Authentication Wireless Area Network Menggunakan *Captive Portal* Berbasis Mikrotik pada Madrasah Ibtidaiyah Misbahul Athfal Bogor

Toni Sukendar [1)], M. Ikhsan Saputro[2)*)], Ahmad Ishaq [3)], Achmad Sumbaryadi [4)]

[1)] Teknologi Komputer, Universitas Bina Sarana Informatika
[2)] Teknik Informatika, Universitas Mohammad Husni Thamrin
[3)] Sistem Informasi, Universitas Bina Sarana Informatika
[4)] Teknologi Informasi, Universitas Bina Sarana Informatika
Correspondence author: m.ikhsan68@gmail.com, Jakarta, Indonesia
DOI: https://doi.org/10.37012/jtik.v9i1.1465

Abstrak

Madrasah Ibtidaiyah Misbahul Athfal merupakan sekolah dengan jenjang dasar pada pendidikan formal di Indonesia yang setara dengan sekolah dasar. Madrasah Misbahul Athfal ini memiki jaringan *wireless* (WLAN) yang digunakan sebagai media pertukaran data serta informasi dengan memanfaatkan media transmisi *wireless*. Sistem keamanan yang di terapkan di madrasah tersebut adalah WPA2-PSK (*Wi-Fi Protected Access 2 Pre Shared Key*). Sistem keamanan WPA2-PSK untuk saat ini dirasa memiliki kelemahan dikarenaan hanya menggunakan satu password untuk seluruh user yang akan terhubung ke internet dan ini merupakan satu kelemahan pada system keamanan WPA2-PSK. Hal tersebut memberikan peluang bagi user yang tidak bertanggung jawab untuk masuk kedalam jaringan WLAN Madrasah Ibtidaiyah Misbahul Athfal. Oleh karena itu pada penelitian kali ini mencoba menerapkan sistem keamanan *Authentication Captive Portal* sebagai salah satu upaya dalam meningkatkan keamanan WLAN Madrasah Misbahul Athfal. Metode *Authentication* ini menggunakan router mikrotik dan aplikasi winbox sebagai untuk konfigurasi dan *monitoring*. Pada metode ini semua user memungkinkan untuk mempunyai *password* dan *Account* yang berbeda.

Kata Kunci: *Authentication, Captive Portal, Wireless Local Area Network*

Abstract

Madrasah Ibtidaiyah Misbahul Athfal is a school with a basic level of formal education in Indonesia which is equivalent to elementary school. Madrasah Misbahul Athfal has a wireless network (WLAN) which is used as a medium for exchanging data and information by utilizing wireless transmission media. The security system implemented at the madrasah is WPA2-PSK (Wi-Fi Protected Access 2 Pre Shared Key). The WPA2-PSK security system is currently considered to have a weakness because it only uses one password for all users who will connect to the internet and this is a weakness in the WPA2-PSK security system. This provides an opportunity for irresponsible users to enter the Madrasah Ibtidaiyah Misbahul Athfal WLAN network. Therefore, this research tries to implement a Captive Portal Authentication security system as an effort to improve the security of Misbahul Athfal Madrasah WLAN. This Authentication method uses a proxy router and the Winbox application as configuration and monitoring. In this method it is possible for all users to have different passwords and accounts.

Keywords: *Authentication, Captive Portal, Wireless Local Area Network*

PENDAHULUAN

Madrasah Ibtidaiyah Misbahul Athfal sudah mempunyai jaringan *Lokal Area Network* dan juga *Wireless Area Network* yang biasa di sebut juga dengan WLAN. Seiring berkembang pesatnya Madrasah Ibtidaiyah Misbahul Athfal terbukti dengan bertambahnya

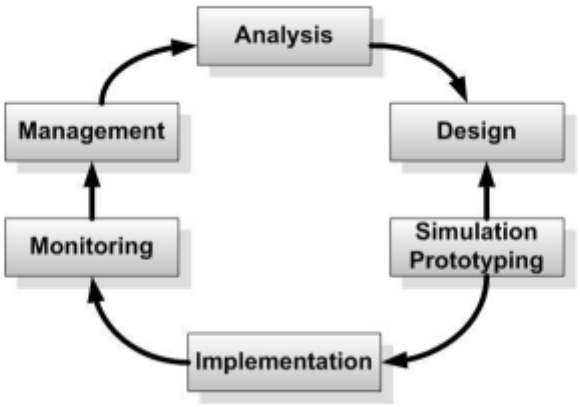
jumlah siswa dan guru, diperlukan Penambahan Akses Point di beberapa titik di Madrasah itu untuk menjangkau area yang sebelumnya tidak terjangkau oleh siswa dan guru.

Selama ini sistem keamanan *Wireless* pada Madrasah Misbahul Athfal adalah dengan menggunakan system WPA-2 PSK (*Wi-Fi Protected Access 2 Pre Shared Key*). Pada sistem keamanan ini user cukup memasukan *Password* untuk dapat memasuki jaringan *wireless*, berapapun jumlah user atau pengguna untuk dapat memasuki jaringan *wireless password*nya tetap sama. Jika seperti ini admin jaringan sangat sulit untuk memantau user yang berhak atau user yang hanya ingin internetan saja ataupun user yang berniat jahat terhadap jaringan. Mempertimbangkan permasalahan diatas maka penelitian ini ditujukan untuk meningkatkan keamanan *wireless* menggunakan *Authentikasi Captive Portal* yang berbasis mikrotik pada WLAN Madrasah Misbahul Athfal.

Authentikasi Captive Portal adalah jika user memilihnya SSID nya maka user tersebut akan dialihkan ke halaman web untuk melakukan *login hotspot*. Yang dapat login hanya user yang sudah terdaftar di *server hotspot* mikrotik dan masing-masing user mempunyai *username* dan *password* yang berbeda. Admin jaringan dapat dengan mudah mengontrol user-user yang sudah login. Inilah yang membedakan antara *Authentication Captive Portal* dengan WPA2-PSK.

METODE

NDLC (*Network Development Life Cycle*) adalah metode yang digunakan pada penelitian ini. Metode ini melakukan pendekatan pada proses komunikasi data yang berorientasi Jaringan (*Network*) yang memiliki suatu tahapan lingkaran yang tidak ada awal maupun akhir proses. Tahapan-tahapan pada NDLC (*Network Development Life Cycle*) adalah *Analysis*, *Design*, *Simulation prototyping*, *Implementation*, *Monitoring* dan yang terakhir adalah tahapan management.



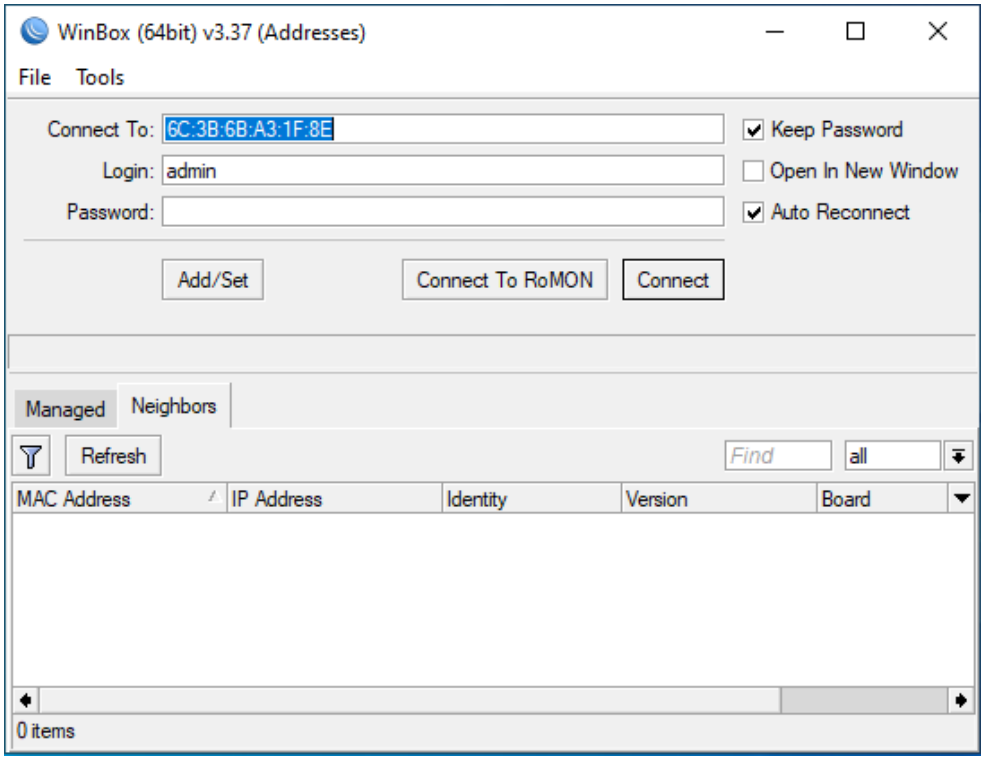
Gambar 1. *Metode Network Development Life Cycle* (NDLC)

Tahapan-tahapan pada *Network Development life cycle* (NDLC):

1. *Analysis* : yaitu melakukan observasi langsung ke lokasi dan melakukan wawancara kepada karyawan berkaitan dengan permasalahan keamanan *wireless* yang dialami oleh Madrasah Ibtidaiyah Misbahul Athfal.
2. *Design* : yaitu melakukan pembuatan topologi yang cocok untuk Madrasah Ibtidaiyah Misbahul Athfal. Dalam hal ini topologi WLAN.
3. *Simulation Prototyping* : melakukan simulasi dengan menggunakan router mikrotik serta software aplikasi winbox untuk membuat konfigurasi *Authentication Captive Portal*.
4. *Implementation* : tahap ini adalah tahap penerapan dan pengujian *Authentication Captive Portal.*
5. *Monitoring* : tahap ini adalah tahap memantau user yang terhubung ke WLAN menggunakan aplikasi Winbox.
6. *Management* : tahap ini merupakan tahap pemeliharaan dan pengaturan dari hasil penelitian.

HASIL DAN PEMBAHASAN

Berikut ini beberapa tools yang digunakan dalam merancang *Authentication Wireless Area Network* Menggunakan *Captive Portal* Berbasis Mikrotik:

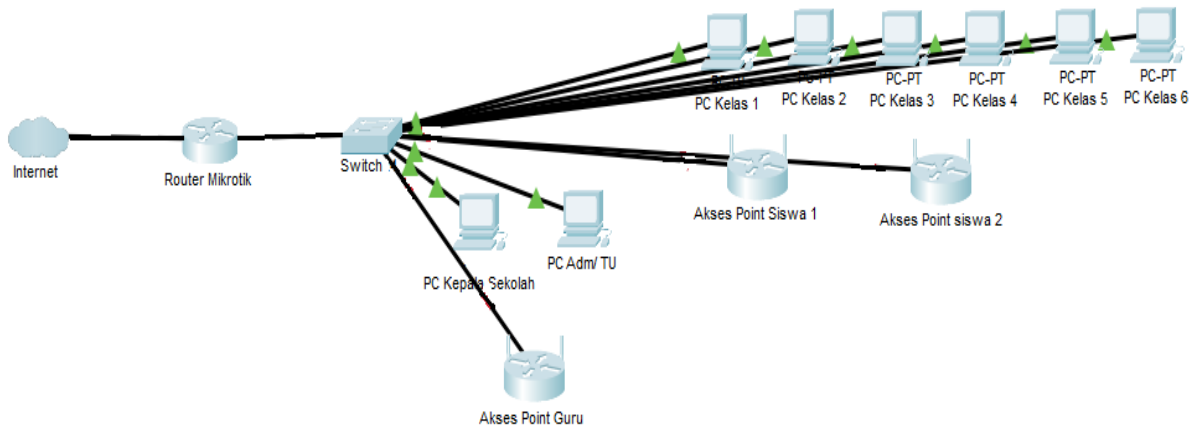


Gambar 2. Aplikasi Winbox

Gambar 3. Routerboard Mikrotik RB941

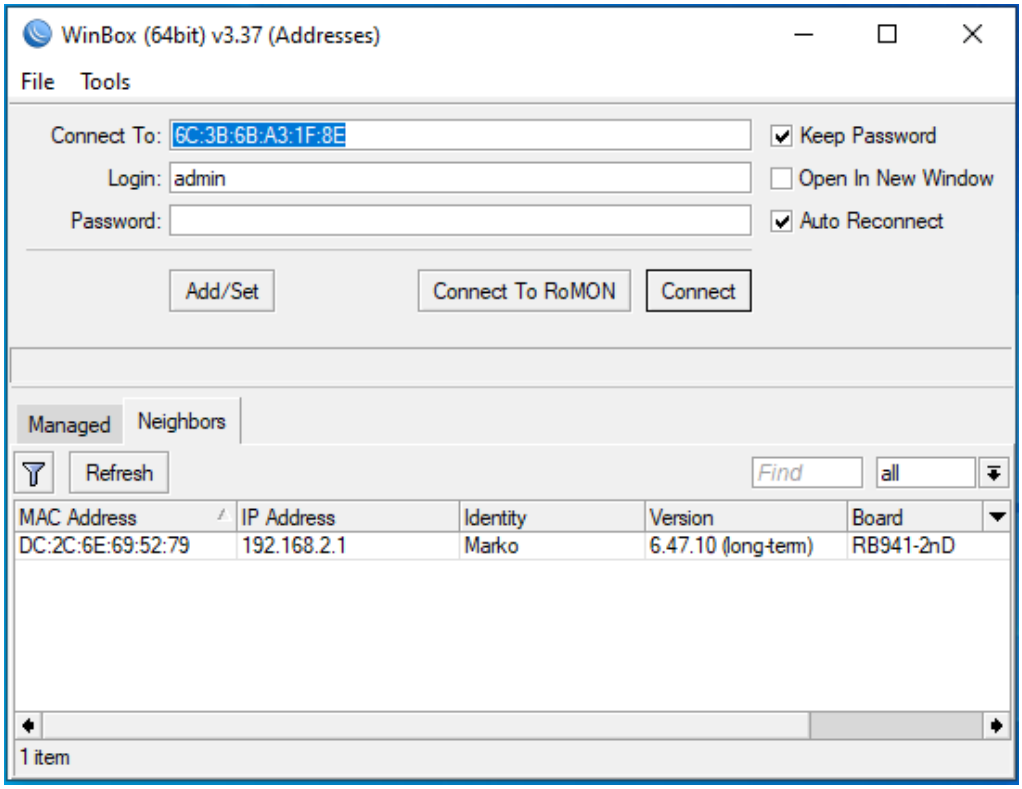
Gambar 4. *Access Point* Ubiquity

Pada Topologi di gambar 5 terdapat jaringan *Wireless* dengan dihubungkan melalui tiga Akses Point yang peruntukannya untuk staff karyawan, guru dan siswa. Juga terdapat jaringan wire atau melalui media kabel yang terhubung dengan 8 (PC) Personal Komputer. Semua itu baik wireless maupun kabel terhubung ke router mikrotik. Penempatan PC atau peletakan Akses Point itu semua sudah disesuaikan dengan ruangan. Penempatan Akses Point sudah sesuai atau dapat menjangkau pengguna wireless baik itu laptop ataupun smartphone.



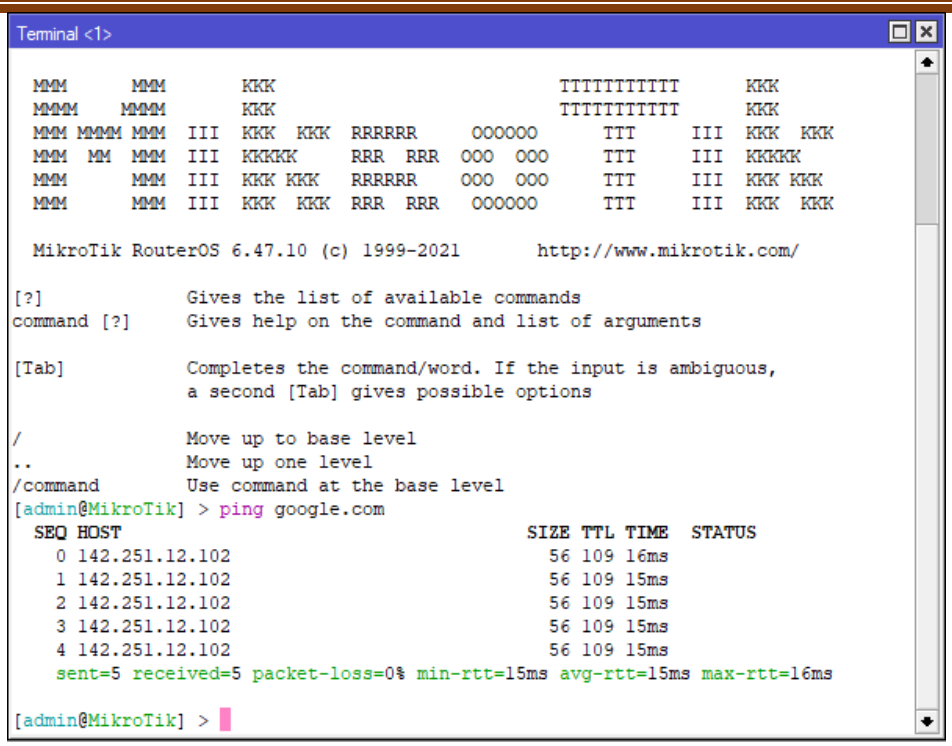
Gambar 5. Topologi Jaringan Madrasah Ibtidaiyah Misbahul Athfal

Konfigurasi Mikrotik pada Routerboard RB941 ini menggunakan aplikasi Winbox versi 3.37 yang 64 bit. Penggunaan 64 bit karena disesuaikan dengan sistem operasi yang gunakan yang windows 10 64 bit. Apabila system operasinya yang 32 bit maka winboxnya pun harus yang 32 bit. Untuk mendapatkan software winbox bisa langsung download pada laman https://mikrotik.com/download. Untuk dapat mengkonfigurasi mikrotik masukan kabel LAN pada port 2 selanjutnya ujung port yang satunya masukan ke port LAN yang ada pada Laptop atau PC, sehingga muncul serperti gambar dibawah ini.

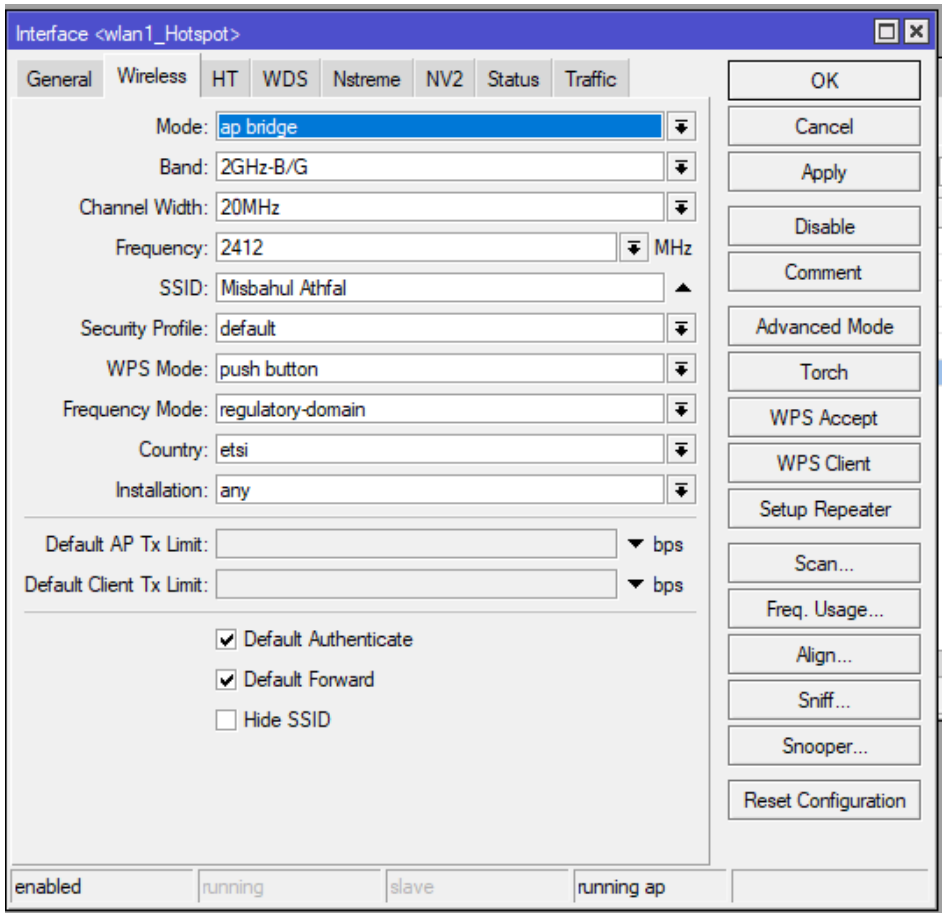


Gambar 6. Aplikasi winbox yang terhubung dengan router mikrotik

Pada gambar diatas menunjukan aplikasi winbox yang terhubung dengan routerboard mikrotik yaitu tandanya terdapat angka hexa pada Mac Address nya. Untuk koneksi hingga bisa terhubung ke internet yang dimulai dengan DHCP Client, pembuatan DNS, membuat NAT (*Network Address Translation*) dengan memilih *chain*nya scrnat dan *action*nya masquerade, untuk mengetahui apakah koneksi internetnya sudah bisa atau belum bisa mengujinya melalui *new terminal*. Seperti pada gambar dibawah ini.

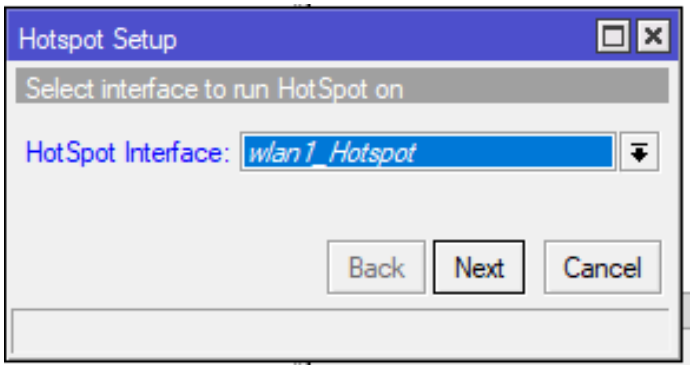


Gambar 7. Pengujian koneksi pada google.com

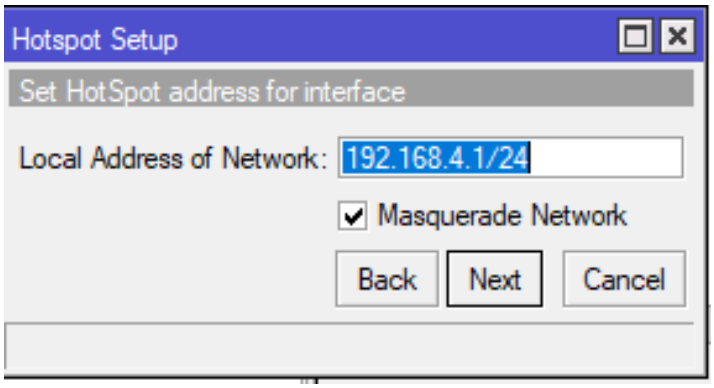


Gambar 8. Pembuatan SSID

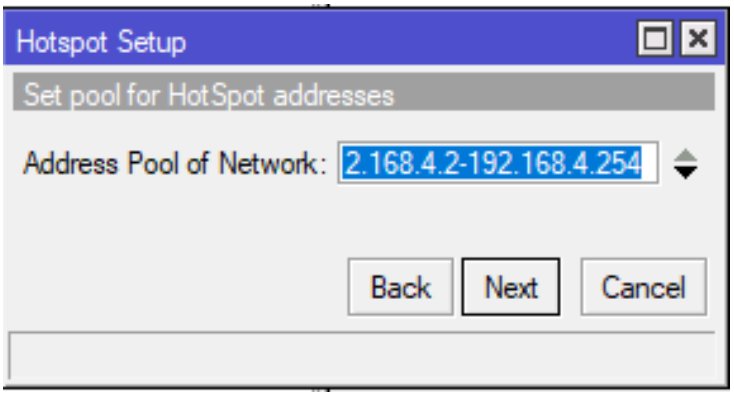
Untuk membuat Hotspot klik IP – Hotspot – Hotspot Setup



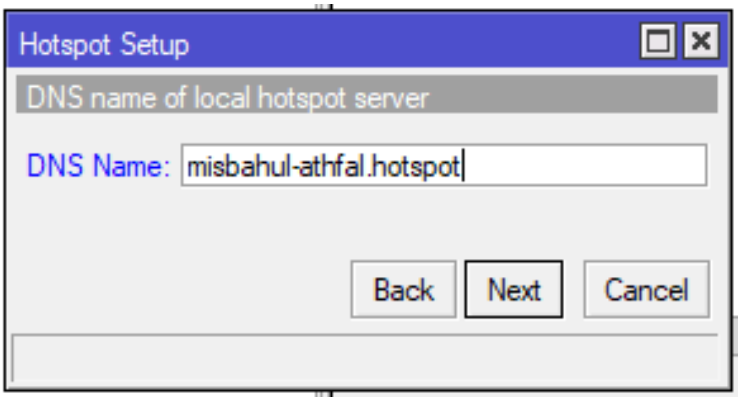
Gambar 9. Hotspot Setup



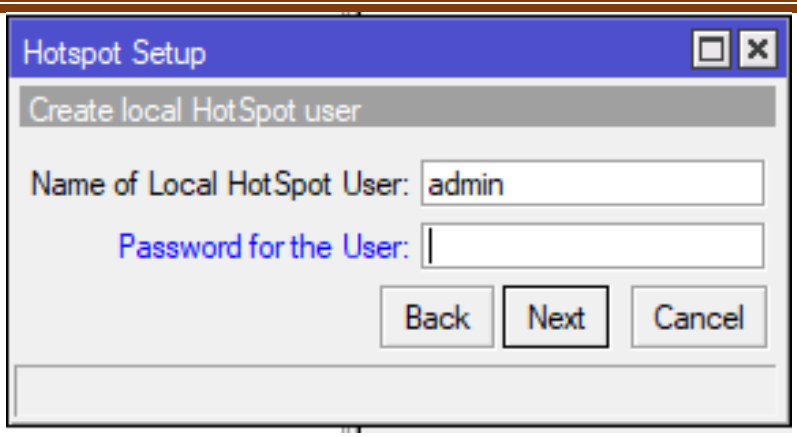
Gambar 10. Memasukan *Adress Network*



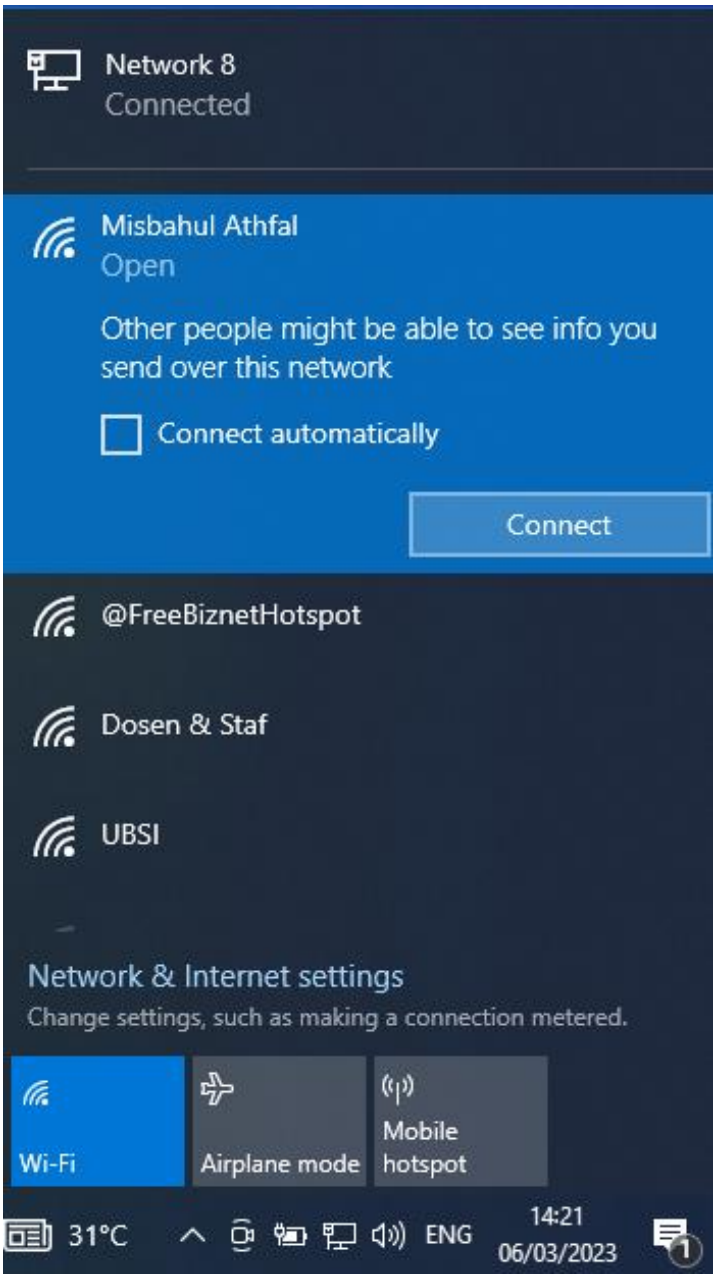
Gambar 11. Range DHCP



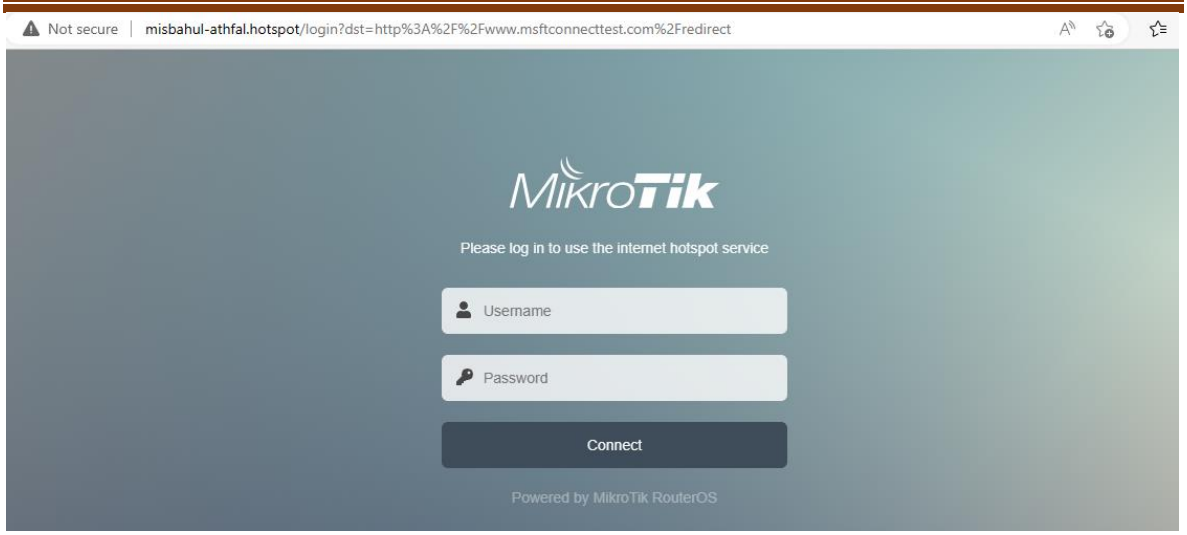
Gambar 12. Membuat nama DNS



Gambar 13. Masukan Password

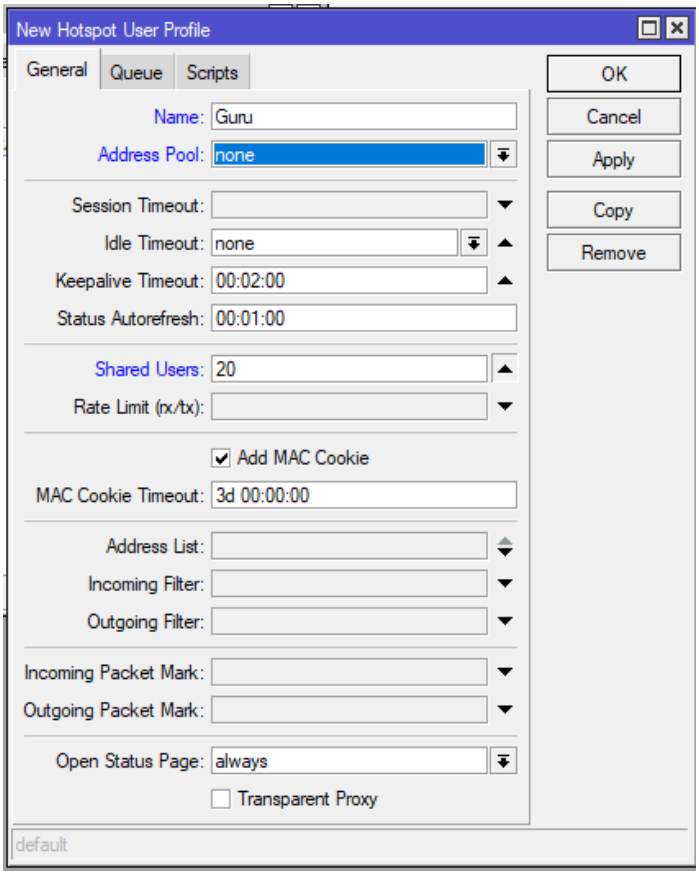


Gambar 14. Lakukan Koneksi pada SSID Misbahul Athfal



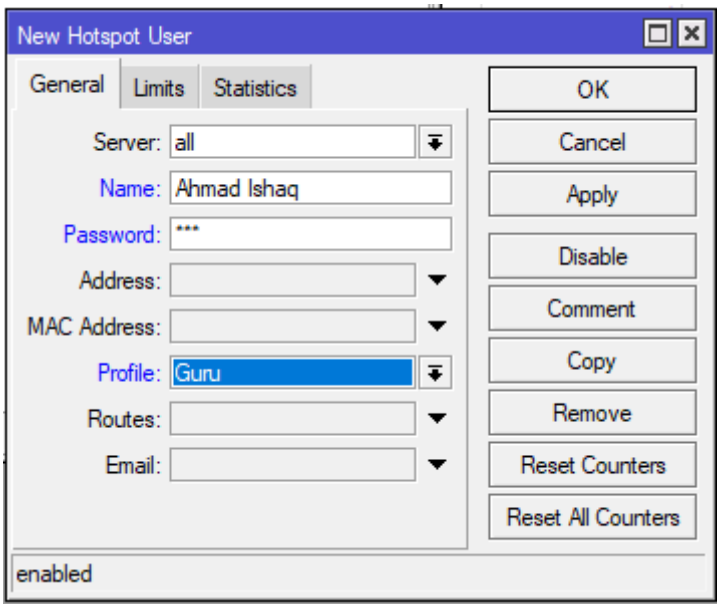
Gambar 15. Masukan Username dan Password

Pada menu hotspot dapat membuat kategori dari user misalkan dibuat kategori Guru seperti pada gambar dibawah ini.



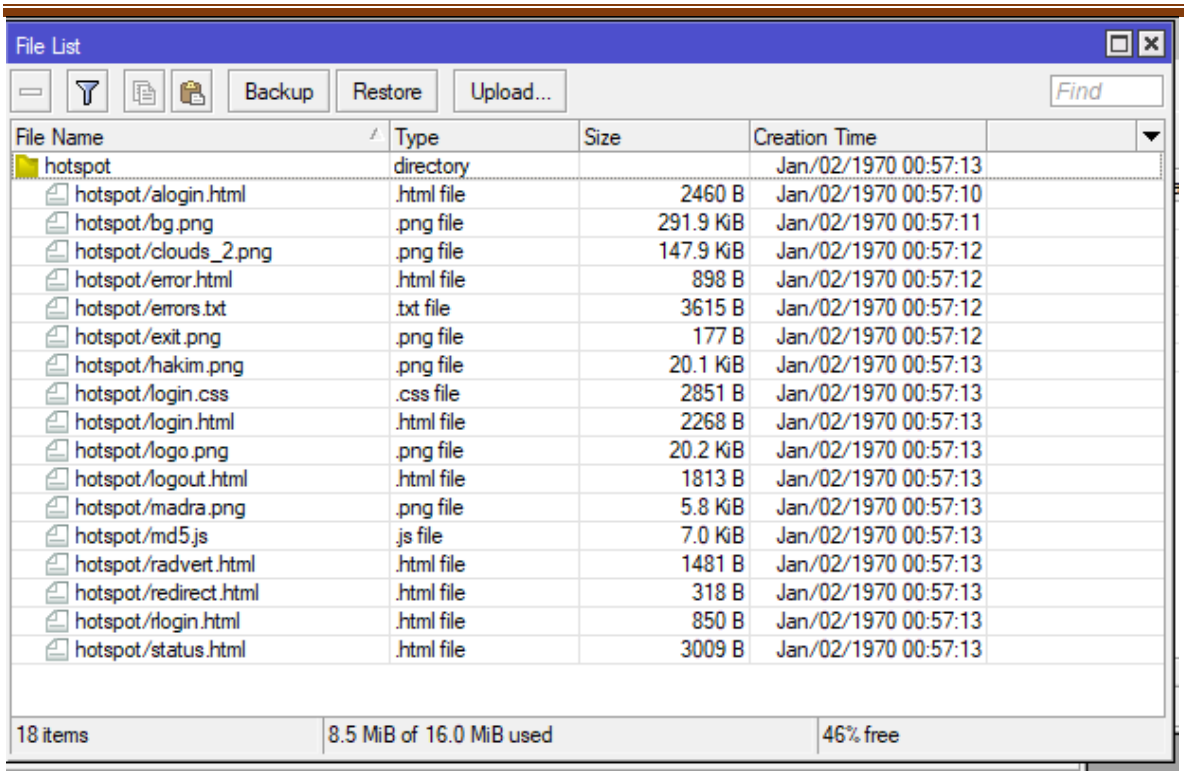
Gambar 16. Membuat User profile dengan Nama Guru

Selanjutnya buat usernya sebanyak pengguna yang ada di Madrasah Ibtidaiyah Misbahul Athfal baik guru maupun siswanya.



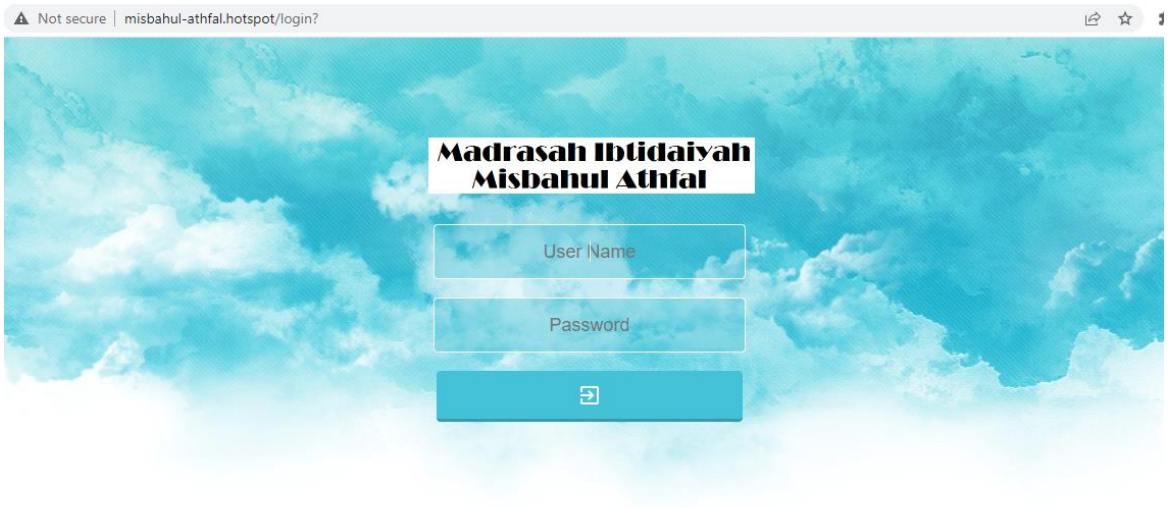
Gambar 17. Membuat user

Gambar 17 Menerangkan membuat User dengan nama Ahmad Ishaq dengan kelompok Guru, Selanjutnya adalah mengganti tampilan page loginnya, Yaitu buat page login menggunakan web programming atau cari template page login lalu di edit. Untuk merubah atau mengedit page login bisa menggunakan notepad atau notepad++ atau editor lainnya. Jika sudah membuat page login atau mengeditnya maka lakukan pengcopyan atau di drag ke dalam files yang ada di menu winbox.



Gambar 18. Page login di drag ke Files winbox

Selanjutnya lakukan koneksi ke SSID Misbahul-Athfal dan tampilan loginnya menjadi seperti dibawah ini.



Gambar 19. Tampilan Login page setelah di edit

KESIMPULAN DAN REKOMENDASI

Dari hasil pengujian yang dilakukan maka dapat disimpulkan bahwa *Authentication Captive Portal* memiliki tingkat keamanan yang lebih baik dibandingkan dengan WPA2-PSK. Dimana setiap user mempunyai *username* dan *password* yang berbeda-beda tidak seperti pada WPA2-PSK. Selain itu user yang terdaftar dapat di*share* sebanyak yang dibutuhkan dengan istilah *shared users*. Dari kesimpulan itu maka sistem keamanan *wireless* menggunakan *Authentication Captive Portal* sangat dianjurkan, serta perangkat yang digunakan level dan versinya yang sesuai agar berfungsi dengan sebaik-baiknya.

REFERENSI

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)

Hariadi, Yutanto. (2019). Penerapan Model Promosi Berbasis Web Captive Portal Hotspot dengan Manajemen Terpusat. Jurnal Sistem Informasi Bisnis.

I, Made Edy Listharta (2020). Automasi Website Browser untuk melakukan Autologin kedalam Captive Portal. Jurnal Ilmiah Informatika Komputer.

Purwanto, T. D., & Cholil, W. (2013). Analisa Kinerja Wireless Radius Server Pada Perangkat Access Point 802.11 g (Studi Kasus di Universitas Bina Darma)

Rahmat. Novrianda. (2018). Implementasi Authentication Captive Portal pada wireless Local Area Network PT. Rikku Mitra Sriwijaya. Jurnal Ilmiah Teknologi Sistem Informasi.

Silitonga, P. (2014). Analisis QoS (Quality of Service) Jaringan Kampus dengan Menggunakan Microtic Routerboard. Jurnal Times