JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

Performance Analysis of Mesh Network Implementation Using Mikrotik RouterBoard 941 in Radio Link-Based Secure Networks

Riska Andian Turnip[1], Kitu Gea[2], Yoga Pramadio Purba[3], Rasme Kita Kaban[4], Sumarlin[5], Ita Margaretta Br Tarigan[6]
[1)2)3)4)5)6)] Institut Teknologi dan Bisnis Indonesia, Kab. Deli Serdang, Sumatera Utara, Indonesia
Email: [1]riskaandian9@gmail.com, [2]demikiangea2018@gmail.com, [3]yogapramdiopurba@email.com
[4]rasmekitakaban1432@gmail.com, [5]netcommmandiri@gmail.com, [6]itamargaretta1997@gmail.com

Submitted :10 February 2026 | **Accepted** : 28 February 2026 | **Published** : 31 March 2026

Abstract: The increasingly rapid development of computer network technology demands a network system that is reliable, flexible, and able to adapt to dynamic environmental conditions. One of the network technologies that is currently developing is mesh networking. Mesh networking is a network topology where each node can be connected to each other directly or indirectly through other nodes. This research aims to analyze the application of the mesh networking method using the Mikrotik RouterBoard 941 device. The research method used is experimental by configuring, implementing, and testing mesh networking on the Mikrotik RouterBoard 941. The results of the research show that mesh networking can be applied to the Mikrotik RouterBoard 941 by utilizing available features, such as OLSR (Optimized Link State Routing) and WDS (Wireless Distribution System). Mesh networking is able to increase redundancy and network availability, and can adapt to changes in network topology. However, mesh networking also has several disadvantages, such as configuration complexity, routing overhead, and the possibility of bottlenecks at certain nodes.

Keywords: Mesh Networking; Mikrotik RouterBoard 941; OLSR; Wireless Distribution System (WDS); Network Performance Analysis

INTRODUCTION

In the era of globalization and rapid digital transformation, the advancement of information and communication technology (ICT) has significantly influenced various aspects of human life, including education, business, and communication systems. The increasing dependency on internet-based services has led to the necessity of reliable, efficient, and secure computer network infrastructures. Modern institutions, especially universities, require stable and secure network systems to support academic activities, research, and administrative operations.

Along with technological growth, the complexity of cyber threats has also increased. Initially, network usage was limited to simple activities such as information browsing and basic communication. However, today's networks support complex operations involving sensitive data exchange, cloud computing, and real-time collaboration. This evolution demands more advanced network security mechanisms to prevent unauthorized access, data breaches, and other cyberattacks. Therefore, network security has become a critical component in maintaining system integrity, confidentiality, and availability.

Historically, the concept of network security has evolved since the development of early computer networks such as ARPANET in the 1970s. Over time, various security protocols and mechanisms have been developed, including Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA/WPA2). Research shows that WPA2-PSK provides better security compared to earlier methods due to its stronger encryption techniques. (Efendi, 2021) stated that WPA offers a higher level of security than WEP, especially in terms of resistance to password cracking, making it more suitable for modern wireless networks.

In addition, vulnerabilities in wireless networks are still a major concern. (Adiguna, 2022) explained that during network scanning and discovery processes, vulnerabilities can be identified through open ports, which may

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

be exploited by attackers using tools such as Metasploit Framework on Kali Linux. This indicates that even networks using modern security protocols still require additional protection mechanisms and continuous monitoring.

Computer network security plays an important role in anticipating risks that may occur in network systems, which can disrupt ongoing activities. There are three main aspects of network security: threats, vulnerabilities, and risks. Computer security is defined as a preventive measure against attacks from unauthorized users or malicious actors attempting to access network systems. This highlights the importance of implementing robust security systems to protect sensitive data and maintain network reliability.

In the context of wireless networking, one of the emerging technologies is mesh networking. Mesh networks offer advantages such as self-healing capability, scalability, and improved coverage, making them suitable for complex environments like multi-storey campus buildings. By utilizing mesh topology, each node can communicate with other nodes, ensuring continuous connectivity even if one node fails. This characteristic is highly beneficial for maintaining network stability and performance in large-scale implementations.

At ITB Indonesia Campus, the implementation of wireless networks has become essential to support academic and administrative activities. The campus infrastructure consists of multiple buildings with varying network demands, making traditional network topologies less effective. To address this issue, the use of radio link-based communication combined with mesh networking technology presents a promising solution. Radio link systems enable long-distance wireless communication between network nodes, while mesh networking enhances connectivity and redundancy.

The use of MikroTik RouterBoard 941 as a networking device provides a cost-effective and flexible solution for implementing mesh networks. MikroTik devices are widely used due to their robust features, including routing, firewall, bandwidth management, and wireless configuration. By integrating MikroTik RouterBoard 941 into a mesh network architecture, it is possible to build a secure and efficient network system that supports radio link communication.

However, despite the potential advantages, the performance of mesh networking implementation using MikroTik RouterBoard 941 in terms of network security, stability, throughput, latency, and packet loss still needs to be analyzed comprehensively. Performance evaluation is essential to ensure that the implemented system meets the required standards for secure and reliable communication within the campus environment.

Based on the above considerations, this study focuses on analyzing the performance of mesh networking implementation using MikroTik RouterBoard 941 for radio link-based network security at ITB Indonesia Campus. This research is expected to provide insights into the effectiveness of mesh networking in enhancing network security and performance, as well as to offer recommendations for optimizing wireless network infrastructure in educational institutions.

LITERATURE REVIEW

1. Implementation

In general, the term "implementation" in the Great Dictionary of the Indonesian Language refers to the implementation or application. The term is often associated with activities carried out to achieve a specific goal. Implementation is the action or implementation of a plan that has been carefully prepared, carefully and in detail (Wirano, 2020). Implementation is carried out if there is a good and mature plan, or a plan that has been prepared long in advance, so that there is certainty and clarity about the plan.

2. Network Security System

In general, a network security system is a set of technologies, procedures, and measures designed to protect a computer network and the data stored on it from unauthorized access, alteration, or deletion (Jackson, 2020). The system aims to prevent or limit unauthorized access to networks, identify and prevent malicious activities, and ensure that data stored on the network remains secure and inaccessible to unauthorized parties (Brown, 2021).

Network security systems include various measures, such as access control, encryption, firewalls, intrusion detection, and disaster recovery (Synapsis, 2021). The primary purpose of a network security system is to protect sensitive data, including financial information, personal data, and business information that has the potential to become a target for theft or misuse if not adequately protected (Sutiono, 2020).

3. TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol, which refers to a series of communication protocols used to connect network devices on the Internet (Tanenbaum, 2020). This protocol is also applied in private computer networks, both intranets and extranets. TCP and IP were originally developed by the United States Department of Defense (DOD) with the goal of connecting a variety of different networks from various

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

vendors into a single network unit known as the Internet. The success of this protocol relies heavily on the provision of services such as file transfer, e-mail, and remote access across various client systems and servers (Stevens, 2020). Multiple computers in a small department can use TCP/IP in conjunction with other protocols within a single Local Area Network (LAN). The IP component serves to provide routing from departments to the corporate network, then to the regional network, and finally to the global Internet (Kozierok, 2021).

4. OBITUARY

OSI (Open Systems Interconnection) is a model that describes how network protocols communicate with each other and share data between devices (Michael, 2021). In general, the OSI model divides the various functions of the network into seven layers (Cisco, 2020). The seven layers are: the physical layer, the link data layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer. The institution responsible for the publication of the seven-layer OSI model is the International Organization for Standardization (ISO) (Sofana, 2021).

5. Internet

The Internet began in 1969 when the United States Department of Defense decided to conduct research using a method of communication between several computers, which eventually formed an organic network (G., 2021). The internet has now become an urgent need throughout the country, considering that humans have felt comfort and convenience in various aspects of life. The rapid development of the internet has resulted in significant changes in people's perspectives and lifestyles. However, there is an imbalance between the demand for internet services and the availability of facilities, known as the phenomenon of "clogging."(Anhar, 2020).

6. IP Address

An IP address is a series of numbers that serves as the identity of a device connected to the Internet or other network infrastructure (Danniel, 2021). What is the function of the IP address? Its function can be likened to a home number on an address, which aims to ensure that data is sent to the right device. The range of a series of IP address numbers starts from 0. 0. 0. 0 to 255. 255. 255. 255 (Cisco, 2020).

7. Definition of Computer

In general, a computer can be defined as an electronic device that functions to receive data input, then process the data, and produce information output in various forms, including text, images, sound, and video (Harmayani et al., 2021). Computers are also dubbed as electronic counting machines that can receive digital input information, process it according to the programs stored in their memory, and produce information output quickly (Hamacher, 2020). On the other hand, computer networks refer to the relationship between two or more computers that are connected to each other through a transmission medium, either wired or wireless (wireless).

8. Bandwidth

Bandwidth, or bits per second (bps), is a measure that indicates the level of data transfer consumption (Athailah, 2020). The measurement is done in bits per second between the server and the client over a period of time. In addition, bandwidth can also be interpreted as the area or width of the frequency range used by the signal in a transmission medium (Supendar & Handrianto, 2017). Therefore, bandwidth can be said to be the maximum capacity of a communication path used to transfer data in a given time span.

9. Mikrotik

Mikrotik is an operating system created by Mikrotik, a company founded in 1996 in Latvia. This company is engaged in internet services or is an Internet Service Provider. Mikrotik can be said to be an operating system and software used to turn a computer into a network router. Mikrotik includes various features made for IP networks and wireless networks (Hart, 2020). Mikrotik initially focused on Internet Service Provider (ISP) services that use wireless technology. In the course of history, the founders (John, 2021) just want to develop Routing software, but as the hardware needs develop, it is increasing. Therefore, they then develop various hardware that integrates with the software they develop

10. Winbox

Winbox is a Mikrotik-specific program for Microsoft Windows that makes it possible for a router to be configured and monitored remotely. The program can also be used in Linux with Wine Emulator, but this Statement is not officially endorsed by MikroTik (Hart, 2020). By default, the Winbox app connects to the Router OS device via Transmission Control Protocol (TCP) port 8291. MikroTik configurations using Winbox are more often chosen because of their ease of use, where users do not need to memorize the commands that must be used in the console interface (Madcoms, 2020).

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

11. WPA2-PSK

WPA2-PSK stands for Wifi Protected Access Pre-Shared Key, which is an encryption system used to verify users within a wireless local area network (Scott, 2020). With this system, users can stay connected to the internet through the WiFi network without being seen by other WiFi users. WPA2-PSK operates using a router equipped with a passphrase (Harefa, 2021). Between 8 and 63 characters are required for passphrases to ensure the encryption of the data contained in the network. There are two method options that can be used to obtain a unique encryption key for each WiFi network user. In addition, according to (Prayoga, 2021)The WPA2-PSK stands for Wireless Fidelity Protected Access 2- Pre-Shared Key, a type of security encryption that allows wifi users to secure their network without having to use server authentication.

12. Radio Link

Radio Link is a communication device that uses radio waves to transmit data between two or more points that are spaced apart. This is also in line with the opinion of some experts, according to (Goldsmith, 2020) Radio Link is a communication technology that utilizes radio waves to provide wireless connectivity between devices that are far apart, often used in modern telecommunications networks (Kamila, 2024). Radio Link is a communication line that uses radio frequencies to transmit data wirelessly between two or more points, especially in Internet of Things (IoT) and 5G networks (Molisch, 2021). Radio Link refers to systems that allow the transmission of data over the air using radio waves, essential in the development of the next generation of wireless communication networks.

2.2 Running System Analysis

System analysis is the activity of describing parts of system components with the aim of identifying, evaluating problems, and needs so that improvements can be proposed. Running systems are used to analyze the flow of the running system path, evaluate, and build a new security system, so that the new system can be implemented effectively and efficiently. The ongoing network security procedure is in the form of a simple security system that can be entered and accessed by any user. The system that runs is as follows:

a. The user enters the available network menu.
b. The user logged in to the web login and selected the network.
c. The user performs security verification.
d. The system verifies the security that the user uses.
e. Users log in and can use network access.

With procedures that are implemented simply, system data will affect the security of data network traffic. So that the target of the research focuses on security, data transmission that uses wireless networks can be used by other parties, to be used for things that should not be used.

2. 3 System Evaluation

Based on the analysts on network and security systems. The author states that the current system has shortcomings in network security, access that only uses simple passwords, so that any user can log in easily with easy security verification.

2.4 Analysis of the Security System to be Designed

The analysis of the flow of the security system that will be designed will be a reference for mapping the network security system design process. The mapping process can be described as a work process and reference in designing a WPA2-PSK network security system that is connected to radio links, the stages can be seen as follows:

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

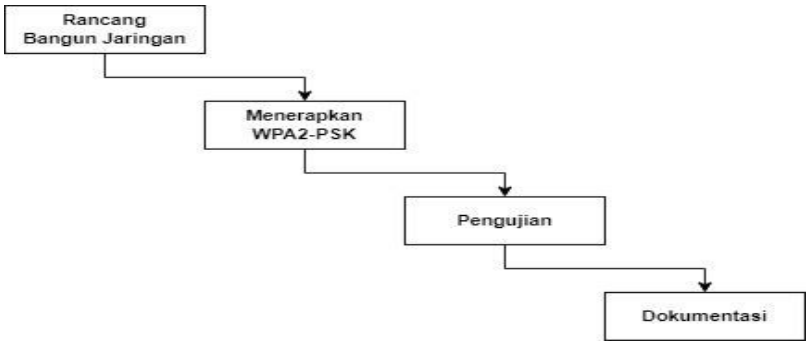

Fig 1. Designed System Flow View

The process of analyzing the security system that will be designed is as follows:

1. Network Design

Build network simulations on a small scale as a medium for the implementation of the WPA2-PSK system and expand the scope of testing sites, including Servers, clients to support the testing process. At this stage, it focuses on connecting between servers and other clients.

2. Implementing WPA2-PSK

This stage is a place for the implementation of the security system of WPA2-PSK in the form of importing keywords in the form of code in the form of numbers or letters that are arranged to be the keywords to be used later by Stuart T.

3. Testing

The next stage of the design and implementation of the security code will be tested; this test is carried out by the user using a laptop device. So that the results are in the form of success or
whether the WPA2-PSK system is implemented in the form of network access or not.

4. Documentation

As a form of report that will be a reference material, it determines whether or not the implementation of the WPA2-PSK security system that has been simulated is successful or not

2.5 System Planning

System design is to design a system that will be built as a logical problem-solving step. The design of the system that is built focuses on how the system is built to meet the needs in network simulation and testing. The steps in designing the security system to be built are as follows:

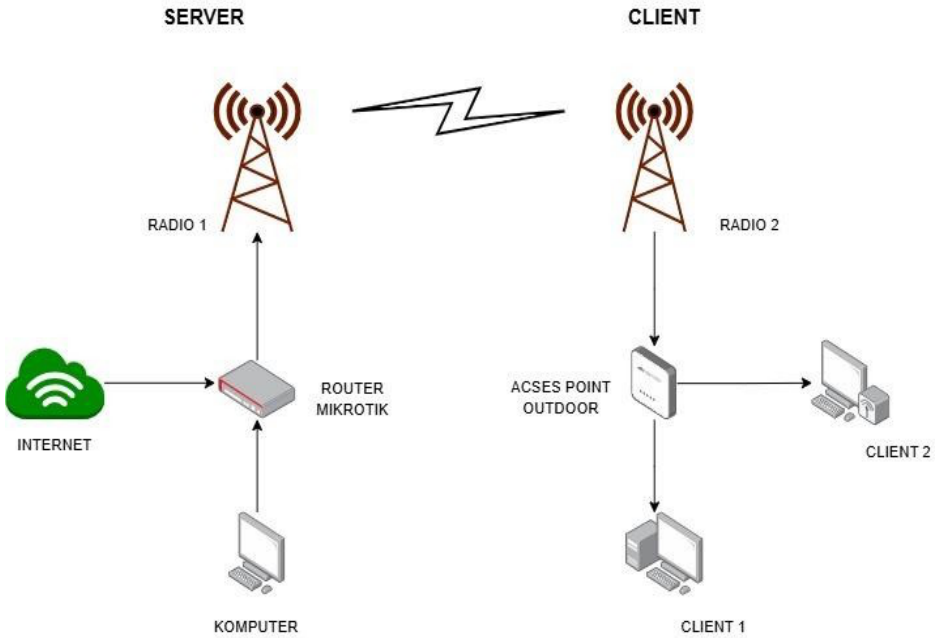

Fig 2. Network Topology Design

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

This design starts with building a server system and then building a client system. The above network topology design is built in stages according to the steps below:

a. Activate the router, which serves as a container for the configuration of the internet and computers. Once the configuration is successful, the network will automatically connect to the router and computer; this internet will be the basic internet source that will divide the internet into radio 1 and radio 2.
b. After the internet data source is transmitted using a Mikrotik router, it will be transmitted to Radio 1.
c. Then radio 1 transmits internet data to radio 2 devices, which are configured to be clients or receivers of internet sources.
d. After radio 2 is connected, activate the Toto link, which will be the Access point outdoors as the network transmitting medium to the client.

2.6 Implementation of the Designed System

After conducting analysis and design, the next process is to implement a system designed to be built in the form of small-scale originalization, using 1 unit of cellphone as an internet data source, 2 units of computers/laptops, 1 Mikrotik router, 2 TP-Link radios, 1 Totolink outdoor access point, RG45 ethernet cables, and Mikrotik winboxes. The process of creating a network security system connected to a radio link uses the WPA2-PSK method, as follows:

a. The first step is to connect the internet and computers to the router; the internet functions as an internet source that will be configured by the router, where this internet is a source of distribution for the construction of radio links. Enter the WinBox as a configuration setting software.

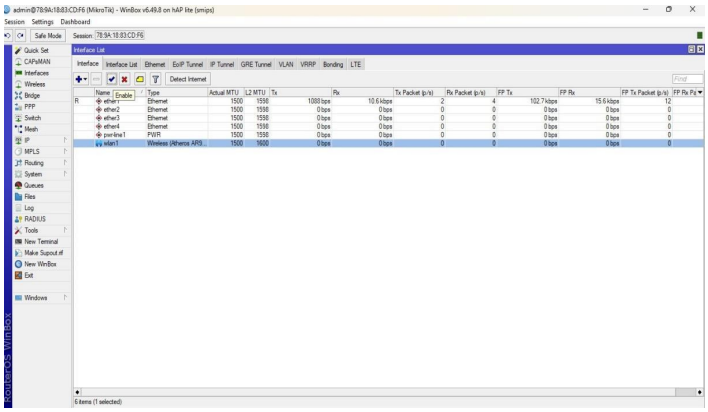

Fig 3. Winbox Interface Display

b. The computer functions as a hardware device where the configuration must be connected first to the port and router. Once the internet configuration on the computer and router is running smoothly, the internet source will generate the IP address 192.168.10.1/24. Then this internet source will be configured on radio 1, which will emit internet that has the IP address 192.168.10.10.

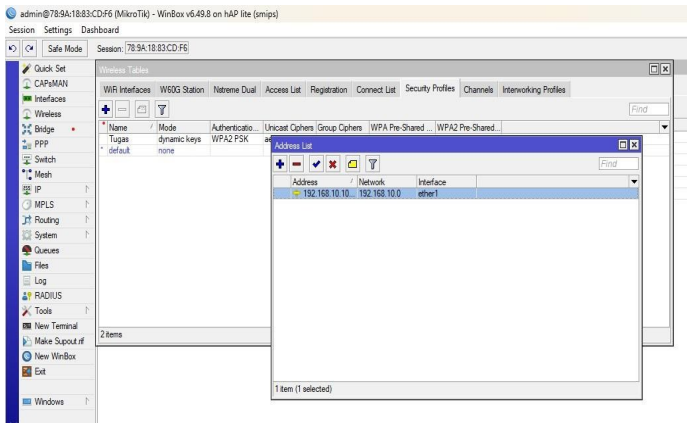

Fig 4. IP Configuration view

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

c. After the internet is connected to the Mikrotik WinBox router, network access and stability checks can be carried out to continue the implementation. If the internet runs and is stable, it can be taken to the next stage, and if it cannot be checked and reconfigured, then associate the internet from the router with the radio link.

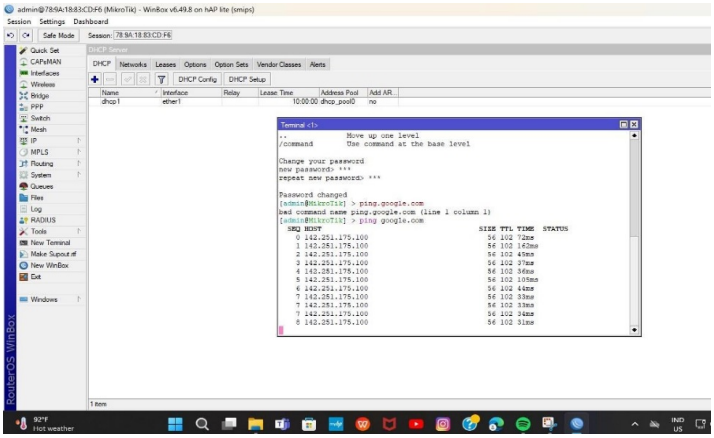

Fig 5. Thermal Display Configuration

d. After the internet source emitted by radio 1 has run smoothly or there is no sign of interference, then, radio 1 is configured to the radio, where this serves to unify the source of IP addresses. After the configuration is successful, radio 2 obtains its own IP address, which is 192.168.10.3.

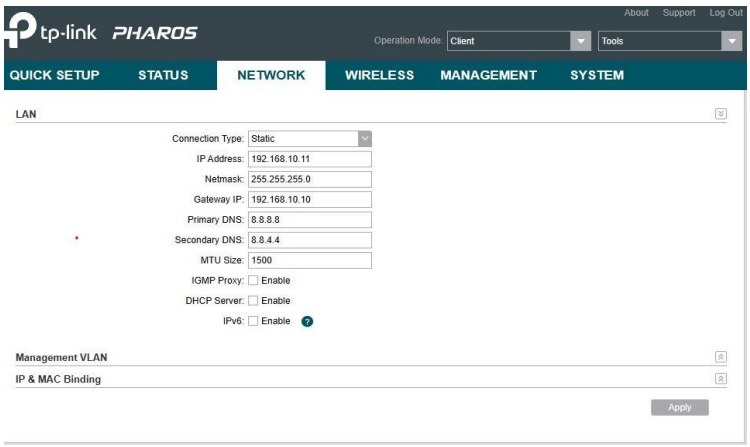

Fig 6. Radio Link Interface Display

e. After IP radio 2 is not disturbed, radio 2 will be channeled to an outdoor access point, where the function of this outdoor AP is to make it easier for computers to monitor network security because the IP address accessed is only one IP address.

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

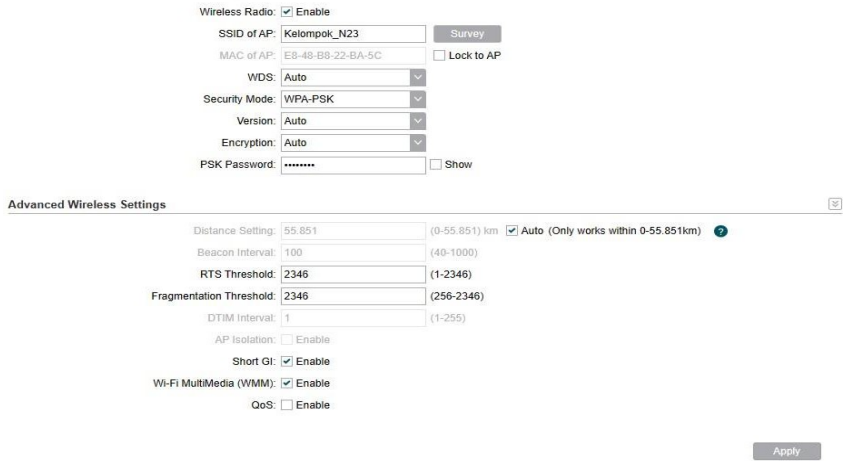

Fig 7. Radio Link Configuration Display

After the configuration is complete, network testing can be performed. Network testing is carried out after creating a server to check whether the network or server is ready to be used. The final test is carried out after the server and client are connected, to test the stability of the network and the security system implemented, whether it is running and functioning properly. After being connected, enter the browser to check the internet connection in the second search (free website). If connected, it means successfully connecting Mikrotik and the radio.

METHOD

This research applies a research method known as library research. According to Dr. Mary J. Rishel (2020), library research is defined as a research process that utilizes libraries as the main source of information. Meanwhile, Dr. William H. Guthrie (2020) stated that library research is a research method that uses the resources available in the library to identify, collect, and analyze information relevant to the research objectives. This method requires a deep understanding of the research process, the ability to collect and evaluate diverse sources of information, and the ability to understand and apply research results appropriately.

The technique used in data collection in this study is the experimental method, where the data collection process of this library research method is by manipulating a variable and measuring its effect on other variables. In this sense, this method emphasizes the relationship between one variable and another. In this study, the variables that will be related to each other are implementation variables, computer network security systems, and connected radio links. These variables must be applied one by one to network security so that the results of this research can be applied in the real world. The data obtained by the author comes from several sources, including online and offline surveys, and observations where the author goes directly to the field to see. In the context of research, it is important to consider the existing field conditions. The data collection technique is carried out through document review, where the researcher collects information from research sources or objects derived from documents or records about events that have occurred. This source of information can be in the form of writings or pictures, such as those found in journals or books.

RESULTS

Before carrying out the research, it is necessary to carry out observations at the research site, in the form of collecting data about the security that is being used at the research site, namely the ITB Indonesia campus. The results of the observation obtained are that the ITB Indonesia campus still uses a fairly simple security system by only using a web login to enter internet access. This makes the author implement a security system that will be designed by the author on the ITB Indonesia campus.

1. Cycle

The system cycle that is built has several stages, including:

a. Planning

Planning in this study, the author designed an internet computer security system that is connected to a radio link that uses the WPA2-PSK security method, this planning is carried out to support and map and organize the

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

course of the research simulation, planning starts from determining the purpose of the problem to be solved, collecting and analyzing research data, analyzing and evaluating data, identifying problems, developing a plan and re-authenticate the research.

b. Planning

Research design can enter the stages of things that will be built on the planned security system. Here is the system planned at this planning stage:

a. Determine what security system will be used on the ITB Indonesia campus.
b. After getting a design of what will be used, the author begins to make the stages of the design security system process.
c. Then the author began to make an implementation of the designed system.
d. After that, the author evaluates the security system designed to be feasible to be implemented on the ITB Indonesia campus.
e. After the evaluation went smoothly and the author felt that the security design was feasible to implement, the author included the security system that was designed as a system that would be applied to the security system design plan.

c. Results display at the end of the design

The results of the design of this study can be seen in Figure V.1 below:

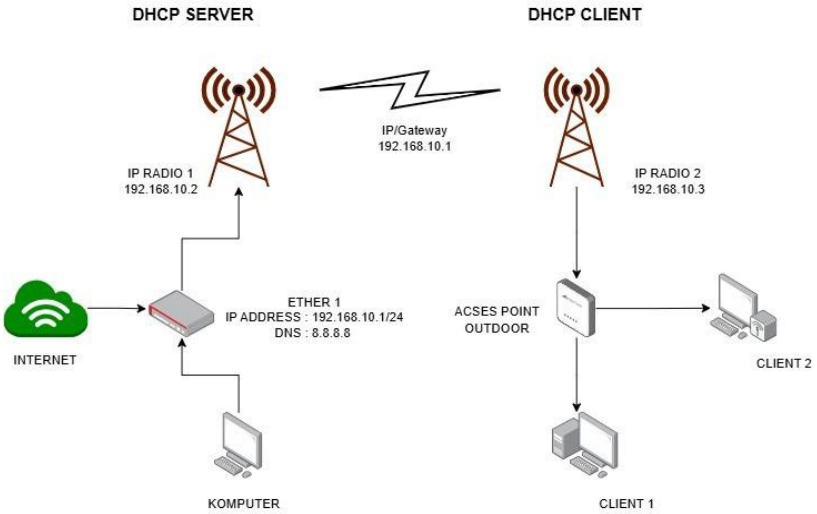

Fig 8. Display of results at the end of the design

The image above is the final view of the system design that was made to fulfill the title of the research, "Implementation of Radio Link-Connected Computer Network Security System on the ITB Indonesia Campus".

2. Evaluate Data Transfer Speed Performance

This study also aims to find out what the speed of data transfer, both uploads and downloads, aims to find out what is the speed of the network capacity that is running. To find out the speed of data transfer that is running, it is necessary to evaluate the speed of data transfer. The steps include:

a. Selection of data transfer speed testing locations, such as indoor and outdoor.
b. Ensure that there are no significant interferences that could affect the test results, such as strong electromagnetic interference or physical obstruction.
c. Once the test location is available, set up the tool for configuration.
d. Run the test, start transmitting data between connected devices via radio link using an application or speedtest in Google Chrome or the appropriate measurement tool. Perform tests for different types of data, such as continuous and burst testing, to measure the system's response to different traffic loads.
e. Record and analyze data, which aims to monitor the results of data transfer speed testing.
f. Documentation of test results.

After the creation of a network security system is successful, the network speed can be detected through a speed test. From the results of this speed test, it can be found what the network speed is for download and upload. Speedtest measures the speed of internet traffic data that is running and being used. The results of the speed test measurement are a benchmark of the speed of data traffic running from the server to the client. The measurement

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

results and the speed of data traffic are influenced by several things, such as the services used, network devices and tools, location, and weather at the location, and stable and variable network speed caused by these factors.

Fig 9. Download and Upload Speed Display

Figure 9 shows that these different download and upload speeds are influenced by the internet source used, but this does not interfere with the system security connection. Usually, the loading and upload speeds are different; the download speed is faster than the upload due to more download activities than uploads. The results of the Mbps speed upload and download. The test is said to be successful if the upload and download speed displayed at the time of the speed test can be detected and has a fixed or unchanging display.

DISCUSSIONS

After going through the design, implementation, and testing stages of the system, this study then analyzes the results obtained to evaluate network performance and security. The analysis focuses on the performance of radio link-based mesh networking with WPA2-PSK and compares it with previous research to comprehensively determine the contribution and effectiveness of the developed system.

1. Performance of Security System Design in Radio Link-Based Mesh Network

The implementation of a network security system in a radio link-based mesh topology demonstrates a significant contribution to maintaining data integrity and communication reliability within the ITB Indonesia campus environment. The designed system integrates a point-to-point radio link within a broader mesh networking framework, enabling stable interconnection between nodes while maintaining controlled data flow through firewall mechanisms.

The results indicate that the applied topology enhances network resilience, particularly in multi-building environments. Unlike conventional single-path configurations, the mesh-based approach provides alternative communication routes, thereby reducing the impact of node failure. This characteristic directly improves network availability and minimizes downtime.

In terms of security structure, the incorporation of firewall filtering mechanisms ensures that only authorized traffic is permitted across the network. Continuous monitoring further strengthens the system by enabling early detection of anomalies or suspicious activities. This finding aligns with previous research by Adiguna (2022), which emphasized that vulnerabilities in network systems often emerge from open ports and insufficient monitoring processes. Therefore, integrating topology design with active supervision contributes to a more robust security posture.

2. Implementation and Performance Analysis of WPA2-PSK Security Mechanism

The implementation of WPA2-PSK within the mesh network architecture shows measurable improvements in securing wireless communication over radio links. The system successfully encrypts transmitted data, reducing the likelihood of unauthorized interception.

From the performance perspective, WPA2-PSK demonstrates efficiency in authentication and encryption without requiring complex infrastructure. The absence of centralized authentication servers simplifies deployment, making it suitable for campus-scale networks with limited resources. However, this simplicity also introduces certain limitations, particularly in scalability and key management.

When compared to earlier security protocols, the findings are consistent with the study conducted by (Efendi ,2021), which concluded that WPA provides stronger resistance to attacks than WEP due to its improved encryption algorithms. In this study, WPA2-PSK not only enhances confidentiality but also maintains stable throughput and acceptable latency levels in radio link communication.

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

Despite its advantages, the analysis reveals that WPA2-PSK relies heavily on the strength and confidentiality of the pre-shared key. Weak password configurations may still expose the system to brute-force attacks. This observation supports (Howard's, 2021) perspective that preventive security mechanisms must be complemented by proper user management and policy enforcement.

3. System Flexibility and Efficiency in Mesh Networking Environment

The evaluation results show that the designed system offers a high level of flexibility and efficiency in securing radio link-based networks. The integration of MikroTik RouterBoard 941 devices within a mesh topology allows dynamic configuration and adaptability to changing network conditions.

One of the key findings is the system's ease of deployment compared to more complex enterprise-level security architectures. The use of a single authentication mechanism simplifies configuration while maintaining adequate security for medium-scale environments such as educational institutions. Additionally, compatibility with various end-user devices ensures seamless connectivity across different platforms.

Compared to previous studies that focused solely on security protocol analysis, this research provides a more comprehensive approach by combining network topology (mesh), hardware implementation (MikroTik), and security mechanism (WPA2-PSK). This integration results in a balanced system that not only secures data transmission but also improves overall network performance.

However, in contrast to enterprise-grade solutions utilizing WPA2-Enterprise or RADIUS-based authentication, the current system shows limitations in user access control granularity. While suitable for general campus use, further development is required to support larger-scale deployments with higher security demands.

This research has a key advantage in its approach that integrates security, network performance, and technology implementation into a single, comprehensive system. Unlike previous research that generally focused solely on encryption method analysis or vulnerability identification, this research combines the use of WPA2-PSK, mesh networking topology, and radio link communication into a single, concrete architecture. This integration allows for increased network stability while effectively maintaining data security. Furthermore, the use of the MikroTik RouterBoard 941 offers advantages in terms of cost efficiency and ease of configuration, making the system more applicable to campus environments. Another advantage lies in the system's ability to maintain connectivity through a self-healing mechanism in mesh networks, a feature not widely discussed in previous research. Thus, this research provides not only theoretical analysis but also practical solutions that can be immediately implemented.

CONCLUSION

Based on the evaluation, testing, and validation processes carried out on the implemented system, the network security design using WPA2-PSK within a radio link-based mesh networking environment demonstrates significant effectiveness in securing data transmission and maintaining network performance at ITB Indonesia Campus. The findings indicate that the developed system provides a practical and efficient solution for securing wireless communication. The configuration process is relatively simple, as it only requires a pre-shared key (PSK) to authenticate users without involving additional infrastructure such as RADIUS servers. This simplicity contributes to faster deployment and easier management, particularly in campus environments with dynamic user access. In terms of security performance, the application of WPA2-PSK enhances data protection through strong encryption mechanisms. This ensures that transmitted information remains confidential and can only be accessed by authorized users. As a result, the risk of unauthorized access, data interception, and potential cyberattacks is significantly reduced. The system also supports various modern devices, including computers, smartphones, tablets, and IoT devices, ensuring broad compatibility across the network.

Furthermore, the integration of this security mechanism within a radio link-based mesh topology contributes to improved network stability and reliability. The system is capable of maintaining secure connections even in complex infrastructure conditions, such as multi-building campus environments.

Overall, the results confirm two main advantages of the implemented WPA2-PSK security system. First, it effectively improves the overall security level of the wireless network by minimizing potential threats and unauthorized access. Second, it strengthens data protection by ensuring that sensitive information transmitted across the network is safeguarded against eavesdropping and malicious activities.

These outcomes demonstrate that the proposed system not only meets security requirements but also supports efficient and stable network performance, making it suitable for implementation in educational institutions.

REFERENCES

Adiguna, M. A. (2022). WPA2-PSK network security analysis using penetration testing method (Case study: TP-Link Mercusys MW302R router).

JCEIT: Journal of Computer Engineering and Information Technology
Volume 2, Number 2, March 2026
Page: 138-149
ISSN 3089-106X
(online)

Anhar. (2020). Jaringan komputer dan internet. Informatika.
Athailah. (2020). Bandwidth management in optimizing the use of Mikrotik routers for network connection services. Journal of Informatics, 7(2), 70–78.
Brown, S. (2021). Computer network development system. McGraw-Hill.
Cisco Networking Academy. (2020a). Introduction to networks: OSI model. Cisco Press.
Cisco Networking Academy. (2020b). The application of virtual local area network. Journal of Electrical Engineering Innovation, 1(1), 70–80.
Danniel. (2021). Comparison of IPv4 and IPv6 in building networks. International Journal of Computer Networks, 3(2), 30–40.
Efendi, M. Y. (2021). Comparative analysis of 128-bit WEP and WPA wireless security methods to improve wireless security. Journal of Information Security, 5(1), 10–18.
Goldsmith, A. (2020). Wireless communications. Cambridge University Press.
Hamacher, V. C. (2020). Decision-making model under complex picture fuzzy Hamacher aggregation operators. Journal of Intelligent Systems, 9(8), 47–68.
Harefa, M. F. (2021). User data security applications and wireless security systems using two-factor authentication and MAC address filtering. Journal of Computer Security, 4(1), 20–28.
Harmayani, H., Abdilah, D., Mapilindo, M., Oktopanda, O., & Hutahaean, J. (2021). Aplikasi komputer. Yayasan Drestanta Pelita Indonesia.
Heart, A. (2020). Analysis and implementation of Mikrotik router security system from Winbox exploitation, brute-force, and DoS attacks. Jurnal Media Informatika Budidarma, 4(1), 57–59.
Jackson, M. (2020). Hierarchical network design-based network security system design. International Journal of Network Security, 5(8), 1–9.
John, A. (2021). Analysis and application of Mikrotik RB890. Journal of Network Engineering, 2(6), 50–60.
Kamila, M. (2024). Design and construction of practicum module simulation of microwave link installation on mobile systems based on virtual reality technology.
Kozierok, C. M. (2021). The TCP/IP guide: A comprehensive, illustrated internet protocols reference. No Starch Press.
Madcoms. (2020). Network security implementation using port blocking and port knocking methods on Mikrotik RB941. Journal of ICT: Information Communication & Technology, 5(1), 16–17.
Michael, J. (2021). OSI model fundamentals. Computer Networks Journal, 1(5), 1–8.
Molisch, A. F. (2021). Wireless communications (2nd ed.). Wiley.
Prayoga, J. (2021). Comparison of WPA2 EAP-PSK authentication system on wireless networks using penetration testing method with fluxion tools. Journal of Cyber Security, 3(1), 1–10.
Permatasari, U. S., & Widiasari, I. R. (2020). Analisis routing protokol optimized link state routing (OLSR) pada Raspberry Pi. Jurnal Teknologi Informasi (AITI), 16(2), 151–164.
Primaned, A., Widyawan, W., & Kusumawardani, S. S. (2014). Unjuk kerja routing protocol OLSR pada wireless mesh network berbasis IEEE 802.11b/g. Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 1(1), 8–12.
Defri, E. O., Kusmaryanto, S., & Mustofa, A. (2019). Implementasi jaringan access point dengan wireless distribution system (WDS) berbasis Mikrotik. Jurnal Mahasiswa Teknik Elektro Universitas Brawijaya, 7(7).
Politeknik Sawunggalih Aji. (2021). Rancang bangun wireless mesh network menggunakan routing OLSR. Jurnal Nasional Teknik Informatika, 9(2).
Sofana, I. (2021). Jaringan komputer berbasis TCP/IP. Informatika.
Stevens, W. R. (2020). TCP/IP illustrated (Vol. 1). Addison-Wesley.
Supendar, H., & Handrianto, Y. (2017). Simple queue in resolving bandwidth management issues on the Mikrotik bridge. Bina Insani ICT Journal, 4(1), 21–30.
Sutiono. (2020). Sistem keamanan jaringan. Deepublish.
Tanenbaum, A. S., & Wetherall, D. J. (2020). Computer networks (5th ed.). Pearson.
Wheeb, A. H., Nordin, R., Samah, A. A., & Kanellopoulos, D. (2023). Performance evaluation of standard and modified OLSR protocols. Electronics, 12(6), 1334.
Widiyawati, S. (2020). Network security system firewall using port blocking and firewall filtering methods. Journal of Information Security, 5(2), 78–96.
Wirano, B. (2020). Policy analysis from formulation to implementation. Deepublish.