



EFEKTIVITAS MAC ADDRESS FILTERING SEBAGAI SISTEM KEAMANAN TRANSFER DATA PADA JARINGAN WIRELESS

Aditya Bayu Anugrah^{1*}, Neilcy Tjahjamoonsih², Jannus Marpaung³

^{1,2,3}Program Studi Teknik Elektro, Fakultas Teknik,
Universitas Tanjungpura Pontianak

¹d1021211099@student.untan.ac.id, ²neilcy.mooniarsih@ee.untan.ac.id,

³jannus.marpaung@ee.untan.ac.id,

Abstract

Wireless networks are highly vulnerable to security threats, particularly unauthorized access. PT Borneo Cakrawala Media currently relies on the WPA2-PSK security mechanism, which has certain limitations. This study aims to implement MAC Address Filtering as an additional security mechanism for a wireless network. The research methodology includes the design, configuration, and testing of MAC Address Filtering using a Mikrotik RB750GR3 router and a Ruijie RG-720L access point. The tests were conducted on registered and unregistered device access, device addition and removal, false positive and false negative cases, MAC Address Spoofing handling, and network performance evaluation using Quality of Service (QoS) parameters based on the TIPHON standard. The results indicate that MAC Address Filtering is capable of accurately verifying registered devices and rejecting unauthorized devices, managing MAC Address addition and removal, and handling false positive and false negative cases with a 100% success rate without significantly degrading network performance. Furthermore, the MAC Address Spoofing tests demonstrate that the system can distinguish devices even when identical or similar MAC Addresses are used. It can be concluded that MAC Address Filtering is effective as an additional security mechanism for protecting wireless networks.

Keywords: Network Security, Wireless Network, MAC Address Filtering, MAC Address spoofing, Quality of Service.

Article History

Received: January 2026

Reviewed: January 2026

Published: January 2026

Plagiarism Checker No: 235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



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



Abstrak

Jaringan *wireless* memiliki risiko keamanan yang tinggi terhadap akses tidak sah. PT Borneo Cakrawala Media masih menggunakan sistem keamanan WPA2-PSK yang memiliki keterbatasan. Penelitian ini bertujuan menerapkan *MAC Address Filtering* sebagai sistem keamanan tambahan pada jaringan *wireless*. Metode penelitian meliputi perancangan, konfigurasi, dan pengujian *MAC Address Filtering* menggunakan router Mikrotik RB750GR3 dan *access point* Ruijie RG-720L. Pengujian dilakukan terhadap akses perangkat terdaftar/tidak terdaftar, penambahan dan penghapusan perangkat, kasus *false positive* dan *negative*, penanganan *MAC Address Spoofing*, serta evaluasi performansi jaringan menggunakan parameter *Quality of Service* (QoS) berdasarkan standar TIPHON. Hasil penelitian menunjukkan bahwa *MAC Address Filtering* mampu memverifikasi perangkat terdaftar atau menolak perangkat tidak sah, penambahan atau penghapusan *MAC Address*, kasus *false positive* dan *negative* dengan tingkat keberhasilan 100% tanpa menurunkan performansi jaringan secara signifikan dan juga hasil dari pengujian *MAC Address Spoofing* mampu membedakan perangkat walaupun *MAC Address*nya sama atau mirip. Dapat disimpulkan bahwa *MAC Address Filtering* efektif digunakan sebagai sistem keamanan tambahan untuk melindungi jaringan *wireless*.

Kata Kunci: Keamanan Jaringan, Jaringan Wireless, *MAC Address Filtering*, *MAC Address Spoofing*, *Quality of Service*.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong pemanfaatan jaringan nirkabel (*wireless*) secara luas di berbagai sektor, mulai dari perkantoran hingga industri manufaktur. Jaringan *wireless* menawarkan sejumlah keunggulan, seperti fleksibilitas penggunaan, kemudahan instalasi, serta efisiensi biaya dibandingkan jaringan berbasis kabel. Namun, di balik keunggulan tersebut, jaringan *wireless* memiliki tingkat kerentanan yang relatif tinggi terhadap berbagai ancaman keamanan, antara lain akses tidak sah, penyadapan data, dan penyalahgunaan jaringan oleh pihak yang tidak berwenang.

Salah satu mekanisme keamanan yang paling umum diterapkan pada jaringan *wireless* adalah *Wi-Fi Protected Access 2* dengan *Pre-Shared Key* (WPA2-PSK), yang mengandalkan autentikasi berbasis kata sandi. Meskipun metode ini cukup efektif dalam membatasi akses pengguna awam, sistem berbasis kata sandi memiliki beberapa kelemahan, seperti kecenderungan kata sandi untuk dibagikan, kerentanan terhadap serangan *brute force*, serta potensi eksploitasi melalui teknik *spoofing*. Kelemahan tersebut dapat meningkatkan risiko kebocoran data dan gangguan layanan jaringan, khususnya pada lingkungan organisasi dengan jumlah pengguna yang besar.

Saat ini, PT Borneo Cakrawala Media (BCMedia) masih mengandalkan WPA2-PSK sebagai satu-satunya mekanisme keamanan pada jaringan *wireless*. Meskipun belum terjadi insiden keamanan yang serius, telah terdeteksi beberapa upaya koneksi dari perangkat asing pada jaringan internal perusahaan, yang menunjukkan adanya potensi ancaman terhadap keamanan jaringan. Kondisi ini mengindikasikan bahwa sistem keamanan yang digunakan masih memiliki celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, sehingga diperlukan penambahan lapisan keamanan untuk memperketat kontrol akses perangkat.



Salah satu solusi yang dapat diterapkan sebagai mekanisme keamanan tambahan adalah *MAC Address Filtering*, yaitu metode yang membatasi akses jaringan hanya kepada perangkat dengan alamat MAC (*Media Access Control*) yang telah terdaftar dalam daftar putih (*whitelist*). Dengan mekanisme ini, meskipun seseorang mengetahui kata sandi *Wi-Fi*, perangkat tersebut tetap tidak dapat mengakses jaringan apabila alamat MAC-nya tidak terdaftar. Penerapan *MAC Address Filtering* diharapkan dapat meningkatkan kontrol akses perangkat, mengurangi risiko akses tidak sah, serta menambah lapisan perlindungan pada jaringan *wireless*.

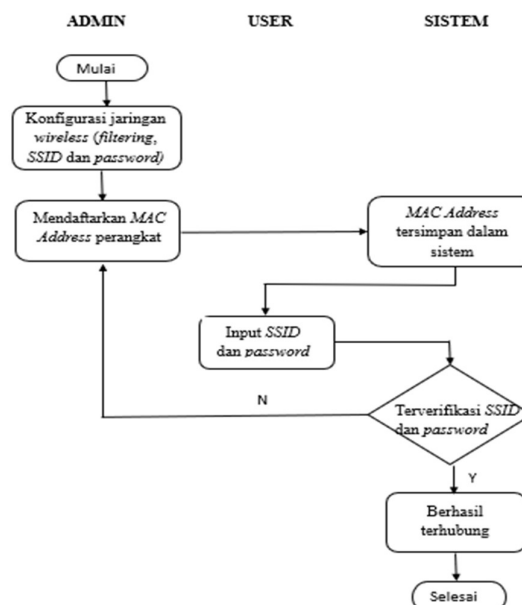
Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis efektivitas *MAC Address Filtering* sebagai sistem keamanan tambahan pada jaringan *wireless* di PT Borneo Cakrawala Media. Analisis dilakukan dengan mengevaluasi kemampuan sistem dalam memverifikasi perangkat terdaftar, menolak perangkat tidak sah, menangani skenario serangan *MAC Address spoofing*, serta menilai dampaknya terhadap performansi jaringan berdasarkan parameter *Quality of Service* (QoS). Hasil penelitian ini diharapkan dapat memberikan gambaran empiris mengenai tingkat efektivitas *MAC Address Filtering* dan menjadi bahan pertimbangan dalam perancangan sistem keamanan jaringan *wireless* yang lebih andal.

2. METODE PENELITIAN

Pada metode penelitian ini menjelaskan langkah-langkah yang akan dilakukan dalam penelitian tentang penerapan sistem keamanan *MAC Address Filtering* sebagai meningkatkan keamanan koneksi jaringan di PT.BCMedia. Metode penelitian ini dirancang tidak hanya untuk mengimplementasikan sistem *MAC Address Filtering*, tetapi juga untuk mengevaluasi efektivitas sistem sebagai mekanisme keamanan jaringan. Evaluasi dilakukan melalui pengujian fungsional sistem keamanan dan analisis performansi jaringan menggunakan parameter *Quality of Service* (QoS).

2.1 Perancangan Sistem

Sejalan dengan hasil analisis kebutuhan pada tahap sebelumnya, tugas akhir ini merancang sebuah sistem keamanan yang bertujuan membatasi perangkat yang dapat mengakses jaringan internet. Sistem yang diusulkan menerapkan metode *MAC Address Filtering*, di mana setiap perangkat seperti laptop dan *smartphone* harus didaftarkan terlebih dahulu kepada administrator sebelum diizinkan terhubung ke jaringan *Wi-Fi*. Rancangan sistem yang diusulkan ditampilkan pada **Gambar 1**.



Gambar 1. Sistem Yang Diusulkan

2.2 Perancangan Dan Konfigurasi Sistem

Pada tahap implementasi, konfigurasi jaringan dilakukan untuk menerapkan sistem keamanan yang telah dirancang. Winbox digunakan untuk melakukan pengaturan pada MikroTik RouterBoard, sementara Ruijie Cloud dimanfaatkan untuk mengelola *access point* serta mengaktifkan fitur *MAC Address Filtering*.

Konfigurasi awal mencakup pengaturan *DHCP Client* agar *router* memperoleh alamat IP secara otomatis dari ISP. Selanjutnya dilakukan pengaturan alamat IP, dengan antarmuka WAN menggunakan IP dinamis dan antarmuka LAN menggunakan IP lokal. Beberapa *port Ethernet* digabungkan melalui konfigurasi *bridge*, kemudian DNS diatur menggunakan Google DNS (8.8.8.8). Fitur NAT dengan metode *masquerade* diaktifkan untuk memungkinkan perangkat dalam jaringan mengakses internet.

DHCP Server kemudian dikonfigurasi untuk mendistribusikan alamat IP secara otomatis kepada perangkat yang terhubung. Konektivitas jaringan diuji menggunakan perintah ping untuk memastikan jaringan berjalan dengan baik. *Access point* diadopsi melalui Ruijie Cloud dengan mendaftarkan nomor seri perangkat dan mengatur akun administrator, kemudian memperoleh alamat IP dari *DHCP Server* MikroTik.

Pengaturan jaringan nirkabel dilakukan dengan menentukan SSID dan parameter keamanan pada frekuensi 2,4 GHz dan 5 GHz. Selanjutnya, *MAC Address Filtering* diterapkan menggunakan mekanisme *whitelist*, sehingga hanya perangkat dengan alamat MAC terdaftar yang diizinkan terhubung ke jaringan, sedangkan perangkat lain secara otomatis ditolak untuk menjaga keamanan jaringan.

2.3 Pengujian Efektivitas *MAC Address Filtering*

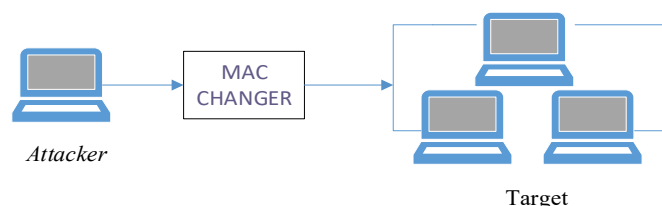
Pada tahap ini akan dilakukan skenario pengujian yang bertujuan untuk menguji suatu sistem, perangkat, atau metode yang dikembangkan dapat berjalan sesuai dengan fungsinya dan memenuhi tujuan yang telah ditentukan. Berikut skenario pengujian yang akan dilakukan yaitu

a) Verifikasi *MAC Address Filtering* Pada Sistem Sistem Keamanan Jaringan

Pada tahap inisiasi, sistem diuji dan menunjukkan kinerja yang berjalan dengan baik. Pengujian ini bertujuan untuk memastikan bahwa mekanisme *MAC Address Filtering* mampu mengizinkan perangkat yang terdaftar dalam *whitelist* serta menolak perangkat yang tidak terdaftar. Selain itu, sistem juga diuji dalam mendukung proses penambahan dan penghapusan alamat MAC, serta untuk memastikan tidak terjadinya kesalahan klasifikasi berupa *false positive* maupun *false negative*. Pengujian dilakukan menggunakan empat perangkat.

Parameter kinerja yang diamati adalah tingkat keberhasilan penyaringan *MAC Address*, yang diukur berdasarkan persentase perangkat yang berhasil diizinkan atau diblokir sesuai dengan daftar *whitelist*. Skenario pengujian meliputi akses perangkat terdaftar yang berhasil terhubung ke jaringan, penolakan perangkat yang tidak terdaftar, keberhasilan proses penambahan dan penghapusan alamat MAC sesuai perubahan yang dilakukan, serta verifikasi bahwa tidak terjadi penolakan terhadap perangkat valid maupun penerimaan perangkat yang tidak valid.

b) Inisiasi Pengujian Penanganan *MAC Address Spoofing*



Gambar 2. Proses *MAC Address Spoofing*



MAC Address Spoofing adalah tindakan memalsukan atau mengubah alamat MAC dari sebuah perangkat jaringan agar tampak seperti perangkat lain. Alamat MAC bisa diubah (*spoofing*) menggunakan perintah sistem, dengan begitu perangkat bisa menyamar sebagai perangkat lain dalam jaringan.

c) Pengujian Peformansi Jaringan

Pada tahap pengujian performansi jaringan melihat apakah *MAC Address Filtering* memberikan dampak negative pada kecepatan dan latensi jaringan. Parameter kinerja yang akan digunakan yaitu dengan metode QoS (*Quality Of Service*) dengan perangkat lunak wireshark.

Setelah data dikumpulkan maka data tersebut diolah untuk mengetahui kategori kualitas *throughput*, *packet loss*, *delay* dan *jitter* dengan menggunakan standar dari TIPHON. Pada standar tersebut menjelaskan perhitungan dan indeks karakteristik dari *throughput*, *packet loss*, *delay* dan *jitter*. Kategori pada setiap parameter tersebut terdiri dari empat kategori kualitas layanan seperti sangat bagus, bagus, sedang dan buruk. Berdasarkan setiap nilai yang didapatkan dari empat parameter *Quality of Service*.

2.4 Analisis Efektivitas Sistem Keamanan Jaringan

Analisis dilakukan untuk menilai efektivitas *MAC Address Filtering* dalam membatasi akses perangkat dan menghadapi serangan *MAC spoofing*. Tahap ini juga mengevaluasi potensi kelemahan atau celah keamanan yang masih mungkin terjadi.

3. HASIL DAN PEMBAHASAN

Bagian ini mengevaluasi penerapan sistem keamanan jaringan nirkabel berbasis *MAC Address Filtering* untuk memastikan efektivitas, akurasi, serta dampaknya terhadap kinerja jaringan. Pengujian dilakukan secara langsung pada *access point* dengan menggunakan empat perangkat uji, yang terdiri dari perangkat terdaftar (*whitelist*) dan perangkat tidak terdaftar.

3.1 Verifikasi *MAC Address Filtering* Pada Sistem Keamanan Jaringan

Pengujian pertama dilakukan untuk memastikan fungsi dasar *MAC Address Filtering* bekerja dengan baik. Pada tahap ini ada 3 pengujian yang akan dilakukan yaitu akses perangkat terdaftar dan penolakan perangkat tidak terdaftar, penambahan/penghapusan MAC dan kasus *false positive/negative*.

Tabel 1. Hasil Pengujian Verifikasi *MAC Address Filtering*

No	Skenario Pengujian	Langkah Uji	Hasil yang Diharapkan	Hasil Pengujian
1	Akses Perangkat Terdaftar dan Penolakan Perangkat Tidak Terdaftar	-Perangkat yang <i>MAC Address</i> -nya terdaftar di <i>whitelist</i> mencoba mengakses <i>Wi-Fi</i> . -Perangkat lain yang tidak terdaftar mencoba mengakses <i>Wi-Fi</i> .	-Perangkat terdaftar dapat terhubung. -Perangkat tidak terdaftar ditolak oleh sistem.	Perangkat terdaftar berhasil terhubung ke jaringan, sedangkan perangkat tidak terdaftar gagal terhubung.
2	Penambahan <i>MAC Address</i> ke <i>Whitelist</i>	Menambahkan alamat <i>MAC</i> baru melalui menu <i>Add Users</i> pada daftar <i>whitelist</i>	Perangkat yang baru ditambahkan dapat langsung terhubung ke <i>Wi-Fi</i> .	Perangkat berhasil terkoneksi setelah <i>MAC Address</i> ditambahkan ke <i>whitelist</i> .



	Penghapusan MAC Address Dari Whitelist	Menghapus MAC Address perangkat dari daftar <i>whitelist</i> .	Perangkat yang dihapus tidak dapat lagi akses ke WiFi	Setelah dihapus, perangkat tidak dapat terhubung ke jaringan.
3	Kasus <i>False Positve</i>	Menguji apakah perangkat yang valid (terdaftar) ditolak oleh sistem	Sistem seharusnya tidak menolak perangkat valid.	Tidak ditemukan kasus <i>false positive</i> .
	Kasus <i>False Negative</i>	Menguji apakah perangkat tidak terdaftar dapat terhubung ke jaringan.	Sistem seharusnya menolak perangkat yang tidak terdaftar.	Tidak ditemukan kasus <i>false negative</i> .

Berdasarkan seluruh rangkaian pengujian yang dilakukan, yang mencakup pengujian akses perangkat terdaftar dan tidak terdaftar, proses penambahan serta penghapusan *MAC Address*, hingga pengujian kasus *false positive* dan *false negative*, dapat disimpulkan bahwa seluruh fungsi sistem berjalan sesuai dengan konfigurasi yang telah dirancang. Setiap perangkat yang memang berhak memperoleh akses jaringan berhasil terhubung dengan baik, sedangkan perangkat yang tidak diizinkan secara konsisten ditolak oleh sistem.

Hasil tersebut menunjukkan bahwa penerapan fitur *MAC Address Filtering* mampu bekerja sebagaimana yang diharapkan. Mekanisme *whitelist* yang diterapkan terbukti efektif dan andal dalam membedakan antara perangkat sah dan perangkat tidak sah. Dengan demikian, sistem dapat dikatakan bekerja secara optimal dalam melakukan proses penyaringan, verifikasi, serta pengendalian akses perangkat terhadap jaringan Wi-Fi.

3.2 Inisiasi Pengujian Penanganan *MAC Address Spoofing*

Pengujian selanjutnya dilakukan untuk mengevaluasi ketahanan sistem terhadap ancaman *MAC Address Spoofing*, yaitu teknik pemalsuan alamat MAC agar menyerupai perangkat lain yang telah memiliki izin akses. Dalam pengujian ini, salah satu perangkat tidak terdaftar memodifikasi alamat MAC-nya agar sama dengan alamat MAC perangkat dalam *whitelist*. Tujuan pengujian adalah untuk menilai kemampuan sistem keamanan jaringan dalam menangani upaya pemalsuan alamat MAC pada jaringan nirkabel yang menerapkan *MAC Address Filtering*. Proses *spoofing* dilakukan menggunakan aplikasi seperti TMAC atau *Macchanger*. Pengujian dilakukan melalui dua skenario menggunakan perangkat laptop untuk mengamati respons sistem terhadap perangkat yang mencoba mengakses jaringan dengan alamat MAC hasil pemalsuan.

Tabel 2. Hasil Pengujian Inisiasi *MAC Address Spoofing*

No	Skenario Pengujian	Deskripsi Pengujian	Kondisi Alamat MAC	Hasil Pengujian
1	<i>Spoofing</i> dengan MAC Address yang Sama (<i>Cloning</i>)	Laptop mengubah alamat MAC Wi-Fi menjadi sama persis dengan perangkat sah yang terdaftar di <i>whitelist</i>	Dari D4:3B:04:94:64:B6 diubah menjadi 8A:95:41:2F:88:D5	Sistem mendeteksi perangkat berbeda meskipun alamat MAC sama. Status koneksi menolak (<i>rejected</i>)



2	<i>Spoofing</i> dengan MAC Address yang Hampir Sama	Laptop mengubah alamat MAC dengan mengubah bagian depan menjadi "02" namun 6 digit terakhir tetap sama	Dari D0-9C-7A-0D-85-4C diubah menjadi 02-9C-7A-0D-85-4C	Sistem menolak koneksi karena MAC berbeda dari <i>whitelist</i> . Status koneksi menolak (<i>rejected</i>)
---	---	--	---	--

3.3 Pengujian Performansi Jaringan

Selain aspek keamanan, pengujian performansi jaringan dilakukan untuk melihat dampak penerapan *MAC Address Filtering* terhadap kinerja jaringan. Parameter yang digunakan mengacu pada *Quality of Service (QoS)*, yaitu *throughput*, *delay*, *jitter*, dan *packet loss*. Data diambil menggunakan perangkat lunak Wireshark pada kondisi sebelum dan sesudah sistem *MAC Filtering* diaktifkan.

Tabel 3. Hasil Pengujian Performansi Jaringan

Kondisi	Parameter QoS	Nilai	Indeks	Kategori
Sebelum	<i>Throughput</i>	2.192k Kbits/s	4	Sangat Bagus
	<i>Packet Loss</i>	0,1%	4	Sangat Bagus
	<i>Delay</i>	4,674101 ms	4	Sangat Bagus
	<i>Jitter</i>	4,680727	3	Bagus
Sesudah	<i>Throughput</i>	14.381.296.527,96442 Kbits/s	4	Sangat Bagus
	<i>Packet Loss</i>	0,2%	4	Sangat Bagus
	<i>Delay</i>	0,65323 ms	4	Sangat Bagus
	<i>Jitter</i>	0,653711 ms	3	Bagus

Berdasarkan hasil pengujian, dapat disimpulkan bahwa penerapan *MAC Address Filtering* tidak memberikan pengaruh yang signifikan terhadap performa jaringan. Hal ini disebabkan karena mekanisme *MAC Address Filtering* hanya bekerja pada tahap autentikasi awal, yaitu ketika perangkat mencoba terhubung ke jaringan. Setelah perangkat berhasil terhubung, proses transmisi data berlangsung seperti biasa tanpa ada tambahan proses atau beban kerja yang dapat memengaruhi *throughput*, *delay*, *jitter*, maupun *packet loss*.

3.4 Analisis Efektivitas *MAC Address Filtering* Sebagai Sistem Keamanan

Analisis efektivitas penelitian ini bertujuan menilai sejauh mana *MAC Address Filtering* berfungsi sebagai sistem keamanan tambahan pada jaringan *wireless* di PT Borneo Cakrawala Media. Penilaian tidak hanya didasarkan pada keberhasilan konfigurasi teknis, tetapi juga pada kemampuan sistem dalam membatasi akses perangkat tidak sah, menjaga konektivitas perangkat terotorisasi, serta mempertahankan kestabilan kualitas transfer data. Efektivitas sistem dievaluasi melalui indikator seperti keberhasilan verifikasi perangkat, penolakan perangkat yang tidak terdaftar dalam *whitelist*, respons terhadap perubahan data *whitelist*, akurasi identifikasi perangkat, serta ketahanan terhadap potensi serangan *MAC Address Spoofing*.

Hasil pengujian menunjukkan bahwa *MAC Address Filtering* bekerja secara konsisten dalam memverifikasi perangkat. Seluruh perangkat yang terdaftar berhasil terhubung ke jaringan, sedangkan perangkat yang tidak terdaftar ditolak secara otomatis. Setiap perubahan pada data *whitelist* langsung memengaruhi status akses perangkat. Selain itu, tidak ditemukan kesalahan



identifikasi berupa *false positive* maupun *false negative* selama pengujian. Seluruh skenario menunjukkan tingkat keberhasilan 100%, yang menegaskan bahwa *MAC Address Filtering* efektif digunakan sebagai sistem keamanan tambahan untuk membatasi akses jaringan *wireless* dan melindungi proses transfer data dari perangkat yang tidak berwenang.

3.5 Analisis Efektivitas Terhadap Penanganan *MAC Address Spoofing*

Selain pengujian dasar kinerja sistem, penelitian ini juga mengevaluasi efektivitas *MAC Address Filtering* dalam menghadapi ancaman *MAC Address Spoofing*. Dalam skenario pengujian, sebuah perangkat yang tidak memiliki izin akses mengubah alamat MAC-nya agar menyerupai alamat MAC perangkat yang terdaftar dalam *whitelist* untuk mensimulasikan upaya penyusupan. Hasil pengujian menunjukkan bahwa meskipun alamat MAC berhasil diubah, sistem tidak memberikan akses penuh ke jaringan. *Access point* mendeteksi adanya kejanggalan pada proses koneksi, seperti konflik identitas perangkat dan ketidakkonsistenan status autentikasi, sehingga akses dibatasi. Temuan ini menunjukkan bahwa *MAC Address Filtering* tetap memberikan lapisan perlindungan tambahan terhadap upaya *spoofing*, meskipun belum sepenuhnya kebal terhadap serangan tingkat lanjut. Oleh karena itu, mekanisme ini lebih tepat digunakan sebagai lapisan keamanan awal dan perlu dikombinasikan dengan metode keamanan lain, seperti autentikasi berbasis pengguna, enkripsi yang lebih kuat, dan firewall, untuk meningkatkan ketahanan jaringan secara menyeluruh.

3.6 Analisis Efektivitas Terhadap Performansi Jaringan

Efektivitas sistem keamanan jaringan tidak hanya ditentukan oleh kemampuannya dalam mencegah akses tidak sah, tetapi juga oleh dampaknya terhadap kinerja jaringan. Oleh karena itu, penelitian ini mengevaluasi pengaruh penerapan *MAC Address Filtering* terhadap performansi jaringan *wireless* menggunakan parameter *Quality of Service (QoS)*, yaitu *throughput*, *delay*, *jitter*, dan *packet loss*. Hasil pengujian menunjukkan bahwa penerapan *MAC Address Filtering* tidak menimbulkan penurunan performansi yang signifikan. Nilai *throughput* tetap stabil dan berada dalam kategori baik berdasarkan standar TIPHON, sementara nilai *delay* dan *jitter* masih berada dalam batas toleransi yang dapat diterima. Selain itu, tingkat *packet loss* yang diperoleh tergolong rendah, sehingga tidak mengganggu kualitas layanan jaringan. Temuan ini menunjukkan bahwa *MAC Address Filtering* mampu meningkatkan keamanan jaringan dengan membatasi akses perangkat secara selektif tanpa mengorbankan kualitas layanan dan stabilitas performansi jaringan *wireless*.

KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, penerapan *MAC Address Filtering* pada *access point* Ruijie RG-AP720 L terbukti mampu meningkatkan keamanan jaringan *wireless* di PT Borneo Cakrawala Media dengan membatasi akses hanya kepada perangkat yang terdaftar dalam *whitelist*. Sistem dapat memverifikasi perangkat sah dan menolak perangkat yang tidak terdaftar secara konsisten, sehingga mencegah akses tidak berwenang ke jaringan perusahaan. Selain itu, proses penambahan dan penghapusan alamat MAC pada *whitelist* berjalan dengan baik dan diterapkan secara *real-time*, di mana perangkat yang ditambahkan langsung memperoleh akses, sedangkan perangkat yang dihapus otomatis ditolak oleh sistem.

Selama seluruh rangkaian pengujian, tidak ditemukan kesalahan identifikasi berupa *false positive* maupun *false negative*, yang menunjukkan bahwa sistem mampu mengenali perangkat secara akurat sesuai daftar *MAC Address* yang dikonfigurasi. Pengujian terhadap skenario *MAC Address Spoofing* menunjukkan bahwa *MAC Address Filtering* dapat berfungsi sebagai lapisan keamanan awal dengan membatasi akses perangkat yang tidak dikenali, meskipun masih memiliki keterbatasan apabila digunakan sebagai satu-satunya mekanisme keamanan. Selain itu, hasil pengukuran *Quality of Service (QoS)* menunjukkan bahwa penerapan *MAC Address Filtering*



tidak memberikan dampak signifikan terhadap *throughput*, *delay*, *jitter*, dan *packet loss*, sehingga kualitas layanan jaringan tetap berada pada kategori baik sesuai standar TIPHON.

DAFTAR PUSTAKA

- [1] L. D. Samsumar and S. Hadi, "Pengembangan Jaringan Komputer Jaringan Komputer Nirkabel (*WiFi*) Menggunakan Mikrotik Router (Studi Kasus Pada SMA PGRI Aikmel)," vol. 4, no. 1, pp. 1-9, 2018.
- [2] A. N. Bayu, "Analisis Keamanan Jaringan Pada Fasilitas Internet (*WiFi*) Terhadap Serangan *Packet Sniffing*," 2012.
- [3] D. Era Glnanti, A. Christian, and T. Hidayat, "Analisa Dan Implementasi Jaringan *Wireless MAC Address* Menggunakan *Filtering* Pada PT.Faya Kuntura Agung Konsultindo," vol. 16, no. 2, pp. 79-84, 2022.
- [4] Irsan, "Keamanan Jaringan *Wireless Lan* Dengan Metode *MAC Address Filtering* Di SDN Kunciran 8," vol. 1, no. 6, pp. 1536-1540, 2023.
- [5] R. A. Purnama, "Optimalisasi Keamanan Jaringan *Wireless* Menggunakan *Firewall Filtering MAC Address*," vol. 8, no. 4, 2019.
- [6] Firmansyah, R. A. Purnama, and R. D. Astuti, "Optimalisasi Keamanan *Wireless* Menggunakan," vol. 15, no. 1, pp. 25-33, 2021.
- [7] A. S. Hidayat, U. Nuha, and Y. Nuryamin, "*Quality Of Service Filtering* Dengan Metode *Filtering MAC Address* Jaringan *Wireless*," vol. 7, no. 1, pp. 52-59, 2021.
- [8] P. R. Kumar, P. H. Raj, and P. Jelciana, "*ScienceDirect Procedia Computer Science Exploring Data Security Issues and Solutions in Cloud Computing*," *Procedia Comput. Sci.*, vol. 125, no. 2009, pp. 691-697, 2018, doi: 10.1016/j.procs.2017.12.089.
- [9] P. Pratama Putra, "Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan *Snort Rule* (Hids) untuk Mendeteksi Serangan *Nmap*," vol. 2, no. 1, 2016.
- [10] J. Dwi Santoso, "Keamanan Jaringan Nirkabel Menggunakan *Wireless Intrusion* Joko Dwi Santoso Abstraksi Keywords : Pendahuluan," vol. 1, no. 3.
- [11] Febriyandi, "Perancangan Sistem Keamanan Jaringan Dengan Metode *MAC Address Filtering* Dan Penerapan Fitur *Hotspot* Di Mikrotik RB-941 hAP Lite Pada Kantor Konsultan Pajak Edi Kurniawan," 2022.
- [12] K. Anugrah, "Pengenalan Osi Layer Kata Kunci : Pengenalan Osi Layer," pp. 1-5, 1980.
- [13] W. Stallings, *Data Dan Computer*.
- [14] Rico, "Analisis Kelemahan Celah Lapisan Keamanan Pada Jaringan Nirkabel," vol. 9, no. 1, pp. 6-13, 2014.
- [15] A. Maulana, M. Kom, A. Fauzi, and M. Kom, "Jaringan komputer".
- [16] A. M. Candra, S. Samsugi, and Jupriyadi, "Percangan Dan Implementasi *Controller Access Point System Manager* (CAPSMAN) Mikrotik Menggunakan Aplikasi Winbox," vol. 2, no. 2, pp. 26-32, 2021.
- [17] M. Adias Sabara and A. Prayogi, "Konfigurasi Manajemen *Bandwidth* Menggunakan Router Mikrotik RB2011UiAS-RM Untuk Mengontrol Penggunaan Internet di PT.Rekan Usaha Mikro Anda Tegal," vol. 9, no. 2, pp. 43-46, 2020.
- [18] M. Iqbal, "Perancangan Sistem Informasi Pengontrolan *Access Point* Jaringan Pada UIN Mahmud Yunus Batu Sangkar Berbasis Web," 2022.
- [19] H. Anom, S. Aji, and A. C. Prasetyo, "Evaluasi Kinerja Jaringan *WiFi* Mahasiswa : Analisis *Throughput* , *Delay* , *Jitter* , dan *Packet loss*," vol. 8, no. 1, pp. 23-27, 2024.