Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Wireless Network Security Using Hotspot Login Authentication Method: Keamanan Jaringan Nirkabel Menggunakan Metode Otentikasi Masuk Hotspot

Bima Yusup Septiana — Program Studi Pendidikan Teknologi Informasi, Fakultas Keguruan & Ilmu Pendidikan, Universitas Muhammadiyah Muara Bungo
Yogi Irdes Putra — Program Studi Pendidikan Teknologi Informasi, Fakultas Keguruan & Ilmu Pendidikan, Universitas Muhammadiyah Muara Bungo
Fitri Yanti — Program Studi Pendidikan Teknologi Informasi, Fakultas Keguruan & Ilmu Pendidikan, Universitas Muhammadiyah Muara Bungo

Abstract. General Background: Wireless networks are widely used in public spaces such as cafés, yet their openness often poses risks of security breaches, uncontrolled bandwidth usage, and poor service quality. **Specific Background:** At Café Lilnook Karawaci, Tangerang, the Wi-Fi network lacked authentication, user restrictions, and bandwidth management, making it vulnerable to misuse and inefficiency. **Knowledge Gap:** While prior studies emphasize the importance of network authentication and monitoring, limited research explores practical hotspot login authentication using MikroTik RouterBoard in small business environments. **Aims:** This study aims to design, implement, and evaluate a secure wireless network system with hotspot login authentication using MikroTik RB50UG, guided by the Network Development Life Cycle (NDLC) method. **Results:** Functionality testing with five users and two administrators achieved a feasibility score of 1 (feasible), while usability testing reached 100% (very feasible), confirming effectiveness in both security and performance management. **Novelty:** The research integrates captive portal-based hotspot authentication with customized configurations in a café setting, demonstrating an adaptable and cost-effective approach to small-scale network security. **Implications:** Findings indicate that implementing hotspot login authentication not only enhances security and service quality but also provides a scalable model for similar public access networks, supporting safer digital environments in hospitality sectors.

Highlight :

1. Hotspot login authentication enhances network security in public environments.
2. Functionality and usability tests show the system is feasible and effective.
3. Applying the NDLC method provides a structured process from design to network management.

Keywords : Authentication, Login Hotspot, NDLC, Functionality, Usability

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Introduction

Based on field observations, several fundamental issues related to the internet network system at Café Lilnook Karawaci, Tangerang, have been found that can disrupt user security, performance, and comfort. Currently, the Wi-Fi network in use still operates without password protection, without limitations on the number of users, and without bandwidth management.[1] This condition results in uncontrolled internet consumption and poses a risk of degrading service quality.[2] In addition, open network access allows anyone, including irrelevant parties, to connect without restrictions, thus increasing the risk of access abuse and threatening network security.[3]

Without adequate authentication and encryption mechanisms, data transmitted over the network can be easily accessed by unauthorized parties. Sensitive information such as login credentials, personal data, or online transaction activities is at risk of interception.[4] The lack of access control makes it easier for irresponsible actors to engage in illegal activities over the network, such as spreading malware, phishing, or even attacking third-party systems. The majority of customers access the internet using more than one device (for example, smartphones and laptops simultaneously). Without restrictions, this leads to excessive bandwidth consumption, which ultimately slows down the internet connection and reduces service quality.

The solution designed to address security issues and network management at Café Lilnook Karawaci is to build an internet access management system based on hotspot login authentication using the MikroTik RouterBoard 50UG device.[5] The captive portal or hotspot login authentication method was chosen because it can automatically direct every user to the login page before granting internet access.[6] According to, The captive portal functions as an administrative control layer that ensures every connection has been verified, so it can be accounted for in terms of security.

The MikroTik RouterBoard 50UG device acts as a gateway and also as a hotspot server that manages the authentication process, bandwidth settings, and access restrictions. This is in line with the opinion.[7] which states that logging on public networks is important to detect and prevent illegal activities. As a final stage, system testing was carried out using the Blackbox Testing method to ensure that all functions operate according to the design. This method is considered appropriate because it focuses on testing the output of the system based on the input without looking at the internal code, as explained by that Blackbox Testing is effective for testing system functionality from the user's perspective.

Theoretical Studies

According to, Wireless networks utilize transmission media in the form of electromagnetic waves which enable data communication processes to be carried out efficiently without requiring physical conductors like copper cables or fiber optics.[8] Wireless networks have high efficiency, both in terms of cost and speed of dissemination, especially in areas that lack cable infrastructure.[9]. A computer network security system is a machine used to carry out and prevent unauthorized or improper users from accessing a computer network.[10] The weakness of wireless networks lies in the configuration and type of encryption used; it is often found that wireless networks still use default vendor configurations such as SSID, IP Address, remote management, DHCP enabled, frequency channel, and even user/password for administration.[11]

The MikroTik RouterBoard 50UG is one of the router devices based on RouterOS designed to combine routing, network management, firewall, VPN, and hotspot system functions into a compact hardware device. The RouterOS, which is its operating system, provides a Hotspot Gateway module that can automatically display a login page (captive portal) to new users, manage authorization both locally and through a RADIUS server, as well as restrict access based on usage duration (timeout) or bandwidth capacity (MikroTik Documentation in.[12] Customization of the login page

can be done by modifying the default HTML/CSS files of RouterOS, so that it can be tailored to the identity or branding of the network being built.[13]

According to MikroTik documentation in, Winbox supports connections to the router via both IP and MAC addresses, allowing access even if the IP configuration has not been completed. In the implementation of the hotspot login authentication system, Winbox is used to configure the Hotspot Server, User Profile, and the captive portal page. Administrators can upload custom HTML/CSS files directly to the router's hotspot directory through the File feature in Winbox.[14] This enables personalization of the login page according to the network's identity. LAN cable is a copper-based transmission medium used to physically connect network devices. According to, UTP cables have four pairs of twisted copper wires to reduce electromagnetic interference.[15]

An Access Point is a device that emits Wi-Fi signals so that user devices can connect to a hotspot network. According to Gast, the AP acts as a bridge between wireless and wired networks, and supports IEEE 802.11 standards such as 802.11n, 802.11ac, or 802.11ax for better speed and range.[16] According to MikroTik documentation in, The integration of AP with the Hotspot Server facilitates the detection of new users, displays the captive portal, and manages login sessions more accurately.[17] Configuration on the Mikrotik RouterBoard is an important step in building a secure, managed, and efficient hotspot network system.

According to explains that NDLC is a key model in the computer network design process, adopting an approach similar to the software development life cycle (SDLC) and consisting of phases such as analysis, design, simulation prototyping, implementation, monitoring, and management.[18] explains that NDLC is a methodology for designing or developing network infrastructure that allows for statistical monitoring and network performance. Based on the literature review that has been described, this study poses the hypothesis of how the design, functionality, and usability of the Design and Security of Wireless Networks with the Hotspot Authentication Login Method using Mikrotik RouterBoard 50UG at Café Lilnook Karawaci Tangerang.[19]

Research Method

This research uses the Research and Development (R&D) method, which aims to produce a specific product and test the effectiveness of that product. Research and development methods are research methods used to produce specific products and test the effectiveness of those products. The design model in this research uses the NDLC (Network Development Life Cycle) method, which is a systematic approach to the planning, development, implementation, and maintenance of computer networks. The stages in NDLC include needs analysis, design, prototype simulation, implementation, monitoring, and management.[20]

Product testing is conducted to ensure that the developed system meets the requirements and functions according to the established goals.[21] This testing phase aims to assess the functionality and usability of the MikroTik RB 50UG-based hotspot login authentication with the captive portal method that has been implemented at Café Lilnook Karawaci Tangerang. The number of subjects in the small-scale trial ranged from 6 to 8 people. In this study, the trial involved 5 users and 2 managers of Café Lilnook Karawaci Tangerang. Primary data was collected at the research site, namely Café Lilnook Karawaci, Tangerang. This data was obtained through system trials, so the information gathered is current and relevant to the research objectives.

Results and Discussion

1.The Analysis Stage is carried out to ensure that the design created can be targeted accurately and is in accordance with the management needs of the Lilnook café network in Karawaci Tangerang.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

a.The interview was conducted with the relevant parties directly involved in network management at the location, resulting in findings: frequent obstacles (users freely access without logging in, bandwidth runs out quickly, difficult to monitor usage) as well as main needs, such as the existence of a login system before accessing the internet, bandwidth limitation settings, and user activity logging.

b.Observation of the network topology in use, available hardware, and the quality and capacity of the internet connection.

Figure 1. *Network topology at lilnook café Karawaci Tangerang*

Figure 2. *Bandwidth Capacity at lilnook café*

c.Hardware and Software Requirements

Hardware and Software used for designing a wireless network with hotspot login authentication. The purpose of the Hardware and Software at Café Lilnook is to regulate, limit, and monitor visitors' internet access securely, structurally, and efficiently. The specifications of the hardware and software can be described as follows:

Perangkat keras (*hardware*)	Perangkat lunak (*software*)
1. MikroTik RouterBoard 50UG (5 port Gigabit Ethernet, 1 port USB 2.0, CPU Atheros ARM 950 MHz, RAM 512 MB, RouterOS Level 4). 2. *Access Point* (untuk penyebaran sinyal Wi-Fi). 3. Kabel LAN CAT5E untuk koneksi antar perangkat.	1. RouterOS bawaan MikroTik. 2. Winbox untuk konfigurasi. 3. Sublime text untuk kustomisasi halaman login.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Figure 3. *Hardware and Software Requirements*

2.Design Stage

Based on the results of the observation and analysis of network needs at Café Lilnook Karawaci, an initial design of an internet network system has been carried out, utilizing a captive portal-based hotspot login authentication method on the MikroTik RouterBoard 50UG. This design aims to regulate and secure internet access for visitors, while also facilitating the process of network management by the café management.

3.Prototyping Simulation Stage

a.Installation of Mikrotik Routerboard 50UG hardware, using a laptop with a LAN CAT5E cable on port 2 of the Mikrotik.

b.Installation of F477V2 access point hardware with a cable length of 7m, then connect the access point to the laptop using a LAN CAT5E cable on port 1 of the access point.

c.Installation of Winbox software by entering the MAC Address of the Mikrotik, for example F4:1E:57:6B:88:EE, for the first login use admin while the password is stated at the bottom of the router.

4.Implementation Stage

a.Administrator Configuration

The administrator configuration aims to set a password for accessing the administrator window on WinBox to prevent unrestricted access. The identity of the router and administrator can be changed using the WinBox facility in the System > Identity tab to set the Router Identity, and System > users to change the login user and set the router password when logging into WinBox.

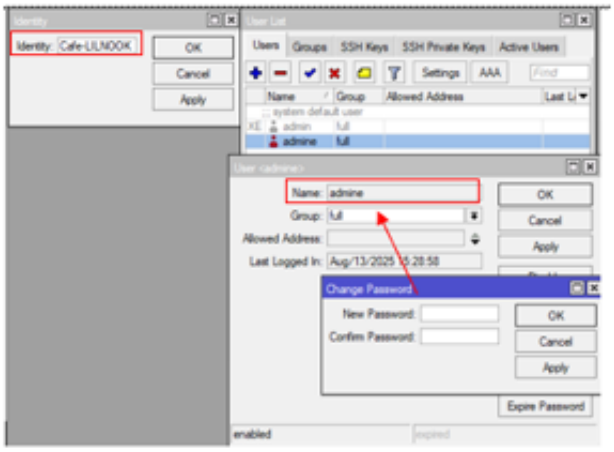


Figure 4. *Router Names and Administrator*

b.Interface Configuration

The LAN interface is used to configure the local network parameters that connect the Router with the users/administrators connected to the Router's LAN Port. The Wi-Fi interface is intended to

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

configure the WLAN network parameters or to connect the Router with clients/users connected via wireless media, as well as to separate the wireless network from the wired network.

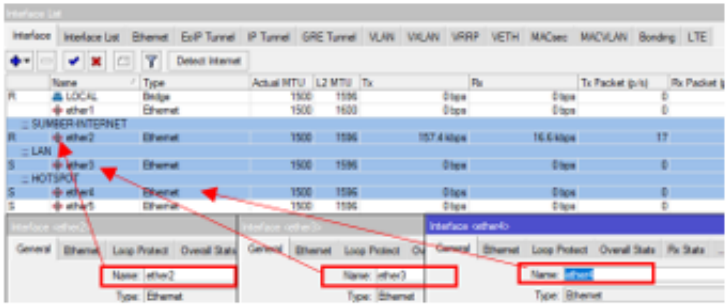


Figure 5. *Router Interface*

c.IP Address Configuration

An IP Address is a primary requirement in building a network, because without an IP Address the network will not be connected. According to the design of the network topology, the design of the IP Address is as follows:

a)Ether2: Using DHCP Client from ISP (Internet Service Provider)

b)Ether3: As a local network parameter with IP Address 192.168.101.1/24

c)Ether3: As the hotspot gateway with IP Address 192.168.201.1/24

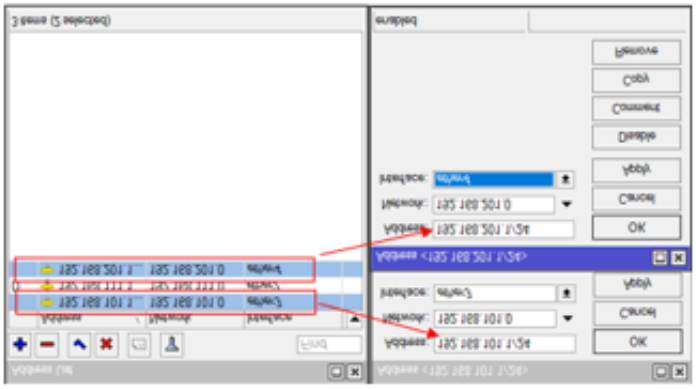


Figure 6. *IP Address Configuration*

d.DNS Configuration

Domain Name Server (DNS) functions to translate domain names into a series of IP numbers. The DNS on the router is usually automatically filled from internet sources.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

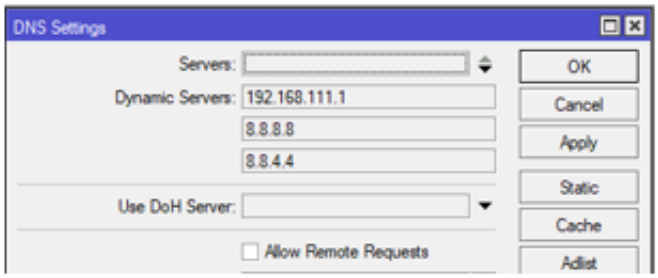


Figure 7. *DNS Configuration*

e.DHCP Client Configuration

The steps to configure the DHCP Client are by going to IP > DHCP Client and then selecting the interface ether2-internet. If the configuration is correct, an IP Address will appear with a bound status indicating that the configuration is correct. As shown in the following image.

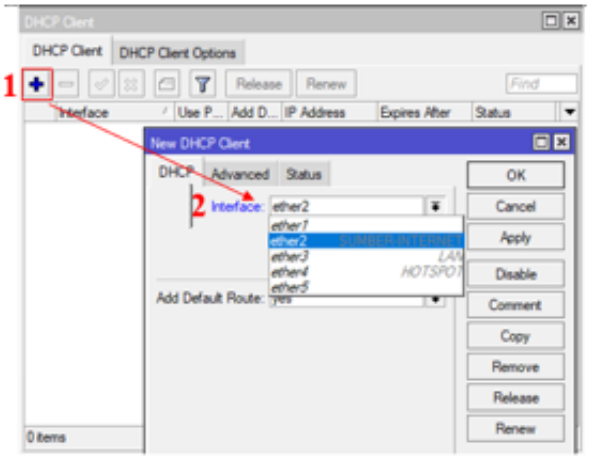


Figure 8. *DHCP Client Configuration*

f.DHCP Server Configuration

1)The first step is to click on IP > DHCP Server > click on DHCP Setup, then to create a DHCP Server, click on DHCP Setup, which will display an image like the one below. In the DHCP Server Interface, select ether4, because we will be assigning IPs to clients on the local network.

2)Then determine the IP Pool that will be distributed to the clients connected to the local network, for the distributed IP Address which is 192.168.201.2-192.168.201.254, but it can be changed according to needs.

3)Determine the DNS Server for internet network connections, which can be adjusted to the ISP modem IP or Google.

4)After the configuration is completed, a message “Setup has completed successfully” will appear as shown in the following image. Thus, the DHCP server we created will automatically be displayed.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

g.Hotspot Gateway Configuration

Before performing the hotspot gateway installation, make sure that the DNS and IP Pool have been configured first. Here is the installation of the hotspot gateway. Configure through IP > Hotspot in the menu, click Hotspot Setup to select the hotspot interface. Then a local IP appears according to what has been previously created in ether4. After that, click Next. Then determine the IP Pool according to the desired needs, then Next. Determine the DNS that has been predetermined. Then Next. After 'Setup has completed successfully' appears, as shown in the picture below, it means the hotspot has been successfully created.

h.Network Address Translations (NAT) Configuration

To configure the NAT firewall rule using the src-address parameter. The rule used is chain=srcnat out-interface=ether2, then in the action menu select Masquerade. Configuration can be done using Winbox through the menu IP > Firewall> NAT tab. As shown in the image below:

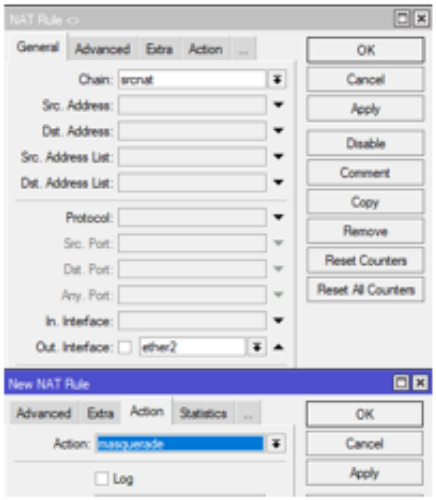
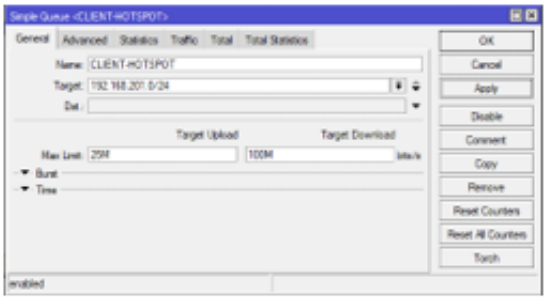


Figure 9. *Network Address Translation (NAT) Configuration*

i.Simple Queue Configuration

In the Simple Queues menu on Mikrotik, click Add (+) to create a new queue. In the General tab, provide a queue name as needed, for example, Name = CLIENT-HOTSPOT, then specify the Target by entering the IP address or network to be limited, such as 192.168.201.0/24. Next, set the Max Limit to establish upload and download speed limits, for example, 25M/100M. After all settings are completed, click Apply to apply the configuration and OK to save it.



Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Figure 10. *Simple Queue Configuration*

j.User Profiles Configuration

In the Hotspot menu on Mikrotik, select the User Profiles tab, then click Add (+) to create a new profile. Provide a name for the profile as needed, then set parameters such as Address Pool to determine the IP range, Rate Limit to restrict upload/download speed for example 3M/3M, Shared Users for the number of devices allowed, and time settings such as Session Timeout, Uptime Limit, and Idle Timeout. Then navigate to the Queue tab, set Insert queue before = bottom and Parent queue = CLIENT-HOTSPOT (the Parent we created earlier). After all settings are correct, click Apply to implement, then OK.

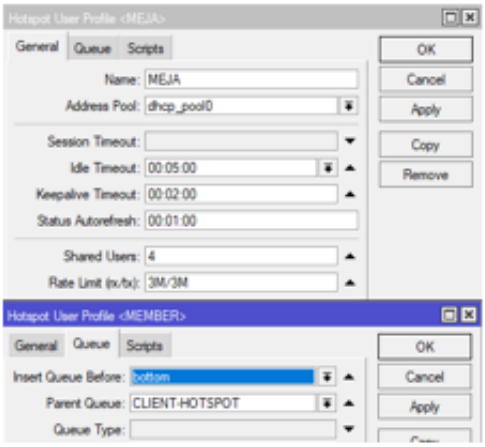


Figure 11. *User Profile Configuration*

k.Access Point (AP) Configuration

Configuration of the access point to add and configure the access point that functions to broadcast the IP Address to clients.

1)IP Address configuration and login to F477v2

The IP Address configuration on the access point is aimed at ensuring smooth access into the access point, and here we are using the Fiberhome F477v2 access point. First, we need to align the laptop's IP with the access point's IP, such as the default IP of F477v2 which is 192.168.1.1, so the laptop should be changed to 192.168.1.2. Then, open the Chrome browser and type in 192.168.1.1. After that, select Administrator and log in with the password admin.

2)Set the F477v2 configuration to Hotspot Access Point

After logging in as an administrator, the first step that needs to be taken is to change the device mode from Router to Bridge, so that the network management function will be completely transferred to Mikrotik. After that, disable the DHCP Server feature on the access point so that the distribution of IP addresses is fully controlled by Mikrotik. Connect the LAN port of the access point to Mikrotik using an ethernet cable. Next, enable the Wi-Fi feature on the access point and set the SSID, for example, using a name that matches the café branding, and set the password or security to open since there will be a captive portal from Mikrotik later. Finally, ensure that the IP address used by the access point does not conflict or is the same as the Mikrotik IP address to avoid

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

network conflicts. Then click submit on every action taken to ensure the configuration is saved on the access point.

3)Authentication login hotspot page configuration

As we know, the Mikrotik RB-50UG has a very simple default login page. This default Mikrotik login page can be edited, modified, and customized according to the individual user's needs.

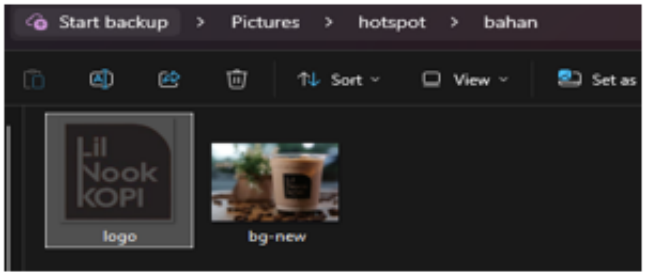
a)Taking the default display file from Mikrotik

Open winbox, go to the file menu. All the files for the hotspot login page are in the hotspot folder. To edit the file, right-click on the hotspot file in the Mikrotik files. Then download and place it in the folder of your choice. Next, enter the hotspot folder and select the login.html file to edit; you can use Sublime Text software for editing. Once the login.html file is opened with Sublime Text, this is what the entire script of the login.html file looks like.

b)Design the Login Page Appearance

Here is the script that has been edited to enhance the appearance of the login page according to requirements.

Figure 12. *Default Mikrotik Hotspot Script*



Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Figure 13. *Import Background and Logo File*

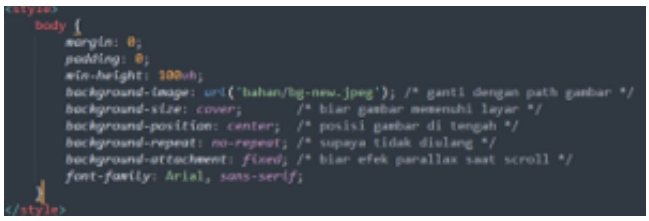


Figure 14. *Changes the Login Background Display*

Figure 15. *Changing the Logo*

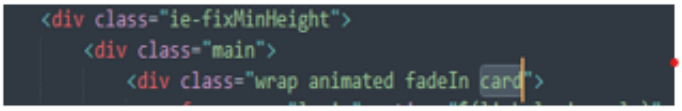


Figure 16. *Giving a Class Card on the Login Display*

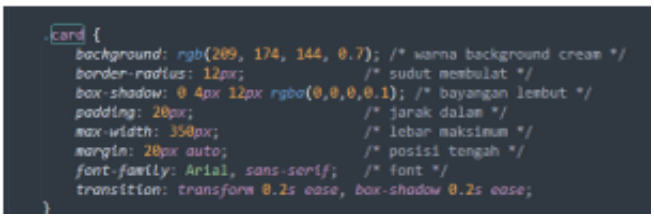


Figure 17. *Provides a Style Card for the Login Display.*

Figure 18. *Adds the btn-link class*

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

```css
.btn-link {
    display: inline-block;
    padding: 10px 20px;
    background-color: #6b5b4d;        /* warna krem logo */
    color: white; /* teks hitam pekat */
    font-weight: bold;
    text-decoration: none;
    border-radius: 8px;
    box-shadow: 0 4px 8px rgba(0,0,0,0.25);
    transition: all 0.2s ease;
}
.btn-link:hover {
    background-color: #d1ae90;        /* warna krem logo */
    color: black; /* teks putih saat hover */
    transform: translateY(-3px);
    box-shadow: 0 6px 12px rgba(0,0,0,0.35);
}
```

Figure 19. *Changing the Button Style Click Here*

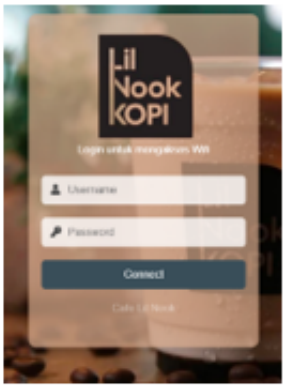


Figure 20. *Hotspot Login Display Results*

c)Creating Status Page

Here is the script that has been edited to enhance the appearance of the status page according to requirements.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

Figure 21. *Default Script of the Status Page*

```
<style>
    body {
        margin: 0;
        padding: 0;
        min-height: 100vh;
        background-image: url('bahan/bg-new.jpeg'); /* ganti dengan path gambar kamu */
        background-size: cover;       /* biar gambar menutupi layar */
        background-position: center;  /* posisi gambar di tengah */
        background-repeat: no-repeat; /* supaya tidak diulang */
        background-attachment: fixed; /* biar efek parallax saat scroll */
        font-family: Arial, sans-serif;
    }

    .card {
        background: rgba(209, 174, 144, 0.7);              /* warna background putih */
        border-radius: 12px;                /* sudut membulat */
        box-shadow: 0 4px 12px rgba(0,0,0,0.1); /* bayangan lembut */
        padding: 20px;                      /* jarak dalam */
        max-width: 350px;                   /* lebar maksimum */
        margin: 20px auto;                  /* posisi tengah */
        font-family: Arial, sans-serif;   /* font */
        transition: transform 0.2s ease, box-shadow 0.2s ease;
    }
</style>
```

Figure 22. *Changing the Background Appearance and Adding a Card*

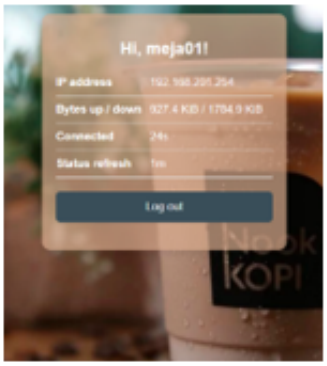


Figure 23. *Status Display Results*

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

d)Initial Testing

Conduct experiments on the previously configured network system to see if it works or not. To perform the testing, the steps are as follows:

i.Hotspot network trial, on the MikroTik hotspot login page, users are asked to enter the username and password that were created previously. If the information is correct, users will be granted internet access according to the configured hotspot profile set earlier. Below is the appearance of the captive portal or authentication login for Lilnook café hotspot.

ii.If the user is not registered, they will not be able to log into the network with a notification of invalid username or password. As shown in the following image.

iii.If the client successfully logs in, they will automatically connect.

iv.Network speed or bandwidth test.

Figure 24. *Network Speedtest*

v.The next step is to check through winbox.

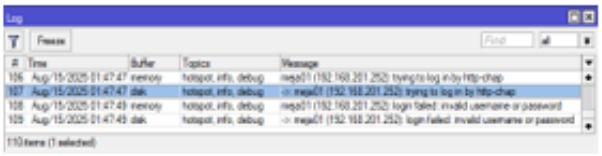


Figure 25. *Monitoring Invalid Username and Password in Winbox*

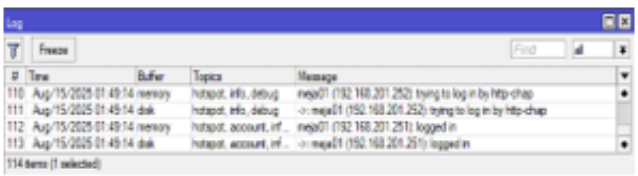


Figure 26. *Monitoring Valid Username and Password in Winbox*

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

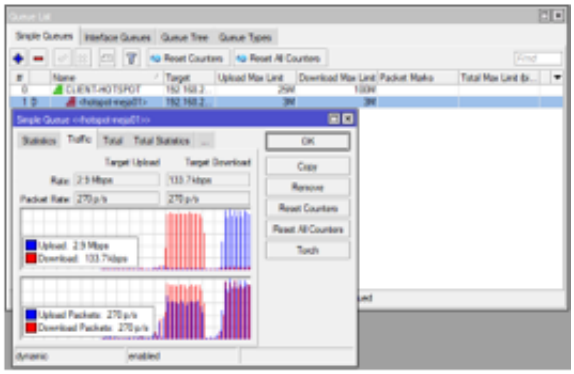


Figure 27. *Upload and Download Bandwidth Restrictions and Tests*

5.The Monitoring stage is an evaluation process to ensure that the hotspot network system that has been built operates according to the functional specifications and user needs established during the design phase.

6.The testing is conducted to assess two main aspects, namely functionality and usability.

a.Functionality test results

The results of testing the functionality of the MikroTik RB 50UG based hotspot system using the captive portal method are able to operate according to the designed functions, ranging from navigation, login process, to internet connection stability. The test subjects included 5 customers of Café Lilnook and the network administrator of Café Lilnook.

No	Aspek *Functionality*	Jawaban	
		Berhasil	Tidak berhasil
1	Navigasi pada halaman *login*	7	0
2	Login menggunakan username dan password	7	0
3	Akses halaman *captive portal*	7	0
4	Validasi *username* dan *password*	7	0
5	Pembatasan bandwidth sesuai pengaturan	7	0
6	Koneksi internet berjalan stabil selama penggunaan	7	0

Figure 28. *Results of Functionality Testing Using Blackbox Testing*

From the test results table of 5 customers and 2 network managers, the compiled answers show success = 6 and failure = 0. The results of the Black Box Testing indicate that the system operates as expected. Each test scenario related to the username, password, and login process, as well as bandwidth restrictions, meets the previously established expectations. This indicates that the main functions being tested in the system are working well and according to the specifications previously set.

Based on the calculation using the formula X = A/B, the result is X = 1. The condition for the calculation result is that if it approaches 1, then the product is considered appropriate and meets the requirements. It can be concluded that the security of the wireless network with hotspot login authentication at Café Lilnook Tangerang is appropriate and meets the requirements.

Academia Open
Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12146

b.Usability Test Results

The testing phase was conducted for the network managers at Café Lilnook using a questionnaire containing several indicator questions from the usability aspect of the authentication login security design for the hotspot at Café Lilnook. The results of the product testing were implemented in the questionnaire that was distributed, and the following scores were obtained:

No	Pertanyaan	SS	S	RG	TS	STS
1	Mengatasi akses bebas tanpa *login*	2	0	0	0	0
2	Mempermudah manajemen akun	2	0	0	0	0
3	Mengatasi sulit memantau penggunaan	2	0	0	0	0
4	Mengatasi *bandwidth* cepat habis	2	0	0	0	0
5	Monitoring & reporting	2	0	0	0	0

Figure 29. *Usability Test Results*

From the table on the previous page, it can be obtained that the preliminary results of the answers from the five respondents refer to very feasible. In determining the quality of the assessed product, it is necessary to use assessment categories as a reference for whether a product is feasible or not. Below is the table of assessment categories for usability aspects.

Figure 30. *Results of Likert Scale Calculations*

After performing the Likert scale calculations above and finding the total score and the highest score, the next step is to calculate the eligibility percentage of the tested product using the Interval Index (%). Based on the final results of the eligibility percentage index calculation, it can be concluded that the usability testing aspects on 2 respondents regarding the wireless network security design with hotspot login authentication at Café Lilnook Karawaci Tangerang received a result of 'very eligible' with a percentage of 100%.

7.The implementation of the management phase includes three main activities:

a.Basic knowledge training for management is conducted through a knowledge transfer session aimed at network managers or staff responsible at the site. The material covered includes steps for logging into network devices, checking connection status, procedures for restarting devices in case of disturbances, and how to report problems to the central technical team. The goal is to ensure that simple issues can be handled directly on-site without having to wait for the arrival of the

technical team, thus speeding up service recovery time.

b.The implementation of routine network system maintenance includes a schedule that covers device cleaning from dust, inspection of cable and connector conditions, firmware updates, and stability checks of connections. This maintenance is carried out periodically to keep the device performance optimal and to minimize the potential for damage or disruptions that could hinder network operations.

c.Labeling of Network Structure, all network elements, from cables, ports, devices, to racks, are given labels according to the previously designed topology structure. These labels use a uniform and easily readable code, which facilitates troubleshooting, the addition of new devices, and repairs in the future.

This research produces a design and implementation of a captive portal based hotspot login system using MikroTik RouterBoard at the Lilnook Internet Cafe in Karawaci. The Network Development Life Cycle (NDLC) model is used as the framework for system design because it has systematic stages for optimally building and managing a network. NDLC facilitates the process from needs analysis, design, simulation, implementation, to monitoring and network management. In the design and implementation of wireless network security with hotspot login authentication using MikroTik RB50UG at Café Lilnook Karawaci Tangerang, the NDLC method is applied. The initial step involves creating a flowchart of the research to obtain an overview of the conducted research.

In the early stages of this research, observations were made with the aim of obtaining the necessary data. The researcher conducted interviews with network administrators regarding the networks currently in operation. The condition of the network does not have security measures such as a password, allowing clients to connect automatically when the Wi-Fi on the client devices is active. It can be concluded that due to the lack of security measures like password usage, the large number of devices connected to the Wi-Fi network has led to internet connection failures on that network. After conducting observations, the researcher created a new network topology design with the addition of MikroTik within it, as well as analyzing the hardware and software requirements needed in the research process.

After designing the new network system, the researchers proceeded to install the hardware and software before implementation. Next, during the implementation stage, several steps were carried out, including the configuration of MikroTik, configuring the access point, setting up the authentication login page of the hotspot, and conducting initial testing. Once the implementation was completed, the monitoring phase followed as an evaluation process to ensure that the constructed hotspot network system operates according to the functional specifications and user requirements established during the design phase. The testing was conducted to assess two tests, namely functionality and usability. The functionality test score was calculated to obtain a result of X = 1. It can be concluded that the security of the wireless network with hotspot login authentication at Café Lilnook Karawaci Tangerang is feasible and functions well without any issues. Furthermore, the usability test results from the summary of respondents regarding the design of the wireless network security with hotspot login authentication at Café Lilnook Karawaci Tangerang received a result of 'very feasible' with a percentage of 100%.

Conclusion

Based on the research conducted at Café Lilnook Karawaci Tangerang, issues related to internet network access were found, specifically the lack of password protection and user restrictions, resulting in unrestricted internet access, bandwidth overload, and decline in performance. This study successfully established a wireless network using a hotspot login authentication method with Mikrotik RB50UG at Café Lilnook Karawaci Tangerang. Better access control through network configuration and hotspot login authentication has provided improved management of excessive bandwidth usage. Based on functionality assessment results, a score of 1 was obtained, concluding

that the design of the wireless network security using the hotspot login authentication method meets the criteria for use with the designation "feasible." The usability assessment resulted in an index of 100%, categorized as "very feasible."

THANK YOU

The researchers would like to thank those who have helped with this research until its completion.

References

1. S. Aji, A. Fadlil, and I. Riadi, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," J. Tek. Elektro Komput. dan Inform., vol. 4, no. 4, pp. 134–144, 2017, doi: 10.26555/jiteki.v3i1.5665.
2. M. S. Sinta, "Konsep Isolasi Dalam Jaringan Sosial Untuk Meminimalisasi Efek Contagious (Kasus Penyebaran Virus Corona di Indonesia)," J. Sosial Hukum Terap., vol. 6, no. 2, pp. 88–95, 2020, doi: 10.7454/jsht.v2i2.86.
3. M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," J. Nashihin Komputasi dan Teknol. Inform., vol. 8, no. 9, pp. 171–181, 2021, doi: 10.32672/jnkti.v4i4.3098.
4. A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik RouterOS Menggunakan Metode Port Knocking," J. Teknol. Inform., vol. 7, no. 3, pp. 222–232, 2018, doi: 10.33365/jti.v12i2.121.
5. R. N. Dasmen, M. H. Firmansyah, M. Khadafi, and T. Yolanda, "Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port," Decod. J. Pendidik. Teknol. Inform., vol. 8, no. 2, pp. 522–532, 2022, doi: 10.51454/decode.v2i1.29.
6. I. B. A. E. M. Putra, M. S. I. D. Adnyana, and L. Jasa, "Analisis Quality of Service Pada Jaringan Komputer," Maj. Ilmu Teknol. Elektronik, vol. 20, no. 1, pp. 171–181, 2021, doi: 10.24843/mite.2021.v20i01.p11.
7. J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 7th ed. Boston, MA, USA: Pearson, 2017.
8. S. F. Ahmada, F. D. Marsetyo, and R. A. Putri, "Solidaritas Pangan Jogja Sebagai Aktor Alternatif Penyedia Kesejahteraan di Masa Krisis Pandemi COVID-19," J. Soc. Dev. Stud., vol. 10, no. 2, pp. 118–128, 2020, doi: 10.22146/jsds.524.
9. G. Held, Wireless Communications. Clifton Park, NY, USA: Thomson Delmar Learning, 2005.
10. T. Jarwa and D. Suhardi, "Analisa Pembangunan dan Pemasangan Jaringan Distribusi Tegangan Menengah pada Pelanggan Premium," Semin. Keinsinyuran Progr. Studi Profesi Insinyur, vol. 2, no. 1, pp. 171–181, 2021, doi: 10.22219/skpsppi.v2i1.4357.
11. F. A. Sihombing, Teknologi Jaringan Nirkabel. Jakarta, Indonesia: Inovatif, 2021, doi: 10.32832/inova-tif.v3i2.4129.
12. T. Taufikurrahman, R. Andriani, and A. Sa’di, "Perancangan Sistem Autentikasi Wireless Hotspot Berbasis Radius Menggunakan Mikrotik," J. Inf. Syst. Manag., vol. 4, no. 2, pp. 118–128, 2023, doi: 10.24076/joism.2023v4i2.953.
13. M. Syafrizal, Pengantar Jaringan Komputer. Yogyakarta, Indonesia: Andi, 2019.
14. D. Quroturohman, "Penetration Testing Dalam Forensik Digital Pada Jaringan Fakultas Teknik Universitas Ibn Khaldun Bogor Dengan Ping of Death," INOVA-TIF, vol. 9, no. 4, pp. 229–238, 2020, doi: 10.32832/inova-tif.v3i2.4129.
15. Z. Awaldi and H. Habibullah, "Sistem Pengaman Sepeda Motor Menggunakan Aplikasi Blynk," JTEIN J. Tek. Elektro Indones., vol. 7, no. 3, pp. 222–232, 2022, doi: 10.24036/jtein.v3i1.209.
16. P. Tiar, Y. Saragih, and U. Latifa, "Analisis Quality of Service (QoS) Jaringan Wi-Fi Untuk Sistem Pendeteksi Kebocoran Gas LPG Menggunakan Wireshark," J. Telekomun. dan Komput., vol. 11, no. 2, pp. 220–230, 2021, doi: 10.22441/incomtech.v11i2.11000.
17. G. Efendi and N. K. Effendi, "Konsiliasi Pemerintah Terhadap Program Jaringan Pengaman Sosial Provinsi Jambi," J. Soc. Bridge, vol. 6, no. 2, pp. 88–95, 2023, doi: 10.59012/jsb.v1i2.7.

18. G. James, "Chapter 10: The Network Development Life Cycle," in Applied Data Communications: A Business-Oriented Approach, 4th ed. Hoboken, NJ, USA: Wiley, 2004.
19. D. Sumarni and G. Purnama, "Perancangan Infrastruktur Jaringan Komputer Berbasis Cisco Packet Tracer dengan Penerapan Metode NDLC pada Lembaga Pendidikan (Studi Kasus SMK Pelayaran Malahayati)," J. Ilm. Ilk. - Ilmu Komput. dan Inform., vol. 6, no. 2, pp. 88–95, 2019, doi: 10.47324/ilkominfo.v6i2.200.
20. A. Petandung, "Penerapan Metode NDLC (Network Development Life Cycle) Untuk Mengoptimalkan Jaringan Wireless pada SMAN 6 Luwu," J. Inf. Syst. Manag., vol. 4, no. 2, pp. 88–95, 2020, doi: 10.24076/joism.2023v4i2.953.
21. E. Sulasmi, "Evaluation of the Operational Assistance Management (BOP) Management Funding Program at the Bengkulu City PAUD Institution," Indones. J. Educ. Math. Sci. (IJEMS), vol. 1, no. 1, pp. 88–95, 2019, doi: 10.30596/ijems.v1i1.3911.