

# IMPLEMENTASI JARINGAN WLAN DENGAN MANAJEMEN HOTSPOT DAN BANDWIDTH BERBASIS MIKROTIK PADA LABORATORIUM KOMPUTER FASILKOM UBHARA JAYA

<sup>1</sup>Muhammad Yasir, <sup>2</sup>Agus Hidayat\*, <sup>3</sup>Achmad Noeman, <sup>4</sup>Asep Ramdhani Mahbub, <sup>5</sup>Rasim, <sup>6</sup>Robertus Suraji, <sup>7</sup>Hendarman Lubis

<sup>1,2,3,4,5,6,7</sup>Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya  
Jl. Raya Perjuangan No. 81, RT. 003/RW. 002, Marga Mulya, Kec. Bekasi Utara, Kota Bekasi, Jawa Barat, 17143, Indonesia

\*e-mail: [muhammad.yasir@dsn.ubharajaya.ac.id](mailto:muhammad.yasir@dsn.ubharajaya.ac.id), [agus.hidayat@dsn.ubharajaya.ac.id](mailto:agus.hidayat@dsn.ubharajaya.ac.id),  
[achmad.noeman@dsn.ubharajaya.ac.id](mailto:achmad.noeman@dsn.ubharajaya.ac.id), [aseprm@dsn.ubharajaya.ac.id](mailto:aseprm@dsn.ubharajaya.ac.id),  
[rasim@dsn.ubharajaya.ac.id](mailto:rasim@dsn.ubharajaya.ac.id), [robertus.suraji@dsn.ubharajaya.ac.id](mailto:robertus.suraji@dsn.ubharajaya.ac.id),  
[hendarman.lubis@dsn.ubharajaya.ac.id](mailto:hendarman.lubis@dsn.ubharajaya.ac.id)

## Abstrak

Laboratorium komputer Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya (Fasilkom Ubhara) sebelumnya bergantung pada jaringan hotspot dari provider ISP yang tidak dapat dikonfigurasi secara mandiri, sehingga tidak tersedia mekanisme pembatasan bandwidth, manajemen pengguna, maupun autentikasi akses yang memadai. Kondisi ini menyebabkan penggunaan bandwidth yang tidak terkontrol dan ketidakmampuan administrator dalam memonitor aktivitas jaringan. Penelitian ini bertujuan untuk mengimplementasikan infrastruktur jaringan WLAN mandiri berbasis MikroTik RouterOS yang dilengkapi dengan manajemen hotspot menggunakan captive portal dan pembatasan bandwidth melalui Simple Queue. Metode yang digunakan adalah *Network Development Life Cycle* (NDLC) yang mencakup tahapan analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Hasil implementasi menunjukkan bahwa jaringan WLAN berhasil dibangun dengan konektivitas penuh ke internet (packet loss 0%, avg-rtt 1ms), pembatasan bandwidth efektif pada 5 Mbps upload/download per segmen jaringan dengan hasil speedtest mencapai 4,31 Mbps download dan 4,72 Mbps upload, serta sistem hotspot captive portal yang berfungsi dengan autentikasi berbasis username dan password melalui domain labsiber.com. Penelitian ini menyimpulkan bahwa implementasi MikroTik secara signifikan meningkatkan kontrol administrator terhadap jaringan laboratorium dibandingkan kondisi sebelumnya.

**Kata kunci:** MikroTik, WLAN, Hotspot, Bandwidth Management, Simple Queue

## Abstract

*The computer laboratory of the Faculty of Computer Science, Bhayangkara Jakarta Raya University (Fasilkom Ubhara) previously relied on a hotspot network provided by an ISP that could not be independently configured, resulting in no available mechanism for bandwidth limitation, user management, or adequate access authentication. This condition led to uncontrolled bandwidth usage and the inability of administrators to monitor network activity. This study aims to implement an independent WLAN infrastructure based on MikroTik RouterOS, equipped with hotspot management using a captive portal and bandwidth limitation through Simple Queue. The method used is the Network Development Life Cycle (NDLC), encompassing analysis, design, simulation, implementation, monitoring, and management phases. Implementation results demonstrate that the WLAN network was successfully built with full internet connectivity (0% packet loss, avg-rtt 1ms),*



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).  
<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

*effective bandwidth limitation at 5 Mbps upload/download per network segment with speedtest results reaching 4.31 Mbps download and 4.72 Mbps upload, and a functioning hotspot captive portal system with username-password authentication via the labsiber.com domain. This study concludes that MikroTik implementation significantly improves administrator control over the laboratory network compared to the previous condition.*

**Keywords:** MikroTik, WLAN, Hotspot, Bandwidth Management, Simple Queue

## 1 Pendahuluan (or Introduction)

Perkembangan kebutuhan akses internet di lingkungan pendidikan tinggi terus meningkat seiring dengan meluasnya adopsi model pembelajaran berbasis teknologi. Laboratorium komputer tidak lagi sekadar ruang praktikum perangkat keras, melainkan telah berkembang menjadi infrastruktur jaringan yang kompleks dengan beragam pengguna dan kebutuhan akses yang berbeda-beda [1]. Dalam konteks ini, ketersediaan jaringan yang andal, terkelola, dan dapat dikonfigurasi secara mandiri oleh administrator institusi menjadi kebutuhan yang tidak dapat ditawar.

Laboratorium komputer Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya (Fasilkom Ubhara) sebelumnya menggunakan jaringan hotspot yang disediakan langsung oleh provider ISP. Meskipun memberikan akses internet dasar, pendekatan ini memiliki keterbatasan fundamental: administrator tidak memiliki kendali atas pembagian bandwidth antar pengguna, tidak ada mekanisme autentikasi yang dapat dikustomisasi, dan tidak tersedia alat untuk memonitor aktivitas jaringan secara real-time. Akibatnya, pada saat penggunaan jaringan mencapai puncaknya misalnya ketika beberapa kelas praktikum berlangsung bersamaan terjadi penurunan kecepatan yang signifikan karena tidak ada prioritas atau pembatasan alokasi bandwidth [2].

MikroTik RouterOS merupakan sistem operasi jaringan berbasis Linux yang telah banyak digunakan sebagai solusi manajemen jaringan skala menengah, termasuk di lingkungan kampus dan laboratorium [3]. Kemampuannya mencakup routing, firewall, manajemen bandwidth melalui Simple Queue dan Queue Tree, server DHCP, wireless access point, serta hotspot berbasis captive portal yang dapat dikonfigurasi secara granular sesuai kebutuhan institusi [4]. Kelebihan utama MikroTik dibandingkan solusi berbasis provider ISP adalah kendali penuh berada di tangan administrator lokal, sehingga kebijakan jaringan dapat disesuaikan dengan kebutuhan operasional laboratorium secara dinamis.

Penelitian ini bertujuan untuk mengimplementasikan infrastruktur jaringan WLAN berbasis MikroTik pada laboratorium komputer Fasilkom Ubhara dengan tiga objektif spesifik: (1) membangun konektivitas internet yang stabil melalui konfigurasi DHCP Client, DNS, dan NAT Masquerade; (2) menerapkan pembatasan bandwidth berbasis Simple Queue untuk mengendalikan penggunaan sumber daya jaringan; dan (3) mengimplementasikan sistem hotspot dengan captive portal untuk manajemen autentikasi pengguna. Hasil penelitian ini diharapkan dapat menjadi referensi implementasi praktis bagi institusi pendidikan lain yang menghadapi permasalahan serupa.

## 2 Tinjauan Literatur (or Literature Review)

Manajemen jaringan komputer di lingkungan akademik telah menjadi subjek penelitian yang aktif dalam dekade terakhir, didorong oleh meningkatnya kompleksitas infrastruktur dan keberagaman kebutuhan pengguna. Herawan dan Prihantoro (2024) mendokumentasikan implementasi pengembangan sistem jaringan internet berbasis router MikroTik pada lingkungan korporat dan menemukan bahwa penerapan Simple Queue secara signifikan mengurangi keluhan pengguna terkait kecepatan internet dengan mengalokasikan bandwidth yang tidak terpakai secara dinamis kepada pengguna yang membutuhkan [5]. Temuan ini relevan untuk konteks laboratorium akademik di mana pola penggunaan bandwidth bersifat bursty dan tidak merata antar sesi praktikum.

Dalam aspek autentikasi pengguna jaringan nirkabel, Dwiyatno et al. menunjukkan bahwa implementasi User Manager MikroTik pada sistem hotspot mampu membatasi akses hanya kepada pengguna yang terautentikasi, sekaligus memberikan administrator kemampuan untuk memonitor sesi



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

aktif, waktu penggunaan, dan volume data per pengguna [6]. Pendekatan ini mengatasi kelemahan mendasar jaringan hotspot dari provider ISP yang tidak menyediakan visibilitas terhadap perilaku pengguna individual. Lebih lanjut, Hendrian dan Trisativa (2023) mengusulkan penerapan CAPsMAN (Controlled Access Point system Manager) pada jaringan nirkabel sekolah menengah dan menemukan bahwa sentralisasi manajemen AP dengan pembatasan bandwidth terbukti meningkatkan stabilitas jaringan secara keseluruhan [7].

Aspek keamanan autentikasi wireless juga menjadi pertimbangan penting dalam desain jaringan laboratorium. Siregar et al. (2023) mengimplementasikan sistem hotspot berbasis voucher pada jaringan RT/RW Net menggunakan MikroTik dan menemukan bahwa kombinasi WPA2-PSK dengan autentikasi captive portal memberikan lapisan keamanan ganda yang efektif WPA2 mencegah akses tanpa kredensial WiFi, sementara captive portal memastikan hanya pengguna terdaftar yang dapat mengakses internet [8]. Pendekatan berlapis ini sejalan dengan prinsip defense-in-depth dalam keamanan jaringan dan cocok diterapkan pada lingkungan laboratorium dengan pengguna yang heterogen.

Dari tinjauan literatur yang ada, dapat diidentifikasi bahwa penelitian terdahulu umumnya berfokus pada satu aspek manajemen jaringan baik bandwidth, autentikasi, atau monitoring secara terpisah. Belum banyak penelitian yang mendokumentasikan implementasi terpadu ketiga aspek tersebut dalam satu infrastruktur MikroTik pada konteks laboratorium komputer perguruan tinggi di Indonesia. Penelitian ini mengisi celah tersebut dengan mendokumentasikan implementasi komprehensif yang mencakup manajemen konektivitas, bandwidth, dan autentikasi pengguna secara simultan pada laboratorium Fasilkom Ubhara.

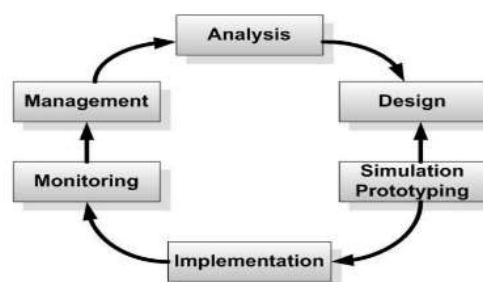
**Tabel 1 Perbandingan Kondisi Jaringan Sebelum dan Sesudah Implementasi MikroTik**

Aspek	Kondisi Sebelumnya	Setelah Implementasi
Manajemen Bandwidth	Tidak ada pembatasan	Simple Queue 5M/5M per segmen
Autentikasi Pengguna	Terbuka, tanpa login	Hotspot captive portal (WPA2 + web login)
Cakupan Wireless	Terbatas (provider ISP)	AP MikroTik wlan1, SSID Lab Siber
Monitoring Pengguna	Tidak tersedia	Address list dinamis + log MikroTik
DNS	Default ISP	8.8.8.8 & 8.8.4.4 (Google DNS)

### 3 Metode Penelitian (or Research Method)

Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) yang terdiri dari enam tahapan iteratif: *Analysis, Design, Simulation, Implementation, Monitoring, dan Management* [8].

NDLC dipilih karena pendekatannya yang sistematis dan berorientasi pada siklus hidup pengembangan jaringan, sehingga setiap tahapan menghasilkan deliverable yang terverifikasi sebelum melanjutkan ke tahap berikutnya [9].



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

**Gambar 1. Tahapan *Network Development Life Cycle***

Pada tahap Analysis, dilakukan observasi langsung terhadap kondisi jaringan laboratorium komputer Fasilkom Ubhara yang sedang berjalan. Identifikasi masalah mencakup: ketidakmampuan administrator mengontrol alokasi bandwidth, tidak adanya mekanisme autentikasi pengguna, dan ketergantungan penuh pada konfigurasi ISP provider. Data dikumpulkan melalui observasi trafik jaringan dan wawancara dengan administrator laboratorium dan pengguna aktif (mahasiswa dan dosen). Pada tahap Design, dirancang topologi jaringan baru dengan MikroTik sebagai router utama yang menghubungkan koneksi ISP (ether1/WAN) ke segmen LAN kabel (ether2, subnet 192.168.20.0/24) dan segmen wireless (wlan1, subnet 192.168.40.0/24). Desain mencakup skema pengalamatan IP, konfigurasi DHCP server untuk kedua segmen, aturan NAT Masquerade, Simple Queue untuk pembatasan bandwidth, dan hotspot server pada antarmuka wireless.

Pada tahap Simulation, topologi yang dirancang diverifikasi secara konseptual menggunakan Packet Tracer untuk memastikan routing antar subnet berjalan dengan benar sebelum implementasi fisik. Tahap Implementation dilakukan langsung pada perangkat MikroTik RB941-2nD di laboratorium Fasilkom Ubhara menggunakan WinBox v3.41 sebagai antarmuka konfigurasi. Urutan implementasi mengikuti dependensi konfigurasi: (1) Identity dan DNS, (2) DHCP Client pada WAN, (3) IP address dan DHCP Server pada LAN dan WLAN, (4) Firewall NAT, (5) Simple Queue, (6) Wireless AP dan Security Profile, serta (7) Hotspot Setup. Pada tahap Monitoring, seluruh fungsi yang diimplementasikan diuji menggunakan skenario pengujian terstruktur. Tahap Management menetapkan prosedur pemeliharaan rutin oleh administrator laboratorium.

**Tabel 2 Spesifikasi Teknis Implementasi**

Parameter	Nilai / Keterangan
Perangkat Router	MikroTik RB941-2nD (hAP lite)
Sistem Operasi	MikroTik RouterOS v6.42.11
Interface WAN	ether1 — DHCP Client (ISP), IP: 192.168.30.95/23
Interface LAN	ether2 — IP: 192.168.20.1/24, DHCP Server
Interface Wireless	wlan1 — IP: 192.168.40.1/24, Mode: AP Bridge
SSID	Lab Siber
Enkripsi Wireless	WPA2-PSK (AES-CCMP)
DNS Server	Primary: 8.8.8.8   Secondary: 8.8.4.4
Bandwidth Limit	Upload: 5 Mbps   Download: 5 Mbps (Simple Queue)
Hotspot Domain	labsiber.com
Hotspot Akun Uji	Username: siber   Password: labsiber123
ISP / Koneksi Masuk	CBN Jakarta (Moratelindo), IP: 119.235.210.178

#### 4 Hasil dan Pembahasan (or Results and Analysis)

Implementasi dilakukan secara bertahap mengikuti urutan yang telah ditetapkan pada metodologi. Pada tahap awal, MikroTik dikonfigurasi dengan identitas "Lab Siber" untuk memudahkan identifikasi perangkat dalam jaringan. DNS server ditetapkan menggunakan layanan Google Public DNS (8.8.8.8 dan 8.8.4.4) dengan opsi Allow Remote Requests diaktifkan agar klien lokal dapat menggunakan MikroTik sebagai DNS resolver, sehingga mengurangi dependensi terhadap DNS dari provider ISP yang dapat mengalami gangguan.

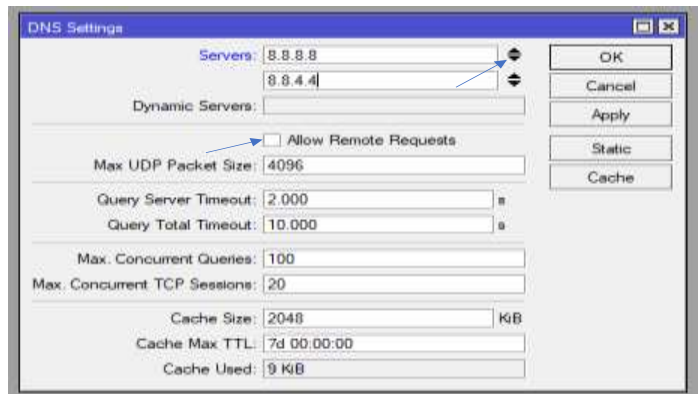
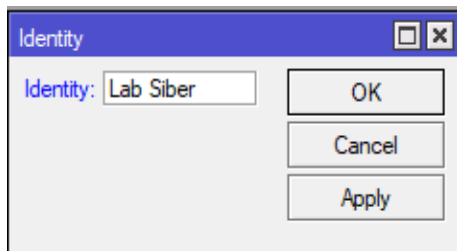


DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

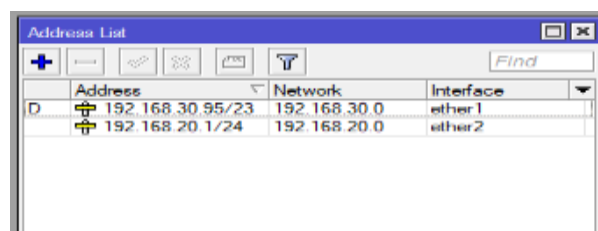
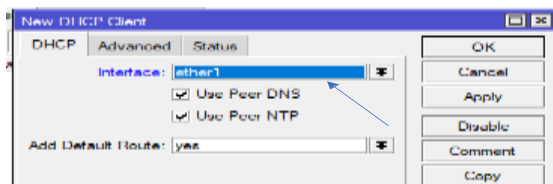
This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>



Konfigurasi DHCP Client pada ether1 berhasil memperoleh alamat IP dinamis dari ISP (192.168.30.95/23) secara otomatis. Hal ini dikonfirmasi melalui terminal Mikrotik dengan perintah ping 8.8.8.8 yang menghasilkan 14 paket terkirim dengan packet loss 0% dan rata-rata round-trip time sebesar 1 ms, menunjukkan konektivitas WAN yang stabil. Selanjutnya, DHCP Server dikonfigurasi pada ether2 dengan pool alamat 192.168.20.0/24 dan gateway 192.168.20.1. Pengujian pada PC klien yang terhubung melalui kabel ethernet mengkonfirmasi bahwa komputer memperoleh alamat IP 192.168.20.254 secara otomatis dengan gateway dan DNS yang benar. Uji konektivitas dari PC klien menggunakan perintah ping 8.8.8.8 menghasilkan rata-rata 3 ms dengan packet loss 0%, membuktikan bahwa NAT Masquerade berfungsi dengan benar dalam meneruskan trafik dari jaringan lokal ke internet.



Konfigurasi Simple Queue dengan nama "Lab Siber" diterapkan pada antarmuka ether2 dengan batas maksimum 5 Mbps untuk upload maupun download. Efektivitas pembatasan ini diverifikasi menggunakan speedtest.net dari PC klien, yang menghasilkan kecepatan download 4,31 Mbps dan upload 4,72 Mbps. Nilai ini berada di bawah batas yang ditetapkan (5 Mbps) dengan selisih yang wajar akibat overhead protokol TCP/IP, membuktikan bahwa Simple Queue berfungsi efektif. Tanpa pembatasan ini, koneksi klien berpotensi mengkonsumsi seluruh kapasitas bandwidth ISP dan merugikan pengguna lain dalam jaringan yang sama.



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).  
<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>



Pada segmen wireless, antarmuka wlan1 dikonfigurasi dalam mode AP Bridge dengan SSID "Lab Siber" pada band 2.4 GHz (B/G). Security Profile ditetapkan menggunakan autentikasi WPA2-PSK dengan enkripsi AES-CCMP, yang merupakan standar keamanan WiFi terkini untuk mencegah akses tidak sah ke jaringan nirkabel. Pengujian dari smartphone mengkonfirmasi bahwa SSID "Lab Siber" terdeteksi dan dapat dihubungkan menggunakan password yang ditetapkan. IP address 192.168.40.1/24 ditetapkan pada wlan1, diikuti konfigurasi DHCP Server kedua untuk segmen wireless agar klien wireless memperoleh alamat IP secara otomatis dari pool yang berbeda dengan segmen LAN kabel.



Sistem Hotspot dikonfigurasi pada antarmuka wlan1 dengan nama domain labsiber.com. Mekanisme ini mengimplementasikan captive portal yang secara otomatis mengalihkan semua permintaan HTTP dari klien yang belum terautentikasi ke halaman login labsiber.com. Tabel 3 menunjukkan konfigurasi akun pengguna hotspot yang dibuat.

**Tabel 3 Konfigurasi Akun Pengguna Hotspot**

Username	Password	Profile	Server	Keterangan
admin	admin	default	hotspot1	Administrator sistem, akses penuh
siber	labsiber123	default	hotspot1	Pengguna laboratorium (mahasiswa/teknisi)

Pengujian hotspot dilakukan dari smartphone yang terhubung ke SSID "Lab Siber". Setelah terhubung, browser secara otomatis dialihkan ke halaman captive portal labsiber.com yang menampilkan form login. Login menggunakan kredensial "siber/labsiber123" berhasil dilakukan, dan akses internet tersedia setelah autentikasi. Mekanisme ini secara efektif memastikan bahwa hanya



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

pengguna dengan kredensial yang valid dapat menggunakan jaringan internet laboratorium, sekaligus memberikan administrator kemampuan untuk mencabut akses sewaktu-waktu melalui panel manajemen hotspot MikroTik.



Secara keseluruhan, seluruh skenario pengujian yang direncanakan menghasilkan status berhasil sebagaimana dirangkum dalam Tabel 4. Implementasi MikroTik secara fundamental mengubah posisi administrator dari sebelumnya tidak memiliki kendali atas jaringan menjadi memiliki visibilitas dan kontrol penuh terhadap seluruh aspek jaringan laboratorium, mulai dari alokasi bandwidth hingga autentikasi pengguna.

**Tabel 4 Rekapitulasi Hasil Pengujian**

Skenario Pengujian	Metode Uji	Hasil	Status
Konektivitas MikroTik ke Internet	ping 8.8.8.8 interval=0.2s	14 paket terkirim, 0% packet loss, avg-rtt=1ms	Berhasil ✓
Konektivitas PC Client (kabel)	ping 8.8.8.8 dari CMD	4 paket terkirim, 0% loss, avg=3ms	Berhasil ✓
DHCP assignment client kabel	ipconfig pada PC	IP: 192.168.20.254, Gateway: 192.168.20.1	Berhasil ✓

[1] M. Yasir, A. Hidayat, D. Handayani, R. Suraji, H. Lubis, and F. Sinlae, "Penerapan Simple Queue Berbasis Mikrotik Dengan Fitur Notifikasi Telegram Dalam Pengelolaan Bandwidth Di Laboratorium Fasilkom Ubhara," vol. 9, no. 2, pp. 359–368, 2025, doi: 10.52362/jisicom.v9i2.2076.

Pembatasan bandwidth (Simple Queue)

SpeedTest.net dari client  
Download: 4.31 Mbps, Upload: 4.72 Mbps (limit 5M) Berhasil ✓



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

Koneksi WiFi (wlan1)	Scan WiFi dari smartphone	dari SSID "Lab Siber" terdeteksi, koneksi WPA2-PSK	Berhasil ✓
Autentikasi Hotspot (captive portal)	Login labsiber.com	via Redirect ke portal, login user siber berhasil	Berhasil ✓
DHCP assignment client wireless	Cek IP setelah login hotspot	IP dari pool 192.168.40.0/24	Berhasil ✓

Dibandingkan dengan kondisi sebelum implementasi, terdapat perbedaan yang signifikan dalam kemampuan pengelolaan jaringan. Sebelumnya, administrator tidak memiliki alat untuk memonitor siapa saja yang menggunakan jaringan atau berapa banyak bandwidth yang dikonsumsi. Dengan MikroTik, administrator dapat mengakses log koneksi hotspot, daftar klien aktif beserta IP address dan konsumsi data masing-masing, serta mengubah kebijakan bandwidth secara real-time tanpa memerlukan intervensi dari pihak ISP. Hal ini sejalan dengan temuan Herawan dan Prihantoro (2024) yang menyimpulkan bahwa MikroTik memberikan fleksibilitas manajemen yang tidak tersedia pada solusi ISP konvensional [5].

## 5 Kesimpulan (or Conclusion)

Penelitian ini berhasil mengimplementasikan infrastruktur jaringan WLAN berbasis MikroTik RouterOS pada laboratorium komputer Fasilkom Ubhara yang mencakup tiga komponen utama secara terpadu. Pertama, konektivitas internet yang stabil berhasil dibangun melalui konfigurasi DHCP Client, DNS publik Google, dan NAT Masquerade, dengan hasil pengujian menunjukkan packet loss 0% dan rata-rata latensi 1 ms pada sisi router serta 3 ms pada sisi klien. Kedua, mekanisme pembatasan bandwidth melalui Simple Queue berhasil diterapkan dengan batas 5 Mbps per segmen, yang terkonfirmasi dari hasil speedtest sebesar 4,31 Mbps download dan 4,72 Mbps upload menunjukkan bahwa alokasi bandwidth kini dapat dikendalikan secara mandiri oleh administrator tanpa bergantung pada ISP. Ketiga, sistem hotspot captive portal berhasil diimplementasikan pada segmen wireless dengan autentikasi berbasis username/password melalui domain labsiber.com, yang memastikan hanya pengguna terautentikasi yang dapat mengakses internet dari jaringan laboratorium.

Implementasi ini secara menyeluruh mengatasi permasalahan yang diidentifikasi pada kondisi awal: ketidakmampuan mengontrol bandwidth, tidak adanya autentikasi pengguna, dan ketiadaan visibilitas jaringan. Untuk pengembangan selanjutnya, disarankan agar penelitian berikutnya mengeksplorasi implementasi CAPsMAN untuk manajemen multi-access point yang terpusat, integrasi RADIUS server untuk autentikasi yang lebih skalabel, serta penerapan Quality of Service (QoS) berbasis Queue Tree untuk diferensiasi prioritas trafik yang lebih granular sesuai dengan jenis penggunaan jaringan di laboratorium akademik.

## Referensi (Reference)

- [1] Y. Hendrian and Z. A. Trisativa, "Desain dan manajemen jaringan nirkabel SMK Harapan Bangsa dengan penerapan CAPsMAN dan pembatasan bandwidth," SATIN - Sains dan Teknologi Informasi, vol. 9, no. 1, pp. 82–92, Jun. 2023, doi: 10.33372/stn.v9i1.864.
- [2] S. Dwiyatno, A. D. Jubaedi, Y. Ferdiansyah, and E. Krisnaningsih, "Implementasi user manager MikroTik dalam authentication login pada hotspot," JISICOM, vol. 7, no. 1, pp. 145–157, 2023.
- [3] M. H. Siregar et al., "Implementation of RT/RW Net hotspot network with MikroTik-based voucher system at Unitex Bogor Housing," JISICOM, vol. 7, no. 2, pp. 487–497, 2023, doi: 10.52362/jisicom.v7i2.1332.



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>

DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

- [4] R. M. Herawan and C. Prihantoro, "Implementasi pengembangan sistem jaringan internet PT. Inka Multi Solusi Service berbasis router MikroTik," *Jurnal PROVISI*, vol. 15, no. 1, pp. 53–60, 2024.
- [5] R. M. Herawan and C. Prihantoro, "Implementasi pengembangan sistem jaringan internet berbasis router MikroTik," vol. 15, no. 1, pp. 53–60, 2024.
- [6] S. Dwiyatno, A. D. Jubaedi, Y. Ferdiansyah, and E. Krisnaningsih, "Implementasi user manager MikroTik dalam authentication login pada hotspot," *JISICOM*, vol. 7, no. 1, 2023.
- [7] Y. Hendrian and Z. A. Trisativa, "Desain dan manajemen jaringan nirkabel SMK Harapan Bangsa," *SATIN*, vol. 9, no. 1, pp. 82–92, 2023.
- [8] M. Yasir, A. Hidayat, D. Handayani, R. Suraji, H. Lubis, and F. Sinlae, "Penerapan Simple Queue Berbasis Mikrotik Dengan Fitur Notifikasi Telegram Dalam Pengelolaan Bandwidth Di Laboratorium Fasilkom Ubhara" vol. 9, no. 2, pp. 359–368, 2025, doi: 10.52362/jisicom.v9i2.2076.
- [9] M. H. Siregar et al., "Implementation of RT/RW Net hotspot network with MikroTik-based voucher system," *JISICOM*, vol. 7, no. 2, pp. 487–497, 2023.
- [10] K. T. Dewo, V. Yasin, T. Budiman, A. Z. Sianipar, and A. B. Yulianto, "IT infrastructure dashboard monitoring application development using Grafana and Prometheus," in *Proc. ICOSNIKOM*, 2023, pp. 1–5, doi: 10.1109/ICoSNiKOM60230.2023.10364485.
- [11] V. Yasin et al., "Disaster control system for landslides using Sugeno Fuzzy algorithm," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 6, 2024.
- [12] H. Iswanto, V. Yasin, J. Johan, and R. Hartawan, "Monitoring application for submission of PBJ transaction reports on PPATK," *JISICOM*, vol. 7, no. 1, pp. 179–187, 2023.
- [13] M. Usnaini, V. Yasin, and A. Z. Sianipar, "Perancangan sistem informasi inventarisasi aset berbasis web menggunakan metode waterfall," *J. Manajemen Informatika Jayakarta*, vol. 1, no. 1, pp. 36–55, 2021.
- [14] A. Mardian, T. Budiman, R. Haroen, and V. Yasin, "Perancangan aplikasi pemantauan kinerja karyawan berbasis Android di PT. Salestrade Corp. Indonesia," *J. Manajemen Informatika Jayakarta*, vol. 1, no. 3, pp. 169–185, 2021.
- [15] V. Yasin, P. Peniarsih, A. Gozali, and I. Junaedi, "Application of expert system diagnosis of color blindness with Ishihara method," *Int. J. Informatics, Econ. Manag. Sci.*, vol. 1, no. 1, pp. 13–31, 2022.
- [16] A. V. Vitianingsih, C. Ullum, A. L. Maukar, V. Yasin, and S. F. A. Wati, "Mapping residential land suitability using a WEB-GIS-based multi-criteria spatial analysis approach," *J. RESTI*, vol. 8, no. 2, pp. 208–215, 2024.



DOI: <https://doi.org/10.52362/jmijayakarta.v6i.2390>

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

<http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta>