jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 4, PP. 960-967
Manuscript received July 01, 2024; revised October, 2024. doi: 10.24425/ijet.2024.152083

Software Define Wide Area Network (SDWAN) network optimization analysis on radiolink-fiber optic access media migration

Beny Nugraha, Muslim Muslim, Mega Nur Khotimah, Lukman Medriavin Silalahi, Dhiya Akmal Firdaus, and Christ Geofany

***Abstract*—The development of technology in radiolink networks has grown rapidly and is suitable to be implemented on wide coverage area networks, but weather and physical environment factors greatly affect signal conditions. The background that has been stated, this study proposes migration to fiber optic access media because it is able to send data faster and is not affected by electromagnetic interference and is stable. Furthermore, this study conducted an optimization analysis on the SDWAN (Software Defined Wide Area Network) network, SDWAN functions as a firewall that can provide connectivity support and infrastructure network development in branch offices with system security in one centralized platform. The test method used in this study is a connectivity test from each remote fortigate located in the branch office. While the analysis method used is Quality of Service (QoS), which is a method to find out data delivery (Packet Loss, Delay and Jitter) using the FortiManager application, which is the analytical and experimental proof of concept of the SDWAN network model using the BGP method for auto failover testing.**

***Keywords*—SD-WAN; Radiolink; QoS; Firewall; ISPs**

I. Introduction

THE development of technology in radiolink networks has now grown rapidly. Users can connect by accessing files in the form of data, images and videos and making an internet connection without the need to use cable media. Radiolink is very suitable for use in networks with a wide coverage area, but signal strength is highly dependent on weather conditions and is influenced by the physical environment as a barrier. Such conditions require the replacement of access media, then migration to Fiber Optic (FO). FO is able to transmit data faster and is not affected by electromagnetic interference so that it can be more stable in use [1].

According to [2] that Metro Ethernet (ME) is an Ethernet-based high capacity data network service that provides flexibility and Quality of Service (QoS) assurance for customers, but the QoS results in ME settings are less than optimal because the access media used is still radiolink so that internet links need to be optimized.

SDWAN (Software Defined Wide Area Network) solution can support connectivity and infrastructure network development in branch offices with system security in one centralized platform. SDWAN solution is to build an integrated application system with full services and integrated security, so that it is more effective and secure in supporting WAN (World Area Network) connectivity. SDWAN will minimize early detection if there is cybercrime [3].

Based on the results of research [4]–[6], it is proposed to develop a Traffic Engineering (TE) algorithm to improve overall network availability and ensure the protection and recovery of SDWAN networks through the TE method to efficiently manage network traffic among Customer Premises Edge (CPE) and maintain the availability of internet services. SDWAN supports different services over a public WAN with dynamic configuration within the device according to network measurements and service requirements.

According to literature review [7]–[9] proposed the Internet Protocol Security (IPSec) method. IPSec is a protocol method that defines cryptographic algorithms for encryption, authentication, and describes the packets that provide security at the IP layer. Fiber optic access is highly recommended due to the delay of 0.105s, packet loss of 1%, and the dual link latency is very good based on ITU-T standards. Failover configuration during dual-link implementations can minimize downtime by 80%.

Furthermore, based on the results of research [10]–[12], it is revealed that the use of QoS methods to manage bandwidth, delay, packet loss and jitter in the flow network. Internet network QoS analysis prioritizes the monitoring and measurement process to improve QoS parameters and strive to improve congested traffic and avoid congestion. Based on [13] explain the comparison of network service performance between two internet service providers using QoS parameters.

Furthermore, [14]–[16] explained that the multi-constrained multi-objective algorithm method successfully optimizes the path and ensures the flow of requests that are sensitive to delay, and makes better use of network resources. The evaluation model is based on delay propagation, bandwidth, and issues with jitter for SDWAN. The results show that the proposed algorithm successfully reduces the average propagation delay to a certain extent and ensures the load balance between different domains. However, the SDWAN results, on the controller, are optimally deployed, without considering the delay between the controller and the switch.

This has been studied by several research results and hypotheses reveal that the analysis of the SDWAN model by designing a backup link using a failover system on access media

The first, until fourth authors are with Universitas Mercu Buana, Indonesia (e-mail: benynugraha@mercubuana.ac.id, mus2828@gmail.com, lukmanmedriavinsilalahi@lecturer.unsia.ac.id, meganurkhotimah99@gmail.com).

The fifth and sixth author is with PT. Datacomm Diangraha, Indonesia (e-mail: akmlfrds20@gmail.com, geofanychrist@gmail.com).

migration provides new convenience to the firewall and SDWAN configuration that is integrated with the security system so that the branch network is not too long in a downtime condition. Based on the statement, it becomes a novelty of research.

Based on observations on existing networks, the use of radiolinks can hinder internet services so that Service Level Agreement (SLA) are not met. So, the novelty of this research is to make efforts to improve the quality of SLA by building a network system that can overcome ongoing disruptions in customer branches by migrating access media and designing backup links with a failover system equipped with SDWAN technology.

Next, this research supports the 9th Sustainable Development Goals (SDGs), namely building resilient infrastructure, promoting inclusive and sustainable industrialization, and encouraging innovation involving various parties, including Internet Service Provider (ISP) managers, and companies. This research contributes to the development of network security research, so that users can experience the benefits of secure network security. Through Steps towards achieving SDG 9, this research can increase innovation in network security systems.

Based on the background, this research has a state of art and novelty in the analysis of the SDWAN model with a backup link designer using a failover system. This brings new convenience to the firewall with SDWAN configuration integrated with the security system. So, the purpose of this study:

1. Improve quality by changing the access media from radiolink to fiber optic.
2. Migrate services from metro ethernet to internet and create backup links with SDWAN technology.

II. Research Method

Figure 1 shows the results of the network topology. The topology used is the star topology because of its advantages to facilitate the detection of damage to the network and if one device is damaged, it will not interfere with other devices. This research service network scheme includes ME – backhaul interconnection using radiolink access media. It takes 2 (two) routers to connect to the internet so that users can browse.

Furthermore, entering the stage of migrating access media to FO and changing services from ME to SDWAN internet, from the backhaul is directed to the FortiGate 100F device which functions as a link from the remote FortiGate which is in one branch to another, so that it can be interconnected with each other. If the FO experiences an outage or known as FO-cut on the FO cable path towards the FortiGate interface, it will result in the connection to the company's application not being able to operate. So, when that happens, a network backup is applied as an effort when the main link is disconnected using another provider.

After that, the branch location uses the FortiGate 50E as a router and firewall, which connects the branch office network with the head office network. Furthermore, it serves to connect branch networks to the internet. This is a replacement for the two routers previously used in ME services, with SDWAN technology minimizing device usage making it easier to configure the network and save on installation costs. Table I is a list of router interface allocations, and table II describes software and hardware specifications.

Table I
List of Interface Allocations

No	Value (%)	Description	IP Address	Remote Device
1	WAN1	Main Link	202.152.22.33	Router ISP Main
2	WAN2	Backup Link	182.23.40.149	Router ISP Backup
3	LAN	To-LAN	192.168.210.254	Client
4	Tunnel SPOKE-M	Tunnel Main Link	169.254.253.254	FortiGate 100F
5	Tunnel SPOKE-B	Tunnel Backup Link	169.254.254.254	FortiGate 100F

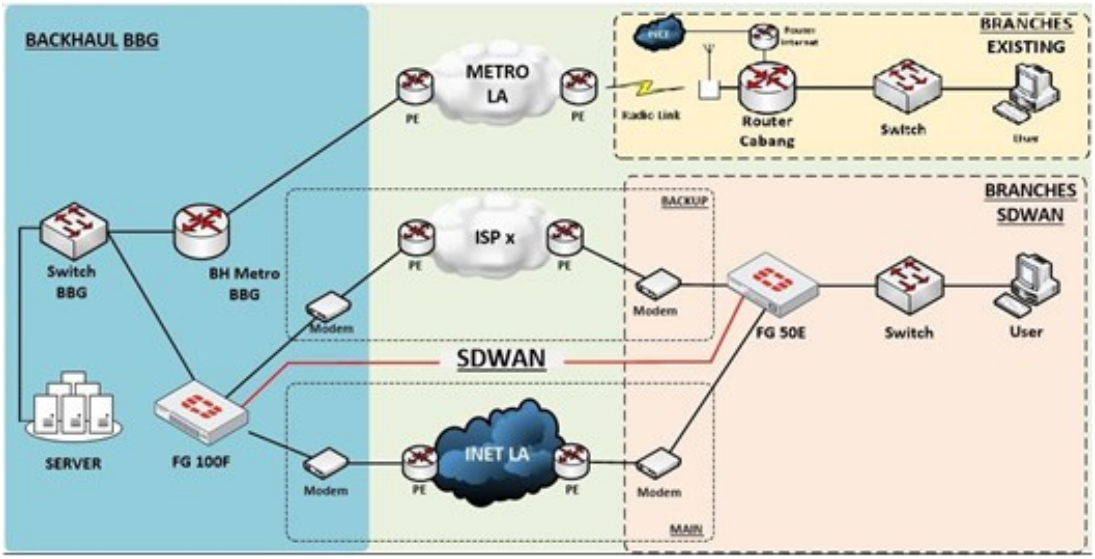

Fig. 1. Network topology design

TABLE II
LIST OF HARDWARE AND SOFTWARE

No	Category	Description	Remark
1	Software	FortiManager	v6.4.2 GA *build*1112
2	Software	FortiGate	v6.4.2 GA *build*2112
3	Software	SIAE Microelettronica	N10052 01.04.08
4	Software	System Operation	Windows 10 Pro Home
5	Hardware	Laptop	Intel® Core™ i7-8550UCPU @1.80 GHz 1.99 GHz + RAM 8 GB
6	Hardware	Modem	*Raisecom* HT803G
7	Hardware	Router	*Fortigate* 100F dan 50E
8	Hardware	Radiolink	*SIAE ALCplus2* diameter 0.6m

A. Existing Network

Existing networks use electromagnetic wave transmission media in transmitting information with the help of microwave antenna devices. On the customer side, the device used is a SIAE radiolink type ALCplus2 which functions as an outdoor unit (ODU) and indoor unit (IDU).

Figure 2a describes ODU microwaves that are installed on rooftops or tall buildings or towers to obtain a Line of Sight (LOS) between the two ends of the microwave. Figure 2b described the IDU, IDU is installed in the server room and serves as an interface between the user's devices. All displays related to the device system, namely frequency settings, Tx power settings, Rx power settings, remote controls, alarm conditions, can be accessed through the IDU. The interface used between IDU and ODU is a coaxial cable [17].

After the antenna and modem are installed, then tests are carried out to determine the quality of transceiver on the central side. This quality check uses the SIAE Microelettronica application. The signal range is categorized as good ranging from -40 to -75 dBm. Figure 3 shows the degradation due to the signal quality performance of the service used at -77dBm. Figure 4 shows the observation results on the remote side and obtained a signal quality performance of -80dBm, this result is worse than the quality when compared to the center side antenna.

Fig. 2. Radiolink (a) ODU (b) IDU

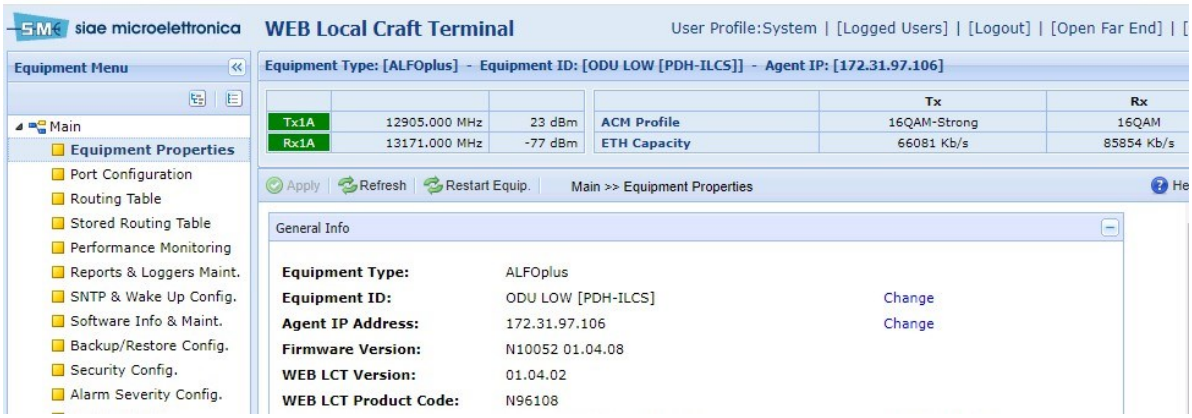

Fig. 3. Center-side antenna signal quality

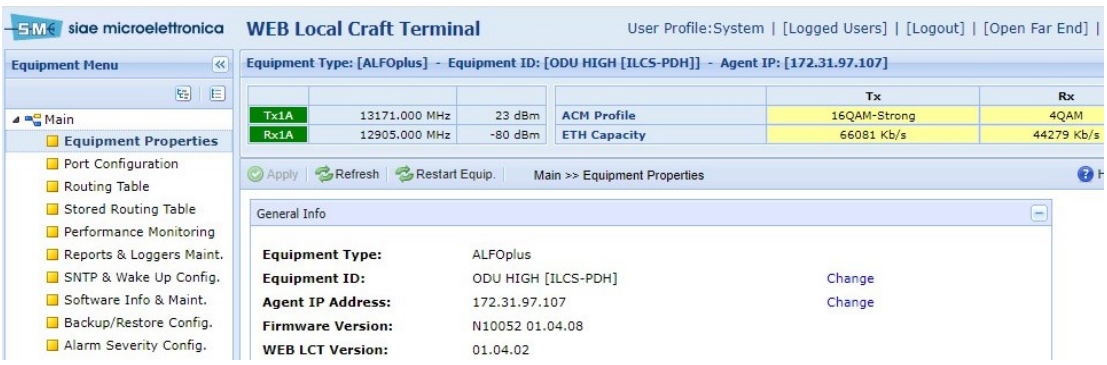

Fig. 4. Remote side antenna signal quality

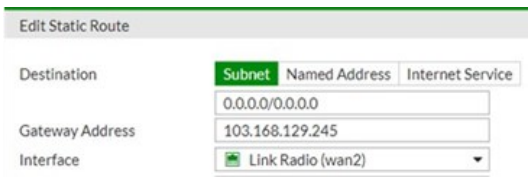

Fig. 5. Radiolink static route configuration

B. Radiolink Configuration on Metro Ethernet Service

Link checks using radiolink access are done by ping detik.com and google using the features found on FortiGate. Figure 5 shows the IP allocation for the customer which is 103.168.129.245/29. Figure 6 can be described:

1. The results of the packet loss quality check to detik.com get 26% and google ping of 19%. Meanwhile, the TIPHON standard that packet loss in the good category is in the range of 3 to 14 %.
2. The result of the latency/delay quality check, ping to detik.com gets 245.06ms and google gets 201.8ms. Meanwhile, according to the TIPHON standard, the latency of the good category is in the range of 151 to 300 ms, which can be interpreted for radiolink latency is still said to be good.
3. Jitter quality check result, ping to detik.com get 84.19ms and google get 117.62ms. Meanwhile, according to the TIPHON standard, the jitter of the good category is in the range of 75 to 124 ms. Referring to the results of the radiolink latency is included in the good category.

Figure 7 shows a quality test using PRTG. Referring to the ping monitoring capture, the ping time was unstable and there was an average request time out of 575msec, packet loss of 17% and downtime of 14%. For the high request time out and delay ping, this is due to the radio signal between the central side radiolink and the remote side radiolink being disconnected due to poor signal quality. Furthermore, Figure 8 shows that the jitter test results are at an average of 185ms, which is included in the medium category based on the TIPHON standard.

III. Result And Discussion

This section discusses the implementation and analysis of access and service changes obtained from the test scenarios and planned network topologies. However, the reference Key Performance Indicator (KPI) is 99.8%, so in a month it is only allowed to downtime, or the link is dead for 3-4 hours.

In the topology, from the server to the switch located in the backhaul or center using the FortiGate 100F uses static IP settings on the ethernet port whose function is to make the IP configured dedicated, so that it does not change dynamically. Furthermore, data traffic coming from the ISP will flow through the utp cable to the main router or FortiGate 50E using SDWAN technology. Then the traffic will be forwarded to the customer's LAN, through a switch so that it can be connected to several users. SDWAN technology enables secure connection with branch and backhaul applications through centralized architecture support.

Fig. 6. Radiolink performance

Fig. 7. PRTG *ping radiolink*

Date Time	Jitter	Execution Time	Downtime	Coverage
Averages (of 50 values)	185	43,206 msec	59 %	100 %

Fig. 8. PRTG *jitter radiolink*

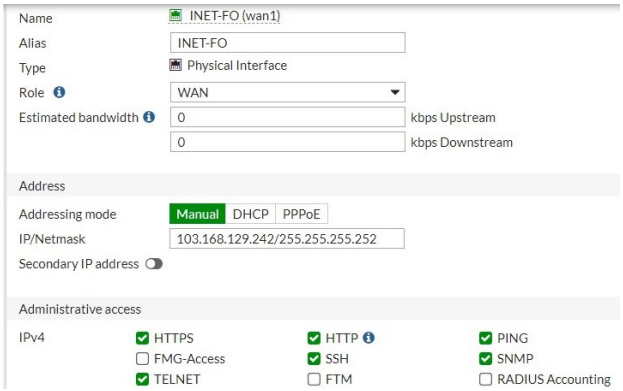

Fig. 9. FO interface configuration

A. Router Interconnect using fiber optic

Previously, it had been simulated using radiolink access as a physical connection too. The next simulation uses FO. The following is a comprehensive discussion.

1. Router Configuration

Figure 9 shows the configuration of the FortiGate interface using FO access. FortiGate can be accessed through an interface that has a well-known port limit that has been defined, namely HTTPS, HTTP, SSH, SNMP, PING, TELNET. Well known port is a list of port numbers that are known in general for the use of a service so that it cannot be used by other services. However, there are some that are not chosen because they adjust to the needs of the location.

Figure 10 shows the static route configuration to enable the FortiGate routing function to connect to the internet by listing the target destination IP Address prefix 0.0.0.0/0 (default route) using the peer IP address of the internet as the next hop.

2. FO Network Monitoring

Figure 11 shows the monitoring of the PRTG server towards the IP address of the FortiGate, the packet loss when switching to FO, on the green graph has an average of 1% including the very good category. Packet loss is the failure of the process of transmitting data to the destination address so that some data is found lost. Furthermore, the tosca graphic is the minimum value that functions to send files, while the blue graphic is the maximum value that is useful as a process of receiving or retrieving files from the server to the user. The pink graphic is the average value between the sender and receiver of the file.

Furthermore, jitter monitoring, which is a time lag in receiving packages that are not received together. If the load is heavier, the potential for collisions between packages will also increase. Figure 12 shows a jitter result of 34.9ms and is categorized as very good based on the TIPHON standard.

Destination	Gateway IP	Interface	Status
IPv4 4			
0.0.0.0/0	103.168.129.241	INET-FO (wan1)	Enabled

Fig. 10. Static route configuration

Date Time	Ping Time	Minimum	Maximum	Packet Loss	Downtime	Coverage
Averages (of 120 values)	2 msec	1 msec	4 msec	1 %	0 %	100 %

Fig. 11. Ping test

Fig. 12. Jitter test

3. Comparison of FO with Radiolink

This section discusses the results of the fiber optic access check using radiolink before being set up using SDWAN, table 3 is a reference for monitoring using fortigate, in the results of the inspection obtained a packet loss of 26%. The delay is 245.06 ms, and the jitter is 84.19 ms.

TABLE III
RADIOLINK ACCESS PERFORMANCE

Parameter	Result	Category
Packet Loss	202.152.22.33	Bad
Delay	182.23.40.149	Good
Jitter	192.168.210.254	Good

Table 4 is the results of the examination using fiber optic access, in the results of the examination obtained packet loss of 0.00%, delay of 4.04ms, and jitter of 1.55ms.

So based on table 3 and table 4 showing a comparison of link quality using radiolink and fiber optic access media, it can be revealed that fiber optic links are much better than radio links. Thus, this support is a reinforcement for the migration of access media to fiber optic.

TABLE IV
FO ACCESS PERFORMANCE

Parameter	Result	Category
Packet Loss	0%	Very Good
Delay	4.04ms	Very Good
Jitter	1.55ms	Very Good

B. FO Configuration using SDWAN

Configure the FO interface using manual addressing mode, by entering the IP that has been allocated by the ISP as shown in figure 13. After configuring the FO interface, proceed by setting up the tunnel. Tunnel is a way for branch FortiGate to be able to connect privately to backhaul FortiGate via the internet.

The first stage is to create a tunnel between the branch FortiGate to the FortiGate backhaul. Then, the branch will customize the tunneling process by using the same encryption method used by FortiGate backhaul. Then, the branch will direct the tunnel created towards the FortiGate public IP backhaul.

Each link (main link and backup link) uses its own tunnel interface, which points to the backhaul FortiGate IP address. After the 2 (two) FortiGate have been connected, the process of creating an interface tunnel has been completed.

SDWAN is designed to be redundancy with different dual paths between the main link and the backup link. Redundant functions to avoid downtime or link outages for too long, which is caused by an increase in the amount of traffic and load to serve many requests from ISP users. When there is a malfunction on one ISP, there is still another ISP that is backed up so that there is no downtime for too long and traffic will continue to run [18].

FortiGate requires creating an IPv4 Policy that works to allow traffic from inside to outside. In addition, the IPv4 Policy is used to define which traffic is allowed and which should be denied, both based on the direction of traffic, port address, to IP address source and destination as shown in Figure 13.

After successfully configuring the IPv4 Policy, the tunnel creation process is shown in figure 14. The result of creating a tunnel that has been carried out and is in a state of being connected to the UP status. If all interfaces are configured, then the main link interface and the backup link interface are inserted into the SDWAN Interface Members as shown in figure 15.

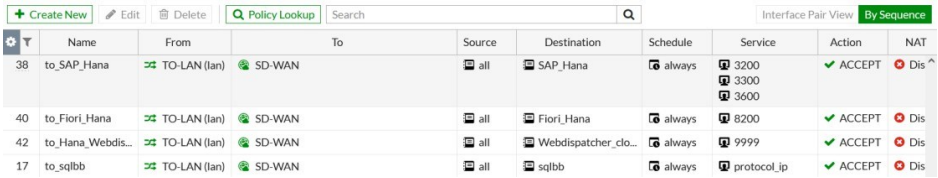

Fig. 13. IPv4 policy configuration

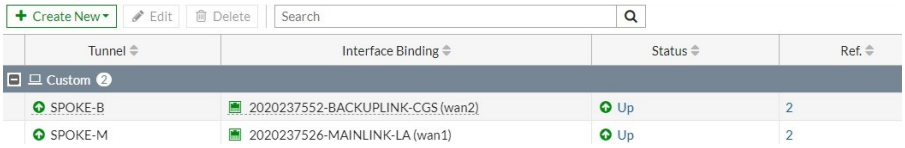

Fig. 14. Results of creating tunnel

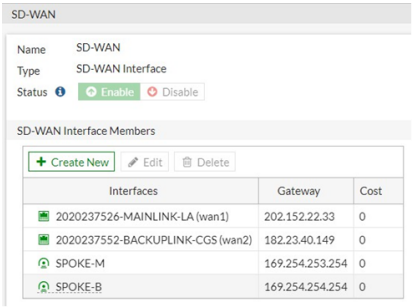

Fig. 15. SDWAN interface members

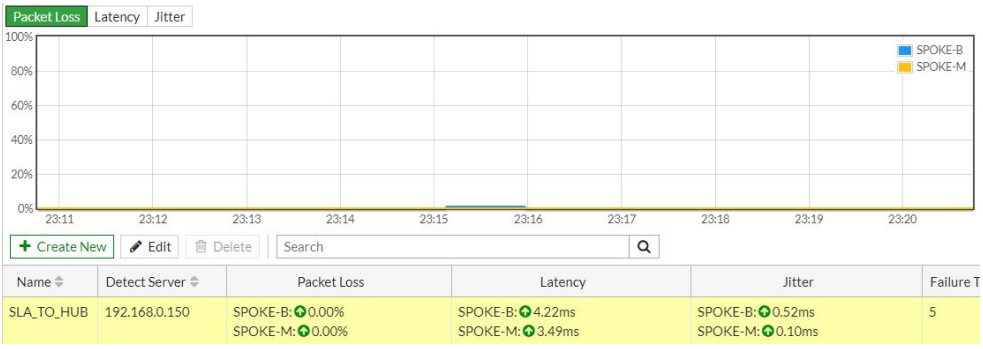

Fig. 16. Performance tunnel packet loss FO-SDWAN

Fig. 17. Performance tunnel latency FO-SDWAN

Fig. 18. Performance tunnel jitter FO-SDWAN

The difference between main link and backup link tunnels lies in the IP Address used. Main link with WAN 1 interface uses IP Address 182.23.25.195 while backup link with WAN 2 interface uses IP Address 202.152.40.226 is a different line and ISP.

Figure 16 is the Performance display of the tunnel display that has been successfully created using FO access. In the tunnel packet loss performance above, it can be known that the link is running well Point to Point without any downtime. From the tunnel performance, the latency performance with fiber optic access is very good, because the average delay time is below 10ms shown in figure 17.

Figure 18 shows the performance of the jitter tunnel which has been known to be in the very good category. High jitter can result in buffering and other interruptions during data transmission.

Conclusion

The conclusions of this research are Latency, Packet loss and Jitter values become much smaller when the access media is replaced using FO, Packet Loss 0.00%, Delay 4.04ms, and Jitter 1.55ms compared to radiolink. The use or implementation of SDWAN technology makes steering customer traffic easier to manage, so that it can be in accordance with the needs requested by customers. In addition, it can be managed centrally using FortiManager tools. Reduce the need for router devices and access links that are delivered, so that it can optimize the use of FortiGate devices located in branches. The security features in FortiGate can also be used for office network security purposes, thereby minimizing the occurrence of abnormal traffic or forbidden access from users. The level of network interference that occurred before using SDWAN had an average of 44%, while after using SDWAN the average interference was only 15%.

Acknowledgements

We would like to thank Universitas Mercu Buana and PT. Datacomm Diangraha for the domestic co-operation research, hopefully this article will be published and become a consumption for scholars.

References

[1] Y. S. Putri and L. Medriavin Silalahi, “Analysis Performance Long Term Evolution Network on Route of Subway Tunnel Mass Rapid Transit (MRT) Bundaran HI - Senayan,” in *2020 International Conference on ICT for Smart Society (ICISS)*, Nov. 2020, pp. 1–6. https://doi.org/10.1109/ICISS50791.2020.9307595

[2] L. M. Silalahi, S. Budiyanto, F. A. Silaban, I. U. V. Simanjuntak, and A. D. Rochendi, “Improvement Of Quality And Signal Coverage LTE In Bali Province Using Drive Test Method,” in *2021 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Jul. 2021, pp. 376–380. https://doi.org/10.1109/ISITIA52817.2021.9502227

[3] R. Liu, S. Li, H. Wang, and Z. Tang, “A QoS Routing Optimization Algorithm Based on Hierarchical Multi-Controller Coordination,” in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2019, pp. 1820–1825.

[4] S. Troia, F. Sapienza, L. Varé, and G. Maier, “On Deep Reinforcement Learning for Traffic Engineering in SD-WAN,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 2198–2212, Jul. 2021, https://doi.org/10.1109/JSAC.2020.3041385

[5] L. M. Silalahi *et al.*, “Application of MPLS Tunnel Service L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Service Analysis,” *Int. J. Electron. Telecommun.*, pp. 115–120, 2023.

[6] 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,” *Int. J. Electron. Telecommun.*, pp. 5–11, 2024.

[7] E. Darmawan, S. Budiyanto, and L. M. Silalahi, “QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method,” in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Nov. 2022, pp. 130–136. https://doi.org/10.1109/COMNETSAT56033.2022.9994572

[8] Ubedilah, S. Budiyanto, and L. M. Silalahi, “Analysis QoS VoIP using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol,” in *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 2022, pp. 47–54. https://doi.org/10.1109/IC2IE56416.2022.9970120

[9] S. Budiyanto and D. Gunawan, “Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol,” 2022.

[10] E. Ramadhan, A. Firdausi, and S. Budiyanto, “Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP),” in *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)*, Nov. 2017, pp. 1–4. https://doi.org/10.1109/BCWSP.2017.8272556

[11] D. A. Nursafitri, U. K. Usman, and M. I. Maulana, “Long Term Evolution (LTE) Network Planning in Jakarta-Cikampek Elevated Toll,” in *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, Jul. 2020, pp. 146–150. https://doi.org/10.1109/IAICT50021.2020.9172013

[12] E. M. Gales and V. Croitoru, “Traffic Engineering and QoS in a Proposed MPLS-VPN,” *2020 14th Int. Symp. Electron. Telecommun. ISETC 2020 - Conf. Proc.*, pp. 3–6, 2020, https://doi.org/10.1109/ISETC50328.2020.9301135

[13] I. U. V. Simanjuntak, Heryanto, A. D. Rochendi, and L. M. Silalahi, “Simulation and Analysis of Link Failover Using Routing Border Gateway Protocol (BGP) Multi- Protocol Label Switching (MPLS) Networks,” in *2023 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, Nov. 2023, pp. 341–346. https://doi.org/10.1109/ICRAMET60171.2023.10366652

[14] R. Mubarak, S. Budiyanto, M. Alaydrus, and A. Adriansyah, “The Utilisation of Information Systems for VSAT Development in Rural Areas,” in *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020, pp. 119–122. https://doi.org/10.1109/BCWSP50066.2020.9249393

[15] S. Budiyanto, L. M. Silalahi, F. A. Silaban, R. Muwardi, and H. Gao, “Delivery of Data Digital High Frequency Radio Wave Using Advanced Encryption Standard Security Mechanism,” *Proc. - 2021 Int. Semin. Intell. Technol. Its Appl. Intell. Syst. New Norm. Era, ISITIA 2021*, pp. 386–390, 2021, https://doi.org/10.1109/ISITIA52817.2021.9502262

[16] L. M. Silalahi, S. Budiyanto, F. A. Silaban, H. B. H. Sitorus, A. D. Rochendi, and M. F. Ismail, “Analysis of the effectiveness of online electronic learning system using data traffic network performance management to succeed merdeka learning--Merdeka campus during the Covid-19 pandemic,” *Int. J. Electron. Telecommun.*, vol. 67, no. 4, pp. 595–601, 2021.

[17] P. Jubaedah and H. Abrianto, “Perancangan Sistem Komunikasi Radio Microwave Antara Onshore Dan Offshore,” *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 25, no. 1, Feb. 2018, https://doi.org/10.37277/stch.v25i1.134

[18] W. Adhiwibowo and A. R. Irawan, “IMPLEMENTASI REDUNDANT LINK UNTUK MENGATASI DOWNTIME DENGAN METODE FAILOVER,” *J. Pengemb. Rekayasa dan Teknol.*, vol. 15, no. 1, p. 48, Jul. 2019, https://doi.org/10.26623/jprt.v15i1.1490