ISSN : 2085-4218

Rancang Bangun Jaringan Wirelless Di Politeknik Negeri Bengkalis Menggunakan MAC Filtering

Agus Tedyyana
Teknik Informatika Politeknik Negeri Bengkalis
Jl. Bathin Alam, Sungai Alam - Bengkalis
Kode Pos : 28711 Telp. (+62766) 24566
E-mail : agustedyyana@polbeng.ac.id

Abstrak. Pengguna jaringan internet harus mengeluarkan investasi yang tidak sedikit untuk dapat mengakses Internet. Internet telah memberikan pengaruh yang sangat besar pada penyebaran informasi, sehingga semakin banyak orang yang mengakses data melalui Internet. Permasalahan tersebut dapat diatasi dengan menggunakan MikroTik sebagai pengatur lalu lintas data Internet serta melakukan pemfilteran beberapa aplikasi yang dapat mengganggu konektifitas jaringan komputer sesuai dengan aturan yang telah ditetapkan Penelitian ini dilakukan menggunakan beberapa tahapan antara lain : analisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan firewall, desain untuk mendapatkan cara yang paling efektif, aman dan efisien dalam mengimplementasikan penggunaan internet di kampus Politeknik Negeri Bengkalis. IP Address dan *MAC address* pasti dimiliki oleh setiap Network adapter, Ketika wireless klien terhubung dengan router, maka *MAC address* akan terdaftar secara otomatis, pada router inilah sang admin bisa memblok MAC address yang bukan merupakan anggota di kampus Politeknik Negeri Bengkalis. Berdasarkan penelitian yang telah dilakukan aplikasi router menggunakan MikroTik dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran *MAC address* sesuai dengan kebutuhan pengguna.

Kata Kunci: *IP Address*, Jaringan *Internet,* Keamanan Jaringan, *MAC Address*

1. Pendahuluan

Semakin banyaknya permasalahan yang dihadapi dikala menggunakan pemanfaatan teknologi jaringan komputer dan komunikasi, juga semakin tingginya tingkat kebutuhan serta semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri, maka dibutuhkan suatu infrastruktur jaringan yang bagus yang dapat menjawab kebutuhan itu. Suatu infrastruktur jaringan harus dapat melayani lebih banyak user, lebih banyak aplikasi serta lebih banyak workstation.

Internet atau Internetworking secara umum didefenisikan sebagai jaringan komputer terbesar di dunia yang menghubungkan semua jaringan komputer yang ada (Intranet, Wide Area Network, Metropolitan Area Network, Personal Area Network, dan lain-lain) beserta dengan semua komputer, perangkat terhubung (Smartphone, Tablet, Switch, Router, Hub, dan perangkat penghubung lainnya), serta pengguna komputer itu sendiri, ke dalam satu wadah jaringan komputer dunia. [1] Kehadiran berbagai vendor produk wireless yang menyajikan beragam produk dengan harga terjangkau turut andil menjadi pendorong maraknya penggunaan teknologi wireless. Teknologi wireless ini tidak hanya cocok untuk digunakan pada kantor ataupun pengguna bisnis. Kampus juga biasa menggunakan teknologi ini untuk mempermudah konektivitas. Makalah ini lebih ditujukan untuk memberikan informasi mengenai ancaman serta cara cepat dan mudah untuk mengamankan jaringan wireless. teknologi wireless memang relatif lebih rentan terhadap masalah keamanan. Sesuai namanya, teknologi wireless menggunakan gelombang radio sebagai sarana transmisi data. Proses pengamanan akan menjadi lebih sulit karena Anda tidak dapat melihat gelombang radio yang digunakan untuk transmisi data, Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh

ISSN : 2085-4218

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 sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor. Seringkali wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut masih standart bawaan pabrik. Banyak pengguna jaringan wireless tidak bisa membayangkan jenis bahaya apa yang sedang menghampiri mereka saat sedang berasosiasi dengan wireless access point (WAP), misalnya seperti sinyal WLAN dapat disusupi oleh hacker. Berikut ini dapat menjadi ancaman dalam jaringan wireless, di antaranya:

a. Sniffing to Eavesdrop, Paket yang merupakan data seperti akses HTTP, email, dan Iain-Iain, yang dilewatkan oleh gelombang wireless dapat dengan mudah ditangkap dan dianalisis oleh attacker menggunakan aplikasi Packet Sniffer seperti wireshark dan Kismet.
b. Denial of Service Attack, Serangan jenis ini dilakukan dengan membanjiri atau memberikan data secara terus menerus (flooding) jaringan sehingga sinyal wireless berbenturan dan menghasilkan paket-paket yang rusak.
c. Man in the Middle Attack, Peningkatan keamanan dengan teknik enkripsi dan authentikasi masih dapat ditembus dengan cara mencari kelemahan operasi protokol jaringan tersebut. Salah satunya dengan mengeksploitasi Address Resolution Protocol (ARP) pada TCP/IP sehingga hacker yang cerdik dapat mengambil alih jaringan wireless tersebut.
d. Rogue/Unauthorized Access Point, Rogue AP ini dapat dipasang oleh orang yang ingin menyebarkan/memancarkan lagi tranmisi wireless dengan cara ilegal/tanpa izin. Tujuannya, penyerang dapat menyusup ke jaringan melalui AP liar ini.
e. Konfigurasi access point yang tidak benar, Kondisi ini sangat banyak terjadi karena kurangnya pemahaman dalam mengkonfigurasi sistem keamanan AP.

Kegiatan yang mengancam keamanan jaringan wireless di atas dilakukan dengan cara yang dikenal sebagai Warchalking, WarDriving, WarFlying, WarSpamming, atau WarSpying. Banyaknya access point/ base station yang dibangun seiring dengan semakin murahnya biaya berlangganan koneksi Internet, menyebabkan kegiatan hacking tersebut sering diterapkan untuk mendapatkan akses Internet secara ilegal. Tentunya, tanpa perlu membayar.

Mikrotik adalah sistem operasi independen berbasis Linux khusus untuk komputer yang difungsikan sebagai router. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks.[2] MikroTik Router adalah salah satu sistem operasi yang dapat digunakan sebagai penghubung jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan wireless. Selain itu MikroTik dapat juga berfungsi sebagai firewall bagi komputer lain dan memberikan prioritas bagi komputer lain agar bisa mengakses data internet maupun data lokal. MikroTik bertujuan untuk mengatur bandwith serta melakukan manajemen jaringan komputer. Penempatan router MikroTik ditempatkan pada sebuah komputer yang dijadikan sebagai gateway suatu jaringan. Komputer gateway tersebut berfungsi untuk mendistribusikan data keluar masuknya dari dan ke komputer lainnya sehingga seluruh komputer dapat mengakses data bersama-sama seperti Internet sharing.

Pengelolaan jaringan lokal (Local Area Network, LAN) merupakan salah satu alternatif penyelesaian masalah supaya didapatkan layanan yang maksimal. pembagian akses jaringan menggunakan teknologi nirkabel/ wireless saat ini semakin menjadi pilihan. Cakupan area, kemudahan serta sifat flexible pada wireless menjadi alasan admin jaringan menggunakan nya. Alasan keamanan merupakan hal yang sangat penting dalam jaringan komputer, terutama dalam jaringan wireless.

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

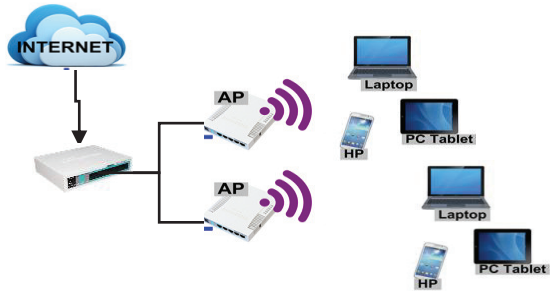
ISSN : 2085-4218

merupakan pemfilteran di atas standar 802.11b untuk mengamankan jaringan. Dalam hal ini setiap MAC address client memiliki alamat fisik yang pasti berbeda untuk setiap cardnya. Cara kerja sistem ini yaitu mendaftarkan alamat MAC address nya agar mendapat otorisasi dari Access Point/ router saat akan berasosiasi. [3]

2. Pembahasan

2.1 Konfigurasi Dasar Mikrotik

Langkah pertama yang harus dilakukan adalah konfigurasi dasar Mikrotik agar dapat menerima akses dari provider. Ada banyak metode yang bisa diterapkan, disesuaikan dengan metode distribusi yang diterapkan oleh provider, metode yang bisa digunakan dalam melakukan distribusi *wireless* ke arah client. adalah point to multipoint. Biasa diterapkan untuk distribusi akses langsung ke arah client. Misal pada mall, cafe, kantor dsb dimana user menggunakan laptop / gadget untuk akses internet.



Gambar 1. Topologi Jaringan

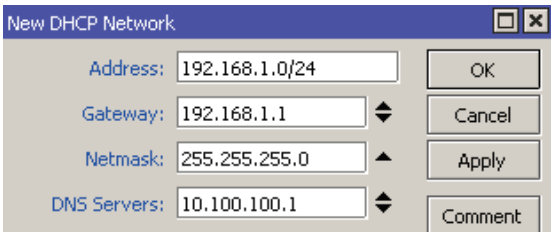
2.2 Pengaturan IPAddress

Pengarturan IP Address menggunakan kelas B dengan asumsi tersedia 1500host yang terhubung ke internet, dengan 2 bangunan utama maka perhitungan IPnya: 1000 host >=1000 host yang sesuai dengan kebutuhan host yang digunakan 2^10= 1024 dan subnet mask 255.255.252.0 atau /22. Untuk mencari nilai IP range seperti dibawah ini:

255.255.255.255
255.255.253.0 -
0. 0. 3. 255

Network: 172.16.0.0/22, IP Pertama: 172.16.0.1, IP Terakhir: 172.16.3.254, IP Broadcast: 172.16.3.255, Subnet Mask: 255.255.252.0, Sedangkan untuk gedung kedua dengan 500 host menggunakan IP: Network: 172.16.0.0/23, IP Pertama: 172.16.0.1, IP Terakhir: 172.16.1.254, IP Broadcast: 172.16.1.255 Subnet Mask: 255.255.254.0. Pada router MikroTik terdapat fitur yang berfungsi untuk manajemen distribusi IP Address, yaitu DHCP *(Dynamic Host Confguration Protocol)*. Diantara fitur DHCP yang sudah didukung oleh MikroTik antara lain DHCP Server, DHCP Client dan DHCP Relay. DHCP Relay merupakan sebuah metode untuk distribusi *IP Address* ke perangkat client dengan memanfaatkan DHCP server yang terpusat pada router lain. Sehingga bisa dikatakan router yang menjadi DHCP relay hanya meneruskan *DHCP Reques*' dari perangkat client ke DHCP server. Hal ini sangat membantu jika perangkat-perangkat client tidak berada dalam satu network dengan DHCP Server [4] DHCP merupakan salah satu keunggulan dari Ipv4, dimana dengan DHCP tersebut alamat IP dan subnetmask dapat diberikan otomatis oleh *server* ketika komputer baru akan terhubung ke dalam suatu jaringan. [5] Untuk menambahkan *network* yang akan mendapatkan distribusi IP Address dari DHCP server tersebut. Pilih menu IP -> DHCP Server -> Networks.

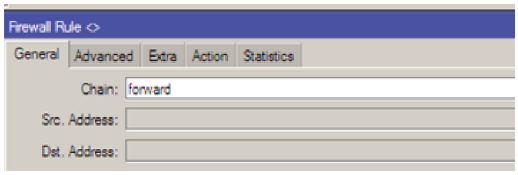
ISSN : 2085-4218



Gambar 2. *Pengaturan DHCP (192.168.1.0/24)*

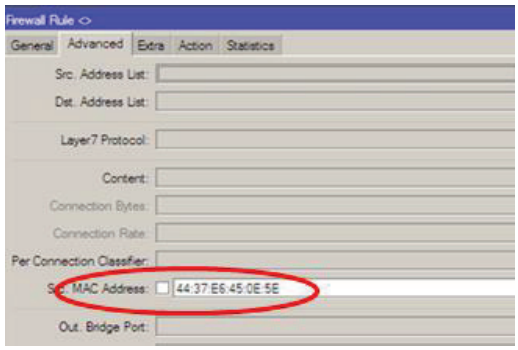
2.3 Access List Filter dan MAC Filter

Access list untuk membuat manajemen *wireless* client berdasarkan *MAC Address*. Dengan pengaturan tersebut tidak semua client bisa terkoneksi, hanya client dengan *MAC address* yang sudah terdaftar pada Access-List yang dapat terkoneksi. Proses blocking akses client dengan *MAC address* dilakukan Settingan pada mikrotik dapat dilakukan dengan cara:
pilih IP>>Firewall>>general
Chain = forward
Out interface = ether3_WAN



Gambar 3. Pengaturan Akses Internet

Alamat MAC yang unik ditugaskan untuk setiap kartu, sehingga dengan MAC filtering pada izin jaringan dan menolak akses jaringan ke perangkat tertentu melalui penggunaan *blackliast* dan *Whitelist*, Sedangkan pembatasan akses jaringan melalui penggunaan daftar sangat mudah, seorang individu tidak diidentifikasi oleh alamat MAC, bukan perangkat saja, jadi orang yang berwenang akan perlu memiliki entri daftar putih untuk setiap perangkat yang ia akan menggunakan untuk mengakses jaringan.



Gambar 4. Pemberian akses terhadap MAC Address

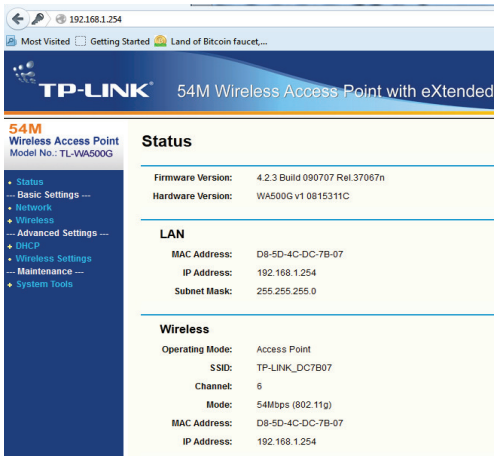
MAC filter fungsinya untuk menseleksi komputer mana yang boleh masuk ke dalam jaringan berdasarkan MAC Address. Bila tidak terdaftar, tidak akan bisa masuk ke jaringan MAC filter Address akan membatasi user dalam mengakses jaringan *wireless*. Alamat MAC dari perangkat komputer user akan didaftarkan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

2.4 Konfigurasi Access Point

Wireless Access Point berfungsi untuk menghubungkan beberapa *wireless* klien dengan perangkat jaringan atau komputer-komputer yang tergabung dalam sebuah jaringan. Bila diibaratkan jaringan berkabel, *Wireless* Access Point ini dianggap sebagai Hub atau Switch. *Wireless* Access

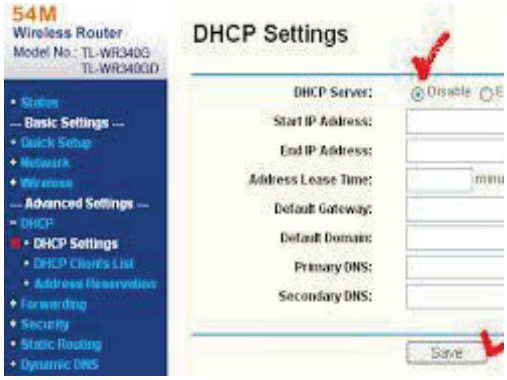
ISSN : 2085-4218

Point digunakan untuk membuat jaringan WLAN (*Wireless* Local Area Network) ataupun untuk memperbesar cakupan jaringan wifi yang sudah ada (menggunakan mode bridge).
Access Point berfungsi sebagai Hub/Switch yang bertindak untuk menghubungkan jaringan lokal dengan jaringan *wireless*/ nirkabel, di access point inilah koneksi data/ internet dipancarkan melalui gelombang radio, ukuran kekuatan sinyal juga mempengaruhi area coverage yang akan dijangkau, semakin besar kekuatan sinyal (ukurannya dalam satuan dBm atau mW) semakin luas jangkauannya.



Gambar 5. Konfigurasi Acces Point1

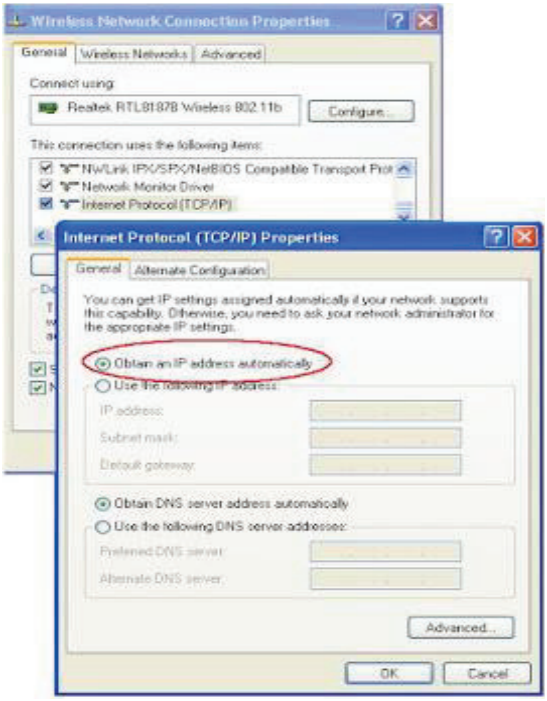
Access point memiliki kemampuan untuk mendistribusikan alamat IP ke *wireless* klien secara otomatis. Sedangkan *wireless* router dapat bertindak sebagai DHCP Server. DHCP Server biasanya hanya bisa dijalankan pada perangkat router ataupun server.



Gambar 6. Konfigurasi Acces Point2

Memastikan bahwa pengaturan TPC IP pada *Wireless* Network Connetion sudah menggunakan Obtain IP Address Automatically seperti pada gambar 8 berikut:

ISSN : 2085-4218



Gambar 7. Konfigurasi Ip di client

3. Kesimpulan

1 *MAC Address* filtering merupakan metoda filtering untuk membatasi hak akses dari *MAC address* yang akan terkoneksi ke internet. Hampir setiap wirelees access point maupun router difasilitasi dengan keamanan yang baik dalam WLAN
2 Proses blocking *MAC address* bersifat tetap untuk sebuah client yang di drop, karena IP tersebut bersifat DHCP.
3 Manfaat MAC Filter Sebagai Salah satu alternatif untuk mengurangi kelemahan jaringan *wireless* karena hampir setiap *wireless* access point maupun router difasilitasi dengan keamanan MAC Filtering.
4 Dengan sistem mendeteksi *MAC Address* maka hanya PC yang telah di registerkan *MAC Address* nya yang akan terkoneksi internet.

4. Daftar Pustaka

[1] I Putu Agus Eka Pratama, 2014, "Handbook Jaringan Komputer Teori dan Praktik Berbasiskan Open Source," Informatika Bandung
[2] Imam Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik", JUSI Vol. 1, No. 1 ISSN 2087-8737, Februari 2011
[3] Jutono Gondohanindijo, "Sistem Keamanan Jaringan Nirkabel," Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei 2012
[4] MikroTik Team's, "Distribusi DHCP pada Jaringan Multihop" http://mikrotik.co.id/artikel.php, Desember0, 2015
[5] Winarno Sugeng, 2010, "Jaringan Komputer Dengan TCP/IP," Modula Bandung