

Rancang Bangun Wireless Access Point dengan Capsman dan Mac Mask Access list

Zaenal Mutaqin Subekti^{1*)}, Subandri²

¹Jurusan Teknik Komputer, STMIK Bani Saleh, Bekasi

²Jurusan Teknologi Informasi, STMIK Bani Saleh, Bekasi

^{1,2}Jln. M Hasibuan No 68, Kota Bekasi, 50272, Indonesia

email: ¹zms.stmikbanisaleh@gmail.com, ²andri.subandri@ymail.com

Special Issue on Seminar Nasional - Inovasi Dalam Teknologi Informasi & Teknologi Pembelajaran 2019

Abstrac - In the era of millennial needs using the internet became the primary needs of everyone, to connect to the internet one of them by connecting through an access point. The problem that occurs is the difficulty of getting legal internet access that is already connected to an access point then moving place or room. Because the number of access point devices installed with SSID (Service Set Identifier) is different for each device that the user needs to log in again to get internet access, and there is no filtering of users who are entitled to use hotspot facilities based on certain devices. With the number of access points being hotspots, this becomes a consideration for network managers to set hotspot passwords or other settings, this is a new challenge for network managers. Therefore, to overcome this problem a wireless access point management system was built that uses centrally using CAPsMAN (Controller Access Point System Manager) and MAC Mask Access Lists as filtering. By using the NDLC (Network Development Life Cycle) method in floating network design.

Keywords: access point, capsman, mac mask, access list, filtering.

Abstrak - Pada era milenial kebutuhan menggunakan internet mejadi kebutuhan primer setiap orang, untuk terkoneksi dengan internet salah satunya dengan terhubung melalui access point. Permasalahan yang terjadi adalah sulitnya mendapatkan akses internet secara legal ketika sudah terhubung dengan access point kemudian berpindah tempat atau ruangan. karena banyaknya perangkat access point yang terpasang dengan SSID (Service Set Identifier) yang berbeda-beda pada setiap perangkat mengharuskan user harus login kembali untuk mendapatkan akses internet, dan belum adanya filtering pengguna yang berhak menggunakan fasilitas hotspot berdasarkan perangkat tertentu. Dengan banyaknya access point yang menjadi hotspot, ini menjadi kendala bagi seorang pengelola jaringan dalam melakukan rekonfigurasi password hotspot maupun setting yang lain, hal ini menjadi tantangan baru bagi pengelola jaringan. Oleh karena itu, untuk mengatasi masalah tersebut dibangun sistem manajemen wireless access point secara terpusat menggunakan CAPsMAN (Controller Access Point system Manager) dan MAC Mask Access List sebagai filtering. Dengan menggunakan pendekatan metode NDLC (Network Development Life Cycle) dalam pengembangan rancang bangun jaringan.

Kata Kunci: access point, capsman, mac mask, access list, filtering.

*) penulis korespondensi: Zaenal Mutaqin Subekti
Email: zms.stmikbanisaleh@gmail.com

I. PENDAHULUAN

Dewasa ini perkembangan teknologi informasi sangat berkembang pesat dan menjadi sebuah bagian penting dalam hidup kita dimana setiap orang pada masa ini semua menggunakan teknologi informasi. Karena pentingnya teknologi informasi banyak sekali perusahaan, kampus, sekolah maupun instansi lain merancang sebuah teknologi informasi dengan kualitas jaringan komputer yang baik. Dengan adanya kualitas jaringan komputer yang baik diharapkan dapat membantu instansi dalam pengelolaan data atau pertukaran informasi menjadi lebih cepat.

Pada era milenial kebutuhan menggunakan internet mejadi kebutuhan primer setiap orang, untuk terkoneksi dengan internet salah satunya dengan menggunakan access point [1]. Banyaknya perangkat access point yang terpasang dengan SSID (Service Set Identifier) yang berbeda-beda pada setiap perangkat dapat membingungkan pengguna hotspot untuk dapat terkoneksi dengan jaringan internet, hal ini mengganggu kinerja user, dikarenakan pada saat berpindah tempat harus login kembali untuk mendapatkan akses secara legal. Selain itu, belum adanya filtering khusus siapa saja yang berhak memakai fasilitas hotspot berdasarkan device tertentu, kemudian dengan banyaknya access point yang menjadi hotspot untuk akses internet, ini menjadi kendala bagi seorang pengelola jaringan ketika dalam melakukan penggantian password pada hotspot dan melakukan setting konfigurasi yang lain pada hotspot. hal ini menjadi tantangan baru bagi pengelola jaringan.

Untuk dapat mendaftarkan mac address yang boleh terkoneksi dengan jaringan sehingga menjadi salah satu keamanan hanya mac address yang dikenali saja yang dapat mengakses internet. Capsman merupakan suatu fitur access point controller yang memungkinkan dilakukan kontrol monitoring maupun konfigurasi terhadap beberapa access point secara bersamaan [2]. Capsman [3] menjadi salah satu solusi dalam melakukan manajemen pada wireless access point atau hotspot agar lebih mudah dalam melakukan penggantian password atau setting konfigurasi yang lain.

II. PENELITIAN YANG TERKAIT

Terdapat beberapa penulisan terkait yang sudah dilakukan terlebih dahulu tentang capsman diantaranya penulisan terkait analisis dan perancangan centralized authentication access point menggunakan CAPsMAN pada jaringan komputer PT. Media Sarana Data Subnet Solo [4] menerangkan bahwa

penggunaan capsman dapat untuk mengontrol beberapa perangkat access point. Pada penelitian selanjutnya adalah mengenai analisa perbandingan kinerja fitur Mikrotik CAPsMAN dengan konfigurasi tunnel dan tanpa menggunakan tunnel pada router mikrotik Rb951-2n [2] menjelaskan Perbandingan Kinerja Fitur Mikrotik CAPsMAN dengan konfigurasi tunnel dan tanpa menggunakan tunnel pada Router Mikrotik.

Pada penulisan terkait yang ketiga adalah mengenai implementasi controller access point system manager (CAPsMAN) dan Wireless Distribution System (WDS) Jaringan Wireless di SMK Terpadu Al Ishlahiyah Singosari Malang [5], menjelaskan tentang keamanan internet dengan wpa-psk, manajemen bandwidth menggunakan queue tree dan per Connection queue dengan menerapkan capsman dan WDS. Beberapa penelitian lainnya adalah melakukan penelitian terkait dengan manajemen bandwidth [6], [7], dan implementasi pengembangan jaringan yang dilakukan terhadap beberapa objek yang diterapkan [8].

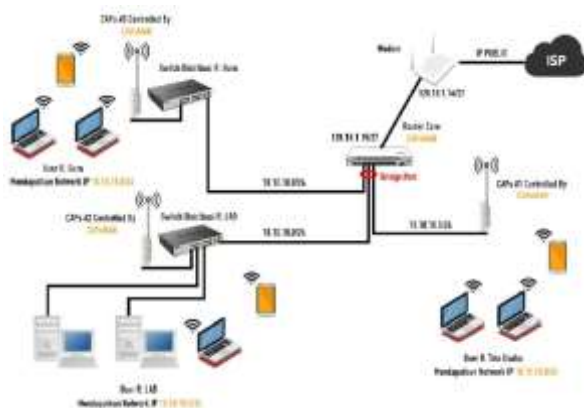
Sedangkan penelitian ini yang akan disajikan adalah tentang bagaimana melakukan manajemen pada wireless access point atau hotspot dengan menggunakan capsman dan memudahkan user dalam mengakses internet tanpa harus login kembali untuk mendapatkan akses internet ketika berpindah hotspot atau access point.

III. METODE PENELITIAN

Metode yang digunakan dalam pengembangan jaringan adalah metode NDLC dengan beberapa tahapan dimulai dari analysis, design, simulation / prototyping, implementation, monitoring dan management.

A. Analysis

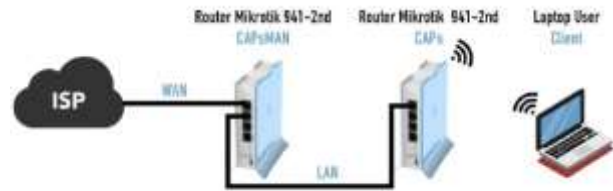
Pada tahapan ini dilakukan pengumpulan data yang diperlukan kebutuhan user yaitu kebutuhan hardware yang diantaranya adalah Router menggunakan mikrotik sebagai core router atau router utama yang akan dijadikan CAPsMAN, Access Point menggunakan mikrotik sebagai pemancar jaringan wireless (CAPs) yang sudah di konfigurasi di Router CAPsMAN, serta Laptop Client dibutuhkan untuk pengujian sistem jaringan yang baru. Selain itu terdapat Kebutuhan Software berupa Browser yang digunakan untuk tes hasil implementasi adalah google chrome dan Command prompt ini digunakan untuk memastikan status akses internet tidak terputus saat berpindah ruangan. Berdasarkan analisis kebutuhan pada Gbr.1 adalah design jaringan.



Gbr. 1 Rancangan topologi Jaringan

B. Simulation / Prototyping

Pada tahap ini berdasarkan kinerja awal dari jaringan yang akan dibangun dan sebagai bahan pertimbangan sebelum jaringan benar-benar akan diterapkan. pada tahap ini menggambarkan secara simulasi atau uji coba jaringan menggunakan 2 buah perangkat Mikrotik 941-2nd [9] sebagai CAPsMAN dan CAPs, penerapan seperti pada Gbr.2.



Gbr. 2 Topologi jaringan pada simulasi

C. Implementation

Pada tahap ini langkah-langkah konfigurasi Access List Controller Access Point System Manager (CAPsMAN) pada Mikrotik, yaitu Membuat Mikrotik CAPsMAN mendapatkan akses internet, Melakukan konfigurasi IP Address untuk Network bridge Mikrotik CAPs. Selin itu dilakukan konfigurasi aktifasi CAPsMAN pada fitur CAPsMAN serta menambahkan list Mac Address Vendor yang akan dilakukan filtering. Tahapan selanjutnya adalah melakukan konfigurasi CAPs pada Mikrotik CAPs 1 dan 2 pada fitur wireless dengan cara mencentang CAPs, ditunjukkan oleh Gbr.3, Gbr.4, Gbr.5, dan Gbr.6.

```
Terminal
Mikrotik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPs-1] > interface enable wlan1
[admin@CAPs-1] >
```

Gbr. 3 Mengaktifkan Interface Wlan1

```
Terminal
Mikrotik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPs-1] > interface wireless cap set enabled=yes interfaces=wlan1 discover
y-interfaces-ether1 bridge-mcna
[admin@CAPs-1] >
```

Gbr. 4 Mengaktifkan CAP Pada CAPs 1

Pada tahapan Konfigurasi pada Mikrotik CAPsMAN dilakukan seperti ditunjukkan pada Gbr. 7 sampai dengan Gbr.16. Proses tahapan Konfigurasi MAC Mask Access List

CAPsMAN dilakukan seperti pada Gbr.17 dan Gbr.18. Pada tahapan menerapkan hasil konfigurasi *template Access Point* dilakukan seperti pada Gbr.19.

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPs-1] > interface enable wlan1
[admin@CAPs-1] >

```

Gbr. 5 Mengaktifkan Interface Wlan1

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPs-2] > interface wireless cap set enabled=yes interfaces-wlan1 discovery
~interface-ether1 bridge-mnns
[admin@CAPs-2] >

```

Gbr. 6 Mengaktifkan CAP Pada CAPs 2

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPs-2] > ip dhcp-client add interface-ether1 disabled=no
[admin@CAPs-2] >
[admin@CAPs-2] >

```

Gbr. 7 Konfigurasi DHCP Client

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPsMAN] > interface bridge add name-bridge_CAP
[admin@CAPsMAN] > interface bridge port add bridge-bridge_CAP interface-ether2
[admin@CAPsMAN] > interface bridge port add bridge-bridge_CAP interface-ether3
[admin@CAPsMAN] > interface bridge port add bridge-bridge_CAP interface-ether4
[admin@CAPsMAN] >

```

Gbr. 8 Konfigurasi Bridge Untuk CAPs

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPsMAN] > ip address add address-10.10.10.1/24 interface-bridge_CAP
[admin@CAPsMAN] >

```

Gbr. 9 Konfigurasi IP Address Bridge CAP

```

Terminal
[admin@CAPsMAN] > ip dhcp-server setup
Select interface to run DHCP server on
dhcp server interface: bridge_CAP
Select network for DHCP addresses
dhcp address space: 10.10.10.0/24
Select gateway for given network
gateway for dhcp network: 10.10.10.1
Select pool of ip addresses given out by DHCP server
addresses to give out: 10.10.10.2-10.10.10.254
Select DNS servers
dns servers: 8.8.8.8,8.8.4.4
Select lease time
lease time: 10m
[admin@CAPsMAN] > ip dhcp-server pr
Flags: X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 dhcp1 bridge_CAP dhcp_pool0 10m
[admin@CAPsMAN] >

```

Gbr. 10 Konfigurasi DHCP Server

```

Terminal
MikroTik RouterOS 6.42.9 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPsMAN] > ip firewall nat add chain=srcnat action=masquerade out-interface=ether1
[admin@CAPsMAN] >

```

Gbr. 11 Konfigurasi NAT Jaringan

```

Terminal
MikroTik RouterOS 6.40.9 (c) 1999-2018 http://www.mikrotik.com/

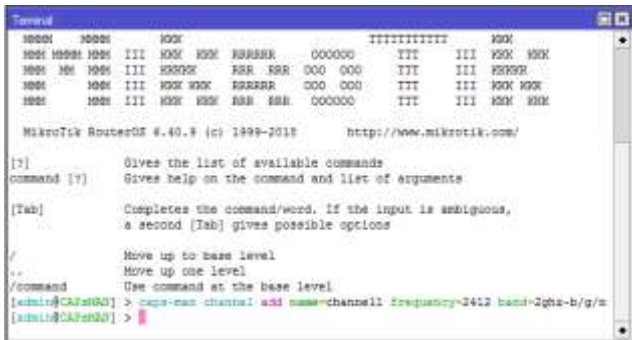
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

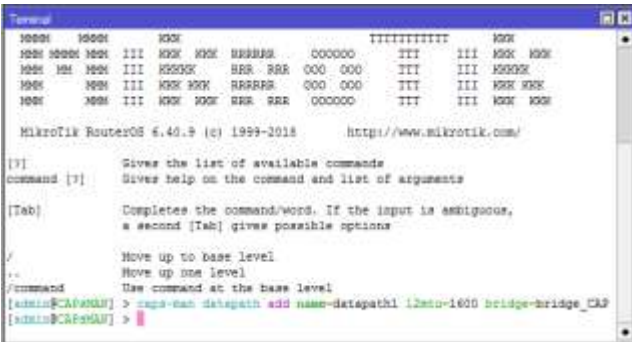
/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@CAPsMAN] > cap-man manager set enabled=yes
[admin@CAPsMAN] >

```

Gbr. 12 Konfigurasi CAPs Manager



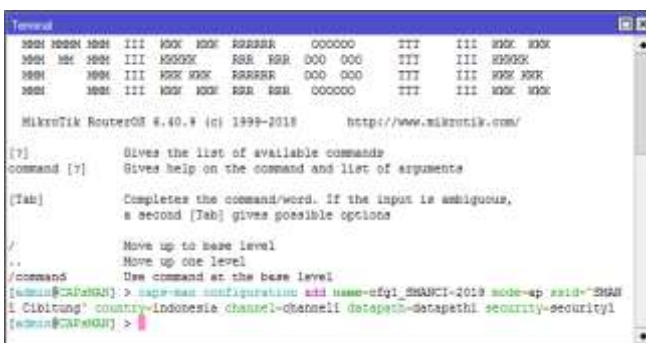
Gbr. 13 Konfigurasi Template Channel



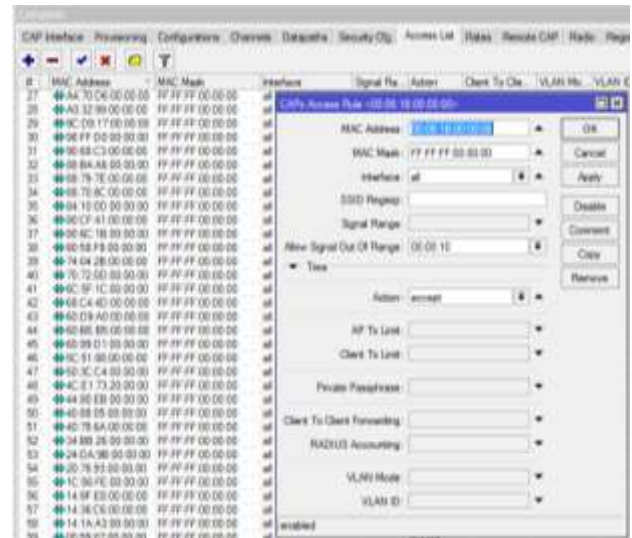
Gbr. 14 Konfigurasi Template Datapath



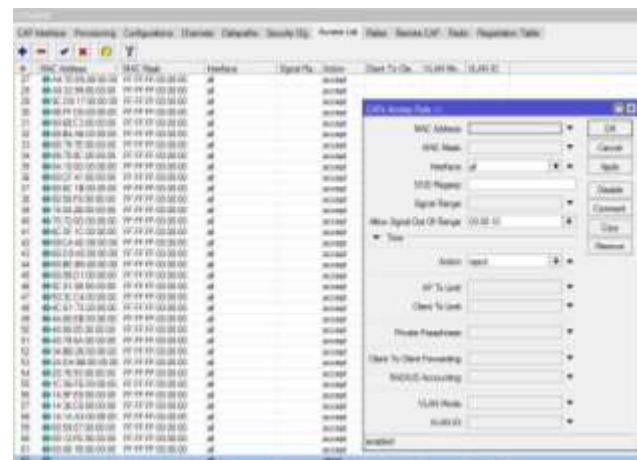
Gbr. 15 Konfigurasi Template Security Cfg



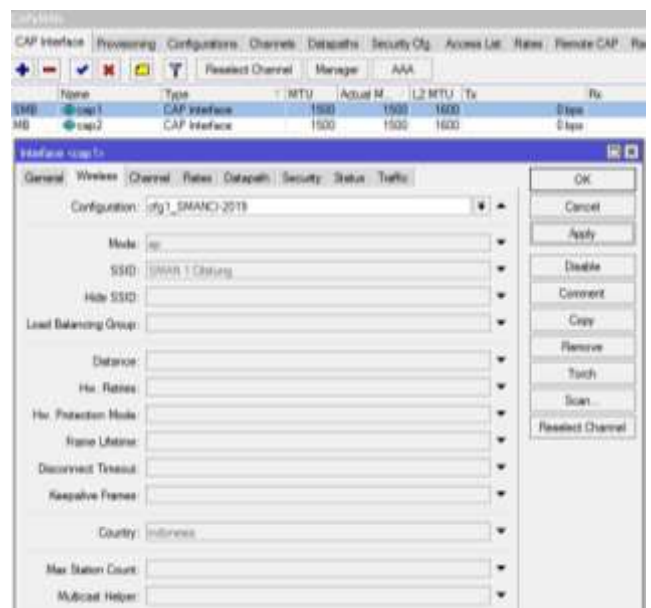
Gbr. 16 Konfigurasi Template Master Cfg



Gbr. 17 MAC Mask CAPs Access Rule Allow



Gbr. 18 MAC Mask CAPs Access Rule Reject



Gbr. 19 Menerapkan Template Access Point

D. Monitoring

Untuk memastikan kedua perangkat Mikrotik CAPs atau access point ini terdeteksi oleh Mikrotik CAPsMAN. Pada tahapan ini langkah-langkah untuk memonitoring jaringan yang telah dibangun berupa melakukan pengamatan pada pemantauan *traffic* yang berjalan di jaringan sudah sesuai dengan semestinya [10], melihat koneksi yang aktif pada jaringan, serta evaluasi *Controller Access Point* secara terpusat.

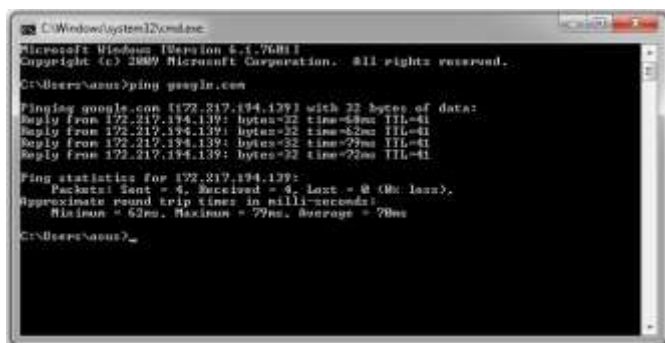
E. Management

Pada tahap ini penulis akan menjelaskan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yang diharapkan. Diantara langkah-langkah yang akan dilakukan adalah membuat *Wireless Password* agar tidak sembarang orang dapat masuk ke jaringan tersebut, serta melakukan *backup* konfigurasi yang dilakukan agar sewaktu-waktu terjadi hal yang dapat membuat jaringan rusak kita dapat mengembalikan pada konfigurasi semula.

IV. HASIL DAN PEMBAHASAN

Pada pembahasan disini dilakukan setelah pengujian dengan melakukan koneksi internet semua berjalan dengan sukses dan tanpa error. Pada gbr.20 merupakan tes akses internet yang dilakukan. Selanjutnya pengujian CAPs yang sudah *running* dan berhasil melayani *user*, ditandai dengan status *RSMB* dan menerima *traffic*, *RSMB* = *Running Slave Master Bound*, seperti pada Gbr.21.

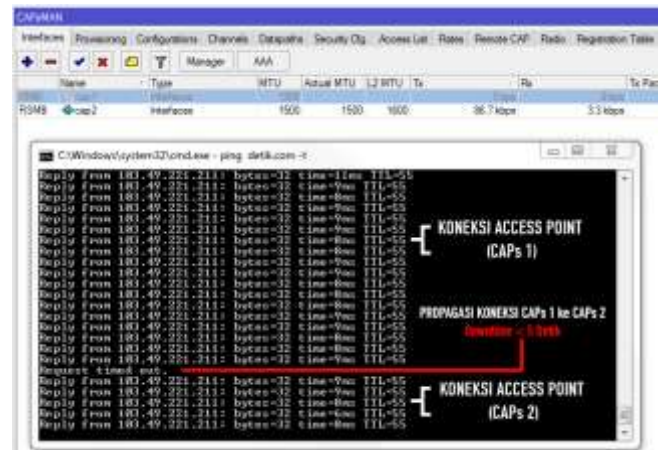
Pengujian perpindahan koneksi *access point*, hasil dari pengujian ini berjalan dengan baik dimana saat dilakukan perpindahan koneksi *access point* user tidak perlu lagi *login* untuk mendapatkan akses internet secara legal, hal ini dikarenakan *access point* CAPs 1 dan CAPs 2 memiliki *SSID* yang sama yang dikontrol oleh CAPsMAN dan pada saat perpindahan koneksi *access point* jaringan internet yang terhubung tidak mengalami *downtime* yang lama, *downtime* yang terjadi berlangsung dibawah 5 detik, hal ini dikarenakan adanya propagasi koneksi perangkat yang terhubung dari CAPs 1 ke CAPs 2. Penggambaran *realtime* perpindahan koneksi *access point* diperlihatkan pada Gbr.22.



Gbr. 20 Tes Koneksi ke internet



Gbr. 21 Status CAPs Telah Sukses Melayani User



Gbr. 22 Realtime Perpindahan Koneksi Access Point

Pengujian *MAC Mask Access List* CAPsMAN, hasil dari pengujian ini berjalan dengan baik dimana saat dilakukan implementasi *MAC Mask Access List* CAPsMAN perangkat yang sebelumnya terhubung ke CAPs 1 Dan CAPs 2 menjadi berkurang menyisakan perangkat dengan *vendor* *Lenovo* lah yang dapat terkoneksi ke CAPs 1 dan CAPs 2 dikarenakan *rules* yang telah dibuat pada menu *Access List* CAPsMAN hanya mengizinkan perangkat dengan *mac address* *vendor* *Lenovo* lah yang dapat terkoneksi, selain *mac address* *vendor* *Lenovo* sesuai *rules* akan di *reject* atau tidak diizinkan untuk terkoneksi ke CAPs 1 dan CAPs 2, diperlihatkan pada Gbr.23.

Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Us
cap1	SMAN 1 Gbong	AC C1 EE FE 42 72	135Mbps-40MHz/15	135Mbps-40MHz/15	0	21.00	
cap2	SMAN 1 Gbong	68 76 3F 5F 38 38	65Mbps-20MHz/15	65Mbps-20MHz/15	0	39.00	
cap3	SMAN 1 Gbong	10 2A B3 4C 13 F9	135Mbps-40MHz/15	135Mbps-40MHz/15	0	22.00	
cap1	SMAN 1 Gbong	98 FF D0 68 BFC3	135Mbps-40MHz/15	135Mbps-40MHz/15	0	23.00	

Gbr. 23 Sebelum Rule Mac Mask diaktifkan

Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Us
cap2	SMAN 1 Gbong	98 FF D0 68 BFC3	135Mbps-40MHz/15	135Mbps-40MHz/15	0	40.00	

Gbr. 24 Setelah Rules MAC Mask diaktifkan

Selanjutnya pada Gbr.24 hanya perangkat *Lenovo* dengan *MAC Mask* *98:FF:D0* yang dapat terkoneksi ke CAPs, perangkat lain yang bukan *vendor* *Lenovo* tidak dapat terkoneksi ke CAPs dikarenakan *rules* *MAC Mask Access List* CAPsMAN yang telah diaktifkan. Dapat dilihat pada *Registration Table* setelah *rules* diaktifkan *user* yang terkoneksi ke CAPs berkurang dan menyisakan *user* yang menggunakan *MACAddress* *Vendor* *Lenovo* yang bisa terkoneksi.

V. KESIMPULAN

Dari hasil pengujian diatas terdapat beberapa kesimpulan yaitu dengan terbangunnya *Controller Access Point System Manager* (CAPsMAN), dapat membantu pengguna dalam

melaksanakan aktifitas perkantoran, belajar mengajar tanpa memikirkan terputus jaringan internet serta tidak perlu *login* kembali saat berpindah tempat dari ruangan satu ke ruangan yang lainnya. CAPsMAN berfungsi sebagai *wireless* manajemen pada perangkat berbasis Mikrotik sangat membantu pengelola perangkat jaringan. Data dalam uji coba ini, pada beberapa perangkat Controlled Access Point (CAP) dapat di manajemen dengan mudah secara bersamaan oleh CAPsMAN. *Mac Mask Access List CAPsMAN* berfungsi untuk memfilter perangkat yang terkoneksi kedalam sebuah *access point* yang sudah dicontrol oleh CAPsMAN.

Sebagai pengembangan selanjutnya dari penelitian yang dilakukan penulis, maka penulis memberikan saran yaitu hasil perancangan jaringan ini masih sederhana dapat dikembangkan lagi baik dari segi *design* maupun fungsi-fungsi yang tersedia di CAPsMAN secara keseluruhan.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis kepada pihak yang membantu seperti puskom STMIK Bani Saleh dalam mengakses perangkat untuk, dan kepada mahasiswa yang membantu dalam melakukan penelitian sehingga jurnal ini dapat diselesaikan.

DAFTAR PUSTAKA

- [1] I. Sofana, *Membangun Jaringan Komputer Mudah Membuat Jaringan Komputer (Wire & Wireless) Untuk Pengguna Windows dan Linux*. Bandung: Informatika, 2013.

- [2] 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, 2016.
- [3] Mikrotik ID, "MAC Mask pada Access List CAPsMAN," *mikrotik ID*. [Online]. Available: http://www.mikrotik.co.id/artikel_lihat.php?id=312 . [Accessed: 29-Jun-2019].
- [4] B. Novianto, "Analisis Dan Perancangan Centralized Authentication Access Point Menggunakan Capsman Pada Jaringan Komputer Pt. Media Sarana Data Subnet Solo," Sekolah Tinggi Manajemen Informatika Dan Komputer AMIKOM YOGYAKARTA, 2015.
- [5] Ratnasari, S. Dwi, E. Farida, and N. Firdaus, "Implementasi Controller Access Point System Manager (CAPsMAN) Dan Wireless Distribution System (WDS) Jaringan Wireless Di SMK Terpadu Al Ishlahiyah Singosari Malang," in *Seminar Nasional Sistem Informasi (SENASIF)*, 2017, pp. 624–635.
- [6] Z. M. Subekti and A. Suwarno, "Analisis Perbandingan Manajemen Bandwidth Jaringan Wifi Autentikasi User Password Methode Hierarchical Token Bucket (HTB) dengan Per Connection Queue (PCQ)," *J. INFORMATICS, Sci. Technol.*, vol. 8, no. 1, 2018.
- [7] A. R. Mukti and R. N. Dasmen, "Prototipe Manajemen Bandwidth pada Jaringan Internet Hotel Harvani dengan Mikrotik RB 750r2," *J. Inform. J. Pengemb. IT*, vol. 4, no. 2, pp. 87–92, 2019.
- [8] A. W. Syaputra and S. Assegaff, "Analisis Dan Implementasi Load Balancing Dengan Metode Nth Pada Jaringan Dinas Pendidikan Provinsi Jambi," *J. Manaj. Sist. Inf.*, vol. 2, no. 4, pp. 831–844, 2017.
- [9] R. Towidjojo, *Mikrotik Kungfu Kitab 2*. Jakarta: Jasakom, 2013.
- [10] S. Melwin, *Pengantar jaringan komputer*. Yogyakarta: Penerbit ANDI, 2005.