p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

IMPLEMENTASI *WIRELESS CLIENT* PADA PT.MNC *TELEVISI NETWORK (iNEWS)* MENGGUNAKAN *MIKROTIK ACCESS LIST CAPsMAN*

Mohamad Yudha Bayhaky[1)] **, Aziz Setyawan Hidayat**[2)] **, Yamin Nuryamin**[3)]
[1,2),] *Teknik Informatika, STMIK Nusa Mandiri*
Jl. Margonda Raya No. 545, Pondok Cina Depok, Jawa Barat
Email : myudhatkj3@gmail.com[1)]*,aziz.aiz@bsi.ac.id*[2)]*,yamin.yny@nusamandiri.ac.id*[3)]

Abstrak

PT. MNC Televisi Network (iNews) merupakan salah satu stasiun televisi swasta di Indonesia. Penelitian yang dilakukan di PT. MNC Televisi Network ini akan memanfaatkan fitur dari *router mikrotik* untuk mengatasi permasalahan yang ada pada sistem keamanan jaringan *wireless* dan memanfaatkan *router mikrotik* untuk mengontrol banyak *access point* secara terpusat. Masalah yang dihadapi pada keamanan jaringan *wireless*nya hanya menggunakan *authentication* WPA2-PSK, sehingga apabila orang asing mengetahui *password* akan rawan untuk penyalahgunaan lalu lintas. Selain itu dibutuhkan fitur untuk memonitor perangkat-perangkat yang masuk kedalam jaringan *wireless* untuk mengendalikan *access point* secara terpusat. Tujuan dari penelitian ini adalah untuk menambahkan keamanan jaringan *wireless* dengan menggunakan *access list.* Dalam metode *access list,* admin jaringan mempunyai hak untuk memberikan hak akses internet kepada *client* dan admin jaringan juga berhak menutup akses jaringan *wireless* dengan tujuan agar orang asing tidak dapat masuk kedalam jaringan *wireless* walaupun sudah mengetahui *password* dari jaringan *wireless* tersebut. Tujuan dari penelitian ini adalah untuk memanfaatkan *CAPsMAN* sebagai pengontrol *access point*, sehingga memudahkan IT *Network* untuk mengatur semua perangkat *access point* yang terhubung dengan *CAPsMAN*.

Kata kunci: ***Access List; CAPsMAN; Access Point; Wireless; Jaringan***.

Abstract

PT. MNC Televisi Network (iNews) is one of the private television stations in Indonesia. Research conducted at PT. This MNC Television Network will take advantage of the features of the Mikrotik router to solve problems that exist in the wireless network security system and utilize the Mikrotik router to control many access points centrally. The problem faced in the security of the wireless network is only using WPA2-PSK authentication, so that if a stranger knows the password, it is prone to traffic misuse. In addition, a feature is needed to monitor devices that enter the wireless network to control the access point centrally. The purpose of this research is to add wireless network security by using an access list. In the access list method, the network admin has the right to grant internet access rights to clients and the network admin is also entitled to close wireless network access in order to prevent foreigners from entering the wireless network even though they already know the password of the wireless network. The purpose of this research is to utilize CAPsMAN as access point controller, making it easier for IT Networks to manage all access point devices connected to CAPsMAN.

Keywords: Access List; CAPsMAN; Access Point; Wireless; Network.

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

1. PENDAHULUAN

Pengguna jaringan internet di indonesia terus meningkat seiring berkembangannya teknologi informasi di dunia yang begitu pesat. Kebutuhan untuk mengakses internet sangatlah tinggi, mulai dari mencari informasi, berkomunikasi seperti *chatting* atau video *call*, mencari artikel, bermain game *online*, *streamimg*, belajar *online* dan jual atau belanja *online*. Banyak orang menggunakan akses internet untuk kebutuhan sehari-hari sebagai contohnya untuk metode belajar atau untuk menjalani pekerjaan. Salah satunya untuk mengakses internet yaitu menggunakan *wifi*. Kini *wifi* banyak digemari sebagai alternatif penggunaan paket data. *Wifi* tidak lagi menggunakan kabel sehingga mempermudah untuk bertukar data dan mengakses internet.

Serangan terhadap keamanan jaringan sering terjadi khususnya di dunia maya yang dilakukan perorangan atau sekelompok orang yang ingin masuk kedalam sistem jaringan tersebut. Dalam hal ini terntunya dibutuhkan keamanan jaringan untuk mencegah pihak luar tidak masuk kedalam sistem jaringan.

Dalam reverensi jurnal [1] Jaringan *Wireless* menggunakan sinyal gelombang radio untuk media transmisinya dan mempunyai sedikit kelemahan yaitu pada konfigurasi. Beragam macam vendor yang menyediakan fasilitas yang baik memiliki maksud untuk memudahkan pengguna dan *administrator*. Banyak juga jaringan *wireless* yang digunakan masih dengan settingan bawaan vendor contohnya seperi SSID, IP Address, DHCP *enable*, *Remote* Manajemen, kanal frekuensi, tanpa enkripsi bahkan *user/password* untuk administrasi *wireless* tersebut masih bawaan pabrik.

Dalam [2] berpendapat *access list* biasanya digunakan untuk *filltering* paket yang tidak diperbolehkan pada saat penerapan kebijakan keamanan. *Access list* memberikan izin atau tidak pernyataan yaitu *fillter traffic* dapat ke bagian jaringan dan dari segi pembagian jaringan bersumber dari source address, destination address, tipe protokol dan port dari paket.

PT. MNC Televisi Network (iNews) adalah sebuah stasiun televisi swasta di Indonesia. Dalam penelitian di PT. MNC Televisi Network penulis menemukan kelemahan pada keamanan jaringan *wireless* yang ada dan dapat terjadi suatu permasalahan, yaitu PT. MNC Televisi Network dalam keamanan jaringan *wireless* nya menggunakan keamanan WPA2-PSK. Keamanan jaringan *wireless* tersebut dapat digunakan oleh orang asing apabila sudah mendapatkan *password* tanpa ada persetujuan dari seorang administrator, dan rawan untuk terjadi penyalahgunaan lalu lintas jaringan pada orang asing. Selain itu banyaknya *access point* pada PT. MNC Televisi Network dibutuhkan fitur yang dapat mengontrol banyak *access point* secara bersamaan.

2. METODE PENELITIAN

2.1. Metode Pengumpulan Data

a. Observasi

Penulis melakukan riset atau kunjungan ke PT. MNC Televisi Network (iNews) untuk mengamati secara langsung jaringan yang sedang berjalan dan penulis mengusulkan skema jaringan usulan untuk meminimalisir permasalahan dalam jaringan yang sudah ada.

b. Wawancara

Dalam penulisan skripsi ini, penulis melakukan wawancara atau tanya jawab dengan karyawan divisi IT mengenai kegiatan-kegiatan yang berhungan dengan penggunaan jaringan di PT. MNC Televisi Network (iNews).

c. Studi Pustaka

Penulis mencari informasi-informasi untuk mendapatkan referensi baik dalam bentuk kertas seperti buku ataupun digital seperti jurnal dan *e-book* dengan tujuan

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

mendapatkan data yang teoritis sesuai dengan judul skripsi yang diambil oleh penulis.

2.2. Analisa Penelitian

a. Analisa Kebutuhan

Untuk meng-implementasikan sistem ini maka penulis membutuhkan 1 Mikrotik router Wireless type RB952Ui-5ac2nD (Hap-AC-Lite), 1 laptop sebagai server, 1 laptop sebagai client dan 1 unit handphone sebagai client.

b. Desain

Pada tahap ini penulis menggunakan *software Draw.io* untuk menggambarkan skema jaringan usulan yang menjadi bahan penelitian yang menghubungkan perangkat jaringan seperti router, komputer dan laptop.

c. Testing

Pada tahap ini penulis melakukan pengujian menggunakan perangkat Mikrotik dan *software* Winbox untuk konfigurasinya. Dengan tujuan menjalankan sistem jaringan *wireless* berjalan dengan baik atau tidak.

d. Implementasi

Tahap akhir dalam penelitian ini adalah memonitoring perangkat yang terkoneksi kedalam jaringan *wireless* apabila MAC Address sudah didaftarkan oleh seorang network administrator maka client atau karyawan tersebut bisa mengakses internet, dan memantau user yang sudah terkoneksi dengan jaringan.

2.3. Tinjauan Jurnal

a. Jaringan Komputer

Dalam buku [3] Jaringan komputer adalah jaringan tele-komunikasi yang memberikan izin *node-node* dengan tujuan agar dapat saling berbagi informasi. Sehingga masing-masing komputer yang tersambung dapat ber-komunikasi satu sama lain.

b. Mikrotik

Menurut jurnal [4] Mikrotik merupakan sistem operasi komputer dan *software* komputer agar komputer dapat diaplikasikan menjadi sebuah *router*. Ada 2 jenis mikrotik yaitu dalam bentuk sistem operasi mikrotik (OS) dan mikrotik *board*. Mikrotik *board* ini didalamnya sudah termasuk dengan sistem operasi mikrotik sehingga tidak menggunakan komputer, cukup dengan *board*.. Router mikrotik ini mencakup untuk IP *Network* dan *Wireless.*

c. Winbox

Dalam buku [5] Untuk melakukan konfigurasi pada server mikrotik tentunya kita membutuhkan aplikasi untuk melakukan remote salah satu *software* yang bisa digunakan adalah Winbox. Aplikasi winbox ini bisa dikonfigurasi mode GUI dan bisa disetting pada sisi *client*, apabila ingin melakukan konfigurasi *test mode* maka bisa disetting dengan menggunakan PC itu sendiri.

d. CAPsMAN

CAPsMAN adalah sebuah fitur pada *mikrotik* yang berfungsi untuk mengendalikan *Access Point* secara terpusat. Fitur CAPsMAN dapat mengontrol banyak *Access Point* sehingga mempermudah konfigurasi jaringan nirkabel pada *Router Mikrotik* CAPsMAN[6].

e. Access List

Menurut jurnal [7] Access list merupakan suatu fungsi yang dipakai dari di sisi AP (Access Point) untuk menjalankan sebuah *filltering* koneksi dari pengguna. Sehingga AP dapat memilih client yang dapat tersambung dengan menggunakan MAC *Address* dan signal-range.

3. HASIL DAN PEMBAHASAN

3.1. Jaringan Usulan

Berdasarkan penelitian yang telah dilakukan oleh penulis pada jaringan yang ada di PT. MNC Televisi

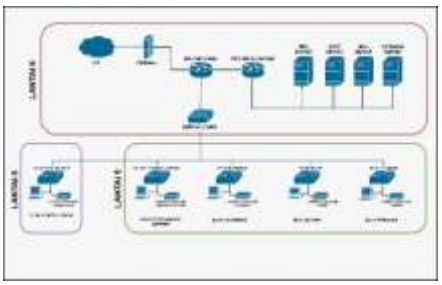
p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

Network ada sedikit kekurangan pada jaringan *wireless* dan mengusulkan untuk mengimplementasikan *wireless* menggunakan *access list* capsman. Metode *access list* ini merupakan salah satu fitur keamanan jaringan *wireless* yang disediakan oleh mikrotik sedangkan capsman merupakan fitur pada mikrotik yang berfungsi untuk mempermudah konfigurasi banyak *access point* secara bersamaan. Penulis menggunakan perangkat *mikrotik* dan software *winbox* untuk merancang dan mensimulasikan jaringan usulan pada proses implementasinya.

3.2. Topologi Jaringan

Berdasarkan analisa di PT. MNC Televisi Network penulis tetap mempertahankan topologi jaringan yang ada yaitu topologi *tree*. Karna topologi *tree* ini menyediakan ruang untuk ekspansi jaringan masa depan, selain itu topologi *tree* ini juga mudah untuk mendeteksi kerusakan atau kesalahan dan memungkinkan untuk jaringan *point to point*

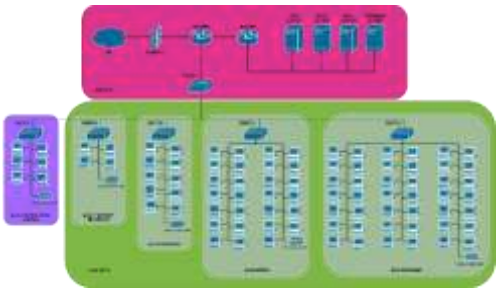
Penulis tidak memberikan topologi usulan dan tidak menambah perangkat jaringan, disini penulis memberikan usulan pada sistem keamanan jaringan nirkabel dengan mengimplementasi *wireless* dengan menggunakan *access list* capsman.



Gambar 1. Topologi Jaringan Usulan

3.3. Skema Jaringan

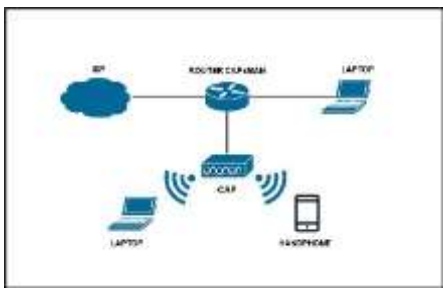
Pada Infrastruktur Jaringan Wide Area Network (WAN) di PT. MNC Televisi Network menurut penulis sudah sangat baik, penulis hanya mengusulkan sistem keamanan *wireless access list* dan implementasi capsman untuk efisien waktu dalam proses konfigurasi *access point* secara bersamaan serta memonitor perangkat yang masuk kedalam jaringan *wireless*.



Gambar 2. Skema Jaringan Usulan

3.4. Rancangan Aplikasi

Dalam rancangan aplikasi, penulis akan merancang untuk meng-implentasikan *wireless client* metode *access list* capsman dengan menggunakan *router* mikrotik RBD52G-5HacD2HnD-TC hAP-AC2 *router wireless* dan untuk konfigurasi menggunakan *software* winbox. Berikut gambar 3 dibawah ini merupakan jaringan *wireless* yang akan dirancang oleh penulis.



Gambar 3. Rancangan Aplikasi

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

Pada rancangan aplikasi penulis melakukan konfigurasi *access list capsman* dengan menggunakan perangkat *mikrotik* dan menggunakan *software winbox*. Berikut adalah implementasinya :

1. Interface

Penjelasan gambar 4 :

Untuk dapat mengakses jaringan *wireless* perlu mengaktifkan *wlan* pada bagian interface. Cara mengkatifkannya cukup klik tanda centang pada bagian *wlan*. Disini penulis membuat 2 jaringan *wlan* untuk membuat 2 SSID yang berbeda. Untuk konfigurasi *command line* harus dicek terlebih dahulu urutan keberapa wlan pada router tersebut. Pada router tipe mikrotik RBD52G-5HacD2HnD-TC hAP-AC2 *router wireless* pada urutan 0 sampai 4 digunakan untuk ether, sedangkan 5 sampai 6 digunakan untuk jaringan *wlan*.

Keterangan : Konfigurasi GUI

Gambar 4. *WiFi Interface*

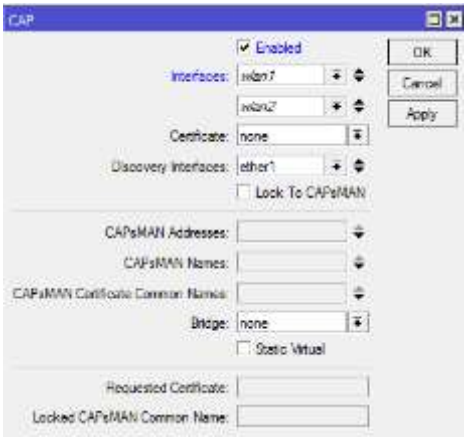
Keterangan : Konfigurasi *command line*
#interface print
#interface *wireless* enable wlan1,wlan2

2. *Wireless*

Penjelasan gambar 5 :

Pada *mikrotik* ini terdapat fitur CAP di *WiFi Interface* yaitu perangkat *wireless* yang dapat dikonfigurasi secara terpusat yang nantinya dikontrol oleh CAPsMAN. Aktifkan fitur CAP ini, untuk *interface* arahkan ke wlan1 dan wlan 2. Pada *discovery interface* ini arahkan ke ether1 yang merupakan jalur untuk me*remote* ke CAP.

Keterangan : Konfigurasi GUI



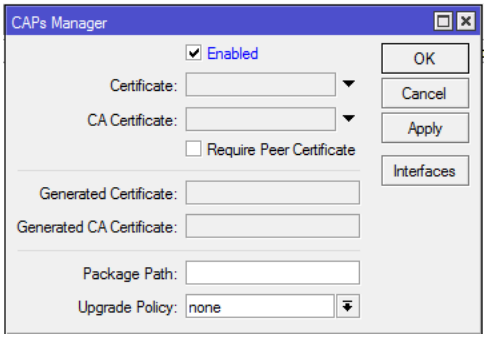
Gambar 5. CAP

3. CAPsMAN

Penjelasan gambar 6 :

Pada fitur CAPsMAN ini aktifkan CAPs Manager dengan memberi tanda centang pada kolom *enabled* yaitu perangkat yang digunakan untuk mengatur CAP, lalu simpan *Apply* dan OK.

Keterangan : Konfigurasi GUI



Gambar 6. *CAPs Manager*

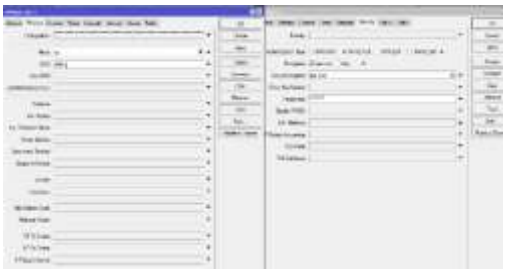
Keterangan : Konfigurasi *command line*
#caps-man manager set enabled=yes

Penjelasan gambar 7 :

Pada fitur CAPsMAN tab *general* penulis berikan nama *interface* wlan= "cap1" sebagai *access point 1*. Pada tab *wireless* menggunakan mode *access point* (ap) dan buat SSID sesuai keinginan, disini penulis membuat SSID "sidang" untuk

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

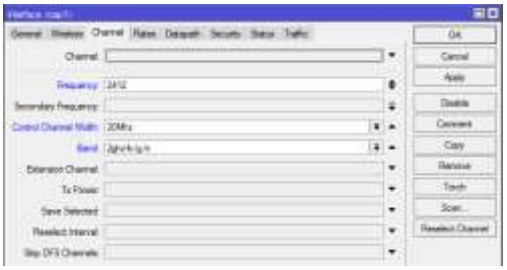
cap1. Lalu buat *security* sebagai keamanan jaringan *wireless*-nya, untuk *authentication*nya menggunakan WPA2-PSK dengan enkripsi aes ccm. Pada kolom *passphrase* adalah *password* yang ingin digunakan, disini penulis memberikan password "123sidang" untuk SSID "sidang".



Gambar 7. *Interface* cap1

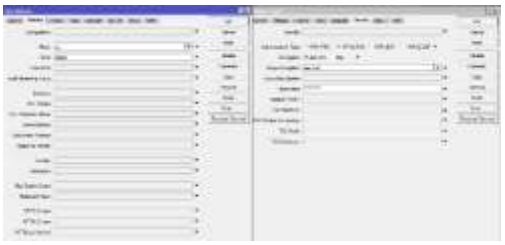
Keterangan : Konfigurasi *command line*
#capsman
#interface add configuration.mode=ap configuration.ssid=sidang
#interface set security.authentication-types=wpa2-psk security.encryption=aes-ccm security.group-encryption=aes-ccm security.passphrase=123sidang

Penjelasan gambar 8 :
Pada pengaturan parameter *channel* cap1 di kolom *control channel width* pilih 20Mhz yang merupakan channel standart yang berbanding lurus dengan throughput data. Dengan menggunakan mode band 2ghz b/g/n maka berkerja di *frequency* 2412 atau 2,4 Ghz lalu simpan *Apply dan OK*.



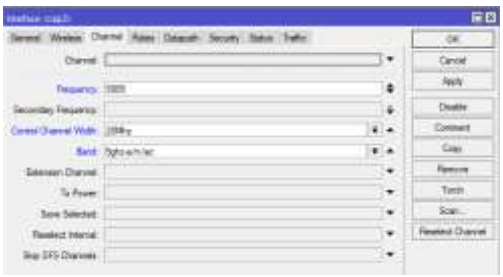
Gambar 8. *Channel* cap2

Penjelasan gambar 9 :
Disini penulis ingin membuat 2 jaringan *wlan*, konfigurasinya sama seperti cap1 yaitu pada tab *general* berikan nama *interface* wlan= "cap2" sebagai *access point* 2. Pada tab *wireless* menggunakan mode *access point* (ap) dan buat SSID sesuai keinginan, disini penulis membuat SSID "skripsi" untuk cap2. Lalu buat *security* untuk keamanan jaringan *wireless*-nya, pada kolom *authentication* penulis menggunakan tipe WPA2-PSK dengan enkripsi aes ccm. Pada kolom *passphrase* isikan *password* yang ingin digunakan, penulis memberikan password "123skripsi" untuk SSID "skripsi".



Gambar 9. *Interface* cap2

Penjelasan gambar 10 :
Pada pengaturan parameter *channel* dicap2 kolom *control channel width* pilih 20Mhz yang merupakan channel standart yang berbanding lurus dengan throughput data. Dengan menggunakan mode band 5ghz b/g/n maka berkerja di *frequency* 5805 atau 5 Ghz lalu simpan *Apply* dan OK.



Gambar 10. *Channel* cap2

Keterangan : Konfigurasi *command line*

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

#caps-man interface set channel.frequency=5805 channel.control-channel-width=20mhz channel.band=5ghz-a/n/ac numbers:cap2

4. IP Address

Penjelasan :

Berikutnya buat IP Address, penulis memakai IP Kelas C diantaranya adalah :

a. 192.168.42.2/24 = Merupakan IP yang diperuntukan untuk *client* yang connect kedalam *wireless* dan arahkan *interface* ke ISP.
b. 192.168.100.11/24 = Merupakan IP yang dipakai untuk koneksi ke ISP dan arahkan *interface* ke *cap1* yang merupakan *interface* wlan1.
c. 192.168.101.11/24 = Merupakan IP yang digunakan untuk koneksi ke ISP dan arahkan *interface* ke *cap2* yang merupakan interface wlan2.

Keterangan : Konfigurasi *Command line*

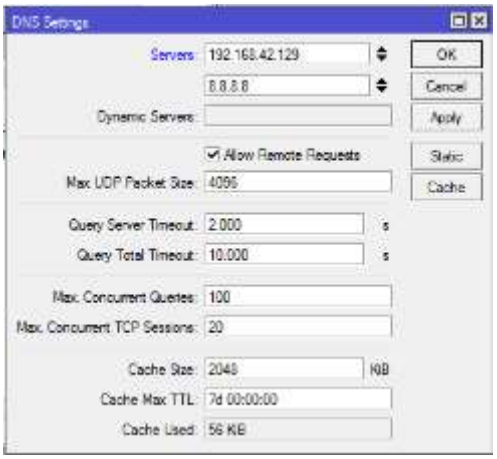
#add address=192.168.42.2/24 interface =ISP
#add address=192.168.100.11/24 interface=cap1
#add address=192.168.101.11/24 interface=cap2

5. IP DNS

Penjelasan gambar 11 :

Selanjutnya mengatur DNS, untuk IP DNS Servers gunakan IP ISP yang kita gunakan yaitu 192.168.42.129, lalu tambahkan IP 8.8.8.8 yang merupakan IP *google* dan berikan tanda ceklis pada *Allow Remote Requests*. Lalu simpan dengan klik *Apply* dan Ok.

Keterangan : Konfigurasi GUI



Gambar 11. IP DNS

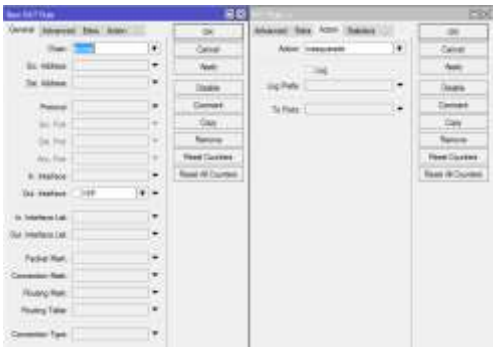
Keterangan : Konfigurasi *Command line*

#setservers=192.168.42.129,8.8.8.8 allow-remote-access=yes

6. Firewall

Penjelasan gambar 12 :

Berikutnya atur pada fitur *firewall*, tab NAT *General* pada kolom *chain* pilih "srcnat" dan arahkan *out interface* kedalam jaringan ISP. Disini penulis untuk jaringan ISP berada pada *interface* wlan "ISP". Pada fitur NAT klik tab *Action* lalu pilih masquerade lalu simpan *Apply* dan *Ok*. Fungsi dari Action masquerade ini adalah mengubah IP Private pada mikrotik menjadi IP Publik.



Gambar 12. *Firewall*

Keterangan : Konfigurasi *Command line*

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

#ip firewall nat add chain=srcnat out-interface=ISP action=masquerade

7. IP Route

Penjelasan :

Langkah selanjutnya mengatur IP route, pada IP route ini isikan dst address 0.0.0.0/0 dan IP Gateway menggunakan IP ISP yang kita gunakan yaitu 192.168.42.129 lalu simpan *Apply* dan OK.

Keterangan : Konfigurasi *Command line*
#ip route add gateway=192.168.42.129

8. DHCP Server

Penjelasan :

Selanjutnya buat IP DHCP yang diperuntukan untuk *client* yang *connect* kedalam jaringan *wireless*. Disini penulis membuat 2 jaringan *wireless* untuk 2 SSID yang akan digunakan. Buat 2 *interface* yaitu *cap1* dan *cap2* yang merupakan koneksi untuk IP DHCP. Pada fitur DHCP ini penulis mengatur Lease Time 1 *day*, yang berfungsi apabila IP DHCP sudah 1 hari maka IP akan secara otomatis berubah. Pada DHCP Server ini penulis mengatur *range* atau batasan IP yang dapat digunakan untuk jaringan *wireless* pada *client*. IP yang digunakan mulai dari 192.168.100.12 sampai 192.168.100.254 untuk client *cap1* sedangkan IP yang digunakan mulai dari 192.168.101.11 sampai 192.168.101.254 untuk client *cap2*.

Keterangan : Konfigurasi *command line*
#ip pool add name=dhcp_pool1 ranges=192.168.100.12-192.168.100.254
/ip dhcp servers
#network add address=192.168.100.0/24 gateway=192.168.100.11 dns-servers=192.168.42.129,8.8.8.8 enable 0
#ip pool add name=dhcp_pool2 ranges=192.168.101.12-192.168.101.254
/ip dhcp servers
#network add address=192.168.101.0/24 gateway=192.168.101.11 dns-servers= 192.168.42.129,8.8.8.8 enable 0

9. CAPsMAN Registration Table

Penjelasan :

Lalu pada tab Registration Table di fitur CAPsMAN ini merupakan perangkat yang masuk kedalam jaringan *wireless* SSID "sidang" dan sudah mendapatkan akses internet dikarenakan *action reject* pada *access list* belum dibuat.

Keterangan : Konfigurasi *command line*
#**caps-man**
#registration-table print

Penjelasan gambar 13 :

Untuk tahap ini merupakan hak dari admin jaringan untuk memberikan izin koneksi kepada client atau tidak. Apabila diizinkan MAC Address harus di *copy to access list*.

Keterangan : Konfigurasi GUI

Gambar 13. CAPs AP *client*

Keterangan : Konfigurasi *command line*
#caps-man access-list
#add mac-address 24:FD:52:E4:ED:00 interface=any action=accept

10. Selanjutnya pada tab Access List, tambahkan *Action reject* dan arahkan ke *interface* "*any"*. Pada kolom *interface* merupakan CAP atau *access point* mana yang ingin di*remote*, disini penulis menggunakan "*any*" artinya untuk

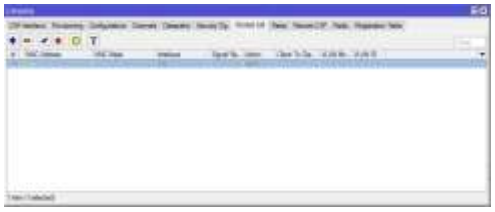
p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

keseluruhan CAP atau *access point* yang ada dengan *action "reject"* yang di*manage* oleh CAPsMAN. *Action reject* ini apabila diaktifkan maka perangkat lain yang ingin masuk kedalam SSID akan tidak bisa *connect*. Jadi apabila ada karyawan baru maka wajib mengkonfirmasi kepada admin jaringan agar MAC Address karyawan tersebut didaftarkan kedalam *access list* untuk mendapatkan akses internet.

Keterangan : Konfigurasi *command line*
#caps-man access list
#add interface=any action=reject

11. Setelah *action reject* dibuat akan secara otomatis tampil di parameter *access list* dan masih dalam keadaan disable. pada pabila perangkat MAC Address sudah di daftarkan dari Registration Table ke *access list* oleh seorang *administrator* maka perangkat yang berada pada *access list* ini sudah mendapatkan hak akses internet.

Keterangan : Konfigurasi GUI

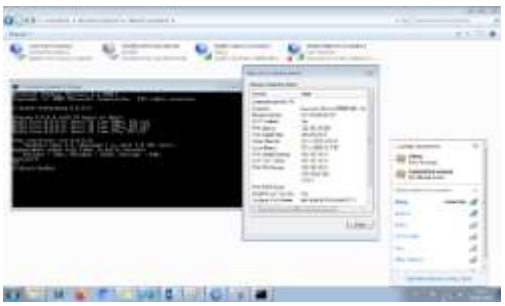


Gambar 14. *Access List Reject*

3.5. Pengujian Jaringan

3.5.1. Pengujian Jaringan Awal

Tahap pengujian awal ini merupakan hasil dari jaringan yang belum menggunakan metode *access list* dimana perangkat yang berhasil masuk kedalam SSID sidang dengan menggunakan password akan mendapatkan akses internet *wireless* dan akan mendapatkan IP secara DHCP sesuai dengan *range* yang ditentukan. Seperti gambar 15 adalah hasil test ping dan dhcp server.
Keterangan: IP yang didapatkan 192.168.100.253



Gambar 15. Pengujian Jaringan Awal Laptop

Penulis juga melakukan pengujian awal pada perangkat handphone menggunakan SSID "skripsi" dengan *password* "123skripsi". Pada pengujian ini juga belum menggunakan *access list* dan secara otomastis akan terhubung ke jaringan serta mendapatkan IP secara DHCP untuk jaringan *wireless*nya.

Keterangan : IP yang didapatkan 192.168.101.254

Gambar 16. Pengujian Jaringan Awal di Handphone

3.5.2. Pengujian Jaringan Akhir

Pada tahap pengujian jaringan akhir ini sudah menggunakan metode *access list* dan *reject* pada *access list* sudah diaktifkan jadi apabila ada perangkat yang ingin masuk kedalam SSID maka tidak akan bisa masuk kedalam jaringan *wireless* dikarenakan MAC Address perangkat tersebut tidak didaftarkan kedalam *access list*. Jadi apabila ada karyawan baru wajib

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

untuk mengkonfirmasi ke admin jaringan agar mendapatkan hak akses internet. Pada gambar 23 merupakan tampilan *access list* yang sudah diizinkan masuk berdasarkan MAC address kedalam jaringan *wireless* dan sudah diaktifkan fitur *access list.*

Gambar 17. *Access List*

Pada gambar 18 merupakan perangkat yang diizinkan masuk kedalam SSID oleh seorang admin jaringan dan mendapatkan IP DHCP.

Gambar 18. Pengujian Jaringan Akhir

Sedangkan pada gambar19 merupakan perangkat laptop yang mencoba masuk kedalam jaringan *wireless* SSID *"*sidang" yang telah diaktifkan fitur *access list reject* oleh admin jaringan maka secara otomatis perangkat akan tidak bisa masuk kedalam jaringan *wireless* tersebut.

Gambar 19. Pengujian Jaringan Akhir

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah diimplementasikan pada jaringan komputer di PT. MNC Televisi Network, maka dapat ditarik kesimpulan bahwa:

1. Dengan metode *access list* ini lalu lintas jaringan *wireless* dapat dimanage dan dimonitor oleh seorang admin jaringan perangkat-perangkat yang masuk kedalam SSID.
2. Dengan metode *access list* ini apabila ada karyawan baru wajib mengkonfirmasi kepada admin jaringan untuk mendaftarkan hak akses internet.
3. Dengan penerapan fitur capsman ini dapat mempermudah IT *Network* dalam mengatur *access point* secara bersamaan sehingga efisien waktu pada proses konfigurasinya.

5. SARAN

Berdasarkan penelitian yang telah dilakukan, penulis akan memberikan saran untuk penelitian selanjutnya agar penelitian selanjutnya dapat mengeksplor lebih dalam, penulis memberikan saran sebagai berikut:

1. Penulis menyarankan untuk penelitian selanjutnya agar mengimplementasikan *load balancing group* pada fitur CAPsMAN. *Load balancing group* ini berfungsi agar setiap perangkat yang terkoneksi ke dalam *access point* tetap stabil dengan membagi perangkat yang terkoneksi ke *access point* lainnya.
2. Penulis memberikan saran agar menggunakan hotspot untuk para tamu yang diberikan authentikasi via hotspot pada penelitian selanjutnya.
3. Disarankan untuk penelitian selanjutnya agar meng*eksplor* lebih dalam fitur CAPsMAN pada *router mikrotik*.

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

UCAPAN TERIMA KASIH

Dengan mengucap puji serta syukur kepada Allah SWT, pembuatan skripsi ini kupersembahkan untuk:

1. Bapak Ujang Yusuf dan Ibu Ida Farida tercinta yang telah membesarkan aku dan selalu membimbing, mendukung, memotivasi serta mendoakan aku untuk meraih kesuksesan.
2. Kakak (Eka Nur Fadilla) dan adik (Daffa Saputra Yusuf) yang telah memberikan dukungan dan semangat.

DAFTAR PUSTAKA

[1] D. M. Sari, M. Yamin, and L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing," *SemanTIK*, vol. 3, no. 2, pp. 203–208, 2017, doi: 10.1016/j.neuropharm.2007.08.010.

[2] M. B. Agus Didi Purwanto, "Implementasi Access List Sebagai Filter Traffic Jaringan (Study Kasus Pt. Usaha Entertainment Indonesia)," *J. Tek. Komput. AMIK BSI*, vol. II, no. 1, pp. 78–88, 2016, [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/365/274.

[3] Iwan Sofana, *JARINGAN KOMPUTER BERBASIS MIKROTIK*. Bandung: Informatika Bandung, 2017.

[4] H. Hasrul and A. M. Lawani, "Pengembangan Jaringan Wireless Menggunakan Mikrotik Router Os Rb750 Pada Pt . Amanah Finance Palu," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 11–19, 2017, [Online]. Available: http://jesik.web.id/index.php/jesik/article/view/56/38.

[5] MADCOMS, *Manajemen Sistem Jaringan Komputer Dengan Mikrotik RouterOS*. ANDI, 2016.

[6] I. Warman and Nofrizal, "Analisa Perbandingan Kinerja Fitur Mikrotik Capsman Dengan Konfigurasi Tunnel dan Tanpa Menggunakan Tunnel pada Router Mikrotik RB951-2N," *J. TeknoIF Vol. 4 No. 2 Oktober 2016*, vol. 4, no. 2, pp. 96–105, 2016.

[7] C. N. Syaiful, "Perancangan jaringan internet dengan hotspot mikrotik dan mac address Filtering," vol. 12, no. 02, pp. 13–24, 2018.