BAB 1
PENDAHULUAN

1.1 Latar Belakang

Di era menuju *society* 5.0 bahwa masyarakat yang berpusat pada manusia dan berbasis teknologi sebagai tujuan menaikkan kualitas hidup secara berkelanjutan seperti saat ini, penggunaan *device* seluler yang cerdas tak jarang diterapkan serta digunakan. Kegunaan seperti *device* laptop (*notebook*) dan *smartphone* yang memakai media sinyal gelombang mampu menjadikan lebih mudah secara mobilitas serta mempercepat aktivitas, selain itu *device* seluler yang cerdas pula ada teknologi yang bisa mempermudah pekerjaan manusia satu di antara yang ada ialah jaringan nirkabel (*Wireless Local Area Network*). *Wireless Local Area Network* menjadi sesuatu hal yang menarik bagi pengguna, karena dapat menggunakan jaringan internet dengan kelebihan pada mengakses jaringan internet lebih praktis secara *Wireless*, *Wireless Local Area Network* juga sering dijumpai di beberapa lokasi antara lain sekolah, kampus, perpustakaan, perkantoran, area publik, *cafe* serta lokasi lain yang memiliki titik internet secara *Wireless Local Area Network*.

Namun, dengan segala kemudahan teknologi nirkabel (*Wireless Local Area Network*). Selalu diikuti dengan kemajuan teknologi privasi dari produsen perangkat *End device* karena pada saat ini produsen perangkat *End device* sedang membuat teknologi baru, yaitu *Random* MAC *Address* sebab alamat MAC *Address* dipergunakan oleh perangkat ketika menghubungkan ke jaringan *Wireless Local Area Network* (Andres Gomez et al., 2022). Karena alamat MAC *Address* ini ditransmisikan tanpa enkripsi, alamat tersebut dapat ditangkap dan dipergunakan untuk melacak lokasi pengguna secara potensial. Secara historis, perangkat memakai MAC *Address* pabrik buat terhubung ke jaringan *Wireless Local Area Network*. MAC *Address* pabrik secara global unik serta statis, memungkinkan perangkat dilacak dan diidentifikasi satu per satu. Atas dasar ini lahir teknologi *Random* MAC *Address* atau bisa disebut *Random* MAC *Address* untuk meningkatkan privasi pengguna dengan memakai MAC *Address* secara *Random* ketika setiap kali

menghubungkan ke jaringan *Wireless Local Area Network*.

Saat masa *new* normal ini, sekolah maupun kantor sudah menerapkan peraturan 50% tatap muka yang membuat para siswa dan pegawai sudah mulai masuk serta mulai menggunakan akses jaringan *Wireless Local Area Network* dengan perangkat *End device* android atau laptop (*notebook*) versi baru (10,12, iOS 16, windows 10) yang mana *default* konfigurasi pada jaringan nirkabel perangkat *End device* tersebut telah menggunakan *Random* MAC *Address*. Yang membuat timbul masalah dalam keamanan manajemen jaringan dari asal sisi *End device* menciptakan sebuah permasalahan terhadap sebuah manajemen jaringan *Wireless Local Area Network.* Serta keamanan yang masih menerapkan standar keamanan *Wireless* yang pada umumnya yaitu WPA/WPA2-PSK (Bagas Permadi et al., 2020), mengakibatkan sistem manajemen jaringan *Wireless Local Area Network* yang sudah diatur oleh administrator jaringan jadi tidak berjalan normal atau sama sekali tidak berjalan serta tidak bisa mengidentifikasi pengguna yang mengakses jaringan *Wireless Local Area Network*. Karena hal tersebut, tentu *update* sistem manajemen dan keamanan dari *Wireless Local Area Network* sangatlah penting karena kemajuan teknologi perangkat *End device* itu sendiri juga akan sangat cepat.

Berawal dari lingkup manajemen dan keamanan jaringan *Wireless Local Area Network* di area yang kecil beberapa *Access Point*, berubah menjadi lingkup manajemen dan keamanan jaringan *Wireless Local Area Network* yang luas memiliki banyak *Access Point* dan kompleks dalam skala besar, maka dapat menimbulkan masalah bagi administrator jaringan yang kompleks dan rumit karena pembaruan teknologi *Random* MAC *Address* ini. Oleh karenanya perlu adanya sebuah peningkatan keamanan sekaligus manajemen yang diterapkan pada mikrotik sebagai router dari *Access Point Wireless Local Area Network* yang berfungsi untuk mencegah serangan *Random* MAC *Address* dari perangkat *End device* secara optimal tanpa mengganggu sistem yang sudah berjalan seperti manajemen bandwidth dan lain-lain.

Berdasarkan latar belakang di atas, maka penelitian ini membuat

sebuah peningkatan sistem keamanan dan manajemen yang dapat mencegah serangan *Random* MAC *Address* dengan dasar melakukan analisis dengan pendekatan secara literatur pada penelitian terdahulu yang ada mengenai keamanan jaringan *Wireless Local Area Network* yaitu implementasi EAP-TLS protokol yang paling aman dalam metode otentikasi untuk *Wireless Local Area Network*, karena wajib menggunakan digital sertifikat untuk mengotentikasi *Server* ke klien dan klien untuk *Server*. Namun, ini lebih kompleks dan mahal karena memerlukan pemasangan sertifikat unik untuk setiap klien serta menjadi tugas yang sangat rumit bila diterapkan dalam instalasi *Wireless Local Area Network* yang besar (Abo-Soliman & Azer, 2018). Implementasi protokol otentikasi EAP PEAP-MSCHAPv2 memiliki keunggulan berupa hanya menggunakan sertifikat digital pada sisi *Server*, sedangkan di sisi klien tidak wajib menggunakan sertifikat digital klien melainkan bisa digantikan dengan menggunakan *username* dan *password*, serta protokol ini bersifat *mutual Authentication* yang membuat skema implementasi EAP PEAP-MSCHAPv2 fleksibel serta dapat meningkatkan efisiensi dari pada EAP-TLS (Wati & Apriansyah, 2019). Dari kedua literatur di atas bahwa ada protokol yang memiliki implementasi yang sama dari EAP PEAP-MSCHAPv2 adalah protokol EAP-TTLS. Didapatkan analisis bahwa EAP PEAP-MSCHAPv2 dan EAP-TTLS dari segi implementasi sama hanya saja yang membuat beda yaitu vendor atau distributor.

Dipilih pemasangan teknologi keamanan *Wireless Local Area Network* dengan protokol otentikasi EAP PEAP-MSCHAPv2 karena dari segi keamanan masuk kategori aman sebab sudah *mutual Authentication* serta lebih fleksibel dari EAP-TLS. Memakai mekanisme standar 802.1x, yaitu kombinasi *username* serta *password* untuk menggantikan sertifikat digital pada sisi *Client* yang opsional. Dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat untuk manajemen beberapa layanan di jaringan *Wireless Local Area Network* melalui *User Manager* v7 yang mengalami pembaruan yaitu tidak lagi menggunakan antarmuka *web base* melainkan sekarang sudah menyatu dalam winbox mikrotik sebagai implementasi *Radius Server* di RouterOS

Mikrotik. Dengan harapan kedua teknologi tersebut akan dapat mencegah serangan *Random* MAC *Address* yang mengganggu keamanan dan manajemen jaringan *Wireless Local Area Network* yang sudah diterapkan oleh administrator jaringan.

Karena hal tersebut, penulis akan melakukan penelitian dengan judul **"Pengamanan Jaringan *Wireless* LAN Dengan Menggunakan *Authentication*, *Authorization*, *Accounting* (AAA) Dalam Mencegah Serangan *Random* MAC *Address*"**

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, penulis menarik suatu persoalan yang kemudian dicari pemecahan penyelesaiannya, yang dapat disimpulkan bahwa terdapat rumusan masalah sebagai berikut:

1. Bagaimana metode dan cara penerapan keamanan serta manajemen jaringan *Wireless* LAN menggunakan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* mikrotik dalam mencegah serangan *Random* MAC *Address*?
2. Apakah penerapan keamanan serta manajemen jaringan *Wireless* LAN menggunakan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* mikrotik bisa dapat mencegah serangan *Random* MAC *Address?*

1.3 Tujuan Penelitian

Tujuan penelitian berdasarkan penjabaran penulisan latar belakang dan rumusan masalah dalam hal ini adalah penerapan teknologi keamanan *Wireless* LAN dengan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius*

Server mikrotik untuk mencegah serangan *Random* MAC *Address* pada jaringan *Wireless Local Area Network*.

1.4 Manfaat

Merujuk pada latar belakang, rumusan masalah, serta tujuan penelitian yang sudah diuraikan di atas, maka dapat diperoleh bahwa penelitian ini mempunyai manfaat sebagai berikut:

1. Luaran dapat membantu peningkatan sistem keamanan manajemen jaringan *Wireless* LAN dan bisa mencegah serangan *Random* MAC *Address*.
2. Dapat menjadi *Security control* sekaligus manajemen dengan teknologi keamanan *Wireless* LAN menggunakan protokol otentikasi *PEAP*-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* mikrotik untuk manajemen jaringan yang aman, mudah dan tidak menghambat sistem jaringan yang telah berjalan.
3. Manfaat secara umum menjadikan referensi atau dasar untuk penelitian seterusnya yang terkait tentang peningkatan sistem keamanan serta manajemen jaringan *Wireless* LAN terbaru yang dapat mencegah serangan *Random* MAC *Address*.

1.5 Ruang Lingkup

Pada Penjabaran latar belakang sebelumnya, penulis menetapkan ruang lingkup dari pembahasan pada penelitian ini sebagai berikut:

1. Sistem keamanan dan manajemen menggunakan teknologi keamanan *Wireless Local Area Network* dengan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* mikrotik, bekerja pada jaringan *Wireless Local Area Network* dalam mencegah serangan *Random* MAC *Address*.

2. Penelitian ini berfokus membahas metode dan cara mencegah serangan *Random* MAC *Address* dengan teknologi keamanan *Wireless Local Area Network* dengan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication, Authorization, Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* mikrotik, menargetkan seluruh perangkat *End device* yang ada di jaringan.
3. Router, serta *Access Point* yang digunakan adalah Mikrotik RB750Gr3 dan Ubiquiti UniFi AP AC Lite.
4. Dalam penelitian ini teknologi model protokol *Authentication, Authorization, Accounting* (AAA) diterapkan dalam *User Manager* v7 saja di *Radius Server* mikrotik RB750Gr3.
5. Perangkat *End device* yang digunakan adalah android atau laptop (*notebook*) versi baru (Android 10, 12, iOS 16 dan windows 10).

1.6 Luaran Yang Diharapkan

Luaran yang dapat diterapkan pada pembahasan penelitian ini yaitu sebuah peningkatan sistem keamanan dan manajemen yang dapat digunakan oleh administrator jaringan sebagai keamanan jaringan *Wireless* LAN untuk mencegah serangan *Random* MAC *Address*.

1.7 Sistematika Penulisan

Berikut ini adalah sistematika penulisan berupa uraian rinci setiap bab secara tertulis yang menjelaskan kesinambungan setiap bab satu sama lain yang akan dijelaskan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi dan membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi dan menjelaskan landasan teori yang akan mendukung penelitian Pengamanan Jaringan *Wireless* LAN

Dengan Menggunakan *Authentication, Authorization, Accounting* (AAA) Dalam Mencegah Serangan *Random* MAC *Address*, dari metode-metode yang menjadi dasar analisis permasalahan yang ada dan pemecahannya, tinjauan pustaka ini diperoleh dari studi kepustakaan mengenai hal-hal yang berkaitan dengan penelitian ini.

BAB 3 METODE PENELITIAN

Bab ini membahas secara rinci tahapan dan metode penelitian yang digunakan untuk memecahkan masalah penelitian serta untuk mencapai tujuan penelitian yang diharapkan.

BAB 4 HASIL DAN PEMBAHASAN

Di dalam bab ini, terdapat pembahasan yang mendalam mengenai analisis dan pengujian terhadap permasalahan yang muncul selama proses penelitian berlangsung. Selain itu, juga dibahas secara rinci mengenai analisis, pengujian, dan konfigurasi yang terkait dengan sistem keamanan *Wireless* LAN.

BAB 5 SIMPULAN DAN SARAN

Bab ini membahas sebuah kesimpulan yang disimpulkan dari hasil analisis dan pengujian sistem dalam penelitian ini, serta memberikan saran yang berharga dari penulis untuk pengembangan penelitian di masa mendatang.

DAFTAR PUSTAKA

LAMPIRAN