPLS-TE the following can also be achieved [**17**]:

a. A one-tier network which can only be attained by overlaying a L3 network on a L2 network.
b. High transmission capacity in ISPs networks.
c. Overcome link or node failure.
d. IP routing through overcoming limitations brought upon by backbone capacity and network topology.

The following subsections discuss the fundamental elements that form an MPLS network as depicted in Figure 2.1.

2.2.1 Label Distribution Protocol (LDP) in MPLS

Label Distribution Protocol (LDP) is a signaling protocol used to distribute labels across an MPLS enabled network. LDP enables the Label Switching Routers (LSR) to establish Label Switched Paths (LSP) through mapping of the network-layer routing information to the data-link layer switched paths [**26**]. It is through the LDP protocol that the enabled LSPs provide a reliable distribution of label binding information between peering LSRs [**27**].

In the exchange/forwarding of traffic between the LSRs labels are attached to the traffic thus representing the FEC to which the packets are assigned, as previously mentioned. The LDP uses two parts of information to exchange and distribute labels:

- Label value – this is used by the receiver to encapsulate packets/frames and send them out to the egress router.
- Forward Equivalent Class (FEC) – this determines the function of the label. The label distribution is also referred to as the *FEC-Label binding* information.

The FECs in LDP are represented as IPv4 prefixes because the MPLS capable routerswere originally used to distribute IPv4 addresses [**11**]. Howeverthey can also be represented using IPv6 prefixes (RFC 4379 and RFC 6426)[**28**] and [**29**].

In LDP, the LSR makes a local decision to assign a label value to a forward equivalent class this action is known as *label binding*. However for each LSR to successfully inform its neighbors about its label bindings, the following protocols are required:

- Tag Distribution Protocol (TDP) – supports MPLS along normally routed paths
- Resource Reservation Protocol (RSVP) – supports MPLS traffic engineering
- Border Gateway Protocol (BGP) – supports MPLS VPNs/VPLS

In MPLS based networks, LDP ensures that the traffic traversing the network is assigned label values which represent the FECs of the traffic and these (label values) change across the network [**17**], this is further discussed in the following section.

2.2.2 MPLS Label Switching Routers

A router which supports MPLS is known as a Label Switching Router (LSR) [**21**]. In the MPLS structure, Label Switching Routers (LSRs) and Label Edge Routers (LERs) form the fundamental concept of MPLS, in which, LSRs and LERs must agree on the forwarding mechanism of traffic through them and between them respectively [**26**]. The LSRs and LERs use label distribution protocol (LDP) to achieve the exchange of traffic amongst each other.

In the distribution and exchange of labels, the LSR looks at the top label of the received packet and matches it to the corresponding entry in the LFIB from which it determines whether to swap, push or pop it (the label) to the next hop that the packet is being forwarded to[**30**].

In Figure 2.2,the mentioned forwarding operations performed by the LSR ensure the packets are delivered from the source to the intended destination. In the swap operation, the top label is replaced by another label. In the push operation, the top label is replaced but additional labels are pushed onto the label stack and in the pop operation the top label is either replaced with another or is removed[**30**].

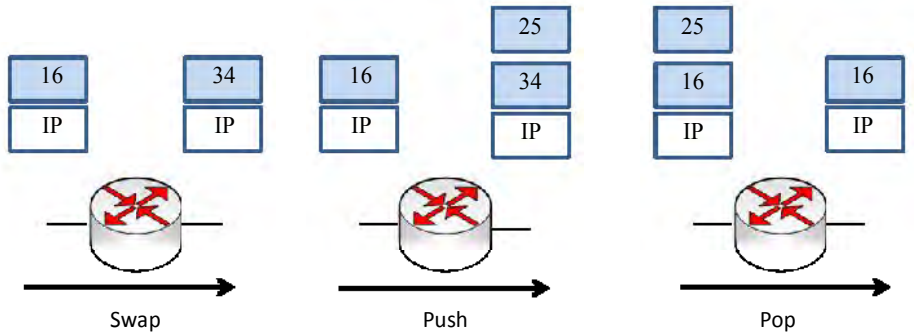

Figure 2.2: Label exchange in LSRs [30**].**

In the pop operation, the action of removing the outermost MPLS label prior to the packet leaving the MPLS environment is known as Penultimate Hop Popping (PHP) as shown in Figure2.3below. The penultimate LSR then forwards the packet to the egress router which finally delivers the packet to the egress router [**31**].

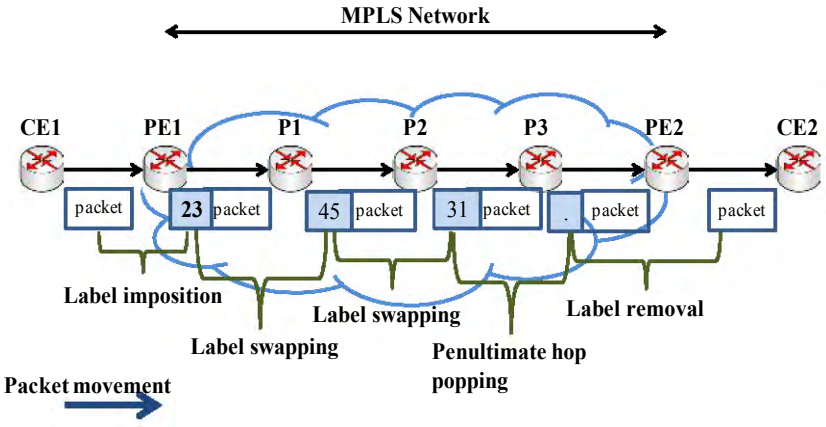

Figure 2.3: Label swapping with PHP [31**]**

RFC 3443 further suggests that an MPLS network is also configured such that the penultimate LSR is also the egress router as shown in Figure2.4

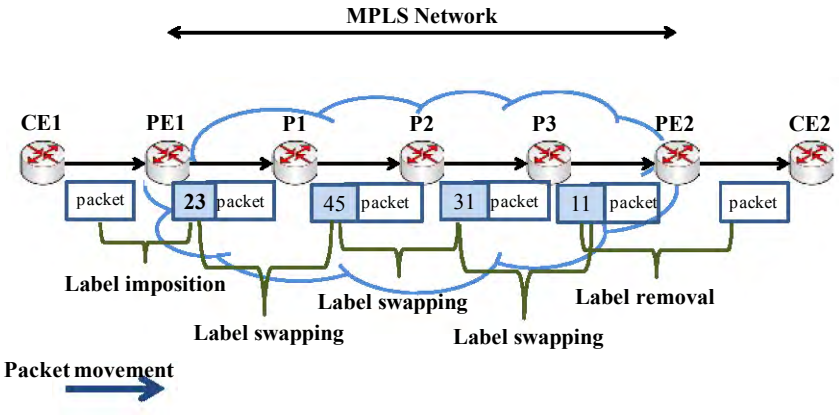

Figure 2.4: Label swapping without PHP [31**]**

Comparing Figure2.3 and Figure2.4suggests that the packet will still be delivered from CE1 to CE2 however, RFC 5462 suggests otherwise. RFC 5462, update to RFC 3443, stipulates that having a penultimate LSR before the egress router will lead to the packet being dropped early i.e. before getting to router CE2 as depicted in Figure2.3.

2.2.3 MPLS Label Switched Paths

In the MPLS-TP (transport profile), a Label Switched Path is a path in an MPLS network setup by signaling protocols such LDP and is based upon the FEC exchanges between the LSRs. MPLS LSPs have the following characteristics [**32**]:

- They are traffic engineered
- They are point-to-point (P2P) or point-to-multipoint (P2MP)
- Are established and managed in the control plane
- Support 1+1, 1:1 and 1:N protection functions

The created LSPs can be used to modify assigned network resources like bandwidth or support specific QoS guarantees and traffic engineering objectives [**33**].

MPLS uses the Label Switched Paths (LSPs)to set up links that are used to carry traffic across the network to different clients[**34**]. The setup links are also known as MPLS-Traffic Engineering tunnels [**35**]. During the setup of unidirectional and bidirectional label switched paths within the network, signaling starts at the ingress router (LSR) to the egress router (LSR). The ingress LSR initiates the signaling and the egress LSR learns the LSP as described in RFC 3209 and RFC 3473.

2.3 Virtual Private LAN Service (VPLS) Networks

Virtual Private LAN Service (VPLS) also known as Transparent LAN Service and Virtual Private Switched [**36**] is a multipoint-to-multipoint Ethernet bridging service over a Multiprotocol Label Switching (MPLS) backbone [**11**]. VPLS emulates an Ethernet LAN service in such a way that the SPs clients appear as if they are on a single LAN, but they (customers) are however spread across a wide area.

Service providers with an existing MPLS backbone network offer an improved delivery of services to their clients. The MPLS backbone is complemented by the existing Layer 3 VPN routing technology [**11**]. As a Layer 2 technology, VPLS provides two applications from the customers' point of view[**37**]:

- Provides LAN connectivity to its routers i.e. LAN routing application
- Provides LAN connectivity to its Ethernet switches i.e. LAN switching application

By using MPLS as its transport protocol, VPLS ensures an optimized quality of service (QoS) delivery through MPLS-TE [**38**].

The possibilities of using VPLS include:

- High throughput: Ethernet can provide up to 900Gbps. For example the Amsterdam Internet exchange (AMS-ix) provided peak traffic of over 920Gbps in traffic within their VPLS networks [**10**], as illustrated inFigure 2.5.

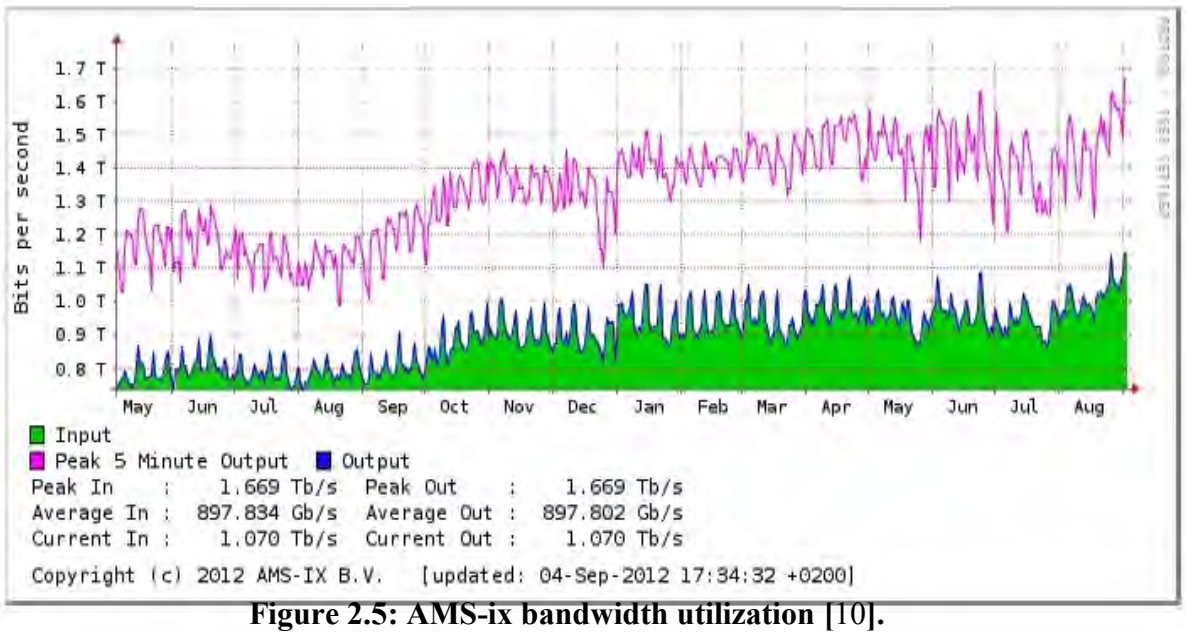

Figure 2.5: AMS-ix bandwidth utilization [10**].**

- Ethernet has simple and well known switching techniques for example Plug and Play, which are extended to VPLS [**39**].

- MPLS traffic engineering, (MPLS-TE), can support reliable QoS end-to-end (RFC 4762, RFC 4105), to facilitate efficient use of network resources.

- Emulating a bridging domain to connect multiple geographically separated sites [**15**].

- Architectural simplicity to the service provider (SP): The SP provides Layer 2 resource connectivity to the enterprise clients who will themselves govern the design of their IP and routing protocols [**11**].

- Takes advantage of MPLS' network characteristics, i.e. maintaining the resilience and scalability, while being consistent with the core network organisation [**36**].

The functions of the LER and LSR are to encapsulate/decapsulate and forward the frames, respectively, with dynamic labels in this particular instance as shown in Figure8. VPLS relies on MPLS as a transport protocol. However it has its configuration setup that occurs at the LER nodes of a network running MPLS which is explained in subsequent sections.

When configuring VPLS instances, the following are core requirements namely [**36**], [**15**] and [**40**]:

a) MPLS core. The routers in the core network known as "Label Edge/Switching Routers" LERs/LSRs are responsible for the encapsulation/de-capsulation and switching of labels on frames traversing the MPLS network between VPLS sites
b) Provider Edge Router (PE), encapsulates the Ethernet frames into MPLS, forwards packet to outgoing interface and vice versa. It is located at a service provider's network and is connected to a customer edge (CE) router directly. PEs are capable of running signaling and routing protocols for Pseudowire (PW) setup.
c) Pseudowires (PW), bi-directional in nature and consist of a pair of uni-directional MPLS Virtual Circuits (VCs).
d) Customer Edge Router (CE), Provides an Ethernet interface between the customer's LAN and the provider's core network. CEs are VPLS-unaware and are placed at the customers' premises.

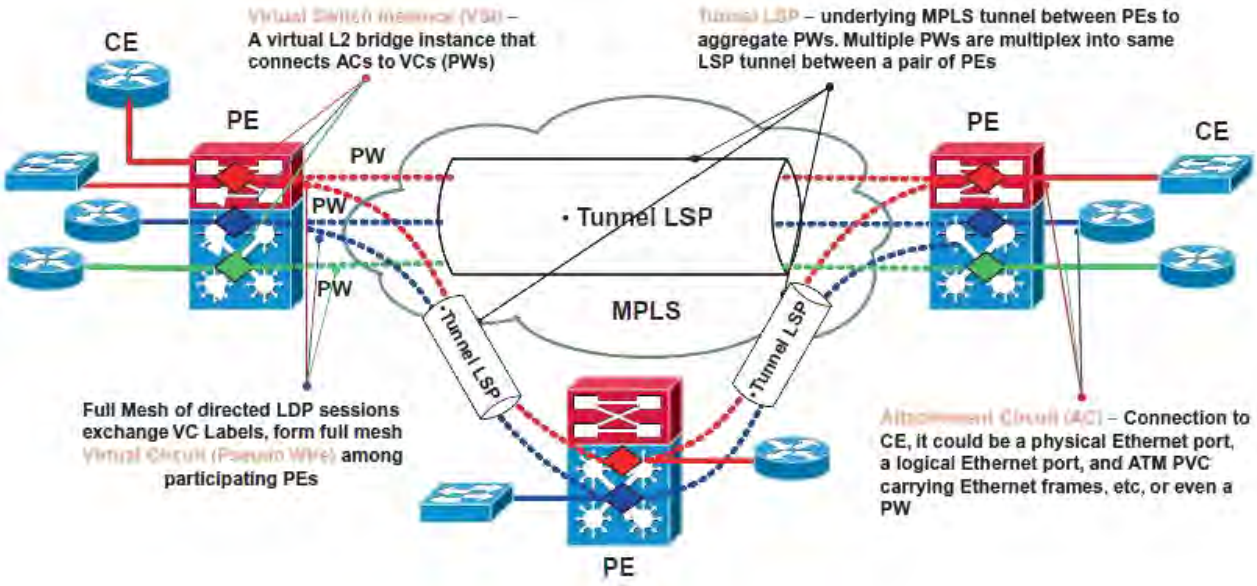

Figure 2.6: VPLS network [41**]**

A VPLS network uses MPLS as its transport protocol however it has its own control plane. The VPLS control plane has two primary functions: auto-discovery and signaling[**33**]. The mentioned functions of the VPLS control plane enable the auto-discovery of client-member sites i.e. belong to a similar VPLS instance and the setup and teardown of pseudowires (PWs) also known as signaling [**36**].

In VPLS, discovery means the process of identifying provider edge nodes that are participating in the same VPLS instance. The use of protocols by PEs to discover other PEs is known as auto-discovery. PEs can also be configured with the identities of other PEs in the same VPLS instance this however presents a tedious job of manually configuring PE neighbors to the service provider when and if there are multiple PEs joining and leaving the VPLS instance [**36**].

In the auto-discovery method, the Border Gateway Protocol is used to configure PEs with only the information of which VPLS instance they belong to rather than the identity of all other PEs. In case there is a PE joining or leaving the rest of the remaining PEs, in the same VPLS instance, are not affected in regards to configuration changes and the VPLS network topology automatically reconfigures to accommodate the new or withdrawn PEs [**33**].

2.3.1 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is an inter-autonomous routing system/protocol that is used for TCP/IP internet community. BGP is used in the design and administration of large networks thereby ensuring scalability of the network [**42**].

BGP configured PEs do not exchange information on the networks' topology but rather the reachability of neighboring peers; this is because the BGP protocol is based on a distance-vector algorithm [**43**]. The inter-autonomous systems are networks residing in Autonomous Systems (AS), thus these networks are able to communicate and exchange routing information with other networks homed in other autonomous systems using the Border Gateway Protocol (BGP) [**20**]. An autonomous system is thus one in which a group of routers is under the same administration although they (routers) may have different interior gateway protocols (IGP) [**44**].

As the meshed network expands, it presents a problem of scalability. However BGP employs the use of route reflectors to counter the problem of scalability. The notion behind the use of route reflectors is to configure strategically placed routers/IBGP speakers as *concentration routers* or *route-reflectors* as shown in Figure2.7 (b) below [**20**].

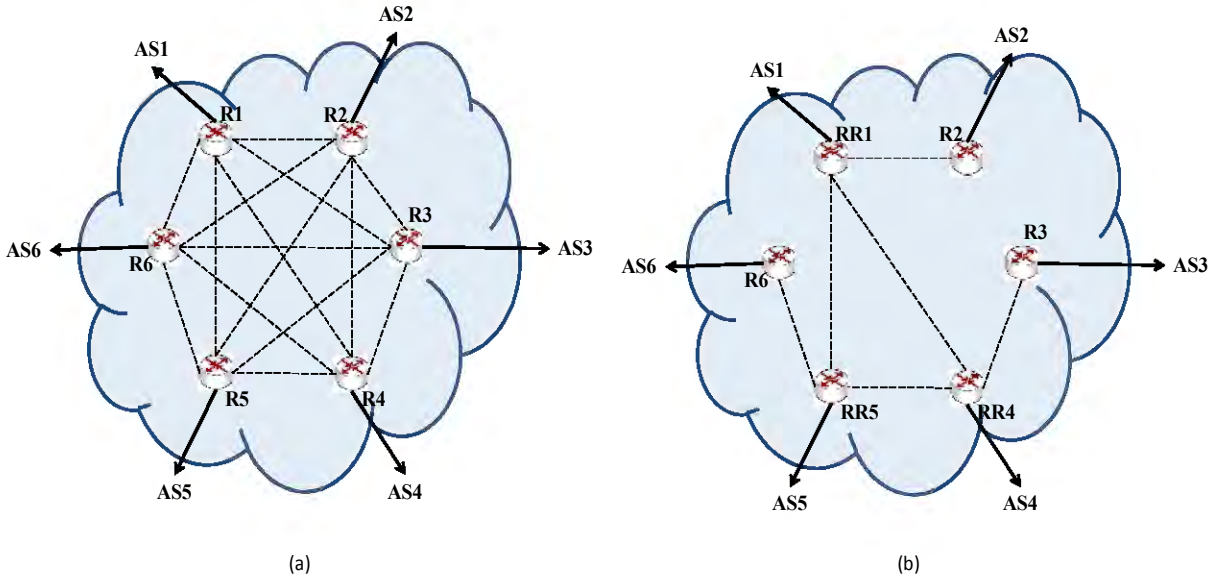

Figure 2.7: Border Gateway Protocol [20]

In Figure 2.7, routers R1, R2, R3, R4, R5 and R6 are referred to as Internal BGP (IBGP) speakers because they are peers in the same autonomous system (AS). AS1, AS2, AS3, AS4, AS5 and AS6 are external autonomous systems linked together by their respective routers. In comparison, Figure 2.7(a) will have a scalability problem as the number of routers increases. The reason being each router needs to learn the information about its peers in its AS, but in Figure 2.7(b) scalability has been improved due to the use of route reflectors.

During the exchange of information, there are rules that govern the way routing information is passed on while using route reflectors in Figure 2.7(b) [**20**]:

- An announcement from a route reflector will be sent to the other route reflectors i.e. RR1 will send information to RR4 and RR5 and this will then be sent to clients R3 and R6 respectively.
- Information received from a route reflector client is sent to the other routers through their respective route reflectors i.e. information from R2 is sent to R3 and R4 via RR4 and RR5 respectively.
- External IP prefixes from other autonomous systems are sent to the other routers through their route reflectors i.e. information AS2 is sent R3 and R6 through RR1 and then RR4 and RR5 respectively.

Advantages of using a route reflector include:

- Simple – the configuration of having concentrated routers from which other routers learn peer information of routers in the same AS [**42**].
- The ease of transition from a full-mesh network without having to change the network topology as proposed in RFC 3056 although has been updated to RFC 5056 [26, 27].
- The *route-reflect* mechanism allows for non IBGP members to stay as part of the initial autonomous system thereby being compatible to the network [**42**].

2.3.2 LDP-VPLS

Provider edge nodes are setup using the LDP protocol to ensure the signaling and establishment of pseudowires that constitute the VPLS network. Having setup the pseudowires, LDP further ensures that there are tunnels present to deliver the traffic over them (PWs) [**15**].

Label Distribution Protocol is suitable for signaling purposes during the setup of an LDP-VPLS network.However unlike the Border Gateway Protocol it sets up a fully meshed network without the option of route reflectors. The duty of the service providers is to ensure that the network is scalable and loop free.

Scalability and loop avoidance in the VPLS network ensures the integrity and proper use of resources available in the network to both the clients and service provider, this is applicable and must be addressed in both the BGP based VPLS and the LDP based VPLS.

As discussed in the BGP section above, the issue of scalability is dealt with by having route reflectors within the VPLS network [**36**]. In LDP, scalability is addressed by matching the Provider-VLAN (P-VLAN) to a VPLS instance after which the P-VLAN is set with a delimiter. The P-VLAN then acts as a local delimiter within the providers' network. However, this delimiter is stripped before being mapped onto the PWs in a VPLS instance. The limit only applies to Ethernet islands which are linked together over the service providers' MPLS core. Therefore, the number of Ethernet islands dictates the number of VPLS instances [**15**].

In the case of loop avoidance, since there is a fully meshed network of PWs attached to PEs, using the "split horizon" rule is essential. In the "split horizon" rule, PEs can only send/forward traffic to only one PW within the same VPLS instance. This rule applies to both the BGP and LDP based VPLS networks [**36**]and [**15**].

2.3.3 Pseudowires

A Pseudowire (PW) is a point-to-point connection between two provider edge routers [**33**]. The provider edge (PE) routers are connected to attachment circuits that are used to carry frames from the CE to the PE whereas the pseudowire carries the frames between the connected PEs [**45**]. Pseudowires are also interpreted as label agreements by two communicating provider edge routers [**11**].

Pseudowires link attachment circuits (ACs) thereby enabling the transfer of information between them. The attachment circuits (ACs) may comprise of Ethernet ports, MPLS label switched paths, PPP sessions from a Layer 2 Tunneling Protocol (L2TP) and many more [**33**]. PWs enable the emulation of Layer 2 services over an MPLS based network by encapsulating the

Layer 2 Protocol Data Units (PDU) and sending them across the network in the PW. Pseudowires are also used to deliver low-rate Time Division Multiplexed and Synchronous networking circuits over the MPLS based network [**46**]. Figure 2.8 below shows the emulation of a Layer 2 service (Ethernet service network) over an MPLS enabled network

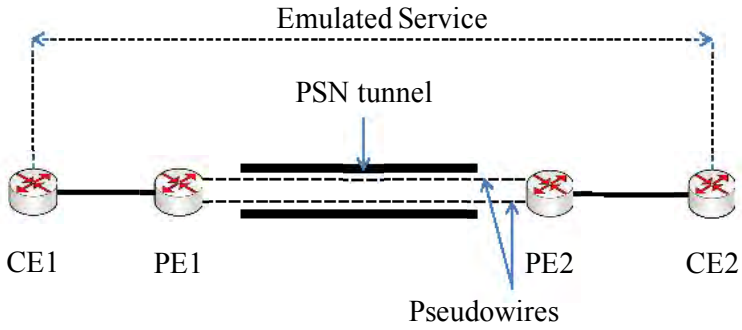

Figure 2.8: Pseudowire link[46**]**

The pseudowire mechanism enables the transfer of essential elements that constitute the emulated service between provider edge nodes in a packet switched network (PSN) as shown in Figure 2.8 above. Pseudowires are deployed for example when a service provide is transferring from their Layer 2 VPN (L2VPN) service to a PSN whilst keeping the integrity of the network topology [**47**].

The deployment of pseudowires is not restricted to only one domain, i.e. to only one service provider, but also to multiple domains thereby traversing different autonomous systems through targeted LDP sessions [**47**]. In a PSN tunnel the different PWs are identified using an MPLS label which is a multiplexing field and the encapsulation in the PWs is identified by the IETF Pseudo-Wire Encapsulation Edge to Edge (PWE3) working group [**33**].

Pseudowires can be setup using either the Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP):

a. In BGP, the pseudowires are setup after the discovery has been completed. Once the peering PE nodes have been discovered, they exchange demultiplexors that distinguish the type of traffic being carried over the tunnel. This process is known as signaling. BGP peering nodes send a single Update message containing the demultiplexors to the route

reflectors that relay message to other PEs thus reducing the load on the control plane [**36**].

b. In LDP, the pseudowires are setup by establishing a full mesh of LDP sessions between the LDP peering routers. Because there is a need of a full mesh of LDP sessions, this increases the number of target sessions thus increases the load in the control plane. The pseudowires are then created over the established LDP sessions [**15**].

Having setup the pseudowires, the VPLS network elements i.e. PE routers are expected to deliver services such as broadcasting and multicasting to users, exchanging information, maintaining high levels of quality of service (QOS) while efficiently utilizing the network's resources for example bandwidth.

2.4 Multicasting in Virtual Private LAN Service Networks

The growing commercial need of multicast based VPLS services such as multimedia real-time delivery require more efficient support from the previous VPLS deployments. As multimedia traffic increases, VPLS network service providers strive to guarantee better quality of service provision to their corporate/commercial clients [**12**].

In a network routers are responsible for the distribution and the replication of information that is traversing the network routes. To efficiently distribute and deliver traffic to its respective user's multicasting only replicates data to its intended clients. The benefits of multicasting to its users include [**41**]:

- For the SP, it improves the network scalability
- Offers enterprise friendlyservices such as Virtual Multicast Networks
- Offers transparency of the SP's network
- Reduces control and data plane computation costs across the networks' routers since the replication occurs only at the ingress node
- Improves the networks' bandwidth utilization. Only the clients subscribed to a multicast group receive the data therefore flooding the network with traffic not intended for every client is minimized.

Examples of multicast traffic include:

- IP-TV which is currently on the increase
- IP surveillance systems
- Interactive gaming
- Video conferencing both commercial and non-commercial
- Real time data delivery for example corporate financial statements, stock exchange share price changes
- E-learning i.e. distance learning and white-boarding solutions

The multicast traffic is real-time on demand therefore the quality of service (QoS) delivery is paramount to its users.

2.4.1 Ingress replication

Multicasting relies on ingress replication in which the forwarding packets from the source are multiplied at the ingress PE router [**12**]. The VPLS networks rely on the use of ingress replication to deliver frames to egress routers. The multicast frames sent over the VPLS network may use more than one PW but the relationship between the ingress and egress routers is regarded as a point-to-point [**45**][**29**] or point to multipoint. The provider edge router uses the frames' Layer 2 header to attain the addressing information of the egress router.

Furthermore, the relationship between a provider edge and a customer edge router in a VPLS environment is that only allows for a single CE to transmit to multiple CEs [**45**].In ingress router replication multiple copies of the same data is flooded into the network. This is shown in Figure 2.9, the consequence of this causes inefficient utilization of bandwidth utilization and low scalability in an expanding network [**48**].

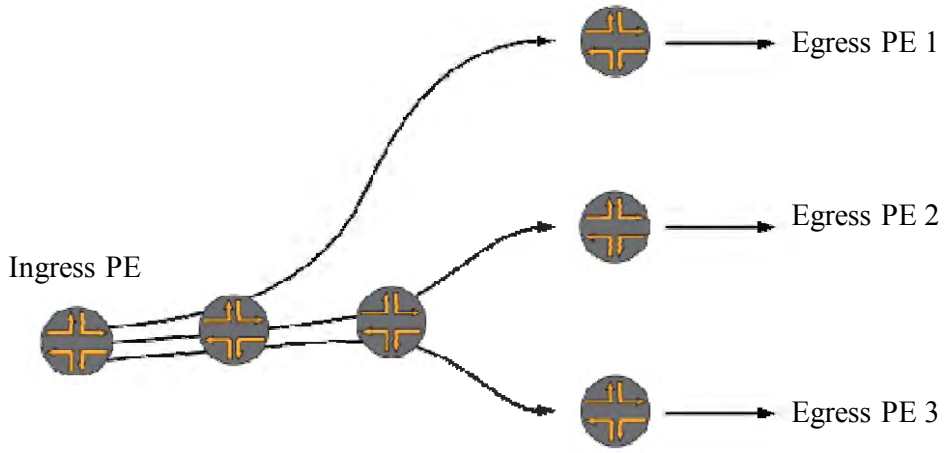

Figure 2.9: Ingress Replication[48**]**

However while using P2MP label switched paths only one single data or Ethernet frame is forwarded to the next router by the ingress router. Figure 2.10 illustrates how VPLS can offer a P2MP service in which the replication only occurs closer to the egress routers and not at the ingress router.

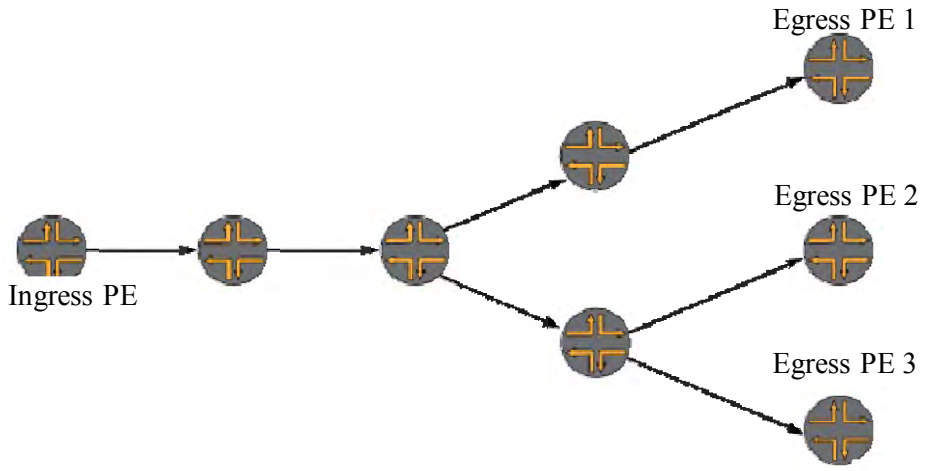

Figure 2.10: Point to Multipoint Ingress Replication[48**].**

With P2MP ingress router replication as shown in Figure 2.10, by moving replication point closer to the egress routers this improves on the utilization of the available network bandwidth [**48**].

2.5 Auto-bandwidth Management

The management of bandwidth in a network can be done manually or automatically. By using the manual adjustment of the reserved bandwidth in a network, may lead to some inconsistencies especially depending on the applications that are sensitive to fluctuations in bandwidth adjustment. For example voice application requires a dedicated/non-interrupted service end delivery therefore the bandwidth management scheme in place must ensure that adjustments do not interrupt the flow of traffic in the network [**49**].

The manual adjustment of bandwidth is based on using offline calculations of the traffic where the reserved bandwidth is set after analyzing the used bandwidth over a long period of time. The analyzed bandwidth is then averaged and a new reservation limit is setas shown in Figure 2.11.

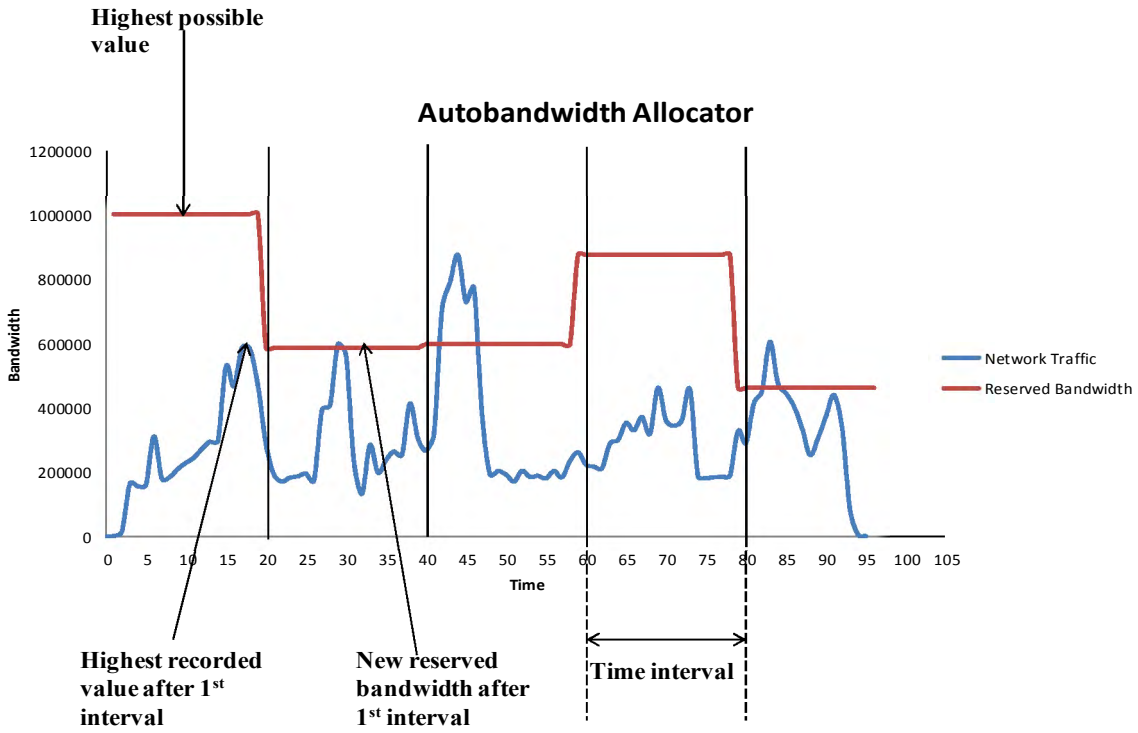

Figure 2.11: Bandwidth Adjustment using Offline Calculation

Using offline calculation to manage the bandwidth allocation presents a problem of either under assignment or over assignment of the bandwidth thus not efficiently utilizing bandwidth as

a resource as shown in Figure 2.11. Therefore there is a need to use an automatic bandwidth allocator that will respond to traffic variations and optimally utilize the available bandwidth [**50**].

Auto-bandwidth management is an administrative scheme in which service providers control the networks' bandwidth to ensure that it is efficiently utilized amongst its clients. Router vendors (for example Cisco, Juniper and Mikrotik) provide auto-bandwidth to clients on an MPLS supported network. In Mikrotik MPLS enabled routers, the LSPs created exploit the MPLS-TE property to manipulate and adjust the amount of data traversing the tunnel [**51**].

The automatic allocation bandwidth in MPLS tunnels is based on prior statistics of the volume of traffic that traverses the networks' tunnels. In the setup of an LSP's bandwidth allocation, it (LSP tunnel) is configured with minimal reserved bandwidth. The reserved bandwidth can then be either manually or dynamically adjusted based on traffic patterns in the LSP [**49**].

Benefits of using the auto-bandwidth approach to adjust traffic rates in the LSP include [**50**]:

- Offline calculation doesn't support real-time traffic adjustment, therefore may result to either over/under assignment of bandwidth to the LSP.
- Reduced delay in bandwidth adjustment
- Allocated bandwidth is optimally utilized given the shorter adjustment period for the LSPs' reserved bandwidth.

2.6 Summary

This chapter presented the background information on specific aspects of MPLS, Multicasting and Auto-bandwidth management of VPLS networks. The focus is placed on how VPLS networks may be developed to ensure they are multicast aware. The development of application aware multicasting in VPLS networks is intended to achieve efficient use of bandwidth as a resource within the VPLS network.

As discussed, VPLS is a Layer 2 technology that uses MPLS as its transport protocol. An overview of MPLS is presented explaining the key features and aspects that make up a VPLS

network for example LERs and LSPs. The advantages of using MPLS as a transport technology are also inherited by the VPLS networks thereby ensuring resilience and scalability within the network.

The process of ensuring efficient bandwidth utilization within VPLS networks doesn't stop at ensuring the network is multicast aware but also involves techniques like propagating advantages of the underlying mechanisms being used to setup the VPLS network. MPLS-TE is one such mechanism in which the use of the multiple-timers provides Auto-bandwidth management within the network. BGP and LDP protocols are used to provide signaling and auto-discovery techniques. The Split-horizon aspect of BGP ensures multicasting. MPLS provides scalability and resilience of the network. The mentioned advantages of these technologies can be propagated within the network thereby guaranteeing QoS across the customer enterprise network. In Chapter 3, the above mentioned techniques and technologies are used in the design implementation of the VPLS network platform.

Chapter 3 Resource Splitting Design

3.1 Introduction

Resource splitting in this instance entails the distribution of the test bed network elements (e.g. routers, clients and servers) amongst the available different physical components. Three physical Windows XP machines are used to create virtual machines which are then converted into network elements. The physical hardware of these machines, such as network interface cards and the RAMs, are shared amongst the created virtual machines. The virtual machines are assigned optimal resources to guarantee their functionality.

The proposed resource splitting design of the multicast aware VPLS network is presented in this chapter. Resource splitting steps aimed at building a functional multicast aware VPLS network include: Multiprotocol Label Switching protocol, Virtual Private LAN Service and Pseudowires. The mentioned actions/functions form the core of the VPLS network.

Multicast awareness aspects, for example ingress replication and resource discovery are aimed at improving bandwidth network utilization. In this chapter, design assumptions proposed while setting up the network are brought forward, followed by an introduction to implementation techniques of the network core. The proposed setup of the transparent LAN service between client sites to emulate an Ethernet LAN network with multicast session awareness is also presented.

3.2 Design Assumptions

The following network properties were assumed

i. VMware Workstation 7.0 is only used to create virtual machines to be used as network elements which can access the pooled physical machines resources like memory through the hypervisor.
ii. Network provider nodes i.e. routers are configured using MIKROTIK^{TM} routerOS v5.2. Furthermore, MIKROTIK^{TM} routerOS v5.2 running the network routers is specifically used to configure MPLS, VPLS and routing protocols (IP loopback and OSPF). The customer end machines i.e. clients and servers are configured with WINDOWS XP SP3.

iii. Within the network, MPLS-TE is used for the bandwidth management and the invocation of auto-bandwidth timers within the LSP. The network security for example firewall settings are not taken into consideration.

iv. The VPLS network is based on an MPLS backbone and the peering between provider edge nodes is achieved through using the Border Gateway Protocol (BGP).

3.3 Design Topology

Prior to setting the test bed, an analysis of the configurable hardware is undertaken to ensure an appropriate environment is achieved. This means the formulation of a network in which the available elements are organized in a manner that will facilitate the realization of a Multicast aware VPLS network.

In setting up the test bed platform, there was a consideration of using physical hardware from which the network elements would be configured. However this wasn't an economic choice as the amount of physical components required were deemed non-cost effective, therefore the use of virtual machines running on three physical Windows XP machines was considered as a relatively more effective choice.

3.3.1 Network Setup

Having identified the three physical machines that will host the network elements, the VMware hypervisor is installed on them. Creating the network elements also entails deciding those to be used as customer nodes or service provider nodes. The customer nodes comprise of servers and clients while the service provider nodes contain provider edge, provider and customer edge routers.

Due to the configuration nature of the network test bed elements, the tasks will be divided into the three most significant requirements needed to achieve a transparent LAN service between the participating customer sites. The three configuration tasks are: MPLS invocation, VPLS instance client site participation and pseudowire formation.

Figure 3.1 shows the test bed based on an MPLS core, 3 VPLS sites and the respective client/server sites. In this case, the assumption is that of a company with three different sites of which site 1 and site 3 are hosting a real-time communications server and a database server respectively. Within the sites, there are client edge (CE) routers denoted by letters A and B which correspond to the end users (clients) of either the real-time server (A) or the database server (B).

The MPLS core is comprised of provider edge (PE) routers and provider (P) routers. The PE and P routers are Mikrotik routers with MPLS capability with which the VPLS network and instances are configured. The configuration of the VPLS network in Figure 15 is detailed in later sections of this thesis.

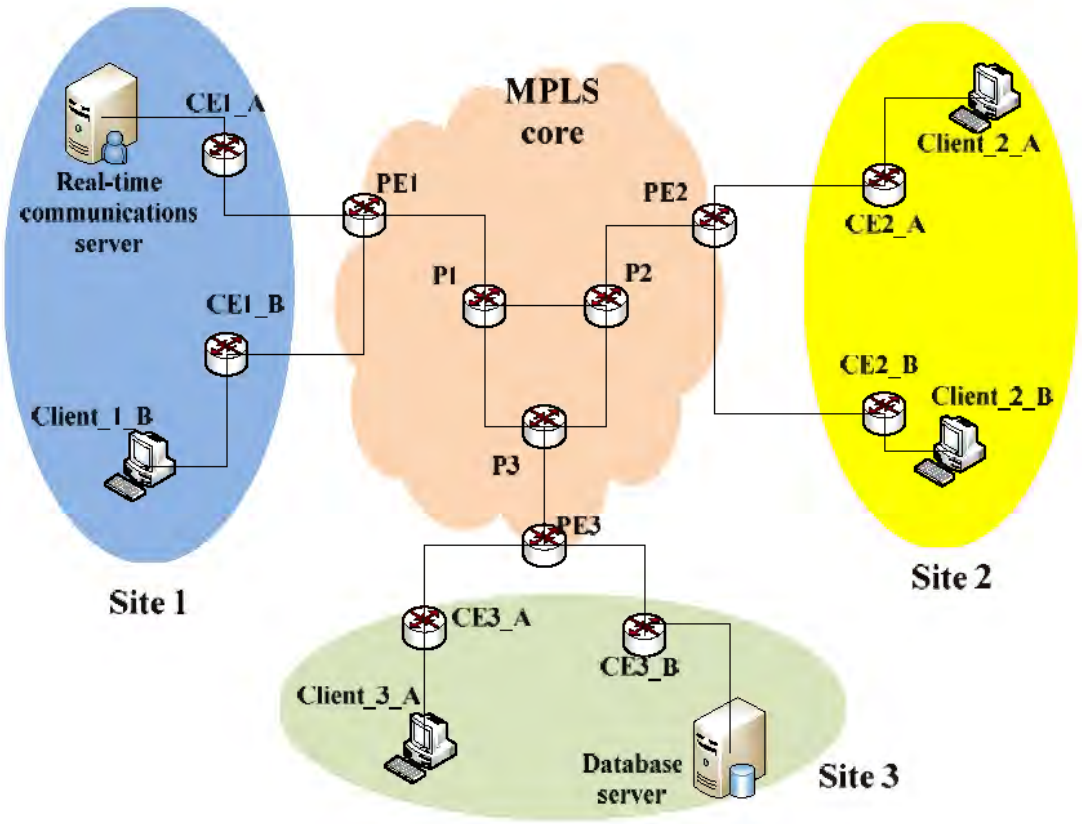

Figure 3.1: Network Setup

3.3.2 VPLS Network Design Functionality

Having identified the core constituents of the network as shown in Figure 3.1, Figure 3.2 illustrates how the network is setup. The setup operates in the following way:

- The network is examined as to whether it is a multicast aware VPLS network. If it is then multicast sessions within the network are monitored. If it isn't the node are examined to determine if they are client nodes or service provider nodes.
- The service provider nodes (PE routers) are then configured to run VPLS service amongst them. The VPLS network is based on having dynamically setup PWs using the BGP protocol.
- Having dynamically setup the PWs, the emulated Ethernet service between the customer sites is checked to see if it is up and running. The emulated service connects the client edge routers of their respective sites. At the client sites, client nodes and server nodes are configured in order to identify the destination and source elements respectively.
- Having setup the emulated Ethernet service, the multicast awareness of the network is checked by having different servers exchanging information throughout the network. As shown in Figure3.1, a Real-time server and Database server forward packets to their respective clients at their different sites. The multicast ability of the network is continuously monitored while streams of data are traversing the network.
- The multicast awareness of the VPLS network is monitored during which ingress replication is confirmed at the closest egress PE node. This improves the utilization of the available bandwidth. Furthermore, it is ensured that packets are not flooded into the network but rather forwarded to their respective destinations or client end nodes in the same VPLS instance.

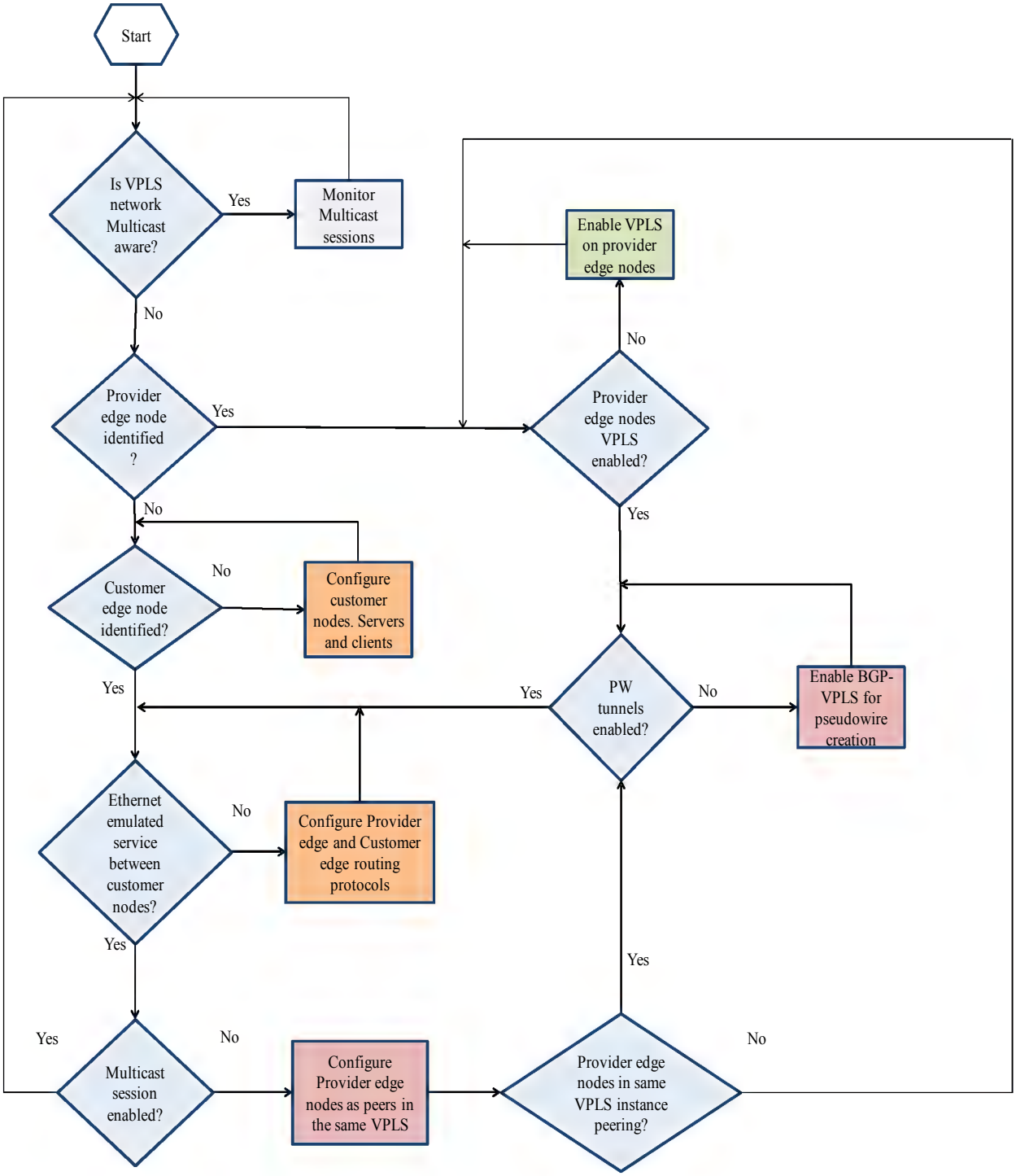

Figure 3.2: Test bed design functionality

3.4 MPLS

The core of the network test bed uses the MPLS protocol to achieve the label switching required for the VPLS instance configuration. MPLS is used as the transport protocol so as to deliver Ethernet services over the test bed network. This section describes the setup/configuration of the MPLS core network elements which are the Provider Edge (PE) nodes and the Provider (P) nodes.

The identification of customer edge (CE) and network (PE and P) routers is important prior to configuring loopback and IP addresses onto the participating network routers. The reason being they (CEs, PEs and Ps) have different roles in the setup of emulated Ethernet links between the three VPLS sites.

In the configuration of the routers participating in the MPLS setup, the identified network facing nodes are configured with appropriate loopback and IP addresses for router Ethernet facing interfaces. The configuring of loopback adapters, in this case lobridge, on routers participating in the MPLS network ensures the following:

- Only one LDP session occurs between any two participating routers regardless of how many connections are linked to them. Therefore ensuring interface state or address change doesn't interfere with the ongoing LDP session [**52**].
- Proper penultimate hop popping behavior when multiple labels are used as is in the case of VPLS frame encapsulation while using MPLS-LDP as the transport protocol [**53**].
- In the instance of a router not having a router ID, a loopback address can be used to acquire the router ID. The loopback address is a virtual interface, it offers flexibility to SPs in relation to router management [**54**].

Having configured the loopback adapters, on the MPLS participating routers, the interactive Ethernet interfaces are assigned IP addresses. It is important that the IP routes are assigned appropriately because when configuring the MPLS-LDP protocol, the LDP distributes labels for active (connected, static and routing protocols learned routes) routes [**53**].

OSPF is then configured on the routers participating in the network. OSPF ensures the distribution of routing information between the routers forming the network. Having configured

OSPF, a ping test between the participating network routers is run to verify routing properties of the network elements (routers). The routes created the OSPF protocol are loop free and scalable to larger networks [**55**].

The communication of OSPF enabled routers occurs over the IP layer. In this instance OSPF version 2 is used for the distribution of routing information across the network. Figure 3.3 describes the OSPF header which has a standard 24-byte header [**56**].

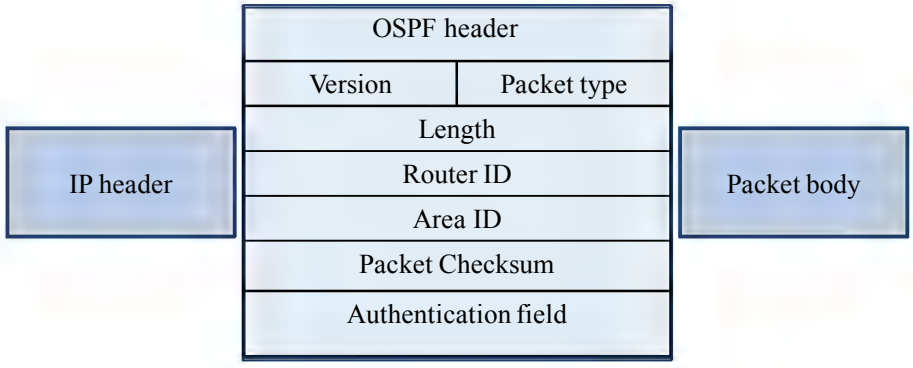

Figure 3.3: OSPF header

The IP header contains addressing and control fields, whereas the packet type is used in link-state synchronization. The length is the Size of the OSPF message including the OSPF header in bytes. The loopback address is used as the Router ID while the Area ID enables the router to match the packet with the appropriate area. Checksum enables the router detect broken packets and the Authentication field ensures that the receiving router's packets weren't tampered [**56**].

To facilitate the distribution of labels, the Label Distribution Protocol (LDP) is enabled under the MPLS attribute section. While enabling LDP, the router's loopback address is used as the transport-address thus ensuring the router can create and initialize LDP sessions. The created LDP sessions originating from the router also advertise its loopback IP address as a transport address to LDP neighbors. However while MPLS-LDP can be further extended to facilitate the creation of Pseudowires (PWs) thus initiating a VPLS network that is LDP based, LDP in this case will only be used for signaling purposes as illustrated in Figure 3.4.

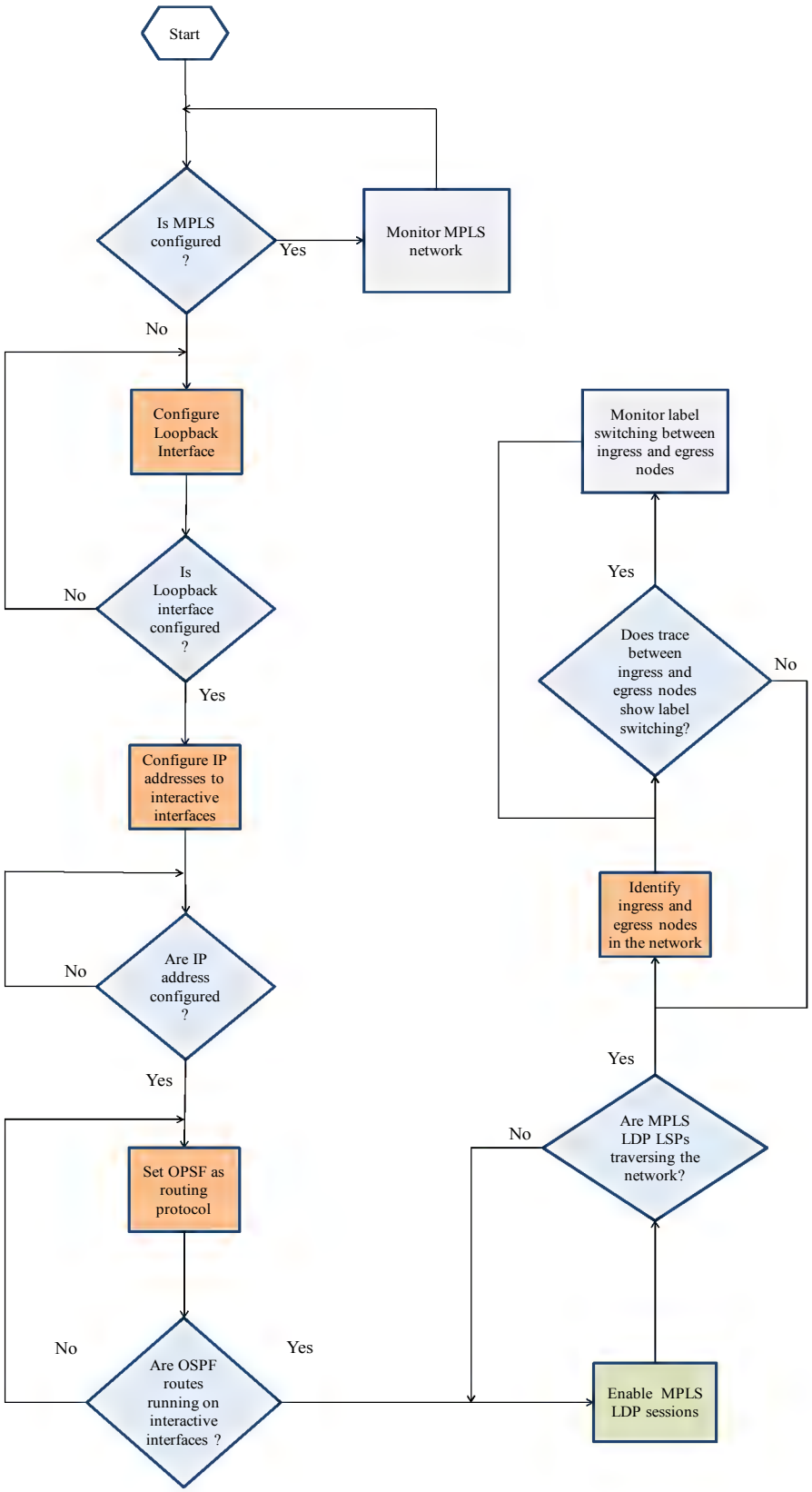

Figure 3.4: MPLS LDP enabling

Configuring a point-to-point (P2P) link with LDP ensued having obtained satisfactory results from the invocation of the OSPF protocol. LDP in this test bed is used for signaling between ingress and egress and forwarding, also known as label edge routers (LER) and label switching routers.

Figure 3.4illustrates the enabling of an MPLS network. This is done in the following sequence:

- At the start, the router is examined to check whether it is MPLS compatible or MPLS has been enabled. If MPLS has been enabled then a check is done to determine whether the labels between the LSRs are properly being exchanged. This is done using the trace route command from the ingress router to the egress router. Otherwise if MPLS is not enabled then the loopback addresses of the routers are then confirmed as existing.
- Having configured the loopback addresses, the participating interfaces of the routers are assigned IP addresses. OSPF is then enabled on the IP subnets to which the participating interfaces are a part of; this is to enable routing exchange between the routers.
- Once the OSPF routing protocol has been configured, MPLS LDP is then enabled on the participating router interfaces. Having identified the ingress and egress nodes within the network the trace route command is executed to determine whether there is label attachment and stripping occurring in the network.

As mentioned in Chapter 2, the pop operation in which the outer most label is removed before leaving the MPLS environment is known as Penultimate Hop Popping. The penultimate LSR is known as the egress router and it is responsible for striping off labels on frames prior to them leaving the MPLS environment. In the design process, care is taken to ensure that the penultimate LSR is the egress router attached to the customer router. This ensures that no packets are dropped in the network before they reach their destination or customer edge router. Figure 3.5 illustrates how this can be achieved .

Figure 3.5 is a segment of the VPLS network for which the LDP protocol is tested prior to it being configured on all other routers. The configuration of LDP on the PE and P routers creates label switched paths in which upstream and downstream labels are exchanged.

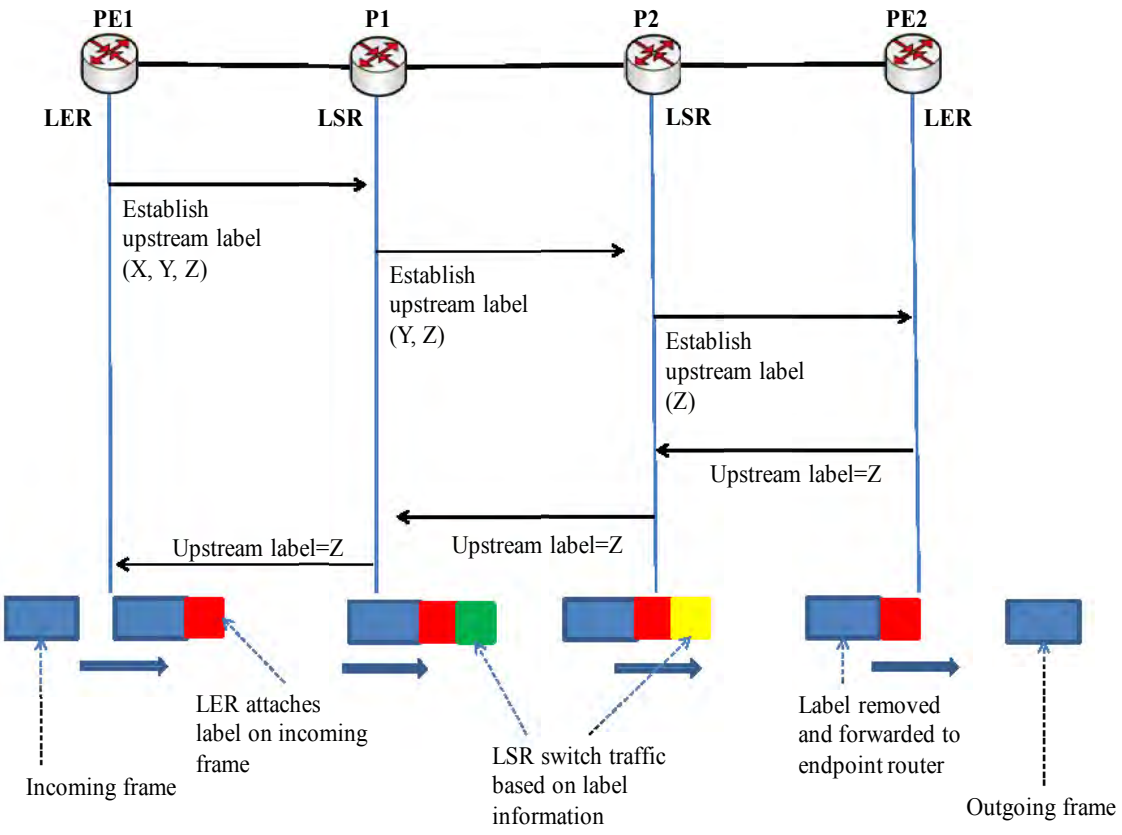

Figure 3.5: Label switched path creation and frame encapsulation

From Figure 3.5, the assumed labels X, Y and Z are upstream labels between PE1 and PE2. These labels are also color coded to highlight the movement of a frame within the label switched path, where labels X, Y and Z are represented by colors green, yellow and red respectively.

The ingress LER, PE1, encapsulates the frame with an MPLS label (Z). The encapsulated frame is then forwarded to the LSRs (P1 and P2) which instead of peering deep into the frame attach labels X and Y and sent to the egress router LER (PE2). Upon arrival at PE2, the labels are stripped off and the frame is forwarded to the endpoint router, in this case a customer edge router.

Figure 3.6 illustrates the structure of the MPLS label. The label is a 4-byte local significant identifier that is used to identify a forwarding equivalent class (FEC). The FEC corresponds to a type of IP subnet destination which is significant to an edge LSR.

Figure 3.6: MPLS Label Structure[57].

In the label structure [**57**], [**58**] and [**59**]:

- The Label is a 20 bit that carries the actual value of the label. When a labeled packet is received, the label value is looked up and the following happens:
    a) The next hop to which the packet is to be forwarded is learned;
    b) The pop, swap or push operation occurs depending on whether the learned next hop is an edge LSR or customer edge/site (CE) router.
- The Exp has 3 bits, Experimental use, currently as a class of service field
- S is 1 bit, which is in the bottom of the stack. It is set to one for the last entry of the label stack and zero for all other label stack entries.
- TTL is the Time-To-Live field used to encode the TTL value.

Having identified and described how MPLS enabled routers exchange and switch labels, the following section illustrates the setup of the VPLS network.

3.5 VPLS

To emulate Ethernet switching over an MPLS network, the PE (Label Edge Router) routers establish tunnels to other LERs to form paths to forward the encapsulated Ethernet frames. The virtual circuits formed are referred to as Pseudowires (PWs). RFC 4761 and RFC 4762 offer mechanisms for signaling and forwarding VPLS frames over a network.

In the formulation of a VPLS network onto the test bed, the PEs (LERs) are configured with signaling and discovery protocols, namely LDP for signaling and BGP for auto-discovery. The flowchart below describes the steps taken to configure the provider edge (PE) routers that will constitute the creation of the member VPLS sites. Figure 3.7 is a representation of VPLS setup based on the BGP protocol.

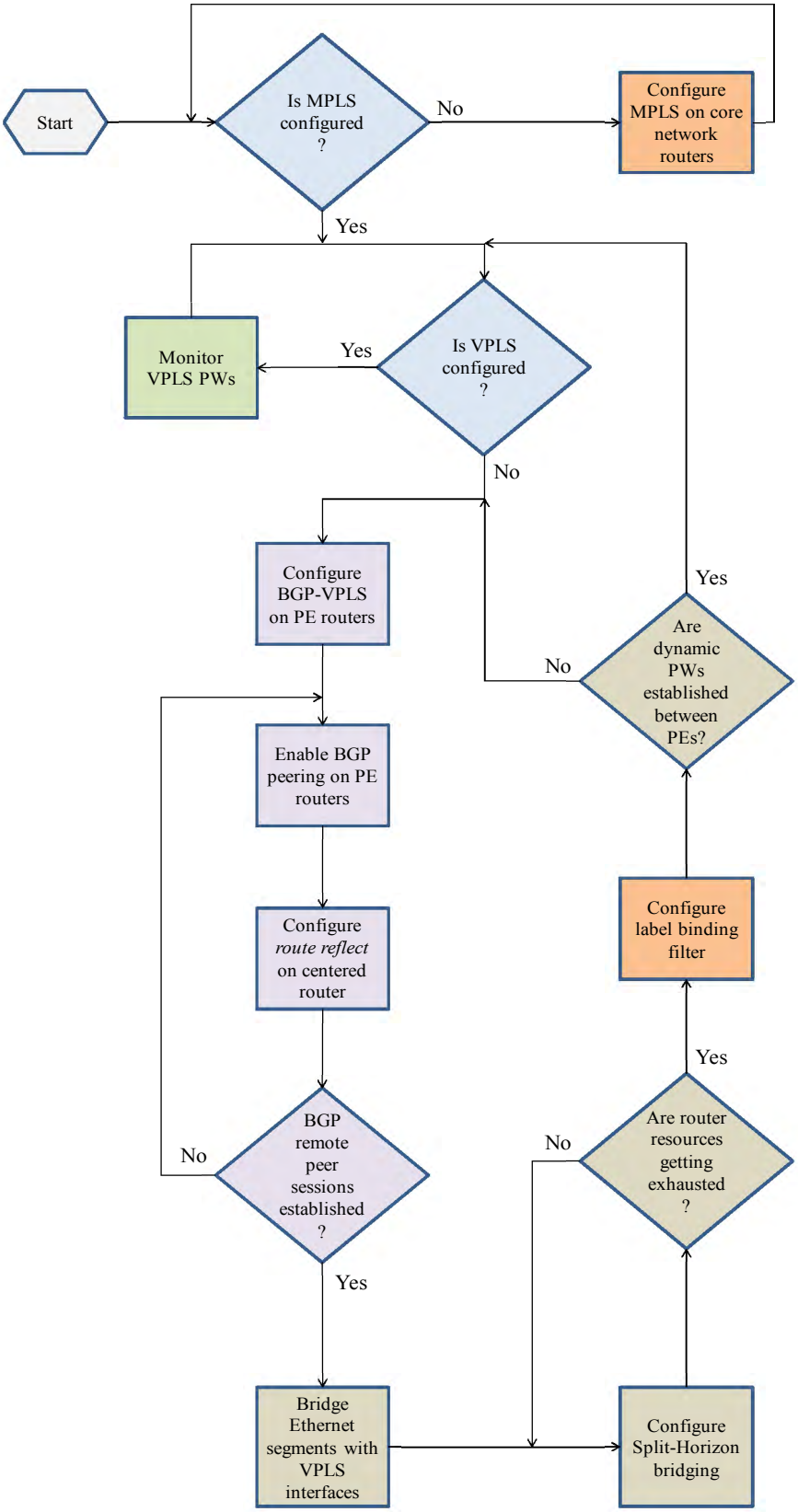

Figure 3.7: BGP based VPLS configuration

Once MPLS has been configured where frame encapsulation and label exchange has been achieved, the LERs (PEs) are configured with the BGP protocol. BGP is used to configure VPLS on the provider edge nodes in the following way:

- Having enabled MPLS on the edge routers, the loopback address of the router is identified as the router's remote address, by doing this the next hop of the PE router will be its peering router.
- Once BGP has been enabled, the route reflect is configured on the "centered" router. As previously discussed, the RR router improves on the scalability of the network rather than having a fully meshed network. The VPLS interfaces are configured and bridged to their respective Ethernet segments.
- Split-Horizon bridging is then configured to ensure loop avoidance. A combination Split-Horizon bridging and disabling penultimate hop popping behavior on the MPLS LSPs ensures that the test bed router CPUs do not get exhausted due to recurring loops in the network where multiple copies of the same packet are sent to the same destination,[**60**] and [**36**].
- To ensure resource utilization and low network load a label binding filter is configured. In so doing, label bindings from LDP neighbors are advertised and accepted by their peering routers [**53**]. Having setup the dynamic PWs between the LERs, the PWs are then monitored.

Enabling the BGP peering attribute on the PEs ensures the creation of BGP sessions where NLRI exchange occurs. In this test bed design, the exchange of BGP NLRI between PE routers means that a route reflector will be configured to ensure successful BGP sessions. The alternative to using a route reflector is having a full mesh, or meshed network. The decision to have a route reflector within the network is based on the network layout as illustrated in Figure 2.7 (b).

In Figure 3.8 a BGP peering session occurs between PE1 and PE2. The provider edge routers are attached to different autonomous systems denoted as AS1 and AS2 for PE1 and PE2 respectively.

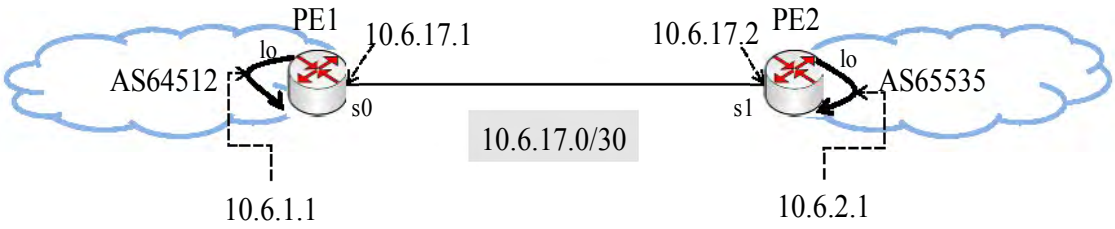

Figure 3.8: BGP peering[54]

The peering session illustrated in Figure3.8 shows a BGP speaker 10.17.1.1 (PE1) in AS64512 with a loopback (lo) created with IP address 10.6.1.1 peering with PE2 (10.17.1.2) in AS65535 with a loopback (lo) created with IP address 10.6.1.2. Serial interfaces s0 and s1 are used as remote ends for AS65535 and AS64512 respectively i.e. PE1 (10.6.17.1) uses 10.6.1.2 as the remote end connection for AS65535 via serial interface s0. Thus a packet from PE1 destined to AS65535 uses interface s0 to reach PE2 where it loops back to feed the BGP session. This process is similar in the reverse direction where PE2 reaches AS64512 through 10.6.1.1 using interface s1 [**54**].The BGP operation described is illustrated in Figure 3.9.

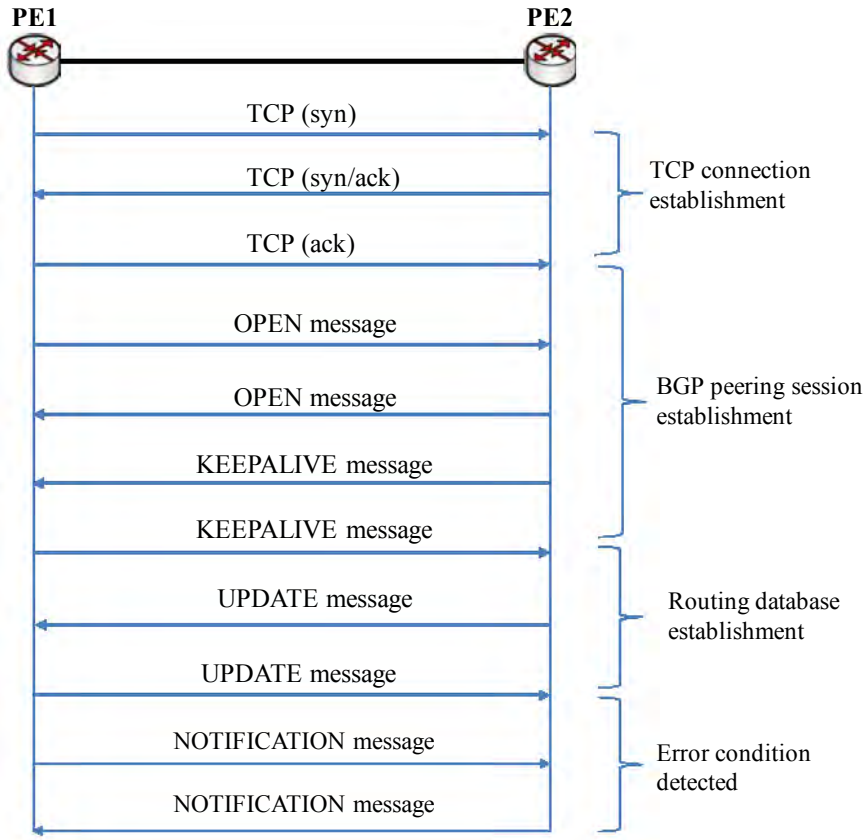

Figure 3.9: BGP provider edge (PE) peering[61], [62]

BGP operates by establishing a TCP connection between peering routers. Having established the TCP link between routers PE1 and PE2, the OPEN BGP messages are exchanged. KEEPALIVE messages are then exchanged between the routers to acknowledge the OPEN messages. An UPDATE message is then sent between the routers and is used to transfer routing information between the BGP peers. Finally, in case an error is detected a NOTIFICATION message is sent thereby terminating the BGP connection[**61**].

From the BGP operation illustration, the BGP messages are structured to be exchanged between routers in the same autonomous system (AS) in this particular test bed setup. The routers running internal BGP (IBGP) sessions between each other are not next to each other therefore a TCP connection links them. The IBGP sessions running on routers within the same AS further ensure synchronization of the routing policies [**63**].Figure 3.10 is a representation of the BGP finite state machine (FSM)

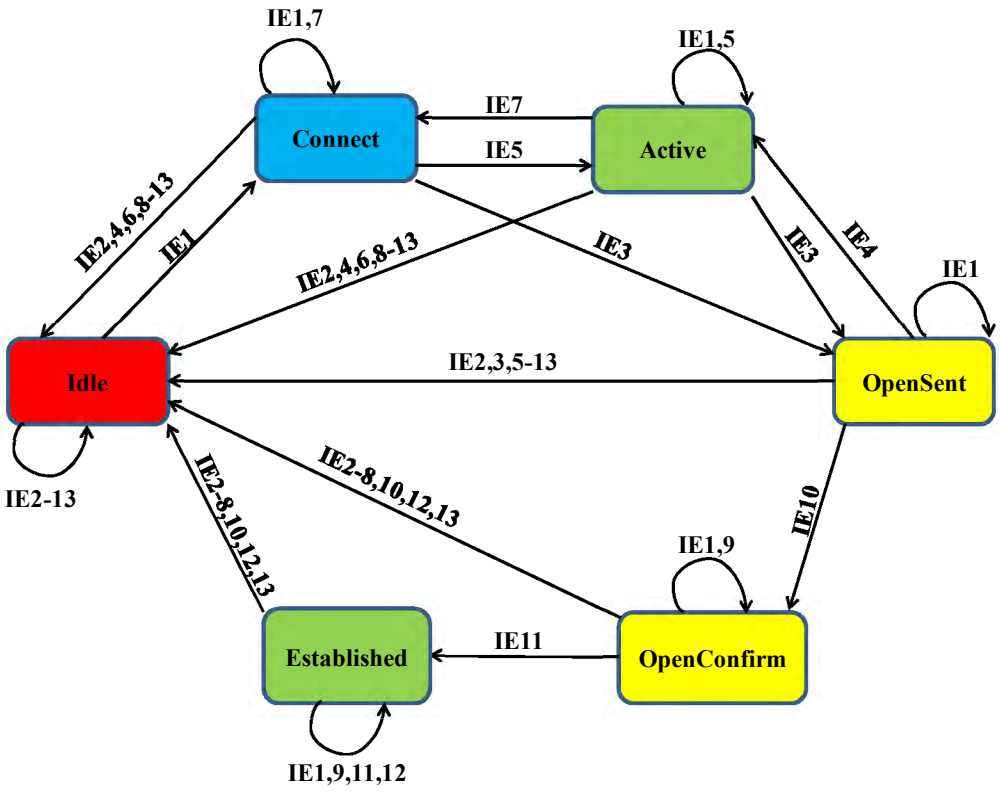

Figure 3.10: BGP FSM[64], [54].

Table 3.1 describes the input events labeled IE1-13 as illustrated in Figure 3.10. The input events and the actions taken by the BGP FSM automata determine the transitional states achieved by the peering PEs.

Table 3.1: BGP FSM messages[54**], [**63**], [**64**]**

Input Event (IE)	**Action**
1	BGP Start
2	BGP Stop
3	BGP Transport connection open
4	BGP Transport connection closed
5	BGP Transport connection open failed
6	BGP Transport fatal error
7	ConnectRetry timer expired
8	Hold timer expired
9	KEEPALIVE timer expired
10	Receive Open message
11	Receive KEEPALIVE message
12	Receive UPDATE message
13	Receive NOTIFICATION message

The Table 3.2 is based on [**54**], [**64**] and RFC 4272 in which BGP peers exchange messages regarding their state changes and it describes the input event actions in Table 3.3 and illustrated in Figure 3.10.

Table 3.2: BGP state description

State	State description
Idle state	In this state, the BGP peer refuses all incoming connections. At Input Event 1(IE1) shown in Table 3.1, the following processes occur; all BGP recourses are initialized, the ConnectRetry timer is started, TCP connections are initialized to neighbors, listens to TCP connections from neighbors and changes its state to Connect. The Start event can be triggered manually by the operator through configuring BGP or resetting the BGP peer, or by the BGP router automatically resetting the BGP process. The first transition back to the Idle state is caused when the router sets the ConnectRetry timer and cannot start the BGP peering process until the timer expires.
Connect state	The BGP peer in this state waits for the TCP connection to be established. Once the TCP connection is established, the initialization is completed by the ConnectRetry timer through sending an Open message. The BGP peer now changes to the OpenSent state. Otherwise if the TCP connection isn't established, the BGP peer continues to listen to initializations from neighbors resets the ConnectRetry timer and changes into an Active state. Once the ConnectRetry timer expires while in Connect state, the timer is reset to allow a connection to other BGP peers otherwise the BGP router goes into the Idle state caused by any other input.
Active state	This is the state, through listening and accepting, the BGP peer initiates a TCP connection with its neighbor. Once the TCP connection is made, the ConnectRetry timer is cleared and the initialization is completed. The BGP peer then sends an Open message to its neighbor and then changes its state to OpenSent. The Hold timer is by default set to 4 minutes. The BGP peer changes back to the Connect state once the ConnectRetry timer expires. The ConnectRetry timer is then reset so that the BGP peer may continue to listen for TCP connections from neighbors. If the TCP connection is refused e.g. if the IP address is wrong, the local process remains in the Active state unless it's triggered by an input event, except the start event, which changes its state to

	Idle.
OpenSent state	In this state, the BGP peer waits for an Open message from its neighbor. Upon receiving the Open message if errors are found in its checked fields, a Notification message is sent and the state changes to Idle. If there is no error, a Keepalive message is sent and the Keepalive timer is set. The Hold and Keepalive timers aren't started if the smallest negotiated value of the Hold time is zero. The successful start of both timers triggers a state change to OpenConfirm of the BGP router. A failed TCP connection leads to the resetting of the ConnectRetry timer and listens for a new TCP connection failure of which leads to the state changing to Active state. The state changes to Idle if there is any other input event other than the start event.
OpenConfirm state	In this state, the BGP peer waits for a Keepalive or Notification message from its peer. A received Keepalive message triggers a state change to Established whereas a Notification or a TCP connection failure message signals a state change to Idle. The Notification message is sent when there is an error detected, the Hold timer has expired or a Stop event occurs.
Established state	In this state, the BGP peer connection has been established and an exchange of Update, Notification and Keepalive messages occurs between the peering routers. The Hold timer is reset after an Update or Keepalive message is received. In case a Notification message is received, the BGP changes its state to Idle.

3.6 Pseudowire Enabling

The enabling of pseudowires in the test bed environment ensures the creation of emulated Ethernet links between the various sites. PE1 can transport L2 frames to PE2, or to multiple PEs, across an MPLS by encapsulating the frames and sending them through the LSPs to their destinations. A PW is a relation between two PEs and it can be P2P, P2MP or MP2P [**45**].

In the design setup of the test bed, VPLS is considered as a Layer 2 technology which is MP2MP. The discovery mechanism used is BGP as stipulated in RFC 4761 whereas the signaling protocol is handled by the label distribution protocol (LDP). MPLS is used as the transport and tunneling protocol, this is illustrated in Table 3.3 below.

Table 3.3: Test bed protocol and technology layout

L2-VPLS	Multipoint
Discovery	BGP
Signaling Protocol	LDP
Tunneling Protocol	MPLS

In the design of the VPLS test bed network, point-to-multipoint (P2MP) connections are established in which participating PE network nodes are discovered using the BGP protocol. The network elements that form the MPLS core use LDP as the signaling protocol. The LSP tunnels created using the MPLS protocol ensure the establishment of pseudowires.

3.6.1 Pseudowire Setup and Teardown

In the setup and teardown of pseudowires, participating PEs of a particular VPLS instance must declare to each other that they are members of VPLS instance and also be able to declare that they are no longer participating in the VPLS instance [**8**]. Through declaring membership, PEs ensure that they are discovered by participating members of the VPLS instance.

There are two ways in which discovery can be archived [**8**]:

a) Manually configuring a PE with the identity of all the other PEs in the fully meshed VPLS instance. However, in this instance a route reflector will be used to re-advertise learned routes to its BGP peers.
b) A PE router can use a protocol to identify all other PEs in the same VPLS instance, this is known as Auto-discovery**.**

Using BGP's auto-discovery and *route-reflect* characteristics, VPLS memberships of participating PEs ensure the pseudowires are setup dynamically. This is advantageous for purposes of scalability and flexibility in regards to an ever expanding and changing topology, therefore pseudowire establishment within the test bed network is BGP based.

As demonstrated in Figure 3.11, the establishment of pseudowires starts with the configuration of the virtual switch instance (VSI) on both PEs stating each as the others specific peer. Mapping peer (mp) messages are then exchanged and are updated at both PEs with an mp-

reach message. Having confirmed that the respective PE interface parameters are matched, the pseudowire is established.

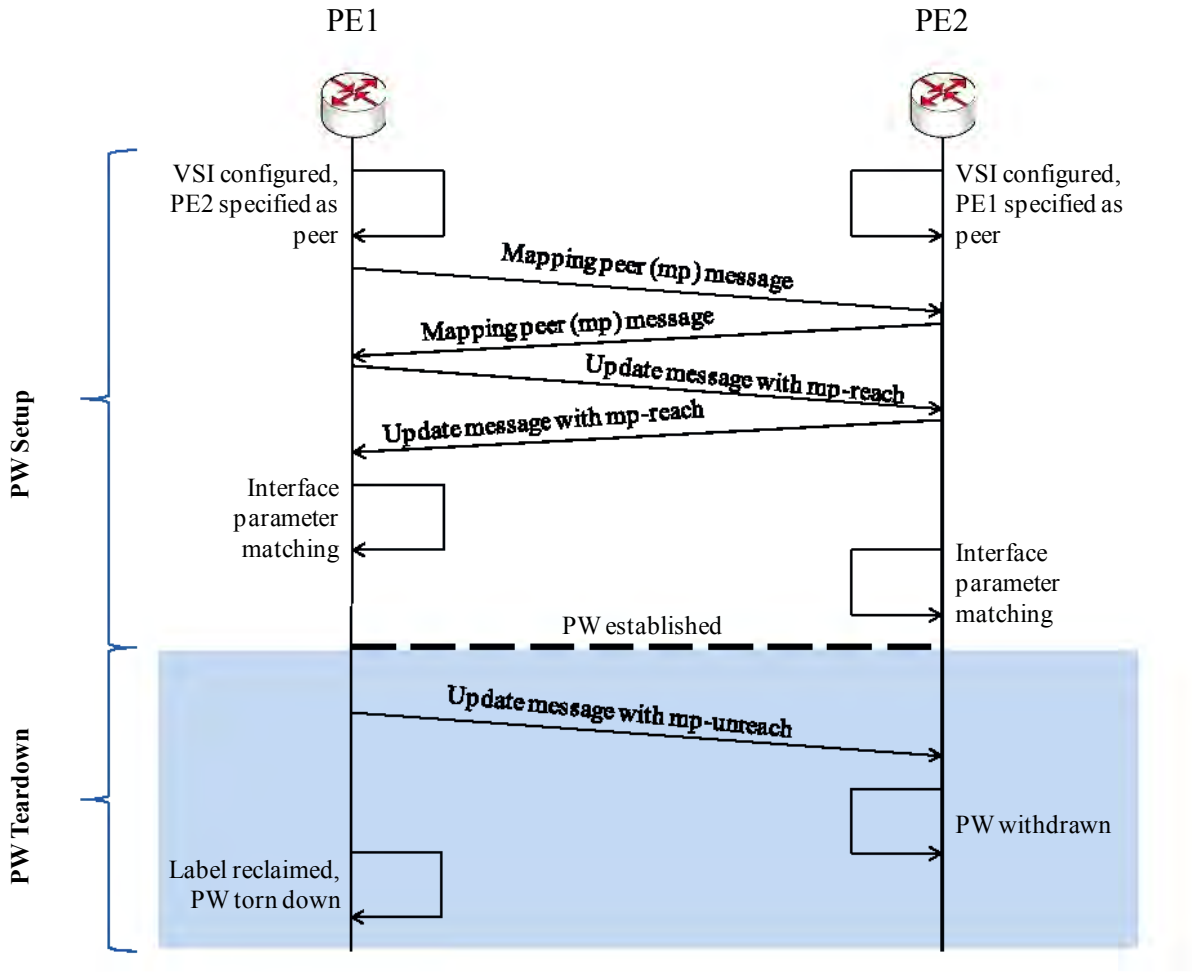

Figure 3.11: BGP Based PW Setup and Teardown[8].

The mp-un-reach update message originating from a PE participating in a VPLS instance signifies the withdrawal of the pseudowire and the reclaiming of labels between the PEs.

In Figure 3.12, the VSI is configured on both LERs and each is configured as the others' neighbor. Once mapping messages have been exchanged and their interface parameters matched, the PW is setup. For the teardown of the PW, the mapping messages are withdrawn and release messages are exchanged which lead to retrieval of labels and teardown of PWs [**8**].

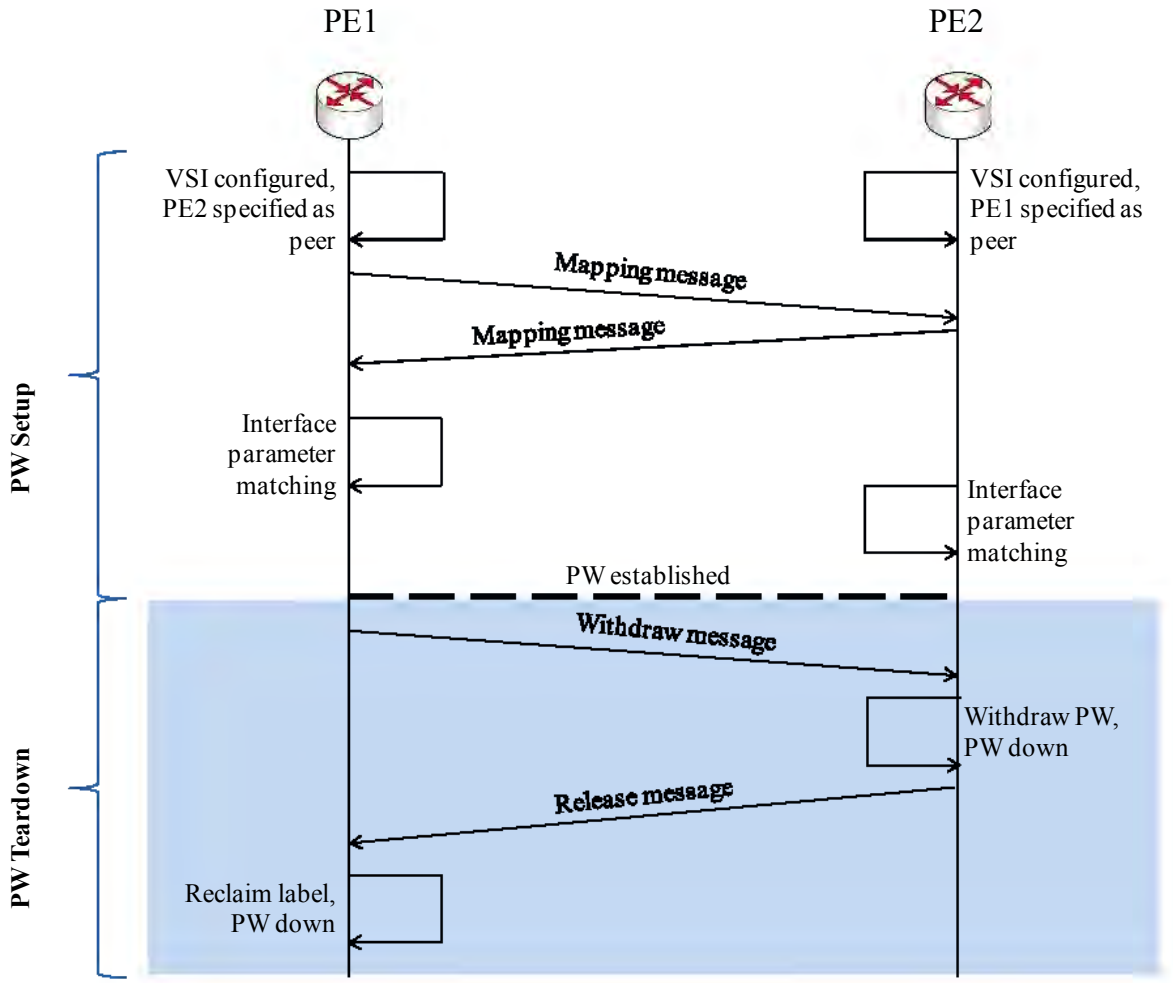

Figure 3.12: LDP Based PW Setup and Teardown[8].

However, in the design of the VPLS test bed, PWs are setup using BGP as discussed in the previous BGP section. The VPLS network on the test bed has dynamically setup PWs with a specific emulated service in which instances are in the Ethernet Raw mode. Therefore the Ethernet frames from CEs attached to PEs are transmitted over a single PW [**65**]. In so doing, the PW can carry Ethernet or IEEE 802.3 PDUs over the MPLS backbone network and also ensure emulated Ethernet services over the network [**65**].

3.6.2 Ethernet Emulation

In the setup of the test bed, consideration and emphasis is placed on connecting the VPLS sites to the service provider's network at the OSI layer 2, reason being the ease of frame encapsulation across the network [RFC 6624]. Prior to setting up an emulated service between

the client edge routers at the different sites, as Figure 3.13 illustrates, the provider edge nodes have been configured with VPLS.

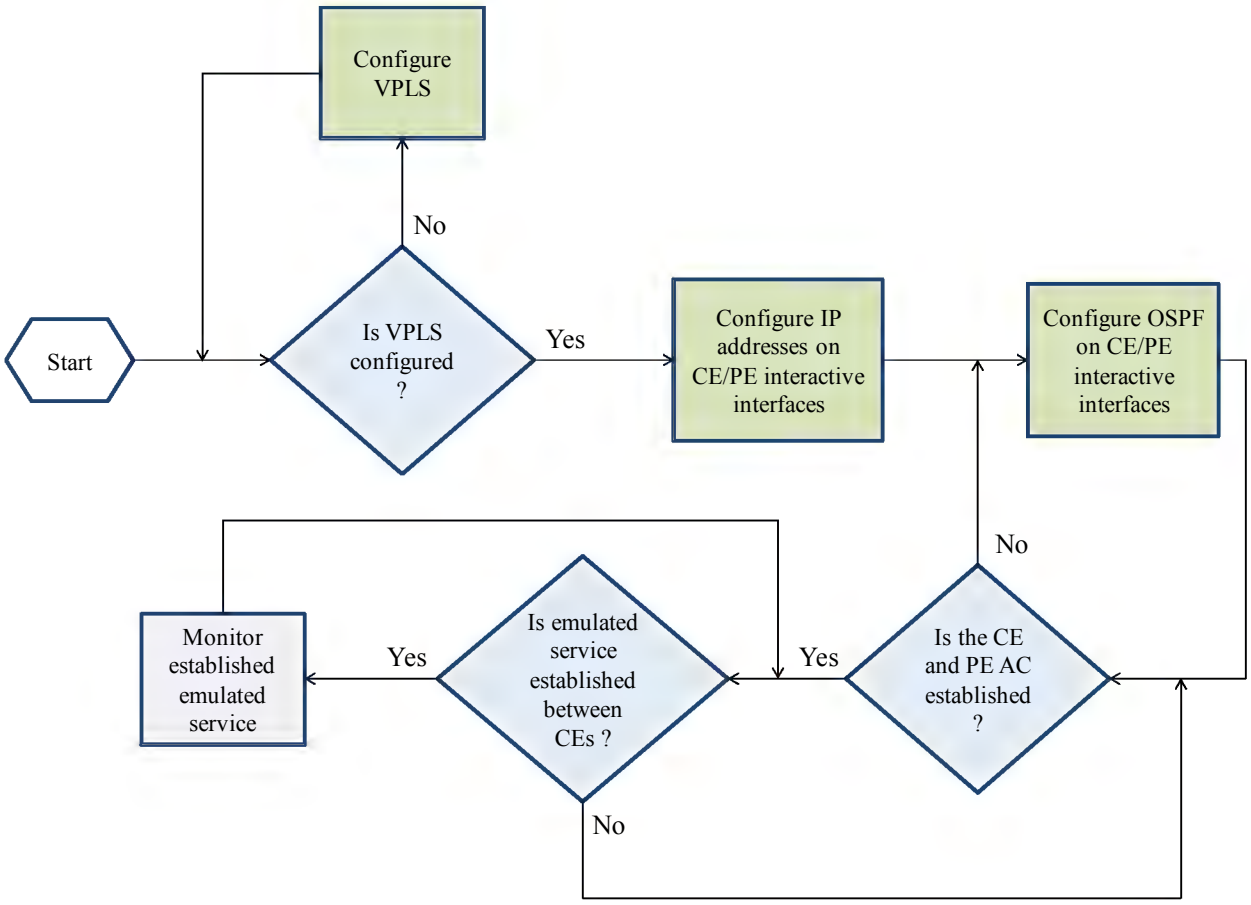

Figure 3.13: Ethernet service emulation

The PE routers in the network are running BGP-VPLS, which provides a dynamic setup of pseudowires and auto-discovery of VPLS peers within the network.

The participating interfaces of the customer edge routers are assigned IP addresses after which OSPF routing protocol is configured for these interfaces. At the provider edge interface facing the CE, an IP is assigned and is also configured with OSPF, thus enabling peering and exchanging of routing information.

With the core routers having formed the necessary LSP, the pseudowires between the PEs are established. Customer edge routers belonging to a particular VPLS instance exchange routing information and build routing tables.

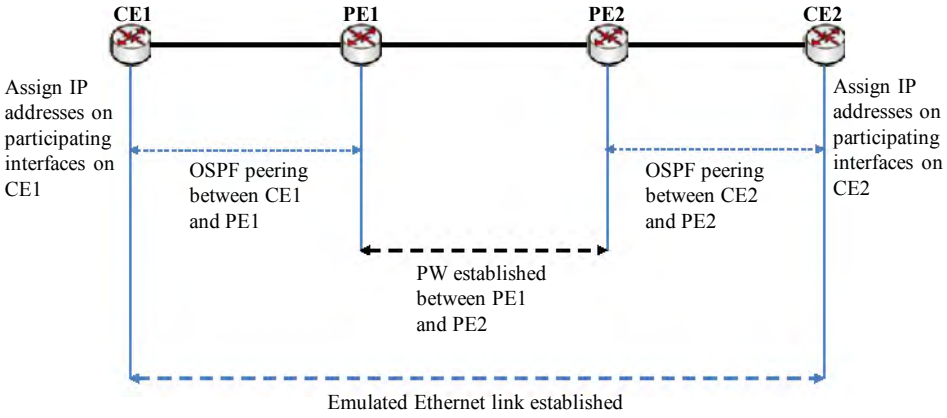

Figure 3.14: Emulated Ethernet Link

Having setup an emulated Ethernet link between the customer edge routers, as shown in Figure 3.14, server and client machines are attached to their respective CEs. The interactive interfaces of the server and client with their CEs are assigned IP addresses as illustrated in Figure.15. The default gateways of the server and client are set as their CE's respective IP addresses.

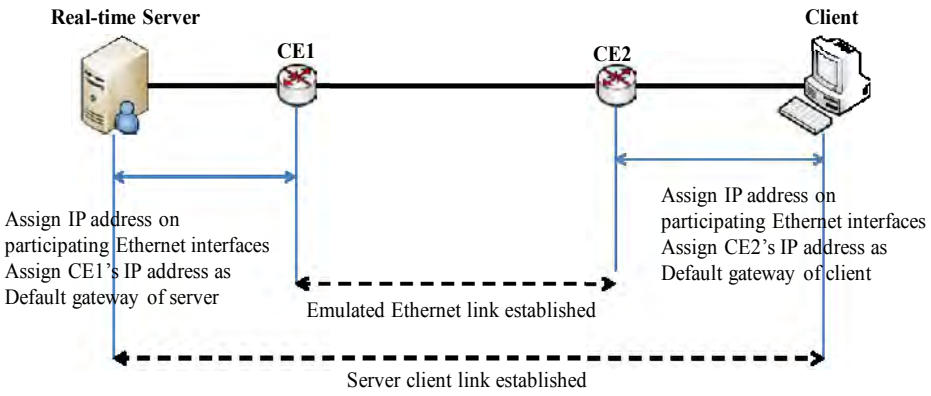

Figure 3.15: Emulated Ethernet Server Client Link

Figures 3.14 and 3.15 demonstrate a point-to-point (P2P) emulated service between customer edge routers and a server and client belonging to the same VPLS instance.

3.7 Summary

This chapter has discussed the setup of a VPLS environment over an MPLS enabled backbone network. It has also discussed the realization of the VPLS network in a virtualized environment. This chapter also introduces the tool that will ensure the creation of a virtualized VPLS network for example VMware Workstation and Mikrotik routerOS which create virtual machines and routers respectively.

The virtualization of the network is aimed at minimizing setup costs that would have been incurred through the use of physical network elements, for example routers. The resource splitting design coupled with the setting up of the network provides SPs easy management and maintenance of the overall network.

Through the use of MPLS as a transport technology, a VPLS network is setup. LDP as a signaling protocol and BGP as an auto-discovery protocol offer the VPLS network both scalability and resilience which are vital to both the SP and the client. Furthermore, VPLS offers the point-to-multipoint connectivity through which different sites are linked with advantages as those found in Ethernet type connections.

Multicast awareness in VPLS networks can be achieved in the way they are setup. Dispersed client sites that belong to the same VPLS instance are multicast aware i.e. only members belonging to that VPLS instance are the only ones that are able to participate in the multicasting. The next chapter presents the implementation of the multicast aware VPLS network as discussed in this chapter.

Chapter 4 Application Aware Multicasting Implementation

4.1 Introduction

Chapter 3 presented the design details of the Virtual Private LAN Service network functionality. This chapter discusses the implementation details of the network design. In this chapter, the framework or platform used to implement the VPLS test bed is introduced through the creation of virtual machines. This chapter presents the software tool, Mikrotik routerOS, used in the implement of the VPLS network. This is then followed by a discussion of the implementation of the network. Finally the realized network is mapped out using The Dude. The Dude provides a diagrammatic representation of networks that are using Mikrotik routers.

4.2 VPLS Network Deployment

As mentioned in chapter 3, the decision to have a virtualized test-bed is based on the cost of setting up the network. VMware Environment enables the creation of multiple network elements without the need to physically buy them thus ensuring minimal hardware costs.

Virtualization further aids multiple operating systems to run simultaneously on a single host and this is vital while setting up the test-bed because the different elements run on different operating systems. The routers, server and client nodes in the network are created by allocating the hosts' resources based on each ones' minimal operating system requirements. The routers run on MIKROTIK™ routerOS v5.2which requires a minimum of 32 MB of RAM whereas the customer premise machines (servers and clients) are configured with Windows XP operating system.Figure30 illustrates how the virtualized network was conceptualized.

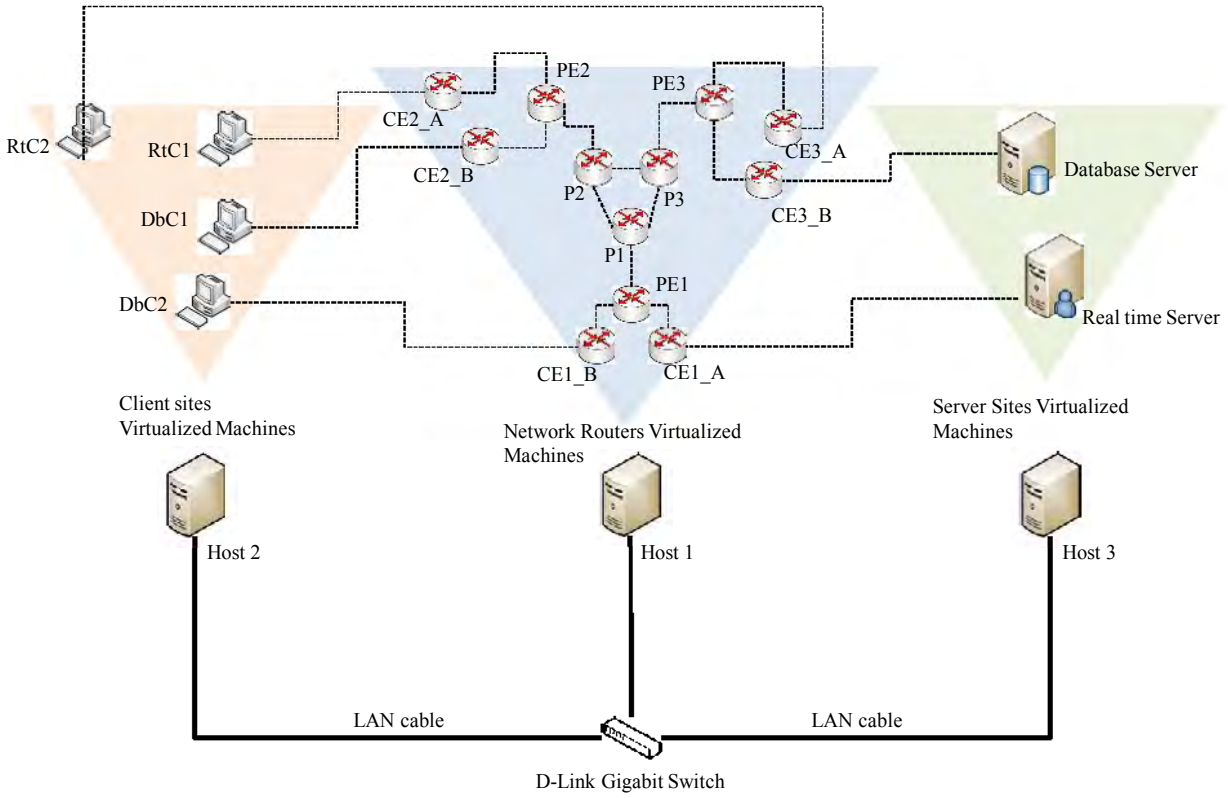

Figure 4.1: VPLS Network on a Multi-tenant VM Platform

In Figure 4.1, the VPLS network is realized through virtualization of the network elements. Hosts 1, 2 and 3 have virtual machines running on them as: network routers, client end machines and the application servers respectively. Figure 30 is an illustration of a multi-tenant VM platform due to the nature of the multiple hosts that are combined to realize the VPLS network. The D-link Gigabit switch and the LAN cables shown are physical devices.

Host 1 contains virtualized routers which are labeled as follows:

- PE1, 2 and 3 represent provider edge routers. These have MPLS capability, run VPLS and connect client/server sites to the network.
- P 1, 2 and 3 represent network-core provider routers within the network. These are MPLS capable.
- CE 1, 2 and 3 represent client/server site customer edge routers. These are further denoted by A and B to represent the two different VPLS instances in the network.

Host 2contains virtualized client end machines which are labeled as follows:

- RtC1 and RtC2 are real-time clients that belong to VPLS instance A.
- DbC1 and DbC2 are database clients that belong to VPLS instance B.

Host 3 contains 2 virtualized servers:

- Real-time server which is a source of real-time data applications such as video and voice.
- Database server which will serve as the source of the file transfers.

Table 4.1 below illustrates how the host resources were allocated to the virtual machines.

Table 4.1: Allocation of hosts' resources to virtual machines

Type of VMware device	Number of devices	Virtual machine allocated RAM (MB)	Virtual machine allocated Hard disk space (GB)	Number of bridged Network adapters
Database server	1	1024	20	1
Real-time server	1	1024	20	1
Database clients	2	512	20	1
Real-time clients	2	512	20	1
Customer edge routers (CEs)	6	64	1	4
Provider edge routers (PEs)	3	64	1	10
Provider routers (Ps)	3	64	1	4

The criterion used for the allocation of resources was based on the basic requirements needed to ensure network element functionality.

4.3 RouterOS Installation

As mentioned in the design assumptions, MIKROTIK™ is used as the routing operating system for the VPLS network. Mikrotik routerOS is used on RouterBOARD hardware as its operating system. RouterOS is a stand-alone operating system based on the Linux v2.6 kernel which can transform a PC into a fully functional router [**66**]. Having a router operating system ensured that created virtual machines could easily be transformed into fully functional routers.

4.4 MPLS Configuration

Having setup the virtual machines, the network elements are configured in respect to their functionality. In the core of the network the routers are MPLS enabled. The MPLS enabled routers facing the network and clients are the provider edge routers and are setup to dynamically establish pseudowires between routers participating in the same VPLS instance. In this section, the process of enabling an MPLS network is discussed.

4.4.1 Loopback Addressing

Loopback addressing as mentioned in section 2 is not configured on any network interfaces but used for LDP sessions. This serves two purposes [**66**]:

- Ensures proper penultimate hop popping (PHP) behavior when multiple labels are attached to packets.
- Ensures that the LDP sessions are not interrupted by changes in the addresses or network interface states of the router and its participating peers.

Figure 4.2 shows the loopback IP address configuration for the MPLS participating routers.

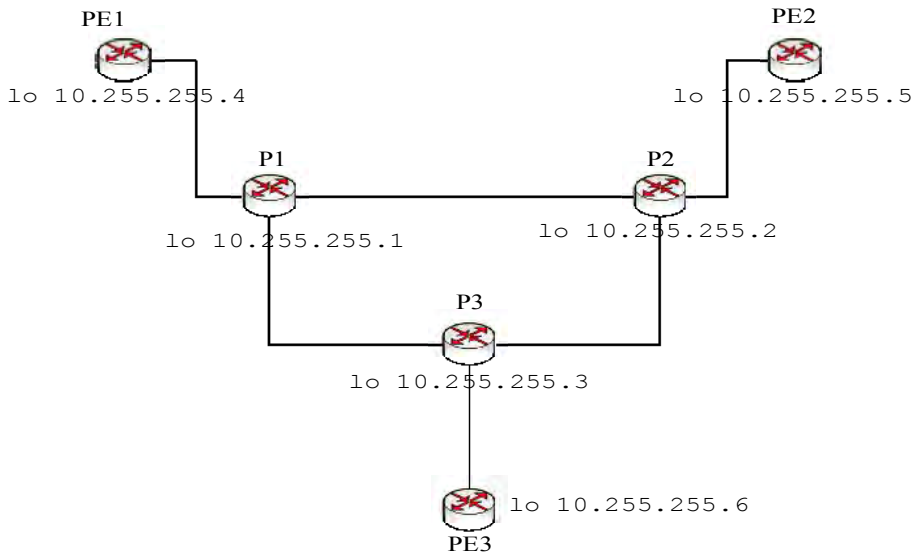

Figure 4.2: Loopback IP Addressing

P1

```
[admin@P1] >interface bridge add name=lobridge
[admin@P1] >ip address add address=10.255.255.1/32
interface=lobridge
```

From Figure 4.2, the above loopback configuration is also applied to routers P2, P3, PE1, PE2 and PE3 with a range of 10.255.255.2-6/32 respectively in a similar fashion as P1. During the configuration of the loopback, a bridge is created and is assigned the name "*lobridge*". It is this bridge that is then assigned the loopback address [**66**].

Having setup the loopback addresses, the network interfaces are assigned IP routing addresses to structure links as shown in Figure 4.3.

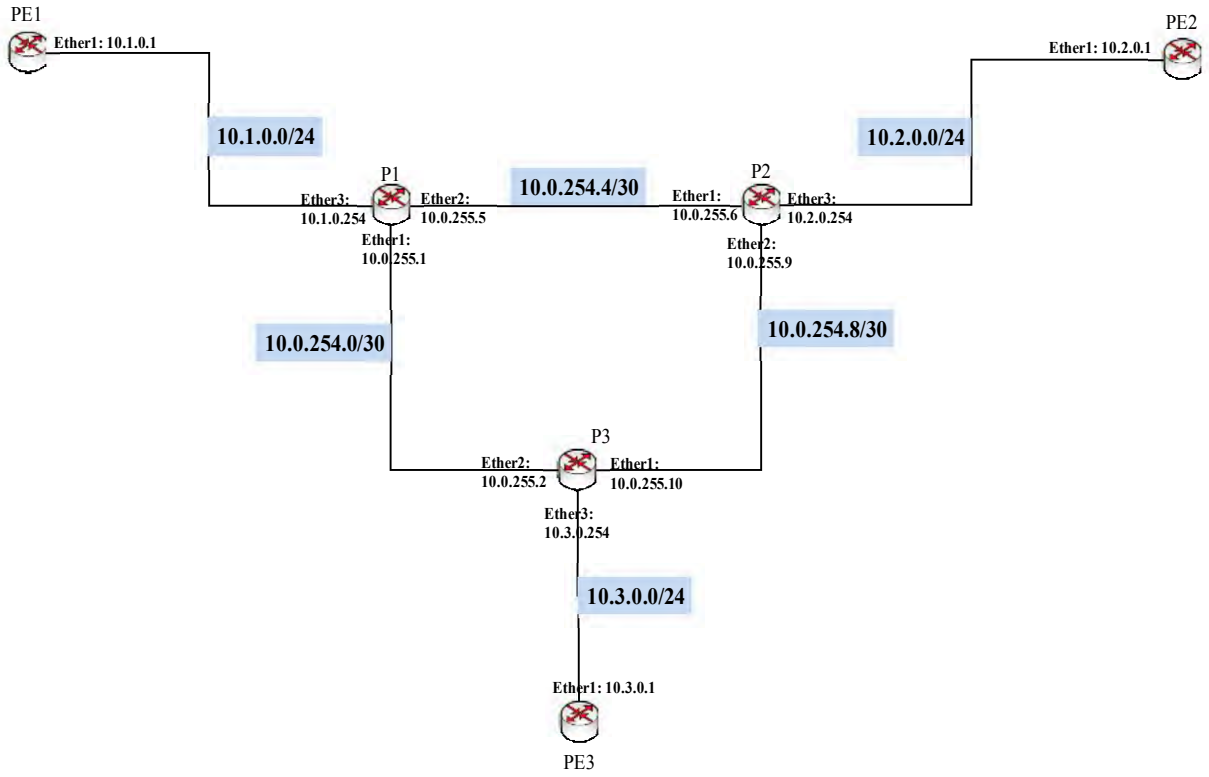

Figure 4.3: Interface IP Addressing

P1

```
[admin@P1] >ip address
[admin@P1] /ip address>add address=10.0.255.1/30 interface=ether1
[admin@P1] /ip address>add address=10.0.255.5/30 interface=ether2
[admin@P1] /ip address>add address=10.1.0.254/24 interface=ether3
```

The above routing invocation is also used to setup the rest of the peering routers. However the different interfaces are assigned different IP addresses as shown in Figure 4.3.

4.4.2 OSPF Configuration

Having setup the router IP network interfaces, they are dynamically designed to distribute routes across the network using the OSPF routing protocol. While setting up OSPF to dynamically distribute the routes, a loopback address is set as the routers' identification i.e. *router-id=loopback address* [**66**]. This is shown in the OSPF settings of P1 below.

P1

```
[admin@P1] > routing ospf
[admin@P1] /routing ospf>instance set distribute-default=never
redistribute-connected=as-type-1 router-id=10.255.255.1
[admin@P1] > routing ospf network
[admin@P1] /routing ospf network>add area=backbone network=10.0.255.0/30
[admin@P1] /routing ospf network>add area=backbone network=10.0.255.4/30
[admin@P1] /routing ospf network>add area=backbone network=10.1.0.0/24
```

The above configuration is also done on the other participating routers' interfaces. After setting the router id, it is important to specify that the router must not distribute its own default route to other routers. Secondly the router redistributes routes to directly reachable networks using the OSPF metric *type-1*. The OPSF metric *type-1* is the sum of the internal OSPF cost and the external OSPF cost [**66**]. Finally the links attached to the router are set as part of the networks' backbone areas. The link addresses are represented in blue as shown in Figure 4.3.

4.4.3 LDP Configuration

In order to distribute labels on the setup routes, MPLS is enabled using the label distribution protocol (LDP) [**15**]. In the setup of MPLS, the router-id now known as a label switching router LSR-id is assigned to the loopback address. Furthermore, the LSR uses its loopback address as the transport address [**66**]. Thereafter all participating interfaces are then added as LDP interfaces.

P1

```
[admin@P1] >mplsldp
[admin@P1] /mpls ldp>set enabaled=yes lsr-id=10.255.255.1 transport-
address=10.255.255.1
[admin@P1] > mpls ldp interface
[admin@P1] /mpls ldp interface>add interface=ether1
[admin@P1] /mpls ldp interface>add interface=ether2
[admin@P1] /mpls ldp interface>add interface=ether3
```

Having enabled MPLS on the interfaces of the participating routers, Figure 4.4describes how labels are processed within the routers. From Figure 4.4, the IP routing, IP forwarding and label forwarding tables are built through the exchange of routing and binding information with peering LSR routers. Once the router has received all the IP information/prefixes the MPLS enabled LSR starts to forward the IP traffic [**67**].

Prior to forwarding the traffic throughout the network, the LSR uses local labeling, globally unique labels or centralized labels assigned to the packets thus ensuring scalability. The assigned labels are recorded into the *label information base* (LIB) even though the IP address is not from a next-hop router [**11**]. The *label forwarding information base* (LFIB) is the forwarding table in which input labels are entered. It must be noted that the label stored from an IP address that is not a next-hop router in the LIB isn't used as an active label; therefore it will stay in the control plane and not move further into the data plane where active labels are placed in the LFIB. However, a label assigned to a next-hop router IP address is entered as an output label in the LFIB and also into the *forward information base* (FIB) to facilitate IP-to-label forwarding [**67**].

During label assignment and forwarding, when an input label is received a table lookup is performed on the LFIB and an output label replaces the input label. The new output label is then forwarded to the next-hop router. In this process, LSRs can be ingress, switching or egress routers in which labels are assigned, switched or stripped off the packets depending on the topology of the network.

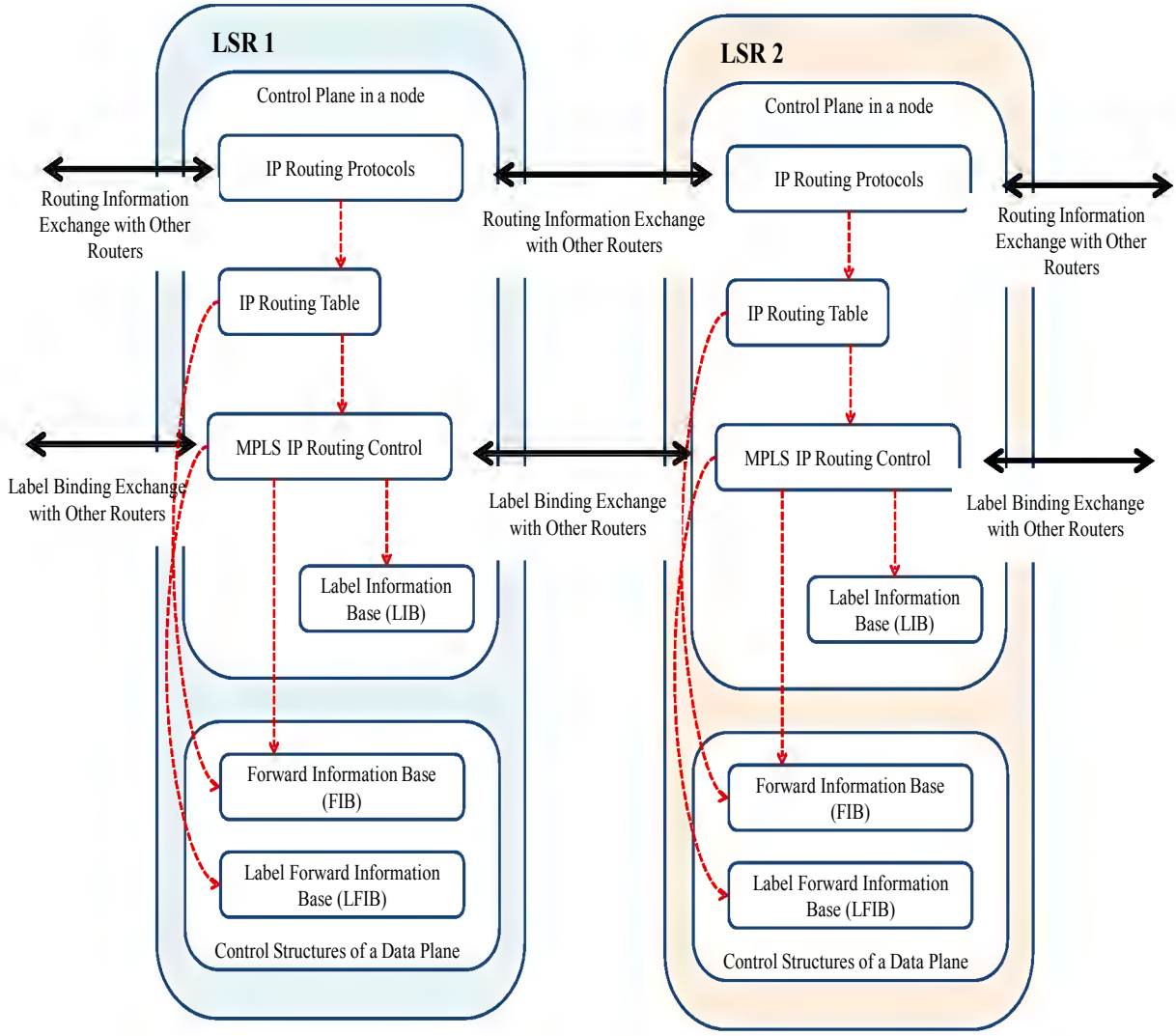

Figure 4.4: MPLS Router Label Processing[67].

Before forwarding traffic across the network, the LSR through its control plane has various applications that are all connected to the LFIB. These different applications such as QoS, MPLS-TE, and Any Transport over MPLS (AToM) are essential for the scalability of the network. Theapplications might have different routing protocols within the control plane of the LSR but they are later on entered into the LFIB, which as mentioned previously is responsible for forwarding label-attached IP packets to their respective next-hop routers [**67**].

4.5 VPLS Configuration

Once MPLS switching has been achieved between the participating routers in the network core, the VPLS mechanism can be implemented. A VPLS environment can be achieved in two different ways:

- Using Label Distribution Protocol (LDP) in which a full mesh of LDP tunnels will have to be established RFC 4762
- Using Border Gateway Protocol (BGP) in which either a full mesh or route reflected tunnels can be established RFC 4761.

The establishment of VPLS tunnels using either the LDP or BGP protocols was discussed in Chapter 3. However during the setup of the network, both protocols were analyzed and based on each one's advantages and disadvantages only one protocol was used to establish the VPLS tunnels.Table 4.2 illustrates the advantages and disadvantages of either using BGP-VPLS or LDP-VPLS for the establishment of a fully functional VPLS environment [**36**], [**8**], [**42**], [**13**] and [**15**]

Table 4.2: LDP versus BGP attributes

Protocol	Advantageous attributes	Disadvantageous attributes
Label Distribution Protocol (LDP)	• Low complexity of implementation i.e. requires fewer protocol extensions to distribute labels. • Easier to establish VPLS over an existing MPLS network that is primarily based on LDP.	• Doesn't support auto-discovery of peer nodes • Has a low scalability option in case the network is expanding.
Border Gateway Protocol (BGP)	• Offers auto-discovery support to peering routers thereby enhancing the network's scalability. • Offers the SP lower network configuration workload through the option of having route reflectors with the network instead of having a fully meshed network	• BGP has a high complexity of implementation.

4.5.1 BGP Configuration

In Table 4.2, although BGP has a higher complexity of implementation while setting up a VPLS network, it is a better choice for service providers planning their networks. The reason being that as nodes in the network increase, BGP offers better scalability and PE peer discovery. The test bed setup draws advantages from both LDP and BGP in the setup of PWs in a VPLS network.

Figure 4.5 illustrates how the PE nodes in the network are connected. PE3 is the *route-reflect* router and it passes information learned from its neighboring router to the other routers i.e. PE1 interacts with PE2 through PE3.

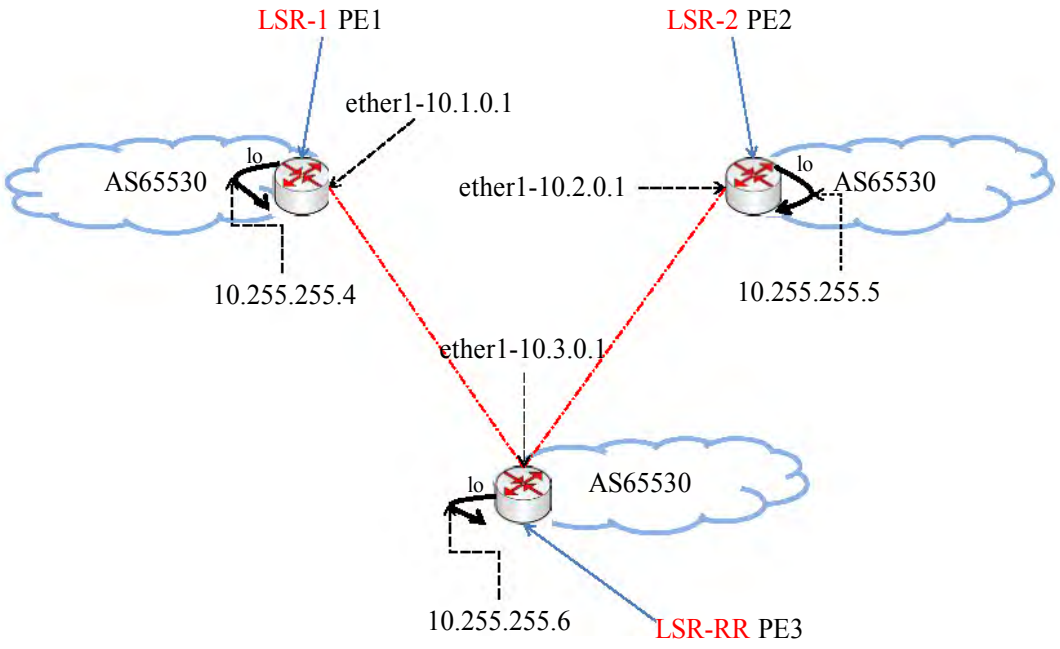

Figure 4.5: BGP Configuration

In the configuration of a virtual service instance on a PE to peer with other predetermined PEs, the BGP advertisement message contains the following next hops in the network as the loopback addresses of the participating PEs [**13**].In Figure 4.5, the route reflector PE3 is configured as follows.

```
[admin@PE3] > routing bgp peer add remote-address=10.255.255.4 remote-
as=65530 address-families=l2vpn \ update-source=lobridge
[admin@PE3] > routing bgp peer add remote-address=10.255.255.5 remote-
as=65530 address-families=l2vpn \ update-source=lobridge
```

From the BGP configuration, PE remotes to both PE1 and PE2 by using their assigned loopback addresses, however PE1 and PE2 can only remote to PE3 and not to each other [**66**]. By specifying l2vpn as the address-families setting, this ensures that the BGP multiprotocol feature delivers VPLS NLRI messages between peering routers. The update-source setting is a means by which the router's loopback (lobridge) interface is configured and acts as the BGP peering address, furthermore using the loopback address ensures proper PHP behavior as previously mentioned. The various BGP routers are configured with the same autonomous system (as) value to which they remote to, this also applies to PE1 and PE2.Having configured the BGP peering nodes, the route reflector instance on PE3 is enabled using the command line shown below.

```
[admin@PE3] > routing bgp peer set 0 route-reflect=yes
[admin@PE3] > routing bgp peer set 1 route-reflect=yes
```

Numbers 0 and 1 represent the routing instances to which routers PE1 and PE2 peer with PE3 respectively. Having configured the provider edge routers with BGP, the next step is to enable VPLS and setup dynamic pseudowires between the PE routers.

4.5.2 BGP Signaling for VPLS Instances

As previously stated VPLS is also known as a transparent LAN service, therefore bridging is required to transparently deliver the Ethernet frames across the VPLS network. To archive dynamic BGP VPLS tunnels that suitably exchange BGP NLRI information and maintain the transparent nature of VPLS, two bridges are created on the PE routers on the customer facing end [**66**]. This is done on all PE routers as they have different client-user end service needs

```
[admin@PE3] >interface bridge add name=A
[admin@PE3] > interface bridge add name=B
[admin@PE3] > interface bridge port add interface=ether9 bridge=A
horizon=1
[admin@PE3] >interface bridge port add interface=ether10 bridge=B horizon=1
[admin@PE3] >interfacevpls bgp-vpls add bridge=A bridge-horizon=1 route-
distinguisher=1:1 \
site-id=3 import-route-targets=1:1 export-route-targets=1:1
[admin@PE3] >interfacevpls bgp-vpls add bridge=B bridge-horizon=1 route-
distinguisher=2:2 \
site-id=3 import-route-targets=2:2 export-route-targets=2:2
```

The created bridges, A and B, correspond to the two different VPLS instances to which the client sites belong. The bridges are assigned to two PE Ethernet router interfaces ether9 and ether10. The bridge setting specifies to which bridge the dynamic VPLS tunnels are attached too. In the setting up of VPLS tunnels, split-horizon warrants loop avoidance through ensuring that packets received over a port are not flooded to another port with the same horizon value, thus in VPLS meshed networks the same horizon value is set to VPLS tunnels that are bridged together. The split-horizon value only acts locally and is not forwarded across the network; therefore it doesn't matter if the same value is used on all routers across the network [**66**].

To ensure that the routers distinguish VPLS NLRI messages that might look the same from different VPLS instances, the router-distinguisher attribute is different for the different client ends A and B. The import-route-targets match BGP NLRIs to their corresponding VPLS whereas the export-route-targets are used for tagging the BGP NLRI [**66**]. The site-id setting emphasizes the exchanged VPLS NLRI are unique [**36**]. Figure 4.6 illustrates the settings as discussed.

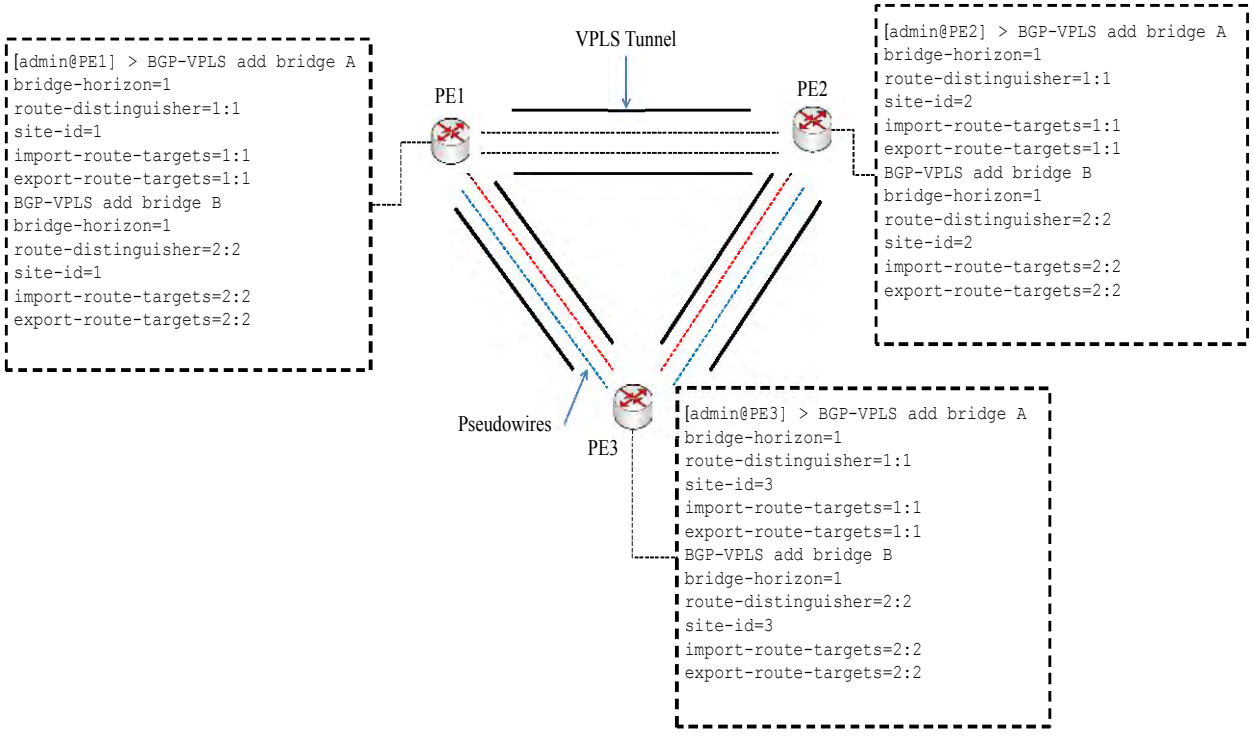

Figure 4.6: BGP-VPLS Setup

4.6 Traffic Engineered Tunnel Configuration

MPLS-TE tunnels are established using LDP and are independent of the services running over them, in this case VPLS [**36**]. Through having loopback addressing the tunnel endpoints are not affected by link state change and TE tunnels restrict PHP behavior in which packets can be dropped before reaching their intended destination [**68**].Constrained Shortest Path First(CSPF) is for tunnel path selection whereas, OSPF is used to distribute TE information.

```
[admin@PE3] > routing ospf instance set mpls-te-area=backbone mpls-te-
router-id=lobridge
[admin@PE3] > mpls traffic-eng interface add interface=ether1
bandwidth=100000000
```

The first command line above states that OSPF distributes MPLS traffic engineering information using the routers loopback address denoted by lobridge in the network area backbone. The second line states that through assigning PE3 interface ether1 (interface on router facing the network), the router is a participant in the TE tunnel. The interface is assigned a maximum bandwidth value of 100MBps; TE interfaces on the other routers are configured in the same order.

Once the TE interfaces have been configured, the TE tunnels are setup. Dynamic paths are used in the setup of the MPLS-TE tunnels in which the dynamically created VPLS PWs are interconnected to their respective PEs. A dynamic path template is created using CSPF in command line 1, then the tunnel is created as shown in the command line 2 below.

```
[admin@PE3] >mpls traffic-eng tunnel-path add use-cspf=yes name=dynamic
[admin@PE3] > interface traffic-eng add name=tepe3_to_pe1
bandwidth=83000000 primary-path=dynamic from-address=10.255.255.6 to-
address=10.255.255.4 disabled=no record-route=yes
```

Prior to the LAN traffic being routed over the TE tunnel, it traversed the VPLS network using the label switched paths that were created by the LSRs. Routing LAN traffic over the created TE tunnels entails the assignment of IP addresses to the MPLS-TE tunnels. LAN traffic over the tunnels can be achieved as shown below.

```
[admin@PE3] >ip address add address=10.99.99.6/30 interface=tepe3_to_pe1
[admin@PE3] > ip route add dst-address=10.10.0.1 gateway=10.99.99.5
```

In the above configuration “interface = tepe3_to_pe1” refers to the interface TE tunnel at PE3 that connects to PE1. The first line states that interface = tepe3_to_pe1 belongs to IP subnet 10.99.99.6/30. The second line states that the interface facing the client end (at PE1) with IP address 10.10.0.1 uses the TE tunnel with static IP address 10.99.99.5 as its gateway to reach router PE3, this is illustrated in Figure 4.7 below. A similar configuration is applied between PE3 and PE2.

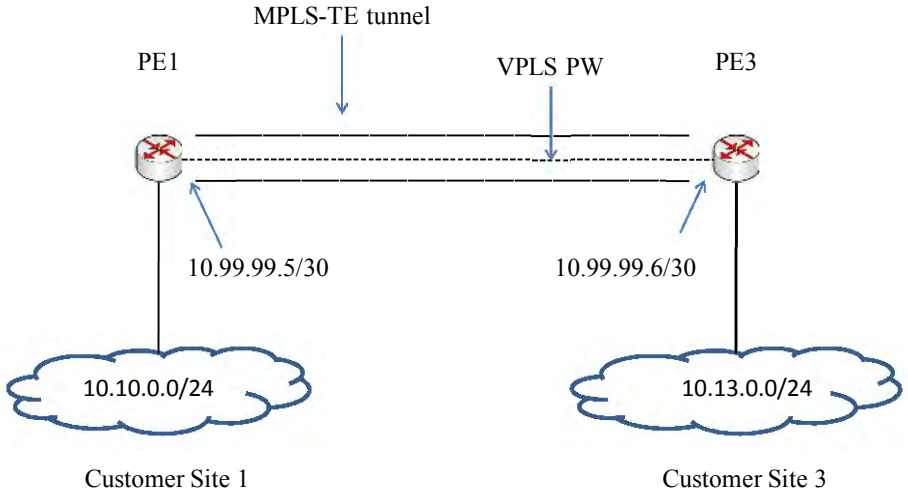

Figure 4.7: Point-to-Point TE Tunnel Setup

The confirmation of traffic traversing through the created tunnel is shown below in which a *traceroute* test verifies label encapsulation within the TE tunnel between client edge routers at customer site 3 and customer site 1

```
[admin@CE3_A] >tooltraceroute 10.10.0.1
 # ADDRESS           RT1    RT2    RT3    STATUS
 1 10.13.0.2         1ms    1ms    1ms
 2 10.3.0.254        2ms    1ms    1ms    <MPLS:L=53,E=0>
 3 10.0.255.1        1ms    1ms    1ms    <MPLS:L=42,E=0>
 4 10.99.99.5        1ms    1ms    1ms
```

The trace route run from customer site 3 to customer site 1 depicts label encapsulation within the tunnel is fully functional. From the result above, MPLS labels 53 and 42 were dynamically assigned to the data traversing the network using static IP 10.99.99.5 as their gateway address as previously mentioned. The dynamically setup VPLS PWs traverse the

network through the MPLS-TE tunnels as illustrated in Figure 4.7. Having achieved label encapsulation the next step is to setup the auto-bandwidth allocation within the MPLS-TE tunnels.

4.7 Auto-Bandwidth Allocation

As mentioned in Chapter 2 based on the amount of traffic flowing through a tunnel, auto-bandwidth management is able to ensure the adjustment or allocation of bandwidth within tunnels depending on the traffic patterns. Unlike having a 3rd party to adjust the tunnel bandwidth requirements, auto-bandwidth allocation guarantees no interruption of traffic flow in the tunnels.

In the test bed, auto-bandwidth allocation is performed by setting multiple timers at particular intervals to sample the traffic within the tunnel. Having set the sampling period, the tunnel's reserved bandwidth is adjusted, dynamically, depending on the maximum average value recorded in the previous sample.

However, prior to setting any interval times, the traffic traversing the network was monitored and the pattern realized was one with sudden bursts of traffic and a steady rise of traffic. This then brought forward the notion of setting the highest possible traffic on to the TE tunnel, sampling the traffic bandwidth every 1second and adjusting the tunnel's bandwidth every 1 minute.

A physical 100BaseT LAN cable connection between the host machines, in which the network nodes reside, meant that the maximum transfer speed is expected to be 100Mbps from the servers to the network and from the network to the clients. With this in mind a maximum value of 100Mbps is set on the tunnels.

The auto-bandwidth allocation minimum and maximum limits of the tunnel, from PE3 to PE1, are set from the ingress router as shown in the configuration below [**69**].

```
[admin@PE3] >interface traffic-eng
[admin@PE3] /interface traffic-eng> add name=tepe3_to_pe1 from-
address=10.255.255.6 to-address=10.255.255.4 bandwidth=100000000 primary-
path=stat auto-bandwidth-range=1000-100000000 \
auto-bandwidth-avg-interval=1s
auto-bandwidth-update-interval=1m
```

From the above configuration, the TE tunnel PE3 to PE1 is assigned a maximum bandwidth of 100Mbps which is also the limit that the physical LAN cables are able to transmit. Loopback IP addresses 10.255.255.6 and 10.255.255.4 belong to PE3 and PE1 respectively. The primary path "*tepe3_to_pe1*" is set as the static path as it was not dynamically setup.

Once the tunnel has been set, the auto-bandwidth values and parameters are then defined. The auto-bandwidth range of 1Kbps to 100Mbps defines the range of the amount of data through the tunnel. A sampling rate of 1second is used to collect an average rate of data through the tunnel. Having acquired the average traffic, an auto-bandwidth update interval of 1 minute adjusts the new reserved bandwidth to the highest recorded bandwidth average. It should also be noted that different sampling periods were taken into consideration as will be discussed in Chapter 5

By setting the maximum possible value to the tunnel/s ensures that incase of sudden bursts in traffic, a foreseeable problem like congestion which leads to packet loss is mitigated. The CSPF protocol, used for path selection, is invoked by the TE tunnel if and when the maximum traffic demand is greater than the existing reserved bandwidth but falls within the minimum and maximum set limits [**25**].

4.8 Summary

This chapter has presented the implementation of a multicast aware VPLS network created in a virtualized environment. Tools such as VMware environment and Mikrotik routerOS offer the building blocks to the setting up of the VPLS network. The VMware environment is a hypervisor that is used to setup and manage created virtual machines. From this hypervisor, which resides in the host machines, virtual machines are allocated optimal requirements needed by their guest operating systems.

Mikrotik routerOS is a guest operating system that resides in the virtual machines intended to be used as network routers. The Mikrotik operating system enabled the configuration of a VPLS active environment. In the setup of the network, the network core routers were configured with MPLS over which VPLS is implemented. Once the VPLS network had been setup, the

client sites were then added to the network. For the client sites, the Windows XP guest operating system is used in the server and client virtual machines. Figure 4.8 shows the resulting network topography, this was obtained using The DUDE network monitoring tool.

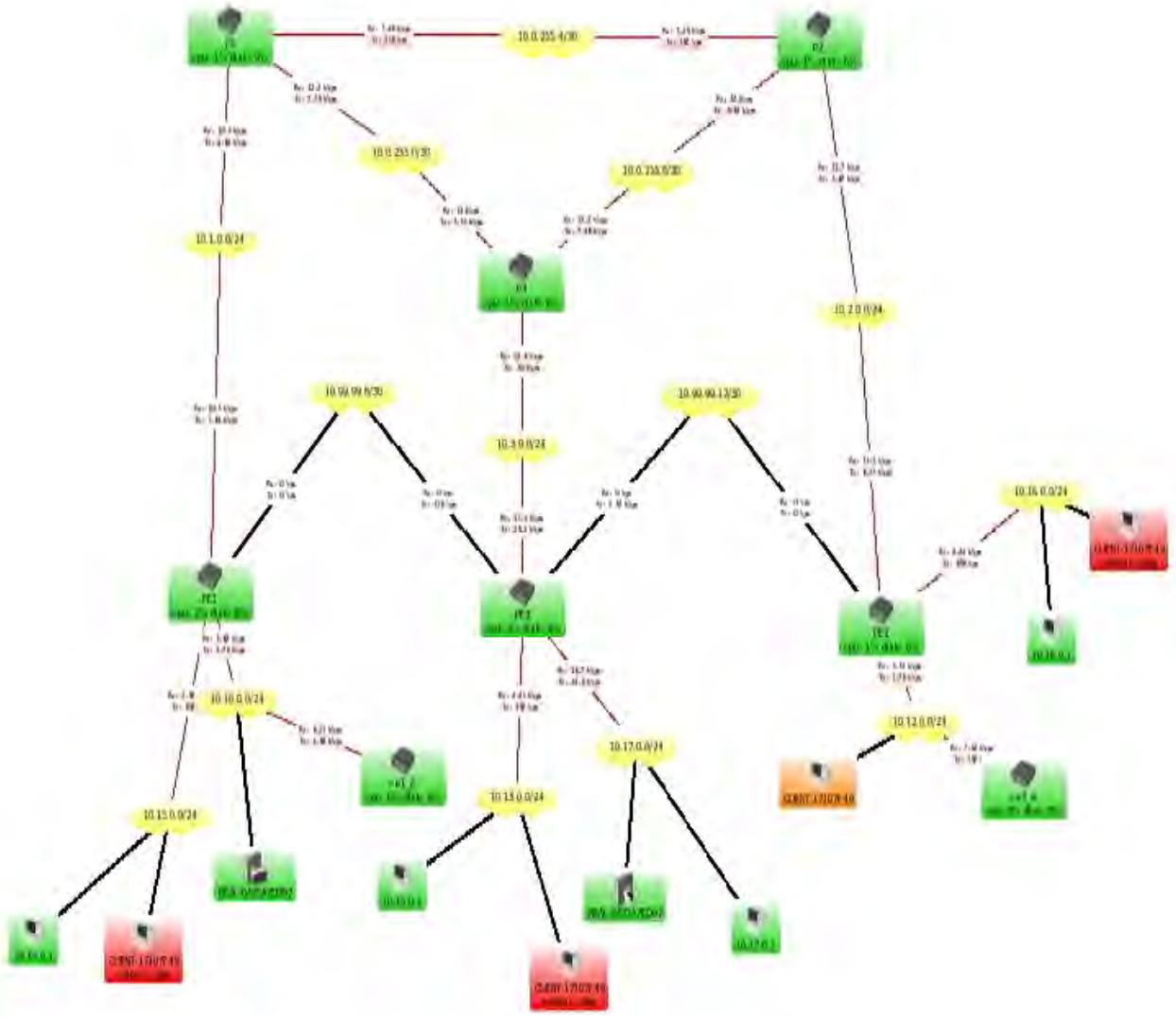

Figure 4.8: Network Topology

Figure 4.8 is a representation of all the network elements. Using The DUDE, it is easy to have an overview of the network and also identify nodes that are reachable, partially down or completely down. These states are represented by the colors green, orange and red respectively. The network subnets are represented by the yellow clouds whereas the pink clouds represent the node's interface traffic as represented in Figure 4.9.

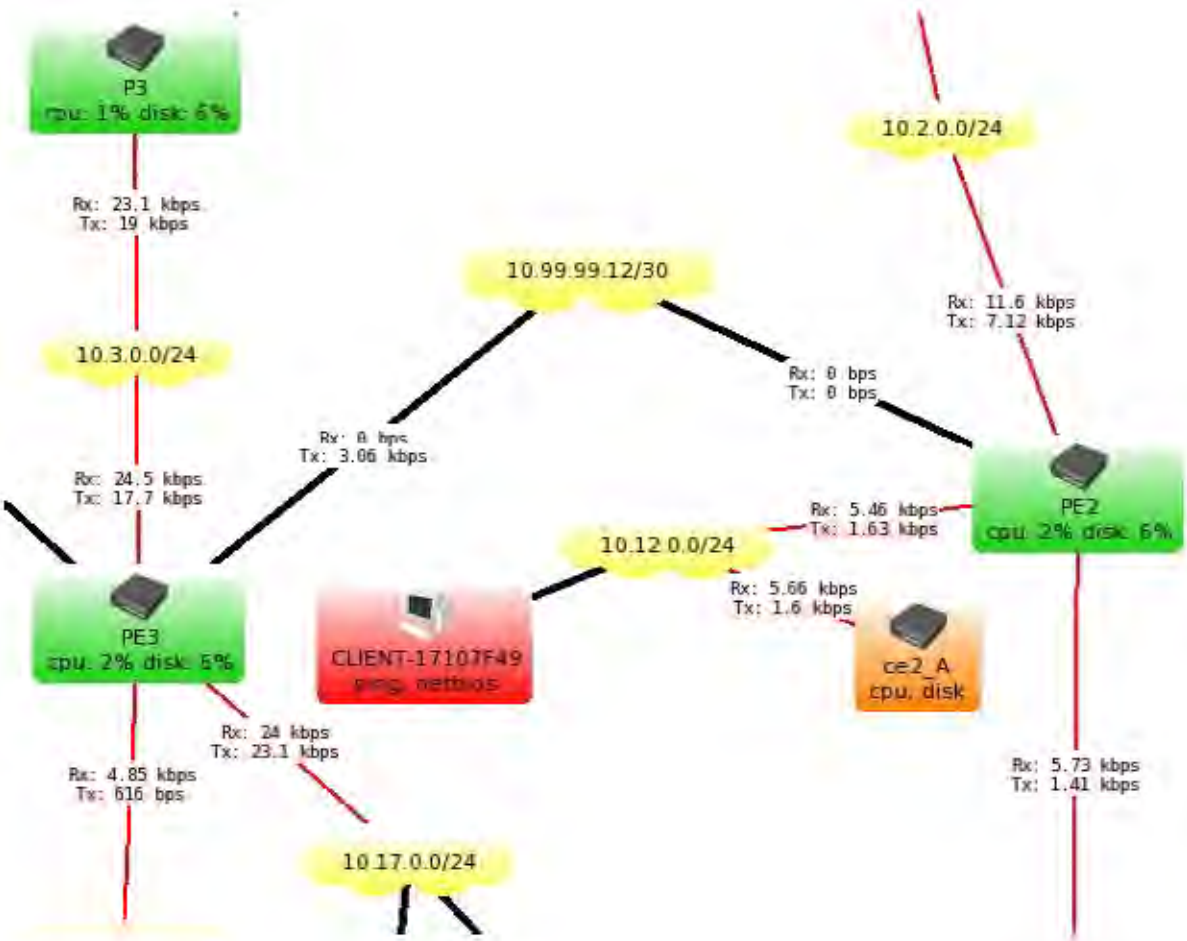

Figure 4.9: Network Links and Nodes

In Figure 4.9, the links denoted in the black and red colors represent LAN emulated links and network connections. The traffic shown in Figure 4.9 is signaling traffic between the network nodes. The VPLS network that is setup is multicast aware through the use of different VPLS instances in the network. Having setup the VPLS network, the traffic engineered tunnels are configured to offer bandwidth management across the network. Auto-bandwidth control is then established within the tunnels.Another monitoring tool used is Wireshark. This offers a wider range of output based results in both the control and data planes. These results are discussed in the following chapter.

Chapter 5 Application Aware Multicasting Performance

5.1 Introduction

This chapter presents the control plane results which are primarily based on signaling bits exchanged during the setup of the network. The performance metrics of the network in relation to the data plane are then presented and evaluated.

5.2 VMware Management Tool

The implementation of a multicast aware VPLS network as discussed in the previous chapter addresses how it can be realized in a virtualized environment. Figure 1 is a representation of the virtualized environment as previously discussed in Chapter 4.

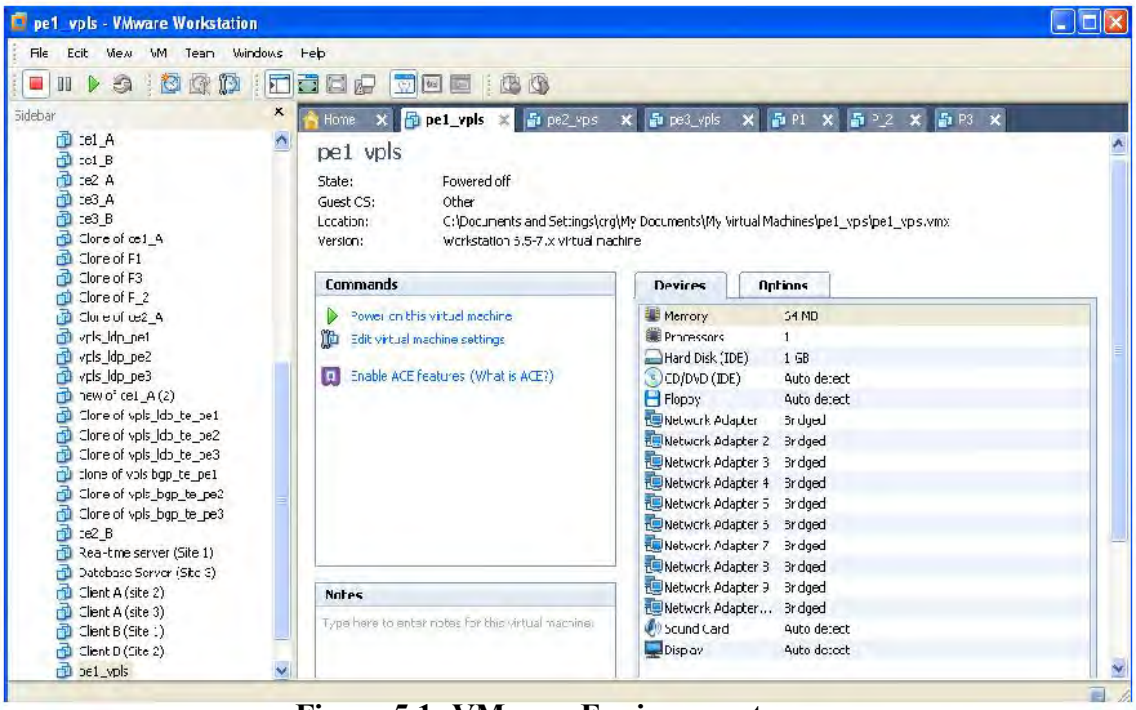

Figure 5.1: VMware Environment

The virtualized machine in Figure 5.1 is a VPLS network router. From this hypervisor, the router's: interfaces, RAM and processors are defined in relation to its host.

The previous chapter introduced monitoring tools essential in the evaluation of the established VPLS network. The performance of the VPLS network is based on existing quality of service (QoS) metrics used to appraise the validity of the network.

5.3 Control Plane Performance

In this section, control plane based signaling results are presented and evaluated.

5.3.1 OSPF Signaling Activity

Having setup the loopback addresses of the routers and configuring IP addresses on their interactive interfaces, the OSPF protocol is used to ensure the distribution of routing information amongst the routers forming the network.

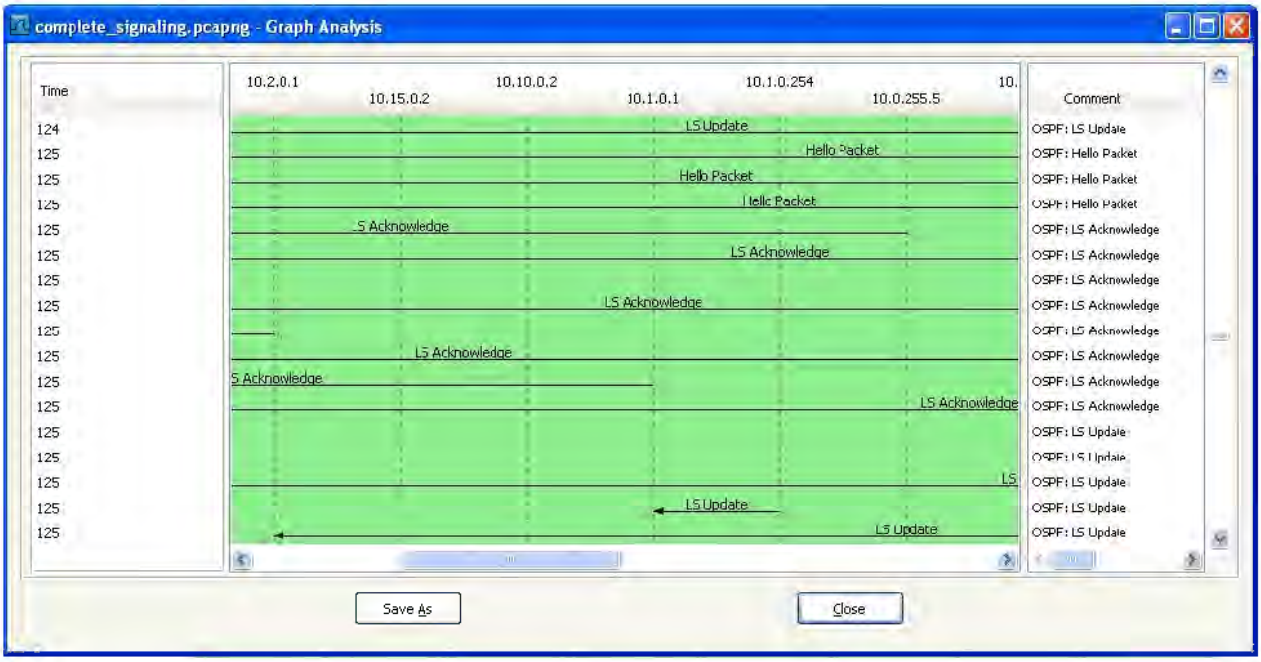

Figure 5.2: OSPF Interactions at Router Interfaces

Figure 5.2illustrates the interaction of the router interfaces in which routing information is exchanged. During the exchange of messages, OSPF sends five messages [**70**]:

- The “Hello” message - is used for neighbor discovery.
- Database (DB) description - is used to exchange topological information

- Link-state (LS) request - is used to request the neighboring routers for topological information.
- Link-state (LS) update - is used to reply to the LS request message.
- Link-state (LS) acknowledge - is used to acknowledge the receipt of a LS update message.

Figure 5.2 and Figure 5.3 are obtained by the Wireshark tool which captures the exchange of the signaling bits between the routers. Having captured such information, offline analysis of the messages can be achieved.

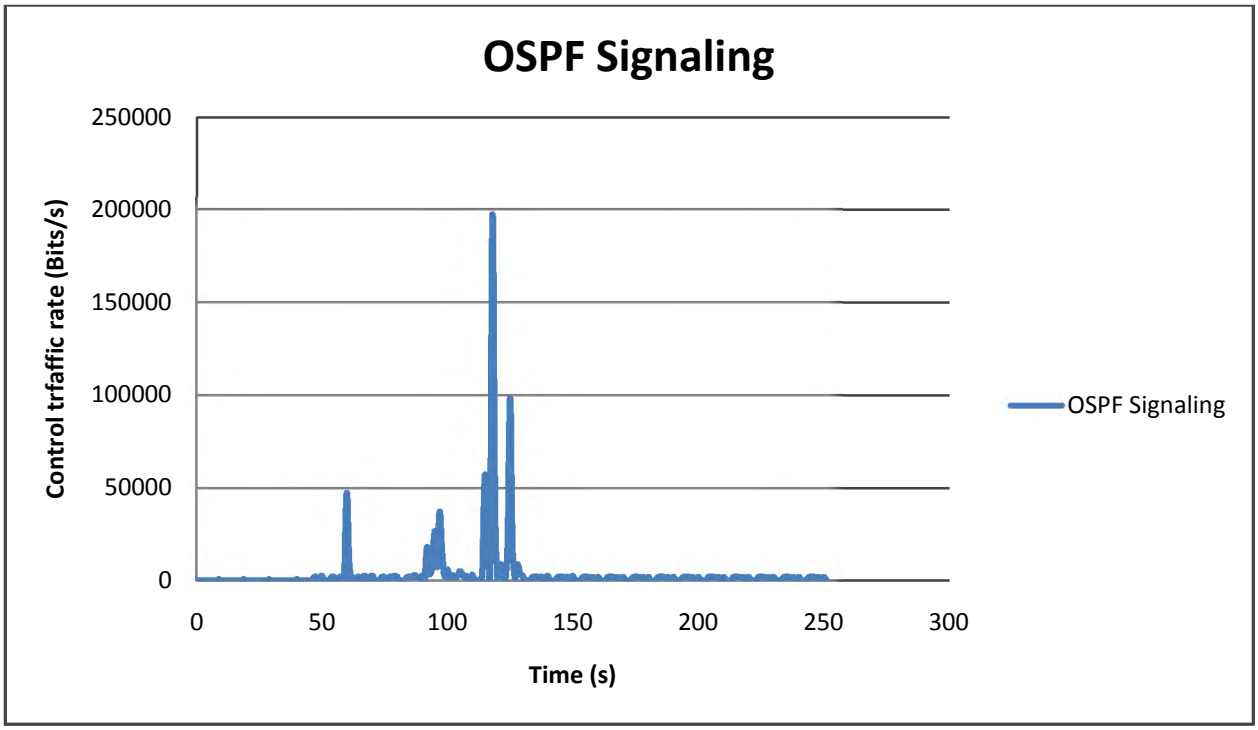

Figure 5.3: OSPF Signaling Traffic

In Figure 5.3, the signaling messages that were previously discussed are plotted as a function of utilized bandwidth (bits/s) against time in seconds. From this illustration, it can be seen that the routers in the network started exchanging OSPF information after 50 seconds and continued to do so for the entire duration of the networks up time. Hello messages are exchanged between 0-50 seconds. The first spike in the graph was due to the exchange of topological information. The pikes in-between the first and the highest illustrate the exchange of LS request, LS update and LS acknowledge messages. The highest spike is as a result of the exchange of Hello messages between the routers' participating interfaces.

Table 5.1: OSPF output

```
[admin@PE3] > routing ospf as-border-router print
 # ROUTERID         STATE      GATEWAY          COST
 0 10.255.255.1     intra-area 10.3.0.254       20
 1 10.255.255.2     intra-area 10.3.0.254       20
 2 10.255.255.3     intra-area 10.3.0.254       10
 3 10.255.255.4     intra-area 10.3.0.254       30
 4 10.255.255.5     intra-area 10.3.0.254       30
 5 10.255.255.6     intra-area                  0
```

Table 1: OSPF as-border-router Information

Table 5.1 illustrates the OSPF routing protocol in relation to PE3 and its peers. From this information, the OSPF cost metric is determined by the sum of the internal and external routes i.e. PE3 with address 10.255.255.6 has a cost of 0, the next hop is P3 with address 10.255.25.3 has a cost of 10, P1 and P2 (10.255.255.1 and 10.255.255.2 respectively) have a cost of 20 and PE1 and PE2 (10.255.255.4 and 19.255.255.5 respectively) have a cost of 30. The OSPF cost metric can also be expressed as a link state metric within the network.

5.3.2 LDP Signaling Performance

Having established OSPF routing within the network, MPLS is enabled using the LDP protocol. In a similar fashion, Wireshark was used to capture the LDP signaling between the participating router interfaces in the creation of LSPs within the network as shown in Figure 5.4.

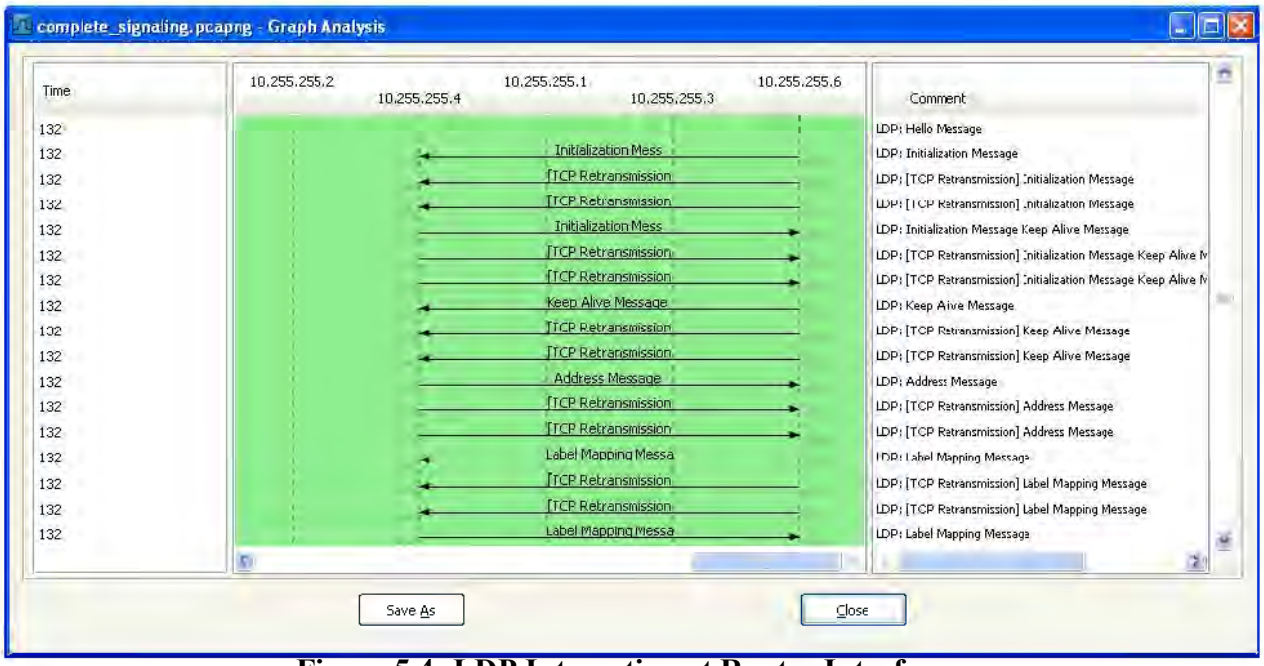

Figure 5.4: LDP Interaction at Router Interface

In Figure 5.4, during the setup of LSPs, the following signaling messages are exchanged [**11**]:

- Notification message - this informs the router of a an error caused by malformed or unknown messages.
- Hello messages are for discovering LDP adjacencies.
- The Initialization message is used for establishing LDP sessions between routing peers.
- Address and Withdrawal messages - these are used to advertise and withdraw the router's interface addresses.
- The Label Mapping message - is used by the router to advertise to its peers and to bind labels to their required FEC fields.

The exchange of the LDP signaling bits is captured and graphed as illustrated in Figure 5.5.

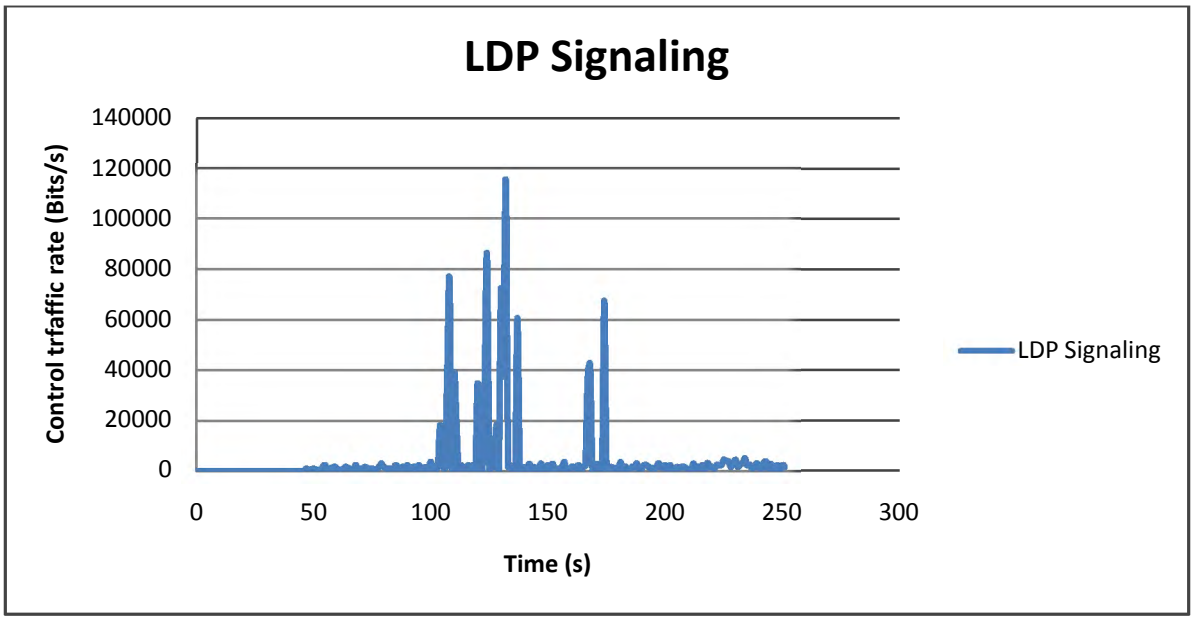

Figure 5.5: LDP Signaling Traffic

Figure 5.5 illustrates LDP signaling traffic. However when compared, Figure 5.3highest spike occurs at t≈ 60 whereas in Figure 5.5 the highest spike occurs after t ≈ 110s. Therefore LDP can only exchange initialization messages after OSPF has established the routes in the network, prior to which only Hello messages are generated at the router interfaces without them actually traversing the network.

The highest spike in Figure 5.5 corresponds to a label mapping message exchange between the routers. Once MPLS has been setup in the network Hello messages are constantly exchanged by the router interfaces .Having setup the label switched paths within the network, the BGP protocol is used to setup PWs that will form emulated LAN connections between the PE routers.

Table 5.2: LDP label encapsulation

```
[[admin@PE3] > tool traceroute 10.255.255.5
 # ADDRESS                                 RT1    RT2    RT3    STATUS
 1 10.3.0.254                              1ms    1ms    1ms    <MPLS:L=18,E=0>
 2 10.0.255.9                              1ms    1ms    1ms    <MPLS:L=16,E=0>
 3 10.255.255.5                            1ms    1ms    1ms
```

As previously stated, LDP is responsible for the encapsulation of frames in an MPLS network. Table 5.2 illustrates a trace route to PE2 with address 10.255.255.5 from PE3 with address 10.255.255.6. From the trace route table it is shown that labels are used to encapsulate the trace route frames, thus the network is MPLS enabled.

5.3.3 BGP Signaling Performance

In the setting up of the VPLS pseudowires, the BGP protocol is used to ensure that there is scalability in the network and dynamically creates PWs. There are two VPLS instances which are created and it is by these instances that the different clients requesting for different services are able exchange information reliantly. Under the BGP protocol, the notion of split horizon ensures that there is loop avoidance within the network, for example, even though the PE routers belong to the same VPLS instance, they (PE routers) will not flood the network with frames previously forwarded to them by their peering routers.

Figure 5.6 illustrates the previously presented notion of using route reflection or a *route reflect* router/s within a VPLS network for purposes of scalability

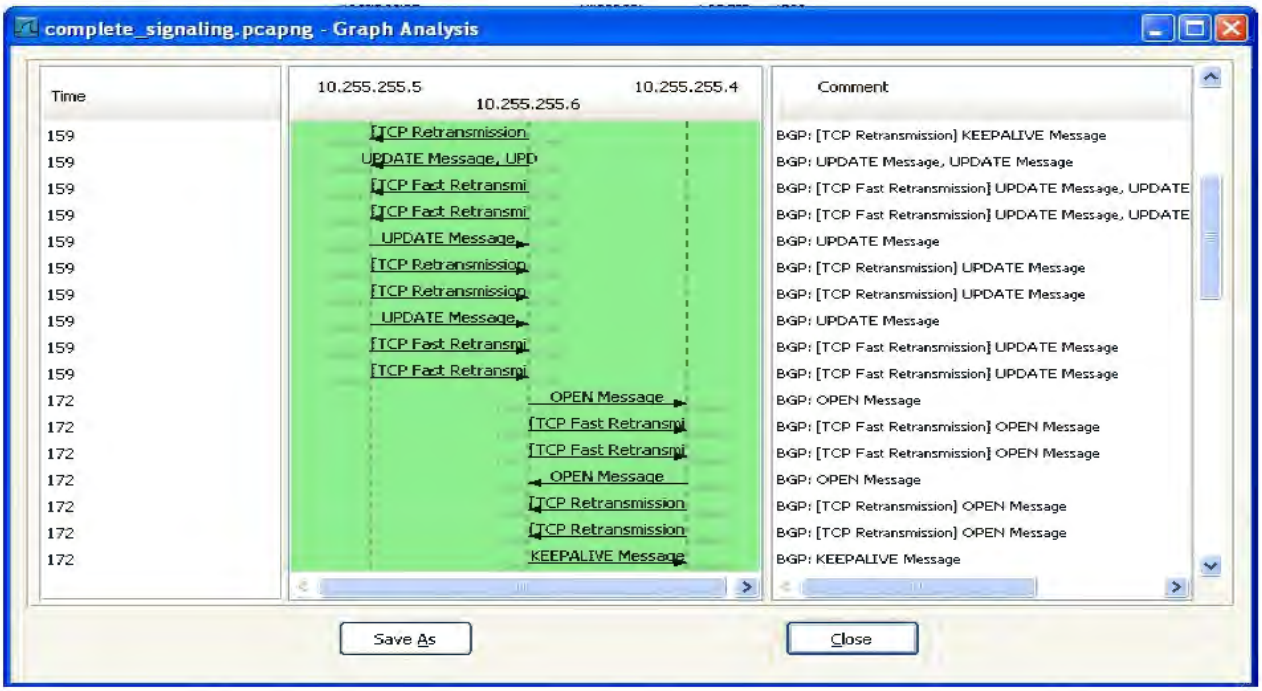

Figure 5.6: BGP interactions at router interfaces

In the illustration above, loopback addresses 10.255.255.4 and 10.255.255.5 belong to routers PE1 and PE2 respectively whereas 10.255.255.6 belongs to the *route reflect* router PE3. As shown in the illustration PE1 and PE2 only peer with PE3 and not with each other while PE3 peers with both PE1 and PE2.

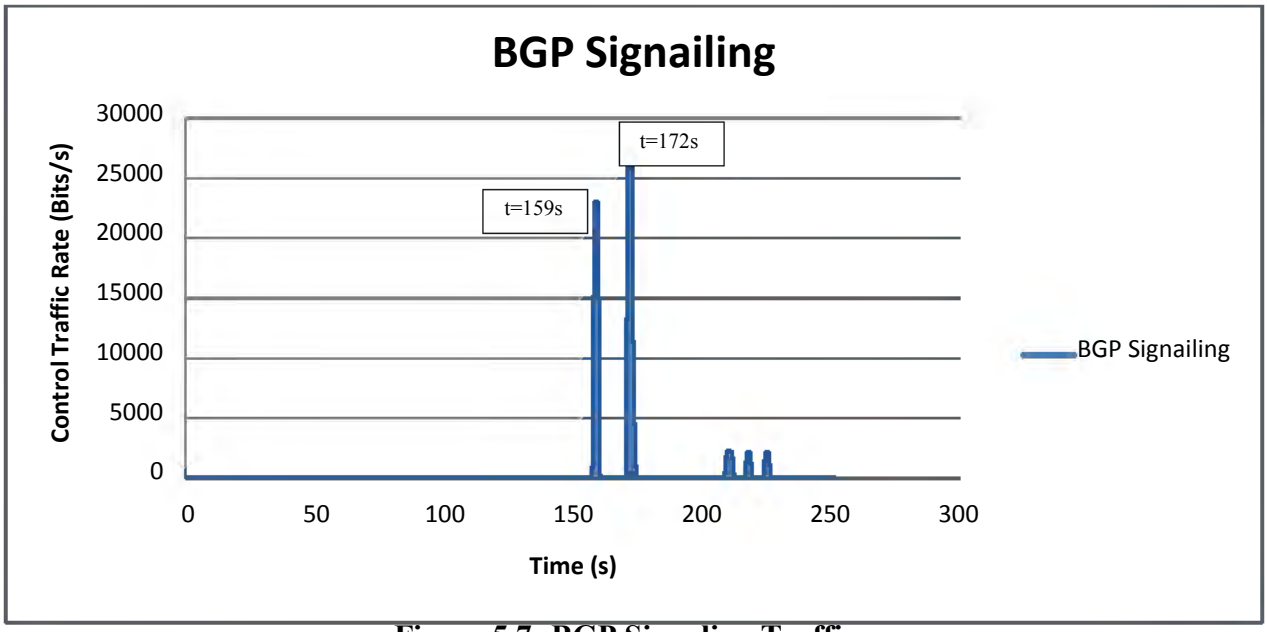

Figure 5.7: BGP Signaling Traffic

From Figure 5.6, the signaling bits between the peering routers were captured and illustrated in Figure 5.7. In the configuration of BGP within the router, the BGP Hold Time is left at its default value of 3minutes. It is this default hold time that the dynamically setup PWs were stable and most importantly the BGP peer connection wasn't lost. Losing the BGP peer connections would mean that there wasn't a successive order in which the control messages were sent.

Comparing the time stamps depicted in Figure 5.6 and Figure 5.7, they verify the successive order of the exchanged BGP messages by the two highest spikes at t=159s and t=172s. The exchanged BGP messages shown in Figure 3 are similar to those explained in Chapter 4.

Table 5.3: BGP peers of router PE3

```
[admin@PE3] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE       REMOTE-ADDRESS       REMOTE-AS
 0 E default       10.255.255.4          65530
 1 E default       10.255.255.5          65530
```

Table 5.3 illustrates the established BGP states between PE3 and its peers PE1 and PE2 represented by addresses 10.255.255.4 and 10.255.255.5 respectively. The provider edge routers are configured with the same autonomous system (AS) value of 65530 to which they remote to, as they are configured with different site identifications.The result of using BGP to establish the VPLS PWs results in the creation of dynamic pseudowires as illustrated in Table 5.4.

Table 5.4: VPLS based BGP pseudowires

```
[admin@PE3] > interface vpls print brief
Flags: X - disabled, R - running, D - dynamic, B - bgp-signaled, C - cisco-bgp-
signaled
 #     NAME     REMOTE-PEER      VPLS
 0 RDB vpls1     10.255.255.5   bgp-vpls1
 1 RDB vpls2     10.255.255.5   bgp-vpls2
 2 RDB vpls3     10.255.255.4   bgp-vpls1
 3 RDB vpls4     10.255.255.4   bgp-vpls2
```

Table 5.4 shows four different dynamically setup PWs in a VPLS environment.Similarly, all the other PEs (1 and 2) also have their PWs setup as PE3.

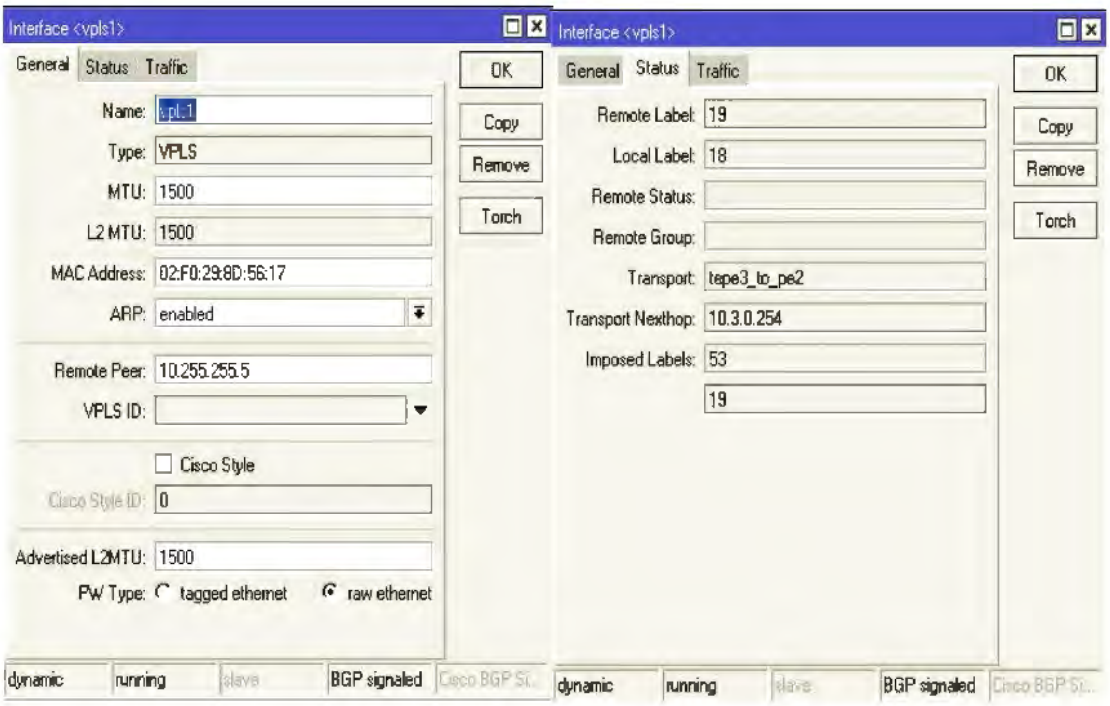

Figure 5.8: PE3 VPLS Interface-1

Figure 5.8 shows screen shots of a VPLS-PW on the interface of PE3, which illustrates the general nature and the status of the PW. The PW shown remotes with PE2 (10.255.255.5) and uses the MPLS-TE tunnel as its transport protocol. If the MPLS-TE tunnel had not been created then the PW would utilize the label switched paths (LSPs) created by the LDP protocol in the LERs.

The maximum frame size that can be sent out by this interface, without a MAC header, is 1500. This value is the maximum L2MTU also known as the Layer 2 Maximum Transmission Unit.In reference to RFC 4448, an Ethernet PW operates in two modes: raw mode or tagged mode. The setup PWs all operate in raw mode, they are dynamic and BGP signaled as shown in Figure 4. In raw mode, a frame is encapsulated and transparently transported over the PW to its destination. Whereas in tagged mode the PWs' endpoints must know how to process frames with tags. The remote label 19 is retained by the router whereas the local label 18 is attached to frames leaving the VPLS interface as shown in Table 5.2.

5.4 Multicast Awareness Performance

These data plane results seek to validate the reliability of the VPLS network. Through these results the efficiency of the VPLS network and its multicast awareness attribute are evaluated.

5.4.1 Topology Auto-Discovery for Multicasting

In the control plane the BGP protocol facilitates the auto-discovery of PE routers that participate in the same VPLS instance. The PWs in the VPLS instance are based on BPG and this ensures that they (the PWs) can be dynamically setup as interfaces on the PE routers. The PWs form the data plane in which VPLS traffic is sent to other PEs. Figure 5.9 below illustrates the auto-discovery notion in which an existing link is disabled during the transfer of traffic.

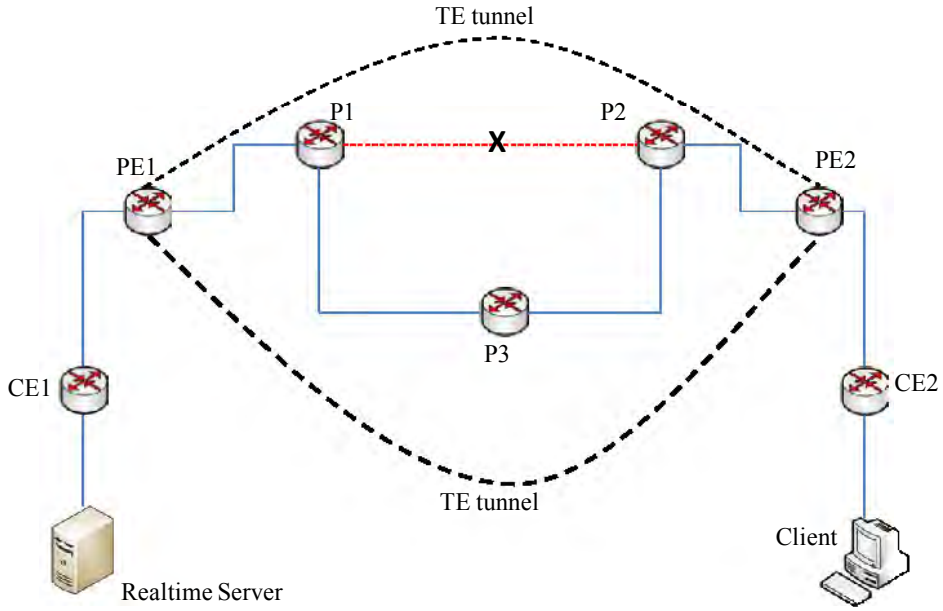

Figure 5.9: BGP peer auto-discovery

Figure 5.9illustrates a link failure between P1 and P2, which are LSRs. PE1, P1, P2, P3 and PE2 are MPLS enabled routers which form the label switched path through which label

encapsulated frames are transported in the network. With the introduction of VPLS PWs, connection between peering PE routers is made with the PWs. The PWs make the connection through the existing LSPs. However since MPLS-TE tunnels are used in the test bed, the PWs automatically use them instead of the LSPs. This offers the SPs more control over traffic and resources in the network such as bandwidth.

Having disabled the P1-P2 link, the BGP protocol ensures that PWs are dynamically established and are transported through the MPLS-TE tunnel PE1-P1-P3-P2-PE2. Therefore auto-discovery property allows the VPLS aware devices to learn about similar devices on the same VPLS instance. In so doing, frames are exchanged and a degree of connectivity is maintained. Figure 5.10 illustrates traffic continuity during the link failure.

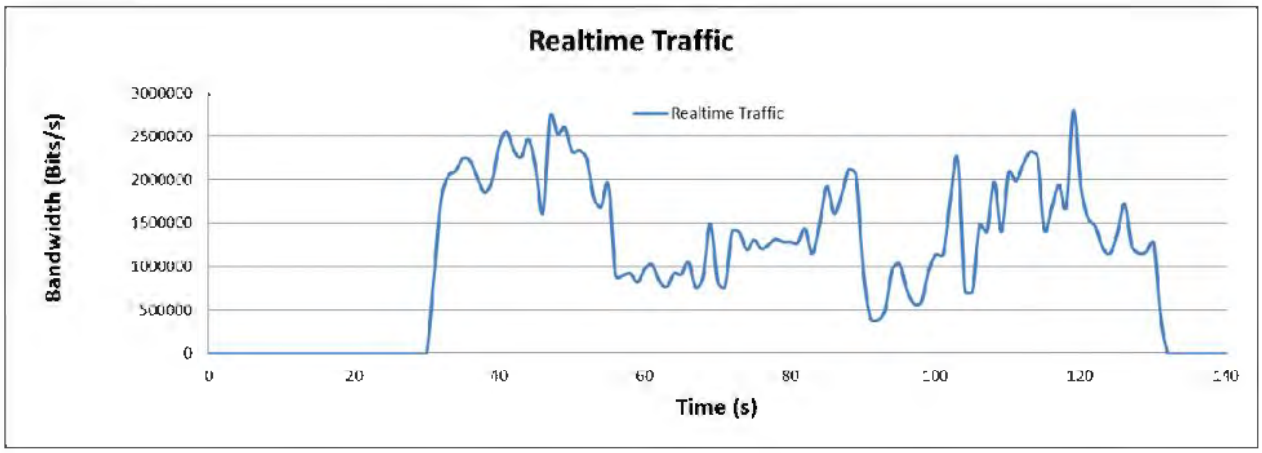

Figure 5.10: Real time traffic profile during auto-discovery

The real time traffic was generated by a VLC server connected to CE1.

5.4.2 Multicast Metrics

The multicast awareness aspect of VPLS reduces the number of similar frames to be replicated to other destinations by the source. This reduces the traffic load on the network thus efficiently utilizing the available bandwidth. Replication of frames to different client sites occurs closest to the client site that has requested the application or service.

Some of the metrics used for the multicast awareness performance evaluation include:

- Ingress replication
- High traffic rate throughput
- Auto-bandwidth budgeting
- Quality of service

These are discussed in later sections of this chapter.

Ingress replication of frames to the different client sites occurs at the nearest possible node, which is PE3. The server and client sitesbelong to the same VPLS instance. PE3 is the only replication point which reduces bandwidth wastage in the network when client-end nodes at PE1 and PE2 request for data from client-end at PE3, as shown in Figure 5.11.

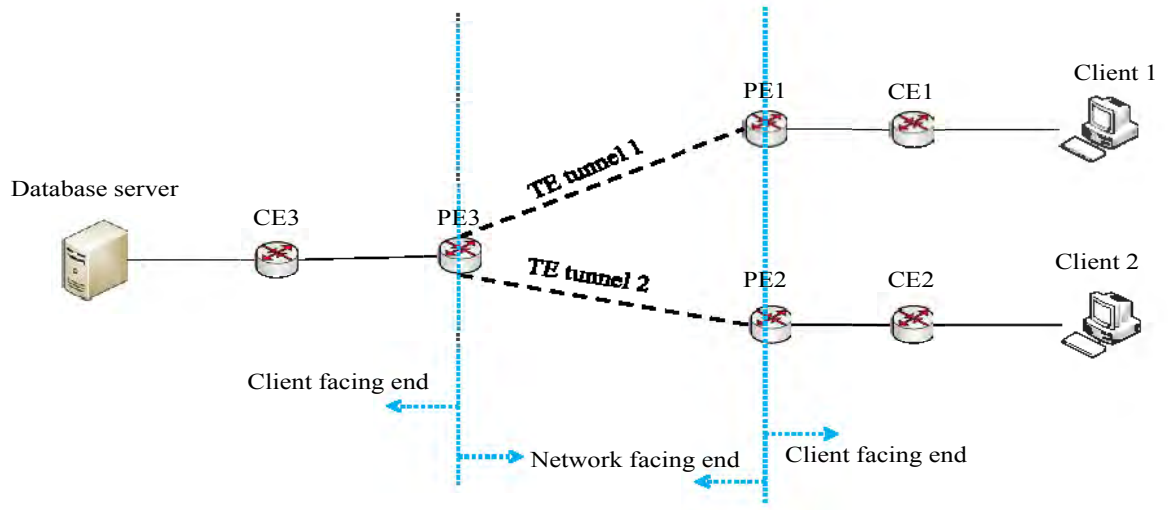

Figure 5.11: VPLS aware multicasting

In order to achieve multicasting, it is important that multicast members belong to the same group. That is why in the setup of the VPLS test bed environment, care was taken to assign the same import-route-target value to the router's interface belonging to a particular VPLS instance. Having specified the import route target value to an interface, this interface is then

bridged to the client facing end router.Figure 49 depicts the traffic flow from a server to router CE3 and then to the network router PE3.

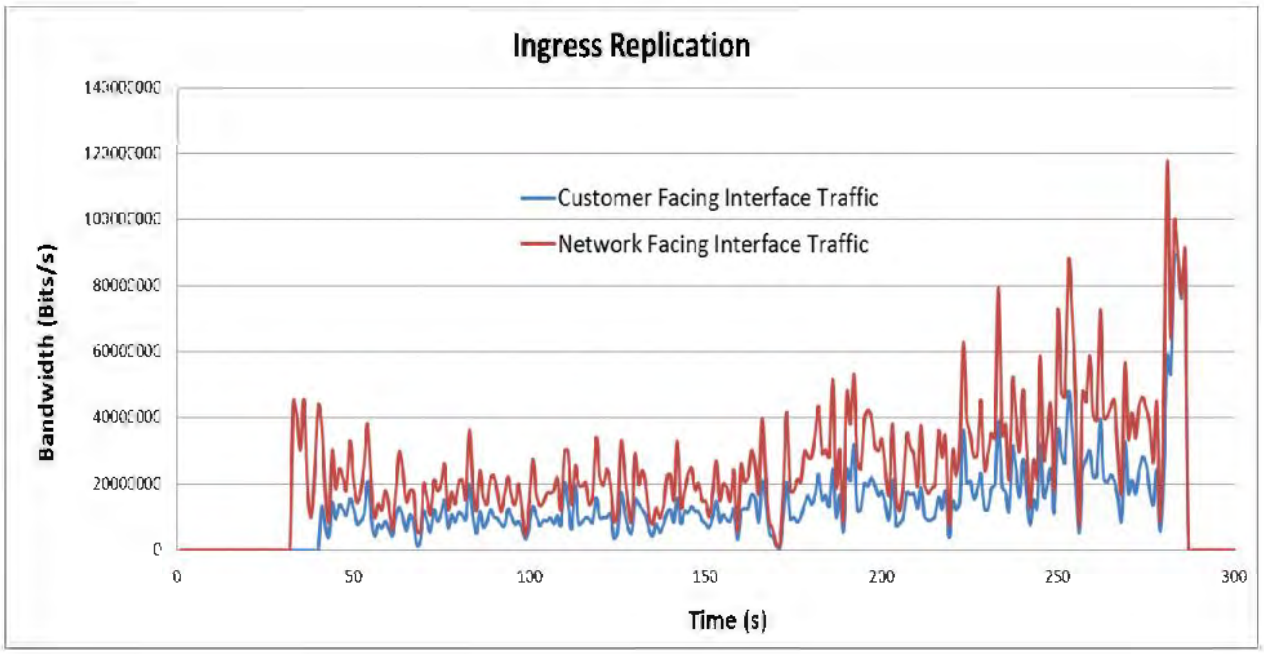

Figure 5.12: Ingress replication traffic profile

From Figure 5.12, it is shown that the traffic on the client facing end of router PE1 is approximately half that of the traffic on the network facing interface of router PE3. This implies that there is ingress replication at router PE3. However, if the replication had occurred prior to reaching router PE3, this would mean that the clients' bandwidth requirements would have to be increased to facilitate the transfer of the frames. Therefore by having the replication of the frames within the network and close to the destinations, leads to lower bandwidth costs for the client and utilization of the available bandwidth within the network. Figure 5.13 below shows the network facing traffic values from PE3.

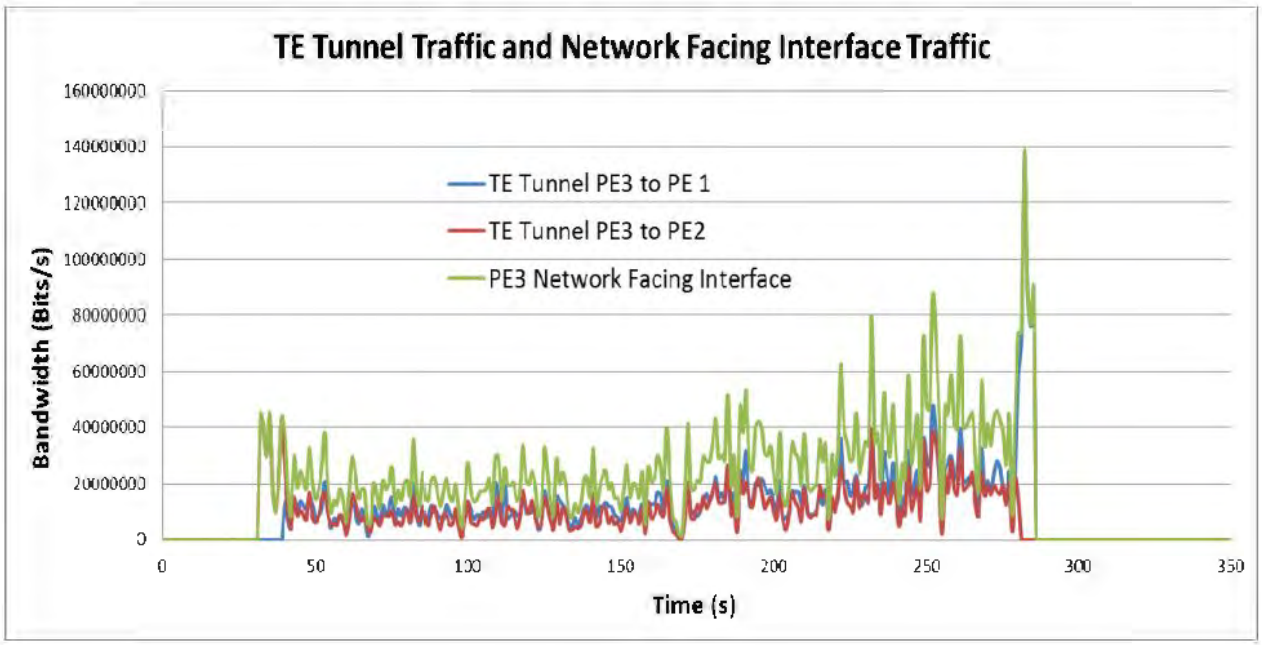

Figure 5.13: VPLS aware multicast traffic profile

Figure 5.13 illustrates the different amounts of traffic that is entering the network. The highest bandwidth is a representation of the traffic on the physical interface of router PE1. That means the other bandwidth traffic profiles represent the frames going through the MPLS-TE tunnels in the VPLS network. It is not possible to have a combined value of traffic volume over the two tunnels being greater than that of the actual interface at PE3, this is because they are connected to virtual interfaces and it is not possible to have virtual traffic greater than the actual traffic. Therefore it is suffice to say that the traffic over the physical interface is approximately equal to that over the tunnels. Having this kind of traffic traversing the tunnels is advantageous in that it offer the SP control of how to manage it as will be discussed in the subsequent section under auto-bandwidth allocation.

5.4.3 Auto-bandwidth Allocation

As previously discussed auto-bandwidth allocation offers control of traffic traversing the tunnels. In the VPLS test bed, the traffic was initially learned and this offered an insight into how and what kind of adjustment settings will be implemented to automatically adjust the bandwidth within the tunnels. By setting these adjustments, the tunnels are able to dynamically change their

bandwidth allocation within the tunnels. Figure 5.14 is a representation of TE tunnels that can be used to control multiple time intervals in a multicast aware VPLS network.

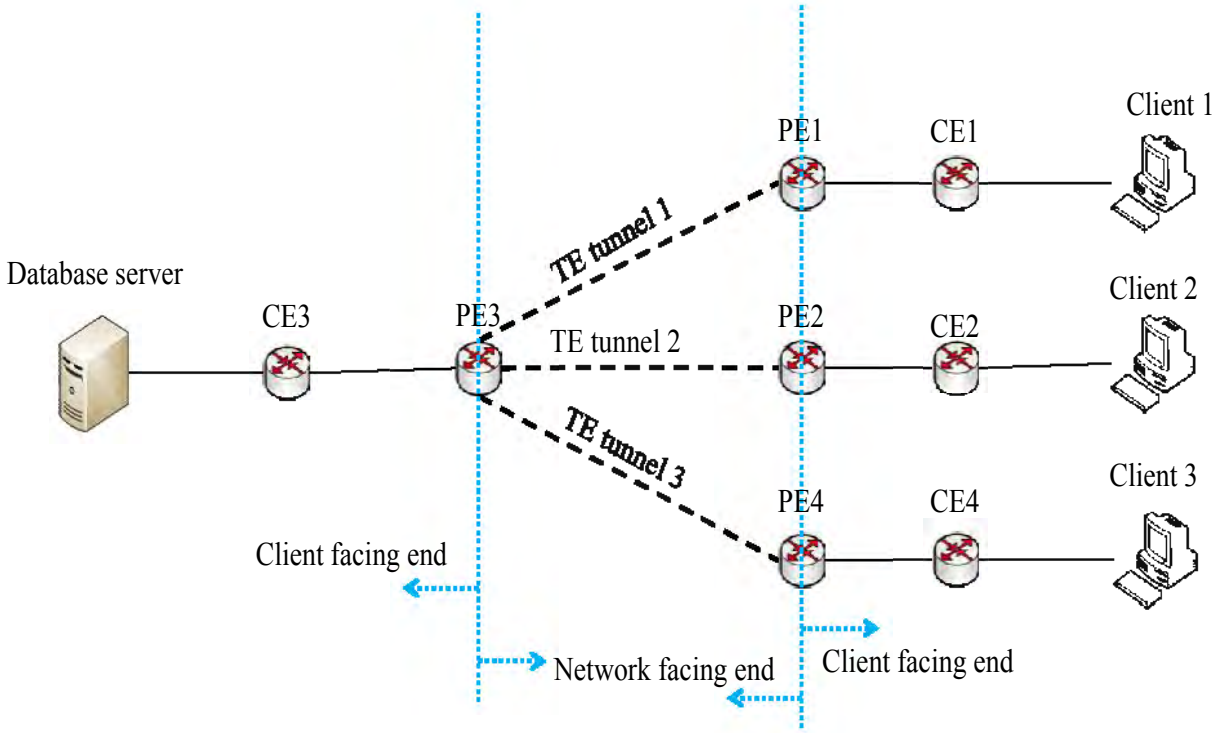

Figure 5.14: Auto-bandwidth allocation in a multicast aware VPLS network

VPLS as stated offers Ethernet type connectivity therefore it is able to deliver high volumes of data to its enterprise clients. Taking this into consideration it is important to avoid instances in which the allocated bandwidth is not sufficient thus leading to either network congestion or dropping of some frames. Figure 5.15 is a representation of a short time interval in which frames are dropped in the network.

The MPLS-TE tunnels are configured with different interval times for their reserved bandwidth will automatically adjust depending on the highest sampled rate, in relation to their respective adjustment intervals. The sampling rate of 1second is standard across all tunnels however the adjustment period is different. Tunnel 1 has an adjustment period of t=30seconds. Tunnel 2 has an adjustment interval of t=60seconds. Tunnel 3 has an adjustment interval of t=90seconds.

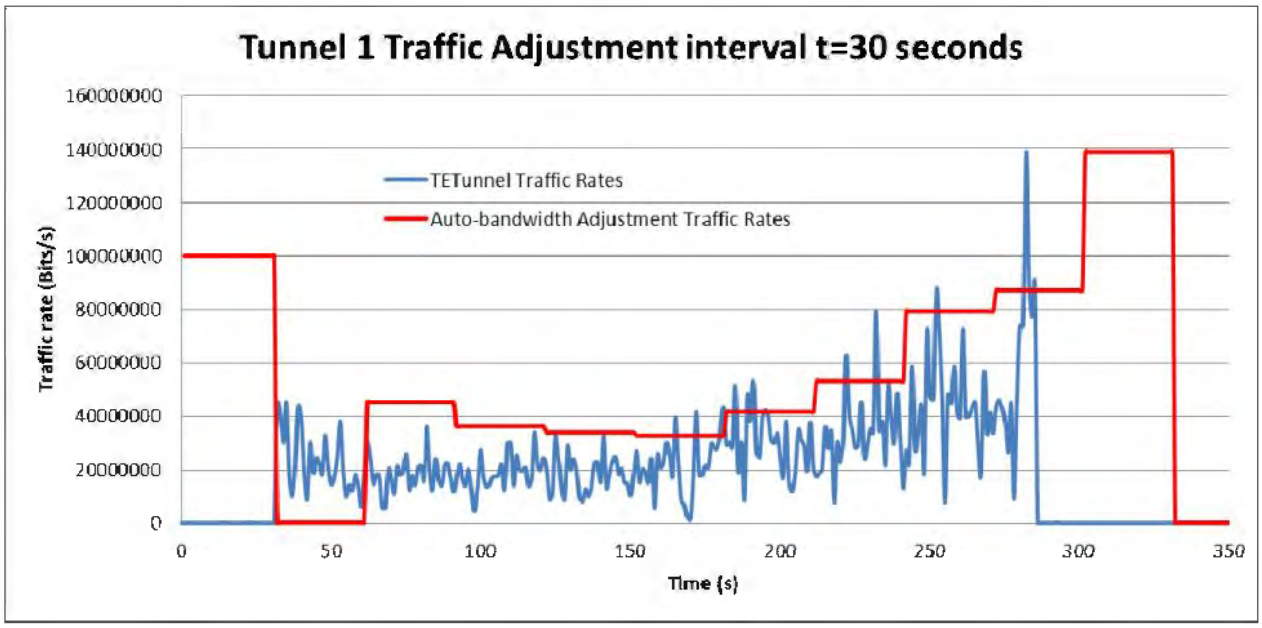

Figure 5.15: Auto-bandwidth timer t = 30 seconds

The time interval in tunnel 1 is set to t = 30 seconds. It is however noted that there are intervals in which the reserved bandwidth is less than the actual traffic rate in the tunnel. This in turn leads to frames being dropped in the network. However in Figure 5.16, the auto-bandwidth interval in the tunnel was set at t = 60 seconds.

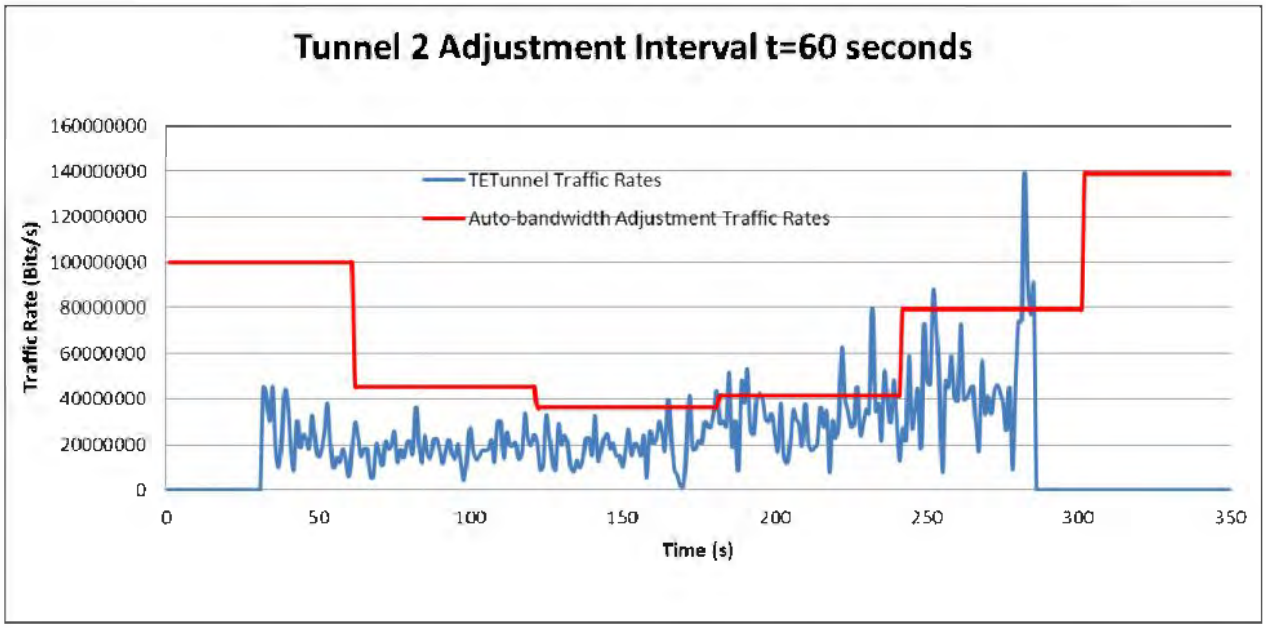

Figure 5.16: Auto-bandwidth timer t = 60 seconds

Comparing Figure 5.16 to Figure 5.16 shows that the reserved bandwidth is sufficient for the traffic rates in tunnel 2. However even though there are instances in which the traffic rate is higher than the reserved limit, tunnel 2 drops less frames compared to tunnel 1.

Figure 5.16 is a diagrammatic representation of the traffic at the TE tunnel interface of PE3 and the bandwidth adjustment at the same interface. The interface traffic was captured using the Wireshark monitoring tool. The adjustment of the bandwidth was also noted monitored by the Mikrotik router as shown below.

```
[admin@PE3] >interface traffic-eng monitor 0
tunnel-id: 1
primary-path-state: established
primary-path: dynpe3_to_pe1
secondary-path-state: not-necessary
active-path: dynpe3_to_pe1
active-lspid: 2
active-label: 121
explicit-route:
"S:10.3.0.254/32,S:10.0.255.2/32,S:10.0.255.1/32,S:10.1.0.254/32,S:10.1.0.1
/32"
recorded-route: "10.0.255.2[121],10.1.0.254[132],10.1.0.1[3]"
reserved-bandwidth: 52.3Mbps
rate-limit: 61.7Mbps
rate-measured-last: 45.3Mbps
rate-measured-highest: 46.3Mbps
```

The above Mikrotik based result agrees with a point in time t=100s on Figure 5.16. Monitoring the tunnel's behavior using Mikrotik gives an insight into the labels attached and the route the traffic traverses. It also shows the relationship between the reserved bandwidth and the rate limit, the later will always be higher than the former. From the Mikrotik result, in the next interval the reserved bandwidth in the next interval will be highest recorded average form the previous interval.

The auto-bandwidth allocator in the tunnel ensures that that the maximum recorded mean is set as the next bandwidth reservation value in the subsequent interval. In the implementation of the auto-bandwidth parameters, as mentioned earlier, a sampling period of one second and an adjustment interval of one minute are set. These were seen as optimal parameters in the way in

which the adjustment interval was not too short that would consequently lead to packets being dropped in case of sudden spikes in the data flowing through the tunnel.

The adjustment period is not too long such that it would lead to bandwidth underutilization i.e. in the case of a high reserved limit in which there is minimal use of the allocated bandwidth. As shown in Figure 5.17.

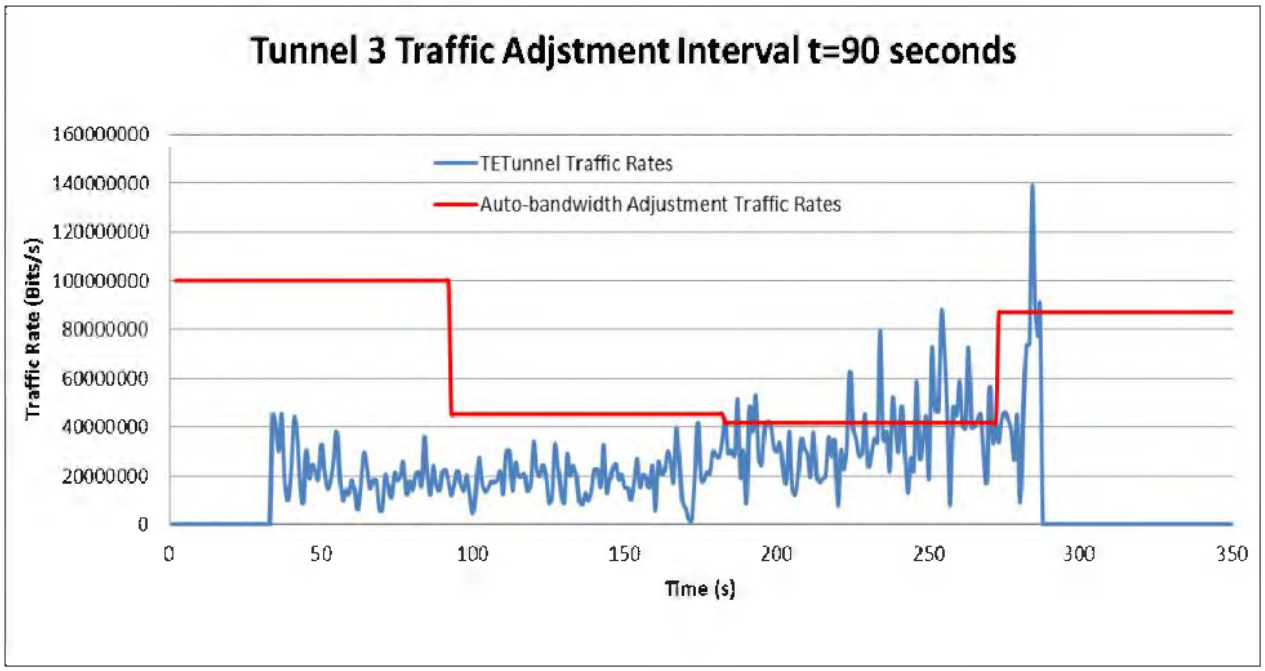

Figure 5.17: Auto-bandwidth timer t = 90 seconds

Comparing tunnel 3to tunnels 1 and 2 shows that the largest time interval leads to underutilization of the reserved bandwidth. More so there are also instances in which the reserved bandwidth is less than the traffic rate in the tunnel.

From the above comparisons, it is noted that tunnel 2 is the most efficient when it comes to bandwidth utilization amongst all the 3 tunnels. Having achieved auto-bandwidth allocation within the tunnels, the performance of the traffic traversing the network is monitored to validate its quality of service delivery.

5.4.4 Classical QoS Performance Metrics

QoS parameters ensure the delivery of services across a network. The availability of bandwidth coupled with the availability of network nodes and routes offer delivery of frames across the network. Figure 5.9 and 5.10 in the previous sections showed that the delivery of real-time traffic was not affected by the link disconnection between P1 and P2. However, it is important to know the behavior of frames traversing the network. A performance metric such as jitter offers an insight into how real time applications, such as voice traffic, are handled. Jitter is termed as the average deviation from the network's latency. Network performance metrics are determined by the jitter value [**33**]. The results represented by Figure 5.18 illustrate the amount of jitter within the network when a link is disabled during the streaming of video traffic.

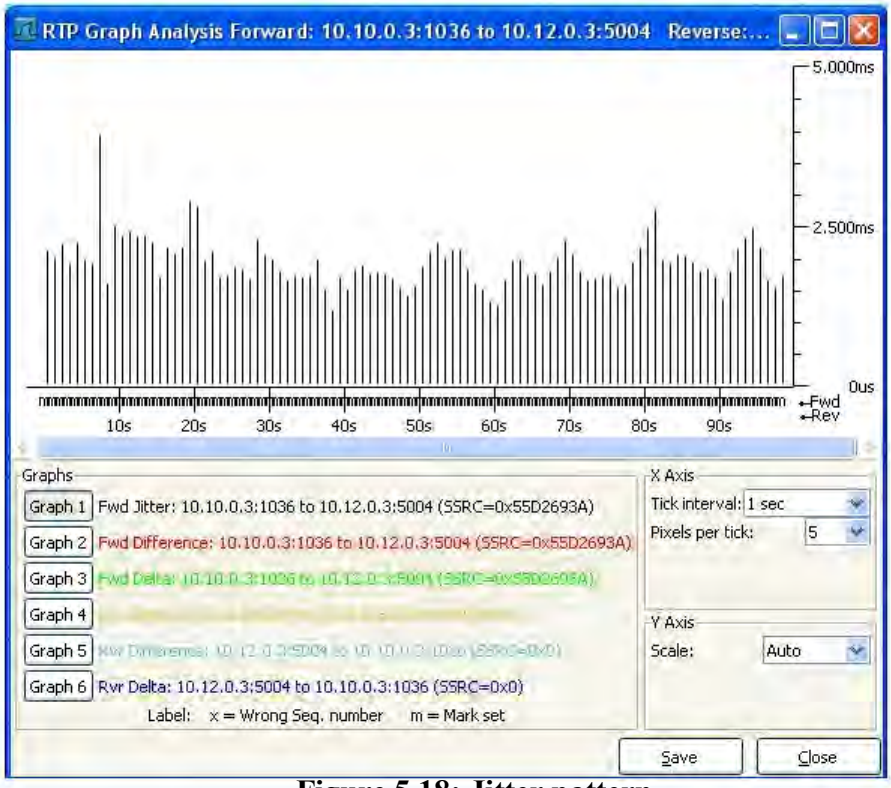

Figure 5.18: Jitter pattern

Figure 5.18 was obtained from an RTP stream and with the aid of Wireshark. During the RTP stream the link between P1 and P2 was disabled, similar to Figure 5 and the traffic was monitored. The average jitter recorded is low and this suggests a high quality of service delivery for real time traffic even though there is link disruption in the network.

VPLS networks are susceptible to delay with the tunnels that deliver the service(s) to their destination. The delayed delivery of frames coupled with insufficient bandwidth leads to frame loss or packets being dropped in the network. Figure 5.19 shows the total RTP stream analysis of the frames traversing the network after link P1 to P2 has been disconnected.

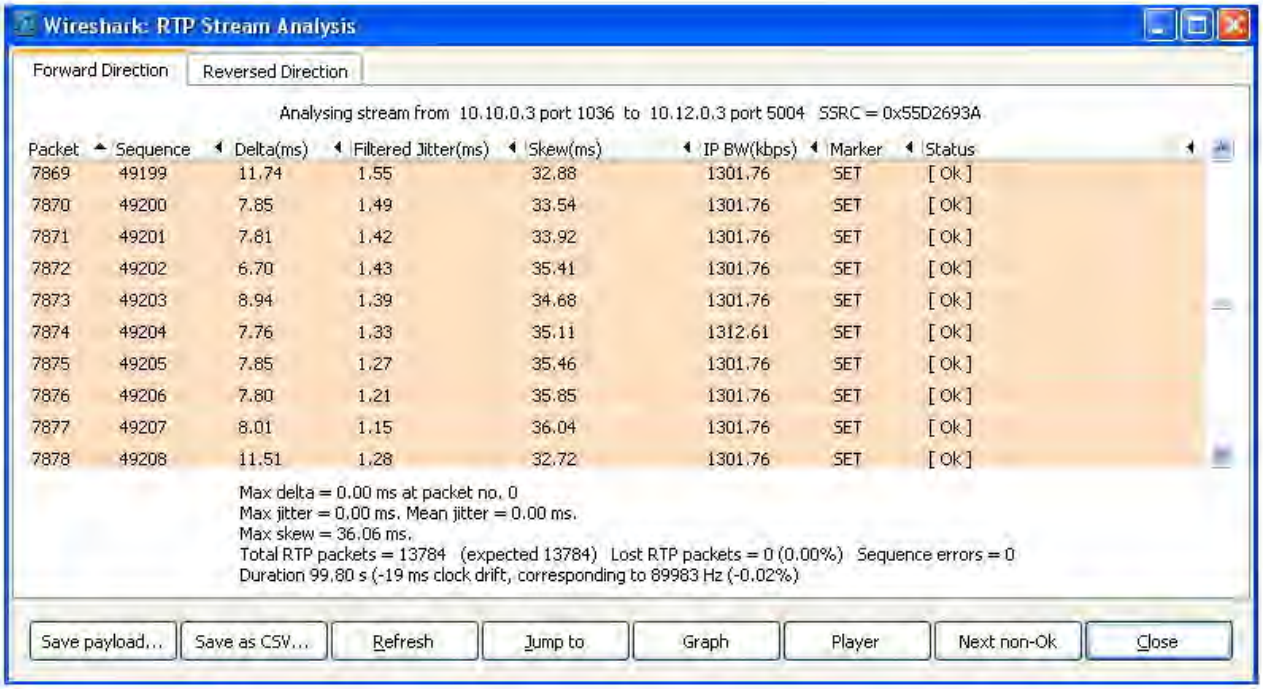

Figure 5.19: Packet loss pattern

From Figure 5.19, there were no packet dropped when the link was disrupted thus showing the high quality of service delivery of the VPLS network. The skew parameter is the time difference between the current packet arrival rate relative to the nominal packet rate. A low maximum skew time of 36.06ms was recorded which is ideal for real time communication. From the above QoS results, the VPLS network was not degraded even though there was link disruption. Therefore as long there is an alternative path in a network, VPLS ensures consistent traffic delivery.

5.5 Summary

This chapter presented the results and analysis of the experiments carried out on the VPLS network. The results were obtained using the Wireshark monitoring tool as described in Chapter 4. The VPLS network under investigation is virtualized using the VMware station 7.0 hypervisor. The virtualized network nodes are created within the limits of the host machines as

discussed in Chapter 4. Monitoring tools are used to investigate the performance of the VPLS network in both the control and data plane.

In the control plane, the performance of the signaling protocols is monitored using Wireshark. Results of protocols such as OSPF, LDP and BGP present and describe in greater lengths the operation of the data plane in a VPLS network. The OSPF routing results presented describe router interface interaction and also offer topological information of the network. The LDP signaling results present how and where label encapsulation/de-capsulation occurs in the network. The BGP auto-discovery results show how the PWs are setup within the VPLS network. They further show how auto-discovery can be achieved with VPLS peering nodes.

In the data plane, the results presented show the multicast awareness of the VPLS network. Frames from the Real-time and Database servers were not flooded into the network but they were delivered to specific clients participating in different VPLS instances. The multicast awareness of the VPLS network ensured the efficient use of the available bandwidth.

The use of MPLS-TE tunnels for the delivery of frames across the network also improves the utilization of the network bandwidth by offering control over allocated and reserved bandwidth. The results presented by the auto-bandwidth allocation mechanism showed that having a constantly reserved bandwidth leads to underutilization of network resources.

Furthermore, the QoS results presented showed that by using traffic engineered tunnel there is no network degradation. This is advantageous due to the fact that the TE tunnels and the PWs are dynamic in nature and will therefore reconstruct a network path to ensure the delivery of frames from the servers to client machines. Therefore the VPLS network presented is not only multicast aware but it also utilizes the available bandwidth efficiently. The network is also virtualized therefore has low setup costs.

Chapter 6 Conclusions and Research Recommendations

6.1 Concluding Remarks

This thesis was aimed at developing techniques for the efficient utilization of bandwidth in a VPLS environment. Furthermore, this thesis was aimed at showing the multicast awareness of VPLS networks. The VPLS network was based on a Point-to-Multipoint MPLS transport protocol. The VPLS network addresses how enterprise networks are able to benefit from its advantages. Challenges that are faced by SPs such as network resiliency, scalability and multi-service connectivity are addressed in this thesis research.

A customized research platform was built in which the multicast awareness and the efficient utilization of bandwidth within a VPLS network was tested. This platform was based on a virtualized environment in which network nodes, like routers servers and clients, were formed. For the virtualization of the environment VMware software was used. It was also used in the creation of server and clients at different client sites. The routers that made up the network were established by the use of MIKROTIK routerOS software. This router software resided in the created virtual machines and was the operating system. Using this router software converted the virtual machines into routers from which a network was built. Even though the size of the network was restricted to the capacity of the host machines in which the network nodes resided, care was taken in choosing how many nodes would be appropriate to guarantee that sufficient tests were carried out.

Based on a customized research platform, the stated challenges are addressed while taking into consideration the fundamentals of having a consistent organization of a network's core. The development of bandwidth as a network resource formed the basis on which the research platform was built. From the research platform the following objectives were achieved:

- Signaling and Auto-discovery
- Multicast ingress replication
- Auto-bandwidth allocation

The development of the stated objectives led to the improvement of bandwidth as a resource and how it is efficiently used by both the SP and the client. The stated objectives also led to the improvement of scalability and network resilience in terms of link failure. The discussion that follows explains how the consolidation of the stated objectives improved the efficiency of bandwidth in the VPLS network.

The signaling mechanism was based on the use of the Label Distribution Protocol (LDP). The implementation of LDP in the network provider routers ensured the use of MPLS as the transport protocol. MPLS facilitated the use of labels to encapsulate frames/packets that transverse the network. MPLS offered the network the following advantages:

- The Traffic Engineering attribute in MPLS ensured that different sets of traffic can be allocated individual characteristics. For example tunnels that transported bulky data traffic were assigned larger bandwidth traffic profiles compared to those that carried video.
- Since MPLS offers TE tunnels, there is a guarantee of Quality of Service for the different services delivered over the tunnels.
- There are lesser signaling overheads while using labels to encapsulate the data frames.

In the VPLS network, auto-discovery of peering network nodes was achieved with the Border Gateway Protocol (BGP). Furthermore, the BGP was used to dynamically establish pseudowires (PW). The PWs link the provider edge routers over the TE tunnels and these in turn created the emulated Ethernet LAN connections between the sites. Using BGP in the VPLS environment offered scalability to the network.

The realization of a VPLS network then led to control and data plane tests. These tests identified and confirmed previous notions of how signaling bits and data traffic behaved within the VPLS network. It was noted that the efficient utilization of bandwidth was achieved and also the networks' awareness of multicast streams. Through ingress replication, only one copy of the same data stream was forwarded to the network as opposed to flooding the network with multiple copies of the same data. The ingress replication occurred at the first network provider edge router closest to the server. It was at this PE node that multicast streams were forwarded to other PE nodes that belonged to the same VPLS instance. Having a multicast aware VPLS network implied that the assigned bandwidth to both the client and the tunnels within the network was being efficiently used.

Traffic Engineering in MPLS not only guaranteed QoS of the VPLS network but it also further facilitated the implementation of a bandwidth allocation scheme. The bandwidth allocation was automated and performed in the traffic engineered tunnels. In the implantation of the auto-bandwidth allocation, sampling intervals were observed and it was from these that the reserved bandwidth was automatically assigned in the next period. Based on this method, a sampling time of one second and a period (interval) of one minute were considered as the optimal rates for the auto-bandwidth allocation. Under these rates, the reserved rate limits did not cause inefficient utilization of the set limits. Setting the maximum possible rate as that of the link

capacity ensures no packets are lost due to tunnel congestion. Under the auto-bandwidth allocation, tunnel bandwidth was efficiently utilized within the traffic engineered tunnels.

Having addressed the efficient utilization of bandwidth, data streams were transported across the VPLS network to not only test its multicast awareness but also to show the emulated Ethernet type of connectivity that VPLS offers. It was found that the VPLS network indeed offers an emulated LAN connectivity and further enjoys the data rates synonymous with Ethernet type services. The high data rates were a measure of the networks' capacity coupled with the physical hardware limitations, for example, the hosts' network interface card (NIC) rates and the LAN cables connecting the hosts.

The novelty of this research was obtained through completely virtualizing a VPLS network together with server client nodes. In so doing, this illustrated how SPs can reduce costs incurred in the setup of their networks. Reduced costs appeal to a business type model which gives the SPs the freedom to redistribute their setup costs. Lesser physical infrastructure required in the building a VPLS environment facilitates the SPs to invest more in offering quality services to their enterprise clients such as front desk technical help and an improvement in the operations, administration and management of the network.

6.2 Recommendations for Future Research Work

During the course of conducting this research, a number of interesting avenues for further research surfaced and provide a source for future work in regards to the adaptation of VPLS environments over MPLS transport networks. These ideas/avenues include:

- In the VPLS environment, pseudowires can use flow labels to implement an equal cost of multiple paths (ECMPs). RFC 6391 suggests that identifying label flows within PWs ensures that the LSRs perform flow balancing with finer granularity as compared to individual PWs. This can be achieved by using an additional label on the pseudowire. However this would require a larger network to carry out sufficient analysis. Furthermore the building of a customized research platform would be facilitated by a host or hosts with larger resources to virtualize the VPLS environment.
- Furthermore, in the OAM requirements of a network, it is important to determine how the VPLS environment handles faults within the network. It is important to the SP that they know how service connectivity between their VPLS aware sites and devices is handled before, during and after a fault occurs. Therefore fault detection and handling within a VPLS network through monitoring can lead to methods of improving any degradation of the services traversing the network.

- The research platform mainly focused on achieving a VPLS aware multicast network and auto-bandwidth allocation but concerns over the network security were not addressed. The filtering of frames that traverse the network must be identified in order to distinguish or separate client frames from network frames.

Bibliography

[1] J. Witters, J. De Clercq, and S. Khandekar, Technical introduction to multipoint Ethernet services over MPLS, 2004, Alcatel Telecommunications Review - 4th Quarter 2004.

[2] CISCO, "Virtual Private LAN Service Architectures and Operation" White Paper, 2004.

[3] Saad Z. Asif, *Next Generation Mobile Communications Ecosystem: Technology Management for Mobile Communications*, John Wiley & Sons, Ed., 2011.

[4] France Telecom, "2011 Annual Report on Form 20-F of France Telecom," France Telecom, 2011.

[5] Packet Exchange. (2012) [Online]. http://packetexchange.com/index.html

[6] N3 NHS. [Online]. http://n3.nhs.uk/ProductsandServices/N3Connectivity/default.cfm

[7] S. HomChaudhuri and M. Foschiano, "Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment", RFC 5517, 2010.

[8] Huawei Technologies, Technical White Paper for VPLS, 2007.

[9] Giuseppe Di Battista, Massimo Rimondini, and Giorgio Sadolfo, "Monitoring the Status of MPLS VPN and VPLS Based on BGP Signaling Information," in *2012 IEEE Network Operations and Management Symposium (NOMS)*, 2012, pp. 237-244.

[10] Amsterdam Internet Exchange. (2010) AMS-IX Partner Program Training. [Online]. http://www.ams-ix.net/statistics/

[11] Zhuo (Frank) Xu, *Designing and Implementing IP/Mpls-Based Ethernet Layer 2 VPN Services: An Advanced Guide for Vpls and VLL*.: Wiley Publishiing, 2009.

[12] Y. Kamite, Y. Wada, Y. Serbest, T. Morin, and L. Fang, "Requirements for Multicast Support in Virtual Private LAN Services" IETF, RFC5501, 2009.

[13] E. Rosen, B. Davie, V. Radoaca, and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", RFC 6074, 2011.

[14] R. Aggarwal, Y. Kamite, and L. Fang, "Multicast in VPLS", draft-ietf-l2vpn-vpls-mcast-11.txt, 2012.

[15] Kompella.V Lasserre.M, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling" RFC 4762, 2007.

[16] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" RFC 4761, 2007.

[17] CISCO. (2011, March) Cisco IOS Switching Services Configuration Guide, Release 12.2. Multiprotocol Label Switching Overview.

[18] A. Sajassi and D. Mohan, "Layer 2 Virtual Private Network (L2VPN) Operations, Administration, and Maintenance (OAM) Requirements and Framework", IETF, RFC 6136, 2011.

[19] Juniper Networks, "Network Configuration: Configuring BGP Autodiscovery for LDP VPLS", 2012.

[20] Medhi Deepankar and Ramasamy Karthikeyan, *Network Routing, Algorithms, Protocols, and Architectures*. San Francisco, U.S.A: Morgan Kaufmann, 2007.

[21] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture" IETF RFC 3031, 2001.

[22] Wei Luo, Carlos Pignataro, Dmitry Bokotey, and Anthony Chan, *Layer 2 VPN Architectures*.: Cisco Press, 2005.

[23] Vivek Alwayn, *Advanced MPLS Design and Implementation*. Indianapolis, U.S.A: Cisco Press, 2002.

[24] iTrinegy Network Emulator Enterprise. (2012, June) www.ine.com. [Online]. www.ine.com/2010/06/28/mpls-components-part-2/#more-3968

[25] Abhinav Pathak, Ming Zhang, Y. Charlie Hu, Ratul Mahajan, and Dave Maltz, "Latency Inflation with MPLS-based Traffic Engineering," in *Internet Measurement Conference IMC'11*, Berlin, Germany, 2011, pp. 463-471.

[26] Andersson L, Minei I, and Thomas B, "LDP Specification", RFC 5036, 2007.

[27] CISCO. (2008, May) [Online]. http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_overview.pdf

[28] K. Kompella and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures" IETF, RFC4379, 2006.

[29] E. Gray, N. Bahadur, S. Boutros, and R. Aggarwal, "MPLS On-Demand Connectivity Verification and Route Tracing" IETF, RFC6426, 2011.

[30] Luc De Ghein, *MPLS Fundamentals*. MPLS Fundamentals, USA: Cisco Press, 2007.

[31] P. Agarwal and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks", IETF, RFC 3443, 2003.

[32] M. Bocci, S. Bryant, D. Frost, L. Levrau, and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, 2010.

[33] Vinod Joseph and Srinivas Mulugu, *Deploying Next Generation Multicast-Enabled Applications*. USA: Morgan Kaufmann, 2011.

[34] K. Shiomoto and A. Farrel, "Procedures for Dynamically Signaled Hierarchical Label Switched Paths", IETF, RFC 6107, 2011.

[35] K. Kompella and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", IETF, RFC 4206, 2005.

[36] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" IETF, RFC 4761, 2007.

[37] Kamite.Y, Wada.Y, Serbest.Y, Morin.T, and Fang.L, "Requirements for Multicast Support in Virtual Private LAN Services," RFC 5501, 2009.

[38] J. Le Roux, P. Vasseur, and J. Boyle, "Requirements for Inter-Area MPLS Traffic Engineering", IETF, RFC 4105, 2005.

[39] Cisco, Cisco IOS MPLS Virtual Private LAN Service, 2004.

[40] D. Smith, J. Mullooly, W. Jaeger, and T. Scholl, "Label Edge Router Forwarding of IPv4 Option Packets",IETF, RFC 6178, 2011.

[41] Vinod Joseph and Srinivas Mulugu, *Deploying Next Generation Multicast-Enabled Applications*.

[42] T. Bates, E. Chen, and R. Chandra, "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)", IETF, RFC 4456, 2006.

[43] Mikrotik. (2010, April) [Online]. http://wiki.mikrotik.com/wiki/Manual:BGP_Case_Studies

[44] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", IETF, RFC 4271, 2006.

[45] L. Andersson and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", IETF, RFC 4664, 2006.

[46] L. Martini, E. Rosen, N. El-Aawar, T. Smith, and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", IETF, RFC 4447, 2006.

[47] L. Martini, C. Metz, T. Nadeau, M. Bocci, and M. Aissaoui, "Segmented Pseudowire", IETF, RFC 6073, 2011.

[48] Juniper Networks, "Next-Generation VPLS Point-to-Multipoint Forwarding Overview", 2011.

[49] Juniper Networks, Inc, *MPLS Applications Configuration Guide*, 121st ed. Californiav, USA: Juniper Networks, Inc, 2012.

[50] Mohan Nanduri, Mark Kasten, and Naoki Kitajima. (2012, Febuary) MPLS Traffic Engineering with Auto-Bandwidth: Operational Experience and Lessons Learned. [Online]. http://meetings.apnic.net/__data/assets/pdf_file/0020/45623/MPLS-Traffic-Engineering-with-Auto-Bandwidth.pdf

[51] Mikrotik. (2012, September) Mikrotik wiki. [Online]. http://wiki.mikrotik.com/wiki/Manual:TE_tunnel_auto_bandwidth

[52] Cisco, MPLS VPN Mapping of RFC 1483 Routed Sessions.

[53] Mikrotik. (2010, March) http://wiki.mikrotik.com/wiki/MPLSVPLS. [Online]. http://wiki.mikrotik.com/wiki/MPLSVPLS

[54] Deepankar Medhi and Karthikeyan Ramasamy, *Network Routing, Algorithms, Protocols, and Architectures*, David Clark, Ed. San Francisco, U.S.A: Morgan Kaufmann, 2007.

[55] E. Rosen, P. Psenak, and P. Pillay-Esnault, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)", IETF, RFC 4577, 2006.

[56] Mikrotik. (2012, January) [Online]. http://wiki.mikrotik.com/wiki/Manual:OSPF_Case_Studies

[57] R. Bonica, D. Gan, D. Tappan, and C. Pignataro, "ICMP Extensions for Multiprotocol Label Switching", RFC 4950, 2007.

[58] Javin Network Management and Security. (2012) [Online]. http://www.javvin.com/protocolMPLS.html

[59] Cisco. (2008, September) MPLS FAQ For Beginners. [Online]. http://www.cisco.com

[60] Aggarwal.R, Kamite.Y, and Kamite.L, "Multicast in VPLS," draft-ietf-l2vpn-vpls-mcast-10.txt, 2012.

[61] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, 2006.

[62] The Crankshaft Publishing. (2012) [Online]. http://what-when-how.com/ipv6-advanced-protocols-implementation/introduction-to-bgp4-ipv6-unicast-routing-protocols-part-1/

[63] D. Meyer and K. Patel, "BGP-4 Protocol Analysis", RFC 4274, 2006.

[64] Jeff Doyle and Jennifer DeHaven Carroll, *Routing TCP/IP, Volume II (CCIE Professional Development)*. Indianapolis, USA: Cisco Press, 2001.

[65] L. Martini, E. Rosen, N. El-Aawar, and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, 2006.

[66] Mikrotik. (2011, September) Mikrotik Wiki. [Online]. http://wiki.mikrotik.com/wiki/Category:Manual

[67] Jim Guichard, Ivan Pepelnjak, and Jeff Apcar, *MPLS and VPN Architectures Volume II*. Indianapolis, USA: Cisco Press, 2003.

[68] L. Andersson and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, 2009.

[69] Mikrotik. (2010, March) Mikrotik Wiki. [Online]. http://wiki.mikrotik.com/wiki/Manual:TE_tunnel_auto_bandwidth

[70] Sumit Kasera, Nishit Narang, and Sumita Narang, *Communication Networks: Principles and Practice*.: Tata McGraw-Hill , 2005.

Appendix A

Accompanying CD-ROM

- **Thesis hard copy**

  The electronic copy of the thesis can be found in the "Thesis" directory

- **Software**

  The software monitoring tools used in the VPLS network can be found in the "Monitoring Tools" directory

- **Deployed Network**

  The VPLS network created can be found it the "VPLS Network" directory. ISO files in this directory represent the different network elements such as the Provider Edge nodes and Provider nodes.

- **Manual**

  A manual is also included in the "Manual" directory. This manual can be used to further develop and expand on the current VPLS network.