

Manajemen Otentikasi Pengguna Hotspot menggunakan Radius pada Jaringan Wireless berbasis Controller (Studi Kasus: STMIK PalComTech)

HOTSPOT USER AUTHENTICATION MANAGEMENT BY USING A RADIUS SERVER AS WIRELESS LAN CONTROLLER (CASE STUDY: STMIK PALCOMTECH)

Mahmud*

STMIK PalComTech: Jln. Basuki Rahmat No. 05, Telp:0711-358916 Palembang
Jurusa Teknik Informatika, STMIK PalComTech
e-mail: *m4h86mud@gmail.com

Abstrak

STMIK PalComTech merupakan salah satu perguruan tinggi swasta yang telah menerapkan teknologi jaringan *wireless*. Keamanan jaringan yang berbasis *wireless (hotspot)* yang digunakan pada suatu perguruan tinggi sangatlah penting, maka diperlukan sebuah manajemen *user* dan *password* untuk memastikan bahwa orang yang berhak mendapatkan akses ke dalam jaringan hotspot. Selain itu fleksibilitas dalam pengelolaan manajemen *user* dan *password* yang terintegrasi dengan *worksheet* masing-masing mahasiswa, karyawan dan dosen merupakan hal yang sangat penting. Penelitian ini bertujuan untuk mengimplementasikan sistem otentikasi pengguna *hotspot* dengan menggunakan Radius dengan melakukan pembatasan penggunaan berdasarkan besaran kuota volume data dan memiliki integrasi dalam pengelolaan user dan *password*. Setiap mahasiswa, karyawan dan dosen akan mendapatkan masing-masing user dan password yang digunakan untuk akses ke jaringan hotspot. Selain itu sistem ini juga dapat melakukan pembuatan voucher hotspot berdasarkan skema kuota volume/time.

Kata kunci— hotspot, wireless, freeradius, volume data, time data

Abstract

STMIK PalComTech is one of the private universities that has implemented wireless network technology. Wireless network security (hotspots) that are used in a college is very important, so a user and password management is needed to ensure that people who are entitled to get access to a hotspot network. In addition, flexibility in managing user management and passwords that are integrated with each student's worksheet, employee and lecturer is very important. This study aims to implement a system of authentication for hotspot users by using Radius through usage restrictions based on the amount of data quota volume and has integration in the management of users and passwords. Every student, employee and lecturer will get each user and password used for access to hotspot networks. In addition, this system can also make hotspot vouchers based on the quota volume / time scheme.

Keywords --- hotspot, wireless, freeradius, volume data, time data

1. PENDAHULUAN

Terdapat ratusan komputer yang digunakan di dunia, oleh karena itu tekanan dari pengguna sistem terhadap cara-cara berkomunikasi di antara semua mesin ini tak terelakkan lagi[1]. Salah satu tipe jaringan adalah *Local Area Network (LAN)* yaitu

jaringan komputer yang dibangun pada area terbatas seperti ruangan, kantor dan kampus[1]. Dengan adanya jaringan komputer ini maka seluruh pengguna komputer dapat terhubung dari manapun melalui *internet*. Dalam perkembangannya jaringan komputer memiliki media komunikasi berbasis *wireless*, dengan adanya media tersebut maka mobilitas dari pengguna internet menjadi semakin meningkat. Penyediaan *hotspot* oleh pengelola jaringan dengan menggunakan media jaringan *wireless*, tentu akan meningkatkan layanan internet dan memberikan kemudahan bagi para pengguna internet. *Hotspot* adalah tempat khusus yang disediakan untuk mengakses internet menggunakan peralatan *Wi-Fi*[2]. Dibalik kemudahan tersebut, pengelolaan *hotspot* memiliki kerentanan dalam hak akses, karena siapapun dapat terhubung ke jaringan apabila berada di area jangkauan *wireless*. Sehingga penyediaan internet bagi para pengguna yang benar-benar berhak yang dapat menggunakan atau mendapatkan akses ke jaringan menjadi sangat penting. Manajemen otentikasi *user* dan *password* pada *hotspot* menggunakan Radius dapat memberikan hak akses kepada pengguna internet ke dalam jaringan. Radius (*Remote Authentication Dial-in User Service*) yang berfungsi untuk menyediakan mekanisme keamanan dan manajemen user pada jaringan komputer.

Pada penelitian sebelumnya mengenai pemanfaatan Radius sebagai manajemen user dan *password* pada jaringan komputer yaitu yang pertama dilakukan oleh Raymond Powers Tenggario dan Jonathan Lukas pada manajemen jaringan *wireless* menggunakan *server* Radius menyimpulkan bahwa pembatasan akses pengguna dapat dilakukan berdasarkan *time based* (waktu) atau *volume data* (paket) dan dengan menggunakan Radius mekanisme pengelolaan user dapat dilakukan secara terpusat[3].

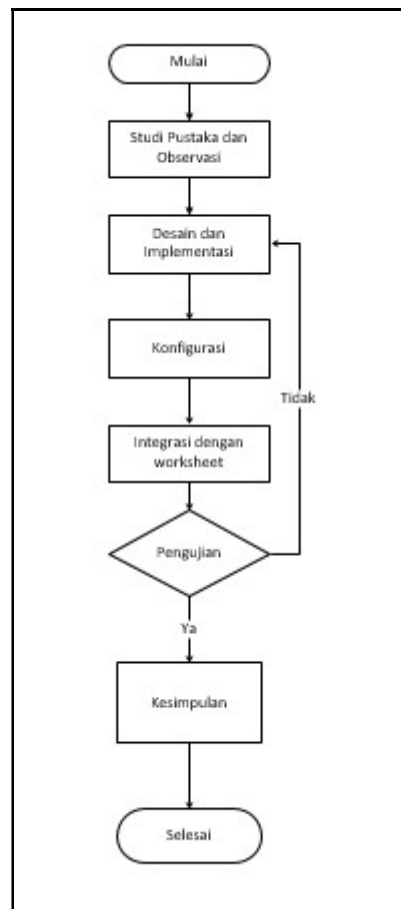
Penelitian yang dilakukan oleh Denda Aristiara dan Cahyani Budihartanti tentang otentikasi pengguna jaringan menggunakan Radius windows 2008 *server* pada PT. Pertamina memberikan kesimpulan bahwa dengan penggunaan Radius membuat mekanisme keamanan dalam jaringan tersedia serta adanya sistem otentikasi dan otorisasi untuk pengguna jaringan kabel, membuat akses pengguna jaringan menjadi lebih aman, sehingga tidak sembarang orang dapat menggunakan jaringan kabel untuk akses ke sistem jaringan perusahaan[4].

Penelitian yang dilakukan oleh Apolinarius Gusala, Suwanto Raharjo dan Naniek Widyastuti tentang Implementasi Freeradius pada jaringan *hotspot* dengan menggunakan MYSQL dan EAP-TLS menyimpulkan bahwa otentikasi *user* terpusat memudahkan *administrator* dan *user* menggunakan sumber daya jaringan dengan menggunakan proses otentikasi EAP-TLS. Penggunaan Freeradius dengan MYSQL dan EAP-TLS dapat memberi keamanan yang berlapis pada jaringan *hotspot*[5].

Pada penelitian ini diawali dengan melakukan observasi serta studi pustaka untuk menentukan solusi sehingga dapat diimplementasikan ke dalam jaringan, serta pengelolaan manajemen Radius menggunakan *Web Base Administration Control Panel* dengan penerapan pembatasan akses berdasarkan *volume based* (paket data) dan pengelolaan *user* dan *password* dapat dilakukan dari *worksheet* masing-masing.

2. METODE PENELITIAN

Penelitian ini memiliki beberapa tahapan yang akan dilaksanakan yaitu meliputi perencanaan sampai dengan menghasilkan sebuah kesimpulan, yang dapat dilihat dari gambar rancangan penelitian berikut ini:



Gambar 1. Rancangan Penelitian

1. Studi Pustaka dan Observasi
Pada tahap ini dilakukan pengumpulan bahan-bahan referensi, yang nantinya akan dijadikan sumber informasi dalam menyelesaikan masalah yang sedang diteliti. Bahan-bahan referensi yang didapat baik dalam bentuk buku-buku teori, modul praktikum, ataupun informasi yang didapat dari suatu halaman *web* di *internet*[1], dalam hal ini mengenai implementasi *freeradius*.
2. Desain dan Instalasi
Melakukan perancangan terhadap topologi jaringan yang telah berjalan serta melakukan instalasi *freeradius*.
3. Konfigurasi
Melakukan konfigurasi pada router dan *Web based Administration Control Panel freeradius* dengan menggunakan panduan pada *Radius Manager Billing System User Manual*[6].
4. Integrasi dengan *worksheet*
Melakukan konfigurasi pada *worksheet* yang diintegrasikan dengan *freeradius*.
5. Pengujian
Melakukan pengujian terhadap sistem yang dibuat
6. Kesimpulan
Membuat kesimpulan dari hasil pengujian

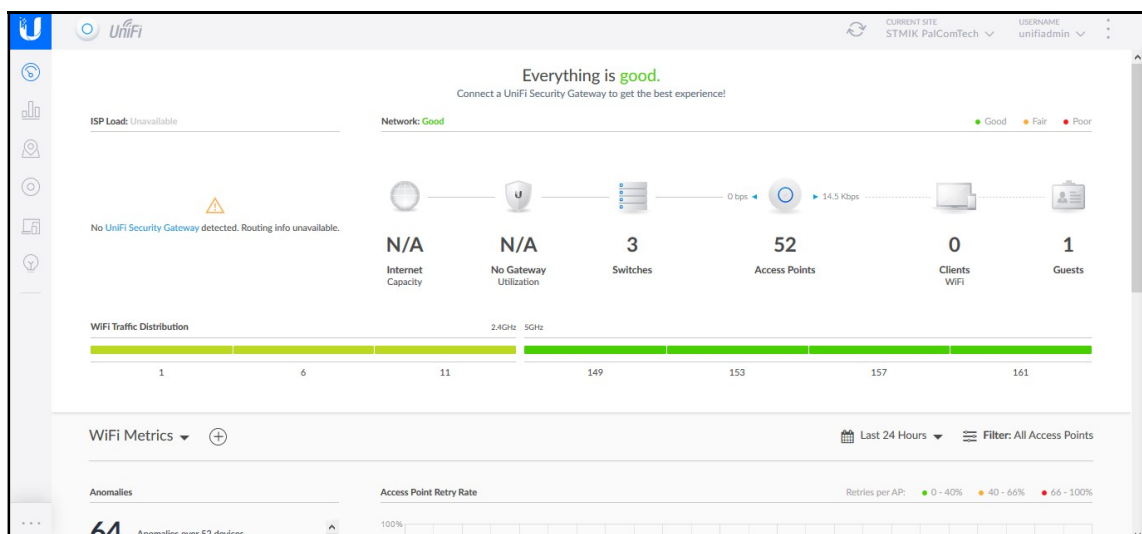
3. HASIL DAN PEMBAHASAN

Pada penelitian ini, Penulis melakukan implementasi Radius *Server* untuk pengelolaan otentikasi user dan password bagi para mahasiswa, dosen dan karyawan yang terintegrasi ke *worksheet* masing-masing. Pada tahapan-tahapan dalam penelitian ini adalah sebagai berikut:

a) Studi Pustaka dan Observasi

Pada tahapan awal ini Penulis melakukan observasi ke lapangan untuk mengambil beberapa data sebagai berikut:

1. Sudah memiliki jaringan *hotspot* bagi para mahasiswa, dosen dan karyawan
2. Perangkat *hardware* yang digunakan yaitu: Access Point menggunakan Unifi AP, Router menggunakan mikrotik, Switch menggunakan Unifi Switch yang memiliki Gigabit ethernet yang berbasis manageable switch dan Media Kabel menggunakan Belden *Category* 6.
3. Untuk pengelolaan/manajemen jaringan *wireless* menggunakan controller dari Unifi
4. Memiliki 52 titik *access point*.
5. Semua lingkungan dalam gedung sudah terjangkau ke dalam jaringan *hotspot*.
6. Jumlah *device*/perangkat yang terkoneksi dalam satu waktu lebih kurang maksimal 300 perangkat
7. Semua perangkat dapat bebas mendapatkan akses ke dalam jaringan *hotspot*.

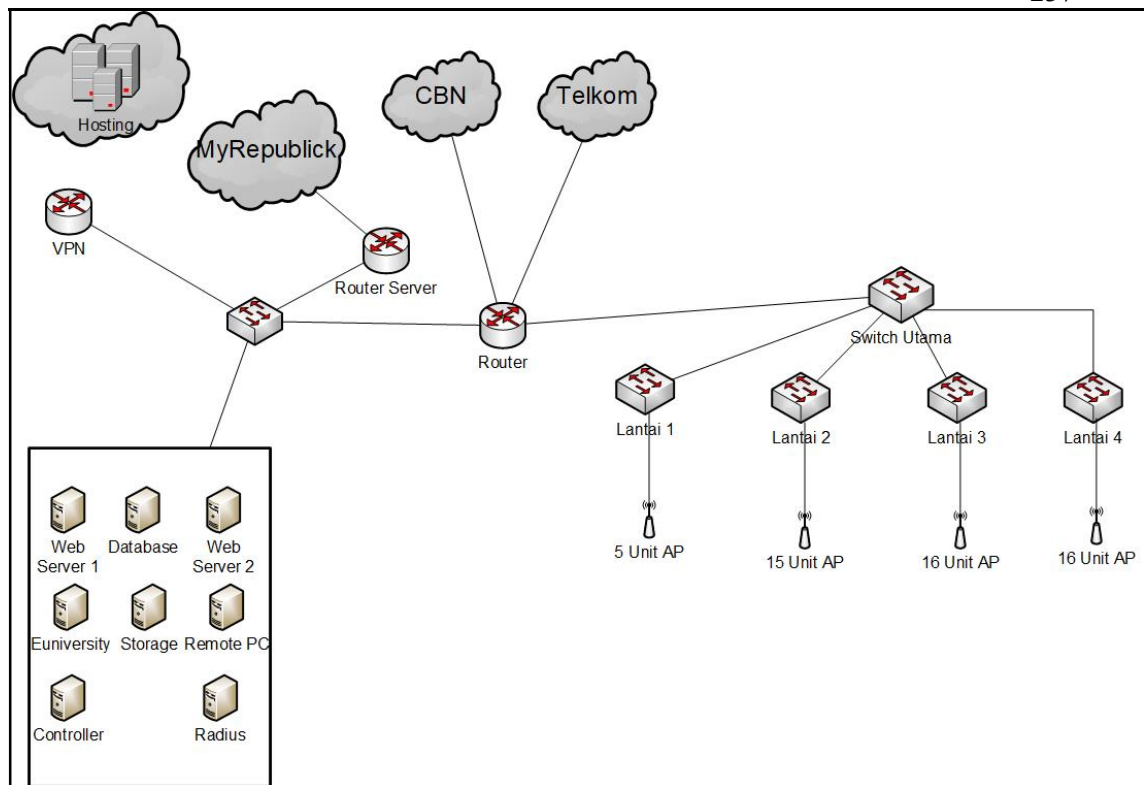


Gambar 2. Unifi Controller

Selain dari jurnal-jurnal yang Penulis jadikan sebagai referensi, Penulis juga memanfaatkan search engine dari google untuk mengembangkan solusi dari permasalahan.

b) Desain dan Instalasi

Pada rancangan topologi jaringan yang di lakukan untuk penelitian, tidak diperlukan perubahan pada topologi. Jadi topologi yang digunakan adalah topologi yang sudah existing. Berikut di bawah ini adalah gambar topologi jaringan *existing*:



Gambar 3. Topologi Jaringan Komputer STMIK PalComTech

Pada gambar 3, menggambarkan bahwa topologi yang digunakan merupakan topologi star, menggunakan 52 Access Point yang tersebar di lingkungan gedung STMIK PalComTech dan memiliki sebuah switch utama dan switch di setiap lantai, menggunakan mikrotik sebagai router dan memiliki sebuah unifi controller untuk manajemen access point dalam jaringan. Adapun model *Access Point* yang digunakan yaitu Unifi AP Pro dan Unifi AC Lite, kedua model tersebut telah mendukung jaringan *wireless IEEE 802.11ac*.

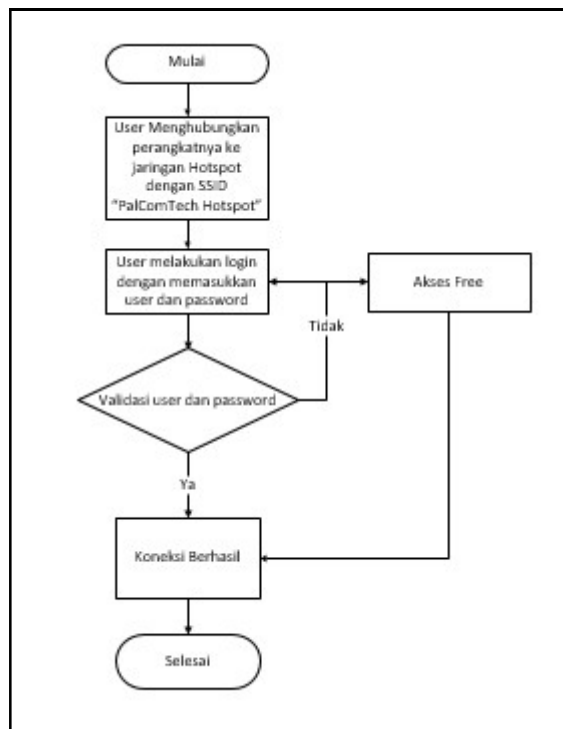
Setelah memastikan topologi jaringan, Penulis melakukan instalasi pada *server*. Aplikasi yang dipakai pada *server* Radius yaitu *Freeradius* yang menggunakan *Radius Manager* sebagai *Web Based Administration Control Panel*. *Radius Manager* ini merupakan sebuah Control Panel Radius yang dapat memudahkan bagi para administrator jaringan dalam melakukan manajemen pada *Radius Server* dan *user* dalam mengelola informasi mengenai *account*-nya seperti yang di tunjukkan pada gambar 4 dibawah ini.



Gambar 4. Radius Manager sebagai *Web Administration Control Panel Radius Server*

c) Konfigurasi

Pada tahapan konfigurasi Penulis menerapkan *captive portal* yang di konfigurasi dari *router* mikrotik, *captive portal* ini berfungsi sebagai otentikasi bagi para pengguna jaringan hotspot dengan memasukkan *user* dan *password* yang telah di berikan melalui *worksheet*. Dalam hal kebijakan akses ke jaringan *hotspot*, memiliki 2 akses yaitu Akses Reguler dan Akses *Free*. Pada Akses Reguler setiap masing-masing user memiliki kuota *volume data* sebesar 5 GB per bulan, yang mana di setiap akhir bulan akan direset kuotanya menjadi 0 secara otomatis oleh sistem. Dan pada akses *Free* memiliki *volume data* tidak terbatas namun dibatasi dari sisi kecepatan akses yaitu sebesar 512 Kbps per *user*. Dibawah ini merupakan skema untuk akses ke jaringan *hotspot*:



Gambar 5. Skema akses ke jaringan *hotspot*

Pada gambar 5, menunjukkan bahwa setiap *user* harus melakukan otentikasi terlebih dahulu untuk mendapatkan akses ke dalam jaringan *hotspot*, bila *user* tersebut bisa mendapatkan akses ke jaringan dengan memasukkan *user* dan *password* yang akan divalidasi oleh *server radius* maka koneksi akan berhasil, namun apabila *user* dan *password* tidak dapat di validasi oleh *server radius* maka *user* diminta untuk memasukkan ulang *user* dan *password*. Kemungkinan dari kegagalan di validasi oleh *server* adalah salah kombinasi *user* dan *password* atau kuota sudah *expire* (habis). Apabila *user* tidak memiliki kuota lagi maka dapat menggunakan akses *Free*.

d) Integrasi dengan worksheet

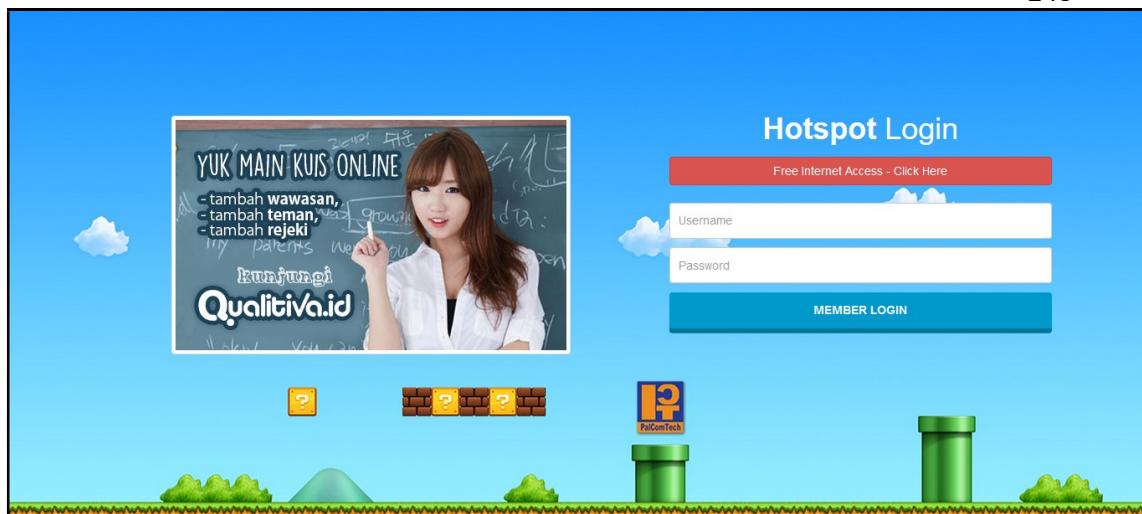
Pada tahapan integrasi yaitu dengan melakukan *input query* ke *database MySQL* pada *server Radius* melalui *worksheet* yang dimiliki masing-masing mahasiswa, dosen dan karyawan. Dalam *worksheet* tersebut memiliki 1 fitur yaitu *Password Hotspot* yang disediakan untuk mengelola *user* dan *password* setiap pengguna, ini dapat dilihat pada gambar 6.

Gambar 6. Manajemen *user* dan *password hotspot* pada *worksheet*

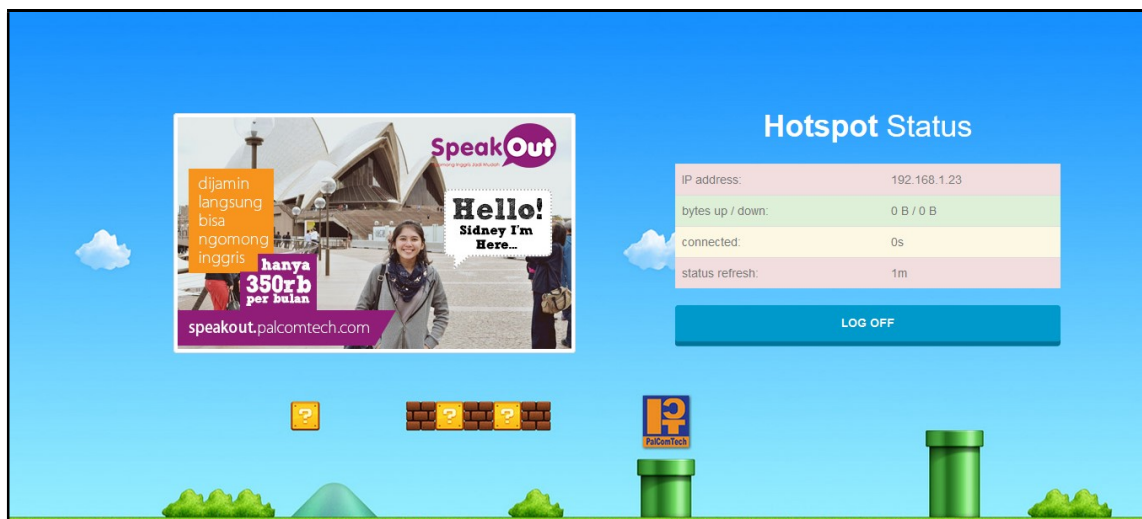
Dalam gambar 6 tersebut menunjukkan pengguna memiliki akses ke dalam jaringan *hotspot* dengan mendapatkan sebuah *user* dan *password* serta memiliki kuota sebesar 5 GB. Untuk *password* disediakan fitur untuk membuat *password* baru apabila pengguna tidak ingat terhadap *password* sebelumnya. Pada *input data query* MYSQL pada *server radius*, tabel yang digunakan adalah *radcheck* dan *rm_users*.

e) Pengujian

Dari hasil pengujian sistem otentikasi pengguna *hotspot* pada jaringan komputer di STMIK PalComTech menggunakan Radius Manager cukup praktis dan efisien. Untuk mendapatkan akses ke jaringan *hotspot* pengguna melakukannya dengan menghubungkan perangkatnya ke jaringan *hotspot* melalui SSID PalComTech Hotspot, setelah itu secara otomatis perangkat akan diarahkan ke halaman *login (captive portal)* yang muncul melalui *browser* dapat dilihat pada gambar 7. *Captive Portal* adalah suatu teknik autentikasi dan pengamanan data yang lewat dari *network* internal ke *network* eksternal [7]. Setelah itu pengguna memasukkan *user password* yang telah di dapatkan dari *worksheet*, yang apabila berhasil akan di arahkan halaman *hotspot* status seperti pada gambar 8. Selain akses Reguler, pengguna *hotspot* juga dapat menggunakan akses *Free* yang di digunakan tanpa perlu *user* dan *password* melalui halaman *login*.



Gambar 7. Halaman *Login Hotspot*




Gambar 8. Halaman *Hotspot Status*

Pengguna juga dapat melihat status penggunaan kuota, seperti pada gambar 9. Dengan fitur *user detail* ini maka pengguna hotspot dapat mengetahui penggunaan sementara dan status dari kuota yang dimiliki, status *active* yaitu masih memiliki kuota serta dapat di gunakan dan untuk status *expire* yaitu *account* sudah tidak dapat digunakan dikarenakan kuota habis. Di bagian *traffic report* pengguna dapat melihat penggunaan setiap harinya berapa besar jumlah *data* yang di habiskan.


Home Traffic report List invoices Change password Redeem voucher Purchase credits Change service

User's details



General information

User name:	[redacted]
Account type:	regular
Account status:	active
Static IP address:	n/a
Allowed MAC address:	n/a
Deposit:	0.00 IDR
Language:	English



Service data

Active service:	Regular
Service type:	postpaid
Download datarate:	5120 kbps (10240 kbps)
Upload datarate:	5120 kbps (10240 kbps)
Next service change date:	n/a
Scheduled service name:	n/a

Traffic report

Date	User name	Online time	Download	Upload	Total
2018-09	[redacted]	00:20:35	521.4 kB	342.6 kB	864.0 kB
2018-10	[redacted]	3d 08:04:30	5.0 GB	491.4 MB	5.5 GB

Found: 4

Gambar 9. Halaman User detail account hotspot

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

Reset Counters Reset All Counters

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit
168 D	<hotspot-pct-berry_alhazi>	192.168.3.248	5242880	5242880		
89 D	<hotspot-pct-berry_alhazi-2>	192.168.0.219	5242880	5242880		
66 D	<hotspot-pct-benny_effendi>	192.168.3.172	5242880	5242880		
152 D	<hotspot-pct-benny_trianra>	192.168.2.138	5242880	5242880		
80 D	<hotspot-pct-benedictus_effendi>	192.168.0.232	5242880	5242880		
69 D	<hotspot-pct-arsia>	192.168.2.251	5242880	5242880		
37 D	<hotspot-pct-aprilia_13>	192.168.0.241	5242880	5242880		
64 D	<hotspot-pct-andri_saputra>	192.168.0.183	5242880	5242880		
40 D	<hotspot-pct-alfred_tenggono>	192.168.1.185	5242880	5242880		
231 D	<hotspot-pct-alan_saputra>	192.168.2.100	5242880	5242880		
246 D	<hotspot-pct-alamasyah>	192.168.3.129	5242880	5242880		
0 D	<hotspot-pct-akbar12>	192.168.1.245	5242880	5242880		
9 D	<hotspot-pct-ahmad_db>	192.168.1.27	5242880	5242880		
29 D	<hotspot-pct-adyansyah>	192.168.2.6	5242880	5242880		
24 D	<hotspot-pct-abadwitama>	192.168.0.228	5242880	5242880		
126 D	<hotspot-pct-Samuel_h>	192.168.0.174	5242880	5242880		
10 D	<hotspot-T-FC:42:03:44:43:AD>	192.168.1.35	256k	512k		
244 D	<hotspot-T-F4:F5:DB:18:8D:3C>	192.168.3.147	256k	512k		
243 D	<hotspot-T-F4:F5:DB:0A:A8:E5>	192.168.3.155	256k	512k		
21 D	<hotspot-T-F4:37:B7:33:A6:76>	192.168.3.195	256k	512k		
30 D	<hotspot-T-F0:6D:78:40:ED:C0>	192.168.3.136	256k	512k		
228 D	<hotspot-T-EC:D0:9F:12:EA:12>	192.168.2.246	256k	512k		
202 D	<hotspot-T-EC:51:BC:61:EF:41>	192.168.3.220	256k	512k		
169 D	<hotspot-T-EC:51:BC:60:21:87>	192.168.2.126	256k	512k		
113 D	<hotspot-T-E4:C4:83:4E:78:C1>	192.168.0.205	256k	512k		
235 D	<hotspot-T-E4:C4:83:4C:D2:6F>	192.168.3.169	256k	512k		
197 D	<hotspot-T-E4:C4:83:4B:AE:DB>	192.168.3.229	256k	512k		
227 D	<hotspot-T-E4:5A:A2:E1:1D:60>	192.168.3.185	256k	512k		
205 D	<hotspot-T-E0:B5:2D:D0:38:45>	192.168.3.199	256k	512k		
189 D	<hotspot-T-E0:99:71:CF:35:DE>	192.168.2.104	256k	512k		
127 D	<hotspot-T-E0:62:67:63:75:C5>	192.168.0.201	256k	512k		
6 D	<hotspot-T-DC:85:DE:30:4E:98>	192.168.0.181	256k	512k		
128 D	<hotspot-T-DC:9B:9C:6A:8B:0B>	192.168.2.17	256k	512k		
7 D	<hotspot-T-D8:63:75:06:2C:AB>	192.168.1.37	256k	512k		
188 D	<hotspot-T-D0:53:49:05:ED:49>	192.168.1.240	256k	512k		
39 D	<hotspot-T-D0:53:49:00:09:95>	192.168.1.14	256k	512k		
94 D	<hotspot-T-D0:17:C2:47:AC:32>	192.168.0.225	256k	512k		

255 items (1 selected) 0 B queued 0 packets queued

Gambar 10. Simple Queue pada router melihat jumlah dan kecepatan akses pengguna

Pada sisi pengelola jaringan dengan adanya sistem ini maka pengelola dapat mengetahui user-user siapa saja yang masih atau tidak ada lagi kuota *data*. Pengelola jaringan juga dengan mudah dapat membuat *service* baru untuk membuat sebuah kebijakan pemakaian dengan *volume/time based* dan mengatur kecepatan akses jaringan melalui *Web Administration Control Panel* dari Radius Manager. Pada *router* mikrotik, pengelola dapat melihat jumlah perangkat yang terhubung ke dalam jaringan *hotspot* dengan masing – masing pengguna *reguler* dan *free*, seperti pada gambar 10.

4. KESIMPULAN

Dengan adanya otentikasi penggunaa *hotspot* maka keamanan bagi para pengguna lebih terjamin karena membutuhkan *user* dan *password*. Serta pengguna *hotspot* dapat menikmati akses internet cepat melalui akses reguler yang dapat di manfaatkan ketika sangat diperlukan dengan maksimal kuota *data* sebesar 5 Gb, serta akses *free* yang dapat digunakan untuk keperluan-keperluan yang bersifat penggunaan biasa dan memiliki akses *volume data* tidak terbatas dan di batasi kecepatan 512 Kbps. Untuk pengelola jaringan, dengan adanya Radius Manager dapat memudahkan dan mengkonfigurasi *user* dan *service* pada *hotspot*, unifi *wireless controller* untuk mengelola *access point* dengan kontrol terpusat, router mikrotik sebagai penyedia *captive portal* dan sekaligus sebagai *traffic control* jaringan dan integrasi sistem *hotspot* dengan *worksheet* dapat membuat sistem ini berjalan secara otomatis ketika ada pengguna baru yang dijalankan oleh bagian administrasi STMIK PalComTech tanpa perlu adanya intervensi dari pengelola jaringan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada STMIK PalComTech yang telah memberikan kesempatan dalam melakukan penelitian ini.

DAFTAR PUSTAKA

- [1] S. Oei. 2014. Rancang Bangun Jaringan Hotspot pada Kampus Universitas Nusantara Manado menggunakan Router Mikrotik. Seminar Nasional Informatika 2014.
 - [2] E. Purwanto. 2015. Implementasi Jaringan Hotspot Dengan Menggunakan Router Miktorik Sebagai Penunjang Pembelajaran. Jurnal Informa. Vol. 1 : 2
 - [3] D. Aristiara, C. Budihartanti. 2014. Otentikasi Pengguna Jaringan Menggunakan Radius Windows 2008 *Server* pada PT. Pertamina. Jurnal Techno Nusa Mandiri Vol. XI : 2
 - [4] R. Powers, J. Lukas. 2011. Manajemen Jaringan *Wireless* Menggunakan *Server* Radius. Jurnal Teknik Informartika. Vol. 19 : 1.
 - [5] A. Gusala, S. Raharjo, N. Widyastuti. 2016. Implementasi Freeradius Pada Jaringan *Hotspot* Dengan Menggunakan MYSQL dan EAP-TLS. Jurnal Jarkom vol. 3 : 2.
 - [6] DMA Softlab LLC. 2018. *DMA Radius Manager Billing System User Manual*. http://www.dmasoftlab.com/documents/user_manual_4.2.pdf, diakses pada tanggal 18 September 2018.
 - [7] A. Supriyono, I. Riadi. 2013. Rancang Bangun Sistem *Hotspot* Menggunakan *Captive Portal*. Jurnal Sarjana Teknik Informatika. Vol. 1 : 1
-

