BAB V

PENUTUP

A. Kesimpulan

Kesimpulan dari penelitian tentang *autentikasi* jaringan *WiFi* menggunakan metode *login* otomatis dengan *MAC Address* untuk meningkatkan keamanan jaringan *WiFi* PKBM RONAA, dengan fokus pada penggunaan *Router Board RB750 Gr3* sebagai alat konfigurasi dan penerapan *Network Development Life Cycle (NDLC)*, adalah sebagai berikut:

1. Implementasi metode *login otomatis* dengan *MAC Address* dapat efektif meningkatkan keamanan jaringan *WiFi* PKBM RONAA dengan membatasi akses hanya kepada perangkat-perangkat yang telah terdaftar. Hal ini mengurangi risiko akses tidak sah dan memperkuat pertahanan jaringan secara keseluruhan.
2. Penelitian ini secara khusus memusatkan perhatian pada jaringan *WiFi* di PKBM RONAA, mempertimbangkan kebutuhan dan konteks spesifik lembaga tersebut dalam meningkatkan keamanan dan efisiensi jaringan.
3. Pemilihan *Router Board RB750 Gr3* sebagai alat konfigurasi menunjukkan komitmen untuk menggunakan perangkat yang dapat diandalkan dan sesuai dengan kebutuhan jaringan yang ada di PKBM RONAA.
4. Penggunaan *Network Development Life Cycle (NDLC)* sebagai metodologi pengembangan memastikan bahwa implementasi dan pengelolaan jaringan *WiFi* dilakukan secara terstruktur dan terencana. *NDLC* membantu dalam tahap perencanaan, pengembangan, implementasi, dan pemeliharaan jaringan *WiFi* dengan mempertimbangkan aspek keamanan sebagai prioritas utama.

Setelah penulis melakukan penerapan pada PKBM RONAA, perancangan sistem tersebut telah berhasil diterapkan. Pengujian dilakukan oleh penulis dan diawasi langsung oleh operator PKBM RONAA, hasil pengujian sistem tersebut mewujudkan peningkatan keamanan jaringan *WiFi* dengan *login* otomatis menggunakan *MAC Address* dan manajemen *bandwidth* dari karyawan, guru serta siswa dari PKBM RONAA.

B. Saran

Adapun beberapa saran yang disampaikan oleh penulis berdasarkan penelitian ini adalah sebagai berikut:

1. Meskipun *autentikasi MAC Address* meningkatkan keamanan, disarankan untuk melengkapi dengan mekanisme keamanan tambahan seperti implementasi *firewall* untuk mencegah akses tidak sah dari luar jaringan.
2. Perbarui secara berkala daftar *MAC address* perangkat yang diizinkan untuk mengakses jaringan. Hal ini penting untuk memastikan bahwa hanya perangkat yang masih digunakan yang dapat terhubung, dan mencegah perangkat yang tidak sah atau usang mendapatkan akses.
3. Disarankan untuk *menonaktifkan MAC Address* acak pada perangkat *handphone* yang akan di daftarkan *MAC Address* nya.
4. Lakukan *monitoring* dan *audit* jaringan secara rutin untuk mendeteksi aktivitas yang mencurigakan atau tidak sah.
5. Operator jaringan disarankan melakukankukan *Maintenance* Jaringan secara berkala untuk menjaga jaringan tetap beroperasi dengan baik dan efisien.