

IMPLEMENTASI SISTEM AUTENTIKASI DAN PENGAMANAN JARINGAN WIRELESS BERBASIS CAPTIVE PORTAL DI PKBM ALSUROYA METRO

Mega Ramadanti¹, Arif Hidayat², Mustika³

^{1,2,3} Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro

^{1,2,3} Jl. Gatot Subroto No.100, Yosodadi, Metro Timur, Kota Metro, Lampung, Indonesia

¹ megar8660@gmail.com, ² androidarifhidayat@gmail.com, ³ dosen.mustika@gmail.com

Abstrak : Kebutuhan akan akses internet sudah menjadi kebutuhan penting di kalangan pemerintahan, bisnis, maupun bidang pendidikan. Teknologi internet ini sudah semakin pesat dan telah mencapai kebutuhan puncak. Begitu juga pada PKBM AI Suroya Metro Timur yang telah ikut dalam perkembangan jaringan internet. Pada PKBM AI Suroya Metro Timur sendiri sudah menggunakan teknologi wireless sebagai sarana prasarana hotspot bagi siswa/siswi dan guru. Dalam hal ini penulis akan mengembangkan suatu jaringan wireless berbasis captive portal menggunakan MikroTik Router RB-941-2ND. Didalam penyusunannya penulis menggunakan metode NDLC Network Development Life Cycle, dan hasil dari penulisan ini yaitu berupa pengembangan sistem jaringan pada PKBM AI Suroya Metro Timur yang meliputi, terbentuknya page login captive portal jaringan pada PKBM AI Suroya Metro Timur memperkuat keamanan jaringan dan konfigurasi manajemen bandwidth di PKBM AI Suroya Metro Timur.

Kata Kunci : Captive Portal, Autentikasi Pengguna Wireless, MikroTik.

Abstract: *The need for internet access has become an important need in government, business and education. Internet technology is increasingly rapid and has reached peak demand. As well at the PKBM AI Suroya, East Metro, which has participated in the development of the internet network. At the PKBM AI Suroya, East Metro it has used wireless technology has been used as a hotspot infrastructure for students and teachers. In this case the author will develop a captive portal-based wireless network using the MikroTik Router RB-941-2ND. In its preparation, the author used the NDLC Network Development Life Cycle method, and the result of this writing is the development of a network system at PKBM AI Suroya Metro Timur which includes the formation of a network captive portal login page at PKBM AI Suroya, East Metro strengthening network security and bandwidth management configuration in PKBM AI Suroya Metro Timur.*

Keywords: *Captive Portal, User Authentication Wireless, MikroTik*

PENDAHULUAN

Perkembangan teknologi akses internet telah mencapai tahapan yang lebih mudah penggunaannya dengan memanfaatkan media akses berbasis wireless atau disebut juga jaringan nirkabel. Jaringan komputer nirkabel adalah salah satu

teknologi yang saat ini sudah digunakan secara luas diberbagai bidang institusi baik perusahaan, dunia pendidikan, instansi pemerintahan bahkan dilingkungan rumah. Selain banyak menguntungkan bagi pengguna dalam memakai jaringan komputer nirkabel, terdapat juga

kekurangan seperti dalam keamanan mentransfer data dan membagi hak akses karena media udara (gelombang elektromagnet). Perangkat keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel koaxial, kini banyak telah diantaranya dibangun dari serat optik (fiber optics) atau komunikasi tanpa kabel (wireless).

Captive Portal adalah suatu proses bagi pengguna dan pengamanan data sebelum terkoneksi ke jaringan internal dan eksternal. Captive Portal merupakan sebuah perangkat router atau gateway yang memproteksi jaringan, sampai pengguna melakukan login terlebih dahulu kedalam sistem. Captive Portal pada umumnya digunakan pada infrastruktur jaringan wireless seperti hotspot area, akan tetapi tidak menutup kemungkinan diterapkan pada infrastruktur jaringan kabel. Jika jaringan hotspot yang dikelola menggunakan router mikrotik dapat dikembangkan sebagai media promosi melalui web dengan memanfaatkan halaman portal login dan dapat dilakukan secara terpusat akan memudahkan bagi admin jaringan dan meningkatkan promosi berbasis portal hotspot.

PKBM AL-Suroya Metro Timur merupakan lembaga Pendidikan non formal yang terletak di Jalan Selagai, Gang.Parto, No.11, Iringmulyo, Kec. Metro Timur, Kota Metro. Lembaga Pendidikan non formal ini berada dibawah naungan dari Dinas Pendidikan Nasional, saat ini PKBM Al-Suroya memiliki 26 pengguna aktif yang menggunakan jaringan wireless yang terdiri dari 18 siswa dan 8 staff. PKBM Al-Suroya Metro Timur memiliki akses internet jaringan dengan kecepatan bandwidth 30

Mbps dari Internet Service Provider (ISP) Indihome.

Berdasarkan hasil wawancara dengan mas Rizky selaku teknisi jaringan di PKBM Al-Suroya adapun kendala yang dirasakan adalah karena jaringan wireless pada PKBM Al-Suroya masih menggunakan konfigurasi keamanan berupa WPA2 yang mana keamanan ini masih menggunakan password yang sama untuk semua penggunaannya, jadi sering kali ada yang membagikan password tersebut ke orang luar lingkungan PKBM Al-Suroya yang menyebabkan jaringan internet menjadi lambat serta lemahnya keamanan jaringan, untuk itu perlu adanya sistem autentikasi dan pengamanan terhadap user yang ingin menggunakan jaringan wireless, sehingga penulis akan mengaplikasikan sebuah jaringan wireless yang didalamnya terdapat akses kontrol, disetiap user akan memiliki akun login sendiri dan memiliki bandwidth atau kecepatan internet sendiri yang berjalan melalui penerapan captive portal. Captive Portal adalah sebuah router yang bisa dikonfigurasi oleh sistem operasi mikrotik, penulis akan menggunakan mikrotik sebagai penerapan sistem operasi jaringan wireless.

Dari uraian diatas, maka penulis melakukan penelitian di PKBM Al-Suroya Metro Timur adapun judul yang di ambil dalam penelitian ini adalah; "IMPLEMENTASI SISTEM AUTENTIKASI DAN PENGAMANAN JARINGAN WIRELESS BERBASIS CAPTIVE PORTAL DI PKBM ALSUROYA METRO".

Tujuan dari penelitian ini yaitu mengimplementasikan sistem autentikasi dan pengamanan pada jaringan wireless berbasis captive portal di PKBM Al-Suroya Metro Timur. Kegunaan penelitian ini diharapkan dapat meningkatkan keamanan

dengan manajemen user pada jaringan wireless di PKBM Al-Suroya dan membantu operator jaringan mengontrol aktifitas user yang telah login kedalam jaringan wireless.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Jaringan Komputer

Syafrizal (2020:2) menjelaskan bahwa jaringan komputer adalah himpunan "interkoneksi" antara 2 komputer autonomous atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel. Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan autonomous.

Topologi Jaringan

Syafrizal (2020:39) menjelaskan bahwa topologi jaringan atau arsitektur jaringan merupakan gambaran perencanaan hubungan antar komputer dalam Local Area Network yang pada umumnya menggunakan kabel (sebagai media transisi), dengan konektor, ethernet card, dan perangkat pendukung lainnya.

Model Jaringan

Terdapat 2 (dua) model jaringan komputer yang digunakan dalam sebuah sistem jaringan computer yaitu jaringan peer to peer dan jaringan client server. Pelealu (2020:5) jaringan peer to peer dapat disimpulkan bahwa pada jaringan jenis ini, setiap komputer yang telah terhubung pada jaringan tersebut dapat berkomunikasi secara langsung dengan komputer lainnya tanpa adanya suatu perantara. Setiap komputer yang terhubung juga dapat berbagi beberapa fasilitas seperti printer, hard disk, dan drive. Sedangkan, Menurut Syafrizal (2020:3) dapat disimpulkan bahwa jaringan client server di mana jaringan yang berperan sebagai server dan client, server hanya sebagai pusat pengendali data untuk memberikan data atau informasi sesuai dengan request client, akses data pada server dengan cara login terlebih dulu kepada server yang dituju.

Perangkat Keras Jaringan

Kurniawan (2020:1) mengemukakan bahwa perangkat keras komputer adalah semua bagian fisik komputer.

Perangkat Lunak Jaringan

Winarno (2019 :11) mengemukakan bahwa "Perangkat lunak adalah perintah (program komputer) yang di eksekusi memberikan fungsi dan petunjuk kerja seperti yang diinginkan.

NDLC (*Network Development Life Cycle*)

Novrianda (2018) menjelaskan bahwa Network Development Life Cycle (NDLC) digunakan dengan melakukan pendekatan terhadap proses komunikasi data berorientasi network yang memiliki suatu lingkaran tahapan yang tidak memiliki awal maupun akhir proses. Tahapan pada metode NDLC adalah analysis, design, simulation prototyping, implementation, monitoring serta tahapan terakhir adalah management.

TCP/IP dan Subneting

Nugroho (2017) menyatakan bahwa TCP/IP (*Transmission Control Protocol atau Internet Protocol*) adalah sebuah perangkat lunak jaringan komputer yang terdapat dalam satu sistem dan memungkinkan komputer satu dengan komputer lain dapat mentransfer data dalam satu grup network atau jaringan. Ia mengemukakan bahwa subneting artinya proses untuk membagi wilayah besar menjadi beberapa wilayah kecil. Seperti kata "sub-net" artinya adalah bagian kecil (sub) dari sebuah network (alamat network) dalam membagi wilayah jaringan kecil, cara yang di lakukan adalah dengan mengubah-ubah parameter pada nilai subnet mask yang di gunakan. Jadi kata kunci dalam proses subnetting adalah pada penggunaan nilai subnetmask.

Sistem Keamanan Jaringan

Keamanan Jaringan

Mutaqqin (2016:3) menyatakan bahwa Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer.

Mikrotik

Madcoms (2015: 212) menyatakan bahwa Mikrotik awalnya ditujukan untuk

perusahaan jasa layanan internet (PJI) atau Internet Service Provider (ISP) yang melayani pelanggannya menggunakan teknologi nirkabel atau wireless. Produk Hardware unggulan Mikrotik berupa Router, Switch, Antena, dan perangkat pendukung lainnya. Sedangkan produk Software unggulan Mikrotik adalah Mikrotik Router OS.

Manajemen Bandwidth

Supendar (2019:23) mengemukakan bahwa manajemen bandwidth adalah proses mengukur dan mengontrol komunikasi (lalu lintas, paket) pada link jaringan, untuk menghindari mengisi link untuk kapasitas atau overflowing link, yang akan mengakibatkan kemacetan jaringan dan kinerja yang buruk. Maksud dari manajemen bandwidth ini adalah bagaimana kita menerapkan pengalokasian atau pengaturan bandwidth dengan menggunakan sebuah PC Router Mikrotik.

Wireless

Rohmah dan Alexander (2019:11) dapat disimpulkan bahwa wireless atau wireless network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Pada dasarnya wireless dengan LAN merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainnya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika LAN masih menggunakan kabel sebagai media lintas data, sedangkan wireless menggunakan media gelombang radio/udara.

Captive Portal

Setyawan dan Syafrizal (2020:14) dapat disimpulkan bahwa captive portal adalah suatu teknik autentikasi dan pengamanan data yang lewat dari network internal ke network eksternal. Captive Portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik, hingga user melakukan registrasi.

Metode Autentikasi Jaringan Wireless

Pratama (2019:1) menyatakan bahwa autentikasi user merupakan suatu usaha untuk mempermudah pengguna dalam melakukan koneksi jaringan wireless melalui perangkat laptop dan smartphone. Dengan sistem tersebut, hanya tinggal menggunakan username dan password yang berbeda dan unik bagi masing-masing pengguna.

Black Box Testing

Hermanto (2019:19) dapat disimpulkan bahwa pengujian dilakukan menggunakan sekumpulan aktifitas validasi, dengan pendekatan black box testing. Black Box Testing adalah menguji perangkat lunak dari segi spesifikasi fungsional tanpa menguji desain dan kode program. Pengujian dimaksudkan untuk mengetahui apakah fungsi-fungsi, masukan, dan keluaran dari perangkat lunak sesuai dengan spesifikasi yang dibutuhkan.

Flowchart

Fauzi (2020: 3) menyatakan bahwa flowchart adalah cara penulisan algoritma dengan menggunakan notasi grafis. Flowchart merupakan gambar atau bagan yang memperlihatkan urutan atau langkah-langkah dari suatu program dan hubungan antar proses beserta pernyataannya. Gambaran ini dinyatakan dengan simbol. Dengan demikian setiap simbol menggambarkan proses tertentu.

METODE

Untuk mencapai tujuan penelitian tersebut, penulis menggunakan metode pengembangan metode pengembangan *Network Development Life Cycle* (NDLC) dengan tahapan analisis, perancangan (design), simulasi (simulation), implementasi, monitoring, dan management. Tahapan yang dilakukan dalam penelitian ini baru sampai pada tahap monitoring.

Metode penelitian yang digunakan adalah data kualitatif dengan teknik pengumpulan data berupa studi lapangan dan studi pustaka. Studi lapangan sendiri dilakukan dengan wawancara, dokumentasi, dan observasi. Teknik wawancara dari teknisi jaringan PKBM AL-Suroya Metro Timur yaitu mengumpulkan data dengan cara

tanya-jawab langsung dengan yang berwenang yang ada kaitannya dengan objek penelitian. Dari hasil wawancara penulis akan memperoleh data mengenai gambaran umum dan sejarah perkembangan PKBM AL-Suroya Metro Timur. Teknik dokumentasi ini, penulis mengumpulkan dan menganalisa data-data penting tentang PKBM AL-Suroya Metro Timur, terutama yang berhubungan dengan Jaringan Wireless. Dokumentasi yang dilakukan adalah topologi jaringan, dokumentasi ruangan, dokumentasi Kecepatan Jaringan PKBM AL-Suroya Metro, dokumentasi router, sejarah singkat organisasi, lokasi organisasi, struktur organisasi, manajemen organisasi, analisis sistem yang berjalan. Sedangkan tahap pengumpulan observasi dilihat dengan cara mengamati dan melakukan analisa secara langsung keadaan objek penelitian di lapangan, yaitu PKBM AL-Suroya Metro Timur.

Sedangkan untuk studi pustaka diperoleh dari buku, jurnal, majalah, hasil-hasil penelitian (tesis dan disertasi), dan sumber-sumber lainnya yang sesuai (internet, koran dll).

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk dapat merancang dan menerapkan captive portal dan manajemen bandwidth pada PKBM AL-Suroya Metro Pusat menggunakan router mikrotik. Selain itu mampu untuk setiap pengguna (user) mendapatkan user dan password dan setiap pengguna (user) mendapatkan kecepatan bandwidth yang telah ditetapkan. Agar mencapai tujuan penelitian tersebut, Penulis menggunakan metode pengembangan NDLC (*Network Development Life Cycle*) yang dimana metode ini memiliki tahapan-tahapan dalam penyusunan. Tahapan-tahapan tersebut diantaranya Analisis, Perancangan (design), Simulasi (Simulation), Implementasi, Monitoring, dan Management.

Analisis

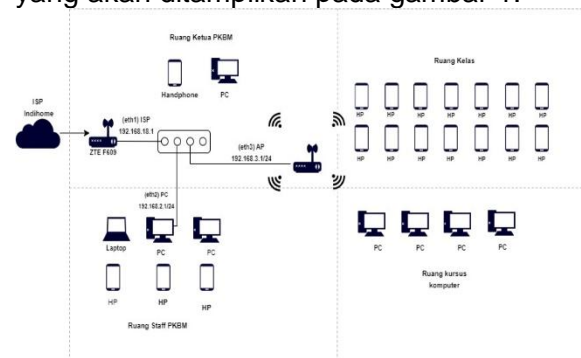
Dari hasil wawancara dan riset pada PKBM AL-Suroya membutuhkan sebuah perancangan captive portal guna

mendapatkan user dan password sesuai kebutuhannya. Maka demikian dengan menggunakan perancangan captive portal jaringan yang ada di PKBM AL-Suroya dapat memmanagement jaringan secara keseluruhan dan memiliki bandwidth atau kecepatan internet sendiri yang berjalan melalui penerapan captive portal.

Perancangan (Design)

Design topologi yang sudah dibuat oleh penulis sesuai dengan analisis yang dilakukan. Berikut ini hasil design topologi yang sudah dibuat, topologi yang digunakan adalah topologi star. Alur sistemnya berawal dari internet menuju ke router mikrotik lalu mengkonfigurasi sebuah captive portal dan manajemen bandwidth pada router mikrotik. Sesudah itu menuju ke acces point.

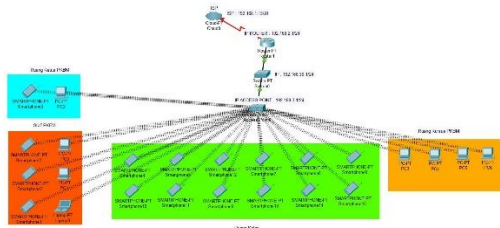
Dari penerapan topologi jaringan yang dibangun pada gambar 1. Adapun penulis menerapkan topologi jaringan pada PKBM AL-Suroya Metro Timur. Berikut ini merupakan penerapan gambaran topologi yang akan ditampilkan pada gambar 1.



Gambar 1 Menerapkan Topologi Jaringan Pada PKBM AL-Suroya Metro Timur

Simulasi (Simulation)

Pada tahap simulasi ini, penulis membuat simulasi dengan bantuan tools cisco packet tracer. Hal ini bermaksud untuk membuat simulasi jaringan sebelum dibangun dan juga proses jaringan yang akan dibangun.

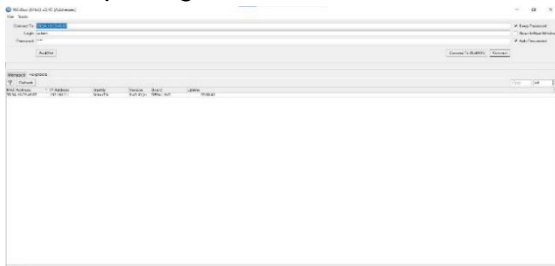


Gambar 2 Simulasi Cisco Packet Tracer yang digunakan Pada PKBM AI Suroya Metro Timur

Implementasi

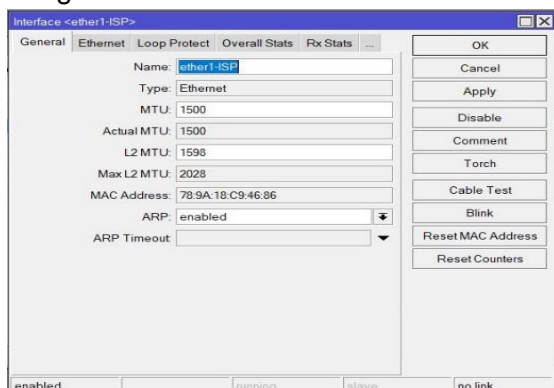
Konfigurasi Router Mikrotik

Pertama membuka aplikasi winbox yang sudah terinstal dilaptop untuk mengatur router mikrotik. Seperti dilihat tampilan winbox pada gambar 3.



Gambar 3 Tampilan Winbox

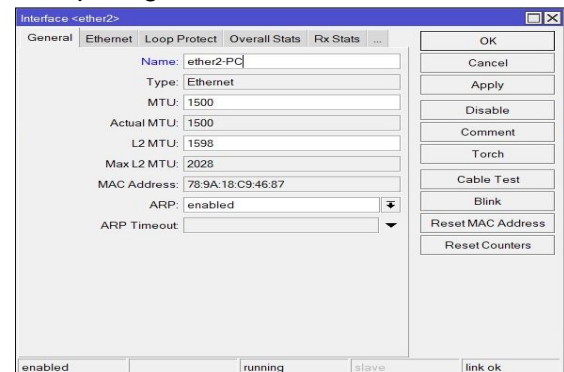
Selanjutnya masuk menu interface, lalu berikan nama pada setiap ether, seperti pada gambar 4. Yang berguna untuk mempermudah penulis dalam mengingat fungsi setiap ether, lakukan rename ether1 dengan nama ether1-ISP.



Gambar 4 Tampilan menu rename interface ether1

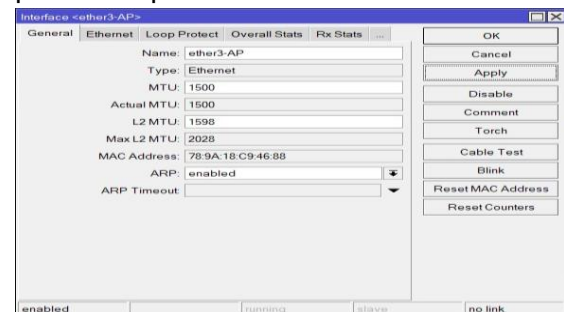
Berikutnya, lakukan rename pada ether2 dengan nama ether2-PC, seperti pada gambar 5 yang berguna untuk

mempermudah penulis dalam mengingat setiap fungsi ether.



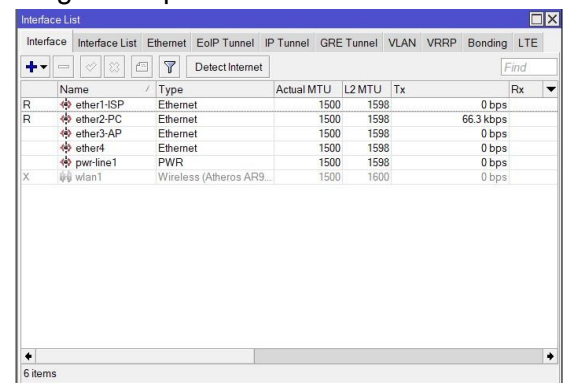
Gambar 5 Tampilan Menu Interface Saat Rename Ether2

Kemudian lakukan rename pada ether3 dengan nama ether3-AP seperti pada gambar 6 yang berguna untuk mempermudah penulis mengingat fungsi pada setiap ether.



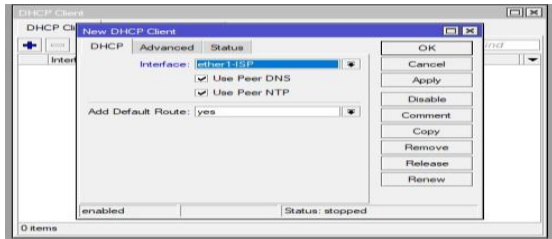
Gambar 6 Tampilan Menu Interface Saat Rename Ether3

Kemudian berikut tampilan pada interface yang sudah di rename seperti pada gambar 7 yang berguna untuk mengingat fungsi setiap ether.



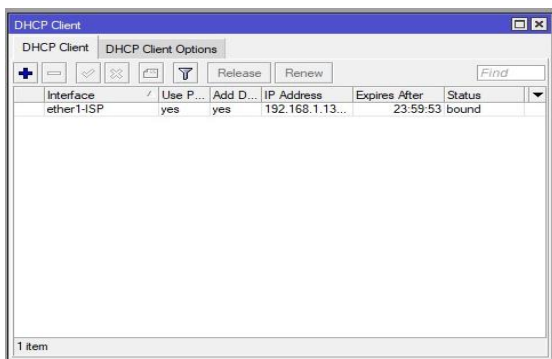
Gambar 7 Tampilan Menu Interface Yang Telah Diganti Nama Di Setiap Ether

Masuk ke menu DHCP Client, kemudian pilih tanda plus (+). Pada bagian interfaces pilih eth 1 sebagai sumber internet atau ISP, seperti tampilan konfigurasi DHCP Client pada gambar 8.



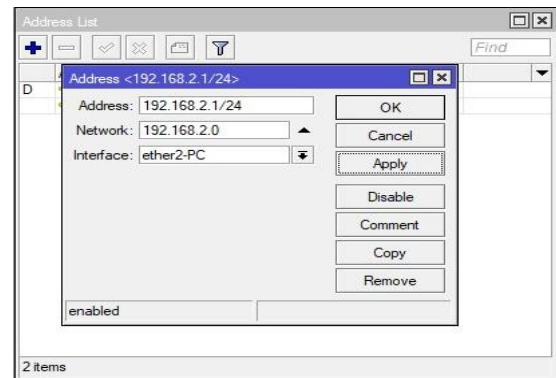
Gambar 8 Tampilan Konfigurasi Dhcp Client

Untuk mengetahui setting DHCP Client berhasil, dengan melihat status DHCP Client apabila bound, maka settingan DHCP Client berhasil. Dapat dilihat tampilan DHCP Client bound pada gambar 9.



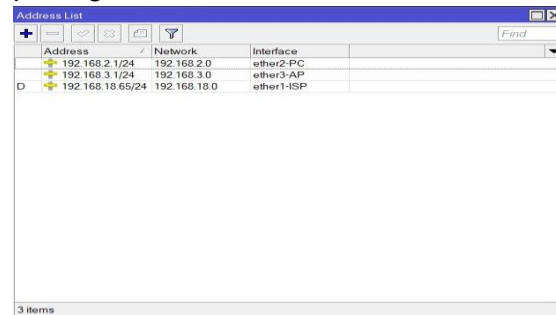
Gambar 9 Tampilan DHCP Client Bound

Berikutnya setting IP Address, IP address berfungsi sebagai alamat pengiriman data ke perangkat yang kita gunakan. Pada menu IP Address pilih tanda plus (+), lalu masukkan IP pada menu IP address dan pilih interfaces eth2 sebagai client. Selanjutnya klik Apply dan OK.



Gambar 10 Tampilan Konfigurasi IP Address

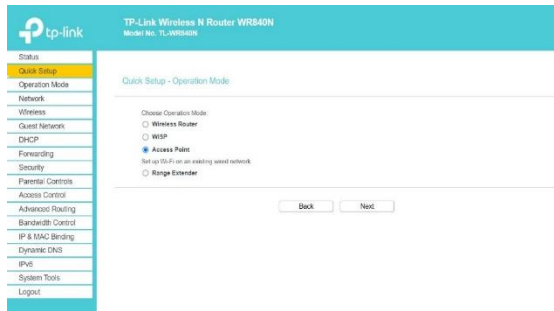
Berikut tampilan IP Address yang digunakan. Pada eth1 mendapatkan sumber internet dengan IP 192.168.18.1/24, eth2 sebagai client dengan IP 192.168.2.1/24 dan eth3 sebagai access point dengan menggunakan IP 192.168.3.1/24. Adapun address list interfaces yang dapat dilihat pada gambar 11.



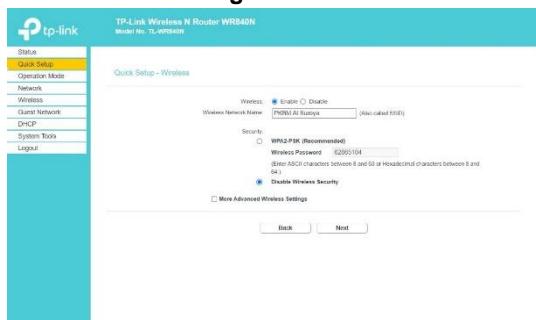
Gambar 11 Tampilan Address List Interfaces

Konfigurasi Access Point

Konfigurasi awal pada tahap ini dilakukan adalah konfigurasi dasar, pada penelitian ini digunakan 1 buah perangkat access point dengan merk tp-link WR840N, berikut ini konfigurasi dasar untuk access point. Untuk membuka menu konfigurasi access point untuk membuka menu konfigurasi access point dapat dilihat pada gambar 12 menu awal konfigurasi perangkat tp-link karena perangkat akan kita gunakan sebagai access point maka pada tab quick setup silahkan pilih access point, kemudian klik next.

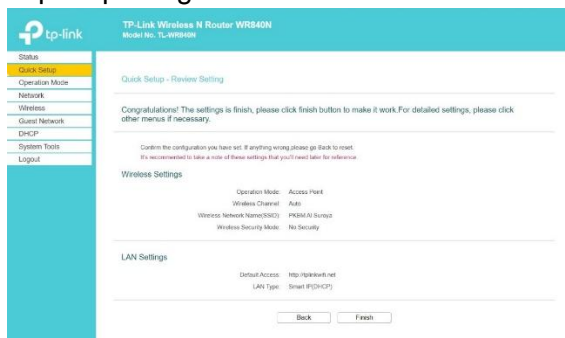


Gambar 12 Konfigurasi Dasar Access Point



Gambar 13 Konfigurasi SSID Access Point

Kemudian jika konfigurasi perangkat tp-link sudah berhasil diubah maka sekarang tp-link dapat digunakan sebagai access point seperti pada gambar 14.



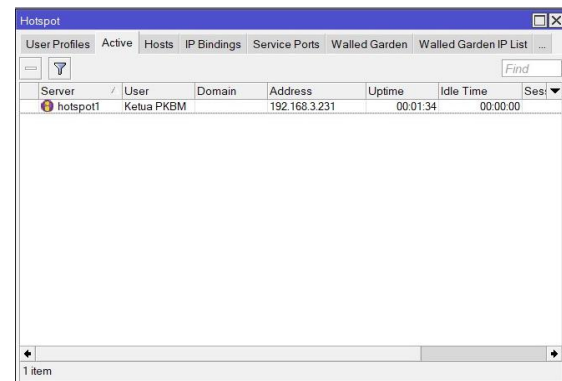
Gambar 14 Tampilan Perangkat Tp-Link Jika Sudah Berhasil Diubah

Monitoring

Adapun tahapan monitoring dalam NDLC (Network Development Life Cycle) yang mengkategorikan yaitu adanya proses pengujian. Dalam proses pengujian (testing) dibutuhkan guna menjamin dan memastikan bahwa system yang dibangun pada PKBM AI-Suroya berjalan dengan baik.

Men-Testing User (Pengguna)

Pada uji tahap Men-Testing User (Pengguna) yang berada aktif menggunakan hotspot dan kecepatan data yang dipakai oleh User (Pengguna). Berikut Testing user (pengguna) yang aktif pada gambar 15.

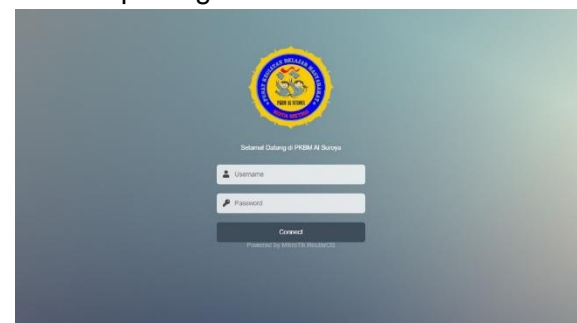


Gambar 15 Menampilkan Hasil User Yang Aktif

Testing Bandwidth setiap User

Dari hasil konfigurasi yang sudah dilakukan, penulis melakukan testing jaringan yaitu apakah konfigurasi jaringan tersebut berjalan dengan baik ataupun tidak. Maka dari itu diperlukan dengan melakukan testing jaringan sebagai berikut:

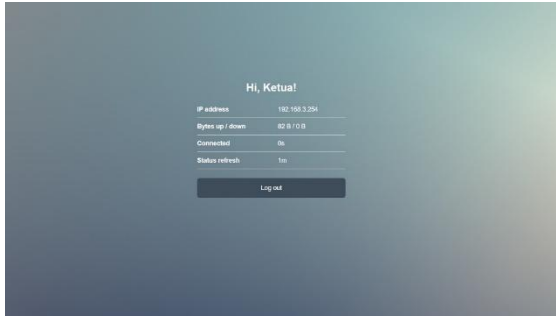
- 1) Men-Testing jaringan hotspot, berikut ini merupakan tampilan awal yaitu captive portal pada PKBM AI-Suroya. Terlihat pada gambar 16.



Gambar 16 Tampilan Captive Portal PKBM AI-Suroya Metro Timur

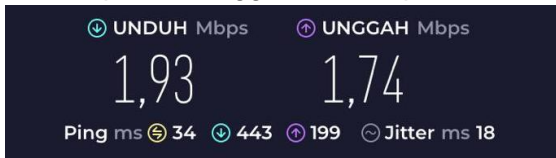
- 2) Tampilan status login captive portal dengan menggunakan user login Ketua PKBM dapat dilihat pada gambar 84 yang menampilkan user Ketua dan

mendapatkan IP 192.168.3.254 dengan total jumlah pemakaian download/upload sebesar 82B/0B.



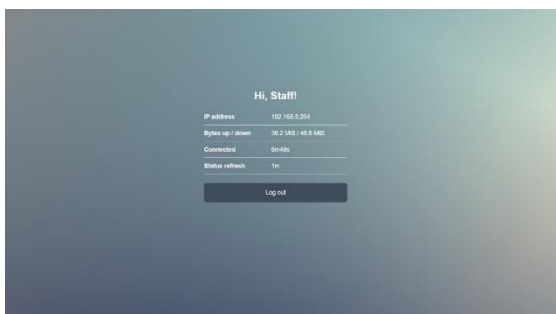
Gambar 17 Tampilan Status Login Captive Portal Pada User Ketua PKBM

3) Hasil Kecepatan Bandwidth yang didapat pada User Ketua PKBM dengan menggunakan speedtest Ookla. Seperti pada gambar 18 yang menampilkan hasil uji kecepatan dengan hasil unduh sebesar 1.93Mbps dan unggah 1.74Mbps.



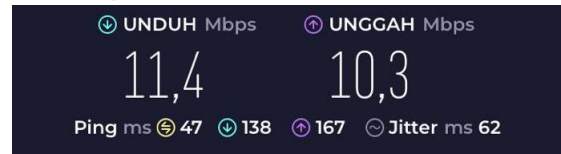
Gambar 18 Tampilan Kecepatan Bandwidth yang didapat pada User Ketua PKBM

4) Tampilan status Login captive portal menggunakan user staff PKBM. Seperti pada gambar 19 yang menampilkan user staff mendapatkan IP 192.168.3.254 dengan total jumlah pemakaian download/upload sebesar 38.2B/48.6B.



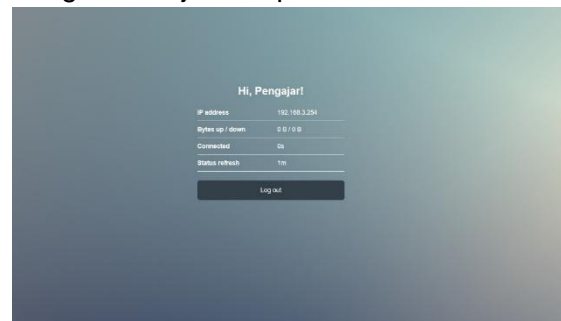
Gambar 19 Tampilan Status login captive portal pada user Staff PKBM

5) Hasil Kecepatan Bandwidth yang didapat pada user Staff PKBM dengan menggunakan speedtest Ookla. Dapat dilihat pada gambar 20 yang menampilkan hasil uji kecepatan dengan hasil download sebesar 11.4Mbps dan unggah sebesar 10.3Mbps.



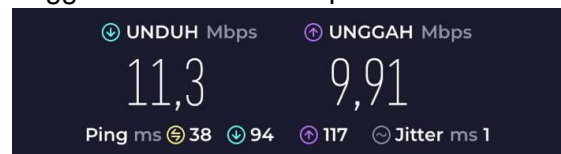
Gambar 20 Tampilan Kecepatan Bandwidth yang didapat pada User Staff PKBM

6) Tampilan Status login captive portal menggunakan user Pengajar. Seperti pada gambar 21 yang menampilkan user pengajar mendapatkan IP 192.168.3.254 dengan total jumlah pemakaian 0B/0B.



Gambar 21 Tampilan Status Login Captive Portal Pada User Pengajar

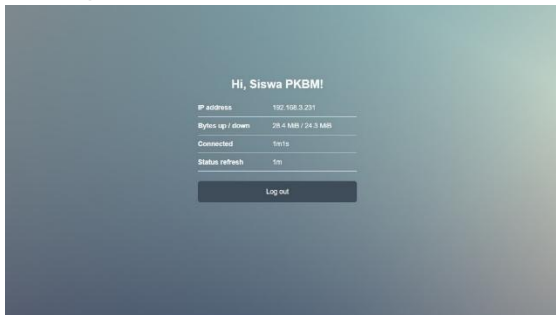
7) Hasil Kecepatan Bandwidth yang didapat pada user Tenaga Pengajar dengan menggunakan speedtest Ookla. Dapat dilihat pada gambar 22 yang menampilkan hasil uji kecepatan dengan hasil download sebesar 11.3Mbps dan unggah sebesar 9.91Mbps.



Gambar 22 Tampilan Kecepatan Bandwidth yang didapat pada User Pengajar

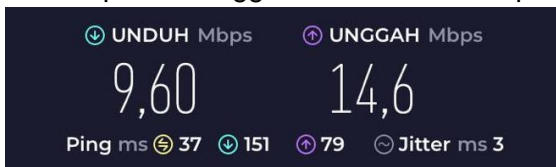
8) Tampilan status Login captive portal menggunakan user siswa. Seperti

pada gambar 23 yang menampilkan user siswa mendapatkan IP 192.168.3.231 dengan jumlah total pemakaian download atau upload sebesar 28.4MB/24.3MB.



Gambar 23 Tampilan Status Login Pada User Siswa

9) Hasil Kecepatan Bandwidth yang didapat pada user Siswa menggunakan speedtest Ookla. Dapat dilihat pada gambar 91 yang menampilkan hasil uji kecepatan dengan hasil download sebesar 9.60Mbps dan unggah sebesar 14.6Mbps.



Gambar 24 Tampilan Kecepatan Bandwidth Yang Didapat Pada User Siswa

Hasil Pengujian

Pengujian ini berfokus pada persyaratan fungsional dengan memeriksa apakah sistem menghasilkan output yang diharapkan dan sesuai dengan fungsinya, pada tabel 1 menampilkan hasil dari pengujian black box testing.

Tabel 1 Hasil Pengujian Black Box

No.	Skenario	Output	Kesimpulan
1	Mengetikkan <i>username</i> dan <i>password</i> dengan <i>user</i> yang salah dihalaman <i>login</i>	Tampilan halaman <i>login</i> akan muncul pesan <i>username</i> dan <i>password</i> <i>invalid</i> .	Berhasil

2	Mengetikkan <i>username</i> dan <i>password</i> dengan <i>user</i> yang benar dihalaman <i>login</i> kemudian klik tombol <i>connect</i>	Berhasil masuk dan muncul sebuah halaman sukses <i>login</i> .	Berhasil
3	Melakukan browsing tanpa proses autentikasi pada halaman <i>login</i> jaringan <i>wireless</i>	Pengguna tidak dapat terkoneksi internet	Berhasil
4	Username dan password tidak diisi kemudian klik tombol <i>login</i> .	Sistem akan menolak dan muncul pesan "invalid username or password"	Berhasil
5	Memasukkan password dan mengosongkan <i>username</i> kemudian klik tombol <i>login</i>	Sistem akan menolak dan muncul pesan "invalid username or password"	Berhasil
6	Memasukkan <i>username</i> dan mengosongkan password kemudian klik <i>login</i>	Sistem akan menolak dan muncul pesan "invalid username or password"	Berhasil

(Sumber: Penulis, 2024)

Management

Router mikrotik berperan sebagai manajemen jaringan salah satunya yaitu manajemen bandwidth, manajemen user.

Hal ini bertujuan guna jaringan berjalan dengan baik.

Selanjutnya, pada perangkat access point memiliki peranan sebagai penyebar jaringan wireless. Adapun kinerja menggunakan hotspot pada PKBM Al-Suroya Metro Timur adalah setiap pengguna mendapatkan akses jaringan sesuai dengan username dan password jaringan yang sudah ditentukan oleh admin dan kecepatan bandwidth yang sudah ditentukan oleh admin.

KESIMPULAN

Penelitian ini berhasil mencapai tujuannya, yaitu mengimplementasikan sistem autentikasi dan pengamanan berbasis captive portal pada jaringan wireless di PKBM Al Suroya Metro Timur. Berdasarkan hasil pengujian Black Box Testing dan uji kelayakan yang dilakukan bersama admin jaringan dan pendamping instansi menunjukkan bahwa captive portal berhasil mengatasi masalah yang ada pada PKBM dan setiap pengguna yang terhubung dengan jaringan yang tersedia diharuskan login terlebih dulu dengan username dan password yang telah disediakan.

Beberapa kelebihan yang ada pada implementasi sistem autentikasi dan pengamanan berbasis captive portal di PKBM Al Suroya Metro Timur adalah sistem keamanan jaringan yang dibuat memberikan page login terlebih dahulu dan melakukan autentikasi berupa captive portal sebelum mengakses jaringan. Sistem ini memberikan solusi pada kendala yang sedang dihadapi yaitu masih menggunakan password yang sama untuk semua penggunaannya, sehingga keamanan jaringan masih rentan dibobol atau diketahui oleh pihak yang tidak berwenang yang ikut mengakses jaringan dan penelitian ini menghasilkan perancangan jaringan yang didalamnya terdapat

manajemen bandwidth sehingga setiap username memiliki kecepatannya masing-masing, ini berguna untuk memastikan bahwa semua pengguna dapat memiliki akses internet yang stabil.

Adapun beberapa saran dari penulis seperti, penambahan filtering akses pada jaringan wireless sehingga jaringan hanya dapat digunakan pada kebutuhan yang memang diperlukan dan penambahan fitur penggunaan MAC Address sebagai akses login user sehingga pengguna jaringan akan lebih mudah di kontrol.

REFERENSI.

- [1] Darmadi, E. A., 2018. Optimalisasi jaringan menggunakan firewall. *IKRA-ITH Informatika: Jurnal Komputer dan Informatika*, 2(3), h. 17-23.
- [2] Fatayana, N. F., Mustika, & Hidayat, A. 2022. Pengembangan Keamanan Jaringan Hotspot Berbasis Mikrotik Menggunakan Otentikasi Pengguna (User) Di SMP Negeri 7 Metro. *Jurnal Mahasiswa Ilmu Komputer (JMik)*, 3(2), h. 376–384.
- [3] Hasan, I. 2016. Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V. 5.20 Di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*, 2(1), h. 10-19.
- [4] Hermanto, B. 2019. Sistem Informasi Manajemen Keuangan pada PT. Hulu Balang Mandiri Menggunakan Framework Laravel. *Jurnal Komputasi*, 7(1), h. 17-26.
- [5] Mutaqin, A. F. 2016. Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol*, 1(1), 4-5.
- [6] Novrianda, R. 2018. Implementasi authentication Captive Portal pada

Wireless Local Area Network PT. Rikku Mitra Sriwijaya. Register: *Jurnal Ilmiah Teknologi Sistem Informasi*, 4(2), h. 67-80.

[7] Pelealu, R. R. A. A., Wonggo. 2020. Perancangan Dan Implementasi Jaringan Komputer Smk Negeri 1 Tahuna. JOINTER: *Journal of Informatics Engineering*, 1(01), h. 5-11.

[8] Ramanda, B. D., Irawan, D., & Hidayat, A. (2024). Rancang Bangun Manajemen Bandwidth Menggunakan Metode Simple Queue Mikrotik Router Pada SMK N 1 Trimurjo. *Jurnal Mahasiswa Ilmu Komputer*, 5(1), 86-95.

[9] Supendar, H. 2019. Simple Queue Dalam Menyelesaikan Masalah Manajemen Bandwidth Pada Mikrotik Bridge. *Bina Insani ICT Journal*, 4(1), h. 21-30.

[10] Wulandari, R. 2016. Analisis Qos (Quality Of Service) Pada Jaringan Internet (Studi Kasus: Upt Loka Uji Teknik Penambangan Jampang Kulon "LIPI). *Jurnal teknik informatika dan sistem informasi*, 2(2).