International Journal Software Engineering and Computer Science (IJSECS)
4 (1), 2024, 24-39
Published Online April 2024 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN : 2776-4869, E-ISSN : 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v4i1.2100.

RESEARCH ARTICLE Open Access

Application of The SD-WAN Load Balancing Method in Managing Internet Bandwidth at IDN Bogor Vocational School

Dadang Iskandar Mulyana
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

Joe Renaldy Farisyihab
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

Muhamad Hasbi Toharudin Bahari
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

Muhammad Dzaky Nurfaishal *
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Corresponding Email: dzakymuh22@gmail.com.

Muhammad Daffa Khairullah
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

Received: January 13, 2024; Accepted: March 10, 2024; Published: April 1, 2024.

Abstract: The rapid growth of SMK IDN since its establishment in 2016 has necessitated the addition of several branches. With the increasing number of branches, SMK IDN's administrative activities need to be centralized at SMK IDN Jonggol (Central), where the school leases and utilizes MPLS services to support interconnections between branches and the central office. However, there are considerations regarding using MPLS services as the number of SMK IDN branches continues to grow. Concerns from the SMK IDN IT team include issues related to the inflexibility of MPLS links, which can only be specifically used for interconnecting branches or private links that cannot simultaneously accommodate the internet needs of branches. In this situation, the SMK IDN IT team seeks an efficient solution that provides flexibility in interconnections from branches to the central office, with capabilities and stability equal to or better than before. In response to the challenges faced by SMK IDN, we propose the Load Balancing SDWAN solution, where SMK IDN only needs to use internet services available at the central office and branches. The Load Balancing SDWAN solution offers flexibility in terms of cost efficiency and link usage because links can simultaneously fulfill internet and interconnection needs for branches. In its implementation, the Load-balancing SDWAN method effectively addresses the challenges encountered by SMK IDN. Test results show that after implementing the Load Balancing SDWAN method, there is a significant improvement in internet access stability for users, with the ability to failover if there are issues with one internet link, as well as maintaining secure and private connections between the central office and branches. Another benefit of implementing the Load Balancing SDWAN method is budget efficiency, as SMK IDN can provide dedicated internet services per month at a 63% lower cost compared to renting MPLS links previously used.

Keywords: MPLS; Load Balancing; SDWAN; Internet; Fail Over.

1. Introduction

In managing data from IDN Vocational School branches spread across several regions, technology is needed to connect each branch to the Central IDN Vocational School. Each IDN Vocational School branch requires this because input access is required to the Central IDN Vocational School server. In response to this need, IDN Vocational School currently uses MPLS technology. MultiProtocol Label Switching (MPLS) is a packet delivery technology on a high-speed backbone network. It combines several advantages of circuit-switched and packet-switched communication systems, which gives rise to better technology than both. Behind the advantages that MPLS technology can provide, several disadvantages can be reconsidered in terms of high service costs both in terms of implementation and maintenance, limited flexibility because the MPLS link service itself can only be used for interconnection between branches, MPLS also has several disadvantages such as the length of time professionalization of service on MPLS networks with different domains, as well as limited scalability when agencies want to add new branches. SDWAN Load Balancing can be an answer or solution to the problems experienced by IDN Vocational School, where researchers combine 2 technologies, namely Load Balance and SD-WAN. Load balancing is a technique for distributing traffic loads on two or more connection lines in a balanced way so that traffic can run optimally, maximize throughput, reduce response time, and avoid overload on one of the connection lines.

Meanwhile, the general function of SDWAN itself, usually called Software Defined Networking (SDN), offers a paradigm in network control that makes it easier to manage, control, and monitor the network and also makes it possible to improve network performance; this is because SDN carries the concept of separating the data plane and control plane. Where the existing control fields are combined into one control point. Implementing SDWAN Load Balancing produces several benefits, such as lower costs because SDWAN can use a public internet connection, which can replace dependence on costly MPLS lines, supports active-active link conditions which are very profitable for sharing data traffic from the user's side goes to the internet, as well as the ability to auto failover which helps when a problem occurs on one internet link, it can automatically switch to another internet link without needing to do it manually.

Various studies have been conducted to optimize network security and load distribution that offer valuable insights into multiple aspects of network design and technology implementation. Nana and Dadang Iskandar Mulyana (2022) research explores point-to-point network security optimization using VPN IPSec and GRE [1]. Likewise, Untung Wahyudi, Dadang Iskandar Mulyana, and Yuma Akbar, as explained in the Computer Scientific Journal (2023), explored improving internet gateway optimization through the Virtual Router Redundancy Protocol [2]. Furthermore, Oky Tria Saputra *et al*. (2023) explored optimizing load distribution and network security using OpenVPN with the OSPF Routing Protocol [3]. Meanwhile, research by Enggar Bagoes Pabelan *et al*. (2023) presented the implementation of load balancing via PCC methodology to optimize internet usage across two ISPs [4]. Beyond traditional network optimization methods, studies such as Muhammad Fikri's (2023) analysis of VPN implementation in branches using SDWAN technology with load-balancing methodology provide insight into advanced network management approaches [5]. Furthermore, an examination by Sahrul Hidayat (2023) regarding the implementation of VPN failover using SDWAN technology confirms the importance of network continuity strategies [6]. Likewise, a study by Estu Rizky Huddiniah *et al*. (2018) provides insights into route optimization for SDN-WAN using the OpenFlow protocol [7]. By combining contemporary technology, analysis by Andi Dinda Nurul Fauziah *et al*. (2022) on implementing traffic diversion technology in SD-WAN using Fortigate devices displays an innovative approach to network management [8]. In addition, a comparative study by Ahmad Tariq Sabiq *et al*. (2023) on UDP and DCCP protocols in SD-WAN networks enriches our understanding of protocol selection in network optimization [8][9]. Based on this variety of research, we aim to develop a comprehensive theory about applying the SD-WAN load balancing methodology to manage internet bandwidth at IDN Bogor Vocational School effectively. Leveraging insights from this research, we strive to establish a resilient network infrastructure that not only optimizes internet bandwidth but also ensures enhanced security and seamless connectivity for users.

Feby Ardianto, Bengawan Alfaresi, and Agus Darmadi (2018) discussed load balancing design for two Internet Service Providers (ISPs) using MikroTik technology. Their research most likely explored the implementation of load-balancing techniques to efficiently distribute network traffic between multiple ISPs efficiently, thereby ensuring optimal bandwidth utilization and network reliability [10]. Ricky Oktariyadi, Ikhwan Ruslianto, and Syamsul Bahri (2021) analyzed load balancing performance using the Round Robin and Weighted Round Robin methods. This research compares the effectiveness of these two load-balancing techniques in distributing network traffic efficiently, providing valuable insights into load-balancing strategies [11]. Tania Octavriana, Koko Joni, and Achmad Fiqhi Ibadillah (2021) explore internet network optimization with load balancing, especially in high-traffic environments. Their research likely focuses on strategies to improve network performance and stability under high traffic conditions through effective load-balancing mechanisms [12]. Riyan Almakhi, Anton Anton, and Fitra Septia Nugraha (2022) implemented load balancing and failover using IP SLA at PT. Pan Pacific Insurance. This research possibly investigates implementing failover mechanisms and load-balancing strategies to ensure network reliability and continuity in an insurance company's network infrastructure [13]. Marchand Satriawan and Benfano Soewito designed an SD-WAN for the insurance holding company PT. XYZ [14]. Increasing connectivity and network efficiency through implementing SD-WAN technology in the insurance sector. Ilmalik Muhammad Alviendra, Eko Setijadi, and Gatot Kusrahardjo (2022), developed and implemented a Virtual Private Network (VPN) system for the Internet of Things (IoT) using simulation techniques [15]. This research explores integrating VPN technology with IoT systems to improve data and communication security in IoT environments. Rio Febrial Syarif and Irwan Agus Sobari (2022) implemented a Virtual Private Network (VPN) using Point-to-Point Tunneling Protocol (PPTP) at PT. Sinar Quality Internusa [16]. Their research likely focuses on implementing VPN technology to establish secure communication channels within corporate network infrastructure. Novandi Rizki Fattahillah, Farah Nurfadila, and Yanto Setiawan (2023), implemented the availability feature on the Fortigate firewall using an SD-WAN zone configuration and a High Availability (HA) active-passive cluster [17]. This research may explore strategies to increase network availability and resilience by integrating SD-WAN technology with firewall systems. Sari Dewi (2020) investigated network security using VPN with Point-to-Point Tunneling Protocol (PPTP) at the Kertarahaja Ciamis Village Office [18]. This research will likely focus on improving network security by implementing VPN technology with the PPTP protocol in local government office settings. Rully Mujiastuti and Ibnu Prasetyo (2021) developed a VPN-based network security system that is integrated with Pi-hole DNS filtering [19]. This research explores integrating VPN technology with DNS filtering mechanisms to improve network security and privacy. Tanda Budimulya and Maryanah Safitri (2022) designed a VPN system as an employee information system at the Ministry of Health office [20]. This research will likely focus on developing a VPN-based system to facilitate safe and efficient information management for employees within the Ministry of Health.

Arham Bakri and Sulistianto SW (2019) modeled a computer network using site-to-site VPN at Juwita Hospital Bekasi, as documented in the Teknokris Journal. This study possibly explores the configuration and setup of VPN connections between different locations in a hospital network to ensure secure and smooth communication [21]. Hari Antoni Musril (2019) designed a Virtual Private Network (VPN) based on the Open Shortest Path First (OSPF) protocol, as published in the National Journal of Informatics and Network Technology. This research may utilize the OSPF routing protocol to establish VPN connections efficiently and securely [22]. Luthfi Firdhaus, Fatmawati, and Bambang Wijonarko (2019) implemented a Virtual Private Network (VPN) using IP Security for site-to-site connections at the Ministry of Transportation, as the Inti Nusa Mandiri Journal explained. This study likely emphasizes using the IPsec protocol to ensure secure data transmission between different locations in the ministry's network [23]. Putri Agustyaningsih, Cahyo Prihantoro, and Iqsyahiro Kresna A (2023) conducted a performance analysis of computer networks using the Unequal Load Balance method on local networks, as reported in the Journal of Information Technology Education. This study likely evaluates the effectiveness of load-balancing techniques in optimizing network resources and improving performance in local network environments [24]. La Surimi, Subardin, and Nurmiati (2022) analyzed the performance of load balancing on internet networks using the Equal Cost Multi-Path (ECMP) method. This research will likely focus on assessing the efficiency and effectiveness of ECMP in distributing network traffic across multiple paths to improve network performance [25]. Achmmad Mustofa and Desi Ramayanti (2020) implemented load balancing and failover to MikroTik routers using the Nth method at PT. GO-JEK Indonesia. This study explores implementing a load-balancing strategy with a failover mechanism to ensure network reliability and continuity in a real case study scenario at PT. GO-JEK Indonesia [26]. Iwan Rijayana, in his study in 2005, used Multi-Protocol Label Switching (MPLS) technology to improve network performance [27]. Nisa Aulia Nurhasanah, Ida Wahidah, and Bambang Cahyono (2017) explored the implementation of Seamless Multi-Protocol Label Switching (MPLS) in MPLS networks [28]. Abe Wisnu Syaputra and Setiawan Assegaff (2017) analyzed and implemented load balancing using the Nth method in the Jambi Province education department network [29]. Andry Maulana and Ahmad Fauzi (2018) discuss PVST (Per VLAN Spanning Tree) and load balancing in their book "Computer Networks," published by Nusa Mandiri University [30]. The work of Muhammad Hafizh (2011) focuses on load balancing using the per-connection classifier method with a proxy server for caching, published by UIN Jakarta [31]. Ai Ilah Warnilah and Bambang Kelana Simpony (2019) discuss load balancing in their book "Computer Networks," published by BSI University [32]. Sritrusta Sukaridhoto, ST. PhD (2014), in the second edition of the book "Computer Networks," discusses load balancing and scalability [33]. Andri Dwi Utomo work focused on implementing load balancing for two ISPs using MikroTik devices, published by UIN Jakarta [34]. T. Sukendar's study in the Computer Technology Journal at AMIK BSI in 2017 discussed bandwidth balancing using two ISPs via the Nth load balancing method [35].

The problems faced by the IDN Vocational School IT Team include: Can an SDWAN load balancing solution using the internet replace the MPLS currently used? What will happen when one of the internet links experiences problems? This research aims to answer several issues experienced by IDN Vocational School, namely by implementing the SD-WAN Load Balancing Method in Internet Bandwidth Management at IDN Vocational School Bogor to replace the existing MPLS technology without reducing its security features.

2. Research Method

This research used a qualitative data collection method focused on in-depth observation. The qualitative approach allows researchers to be directly involved with the research subject, in this case, the internet network in the IDN Vocational School environment. The use of this method is expected to produce a more comprehensive analysis of the phenomenon being studied, as emphasized by Anton Wibisono (2019) [13]. Researchers understand the phenomenon's social, cultural, and environmental context through direct involvement with research subjects. This research applies a qualitative approach to researching natural places without providing any particular treatment because the data is collected by Emily based on the views of the data source, not the researchers. Qualitative data was obtained through an in-depth analysis process. In qualitative data collection methods, various techniques are used, such as observation, interviews, and data collection from other sources such as books, journals, and related research results. Direct observations were carried out at IDN Bogor Vocational School to obtain accurate and complete information related to the research title. The interview was conducted with representatives from the IDN Vocational School IT Team, although it had certain limitations because it involved confidential information related to the internal network. Apart from that, data collection was also carried out through literature studies, taking information from various sources such as books, journals, and related research. Hopefully, these techniques can provide a deep understanding of the phenomenon being studied.

In this research, the definition and understanding of Local Area Networks (LAN), TCP/IP, Router, Load Balancing, SD-WAN, and Virtual Private networks (VPN) are described in detail. A Local Area Network (LAN) is a computer network with a limited area coverage, allowing devices to communicate and share resources. TCP/IP is the dominant data communication standard in exchanging data between computers. A router is a device that directs data traffic between networks with the best route decisions. Load balancing refers to the practice of distributing traffic evenly among resources or paths to improve performance and prevent overload. SD-WAN is a network technology that uses software concepts to distribute traffic across a wide area network more intelligently. VPN is an encrypted network for secure data transactions between authorized users. This research applies the Network Development Life Cycle (NDLC) methodology, which involves analysis, design, prototype simulation, implementation, monitoring, and management. Research data is divided into internal (from the school environment) and external (best practices from external sources). Test design involves stress test methods to assess network performance and reliability when exposed to extreme loads or pressure.

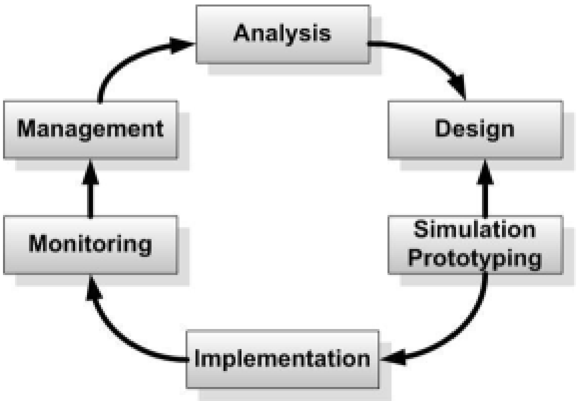


Figure 2. NDLC stages

Testing was carried out on the router and internet link of SMK IDN Bogor to ensure that the Load Balancing, VPN, and failover configurations functioned as expected. The test results will show how effective the implementation is in improving network performance and security. The testing stages for SDWAN Load Balancing implementation at IDN Bogor Vocational School have four main steps:

1) Testing the router's access to the internet aims to ensure that the router can access the internet segment stably and reliably.
2) Traffic load and Load Balancing testing is carried out to assess whether the traffic load is distributed evenly between internet links according to the load balancing concept.
3) Failover and backup transition testing aim to ensure that if one internet link goes down, the router can automatically switch to the link that is still active to prevent connection failure.
4) Testing user access to the internet is carried out to evaluate whether the user or user device can access the internet segment without problems.

After the testing process is complete, the processed data is used as a source of information for evaluating and updating the configuration applied to the network.

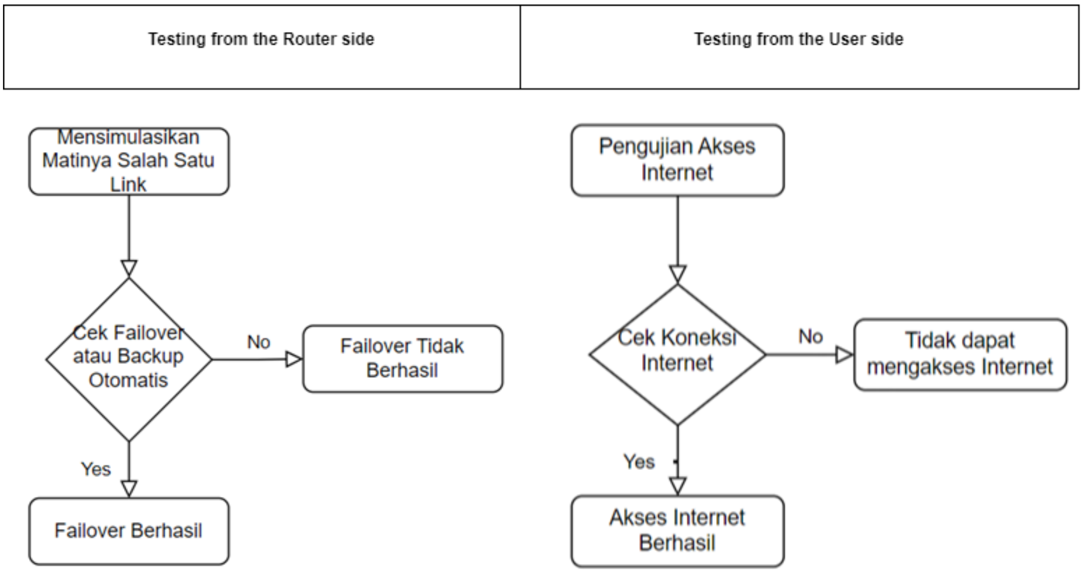

Testing from the Router side
Testing from the User side
Mensimulasikan Matinya Salah Satu Link
Cek Failover atau Backup Otomatis
No
Failover Tidak Berhasil
Yes
Failover Berhasil
Pengujian Akses Internet
Cek Koneksi Internet
No
Tidak dapat mengakses Internet
Yes
Akses Internet Berhasil

Figure 2. Flow of The Implementation Testing Stage
Source: data from the results of data processing.

3. Result and Discussion

3.1 Results

3.1.1 Research Tools

Research tools are important in this research, playing a role in collecting relevant data and information. In the IDN Vocational School network context, research tools involve Routers, Switches, Access Points, and endpoints such as PCs and Laptops. The IDN Vocational School IT team uses specific hardware, such as the Mikrotik RB951G-2HnD Router, Huawei ISP1 Modem, TP-Link ISP2 Modem, and HPE Switch.

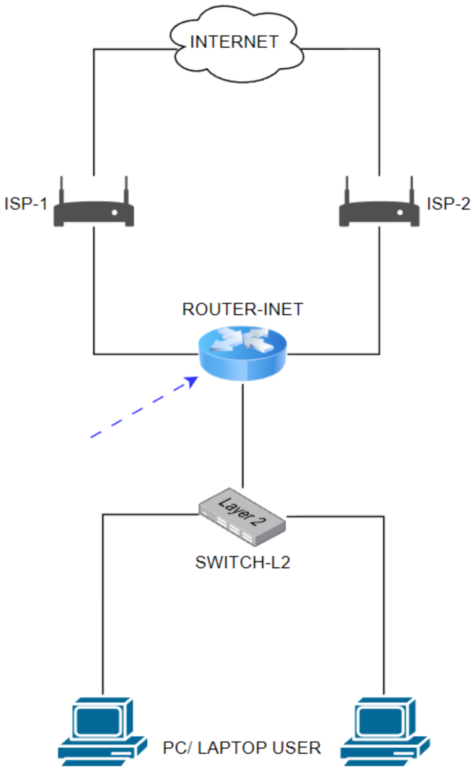


Figure 3. Types of Devices

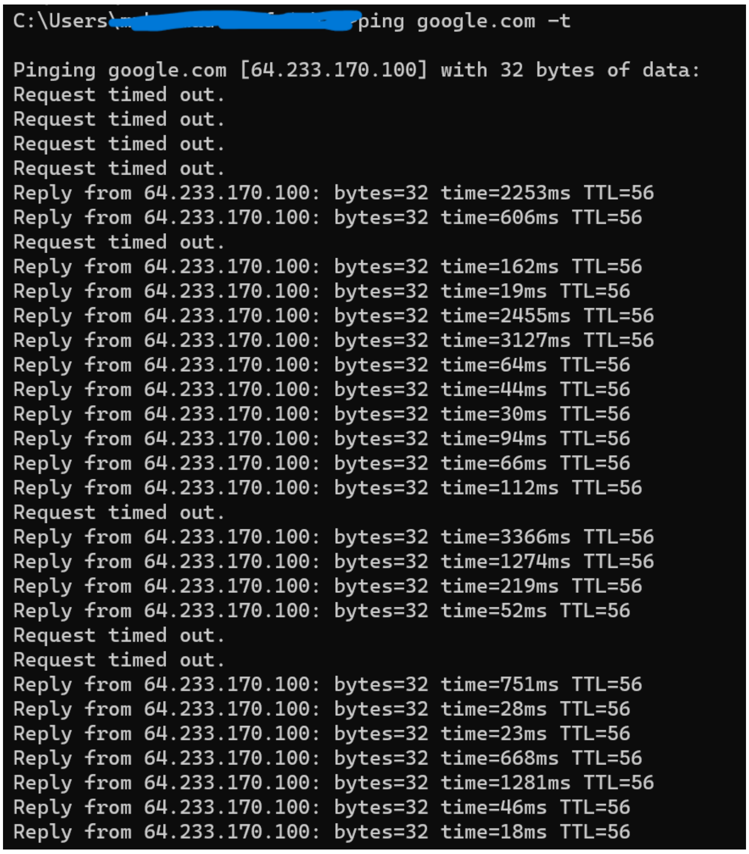
The following are the hardware specifications used:

Table 1. Types and Types of Devices

No.	Hardware	Specification	Description
1	Mikrotik Router	- CPU AR9344 600MHz	ROUTER-INET
		- Main Storage/NAND 64MB	
		- RAM 128MB	
		- LAN Ports 5	
		- Gigabit Yes	
2	Huawei ISP1 modem		ISP1
3	Modem TP-Link ISP2		ISP2
4	HPE Switches	- Managed Switch	SWITCH-L2
		- 24 x 10/100/1000Mbps Ethernet Ports	
		- 2 x SFP Gigabit Ports	

3.1.2 Implementation and Testing

Implementation is carried out with a scheme that involves several functions, including user/client device analysis. In Figure 4, several user devices/laptops experience problems with intermittent networks. Router side analysis (Figure 4) shows that there is only one active route.



```
C:\Users\[redacted]ping google.com -t

Pinging google.com [64.233.170.100] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 64.233.170.100: bytes=32 time=2253ms TTL=56
Reply from 64.233.170.100: bytes=32 time=606ms TTL=56
Request timed out.
Reply from 64.233.170.100: bytes=32 time=162ms TTL=56
Reply from 64.233.170.100: bytes=32 time=19ms TTL=56
Reply from 64.233.170.100: bytes=32 time=2455ms TTL=56
Reply from 64.233.170.100: bytes=32 time=3127ms TTL=56
Reply from 64.233.170.100: bytes=32 time=64ms TTL=56
Reply from 64.233.170.100: bytes=32 time=44ms TTL=56
Reply from 64.233.170.100: bytes=32 time=30ms TTL=56
Reply from 64.233.170.100: bytes=32 time=94ms TTL=56
Reply from 64.233.170.100: bytes=32 time=66ms TTL=56
Reply from 64.233.170.100: bytes=32 time=112ms TTL=56
Request timed out.
Reply from 64.233.170.100: bytes=32 time=3366ms TTL=56
Reply from 64.233.170.100: bytes=32 time=1274ms TTL=56
Reply from 64.233.170.100: bytes=32 time=219ms TTL=56
Reply from 64.233.170.100: bytes=32 time=52ms TTL=56
Request timed out.
Request timed out.
Reply from 64.233.170.100: bytes=32 time=751ms TTL=56
Reply from 64.233.170.100: bytes=32 time=28ms TTL=56
Reply from 64.233.170.100: bytes=32 time=23ms TTL=56
Reply from 64.233.170.100: bytes=32 time=668ms TTL=56
Reply from 64.233.170.100: bytes=32 time=1281ms TTL=56
Reply from 64.233.170.100: bytes=32 time=46ms TTL=56
Reply from 64.233.170.100: bytes=32 time=18ms TTL=56
```

Figure 4. User Side Analysis

```
[admin@MikroTik-MAIN] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp,
o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 A S 0.0.0.0/0 200.100.100.1 1
1 DS 0.0.0.0/0 192.168.200.1 1
2 X S 10.0.0.0/8 192.168.100.253 1
3 ADC 20.20.20.1/32 20.20.20.1 Loopback22 0
4 A S 80.80.80.80/32 103.111.212.1 1
5 ADC 103.111.212.0/30 103.111.212.2 ether2 0
6 ADC 192.168.1.0/24 192.168.1.1 ether3 255
7 ADC 192.168.200.0/24 192.168.200.15 ether5 0
8 ADC 200.100.100.0/30 200.100.100.2 ether1 0
[admin@MikroTik-MAIN] >
```

3.1.3 Design

The design involves managing the internet traffic and VPN process flow, as seen in Figure 5. This design ensures direct internet access via the modem while the connection between branches remains secure using an IPSec VPN.

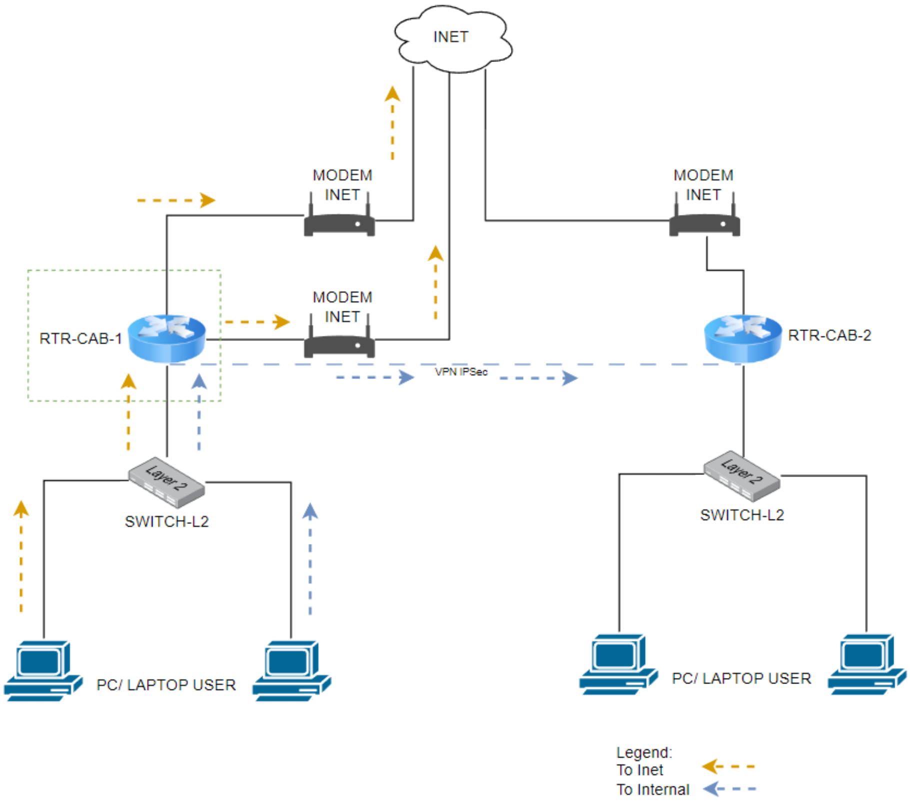


Figure 5. Internet and VPN Traffic Process Flow

In this design, two lines are used: Internet Line, which connects all devices to the modem directly; This path is used for general internet access and is represented by the default route via the modem gateway. VPN Line: Connects IDN Vocational School branches using an IPSec VPN connection. A specific route to the VPN subnet represents this path.

3.1.4 Testing

Testing is carried out using user devices that try to access the internet and also communicate between branches. In order to achieve the implementation objectives carried out in the IDN Vocational School branch environment, below we explain the methods used:

1) Analyze the overall condition of the internet network in the internet segment of the IDN Vocational School branch as well as make notes of any problems that may be the root cause/main problem they have.
2) Check how much bandwidth the IDN Vocational School Branch has, to ensure that there is no shortage of bandwidth when peak traffic/large traffic occurs on the internet network at the same time.
3) Carry out several additional configurations to achieve the goals of the current problem, including configuring the Per connection classifier for the Load Balancing function and VPN for the SDWAN function. For details, see the next point.

Further analysis of the router shows that there is a problem with the default route configuration. A configuration update was performed to fix the issue.

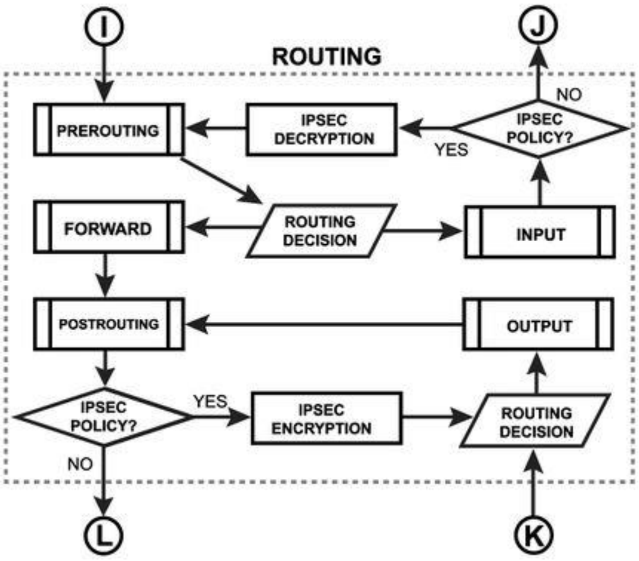


Figure 6. Default Route Configuration Update

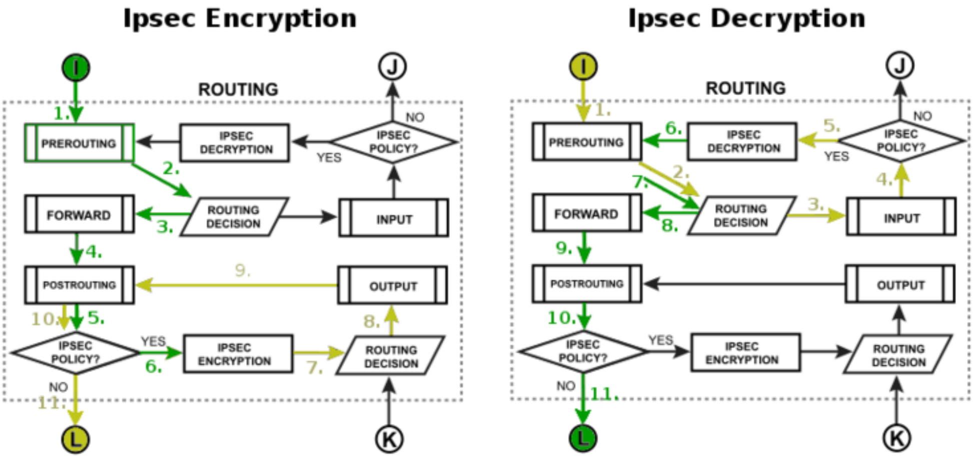
After the configuration update, testing was carried out again, and the results showed improvements in internet connections for all users. Each Routing protocol (except BGP) has its own internal table. This is where the routing decisions are made on a per-routing basis. BGP has no internal routing table and stores complete routing information of all peers in the RIB. The RIB contains routes that are grouped in separate routing tables based on their routing mark values. All routes without routing marks are stored in the main routing table. This table is used to select the best route. The main table is also used for next-hop lookups. The detailed information & configuration that will be implemented this time is as follows:

Table 2. Peer to Peer IP Address Information

No.	Device	IP Address	Notes
1	Mikrotik-BRANCH1	200.100.100.0/30	In the direction of ISP-1
2	Mikrotik-BRANCH1	103.111.212.0/30	In the direction of ISP-2
3	Mikrotik-BRANCH1	192.168.1.1/24	Towards User
4	Mikrotik-BRANCH2	192.168.200.1/24	Go to the ISP
5	Mikrotik-BRANCH2	10.10.10.1/24	Towards User

Source: data from the results of data processing

The second flow mechanism that will be used in this implementation will use an IPSec VPN flow diagram as follows:


Ipsec Encryption

Ipsec Decryption

Figure 7. IPSEC Flow Diagram

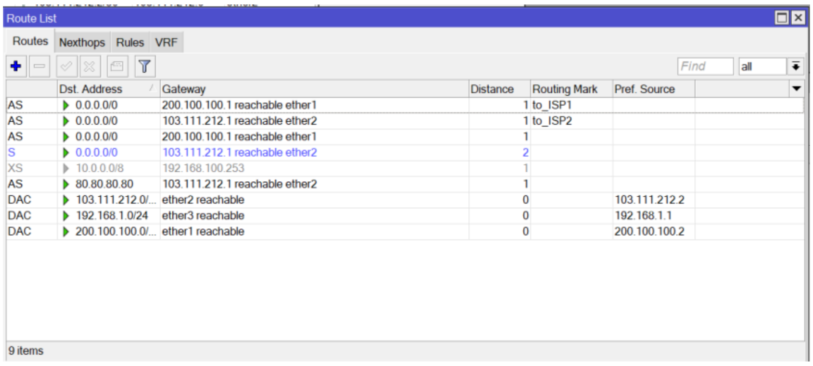
3.1.5 Final Test Results

The assessment and evaluation of the implementation results on the previously described devices became the focal point at this stage. Detailed explanations regarding the culmination of all configurations implemented and user testing perspectives are presented below. In the final testing step, the stress test method was chosen by the researchers as the most relevant and applicable approach according to the implementation context. After conducting in-depth analysis based on the data gathered in the previous sections, several changes and additions to the configurations of the devices became imperative. Detailed explanations of these changes, aimed not only at improving performance but also ensuring the optimal functionality of the devices owned by the SMK IDN IT team, are provided below:

1) First Change: IP Address Configuration
   This change involved additions and reconfigurations to the IP Address section, aligning with the transition from 1 MPLS link to 2 internet links.
2) Second Change: Default Route Configuration Adjustment
   Careful adjustment of the default route configuration on the SMK IDN router was made. Previously having only 1 default route via MPLS, the change was implemented by setting up 2 default routes equipped with load balancing and auto failover features.
3) Third Change: NAT Configuration Addition
   Adding NAT configuration became imperative considering the current connections used as internet links, which require NAT configuration for users to access the internet. Meanwhile, MPLS remains a private network for private link usage only.
4) Fourth Change: Load Balancing Configuration Addition
   Addition of Load Balancing configuration using the Per Connection Classifier method was implemented to ensure each connection has uniform traffic load, and both paths can be used simultaneously to minimize bottleneck traffic or overweight traffic.
5) Final Change: IPSec VPN Configuration Addition
   This configuration addition was aimed at meeting SD-WAN requirements, including establishing secure private connections between SMK IDN branches. IPSec VPN was chosen as the solution because it allows the formation of private connections via the internet with uniform profile and proposal requirements.

3.1.6 Final Testing Results from the User Side

At the final testing results stage from the user side, a series of tests are carried out to evaluate internet access and network conditions from the user's perspective. This includes stress tests to ensure network reliability in extreme situations. Testing covers various scenarios, such as user-side internet access, outage of the physical interface leading to ISP-2, and gateway relocation. Evaluation was also carried out on the condition of the default route configuration on the primary router after one of the internet links was turned off. Stress testing also involves shutting down the interface for failover testing and capturing the default route results when stress testing is performed. Additionally, test results from primary users to branches are also reflected in the final results. All documentation of the results of this testing provides an in-depth understanding of the network's readiness to face various scenarios and ensures that all configurations and changes that have been made function as expected. Final Result of Default Route After All Stress Tests Have Been Done and Returned to Original/Normal Condition with Both ISP Internet Links Can Run Simultaneously. Visualization of the final results of the default route condition on the router device after all stress tests have been carried out is presented in Figure 8.



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	200.100.100.1 reachable ether1	1	to_ISP1	
AS	0.0.0.0/0	103.111.212.1 reachable ether2	1	to_ISP2	
AS	0.0.0.0/0	200.100.100.1 reachable ether1	1		
S	0.0.0.0/0	103.111.212.1 reachable ether2	2		
XS	10.0.0.0/8	192.168.100.253	1		
AS	80.80.80.80	103.111.212.1 reachable ether2	1		
DAC	103.111.212.0/...	ether2 reachable	0		103.111.212.2
DAC	192.168.1.0/24	ether3 reachable	0		192.168.1.1
DAC	200.100.100.0/...	ether1 reachable	0		200.100.100.2

9 items

Figure 8. Final result of the default route condition on the router device
Source: data from the results of data processing

3.1.7 Socialization and Explanations that Have Been Done

Socialization and explanations regarding this project have been carried out online, considering the constraints of official travel, which prevents physical meetings for the IDN Vocational School IT team. Communication efforts continue to be carried out through the Gmeet platform and various documents, such as interviews, discussions, physical device inspections, and conveying information to students. This documentation includes various activities, as seen in Figure 9, which depict the interview and discussion process, physical inspection of the device, and interactions with students. Even though it is carried out online, this socialization remains an important part of ensuring a comprehensive understanding of the project and obtaining the necessary input and feedback from various related parties.

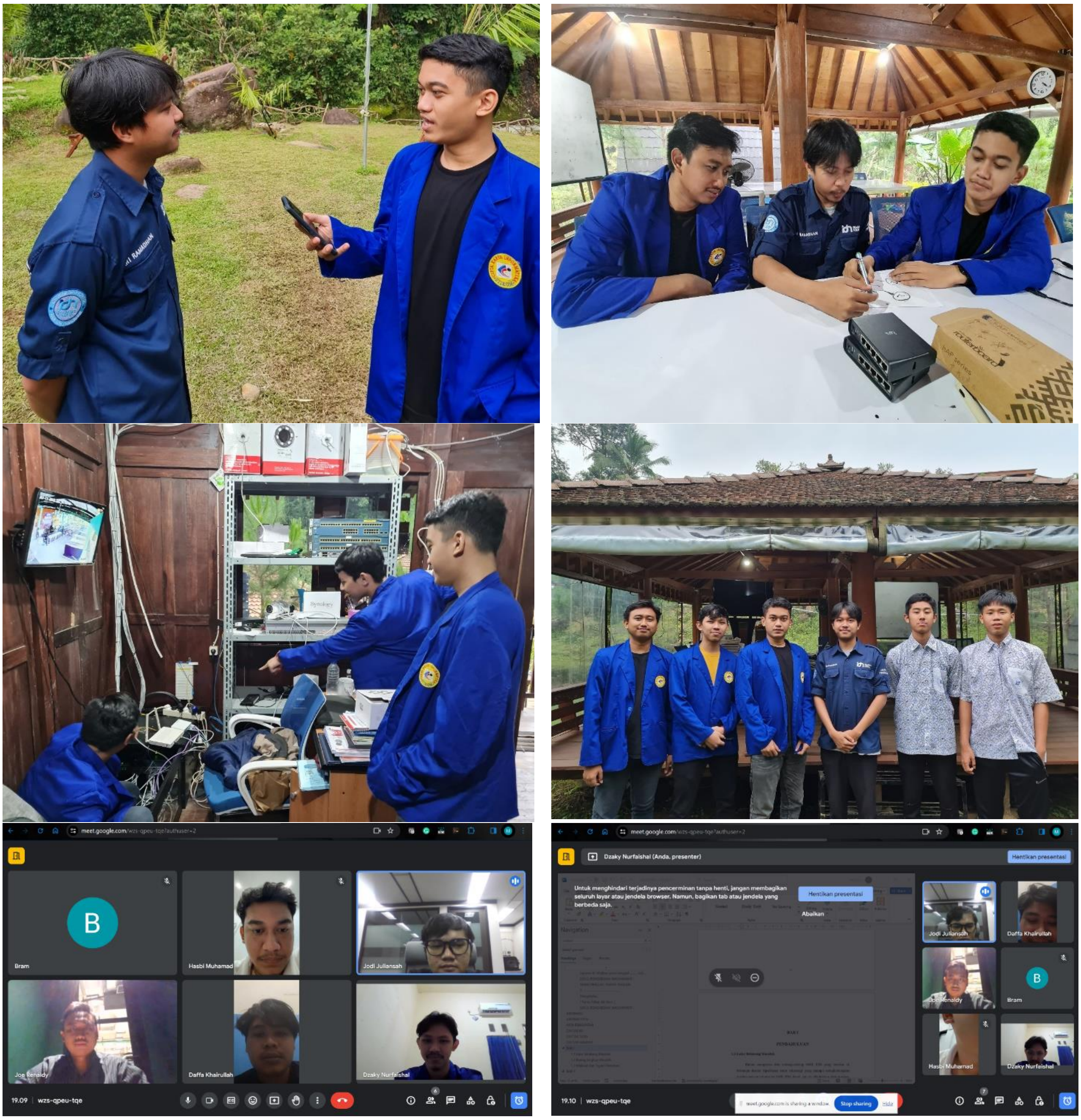


Figure 9. Activity Documentation

3.2 Discussion

The discussion of testing and implementation results is a crucial stage in this project, and it involves a series of thorough processes from the IDN Vocational School IT team. First, the research tools used are vital in the entire research. The hardware includes routers, switches, access points, and end devices such as PCs and laptops. The existence of specific hardware, such as the Mikrotik RB951G-2HnD Router, Huawei ISP1 Modem, TP-Link ISP2 Modem, and HPE Switch, is the primary basis for the process of collecting relevant data and information. After determining the hardware to be used, the implementation and testing stages are the next steps in ensuring the readiness of the IDN Vocational School network. The implementation scheme involves analysis of user/client devices, with a focus on connectivity and network performance. The results of this test show that there are problems, especially related to intermittent networks on several user devices/laptops.

Further analysis on the router side discovered an issue with the default route configuration, which was later fixed via a configuration update. Next, the design stage is crucial in designing the internet traffic and VPN process flow. This design aims to ensure direct internet access via modem while connections between branches remain secure using IPSec VPN. This arrangement requires special attention so that the process runs smoothly and by the specified requirements.

Testing is then carried out using user devices to evaluate internet access and communication between branches. A series of scenarios were tested, including analyzing the condition of the internet network as a whole, checking the amount of bandwidth owned by the IDN Vocational School Branch, and adding configurations such as Load Balancing and VPN for SDWAN. The results of this testing become the basis for the next stage, namely configuration updates to fix identified problems. Configuration updates are performed after identifying issues with the default route configuration. Change steps include:

1) Adjusting the IP Address.
2) Adding NAT configuration.
3) Load balancing.
4) Adding IPSec VPN configuration.

After all changes are implemented, testing is performed again to ensure that all configurations operate properly. The final results of the testing showed a significant increase in network performance and internet connections for all users. Lastly, socialization and an explanation of the project were carried out to related parties. Even though it is carried out online via the Gmeet platform and documents, this step is still essential to ensure a comprehensive understanding of the project and to obtain important input and feedback from various related parties. Thus, the entire implementation and testing process brings significant benefits to the readiness and performance of the IDN Vocational School network in facing existing challenges

4. Related Work

Studies conducted in network security optimization and load distribution offer significant contributions to understanding and improving modern information technology (IT) infrastructure. This research proposes several new approaches that combine VPN (Virtual Private Network), SD-WAN (Software-Defined Wide Area Network) technology, and load-balancing methods to optimize network security and performance. Research by Nana and Dadang Iskandar Mulyana (2022) highlights the importance of using IPSec and GRE VPNs to improve point-to-point network security. This study shows that implementing VPN technology with the proper protocols can significantly improve the security and privacy of data in the network. This research is an essential foundation for understanding the primary network security concepts via VPN [1]. However, a more recent study by Oky Tria Saputra *et al*. (2023) shows that using OpenVPN with the OSPF Routing Protocol can provide better optimization in load distribution and network security. They emphasize the importance of considering factors such as flexibility, scalability, and security in selecting appropriate technologies for network infrastructure [3]. In addition, research by Muhammad Fikri (2023) and Sahrul Hidayat (2023) discusses the implementation of SDWAN technology in the context of VPN and failover. They highlight the benefits of SDWAN in improving network performance and connection reliability, especially in scenarios where availability and reliability are critical [5][6].

Furthermore, research by Estu Rizky Huddiniah *et al*. (2018) explored route optimization for SDN-WAN using the OpenFlow protocol. They show that a centralized and automated approach can improve network management efficiency and speed up the response to environmental changes [7]. On the other hand, research by Enggar Bagoes Pabelan *et al*. (2023) highlighted implementing load balancing via PCC methodology to optimize internet usage across two ISPs. They emphasize the importance of using the right approach according to the organization's or network environment's specific needs [4]. Apart from that, some studies compare various protocols and technologies, such as those carried out by Ahmad Tariq Sabiq *et al*. (2023), who compared UDP and DCCP protocols in SD-WAN networks. This study highlights the importance of understanding the characteristics and advantages of each protocol to select the one that best suits network needs [9]. In security, research by Novandi Rizki Fattahillah *et al*. (2023) highlighted the importance of availability features on Fortigate firewalls using SD-WAN zone configurations and High Availability (HA) active-passive clusters. They show that integrating security features with the network infrastructure can improve defense against attacks and service reliability [17].

These studies prove that a deep understanding of various technologies, protocols, and network management methods is the basis for designing a secure, efficient, and reliable IT infrastructure. By continuing to integrate the latest research and considering evolving challenges in the world of IT, we can continue to improve the quality and reliability of networks to support the increasingly complex needs of organizations and their uses. Comparative analysis with previous research highlights several aspects that illustrate the significant progress obtained in this research. First, within the algorithm analysis framework, this research introduces the current implementation in a series of complex network architectures. In comparison, most previous research focuses on more straightforward methods or conventional paradigms. Thus, this research illustrates a substantial evolution in modern network design, underscoring the need for more sophisticated approaches to address increasingly complex challenges. Second, this study goes beyond previous research's limitations by evaluating network protocols' performance in a broader context, including more heterogeneous environments and more dynamic traffic scenarios. While previous research has often been limited to more controlled situations or more straightforward simulations, the approach proposed in this research provides deeper insight into the behavior of network protocols in complex real-life scenarios.

Furthermore, this research highlights the importance of security aspects in network design, focusing on detecting and mitigating increasingly complex and distributed threats. Although network security has been the focus of previous research, this research offers a more proactive and adaptive approach to dealing with rapidly evolving threats, demonstrating a commitment to an increasingly important security aspect in an ever-evolving network environment. It is also essential to emphasize sustainability and energy efficiency in network operations, which may have yet to be explicitly considered in previous research. Thus, this research makes a substantial contribution to broadening the understanding of how network designs can be optimized from a performance and security perspective and an environmental impact and sustainability perspective. Finally, this research produces new methods and tools practitioners can employ to design, implement, and manage networks more effectively. While previous research may have been more oriented toward theoretical or experimental approaches, this research focuses more on practical solutions that can be implemented in natural production environments. Thus, comparison with previous research confirms that this research not only fills the knowledge gap in the field of computer networks and information technology but also makes a substantial contribution to pushing the boundaries of existing knowledge.

5. Conclusion and Recommendations

Several important conclusions can be drawn based on the results of research on the Application of SD-WAN Load Balancing Technology in the management of IDN Vocational School branches. This research is a response to the development of internet technology, which is increasingly dynamic and demands features and technology that can meet various operational and network security needs. This research focuses primarily on optimizing internet links, which has been a significant administrative and functional challenge. This research responds to the rapid growth of IDN Vocational Schools since 2016, which requires an effective solution to manage interconnections between branches while still considering link flexibility and associated costs. SD-WAN Load Balancing offers a profitable solution by increasing the flexibility of link usage, dividing traffic loads on a priority scale, and automatic backup features to improve network reliability. The SD-WAN Load-balancing method has proven effective in overcoming the challenges faced by IDN Vocational Schools while maintaining network capability and stability. The research results show that by implementing this method, IDN Vocational School can achieve monthly cost efficiency of up to 63%, as depicted in A comparison of monthly costs before and after using SD-WAN Load Balancing highlights the significant impact that can be achieved in terms of efficiency.

Regarding suggestions for further implementation, the researcher suggested several steps to SMK IDN Bogor to improve the SD-WAN load-balancing implementation results:

1. Routine monitoring should occur several days or weeks after implementation to ensure no new problems arise.
2. Carryar security checks must be carried out to ensure the security of the router device by periodically updating the permitted ac
3. Consider, consider upgrading the bandwidth if the user needs to continue to increase so that the connection does not experience disruption due to limited.

Implementing new technologies such as SD-WAN Load Balancing requires ongoing maintenance and monitoring to ensure optimal performance and overall system security. By implementing these suggestions, IDN Bogor Vocational School can maximize the benefits of this technology in its daily operations.

References

[1] Mulyana, D. I. (2022). Optimasi Keamanan Jaringan Point to Point Menggunakan VPN IPSec dan GRE. *JUPITER: Jurnal Penelitian Ilmu dan Teknologi Komputer*, *14*(2-b), 297-305. https://doi.org/10.5281./5094/5.jupiter.2022.10.

[2] Wahyudi, U., Mulyana, D. I., & Akbar, Y. (2023). Optimasi Internet Gateway Menggunakan Virtual Router Redundancy Protocol. *Progresif: Jurnal Ilmiah Komputer*, *19*(1), 29-38. http://dx.doi.org/10.35889/progresif.v19i1.988.

[3] Saputra, O. T., Mulyana, D. I., & Akbar, Y. (2023). Optimasi Pembagian Beban Dan Keamanan Jaringan Menggunakan OpenVPN Dengan OSPF Routing Protocol. *Progresif: Jurnal Ilmiah Komputer*, *19*(1), 61-70. http://dx.doi.org/10.35889/progresif.v19i1.969.

[4] Pabelan, E. B., Salim, A., Raizaldi, A., & Rizal, R. (2023). Implementasi Load Balancing Metode PCC (Per Connection Classifier) untuk Oplimalisasi Internet dengan 2 ISP (Studi Kasus Pt. Zyrexindo Mandiri Buana Jakarta). *Jurnal Bidang Penelitian Informatika*, *1*(2), 105-118.

[5] Fikri, M., & Rifqi, M. (2023). Implementasi VPN Antar Cabang Menggunakan Teknologi SDWAN dengan Metode Load Balance (Studi Kasus: PT. Mitra Solusi Infokom). *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *10*(1), 105-113.

[6] Hidayat, S., & Akbar, Y. (2023). IMPLEMENTASI FAILOVER VPN KANTOR PUSAT DAN CABANG MENGGUNAKAN TEKNOLOGI SDWAN DENGAN STRATEGI BEST QUALITY. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, *4*(3), 1598-1608. https://doi.org/10.35870/jimik.v4i3.386.

[7] Huddiniah, E. R., Safitri, E. M., Priyambada, S. A., Nasrullah, M., & Angresti, N. D. (2018). Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *13*(1), 7-13.

[8] Fauziah, A. D. N., Nirwana, H., Litha, A., & Mahjud, I. (2022). Analasis Penerapan Teknologi Traffic Steering SD-WAN Menggunakan Perangkat FortiGate. *Jurnal Teknologi Elekterika*, *19*(2), 97-105.

[9] Sabiq, A. T., Karimah, S. A., & Jadied, E. M. (2023). Analisis Perbandingan UDP dan DCCP Pada Jaringan SD-WAN. *eProceedings of Engineering*, *10*(3).

[10] Ardianto, F., Alfaresi, B., & Darmadi, A. (2018). Rancang Bangun Load Balancing Dua Internet Service Provider (ISP) Berbasis Mikrotik. *Jurnal Surya Energy*, *3*(1), 198-202. https://doi.org/10.32502/jse.v3i1.1232.

[11] Oktariyadi, R., Ruslianto, I., & Bahri, S. ANALISA KINERJA LOAD BALANCING MENGGUNAKAN METODE ROUND ROBIN DAN WEIGHTED ROUND ROBIN. *Coding Jurnal Komputer dan Aplikasi*, *9*(01), 131-141. https://dx.doi.org/10.26418/coding.v9i01.45871.

[12] Octavriana, T., Joni, K., & Ibadillah, A. F. (2021). Optimalisasi Jaringan Internet Dengan Load Balancing Pada High Traffic Network. *Jurnal Teknik Informatika*, *14*(1), 28-39. https://doi.org/10.15408/jti.v14i1.15018.

[13] Almakhi, R., & Nugraha, F. S. (2022). Implementasi Load Balancing Dan Failover Menggunakan IP SLA Pada PT Pan Pacific Insurance. *Jurnal Infortech*, *4*(2), 98-104. https://doi.org/10.31294/jtk.v10i1.19054.

[14] Satriawan, M., & Soewito, B. (2022). DESIGN OF SD-WAN ON INSURANCE HOLDING COMPANY PT. XYZ USING ON-DEMAND TUNNEL FULL MESH CONNECTIVITY. *Jurnal Pendidikan Tambusai, 6*(1), April.

[15] Alviendra, I. M., Setijadi, E., & Kusrahardjo, G. (2022). PENGEMBANG & PENERAPAN SISTEM VIRTUAL PRIVATE NETWORK (VPN) PADA INTERNET OF THINGS (AOI) MENGGUNAKAN SIMULASI. *Jurnal Teknik ITS, 11*(1), Januari.

[16] Syarif, R. F., & Sobari, I. A. (2022). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN METODE PPTP PADA PT. SINAR QUALITY INTERNUSA. *Jurnal Pendidikan Tambusai, 6*(2), Agustus.

[17] Fattahillah, N. R., Nurfadila, F., & Setiawan, Y. (2023). IMPLEMENTASI AVAILABILITY PADA FORTIGATE FIREWALL MENGGUNAKAN SD-WAN ZONE & HA CLUSTER ACTIVE-PASSIVE. *Jurnal Multi disiplin, 2*(11), Agustus.

[18] Dewi, S. (2020). KEAMANAN JARINGAN MENGGUNAKAN VPN (VIRTUAL PRIVATE NETWORK) DENGAN METODE PPTP (POINT TO POINT TUNNELING PROTOCOL) PADA KANTOR DESA KERTARAHAJA CIAMIS. *Jurnal Sains dan Manajemen, 8*(1).

[19] Mujiastuti, R., & Prasetyo, I. (2021). MEMBANGUN SISTEM KEAMANAN JARINGAN BERBASIS VPN YANG TERINTEGRASI DENGAN DNS FILTERING PIHOLE. *Jurnal Prosiding seminar Nasional Sains, 1*(1), November.

[20] Budimulya, T., & Safitri, M. (2022). PERANCANGAN VPN SEBAGAI SISTEM INFORMASI KEPEGAWAIAN PADA KANTOR KEMENTERIAN KESEHATAN RI. *Jurnal Informatika, 6*(2), Juni.

[21] Bakri, A., & SW, S. (2019). PEMODELAN JARINGAN KOMPUTER MENGGUNAKAN SITE TO SITE VPN PADA RUMAH SAKIT JUWITA BEKASI. *Jurnal Teknokris, 22*(2), Desember.

[22] Musril, H. A. (2019). DESAIN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS OPEN SHORTEST PATH FIRST. *Jurnal Nasional Informatika dan Teknologi Jaringan, 3*(2), Maret.

[23] Luthfi, Firdhaus,Fatmawati, & Wijonarko, B. (2019). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) IP SECURITY SITE TO SITE PADA KEMENTRIAN PERHUBUNGAN. *Jurnal Inti Nusa Mandiri, 14*(1), Agustus.

[24] Agustyaningsih, P., Prihantoro, C., & A, I. K. (2023). Analisis Performansi Jaringan Komputer Menggunakan Metode Unequal Load Balance Pada Jaringan Lokal. *Jurnal Pendidikan Teknologi Informasi, 3*(2), September.

[25] Surimi, L., Subardin, & Nurmiati. (2022). Analisis Kinerja Load Balancing Terhadap Jaringan Internet Menggunakan Metode Equal Cost Multi Path (ECMP). *Jurnal Digital Transformation Technology (Digitech), 2*(2), November.

[26] Mustofa, A., & Ramayanti, D. (2020). IMPLEMENTASI LOAD BALANCING DAN FAILOVER TO DEVICE MIKROTIK ROUTER MENGGUNAKAN METODE NTH (STUDI KASUS : PT. GO-JEK INDONESIA). *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK, 7*(1), Februari.

[27] Rijayana, I. (2005). TEKNOLOGI MULTI PROTOCOL LABEL SWITCHING (MPLS) UNTUK MENINGKATKAN PERFORMA JARINGAN. *Jurnal Seminar Aplikasi Teknologi Informasi 2005, Juni.*

[28] Nurhasanah, N. A., Wahidah, I., & Cahyono, B. (2017). IMPLEMENTASI SEAMLESS MULTIPROTOCOL LABEL SWITCHING(MPLS) PADA JARINGAN MPLS. *Jurnal Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri 2017, Februari.*

[29] Syaputra, A. W., & Assegaff, S. (2017). ANALISIS DAN IMPLEMENTASI LOAD BALANCING DENGAN METODE NTH PADA JARINGAN DINAS PENDIDIKAN PROVINSI JAMBI. *Jurnal Manajemen Sistem Informasi, 2*(4), Desember.

[30] Maulana, A., & FAUZI, A. (2018). PVST dan Load Balancing. Dalam *Buku Jaringan Komputer* (Edisi pertama, Bab IV, pp. 27 – 31). Indonesia:Universitas Nusa Mandiri.

[31] Hafizh, M. (2011). Load Balancing dengan metode per connection classifier menggunakan proxy server sebagai caching. Indonesia:UIN Jakarta.

[32] Warnilah, A. I., & Simpony, B. K. (2019). Load Balancing. Dalam *Buku Ajar Jarkom* (Edisi pertama, Bab 12, pp. 66 – 67). Indonesia:Universitas BSI.

[33] Sukaridhoto, S., ST. PhD. (2014). Load balancing dan Scalability. Dalam *Buku Jaringan Komputer* (Edisi Kedua, Bab 8, pp. 154 – 165). Indonesia:Politeknik Elektronika Negeri Surabaya.

[34] Utomo, A. D. (2011). Implementasi Load Balancing Dua Isp Menggunakan Mikrotik. Indonesia:UIN Jakarta.

[35] Sukendar, T. (2017). Keseimbangan Bandwidth Dengan Menggunakan Dua ISP Melalui Metode Nth Load Balancing Berbasiskan Mikrotik. *J. Tek. Komput. Amik Bsi, III*(1), 86–92.