BAB I
PENDAHULUAN

1.1 Latar Belakang

Undang-undang Republik Indonesia Nomor. 11 tahun 2008 tentang informasi dan transaksi elektronik sudah diatur dalam Bab VII perbuatan yang dilarang, pasal 30 ayat (3), dinyatakan bahwa "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".

Penggunaan internet (*Interconnection Networking*) dengan jasa wifi (*wireless fidelity*) berkembang sangat cepat sejalan dengan kebutuhan sistem informasi sekarang. Banyak yang sudah memanfaatkan wifi pada jaringan masing-masing pengguna. Tidak sedikit yang belum memperhatikan keamanan dalam komunikasi pertukaran data pada jaringan wifi tersebut. Teknologi wifi tidak hanya digunakan pada kantor, perusahaan, rumah. Tetapi juga cocok untuk digunakan pada lingkungan pendidikan yaitu sekolah untuk memudahkan guru maupun siswa dalam proses belajar mengajar dan untuk mendapatkan informasi melalui internet. Perkembangan teknologi wifi saat ini sangat pesat sejalan dengan kebutuhan sistem informasi yang mobile. Teknologi wifi banyak diaplikasikan untuk hotspot komersil, ISP (*Internet Service Provider*), kampus-kampus, perkantoran, termasuk sekolah namun hanya sebagian pengelola jaringan yang memperhatikan keamanan komunikasi data pada jaringan wifi tersebut.

Perkembangan teknologi jaringan komputer saat ini begitu cepat. Setiap hari kita dihadapkan dengan kebutuhan akan berbagai macam informasi, baik secara tertulis maupun visual. Salah satu media yang menjadi sumber informasi ialah internet yang dapat melakukan berbagai macam aktivitas bagi kita seperti *browsing*, *chatting*, *surfing*, *blogging* dan lain sebagainya. Internet yang merupakan salah satu yang memanfaatkan teknologi jaringan komputer semakin familiar dengan para user dari berbagai macam kalangan diseluruh dunia.

Jaringan wifi memiliki banyak kelemahan dibandingkan dengan jaringan kabel. Jaringan wifi juga rentan terhadap masalah keamanan jaringannya. Karena

dalam pengamanan, penulis tidak dapat melihat gelombang radio yang digunakan dalam pertukaran data.Tetapi jaringan wifi sangat membantu dalam proses penggunaannya dilihat dari sistem yang efisien efektif karena mudah dibawa dan lebih praktif.

Jaringan wifi menawarkan berbagai kemudahan dalam penggunaannya, akan tetapi masih ada kendala yang ditemui dalam penggunaan jaringan tersebut. Kekurangan jaringan wifi dibagi menjadi dua jenis yaitu kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi yaitu karena sekarang ini untuk membangun sebuah jaringan *wireless fidelity (wifi)* mudah. Saat ini sudah banyak orang yang membuat dan menyediakan produk atau aplikasi peretas wifi. Biasanya seringkali wifi yang dipasang masih menggunakan setting default bawaan penyedia layanan atau pembuat seperti *IP Address (internet protocol)*, SSID (*service set IDentifier*), tanpa enkripsi untuk login atau masuk ke jaringan wifi tersebut.

SMP Negeri 3 Palopo adalah Sekolah Negeri dibawah naungan Menteri Pendidikan Nasional berdiri pada tahun 1982 sampai sekarang. Pada awal beroperasinya sekolah ini jumlah kelas 1,2, dan 3.

Sekolah ini terletak di jalan Andi Kambo Kecamatan Wara Timur Kota Palopo. Sekolah ini adalah salah satu sekolah yang bergerak dalam bidang pendidikan di Palopo dan telah menerapkan teknologi jaringan *wifi*. SMP Negeri 3 Palopo memiliki laboratorium komputer yang berdiri sejak tahun 2000 dan memiliki akses internet yang bersumber dari ruang laboratorium 1 yang dihubungkan ke masing-masing ruangan seperti : laboratorium 2, dan laboratorium 3.

Menurut Jamilah selaku kepala laboratorium komputer pada SMP Negeri 3 Palopo, sistem jaringan masih menggunakan sistem proteksi satu *password* untuk semua pengguna di ruangan yang terdapat jaringan *wifi* untuk mengakses jaringan internet, pengaksesan jaringan dengan bebas membuat koneksi internet yg terhubung menjadi lambat akibat *overload*. Dimana jaringan seperti ini dapat diretas oleh orang yang tidak bertanggung jawab, dan belum memiliki keamanan jaringan yang optimal. Maka diperlukan suatu alat yang dapat mengatur

dan menganalisis sistem keamanan jaringan *wifi* yang ada.

Untuk itu penulis perlu menganalisis lebih lanjut pada jaringan di lokasi penelitian, tepatnya SMP Negeri 3 Palopo untuk membangun keamanan jaringan dengan memanfaatkan sistem konfigurasi yang ada di perangkat *Mikrotik* agar jaringan *wifi* tersebut tidak mudah diretas dan dapat terkontrol.

Berdasarkan pemaparan diatas, maka penulis mengangkat judul penelitian yaitu "Analisis dan Pembuatan Keamanan Jaringan *Wireless Fidelity* Berbasis *Mikrotik* di SMP Negeri 3 Palopo".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, dirumuskan masalah pokok dalam penelitian adalah "Bagaimana keamanan jaringan wifi dan pembuatan konfigurasi keamanan paket *Sniffing* berbasis *Mikrotik* di SMP Negeri 3 Palopo ?"

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu untuk mengetahui keamanan jaringan wifi dan pembuatan konfigurasi keamanan paket *Sniffing* berbasis *Mikrotik* di SMP Negeri 3 Palopo.

1.4 Manfaat Penelitian

1. Penulis

Penulis dapat mengaplikasikan ilmu pengetahuan yang dimiliki dan didapatkan dibangku perkuliahan.

2. Instansi

Memberikan pengetahuan tentang sistem yang lebih optimal untuk keamanan jaringan wifi yang diterapkan di lokasi penelitian menggunakan Mikrotik.

3. Akademik

Memberikan pengetahuan dan informasi pada mahasiswa di lingkungan kampus, serta menambah wawasan dan pemahaman tentang jaringan wifi dan pembuatan keamanan jaringan berbasis *Mikrotik*.

1.5 Batasan Penelitian

Batasan penelitian merupakan ruang lingkup untuk membatasi permasalahan yang diteliti sehingga pembahasan tidak meluas dan penelitian dapat terarah dengan baik. Batasan dalam penelitian ini yaitu:

1. Penelitian ini hanya difokuskan pada laboratorium SMP Negeri 3 Palopo.
2. Penelitian ini hanya berfokus pada analisis dan konfigurasi keamanan dari serangan paket *Sniffing* dari jaringan *wifi* tanpa mengurangi sistem jaringan yang sudah ada.
3. Proses analisis keamanan untuk melihat port-port yang terbuka menggunakan aplikasi Nmap (*network mapper*).
4. Proses konfigurasi keamanan jaringan wifi menggunakan perangkat router Mikrotik RB750.
5. Melakukan konfigurasi *Mikrotik* dengan menggunakan aplikasi *winbox*.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian teori

Kajian teori berisikan topik-topik yang akan dibahas dalam penelitian ini. Kajian teori mempunyai peranan penting dalam hal melakukan penelitian kualitatif. Dengan kajian teori, penelitian dapat menjustifikasikan adanya masalah penelitian dan mengidentifikasi arah penelitian. Justifikasi masalah penelitian permasalahan penelitian untuk diteliti. Mengidentifikasi arah penelitian berarti penelitian mengkaji kepustakaan dan mengidentifikasi *variabel-variabel* yang layak dan berhubungan serta memiliki kecenderungan potensial yang perlu diuji.

1. Analisis

Menurut Fatoni & Solikin (Fatoni & Solikin, 2019) analisis kinerja pada jaringan komputer membahas tentang sifat dasar dan karakteristik aliran data, yaitu efisiensi daya kerja, penundaan dan parameter lain yang diukur untuk dapat mengetahui bagaimana suatu pesan diproses pada jaringan dan dikirim secara lengkap sesuai fungsinya.

Menurut Jasmin, dkk (Jasmin et al., 2021) mengatakan bahwa analisis adalah kegiatan objektif yang menghasilkan informasi sesuai dengan kebutuhan yang diperoleh dalam penelitian selain itu analisis adalah suatu kerangka acuan yang mengacu pada beberapa tes sistematik untuk menelaah bagian-bagian hubungan antar bagian-bagian tersebut. Menurut Syahidin dan Adnan (Syahidin & Adnan, 2022) Analisis didefinisikan sebagai memecah suatu objek menjadi berbagai bagiannya dan memeriksa bagian-bagian itu sendiri dan hubungan antara bagian-bagian itu untuk memahami dan memahami makna keseluruhan dengan benar. Sehingga analisis adalah suatu kegiatan yang mencakup beberapa kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsirkan maknanya dengan kata lain analisis adalah sekumpulan kegiatan fungsi dan proses yang berhubungan satu sama lain untuk memecahkan masalah atau memecahkan komponen-komponen secara lebih rinci dan

menggabungkannya lagi dan menarik kesimpulan.

2. Keamanan Jaringan

Menurut Wajong (Wajong, n.d.) keamanan jaringan didefinisikan sebagai perlindungan dari sumber daya terhadap upaya perubahan dan gangguan oleh seseorang yang tidak diizinkan. Keamanan jaringan adalah bagaimana suatu jaringan dapat mengamankan jaringannya sendiri. Untuk mengatasi keamanan ini, diperlukan penerapan kebijakan teknis yang digunakan untuk mengatur pengguna, mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan Kemudian Menurut Mutaqin (Mutaqin, 2019) keamanan jaringan adalah proses untuk mencegah dan memantau penggunaan jaringan yang tidak sah dari jaringan komputer. Tujuannya untuk mengantisipasi resiko jaringan komputer yang berupa ancaman fisik dan logis, baik langsung maupun tidak langsung.

Lalu menurut Akbar, dkk. (Akbar et al., 2021) Keamanan jaringan adalah proses mencegah dan mengidentifikasi penggunaan jaringan komputer yang tidak sah. Dari beberapa pengertian mengenai keamanan jaringan maka dapat disimpulkan bahwa Keamanan jaringan komputer adalah suatu proses atau upaya pencegahan penggunaaan jaringan dari seseorang yang bukan haknya sehingga bertujuan untuk mengantisipasi risiko terhadap jaringan komputer berupa ancaman fisik dan logis yang secara langsung atau tidak langsung mempengaruhi operasi sehari-hari pada jaringan komputer. juga melindungi sistem komputer dari berbagai ancaman.

3. Jaringan Komputer

Menurut Hadi (Hadi, 2019), jaringan komputer dapat diartikan sebagai kumpulan dari sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri lebih dari satu komputer yang saling berhubungan. Menurut Ariawal & Purbo (Ariawal & Purbo, 2019) jaringan komputer adalah sekumpulan komputer yang terhubung dan membentuk jaringan yang dapat saling terkoneksi satu sama lain. Menurut Mastiara dan Afriyudi (Mastiara & Afriyudi, 2020) bahwa jaringan komputer adalah jaringan yang menghubungkan beberapa komputer (lebih dari satu) yang memungkinkan terjadinya pertukaran data dan informasi.

Adapun menurut Irawati, dkk. (Irawati et al., 2022) Jaringan komputer adalah sekumpulan perangkat jaringan yang terhubung melalui media transmisi. Beberapa perangkat jaringan yang umum digunakan adalah *repeater*, *hub*, *NIC*, *bridge*, *switch*, *router*, *access point*, dan sebagainya. Sehingga Penulis menyimpulkan jaringan komputer adalah 2 perangkat komputer atau lebih yang dihubungkan dengan alat komunikasi dengan tujuan untuk terhubung satu sama lain agar dapat berbagi informasi dan sumber daya.

4. Manfaat Jaringan Komputer

a. Jaringan untuk perusahaan/organisasi

Menurut Abdullah (Abdullah, 2019) dalam membangun jaringan komputer di suatu perusahaan atau organisasi, terdapat beberapa keuntungan yang dapat diperoleh dari segi *resource sharing*, *reliabilitas* tinggi, lebih hemat, skalabilitas, dan media komunikasi.

1) *Resource sharing* bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan tanpa terpengaruh oleh lokasi *resource* dan pemakai. Jadi *resource sharing* adalah suatu usaha untuk menghilangkan kendala jarak.
2) Dengan menggunakan jaringan komputer akan memberikan reliabilitas tinggi yaitu adanya sumber-sumber alternatif pengganti jika terjadi masalah pada salah satu perangkat dalam jaringan, artinya karena perangkat yang digunakan lebih dari satu jika salah satu perangkat mengalami masalah, maka perangkat yang lain dapat menggantikannya.
3) Komputer yang kecil memiliki rasio harga/kinerja yang lebih baik dibanding dengan komputer besar. Komputer mainframe memiliki kecepatan kurang lebih sepuluh kali lipat kecepatan komputer pribadi, akan tetapi harga mainframe seribu kalinya lebih mahal.
4) Skalabilitas yaitu kemampuan untuk meningkatkan kinerja sistem secara berangsur-angsur sesuai dengan beban pekerjaan dengan hanya menambahkan sejumlah prosesor.
5) Sebuah jaringan komputer mampu bertindak sebagai media komunikasi yang baik bagi para pegawai yang terpisah jauh. Dengan menggunakan jaringan, dua orang atau lebih yang tinggal berjauhan akan lebih mudah

bekerja sama dalam menyusun laporan.

b. Jaringan untuk umum

Menurut Abdullah (Abdullah, 2019) jaringan komputer akan memberikan layanan yang berbeda kepada individu di rumah-rumah dibandingkan dengan layanan yang diberikan kepada perusahaan. Terdapat 3 hal pokok yang menjadi daya tarik jaringan komputer pada perorangan yaitu:

1) Access ke informasi yang berada di tempat yang jauh

Ada bermacam-macam bentuk access ke informasi jarak jauh yang dapat dilakukan, terutama setelah berkembangnya teknologi internet, berita-berita di koran sekarang dapat di *download* ke komputer kita melalui internet, dan tidak hanya itu sekarang kita dapat melakukan pemesanan suatu produk melalui internet, bisnis yang dikenal dengan istilah *electronic commerce* (*e-commerce*), inisekarang sedang berkembang dengan pesat.

2) Komunikasi orang ke orang

Dengan menggunakan internet kita juga dapat melakukan komunikasi orang ke orang, fasilitas *electronic mail* (*e-mail*) telah dipakai secara meluas oleh jutaan orang. Komunikasi menggunakan e-mail ini masih mengandung delay atau waktu tunda.

3) *Video conference* atau pertemuan maya

Video conference atau pertemuan maya merupakan teknologi yang memungkinkan terjadinya komunikasi jarak jauh tanpa *delay*. Pertemuan maya ini dapat pula digunakan untuk keperluan sekolah jarak jauh, memperoleh hasil pemeriksaan medis seorang dokter yang berada di tempat yang jauh, dan sejumlah aplikasi lainnya.

4) Hiburan interaktif

Video on demand merupakan daya tarik ketiga dari jaringan komputer bagi orang per orang dimana kita dapat memilih film atau acara televisi dari negara mana saja dan kemudian ditampilkan di layar monitor kita

5. Jenis-Jenis Jaringan Komputer

a. Berdasarkan Jangkauan

1). Local Area Network (*LAN*)

LAN adalah singkatan dari *Local Area Network*. *LAN* terdiri dari beberapa

komputer yang terhubung dalam suatu jaringan. Pada jaringan ini, setiap komputer dapat mengakses data dari komputer lain. Selain itu, komputer yangterhubung dalam *LAN* juga dapat menjalankan *Hardware* seperti *printer* dan komputer lain, chatting dengan pemilik komputer lain, atau main *game* bersama (Anggraeni, Elisabet Yunaeti, & Irviani, 2018). Kemudian menurut Marpaung dkk (Marpaung et al., 2019) *LAN* adalah jaringan komputer yang mencakup wilayah kecil, seperti jaringan kampus, gedung, kantor, dalam rumah dan sekolah. Sebuah *LAN* adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran disebuah gedung, atau sebuah sekolah dan biasanya tidak jauh dari sekitar 1 km persegi.

Lalu menurut Abdullah, Tamam Asrori, (Abdullah, 2019) *LAN* adalah jaringan komputer dengan jangkauan area yang terbatas dan hubungan fisik antar komputer saling berdekatan. Misalnya jaringan komputer di sebuah kantor, labolatorium, kampus. *LAN* sering kali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk pemakaian bersama sumber daya dan saling bertukar informasi. Dari beberapa pendapat diatas dapat disimpulkan bahwa *Local Area Network* (*LAN*) adalah jaringan yang jangkauannya terbatas atau hanya wilayah kecil saja.



Gambar 1. *Local Area Network (LAN)*
Sumber: Daulay, 2022

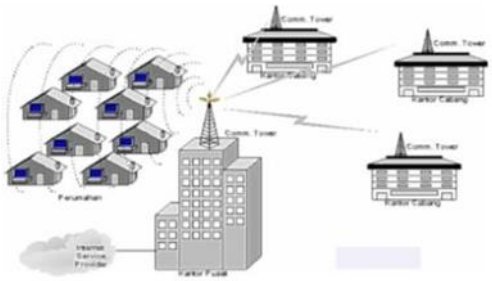
2). Metropolitan Area Network (MAN)

MAN atau *metropolitan Area Network* adalah jaringan yang lebih luas dari pada *LAN*. Beberpa *LAN* yang menjadi satu jaringan juga dapat disebut *MAN*. *MAN* biasanya terdapat dalam satu kampus atau dalam satu wilayah yang agak

luas (dapat juga satu kota). *MAN* biasanya tidak dimiliki oleh satu organisasi saja.Sama seperti *LAN*, *MAN* juga memiliki *wireless MAN* dengan kekurangan dan kelebihan yang relatif sama (Elisabet Yunaeti Anggraeni & Irviani, 2018).

Menurut Abdullah, (Abdullah, 2019) *MAN* adalah penggabungan dari beberapa jaringan *LAN* kedalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan pada bank ataupun kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

Menurut Rismawati, dkk (Rismawati & Mulya, 2020) *Man* adalah suatu jaringan komputer dalamsuatu kota dengan *transfer data* berkecepatan tinggi yang menghubungkan suatu lokasi seperti sekolah, kampus, perkantoran dan pemerintahan. Dari beberapa definisi diatas dapat disimpulkan *Metropolitan Area Network* (*MAN*) adalah suatu jaringan komputer dalam suatu daerah kota dengan *transfer* dan kecepatan tinggi mampu menghubungkan banyak lokasi.



Gambar 2. *Metropolitan Area Network (MAN)*
Sumber: Daulay, 2022

b.) *Wide Area Network* (WAN)

Menurut Pratama, dkk (Pratama et al., 2020) *Wan* (*Wide Area Network*) adalah kumpulan dari *LAN* atau *workgroup* yang dihubungkan dengan menggunakan alat komunikasi *modem* dan jaringan internet ke kantor pusat dan kantor cabang, ataupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data anatar kantor dapat dilakukan dengan cepat, serta dengan biaya yang relatif murah. System jaringan ini dapat menggunakan jaringan internet yang sudah ada untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan *PC Stand Alone Notebook* yang berada di kota lain ataupun negara.

Menurut Abdullah, (Abdullah, 2019) *WAN* adalah jaringan komputer dengan area geografi yang paling luas antar negara, antar benua bahkan keluar angkasa. *WAN* terdiri dari mesin-mesin yang bertujuan untuk menjalankan program-program pemakai.



Gambar 3. *Wide Area Network (WAN)*
Sumber: Daulay, 2022

c.) Wireless

Menurut Rusdan dan Sabar (Rusdan & Sabar, 2020) *Wireless* merupakan Jaringan nirkabel adalah jaringan yang tidak menggunakan media kabel tetapi menggunakan radiasi gelombang radio untuk berinteraksi atau berkomunikasi antar perangkat yang mendukung koneksi nirkabel. Beroperasi pada 2,4 GHz (802,11 b/g/n/ac) atau 5 GHz (802,11 a/n/ac). *Backbone* jaringan jaringan *Wireless* biasanya berkabel dan memiliki satu atau lebih stasiun pangkalan. Jaringan *Wireless* merupakan teknologi yang saat ini banyak digunakan di berbagai institusi, kantor, kafe, pusat perbelanjaan, bandara, hotel, bahkan sekolah dan universitas. Jaringan nirkabel menawarkan kemudahan dan fleksibilitas yang tinggi, serta nyaman digunakan. Selama berada dalam area jangkauan jaringan nirkabel, pengguna dapat mengakses Internet kapan saja. Untuk membuat jaringan nirkabel yang terhubung ke Internet dengan cara yang aman dan ramah pengguna, kita dapat membuat sistem otentikasi pengguna *RADIUS (Remote Access Dial In User Service)* berbasis server yang akan digunakan untuk melakukan *Authentication, Authorization* dan *Accounting (AAA).*



Gambar *4. Wireless*
Sumber: Daulay, 2022

6. Perangkat-Perangkat Jaringan Komputer

a. Hub

Menurut Irawati, ddk. (Irawati et al., 2022) *Hub* merupakan peralatan yang memiliki fungsi yang sama denga repeater hanya hub terdiri dari beberapa *port*, sehingga *hub* disebut juga *multiport repeater*. *Repeater* dan *hub* bekerja pada *Physical Layer* sehingga tidak mempunyai pengetahuan mengenai alamat yang dituju. Meskipun *hub* memiliki beberapa *port* tetapi tetap menggunakan metode *broadcast* dalam mengirimkan sinyal, sehingga bila salah *port* sibuk maka *port* yang lain harus menunggu jika ingin mengirimkan sinyal.



Gambar 5. *Hub*
(Sumber: Septanto, 2022)

b. Switch

Menurut Irawati, ddk. (Irawati et al., 2022) *switch* merupakan perangkat yang berfungsi untuk menghubungkan beberapa komputer ataupun perangkat jaringan agar dapat berbagi sumber dayanya. *switch* merupakan sebuah perangkat keras yang memungkinkan terjadinya distribusi packet data antar *computer* dalam jaringan dan mampu untuk mengenalitopologi jaringan dibanyak *layer* sehingga data dapat langsung sampai ketujuan.



Gambar 6. *Switch*
(Sumber: Alfurqon dan Assegaff, 2022)

c. Access Point

Menurut Irawati, ddk. (Irawati et al., 2022) *Access Point* adalah perangkat jaringan komputer bekerja pada lapisan *OSI* kedua, lapisan *Data Link*, dan dapat beroperasi baik sebagai *Bridge* yang menghubungkan jaringan kabel standar ke perangkat nirkabel atau sebagai *router* yang mengirimkan transmisi data dari satu titik akses ke titik akses lainnya.



Gambar 7. *Access Point*
(Sumber: Alfurqon & Assegaff, 2022)

d. Router

Menurut Irawati, ddk. (Irawati et al., 2022) *router* adalah perangkat antara yang dapat digunakan untuk menghubungkan dua jaringan local yang mempunyai protokol yang sama pada lapisan jaringan *OSI* sedangkan protokol pada lapisan fisik dan data link berbeda. *Router* merupakan perangkat pencari jalan yang handal pada situasi interkoneksi yang kompleks, karena memiliki kemampuan menejemen jaringan yang baik sehingga router sangat tepat digunakan pada pembangunan jaringan luas. Jadi dapat disimpulkan bahwa *router* adalah alat yang digunakan untuk pembangunan jaringan yang luas dan memiliki menejemen jaringan yang baik.



Gambar 8. *Router*
(Sumber: Alfuqon & Assegaff, 2022)

7. *Wireless Fidelity (WIFI)*

Menurut Komputer (Komputer, 2019) *Wifi* adalah seperangkat standar yang digunakan untuk jaringan lokal nirkabel (*Wireless Local Area Networks*) yang didasarkan pada spesifikasi *IEEE 802.11*. *Wifi* adalah standar koneksi yang digunakan untuk menghubungkan 1 komputer ke 1 komputer atau ke banyak komputer. Menurut Sutrisno, dkk. (Sutrisno et al., 2014) *wifi* adalah sebuah teknologi terkenal yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel (menggunakan gelombang radio) melalui sebuah jaringan komputer.

Menurut Efendi dan Riadi (Efendi & Riadi, 2019) *Wi-Fi (Wireless Fidelity)* adalah istilah umum untuk peralatan *wireles*s LAN yang juga dikenal dengan WLAN. Biasanya peralatan *Wi-Fi* mengadopsi standar keluarga IEEE 802.11, yang didukung oleh banyak vendo *Wireless Fidelity* (*wifi*) adalah teknologi yang terdiri dari beberapa komputer yang tersambung dalam jaringan tanpa menggunakan kabel penghubung melainkan menggunakan *local area network* (*WLAN*) lalu *wifi* (*Wireless Fidelity*) memiliki pengertian yaitu merupakan koneksi nirkabel yang menggunakan teknologi radio sehingga pengguna dapat mentransfer data dengan cepat dan menghemat biaya. Sehingga Penulis menyimpulkan *wireless fidelity* adalah sekumpulan standar yang digunakan untuk jaringan lokal nirkabel (*Wireless Local Area Network* atau *WLAN*) yang didasari pada spesifikasi *IEEE 802.11* untuk komunikasi jaringan lokal tanpa kabel yang memanfaatkan udara sebagai tempat perantara untuk melakukan pertukaran data.

Menurut Hadi (Hadi, 2019) beberapa keunggulan jaringan *wifi* dibandingkan jaringan menggunakan kabel adalah:

1) Biaya pemeliharaan murah.
2) Peralatan atau infrastruktur jaringan umumnya berdimensi kecil.
3) Untuk membangun sistem jaringan dapat dilakukan dengan cepat.
4) Mudah dan murah untuk direlokasi jika diperlukan.
5) Sistem sangat mendukung portabilitas.

Menurut Hadi (Hadi, 2019) kelemahan jaringan *wifi* adalah:

1) Biaya peralatan jaringan pada saat ini relatif masih mahal.
2) Terjadi delay yang relatif besar untuk saat ini, apalagi jika jumlah user meningkat.
3) Kadang terjadi kesulitan dan gangguan karena masalah propagasi frekuensiradio.
4) Mudah sekali terjadi interferensi oleh sistem lain.
5) Keamanan dan kerahasiaan data relatif kurang terjamin.
6) Kapasitas jaringan terbatas karena keterbatasan spektrum karena pita frekuensi(Bandwidth) tidak dapat diperlebar.

8. Komponen Utama Jaringan *Wifi*

Menurut Amin, Dkk (Amin et al., 2022) ada beberapa komponen utama pada jaringan *wifi* yang harus ada pada suatu sistem *networking*, diantaranya:

Access Point, komponen yang berfungsi menerima dan mengirimkan data dari adapter *wireless*, *access point* mengonversi sinyal frekuensi radio menjadi sinyal digital atau sebaliknya. Komponen tersebut bertindak layaknya

a. sebuah *hub/switch* pada jaringan *ethernet*. Satu *access point* secara teori mampu menampung beberapa sampai ratusan klien. Walaupun demikian, *access point* direkomendasikan dapat menampung maksimal 40-an klien.
b. *Wireless-LAN Device*, komponen yang dipasangkan di *Mobile*/*Dekstop PC*.
c. *Mobile*/*Desktop PC*, Komponen untuk klien, *mobile PC* pada umunya sudah terpasang port *PCMCIA* (*Personal Computer Memory Card International Association*), sedangkan *Dekstop PC* harus ditambahkan *PCI* (*Peripheral Componen Interconnect*) *Card*, serta *USB* (*Universal Serial Bus*) *Adapter*.
d. *Ethernet LAN* dan jaringan kabel yang sudah ada.

9. Topologi Jaringan *Wifi*

Jika dalam jaringan konvensional dikenal berbagai jenis topologi jaringan, seperti *star*, *ring*, dan *bus*, sedangkan pada jaringan *wifi* hanya dikenal 2 jenis

topologi jaringan, yaitu ad hoc dan infrastructure.

a. Topologi *Ad-Hoc*

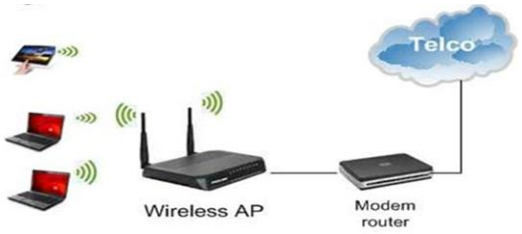
Topologi jaringan *ad hoc* terdiri dari beberapa mobile node yang dapat saling berkomunikasi secara *Peer-to-Peer* tanpa menggunakan infrastruktur seperti *acces point* maupun *base station*. Setiap mobile node memiliki *wireless network interface* dan saling berkomunikasi dengan memanfaatkan media radio atau infra merah. Contoh node pada jaringan *ad hoc* adalah laptop *computer* dan *PDA* (*Personal Digital Assistant)* yang dapat berkomunikasi secara langsung satu dengan yang lainnya. Node-node pada konfigurasi jaringan *ad hoc* dapat bergerak dengan bebas atau diam pada posisinya.



Gambar 9. Toplogi *Ad-Hoc*
Sumber: http://budi-aog.blogspot.com/2013/02/perbedaan-jaringan-ad-hoc-dengan.html

b. Topologi Infrastruktur

Topologi jaringan ini dibangun dengan *fixed infrastruktur* yang terdiri atas *Base Station* (BS) atau *Access Point* (AP). BS atau AP berfungsi memberikan service dan kontrol pada user bergerak yang berada di area cakupannya. Pada topologi ini, setiap AP saling dihubungkan dengan media kabel dan setiap user bergerak dihubungkan ke *Access Point* melalui media *wireless*. *Access point* dapat berkomunikasi dengan semua user bergerak yang berada di area cakupan yang dimilikinya.



Gambar 10. Topologi Infrastruktur
Sumber: http://budi-aog.blogspot.com/2013/02/perbedaan-jaringan-ad-hoc-dengan.html

10. Keamanan Jaringan *Wifi*

Sinyal frekuensi *wifi* dipancarkan secara bebas kesegala arah sehingga akan dapat ditangkap oleh semua komputer lain sebagai pengguna frekuensi *wifi*. Untuk mencegah *user* lain yang tidak berhak masuk ke dalam jaringan, maka mekanisme jaringan perlu dilengkapi dengan sistem pengamanan, seumpama *WEP* (*Wired Equivalent Privacy*). Sehingga hanya user tertentu yang telah mempunyai otorisasi saja yang dapat menggunakan sumber daya jaringan *wifi*.

Menurut Hadi (Hadi, 2019) keamanan jaringan *wifi* secara umum terdiri dari *Non-Secure* (*Open*) dan *Secure* atau *Share Key*.

a. *Non-Secure*/*Open*: setiap komputer yang memiliki *wifi* akan dapat menangkap pancaran sinyal dari sebuah access point *wifi* dan dapat langsung masuk ke dalam jaringan tersebut.

b. *Share Key* (*Secure*): walaupun semua komputer yang mempunyai *wifi* mendapat pancaran sinyal *wifi*, namun untuk masuk ke dalam jaringan diperlukan kunci (*key*) atau *password*, contohnya jaringan nirkabel yang menggunakan *WPE*.

Menurut Hadi (Hadi, 2019) beberapa mekanisme yang juga dapat mengamankan sebuah jaringan nirkabel tipe *wifi* antara lain adalah:

1) *Access point* dengan fasilitas *password* bagi *administrator* jaringannya sehingga tidak sembarangan *user* dengan mudah mengacak-acak jaringan.
2) Selain menggunakan *WEP* disarankan juga menambah peralatan *WPA* (*Wi-FiProtected Access*).
3) Melakukan pembatasan akses ke jaringan dengan mendaftarkan laman fisik(*MAC Address*) dari komputer klien yang berhak mengakses jaringan.

11. Mikrotik

Menurut Riadi (Riadi, n.d.) *Mikrotik* pada standar perangkat keras berbasis *Personal Computer* (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses *rute* atau yang lebih dikenal dengan sebutan routing.

Menurut Prasetyo, dkk. (Prasetyo et al., 2019) *Mikrotik*adalah sistem operasi dan perangkat lunak yang digunakan untuk memfungsikan komputer sebagai *router*. *Mikrotik* saat ini banyak digunakan oleh *ISP*, penyedia *hotspot*, ataupun oleh pemilik warnet.

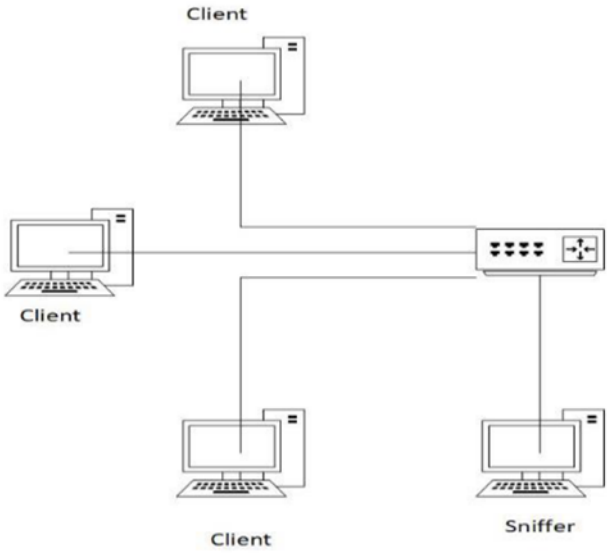
Menurut Husna dan Rosyani (Husna & Rosyani, 2021) *Mikrotik* adalah sebuah perusahaan yang bergerak pada bidang produksi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang berkaitan dengan sistem jaringan komputer yang berkantor pusat di Latvia, berdekatan dengan Rusia. Menurut Amarudin (Amarudin, 2022) *Mikrotik* adalah perangkat jaringan komputer berupa *hardware* dan *software* yang dapat berfungsi sebagai *router*, sebagai *filtering*, *switching* atau alat lainnya. Sehingga Penulis menyimpulkan *Mikrotik* adalah perangkat jaringan komputer yang terdiri dari *hardware* berupa *Router Board* yang didalamnya sudah terinstal sistem operasi *Mikrotik RouterOS* yang sudah dibangun langsung dari perusahaan *Mikrotik*. Dan *Mikrotik* dalam bentuk *software* yang diinstall pada *personalcomputer* melalui *Compact Disc* (*CD*).

Nurhadi, dkk. (Nurhadi et al., 2019) menyatakan bahwa fungsi utama router *Mikrotik*
sebagai berikut:

a. *Routing Device*, fungsi utama *router* yaitu bertugas menghubungkan dari jaringan satu ke jaringan lain, memeriksa dan menentukan jalur terbaik routing.
b. *Internet Gateway*, sebagai penghubung pintu masuk internet atau bisa dibilang gerbang utama, lalu lintas internet dari luar manapun didalam jaringan. Mengfilter akses layanan tertentu sampai membagi *bandwidth* data.
c. *Access Point*, ada yang dilengkapi *wlan interface* yang bisa berfungsi sebagai *access point* sebuah jaringan *wireless*.

12. Paket *Sniffing*

Menurut Wulandari dan Ariyandi (Wulandari, 2022) *Sniffing* ilmu keamanan jaringan *Sniffing* adalah kegiatan menangkap paket yang melewati jaringan. *Sniffing* sendiri sering digunakan untuk menangkap informasi penting dari jaringan, seperti password, teks email, dan file *Sniffing*. *Sniffing* adalah proses mengendus paket pada sistem jaringan komputer, yang memantau dan menangkap semua lalu lintas jaringan yang lewat, terlepas dari siapa paket dikirim. Adapun menurut Dharmesta, dkk bahwa *Packet Sniffing* adalah proses membaca paket data yang dikirim melalui jaringan. Ini dapat dilakukan dengan perangkat lunak atau peralatan khusus. Berikut adalah gambaran cara kerja dari *Sniffing* yaitu :



Gambar 11. Cara Kerja *Sniffing*
Sumber : (Putu Adhika Dharmesta, I Made Agus Dwi Suarjaya, 2020)

Mekanisme kerja dari *sniffer* ditunjukkan pada Gambar 1. Ketika sebuah paket berjalan dari sumber ke tujuan, paket melewati banyak media perantara. Setiap *NIC* di komputer memiliki alamat fisik yang unik dari satu perangkat ke perangkat lainnya. Ketika paket tiba di kartu jaringan, alamat perangkat keras pada bingkai paket akan cocok dengan alamat fisik pada kartu jaringan. Jika alamatnya sama, *NIC* akan menerima paket. Namun, jika berbeda, paket akan dijatuhkan. Tetapi jika kartu jaringan perangkat diubah ke mode *promiscuous*, kartu jaringan dapat menangkap semua paket data yang masuk (Putu Adhika Dharmesta, I Made Agus Dwi Suarjaya, 2020)

2.2 Hasil Penelitian yang Relavan

Bahan penelitian yang relevan ini peneliti gunakan sebagai acuan untuk membantu dalam penyusunan kerangka pikir.

1. Penelitian Syafriadi & Nirsal, (Syafriadi & Nirsal, 2018) dengan judul penelitian "Analisis dan Perancangan Keamanan Jaringan Menggunakan *Network Mapper* Pada Jaringan Komputer Dinas Sosial Tenaga Kerja dan Transmigrasi Kabupaten Luwu". Pada penelitian ini sistem keamanan jaringan yang lama pada Dinas Sosial Tenaga Kerja dan Transmigrasi Kabupaten Luwu sangat rentan terhadap kejahatan, karena masih banyak kekurangan pada sistem yang lama. Penelitian ini bertujuan menganalisis keamanan jaringan yang ada di Kantor Dinas Sosial Tenaga Kerja dan Transmigrasi Kabupaten Luwu menggunakan *Nmap* untuk melihat kelemahan yang ada, kemudian dibuatkan sebuah sistem keamanan yang baru menggunakan *firewall Mikrotik* agar jaringan tidak bisa lagi digunakan secara ilegal dan dapat berjalan optimal.

   Metode penelitian yang digunakan meliputi metode wawancara (terhadap sistem yang sedang berjalan, serta analisis masalah dan kebutuhan) dan metode observasi berupa perancangan topologi jaringan, perancangan sistem, peralatan jaringan yang akan digunakan dan konfigurasi pada setiap peralatan jaringan. Hasil penelitian adalah perancangan sistem keamanan jaringan menggunakan firewall *Mikrotik* telah berjalan sebagaimana mestinya. Perangkat ilegal yang mencoba melakukan scanning terhadap sistem jaringan akan secara otomatis didrop oleh sistem. Celah Port sistem yang terbuka telah tertutup dan tidak lagi dapat dilewati oleh perangkat lain selain perangkat resmi yang telah didaftarkankedalam sistem jaringan.

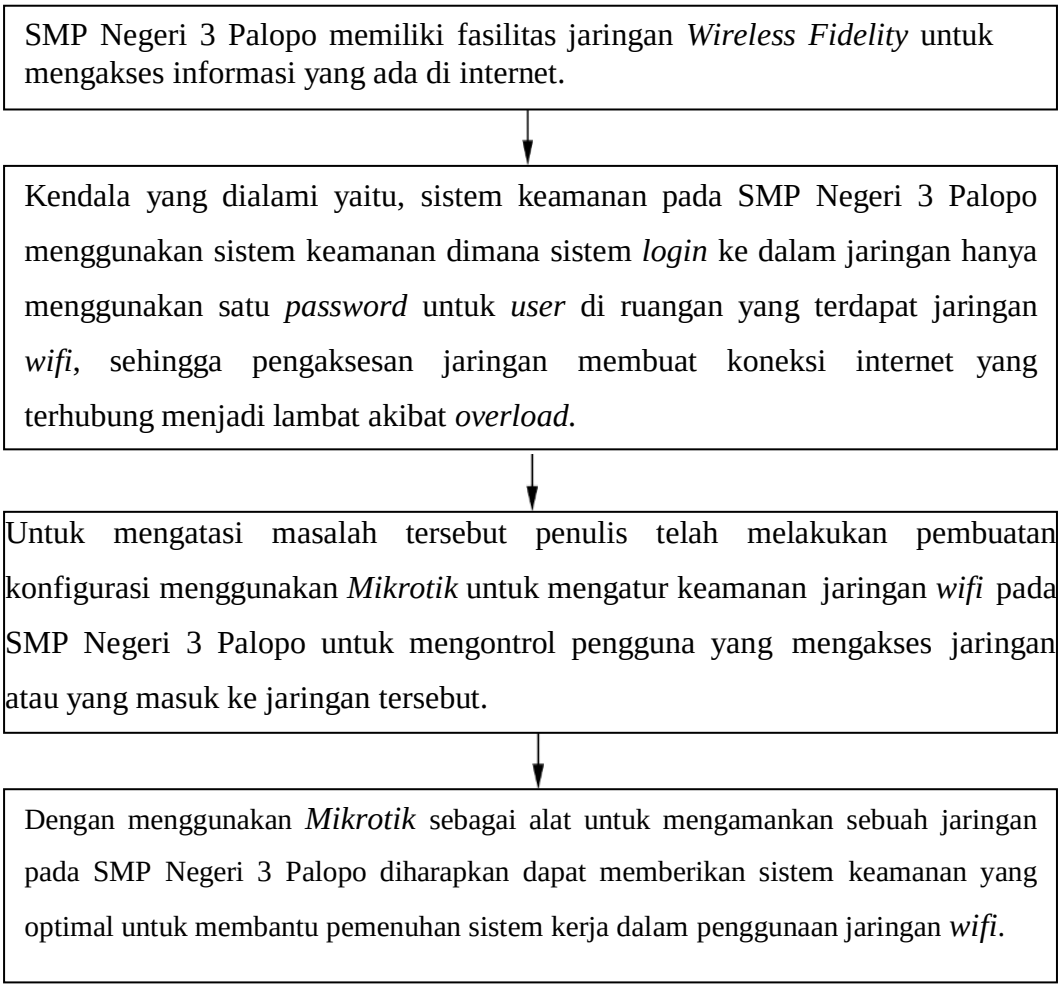
2. Penelitian Asteroid & Hendrian, (Asteroid, K. M., & Hendrian, 2019) dengan judul penelitian "Analisis *Wireless Local Area Network* (*WLAN*) dan Perancangan *MAC Address Filtering* Menggunakan *Mikrotik* (Studi Kasus Pada PT. Graha Prima Swara Jakarta)". Pada penelitian ini PT. Graha Prima Swara menerapkan teknologi *WLAN* pada kantornya. Didalam jaringan komputer tersebut, *access point* digunakan sebagai base station jaringan *WLAN* dengan sistem keamanan yang digunakan adalah *WPA2*-

PSK (*Wi-Fi Protected Access 2-Pre Shared Key*). Terdapat celah keamanan pada *WPA2-PSK* yaitu selama masih berada dalam jangkauan sinyal *wireless* dan mengetahui *passwordnya*, maka orang lain yang tidak berhak dapat mengakses internet. Dengan menggunakan *MAC Address filtering* pada *Mikrotik*, admin dapat membatasi *user* yang berhak terkoneksi dengan cara mendaftarkan *MAC Address client*. Agar jaringan komputer dapat bekerja lebih optimal penulis mengubah letak *switch* yang awalnya terhubung dengan *port access point*, kini terhubung pada *port router*. Sehingga jaringan *WLAN* pada PT. Graha Prima Swara dapat bekerja optimal, aman dan efisien.

3. Penelitian Sundari, (2021) dengan judul penelitian "Analisis Keamanan Jaringan Komputer pada Fasilitas *Wireless Fidelity* (*wifi*) terhadap Serangan Paket *Sniffing* di Sentral Yamaha Palopo". Penelitian ini bertujuan untuk menganalisis keamanan pada Jaringan pada Sentral Yamaha Palopo dan membantu administrator untuk dapat mengetahui adanya kemungkinan celah keamanan pada jaringan kantor, sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada jaringan. Penelitian ini dilaksanakan di Sentral Yamaha Palopo. Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif. Metode pengumpulan data yang terdiri dari metode observasi langsung ke tempat lokasi penelitian, wawancara salah satu staf yang ada di kantor tersebut, instrumen penelitian dan studi pustaka. Dalam penelitian ini dilakukan dua tahap, yang pertama mengidentifikasi keberadaan dan keamanan wifi yang dipakai menggunakan software *inSSIDer*. Tahap kedua melakukan serangan *packet sniffing* menggunakan software *ettercap* sebagai langkah pengujian keamanan di Sentral Yamaha Palopo.

2.3 Kerangka Pikir

Sebuah kerangka pikir merupakan susunan dari pokok permasalahan sehingga menghasilkan suatu solusi. Kerangka pikir penelitian ini dibuat dalam bentuk skema seperti gambar berikut:



Gambar 12. Kerangka Pikir