

IMPLEMENTASI PENDAFTARAN HOTSPOT MENGGUNAKAN MIKROTIK *APPLICATION PROGRAMMING INTERFACE* (API) PADA JARINGAN *WIRELESS DISTRIBUTION SYSTEM* (WDS) UNTUK PENINGKATAN PENGELOLAAN JARINGAN

Ahmad Roziqin ¹, Joko Triyono ², Rr. Yulia Rachmawati Kusumaningsih ³

¹Jurusan Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta

Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029

ahmadroziqin488@gmail.com¹, jack@akprind.ac.id², yuliana@akprind.ac.id³

Abstract

The increasing number of internet users today has a positive impact on the development of internet connectivity media. The high mobility demand makes many people switch to using wireless internet-based access media rather than wired or cable media. One of these wireless media breakthroughs in the development of hotspot-based internet access services. The authentication methods used by these service providers vary, starting with using 1 key (password) together with encryption methods such as WEP, WPA. In terms of security, the use of a captive portal with the method of 1 keyword for 1 user is better than the use of 1 keyword together. In this service, the user must first have a username and password that has been created by the manager of the hotspot. Based on these problems generated research that aims to create a web-based hotspot registration system to make it easier for new users to get internet services at the ISPR AKPRIND campus. This application is developed based on Web using PHP Programming Language, MikroTik PHP Class API, and MySQL Database for registering, managing, and verifying user data. The benefit obtained from this research is the smooth running of hotspot service users by applying the username and password for each user. The results of the study are expected to be a solution to overcome the problem of managing hotspot services at the AKPRIND YOGYAKARTA Institute of Science & Technology.

Keywords: Hotspot, API Class PHP, Mikrotik

Abstrak

Peningkatan jumlah pengguna internet dewasa ini berdampak positif pada perkembangan media konektivitas internet. Tuntutan mobilitas yang tinggi membuat banyak orang beralih menggunakan media pengaksesan internet berbasis *wireless* ketimbang media *wired* atau kabel. Salah satu terobosan media *wireless* ini adalah pengembangan layanan akses internet berbasis *hotspot*. Metode *otentifikasi* yang digunakan para penyedia layanan ini berbeda-beda, mulai dengan menggunakan 1 kunci (password) secara bersama dengan metode enkripsi seperti *WEP*, *WPA*. Di tinjau dari aspek keamanan, penggunaan *captive* portal dengan metode 1 kata kunci untuk 1 pengguna lebih baik di bandingkan penggunaan 1 kata kunci secara bersama-sama. Pada layanan ini pengguna harus terlebih dahulu memiliki *username* dan *password* yang telah dibuat oleh pengelola *hotspot*. Berdasarkan dari permasalahan tersebut dihasilkan penelitian yang bertujuan untuk menciptakan sistem pendaftaran hotspot berbasis web agar memudahkan pengguna baru untuk mendapatkan layanan internet dikampus IST AKPRIND. Aplikasi ini dikembangkan berbasis Web dengan memanfaatkan Bahasa Pemrograman PHP, API PHP Class MikroTik, dan Database MySQL untuk pendaftaran, pengelolaan, dan verifikasi data pengguna. Manfaat yang diperoleh dari penelitian ini adalah kelancaran penggunaan layanan hotspot dengan penerapan *username* dan *password* untuk tiap pengguna. Hasil penelitian diharapkan dapat menjadi solusi mengatasi permasalahan pengelolaan layanan hotspot pada Institut Sains & Teknologi AKPRIND YOGYAKARTA.

Kata kunci: Hotspot, API Class PHP, Mikrotik

Pendahuluan

Peningkatan jumlah pengguna internet dewasa ini berdampak positif pada perkembangan media konektivitas internet. Tuntutan mobilitas yang tinggi membuat banyak orang beralih menggunakan media pengaksesan internet berbasis *wireless* ketimbang media *wired*. Salah satu terobosan media *wireless* ini adalah pengembangan layanan akses internet berbasis *hotspot*. Metode *otentikasi* yang digunakan para penyedia layanan ini berbeda-beda, mulai dengan menggunakan 1 kunci (password) secara bersama dengan metode enkripsi seperti *WEP*, *WPA*. Pada saat ini gedung baru kampus III IST AKPRIND menggunakan sistem *captive portal* yang mengharuskan pengguna memasukkan *username* dan *password* yang telah disediakan oleh admin untuk menggunakan layanan hotspot dan belum menggunakan sistem *WDS*. Di tinjau dari aspek keamanan, penggunaan *captive portal* dengan metode 1 kata kunci untuk 1 pengguna lebih baik di bandingkan penggunaan 1 kata kunci secara bersama-sama. Pada layanan ini pengguna harus terlebih dahulu memiliki *username* dan *password* yang telah dibuat oleh pengelola *hotspot*.

Berdasarkan pada permasalahan tersebut, perlu dirancang sistem yang memungkinkan pengguna layanan *hotspot* melakukan pendaftaran secara mandiri dan pengelola *hotspot* hanya perlu melakukan verifikasi validitas data sesuai dengan ketentuan yang diterapkan.

Tinjauan Pustaka

Implementasi *Hotspot Login Menggunakan Capsman Mikrotik Pada Wilayah Yang Berbeda*. Merupakan penelitian yang menerapkan *hotspot login* menggunakan *CAPsMAN* yang disinergikan dengan *Userman* dan *Radius Server* yang menggunakan topologi *Extended Service Set* dan menghubungkan antar wilayah melalui VPN menjadikan jaringan *wireless* tersebut akan dikendalikan dipantau dan dikonfigurasi secara terpusat, menghadirkan fitur Otentikasi, Otorisasi dan Akuntansi dalam *userman* menjadikan jaringan tersebut bisa digunakan menggunakan akun tersendiri, dengan menggunakan VPN untuk interkoneksi menjamin penggunaan akun dapat dilakukan menggunakan akun yang sama, dan menerapkan topologi *extended service set* dapat menghasilkan jaringan yang stabil tanpa adanya gangguan terputus. (Sandi, 2019)

Implementasi Sistem Autentikasi User Menggunakan Radius Server dan Active Directory Pada Jaringan Wireless Di Pt. Kudo Teknologi Indonesia. Pada penelitian ini, guna menunjang dan membangun sistem itu, dilakukan konfigurasi pada beberapa titik, seperti pada *Radius Server*, *Mikrotik*, *Switch* dan *Access Point*. Penelitian dan implementasi sistem dilaksanakan di PT. Kudo Teknologi Indonesia pada kantor cabang Kudoplex 1. Tahapan yang dilakukan adalah membuat topologi dan desain jaringan *wireless*, penentuan IP Address yang akan digunakan. Melakukan konfigurasi hingga pengujian hasil implementasi sistem. Hasil akhir yang diuji adalah keberhasilan koneksi yang dilakukan oleh pengguna, dan pengujian keamanan. Dengan implementasi sistem ini, akan menjadikan jaringan *wireless* di PT. Kudo Teknologi Indonesia menjadi lebih terjamin keamanannya, hingga akan menjaga stabilitas dan konektivitas pada jaringan *wireless* yang digunakan oleh pengguna. (Pratama, 2019)

Perancangan Sistem *Single Sign-On* Terintegrasi Pada Jaringan Universitas Multimedia Nusantara. Penelitian ini menghasilkan purwarupa yang akan diaplikasikan secara langsung kepada sistem sebenarnya. Proyek ini menggunakan basis sistem operasi Windows Server yang digunakan sebagai *Server* dan juga menggunakan fitur *Hotspot* pada *MikroTik* yang dimiliki oleh UMN dan mengintegrasikan login form website dan web application untuk melakukan autentikasi kepada *Active Directory Server* sehingga setiap *user* hanya memiliki satu akun dan satu kata sandi untuk semua aplikasi yang ada di UMN sesuai dengan konsep *single sign-on*. Dengan perancangan sistem *single-sign on* yang dikerjakan dalam penelitian ini membuat semua sistem yang sudah ada di UMN ini memiliki satu database kredensial. Setiap perubahan hanya akan dilakukan sekali saja dan akan tersinkronisasi pada semua sistem. Permasalahan muncul pada saat semua sistem mengakses satu database kredensial yang sama sehingga terjadi *bottleneck* pada sistem, sehingga perlu dilakukan beberapa optimisasi yaitu dengan melakukan *load balancing* melalui *clustering* dan *backup failover* sehingga *request* yang diterima oleh *Server* akan dibagi secara *round robin* sehingga dapat membagi beban. (Leonard, 2016).

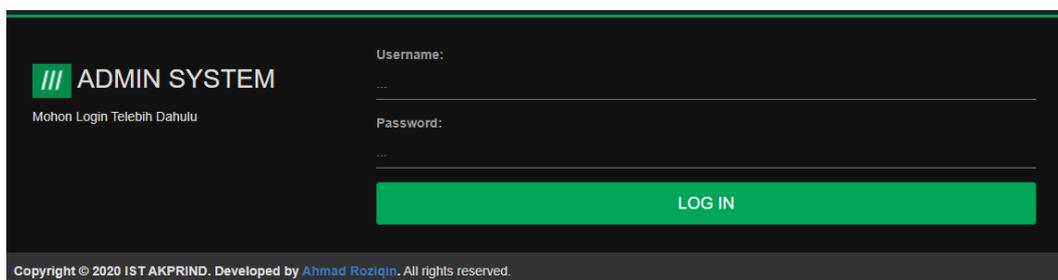
Jaringan *Hotspot* Berbasis *Mikrotik* Menggunakan Metode Otentikasi Pengguna (User). Pada penelitian yang lain dibahas implementasi jaringan hotspot menggunakan *Mikrotik Router Board* sebagai server utama jaringan *hotspot*. Keamanan jaringan ini menggunakan metode

otentikasi guna mengontrol dan membatasi setiap *user* yang akan menggunakan jaringan *hotspot*. Manajemen *bandwidth* pada setiap *user* juga diperlukan dengan tujuan agar penggunaan jaringan internet dapat berjalan dengan lancar dan stabil sesuai dengan kebutuhan penggunaannya. Metode penelitian yang digunakan yaitu diagram *fishbone* yang meliputi empat tahapan 1). Identifikasi. 2). Pengadaan perangkat software & hardware. 3). Perancangan / desain jaringan 4). Konfigurasi jaringan hotspot berbasis mikrotik RB750 ini menggunakan topologi star, dimana pada port 1 menggunakan (IP:192.168.1.1), port 2 (IP:192.168.120.1), port 3 (IP:192.168.130.1), port 4 (IP:192.168.140.1) port 5 (IP:192.168.150.1). konfigurasi user hotspot meliputi 4 clien yaitu: 1). Dosen, 2). Karyawan, 3). Mahasiswa, 4). Tamu. konfigurasi bandwidth user : 1). Dosen rx/tx 3Mbps/3Mbps. 2). Karyawan rx/tx 2Mbps/2Mbps. 3). Mahasiswa rx/tx 1Mbps/1Mbps. 4) Tamu rx/tx 512Kbps/512Kbps. (Ardianto, 2018).

Berdasarkan empat penelitian di atas, mengacu pada penelitian Rifki Wahyu Pratama, yang berjudul Implementasi Sistem Autentikasi *User* Menggunakan *Radius Server* dan *Active Directory* Pada Jaringan *Wireless* Di Pt. Kudo Teknologi Indonesia. maka akan dibangun sistem pendaftaran mandiri pada *hotspot* gedung baru kampus III IST APRIND. Pada penelitian diatas belum dibangun *hotspot* dengan memanfaatkan *API mikrotik*, dengan itu penelitian ini akan membangun *hotspot* dengan memanfaatkan fitur *API mikrotik* dan penelitian ini tidak membangun *Radius server* seperti halnya penelitian sebelumnya. Pada penelitian ini juga akan dilakukan pendaftaran pengguna hotspot secara mandiri dan akan di verifikasi melalui email yang telah didaftarkan sehingga nantinya admin akan mengaktifkan *user* baru tersebut.

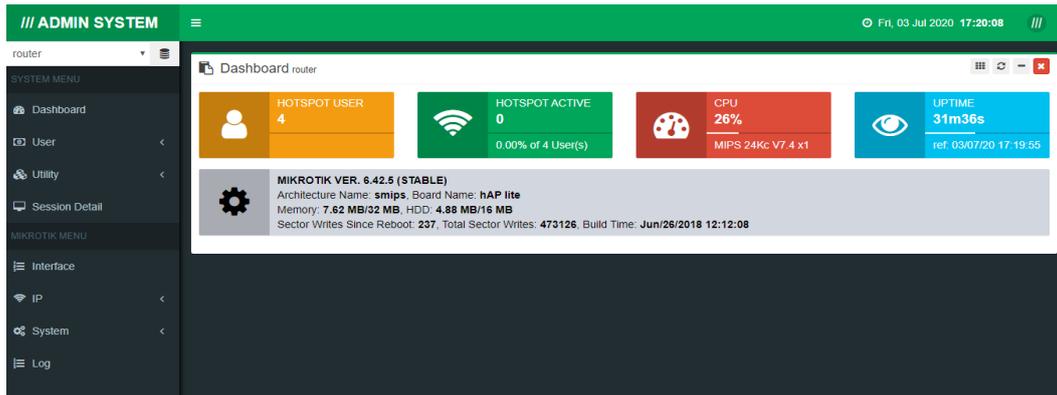
Pembahasan

Bab ini menampilkan hasil dan pembahasan dari penelitian implementasi pendaftaran *hotspot* menggunakan *mikrotik application programming interface (API)* pada jaringan *wireless distribution system (WDS)* untuk peningkatan pengelolaan jaringan pada gedung baru kampus 3 IST AKPRIND YOGYAKARTA. Dari penelitian ini didapatkan hasil yaitu, halaman web untuk admin dan halaman registrasi untuk *user*. Pada gambar 1 merupakan halaman login untuk admin.



Gambar 1. Login Admin

Halaman admin merupakan halaman bagi admin untuk mengaktifkan *user* yang telah melakukan registrasi dan sudah *terverifikasi* melalui email. Pada nantinya admin akan inputkan username dan password ke sistem mikrotik melalui mikrotik API. Halaman admin dapat dilihat pada gambar 2.



Gambar 2. Halaman Admin

Dalam melakukan pendaftaran baru disistem *hotspot* ini dilakukan secara *online* dan mandiri dengan website akprindhotspot.000webhostapp.com/register sehingga nantinya *user* dapat menentukan *username* dengan yang diinginkan. Sedangkan untuk *password* akan ditentukan secara acak oleh sistem yang berupa angka.

IST AKPRIND HOTSPOT

Register

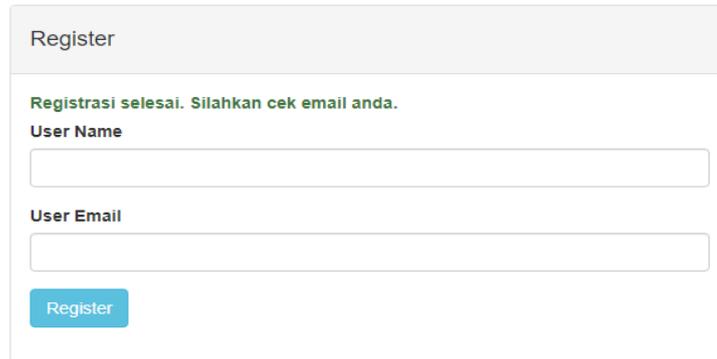
User Name

User Email

Gambar 3. Proses Pendaftaran Pengguna Baru

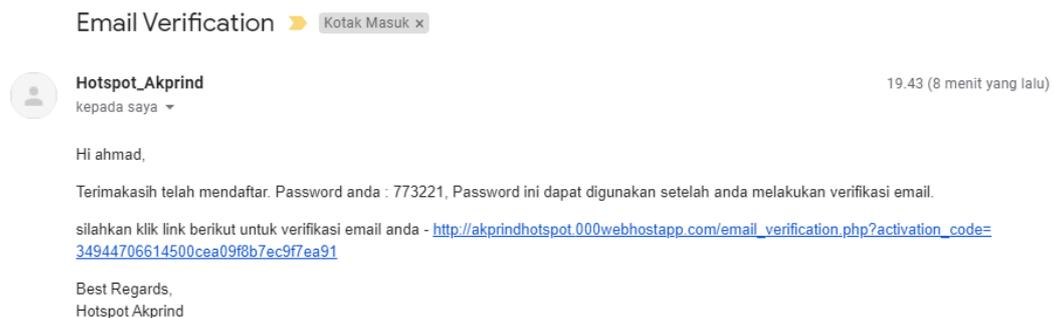
Pada gambar 3 merupakan proses pendaftaran baru oleh *user* dengan mengisi *username* dan *email* yang akan digunakan. Dalam hal ini *email* harus aktif, jika *email* tidak aktif maka pesan verifikasi tidak akan terkirim atau *user* tidak bisa memverifikasi emailnya tersebut. Pada sistem pendaftaran ini tidak mengizinkan satu *email* digunakan secara bersama dengan kata lain jika *email* sudah terdaftar maka akan tersimpan pada *database* sistem, jadi ketika *user* akan memasukkan *email* yang sama dan sudah terdaftar sudah dipastikan akan ditolak oleh sistem. jika *form* pendaftaran sudah diinputkan maka akan ditampilkan seperti pada gambar 4 dan akan ada *notification* di atas *form* yang menjelaskan bahwa pendaftaran selesai dan *user* akan diarahkan untuk memeriksa *email* yang sudah dikirim dari sistem *hotspot* untuk memverifikasi *email* yang sudah diinputkan.

IST AKPRIND HOTSPOT



Gambar 4. Daftar Selesai

Dalam tahap ini *user* belum dapat menggunakan *username* dan *password* yang sudah di kirimkan ke *email*. Maka dari itu *user* perlu memverifikasi *email* dengan cara klik *link* yang sudah dicantumkan dalam *email*. Berikut merupakan contoh isi dari *email* verifikasi dapat dilihat pada gambar IV.32.



Gambar 5. Email Verifikasi

Setelah *user* mendaftar dan memverifikasi *email*, maka *admin* memiliki tugas untuk mengaktifkan *username* dan *password* *user* yang baru agar nantinya *user* dapat melakukan *login* pada halaman *hotspot*. Pada aktivasi ini dilakukan *admin* menggunakan halaman *admin* dengan memanfaatkan fitur API Mikrotik, sebelum menambahkan *user* seorang *admin* akan menyambungkan antara halaman *admin* dengan *router* menggunakan API Mikrotik yang bertujuan untuk memudahkan *admin* dalam melakukan kontrol terhadap *router*. Untuk melakukan koneksi antara halaman *admin* dengan *router* dapat dilihat pada gambar 6.

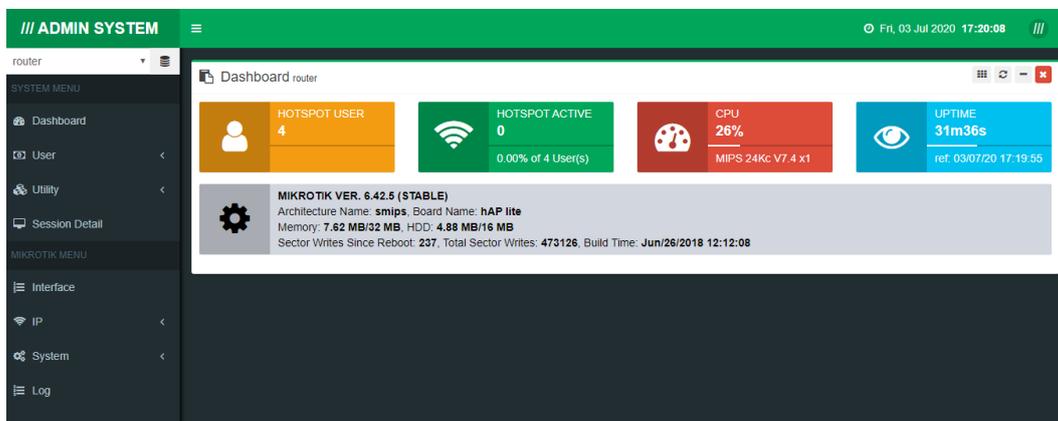


Gambar 6. Add Router

Pada halaman utama *admin* klik logo *session* menu untuk menambahkan *router* yang akan dijadikan sebagai *hotspot*.

Gambar 7. Proses Input Router

Gambar 7 merupakan proses dari penambahan atau memilih jika sudah pernah diinputkan. *Admin* harus memasukkan nama *router host* mikrotik atau ip login mikrotik dapat menggunakan kabel atau secara wireless lalu port API Mikrotik secara *default port* API menggunakan 8728 selanjutnya inputkan juga *username* dan *password login* mikrotik yang sama dengan *username* dan *password* yang digunakan untuk *login* melalui *winbox* lalu tinggal tekan tombol *connect*. Pada tahap selanjutnya *admin* akan memilih sesi *router* yang telah ditambahkan sebelumnya agar *admin* dapat menambahkan *user hotspot* dan kontrol *router* tanpa menggunakan *winbox*. Dengan tampilan yang mudah dimengerti oleh kebanyakan orang maka sistem ini dapat memudahkan pekerjaan seorang *admin*. Halaman utama *admin* setelah berhasil koneksi dengan mikrotik dapat dilihat pada gambar 8.



Gambar 8. Halaman Utama Admin

Ketika seorang *admin* berhasil melakukan kontrol *router* melalui halaman *admin* yang berbasis *web* akan tercatat *log* aktivitas *login* pada *router* melalui API mikrotik. Berikut merupakan log aktivitas pada *router* mikrotik dapat dilihat pada gambar 9.

Jul/10/2020 21:05:33	memory	system, info, account	user admin logged in from 192.168.2.254 via api
Jul/10/2020 21:05:33	memory	system, info, account	user admin logged out from 192.168.2.254 via api
Jul/10/2020 21:05:37	memory	system, info, account	user admin logged in from 192.168.2.254 via api
Jul/10/2020 21:05:37	memory	system, info, account	user admin logged out from 192.168.2.254 via api
Jul/10/2020 21:05:44	memory	system, info, account	user admin logged in from 192.168.2.254 via api
Jul/10/2020 21:05:44	memory	system, info, account	user admin logged out from 192.168.2.254 via api
Jul/10/2020 21:05:56	memory	system, info, account	user admin logged in from 192.168.2.254 via api
Jul/10/2020 21:05:57	memory	system, info, account	user admin logged out from 192.168.2.254 via api
Jul/10/2020 21:06:16	memory	system, info, account	user admin logged in from 192.168.2.254 via api
Jul/10/2020 21:06:16	memory	system, info, account	user admin logged out from 192.168.2.254 via api

Gambar 9. Log Aktivitas Router

selanjutnya yaitu *admin* menambahkan *user* yang sudah melakukan registrasi kedalam sistem *hotspot* mikrotik dengan cara klik menu *user* pada halaman admin lalu pilih *add user hotspot* maka akan tampil sebuah tabel yang akan menampilkan isi dari *user* yang sudah ada sebelumnya. Tabel tersebut dapat dilihat pada gambar 10.

no.	.id	name	password	server	profile	address	mac-address	limit-uptime	LU (m)	uptime	U (m)	session-time-left	ST
2	*1	admin	***		default					38m13s	38		
1	*0	default-trial	***							0s	0		
4	*3	kamu	***	hotspot1	default					2m59s	2		
3	*2	saya	***	hotspot1	default					0s	0		

Gambar 10. Halaman User Hotspot

Setelah muncul seperti tampilan pada gambar 10 lalu pilih *add new* setelah dipilih akan diarahkan ke *form* pengaktifan *user* baru. Adapun isian *form* tersebut antara lain pemilihan *server hotspot*, *profil hotspot*, *username* dan *password*. Gambar 11 merupakan *form* untuk penambahan *user* baru, jika sudah diisi dengan baik dan benar lalu klik *save changes* untuk menyimpan *user* baru tersebut.

Hotspot User

Basic | Advanced | Limits

Server: all

Profile: default

Name:

Password:

Disabled: No

Save changes Close

Gambar 11. Submenu Basic

Didalam *form* penambahan *hotspot* ada tiga submenu yang masing-masing memiliki fungsi berbeda yang pertama seperti pada gambar 11 yang merupakan gambar dari menu *basic* yang berfungsi menambahkan user dengan secara singkat tanpa menambahkan embel-embel lainnya.

Selanjutnya terdapat submenu *advanced* yang berfungsi untuk menambahkan *user* dengan lebih detail lagi seperti menambahkan alamat IP,MAC *address* dan lain-lain. Tampilan submenu *advanced* dapat dilihat pada gambar 12.

The screenshot shows a web form titled 'Hotspot User' with three tabs: 'Basic', 'Advanced', and 'Limits'. The 'Advanced' tab is selected. It contains the following fields:

- Address:** A text input field.
- MAC Address:** A text input field.
- Routes:** A text input field.
- Email:** A text input field.
- Comment:** A larger text area for notes.

 At the bottom right, there are two buttons: 'Save changes' (highlighted in blue) and 'Close'.

Gambar 12. Submenu Advance

Lalu terdapat submenu *limits* berfungsi bagi *admin* yang menginginkan setiap *user* untuk membatasi *bandwidth* atau untuk membedakan antara *user* prioritas dan *user* tamu. Pembatasan *bandwidth* ini juga berfungsi bagi yang memiliki kapasitas internet yang tidak terlalu besar agar mencukupi kebutuhan internet tanpa menambah *bandwidth* dari *ISP*. Berikut merupakan tampilan dari menu *limits* dapat dilihat pada gambar 13.

The screenshot shows the 'Limits' tab of the 'Hotspot User' form. It contains the following fields:

- Limit Uptime:** A text input field with a note below it: 'Example: 1w2d3h4m5s (w=week, d=day, h=hour, m=minute, s=second)'. The input field is currently empty.
- Limit Bytes In:** A text input field with a '0' in a small box to its right.
- Limit Bytes Out:** A text input field with a '0' in a small box to its right.
- Limit Bytes Total:** A text input field with a '0' in a small box to its right.

 At the bottom right, there are two buttons: 'Save changes' (highlighted in blue) and 'Close'.

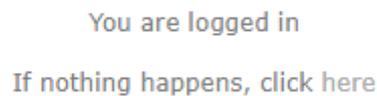
Gambar 13. Submenu Limits

Pada tahap ini *user* hanya tinggal menyambungkan ke jaringan *wifi hotspot* dengan *username* dan *password* yang dimiliki agar dapat menikmati jaringan internet dari *hotspot* yang sudah di bangun, halaman *login hotspot* dapat dilihat pada gambar 14.



Gambar 14. Login Page Hotspot

Setelah memasukan *username* dan *password* pengguna pada *web browser smartphone*, jika *username* dan *password* benar maka pengguna akan otomatis masuk ke halaman selamat datang seperti ditunjukkan oleh gambar 15.



Gambar 15. Login Sukses

Kesimpulan

Berdasarkan pengujian yang sudah dilakukan, dihasilkan beberapa kesimpulan dibawah ini.

1. Pendaftaran pengguna dapat dilakukan secara mandiri melalui web pendaftaran yang tersedia.
2. Sistem ini akan mengirimkan username dan password ke email yang sudah didaftarkan guna untuk verifikasi email.
3. Admin dapat melakukan kontrol atau aktivasi pengguna baru melalui sistem admin yang terhubung menggunakan API mikrotik.

Saran

Dalam pembuatan sistem ini penulis merasakan banyak sekali kekurangan, oleh karna itu masukan dan saran yang sifatnya membangun yang perlu penulis harapkan sehingga harapannya sistem ini kedepannya jauh lebih bagus dengan banyak fitur tambahan seperti:

1. Mengirimkan verifikasi username dan password melalui Whatsapp
2. Pengguna dapat melakukan pendaftaran melalui sistem yang terhubung dengan API mikrotik langsung, sehingga admin tidak perlu aktivasi pengguna baru agar nantinya alur pendaftaran dapat diperpendek dan mempersingkat waktu.
3. Untuk pengembangan selanjutnya dapat menggunakan SMTP dari Google dan untuk email verifikasi tidak masuk dalam kategori spam.
4. Pada penelitian ini *backbone* masih menggunakan kabel *utp* dikarenakan jika menggunakan *wireless* sistem *wds* belum bisa berjalan dengan semestinya. Selain itu penggunaan perangkat yang berbeda merk belum dapat diterapkan sistem *wds* dengan *backbone wireless*. Oleh karena itu harapan kedepannya dapat dikembangkan lagi agar sistem ini dapat diterapkan dengan lebih mudah.

Daftar Pustaka

- Ardian, W. C. (2016). *ANALISA DAN PERANCANGAN WIRELESS DISTRIBUTION SYSTEM (WDS) PADA HOTSPOT*. Yogyakarta: STMIK AMIKOM Yogyakarta.
- Ardianto, F. (2018). JARINGAN HOTSPOT BERBASIS MIKROTIK MENGGUNAKAN METODE OTENTIKASI PENGGUNA (USER). *Jurnal Surya Energy* Vol. 2 No. 2.
- Basta, D. (2015). *MIKROTIK ROUTER OS API*. YOGYAKARTA: mum.mikrotik.com/presentations.
- Leonard, A. (2016). PERANCANGAN SISTEM SINGLE SIGN-ON TERINTEGRASI. Skripsi. Universitas Multimedia Nusantara.
- Nijim, S. (2014). *APIs for dummies a wiley brand*. United States of America: Jhon wiley & Sons, inc .
- Pratama, R. W. (2019). Implementasi Sistem Autentikasi User Menggunakan Radius Server dan Active Directory Pada Jaringan Wireless Di Pt. Kudo Teknologi Indonesia. skripsi. Politeknik Negeri Jakarta.
- Sandi, T. A. (2019). IMPLEMENTASI HOTSPOT LOGIN MENGGUNAKAN CAPSMAN MIKROTIK PADA WILAYAH YANG BERBEDA. Volume 4 Nomor 1 Edisi Februari 2019 (18-26) .
- Solichin, A. (2016). *Pemrograman Web dengan PHP dan MySQL*. jakarta: Universitas Budi Luhur, Jakarta.
- Towidjojo, R. (2016). *Mikrotik Kung Fu : Kitab 4*. jakarta: jasakom.
- Towidjojo, R. (2017). *Mikrotik Hotspot Server*. jakarta: [ilmujaringan\(dot\)com](http://ilmujaringan(dot)com).