Implementation of AAA on Hotspot Network using RADIUS Server and MikroTik Router (Case Study: SMK Negeri 1 Tabanan)

Hasna Afifah[a1], **I Made Agus Dwi Suarjaya**[a2], **Gusti Made Arya Sasmita**[a3]
[a]Dept. of. Information Technology, Faculty of Engineering, Udayana University, Jimbaran, Bali, Indonesia
e-mail: [1]hasnaafifah297@gmail.com, [2]agussuarjaya@it.unud.ac.id, [3]aryasasmita@unud.ac.id

Abstrak

Perkembangan teknologi yang pesat menjadikan internet sebagai kebutuhan pokok masyarakat, termasuk di lingkungan pendidikan. Penelitian ini bertujuan untuk mengimplementasikan sistem AAA (Authentication, Authorization, Accounting) pada jaringan hotspot di SMK Negeri 1 Tabanan menggunakan RADIUS Server dan Router MikroTik. Sistem ini dilengkapi dengan DNS bersama dari APJII yang secara otomatis memblokir akses ke situs negatif saat pengguna terhubung ke jaringan sekolah. Selain itu, diterapkan fitur bandwidth dinamis, di mana bandwidth akan meningkat atau menurun sesuai kondisi trafik suatu profil pengguna. Pengembangan sistem menggunakan metode Network Development Life Cycle (NDLC), mulai dari analisis kebutuhan hingga pengujian performa dengan Apache JMeter. Hasil pengujian kualitas layanan (QoS) berdasarkan standar TIPHON menunjukkan bahwa semua kategori pengguna (Siswa, Staf, Tamu) memperoleh klasifikasi "Memuaskan", dengan indeks rata-rata antara 3.25 hingga 3.5. Sistem AAA terbukti mampu menerapkan autentikasi dan otorisasi akses, mencatat aktivitas jaringan, serta meningkatkan keamanan dan efisiensi pengelolaan jaringan hotspot sekolah melalui pemantauan berbasis web menggunakan daloRADIUS.

Kata kunci: *AAA, RADIUS Server, MikroTik, QoS, Bandwidth Dinamis*

Abstract

The rapid advancement of technology has made the internet a basic necessity for society, including within educational environments. This study aims to implement an AAA (Authentication, Authorization, Accounting) system on the hotspot network at SMK Negeri 1 Tabanan using a RADIUS Server and MikroTik Router. The system is integrated with a shared DNS service from APJII, which automatically blocks access to harmful or restricted websites when users connect to the school network. Additionally, a dynamic bandwidth feature is implemented, allowing bandwidth to increase or decrease based on the traffic conditions of each user profile. The system was developed using the Network Development Life Cycle (NDLC) method, starting from requirements analysis to performance testing using Apache JMeter. Quality of Service (QoS) testing, based on the TIPHON standard, shows that all user categories (Students, Staff, and Guests) received a "Satisfactory" classification, with average index scores ranging from 3.25 to 3.5. The AAA system has proven effective in implementing access authentication and authorization, recording user activity, and improving the security and efficiency of hotspot network management through web-based monitoring using daloRADIUS.

Keywords: *AAA, RADIUS Server, MikroTik, QoS, Dynamic Bandwidth*

1. Introduction

The rapid advancement of digital technology has made the internet a primary necessity for society, including in the field of education. Fast, stable, and secure internet access is essential to ensure that individuals can obtain information quickly, safely, and reliably. This demand for instant access to information has made internet connectivity a fundamental requirement, particularly in educational institutions such as SMK Negeri 1 Tabanan. As an institution that actively integrates information technology into its operations, SMK Negeri 1 Tabanan requires a network system capable of efficiently managing user access in a controlled manner. A common issue faced is the lack of a robust Authentication, Authorization, and Accounting (AAA) system, leading to misuse of network access, inefficient bandwidth usage, and difficulty in monitoring user activities. Therefore, a centralized and secure network management solution is needed. One effective approach is the implementation of a RADIUS server in combination with MikroTik routers, enabling optimal execution of the AAA process. As network technologies continue to evolve, the demand for reliable security systems becomes increasingly critical to protect user data. A widely adopted solution is the AAA framework, implemented through RADIUS servers and devices such as MikroTik routers.

Several relevant studies have addressed similar concerns. Audy (2022) implemented AAA in a SOHO network using NAS and Windows Server as the authentication backend. Widya et al. (2023) optimized campus hotspot networks with FreeRADIUS, allowing students to log in once across multiple hotspot zones. Sa & Andriani (2023) designed a hotspot authentication system for cafés using dual routers and temporary accounts to enhance efficiency and security.

Fauzi et al. (2020) developed a web-based user management and monitoring system using Ubuntu and RADIUS. Unfeto & Suban (2023) addressed public Wi-Fi abuse with bandwidth management via the Queue Tree method. Ruslianto et al. (2021) compared WPA2-PSK security with captive portals, revealing the latter's vulnerability to MAC address cloning without additional firewall protection.

Rahman et al. (2024) utilized a Telegram Bot for remote MikroTik monitoring. Sumiah et al. (2023) implemented VPN L2TP with RADIUS to securely connect multiple campuses. Ferdiansyah & Satria (2022) managed MikroTik hotspots using FreeRADIUS on a Debian server, along with real-time monitoring through Telegram. Finally, Zia Ul Haq et al. (2019) applied AAA with RADIUS in corporate VPN networks to enhance inter-office communication security.

These studies collectively demonstrate that AAA implementations based on RADIUS can significantly improve the security, efficiency, and monitoring capabilities of hotspot networks.

2. Research Method

This study adopts the Network Development Life Cycle (NDLC) method as an approach to design and implement a hotspot network security system based on AAA (Authentication, Authorization, Accounting) using a RADIUS server and MikroTik router. NDLC is a structured methodology that outlines the systematic life cycle of developing a computer network.

The NDLC method is chosen for its ability to facilitate the planning, development, and evaluation of networks, thereby helping researchers achieve results aligned with the research objectives. NDLC consists of six main stages, namely:

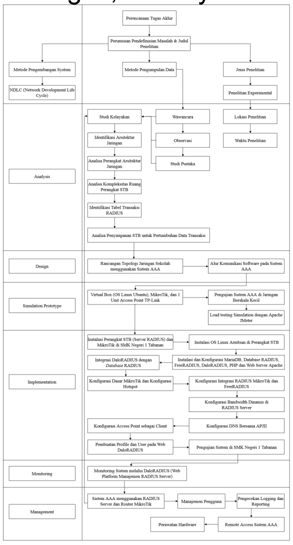

Perencanaan Tugas Akhir
Perumusan Pendefinisian Masalah & Judul Penelitian
Metode Pengembangan System
NDLC (Network Development Life Cycle)
Metode Pengumpulan Data
Jenis Penelitian
Penelitian Experimental
Analysis
Studi Kelayakan
Wawancara
Lokasi Penelitian
Identifikasi Arsitektur Jaringan
Observasi
Waktu Penelitian
Analisa Perangkat Arsitektur Jaringan
Studi Pustaka
Analisa Kompleksitas Ruang Perangkat STB
Identifikasi Tabel Transaksi RADIUS
Analisa Penyimpanan STB untuk Pertumbuhan Data Transaksi
Design
Rancangan Topologi Jaringan Sekolah menggunakan Sistem AAA
Alur Komunikasi Software pada Sistem AAA
Simulation Prototype
Virtual Box (OS Linux Ubuntu), MikroTik, dan 1 Unit Access Point TP-Link
Pengujian Sistem AAA di Jaringan Berskala Kecil
Load testing Simulation dengan Apache JMeter
Implementation
Instalasi Perangkat STB (Server RADIUS) dan MikroTik di SMK Negeri 1 Tabanan
Instalasi OS Linux Armbian di Perangkat STB
Integrasi DaloRADIUS dengan Database RADIUS
Instalasi dan Konfigurasi MariaDB, Database RADIUS, FreeRADIUS, DaloRADIUS, PHP dan Web Server Apache
Konfigurasi Dasar MikroTik dan Konfigurasi Hotspot
Konfigurasi Integrasi RADIUS MikroTik dan FreeRADIUS
Konfigurasi Bandwidth Dinamis di RADIUS Server
Konfigurasi Access Point sebagai Client
Konfigurasi DNS Bersama APJII
Pembuatan Profile dan User pada Web DaloRADIUS
Pengujian Sistem di SMK Negeri 1 Tabanan
Monitoring
Monitoring Sistem melalui DaloRADIUS (Web Platform Manajemen RADIUS Server)
Management
Sistem AAA menggunakan RADIUS Server dan Router MikroTik
Manajemen Pengguna
Pengecekan Logging dan Reporting
Perawatan Hardware
Remote Access Sistem AAA

Figure 1. Research Workflow Based on the NDLC Method

Figure 1 illustrates the hotspot network topology implemented at SMK Negeri 1 Tabanan using the AAA (Authentication, Authorization, Accounting) framework. In this topology, client devices connect to the hotspot network managed by a MikroTik router. The MikroTik router is linked to a RADIUS server, which functions as the central system for managing user authentication. Additionally, the network is connected to the internet, allowing users to access online resources after completing a valid login process. This diagram presents a structured and centralized flow of user access and authentication.

3. Literature Study

This literature review serves as the theoretical foundation for understanding the core concepts related to the implementation of authentication systems in hotspot networks, particularly through the use of the AAA framework and supporting technologies such as RADIUS Server and MikroTik Router. This study refers to a journal entitled *"Implementation of AAA in Hotspot Networks using RADIUS Server and MikroTik Router (Case Study: SMK Negeri 1 Tabanan)"*, which discusses centralized user authentication in a school network environment.

3.1 Definition of AAA (Authentication, Authorization, Accounting)

AAA is a framework in network management that consists of three primary components:

1) Authentication: The process of verifying a user's identity before granting access to the network.
2) Authorization: The process of granting specific access rights based on the authenticated user's identity.
3) Accounting: The process of recording user activities on the network, such as login time, session duration, and data usage.

3.2 Hotspot

A hotspot is a wireless access point (Wi-Fi) that enables user devices to connect to the internet. In an educational context, such as at SMK Negeri 1 Tabanan, hotspots are used to provide internet access for students and staff, which must be equipped with control systems to ensure secure and efficient usage.

3.3 RADIUS (Remote Authentication Dial-In User Service)

RADIUS is a protocol used to centrally manage the AAA process. With RADIUS, authentication, authorization, and accounting are handled by a dedicated server, allowing for more structured and secure user management.

3.4 MikroTik Router

MikroTik is a widely used network device functioning as a router, equipped with comprehensive features for network management, including hotspot configuration and RADIUS server integration. In this case study, MikroTik is used to manage hotspot connections and to connect to the RADIUS server to execute AAA functions.

3.5 NDLC (Network Development Life Cycle) Method

The Network Development Life Cycle (NDLC) is a structured and systematic methodology used to design, develop, and manage computer network systems. NDLC adopts a life-cycle-oriented approach to ensure that network development is efficient, user-oriented, and sustainable through continuous evaluation and maintenance. The NDLC consists of six main phases:

1) Analysis: Initial stage to identify network requirements and existing problems.
2) Design: Designing the network topology, hardware, software, and systems to be implemented.
3) Simulation/Prototyping: Creating a simulation or prototype of the network to test the design before actual implementation.
4) Implementation: Constructing the network according to the simulated design.
5) Monitoring: Regularly monitoring the network system to ensure it operates as expected and to detect potential issues.
6) Management: Comprehensive network management, including maintenance, system updates, and documentation to ensure continuity.

4. Result and Discussion

This research was developed using the Network Development Life Cycle (NDLC) methodology, which consists of several stages: initiation, planning, analysis, design, implementation, and maintenance. Each phase is carried out systematically to ensure that the development of the hotspot network at SMK Negeri 1 Tabanan operates optimally and meets the institution's requirements. A critical component of the implementation and evaluation phases in the NDLC method is the Quality of Service (QoS) testing, aimed at assessing the performance of the network in supporting digital learning activities and information access within the school environment. The QoS evaluation focuses on four key parameters: throughput, delay, jitter, and packet loss, which reflect the quality and stability of internet service delivery. The testing was conducted in real-world conditions during peak internet usage hours, specifically from 08:00 to 09:30 WITA and 12:00 to 13:00 WITA on weekdays (Monday to Friday). The testing methods included issuing ping commands from the server to the client and monitoring network traffic using the Simple Queue feature on the MikroTik Router. The results of these tests provide a realistic overview of the network performance following the implementation of the AAA-based system and RADIUS server configuration. The application of the NDLC methodology in this research is further elaborated in the subsequent sections.

4.1 Analysis

At this stage, data collection and requirements analysis were conducted for the hotspot network system at the research site, SMK Negeri 1 Tabanan. Several issues were identified, including the lack of user access control, vulnerability to Wi-Fi misuse, and the absence of a centralized authentication system.

4.2 Design

Following the needs analysis of the hotspot network at SMK Negeri 1 Tabanan, the next step was to design the network system to be implemented. The design aims to build a comprehensive AAA (Authentication, Authorization, Accounting) system architecture to enhance network security and usage efficiency. The design phase consists of several components, including:

4.2.1 School Network Topology

At this stage, the existing network infrastructure used by the school was mapped. The initial topology revealed the absence of a centralized authentication system and the lack of optimal bandwidth allocation.

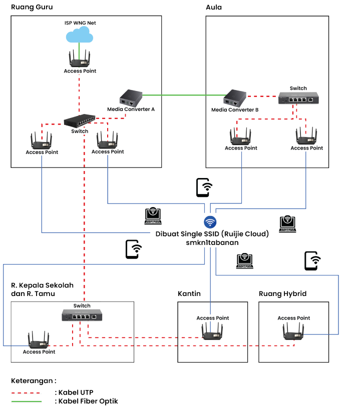


Figure 2. School Network Topology Before the Implementation of the AAA System

Figure 2 illustrates the network topology of SMK Negeri 1 Tabanan prior to the implementation of the AAA system. At that time, the hotspot network utilized a Pre-Shared Key (PSK) method with WPA/WPA2 protocols, where a single password was shared across all SSIDs. This approach allowed unauthorized users to access the network, as the password was rarely changed and often remained active for extended periods, sometimes exceeding one year. As a result, bandwidth usage became uncontrollable, and there was no differentiation in access rights between students, teachers, staff, and guests. These challenges underscored the need for implementing an AAA (Authentication, Authorization, Accounting) system to provide more secure, controlled, and role-based internet access. The subsequent section presents the proposed network topology following the AAA system implementation.

4.2.2 Proposed School Network Topology Design Using the AAA System

The design integrates a MikroTik router and a RADIUS server to establish the AAA system. The RADIUS server functions as the central authentication hub for users, while the MikroTik router manages and directs network traffic, including captive portal login and bandwidth management.

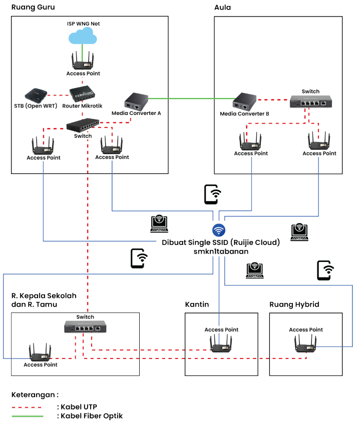


Figure 3. School Network Topology After AAA System Implementation

Figure 3 illustrates the network topology design of SMK Negeri 1 Tabanan following the implementation of the AAA system. This implementation requires only minimal additional hardware, namely a Set-Top Box (STB) to serve as the RADIUS server and a MikroTik router functioning as the Network Access Server (NAS).

4.2.3 Software Communication Flow in the AAA System

This design outlines the communication process between the client device, MikroTik router (NAS), and the RADIUS server. When a user connects to the hotspot, they are redirected to a captive portal for login. The authentication request is sent to the RADIUS server, which verifies the credentials, grants access permissions, and logs network activity.

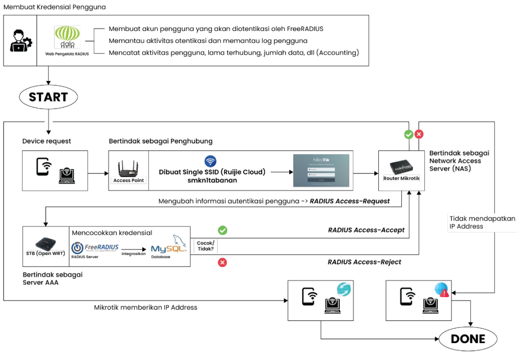

Membuat Kredensial Pengguna
Web Pengelola RADIUS
Membuat akun pengguna yang akan diotentikasi oleh FreeRADIUS
Memantau aktivitas otentikasi dan memantau log pengguna
Mencatat aktivitas pengguna, lama terhubung, jumlah data, dll (Accounting)
START
Device request
Bertindak sebagai Penghubung
Access Point
Dibuat Single SSID (Ruijie Cloud)
smkn1tabanan
Router Mikrotik
Bertindak sebagai Network Access Server (NAS)
Mengubah informasi autentikasi pengguna -> RADIUS Access-Request
Mencocokkan kredensial
STB (Open WRT)
FreeRADIUS
RADIUS Server
integrasikan
MySQL
Database
Cocok/ Tidak?
RADIUS Access-Accept
RADIUS Access-Reject
Tidak mendapatkan IP Address
Bertindak sebagai Server AAA
Mikrotik memberikan IP Address
DONE

Figure 4. Software Communication Flow in the AAA Framework System

Figure 4 illustrates the software communication flow within the AAA system implemented on the hotspot network. The process begins with the administrator creating user credentials for students, teachers, staff, and guests. When users connect to the SSID *smkn1tabanan*, they are redirected to the MikroTik captive portal for login. The login data is sent to the RADIUS server for verification. If the credentials are valid, internet access is granted; if not, an error message is displayed. All login activities are logged in FreeRADIUS or DaloRADIUS. The main difference between simulation and real implementation lies in the AAA server: the simulation uses Linux Ubuntu on VirtualBox, while the actual implementation uses a Set-Top Box (STB) running the Armbian Linux operating system.

4.3 Simulation/Prototype

This phase involves creating a simulation or prototype of the previously designed network. The simulation and initial testing are carried out in a smaller network environment, such as a home network. The purpose is to ensure that the system operates as intended before full implementation at the case study location.

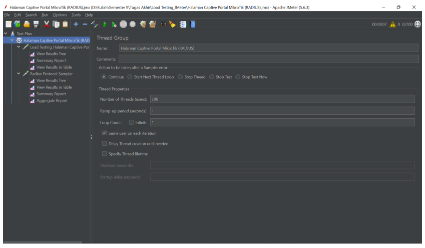
4.3.1 RADIUS Load Testing Using Apache JMeter

Load testing was conducted using Apache JMeter by simulating mass authentication requests through the captive portal, which serves as the gateway for users to access the hotspot network. The testing scenario was designed to flood the server in order to evaluate the performance and reliability of the RADIUS server under heavy load.

Table 1. Test Results Using JMeter

Test Case ID	**Actual Result**	**Status**	**Notes**
CP-001	The captive portal page displaying the login form (username and password) was successfully loaded.	Passed	-
CP-002	The user successfully logged in and obtained internet access.	Passed	*The laptop/PC device automatically redirected the user to the browser's first loaded page (captive portal). The database recorded the activity as an Access-Accept.*
CP-003	An error message "RADIUS server is not responding" was displayed, and the user remained on the login page.	Passed	This occurred because the username and password were not registered in the database. The database and DaloRADIUS logged the activity as *Access-Reject*.
CP-004	The login page was successfully loaded with an average response time of 1.032 seconds.	Passed	The more users attempting to connect simultaneously, the higher the response time will be.

Table 1 presents the results of RADIUS system testing using Apache JMeter. The table displays actual outcomes based on virtual users simulated by JMeter, which served as samplers to evaluate the system's performance. The testing process began by verifying that the DHCP Server functionality on the Network Access Server (NAS) device was operating correctly. Once a user successfully obtained a DHCP-assigned IP address from the MikroTik router, they were automatically redirected to the captive portal page (192.168.2.1) to input their credentials. The HTTP Request test was conducted with a scenario involving 700 virtual users, with a ramp-up period of 1 second.


Halaman Captive Portal MikroTik (RADIUS).jmx (D:\Kuliah\Semester 9\Tugas Akhir\Load Testing_JMeter\Halaman Captive Portal MikroTik (RADIUS).jmx) - Apache JMeter (5.6.3)

Thread Group

Name: Halaman Captive Portal MikroTik (RADIUS)

Comments:

Action to be taken after a Sampler error

● Continue ○ Start Next Thread Loop ○ Stop Thread ○ Stop Test ○ Stop Test Now

Thread Properties

Number of Threads (users): 700

Ramp-up period (seconds): 1

Loop Count: □ Infinite 1

☑ Same user on each iteration

□ Delay Thread creation until needed

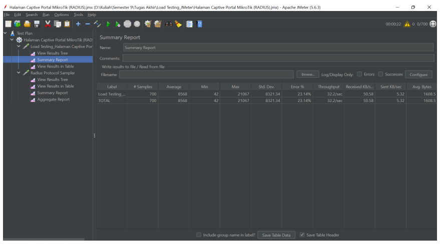
□ Specify Thread lifetime

Duration (seconds):

Startup delay (seconds):

Figure 5. HTTP Request Testing with a Scenario of 700 Users

Figure 5 above shows the configuration fields required to conduct an HTTP Request test with 700 users and a ramp-up period of 1 second. The results of this test are presented as follows.


Halaman Captive Portal MikroTik (RADIUS).jmx (D:\Kuliah\Semester 9\Tugas Akhir\Load Testing_JMeter\Halaman Captive Portal MikroTik (RADIUS).jmx) - Apache JMeter (5.6.3)

Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename Log/Display Only: □ Errors □ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/s...	Sent KB/sec	Avg. Bytes
Load Testing_...	700	8568	42	21067	8321.34	23.14%	32.2/sec	50.58	5.32	1608.5
TOTAL	700	8568	42	21067	8321.34	23.14%	32.2/sec	50.58	5.32	1608.5

□ Include group name in label? ☑ Save Table Header

Figure 6. HTTP Request Test Results with a Scenario of 700 Users

Figure 6 above shows the results of the HTTP Request test under a scenario where 700 users attempt to access the system simultaneously within 1 second. The test recorded a failure rate of 23.14%, while the remaining users successfully logged in within the same time frame. This indicates that the RADIUS server was able to handle 76.86% of the authentication requests simultaneously within 1 second.

4.4 Implementation

The implementation phase was carried out in a real-world environment, specifically within the hotspot network of SMK Negeri 1 Tabanan. This stage included the installation and configuration of the RADIUS server, MikroTik router, captive portal integration, user account setup, as well as Quality of Service (QoS) testing and joint DNS configuration in collaboration with APJII. The implementation was conducted in stages to minimize disruption during active network usage, as outlined below.

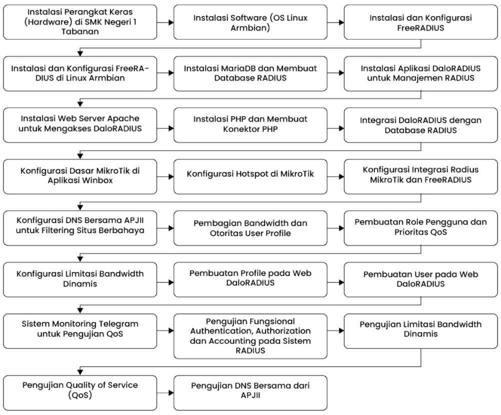

Instalasi Perangkat Keras (Hardware) di SMK Negeri 1 Tabanan
Instalasi Software (OS Linux Armbian)
Instalasi dan Konfigurasi FreeRADIUS
Instalasi dan Konfigurasi FreeRA-DIUS di Linux Armbian
Instalasi MariaDB dan Membuat Database RADIUS
Instalasi Aplikasi DaloRADIUS untuk Manajemen RADIUS
Instalasi Web Server Apache untuk Mengakses DaloRADIUS
Instalasi PHP dan Membuat Konektor PHP
Integrasi DaloRADIUS dengan Database RADIUS
Konfigurasi Dasar MikroTik di Aplikasi Winbox
Konfigurasi Hotspot di MikroTik
Konfigurasi Integrasi Radius MikroTik dan FreeRADIUS
Konfigurasi DNS Bersama APJII untuk Filtering Situs Berbahaya
Pembagian Bandwidth dan Otoritas User Profile
Pembuatan Role Pengguna dan Prioritas QoS
Konfigurasi Limitasi Bandwidth Dinamis
Pembuatan Profile pada Web DaloRADIUS
Pembuatan User pada Web DaloRADIUS
Sistem Monitoring Telegram untuk Pengujian QoS
Pengujian Fungsional Authentication, Authorization dan Accounting pada Sistem RADIUS
Pengujian Limitasi Bandwidth Dinamis
Pengujian Quality of Service (QoS)
Pengujian DNS Bersama dari APJII

Figure 7. Implementation Stages of AAA in Hotspot Network Using RADIUS Server and MikroTik Router

Figure 7 illustrates the sequential stages of implementing a network security system based on AAA (Authentication, Authorization, Accounting) using a FreeRADIUS server and MikroTik router at SMK Negeri 1 Tabanan. The implementation process consists of six main stages, as follows:

1. System Preparation Stage
   This stage involves the installation of hardware and the Linux Armbian operating system on the server. Following that, FreeRADIUS is installed and configured as the AAA server.
2. Database and Web Management Setup
   The server is equipped with MariaDB to store user data. Additionally, the DaloRADIUS application is installed as a web-based interface for user management. To access DaloRADIUS, Apache web server and PHP are used as connectors and are integrated with the RADIUS database.
3. MikroTik Configuration Stage
   MikroTik is configured starting from basic setup, hotspot creation, to integration with the FreeRADIUS server to enable external authentication.
4. Network Configuration and Bandwidth Management
   DNS filtering is configured in collaboration with APJII to block malicious websites. Bandwidth allocation is managed based on user authority levels using defined profiles and Quality of Service (QoS) prioritization.
5. User Management Stage
   In this stage, user profiles and accounts are created via the DaloRADIUS web interface. Dynamic bandwidth limitation is also applied to control network usage per user.
6. Monitoring and Testing Stage
   Testing is conducted to ensure that authentication, authorization, and accounting (AAA) functionalities operate correctly. Service quality is monitored through Telegram notifications, as well as through QoS and DNS filtering tests provided by APJII (Indonesian Internet Service Providers Association).

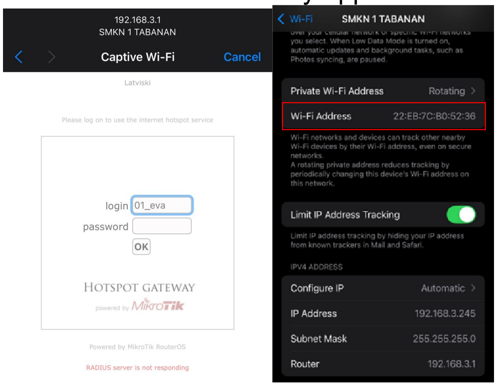
The following sections will present functionality tests of the AAA framework using the RADIUS Server, dynamic bandwidth limitation testing, QoS testing, and DNS filtering tests using APJII's joint DNS service as an additional feature for blocking harmful websites.

4.4.1 AAA Functionality and Dynamic Bandwidth Testing

The AAA functionality testing was conducted to ensure that the implementation of FreeRADIUS and MikroTik on the hotspot network at SMK Negeri 1 Tabanan operates effectively and meets the intended objectives.

1) Authentication Testing

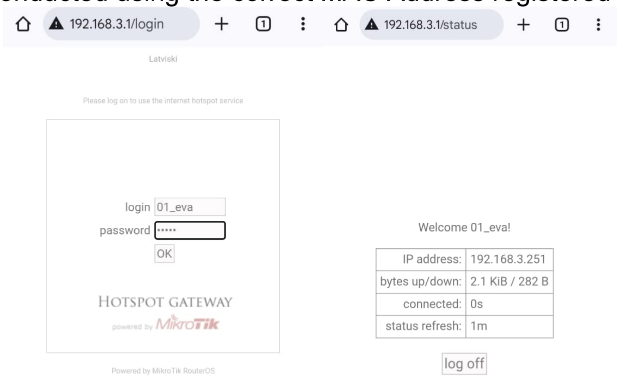
Authentication testing was performed when a device connected to the "SMKN 1 TABANAN" hotspot network and was redirected to the captive portal page. Three user profiles were created (staff, guest, and student), each with corresponding user accounts. The testing results confirmed that authentication was successfully applied for all user profiles.


192.168.3.1
SMKN 1 TABANAN
Captive Wi-Fi
Cancel
Latviski
Please log on to use the internet hotspot service
login 01_eva
password
OK
HOTSPOT GATEWAY
powered by MikroTik
Powered by MikroTik RouterOS
RADIUS server is not responding

Wi-Fi
SMKN 1 TABANAN
over your cellular network or specific Wi-Fi networks you select. When Low Data Mode is turned on, automatic updates and background tasks, such as Photos syncing, are paused.
Private Wi-Fi Address Rotating
Wi-Fi Address 22:EB:7C:B0:52:36
Wi-Fi networks and devices can track other nearby Wi-Fi devices by their Wi-Fi address, even on secure networks.
A rotating private address reduces tracking by periodically changing this device's Wi-Fi address on this network.
Limit IP Address Tracking
Limit IP address tracking by hiding your IP address from known trackers in Mail and Safari.
IPV4 ADDRESS
Configure IP Automatic
IP Address 192.168.3.245
Subnet Mask 255.255.255.0
Router 192.168.3.1

Figure 8. User Authentication via MAC Address

Figure 8 illustrates the authentication testing using the *Calling-Station-Id* attribute (MAC Address) for the account 01_eva (12:01:8B:CA:D9:A9). The authentication attempt failed because the device's MAC Address did not match the one registered in the RADIUS database. Subsequent testing was conducted using the correct MAC Address registered in daloRADIUS.


192.168.3.1/login
Latviski
Please log on to use the internet hotspot service
login 01_eva
password •••••
OK
HOTSPOT GATEWAY
powered by MikroTik
Powered by MikroTik RouterOS

192.168.3.1/status
Welcome 01_eva!

IP address:	192.168.3.251
bytes up/down:	2.1 KiB / 282 B
connected:	0s
status refresh:	1m

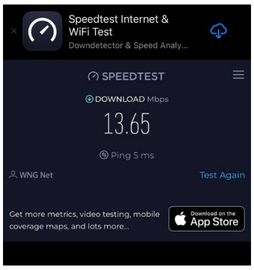
log off

Figure 9. Successful MAC Address Authentication

Figure 9 shows a successful authentication because the user device 01_eva has a MAC Address that matches the data registered in daloRADIUS. This process enhances network security by providing dual verification, in addition to the standard username and password authentication.

2) Authorization Testing

Authorization testing was conducted after users successfully logged in, during which access rights were applied according to their assigned profiles. The Mikrotik-Rate-Limit attribute was used to enforce bandwidth limitations for the student, staff, and guest profiles. Students were assigned an initial bandwidth limit of 5 Mbps (upload/download) with a maximum cap of 15 Mbps. Below is the result of the bandwidth test for the user 01_rai.



Speedtest Internet & WiFi Test

Downdetector & Speed Analy...

SPEEDTEST

DOWNLOAD Mbps

13.65

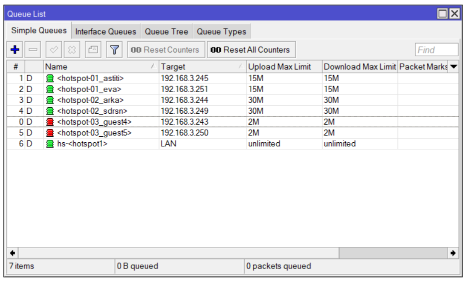
Ping 5 ms

WNG Net

Test Again

Get more metrics, video testing, mobile coverage maps, and lots more...

Figure 10 *Speed Test of Bandwidth Limitation*



Queue List

#		Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
1	D	🟩 <hotspot-01_astiti>	192.168.3.245	15M	15M	
2	D	🟩 <hotspot-01_eva>	192.168.3.251	15M	15M	
3	D	🟩 <hotspot-02_arka>	192.168.3.244	30M	30M	
4	D	🟩 <hotspot-02_sdrsn>	192.168.3.249	30M	30M	
0	D	🟥 <hotspot-03_guest4>	192.168.3.243	2M	2M	
5	D	🟥 <hotspot-03_guest5>	192.168.3.250	2M	2M	
6	D	🟩 hs-<hotspot1>	LAN	unlimited	unlimited	

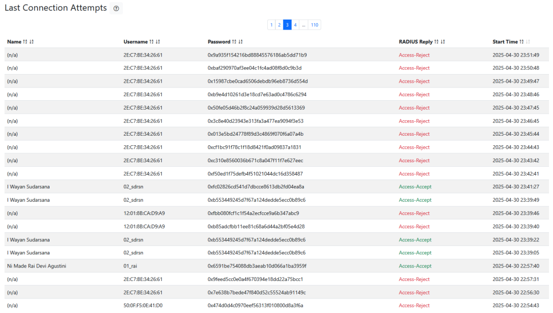
7 items | 0 B queued | 0 packets queued

Figure 11 *Queue List Menu on MikroTik*

Figure 10 shows the speed test result for user *01_rai* (student profile), with a bandwidth limitation of 5 Mbps upload/download and a maximum of 15 Mbps. During the test, the entire allocated bandwidth was utilized, as speed tests typically measure the maximum achievable bandwidth on the device. Figure 11 displays the bandwidth usage for the *Guest* profile, which nearly exceeds the initial 2 Mbps limit (≥80%), indicated by a red icon. If usage remains above 80% for 30 seconds, the data on daloRADIUS and the database is automatically updated, and the bandwidth is upgraded accordingly.

3) Accounting Testing

Accounting is a crucial part of network monitoring that records user activities from login to logout. In the RADIUS system, these records are stored in a MariaDB database and presented through the DaloRADIUS interface. This feature plays an essential role in network auditing at SMK Negeri 1 Tabanan and serves as a valuable reference for evaluating and planning future bandwidth capacity improvements. DaloRADIUS simplifies the administrator's task by providing a user-friendly graphical interface to monitor hotspot activity logs, eliminating the need to access the database directly. All RADIUS database tables can be accessed and managed through this application.



Last Connection Attempts

Name	Username	Password	RADIUS Reply	Start Time
(n/a)	2E:C7:BE:34:26:61	0x9a935f154216bd88845576186ab5dd71b9	Access-Reject	2025-04-30 23:51:49
(n/a)	2E:C7:BE:34:26:61	0xbaf290970af3ee04c1fc4ad08f8d0c9b3d	Access-Reject	2025-04-30 23:50:48
(n/a)	2E:C7:BE:34:26:61	0x15987cbe0cad6506debdb96eb8736d554d	Access-Reject	2025-04-30 23:49:47
(n/a)	2E:C7:BE:34:26:61	0xb9e4d10261d3e18cd7e63ad0c4786c6294	Access-Reject	2025-04-30 23:48:46
(n/a)	2E:C7:BE:34:26:61	0x50fe05d46b2f8c24a059939d28d5613369	Access-Reject	2025-04-30 23:47:45
(n/a)	2E:C7:BE:34:26:61	0x3c8e40d23943e313fa3a477ea9094f3e53	Access-Reject	2025-04-30 23:46:45
(n/a)	2E:C7:BE:34:26:61	0x013e5bd24778f89d3c4869f070f6a07a4b	Access-Reject	2025-04-30 23:45:44
(n/a)	2E:C7:BE:34:26:61	0xcf1bc91f78c1f18d8421f0ad09837a1831	Access-Reject	2025-04-30 23:44:43
(n/a)	2E:C7:BE:34:26:61	0xc310e8560036b671c8a047f11f7e627eec	Access-Reject	2025-04-30 23:43:42
(n/a)	2E:C7:BE:34:26:61	0xf50ed1f75defb4f51021044dc16d358487	Access-Reject	2025-04-30 23:42:41
I Wayan Sudarsana	02_sdrsn	0xfc02826cd541d7dbcce8613db2fd04ea8a	Access-Accept	2025-04-30 23:41:27
I Wayan Sudarsana	02_sdrsn	0xb553449245d7f67a124dedde5ecc0b89c6	Access-Accept	2025-04-30 23:39:49
(n/a)	12:01:8B:CA:D9:A9	0xfbb080fcf1c1f54a2ecfcce9a6b347abc9	Access-Reject	2025-04-30 23:39:46
(n/a)	12:01:8B:CA:D9:A9	0xb85adcfbb11ee81c68a6d44a2bf05e4d28	Access-Reject	2025-04-30 23:39:40
I Wayan Sudarsana	02_sdrsn	0xb553449245d7f67a124dedde5ecc0b89c6	Access-Accept	2025-04-30 23:39:22
I Wayan Sudarsana	02_sdrsn	0xb553449245d7f67a124dedde5ecc0b89c6	Access-Accept	2025-04-30 23:39:05
Ni Made Rai Devi Agustini	01_rai	0x6591be754088db3aeab10d066a1ba3959f	Access-Accept	2025-04-30 22:57:40
(n/a)	2E:C7:BE:34:26:61	0x9feed5cc0e0a4f670394e18dd22a75bcc1	Access-Reject	2025-04-30 22:57:31
(n/a)	2E:C7:BE:34:26:61	0x7e638b7bede47f840d52c55524ab91149c	Access-Reject	2025-04-30 22:56:30
(n/a)	50:0F:F5:0E:41:D0	0x474d0d4c0970eef56313f010800d8a3f6a	Access-Reject	2025-04-30 22:54:43

Figure 12. DaloRADIUS Accounting Menu

Figure 12 displays the accounting menu in DaloRADIUS, which shows both successful and failed login attempts. This feature enables administrators to identify unauthorized access attempts and monitor user activity effectively.

4.4.2 Quality of Service (QoS) Testing for the SMKN 1 Tabanan Hotspot Network

QoS testing was conducted on 30 active user accounts, consisting of 10 staff accounts, 15 student accounts, and 5 guest accounts. The parameters measured included jitter, packet loss, throughput, and delay. Data collection was carried out over a period of 10 days, specifically on May 14–16, May 19–23, and May 26–27, 2025.

Table 2. QoS Test Results Based on TIPHON Standards

Hasil Pengujian QoS				
User Category	**Parameter**	**Value**	**Index**	**Rating**
Student	Latency (ms)	21.1362833	4	Very Satisfactory
	Jitter (ms)	32.25368256	3	Satisfactory
	Packet Loss (%)	5.759337995	3	Satisfactory
	Throughput (Kbps)	1691.124412	4	Very Satisfactory
	Quality of Service		**3.5**	**Satisfactory**
Staff	Latency (ms)	19.68153275	4	Very Satisfactory

	Jitter (ms)	29.18838149	3	Satisfactory
	Packet Loss (%)	4.666136911	3	Satisfactory
	Throughput (Kbps)	1624.738849	4	Very Satisfactory
	Quality of Service		**3.5**	**Satisfactory**
Guest	Latency (ms)	22.68371992	4	Very Satisfactory
	Jitter (ms)	32.26805556	3	Satisfactory
	Packet Loss (%)	3.39702381	3	Satisfactory
	Throughput (Kbps)	819.2756508	3	Satisfactory
	Quality of Service		**3.25**	**Satisfactory**

Table 2 presents the evaluation results of network Quality of Service (QoS) at SMKN 1 Tabanan based on TIPHON standards for three user categories: students, staff, and guests. The tested parameters include latency, jitter, packet loss, and throughput. Both students and staff recorded *Very Satisfactory* ratings for latency and throughput, and *Satisfactory* ratings for jitter and packet loss. Guest users showed *Very Satisfactory* performance in latency and *Satisfactory* in the remaining three parameters. The average QoS index was 3.5 for students and staff, and 3.25 for guests. These results indicate that overall network service quality falls within the *Satisfactory* category, and that the AAA system based on RADIUS has successfully enhanced both network security and bandwidth allocation efficiency.

The following section presents the percentage-based criteria used to evaluate network Quality of Service (QoS).

Table 3 Percentage of QoS Parameters

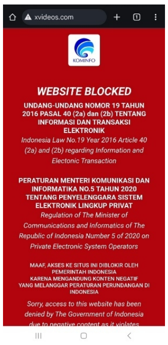
Score Range	Percentage (%)	Rating Category
3,8 – 4	95 – 100	Very Satisfactory
3 – 3,79	75 – 94,75	Satisfactory
2 – 2,99	50 – 74,75	Fair
1 – 1,99	25 – 49,75	Poor

Source: TIPHON

Table 3 presents the Quality of Service (QoS) assessment results based on four key parameters: throughput, delay, jitter, and packet loss, referring to the TIPHON standard from ETSI. This standard is used to evaluate network service quality to ensure it meets the expected performance criteria.

4.4.3 Testing of APJII Shared DNS Implementation

This test presents the results of implementing the "DNS Bersama" (Shared DNS) developed by APJII and the Indonesian Ministry of Communication and Information Technology (Kominfo) on the MikroTik router. This DNS configuration is designed to block access to restricted or blacklisted websites. With this setup, all users connected to the hotspot network are automatically filtered and prevented from accessing any websites listed in the national blocklist.



WEBSITE BLOCKED

UNDANG-UNDANG NOMOR 19 TAHUN 2016 PASAL 40 (2a) dan (2b) TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Indonesia Law No.19 Year 2016 Article 40 (2a) and (2b) regarding Information and Electonic Transaction

PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA NO.5 TAHUN 2020 TENTANG PENYELENGGARA SISTEM ELEKTRONIK LINGKUP PRIVAT

Regulation of The Minister of Communications and Informatics of The Republic of Indonesia Number 5 of 2020 on Private Electronic System Operators

MAAF, AKSES KE SITUS INI DIBLOKIR OLEH PEMERINTAH INDONESIA
KARENA MENGANDUNG KONTEN NEGATIF YANG MELANGGAR PERATURAN PERUNDANGAN DI INDONESIA

Sorry, access to this website has been denied by The Government of Indonesia due to negative content as it violates

Figure 8. Testing of Shared DNS from APJII and Kominfo

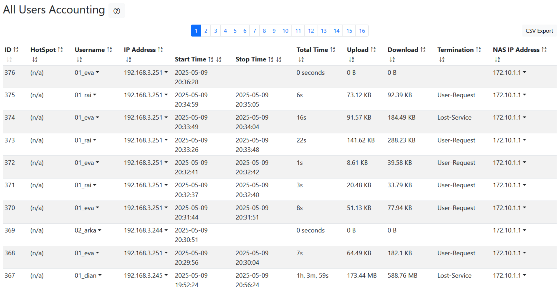
Figure 8 illustrates the result of testing the Shared DNS provided by APJII and Kominfo, which supports the “Internet Sehat” (Safe Internet) initiative. The test confirms that access to restricted websites is successfully blocked when users are connected to the hotspot network.

4.5 Monitoring

After the AAA system was implemented, a monitoring phase was carried out to ensure the functionality and stability of the network. Monitoring focused on two main areas:

1. **User Activity Monitoring**

User activity is monitored through the DaloRADIUS interface on the accounting page. Recorded information includes login history, bandwidth usage, connection duration, and user authentication status. This data assists network administrators in evaluating the effectiveness of access management and optimizing network resource allocation.



All Users Accounting

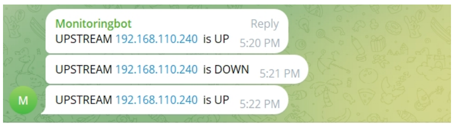
ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload	Download	Termination	NAS IP Address
376	(n/a)	01_eva	192.168.3.251	2025-05-09 20:36:28		0 seconds	0 B	0 B		172.10.1.1
375	(n/a)	01_rai	192.168.3.251	2025-05-09 20:34:59	2025-05-09 20:35:05	6s	73.12 KB	92.39 KB	User-Request	172.10.1.1
374	(n/a)	01_eva	192.168.3.251	2025-05-09 20:33:49	2025-05-09 20:34:04	16s	91.57 KB	184.49 KB	Lost-Service	172.10.1.1
373	(n/a)	01_rai	192.168.3.251	2025-05-09 20:33:26	2025-05-09 20:33:48	22s	141.62 KB	288.23 KB	User-Request	172.10.1.1
372	(n/a)	01_eva	192.168.3.251	2025-05-09 20:32:41	2025-05-09 20:32:42	1s	8.61 KB	39.58 KB	User-Request	172.10.1.1
371	(n/a)	01_rai	192.168.3.251	2025-05-09 20:32:37	2025-05-09 20:32:40	3s	20.48 KB	33.79 KB	User-Request	172.10.1.1
370	(n/a)	01_eva	192.168.3.251	2025-05-09 20:31:44	2025-05-09 20:31:51	8s	51.13 KB	77.94 KB	User-Request	172.10.1.1
369	(n/a)	02_arka	192.168.3.244	2025-05-09 20:30:51		0 seconds	0 B	0 B		172.10.1.1
368	(n/a)	01_eva	192.168.3.251	2025-05-09 20:29:56	2025-05-09 20:30:04	7s	64.49 KB	182.1 KB	User-Request	172.10.1.1
367	(n/a)	01_dian	192.168.3.245	2025-05-09 19:52:24	2025-05-09 20:56:24	1h, 3m, 59s	173.44 MB	588.76 MB	Lost-Service	172.10.1.1

Figure 8. Accounting Feature in the DaloRADIUS Web Interface

Figure 8 shows the accounting menu in DaloRADIUS, which logs all user network activity by displaying data from the radacct table. The "termination" column indicates how each session ended. This accounting data helps enhance network security and serves as a reference for evaluating and planning future bandwidth capacity at SMK Negeri 1 Tabanan. DaloRADIUS also supports additional administrative features for analysis and reporting.

2. **System and Device Status Monitoring**

To monitor network availability and device health, a Telegram-based notification system is used. This mechanism detects the status of the gateway connected to the ISP. If the gateway goes down, the system automatically sends a Telegram alert, allowing the administrator to respond promptly.



UPSTREAM 192.168.110.240 is UP 5:20 PM

UPSTREAM 192.168.110.240 is DOWN 5:21 PM

UPSTREAM 192.168.110.240 is UP 5:22 PM

Figure 8. Upstream Status Monitoring via Telegram

This real-time monitoring system ensures optimal network performance, proper user authentication, and early detection of potential issues.

4.6 Management

The final stage involves evaluating the implementation outcomes, managing user accounts, updating configurations when necessary, and compiling technical documentation. This phase also assesses whether the implemented system has met the research objectives and provides tangible benefits for network management at the school.

5. Conclusion

The following are the conclusions drawn from the implementation of the AAA (Authentication, Authorization, and Accounting) framework using a RADIUS Server and MikroTik router on the hotspot network at SMK Negeri 1 Tabanan:

1. The implementation of AAA using FreeRADIUS and MikroTik successfully addressed issues of unstable and uneven bandwidth usage by centralizing network management. The system enhances security through user authentication, prevents unauthorized access, and simplifies user account management via the DaloRADIUS web interface. Users benefit from a single sign-on experience, with session control tailored to each user profile.
2. From the accounting perspective, the system provides detailed usage logs, including bandwidth consumption and session duration, which support future resource planning. Testing on a small-scale network confirmed that the AAA system effectively performs authentication, authorization, and accounting, proving its reliability and functionality in real-world scenarios.

References

[1] Audy, M. F. (2022). *Penerapan Authentication, Authorization, and Accounting untuk Pengamanan Jaringan Small Office/Home Office* (Vol. 6, Issue 1). http://j-ptiik.ub.ac.id

[2] Eben, E., Mukramin, M., & Abduh, H. (2024). PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.4716

[3] Fauzi, A., Dedy Irawan, J., & Vendyansyah, N. (2020). RANCANG BANGUN SISTEM MANAJEMEN USER AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING) DAN MONITORING JARINGAN HOTSPOT BERBASIS WEB. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 4, Issue 1).

[4] Ferdiansyah, P., & Adi Satria, D. (2022). Manajemen Hotspot Mikrotik Menggunakan FreeRadius dan Sistem Monitoring. *Volume*, *5*, 153–160. https://ojs.trigunadharma.ac.id/index.php/jsk/index

[5] Haq, M. Z. U., Timur, T. W., & Rahmadi, Y. (2019). *IMPLEMENTASI AAA MENGGUNAKAN RADIUS SEVER PADA JARINGAN VPN (STUDY KASUS PT. FORUM AGRO SUKSES TIMUR)*.

[6] Gulo, E., & Ferdiansyah, I. (2024). *PENGUJIAN PERFORMA APLIKASI E-COMMERCE MENINGKATKAN SKALABILITAS DAN RESPONSIVITAS MENGGUNAKAN JMETER*. *3*.

[7] Lestari, M., Haryani, E., & Wahyono, T. (2021). Analisis Kelayakan Sistem Informasi Akademik Universitas Menggunakan PIECES dan TELOS. *Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(2). https://doi.org/10.28932/jutisi.v7i2.3612

[8] Army, W. L., Ilham, W., & Syafrinal, I. (2023). *OTENTIKASI PENGGUNA SECARA TERPUSAT MENGGUNAKAN FREERADIUS DALAM UPAYA MENGOPTIMALKAN JARINGAN HOTSPOT PADA KAMPUS UPI "YPTK" PADANG*. *13*.

[9] Pradita, G., & Pramono, A. (2024). IMPLEMENTASI MONITORING KEAMANAN JARINGAN PADA SERVER UBUNTU MENGGUNAKAN SNORT INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DAN TELEGRAM BOT SEBAGAI MEDIA NOTIFIKASI DI PT SS UTAMA. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 4).

[10] Rahman, T., Nibras, I. Z., & Sumarna, S. (2024). MONITORING ADMINSTRASI JARINGAN DENGAN MIKROTIK DAN TELEGRAM BOT PADA INTERNET SERVICE PROVIDER. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *9*(2), 162–172. https://doi.org/10.36341/rabit.v9i2.4736

[11] Ruslianto, I., Hidayati, R., Rekayasa Sistem Komputer, J., & Hadari Nawawi, J. H. (2021). ANALISIS PERBANDINGAN SISTEM KEAMANAN JARINGAN WI-FI PROTECTED ACCESS 2-PRE SHARED KEY (WPA2-PSK) DAN CAPTIVE PORTAL PADA JARINGAN PUBLIK WIRELESS. In *Coding : Jurnal Komputer dan Aplikasi* (Vol. 09, Issue 01).

[12] Sa, A., & Andriani, R. (2023). PERANCANGAN SISTEM AUTENTIKASI WIRELLESS HOTSPOT BERBASIS RADIUS MENGGUNAKAN MIKROTIK. In *Journal of Information System Management (JOISM) e-ISSN* (Vol. 4, Issue 2).

[13] Sumiah, A., Nugraha, F., & Permana, A. (2023). *PENERAPAN TEKNOLOGI VPN L2TP DAN PROTOKOL AAA RADIUS PADA JARINGAN HOTSPOT* (Vol. 17, Issue 2). https://journal.fkom.uniku.ac.id/ilkom

[14] Dubois, X., Petrov, V., & Anugrah, R. W. (2024). *TRANSFORMASI SOSIAL PERUBAHAN KEHIDUPAN MASYARAKAT MELALUI PENYEBARAN JARINGAN KOMPUTER*. *4*.

[15] Unfeto, M. R., & Suban Belutowe, Y. (2023). IMPLEMENTASI RADIUS SERVER PADA JARINGAN HOTSPOT MENGGUNAKAN MIKROTIK. *Jurnal Teknologi Informasi*, *7*(1).

[16] Yoga, V., Ardhana, P., & Dermawan Mulyodiputro, M. (2024). *Pelatihan Teknologi Jaringan Komputer Bagi Pelajar Tingkat SMP di Kota Mataram*. https://doi.org/10.57119/abdimas.v3i1.112