ANALYSIS OF THREE PUBLICALLY AVAILABLE INTER-AS MPLS L3 VPN IMPLEMENTATIONS

A Thesis by

Abdulhakim Abubaker Abushaala

Bachelor of Engineering, Higher Institute of Industry, 1999

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

May 2012

AN ANALYTICAL DISCUSSION OF THREE PUBLICALLY AVAILABLE INTER-AS MPLS L3 VPN IMPLEMENTATIONS

The following faculty members have examined the final copy of this thesis for form and content, and recommends that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Computer Networking.

_____
Ravi Pendse, Committee Chair

_____
Neeraj Jaggi, Committee Member

_____
Linda Kliment, Committee Member

DEDICATION

To my hardworking family

ACKNOWLEDGEMENTS

On behalf of my entire family, I would like to extend my sincere gratitude to my advisor and mentor Dr. Ravi Pendse for his friendliness, continuous guidance, encouragement, and support during the course of this my MS study at Wichita State University; I shall never forget this unique period in my whole life. I am very thankful to my thesis examining committee members Dr. Neeraj Jaggi and Dr. Linda Kliment for their time and effort in reading this work and providing their comments and suggestions. Special thanks go to Murali Krishna Kadiyala for all his great advice on how to select, work on a research topic, and present the results. My appreciation goes to Amarnath Jasti and Vijay Ragothaman for their assistance at ANRI. Finally, my sincere thanks go to my affectionate parents and my whole family for their endless support in achieving such an important goal of my life and career.

ABSTRACT

In this thesis, an analytical discussion of the three publicly available Inter-autonomous system Multiprotocol Label Switching Layer-3 Virtual Private Network (Inter-AS MPLS L3 VPN) implementations, namely, Back-to-Back Virtual Route Forwarding, Single-Hop MP-BGP with static routes, and Multi-hop External Multiprotocol Border Gateway Protocol (MP-EBGP) between Autonomous System(AS)'s route reflectors. An analytical model is developed to evaluate the round-trip delay of a packet with respect to these three implementations. These implementations are used to provide MPLS L3 VPN between Internet Service Providers (ISP) or between different backbone networks within an enterprise. A testbed consisting of Cisco routers and switches is used to evaluate the three implementations in terms of impact of the design of these three implementation implementations on the round-trip delay. Priority queue is used on all routers in the testbed and the background traffic is assigned with the best-effort service. Priority traffic is marked CE routers. The testbed analysis shows that Single-Hop MP-BGP with static routes is the best among the three implementations with the least round-trip delay. Back-to-back virtual route forwarding exhibits the maximum delay.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AFI	Address Family Information
ASBR	Autonomous System Border Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CE Router	Customer Edge router
CEF	Cisco Express Forwarding
DSCP	Differentiated Service Code Point
EBGP	External Border Gateway Protocol
FEC	Forward Equivalent Class
FR	Frame Relay
GRE	Generic Routing Encapsulation
IBGP	Internal Border Gateway Protocol
Inter-AS	Inter-autonomous system
IPP	IP Precedence
IPSec	IP Security
ISP	Internet Service Provider
LFIB	Label Forwarding Information Base
LFIB	Label Forwarding Information Base
LSP	Label Switched Path
LSR	Label Switched Router
MAC	Medium Access Control
MP_REACH_NLRI	Multiprotocol Reachability Network Reachability Information

MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
OSI	Open System Interconnect
OSPF	Open Shortest Path First
P Router	Provider Router
P2P	Point to Point
PE	Provider Edge router
PQ	Priority Queue
QoS	Quality of Service
RD	Route Distinguisher
RIB	Routing Information Base
RR	Route Reflector
RT	Route Target
SAFI	Subsequent Address Family Information
UDP	User Datagram Protocol
VPN	Virtual Private Network
VPNv4	Virtual Private Network Version 4
VRF	Virtual Routing Forwarding
WRED	Weighted Round Early Detection

CHAPTER 1

INTRODUCTION

There are three implementations to establish Inter-AS MPLS L3 VPNs, namely, Back-to-Back VRFs, Single-Hop-MP-EBGP-between ASBRs, and Multi-Hop-MP-EBGP-between ASs' RRs, respectively. These implementations use different concepts to accomplish each one, however, each concept has advantages and disadvantages. More specifically, delay, the most important factor that impacts the overall performance, varies in each implementation. This thesis addresses this essential factor.

This chapter explains the essential concepts associated with MPLS L3 VPN, followed by the thesis organization.

1.1 MPLS

In IP routing and forwarding, route next hop, egress interface, and frame forwarding treatment look up must happen in every single hop from source to destination, and we can call this per hop behavior (PHB). Even though nodes do exchange dynamic routing routes between them, each node (hop) will individually need to do the route and egress interface look up and either use process switching or fast switching to switch the frame from ingress to egress interfaces. In MPLS, however, this lookup process for: route next hop, egress interface, and frame forwarding treatment is calculated only by the ingress label switching router (LSR) because the next hop for the packet is actually not the directly connected router but is instead the egress LSR (E-LSR) of the LSP which label is known from the directly connected Ingress LSR's (I-LSR) next hop router. So I-LSR will push the label and other routers in the path just swap labels from inbound to outbound interfaces. Therefore, delay in calculating Forward Equivalent Class (FEC) and Label Switched Path (LSP) establishment can be ignored as it is not calculated

for every single packet traversing the LSP. But it is worth mentioning this step because it does count as a fundamental difference between the IP routing and the MPLS switching. [14]

1.2 Virtual Private Networks (VPNs)

The need to interconnect private networks of the same administrative domain through public networks (e.g. Internet) is rapidly increasing as new business models evolve and emerge. This GRE technique is known as Virtual Private Network (VPN). VPNs can be established at Open System Interconnect (OSI) L2, L3, or L4. The basic requirement in such technology is that VPN sites stay separate from other provider traffic and VPN packets' data stay intact when traversing the provider's network. The most common method for providing VPN is by tunneling VPN traffic inside other L3 or L2 protocols, IP Security (IPsec)/Generic Routing Encapsulation (GRE), Asynchronous Transfer Mode (ATM), and Frame-relay (FR) respectively. This method is known as Overlay Networks (ON). This manner has some drawbacks in terms of limitation, and scalability. The main scalability issue occurs when VPN sites need to be fully connected (meshed) together. This requirement requires $N(N-1)/2$ VPNs, point-to-point (P2P) tunnels, and is very complicated to setup as well as manage, in addition to over utilizing the edge VPN devices' resources. The other challenge or limitation is applying different QoS treatment to the tunnel VPN traffic, where the VPN would carry multiple flows using different transportation protocols, e.g. User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). Since the intermediate routers cannot read the VPN traffic, there is no way that Quality of Service (QoS) can be effectively applied. Nonetheless, encapsulating VPN data inside other protocols means that payload size is affected as the VPN protocols' headers size is deducted from the packet payload so that the L2 frame does not exceed the Maximum Transmission Unit (MTU) of the data-link layer. [15]. To overcome the above challenges and limitations in the overlay VPNs,

MPLS, as a data-plane protocol, and as a transport protocol, is used to carry the VPN routes/packets/frames across backbone networks or ISPs. Routing protocols (IGP or EGP) are used to signal or exchange the routes between the end VPN sites. MPLS VPN is comprised of the following elements:

- Virtual Routing Forwarding (VRF)
- Route Distinguisher (RD)
- Route Target (RT)
- Multiprotocol-Border Gateway Protocol (MP-BGP)

A brief description of these elements is as follows.

1.3 Virtual Routing Forwarding (VRF)

As a first point of separating VPN routes from other VPN or provider routes, VRFs are private-virtual routers inside the PE routers, and are attached to the interfaces connected to the CE routers to provide separate control and data planes to other VPN routes and/or global routing protocols. Each VRF has its own VPN routing table, IP routing table, and data forwarding table (Cisco Express Forwarding (CEF)). The consolidation of the VPN IP routing table and the VPN IP forwarding table is known as the VPN Routing and Forwarding instance (VRF). VRF is what makes MPLS VPN private as a fundamental VPN concept. PE interface connected to the CE routers can have only one VRF attached to it so that packets that enter this interface are forwarded to the attached VRF instance. As in the global data forwarding table, the CEF table is derived from the VPN routing table. [5]

1.4 Route Distinguisher RD

To propagate the VPN routes between PE routers, and since the VRFs are kept separate, IGP cannot be used to distribute VPN routes, which should not be seen in the core, between VRF

instances on peer PE routers as. The only protocol that supports inserting VRF routes into its update messages is the extended version of BGP known as Multi-Protocol BGP (MP-BGP). Since these update messages may contain other VRF routes and due to the fundamental concept of VPN where VPN sites can use the same private range IP addressing, route overlap can occur, and so a way to identify/tag VPN routes is needed and that is known as the Route Distinguisher (RD). Basically it is a string of 64-bit field appended to VPN routes for each VRF instance. In other words, each VRF must have one RD associated with it at the PE routers. The RD is locally significant to the PE router and is not the VPN identifier. The following formats can be used to compose the RD string: 2-byte AS number+ 4-byte NN, 4-byte AS number (ASN)+ 2-byte NN, and 4-byte IP address (router ID) + 2-byte NN where NN is an unique number, represents a code to a VRF, and ASN is the AS number. Usually, ISPs use ASN:NN format. ASN is assigned to providers by the Internet Assigned Numbers Authority (IANA). The combination of RD and IP prefix is known as the VPNv4 route, which is 96 bits long for the address and 32 bits for the subnet mask. As an example, if the IP address is 10.10.10.1/24 and the RD is 65001:44, the VPNv4 address will become 65001.44:10.10.10.1/24. The combination of RD and IP prefix is known as BGP VPN-IPv4 Address Family Information (AFI) and is the one carried in the MP-BGP updates. [17] [5]

1.5 Router Target (RT)

With RD VPN routes are distinguished by the 64-bit field, however, RD is not a sufficient attribute to distribute VPN routes between PE routers with multiple VRFs. The reasons for that are: that RD should not be identical at PE routers, that RD is not the VPN identifier, that MP-BGP does not know which VRF the routes should be imported to (when receiving updates from the peer PE) that another tagging is used, and that the possibility that one VRF can talk to

multiple VRFs e.g. the VPN VRF and the Internet VRF. To overcome these issues, another attribute is used which is known as Route Target (RT). RT is an additional attribute appended to the VPNv4 routes to globally distinguish them and indicate the membership of each VRF/VPN. MP-BGP, as depicted in the figure 1.1, uses this attribute to import and export routes, from/to VRFs. RTs are attached to VPN routes during the conversion from IPv4 to VPNv4 routes. When receiving VPNv4 routes from a peer PE, the receiver, has the choice as to whether or not it should receive the routes based on the configured RT Export and Import statements. After receiving the routes PE converts them to VPN IPv4 routes and adds them to the VRF-VPN IPv4 routing table, then the VRF routing protocol (IGP or EGP) redistributes these routes to the CE routers to complete the route propagation process. RTs are encoded in the MP-BGP updates as an extended community route target [17].

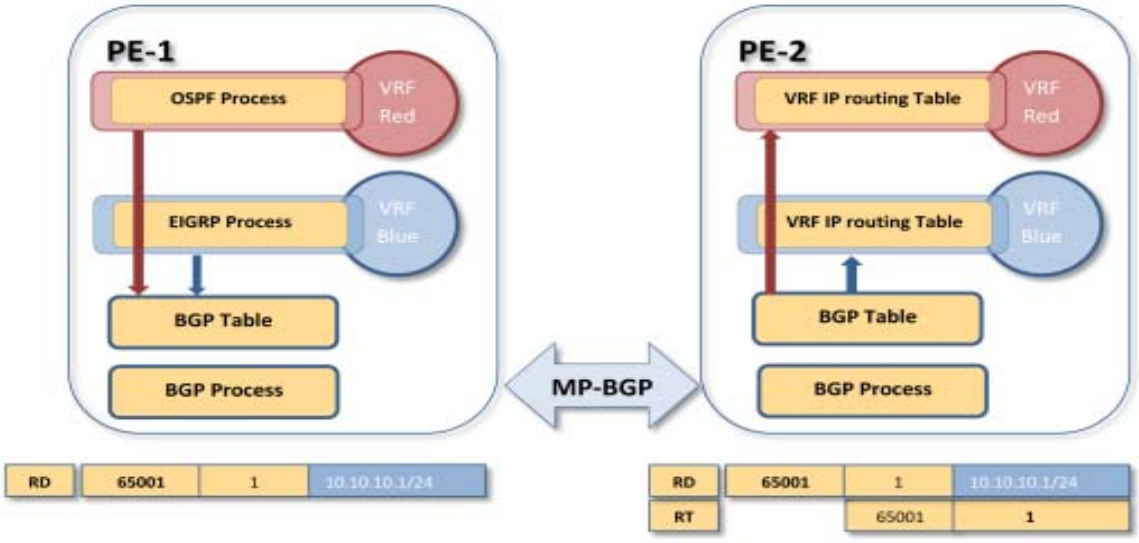


Figure 1.1. Relationship between Route Distinguisher and Router Target

1.6 Multi-Protocol Border Gateway Protocol (MP-BGP)

MP-BGP is an extension to the traditional BGP and is the building block of MPLS VPN as it exchanges VRF information between PE routers for unicast and multicast routing to be

carried in interconnected networks. Native BGP protocol is limited to support carrying unicast routes for IPV4 forwarding and does not carry any information besides that one associated with the IPv4 unicast routes. MP-BGP came to support multiple features or protocols (IPv6, CNLS, IPv6, MPLS tags, and VPNv4 routes) which were not supported. There are two attributes that carry the new supported protocols and features: MP_REACH_NLRI and MP_UNREACH_NLRI. NLRI stands for Network Layer Reachability Information. NLRI is exchanged between the MP-BGP speaking routers through the UPDATE message. MP-BGP sends updates about reachable destinations using the MP_REACH_NLRI attribute, and updates about the unreachable destinations using MP_UNREACH_NLRI attribute. MP_REACH_NLRI attribute contains one or multiple triples. The following are the attributes which MP-BGP uses for MPLS VPN: Address Family Information (AFI), Subsequent Address Family Identifier (SAFI), Next Hop Information, and the NLRI. AFI represents the network layer protocol, and AFI =1 means the network protocol is IPv4. SAFI carries the subsequent protocol along with the network layer protocol. When AFI is set to 1 and SAFI is set to 128 the NLRI is an MPLS-labeled VPNv4 address/route. This particular NLRI is encoded in such a manner that 8-byte for the RD is followed by the IPv4 prefix. MP_UNREACH_NLRI attribute carries AFI, SAFI, and withdrawn routes. The withdrawn-routes field lists the NLRI for the prefixes the router withdrew from its BGP routing table as well as the global routing table.

1.7 MPLS L3 VPN

Multiprotocol Label Switching Layer-3 Virtual Private Networks (MPLS L3 VPN) rely on MP-BGP to exchange VPNv4 prefixes between PE routers and on MPLS to transport these prefixes across the core routers, which are unaware of the VPNv4 prefixes. Figure 1.2 depicts how the end-to-end MPLS-VPN messages exchange in the control plane. In Inter-AS MPLS L3

VPN, there are three implementations to transport VPNv4 routes between PE routers across multi-AS boundaries. In implementation one, known as Back-to-Back VRF, each VRF works as ASBR when receiving routes from the peer ASBR, and also as a CE when sending routes to the peer ASBR. In this implementation, ASBR routers must have a VRF for each VPN network which must be attached to either a physical interface or a sub-interface. In the second implementation known as Multi-Hop MP-BGP between ASBR routers, the routers exchange their loopback IP addresses to preserve the VPNv4 label to reach each ASBR. This will preserve the QoS marking in the EXP field. In this implementation, ASBR routers store VPNv4 routes in their RIB tables. The third implementation is known as Multi-Hop MP-BGP with next-hop unchanged between AS's P routers. In this implementation, only one MP-BGP label is used to carry the VPNv4 routes between AS's PE routers. ASBR routers are unaware of the VPNv4 routes and labels, and therefore do not store any VPNv4 routes in their RIB and LFIB tables. Therefore, the end-to-end delay varies in the three implementations and is analyzed in this paper.

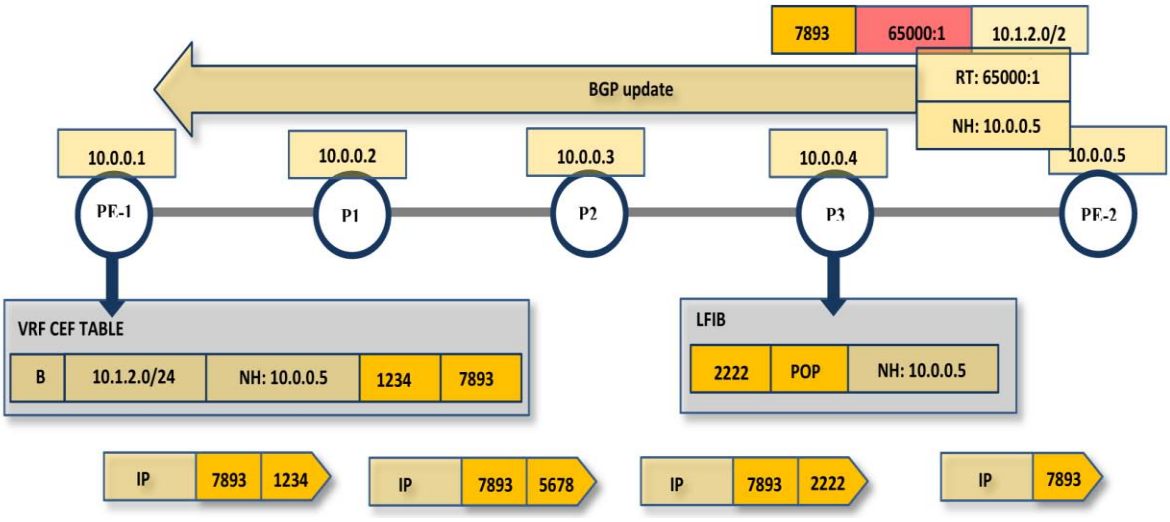


Figure 1.2 End-to-End MPLS-VPN Forwarding

1.8 Queuing

Ideally, after marking and classification, packets should be switched from the ingress to egress directly. However, in reality this is not the case because packets from multiple ingress interfaces are sent to a lesser number of egress interfaces which means that the packets need to be buffered and scheduled based on different parameters. Therefore, queuing is a very important stage in switching packets as it buffers packets for an inconstant time, which is called the queuing delay. As there are different queuing techniques and different drop methods queuing delay should be carefully studied along with the drop method when the particular queue becomes full. In this case some protocols like UDP will not be affected; however TCP can be degraded even if the queuing delay is minimal. For instance, when the TCP ACK packet gets dropped using the tail drop method when the particular queue was full, the TCP throughput will be impacted, as a result.

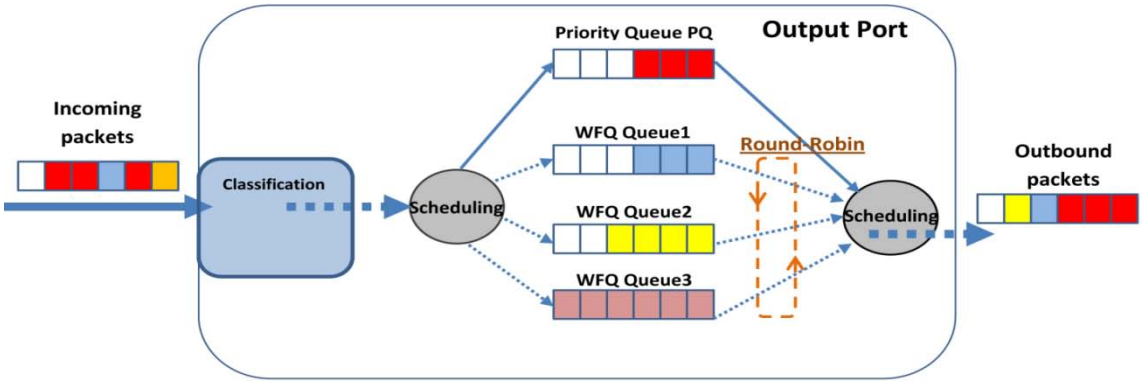


Figure 1.3 Weighted Fair Queuing and Priority Queuing

1.9 Thesis Organization

The reminder of this thesis is organized as follows. The second chapter presents problem description, related work and the proposed analysis. The third chapter presents an analytical discussion of the three implementations. The fourth chapter presents the simulation results and their analysis. Chapter 5 presents the conclusions.

CHAPTER 2

LITERATURE SURVEY

This chapter presents the literature survey on MPLS, MPLS VPN, and Inter-AS MPLS VPN networks in the following sections. Extensive research has been done to test the performance of MPLS VPN, single AS and multi-AS, with respect to MPLS as a transport technology as well as a QoS solution for complex network design requirements. However, much less research has been done on the impact of the three- Inter-AS implementations on the end-to-end delay when QoS is applied to the routers in the path. Delay is the most important factor to most applications as it can have an unavoidable impact on the performance. No research has been done to evaluate the three implementations with respect to the end-to-end delay and for that an analytical model in proposed which shows the different delays that occur on every hop on the path and their impact on the end-to-end delay. The results show that implementation 1 has the highest delay, implementation 2 and 3 are similar and have the least delay. The results from the test-bed show a similar result to back the proposed analytical model.

Hachimi et al [2] studied the performance of single-domain MPLS VPN with QoS techniques with regard to utilizing the interface queues in routers when traffic conforms or exceeds the specified thresholds. The authors proposed a scheme of sharing the interface queue between two sub-queues for different VRFs so that these queues utilize the unused buffer space of the interface queue when one queue's buffer is getting filled. They used a two-stage scheduler, one for each VPN, before the main interface scheduler. A sub-scheduler can dynamically mark the out-of-contract traffic or bandwidth in such a way that guarantees forwarding packets and not dropping them or remarking them with the least treatment which can cause high jitter. However, the impact of proposed scheme on delay was not studied.

H. Yamada's [1] analysis of the performance of Inter-AS MPLS VPN was carried out using OPNET as a simulation program; however, due to the complexity of the implementations of this Inter-AS VPN techniques, the current OPNET software does NOT support this technology of VPN. The research was carried out using only the first implementation, Back-to-Back VRFs. Hachimi et al. [2] and Ming-hu [3] research showed that OPNET is the most suitable simulation software for MPLS VPN [3]. Several analytical models have been proposed to evaluate the performance of traditional, single-domain, MPLS VPN with regard to Differentiated Service (DiffServ), Integrated Service (IntServ) QoS, Traffic Engineering (TE), and TE re-route, using network simulators e.g. NS-2, OPNET, etc. Xia et al. [4] concludes that MPLS VPN does synthesize the traditional IP and ATM VPN implementations and does offer great scalability over traditional IP or ATM VPNs.

Khan et al. [6] focused on using MPLS VPN as a Wide Area Network (WAN) technology with a full support of QoS. Their analysis showed that implementing MPLS VPN with DiffServ showed a better performance over IP and MPLS without DiffServ. Using a real testbed consisting of Cisco Routers, results showed that end-to-end delay, jitter, and packet loss in different packet transmission rates and in different traffic types had very low variations or was almost constant. The NS-2 simulations done by Veni et al. [5] showed that delay and packet loss improved after applying MPLS over a traditional IP network. Also MPLS TE utilized links much more than when a traditional IP network was used.

Analysis in Palmieri [7] was carried out to compare the two predominate VPN technologies, IPSec and MPLS VPN, with respect to scalability as long as performance on the high speed Fiber core networks. This study showed that single-AS MPLs VPN has a better performance in terms of RTD and packet loss, and is more scalable than the aging IPSec as it

does not require a full mesh overlaid on IP network(s). It requires only adding small changes on two PE routers without encryption/decryption needed (less end-to-end- delay), does not need Network Address Translation (NAT), which means that audio and video applications can work natively; and it fully supports guaranteed QoS implementations end-to-end as it is completely independent and isolated from the ISP network.

Research by Zhang et al. [8] focused on node mobility as well as site mobility has been utilizing the MPLS L3 VPN interconnect-network to study the behaviors of the mobile applications when either mobile host leaves one wireless site or the wireless site leaves the provider core (lose connection to the PE routers), and the impact of such scenarios on the mobile application. Furthermore, solutions were proposed to help perform a free hand-off when joining other connections to the backbone (core) network without losing the connection to the backbone network, and reducing the chance of packet loss during the hand-off.

Ren et al. [9] studied securing the packet's payload by encrypting the payload at the CE routers, before forwarding the packets to the PE routers. IPsec was used in tunnel mode between CE routers on different VPN sites to guarantee the confidentiality of the data packet. This extra layer of security impacted the overall performance in terms of encryption and decryption delay as well as reducing the packet payload because of the overhead IPsec header appended to every packet. This can impact the TCP more than the UDP as the TCP Maximum Segment Size (MSS) was less than when there is no IPsec used.

To overcome the requirement that ISPs network must run IP MPLS to be able to offer MPLS VPN service, GRE was used to tunnel MPLS traffic over the traditional IP networks in ISP. Lee et al. [10] MPLS signaling and encapsulation is enclosed inside a GRE header between VPN sites routers, PE or CE. The drawback of this approach is less performance the native

MPLS VPN and limited QoS guarantee when IP packets traverse single or multiple provider managed backbones.

One of the main features of MPLS is that it's ability to preserve QoS marking, end-to-end. As the label swapping copies the bits in the EXP field of the ingress label to the EXP field of the newly imposed/pushed label, and when MPLS tagged packets are carried on packet switched networks either native IP MPLS or tunneled IP MPLS (using GRE and/or IPsec). As with IP QoS, different queuing techniques are used to achieve effective queuing depending on the SLA agreed upon when using MPLS QoS. Results showed that packet loss of background traffic (best-effort traffic) is higher when assigning priority traffic to the priority queue, as by design packets in this queue get serviced ahead of any other packets in the other queues. Misconfigured priority queuing can starve the egress interface's bandwidth only for priority traffic. On the other hand, Mirjalily et al. [11] confirmed, using a Hardware (HW) testbed, that priority queuing helps with offering less constant delay and jitter, which are the main measures of performance. Hošek et al. [12] and Aziz et al. [13] used another queuing method known as Weighted Fair Queuing (WFQ) and concluded that this method helps with compromising the delay as well as packet loss when configured properly. The test results showed that tuning PQ and WFQ with the use of MPLS can result in better overall performance, and meet SLA requirements for priority traffic as well as best-effort traffic with multiple classes/weights. And for queuing management, Assured Forwarding (AF) Per Hop Behavior (PHB) type and Weighted Random Early Detection (WRED) queue management are the most suitable for leveraging networks resources for average loaded networks. Guofu [14] evaluated MPLS VPN QoS as an alternative to IP QoS for a monitoring system for high way traffic and operation, and results showed that the system maintained better performance and scalable-efficient use of QoS

requirements in the system. Wu and Zhan [15] studied how MPLS with QoS can offer scalable enhancements to the user in IP Multi-media Subsystem (IMS) interconnect. Their results show that MPLS can integrate the guaranteed QoS with IMS user sessions even when crossing multiple network domains that comprise the Next Generation Networks (NGNs) with regard to Multimedia stream sharing.

Saika et al. [16] proposed a solution to the labels consumption when if MPLS is used as a core transport in the internet core. They used MPLS-TE to encapsulate the MPLS tagged IP packet in the network core which may work with multicast to reduce the label consumption and thus enhance the overall performance of the internet.

From the above discussion, it can be seen that the previous research focused on the MPLS technology for better solutions in terms of QoS as well as scalabilities. However, the three implementations for Inter-AS MPLS L3 VPN were not discussed and tested. This thesis presents an analytical discussion of the three inter-AS MPLS L3 VPN implementations, and compares them in terms of round-trip delay. The following chapter presents the analytical discussions.

CHAPTER 3

ANALYTICAL MODEL FOR MPLS VPN DELAYS

This chapter presents an analytical discussion of the three, publicly available Inter-AS MPLS L3 VPN implementations, and compares them in terms of packet round-trip delay. This chapter is divided into two sections. Section 3.1 discusses various delays involved in transmitting a packet on an Inter-AS MPLS L3 VPN network. Section 3.2 presents the analysis of the three implementations with the network diagrams.

3.1 Data-Plane Delays Analysis

This section discusses the delays associated with the MPLS. We will focus on the data-plane delay as it is the one which will positively impact the data transmission delay, the goal of this thesis.

Since most of the data forwarding is done by MPLS, the time taken by the routers to forward packets from ingress to egress interfaces is very small and can be ignored. However, as mentioned in the previous chapter, congestions can occur in the real life networks which will cause the router to hold the packets in the queues before forwarding packets to the egress interface queue. This packet holding delay is known as the queuing delay. One of the important delays that can cause a slightly more considerable delay is the packet classification delay($D_{CL_{ip}}$). It occurs when matching interesting traffic packets using IP Precedence (IPP), Differentiated Code Point (DSCP), and the MPLS header's Experimental (EXP) field. Another considerable delay is the route lookup delay the routers take to find the destination route, inside the VRFs forwarding table, when receiving a packet destined for that particular VRF. This delay occurs at the PE routers only. Provider (P) routers are unaware of the VPN traffic and look up. In the coming section we are going to discuss the number of times this delay occurs and its impact on

the overall delay. Hardware interrupts are generated by the routers interface controllers when the egress interface queue gets filled up. The interrupts are generated to inform the router to slow down as the newly sent packets are going to be dropped at the interface queue. This queue is First-In First-Out (FIFO) and thus the router cannot use any kind of scheduling at this point. This type of delay occurs in bursty traffic scenarios, where a particular interface is receiving more packets than the interface controller can send on the wire, or the interface queue is filled up. The last data-plane delay is associated with marking the packets, both in IPv4 format or in MPLS frames. When dealing with IP packets marking can be done only at the ingress interface or either the CE or PE routers. On the other hand, marking MPLS frames could be necessary at multiple routers and ingress interfaces. As an example, if the CE routers mark the IP packet using the DSCP field, the 6-bit long field, then marking at the PE router or ASBR, ingress interfaces is required. Marking at these routers is necessary because DSCP field is longer than the EXP, and so manual marking is required when needed.

Following subsection discusses the three implementation scenarios with respect to data forwarding

3.2 Inter-AS MPLS VPN Operation

This section presents a scenario-based discussion of the Inter-AS MPLS L3 VPN along with the network topology.

Figure 3.1 presents the topology of implementation 1. CE -1 represents VPN site-1 and CE-2 represents VPN site-2. Both CEs act as the source as well as the destination. VRFs are used in PE and ASBR routers in both AS clouds to tunnel VPNv4 routes between PE routers. The interfaces connecting the ASBR routers do not run LDP. Instead, eBGP is configured between

these interfaces. The MPLS domains of both AS clouds are completely isolated, and they do not exchange VPNv4 routes. Therefore, both ASBRs send VPN packets as layer 3 IPv4 packets.

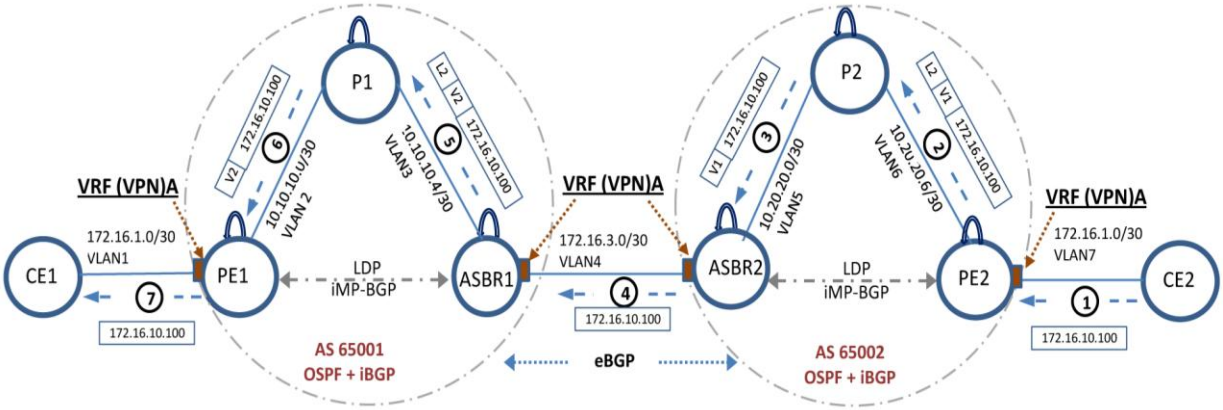


Figure: 3.1 Testbed for implementation-1

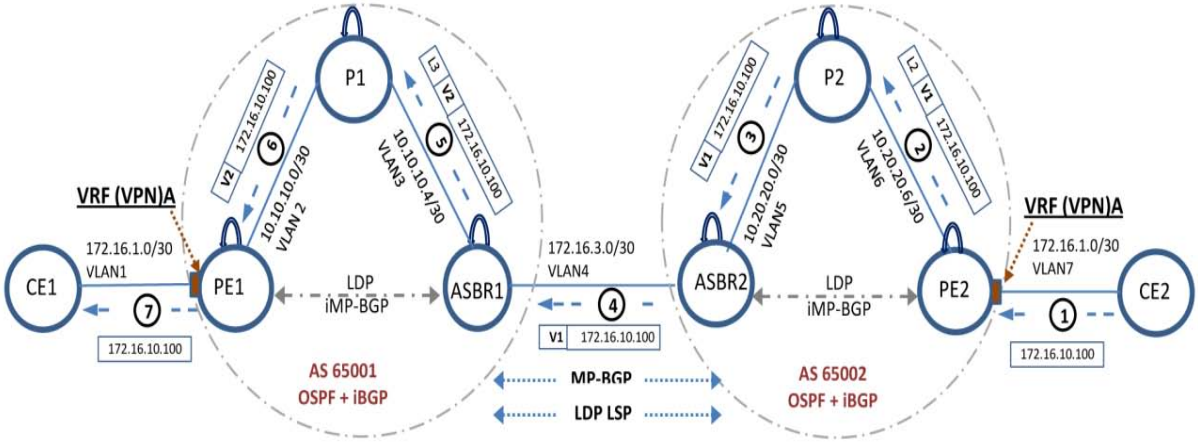
When receiving IPv4 packets, each ASBR acts as a CE router to the other ASBR, and vice versa. RT delay associated with implementation-1 ($D_{RT}Im1$) for number of the ISPs or ASs (nISP) consisting of nRTR each is presented in the following equation; where $nRtrN$ is the number of routers in the whole network (testbed), $D_{CL_{ip}}$ is the IP classification delay, $D_{VRF_{lkup}}$ is the look up delay within each VRF, and similarly $D_{CL_{exp}}$ is the delay associated with classification of packets based on MPLS EXP value. D_{POP} and D_{PUSH} are the delays associated with POPing and PUSHing labels respectively.

$$D_{RT}Im1 = 2\Big[(n\text{ISP} * n\text{RTR}) * (3 * D_{CL_{ip}} + 2D_{CL_{exp}}) + \big(nRtrN * D_Q\big) + (2 * D_{PUSH} + D_{POP}) + (nPRtrN * D_{POP}) + (2 * D_{PUSH} + D_{POP}) + \Big[(n\text{ISP}) * 2\Big(D_{VRF_{lkup}} + D_{LFIB_{lkup}}\Big)\Big]\Big] \quad (1)$$

Figure 3.2 presents the topology of implementation-2. The difference between the implementation-1 and 2 is that the ASBR routers do not have VRFs. ASBR routers run LDP and enabled MPLS on inter-AS link's interfaces to have LSP between ASBRs' loopbacks. eMP-BGP

was used between ASBRs' loopback interfaces to distribute VPNv4 routes and signal their labels to be used in the MPLS data-plane. As a result, each ASBR resets VPNv4 labels when receiving them for the peer ASBR. However, egress ASBR does not reset these labels.

Figure: 3.2 Network topology of implementation-2



RT delay associated with the implementation-2 ($D_{RT}Im2$) is represented by the following equation. The same previously mentioned delay names are used in this equation as well. The difference between the two equations is the number of occurrences of particular delays e.g. $D_{VRF_{lkup}}$.

$$D_{RT}Im2 = 2\Big[(n\text{ISP} * n\text{RTR}) * (2 * D_{CL_{ip}} + D_{CL_{exp}}) + \big(nRtrN * D_Q\big) + (2 * D_{PUSH} + D_{POP}) + (nPRtrN * D_{POP}) + (2 * D_{PUSH} + D_{POP}) + \Big[(n\text{ISP}) * \Big(D_{VRF_{lkup}} + D_{LFIB_{lkup}}\Big)\Big]\Big] \quad (2)$$

Figure 3.3 presents the network topology of implementation-3. In this scenario, no VRFs are used in the ASBR routers. Multi-Hop EMP-BGP is running between either P routers' loopback interfaces to exchange VPNv4 routes and signal their labels. Also, a Single-Hop eMP-BGP is configured between the ASBRs' physical interfaces on the Inter-AS link to redistribute

the host routes associated with the PE and P loopback interfaces of each AS to the other ASBR, and then to their peer AS cloud. As a result, PE routers have an end-to-end VPNv4 LSP path between them as the next hop does not change when the BGP advertises the routes to peers on intermediate routers. ASBRs swap IPv4 labels when sending packets to peer the ASBR. QoS matching is done using either the MPLS topmost label's EXP value (value 7) on the ingress interface facing P routers or qos-group on the egress interface facing the other ASBR. Seventy percent (70%) of the interface bandwidth capacity is allocated to the priority queue and 30% is allocated to the best-effort queue on all routers. In this scenario, the ASBR routers do not participate in signaling the VPNv4 routes' labels, and they do not store VPNv4 routes in the RIB table. The routers only signal the labels of the IPv4 routes and RESET/SWAP labels from both P and peer ASBRs.

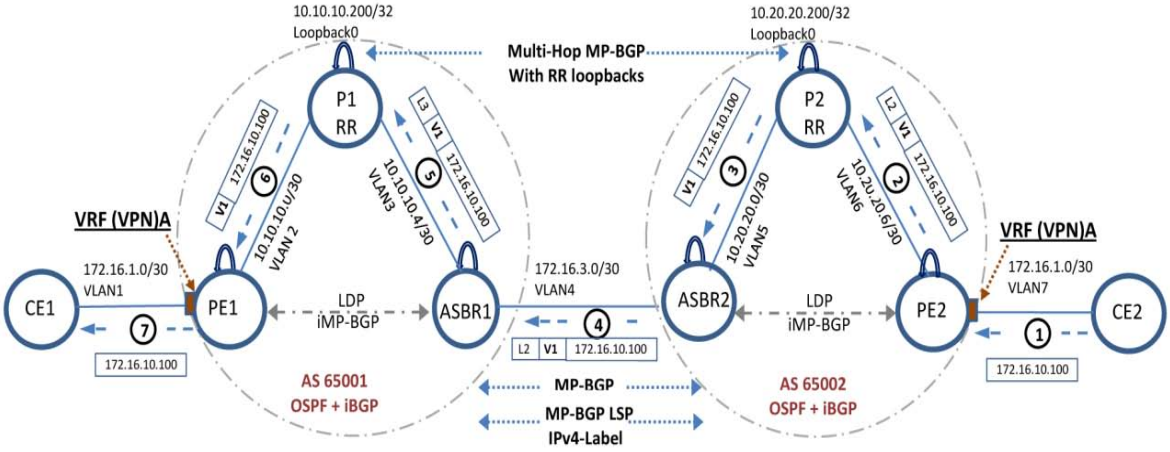


Figure: 3.2 Network topology of implementation-3

The following equation represents the RTD associated with implementation-3 ($D_{RT}Iml3$)

$$D_{RT}Iml3 = 2\Big[(n\text{ISP} * n\text{RTR}) * (2 * D_{CL_{ip}} + D_{CL_{exp}}) + \big(nRtrN * D_Q\big) + (2 * D_{PUSH} + D_{POP})$$
$$+ (nPRtrN * D_{POP}) + (2 * D_{PUSH} + D_{POP})$$
$$+ \Big[(n\text{ISP}) * \Big(D_{VRF_{lkup}} + D_{LFIB_{lkup}}\Big)\Big]\Big] \qquad (3)$$

Thus, this chapter presented an analytical discussion of the Inter-AS MPLS-L3-VPN implementations.

CHAPTER 4

SIMULATIONS AND RESULTS

This chapter presents simulations, their results, and an analysis of their results. Figures 4.1, 4.2, and 4.3, present the Inter-AS MPLS L3 VPN implementations, namely, Back-to-Back VRFs, Single-Hop-MP-EBGP between ASBRs, and Multi-Hop-MB-EBGP between ASs' RRs, respectively.

A testbed consisting of 3640 and 3660 Cisco routers and Catalyst 3550 Cisco switch, was built to test the three implementations. All devices interfaces are Fastethernet set to full duplex and a speed of 100Mbps. The Open Shortest Path First (OSPF) routing protocol was used as the Interior Gateway Protocol (IGP). MP-BGP were used to carry VPNv4 routes as well as exchange VPNv4 labels. EBGP and MP-BGP were used between the ASBR routers to carry IPv4 and/or VPNv4 routes and labels.

Table 4.1 shows the different packet sizes and different packet rates used in the simulations. The packet payload varies from 560B to 1440B. The packet transmission rate varies from 1000 packet per second (PPS) to 2000PPS. The UDP background traffic was fixed to a payload of 590B and a transmission rate of 1000PPS.

TABLE: 4.1
SIMULATION PACKET SIZE(S) AND PACKET TRANSMISSION RATE(S) FOR THE SIMULATION PRIORITY TRAFFIC AND BACKGROUND TRAFFIC

Packet Size In Bytes	**Rate Packets/Sec**	**Background Packet Size In Bytes**	**Background Traffic Rate Packets/Sec**
560	1000	590	1000
100	1400		
2000	1600		
	2000		

4.1 Simulation Results

This section presents the simulation results for the three Inter-AS MPLS L3 VPN implementations testbeds. Priority queue has been used on all routers in the path, CE-to-CE, in order to guarantee that packets get routed ahead of any other packet, to have an accurate results, which makes this simulation valid for evaluating the performance of the three implementations with respect to RT delay. Interface bandwidth was set to the maximum interface capacity. Marking was done in the CE routers and no traffic policing was used. QoS policies were applied to all interfaces, ingress and egress, from CE-1 to CE-2, end-to-end. That way we can guarantee that routers treat priority traffic ahead of the background traffic and to get accurate delay measurement. The priority queue was given 70% of the egress interface bandwidth and the best-effort queue was given the remaining 30%.

Table 4.2 shows the effect of packet size and packet transmission rate on the round-trip delay for traffic sourced and destined from/to CE routers, when using implementation-1. Background traffic was fixed to a packet payload of 560B and 500PPS.

TABLE: 4.2
THE VARIATIONS IN THE ROUND-TRIP DELAY FOR IMPLEMENTATION-1 FOR THE VARIATION IN PACKET PAYLOAD SIZE AND PACKET TRANSMISSION RATE

Method I Round-trip Delay in seconds		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Packet in Bytes	560B	0.006305 sec	0.006482 sec	0.006698 sec	0.006879 sec
	1000B	0.007757 sec	0.00824 sec	0.008518 sec	0.009175 sec
	1440B	0.009613 sec	0.010387 sec	0.01062 sec	0.012251 sec

Table 4.2 represents the simulation results, round-trip delay, for implementation 1. For each payload size (in rows), delay increased with an increase in the packet transmission rate

(presented in columns). Since priority queue is used, the increase in delay is the sum of a number of delays, including the queuing delay at every hop, the delay associated with the addition (PUSH) of MPLS labels on IPv4 packets on PE routers, and the delay associated with the removal (POP) of the MPLS labels from the IPv4 packets on the ASBR routers. Also included is the marking delay when marking IPv4 packets at CE routers when using the access-list and the policy map, as well as when marking labels, which happens automatically by copying the IPP field of the IPv4 header to the EXP field of the MPLS header of the topmost label. Additionally included is the delay of classifying the IPP or the EXP of the IPv4 packets or labels respectively. In this implementation, classifying IPP occurs six times, at six different interfaces of the CE, the PE and the ASBR. Each AS network is considered to be a completely isolated MPLS domain. This makes ASBRs to do extra work by looking at the IP packet to match by IPP field. ASBRs act like both the CE and the ASBR at the same time, meaning that they only POP and/or impose labels.

Table 4.3 shows the effect of the packet size and the packet transmission rate on the round-trip delay for traffic sourced and destined from/to CE routers, when using scenario/implementation 2. Background traffic was fixed to packet payload of 560B and 500PPS.

TABLE: 4.3
THE VARIATIONS IN THE ROUND-TRIP DELAY FOR IMPLEMENTATION-2 FOR THE VARIATION IN PACKET PAYLOAD SIZE AND PACKET TRANSMISSION RATE

Method II Round-trip Delay in seconds		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Packet in Bytes	560B	0.006105 sec	0.006195 sec	0.006375 sec	0.006618 sec
	1000B	0.007417 sec	0.00789 sec	0.008152 sec	0.008516 sec
	1440B	0.009376 sec	0.009828 sec	0.010086 sec	0.011442 sec

Table 4.3 represents the simulation results, round-trip delay, for implementation 2. Rows represent the different payload size and columns represent the different packet transmission rates. In this implementation, delay increases with the increase of the packet transmission rate. Along with the queuing delay, the matching delay is considered less than with implementation-1 as matching by IPP is only done at two places, CE and PE. Moreover, and unlike in implementation-1, matching interesting packets at ASBRs is done using MPLS EXP. ASBR impose, and POP and swap labels. ASBR routers maintain all VPN routes in their RIB table.

Table 4.4 shows the effect of packet size and packet transmission rate on the round-trip delay for traffic sourced and destined from/to CE routers, when using scenario/implementation 3. Background traffic was fixed to a packet payload of 560B and 500PPS.

TABLE: 4.4
THE VARIATIONS IN THE ROUND-TRIP DELAY FOR IMPLEMENTATION-3 FOR THE VARIATION IN PACKET PAYLOAD SIZE AND PACKET TRANSMISSION RATE

Method III Round-trip Delay in seconds		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Packet in Bytes	560B	0.006132 sec	0.00615 sec	0.006373 sec	0.006719 sec
	1000B	0.00745 sec	0.007927 sec	0.008183 sec	0.008546 sec
	1440B	0.009401 sec	0.009853 sec	0.010155 sec	0.011435 sec

Table 4.4 represents the simulation results, round-trip delay, for implementation 3. Rows represent the different payload sizes and columns represent the different packet transmission rates. In this implementation, delay increases with the increase of the packet transmission rates. Along with the queuing delay, and (same as in implementation-2), the matching delay is considered less than with implementation-1 as matching by IPP is only done at two places, CE and PE. Moreover, and as in implementation-2, matching at the ASBRs is done using the MPLS

EXP. ASBR routers do not maintain any VPN routes at all. This is what makes this implementation the most scalable one among the three.

Table 4.5 compares the effect of a constant packet payload size of 560 and a varied packet transmission rate on the RTD for traffic sourced and destined from/to CE routers, using the three scenarios. Rows represent the round-trip delay of implementation-1, 2 and 3 respectively. Columns represent different packet transmission rates, from 1000 PPS to 2000PPS.

TABLE: 4.5
EFFECT OF VARIES PACKET TRANSMISSION RATE AND PACKET PAYLOAD OF 560B ON THE ROUND-TRIP DELAY, USING THE THREE SCENARIOS

560 Byte packets		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Methods	I	0.006305 sec	0.006482 sec	0.006698 sec	0.006879 sec
	II	0.006105 sec	0.006195 sec	0.006375 sec	0.006618 sec
	III	0.006132 sec	0.00615 sec	0.006373 sec	0.006679 sec

Table 4.6 compares the effect of a constant packet payload size of 1000B and a varied packet transmission rates on the round-trip delay, for traffic sourced and destined from/to CE routers, using the three scenarios. Rows represent the round-trip delay of method one, two and three respectively. Columns represent different packet transmission rates, from 1000 PPS to 2000PPS.

TABLE: 4.6
EFFECT OF VARIED PACKET TRANSMISSION RATE AND PACKET PAYLOAD OF 1000B ON THE ROUND-TRIP DELAY, USING THE THREE SCENARIOS

1000 Byte packets		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Methods	I	0.007757 sec	0.00824 sec	0.008518 sec	0.009175 sec
	II	0.007417 sec	0.007868 sec	0.008152 sec	0.008516 sec
	III	0.00745 sec	0.007927 sec	0.008183 sec	0.008546 sec

Table 4.7 compares the effect of a constant packet payload size of 1440B and a varied packet transmission rate on the round-trip delay, for traffic sourced and destined from/to CE routers, using the three scenarios. Rows represent the round-trip delay of method one, two and three respectively. Columns represent different packet transmission rates, from 1000 PPS to 2000PPS.

TABLE: 4.7
EFFECT OF VARIED PACKET TRANSMISSION RATE AND PACKET PAYLOAD OF 1440B ON THE ROUND-TRIP DELAY, USING THE THREE SCENARIOS

1440 Byte packets		Packets Per Sec (PPS)			
		1000 PPS	1400 PPS	1600 PPS	2000 PPS
Methods	I	0.009613	0.010387	0.01062	0.012251
	II	0.009376	0.009828	0.010086	0.011442
	III	0.009401	0.009853	0.010155	0.011435

4.2 Analysis of Simulation Results

4.2.1 Analysis of Simulation Results for a Fixed Packet Payload

Figures 4.1, 4.2, and 4.3 present the variations in round-trip delay for different packet transmission rates for a fixed packet payload size for the three, Inter-AS MPLS L3 VPN implementations. Results were taken from the tables presented in the previous subsections. The *X*-axis presents the packet transmission rate in seconds (PPS) and the *Y*-axis presents the round-trip delay in seconds, from a PC connected to CE1 to another PC connected to CE2.

Figure 4.1 presents the variation in round-trip delay for the variations in the packet transmission rate for a constant payload of 560B, with the three implementations. With respect to the payload of 560B, the RTD increased for a variation of packet transmission rates for the three implementations. From this, implementation-1 produced the highest round-trip delay of the three implementations which produced a similar delay. Implementation-1 has the IPV4-route lookup time within the VRF repeated at four routers, PEs and ASBRs. This lookup time repeats only twice with the other two implementations. Moreover, implementation-1 matches the priority packets from ASBRs using the IPP field in the IP header, while the other two implementations use the MPLS EXP field.

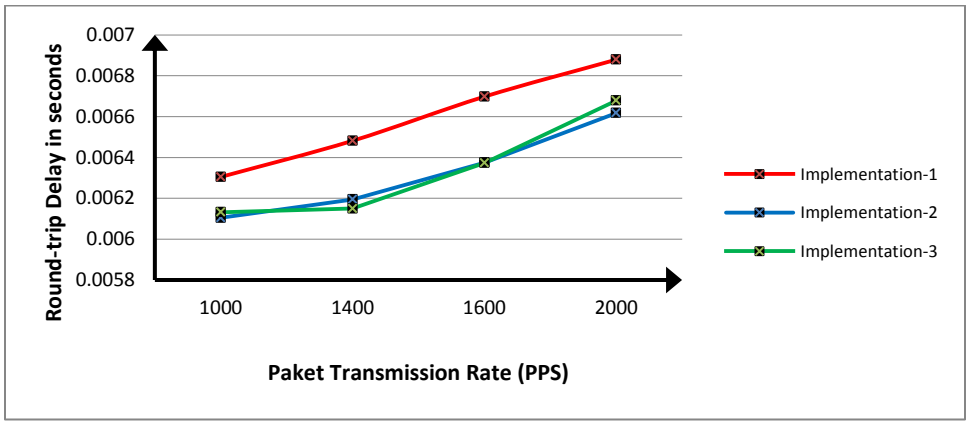


Figure 4.1. The variations in round-trip delay for a payload of 560B and a variant packet transmission rate

Figure 4.2 presents the variation in round-trip delay for the variations in the packet transmission rate for a constant payload of 1000B, with respect to using the three implementations. Implementation-1 produced the highest round-trip delay out if the three implementations which produced approximately same delay.

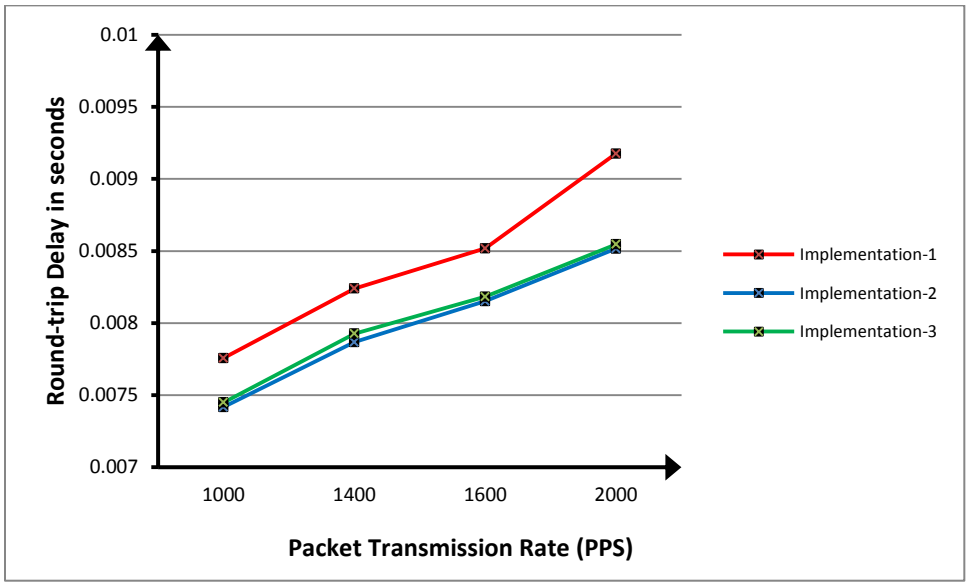


Figure 4.2. The variations in round-trip delay for a payload of 1000B and variant a packet transmission rate

Figure 4.3 presents the variation in round-trip delay for the variations in the packet transmission rate and for a constant payload of 1440B, with the three implementations. Implementation-1 produced the highest round-trip delay out of the three implementations which produced approximately the same delay.

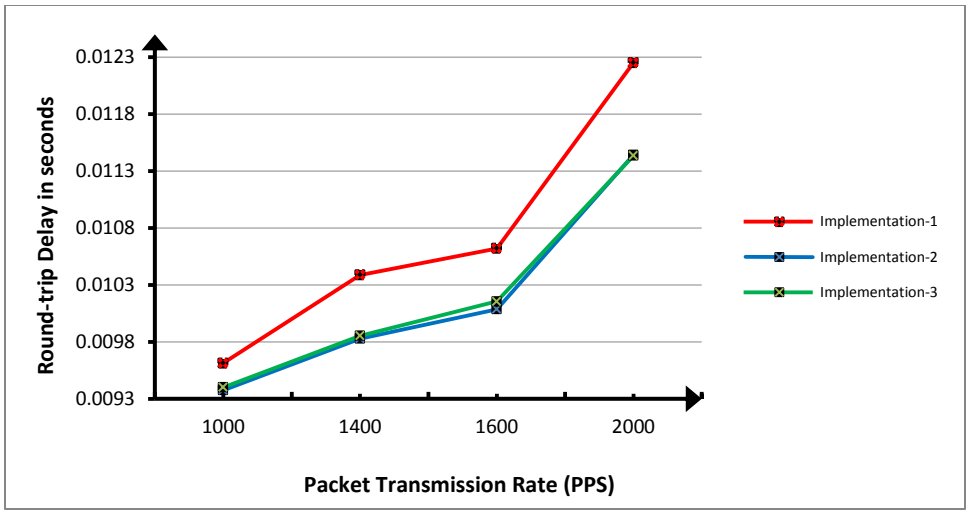


Figure 4.3. The variations in round-trip delay for a payload of 1440B and a variant packet transmission rate

Figure 4.4 presents the variation in round-trip delay for the variations in the packet payload size for a constant packet transmission rate of 1000PPS, with the three implementations. With respect to the packet transmission rate of 1000PPS, RT delay increased for variation of packet payload sizes, for the three implementations, from which implementation -1 produced the highest round-trip delay out of the three implementations which produced similar delay. This is due to the associated delays mentioned in the previous section.

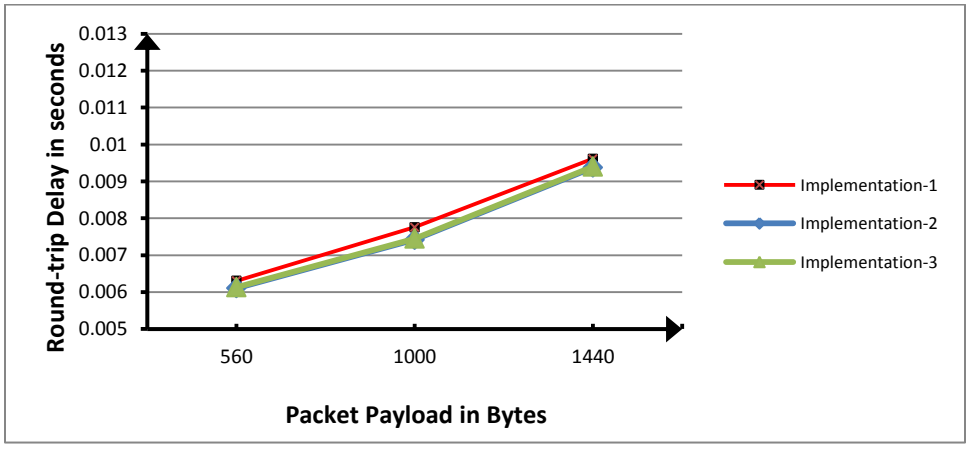


Figure 4.4. The variations in round-trip delay for a packet transmission rate of 1000PPS and a variant packet payload size

Figure 4.5 presents the variation in round-trip delay for the variations in the packet payload size for a constant packet transmission rate of 1400PPS, with the three implementations. With respect to the packet transmission rate of 1400PPS, the RTD increased for a variation of packet payload sizes, for the three implementations, from which implementation -1 produced the highest round-trip delay out of the three implementations which produced similar delay. This is due to the associated delays mentioned in the previous section.

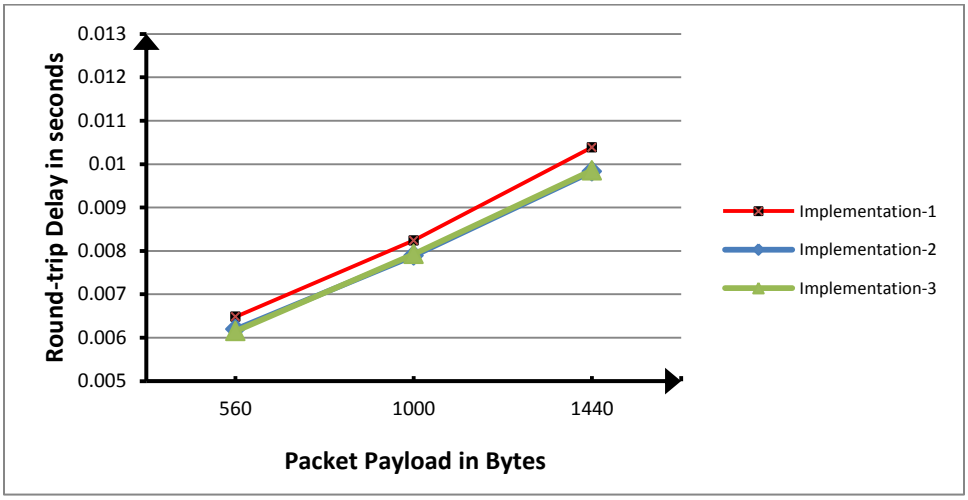


Figure 4.5. The variations in round-trip delay for a packet transmission rate of 1400PPS and a variant packet payload size

Figure 4.6 presents the variation in round-trip delay for the variations in packet the payload size for a constant packet transmission rate of 1600PPS, with the three implementations. With respect to the packet transmission rate of 1600PPS, the RTD increased for a variation of packet payload sizes, for the three implementations, from which implementation -1 produced the highest round-trip delay out of the three implementations which produced similar delay. This is due to the associated delays mentioned in the previous section.

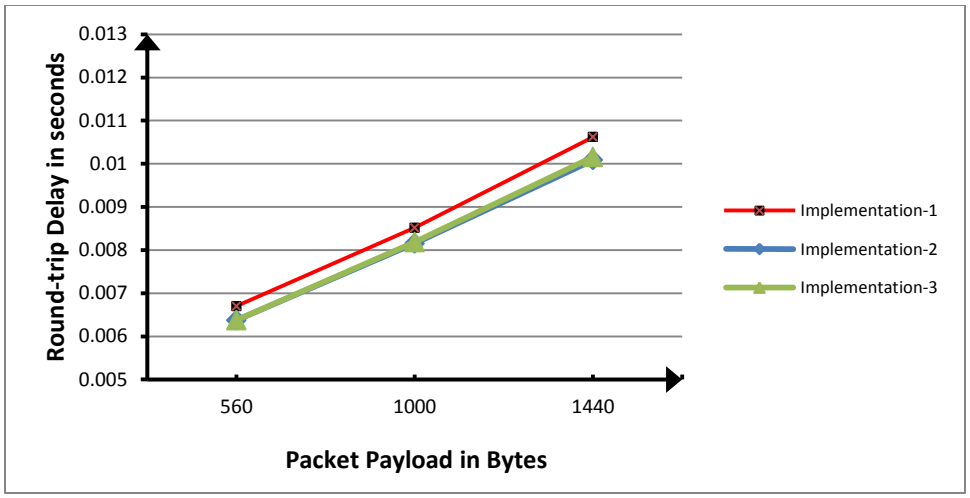


Figure 4.6. The variations in round-trip delay for a packet transmission rate of 1600PPS and a variant packet payload size

Figure 4.7 presents the variation in round-trip delay for the variations in the packet payload size for a constant packet transmission rate of 2000PPS, with the three implementations. With respect to the packet transmission rate of 2000PPS, the RTD increased for a variation of packet payload sizes, for the three implementations, from which implementation -1 produced the highest round-trip delay out of the three implementations which produced a similar delay. This is due to the associated delays mentioned in the previous section.

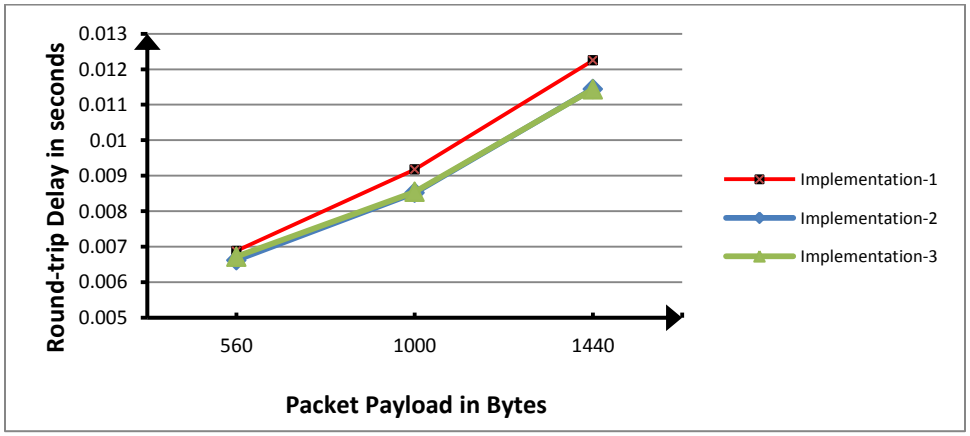


Figure 4.7. The variations in round-trip delay for a packet transmission rate of 2000PPS and a variant packet payload size

4.2.2 Analysis of Simulation Results for a Variable Packet Size

Figures 4.1, 4.2, and 4.3 present the variations in round-trip delay for the variation in packet transmission rate, for all the three implementations, for the packet payload sizes of 560B, 1000B, and 1440B, respectively. The RTD for implementation-1 is higher than that for implementation-2 and 3. The delays associated with implementation-2 and 3 were very close to each other while that for implementation-2 was the lowest out of the two. Typically, with an increase in the packet transmission rate, the delay increased for all the three implementations, for a fixed packet payload size. Also, for a fixed packet transmission rate, the RTD increased for an increase in the packet payload size. While implementation-1 had the highest delays, implementations 2 and 3 showed very close results, with the delays for implementation-2 being the lowest. The theoretical analysis supporting these results is discussed in the following paragraph.

As mentioned in the analytical discussion section of chapter 3, the additional activity at the ASBRs of converting the packet from IPv4-to-MPLS and vice versa, as well as classifying packets by matching the IPP values, was the reason that implementation-1 had the highest RTD. As IPv4 packets are only seen and processed at PE and CE routers, in implementations 2 and 3, delays of these implementations were close. In implementation-2, packets between ASBRs are labeled by the MPLS protocol and not the MP-BGP as in implementation-3 and that is the reason implementation-2 had the lowest RTD.

By adding more VPN sites, implementation-1 would consume more resources on the ASBRs such as memory for each VPN VRF, and further divide the inter-AS link(s) physical interface(s) into sub-interfaces which will impact each VPN traffic by reducing the dedicated bandwidth due to sharing the physical interface bandwidth with all VRFs impacting it. As a

result, implementation-1 is the least scalable and efficient among the three. Moreover, the ASBRs in implelentation-2 consume more memory for each VPNv4 route for each VPN site. Implementation-3 is the best in terms of scalability as it does not require storing of any VPNv4 routes for each VPN site, as P routers and RRs have a direct eMP-BGP with BGP next-hop unchanged enabled which makes one PE-to-PE VPNv4 (VRF) LSP. Hence, it can be seen that implementations 2 and 3 (Single-Hop MP-BGP with static routes and Multi-hop MP-EBGP between AS's RRs) can result in similar delays respectively, and implementation-2 (Single-Hop MP-BGP with static routes) shows the lowest delay while implementation-1 shows the highest.

CHAPTER 5

CONCLUSIONS

This thesis analyzes the three, publicly available Inter-AS MPLS VPN implementations, namely, Back-to-Back Virtual Routing Forwarding (VRF), single-hop MP-BGP with static routes, and Multi-hope MP-BGP between AS's route reflectors and compares these implementations with respect to packet round-trip time. The delays increased for an increase in packet transmission rate, for a fixed packet payload size, for all the three implementations. Similarly, the round-trip delay increased for an increase in packet payload size for a fixed packet transmission rate. The analysis shows that the delays associated with implementation-1 are the highest, and those associated with implementation-2 are lowest. Also, implementation-2 and 3 had very similar delays.

REFERENCES

LIST OF REFERENCES

[1] H. Yamada, "End-to-End Performance Design Framework of MPLS Virtual Private Network Service across Autonomous System Boundaries", in Proc. Telecommunications Network strategy and planning Symposium, New Delhi, India Nov. 2006

[2] M. EL Hachimi, M. Breto, and M. Bennan, "Efficient QoS implementation for MPLS VPN," in Proc. 22nd International Conference on Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008, Okinawa, Japan, March 2008

[3] L. Ming-hu and X. Jing-b, "Research and Simulation on VPN Networking Based on MPLS", in Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM '08, Dalian, China Oct 2008

[4] J. Xia, M. Li, and L. Wan "Research on MPLS VPN Networking Application Based on OPNET", International Symposium on Information Science and Engineering, ISISE '08, Shanghai, China Dec 2008

[5] S. Veni, G.M.K. Nawaz and P.Prab, "Performance Analysis of Network Traffic Behavior in Conventional Network over MPLS", in Proc ICCCCT '10, pp 222-226, Ramanathapuram, India October 2010

[6] A. S. Khan and B. Afzal (2010). *MPLS VPNs with DiffServ – A QoS Performance study* (Master's thesis). Retrieved from http:// hh.diva-portal.org/smash/get/diva2:400278/FULLTEXT01

[7] F. Palmieri, "VPN scalability over high performance backbones Evaluating MPLS VPN against traditional approaches", in Proc. Eighth IEEE International Symposium on Computers and Communication, ISCC 2003. Rome, Italy July 2003

[8] H. Zhang, Y. Qin, H. Zhang, and J. Guan, "Study on host and station mobility in BGP/MPLS VPN", 2006 IET in Proc International Conference Wireless, Mobile and Multimedia Networks, pages 1-3, Hangzhou, China Nov 2006

[9] R. Ren, D. Feng, and K. Ma, "A detailed implement and analysis of MPLS VPN based on IPSec", in Proc International Conference on Machine Learning and Cybernetics, vol. 5, pp. 2279-2783, Shanghai, China August 2004

[10] W. Lee, R. Bhagavathula, N. Thanthry, and R. Pendse, "MPLS-over-GRE based VPN architecture: a performance comparison", 45th Midwest Symposium on Circuits and Systems, MWSCAS-'02, vol.3, pp III280-III283, Tulsa, Oklahoma, USA August 2002

[11] G. Mirjalily, P. Bastani, and S.M.T. Almodarresi, "Connecting Telephone Exchange Centers over Metro Ethernet Networks by using Diffserv-MPLS", in Proc of 11th International Conference on Computer and Information Technology (ICCIT 2008), vol.2, pp 975-981, Khulna, Bangladesh December, 2008

[12] J. Hošek, L. Růčka and K. Molnár, "Advanced modelling of DiffServ technology", In Proc 32nd International Conference on Telecommunications and Signal Processing, Budapest: Hungary May 2009.

[13] Md. T. Aziz and M. S. Islam, *Performance Evaluation of Real–Time Applications over DiffServ/MPLS in IPv4/IPv6 Networks* (Master's thesis). Retrieved from http://www.bth.se/com/mscee.nsf/attachments/Binder1_pdf/$file/Binder1.pdf

[14] Yin Guofu, "A monitoring network on highways based on VPN and study of its QOS mechanism", in Proc 2nd ICNDS, pp 278-281, Wenzhou, China May 2010

[15] J. Wu and Y. Zhan, "A Layered MPLS Network Architecture", in Proc 6th WiCOM '10, pp 1-4, Chengdu, China Sept 2010

[16] A. Saika, r. El Kouch, M. Bellafkih and B. Raouyane, "Functioning and Management of MPLS/QOS In the IMS architecture", in Proc ICMCS '11, pp 1-6, Ouarzazate, Morocco April 2011

[17] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February, 2006