Revolutionizing Networking: Unleashing the Potential of Embedded IP/MPLS Framework for Advanced VPN Services

Mr. Manoj Kumar Vemula[1], Mrs B.Madhuri[2], Mr.Dhondi Pandu Ranga[3], P V Ramanaiah[4]

[1]Assistant Professor, Department of Information Technology, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad,Telangana, India 500090
[2]Assistant Professor, Department of Computer science and Engineering, Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana, India-500100
[3]Assistant Professor, Department of CSE-Artificial Intelligence and Machine Learning, Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana, India-500100
[4]Assistant Professor, Department of CSE-Cyber Security, Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana, India-500100

Email: [1]manojkumarv2251@gmail.com,[2]madhuri16.b@gmail.com, [3]dhondi.pandu@gmail.com, [4]pvrcseit@gmail.com

Received 16/11/2023; **Accepted** 11/12/2023

Abstract:

This paper presents a novel hybrid hardware and software approach for the implementation of an integrated IP/MPLS framework. MPLS is recognized for its efficacy in prioritizing packet traffic and optimizing bandwidth utilization, contributing to enhanced overall network efficiency and scalability. The study showcases MPLS performance through the configuration of a network on the GNS3 platform, leveraging three virtual CISCO 3700 series routers – two designated as PE routers (Edge-LSR) and one as a P router (LSR) within a single PC. Complementary network components consist of two CISCO 2811 series routers, two CISCO 2950 series switches, and four desktop PCs. The paper delves into the practical application of Virtual Private Network (VPN) technology, emphasizing its secure use of the global Internet. To evaluate the performance of the embedded IP/MPLS-based model, various VPN configurations are implemented and comprehensively analyzed. The primary aim of this research is to present an experimental networking model designed as an educational tool, facilitating students' understanding of the fundamental principles of real-world networking.

Keywords: MPLS, IP/MPLS Integration, VPN, Networking.

1. INTRODUCTION

Amid the growing demand for Internet applications like voice over IP (VoIP), real-time streaming, and video conferencing, the core network grapples with escalating congestion. Simply enhancing bandwidth proves insufficient as a sustainable solution. Multiprotocol Label Switching (MPLS) [1] emerges as an effective remedy, providing scalability, swift switching, a diverse range of Quality of Service (QoS), and Traffic Engineering (TE) capabilities within the core network. Consequently, an IP/MPLS integrated model from the service provider's standpoint ensures increased capacity, extensive scalability, end-to-end QoS delivery, and comprehensive service coverage. Virtual Private Network (VPN) technology interconnects multiple sites under a single customer through a Service Provider's (SP) backbone. In the past, IP-based VPNs [2] facilitated connections. Recognizing the advantages of MPLS, there is a growing trend towards integrating MPLS with IP in the backbone network, as evidenced by [3], emphasizing IP/MPLS integration as a robust technology for standard VPN services.

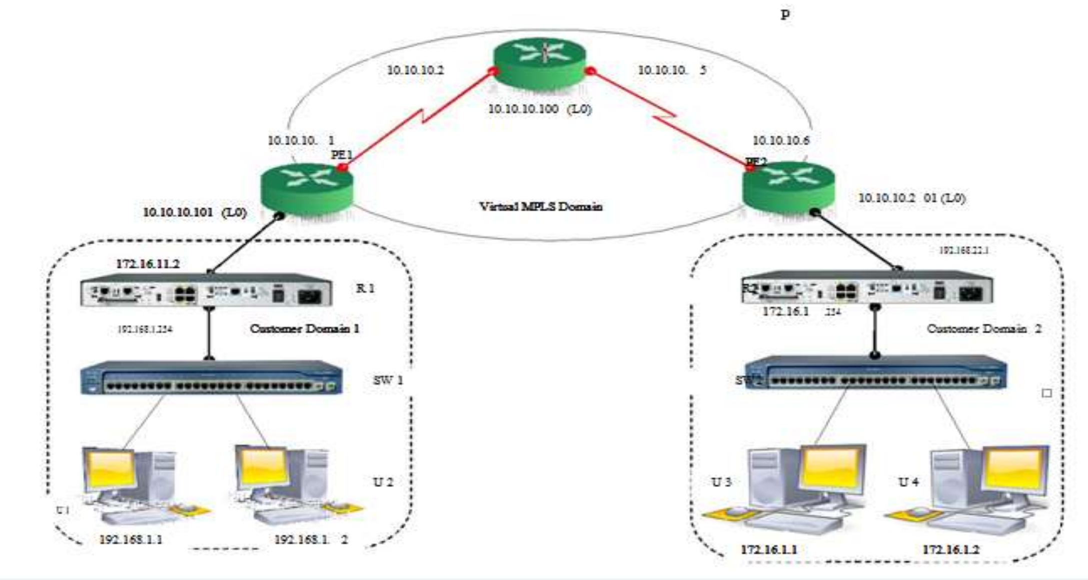
Several theories and models [4-8] have been suggested to enhance VPN services in networking; however all the suggested approaches is either complex or having more delay to access the network in real time applications. Ridwan et al [9] suggested recent trends in MPLS networks; however no attention was given towards the solutions of the current problems associated with the system. Gupron et al [10] proposed an automation system for CE router; however the algorithm design is too complex to work in real time applications efficiently, therefore may not be the optimal solution for network system applications. Vanerio et al [11] presented an approach in which the authors designed MPLS Data plane toolkit; however no attention was given towards the enhancement of the networking system design which can advance the arrangement of connection between end users. Silalahi et al [12] suggested applications of MPLS, where the authors tried to implement looping protection services. But the authors did not pay any attention to develop the VPN network system

This paper introduces an approach that applies theoretical networking knowledge within an experimental interworking environment. It conducts a series of measurements, including drop packet analysis, forwarding delay assessment, throughput evaluation for lost and received packets, and forwarding delay during file transfer in both IP and IP/MPLS integrated networks. The results unequivocally demonstrate the superior performance of IP/MPLS integrated networks over their IP-based counterparts. Subsequent sections delve into the implementation details of our embedded IP/MPLS integrated model in the laboratory (Section II), the configuration methods of our integrated model (Section III), and performance analyses showcasing MPLS's enhanced performance compared to IP (Section IV). Also it provides insights into VPN configurations on our embedded IP/MPLS model, complemented by relevant results. The paper concludes in Section V.

Embedded IP/MPLS Implementation for Seamless Connectivity

Illustrated in Figure 1 is the experimental layout of our IP/MPLS-based network model, featuring PE1 and PE2 as edge label switch routers (LSRs), while router P serves as an additional LSR. This trio of virtual routers collectively establishes an MPLS domain using virtual CISCO 3700 series routers within our framework. Employing Graphics Network Simulator (GNS3) on a PC equipped with an Enterprise IOS 3700 operating system, dual-core processor, and 4GB RAM, we successfully set up the MPLS domain. Physical routers R1 and R2, belonging to the CISCO-2811 series, function as external IP-based clients, linked to the virtual MPLS domain via PE1 and PE2 using CAT-5e cables boasting a 100 Mbps bandwidth. Each client unit comprises a CISCO 2950 series switch (SW1 and SW2) and two computers connected through CAT-5e cables, each supporting a 100 Mbps bandwidth. Figure 1 further details the complete IP and loopback addresses (L0) assigned to individual routers and PC interfaces. Complementing this, Figure 2 provides a visual representation of our embedded model within the laboratory setting. Configuration-wise, we implement the Border Gateway Protocol (BGP) within the MPLS domain and opt for the static routing protocol in

TELEMATIQUE
ISSN: 1856-4194



Configuration methods of Embedded IP/MPLS based model

Figure 2 represents the Snapshot of IP/MPLS embedded network model.

Figure 2: Snapshot of IP/MPLS embedded network model

Moreover the configuration and various types of arrangements of virtual routers can be configured as

Virtual Router Configuration for PE1

PE1>enable PE1#configure terminal PE1(config)#int f0/0
PE1(config-if)#ipaddress172.16.11.1 255.255.255.252 PE1(config-if)#no shutdown
PE1(config)#int s0/0
PE1(config-if)#ip address 10.10.10.1 255.255.255.252 PE1(config-if)#no shutdown

Virtual Router Configuration For P

P>enable P#configure terminal P(config)#int s0/0
P(config-if)#ipaddress10.10.10.2 255.255.255.252 P(config-if)#no shutdown
P(config)#int s0/1
P(config-if)#ip address 10.10.10.5 255.255.255.252 P(config-if)#no shutdown

Virtual Router Configuration For PE2 is same as PE1

a) To Enable OSPF Protocol:

For PE1 router

PE1(config)#router ospf 1 PE1(config-router)#network 10.10.10.0 0.0.0.3 area 0

For P router

P(config)#router ospf 1
P(config-router)#network 10.10.10.0 0.0.0.3 area 0 P(config-router)#network 10.10.10.4 0.0.0.3 area 0

For PE2 router

PE2(config)#router ospf 1 PE2(config-router)#network 10.10.10.4 0 0.0.0.3 area 0

b) To set loopback address:

For PE1

PE1(config)# int l0
PE1(config-if)#ip address 10.10.10.101 255.255.255.255

For PE2

PE2(config)# int l0
PE2(config-if)#ip address 10.10.10.201 255.255.255.255

For P

P#configure terminal P(config)# int l0
P(config-if)#ip address 10.10.10.100 255.255.255.255 P(config-if)#exit

c) To enable MPLS on PE1, P & PE2

For PE1

PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id loopback0
PE1(config)#int s0/0
PE1(config-if)#mpls ip

For P

P(config)#mpls label protocol ldp
P(config)#mpls ldp router-id loopback0
P(config)#int s0/0
P(config-if)#mpls ip
P(config)#int s0/1
P(config-if)#mpls ip

For PE2

PE2(config)#mpls label protocol ldp
PE2(config)#mpls ldp router-id loopback0
PE2(config)#int s0/0
PE2(config-if)#mpls ip

d) Configuration of MPLS forwarding & VRF definition

PE1(config)# ip vrf CustomerA PE1(config-vrf)#rd 1:100 PE1(config-vrf)#route-target both 1:100 PE1(config-vrf)#exit

PE1(config)#int f0/0
PE1(config-if)#ip vrf forwarding CustomerA
PE2(config)# ip vrf CustomerA PE2(config-vrf)#rd 1:100 PE2(config-vrf)#route-target both 1:100 PE2(config-vrf)#exit
PE2(config)#int f0/0
PE2(config-if)#ip vrf forwarding CustomerA

e) Configuration of BGP PE-PE Routing
PE1(config)#router bgp 1 PE1(config-router)#neighbor 10.10.10.201 remote-as 1
PE1(config-router)#neighbor 10.10.10.201 update-source l0
f)
PE1(config-router)#address-family vpnv4 PE1(config-router-af)#neighbor 10.10.10.201 activate PE1(config-router-af)#neighbor 10.10.10.201 send-community extended PE1(config-router-af)#exit-address-family PE1(config-router)#address-family ipv4 vrf CustomerA PE1(config-router-af)#redistribute connected PE1(config-router-af)#redistribute static
PE2(config)#router bgp 1 PE2(config-router)#neighbor 10.10.10.101 remote-as 1
PE2(config-router)#neighbor 10.10.10.101 update-source l0
PE2(config-router)#address-family vpnv4 PE2(config-router-af)#neighbor 10.10.10.101 activate PE2(config-router-af)#neighbor 10.10.10.101 send-community extended PE2(config-router-af)#exit-address-family PE2(config-router)#address-family ipv4 vrf CustomerA PE2(config-router-af)#redistribute connected PE2(config-router-af)#redistribute static

f). Configure per VRF static route on PE router
PE1(config)#ip route vrf CustomerA 192.168.1.0 255.255.255.0 172.16.11.2
PE2(config)#ip route vrf CustomerA 172.16.1.0 255.255.255.0 192.168.22.2

I. Performance analysis of MPLS over IP

Within this segment, our focus shifts to introducing key facets of MPLS design subsequent to the establishment of the IP/MPLS standard. Following this introduction, we delve into graphical analyses, drawing comparisons between IP-based and IP/MPLS-based hybrid models. The graphical representation in Figure 3 illustrates MPLS messages transmitted to router PE1, captured via HyperTerminal. Complementing this, Figure 4 provides insights into the LDP binding process with router PE1.

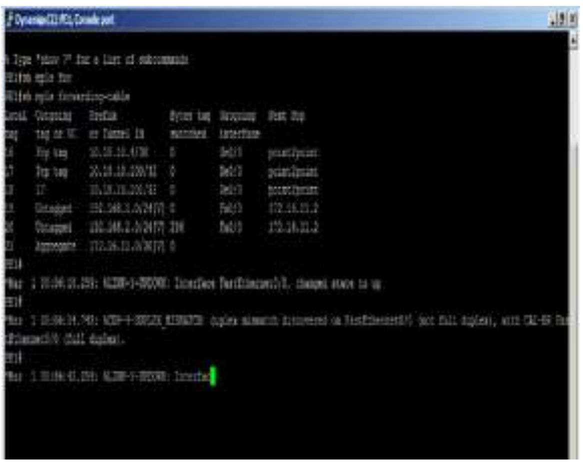


Figure 3: MPLS forwarding table for PE1 router

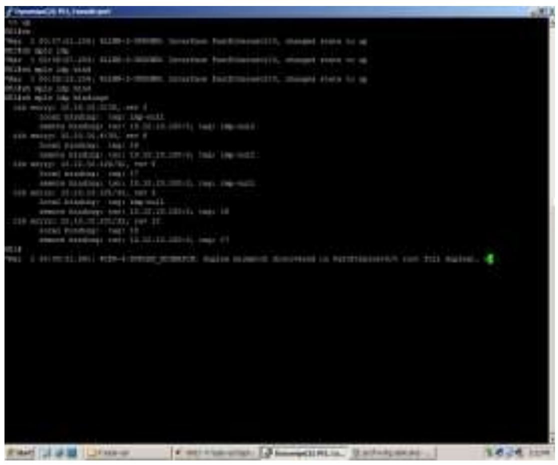


Figure 4: LDP binding for PE1 router

To highlight the efficacy of the IP/MPLS-based model, we employ constant bit rate (CBR) traffic between two clients traversing both the IP/MPLS-based network and each individual IP-based network model. In Figure 5, we present the correlation between transmission delay and packet size for these two protocols. Notably, the average transmission delay in IP/MPLS-based networks exhibits a reduction ranging from 7.5% to 20%, showcasing superior performance compared to other networks, which experience higher packet volumes and increased congestion

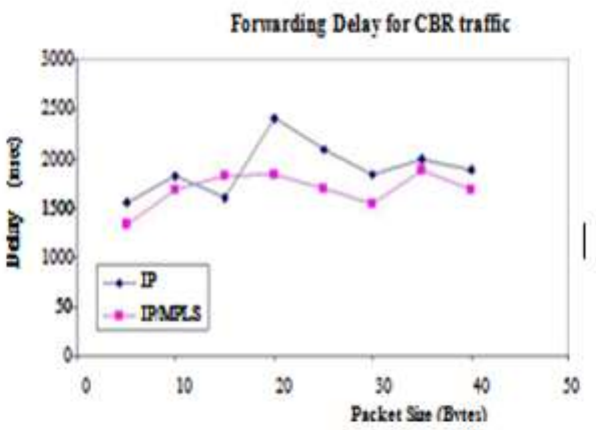


Figure 5: Forwarding Delay for CBR traffic

Figure 6 delves into the relationship between network throughput and the quantity of received packets under identical CBR traffic conditions. Within the IP/MPLS-based environment, a significant observation emerges— a notable majority of packets successfully reach their designated destination, underscoring the robustness of the IP/MPLS-based network in facilitating efficient packet delivery.

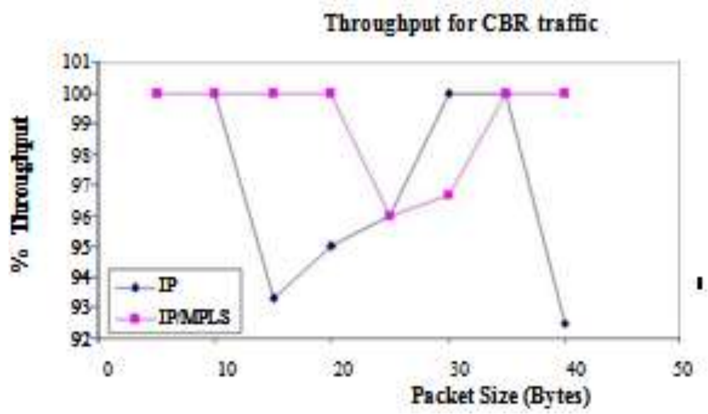


Figure 6: Throughput w.r.t. received packet for CBR traffic

Examining network performance within an FTP environment involved the transfer of files varying in size between two clients. As depicted in Figure 7, the FTP transfer latency experiences a noteworthy 50% reduction, particularly within the IP/MPLS context. This underscores the potential of our IP/MPLS-based design as a viable network model. To enhance the practicality of our model, we implemented a VPN within the IP/MPLS-based network, as detailed in section III. Subsequently, we employed VPN from one customer record to other Constant Bit Rate (CBR) tools. Figure 8 illustrates the forwarding latency of CBR traffic post the establishment of VPN in our scenario. Intriguingly, we discovered that the average transmission delay in MPLS-VPN is significantly lower by 44.5% compared to IPSec-VPN. Further insights into network connectivity, measured as packet loss relative to CBR traffic, are provided in Figure 9, demonstrating a reduction in packet loss within the MPLS-VPN model.

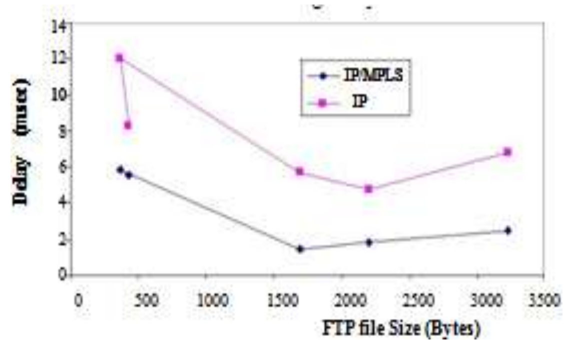


Figure 7: Forwarding Delay for FTP traffic

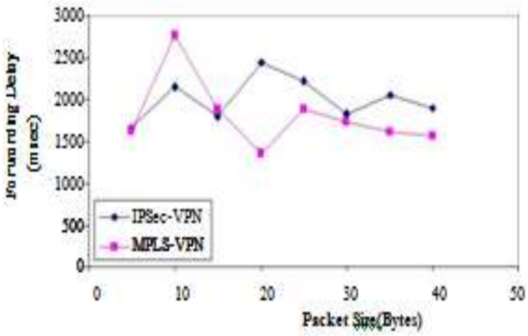


Figure 8: Forwarding Delay for IPSec-VPN and MPLS-VPN model

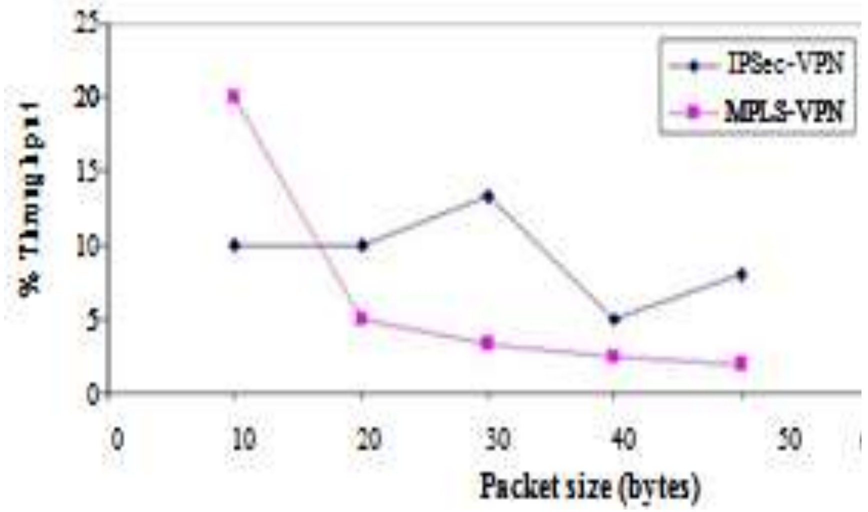


Figure 9: Percentage Throughput for IPSec-VPN and MPLS-VPN model

2. CONCLUSION

This paper establishes an integrated architecture founded on IP/MPLS, delving into both hardware and software considerations associated with MPLS implementation within a clinical context. Detailed insights into the challenges and outcomes are presented, shedding light on the operational aspects of the framework. The preliminary results outlined herein illuminate our concerted efforts towards optimizing MPLS performance in this specific application domain.

3. REFERENCES

[1] Jha, Sanjay, and Mahbub Hassan. Engineering Internet QoS. Artech House, 2002.

[2] Steve Smith, “Introduction to Cisco MPLS VPN Technology” 2007.
[3] Umesh Lakshman and Lancy Lobo, “MPLS Configuration on Cisco IOS Software” Published Oct 17, 2005 by Cisco Press. Part of the Networking Technology series.
[4] Gurpreet, Kaur and Kumar, Dinesh “MPLS Technology on IP Backbone Network” International Journal of Computer Applications, vol 5,pp13-16,2010.
[5] Ramakrishnan, V.; Wargo, C.; John, S.,”GMPLS Network Security: Gap Analysis”. ICNS Conference, 2008 IEEE Systems, pp. 1-7, 5-7 May 2008
[6] Shah. S. A. A. Ahmed. L.,”MPLS Feasibility for General & Core IP Networks using Open Source System”. Second International on Electrical Engineering, pp. 1-6, March 2008.
[7] Han L.; Wang J.; Wang C.; Cai L.,”A Variable Forwarding Equivalence Class for MPLS Networks”. Multimedia Information Networking and Security, MINES '09. International Conference on , pp.273-276, 18-20 Nov. 2009
[8] Liwen He; Botham, P.,” Pure MPLS Technology”. Availability, Reliability and Security, ARES 08, Third International Conference on , pp.253-259, 4-7 March 2008
[9] Ridwan, Mohammad Azmi, Mohamed Radzi, Nurul Asyikin,Wan Ahmad, Wan Siti Halimatul Munirah, Abdullah, Fairuz,Jamaludin, M.Z.Zakaria, Mohd Nasim, “Recent trends in MPLS Networks: Technologies, Applications and Challenges” IET Communications, vol 14,pp1-10, 2020.
[10] M. Y. Gupron, U. Umaisaroh and A. Wicaksono, "Network Automation for CE Router with Route Leaking in MPLS-VPN Network," *2022 International Symposium on Information Technology and Digital Innovation (ISITDI)*, Padang, Indonesia, 2022, pp. 162-167, doi: 10.1109/ISITDI55734.2022.9944460.
[11] J. Vanerio, S. Schmid, M. K. Schou and J. Srba, "MPLS-Kit: An MPLS Data Plane Toolkit," *2022 IEEE 11th International Conference on Cloud Networking (CloudNet)*, Paris, France, 2022, pp. 49-54, doi: 10.1109/CloudNet55617.2022.9978791.
[12] Lukman Medriavin Silalahi, Setiyo Budiyanto, Imelda Uli Vistalina Simanjuntak, Rukhi Ali Effendi, Fernando, Agus Dendi Rochendi, and Irfan Kampono, “Application of MPLS Tunnel Service L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Service Analysis” Intl Journal of Electronics and Telecommunications, 2023, vol. 69, no. 1, pp. 115-120.