Far East Journal of Electronics and Communications

http://www.pphmj.com
http://dx.doi.org/10.17654/0973700623002
Volume 27, 2023, Pages 13-40 **P-ISSN: 0973-7006**

A SURVEY ON INTRADOMAIN AND INTERDOMAIN ROUTING IN TRADITIONAL IP AND MPLS BASED VPN ENVIRONMENTS

V. Naren Thiruvalar and T. L. Kayathri

Department of EEE
Anna University Regional Campus
Coimbatore, India
e-mail: narenthirupsg@gmail.com

Department of ECE
Anna University Regional Campus
Coimbatore, India
e-mail: kayathrithanggam@gmail.com

Abstract

This survey describes how securely the information is shared between various provider edge (PE) and customer edge (CE) services. For sharing that information securely, the user needs a secure routing environment. Further, this paper discusses and compares various intradomain and interdomain routing techniques in traditional internet

Received: July 26, 2023; Accepted: September 7, 2023

Keywords and phrases: MPLS-VPN, multi-VRF, VoIP, IPsec.

How to cite this article: V. Naren Thiruvalar and T. L. Kayathri, A survey on intradomain and interdomain routing in traditional IP and MPLS based VPN environments, Far East Journal of Electronics and Communications 27 (2023), 13-40.

http://dx.doi.org/10.17654/0973700623002

Published Online: September 20, 2023

protocol (IP) and multi-protocol label switching (MPLS) based VPN environments through the comparison table and graphical representations.

1. Introduction

For a piece of information that needs to be transferred from source to destination, a proper routing has to occur. Routing acts as a transmission medium between routers to share information about network topology, the status of the network, maintenance, and availability of the network and allows the router to maintain and update the routing table information between them. The major classification of routing is intradomain routing and interdomain routing. In intradomain routing, the information has been shared only within the particular autonomous system (between the group of routers and networks under the control of one entity). It ignores the internet outside the domain. Since the routing has to interact only within a particular autonomous system, the information about the different components presented in a network within a particular domain is required. The most important protocol used in intradomain routing is interior gateway protocol (IGP), which is further classified into distance vector and link state. The most popular example for distance vector is routing information protocol (RIP) whereas, as for link-state, the important example is open shortest path first (OSPF). On the other hand, in interdomain routing, the routing algorithm works within the domain and also between the autonomous systems. Since the data is shared between two autonomous systems, the entire domain must know the different components present in the network. The most important interdomain routing is the exterior gateway protocol (EGP). A popular example of this is the border gateway protocol (BGP), which is used to connect two or more autonomous systems with the help of an MPLS based VPN environment.

In traditional IP networks, clients like to involve BGP as a provider edge – customer edge sites when moving from traditional IP to MPLS-VPN based environment. This assists the clients to build a consistent end-to-end routing policy. In an MPLS-VPN organization, BGP makes use of VPN sites that are

transparently carried across the internet backbone to another site in the same VPN. Because there is a single routing protocol that is used for the entire process of VPN between sources to destination sites, hence the concept of redistribution does not occur.

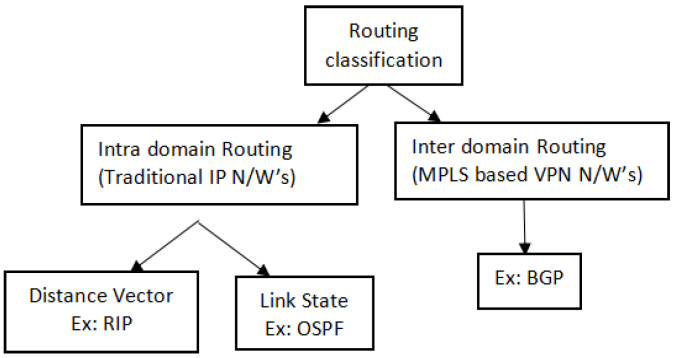


Figure 1. Classification of routing protocols.

2. Literature Survey

Reference [1] modified a traditional crank back and proposed a simple "Crank back with cache" scheme to focus on the scalability of routing to establish on-demand end-to-end QoS requirements. Further developed a new routing protocol, service model, signaling mechanism, and service discipline schemes to support various QoS applications in Internet Protocol. In general, QoS is referred to as a path finding algorithm that mainly depends on the accuracy of routing information such as link residual bandwidth. Here the path finding algorithm uses Dijkstra's shortest path algorithm for load balancing. For the routing information advertisement, three schemes have been used. They are periodic schemes, threshold schemes, and exponential class schemes and also use integrated service and rate-based service discipline schemes which are simulated in the C language to implement intradomain QoS routing on a per-connection and on-demand basis. Thus the proposed crank back with cache had improved the performance for using large values of clampdown timer and also reduced the advertisement traffic.

Reference [2] presented a key difference between IP routing and MPLS approach and provided a solution to IP QoS, gigabit forwarding, network scaling, and traffic engineering. MPLS technique solves the IP scaling problems and finds a solution to IP network traffic, per-hop QoS, traffic engineering, and signaling/provisioning. It also implements traffic engineering techniques to emulate high-speed tunnels and to forward packets over non-shortest paths. Here IP router and MPLS LSR get divided into two different engines, i.e., the management engine and packet forwarding engine. MPLS supports constraint routed LSPs (label switching protocols) which is a real selling point for MPLS by using two techniques, namely, CR-LDP and M-RSVP. These LSPs associated with QoS guarantee to provide topological isolation and temporal isolation that lead to sophisticated load balancing and MPLS to be deployed by services. Thus the paper finally states that MPLS will remain a mixture of magic and myth.

Handover latency and signaling traffic are the major drawbacks that occur when a mobile node migrates to an adjacent subnet without getting registered with LSP [3]. To overcome this drawback, we proposed MPLS based mobile IP architecture that allows frequent location management and LSP setup operations by using label distribution protocol (LDP). After analyzing several LSP re-routing schemes, it finally proposed a multicast re-routing scheme that supports smooth handover in MPLS based mobile IP networks. The major components used in this network are hierarchical architecture, registration procedure, communication protocol using LSP, handover, and re-routing procedure. The handover procedure mainly concentrates on LSP re-establishment, dynamic re-routing, and multicast-based re-routing. The performance analysis made here is handover delay, disruption delay, and buffer requirement. This analysis concludes that the multicast re-routing scheme has reduced the handover latency and signaling traffic and provides the best shortest disruption period.

An approach to traffic engineering in intradomain networks by using interior gateway protocols such as OSPF and IS-IS has been described in [4]. This paper explains the idea of how to adapt the configuration of link

weights based on traffic and topology within the network domain and summarizes the results for optimizing OSPF and IS-IS weights to the prevailing traffic. It also states that the traditional shortest path routing protocols with the traffic engineering technique are the most effective ones for controlling the flow of traffic in large IP networks by incorporating the traffic load in the link state advertisements and the path selection decisions. The framework for traffic engineering has two main features that are the centralized approach for setting the routing parameters and the use of link weight to drive the path selection process. The major advantages of using traditional OSPF/IS-IS are low protocol overhead, diverse performance constraints, and compatibility with traditional shortest path IGP's. The traffic engineering approach has three main steps: measure, model, and control. The measure consists of topology/configuration and traffic demands, the model consists of path selection based on IGP configuration, and finally control consists of reinforcing the IGP weight/utilization. Thus finally, it concludes that the establishment of backup paths and faster re-routing are the effective ways to reduce the disruption of traffic and network failures.

The characteristics of interdomain routing with traffic engineering techniques by measuring the basis of three different internet service providers have been analyzed in [5] explaining how tuning is used to control the incoming and outgoing traffic with its limitations. Here tuning is done based on the trial and error method. For better control of packets flow in an IP network, the traffic engineering technique has been employed. In interdomain routing, BGP is particularly used to route packets between the domains. The stub domain and transit domain are the two main domains in which the packets have been transferred. The stub domain produces the IP packets whereas the transit domain interconnects the different domains and carries the packets to an external domain. The major challenges faced in traditional IP networks are the size of the internet and the best-effort service. To overcome this challenge, the BGP is proposed with traffic engineering technique to control packets' flow and show that the autonomous system has more control over its outgoing traffic than its incoming traffic.

A mechanism for traffic engineering techniques by combining differentiated services and constraint-based routing to meet different QoS requirements, load balancing, and throughput to improve the capability of the network has been developed in [6]. The major drawbacks of traditional IP networks are that the internet cannot meet different QoS requirements according to different traffic flows, it also meets serious local congestion and inefficient utilization. The proposed differentiated service model performs traffic differentiation by using three different service classes, they are expedited forwarding (EF), assured forwarding (AF), and best effort (BE), to forward traffic flows to different per-hop behavior. Traffic engineering provides the most efficient methods to solve the problems of congestion, uneven load distribution, network resource utilization and optimizes traffic performance. MPLS provides the solution to improve packet forwarding performance by using an efficient packet forwarding technique. Thus the proposed method combines differentiated service and traffic engineering mechanisms to provide new traffic engineering over an MPLS based network and achieves high network performance.

Reference [7] proposed two routing techniques over traditional IP networks, namely, routing with a clue (RC) technique and MPLS technique. Here routing with a clue technique is mainly used to improve the performance of routing in IP networks by distributing the IP lookup process to all nodes. A “clue” is a small unit that is used to carry IP lookup information into the next node which is presented in the path. MPLS is another technique that uses “label” to carry routing information from source to destination. Throughput, mean queue length, mean waiting time, and network utilization are the few parameters that are simulated to analyze the performance between RC and MPLS networks. In an RC network, packets are freely routed and distributed all over the path in a network. It does not require any pre-calculation so the packets are traversed equally to all nodes in the path. Whereas in MPLS network, it requires pre-calculation to find a path to transmit the packets and utilize the same path for transmission of all packets which leads to an increase in mean waiting time and mean queue length at every node. It also takes more time to calculate the path. By

comparing the performance between RC and MPLS, the result shows that RC is much better than MPLS routing in terms of throughput and queue management.

Reference [8] presented a comparative performance analysis of traditional IP and MPLS based networks in case of heavy traffic environments for multimedia applications. Traffic engineering is the major technique applied in MPLS networks to provide business class transports and also handle various real-time services, where IP-based networks are connectionless. For multimedia applications, IP networking has many drawbacks in terms of delay time, jitter, packet loss, and low reliability. The simulations are done in the NS-2 simulator in terms of throughput, utilization, packet loss, and reception packet and finally, the result shows that IP networks do not provide any resource assurance for traffic flows and it also causes some network performance problems such as starvation and unfairness for certain traffic. In the case of MPLS-TE, the performance of the network has been improved significantly with good quality of service.

Multi-constrained is the major problem that considers several terms like delay, jitter, packet loss, and bandwidth [9]. To overcome this problem, we proposed a routing-based dynamic admission control mechanism in the MPLS network to control the IP traffic flows and to provide end-to-end delay constraints for all flows without re-routing. A dynamic admission control mechanism is mainly used to accept or reject the new flow based on the requested bandwidth and the resource available in the network. This also solves the mathematical programming model for all traffic flows and the numerical results reduce the end-to-end delay for each flow. In this paper, the concept of re-routing is avoided as it leads to QoS effect. Performance evaluation has been done for blocking rate, a ratio of constraint violated, end-to-end delay, and blocking rate for different numbers of LSPs allowed in the path and the result shows that it significantly reduces the mean end-to-end delay for each flow.

A new dynamic routing scheme with minimum interference in MPLS networks to achieve traffic engineering in traditional IP networks and provide route optimization and performance improvements has been

proposed in [10]. LSP routing algorithm reduces the interference to achieve efficient routing of MPLS bandwidth. The traffic engineering technique employed in MPLS networks has been used to achieve the performance of the network goals such as delay minimization and throughput maximization. The commonly used algorithm is the minimum hop algorithm whereas MIRA is referred to as the minimum interference routing algorithm that increases the number of paths in a network for improving online routing. It also identifies the critical paths and avoids overloading a network. Performance measurement for MIRA network consists of several LSP setup requests rejected for 10 experiments, deviation of bandwidth utilization ratio for 10 experiments, and time cost with LSP number increasing whereas dynamic routing algorithm scheme considers bandwidth available of links in the network, traffic flow distribution, and cost metric balances. Thus the simulation result shows that the algorithm (BU-MIRA) has good performance in route optimization, load balancing, and computation complexity.

Route reconvergence in VoIP users has impacts on latency and jitter [11]. When the routing table becomes complex, there will be more utilization of RAM and CPU power. This slows down the routers and affects the speed of the network. Thus is shown the analysis of how VoIP performance is being affected by different interior routing protocols such as RIP, OSPF, and EIGRP. In general, VoIP is performed well in an enterprise network based on interoperability, security, and bandwidth management. Network performance has been simulated in the OPNET modeler including the measurements of hop count, delay, bandwidth, load, reliability, cost and mean opinion score. The simulation result shows that RIP performs well with the fastest possible route and carries out the low efficient routing, where enhanced interior gateway routing protocol (EIGRP) has link failure and affects the performance of the network and finally OSPF maintains acceptable performance, flexibility, and efficiency for VoIP service networks. Thus the statistical analysis for this overall performance of interior routing protocol concludes that OSPF performs well for enterprise networks in case of resilience and efficiency to support VoIP services.

Reference [12] proposed an MPLS layered network architecture and introduced a mechanism that integrates both IPv4 and IPv6 networks which help to improve the performance of the whole internet environment. MPLS becomes popular in fast-forwarding of packets and helps the customer and provider sites with fast data exchanging environments such as unicast, multicast, VPN, and TE with help of RSVP (resource reservation protocol) in both IPv4 and IPv6 networks. Layered MPLS architecture is mainly referred to as dividing the basic MPLS network layer into several sub-layers based on their functionalities. This mechanism not only solves the high label consumption problem but also meets QoS requirements with lower resource consumption for the entire network without causing cross-layer talks. The major issues present in the existing MPLS networks are increasing the amount of label consumption and QoS requirements which are countered by introducing layered MPLS network architecture.

Dynamic routing implementation decisions between distance vector routing protocol or link-state routing protocol or between the combinations of both routing protocols have been presented in [13]. These routing protocols are simulated by using the OPNET modeler. The result shows that EIGRP performance is better when compared with RIP and OSPF in terms of network convergence activity, network convergence duration, routing protocol traffic, CPU utilization, network bandwidth utilization, throughput, and queuing delay. It also has control over timing issues and does not need any hierarchical designs to operate efficiently. Thus EIGRP results in greater functionality and stabilization with ease of greater network maintenance when compared with RIP and OSPF.

An experimental OpenFlow 1.0 extension to support MPLS has been designed [14]. By utilizing OpenFlow MPLS, it implements an OpenFlow source prototype based on NetFGPA and compares the performance measurements of the prototype with software routers. The measurement shows that the protocol is an efficient tool in testbeds for achieving line-speed forwarding. The OpenFlow extension modifies the flow table of OpenFlow so that it can include two MPLS labels and allows the definition

of virtual ports. The implementation of NetFGPA supports up to two virtual ports for MPLS networks. The testbeds ensure that the open-source label switched router improves the performance of line-speed forwarding in prototype networks. In the proposed method, the current NetFPGA 1G supports only upto 32 flows in a network, so these are targeted to use of NetFPGA 10G for better performance in the future.

Multiprotocol label switching virtual private networks (MPLS-VPNs) and virtual private LAN service (VPLS) are most efficient due to their scalability, ease of setup, and support by major vendors [15]. A methodology is used to analyze the performance of MPLS and VPLS by considering BGP to maintain VPN information. An extensive tradeoff between scalability and visibility of network events for which architecture and prototype were implemented has been proposed. The major solution provided by some industries for the management of MPLS and VPLS includes Cisco's IP solution center, Alcatel-Lucent's service-aware management, HP's service activator solution for VPN services, and IBM's Tivoli network manager. But these solutions also suffer from several drawbacks like offering a limited view of the effect of network events such as reconfiguration and device failures, being more targeted at provisioning, more focused on a single technology, and based on proprietary. Thus the proposed research area mainly focused on routing convergence and scalability rather than monitoring. This monitoring tool could spot a subtle routing anomaly and it was being reported to vendors. Quagga routing site is used for best interoperability.

Reference [16] compared and analyzed two interior gateways routing such as EIGRP and OSPF based on the performance of VoIP in BGP-MPLS and IP VPN. The combination of MPLS and IP routing improves the forwarding mechanism, scalability, and overall network performance. VoIP is a transmission technique that provides reliable communication for voice and data transmission and it is more cost-effective. It does not guarantee to provide the best quality of traffic in a network when it uses conventional routing which leads to delay and packet loss. To overcome this issue, VoIP

uses an MPLS based VPN which offers better routing in packet-switched networks. OPNET modeler 14.5 is a simulating tool that has been used to simulate the performance between EIGRP and OSPF based on delay, jitter, and mean opinion score. The result shows that EIGRP has a high delay, jitter, and decreased MOS value when the rate of the call gets increased. Thus OSPF and BGP-MPLS-VPN provide a better solution for VoIP VPN applications.

Virtual private networks do not perform well for some applications such as VoIP, data application, and financial transactions even when there are small disruptions in connectivity [17]. It also leads to a deficiency of BGP scalability when network scaling is larger and larger which has become a bottleneck in the VPN network. The reason behind the deficiency of BGP scalability in large scale MPLS-VPN is slow route convergence which utilizes more time to exchange update routes between routers and slow route table transfer makes lower utilization of the provider network backbone due to the presence of the idle state in a period. The simulation of BGP is done in an OPNET modeler and the result shows that BGP is the most important protocol that has been used for large and complex networks but in the case of very large scale MPLS-VPN networks, there is a convergence delay in a network due to failure detection and route invisibility which has become the bottleneck that affects the QoS of VPN network.

Traditional IP networks, namely, frame relay and ATM networks have many drawbacks while operating in larger networks such as cost, security, flexibility, and scalability [18]. To overcome this problem, MPLS based VPN networks have been used that allow an organization to interconnect with provider and customer sites through secure links and provide a better understanding of the large network management operation of service provider networks. The proposed work focuses on IGRP routing in MPLS-VPN networks. For investigation purposes, two routing protocols of IGRP, namely, OSPF and IS-IS were used. These routing protocols were simulated by using the OPNET modeler, and performance was analyzed. Based on the results, it concludes that MPLS-VPN gives the best service to the service

provider networks when compared with traditional IP networks. By comparing the simulation performance of OSPF and IS-IS routing protocols, it concludes that IS-IS gives better performance in terms of delay, convergence and can build a single large network area. It also supports a single topology for IPv6 network routing.

For uni-cast flows in the MPLS network, a fault-tolerant routing model has been proposed in [19]. This model includes three backup schemes such as link, node, and path protection by fast re-route. Overloading in the network causes QoS degradation, this can be solved by changing the fast re-route in the MPLS network to a flow-based model. This model calculates two types of paths for the same flow: primary and backup. It also introduces non-linear restrictions to prevent link, node, and path intersection of primary and backup routes in an MPLS network.

Reference [20] described modeling and simulation tools to evaluate the performance of MPLS based networks. Three different simulation tools have been used to analyze the performance, which are GNS3, OpenSimMPLS, and OPNET modeler. The first simulation tool is GNS3 which is used by CISCO devices for designing and modeling computer networks. Here Wireshark is used to analyze the results of topology and protocols employed. The second tool is OpenSimMPLS which helps the designers to know packet flow, packet re-routing due to some major issues like congestion, link failure, and buffer overflow. The third tool is the OPNET modeler which is used to investigate VoIP applications between MPLS networks and traditional IP networks. These three experimental result shows that MPLS networks perform better than traditional IP networks because MPLS networks use the Label Switching Technique to improve the speed of routing in a network.

A comparative study of dynamic routing protocols, namely, distance vector and link state has been presented in [21]. The main example for distance vector is RIP and for link-state is OSPF. In general, routing is the most important process for communication purposes on the internet. For transferring information securely among routers from source to destination,

routing protocols are used in the interconnection of networks. Several routing protocols have their applications for packet routing on the internet, namely, RIP, OSPF, EIGRP, OPNET, IGRP, etc. In the proposed method, the simulation has been done by using GNS3 which compares the performance of RIP and OSPF. RIP is suitable only for smaller networks as it sends the complete routing information using periodic updates which causes overheads in the network and results in unnecessary wastage of bandwidth, high latency, and higher convergence time. On the other hand, OSPF has a faster convergence rate, efficient use of bandwidth, less packet loss, and a higher throughput rate. Hence the simulation result shows that OSPF has the least transmission rate, high reliability, high efficiency, and lower administrative distance value when compared with RIP. Thus OSPF performs well for larger networks and RIP can be used only for small and simple networks.

Reference [22] designed a multi-VRF MPLS network that separates larger networks into smaller networks in a cost-effective way and provides a solution to many problems that are faced between customer edge and provider edge by using a limited number of resources. In the case of customer edge routers, virtual private networks do not provide any customary LAN for private networks. To overcome this, the multi-VRF CE feature also called *VRF-lite* is used, where the customer edge routers can be performed more economically with the help of VPN functionality. The simulation tool used here is GNS3 with VMware visualization which is well suited for real-time network environments. The result shows that privatization and security can be achieved with a minimum number of links in a network. Thus the use of this design limits the wastage of links and provides cost-effective operation for both the customer and service provider edge in a network.

An upgraded topology for internet service provider (ISP) in MPLS and BGP environments has been proposed in [23]. The major drawbacks present in the traditional service provider networks are reliability, availability, and management. These drawbacks can be removed by an upgraded virtual environment using two simulator tools. The first simulator design is a

network topology that can be used to evaluate real-time architecture, process all packet exchange, and finally check all protocols within a network. The second simulator is used to evaluate the amount of traffic in a network. This also deals with the simulation and analysis of double-layer design. This design provides high reliability, availability, and management feature for both, logical and physical links and also backup schemes for protocols such as MPLS, BGP, and VRF making the network easier to understand about network topology and become more stable. MPLS and BGP decrease the cost of network management and also create a link on their own. Thus the simulation result shows that an upgraded topology performs better when compared with a traditional topology in terms of speed and capacity.

Dynamic multipoint virtual private network provides better scale for hub-to-spoke and spoke-to-spoke network designs by allowing IP security VPN networks to optimize their performance and reduce the latency for better communication [24]. This technique integrates different concepts such as generic routing encapsulation (GRE), IPsec encryption, next-hop resolution protocol (NHRP), and routing that allows end-users to communicate effectively by using IPsec tunnels. In the existing work, we use RIP for smaller networks and EIGRP for larger networks in spoke-to-spoke topology whereas in the proposed work, we analyze and simulate routing protocols for Dual Hub Dual DMVPN hub-to-spoke topology that ensures the least delay, less jitter value, fast convergence time and link utilization. The simulation uses the OPNET modeler and compares the performance between EIGRP and OSPF based on convergence time, link utilization, and end-to-end delay. The result shows that both OSPF and EIGRP provide the best routes for securing large enterprise networks by using Dual Hub Dual DMVPN hub-to-spoke topology because of their fast convergence and utilization. But the proposed work strongly recommends using OSPF since it is a standard routing protocol for multi-vendor enterprise network architecture.

The potential threats to the privacy and security of users' data are being hacked, lost, and exposed by cybercriminals [25]. These threats can be countered by using virtual private networks (VPN) providing secure

communication, anonymity, and privacy to users and organizations to a greater extent. We compare the working principle of three VPNs, namely, MPLS, IPsec and SSL, based on their features, performance, security, quality of service, convenience, scalability, maintainability, speed, development, technology, the impact of VPN on firewalls, and cost-efficiency. By comparing the performance of three VPNs, the result shows that the internet protocol security (IPsec) VPN is highly secured and the most commonly used VPN but it does not have fine-grained access control over the network. Secure sockets layer (SSL) is the most secure VPN used on the internet for secure communication but it cannot meet QoS requirements as expected. Multi-protocol label switching VPN is the least safe but it provides perfect QoS requirements for more local area networks. Thus the final result shows that SSL VPN is the best choice of VPN for secure communication.

Intradomain routing is one of the most fundamental building blocks of the internet [26]. The paper answers the question of whether the performance of intradomain routing can be improved with the help of reinforcement learning (RL). It is difficult to answer for RL based routing solution as it suffers from complex network traffic and large action space in routing. To overcome, the challenges of RL based routing users have to investigate the performance of several approaches in terms of scalability, stability, robustness, and convergence. The authors also proposed two methods based on the lessons learned from the solutions of R-based routing. The two methods are, namely, supervised Q-network routing (SQR), discrete link weight based routing (DLWR) which outperform the shortest path intradomain routing and boost the performance of RL routing. The result shows that Q-routing cannot be used for high-speed networks due to its high frequency in routing updates and had some scalability and robustness issues. The link weight-based routing (LWR) also had some implicit problems when the RL routing algorithm is applied. Thus the proposed SQR and DLWR methods can handle the core problems that are presented in Q-routing and LWR and outperform the shortest path intradomain routing by 57% and 17%, respectively.

Current approaches for transport service design and configuration face several challenges [27]. The challenges are listed as a lack of interface between OSS and network layer due to limited programmability and lack of services in the case of IP/MPLS operator networks. To solve this challenge, an approach based on hybrid SDN is proposed presenting the MPLS L3 VPN services for intent-based configuration in a carrier-grade ecosystem. An existing SDN controller is tested by using RESTCONF NBI (northbound interface). This controller is used to abstract the network configuration complexity by implementing the YANG network model which is also called *L3NM* (*Layer* 3 *VPN network YANG model*). Thus the result shows that the YANG model affects the time consumed between the controller and the network level to create services and limits the deployment of interfaces between the network layer and the operational support systems.

Article [28] proposed a traffic tunneling technique known as MPLS-TE and described the design and implementation for IPv6 customers with the help of RSVP, OSPF, and BGP. The proposed work mainly focuses on traffic congestion minimization in the MPLS network by using tunneling techniques from traffic engineering and also compares the performance between disabled MPLS networks and tunnel-enabled networks for IPv6 customer sites. The simulation result shows that the tunnel-enabled network has high throughput, low latency, less packet loss, fast convergence time, and minimum round trip time when compared with the disabled MPLS network. Thus the packet delivery ratio obtained in the tunnel enabled network was about 97.43%.

MINA algorithm is used to find errors presented in MPLS architecture without using service provider networks [29]. However, it can be implemented only for single-homed CE configuration. Thus it extends their proposed work by using the heuristic-based approach in the MINA algorithm which helps to detect misconfiguration in MPLS architecture connected to multi-VRF, multi-homed configuration, and site-redundant CE environments. Thus the result shows that the MINA algorithm with a heuristic-based approach not only detects the misconfiguration but also

locates the misconfiguration in multi-VRF CE environments that making the network highly scalable by fixing the prefixes both inside and outside the administrative domain legitimately.

Multi-layer multi-domain (MLMD) routing faces major issues between different layers and domains based on different technologies and cooperation [30]. There is also no attention to interdomain network topology and inter-layer links which are not optimized due to lack of visibility. Thus the proposed way gives the solution to these orchestrating MLMD networks by using path computation engine (PCE). By using PCE, it makes the performance of flexible Ethernet technology to link IP and optical network domains. The issue of missing network information in MLMD can be dealt with by using a new implicit routing strategy by considering the boundary link metrics. Experimental result shows that the proposed method achieves 87% of optimal throughput which is higher than current practices. Thus the proposed method optimizes the global network utilization for routing flexible Ethernet traffic in MLMD networks by preserving the intradomain network information.

A multipath routing solution for load balancing is called *BGP-multipath* (*BGP-M*) [31]. There has not been much research on BGP-M despite recent interest in multipath routing. Here, we present the first measurement and in-depth investigation of internet BGP-M routing. BGP's default configuration calls for only one "best" path to be used for each prefix. A method called *BGP-multipath* (*BGP-M*) allows load balancing on several equally expensive IP-level inter-domain pathways. The ECMP feature is supported by routers made by the majority of significant suppliers, including Juniper, Cisco, and Huawei. Despite numerous research studies on multipath routing, BGP-M is still a mysterious method.

After defining the terms MPLS-VPN and BGP, the benefits of MPLS-VPN are discussed [32]. A computer network experiment based on MPLS-VPN and BGP is then developed. Following the experiment, the related evaluation is immediately available, and all network parameters are tested successfully. More and more businesses have access to the internet as

society and the economy expand. Personal virtual local area networks, or VPNs, can be utilized to create these businesses' LANs in order to address this issue. In order to fully understand MPLS-VPN, this research created an experiment based on MPLS-VPN and BGP. Experimental teaching is a crucial teaching component in the educational system of colleges and universities compared with the theoretical one.

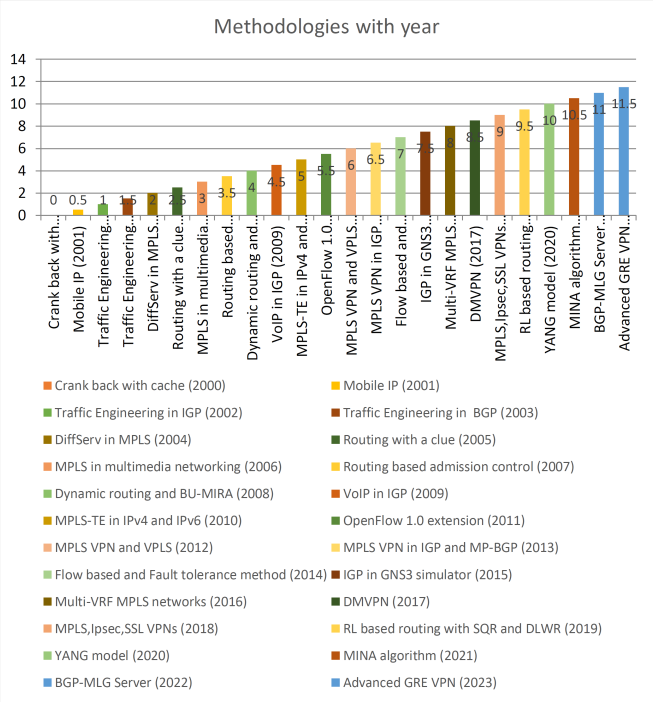
Table 1. Comparison table between traditional IP and MPLS based VPN methodologies

Author and year	Methodology	Limitations	Remarks
Ke and Copeland [1]	Crank back with cache, RIP, OSPF	RIP and OSPF advertise only topological information	The proposed crank back with cache boosts the performance and reduces the advertisement traffic
Armitage [2]	Traditional IP, MPLS, CR-LDP, M-RSVP, LSR	IP VPNs have complex network management and virtual routing issues	MPLS provides a solution to per-hop QoS, gigabit forwarding, network scaling, and traffic engineering. It also supports constrained-routed LSPs
Um and Choi [3]	MPLS, mobile IP, LSP, LDP	Low bandwidth efficiency, high handover latency, and heavy signaling traffic	Multicast re-routing was proposed to support smooth handover and allow frequent and seamless location management on MPLS mobile IP architecture
Fortz et al. [4]	Traditional IP, traffic engineering, OSPF, IS-IS	Robust communication, heavy traffic, and failure of network elements in case of TCP based IP networks	The use of traffic engineering provides good user performance, efficient use of network resources, and allows OSPF and IS-IS to incorporate traffic and make path selection decisions
Quoitin et al. [5]	Traffic engineering, BGP, stub domain, transit domain, tuning	Sizes of the internet and best-effort service are the major challenges in IP networks	The proposed traffic engineering technique in BGP also had some drawbacks such as increasing the size of the BGP routing table and difficulty to select appropriate values but it shows that AS has high control over its outgoing traffic
Yuzhong et al. [6]	Differentiated services, MPLS, constraint-based routing, traffic engineering	Traditional IP network suffers from serious local congestion and inefficient utilization of bandwidth	Combined differentiated service and constrained-based routing to propose a new TE mechanism that achieves network load balancing, improved network resource utilization ratio, and also meets QoS requirements
Viriyaphol and Jittaiviriyanukoon [7]	Routing with a clue, label switching, IP routing technique, MPLS	MPLS suffers from high MQL, increases MWT, and time-consuming is high at every single node	They proposed routing with a clue technique to improve the performance of routing, it also has a higher throughput rate when compared to the MPLS network

Barakovic et al. [8]	MPLS, multimedia networking, routing protocols, NS-2	Multimedia applications in IP networks suffer from delay, jitter, packet loss, low reliability, starvation, and unfairness of certain traffic	Multimedia applications in MPLS TE provide improved network performance in terms of throughput, utilization, packet loss, and reception packet, it also delivers a good quality of service
Oulai et al. [9]	MPLS networks, routing-based admission control, end-to-end delay	Suffers from multi-constrained problems like delay, bandwidth inefficiency, packetloss, and jitter	Proposed a routing-based admission control technique in the MPLS network that provides end-to-end delay constrained for all IP traffic flows without re-routing
Zhu et al. [10]	Dynamic routing, traffic engineering, min-hop algorithm, MIRA algorithm, MPLS, LSP routing	Traditional networks had the problem of delay and throughput inefficiency	Presented a dynamic routing algorithm that reduces the interference among competing flows and BU-MIRA algorithm results in good network performance in terms of routing optimization, load balancing, and computation complexity
Che and Cobley [11]	VoIP, IGP, RIPv1, OSPF, EIGRP, OPNET modeler	VoIP applications over large enterprises suffer from latency and jitter whereas RIP carries out inefficient routing and EIGRP suffers from link failure	Compared the performance of RIP, OSPF, and EIGRP in the OPNET simulation tool and the result shows that OSPF provides high resilience and efficiency in large enterprise networks to support VoIP services. It also provides flexibility and uses the same route for VoIP applications with the same network specifications
Wu and Zhang [12]	MPLS, RSVP, traffic engineering, QoS, IPv4, and IPv6 networks	An increasing amount of label consumption and QoS requirements are the two major issues in the basic MPLS architecture	Proposed a layered network MPLS architecture that integrates both IPv4 and IPv6 to upgrade the performance of the internet and helps to solve the problem of high label consumption in the network
Thorenoor [13]	RIP, EIGRP, OSPF, OPNET Modeler	RIP and OSPF perform poor in terms of CPU utilization, memory, and bandwidth control	EIGRP performs well when compared to RIP and OSPF. Hence it can be implemented to provide functionality as well as stabilization in the network
Kempf et al. [14]	Open flow, NetFGPA, MPLS, open source LSR	OpenFlow 1.0 does not support MPLS	Proposed an extension of open flow to support MPLS and describes its use in the design and implementation of open source MPLS LSR based on the NetFPGA hardware platform
Battista et al. [15]	MPLS-VPN, ISP, BGP, VPLS	Effect of network events such as reconfiguration, devicefailures, targeted at provisioning, focused on single topology and based on proprietary	It merges the concept of both MPLS VPNs and VPLS to provide scalability, best interoperability, and faster routing convergence in the network
Yunos et al. [16]	OPNET modeler 14.5, MPLS-VPN, EIGRP, OSPF	Delay and jitter in EIGRP is reflected in MOS value as it decreases as the rate of call increases	Compared the performance of OSPF and EIGRP in an OPNET modeler and the result shows that OSPF performance is better when compared to EIGRP in terms of delay, jitter, andmean opinion score

Mai and Du [17]	MPLS, MP-BGP, OPNET modeler	BGP scalability deficiency and VoIP do not react well even when the smallest disruption occurs	Presented slow routing table transfer and route convergence delays in large scale VPNs. The simulation result shows that BGP is the standard protocol to deal with large and complex networks
Eljack and Abdelkarim [18]	MPLS-VPN, OSPF, IS-IS, IGP, OPNET modeler	Traditional IP based, frame relay, and ATM networks have many drawbacks in the management operation of large scale networks	IGP allows the router to exchange information within an AS. Example: RIP, OSPF, and IS-IS. The simulation result shows that IS-IS gets better results than OSPF concerning the delay
Lemeshko and Arous [19]	3 backup schemes such as link, node, and path protection, flow-based and fault-tolerance method, conditions for fast re-route	Does not provide an efficient response to overload in the traditional networks	Responsible for prevention of node, link, or path intersection of primary and backup routes that are introduced in this structure model
Sllame [20]	GNS3, OpenSimMPLS, OPNET modeler, MPLS, traditional IP networks	Traditional IP network does not provide the expected results in simulation	Compared the performance of MPLS and traditional IP networks in GNS3, OpenSimMPLS, and OPNET simulation tools. The result shows that MPLS outperforms well by using the label switching technique
Jayakumar et al. [21]	RIP, OSPF, GNS3	RIP results in unnecessary wastage of bandwidth and higher convergence hence it can be suitable only for smaller networks	The simulation result in GNS3 shows that OSPF has faster convergence and efficient bandwidth. Hence it can be chosen as a better choice for larger networks
Yadav and Jeyakumar [22]	MPLS-VPN, multi-VRF, GNS	CE routers cannot perform functions like label exchange because MPLS is not enabled on the CE routers	Designed a multi-VRF MPLS network on the service provider's end which limits the wastage of links and provides a route for every customer at the same network in a cost-efficient way
Song et al. [23]	MPLS, OSPF, GNS3, VRF	The basic service provider network suffers from reliability, availability, and management of network operations	Double-layer design has been simulated and analyzed. The result shows that the upgraded topology performs better in terms of speed and capacity when compared with the current topology performance
Tizazu et al. [24]	DMVPN, RIP, OSPF, EIGRP, hub-to-spoke, spoke-to-spoke	RIP can be only used for smaller networks hence it cannot be suitable for dual hub dual DMVPN hub to spoke topology	Both EIGRP and OSPF perform better for dual hub-to-spoke topology but since OSPF is a standard protocol, it can be recommended to use in multi-vendor enterprise networks
Zhipeng et al. [25]	VPN, MPLS, IPsec, SSL, network security	A potential threat to the security and privacy of data by cyber criminals	Compared the performance of IPsec VPN, MPLS-VPN, and SSL VPN. The result shows that SSL VPN is the most secure one of the three

Xu et al. [26]	Intradomain routing, reinforcement learning, RL based routing, SQR, DLWR	Complex network traffic and large action space in routing does not provide a proper solution for an existing RL based routing	The proposed methods SQR and DLWR can easily handle the core problems in Q-network routing and outperform the shortest path routing by 57% and 17%, respectively
Barguil et al. [27]	L3 VPN, IP networks, SDN, YANG model, service provisioning	Lack of open interface between (OSS) operational support systems and the network layer	Presented an intent-based configuration of MPLS L3 VPN services in the carrier-grade ecosystem and implemented the YANG model to abstract the complexity of networks configuration and further limit the deployment of common interfaces in the network
Prasad et al. [28]	MPLS-TE, VPN, RSVP, OSPF, IPv6	Routers are overloaded due to uneven utilization of network links are the major drawback in basic MPLS networks	The proposed work mainly focuses on the minimization of traffic in the MPLS network by using the tunneling concept. It also shows that the tunnel-enabled MPLS network performs better and obtains the packet delivery ratio of up to 97%, respectively
Ojha and Hansdah [29]	MPLS L3 VPN privacy, Multi-VRF, CE security and privacy, MINA algorithm	MPLS L3 VPN is often prone to errors and misconfigured the VPN customer's data privacy and security	Proposed an extended MINA algorithm based on a heuristic approach to detect and locate the misconfiguration in a multi-VRF environment that makes the network highly scalable
Koulougli et al. [30]	Flexible Ethernet, IP-optical networks, path computation engine, SDN orchestration	Issue of missing network information in an MLMD network due to privacy, security, and lack of visibility in intradomain network topology	Proposed a new method for routing flexible Ethernet traffic in MLMD networks to obtain the global network utilization and achieve 87% of optimal throughput which is higher than current practices
Li et al. [43]	Border router, multipath routing, BGP-MLG server	The key challenge is to map the AS borders accurately. The goal is to provide a more comprehensive and accurate picture of BGP-M implementation on the worldwide Internet. It would be interesting to learn whether BGP-M has been widely deployed	This study describes the first measurement of BGP-M deployment throughout the internet. Our measurement was based on looking glass server data, which not only offers the ground truth but also a wealth of information on numerous aspects of BGP-M
Tao et al. [44]	L2TP VPN, GRE VPN and MPLS VPN, NS2 simulator	SDN and IPv6 are not supported by the MPLS VPN experiment, necessitating more study and system upgrades	An extensively utilized networking technology is MPLS-VPN. Following the conclusion of the MPLS-VPN experiment by the students, it was discovered that the only way to determine the truth is through practice. The best technique to solidify theoretical information and improve one's capacity to fully apply learnt theoretical knowledge to solve practical difficulties is through experimentation



Line Chart 1. Methodology used with its appropriate year.

3. Conclusion

This survey analyzes the various techniques that are used in intradomain and interdomain routing protocols by comparing the performance between traditional IP and MPLS based networks. The literature review of this paper shows how important is the sharing of information in a real-time environment by using different technologies. The main aim of this article is to identify the technique that is used for sharing the information more securely and efficiently between the customer edge and the provider edge in a network. The performance analysis shows that MPLS-VPN plays a prominent role in a real-time environment for sharing information in large enterprise networks. There is still a potential threat that arises in the area of information hijacking even in the BGP environment which has to be detected and analyzed to provide proper protective mechanisms as a result of future work.

4. Future Scope

In future, there is a wide scope in the area of block-chain based cloud computing technology to do the research work for preventing the information from hackers.

Acknowledgement

We thank the research center at Anna University Regional Campus Coimbatore which is well established with all the laboratory facilities to carry out the research work and was approved by Anna University Chennai, Tamilnadu, India.

References

[1] Yu-Kung Ke and John A. Copeland, Scalability of routing advertisement for QoS routing in an IP network with guaranteed QoS, Globecom'00-IEEE Global Telecommunications Conference (Cat. No. 00CH37137), Vol. 1, 2000, pp. 605-610. https://doi.org/10.1109/GLOCOM.2000.892087.

[2] Grenville Armitage, MPLS: the magic behind the myths [multiprotocol label switching], IEEE Communication Magazine 38(1) (2000), 124-131. https://doi.org/10.1109/35.815462.

[3] Tai Won Um and Jun Kyun Choi, Path re-routing algorithm for mobile IP service at the ATM-based MPLS network, Fourth IEEE International Conference on ATM (ICATM'01) and High-speed Intelligent Internet Symposium, ICATM (Cat. No. 00EX486), 2001, pp. 70-74. https://doi.org/10.1109/ICATM.2001.932059.

[4] B. Fortz, J. Rexford and M. Thorup, Traffic engineering with traditional IP routing protocols, IEEE Communication Magazine 40(10) (2002), 118-124. https://doi.org/10.1109/MCOM.2002.1039866.

[5] B. Quoitin, C. Pelser, L. Swinnen, O. Bonaventure and S. Uhlig, Interdomain traffic engineering with BGP, IEEE Communication Magazine 41(5) (2003), 122-128. https://doi.org/10.1109/MCOM.2003.1200112.

[6] Chen Yuzhong, Yang Bingqing, Ren Rong, Geng Yanhul and Yu Nenghai, Traffic engineering with constraint-based routing in Diffserv/MPLS network, 13th IEEE Workshop on Local and Metropolitan Area Networks, 2004, pp. 125-128. https://doi.org/10.1109/LANMAN.2004.1338416.

[7] P. Viriyaphol and C. Jittaiviriyanukoon, A study of routing with a clue versus label switching over IP based networks, 2nd Asia Pacific Conference on Mobile Technology, Applications, and Systems, 2005. https://doi.org/10.1109/MTAS.2005.243882.

[8] Jasmina Barakovic, Himzo Bajric and Amir Husic, Multimedia traffic analysis of MPLS and non-MPLS network, Proceedings 48th International Symposium ELMAR, 2006, pp. 285-288. https://doi.org/10.1109/ELMAR.2006.329567.

[9] Desire Oulai, Steven Chamberland and Samuel Pierre, A new routing-based admission control for MPLS networks, IEEE Communications Letters 11(2) (2007), 216-218. https://doi.org/10.1109/LCOMM.2007.061618.

[10] Mingying Zhu, Wu Ye and Suili Feng, A new dynamic routing algorithm based on minimum interference in MPLS networks, 4th International Conference on Wireless Communications, Networking, and Mobile Computing, 2008, pp. 1-4. https://doi.org/10.1109/WiCom.2008.1012.

[11] Xianhui Che and Lee J. Cobley, VoIP performance over different interior gateway protocols, International Journal of Communication, Networks and Information Security (IJCNIS) 1(1) (2009), 34-41. https://doi.org/10.17762/ijcnis.v1i1.6.

[12] Jialei Wu and Yuanping Zhang, A layered MPLS network architecture, 6th International Conference on Wireless Communications Networking and Mobile Computing (WICOM), 2010. https://doi.org/10.1109/WICOM.2010.5601465.

[13] Sheela Ganesh Thorenoor, Dynamic routing protocol implementation decision between EIGRP, OSPF, and RIP based on technical background using OPNET modeler, Second International Conference on Computer and Network Technology 2010, pp. 191-195. https://doi.org/10.1109/ICCNT.2010.66.

[14] James Kempf, Scott Whyte, Jonathan Ellithorpe, Peyman Kazemian, Mart Haitjema, Neda Beheshti, Stephen Stuart and Howard Green, OpenFlow MPLS and the open source label switched router, 23rd International Teletraffic Congress (ITC), 2011, pp. 8-14. https://ieeexplore.ieee.org/document/6038458.

[15] Giuseppe Di Battista, Massimo Rinondini and Giorgio Sadolfo, Monitoring the status of MPLS VPN and VPLS based on BGP signaling information, IEEE Network Operations and Management Symposium (NOMS), 2012, pp. 237-244. https://doi.org/10.1109/NOMS.2012.6211904.

[16] Rozita Yunos, Siti Arpah Ahmed, Noorhayati Mohamed Noor, Raihana Md Saidi and Zarina Zainol, Analysis of routing protocols of VoIP VPN over MPLS networks, IEEE Conference on Systems, Process, and Control (ICSPC), 2013, pp. 139-143. https://doi.org/10.1109/SPC.2013.6735120.

[17] Jian Mai and Jiang Du, BGP performance analysis for large scale VPN, IEEE Third International Conference on Information Science and Technology (ICIST), 2013, pp. 722-725. https://doi.org/10.1109/ICIST.2013.6747647.

[18] Sarah Mustafa Eljack and Suhail Badawi Abdelkarim, Effect of the interior gateway routing protocols in the multiprotocol label switching networks, International Conference on Computing, Electrical and Electronic Engineering (ICCEEE) 2013, pp. 565-570. https://doi.org/10.1109/ICCEEE.2013.6634002.

[19] Olexandr Lemeshko and Kinan Arous, Fast re-route model for different backup schemes in MPLS-network, First International Scientific-practical Conference Problems of Infocommunications Science and Technology, 2014, pp. 39-41. https://doi.org/10.1109/INFOCOMMST.2014.6992292.

[20] Azeddien M. Sllame, Modelling and simulating MPLS networks, International Symposium on Networks, Computers, and Communications, 2014. https://doi.org/10.1109/SNCC.2014.6866512.

[21] Megha Jayakumar, N. Ramya Shanthi Rekha and B. Bharathi, A comparative study on RIP and OSPF protocols, International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015. https://doi.org/10.1109/ICIIECS.2015.7193275.

[22] Snehal Yadav and Amutha Jeyakumar, MPLS multi-VRF design and implementation using GNS simulator, IEEE International Conference on Engineering and Technology (ICETECH), 2016. https://doi.org/10.1109/ICETECH.2016.7569391.

[23] Zhenxing Song, P. W. C. Prasad, Abeer Alsadoon, L. Pham and A. Elchouemi, Upgrading Internet Service Provider (ISP) network in Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) environment, International Conference on Advances in Electrical, Electronics, and Systems Engineering (ICAEES), 2016, pp. 207-211. https://doi.org/10.1109/ICAEES.2016.7888045.

[24] Gebere Akele Tizazu, Ki-Hyung Kim and Abraham Beley Berhe, Dynamic routing influence on secure enterprise network based on DMVPN, Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017, pp. 756-759. https://doi.org/10.1109/ICUFN.2017.7993894.

[25] Zhang Zhipeng, Sonali Chandel, Sun Jingyao, Yan Shilin, Yu Yunnan and Zang Jingji, VPN: a boon or trap? A comparative study of MPLS, IPsec, and SSL virtual private networks, Second International Conference on Computing Methodologies and Communication (ICCMC), 2018, pp. 510-515. https://doi.org/10.1109/ICCMC.2018.8487653.

[26] Qian Xu, Yifan Zhang, Kui Wu, Jianping Wang and Kejie Lu, Evaluating and boosting reinforcement learning for intra-domain routing, IEEE 16TH International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2019, pp. 265-273. https://doi.org/10.1109/MASS.2019.00039.

[27] Samier Barguil, Oscar Gonzalez de Dios, Roque Gaglino and Ignacio Carretero, Experimental validation of L3 VPN network model for improving VPN service design and provisioning, 16th International Conference on Network and Service Management (CNSM), 2020. https://doi.org/10.23919/CNSM50824.2020.9269043.

[28] N. Sai Prasad, M. Sri Kumaran, Sachin Prasad and N. Sathish Kumar, Implementation and performance analysis of traffic engineered multiprotocol label switching network for IPv6 clients, International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 766-773. https://doi.org/10.1109/ICESC48915.2020.9155933.

[29] Puran Deo Ojha and R. C. Hansdah, A heuristic approach to detect MPLS L3 VPN misconfiguration in multi-homed, multi-VRF site-redundant CE environments, IEEE Transactions on Network and Service Management 18(2) (2021), 2294-2307. https://doi.org/10.1109/TNSM.2020.3009301.

[30] Dahina Koulougli, Kim Khoa Nguyen and Mohamed Cheriet, Efficient routing using flexible Ethernet in multi-layer multi-domain networks, Journal of Lightwave Technology 39(7) (2021), 1925-1936. https://doi.org/10.1109/JLT.2020.3044845.

[31] Ray Hunt, A review of QoS mechanisms in IP-based networks – integrated and differentiated services, multilayer switching, MPLS, and traffic engineering, Computer Communications Elsevier, 2002, 100-108. https://doi.org/10.1016/S0140-3664(01)00334-6.

[32] F. M. Chuissi, D. A. Khotimsky and S. Krishnan, Mobility management in a third-generation all IP networks, IEEE Communication Magazine 40(9) (2002), 124-135. https://doi.org/10.1109/MCOM.2002.1031839.

[33] S. Yasukawa, K. Sugisono, I. Inoue and S. Urushidani, Scalable multicast MPLS protocol for next-generation broadband service convergence network, IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Vol. 2, 2004, pp. 1019-1023. https://doi.org/10.1109/ICC.2004.1312655.

[34] Pradosh Mohapatra, Chris Metz and Yong Cui, Layer3 VPN services over IPv6 backbone networks, requirements, technology, and standardization efforts, IEEE Communication Magazine 45(4) (2007), 32-37. https://doi.org/10.1109/MCOM.2007.343609.

[35] Antonio Cianfrani, Vincenzo Eramo, Marco Listanti, Macro Marazza and Enrico Vittorini, An energy saving routing algorithm for a green OSPF protocol, INFOCOM IEEE Conference on Computer Communications Workshops, 2010. https://doi.org/10.1109/INFCOMW.2010.5466646.

[36] Virginie Van den Schrieck, Pierre Francois and Oliver Bonaventure, BGP add-paths: the scaling/performance tradeoffs, IEEE Journal on Selected Areas in Communications 28(8) (2010), 1299-1307. https://doi.org/10.1109/JSAC.2010.101007.

[37] Ioan Fitigau and Gavril Toderean, Network performance evaluation for RIP, OSPF, and EIGRP routing protocols, Proceedings of the International Conference on Electronics, Computers and Artificial Intelligence – ECAI, 2013. https://doi.org/10.1109/ECAI.2013.6636217.

[38] Chen Haihong and Sun Xiaoling, Simulation and research of OSPFv3 performance, International Conference on Computational and Information Sciences, 2013, pp. 1901-1903. https://doi.org/10.1109/ICCIS.2013.497.

[39] Haresh N. Patel and Rashmi Pandey, Extensive reviews of OSPF and EIGRP routing protocols based on route summarization and route redistribution, International Journal of Engineering Research and Applications 4(9) (2014), 141-144. http://www.ijera.com/papers/Vol4_issue9/Version%204/U4904141144.pdf.

[40] Muhammet Macit, Emrullah Delibas, Bahtiyar Karanlik, Alperen Inal Sekon Yazilim and Tevfik Aytekin, Real-time distributed analysis of MPLS network logs for anomaly detection, IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 750-753. https://doi.org/10.1109/NOMS.2016.7502891.

[41] Gustavo Lopez and Eduardo Grampin, Scalability testing of legacy MPLS-based virtual private networks, IEEE URUCON, 2017. https://doi.org/10.1109/URUCON.2017.8171874.

[42] Haijin Geng, Han Zhang, Xingang Shi, Zhiliang Wang, Xia Yin, Ju Zhang, Zhiguo Hu and Yong Wu, A hybrid link protection scheme for ensuring network service availability in link-state routing networks, Journal of Communication and Networks 22(1) (2020), 46-60. https://doi.org/10.1109/JCN.2019.000056.

[43] J. Li, V. Giotsas, Y. Wang and S. Zhou, BGP-multipath routing in the internet, IEEE Transactions on Network and Service Management 19(3) (2022), 2812-2826. https://doi.org//10.1109/TNSM.2022.3177471.

[44] J. Tao, H. Chen, H. Liu and X. She, Experimental design and teaching research of a MPLS VPN network based on BGP, 2023 IEEE 12th International Conference on Educational and Information Technology (ICEIT), Chongqing, China, 2023, pp. 289-293. https://doi.org/10.1109/ICEIT57125.2023.10107884.