Performance Analysis of QoS enabled MPLS Virtual Private Enterprise Network through Simulation

1- Yonos Almehdi Qnedi[1] , College of Education Kikla, University of Gharyan
qnedi42@gmail.com
2- Khaled Elhashmi Algarari[2] ,College of Education, Kikla
University of Gharyan , m.algarari2007@gmil.com
3- Maisam Abdullatif Aborass[3] , Faculty of Science, Gharyan , University of Gharyan
m_aborass@yahoo.com

Abstract

As businesses are spreading to different locations they require a strong and secure way of communication between the different offices. There are different services which require nonstop flow of traffic. The multimedia applications with voice and video needs more priority than other applications, as it is sensitive to delay. The MPLS (Multiprotocol Label Switching) based VPN (Virtual Private Network) can provide QoS (Quality of Service) features. This paper investigate on how DiffServ QoS Model parameters over MPLS VPNs environment can help the enterprise network customers to maintain the quality for their multimedia application usage in their network. To test our approach, a MPLS VPN Traffic Engineering approach was configured on two distinct enterprise businesses and MPLS VPN networking with and without DiffServ QoS parameters for voice, email and data were implemented on GNS3. The results reveal good bandwidth with reliable speed and less delay.

Keywords — component MPLS VPN; Traffic Engineering; IP Voice; DiffServ QoS; LAN; WAN; Jitter.

I. INTRODUCTION

The QoS is a set of techniques that are necessary in a business environment because of their ability to manage network bandwidth delay, jitter, and packet loss to maintain a constant flow of data [1]. From a business perspective, it is essential to ensure that the transmission of data from source to destination is guaranteed and that all resources required for the network are provided regardless of the network traffic load. A very good example of QoS required for an enterprise business is VoIP (voice over IP) traffic because it requires a

certain time to destination in the packet delivery, also known as absolute time [2]. A small delay can have a huge impact on a business's important data or meetings. For enterprises, many new technologies are available for smooth conversation, such as mobile networks and telephonic systems, but these are expensive and pose several security issues.

A new network infrastructures are more favourable and better fulfil business requirements. However, with delay and availability issues, matters such as a service guarantee across the network must be ensured, which means that service quality is required for real-time traffic. A Differentiated services (DiffServ) is a protocol that can help to prioritise and specify traffic by class, which means that the most important data takes precedence over low-priority data [3]. For example, in most cases, VoIP traffic requires a relatively uninterrupted flow of data from source to destination. Multiprotocol Label Switching (MPLS) is a standard-based technology that is used to speed up the delivery of network packets over multiple protocols, such as IP (Internet Protocol), ATM (Asynchronous Transport Mode), and the Frame Relay network protocol [4]. A VPN's (virtual private network) use of shared public telecom infrastructure to provide secure network data transmission between two paths is known as a tunnelling protocol and procedure [5].

Therefore, to achieve service quality, a DiffServ is the most advanced method of managing traffic because it is a set of end-to-end quality measures for QoS capabilities that have the ability to deliver the services required by specific network traffic from source to destination. QoS (quality of service) parameters work efficiently in an MPLS VPN environment at the enterprise level.

According to [6] MPLS service providers offer a variety of solutions to ensure efficient services; however, none of them provides complete QoS appliances to meet the requirements. Therefore, this paper focuses mainly on the use of MPLS VPNs and DiffServ technologies together to ensure a secure environment with guaranteed QoS for enterprise-level businesses. Further, it will ensure the secure transmission of data from source to destination.

II. LITERATURE REVIEW

Many enterprise businesses around the world are looking for an appropriate solution for their networks, including local area networks (LAN) and wide area networks (WAN), to improve the traffic between different hosts [7]. The purpose they purchase lease lines for their WAN networks for faster traffic or data transmission over networks without any delays. They are also seeking to provide a secure environment for their data; however, recent cyber-attacks on enterprise businesses around the world have changed business strategies toward security and privacy issues. According to [8] criminals have intensified their data breaches, which are becoming increasingly common; the number of DDoS events reached 20 Gbps at the beginning of 2014. Cyber-attacks and DDoS attacks have been undertaken against enterprise businesses and agencies including eBay, the Montana Health Department, Domino's Pizza, Evernote and Freedly, and P.F. Chang's [6]. These businesses went down because of either cyber-attacks from intruder or DDoS attacks on their mainstream servers, resulting in the theft of the personal records of a million customers [8].

A. QoS

In multi-service IP networks that are specially designed for enterprise businesses, many types of services are transported on a same network infrastructure. QoS assurance must be provided in both ISP and network architecture in terms of jitter, latency, packet loss, resilience in the face of failure, bandwidth guarantees, and down time[9].

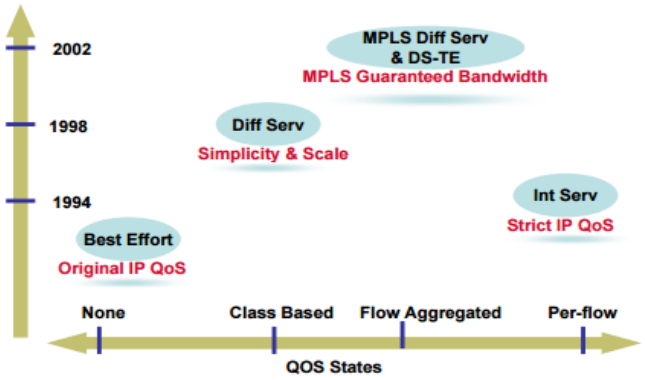

Fig. 1. QoS Model Timeline [12]

Therefore, QoS is a mechanism that has the main goal of providing different service levels of different traffic types in accordance with business needs without any delays, which means offering network services of good quality [7]. For this purpose, an SLA (service-level agreement) provides all parameters of QoS details, such as end-to-end jitter, delays, and packet loss. It can be referred to as an intelligent service that provides a guideline to network devices on how to deal with the different applications' traffic based on their set service level under the SLA [10].

Therefore, QoS actually manages four main network elements: 1) bandwidth, which is the maximum payload or the payload that can be carried by a network; 2) delay, which is the time required to send data or payload from source to destination; 3) jitter, a variation associated with delay; and 4) reliability, which deals with packet loss [11].

The fundamental aim of QoS is to ensure free and fast network transmission between different hosts and to ensure that excessive congestion does not occur [12]. In the last few years, several mechanisms and techniques have emerged that allow network communication through QoS services, as shown in Figure 1. In this regard, the IETF (Internet Engineering Task Force) has proposed many service models to meet the demands of QoS, and IntServ (integrated services) and DiffServ (differentiated services) are the main models for providing QoS [11].

IntServ with the RSVP (Resource Reservation Protocol) is considered efficient for end-to-end services in connectionless IP networks where additional services such as controlled load services and guaranteed services can be used to complete the transmission without any disruption [13]. Guaranteed services provide services with no packet loss caused by overflow in buffer size and a specified upper bound on the queuing delay specified through the network [9]. In contrast, controlled load services ensure that a high percentage of packets are delivered without any delays [7]. The most frequently noted problems identified with the IntServ architecture are stability and scalability issues because it possesses per-flow classifications, per-flow scheduling, and per-flow buffering because it is stored in a control panel that is overhead on the routers [12].

The DiffServ architecture is different from the IntServ architecture because its main aim is to provide different levels of QoS for the traffic flow, unlike IntServ, which provides a point-to-point level [14]. The important feature of DiffServ is that it provides more robust and scalable network architectures for enterprise businesses because it supports multiple nodes flow bandwidth and guarantees availability without jitter or delay [15]. According to [11] the other main features of DiffServ are as follows: a) Premium Service, which requires low delay and jitter; b) Assured Service, which requires applications for better reliability to provide the best services; c) Olympic Service, which provides a three-tier architecture for network services; and d) Gold and Bronze Service, which require better bandwidth in case the quality of services declines.

B. MPLS VPN

Many IT companies around the world are looking for mechanisms and techniques for their wide area networks that support strong security and privacy for their core business data. For this reason, they have purchased Frame Relay or ATM leased lines and established virtual private networks to provide their businesses with maximum security through a tunnel route for their data traffic over the Internet [9]. This type of technology and network architecture works on a layer 2 data link layer. Businesses around the world are receiving benefits such as security and protection against intruders and hackers' attacks on their backbone networks. However, VPNs have faced many problems that have recently been discovered, such as the scalability problem and multiple QoSs over large networks, especially in a VoIP environment [10]. These problems have been consistently reported for several years, since VPN gained popularity among many enterprise-level companies.

Therefore, to overcome these problems MPLS (Multiprotocol Label Switching) was introduced [16]. The main purpose was to deliver an efficient and effective way of transmitting IP packets over a network or VPN. MPLS is standardised by the IETF as the layer 3 network protocol and packet switching technology, which transmits traffic through a network using information contained in labels attached to IP packets, which is a more secure model [17].

Figure 2 shows the common MPLS deployment models where the customer's routers are attached to service provider (SP) routers and the

negotiated routing protocols or a static router advertises the customer's IP routers to the SP, and this SP MPLS network advertises these incoming routers to all participating locations.

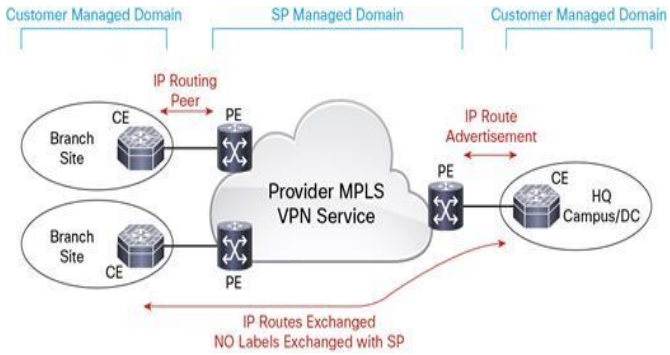

Fig. 2. Common MPLS Deployment Model [5]

This means that the customer end does not participate in the SP's MPLS backbone network, which is secure and maintains data integrity.

C. MPLS (Architecture)

MPLS consists of two main planes, known as the control plane and the data plane [18]. The control plane is responsible for the routing and label information exchange with the adjacent routers; therefore, two kinds of protocols such as routing protocols and label exchange information protocols [17]. This means that every MPLS node must run IP routing protocols to exchange the routing information with other similar nodes on the control plane. However, in the traditional routing mechanism, it is done by the IP routing table, which is used to build the IP forwarding cache. The MPLS data plane has a simple forwarding mechanism that is based on the information attached to the labels formed in two types of tables, known as LIB and LFIB [18]. Labelled packets are forwarded by the label forwarding information base (LFIB), and the label information base (LIB) table contains all local assigned by the local routers. Further, actual packet forwarding labels are contained in the labels contained in LIB, as shown in Figure 3.

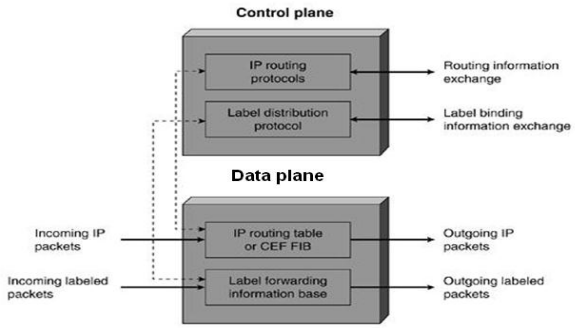

Fig.3. MPLS Architecture [9]

D. MPLS VPN QoS

MPLS integrates a label-swapping framework with network layer routing, which is a basic idea that involves the attachment of short fixed-length labels to packets upon access to an MPLS cloud [19]. In this way, labels attached to packets are actually making forwarding decisions to provide a more secure means of transmission. Further, this mechanism also provides an efficient tunnelling technique for connectionless IP networks as well [20]. This means that end-to-end connections for a connectionless IP network are more favourable with this technique. According to [21] QoS in the context of VPN is mainly described using two models: a) a pipe model and b) a hose model.

The most important issue in enterprise networks arises when they support different types of applications for their business operations, such as voice, video, browsing, and network management, also known as converged networks [22]. In such a model, different applications have sensitivities and requirements; though all applications require the same network infrastructure, they require different priorities, as shown in Figure 4.

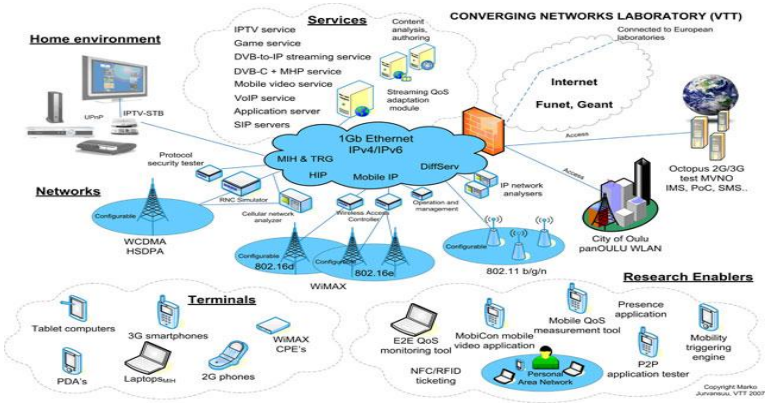

Fig.4. Converged Network Architecture [23].

Such a complex architecture shown in Figure 4 requires that different services and applications run on the same infrastructure, and each application requires a high level of availability and performance. In such a network architecture, some applications are delay-sensitive; some require more bandwidth, and some applications require a constant amount of bandwidth, as shown in Figure 5. For example, voice over IP (VoIP) applications are always delay-sensitive in enterprise businesses, requiring smooth operations with an end-to-end delay of only 150ms to 200ms because a longer delay will disrupt the conversation [23].

In contrast, File Transfer Protocol (FTP) is not delay-sensitive, and jitter cannot disrupt the functionality because they can easily adapt to the network architecture and work accordingly. However, some applications use UDP, and no acknowledgement is required for their data transmission over networks. These types of applications cannot tolerate a packet drop because UDP has no acknowledgement mechanisms, as TCP-based applications usually do, for their transmissions [11]. For example, for VoIP (video over IP), online streaming for conferences, and online gaming (e.g., Sony Inc.) it is necessary to handle applications properly, without any interruption and delay, with high-quality services. These problems can be addressed by using MPLS VPN with either an IntServ or DiffServ mechanism to achieve QoS [23].

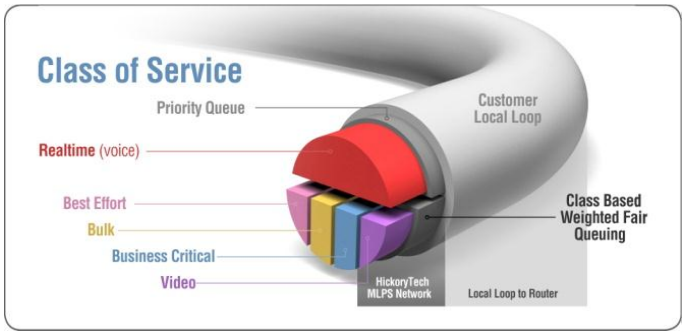

Fig.5. QoS Involves Prioritisation of Network Traffic [22]

Two main MPLS QoS classes of service (CoS) are available: the pipe model and the hose model [13]. The pipe model provides certain QoS guarantees to VPN customers for data transmission between two nodes or hosts within the VPN architectures. It is like a pipe established between two CE routers using minimum bandwidth, similar to the Frame Relay or ATM model; however, both ATM and Frame Relay are bidirectional, while the pipe model is unidirectional, allowing traffic in each direction between CE routers [20]. The hose model provides a guarantee for traffic transmitted between CE routers in the same VPN architecture [24]. It is easy to configure QoS in a MPLS VPN environment because the customer does not require a capacity planning, distribution, and traffic analysis between different CE routers [25]. The hose model and DiffServ model are similar because both support multiple CoSs, which means that, in the hose model, CoSs are supported by DiffServ, while the pipe model resembles the IntServ model for QoS [21].

E. Traffic Engineering in MPLS Networks

The modern networks are considered highly converged networks that carry multiple data types simultaneously using the same network resources [19]. This means that enterprise businesses are facing huge challenges considering the increasing numbers of users and traffic types that pose an enormous challenge for traffic engineering [23].

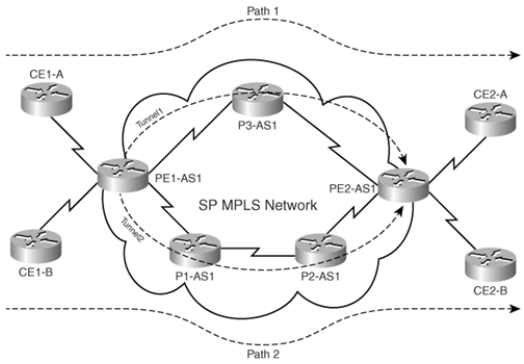

Fig. 6. MPLS Traffic Engineering Network [7]

In some networks, the IP packets are forwarded under the OSPF (Open Shortest Path First) protocol, which choses the shortest path to save network resources. However, they may create an extra burden because of low delay and packet loss during the delivery of UDP based transmission (e.g., multimedia applications). Therefore, MPLS-TE provides mechanisms to facilitate fast packet switching to support traffic engineering to provide QoS [20].

The MPLS traffic engineering (MPLS TE) is growing acceptance. This has also been seen among service providers because it replicates and expands the traffic engineering capabilities of layer 2 networks [26]. Further, MPLS TE allows MPLS-enabled networks to integrate into layer 3 as well, which can be implemented for more efficient bandwidth utilisation between a service provider's routers.

III. METHODOLOGY

Every research area requires some kind of systematic data collection, called a methodology [27]. The main purpose of selecting a methodology for research is highly important because it directly deals with the data collection method when the researcher needs primary or secondary data sources for research analysis.

According to [28] the two most famous research data collection approaches are qualitative (e.g., background research/literature review, document analysis, case studies, observations, ethnography, etc.) and quantitative (e.g., questionnaires, interviews, etc.). There are several advantages and drawbacks to both research approaches because each data collection method deals with different research situations and data analysis techniques. Sometimes, qualitative methods are preferred to a quantitative research approach because they are easy to perform [28].

In the current research, the following methodological techniques were used for data generation:

- The first contribution of this research is derived from secondary sources, as the author conducted comprehensive background research about MPLS VPN and related techniques. The sources included authentic sources such as academic journals, IEEE articles, ACM Digital Library, etc. The main goal of conducting the background research was to increase the author's current knowledge in the chosen research domain.

- The second contribution is derived from a practical exercise performed using the GNS3 network simulation tool and the Wireshark data capture tool, as the research mainly focuses on the use of the MPLS VPN and DiffServ technologies together to ensure a secure environment that guarantees QoS for enterprise-level businesses. Further, it ensured the secure transmission of data from source to destination. For this reason, various scenarios were established using GNS3 because it is open source and supports all CLIs (command line interfaces) for MPLS VPN, traffic engineering, DiffServ, OSPF, BGP, EIGRP, IPv4, IPv6, MPLS DiffServ tunnelling modes, enterprise-to-service provider mapping models, etc. These scenarios helped in proposing a network architectural model for enterprise businesses to achieve the research aim and objectives. Wireshark was also used to capture the data transmission between two hosts/networks. In addition, security issues and how to tackle them are also discussed for all developed scenarios.

- The final part of this report analyses and reports all information with further recommendations: 1) a new architectural design for an efficient and advanced WAN network to ensure high-performance data transactions and high availability (e.g., equal and non-equal load balance) of data transmission and 2) a report for network administrator or a network architecture to guide users how to achieve QoS by utilising advanced networking tools and technologies.

IV. NETWORK DEVELOPMENT

The research aim is to develop a theory based on a practical approach using MPLS VPNs and DiffServ technologies together to ensure a secure environment that guarantees QoS for enterprise-level businesses. For this reason, various scenarios were established using GNS3 for MPLS network architecture. The lab development for the scenarios involved the following tools and technologies:

A. GNS3 Simulation Tool

A GNS3 is the first free multi-vendor network simulation tool to provide a virtual environment to design, test, and optimise a network without having to purchase original hardware, which is expensive and requires a great deal of space to conduct experiments [29]. Further, GNS3 is recognised worldwide, as one out of five enterprise businesses in the world are using GNS3 for their lab tests and implementation before actual implementation. These organisations include NASA, the US Department of Defence, Walmart, Exxon, and Twitter.

According to [30] the tool offers several benefits to organisations in the testing of network scenarios and for further improvements. For example, it can save a great deal of money, time, and frustration that comes directly from hardware configuration and cabling. Further, GNS3 is very helpful in understanding network software management, as it can help in designing a flawless network architecture that will be practical and relevant to the customers. GNS3 is proprietary software from GNS3 Technologies Inc., which was established in 2013 in Calgary and Silicon Valley [29]. The simulation tool provides an attractive graphical user interface (GUI) to design and configure virtual networks that run on several machines and hardware. These machines include traditional PC hardware that can be used on multiple platforms, such as Windows, Linux, and Mac OSX. Further, more than two million people all over the world are using GNS3.

B. Wireshark Tool

Wireshark is a network packet analyser that helps to capture network packets and displays proper data that can be used for further analysis for the development for network architecture [31]. It functions like a measurement tool or a device that helps to display what is actually happening inside the network to the network engineer, who can actually see using Wireshark what is happening in the cables during the transfer of payload from one host to another. It operates similarly to a voltmeter, which allows electricians to examine the functionality of electric cables at a high level so that they can be easily adjusted by an electrician once a fault is found.

The major purposes of using Wireshark include the following: a) troubleshooting problems that exist in the network; b) examining

security problems in the network;c) debugging protocol implementations in lab scenarios; and d) learning about the network protocol's internal behaviour. In the current research, the Wireshark tool is used to capture traffic that is initiated in one branch is sent to another branch with and without using DiffServ QoS model parameters to examine the network efficiency.

C. Lab Scenario

Different Scenarios were configured by using GNS3 for MPLS network architecture as shown in topology figure 7. The Scenario was done for two enterprise customers named City Bank and Swiss Bank, which both have active branches in different cities. Both enterprise businesses have two branches where one is in London and other branch is in New York. In between there is a service provider which is also known as MPLS Cloud using Integrated Gateway Protocol OSPF.

CITY BANK:

Two sites are in operation and want secure communication between each other using the MPLS VPN and DiffServ QoS model to provide flawless and timely communication. Site one consists of PC1 and customer end router 1 (CE-1), using EIGRP routing protocols with the private IP Address 192.168.1.0/24. This router (CE-1) is connected with service provider router PE-1. PE-1 to CE-1 is running an EIGRP routing protocol with Autonomous No. 1 and have Virtual Routing and Forwarding (VRF) (CB-VRF) on PE-1 for CE-1 with RD/RT (100:100) for both import and export values.

The service provider uses label-switched path routers to exchange the routes from PE-1 to PE-2 to ensure that the communication process from the London branch to the New York branch was completed.

The New York branch uses the customer end three (CE-3) router, which communicates with the PE-2 router of the service provider. The customer end router uses the OSPF (Area-1) protocol running PE-2 to CE-3 and has VRF (CB-VRF) on PE-2 for CE-3 with RD/RT (100:100) import/export both. The private network IP scheme is used in this network, which is 172.16.1.0/24. The WAN IP address between CE-3 and PE-2 is 9.9.67.0/24, where serial interface 1/0 from CE-3

communicates with serial interface 1/0 of PE-2 to exchange VRFs. CE-1 uses the 9.9.12.0/24 IP address to communicate with the PE-1 router.

SWISS BANK:

Two sites are in operation and want secure communication between each other using a MPLS VPN and DiffServ QoS model to provide flawless and timely communication. The service provider uses label-switched path routers to exchange the routes from PE-1 to PE-2 to ensure that the communication process from the London branch to the New York branch is completed.

The New York branch uses the customer end three (CE-4) router, which communicates with the PE-2 router of the service provider. Two routers are used for the two provider ends: PE-1 (London branch) and PE-2 (New York branch).

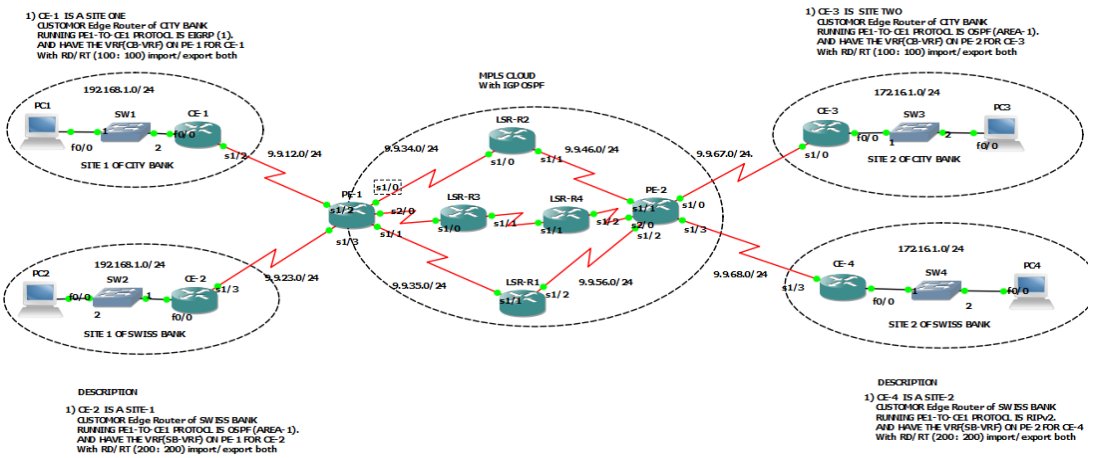

Fig. 7. MPLS Traffic Engineering Network Lab Topology

Further, the lab work used all important commands in the GNS3 command line interface (CLI) to retrieve the table's information.

V. TESTING RESULTS

The GNS3 experiment shows that the MPLS service provider (SP) have 2 customers (CB-VRF/SB-VRF) connected to PE-1 with RD/RT, as mentioned in the previous section. The two customers exchange routing

information between their branches, which are connected with PE-2 and communicate with each other.

During the test scenario all routing tables in routing provider end (PE-1) and one and routing provider end (PE-2) was checked by command for peering BGP VPN V4 with PE-2:

PE-1 # Show BGP VPnv4 Unicast All Summary as shown in figure 8 below:

```
class-map match-all DATA
  match protocol telnet
class-map match-all SMTP
  match protocol smtp
class-map match-all QOS
  match input-interface Serial1/2
class-map match-all VOICE
  match protocol rtp
!
policy-map ABC
  class DATA
   set ip dscp af43
  class VOICE
   set ip dscp ef
  class SMTP
   set ip dscp 33
  class QOS
    priority 512
```

Fig. 8. QoS Configuration with four Classes

```
interface Tunnel36
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 9.9.0.6
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 512
 tunnel mpls traffic-eng path-option 1 explicit name PE1-TO-PE2
!
```

Fig. 9. Traffic Engineering Configuration

PE-2 # Show BGP VPnv4 Unicast All Summary as shown in figure 10.

The service provider gives special treatment/QoS to the customer CB-VRF. For CB-VRF four classes were made, as shown in Figure 12, along with the QoS configuration.

Further, in the lab, three main parameters were also configured with priorities as follows:

- For voice, high priority with expedited forwarding was set with the DSCP value ‘ef’.
- For email, the DSCP value ‘af33’ assigned.

- For data, the DSCP value ‘af43’ was assigned for Telnet.

In this network activity, three main objectives were achieved as follows:

1) Configuration of MPLS VPN and MPBGP for the VPN V.4 route.

2) Configuration of MPLS traffic engineering (TE) for committed bandwidth where PE-1 is the head-end router, PE-1 is the tail-end router, and the explicated path is defined with a bandwidth of 512 Kb/s.

3) Configuration of a DiffServ QoS model to prioritise different traffic types initiated from a specific customer (CB-VRF). The output of the QoS parameters was taken from PE-1 to the LSR-2 link using the Wireshark tool. The bit was recorded through Wireshark as 0 without using QoS parameters; however, with configuration of QoS parameters for Telnet packets, the bit was 4.

Some of the other configuration files on BGP VPN and MPLS are shown as follows in figure 10 and 11.

```
PE-1#SH BGp VPnv4 Unicast ALL SUmmary
BGP router identifier 9.9.0.3, local AS number 9
BGP table version is 33, main routing table version 33
8 network entries using 1216 bytes of memory
8 path entries using 416 bytes of memory
8/8 BGP path/bestpath attribute entries using 1056 bytes of memory
5 BGP extended community entries using 604 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3292 total bytes of memory
BGP activity 16/8 prefixes, 16/8 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
9.9.0.6         4            9     215     216       33    0    0 03:06:13        4
PE-1#
```

Fig. 10. BGP VPNV4 in PE-1 peering with PE-2

```
PE-1#SHow MPLs FORwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing    Next Hop
Label      Label      or Tunnel Id     Switched      interface
17         No Label   192.168.1.0/24[V]   \
                                       0             Se1/2       point2point
19         No Label   192.168.1.0/24[V]   \
                                       0             Se1/3       point2point
20         Pop Label  9.9.0.4/32       0             Se1/0       point2point
21         17         9.9.0.6/32       0             Se1/0       point2point
           17         9.9.0.6/32       0             Se1/1       point2point
22         Pop Label  9.9.0.9/32       0             Se2/0       point2point
23         19         9.9.0.10/32      0             Se2/0       point2point
24         Pop Label  9.9.46.0/24       0             Se1/0       point2point
25         Pop Label  9.9.56.0/24       0             Se1/1       point2point
26         23         9.9.106.0/24     0             Se1/0       point2point
           23         9.9.106.0/24     0             Se1/1       point2point
           24         9.9.106.0/24     0             Se2/0       point2point
27         Pop Label  9.9.109.0/24     0             Se2/0       point2point
28         28         9.9.67.0/24[V]   0
29         32         172.16.1.0/24[V] 0
30         29         9.9.68.0/24[V]   0
31         30         172.16.1.0/24[V] 0
32         Pop Label  9.9.0.5/32       0             Se1/1       point2point
Local      Outgoing   Prefix           Bytes Label   Outgoing    Next Hop
Label      Label      or Tunnel Id     Switched      interface
33         Pop Label  9.9.13.0/24[V]   0             Se1/2       point2point
           Pop Label  9.9.13.0/24[V]   0             aggregate/CB-VRF
34         Pop Label  9.9.23.0/24[V]   0             Se1/3       point2point
           Pop Label  9.9.23.0/24[V]   0             aggregate/SB-VRF
PE-1#
```

Fig.11. MPLS forwarding table (LFIB-Lable forwarding Instance base table) of PE-1

A. MPLS Enabled Network

In the first case scenario, the routers were configured with MPLS VPNs on CE-1, CE-2 through the PE-1 and PE-2 routers, as shown in Figure 7 topology. The results captured by Wireshark software and are shown in table 1 (of delay, jitter and packet loss).

Table.1. MPLS Enabled VPN Network without QoS

PPS (as 1000)	Delay	Jitter	Packet Loss
3	0.000205	0.000040	0
6	0.000302	0.000056	0
9	0.000450	0.000150	4.5002
12	0.000660	0.000360	5.9900
15	0.000880	0.000550	10.89
18	0.000950	0.001101	12.506
21	0.001502	0.001255	17.95
24	0.001650	0.001425	18.558

B. MPLS-Enabled Network with QoS Parameters

In the second case scenario, the routers were configured with MPLS VPNs with DiffServ QoS model and took the results which CE-1 and CE-2 through PE-1 and PE-2 were generated as shown in table 2.

Table 2. MPLS-Enabled VPN Network with QoS

PPS (as 1000)	Delay	Jitter	Packet Loss
3	0.000656	0.000110	0
6	0.000698	0.000116	0
9	0.000710	0.000120	0
12	0.000720	0.000136	0
15	0.000725	0.000139	0
18	0.000729	0.000141	0
21	0.000735	0.000145	0
24	0.000741	0.000148	0

C. Result Analysis

From the lab test scenario described above, detailed values for delay, jitter, and packet loss are gathered with and without using the DiffServ QoS model over MPLS VPN. The results clearly show that, when QoS parameters are not used in the network lab, delay and jitter increased and varied with increased load; the load started with 3k packets per second and continue until 24k packets per second. The packet loos is also discovered high along with delay and jitter values. On the other hand, When DiffServ QoS model is implemented with same scenario and with same data the packet loss is remained zero and delay and jitter recorded is minimum as possible. This is because the parameters set priority to the data for voice, email and data.

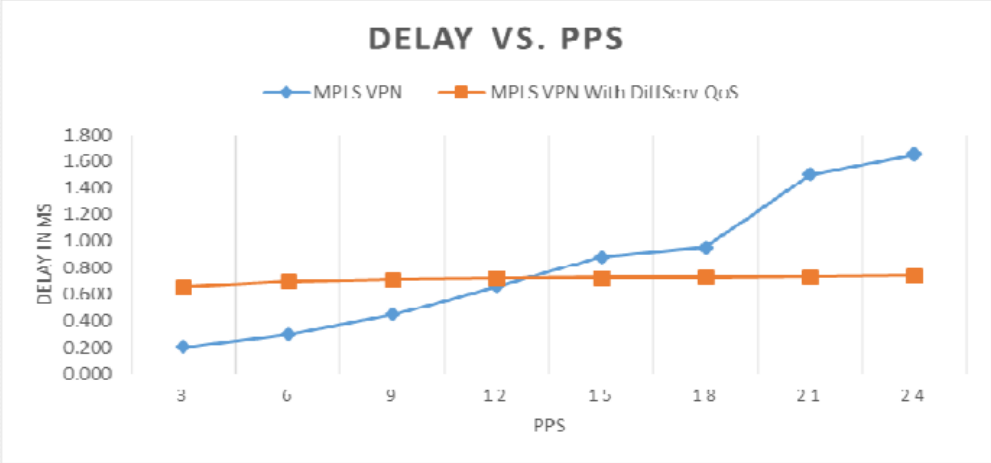

Figure.12. Delay Comparison

The graph in figure 12 shows delay versus packets per second (PPS). In MPLS VPN network the delay increases with the traffic increase on the network. However, in MPLS VPN with QoS, the average packet delay is 0.714 and is almost constant and low. The graph in figure 13 shows jitter versus PPS. In the case of MPLS VPN the jitter increases with traffic load and has more jitter compared to MPLS VPN with QoS. After Diffserv QoS is configured over MPLS VPN the jitter value is almost constant for increasing PPS. MPLS VPN with QoS jitter is almost 0.110ms. The variation with QoS is very low.

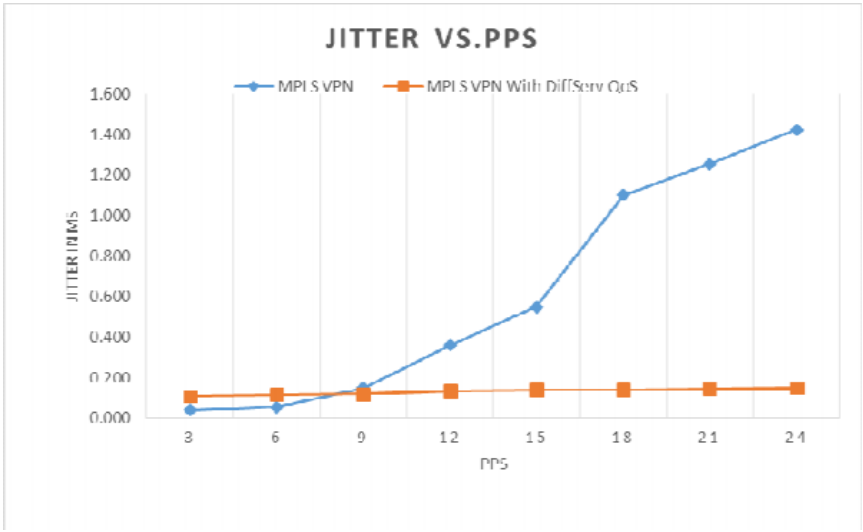

Figure.13. Jitter Comparison

The graph in figure 14 shows the relationship between packet losses in percentage with respect to PPS. In simple MPLS VPN enabled network

the packet loss is higher than in the MPLS VPN QoS. As we can see in figure 14, after configuring DiffServ QoS model the packet loss is 0%.

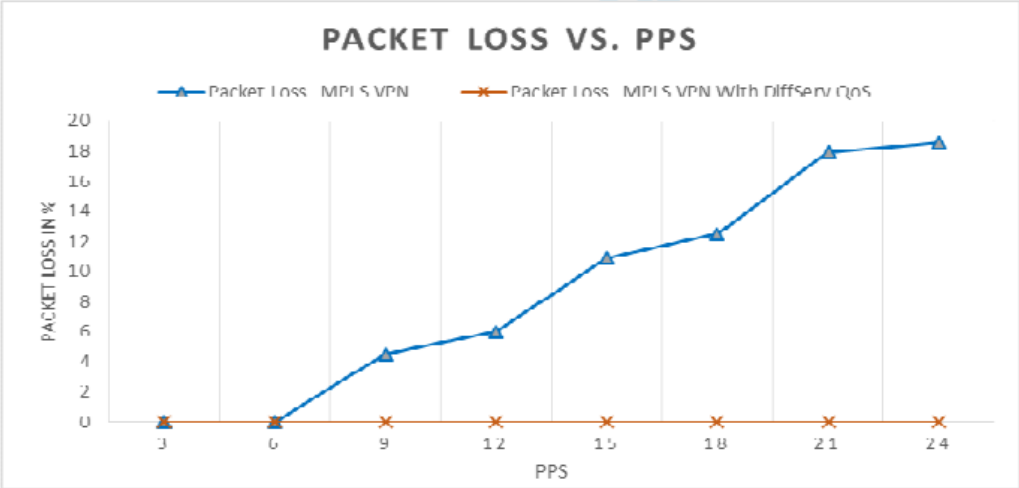

Figure.14. Packet Loss Comparison

VI. CONCLUSION AND RECOMMENDATIONS

There is growing concern in enterprise businesses around the world to improve their quality of services provided to their customers especially those companies who are dealing as Service Providers (SPs) as delays can cause huge amount of loss to the businesses that totally depends on their services and networks. Therefore, the popularity of MPLS VPN is growing for the WAN connectivity because it combines the features of VPNs and private WAN connectivity and that reduces the complexity of network operations and makes it more secure. There are generally concerns of the packet loss due to payload increase and hence more delay and jitter are expected. This problem can be resolved through utilizing DiffServ QoS model which is easy to implement over MPLS VPN network architectures. The enterprise networks mostly rely on the advance technologies to reduce their overall cost of services and improve the quality of their services through using these technologies. The DiffServ QoS model implemented in such scenario can really help where large business communicates with other branches around the world and trying to maintain the services at high level. This type of model provides a comprehensive solution framework for customer and service provider to use their resources more effectively and efficiently with minimum

delay and almost zero or low packet loss. The model itself doesn't create bandwidth but manage the bandwidth utilization where different applications can be set priorities. Our experimental results verify the effectiveness of MPLS VPN with DiffServ QoS model in enterprise networks.

REFERENCES

[1]. Hassani, S., Garmabdary, A. and Farahzadi, A. (2014). "The Presentation of MPLS-based Architecture (Multi-Protocol Label Switching) with Emphasis on Quality of Service (QoS)". Advances in Natural Applied Sciences, AENSI Journals, Vol. 8 (11), pp. 30-39.

[2]. Hyung-Woo, C, and Young-Tak, K. (2014). "Configuration Management for BGP/MPLS/VPN and DiffServ-aware-MPLS VPN". Dept. of Information and Commn, Eng., Yeungnam University, Korea.

[3]. Ya-qin, F., Lin-zhu, W. and Li-cui, Z. (2008). "Research for QoS of MPLS VPN Based on Log-infinitely Divisible Cascades". IEEE, 2008 International Symposium on Computational Intelligence and Design, Issued Date: Oct. 2008.

[4]. Kumar, S. (2014)." Study Paper on Implementation Quality of Services in IP Networks". Department of Telecommunications, Telecom Engineering Centre, New Delhi.

[5]. Al-Hadidi, M.R., Al-Gawagzeh, Y.M., Al-Zubi, N, Al-Saaidah, B. and Alweshah. (2014). "Performance Analysis of EIGRP via OSPF Based on OPNET and GNS3". Research Journal of Applied Science Engineering and Technology, 8(8), pp. 989-994.

[6]. Kaur, G. and Kumar, D. (2010). "MPLS Technology on IP Backbone Network". International Journal Computing application, 5(1), pp. 13–16.

[7]. Qureshi, K.N. and Abdullah, H.A. (2014).. "Multiprotocol Label Switching in Vehicular Ad Hoc Network for QoS". Information Management and Business Review, 6(3), pp. 115-120.

[8]. Alghawli, A.S. (2015). :"Method for Evaluating the Routing Cost in Mpls Network with Regard to Fractal Properties of the Traffic", International Journal of Soft Computing and Engineering (IJSCE), 4(6).

[9]. Naz, S., Siraj, T., Akbar, M., Yousaf, M., Qayyum, A. Tufail, M. (2014). "Performance Analysis of IPV6 QoS for Multimedia Applications Using Real Testbed". Procedia Computer Science, 32, pp. 182-189.

[10]. Ali, A.N.A. (2012)." Comparison Study between IPv4 & IPv6". International Journal of Computer Science, 9(3).

[11]. Pethe, R.M. and Burnase, S.R. (2011). "Technical Era Language of the Networking-EIGRP". International Journal of Engineering Science Technology, 3, pp. 1-5.

[12]. Zhang, D. and Ionescu, D. (2007). "QoS Performance Analysis in Deployment of DiffServ-aware MPLS Traffic Engineering". Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE Computer Society.

[13]. Luo, J., Zhao, T. and Yan, W. (2010)." A Mobile Infrastructure Based VANET Routing Protocol in the Urban Environment". Paper presented at the Communications and Mobile Computing (CMC), International Conference on.

[14]. Kiani, H.S. and Baig, M.H. (2010). "Performance Evaluation of MANET Using MPLS". MS Thesis. Bleking Institute of Technology, Sweden.

[15]. Fathy, M., Gholamalitabar-Firouzjaee, S. and Raahemifar, K. (2012). "Improving QoS in VANET Using MPLS". Procedia Computer Science, 10, pp. 1018-1025.

[16]. Daugherty, B. & Metz, C. (2005). "Multiprotocol Label Switching and IP. Part I. MPLS VPNs over IP Tunnels". Internet Computing, IEEE, 9(3), pp. 68-72.

[17]. Cisco (2015). "ICT at the Heart of NHS Reform". [Online]. Available online at: http://www.cisco.com/cisco/web/UK/public_sector/health_care/CiscoCNab/pdf/C-NAB_Post-Event_Slideware.pdf (Accessed: 10 April 2015).

[18]. Fan, Y., Wang, L., Zhang, L. (2008). "Research for QoS of MPLS VPN Based on Log-infinitely Divisible Cascades". IEEE, 2008 International Symposium on Computational Intelligence and Design.

[19]. Hacene, S.B. and Lehireche, A. (2011). "Coherent Route Cache in Dynamic Source Routing for Ad Hoc Networks". Computer Science Journal, 19, pp. 304-319.

[20]. Sulaiman, A. and Alhafidh, O.S.K. (2014). "Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering". International Journal of computer networks and communications security, 2(3), 93-101.

[21]. Jain, E.S. (2012). "Performance Analysis of Voice over Multiprotocol Label Switching Communication Networks with Traffic Engineering". International Journal of Advanced Research in Computer Science and Software Engineering, 2(7).

[22]. laSalle (2013). "The Importance of the QoS". [Online]. Available online at: http://blogs.salleurl.edu/raising-a-data-center/files/2013/04/qos.jpg (Accessed: 16 April 2015).

[23]. Khan, A.S. and Afzal, B. (2011). "MPLS VPNs with DiffServ – A QOS Performance Study". Master Thesis, Halmstad University, Sweden.

[24]. Kharel, J. (2011). "Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation". M.Sc. Thesis, School of Computing Blekinge Institute of Technology, Sweden.

[25]. Jamali, A., Naja, N., Ouadghiri, D.R. and Benaini, R. (2009). "Improving Quality of Service (QoS) in Multi-protocol Label Switching Module". IEEE Mediterranean Microwave Symposium.

[26]. Cisco (2006). "MPLS Traffic Engineering. Cisco Press. [Online]. Available at: http://www.ciscopress.com/articles/article.asp?p=426640 (Accessed: 20 April 2015).

[27]. Saunders, M. et al. (2010). "Organizational Trust: A Cultural Perspective".: Cambridge University Press.

[28]. Oates, B.J. (2006). Researching Information Systems and Computing. London: Sage.

[29]. GNS3 (2015). Information. [Online]. Available at: http://www.gns3.com (Accessed: 02 April 2015).

[30]. Press Release GNS3 (2014). GNS3 Technology. [Online]. Available at: http://www.gns3.com/media/Press_Release_Oct202014.pdf (Accessed: 25 April 2015).

[31]. Wireshark.org (2015). Introduction. [Online]. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html (Accessed: 20 April 2015).