iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67201

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Design and Implementation of MPLS Layer 3 VPN

Ahmad Kalifa Mohamad Hadod[1], Ashraf Khalifa M. Hadood[2]
[1]*Faculty of Engineering. University of Gharyan, Libya*
[2]*Faculty of Science, University of Gharyan, Libya*

Abstract: ***This paper presents a proposal for the construction and use of MPLS Layer 3 VPNs, with their design for interconnection of physical routers either without traffic redundancy or offering this quality. The incentive for the study and use of VPNs is given not only by the flexibility and privacy that these capabilities can offer to service providers and users, but mainly by the reduced cost they impose when compared to traditional circuits. The rapid growth of new protocols and solutions for implementing both the benefits of traffic engineering and quality of service offers the possibility of exploring noteworthy prospects for VPN implementation in the market scenario. The following topics cover the general design of MPLS Layer 3 VPNs, VPN feature interconnections, the implementation according to the test setup, and finally performance evaluation. The results are of critical importance for the benefits offered to service providers and users, and other events involved when adopting MPLS VPNs in their environments. The results also contribute to the conclusion that the implementation of MPLS VPNs is a migratory phase, given that the cost of an end-to-end VPN connection becomes smaller when we think about the capacity crunch issue in the production of optical equipment for the size of the CPE market.***

I. INTRODUCTION

A Virtual Private Network (VPN) is a communication network that shares the same characteristics as a private network, including security, and can be provided easily and cost-effectively to end users over a shared infrastructure. IP-based networks are widely deployed due to their flexibility and features. Internet Protocol (IP) is the most popular among IP-based networks since there are many communication equipment vendors and multimedia applications are becoming more popular. Therefore, developing an IP-based VPN is very important. However, building the entire IP-based VPN using expensive private lines is often not cost-effective. [1]

Instead, the VPN provider could offer a shared infrastructure, while corresponding virtual private networks could be provided for different customers. To guarantee a private tunnel, several basic technologies can be used: IP security, IPSec, or multi-protocol label switching (MPLS). IPSec is a security protocol that adds an extension to the IP layer, while MPLS extends the layer of multiprotocols. IPSec protects the data in tunnel mode, improves security, but reduces tunneling performance. Shared encryption between multiple customer sites in the ISP reduces the economic value of IPSec. [2]

The main functions of MPLS technology are to improve QoS ability and meet service requirements for real-time transmission applications. Especially for campus networks, the functionality of MPLS includes: configuring static LSP tunnels, supporting QoS tunnel policy functions, and selecting services based on tunnels rather than on IP addresses. The basic concept of an MPLS VPN (Layer 3) is to use an MPLS-based backbone network to provide IP interconnection for a user's branch and headquarters (called Customer Edge, CE). The user's internal part (called Private Network, P) is not directly connected to the MPLS backbone. [3]

Customer sites' routers are logically divided into two virtual classes through LDP; one class is P routers, the data of which will be transparently transmitted to PEs through the MPLS backbone, and the other class is PE routers, where the VPN protocols are installed. The PE routers have LDP neighbor relationships with PE routers in other customers only. This ensures the isolation of the VPNs owned by different customers. There are two different VPN models according to different operational logic: one is called P2P (point-to-point), and the other is called MP2P (multi-point-to-point). In the P2P type VPN, only one CEP pair is required, in which the two CEs can connect to each other directly or through a P router. The MP2P VPN does not need a physical design tunnel pair but requires a common subtree structure, which can be realized by traffic engineering techniques. [4][5]

The Layer 3 MPLS VPN is typically built on the MPLS-based Layer 3 routing protocol. In terms of current hardware development, a Layer 3 MPLS VPN protocol structure is presented and its implementation is designed. The device supports routing and switching, meeting the basic demand for the Layer 3 MPLS VPN. In addition, a typical deployment of the Layer 3 MPLS VPN in the campus area is proposed, which is built on the inner CS/domain structure and binds the campus network. The proposed approach improves network security and reduces the impact of the influence problem. These two features are consistent with the campus network operation characteristics and requirements. [6]

II. OVERVIEW OF MPLS TECHNOLOGY

Multiprotocol Label Switching (MPLS) is a high-performance routing technology that integrates the speed of Layer 2 switching with the advanced intelligence of Layer 3 routing. This model allows for the creation of "virtual private clouds" that provide reliable, accurate, and secure communication channels between multiple customer sites, while not incurring the cost of ownership at the level of high-cost intranet solutions provided. This guide walks you through the basic building blocks of MPLS and the configuration of a custom VPN in a lab environment. The Label Distribution Protocol (LDP) is selected as the label distribution protocol, but the Border Gateway Protocol (BGP) can be configured as an alternative. [7 Labels are distributed among the BGP and environment routers and service providers. RSVP (Resource Reservation Protocol) is a label distribution protocol for LSPs, which require guaranteed quality of service. Services that use RSVP for LSPs include L2VPN/VPLS, VPRN, MPLS TE, and expansion services to name just a few. Although these services also use LDP, LDP cannot provide the same service as RSVP. Therefore, for these services, RSVP is used as a label distribution protocol. On the other hand, MPLS TE could also use LDP for label distribution, but RSVP is preferred. [8]

1) Layer 3 VPN Concepts

Layer 3 VPN or VPRN utilizes a routing model that allows packets to be forwarded to customer VPN sites through a service provider IP network while maintaining packet segregation. Layer 3 provider edge (PE) routers participating in Layer 3 VPN are online Layer 3 routing devices that provide Layer 3 VPN services to the customers connected to the Layer 3 PE routers. The PE router, acting as the provider's VPN edge, exchanges the customer's private routing information with each other. It also routes and forwards the VPN routing information for VPN members. On the PE router, the data packet sent from the CE router first enters the assigned virtual routing sites according to the VPN label, the source address, and the VPN protocol with which the CE router is connected via the PE, and then packet forwarding is performed. [9][10] The CE routers based on the VPN routing must be able to provide multi-routing forwarding. It is important to note that Layer 3 VPN is not intended for massive exchange of IP routing information. If the number of VPN members increases, the PE routers may become overwhelmed by the routing processing and memory consumption required to maintain routing information for VPNs. With Layer 3 VPN, each VPN community must establish a direct connection between each CE router and the service carrier PE router, and configure and maintain the IGP of VPN for independent routing domain consistency. [11]

2) Purpose and Scope of MPLS Layer 3 VPNs

Virtual Private Networks (VPNs) are a means of providing connectivity for an organization over a regular public data network while maintaining privacy through the use of tunneling protocols and security procedures. The Internet and IP protocol are widely used for constructing VPNs, not only because of the richness of the services supported by IP, but because it is ever-present. Currently, one of the most popular technologies for building IP VPNs is MPLS. We want to study several features of the most widely applied type of MPLS-based VPNs, the MPLS Layer 3 VPN, in order to fine-tune and make a reference to its implementation. Our industry standard exercises lead us to undertake different approaches and conclusions. The results of our experiments and evaluations will be of great interest to a wide set of network administrators who desire to fine-tune their systems in an efficient way. [12]

The purpose of this paper is to study the design and implementation of Layer 3 MPLS VPNs and test the different alternatives as a way of choosing the most appropriate one. With the advances in capacity and QoS levels, applying MPLS to the construction of VPNs seems natural due to the fact that the low-level functionality of IP has left the deployment of private networks to be virtual router platform vendor-specific, and the level of security remains proprietary in each case and has not changed over time. What has changed are the speeds and functionality levels inherent to the new hardware/software platforms. The scope of the study is to study how MPLS works and to gain some insight into the functionalities of several existing MPLS VPN solutions from a wide set of vendors. The initial goal is to build MPLS Layer 3 (L3) VPNs with Cisco 7200 and 7206VXR series routers using Cisco IOS release 12. Small scenarios will be implemented and evaluated, changing router configuration options in order to get some reference for the time consumed by different operations. [13]

3) MPLS VPN component

Figure shows MPLS core network component

a) Customer Edge (CE)

- Owned and managed by the end customer.
- Interface with the MPLS service provider network.
- Runs either static of dynamic routing with the adjacent PE router.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

b) Provider Edge (PE)

- Define the boundary of the service provider network.
- Interface with customer edge routers.
- Runs either static or dynamic routing with the adjacent CE router.
- Runs either ISIS or OSPF with the core routers.
- Also in MPLS network called Label edge router **(LER)**

These routers must run BGP, including the BGP/MPLS VPN extensions. They must also be able to originate and terminate MPLS LSPs

c) Provider Router (P)

- Routers in the core of the provider network.
- Interface with other core routers or provider edge routers.
- Runs either ISIS or OSPF with the core routers and PE routers.
- Also in MPLS network called Label switched router **(LSR)**

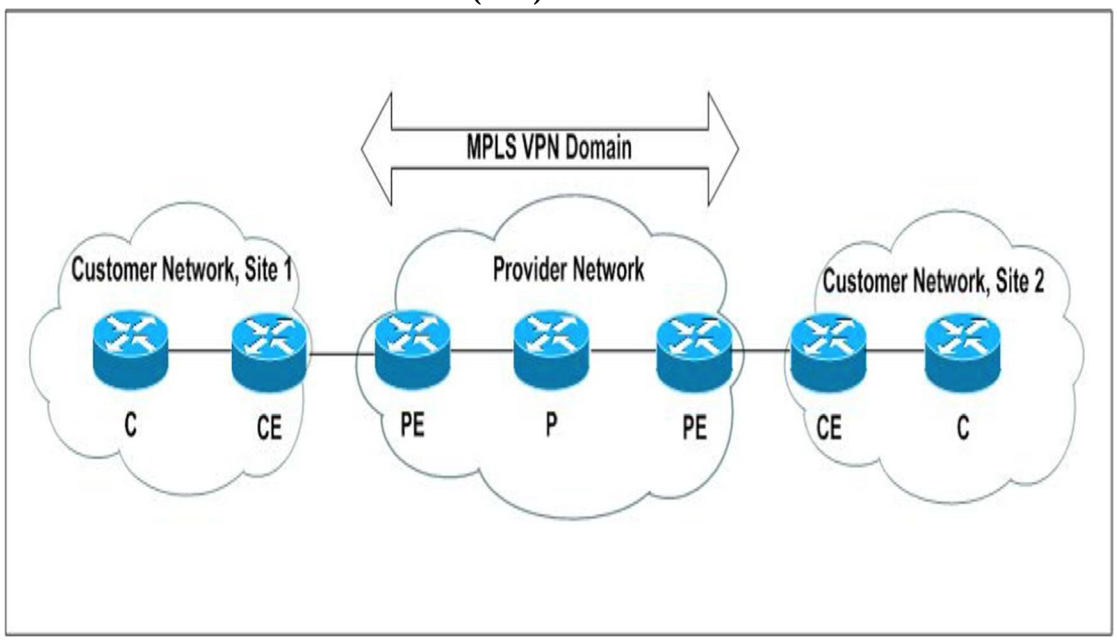


Figure (1.1) MPLS core network component

4) Layer 3 VPN services

In Layer 3 VPN service, the customer's edge routers perform the routing and forwarding functions they are accustomed to using static routes, RIP, OSPF, BGP, or other routing protocols. The service provider network, meanwhile, exchanges with the customer's edge routers only the single customer routing table associated with the VPN's backbone and at the same time preserves the customer's route and encapsulation information. The distinguishing feature of MPLS VPN service is that it provides GRE function and maintains the customer's IP addresses between the CE devices. It's important to take into account that all customer's routes used inside the MPLS VPN cloud have to be unique and not advertised to the public Internet. The guiding principle is as follows: if reached from one customer site, a destination must expose the whole customer Internet. There are three types of redundancy in an MPLS Layer 3 VPN: CE-Side Redundancy, PE-Side Redundancy, and Intra PE Redundancy. [14]

5) Virtual routing and forwarding (VRF)

Virtual Routing and Forwarding (VRF) is a technology used to create multiple routing tables in the routing instance and a separate instance of routing separation. Any kind of traffic that can be transported through a network can be segmented using the VRF facility provided by MPLS VPN solutions. The VRF can share the same link and interface in the routing instance. The Layer 3 device supports the assignment of some interfaces to a certain VRF routing instance, which makes the corresponding VLAN benefit from VPN switching.

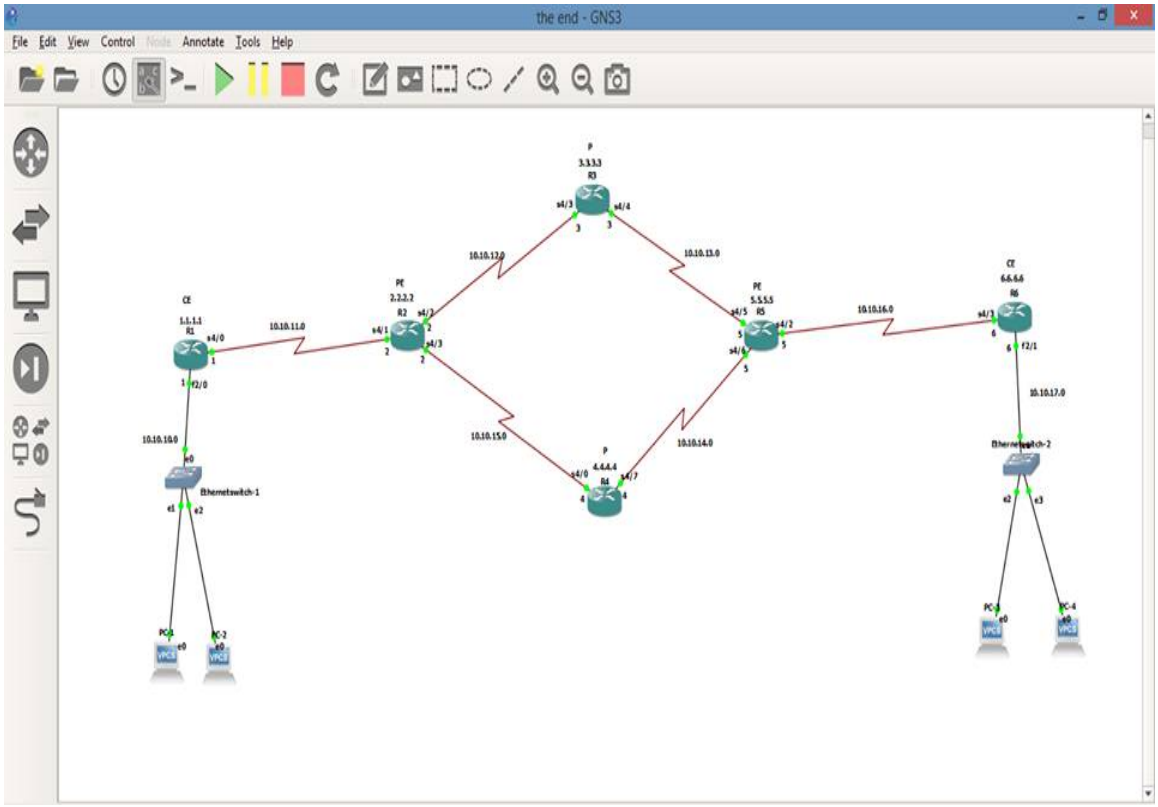
VPN switching sends and receives packets with the lowest label stack in the Control Plane and forwards in the Data Plane according to the label stack value. The label stack is added or popped when the standard MPLS technology is used in the forwarding process. In this way, the devices at the same level share the same resources to avoid purchasing additional services and related equipment. In the latter study, it will be introduced how to set the eBGP between the CE and PE-1, distribute the VPN routing message, OSPF protocol between the PE and PE, and implement the MPLS VPN on NMS. [15]

6) Process of MPLS Layer 3 VPN

In this paper, we talk about the implementation as well as the configuration of a very common MPLS technology or service called Layer 3 MPLS VPN. MPLS Layer 3 VPNs are quite common in service provider and even enterprise networks. Network service providers tend to segment their operations and provide VPN functionality within the network to various customers. The number of VPNs that can be established is often controlled by charging customers a fee based upon the number of VPNs or by the revenue opportunity that multiple VPNs provide. This is much like your phone company providing different services at different costs. This is a significant aspect of the MPLS technology. It can be used to develop a managed services offering for enterprise and service provider networks. In this section, we implement an MPLS L3 VPN service using IOS configuration. We use a spine-leaf network topology that is shown for this lab, which is a subset of our module topology. The lab topology for our MPLS L3 VPN consists of the following devices: ISP rack, ISP rack, CE rack 3, or CE rack 4. Both ISP routers have MPLS/VPN plans implemented for complete routing separation between customer networks, as well as the use of unique route distinguishers handled per site. The PE devices use unique VRFs and route target import/export statements along with route target DISTYLE-ORD. Customer site CE routers run OSPF in the implementation. The VPN service allows for the availability of two backdoor routes into the customer network from each provider router. We will use both architectures to validate the MPLS VPN service. [16]

III. SIMULATION TOOLS USED

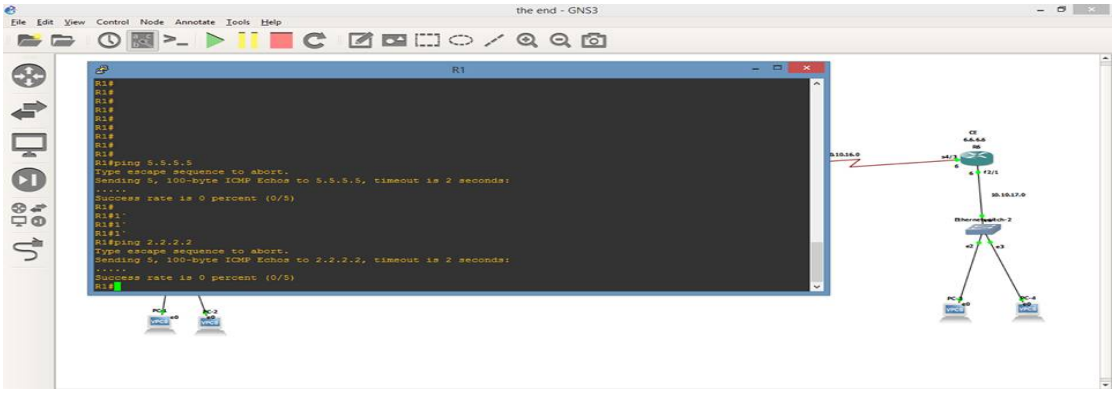
This paper simulates MPLS Layer 3 VPN which be design and verify by using GNS3 software tool and the solutions that provides a secure packet travelling between the customers.



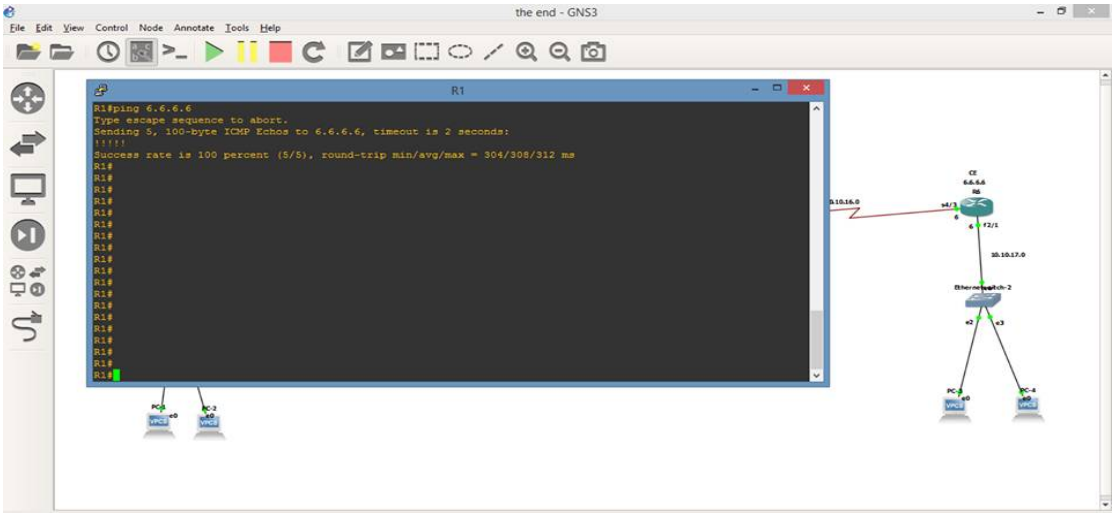
Figure(1.2) show the topology of implementation of MPLS layer 3 VPN

IV. RESULT OF PROJECT

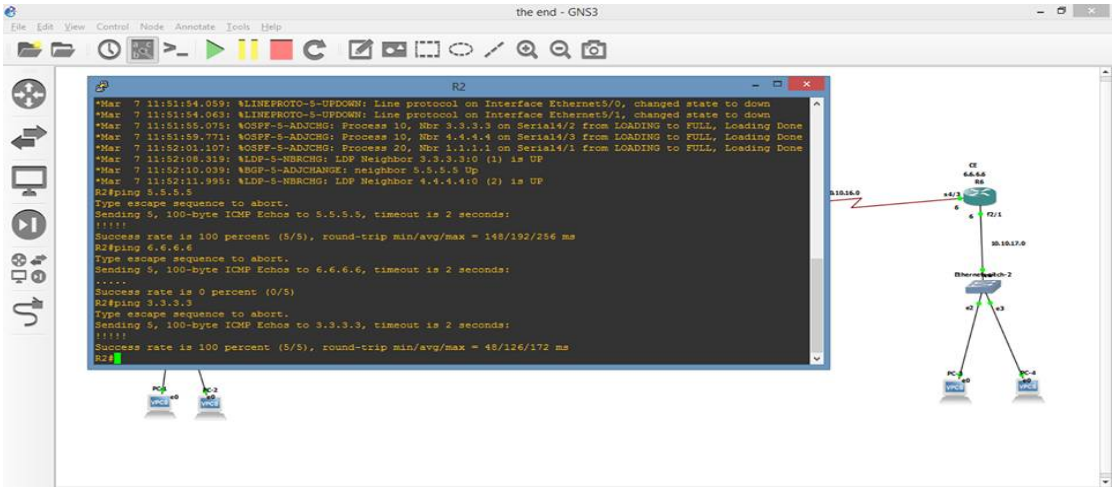
In this result represent R1 and R6 the CE (Customer Edge), R2 and R5 the PE (provider Edge) , R3 and R4 P (provider)
First ping from R1 to R6 , it is mean from site to other site which result is successful and from R1 to R2 ,it's mean same site which result is successful.



R1# ping 6.6.6.6
In this case the result was successful because from CE to CE must be success

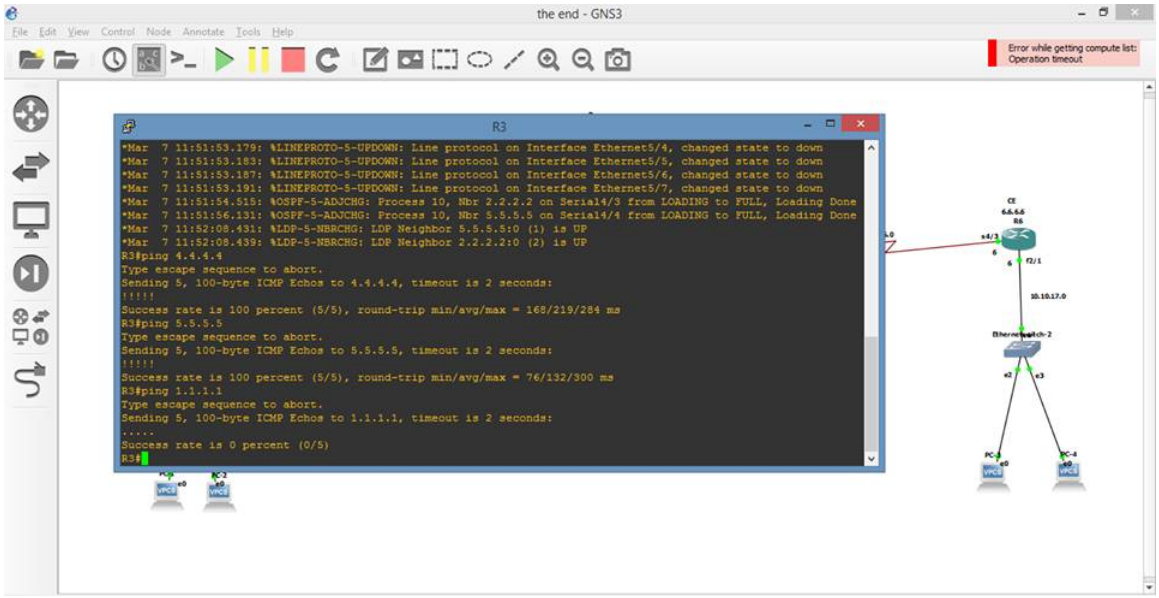


R2#ping 3.3.3.3
In this case the result was successful because this is ping inside the P (provider)



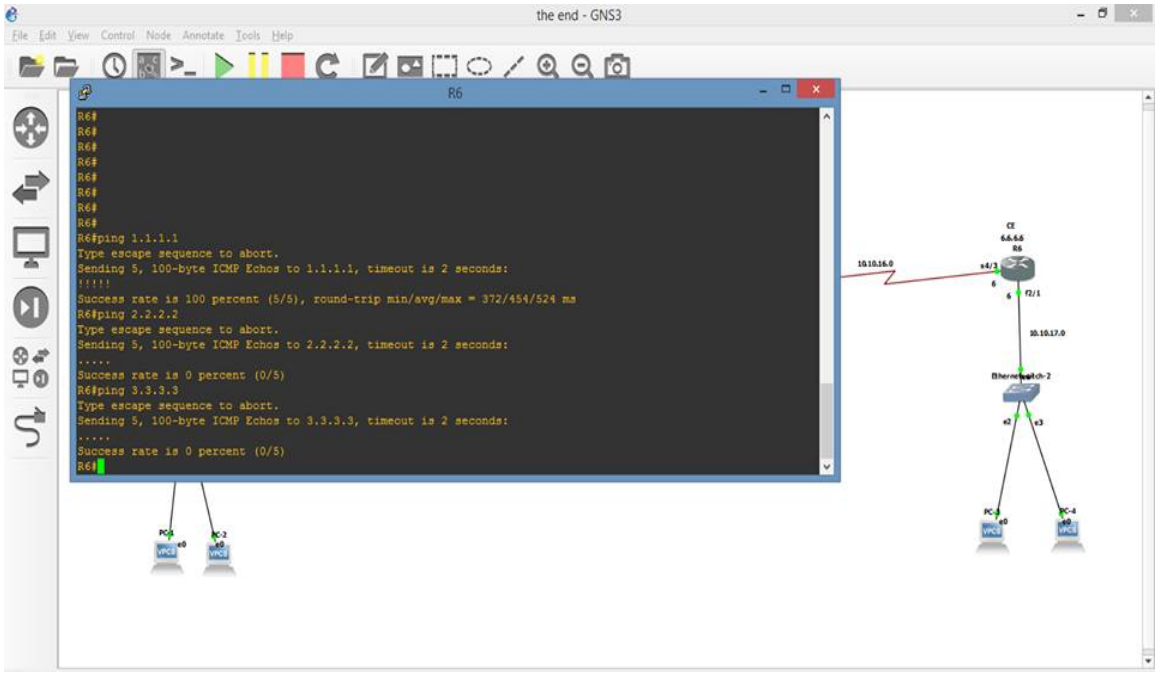
R3#ping 1.1.1.1

In this case the result was fail because this is ping from P which represents ISP to CE which represents any company or organization



R6#ping 3.3.3.3

In this case the result was fail because can't connect from the company supposed be to the P which represent ISP



V. CONCLUSION

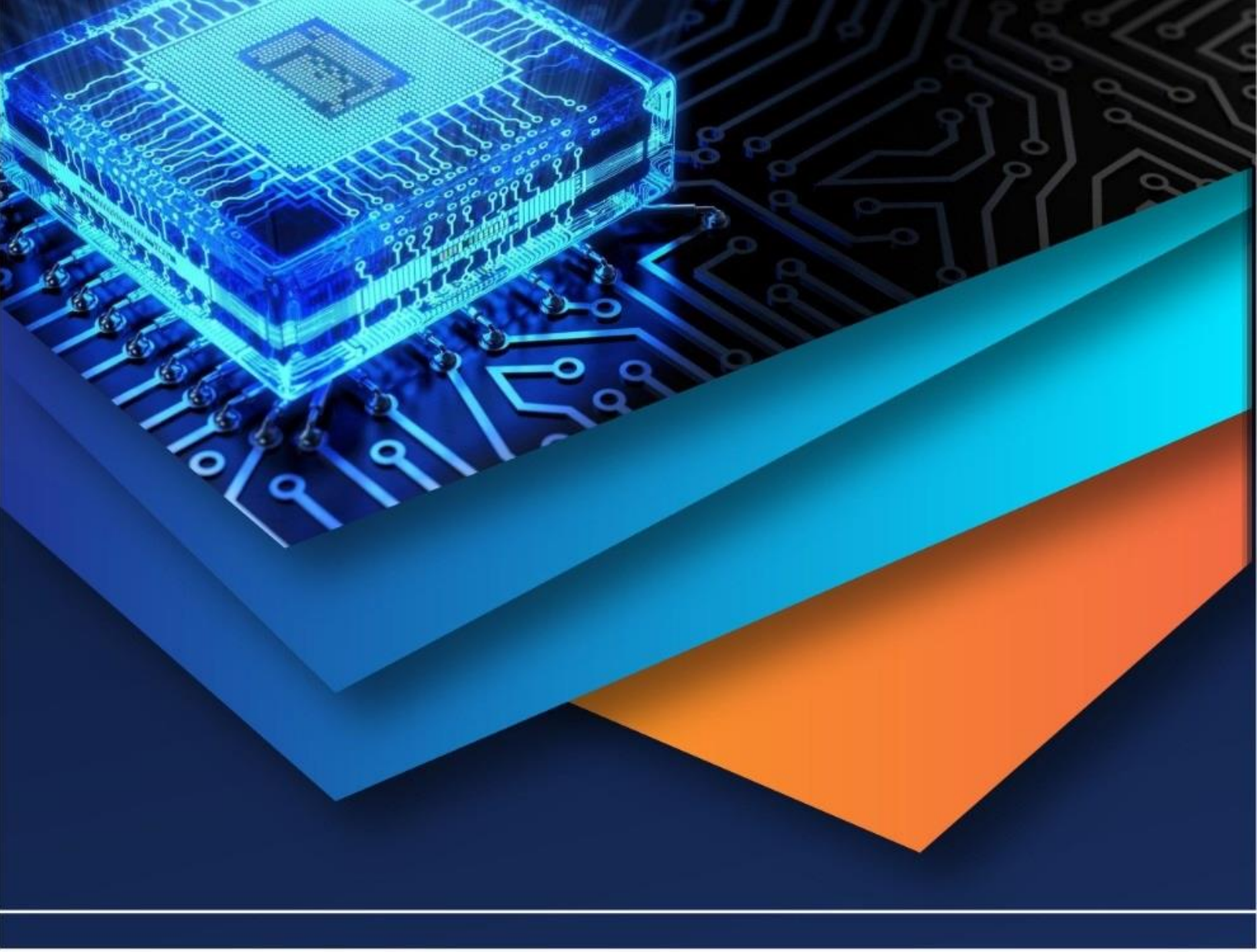
Towards the end of this paper the study has been done in light of identification and clarification of the structure of MPLS VPN layer 3 and examination of sending traffic with layer 3

Probably L3 MPLS VPNs apply well to remote access in a VPN scenarios, the configuration occur on CE, PE, and P routers to support MPLS L3 VPN functionalities.

The implementation of this paper was successfully done by using Graphical Network Simulation (GNS3) as a virtual lab with real cisco 7200 routers IOS images.

REFERENCES

[1] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, "Virtual private networks (VPN): A conceptual review of security protocols and their application in modern networks," Engineering Science & ..., 2024. fepbl.com
[2] H. Akter, S. Jahan, S. Saha, and R. H. Faisal, "Evaluating performances of VPN tunneling protocols based on application service requirements," in *Proceedings of the Third*, 2022. researchgate.net
[3] F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "Recent trends in MPLS networks: technologies, applications and challenges," IET, 2020. wiley.com
[4] M. Biabani, N. Yazdani, and H. Fotouhi, "Developing a Novel Hierarchical VPLS Architecture Using Q-in-Q Tunneling in Router and Switch Design," Computers, 2023. mdpi.com
[5] K. Gaur, A. Kalla, J. Grover, M. Borhani, and A. Gurtov, "A survey of virtual private LAN services (VPLS): Past, present and future," *Computer Networks*, Elsevier, 2021. sciencedirect.com
[6] S. Troia, F. Sapienza, and L. Varé, "On deep reinforcement learning for traffic engineering in SD-WAN," IEEE Journal on Selected Areas in Communications, 2020. polimi.it
[7] S. Kumaran, S. Prasad, and N. S. Kumar, "Implementation and performance analysis of traffic engineered multiprotocol label switching network for IPv6 clients," in Conference on Electronics, 2020. [HTML]
[8] OZ Mustapha, YF Hu, and R Sheriff, "Evaluation of bandwidth resource allocation using dynamic LSP and LDP in MPLS for wireless networks," Journal of Computing, 2020. researchgate.net
[9] R. A. A. P. Soepeno, "Comprehensive Network Analysis Through a Single Main Network Architecture," 2023. researchgate.net
[10] NQ Tran, KDL Nguyen, and CDT Thai, "Implementation and Evaluation of IPSec in an NFV-Based Network," in *International Conference on …*, Springer, 2023. [HTML]
[11] I. Siddique, "Comprehensive Network Architectures: Bridging Layer-2 Switching, Layer-3 Routing, and Emerging Digital Systems," 2020. ssrn.com
[12] E. S. Hassan, A. E. A. Abdelaal, A. S. Oshaba, and A. El-Emary, "Exploring Complex MPLS VPN Applications: Models and Implementations for Modern Communication Demands," 2023. researchsquare.com
[13] C. R. Komala, M. Hema, and H. R. Goyal, "Performance Evaluation of VPNS over MPLS-Linux Networks," in … on Advances in …, 2023. [HTML]
[14] J. C. Mwape, "Performance evaluation of internet protocol security (IPSec) over multiprotocol label switching (MPLS).," 2024. dspace.unza.zm
[15] J. Jasmine and N. Yuvaraj, "DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network," in Information Technology, 2022. researchgate.net
[16] S. T. Aung and T. Thein, "Comparative analysis of site-to-site layer 2 virtual private networks," in 2020 IEEE Conference on Computer, 2020. meral.edu.mm



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY