PERANCANGAN SISTEM KEAMANAN JARINGAN WIRELESS LOCAL AREA NETWORK PADA KANTOR DINAS KETAHANAN PANGAN KABUPATEN BENGKALIS

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Mendapatkan Gelar Sarjana Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru

Oleh:

NANDA BAYUNDA
153510239

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2021

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Penyayang, Penulis ucapkan puji syukur atas kehadirat-Nya, yang telah melimpahkan rahmat, hidayah, dan inayah-Nya kepada kami, sehingga penulis dapat menyelesaikan proposal skripsi yang berjudul "Perancangan Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis" ini tepat pada waktunya.

Proposal skripsi ini telah penulis susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan proposal skripsi ini. Untuk itu penulis menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan proposal skripsi ini.

Terlepas dari semua itu, penulis menyadari sepenuhnya bahwa masih ada kekurangan baik dari segi susunan kalimat maupun tata bahasanya. Oleh karena itu dengan tangan terbuka penulis menerima segala saran dan kritik agar penulis dapat menyempurnakan laporan ini.

Akhir kata penulis berharap semoga proposal ini dapat memberikan manfaat, inpirasi, dan dapat dipergunakan oleh instansi terkait.

Pekanbaru, 09 Maret 2021

Penulis

DAFTAR ISI

Halaman

BAB IV IMPLEMENTASI DAN PENGUJIAN

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi akses internet telah mencapai tahapan yang lebih mudah penggunaannya dengan memanfaatkan media akses jaringan *wireless* atau disebut dengan nirkabel. Menurut Setiawan (2018), jaringan komputer *wireless* merupakan teknologi yang sering digunakan diberbagai instansi, perusahaan, cafe, toko, dan lain-lain. Jaringan *wireless* tidak hanya digunakan pada intsansi saja, tetapi sebagian rumah tangga juga menggunakannya.

Masalah yang perlu diperhatikan pada jaringan *wireless* adalah keamanannya. Riyasa dkk (2018), Apabila keamanan jaringan nirkabel tersebut memiliki celah, maka akan mudah dimanfaatkan celah tersebut oleh orang yang tidak bertanggung jawab. Hal ini dapat merugikan bagi Instansi yang memiliki jaringan nirkabel tersebut.

Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis merupakan sebuah instansi pemerintahan yang bertempat di Bengkalis. Pada saat ini Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis sudah menggunakan layanan jaringan *wireless*. Namun permasalahan yang terjadi di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis saat ini adalah apabila pengguna ingin mengakses internet

harus melakukan *login* terlebih dahulu dan *password* mudah didapatkan selain itu juga masih bisa membuka situs yang tidak dibenarkan.

Hal ini terjadi karena jaringan *wireless* berada di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis menggunakan keamanan *Wi-Fi Protected Access* (WAP). Dari masalah tersebut dibutuhkan juga keamanan jaringan dengan menggunakan *radius mac authentication* agar pengguna jaringan *wireless* tidak perlu melakukan *login* dan apabila membuka situs yang tidak dibenarkan maka akan diblokir.

Setiawan dan Rini (2019), *Radius mac* merupakan keamanan jaringan yang bekerja dengan memberikan autentikasi dengan *MAC address*. Berdasarkan uraian diatas maka diperlukan perancangan *wireless security* menggunakan *radius mac authentikasi* di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Jaringan *wireless* yang dibangun dapat digunakan untuk pengguna yang sudah mendaftar kepada *administrator*

Dengan menggunakan *wireless security* pengguna jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis dapat langsung terhubung tanpa harus memasukan *login* dan *password* apabila berpindah tempat di area Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Apabila pengguna yang terdaftar membuka situs yang tidak dibenarkan akan terblokir secara otomatis dan pengguna yang ingin menggunakannya kembali harus mendaftarkan *MAC addressnya* kembali dengan *administrator.*

Media Access Control adalah sebuah metode untuk mentransmisikan sinyal yang dimiliki oleh node-node atau disebut satu titik sambungan yang terhubung ke jaringan tanpa terjadi konflik.

Router yang digunakan adalah *router mikrotik* yang dimaksudkan untuk memonitoring dan menjadi keamanan jaringan di sesuaikan dengan kebutuhan di masing masing bagian kantor, Konfigurasi *mikrotik* yang dilakukan dalam penelitian ini adalah dengan menggunakan *winbox* hal ini memudahkan *administrator* dalam memantau akses *internet* dan memantau pengguna yang sudah terdaftar yang dilakukan oleh masing-masing *user* karena telah dilakukan keamanan jaringan tersebut.

Berdasarkan masalah-masalah yang dipaparkan, penulis akan merancang sebuah **"Perancangan Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis"** yang dapat mengatasi masalah-masalah tersebut. Keamanan jaringan ini adalah sebuah keamanan yang akan menangani masalah *login* kepada pengguna agar tidak berulang ulang kali *login* mudah di bobol dan situs yang tidak dibenarkan terbuka.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukakan identifikasi masalah sebagai berikut :

1. Tidak adanya monitoring pengguna jaringan internet sehingga bebasnya pengguna lain untuk menggunakan jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.
2. Setiap mengakses internet harus melakukan *login* terlebih dahulu sehingga menjadi kebosanan bagi pengguna saat ingin mengakses internet
3. Kurangnya keamanan dan tidak optimal jaringan *wireless* di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis
4. Mudahnya pengguna yang tidak bertanggung jawab untuk membobol dan mendapatkan jaringan *wireless* dan bisa membuka situs yang dilarang oleh instansi.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah di uraikan sebelumnya, maka dapat di ambil beberapa poin yang dapat di jadikan rumusan masalah sebagai berikut.

1. Bagaimana Merancang konfigurasi mikrotik dengan sistem keamanan *Radius Media Access Control Authentication*?
2. Bagaimana Merancang konfigurasi mikrotik dengan memonitoring pengguna jaringan internet?

3. Bagaimana cara mengatasi akses internet pengguna dalam 1 kali *login* untuk seterusnya sehingga pengguna tidak perlu berulang-ulang kali *login*?
4. Bagaimana cara untuk memperkuat keamanan serta dapat mengoptimalkan jaringan *wireless hotspot* Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis?
5. Bagaimana cara untuk memblokir situs yang dilarang dari pengguna yang tidak bertanggung jawab?

1.4 Batasan Masalah

Sehubungan dengan keterbatasan yang dimiliki, dari segi waktu, pemikiran serta biaya, maka batasan masalah pada penelitian ini yaitu :

1. Keamanan *Radius MAC Authentication* di implementasikan dengan menggunakan *mikrotik*.
2. Penggunaan Winbox sebagai *GUI* (*Graphical User Interface*) dalam konfigurasi mikrotik.
3. Keamanan *Radius MAC Authentication* yang difokuskan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis menggunakan sistem pendaftaran pada *administrator*.
4. Tipe jaringan yang di gunakan *LAN* dan topologi yang dipakai adalah Star.

1.5 Tujuan Penelitian

Adapun tujuan dalam penelitian ini sebagai berikut :

1. Merancang sistem keamanan jaringan menggunakan *radius mac authentication* di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.
2. Semua bagian unit komputer dan perangkat yang sudah terdaftar sesuai dengan kebutuhan langsung terhubung ke jaringan internet
3. Tercapainya kemudahan bagi pengguna jaringan *wireless hotspot* Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.
4. Meningkatkan Keamanan dan mengoptimalkan jaringan *wireless hotspot* Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.
5. Mengurangi Pengguna *wireless hotspot* yang tidak bertanggung jawab di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.
6. Keamanan jaringan dengan menggunakan *Radius Media Access Control Authentication*.

1.6 Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Memberikan solusi terbaik untuk keamanan jaringan
2. Membantu administrator dalam mengontrol jaringan dan pengguna yang menggunakan jaringan internet.
3. Pengguna akan merasa nyaman menggunakan internet.
4. Memperkuat keamanan dan mengoptimalkan jaringan *wireless hotspot* Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Studi kepustakaan yang pertama adalah berdasarkan penelitian yang dilakukan oleh Yesi Novaria Kunang, Taqrim Ibadi, Suryayusra (2018) tentang Celah Keamanan Sistem Autentikasi *Wireless* Berbasis *RADIUS*. Dengan latar belakang yaitu Penggunaan teknologi jaringan berbasis *wireless* (tanpa kabel) memiliki resiko yang besar akan bahaya serangan dan pencurian informasi. Salah satu teknik pengamanan yang banyak digunakan pada jaringan *wireless* adalah system autentikasi yang menggunakan *RADIUS*. Untuk itu pada penelitian ini membahas pengujian penetrasi pada system Autentikasi *Wireless* berbasis *RADIUS* dengan tujuan untuk mencari celah keamanan pada sistem autentikasi berbasis *RADIUS*. Hasil yang didapatkan dari penelitian ini memperlihatkan bahwa Sistem autentikasi wireless berbasis *RADIUS* masih memiliki beberapa celah keamanan antara lain kemungkinan serangan *DoS* ke *Access point*, pencurian data *clien*t menggunakan *session hijacking*, dan pemutusan koneksi *client* untuk mengambil alih sesi koneksi. Rekomendasi dari penelitian ini diharapkan bisa menjadi acuan bagi administrator dan pengembang jaringan untuk menutup celah keamanan yang bisa dieksploitasi tersebut.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu Mencari celah keamann menggunakan metode RADIUS

Studi kepustakaan yang kedua adalah berdasarkan penelitian yang dilakukan oleh Deny Purwanto, Raditya Danar Dana (2015), tentang Sistem Keamanan Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon. Dengan latar belakang yaitu Keamanan data dalam suatu jaringan komputer sangatlah penting sehingga diperlukannya suatu filter keamanan dan sistem yang mampu mengenkripsi data, dengan adanya filter keamanan dan system mengenkripsi data pihak-pihak yang tidak bertanggung jawab tidak dapat mencuri data dengan mudah karena data tersebut sudah diamankan oleh filter keamanan dan system mengenkripsi data. Sehingga dengan adanya sistem ini tidak ada lagi kehilangan atau kebocoran data pada suatu jaringan komputer. Suatu keamanan jaringan yang dibuat agar data tidak mudah dibaca atau dibobol dan tidak terjadinya lagi kebocoran data oleh pihak ketiga dengan cara data pada komputer server diproteksi dengan menggunakan mikrotik dan Password, Username dan data terenkripsi dengan menggunakan md5.

MD5 yang merupakan singkatan dari Message-Digest algortihm 5, adalah fungsi hash (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografik yang digunakan secara luas dengan hash value 128-bit.

MD5 dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk menguji integritas sebuah file. Sehingga password, username dan data yang terenkripsi. Sehingga tidak mudah dibaca atau dibobol oleh pihak ketiga yang tidak bertanggung jawab. Karena begitu pentingnya keamanan data pada suatu jaringan dalam dunia jaringan komputer.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu menjaga kehilangan atau kebocoran data pada suatu jaringan komputer menggunakan metode Message-Digest algortihm 5.

Studi kepustakaan yang ketiga adalah berdasarkan penelitian yang dilakukan oleh Ahmad Herdinal Muttaqin, Adian Fatur Rochim, Eko Didik Widianto (2016) tentang Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. Dengan latar belakang yaitu Jaringan nirkabel adalah jaringan yang memanfaatkan gelombang radio yang menyebar secara terbuka. Jaringan ini membutuhkan keamanan untuk menyederhanakan proses dengan menggunakan Otentikasi pengguna. Salah satu teknologi yang dapat digunakan untuk membuatnya lebih aman adalah Lightweight Directory Access Protocol (LDAP) dan Remote Authentication Dila In User Service (RADIUS).

Jurusan Teknik Sistem Komputer adalah salah satu program studi di Fakultas Teknik, Universitas Diponegoro yang memesan layanan internet setiap hari untuk kebutuhan mahasiswa. Namun, jaringan nirkabel internet di departemen ini belum cukup aman, untuk itu perlu dibuat sistem keamanan dengan LDAP dan RADIUS. Hasil penelitian ini adalah server otentikasi jaringan menggunakan Open LDAP dan FreeRadius Hotspot yang akan diintegrasikan dengan akun Sistem Informasi Akademik, yang diterapkan pada Prodi Teknik Sistem Komputer Universitas Diponegoro.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu Sistem Autentikasi Hotspot menggunakan metode LDAP dan RADIUS

Dalam penelitian ini, diambil beberapa referensi kepustakaan yang bersumber pada penelitian-penelitian sebelumnya. Hal ini berguna sebagai perbandingan bahan referensi dalam menyelesaikan penelitian ini. Adapun penelitian yang berkaitan dengan masalah yang diteliti yaitu dapat dilihat pada table 2.1.

Tabel 2.1 Kajian Terdahulu

NO	Judul Penelitian	Tahun	Penulis	Keterangan
1	Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS	2017	Yesi Novaria Kunang, Taqrim Ibadi, Suryayusra	Keamanan sistem ini dibangun sebagai pengguna yang mempunyai satu akun terintregasi untuk bisa mendapat fasilitas internet
2	Sistem Keamanan Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon	2015	Deny Purwanto, Raditya Danar Dana	Sistem keamanan ini bertujuan untuk memproteksi kehilangan atau kebocoran data pada suatu jaringan computer
3	Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer	2016	Ahmad Herdinal Muttaqin, Adian Fatur Rochim, Eko Didik Widianto	Sistem ini dibangun sebagai kemudahan bagi setiap pengguna yang mempunyai satu akun terintregasi untuk bisa mendapakan fasilitas internet tanpa mengenyampingkan aspek keamanan yang ada.

2.2 Dasar Teori

2.2.1 Jaringan

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lain yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data.

Mencetak pada printer yang sama dan bersama sama menggunakan *software/hardware* yang terhubung dengan jaringan. Tiap komputer, printer atau periperal yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ratusan, ribuan, atau bahkan jutaan *node*. Sebuah jaringan biasanya terdiri dari dua atau lebih komponen yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya *CDROM*, printer, pertukaran file, atau memungkinkan untuk saling berkomunikasi secara elektronik (Basten, 2019)

2.2.2 *Router*

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasarannya, melalui sebuah proses yang dikenal sebagai *routing*. Proses *routing* dapat dilakukan dengan memasukkan informasi suatu alamat jaringan secara manual kedalam tabel *routing* ataupun dengan bantuan protokol *routing*. Sebuah *router* mampu mengirimkan data / informasi dari satu jaringan ke jaringan lain yang berbeda, *router* hampir sama dengan *bridge*, namun *router* lebih pintar dibandingkan dengan *bridge*. Karena *router* mampu menghubungkan dua atau lebih jaringan yang berbeda, sedangkan *bridge* hanya mampu menghubungkan jaringan yang sama. Dalam pengembangan perangkat *router* dewasa ini sudah mulai mencapai atau bahkan melampaui batas tuntutan teknologi yang diharapkan.

Router akan mencari jalur terbaik untuk mengirimkan sebuah pesan yang berdasarkan atau alamat tujuan dan alamat asal. *Router* mengetahui alamat secara keseluruhan dari masing-masing komputer dilingkungan jaringan lokalnya, dan *router* lainnya (Sumarianta, 2011).

2.2.3 *Radius Server*

Radius server merupakan suatu mekanisme kontrol yang mengecek dan mengautentifikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme *autentifikasi* dengan menggunakan metode *callenge/response remote acces dial in user service* (*radius*) merupakan *protokol connectionless* berbasis UDP yang tidak menggunakan koneksi langsung. Satu paket *radius* ditandai dengan *field* UDP yang menggunakan *port* 1812 *Radius* menggunakan lapisan *transport* UPD dan radius memiliki tempat yang paling penting pada layanan internet, pada pengaturan, otorisasi, dan rinci *accounting* pengguna baik yang diperlukan atau diinginkan (Jonatan, 2012).

2.2.4 *Wireless* LAN

Jaringan *wireless* LAN merupakan suatu sistem komunikasi data tanpa kabel yang merupakan solusi alternatif dari jaringan komputer yang menggunakan kabel (*Wireless* LAN). Dengan kata lain jaringan *Wireless* LAN TEKNO ISSN : 0215 – 9617 Nomor /// ‟09 /3 merupakan salah satu pengembangan media transmisi dari teknologi jaringan komputer dengan menggunakan perangkat radio komunikasi data yang dapat menghubungkan sebuah komputer ke jaringan *local Area Network*

(LAN). Jaringan *Wireless* LAN dapat dipasang didalam sebuah gedung, maupu diluar gedung (Najoan,2019).

2.2.5 *Mikrotik*

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi *router* jaringan yang handal, mencakup berbagai fitur yang dibuat untuk IP *network* dan jaringan *wireless*, cocok digunakan oleh ISP dan provider *hotspot* (mikrotik.co.id). Jenis *Mikrotik* sebagai berikut:

a. *Mikrotik RouterOS™* adalah versi *MikroTik* dalam bentuk perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. Anda dapat mengunduh file gambar *mikrotik router OS* dari website resmi *mikrotik*, www.mikrotik.com. Namun, file image ini merupakan versi *trial mikrotik* yang hanya dapat dalam waktu 24 jam saja. Untuk dapat menggunakannya secara penuh, anda harus membeli lisensi *key* dengan catatan satu lisensi hanya untuk satu hardisk.

b. *BUILT IN Hardware* adalah *mikrotik* dalam bentuk perangkat keras yang khusus dikemas dalam *routerboard* yang didalamnya sudah terinstal *mikrotik router operating system*.

   Terdapat beberapa cara untuk me-remote *MikroTik*, antara lain, melalui winbox, Browser, telnet dan ssh.

2.2.6 Keamanan *Wireless*

Kelemahan *wireless* dapat dibagi menjadi 2 jenis, yaitu kelemahan pada konfigurasi dan pada jenis enkripsi yang digunakan. Secara umum, celah pada jaringan wireless terbentang diatas empat layer dimana keempat lapis (layer) sebenarnya merupakan proses terjadinya komunikasi data pada media wireless. Keempat lapis tersebut yaitu lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi wireless tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC filtering, pemasangan infrastruktur captive portal dan lain sebagainya (Supriyono dan Riadi, 2013).

2.2.7 *Proxy*

Proxy Server adalah server yang diletakkan antara suatu aplikasi *client* dan aplikasi server yang dihubungi. Aplikasi *client* dapat berupa *browser web, client FTP,* dan sebagainya. Sedangkan aplikasi *server* dapat berupa *server web, server FTP* dan sebagainya. Proxy Server yang diletakkan di antara aplikasi *client* dan aplikasi server tersebut, dapat digunakan untuk mengendalikan maupun memonitor lalu-lintas paket data yang melewatinya. Proxy memiliki 3 fungsi :

1. *Connection Sharing*

Bertindak sebagai *gateway* yang menjadi batas antara jaringan lokal dan jaringan luar. *Gateway* juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya dan koneksi jaringan luar juga terhubung kepadanya. Dengan demikian koneksi dari jaringan lokal ke internet akan menggunkan sambungan yang dimiliki oleh *gateway* secara bersama-sama.

2. *Filtering*

Bekerja pada layer aplikasi sehingga berfungsi sebagai *firewall* paket *filtering* yang digunakan untuk melindungi jaringan lokal terhadap gangguan atau serangan dari jaringan luar. Dapat dikonfigurasi untuk menolak situs web tertentu pada waktu-waktu tertentu.

3. *Caching*

Proxy server memiliki mekanisme penyimpanan obyek-obyek yang sudah diminta dari server-server di internet. Mekanisme *caching* akan menyimpan obyek-obyek yang merupakan permintaan dari para pengguna yang di dapat dari internet. Jadi ketika obyek-obyek yang pernah diminta akan diminta lagi, tidak perlu lagi untuk meminta ke server-server internet melaikan cukup me-*reload* di proxy server. (Wijaya, 2015).

2.2.8 *Best Effort Wireless Security*

Untuk penggunaan *wireless security* saat ini yang *reliable* adalah WPA/WPA2 dimana *enkripsi* yang digunakan sudah mendukung keutuhan dan kerahasiaan data lebih tinggi. Tentu ingin menerapkan sebuah metode keamanan yang tinggi untuk menjaga jalur koneksi *wireless* agar tetap aman.

Akan tetapi perlu diketahui bahwa tidak semua perangkat *wireless support* untuk penerapan metode *wireless security*. Dalam membangun jaringan *wireless*, sebagai *administrator* jaringan kita harus mengetahui detail spesifikasi perangkat *wireless* yang akan digunakan, termasuk dukungan metode *wireless security* yang bisa diterapkan. Dua buah perangkat *wireless* dengan dukungan dan penerapan metode *wireless security* yang berbeda tidak akan bisa terkoneksi (Wijaya, 2015).

2.2.9 *Remote Access Dial In User Service (RADIUS)*

Radius dikembangkan untuk menjawab kebutuhan *user* dalam melakukan akses berbagai macam *resource* computer dari lokasi lain secara remote, serta memberikan layanan standar pada beberapa lingkungan perusahaan yang menginginkan proteksi atas akses jaringannya.

2.2.10 *Authentication*

Authentication adalah suatu proses dimana user diidentifikasi oleh server sebelum user menggunakan jaringan. Pada proses ini, user meminta hak akses kepada NAS (*Network access Server*) untuk menggunakan suatu jaringan.

NAS kemudian menghubungi kepada server apakah user yang bersangkutan berhak untuk menggunakan jaringan atau tidak.

2.2.11 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer.

Bagaimana tidak banyak ancaman-ancaman yang terjadi pada sistem informasi yang akan merugikan banyak pihak, baik individu, masyarkat, dan lain sebagainya. Oleh karena itu untuk mencegah ancaman-ancaman terhadap sistem informasi yaitu perlu adanya keamanan yang sangat canggih agar dapat mendeteksi atau membenarkan dari sebagian sistem yang rusak akibat gangguan pada sistem informasi.Ada beberapa tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuantujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

a. Setiap penyusup hanya ingin tau susunan sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini disebut dengan *the curius.*
b. Hanya ingin membuat sebuah sistem jaringan menjadi *down,* atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini disebut sebagai *the malicious.*

c. Penyusup hanya berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini disebut sebagai *the high-profile intruder.*

d. Penyusup hanya ingin tau susunan data apa saja yang ada di dalam jaringan komputer dan selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini disebut sebagai *the competition.*

2.2.12 Kelemahan

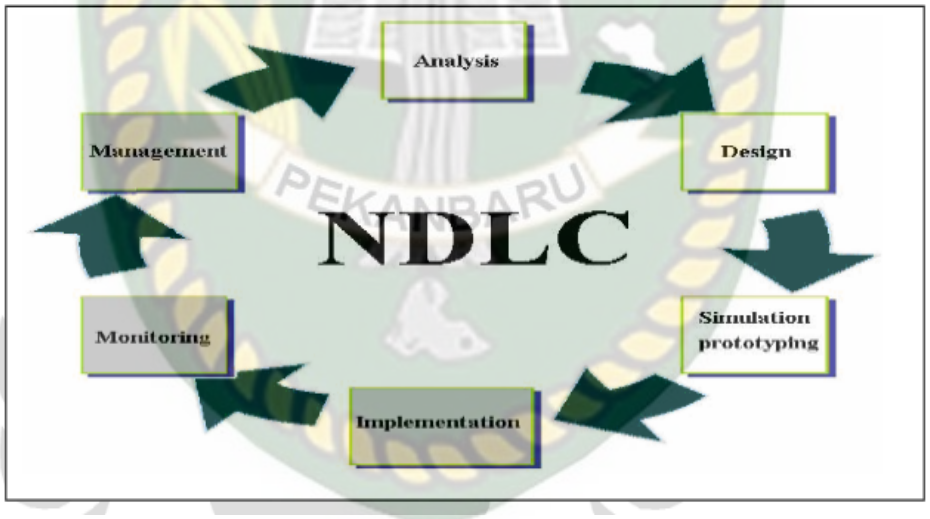
Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya.

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Pada metode ini akan di terangkan mengenai cara dan langkah-langkah yang akan di lakukan dalam penelitian tentang Perancangan Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis, Pada penelitian ini digunakan metode pengembangan sistem *Network Development Life Cycle* (NDLC), adapun metode dapat dilihat pada gambar 3.1 di bawah ini



Gambar 3.1 *Network Developmen Life Cycle*

3.1.1 *Analysis*

Tahapan Analisa sistem ini meliputi analisa dari sistem yang ada dan analisa sistem yang diusulkan. Dilakukan dengan pengujian perbandingan beberapa jenis keamanan yang sering dipakai seperti WAP2, WPA, SSID, WPA/WPA2 dan PROXY Menganalisa kelebihan dan kelemahan teknik keamanan tersebut secara mendalam dengan melakukan hacking.

3.1.2. *Design*

Data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa *design* struktur topologi, *design* akses data, *design* tata *layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang *project* yang akan dibangun.

3.1.3. *Simulation Prototype*

Beberapa *network* akan membuat dalam bentuk simulasi dengan bantuan *Tools* khusus di bidang *network* seperti *Packet Tracert*, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun dan sebagai bahan resentasi dan *sharing* dengan *team work* lainnya.

3.1.4. *Implementation*

Tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi *network* akan menerapkan semua yang telah direncanakan dan di *design* sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan ditahap inilah akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

3.1.5 *Monitoring*

Setelah implementasi tahapan *monitoring* merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*. *Monitoring* bisa berupa melakukan pengamatan.

3.1.6. *Management*

Management atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah keamanan, kebijakan perlu dibuat untuk membuat / mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur Reliability terjaga. Keamanan akan sangat tergantung dengan kebijakan level management dan strategi kantor.

3.1.1 Alat Dan Bahan Penelitian yang Digunakan

Adapun alat dan bahan yang digunakan pada penelitian ini sebagai berikut.

3.1.1.1 Spesifikasi Perangkat Lunak (*Software*)

Spesifikasi perangkat lunak pada penelitian ini sebagai berikut :

Tabel 3.1 Spesifikasi Perangkat Lunak

NO	Kebutuhan	Keterangan	Fungsi
1	Sistem Operasi	Window 7 Ultimate 32 bit	Mengontrol operasi-operasi dasar sistem, termasuk menjalankan perangkat lunak Aplikasi.
2	Aplikasi	Winbox	Penghubung antar kemputer ke mikroting dan sebagai tool untuk mengkonfigurasi perangkat mikrotik

3.1.1.2 Spesifikasi Perangkat Keras (*Hardware*)

Spesifikasi perangkat keras pada penelitian ini sebagai berikut :

Tabel 3.2 Spesifikasi Perangkat Keras

NO	*Hardware*	Spesifikasi	Jumlah	Fungsi
1	Laptop	Intel(R) Core (TM) i5 CPU M 460 @ 2.53 GHz (4CPUz) Memory 4 Gb Harddisk 500 Gb	1	Sebagai alat antar muka penampilan dan pengendalian
2	Mikrotik	RB 950	2	Sebagai alat *Router*

				untuk membagi jaringan ke pengguna dan sebagai *server* keamanan jaringan
3	Switch	D-Link Switch Hub 16 Port Gigabit	1	Sebagai alat untuk meneruskan jaringan
4	Access Point	TP-Link TL-WA801ND 300 Mbps Wireless N Access Point	1	Sebagai alat menyebar jaringan
5	Kabel	UTP 10 M	1	Sebagai Penghubung dari Internet Service Provider Ke *Router*
6	Konektor	RJ 45	1	Sebagai kepala kabel
7	Printer	Epson L120	1	Sebagai alat untuk mencetak laporan

3.1.2 Metode Pengumpulan Data

Pengumpulan data dalam penelitian ini akan menggunakan teknik observasi, wawancara, dan studi Literatur. Metode ini bertujuan untuk memperoleh data-data yang berhubungan dengan penelitian mengenai Perancangan keamanan jaringan Menggunakan *Radius Media Access Control Authentication* di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.

1. Observasi

   Observasi merupakan sutau teknik pengumpulan data yang mempelajari sistem, dengan cara mengamati langsung objek penelitian Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis termasuk tempat dan jumlah pengguna jaringan.

2. Wawancara

   Wawancara merupakan pertanya langsung yang di tanyakan oleh pihak terkait khsusnya Tim jaringan / pengguna jaringan, yang di lakukan adalah dengan Tim jaringan / pengguna jaringan tersebut menanyakan jaringan yang sedang berjalan untuk menunjang penelitian yang di buat.

3. Studi Literatur

   Studi Literatur yaitu pengumpulan data dengan membaca, mempelajari dan menganalisa beberapa buku, jurnal, dan website yang berkaitan dengan masalah penelitian ini

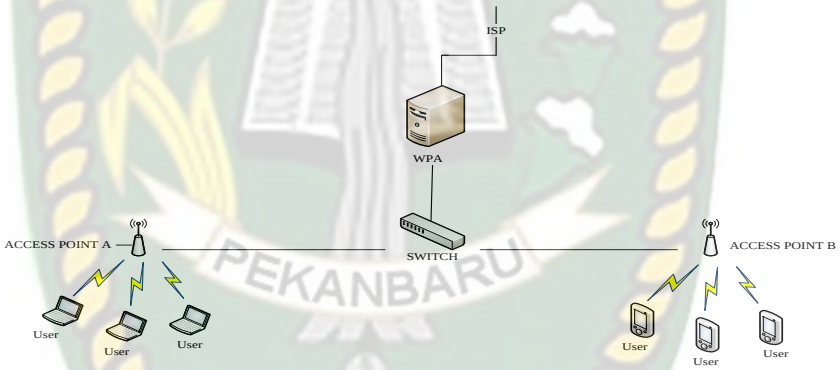
3.2 Perancangan Sistem

Pada tahap ini akan dijelaskan tentang perancangan sistem yang akan dikembangkan.

3.2.1 Perancangan Sistem Jaringan Kantor Dinas Ketahanan Pangan Bengkalis

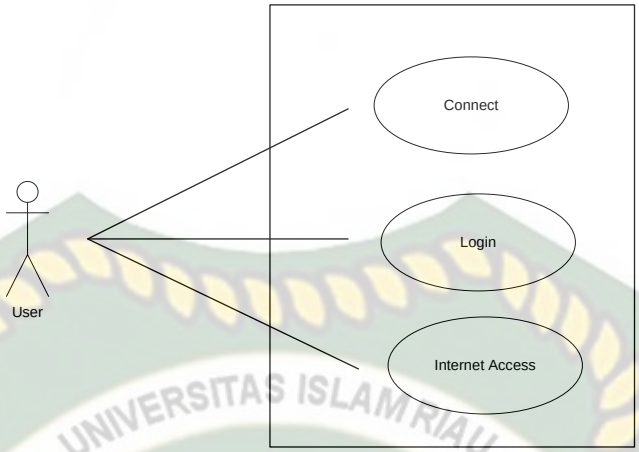
Sistem jaringan yang ada di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis yang menggunakan sistem keamanan wi-fi protected access (wpa) dan menggunakan OS Windows 7.

Dalam perancangan topologi, Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis menggunakan jaringan kabel yang terhubung dan dapat diakses jika terhubung ke internet. Topologi yang digunakan adalah topologi star. Prosesnya dapat dilihat pada gambar 3.1.



Gambar 3.1 *Topologi* Jaringan

Sistem wi-fi protected access yang ada di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis yaitu jika ingin mengakses internet harus memasukkan *Login*. Proses sistem yang sedang berjalan dapat dilihat pada gambar 3.2.

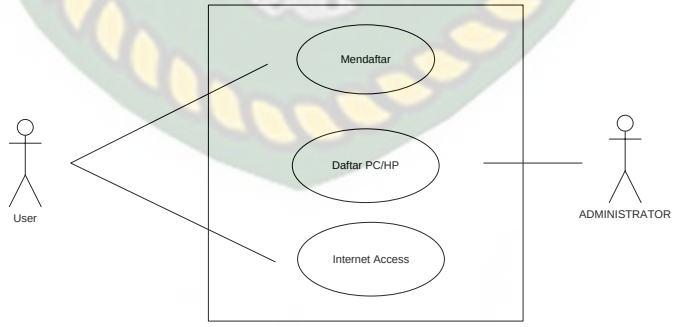


Gambar 3.2 Sistem yang sedang berjalan

3.3 Perancangan Sistem

Dengan adanya permasalahan yang terjadi, maka perlu diusulkan sebuah sistem keamanan jaringan menggunakan Radius Media Access Control Authentication, menggunakan system pendaftaran kepada administrator.

Dimana pengguna harus mengdaftarkan Laptop/PC dan Handphone yang digunakan untuk mengakses internet. Proses sistem yang diusulkan dapat dilihat pada gambar 3.3.



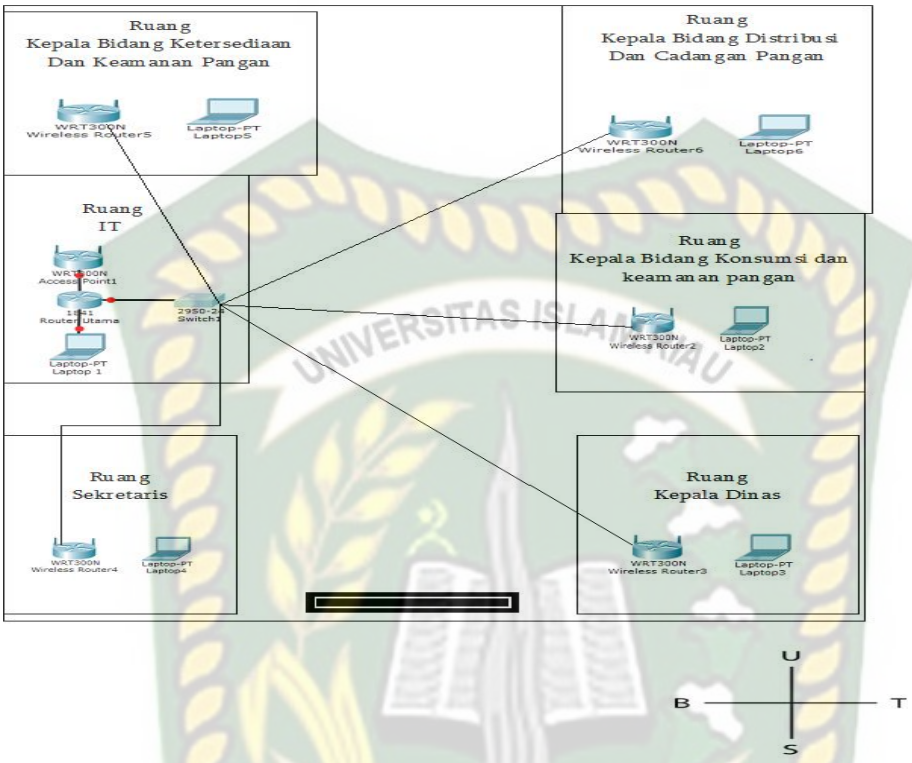
Gambar 3.3 Sistem yang di usulkan

3.3.1 Perancangan Desain Topologi Fisik

Melihat kondisi serta keadaan dari sisi hardware, software serta komponen perangkat pendukung jaringan dengan skala local area network Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis akan menghasilkan skema secara keseluruhan yang akan menggambarkan bentuk terstruktur dari jaringan yang akan dibangun pada Ruangan komputer di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Dapat di lihat skema jaringan bisa bermacam-macam, itu akan sangat tergantung dengan kebutuhan dan skala besar kecilnya suatu jaringan.

Ada skema yang baku yang diperlukan dalam kebutuhan diagram jaringan skala besar yang biasa dibutuhkan untuk kebutuhan dokumentasi yang dalam kebutuhannya diperlukan sebagai alat bantu untuk memudahkan troubleshooting jaringan jika ada masalah.

Selain itu, skema ini akan menyangkut tentang bagaimana menghubungkan perangkat jaringan untuk membentuk suatu jaringan komputer yang dapat memaksimalkan komponen yang ada pada ruangan tersebut, ini dapat dilihat dari skema desain ruangan serta tata letak dari setiap komponen yang digunakan didalam ruang Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis seperti gambar dibawah ini :



Gambar 3.4 Denah Ruang Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis

3.3.2 Perancangan Desain Topologi Logic

Perancangan desain topologi logic dilakukan dengan melakukan pengaturan IP address. Ip address itu sendiri dapat diartikan dengan identitas komputer/host yang terkoneksi ke jaringan (Local Area Network), dan identitas komputer dalam jaringan yg sama pasti unik, artinya satu alamat ip dipakai oleh satu komputer dalam satu jaringan, tidak bisa lebih.

Manajemen IP Address digunakan agar dapat mengelola dan mengatur IP dengan baik dan lebih efisien. Ada beberapa teknik memanajemen IP Address,diantaranya adalah subnetting dan VLSM. Subnetting adalah proses memecah suatuIP jaringan ke sub jaringan yang lebih kecil yang disebut "subnet". Dan VLSM (Variable Length Subnet Mask) adalah teknik yang memungkinkan administrator jaringan untuk membagi ruang alamat IP ke subnet yang berbeda ukuran tidak seperti ukuran subnetting.

Untuk menyederhanakan VLSM adalah dengan memecah alamat IP ke subnet (beberapa tingkat) dan mengalokasikan sesuai dengan kebutuhan individu pada jaringan. VLSM merupakan pengembangan mekanisme subneting, dimana dalam VLSM dilakukan peningkatan dari kelemahan subneting klasikyang mana dalam klasik subnetingVLSM digunakan karena memudahkan admin jaringan untuk mengatur banyak subnetmask dalam ruang alamat IP yang sama dan mengurangi masalah kekurangan alamat IP. Maka dapat digunakan teknik VLSM ini untuk memanajemen IP Address pada perancangan sesuai topologi di ruang Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Ada beberapa bagian yang akan di set IP address, dengan asumsi IP server masih default yaitu :

IP Address 192.168.100.1

Subnet Mask 255.255.255.0

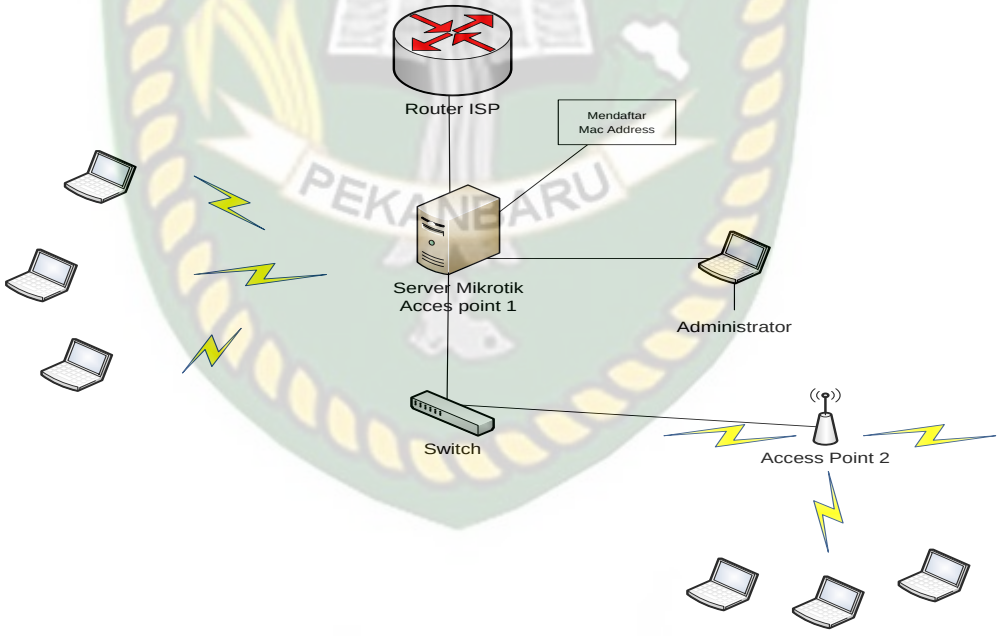
Tabel 3.3 Pengaturan IP Address

Nama Ruangan	IP Address	Prefix	Netmask
Ruang IT -Router Utama -Switch -Access Point1 -PC	 -192.168.100.1 -DHCP -DHCP -DHCP	 /24 /24 /24 /24	 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0
-Ruang Kepala Bidang Konsumsi Dan Keamanan Pangan -Access Point 2 -PC/Laptop	-192.168.10.1 -DHCP	/24 /24	255.255.255.0 255.255.255.0
-Ruang Kepala Dinas -Access Point 3 -PC/Laptop	 -192.168.20.1 -DHCP	 /24 /24	 255.255.255.0 255.255.255.0
-Ruang Sekretaris -Access Point 4 -PC/Laptop	 -192.168.30.1 -DHCP	 /24 /24	 255.255.255.0 255.255.255.0
-Ruang Kepala Bidang ketersediaan Dan Keamanan Pangan -Access Point 5 -PC/Laptop	-192.168.40.1 -DHCP	/24 /24	255.255.255.0 255.255.255.0
-Ruang Kepala Bidang Distribusi dan Cadangan Pangan -Access Point 6 -PC/Laptop	-192.168.10.1 -DHCP	/24 /24	255.255.255.0 255.255.255.0

3.3.3 Perancangan Arsitektur Jaringan

Dari permasalahan yang dijadikan penelitian maka harus dirancang sebuah topologi jaringan yang bisa menghubungkan antara *server* dan *client* yang terkoneksi internet. Dalam perancangan topologi menggunakan jaringan nirkabel yang terkoneksi internet dan dapat diakses jika terhubung ke internet.

Topologi yang digunakan adalah topologi star dengan terkoneksi internet dan akan dipancarkan oleh *acces point* sehingga komputer memiliki *wireless* yang *connect* akan terhubung ke internet secara otomatis dan apabila pengguna ingin berpindah tempat dalam satu area maka tidak perlu memasukkan *login* ulang. Topologi jaringannya dapat dilihat pada gambar 3.4



Gambar 3.5 Perancangan Arsitektur Jaringan

Dari gambar 3.4, menujukkan bahwa komponen yang digunakan terdiri dari dua buah *access point* yang telah di konfigurasi dan terkoneksi internet, AP1 sebagai *server radius*, AP2, dan beberapa *Client*.

Dua buah akses point memiliki fungsi sebagai pemancar. Keamanan jaringan disini yaitu apabila pengguna berpindah tempat maka pengguna tidak melakukan *login* ulang dan akan tersambung oleh *access point* terdekat secara otomatis bagi pengguna yang telah terdaftar dan apabila pengguna membuka situs yang dilarang maka akan terblokir.

Cara pendaftarannya yaitu pengguna hanya tinggal membawa *MAC address* laptop/PC ke administrator. Fungsi *MAC adrress* yaitu sebagai alamat yang di pastikan setiap laptop/PC pasti memiliki satu *MAC address.*

BAB IV

IMPLEMENTASI DAN PENGUJIAN

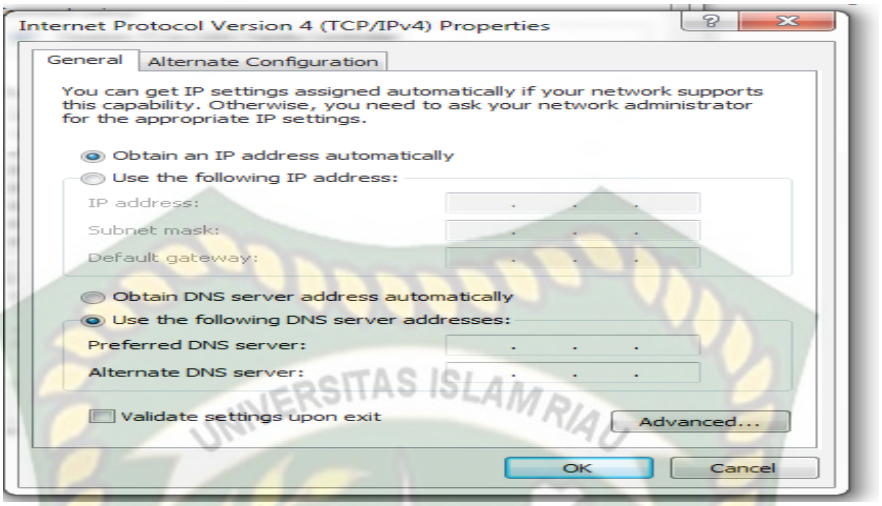
4.1 Implementasi dan Pengujian

Analisis ini perlu dilakukan agar dapat mengetahui seberapa aman tingkat keamanan yang ada dalam sebuah jaringan *wireless* pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Seperti pada umumnya tingkat keamanan bukan berasal dari *hardware* dan *software* yang sudah ada namun terdapat peran penting dari manusia / pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri.

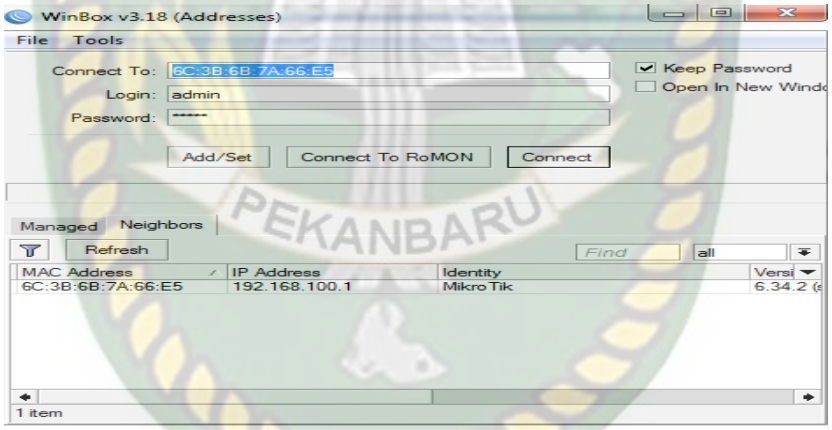
Keamanan jaringan komputer yang terpasang di area Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis pada umumnya masih perlu peningkatan keamanan, terbukti pada *wifi* yang terpasang tidak menggunakan keamanan atau terbuka. Disamping itu masih banyak pegawai yang masih awam tentang keamanan jaringan *wifi.*

4.1.1 Implementasi *Networking*

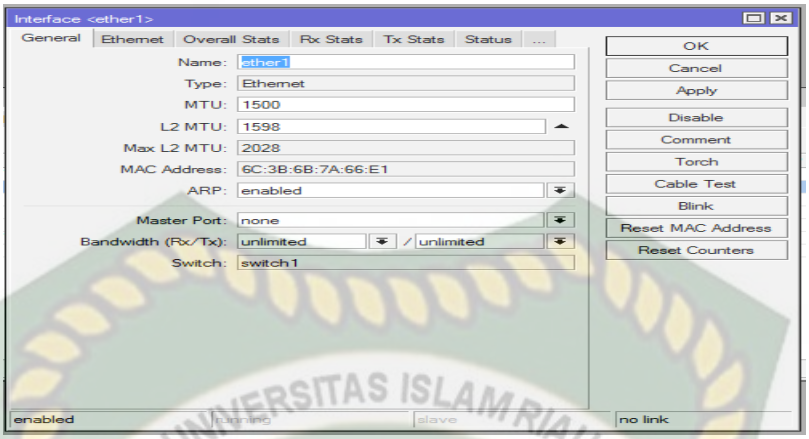
Sebelum melakukan keamanan jaringan, terlebih dahulu melakukan kinfigurasi *networking* agar pengguna jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis dapat terhubung atau terkoneksi jaringan. Berikut ini adalah tampilan-tampilan konfigurasi jaringan mikrotik untuk mengaktifkan jaringan wireless, sehingga pengguna bisa mengakses internet, dapat dilihat pada gambar 4.1 – 4.13.



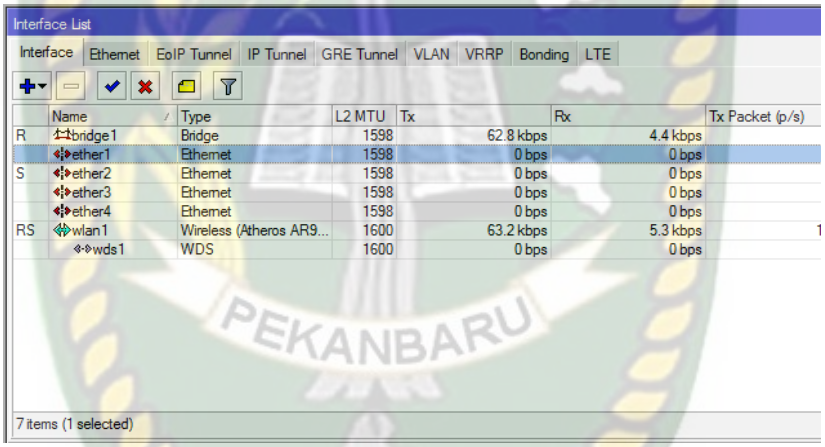
Gambar 4.1 Setting IP Laptop



Gambar 4.2 Tampilan Awal Winbox

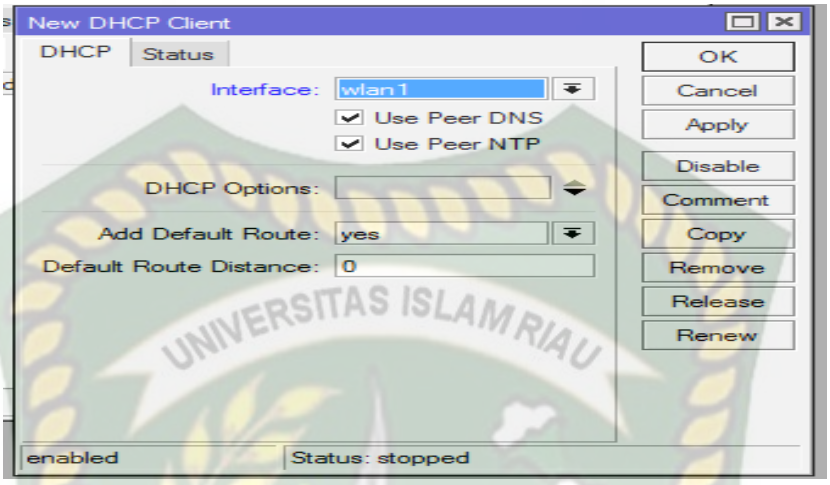


Gambar 4.3 *Setting Interfaces Mikrotik*

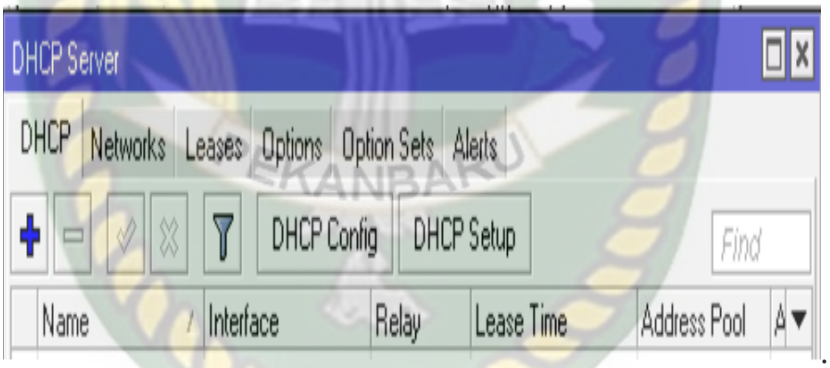


Gambar 4.4 *Setting Nama Interface*

Gambar 4.5 *Setting IP Address*

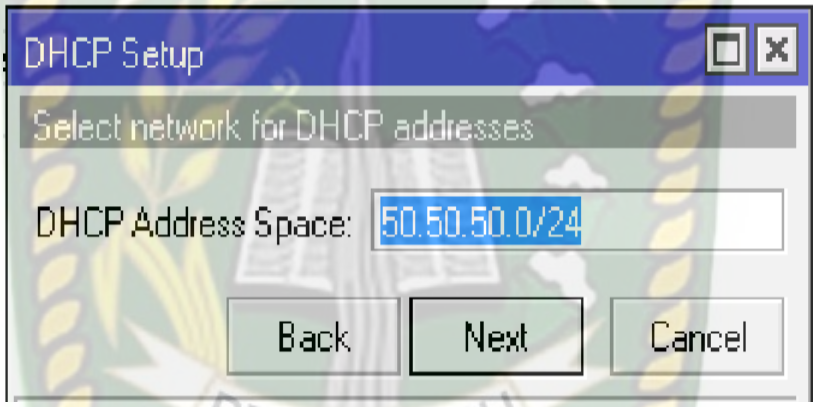


Gambar 4.6 *Setting DHCP Client*

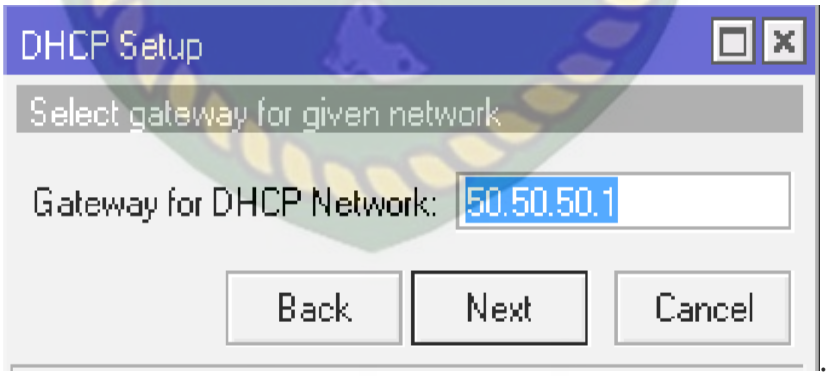


Gambar 4.7 *Setting DHCP Setup*

Gambar 4.8 *DHCP Server Interface*



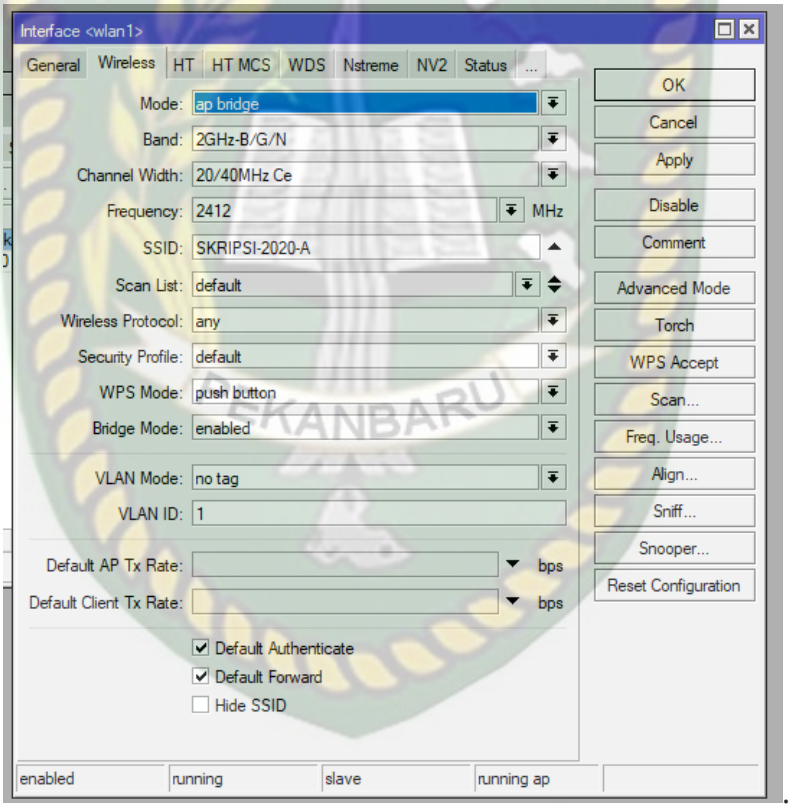
Gambar 4.9 *DHCP Address Space*



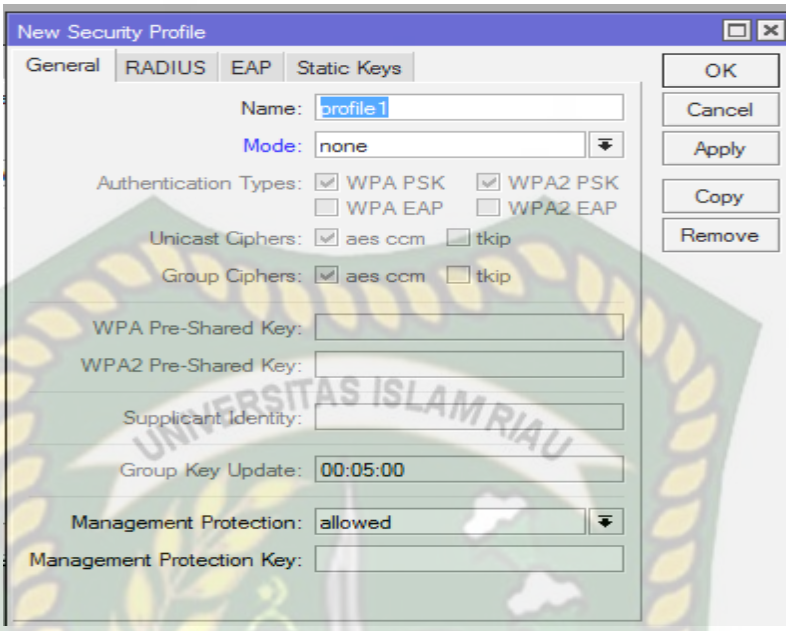
Gambar 4.10 *Gateway DHCP Network*

.

Gambar 4.11 *DHCP Relay*



Gambar. 4.12 *Setting WLAN*



Gambar 4.13 *Setting Security Wireless*

4.1.2 Implementasi Network

Secara teknis proses implementasi agar terarah nantinya maka pengujian membuat sebuah topologi untuk memberikan simulasi terhadap jangkauan keamanan jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis dapat dilihat pada gambar 4.14.

Gambar 4.14 Topologi jaringan

4.1.3 Implementasi Bandwidth Masing-Masing Ruangan

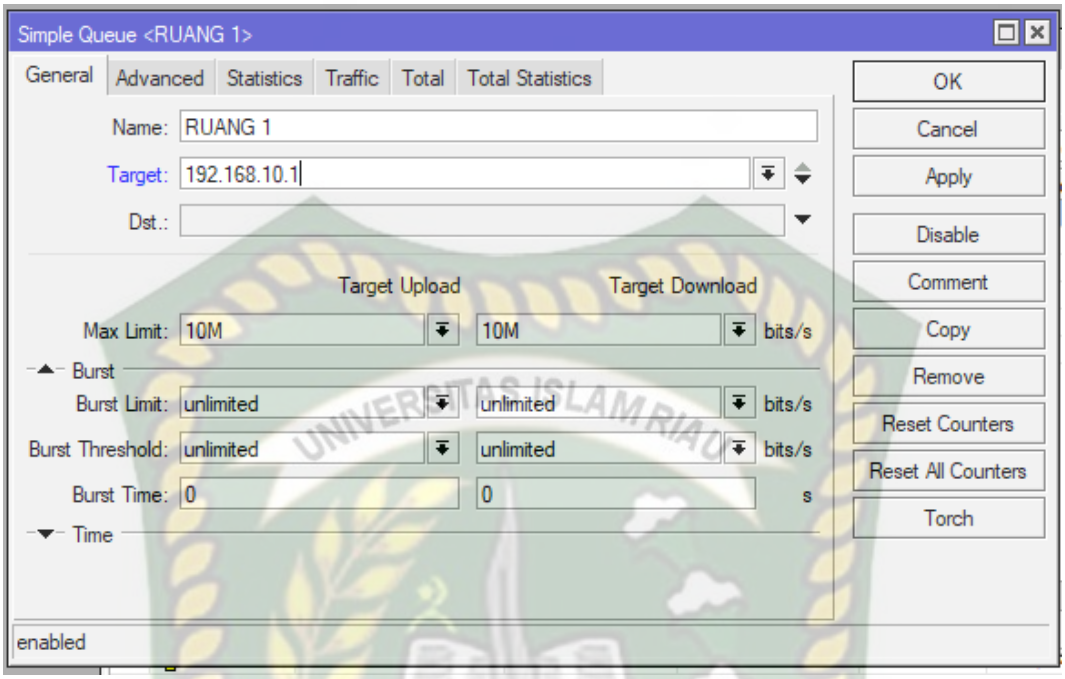
Bandwidth yaitu kecepatan transfer data client pada lalu lintas internet yang diukur dalam bit per second (bps) atau bytes per second (Bps). Pembagian yang dilakukan Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis adalah menurut level Ruangan. Berikut table pembagian bandwidth 50 MBps yang ada di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis

Tabel 4.1 Pembagian *Bandwidth*

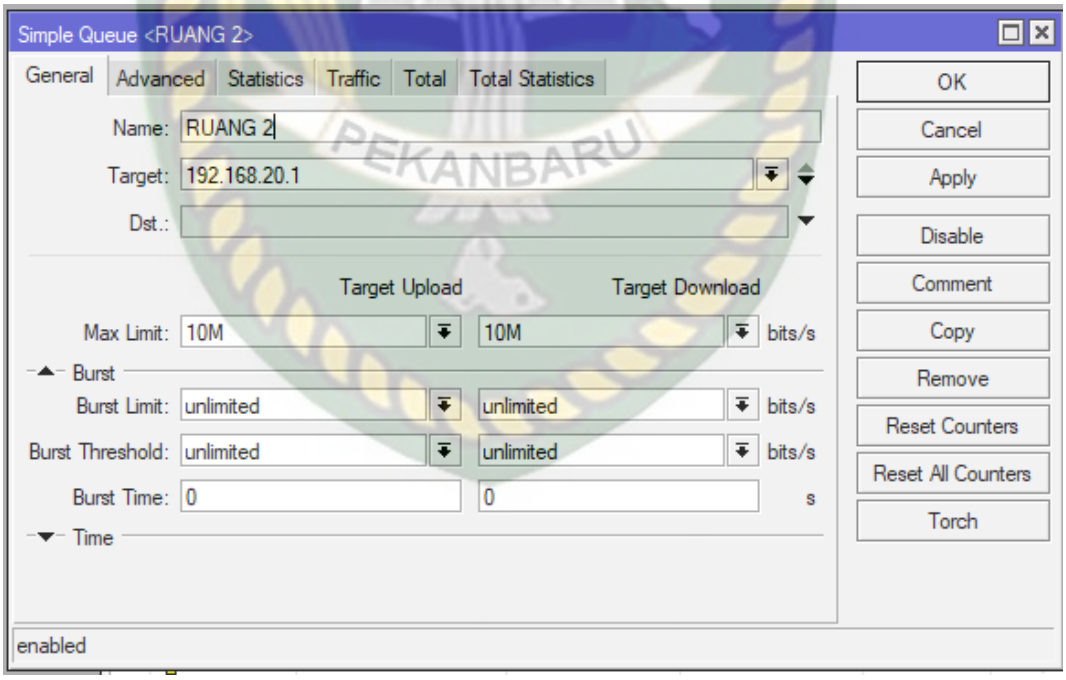
NO	Ruangan	Total Bandwidth	Download	Upload
1	Ruang 1	10 MBps	10 MBps	10 MBps
2	Ruang 2	10 MBps	10 MBps	10 MBps
3	Ruang 3	10 MBps	10 MBps	10 MBps
4	Ruang 4	10 MBps	10 MBps	10 MBps
5	Ruang 5	10 MBps	10 MBps	10 MBps

4.1.3.1 Implemetasi Bandwidth Simple Queue

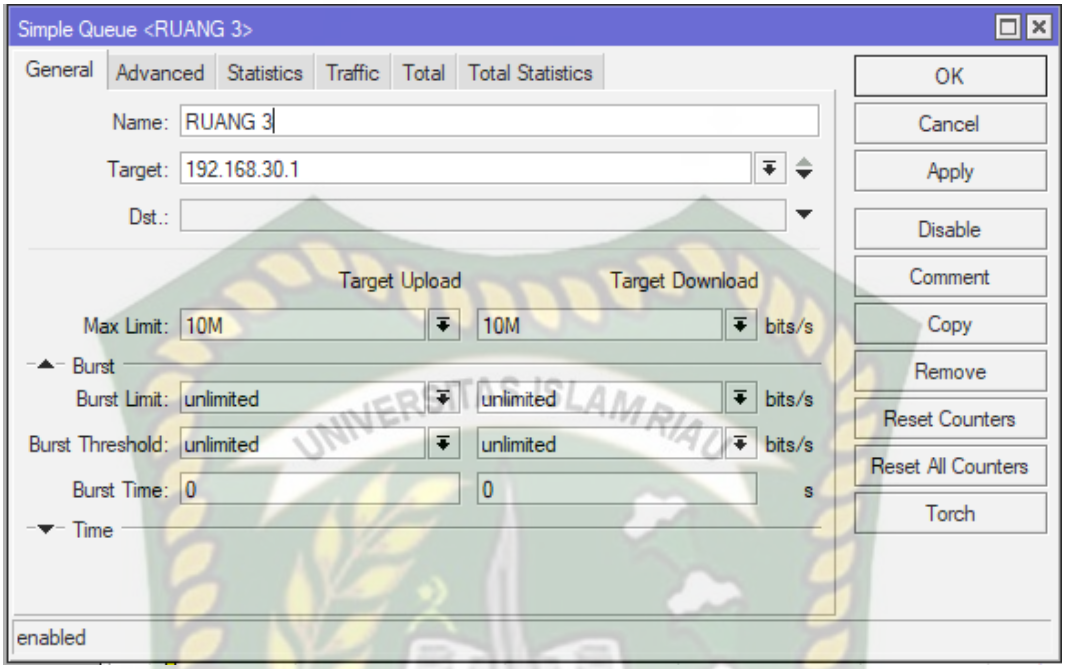
Dalam pengembangan sistem yang sedang berjalan ini digunakan metode simple queue hal ini digunakan untuk memanajemen bandwidth yang tersedia secara efektif dan efisien, dapat dilihat pada gambar 4.15 – 4.19.



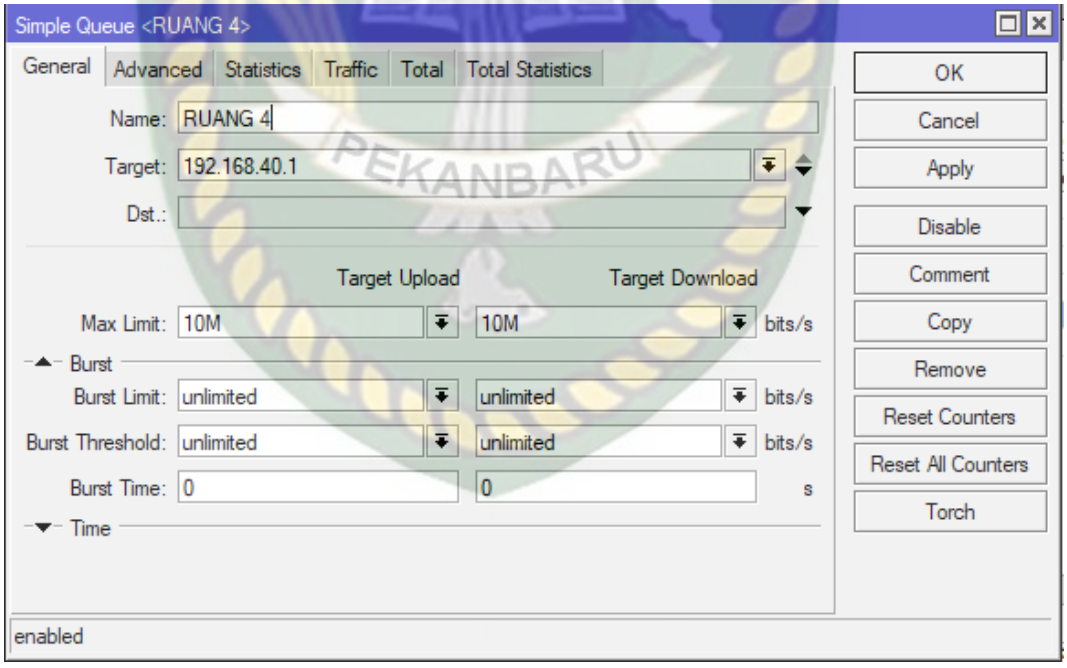
Gambar 4.15 Ruang 1



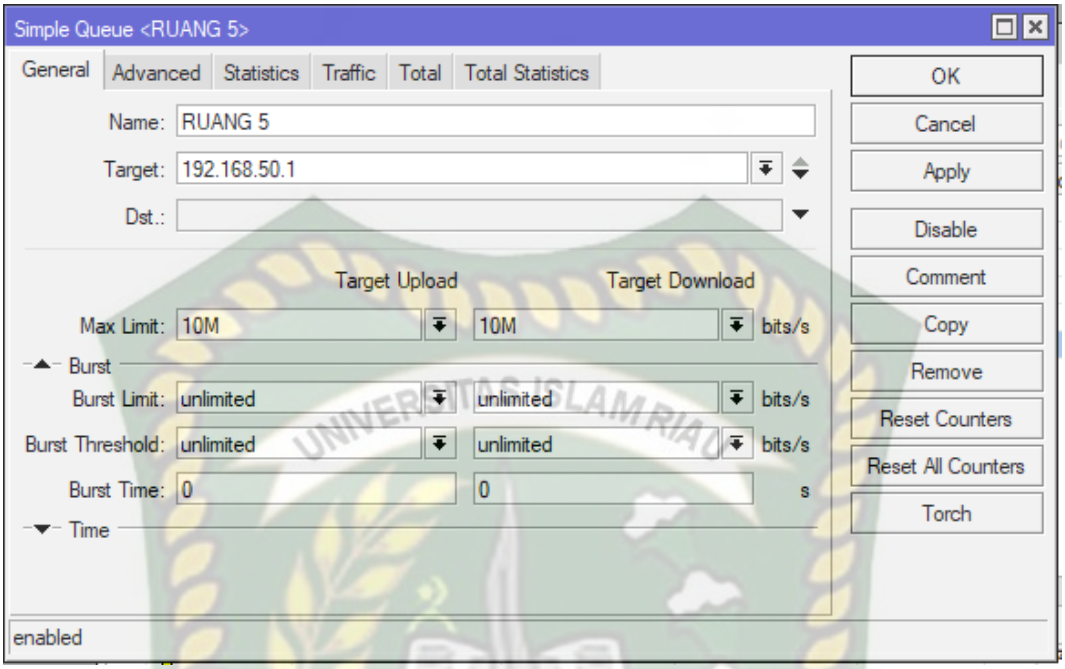
Gambar 4.16 Ruang 2



Gambar 4.17 Ruang 3



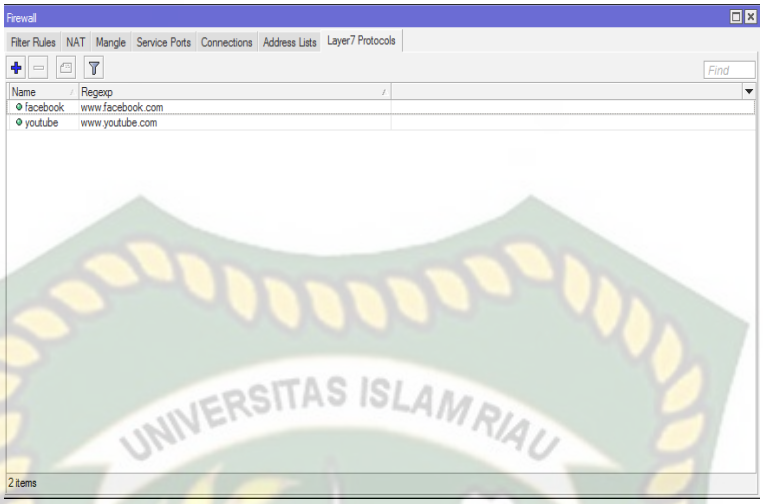
Gambar 4.18 Ruang 4



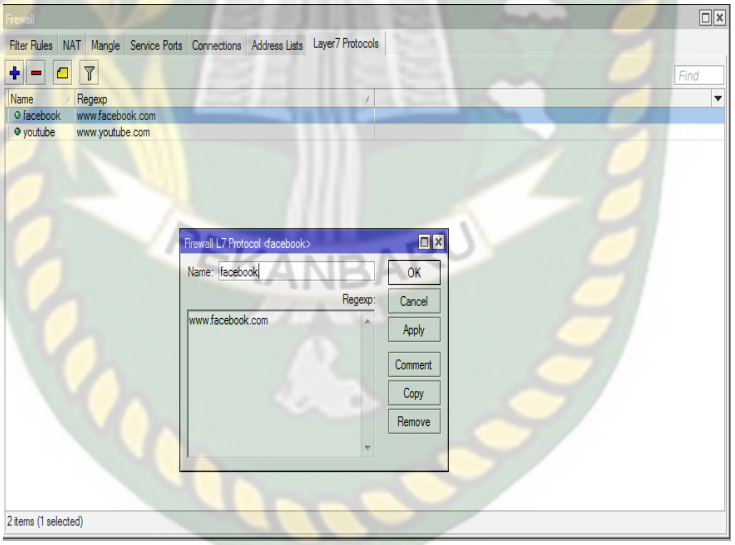
Gambar 4.19 Ruang 5

4.1.4 Implementasi Situs Diblokir

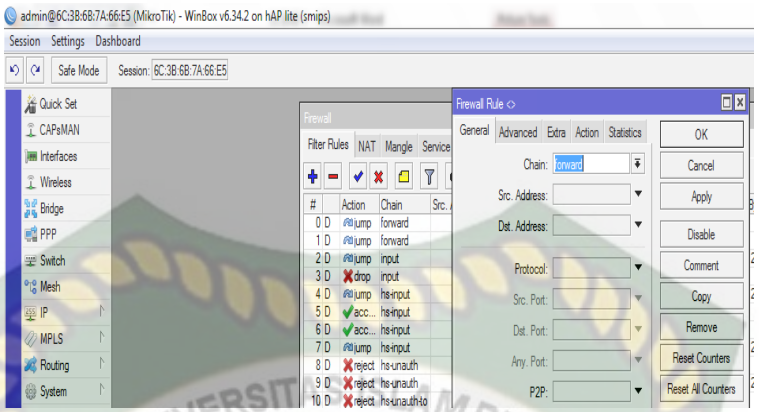
Ini adalah tampilan menu daftar situs yang diblokir, jika ada penambahan situs yang akan diblokir maka disinilah tempat pemblokiran situs, sehingga pengguna tidak bisa mengakses situs yang dilarang, berikut ini adalah tampilan-tampilan pemblokiran situs, dapat dilihat pada gambar 4.20 – 4.24.



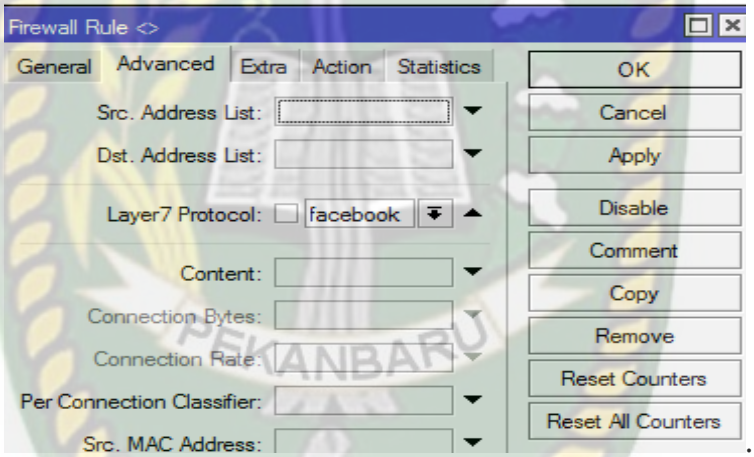
Gambar 4.20 *Setting Firewall*



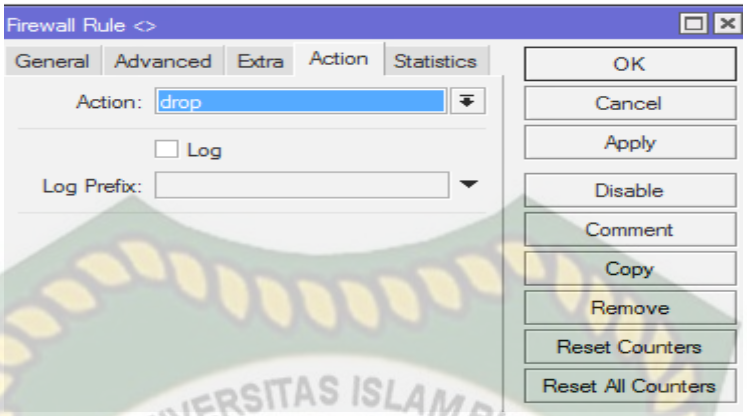
Gambar 4.21 *Layer 7 Protocol*



Gambar 4.22 *Filter Rule Tab General*



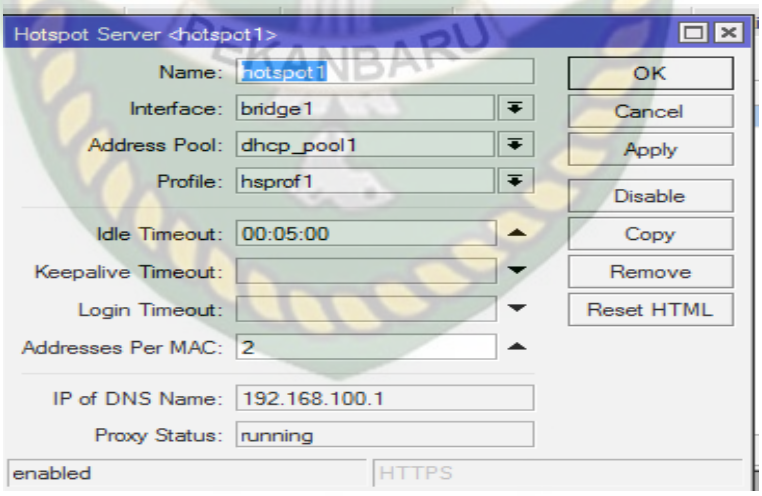
Gambar 4.23 *Firewall Rule Tab Advance*



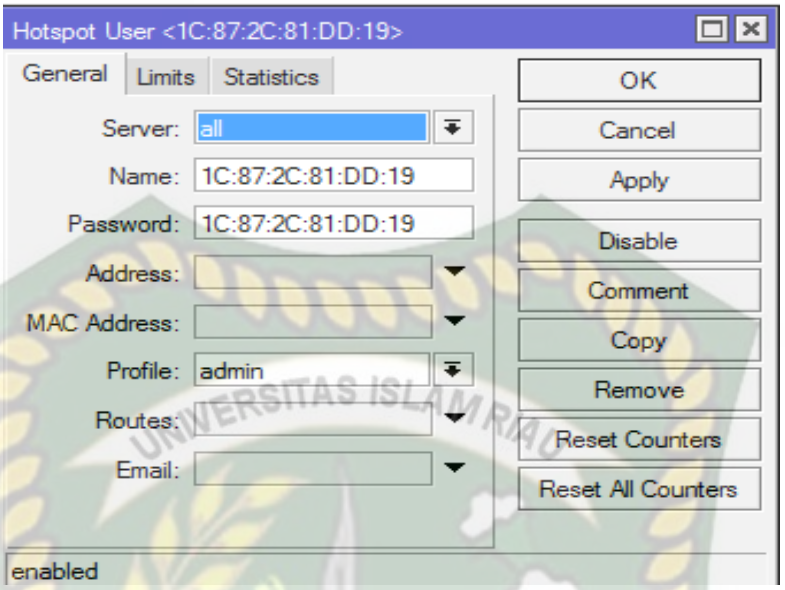
Gambar 4.24 *Firewall Rule Tab Action*

4.1.5 Implementasi *Radius MAC Authentication*

Berikut ini adalah tampilan penambahan pengguna atau juga pendaftaran, sehingga pengguna yang sudah terdaftar bisa langsung mengakses internet tanpa melakukan *login hotspot*, jika pengguna belum mendaftar maka pegguna tidak bisa mengakses internet. Dapat dilihat pada gambar 4.25 dan 4.26 sebagai berikut.



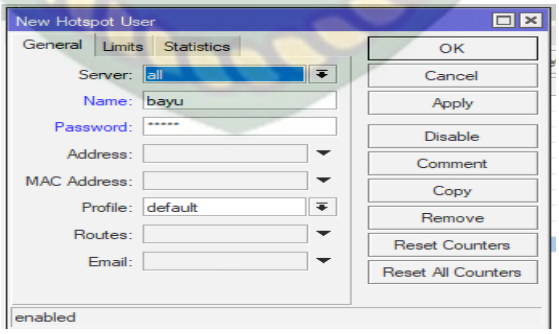
Gambar 4.25 *Setting IP Server*



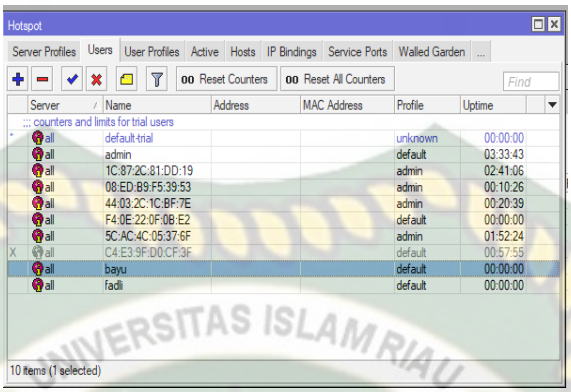
Gambar 4.26 *MAC Authentication*

4.1.6 Implementasi Akun *Login*

Berikut ini adalah tampilan penambahan pengguna yang menggunakan akun login, sehingga pengguna yang sudah terdaftar bisa langsung mengakses internet jika melakukan login yang sudah didaftar, jika pengguna belum mendaftar maka pegguna tidak bisa mengakses internet. Dapat dilihat pada gambar 4.27 dan 4.28 sebagai berikut.



Gambar 4.27 Pendaftaran Akun



Gambar 4.28 Akun Yang Sudah Terdaftar

4.2 Pengujian Sistem

Pengujian adalah bagian penting dalam membangun keamanan jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis, pengujian dilakukan untuk menjamin kualitas dan juga mengetahui kelemahan dari perangkat keamanan jaringan, tujuan dalam memiliki kualitas yang baik sesuai dengan analisis dan perancangan sistem serta konfigurasi pada sistem yang dibangun tersebut sehingga sistem tersebut berfungsi sesuai kegunaannya.

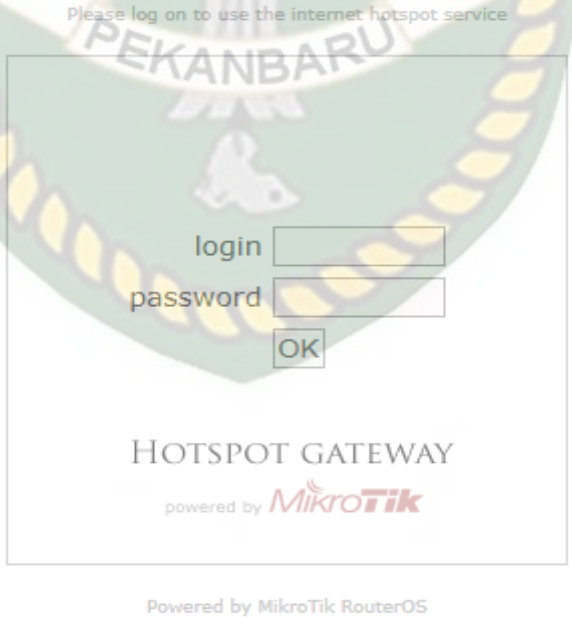
4.2.1 Hasil Pengujian *MAC Address* Sudah Terdaftar

Hasil pengujian setelah *MAC Address* pengguna di *Server* oleh *Administrator*, maka akan langsung keluar tampilan salah satu *website* yaitu *google*, dan dimanapun pengguna bepindah tempat dalam satu area maka tidak perlu menghubugkan ke jaringan disekitarnya untuk dapat mengakses internet. Seperti pada gambar 4.29.

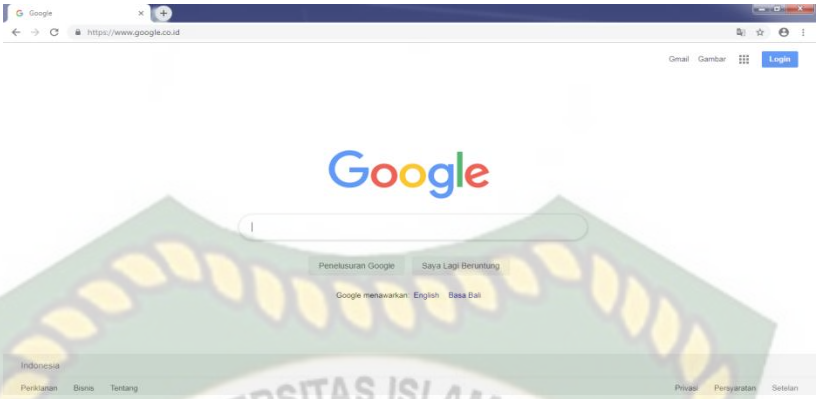
Gambar 4.29 Hasil setelah MAC Address sudah terdaftar

4.2.2 Hasil Pengujian Login Akun

Hasil pengujian setelah akun login yang sudah mendaftar pengguna di *Server* oleh *Administrator*, maka akan langsung keluar tampilan login di browser pengguna, dimanapun pengguna diminta untuk masuk username dan password.



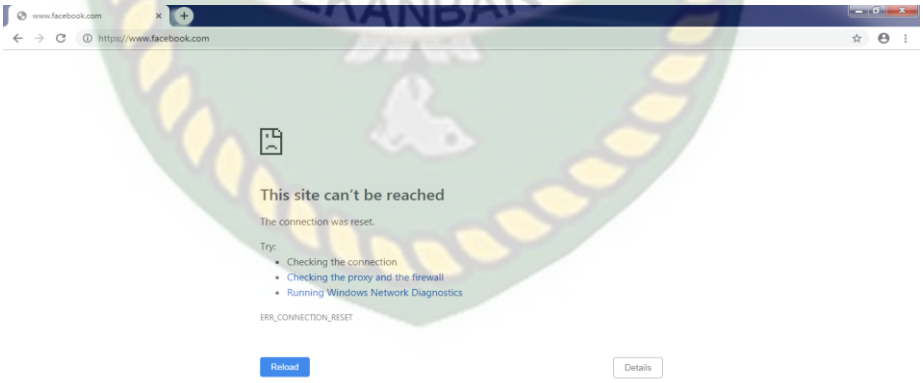
Gambar 4.30 Login Akun Pengguna



Gambar 4.31 Hasil Setelah Login

4.2.3 Hasil Pengujian Pemblokiran Situs

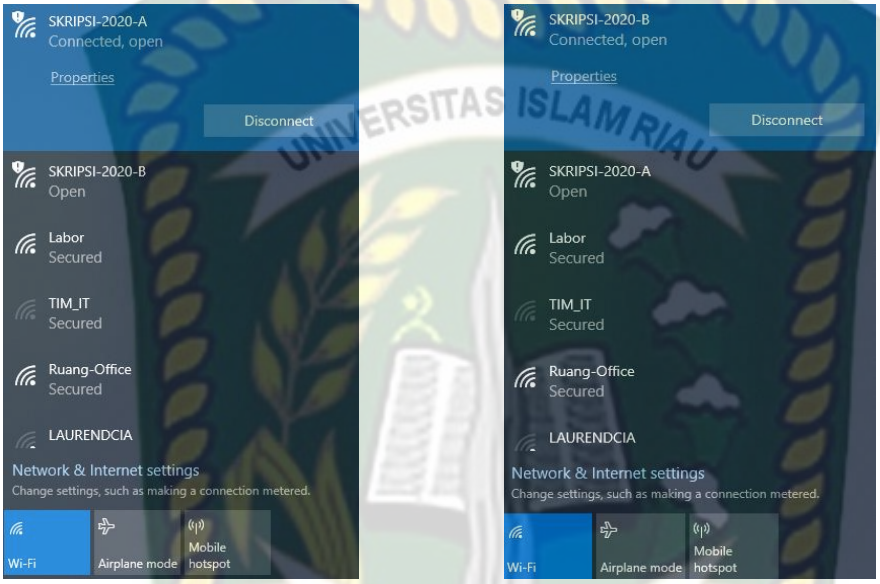
Hasil pengujian pada keamanan jaringan menggunakan *Radius MAC Authentication* didapatkan bahwa bagi pengguna yang ingin membuka situs *www.facebook.com* maka situs itu tidak akan terbuka Unlimited. Seperti pada gambar 4.32.



Gambar 4.32 Pengujian Sistem Mac Address

4.2.4 Pengujian Perpindahan *Hotspot*

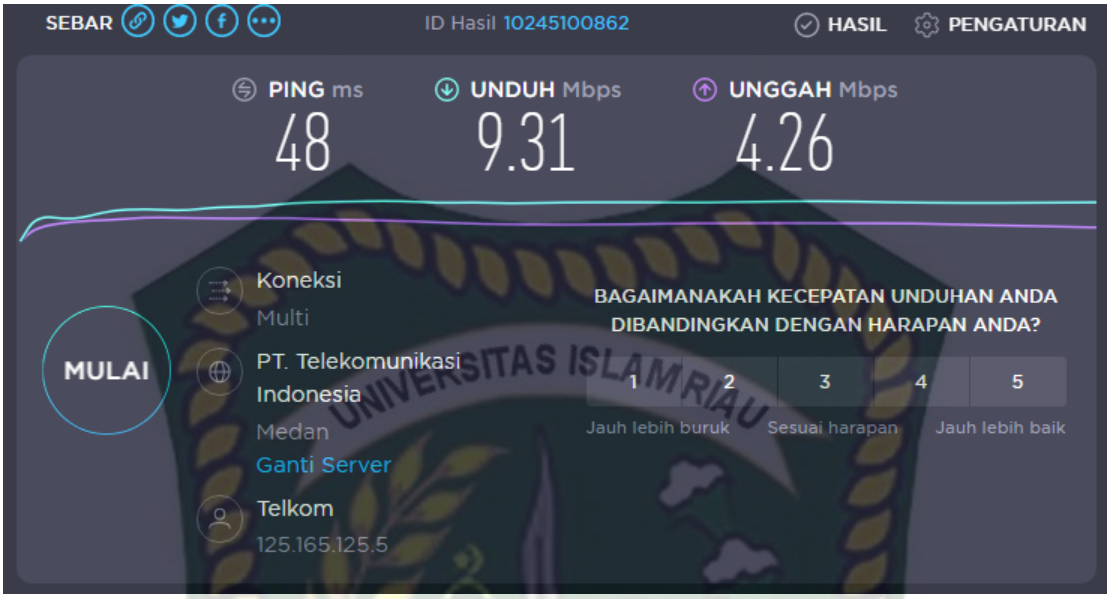
Pada hasil pengujian menggunakan sistem Radius MAC Authentication hasil pengujian menujukkan perpindahan dari *hotspot* yang satu ke yang satunya dapat dilihat pada gambar 4.33



Gambar 4.33 Perpindahan Hotspot

4.2.5 Pengujian Kecepatan Bandwidth

Pada hasil pengujian menggunakan sistem manajemen bandwidth pada setiap ruangan Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis dapat dilihat pada gambar 4.34



Gambar 4.34 Kecepatan Bandwidth

Mengetahui hasil dari *speedtest* tersebut maka penulis merumuskan sebagai berikut :

a. *Ping*

Ping merupakan hasil dari pengujian pada jaringan pada *frequensi* 2,4 Ghz dimana *ping* tersebut di terjemahkan sebagai jeda waktu, nilai yang muncul pada *ping* di tes kecepatan internet di atas artinya jumlah jeda waktu yang dibutuhkan jaringan 48 ms 48sec, atau proses yang kita gunakan untuk memindahkan data secepat 48 *miliseconds*. Biasanya, nilai *ping* tidak disajikan dalam mbps, namun *48 ms 48 seconds*

b. *Download*

Download merupakan kecepatan koneksi internet yang kita gunakan dalam mengunduh data. Pengujian saat menggunakan jaringan Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis 2,4 Ghz.

Bahwa rata-rata di angka 9,31 Mbps jika di rumuskan angka 9,31 masuk di kategori rumus 1 – 10 mbps menunjukan kecepatan ini kita bisa melakukan *video streaming* dengan kualitas baik.

c. *Upload*

Upload merupakan kecepatan yang kita butuhkan untuk mengunggah data ke internet. Pengujian saat menggunakan jaringan Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis. Bahwa rata-rata angka upload berada pada 4,26 Mbps jika di rumuskan angka 4,26 masuk di kategori rumus 10 mbps menunjukan kecepatan koneksi lebih baik digunakan *upload* melalui *website*.

4.2.6 Pengujian

Berikut ini table yang mengambarkan metode pengujian *black-box* pada keamanan jaringan di Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis.

Tabel 4.2 Metode Pengujian *Blackbox*

Interface	Test Case	Input	Output	Kesimpulan
Tampilan Mac Address Terdaftar	Gambar 5.24	Username : 5C:AC:4C:05:37:6F Password : 5C:AC:4C:05:37:6F	Login Menggunakan MAC Address	Valid
		Username : 1C:87:2C:81:DD:19 Password : 1C:87:2C:81:DD:19		Valid
Form Login Menggunakan Akun	Gambar 5.25	Username : bayu Password : 12345	Login Menggunakan Akun	Valid
		Username : fadli Password : 12345		Valid
Tampilan Pemblokiran Situs	Gambar 5.26	Situs Yang DiBlokir	Situs Tidak Dapat Dikunjungi	Valid
Tampilan Perpindahan Hotspot	Gambar 5.27	Hotspot Yang Tersedia	Berpindah Hotspot	Valid

BAB V

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan pengujian yang dilakukan Analisa Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis dapat disimpulkan sebagai berikut:

1. Apabila pengguna yang telah mendaftarkan *MAC address*nya ke *administrator* maka pengguna bisa mengakses internet yang terhubung ke *wireless* di satu area.
2. Apabila wireless yang satunya mati maka akan langsung terhubung ke wireless dua tanpa menggunakan login ulang.
3. Dengan adanya *wireless security* menggunakan *radius media access control authentication,* pengguna tidak berulang-ulang untuk login mengakses internet.
4. Dengan adanya *wireless security* menggunakan *radius media access control authentication,* dapat mengoptimalkan jaringan wireless.
5. Dengan adanya *wireless security* menggunakan *radius media access control authentication,* membatasi situs yang tidak diinginkan terbuka.

6.2 Saran

Dengan segala keterbatasan tentang Analisa Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis yang masih sangat sederhana terutama dalam performa kerja.

Saran terhadap tahap pengembangan sistem keamanan jaringan ini kedepannya agar lebih baik lagi yaitu :

Untuk kedepannya diharapkan mengembangkan lagi ke tahap yang lebih sempurna dengan menggunakan *Radius MAC Authentication* yang lebih mengandalkan keamanannya sampai ke tahap apabila ada pengguna yang membuka situs atau mencoba *hacking* akan terdeteksi oleh administrator.

DAFTAR PUSTAKA

Alfurqon,D.,Assegaff,S, 2018, Analisa Perancangan Jaringan Local Area Network Pada Laboratorium SMK Negeri 1 Kota Jambi, Jurnal Manajemen Sistem Informasi, Vol 3, No 3, ISSN: 2528-0082.

Basten, 2019, Analisa Manejemen Hotspot dengan Captive Portal, *Skripsi*, Program Pasca Sarjana Universitas Negeri Semarang, Unpublished

Jonathan, 2012, Manejemen Jaringan Wireless Menggunakan server Radius, Vol. 20 Nomor 1, ISSN 0853 – 6732

Kunang,Y.S., Ibadi,T., dan Suryayusa, 2018, Celah Keamanan Sistem Autentikasi wireless Berbasis RADIUS, *Seminar Nasional Aplikasi Teknologi Informasi* (SNATI 2013), Yogyakarta, hal. M-34 – M-40, ISSN:

Muttaqin,A.H., Rochim,A.F., dan Widianto,E.D., 2016, Sistem Outentikasi Hotspot Menggunakan LDAP Dan Radius Pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer, *Jurnal Teknologi dan Sistem Komputer*, Vol. 4 Nomor 2, hal Jtsiskom 282 – 288, E-ISSN:2338-0304

Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), *Bianglala Informatika*,Vol. 2 No 2, Hal. 112-119

Purwanto,D., dan Dana,RD., 2015, Sistem Keamana Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebone, *Jurnal Online ICT STMIK IKM*, Vol. 13 Nomor 1

Riyasa,S., Mulyadi,A., dan Purwanto,Y., 2018, Analisa Dan Implementasi Sistem Redundasi Hot Standby Network Security Menggunakan Metode Intrusion Prevention System (IPS) Dan Captive Portal Pada Jaringan Nirkabel, *Jurnal Teknik Komputer*, No. 1 Vol.10

Setiawan,H, 2018, Rancangan Bangun Captive Portal Untuk Jaringan Wireless Berbasi open Source pada CV. Gempar production Palembang, *Jurnal Teknologi Informasi*, Vol. 7 No. 1, Hal. 36-44.

Sumarianta, 2011, Instalasi dan Konfigurasi Jaringan Komputer, Pustaka Setia, Bandung

Suprianto,A., Riadi,I., 2013, Rancang Bangun Sistem Hotspot Menggunakan Captive Portal, *Jurnal Sarjana Teknik Informatika*, Vol. 1 Nomor 1, hal 172-180, E-ISSN: 2338-5197

Wijaya,I.H., 2015, Analisis Dan Implementasi Proxy Server Sebagai Web Caching, Blocking Situs, Dan Monitoring Menggunakan Centos 6 Di Smkn Ganesha Tama Boyolali, *Jurnal Teknologi Informasi & Pendidikan*, Vol. 3 No 1