

IMPLEMENTASI AUTENTIKASI LOGIN MENGGUNAKAN QR CODE PADA JARINGAN SETDA KAB LAMPUNG TENGAH

Gilang Mahendra Akbar¹, Sudarmaji², Mujito³.

¹²³Program Studi S1 Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro.

¹²³Jalan Gatot Subroto No. 100, Yosodadi, Metro Timur, Kota Metro,

¹gilangakbar2456@gmail.com, ²majidarma5022-@gmail.com, ³mujito@ummetro.ac.id.

Abstrak : Permasalahan utama dalam sistem jaringan instansi pemerintahan adalah keterbatasan dalam efisiensi dan keamanan proses autentikasi login. Penelitian ini bertujuan untuk mengimplementasikan sistem autentikasi login jaringan berbasis QR Code sebagai solusi yang praktis dan aman, khususnya pada lingkungan Sekretariat Daerah (SETDA) Lampung Tengah. Penelitian ini menggunakan metode Network Development Life Cycle (NDLC) yang terdiri dari tahap analisis, desain, simulasi prototipe, implementasi, evaluasi, dan dokumentasi. Sistem jaringan dirancang dengan membagi akses menjadi dua kategori pengguna, yaitu staf dan tamu, masing-masing dengan alokasi bandwidth 40 Mbps dan 10 Mbps. Autentikasi dilakukan melalui pemindaian QR Code tanpa perlu input manual username dan password. Untuk meningkatkan keamanan, diterapkan filtering MAC Address khusus pada jaringan staf, sehingga hanya perangkat terdaftar yang dapat terhubung. Hasil penelitian menunjukkan bahwa penggunaan QR Code mempercepat proses login dan mengurangi beban administrasi, sedangkan filtering MAC Address berhasil meningkatkan kontrol akses jaringan. Implementasi sistem ini dinilai efektif dalam mendukung operasional jaringan yang lebih efisien dan aman di lingkungan pemerintahan.

Kata kunci: Autentikasi jaringan; QR Code; NDLC; MAC Address

Abstract : The main problem in government agency network systems is the limited efficiency and security of the login authentication process. This research aims to implement a QR Code-based network login authentication system as a practical and secure solution, particularly within the Central Lampung Regional Secretariat (SETDA). This research uses the Network Development Life Cycle (NDLC) method, which consists of analysis, design, prototype simulation, implementation, evaluation, and documentation. The network system is designed by dividing access into two user categories: staff and guests, with bandwidth allocations of 40 Mbps and 10 Mbps, respectively. Authentication is performed by scanning a QR Code without requiring manual input of a username and password. To enhance security, MAC Address filtering is implemented specifically on the staff network, so that only registered devices can connect. The results show that the use of QR Codes speeds up the login process and reduces administrative burden, while MAC Address filtering successfully improves network access control. The implementation of this system is considered effective in supporting more efficient and secure network operations in government environments.

Keywords: Network authentication; QR code; NDLC; MAC address

PENDAHULUAN

Seiring dengan perkembangan teknologi, ilmu pengetahuan juga berkembang pesat, terutama dalam bidang teknologi informasi dan komunikasi. Internet, sebagai salah satu hasil perkembangan ilmu pengetahuan, telah menjadi bagian penting dari kehidupan masyarakat. Berdasarkan hasil wawancara dengan Ibu Rosaria Agustina, SE selaku Analis Kebijakan Ahli Muda Administrasi Pembangunan, diketahui bahwa Kantor Administrasi Pembangunan memiliki 3 ruangan, 5 unit PC, 3 laptop, dan 17 unit handphone, serta menggunakan layanan internet Indihome dengan kecepatan 50 Mbps. Meskipun kecepatan internet tersebut tergolong cukup memadai, masih terdapat kendala dalam konektivitas jaringan akibat Wi-Fi yang bersifat terbuka untuk umum (public), sehingga memungkinkan banyak pengguna di luar staf Administrasi Pembangunan untuk mengakses jaringan tersebut. Hal ini menyebabkan terjadinya pembagian bandwidth yang tidak merata, dan ketika terlalu banyak perangkat seperti komputer, laptop, dan smartphone terhubung secara bersamaan, koneksi internet menjadi lambat karena setiap perangkat hanya memperoleh sebagian kecil dari kapasitas yang tersedia. Untuk mengatasi permasalahan yang ada, maka diberikan solusi autentikasi login jaringan berbasis QR Code dengan menciptakan dua QR Code yang terhubung pada server hotspot kantor, yaitu QR Code untuk staf dengan bandwidth 40 Mbps dan QR Code untuk tamu dengan bandwidth 10 Mbps, serta menerapkan filtering MAC Address untuk membatasi pengguna (user) yang dapat login ke jaringan Wi-Fi Kantor Administrasi

Pembangunan. Berdasarkan penjelasan mengenai latar belakang dan perumusan masalah tersebut, maka tujuan dari penelitian ini adalah untuk memudahkan proses autentikasi login jaringan menggunakan QR.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Implementasi

Kumar dan Dhillon (2019: 90-105): salah satu keunggulan dari implementasi QR Code dalam jaringan adalah meningkatkan keamanan serta kenyamanan pengguna. Pengguna hanya perlu memindai kode QR untuk masuk ke dalam sistem jaringan, tanpa harus mengingat kata sandi yang kompleks. Ini juga mengurangi risiko serangan siber seperti phishing, karena proses autentikasi menggunakan kode unik yang terus berubah. Teknologi ini banyak diadopsi dalam sistem manajemen jaringan, akses Wi-Fi, dan aplikasi berbasis cloud untuk mengotentikasi pengguna.

Topologi Jaringan

Singh (2021 20-35): menjelaskan bahwa ada beberapa jenis topologi jaringan yang umum digunakan, yaitu topologi star, bus, ring, dan mesh. Masing-masing topologi memiliki kelebihan dan kekurangan. Topologi star, misalnya, memungkinkan perangkat terhubung ke satu perangkat pusat, sehingga jika satu koneksi putus, perangkat lain tetap dapat berfungsi. Namun, jika perangkat pusat mengalami kerusakan, seluruh jaringan dapat terpengaruh.

Login

Zhang (2020: 120-135): login berbasis QR Code memungkinkan pengguna untuk mengakses layanan tanpa perlu

memasukkan kata sandi secara manual. Proses ini meningkatkan pengalaman pengguna dengan menyediakan akses yang lebih cepat dan aman, karena QR Code mengandung informasi unik yang hanya berlaku untuk satu sesi login. Selain itu, metode ini mengurangi risiko serangan siber seperti phishing, karena kode yang digunakan selalu berubah dan tidak dapat diprediksi.

QR Code

Liu (2020: 150-165): QR Code memungkinkan pengguna untuk mengakses informasi atau layanan dengan hanya memindai kode tersebut menggunakan perangkat mobile. Ini sangat memudahkan proses seperti login ke sistem atau pembayaran tanpa harus memasukkan informasi secara manual. Penggunaan QR Code dalam autentikasi juga memberikan keamanan tambahan karena kode dapat dihasilkan secara dinamis dan berumur pendek, sehingga mengurangi risiko serangan siber.

Bandwidth

Joshi dan Patel (2019: 45-59): manajemen *bandwidth* penting untuk mengoptimalkan kinerja jaringan dalam organisasi, karena permintaan terhadap kapasitas jaringan semakin tinggi seiring dengan peningkatan perangkat yang terhubung dan data yang diakses. Dengan menerapkan manajemen bandwidth, administrator dapat membatasi atau mengalokasikan bandwidth secara adil kepada setiap pengguna atau aplikasi, sehingga mencegah beberapa pengguna menguasai seluruh kapasitas jaringan, yang dapat menyebabkan kinerja jaringan menurun.

Filtering

Sharma dan Gupta (2019: 110-125):

filtering sangat penting untuk menjaga keamanan jaringan dari ancaman eksternal seperti malware, serangan DDoS, atau akses tidak sah. Filtering konten juga sering digunakan dalam perusahaan atau institusi untuk membatasi akses pengguna ke situs web atau layanan yang dianggap tidak produktif atau berbahaya, seperti situs jejaring sosial atau platform streaming.

Mac Address

Yadav (2021: 140-155): *MAC Address* berperan penting dalam pengelolaan jaringan, terutama dalam jaringan berbasis Ethernet dan Wi-Fi. Alamat ini memungkinkan perangkat untuk saling berkomunikasi dan membantu dalam proses autentikasi saat terhubung ke jaringan. Selain itu, *MAC Address* digunakan dalam pengaturan akses kontrol dan filtering, yang memungkinkan administrator jaringan untuk mengizinkan atau memblokir perangkat tertentu berdasarkan alamat MAC-nya.

Mikhmon

Santoso (2020: 200-215): *Mikhmon* menawarkan berbagai fitur yang memudahkan administrasi jaringan, termasuk pengelolaan pengguna, pengaturan kuota, dan analisis statistik penggunaan. Selain itu, *Mikhmon* memungkinkan integrasi dengan sistem pembayaran, sehingga pengguna dapat melakukan pembayaran untuk akses internet dengan lebih mudah. Hal ini menjadikan *Mikhmon* sebagai solusi yang efisien bagi penyedia layanan yang ingin memberikan pengalaman pengguna yang lebih baik dan terorganisir.

Blackbox Testing

Kumar (2021: 120-135): Metode pengujian

ini sangat penting dalam memastikan bahwa perangkat lunak dapat memenuhi kebutuhan pengguna tanpa harus memahami kode sumber atau arsitektur sistem. *Blackbox* Testing memprioritaskan aspek fungsionalitas dan perilaku aplikasi dari sudut pandang pengguna. Sebagai contoh, teknik ini sering digunakan dalam pengujian aplikasi seperti sistem login, di mana penguji memvalidasi apakah sistem menerima atau menolak akses berdasarkan input yang diberikan.

Access Point

Gupta dan Sharma (2020: 78-92): menyatakan bahwa *Access Point* berperan penting dalam jaringan nirkabel karena memungkinkan pengguna untuk terhubung tanpa memerlukan kabel fisik. Dalam konteks lingkungan yang padat, AP sangat diperlukan untuk memberikan koneksi yang stabil dan handal kepada banyak pengguna. AP dapat dikelompokkan menjadi beberapa jenis, termasuk Standalone, Controller-Based, dan Mesh, yang masing-masing memiliki kelebihan dan kekurangan yang berbeda

NDLC

Mehta (2019: 75-90): NDLC memiliki beberapa tahapan utama, yaitu analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan pemeliharaan. Di fase analisis kebutuhan, semua persyaratan pengguna dan organisasi dikumpulkan untuk memastikan bahwa sistem yang dikembangkan memenuhi ekspektasi. Fase perancangan melibatkan pengembangan arsitektur jaringan, di mana pertimbangan seperti keamanan, kecepatan, dan kapasitas harus diperhatikan.

METODE

metode yang digunakan untuk merencanakan, mengembangkan, dan mengelola sistem jaringan dengan efisien. Metode ini mencakup berbagai tahap, mulai dari perencanaan awal hingga implementasi dan pemeliharaan sistem jaringan. Tahapan dalam metode ini, yaitu:

- a. Analisis (Analysis)
- b. Perancangan (Design)
- c. Simulasi (Simulation Prototyping)
- d. Implementasi (Implementation)
- e. Monitoring
- f. Management

HASIL DAN PEMBAHASAN

mengembangkan sistem keamanan jaringan hotspot berbasis Mikrotik yang dilengkapi fitur autentikasi pengguna dan manajemen bandwidth. Dalam implementasinya, digunakan perangkat keras Router Mikrotik dan perangkat lunak Winbox sebagai alat bantu konfigurasi jaringan. Sistem ini dibangun dan diuji menggunakan metode NDLC (Network Development Life Cycle) yang terdiri dari tujuh tahapan, yaitu: Analysis, Design, Simulation, Prototype, Implementation, Monitoring, dan Management.

Analisis

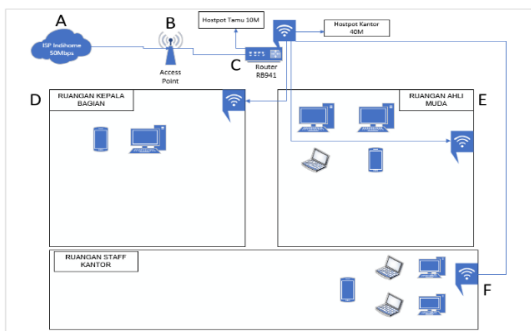


Gambar 1. Speed Test

Dilihat dari hasil analisis sistem jaringan yang ada pada kantor administrasi pembangunan. Dengan menggunakan provider indihome.

Design

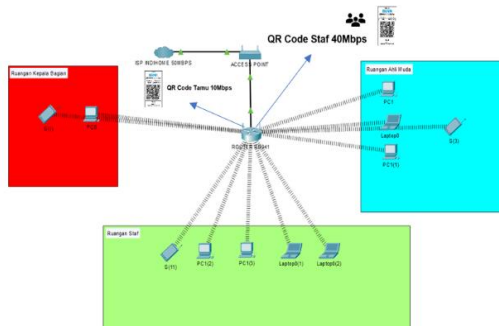
Dalam Perancangan topologi jaringan di Kantor Administrasi Pembangunan menggunakan topologi Star. Topologi Star adalah desain topologi jaringan computer yang akan penulis bangun nantinya. Karena topologi ini banyak digunakan diberbagai tempat dan mudah untuk menambah, mengurangi dan mendeteksi kerusakan jaringan yang ada.



Gambar 2. Topologi Star yang dibangun

Simulation

penulis akan melakukan simulasi dengan menggunakan Cisco Packet Tracer,



Gambar 6. Filtering Mac Address

Gambar 3. Simulasi Cisco Packet Tracer

Tujuannya adalah untuk menguji jaringan sebelum dibangun dan memahami cara kerja jaringan yang akan dirancang

Implementation

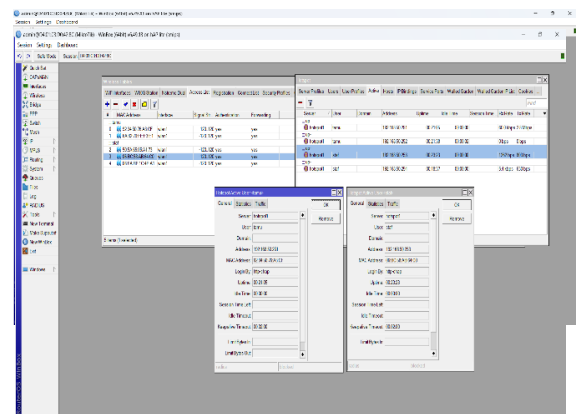
Pada tahap implementation ini ada beberapa konfigurasi yang akan kerjakan oleh penulis, diantaranya konfigurasi perancangan hotspot, *banwitdh*, *mac address*, dan pembuatan QR Code.



Gambar 4. Hasil Tampilan QR Code

Monitoring

Pada tahap ini penulis melakukan monitoring terhadap user yang menggunakan jaringan internet, apakah setiap user berhasil login menggunakan barcode yang telah dibuat dengan mikhmon.



Management

Filtering MAC Address diterapkan sebagai langkah pengamanan jaringan, dengan cara membatasi akses hanya untuk perangkat yang alamat MAC-nya terdaftar. Berdasarkan gambar tampilan Winbox, terlihat bahwa sistem hotspot aktif pada

server hotspot telah mencatat alamat MAC dari setiap pengguna yang terhubung. Misalnya, user staf dan tamu masing-masing memiliki alamat MAC unik yang terdaftar dan ditampilkan di tab Hotspot Active Users.

KESIMPULAN

Penulis menyimpulkan bahwa ditemukan kendala terhadap jaringan internet yang terdapat pada Kantor Administrasi Pembangunan, yaitu Wi-Fi masih bersifat terbuka (public), sehingga banyak perangkat yang bukan staf Administrasi Pembangunan bisa masuk ke Wi-Fi tersebut. Akibatnya, kecepatan internet menjadi lambat serta belum adanya konfigurasi jaringan seperti login autentikasi jaringan menggunakan QR Code, manajemen bandwidth dan filtering mac address. Untuk mengatasi permasalahan tersebut, solusi yang diterapkan adalah dengan membuat 2 sistem autentikasi login staf dan tamu menggunakan QR Code, setiap user profile mendapatkan kecepatan internet 40Mbps untuk staf dan 10Mbps untuk tamu,. Pengguna hanya perlu memindai QR Code untuk bisa terhubung ke jaringan, tanpa harus memasukkan username dan password secara manual. Selain itu, filtering MAC Address untuk membatasi perangkat yang tidak dikenal masuk ke jaringan, terutama pada jaringan staf.

REFERENSI

Kumar, R., & Dhillon, A. (2019). Meningkatkan keamanan jaringan dan kenyamanan pengguna melalui autentikasi kode QR. *Jurnal Sistem Jaringan Aman*, 11(3), 90-105.

Singh, R. (2021). Topologi jaringan umum: Star, bus, ring, dan mesh. *Journal of Computer Network Architecture*, 15(1), 20-

35.

Zhang, et al (2020). Autentikasi berbasis Kode QR: Meningkatkan keamanan dan pengalaman pengguna. *Jurnal Sistem Autentikasi Lanjutan*, 9(2), 120-135.

Liu, (2020). Autentikasi Kode QR: Menyederhanakan akses sekaligus meningkatkan keamanan. *Journal of Mobile Security*, 6(3), 150-165.

Joshi, P., & Patel, S. (2019). Manajemen bandwidth: Mengoptimalkan kinerja jaringan dalam organisasi. *Journal of Network Management*, 22(1), 45-59.

Sharma, R., & Gupta, A. (2019). Filtering: Meningkatkan keamanan dan produktivitas jaringan. *Journal of Network Security*, 13(2), 110-125.

Santoso (2020). Mikhmon: Solusi untuk administrasi jaringan dan integrasi pembayaran. *Jurnal Manajemen Jaringan dan Solusi Layanan*, 18(4), 200-215.

Singh, V. (2021). Pengujian Kotak Hitam: Memastikan fungsionalitas dari sudut pandang pengguna. *Jurnal Pengujian Perangkat Lunak dan Jaminan Kualitas*, 15(3), 120-135.

Gupta, P., & Sharma, K. (2020). Peran titik akses dalam jaringan nirkabel: Jenis dan fungsi. *Jurnal Sistem Komunikasi Nirkabel*, 18(2), 78 -92.

Mehta, A. (2019). Siklus Hidup Pengembangan Jaringan (NDLC): Tahapan dan pertimbangan utama. *Jurnal Rekayasa dan Pengembangan Jaringan*, 8(3), 75-90.