BAB I

PENDAHULUAN

A Latar Belakang

Jaringan komputer tanpa kabel yang dikenal sebagai Wireless LAN (WLAN) atau juga disebut dengan istilah Wi-Fi (Wireless Fidelity), merupakan sebuah jaringan lokal yang menggunakan teknologi gelombang radio untuk pertukaran data. Dalam era globalisasi sekarang penggunaan internet semakin berkembang pesat, dapat kita lihat bahwa hampir di seluruh belahan bumi ini sudah terkoneksi internet. Keuntungan diantaranya yaitu user bisa melakukan koneksi internet kapan saja dan dimana saja asal masih berada dalam ruang lingkup hotspot, selain itu dalam segi biaya pembangunan, wireless jauh lebih murah bila dibandingkan dengan kabel. Walaupun demikian, wireless memiliki lebih banyak kelemahan dibandingkan dengan kabel, khususnya dari segi keamanan. Keamanan jaringan WLAN sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan WLAN harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem keamanan jaringan menjadi faktor yang sangat penting untuk dipertimbangkan bagi seorang administrator jaringan, dan berbagai upaya dilakukan

dalam mengamankan jaringan dari ancaman dan serangan baik oleh hacker maupun penyebaran virus. Atas dasar permasalahan tersebut, penulis ingin menganalisa keamanan jaringan WLAN pada PT.Sporte Indonesia Sejahtera. Sehingga jaringan WLAN PT.Sporte Indonesia Sejahtera dapat dimanfaatkan secara optimal dan juga memiliki keamanan jaringan yang aman. Karena sebelumnya perusahaan pernah mengalami penurunan kecepatan internet yang mengganggu produktivitas kerja dan serangan dari pihak yang tidak bertanggung jawab dengan merusak data serta keuangan perusahaan sehingga mengalami kerugian yang cukup tinggi.

Access Control List (ACL) merupakan salah satu alternatif upaya untuk mengamankan jaringan computer. Untuk dapat mengakses jaringan wireless maka setiap perangkat komputer harus mendaftarkan alamat Media Access Control (MAC)-nya kepada administrator penelitian ini dilakukan untuk mengkaji langkah-langkah yang perlu dilakukan untuk memberikan hak akses ke jaringan berdasarkan MAC address komputer agar dapat membangun komunikasi data ke komputer lain.

B Rumusan Masalah

Dalam penelitian ini dapat dirumuskan permasalahan, yaitu:

1. Kejanggalan penggunaan jaringan computer sehingga kecepatan internet melemah dan meyebabkan produktivitas kerja menurun
2. Lemahnya sitem keamanan jaringan nirkabel pada pada PT.Sporte Indonesia Sejahtera terjadi kerugian kantor karena peretasan oleh pihak tidak bertanggung jawab

C Tujuan dan Manfaat

C.1 Tujuan Penelitian

Tujuan dari penelitian ini penulis dapat merancang keamanan jaringan nirkabel pada PT.Sporte Indonesia Sejahtera.

1. Menggunakan akses control list untuk mengetahui user yang menggunakan jaringan di PT Sporte Indonesia Sejahtera
2. Merancang keamanan jaringan nirkabel dengan menyaring alamat device dengan cara mendaftarkan pada router sehingga pihak yang tidak didaftarkan maka tidak bisa masuk ke dalam jaringan PT Sporte Indonesia Sejahtera

C.2 Manfaat Penelitian

Diharapkan dengan adanya penelitian ini dapat diambil beberapa manfaat yang mencakup beberapa hal berikut :

1. Manfaat bagi dunia akademik

   Dapat menjadi referensi dan dapat dikembangkan dalam penelitian yang berkaitan dengan keamanan jaringan nirkabel.
2. Manfaat bagi pengguna
   a. Mencegah adanya penggunaan nirkabel selain lingkup kantor.
   b. Meminimalisir terjadinya kejahatan internet pada perusahaan.
3. Manfaat bagi penulis

   Memenuhi syarat kelulusan untuk memperoleh gelar sarjana serta menambah pengetahuan dan pengalama dalam penerapan keamanan jaringan.

D Batasan Masalah

Di dalam melakukan suatu penelitian di perlukan adanya pembatasan suatu masalah supaya penelitian tersebut lebih terarah dan memudahkan dalam pembahasan sehingga tujuan penelitian akan tercapai. Beberapa Batasan masalah dalam penelitian ini adalah sebagai berikut,

1. Keamanan yang diuji hanya pada keamanan access point yang meliputi mac filtering.
2. Alat yang digunakan adalah Tp link TD- W8951ND.

E Metodologi

Dalam pembuatan penulisan laporan ini, penulisa mendapat data dan informasi melalui internet, jurnal serta buku – buku yang dapat dijadikan referensi untuk membantu dalam menyelesaikan penulisan Skripsi ini.

Sedangkan untuk mendapat data dari alat yang telah dikerjakan, penulis menggunakan metode pengujian dan pengamatan, dengan cara melakukan pengetesan dengan program dan lain lain. Hasil akhir dari pengujian, penulis melakukan perbandingan teori dan analisa praktek.

F Sistematika Penulisan

Dalam penulisan laporan ini terdiri dari 5 bab, dimana masing-masing bab terdiri dari

BAB I : PENDAHULUAN

Pada BAB I ini akan dibahas tentang Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan, Manfaat, dan Metode Penelitian Penulisan.

BAB II : TEORI PENUNJANG

Bab ini berisi tentang teori-teori yang berhubungan dengan teori yang ada dalam laporan. Masalah dan hambatan yang mungkin di hadapi dan pemecahan masalahnya dan hasil dari analisa.

BAB III : PERANCANGAN

Bab ini berisi tentang perencanaan secara detail bagian – bagian system yang mulai dari proses desain, simulasi sampai dengan implementasi lengkap dengan penjelasannya, parameter – parameter system dan hal – hal yang berhubungan dengan prosen perencanaan.

BAB IV : PENGUJIAN DAN ANALISA

Bab ini berisi penjelasan pengujian yang didapat dari hasil simulasi, spesifikasi alat, nilai parameter yang sudah diukur dan disimulasikan, dan lain sebagainya.

BAB V : KESIMPULAN DAN SARAN

Pada BAB V ini penulis menyimpulkan dan memberi saran setelah mengkaji hasil dari perhitungan sampel yang telah didapat.

BAB II

LANDASAN TEORI

A Literatur Penelitian

Dalam penyusunan tugas akhir ini penulis sedikit banyak terinspirasi dan merefrensi dari penelitian – penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada skripsi ini. Adapun penelitian yang berhubungan dengan skripsi ini antara lain :

1. Penelitian yang dilakukan oleh (Nina Hendrarini, 2011) yang berjudul " Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet " riset ini telah membuktikan proses filtering dan selektivitas permintaan panggilan/sambungan dalam keamanan akses jaringan ke internet pada infrastruktur sebuah LAN (Local Area Network) dengan cara terpusat, dengan menyediakan metode filtering berbasiskan Access Control List, serta model jaringan intranet berbasis Access Control List yang telah dapat menyaring identifikasi perangkat berdasar IP-Address dan MAC-Address serta seletivitas permintaan layanan data berdasarkan URL yang dikunjungi.

2. Penelitian yang dilakukan oleh (Kurnia Mega Asteroid, 2016) yang berjudul " Analisi Wireless Local Area Network (WLAN) Dan Perancangan Mac Address Filtering Menggunakan Mikrotik " keunggulannya dalam hal portabilitas dan fleksibilitas untuk mendukung kinerja perusahaan. Di dalam jaringan komputer tersebut, ISP yang digunakan adalah Maxindo dengan bandwidth 7Mbps yang terhubung pada routerboard mikrotik 750 sebagai pusat kontrol jaringan.

3. Penelitian yang dilakukan oleh (Tedyyana, 2016) yang berjudul " Rancang Bangun Jaringan Wirelless Di Politeknik Negeri Bengkalis Menggunakan MAC Filtering " Penelitian ini dilakukan menggunakan beberapa tahapan antara lain : analisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan firewall, desain untuk mendapatkan cara yang paling efektif, aman dan efisien dalam mengimplementasikan penggunaan internet di kampus Politeknik Negeri Bengkalis. IP Address dan MAC address pasti dimiliki oleh setiap Network adapter, Ketika wireless klien terhubung dengan router, maka MAC address akan terdaftar secara otomatis, pada router inilah sang admin bisa memblok MAC address yang bukan merupakan anggota di kampus Politeknik Negeri Bengkalis.

B Jenis Jaringan Komputer

B.1 Local Aren Network

(Local Area Network) adalah jaringan komputer yang menghubungkan komputer dalam area terbatas seperti rumah, sekolah, laboratorium, universitas atau kantor dan memiliki peralatan jaringan sendiri dan interkoneksi yang dikelola secara lokal. LAN sangat bermanfaat untuk membagi sumber daya, seperti penyimpanan data dan printer. Jaringan komputer jenis ini dapat dibangun dengan hardware yang relatif murah, seperti wireless access point, hub, adapter jaringan dan kabel Ethernet. Jaringan komputer jenis LAN yang terkecil dapat terdiri dari hanya dua komputer, sedangkan LAN yang lebih besar dapat terdiri dari ribuan komputer. LAN biasanya sebagian besar mengandalkan koneksi kabel untuk meningkatkan kecepatan dan keamanan, namun koneksi wireless juga dapat menjadi bagian dari LAN. kecepatan tinggi dan biaya yang relatif rendah merupakan karakteristik jaringan jenis LAN.

LAN biasanya digunakan pada satu tempat di mana orang-orang harus berbagi sumber daya diantara mereka sendiri tetapi tidak dengan orang luar. Misalnya sebuah gedung perkantoran dimana semua karyawan harus dapat mengakses file pada server pusat atau dapat mencetak dokumen melalui satu atau lebih printer pusat. Hal ini akan memudahkan karyawan dalam mengerjakan tugas-tugas mereka, tetapi Karyawan/Perusahaan tentunya tidak ingin jika orang luar yang hanya kebetulan lewat juga dapat mengakses file pada server pusat atau mengirim dokumen ke printer melalui laptop atau ponsel mereka. Jika LAN, sepenuhnya

menggunakan teknologi wireless, maka jenis jaringan ini disebut sebagai WLAN (Wireless Local Area Network).

B.2 Metropolitan Area Network

MAN adalah jaringan komputer yang menghubungkan para pengguna dengan sumber daya komputer pada sebuah area geografis atau area yang lebih besar dari yang tercakup oleh LAN yang luas, tetapi lebih kecil dari area yang tercakup oleh WAN (wide area network).Tergantung pada konfigurasi-nya, jaringan jenis ini dapat mencakup area mulai dari beberapa mil hingga puluhan mil. MAN sering digunakan untuk menghubungkan beberapa LAN untuk membentuk jaringan yang lebih luas. Saat jaringan jenis ini dirancang khusus untuk sebuah Universitas, makan terkadang disebut sebagai CAN (Campus Area Network).

B.3 Wide Area Network

WAN (Wide Area Network) adalah jaringan komputer atau jaringan telekomunikasi yang membentang di atas jarak geografis yang sangat luas, seperti seluruh Negara atau seluruh Dunia. Jaringan komputer jenis WAN biasanya terdiri dari beberapa jenis jaringan yang lebih kecil, seperti LAN atau MAN. Bisnis, Pendidikan dan Lembaga Pendidikan menggunakan jaringan jenis WAN untuk relay data antara para staf, mahasiswa, klien, pembeli dan pemasok dari berbagai daerah. Dengan menggunakan WAN, akan memungkinkan bisnis untuk secara efektif melaksanakan fungsi harian-nya dimanapun lokasinya. Internet merupakan contoh yang paling terkenal untu WAN publik.

C Wireless

Wifi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat Wireless Local Area Network (WLAN). (Interprice, 2012)

Wifi adalah singkatan dari Wireles Fidelity, yaitu seperangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (Wireless Local Area Network-WLAN). yang didasari pada spesifikasi IEEE 802.11. (Arifin, 2008)

Wireless adalah jika dari arti katanya dapat diartikan "tanpa kabel", yaitu melakukan suatu hubungan telekomunikasi menggunakan gelombang elektromagnetik sebagai pengganti media kabel. Saat ini teknologi wireless sudah berkembang pesat, buktinya dapat dilihat dapat dilihat dengan semakin banyaknya yang menggunakan telepon sellular, selain itu berkembang juga teknologi wireless yang dipakai untuk mengakses internet yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.16 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya.

C.1 Standar Wireless

Teknologi wifi memiliki standar yang ditetapkan oleh sebuah instusi internasional yang bernama institute of electrical and electronic engineers (IEEE), yang secara umum sebagai berikut :

Tabel 1

Spesifikasi Wifi

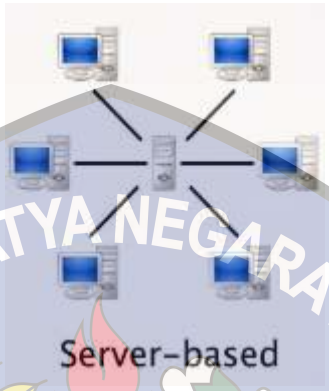
Spesifikasi	Kecepatan (mbps)	Frekuensi (Ghz)	Kompatibilitas
802.11 b	11	2,4	B
802.11 a	54	5	A
802.11 g	54	2,4	b.g
802.11 n	100	2,4	b.g.n

Table 1. Spesifikasi Wifi

1. Standar IEEE 802.11b, merupakan standar dengan frekuensi 2.4 Ghz dengan kecepatan 11 Mbps dan jangkauan jaringan 100 m.
2. Standar IEEE 802.11a, merupakan standar dengan frekuensi 5Ghz dengan kecepatan 54 Mbps. Keuntungan standar 802.11a adalah kapasitas yang cukup tinggi, mencapai 12 channel dan mendukung aplikasi yang membutuhkan performa tinggi. Standar 802.11a tidak kompatibel dengan standar 802.11b/g.
3. Standar IEEE 802.11g, merupakan standar dengan frekuensi 2.4 Ghz dengan kecepatan 54 Mbps.
4. Standar IEEE 802.11n, ditujukan untuk WLAN dengan kecepatan transfer 100Mbps dan bekerja pada frekuensi 2.4 Ghz.

C.2 Tipe Jaringan Wifi

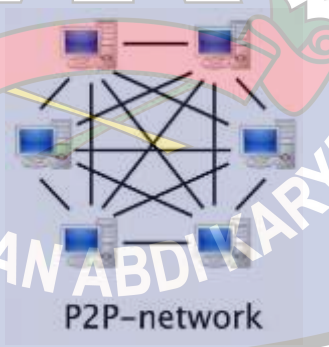
C.2.a Jaringan server based/wireless infrastruktur



Gambar 1. Server based

Sistem infrastruktur membutuhkan sebuah komponen khusus yang berfungsi sebagai access point.

C.2.b Jaringan peer to peer / Ad Hoc wireless LAN



Gambar 2. Jaringan P2P

Sistem Ad-hoc adalah sistem peer-to-peer, dalam arti satu komputer dihubungkan ke satu komputer dengan saling mengenal SSID. Bila digambarkan mungkin lebih mudah membayangkan sistem koneksi langsung dari satu komputer

ke satu komputer lainnya dengan menggunakan twist pair cable tanpa perangkat HUB.

C.3 Komponen Utama Jaringan Wifi

Terdapat beberapa komponen utma untuk membangun sebuah jaringan Wifi yaitu :

1. Wireless-LAN device, komponen yang dipasangkan di Mobile/Dekstop PC.
2. Ethernet LAN, Jaringan kabel yang sudah ada
3. 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 sebuah hub/switch pada jaringan Ethernet.
4. Mobile/Dekstop PC, Komponen akses untuk klien, mobile PC pada umunya sudah terpasang port PCMCIA (Personal Computer Memory Card International Association)

D Password

Password adalah kode sandi yang harus dimasukkan ke dalam suatu sistem baik itu sistem komputer yang menggunakan system oprasi windows atau bukan yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat. Kekuatan kata sandi adalah satu tolok ukur terhadap kekuatan, kerumitan dan keamanan dari suatu kata sandi rahasia yang digunakan sebagai pengenal Kekuatan suatu kata sandi bergantung pada kombinasi, kerumitan dan panjang dari kata sandi tersebut. Walaupun kata sandi memegang peranan yang penting dalam keselamatan komputer, kata sandi perlu digunakan secara wajar dan masuk akal dan berfungsi kepada pengguna. Kata sandi yang terlalu kuat akan sangat sulit untuk diingat dan biasanya akan ditulis dalam media kertas dan hal itu akan meningkatkan risiko kebocoran kata sandi tersebut.

E IP Address

Ip Adrress merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet. Angka 32 bit digunakan untuk alamat IP Address versi IPv4 dan angka 128 bit digunakan untuk IP Address versi IPv6 untuk menunjukkan alamat dari komputer pada jaringan internet berbasis TCP/IP.

IP Address tersebut memiliki identitas numerik yang akan dilabelkan kepada suatu device seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protocol sebagai sarana komunikasi.

F Perbedaan WEP, WPA dan WPA2

F.1 Wired Equivalent Privacy

WEP adalah security untuk wireless yang agak lama. Jenis security ini mudah untuk dicrack atau di sadap orang luar/suatu metoda pengamanan jaringan nirkabel atau wireless. WEP menggunakan 64bit dan 128bit, wep hanya boleh memasukkan 0-9 dan A-F(hexadecimal). Kepanjangan key bergantung jenis securiy anda, jika 64bit, anda kene masukkan 10key, dan untuk 128key anda kena masukkan 26key. Tak boleh kurang dan lebih.Enkripsi WEP menggunakan kunci yang dimasukkan oleh administrator ke client maupun access point, kunci tersebut harus cocok dari yang diberikan access point ke client, dengan yang di masukkan client untukk authentikasi menuju access point, dan WEP mempunyai standart 802.11b Sekarang ini WEP sudah banyak yang meninggalkannya, karena berbagai kelemahan yang ada. Sehingga penggemar wifi dan memiliki kemampuan hacking wireless mampu dengan mudah membobol enkripsi tersebut.

F.2 Wireless Protected Access

WPA adalah security yang lebih update dari WEP. WPA-PSK mempunyai decryption yang ada pada WEP. Wpa adalah model kompatible dengan spesifikasi standar draf IEEE 802.11i. Adanya WPA yang menggantikan WEP mungkin membuat pengguna wireless sedikit lebih tenang karena mempunyai mekanisme enkripsi yang lebih kuat dari pada WEP. Mungkin saat ini sudah ada yang mampu memecahkan enkripsi WPA, tetapi mungkin memerlukan waktu yang lama untuk

memecahkan enkripsi tersebut. Namun bukan tidak mungkin seiring berkembangnya ilmu dan teknologi suatu saat WPA akan dengan mudah di pecahkan dalam waktu yang lebih cepat.Panjang key adalah 8-63, anda boleh memasukkan sama ada 64 hexadecimal atau ASCII(seperti biasa).

F.3 WPA2 PreShared Key

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.

G Firewall

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik akses dalam jaringan. Tugas firewall adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. Firewall sama seperti alat – alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun tidak seperti alat – alat jaringan lain, sebuah firewall harus mengontrol lalu lintas dengan memasukan factor pertimbangan bahwa tidak semua paket – paket data dilihatnya adalah apa yang

seperti terlihat. Firewall digunakan untuk mengontrol akses antara network internal sebuah organisasi internet.

Sekarang ini firewall semakin menjadi fungsi standar yang ditambahkan untuk semua host yang berhubungan dengan network. (Purbo, 2000)

H Mac Address

MAC Address (Media Access Control Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address. (Thomas, 2004)

H.1 Mac Addreess Filtering

MAC Address Filtering merupakan metode filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti pencurian pc card dalam MAC filter dari suatu access point sniffing terhadap WLAN.

H.2 Fungsi Mac Address Filtering

Fitur MAC Address Filter ini berfungsi untuk membantu anda untuk mencegah pengguna asing (tidak diinginkan) yang berniat untuk mengakses masuk ke jaringan router nirkabel anda. Dengan menerapkan fitur ini, maka hanya perangkat nirkabel yang memiliki alamat MAC yang telah terdaftar (ditetapkan) saja yang dapat memperoleh akses ke router nirkabel. Wireless LAN dapat memfilter berdasarkan MAC address dari station/client, hampir semua access point mempunyai kemampuan untuk memfilter berdasarkan MAC address. Administrator jaringan dapat mengompilassi, mendistribusikan, dan memelihara daftar MAC address yang diizinkandan memprogram masing-masing access point, jika sebuah PC card atau client lain dengan sebuah MAC address yang tidak terdaftar mencoba untuk mengakses wifi, kemampuan MAC address filtering tidak akan mengizinkan client berhubungan dengan access point.