

Tersedia online di [www.journal.unipdu.ac.id](http://www.journal.unipdu.ac.id)  
UnipduHalaman jurnal di [www.journal.unipdu.ac.id/index.php/register](http://www.journal.unipdu.ac.id/index.php/register)

## Implementasi *authentication Captive Portal* pada *Wireless Local Area Network* PT. Rikku Mitra Sriwijaya

Rahmat Novrianda

Teknik Komputer, Universitas Bina Darma, Kota Palembang, Indonesia

email: [rahmat.novrianda.d@gmail.com](mailto:rahmat.novrianda.d@gmail.com)

### INFO ARTIKEL

**Sejarah artikel:**

Menerima 31 Juli 2018  
Revisi 10 Agustus 2018  
Diterima 11 Agustus 2018  
Online 11 Agustus 2018

**Kata kunci:**

*Captive Portal*  
*cyber crime*  
NDLC  
WLAN  
WPA2-PSK

**Keywords:**

*Captive Portal*  
*cyber crime*  
NDLC  
WLAN  
WPA2-PSK

**Style APA dalam mensitasi artikel ini:**

Novrianda, R. (2018). Implementasi *authentication Captive Portal* pada *Wireless Local Area Network* PT. Rikku Mitra Sriwijaya. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, 4(2), 67-80.

### ABSTRAK

PT. Rikku Mitra Sriwijaya merupakan salah satu perusahaan yang menyalurkan tenaga *cleaning service*. Perusahaan ini telah memiliki *Wireless Local Area Network* (WLAN) yang digunakan sebagai media pertukaran data serta informasi dengan memanfaatkan media transmisi *wireless*, WLAN PT. Rikku Mitra Sriwijaya saat ini menggunakan WPA2-PSK sebagai sistem keamanan untuk otentikasi pengguna agar dapat mengakses internet. Akan tetapi, penggunaan WPA2-PSK sebagai keamanan WLAN masih memiliki kelemahan dikarenakan penggunaan 1 *password* yang sama untuk banyak *user* agar dapat terhubung dengan *hotspot* WLAN PT. Rikku Mitra Sriwijaya akan menjadi peluang terjadinya *cyber crime*. Hal ini terjadi karena akan sangat mudah *user* yang tidak bertanggung jawab untuk masuk ke dalam WLAN PT. Rikku Mitra Sriwijaya. Dari informasi yang diperoleh, pada tahun 2017 PT. Rikku Mitra Sriwijaya mengalami kehilangan serta perusakan data dan informasi yang dimilikinya. Oleh karena itu, pada penelitian ini akan diterapkan *authentication Captive Portal* sebagai usaha peningkatan keamanan WLAN PT. Rikku Mitra Sriwijaya menggantikan WPA2-PSK. Proses penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC), metode ini berorientasi pada *network* yang memiliki 6 tahapan dengan siklus yang tidak memiliki awal dan akhir. Keseluruhan konfigurasi yang dibutuhkan dalam membangun *authentication Captive Portal* memanfaatkan program Winbox. Penelitian yang telah dilakukan ini menghasilkan suatu pembatasan otentikasi *user* khusus bagi *user* yang telah terdaftar pada WLAN PT. Rikku Mitra Sriwijaya yang diizinkan mengakses internet perusahaan ini. Selain itu, program Winbox juga dapat digunakan untuk *monitoring* seluruh *user* yang terhubung ke WLAN PT. Rikku Mitra Sriwijaya, baik *user* yang sedang aktif maupun yang tidak aktif.

### ABSTRACT

PT. Rikku Mitra Sriwijaya is one of the companies that supply cleaning service personnel. This company already has *Wireless Local Area Network* (WLAN) which is used as a medium for exchanging data and information by utilizing *wireless transmission media*, LAN PT. Rikku Mitra Sriwijaya currently uses WPA2-PSK as a security system for authenticate users to be able to access the internet. However, the use of WPA2-PSK as WLAN security still has weaknesses due to the use of the a same password for many users can be connected to the PT. Rikku Mitra Sriwijaya WLAN hotspot will be a chance of occurrence the *cyber crime*. This happens because it will be very easy for users who are not responsible for enter to WLAN PT. Rikku Mitra Sriwijaya. From the information obtained, in 2017 PT. Rikku Mitra Sriwijaya has lost and damaged their data and information. Therefore, *captive portal authentication* will be applied in this research as an effort to increase PT. Rikku Mitra Sriwijaya WLAN security that replace WPA2-PSK. This research process uses the *Network Development Life Cycle* (NDLC) method, this method is network oriented which has 6 stages with a cycle that has no beginning and ending. The entire configuration needed to build an *captive portal authentication* utilizes

*the Winbox program. This research has been carried out resulted limitation for users authentication specifically for users who have registered on PT. Rikku Mitra Sriwijaya WLAN is allowed to access the internet of this company. Furthermore, Winbox program also can be used for monitoring all connected users to PT. Rikku Mitra Sriwijaya WLAN both active and inactive users.*

© 2018 Register: Jurnal Ilmiah Teknologi Sistem Informasi. Semua hak cipta dilindungi undang-undang.

## 1. Pendahuluan

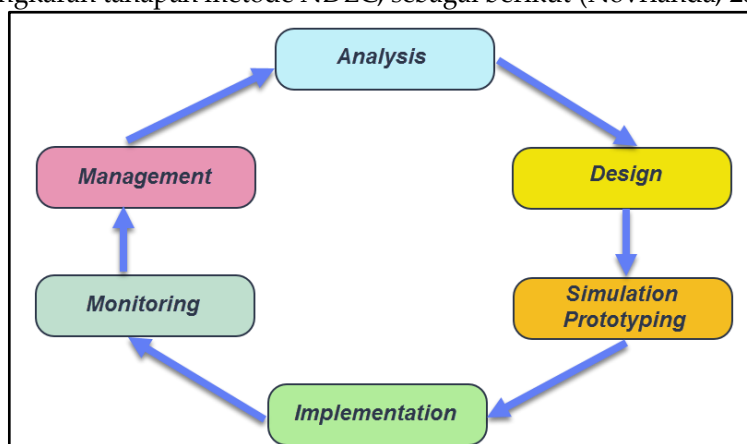
PT. Rikku Mitra Sriwijaya merupakan salah satu perusahaan penyalur petugas *cleaning service* yang berada di kota Palembang. Saat ini, PT. Rikku Mitra Sriwijaya telah memiliki jaringan komputer lokal dengan memanfaatkan media transmisi *wireless* atau lebih dikenal dengan sebutan *Wireless Local Area Network* (WLAN). WLAN merupakan pilihan yang dapat dijadikan sebagai pengganti jaringan lokal dengan media transmisi kabel atau *Local Area Network* (LAN), serta dapat lebih fleksibel dalam proses komunikasi data (Wongkar, Sinsuw, & Najoran, 2015). WLAN merupakan jaringan yang menghubungkan *user* dengan media transmisi *wireless*, sehingga *switch* yang digunakan juga harus dapat mendukung teknologi *wireless* yaitu *Access Point* (AP) (Purwanto & Cholil, 2013). Saat ini WLAN PT. Rikku Mitra Sriwijaya menggunakan WPA2-PSK sebagai teknik keamanan jaringan, yang berfungsi untuk otentikasi pengguna, sehingga dapat mengakses *internet*. WPA2-PSK adalah suatu teknik keamanan jaringan yang dilengkapi dengan suatu teknik enkripsi yaitu *Advanced Encryption Standard* (AES) (Ratnasari, Farida, & Firdaus, 2017). Akan tetapi, teknik keamanan jaringan WPA2-PSK pada WLAN masih memiliki kelemahan, yaitu menggunakan 1 *password* yang sama untuk banyak *user* untuk dapat terkoneksi dengan WLAN PT. Rikku Mitra Sriwijaya. Hal ini menyebabkan WLAN PT. Rikku Mitra Sriwijaya sangat rentan terhadap gangguan keamanan, di mana sangat memungkinkan terjadinya *cyber crime* oleh *user* yang tidak bertanggung jawab yang telah mengetahui *password hotspot* pada WLAN PT. Rikku Mitra Sriwijaya. *Cyber crime* adalah kejahatan dalam dunia digital yang berdasarkan pada perkembangan teknologi komputer, di mana *cyber crime* memanfaatkan koneksi internet, serta tergolong ke dalam tindakan yang mengganggu proses telekomunikasi dan bertentangan dengan hukum (Hermawan, 2015). Permasalahan tentang *cyber crime* telah dialami oleh PT. Rikku Mitra Sriwijaya pada tahun lalu terhadap WLAN yang dimilikinya, di mana perusahaan ini mengalami kehilangan serta perusakan data dan informasi miliknya akibat dari tindakan kriminal yang dilakukan oleh *user* yang tidak bertanggung jawab.

Oleh karena itu, pada penelitian ini dilakukan upaya dalam peningkatan keamanan WLAN yang dimiliki oleh PT. Rikku Mitra Sriwijaya. Peneliti memilih untuk mengimplementasikan *authentication Captive Portal* pada WLAN yang berada di PT. Rikku Mitra Sriwijaya. Teknik *authentication Captive Portal* berupaya dalam mencegah *user* untuk dapat mengakses internet hingga *user* tersebut melakukan otentikasi dengan *server*, di mana *user* tersebut akan dialihkan ke suatu halaman *web* yang digunakan untuk melakukan *login hotspot* bagi *user* yang telah terdaftar sebagai *user* yang sah. Setelah berhasil *login*, *user* diizinkan mengakses internet secara normal. Teknik *authentication Captive Portal* ini menggunakan *firewall* dinamis yang secara *default* akan menolak semua usaha akses yang dilakukan oleh *user* yang tidak sah (Sharma & Benith, 2014). Teknik *authentication Captive Portal* merespon setiap permintaan *Hypertext Transfer Protocol* (HTTP) dari *user* melalui sebuah *web browser* dengan menyediakan sebuah halaman *web* yang berguna untuk otentikasi *user* yang sah. Setelah *user* melakukan *login* dengan memasukan *user name* dan *password* yang tepat, maka *Media Access Control address* (MAC address) dari *Network Interface Card* (NIC) WLAN *user* tersebut terdaftar ke dalam *portal* serta kemudian proses transfer data *user* dibuatkan rute (*routing*) secara normal (Idland, Jelle, & Mjøl̄snes, 2012). Dalam penerapan teknik *authentication Captive Portal* tentunya harus menggunakan *hardware* yaitu MikroTik routerBOARD, di mana *hardware* tersebut termasuk ke dalam jenis-jenis perangkat komputer yang telah dilengkapi dengan sistem operasi routerOS dengan basis Linux, serta ditujukan untuk menjadi *router* jaringan. Perangkat komputer ini juga dilengkapi dengan beberapa fitur yang dapat digunakan untuk *bandwidth management* hingga pengaturan *hotspot* dan *routing* (Silitonga, 2014). Sistem operasi yang digunakan MikroTik routerBOARD ini merupakan *software* yang digunakan dalam mengembangkan *Personal Computer* (PC) biasa yang dimodifikasi menjadi *router* jaringan yang sangat bermanfaat, di mana pengembangan ini juga melingkupi bermacam-macam fasilitas yang dapat digunakan pada jaringan *wireless* (Tampi, Najoran, Sinsuw, & Lumenta, 2013). Pada proses pengaturan

dan konfigurasi perangkat MikroTik routerBOARD digunakan program Winbox, di mana program Winbox adalah *tools* yang dapat dimanfaatkan untuk mengatur MikroTik routerBOARD dari jarak jauh dengan *mode Graphical User Interface (GUI)* yang telah terkoneksi menggunakan *MAC address* atau *Internet Protocol address (IP address)* (Hidayat, 2018). Selain itu, program Winbox juga digunakan untuk melakukan *monitoring* seluruh *user* yang telah terhubung ke WLAN PT. Rikku Mitra Sriwijaya baik yang sedang aktif (*online*) ataupun sedang tidak aktif (*offline*).

## 2. Metode Penelitian

Pada penelitian ini menggunakan metode penelitian yaitu metode *Network Development Life Cycle (NDLC)*, di mana metode ini melakukan pendekatan terhadap proses komunikasi data berorientasi *network* yang memiliki suatu lingkaran tahapan yang tidak memiliki awal maupun akhir proses. Tahapan pada metode NDLC adalah *analysis, design, simulation prototyping, implementation, monitoring* serta tahapan terakhir adalah *management* (Novrianda, 2017). Berikut ini pada Gambar 1 memperlihatkan lingkaran tahapan metode NDLC, sebagai berikut (Novrianda, 2017):



Gambar 1. Metode *Network Development Life Cycle (NDLC)* (Novrianda, 2017)

Lingkaran tahapan pada NDLC:

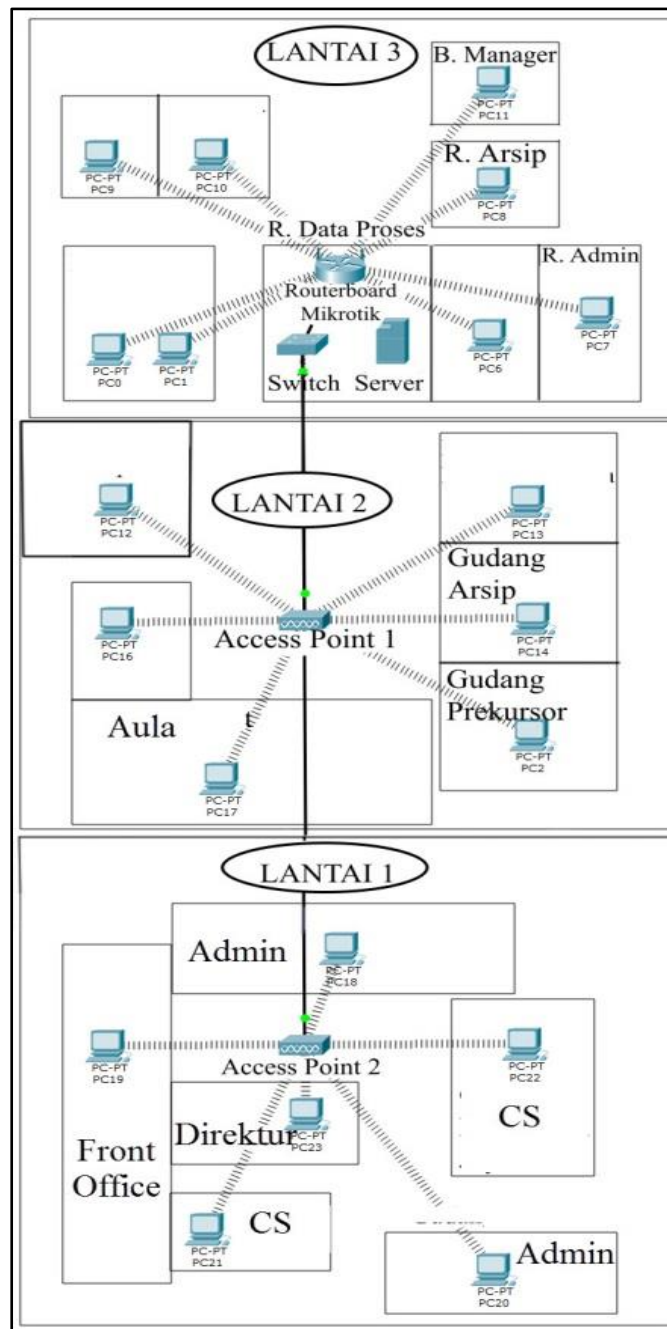
- Analysis:** Pada tahap ini, penelitian dilakukan survei ke lokasi serta *interview* kepada beberapa staf berkaitan dengan permasalahan keamanan jaringan yang dialami oleh PT. Rikku Mitra Sriwijaya. Di mana diketahui bahwa permasalahan yang dialami adalah pada pembatasan *user* yang sah melalui otentikasi *user* dengan WPA-PSK yang masih memiliki kelemahan dalam hal keamanan WLAN.
- Design:** Sebagai salah satu metode penelitian berorientasi *network*, tentunya pada tahap *design* ini berkaitan dengan perancangan topologi jaringan. Pada tahapan ini, dirancanglah topologi WLAN PT. Rikku Mitra Sriwijaya sesuai dengan hasil survei pada lokasi PT. Rikku Mitra Sriwijaya dengan menggunakan *software Cisco Packet Tracer*.
- Simulation Prototyping:** Pada penelitian ini, *simulation prototyping* tidak dapat dilakukan dengan memanfaatkan *software Cisco Packet Tracer*, tetapi harus menggunakan perangkat MikroTik routerBOARD serta dibantu program Winbox. Berdasarkan topologi WLAN PT. Rikku Mitra Sriwijaya yang sebelumnya telah didesain menggunakan *software Cisco Packet Tracer*, dilakukan pembuatan *prototype* dengan memanfaatkan MikroTik routerBOARD serta beberapa konfigurasi untuk membangun *authentication Captive Portal* menggunakan program Winbox. Setelah selesai keseluruhan konfigurasi, maka dilakukan pengujian terhadap *prototype* tersebut untuk mengetahui apakah *authentication Captive Portal* telah dapat digunakan sesuai tujuan penelitian.
- Implementation:** Pada tahapan ini, penelitian dilakukan implementasi hasil dari tahapan sebelumnya terhadap WLAN yang ada pada PT. Rikku Mitra Sriwijaya. Pada proses ini, peneliti mengatur ulang (*reset*) sistem keamanan jaringan yang sebelumnya menggunakan WPA2-PSK, kemudian penelitian dilakukan konfigurasi ulang untuk membangun *authentication Captive Portal* serta telah dilakukan pengujian yang dapat dilihat pada hasil penelitian.
- Monitoring:** Tahapan ini merupakan kelanjutan dari tahapan sebelumnya, di mana peneliti tetap dapat melakukan *monitoring* terhadap *user* yang terhubung ke dalam WLAN PT. Rikku Mitra

Sriwijaya, baik *user* yang *online* maupun *user* yang *offline* dengan menggunakan program Winbox. Selain itu, peneliti juga dapat melakukan *monitoring* jika ada *user* yang tidak sah, di mana diketahui berdasarkan *MAC address* atau *IP address user* tersebut tidak terdaftar pada *database WLAN PT*. Rikku Mitra Sriwijaya.

- f. **Management:** Tahapan selanjutnya ialah *management* yang merupakan tahapan yang dilaksanakan dalam rangka pemeliharaan hasil penelitian yang telah diperoleh, dalam hal ini dilakukan *management* terhadap teknik *authentication Captive Portal* yang merupakan hasil dari penelitian yang telah dilakukan, baik itu bertujuan untuk perbaikan ataupun pengembangan sesuai dengan kebutuhan WLAN PT. Rikku Mitra Sriwijaya.

### 3. Hasil dan Pembahasan

#### 3.1. Topologi PT. Rikku Mitra Sriwijaya



Gambar 2. Topologi Jaringan PT. Rikku Mitra Sriwijaya

Gambar 2 merupakan topologi *Wireless Local Area Network (WLAN)* pada PT. Rikku Mitra Sriwijaya, di mana terdapat 3 lantai yang saling terhubung. Gambar 2 dapat dijelaskan bahwa pada lantai 1 memiliki

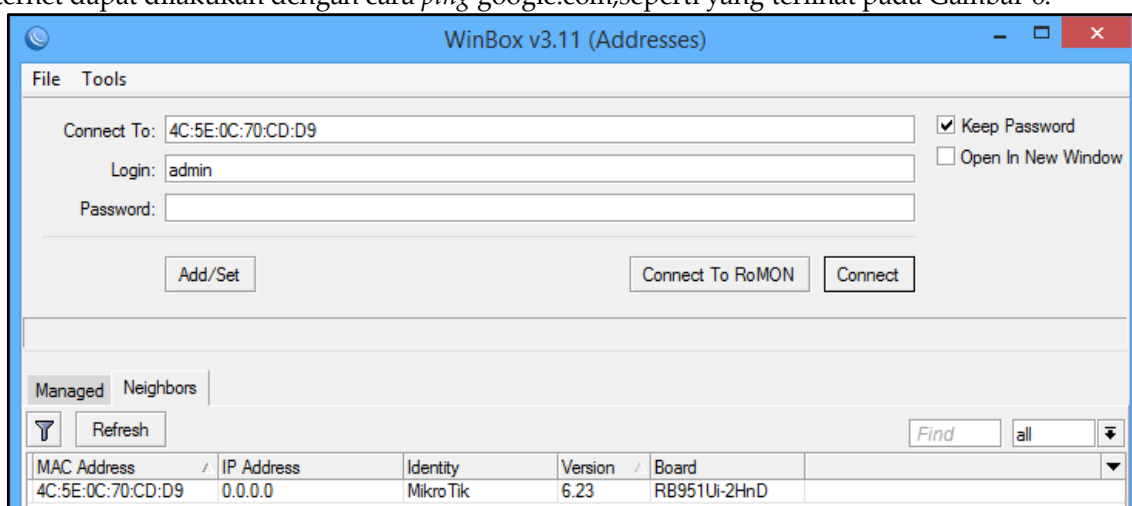


6 *Personal Computer* (PC) yang terhubung menggunakan media transmisi *wireless* pada *Access Point* (AP) 2. Kemudian, pada lantai 2 terdapat 6 PC yang terhubung pada AP 1 dengan memanfaatkan media transmisi *wireless*, serta pada lantai 3 terdapat 8 PC yang langsung terhubung pada MikroTik routerBOARD yang juga menggunakan media transmisi *wireless*. Gambar 2 terlihat bahwa jaringan komputer pada lantai 1 dan lantai 2 terhubung dengan *switch* yang telah terhubung langsung dengan MikroTik routerBOARD yang terdapat pada lantai 3 dengan menggunakan media transmisi kabel. Selain itu, pada lantai 3 juga terdapat 1 server yang merupakan pusat pengendalian seluruh jaringan komputer dari lantai 1 hingga lantai 3.

Topologi WLAN Gambar 2 disusun berdasarkan posisi ruangan yang ada pada PT. Rikku Mitra Sriwijaya, di mana posisi *user* ditempatkan sesuai dengan tugas dan fungsi mereka masing-masing. Ruangan-ruangan yang tergolong penting diposisikan pada lantai 3 agar tidak mengalami gangguan dari pengunjung ataupun staf PT. Rikku Mitra Sriwijaya, di mana pada lantai 3 terdapat ruangan arsip serta ruangan data proses yang diawasi oleh *Branch Manager* dan 1 orang admin *Information Technology* (IT). Selain itu, perangkat server dan MikroTik routerBOARD juga diamankan pada lantai 3 tepatnya pada ruangan data proses.

### 3.2. Konfigurasi MikroTik routerBOARD

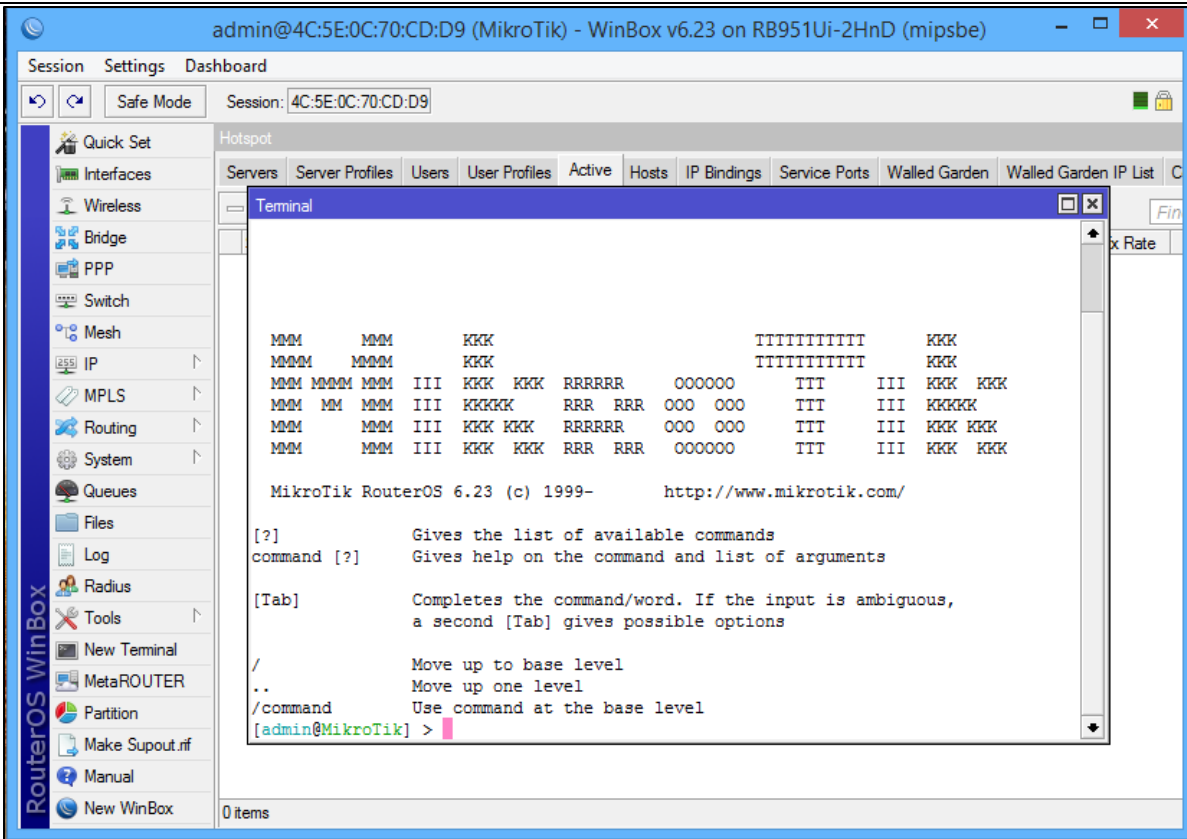
Pada penelitian ini, konfigurasi MikroTik routerBOARD menggunakan program Winbox v3.11 yang memanfaatkan *Graphical User Interface* (GUI), sehingga memberikan kemudahan dalam proses konfigurasi MikroTik routerBOARD. Gambar 3 adalah tampilan program Winbox v3.11. Langkah pertama yang dilakukan dalam proses konfigurasi MikroTik routerBOARD adalah dengan cara menghubungkan Mikrotik dengan PC menggunakan kabel *Unshielded Twisted Pair* (UTP). Setelah itu, buka program Winbox maka akan tampil seperti pada Gambar 3. Selanjutnya pastikan sudah terdeteksi *MAC address* dan nama perangkat pada MikroTik routerBOARD. Kemudian klik *connect* maka akan tampil seperti pada Gambar 4. Untuk dapat menghubungkan MikroTik routerBOARD dengan internet, maka perlu membuka *Dynamic Host Configuration Protocol Client* (DHCP) *Client* pada MikroTik routerBOARD, di mana hal ini dilakukan agar MikroTik routerBOARD memperoleh *IP address* dari jaringan publik. Hal tersebut dapat dilakukan dengan cara menghubungkan MikroTik routerBOARD dengan modem, kemudian pilih menu *IP - DHCP Client* - pilih tambah pada *Address List* - pilih Internet - Ok dan Mikrotik, setelah itu MikroTik routerBOARD memperoleh *IP address* seperti pada Gambar 5. Pengujian yang dapat dilakukan untuk memastikan MikroTik routerBOARD sudah terhubung dengan internet dapat dilakukan dengan cara *ping google.com*, seperti yang terlihat pada Gambar 6.



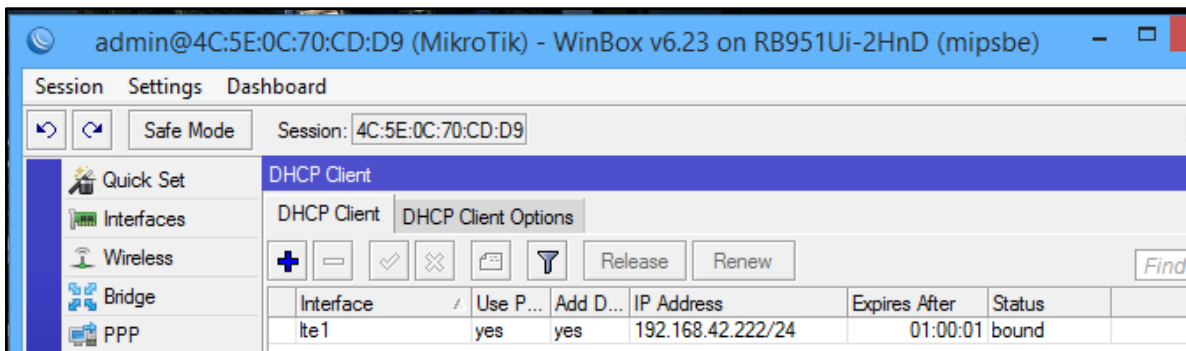
Gambar 3. Tampilan *login* Mikrotik dengan Winbox v3.11

### 3.3. Konfigurasi Wireless Access Point (WAP)

Konfigurasi *Wireless Access Point* (WAP) MikroTik routerBOARD perlu dilakukan dengan tujuan untuk menjadikan MikroTik routerBOARD sebagai pemancar layaknya AP. Konfigurasi ini dapat dilakukan dengan cara buka *setting wireless* di menu *wireless* kemudian aktifkan wlan1 dengan cara klik *enable*, selanjutnya atur WAP seperti pada Gambar 7.



Gambar 4. Tampilan awal Mikrotik pada Winbox



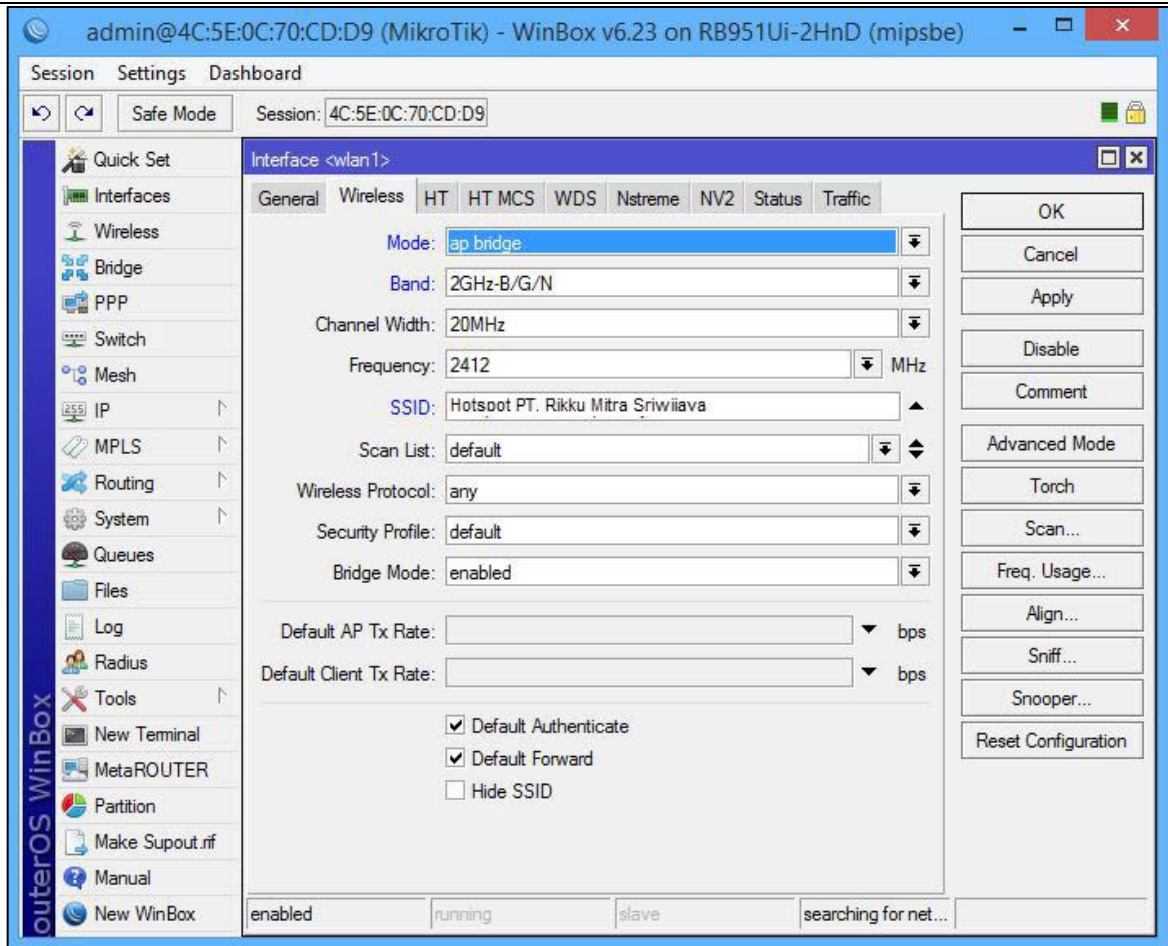
Gambar 5. Tampilan Address List



Gambar 6. Proses ping google.com

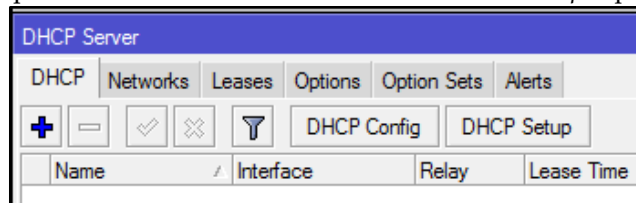
### 3.4. Konfigurasi DHCP Server

Konfigurasi ini dilakukan dengan tujuan agar perangkat *client* yang terhubung memperoleh IP *address* secara dinamis. Adapun langkah-langkah konfigurasi DHCP *Server* ini sebagai berikut:



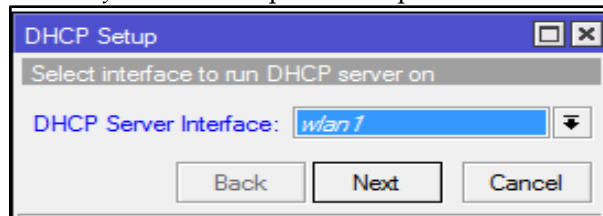
Gambar 7. Tampilan interface wlan1

- a. Langkah pertama pilih menu DHCP Server kemudian DHCP Setup seperti pada Gambar 8.



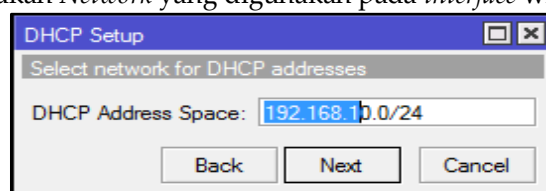
Gambar 8. Menu DHCP Server

- b. Langkah kedua pilih interface wlan1, dapat dilihat pada Gambar 9.



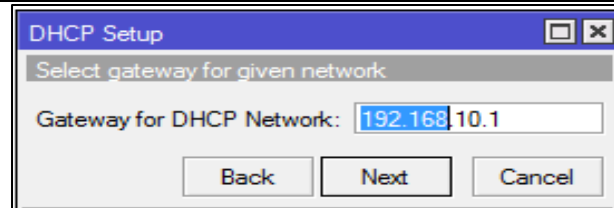
Gambar 9. DHCP Server Interface pada DHCP Setup.

- c. Langkah ketiga masukan Network yang digunakan pada interface wlan1 seperti pada Gambar 10.



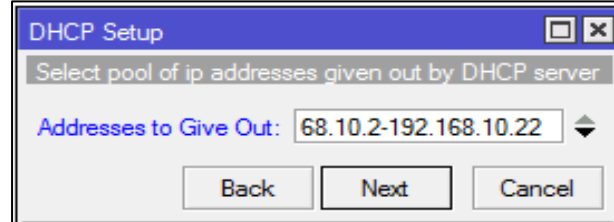
Gambar 10. DHCP Address Space pada DHCP Setup.

- d. Langkah keempat masukan IP address Gateway, dapat dilihat pada Gambar 11.



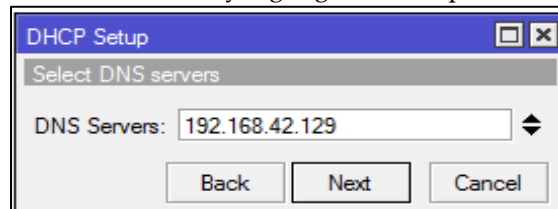
Gambar 11. Gateway for DHCP Network pada DHCP Setup

- e. Pada langkah kelima ini, isikanlah *addresses to give out* seperti Gambar 12.



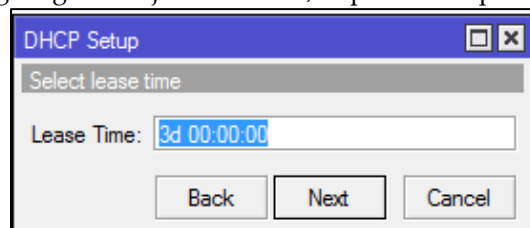
Gambar 12. Address to Give Out pada DHCP Setup

- f. Langkah keenam masukan DNS Server yang digunakan seperti Gambar 13.



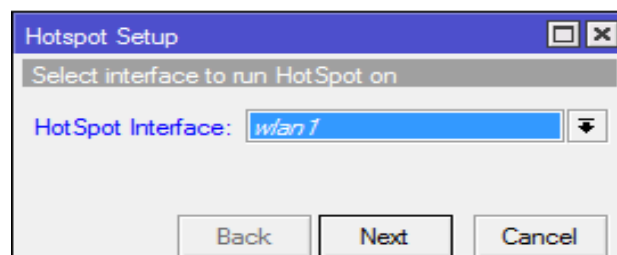
Gambar 13. DNS Server pada DHCP Setup

- g. Langkah terakhir langsung *next* saja dan selesai, dapat dilihat pada Gambar 14.

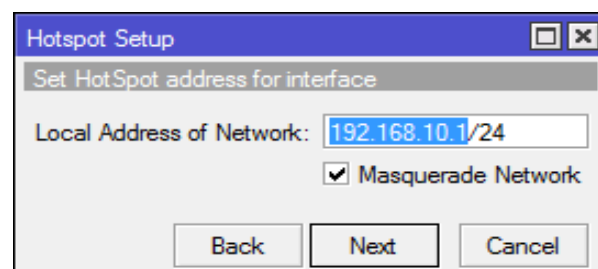


Gambar 14. Lease Time pada DHCP Setup

### 3.5. Konfigurasi Hotspot



Gambar 15. Hotspot interface pada Hotspot Setup

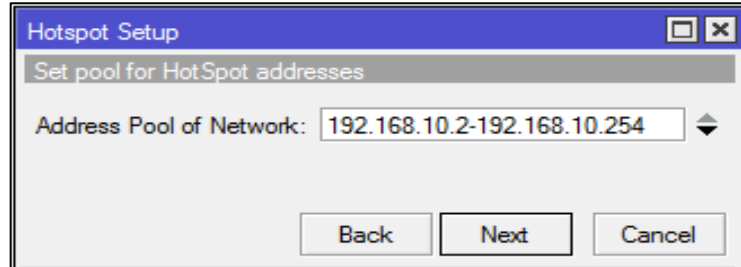


Gambar 16. Tampilan Local of Network



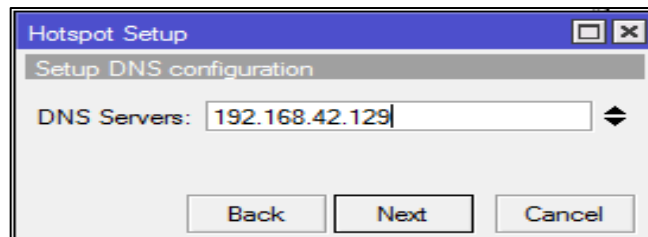
Konfigurasi *hotspot* dilakukan dengan beberapa langkah agar perangkat yang terhubung dengan WAP MikroTik routerBOARD akan melewati portal otentikasi dengan menggunakan *user* yang terdaftar agar dapat mengakses internet, dan konfigurasi ini dilakukan dengan langkah-langkah sebagai berikut:

- a. Langkah pertama pilih *hotspot interface wlan1* dapat dilihat pada Gambar 15.
- b. Selanjutnya isi *Local of Network, next*. Seperti Gambar 16.
- c. Kemudian isi *Address Pool of Network, next*, seperti Gambar 17.



Gambar 17. Tampilan *Address Pool of Network*

- d. Isi *Domain Name Server (DNS)* sesuai dengan modem yang dipakai, *next* dapat dilihat pada Gambar 18.



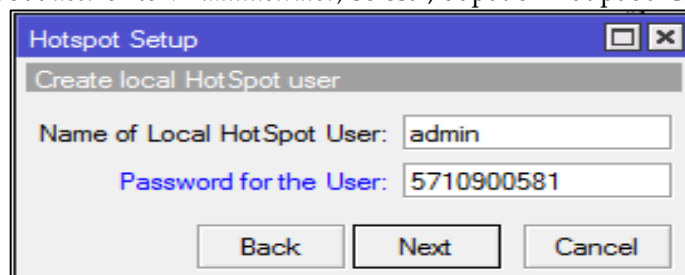
Gambar 18. Tampilan *DNS Servers* pada *Hotspot Setup*

- e. Isi *DNS Name* yang akan digunakan, *next* seperti pada Gambar 19.



Gambar 19. *DNS Name* pada *Hotspot Setup*

- f. Terakhir membuat *user* untuk *Administrator*, selesai, dapat dilihat pada Gambar 20.

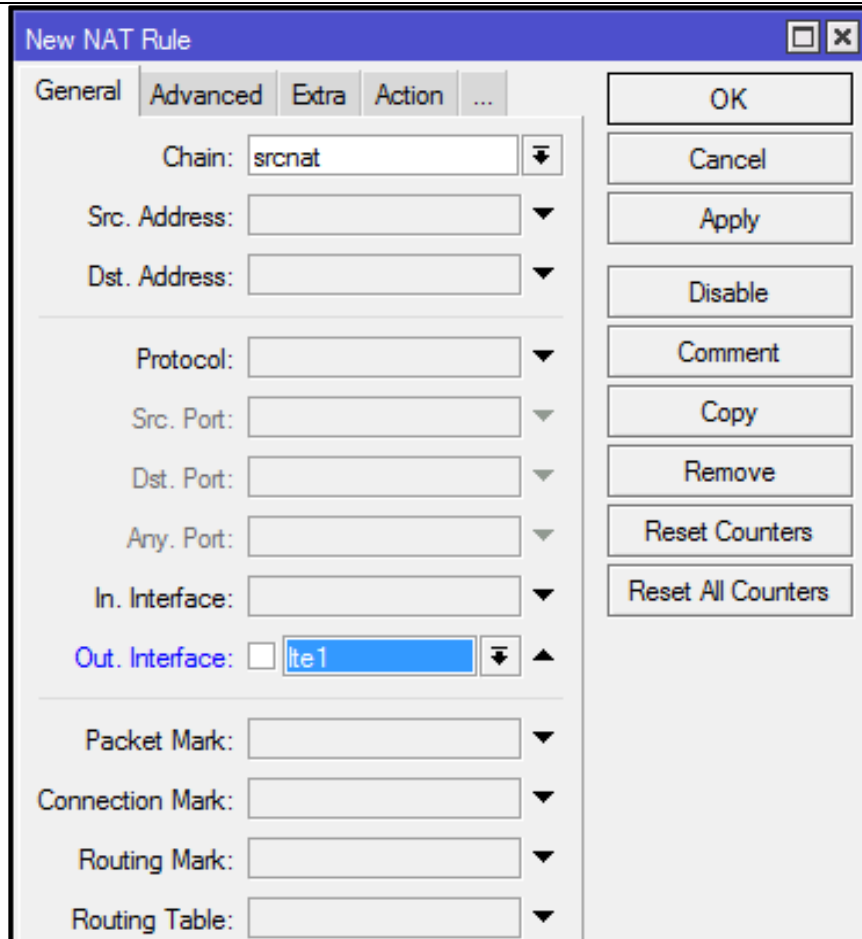


Gambar 20. *User administrator* pada *Hotspot Setup*

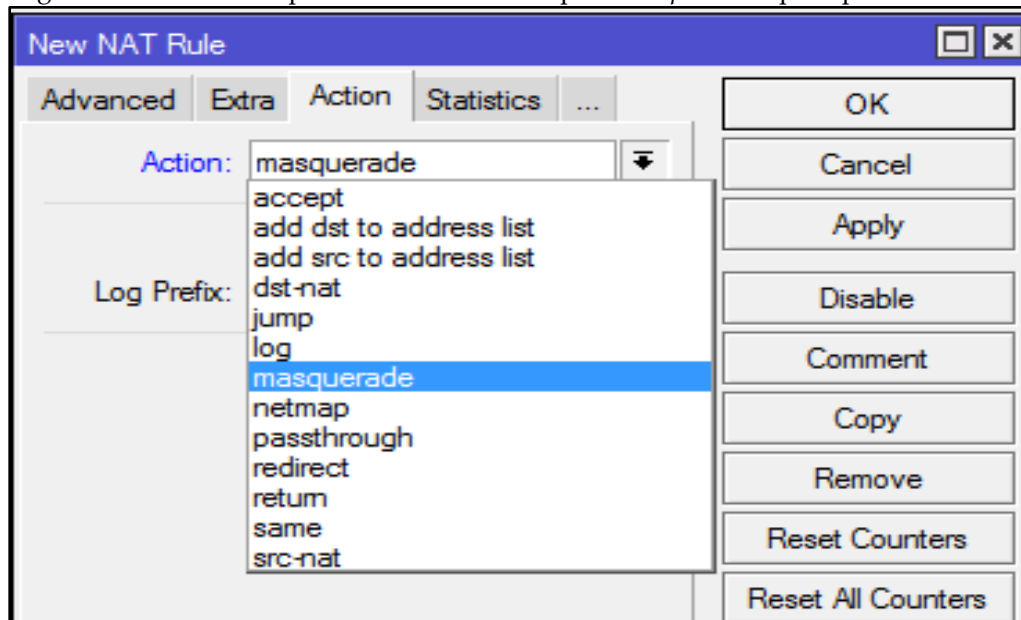
### 3.6. Konfigurasi Firewall Network Address Translation (NAT)

Konfigurasi ini bertujuan untuk mengizinkan perangkat yang terhubung WLAN agar dapat mengakses internet atau melakukan *browsing*, adapun konfigurasinya yaitu:

- a. Langkah pertama masuk pada menu *Firewall* kemudian pilih *Network Address Translation (NAT)* dan tambahkan *rule*, dapat dilihat pada Gambar 21.

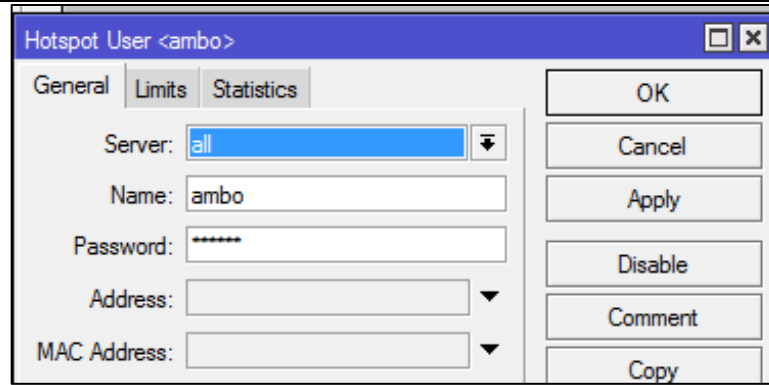
Gambar 21. Menu *General* NAT Rule

- b. Langkah terakhir masuk pada menu *Action* dan pilih *masquerade* seperti pada Gambar 22.

Gambar 22. Menu *Action* NAT Rule

### 3.7. Konfigurasi Manajemen User

Manajemen *user* ini berguna untuk membuat atau mendaftarkan *user* baru, di mana *user* tersebut menyimpan *username* dan *password* *user* yang nantinya akan digunakan dalam melakukan *login hotspot*, sehingga *user* dapat mengakses *internet*. Pembuatan *user* ini terdapat pada *menu hotspot* program Winbox seperti pada Gambar 23.



Gambar 23. Pembuatan/Pendaftaran user

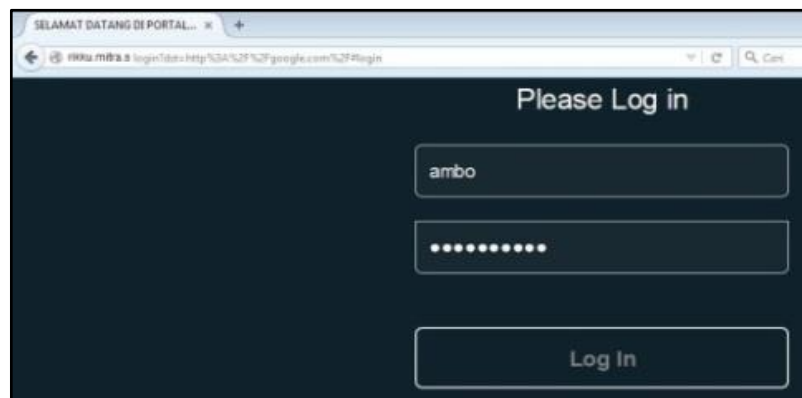
### 3.8. Pengujian Login Hotspot

Pengujian ini dilakukan untuk mengetahui apakah konfigurasi yang telah diatur serta data user yang telah didaftarkan dengan cara yang dijelaskan pada Gambar 23 dapat diakses dengan baik dan lancar. Berikut ini tahapan pengujian login hotspot WLAN PT. Rikku Mitra Sriwijaya:

- a. Koneksikan PC client dengan hotspot PT. Rikku Mitra Sriwijaya kemudian buka browser, maka akan tampil Menu Home hotspot PT. Rikku Mitra Sriwijaya seperti pada Gambar 24, kemudian pilih masuk.

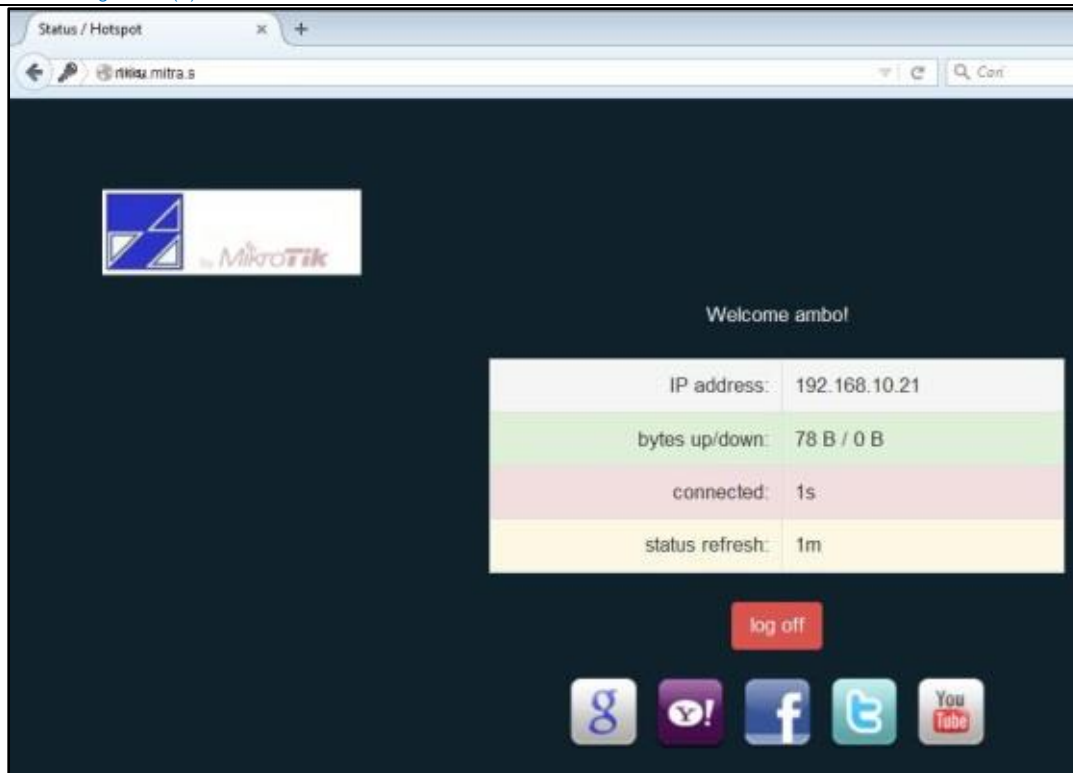


Gambar 24. Halaman Home

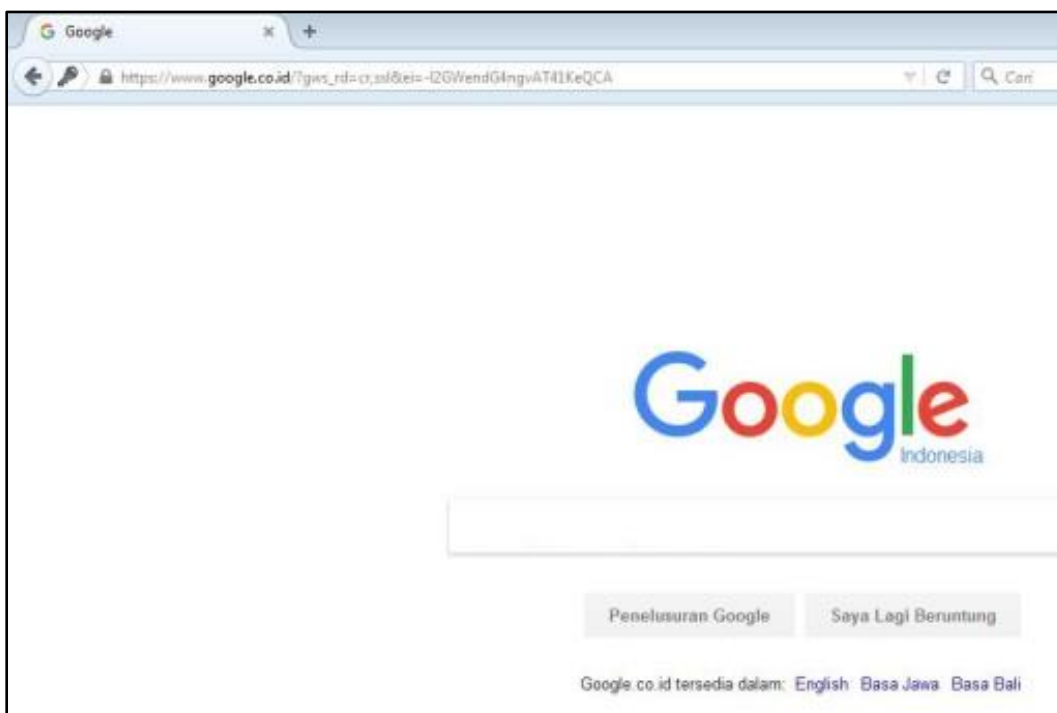


Gambar 25. Halaman login

- b. Selanjutnya login dengan salah satu user yang telah dibuat dengan mengisi username dan password, kemudian klik Log In seperti pada Gambar 25.
- c. Jika berhasil maka akan tampil seperti pada Gambar 26.

Gambar 26. Tampilan *login* sukses

- d. Setelah berhasil masuk, maka *user* sudah dapat mengakses internet, dapat dilihat pada Gambar 27.

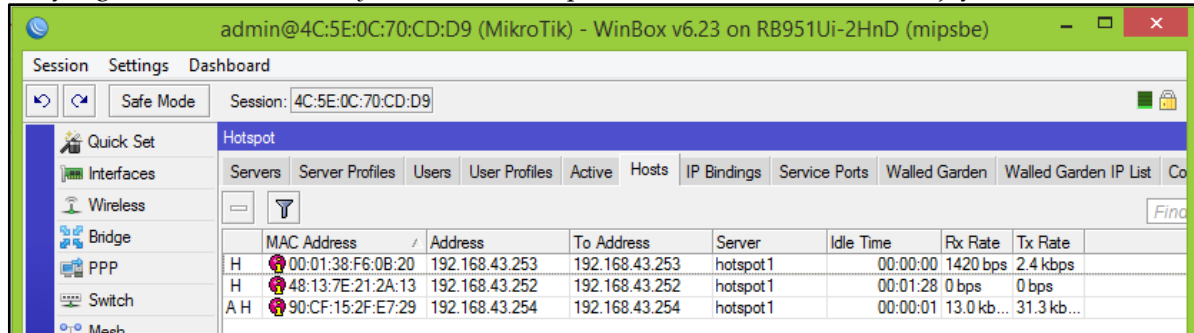
Gambar 27. Akses *Internet*.

### 3.9. Pengujian *Monitoring*

*Monitoring* dilakukan untuk melihat perangkat (*user*) siapa saja yang terhubung dengan jaringan dan *user* valid yang sedang aktif pada *hotspot* PT. Rikku Mitra Sriwijaya. Hal ini juga untuk melihat apakah ada *user* yang mencurigakan terhubung pada WLAN perusahaan atau tidak. *User* valid merupakan *user* yang telah melakukan registrasi serta *username*, *password*, *MAC address* dan *IP address*-nya telah



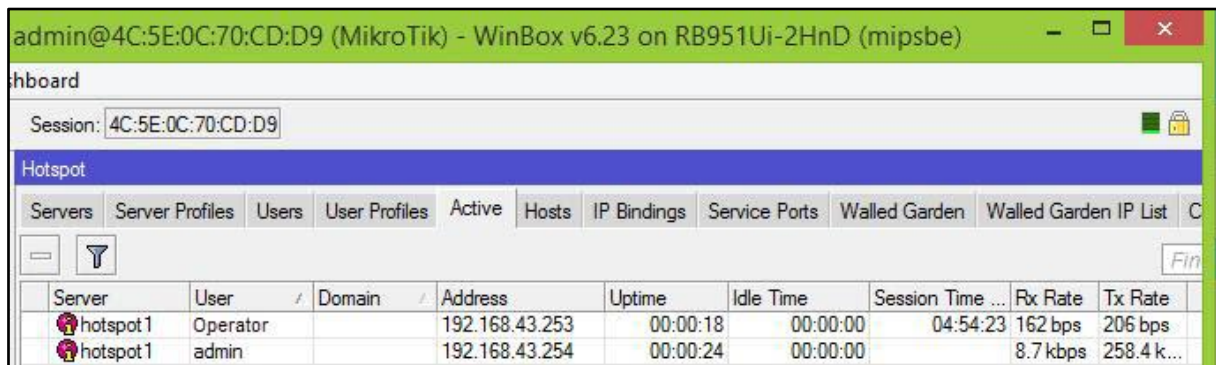
tersimpan pada *database* PT. Rikku Mitra Sriwijaya, sehingga jika pada menu *host* yang dapat dilihat pada Gambar 28 terdeteksi *MAC address* ataupun *IP address* yang tidak terdaftar sebagai *user* WLAN PT. Rikku Mitra Sriwijaya, maka dapat dipastikan bahwa itu adalah *user* yang mencurigakan ataupun *user* yang berniat melakukan *cyber crime* terhadap WLAN PT. Rikku Mitra Sriwijaya.



	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate
H	00:01:38:F6:0B:20	192.168.43.253	192.168.43.253	hotspot1	00:00:00	1420 bps	2.4 kbps
H	48:13:7E:21:2A:13	192.168.43.252	192.168.43.252	hotspot1	00:01:28	0 bps	0 bps
A H	90:CF:15:2F:E7:29	192.168.43.254	192.168.43.254	hotspot1	00:00:01	13.0 kb...	31.3 kb...

Gambar 28. Menu *Host* pada *Hotspot* Mikrotik

Gambar 29 diperlihatkan beberapa *user* atau perangkat yang terhubung dengan *hotspot* PT. Rikku Mitra Sriwijaya. Perangkat terhubung baik yang sudah melakukan *login* atau belum dapat di *monitoring* di menu *host* ini. Gambar 29 diperlihatkan ada 2 (dua) *user* yang sedang aktif mengakses *hotspot* PT. Rikku Mitra Sriwijaya yaitu operator dan admin. Selain itu juga, pada menu ini kita bisa melihat *session time* dari setiap *user* yang terhubung.



Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx Rate	Tx Rate
hotspot1	Operator		192.168.43.253	00:00:18	00:00:00	04:54:23	162 bps	206 bps
hotspot1	admin		192.168.43.254	00:00:24	00:00:00		8.7 kbps	258.4 k...

Gambar 29. Menu *Active* pada *Hotspot* Mikrotik

Pada penelitian ini, dilakukan beberapa konfigurasi untuk membangun *authentication Captive Portal* dengan menggunakan Mikrotik routerBOARD serta keseluruhan konfigurasi diproses memanfaatkan program Winbox v3.11. Hasil penelitian diperoleh bahwa keamanan WLAN pada PT. Rikku Mitra Sriwijaya telah berhasil ditingkatkan dengan mengimplementasikan *authentication Captive Portal*. Dengan begitu, *user* yang ingin memanfaatkan *hotspot* PT. Rikku Mitra Sriwijaya terlebih dahulu harus melakukan registrasi dengan mengisikan data-data lengkap *user* termasuk *username* dan *password* masing-masing *user*, sehingga untuk 1 *user* hanya memiliki 1 *username* dan *password* untuk dapat mengakses *internet* pada WLAN PT. Rikku Mitra Sriwijaya. Tidak hanya sebatas itu, pada penelitian ini juga dapat melakukan *monitoring* seluruh *user* yang terhubung dengan WLAN PT. Rikku Mitra Sriwijaya dengan bantuan program Winbox v3.11.

#### 4. Kesimpulan

Hasil penelitian yang diperoleh dapat ditarik beberapa kesimpulan, yaitu *authentication Captive Portal* dapat meningkatkan keamanan jaringan dibandingkan dengan WPA2-PSK dalam hal membatasi *user* yang dapat mengakses WLAN PT. Rikku Mitra Sriwijaya, di mana setiap *user* yang telah terdaftar akan memiliki *username* dan *password* yang berbeda-beda. Untuk mengatur *authentication Captive Portal* dibutuhkan perangkat Mikrotik routerBOARD yang telah dilakukan beberapa konfigurasi, seperti konfigurasi Mikrotik routerBOARD, konfigurasi *Wireless Access Point*, konfigurasi DHCP server, Konfigurasi *hotspot* hingga konfigurasi *Firewall NAT*. Keseluruhan konfigurasi dijalankan menggunakan program Winbox v3.11, tetapi program Winbox v3.11 tidak hanya dapat digunakan

sebagai media untuk melakukan konfigurasi *authentication Captive Portal*, tetapi juga dapat dijadikan sebagai media untuk *monitoring* keseluruhan aktifitas *user* yang telah terdaftar pada WLAN PT. Rikku Mitra Sriwijaya.

Hasil penelitian yang telah diperoleh serta mengingat juga keterbatasan teori yang digunakan peneliti, maka peneliti memberikan saran untuk peneliti selanjutnya agar dapat menggali serta menggunakan metode penelitian yang lain dalam pengembangan penelitian selanjutnya. Selain itu, peneliti selanjutnya juga dapat menerapkan hasil penelitian ini pada objek yang lainnya, bahkan akan lebih baik jika peneliti selanjutnya juga dapat melakukan penambahan protokol keamanan WLAN yang dapat dikombinasikan dengan *authentication Captive Portal*.

## 5. Ucapan Terima Kasih

Pada penelitian ini, peneliti mengucapkan terima kasih kepada teman-teman yang namanya disebutkan pada referensi, sehingga penelitian ini dapat diselesaikan dengan baik. Selain itu, peneliti juga mengucapkan terima kasih kepada beberapa mahasiswa Program Studi Teknik Komputer Universitas Bina Darma yang telah membantu dalam pengumpulan data-data yang dibutuhkan pada penelitian ini.

## 6. Referensi

- Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, 6(1), 43-50.
- Hidayat, A. (2018). Design of radius server on server network internet faculty of Computer Science University Muhammadiyah Metro. *IJISCS (International Journal Of Information System and Computer Science)*, 2(1), 13-30.
- Idland, C., Jelle, T., & Mjølunes, S. F. (2012). Detection of Masqueraded Wireless Access Using 802.11 MAC Layer Fingerprints. *International Conference on Digital Forensics and Cyber Crime* (pp. 283-301). Berlin: Springer.
- Novrianda, R. (2017). Rancang bangun keamanan jaringan wireless pada STIPER Sriwigama Palembang dengan radius server. *Jurnal Maklumatika*, 4(1), 19-29.
- Purwanto, T. D., & Cholil, W. (2013). Analisa Kinerja Wireless Radius Server Pada Perangkat Access Point 802.11 g (Studi Kasus di Universitas Bina Darma). *Semantik*, 3(1), 371-376.
- Ratnasari, S. D., Farida, E., & Firdaus, N. (2017). Implementasi Controller Access Point System Manager (CAPsMAN) Dan Wireless Distribution System (WDS) Jaringan Wireless Di SMK Terpadu Al Ishlahiyah Singosari Malang. *Seminar Nasional Sistem Informasi (SENASIF)*. 1, pp. 624-635. Malang: Universitas Merdeka Malang.
- Sharma, P., & Benith, T. (2014). Design and Configuration of App Supportive Indirect Internet Access using a Transparent Proxy Server. *International Journal Of Modern Engineering Research (IJMER)*, 4(10), 9-17.
- Silitonga, P. (2014). Analisis QoS (Quality of Service) Jaringan Kampus dengan Menggunakan Microtic Routerboard. *Jurnal Times*, 3(2), 19-24.
- Tampi, B. A., Najoran, M. E., Sinsuw, A. A., & Lumenta, A. S. (2013). Implementasi Routing Pada IP Camera Untuk Monitoring Ruang di Universitas Sam Ratulangi. *e-journal Teknik Elektro dan Komputer*, 2(2), 1-7.
- Wongkar, S., Sinsuw, A. A., & Najoran, X. (2015). Analisa Implementasi Jaringan Internet dengan Menggabungkan Jaringan LAN dan WLAN di Desa Kawangkoan Bawah wilayah Amurang II. *Jurnal Teknik Elektro dan Komputer*, 4(6), 62-68.