BAB II

LANDASAN TEORI

2.1. JARINGAN KOMPUTER

2.1.1. Pengertian Jaringan Komputer

Menurut Hadi [6] "jaringan komputer adalah kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri lebih satu komputer yang saling berhubungan". Sedangkan [7] menyatakan "jaringan komputer adalah sekumpulan komputer, *printer,*peralatan lainnya yang saling terhubung.informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen atau data".

Didalam buku Wahana Komputer [8] "jaringan komputer adalah sistem yang terdiri dari komponen-komponen serta piranti-piranti yang saling terhubung sebagai satu kesatuan. Dengan dihubungkannya piranti tersebut, alhasil dapat saling berbagi sumber daya antar satu piranti dengan piranti lainnya".

Jaringan komputer adalah kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang dapat saling terhubung, dan bergerak melalui kabel-kabel sehingga dapat memungkinkan pengguna bisa saling bertukar dokumen atau data antar satu piranti dengan piranti lainnya.[6],[7],[8]

2.2 Jaringan Nirkabel

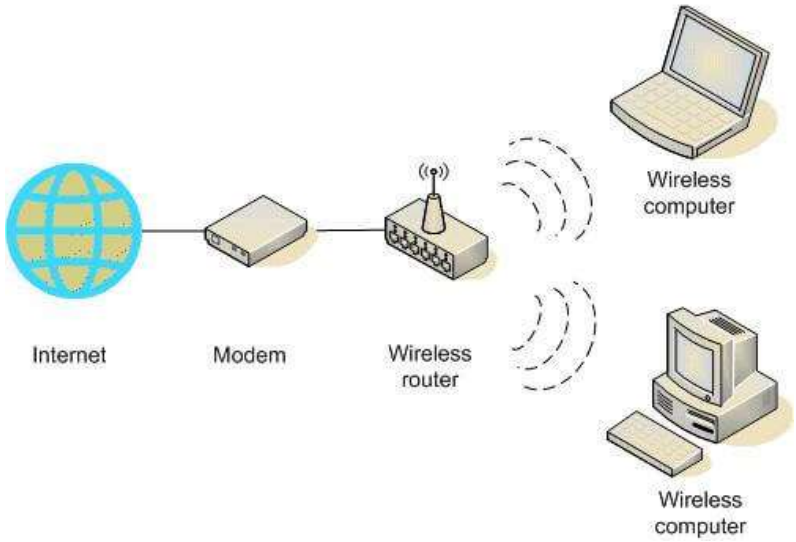
2.2.1. Pengertian Jaringan Nirkabel

Didalam buku Wahana Komputer [8] "Jaringan Nirkabel adalah jaringan yang lebih mudah dibuat serta perawatannya tidak mahal. Jika jumlah komputer

banyak, jaringan nirkabel ini lebih murah jika dibandingkan jaringan kabel. Tidak adanya kabel digantikan dengan gelombang radio".

"Jaringan Nirkabel adalah teknologi jaringan yang tidak menggunakan atau membutuhkan kabel sebagai media teransfer data atau melakukan komunikasi antara satu perangkat ke perangkat yang lainnya" [9]. sedangkan menurut [10] " jaringan nirkabel adalah sekumpulan komputer yang saling terhubuntg antara satu dengan lainnya sehingga tercipta sebuah jaringan komputer yang menggunakan media udara atau gelombang sebagai jalur lintas datanya.

Jaringan nirkabel adalah jaringan komputer yang lebih mudah dibuat dan tidak menggunakan kabel sebagai media transfer data akan tetapi menggunakan media udara atau gelombang radio sebagai jalur lintas datanya.[8],[9],[10]



Gambar 2.1 Jaringan Nirkabel [9]

2.2.2. Topologi Jaringan Nikabel

Anas, Soepriyanto dan Susilaningsih [11] menyatakan "Topologi adalah cara menghubungkan beberapa komputer sehingga menciptakan sebuah jaringan

komputer. Topologi jaringan memiliki berbagai bentuk susunan komputer dengan berbagai jenis kabel, konektor dan spesifikasi yang berbeda". sedangkan menurut Halawa [12] "Topologi merupakan suatu aturan untuk menghubungkan komputer satu sama lain secara fisik dan hubungan antara yang berkomunikasi sehingga jaringan komputer dapat terbentuk. Dalam suatu jaringan komputer memilih topologi akan sangat mempengaruhi kecepatan komunikasi".

Topologi adalah sebuah aturan atau standar dalam membangun sebuah jaringan komputer yang nantinya sangat mempengaruhi spesifikasi dalam sebuah jaringan mulai dari kecepatan berkomunikasi antara satu komputer dengan komputer lainnya, hingga dari segi keamanan jaringan yang ada. [11],[12]

2.2.3. Jenis – jenis Topologi Jaringan Nirkabel

1. **Topologi *Ad-Hoc***

Menurut Zam [13] "Topologi *Ad-Hoc* adalah perangkat komputer yang terhubung melalui jaringan nirkabel dengan tidak menggunakan perantara, atau boleh di bilang sebagai koneksi *peer to peer*". Sedangkan [14] menyatakan "Topologi *Ad-Hoc* adalah Sebuah grup dengan dua atau lebih *station* nirkabel yang saling berkomunikasi tanpa harus menggunakan *access point*".

"Topologi *Ad-Hoc* adalah jaringan yang memiliki dua atau lebih *client* atau *device wireless* berkomunikasi secara langsung dalam radius 300 kaki, *Device* ini dapat saling berhubungan berdasarkan nama *Service Set Identifier* (SSID)". [15]

Topologi Ad-Hoc adalah sebuah atau sekumpulan *client* yang berkomunikasi melalui jaringan nirkabel secara langsung tanpa harus menggunakan perangkat jaringan yaitu *access point* sebagai alat komunikasinya.[13],[14],[15]

2. Topologi Infrastuktur

Menurut Manurung dan Mubarakah [14] **"**Topologi Infrastruktur adalah struktur jaringan yang didukung oleh *WLAN* IEEE 802.11 yang setiap *station* membutuhkan *access point* untuk saling berkomunikasi". Sedangkan menurut Kartini dan Adiansyah [15] "Topologi Infrastruktur adalah Jaringan *server based* yang memerlukan sebuah komponen khusus yang memiliki fungsi sebagai *access point*. Masing-masing *client* akan mengirimkan datanya ke *access point*. Sedangkan Menurut Zam [13] "Topologi Infrastruktur adalah komputer yang terhubung melalui *wireless* atau nirkabel yang dinamakan dengan *wireless access point*",

Topologi infrastruktur merupakan struktur jaringan yang di mana setiap pengguna akan menggunakan *access point* sebagai penghubung untuk melakukan komunikasi antar pengguna satu dengan pengguna lainnya.[13],[14],[15]

2.3. KEAMANAN JARINGAN KOMPUTER

2.3.1. Pengertian Keamanan Jaringan Komputer

Menurut Fahriani, Devi dan Aditama [16] "Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan".

Purba dan Effendi [17] menyatakan "keamanan jaringan merupakan sistem yang dapat menjamin agar dapat meminimalisir ataupun bahkan menghilangkan kerugian yang disebabkan oleh serangan keamanan jaringan tersebut". sedangkan menurut [18] "Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin

ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak".

Keamanan jaringan komputer adalah bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta juga memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan dan meminimalisir ataupun bahkan menghilangkan kerugian yang disebabkan oleh serangan keamanan jaringan tersebut.[16],[17],[18]

2.3.2. Jenis – Jenis Ancaman Keamanan Jaringan Wireless

1. ***ARP Poisioning* (*Address Resolution Protocol*)**

ARP (*Address Resolution Protocol*) *poisoning* ini adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengendus *frame* data pada jaringan lokal dan atau melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*. ARP *spoofing* merupakan konsep dari serangan penyadapan diantara terhadap dua mesin yang sedang berkomunikasi atau yang disebut dengan MITM (*Man in The Middle Attack*). [19]

2. ***Cracking WPA/WPA Keys***

WPA dan WPA2 merupakan protokol keamanan yang diciptakan untuk mengatasi permasalahan pada WEP. Penggunaan WPA dan WPA2 akan menyulitkan *hacker* dalam melakukan injeksi paket, mengirimkan paket yang

diambil sebelumnya (*replay attack*), atau serangan lain yang mengancam WEP. *Hacking* terhadap jaringan yang menggunakan WPAatau WPA2 menjadi jauh lebih sulit dilakukan . WPA dan WPA2 bisa dijalankan dengan dua modus yaitu personal menggunakan PSK(*pre shared key*) dan *enterprises* menggunakan server *RADIUS*. Kemungkinan *hacking* hanya bisa dilakukan pada WPA dan WPA2 PSKyang paling banyak digunakan oleh pengguna rumahan maupun perusahaan. WPA dan WPA2 PSK menggunakan *passphrase* yang harus diatur di setiap komputer seperti halnya WEP. Berbeda dengan *hacking* WEP, metode yang digunakan untuk melakukan *hacking* terhadap WPA dan WPA2 tidak bisa menggunakan metode statistik. WPA dan WPA2 mempunyai IV (*initial vector*) yang berubah-ubah sehingga tidak ada gunanya mengumpulkan paket data sebanyak-banyaknya seperti pada WEP untuk melakukan mendapatkan *keys* yang digunakan. *Hacking* dengan cara ini membutuhkan waktu yang sangat lama sehingga metode yang paling memungkinkan adalah *brute force* berdasarkan *dictionary file*. *Brute force* membutuhkan sebuah *file* yang berisi *passphrase* yang akan dicoba satu persatu dengan paket *handshake* untuk mencari *keys* yang digunakan. [19]

3. Bypassing MAC Address

Bypassing MAC address adalah proses mengubah identitas *MAC* untuk mengatasi *MAC address filtering*. *Attacker* dapat mengubah *MAC address* yang sesungguhnya agar bisa masuk ke dalam jaringan *WLAN* yang ingin diserang. Serangan *Bypassing MAC address* bisa dilakukan menggunakan media transmisi kabel karena tidak adanya otentikasikeamanan pada jaringan internet yang menggunakan media transmisi kabel. Mengganti *MAC address* memungkinkan

dilakukan pada sistem operasi *windows* karena *MAC address* telah dibaca pada NIC (*network interface card*) dan tersimpan pada basis data *windows registry*. [19]

4. Menyerang WPS Aktif

WPS (*Wireless Protected Setup*) adalah program sertifikasi opsional yang dikembangkan oleh aliansi *WiFi*. WPS dirancang untuk memudahkan pengaturan keamanan *WiFi* di rumah dan kantor kecil. WPS berguna jika suatu saat pemilik jaringan *WLAN* mengalami lupa password, hanya dengan menekan tombol WPS maka pemilik jaringan tersebut dapat mengkoneksikan perangkatnya secara otomatis. Jenis serangan ini hanya bisa menyerang jaringan WLAN bertipe otentikasi WPA_PSK dan WPS_PSK, dan memiliki tipe enkripsi TKIP. Jaringan WLAN pada *smartphone* tidak bisa diserang dengan cara ini karena otentikasinya sudah menggunakan WPA2_PSK. [19]

2.4 PERANGKAT JARINGAN

1. Router

Menurut Haryanto [7] "*Router* adalah suatu perangkat yang berfungsi untuk menghubungkan dua buah jaringan yang memiliki perbedaan pada lapisan *OSI* I, II, dan Ill, *misal LAN dengan Netware* akan dihubungkan dengan jaringan yang menggunakan *UNIX*.".

Didalam buku [8] "*Router* adalah piranti di mana *software* dan *hardware* di*setting* untuk melakukan *routing* dan mem-*forward* informasi. *Router* akan menghubungkan dua atau lebih *subnet*. *Routing* bekerja di *level* 3 dan berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu

jaringan ke jaringan lainnya". Sedangkan Yulinadoko [19] menyatakan "*Router* Merupakan perangkat keras yang memiliki komponen-komponen dasar yang sama dengan *PC desktop, router* mempunyai *CPU*, memori, sistem bus, dan banyak *interface input/output* sehingga banyak yang mengatakan bahwa *router* adalah sebuah komputer khusus. Akan tetapi *router* didesain untuk melakukan tugas khusus yang tidak dimiliki oleh *PC desktop*".

Router merupakan sebuah perangkat keras yang bekerja di lapisan ke tiga dalam *OSI layer* memiliki komponen yang hampir mirip dengan komputer, sehingga *router* dapat melakukan tugas khusus seperti melakukan *routing* dan mem-*forward* informasi dan menghubungkan dua atau lebih *subnet*.[7],[8],[19]

Dengan adanya perangkat *router* ini, data dari satu jaringan dengan protokol yang berbeda bisa diteruskan ke jaringan lain. Prinsip kerja *router* sebagai berikut :

a. Menggunakan alamat *network* yang berbeda pada semua *port*.
b. Membuat tabel berdasarkan alamat *layer network.*
c. Memfilter lalu lintas *network* berdasarkan informasi *network*
d. Memblokir lalu lintas ke alamat yang tidak diketahui

Gambar 2.2 *Router* [19]

2. Wi-Fi Adapter

Menurut [20] "*Wifi Adapter* adalah perangkat baru dan praktis pada teknologi *WIFI* saat ini. Alat ini mengambil *power* 5V dari *USB port* dari *PC*/Laptop. Untuk mempermudah *USB WIFI adapter* dengan fleksibel dapat ditempatkan pada *notebook* dan *PC*". sedangkan Rianto, Imamsyah dan Suryadi [21] menyatakan "*Wifi adapter* adalah alat yang membantu menerima sinyal *wifi* pada komputer atau laptop dengan jarak jangkau yang di capai dari *wireless USB* adapter tidak cukup luas".

Wifi Adapter sering juga disebut dengan *WLAN Card*. *Wifi Adapter* adalah alat yang dipakai pada perangkat komputer atau laptop agar dapat tersambung dengan koneksi *Wifi* yang tersedia di sekitarnya. Koneksi pada *wifi adapter* dapat terjadi dalam dua mode yaitu mode infrastruktur dan mode *ad hoc*. Pada mode infrastruktur, data pada jaringan ditransfer menggunakan *access point* yang berfungsi sebagai pusat.Semua koneksi yang terlibat dalam jaringan tersebut akan berbagi *identitas service set identifier (SSID)* yang sama sebagai *access point*. Selain itu juga akan menggunakan kode keamanan seperti *WEP* atau *WPA* sesuai dengan pengaturan. Sementara itu pada mode *ad-hoc*, koneksi jaringan tidak membutuhkan *access point* dan secara langsung bisa terhubung dengan semua perangkat *wireless*. Cara kerja dari *wifi adapter* ini sangat mudah sekali. Anda hanya perlu membuka *casing desktop* pada komputer untuk menambahkan *wifi adapter*. Kemudian pasang pada *slot PCI express* atau *slot* sejenis yang lainnya. Proses selanjutnya adalah tutup kembali *desktop* komputer dan lakukan *booting*.

Wifi Adapter merupakan sebuah perangkat yang penggunaanya praktis dan berfungsi sebagai alat yang menerima sinyal *wifi* pada komputer ataupun perangkat jaringan yang belum mendukung teknologi jaringan nirkabel.[20],[21]

Gambar 2.3 *Wi-Fi Adapter* [22]

2.5 MIKROTIK

2.5.1 Pengertian Mikrotik

Menurut Sabara dan Prayogi [23] "Mikrotik merupakan perangkat keras yang didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah system jaringan komputer skala kecil hingga yang kompleks sekalipun".

Prasetyo, Budiman dan Putra [24] menyatakan "Mikrotik adalah sebuah sistem operasi *router* yang bisa menjalankan dan mengatur aktivitas *network* secara menyeluruh. Mulai dari *management bandwidth, routing, billing hotspot, data user, load balancing,* hingga *routing BGP*".

MikroTik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup

berbagai fitur yang dibuat untuk *IP network* dan jaringan *wireless*, cocok digunakan oleh *ISP, provider hotspot*, & warnet.[23],[24]

Gambar 2.4 Mikrotik [24]

2.5.2 Jenis - Jenis Mikrotik

2.5.2.1 Mikrotik *Router OS TM*

Router OS merupakan router yang bisa dipasang menggunakan komputer manapun. Hal ini karena mikrotik jenis ini merupakan sebuah *software* yang dapat dipasang pada perangkat *PC* menggunakan bantuan *CD*. Mikrotik *Router OS TM* merupakan perangkat lunak dan *OS* yang diperuntukkan sebagai *router network*. Penggunaannya mencakup fitur untuk *wireless network* dan membuat *IP address*. Namun, juga dibekali oleh banyak fitur yang sangat bagus. [24]

Gambar 2.5 Mikrotik *Router OS* [23]

2.5.2.2 Mikrotik Router Board

Mikrotik *router board* merupakan jenis perangkat keras. Sehingga, terdapat bentuk fisik apabila ingin menjalankan program yang dimiliki olehnya. Namun, ukuran dari *hardware* tersebut sangat kecil sehingga tidak akan mengganggu. Fungsi dari *Router OS* ini sudah melekat pada *board* sehingga tidak tergantung pada *PC*. Namun, terdapat dalam sebuah *board* yang dimilikinya. Tertanam *processor*, *RAM, ROM*, dan *memory Flash*. Sehingga, sistem di dalamnya sangat terintegrasi satu sama lain. [24]

Gambar 2.6 Mikrotik *Router Board* [23]

2.6 METODE KEAMANAN JARINGAN WIRELESS

1. **WEP (*Wired Equivalent Privacy*)**

Daulay [25] menyatakan "WEP merupakan Shared Key atau WEP (*Wired Equivalent Privacy*) adalah suatu metode pengamanan jaringan nirkabel, disebut juga dengan *Shared Key Authentication* adalah metode otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukan (oleh administrator) ke *client* maupun *access point"*.

"WEP adalah Metode yang menggunakan *authentication* dengan "*shared key*" daripada "*open system*". Untuk "*open system*", dia tidak meng-*encrypt* data, tetapi hanya melakukan *otentifikasi client*" [26]. sedangkan menurut [27] "WEP Mendefinisikan protokol keamanan yang menyediakan keamanan dari segi otentikasi, enkripsi dan integritas data. Tujuan utama dari protokol WEP adalah berusaha untuk memberikan tingkat privasi yang diberikan kepada penggunaan jaringan berbasiskan kabel".

WEP adalah sebuah metode keamanan yang ada dalam teknologi jaringan nirkabel yang berfungsi untuk menyediakan keamanan dari segi otentikasi, enkripsi dan integritas data, cara kerja dari WEP menggunakan *authentication* dengan "*shared key*" daripada "*open system*". Untuk "*open system*", dia tidak meng-*encrypt* data, tetapi hanya melakukan *otentifikasi client*.[25],[26],[27]

2. WPA-PSK / WPA2-PSK (*Wi-Fi Protected Access Pre-Shared Key*)

"WPA-PSK atau WPA2-PSK merupakan pengamanan jaringan nirkabel dengan menggunakan metode WPA-PSK jika tidak ada authentikasi server yang digunakan. Dengan demikian *Access Point* dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Setelah *Shared-Key* didapat maka *client* yang akan bergabung dengan AP cukup memasukkan angka/kode yang diijinkan dan dikenal oleh AP. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metode *Shared-Key*. [27]"

Menurut Feraldi, Ringgo [28] “WPA-PSK merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS. Saat ini yang sudah dapat di *crack* adalah WPA-PSK, yakni dengan metode *brute force attack* secara *offline*. *Brute force* dengan menggunakan mencobacoba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *passphrase* yang yang digunakan *wireless* tersebut memang terapat pada kamus kata yang digunakan si *hacker*”. Sedangkan Daulay [25] menyatakan “WPA-PSK (*Wi-Fi Protected Access – Pre Shared Key*) adalah pengamanan jaringan nirkabel dengan menggunakan metode WPA-PSK jika tidak ada authentikasi *server* yang digunakan.sedangkan WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan *wired equivalent privacy* (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA. *Update* WPA2/WPS IE yang 9 mendukung WPA2 fitur berupa WPA2 *Enterprise* IEEE 802.1X menggunakan otentikasi dan WPA2 *Personal* menggunakan tombol *preshared* (PSK)”.

WPA-PSK atau WPA2-PSK adalah teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP, WPA-PSK atau WPA2-PSK menggunakan metode WPA-PSK jika tidak ada authentikasi *server* yang digunakan.sedangkan WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi

Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan *wired equivalent privacy* (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. [25],[27],[28]

2.7 MAC ADDRESS FILTERING

2.7.1 Pengertian Mac Address Filtering

Menurut Wijaya [22] "*MAC Address Filtering* merupakan metode *filtering* untuk membatasi hak akses dari *MAC Address* yang bersangkutan". Sedangkan menurut [10] " MAC Address Filtering adalah metode keamanan jaringan yang memfilter alamat MAC suatu perangkat yang fungsinya memberi list perangkat mana yang boleh menggunakan jaringan atau perangkat mana yang tidak diperbolehkan untuk menggunakan jaringan".

MAC-address filtering (alias *link-layer filtering*) adalah fitur untuk alamat IPv4 yang memungkinkan Anda untuk memasukkan atau mengeluarkan komputer dan perangkat berdasarkan alamat *MAC* mereka.Bila Anda mengkonfigurasi alamat *MAC filtering*, Anda dapat menentukan jenis hardware yang dibebaskan dari penyaringan. [10],[22]

2.7.2 Cara kerja Mac Address Filtering

WAP (*Wireless Access Point*) akan memperbolehkan memakai filter *media access control* (MAC) artinya dapat membuat "*white list*" dari komputer komputer yang boleh mengakses *wireless network*, berdasarkan dari MAC atau alamat fisik yang ada di *network card* masing-masing *pc*. Koneksi dari MAC yang tidak ada dalam list akan ditolak,

Pembuatan *Access list* untuk membuat manajemen *wireless client* berdasarkan *MAC Address*. Dengan pengaturan tersebut tidak semua *client* bisa terkoneksi, hanya *client* dengan *MAC address* yang sudah terdaftar pada *Access-List* yang dapat terkoneksi. Alamat MAC yang unik ditugaskan untuk setiap kartu, sehingga dengan *MAC filtering* pada izin jaringan dan menolak akses jaringan ke perangkat tertentu melalui penggunaan *black list* dan *White list*, Sedangkan pembatasan akses jaringan melalui penggunaan daftar sangat mudah, seorang individu tidak diidentifikasi oleh alamat MAC, bukan perangkat saja, jadi orang yang berwenang akan perlu memiliki entri daftar putih untuk setiap perangkat yang ia akan menggunakan untuk mengakses jaringan.

MAC filter fungsinya untuk menseleksi komputer mana yang boleh masuk ke dalam jaringan berdasarkan *MAC Address*. Bila tidak terdaftar, tidak akan bisa masuk ke jaringan *MAC filter Address* akan membatasi *user* dalam mengakses jaringan *wireless*. Alamat MAC dari perangkat komputer user akan didaftarkan terlebih dahulu agar bisa terkoneksi dengan jaringan wireless. [29]

2.8 HOTSPOT

2.8.1 Pengertian Hotspot

Menurut Agusli [29] "*Hotspot* adalah suatu jaringan komputer atau jaringan internet yang memiliki area yang disekitarnya ada jaringan nirkabel atau WLAN (*Wireless Local Area Network*)".

Nuromah, Alexander [30] menyatakan"Hotspot adalah lokasi dimana *user* dapat mengakses melalui *mobile* komputer (seperti laptop) tanpa menggunakan koneksi kabel dengan tujuan suatu jaringan seperti internet. Jaringan nirkabel

menggunakan radio frekuensi untuk melakukan komunikasi antara 19 perangkat komputer dengan *access point* dimana pada dasarnya berupa penerima dua arah yang bekerja pada frekuensi 2.4 GHz dan 5.4 GHz".

Hotspot merupakan lokasi dimana *user* dapat mengakses jaringan internet tanpa menggunakan koneksi kabel dan memiliki area yang disekitarnya ada jaringan nirkabel atau WLAN (*Wireless Local Area Network*).[29],[30]

2.9 PENELITIAN SEJENIS

Pada setiap penelitian tentunya memiliki penelitian terlebih dahulu. Bagian ini dilakukan sebagai pembanding antara peneliti dengan penelitian sejenis yang sebelumnya dan sebagai referensi untuk lebih baik kedepannya. Disini peneliti menggunakan beberapa penelitian sejenis sebagai berikut pada tabel 2.1:

Tabel 2.1 Penelitian Sejenis

NO	**Penulis (Tahun)**	**Masalah**	**Metode**	**Hasil**
1	Agus Tedyyana [31] (2016)	kampus Politeknik Negeri Bengkalis, menentukan alur lalu lintas yang melewati proses pemfilteran	Metode yang digunakan oleh peneliti adalah *Mac Address Filtering*	Dengan sistem mendeteksi *MAC Address* maka hanya PC yang telah di registerkan *MAC Address*

		menggunakan firewall, desain untuk mendapatkan cara yang paling efektif, aman dan efisien dalam mengimplementasikan penggunaan internet.		nya yang akan terkoneksi interne
2	Dipo Era Ginanti, Ade Christian, Taopik Hidayat [32] 2022	PT. Faya Kuntura Agung Konsultindo, filtering MAC Address diterapkan pada PT. Faya Kuntura Agung Konsultindo agar dapat menghalangi pihak diluar karyawan yang masuk ke dalam jaringan	Metode yang digunakan oleh peneliti adalah Metode Mac Address filtering dan hotspot	mengoptimalkan keamanan jaringan komputer khusunya jaringan wireless dari para pihak yang tidak bertanggung jawab. dapat melakukan 2 verifikasi keamanan, yang pertama adalah

		internet. Hal ini dilakukan agar tidak menganggu kinerja para pegawai yang ada		hotspot log in dan yang kedua adalah MAC Address Filtering.
3	Zaenal Mutaqin Subekti, Subandri [33] (2020)	Kendala yang dihadapi pada sebuah jaringan local area network atau jaringan wireless tidak diatur dengan baik dalam pembagian bandwidth, sehingga akses internet pada setiap pengguna tidak merata dan mengakibatkan ada beberapa client yang memiliki kendala pada akses internet	Metode yang digunakan oleh peneliti adalah mac address filtering	setelah menerapkan pembagian bandwidth dengan Per Connection Queue (PCQ), bahwa semua user akses download lebih merata dengan mendapat dibawah 2Mbps, untuk akses upload semua user mendaptkan hampir 2Mbps juga.

		karena bandwidth yang tidak di atur		
4	slamet widodo, Adi Sutrisman, M. Miftakul Amin, Muhammad fernaldo harefa, Muhammad Aulia Farhan, Muhammad Reinaldo [30](2022)	Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya, Sering terjadi serangan yang mengganggu jaringan internet seperti Wireless Hacking. Penelitian ini membahas tentang aplikasi keamanan data user dan sistem keamanan wireless menggunakan Two factor, password dan MAC address filter dijurusan teknik komputer.	Metode yang digunakan oleh peneliti adalah Metode password dan mac address filtering	Dengan adanya aplikasi keamanan data *user* berbasis web ini memudahkan operator jaringan untuk mendaftarkan MAC *Address* mahasiswa dan pengguna *wireless* di jurusan Teknik Komputer.

5	Noviar Armanda Nurdin, Septian Ardiansyah [31] (2018)	PT. Pertamina Drilling Service Indonesia Jakarta yang bergerak pada bidang eksplorasi dan eksploitasi pengeboran minyak dan gas bumi. PT. PDSI Jakarta menerapkan teknologi WLAN Di perusahaannya, karena jaringan ini begitu kompatibel yang memudahkan para karyawannya dalam melakukan aktivitas kerja seperti mengolah data, sharing resources maupun mencari informasi penting lainnya.	Metode yang digunakan oleh peneliti adalah mac address filtering	jaringan yang berada pada PT PDSI Jakarta di lantai 2 menggunakan topologi star yang dikarenakan terhubungnya semua client ke access point yang dapat diartikan bahwa client menggunakan access point untuk menghubungkanny a ke client yang lain

		Sistem keamanan jaringan WLAN harus dilindungi dari Segala macam serangan		
6	MUHAMMAD FAHMI AL ABRAR [32] (2020)	Penyedia ISP tanpa melakukan menyetingan bandwith dan jalur 3 internet game dan browsing akan menyebab kan Lag/Lambat nya koneksi internet, belum lagi ketika seseorang mendownload bandwith akan terambil seluruh nya dan pengguna hotspot yang lain	Metode yang digunakan adalah penerapan fitur hotspot dengan metode keamanan wpa2sk	setelah melakukan pengkonfigurasia n fitur hotspot ini bandwith yang di hasilkan bisa dikelompokan sesuai dengan harga di daftar menu.

		akan mendapatkan bandwith yang sedikit/Lag		
7	Beni Andesta ,Ahmad Luthfi ,Suryayusra[33] (2014)	Dalam operasi bisnis yang telah terintegrasi dengan komputer, saat ini PT. Semen Baturaja telah memanfaatkan teknologi berbasis Wireless LAN sebagai media pendukung operasi bisnis dan sebagai penghubung karyawan maupun tamu yang menggunakan perangkat mobile (Laptop, tablet, smartphone, dll) ke jaringan lokal (Intranet) maupun	Metode yang digunakan adalah mac address filtering dan penerapan fitur hotspot.	merancang keamanan dan manajemen jaringan wireless dengan multiple SSID, STAFFONLY dan HOTSPOTPTSB, sebuah peralatan WLAN dapat mendeteksi kedua buah SSID. Kedua SSID tersebutpun dapat diakses sesuai dengan username dan password yang telah dibuat pada usermanager mikrotik. Pengguna jaringan WLAN

		publik (Internet). Namun jaringan WLAN yang sedang berjalan saat ini belum termanajemen dengan baik.		baik dari SSID STAFFONLY maupun SSID HOTSPOTPTSB, juga belum termanajemen dengan baik. mendapat IP Address secara otomatis dari sebuah DHCP server.

Berdasarkan table 2.1 dapat disimpulkan bahwa penggunaan Metode *MAC Address filtering* memiliki kekurangan yaitu masih terdapat cela untuk dibobol yaitu dengan cara membobol alamat *MAC address* yang terdaftar di jaringan *wireless*, maka dari itu menurut penulis penggunaan *MAC address filtering* harus digabungkan dengan penerapan fitur *hotspot* yang ada di *router* mikrotik, penggunaan *MAC address* sebagai *filter* pertama untuk mengautentikasikan alamat perangkat, setelah authentikasi berhasil maka akan diminta untuk memasukan *username* dan *password* di fitur *login page hotspot*, jika alamat *MAC* perangkat terdaftar akan terkoneksi ke jaringan, jika alamat *MAC* perangkat tidak terdaftar maka perangkat tidak dapat terkoneksi kejaringan yang ada. Perangkat yang di

daftarkan akan memiliki *username* dan *password* berbeda agar dapat mempermudah melakukan manajemen jaringan yang ada.