

Implementasi Freeradius pada Jaringan Hotspot dengan Mikrotik dan MySQL

Setyo Abdi Nugroho¹, Herdianto Herdianto², Hendry³

⁽¹⁾ Mahasiswa Sistem Komputer Universitas Pembangunan Panca Budi Medan

⁽²⁾ Dosen Sistem Komputer Universitas Pembangunan Panca Budi Medan

⁽³⁾ Dosen Sistem Komputer Universitas Pembangunan Panca Budi Medan

*Email

setyoabdi6@gmail.com; herdianto@dosen.pancabudi.ac.id; hendry@dosen.pancabudi.ac.id

Sejarah Artikel:

Diterima 10-08-2025
Disetujui 19-08-2025
Diterbitkan 21-08-2025

ABSTRACT

A computer network is a collection of devices connected to communicate and exchange data. The internet is a global network that connects users worldwide. To access the internet, Mikrotik network devices and LAN cables are commonly used. However, LAN cables are less efficient for multiple users, especially smartphone users, as Android devices do not support LAN connections. Mikrotik offers a hotspot feature that allows users to connect wirelessly. To ensure security and prevent unauthorized access, login authentication is required. This can be achieved by integrating the RADIUS feature on Mikrotik with FreeRADIUS and MySQL on an Ubuntu server. User accounts for authentication can be managed through the daloRADIUS web application. The integration of FreeRADIUS, MySQL, and daloRADIUS with Mikrotik simplifies user account management and prevents unauthorized users from accessing the network. This system enhances security and ensures only registered users are able to access the internet via the hotspot.

Keyword: Computer networks, internet, Mikrotik, hotspot, hotspot manager, users, RADIUS, FreeRADIUS, MySQL, daloRADIUS, Ubuntu server.

ABSTRAK

Jaringan komputer adalah sekumpulan perangkat yang saling terhubung untuk berkomunikasi dan bertukar data. Jaringan yang lebih luas dan menghubungkan pengguna di seluruh dunia disebut internet. Untuk terhubung ke internet, umumnya digunakan perangkat Mikrotik dan kabel LAN. Namun, penggunaan kabel LAN kurang efisien bagi banyak pengguna, terutama pengguna smartphone Android yang tidak mendukung koneksi LAN. Mikrotik menyediakan fitur hotspot yang memungkinkan koneksi internet tanpa kabel. Untuk menjaga keamanan dan membatasi akses tidak sah, diperlukan sistem login autentikasi. Sistem ini dapat diterapkan dengan mengintegrasikan fitur RADIUS pada Mikrotik dengan FreeRADIUS dan MySQL di server Ubuntu, serta dikelola melalui aplikasi web daloRADIUS. Hasil implementasi menunjukkan bahwa integrasi ini mempermudah pengelolaan akun login pengguna dan mencegah akses dari pengguna yang tidak terdaftar di server RADIUS.

Kata Kunci : Jaringan komputer, internet, Mikrotik, hotspot, pengelola hotspot, pengguna, RADIUS, FreeRADIUS, MySQL, daloRADIUS, server Ubuntu.

Bagaimana Cara Sitasi Artikel ini:

Setyo Abdi Nugroho, Herdianto Herdianto, & Hendry. (2025). Implementasi Freeradius pada Jaringan Hotspot dengan Mikrotik dan MySQL. Jejak Digital: Jurnal Ilmiah Multidisiplin, 1(5), 3342-3359. <https://doi.org/10.63822/c3q5p667>

PENDAHULUAN

Hotspot merupakan titik lokasi atau area tertentu yang dirancang untuk berbagi jaringan yang disediakan oleh penyedia layanan jaringan (Internet Service Provider) dalam mengakses internet melalui jaringan nirkabel (wireless network). Layanan jaringan internet tersebut dapat berupa layanan berbayar maupun gratis. Agar layanan jaringan internet dapat dibagikan ke beberapa pengguna, dibutuhkan perangkat jaringan untuk memancarkan sinyal hotspot. Salah satunya yaitu perangkat jaringan Router MikroTik (Ikhsan and Wagito 2023)

Router Mikrotik merupakan perangkat keras (hardware) yang didalamnya terdapat Sistem Operasi MikroTik yang digunakan untuk mengelola jaringan komputer ataupun jaringan internet. Salah satu fitur didalam Router MikroTik yaitu hotspot. Dengan mengaktifkan fitur hotspot pada MikroTik, maka pengguna dapat terhubung ke jaringan internet melalui koneksi wireless. Fitur hotspot pada MikroTik juga dapat dikonfigurasi untuk menyediakan akses jaringan internet yang aman dan terkendali secara terpusat dengan menggunakan RADIUS (Ikhsan and Wagito 2023)

RADIUS (Remote Authentication Dial-In User Service) adalah sebuah protokol keamanan untuk melakukan Autentikasi, Otorisasi dan Manajemen Akun pengguna secara terpusat (AAA) untuk mengakses jaringan (Aziz and Safriatullah 2021)

FreeRADIUS merupakan server RADIUS yang digunakan untuk autentifikasi login, dimana didalamnya terdapat protokol AAA (Authentication, Authorized, Accounting) untuk memungkinkan pengelola mengamankan dan memonitor jaringan (Pratama, Wahyuni, and Lubis 2023). Proses awal dimulai dari Authentication atau Autentikasi yaitu proses dimana pengguna yang mencoba untuk akses jaringan internet ke penyedia jaringan dan diidentifikasi oleh server terlebih dahulu sebelum menggunakan jaringan (Fitriani, 2024). Pengguna meminta akses jaringan internet ke NAS (Network Access Server), kemudian mengidentifikasi username dan password yang telah diinput (Tri, 2025). Jika sama dengan data yang sudah tersimpan dengan database mySQL pada server freeRADIUS, maka pengguna dapat mengakses internet (Fitriani, 2024). Selanjutnya Authorization atau otorisasi yaitu layanan apa saja yang berhak diakses ataupun batasan bandwidth yang dapat digunakan oleh pengguna setelah masuk kedalam akses jaringan internet. Terakhir adalah Accounting atau manajemen akun pengguna yaitu proses yang dilakukan oleh NAS (Network Access Server) pada server freeRADIUS untuk mencatat semua aktivitas pengguna didalam jaringan, seperti log / riwayat waktu saat pertama kali login atau logout dan banyaknya data yang diakses oleh pengguna saat masih terhubung ke jaringan (Hendarto 2018)

Namun dengan mengintegrasikan hotspot RADIUS pada MikroTik dan server FreeRADIUS pada server, belum cukup untuk dapat mempermudah pengelola (administrator) hotspot untuk manajemen user pengguna (Ramadhan, 2024). Untuk itu, diperlukan instalasi DaloRADIUS pada server agar dapat dengan mudah menambah akun, menghapus akun dan manajemen akun pengguna (Tambunan, 2024). DaloRADIUS merupakan aplikasi berbasis web yang didalamnya terdapat berbagai fitur dalam manajemen user pengguna hotspot. Pengelola hotspot juga tidak perlu secara langsung melakukan konfigurasi username dan password untuk pengguna hotspot ke MikroTik untuk menghindari kesalahan konfigurasi jaringan dan juga demi keamanan jaringan.

Untuk memberikan kemudahan bagi pengelola hotspot dalam manajemen pengguna hotspot terutama memberikan keamanan dan kenyamanan bagi pengguna saat akses jaringan internet melalui hotspot MikroTik, maka perlu dilakukan penerapan sistem autentikasi terpusat dengan mengintegrasikan MikroTik, FreeRADIUS dan MySQL. Dari hasil paparan tersebut, maka penulis membuat tugas akhir dengan judul "Implementasi FreeRADIUS pada jaringan hotspot dengan MikroTik dan MySQL".

METODE PENELITIAN

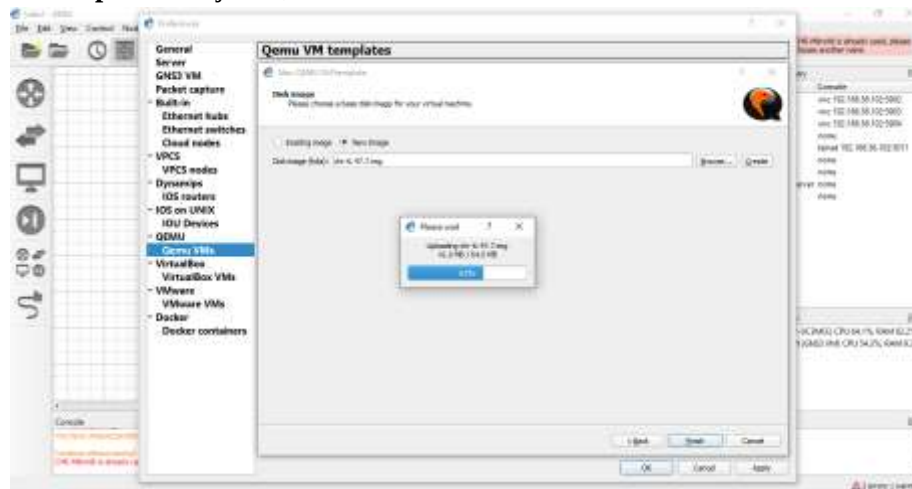
Penelitian ini menggunakan pendekatan eksperimental dengan studi kasus implementasi sistem autentikasi jaringan menggunakan FreeRADIUS pada hotspot berbasis MikroTik dan MySQL. Metode penelitian dilakukan melalui tiga tahapan utama. Tahap pertama adalah analisis kebutuhan dan infrastruktur jaringan, yang mencakup identifikasi spesifikasi perangkat keras seperti router MikroTik, server Ubuntu, serta perangkat klien, dan perangkat lunak seperti VirtualBox, GNS3, Apache, MySQL, FreeRADIUS, dan daloRADIUS, serta perancangan topologi jaringan.

Tahap kedua adalah instalasi dan konfigurasi sistem, meliputi pemasangan lingkungan simulasi menggunakan VirtualBox dan GNS3, konfigurasi MikroTik (termasuk DHCP, firewall, dan pengaturan hotspot RADIUS), serta instalasi dan integrasi FreeRADIUS dan daloRADIUS di server Ubuntu. Tahap ketiga adalah pengujian dan evaluasi sistem, yang dilakukan dengan mengukur keberhasilan autentikasi pengguna, kecepatan respons sistem, stabilitas jaringan, dan keamanan akses, dengan memastikan hanya pengguna terdaftar yang dapat terhubung ke jaringan.

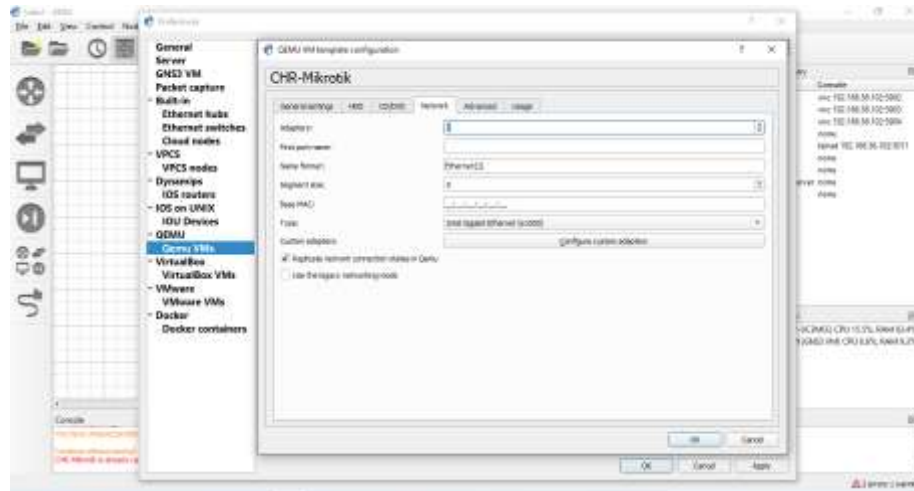
HASIL DAN PEMBAHASAN

1. Implementasi MikroTik CHR, Mozilla Client dan Server Ubuntu pada GNS3 Client

Sesuai dengan Perancangan Topologi Jaringan Sistem Autentikasi Terpusat (Gambar 4.1) yang telah dibahas sebelumnya, maka beberapa hal yang perlu dipersiapkan adalah melakukan instalasi dan konfigurasi network untuk file Disk Image MikroTik CHR (tabel 1) pada GNS3 Client yaitu dengan klik menu **Edit > Preferences**. Di tab **Qemu VMs**, klik **New > GNS3 VM > Qemu VM Name**. Pilih Opsi **New Image > Browse**, pilih file image MikroTik CHR, lalu klik **Finish**. Untuk konfigurasi network, klik interface MikroTik yang sudah dibuat sebelumnya, klik tombol **Edit**. Pada bagian tab **Network**, ganti jumlah interface **Adapters** menjadi 5, lalu **OK**.

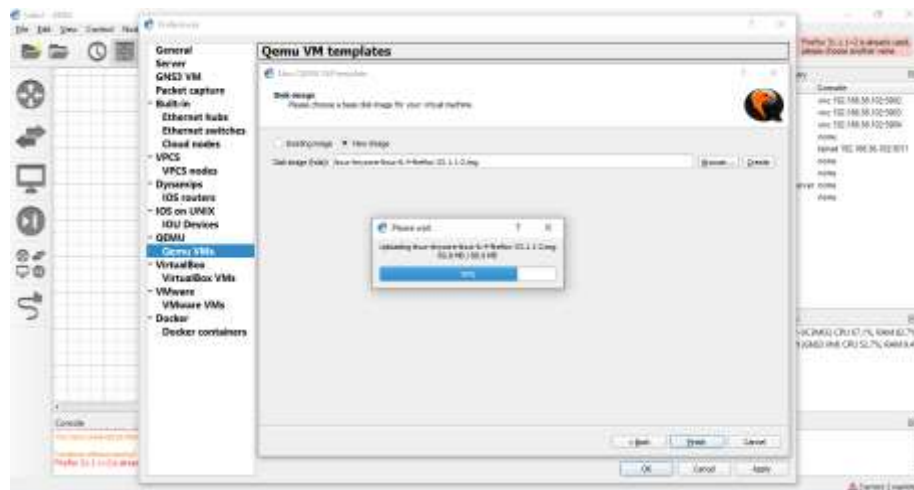


Gambar.1. Instalasi MikroTik CHR pada GNS3 Client



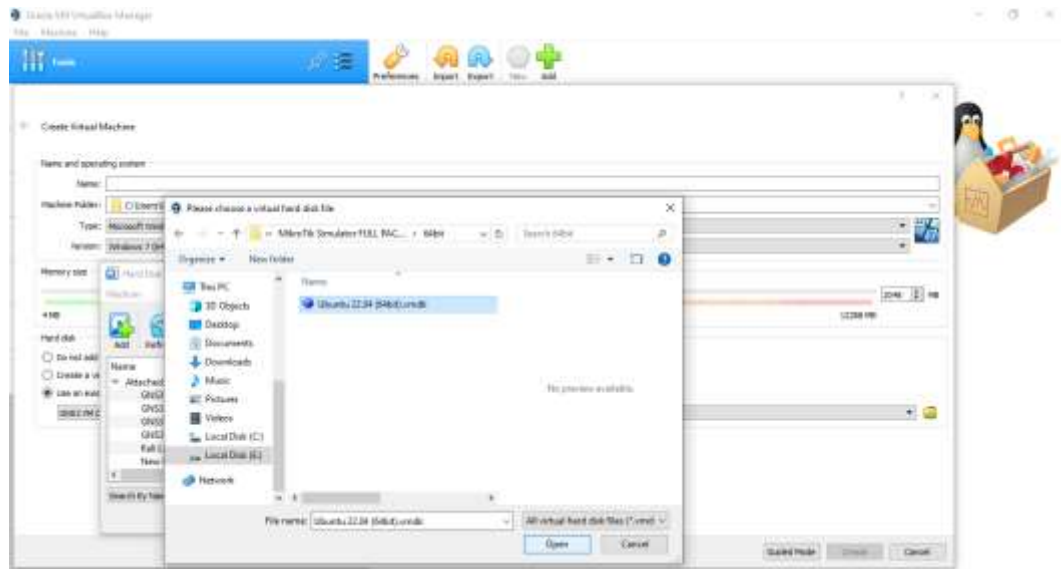
Gambar.2. Konfigurasi Network Adapters MikroTik

Proses instalasi emulator browser Mozilla yang akan digunakan sebagai client juga sama seperti proses instalasi MikroTik. Namun konfigurasi untuk network adapter tidak diperlukan.

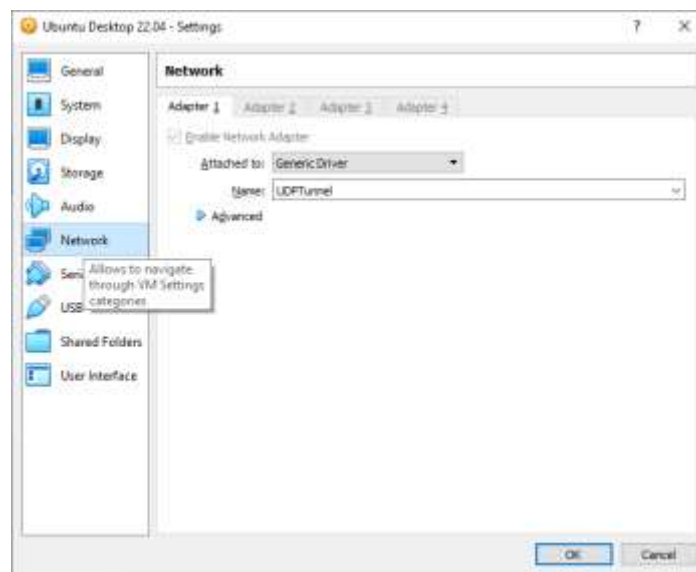


Gambar.3. Instalasi Mozilla Client pada GNS3 Client

Proses instalasi Server Ubuntu berbeda dengan MikroTik dan Mozilla Client. Server Ubuntu harus diinstall dan dikonfigurasi terlebih dahulu pada Virtualbox dengan cara klik tombol **New > Use an existing virtual hard disk file** > klik tombol **Browse**. Setelah muncul tab window baru **Hard Disk Selector** > klik tombol **Add**, pilih file **Ubuntu Desktop 22.04** (dengan ekstensi .vmdk). setelah berhasil ditambahkan, klik tombol **Settings** > pilih tab **Network** > **Adapter 1** > checklist **Enable Network Adapter**.

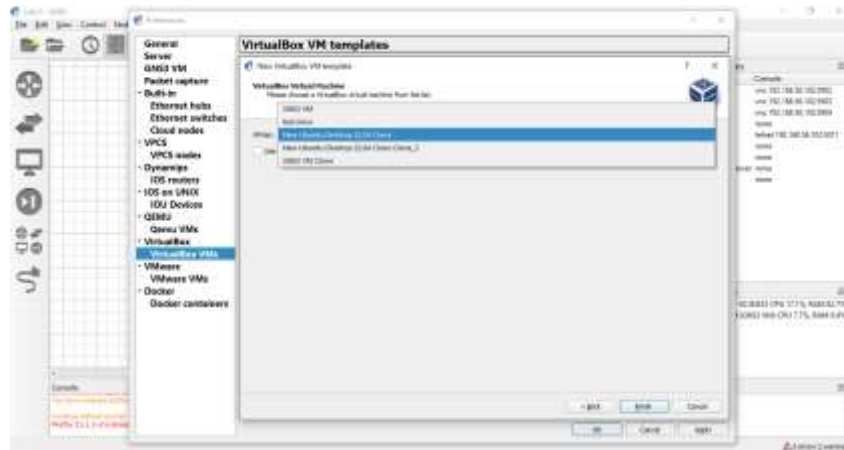


Gambar 4. Instalasi Server Ubuntu pada Virtualbox



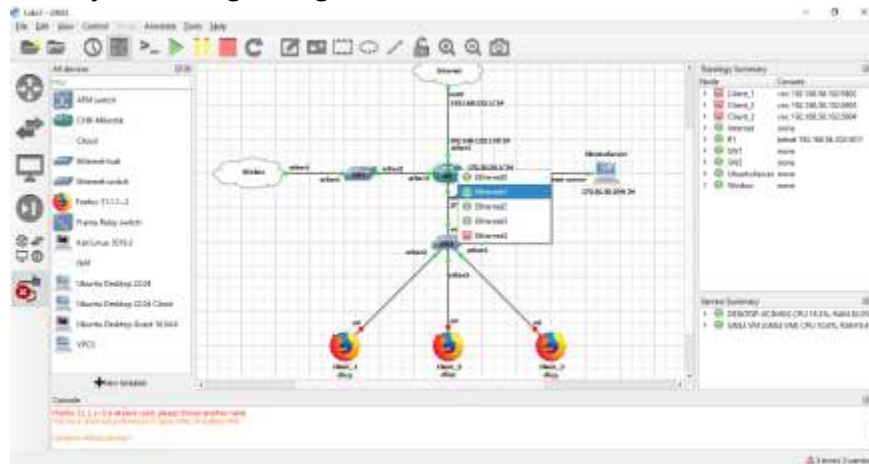
Gambar 5. Konfigurasi Network Adapter Ubuntu

Tahap terakhir untuk instalasi Ubuntu adalah menambahkan Ubuntu pada GNS3 Client dengan cara klik menu **Edit > Preferences > klik tab VirtualBox VMs > New > VM list** > pilih VM Ubuntu yang sudah ditambahkan sebelumnya pada Virtualbox, lalu klik **Finish**.



Gambar.6. Konfigurasi VM Server Ubuntu pada GNS3 Client

Selanjutnya merancang topologi jaringan dengan cara drag and drop device yang sudah ditambahkan sebelumnya dan menghubungkan semua device.



Gambar.7. Desain topologi jaringan

2. Konfigurasi Sistem MikroTik CHR

Setelah selesai instalasi semua perangkat pada GNS3 Client, tahap berikutnya adalah melakukan beberapa konfigurasi untuk perangkat khususnya MikroTik dan Ubuntu. Untuk MikroTik, klik kanan perangkat lalu pilih **Start**. Setelah itu, klik kanan kembali MikroTik lalu pilih **console**. Setelah muncul tab window terminal, masukkan user login **admin** dan password (kosong), lalu konfigurasi MikroTik dengan beberapa perintah sebagai berikut :

- Menambahkan interface untuk masing - masing port di router1 :
/ip address add address=172.20.20.1/24 interface=ether2 → Enter
/ip address add address=172.20.30.1/24 interface=ether4 → Enter
- Menambahkan Masquerade agar masing - masing ip private dapat saling terhubung dan dapat terkoneksi ke jaringan internet (ip public) melalui Mikrotik :
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade → Enter
- Melakukan konfigurasi ip dhcp untuk interface ether2 dan ether4 agar masing - masing perangkat yang terhubung ke masing - masing interface mendapatkan ip private secara otomatis sesuai dengan ip route

masing - masing interface :

/ip dhcp-server setup → Enter

dhcp server interface: ether2 → Enter

dhcp address space: 172.20.20.0/24 → Enter

gateway for dhcp network: 172.20.20.1 → Enter

dns servers: 192.168.122.1 → Enter

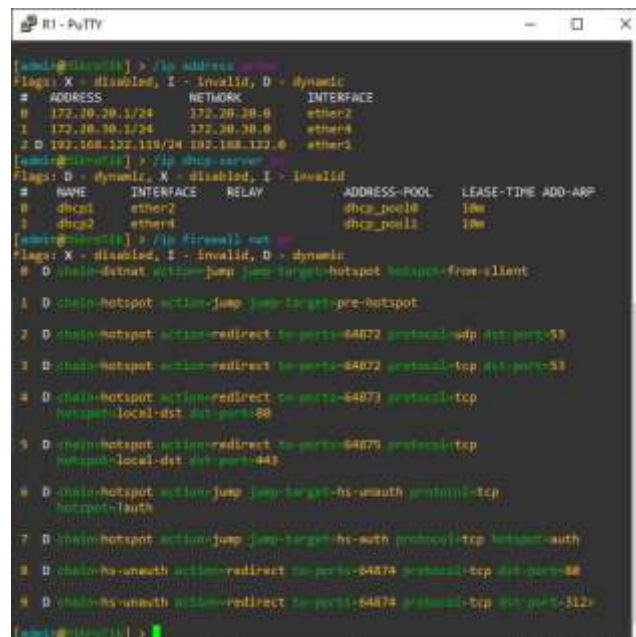
/ip dhcp-server setup → Enter

dhcp server interface: ether4 → Enter

dhcp address space: 172.20.30.0/24 → Enter

gateway for dhcp network: 172.20.30.1 → Enter

dns servers: 192.168.122.1 → Enter



```
[admin@Mikrotik] > /ip address
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 172.20.20.1/24 172.20.20.0 ether2
1 172.20.30.1/24 172.20.30.0 ether4
2 D 192.168.122.1/24 192.168.122.0 ether1

[admin@Mikrotik] > /ip dhcp-server
Flags: D - dynamic, X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 dhcp1 ether2 dhcp_pool0 10m
1 dhcp2 ether4 dhcp_pool1 10m

[admin@Mikrotik] > /ip firewall nat
Flags: X - disabled, I - invalid, D - dynamic
# D chain=dstnat action=jump jump-target=hotspot hotspot-from-client

1 D chain=hotspot action=jump jump-target=pre-hotspot
2 D chain=hotspot action=redirect to-ports=64872 protocol=udp dst-port=55
3 D chain=hotspot action=redirect to-ports=64872 protocol=tcp dst-port=31
4 D chain=hotspot action=redirect to-ports=64873 protocol=tcp
hotspot-local-dst dst-port=80
5 D chain=hotspot action=redirect to-ports=64879 protocol=tcp
hotspot-local-dst dst-port=443
6 D chain=hotspot action=jump jump-target=hs-unauth protocol=tcp
hotspot-auth
7 D chain=hotspot action=jump jump-target=hs-auth protocol=tcp hotspot-auth
8 D chain=hs-unauth action=redirect to-ports=64874 protocol=tcp dst-port=88
9 D chain=hs-unauth action=redirect to-ports=64874 protocol=tcp dst-port=3112

[admin@Mikrotik] >
```

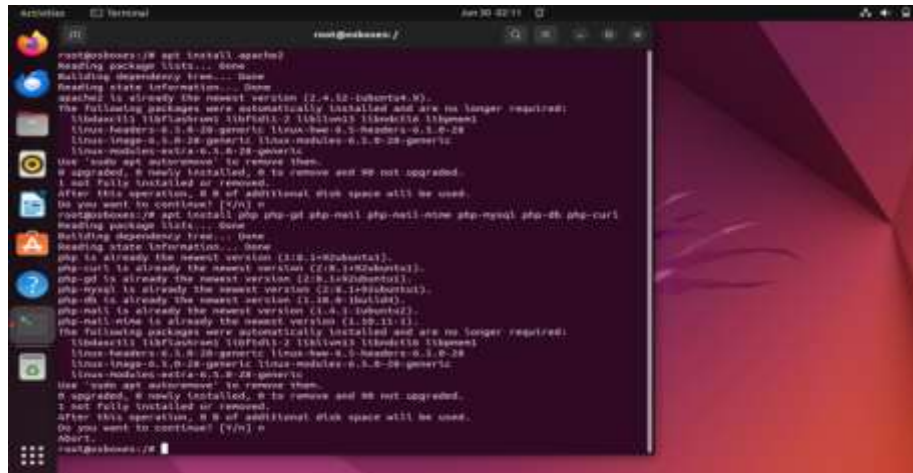
Gambar.8. Hasil Konfigurasi Interface, Masquerade dan DHCP Setup pada MikroTik CHR

3. Konfigurasi Sistem Server Ubuntu

Tahap selanjutnya adalah melakukan konfigurasi Ubuntu. Klik kanan perangkat, pilih **Start** dan tunggu sampai muncul tab window VM Ubuntu. Jalankan terminal sebagai root lalu lakukan beberapa instalasi aplikasi seperti apache, MariaDB, freeRADIUS dan daloRADIUS dengan beberapa perintah sebagai berikut :

- a. Melakukan instalasi aplikasi apache2 sebagai web server :

```
root@osboxes:/# apt install apache2
```



Gambar.9. Instalasi web server apache

- b. Instalasi dan konfigurasi database server MariaDB :

```
root@osboxes:~# apt install mariadb-server
root@osboxes:~# mysql_secure_installation
Enter current password for root (enter for none): [enter]
Switch to unix_socket authentication [Y/n] n
Change the root password? [Y/n] n
Remove anonymous users? [Y/n] y
Disallow root login remotely? [Y/n] y
Remove test database and access to it? [Y/n] y
Reload privilege tables now? [Y/n] y
```

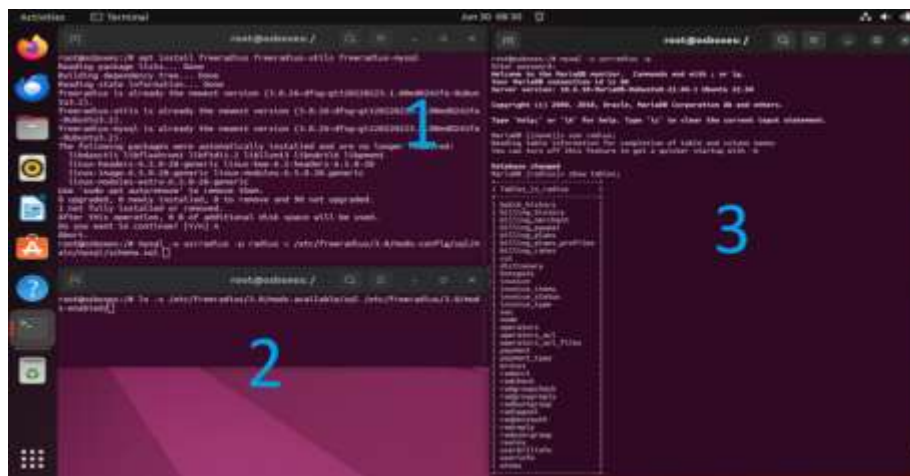
```
root@osboxes:~# mysql -u root -p [enter]
Enter password: [enter]
MariaDB [(none)]> create database radius;
MariaDB [(none)]> grant all on radius.* to usrradius@localhost identified by 'pwdradius';
MariaDB [(none)]> show grants for usrradius@localhost;
MariaDB [(none)]> flush privileges;
MariaDB [(none)]> quit;
```



Gambar 10. Instalasi dan konfigurasi database server MariaDB

- c. Download, install, konfigurasi dan import schema FreeRADIUS :

```
root@osboxes:/# apt install freeradius freeradius-utils freeradius-mysql
root@osboxes:/# mysql -u usrradius -p radius < /etc/freeradius/3.0/mods-
config/sql/main/mysql/schema.sql
root@osboxes:/# ln -s /etc/freeradius/3.0/mods-available/sql /etc/freeradius/3.0/mods-enabled/
root@osboxes:/# mysql -u usrradius -p
Enter password: pwdradius [enter]
MariaDB [(none)]> use radius;
MariaDB [radius]> show tables;
MariaDB [radius]> quit;
```



Gambar 11. Instalasi, konfigurasi dan import schema FreeRADIUS

- d. Melakukan beberapa perubahan pengaturan di SQL FreeRADIUS :

```
root@osboxes:/# nano /etc/freeradius/3.0/mods-available/sql
```

- 1) Hapus tanda (#) driver = "rlm_sql_\${dialect}"
- 2) Hapus tanda (#) dialect = "sqlite", ubah menjadi dialect = "mysql"
- 3) Dibagian kode mysql {}, tutup semua bagian konfigurasi TLS dengan Komentar (#)
- 4) Hapus semua tanda komentar (#) pada baris kode server, port, login, password dan radius_db.
Untuk user login dan password, sesuaikan dengan user dan password login di database radius pada server MariaDB. Untuk radius_db, ganti sesuai dengan nama database pada server MariaDB.

```
server = "localhost"
```

```
port = 3306
```

```
login = "usrradius"
```

```
password = "pwdradius"
```

```
radius_db = "radius"
```

- a. Hapus tanda komentar (#) pada baris kode :

```
read_clients = yes
```

```
client_table = "nas"
```



Gambar.12. Perubahan pengaturan pada SQL FreeRADIUS

- e. Menambahkan IP Client dan Secret password untuk digunakan pada MikroTik :

```
root@osboxes:/# nano /etc/freeradius/3.0/clients.conf
```

```
client 172.20.20.1 {secret = frengkiserver}
```



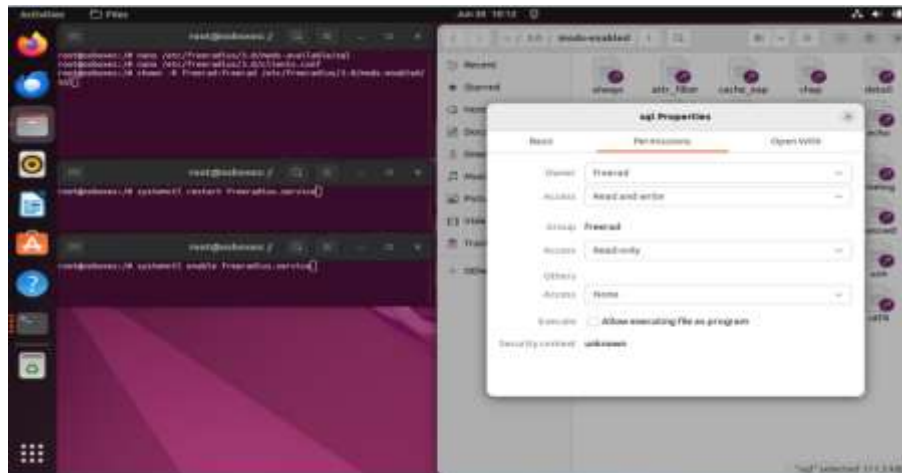
Gambar 13. Setting IP Client dan Secret Password

- f. Mengubah Permissions sql FreeRADIUS :

```
root@osboxes:/# chown -R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql
```

```
root@osboxes:/# systemctl restart freeradius.service
```

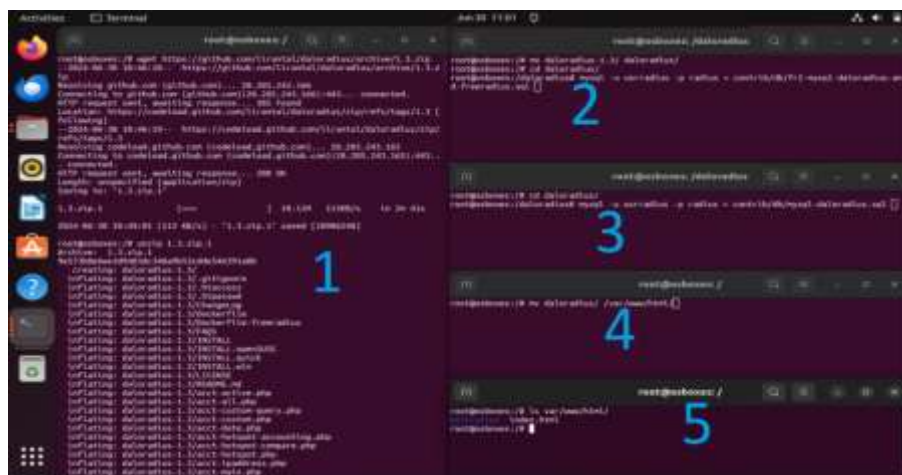
```
root@osboxes:/# systemctl enable freeradius.service
```



Gambar.14. Setting Permissions sql FreeRADIUS

- g. Instalasi dan konfigurasi web management DaloRADIUS :

```
root@osboxes:/# wget https://github.com/lirantal/daloradius/archive/1.3.zip
root@osboxes:/# unzip 1.3.zip
root@osboxes:/# mv daloradius-1.3/ daloradius/
root@osboxes:/# cd daloradius/
root@osboxes:daloradius/# mysql -u usrradius -p radius < contrib/db/fr2-mysql-daloradius-and-freeradius.sql
root@osboxes:daloradius/# mysql -u usrradius -p radius < contrib/db/mysql-daloradius.sql
root@osboxes:/# mv daloradius/ /var/www/html/
```



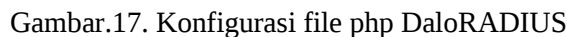
Gambar.15. Instalasi dan konfigurasi web management DaloRADIUS

- h. Konfigurasi file direktori DaloRADIUS :

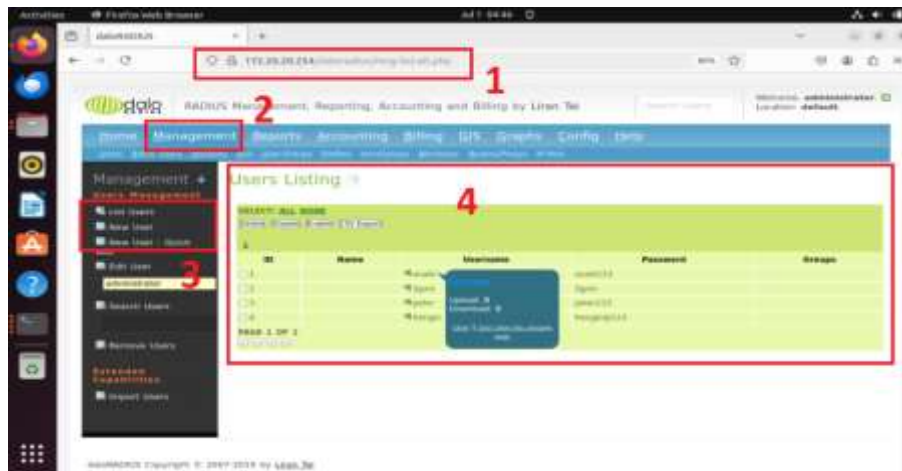
```
root@osboxes:/# chown -R www-data:www-data /var/www/html/daloradius/
root@osboxes:/# cp /var/www/html/daloradius/library/daloradius.conf.php.sample /var/www/html/daloradius/library/daloradius.conf.php
root@osboxes:/# chmod 664 /var/www/html/daloradius/library/daloradius.conf.php
```



- ```
root@osboxes:~# nano /var/www/html/daloradius/library/daloradius.conf.php
```



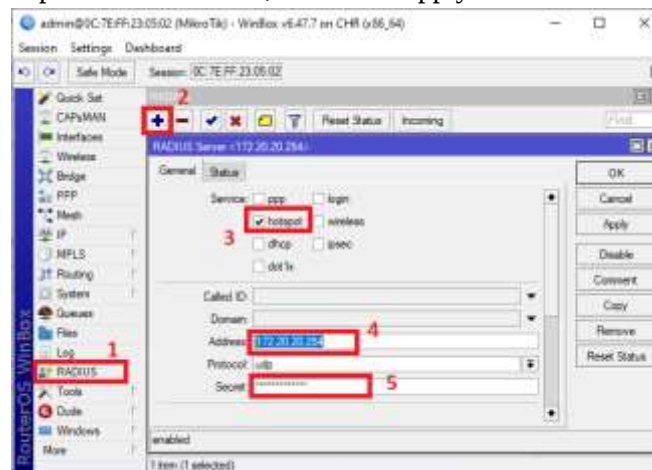
- 1) Masukkan alamat ip server Ubuntu atau menggunakan "localhost"
  - 172.20.20.254/daloradius/login.php
  - user : administrator, password : radius
- 2) Klik Tab Management untuk menampilkan submenu Users Management
- 3) Dibagian Users Management, Klik "New User" untuk membuat user dan password yang akan digunakan para client saat proses autentikasi login
- 4) Klik "List Users" untuk menampilkan daftar user yang sudah dibuat pada bagian tab sebelah kanan



Gambar 18. Menambah User Client dari web management DaloRADIUS

k. Konfigurasi RADIUS pada MikroTik :

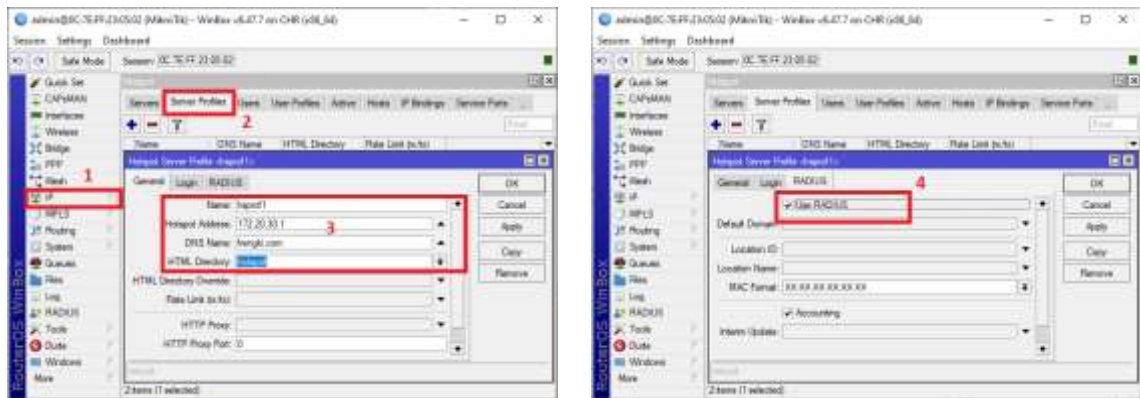
- 1) Klik bagian RADIUS
- 2) Klik tombol add (+)
- 3) Klik checkbox pada bagian hotspot
- 4) Masukkan alamat ip server Ubuntu
- 5) Masukkan Secret password RADIUS, lalu klik "Apply" dan "OK"



Gambar 19. Konfigurasi RADIUS pada MikroTik CHR

l. Konfigurasi Hotspot RADIUS :

- 1) Klik Ip > Hotspot
- 2) Klik tab Server Profiles, klik tombol add (+)
- 3) Masukkan alamat Ip hotspot sesuai dengan interface yang sudah dibuat sebelumnya untuk jalur akses internet client, nama DNS dan HTML Directory
- 4) Klik tab RADIUS, checklist bagian "Use RADIUS", klik "Apply" dan "OK"

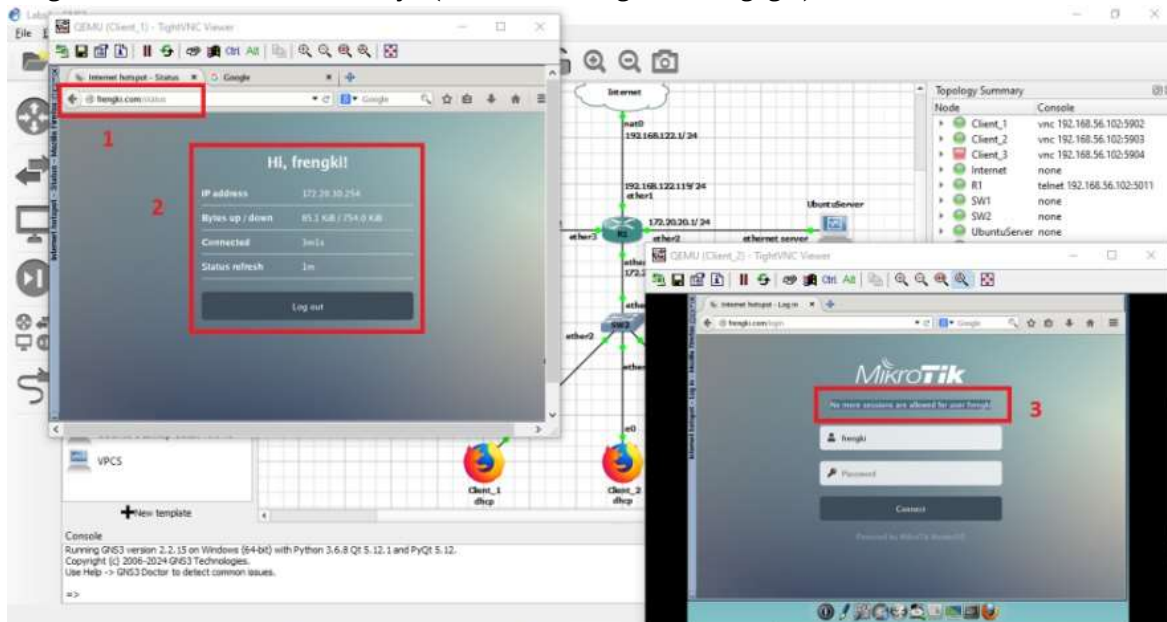


Gambar.20. Konfigurasi Hotspot RADIUS pada MikroTik CHR

#### 4. Hasil Pengujian Autentikasi Login pada Client

Berikut uji coba dan hasil dari proses autentikasi login pada client :

- Masukkan alamat domain (frengki.com) atau langsung akses ke google.com (Secara otomatis akan diarahkan langsung ke domain autentikasi login RADIUS)
- Login menggunakan user dan password yang sudah ditentukan di database radius di server Ubuntu (Autentikasi Login Client berhasil)
- Autentikasi Login client yang lain gagal dikarenakan menggunakan user dan password yang sudah digunakan oleh client sebelumnya (Autentikasi Login Client gagal)

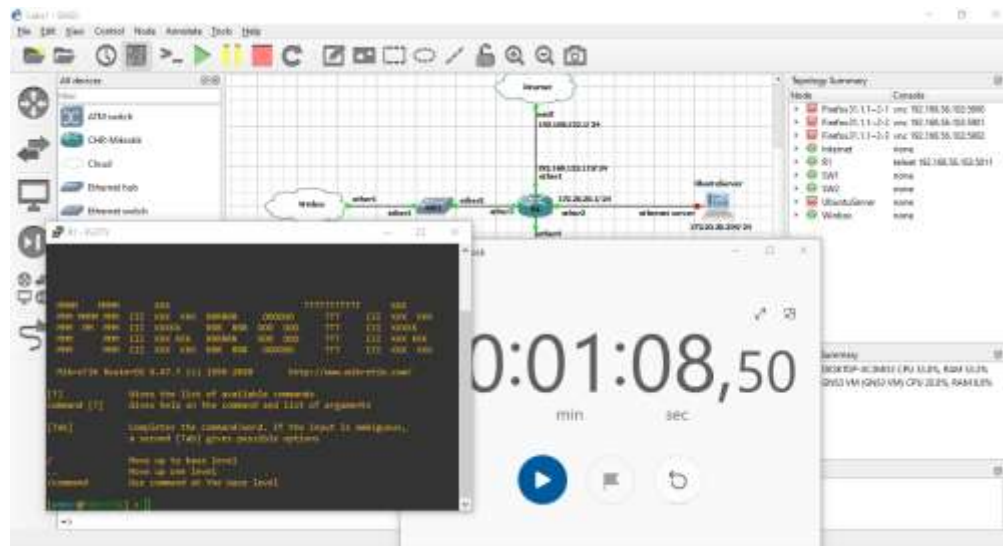


Gambar.21. Hasil uji coba proses autentikasi (berhasil dan gagal) menggunakan FreeRADIUS

#### 5. Hasil Response Time saat Pengujian Sistem

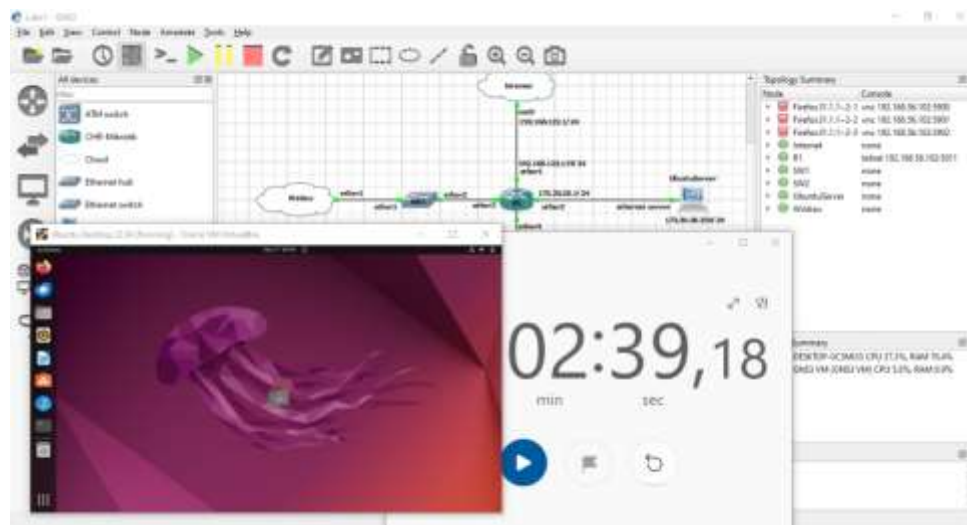
Berikut hasil waktu respon yang didapat saat menjalankan perangkat jaringan MikroTik, server Ubuntu dan client saat uji coba di GNS3 :

- Waktu yang dibutuhkan perangkat jaringan MikroTik mulai dari proses dinyalakan sampai perangkat dalam keadaan online adalah 1 menit 8 detik.



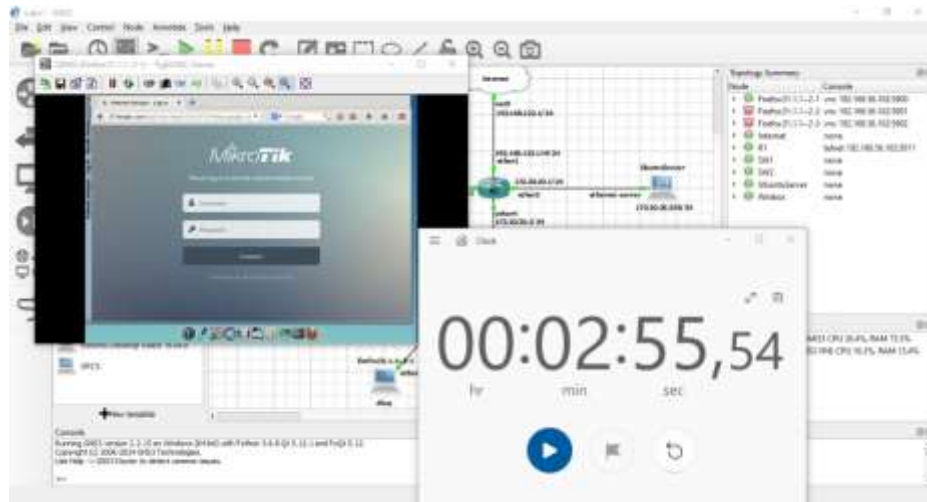
Gambar.22. Hasil response time perangkat jaringan MikroTik

- b. Waktu yang dibutuhkan server Ubuntu untuk menyala hingga terhubung ke jaringan internet adalah 2 menit 39 detik.



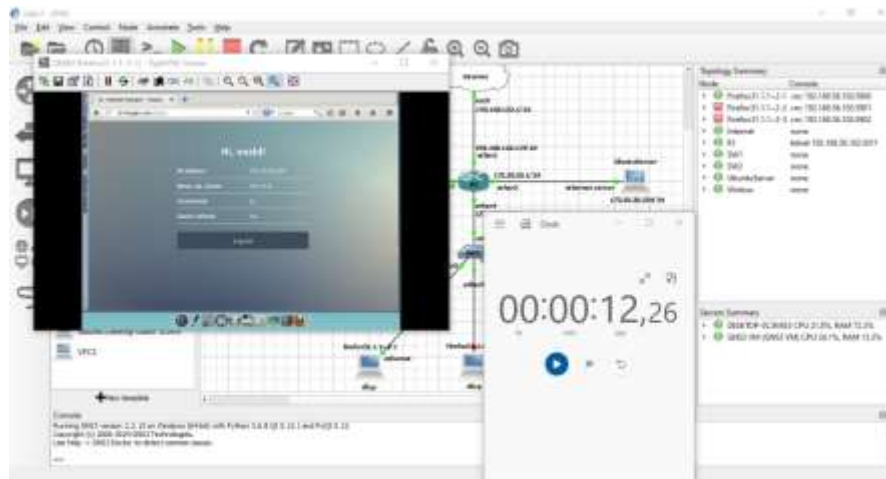
Gambar.23. Hasil response time server Ubuntu

- c. Waktu yang dibutuhkan perangkat client untuk menyala hingga saat menjalankan aplikasi browser Mozilla adalah 2 menit 55 detik.



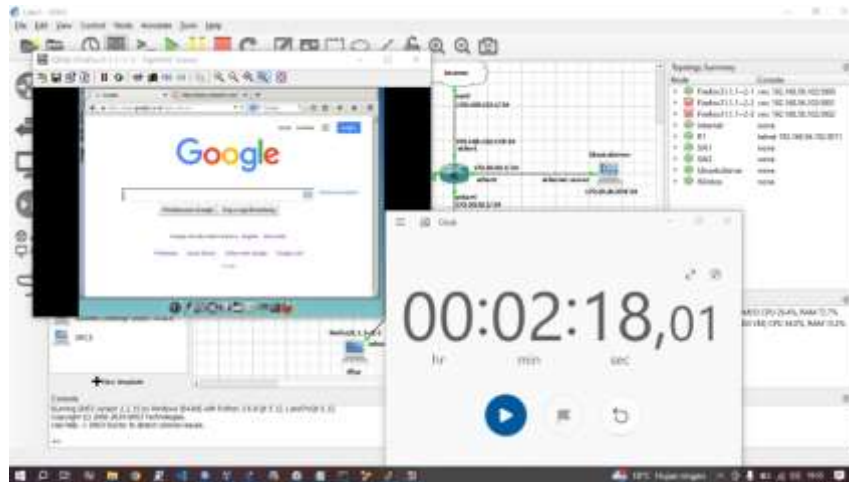
Gambar.24. Hasil response time proses nyala perangkat client

- d. Waktu yang dibutuhkan client untuk proses autentikasi login ke server freeRADIUS di server Ubuntu adalah 12 detik.



Gambar 25. Hasil response time proses autentikasi login client

- e. Waktu yang dibutuhkan client untuk akses jaringan internet setelah proses autentikasi login adalah 2 menit 18 detik.



Gambar 26. Hasil response time proses akses jaringan internet client

Berdasarkan hasil pengujian sistem perangkat diatas, maka dapat disimpulkan bahwa tidak ada kesalahan atau kegagalan sistem. Namun saat proses akses jaringan internet pada perangkat client membutuhkan waktu hingga 2 menit 18 detik. Hal ini dikarenakan jaringan ISP pada saat proses pengujian tidak stabil.

## SIMPULAN

Berdasarkan hasil pengujian dari implementasi FreeRADIUS pada jaringan hotspot dengan MikroTik dan MySQL dapat disimpulkan bahwa :

1. Desain infrastruktur jaringan hotspot MikroTik dan FreeRADIUS Server cukup mudah dilakukan dengan mempersiapkan MikroTik untuk konfigurasi dasar jaringan (akses hotspot dan konfigurasi RADIUS Server untuk autentikasi pengguna) dan Server Ubuntu sebagai penyedia user dan password autentikasi login saat pengguna akses jaringan internet melalui hotspot MikroTik.
2. Pengelola hotspot dapat dengan mudah dalam manajemen akun user dan password (menambahkan atau mengurangi) untuk digunakan oleh pengguna jaringan internet melalui web management DaloRADIUS tanpa harus melakukan konfigurasi user dan password langsung di MikroTik untuk menghindari kesalahan konfigurasi jaringan.
3. Berdasarkan hasil uji implementasi, pengguna yang akan mencoba akses internet melalui hotspot MikroTik akan terlebih dahulu dilakukan autentikasi login. Jika pengguna menggunakan user dan password yang tepat sesuai dengan yang ada pada database FreeRADIUS (yang sudah ditentukan oleh pengelola hotspot), maka pengguna dapat mengakses jaringan internet dengan mudah dan sebaliknya.

## DAFTAR PUSTAKA

- Aziz, A. S., & Safriatullah. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius. *Journal of Informatics and Computer Science*, 7(2), 106–112.
- Fitriani, Wirda, Fachrid Wadly, and Zuhri Ramadhan. 2024. "Network Security Implementation From Ddos Attacks With Mikrotik Routers." *International Journal of Computer Sciences and Mathematics Engineering* 3 (2): 18–29

- Hendarto, E. (2018). Sistem Manajemen User Login Hotspot Mikrotik Dengan Radius Server Menggunakan Raspberry Pi. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 2(2), 72–81.
- Ikhsan, A. M., & Wagito, W. (2023). Implementasi Freeradius Pada Platform Itg Gmedia. *JIKO (Jurnal Informatika Dan Komputer)*, 7(1), 147. <https://doi.org/10.26798/jiko.v7i1.737>
- Pratama, Rahmad Milsa, Sri Wahyuni, and Akhyar Lubis. 2023. “Rancang Bangun Keamanan Koneksi Pribadi Melalui Open VPN Berbasis Cloud.” *INTECOMS: Journal of Information Technology and Computer Science* 6 (1): 30–35. <https://doi.org/10.31539/intecom.v6i1.5368>
- Ramadhan, Zuhri, Fachrid Wadly, and Geby Citra Ananda. 2024. “E-Commerce Application Design With Web-Based Codeigniter Framework” 1 (3): 96–105. <https://doi.org/10.30596/jitcse>
- Tambunan, Marcella D, Candra Tandi, Reinhard Siagian, Habib Muharry Yusdartono, Universitas Sumatera Utara, Institut Agama, Kristen Negeri, and Universitas Sumatera. 2024. “Design of a Technician Attendance System for Internet Network Disturbances at PT Telkom Indonesia Using a Website.” *Journalinstal* 16 (05): 13. <https://journalinstal.cattleyadf.org/index.php/Instal/article/view/297/173>
- Tri, Muhammad, Madja Pandia, and Fachrid Wadly. 2025. “Design and Build a Network Monitoring System Using Nagios at PT . Telkom Access” 2 (1): 47–57
- Ikhsan, Arief Maulana, and Wagito Wagito. 2023. “Implementasi Freeradius Pada Platform Itg Gmedia.” *JIKO (Jurnal Informatika Dan Komputer)* 7 (1): 147. <https://doi.org/10.26798/jiko.v7i1.737>.