# MPLS VPN Layer 3 Implementation and Comparative Analysis on Cisco and Huawei Devices Using GNS3

Fauzan Fadillah[*1], Frencis Matheos Sarimolle[2], Dadang Iskandar Mulyana[3]

[1,2,3]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika (Stikomcki) Jakarta, Indonesia
*Corresponding Author:
Email: fznfdlh30@gmail.com

***Abstract***

*This study discusses the implementation and comparative analysis of MPLS VPN Layer 3 on Cisco and Huawei devices using GNS3 simulation in an effort to understand the differences in performance and configuration characteristics of the two network vendors that are widely used in backbone infrastructure. The problem raised is how the configuration, routing stability, and performance of the MPLS VPN L3 service differ when running on devices with different architectures and operating systems. This study aims to provide a comprehensive overview of the structural and operational differences between Cisco IOS and Huawei VRP, including the OSPF routing process, MPLS label exchange, and the formation of VPNv4 BGP. The methods used include simulated topology design, device configuration, parameter testing such as latency, convergence time, throughput, and result analysis using a comparative approach. The results of the study are expected to be able to show the advantages and disadvantages of each vendor in the implementation of MPLS VPN L3 and provide a basis for consideration for practitioners or agencies in choosing network devices that suit operational needs. This research also contributes in the form of configuration documentation and performance analysis that can be a reference for the development of MPLS-based networks in academic and industrial environments.*

***Keywords:*** *MPLS; L3VPN; Cisco; Huawei and GNS3.*

## I. INTRODUCTION

The rapid growth of data and communication technology has prompted the increasing need for PC network infrastructure that is able to provide information communication services in a light, reliable, convenient and scalable manner. Modern organizations, whether in government or industrial learning zones, usually have networks spread across various geographical positions so that they require effective network breakdown to connect all these branches in one integrated communication system. One of the technologies that is widely used to meet this need is Multiprotocol Label Switching (MPLS). MPLS is a forwarding technology that works by distributing labels on information packets so that the delivery process is no longer entirely dependent on searching conventional IP routing tables. With this mechanism, MPLS is able to improve the efficiency of the forwarding process, reduce latency, and support better traffic management on large-scale networks [1].In the implementation of the Wide Zone Network (WAN), MPLS technology is often combined with Virtual Private Network (VPN) to provide connectivity between positions comfortably through the service provider's backbone network. One of the most widely used implementations is MPLS VPN Layer 3 (L3VPN). MPLS L3VPN allows segmentation of the customer's network using the concept of Virtual Routing and Forwarding (VRF), so that each client or network domain has an isolated routing table.

This approach shares a high level of security, routing management flexibility, and ease of integration with dynamic routing protocols such as OSPF and BGP [2]. Several studies show that the implementation of MPLS L3VPN can improve network performance compared to traditional IP networks, especially in terms of latency, throughput, and stability of information transmission [3], [4]. Not only that, but L3VPN's MPLS also supports better network scalability, making it perfect for use on backbone networks with a large number of branches and traffic. However, in practice, the implementation of MPLS VPN is inseparable from various

challenges, especially in the multi-vendor area. Network features from different vendors, such as Cisco and Huawei, have architecture, configuration syntax, and MPLS protocol implementation mechanisms that are not entirely identical. The comparison includes setting the Label Distribution Protocol (LDP), using MP-BGP for VPN data distribution, and interoperability mechanisms between features The research first shows that the comparison of implementations between vendors can affect the network performance and stability of MPLS VPN services as a whole [5].

To avoid the risk of network problems, MPLS VPN implementation and testing are usually tried first in the simulation area. One of the widely used network simulation software features is Graphical Network Simulator 3 (GNS3). GNS3 allows users to build a virtual network topology that matches the state of the real network and supports the use of features from various vendors. Some research confirms that GNS3 is an efficient medium for analyzing MPLS network performance, testing feature interoperability, and evaluating quality of service (QoS) in various network scenarios [6], [11]. Based on this explanation, it can be concluded that although MPLS VPN Layer 3 technology has been widely applied and researched, studies that specifically equate the implementation and performance of MPLS L3VPN with Cisco and Huawei features in the same simulation area are still relatively limited. Therefore, this research is tried to analyze the implementation and equalize the performance of MPLS VPN Layer 3 on Cisco and Huawei features using GNS3 simulators. The results of the research are expected to provide a comprehensive reflection of the comparison of configurations, interoperability, and performance characteristics of the two vendors in providing MPLS L3VPN services [7], [8].

## II. METHODS

This study used experimental and comparative design to analyze the implementation and performance of Multiprotocol Label Switching Virtual Private Network Layer 3 (MPLS L3VPN) in multi-vendor environments, namely Cisco and Huawei devices. All experiments were conducted in a controlled simulation environment using GNS3, allowing for objective testing of protocols and network performance without impacting the production network. This approach aims to compare the configuration effectiveness, protocol interoperability, and quality of network services on both vendors under identical topological conditions and traffic scenarios.The experimental environment is designed to represent a small-scale ISP backbone architecture with a P–PE–CE model, consisting of two Provider Edge (PE) routers from Cisco and Huawei vendors, one Provider Core (P) router, and two Customer Edge (CE) routers as customer endpoints. Each backbone device is configured using OSPF as the Interior Gateway Protocol (IGP) on a single backbone area, while MPLS with Label Distribution Protocol (LDP) is used to distribute labels and form a Label Switched Path (LSP). For VPN services, MP-BGP VPNv4 is enabled on PE routers to carry the customer's route along with the Route Distinguisher (RD) and Route Target (RT) attributes, while the core router only functions as a label switcher without storing the customer's route.The implementation of MPLS L3VPN is carried out in stages, starting from the configuration of the backbone connectivity, the activation of OSPF, and the activation of MPLS and LDP on all backbone links. Furthermore, Virtual Routing and Forwarding (VRF) is defined on each PE router to separate customer traffic, followed by routing configuration between CE and PE.

After that, the VPNv4 MP-BGP session is built between PEs using loopback addresses as the peering source, and the customer routes are distributed into the VPNv4 table. Successful implementation is verified through protocol status checks, MPLS forwarding tables, and end-to-end connectivity testing between CE-A and CE-B.Network performance testing is focused on end-to-end communication paths that pass through the MPLS L3VPN backbone. The Quality of Service (QoS) parameters evaluated include latency (Round Trip Time), packet loss, throughput, and MPLS path stability. Latency and packet loss measurements are performed using ICMP testing with small and large packet sizes in a given number of repeats, while throughput is measured using a traffic generation tool such as iperf over a specified time interval. The test was carried out in two directions, namely from the Cisco side to Huawei and vice versa, to ensure objective and balanced comparison results.The data obtained from the testing process included quantitative data in the form of network performance measurement results as well as qualitative data in the

form of device configurations and protocol logs, such as OSPF, LDP, MPLS forwarding, and BGP VPNv4. All data were analyzed by comparing the average values and performance trends of each vendor, as well as observing the consistency of switching labels and route stability. With this methodology, the research is expected to be able to provide an objective evaluation of the performance, interoperability, and implementation characteristics of MPLS L3VPN on Cisco and Huawei devices in a multi-vendor environment.

## III. RESULT AND DISCUSSION

This section discusses the results of the implementation, testing, and analysis of the MPLS VPN Layer 3 network made in imitation areas using GNS3 with Cisco and Huawei tools. The discussion focused on the application level of the form of connectivity testing, and the record of network performance based on *latency, packet loss, throughput*, and route stability.The analysis was carried out by comparing the results of MPLS L3VPN testing on both vendors in the same topology and similar scenarios as a result of obtaining an objective picture of the implementation character and performance of each device.

### 3.1 Research Tools

The research tools in this thesis are used to support the process of implementation, testing, and analysis of MPLS VPN Layer 3 networks on CiscoASR920 and HuaweiNE8000 devices using a simulation environment. The selection of research tools aims to ensure that the testing process can be carried out in a controlled, efficient, and close to real network conditions.

### 3.2 HardwareThis

Research was conducted using one computer unit as a simulator host with the following specifications:

a) **Processor**: Intel(R) Core(TM) Ultra 7 165U (1.70 GHz)
b) **RAM :** 16GB
c) **Virtualization :** *Platform: VirtualBox*
d) **Network :** *Virtual Network (Internal Network)*

### 3.3 Software

The software used in this study includes:

a. Host Operating System : Windows 10 / Windows 11
b. Network Simulator : GNS3 version 2.2.
c. *Virtualization Engine* : *VirtualBox*
d. Cisco Router: Cisco IOS (*Virtual Router*)
e. Huawei Router : Huawei VRP (*Virtual Router*)

The software is used to build network topologies, configure MPLS VPN Layer 3, and run network connectivity and performance tests.

### 3.4 Research Scenarios

The research scenario was compiled with reference to the standard architecture of the MPLS VPN Layer 3 network which consists of:

*a. Customer Edge (CE)*
*b. Provider Edge (PE)*
*c. Provider Core (P)*

Then each device is configured using the protocol:

a. **OSPF** as *the Interior Gateway Protocol*.
b. **LDP** for label distribution.
c. **MP-BGP** for VPNv4 route switching.
d. **VRF** for the separation of the customer's network.

This scenario is used to test the interoperability as well as performance of MPLS VPN Layer 3 between CiscoASR920 and HuaweiNE8000 devices in the same simulated topology.

### 3.5 Implementation and Testing

In this step, the application and testing of the MPLS VPN Layer 3 network are carried out based on the concept and research methodology that has been described in Chapter III. The implementation was carried out using a GNS3 simulator by practicing the form of MPLS VPN L3 on multi-vendor tools, namely Cisco routers and Huawei routers. How to implement it includes building a network topology, configuring routing, implementing MPLS and VPNs, and testing network connectivity and performance. The test is carried out to ensure that the configuration applied is compatible with the research objectives and to obtain information on the appearance of the network which is then analyzed in the next chapter.

### 3.6 MPLS VPN Layer 3 Simulation Implementation

The practical step is carried out by creating a network simulation environment using GNS3 as a test tool This simulation environment is designed to represent the MPLS VPN Layer 3 backbone network in real situations using multi-vendor devices, namely Cisco routers and Huawei routers.

The network topology is structured with a Provider – Customer scheme, which consists of some important components, namely:

1. **Provider Edge (PE)**

The PE router acts as a link between the client network (Customer Edge) and the MPLS backbone network. In this research, two types of PE routers from different vendors, Cisco and Huawei, were used to test the interoperability of MPLS L3VPN.

2. **Provider (P)**

Router P acts as a core router in the MPLS network that works to execute the label switching method without knowing the client's network information

3. **Customer Edge (CE)**

CE routers act as client routers that connect directly to PE routers and use standard IP routing without MPLS configuration.

The MPLS VPN Layer 3 network topology used in this research can be observed in the following image:

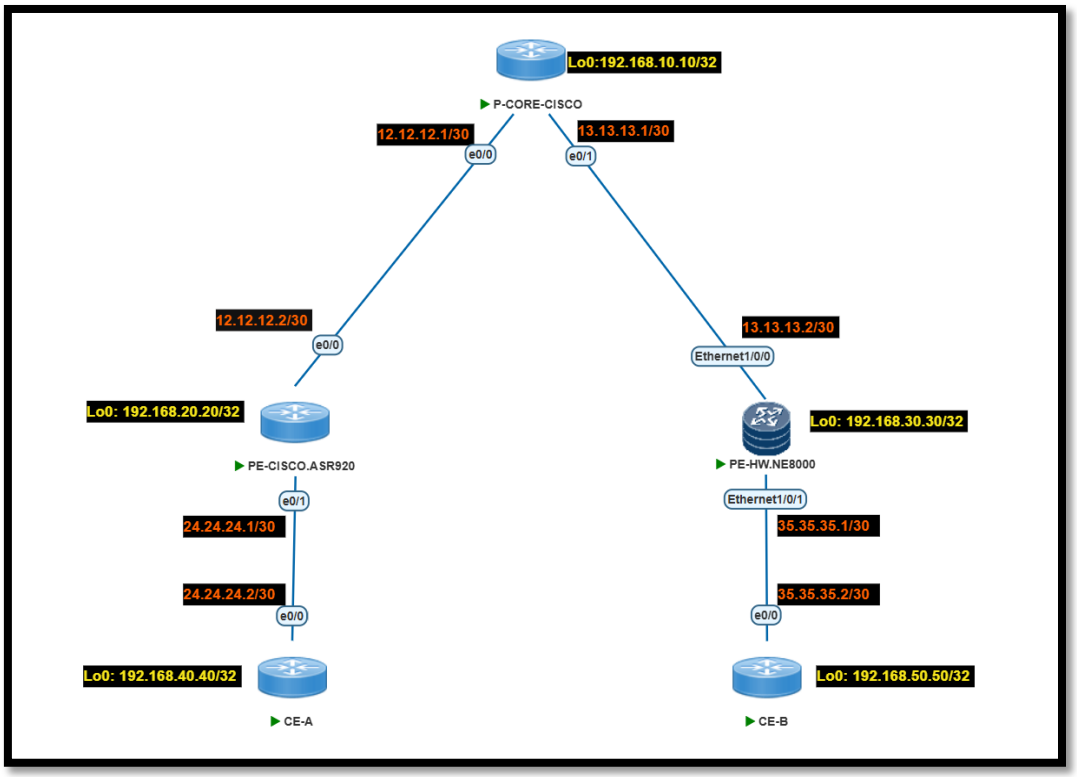


**Fig 1.** Mpls Vpn Layer 3 Simulation

### 3.7 Research Roadmap

In the study titled "Implementation and Comparative Analysis of MPLS VPN Layer 3 on Cisco and Huawei Devices Using GNS3", the research roadmap is as follows:

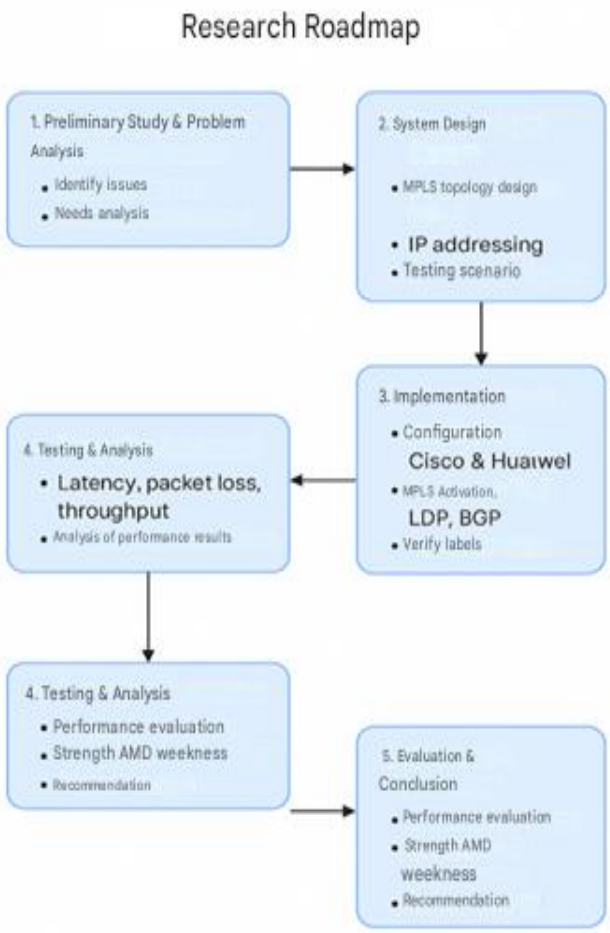


**Fig 2.** Research Roadmap

From the picture above, it can be explained as follows:

1. **Stage 1: Preliminary Study and Problem Analysis**

This stage focuses on identifying the main issue in the study, which is the need to compare the performance of MPLS L3VPN on two different network devices of the vendor.

a. Identify network issues, such as differences in MPLS protocol performance, compatibility, and stability between Cisco and Huawei devices.

b. Analyze system requirements, including the determination of the protocols used (OSPF, LDP, MP-BGP) as well as the QoS parameters to be tested (latency, packet loss, throughput)

c. Gather journal references, standard RFCs, and vendor documentation to build theoretical foundations regarding MPLS L3VPN, LDP, VRF, and multi-vendor interops.

2. **Stage 2: System Planning**

This stage is to develop the network design that will be used in the MPLS L3VPN simulation.

a. Designing MPLS backbone topology, including P-Core, PE-Cisco, PE-Huawei, and CE-A/CE-B routers.

b. Define IP addressing, loopback, and subnet schemes between devices to match the needs of MPLS, LDP, and BGP VPNv4.

c. Define performance test scenarios, such as CE-A → CE-B traffic direction and vice versa, as well as the size of the test package.

3. **Stage 3: Implementation**

This stage is the stage of implementing the MPLS L3VPN configuration on the GNS3 simulator.

a. Cisco and Huawei device configurations, including:

1) MPLS and LDP activation
2) VRF, RD/RT configuration
3) OSPF *backbone settings*
4) MP-BGP Configuration for VPNv4

b. Verify connectivity, ensure the distribution label is running and the VPN path is formed correctly.

c. Configuration adjustments when differences in behavior between vendors are found.

**4. Stage 4: Testing and Analysis**

This stage measures the performance of MPLS L3VPN and analyzes the differences between vendors.

a. Perform network performance tests, such as latency, throughput, and packet loss, using ping test & iperf.

b. Retrieve performance data from both MPLS lines, namely Cisco → Huawei and Huawei → Cisco.

c. Analyze test results, including the stability of switching labels and the effectiveness of each protocol

**5. Stage 5: Evaluation and conclusion**

This stage results in research conclusions based on performance and configuration data.

a. Evaluate the advantages and disadvantages of MPLS L3VPN on Cisco and Huawei based on the test results.

b. Draw final conclusions regarding the effectiveness of implementation, including recommendations for use in real-world scenarios.

c. Drafting advanced research suggestions such as TE TESTING, RSVP-TE, or other multi-topologies.

### 3.8 Research Timeline

In the study titled *"Implementation and Comparative Analysis of MPLS VPN Layer 3 on Cisco and Huawei Devices Using GNS3"* the research timeline is as follows

| No | Activity Name | Main Activities | October 2025 | | | | November 2025 | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | W1 | W2 | W3 | W4 | W1 | W2 | W3 | W4 |
| 1 | Preliminary Study | Problem Identification, Reference Collection | | | | | | | | |
| 2 | System Design Analysis | MPLS L3VPN Topology Design, QoS Parameter Design, Test Scenario Design | | | | | | | | |
| 3 | MPLS L3VPN Implementation | IOS and VRP Image Installation, OSPF, LDP, VRF, MP-BGP Configuration | | | | | | | | |
| 4 | Performance Testing | RTT, Packet Loss, Throughput testing; log capture; label switching analysis | | | | | | | | |
| 5 | Analysis and Evaluation | Data interpretation, Cisco vs Huawei performance comparison | | | | | | | | |
| 6 | Report Preparation and Presentation | Report writing, revision, and SEMPRO preparation | | | | | | | | |

**Fig 3.** Research timeline

## IV. CONCLUSION

Based on the results of the implementation, testing, and analysis that has been carried out in Chapter IV, several conclusions can be drawn regarding the research on the Implementation and Comparative Analysis of MPLS VPN Layer 3 on Cisco and Huawei Devices Using GNS3, as follows:

1. The implementation of MPLS VPN Layer 3 on Cisco and Huawei devices was successfully carried out using a GNS3 simulation environment, which includes backbone OSPF configuration, MPLS LDP, Virtual Routing and Forwarding (VRF), Multi-Protocol BGP (MP-BGP VPNv4), as well as routing between Customer Edge (CE) and Provider Edge (PE).
2. The verification results show that the switching label mechanism on the MPLS backbone network has been running well, characterized by the formation of LDP sessions, active MPLS forwarding tables, and consistent routing paths based on traceroute results.
3. Quality of Service (QoS) testing shows that MPLS VPN Layer 3 networks are able to provide end-to-end connectivity with low latency, no packet loss, and stable packet delivery in both small (64 bytes) and large (1400 bytes) packets
4. Throughput analysis comparatively shows that the network is capable of sustainably delivering large packets without significant performance degradation, which indicates adequate bandwidth capacity on the MPLS backbone.
5. Based on the performance comparison results, Cisco and Huawei devices show relatively equivalent network service quality in MPLS VPN Layer 3 implementations. The differences found are more dominant in the aspects of the configuration mechanism and command structure, rather than in the functional performance of the network.
6. Thus, it can be concluded that MPLS VPN Layer 3 is an effective and reliable networking solution to be applied in multi-vendor environments, especially on Cisco and Huawei devices, in support of large-scale network connectivity needs.

## REFERENCES


[1] A. K. M. Hadod and A. K. M. Hadood, "Design and Implementation of MPLS Layer 3 VPN," ***International Journal for Research in Applied Science & Engineering Technology (IJRASET),*** vol. 13, no. 3, Mar. 2025.

[2] S. Dewi and S. Sulistiyah, "Analysis of Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) for Wide Area Network (WAN)," ***Journal of Information System, Applied, Management, Accounting and Research (JISAMAR),*** vol. 6, no. 1, pp. 16–25, 2022.

[3] I. Nedyalkov, "Performance comparison between virtual MPLS IP network and real IP network without MPLS," ***International Journal of Electrical and Computer Engineering Systems***, vol. 12, no. 2, pp. 83–90, Jun. 2021.

[4] K. O. Okokpujie et al., "Performance of MPLS-based Virtual Private Networks and Classic Virtual Private Networks Using Advanced Metrics," TELKOMNIKA (Telecommunication, Computing, Electronics and Control), vol. 16, no. 5, pp. 2073–2081, 2018.

[5] N. Ismail, E. A. Zaki, and M. Arghifary, "Interoperability and Reliability of Multiplatform MPLS VPN: Comparison of Traffic Engineering with RSVP-TE Protocol and LDP Protocol," ***CommIT (Communication and Information Technology) Journal***, vol. 11, no. 2, pp. 81–90, 2017.

[6] W. Chen, "Architecture Design and Performance Analysis of MPLS VPN in Meteorological Wide-Area Networks," ***International Journal of Advance in Applied Science Research,*** 2024 (online first).

[7] Fathurrahmad and S. Yusuf, "Implementation of VPN Network with Routing Protocol on Multiprotocol Label Switching (MPLS) Network," ***Journal of Information and Communication Technology (JTIK),*** vol. 3, no. 1, pp. 1–8, 2019.

[8] Y. Rahmawati, S. Ikhwan, and I. P. Hadi, "Multiprotocol Label Switching Virtual Private Network (MPLS VPN) Design Using MX Juniper 14.1R1.10 Router Simulator," Proceedings of the CENTIVE National Conference (Electrical and Informatics Engineering), Telkom Purwokerto, 2018.

[9] Efendi and Haeruddin, "Analysis of MPLS L3 and L2 VPN Networks in the Pandemic Period," ***Journal of Computer Science and Business,*** vol. 12, no. 2, 2022.

[10] Mardianto, "Quality Of Service (QoS) Analysis on VPN Networks and MPLS VPNs Using GNS3," ***Journal of Science and Informatics,*** vol. 5, no. 2, pp. 98–107, 2019.

[11] R. Apsari, M. Rosmiati, and T. Zani, “Building MPLS Network Simulation Using GNS3 at PT. Telkom," ***International Journal of Engineering and Technology (IJET),*** vol. 8, no. 1.9, pp. 246–249, 2019.

[12] I. Grgurevic, G. Barišić, and A. Stančić, "Analysis of MPLS and SD-WAN Network Performances Using GNS3," in FABULOUS 2020, Springer, 2021.

[13] I. G. J. Putra, P. K. Sudiarta, and I. M. A. Suyadnya, "Comparative Analysis of OSPF Routing on MPLS and Non-MPLS Networks Using GNS3," ***SPEKTRUM Journal***, vol. 4, no. 1, pp. 1–8, 2017.

[14] N. K. Handayani, A. F. Rochim, and R. R. Isnanto, "Network Simulation of Diponegoro University with Multiprotocol Label Switching (MPLS) Using Graphical Network Simulator (GNS3)," Transient: ***Scientific Journal of Electrical Engineering***, vol. 1, no. 3, 2012.

[15] M. Farhan et al., "A Comparative Analysis of Unicast Routing Protocols for MPLS-VPN," Lahore Garrison University ***Research Journal of Computer Science and Information Technology***, vol.3, no. 1, pp. 43–49, 2019.

[16] K. A. Amusa et al., "Mitigating the Traffic Congestion Using MPLS Routing Towards Greater Efficiency in an IP Based Network," ***LAUTECH Journal of Engineering and Technology,*** vol. 14, no. 1, 2020.

[17] A. M. Sllame, "Modeling and Simulating MPLS Networks," in Proc. 2014 International Conference on Systems, Signals and Communication (SNCC), IEEE, 2014.

[18] B. Mohamed et al., "Comparative Analysis of DMVPN Phase 3 Performance Across Dynamic Routing Protocols," ***Libyan Journal of Informatics***, vol. 1, no. 1, pp. 18–36, Jun. 2024.

[19] M. Mansour, A. Samood, and N. B. Saud, "Assessing Queue Management Strategies to Enhance Quality of Service in MPLS VPN Networks," ***Libyan Journal of Informatics***, vol. 1, no. 2, 2024.

[20] L. M. Silalahi et al., "Application of MPLS Tunnel Service L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Service Analysis," ***International Journal of Electronics and Telecommunication***, vol. 69, no. 4, pp. 1–8, 2023.