Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

OPTIMASI PENGGUNAAN *BANDWIDTH* DAN KEAMANAN JARINGAN *WI-FI* DI PULUHDADI *RESIDENCE* MENGGUNAKAN MIKROTIK

Optimizing Bandwidth Usage and Wi-Fi Network Security in Puluhdadi Residence Using MikroTik

Kevin Chandra Christanto[1], Yudi Sutanto[2]
[1,2] Informatika, Universitas Amikom Yogyakarta
Email : [1]kevinchandra@students.amikom.ac.id, [2]yudisuta@amikom.ac.id

ABSTRACT

Puluhdadi Residence provides Wi-Fi service facilities with a speed of 50 Mbps which is sufficient to accommodate the needs of residents in working and accessing entertainment. However, because bandwidth management has not been implemented optimally, it has the opportunity to cause misuse or excessive use by some users, causing disruption of fair bandwidth distribution. Furthermore, the security aspect of Wi-Fi networks is also an important concern in the area. This research aims to address these issues through bandwidth management, client isolation, access regulation based on MAC Address, and authentication using captive portal with MikroTik device. The methods used include bandwidth management for more even internet distribution, increased privacy through user isolation, access restriction with MAC Address filters, and access control using captive portals. Based on the results of the study, it was found that the implementation of bandwidth management with MikroTik hAP lite RB941-2nD devices was effective in distributing bandwidth evenly, with stable network performance approaching the allocation of 10 Mbps per user. Isolation efforts between users succeeded in improving the level of privacy and security of the network, while the captive portal was successful in authenticating identities and restricting access to the Wi-Fi network for registered users. This research contributes to creating a more secure and efficient Wi-Fi network, and can be utilised by network managers in similar environments. Further research can be conducted to test the effectiveness of the applied methods in the long run as well as on a larger scale.

Keywords : bandwidth management, captive portal, client isolation, MAC Address, MikroTik.

ABSTRAK

Puluhdadi *Residence* memberikan fasilitas layanan *Wi-Fi* dengan kecepatan 50 *Mbps* yang memadai untuk mengakomodasi kebutuhan penghuni dalam bekerja maupun mengakses hiburan. Akan tetapi dikarenakan belum diterapkannya pengelolaan *bandwidth* secara optimal berpeluang menyebabkan penyalahgunaan atau penggunaan berlebihan oleh sebagian pengguna, sehingga menyebabkan gangguan distribusi *bandwidth* yang adil. Lebih lanjut, aspek keamanan jaringan *Wi-Fi* juga menjadi perhatian penting di *area* tersebut. Penelitian ini bertujuan untuk menangani permasalahan tersebut melalui pengaturan alokasi *bandwidth* (*bandwidth management*), penyekatan atau isolasi antar pengguna (*client isolation*), regulasi akses berdasarkan *MAC Address*, serta autentikasi menggunakan *captive portal* dengan perangkat MikroTik. Metode yang digunakan meliputi pengaturan *bandwidth* agar distribusi internet lebih merata, peningkatan privasi melalui isolasi pengguna, pembatasan akses dengan *filter MAC Address*, dan kontrol akses menggunakan *captive portal*. Berdasarkan hasil penelitian, ditemukan bahwa penerapan manajemen *bandwidth* dengan perangkat MikroTik *hAP lite RB941-2nD* efektif dalam mendistribusikan *bandwidth* secara merata, dengan kinerja jaringan stabil mendekati alokasi 10 *Mbps* per pengguna. Upaya isolasi antar pengguna berhasil memperbaiki tingkat privasi dan keamanan jaringan, sementara *captive portal* berhasil dalam mengautentikasi identitas dan membatasi akses ke jaringan *Wi-Fi* bagi pengguna yang terdaftar. Penelitian ini memberikan kontribusi dalam menciptakan jaringan *Wi-Fi* yang lebih aman dan efisien, dan dapat dimanfaatkan oleh pengelola jaringan di lingkungan yang serupa. Penelitian lebih lanjut dapat dilakukan untuk menguji efektivitas metode yang diterapkan dalam jangka panjang serta pada skala yang lebih besar.

Kata kunci: manajemen *bandwitdh*, *captive portal*, *client isolation*, *MAC Address*, MikroTik.

I. PENDAHULUAN

Di era digital saat ini, kebutuhan akan jaringan *internet* yang cepat dan aman menjadi faktor penting bagi penghuni rumah kos, termasuk di Puluhdadi *Residence*. Rumah kos umumnya dihuni oleh mahasiswa, pekerja, dan individu lain yang

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

mengandalkan *internet* untuk berbagai aktivitas, seperti belajar, bekerja jarak jauh, serta mengakses hiburan. Di Puluhdadi *Residence* terpasang jaringan *Wi-Fi* dengan kecepatan 50 *Mbps*. Koneksi yang tersedia sudah mampu memenuhi kebutuhan penggunanya, baik untuk keperluan pekerjaan maupun hiburan.

Namun pengelolaan penggunaan *bandwidth* yang optimal masih belum diterapkan secara maksimal. Akibatnya, potensi penyalahgunaan atau pemakaian berlebihan oleh beberapa pengguna dapat mempengaruhi distribusi *bandwidth* secara adil bagi semua pengguna. Selain itu, keamanan jaringan *Wi-Fi* di lingkungan kos juga menjadi perhatian penting.

Beberapa studi sebelumnya telah mencoba mengatasi masalah serupa dengan menerapkan manajemen *bandwidth* menggunakan fitur dasar MikroTik, seperti *Simple Queue.* Misalnya, Suharyanto dkk. [1] dan Afandi [2] hanya menggunakan *Simple Queue* tanpa autentikasi pengguna maupun pembagian *bandwidth* berbasis jenis perangkat atau prioritas. Pendekatan ini bersifat statis dan kurang adil karena pengguna dengan aktivitas tinggi tetap dapat menyerap lebih banyak *bandwidth*. Selain itu, tidak adanya kontrol akses berbasis *MAC Address* maupun isolasi klien menyebabkan jaringan tetap rentan terhadap penyalahgunaan. Penelitian oleh Hakim dkk. [3] menggunakan *Queue Tree*, namun belum mengintegrasikan fitur keamanan seperti *Captive Portal* dan *Client Isolation*, sehingga hasilnya belum maksimal dalam menciptakan jaringan yang efisien dan aman.

Seiring dengan perkembangan teknologi, semakin banyak perangkat yang terhubung ke jaringan nirkabel, sehingga meningkatkan risiko terhadap keamanan jaringan. Jaringan yang tidak di lengkapi dengan pengaman yang memadai rentan terhadap ancaman seperti penyusupan dan pencurian data. Oleh karena itu, upaya penguatan keamanan jaringan perlu dilakukan, termasuk penerapan isolasi antar pengguna, pembatasan akses berdasarkan *MAC Address*, dan otentikasi melalui *captive portal*.

Beberapa metode pengelolaan *bandwidth* yang umum digunakan di lingkungan kos atau kantor kecil biasanya hanya menggunakan pengaturan sederhana, seperti *Simple Queue* tanpa kontrol tambahan, atau pembatasan *bandwidth* berbasis *IP Address* statis. Pendekatan ini mudah diterapkan, namun tidak memberikan pengelolaan yang adil karena pengguna dengan aktivitas tinggi tetap bisa mengonsumsi *bandwidth* lebih besar. Selain itu, tidak adanya isolasi pengguna dan kontrol autentikasi menyebabkan ketidakamanan jaringan dan pemborosan sumber daya. Oleh karena itu, penelitian ini menggabungkan berbagai fitur pada MikroTik seperti *Queue Tree*, *Client Isolation*, dan *Captive Portal* untuk menciptakan pendekatan yang lebih terkontrol dan adil, khususnya dalam lingkungan dengan pengguna yang heterogen seperti rumah kos.

Penelitian ini bertujuan untuk mengoptimalkan penggunaan *bandwidth* dan mengningkatkan keamanan jaringan *Wi-Fi* di Puluhdadi *Residence* melalui pemanfaatan perangkat MikroTik. Kebaruan dari penelitian ini terletak pada penerapan kombinasi MikroTik (*Simple Queue, Queue Tree, Captive Portal, Client Isolation,* dan *Mac Filtering*) di lingkungan kos yang memiliki keterbatasan sumber daya dan kebutuhan pengguna yang beragam. Penelitian ini memberikan kontribusi praktis terhadap pengelolaan jaringan di lingkungan skala kecil dengan pendekatan yang efisien dan dapat diimplementasikan oleh pengguna jaringan non-teknis sekalipun.

II. LANDASAN TEORI

A. Manajemen *Bandwidth*

Bandwidth adalah kapasitas maksimum jalur komunikasi untuk mentransfer data dalam suatu jaringan dalam satuan waktu tertentu, biasanya diukur dalam *bit per second (bps)*. Menurut Stallings (2007), *bandwidth* menggambarkan "jumlah data maksimum yang dapat ditransmisikan melalui jalur jaringan tertentu dalam satuan waktu tertentu" [4]. Manajemen *bandwidth* adalah proses pengalokasian dan pengaturan penggunaan *bandwidth* jaringan agar berjalan optimal dan efisien. Menurut Forouzan (2007), "manajemen *bandwidth* melibatkan pengaturan lalu lintas jaringan dengan cara memprioritaskan, membatasi, atau menjadwalkan aliran data agar dapat memenuhi kebutuhan layanan secara adil dan efektif" [5]. Liu et al. (2024) menyebutkan bahwa pendekatan adaptif berbasis perilaku pengguna lebih efisien dalam menjaga kualitas layanan (QoS) pada jaringan padat [6]. MikroTik menyediakan berbagai metode untuk manajemen *bandwidth*, termasuk *Queue Tree* dan *Simple Queue*.

Queue Tree adalah teknik pengelolaan *bandwidth* yang memungkinkan pembagian *bandwidth* secara hierarkis berdasarkan pengelompokan kelas. Pada

MikroTik, *Queue Tree* bekerja dengan membuat pembagian atau pengantrian paket berdasarkan *packet marks* yang ditentukan, sehingga alokasi *bandwidth* dapat diatur sesuai dengan kelas pengguna [3].

Simple Queue adalah metode yang lebih sederhana dibandingkan *Queue Tree*, tetapi efektif untuk mengalokasikan *bandwidth* secara langsung ke tiap pengguna atau perangkat. Dengan *Simple Queue*, admin jaringan dapat mengatur batas maksimum *bandwidth* untuk setiap perangkat, sehingga distribusi *bandwidth* menjadi lebih adil [1], [2].

Beberapa metode lain adalah *Hierarchical Token Bucket (HTB), Burst,* dan *Perconnection Queue (PCQ)*. *HTB* memungkinkan pembagian *bandwidth* secara hierarkis dan dapat digunakan bersama *Queue Tree* untuk pembagian kompleks. *Burst* digunakan untuk memberikan *bandwidth* lebih tinggi dalam waktu singkat, namun dapat menyebabkan ketidakstabilan jika digunakan tanpa batas. *PCQ* ideal untuk distribusi *bandwitdh* otomatis antar klien, namun memerlukan konfigurasi lebih kompleks. Dalam penelitian ini, *Simple Queue* dan *Queue Tree* dipilih karena kemudahan implementasi dan kontrol granular yang cocok untuk skala rumah kos.

B. Keamanan Jaringan

Keamanan jaringan (*network security*) adalah praktik untuk melindungi jaringan komputer serta data yang mengalir di dalamnya dari berbagai ancaman, seperti akses tidak sah, penyalahgunaan, gangguan, modifikasi, atau perusakan data. Menurut Stallings (2012), "keamanan jaringan mencakup ketentuan dan kebijakan yang diterapkan oleh *administrator* jaringan untuk mencegah dan memantau akses tidak sah, penyalahgunaan, modifikasi, atau penolakan jaringan komputer" [7]. MikroTik menawarkan beberapa fitur keamanan jaringan, termasuk *MAC Address Filtering, Client Isolation,* dan *Captive Portal* untuk autentikasi.

MAC Address Filtering adalah teknik yang digunakan untuk mengendalikan akses ke jaringan berdasarkan alamat fisik *(MAC Address)* perangkat yang terhubung. Dengan metode ini, hanya perangkat yang *MAC Address*-nya telah terdaftar di sistem yang dapat mengakses jaringan [8].

Captive Portal adalah metode autentikasi yang memaksa pengguna untuk melakukan login terlebih dahulu sebelum dapat mengakses jaringan. Pada jaringan yang menggunakan *Captive Portal*, pengguna diarahkan ke halaman *login* di mana mereka harus memasukkan kredensial yang *valid*. Metode ini memastikan bahwa hanya pengguna yang sah yang dapat mengakses jaringan, meningkatkan keamanan sekaligus menghindari penggunaan yang tidak sah [9], [10].

Client Isolation adalah fitur keamanan yang membatasi interaksi langsung antar perangkat dalam jaringan yang sama, sehingga perangkat yang terhubung ke jaringan hanya dapat berkomunikasi dengan *router* atau *accest poin (AP)* dan tidak dengan perangkat lain di jaringan yang sama. Hal ini mencegah risiko serangan seperti *man-in-the-middle* dan meminimalkan akses ilegal antar perangkat dalam lingkungan ramai. Menurut studi Liu et al. (2024), *client isolation* efektif untuk meningkatkan keamanan jaringan di lingkungan publik atau residensial dengan banyak pengguna [3].

Penelitian Liu et al. (2024) menunjukkan bahwa *Client Isolation* secara signifikan mengurangi risiko serangan ARP spoofing pada jaringan publik [3]. Penelitian oleh Zhang et al. (2022) juga menyoroti tantangan pada *Captive Portal*, termasuk potensi *bypass* melalui spoofing *MAC Address* dan pentingnya integrasi dengan autentikasi dua faktor (2FA) pada jaringan publik [11].

C. MikroTik sebagai Perangkat Manajemen Jaringan

MikroTik adalah perangkat jaringan yang populer untuk manajemen *bandwidth* dan keamanan, terutama di lingkungan skala kecil hingga menengah. Dalam penelitian ini, MikroTik *hAP lite RB941-2nD* digunakan karena kemampuannya dalam mengatur distribusi *bandwidth* secara efisien dan meningkatkan keamanan jaringan. Studi oleh Hendri Adi dkk. (2022) menunjukkan bahwa perangkat ini memungkinkan pembagian *rate limit* yang adil serta pembatasan akses menggunakan *username* dan *password*, sehingga memastikan stabilitas dan keamanan jaringan bagi setiap pengguna [12], [13].

D. Perbandingan MikroTik dengan Solusi Alternatif

MikroTik merupakan pilihan populer di jaringan skala kecil ke menengah karena efisiensi biaya dan fleksibilitas konfigurasinya. Namun, MikroTik memerlukan konfigurasi manual dan tidak menawarkan visualisasi lalu lintas secara *real-time* seperti yang dimiliki oleh sistem *cloud-based management* milik Cisco Meraki atau Unifi Controller dari Ubiquiti. Cisco Meraki mendukung kontrol terpusat *multi-site* dan *dashboard* visual berbasis *web*, namun dengan biaya lisensi tinggi. Unifi

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

menyediakan *Captive Portal* dengan tampilan antarmuka ramah pengguna, namun memerlukan perangkat keras khusus. Berbeda dengan itu, MikroTik memungkinkan implementasi fitur seperti *Queue Tree, Client Isolation,* dan *Mac Filtering* secara modular di perangkat murah. Pendekatan ini cocok untuk resedensial, namun kurang skalabel untuk jaringan besar.

III. METODE PENELITIAN

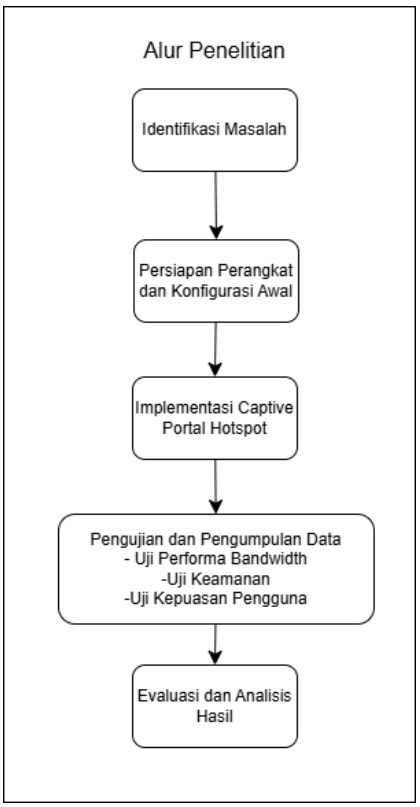
Penelitian ini termasuk dalam kategori studi kasus rekayasa teknis, yang bertujuan untuk mengevaluasi efektifitas penerapan teknologi dalam konteks nyata. Variabel bebas dalam penelitian ini meliputi metode manajemen *bandwidth (Simple Queue, Queue Tree)*, *Client Isolation*, dan *Captive Portal*. Variabel terikat adalah performa jaringan dan tingkat kepuasan pengguna.

A. Objek Penelitian

Jaringan *Wi-Fi* di Puluhdadi *Residence*, sebagai objek penelitian, adalah jaringan *Wi-Fi* yang terpasang di rumah kos Puluhdadi *Residence* yang menyediakan akses jaringan *Wi-Fi* bagi penghuni, dengan target pengguna utama mahasiswa, pekerja, dan individu lainnya. Jaringan yang tersedia menggunakan *bandwidth* sebesar 50 *Mbps* yang disediakan oleh *ISP* Biznet. Penelitian ini bertujuan mengoptimalkan penggunaan *bandwidth* dan meningkatkan keamanan jaringan *Wi-Fi* di lingkungan ini menggunakan perangkat MikroTik *hAP lite RB941-2nD*.

Jumlah pengguna yang terlibat dalam penelitian ini adalah 5 orang penghuni yang secara aktif menggunakan jaringan *Wi-Fi*. Hasil survei yang dilakukan menunjukkan bahwa pada saat akses ramai (lebih dari 3 pengguna mengakses internet secara bersama), 60% dari pengguna melaporkan bahwa koneksi *internet* mereka mengalami penurunan kecepatan (melambat), sementara 40% lainnya menjawab bahwa kecepatan internet mereka tetap terjaga. Sebaliknya, saat kondisi akses tidak ramai, 100% dari pengguna menjawab bahwa koneksi *internet* tetap *stabil* dan terjaga dengan baik.

B. Alur Penelitian



Gambar 1. Alur penelitian.

Tahapan-tahapan dalam alur penelitian adalah sebagai berikut:

1. Identifikasi Masalah

Mengidentifikasi permasalahan utama pada jaringan *Wi-Fi* di Puluhdadi *Residence*, seperti distribusi *bandwidth* yang tidak merata dan potensi akses ilegal dan mengumpulkan data awal tentang penggunaan *bandwidth*, jumlah pengguna, dan kondisi keamanan jaringan sebelum optimasi.

2. Persiapan Perangkat dan Konfigurasi Awal

Menyiapkan perangkat MikroTik *hAP lite RB941-2nD* dan melakukan konfigurasi awal jaringan dan mengatur pengaturan dasar *Captive Portal* untuk *hotspot* agar siap untuk implementasi fitur manajemen *bandwidth* dan keamanan.

3. Implementasi *Captive Portal*

Membuat konfigurasi *captive portal* untuk autentikasi pengguna sebelum pengguna dapat mengakses jaringan *Wi-Fi*. Hal ini memastikan hanya pengguna yang terverifikasi yang dapat terhubung.

Pembatasan berdasarkan *MAC Address* mengaktifkan penyaringan *MAC Address* untuk mencegah perangkat yang tidak terdaftar dari mengakses jarigan melalui *captive portal.*

Isolasi klien (*client isolation)* dengan mengaktifkan isolasi antar pengguna untuk

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

meningkatkan privasi dan keamanan jaringan dengan mencegah perangkat pengguna lain berinteraksi di dalam jaringan.

Menggunakan *queue tree* untuk membagi *bandwidth* secara hierarki berdasarkan kelompok atau prioritas pengguna dan mengatur *simple queue* untuk alokasi *bandwidth* individu pengguna atau perangkat, memastikan distribusi.

4. Pengujian dan Pengumpulan Data

Data dikumpulkan untuk mengukur kinerja dan keamanan jaringan *Wi-Fi* di Puluhdadi *Residence*. Pengujian dilakukan melalui tiga tahapan utama yaitu, uji performa *bandwidth*, uji keamanan, dan uji kepuasan pengguna.

Uji performa *bandwitdh* dengan tujuan mengukur kecepatan unduh *(download)* dan kecepatan unggah *(upload)* jaringan *internet* yang ada pada kondisi akses ramai (5 pengguna mengakses *internet* secara bersamaan) dan tidak ramai (kurang dari 3 pengguna mengakses *internet* secara bersama) dan menggunakan aplikasi pengujian kecepatan seperti *Speedtest* untuk mengukur performa *bandwidth* baik pada perangkat *laptop* maupun *smartphone*.

Skema pengujian akses tidak ramai adalah pengujian dilakukan ketika pengguna yang mengakses jaringan *Wi-Fi* kurang dari sama dengan 3 pengguna, baik menggunakan perangkat *laptop* maupun *smartphone*, dan pengujian akses ramai yaitu ketika pengguna yang mengakses jaringan *Wi-Fi* lebih dari 3, baik menggunakan perangkat *laptop* maupun *smartphone*. Setiap skenario (akses tidak ramai dan akses ramai) diuji sebanyak 30 kali untuk mendapatkan nilai rata-rata yang representatif dan mengidentifikasi fluktuasi performa jaringan.

Uji keamanan dengan tujuan menguji penerapan fitur keamanan jaringan, seperti *Client Isolation* dan pembatasan *MAC Address*. *Client Isolation* menggunakan fitur *Filter rules* untuk memastikan bahwa setiap perangkat pengguna tidak dapat saling berkomunikasi. *Filter rules* ini akan membatasi komunikasi langsung antar perangkat yang terhubung ke jaringan *Wi-Fi* yang sama. Pembatasan *MAC Address* dengan cara membatasi perangkat tertentu yang dapat terhubung ke jaringan berdasarkan *MAC Address* yang telah di daftarkan di MikroTik.

Skema pengujian *client isolation* dengan cara menghubungkan dua perangkat (*laptop* dan *smartphone*) ke jaringan *Wi-Fi* yang sama, setelah itu perangkat laptop akan melakukan *Ping* ke *ip address smartphone* dan memverifikasi apakah perangkat tersebut dapat berkomunikasi atau tidak. Pembatasan *MAC Address* dilakukan pengujian dengan cara mencoba menghubungkan perangkat dengan *MAC Address* yang tidak terdaftar di jaringan. Hanya perangkat dengan *MAC Address* yang terdaftar yang dapat mengakses jaringan.

Uji kepuasan pengguna dengan tujuan mengumpulkan *feedback* pengguna mengenai kualitas koneksi dan keamanan jaringan. Metode yang digunakan adalah survei atau kuesioner yang diisi oleh 5 pengguna mengenai kecepatan, kestabilan, dan fitur keamanan yang diterapkan.

C. Alat dan Bahan

1. Data Penelitian

Data jumlah pengguna jaringan *Wi-Fi* yang terhubung pada waktu-waktu tertentu, seperti jam sibuk dan jam tidak sibuk. Data ini bisa diperoleh dengan melihat perangkat yang terhubung melalui *log* di perangkat MikroTik setelah impelementasi, dan data jenis perangkat yang terhubung seperti *smartphone* atau *laptop*. Data ini bisa membantu memahami pola penggunaan jaringan dan diestimasi melalui pengamatan saat implementasi.

Data kinerja jaringan pasca implementasi diperoleh dengan pengukuran kecepatan jaringan setelah optimasi, yang bisa dilakukan dengan tes kecepatan sederhana di perangkat pengguna. Distribusi *bandwidth*, dengan simple *Queue* dan *Queue Tree*, dapat mengalokasikan *bandwidth* tertentu untuk pengguna, setelah implementasi mencatat hasil pengujian kecepatan untuk memastikan bahwa distribusi *bandwidth* berjalan sesuai pengaturan.

Data keamanan jaringan, setelah pembatasan *MAC Address* diterapkan, data ini bisa diperoleh dari *log* MikroTik yang menunjukkan upaya perangkat yang tidak terdaftar untuk mengakses jaringan. Jumlah pengguna yang terverifikasi di *captive portal* adalah data mengenai berapa banyak pengguna yang berhasil melakukan login melalui *captive portal* dapat memberikan informasi terkait efektivitas sistem autentikasi.

2. Alat/Instrumen Penelitian dan Pengguna.
   a. MikroTik *hAP lite RB941-2nd* sebagai perangkat utama untuk pengelolaan *bandwidth* dan keamanan jaringan di Puluhdadi *Residence*. Dikonfigurasi untuk captive portal, pembatasan *MAC Address*, *Client Isolation*, serta manajemen *bandwidth* dengan *Queue Tree* dan *Simple Queue*.

b. *Laptop ASUS ROG Strix G713IC, user* Kevin digunakan untuk konfigurasi perangkat MikroTik, mengelola data hasil pengukuran, dan sebagai alat melakukan pengukuran *bandwidth*.
c. *Laptop Acer Predator Helios Neo 16 (PHN16-72-74Z8) user* Benz digunakan untuk melakukan pengukuran *bandwidth*.
d. *Smartphone Xiaomi Poco X3 Pro user* Adam, *Smartphone HP Infinix Note 40 user* Daniel, *dan HP Xiaomi Redmi Note 13 Pro user* Haikal digunakan sebagai alat untuk melakukan pengukuran *banwidth*.
e. *Software* pendukung yaitu *Winbox* untuk konfigurasi dan pengelolaan perangkat MikroTik, serta *monitoring* jaringan.

IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Sebelum Implementasi

1. Distribusi *Bandwidth* yang Tidak Merata.

Pengukuran dilakukan sebanyak 30 kali pada kelima perangkat yang dilakukan *test* secara bersama untuk mengetahui bagaimana kecepatan *bandwidth* yang didapat ketika akses ramai, selain itu juga di lakukan pengukuran kecepatan dengan 3 pengguna untuk mengetahui berapa kecepatan *bandwidth* yang didapat ketika akses tidak ramai. Berikut ringkasan hasil pengukuran kecepatan rata-rata pada kondisi ramai dengan yang di lakukan ketika 5 pengguna mengakses internet secara bersamaan:

Tabel 1. Ringkasan Kecepatan Rata-Rata Pada Kondisi Ramai.

Pengguna	Download (*Mbps*)	Upload (*Mbps*)
Smartphone Daniel	7,35	8,62
Smartphone Adam	6,53	7,82
Smartphone Haikal	5,94	7,62
Laptop Benz	10,94	10,61
Laptop Kevin	9,87	10,24

Pada Tabel 1 menunjukkan kecepatan rata-rata *download* dan *upload* pengguna pada kondisi akses ramai. Pada kondisi ini, distribusi *bandwidth* tidak merata, di mana perangkat *laptop* cenderung mendapatkan kecepatan lebih tinggi di bandingkan perangkat *smartphone*. Ketimpangan ini terjadi ketika lebih dari tiga pengguna mengakses *internet* secara bersamaan, yang menyebabkan beberapa perangkat memperoleh alokasi *bandwidth* lebih besar dibandingkan yang lain.

Berikut di bawah ini adalah ringkasan hasil pengukuran kecepatan rata-rata di lakukan untuk mengetahui berapa kecepatan ketika kondisi tidak ramai yaitu dengan pengguna (*user*) kurang atau 3 pengguna.

Tabel 2. Ringkasan Kecepatan Rata-Rata Pada Kondisi Tidak Ramai.

Pengguna	Download (*Mbps*)	Upload (*Mbps*)
Smartphone Adam	16,28	14,08
Smartphone Haikal	15,34	13,83
Laptop Kevin	18,37	19,28

Pada Tabel 2 menunjukkan kecepatan rata-rata *download* dan *upload* pengguna pada kondisi akses ramai. Pada kondisi ini, distribusi *bandwidth* lebih merata dibandingkan saat akses ramai, di mana setiap pengguna mendapatkan kecepatan yang lebih tinggi dan relative seimbang, baik pada perangkat *smartphone* maupun *laptop*. Hal ini menunjukkan bahwa ketika jumlah pengguna yang aktif lebih sedikit, alokasi *bandwidth* dapat terbagi lebih optimal.

2. Keamanan Jaringan yang minimum.

Selain masalah distribusi *bandwidth* yang tidak merata, keamanan jaringan di Puluhdadi *Residence* juga teridentifikasi sebagai permasalahan utama. Berdasarkan pengujian yang dilakukan, ditemukan bahwa perangkat laptop dapat melakukan *Ping* ke perangkat HP melalui *Command Prompt* begitu juga sebaliknya dari perangkat HP dapat melakukan *Ping* ke perangkat *laptop*, seperti yang ditunjukkan pada gambar hasil pengujian di bawah ini dengan hasil *received* = 4 , *lost* = 0 (0% *loss*). Hal ini menunjukkan bahwa tidak ada isolasi antara perangkat yang terhubung ke jaringan *Wi-Fi*, sehingga setiap perangkat dapat saling berkomunikasi secara langsung melalui alamat *ip* (*ip adrress*) tanpa pembatasan.

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

```
C:\Users\acer>ping 192.168.18.237

Pinging 192.168.18.237 with 32 bytes of data:
Reply from 192.168.18.237: bytes=32 time=363ms TTL=64
Reply from 192.168.18.237: bytes=32 time=68ms TTL=64
Reply from 192.168.18.237: bytes=32 time=1127ms TTL=64
Reply from 192.168.18.237: bytes=32 time=81ms TTL=64

Ping statistics for 192.168.18.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 1127ms, Average = 409ms
```

Gambar 2. Hasil pengujian dengan *ping* dari *Laptop* Benz ke *Laptop* Kevin.

```
C:\Users\acer>ping 192.168.18.145

Pinging 192.168.18.145 with 32 bytes of data:
Reply from 192.168.18.145: bytes=32 time=796ms TTL=64
Reply from 192.168.18.145: bytes=32 time=68ms TTL=64
Reply from 192.168.18.145: bytes=32 time=89ms TTL=64
Reply from 192.168.18.145: bytes=32 time=95ms TTL=64

Ping statistics for 192.168.18.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 796ms, Average = 262ms
```

Gambar 3. Hasil pengujian dengan *ping* dari *Laptop* Benz ke *Smartphone* Haikal.

```
C:\Users\Kevin>ping 192.168.18.145

Pinging 192.168.18.145 with 32 bytes of data:
Reply from 192.168.18.145: bytes=32 time=80ms TTL=64
Reply from 192.168.18.145: bytes=32 time=1ms TTL=64
Reply from 192.168.18.145: bytes=32 time=110ms TTL=64
Reply from 192.168.18.145: bytes=32 time=28ms TTL=64

Ping statistics for 192.168.18.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 110ms, Average = 54ms
```

Gambar 4. Hasil Pengujian dengan *Ping* dari *Laptop* Kevin ke *Smartphone* Haikal.

```
C:\Users\Kevin>ping 192.168.18.210

Pinging 192.168.18.210 with 32 bytes of data:
Reply from 192.168.18.210: bytes=32 time=198ms TTL=64
Reply from 192.168.18.210: bytes=32 time=113ms TTL=64
Reply from 192.168.18.210: bytes=32 time=32ms TTL=64
Reply from 192.168.18.210: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.18.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 198ms, Average = 86ms
```

Gambar 5. Hasil pengujian dengan *ping* dari *Laptop* Kevin ke S*martphone* Adam.

```
Starting ...
PING 192.168.18.237 (192.168.18.237) 56(84) bytes of data.
Reply from 192.168.18.237: icmp_seq=1 ttl=63 time=755 ms
Reply from 192.168.18.237: icmp_seq=2 ttl=63 time=229 ms
Reply from 192.168.18.237: icmp_seq=3 ttl=63 time=1249 ms
Reply from 192.168.18.237: icmp_seq=4 ttl=63 time=189 ms
Reply from 192.168.18.237: icmp_seq=5 ttl=63 time=272 ms
----- 192.168.18.237 ping statistics -----
  Packets: Sent = 5, Received = 5, Lost = 0 (0.0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 189.0ms, Maximum = 1249.0ms, Average = 538.8ms
```

Gambar 6. Hasil pengujian dengan *ping* dari *Smartphone* Haikal ke *Laptop* Kevin.

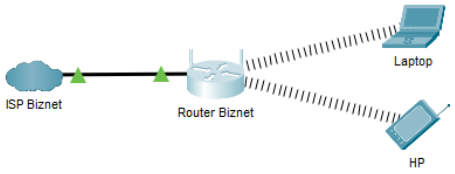
```
PING 192.168.18.227 (192.168.18.227) 56(84) bytes of data.
Reply from 192.168.18.227: icmp_seq=1 ttl=63 time=6.69 ms
Reply from 192.168.18.227: icmp_seq=2 ttl=63 time=2.56 ms
Reply from 192.168.18.227: icmp_seq=3 ttl=63 time=24.3 ms
Reply from 192.168.18.227: icmp_seq=4 ttl=63 time=16.8 ms
Reply from 192.168.18.227: icmp_seq=5 ttl=63 time=2.57 ms
----- 192.168.18.227 ping statistics -----
  Packets: Sent = 5, Received = 5, Lost = 0 (0.0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 2.56ms, Maximum = 24.3ms, Average = 10.58ms
```

Gambar 7. Hasil pengujian dengan *ping* dari *Smartphone* Haikal ke *Laptop* Benz.

Dalam pengujian ini, ketika perangkat melakukan *Ping* ke perangkat yang lain contoh *smartphone* Haikal ke *laptop* Kevin, berhasil mengirimkan paket data dengan keterangan *sent* = 5, *received* = 5, *lost* = 0% (0,0% *loss*) yang menunjukkan mengirim paket ke *smartphone* Daniel sebanyak 5 dan diterima sejumlah 5, kehilangan paket 0. Hal ini menandakan bahwa perangkat dalam jaringan tidak dipisahkan atau diisolasi, sehingga semua perangkat yang terhubung ke jaringan dapat berinteraksi satu sama lain. Kondisi ini mengindikasikan adanya risiko keamanan, seperti potensi akses tidak sah oleh perangkat yang tidak diinginkan atau yang tidak terverifikasi.

3. Persiapan perangkat dan Konfigurasi Awal

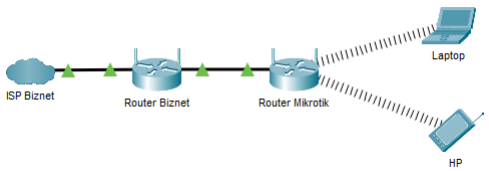
Pada tahap kedua, dilakukan persiapan perangkat dan konfigurasi awal, perangkat yang di gunakan adalah MikroTik *hAP lite RB941-2nD*. Berikut bentuk topologi awal dan setelah implementasi.



Gambar 8. Toplogi jaringan awal sebelum implementasi.

Topologi jaringan sebelum implementasi pada Puluhdadi *Residence* masih bersifat sederhana tanpa adanya pengaturan manajemen *bandwidth* dan keamanan jaringan. Perangkat *router* langsung terhubung ke internet melalu *port WAN* dan mendistribusikan koneksi secara langsung kepada semua pengguna melalui jaringan *Wi-Fi* tanpa kontrol autentikasi atau pembatasan akses. Tidak terdapat mekanisme untuk pembagian *bandwidth* secara adil, sehingga pengguna dengan aktivitas tinggi dapat menyerap lebih banyak *bandwidth*. Selain itu, seluruh perangkat dalam jaringan dapat saling berkomunikasi tanpa batas, yang meningkatkan potensi risiko keamanan seperti penyadapan data atau akses tidak sah antar perangkat.

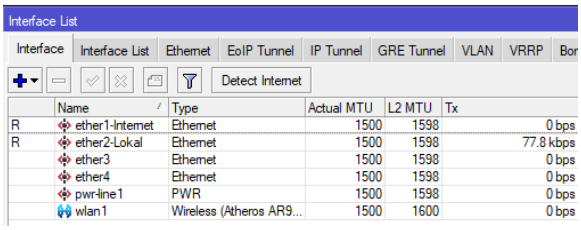
Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373



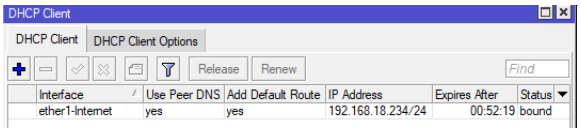
Gambar 9. Topologi jaringan setelah implementasi

Topologi jaringan setelah implementasi menunjukkan perangkat MikroTik sebagai pusat pengendali akses, dihubungkan langsung dengan internet melalui *port ether1*. *Port ether2* hingga *ether4* digunakan untuk mendistribusikan koneksi ke klien, baik melalui kabel *LAN* maupun *Wi-Fi*. MikroTik juga bertanggung jawab atas pengaturan *bandwidth*, autentikasi pengguna, serta isolasi antar perangkat.

Berikut adalah konfigurasi awal untuk MikroTik dan pengaturan dasar untuk *Captive Portal hotspot* agar siap untuk implementasi pada tahap selanjutnya.

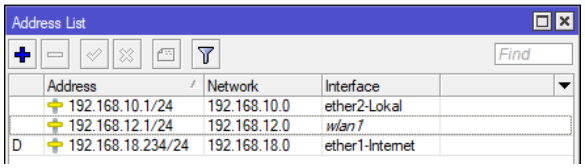


Gambar 10. *Interface list.*

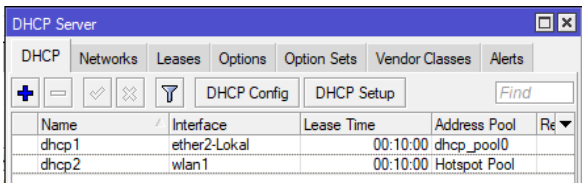


Gambar 11. *DHCP Client* untuk ether 1 (koneksi internet).

Pada Gambar 10-11, *interface list* mengatur *port* yang digunakan untuk koneksi *internet* dan jaringan lokal. *DHCP Client* pada *ether1* memungkinkan MikroTik menerima *IP Address* secara otomatis dari *ISP*.

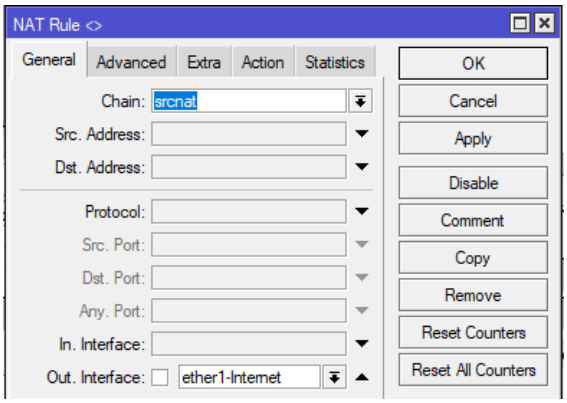


Gambar 12. *Address list.*

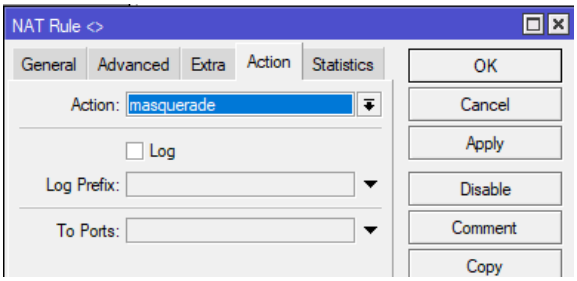


Gambar 13. *DHCP Server.*

Pada Gambar 12-13, *address list* menyimpan *IP address* lokal yang diberikan kepada klien. *DHCP Server* mengatur pembagian *IP address* otomatis ke perangkat pengguna.



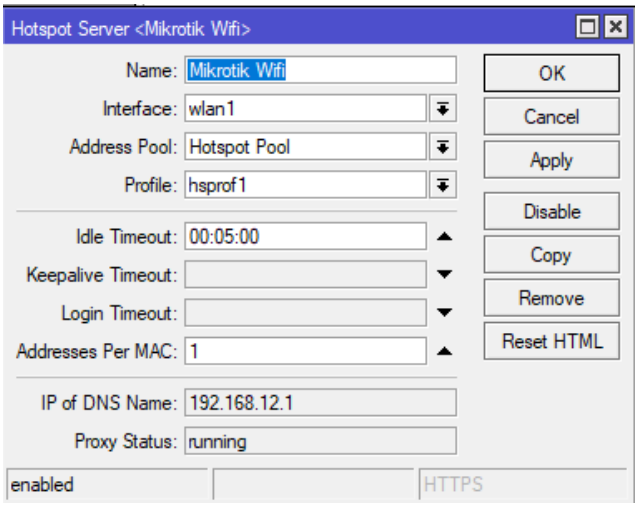
Gambar 14. *Setting NAT* pertama.



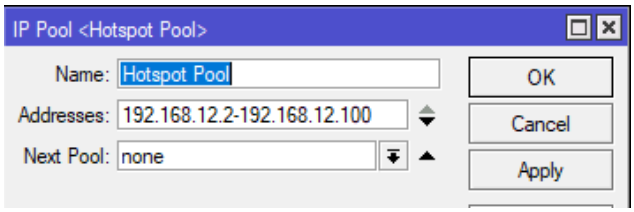
Gambar 15. *Setting NAT* kedua.

Pada Gambar 14-15, *Network Address Translation (NAT)* mengatur klien bisa mengakses *internet* dengan *IP address* publik MikroTik. Dua konfigurasi *NAT* digunakan untuk *masquerading* trafik keluar dan mengarahkan pengguna ke halaman *login Captive Portal.*

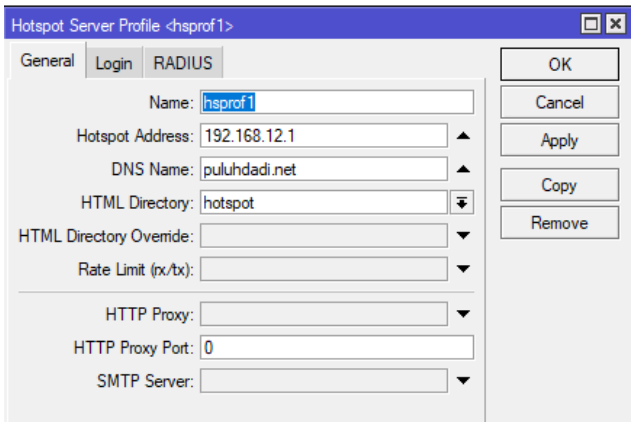
Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373



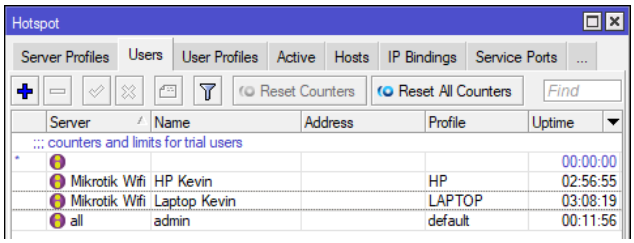
Gambar 16. *Setting Hotspot Setup.*



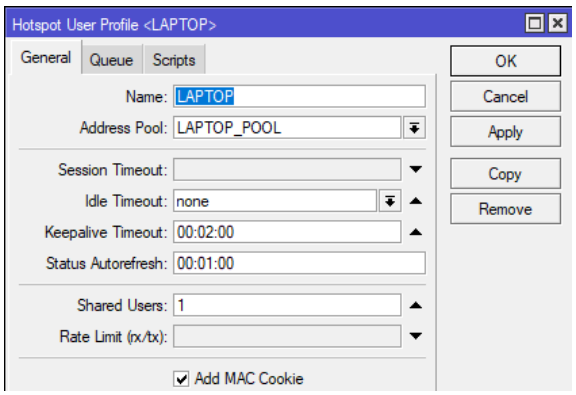
Gambar 17. *IP Pool* untuk *Hotspot.*



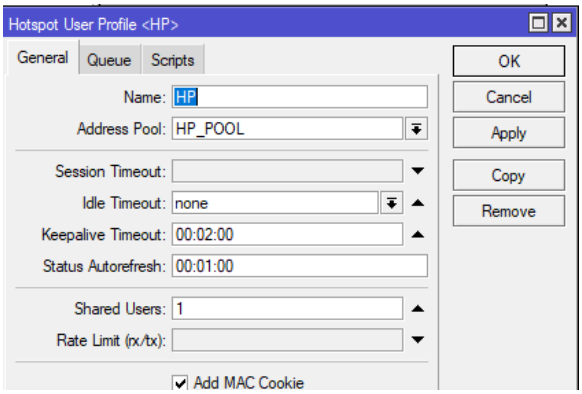
Gambar 18. *Hotspot Server Profile.*



Gambar 19. *Hotspot Users.*

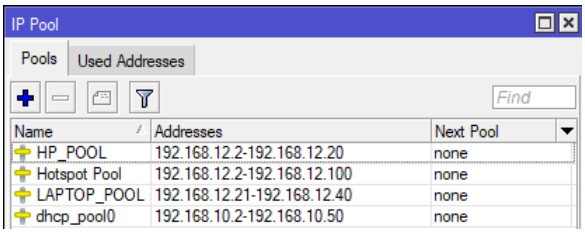


Gambar 20. *Hotspot User Profile* Laptop.

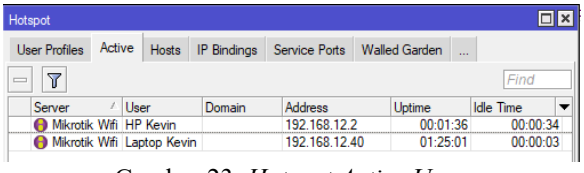


Gambar 21. *Hotspot User Profile* HP

Pada Gambar 16–21, *Hotspot Setup* dan *User Profiles*, konfigurasi *hotspot* digunakan untuk mengaktifkan *captive portal*. *Hotspot server* dan *user profiles* mengatur autentikasi berdasarkan perangkat *(laptop/smartphone)* dan memberikan kontrol granular seperti durasi *login* dan batas *bandwidth*.

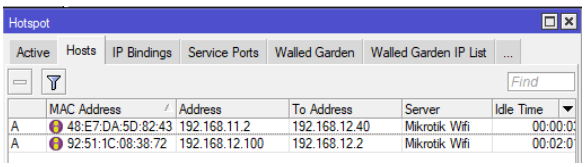


Gambar 22. *IP Pool* yang digunakan.

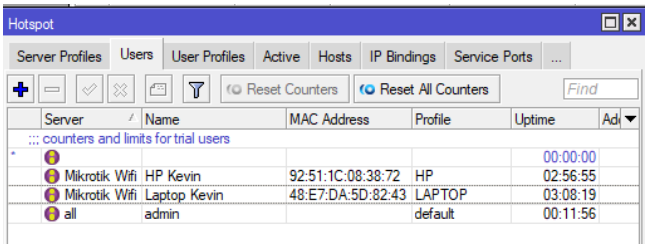


Gambar 23. *Hotspot Active User.*

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

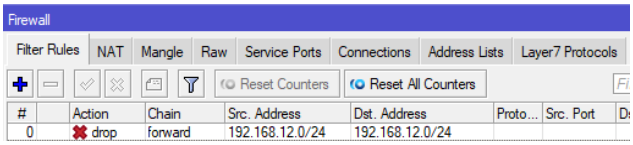


Gambar 24. *Hotspot Host.*



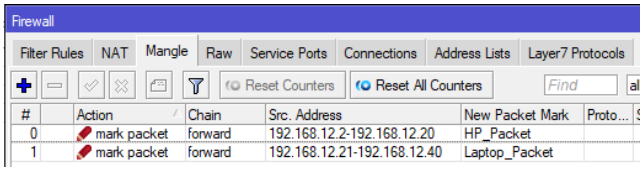
Gambar 25. *User MAC Address* perangkat pengguna.

Pada Gambar 22–25, *IP Pool, Host,* dan *MAC Binding*. *IP Pool* menentukan rentang *IP address* lokal yang tersedia untuk klien. *MAC Binding* mencatat dan mengizinkan hanya perangkat tertentu untuk terhubung.



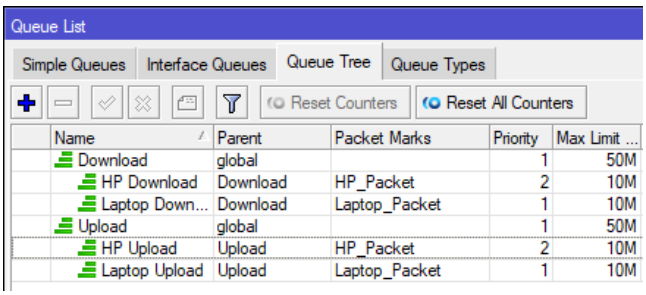
Gambar 26. *Firewall Filter rules* (*Client Isolation).*

Pada Gambar 26, *Firewall Filter Rule (Client Isolation)* digunakan untuk mencegah komunikasi antar perangkat yang terhubung ke jaringan, sehingga meningkatkan keamanan antar pengguna.

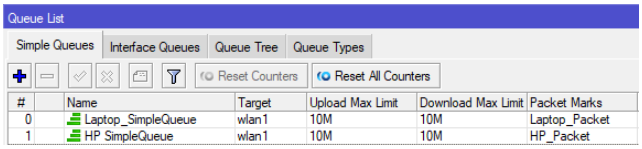


Gambar 27. Pengaturan *Firewall* pada *Mangle.*

Pada Gambar 27, *Firewall Mangle* digunakan untuk menandai paket data berdasarkan alamat *IP address* atau *port*, sebagai dasar pengaturan *bandwidth* melalui *Queue Tree*.



Gambar 28. Pengaturan *Queue Tree.*



Gambar 29. Pengaturan *Simple Queue.*

Pada Gambar 28–29, *Queue Tree dan Simple Queue*. *Queue Tree* digunakan untuk mengelola *bandwidth* secara global dan berjenjang berdasarkan kelompok pengguna. *Simple Queue* digunakan untuk mengalokasikan *bandwidth* spesifik ke tiap perangkat pengguna agar adil.

B. Setelah Implementasi

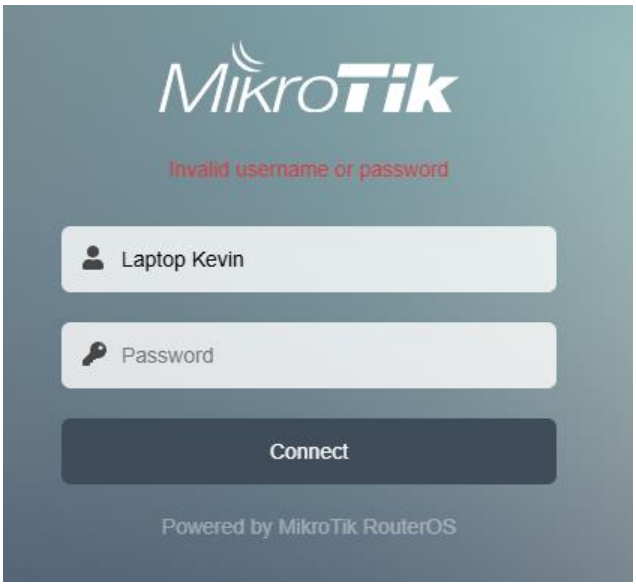
Pada tahap ini, dilakukan pengujian untuk mengevaluasi keberhasilan implementasi *Captive Portal* berdasarkan tiga skema utama, yaitu uji performa *bandwidth*, uji keamanan jaringan, dan uji kepuasan pengguna. Masing-masing skema pengujian memiliki metode dan tujuan yang spesifik sebagai berikut.

Gambar 30. Hasil *login Captive Portal* pada Laptop Kevin.

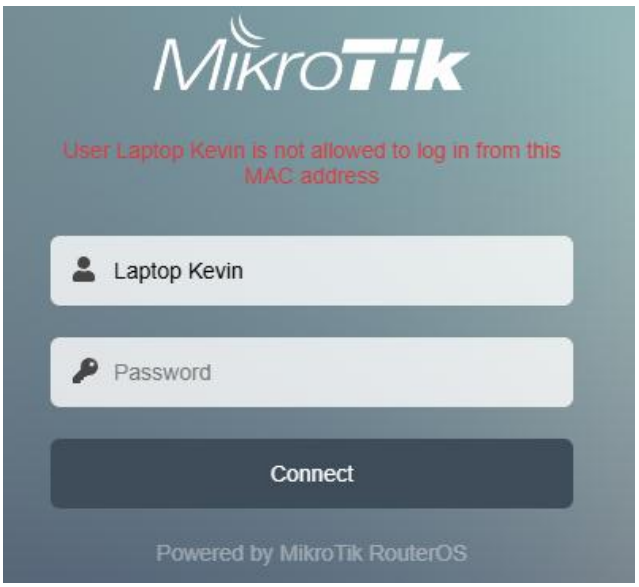
Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

Gambar 31. Hasil *login Captive Portal* pada Laptop Benz.

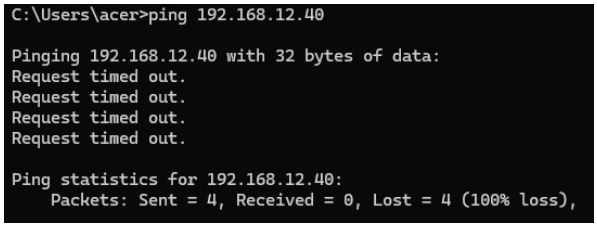
Gambar 32. Hasil *login Captive Portal* pada *Smartphone* Daniel.



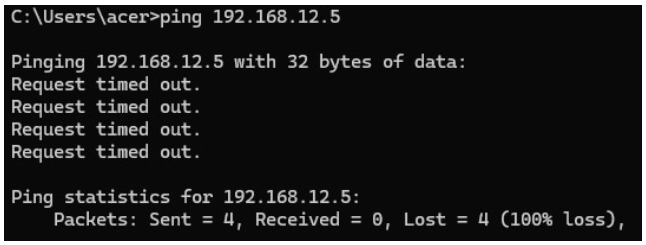
Gambar 33. Hasil login gagal saat *ID* atau *password* salah.



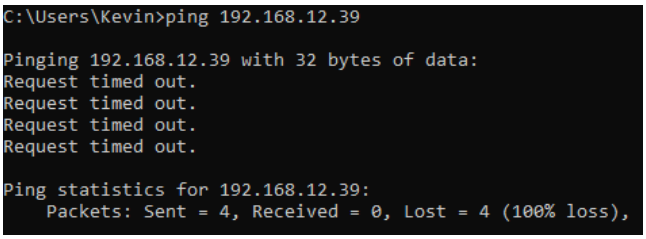
Gambar 34. Hasil *login* gagal karena *MAC Address* berbeda.



Gambar 35. *Ping* dari *Laptop* Benz ke *Laptop* Kevin tidak berhasil.



Gambar 36. *Ping* dari *Laptop* Benz ke *Smartphone* Haikal tidak berhasil.



Gambar 37. *Ping* dari *Laptop* Kevin ke *Smartphone* Haikal tidak berhasil.

Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

```
C:\Users\Kevin>ping 192.168.12.39

Pinging 192.168.12.39 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.12.39:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 38. *Ping* dari *Laptop* Kevin ke *Laptop* Benz tidak.

```
Starting ...
PING 192.168.12.40 (192.168.12.40) 56(84) bytes of data.
Request time out.
Request time out.
Request time out.
Request time out.
----- 192.168.12.40 ping statistics -----
  Packets: Sent = 4, Received = 0, Lost = 4 (100.0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0.0ms, Maximum = 0.0ms, Average = 0.0ms
```

Gambar 39. *Ping* dari *Smartphone* Haikal ke *Laptop* Kevin tidak berhasil.

```
Starting ...
PING 192.168.12.6 (192.168.12.6) 56(84) bytes of data.
Request time out.
Request time out.
Request time out.
Request time out.
----- 192.168.12.6 ping statistics -----
  Packets: Sent = 4, Received = 0, Lost = 4 (100.0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0.0ms, Maximum = 0.0ms, Average = 0.0ms
```

Gambar 40. *Ping* dari *Smartphone* Haikal ke *Smartphone* Daniel tidak berhasil.

Pada tahap ini dilakukan pengujian performa *bandwidth* setelah implementasi. Pengukuran ini juga dilakukan sebanyak 30 kali pada kelima perangkat yang dilakukan *test* secara bersama untuk mengetahui bagaimana kecepatan *bandwidth* yang didapat ketika akses ramai, selain itu juga di lakukan pengukuran kecepatan dengan 3 pengguna untuk mengetahui berapa kecepatan *bandwidth* yang didapat ketika akses tidak ramai. Berikut ringkasan hasil pengukuran kecepatan rata-rata pada kondisi ramai dengan yang di lakukan ketika 5 pengguna mengakses internet secara bersamaan:

Tabel 3. Ringkasan Kecepatan Rata-Rata Pada Kondisi Ramai Setelah Implementasi.

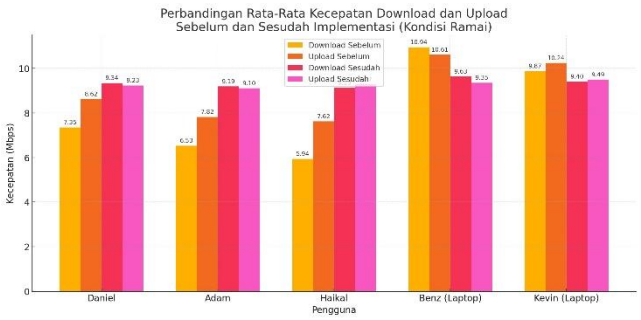
Pengguna	Download (*Mbps*)	Upload (*Mbps*)
Smartphone Daniel	9,34	9,23
Smartphone Adam	9,19	9,10
Smartphone Haikal	9,13	9,27
Laptop Benz	9,63	9,35
Laptop Kevin	9,40	9,49

Pada Tabel 3 menunjukkan kecepatan rata-rata *download* dan *upload* tiap pengguna pada kondisi akses ramai. Pada kondisi ini setelah di lakukan implementasi optimasi penggunaan *bandwidth*, distribusi *bandwidth* yang sebelumnya tidak merata, di mana perangkat *laptop* cenderung mendapatkan kecepatan lebih tinggi di bandingkan perangkat *smartphone*. Kini hal tersebut sudah tidak terjadi di mana setiap pengguna mendapat rata-rata kecepatan *bandwidth* yang sama yaitu berkisar 9-10 *Mbps* sesuai dengan alokasi 10*Mbps* tiap pengguna

Tabel 4. Ringkasan Kecepatan Rata-Rata Pada Kondisi Tidak Ramai.

Pengguna	Download (*Mbps*)	Upload (*Mbps*)
Smartphone Adam	16,54	16,31
Smartphone Haikal	16,15	17,12
Laptop Kevin	17,23	16,49

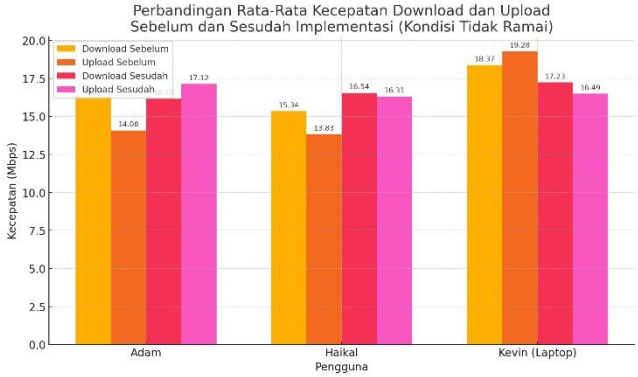
Pada Tabel 4 menunjukkan kecepatan rata-rata *download* dan *upload* pengguna pada kondisi akses ramai. Pada kondisi ini, distribusi *bandwidth* yang di terima tiap pengguna memiliki rata-rata yang mendekati sama walaupun tiap pengguna mendapat alokasi 10 *Mbps* namun ketika jumlah pengguna yang terhubung hanya 3 seperti contoh di bawah ini tiap pengguna akan mendapat lebih banyak *bandwidth* atau lebih dari 10 *Mbps*.



Jurnal EEMISAS, Vol. 4, No.1, Juni 2025, Hal. 1-14
Journal of Electrical, Electronic, Mechanical, Informatic, and Social applied Science
ISSN 2964-1373

Gambar 41. Grafik perbandingan kecepatan sebelum dan sesudah implementasi pada kondisi ramai.

Grafik ini menunjukkan bahwa setelah implementasi, kecepatan unduh *(download)* dan kecepatan unggah *(upload)* menjadi lebih seimbang antar pengguna, dengan selisih antar perangkat yang jauh lebih kecil dibandingkan sebelumnya. Ini menandakan bahwa distribusi *bandwidth* menjadi adil dan sesuai alokasi yang ditentukan.



Gambar 42. Grafik perbandingan kecepatan sebelum dan sesudah implementasi pada kondisi tidak ramai.

Grafik ini menunjukkan bahwa meskipun kecepatan pengguna sebelum implementasi relatif tinggi, terdapat peningkatan stabilitas dan keseimbangan antar perangkat setelah optimasi. *Upload rate* yang sebelumnya bervariasi kini lebih stabil, menunjukkan alokasi *bandwidth* yang lebih terkendali.

Dari 5 responden, tingkat kepuasan pengguna setelah selesai implementasi meninggkat secara signifikan. 80% pengguna menyatakan puas terhadap kestabilan koneksi, dan 100% merasa jaringan lebih aman. Sebelum implementasi, hanya 20% pengguna yang merasa koneksi stabil saat jam ramai.

Dari hasil pengujian kecepatan sebelum implementasi, ditemukan bahwa nilai standar deviasi kecepatan unduh *(download)* dari *smartphone* sebesar 0,52 *Mbps*, sedangkan setelah implementasi turun menjadi 0,18 *Mbps*. Ini menunjukkan bahwa distribusi *bandwidth* menjadi lebih seragam. Selain itu, skor rata-rata kepuasan pengguna meningkat dari 2,4 menjadi 4,6 (skala 1-5) berdasarkan kuesioner yang disebarkan. Temuan ini memperkuat efektivitas pendekatan teknis yang digunakan dalam meningkatkan performa dan stabilitas jaringan di Puluhdadi *Residence*.

Fitur MikroTik seperti *Captive Portal, Simple Queue*, dan *Client Isolation* sangat membantu dalam pengelolaan jaringan, tetapi masih terdapat beberapa keterbatasan. *Captive Portal* dapat rentan terhadap *bypass* melalui *spoofing MAC Address* jika tidak dikombinasikan dengan autentikasi dua faktor. *Simple Queue* cenderung tidak efisien untuk jumlah klien yang besar. *Client Isolation* juga dapat membatasi fungsi perangkat yang memerlukan komunikasi lokal.

V. KESIMPULAN

Penerapan manajemen *bandwidth, Client Isolation, dan Captive Portal* menggunakan perangkat MikroTik *hAP lite RB941-2nD* di Puluhdadi *Residence* menunjukkan hasil yang efektif dalam mengatasi permasalahan distribusi *bandwidth* dan keamanan jaringan. Berdasarkan hasil implementasi dan pengujian yang dilakukan, diperoleh beberapa kesimpulan sebagai berikut:

1. Distribusi *bandwidth* menjadi lebih merata setelah implementasi. Kecepatan rata-rata pengguna saat kondisi ramai berada pada kisaran 9-10 *Mbps* sesuai dengan alokasi yang ditentukan, dan meningkat hingga 16-17 *Mbps* pada saat kondisi ramai. Hal ini menandakan alokasi *bandwidth* setelah berjalan optimal.

2. Stabilitas jaringan meningkat, ditunjukkan dengan penurunan nilai standar deviasi kecepatan unduh dari 0,52 *Mbps* menjadi 0,18 *Mbps*. Hal ini menunjukkan bahwa variasi kecepatan antar pengguna berkurang dan distribusi *bandwidth* menjadi lebih konsisten.

3. Penggunaan *Captive Portal* berhasil memberikan kontrol akses yang lebih baik terhadap jaringan *Wi-Fi*. Hanya pengguna dengan kredensial *valid* yang dapat mengakses jaringan, sehingga potensi penyalahgunaan akses oleh perangkat tidak sah dapat diminimalkan.

4. Fitur *Client Isolation* efektif dalam mencegah komunikasi antar pengguna dalam jaringan. Hasil pengujian menunjukkan seluruh percobaan *ping* antar perangkat mengalami kegagalan (100 % *packet loss*), menandakan bahwa isolasi berjalan sebagaimana mestinya dan meningkatkan keamanan.

5. Tingkat kepuasan pengguna mengalami peningkatan signifikan. Skor rata-rata meningkat dari 2,4 menjadi 4,6 (skala 1-50), dengan 80% pengguna menyatakan puas terhadap kestabilan koneksi, dan 100 % merasa jaringan lebih aman setelah implementasi.

6. Meskipun sistem yang diterapkan sudah berjalan efektif, pengembangan lebih lanjut tetap dimungkinkan, seperti integrasi teknologi *Virtual Private Network (VPN)* dan autentikasi dua faktor (2FA) untuk meningkatkan keamanan dan privasi pada jaringan *Wi-Fi*, terutama bagi pengguna yang memerlukan tingkat keamanan lebih tinggi dalam akses jaringan.

REFERENSI

[1] C. E. Suharyanto, P. Simanjuntak, and S. Adam, "Optimalisasi Sistem Keamanan Jaringan dan Manajemen *Bandwidth* pada Jaringan (Studi Kasus: CU Tunas Harapan)," J. Desain dan Anal. Teknol., vol. 1, no. 1, pp. 13–18, Jul. 2022, doi: 10.58520/jddat.v1i1.14.

[2] N. N. Afandi, "*Optimization of Bandwidth Management with Simple Queue Limitation Using* MikroTik *devices in* SukarajaKulon *Village*," Seminar Teknologi Majalengka (STIMA), vol. 8, pp. 224–232, Oct. 2024, doi: 10.31949/stima.v8i0.1169.

[3] R. P. N. M. Hakim, S. Raharjo, and Y. R. Kusumaningsih, "Manajemen *Bandwidth* Menggunakan Metode *Queue Tree* dan Keamanan *Hotspot* Menggunakan MikroTik OS dan GNS3 di Balai Desa Sidorejo," Jurnal Jarkom, vol. 11, no. 1, pp. 24–31, Jun. 2023, doi: 10.34151/jarkom.v11i1.4781.

[4] W. Stallings, *Data and Computer Communications, 8th ed. Boston*, MA: Pearson *Education*, 2007.

[5] B. A. Forouzan, *Data Communications and Networking, 4th ed*. New York, NY: McGraw-Hill, 2007.

[6] Y.-F. Liu, L. Zhu, X. Chen, J. Wang, and M. Tao, "*A Survey of Recent Advances in Optimization Methods for Wireless Communications,*" IEEE J. Sel. Areas Commun., vol. 42, no. 11, pp. 2992–3031, Nov. 2024, doi: 10.1109/JSAC.2024.3443759.

[7] W. Stallings, *Network Security Essentials: Applications and Standards, 4th ed. Boston*, MA: Pearson, 2012.

[8] Suhadin, "*Evaluation of Network Access Restrictions Using MAC Address Filtering on MikroTik to Improve Network Security*," J. World Sci., vol. 1, no. 3, pp. 112–120, Mar. 2022, doi: 10.58344/jws.v1i3.12.

[9] M. F. Altarik and A. D. Putra, "Perancangan Keamanan Jaringan Metode Authentication Login Hotspot Menggunakan Router MikroTik di PT. Nusindo Rekatama Semesta," J. Nasional Ilmu Komputer, vol. 4, no. 4, pp. 103–120, Nov. 2023, doi: 10.47747/jurnalnik.v4i4.1502.

[10] N. Ngatono, S. Dwiyatno, A. D. Jubaedi, Y. Ferdiansyah, E. Krisnaningsih, and R. Rahmat, "Implementasi User Manager MikroTik dalam Authentication Login pada Hotspot," Prosisko, vol. 11, no. 1, pp. 137–144, Mar. 2024, doi: 10.30656/prosisko.v11i1.8297.

[11] Y. Zhang, J. Li, and K. Zhao, "*Security Analysis of Captive Portal Systems and Proposals for Enhancement*," Int. J. Network Security, vol. 24, no. 3, pp. 188–195, 2022.

[12] N. Asyifah and D. Ramayanti, "Optimasi Kinerja Jaringan di SMK Al Fudhola Bekasi: Pengaturan *Bandwidth* dengan MikroTik RB951Ui-2HnD dan Penerapan Algoritma *Simple Queue*," J. Ilm. Ilkominfo, vol. 7, no. 1, Jan. 2024, doi: 10.47324/ilkominfo.v7i1.210.

[13] N. H. Adi and C. F. Suriansyah, "Pengembangan Jaringan *Wireless* Menggunakan MikroTik *Router* hAP lite RB941-2nD," J. Rekayasa, vol. 6, no. 2, Dec. 2022, doi: 10.36352/jr.v6i2.