JURNAL SYNTAX TRANSFORMATION

Volume 6, No. 6 June, 2025
p-ISSN 2721-3854 | e-ISSN 2721-2769

Development Of L2TP IPSec for Enhancing Private Network Scalability: Performance, Cost, and Regulatory Framework

Mochammad Iqbal Fahriza, Rendy Munadi, Helni Mutiarsih Jumhur
Telkom University, Bandung, Indonesia
E-mail: mochammadiqbalf@student.telkomuniversity.ac.id,
rendymunadi@telkomuniversity.ac.id, helnimj@telkomuniversity.ac.id

ABSTRACT
This research explores the implementation of L2TP IPSec private networks as a secure and cost-effective solution for data transmission in corporate environments. The primary objective is to address the challenges of ensuring secure data transfer over private networks while meeting technical, economic, and regulatory requirements, particularly within the context of Indonesia. The research employs a comprehensive methodology that includes network topology design and simulation using Cisco Packet Tracer, an economic feasibility analysis incorporating CAPEX, OPEX, NPV, IRR, PI, and PP metrics, and a regulatory review based on Indonesia's Electronic Information and Trans- action Law (UU ITE). By examining the integration of L2TP and IPSec protocols, this study evaluates their effectiveness in safe- guarding sensitive corporate data when transmitted over public networks. The hypotheses focus on enhanced transmission data, cost, and regulatory compliance. The findings provide insights into the technical performance, economic viability, and legal alignment of L2TP IPSec private networks in Indonesia. This research offers a robust framework for enterprises to develop secure, scalable, and compliant private network infrastructures.
Keywords: Private Network, L2TP, IPSec.

INTRODUCTION
In the era of digital transformation, organizations across various sectors face increasing challenges in ensuring infor- mation and communication security. The rise in online trans- actions and interactions demands that companies safeguard the integrity, privacy, and security of data exchanged internally and with external partners (Wylde et al., 2022). The growing frequency and sophistication of cyberattacks have exposed the vulnerabilities of public networks, especially unsecured public Wi-Fi, where data is often transmitted without encryption (Sombatruang et al., 2018).

The implementation of Private Network technology using L2TP IPSec provides a secure solution by encrypting and authenticating data transmitted over public networks such as the Internet. This technology enables secure communication channels between business partners and corporate systems, protecting sensitive information like financial transactions from unauthorized access (Sargiotis, 2024). Moreover, L2TP IPSec supports network scalability and integration

without requiring complex infrastructure, helping companies maintain operational quality and customer trust amid rising digital security threats (Bitbit et al., 2023).

Furthermore, the use of L2TP IPSec aligns with regula- tory requirements in Indonesia related to data privacy and information security, including the Electronic Information and Transaction Law (ITE) and telecommunications regulations (Parulian & Putranto, 2022). Although specific regulations governing private network use remain limited, existing laws provide a legal framework to ensure compliance. Nevertheless, there is a need for clearer regulations addressing private network implementation to sup- port secure and lawful operations.

This study aims to evaluate the implementation of L2TP IPSec in private network design from technical, economic, and regulatory perspectives. Technical evaluation includes topology design and network simulation to ensure optimal and secure operation, while economic feasibility is assessed through financial indicators such as CAPEX, OPEX, NPV, IRR, PI, and PP. This comprehensive analysis intends to sup- port enterprises in developing secure, efficient, and regulation- compliant network infrastructures that meet growing demands in digital security. The implementation and feasibility of L2TP IPSec will assist the government in determining and making regulatory recommendations on private networks.

Previous studies have highlighted the critical role of virtual private networks (VPNs) in enhancing data security across public communication channels. For instance, Oktavia et al., (2023) conducted a comparative analysis between PPTP, L2TP, and OpenVPN protocols, concluding that L2TP combined with IPSec offers superior security features, including encryption and authentication, especially for corporate environments dealing with sensitive data. In another study, Chen et al., (2024) explored the implementation of L2TP IPSec in educational institutions, revealing its effectiveness in securing administrative systems and academic data with minimal infrastructure investment. However, these studies were limited to technical and security performance, without examining economic viability or regulatory compliance.

This study aims to evaluate the implementation of L2TP IPSec in the design of private networks from three essential perspectives: technical, economic, and regulatory. From a technical standpoint, the research focuses on designing and simulating a secure and scalable network topology using Cisco Packet Tracer to assess operational feasibility. Economically, the study analyzes investment viability through financial indicators such as Capital Expenditure (CAPEX), Operational Expenditure (OPEX), Net Present Value (NPV), Internal Rate of Return (IRR), Profitability Index (PI), and Payback Period (PP). Meanwhile, the regulatory aspect involves examining existing Indonesian laws and policies to identify gaps and propose improvements that support secure and lawful deployment of private network technologies. The results of this research are expected to benefit companies and IT practitioners by providing strategic insights into building cost-efficient and secure communication networks. For regulators and government stakeholders, the findings offer practical recommendations to strengthen the legal framework for private network implementation. Additionally, the study contributes to the academic field by offering an integrated analysis that combines network security, economic evaluation, and regulatory compliance, supporting the development of secure, reliable, and future-proof digital infrastructures.The novelty

of this study lies in its integrated analysis of technical, economic, and regulatory aspects of L2TP IPSec implementation in private network design. Unlike prior research which focused solely on protocol performance or security metrics, this study offers a holistic evaluation that includes network simulation using Cisco Packet Tracer, financial feasibility modeling (CAPEX, OPEX, NPV, IRR, PI, PP), and a regulatory gap assessment based on Indonesian law. Furthermore, the study proposes practical regulatory recommendations tailored to current digital security needs in Indonesia.

RESEARCH METHODS

This study adopts a mixed-methods approach, combining quantitative simulation and financial modeling with qualitative regulatory analysis. The research design follows an exploratory-descriptive model, wherein technical, economic, and legal aspects are systematically investigated to offer a holistic understanding of L2TP IPSec implementation. Technical simulation and economic feasibility are analyzed quantitatively, while regulatory implications are explored through qualitative legal analysis.

This research will analyze the feasibility of implement- ing L2TP IPSec for private network design, particularly for companies related to the project. Using the Cisco Packet Tracer network simulator, the research will simulate real-world conditions to assess L2TP IPSec. A techno-economic analysis will determine its viability as a private network solution. Additionally, the study will evaluate relevant regulations and propose improvements to Indonesia's legal framework regard- ing commercial private networks. The goal is to align these regulations with current technological and business needs, pro- viding recommendations to help regulators and the government better support IPSec based private networks in Indonesia.

Table I Research Scenario Parameter

Technical Simulation	Three routers to represent three regional clients with dif- ferent IP versions.
Network Simulator	Cisco Packet Tracer 8.2.2
Router	Cisco 2811
Method	L2TP IPSec and IPv6 over IPv4

The research process initiated by obtaining basic informa- tion through an literature review focused on understanding the parameters and operational mechanisms of the L2TP IPSec protocol in a network simulator environment. This step is critical to accurately design the network architecture. Regarding the regulatory aspects, the study involved collect- ing and analyzing relevant Indonesian laws and regulations regarding private networks. Once the initial data was obtained, a technical analysis was performed by simulating the L2TP IPSec network architecture using a network simulator. The topology consists of three interconnected routers representing

different areas in Jakarta, with each client router connected to client devices. The economic analysis involves combin- ing all expenses incurred during implementation to obtain CapEx and OpEx values. To further evaluate the feasibility of the investment, revenue modeling techniques were applied by calculating financial metrics such as Net Present Value, Internal Rate of Return, Profitability Index, and Payback Period. The regulatory analysis involves examining existing regulations that are directly relevant to the implementation of private networks within companies. Based on this review, refined regulatory recommendations for private networks in Indonesia will be developed. The combined outcomes of the technical, economic, and regulatory analyses are intended to provide well-founded suggestions for regulators or government authorities to establish or formalize regulations governing private networks.

RESULTS AND DISCUSSION

Technical Analysis

In the technical analysis process, the design and implemen- tation of a private network simulation were carried out using L2TP IPSec technology, operated through the Cisco Packet Tracer network simulator. The designed network topology underwent comprehensive research to ensure that it meets the requirements of a private network, while also guaranteeing an optimal level of system availability and reliability. The success of the simulation provides evidence of the effectiveness and robustness of the proposed network solution. Furthermore, the results from this stage serve as an important foundation for proceeding to the economic analysis.

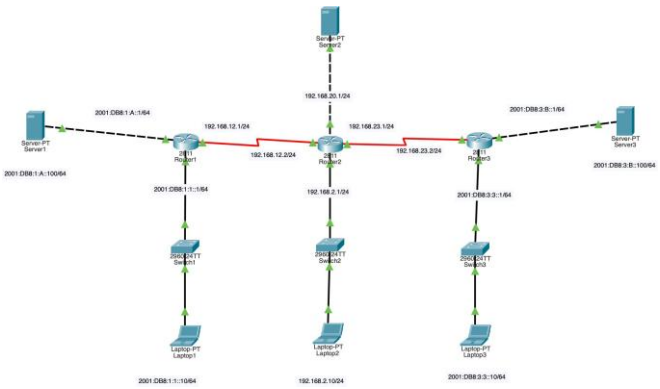

Fig. 1. L2TP IPSec Network Topology

Network Topology

In this topology, there is a central router responsible for managing the entire network of routers, such as those of ser- vice providers, and for implementing label-based mechanisms to direct traffic. Client routers are connected to this central router, each representing a company branch located in different areas of Jakarta. This setup ensures that data traffic from each region is routed efficiently and securely. The configuration of this private network utilizes the tunneling concept of L2TP, combined with additional security provided by IPSec. This allows sensitive data from each branch office to remain secure and isolated from one another.

Simulation Result

The results of the simulation of implementing a private network with IPv4 tunneling over IPv6 on the created network topology show success in connecting devices with different IP address versions. Despite each router using a different IP ver- sion, communication between devices, such as client laptops, remains possible without packet loss, thanks to the successful tunneling configuration that connects the IPv4 network with IPv6. Network security is also implemented using IPSec with IP filters and ACL (Access Control Lists), ensuring that only devices with specific IP addresses can connect to each other and exchange data. This can be tested by performing a ping between client laptops connected through routers with different IP addresses, where only IPs permitted by the ACL can connect. The success of this simulation indicates that tunneling and network security settings can optimize communication within the network by utilizing both types of IP addresses simultaneously while limiting unauthorized data access. Thus, this system can be used to build a more secure, efficient, and integrated private network. In addition, the ACL settings ensure that communication can only be carried out by verified devices. Overall, this simulation successfully demonstrates how network settings can facilitate communication between devices, even under complex conditions and with diverse IP addresses.

Conclusion of Technical Analysis

From a technical analysis using L2TP IPSec and IPv4 over IPv6, this technology demonstrates several important advantages in providing secure and efficient network services. L2TP IPSec enables companies to establish encrypted vir- tual connections between separate locations, ensuring high data security through encryption. With support for IPv4 over IPv6, this solution allows for more flexible and efficient data transmission, as well as better network address management at scale. These advantages can support higher productivity and improve overall network infrastructure performance be- tween offices. However, despite the many technical benefits, it is important to conduct an economic evaluation of this technology. The economic analysis must consider the initial implementation costs, ongoing operational costs, and potential long-term benefits. Therefore, to comprehensively assess the implementation of the L2TP IPSec Private Network, this eco- nomic analysis is essential to determine its financial viability and its impact on the company's long-term business growth strategy.

Techno Economic Analysis

In this techno-economic analysis, economic projections will be made regarding the construction of data centers in com- panies connected using the L2TP IPSec topology over the next five years. The projection is carried out by calculating detailed expenditure costs, including the initial investment required to set up a data center (Pärssinen et al., 2019), such as physical infras- tructure, hardware, and software. In addition, it will estimate the operational and maintenance costs incurred over the five- year period, which include the costs necessary to ensure the continuity and stability of the data center's operations, as well as the calculation of asset costs associated with this project. This study aims to provide a comprehensive overview of the financial viability and potential benefits of implementing a private network project within the company.

Investment and Operational Cost Analysis

In developing the initial cost plan for the project of creating an enterprise data center interconnected through a private network using the L2TP IPSec topology, costs will be divided into two main categories CAPEX and OPEX. CAPEX includes all expenses related to the initial long-term investment. Mean- while, OPEX covers the operational and maintenance costs of the data center that are routinely incurred over the next five years in the short term. This cost separation aims to facilitate more systematic budget planning and improve the overall financial management of the project. Table II and III present the details of the CAPEX and OPEX costs used in the private network implementation.

The CAPEX plan outlines the components essential for im- plementing a private network, including the Cisco 1941 router for reliable data traffic management, the Cisco Catalyst 2960 switch for efficient network traffic control, and the HP DL380 Gen9 server for robust processing power. The Indorack Server IR11542D 42U provides secure hardware storage, while UTP.

Table 2. Capex Cost For Data Center Development

Item	Item Price (IDR)	Quantity	Total (IDR)
Router Cisco 1941	4.570.000	3	13.710.000
Switch Cisco Catalyst 2960	13.900.000	3	41.700.000
Server HP DL380 Gen9	22.450.000	3	67.350.000
Lenovo PC Monitor	2.552.000	3	7.656.000
Indorack Server IR11542D 42U	13.000.000	3	39.000.000
UTP Cable CAT 6	1.500.000	9	13.500.000
Fiber Optic Cable	400.000	6	2.400.000
APC UPS Electric	28.000.000	3	84.000.000
Air Conditioner LG 1 PK	3.399.000	3	10.197.000
CCTV Smart Camera	358.000	6	2.148.000
Security Smart Door Lock	1.200.000	3	3.600.000
Temperature Measuring Device	210.000	3	630.000
Portable Fire Extinguisher	488.000	3	1.464.000
Smoke Detector	600.000	3	1.800.000
Cable Terminal	17.000	6	102.000
Linear Lighting LED Blok	245.000	9	2.205.000
		Grand Total	**291.462.000**

Cat 6 and fiber optic cables ensure stable data connections. A 1 PK LG Air Conditioner maintains optimal cooling, and LED block lighting offers energy-efficient illumination. A UPS ensures continuous power supply, and smart door locks, temperature measuring devices, and

smoke detectors enhance security and environmental monitoring, ensuring the smooth operation and safety of the data center. This comprehensive setup is designed to deliver a reliable, efficient, and secure private network for the company.

Table 3. Opex Cost For Data Center Operations

Item	Monthly Cost (IDR)	Period (Month)	Total (IDR)
IT Employee Salary	23.100.000	12	277.200.000
Security Employee Salary	17.700.000	12	212.400.000
Monitoring and Maintenance of Equipment	4.500.000	12	54.000.000
Infrastructure and Facilities Operations	6.000.000	12	72.000.000
Patch System Upgrade and Customization	4.500.000	12	54.000.000
Remote System Subscrip-tion	747.000	12	8.964.000
Information Security Audit and Regulation	10.000.000	12	120.000.000
		Grand Total	**798.564.000**

The OPEX section details the annual costs for operating the data centers, including salaries for IT and security personnel, energy consumption, maintenance, and system updates. Em- ployee salaries for three IT staff and three security personnel are expected to increase starting from the second year of operation. Energy costs are based on the operation of devices such as a UPS, air conditioners, lighting, and routers, with a usage rate of 90% and an electricity tariff of Rp 1,600 per kWh. Routine maintenance and hardware updates are conducted monthly to ensure the data centers remain stable and efficient. Additionally, annual audits are performed to verify compliance with operational and financial standards (Alzeban, 2019; Mustapha, 2025). This comprehensive cost breakdown supports the economic analysis of the private network's financial viability.

Table 4. Projected Cost Of Operations

Period	Expense (IDR)	Depreciation (IDR)	Total (IDR)
First year	798.564.000	52.463.160	851.027.160
Second year	838.492.200	52.463.160	890.955.360
Third year	880.416.810	52.463.160	932.879.970
Fourth year	924.437.650	52.463.160	976.900.810
Fifth year	970.659.530	52.463.160	1.023.122.690

Projected Cost and Revenue

Table IV shows the operating expenses per year that a company would incur when building data centers for three offices, including the additional annual depreciation costs of the equipment

used. Depreciation is recalculated based on the updated CAPEX multiplied by three offices (total Rp 291.462.000) minus residual value 10% (Rp 29.146.200). De- preciation calculations are carried out using the Straight Line Depreciation (SLD) method. The formula used to calculate annual depreciation is:

$$\text{Depreciation} = \frac{291.462.000 - 29.146.200}{} = 52.463.160$$

This calculation method assumes that the asset will depreci- ate evenly over its useful life. These operational costs include components such as employees, routine maintenance, electric- ity related to energy consumption, equipment maintenance, system upgrades, remote system subscriptions, and regulatory audit requirements. Other operating costs are expected to increase annually according to the inflation rate, with an estimated cost increase of 5% per year. Therefore, the annual cost projections accurately reflect changes in operating costs as well as depreciation allocation (Anton, 2013).

Table 5. PROJECTED REVENUE BASED ON DATA TRANSACTIONS

Period	Total Transaction	Annual Income (IDR)
First year	54.000	853.200.000
Second year	59.400	938.520.000
Third year	65.340	1.032.480.000
Fourth year	71.874	1.136.016.000
Fifth year	79.061	1.249.812.000
Total	**329.675**	**5.309.028.000**

Table V estimates the potential revenue from data transmis- sion over private networks using a tiered pricing model based on data volume. Transactions up to 500 MB are charged Rp 13,000, those between 501 MB and 1,000 MB are charged Rp 16,000, and those over 1 GB are charged Rp 19,000. In the first year, the projected monthly revenue is Rp 80,100,000, with an annual total of Rp 853,200,000. With a 10% annual growth in transaction volume, the total projected revenue over five years is Rp 5,309,028,000. This projection highlights the monetization potential and strategic value of implementing a private network for secure data transmission.

Table 6. Projection Tax For Data Center Development

Period	EBITDA (IDR)	EBIT (IDR)	Tax 10% (IDR)	Net Income (IDR)
First-year	54.636.000	2.172.840	217.284	1.955.556

Second year	100.027.800	47.564.640	4.756.464	42.808.176
Third year	152.063.190	99.600.030	9.960.003	89.640.027
Fourth year	211.578.350	159.115.190	15.911.519	143.203.671
Fifth year	279.152.470	226.689.310	22.668.931	204.020.379

Table 6 presents the annual income before tax deductions, offering insights into the company's gross income and financial performance. EBITDA reflects operating profit before depre- ciation and tax, showing growth from Rp 54,636,000 in the first year to Rp 279,152,470 in the fifth year. EBIT, after ac- counting for depreciation, increases from Rp 2,172.840 to Rp 226.689.310, demonstrating improved operational profitability. Tax, calculated at 10% of EBIT, rises from Rp 217.284 in the first year to Rp 22.668.931 in the fifth year. Net income after tax grows from Rp 1.955.556 to Rp 204.020.379, indicating improved financial health and business sustainability. This projection provides a clear overview of the company's financial trajectory and the impact of private network implementation on its profitability.

Feasibility Analysis

The feasibility analysis was conducted to provide an overview of the potential success and risks of the research, allowing for a conclusion on whether the research can be continued, modified, or discontinued. NPV is an economic valuation method that calculates the difference between the present value of discounted future cash flows and the initial investment cost, assessing the added value generated by a project (Bora, 2015; Shrieves & Wachowicz Jr, 2001). IRR is the project's rate of return that indicates the feasibility of an investment if it exceeds the cost of capital. PI is a financial indicator that measures the feasibility of a project by comparing the present value of future cash flows to the initial investment cost. PP is an investment appraisal method that measures the time required to recover the initial investment cost from project cash flows.

- Net Present Value (NPV):
  - CF_0 is the initial investment (usually a negative value),
  - CF_t is the net cash flow at year t,
  - i is the discount rate,
  - n is the length of the evaluation period (in years). Based on the data, in Table 4.6 the initial investment is Rp 291.462.000, and the net cash flows over five years are as follows:

The total present value of the net cash flows over five years is:

$$1.776.869 + 35.387.107 + 67.396.116 = 104.560.092$$
$$+97.845.838 + 126.617.697 = 328.023.627$$

Therefore, the project's NPV is:

$$NPV = -291.462.000 + 328.023.627 = 36.561.627$$

NPV is an economic evaluation method that calculates the difference between the present value of expected cash inflows and outflows discounted at a required rate of return. In this project, NPV is computed by discounting the net cash flows over five years at a 10% discount rate, reflecting the investment's cost of capital and risk. The resulting NPV of approximately IDR 36.561.627 is positive, indicating that the project is expected to generate additional value and financial benefits beyond the initial investment. A positive NPV implies that the discounted revenues exceed the discounted costs, making this private network implementation economically viable.

Conclusion of Techno Economic Analysis

Based on the results of the technological and economic analysis, this study demonstrates that the proposed project is both feasible and financially advantageous. This conclusion is drawn from an in-depth evaluation using several key financial indicators for ROI, including NPV, IRR, PI, and PP. A positive NPV of IDR 36,561,627 suggests that, after accounting for the discount rate, the project will provide a net return on investment, while an IRR of 14.30% exceeds the cost of capital (10%), confirming that the project will generate returns higher than the initial capital costs. A PI of 1.13 further indicates that the expected benefits surpass the required investment costs, and the relatively short payback period of 3.03 years ensures the quick recovery of the initial capital, reducing financial risk. Additionally, the projected annual revenue growth, anticipated to reach IDR 5.31 billion by the fifth year, along with realistic operational cost and depreciation calculations, further reflects the long-term profitability of the project. This consistent growth in revenue highlights the scalability and sustainability of the investment. The strategic value of the private network extends beyond financial returns, as it will significantly en- hance data security and protect the company's infrastructure (Dutta & McCrohan, 2002). Therefore, investing in the development of this private network is not only financially viable but also strategically critical to enhancing the company's data protection capabilities and ensuring effective financial management over the long term.

Regulation Analysis

In Indonesia, although private networks have been widely implemented by companies, the regulations governing them remain limited. These private networks are legally classified as special telecommunications, as stated in Article 9 of Law No. 36 of 1999 concerning Telecommunications (Fischer, 2010). While regulated as special telecommunications, there are no regulations that specifically address private networks. Government Regulation No. 52/2000 regulates the implementation of telecommunica- tions, including private networks, by providing guidelines on the operational permits that must be adhered to. Additionally, Government Regulation No. 71/2019 provides guidance on the implementation of electronic systems and transactions, focusing on data protection and network security, which are crucial for managing private networks. However, despite this legal framework, supervision and compliance with

security and service quality standards remain a challenge, as existing regulations primarily focus on public service providers and do not comprehensively address commercial private network operators. Therefore, a more comprehensive policy design is needed to ensure that private network regulations support sustainable technological and economic development while maintaining fairness and data security.

Regulatory Issue Identification

The implementation of private networks in Indonesia is still not fully regulated by existing regulations, especially concern- ing commercial use. Currently, private networks are classified as special telecommunications, which means private network operators are not subject to non-tax state revenue (PNBP) fees or universal service obligation (USO) requirements, as is the case for public telecommunications service providers (Aldiano & Simatupang, 2022). This exemption from financial obligations is outlined in Minister of Communication and Information Technology Regulation No. 5 of 2021 on the Implementation of Telecommunications, which governs the obligations of Universal Telecommunica- tions Services. However, this policy creates an imbalance in the telecommunications sector, where public service providers must bear greater costs to support the development of na- tional telecommunications infrastructure and provide universal services, while commercial private network operators are not burdened with the same costs. When these private networks are used for commercial purposes and serve external parties, they should also be subject to obligations equivalent to those of public service providers. However, to date, the status of private networks as special telecommunications continues to exempt them from these costs.

Existing regulations also fail to adequately address the development and dynamics of private network usage, particularly when used for commercial purposes. Therefore, policymakers need to review and update the existing regulations to ensure they align with current and future practices. Such regulatory adjustments should include a clearer definition of private network usage, distinguishing between internal and commercial use, to prevent unfair fi- nancial advantages between private network operators and public telecommunications service providers. Additionally, more effective monitoring systems must be implemented to ensure that private networks are used in accordance with their intended purposes and to prevent misuse that could harm consumers and the government. This regulatory update should also include the development of a more intensive monitoring and law enforcement system to maintain equality and fairness in the telecommunications sector. These measures are essential to ensure that Indonesia's telecommunications infrastructure develops fairly and sustainably.

CONCLUSION

This study demonstrates that the implementation of private networks using L2TP IPSec technology in Jakarta can be carried out with excellent results, both from a technical, economic, and regulatory perspective. Simulations conducted using Cisco Packet Tracer show that the infrastructure required to build and operate private networks in Jakarta can be imple- mented effectively and efficiently. Therefore, this technology has the potential to provide a secure and

reliable private network, even in the dense and complex urban environment of Jakarta. From an economic standpoint, the analysis results indicate that this project has high profit potential. The use of methods such as Net Present Value (NPV), Internal Rate of Return (IRR), Profitability Index (PI), and Payback Period (PP) yielded positive results, suggesting that investing in the development of a private network in Jakarta can provide significant financial benefits in the long term. Hence, from an economic perspective, this project is highly feasible, with promising return projections and controlled risks. With proper planning, this investment will generate substantial added value for the company. However, in the regulatory review, this study identified several weaknesses in the existing regulations, particularly regarding the classification of private networks as specialized telecommunications, which exempts private network operators from the obligation to pay Non-Tax State Revenue (PNBP) fees and Universal Service Obligation (USO) contributions. While these regulations are suitable for internal private network use, regulatory updates are needed to accom- modate the commercial use of private networks. Therefore, it is recommended that the regulations be updated to require commercial private network operators to fulfill the same obli- gations as public telecommunications service providers. This regulatory change will foster fairer competition in the telecom- munications industry and support the strengthening of the national telecommunications ecosystem. With these regulatory updates, the sustainability of the telecommunications industry can be better maintained. Additionally, this study recommends the implementation of environmentally friendly green network technology, utilizing renewable energy to reduce the nega- tive environmental impact of network infrastructure. Green network technology will help companies meet their energy needs more efficiently and sustainably. Moreover, the use of artificial intelligence (AI) in the operational management of private networks can provide significant benefits in improving efficiency, reducing operational costs, and enhancing service quality. The application of AI technology will accelerate data processing, reduce downtime, and overall improve the performance of private networks in the long term.

REFERENCES

Aldiano, D., & Simatupang, D. P. N. (2022). Obligation to Pay Telecommunications Operation Rights Fees and Contribution of Universal Service Obligations for The Palapa Ring Project by The Palapa Ring Project Implementing Business Entity. *Legal Brief*, *11*(5), 2914–2931.

Alzeban, A. (2019). An examination of the impact of compliance with internal audit standards on financial reporting quality: Evidence from Saudi Arabia. *Journal of Financial Reporting and Accounting*, *17*(3), 498–518.

Anton, H. R. (2013). Depreciation, cost allocation and investment decisions. In *Depreciation and Capital Maintenance (RLE Accounting)* (pp. 31–48). Routledge.

Bitbit, E. D., Gampoy, M. A. B., Ricafort, T. S., Tinio, R. D., Pula, R. L., Leona, R. F., & Olipas, C. N. P. (2023). Crafting a Network Plan for a Microfinancing Establishment and Its Branch Network through Virtual Private Network (VPN) Implementation. *European Journal of Theoretical and Applied Sciences*, *1*(3), 441–448.

Bora, B. (2015). Comparison between net present value and internal rate of return. *International*

Journal of Research in Finance and Marketing, *5*(12), 61–71.

Chen, Y., Li, Q., Tian, L., & Jiang, Y. (2024). Navigating the VPN Landscape: A Comparative Study of L2TP, IPSec, and MPLS VPN Technologies. *2024 4th International Conference on Electronic Information Engineering and Computer Science (EIECS)*, 614–617.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67–87.

Fischer, J. C. (2010). *Communications network traffic data: technical and legal aspects*.

Mustapha, I. K. (2025). *Audit and Compliance Plan-2025 Financial Year*.

Oktavia, S. T., Priambodo, D. F., Trianto, N., & Purwoko, R. (2023). Comparative Quality of Service Analysis of VPN Protocols on IPv6. *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, *12*(3), 461–471.

Pärssinen, M., Wahlroos, M., Manner, J., & Syri, S. (2019). Waste heat from data centers: An investment analysis. *Sustainable Cities and Society*, *44*, 428–444.

Parulian, H., & Putranto, R. D. (2022). Pidana Ujaran Kebencian Melalui Media Sosial Ditinjau dalam Perspektif Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). *Jurnal Pendidikan Dan Konseling (JPDK)*, *4*(4), 4909–4919.

Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data governance: a guide* (pp. 217–245). Springer.

Shrieves, R. E., & Wachowicz Jr, J. M. (2001). Free cash flow (FCF), economic value added (EVA™), and net present value (NPV):. a reconciliation of variations of discounted-cash-flow (DCF) valuation. *The Engineering Economist*, *46*(1), 33–52.

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 1–11.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, *3*(2), 127.