

ANALISIS DAN IMPLEMENTASI SEGMENTASI JARINGAN WIFI KARYAWAN DAN GUEST BERBASIS USERMAN PADA PT. INTERNETWORK KOMUNIKASI INDONESIA

Taufik Rahman, Lukman Hakim

Teknik Informatika, Universitas Bina Sarana Informatika
Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Senen, Jakarta Pusat, DKI Jakarta 10450
taufik@bsi.ac.id

ABSTRAK

Perkembangan teknologi jaringan nirkabel mendorong perusahaan untuk menyediakan akses WiFi yang fleksibel dan mudah diakses. Namun, tanpa pengelolaan yang baik, jaringan WiFi berpotensi menimbulkan risiko keamanan dan penurunan kinerja jaringan, terutama ketika akses karyawan dan tamu berada pada satu segmen jaringan yang sama. PT. Internetwork Komunikasi Indonesia menghadapi permasalahan berupa belum adanya pemisahan jaringan WiFi antara karyawan dan guest, sehingga berisiko terhadap keamanan data internal, sulitnya pengendalian akses pengguna, serta tidak optimalnya manajemen bandwidth. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan segmentasi jaringan WiFi karyawan dan guest berbasis User Manager (Userman) agar akses jaringan lebih aman, terkontrol, dan mudah dikelola. Metode penelitian yang digunakan adalah studi kasus dengan pendekatan deskriptif, melalui tahapan observasi, wawancara, dan studi pustaka. Implementasi dilakukan dengan konfigurasi VLAN untuk pemisahan jaringan serta autentikasi hotspot berbasis Userman pada perangkat MikroTik. Hasil penelitian menunjukkan bahwa penerapan segmentasi jaringan dan autentikasi Userman berhasil meningkatkan keamanan jaringan, mempermudah manajemen pengguna, serta mengoptimalkan penggunaan bandwidth antara jaringan karyawan dan guest.

Kata kunci : Segmentasi Jaringan, WiFi, User Manager, MikroTik, VLAN, Keamanan Jaringan.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi mendorong perusahaan untuk menyediakan layanan jaringan nirkabel (WiFi) sebagai sarana pendukung aktivitas operasional dan mobilitas kerja. Penggunaan WiFi di lingkungan perusahaan tidak hanya dimanfaatkan oleh karyawan, tetapi juga oleh pihak eksternal seperti tamu atau mitra kerja, sehingga menuntut adanya pengelolaan jaringan yang baik agar aspek keamanan, kinerja, dan keandalan jaringan tetap terjaga. PT. Internetwork Komunikasi Indonesia sebagai perusahaan yang bergerak di bidang teknologi informasi memiliki kebutuhan akses jaringan yang tinggi untuk mendukung aktivitas internal maupun akses sementara bagi tamu. Namun, penggunaan jaringan WiFi yang belum tersegmentasi secara optimal antara karyawan dan guest berpotensi menimbulkan risiko keamanan, seperti kebocoran data, penyalahgunaan akses, serta gangguan performa jaringan akibat penggunaan bandwidth yang tidak terkendali. Selain itu, pengelolaan autentikasi pengguna dan pembatasan bandwidth yang belum dilakukan secara terpusat menyebabkan sulitnya pengawasan dan pengendalian akses jaringan. Oleh karena itu, diperlukan suatu solusi yang mampu memisahkan akses jaringan WiFi antara karyawan dan guest secara terstruktur dan aman, salah satunya dengan memanfaatkan fitur User Manager (Userman) pada router MikroTik.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis kondisi jaringan WiFi yang berjalan di PT. Internetwork Komunikasi Indonesia serta mengimplementasikan segmentasi jaringan WiFi antara karyawan dan guest berbasis

User Manager (Userman). Implementasi ini diharapkan dapat meningkatkan keamanan jaringan melalui pemisahan akses pengguna, mengoptimalkan pengelolaan autentikasi, serta mengatur penggunaan bandwidth agar lebih adil dan stabil bagi setiap kategori pengguna.

WLAN menawarkan fleksibilitas dan mobilitas tinggi sebagai solusi jaringan organisasi, namun memerlukan pengamanan ketat karena sifat transmisinya yang terbuka berpotensi menimbulkan kebocoran data dan gangguan kinerja. [1].

Rencana penyelesaian masalah dalam penelitian ini dilakukan melalui beberapa tahapan, dimulai dari analisis kebutuhan dan permasalahan jaringan yang ada, perancangan topologi jaringan dengan segmentasi WiFi karyawan dan guest menggunakan VLAN atau subnet yang berbeda, implementasi sistem autentikasi dan manajemen pengguna menggunakan User Manager pada router MikroTik, konfigurasi kebijakan akses dan pembatasan bandwidth sesuai kategori pengguna, hingga tahap pengujian dan evaluasi untuk memastikan sistem segmentasi jaringan berjalan sesuai dengan tujuan yang telah ditetapkan.

2. TINJAUAN PUSTAKA

2.1. User Manager

Usermanager sebagai radius server meningkatkan keamanan serta mempermudah pengelolaan dan pemantauan pengguna jaringan [2].

2.2. VLAN

VLAN memfasilitasi pemisahan jaringan pada satu switch untuk meningkatkan keamanan, fleksibilitas, skalabilitas, dan kontrol broadcast. [3].

2.3. Jaringan Komputer

Jaringan komputer dapat diartikan sebagai suatu sistem yang terdiri atas sejumlah komputer dan perangkat jaringan lain yang saling terhubung serta bekerja bersama untuk mencapai tujuan tertentu.

2.4. Router

RouterOS merupakan sistem operasi independen yang menjadikan PC mampu berfungsi sebagai router, firewall, manajemen bandwidth, serta layanan jaringan lainnya. [4].



Gambar 1. RouterOs RB3011

2.5. Access Point

Access point merupakan perangkat jaringan yang memungkinkan terbentuknya Wireless Local Area Network (WLAN) sebagai bagian dari infrastruktur jaringan komputer"[5].



Gambar 2. Access Point

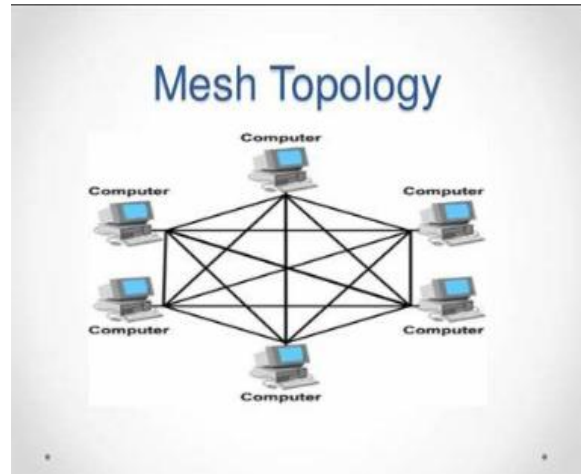
2.6. Kabel Utp

"Kabel UTP merupakan salah satu komponen utama jaringan komputer yang digunakan dalam pembangunan Local Area Network (LAN)" [6].

2.7. Switch

Hub atau switch berfungsi sebagai terminal pembagi sinyal data bagi kartu jaringan, dan apabila perangkat ini mengalami kerusakan, maka seluruh jaringan akan terganggu sehingga komunikasi antar komputer maupun dengan server tidak dapat berlangsung. [7].

2.8. Topologi Mesh



Gambar 3. Topologi Mesh

"Topologi mesh merupakan bentuk jaringan yang menghubungkan setiap perangkat secara langsung dengan perangkat lainnya." [8].

2.9. Penelitian Terkait

Penelitian ini menunjukkan bahwa kecepatan data pada profil dosen dan mahasiswa masih berada di bawah batas rate limit pada konfigurasi Mikrotik. Pemanfaatan Mikrotik server mampu meningkatkan keamanan melalui autentikasi, otorisasi, dan manajemen pengguna terpusat, sehingga mencegah akses ilegal sekaligus mempermudah pengelolaan jaringan bagi administrator[9]. Rancangan arsitektur jaringan komputer diuji melalui simulasi prototipe menggunakan Graphical Network Simulator 3 (GNS3), sehingga konfigurasi dan instalasi perangkat hotspot dapat dipastikan berjalan tanpa kesalahan sebelum penerapan di lapangan[10]. Penelitian ini menunjukkan bahwa penerapan usermanager di Universitas PGRI Semarang telah berjalan dengan baik dan dimanfaatkan untuk manajemen pengguna serta pembatasan bandwidth [11].

Penelitian ini menggunakan metode Network Development Life Cycle (NDLC) untuk merancang dan menguji sistem jaringan nirkabel berbasis Mikrotik di lingkungan restoran cepat saji dengan mengintegrasikan CAPsMAN, VLAN, Virtual Access Point (VAP), dan PCQ untuk pembagian bandwidth yang adil antara pengguna internal dan eksternal. Hasil penelitian menunjukkan bahwa konfigurasi segmentasi jaringan berbasis VLAN efektif membagi bandwidth dan menghindari konflik alamat IP serta dominasi trafik oleh kelompok tertentu, sehingga kinerja jaringan menjadi stabil dan optimal di area dengan banyak pengguna. Penelitian ini relevan dalam konteks segmentasi SSID dan alokasi sumber daya, namun lebih fokus pada manajemen bandwidth dibanding aspek autentikasi dan user-level manajemen yang digunakan pada User Manager[12].

Penelitian ini menggunakan metode eksperimental dengan platform Mikrotik RouterOS untuk mengimplementasikan VLAN dinamis pada jaringan kabel dan nirkabel. Tujuannya adalah

meningkatkan segmentasi, keamanan, dan skalabilitas jaringan dengan memungkinkan penambahan perangkat secara fleksibel. Hasilnya menunjukkan bahwa VLAN dinamis dapat memperluas jaringan tanpa penurunan performa dan mempermudah manajemen trafik. Gap yang terlihat adalah penelitian ini belum mengkombinasikan segmentasi dengan manajemen autentikasi pengguna seperti User Manager[13].

Penelitian ini memakai metode NDLC, terutama dalam tahap analisis, desain, dan simulasi prototyping, untuk membagi akses user melalui VLAN dan multi-SSID menggunakan CAPsMAN pada MikroTik. Hasilnya menunjukkan bahwa setiap VLAN memiliki SSID masing-masing, memudahkan monitoring dan manajemen akses wireless dengan template konfigurasi yang efisien. Penelitian ini sejalan dengan konsep segmentasi dan SSID berbeda, namun tidak menggunakan modul User Manager untuk autentikasi serta manajemen profil user secara terpusat[14]. Penelitian ini menggunakan metode Network Development Life Cycle (NDLC) untuk merancang hotspot WiFi sekolah dengan fitur User Manager pada MikroTik. Pengumpulan data dilakukan melalui observasi, wawancara, dokumentasi, dan studi pustaka. Hasilnya berhasil mengimplementasikan hotspot yang mencakup seluruh area madrasah tanpa gangguan jaringan. Fokus penelitian ini pada implementasi User Manager untuk autentikasi login pengakses wireless, menunjukkan manfaat autentikasi terpusat — namun belum mengevaluasi segmentasi jaringan untuk kelompok user yang berbeda seperti karyawan dan tamu[15].

Dengan pendekatan mendesain jaringan hotspot berbasis MikroTik dan autentikasi menggunakan User Manager, penelitian ini menunjukkan penerapan metode autentikasi login WiFi yang terstruktur di lingkungan sekolah-kejuruan. Hasil laporan menyatakan bahwa desain berhasil memfasilitasi autentikasi pengguna hotspot secara efektif. Walaupun fokusnya belum mencakup segmentasi jaringan WiFi berbasis role (misalnya guest vs internal), penelitian ini relevan dalam penggunaan User Manager untuk manajemen akses yang terorganisir, insight yang kuat untuk memperluas pada segmentasi jaringan perusahaan[16].

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dengan metode studi kasus, yang bertujuan untuk mendeskripsikan secara sistematis, faktual, dan akurat mengenai fakta-fakta dan karakteristik dari kondisi jaringan WiFi yang digunakan oleh karyawan dan tamu di PT. Internetwork Komunikasi Indonesia serta implementasi segmentasinya menggunakan teknologi Userman.

3.1. Teknik Pengumpulan Data

- a. Observasi
Melakukan pengamatan langsung terhadap kondisi jaringan WiFi yang ada di PT. Internetwork Komunikasi Indonesia. Observasi dilakukan untuk mengetahui topologi jaringan, konfigurasi perangkat jaringan, serta pola penggunaan akses WiFi oleh karyawan dan tamu. Melalui teknik ini, diperoleh gambaran nyata mengenai masalah dan kebutuhan sistem segmentasi jaringan.
- b. Wawancara
Wawancara dilakukan secara langsung dengan pihak yang berwenang dalam pengelolaan jaringan di perusahaan, seperti staf IT atau administrator jaringan. Tujuan wawancara ini adalah untuk menggali informasi mendalam mengenai kendala teknis, kebutuhan keamanan jaringan, serta harapan dari pihak perusahaan terhadap sistem segmentasi jaringan WiFi yang akan diterapkan.
- c. Studi Pustaka
Melakukan penelaahan terhadap literatur yang relevan, seperti buku, jurnal, artikel ilmiah, dokumentasi MikroTik, serta referensi lainnya yang berkaitan dengan konsep segmentasi jaringan, manajemen bandwidth, keamanan jaringan, dan teknologi Userman. Studi pustaka ini dilakukan untuk memperkuat dasar teori dan mendukung analisis dalam implementasi solusi yang diajukan.

3.2. Model Pengembangan Jaringan

Untuk menjawab permasalahan terkait tidak adanya segmentasi jaringan dan lemahnya pengelolaan akses WiFi di PT. Internetwork Komunikasi Indonesia, model pengembangan jaringan yang diusulkan adalah Segmentasi Jaringan WiFi Berbasis Teknologi Userman pada MikroTik. Model ini dirancang dengan pendekatan pengembangan jaringan terstruktur, yang mencakup tahapan sebagai berikut:

- a. Analisis Kebutuhan Jaringan
Melalui observasi dan wawancara, dilakukan identifikasi terhadap kebutuhan segmentasi antara pengguna internal (karyawan) dan eksternal (guest), meliputi:
 - Alokasi bandwidth yang adil.
 - b). Pembatasan akses terhadap sumber daya jaringan internal.
 - c). Pengelolaan autentikasi dan durasi akses untuk tamu.
- b. Perancangan Topologi Jaringan Tersegmentasi
Jaringan WiFi dirancang menggunakan dua SSID terpisah:
 - SSID Karyawan: Akses penuh ke sumber daya internal dengan profil Userman khusus.
 - SSID Guest: Akses terbatas hanya ke internet dengan pembatasan kecepatan, waktu, dan autentikasi login.

Perangkat MikroTik digunakan sebagai router utama yang mengatur manajemen pengguna menggunakan User Manager (Userman), dan VLAN digunakan bila diperlukan untuk pemisahan secara fisik/logis.

c. Implementasi Teknologi Userman

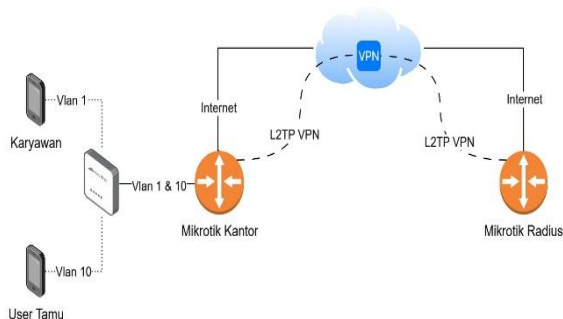
Tahapan ini mencakup:

- Konfigurasi Userman di MikroTik.
 - Pembuatan user profile untuk karyawan dan tamu.
 - Penetapan limitasi (bandwidth, time, quota) sesuai kebutuhan.
 - Pengaturan autentikasi login untuk tamu melalui hotspot captive portal.
- d. Pengujian Dan Evaluasi
- Setelah implementasi, dilakukan pengujian untuk mengukur efektivitas segmentasi, termasuk:
- Pengujian autentikasi pengguna.
 - Monitoring bandwidth dan penggunaan jaringan.
 - Uji coba pembatasan akses ke server internal dari jaringan tamu.
- e. Dokumentasi dan Pemeliharaan
- Seluruh konfigurasi dan hasil evaluasi didokumentasikan untuk dijadikan referensi dalam pemeliharaan dan pengembangan lebih lanjut. Model ini memungkinkan fleksibilitas dalam menambah kebijakan akses sesuai perkembangan kebutuhan perusahaan.

3.3. Topologi jaringan usulan

menggunakan topologi *star* (bintang) yang dimodifikasi untuk mendukung segmentasi logis dengan VLAN dan multiple SSID. Router MikroTik tetap digunakan sebagai pusat kendali jaringan (*core gateway*), dengan fitur Userman diaktifkan untuk:

- Mengelola autentikasi pengguna hotspot tamu (*guest*).
- Mengatur kecepatan dan waktu akses untuk tamu.
- Memberikan IP statis kepada perangkat karyawan melalui VLAN.



Sumber : Penelitian 2025

Gambar 1. Topologi Jaringan Usulan

Skema jaringan usulan dibuat berdasarkan simulasi dengan perangkat dan arsitektur nyata menggunakan *Cisco Paket Tracer* (untuk ilustrasi VLAN dan SSID secara logis). MikroTik RouterOS sebagai perangkat utama diimplementasikan pada perangkat nyata dalam uji coba.

Penjelasan Skema Usulan:

- a. Router MikroTik terhubung ke satu *Access Point* dengan SSID yang di *broadcast*:
 - SSID Karyawan → VLAN 1
 - SSID Guest → VLAN 10
- b. Router MikroTik terhubung ke satu *Access Point*, yang akan digunakan untuk membroadcast dua SSID (karyawan dan tamu).
- c. *Interface bridge* dibuat pada MikroTik untuk menggabungkan *interface* fisik yang terhubung ke *Access Point*.
- d. VLAN 1 dikonfigurasi pada *interface bridge* sebagai jaringan karyawan, dengan alokasi IP 172.168.100.1/24.
- e. VLAN 10 dikonfigurasi pada *interface bridge* sebagai jaringan tamu (*guest*), dengan alokasi IP 172.168.99.1/24.
- f. Segmentasi jaringan dilakukan menggunakan VLAN agar lalu lintas antara karyawan dan tamu dipisahkan secara logis.
- g. Setiap VLAN memiliki konfigurasi DHCP server terpisah agar alokasi IP berjalan otomatis sesuai segmentasinya.
- h. Dengan pemisahan ini, jaringan tamu tidak dapat mengakses jaringan internal karyawan, sehingga meningkatkan keamanan jaringan perusahaan.

4. HASIL DAN PEMBAHASAN

Untuk mewujudkan sistem jaringan yang telah dirancang, konfigurasi dilakukan pada perangkat MikroTik guna mengatur interface, IP address, VLAN, dan bridge secara terstruktur.

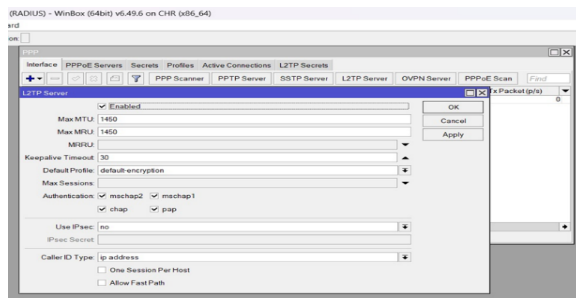


Sumber : Penelitian 2025

Gambar 2. Dashboard UserManager

Keterangan :

- UserManager Di akses melalui Ip yang dibuat pada Mikrotik sisi RADIUS.
- Pada dashboard UserManager terdapat beberapa extension untuk konfigurasi, *Router, Users, Session, Customers, Logs*, Dll.

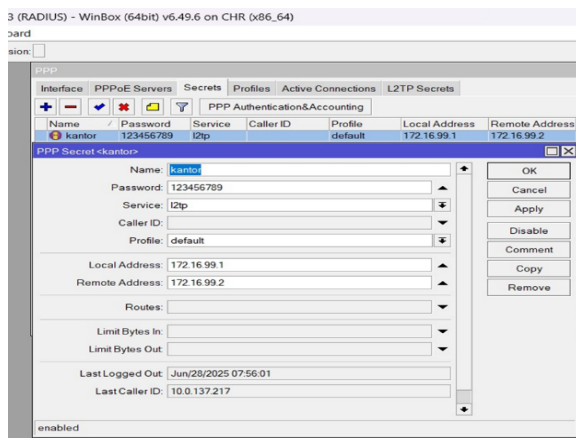


Sumber: penelitian 2025

Gambar 3. Konfigurasi L2TP Server Pada Mikrotik Sisi RADIUS

Keterangan :

- Pada layanan (PPP), *Interface*, L2TP Server centang pada bagian *Enabled* Untuk mengaktifkan service VPN L2TP.

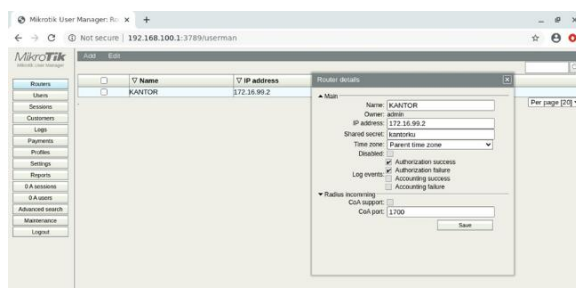


Sumber : Penelitian 2025

Gambar 4. Konfigurasi PPP Secret Pada Sisi Mikrotik RADIUS

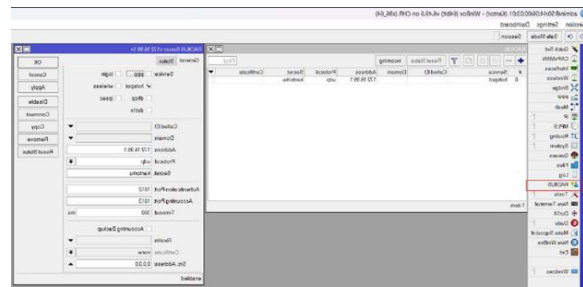
Keterangan :

- *Name*: Nama pengguna (*username*) yang digunakan untuk login.
- *Password*: Kata sandi untuk autentikasi.
- *Service*: Jenis layanan yang digunakan, misalnya l2tp, pptp, atau ovpn.
- *Profile*: Template pengaturan (*IP pool*, *DNS*, *routing*, dll) yang diterapkan untuk user.
- *Local Address*: IP yang digunakan router untuk sesi VPN.
- *Remote Address*: IP yang diberikan ke *client* VPN



Sumber: penelitian 2025

Gambar 5. Konfigurasi router pada sisi UserManager

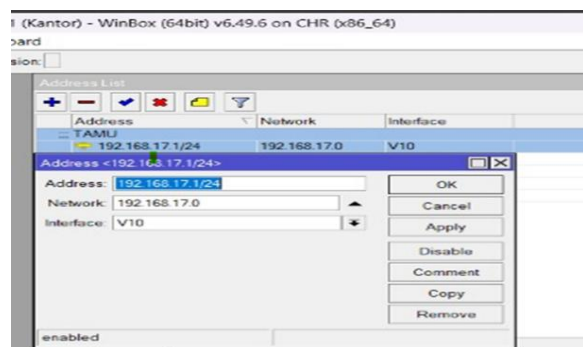


Sumber: penelitian 2025

Gambar 6. Konfigurasi RADIUS Pada Sisi Mikrotik Kantor

Keterangan :

- *Service hotspot* : Menandakan bahwa RADIUS digunakan untuk layanan hotspot (bukan PPP, login, wireless, dll).
- *Address 172.16.99.1* : Alamat IP dari server RADIUS yang akan digunakan oleh MikroTik untuk proses otentikasi.
- *Protocol udp* : Menandakan bahwa komunikasi antara MikroTik dan server RADIUS menggunakan protokol UDP.
- *Secret kantorku* : Kata sandi yang digunakan sebagai shared secret antara MikroTik dan server RADIUS. Ini harus sama dengan yang dikonfigurasi di sisi server RADIUS agar otentikasi berhasil.

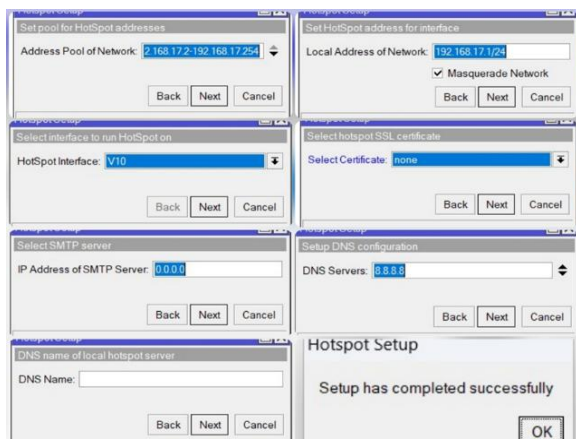


Sumber: penelitian 2025

Gambar 7. Konfigurasi pada layanan Ip Address

Keterangan :

- *Address: 192.168.17.1/24* – Merupakan alamat IP gateway untuk jaringan 192.168.17.0/24.
- *Network: 192.168.17.0* – Merupakan network ID dari subnet tersebut.
- *Interface: V10* – Interface fisik atau virtual tempat IP ini diikatkan. Bisa berupa VLAN atau bridge.
- Keterangan tambahan: IP ini digunakan untuk jaringan TAMU, yang berarti jaringan tamu atau *guest network*. Biasanya, jaringan tamu dipisahkan dari jaringan utama untuk alasan keamanan dan segmentasi lalu lintas.



Sumber: penelitian 2025

Gambar 8. Konfigurasi Hotspot Setup

Keterangan :

- *Set Pool for Hotspot Addresses (Address Pool of Network: 192.168.17.2–192.168.17.254)* : Rentang alamat IP yang akan diberikan secara otomatis (DHCP) kepada *client* yang terkoneksi ke Hotspot. IP ini berasal dari subnet 192.168.17.0/24
- *Set Hotspot Address for Interface (Local Address of Network: 192.168.17.1/24)* : Merupakan IP *gateway* dari router untuk jaringan ini.
- *Select Interface to Run Hotspot On (Hotspot Interface: V10)* : Hotspot akan dijalankan di *interface* V10, yang merupakan *interface* logis (misalnya VLAN atau *bridge*) tempat *client* tamu terhubung.
- *Select Hotspot SSL Certificate (Certificate: none)* : Tidak ada sertifikat SSL yang dipasang, sehingga halaman login hotspot akan menggunakan HTTP (bukan HTTPS). Cocok untuk lingkungan uji coba atau jaringan lokal sederhana.
- *Select SMTP Server (IP Address of SMTP Server: 0.0.0.0)* : Dilewati atau dikosongkan, karena tidak diperlukan konfigurasi pengiriman email melalui SMTP pada sistem hotspot ini
- *Setup DNS Configuration (DNS Servers: 8.8.8.8)* : Server DNS yang digunakan oleh *client* untuk menerjemahkan nama domain ke alamat IP. 8.8.8.8 adalah DNS publik milik Google.
- *DNS Name of Local Hotspot Server (DNS Name: (kosong))* : Tidak diisi, sehingga klien akan diarahkan ke IP *gateway* (192.168.17.1) ketika diarahkan ke halaman login. Biasanya bisa diisi jika menggunakan DNS lokal seperti login.hotspot.local.
- *Hotspot Setup Completed* : Menunjukkan bahwa konfigurasi berhasil diselesaikan tanpa error.

Kesimpulan : Konfigurasi ini menunjukkan bahwa router MikroTik telah disiapkan sebagai *Hotspot Gateway* untuk jaringan 192.168.17.0/24 di *interface* V10. Fitur ini memungkinkan setiap

pengguna yang terhubung untuk melewati halaman login terlebih dahulu sebelum bisa mengakses jaringan/internet, sangat umum digunakan untuk jaringan tamu atau publik.

4.1. Pengujian Jaringan Awal

Pengujian jaringan awal dilakukan sebelum sistem segmentasi diterapkan. Jaringan masih berada dalam kondisi default, yaitu:

- Satu SSID WiFi digunakan bersama oleh karyawan dan tamu.
- Tidak ada sistem login atau autentikasi.
- Tidak ada pembatasan akses atau pemisahan segmen jaringan.

a. Pengujian Konektivitas

- Tools: Ping dan Traceroute
- Tujuan: Menguji koneksi antar perangkat dan ke internet.
- Hasil: Ping antar perangkat (misal dari laptop tamu ke server internal) berhasil.
- Traceroute dari klien tamu ke server internal menunjukkan tidak ada filtering atau firewall.
- Menunjukkan bahwa tidak ada isolasi jaringan antara tamu dan internal.

b. Pengujian Keamanan

- Tidak terdapat login hotspot, sehingga siapa pun yang memiliki password WiFi dapat mengakses jaringan.
- IP address didistribusikan oleh DHCP dalam satu subnet untuk semua pengguna.
- Tamu dapat mengakses file sharing dan printer internal, yang berpotensi melanggar kebijakan keamanan data.

c. Pengujian Penggunaan Bandwith

- Tidak ada pengaturan manajemen bandwidth.
- Tamu dapat melakukan aktivitas streaming/video call yang membebani bandwidth, berdampak pada karyawan yang sedang mengakses sistem internal.

d. Ringkasan Pengujian Awal

Tabel 1. Permasalahan Pengujian Awal

Aspek	Temuan Sebelum Implementasi
Konektivitas	Semua perangkat saling terhubung
Keamanan	Tidak ada autentikasi; akses terbuka
Manajemen Bandwith	Tidak ada pembatasan per pengguna
Isolasi Akses	Tidak ada segmentasi antara tamu dan karyawan

4.2. Pengujian Jaringan Akhir

Setelah penerapan segmentasi jaringan WiFi menggunakan Userman pada MikroTik, dilakukan pengujian kembali untuk mengukur efektivitas implementasi, baik dari sisi aksesibilitas, keamanan, maupun kinerja jaringan. Pengujian dilakukan dengan

metode dan tools yang sama seperti pengujian awal, yaitu: Ping, Traceroute, serta pengamatan terhadap pemisahan akses dan manajemen bandwidth.

a. Pengujian Konektivitas (ping & Traceroute)

- VLAN 10 (Karyawan):
 - Ping ke server internal: Sukses
 - Ping ke internet: Sukses
 - Traceroute menunjukkan jalur melalui router MikroTik dan LAN internal.
- VLAN 1 (Tamu):
 - Ping ke server internal: Gagal (karena dibatasi firewall)
 - Ping ke internet: Sukses
 - Traceroute hanya mengarah ke gateway dan keluar ke internet.

Implementasi firewall dan segmentasi VLAN berhasil mengisolasi akses tamu dari jaringan internal perusahaan.

b. Pengujian Keamanan Jaringan

- Login WiFi tamu kini melalui Hotspot Userman, tidak dapat langsung terkoneksi tanpa autentikasi.
- Username, password, batas waktu, dan bandwidth tamu dikontrol dari Userman.
- VLAN tamu dibatasi oleh firewall (tidak dapat mengakses 192.168.x.x di jaringan internal).
- VLAN karyawan tetap memiliki akses penuh sesuai hak aksesnya.

Hasil: Pengamanan jaringan meningkat secara signifikan karena akses tidak lagi terbuka dan bersifat anonim.

c. Pengujian Manajemen Bandwith

- Profil bandwidth untuk tamu dibatasi menggunakan Simple Queue (misal 1 Mbps up/down).
- Karyawan diberikan bandwidth lebih tinggi (misal 5 Mbps atau tanpa limit di jam kerja).
- Tidak terjadi gangguan trafik karyawan meskipun tamu aktif mengakses internet.

Hasil: Kinerja jaringan lebih stabil dan terkontrol berdasarkan prioritas pengguna.

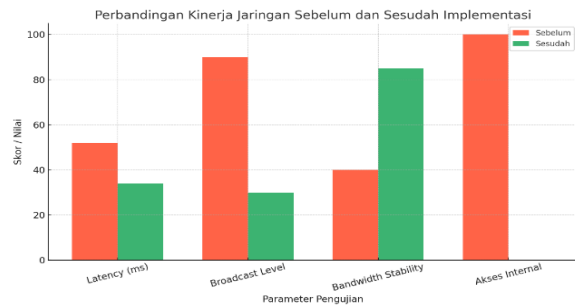
d. Tabel Perbandingan sebelum dan sesudah implementasi

Tabel 2. Perbandingan sebelum dan sesudah

Aspek	Sebelum Implementasi	Setelah Implementasi
Autentikasi WiFi	Tidak ada, hanya pakai password WiFi	Menggunakan Userman + Login Hotspot
Segmentasi Jaringan	Tidak ada, semua dalam 1 jaringan	VLAN 10 (karyawan), VLAN 20 (<i>quest</i>)
Akses Ke Server	Semua user bisa akses file/printer	Hanya VLAN 10 yang bisa akses <i>internal</i>
Manajemen Bandwith	Tidak ada pembatasan	Diatur berdasarkan profil user di Userman

e. Grafik Perbandingan Kinerja Jaringan

Berikut adalah grafik perbandingan kinerja jaringan sebelum dan sesudah implementasi segmentasi WiFi menggunakan Userman di PT. Internetwork Komunikasi Indonesia



Sumber: penelitian 2025

Gambar 9. Perbandingan Sebelum Dan Sesudah Implementasi

5. KESIMPULAN DAN SARAN

Berdasarkan rumusan masalah yang telah disusun, penelitian ini berfokus pada tiga hal utama, yaitu menganalisis kondisi eksisting jaringan WiFi di PT. Internetwork Komunikasi Indonesia yang masih digunakan bersama oleh karyawan dan tamu sehingga berpotensi menimbulkan permasalahan keamanan dan manajemen, merancang serta mengimplementasikan segmentasi jaringan WiFi menggunakan teknologi Userman pada perangkat MikroTik sebagai solusi pemisahan akses antara karyawan dan tamu, serta mengevaluasi efektivitas implementasi tersebut dalam meningkatkan keamanan, efisiensi, dan kemudahan pengelolaan jaringan di lingkungan perusahaan. Sebagai pengembangan lebih lanjut, disarankan agar sistem segmentasi dan Userman diperluas ke seluruh cabang atau kantor lain guna menciptakan standarisasi keamanan dan efisiensi jaringan secara menyeluruh, ditambahkan sistem keamanan lanjutan seperti firewall rule yang lebih kompleks, content filtering, serta IDS/IPS untuk mendeteksi dan mencegah potensi serangan, serta diterapkan sertifikat SSL pada halaman login hotspot demi meningkatkan keamanan autentikasi, khususnya bagi pengguna eksternal. Selain itu, peningkatan dokumentasi dan backup konfigurasi secara berkala sangat penting agar sistem dapat dipulihkan dengan cepat jika terjadi gangguan, serta pelatihan rutin bagi administrator jaringan perlu dilakukan untuk memastikan sistem tetap optimal dan administrator mampu mengikuti perkembangan teknologi jaringan terbaru, termasuk fitur-fitur dari MikroTik dan Userman.

DAFTAR PUSTAKA

- [1] R. Almakhi, A. S. Budiman, and R. D. Astuti, "Implementasi Protokol Keamanan Dan Segmentasi Jaringan Dalam Project Pembangunan WLAN Untuk PT Pan Pacific Insurance," *J. Sist. dan Teknol. Inf.*, vol. 11, no.

- 1, p. 140, 2023, doi: 10.26418/justin.v11i1.53745.
- [2] Z. Zulkarnaen, "Implementasi Usermanager Sebagai Radius Server Pada Router Board Mikrotik Rb750Gr3," *Tek. Teknol. Inf. dan Multimed.*, vol. 2, no. 2, pp. 56–63, 2021, doi: 10.46764/teknimedia.v2i2.43.
- [3] R. Susanto, "Rancang Bangun Jaringan Vlan dengan Menggunakan Simulasi Cisco Packet Tracer," *J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 1–6, 2020.
- [4] R. N. Dasmen, K. Pangestu, and K. Saputra, "Aplikasi Mikrotik Dasar Sebagai Pembatasan Bandwidth pada Warung Internet Teranet One di Prabumulih," *J. Komput. dan Inform.*, vol. 10, no. 1, pp. 72–77, 2022, doi: 10.35508/jicon.v10i1.6270.
- [5] E. A. Habibie and M. Muskhir, "Perancangan Monitoring Robot Kiper Melalui Access Point Sebagai Media Kendali Robot," *JTEIN J. Tek. Elektro Indones.*, vol. 2, no. 1, pp. 113–118, 2021, doi: 10.24036/jtein.v2i1.142.
- [6] H. Septanto, A. K. Wardani, and A. Hidayatullah, "Pelatihan Crimping Kabel UTP Tipe Straight dan Cross Over Jaringan Komputer LAN untuk Para Pemuda Kelurahan Pulo Gebang, Kecamatan Cakung, Jakarta Timur," *J. Karya untuk Masy.*, vol. 5, no. 1, pp. 45–58, 2024, doi: 10.36914/jkum.v5i1.1081.
- [7] I. P. Sari, I. H. Batubara, M. Basri, and A. H. Hazidar, "Implementasi Internet of Things Berbasis Website dalam Pemesanan Jasa Rumah Service Teknisi Komputer dan Jaringan Komputer," *Blend Sains J. Tek.*, vol. 1, no. 2, pp. 157–163, 2022, doi: 10.56211/blendsains.v1i2.136.
- [8] W. S. A. Sigalingging and A. S. Budi, "Sinkronisasi Waktu pada Wireless Sensor Network Berbasis Protokol ESP-Now menggunakan Algoritma Reference Broadcast Synchronization Pada Topology Mesh," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 7, pp. 3466–3470, 2023.
- [9] G. and T. J. and R. R. Y. Maulana Iskhaq, "Simulasi Manajemen Dan Autentikasi User Hotspot Menggunakan Mikhmon Server Pada Lab Basis Data Institut Sains & Teknologi Akprind Yogyakarta," *J. Jarkom*, vol. 9, no. 2, pp. 105–116, 2019.
- [10] J. F. Fitrian and H. Sujadi, "Implementasi Hotspot Dengan Pengelolaan User Manager Dan Bandwidth Menggunakan Mikrotik Rb941-2Nd (Studi Kasus Smk Kesehatan Bhakti Kencana Jatiwangi)," *Pros. Semin. Nas. Penelit. dan Pengabd. Kpd. Masy.*, vol. 1, no. 1, pp. 103–110, 2023.
- [11] A. R. Rozzaqi and F. Amin, "IMPLEMENTASI USER MANAGER DENGAN DATA RESMI UNTUK MONITORING PENGGUNAAN JARINGAN DI," vol. 10, no. 02, 2024.
- [12] D. Satria, "Penerapan VLAN pada VAP Menggunakan Mikrotik CAPsMAN untuk Manajemen Bandwidth Berbasis PCQ," vol. 5, no. 3, pp. 241–249, 2025, doi: 10.47065/jimat.v5i3.696.
- [13] Fatkhurrahman and Arita Witanti, "Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik," *JEKIN - J. Tek. Inform.*, vol. 4, no. 3, pp. 675–687, 2024, doi: 10.58794/jekin.v4i3.904.
- [14] R. Oktiana and L. Widyawati, "Desain dan Implementasi VLAN Untuk Manajemen Access User pada Access Point Multi SSID dengan CAPsMAN Berbasis Mikrotik," pp. 57–66, 2025, doi: 10.30812/juteks.v1i1.5192.
- [15] E. S. Susanto and A. D. Septiarini, "Implementasi Hotspot dengan User Manager untuk Internet Wireless Menggunakan MikroTik RB941-2nd di MTsN 1 Sumbawa Besar," *urnal Inform. Teknol. dan Sains*, vol. 3, no. 3, pp. 415–419, 2021, [Online]. Available: <https://jurnal.uts.ac.id/index.php/JINTEKS/article/download/1274/758>
- [16] R. Al Ajwani, A. . W. Mahfuzhi, Muntahanah, and Khairullah, "Mikrotik-based Hotspot Network Design Using the User Manager Authentication Method at SMKN 4 Bengkulu Selatan," *J. Komputer, Inf. dan Teknol.*, vol. 5, no. 1, p. 9, 2025, doi: 10.53697/jkomitek.v5i1.2352.