

**PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN
NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK
DAN FIREWALL PADA SMK KRISTEN SERITI**

Cindra Abraham Rante¹, Alfhian Makmur², Jumarniati³

Universitas Cokroaminoto Palopo

E-mail: cindraabrahamrante28@gmail.com¹, alon.ftkom@gmail.com², jumarniati@uncp.ac.id³

Abstrak

Penelitian ini bertujuan untuk mengembangkan sistem manajemen keamanan jaringan nirkabel (WiFi) pada SMK Kristen Seriti dengan memanfaatkan perangkat Routerboard Mikrotik dan fitur konfigurasi firewall. Permasalahan utama yang dihadapi sekolah adalah lemahnya sistem keamanan jaringan yang berdampak pada lambatnya koneksi internet serta rentannya jaringan terhadap akses tidak sah. Kondisi ini terjadi karena tidak adanya pembatasan bandwidth, penggunaan satu kata sandi untuk semua pengguna, dan tidak adanya sistem kontrol akses seperti firewall yang efektif. Metode penelitian yang digunakan adalah metode Research and Development (R&D) dengan model pengembangan Network Development Life Cycle (NDLC). Model ini meliputi tahapan analisis, desain, simulasi, implementasi, monitoring, dan manajemen sistem. Hasil dari implementasi menunjukkan bahwa sistem yang dikembangkan mampu membatasi akses terhadap situs-situs yang tidak sesuai, mengatur pembagian bandwidth, serta meningkatkan stabilitas jaringan WiFi di lingkungan sekolah. Evaluasi dilakukan melalui pengamatan langsung dan pengujian firewall, yang menunjukkan peningkatan performa dan keamanan jaringan secara signifikan. Kesimpulan dari penelitian ini adalah bahwa penerapan Routerboard Mikrotik dan firewall dapat meningkatkan kualitas keamanan jaringan nirkabel secara efektif, meskipun masih diperlukan monitoring dan pemeliharaan sistem secara berkala. Penelitian ini diharapkan dapat menjadi referensi dalam pengembangan sistem keamanan jaringan serupa di instansi pendidikan lainnya.

Kata Kunci — Routerboard Mikrotik, Monitoring, Pengembangan, Jaringan Nirkabel (Wifi).

PENDAHULUAN

Perkembangan nilai informasi sangatlah penting dan dibutuhkan oleh berbagai kalangan, baik itu dari kalangan pemakai maupun pembuat informasi maka kehadiran teknologi informasi sangatlah mutlak diperlukan. Pemanfaatan internet telah mengubah pola hidup dan budaya manusia dalam belajar, bekerja, berkomunikasi, berbelanja dan aspek lainnya. Hadirnya jaringan komputer merupakan solusi yang terbaik untuk masalah kecepatan dan keakuratan informasi. Banyak sekali keuntungan apabila menggunakan jaringan komputer. Pengguna atau user diberikan kebebasan dalam berselancar di internet tanpa batasan, serta pengguna atau user dapat membuka situs yang berbaur dewasa dengan merubah DNS (Domain Name Server) secara manual (Firmansyah dan Rachmat, 2019).

Perkembangan teknologi saat ini dan terapan teknologi jaringan wireless telah

berkembang pesat. Perkembangan teknologi selalu membawa perubahan untuk kita. Seiring berkembangnya media transmisi dalam pengiriman data. Namun perlu diketahui bahwa wireless masih cukup rentan terhadap pencurian hak akses seperti pencurian username dan password. Contoh lainnya yaitu serangan DOS (Denial of Service) yang dapat menghabiskan sumber daya dan juga melakukan pencurian data sehingga mengakibatkan kerugian. Maka dari itu, Keamanan jaringan wireless sebagai bagian dari sistem menjadi sangat penting dalam menjaga validitas dan integritas data. Jika tidak ditangani dengan benar, hacker akan dengan mudah mengeksploitasi kemampuan mereka dalam jaringan dan pada akhirnya menimbulkan kerugian bagi pengguna (Alamsyah dan Fatdha, 2020).

Perkembangan itu sendiri seiring dengan semakin tingginya tingkat kebutuhan akses internet dan semakin banyaknya penggunaan internet yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil yang maksimal baik dari segi efisiensi maupun peningkatan keamanannya. Perkembangan teknologi informasi juga menuntut sebagian institusi untuk ikut berperan, karena kebutuhan akses informasi yang mudah merupakan kebutuhan bagi setiap orang saat ini. Hal tersebut dapat dilihat dari penggunaan jaringan komputer baik itu secara umum maupun pribadi. Teknologi informasi ini telah menjadi fasilitator utama dalam berbagai kegiatan tak terkecuali pada bidang pendidikan diantaranya dalam bentuk teknologi yang merupakan suatu era baru dalam dunia informasi modern yang telah berkembang pesat beberapa tahun terakhir (Herusutopo dan Prasetyo, 2019).

SMK Kristen Seriti merupakan salah satu Instansi Pendidikan yang bertempat di Kecamatan Lamasi Timur, Kabupaten Luwu, Sulawesi Selatan. SMK Kristen Seriti sendiri merupakan satu dari sekian banyak instansi yang telah menerapkan sistem jaringan internet dalam sekolah tersebut, tentunya dengan tujuan memperlancar pekerjaan di dalam sekolah tersebut. Keamanan manajemen jaringan wifi pada SMK Kristen Seriti menjadi perhatian penuh, melihat instansi tersebut dimana data-data penting ada di tiap komputer yang terhubung melalui jaringan, hak akses terhadap data-data tersebut harusnya menjadi perhatian utama oleh para staff dan guru yang ada di instansi tersebut.

Setiap komputer yang terhubung ke dalam suatu jaringan dan terkoneksi dengan internet pasti akan sering menghadapi berbagai macam bentuk serangan yang selalu berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Kasus yang terjadi pada SMK Kristen Seriti jaringan komputer yang terkoneksi dengan internet sering mendapatkan serangan-serangan yang mengakibatkan kerusakan bahkan kehilangan data akibat serangan tersebut. Flooding data menjadi salah satu bentuk serangan serangan yang mengakibatkan suatu sistem akan terbanjiri oleh data-data secara terus menerus dalam waktu yang singkat. Hal ini juga mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga lalu lintas yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem.

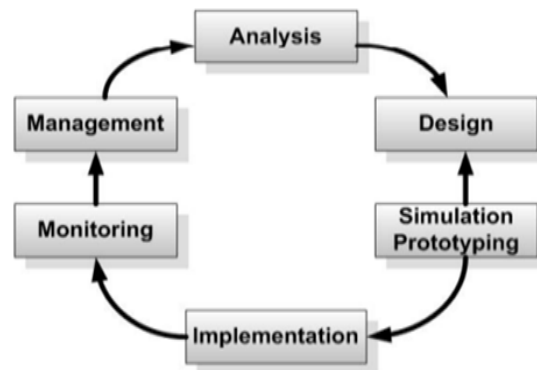
Maka dari itu kondisi keamanan jaringan wifi pada SMK Kristen Seriti kurang baik, permasalahan-permasalahan jaringan yang juga sering dihadapi yaitu seperti data yang dikirim menjadi lambat atau bahkan tidak sampai ke tujuan karena jaringan internet yang lambat, karena disebabkan oleh banyaknya yang mengakses jaringan, selain itu sistem keamanan jaringan yang kurang optimal. Hal yang seperti ini membutuhkan suatu keamanan jaringan dengan menggunakan alat atau aplikasi yang dapat membantu dalam keamanan dan akses jaringan internet yang bagus untuk para staff agar akses jaringan internet dapat digunakan secara optimal dan keamanan jaringan lebih baik lagi pada SMK Kristen Seriti. langkah pengembangan keamanan jaringan yang akan dilakukan penulis bertujuan untuk memberikan rasa aman dan optimal untuk para staff atau orang-orang

terkait yang menggunakan akses jaringan yang berada di lokasi penelitian, dengan penerapan sistem pengembangan keamanan jaringan nirkabel (wifi) menggunakan routerboard mikrotik dan firewall agar dapat mengatasi berbagai masalah keamanan jaringan dan peretasan hacker menggunakan tools sederhana seperti ethercap, wireshark, fiwihack dan lain-lain.

Berdasarkan hal tersebut, akan menjadi landasan bagi penulis untuk memberikan solusi yang dapat membantu mengoptimalkan penggunaan jaringan dengan melakukan “Pengembangan manajemen Keamanan Jaringan Nirkabel (Wifi) Menggunakan RouterBoard Mikrotik dan Firewall pada SMK Kristen Seriti”.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu, metode R&D (Research and Development). Metode Research and Development merupakan metode yang digunakan untuk menghasilkan suatu produk tertentu dan menguji seberapa efektif produk yang telah di buat. Adapun model yang digunakan dalam penelitian ini yaitu penelitian NDLC (Network Development Life Cycle) dimana dengan model ini dapat mengembangkan jaringan yang sudah ada dengan beberapa tahap yaitu analisis, desain, simulasi, implementasi, management dan monitoring. NDLC merupakan sebuah model penelitian yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.

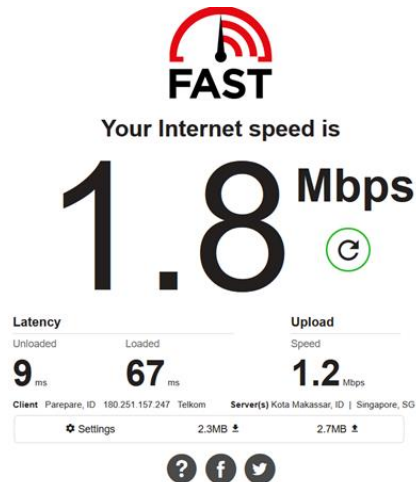


Gambar 1. Network Development Life Cycle (NDLC)
Sumber: duniahosting (2021)

HASIL DAN PEMBAHASAN

Hasil Penelitian

Implementasi sistem merupakan tahapan rancangan yang telah direncanakan sebelumnya dan diwujudkan melalui penerapan aplikasi program. Saat ini masih terdapat beberapa kelemahan dalam sistem jaringan yang digunakan pada SMK Kristen Seriti, salah satunya belum diterapkannya manajemen keamanan jaringan nirkabel (*Wifi*). Hal ini mengakibatkan beberapa komputer *client* di sekolah tersebut dapat mengalami gangguan keamanan jaringan nirkabel (*Wifi*) secara tidak teratur, menyebabkan gangguan bagi client lain yang ingin menggunakan internet. Untuk saat ini kapasitas *bandwidth* yang digunakan pada sistem jaringan komputer yaitu 1,8 Mbps untuk siswa, *download* dan upload dengan kecepatan 1,2 Mbps.



Gambar 2. Kecapatan Jaringan Awal pada SMK Kristen Seriti
Sumber: Penulis (2025)

1. Analisis

Pada tahap ini penulis menganalisis sistem yang berjalan pada SMK Kristen Seriti. Tujuan dari tahap analisis ini yaitu untuk mengetahui performa jaringan pada SMK Kristen Seriti.

Berdasarkan hasil dari analisis, SMK Kristen Seriti memiliki performa jaringan yang kurang memadai dan *switch* yang masih menggunakan satu *password* untuk semua pengguna.

Tahap pengumpulan data yang penulis lakukan berupa observasi, wawancara, dan studi pustaka yang dilakukan secara langsung serta sesuai dengan metode NDLC.

a. Observasi

Hasil dari observasi yang dilakukan penulis di SMK Kristen Seriti yaitu manajemen keamanan jaringan nirkabel (*Wifi*) dan pembagian *bandwidth* yang kurang merata dan penggunaan jaringan yang kurang optimal dan sering terjadi *overload*, selain itu sistem keamanannya hanya menggunakan satu *password* untuk mengakses jaringan.

b. Wawancara

Wawancara dilakukan oleh penulis sebagai salah satu metode pengumpulan data untuk mengetahui kondisi nyata dari jaringan nirkabel yang digunakan di SMK Kristen Seriti. Wawancara pertama dilakukan sebelum sistem keamanan diterapkan, dan wawancara kedua dilakukan setelah proses implementasi selesai.

Pada wawancara pertama, penulis memperoleh informasi dari salah satu staf yang bertugas sebagai operator/admin jaringan di sekolah. Dari hasil wawancara tersebut, diketahui bahwa penggunaan jaringan internet di SMK Kristen Seriti masih belum optimal. Responden menjelaskan bahwa jaringan sering mengalami keterlambatan pengiriman data, bahkan dalam beberapa kasus, data tidak sampai ke tujuan karena lambatnya koneksi. Hal ini terutama disebabkan oleh banyaknya perangkat yang terhubung secara bersamaan ke jaringan tanpa adanya pembatasan atau pengaturan tertentu. Selain itu, sistem keamanan jaringan dinilai masih sangat sederhana karena hanya menggunakan satu kata sandi untuk semua pengguna. Kondisi tersebut memungkinkan jaringan diakses dengan mudah oleh pihak luar, sehingga berpotensi menimbulkan risiko terhadap keamanan data dan kestabilan koneksi.

Wawancara kedua dilakukan setelah penulis menyelesaikan tahapan implementasi sistem keamanan jaringan berbasis *Routerboard Mikrotik* dan *firewall*. Berdasarkan hasil wawancara lanjutan dengan narasumber yang sama, diperoleh tanggapan positif terhadap perubahan yang terjadi. Responden menyampaikan bahwa jaringan kini terasa lebih stabil

dan aman. Sistem login *hotspot* yang diterapkan mampu membatasi akses hanya kepada pengguna yang memiliki kredensial, sementara fitur manajemen bandwidth membantu mendistribusikan koneksi secara lebih merata. Penggunaan firewall juga memberikan efek positif dengan memblokir akses ke situs-situs yang tidak mendukung kegiatan pembelajaran. Dengan adanya sistem yang lebih terstruktur ini, pihak sekolah merasa lebih terbantu dalam memantau dan mengontrol penggunaan jaringan, serta dapat meminimalkan potensi penyalahgunaan akses oleh siswa.

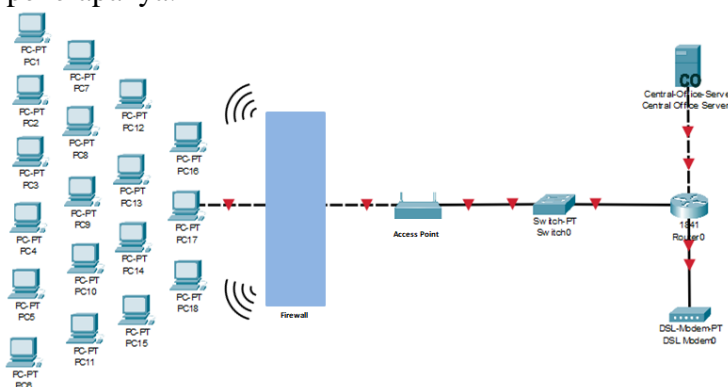
Dari kedua wawancara tersebut, dapat disimpulkan bahwa sistem keamanan jaringan yang dikembangkan telah memberikan dampak yang signifikan terhadap peningkatan kualitas layanan internet di lingkungan sekolah.

c. Studi Pustaka

Hasil dari studi pustaka yaitu menggunakan referensi dari jurnal maupun buku yang berkaitan dan relevan dengan penelitian penulis yang berjudul pengembangan sistem keamanan jaringan nirkabel menggunakan *Routerboard Mikrotik* pada SMK Kristen Seriti.

2. Desain Sistem

Perancangan sistem merupakan salah satu tahapan yang dilakukan oleh penulis setelah melakukan analisis pada sistem yang ada, pada tahap ini penulis merancang sistem keamanan jaringan pada SMK Kristen Seriti. Desain sistem keamanan jaringan bertujuan agar sistem yang diterapkan memiliki gambaran yang jelas, serta dapat maksimal dalam penerapannya.



Gambar 3. Sistem yang Diusulkan

Sumber: Penulis (2025)

Adapun sistem yang diusulkan yaitu penulis merancang pengembangan manajemen keamanan jaringan nirkabel (*Wifi*), jaringan yang berjalan masih bersifat sederhana dan belum terkelola dengan baik. Selain itu, dalam sistem yang diusulkan penulis menggunakan *routerboard mikrotik* dan *firewall* agar dapat mengatasi berbagai masalah keamanan jaringan, karena pada sistem sebelumnya belum terdapat pengamanan jaringan yang memadai, tidak ada *firewall* atau sistem yang mampu mendeteksi adanya serangan, seperti percobaan peretasan, penyebaran *malware*, atau akses yang mencurigakan.

Topologi jaringan ditata secara rapi dan perangkat-perangkat yang terhubung ke modem atau *access point* melalui *MikroTik*, sehingga memudahkan dalam proses pemantauan atau *troubleshooting*. Pada sistem yang diusulkan, jaringan juga ditingkatkan dengan menambahkan perangkat *RouterBoard MikroTik* sebagai pusat pengelolaan koneksi. *MikroTik* berfungsi untuk membagi *bandwidth* secara adil kepada setiap pengguna, sehingga jaringan lebih stabil dan tidak ada pengguna yang mengonsumsi *bandwidth* secara berlebihan. Selain itu, *MikroTik* juga membagikan IP secara otomatis kepada perangkat yang terhubung, membuat pengelolaan jaringan menjadi lebih efisien.

3. Simulasi Sistem

Saat melakukan penelitian, membutuhkan rencana simulasi yang akan memudahkan proses pelaksanaan identifikasi dalam penelitian. Simulasi dilakukan dalam bentuk video suara, nantinya dalam video suara yang telah dibuat akan disimulasikan bagaimana cara melakukan manajemen keamanan jaringan menggunakan *mikrotik* untuk meningkatkan keamanan jaringan.

4. Implementasi Sistem

Implementasi pengembangan manajemen keamanan jaringan nirkabel (Wi-Fi) menggunakan *RouterBoard MikroTik* dan *Firewall* dilakukan melalui beberapa tahap:

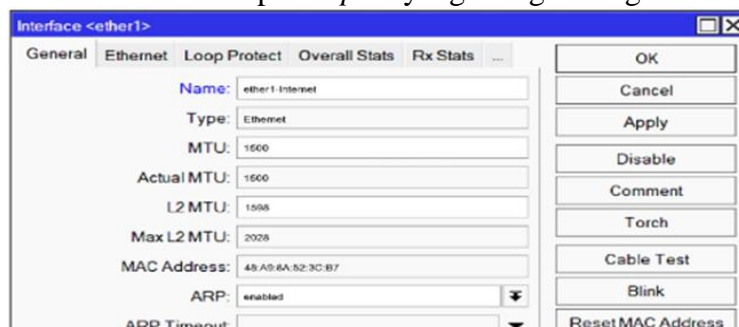
a. Instalasi Perangkat Keras:

- 1) *Modem ZTE HG8245H5M Fiber Home* dihubungkan ke **RouterBoard MikroTik RB-941-2**.
- 2) *RouterBoard MikroTik* kemudian terhubung ke *switch* dan *access point TP-Link TL-WR841N* untuk distribusi jaringan.
- 3) *Firewall* diintegrasikan dengan *MikroTik* untuk memantau dan memfilter lalu lintas data.

b. Konfigurasi Router Mikrotik

Konfigurasi *Router Mikrotik* merupakan fase pertama pada implementasi penelitian ini, mencakup beberapa langkah yaitu:

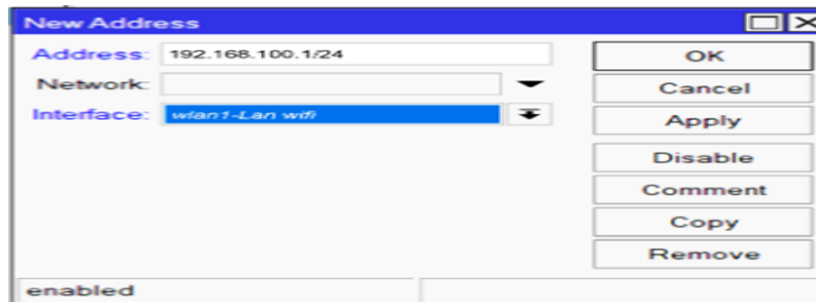
- 1) Konfigurasi *mikrotik RB941-2nD hAP Lite* melalui laptop dalam menghubungkan ke jaringan. Selanjutnya, menghubungkan kabel LAN dari *port mikrotik*, dari *switch* ke *port 2 mikrotik* dan dari laptop ke *port 5 mikrotik*, lalu jalankan aplikasi *winbox* dan pilih *MAC address router* yang sudah terhubung.
- 2) Memberi nama pada setiap *interface* yang terhubung. *Port ether1* diberi nama "*ether1-Internet*" karena merupakan *port* yang menghubungkan *mikrotik*.



Gambar 4. Tampilan Mengubah *Ether1-Internet*

Sumber: Penulis (2025)

- 3) Selanjutnya, menentukan *IP Address* pada setiap antarmuka yang terhubung dengan *router mikrotik*. Antarmuka *ether1* adalah *IP* dari jaringan wifi dan akan mendapatkan *IP* untuk *ether1-Internet* secara *DHCP*. Masuk ke menu *IP* pilih *DHCP Client* lalu + (*new dhcp client*), pilih *interface ether1-Internet*, klik *Apply* dan *Ok*.
- 4) Dengan menggunakan *DHCP Client* akan memberikan *IP* secara dinamis dari *server DHCP* yang ada dalam jaringan, termasuk mendapatkan *Alamat IP*, *Subnet Mask*, *Gateway*, dan *DNS server*. Status "*bound*," berarti *DHCP client* telah berhasil mendapatkan alamat *IP* dari *server DHCP* yaitu *192.168.1.74*.
- 5) Selanjutnya menentukan *IP address* utama dengan, Menu *IP* pilih *Address* lalu + (*new address*), *Interface* = *wlan1*, klik *Apply* dan *Ok*. Pada *wlan1* diberikan *address 192.168.100.1* adalah alamat *IP* utama yang ditetapkan untuk antarmuka jaringan atau perangkat yang disebut sebagai "*wlan1*".



Gambar 5. Tampilan IP Address Wlan1-Lan Wifi

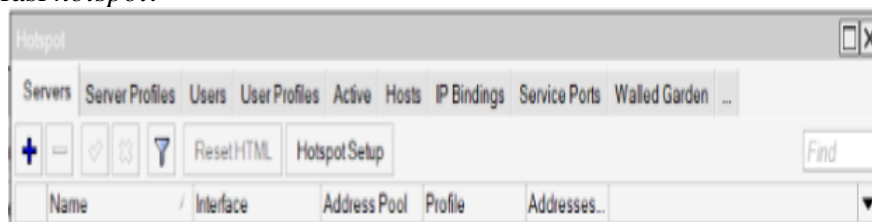
Sumber: Penulis (2025)

- 6) Selanjutnya, mengaktifkan *wlan* kemudian lakukan konfigurasi *wireless* pada menu *interfaces* : klik *wlan* pilih *wireless* lalu *Mode = ap bridge*, *SSID = SMK Kristen Seriti*, klik *Apply* dan *Ok*. *Mode AP-bridge* berfungsi sebagai pemancar dan *access point* yang dapat melayani banyak *client* atau disebut juga *Point to Multi Point (PTMP)*.
- 7) Selanjutnya, menggunakan *mode AP Bridge (Access Point Bridge)* MikroTik, perangkat dapat dikonfigurasi sebagai titik akses nirkabel untuk menghubungkan klien nirkabel ke jaringan kabel atau jaringan nirkabel yang lebih luas.
- 8) Selanjutnya mengaktifkan *wlan* kemudian lakukan konfigurasi *wireless* pada menu *interfaces* pilih klik *wlan* lalu *wireless* kemudian *Mode = ap bridge*, *SSID = SMK Kristen Seriti*, klik *Apply* dan *Ok*.
- 9) Terakhir menambahkan *DNS*, dengan Menu *IP* pilih *DNS* dan isikan *DNS google (8.8.8.8) dan (8.8.4.4)*, klik *Apply* dan *Ok*. Dengan menambahkan *DNS Google* pada *Router Mikrotik* dapat memberikan beberapa manfaat diantaranya yaitu pencegahan *DNS Spoofing*. *DNS Google* dapat digunakan sebagai *server DNS* alternatif yang dapat membantu dalam resolusi nama domain, yang dapat meningkatkan kecepatan dan keandalan akses internet.

c. Konfigurasi Login Hotspot

Konfigurasi *hotspot* dilakukan untuk membuat *IP address hotspot*. Langkah-langkah dalam melakukan konfigurasi *hotspot* dijalankan pada menu *IP* pilih *Hotspot* kemudian *Hotspot Setup* yaitu sebagai berikut:

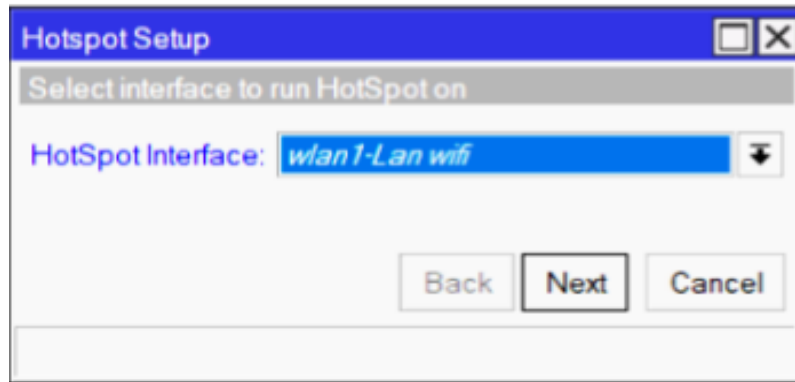
- 1) Klik tombol "*Hotspot Setup*" di bagian layar *interface* untuk memulai proses konfigurasi *hotspot*.



Gambar 6. Tampilan pengaturan hotspot

Sumber: Penulis (2025)

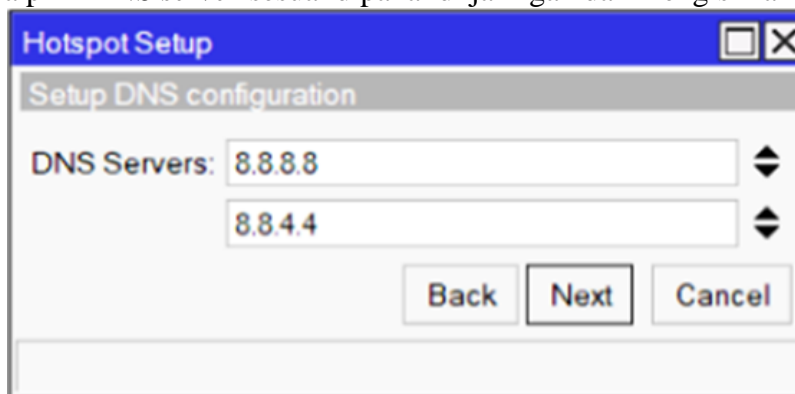
- 2) Melalui antarmuka *WLAN*, MikroTik dapat menjadi titik akses *Wi-Fi* yang menyediakan akses internet nirkabel bagi perangkat *client* yang terhubung. Menentukan rentang alamat *IP* untuk *client hotspot*. Rentang ini akan diberikan kepada perangkat yang terhubung ke *hotspot*.



Gambar 7. Tampilan Pengaturan *Hotspot WLAN*

Sumber: Penulis (2025)

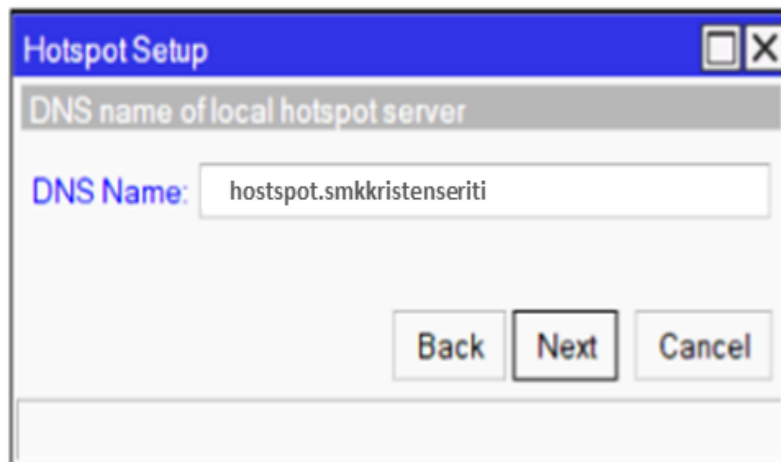
- 3) Selanjutnya pilih *DNS server* sesuai dipakai di jaringan dan mengisi nama dari *DNS*.



Gambar 8. Tampilan pengaturan *DNS Server*

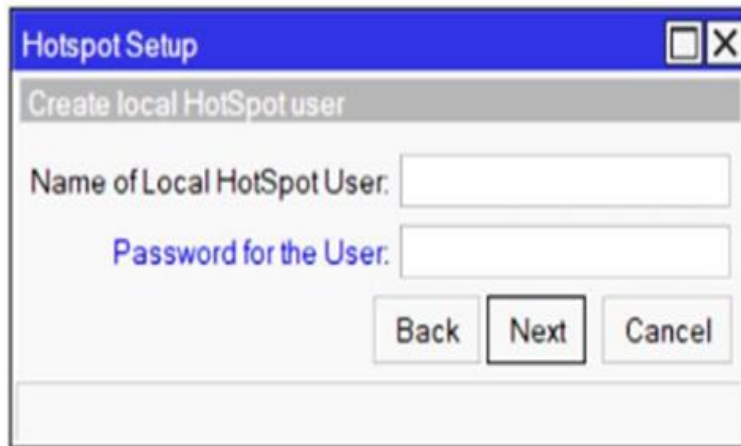
Sumber: Penulis (2025)

- 4) Terakhir menetapkan Nama *DNS* untuk menetapkan Nama domain khusus untuk mengakses halaman *login Hotspot* dan sekaligus membuat *username* dan *password*.



Gambar 9. Tampilan Nama *DNS Server*

Sumber: Penulis (2025)

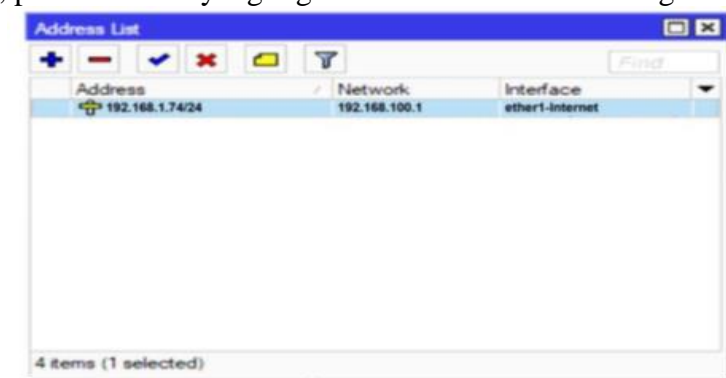


Gambar 10. Tampilan *User Name* dan *Password Hotspot*
Sumber: Penulis (2025)

d. Konfigurasi *Firewall*

Selanjutnya dengan melakukan pembatasan hak akses dengan menggunakan dengan mengatur konfigurasi pada firewall yang ada fitur NAT, hal ini dapat membatasi user dalam mengakses situs-situs yang mengandung unsur pornografi, dan judi online. Dengan langkah-langkah berikut ini:

1. Klik pada interface IP Address. Selanjutnya Klik IP lalu DHCP Server kemudian DHCP Setup, pilih interface yang ingin diberikan IP untuk konfigurasi *firewall*.



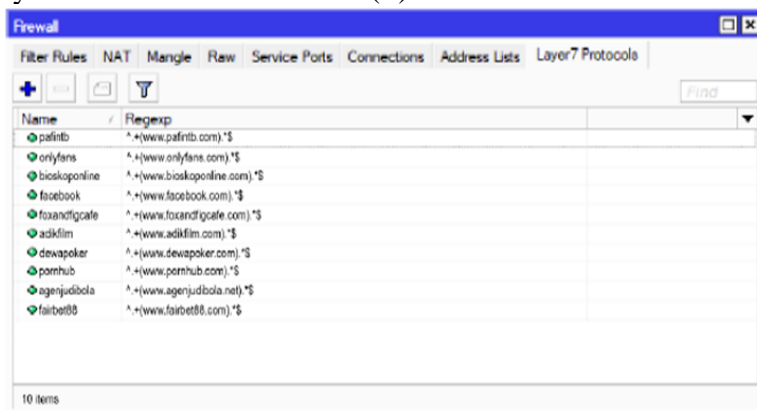
Gambar 11. Tampilan *IP Address*
Sumber: Penulis (2025)

2. Selanjutnya mengatur NAT, bertujuan untuk memberikan keamanan kepada IP Private. Selanjutnya Klik IP pilih Firewall kemudian Tab NAT dan Tambah (+).



Gambar 12. Tampilan Konfigurasi *Firewall NAT*
Sumber: Penulis (2025)

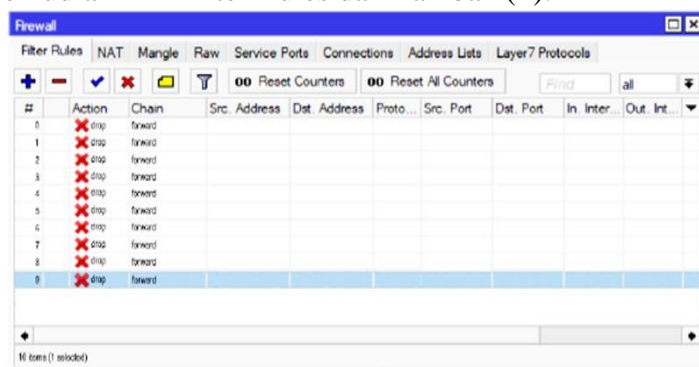
- Selanjutnya mengatur *firewall* di Layer 7 Protocol, Klik IP lalu pilih Firewall kemudian Layer 7 Protocol dan Tambah (+).



Gambar 13. Tampilan Konfigurasi *Layer 7 Protocol*

Sumber: Penulis (2025)

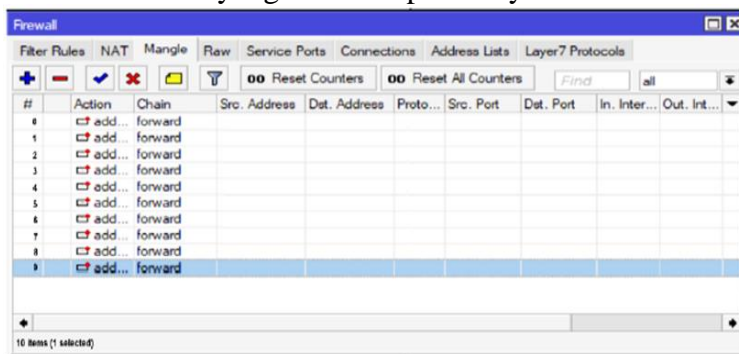
- Selanjutnya mengatur konfigurasi *firewall* berdasarkan bagian Filter Rules, Klik IP lalu klik Firewall kemudian klik Filter Rules dan Tambah (+).



Gambar 14. Tampilan Hasil *Filter Rules*

Sumber: Penulis (2025)

- Terakhir mengatur rules *mangle* akan membuat blacklist IP address yang disebut “site-block, untuk memblokir situs yang di tandai pada Layer 7 Protocol.



Gambar 15. Tampilan Hasil *Mangle Blacklist IP Address*

Sumber: Penulis (2025)

5. Monitoring

Tabel 1. Analisis Sebelum Pengembangan Keamanan Jaringan SMK Kristen Seriti

No	Jam	Situs				
		Onlyfans	Facebook	adikfilm	pornhub	Fairbet88
PC 1	09.03	Terakses	Terakses	Terakses	Terakses	Terakses
	11.49	Terakses	Terakses	Terakses	Terakses	Terakses
	13.28	Terakses	Terakses	Terakses	Terakses	Terakses

	09.46	Terakses	Terakses	Terakses	Terakses	Terakses
PC 2	11.01	Terakses	Terakses	Terakses	Terakses	Terakses
	13.49	Terakses	Terakses	Terakses	Terakses	Terakses
	09.51	Terakses	Terakses	Terakses	Terakses	Terakses
PC 3	11.05	Terakses	Terakses	Terakses	Terakses	Terakses
	13.31	Terakses	Terakses	Terakses	Terakses	Terakses

Sumber: Penulis (2025)

Berdasarkan data tabel di atas, sebelum dilakukannya analisis keamanan jaringan rata-rata hasil analisisnya "terakses". Maka dapat peneliti simpulkan bahwa dampak sebelum manajemen keamanan jaringan diterapkan yaitu masih dapat mengakses situs yang telah masuk *listing* pada fitur NAT salah satunya situs hiburan *facebook* dan lain-lain. Hal ini tentu berdampak pada pembelajaran yang tentunya tidak berguna sebagai ilmu pengetahuan.

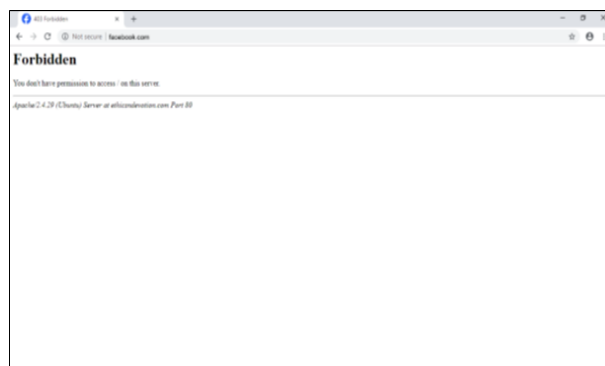
Tabel 2. Analisis Setelah Pengembangan Keamanan Jaringan SMK Kristen Seriti

No	Jam	Proteksi Firewall	Situs					Indeks
			Onlyfans	Facebook	adikfilm	pornhub	Fairbet88	
PC 1	09.23	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Kurang Memuaskan
	11.39	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
	13.28	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
PC 2	09.26	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
	11.41	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Kurang Memuaskan
	13.30	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
PC 3	09.31	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
	11.45	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Memuaskan
	13.32	Aktif	Terblokir	Terblokir	Terblokir	Terblokir	Terblokir	Kurang Memuaskan

Sumber: Penulis (2025)

Berdasarkan data tabel 2, hasil keseluruhan analisis keamanan jaringan rata-rata hasil analisisnya "memuaskan". Maka dapat peneliti simpulkan dampak setelah manajemen keamanan sumber daya jaringan pengguna berhasil.

Evaluasi implemantasi konfigurasi *firewall* sebagai kontrol akses pada SMK Kristen Seriti, pengujian terakhir dilakukan dengan pembatasan hak akses situs internet yang telah di blokir sesuai dengan kebijakan SMK Kristen Seriti, dimana pada pengujian ini dilakukan dengan mencoba mengakses situs yang telah masuk *listing* pada fitur NAT salah satunya situs hiburan *facebook*. Hal ini berfungsi menjaga keamanan jaringan dari pemakaian tidak berhubungan dengan pembelajaran yang tentunya tidak berguna sebagai ilmu pengetahuan.



Gambar 16. Tampilan Saat Membuka Situs Terblokir

Sumber: Penulis (2025)

Pembahasan Penelitian

Pembahasan yang dilakukan pada penelitian ini yaitu membahas tentang pengembangan manajemen keamanan jaringan nirkabel (Wifi) Menggunakan Routerboard Mikrotik dan Firewall pada SMK Kristen Seriti. Dalam pengembangan jaringan menggunakan jenis penelitian R&D dengan model penelitian NDLC.

Perbedaan penelitian penulis dengan penelitian sebelumnya yaitu, penelitian yang dilakukan penulis merupakan penelitian yang dilakukan untuk mengembangkan sistem manajemen keamanan jaringan menggunakan Routerboard Mikrotik dan Firewall dengan jenis penelitian R&D dan model penelitian NDLC dengan hasil penelitian berupa sistem keamanan jaringan yang menjadi lebih baik dan terstruktur, sedangkan pada penelitian sebelumnya melakukan analisis serta pengembangan jaringan wireless berbasis mikrotik router diberbagai tempat ada yang mengembangkan sistem jaringan wireless menggunakan autentifikasi keamanan jaringan dan menghasilkan jaringan wireless tipe infrastruktur dalam penelitiannya. Adapun keunggulan dari pengembangan manajemen keamanan jaringan nirkabel (Wifi) tersebut yaitu dari kegunaan (usability) serta dari segi keamanan jaringan yang dapat berjalan secara efektif dan tidak lagi menghambat staff dalam mengakses internet dan dapat mempermudah siswa maupun guru dalam proses belajar mengajar. Adapun kekurangan dari pengembangan manajemen keamanan jaringan nirkabel (Wifi) tersebut yaitu membutuhkan monitoring lanjutan dan maintenance secara berkala agar keamanan jaringan dapat berfungsi dengan baik dalam jangka panjang.

Peneliti Fauzi, Muhyidin & Singasatia (2023) Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS). Hasil dari penilitian ini adalah suatu rancangan system keamanan jaringan komputer berbasis Intrusion Detection System (IDS) menggunakan snort dan portsentry untuk mendeteksi adanya sebuah serangan yang masuk ke dalam jaringan komputer Madrasah Aliyah Negeri Purwakarta seperti Ping icmp,nmap (port scan) dan DDOS, dengan mendapatkan sebuah notifikasi serangan yang masuk ke jaringan komputerm, serangan tersebut dapat dicegah dengan menerapkan portsentry sehingga serangan seperti Ping icmp,nmap dan DDOS tidak akan bisa masuk ke dalam jaringan komputer.

Peneliti Muhammad dan Hasan (2020) Analisa dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu. Hasil penelitian menunjukkan bahwa jaringan wireless dengan Mikrotik router OS v.5.20 pada PC router untuk mengkonfigurasikan management bandwidth, web filtering dan user management dapat mengamankan dan mengoptimalkan fungsi jaringan wireless yang ada.

Dalam proses pengembangan manajemen keamanan jaringan nirkabel (Wifi) menggunakan Routerboard Mikrotik dan Firewall telah melalui berbagai tahapan yang dilakukan berdasarkan dengan metode penelitian yang digunakan oleh peneliti yaitu metode R&D dan NDLC dengan melakukan pengujian yang dilakukan dengan berfokus pada fungsi sistem saja dengan hasil yang bisa diartikan bahwa pengembangan manajemen keamanan jaringan nirkabel (Wifi) layak digunakan oleh SMK Kristen Seriti, dapat dilihat data yang ada pada tabel , hasil keseluruhan analisis keamanan jaringan rata-rata hasil analisisnya "memuaskan". Maka dapat peneliti simpulkan dampak setelah manajemen keamanan sumber daya jaringan pengguna berhasil.

Hasil akhir dari penelitian yang telah dilakukan oleh penulis yaitu adanya sebuah pengembangan manajemen keamanan jaringan nirkabel (Wifi) pada SMK Kristen Seriti melalui tahapan pengujian yang sudah dilakukan.

KESIMPULAN

Berdasarkan hasil implementasi yang telah dijelaskan dan paparkan, maka peneliti memberi kesimpulan, bahwa:

1. Penelitian yang telah dilakukan yaitu mengembangkan manajemen keamanan jaringan nirkabel (Wifi) menggunakan Routerboard Mikrotik dan Firewall sehingga dapat disesuaikan dengan kebutuhan serta efisiensi terhadap manajemen keamanan jaringan nirkabel (Wifi) pada SMK Kristen Seriti.
2. Dengan diterapkan manajemen keamanan jaringan nirkabel (Wifi), maka proses pekerjaan staff SMK Kristen Seriti akan berjalan secara efektif dan tidak lagi menghambat staff dalam mengakses internet. Cara yang dilakukan untuk mengimplementasikan manajemen keamanan jaringan nirkabel (Wifi) SMK Kristen Seriti yaitu dengan datang langsung ke tempat penelitian kemudian mengkonfigurasi mikrotik ke jaringan SMK Kristen Seriti kemudian menginstal Routerboard Mikrotik dan Firewall untuk memonitoring jaringannya dan untuk memvalidasi jaringan pada SMK Kristen Seriti dengan cara membatasi pengguna, Firewall jaringan selalu dalam keadaan aktif pada semua pengujian, menunjukkan bahwa sistem keamanan dasar berfungsi dengan baik. Situs hiburan dan situs terlarang semuanya dalam status terblokir, yang mengindikasikan bahwa kebijakan pembatasan akses diterapkan secara konsisten.

Saran

Berdasarkan hasil kesimpulan di atas, maka peneliti memberi saran, bahwa:

1. Diharapkan agar manajemen keamanan jaringan nirkabel (Wifi) yang diusulkan untuk laboratorium komputer dan jaringan WiFi di SMK Kristen Seriti dapat memberikan kemudahan bagi para pendidik, peserta didik dan tenaga kependidikan dalam mencapai hasil kerja yang optimal bagi sekolah.
3. Adapun kekurangan dari pengembangan manajemen keamanan jaringan nirkabel (Wifi) tersebut yaitu membutuhkan monitoring lanjutan dan maintenance secara berkala agar keamanan jaringan dapat berfungsi dengan baik dalam jangka panjang.
4. Untuk lebih mengoptimalkan pemakaian, pihak sekolah dapat menambahkan jumlah keamanan jaringan nirkabel (Wifi) pada provider atau jasa layanan produk internet. Selain itu diharapkan adanya seorang teknisi jaringan yang dapat mengelola dan mengatasi permasalahan jaringan.
5. Untuk penelitian selanjutnya, disarankan untuk mengeksplorasi metode manajemen keamanan jaringan yang lebih efisien dan mengembangkan solusi yang dapat diterapkan pada berbagai kondisi jaringan di sekolah, termasuk pengaruhnya terhadap kualitas pembelajaran online dan efektivitas operasional sekolah secara keseluruhan.

DAFTAR PUSTAKA

- Al Fauzan, M. A., & Purwanto, T. D. (2021, June). Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 3, No. 1, pp. 137-146).
- Alamsyah, M., & Fatdha, S. E (2020). Penerapan metode Student Teams Achievement Division (STAD) dalam media pembelajaran multimedia kreatif. *Jurnal Teknologi Dan Open Source*, 3(2), 439804.
- Amriansyah. (2020). Pengukuran dan Analisa Pengaruh Interferensi Bluetooth Terhadap Kinerja Jaringan WLAN 802.11b. *Fakultas Teknik Universitas Mataram*, pp. 1-6.
- ARIF, B., Alex, W., & Qoriani, W. (2020). Redesain Jaringan Komputer Di Dinas Pendidikan Pemuda, Olahraga Dan Pariwisata (Disdikporapar) Kabupaten Banyuwasin SUM-SEL

- (Doctoral dissertation, Universitas Bina Darma).
- Fauzi, R., Muhyidin, Y., & Singasatia, D. (2023). Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS). *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 7(1), 72-86.
- Firmansyah, F., Wahyudi, M., & Purnama, R. A. (2019). Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP. *Juita*, 7(2), 129-135.
- Herusutopo, A., Prasetyo, (2019). Analisis dan Optimalisasi Jaringan Nirkabel dengan Minimalisasi Roaming di Binus Square. Universitas Bina Nusantara. [Http://Journal.Binus.ac.id](http://Journal.Binus.ac.id)
- Khasanah, (2020). Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus PT. Sukses Berkat Mandiri Jakarta). *STMIK Nusa Mandiri Jakarta*. <http://nusamandiri.ac.id>
- Muhammad Muhammad, Ibrahim Hasan, At All. (2020), Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu, Vol.2 No.1 Januari-Juni. *Stmik Bina Mulia Palu*.
- Mulyanto, Y., & Prakoso, S. B. (2020). Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawa dengan Metode Network Development Life Cycle (NDLC) Rancang Bangun Jaringan.
- Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, 2(01), 14-20
- Noviriandini, A., Hermanto, H., Ambarsari, D. A., & Eriawan, D. (2022). Analisis Management Bandwidth Dan Firewall Dengan Router Mikrotik Pada Pt. Bca Multifinance. *Jurnal Teknik dan Science*, 1(3), 40-45..
- Nurhasanah, E. (2021). Pengembangan Multimedia Pembelajaran Sejarah Perkembangan Islam Berbasis Macromedia Flash untuk Meningkatkan Hasil Belajar Mahasiswa. *Ainara Journal (Jurnal Penelitian Dan PKM Bidang Ilmu Pendidikan)*, 2(3), 148-153
- Pamungkas, N. H. T. (2020). Strategi Teknologi Pelatihan dan Sertifikasi Angkatan Muda Informatika di Indonesia. *INDIKATOR*, 1(1), 62-72.
- Rosyidi, S., Wonggo, D., & Djamen, A. C. (2022). Analisis dan Perancangan Jaringan Wireless Local Area Network di SMP. *Edutik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, 2(2), 268-279.
- Setiadi, A., Yuliatmojo, P., & Nurhidayat, D. (2018). Pengembangan aplikasi Android untuk pembelajaran pneumatik. *Jurnal Pendidikan Vokasional Teknik Elektronika (JVOTE)*, 1(1), 1-5.
- Setiawan, M. K., & Putra, P. P. (2020). Jurnal: analisa kinerja koneksi jaringan komputer pada smk teknologi bistek palembang.
- Siahaan, B. P., Pardede, A. M., & Syahputra, S. (2022). Bandwidth Management and Web Filtering with Per Connection Queue (PCQ) Method Using Mikrotik. *International Journal of Health Engineering and Technology (IJHET)*, 1(2).
- Siaulhak. Dkk. (2017). Manajemen Jaringan Bandwidth Dan Manajemen User Berbasis Mikrotik Pada Sekolah Menengah Kejuruan (Bandwidth Network Management And User Management Microtic Based At Vocational High School). Program Studi Pendidikan Teknologi Dan Kejuruan. Program Pascasarjana Universitas Negeri Makassar.
- Sumule, O., Angkasa, W. I., & Retno, H. W. (2020). Manfaat dan Hambatan Pengembangan jaringan inovasi Bagi Peningkatan Daya Saing UKM perikanan. *Prosiding symposium nasional kelautan dan perikanan*, (7).Tim Penyususun Kamus Pusat Bahasa , Kamus Besar Bahasa Indonesia, Jakarta: Balai Pustaka, 2007, h.538.
- Syaifudin, A., & Assegaff, S. (2020). Analisis dan Pengembangan Manajemen Jaringan dengan Menggunakan Mikrotik RB750 Pada PPM Al-Hidayah Jambi. *Jurnal Manajemen Sistem Informasi*, 5(1), 49-60.
- Wahyudin, Y., & Rahayu, D. N. (2020). Analisis metode pengembangan sistem informasi berbasis website: a literatur review. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, 15(3), 119-133.

- Winardi (2019). Optimalisasi Jaringan Lokal. Universitas Telkom Bandung (<http://repository-utb.ac.id/optimalisasi-jaringan-lokal>)
- Zaki, R. W., Fayed, H. A., Abd El Aziz, A., & Aly, M. H. (2019). Outdoor visible light communication in intelligent transportation systems: Impact of snow and rain. *Applied Sciences*, 9(24), 5453.