INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v16i2.2781

VOL. 16. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

ANALISA DAN IMPLEMENTASI JARINGAN WIRELESS MAC ADDRESS MENGGUNAKAN FILTERING PADA PT. FAYA KUNTURA AGUNG KONSULTINDO

Dipo Era Ginanti[1*)]; Ade Christian[2]; Taopik Hidayat[3]

Teknik Informatika[1,2], Sains Data[3]
Universitas Nusa Mandiri [1,2,3]
https://nusamandiri.ac.id/ [1,2,3]
dipoeraginanti@gmail.com **[1*)]**, ade.adc@nusamandiri.ac.id [2], taopik.toi@nusamandiri.ac.id [3]
(*) Corresponding Author

Abstract*—The evolution of this era is become advancing as well for Technology Information and Telecommunications. This evolution has been explored in Wireless Technology, even in all devices such as smartphones, tablets and laptops can use it. The Internet has tremendously impacted culture and it become a daily necessity by people in the world, as the internet can support the process of communicating, learning, and data transfer. Places that use wireless networks have started a lot such as schools, universities, and companies. Yet, wireless networks still have security that is quite vulnerable because it can be misused by other parties. To minimize this problem we can use MAC Address Filtering. MAC Address Filtering is a technique for prevents access to a network if the MAC Address of the devices attempting to connect does not match any addresses marked as allowed. MAC Address Filtering has 2 tasks of verification so before it does filtering, the user must log in first using the MAC Address that has been registered and then enter the username and password if it matches the MAC Address then the login will be successful, otherwise, it will be rejected. This wireless MAC Address Filtering security can avoid hackers who can enter the wireless network which makes a slow network.*

Keywords*: Hotspot Log in*, MAC *Address Filtering,* Mikrotik*, Security*

Abstrak— Semakin berkembangnya jaman juga semakin berkembangnya juga untuk bidang Teknologi Informasi dan Telekomunikasi. Teknologi *wireless* juga sangat berkembang cukup pesat bahkan disemua perangkat seperti *smartphone*, tablet dan laptop sudah dapat menggunakan teknologi *wireless*. Internet sudah menjadi kebutuhan sehari-hari oleh masyarakat yang ada didunia, karena dengan internet dapat menunjang proses berkomunikasi, belajar mengajar dan bertukar data secara daring. Tempat yang menggunakan jaringan *wireless* sudah mulai banyak seperti sekolah, universitas, tempat ibadah dan perusahaan. Namun jaringan *wireless* masih memiliki keamanan yang cukup rentan karena dapat disalah gunakan oleh pihak lain. Untuk meminimalisir dari para oknum tersebut kita dapat menggunakan dengan MAC *Address Filtering*. Dengan menggunakan MAC *Address Filtering* ini dapat memblokir perangkat yang tidak terdaftar. *Filtering* MAC *Address* memiliki 2 tahap verifikasi jadi sebelum melakukan *filtering*, *user* harus melakukan *login* terlebih dahulu menggunakan MAC *Address* yang sudah didaftarkan kemudian memasukan *username* dan *password* jika sesuai dengan MAC *Address* yang didaftarkan maka *login* akan berhasil, jika tidak maka akan ditolak. Keamanan *wireless* MAC *Address Filtering* ini dapat menghindari para peretas yang dapat memasuki jaringan *wireless* yang dapat mengakibatkan jaringan menjadi lambat.

Kata kunci: *Hotspot Log in*, MAC *Address Filtering,* Mikrotik*, Security*

PENDAHULUAN

Semakin majunya jaman maka semakin berkembang pesat juga untuk Teknologi Informasi dan Telekomunikasi. Masyarakat sudah tidak asing dengan jaringan *Internet*, karna *internet* memiliki peran yang cukup penting untuk kehidupan masyarakat. Dengan adanya *internet* dapat memudahkan kita dalam bekerja, bersosialisasi dan bahkan dapat melakukan pembelian atau penjualan melalui *online shop* (*e-commerce*).

Teknologi di bidang komputer juga sudah berkembang sangat signifikan, seperti perangkat lunak (*software*) dan perangkat keras (*hardware*). Di era teknologi informasi dan telekomunikasi yang sudah sangat canggih ini kita juga bisa memanfaatkan dengan mudah seperti jaringan komputer. Sudah banyak masyarakat yang

VOL. 16. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri
INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v16i2.2781

menggunakan jaringan komputer seperti, sekolah, tempat ibadah, tempat makan, kantor atau perusahaan, dan organisasi.

Jaringan komputer didefinisikan sebagai sekumpulan komputer (lebih dari satu) yang terhubung satu dengan lainnya menggunakan media tertentu sehingga memungkinkan diantara komputer tersebut untuk berinteraksi, bertukar data, dan berbagi peralatan bersama misalkan *printer*, *scanner* dll (Yuliandoko, 2018). Jaringan komputer dibagi menjadi beberapa jenis, yang pertama adalah *Local Area Network* atau biasa disingkat LAN adalah jaringan local yang hanya mencakup wilayah kecil saja seperti sekolah, kantor dan lain-lain. Selanjutnya ada *Metropolitan Area Network* atau sering disingkat MAN, jaringan ini dapat mencangkup lebih luas seperti beberapa kota atau wilayah dan yang terkahir adalah *Wide Area Network* atau disingkat dengan WAN, jaringan ini bahkan dapat mencangkup satu negara.

Di dalam dunia perkantoran jaringan *internet* juga sangat dibutuhkan agar memperlancar pekerjaan para pegawai seperti bertukar data, mengirim data dan lain-lain. PT. Faya Kuntura Agung Konsultindo adalah salah satu dari sekian banyak kantor yang sudah menggunakan dan merasakan manfaat dari jaringan komputer. PT. Faya Kuntura Agung Konsultindo berada di Perum Sanghyang Pancanaka Hill Jl Ontario No.26 Cibeber – Cimahi. Untuk keamanan jaringan yang ada pada PT. Faya Kuntura Agung Konsultindo masih cukup riskan karena belum adanya MAC *Address Filtering*.

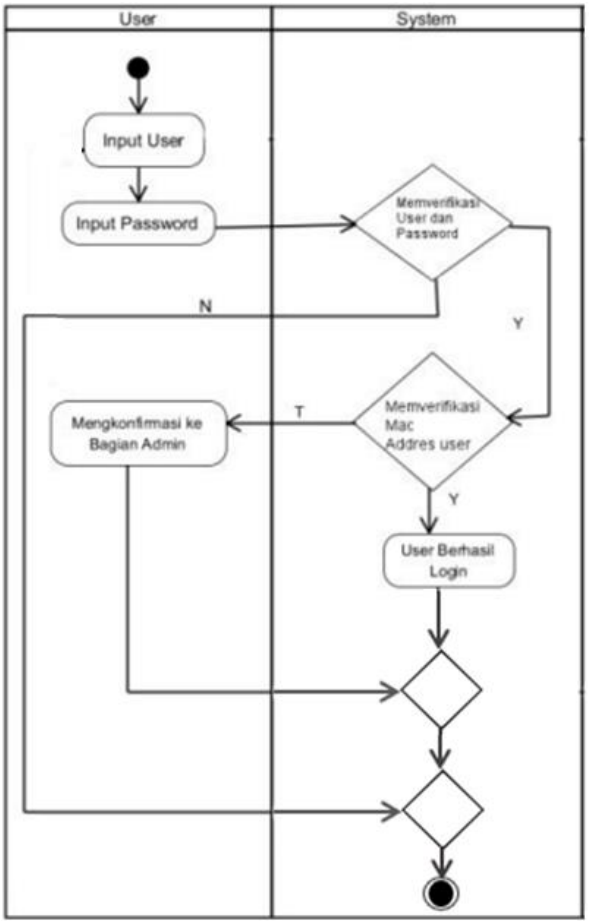
Jaringan nirkabel IEEE 802.11 telah menjadi salah satu jaringan yang paling banyak digunakan (Purnama, 2019). Karena sifat media nirkabel yang terbuka, peretas dan penggangu dapat Memanfaatkan internet untuk menemukan celah keamanannya. Kegiatan yang mengancam keamanan jaringan wireless dapat dilakukan dengan cara *Warchalking, WarDriving, WarFlying, WarSpamming, atau WarSpying*. Untuk meminimalisir pengguna layanan jaringan tanpa melakukan pembayaran dan membatasi akses kedalam jaringan dapat menggunakan sistem keamanan MAC *Address Filtering*. Metode *security* MAC *Address* dapat diimplementasikan menggunakan metode *Filter Rule*. Metode ini dapat bekerja melakukan *filtering* terhadap perangkat yang mencoba melakukan akses kedalam jaringan komputer.

Firewall filtering MAC *Address* telah dikembangkan untuk memberikan perlindungan terhadap pelayanan jaringan *wireless*. Setiap perangkat jaringan memiliki alamat MAC yang berbeda (Hidayat et al., 2021). Oleh karena itu, dengan menerapkan keamanan alamat MAC, setiap pengguna layanan jaringan yang ingin terhubung ke jaringan harus mendaftarkan alamat MAC-nya. Ini dapat digunakan untuk meminimalkan pengguna layanan jaringan yang seharusnya tidak memiliki akses (Syaiful & Novia, 2018)

Penggunaan *filtering* MAC *Address* mampu membatasi beberapa komputer yang dapat terhubung kedalam *wireless hotspot* dengan mempertimbangkan IP *Address* dan MAC *Address* yang terdaftar (Firmansyah et al., 2021). Dengan adanya permasalahan tersebut, maka *filtering* MAC *Address* diterapkan pada PT. Faya Kuntura Agung Konsultindo agae dapat menghalangi pihak diluar karyawan yang masuk ke dalam jaringan internet. Hal ini dilakukan agar tidak menganggu kinerja para pegawai yang ada pada PT. Faya Kuntura Agung Konsultindo.

BAHAN DAN METODE

Tahapan dalam penelitian ini telah dicantumkan dalam diagram alur penelitian yang diilustrasikan pada Gambar 1.



Gambar 1. *Activity Diagram*

Pada saat melakukan penelitian implementasi keamanan jaringan wireless menggunakan *firewall* MAC *address filtering* penulis menggunakan antuan perangkat Mikrotik Routeroard 951Ui2HND yang disearkan

VOL. 16. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

menggunakan mode *access point* 2 GHz untuk terhuung ke jaringan lokal dan menggunakan 2 (dua) perangkat yang akan dijadikan *client* untuk melakukan pemeriksaan keamanan pada koneksi jaringan yang digunakan.

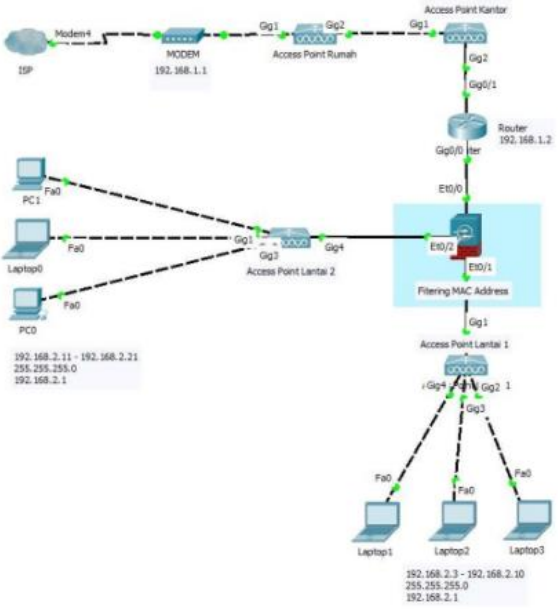
Gambar 1 menunjukkan proses yang digunakan dalam penelitian untuk mengoptimalkan keamanan jaringan nirkabel menggunakan firewall penyaringan alamat MAC. Pelanggan yang akan mengakses internet harus melewati verifikasi keamanan sebanyak 2 (dua) kali yaitu verifikasi *user* dan *password* menggunakan metode koneksi hotspot dan verifikasi perangkat MAC address menggunakan filtering firewall. Mengadopsi model multi-keamanan ini bertujuan untuk meminimalkan masalah kebocoran akses di jaringan nirkabel. Jika klien hanya mengetahui pengguna dan kata sandi tanpa menyimpan alamat MAC, klien tidak dapat mengakses internet.

Penggunaan keamanan nirkabel dua faktor, pencatatan hotspot, dan pemfilteran MAC *Address* merupakan beberapa cara untuk mencegah pihak yang tidak berkepentingan dapat mengakses jaringan nirkabel. Metode *The Security Policy Development Life Cycle* (SPDLC). SPLDC adalah siklus hidup pengembangan system jaringan yang didefinisikan pada sejumlah fase, antara lain: *Analysis, Design, Implementation, Enforcement,* dan *Enhancement* (Santoso, 2019).

1. *Analysis*
   Pada tahap ini dilakukan perumusan masalah, pengumpulan data, dan identifikasi kebutuhan seluruh komponen sistem untuk menentukan risiko dan ancaman pada keamanan jaringan nirkabel.
2. *Design*
   Tahapan *design* atau implementasi terhadap rancangan sistem dengan cara mengonfigurasi keamanan jaringan nirkabel dan melakukan langkah-langkah pengujian konektivitas.
3. *Implementation*
   Proses implementasi meliputi instalasi dan konfigurasi. Dengan mengumpulkan semua perangkat yang diperlukan untuk tes konektivitas untuk memverifikasi sistem keamanan yang dirancang.
4. *Enforment*
   Proses implementasi dengan melakukan pengamatan sistem yang telah dirancang dan diimplementasikan untuk mengetahui apakah sistem dalam keadaan baik dan beroperasi normal serta mengevaluasi pemeliharaan keamanan sistem yang telah diterapkan.

HASIL DAN PEMBAHASAN

Skema yang dilakukan adalah dengan menambah konfigurasi *Filtering* MAC *Address* pada Router sebelum diteruskan ke perangkat lain seperti *access point* yang berada pada Lantai 1 dan Lantai 2 yang fungsinya untuk menyaring MAC *Address* yang ingin masuk ke jaringan *internet* yang digambarkan pada Gambar 2.



Gambar 2. Skema Jaringan

Jaringan komputer pada PT. FAYA KUNTURA AGUNG KONSULTINDO jika sudah dikonfigurasi *Filtering* MAC Address maka keamanan jaringannya dapat dikatakan aman karena *Filtering* MAC Address ini fungsinya untuk menyaring MAC *Address* yang ingin mengakses pada jaringan *internet* yang ada pada PT. FAYA KUNTURA AGUNG KONSULTINDO. Pada saat *client* ingin mengakses ke dalam jaringan *internet* harus melewati sebanyak 2 verifikasi keamanan yaitu keamanan melalui *hotspot login* dengan memasukan *username* dan *password* lalu keamanan yang terakhir adalah memverifikasi MAC *Address* yang digunakan oleh *client*. Jika *client* yang mengakses jaringan internet tersebut sudah mendaftarkan MAC *Address* maka client tersebut dapat mengakses jaringan *internet*.

Kemudian dari skema yang telah dibuat, dilakukan percobaan menggunakan data yang ada pada Tabel.1 untuk mengimplementasikan MAC *Address Filtering* pada jaringan *wireless.*

Tabel 1. Spesifikasi *Username*

MAC *Address*	User	Password
40:E2:30:70:A8:2D	alandra	a2021
88:D5:0C:4A:A2:04	rahayu	r2021

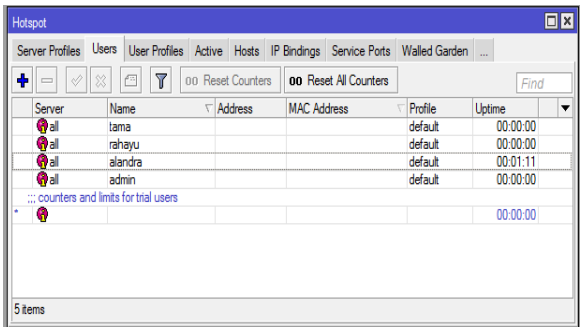
3E:13:40:62:2D:54	tama	t2021

Pada tabel 1. menjelaskan bahwa *username* alandra dengan *password* a2021 hanya bisa *log in* pada MAC *Address* 40:E2:30:70:A8:2D, sedangkan *username* rahayu dengan *password* r2021 hanya bisa *log in* pada MAC *Address* 88:D5:0C:4A:A2:04 dan *username* tama dengan *password* t2021 hanya bisa *log in* pada MAC *Address* 3E:13:40:62:2D:54.

Untuk manajemen jaringan yang ada pada PT. FAYA KUNTURA AGUNG KONSULTINDO penulis menambahkan konfigurasi penyaringan MAC *Address* pada Mikrotik. Agar jika ada client yang tidak mempunyai hak akses ingin mengakses jaringan internet pada PT. FAYA KUNTURA AGUNG KONSULTINDO maka akan langsung ditolak oleh Mikrotik karena MAC *Address* yang digunakan tidak didaftarkan oleh *Network Administrator*.

1. Pengujian Jaringan Awal

Pada tahap pengujian jaringan awal ini akan ada uji koneksi pada jaringan yang ada pada PT. Faya Kuntura Agung Konsultindo hanya dengan menggunakan *hostpot log in* saja tanpa *filtering* MAC *Address* seperti pada Gambar3.



Gambar 3. Tampilan *Username*

Dalam penerapannya, keamanan *hotspot login* mampu untuk membatasi para pengguna layanan berdasarkan *username* dan *password* yang diberikan oleh *network administrator* pada bagian IT, akan tetapi dengan menggunakan keamanan *hotspot login* belum cukup aman karena *hotspot login* cukup rawan.

Namun jika hanya menggunakan keamanan jaringan *hotspot login* maka orang lain dapat dengan mudah *login* di perangkat yang bukan semestinya. Seperti pada Tabel.2 terlihat bahwa dengan MAC *Address* 40:E2:30:70:A8:2D dapat *log in* dengan 3 *username* yang berbeda.

Tabel 2. Uji Konektifitas *Username*

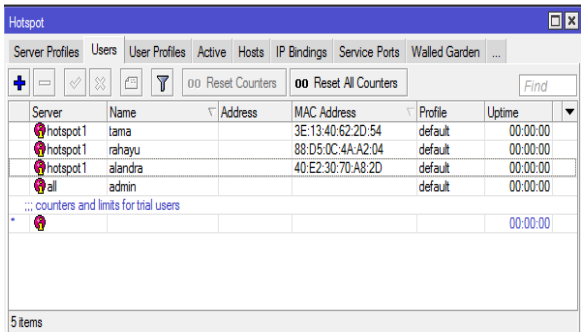
MAC *Address*	*User*	*Pass word*	Konektifitas
40:E2:30:70:A8:2D	alandra	a2021	*Connected*
	rahayu	r2021	*Connected*
	tama	t2021	*Connected*
88:D5:0C:4A:A2:04	alandra	a2021	*Connected*
	rahayu	r2021	*Connected*
	tama	t2021	*Connected*
3E:13:40:62:2D:54	alandra	a2021	*Connected*
	rahayu	r2021	*Connected*
	tama	t2021	*Connected*

Disini terlihat bahwa keamanan *hotspot log in* saja tidak terlalu aman karna dapat dimanfaatkan atau digunakan oleh pengguna yang tidak mempunyai hak akses.

2. Pengujian Jaringan Akhir

Pada tahap pengujian jaringan akhir ini penulis akan melakukan pengujian untuk mengetahui bahwa jaringan yang dibuat berfungsi dengan baik dan tidak ada *error*. Pengujian akhir ini untuk menerapkan atau mngimplementasikan konfigurasi jaringan MAC *Address Filtering* pada PT. Faya Kuntura Agung Konsultindo.

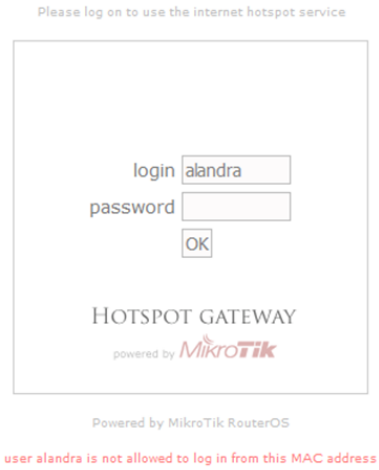
Jika di tahap pengujian awal penulis hanya mencoba menerapkan keamanan jaringan *hotspot login* saja, maka di pengujian kali ini atau pengujian akhir ini penulis mencoba menerapkan keamanan *hotspot login* dan MAC *Address Filtering.* Fungsi dari MAC *Address Filtering* ini sendiri adalah untuk menghindari kejadian seperti yang ada pada tabel.2 yang mana semua *username* dan *password* yang ada dapat digunakan oleh perangkat lain untuk mengakses jaringan internet.



Gambar 4. *username* dan MAC *Address*

Jika ada *client* yang ingin mengakses jaringan internet dengan MAC *Address* yang tidak didaftarkan atau mengakses menggunakan perangkat lain seperti PC, Laptop atau *Smartphone* maka secara langsung akan ditolak oleh Mikrotik.

VOL. 16. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri



Gambar 5. alandra gagal *login*

Seperti pada Gambar 5, terlihat bahwa user alandra mengakses jaringan internet dengan menggunakan MAC *Address* yang berbeda maka hasilnya *user* alandra tidak dapat *login* ke jaringan internet. Web *login* tersebut akan menampilkan pemberitahuan bahwa "*user* alandra *is not allowed to log in for this* MAC *Address*" yang artinya adalah "user alandra tidak dapat *login* dari MAC *Address* ini".

Gambar 6. User alandra berhasil login

Sedangkan pada Gambar 6. menampilkan *username* alandra mencoba untuk mengakses jaringan internet menggunakan MAC *Address* yang sudah didaftarkan maka *user* alandra akan berhasil *log in* dan dapat mengakses jaringan internet seperti yang terlihat pada Gambar 6. Dengan menambahkan konfigurasi MAC *Address Filtering* dapat memberikan keamanan bagi para pegawai dan juga dapat meminimalisir para peretas yang dapat dengan mudah mengakses jaringan internet.

KESIMPULAN

Mengimplementasikan MAC *Address Filtering* dapat mengoptimalkan keamanan jaringan komputer khusunya jaringan *wireless* dari para pihak yang tidak bertanggung jawab. Dengan menggunakan MAC *Address Filtering* dapat melakukan 2 verifikasi keamanan, yang pertama adalah *hotspot log in* dan yang kedua adalah MAC *Address Filtering*. Setelah menganalisa jaringan internet yang ada pada PT. FAYA KUNTURA AGUNG KONSULTINDO maka penulis dapat memberikan saran untuk menangani masalah yang ada pada PT. FAYA KUNTURA AGUNG KONSULTINDO. Dikarenakan belum adanya *Filtering* MAC *Address* yang membuat orang lain selain staff atau pegawai PT. FAYA KUNTURA AGUNG KONSULTINDO dapat dengan mudahnya mengakses jaringan *internet,* maka dari itu penulis menyarankan untuk membuat konfigurasi *Filtering* MAC *Address* menggunakan Mikrotik.

REFERENSI

Ferdiansyah, D. (2017). Perancangan Jaringan Vlan (Virtual Local Area Network) Kementerian Komunikasi Dan Informatika RI Jakarta. *Simnasiptek 2017*, *1*, 1–6

Firmansyah, F., Purnama, R. A., & Astuti, R. D. (2021). Optimalisasi Keamanan Wireless Menggunakan Filtering Mac Address. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *15*(1), 25–33. https://doi.org/10.47111/jti.v15i1.1910

Gani, A. G. (2014). Konfigurasi Sistem Keamanan Jaringan. *Jurnal Sistem Informasi Universitas Suryadarma*, *6*(1), 134–149. https://doi.org/10.35968/jsi.v6i1.280

Gunawan, T., Kurniawan, D. F., Studi, P., Informatika, M., Dian, A., & Cendikia, C. (2020). Rancang Bangun Jaringan Wireless Local Area Network (WLAN) Menggunakan Metode Routing Statik Pada SMPN 7 Pesawaran. *Jurnal Informatika Software Dan Network*, *1*(1), 41–47.

Hidayat, A. S., Nuha, U., Nuryamin, Y., & Suleman, S. (2021). Quality Of Service Filtering Dengan Metode Filtering Mac Address Jaringan Wireless. *Jurnal Teknologi Informatika Dan Komputer*, *7*(1), 52–59. https://doi.org/10.37012/jtik.v7i1.502

Ontoseno, R. D. H., Haqqi, M. N., & Hatta, M. (2017). Limitasi Pengguna Akses Internet Berdasarkan Kuota Waktu Dan Data Menggunakan Pc Router Os Mikrotik. *Teknika: Engineering and Sains Journal*, *1*(2), 125. https://doi.org/10.51804/tesj.v1i2.134.125-130

Purnama, R. A. (2019). Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address. *Indonesian Journal On Networking and Security*, *8*(4), 43–47.

Purnama, R. A. (2019). Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall

Filtering MAC Address. *Indonesian Journal On Networking and Security*, *8*(4), 43–47.

Rachmadi, T. (2020). *Jaringan Komputer*. TIGA Ebook.

Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *Infos*, *1*(3), 44–50.

Siddik, M. (2019). Implementasi Mikrotik Router Board 750 Sebagai Firewall Blok Situs Pada Jaringan Lan. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *3*(2), 70–75. https://doi.org/10.33330/jurteksi.v3i2.304

Syafrizal, M. (U. A. Y. (2020). *Pengantar Jaringan Komputer*. C.V. ANDI OFFSET (Penerbit ANDI).

Syaiful, & Novia, C. (2018). *Perancangan Jaringan Internet Dengan Hotspot Mikrotikdan Mac Address Filtering*. *12*(02), 13–24.

Wulandari, R. (2016). Analisis Qos (Quality Of Service) Pada Jaringan Internet (Studi Kasus: Upt Loka Uji Teknik Penambangan Jampang Kulon -LIPI). *Jurnal Teknik Informatika Dan Sistem Informasi*, *2*(2), 162–172. https://doi.org/10.28932/jutisi.v2i2.454

Yuliandoko, H. (2018). *Jaringan Komputer Wire dan Wireless Beserta Penerapannya*. CV BUDI UTAMA.