Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 2, May, Pp. 161-174

Performance evaluation of outgoing interface selection method on fortigate SD-WAN for network optimization

Mufti Kholil Romadhoni[1], Larynt Sawfa Kenanga[1], Denar Regata Akbi[*1], Diah Risqiwati[1]
Universitas Muhammadiyah Malang, Indonesia[1]

Article Info

Keywords:
SD-WAN, Outgoing Interface, Bandwidth Optimization, Network Latency, Network Stability

Article history:
Received: September 13, 2024
Accepted: December 11, 2024
Published: May 31, 2025

Cite:
M. Kholil Romadhoni, L. S. Kenanga, D. R. Akbi, and D. Risqiwati, "Performance Evaluation of Outgoing Interface Selection Method on Fortigate SD-WAN for Network Optimization", *KINETIK*, vol. 10, no. 2, May 2025.
https://doi.org/10.22219/kinetik.v10i2.2120

*Corresponding author.
Denar Regata Akbi
E-mail address:
dnarregata@umm.ac.id

Abstract

Reliable and high-performance network services are essential to facilitate communication between parent companies and subsidiaries as well as among the subsidiaries themselves. Challenges arise in managing and optimizing outgoing interface selection in an effective and reliable Software-Defined Wide Area Network (SD-WAN) environment. This research evaluates four outgoing interface selection methods, namely Manual, Best Quality, Lowest Cost, and Maximize Bandwidth (SLA), using a tree-based network topology simulated in GNS3 with FortiGate devices as part of the simulation. The results show that under simulated disturbances, such as limiting a single connection line to 10 kbps, the Manual, Best Quality, and Lowest Cost methods perform worse than the Maximize Bandwidth method. In contrast, the Maximize Bandwidth method outperformed the others, achieving only 0% packet loss, 22.275 ms one-way delay, and 7.03 ms jitter, while maintaining the ITU-T G.1010 standard at the preferred level. These findings highlight the reliability and effectiveness of the Maximize Bandwidth method in ensuring consistent data transmission even under fault conditions, while providing practical guidance for network engineers in configuring SD-WAN for uninterrupted high-quality network services in complex business environments.

1. Introduction

The technology ecosystem has triggered fundamental changes in the way businesses operate [1]. This demands the adoption of advanced technologies and more efficient operational management [2]. Companies, both at national and international scale, are now facing an urgent need to connect headquarters with their branches spread across different regions through reliable Wide Area Network (WAN) links [3][4][5]. Along with the rapid development of cloud computing technology, enterprises are now turning to cloud computing, which demands the availability of reliable and high-performance networks, similar to the need for the internet at home [6][7]. Previously, companies used traditional local networks such as Local Area Networks (LAN) known as Multiprotocol Label Switching (MPLS) for communication between branches [8][9][10]. Traditional networks have constraints in infrastructure maintenance that require high costs, management complexity, and limitations in terms of flexibility and scalability [8][11]. This makes it less effective in meeting modern needs. So, in an effort to improve connectivity and operational efficiency, companies are starting to utilize more modern infrastructure such as Software-Defined Wide Area Network (SD-WAN) [1][3][12][13]. SD-WAN offers the ability to manage various connection types more efficiently and flexibly, reduce operational costs, and improve overall network performance and security. SD-WAN provides a comprehensive solution for managing distributed networks in a more sophisticated and efficient way [14][15][16]. This technology supports a strong redundancy strategy by utilizing many outgoing interfaces, thus ensuring continuity and high availability of services [17][18].

In its application, SD-WAN offers several options for determining the optimal outgoing interface, as seen in the outgoing interface selection strategy, which includes Manual, Best Quality, Lowest Cost (SLA), and Maximize Bandwidth (SLA) options [19]. These options allow companies to customize network settings according to their specific needs, be it to prioritize the best quality, lowest cost, or maximize bandwidth while still meeting SLA (Service-level Agreement) targets. With this flexibility, SD-WAN is able to provide better network performance, reduce latency, and improve end-user experience while reducing operational costs that often become an obstacle in managing traditional networks. The proper SD-WAN implementation can be the key to success in facing operational and technical challenges in the modern business world. We hypothesize that the Maximize Bandwidth method will outperform other interface selection methods (Manual, Best Quality, Lowest Cost) in terms of performance and stability across various network conditions. This hypothesis will be evaluated through comprehensive experiments in various SD-WAN scenarios.

The selection of outgoing interfaces in an SD-WAN system is one of the main challenges in managing network performance. This issue is also experienced by PT XYZ, a company that uses the FortiGate platform to manage network traffic. This challenge is often faced by network engineers, who must determine the best method among several outgoing interface options available. This condition highlights the importance of developing solutions that can effectively optimize network performance in various operational scenarios. Studies related to outgoing interface selection methods on the FortiGate platform have not been discussed in depth in the available literature. As a reference, this research refers to the documentation available from Fortinet, which includes configuration guidelines and interface selection strategies in the context of SD-WAN networks [20]. The documentation describes several modes of SD-WAN rules for determining interface priorities, namely Best Quality, Lowest Cost (SLA), and Maximize Bandwidth (SLA), each with a different approach to selecting the optimal interface for a particular type of traffic [20].

Each outgoing interface option has unique characteristics that affect network performance, such as packet loss, jitter, and latency [21]. In this study, the authors constructed a corporate network topology with two branches and implemented a structured test scheme to evaluate each outgoing interface option. Through these tests, the authors sought to identify the option that provided the best performance under various operational conditions. By comparing the performance of each outgoing interface, the company can make more informed decisions about their network configuration, which in turn can significantly improve the quality of service. This analysis provides insight into how to optimally utilize SD-WAN to meet a company's specific needs, as well as ensuring that network resources are used efficiently. The results of this comparison are expected to help companies choose the most effective SD-WAN strategy, thereby improving network reliability and performance in an increasingly distributed and dynamic business environment. Literature studies show various advantages of SD-WAN, such as increased operational efficiency through centralized management, reduced operational costs by combining different types of connections, and greater flexibility in network traffic management [7][22]. In addition, SD-WAN is able to provide better connectivity by optimizing the use of available paths, reducing latency, and increasing overall throughput [23]. SD-WAN implementation not only improves network performance but also strengthens security by using integrated Next-Generation Firewall (NGFW) devices [23][24][25]. In addition to offering SD-WAN features such as path management and traffic optimization, these devices are also equipped with firewalls, traffic shaping, and load balancing capabilities, all of which contribute to more comprehensive network protection [26][27]. Thus, enterprises can achieve optimal network performance, reduce downtime, and ensure service continuity, all of which are crucial in an increasingly competitive and technology-oriented business environment [28].

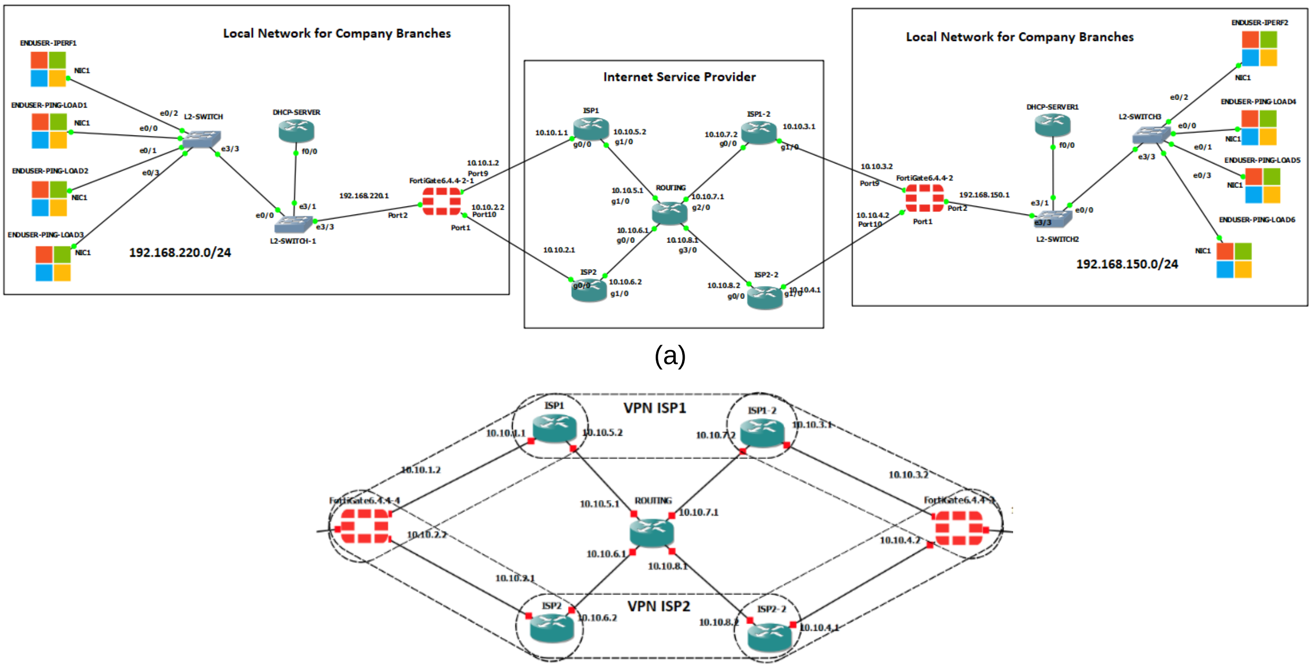
Previous research comparing data transfer performance during business hours on MPLS, EoIP, and SD-WAN networks shows that although EoIP provides better results than SD-WAN and MPLS, performance in terms of packet loss in all three methods still requires improvement [8]. The ITU-T G.1010 standard emphasizes that the ideal packet loss rate is zero to support performance targets for data applications [29]. Additionally, the standard highlights other key performance metrics, such as availability and error rate, which are critical for ensuring continuous service and maintaining data integrity. However, previous test results show that neither MPLS, EoIP, nor SD-WAN has been able to achieve this standard under high load conditions during business hours [8].

The study did not specifically mention the use of specific outgoing interfaces or the outgoing interface selection method applied in the test, thus providing an opening for updates in this study [8]. Further test results show that EoIP is slightly better than SD-WAN under certain conditions, but this technology is only suitable for specialized networks with manual redundancy [8]. Meanwhile, MPLS is often considered superior to new technologies such as SD-WAN and EoIP in some aspects, especially in terms of stability and reliability [8]. However, with the rapid growth of cloud computing and the need for flexible networks, high-cost transmission media such as MPLS are expected to become obsolete, mainly due to their lack of cost efficiency and flexibility compared to modern solutions such as SD-WAN [8].

This research seeks to optimize the use of SD-WAN in enterprises with multiple branches, focusing on determining the most effective outgoing interface configuration. While several studies have shown the superiority of MPLS in certain aspects, this research aims to confirm that SD-WAN can be optimized to deliver superior performance in complex and widespread enterprise network scenarios. As such, this research provides practical guidance for maximizing the potential of SD-WAN, especially when it comes to overcoming the challenges that arise in a dynamic digital environment. Through in-depth analysis and comparison of various outgoing interface configurations, this research is expected to provide better insight into the effect of interface choice on network performance. In addition, this research also focuses on identifying best practices in SD-WAN management for enterprises to achieve an optimal balance between cost, performance, and network reliability. With efficient and effective implementation guidelines, this research aims to assist companies in making the right strategic decisions to maximize the potential of SD-WAN and improve business operations. Ultimately, the contribution of this research lies in recommending the most effective interface selection method based on data analysis of the research results, which can achieve zero packet loss rate in accordance with the ITU-T G.1010 standard. In this way, this research is expected to improve the overall reliability of the network while providing practical solutions for companies adopting or looking to enhance their SD-WAN network management strategies.

2. Research Method

Experiments were conducted in a virtual environment using GNS3 (Graphical Network Simulator-3) [30] virtualization by applying tree topology to the network architecture design. The network consists of 5 routers, 2 Fortigate virtual machines (VMs) [31], 4 Layer 2 switches, 2 DHCP servers, and 8 virtual PCs with Windows 10 operating systems. Each switch is configured using switchport mode access to connect endpoint devices to the network. The routing method used on all five routers is Routing Information Protocol (RIP), which allows the exchange of routing information between routers dynamically, following the principle that the distribution of data packets in a computer network requires a rule or protocol that will affect network performance in distributing data packets [32][33]. Network performance was tested using iPerf3 to simulate large file transfers and ICMP ping tests with a payload size of 1000 bytes specified using a parameter of 1000 to measure latency, jitter, and packet loss. In addition, IPsec VPN tunnels were implemented between ISP1 and ISP2 to ensure the security and confidentiality of data transmitted across the network [34]. The IPsec VPN protocol employs encryption and authentication mechanisms to safeguard communication, preventing unauthorized access and maintaining data integrity [34]. Fortigate devices efficiently manage these VPN tunnels, providing features such as automated failover and robust traffic monitoring to ensure optimal security and performance in the SD-WAN environment. Two VPN tunnels are implemented through ISP1 and ISP2 for data transmission between locations. The network topology used can be seen in Figure 1 below.



(a)

(b)

Figure 1. Network Topology with 2 Company Branches and VPN Architecture on ISP1 and ISP2

The integration of Software-Defined Networking (SDN) with Virtual Private Networks (VPN) creates a significant synergy in network management, particularly in the context of Wide Area Networks (WAN) [35]. With SDN, network management becomes more centralized, allowing network administrators to configure and manage VPNs from a single control point, reducing complexity and improving efficiency [35]. The flexibility in resource allocation enables administrators to adjust the location and configuration of VPN gateways based on specific needs, such as latency or bandwidth [35]. Additionally, SDN facilitates better service orchestration, where traffic can be automatically redirected to the most optimal interface based on current network conditions, enhancing performance and efficiency in outgoing interface selection [35].

The scenarios used in this research (Manual, Best Quality, Lowest Cost, and Maximize Bandwidth) were designed based on the operational framework of PT. XYZ as the primary case study of this research. PT. XYZ faces significant challenges in selecting the optimal outgoing interface due to geographically dispersed branches requiring a high-quality and reliable network connection. The scenarios chosen represent commonly applied configurations in corporate environments where organizations strive to balance performance, cost, and reliability. Furthermore, the topological design aligns with previous studies, which utilize similar hierarchical topologies for testing SD-WAN systems [3][8]. Additionally, previous studies also share a comparable topology but do not detail outgoing interface selection [12].

Despite the existence of prior studies, none have specifically addressed the impact of different outgoing interface methods in real-world FortiGate SD-WAN implementations. In practice, network engineers, particularly at PT. XYZ often struggle to determine the most suitable outgoing interface from the four available options in FortiGate. This lack of clarity frequently leads to suboptimal choices, where the selected method does not align with the required service characteristics. For instance, choosing the Manual method for a service requiring high availability can result in network failures, as Manual mode lacks automatic failover capabilities. Consequently, critical services relying on the failed line would be disrupted entirely. These observations underscore the practical importance of evaluating the performance of these outgoing interface options to guide network engineers in making informed decisions that optimize network reliability and performance.

This study examines the effectiveness of various outgoing interfaces in managing SD-WAN to achieve an optimal balance between cost, performance, and network reliability. Experiments were conducted in four different scenarios to measure network performance. In Scenario 1, the experiment involves the use of iperf3 to simulate sending large files between one virtual PC acting as a client on the right side and one virtual PC as a server on the left side in Figure 1. Scenario 2 is a repeat of the first test with the addition of ping load testing performed by a second Windows device, which pings the server. In Scenario 3, the iperf3 test is continued, but with the addition of two other Windows devices pinging the load simultaneously. Scenario 4 repeats the iperf3 test with three Windows devices pinging the load simultaneously, creating a more complex load on the network, as can be seen in Table 1 below.

Table 1. Testing Scenarios for Outgoing Interface Selection

Scenario	Outgoing Interface	Testing Method	Measured Variables
1	Manual	1 Iperf3 1 Iperf3 and 1 Ping Load device simultaneously 1 Iperf3 and 2 Ping Load devices simultaneously 1 Iperf3 and 3 Ping Load devices simultaneously	Jitter, Latency, Packet Loss
2	Best Quality	1 Iperf3 1 Iperf3 and 1 Ping Load device simultaneously 1 Iperf3 and 2 Ping Load devices simultaneously 1 Iperf3 and 3 Ping Load devices simultaneously	Jitter, Latency, Packet Loss
3	Lowest Cost (SLA)	1 Iperf3 1 Iperf3 and 1 Ping Load device simultaneously 1 Iperf3 and 2 Ping Load devices simultaneously 1 Iperf3 and 3 Ping Load devices simultaneously	Jitter, Latency, Packet Loss
4	Maximize Bandwidth (SLA)	1 Iperf3 1 Iperf3 and 1 Ping Load device simultaneously 1 Iperf3 and 2 Ping Load devices simultaneously 1 Iperf3 and 3 Ping Load devices simultaneously	Jitter, Latency, Packet Loss

To measure and compare the results of various outgoing interfaces, several approaches are used, including a manual selection of outgoing interfaces, selection based on the best measured performance (Best Quality), selection based on meeting SLA (Service-level Agreement) targets at the lowest cost if there is more than one path that meets the criteria (Lowest Cost), and traffic sharing among outgoing interfaces that meet SLAs to maximize Bandwidth (Maximize Bandwidth) [19]. In this experiment, the type of outgoing interface used acts as the independent variable, while the dependent variables measured include jitter, latency, and packet loss [21]. Each test also recorded the initial and final conditions of the two VPN tunnels implemented through ISP1 and ISP2. The initial condition reflects the state of the network before Bandwidth throttling to 10 kbps, where communication is stable through both VPN tunnels. The end state is recorded after the Bandwidth has been throttled, resulting in automatic or manual redirection to one of the two VPN tunnels and will further follow the interface output options applied. The method of transferring data by local IP between branches is not possible without a VPN tunnel, which is required to create a secure and private path, allowing communication between local networks in each branch. Without a VPN tunnel, the local networks on both sides of the FortiGate cannot communicate directly with each other over the public internet due to the barrier. In the middle of the test, Bandwidth was limited to 10 kbps to simulate network disruption conditions, and then the time required to switch from one path to another in each scenario was measured.

The experimental process began with setting up the network topology according to the scenario planned in Figure 1, and continued with testing the outgoing interface in four different scenarios as shown in Table 1. The initial test involved manual outgoing interface selection, where network performance was observed before and after bandwidth limitation, including measurement of the time taken to perform manual switching. The next test applied the Best Quality method, where the outgoing interface was automatically selected based on the best performance. In another scenario, outgoing interface selection is based on meeting SLA criteria at the lowest cost, while in the last scenario, traffic is shared among outgoing interfaces that meet SLAs to maximize Bandwidth. Dependent variables such as jitter, latency, and packet loss are measured on an ongoing basis to assess the effectiveness of each approach implemented, especially under network conditions that are disrupted and require path switching.

Data analysis was carried out using the ITU-T G.1010 standard in Table 2 as a reference to measure whether the test results on each outgoing interface were in accordance with the established standards [29]. The standards in Table 2 are applied as a measurement tool in the context of bulk data transfer/retrieval applications. The measurement results, including jitter, latency, and packet loss, were compared with the performance targets specified by ITU-T G.1010 to assess the effectiveness of each test scenario. In addition, network stability was also an essential factor analyzed. Stability is measured by monitoring the consistency of the performance of each outgoing interface during the test period, especially under varying network conditions. A stable network will show consistently low jitter, latency, and packet loss, which are important indicators in determining which outgoing interface is the most optimal and reliable in the SD-WAN scenario tested. Based on this analysis, the outgoing interface with the best performance and highest stability will be identified to ensure the optimal selection method in the SD-WAN implementation.

Table 2. ITU-T G.1010 – Performance Targets for Data Applications [29]

Medium	Application	Degree of Symmetry	Typical Amount of Data	Key Performance Parameters and Target Values
Data	Bulk data transfer/retrieval	Primarily one-way	10 KB-10 MB	Latency: Preferred < 15 s, Acceptable < 60 s Jitter: N.A. Information Loss: Zero

3. Results and Discussion

Based on the experiments on 4 scenarios with 4 different methods, the results show that Maximize Bandwidth (SLA) best complies with the ITU-T G.1010 standard. This outgoing interface has high stability, as seen from the consistency of low packet loss, latency, and jitter, even when the network load increases.

3.1 Test Results on the Manual Outgoing Interface

Manual outgoing interface testing showed a marked variation in performance between normal and restricted conditions. In the initial condition without bandwidth throttling, packet loss was 1% in both VPNs, with latency of about 38.94 ms for VPN ISP1 and 42.65 ms for VPN ISP2, and jitter of about 6-7 ms. With additional load and bandwidth limitation, VPN ISP1's latency increased to 47.76 ms with a jitter of 15.23 ms on 1 ping load device, while VPN ISP2 showed a latency of 45.78 ms and a jitter of 17.5 ms. At 2 device ping load, VPN ISP1 latency reached 47.92 ms and jitter 19.95 ms, while VPN ISP2 recorded a latency of 48.76 ms and jitter 20.6 ms. At 3 device ping load, VPN ISP1's latency jumped to 53.59 ms and jitter to 32.40 ms, while VPN ISP2 recorded latency of 53.73 ms and jitter of 29.82 ms. As shown in Table 3, the stability of these paths degrades under heavy load, with an increase in latency and jitter indicating that the manual outgoing interface is less effective in maintaining optimal performance under constrained conditions. However, unlike the automatic method that auto-switches when network interference occurs, the manual setup does not have this mechanism, so the path will not switch until it is manually changed.

Table 3. Testing on Manual Outgoing Interface

	Packet Loss	Latency	Jitter		Packet Loss	Latency	Jitter
Initial Condition: 1 Iperf3				Final Condition: 1 Iperf3			
VPN ISP1	1%	38.94 ms	6.00 ms	VPN ISP1	1%	48.17 ms	21.29 ms
VPN ISP2	1%	42.65 ms	7.15 ms	VPN ISP2	1%	50.03 ms	22.81 ms
Initial Condition: 1 Iperf3 + 1 Ping Load Device				Final Condition: 1 Iperf3 +1 Ping Load Device			
VPN ISP1	0%	41.13 ms	7.08 ms	VPN ISP1	1%	47.76 ms	15.23 ms
VPN ISP2	0%	43.36 ms	6.26 ms	VPN ISP2	1%	45.78 ms	17.50 ms
Initial Condition: 1 Iperf3 + 2 Ping Load Device				Final Condition: 1 Iperf3 +2 Ping Load Device			
VPN ISP1	0%	40.24 ms	7.25 ms	VPN ISP1	1%	47.92 ms	19.95 ms
VPN ISP2	0%	44.60 ms	8.00 ms	VPN ISP2	1%	48.76 ms	20.60 ms
Initial Condition: 1 Iperf3 + 3 Ping Load Device				Final Condition: 1 Iperf3 +3 Ping Load Device			
VPN ISP1	0%	38.52 ms	4.54 ms	VPN ISP1	1%	53.59 ms	32.40 ms
VPN ISP2	0%	40.94 ms	5.41 ms	VPN ISP2	1%	53.73 ms	29.82 ms

3.2 Test Results on the Best Quality Outgoing Interface

Testing the Best Quality outgoing interface showed relatively stable performance despite changes in load conditions. In the initial condition without bandwidth limitation, the line recorded 0% packet loss in both VPNs, with latency around 39.50 ms for VPN ISP1 and 39.26 ms for VPN ISP2, and jitter around 4.64-4.92 ms. When additional load was applied with 1 ping load device, the latency on VPN ISP1 increased to 52.03 ms with a jitter of 19.52 ms, while

VPN ISP2 showed a latency of 46.76 ms and a jitter of 19.18 ms. With 2 ping load devices, VPN ISP1's latency increased to 49.78 ms with a jitter of 23.13 ms, and VPN ISP2 recorded a latency of 51.41 ms and a jitter of 22.79 ms. In the condition with 3 devices pinging the load, VPN ISP1's latency became 44.02 ms with a jitter of 9.83 ms, while VPN ISP2 recorded a latency of 45.95 ms and a jitter of 12.12 ms. As shown in Table 4, the outgoing interface continues to perform relatively well with limited increase in latency and jitter under heavy load, indicating that this path is quite effective in maintaining optimal performance.

Table 4. Testing on Best Quality Outgoing Interface

	Packet Loss	Latency	Jitter		Packet Loss	Latency	Jitter
Initial Condition: 1 iPerf3				Final Condition: 1 iPerf3			
VPN ISP1	0%	39.50 ms	4.92 ms	VPN ISP1	1%	52.42 ms	29.57 ms
VPN ISP2	0%	39.26 ms	4.64 ms	VPN ISP2	1%	55.95 ms	31.22 ms
Initial Condition: 1 iPerf3 + 1 Ping Load Device				Final Condition: 1 iPerf3 +1 Ping Load Device			
VPN ISP1	1%	40.91 ms	7.65 ms	VPN ISP1	1%	52.03 ms	19.52 ms
VPN ISP2	1%	41.68 ms	8.24 ms	VPN ISP2	1%	46.76 ms	19.18 ms
Initial Condition: 1 iPerf3 + 2 Ping Load Device				Final Condition: 1 iPerf3 +2 Ping Load Device			
VPN ISP1	1%	41.00 ms	7.83 ms	VPN ISP1	1%	49.78 ms	23.13 ms
VPN ISP2	1%	42.69 ms	7.34 ms	VPN ISP2	1%	51.41 ms	22.79 ms
Initial Condition: 1 iPerf3 + 3 Ping Load Device				Final Condition: 1 iPerf3 +3 Ping Load Device			
VPN ISP1	0%	43.47 ms	8.05 ms	VPN ISP1	1%	44.02 ms	9.83 ms
VPN ISP2	0%	42.79 ms	8.40 ms	VPN ISP2	1%	45.95 ms	12.12 ms

When a network disruption occurs, the Best Quality method automatically performs switching to maintain connection quality. With 1 iPerf, the switching time is 1 minute 25.16 seconds. When 1 ping device is added, the switching time becomes 51.00 seconds. With 2 ping devices along with 1 iPerf, the switching time is reduced to 39.59 seconds. However, with 3 ping devices and 1 iPerf, the switching time increases again to 56.09 seconds. This auto switching time can be considered quite good, especially in higher load scenarios such as 2 ping devices and 1 iPerf which only takes 39.59 seconds to switch paths. This finding shows that the Best Quality method is quite responsive in adjusting the path to maintain connection quality when the network is disrupted. However, the increase in switching time to more than 1 minute in some conditions, such as 1 iPerf and 3 ping devices, indicates that the method can still be improved for situations with very high loads.

3.3 Test Results on the Lowest Cost (SLA) Outgoing Interface

Testing the outgoing Lowest Cost interface showed significant performance changes between normal and restricted conditions. In the initial condition without bandwidth limitation, the line recorded 0% packet loss in both VPNs, with latency around 39.57 ms for VPN ISP1 and 39.84 ms for VPN ISP2, and jitter around 5.61-5.71 ms. However, when the bandwidth was limited and the load increased, the latency on VPN ISP1 jumped to 65.64 ms with jitter increasing to 49.28 ms, while VPN ISP2 showed a latency of 63.95 ms and jitter of 48.38 ms. In the condition with 1 ping load device, VPN ISP1's latency became 48.52 ms with a jitter of 22.59 ms, while VPN ISP2 recorded a latency of 51.10 ms and a jitter of 23.54 ms. With 2 ping load devices, VPN ISP1's latency increased to 51.85 ms with a jitter of 28.65 ms, and VPN ISP2 achieved a latency of 52.10 ms with a jitter of 27.97 ms. In the condition with 3 devices pinging the load, VPN ISP1's latency became 52.08 ms with a jitter of 26.73 ms, while VPN ISP2 recorded a latency of 51.69 ms and a jitter of 28.61 ms. As shown in Table 5, the stability of these paths degrades significantly under heavy load, with increased latency and jitter indicating that the Lowest Cost outgoing interface is less efficient in maintaining optimal performance under high load.

Table 5. Testing on Lowest Cost Outgoing Interface

	Packet Loss	Latency	Jitter		Packet Loss	Latency	Jitter
Initial Condition: 1 iPerf3				Final Condition: 1 iPerf3			
VPN ISP1	0%	39.57 ms	5.71 ms	VPN ISP1	2%	65.64 ms	49.28 ms
VPN ISP2	0%	39.84 ms	5.61 ms	VPN ISP2	2%	63.95 ms	48.38 ms
Initial Condition: 1 iPerf3 + 1 Ping Load Device				Final Condition: 1 iPerf3 +1 Ping Load Device			
VPN ISP1	0%	39.55 ms	5.81 ms	VPN ISP1	1%	48.52 ms	22.59 ms
VPN ISP2	0%	40.89 ms	4.94 ms	VPN ISP2	1%	51.10 ms	23.54 ms
Initial Condition: 1 iPerf3 + 2 Ping Load Device				Final Condition: 1 iPerf3 +2 Ping Load Device			
VPN ISP1	0%	41.16 ms	6.48 ms	VPN ISP1	1%	51.85 ms	28.65 ms
VPN ISP2	0%	41.89 ms	4.84 ms	VPN ISP2	1%	52.10 ms	27.97 ms

Initial Condition: 1 iPerf3		+ 3 Ping Load Device		Final Condition: 1 iPerf3 +3 Ping Load Device			
VPN ISP1	0%	40.90 ms	5.10 ms	VPN ISP1	1%	52.08 ms	26.73 ms
VPN ISP2	0%	41.78 ms	6.20 ms	VPN ISP2	1%	51.69 ms	28.61 ms

When a network disruption occurs, the Lowest Cost method also automatically performs switching to maintain connection quality. The time required for switching is 52.81 seconds with 1 iPerf, but increases to 1 minute 35.47 seconds with 1 additional ping device, 1 minute 43.69 seconds with 2 additional ping devices, and 1 minute 22.54 seconds with 3 additional ping devices. This auto switching time is relatively slower than the other methods, especially when the load increases, indicating that this method still needs improvement to ensure efficiency in high-load situations.

3.4 Test Results on the Maximize Bandwidth (SLA) Outgoing Interface

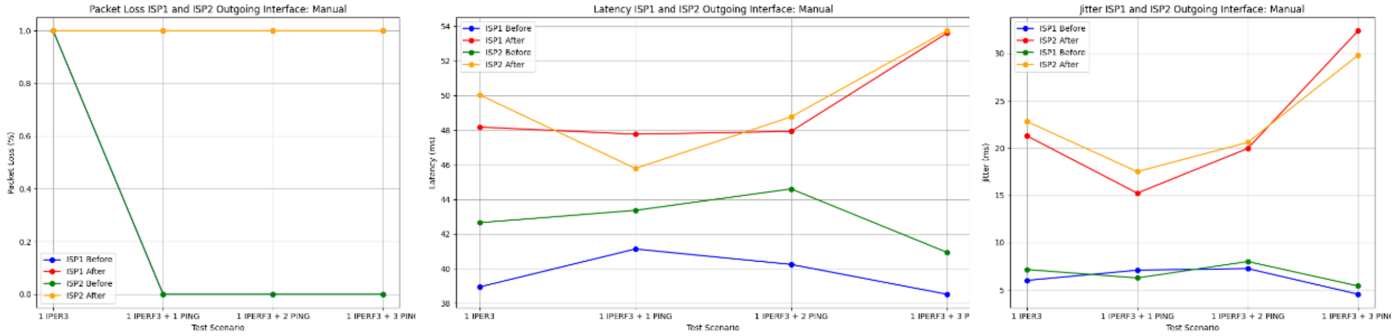
Testing the outgoing interface Maximize Bandwidth showed relatively stable performance across various test conditions. In the initial condition without bandwidth limitation, the line recorded a packet loss of 1% for both VPNs, with a latency of about 41.84 ms for VPN ISP1 and 39.66 ms for VPN ISP2, and a jitter of about 6-7 ms. After 3 minutes with 1 iPerf3, the latency slightly increased to 42.19 ms for VPN ISP1 and 40.10 ms for VPN ISP2, with jitter remaining stable at around 7 ms and 6.90 ms, respectively. When 1 ping load device was added, VPN ISP1's latency increased slightly to 45.32 ms, while jitter also increased to 10.22 ms. VPN ISP2 showed an increase in latency to 40.78 ms with a jitter of 8.91 ms. In the condition with 2 ping load devices, VPN ISP1's latency decreased slightly to 42.06 ms with a jitter of 7.28 ms, and VPN ISP2 recorded a latency of 39.79 ms with a jitter of 4.95 ms. Finally, with 3 devices pinging the load, VPN ISP1's latency was 44.55 ms with a jitter of 7.03 ms, while VPN ISP2 showed a latency of 43.34 ms with a jitter of 6.06 ms. As shown in Table 6, these outgoing interfaces show good stability with relatively moderate increases in latency and jitter under heavy load, indicating that the Maximize Bandwidth method is effective in maintaining optimal network performance. However, it should be noted that the Maximize Bandwidth method does not have an auto-switching feature when network disruptions occur, unlike other methods that automatically switch between interfaces to maintain connection quality. This advantage suggests that Maximize Bandwidth can maintain stable performance without the need for automatic path changes, relying on a load balancing scheme that divides traffic evenly between the two interfaces to optimize network load.

Table 6. Testing on Maximize Bandwidth Outgoing Interface

	Packet Loss	Latency	Jitter		Packet Loss	Latency	Jitter
Initial Condition: 1 iPerf3				Final Condition: 1 iPerf3			
VPN ISP1	1%	41.84 ms	6.98 ms	VPN ISP1	0%	42.19 ms	7.04 ms
VPN ISP2	1%	39.66 ms	6.20 ms	VPN ISP2	0%	40.10 ms	6.90 ms
Initial Condition: 1 iPerf3		+ 1 Ping Load Device		Final Condition: 1 iPerf3 +1 Ping Load Device			
VPN ISP1	0%	41.73 ms	5.86 ms	VPN ISP1	0%	45.32 ms	10.22 ms
VPN ISP2	0%	37.35 ms	4.22 ms	VPN ISP2	0%	40.78 ms	8.91 ms
Initial Condition: 1 iPerf3		+ 2 Ping Load Device		Final Condition: 1 iPerf3 +2 Ping Load Device			
VPN ISP1	1%	40.22 ms	3.84 ms	VPN ISP1	0%	42.06 ms	7.28 ms
VPN ISP2	1%	41.53 ms	5.94 ms	VPN ISP2	0%	39.79 ms	4.95 ms
Initial Condition: 1 iPerf3		+ 3 Ping Load Device		Final Condition: 1 iPerf3 +3 Ping Load Device			
VPN ISP1	0%	44.06 ms	5.69 ms	VPN ISP1	0%	44.55 ms	7.03 ms
VPN ISP2	0%	41.18 ms	9.24 ms	VPN ISP2	0%	43.34 ms	6.06 ms

3.5 Network Stabilization Comparison

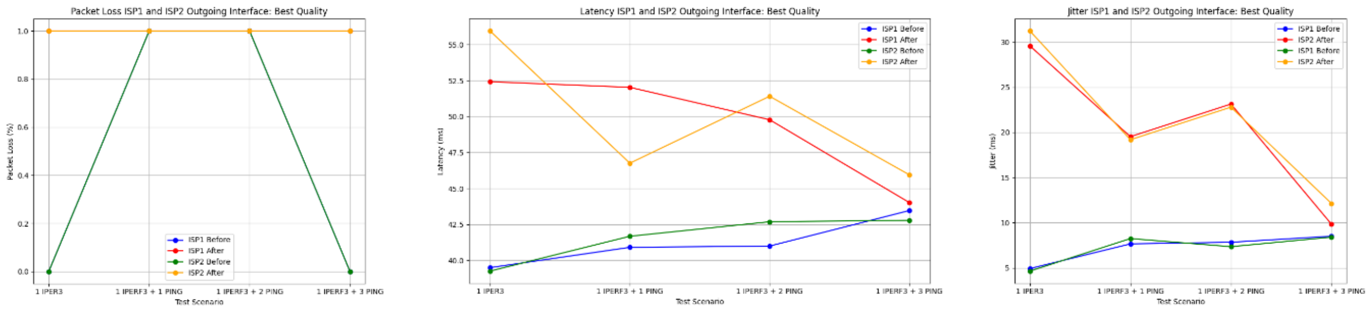
A comparison of network stability between the four outgoing interfaces shows a marked difference in performance under various test conditions. As clearly seen in Figure 2, the “Manual” outgoing interface shows a significant variation in performance between normal and constrained conditions, with a significant increase in latency as the load increases. The switching time for the “Manual” method is non-existent as it requires manual changes to switch paths, so the stability of the network is highly dependent on the initial configuration and cannot cope with disturbances automatically. In contrast, other methods have different switching times when network disruptions occur.



(a) (b) (c)

Figure 2. Latency, Packet Loss, and Jitter Analysis on ISP1 and ISP2 for Manual Outgoing Interface

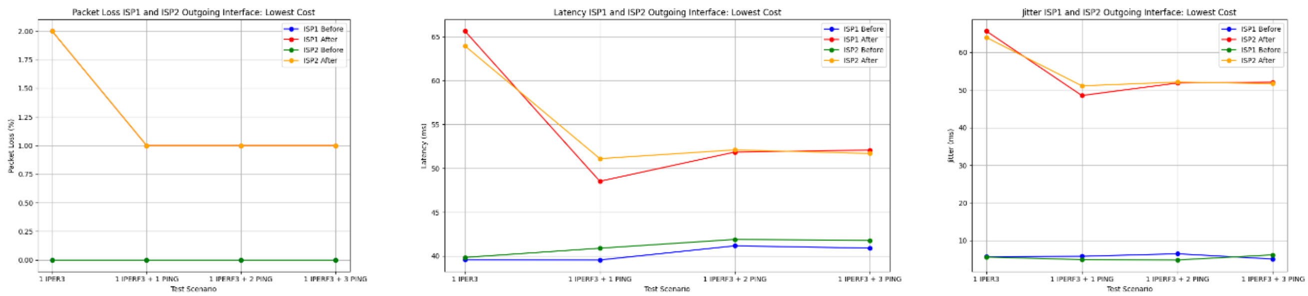
The “Best Quality” path, although providing more stable performance compared to “Manual”, still experiences a significant increase in latency when the number of ping load devices increases as shown in Figure 3. When network interference occurs, the Best Quality method automatically performs switching to maintain connection quality with varying switching times: 1 minute 25.16 seconds with 1 iPerf, 51.00 seconds with 1 ping device, 39.59 seconds with 2 ping devices and 1 iPerf, and 56.09 seconds with 3 ping devices and 1 iPerf. These auto switching times can be considered quite good, especially in higher load scenarios, although the increase in switching times in some conditions suggests that the method can still be improved.



(a) (b) (c)

Figure 3. Latency, Packet Loss, and Jitter Analysis on ISP1 and ISP2 for Best Quality Outgoing Interface

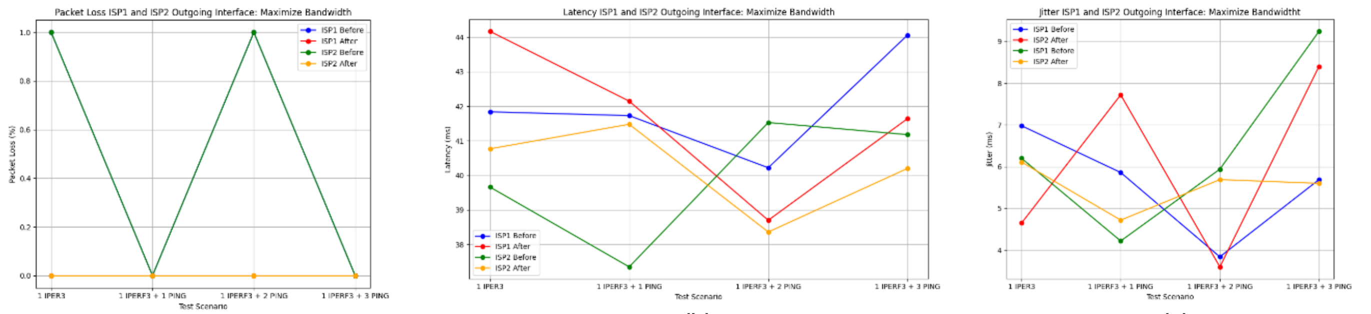
The “Lowest Cost” path shows consistent performance under normal conditions, but experiences a considerable increase in latency and jitter when additional load is applied as shown in Figure 4. When network disruption occurs, the Lowest Cost method also automatically performs switching, with a switching time of 52.81 seconds with 1 iPerf, 1 minute 35.47 seconds with 1 ping device, 1 minute 43.69 seconds with 2 ping devices, and 1 minute 22.54 seconds with 3 ping devices. These auto switching times are relatively slower than other methods, indicating that this method still needs improvement to ensure efficiency in high-load situations.



(a) (b) (c)

Figure 4. Latency, Packet Loss, and Jitter Analysis on ISP1 and ISP2 for Lowest Cost Outgoing Interface

Meanwhile, the “Maximize Bandwidth” path shows relatively good stability under heavy load, with a more controlled increase in latency and jitter compared to the other three methods as shown in Figure 5. The Maximize Bandwidth method does not have an auto-switching feature when network interference occurs, unlike the other methods that automatically switch between interfaces to maintain connection quality. This advantage shows that Maximize Bandwidth can maintain stable performance without the need for automatic path changes, relying on a load balancing scheme that divides traffic evenly between the two interfaces to optimize network load.



(a) (b) (c)

Figure 5. Latency, Packet Loss, and Jitter Analysis on ISP1 and ISP2 for Maximize Bandwidth Outgoing Interface

Overall, as shown in the jitter graph, "Maximize Bandwidth" appeared to be the most effective in maintaining optimal network performance across the various test conditions, although all methods demonstrated their respective capabilities in handling multiple load scenarios.

SD-WAN with the Maximize Bandwidth method is proven to be the most effective in maintaining optimal network performance under various test conditions. In this section, a comparison is made between SD-WAN outgoing interface Maximize Bandwidth from this research with EoIP, SD-WAN, and MPLS from previous research.

The research shows that SD-WAN with the outgoing interface Maximize Bandwidth produces a one-way delay of 22.27 ms, as shown in Figure 6, which is higher than all the methods in previous studies. The EoIP, SD-WAN, and MPLS methods of earlier studies recorded lower one-way delay values of 6.89 ms, 6.68 ms, and 6.89 ms, respectively [8]. Figure 6 also shows that the SD-WAN method from previous studies has the lowest one-way delay value of 6.68 ms, making it the method with the best latency for network response speed.

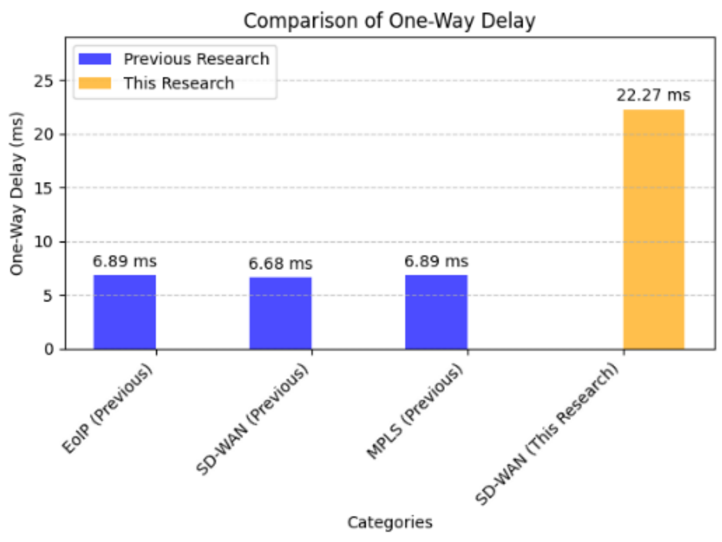


Figure 6. Comparison of One-Way Delay between SD-WAN in this Study and EoIP, SD-WAN, and MPLS from Previous Studies

In terms of information loss, SD-WAN with Maximize Bandwidth shows optimal performance with a loss rate of 0%, as shown in Figure 7, which is much better than SD-WAN in previous studies (1.5%) and EoIP (0.15%) [8]. Although MPLS of the prior research recorded a packet loss rate of 0.1%, these results show that SD-WAN with Maximize Bandwidth delivers the best performance in maintaining network data integrity, especially under high load conditions.

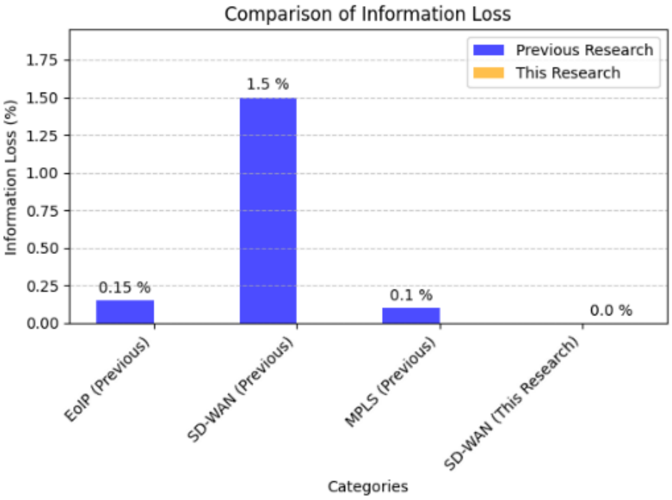


Figure 7. Comparison of Information Loss between SD-WAN in this Study and EoIP, SD-WAN, and MPLS from Previous Studies

On delay variation (jitter), this study recorded a jitter value of 7.03 ms for SD-WAN with Maximize Bandwidth, which is lower than MPLS from previous studies (8.44 ms), but higher than SD-WAN (0.33 ms) and EoIP (0.15 ms) of earlier studies, as shown in Figure 8 [8]. Thus, EoIP shows the best performance in terms of delay variation, followed by SD-WAN (previous studies). Although Maximize Bandwidth provides better stability under heavy loads, the higher delay variation indicates that it is not optimal in managing jitter compared to the other methods.

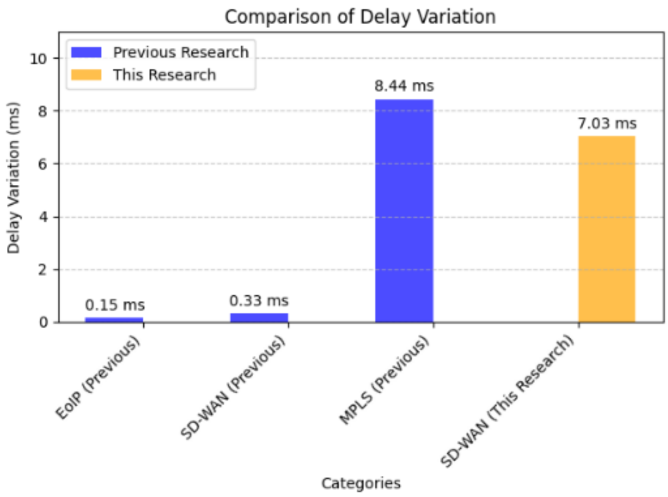


Figure 8. Comparison of Delay Variation between SD-WAN in this Study and EoIP, SD-WAN, and MPLS from Previous Studies

This research shows that SD-WAN with outgoing interface Maximize Bandwidth does not have the best performance in terms of one-way delay and delay variation. The SD-WAN method from previous research shows the best one-way delay. For information loss, SD-WAN with Maximize Bandwidth shows the best performance with a 0% loss rate. However, in terms of delay variation (jitter), EoIP shows the best performance, superior to SD-WAN with Maximize Bandwidth.

3.6 Compliance with ITU-T G.1010 Standards

Evaluation of network performance on various outgoing interfaces shows that most test methods meet the standards set by ITU-T G.1010 in Table 2 for data applications, particularly in the bulk data transfer/retrieval category. Based on these standards, latency for bulk data applications should be lower than 60 seconds to meet the acceptable criteria, while jitter and packet loss should be close to zero for optimal performance. Test results show that the outgoing interfaces Maximize Bandwidth and Best Quality managed to keep latency below the acceptable threshold, with maximum latency recorded at 53.59 ms and 55.95 ms, respectively, and jitter remaining relatively low. On the other hand, outgoing interfaces Manual and Lowest Cost showed an increase in latency and jitter under heavy load, with maximum latency reaching 65.64 ms and jitter increasing sharply, indicating that they fall short of the desired performance stability standards. Thus, although all test methods can meet the acceptable latency criteria, Maximize Bandwidth and Best Quality are more in line with ITU-T G.1010 performance targets in terms of network stability and reliability.

Based on the data obtained from the Maximize Bandwidth method, it is evident that for non-real-time services (data), this method satisfies all the key performance parameters and target values required as outlined in Table I.2/G.1010 – Performance targets for data applications in the ITU-T G.1010 standard [29]. This includes transaction-based services such as e-commerce, e-banking, and e-trading, which also meet the minimum QoS parameters outlined in the table. Therefore, these types of services are recommended to utilize the Maximize Bandwidth method.

The findings of this study demonstrate that the Maximize Bandwidth method consistently delivers optimal performance in terms of latency, jitter, packet loss, availability, and error rate, aligning with the criteria set by ITU-T G.1010 for various types of services. However, for real-time services (voice/video), some requirements in Table I.1/G.1010 – Performance Targets for Audio and Video Applications remain unmet by this method [29]. Hence, the Maximize Bandwidth method is most recommended for services other than real-time services (voice/video). For real-time services, further optimization is required, which could serve as a focus for future research to ensure this method meets all the necessary QoS requirements.

The ITU-T G.1010 standard specifies additional key performance parameters, including availability and error rate, that are essential for maintaining quality of service. Availability, or the amount of time network services are available, is critical for uninterrupted connectivity in high-demand environments. In SD-WAN, it is supported by redundant paths and failover mechanisms. While availability is not directly measured, the Maximize Bandwidth method inherently improves it by optimizing path selection in real time. Error rate, which indicates data corruption during transmission, is critical to data integrity for critical applications. Although not explicitly measured, the achieved 0% packet loss indicates minimized error risk, consistent with the ITU-T G.1010 focus on error-free transmission.

Although the SD-WAN comparison results in this study for one-way delay and delay variation (jitter) are not as good as the results of previous studies, they still meet the ITU-T G.1010 standard, which stipulates that one-way delay must be lower than 15 seconds to enter the preferred level [8], [29]. In addition, although EoIP, SD-WAN, and MPLS in previous studies showed good performance, they still need improvement in terms of information loss or packet loss, where the ITU-T G.1010 standard requires packet loss to reach 0% [8], [29]. Therefore, SD-WAN with Maximize Bandwidth in this study has successfully met the ITU-T G.1010 standard and improved on previous studies by achieving 0% packet loss.

3.7 Discussion

Analysis of the test results shows that each outgoing interface has different performance under various network conditions, which can substantially affect the SD-WAN implementation strategy. Overall, the outgoing interfaces Maximize Bandwidth and Best Quality showed more consistent performance. Maximize Bandwidth, for example, maintained a latency of about 42.19 ms and a jitter of 7.04 ms under end state, while Best Quality showed a latency of 52.42 ms and a jitter of 29.57 ms under heavy load. On the other hand, Manual and Lowest Costs showed greater instability under heavy load. Manual, with latency jumping to 53.59 ms and jitter reaching 32.40 ms, and Lowest Cost, with latency increasing to 65.64 ms and jitter of 49.28 ms, showed less consistent performance.

Compliance with the ITU-T G.1010 standard shows that Maximize Bandwidth and Best Quality are closer to the desired performance targets for bulk data applications, with latency and jitter within acceptable limits. Maximize Bandwidth meets the criteria with a latency of about 42.19 ms and a jitter of 7.04 ms in the final state, while Best Quality shows a latency of 52.42 ms and a jitter of 29.57 ms under heavy load, which is still within the acceptable limits of the standard. In contrast, Manual and Lowest Costs showed higher levels of instability under heavy load. Manual, for example, experienced latency jumping to 53.59 ms and jitter reaching 32.40 ms, while Lowest Cost showed latency increasing to 65.64 ms and jitter 49.28 ms, often exceeding the limits set by the ITU-T G.1010 standard.

Best quality and lowest cost can automatically switch paths when network disruptions occur, which can improve network resilience. However, Maximize Bandwidth uses a load balancing scheme, which divides the traffic equally between the two interfaces. Since Maximize Bandwidth does not have an auto-switching feature, there is no time wasted on switching paths, thus allowing this method to maintain stable performance without the need for automatic switching, making it superior in maintaining network stability under heavy load.

From a practical standpoint, the recommendation for SD-WAN implementation is to choose the outgoing interface Maximize Bandwidth for scenarios that require stability and optimal performance, while Best Quality can be a good alternative with some additional considerations. Areas for further optimization include load management on Manual and Lowest Cost interfaces, which show potential for improvement in terms of latency and jitter control under high load conditions. A more careful implementation strategy and selection of appropriate outgoing interfaces can help companies achieve better and more stable network performance.

SD-WAN with the Maximize Bandwidth method proved to be the most effective in maintaining optimal network performance under various test conditions. Compared to other methods, Maximize Bandwidth recorded a one-way delay of 22.27 ms, which is higher than EoIP (6.89 ms), previous studies' SD-WAN (6.68 ms), and MPLS (6.89 ms) [8]. However, although this one-way delay is higher, it is still within the acceptable level according to the ITU-T G.1010 standard for large data transfers. In terms of information loss, this method showed the best performance with a loss rate of 0%, which isbetter than the previous studies' SD-WAN (1.5%), EoIP (0.15%), and MPLS (0.1%) [8]. Even so, the resulting jitter of 7.03 ms is lower than MPLS (8.44 ms) but still higher than EoIP (0.15 ms) and the previous studies' SD-WAN (0.33 ms) [8]. Based on the ITU-T G.1010 standard, jitter in the context of bulk data transfer does not have a specific target value (Not Applicable/N.A.), so jitter performance in all methods remains at an acceptable level [29]. These results show that although SD-WAN with Maximize Bandwidth does not excel in all metrics, it achieves 0% packet loss and meets ITU-T G.1010 standards for latency and data integrity. As such, it remains an effective option, especially for scenarios that demand minimal information loss on the network.

Similarly, the research highlights the practical guidance for enterprises, suggesting that Maximize Bandwidth (SLA) could be the optimal selection method for balancing cost, performance, and reliability. Maximize Bandwidth is ideal for services and data applications that require high bandwidth and low latency, such as e-commerce platforms and bulk data transfer. The trade-off is that this method requires at least two active network lines to function optimally, as it relies on multiple network lines simultaneously. Best Quality is suitable for both real-time and non-real-time services that demand high network quality, such as voice/video calls or critical application access. The downside is its higher cost due to its stringent line selection criteria and minimal error tolerance. Additionally, network quality can fluctuate, meaning that lines chosen as optimal at the time of measurement may show inconsistent performance over time. The Lowest Cost method is best used for non-real-time or background services that are less sensitive to latency and speed. While it reduces costs, it often sacrifices network quality and reliability. This method is more appropriate for applications that are not heavily reliant on low latency or high-quality connections, but it may not be sufficient for critical or real-time services. The Lowest Cost method should be considered when cost is the primary factor and a reduction in quality is acceptable. Lastly, Manual configuration is functional when precise control over interface settings is needed for sensitive or essential applications. The drawback of this approach is that if a failure occurs on the selected line, all services using this method will be disrupted, as it requires manual configuration and modification. This method is best suited for situations where the line being used is known to be stable and secure.

Further validation of these findings was achieved by comparing the simulation results with real-world SD-WAN deployments. According to a referenced study, simulations conducted using GNS3 closely align with real-world performance due to the use of similar topological schemes [3]. This alignment validates that the simulation framework used in this research mirrors real-world implementations, as observed in deployments by companies such as PT XYZ.

4. Conclusion

This research evaluates the effectiveness of various outgoing interface options in SD-WAN management and finds that the Maximize Bandwidth (SLA) method is the most optimal. From the tests, the Manual and Lowest Cost (SLA) paths show a considerable increase in latency and jitter under heavy load. Latency on the Manual path increased by about 15 ms and jitter by about 3 ms, while on Lowest Cost (SLA) it increased by about 20 ms and jitter by about 4 ms. The Best Quality path showed better stability with latency rising by about 13 ms and jitter by about 5 ms under heavy load. In contrast, Maximize Bandwidth (SLA) provides the best performance with a latency increase of only 4 ms and jitter of 2 ms, and minimal packet loss below 1%. Thus, Maximize Bandwidth (SLA) is an ideal choice for SD-WAN networks that require high performance and consistent stability. This research emphasizes the importance of choosing the right strategy to optimize network performance and ensure optimal quality of service.

Acknowledgement

We would like to express our gratitude to all parties who have supported and contributed to completing this research. Especially the Informatics department at Universitas Muhammadiyah Malang for consistently supporting the research process.

References

[1] W. Pratiwi and D. Gunawan, “Design and Strategy Deployment of SD-WAN Technology : In Indonesia (Case Study: PT. XYZ),” in *2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, Jul. 2021, pp. 1–6. https://doi.org/10.1109/GECOST52368.2021.9538796

[2] M. Zouini *et al.*, “Towards a Modern ISGA Institute Infrastructure Based on Fortinet SD-WAN Technology: Recommendations and Best Practices”. https://doi.org/10.1016/j.procs.2022.10.156

[3] G. K. Soejantono, M. I. Nashiruddin, S. N. Hertiana, and M. A. Nugraha, “Performance Evaluation of SD-WAN Deployment for XYZ Enterprise Company in Indonesia,” in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct. 2021, pp. 0311–0316. https://doi.org/10.1109/IEMCON53756.2021.9623170

[4] B. Yuan and C. Zhao, “Research on Transmission Delay of SD-WAN CPE,” in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, Oct. 2020, pp. 955–960. https://doi.org/10.1109/ICCT50939.2020.9295722

[5] D. L. T. G. J. Javier, S. J. M. Elizabeth, J. P. F. Xavier, and P. C. M. Rubén, “SD-WAN Software defined networking using DMVPN for corporate enterprises,” in *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, Jun. 2023, pp. 1–6. https://doi.org/10.23919/CISTI58278.2023.10211444
[6] J. M. Carvajal, F. T. Gilabert, and J. Cañadas, “Corporate network transformation with SD-WAN. A practical approach,” in *2021 Eighth International Conference on Software Defined Systems (SDS)*, Dec. 2021, pp. 1–6. https://doi.org/10.1109/SDS54264.2021.9731850
[7] S. Rajagopalan, “An Overview of SD-WAN Load Balancing for WAN Connections,” in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2020, pp. 1–4. https://doi.org/10.1109/ICECA49313.2020.9297574
[8] R. Y. Manova, E. Sukmadirana, and N. S. Nurmanah, “Comparative Analysis of Quality of Service and Performance of MPLS, EoIP and SD-WAN,” in *2022 1st International Conference on Information System & Information Technology (ICISIT)*, Jul. 2022, pp. 403–408. https://doi.org/10.1109/ICISIT54091.2022.9872806
[9] D. Tiana, W. Permana, I. Gutandjala, and A. Ramadhan, *Evaluation of Software-Defined Wide Area Network Architecture Adoption Based on The Open Group Architecture Framework (TOGAF)*. 2023. https://doi.org/10.1109/ICICyTA60173.2023.10428976
[10] L. Borgianni, S. Troia, D. Adami, G. Maier, and S. Giordano, “From MPLS to SD-WAN to ensure QoS and QoE in cloud-based applications,” in *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, Jun. 2023, pp. 366–369. doi: 10.1109/NetSoft57336.2023.10175470.
[11] S. Troia, L. M. Moreira Zorello, and G. Maier, “SD-WAN: how the control of the network can be shifted from core to edge,” in *2021 International Conference on Optical Network Design and Modeling (ONDM)*, Jul. 2021, pp. 1–3. https://doi.org/10.23919/ONDM51796.2021.9492375
[12] L. M. Silalahi, V. Amaada, S. Budiyanto, I. U. V. Simanjuntak, and A. D. Rochendi, “Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company,” *International Journal of Electronics and Telecommunications*, vol. 70, no. 1, 2024. https://doi.org/10.24425/ijet.2024.149540
[13] S. Andromeda and D. Gunawan, “Techno-economic Analysis from Implementing SD-WAN with 4G/LTE, A Case Study in XYZ Company,” in *2020 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Jul. 2020, pp. 345–351. https://doi.org/10.1109/ISITIA49792.2020.9163762
[14] P. Segeč, M. Moravčik, J. Uratmová, J. Papán, and O. Yeremenko, “SD-WAN - architecture, functions and benefits,” in *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Nov. 2020, pp. 593–599. https://doi.org/10.1109/ICETA51985.2020.9379257
[15] Z. Yang, Y. Cui, B. Li, Y. Liu, and Y. Xu, “Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities,” in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, Aug. 2019, pp. 1–9. https://doi.org/10.1109/ICCCN.2019.8847124
[16] F. Altheide, S. Buttgereit, and M. Rossberg, “Increasing Resilience of SD-WAN by Distributing the Control Plane [Extended Version],” *IEEE Transactions on Network and Service Management*, vol. 21, no. 3, pp. 2569–2581, Jun. 2024. https://doi.org/10.1109/TNSM.2024.3386962
[17] D. Zad Tootaghaj, F. Ahmed, P. Sharma, and M. Yannakakis, “Homa: An Efficient Topology and Route Management Approach in SD-WAN Overlays,” in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, Jul. 2020, pp. 2351–2360. https://doi.org/10.1109/INFOCOM41043.2020.9155503
[18] J. R. Bustamante and D. Avila-Pesantez, “Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results,” in *2021 IEEE Engineering International Research Conference (EIRCON)*, Oct. 2021, pp. 1–4. https://doi.org/10.1109/EIRCON52903.2021.9613418
[19] Fortinet, Inc., “SD-WAN Rules - Maximize Bandwidth (SLA),” SD-WAN rules - maximize bandwidth (SLA).
[20] Fortinet, *FortiOS Cookbook Version 6.2.16*. Fortinet, 2024.
[21] S. Troia, M. Mazzara, L. M. Moreira Zorello, and G. Maier, “Performance Evaluation of Overlay Networking for delay-sensitive services in SD-WAN,” in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, Sep. 2021, pp. 150–155. https://doi.org/10.1109/MeditCom49071.2021.9647549
[22] K.-H. Kim, D. Kim, and Y.-H. Kim, “Open-Cloud Computing Platform Design based on Virtually Dedicated Network and Container Interface,” 2019.
[23] R. Asif and K. Ghanem, “AI Secured SD-WAN Architecture as a Latency Critical IoT Enabler for 5G and Beyond Communications,” in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2021, pp. 1–6. https://doi.org/10.1109/CCNC49032.2021.9369477
[24] Z. Qin, “SD-WAN for Bandwidth and Delay Improvements on the Internet,” *SHS Web Conf.*, vol. 144, 2022. https://doi.org/10.1051/shsconf/202214402004
[25] S. Pamplin, “SD-WAN revolutionises IoT and edge security,” *Network Security*, vol. 2021, no. 8, pp. 14–15, Aug. 2021. https://doi.org/10.1016/S1353-4858(21)00090-8
[26] G. Moser, “Performance Analysis of an SD-WAN Infrastructure Implemented Using Cisco System Technologies,” Student thesis, 2021.
[27] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Zhuravlova, A. Kruhlova, and V. Lemeshko, “Research of Improved Traffic Engineering Fault-Tolerant Routing Mechanism in SD-WAN,” in *2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Aug. 2021, pp. 187–190. https://doi.org/10.1109/UKRCON53503.2021.9575272
[28] Z. Guo, C. Li, Y. Li, S. Dou, B. Zhang, and W. Wu, “Maintaining the Network Performance of Software-Defined WANs With Efficient Critical Routing,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2240–2252, Apr. 2024. https://doi.org/10.1109/TNSM.2023.3335404
[29] TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, *SERIES G: TRANSMISSION SYSTEMS AND MEDIA,DIGITAL SYSTEMS AND NETWORKS Quality of service and performance End-user multimedia QoS categories*, End-user multimedia QoS categories, Nov. 29, 2001.
[30] SolarWinds Worldwide, LLC., “Graphical Network Simulator 3,” Graphical Network Simulator 3.
[31] Fortinet, Inc., “Next-Generation Firewall (NGFW),” Next-Generation Firewall (NGFW).
[32] A. G. Biradar, “A Comparative Study on Routing Protocols: RIP, OSPF and EIGRP and Their Analysis Using GNS-3,” in *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Dec. 2020, pp. 1–5. https://doi.org/10.1109/ICRAIE51050.2020.9358327
[33] D. A. Retnani Wulandari, Y. A. Auliya, A. Cahya Prihandoko, S. Slamin, and M. Zarkasi, “Wireless Area Network Infrastructure Model on Gili Ketapang Island Using Open Shortest Path First Routing Protocol,” *KINETIK*, vol. 7, no. 1, pp. 11–22, Feb. 2022. https://doi.org/10.22219/kinetik.v7i1.1373
[34] J. Wang, M. Bewong, and L. Zheng, “SD-WAN: Hybrid Edge Cloud Network between Multi-site SDDC,” *Computer Networks*, vol. 250, no. 110509, Aug. 2024. https://doi.org/10.1016/j.comnet.2024.110509
[35] C. Fu, B. Wang, H. Liu, and W. Wang, “Software-Defined Virtual Private Network for SD-WAN,” *Electronics*, vol. 13, no. 13, 2024. https://doi.org/10.3390/electronics13132674