

**MANAJEMEN USER AKSES INTERNET  
PADA JARINGAN WIRELESS  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**



**Disusun sebagai salah satu syarat menyelesaikan Program Studi  
Strata I pada Program Studi Informatika Fakultas Komunikasi dan  
Informatika**

Oleh

**NURRUDIN**

**L200150137**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**2019**



**HALAMAN PERSETUJUAN**

**MANAJEMEN USER AKSES INTERNET  
PADA JARINGAN WIRELESS  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**PUBLIKASI ILMIAH**

Oleh

**NURRUDIN**

**L200150137**

Telah diperiksa dan disetujui untuk diuji oleh:

Dosen Pembimbing

A handwritten signature in blue ink, consisting of a large, stylized loop followed by a horizontal line and a small flourish at the end.

**Ir. Bana Handaga MT., Ph.D**  
**NIK. 793**

HALAMAN PENGESAHAN

MANAJEMEN USER AKSES INTERNET  
PADA JARINGAN WIRELESS  
UNIVERSITAS MUHAMMADIYAH SURAKARTA

OLEH  
NURRUDIN  
L200150137


Telah dipertahankan di depan Dewan Penguji  
Fakultas komunikasi dan informatika  
Universitas Muhammadiyah Surakarta  
Pada hari Kamis, 15 Agustus 2019  
dan dinyatakan telah memenuhi syarat

Dewan Penguji:

1. Bana Handaga. MT., Ph.D  
(Ketua Dewan Penguji)
2. Fatah Yasin Al Irsyadi, S.T., M.T.  
(Anggota I Dewan Penguji)
3. Aris Rakhmadi, S.T., M.Eng.  
(Anggota II Dewan Penguji)

(.....)  
(.....)  
(.....)

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan  
Untuk memperoleh gelar sarjana  
Tanggal 20 Agustus 2019  
Mengetahui,

Dekan  
Fakultas Komunikasi dan Informatika  
  
Nurgiyatna, S.T., M.Sc., Ph.D.  
NIK. 881

Ketua  
Program Studi Informatika  
  
Heru Supriyono, S.T., M.Sc., Ph.D.  
NIK. 970

## PERNYATAAN

Dengan ini saya menyatakan bahwa dalam naskah publikasi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Apabila kelak terbukti ada ketidakbenaran dalam pernyataan saya di atas, maka akan saya pertanggungjawabkan sepenuhnya.

**Surakarta 15 Agustus 2019**

Penulis



**NURRUDIN**  
**L200150137**



UNIVERSITAS MUHAMMADIYAH SURAKARTA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
PROGRAM STUDI INFORMATIKA

Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448  
Surakarta 57102 Indonesia. Web: <http://informatika.ums.ac.id>. Email: [informatika@ums.ac.id](mailto:informatika@ums.ac.id)

The screenshot shows a document viewer interface. The main content is an abstract article titled "MANAJEMEN USER AKSES INTERNET PADA JARINGAN WIRELESS" from Universitas Muhammadiyah Surakarta. The abstract discusses the development of information technology and the need for internet access management in wireless networks. It mentions a system designed to control internet access through wireless access points using captive portals and SSO (Single Sign-On) authentication.

**Abstrak**

Perkembangan teknologi informasi saat ini tidak bisa terelakan lagi terman teknologi – teknologi baru yang sejatinya membantu pekerjaan atau memudahkan manusia melakukan aktivitas kesehariannya sehingga waktu dan tenaga bisa dialihkan pada pekerjaan lain. Jaringan komputer merupakan sekumpulan komputer yang saling terhubung antara satu dengan yang lainnya. Salah satu layanan UMS menyediakan fasilitas koneksi internet melalui jaringan wireless, dengan nama SSID “UMS WIFI”. Namun demikian akses melalui UMS wifi terjadi kendala, terutama pada saat user yang tersambung pada sebuah *Access Point* melebihi kapasitas perangkat pada saat jam sibuk ( 09.00 – 12.00 WIB ). Pada penelitian ini dirancang satu sistem untuk mengontrol sambungan ke wireless *Access Point* dan memantau aktifitas pengguna akses internet melalui UMS wifi dengan menggunakan *Captive Portal* memakai SSO (*Single Single On*) yang sudah dipakai di UMS dengan dibantu menggunakan Mikrotik sebagai jembatan untuk Autentifikasi. setiap user yang tersambung ke *Wireless Access Point* dapat dijamin mendapatkan fasilitas akses internet dengan *bandwith* yang cukup.

**Kata Kunci :** Ums wifi, SSO, Mikrotik .

Page: 1 of 11 | Word Count: 1861 | Text-only Report | High Resolution On



UNIVERSITAS MUHAMMADIYAH SURAKARTA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
PROGRAM STUDI INFORMATIKA

Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448  
Surakarta 57102 Indonesia. Web: <http://informatika.ums.ac.id>. Email: [informatika@ums.ac.id](mailto:informatika@ums.ac.id)

**SURAT KETERANGAN LULUS PLAGIASI**  
**136/A.4-II.3/INF-FKI/VIII/2019**

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika

menerangkan bahwa :

Nama : NURRUDIN  
NIM : L200150137  
Judul : **MANAJEMEN USER AKSES INTERNET  
PADA JARINGAN WIRELESS  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

Program Studi : Informatika

Status : **Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi,  
dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 15 Agustus 2019

Biro Skripsi Informatika

**Hsan Cahyo Utomo, S.Kom., M.Kom.**





**MANAJEMEN USER AKSES INTERNET  
PADA JARINGAN WIRELESS  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**Abstrak**

Perkembangan teknologi informasi saat ini tidak bisa terelakan lagi temuan teknologi – teknologi baru yang sejatinya membantu pekerjaan atau memudahkan manusia melakukan aktivitas kesehariannya sehingga waktu dan tenaga bisa dialihkan pada pekerjaan lain. Jaringan komputer merupakan sekumpulan komputer yang saling terhubung antara satu dengan yang lainnya.

Salah satu layanan UMS menyediakan fasilitas koneksi internet melalui jaringan *wireless*, dengan nama SSID “UMS WIFI”. Namun demikian akses melalui UMS wifi terjadi kendala, terutama pada saat user yang tersambung pada sebuah *Access Point* melebihi kapasitas perangkat pada saat jam sibuk ( 09.00 – 12.00 WIB ).

Pada penelitian ini dirancang satu sistem untuk mengontrol sambungan ke *wireless Access Point* dan memantau aktifitas pengguna akses internet melalui UMS wifi dengan menggunakan *Captive Portal* memakai SSO (*Single Single On*) yang sudah dipakai di UMS dengan dibantu menggunakan Mikrotik sebagai jembatan untuk Autentifikasi.

setiap user yang tersambung ke *Wireless Access Point* dapat dijamin mendapatkan fasilitas akses internet dengan *bandwith* yang cukup.

**Kata Kunci :** Ums wifi, SSO, Mikrotik .

**Abstract**

*The development of information technology today can no longer be avoided by the discovery of new technologies that really help work or make it easier for humans to do their daily activities so that time and energy can be diverted to other jobs. A computer network is a collection of computers that are connected to each other.*

*One UMS service provides an internet connection facility via a wireless network, with the SSID name "UMS WIFI". However, access via UMS wifi is a problem, especially when users who are connected to Access Points exceed the capacity of the device during peak hours (09.00 - 12.00 WIB).*

*In this study a system is designed to control the connection to the wireless Access Point and monitor the activities of users accessing the internet via wifi UMS using Captive Portal using SSO (Single Single On) which has been used at UMS with the help of using Mikrotik as a bridge for Authentication.*

*every user who is connected to the Wireless Access Point can be guaranteed to get internet access facilities with sufficient bandwidth.*

**Keywords:** Ums wifi, SSO, Mikrotik.

## 1. PENDAHULUAN

Jaringan komputer adalah sekelompok komputer yang saling berhubungan satu sama lain dengan memanfaatkan media komunikasi dan suatu protokol komunikasi, sehingga antar komputer dapat saling berbagi dan bertukar informasi.

Masalah umum yang biasanya terjadi dalam sebuah jaringan komputer adalah menumpuknya jumlah pengguna yang menggunakan jalur yang sama. Apabila tidak ada pengaturan, ibarat sebuah jalan, maka akan terjadi kemacetan sehingga semua pengguna tidak bisa mengakses tujuan sama sekali. (Bana Handaga dkk)

Layanan ums.wifi pada saat ini masih memakai *generic password*, akibatnya pada jam sibuk seringkali user kesulitan untuk mendapatkan koneksi *wireless*. Pada tugas akhir ini saya membuat *Hotspot mikrotik* untuk mengetahui *user acces* yang masuk menggunakan SSid Wifi-UMS dengan menggunakan *SSO (Single Sign On)* sehingga bisa terkontrol dan aman dalam mempertahankan jaringan yang mempunyai sifat terbuka di infrastruktur jaringan Wifi.

*Router MikroTik* adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan *wireless*. Selain itu MikroTik dapat juga berfungsi sebagai firewall bagi komputer lain dan memberikan prioritas bagi komputer lain agar bisa mengakses data Internet maupun data lokal. MikroTik bertujuan untuk mengatur bandwidth serta melakukan manajemen jaringan komputer. Penempatan router MikroTik ditempatkan pada sebuah komputer yang dijadikan sebagai *gateway* suatu jaringan. Komputer *gateway* tersebut berfungsi untuk mendistribusikan data keluar masuknya dari dan ke komputer lainnya sehingga seluruh komputer dapat mengakses data bersama-sama seperti Internet sharing (Mancill, 2002).

*Router Mikrotik* memiliki banyak fitur, salah satu fitur yang cukup populer dan banyak digunakan adalah *Hotspot* dengan *Hotspot*, kebanyakan *wifi Hotspot* tidak di *password* dan semua user bisa *connect* dan dialihkan ke halaman login di Web Browser. Tiap user bisa login dengan *username* dan *password* yang berbeda-beda. Metode semacam inilah yang sering kita temukan di kampus, sekolah, kantor, maupun area publik lainnya. ( [http://mikrotik.co.id/artikel\\_lihat.php?id=125](http://mikrotik.co.id/artikel_lihat.php?id=125) ) .

Kelebihan *Hotspot* kita adalah dapat mengkonfigurasi jaringan yang hanya bisa digunakan dengan username dan password tertentu. dapat melakukan manajemen terhadap user-user tersebut. Misalnya mengatur durasi total penggunaan *Hotspot* per user, membatasi berapa besar data yang dapat di download tiap user, mengatur konten apa saja yang boleh diakses user, dll.

Jadi ide dasar Captive Portal sebetulnya cukup sederhana. Daripada kita tergantung pada mekanisme keamanan built-in di peralatan *WiFi 802.11b* untuk mengontrol siapa saja yang dapat berasosiasi ke *Access Point*, menggunakan *Captive Portal* kita mengkonfigurasi agar *Access Point* bekerja dan merupakan network yang terbuka.

Sistematikanya adalah saat seorang pengguna berusaha untuk melakukan browsing ke Internet, Captive Portal akan memaksa pengguna yang belum terautentikasi untuk menuju ke *Authentication web* dan akan di beri *prompt* login termasuk informasi tentang *Hotspot* yang sedang dia gunakan

Teknologi wireless memberikan kemudahan dan *fleksibilitas* yang cukup tinggi dan nyaman digunakan. Selama berada dalam *Hotspot Wireless*, user dapat mengakses internet dimana pun. Untuk membuat sebuah jaringan terkoneksi ke internet yang aman dan user friendly, kita bisa membuat sebuah sistem menggunakan *User Account* untuk melakukan otorisasi dan autentikasi dalam sebuah jaringan, membatasi pemakaian tiap user yang ada di dalam sebuah jaringan dengan menggunakan Mikrotik.

## **2. METODE PENELITIAN**

Penelitian ini diawali dengan pengamatan traffic penggunaan jalur internet di UMS dengan memakai akses wifi sangat tinggi dan membutuhkan *bandwith* besar. Penulis melakukan wawancara terhadap salah satu pengguna selaku mahasiswa dan tendik dilingkungan kampus. Data yang diperoleh dari wawancara tersebut meliputi:

- a. Menggunakan akses wifi di UMS sulit untuk masuk.
- b. *Bandwidth* yang digunakan kurang maksimal.
- c. Mahasiswa perlu mencari bahan untuk kuliah dan referensi mata kuliah.
- d. Kurang stabil bila sudah dapat koneksi.

- e. Harapan dengan adanya penelitian yang dilakukan penulis tentang manajemen user akses wifi ums lancar digunakan dan bermanfaat bagi semua, merata dan koneksi lancar.

### 2.1. Analisa Kebutuhan Sistem Manajemen User

Untuk tahap ini menganalisa kebutuhan untuk membangun *Hotspot Wireless* diperlukan *hardware* maupun *software* sebagai alat pendukung dalam merancang sistem manajemen yang ditampilkan pada tabel 1.

**Table 1**, daftar perangkat yang diperlukan

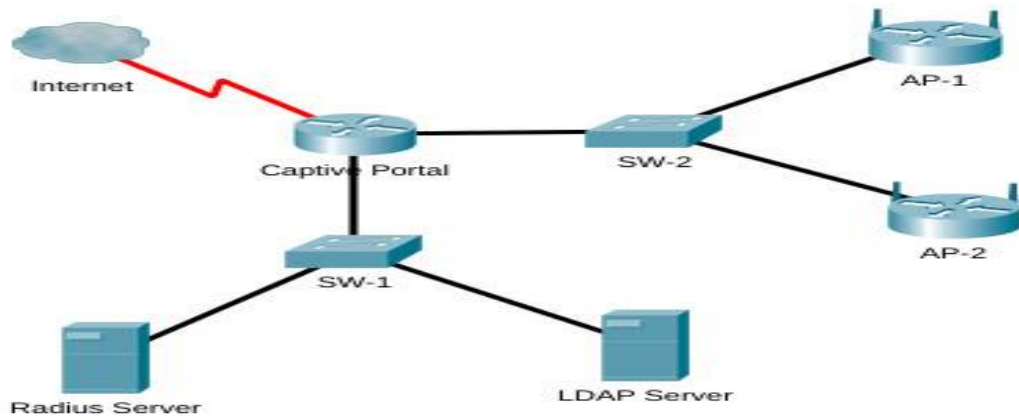
Perangkat keras	Perangkat lunak
Virtual server Processor RAM 2GB Lan 1 Gbps hardisk 64GB	Debian 9
Mikrotik RB 951-2n	Winbox.exe
Kabel UTP	Free Radius LDAP 3.0.12
	LDAP 389 DS V.1.3.4.4

### 2.2 Pengumpulan Data

Pengumpulan data dilakukan dengan cara melakukan survei dan wawancara serta mengumpulkan artikel – artikel jurnal ilmiah sebagai referensi untuk penelitian ini. Metode ini dilakukan dengan cara wawancara terhadap para pengguna terdiri atas mahasiswa dan tendik dilingkungan kampus, untuk mengetahui populasi/rasio jumlah *client* terhadap perangkat *Access Point* ( AP ) .

### 2.3 Topologi Jaringan *Hotspot*

Topologi jaringan yang ada di UMS dengan menggunakan jalur *Hotspot* adalah jalur internet yang berasal dari jalur utama (*backbone*) jaringan dimasukkan *router Hotspot* mikrotik RB 951-2N 8 port, dari *backbone* UMS masuk eth 1, *router* tersebut sebagai *autentifikasi* dengan radius di eth 2, kemudian didalam server radius terdapat free radius yang menghubungkan dengan database LDAP yang sudah ada di UMS. kemudian untuk *Switch* yang kedua masing – masing ke *Access Point*. Kedua *Switch* tersebut adalah *Switch Manageble* ( layer 3 ) yang mempunyai fungsi berbeda. Lihat gambar 1



**Gambar 1.** Topologi Jaringan *Hotspot* UMS

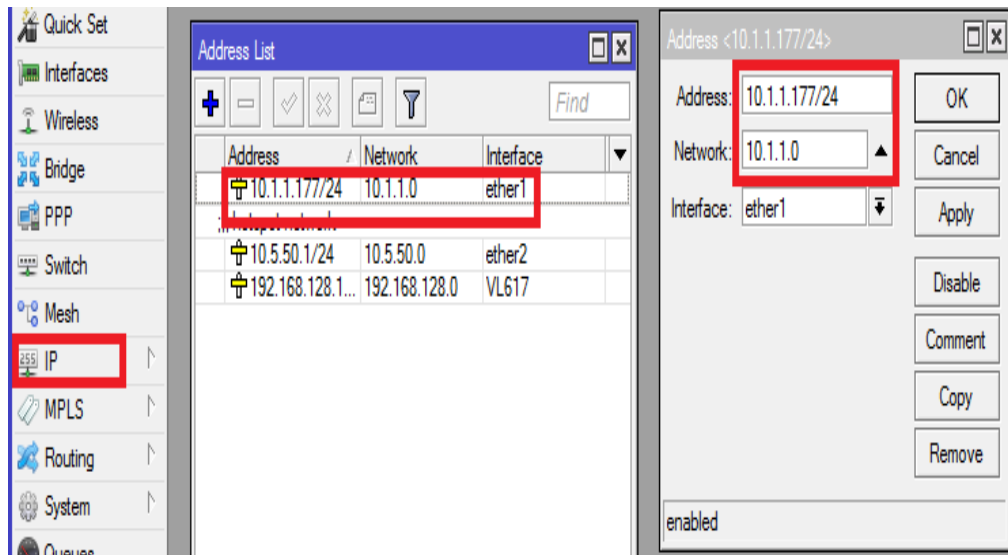
**Tabel 2,** daftar koneksi jaringan *Hotspot*

PERANGKAT	IP ADDRESS	VLAN	GATEWAY
Server Radius	172.16.10.0/24	VL 101	172.16.10.6
LDAP Server	172.16.10.0/24	VL 101	172.16.10.6
RB951 eth 1	10.1.1.0/24	VL 110	
RB 951 eth 2	192.168.128.0/24	VL 617	192.168.128.1

## 2.4 Konfigurasi Manajemen User Akses

### 2.4.1 Konfigurasi Mikrotik

Yang dilakukan pada konfigurasi ini adalah menentukan *interface* local agar dapat terhubung dengan server. Konfigurasi pada Mikrotik melalui *ip > address* kemudian masukkan *ip address*, *ip network* dan *interface*. Setelah konfigurasi *interface* selesai maka diperoleh dua *ip address* yaitu 10.1.1.177 *client Hotspot* di meni IP dalam *ip network* 10.1.1.0/24 sebagai Ip jaringan yang terpasang, Konfigurasi *interface* dan *address list* terdapat pada gambar 2



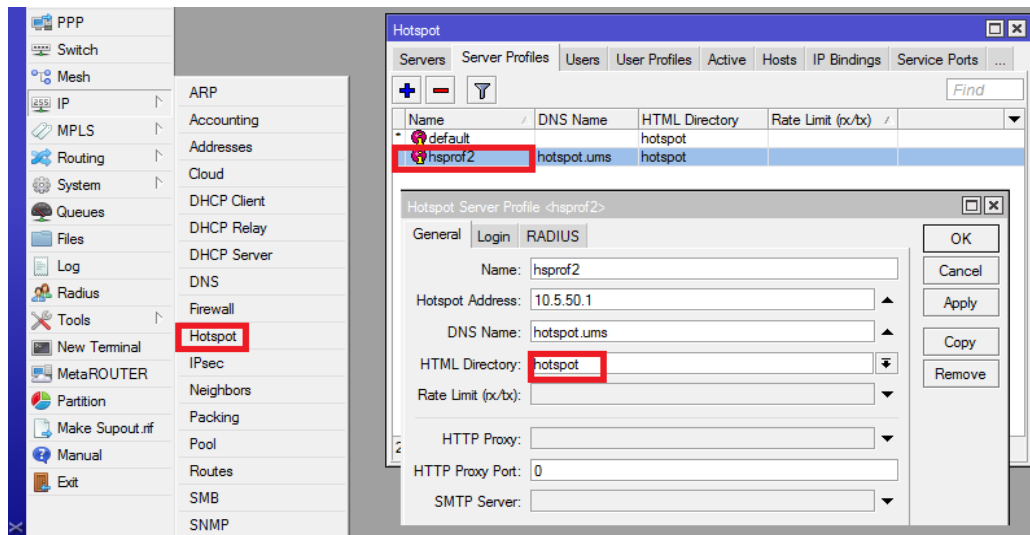
**Gambar 2.** Tampilan *interface* lokal dan *address list*

#### 2.4.2. Hotspot di mikrotik

*Hotspot* adalah sekumpulan dari *Access Point* atau Wireless LAN dengan standar 802.11a/b/g yang melayani sebuah wilayah terbatas dimana pengguna dapat dengan bebas dan mobile untuk bergabung ke dalam *Access Point* menggunakan perangkat yang mendukung, jaringan RT/RW Net tidak termasuk *Hotspot*.( purbo, 2006 )

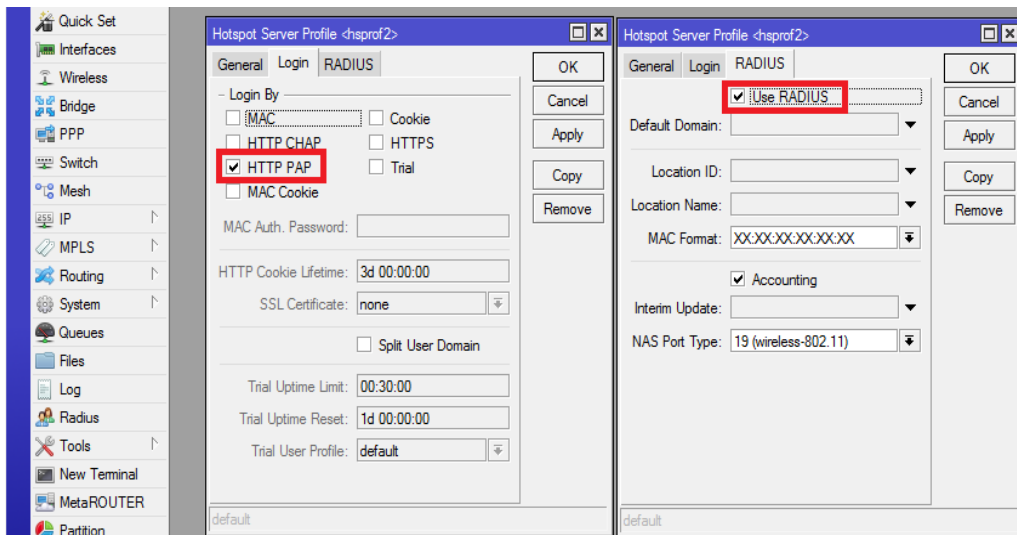
*RADIUS (Remote Authentication Dial-In User Service)* adalah sebuah protokol keamanan komputer digunakan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan.( ardian, 2012 )

Yang dilakukan pertama pada settingan ini adalah masuk di winbox kemudian masukan *user* dan *password* yang sudah di setting, Konfigurasi pada Mikrotik melalui ip *Hotspot* kemudian masukkan server profiles dan general Setelah konfigurasi *HTML Directory* selesai.lihat gambar 3.



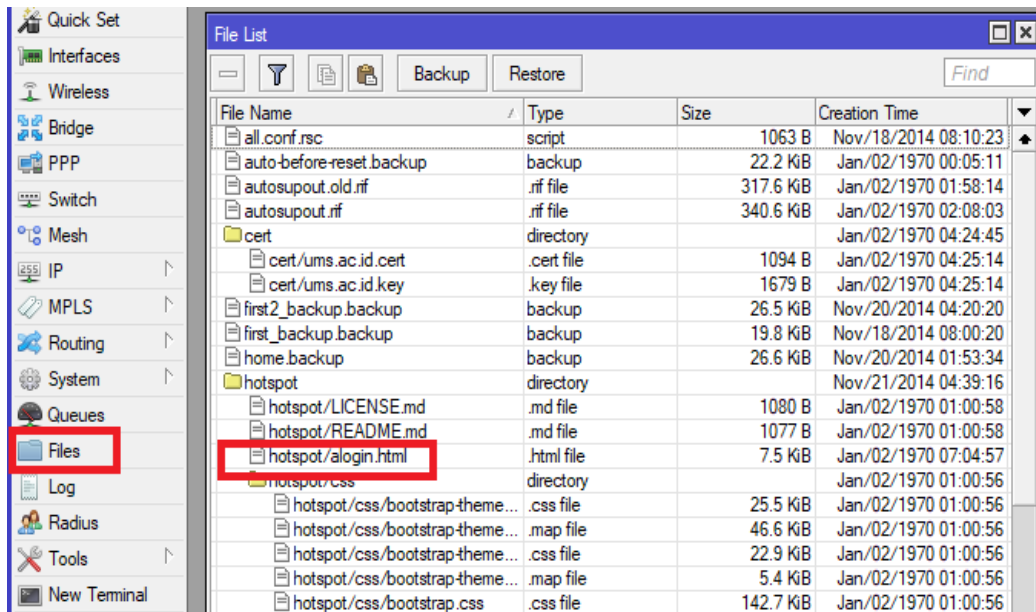
**Gambar 3. Hotspot HTML**

Kemudian masuk di login pilih HTTP PAP kemudian masuk ke Radius klik Use RADIUS gambar 4.

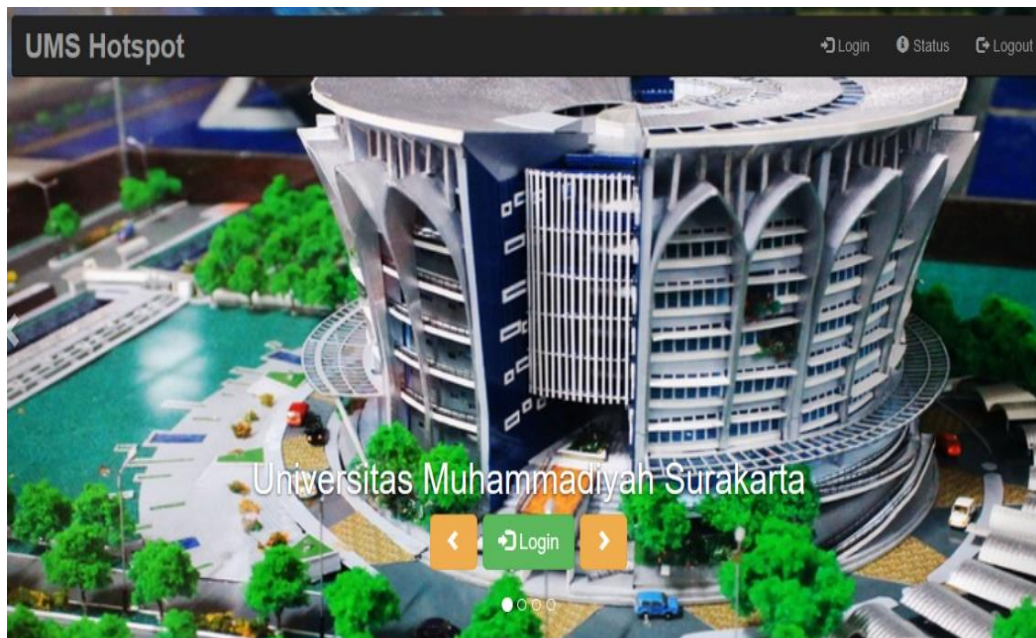


**Gambar 4. Login dan Radius**

Setelah itu untuk menampilkan halaman login diperlukan beberapa file antara lain seperti ditampilkan pada gambar 5, file . “*alogin.html.*” file utama yang mengandung form login ) *user name* dan *password* ) beberapa file yang lain adalah file ( *css* ) untuk mengatur tampilan menggunakan *frame boot strap*.

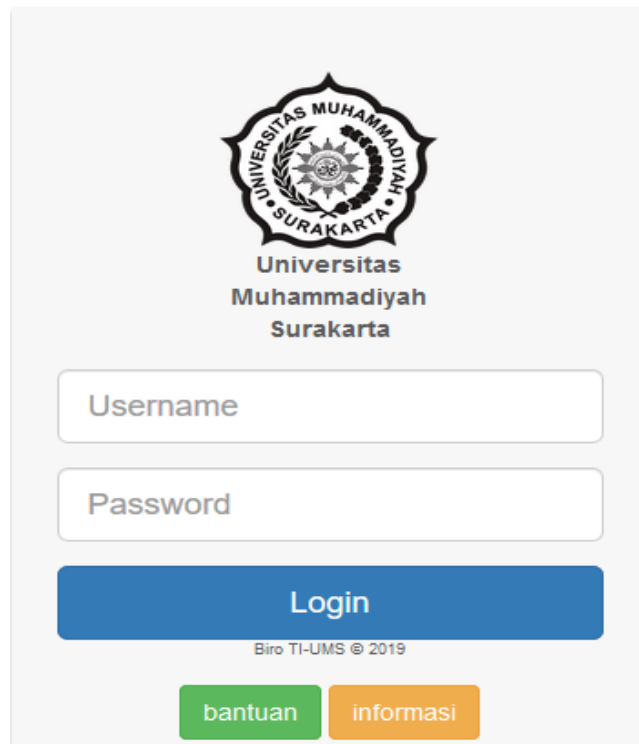


*Gambar 5. Files tampilan login Html.*



*Gambar 6. Halaman depan Html.*





**Gambar 7.** Login dengan Radius

### **2.4.3. Mekanisme *Authentikasi User***

Cara kerja *server* autentikasi ini sebagai berikut, pertama setiap *user* yang masuk kedalam *wireless Hotspot* dan mencoba untuk browsing internet, semuanya akan di-*redirect* ke halaman *login username* dan *password* yang dibuat oleh halaman *Html*. Ketika *username* dan *password* telah dimasukkan, akan menanyakan ke *FreeRADIUS* apakah ada *username* dan *password* yang dimasukkan oleh *user*. *FreeRADIUS* akan mencocokkan *username* dan *password* yang dimasukkan melalui *database* yang dibuat di *LDAP Server*. Jika ada, *FreeRADIUS* akan mengecek batas pemakaian *user* tersebut. Jika *user* tersebut valid, *FreeRADIUS* akan memberikan izin sehingga *user* bisa *surfing* di internet. Jika tidak, *FreeRADIUS* *username* dan *password* yang dimasukkan tidak mendapatkan hak akses ke jaringan. Halaman *HTML* tidak akan membuka akses untuk *surfing* internet, dan akan meminta *login* ulang dan begitu seterusnya. Atau dengan menggunakan bantuan yang sudah tercantum dihalaman depan kolom ( bantuan atau informasi ).

### 3. PENGUJIAN

#### 3.1. Pengujian *Hotspot* Ums

Untuk mengetahui performan UMS *Hotspot* dilakukan implementasi *Hotspot* menggunakan mikrotik RB 951 – 2N di lingkungan gedung induk Siti Walidah lantai 5 sayap utara dengan topologi jaringan seperti tunjukkan pada gambar 1. Sebagai *client* adalah mahasiswa dan staff tendik yang ada dilingkungan tersebut. Contoh Selvia mahasiswa fakultas Komunikasi dan Informatika serta Ginus pandu Tendik Biro TI

USER	MAC. ADDRESS	AUTHENTIFIKASI	STATUS WAKTU KONEKSI
L20016.152	7C:67:A2:49:54:D4	SSO	terhubung
Gps490	0C:98:38:74:BF:F9	SSO	terhubung

### 4. PENUTUP

#### 4.1. Evaluasi Keseluruhan Sistem

Dari hasil pengujian sistem autentikasi pengguna *wireless* berbasis radius *server* untuk konektivitas cukup efisien dan praktis. Untuk terkoneksi ke *Hotspot* seorang *user* membutuhkan waktu kurang dari sepuluh detik. Sistem autentikasi ini juga memungkinkan adanya monitoring dan manajemen *bandwidth* baik *upload* maupun *download*. Sistem autentikasi ini juga relatif aman bagi data pengguna, Sistem autentikasi ini juga memudahkan bagi pengguna untuk terkoneksi ke *Hotspot* tanpa adanya prosedur yang berbelit-belit (seperti meminta *password* WEP/WPA KEY).

## DAFTAR PUSTAKA

- Citra web solusi teknologi. PT. (2019). *Setting dasar Hotspot mikrotik* diakses dari [http://mikrotik.co.id/artikel\\_lihat.php?id=125](http://mikrotik.co.id/artikel_lihat.php?id=125).
- Purbo,O.W.(2006). *Buku Pegangan Internet Wireless dan Hotspot* Jakarta: CHIP.
- Ardian Yusriel , (2012) *Implementasi Sistem Otentikasi pada Pengguna Jaringan Hotspot Jurnal informatika Universitas Kanjuruhan Malang* VOL. 11, NO. 1, MEI 2012: 34-41
- Sujalwo, Bana Handaga, dan Heru Supriyono, *KomuniTi, Vol. II, No.2 , Januari 2011 Manajemen Jaringan Komputer Dengan Menggunakan Mikrotik Router (Computer Network Management Used With Microtic Router)*
- Mancill, T. (2002), *Linux Routers : A Primer for Network Administrator, 2<sup>nd</sup> ed.*, Prentice Hall.