CHAPTER I
INTRODUCTION

1.1 Background

In the rapidly evolving digital era, modern companies rely heavily on computer networks to support their business operations. Many companies with branch offices in various locations rely on a Wide Area Network (WAN) to stay connected efficiently. However, the biggest challenge in using WAN is ensuring that network performance remains optimal, especially in the face of various conditions. One solution that is widely used by companies to overcome this challenge is to implement Virtual Private Network (VPN) technology. VPN allows companies to connect private networks through the public internet or WAN in a secure way through data encryption[1]. Using a VPN, companies can ensure that the data sent and received remains protected, even through unsecured channels. In addition, a VPN allows employees or business partners to access the company's internal network remotely, increasing flexibility and productivity.

VPN is a communication technology that makes it possible to connect to a public network and use it to join a local network[1]. However, the use of VPN on WAN networks often faces challenges related to Quality of Service (QoS). QoS is an important element in network management to prioritize bandwidth usage, reduce latency, and improve connection reliability. Without good QoS management, critical applications and network usage can experience disruptions that negatively impact operations[2]. The challenge of maintaining network quality over WAN demands a more efficient and secure solution.

Therefore, this research focuses on the development and application of optimized VPN technology with QoS management to improve the performance of enterprise networks using WAN. By developing more effective methods of implementing VPN and QoS, enterprises are expected to achieve higher levels of network reliability and efficiency, which in turn will improve productivity and business sustainability. In this study, the QoS measurement will be based on practical usage scenarios within the company, such as the use of an attendance website. This application serves as an example of real-world usage, where the website relies on VPN connectivity for data transmission and consistent access across various locations. As a result, the QoS methods implemented in this research will be tailored to meet

the specific requirements of the attendance website, focusing on reducing latency, ensuring reliable bandwidth allocation, and minimizing packet loss to support optimal user experience and operational efficiency. This research aims to formulate an appropriate strategy for developing an enterprise private network by utilizing VPN and QoS technologies in a WAN environment. The proposed solution will be tested and evaluated to see to what extent improvements in network service quality can be achieved, as well as how network security and efficiency can be further enhanced to support the increasingly complex operational needs of the enterprise.

In the growing digital era, computer networks have become the backbone of modern enterprise operations[3]. Reliance on WAN that allow branch offices in various locations to remain connected creates its challenges for companies, especially in maintaining optimal network performance. This condition is especially relevant for the Indonesian economy, which is increasingly driven by digitalization. Companies that are unable to maintain network quality risk losing productivity and competitiveness in an ever-evolving global market[4].

From an economic perspective, network optimization through the implementation of technologies such as VPN is crucial in supporting the efficiency and effectiveness of company operations. VPN allows companies to connect private networks through public internet lines securely while enabling remote access for employees and business partners[5]. With better network performance, companies can maximize bandwidth usage, reduce latency, and ensure that the network used can run smoothly. This will increase the productivity, operational efficiency, and profitability of the company. In addition, proper implementation of QoS management also has a significant economic impact. In the application of technology used to determine the feasibility of implementation in private network research, it is necessary to analyze the economic feasibility that will be calculated using the Capital Expenditure (CAPEX), Operational Expenditure (OPEX), Net Present Value (NPV), Internal Rate of Return (IRR), Profitability Index (PI), and Payback Period (PP) methods[6].

In terms of regulations, especially private networks, there are no regulations governing them because private networks are only used in internal cases. The application of VPN and QoS technology must also comply with various regulations that apply in Indonesia. The Indonesian government through Law No. 11/2008 on Electronic Information and Transactions (ITE) regulates the safe and responsible use of information technology. In this context, companies must ensure that VPN use and QoS management are in line with personal data protection regulations as well as increasingly stringent cybersecurity policies. On the other hand, regula-

tions relating to network management also require companies to ensure the security of the data they manage, especially in highly regulated industries such as finance and healthcare. By following the security standards set by the government, such as Government Regulation No. 82/2012 on the Implementation of Electronic Systems and Transactions, companies can not only ensure compliance with regulations but also protect themselves from potential legal sanctions that may arise from data protection violations. Therefore, this research focuses on developing VPN technology and QoS management that not only improves network performance and operational efficiency but also complies with applicable regulations, thus providing a comprehensive solution for enterprise in Indonesia.

1.2 Problem Identification

Modern enterprise that rely on WAN connections face several key challenges in maintaining optimal network performance and efficiency:

1. Modern enterprises relying on WAN face challenges in maintaining optimal network performance.
2. VPN usage over WAN often encounters difficulties in ensuring adequate Quality of Service (QoS).
3. Without effective QoS management, critical applications that support enterprise operations may experience disruptions.
4. Disruptions in these critical applications can hinder the operational efficiency of the enterprise.
5. A more efficient solution is needed to optimize VPN and QoS usage, enabling companies to achieve better network reliability and higher operational efficiency.

1.3 Objective and Contributions

This thesis aims to address these challenges through specific objectives and contributions that will improve network performance and support enterprise operations:

1. To implement an efficient QoS management solution on a WAN using VPN to improve network performance for operational tasks.

2. To design a system that optimizes VPN and QoS usage, allowing private networks to operate with higher efficiency in the workplace.

3. To enhance network performance, ensure adequate QoS, and support optimal operational continuity.

4. To offer recommendations for enterprises to adopt VPN-QoS strategies to support business efficiency and sustainability.

1.4 Scope of Work

To keep the experiment from being too long, this thesis limits the works as follows:

1. This research will analyze the implementation of QoS management on WAN that uses a VPN.

2. The application and implementation of this research will be focused on an enterprise network environment in which private networks are needed in daily activities.

3. The case study will focus on optimizing the use of VPN and QoS to improve network performance, especially on a WAN network connecting several branch offices.

4. The topology represents a corporate WAN network scenario that uses VPN technology with QoS optimization to connect various branch offices.

5. Technical analysis will be conducted on the performance of the VPN network integrated with QoS management, including network performance testing, as well as operational efficiency in the WAN network.

1.5 Research Methodology

To achieve the objectives of this research, the methodology used includes several steps as shown in Fig 1.1:

1. Literature Study: Conducting a literature review on VPN, WAN, and QoS management from relevant journals, articles, and sources.

2. Technical Analysis: Tested the implementation of VPN and QoS in the company's WAN network to improve network performance.

3. Economic Analysis: Calculating CAPEX and OPEX costs and analyzing financial feasibility using NPV, IRR, PI, and PP.

4. Regulatory Analysis: Reviewing the compliance of VPN-QoS implementation with Indonesian regulations.

5. Results and Conclusion: Summarize the findings and recommend implementing a VPN-QoS solution for network optimization.

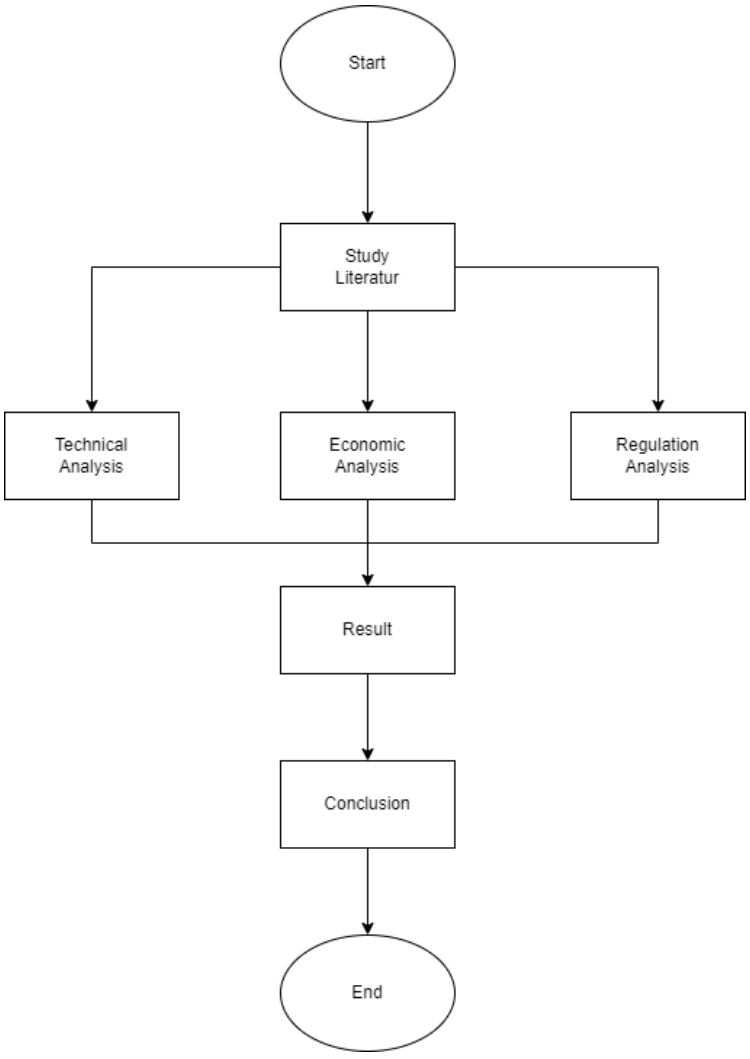

Fig 1.1 Diagram of Research Methodology for VPN-QoS Implementation

1.6 Hypothesis

Based on the literature review and previous research findings, the hypotheses proposed in this study are as follows:

1. Efficient QoS management implementation in WAN networks using VPN can significantly improve the network performance of enterprises, particularly in ensuring stable connectivity, reducing transmission errors, and maintaining consistent service delivery across geographically distributed offices.

2. The combination of VPN and QoS technologies will be able to reduce latency, enhance bandwidth allocation reliability, and minimize packet loss, thereby supporting optimal enterprise operations that depend on time-sensitive and bandwidth-reliant applications such as centralized web services or internal cloud platforms.

3. Evaluating QoS performance by directly observing real-time usage of the web application in a simulated VPN-WAN environment enables a practical assessment of network behavior under realistic conditions, offering actionable insights without the dependency on complex queueing algorithms or specialized traffic shaping methods.

The basis for these hypothesis refers to the study, which demonstrated that the application of QoS in VPN networks significantly improves network efficiency in enterprise environments[7].

1.7 Research Plan and Action Point

To ensure the successful and timely completion of this thesis, a structured research plan has been developed. This plan divides the entire research process into distinct phases, each with a specific objective and time allocation. By following this well-defined roadmap, the researcher aims to maintain consistent progress while systematically addressing all aspects of the study.This research is structured through sequential stages, including problem identification, literature review, technical analysis based on QoS, financial feasibility evaluation (CAPEX and OPEX), and the formulation of recommendation[8].

Table 1.1 outlines the sequence of research activities and their respective durations, offering a clear overview of the planned workflow. It begins with the identification of the core problem surrounding WAN performance and VPN usage, followed by a literature study to understand current technological challenges. The next steps include developing a research methodology, conducting a detailed technical analysis using QoS metrics, and evaluating financial viability through CAPEX and OPEX assessments. The final phase culminates in drawing conclusions and providing actionable recommendations.

Table 1.1 Table 1.1 Research Phases and Action Points

Phase	Duration	Action Points
Problem Identification	2 weeks	Identify issues related to WAN performance and VPN usage.
Research Study	2 weeks	Conduct a study on existing technologies (VPN and QoS) and analyze their challenges in optimizing WAN performance for businesses.
Methodology Development	2 weeks	Develop a research framework for optimizing VPN and QoS for WAN environments, focusing on application performance improvements.
Technical Analysis	4 weeks	Perform an in-depth technical analysis of current VPN and QoS implementations in WAN, including performance metrics like bandwidth, latency, and reliability.
Economic Analysis	2 weeks	Conduct economic analysis (CAPEX/OPEX) to evaluate the financial feasibility of deploying VPN and QoS solutions, including NPV, IRR, PI, and PP methods.
Regulatory Analysis	2 weeks	Analyze regulations related to VPN usage and network management, including compliance with Indonesian laws like the ITE Law and PSTE regulations for network security.
Result and Conclusions	2 weeks	The result findings of the research provide recommendations on the best approach for optimizing VPN and QoS in WAN environments to improve business network performance.