

Perancangan Keamanan Jaringan Metode Authentication Login Hotspot Menggunakan Router Mikrotik di PT. Nusindo Rekatama Semesta

Muhammad Fachry Altarik & Andriyan Dwi Putra
Informatika Universitas Amikom Yogyakarta

email : muhammad.altarik@students.amikom.ac.id &
andriyan.putra@amikom.ac.id

Informasi Artikel:

Received: 17 November 2023, Accepted: 27 November 2023, Published: 30 November 2023

Abstract

PT. Nusindo Rekatama Semesta is a company located in the Sleman Regency area, Jombor Lor, Sinduadi. PT. Nusindo Semesta is a company in the corporate management industry that has been operating since February 2011. PT. Nusindo Rekatama Semesta provides wireless hotspot facilities where employees and visitors who come can take advantage of an internet connection that can be accessed via laptops, smartphones, or other devices such as those that support wireless technology. However, the implementation of hotspots needs to be corrected; for example, per-client bandwidth still needs to be focused. It aims to overcome per-client bandwidth usage and create a captive login portal as a security system so that those who do not have access rights cannot use internet access in the company. Using the hotspot login authentication system within the company. With the application of Mikrotik Router OS as a router in the company's network, it can overcome the instability of wireless network connections, and the captive portal login feature on Mikrotik can prevent users who do not have access rights from being able to use the internet access in the company.

Keywords: Computer Network, Network Security, Mikrotik, Router, Wireless Hotspot, Captive Portal Login And Login Authentication

1. Pendahuluan

Perkembangan jaringan internet semakin berkembang seiring berjalannya waktu, maka diperlukan suatu manajemen agar para *user* merasa nyaman saat menggunakan jaringan internet (Savytri & Ratri, 2023). Hal tersebut dapat dikaitkan dengan penggunaan bandwidth, bandwidth merupakan bagian penting dalam penggunaan layanan internet, distribusi bandwidth yang tidak optimal, dan merata, merupakan masalah yang sering terjadi dan dialami oleh penyedia jaringan internet, khususnya dilingkungan kantor, dengan tingkat pemakaian

bandwidth yang besar, mengakibatkan distribusi bandwidth tidak berjalan maksimal sehingga sering mengakibatkan delay pada jaringan, delay ini disebabkan oleh beberapa faktor, yaitu Bandwidth yang tidak mencukupi, keterbatasan daya serta dapat disebabkan oleh kurang optimalnya kinerja dari router jaringan (Rismayadi et al., 2023). Salah satu contoh dalam permasalahan tersebut yaitu dalam kegiatan mendownload berkas-berkas dan rapat secara bersamaan membuat ketidaknyamanan *user* perusahaan dalam menggunakan jaringan *hotspot*.

Pentingnya pengelolaan bandwidth menjadi sangat signifikan, terutama pada jaringan dengan kapasitas bandwidth yang terbatas (Salam & Kho, 2023). Pengelolaan bandwidth yang efektif dapat memaksimalkan pengaksesan data sehingga *user* akan merasa nyaman dalam mengakses internet (Sidqi et al., 2021). Hal-hal yang biasanya menyebabkan terjadinya penurunan bandwidth adalah banyaknya *user*, sehingga akan terjadi saling berebut bandwidth antar *user* (Syafri, 2023). Selain banyaknya *user* aktivitas video streaming, download dan upload yang dilakukan oleh *user* dapat menyebabkan terjadinya penurunan bandwidth karena akan menggunakan trafik yang tinggi (Qintharah & Utami, 2023).

Permasalahan lain yang muncul pada saat observasi lapangan salah satunya terdapat pada adanya *user* yang *illegal* menggunakan jaringan *hotspot* sehingga pembagian *bandwidth* menjadi tidak merata. *User* yang menggunakan jaringan merupakan penduduk yang berada disekitar area perusahaan. Gambaran *user illegal* merupakan *user* atau pemakai jaringan *hotspot* yang tidak memiliki kepentingan, namun dapat dengan mudah terkoneksi dengan *hotspot* pada perusahaan dan mendapatkan akses internet. Permasalahan diatas menjadi salah satu gambaran kelemahan keamanan jaringan di perusahaan. Perlu adanya upaya untuk mengatasi hal tersebut.

Maka dari itu diperlukan adanya sistem authentication login *hotspot* untuk mengatasi kelemahan tersebut dan pembuatan captive portal login sebagai sistem keamanan sehingga pengguna yang tidak memiliki hak akses tidak dapat menggunakan akses internet di perusahaan tersebut, serta diperlukannya sistem manajemen bandwidth untuk mengatur alur pemakaian bandwidth *hotspot* pada perusahaan. Sehingga semua pengguna yang ingin terhubung dengan internet harus melakukan autentifikasi terlebih dahulu. Proses autentifikasi secara aman dapat dilakukan melalui sebuah aplikasi web browser dan sisi pengguna.

Captive portal melalui Splash Page akan membantu pemilik jaringan memblokir pengguna agar mereka tidak memiliki akses yang lebih luas ke jaringan yang ingin mereka akses sampai tuan rumah membuat verifikasi. Selain membatasi akses, captive portal juga digunakan jika penyedia jaringan ingin menghindari tanggung jawab hukum seandainya pengguna memanfaatkannya untuk tindakan yang melanggar. Misalnya saja, ada orang yang menggunakan jaringan internet gratis untuk melakukan tindakan penipuan, adanya captive portal bisa membebaskan dari tuntutan sebagai penyedia jaringan internet. Dengan menggunakan kustomisasi tertentu, perusahaan sebagai pemilik jaringan dapat secara progresif mengumpulkan data dari pengguna jaringan. Ini bisa mereka manfaatkan untuk mendapatkan informasi terkait kebiasaan konsumen hingga informasi lain yang digunakan saat login (seperti email atau media sosial).

Dalam hal ini penulis memakai router mikrotik hAP series RB941-200-2ND yang digunakan untuk sistem captive portal login dan sistem simple queue untuk sistem keamanan jaringan dan pengaturan bandwidth.

2. Tinjauan Literatur

2.1 Pengertian Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi/ peramban web. Tujuan dari jaringan komputer adalah agar setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan atau mengirim layanan disebut peladen (server) (Barakabitze et al., 2020).

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya (Mohamed et al., 2021).

Menurut Sofana, jaringan komputer adalah sekumpulan koneksi untuk sejumlah besar komputer otonom. Dalam bahasa sehari-hari, jaringan komputer dapat digambarkan sebagai kumpulan komputer yang saling terhubung melalui media perantara seperti media berkabel dan media nirkabel (nirkabel), berdasarkan ukuran dan area (Sofana, 2013). Menurut Abdullah, jaringan komputer adalah kumpulan komputer yang saling berhubungan menjadi satu kesatuan dan perangkat pendukung komputer lainnya. Jaringan komputer, di sisi lain, adalah kumpulan komputer dan alat yang saling berhubungan melalui media komunikasi tertentu (Tahir et al., 2023).

Pengertian beberapa jurnal di atas dapat didefinisikan jaringan komputer yaitu himpunan “interkoneksi” antara 2 komputer autonomous atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless).

Jenis-jenis Jaringan Komputer

Melwin Syafrizal, 2018 menyatakan bahwa jaringan komputer secara umum terbagi dalam 3 jenis, yaitu:

LAN (Local Area Network)

Suatu jaringan komputer yang hanya mencakup wilayah lokal saja. Artinya, jaringan ini hanya dapat digunakan oleh pengguna di area LAN. LAN menghubungkan perangkat ke jaringan internet melalui perangkat jaringan sederhana. Dalam jaringan LAN biasanya ditemukan kabel UTP, Hub, Switch, maupun Router. Contoh dari jaringan ini adalah komputer-komputer di sekolah, perusahaan, atau warung internet. Jaringan pada area yang terbatas tersebut biasanya merupakan jaringan LAN (Melwin Syafrizal, 2005).

MAN (Metropolitan Area Network (MAN))

Suatu jaringan komputer yang dapat mencakup area yang lebih luas dan menggunakan teknologi yang lebih canggih dari LAN. Jaringan MAN merupakan gabungan beberapa jaringan LAN yang mana menjangkau hingga 10 s.d. 50 km. Jaringan MAN cocok dipakai untuk membangun jaringan antar perkantoran atau instansi yang masih dalam satu kota. Biasanya MAN dipakai untuk menghubungkan beberapa lokasi seperti perkantoran, kampus, pemerintahan, dan sebagainya. Metropolitan Area Network digunakan karena kecepatan transfer data yang dinilai tinggi dan proses instalasi yang tidak terlalu rumit. Di dalam MAN, dibutuhkan operator telekomunikasi yang akan menjadi penghubung antar jaringan komputer (Melwin Syafrizal, 2005).

WAN (Wide Area Network)

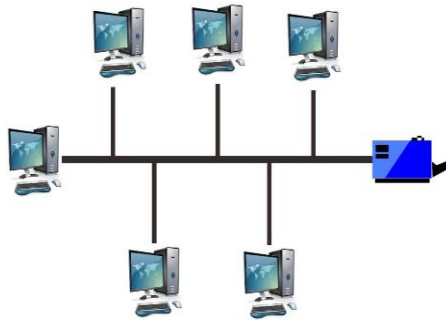
Published by:

Jaringan komputer yang luas cakupannya dapat mencapai satu negara bahkan benua. Jaringan ini merupakan gabungan dari LAN dan MAN yang wilayahnya dipisahkan secara geografis. Membangun jaringan WAN membutuhkan kabel serat optik (*fiber optic*), kabel telepon, atau bisa juga menggunakan satelit. Oleh karena jangkauannya yang luas, membuat WAN memerlukan biaya yang sangat besar. WAN mempunyai transmisi kecepatan mulai dari 2 Mbps, 34 Mbps, 45 Mbps, 155 Mbps, 625 Mbps atau bahkan lebih. Faktor yang menjadi pengaruh design dan performa jaringan ini ada pada siklus komunikasi semacam jaringan telepon atau satelit (Melwin Syafrizal, 2005).

2.2 Topologi Jaringan

2.2.1 Topologi Bus

Topologi bus adalah topologi jaringan dimana semua perangkat dalam jaringan terhubung ke satu kabel atau jalur. Dengan bahasa lain Topologi bus adalah sebuah topologi yang media transmisinya menggunakan kabel tunggal atau kabel pusat yang menggabungkan client dan server (Kweldju, 2023)

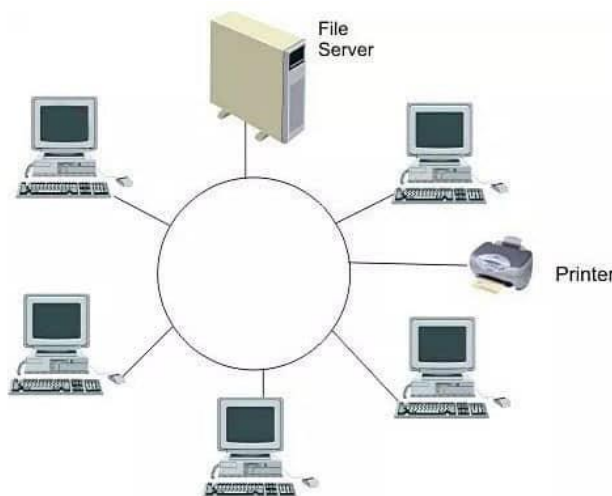


Gambar 1 topologi bus

Sumber: <https://diengcyber.com/mengenal-lebih-dalam-tentang-topologi-bus/>

2.2.2 Topologi Ring

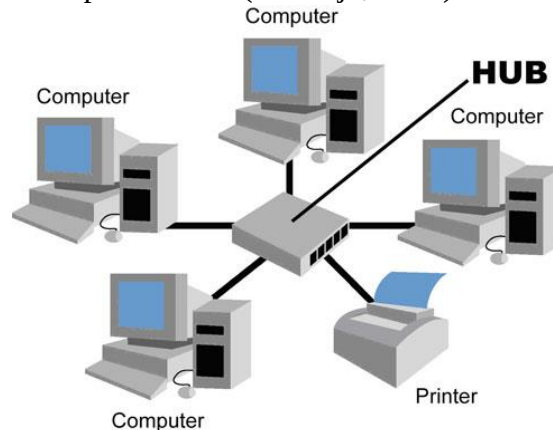
Topologi Ring adalah salah satu jenis topologi jaringan komputer dimana setiap perangkat (Node) terhubung satu sama lain membentuk lingkaran (ring). Dalam topologi ini, setiap node terhubung dengan dua node tetangga yaitu node sebelumnya dan node sesudahnya (Kweldju, 2023)



Gambar 2 topologi ring
Sumber: <https://lamanit.com/topologi-ring/>

2.2.3 Topologi Star

Topologi bintang adalah jenis topologi jaringan di mana semua perangkat dalam jaringan terhubung ke hub atau switch pusat. Setiap perangkat terhubung ke hub dengan koneksi point-to-point, menciptakan struktur seperti bintang. Dalam topologi ini, jika satu perangkat gagal atau mengalami masalah, itu tidak mempengaruhi jaringan lainnya. Ini menjadikannya topologi yang andal dan toleran terhadap kesalahan (Kweldju, 2023).

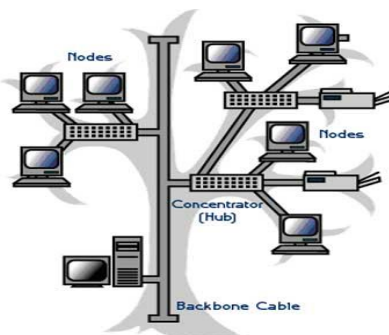


Gambar 3 topologi star

Sumber: <https://kumparan.com/kabar-harian/topologi-star-pengertian-ciri-ciri-kelebihan-dan-kekurangannya-1xZDymY5xJ4>

2.2.4 Topologi Tree

Topologi pohon adalah struktur jaringan di mana semua perangkat terhubung ke perangkat pusat yang disebut root atau switch. Dari root, cabang atau link dibuat untuk menghubungkan perangkat lain dalam struktur hierarkis. Topologi ini menyerupai struktur pohon, oleh karena itu dinamakan demikian. Dalam topologi pohon, setiap perangkat atau node hanya memiliki satu induk, kecuali root yang tidak memiliki induk. Node dapat memiliki beberapa anak atau cabang. Struktur hierarkis ini memungkinkan manajemen dan skalabilitas jaringan yang mudah (Kweldju, 2023).



Gambar 4 topologi tree

Sumber: <https://www.pinhome.id/blog/topologi-tree/>

2.3 Nirkabel (Wireless)

Nirkabel atau wireless pada mikrotik merujuk pada teknologi jaringan yang menghubungkan

Published by:

perangkat tanpa menggunakan kabel fisik. Dalam konteks mikrotik, nirkabel adalah kemampuan untuk menghubungkan perangkat mikrotik dengan perangkat lainnya melalui gelombang elektromagnetik, seperti jaringan Wi-Fi. Dengan menggunakan nirkabel pada mikrotik, pengguna dapat membuat jaringan lokal yang memungkinkan perangkat-perangkat seperti laptop, smartphone, dan printer untuk terhubung ke jaringan dan berkomunikasi satu sama lain. Nirkabel juga memungkinkan akses internet ke perangkat melalui modem atau router yang terhubung dengan jaringan wireless. Selain itu, nirkabel pada mikrotik juga memungkinkan penggunaan fitur-fitur khusus seperti Access Point (AP) untuk membuat hotspot Wi-Fi, Repeater untuk memperluas jangkauan jaringan, dan teknologi keamanan seperti enkripsi untuk melindungi data yang dikirimkan melalui jaringan nirkabel. Dalam pengaturan mikrotik, pengguna dapat mengkonfigurasi berbagai pengaturan nirkabel seperti mode operasi, frekuensi, jangkauan sinyal, pengaturan keamanan, dan banyak lagi. Pengguna juga dapat membatasi akses ke jaringan nirkabel dengan menggunakan fitur autentikasi dan pengelompokan perangkat dalam jaringan yang berbeda. Secara umum, nirkabel pada mikrotik dikenal sebagai solusi yang efisien dan fleksibel untuk menghubungkan perangkat secara tanpa kabel fisik, yang dapat digunakan dalam berbagai aplikasi seperti jaringan rumah, kantor, hotspot publik, dan skenario jaringan yang lebih kompleks (Samsumar & Hadi, 2018).

2.4 Hotspot

Hotspot pada MikroTik adalah fitur yang memungkinkan pengguna untuk membuat area akses internet nirkabel di lokasi tertentu. Dengan menggunakan hotspot, pengguna dapat mengontrol akses internet dengan memberikan username dan password kepada pengguna yang ingin terhubung ke jaringan nirkabel tersebut. Hotspot pada MikroTik mencakup berbagai fitur seperti autentikasi pengguna, penggunaan sistem voucher, kontrol bandwidth, pembatasan waktu akses, serta pembatasan akses untuk website yang tidak diinginkan. Fitur-fitur ini memungkinkan administrator jaringan untuk mengatur dan mengontrol penggunaan internet secara efektif. Selain itu, hotspot pada MikroTik juga mendukung autentikasi menggunakan metode seperti RADIUS Server, LDAP, dan FTP. Fitur-fitur ini memungkinkan administrator untuk mengintegrasikan hotspot MikroTik dengan sistem autentikasi yang sudah ada dalam infrastruktur jaringan yang ada. Adanya fitur hotspot pada MikroTik, pengguna dapat membuat area akses internet nirkabel dengan mudah dan mengontrol penggunaannya dengan lebih efisien (Khalaf et al., 2022).

2.5 Access Point

Access Point pada MikroTik adalah perangkat yang berfungsi sebagai titik akses atau jembatan antara perangkat-perangkat nirkabel dengan jaringan kabel. Access Point ini memungkinkan perangkat nirkabel seperti laptop, smartphone, atau tablet untuk terhubung ke jaringan kabel dan akses internet. MikroTik menawarkan beberapa jenis Access Point yang dapat digunakan, seperti perangkat hAP (home Access Point) yang dirancang untuk digunakan di rumah atau kantor kecil, dan perangkat CAP (capsman Access Point) yang dirancang untuk digunakan dalam jaringan yang lebih besar dengan lebih banyak Access Point. Access Point dari MikroTik memiliki fitur-fitur yang memungkinkan pengguna untuk mengatur dan mengontrol akses ke jaringan nirkabel, seperti pengaturan SSID (Service Set Identifier), keamanan jaringan dengan enkripsi seperti WPA/WPA2, pengaturan tingkat daya transmisi, pengaturan bandwidth, pengaturan antena, dan lain-lain. Dengan menggunakan Access Point pada MikroTik, pengguna dapat membuat jaringan nirkabel yang handal dan dapat diatur dengan baik. Access Point ini juga dapat diintegrasikan dengan fitur hotspot atau sistem autentikasi lainnya untuk mengontrol akses pengguna ke jaringan nirkabel dengan

lebih efisien (Khattak et al., 2022).

2.6 Mikrotik

Salah satu merek perangkat router dan jaringan yang didirikan oleh John Trully pada tahun 1996. MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang digunakan untuk mengelola dan mengoperasikan perangkat MikroTik. MikroTik RouterOS dapat digunakan untuk mengkonfigurasi perangkat jaringan seperti router, switch, wireless access point, jaringan virtual private network (VPN), dan banyak lagi. Perangkat MikroTik banyak digunakan untuk membangun jaringan lokal (LAN) dan jaringan area luas (WAN) dengan kinerja yang cepat dan handal. MikroTik juga dikenal dengan fitur-fiturnya yang lengkap dan harga yang terjangkau, sehingga banyak digunakan oleh perusahaan kecil dan menengah, serta oleh penyedia layanan internet (ISP) (Towidjojo, 2019).

2.6.1 Jenis-Jenis Mikrotik

a) Mikrotik RouterOS

MikroTik RouterOS adalah sistem operasi router yang dikembangkan oleh perusahaan MikroTik. Ini adalah sistem operasi berbasis Linux yang dirancang khusus untuk penggunaan pada perangkat jaringan seperti *router*, *switch*, dan *access point*. RouterOS memiliki fitur lengkap dan menyediakan berbagai fungsi, termasuk routing, firewall, manajemen akses, kontrol bandwidth, jaringan virtual, dan banyak lagi. MikroTik RouterOS sangat populer di kalangan administrator jaringan karena kemampuannya yang kuat dan fleksibel dalam mengelola jaringan (Towidjojo, 2019).

b) Mikrotik RouterBoard

Mikrotik RouterBoard adalah serangkaian perangkat keras (hardware) yang dikembangkan oleh perusahaan MikroTik. RouterBoard ini merupakan router dan switch berbasis Linux yang menggunakan sistem operasi RouterOS yang dikembangkan oleh MikroTik. RouterBoard ini digunakan untuk mengatur lalu lintas jaringan komputer atau membangun jaringan komputer skala kecil hingga besar. RouterBoard ini memiliki berbagai fitur yang lengkap dan dapat dikonfigurasi sesuai dengan kebutuhan pengguna (Towidjojo, 2019).

2.6.2 Fitur-Fitur mikrotik

a) Username Sistem

Username Sistem pada MikroTik adalah sebuah sistem yang memungkinkan pengguna untuk mengatur dan mengelola username dan password pengguna yang dapat mengakses MikroTik RouterOS. Dengan menggunakan username Sistem, admin dapat membuat dan mengelompokkan pengguna berdasarkan hak akses yang diberikan kepada mereka. Dalam *username Sistem*, admin dapat menentukan atribut-atribut pengguna seperti *profile*, *queue type*, *IP address*, dan sebagainya (Towidjojo, 2019).

b) Firewall

Firewall pada MikroTik adalah suatu fitur keamanan yang bertujuan untuk melindungi jaringan MikroTik dari serangan atau akses yang tidak sah. *Firewall* ini bekerja dengan memonitor dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan MikroTik. *Firewall* dapat mengatur kebijakan akses yang dibutuhkan, seperti memblokir atau membatasi akses dari jaringan eksternal ke jaringan internal, serta melindungi jaringan dari serangan yang ada di internet seperti serangan DDoS, Scanning, dan lain sebagainya. Dalam konfigurasi *firewall* pada MikroTik, pengguna dapat membuat aturan-aturan yang memungkinkan atau memblokir akses dari suatu alamat IP atau jaringan, protokol tertentu,

ports, dan lainnya. Hal ini memungkinkan administrator untuk mengontrol akses jaringan dengan tepat sesuai dengan kebutuhan dan kebijakan keamanan yang diinginkan (Towidjojo, 2019)

c) NAT

Network Address Translation (NAT) adalah proses mengubah alamat IP (Internet Protocol) dari satu jaringan ke jaringan lain. Pada Mikrotik, NAT digunakan untuk menghubungkan jaringan internal dengan jaringan eksternal (Internet). NAT dapat melakukan konversi IP address dan port pada paket data yang melewati router Mikrotik. Hal ini menjaga keamanan dan privasi jaringan internal, sambil memungkinkan host di jaringan internal untuk mengakses Internet (Towidjojo, 2019).

d) DHCP

Dynamic Host Configuration Protocol (DHCP) pada MikroTik adalah sebuah layanan yang digunakan untuk mengotomatiskan proses pemberian alamat IP kepada perangkat yang terhubung dengan jaringan komputer. DHCP pada MikroTik bertujuan untuk memudahkan administrasi jaringan dan menghindari konflik alamat IP. DHCP pada MikroTik bekerja dengan mengalokasikan dan mengatur alamat IP secara dinamis kepada perangkat dalam jaringan. Ketika sebuah perangkat terhubung ke jaringan, DHCP akan memberikan alamat IP yang tersedia secara otomatis kepada perangkat tersebut. Selain itu, DHCP juga dapat memberikan informasi tambahan seperti subnet mask, gateway, DNS, dan konfigurasi lainnya kepada perangkat yang terhubung. Penggunaan DHCP pada MikroTik dapat membantu mengelola dan mengontrol perangkat yang terhubung ke jaringan dengan efisien. Admin jaringan dapat mengatur konfigurasi DHCP pada MikroTik seperti rentang alamat IP yang tersedia, waktu sewa alamat IP (lease time), dan konfigurasi tambahan lainnya sesuai dengan kebutuhan jaringan (Towidjojo, 2019).

e) Simple Queue

Simple Queue pada MikroTik adalah sebuah fitur yang digunakan untuk mengatur dan mengontrol penggunaan bandwidth pada jaringan. Dengan menggunakan Simple Queue, administrator jaringan dapat menentukan batasan bandwidth yang akan digunakan oleh setiap klien atau pengguna dalam jaringan. Fitur ini sangat berguna untuk memastikan adanya pembagian bandwidth yang adil dan efisien, sehingga tidak ada satu pengguna pun yang mendominasi penggunaan bandwidth secara berlebihan (Towidjojo, 2019).

f) Captive Portal

Captive portal pada MikroTik adalah sebuah fitur yang memungkinkan Administrator jaringan untuk mengontrol akses Internet dengan menerapkan autentikasi pengguna melalui halaman login khusus sebelum pengguna dapat mengakses jaringan tersebut. Fitur ini sangat berguna dalam lingkungan hotspot atau jaringan publik, di mana Administrator dapat membatasi akses Internet hanya kepada pengguna yang memiliki akun atau sertifikat yang valid. Pengguna yang belum terautentikasi akan diarahkan ke halaman login, di mana mereka harus memasukkan informasi pengguna yang benar atau melakukan pembayaran tertentu untuk mendapatkan hak akses ke jaringan Wi-Fi. Hal ini memungkinkan Administrator untuk mengendalikan dan memonitor pengguna jaringan dengan lebih efektif (Towidjojo, 2019).

g) Radius

Radius pada mikrotik adalah sebuah protokol yang digunakan untuk otentikasi, otorisasi, dan akuntansi dalam jaringan komputer. Protokol ini memungkinkan administrator jaringan untuk mengontrol akses pengguna ke jaringan berdasarkan identitas pengguna. Radius juga mengumpulkan informasi tentang penggunaan jaringan, seperti durasi koneksi dan jumlah data yang ditransfer, untuk keperluan akuntansi dan pemantauan jaringan. Radius pada

mikrotik juga dapat diintegrasikan dengan layanan penggunaan jaringan yang ada, seperti server DHCP untuk pemberian alamat IP dinamis kepada pengguna yang sudah terotentikasi (Towidjojo, 2019).

h) Winbox

Salah satu aplikasi manajemen mikrotik yang digunakan untuk mengkonfigurasi dan mengelola perangkat mikrotik secara grafis. Aplikasi ini memungkinkan pengguna untuk melakukan berbagai tugas seperti mengatur pengaturan jaringan, mengontrol firewall, mengelola user dan password, serta melakukan pemantauan dan pemecahan masalah pada perangkat mikrotik. Dengan antarmuka yang sederhana dan intuitif, Winbox memudahkan pengguna dalam mengelola (Towidjojo, 2019).

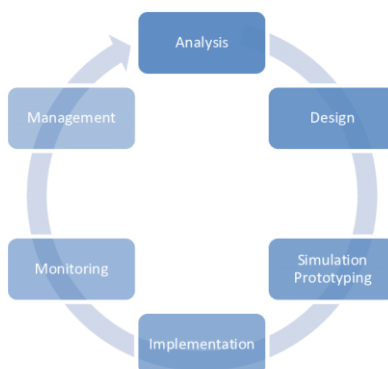
2.7 Visual Studio Code

Visual Studio Code adalah aplikasi editor teks gratis di kembangkan oleh *Microsoft* yang dapat digunakan di semua bahasa pemrograman yang ada tanpa perlu berganti aplikasi editor, serta dapat dijalankan di berbagai platform Operating Sistem (OS) seperti windows, linux, dan mac OS. *Visual*. Aplikasi ini berfungsi untuk pembuatan kode-kode program dibutuhkan sebuah aplikasi yang mumpuni. Dalam hal ini dapat menggunakan *Visual studio code*. *Visual StudioCode* adalah Software yang sangat ringan, namun kuat editor kode sumbernya yang berjalan dari desktop. Muncul dengan built-in dukungan untuk JavaScript, naskah dan Node.js dan memiliki array beragam ekstensi yang tersedia untuk bahasa lain, termasuk C++, C#, Python, dan PHP (Hartati, 2020).

2.8 Chrome

Google Chrome adalah sebuah aplikasi peramban yang digunakan untuk menjelajah dunia maya seperti halnya Firefox, Opera ataupun Microsoft Edge. Jika Firefox dikembangkan oleh Mozilla, Google Chrome dibuat dan dirancang oleh Google, perusahaan internet terbesar di dunia yang juga mempunyai android. Web Browser digunakan untuk menampilkan hasil website yang telah dibuat. Web browser yang paling sering digunakan diantaranya adalah, Mozilla Firefox, Google Chrome dan Safari (Abdulghani & Gozali, 2020).

2.9 Metode NDLC



Gambar 5 metode ndlc (network depelovment life cycle)

Sumber: https://www.researchgate.net/figure/Network-Development-Life-Cycle-NDLC_fig2_338847820

Tahapan Metode NDLC

a) Analysis

Tahap analisis melibatkan pengumpulan data lebih lanjut dan pengidentifikasian masalah

Published by:

atau kekurangan dalam infrastruktur jaringan yang ada. Analisis ini merupakan langkah penting untuk memahami keinginan dan kebutuhan pengguna jaringan (Lusi & Belutowe, 2023).

b) *Design*

Tahap desain melibatkan merancang blueprints atau rencana rinci untuk jaringan komputer yang akan dikembangkan. Pada tahap ini, dilakukan perencanaan perangkat keras, perangkat lunak, arsitektur jaringan, dan konfigurasi jaringan yang spesifik (Lusi & Belutowe, 2023).

c) *Simulation Prototype*

Tahap perencanaan melibatkan analisis kebutuhan jaringan komputer, penentuan tujuan, estimasi biaya, dan perencanaan sumber daya yang diperlukan. Pada tahap ini, dianalisis juga faktor-faktor keamanan dan kebutuhan kapasitas jaringan (Lusi & Belutowe, 2023).

d) *Implementasi*

Tahap implementasi melibatkan pembangunan infrastruktur jaringan yang telah dirancang, termasuk instalasi perangkat keras dan perangkat lunak, serta pengaturan konfigurasi dan pengujian jaringan (Lusi & Belutowe, 2023).

e) *Monitoring*

Tahap operasi melibatkan menjalankan, mengelola, dan memelihara jaringan yang telah dikembangkan. Ini mencakup pemantauan, pemecahan masalah, pembaruan perangkat lunak, dan tindakan preventif lainnya untuk menjaga keandalan dan keamanan jaringan (Lusi & Belutowe, 2023).

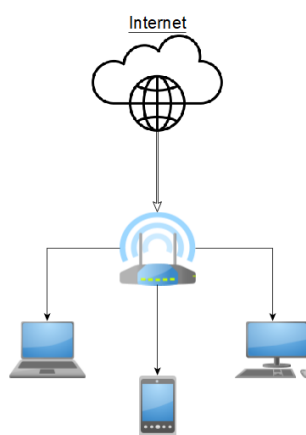
f) *Management*

Tahap ini melibatkan peninjauan berkala terhadap jaringan yang ada untuk mengevaluasi kinerja dan menemukan cara-cara untuk meningkatkannya. Jika diperlukan, pembaruan atau peningkatan dapat diterapkan untuk meningkatkan efisiensi atau memenuhi kebutuhan baru (Lusi & Belutowe, 2023).

3. Metode Penelitian

3.1 Analisis Sistem

3.1.1 Analisis Topologi Jaringan

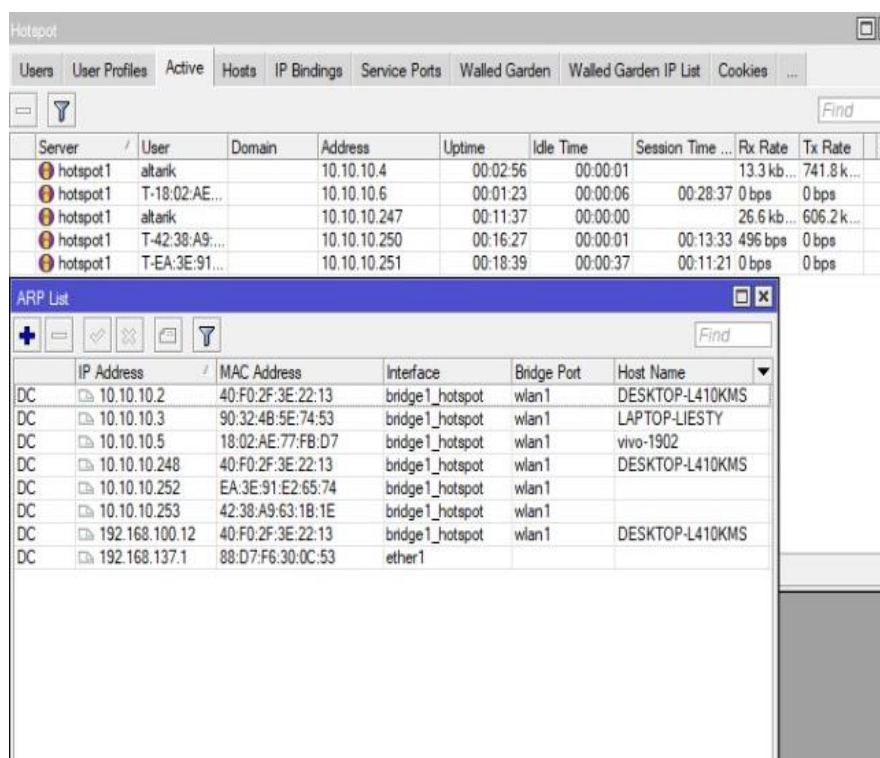


Gambar 6 topologi jaringan

Pada gambar topologi diatas adalah topologi jaringan pada Kantor dimana semua *end device user* terhubung ke access point secara wireless. Pada topologi diatas belum terdapat Sistem pembagian bandwidth dan Sistem autentikasi yang dilakukan oleh router. Pada saat ramai pengguna satu access point menampung 25 lebih perangkat yang terdeteksi. Pada saat tersebut modem dipaksa untuk bekerja keras sehingga modem sering panas, sehingga kecepatan internet cenderung kurang stabil.

3.1.2 Analisis Kelemahan Jaringan

Dari hasil pengamatan langsung yang dilakukan oleh peneliti ditemukan beberapa kekurangan dari segi keamanan dan pengelolaan bandwidth yang terdapat pada jaringan hotspot di Kantor PT.Nusindo Rekatama Semesta, diantaranya adalah belum adanya sistem pembagian bandwidth yang belum merata pada setiap user yang terkoneksi, dan masih ditemukannya IP Address yang terkoneksi bukan dari user kantor.



Server	User	Domain	Address	Uptime	Idle Time	Session Time	Rx Rate	Tx Rate
hotspot1	altank		10.10.10.4	00:02:56	00:00:01		13.3 kb...	741.8 k...
hotspot1	T-18:02:AE...		10.10.10.6	00:01:23	00:00:06	00:28:37	0 bps	0 bps
hotspot1	altank		10.10.10.247	00:11:37	00:00:00		26.6 kb...	606.2 k...
hotspot1	T-42:38:A9...		10.10.10.250	00:16:27	00:00:01	00:13:33	496 bps	0 bps
hotspot1	T-EA:3E:91...		10.10.10.251	00:18:39	00:00:37	00:11:21	0 bps	0 bps

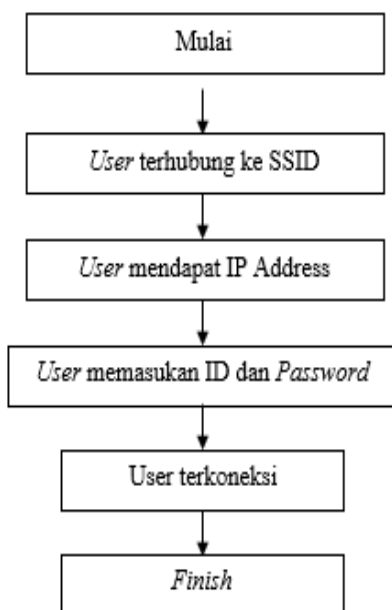
	IP Address	MAC Address	Interface	Bridge Port	Host Name
DC	10.10.10.2	40:F0:2F:3E:22:13	bridge1_hotspot	wlan1	DESKTOP-L410KMS
DC	10.10.10.3	90:32:4B:5E:74:53	bridge1_hotspot	wlan1	LAPTOP-LIESTY
DC	10.10.10.5	18:02:AE:77:FB:D7	bridge1_hotspot	wlan1	vivo-1902
DC	10.10.10.248	40:F0:2F:3E:22:13	bridge1_hotspot	wlan1	DESKTOP-L410KMS
DC	10.10.10.252	EA:3E:91:E2:65:74	bridge1_hotspot	wlan1	
DC	10.10.10.253	42:38:A9:63:1B:1E	bridge1_hotspot	wlan1	
DC	192.168.100.12	40:F0:2F:3E:22:13	bridge1_hotspot	wlan1	DESKTOP-L410KMS
DC	192.168.137.1	88:D7:F6:30:0C:53	ether1		

Gambar 7 Bukti IP yang terdeteksi pada mikrotik

3.1.3 Analisis Performa Sistem

Hasil analisis performa Sistem jaringan wireless pada Kantor PT.Nusindo Rekatama Semesta diperoleh data latency, jitter, dan packet loss menggunakan tools pada situs.

3.2 Analisis Jaringan Awal



Gambar 8 alur penelitian

- Pertama, *user* mulai menyalakan *wi-fi* adapter, kemudian *user* mencari SSID access point yang ada di Kantor PT.Nusindo Rekatama Semesta.
- Kedua, *user* berhasil menemukan SSID Kantor PT.Nusindo Rekatama Semesta.
- Ketiga, *user* mencoba melakukan test koneksi ke SSID.
- Keempat, *user* memasukkan *username* dan *password* masing masing yang diberikan oleh Admin IT.
- Kelima, setelah *username* dan *password* sesuai (benar) maka secara otomatis *user* mendapatkan IP Address dalam bentuk dhcp dari access point yang ada di Kantor PT.Nusindo Rekatama Semesta.
- Keenam, *user* berhasil terkoneksi ke access point pada Kantor PT.Nusindo Rekatama Semesta, dan mendapat akses Internet.

3.3 Alur Penelitian

Pada penelitian ini menggunakan perangkat hardware dan software meliputi:

Tabel 1 nama perangkat hardware dan perangkat software

No	Nama Perangkat Hardware
1	Router Mikrotik hap series RB941-200-2 ND
2	Kabel UTP
3	Laptop Lenovo Fx553v
No	Nama Perangkat Software
1	Winbox
2	Google Chrome
3	Visual Studio Code

4. Hasil dan Pembahasan

4.1 Implementasi

Pada tahap ini, teamwork akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

4.2 Konfigurasi Interface Sistem Mikrotik

4.2.1 Konfigurasi Winbox

Login Interface Mikrotik.

4.2.2 Konfigurasi Interface Mikrotik

Konfigurasi *Interface* berupa pergantian nama *Interface* yang digunakan agar memudahkan untuk membedakan *Interface* mana yang digunakan untuk menyalurkan ke ISP dan *Interface* mana yang mengarahkan ke *Hotspot*.

4.2.3 Konfigurasi WLAN Interface

Buka menu *Interface* lalu *wlan1* lalu buka *tab wireless*, aktifkan *wlan1* lalu kemudian isikan mode dengan *ap-bridge* dan isikan SSID dengan *hotspot* yang akan dibuat.

4.2.4 Konfigurasi IP Address

Untuk konfigurasi IP *Address*, pilih **IP** lalu *Address*, kemudian isikan IP *Address* pada *interface* yang akan dibuat. Pada tahap ini digunakan IP yaitu (10.10.10.1/24) disini penulis membuat IP sendiri tidak sama dengan IP modem . Untuk *interface* yang terhubung adalah *wlan1 Hotspot*, dan untuk ether1-ISP tidak dilakukan konfigurasi karena hanya akan digunakan sebagai jalur gateway internet.

4.2.5 Konfigurasi DHCP Client

DHCP memiliki fungsi utama mendistribusikan IP *Address* secara otomatis kepada setiap client yang terhubung dengan jaringan komputer. DHCP akan memberikan kemudahan bagi seorang network administrator dalam mengelola jaringan komputer, karena alokasi IP *Address* dapat di tentukan secara otomatis dan dalam satu kali kerja. untuk membuat DHCP Client buka IP lalu pilih DHCP Client pilih tanda (+) bagian *interface* pilih ether1 karena penulis menyambungkan kabel LAN ke ether1 lalu pilih OK dan terbaca IP *Address* modem dan tunggu status hingga(Bound).

4.2.6 Konfigurasi Hotspot Mikrotik

Hotspot Gateway merupakan salah satu fitur yang tersedia pada mikrotik yang berfungsi sebagai Sistem untuk memberikan fitur autentikasi pada *user* yang akan menggunakan jaringan. Jadi untuk bias akses ke jaringan, *user* diharuskan memasukan *username* dan *password* pada login page yang disediakan. Untuk membuat hotspot maka buka menu IP lalu *Hotspot* lalu *server* untuk membuat *hotspot*, pilih pada tab wizard *Hotspot setup* kemudian pada kolom option *hotspot interface* pilih wlan 1, klik next.

Lalu pada kolom local Address of Network isikan IP dari wlan1 yang akan dipakai, disini penulis menggunakan IP : 10.10.10.1/24 dan centang pada bagian *Masquerade Network*, lalu klik next *Masquerade Network* adalah sebuah metode yang mengizinkan dan memperbolehkan IP Private untuk terkoneksi ke Internet dengan menggunakan bantuan IP *public*.

Kemudian menentukan range IP address yang akan diberikan ke user (DHCP Server). Setiap

user akan diberikan IP secara otomatis oleh DHCP server antara range IP tersebut.

Selanjutnya adalah mengisi kolom SSL certificate. Pada option ini pilih none karena tidak menggunakannya, klik next.

Setelah itu, lalu mengisi IP Address untuk SMTP Server, apabila tidak menggunakan kosongkan, klik next.

Kemudian selanjutnya, isikan DNS Server yang akan digunakan, penulis mengisi DNS Server yaitu IP : 192.168.1.1

Lalu masukan ke kolom DNS Name, Pada kolom ini bias disikan dengan DNS Name secara bebas, boleh tidak. DNS Name ini digunakan untuk membuat sebuah pintasan alamat URL, yang nantinya dapat digunakan untuk mengakses halaman admin mikrotik.

Pada kolom ini digunakan DNS Name : (nusindo.co.id)

Setelah itu, memasukan ID dan name of local hotspot User yang akan digunakan, dapat dilihat pada gambar 4.14 dibawah ini digunakan “admin” sebagai user dan “admin” sebagai password, lalu klik next.

4.2.7 Konfigurasi User

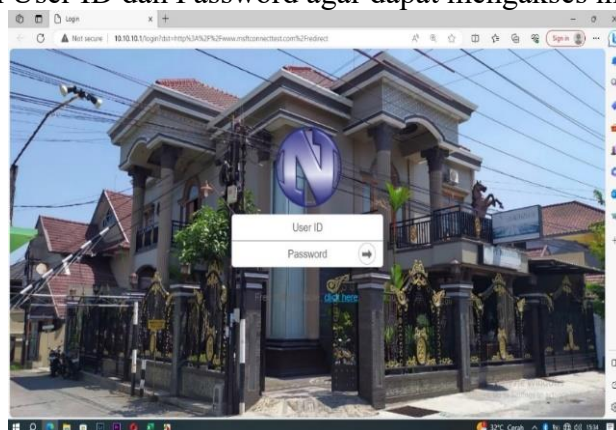
Setting mikrotik hotspot pilih bagian user lalu tanda (+) bagian name sesuaikan dengan username yang ada di PT.Nusindo Rekatama Semesta dan membuat password sesuai yang diinginkan oleh user untuk bagian server pilih All lalu klik OK.

4.2.8 Konfigurasi User Profile

User Profile digunakan untuk memberikan kebijakan pada username yang telah kita buat. Untuk konfigurasi pilih menu lalu IP next Hotspot dan pilih tab User Profile.

4.2.9 Tampilan Halaman Login Hotspot

Konsep Captive Portal adalah user mengizinkan untuk terhubung ke Access Point untuk mendapatkan alamat IP, saat user sudah terhubung maka Sistem akan mengarahkan ke halaman login untuk memasukan User ID dan Password agar dapat mengakses internet.



Gambar 9 Tampilan Halaman Login Hostpot

4.3 Pengujian Keseluruhan Sistem

Dari tahap implementasi yang telah dilakukan, maka dilakukan sebuah pengujian. Dimana pengujian ini didasarkan pada point monitoring di metode NDLC. Monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan dengan baik dan

Published by:

sesuai dengan tujuannya. Tahap monitoring juga dapat menjadi fasilitas pengumpulan data apabila Sistem yang telah dibangun tersebut masih memiliki kelemahan atau gagal dalam mengaksesnya

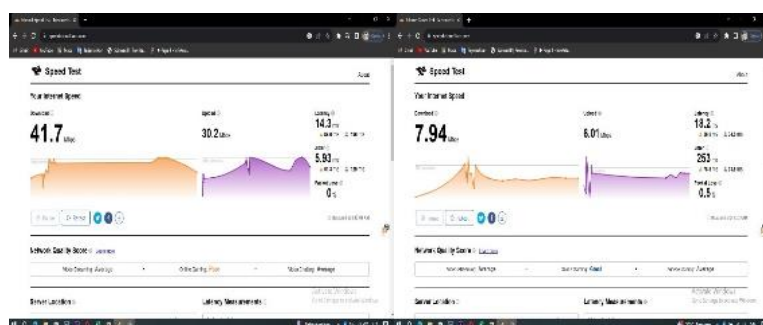
4.3.1 Pengujian terhadap Access Point Wireless

Sebuah device yang menangkap atau mendapatkan internet access dari hotspot. Dimana device tersebut mendapatkan IP Address 10.10.10.249 yang terdapat pada router mikrotik dengan interface 192.168.137.103. Pada saat ada user ingin mencoba mengakses internet pada browser maka otomatis muncul pop-up home page login, yang mana user harus memasukan username dan password terlebih dahulu. Setelah user melakukan login access dengan memasukan username dan password maka halaman otomatis ter-redirect ke halaman google. Apabila user salah memasukan username atau password akan muncul peringatan. Ketika user salah memasukan username atau password maka secara otomatis refresh dihome page dan muncul peringatan Invalid username/password.

4.3.2 Pengujian Limitasi Bandwith

Hasil performa Sistem jaringan wireless pada PT.Nusindo Rekatama Semesta sebelum membatasi jaringan internet agar merata kepada setiap user yang mengakses internet.

Berdasarkan queue yang telah dikonfigurasi sebelumnya, maka akan dilakukan pengujian kecepatan internet pada user profile seperti berikut:



Gambar 10 Sebelum dan Sesudah Limitasi Bandwidth

4.3.3 Pengujian Performa QOS Jaringan

Pengujian Performa QOS Jaringan Pengujian QoS jaringan menggunakan 3 sampel user dalam menilai parameter QoS yaitu *Packet Loss*, *Latency*, dan *Jitter* dan yang dirata-rata selama 4 hari dengan salah satu tools performa QoS pada situs (<https://speed.cloudflare.com/>) dan akan dibandingkan saat sebelum konfigurasi jaringan yang masih menggunakan modem dan setelah konfigurasi jaringan yang baru dengan yang sudah menggunakan router Mikrotik.

4.3.4 Pengujian Latency

Latency merupakan kondisi tertundanya atau terlambatnya suatu paket data tiba di tujuan atau dapat dengan kata lain berapa banyak waktu yang paket data untuk tiba dari satu titik yang ditunjuk ke titik yang dibutuhkan lain, Latency dinyatakan dengan satuan ms yang berarti miliseconds. Pada penelitian ini nilai latency menunjukkan adanya nilai perubahan di bagian sesudah konfigurasi dibandingkan sebelum konfigurasi.

4.3.5 Pengujian Jitter

Published by:

Jitter merupakan variasi latency antara paket yang terjadi pada jaringan Naik berbasis IP yang berarti perbedaan antara hasil latency minimal dan maksimum dalam tes ping. Satuan dalam jitter adalah ms yang berarti miliseconds. Pada penelitian ini nilai jitter pada device sebelum konfigurasi bernilai 130,14 ms dan sesudah konfigurasi bernilai 64,702 ms artinya berkualitas “bagus” menurut standarisasi TIPHON.

4.3.6 Pengujian Packet Lost

Packet Lost adalah banyaknya jumlah paket data yang hilang selama proses transmisi data dari sumber ke tujuan. Satuan Packet Lost yang digunakan adalah persen (%). Berikut data perbandingan Packet Lost sebelum dan sesudah konfigurasi. Pada hasil penelitian ini diatas nilai Packet Lost pada device ada kenaikan menjadi 2,66% karena saat pengujian sesudah konfigurasi kantor sedang ramai karyawan.

4.4 Analisis dan Pembahasan Sistem

Perancangan Jaringan ini menggunakan Mikrotik hAP series RB941-200-2ND memakai sistem operasi RouterOS versi 6.40. Jaringan yang dirancang menggunakan Mikrotik RouterOS berfungsi untuk manajemen akses internet pada jaringan hotspot di PT.Nusindo Rekatama Semesta serta untuk membatasi akses user baik dalam penggunaan bandwidth dan sebagainya. Hasil pengujian rancangan Router Mikrotik berupa keamanan jaringan dan limitasi bandwidth yang terintegrasi dengan user manager yang sebelumnya telah diinstal. Pada jaringan hotspot setiap pengguna harus melakukan login terlebih dahulu melalui sistem Captive Portal yang mana tersematkan metode Authentication Login Hotspot didalamnya jika ingin melakukan akses internet. Dan untuk kecepatan akses internet dan besaran bandwidth yang digunakan oleh masing-masing user sudah ditentukan berdasarkan pengaturan pada router Mikrotik yang terpasang.

4.5 Tahap Management

Tahap Management Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (policy). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga.

4.6. Monitoring Bandwidth dan MRTG Graph

MRTG Graph berfungsi untuk monitoring bandwidth jaringan Mikrotik seperti melihat pemakaian bandwidth client per IP Address atau interface tertentu dalam bentuk grafik agar mempermudah mengetahui tahapan pemakaian bandwidth. Berikut ini adalah tahap membuat bandwidth manajemen mikrotik dan MRTG untuk monitoring bandwidth akses internet user:

- Masuk menu Queues -> klik tab Simple Queue, secara otomatis Simple Queue sudah muncul ketika user sudah connect pada internet mikrotik yang sudah diberikan. Simple Queue LAN inilah yang akan digunakan sebagai parent Queue untuk user.
- Selanjutnya buat konfigurasi untuk MRTG dari simple queue yang telah ada. Untuk konfigurasi masuk Tools->Graphing. Klik tanda(+) dan isikan pada simple queue wlan dan allow address: 0.0.0.0/0, kemudian klik OK.
- Untuk melihat Grafik pemakaian bandwidth jaringan internet. Buka web browser kemudian ketikkan alamat URL (<http://IP-Address-Mikrotik/graphs>)

5. Kesimpulan

Published by:

Dari penelitian dan pengujian sistem jaringan yang telah dibuat dapat ditarik kesimpulan yaitu Captive Portal Login pada PT. Nusindo Rekatama Semesta berhasil dilakukan, pengujian ini dapat diimplementasikan Di PT. Nusindo Rekatama Semesta. Implementasi yang berhasil yaitu pengguna yang tidak berkepentingan memiliki hak akses tidak dapat menggunakan internet secara langsung, dikarenakan tiap device user akan ter-redirect dahulu ke home page login sebelum melakukan konektivitas jaringan Wi-Fi PT.Nusindo Rekatama Semesta dengan memasukan username dan password terlebih dahulu. Pengaplikasian Mikrotik RouterOS sebagai router jaringan pada PT.Nusindo Rekatama Semesta yang mana router tersebut memiliki fitur dan tools yang dapat mengelola jaringan, Sehingga manajemen bandwidth dapat mengatasi ketidakstabilan koneksi jaringan wireless yang telah berhasil pengujian pada limitasi bandwidth. Berdasarkan manajemen bandwidth sesudah implementasi didapatkan hasil 4,327 Mbps untuk download, dari sebelumnya bandwidth download sebesar 25,89 Mbps dan untuk manajemen bandwidth upload sesudah pengujian didapatkan hasil 4,255 Mbps, dari sebelumnya bandwidth upload sebesar 10,278 Mbps.

Acknowledgments

Penelitian ini dapat berjalan dengan baik baik atas bantuan dari berbagai pihak, untuk itu peneliti mengucapkan terima kasih kepada PT. Nusindo Rekatama Semesta, Tim STIKes AMIKOM dan rekan-rekan yang telah membantu pada penelitian ini.

Referensi

- Abdulghani, T., & Gozali, M. M. H. (2020). Sistem Konsultasi dan Bimbingan Online Berbasis Web Menggunakan Webrtc (Studi Kasus : Fakultas Teknik Universitas Suryakencana). *Media Jurnal Informatika*, 11(2), 42. <https://doi.org/10.35194/mji.v11i2.1037>
- Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167(2020), 106984. <https://doi.org/10.1016/j.comnet.2019.106984>
- Hartati, S. (2020). Perancangan Sistem Informasi Inventaris Barang Pada Kantor Notaris Dan Ppat Ra Lia Kholila, Sh Menggunakan Visual Studio Code. *Jurnal Siskomti*, 3(2), 37–48. <https://www.ejournal.lembahdempo.ac.id/index.php/STMIK-SISKOMTI/article/view/123>
- Khalaf, O. I., Romero, C. A. T., Hassan, S., & Iqbal, M. T. (2022). Mitigating Hotspot Issues in Heterogeneous Wireless Sensor Networks. *Journal of Sensors*, 2022. <https://doi.org/10.1155/2022/7909472>
- Khattak, R. Y., Ahmed, Q., Shoaib, S., & Hafeez, M. (2022). Array Antenna for Wireless Access Points and Futuristic Healthcare Devices. *Electronics (Switzerland)*, 11(8), 1–10. <https://doi.org/10.3390/electronics11081226>
- Kweldju, A. De. (2023). *Buku Ajar Pengantar Ilmu Komputer* (Moh. Nasru). PT Nasya Expanding Management.
- Lusi, D., & Belutowe, Y. S. (2023). *BERBASIS MIKROTIK MENGGUNAKAN METODE NDLC (NETWORK DEVELOPMENT LIFE CYCLE) PADA KANTOR BALAI PELAKSANAAN JALAN NASIONAL NTT*. 7(1).
- Melwin Syafrizal. (2005). *Pengantar Jaringan Komputer*.
- Mohamed, A., Hamdan, M., Khan, S., Abdelaziz, A., Babiker, S. F., Imran, M., & Marsono, M. N. (2021). Software-defined networks for resource allocation in cloud computing: A survey.

Computer Networks, 195, 108151. <https://doi.org/10.1016/j.comnet.2021.108151>

Qintharah, Y. N., & Utami, F. L. (2023). Determinants on Environmental Disclosure Moderating by Integrated Corporate Governance (ATT). *Aptisi Transactions on Technopreneurship (ATT)*, 5(1Sp), 26–41. <https://doi.org/10.34306/att.v5i1sp.308>

Rismayadi, A. A., Adhirajasa, U., & Sanjaya, R. (2023). *IMPLEMENTASI HIERRARCHICAL TOKEN BUCKET (HTB) DENGAN METODE DYNAMIC QUEUE UNTUK*. 5(2).

Salam, R., & Kho, A. (2023). Pengaruh Manajemen Pemasaran Virtual Terhadap Produk UMKM. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 1(2), 198–207. <https://doi.org/10.34306/mentari.v1i2.272>

Samsumar, L. D., & Hadi, S. (2018). PENGEMBANGAN JARINGAN KOMPUTER NIRKABEL (WiFi) MENGGUNAKAN MIKROTIK ROUTER (STUDI KASUS PADA SMA PGRI AIKMEL). *METHODIKA: Jurnal Teknik Informatika dan Sistem Informasi*, 4(1), 1–9. <https://doi.org/10.46880/mtk.v4i1.59>

Savytri, A., & Ratri, D. (2023). *A Comprehensive Design Guide to Adaptive e-Learning System Based on VARK Learning Styles*. 3(2), 453–464.

Sidqi, T. O., Fitri, I., & Nathasia, N. D. (2021). Implementasi Manajemen Bandwith Menggunakan Metode Htb (Hierarchical Token Bucket) Pada Jaringan Mikrotik. *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 6(1), 132–138. <https://doi.org/10.29100/jupi.v6i1.1927>

Sofana, I. (2013). *Membangun Jaringan Komputer: Mudah Membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Window dan Linux*.

Syafroni, R. N. (2023). Field of Meaning Theory in Celebgram Endorsement Product Captions. *ADI Journal on Recent Innovation (AJRI)*, 4(2), 172–183. <https://doi.org/10.34306/ajri.v4i2.868>

Tahir, M., Aini, N., Cahyani, L., Wijaya, E. Y., & Afif, M. (2023). *TOP-DOWN (STUDI KASUS SMKN 3 BANGKALAN) COMPUTER NETWORK RECONSTRUCTION WITH TOP-DOWN METHOD (CASE STUDY OF SMKN 3 BANGKALAN)*. 8(1), 21–30.

Towidjojo, R. (2019). *MikroTik Kungfu Kitab 1 Edisi Revisi*.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>)

