ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN WIRELESS PADA PT.ARTHA UTAMA PLASINDO

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

SARJANA KOMPUTER

Program Studi Teknik Informatika

OLEH :

NAMA : LENNI NALURITA SINAGA

NIM : 011401503125016

FAKULTAS TEKNIK
UNIVERSITAS SATYA NEGARA INDONESIA
BEKASI
2019

ANALYSIS AND IMPLEMENTATION OF WIRELESS NETWORK SECURITY AT PT.ARTHA UTAMA PLASINDO

ESSAY

Submitted as One of the Requirements for Obtaining a Degree
BACHELOR OF COMPUTER SCIENCE

Informatics Engineering Study Program

BY:

NAME : LENNI NALURITA SINAGA

NIM : 011401503125016

THE FACULTY OF ENGINEERING
UNIVERSITAS SATYA NEGARA INDONESIA
BEKASI
2019

SURAT PERNYATAAN KARYA SENDIRI

Yang bertandatangan dibaawah ini :

Nama	: Lenni Nalurita Sinaga
NIM	: 011401503125016
Program Studi	: TEKNIK INFORMATIKA

Menyatakan bahwa Skripsi/Tugas Akhir ini adalah murni hasil karya sendiri dan seluruh isi Skripsi/Tugas Akhir menjadi tanggung jawab saya sendiri. Apabila saya mengutip dari karya orang lain maka saya mencantumkan sumber sesuai dengan ketentuan yang berlaku. Saya bersedia dikenai sanksi pembatalan Skripsi/Tugas Akhir ini apabila terbukti melakukan tindakan plagiat(Penjiplakan).

Demikian pernyataan ini saya buat dengan sebenarnya.

Bekasi, 23 Agustus 2019

(**Lenni Nalurita Sinaga**)
011401503125016

LEMBAR PENGESAHAN SKRIPSI/TUGAS AKHIR

NAMA : LENNI NALURITA SINAGA

NIM : 011401503125016

KONSENTRASI : JARINGAN

JUDUL SKRIPSI :"ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN WIRELESS PADA PT.ARTHA UTAMA PLASINDO"

TANGGAL : 23 AGUSTUS 2019

Bekasi, 23 Agustus 2019

Dosen Pembimbing II

(Erick Orlando, S.Kom.,MMSI)

Dosen Pembimbing I

(Hernalom Sitorus,ST,M.Kom)

Dekan

(Ir. Nurhayati, M.Si)

Ketua Program Studi

(Istiqomah Sumadikarta, ST.,M.kom)

LEMBAR PENGESAHAN PENGUJI

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN WIRELESS PADA PT.ARTHA UTAMA PLASINDO

OLEH :

NAMA : LENNI NALURITA SINAGA

NIM : 011401503125016

Telah dipertimbangkan didepan Penguji pada tanggal 23 Agustus 2019

Dan dinyatakan telah memenuhi syarat untuk diterima

Ketua Penguji / Pembimbing I

(Hernalom Sitorus ST.,M.Kom)

Anggota Penguji

(Istiqomah Sumadikarta,ST.,M.Kom)

Anggota Penguji

(Abdul Kholiq S.Kom.,M.Kom)

KATA PENGANTAR

Puji syukur penulis panjatkat kepada Tuhan Yang Maha Esa, karena telah melanjcarkan segala sesuatunya yaitu penulisan skripsi yang berjudul "Analisis Dan Implementasi Keamanan Jaringan Wireless Menggunakan User/Password Dan Mac Address Filter".

Untuk memenuhi syarat menyelesaikan Pendidikan Strata satu (S1) pada program Studi Teknik Informatika. Pada kesempatan yang baik ini, tak lupa penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dan penulisan skripsi ini, terutama kepada :

1. Ibu Dra. Merry L. Panjaitan, MM.,MBA Selaku Rektor Universitas Satya Negara Indonesia.
2. Ibu Ir. Nurhayati.M.Si . Selaku Dekan Fakultas Teknik Universitas Satya Negara Indonesia.
3. Bapak Istiqomah Sumadikarta,ST.,M.Kom. Selaku Kepala Jurusan Teknik Informatika.
4. Bapak Hernalom Sitorus, ST,.M.Kom. Selaku Dosen Pembimbing 1 yang telah memberikan bimbingan dan pengarahan pada penulisan skripsi ini.
5. Bapak Eric Erlando,S.Kom.,M.Kom. Selaku Dosen Pembimbing II yang telah memberikan bimbingan dan pengarahan pada penulisan skripsi ini.

6. Bapak Ridwan . Selaku Pembimbing di PT. Artha Utama Plasindo yang telah memberikan bimbingan dan pengarahan pada penulisan skripsi ini.
7. Seluruh Dosen Fakultas Teknik Informatika Universitas Satya Negara Indonesia yang telah memberikan Ilmu Pengetahuan dan Bimbingannya.
8. Keluarga yang telah memberikan dukungan moril,materil,sehingga tersusunnya skripsi ini dengan baik.
9. Seluruh teman teman yang telah memberikan Dungan dan saran dalam proses penyusunan skripsi ini.

Dalam proposal skripsi ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasannya pengetahuan dari penulisan skripsi ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun demi kesempurnaan dimasa yang akan dating.

Bekasi, 23 Agustus 2019

Penulis

Lenni Nalurita Sinaga

ABSTRAK

PT.Artha Utama Plasindo menerapkan *WLAN(Wireless Local Area Network)* pada kantornya karena keunggulannya dalam hal *portabilitas* dan *fleksibilitas* untuk mendukung kinerja perusahaan. *Wireless* merupakan jaringan tanpa kabel atau sering disebut dengan istilah nirkabel, yang memiliki banyak keuntungan dibandingkan menggunakan kabel. Banyak organisasi dan perusahaan menyediakan layanan hotspot untuk anggota atau karyawannya tetapi karena sistem keamanan yang tidak ada sehingga banyak orang walaupun bukan karyawan tetapi tetap bisa terkoneksi dengan layanan *wireless* secara bebas. Tentu hal ini sangat merugikan pihak organisasi maupun perusahaan. Dalam penelitian dilakukan implementasi keamanan Jaringan pada *hotspot* dengan menggunakan otentikasi *User/Password dan Mac Address Filter*. Karena dengan menggunakan dua otentikasi ini maka jika ada seseorang yang ingin mengakses ke hotspot harus memiliki *User/Password* dan mendaftarkan *Mac Address* perangkatnya ke *Administrato*r, maka dengan begitu client baru dapat menggunakan layanan *hotspot*.

Kata Kunci : *Wireless, User/Password, Mac Address Filter*

ABSTRACT

PT.Artha Utama Plasindo applies WLAN (Wireless Local Area Network) to its office because of its superiority in terms of portability and support to support the improvement of the company. Wireless is a wireless network or often referred to as wireless, which has many benefits compared to using cable. Many organizations and companies provide hotspot services for their members or employees but because the security system does not have many people but not employees but can still be connected to free wireless services. Of course this is very detrimental to the organization or company. In a study conducted Network security implementation on a hotspot using User / Password approval and Mac Address Filter. Because by using these two agreements, someone who wants to access the hotspot must have a User / Password and approve the Mac Address of the device to the Administrator, so that the new client can use the hotspot service.

Keywords: Wireless, User / Password, Mac Address Filter

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

A. Latar Belakang

Wireless merupakan jaringan tanpa kabel atau yang sering dikenal dengan istilah *Wi-Fi* (*Wireless Fidelity*), merupakan sebuah jaringan lokal yang menggunakan teknologi gelombang radio untuk pertukaran data. Tentu teknologi WLAN ini menjadi daya tarik tersendiri bagi pengguna komputer dalam mengakses jaringan komputer atau internet karena menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Pengguna bisa dengan mudah berpindah-pindah duduk tanpa harus terikat dengan tersedia atau tidaknya kabel.

PT. Artha Utama Plasindo merupakan perusahaan yang bergerak di bidang molding plastik, perusahaan ini sudah menerapkan Jaringan *wireless* sebagai penunjang untuk meningkatkan dan membantu segala aktivitas kinerja di perusahaannya contohnya seperti mengolah data, sharing resource maupun mencari informasi penting lainya. Keamanan jaringan WLAN sebagai bagian dari sebuah sistem sangat penting untuk menjaga validasi dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Jaringan WLAN di PT. Artha Utama Plasindo masih bersifat terbuka, siapa saja bisa masuk ke jaringan WLAN selagi berada pada jangkauan akses internet di area tersebut, tanpa memiliki keamanan khusus. Hal ini sangat di khawatirkan adanya celah keamanan yang

bisa di manfaatkan oleh pihak yang tidak bertanggung jawab untuk mencuri data maupun pengaksesan jaringan secara bebas.

Berdasarkan penjelasan di atas, sehingga peneliti memberi solusi kepada PT.Artha Utama Plasindo untuk memberikan keamanan pada jaringan wireless yang ada di perusahaannya dengan memanfaatkan 2 otentikasi User(Password) dan Mac Address Filter guna untuk melindungi jaringan Wireless dan membatasi hak akses jaringan wireless pada PT.Artha Utama Plasindo. Maka peneliti mengambil judul **"Analisis dan Impementasi keamanan Jaringan *Wireless* Pada PT.Artha Utama Plasindo"**.

B. Rumusan Masalah

Berdasarkan uraian di atas maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana menganalisis dan mengimplementasikan keamanan jaringan wireless Pada PT.Artha Utama Plasindo ?

C. Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari rumusan masalah yang ada, maka batasan masalah dari penelitian, yaitu:

1. Melakukan perbandingan antara Wi-Fi (*Wireless Fidelity*) yang tanpa otentikasi dengan WLAN yang menggunakan 2 otentikasi User(*password)* dan *Mac Address Filter*.

2. Melakukan Pengujian dan identifikasi terhadap 2 otentikasi yang di bangun.

D. Tujuan dan Manfaat Penelitian

D.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk menganalisis dan Implementasi keamanan jaringan WirelessLAN di PT. Artha Utama Plasindo dengan menggunakan dua otentikasi keamanan yaitu dengan *User(password)* dan *Mac address filter*.

D.2. Manfaat penelitian

Adapun manfaat dari penelitian ini yaitu:

1. Agar Jaringan Wireless LAN yang ada di PT. Artha Utama Plasindo ter- struktur dengan baik.
2. Memberikan pengamanan jaringan *wireless* pada PT. Artha Utama Plasindo, guna untuk membatasi hak akses jaringan *wireless* dengan memanfaatkan otentikasi *User(password)* dan *Mac address filter*.

E. Sistematika Penulisan

Sistematika penulisan menjelaskan mengenai uraian secara singkat isi dari setiap bab dalam penelitian.

Sistematika penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini memberikan gambaran secara jelas mengenai latar belakang penelitian, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penelitian.

BAB II LANDASAN TEORI

Bab ini menyajikan uraian tentang teori-teori dan konsep-konsep yang relevan dengan masalah yang diteliti serta dapat digunakan sebagai acuan dalam menganalisis masalah.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai waktu dan tempat penelitian, sejarah perusahaan atau organisasi tempat melakukan penelitian, visi dan misi, struktur organisasi serta metode yang dilakukan untuk menyelesaikan permasalahan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil penelitian berupa implementasi sistem dan pembahasan hasil penelitian yang menjawab permasalahan pada bab 1.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran penelitian sebagai masukan terhadap apa yang telah disajikan pada skripsi.

DAFTAR PUSTAKA

LAMPIRAN – LAMPIRAN

BAB II

LANDASAN TEORI

A. Tinjauan Pustaka

Untuk menunjang penelitian ini dibuatkan tinjauan pustaka dari karya-karya ilmiah yang berhubungan dengan penelitian ini yang sudah pernah dibuat sebelumnya.

Adapun beberapa manfaat yang didapat dari tinjauan pustaka adalah sebagai berikut:

a) Mengungkapkan penelitian-penelitian yang serupa dengan penelitian yang akan dilakukan,

b) Membantu memberi gambaran tentang metode dan teknik yang dipakai dalam penelitian yang mempunyai permasalahan serupa atau mirip dengan penelitian yang dihadapi,

c) Mengungkapkan sumber-sumber data atau judul-judul pustaka yang berkaitan yang mungkin belum kita ketahui sebelumnya.

Berikut ini daftar tinjauan pustaka yang digunakan:

1. Jurnal " **MENGAMANKAN *WIRELESS* DENGAN MENGGUNAKAN *PASSWORD* DAN *MAC ADDRESS FILTERING***" Jurnal ini dibuat oleh 2 orang mahasiswa Manajemen Sistem Informasi Dan Teknologi, bernama **Didi Susianto**, **Iis Yulianti**, Jurnal yang dibuat oleh 2 orang mahasiswa ini berisi penelitian yang membahas tentang

keamanan jaringan, salah satunya dengan menggunakan cara *two factor, password dan filtering mac address*. Pada bagian kesimpulan ke 2 Mahasiswa ini menyimpulkan Two factor authentication dapat diterapkan untuk meningkatkan keamanan wifi, yaitu dengan dua tahapan otentikasi password, dan Mac address filtering.

2. Jurnal " **ANALISIS WIRELESS LOCAL AREA NETWORK (WLAN) DAN PERANCANGAN MAC ADDRESS FILTERING MENGGUNAKAN MIKROTIK**"

   Jurnal ini dibuat oleh 2 orang Mahasiswa Amik BSI dengan Program Studi Teknik Komputer, bernama **Kurani Mega Asteroid**, **Yayan Hendrian**, Jurnal yang dibuat oleh 2 orang mahasiswa ini berisi penelitian yang membahas tentang perancangan Mac Address Filter yang menggunakan perangkat Mikrotik, Pada bagian kesimpulan. 2 Mahasiswa ini menyimpulkan keberhasilan mereka atas penelitian dari implementasi yang mereka lakukan. 2 Mahasiswa ini menerapkan WPA2-PSK dan Mac Address Filter sebagai keamanan jaringan Wireless LAN di tempat penelitiannya sehingga keamanannya lebih terjamin.

3. Jurnal " **RANCANG BANGUN KEAMANAN JARINGAN WIRELESS PADA STIPER SRIWIGAMA PALEMBANG**" Jurnal ini dibuat oleh seorang Mahasiswa Universitas Bina Darma dengan Program Studi Teknik Komputer, bernama **Rahmat Novrianda**, Jurnal yang dibuat oleh seorang Mahasiswa Universitas Bina Darma ini berisi penelitian yang membahas tentang pembangunan keamanan jaringan

wireless menggunakan perangkat RouterBoard Mikrotik, Pada bagian kesimpulan. Mahasiswa ini menyimpulkan bawha keamanan yang dilakukan untuk jaringan Wireless pada Stiper Sriwigama Palembang adalah menggunakan *authentication User*, dengan adanya *authentication User*, maka setiap pengguna jaringan *wireless* di haruskan untuk melakukan login terlebih dahulu agar setiap user dapat mengakses jaringan *Wireless* pada Stiper Sriwigama Palembang.

B. Teori Dasar Umum

B.1. Sistem Jaringan Komputer

B.1.a. Pengertian Jaringan Komputer

Jaringan komputer adalah dua komputer atau lebih yang terhubung satu dengan yang lainnya. Perangkat yang dihubungkan tidak terbatas pada komputer saja, melainkan termasuk printer dan perangkat-perangkat keras yang lain. Sebagai penghubung, dapat digunakan kabel, misalnya gelombang radio dan sinar inframerah.

B.2. Skala Jaringan

B.2.a. Skala Jaringan

Pada dasarnya skala Jaringan ada 3 yaitu;

1. LAN (*Local Area Network*)

   Pada awalnya jaringan komputer dilakukan pada jaringan yang sangat terbatas yakni dengan menggunakan dua buah komputer. Kemudian

berkembang lebih luas pada komplek perkantoran, gedung, sekolah yang dikenal dengan Jaringan Lokal atau Local Area Network (LAN).

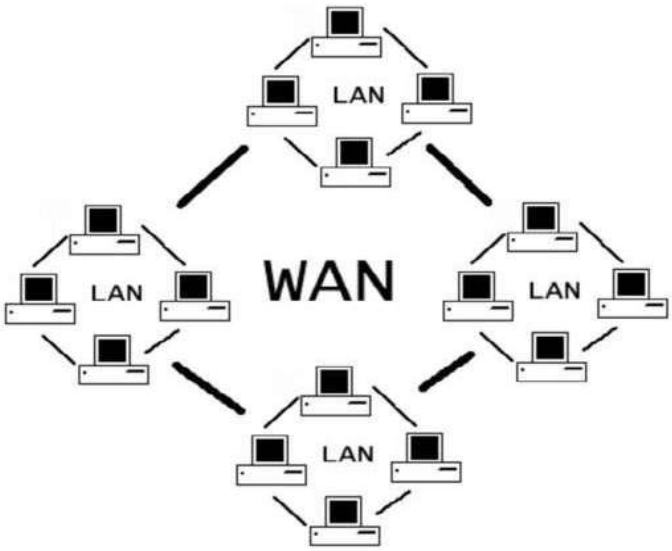
Gambar 2.1. jaringan LAN (Local Area Network)

Sumber : https://www.google.com.

2. WAN (Wide Area Network)

Perkembangan dan kebutuhan atas informasi dan komunikasi menuntut komputer yang digunakan dapat berhubungan secara luas sehingga terbentuk Metropolitan Area Network (MAN). Perkembangan kebutuhan yang lebih luas lagi diperlukan jaringan yang lebih luas juga sehingga digunakan Wide Area Network (WAN). Jadi, MAN dan WAN merupakan perpaduan antara LAN yang simultan.

Jaringan WAN dapat mencapai antarpulau, antarnegara, bahkan antarbenua. WAN biasanya menggunakan perangkat keras (hardware) dan perangkat lunak (software) tertentu sehingga tidak bisa menggunakan sembarang hardware dan software.



Gambar 2.2. Jaringan WAN

https://www.google.com/

3. Internet

Dari besarnya skala, internet sebenarnya sama dengan WAN, tetapi WAN bersifat privat, artinya hanya orang-orang tertentu yang dapat mengaksesnya, misalnya karyawan suatu perusahaan multinasional. Sebaliknya, Internet bersifat publik sehingga semua orang dapat mengakses jaringan tersebut.

Gambar 2.3. Internet.

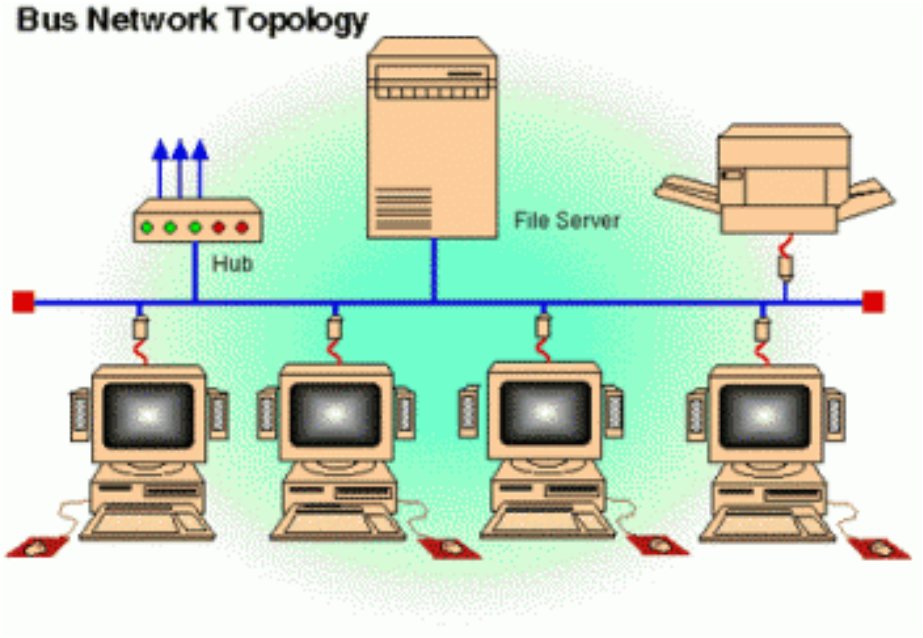
https://www.google.com/

B.3. Topologi Jaringan

B.3.a. Topologi Bus

Topologi bus diimplemenasikan dengan menggunakan media fisik berupa kabel koaksial. Topologi ini umumnya digunakan untuk jaringan komputer yang terhubung secara sederhana sehingga komputer-komputer yang terlibat di dalamnya bisa berkomunikasi satu sama lainnya. Realisasi dari topologi bus ini adalah adanya sebuah jalur utama yang menjadi penghubung antar komputer. Sebelum mengirim data, NIC (Network Interface Card) komputer pengirim akan melihat dahulu apakah jalur transmisi sedang sibuk atau tidak. Apabila jalur sedang sibuk (sedang digunakan oleh komputer lainnya), maka ia akan menunggu selama beberapa waktu yang acak sebelum mencoba mengirimkan data kembali. Data akan dikirimkan begitu ada indikasi bahwa jalur transmisi sedang digunakan.

Hal ini digunakan untuk menghindari terjadinya bentrokan atau tabrakan (*coliision*) pada transmisi data.



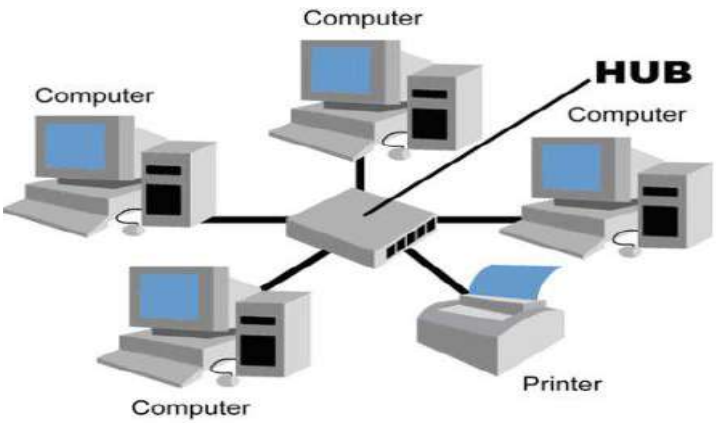
Gambar 2.4. Topologi Bus

Sumber : http://id.wikipedia.org/wiki/Topologi_bus

B.3.b. Topologi Bintang

Topologi ini didesain di mana setiap *node* (*file server, workstation* dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah *hub* atau konsentaror. Data yang terkirim ke jaringan akan melewati *hub*/konsentrator sebelum melanjutkan ke tempat tujuannya. Hub ataupun konsentrator akan mengatur dan mengendalikan keseluruhan fungsi jaringan. dia juga bertindak sebagai *repeater*/penguat aliran data. Konfigurasi pada jaringan model ini menggunakan

kabel *twisted pair*, dan dapet digunakan bersama kabel koaksial atau kabel *fiber optic*.



Gambar 2.5. Topologi bintang

Sumber : http://id.wikipedia.org/wiki/Topologi_bintang

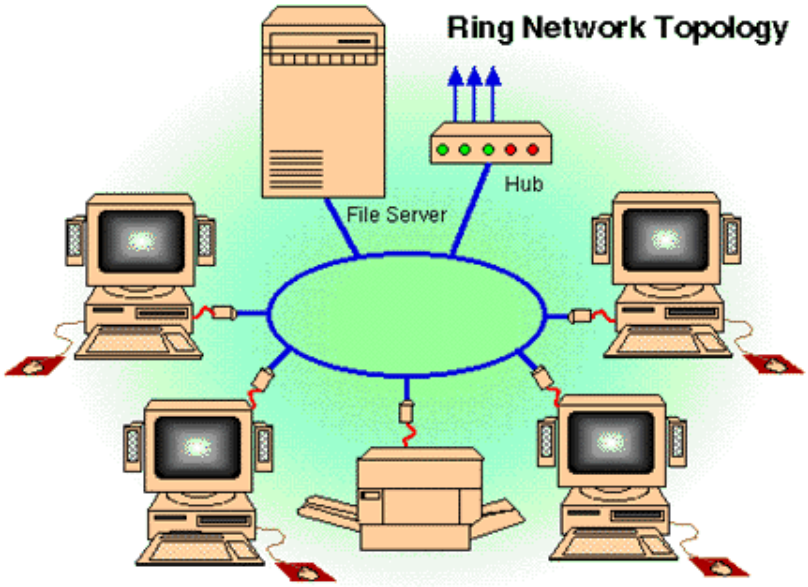
B.3.c. Topologi Ring/Cincin

Bentuk ini merupakan bus jaringan yang ujung-ujungnya dipertemukan kembali sehingga membentuk suatu lingkaran, setiap informasi yang diperoleh diperiksa alamatnya oleh terminal yang dilewati. Jika bukan untuknya, maka informasi akan dilewatkan sampai menemukan alamat yang benar. Pada topologi Ring, salah satu komputer pada jaringan ini berfungsi sebagai penghasil *token* . Token disini dapat dibayakan sebagai kendaraan yang berfungsi membawa data melalui media fisik. Token akan membawa data melalui jalur transmisi hingga menemukan tujuannya.

Sebuah token dapat berada dalam dua jenis keadaan yang berbeda, sedang digunakan, atau sedang bebas. Bila sebuah token berada dalam kondisi sedang

digunakan ini berarti token tersebut sedang membawa data. Ini berarti token tersebut sedang digunakan oleh salah satu komputer untuk mengirimkan datanya. Token yang sedang berada dalam keadaan ini akan berkeliling mencari komputer tujuannya. Selama tujuannnya belum ditemukan, token ini akan berada dalam keadaan tersebut.

Setelah token menemukan tujuannya, ia kan menyampaikan data yang dibawanya. Kemudian token tersebut akan berada dalam keadaan bebas.Ini berarti token tersebut bisa dibebani dengandata lagi, token tersebut siap untuk membawa data baru. Token yang bebas akan berkeliling lagi untuk menerima tugas untuuk membawa data baru. Keuntungan menggunakan topologi Ring ini adalah kemungkinan terjadinya bentrokan dalam transfer data ditiadakan. Kelemahan penggunaan topologi ini adalah harga implementasinya yang lebih mahal. Selain itu tingkat kesulitan untuk menjaga jaringan bertopologi Ring juga lebih susah. Karenanya bila ada kerusakan maka untuk memperbaikinya kemblai juga susah. Topologi Ring kurang begitu banyak diimplementasikan karena membutuhkan peralatan yang khusus.

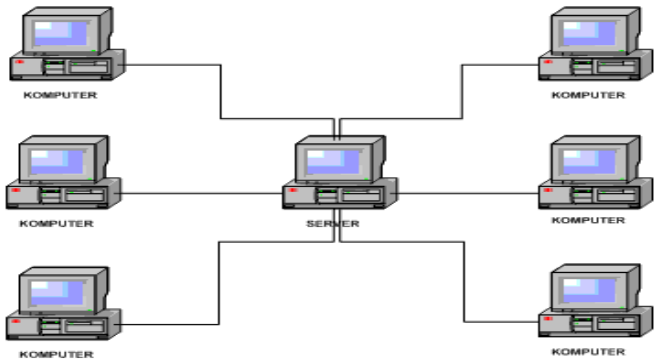


Gambar 2.6. Topologi Ring/Cincin

Sumber : http://id.wikipedia.org/wiki/Topologi_cincin

B.3.d. Topologi Mesh

Topologi ini juga disebut sebagai jaring, karena setiap komputer akan berhubungan pada tiap-tiap komputer yang tersambung. Topologi ini jarang sekali diterapkan dalam LAN karena alasan pemborosan kabel dan sulitnya instalasi, selain itu juga sulit mendeteksi keamanannya. Biasanya model ini diterapkan pada WAN atau internet sehingga disebut sebagai topologi Web. Keuntungannya bahwa kita bisa melakukan komunikasi data melalui banyak jalur, jika jalur satu terputus, maka kita bisa menggunakan jalur yang lain.

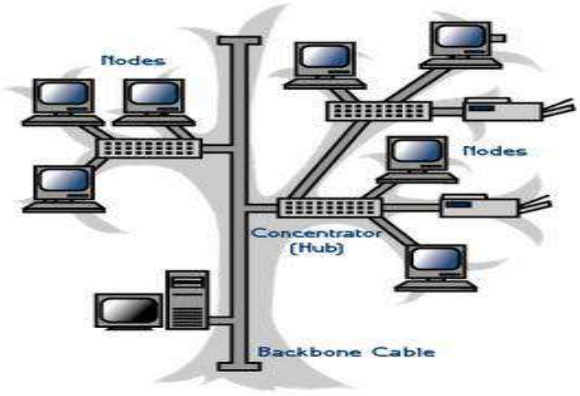


Gambar 2.7.. Topologi Mesh

Sumber : http://id.wikipedia.org/wiki/Topologi_mesh

B.3.e. Topologi Three

Topologi *three* merupakan perpaduan antara topologi Bus dan Star, yang terdiri dari kelompok-kelompok dari *workstation* konfigurasi bintang yang terkoneksi ke kabel utama yang menggunakan topologi Bus. Topologi ini memungkinkan untuk pengembangan jaringan yang telah ada, dan memungkinkan mengonfigurasi jaringan sesuai dengan kebutuhannya.



Gambar 2.8. Topologi Three

Sumber : http://id.wikipedia.org/wiki/Topologi_pohon

B.4. Hotspot Wi-Fi

B.4.a. Pengertian *Hotspot*

Pengertian ***Hotspot*** adalah lokasi fisik di mana orang dapat memperoleh akses Internet, biasanya menggunakan teknologi Wi-Fi, melalui jaringan area lokal nirkabel (*Wireless Local Area Network*, disingkat WLAN) menggunakan router yang terhubung ke penyedia layanan internet (*Internet Service Provider*, disingkat ISP).

Gambar 2.9. Hotspot

Sumber : https://int.search.myway.com/

B.4.b. Jenis-Jenis Hotspot

1. Free Hotspot

merupakan jenis hotspot dimana publik dapat mengakses jaringan dengan bebas. Fasilitas free hotspot biasanya disediakan sebagai fasilitas tambahan untuk pelanggan hotel, Cafe dan usaha-usaha lainnya. Free hotspot juga kadang dipasang semi permanen di acara pameren komputer atau konferensi/seminar komputer.

Pada kasus ini, admin sebagai orang yang mengontrol jaringan menonaktifkan persyaratan otentikasi (authentication requirements) dan membuka koneksi jaringan sehingga siapapun bisa mengakses jaringan tersebut.

2. Hotspot Berbayar

Hotspot berbayar maksudnya ialah gedung menyediakan Hotspot dan Hotspot tersebut tidak di berikan secara gratis,melainkan kita harus membaayar ke gedung yang memiliki hotspot tersebut supaya kita bisa menikmati Hotspot yang ada pada gedung tersebut.

B.5. IP Address

B.5.a. Pengertian IP Address

IP Address (alamat IP) adalah deretan bilangan yang digunakan sebagai media untuk mengidentifikasi setiap perangkat komputer yang terhubung pada jaringan komputer (intranet / internet). Alamat IP terbagi atas 2 bagian, yaitu Net ID dan Host ID. Contoh alamat IP : 192.168.2.10 secara default Net ID nya adalah 192.168.2 dan Host ID nya adalah 10. Agar komputer bisa saling terhubung, alamat IP yang digunakan Net ID nya harus sama, dan Host ID nya harus berbeda.

Untuk lebih mudah memahaminya, Kita anggap alamat IP adalah alamat rumah. Net ID adalah nama jalan dan Host ID adalah nomor rumah. Contoh alamat rumah : Jln. Diponegoro No. 3, jika nama jalan dari beberapa orang sama, maka nomor rumah mereka tidak mungkin sama.

B.5.b. Pembagian Kelas IP Address

Menurut *wikipedia bahasa indonesia*, IP address (alamat IP) dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E. Perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Penentuan kelas ini dilakukan dengan cara berikut :

1. Kelas A : digunakan untuk jaringan WAN, alamat IP-nya pada bagian pertama antara 0-127, dan yang merupakan Net ID nya yaitu 1 bagian yang pertama. Subnet Mask nya 255.0.0.0

   Contoh: 8.254.129.11.
2. Kelas B : biasanya digunakan untuk jaringan MAN, Ip address nya pada bagian pertama antara 128-191, dan yang merupakan network ID nya yaitu 2 bagian pertama. Subnet masknya 255.255.0.0

   Contoh: 128.255.129.7
3. Kelas C : biasanya digunakan untuk jaringan LAN, Ip address nya pada bagian pertama antara 192-223, dan yang merupakan network ID nya yaitu 3 bagian pertama. Subnet masknya 255.255.255.0

   Contoh: 192.168.1.10
4. Kelas D : biasanya digunakan untuk keperluan multicasting. IP address nya pada bagian pertama antara 224-247. Dalam multicasting tidak dikenal network ID dan host ID.
5. Kelas E : biasanya digunakan untuk keperluan umum. IP address nya pada bagian pertama antara 248-255

B.5.c. Fungsi IP Address

Berikut adalah fungsi dasar dari alamat IP, yaitu :

1. Fungsi IP Address yang pertama adalah sebagai alat identifikasi host ataupun antar muka jaringan komputer. Jika diilustrasikan seperti kehidupan nyata, maka IP Address berfungsi sebagai nama ataupun identitas seseorang. Seperti halnya nama, setiap komputer memiliki IP Address yang unik dan berbeda antara satu dengan yang lainnya.
2. Alamat Lokasi Jaringan

   Fungsi IP Address yang kedua adalah sebagai penunjuk alamat lokasi jaringan. Jika kita ilustrasikan kembali dalam kehidupan nyata, maka IP address dapat diilustrasikan sebagai penunjukkan alamat rumah tempat tinggal seseorang. IP Address akan menunjukkan lokasi keberadaan sebuah komputer. Seperti halnya dalam kehidupan nyata, ada rute / jalan yang harus ditempuh agar data yang diinginkan bisa sampai ke komputer yang ingin dituju.

C. Jenis – Jenis Ancaman Keamanan Jaringan

C.1. Packet Sniffer

Packet sniffer adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun nirkabel. Setelah paket paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan

karena pada dasarnya semua koneksi ethernet adalah koneksi yang bersifat broadcast, di mana semua host dalam 6 sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari packet sniffing yang merupakan metode pasif (pihak penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja).

C.2. IP Spoofing

IP Spoofing adalah sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan firewall dan menipu host penerima data. Hal ini dapat dilakukan karena pada dasarnya alamat IP asal sebuah paket dituliskan oleh sistem operasi host yang mengirimkan paket tersebut. Dengan melakukan raw-socket-programming, seseorang dapat menuliskan isi paket yang akan dikirimkan setiap bit-nya sehingga untuk melakukan pemalsuan data dapat dilakukan dengan mudah.

C.3. Hacker

Hacker dalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi lain.

D. Standar Wireless

Sejarah kemunculan wireless LAN(WLAN) dimulai pada tahun 1997, yaitu manakala IEEE(sebuah lembaga Independen) membuat spesifikasi/standar WLAN yang pertama yang diberi kode 802.11.

Standar komuniasi data yang yang digunakan umumnya adalah kluarga IEEE 802.11 Untuk mengetahui perbedaan masing-masing spesifikasi dan infomasi lebih detail, berikut beberapa di antaranya yaitu :

Spesifikasi	Keterangan
802.11	Spesifikasi WLAN yang pertama, dibuat pada tahun 1997. Kecepatan transfer data maksimal yang didapat di capai sebesar 2 Mps.
802.11a	Dibuat pada tahun 1999. Menggunakan frekuensi 5 GHz, Bandwidth 20 MHz,dan kecepatan Transfer data maksimal 54 Mbps.
802.11b	Dibuat pada tahun 1999. Menggunakan frekuensi 2,4 GHz, Bandwidth 22 MHz,dan kecepatan Transfer data maksimal 11 Mbps.
802.11g	Dibuat pada tahun 2003. Menggunakan frekuensi 2,4 GHz, Bandwidth 22 MHz,dan kecepatan Transfer data maksimal 54 Mbps.
802.11n	Dibuat pada tahun 2009. Menggunakan frekuensi 2,4 GHz dan 5 Ghz, dan kecepatan Transfer data maksimal 108 s/d 300 Mbps.

Tabel 3.1 Spesifikasi WI-FI

E. Teknik Keamanan Jaringan Wireless

E.1. Teknik Mengamankan Wireless

Ada beberapa teknik yang dapat digunakan untuk mengamankan *Wireless* yaitu dengan cara sebagai berikut *:*

1. Menyembunyikan SSID

Nama jaringan wireless disebut juga dengan Service Set Identifier (SSID). Secara default SSID dari Access Point akan di broadcast dan hal ini membuat user mudah untuk menemukan jaringan kita. Untuk menghindari adanya user yang tidak bertanggung jawab dalam menggunakan jaringan kita, maka dapat mematikan SSID yang ada pada Access Point agar hanya user yang mengetahui SSID yang terkoneksi.

2. MAC Filtering

Setiap Access Point atau router sudah dilengkapi fitur MAC Filtering. Dengan adanya ini kita dapat menentukan siapa saja yang dapat terkoneksi dengan jaringan kita, yaitu dengan membuat white list berdasarkan MAC. Apabila ada user dengan MAC yang tidak terdaftar maka user tersebut tidak akan diijinkan.

3. Captive Portal

Pada awalnya infra struktur Captive Portal hanya digunakan untuk keperluan komunitas. Captive portal merupakan router gateway yang melindungi atau tidak mengijinkan trafik hingga user melakukan otentikasi. User yang belum melakukan otentikasi (berbasis web) tidak akan mendapatkan akses internet kecuali ke captive portal tersebut.

4. Mengisolasi Wireless Network dari LAN

Untuk melindungi jaringan internal LAN dari ancaman yang berasal dari jaringan wireless, maka perlu diperluakan suatu perangkat perimeter jaringan atau membuat suatu zona DMZ untuk mengisolasi LAN tersebut. Apabila ada permintaan dari user yang menggunakan wireless ke jaringan internal LAN maka diperlukan otentikasi lagi, misalnya menggunakan RAS server atau menggunakan VPN.

5. Mengontrol Sinyal Wireless

Teknologi 802.11b WAP dapat memancarkan gelombang mencapai 300ft (sekitar 91.5 meter). Kemampuan pancaran ini bergantung pada antena yang digunakan. Directional antena akan memancarkan ker arah tertentu dan arah pancarannya tidak melingkar seperti omnidirectional yang biasanya di gunakan oleh Access Point pada umumnya. Dengan memilih antena yang tepat kita dapat mengontrol jarak sinyal dan arahnya untuk melindungi dari orang-orang yang tidak bertanggung jawab.

6. Password

Password adalah kumpulan karakter atau string yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (multiuser) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Kata sandi juga dapat diartikan sebagai kata rahasia yang digunakan sebagai pengenal. 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.

F. Pengenalan Mac Address

F.1. Mac Address

MAC Address (Media Access Control Address) dalah 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 48bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan.

F.2. Mac Address 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 gangguanseperti pencurian pc card dalam MAC filter dari suatu access point sniffing terhadap WLAN.

F.3. 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.

G. Mikrotik

G.1. Pengertian Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot.

G.2. Fitur – Fitur Mikrotik

Berikut Fitur-Fitur Dalam Mikrotik:

1. Address List : Pengelompokan IP Address berdasarkan nama
2. Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.

3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
4. **B**ridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.
6. DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
10. Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
11. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

H. Wireless Security

Untuk keperluan security, Mikrotik menyertakan fitur Enkripsi Standar yang dapat di lihat pada tabel. Masing-masing memiliki keunikan. Berikut daftar protokol wireless security yang di dukung.

Protokol	**Perbandingan**
WEP	• Menggunakan algoritma RC4 yang lemah • Menggunakan CRC32 untuk integritas • Network key bersifat statis • Umumnya telah di dukung oleh semua AP/Card/Driver
WPA	• Menggunakan PSK (Pre shared Key): algoritma RC4+ Temporal key (TKIP) • Menggunakan Radius : RC4+ Temporal key (TKIP) + 802.1x + better ICV (MIC) • Umumnya telah di dukung oleh semua AP/Card, namun butuh upgrade aplikasi, driver atau firmware
WPA2	• Menggunakan algoritma enkripsi AES dan TKIP • Umumnya telah di dukung oleh Hardware baru (Hardware keluaran 2003 atau yang lebih baru)
WPA-Personal	• Lazim disebut sebagai WPA_PSK, yang didisain untuk small home-offices

	• Tidak memerlukan Authentication server • Menggunakan Enkripsi 256-bit key PSK,dapat berupa Password atau passphrase
WPA- Etherprise	• Lazim disebut sebagai WPA-802.1X mode dan didisain untuk enterprise networks • Menggunakan otentikasi medel EAP • Memerlukan Radius authentication server • Lebih sulit diimplementasikan namun menyediakan fitur proteksi yang lebih baik (misal proteksi password dictionary attacks).

Tabel 3.2 Wireless Security

I. Kelemahan Dan Celah Keamanan *Wireless*

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang di gunakan.

Salah satu contoh yang menjadi penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga masih sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor seperti SSID,IP Address, remote managemen,

DHCP enable, kanal frekuensi, tanpa enkripsi bahkan User (Password) untuk administrasi wireless tersebut.

Secara garis besar, celah pada jaringan wireless terbentang di atas empat layer dimana kempat layer tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media wireless. Jadi sebenarnya, pada setiap layer proses komunikasi melalui media wireless terdapat celah-celah yang menunggu untuk dimasuki. Maka dari itu keamanan jaringan wireless menjadi begitu lemah dan perlu dicermati dengan ekstra teliti.

Layer-layer beserta kelemahannya tersebut adalah sebagai berikut:

1. ***Physical Layer***

   Seperti diketahui, physical layer (layer Fisik) dari komunikasi data akan banyak berbicara seputar media pembawa data itu sendiri. Didalam sistem komunikasi data wireless yang menjadi media perantaranya tidak lain adalah udara bebas tersebut, data yang berwujud sinyal-sinyal radio dalam frekuensi tertentu lalu-lalang dengan bebasnya. Tentu sudah kebayang bagaiman rentannya keamanan data tersebut karena lalu-lalang di alam bebas. Namun bagaimana jika hal ini terjadi pada jaringan wireless perusahaan yang didalamnya terdapat berbagai transaksi bisnis, Proyek-proyek perusahaan, info-info rahasia, rahasia keuangan,dan banyak lagi informasi sensitif di dalamnya. Tentu penyadapan tidak dapat ditoleransi lagi kalau tidak mau perusahaan menjadi bulan-bulan orang.

2. ***Network Layer***

Network layer (layer jaringan) akan banyak berbicara seputar tentang perangkat-perangkat yang memiliki kemampuan untuk menciptakan sebuah jaringan komunikasi yang di sertai juga dengan sistem pengalamatannya. Pada jaringan komunikasi wireless, perangkat yang digunakan sering disebut dengan Acces Point (AP). Sistem pengalamatan IP tentu akan banyak ditemukan pada perangkat ini. Karena melayani komunikasi menggunakan media bebas yang terbuka, maka AP-AP tersebut juga dapat dikatakan sebagai perangkat yang terbuka bebas. Perangkat jaringan yang tidak di verifikasi dan di kontrol dengan baik akan menjadi sebuah pintu masuk bagi para pengacau. Mulai dari dilihat-lihat isinya sampai dirubah sedikit-sedikit dan kemungkinan juga sampai dibajak penuh pun sangat mungkin di alami. Untuk itu perlu diperhatikan juga keamanan AP-AP pada jaringan wireless yang ada.

3. User layer

Selain keamanan perangkat jaringan yang perlu diperhatikan, juga perlu di cermati siapa-siapa saja yang mengakses jaringan wireless yang ada. Jaringan *wireless* memang menggunakan media publik untuk lalulintas datanya, namun jika jaringan yang ada bukan merupakan jaringan publik yang dapat diakses oleh siapa saja. Tentu harus ada pembatasan aksesnya.

4. Appcation Layer

Jaringan yang menggunakan media kabel saja dapat membuka celah yang ada pada aplikasi dengan cukup lebar, apalagi jaringan wireless yang memang rentan diseluruh layer-layernya Aplikasi-aplikasi bisnis yang penggunanya

lalu-lalang melalui media wireless tentu sangat rentan keamanannya, baik sekedar di susupi maupun di DoS *(Denial of Service).* Maka dari itu jaringan wireless yang baik harus juga dapat melindungi aplikasi-aplikasi berjalan di dalamnya agar tidak dengan mudah dikacaukan.

BAB III

METODOLOGI PENELITIAN

A. Waktu dan Tempat Penelitian

A.1. Waktu Penelitian

Penelitian dilaksanakan di semester akhir, dimulai awal bulan maret 2019 selama kira-kira 6 bulan hingga akhir bulan juli 2019 menjelang waktu sidang skripsi pada bulan agustus 2019.

A.2. Tempat Penelitian

Penelitian dilaksanakan di sebuah Perusahaan yang bernama PT Artha Utama Plasindo JL.Flores Blok C-1 Kawasan Industri MM2100, Cibitung-Bekasi.

B. Sejarah Umum Perusahaan

PT Artha Utama Plasindo adalah salah satu perusahaan bergerak dibidang *Injecton* plastik, yang berlamatkan di JL.Flores Blok C-1 Kaw.Industri MM2100, Cibitung-Bekasi. Perusahaan ini kepemilikinnya dipegang oleh Orang Indonesia dan didirikan pada tahun 2003 dan sampai saat ini telah memiliki ± 700 karyawan yang bekerja di perusahaan ini. Produksi yang dihasilkan Oleh PT Artha Utama Plasindo adalah berupa part-part plastic untuk elektronik dan otomotive, dan didukung oleh tenaga ahli yang berpengalaman dan profesional dibidangnya

C. Gambaran Umum Perusahaan

C.1. Visi

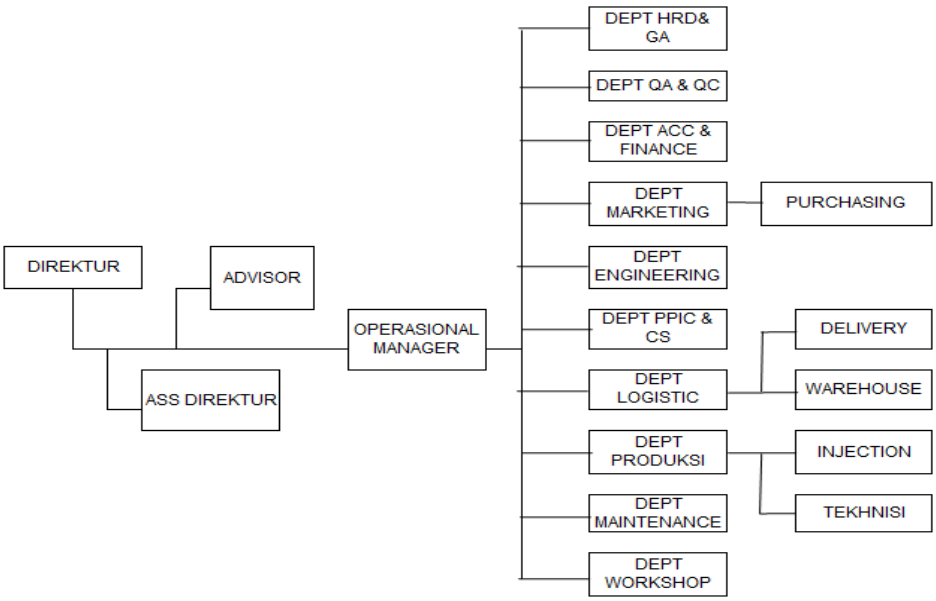
Untuk menjadi manufaktur terkemuka dan pelanggan pilihan pertama pada komponen pemasok otomotif dan ekektronik.

C.2. Misi

Menghasilkan produk berkualitas tinggi pada harga yang kompetitif, meningkatkan kesejahteraan karyawan, menciptakan lingkungan kerja yang baik.

D. Struktur Organisasi dan Uraian Tugas

D.1. Bagan Struktur Organisasi



Gambar 3.1. Struktur Organisasi

Struktur organisasi perusahaan diartikan sebagai susunan dan hubungan antara bagian-bagian dalam perusahaan dengan merinci pembagian aktifitas kerja masing-masing bagian.

D.2. Uraian Tugas dan Tanggung Jawab

Berikut merupakan uraian tugas dan tanggung jawab dari masing-masing jabatan pada PT Artha Utama Plasindo :

a. Direktur

2. Bertindak sebagai pimpinan perusahaan serta bertanggung jawab atas jalannya kegiatan perusahaan.
3. Membuat kebijakan-kebijakan perusahaan dan membuat perencanaan yang menyangkut kelangsungan hidup perusahaan.
4. Menetapkan kebijakan mutu perusahaan.
5. Mengesahkan struktur organisasi yang menandakan fungsi dan wewenang dari masing-masing personel bagian.

b. Ass Direktur

1. Membantu tugas direktur dalam bidang administrasi dan keuangan perusahaan.
2. Melakukan monitoring, evaluasi, review terhadap pelaksanaan tugas pada bagain yang berada di bawah tanggung jawabnya.
3. Menyampaikan pendapat, saran dan opini kepada direktur mengenai masalah-masalah yang berkaitan dengan masalah perusahaan.

4. Melakukan pengembangan produk-produk yang ditawarkan perusahaan.
5. Melakukan kerjasama jaringan dengan perusahaan lain.

c. Departemen Marketing

1. Mempersiapkan dan mengawasi anggaran belanja.
2. Mengawasi dan memelihara asset perusahaan.
3. Mengatur hutang dan tagihan rekening.
4. Melaporkan posisi keuangan perusahaan.
5. Advisor

d. Manager HRD dan GA

1. Membuat dan mengembangkan struktur organisasi, uraian jabatan, peraturan perusahaan sehingga setiap karyawan mengerti tugas dan tanggung jawab serta melaksanakan dengan baik.
2. Membuat perhitungan gaji untuk tingkat operator, Adm Subdept, Group Leader dan Foreman.
3. Membuat surat pengangkatan karywan tetap dan jabatan.
4. Bertanggung jawab atas izin tenaga kerja, izin lingkungan dan izin perusahaan.
5. Mengkoordinir kerapihan area penampungan scrap dan mengatur izin perusahaan.

e. Departemen Purchasing

1. Mengadakan negosiasi, evaluasi penerimaan proposal dan membuat rekomendasi untuk pembelian.
2. Mengontrol pemborongan seperti kontrak, registrasi, kemampuan produksi, kualitas dan pengiriman.
3. Menjaga dan memperbaharui sistem pengisian daftar pemborong, daftar harga, catalog. Pesanan pembelian dan kontrak permintaan pembelian.

f. Kaizen

Bertugas melakukan improvement perusahaan.

g. Operasional Manager

1. Membuat perencanaan dan mengendalikan kegiatan bidang operasional perusahaan.
2. Berkoordinasi dengan Direktur dalam hal kegiatan operasional perusahaan.
3. Bersama para manager menyusun sasaran mutu, Object Plan dan menjabarkan rencana kegiatan operasional perusahaan.
4. Mengkoordinasikan pelaksanakan sistem pemantauan dengan managernya.
5. Mengambil tindakan apabila terjadi penyimpangan pada operasional.
6. Mereview pencapaian target sasaran mutu dari tiap-tiap departemen.
7. Menentukan jumlah komposisi karyawan yang optimal.
8. Bertanggung jawab atas implementasi Management Mutu ISO 9001:2000 dan K3.
9. Bertanggung jawab atas improvement untuk meningkatkan efisiensi agar dapat bersaing dengan perusahaan lain yang sejenis.

h. Manager Engineering

1. Membuat dan mengembangkan setiap aturan dan prosedur, sehingga setiap jenjang pimpinan, mengerti tugas dan tanggung jawab dan dijalankan dengan baik.
2. Menentukan sasaran improvement dan aktivitas penunjang sehingga sasaran tersebut dapat dicapai.
3. Bekerjasama dengan departemen produksi, PPIC, Quality untuk trial item baru.

i. Manager PPIC

1. Menentukan sasaran improvement dan aktivitas-aktivitas yang harus dilaksanakan.
2. Evaluasi master schedule bersama bawahannya.
3. Membuat perencanaan produksi yang mencakup kebutuhan bahan baku, man power, kapasitas produksi dan penjadwalan.
4. Membuat pengendalian produksi yang mencakup kegiatan pengendalian kualitas dan kuantitas produksi, pengendalian biaya dan delivery produksi.

j. Manager Produksi

1. Membuat aturan-aturan prosedur sehingga setiap jenjang pemimpin mengerti, apa tugas dan tanggung jawab dan melaksanakan dengan baik.
2. Menjabarkan kebijakan-kebijakan dari atsan berupa activity plan hingga pelaksanaan dilapangan.

3. Bekerjasama dengan departemen personalia dan GA dalam usaha meningkatkan Sumber Daya Manusia (SDM), penerimaan karyawan, promosi / demosi jabatan.
4. Membuat activity plan tahunan dan master schedule.
5. Mengatur jadwal produksi untuk mencegah stop line di customer.
6. Membuat laporan bulanan dan dilaporkan ke operational manager.
7. Mengevaluasi hasil produksi mingguan dengan departemen PPIC, Engineering, Quality Control dan Quality Anssurance.

k. Manager Quality

1. Membuat dan mengembangkan aturan-aturan prosedur sehingga setiap jenjang pimpinan mengerti, apa tugas dan tanggung jawabnya dan menjaga agar hal tersebut dijalankan dengan baik.
2. Membuat pengendalian kualitas produksi.
3. Menganalisa dan menjawab claim market.
4. Menentukan sasaran improvement dan aktivitas-aktifitas yang harus dilaksanakan.

l. Manager Workshop

1. Merencanakan dan memastikan sistem pengendalian dan perawatn untuk semua mould milik perusahaan ke customer.
2. Membuat dan merencanakan aktifitas perbaikan untuk mencapai sasaran mutu dept workshop.

3. Mengatur dan memastikan proses kerja dept workshop sesuai dengan standar ISO 9001 -2008.
4. Menetapkan target dan sasaran mutu dept workshop.

m. Manager Maintenance

1. Merencanakan dan memastikan sistem pengendalian, perawatan untuk semua mesin dan infrastruktur yang dibawah tanggung jawab dept maintenance.
2. Memastikan setiap ketidaksesuaian atau kerusakan dievaluasi, diperbaiki dan dicegah.
3. Membuat dan merencanakan aktifitas perbaikan untuk mencapai sasaran mutu dept maintenance.

n. Asisten Manager

1. Membantu manager dalam melaksanakan tugas-tugasnya.
2. Menggantikan tugas manager apabila manager tidak masuk atau sedang tugas keluar.

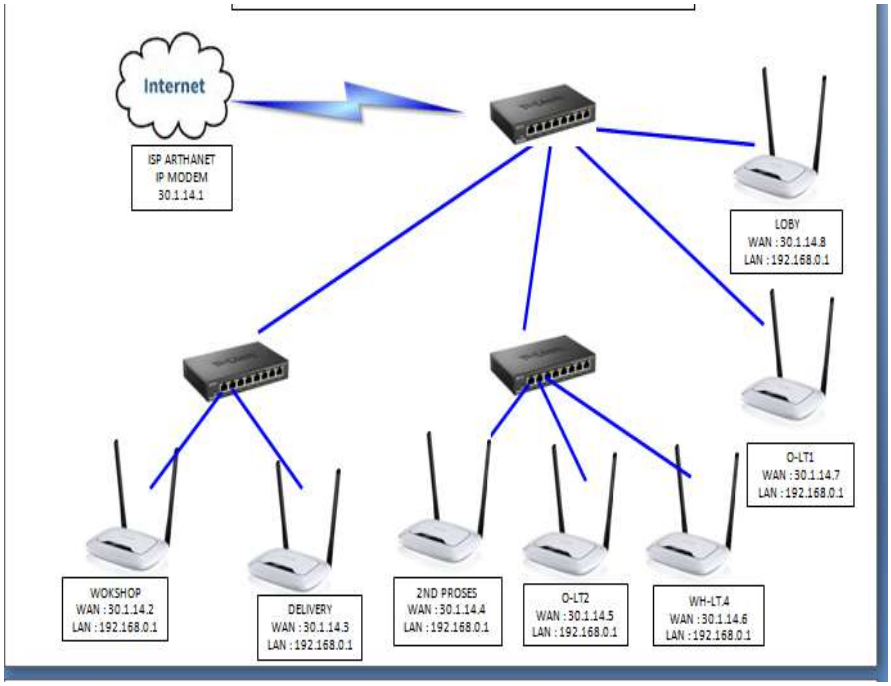
o. Supervisor

1. Mengawasi / mengontrol seluruh pelaksanaan tugas sehari-hari pada karyawan yang ada di dalam pabrik sehingga kegiatan operasional dapat berjalan sebagaimana mestinya.
2. Menindak lanjuti segala sesuatu yang menjadi kendala-kendala bagi para karyawan didalam mereka menjalani tugasnya sehari-hari.

p. Teknisi/ IT

1. Mengawasi / mengontrol seluruh keadaan sistem jaringan internet maupun setiap program, dan komputer yang ada di perusahaan
2. Menindak lanjuti segala sesuatu yang menjadi kendala-kendala bagi para karyawan didalam mereka menjalani tugasnya sehari-hari atas trouble pada jaringan komputer/internet maupun komputer yang rusak.

E. Analisa Sistem berjalan



Gambar 3.2. Sistem Jaringan PT.Artha Utama Plasindo

PT.Artha Utama Plasindo menggunakan ISP Arthanet, bandwidth nya sebanyak 10Mbps. Bandwidth tersebut terhubung lagsung ke switch dan dari switch tehubung ke *Router Wirelless*.

Di PT.Artha Utama Plasindo terdapat 7 buah *Router Wirelless* yang berfungsi sebagai hostpot. Karyawan bebas memakai internet yang di pancarkan oleh *Router Wirelless* tanpa adanya batasan bandwidth dan jaringan tersebut juga bersifat terbuka, siapa saja bisa masuk ke jaringan *wireles*s. Dengan wireless yang bersifat terbuka hal ini sangat di khawatirkan bila sewaktu-waktu ada serangan dari luar yang mencoba utuk menyusup dan mencoba melalukan aksi hacking atau aksi lainya. Untuk saat ini Jaringan wireless masih keadaan aman belum pernah ada terjadi aksi hacking, tetapi dengan *wireless* yang tanpa keamanan khusus akan rentan terhadap serangan yang sewaktu waktu bisa terjadi.

Dari analisa yang di lakukan pada PT.Artha Utama Plasindo penulis merasa perlu untuk melakukan penelitian lebih lanjut, guna untuk memberikan Struktur jaringan yang baik dan memiliki pengamanan khusus atas jaringan *woreless* yang ada di PT.Artha Utama Plasindo.

F. Metode Pengumpulan Data

Metode pengumpulan data yang penulis gunakan dalam penelitian ini, yaitu:

1. Tahap Studi Literature

Pada studi literatur ini dilakukan proses pemilihan suatu masalah yang akan digunakan sebagai tugas akhir. Selanjutnya diteruskan dengan pencarian referensi

sebagai landasan dan penunjang terhadap pengerjaan sekaligus sebagai pemecahan masalah yang dihadapi. Tahapan terakhir dari studi pustaka ini adalah perumusan dan batasan masalah yang dihadapi menjadi lebih jelas.

2. Wawancara

Metode ini dilakukan dengan melakukan komunikasi antar dua orang atau lebih untuk memperoleh informasi yang menyangkut perancangan sistem dan aplikasi yang sedang di rencanakan di Artha Utama Plasindo.

3. Observasi

Melakukan pengamatan dan menganalisa serta berkordinasi dengan bagian IT agar memudahkan proses dokumentasi baik itu informasi yang berhubungan dengan objek dan pekerjaan apa saja yang dilakukan.

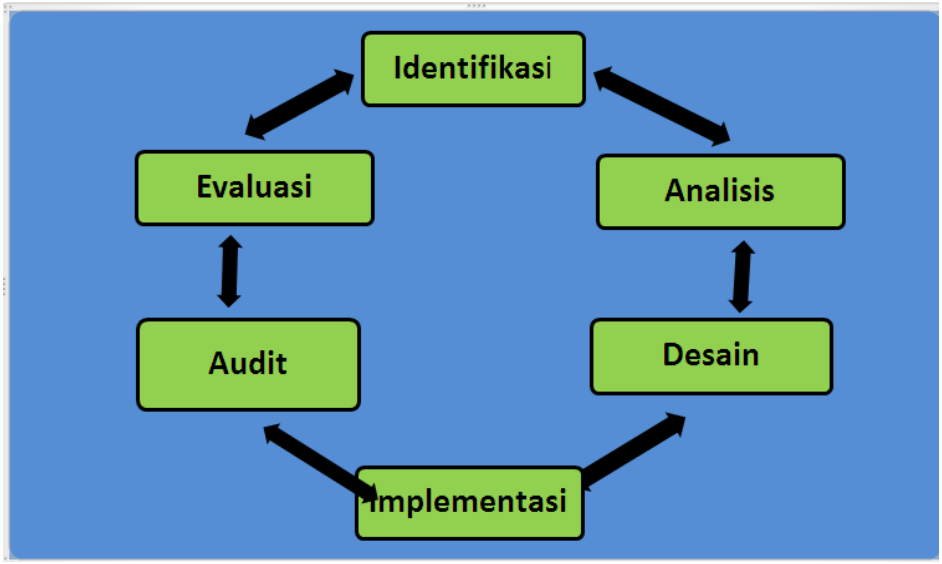
G. Software dan Hardware

Untuk menunjang penelitian, penulis memerlukan software dan hardware sebagai berikut:

1. Mikrotik
2. Acces Point
3. Kabel LAN
4. Laptop

H. Metodologi Penelitian

Metodologi yang akan digunakan dalam penelitian ini adalah *Security Pollicy Development Life Cyle (SPDLC).* Berikut penjelasan tahap-tahap yang akan dilakukan dalam penelitian ini:



Gambar 3.3. *Security Pollicy Development Life Cyle (SPDLC).*

1. **Identifikasi**

   Tahap awal ini penulis mengidentifikasi masalah yang berhubungan dengan jaringan *wireless* dan sistem keamanan *wireless*

2. **Analisis**

   Dari data yang di dapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan user.

3. **Desain**

   Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan di bangun, Yang dilakukan penulis dalam tahapan

perancangan ini yaitu mengatur keamanan pada wireless dengan otentikasi user name Password dan Mac Address filter.

4. **Implementasi**

   Pada tahap ini dilakukan penerapan dari hasil perancangan yang telah dilakukan pada tahap sebelumnya, Setelah setting keamanan pada wireless selesai dikerjakan, penulis melakukan uji coba terhadap sistem keamanan tersebut sehingga sistem keamanan tersebut dapat diimplementasikan/di terapkan pada PT.Artha Utama Plasindo.

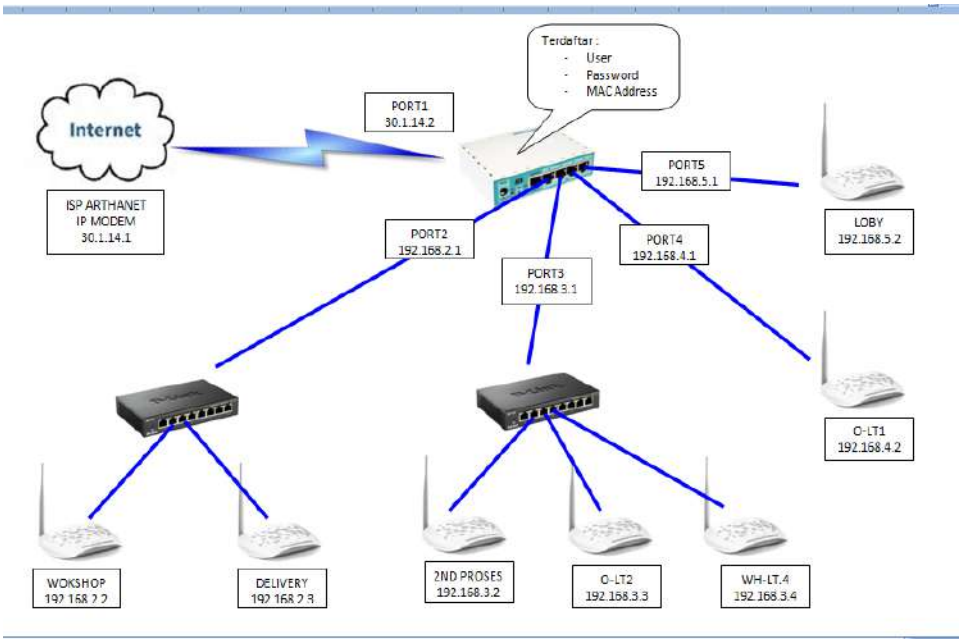
5. **Audit**

   Memeriksa sistem keamanan yang diterapkan.

6. **Evaluasi**

   Mengevaluasi sistem keamanan yang telah diterapkan. Karena keterbatasan waktu dan wewenang yang ada, maka tahap Audit dan Evaluasi tidak akan di bahas akan tetapi diterjemahkan sebagai proses pengujian dan analisisnya.

I. Perancangan Sistem Yang di usulkan



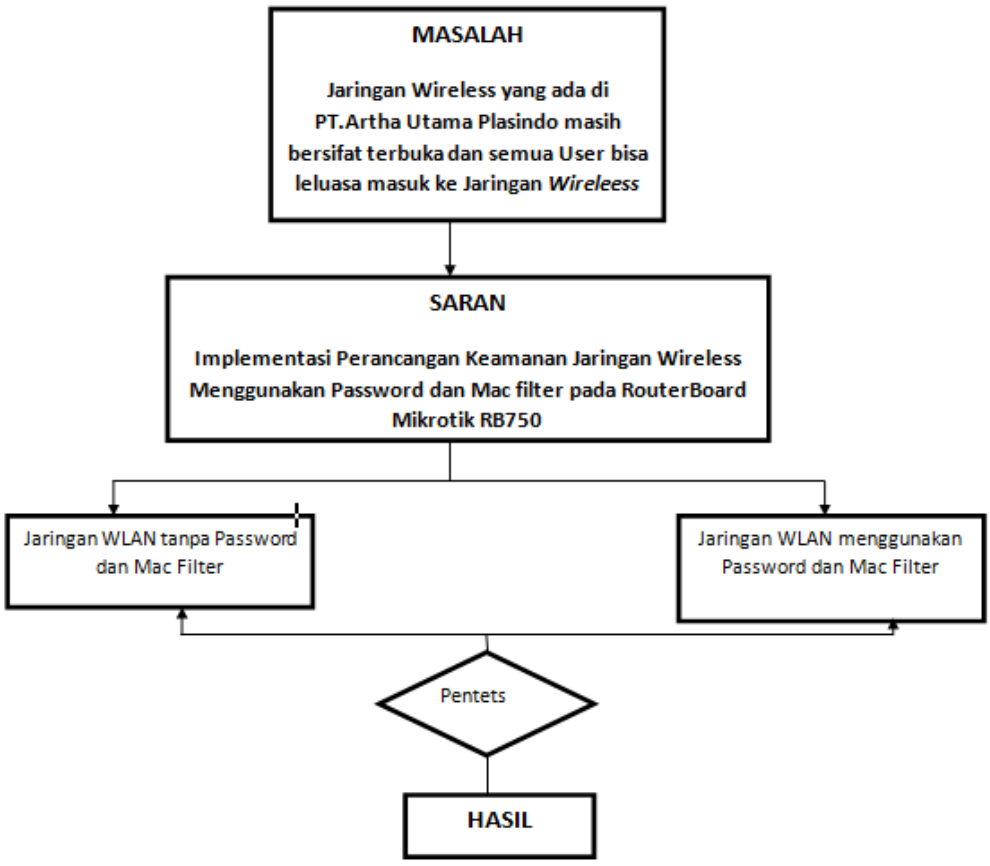
Gambar 3.4. Sistem Yang Di Usulkan

Dari gambar di atas terdapat penambahan perangkat yaitu RouterBoard Mikrotik RB750 dan Acces Point. RouterBoard Mikrotik RB750 ini akan di hubungan dari ISP Arthanet ke Mikrotik RB750 dan dari mikrotik RB750 terhubung ke switch kemudian di teruskan ke Acces Point, dan Acces point ini berfungsi sebagai pemancar Jaringan *Wireless* LAN.

Di RouterBoard Mikrotik RB750 akan dilakukan setting untuk keamanan pada Jaringan Wirelless LAN yang menggunakan User/Password,dan Mac Address Filter supaya jaringan Wireless LAN yang ada di PT.Artha Utama Plasindo terstruktur dengan baik dan memiliki keamanan jaringan yang dapat melindungi jaringan *Wireleess LAN* (*Lokal Area Network*)

J. Kerangka Berfikir

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alur penelitian



Gambar 3.5. kerangka berfikir.

BAB IV

HASIL DAN PEMBAHASAN

A. Hasil Penelitian

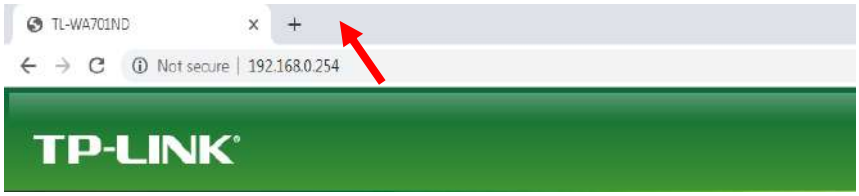
Untuk mengiplementasi rencana yang sudah disusun, maka konsep yang dipakai untuk mengamankan jaringan wireless yaitu dengan dua sistem keamanan yaitu dengan menggunakan otentikasi keamanan User(password) dan Mac Address Filter, Dalam penelitian ini jenis jaringan otentikasi keamanan yang digunakan ialah WPA-PSK, jenis Enkripsinya AES, dan untuk transmisi wirelessnya bertipe 802.11n dengan frekuensi radio 2,4 GHz dan kecepatan data maksimum mencapai 72Mps.

B. Pembahasan

B.1. Setting jaringan *wireless* LOBI pada TP-LINK-TL-701ND

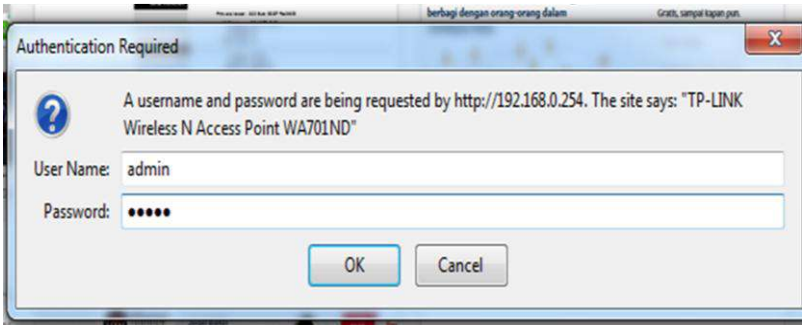
Langkah – langkah untuk setting jaringan wireless LOBI menggunakan TP-LINK-TL-701ND.

a) Langkah pertama, Hidupkan access point dan hubungkan ke PC dengan kabel UTP
b) Langkah ke 2, Buka web browser, kemudian ketik alamat ip router default 192.168.0.254 ke address bar lalu enter.



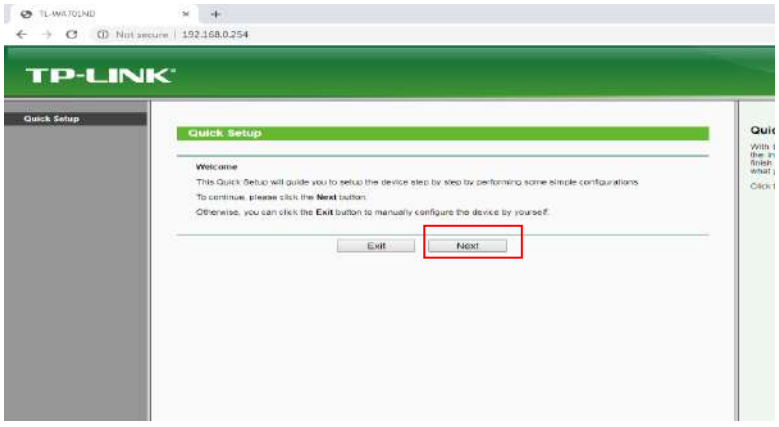
Gambar 4.1. Langkah ke Dua

c) Langkah ke 3, Kemudian Masukkan User dan Password default yaitu admin lalu klik Ok.



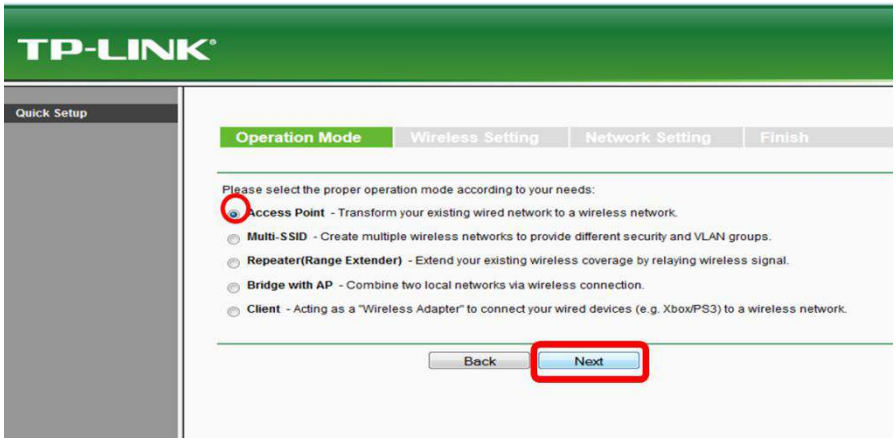
Gambar 4.2. Langkah ke Dua. Tampilan login

Kemudian akan muncul tampilan seperti berikut :



Gambar 4.3. Tampilan TP-LINK-TL-701ND

d) Langkah ke 4, Pada Operation Mode kita Pilih Access Point dan Klik Next.

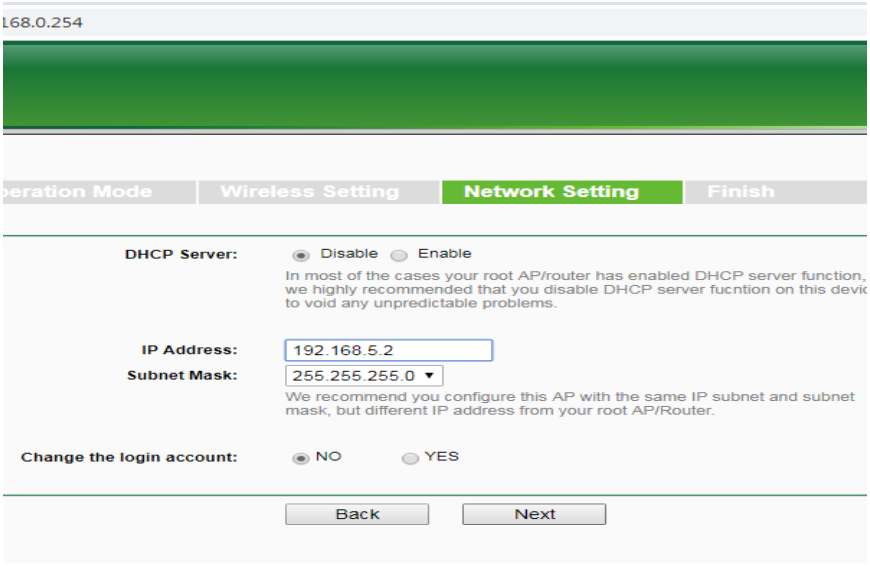


Gambar 4.4. Tampilan gambar Operation Mode.

e) Langkah ke 5, Pada *Wireless Setting*, penulis memberi nama SSID LOBI dan tanpa password, sebab settingan *password* akan di setting di Mikrotik RB750. Berikut tampilan *wireless setting* SSID yang di tandai dengan kotak merah.

Gambar 4.5. gambar kolom *wireless setting* SSID

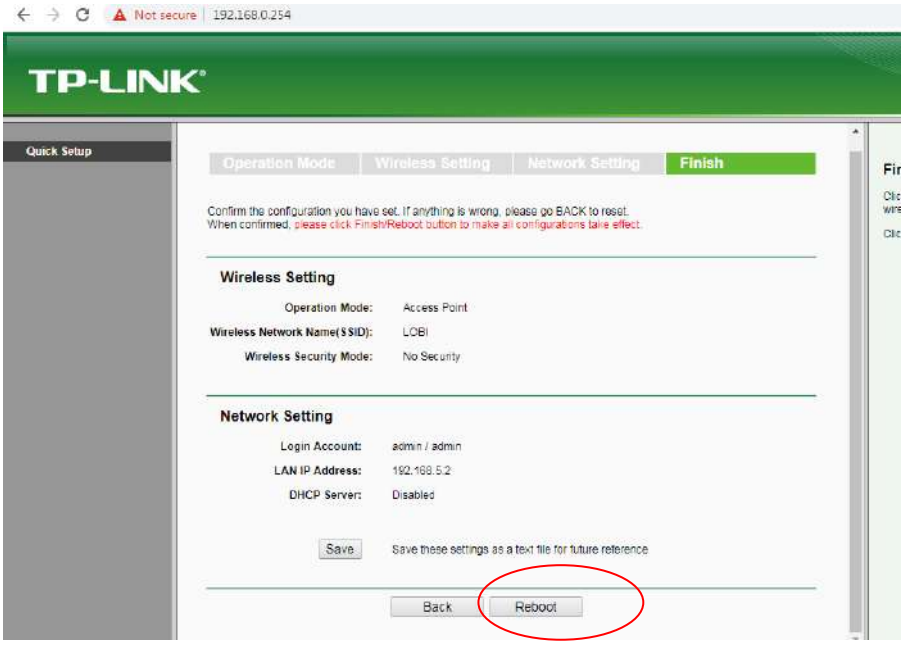
f) Langkah ke 6, Pada *Network Setting*, DHCP Server kita pilih Disable supaya mudah dalam koneksi ke *Access Point*nya, dan pada kolom IP address kita isi sesuai dengan *network* yang kita inginkan. Lalu klik *Next*.



Gambar 4.6. *Network Setting* DHCP

Setelah mucul Tampilan seperti gambar di atas, maka jangan lupa untuk mengisi *IP Address* kemudian enter maka *Subnet Masknya* akan muncul otomatis. Dan untuk status *DHCP Server* dipilih status Disable. Setelah selesai boleh untuk melanjutkan dengan klik Next.

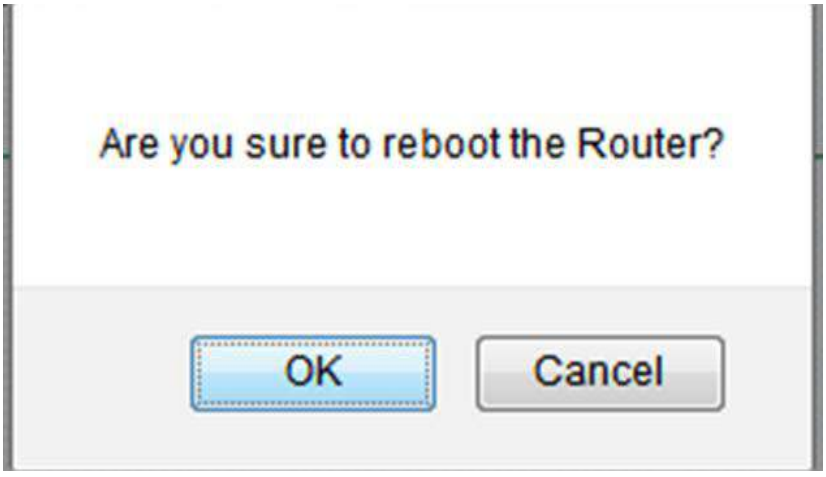
Maka akan muncul Tampilan hasil dari settingan :



Gambar 4.7. Tampilan hasil dari settingan.

g) Langkah ke 7, pada Gambar 4.7. Tampilan hasil dari settingan. Di lanjutkan dengan klik Reboot.

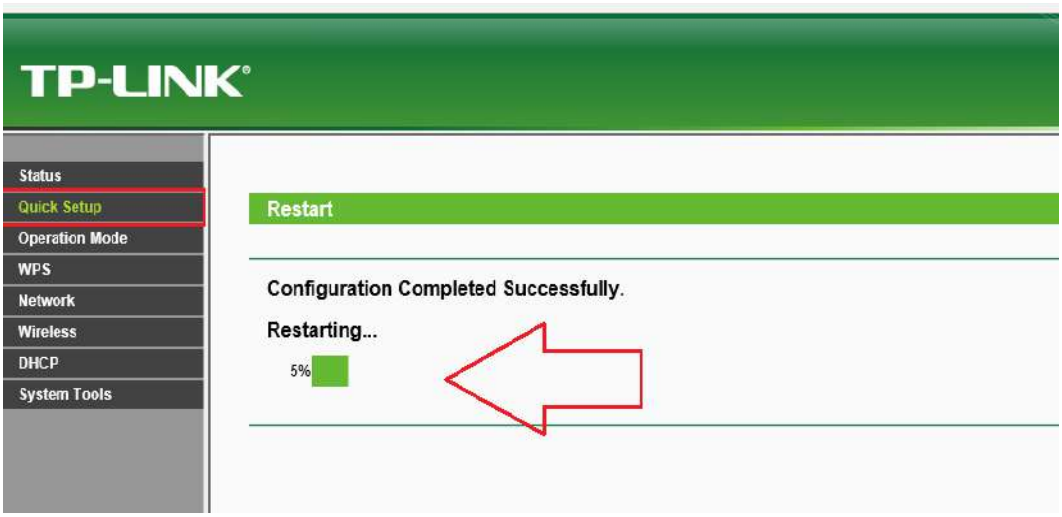
Maka akan muncul tampil seperti berikut :



Gambar 4.8. Tampilan konfirmasi reboot.

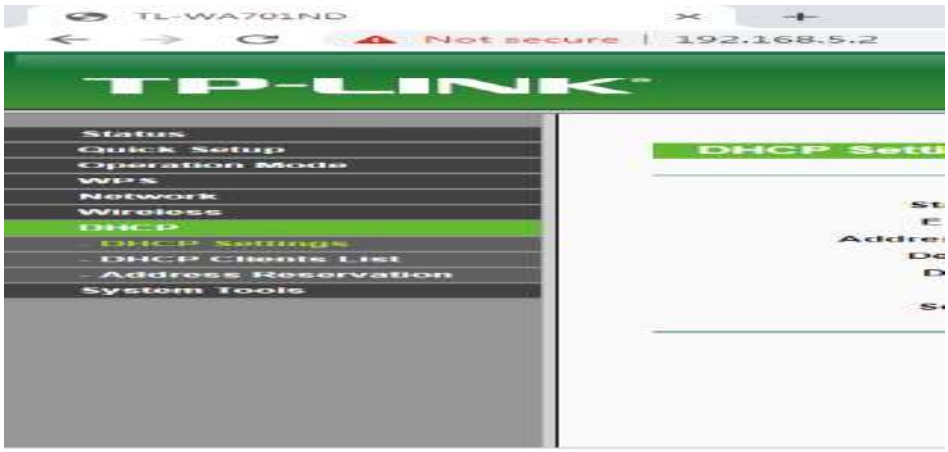
h) Langkah ke 8, adalah klik OK pada tampilan yang ada di Gambar 4.8. Tampilan konfirmasi reboot.

Tunggu hingga proses Reboot Selesai.



Gambar 4.9. Proses Reboot

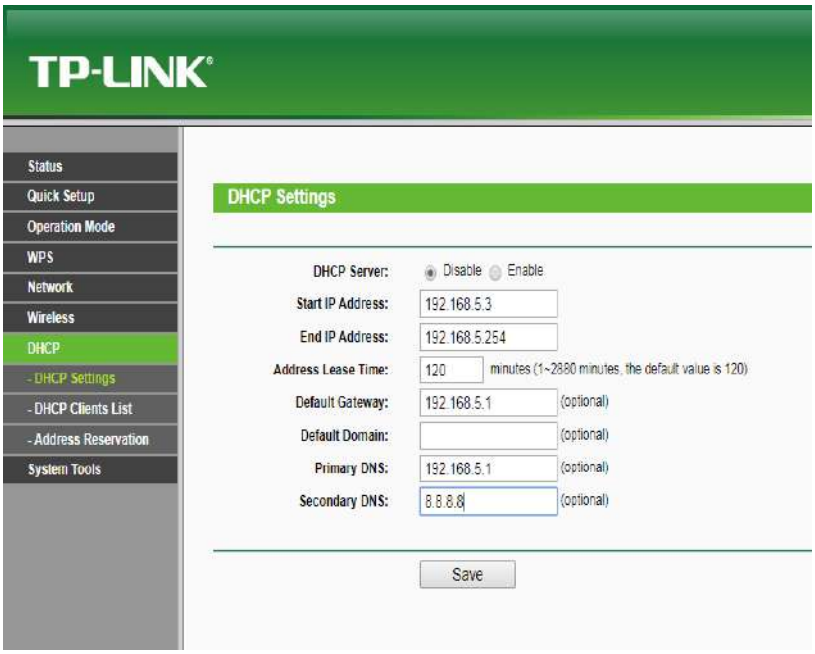
i) Langkah ke 9, Jika sudah Selesai reboot maka tahap selanjutnya adalah masuk ke menu DHCP.



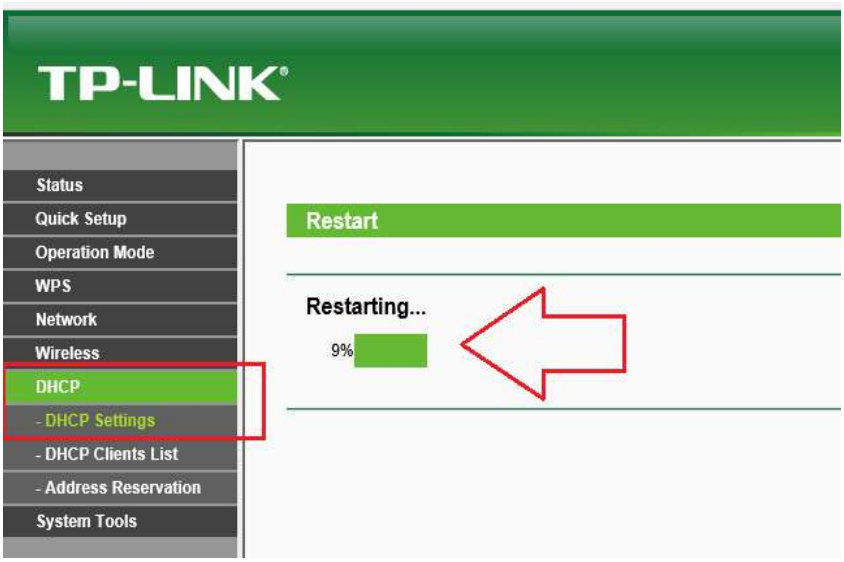
Gambar 4.10. gambar menu DHCP

j) Langkah ke 10, Setting DHCP Server

- Start IP Address 192.168.5.3 (Mulai IP Address)
- End IP Address 192.168.5.254 (Akhir IP Address)
- Default Gateway 192.168.5.1 (Gateway Router)
- Primary DNS 192.168.5.1 – Secondary DNS 8.8.8.8 (Agar terkoneksi ke Internet)
- Lalu klik Save



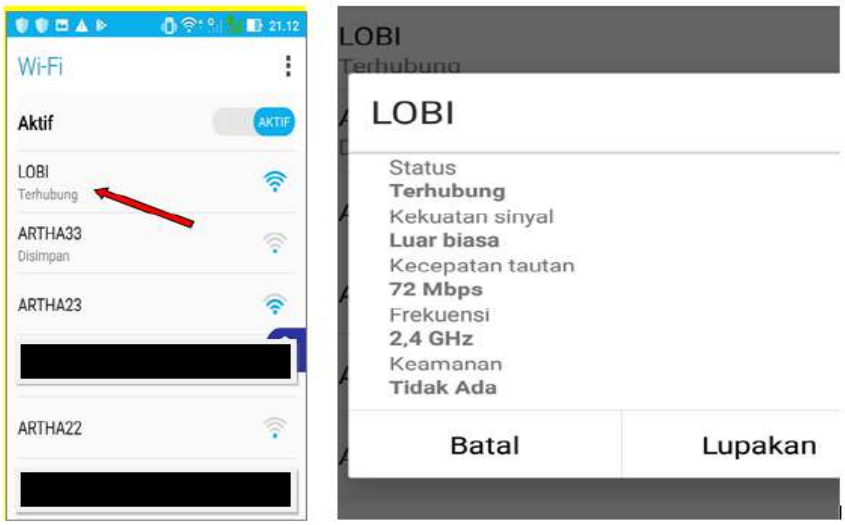
Gambar 4.11. Setting DHCP



Gambar 4.12. Proses Reboot

Tunggu sampai prosses Reboot Selesai.

k) Langkah ke 11, melakukan test koneksi melalui WI-FI (*Wireless Fidelity)*

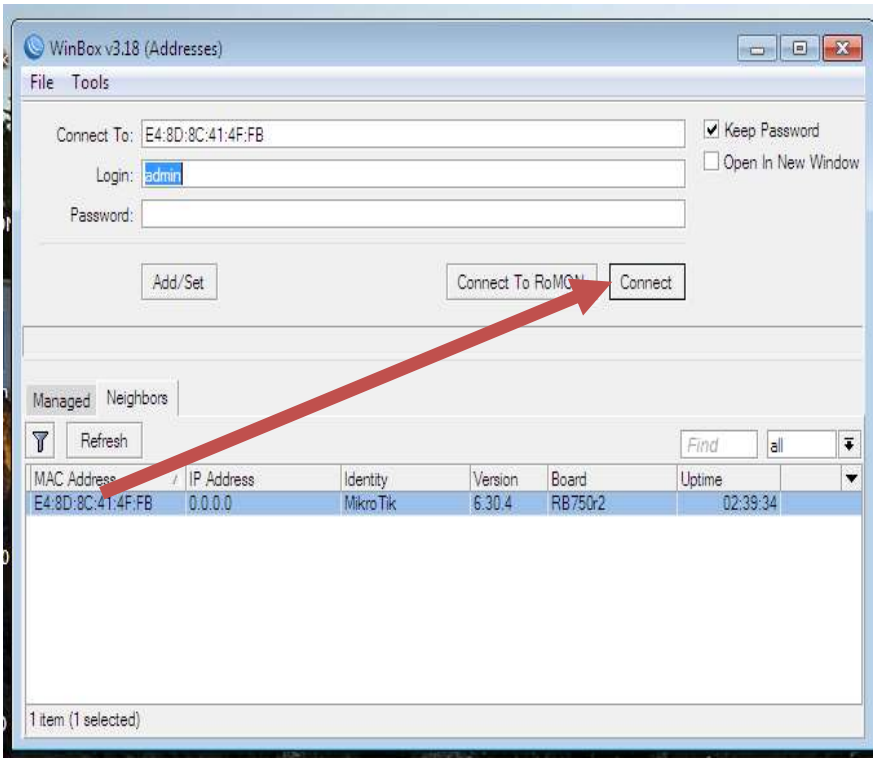


Gambar 4.13. hasil test koneksi.

Hasil test koneksi pada Gambar 4.13. hasil test koneksi. Membuktikan bahwa settingan jaringan wireless yang di lakukan dengan SSID: LOBI telah berhasil.

B.2. Konfigurasi Wifi Access Point dan Mikrotik RB750

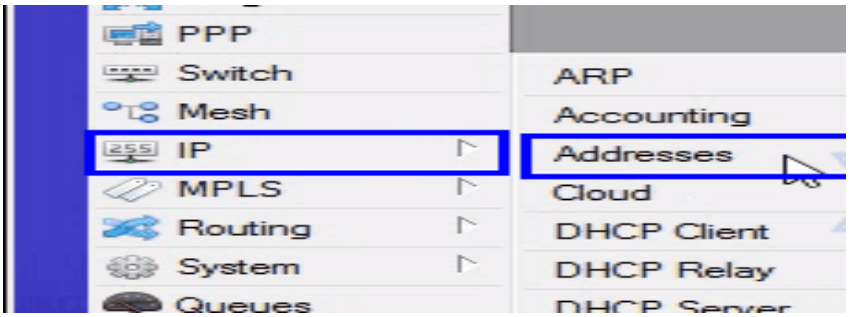
a) Langkah pertama yang harus dilakukan adalah masuk ke *winbox*. *Login* menggunakan *MAC Address*. Lalu connect.



Gambar 4.14.konfigurasi Mikrotik menggunakan *winbox*

b) Mengatur IP pada Router

1. Klik IP>*Address* untuk menambahkan *IP address*

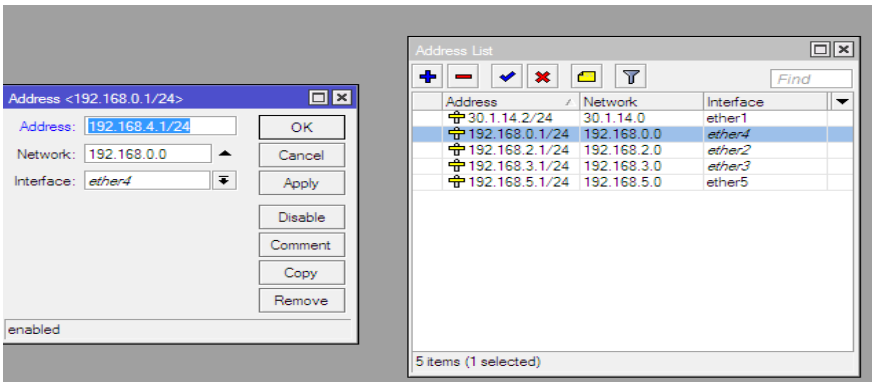


Gambar 4.15. Mengatur IP

2. Selanjutnya jika ingin menambahkan IP untuk ether1, ether 2 dan ether 3 dan seterusnya, caranya klik *icon* tambah (+)

Gambar 4.16. cara menambah icon

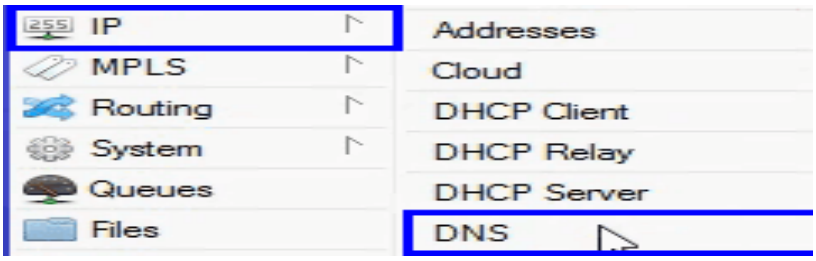
3. Pemberian masing-masing IP untuk masing-masing ether.



Gambar 4.17. cara pemberian IP *ether*

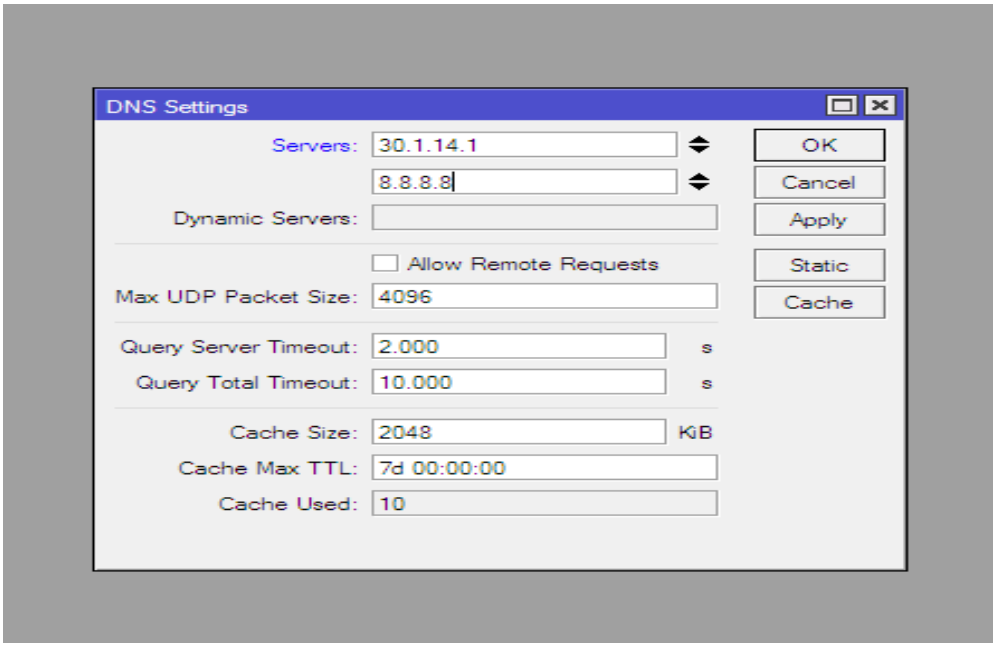
4. *Setting DNS* (*Domain Name System*)

Klik IP>DNS



Gambar 4.18. Setting DNS

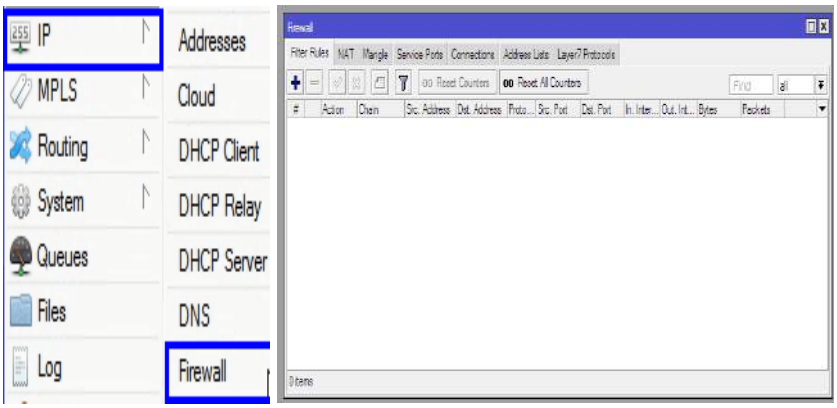
Tampilan *setting DNS* (*Domain Name System*) terlihat pada gambar berikut:



Gambar 4.19. kolom settingan DNS

5. Setting firewall

Selanjutnya jika ingin menambahkan ip *firewall* caranya klik IP>*Firewall*

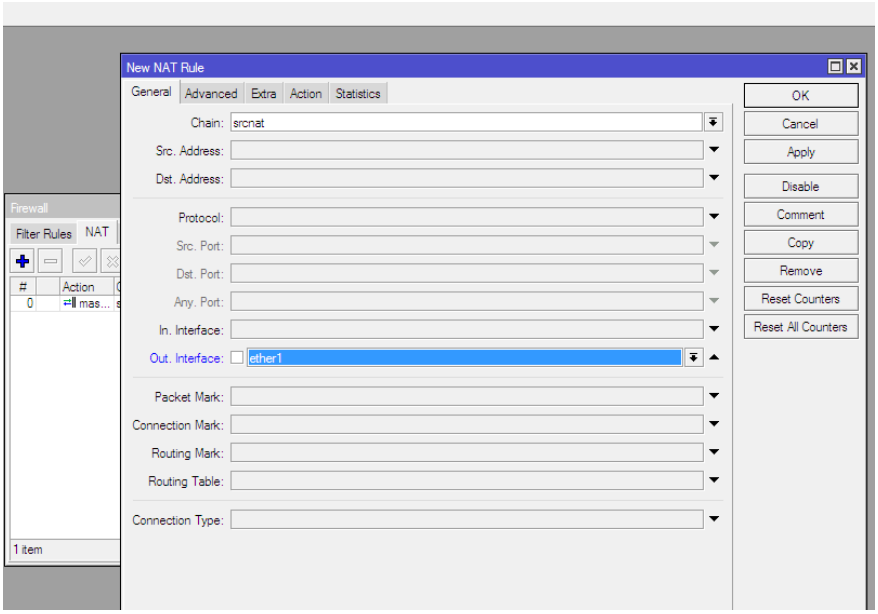


Gambar 4.20.Menambah IP firewall

a) Konfigurasi pertama tambahkan *firewall NAT* (*Network Address Translation*) untuk chain dengan memilih Srcnat dan out interface dengan interface yang terhubung ke IP Public

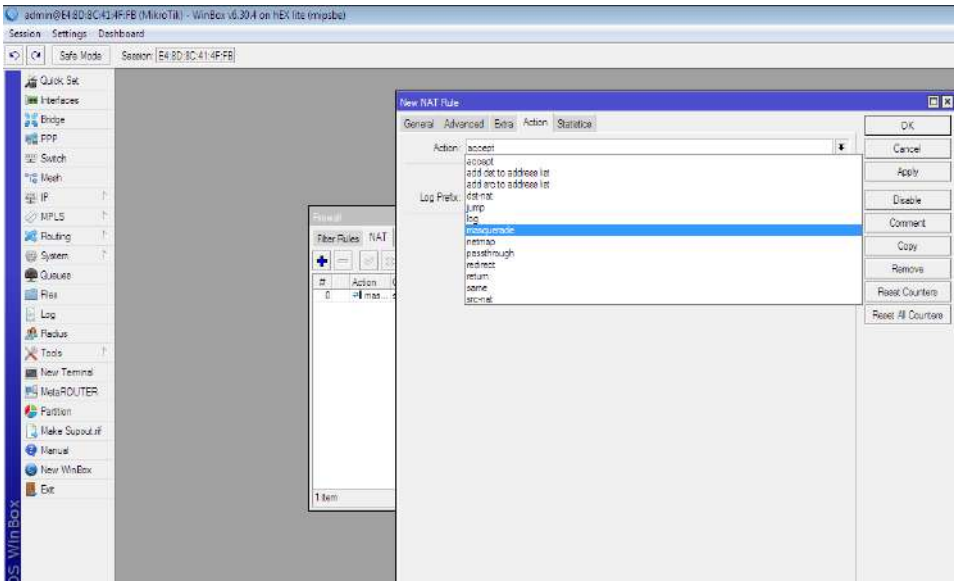
Srcnat, berfungsi untuk mengubah *source address* dari sebuah paket data. Contohnya ketika ingin mengakses *website* di internet melalui koneksi dari router, maka *IP Address* lokal akan disembunyikan oleh Router dan diganti dengan *IP Address* Publik pada router.

Pilih tab *General*>*Chain* pilih *srcnat*, untuk *Out.interface* pilih *ether1* lalu klik OK.



Gambar 4.21. konfigurasi firewall NAT

6. Pada tab Action pilih Masquerade, lalu klik Ok.



Gambar 4.22. ***NAT rule Masquerade*****.**

Masquerade berfungsi untuk menyamarkan IP lokal menjadi *IP Public*.

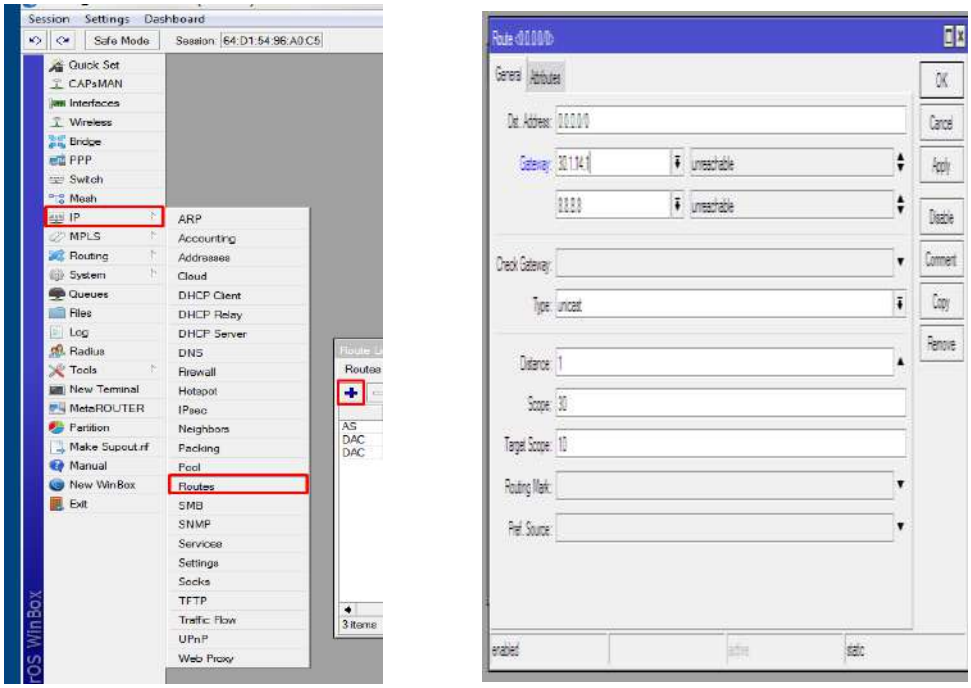
7. Setting Routes.

Klik IP > Routes >"+"

Dst-address : 0.0.0.0/0

Gateway : 30.1.14.1 (yang diberikan oleh *ISP*).

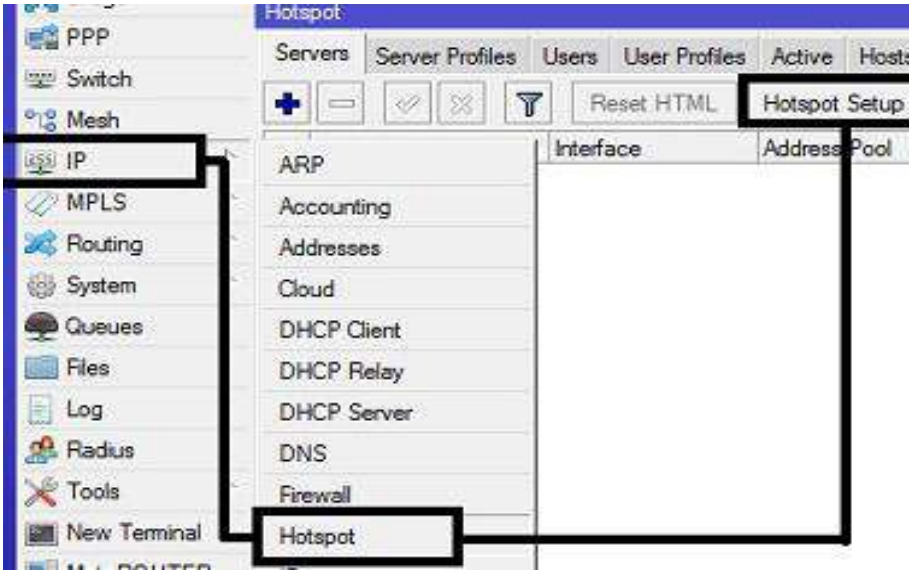
30.1.14.1 digunakan sebagai gateway utama PT.Artha Utama Plasindo.:



Gambar 4.23. Tampilan setting Routes.

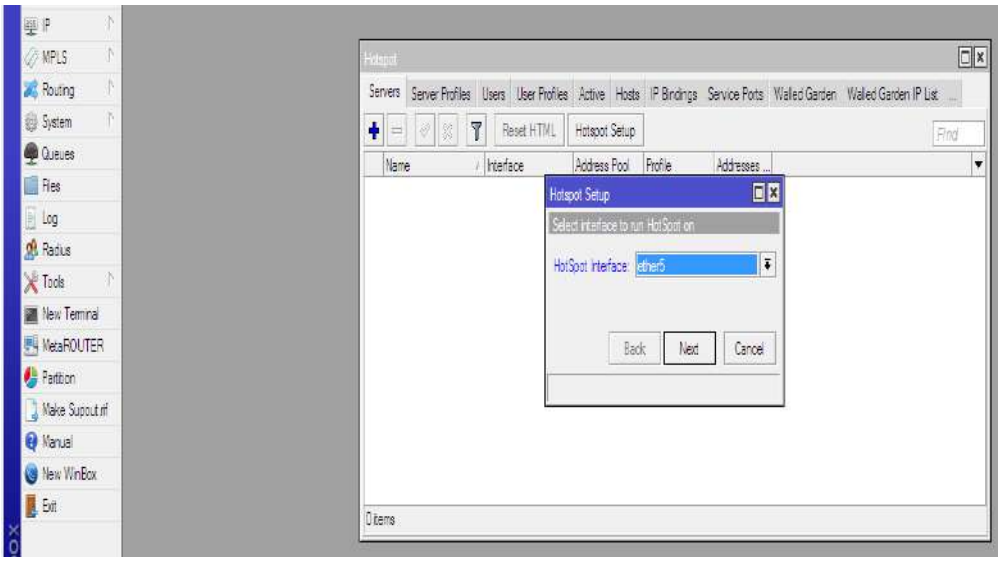
8. Setting hotspot.

Untuk setting hotspot buka di menu *IP > Hotspot > Hotspot Setup.*



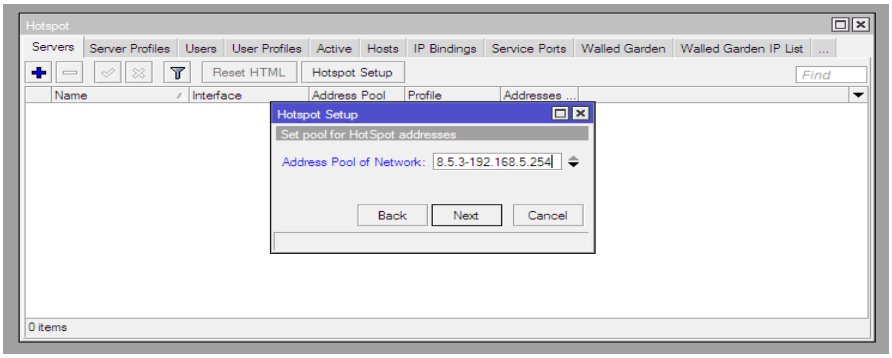
Gambar 4.24. Tampilan setting hotspot.

Dengan klik tombol Hotspot Setup, wizard Hotspot akan menuntun untuk melakukan setting dengan menampilkan kotak-kotak dialog pada setiap langkah.



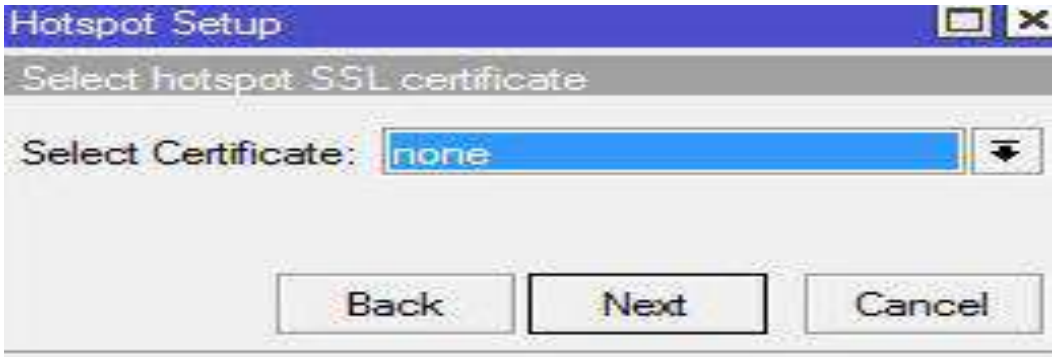
Gambar 4.25. Gambar menentukan interface .

Langkah ini, diminta untuk menentukan interface Hotspot yang akan diaktifkan. Dan hotspot diaktifkan pada ether5, dimana ether5 sudah di set sebagai access point . Selanjutnya klik Next.



Gambar 4.26. Menentukan range IP Address .

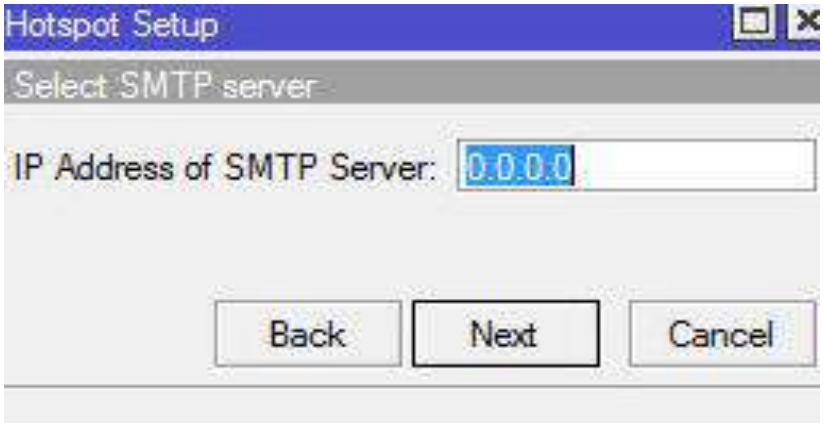
Langkah berikutnya pada Gambar 4.24. menentukan range IP Address yang akan diberikan ke user (DHCP Server) secara default, router otomatis memberikan range IP sesuai dengan prefix/subnet IP yang ada di interface. Tetapi ini juga bisa di rubah jika dibutuhkan. Lalu klik Next.



Gambar 4.27. Tampilan SSL sertificate.

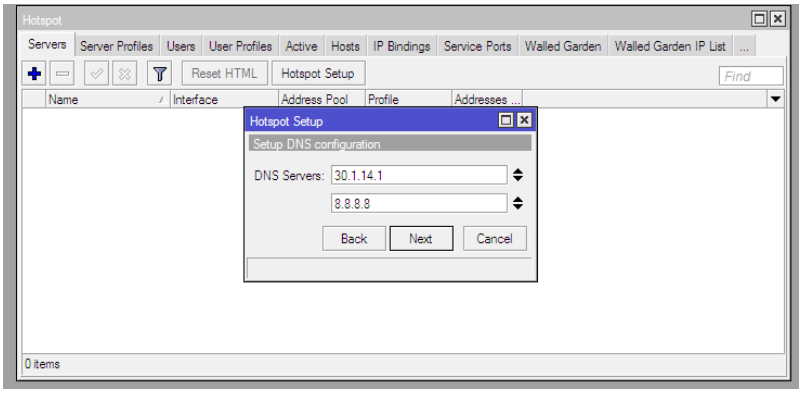
Langkah selanjutnya, menentukan SSL (*Secure Socket Layer*) sertifikat, jika kita akan menggunakan HTTPS untuk halaman loginnya. Tetapi jika kita tidak memiliki sertifikat SSL, kita pilih none, kemudian klik Next.

Maka akan muncul tampilan seperti berikut.



Gambar 4.28. Tampilan SMTP (Simple Mail Transfer Protocol).

SMTP (Simple Mail Transfer Protocol) Server khusus untuk server hotspot bisa ditentukan, sehingga setiap request SMTP client diredirect ke SMTP yang sudah di tentukan. Karena tidak disediakan SMTP server, IP 0.0.0.0 di biarkan default. Kemudian klik Next.

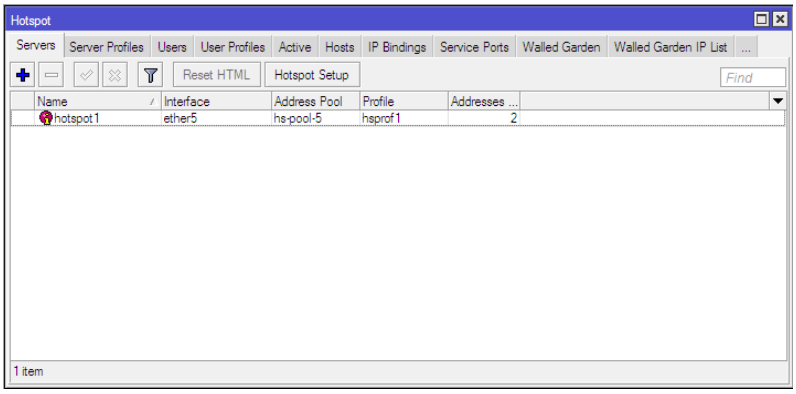


Gambar 4.29. Tampilan DNS Server.

Masukkan DNS Server ke dalam jaringan hotspot, boleh mengisi dengan dns server yang diberikan oleh ISP langganan, atau boleh juga di isi dengan dns public dari google seperti ini, kemudian klik next lagi.

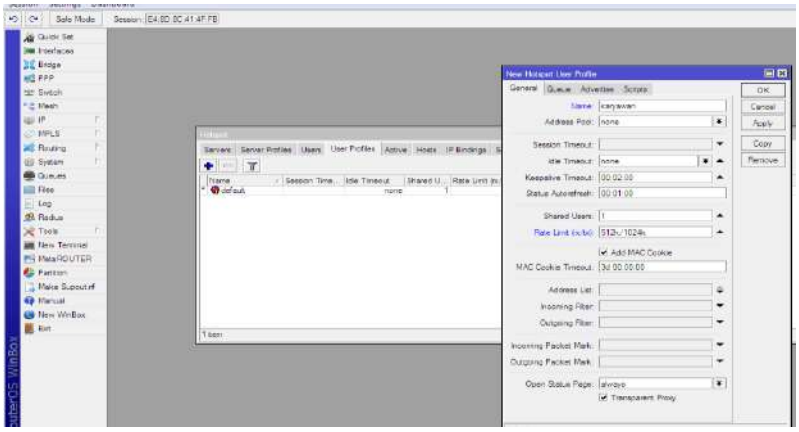
9. Setting User Profile Hotspot

Klik menu IP > Hotspot > User Profile



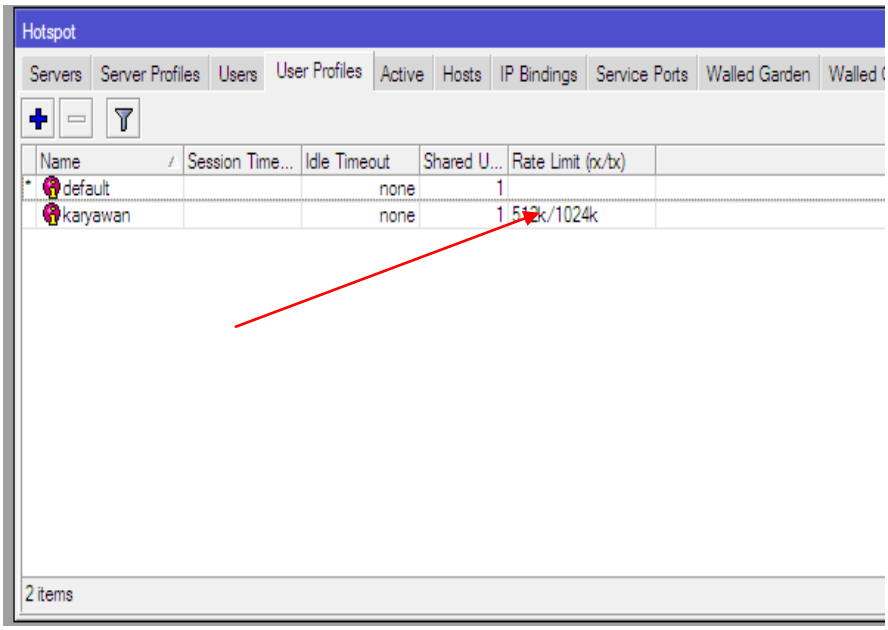
Gambar 4.30. Tampilan User Profile Hotspot.

Setelah muncul user profile, maka dilakukan pengaturan paket seperti berikut :



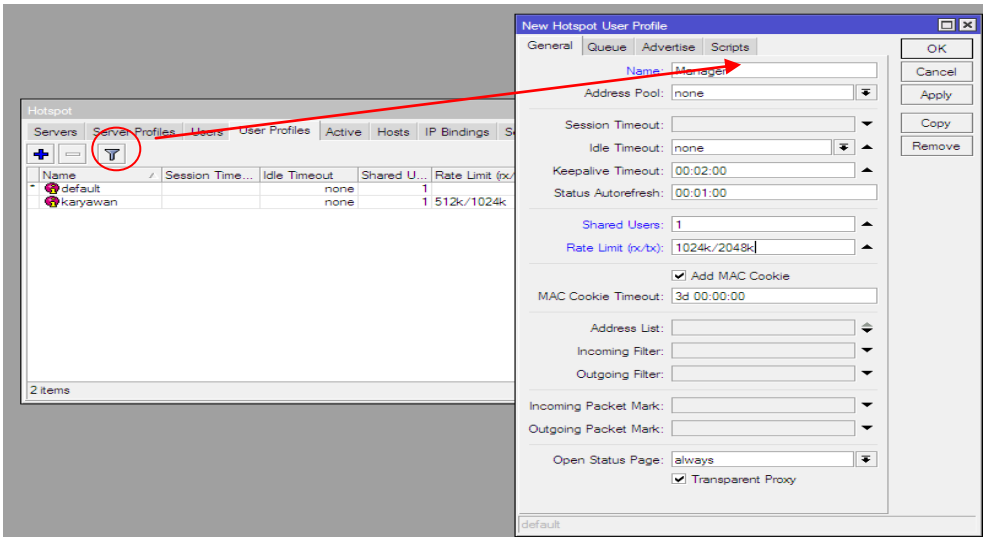
Gambar 4.31. Tampilan Pengaturan Paket.

Hasil pengaturan paket :



Gambar 4.32. Tampilan hasil Pengaturan Paket.

Untuk menambah user profile, klik “+” dan

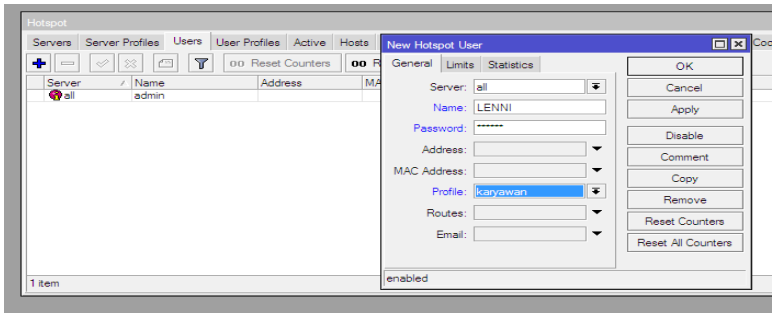


Gambar 4.33. Menambahkan User profile.

.

Setelah selesai melakukan setting, selanjutnya membuat user/ password dan Mac filter untuk masing-masing user.

Menu IP > Hotspot > User

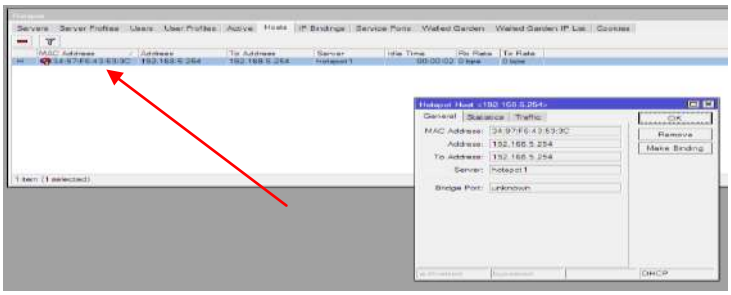


Gambar 4.34. Menambahkan User/password.

- Name – Username untuk HotSpot login
- Password – User password
- Profile – Nama User Profile yang telah di konfigurasi pada menu IP > Hotspot > User Profile.

Untuk melakukan Mac Filter

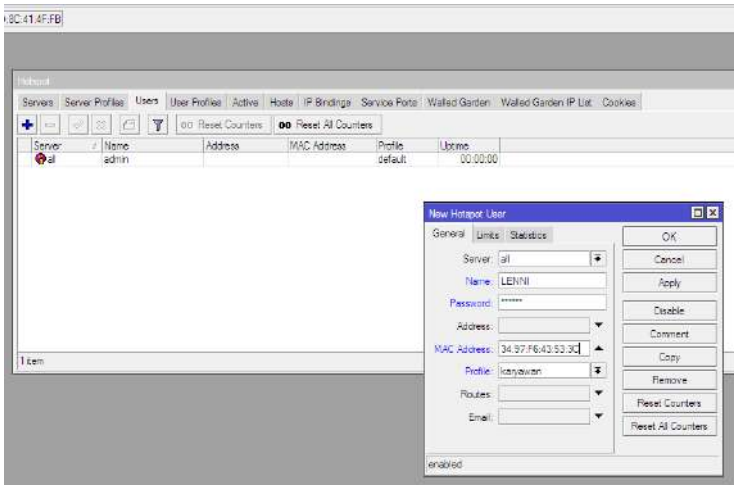
Menu IP > Hotspot > Hotspot



Gambar 4.35. Tampilan Mac Address.

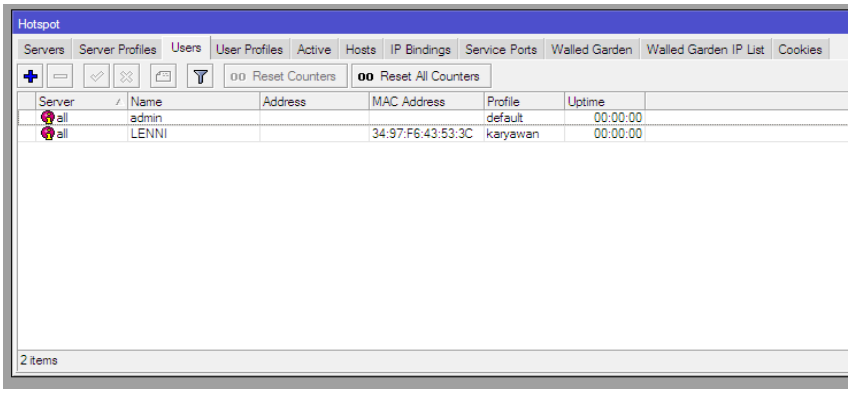
Menambahkan Mac filter sebagai keamanan Jaringan wireless, dengan mendaftarkan Mac address maka user bisa terkoneksi ke jaringan wireless.

Cara mendaftarkan Mac Address.



Gambar 4.36. Mendaftarkan Mac Address Filter.

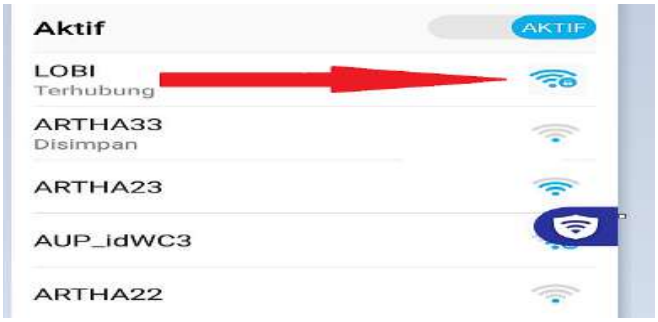
Tampilan hasil setelah mendaftarkan Mac Address :



Gambar 4.37. status Mac Address yang terdaftar.

B.3. Uji Coba Jaringan Wireless

Uji coba koneksi ke jaringan wireless dengan masuk ke jaringan LOBI.



Gambar 4.38. Uji coba koneksi ke jaringan wireless.

Tampilan saat login ke jaringan wireless

Gambar 4.39. Tampilan login ke jaringan wireless LOBI.

Sukses masuk ke jaringan wireless LOBI, dengan hasil bisa terhubung ke internet

:

Gambar 4.40.Berhasil browsing.

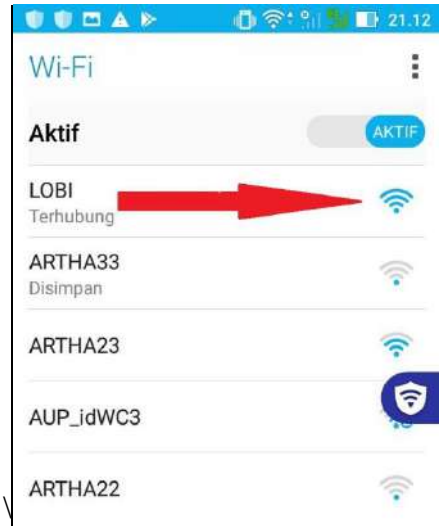
User yang tidak terdaftar maka tidak akan bisa terkoneksi ke jaringan,contohnya sebagai berikut :

Gambar 4.41.Gagal untuk masuk ke jaringan LOBI.

C. Evaluasi Perbandingan Keamanan Wireless

C.1. Jarigan Wireless Sebelumnya

Tampilan keadaan jaringan wireless yang ada di PT.Artha Utama Plasindo sebelum penulis melakukan Implementasi sistem keamanan otentikasi User(password) dan Mac Address Filter ialah sebagai berikut :



Gambar 4.42. Tampilan wireless Tanpa keamanan

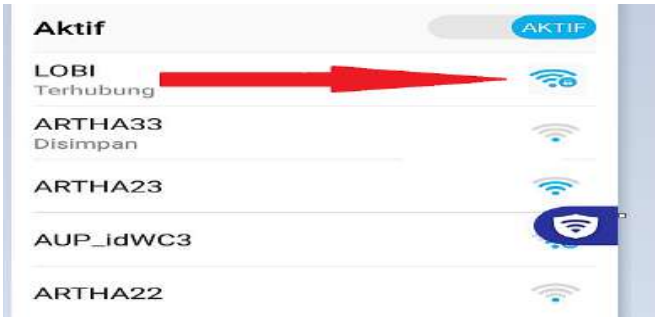
Pada gambar di atas dapat dilihat bahwa jaringan bersifat terbuka tanpa adanya keamanan. Biasanya wireless yang menggunakan keamanan bisa terlihat dengan biasanya ada gambar gembok kecil.

Lebih jelasnya lagi bisa dilihat pada gambar berikut :

Gambar 4.43. Status Wireless

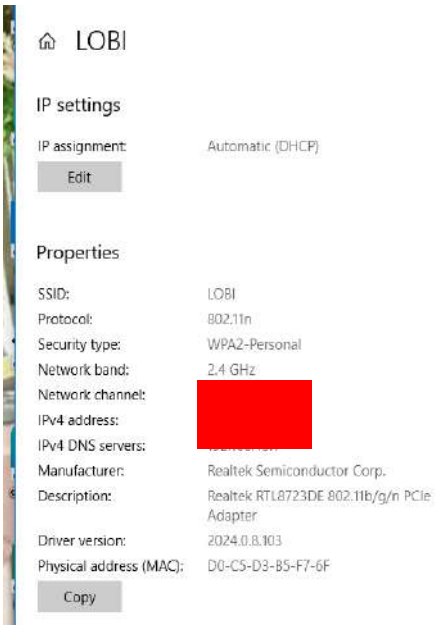
C.2. Jaringan Wireless Sesudah Implementasi

Berikut Tampilan dari jaringan yang sudah dilakukan implementasi keamanan jaringan wireless menggunakan otentikasi User(Password). Dari gambar terlihat bahwa wireless kini berubah pada gambar, pada gambar terlihat ada gambar gembok kecil. Dimana gambar ini merupakan bahwa jaringan memiliki keamanan.



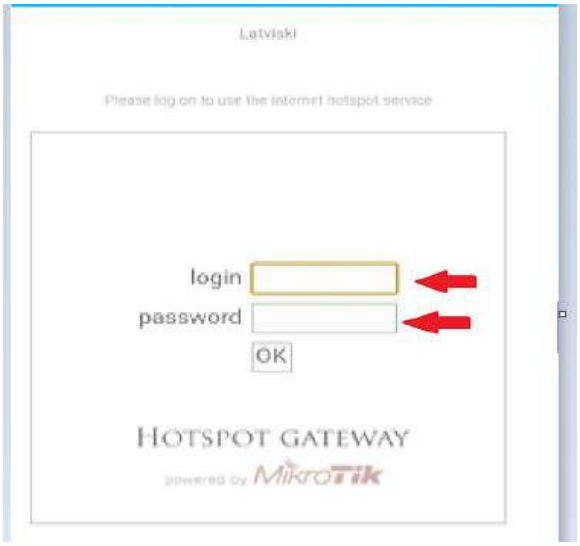
Gambar 4.44. Tampilan Wireless sudah memiliki keamanan

Status keamanan dapat dilihat pada gambar berikut :



Gambar 4.45. Status keamanan *wireless*

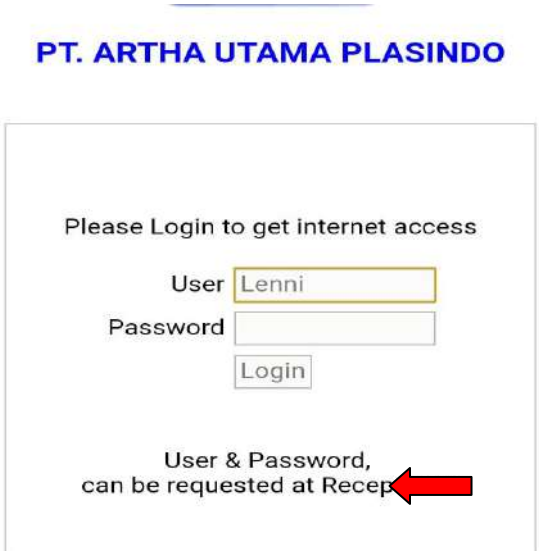
Saat client ingin mencoba terhubung ke wireless, maka client diminta untuk memasukkan User(Password) seperti pada gamabar berikut :



Gambar 4.46. Tampilan Login wireless

Client tidak akan bisa terhubung ke jaringan wireless jika client tersebut tidak memiliki User(password) dimana untuk mendapatkan User(password) tersebut haruslah terlebih dahulu di daftarkn ke administrator. Namun dalam jaringan wireless ini sudah memiliki 2 otentikasi sistem keamanan. Sekalipun client sudah memiliki User(password) teteapi jika Mac Address perangkatnya tidak di daftarkan ke administrator maka client tersebut juga tidak akan bisa terhubung ataupun terkoneksi ke jaringan wireless.

Tampilan saat akses di tolak akibat User(Password) tidak terhubung. Maka akan ada keterangan seperti pada gambar di bawah. Dimana client di perintahkan untuk requested User(Password).



Gambar 4.47. Tampilan Akses di Tolak

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Tahap pertama dari hasil penelitian yang dilakukan dapat disimpulkan bawha implementasi keamanan jaringan *wireless* menggunakan otentikasi *User(Password)* berhasil di terapkan di PT.Artha Utama Plasindo. Dengan adanya otentikasi *Use(/password)* tersebut dapat membatasi client yang terkoneksi ke jaringan wireless, guna untuk memberi pengamanan pada jaringan *wireless* dari orang yang mencoba untuk melakukan aksi yang tidak bertanggung jawab.

Namun Otentikasi keamanan menggunakan *User(Password)* saja tidak cukup, sebab jika ada seseorang mendapatkan *User(Paswword)* dari salah satu karyawan yang sudah terdaftar maka seseorang tersebut bisa memanfatkan *User(password)* tersebut untuk terkoneksi ke *wireless*.

Maka demikian, peneliti merasa perlu menambahkan Otentikasi pengamanan jaringan *Wireless* dengan *Mac Addres Filter* guna untuk meningkatkan keamanan pada jaringan wireless.

Tahap kedua Peneliti berhasil menerapkan Pengamanan jaringan wireless menggunakan *Mac Address Filter* dengan memanfaatkan Mikrotik RB 750. Dalam iplementasi otentikasi ini berhasil dilakukan. Mac Address *Filter* digunakan untuk memfilter client mana saja yang boleh terkoneksi ke jaringan *wireless*. Walaupun client memiliki *User/Password* tetapi jika Mac Address

Perangkat(Laptop/Hp) tidak didaftarkan ke Administrator tetap saja client tersebut tidak dapat akses ke jaringan *Wireless*.

B. SARAN

Saran-saran yang dapat penulis berikan antara lain adalah :

1. Melakukan maintenance pada jaringan wireless secara berkala untuk menjaga serta meningkatkan kinerja jaringan tersebut.
2. Selain otentikasi User/Password Dan Mac filter untuk keamanan jaringan wireless masih ada banyak lagi cara yang bisa dilakukan untuk mengamankan jaringan contohnya dengan cara Hidden SSID.
3. Mikrotik tidak hanya dugunakan untuk setting Mac Address Filter tetapi Mikrotik juga salah satu perangkat lunak yang mampu melakukan fungsi firewall,Bandwidth Management,proxy, Hotspot dan masih banyak fungsi lainya.

DAFTAR PUSTAKA

Novrianda, R. (2017). *Rancang Bangun Keamanan Jaringan Wireless Pada Stiper Sriwigama Palembang Dengan Radius Server, 4*[1].

Nurdin, N. A., & Ardiansyah, S. (2018). *Implementasi Filtering Mac Address menggunakan Fitur Hotspot Dengan Mikrotik Pada PT Pertamina Drilling Service Indonesia Jakarta, 4*[1].

Susianto, D. & Yulianti, I. (2015). *Mengamankan Wireless Dengan Menggunakan Two Factor, Password Dan Mac Address Filtering, 5*[2].

Towidjojo, Rendra. 2016. Mikrotik Kung Fu Kitab 1. Sukmajaya Depok: Jasakom.

Towidjojo, Rendra. 2016. Mikrotik Kung Fu Kitab 2. Sukmajaya Depok: Jasakom.

Zam, E. (2016). Wireless Hacking Temukan Kelemahan Jaringan Wireless Di Sekitar Anda.. Kelompok Gramedia jakarta: PT.Elex Media Komputindo.

Belajar Komputer. 2013. Pengertian IP Address Adalah dan Kelas IP Address. http://www.adalahcara.com/2013/05/pengertian-kelas-ip-address-adalah.html. (diakses 23 juni 2019, pukul 19.00)

Bintara Hengky.Maret 2017.Dasar Keamanan Jaringan Wireless https://netsec.id/author/hengky/ (diakses 26 juni 2019, pukul 16.05)

Susantu Prabekti. 2014. Macam-macam Ancaman dalam Jaringan. https://santisusanti620.wordpress.com/2014/12/28/macam-macam-ancaman-dalam-jaringan/. (diakses 22 juli 2019, pukul 15.25)

UNIVERSITAS SATYA NEGARA INDONESIA

FAKULTAS TEKNIK

Jalan Arteri Pondok Indah No.11 Jakarta Selatan 12240

Telp (021) 7398393 (Hunting), Fax (021) 7200352

Website http://www.usni.ac.id

KARTU BIMBINGAN SKRIPSI/TUGAS AKHIR

FAKULTAS TEKNIK

Nama : Lenni Nalurita Sinaga

No. Mhs : 011401503125016 Prodi : Teknik Informatika

Dosen Pembimbing I : Hernalom Sitorus ST.,M.Kom

Dosen Pembimbing II : Erick Orlando S.kom,M.kom

Judul : Analisis Dan Implementasi Keamanan Jaringan Wireless Pada PT. Atha Utama Plasindo

No	Tanggal	Catatan Pembimbing I	Ttd Dosen Pembimbing
1	25-7-19	Koreksi BAB III dan gambar 2	
2	26-7-19	koreksi BAB IV	
3	29-7-19	Font dan jenis tulisan	
4	30-7-19	Daftar pustaka	
5	31-7-19	REvisi Daftar pustaka, literatur	
6	31-7-19	Penambahan Buku sebagai Acuan.	
7	15-8-19	BAB V kesimpulan dan saran	
8	15-8-19	ACC	

Pembimbing I

Hernalom Sitorus ST.,M.Kom

UNIVERSITAS SATYA NEGARA INDONESIA

FAKULTAS TEKNIK

Jalan Arteri Pondok Indah No.11 Jakarta Selatan 12240

Telp (021) 7398393 (Hunting), Fax (021) 7200352

Website http://www.usni.ac.id

KARTU BIMBINGAN SKRIPSI/TUGAS AKHIR

FAKULTAS TEKNIK

Nama : Lenni Nalurita Sinaga

No. Mhs : 011401503125016 Prodi : Teknik Informatika

Dosen Pembimbing I : Hernalom Sitorus ST.,M.Kom

Dosen Pembimbing II : Erik Orlando S.kom,M.kom

Judul : Analisis Dan Implementasi keamanan jaringan wireless Menggunakan Password Dan Mac Address Filter (Studi Kasus : PT. Atha Utama Plasindo)

No	Tanggal	Catatan Pembimbing II	Ttd Dosen Pembimbing
1	16/06/19	Perbanyak Literatur	
2	20-06-19	koreksi Latar belakang	
3	3-07-19	Penulisan dan gambar	
4	11-07-19	REVisi BAB V	
5	15-07-19	koreksi pada setiap tabel	
6	20-07-19	Cara Penulisan Daftar Pustaka	
7	21-07-19	ukuran font dan Bab IV	
8	22-07-19	ACC Lanjut Sidang	

Pembimbing II

Erik Orlando S.kom,MMSI

PT. Artha Utama Plasindo

SURAT KETERANGAN

Yang bertanda tangan dibawah ini :

Nama	: **Murni Angraini**
Jabatan	: **HRD Personalia**
Perusahaan	: **PT. Artha Utama Plasindo**

Dengan ini menerangkan bahwa :

Nama Mahasiswa	: **LENNI NALURITA SINAGA**
Program Studi	: **TEKNIK INFORMATIKA**
Univesitas	: **UNIVERSITAS SATYA NEGARA INDONESIA (USNI)**

Telah melaksanakan kegiatan penelitian skripsi atau tugas akhir di PT. Artha Utama Plasindo, sejak Tanggal 02 Maret 2019 s.d 30 Juli 2019

Demikian Surata Keterangan ini dibuat dengan sebenarnya agar dapat dipergunakan sebagai mestinya

Bekasi, 26 Agustus 2019

PT. Artha Utama Plasindo

PT. Artha Utama Plasindo

Murni Angraini

HRD PERSONALIA

Tel: (62-21) 89981551 Fax: (62-21) 89981552

Factory/Office: Jl. Flores Blok C1, Kawasan Industri MM2100 Cikarang Barat, Bekasi 17520 - INDONESIA