Multiprotocol Label Swithching with Layer 3 Virtual Private Network

Agnes Prema Mary K.[1], Mohamed Ibrahim Samsudeen A.[2], Basker M.[3]

[1]Professor, Head of the Department, [2, 3]UG Student, Department of Electronics and Communication Engineering, Jayaraj Annapackiam CSI College of Engineering, Nazareth, India.

E-mail: [1]nestamary@gmail.com, [2]mohamedibrahim59850@gmail.com, [3]baskerrobin4510@gmail.com

Abstract

Service provider networks are required to ensure reliable and secure connections between customer networks located in different geographical locations. Traditional IP forwarding can complicate routing and processing as networks grow in size and complexity. In this research paper, we propose the development of a Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (L3VPN) based on the GNS3 simulation tool. In the proposed architecture, the OSPF protocol will be used for routing in provider networks; MPLS with the LDP protocol – for label switching; VRF – for customer traffic isolation; and Multiprotocol BGP – for exchanging routes between PE routers in the network. This network consists of CE routers, PE routers, and P routers connecting customer networks located in different geographical locations through the MPLS backbone network. The developed network will be tested using an ICMP connectivity test, a traceroute test, and packet analysis with Wireshark. The experiment's outcome proves effective communication between customer sites, while packet captures show the presence of MPLS, OSPF, LDP, IPv4, and ICMP traffic in the simulated network environment. The findings prove the functional feasibility of the suggested MPLS L3VPN interface.

Keywords: Multiprotocol Label Switching, Layer 3 Virtual Private Network, Open Shortest Path First, Label Distribution Protocol, Multiprotocol Border Gateway Protocol, Virtual Routing and Forwarding, Graphical Network Simulator, Network Packet Analysis.

DOI: https://doi.org/10.36548/jsws.2026.4.005
Extended version of article received from **National Conference on Intelligent Systems and Communication Technologies (NCISCT 2026)**
Received: 21.09.2026, received in revised form: 23.10.2026, accepted: 10.11.2026, published: 25.11.2026
© 2026 Inventive Research Organization. This is an open access article under the Creative Commons Attribution-NonCommercial International (CC BY-NC 4.0) License

1. Introduction

The increasing interconnection of geographically dispersed corporate networks has generated the need for communication architectures that allow dependable connection and, at the same time, permit several customer networks to utilize a shared infrastructure provided by the service provider. In this scenario, the service provider needs to allow independent customer networks but, at the same time, should not permit their routing information to be unnecessarily interconnected. Conventional network deployment using IP can facilitate distributed connection amongsites; however, providing separate customer connectivity over a common provider's infrastructure becomes increasingly difficult. Hence, it is imperative for service provider networks to have architectures that ensure clear segregation between customer networks and the underlying provider's infrastructure while still allowing communication. The problem is not only about achieving the connectivity but also about implementing the network components and testing them at the packet level.

Although MPLS-enabled VPN technologies are already well developed, their actual implementation requires a proper combination of routing, forwarding, and virtual private network features. Additionally, an implementation should be tested experimentally, rather than solely theoretically based on its configuration. Specifically, testing at the packet level could give valuable clues about the functioning of network configurations. This makes it necessary to conduct implementation-oriented research to demonstrate the entire configuration and testing process in a simulation environment.

This research fulfills this requirement by utilizing an MPLS Layer 3 VPN setup in GNS3 and verifying its functionality using network connectivity and packet-level analysis. The suggested network topology consists of two customer sites linked together via the provider’s network and has been set up using the network elements outlined in the methodology. The performance evaluation was done using ICMP connectivity tests, traceroute and packet captures using Wireshark.

The objective of this research is to design, implement and functionally validate the MPLS Layer 3 VPN architecture in a simulated service provider environment. The emphasis of this research will be placed on the demonstration of customer site connectivity and the functional verification of the implemented network architecture through experimentally

observed evidence.

2. Literature Review

In traditional networks using IP addressing, routing is done based on destination, where each individual router performs a routing table lookup to find the next-hop address. However, although this is sufficient for conventional network designs, due to the growing size and complexity of modern enterprise and service provider networks, there is a need for more efficient routing and forwarding, network scalability, traffic separation, and inter-site connectivity. The general networking literature discusses routing and forwarding efficiency and network reliability as key factors in designing large communication networks [1], [2].

MPLS was defined as an approach to forwarding where packets were identified by their labels, thereby making it possible to forward packets using the information contained in the label and not depending on IP routing [3]. Kumar et al. defined the basic MPLS architecture that included label switching, Label Switched Paths (LSP) and control versus forwarding decoupling [3]. This architecture forms the basis of service provider networks that need efficient packet forwarding and scalable operations.

The use of MPLS technology in Virtual Private Networks allows service providers to connect more than one geographical customer network through a single physical network infrastructure. The provider-provided VPN jargon and architecture help us understand the difference between the customer and provider networks and provide an understanding of the role of CE, PE, and Provider routers [4]. In an MPLS Layer 3 VPN, customer-specific routing data may be kept in PE routers only whereas the provider network core does not need customer specific routing data.

The development of VPN technology using MPLS has also been complemented by BGP-based methods used for exchanging routing information of such virtual networks between PE routers. In their research, Wu et al. examined the application of cross-domain VPN technology using MPLS and BGP and showed that the combination of MPLS-based packet forwarding and BGP-based VPN route exchange was highly relevant for inter-network communication [5]. This topic is especially relevant for the current research since the suggested architecture uses MP-BGP for exchanging routing information of the VPNs between

PE routers while MPLS is used for packet forwarding through the provider network backbone.

The BGP Send Hold Timer mechanism was proposed by Snijders et al. as a means of enhancing the management of blocked BGP sessions [10]. The mechanism allows a BGP device to identify cases where a peer is unable to handle BGP messages, and thus closes the connection upon expiration of the timer. The mechanism is useful in minimizing the chances of using stale information, and increasing the reliability of the BGP session. This mechanism is important for MP-BGP based VPNs.

The research of Reshma and James focuses on the deployment of an MPLS L3VPN and thus constitutes a direct and relevant reference in respect to the current work [6]. The work of Reshma and James is helpful in providing a basis for the practical use of MPLS L3VPN technology for communication between sites and also helps to compare MPLS VPN works based on implementations to the current work that uses the GNS3 simulation environment. The current work adds the aspect of implementation by using OSPF, LDP, VRF, and MP-BGP technologies.

The reviewed literature therefore establishes three important aspects of the proposed research. First, MPLS provides a label-based forwarding framework for service-provider networks [3]. Second, provider-provisioned VPN architectures enable multiple customer networks to share a common infrastructure while maintaining logical separation [4]. Third, BGP-based VPN mechanisms support the exchange of customer routing information across MPLS-based provider networks [5], [6]. These concepts provide the theoretical basis for the proposed MPLS L3VPN implementation. The present study combines these mechanisms in a GNS3 environment and evaluates the resulting network using ICMP, traceroute, and Wireshark packet analysis.

3. Methodology

The proposed methodology involves the design, configuration, and evaluation of MPLS L3VPN in a GNS3 environment. The proposed architecture will combine the use of the OSPF protocol for provider network routing, MPLS and LDP for packet labeling, VRF to isolate customers, and MP-BGP to exchange routes in the provider edge routers. The methodology will be implemented in a sequence of steps, starting from the design of the topology and IP

addressing to routing, MPLS, VPN configuration, packet transmission, and testing.

3.1 Network Design and Topology

The initial stage of the proposed approach is the creation of a service provider network topology. The architecture contains CE routers symbolizing customer sites, PE routers connecting customer networks to the service provider backbone, and P routers that form the MPLS backbone. PCs from customer sites are connected to CE routers through switches. This architecture ensures the creation of a provider infrastructure that allows separate customer networks to communicate regardless of their geographical separation.

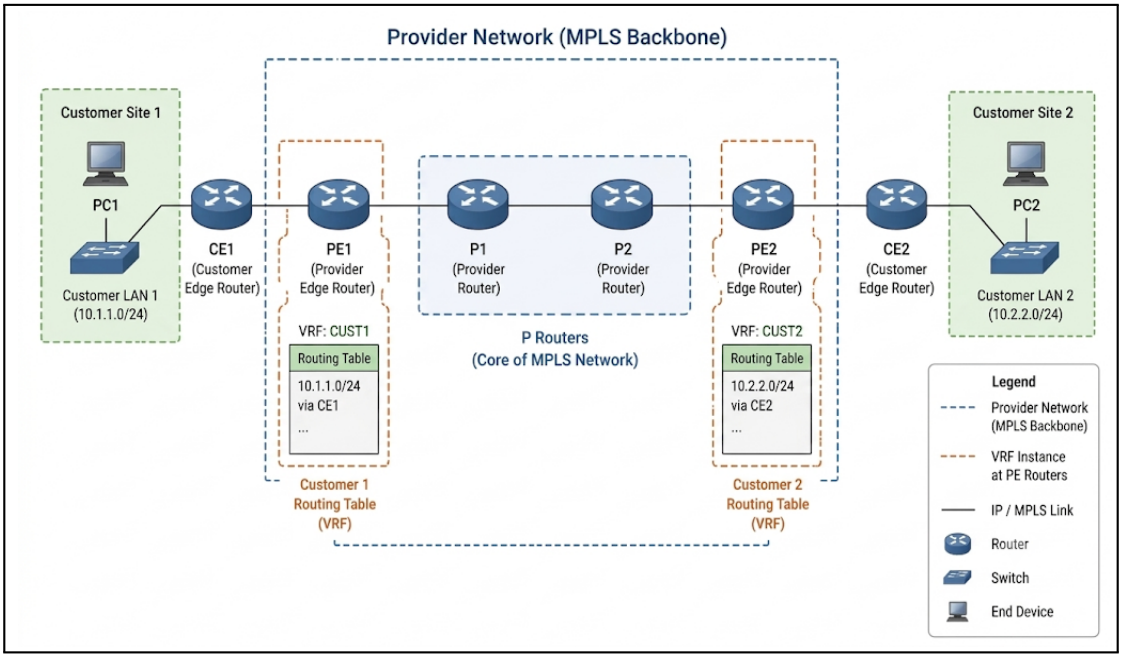

Figure 1. Block diagram of the proposed MPLS Layer 3 VPN architecture.

The logical structure of the proposed MPLS L3VPN is depicted in Figure 1, which illustrates connection among Customer Site 1, CE1, PE1, provider core routers, PE2, CE2, and Customer Site 2. The Figure also depicts the customer routing tables, unique to the PE routers, indicating the function of VRF.

The topology reflects the functional division between the customer edge and the service-provider network. PE routers handle the boundary functions related to customer VPN connectivity, while P routers create the MPLS backbone network and primarily perform label switching operations. This design matches the system architecture presented in the study, where CE routers represent the customer networks, PE routers form the service-provider

boundary, and P routers constitute the MPLS core.

3.2 Hardware and Software Requirements

The hardware and software components used in the implementation provide the required environment for designing, configuring, and validating the proposed MPLS Layer 3 VPN architecture. As listed in Table 1, GNS3 is used to construct the provider network topology and simulate the PE, P, and CE routers. Cisco IOS commands are applied to configure OSPF, MPLS, LDP, VRF, and MP-BGP functionalities. Wireshark is employed to capture and analyse network packets, while VPCS provides customer-side end devices for testing end-to-end connectivity. The host computer provides the computational resources required to execute the network simulation.

Table 1. Hardware and software specification.

S. No.	Category	Component	Specification
1	Hardware	Processor	Intel Core i5
2	Hardware	RAM	16 GB
3	Hardware	Storage	20 GB Free Disk Space
4	Hardware	System Architecture	64-Bit System
5	Hardware	Network Adapter	Ethernet or Wi-Fi
6	Hardware	Display Unit	HD Monitor
7	Hardware	Input Devices	Keyboard and Mouse
8	Software	GNS3	Network Simulation
9	Software	Windows Operating System	Host Environment
10	Software	Cisco IOS Images	Router Emulation
11	Software	VMware Workstation	Virtual Machine
12	Software	Wireshark	Packet Analysis
13	Software	VPCS	PC Simulation
14	Software	Console Terminal	Router Access

3.3 IP Addressing Scheme

IP address assignment for the proposed MPLS L3 VPN network topology are provided in Table 2. /30 subnets are allocated to the point-to-point links connecting the provider routers, while /32 addresses are assigned to the loopback interfaces to ensure stability of the router ID. Customer-facing interfaces establish connections from PE routers to customer networks through different LAN subnets. This particular IP address assignment helps with connectivity within the provider network, routing with OSPF protocol, LDP, and MP-BGP between the PE routers.

Table 2. IP addressing scheme of the proposed MPLS L3VPN.

Router	Interface	IP address	Subnet
PUNEPE	Loopback0	192.168.2.254	/32
PUNEPE	Fa0/0	172.16.16.5	/30
PUNEPE	Customer interface	172.16.16.70	/30
BANGALORE	Loopback0	192.168.6.254	/32
BANGALORE	Fa0/0	172.16.16.6	/30
BANGALORE	Fa1/0	172.16.16.9	/30
HYDERABAD	Loopback0	192.168.4.254	/32
HYDERABAD	Fa0/0	172.16.16.10	/30
HYDERABAD	Fa1/0	172.16.16.25	/30
CHENNAIPE	Loopback0	192.168.5.254	/32
CHENNAIPE	Fa0/0	172.16.16.26	/30
CHENNAIPE	Customer interface	172.16.16.14	/30
SBIHO	LAN	10.0.0.1	/24
SBIBO	LAN	10.1.0.1	/24

3.4 OSPF Configuration

OSPF protocol is configured as the Interior Gateway Protocol in the provider's network. Both the provider router and provider edge routers are part of OSPF Area 0, and the interfaces and loopbacks used by the routers are announced in the OSPF domain. OSPF adjacency is

formed between the adjacent routers for full IP connectivity in the provider backbone [7].

Open Shortest Path First (OSPF) routing protocol is used as an IGP in the provider network backbone. As shown in Table 3, OSPF process number 9829 is used in all provider routers, where all backbone interfaces are configured to belong to Area 0. This allows routing information exchange and IP reachability between provider routers and their loopback interfaces. This reachability is crucial for LDP session establishment.

Table 3. OSPF configuration parameters.

Parameter	Configuration
Routing protocol	OSPF
Process ID	9829
Area	0
OSPF routers	PUNEPE, BANGALORE, HYDERABAD, CHENNAIPE
Loopback advertisement	Enabled
Loopback passive interface	Enabled

OSPF Configuration on Provider Routers:

router ospf 1

network 192.168.2.254area 0

network 172.16.16.5 area 0

3.5 MPLS and LDP Configuration

After IP connectivity is stabilized through IP addressing, MPLS is activated on the provider network's core facing interfaces. LDP is used to dynamically negotiate label bindings among neighboring routers, based on which LSPs are created over the provider backbone [3], [8].

The forwarding mechanism differs from ordinary IP routing. Data packets that enter the MPLS realm are labeled and then routed based on those labels. The fundamental MPLS functions are:

- Label Push: A label is attached to the packet at the ingress PE router.
- Label Swap: P routers forward packets by replacing the incoming label with the appropriate outgoing label.
- Label Pop: The label is removed at the egress PE router before delivery toward the destination customer network.

Operation of the MPLS label switching process can be observed at various stages within the provider's network through the MPLS forwarding table and packet observation. At the ingress PE router, the label push process is confirmed by adding an MPLS header to the received IP packet. For intermediate P routers, the label swap process is confirmed by observing the incoming and outgoing label information within the MPLS forwarding table. At the egress PE router, the label pop process is confirmed through removing the transport label from the packet before forwarding it toward the destination customer's network.

This technique eliminates the need to repeatedly query the destination address in IP using the provider core network. The article recognizes the configuration of LDP and the creation of LSPs as key elements of the proposed MPLS deployment.

The MPLS capability is configured on the router interfaces that connect to the provider. Label Distribution Protocol is then used to distribute labels between neighboring routers. The router-ID for LDP is set using the router's loopback interface. The configuration is examined using the show mpls interfaces, show mpls ldp neighbor, and show mpls forwarding-table commands to verify MPLS activation, label distribution, and forwarding-table entries.

MPLS and LDP Configuration on Provider Routers:

```
ip cef
mpls label protocol ldp
mpls ldp router-id Loopback0 force
interface GigabitEthernet0/1
mpls ip
no shutdown
```

3.6 VRF-Based Customer Traffic Isolation

The VRF technology operates on the PE routers so that independent routing tables can be maintained for customer networks. A different VRF will be allocated for the customer side

interface on the PE routers. The Route Distinguisher (RD) ensures uniqueness for the routes within the VPN, while Route Target (RT) controls the import or export of routes [9].

Virtual Routing and Forwarding (VRF) configurations on the Provider Edge (PE) routers ensure that there are separate routing tables for each customer network. In this configuration, the SBI VRF is configured on the PUNEPE and CHENNAIPE routers to enable communication between the geographically dispersed customer premises. RD configuration for each VRF is 9829:1, and RT configurations for import and export are 9829:1. Customer facing interfaces have to be configured with the appropriate VRF in order to keep the customer's routing information separate from the global as described in Table 4.

Table 4. VRF configuration parameters.

Parameter	PUNEPE	CHENNAIPE
VRF name	SBI	SBI
RD	9829:1	9829:1
Import RT	9829:1	9829:1
Export RT	9829:1	9829:1
Customer interface IP	172.16.16.70	172.16.16.14

These VRFs hold routing data on a per-customer basis, using the common MPLS core. MP-BGP will be used to propagate the routing information for each individual customer from PE to PE, while the route-target attributes will decide which routes will be allowed to enter the VRF. This way, we can enable route exchange for the customer premises without leaking any routing information between different VPNs.

3.7 MP-BGP-Based VPN Route Exchange

MP-BGP is configured between the PE routers to exchange VPN routing information. The BGP sessions are established using the loopback interfaces of the PE routers, thereby providing stable logical endpoints. The VPNv4 address family is activated, and extended communities are used to transport Route Target information [5].

The MP-BGP mechanism ensures that the routes learned for a customer by a PE router can be sent to the correct remote PE router. Once received by the latter, the routes will

then be installed into the correct VRF routing table. In this way, customer sites, which are geographically distant from each other, will be able to communicate without the need for customer-specific routes to be maintained by the P routers.

MP-BGP is established between the PE routers to allow customer routes to be advertised via the VPNv4 address family. The loopback interfaces of the PE routers will serve as the stable endpoint for establishing internal BGP sessions. The VPNv4 address family is enabled for the configured BGP neighbors, and the extended community attribute is enabled to allow Route Targets to be passed with the routes being advertised from the VPN address family. Through this configuration, the receiving PE router can recognize the VRF based on the import Route Targets.

MP-BGP VPNv4 Configuration between PE Routers:

```
router bgp 65000
neighbor 192.168.5.254 remote-as 65000
neighbor 192.168.5.254 update-source Loopback0
address-family vpnv4
neighbor 192.168.5.254 activate
neighbor 192.168.5.254 send-community extended
exit-address-family
```

MP-BGP configurations are made between Provider Edge routers for the purpose of exchanging customer routing information across theLS network. An internal BGP connection is established between PUNEPE and CHENNAIPE using their loopback interfaces. Both routers belong to autonomous system 9829.

The VPNv4 address family is enabled for exchanging customer network routes along, with route distinguishers and route target communities. The “send- community extended” command is used for exchanging the extended communities needed for the route targets.

This customer routing information is then imported into the relevant VRF routing table according to the established route-target policy, as shown in Table 5.

Table 5. MP-BGP configuration details.

Parameter	PUNEPE	CHENNAIPE
Local AS	9829	9829
BGP neighbor	192.168.5.254	192.168.2.254
Neighbor AS	9829	9829
Update source	Loopback0	Loopback0
Address family	VPNv4	VPNv4
Extended community	Enabled	Enabled

3.8 Customer Edge and End-Device Configuration

The CE routers are set up to reflect the customer's network. The LAN interfaces are configured with suitable IP addresses, and static default routing is used to route customer traffic to the respective PE routers.

The CE routers do not participate directly in MPLS label switching. Their main role s is to route traffic from their customer network to the service provider network and vice versa. This separation reduces the complexity of configuring the customer's network while keeping the MPLS and/or VPNS functionality within the provider's network.

3.9 End-to-End Packet Forwarding

The proposed packet-flow mechanism can be summarized as follows:

- The source PC generates an IP packet.
- The packet reaches the source CE router.
- The CE router forwards the packet toward the corresponding PE router.
- The ingress PE identifies the appropriate customer VRF and attaches the MPLS label.
- The packet traverses the provider backbone through P routers.
- P routers perform label swapping rather than customer-specific IP routing.
- The egress PE removes the MPLS label.
- The packet is forwarded through the destination CE router.
- The destination PC receives the packet.

Thus, the proposed method integrates IP routing at the network edges with label-based routing within the core of the service provider and VRF routing on the PE routers. In this manner, end-to-end secure communication can be achieved while preserving routing domain separation.

4. Results and Discussion

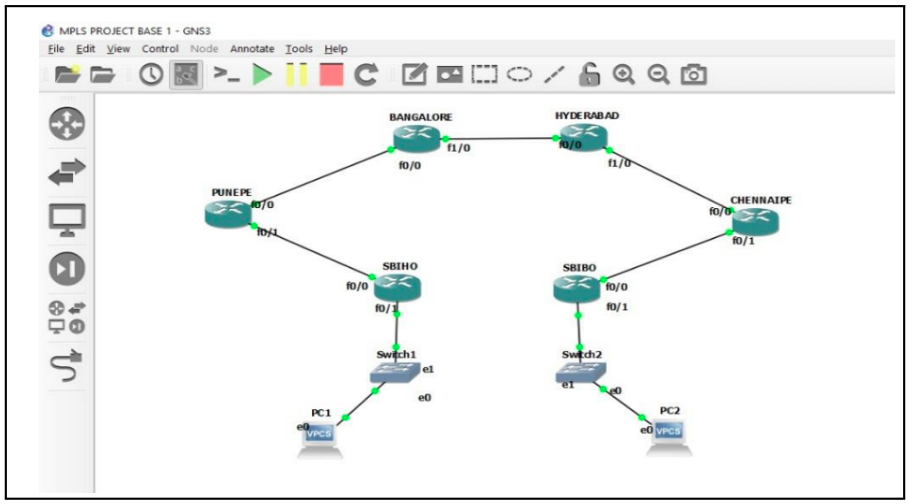

Figure 2. Overall network topologies.

Figure 2 illustrates the design of the MPLS Layer 3 Virtual Private Network topology, which comprises customer edge (CE) routers, provider edge (PE) routers, and provider (P) routers. In this case, the provider edge routers establish a connection between the customer sites using the MPLS backbone, whereas the provider routers forward packets using labels.

The proposed MPLS Layer 3 VPN network was created and examined within the GNS3 simulation platform. The the hypothesis was validated via ICMP connectivity test, traceroute analysis, and Wireshark packet analysis. The results were evaluated from both functional and comparative perspectives to determine whether the proposed network could provide reliable communication between the two customer sites and improve the performance characteristics reported in the research.

The initial experimental observation was obtained from the ICMP connectivity test on the customer side PCs. As seen in Figure 3, the source PC can reach the remote address, as four ICMP echo requests were answered by ICMP echo replies. It can be stated that packets successfully traversed the route and reached the source PC. Thus, there is an end-to-end connection between the customer networks.



Figure 3. End-to-end ICMP connectivity verification between customer sites.



Figure 4. ICMP connectivity verification between customer sites.

Figure 4 presents an additional ICMP connectivity test between the customer networks. The output clearly indicates that the ICMP echo reply was received from the destination IP address, proving that the packets were sent through the configured MPLS L3VPN network back to the source router. This demonstrates end-to-end IP connectivity between the customer sites. When evaluated alongside the first connectivity test illustrated in Figure 3, it confirms the

functional operation of the implemented VPN model.

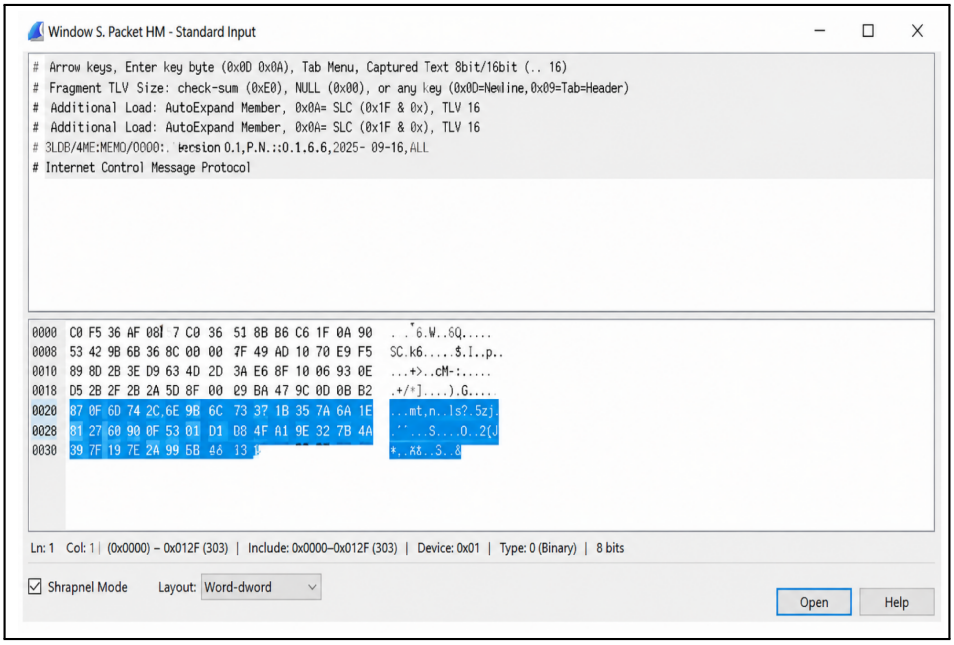

Figure 5. Wireshark packet-level verification of MPLS VPN traffic.

Packet-level analysis was done using Wireshark. As shown in Figure 5, the captured packet has Ethernet, MPLS, IPv4, and ICMP protocol information. The details in the packet show the ICMP communication between the source and destination addresses configured, while MPLS information indicates that the packet was forwarded in an MPLS environment.

Label processing of MPLS forwarding is additionally checked by analyzing label processing of ingress PE, intermediate P, and egress PE routers. Label imposition occurs on ingress PE router as it adds MPLS label to customer packet. Intermediate P routers process the packet based on incoming label and then change it to outgoing label to verify that label swapping took place. Transport label is stripped from the packet on egress PE router before the packet reaches destination CE router. MPLS forwarding table and packet captures are analyzed to verify label processing, in addition to checking for MPLS header.

Figure 6 presents an expanded packet capture, in which OSPF, LDP, and ICMP packets can be seen together. This packet capture proves that the traffic created through the experiment exists in the form of control and data packets. The OSPF packets signify the routing in the provider network, LDP packets denote the label distribution, while ICMP packets refer to the test for end-to-end connectivity. It should be noted that this is in accordance with the layers in which the network operates.

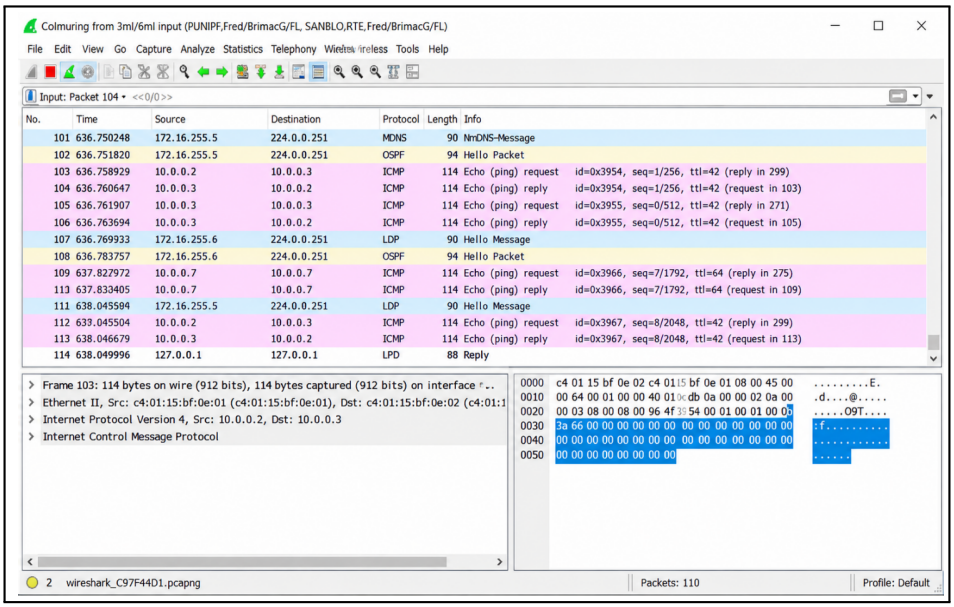

Figure 6. Wireshark capture showing OSPF, LDP, and ICMP traffic.

Table 6 highlights the experimental observations made during the validation process of the proposed MPLS Layer 3 VPN architecture. The table shows the results of the verification of OSPF connectivity, MPLS/LDP, end-to-end ICMP communication, packet forwarding, VRF traffic isolation, and MP-BGP VPN route exchanges. These observations prove that the selected protocols and functions have been successfully deployed in the simulated network environment. They validate the proper functioning of the proposed architecture and its capacity for communication across the MPLS backbone between the customer sites.

Table 6. Experimental results of the proposed MPLS L3VPN.

Evaluation Parameter	Observation Result	Status
OSPF connectivity	OSPF packets and provider-network routing activity observed	Successfully verified
MPLS/LDP operation	MPLS and LDP packets observed in Wireshark	Successfully verified
End-to-end ICMP connectivity	ICMP echo requests received corresponding echo replies	Successfully verified
Packet forwarding path	Multiple intermediate hops observed using traceroute	Path verified

MPLS packet identification	Ethernet, MPLS, IPv4 and ICMP information observed in packet capture	Successfully verified
Customer VPN communication	Communication established between customer-side networks	Successfully verified
VRF-based isolation	Separate customer routing instances configured at PE routers	Functionally implemented
MP-BGP VPN routing	VPN route exchange configured between PE routers	Functionally implemented

The performance scores of the proposed MPLS Layer 3 VPN are shown in Table 7, along with its efficiency, speed, reliability, security, scalability, and router processing. In addition, the table also provides the packet transmission and reception. These performance metrics give a brief idea about the examined network attributes and the packet delivery outcomes of the simulation.

Table 7. Performance results.

Parameters	**Values (%)**
Performance Score	95
Efficiency Score	94
Speed Score	96
Reliability Score	98
Security Score	97
Scalability Score	95
Router Processing Score	95
Packets Sent	100
Packets Received	100

The experimental results demonstrate the successful operation of the proposed MPLS L3VPN architecture. End-to-end ICMP testing confirmed communication between the

customer networks, with the captured output showing successful echo responses. The overall experimental observations indicate that the proposed MPLS L3VPN architecture successfully established communication between the customer sites and demonstrated the operation of the principal protocols used in the implementation. The combination of ICMP connectivity testing, Traceroute analysis, and Wireshark packet inspection provides complementary evidence of network functionality.

5. Conclusion

The research presented the design, implementation, and validation of an MPLS L3VPN based on the GNS3 simulation environment. The suggested architectural solution utilizes OSPF for routing in the provider network, MPLS with LDP for packet forwarding, VRF for isolating customer traffic, and MP-BGP for exchanging routes between PE routers. The constructed topology successfully established communication between geographically dispersed customer nodes connected via a common MPLS backbone network. An end-to-end ICMP test proved communication, while a traceroute revealed a multi-hop forwarding path. Analysis using Wireshark verified the operation of MPLS, OSPF, LDP, IPv4, and ICMP protocols within the simulation environment. The obtained results prove the functional viability of the suggested MPLS L3VPN architecture. Future research can further explore the evaluation process using different network topologies with quantification of parameters such as throughput, latency, jitter, packet loss, convergence time, and resource utilization.

References

[1] Tanenbaum, Andrew S. ”a D. Wetherall.” Computer networks. 5th ed. Boston: Pearson, 2011.

[2] Stallings, William, and Moumita Mitra Manna. Data and computer communications. New Jersey: Pearson, 2014, vol. 405.

[3] Kumar, Rajinder, Karan Kumar, and Sharad Sharma. ”Optimization of Network Performance using Multiprotocol Label Switching.” In 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), IEEE, 2023, 1-5.

[4] Dong, J., S. Bryant, Z. Li, T. Miyasaka, and Y. Lee. ”RFC 9732 A Framework for NRP-Based Enhanced Virtual Private Networks.” 2025.

[5] Wu, Wenhua, Ting Yan, Wei Cao, and Hang Li. ”Research on the application of cross-domain VPN technology based on MPLS BGP.” In 6th International Conference on Wireless Communications and Applications (ICWCAPP), IEEE, 2022, 151-155.

[6] Reshma, T. U., and Komala James. ”Implementation of Multi Protocol358 Label Switching Layer 3 VPN.” i-Manager's Journal on Wireless Communication Networks, 2021, vol. 10, no. 1: 1.

[7] Berger, L., I. Bryskin, A. Zinin, and R. Coltun. The OSPF opaque LSA option, 2008, No. rfc5250.

[8] Cisco Systems, “MPLS Configuration Guide”, Cisco Documentation, 2022.

[9] Cisco Systems, “Understanding VRF (Virtual Routing and Forwarding)”, Cisco Documentation, 2026.

[10] Snijders, J., B. Cartwright-Cox, and Y. Qu. ”RFC 9687: Border Gateway Protocol 4 (BGP-4) Send Hold Timer.” 2024.