Exploring Complex MPLS VPN Applications: Models and Implementations for Modern Communication Demands

A.S. Fayed[a,*], Emad S. Hassan[b], Ehab S. Ali[b], Ayman E. A. Abdelaal[c], Moawad I. Dessouky[c], and Fathi E. Abd El-Samie[c]

[a] *Department of Mechanical Engineering, College of Engineering and Computer Science, Jazan University, Jizan 45142, Saudi Arabia.*
[b] *Department of Electrical and Electronics Engineering, College of Engineering and Computer Science, Jazan University, Jizan 45142, Saudi Arabia.*
[c] *Department of Electronics and Electrical Communication, Faculty of Electronic Engineering, Menoufia University, 32952, Menouf, Egypt.*

[*] *Corresponding Author; E-mail: afayed@jazanu.edu.sa*

Abstract:
In the modern landscape, robust data communication is pivotal for businesses and lifestyles. This has led to intricate demands from enterprise customers for sophisticated communication solutions. As a response, MPLS (Multiprotocol Label Switching) technology is being leveraged to meet these complex connectivity needs. This paper undertakes a comprehensive exploration of intricate MPLS- Virtual Private Networks (VPN) applications. The study entails both in-depth analysis and practical application on an operational network to validate its efficacy. The research primarily delves into diverse models of complex Layer 3 VPNs over MPLS. It commences by elucidating the foundational concept of a simple VPN and subsequently navigates through various designs for deploying Layer-3 VPNs on MPLS networks. MPLS technology has expanded the horizons of VPN services, catering precisely to contemporary business and customer requirements. Beyond conventional peer-to-peer private communication, the technology facilitates sophisticated iterations like managed service VPNs and overlapping VPNs. This paper systematically navigates these intricacies, offering comprehensive insights into their mechanisms and operational feasibility.

Key words: *Multiprotocol Label Switching (MPLS) - VPN services - Modern Communication Demands - Layer-3.*

1. INTRODUCTION

Contemporary customers often express reservations about conventional Internet connectivity, primarily due to security concerns associated with potential risks to confidentiality and integrity in public network access. This apprehension has spurred the concept of Virtual Private Networks (VPNs),

which have emerged in various forms. VPNs leverage public infrastructures, such as the Internet, to establish private networks accessible solely to authorized parties, mirroring the attributes of local networks in accessibility, privacy, and management; Cheng and Zhou (2022), Aung and Thein (2020), Figueiredo and Subratie (2020). These VPNs fall into categories like Customer-Provisioned VPNs (CP-VPNs) and Provider-Provisioned VPNs (PP-VPNs), further subdivided into Layer-2 and Layer-3 VPNs; Guo et al. (2004), Houidi and Meulle (2010).

In the realm of service provider-operated converged networks catering to diverse customer traffic, issues arise, especially concerning time-sensitive data like voice and video, which may experience delivery challenges affecting their desired characteristics. To ensure Service Level Agreement (SLA) adherence, enhancing performance becomes imperative. This research presents an exhaustive survey of both straightforward and intricate applications of Multi-Protocol Label Switching (MPLS) VPNs, serving as the foundation for evaluating voice traffic in this study; Zubilevich et al. (2021), Ganapathy and Joshi (2023), Sahoo et al. (2021).

The VPN is to use a public infrastructure (like the Internet) to build a private network, which is only accessible by its owners and has the full characteristics of the local network in its accessibility, privacy and management. While using the VPNs in the context of converged networks owned by the service providers, which serve many customers with different types of traffic at the same time, some delay-sensitive traffic (like voice and video) may suffer and do not reach its destination with the required characteristics. Performance enhancement is always a need for guaranteeing the commitment of the SLA between the service providers and their customers Sahoo et al. (2021).

The growing reliance on MPLS VPNs for secure and efficient data transmission has become increasingly evident, especially in industries where data integrity and performance are paramount. In the finance sector, MPLS VPNs are essential for ensuring the secure transmission of sensitive financial transactions and customer data across geographically dispersed branches. Similarly, the healthcare industry depends on MPLS VPNs to maintain the confidentiality of patient records while enabling real-time communication between healthcare providers, which is crucial for timely medical interventions. Moreover, with the rise of remote work environments, companies are leveraging MPLS VPNs to create secure and reliable connections for remote employees, ensuring that critical business operations continue uninterrupted. This growing dependence on MPLS VPNs highlights their role in addressing the stringent security and performance requirements of these high-stakes environments, making them an indispensable component of modern network infrastructure; Ganapathy and Joshi (2023).

Communication based on Internet Protocol (IP) has become the dominant communication technique nowadays. Although the IP networks have many benefits, they are still subject to many challenges. In the modern networks and the expected next-generation networks, the IP infrastructure is expected to carry multiple kinds of traffic serving different end users' applications. Although IP communication reigns supreme, it faces ongoing challenges, especially in accommodating the diverse traffic requirements anticipated in modern and next-gen networks. These networks must adeptly manage an array of traffic types serving distinct end-user applications, each with unique characteristics and tolerance levels for disruption. For instance, voice traffic remains relatively constant, whereas video traffic tends to be bursty, differing not only in traffic nature but also in sensitivity to factors like Jitter. Non-real-time data transmissions are more forgiving of delay variations due to their tolerance for queuing. To enable a unified network catering to these diverse applications, performance enhancement techniques are vital to tailor treatment to each application's distinctive needs; Ganapathy and Joshi (2023), Zhang et al. (2022), Peoples et al. (2022).

This paper examines the utilization of MPLS VPNs for voice traffic transmission, evaluating various performance enhancement methods to optimize throughput, minimize delay, and reduce jitter. The intricate scenarios of MPLS VPN application are thoroughly expounded and practically

implemented on an operational network system to validate their efficacy. The study introduces diverse models of complex Layer 3 VPNs over an MPLS infrastructure. It commences with the foundational simple VPN model, elaborated in the initial section. Subsequently, the paper delves into distinct designs for Layer-3 VPNs over MPLS networks, providing insights into their implementation strategies. This paper ensures that the MPLS enabled the service of VPN to be introduced in new fashions which are complex and fit the sophisticated requirements of today's customers and business. In addition to the simple VPN which enables two or more sites to communicate privately over a public network in a peer-to-peer fashion, many other complex forms of VPN are now possible using the MPLS technology like the managed service VPN, overlapping VPN and others Joshi (2023).

2. CLASSIFICATION BASED ON LAYER

2.1. Layer-2 VPN

VPN categorization comprises Layer-2 VPNs and Layer-3 VPNs, aligned with the OSI Model's Seven Layers. Specifically, Layer-2 corresponds to the Data-Link layer, while Layer-3 pertains to the Network Layer; Saputra et al. (2021), Budiyanto and Gunawan (2023). In a Layer-2 VPN, the Service Provider's entire network is perceived by the customer as a Layer-2 Circuit/Switch. This arrangement precludes Layer-3 routing and header checks within the Service Provider's network. Consequently, the Provider's devices remain devoid of customer-specific IP interfaces. This design necessitates point-to-point IP addresses to be configured at both customer sites. For example, if one site employs the IP address 10.1.1.1/30, the other site should adopt the corresponding IP 10.1.1.2/30 from the same subnet; Darmawan et al. (2022).

Customer-Provisioned VPNs are inherently Layer-2 VPNs, wherein the Provider remains unaware of the VPN's creation. In terms of the VPN tunnel, the Provider functions akin to a Layer-2 switch. It's essential to distinguish between the two interfaces at each customer site. The tunnel interface signifies the VPN and presents a Layer-2 perspective, while the physical interface establishes IP peering with the Provider, potentially involving routing protocols, and assumes a Layer-3 connection. Clarifying this hinge on comprehending the tunnel interface's standpoint.

2.2. Layer-3 VPN

The Layer-3 VPN entails active involvement of the Service Provider in the routing process alongside the customer. This involves configuring a Layer-3 interface with an IP address within the Service Provider's network that corresponds to the customer's private network. For instance, if the customer's WAN interface employs the IP address 172.16.1.1/30, the Provider's device facing that peer site configures the IP address 172.16.1.2/30 within the same VPN. Moreover, a distinct subnet is designated for the point-to-point connection between the Provider and the other peer site. For example, the subnet 172.16.7.1/30 and 172.16.7.2/30 might be allocated for this purpose; Yautibug et al. (2021), Pazienza et al. (2022).

In the pre-MPLS era, implementing Layer-3 VPNs was notably intricate. It necessitated a dedicated router for each customer on every Point of Presence (POP) of the provider, a management-intensive and expensive undertaking. The advent of MPLS revolutionized Layer-3 VPN deployment, rendering it more feasible.

2.3. MPLS – VPN

The core concept of MPLS-VPN revolves around the capability to allocate multiple labels (or a label stack) to a single packet. The outer label serves as the transport label, overseeing the packet's conveyance to its intended endpoint. As the packet progresses to the next Label Switching Router (LSR), this outer label is assessed and potentially replaced or removed to facilitate the packet's journey to its ultimate destination. An essential quandary arises: how does the ultimate destination router process this incoming data? This is contingent upon the presence of an additional label, known as the inner label. In its absence, the data advances to the routing engine, where its Layer 3 attributes (IP address) are evaluated, culminating in the definitive decision concerning its ultimate target; Sllame (2022), Gupron et al. (2022), Yan et al. (2022), Gales and Croitoru (2020).

Conversely, if an additional label is present, it serves as a determinant for the associated VPN type (Layer-2 or Layer-3). Consider a Layer-3 VPN scenario: the router scrutinizes the IP destination within the traffic and endeavors to discover a corresponding entry within the Virtual Routing and Forwarding (VRF) table. This specialized table corresponds to the specific VPN, assisting the router in shaping routing determinations for the incoming data.

3. APPLICATIONS OF MPLS LAYER-3 VPN

The conducted experiments were carried out on a Samsung Laptop equipped with an Intel Core i3 processor and 12 GB of RAM. The emulation utilized the renowned GNS3 emulator, which boasts exceptional capabilities for simulating environments of various vendors such as Cisco and Juniper. Cisco routers were emulated through the use of the IOU (IOS over Unix) software. In the provided topology, individual customer routers (labeled as 'x') each possess a corresponding Loopback IP address that corresponds to the router's number. For instance, for router 1, the Loopback address is set as 1.1.1.1, and for router 2, the Loopback address is configured as 2.2.2.2, and so forth.

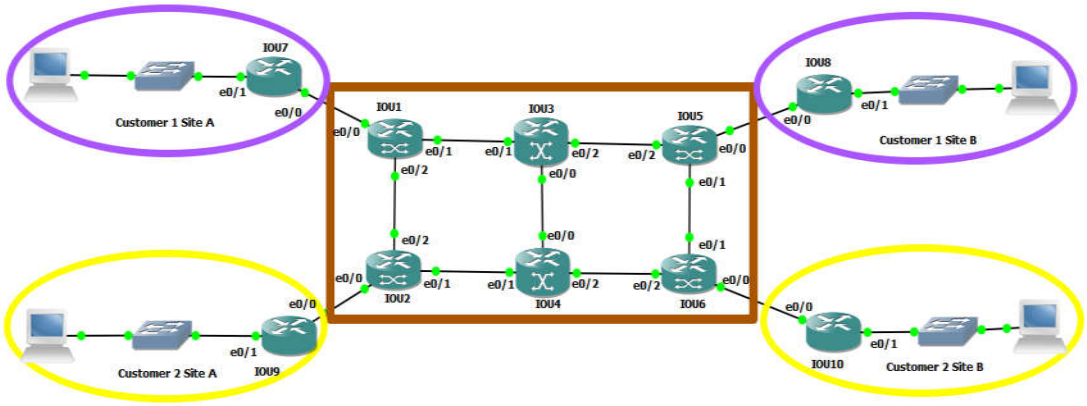

Figure 1. Simple VPN Topology Zaidoun (2022).

3.1. Simple VPN

Figure 1 presents the outlined requisites for the Simple VPN Topology; Zaidoun (2022). The diagram depicts a scenario with two distinct customers, labeled as 1 and 2, each encompassing two sites designated as A and B. The fundamental premise of the simple VPN is to establish communication exclusively between sites within the same VPN, while precluding interaction with any other sites. This traffic flow is explicated in Figure 2, which illustrates the allowed and restricted directions of communication. Achieving this necessitates the allocation of route targets, as visualized in Figure 3. Configuration details regarding the Route-Target assignment across various nodes of the topology are showcased in Figure 4. The ensuing outcomes are outlined in figures 5 (a, b, c, d), where a conspicuous alignment between the theory and the routing tables of customer routers is evident.

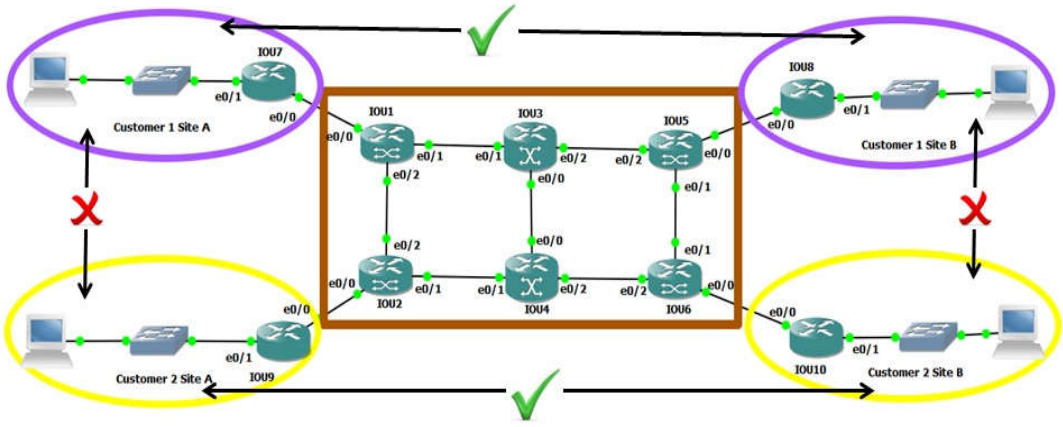

Figure 2. Traffic Flow Direction in Simple VPN.

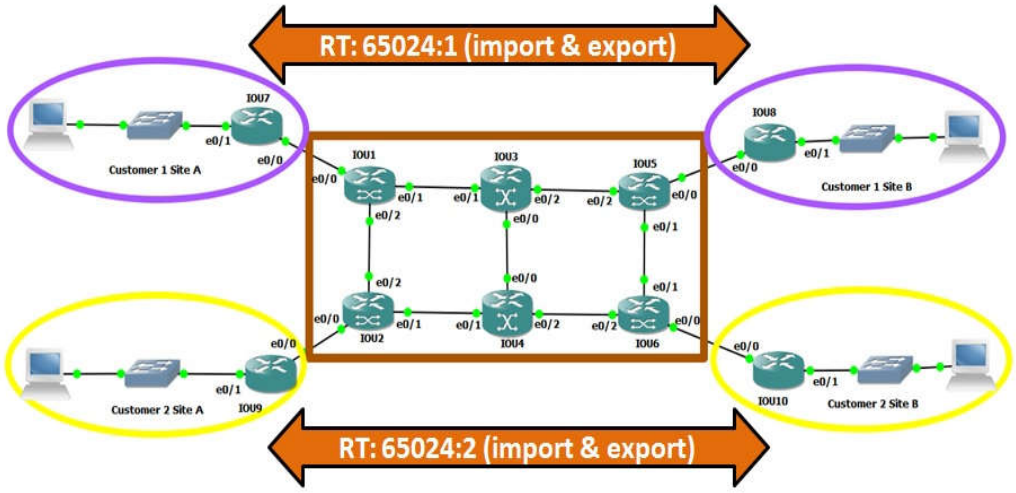

Figure 3. Route-Target assignment for the Simple VPN.

```
R1#sh run | s ip vrf ABC
ip vrf ABC
 rd 65024:1
 route-target export 65024:1
 route-target import 65024:1
R1#
```

```
R2#show run | s ip vrf XYZ
ip vrf XYZ
 rd 65024:2
 route-target export 65024:2
 route-target import 65024:2
R2#
```

```
R5#show run | s ip vrf ABC
ip vrf ABC
 rd 65024:1
 route-target export 65024:1
 route-target import 65024:1
R5#
```

```
R6#show run | s ip vrf XYZ
ip vrf XYZ
 rd 65024:2
 route-target export 65024:2
 route-target import 65024:2
R6#
```

Figure 4. Route target assignment on the network nodes.

```
R7#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.1.7.0/24 is directly connected, Ethernet0/0
L        10.1.7.7/32 is directly connected, Ethernet0/0
C        10.7.7.0/24 is directly connected, Ethernet0/1
L        10.7.7.7/32 is directly connected, Ethernet0/1
B        10.8.8.0/24 [20/0] via 10.1.7.1, 00:04:13
R7#
```

Figure 5. a) Routing table of Router 7 for Simple VPN.

```
R8#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.5.8.0/24 is directly connected, Ethernet0/0
L        10.5.8.8/32 is directly connected, Ethernet0/0
B        10.7.7.0/24 [20/0] via 10.5.8.5, 00:03:28
C        10.8.8.0/24 is directly connected, Ethernet0/1
L        10.8.8.8/32 is directly connected, Ethernet0/1
R8#
```

Figure 5. b) Routing table of Router 8 for Simple VPN.

```
R9#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.2.9.0/24 is directly connected, Ethernet0/0
L        10.2.9.9/32 is directly connected, Ethernet0/0
C        10.9.9.0/24 is directly connected, Ethernet0/1
L        10.9.9.9/32 is directly connected, Ethernet0/1
B        10.10.10.0/24 [20/0] via 10.2.9.2, 00:00:30
R9#
```

Figure 5. c) Routing table of Router 9 for Simple VPN.

```
R10#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.6.10.0/24 is directly connected, Ethernet0/0
L        10.6.10.10/32 is directly connected, Ethernet0/0
B        10.9.9.0/24 [20/0] via 10.6.10.6, 00:00:01
C        10.10.10.0/24 is directly connected, Ethernet0/1
L        10.10.10.10/32 is directly connected, Ethernet0/1
R10#
```

Figure 5. d) Routing table of Router 10 for Simple VPN.

3.2. Overlapping VPN

In the overlapping scenario, every customer features a Headquarters (HQ) site that interacts exclusively with the branches within its own VPN; Sarsembagieva et al. (2012). However, the HQ site needs to communicate solely with the counterpart HQ of the other customer, excluding the branches of that customer. The experimental topology is presented in Figure 6. While the route target configuration remains unaltered for PEs interfacing with regular branch sites, modifications are implemented solely for PEs connected to the HQ sites, represented by R3 and R4. The route-target assignment is elucidated

in Figure 7, offering insight into the topology's configuration adjustments. These changes are visually detailed in Figure 8, encapsulating the configuration adaptations for both R3 and R4.

The anticipated outcome revolves around observing that the routing table of each branch exclusively contains routes from its own branches and the HQ within the same customer. For instance, in the case of Customer 1 Branch A, denoted as R7, we expect to find routes from Customer 1 Branch B and Customer 1 HQ, specifically 10.8.8.0/24 and 10.15.15.0/24, respectively. This pattern extends across the other branches and their corresponding HQs.

Additionally, we foresee the HQ routers of each customer encompassing routes from their own branches alongside the route linked to the counterpart HQ. For example, Customer 2 HQ router (R16) should include routes from Customer 2 Branch A, Customer 2 Branch B, and Customer 1 HQ, which are 10.9.9.0/24, 10.10.10.0/24, and 10.15.15.15.0/24 respectively. Figures 9 (a, b, c, d, e, f) provide a visual depiction of the BGP table for all customer routers. Notably, on HQ routers 15 and 16, certain routes only bear the AS of the provider, indicative of routes stemming from the same VPN of the respective customer. Meanwhile, routes marked with an unfamiliar AS (100 or 200) signify routes originating from the HQ of the other customer. The following paragraphs summarize each figure in Fig. 9 and its connection to the test topology.

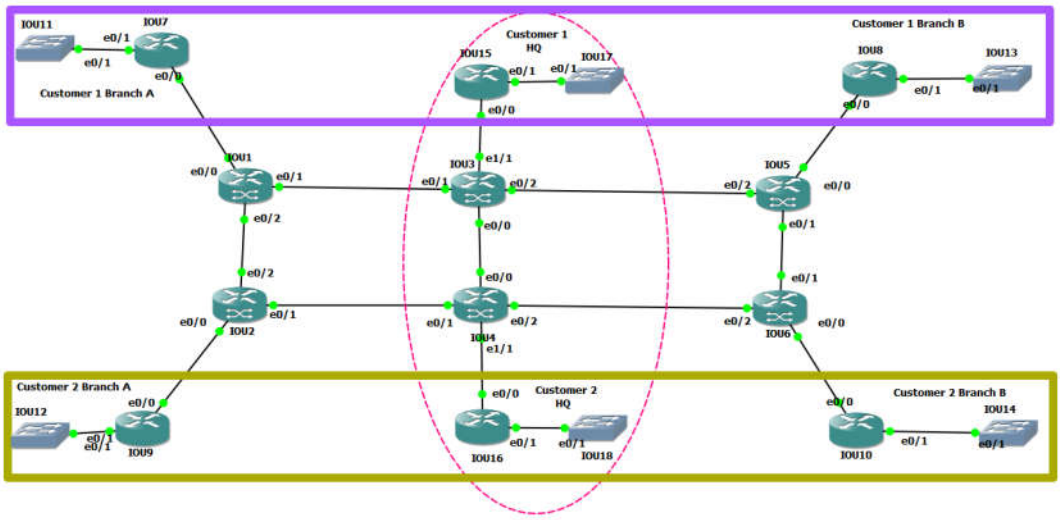

Figure 6. Overlapping VPN Topology.

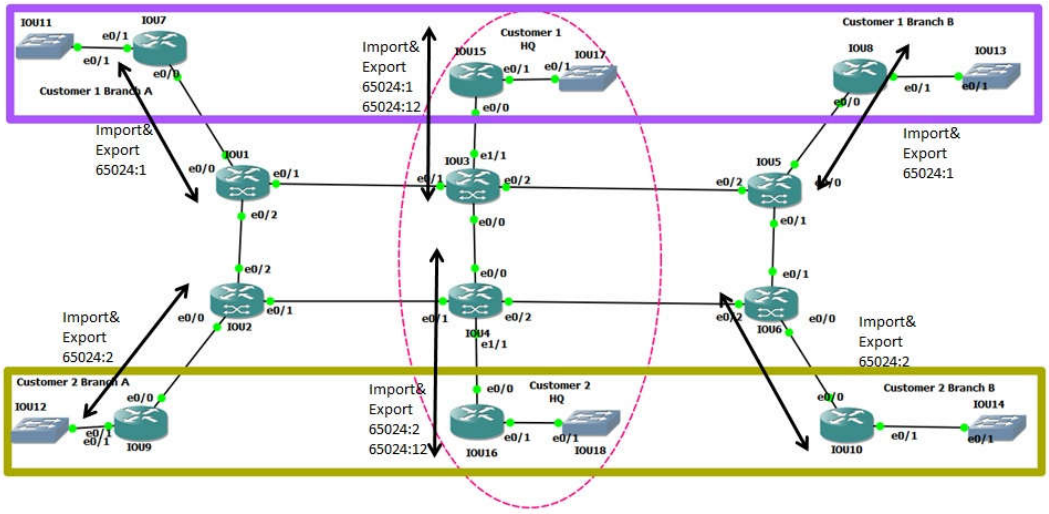

Figure 7. Route Target assignment on Topology.

```
R3#show run | s ip vrf ABC-HQ
ip vrf ABC-HQ
 rd 65024:11
 route-target export 65024:1
 route-target export 65024:12
 route-target import 65024:1
 route-target import 65024:12
R3#
```

```
R4#show run | s ip vrf XYZ-HQ
ip vrf XYZ-HQ
 rd 65024:22
 route-target export 65024:2
 route-target export 65024:12
 route-target import 65024:2
 route-target import 65024:12
R4#
```

Figure 8. RT assignment on PEs facing HQs for Overlapping VPN

```
R7#sh ip bgp
BGP table version is 4, local router ID is 10.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.7.7.0/24     0.0.0.0                  0         32768 i
 *>  10.8.8.0/24     10.1.7.1                               0 65024 65024 i
 *>  10.15.15.0/24   10.1.7.1                               0 65024 65024 i
R7#
```

Figure 9. a) BGP table of R7 for Overlapping VPN.

```
R8#sh ip bgp
BGP table version is 4, local router ID is 10.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.7.7.0/24      10.5.8.5                               0 65024 65024 i
 *>  10.8.8.0/24      0.0.0.0                  0         32768 i
 *>  10.15.15.0/24    10.5.8.5                               0 65024 65024 i
R8#
```

Figure 9. b) BGP table of R8 for Overlapping VPN.

```
R9#show ip bgp
BGP table version is 4, local router ID is 10.9.9.9
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.9.9.0/24      0.0.0.0                  0         32768 i
 *>  10.10.10.0/24    10.2.9.2                               0 65024 65024 i
 *>  10.16.16.0/24    10.2.9.2                               0 65024 65024 i
R9#
```

Figure 9. c) BGP table of R9 for Overlapping VPN.

```
R10#show ip bgp
BGP table version is 4, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.9.9.0/24      10.6.10.6                              0 65024 65024 i
 *>  10.10.10.0/24    0.0.0.0                  0         32768 i
 *>  10.16.16.0/24    10.6.10.6                              0 65024 65024 i
R10#
```

Figure 9. d) BGP table of R10 for Overlapping VPN.

```
R15#show ip bgp
BGP table version is 6, local router ID is 10.15.15.15
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.7.7.0/24      10.3.15.3                              0 65024 65024 i
 *>  10.8.8.0/24      10.3.15.3                              0 65024 65024 i
 *>  10.15.15.0/24    0.0.0.0                  0         32768 i
 *>  10.16.16.0/24    10.3.15.3                              0 65024 200 i
R15#
```

Figure 9. e) BGP table of R15 for Overlapping VPN.

```
R16#show ip bgp
BGP table version is 6, local router ID is 10.18.18.18
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.9.9.0/24      10.4.16.4                              0 65024 65024 i
 *>  10.10.10.0/24    10.4.16.4                              0 65024 65024 i
 *>  10.15.15.0/24    10.4.16.4                              0 65024 100 i
 *>  10.16.16.0/24    0.0.0.0                  0         32768 i
R16#
```

Figure 9. f) BGP table of R16 for Overlapping VPN.

Figure 9 (a) presents the BGP table of R7, representing customer 1's branch A router within the overlapping VPN scenario. The table reflects the expected routes, including those from customer 1's branch B and HQ, demonstrating the correct implementation of the route-target configurations. This confirms that R7 is correctly isolated from customer 2's routes while maintaining connectivity with its designated VPN peers. Figure 9 (b) shows the BGP table of R8, which is customer 1's branch B router. Similar to R7, R8's table lists routes only from its corresponding VPN, specifically customer 1's branch A and HQ. The absence of routes from customer 2 confirms that the overlapping VPN configuration is functioning as intended, with proper isolation between customer networks. In Figure 9 (c), the BGP table of R9, representing customer 2's branch A router, is depicted. The routes present in this table are exclusively from customer 2's branch B and HQ, affirming that the VPN is correctly configured. This figure illustrates the effective isolation of customer 1's network from customer 2's, adhering to the overlapping VPN design. Figure 9 (d) presents the BGP table of R10, customer 2's branch B router. The table lists routes from customer 2's branch A and HQ, mirroring the configuration seen in R9. The consistency across these routers ensures that the overlapping VPN design is robust and correctly implemented. While Figure 9 (e) illustrates the BGP table of R15, which functions as the HQ router for customer 1. The table includes routes from customer 1's branch A and branch B, as well as a route from customer 2's HQ. This confirms that while the HQs of both customers can communicate with each other, their branch routers remain isolated, maintaining the integrity of the overlapping VPN structure. Finally, Figure 9 (f) shows the BGP table of R16, customer 2's HQ router. Similar to R15, R16's table contains routes from its own branches and the HQ of customer 1. This further validates the overlapping VPN setup, where HQ routers communicate across customers while preserving branch isolation. Figure 10 shows the traffic flow on the Overlapping VPN.

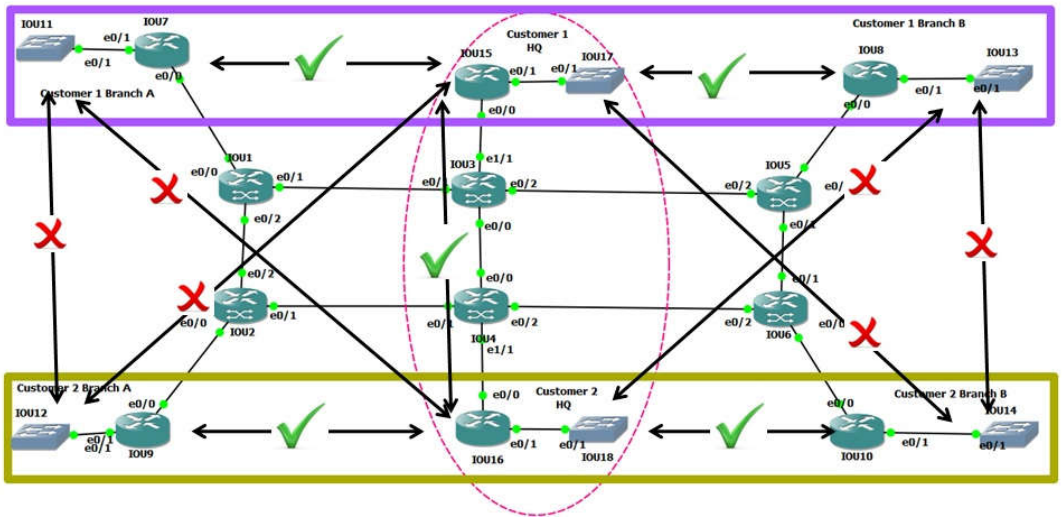

Figure 10. Traffic Flow for Overlapping VPN

3.3. Central Service VPNs

The Central Services VPN concept involves establishing multiple distinct simple VPNs. Each of these simple VPNs may comprise numerous sites, coexisting alongside a centralized VPN accessible to all the aforementioned simple VPNs; Rossberg et al. (2013). Importantly, these simple VPNs remain isolated from one another. This arrangement proves particularly useful when the provider maintains a server farm, offering services to its customers through these servers over pre-existing VPN connections. The experimental setup employs a topology depicted in Figure 11. To implement this, route targets are allocated, as depicted in Figure 12, and subsequently configured, as outlined in Figure 13.

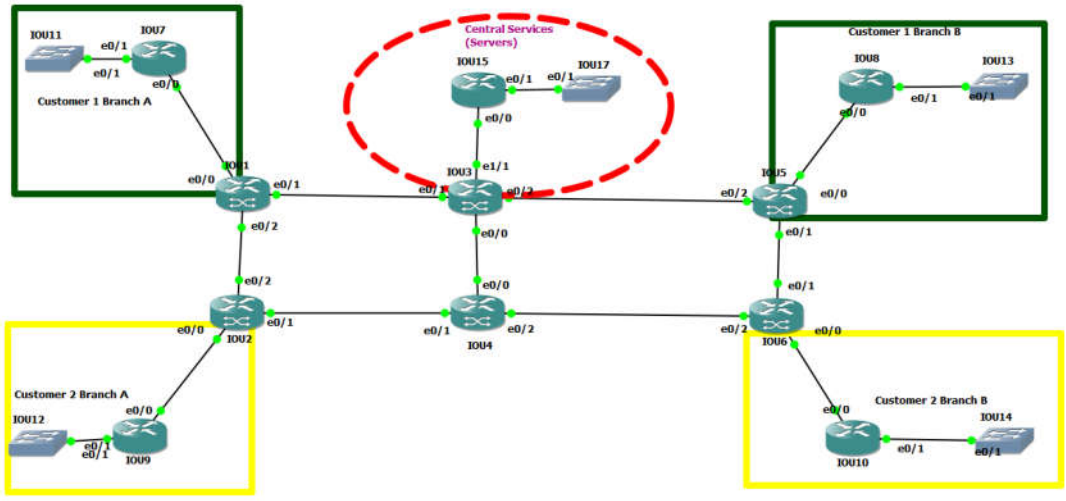

Figure 11. Centralized Services VPN Topology

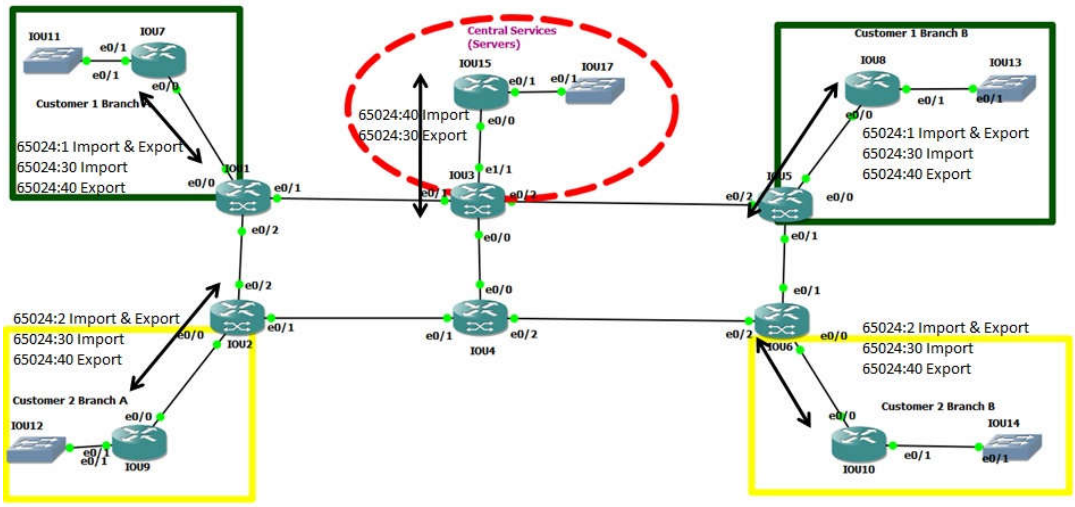

Figure 12. RT assignment on the topology for Centralized Services VPN.

In the preceding scenario, the anticipated outcome involves the presence of routes for all branches' LANs across all customers in the routing table of router 15. Similarly, the LAN associated with the centralized service, denoted as 10.15.15.15.0, is expected to be present in the routing tables of all customer routers. Conversely, no routes pertaining to customer 1 should be present on any router within customer 2. Figures 14 (a, b, c, d, e) visually portray the BGP table for all customer routers, alongside the centralized services router. Upon scrutiny, the centralized services router reveals the coexistence of all LANs, complete with the accurate AS numbers corresponding to the respective customers.

Figure 14 (a) presents the BGP table of Router 7, representing Customer 1's Branch A router in the Centralized Services VPN scenario. The table shows routes from both Customer 1's Branch B and the centralized service. The presence of these routes confirms that Router 7 is correctly receiving routes from its own customer network and the centralized service, while remaining isolated from Customer 2's routes, as intended. Figure 14 (b) displays the BGP table of Router 8, which is Customer 1's Branch B router. Similar to Router 7, the table includes routes from Customer 1's Branch A and the centralized service. This indicates that Router 8 is correctly configured to communicate with the centralized service while maintaining isolation from other customer networks. The BGP table of Router 9, representing Customer 2's Branch A router, is depicted in Figure 14 (c). The routes present in this table include those from Customer 2's Branch B and the centralized service. This demonstrates that Router 9 is correctly integrated into the Centralized Services VPN, receiving only the necessary routes from its own network and the centralized service. Figure 14 (d) presents the BGP table of Router 10, which is Customer 2's Branch B router. The table lists routes from Customer 2's Branch A and the centralized service, mirroring the configuration of Router 9. This ensures that Router 10 is also correctly participating in the Centralized Services VPN. Figure 14 (e) presents the BGP table of Router 10, which is Customer 2's Branch B router. The table lists routes from Customer 2's Branch A and the centralized service, mirroring the configuration of Router 9. This ensures that Router 10 is also correctly participating in the Centralized Services VPN.

Figure 13. RT assignment on configuration for Centralized Services VPN.

3.4. Hybrid VPN configurations

3.4.1 Synthesizing overlapping and centralized services

Various implementation scenarios emerge by amalgamating the distinctive attributes of the preceding complex types. An instance of this integration occurs when solely the HQ sites within the customers' VPNs necessitate communication with the centralized service VPN.

3.4.2 Managed CE VPN

This configuration can be regarded as an offshoot of the centralized services model. Here, the emphasis lies on managing the loopbacks of the Customer Edge (CE) routers, introducing the service of overseeing customer routers through a centralized Network Management System (NMS). This can be executed by means of selective import and export policies. These policies designate the Loopback of the CE routers to be exported with a designated Route Target, which is subsequently imported onto the centralized service router.

```
R7#show ip bgp
BGP table version is 6, local router ID is 10.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.7.7.0/24      0.0.0.0                  0         32768 i
 *>  10.8.8.0/24      10.1.7.1                               0 65024 65024 i
 *>  10.15.15.0/24    10.1.7.1                               0 65024 65100 i
R7#
```

Figure 14. a) BGP table of router 7 for Centralized Services VPN.

```
R8#show ip bgp
BGP table version is 6, local router ID is 10.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.7.7.0/24      10.5.8.5                               0 65024 65024 i
 *>  10.8.8.0/24      0.0.0.0                  0         32768 i
 *>  10.15.15.0/24    10.5.8.5                               0 65024 65100 i
R8#
```

Figure 14. b) BGP table of router 8 for Centralized Services VPN.

```
R9#show ip bgp
BGP table version is 4, local router ID is 10.9.9.9
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.9.9.0/24      0.0.0.0                  0         32768 i
 *>  10.10.10.0/24    10.2.9.2                               0 65024 65024 i
 *>  10.15.15.0/24    10.2.9.2                               0 65024 65100 i
R9#
```

Figure 14. c) BGP table of router 9 for Centralized Services VPN.

```
R10#show ip bgp
BGP table version is 4, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.9.9.0/24      10.6.10.6                              0 65024 65024 i
 *>  10.10.10.0/24    0.0.0.0                  0         32768 i
 *>  10.15.15.0/24    10.6.10.6                              0 65024 65100 i
R10#
```

Figure 14. d) BGP table of router 10 for Centralized Services VPN.

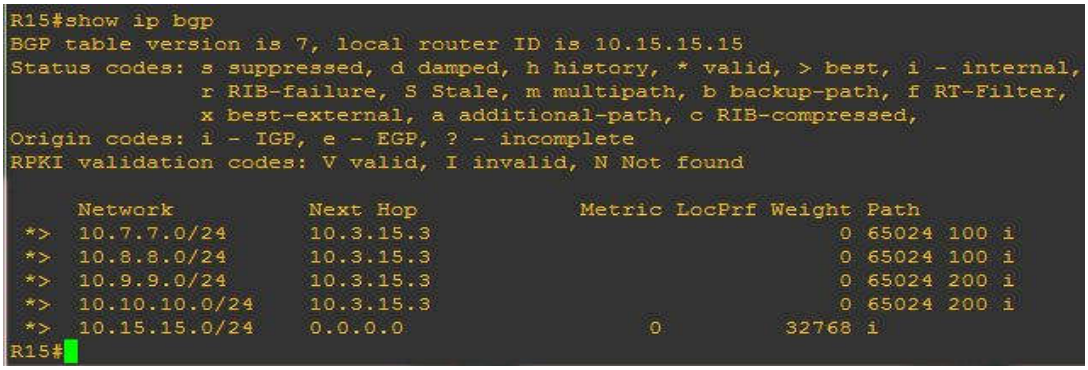

Figure 14. e) BGP table of router 15 for Centralized Services VPN.

3.5. Recommendations, Challenges, and Limitations

3.5.1 Recommendations

Based on the research findings, several recommendations can be made to enhance the implementation and performance of MPLS VPNs:

1. Optimization of Route Targets: Careful planning and assignment of route targets are essential to ensure proper traffic isolation and communication between VPNs, particularly in complex scenarios like overlapping VPNs and centralized services VPNs. Regular audits of route target configurations can help prevent misconfigurations.
2. Scalability Considerations: For networks expected to grow, it's crucial to design the VPN architecture with scalability in mind. Using hierarchical VPN structures can help manage growth without significant reconfiguration.
3. Performance Tuning: Continuous monitoring and performance tuning, especially in delay-sensitive traffic like voice and video, can significantly improve service quality. Techniques such as traffic engineering and QoS policies should be employed to maintain service level agreements (SLAs).

3.5. 2 Challenges Encountered

During the study, several challenges were identified:

1. Complexity in Configuration: The configuration of MPLS VPNs, especially in scenarios involving overlapping and centralized services, proved to be intricate and error-prone. Addressing this required thorough planning, detailed documentation, and frequent validation of configuration changes.
2. Resource Limitations: The emulation environment had limited resources, which occasionally resulted in performance bottlenecks during tests. This was mitigated by optimizing the use of available resources and by carefully scheduling tests to avoid resource contention.
3. Troubleshooting Difficulties: Troubleshooting MPLS VPN issues, particularly when dealing with multiple overlapping and centralized VPNs, was challenging. The complexity of the topology often required extensive use of debugging tools and methods to isolate and resolve issues.

3.5. 3 Limitations and Drawbacks

While the implemented approach demonstrated the viability of complex MPLS VPN configurations, several limitations were noted:

1. Simulation Environment Constraints: The study was conducted in a simulated environment using GNS3, which may not fully capture the nuances of a live network. Therefore, the results, while indicative, may differ in a production environment.
2. Scalability Concerns: Although the configurations tested worked well within the study's scope, scaling the architecture to a larger network might introduce unforeseen challenges, particularly in terms of performance and management overhead.
3. Cost Implications: Implementing MPLS VPNs, especially with complex configurations, can be cost-intensive in terms of both hardware and the expertise required. Organizations need to carefully weigh the benefits against the associated costs.

4. CONCLUSION

Our exploration into complex MPLS VPN applications highlights their pivotal role in addressing contemporary business and communication needs. The study delves deeply into Layer 3 MPLS VPNs, dissecting their intricacies and implementations to cater to diverse demands. Through meticulous experimentation, we analyze scenarios involving overlapping VPNs, centralized services, and managed CE VPNs, showcasing their adaptability in dynamic networking environments. The study's insights hold significance as businesses navigate evolving communication landscapes. The seamless integration of VPNs, optimized performance enhancements, and precise route-target assignments form a robust networking foundation, catering to multifaceted demands. This research underscores MPLS VPNs' versatility in accommodating intricate communication scenarios, ensuring secure data exchange, and facilitating tailored information flow. Ultimately, the study showcases MPLS technology's efficacy, offering insights that guide businesses in constructing resilient, customized networking solutions in today's digital era.

Future research could expand on this study by exploring the use of video data within MPLS VPN environments. Video traffic, known for its high bandwidth requirements and sensitivity to delay and jitter, presents unique challenges that differ from those encountered with voice and standard data traffic. Investigating how MPLS VPNs handle video streams, particularly in complex scenarios like overlapping and centralized services VPNs, could provide valuable insights into optimizing network performance. Specific research questions to explore include: How does video data affect the overall performance of an MPLS VPN? What impact do different QoS policies have on the quality of video transmission? Additionally, testing various traffic engineering techniques to manage video data could uncover strategies to enhance video delivery, ensuring that it meets the stringent quality demands of modern applications.

References

Aung, S. T., Thein, T., 2020. Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks, *IEEE Conference on Computer Applications (ICCA)*, Yangon, Myanmar, p. 1.

Budiyanto, S., Gunawan, D., 2023. Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol, in *IEEE Access*, 11, p. 60853.

Cheng, T., Zhou, F., 2022. 5G Virtual Private Network Planning Methodology Analysis, *14th International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, p. 1.

Darmawan, E., Budiyanto, S., Silalahi, L. M., 2022. QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method, *IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Solo, Indonesia, p. 130.

Figueiredo, R., Subratie, K., 2020. Demo: EdgeVPN.io: Open-source Virtual Private Network for Seamless Edge Computing with Kubernetes, *IEEE/ACM Symposium on Edge Computing (SEC)*, San Jose, CA, USA, p. 190.

Gales, E. M., Croitoru, V., 2020. Traffic Engineering and QoS in a Proposed MPLS-VPN, *International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, Romania, p. 1.

Ganapathy, D. N., Joshi, K. P., 2023. A Semantically Rich Framework to Automate Cloud Service Level Agreements, in *IEEE Transactions on Services Computing*, vol. 16, no. 1, p. 53.

Guo, K., Mukherjee, S., Paul, S., Rangarajan, S., 2004. Optimal customer provisioning in network-based mobile VPNs, *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004.*, Boston, MA, USA, p. 95.

Gupron, M. Y., Umaisaroh, U., Wicaksono, A., 2022. Network Automation for CE Router with Route Leaking in MPLS-VPN Network, *International Symposium on Information Technology and Digital Innovation (ISITDI)*, Padang, Indonesia, p. 162.

Houidi, Z. B., Meulle, M., 2010. A new VPN routing approach for large scale networks, *The 18th IEEE International Conference on Network Protocols*, Kyoto, Japan, p. 124.

Pazienza, A., Lella, E., Noviello, P., Vitulano, F., 2022. Analysis of Network-level Key Exchange Protocols in the Post-Quantum Era, *IEEE 15th Workshop on Low Temperature Electronics (WOLTE)*, Matera, Italy, p. 1.

Peoples, C., Moore, A., Georgalas, N., 2022. Customer Classification Recommender to Support Personalised Service Level Agreements Across the Internet of Things, *IEEE 8th World Forum on Internet of Things (WF-IoT)*, Yokohama, Japan, p. 1.

Rossberg, M., Grey, M., Trapp, M., Girlich, F., Schaefer, G., 2013. Distributed monitoring of self-configuring Virtual Private Networks, *IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, Ghent, Belgium, p. 1080.

Sahoo, S., Bigo, S., Benzaoui, N., 2021. Introducing Best-in-Class Service Level Agreement for Time-Sensitive Edge Computing, *European Conference on Optical Communication (ECOC)*, Bordeaux, France, p. 1.

Saputra, B. G. A., Nugroho, K., Ikhwan, S., 2021. Implementation of Layer 2 MPLS VPN on the SDN Hybrid Network using Ansible and ONOS Controllers, *IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Purwokerto, Indonesia, p. 27.

Sarsembagieva, K., Gardikis, G., Xilouris, G., Kourtis, A., 2012. A fast route planning algorithm for MPLS-TE, *International Conference on Telecommunications and Multimedia (TEMU)*, Heraklion, Greece, p. 142.

Sllame, A. M., 2022. Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks, *IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, Sabratha, Libya, p. 32.

Yan, T., Wu, W., Li, L., Xie, W., 2022. Configuration method of cross-domain MPLS VPN based on double MCE, *6th International Conference on Wireless Communications and Applications (ICWCAPP)*, Haikou, China, p. 106.

Yautibug Coro, A. L., Avila-Pesantez, D., Arellano-Aucancela, A., 2021. Evaluation of 6PE and 6VPE techniques in MPLS-VPN networks for video streaming, *IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*, Soyapango, El Salvador, p. 1.

Zaidoun, A. S., 2022. Techniques and Tools for Encryption, IPSec and VPN, in *Computer Science Security: Concepts and Tools*, Wiley, p. 109.

Zhang, H., Pan, G., Xu, S., Zhang, S., Jiang, Z., 2022. A Hard and Soft Hybrid Slicing Framework for Service Level Agreement Guarantee via Deep Reinforcement Learning, *IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Helsinki, Finland, p. 1.

Zubilevich, A. L., Sidney, S. A., Tsarenko, V. A., 2021. The Effect of the Use of Service Level Agreement for Operators of Transport Systems and On-Board Systems, *Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, p. 1.