Assessing Queue Management Strategies to Enhance Quality of Service in MPLS VPN Networks

Mahmud Mansour[1], Ahmed Samood[1], Najia Bensaoud[1]

Department of Computer Networks, Faculty of Information Technology, University of Tripoli, Tripoli, Libya

bensaoud.najia@gmail.com

Abstract. Multiprotocol Label Switching (MPLS) has emerged as a key technology for providing quality of service (QoS) guarantees in IP networks. This paper presents an extensive simulation-based evaluation of MPLS QoS mechanisms. Specifically, different queuing policies - First In First Out (FIFO), Priority Queuing (PQ), and Weighted Fair Queuing (WFQ) are implemented and analyzed for providing end-to-end QoS for real-time voice and data applications over an MPLS VPN backbone. The network simulations are performed using the OPNET tool with detailed MPLS, VPN, and queuing parameters configuration. Performance is evaluated across multiple metrics including jitter, delay variation, end-to-end delay, traffic sent/received for both voice and data flows. The results demonstrate that FIFO queuing delivers the best QoS performance for voice traffic, providing simple first-in, first-out buffering. WFQ is shown to outperform PQ for voice flows. All queuing mechanisms can meet QoS requirements for voice and data applications. The paper provides a comprehensive investigation into configuring MPLS networks with QoS capabilities. Key findings show that MPLS VPNs effectively reduce network complexity and costs. FIFO emerges as an optimal queuing technique for enabling QoS services in MPLS networks carrying multimedia applications.

Keywords: MPLS, VPN, QoS, FIFO, PQ, WFQ.

1 INTRODUCTION

Quality of service (QoS) has emerged as a critical requirement in today's IP networks that carry a multitude of real-time multimedia applications such as voice over IP, video conferencing, live streaming, and online gaming. Users expect these latency-sensitive applications to function seamlessly without any degradation in quality. However, best-effort IP networks cannot provide any performance guarantees resulting in problems such as jitter, delays, congestion and packet loss that severely impact user experience.

Network operators urgently need solutions that can deliver differentiated quality of service for diverse application traffic flows. With the upcoming advent of 5G networks and use cases like autonomous vehicles, strict service level agreements will be needed more than ever. Multiprotocol Label Switching (MPLS) has proven to be an effective

technology for meeting end-to-end QoS requirements through advanced traffic engineering capabilities.

MPLS augments traditional IP routing and forwarding by incorporating labels into packets that define their forwarding path. This allows granular control over routing based on QoS considerations rather than just using shortest path destination-based routing. MPLS label switched paths can be set up with guaranteed bandwidth reservations using Resource Reservation Protocol (RSVP). Sophisticated queuing and scheduling mechanisms can be implemented to prioritize latency-sensitive real-time traffic over elastic data transfers.

MPLS enables differentiated classes of service where critical applications get preferential treatment over less important background traffic. Service providers use MPLS to offer QoS-enabled IP virtual private networks (VPNs) for enterprises carrying multiple types of applications. Overall, MPLS provides a comprehensive QoS framework for managing end-to-end performance guarantees across sprawling heterogeneous networks.

However, realizing the full benefits of MPLS QoS requires careful planning and configuration involving multiple interrelated components. Network engineers must size bandwidth allocations on label properly switched paths, select queuing policies, specify traffic classifications, and tune other QoS parameters. Therefore, evaluating MPLS QoS performance under different mechanisms like First-In-First-Out (FIFO), Priority Queuing, Fair Queuing through realistic network simulations is crucial.

This paper presents an extensive simulation-based investigation into the efficacy of MPLS in delivering QoS for real-time voice and data applications. Different queuing schemes are implemented and analyzed on an MPLS VPN backbone topology modeled using the OPNET tool. Performance metrics like jitter, delay, packet loss and throughput are evaluated to determine the optimal queuing configuration. The results will provide meaningful insights for network operators to properly design and deploy MPLS networks for supporting QoS-sensitive applications.

2 RELATED WORK

Quality of service (QoS) support in Multiprotocol Label Switching (MPLS) networks has been an active area of research, with several studies analyzing various mechanisms for providing differentiated service classes. Ahmed et al. (2019) [1] evaluated the performance impact of MPLS virtual private networks (VPNs) for voice over IP traffic compared to standard IP routing. Network simulations were conducted using the OPNET tool to model voice flows over an MPLS VPN backbone implementing traffic engineering. Results showed that MPLS provided significantly lower jitter, packet loss and delays than an IP network without QoS capabilities. This demonstrated the benefits of MPLS VPNs for meeting the stringent QoS demands of real-time applications.

Rikli et al. (2013) [2] implemented multiple queuing schemes like first-in-first-out (FIFO), priority queuing (PQ) and weighted fair queuing (WFQ) in an MPLS VPN topology modeled in OPNET. Various traffic types including voice, video, data were simulated to evaluate end-to-end QoS delivery. WFQ exhibited the highest network

utilization while still meeting QoS targets. However, the work did not analyze other metrics like jitter and delay. Rahimi et al. (2009) [3] developed an MPLS simulation using the J-SIM tool that implemented DiffServ-aware traffic engineering. Results showed improvements in higher throughput and lower packet drops with DiffServ-MPLS compared to standard MPLS. The work focused only on aggregate network metrics and did not assess per-flow QoS delivery.

Alkarash et al. (2017) [4] evaluated scheduling algorithms like weighted fair queuing, priority queuing and first-in-first-out in the context of MPLS-based WiMAX networks. Various performance metrics including throughput, delay and jitter were analyzed concerning video and voice traffic requirements. WFQ was concluded to be most effective in meeting QoS needs. However, MPLS VPN networks were not considered. Ema et al. (2020) [5] proposed an algorithm for dynamic MPLS traffic engineering to prevent network congestion. The technique optimized resource allocation and traffic distribution based on application needs. QoS improvements were demonstrated through simulations, but specific mechanisms were not discussed.

Saad et al. (2021) [6] conducted an OPNET-based evaluation of MPLS networks carrying multimedia traffic with different combinations of routing protocols and queuing policies. Performance metrics like jitter, delay and throughput were measured to determine optimal configurations for meeting QoS targets. However, VPN backbone topologies were not explored.

Sachdeva et al. (2002) [7] analyzed various MPLS VPN architectures for QoS delivery using discrete event simulations. The study compared backbone-based and backdoor MPLS VPNs based on metrics like packet loss, delay. Backdoor VPNs were concluded to provide superior QoS performance. Extensive queuing evaluations were not presented.

In summary, existing literature has adopted diverse techniques, including simulations, testbeds, mathematical modeling, software-defined networking and traffic engineering to evaluate and improve QoS provisioning in MPLS and MPLS VPN networks. This further motivates the need for a comprehensive investigation into MPLS queuing mechanisms for end-to-end QoS assurance across VPN backbone topologies carrying real-time multi-service traffic, as presented in this paper.

3 OVERVIEW OF MULTIPROTOCOL LABEL SWITCHING

Multiprotocol Label Switching (MPLS) evolved from a number of industry efforts to improve the Multiprotocol Label Switching (MPLS) was developed to overcome limitations of traditional IP networks and improve packet forwarding performance. In legacy IP networks, routers must perform a routing table lookup and analysis of the IP header for every packet. This can become a bottleneck as traffic volumes grow.

MPLS borrows concepts from connection-oriented networks like ATM that use fixed-length labels to forward packets. It adds a 32-bit label header to packets entering an MPLS domain. Routers within the MPLS network use this label to guide forwarding

rather than examining the IP header. This allows faster label switching through the network core.

A key advantage of MPLS is that it does not completely replace the IP layer. Rather, it works alongside existing IP routing protocols. This provides a smooth evolution path from traditional IP networks to next-generation MPLS-enabled networks [8]. Carriers can deploy MPLS in the core and still maintain compatibility with IP at the edges.

MPLS offers significant enhancements over conventional IP networks:

- Traffic Engineering - Explicit routing of LSPs based on bandwidth, latency, utilization.
- QoS Support - Priority treatment and dedicated bandwidth for critical applications.
- VPN Services - Scalable virtual private networks for enterprises.
- Convergence - Support for Layer 2 and Layer 3 services over a common infrastructure.

As packets enter an MPLS domain, the ingress router adds a label to the packet header. This label identifies the Label Switched Path (LSP) to the destination. The router strips off the incoming label at each hop and adds the appropriate outgoing label based on local label forwarding information. This allows data plane forwarding without repeated network layer lookups.

3.1 MPLS Architecture

The key components of the MPLS architecture are the control plane and data plane as shown in Figure 1.

Control Plane:

The control plane enables an MPLS network's intelligent routing and signaling functions [9]. It is responsible for:

- Exchanging routes between MPLS nodes using interior gateway protocols (IGPs) like OSPF and IS-IS.
- Distributing label bindings between adjacent routers through signaling protocols like Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP).
- Maintaining the Label Information Base (LIB) containing both locally assigned labels and remote labels learned from neighbors.
- Programming the Label Forwarding Information Base (LFIB) used for data plane forwarding.

The control plane runs complex mechanisms for exchange of routing information and labels using protocols like LDP, RSVP, OSPF, IS-IS, and BGP. This enables dynamic discovery of network topology and data plane label switching programmability.

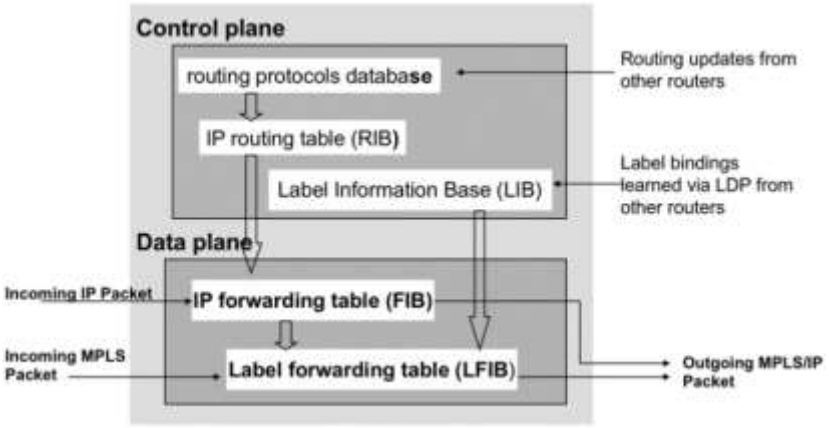

Fig. 1. MPLS Control Plane and Data Plane Components.

Data Plane:

The data plane is responsible for high-speed forwarding of packets based on MPLS label lookup [6]. Key functions include:

- Looking up incoming label value in the LFIB table downloaded from the control plane.
- Switching the packet to the appropriate output interface and replacing the label.
- Applying QoS policies like queuing and traffic shaping configured by control plane.
- Maintaining performance statistics for congestion monitoring.

The data plane uses the label value as an index into the LFIB table to retrieve the corresponding forwarding entry, rather than re-analyzing the IP header. This allows faster forwarding of labeled packets across the MPLS core. The separation between an intelligent control plane and high-speed data plane provides flexibility and scalability in MPLS networks. The control plane dynamically optimizes forwarding paths and policies. The data plane provides hardware-accelerated switching of labelled packets along label-switched paths. This enables advanced traffic engineering and QoS capabilities.

3.2 LABEL DISTRIBUTION PROTOCOL

The Label Distribution Protocol (LDP) enables MPLS routers to exchange label mapping information with peers. The main LDP messages are:

- Discovery Messages: Routers send LDP Hello messages periodically to announce their presence. These packets are transmitted to the all-routers multicast address using UDP.
- Session Messages: Used to establish and maintain LDP sessions between peers. TCP is used for reliability.

• Advertisement Messages: Carry label mappings for prefixes and exchange routing details. Propagate actual label information.
• Notification Messages: Used to provide advisory information and signal errors.

Once an LDP session is established between two routers, they can exchange label advertisements to reach all destinations in the MPLS domain. LDP provides a dynamic and adaptive mechanism for label switching.

3.3 KEY MPLS FEATURES

MPLS operates between the data link layer and the network layer, which is called layer 2.5 protocols as shown in figure 2.

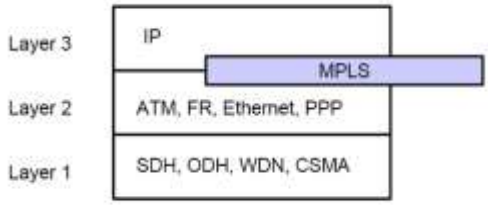

Fig. 2. MPLS Layer.

MULTIPROTOCOL SUPPORT. A key advantage of MPLS is its ability to work over diverse Layer 2 technologies like ATM, Frame Relay, Ethernet. It serves as a convergence layer over heterogeneous networks and protocols.

INCREASED PERFORMANCE. MPLS improves packet forwarding performance by avoiding repeated IP route lookups. Label switching using hardware reduces processing overhead.

EXPLICIT ROUTES. MPLS allows explicit routing of Label Switched Paths (LSPs) based on administrator policies and traffic profiles. LSPs can be precisely controlled.

TRAFFIC ENGINEERING. MPLS permits fine-grained traffic engineering based on measured link characteristics like bandwidth, latency, and traffic load. This enables dynamic load balancing and QoS optimization.

Traffic-oriented, enabled to enhance the QoS of traffic streams.

Resource-oriented, which optimizes resource utilization.

3.4 MPLS HEADER FORMAT

The MPLS header as illustrated in figure 3, has a 32-bit label stack entry that is inserted between the Layer 2 and Layer 3 headers. It contains [10]:

- 20 bit label value used for forwarding packets through the MPLS domain.

- 3 bit Class of Service (CoS) field for prioritizing traffic flows.
- 1 bit bottom-of-stack indicator identifying the final MPLS header.
- 8 bit Time-to-Live (TTL) field copied from the IP header.

The label stack allows multiple MPLS headers to implement hierarchical routing and QoS policies. The IP packet follows the final stack entry.

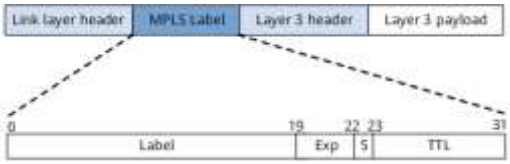

Fig. 3. MPLS label stack header format.

In summary, LDP provides dynamic label distribution and MPLS offers integration of Layer 2 and Layer 3 forwarding to improve performance, traffic engineering, and QoS capabilities. The MPLS header defines label-based switching through the network.

3.5 MPLS OPERATIONS

Multiprotocol Label Switching (MPLS) integrates Layer 2 forwarding information such as link bandwidth, latency, and utilization with Layer 3 IP routing to improve performance and Quality of Service (QoS) capabilities [10]. The core concept behind MPLS networks is establishing Label Switched Paths (LSPs) between ingress and egress routers as shown in figure 4. As packets enter the MPLS domain, they are assigned labels that determine their forwarding path [11]. The incoming IP packets are mapped to an LSP based on routing and QoS considerations at the ingress router. The router adds a 32-bit MPLS header containing the 20-bit label value corresponding to the selected path. Interior Gateway Protocols like OSPF are used to build the routing and labeling information.

Each router analyzes the label value to determine the next hop as the packet travels through the MPLS core. The router replaces the incoming label with the appropriate outbound label and forwards the packet. This allows data plane forwarding using simple table lookups rather than repeated analysis of the IP header [12]. The mapping between incoming and outgoing labels is constant across routers along an LSP. Therefore, the label values dictate the end-to-end forwarding path traversed by packets. MPLS assigns labels to represent groups of IP prefixes sharing the same path i.e. a Forwarding Equivalence Class (FEC).

MPLS allows explicit routing of LSPs based on administrator policies and traffic profiles [13][14]. The control plane can specify loose or strict hop-by-hop paths to meet requirements. Traffic engineering principles can be applied to balance load and optimize QoS. The QoS parameters assigned to an LSP determine the resources committed to it and the forwarding behavior [15]. Bandwidth can be reserved using RSVP. Queuing policies like priority, weighted fair queuing, traffic shaping can be configured. Admission control mechanisms may be employed.

At the MPLS egress, the label is removed, revealing the original IP packet for forwarding. The end-to-end LSP forwarding is defined only by the MPLS labels, achieving separation from IP routing. This allows seamless integration of Layer 2 and Layer 3 services over the converged MPLS core [9].

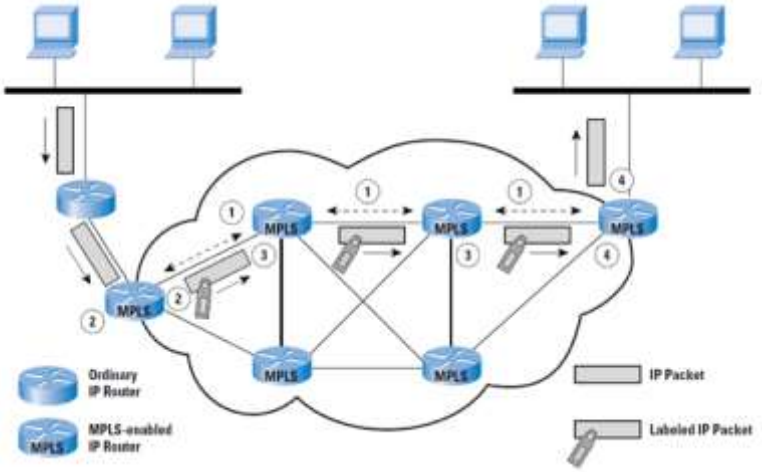

Fig. 4. MPLS Path Creation and Packet Forwarding.

In summary, MPLS uses label switching along predefined LSPs to simplify and accelerate network packet forwarding. This enables advanced traffic management, QoS guarantees, and service integration not possible with traditional IP networks.

4 MPLS VIRTUAL PRIVATE NETWORK (MPLS VPN)

MPLS Virtual Private Networks (VPNs) are a widely deployed application of MPLS technology. MPLS VPNs allow service providers to offer multiple customers private and isolated network connectivity over a shared common infrastructure. This provides benefits such as security, flexibility, scalability and reduced costs. MPLS VPNs overcome limitations of traditional IPSec VPNs which require complex full-mesh topologies to interconnect sites. MPLS VPNs only require single-point configuration changes to add new customer sites. This significantly reduces overhead for providers and enterprises [16]. In an MPLS VPN, Customer Edge (CE) routers connect to Provider Edge (PE) routers using standard routing protocols like OSPF or BGP. The CE devices are unaware of the VPN - the virtualization is managed transparently by the provider's MPLS network [17]. PE routers run Multiprotocol BGP (MP-BGP) to exchange customer VPN routes. This propagates VPN reachability information across the MPLS backbone. The core MPLS network performs label switching to forward customer traffic through label switched paths (LSPs) [18].

MPLS VPNs allow logical isolation and segmentation of traffic belonging to different customers over the shared infrastructure. Traffic from one customer's VPN cannot

reach another customer's VPN without explicit configuration. MPLS VPNs support advanced traffic engineering capabilities. Customer traffic can be load balanced between multiple LSPs based on measured link characteristics [19]. Latency, jitter and loss can be optimized by dynamic routing. In traditional IP networks, all traffic uses shortest path routing based on static link metrics. This can lead to congestion on certain links while others remain underutilized. MPLS traffic engineering provides greater flexibility. MPLS VPNs allow service providers to offer customers private, isolated, virtualized networks in a scalable and cost-efficient manner. The combination of MPLS traffic engineering and VPN services drives widespread adoption in carrier networks.

5 QUEUING TYPE

Queuing and scheduling are vital in providing Quality of Service (QoS) guarantees in MPLS networks. Queues buffer packets while schedulers determine the service order and allocate bandwidth between traffic classes [11]. Queuing mechanisms help regulate traffic flows to conform to contracted rates and minimize congestion [20]. Schedulers prioritize delay-sensitive real-time traffic over elastic traffic based on configured forwarding classes [21]. Bandwidth shaping using queues constrains traffic to avoid oversubscription of resources. Queuing introduces a deliberate delay to smooth out bursts and block non-conformant flows. At the same time, queue delays must be limited to meet application requirements.

Schedulers service high-priority queues first before lower-priority queues to ensure low latency for critical traffic. Schedulers also divide available bandwidth between queues based on weights and fair allocation policies. Common queuing and scheduling options include [22]:

This paper implements and evaluates the performance of FIFO, PQ and WFQ schemes in MPLS networks carrying voice and data traffic. The results will quantify metrics like jitter, delay, loss and throughput to determine the optimal queuing strategy. Queuing and scheduling are essential mechanisms to deliver differentiated QoS services by managing buffering delays and prioritizing forwarding treatment of MPLS traffic flows. Advanced queuing can ensure guaranteed low latency for real-time applications and fair distribution of excess bandwidth.

5.1 FIRST IN FIRST OUT (FIFO)

First in First out (FIFO) is the simplest queuing technique that buffers and forwards packets purely based on arrival order without any concept of priority or traffic classification [22]. FIFO queues treat all incoming packets equally in the same manner. The first packet entering the queue is the first to be transmitted. FIFO does not provide any inherent quality of service capabilities. However, it offers low complexity while avoiding out-of-order packet issues.

5.2 PRIORITY QUEUING (PQ)

Priority queuing (PQ) classifies incoming traffic packets into predefined priority classes [22]. Packets belonging to higher priority traffic classes get scheduled for transmission ahead of all lower priority packets queued in the system. By servicing them first, PQ ensures minimum delays and loss for high priority flows. However, lower priority queues can suffer starvation under congestion and may not meet QoS targets. PQ is not bandwidth aware and does not provide fair allocation between traffic classes.

5.3 WEIGHTED FAIR QUEUING (WFQ)

Weighted fair queuing (WFQ) schedules packet transmission from queues based on configured weights to provide fair bandwidth sharing [22]. WFQ allocates a percentage of link capacity to each queue proportional to its weight. Larger flows that send more traffic get higher weight allocations. This prevents bandwidth hogging issues with FIFO. WFQ interleaves packets from different flows and provides latency benefits for interactive traffic and fair bandwidth distribution. However, computing weighted service order introduces processing overhead.

5.4 MPLS QUEUING FOR QOS

Queuing techniques like priority and fair queuing are essential in MPLS networks to meet quality of service requirements [23]:

- Latency sensitive applications like VoIP demand priority queues to minimize jitter.
- Fair queuing prevents congestion and provides equitable bandwidth sharing between traffic classes.
- Queue buffering smooths traffic bursts and enforces bandwidth limits.

Advanced MPLS queuing mechanisms allow carriers to offer differentiated service classes with guarantees on metrics like delay, jitter and loss.

6 SIMULATION and RESULTS

6.1 *SIMULATION SCENARIO* and CONFIGURATION

To evaluate the performance of MPLS VPNs, a network topology is simulated using the OPNET 14.5 tool as shown in figure 5. The goal is to analyze MPLS VPN behavior concerning metrics like delay, throughput and traffic load under different conditions. The network comprises two customer sites connected over an MPLS VPN backbone implemented using BGP and label switching. PE routers represent provider edge devices connected to customer edge routers labelled CE. Two key applications are configured over the VPN - voice and data. Additionally, background traffic like HTTP, FTP and video are configured to emulate real-world conditions with multiple application flows sharing the network.

A layer 3 MPLS VPN is created between the sites by specifying the PE-CE interfaces and configuring a common route-target. BGP handles routing and exchanges VPN routes between PEs. The P routers form the MPLS-enabled core. Key metrics collected include VPN delay, VPN traffic load, and throughput for voice and data flows. The performance impact of factors like queuing policies, routing protocols and traffic profiles will be analyzed.

The OPNET simulator allows the modeling of complex MPLS VPN networks carrying heterogeneous application traffic. Detailed performance statistics can be measured under varied configurations to identify optimal operating conditions and bottlenecks. The simulations will provide a meaningful characterization of how MPLS VPNs behave for real-time and data applications. The results will quantify the quality-of-service delivery to support carrier-grade voice and multimedia services.

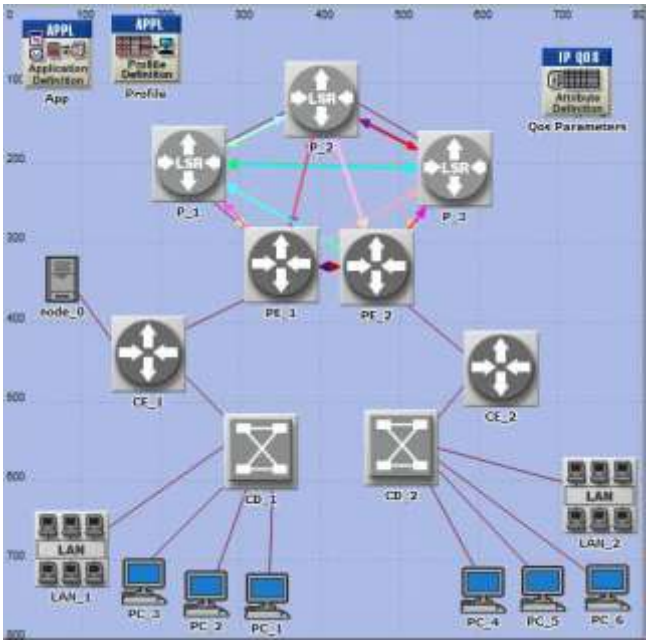

Fig. 5. OPNET network topology for MPLS VPN simulation.

To evaluate MPLS VPN QoS capabilities, VoIP traffic is generated across the MPLS backbone with IP QoS enabled. The interior gateway protocol used for routing is OSPF.

Different queuing schemes are applied including Priority Queuing (PQ), First-In-First-Out (FIFO) and Weighted Fair Queuing (WFQ). Each queuing policy is configured in a separate simulation run for performance comparison. The simulation results are analyzed to determine how the MPLS VPN network behaves under different queuing mechanisms when carrying VoIP traffic. Key metrics assessed are jitter, delay, packet loss and throughput to quantify QoS delivery.

The mix of real-time VoIP and data traffic over the MPLS VPN backbone with configurable queuing allows comprehensive evaluation of quality of service. Prioritization

schemes like PQ aim to minimize jitter and delays for voice calls. FIFO provides simple buffering while WFQ enables fair bandwidth allocation. The simulations will demonstrate how proper configuration of queuing policies following application needs can enable MPLS networks to meet stringent QoS requirements for modern IP-based multimedia services.

Table 1. Simulation Parameters.

Simulation Parameter	Value
Network Workspace	800 X 800 m
Application Configuration	1
Profile Definition	1
Fixed Server	1
Router	2
Router LSR	3
Router LER	2
Switch	2
LAN	2
PC	6

Different queuing schemes are applied including Priority Queuing (PQ), First-In-First-Out (FIFO) and Weighted Fair Queuing (WFQ). Each queuing policy is configured in a separate simulation run for performance comparison. The simulation results are analyzed to determine how the MPLS VPN network behaves under different queuing mechanisms when carrying VoIP traffic. Key metrics assessed are jitter, delay, packet loss and throughput to quantify QoS delivery.
The mix of real-time VoIP and data traffic over the MPLS VPN backbone with configurable queuing allows comprehensive evaluation of quality of service. Prioritization schemes like PQ aim to minimize jitter and delays for voice calls. FIFO provides simple buffering while WFQ enables fair bandwidth allocation. The simulations will demonstrate how proper configuration of queuing policies in accordance with application needs can enable MPLS networks to meet stringent QoS requirements for modern IP-based multimedia services.

6.2 RESULTS OF COMPARING MPLS VPN QUEUES (FIFO, PQ, WFQ)

JITTER. The FIFO queue exhibited the lowest jitter of 0.29 ms compared to WFQ (0.36 ms) and PQ (0.52 ms) as it transmits packets in arrival order without scheduling delays. All queuing schemes achieved jitter within 1 ms target for good voice quality as per ITU standards, as shown in figure 6.

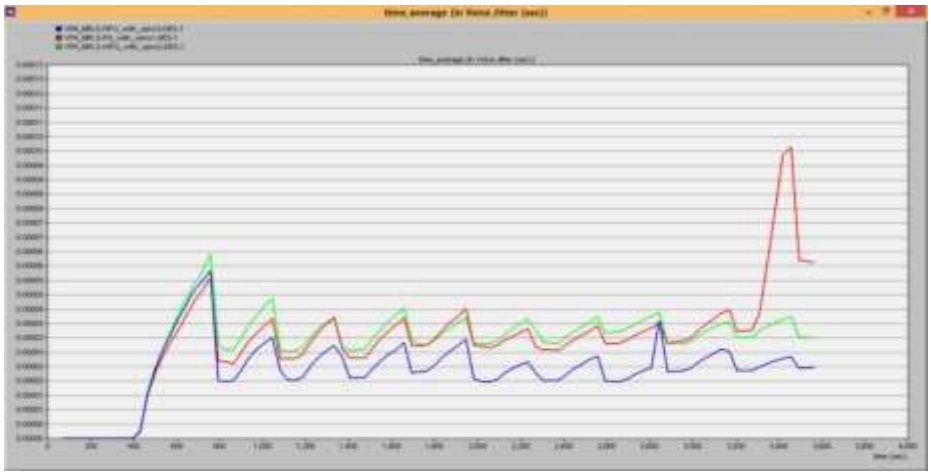

Fig. 6. Voice Jitter (sec).

PACKET DELAY VARIATION. Again, FIFO queuing showed the lowest delay variation of 0.148 ms followed closely by WFQ and PQ which were also within requirements. FIFO's simple first-in first-out buffering prevents variation, as shown in figure 7.

Fig. 7. Packet Delay Variation (sec).

PACKET END-TO-END DELAY. In the preliminary findings, it was observed that PQ exhibited greater delays in comparison to FIFO and WFQ. However, as time progressed, these delays gradually converged to a consistent range of 75 to 79 milliseconds, ultimately meeting the established threshold of 150 milliseconds, as illustrated in

figure 8. Notably, FIFO's implementation of fair buffering played a pivotal role in maintaining the lowest end-to-end delays among all the examined queues. This finding underscores the effectiveness of FIFO in managing and minimizing delays, thereby contributing to the efficient operation of the system.

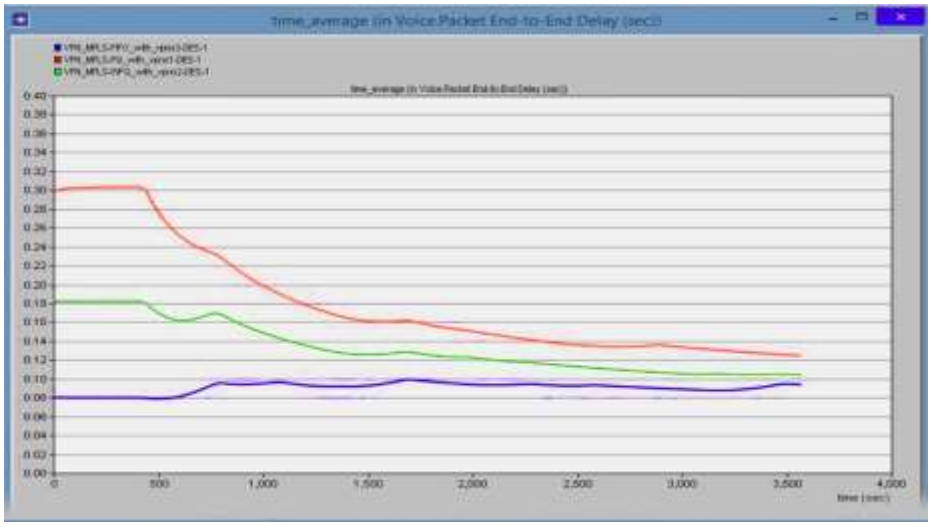

Fig. 8. Packet End-to-End Delay (Sec).

TRAFFIC SENT. The queues received identical traffic loads, ensuring a consistent input for evaluation. In terms of traffic reception rates, as shown in figure 9, FIFO emerged as the leader, achieving the highest rate at 97.26 packets per second, followed by WFQ and PQ. FIFO's superiority in this aspect can be attributed to its efficient handling of scheduling delays, allowing for the maximization of packet delivery rates. This outcome highlights the advantage of using FIFO in scenarios where rapid and uninterrupted packet transmission is of paramount importance, ultimately contributing to improved network performance.

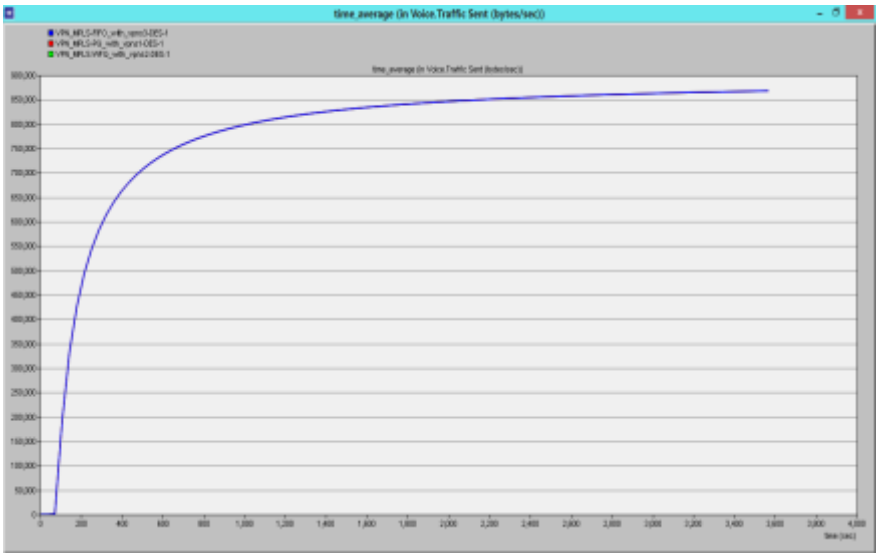

Fig. 9. Traffic sent (Packet/Sec).

TRAFFIC RECEIVED. In the context of email traffic, it was observed that there were minimal differences in both the sent and received traffic volumes across all queuing schemes as shown in figure 9 and figure 10. These minor variations aside, the email traffic patterns remained largely consistent across the different queuing methods. This finding underscores the notion that data applications, such as email, are generally less susceptible to the effects of jitter and delays when compared to voice traffic. Data applications are inherently more forgiving when it comes to variations in network performance, making them less sensitive to fluctuations in packet delivery times, which is a critical consideration in scenarios involving real-time communication like voice transmissions.

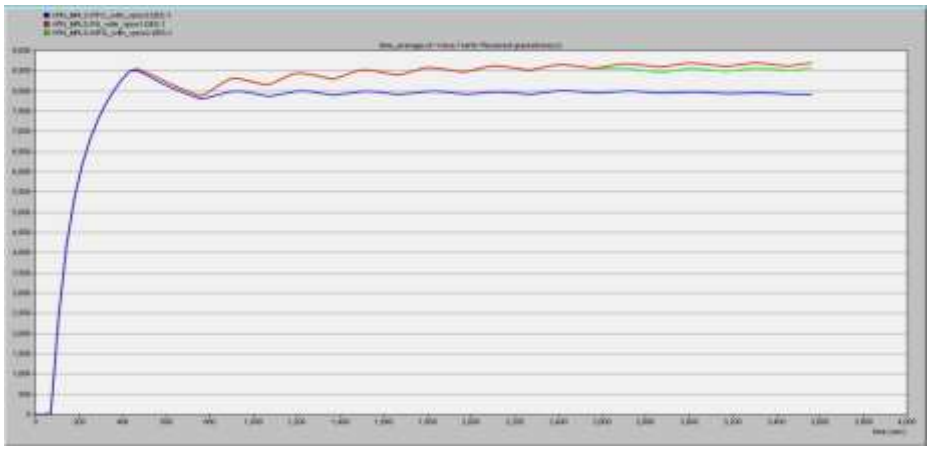

Fig. 10. Traffic Receive (packet/sec).

And they are all within range of the average quality of voice according to the International Telecommunications Union (ITU).

6.3 COMPARISON BETWEEN EMAIL QUEUES (FIFO, PQ, WFQ)

TRAFFIC SENT. In all three scenarios, initial observations yielded identical results for the rate of Traffic Sent. Subsequently, when evaluating the performance of FIFO, PQ, and WFQ, it became evident that they produced fairly similar outcomes, with only minor deviations discernible between them, as shown in figure 11.

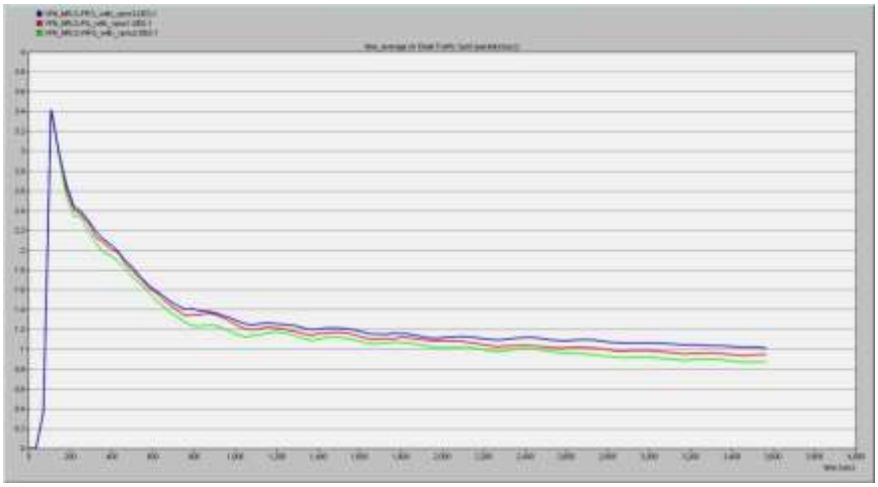

Fig. 11. email traffic sent(packets/sec).

TRAFFIC RECEIVED. Initially, the three scenarios produced identical results for the rate of Traffic Receive. However, upon further examination, it was evident that FIFO, PQ, and WFQ demonstrated relatively similar outcomes, with only slight variations between them, as shown in figure 12.

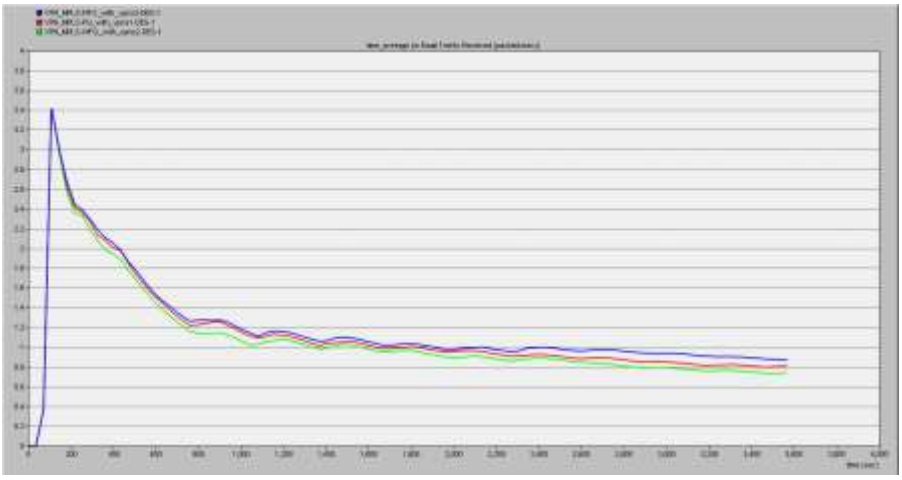

Fig. 12. email traffic received (packets/sec).

The simulation outcomes yield several noteworthy observations regarding MPLS VPN queuing mechanisms:

- FIFO queuing stands out as the top performer for real-time voice traffic, as it adheres to packet order of arrival without introducing scheduling delays.
- WFQ also demonstrates its capacity to meet QoS criteria thanks to equitable bandwidth allocation and the interleaving of voice packets.
- PQ, on the other hand, leads to increased jitter and delays, primarily due to potential blocking of high-priority packets behind lengthy lower-priority queues.
- All queuing strategies effectively adhere to ITU standards for ensuring superior voice quality in terms of jitter, delay, and packet loss.
- In the context of data applications like email, all queuing policies showcase comparable performance levels.
- It's advisable to employ traffic engineering concepts to evenly distribute voice traffic across multiple Label Switched Paths (LSPs).

The simulations underscore the significance of appropriately configuring queuing policies within MPLS VPN networks to fulfill the demanding Quality of Service (QoS) demands of contemporary IP-based multimedia applications. FIFO emerges as a favorable approach for prioritizing voice traffic, while maintaining a simplified architecture. WFQ, on the other hand, demonstrates commendable fairness and delay characteristics. In contrast, PQ necessitates meticulous setup to mitigate excessive jitter. These findings

empower network operators to craft MPLS VPN networks that efficiently deliver carrier-grade voice services and Service Level Agreements (SLAs) to enterprise clients. The study quantifies the impact of queuing trade-offs, balancing complexity, latency, and fairness considerations.

7 Conclusion

This paper presented a comprehensive evaluation of MPLS VPN queuing mechanisms using simulations in OPNET. Different schemes including FIFO, Priority Queuing and Weighted Fair Queuing were implemented and analyzed for a network carrying Voice over IP and data traffic. The performance was assessed across multiple metrics like jitter, delay, loss and throughput to quantify the quality-of-service delivery. The results demonstrated that basic FIFO queuing provides the optimal solution for real-time voice traffic as it transmits packets in arrival order avoiding scheduling delays.
However, FIFO does not prevent bandwidth hogging which can be mitigated using fair queuing schemes like WFQ that allocate bandwidth based on weights. WFQ also delivers excellent QoS results close to FIFO. Strict priority queuing exhibits higher jitter as high priority voice packets can get stuck behind large queues. The key conclusions are that MPLS VPN technology and appropriate queuing mechanisms can enable carriers to offer enterprise-grade SLAs for delay-sensitive voice services. MPLS VPNs simplify network operations with scalable site-to-site connectivity and built-in QoS capabilities. FIFO emerges as the recommended queuing technique for voice-centric MPLS VPNs as it minimizes jitter while being simple to implement without per-flow scheduling. WFQ may be warranted for multifold networks to prevent congestion. The study provides meaningful insights for configuring and optimizing MPLS VPN QoS performance using queuing.

References

1. Ahmed, N., & Tareen, A. (2019). MPLS-VPN impact on VOIP QoS. International Journal of Computer Trends and Technology, 67(12), 8-14.
2. Rikli, N. E., & Almogari, S. (2013). Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks. Journal of King Saud University-Computer and Information Sciences, 25(1), 89-98.
3. Rahimi, M., Hashim, H., & Rahman, R. A. (2009). Implementation of quality of service in multi-protocol label switching networks. In 5th International Colloquium on Signal Processing & Its Applications (CSPA 2009), pp. 98-103, IEEE.
4. Elkarash, H. H., Elshennawy, N. M., & Saliam, E. A. (2017). Evaluating QoS using scheduling algorithms in MPLS/VPN/WiMAX networks. In 13th International Computer Engineering Conference (ICENCO), pp. 14-19.
5. Gales, E. M., & Croitoru, V. (2020). Traffic engineering and QoS in a proposed MPLS-VPN. In International Symposium on Electronics and Telecommunications (ISETC), pp. 1-4.
6. Saad, R. A., Msaad, M. A., & Sllame, A. M. (2021). Performance evaluation of multimedia streaming applications in MPLS networks using OPNET. In IEEE 1st International Maghreb

Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), pp. 333-338.
7. Awduche, D., Chiu, A., Elwalid, A., Widjaja, I., & Xiao, X. (2002). Overview and principles of Internet traffic engineering. RFC 3272.
8. Fortz, B., Rexford, J., & Thorup, M. (2002). Traffic engineering with traditional IP routing protocols. IEEE Communications Magazine, 40(10), 118-124.
9. Rosen, E., Viswanathan, A., & Callon, R. (2001). Multiprotocol label switching architecture. RFC 3031.
10. Farrel, A., Vasseur, J. P., & Ash, J. (2006). A path computation element–based architecture for interdomain MPLS and GMPLS traffic engineering. RFC 4655.
11. Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M., & McManus, J. (1999). Requirements for traffic engineering over MPLS. RFC 2702.
12. Le Faucheur, F., & Lai, W. (2003). Requirements for support of differentiated services-aware MPLS traffic engineering. RFC 3564.
13. Shenker, S., Partridge, C., & Guerin, R. (1997). Specification of guaranteed quality of service. RFC 2212.
14. Shenker, S., & Wroclawski, J. (1997). General characterization parameters for integrated service network elements. RFC 2215.
15. Babiarz, J., Chan, K., & Baker, F. (2006). Configuration guidelines for DiffServ service classes. RFC 4594.
16. Lapukhov, P., Premji, A., & Mitchell, J. (2016). Use of BGP for routing in large-scale data centers. RFC 7938.
17. Patel, K., Aboba, B., Kelly, S., & Gupta, V. (2003). Dynamic host configuration protocol (DHCPv4) configuration of IPsec tunnel mode. RFC 3456.
18. Rosen, E., & Rekhter, Y. (2006). BGP/MPLS IP virtual private networks (VPNs). RFC 4364.
19. Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., & Heinanen, J. (2002). Multiprotocol label switching (MPLS) support of differentiated services. RFC 3270.
20. Heinanen, J., & Baker, F. (1999). Assured forwarding PHB group. RFC 2597.
21. Jacobson, V., Nichols, K., & Poduri, K. (1999). An expedited forwarding PHB. RFC 2598.
22. Demichelis, C., & Chimento, P. (2002). IP packet delay variation metric for IP performance metrics (IPPM). RFC 3393.
23. Blake, S., Black, D., Carlson, M., Davies, E., & Wang, Z. (1998). An architecture for differentiated services. RFC 2475.

تقييم استراتيجيات إدارة الانتظار لتحسين جودة الخدمة في شبكات تبديل المؤشرات متعددة البروتوكولات الافتراضية

محمود منصور[1] ، أحمد صمود[1] ، ناجية بن سعود[1]
[1] جامعة طرابلس ، كلية تقنية المعلومات
bensaoud.najia@gmail.com

الملخص: برزت تقنية تبديل المؤشرات متعددة البروتوكولات (MPLS) كتقنية رئيسية لتوفير ضمانات جودة الخدمة (QoS) في شبكات IP. تقدم هذه الورقة تقييماً شاملاً قائماً على المحاكاة لآليات جودة الخدمة في MPLS. على وجه التحديد، تم تنفيذ وتحليل سياسات انتظار مختلفة –الداخل أولاً خارج أولاً (FIFO) ، والانتظار ذو الأولوية (PQ) ، والانتظار العادل الموزون – (WFQ) لتوفير جودة خدمة شاملة للتطبيقات الصوتية والبيانات عبر شبكة VPN باستخدام MPLS. تم إجراء محاكاة الشبكة باستخدام أداة OPNET مع تكوين تفصيلي لمعلمات MPLS و VPN والانتظار. تم تقييم الأداء عبر العديد من المقاييس بما في ذلك الارتعاش، وتباين التأخير، والتأخير الشامل، وحركة المرور المرسلة / المستلمة لكل من تدفقات الصوت والبيانات. تُظهر النتائج أن انتظار FIFO يوفر أفضل أداء لجودة الخدمة لحركة مرور الصوت، مما يوفر تخزين مؤقت بسيط للدخول الأول والخروج الأول. وقد ثبت أن WFQ يتفوق على PQ لتدفقات الصوت. يمكن لجميع آليات الانتظار تلبية متطلبات جودة الخدمة لتطبيقات الصوت والبيانات. توفر الورقة تحقيقًا شاملاً في تكوين شبكات MPLS مع قدرات جودة الخدمة. تُظهر النتائج الرئيسية أن شبكات MPLS VPN تقلل بشكل فعال من تعقيد الشبكة والتكاليف. يظهر FIFO كتقنية انتظار مثلى لتمكين خدمات جودة الخدمة في شبكات MPLS التي تحمل تطبيقات الوسائط المتعددة.

الكلمات المفتاحية : تبديل المؤشرات متعددة البروتوكولات، الشبكات الخاصة الافتراضية، جودة الخدمة، الداخل أولاً خارج أولاً، الانتظار ذو الأولوية ، الانتظار العادل الموزون.