



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

**PENERAPAN INTEGRASI FREERADIUS DAN OPENLDAP SEBAGAI
LAYANAN AUTENTIKASI JARINGAN NIRKABEL BERBASIS *CAPTIVE*
PORTAL DI PT ELANG STRATEGI ADIDAYA**

SKRIPSI

FAUZAN NUGRAHA DAULAY

0110218090

PROGRAM STUDI TEKNIK INFORMATIKA

JAKARTA

AGUSTUS 2023



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

**PENERAPAN INTEGRASI FREERADIUS DAN OPENLDAP SEBAGAI
LAYANAN AUTENTIKASI JARINGAN NIRKABEL BERBASIS *CAPTIVE*
PORTAL DI PT ELANG STRATEGI ADIDAYA**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh Strata Satu

FAUZAN NUGRAHA DAULAY

0110218090

PROGRAM STUDI TEKNIK INFORMATIKA

JAKARTA

AGUSTUS 2023

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

NAMA : Fauzan Nugraha Daulay

NIM : 0110218090

Jakarta, 1 Agustus 2023



Fauzan Nugraha Daulay

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh :

Nama : Fauzan Nugraha Daulay

NIM : 0110218090

Program Studi : Teknik Informatika

Judul Skripsi : Penerapan Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis *Captive Portal* Di PT Elang Strategi Adidaya

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknik Terpadu Nurul Fikri.

DEWAN PENGUJI

Pembimbing : Henry Saptono, S.Si., M.Kom.

()

Penguji : April Rustianto, S.Komp., M.T.

()

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi/tugas akhir ini. Penulisan skripsi/tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknik Terpadu Nurul Fikri. Saya menyadari bahwa, tanpa bantuan dan bimbingan berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini sangatlah sulit bagi saya untuk menyelesaikan skripsi/tugas akhir ini. Oleh karena itu, saya mengucapkan terimakasih kepada :

1. Allah SWT yang telah memberikan rahmat, karunia, dan hidayahnya sehingga penulis dapat menyelesaikan penyusunan skripsi/tugas akhir ini.
2. Ibunda tercinta Tati Rohayati yang tiada henti – hentinya memberikan dukungan, doa, kasih sayang, serta semangat sehingga penulis dapat menyelesaikan skripsi/tugas akhir ini.
3. Bapak Dr. Lukman Rosyidi, S.T., M.M., M.T. selaku Ketua Sekolah Tinggi Teknik Terpadu Nurul Fikri.
4. Ibu Tifani Nabarian, S.Kom., M.T.i. selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknik Terpadu Nurul Fikri.
5. Bapak Henry Saptono, S.Si., M.Kom. selaku dosen pembimbing yang telah menyediakan waktu, tenaga, serta pikiran untuk mengarahkan penulis dalam penyusunan skripsi/tugas akhir ini.
6. Bapak April Rustianto, S.Komp., M.T. selaku dosen penguji yang telah bersedia untuk menguji serta memberikan saran dalam penyusunan skripsi/tugas akhir ini.

7. Para dosen di lingkungan Sekolah Tinggi Teknik Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. Jajaran Manajemen PT. Elang Strategi Adidaya yang telah mengizinkan penulis untuk melakukan implementasi terkait skripsi/tugas akhir ini.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan – kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan penulis. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap kepada Tuhan Yang Maha Esa membalas segala kebaikan semua pihak yang telah membantu dalam penyusunan skripsi/tugas akhir ini. Semoga skripsi/tugas akhir ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 1 Agustus 2023

Fauzan Nugraha Daulay

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknik Terpadu Nurul Fikri, saya yang bertanda tangan dibawah ini :

Nama : Fauzan Nugraha Daulay
NIM : 0110218090
Program Studi : Teknik Informatika
Jenis Karya : Skripsi/Tugas Akhir

Demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Sekolah Tinggi Teknik Terpadu Nurul Fikri Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty – Free Right*) atas karya ilmiah saya yang berjudul :

Penerapan Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis *Captive Portal* di PT Elang Strategi Adidaya

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini, STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi/tugas akhir selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Dengan pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 1 Agustus 2023

Yang menyatakan

(Fauzan Nugraha Daulay)



ABSTRAK

Nama : Fauzan Nugraha Daulay

Program Studi : Teknik Informatika

Judul : Penerapan Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis Captive Portal di PT Elang Strategi Adidaya

Jaringan komputer pada saat ini sudah menjadi sebuah kebutuhan yang utama bagi sebuah organisasi, institusi ataupun lembaga untuk mendukung berjalannya operasional mereka. Jaringan nirkabel adalah bentuk dari jaringan komputer yang sudah wajib dibangun oleh sebuah organisasi untuk tujuan berkomunikasi hingga bertukar data. Dalam membangun jaringan nirkabel, keamanan sebuah jaringan tersebut tentu harus menjadi sebuah perhatian, seorang pengelola jaringan memerlukan sebuah konsep untuk menjaga jaringan nirkabel agar hanya memiliki otorisasi yang dapat terkoneksi ke dalam jaringan nirkabel karena tentu banyak data – data rahasia sebuah organisasi yang tidak boleh dilihat bahkan diubah oleh orang di luar organisasi. *Captive portal* dapat menjadi sebuah solusi untuk mengamankan jaringan nirkabel, dengan dukungan OpenLDAP dan FreeRADIUS dapat memudahkan seorang pengelola jaringan untuk mengelola jaringan nirkabel dalam mendaftarkan pengguna yang berhak untuk terhubung ke dalam jaringan nirkabel. Dengan OpenLDAP yang sudah tersedia pada layanan *mail server* khususnya zimbra, pengelola jaringan hanya perlu melakukan pendaftaran pengguna pada zimbra *mail server* sehingga pengguna mendapatkan otorisasi seluruh fasilitas yang tersedia pada organisasi.

Kata Kunci : jaringan nirkabel, *captive portal*, *openldap*, *freeradius*

ABSTRACT

Name : Fauzan Nugraha Daulay
Study Program : Informatics Engineering
Title : *Implementation of FreeRADIUS and OpenLDAP Integration as a Captive Portal-Based Wireless Network Authentication Service at PT Elang Strategi Adidaya*

The computer network in the present time has become a foremost requirement for an organization, institution, or agency to support their operations. A wireless network is a form of computer network that must be established by an organization for the purpose of communication and data exchange. In constructing a wireless network, the security of such a network must undoubtedly be a concern. A network administrator requires a concept to safeguard the wireless network so that only authorized individuals can connect to it since there are certainly many confidential data of an organization that should not be viewed or altered by outsiders. A captive portal can be a solution to secure the wireless network, with the support of OpenLDAP and FreeRADIUS, making it easier for a network administrator to manage the wireless network by registering users who are entitled to connect to the wireless network. With OpenLDAP already available in the mail server, particularly zimbra, the network administrator only needs to register users in the zimbra mail server, enabling users to obtain authorization for all the facilities available in the organization.

Keyword : *wireless network, captive portal, openldap, freeradius*

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	vi
ABSTRAK.....	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABLE	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah	2
1.3 Tujuan dan Manfaat Penelitian.....	3
1.3.1 Tujuan Penelitian.....	3
1.3.2 Manfaat Penelitian.....	3
1.2. Batasan Masalah	3
1.3. Sistematika Penulisan	4
BAB II LANDASAN TEORI.....	5
2.1 Tinjauan Pustaka.....	5
2.1.1 Jaringan Komputer	5
2.1.2 Jaringan Nirkabel	9
2.1.3 Keamanan Jaringan Nirkabel	12
2.1.4 RADIUS	15
2.1.5 FreeRADIUS	18
2.1.6 OpenLDAP	19
BAB III METODOLOGI PENELITIAN.....	23
3.1 Jenis Metode Penelitian	23
3.2 Tahapan Penelitian.....	24
3.2.1 Studi Literatur	25
3.2.2 Analisa Kebutuhan	25
3.2.3 Perancangan Sistem.....	25
3.2.4 Implementasi	25
3.2.5 Pengujian.....	26

3.2.6 Evaluasi	26
3.3 Lingkungan Penelitian	26
3.4 Alat dan Bahan Penelitian	26
3.5 Waktu Penelitian.....	27
BAB IV RANCANGAN SISTEM	28
4.1 Analisis Kebutuhan.....	28
4.1.1 Analisis Kebutuhan Perangkat Keras	28
4.1.2 Analisis Kebutuhan Perangkat Lunak	29
4.2 Perancangan Sistem	31
4.2.1 Perancangan Arsitektur Sistem Logika	31
4.2.2 Perancangan Arsitektur Sistem Fisik	32
4.3 Perancangan Pengujian	33
4.4 Skenario Pengujian	34
4.4.1 Skenario Pengujian <i>Log In Captive Portal</i> Menggunakan Laptop	35
4.4.2 Skenario Pengujian <i>Log In Captive Portal</i> Menggunakan <i>Smartphone</i> ...	35
BAB V IMPLEMENTASI DAN PENGUJIAN	37
5.1 Implementasi.....	37
5.1.1 Persiapan	37
5.1.2 Instalasi dan Konfigurasi.....	39
5.2 Pengujian Penerapan Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis <i>Captive Portal</i> Di PT Elang Strategi Adidaya.....	56
5.2.1 Pengujian Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis <i>Captive Portal</i> menggunakan perangkat laptop	56
5.2.2 Pengujian Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis <i>Captive Portal</i> menggunakan perangkat <i>smartphone</i>	58
BAB VI KESIMPULAN DAN SARAN.....	62
6.1 Kesimpulan	62
6.2 Saran	62
LAMPIRAN	65

DAFTAR GAMBAR

Gambar 2.1 : Local Area Network	5
Gambar 2.2 : Topologi Bus	6
Gambar 2.3 : Topologi Ring.....	6
Gambar 2.4 : Topologi Star	7
Gambar 2.5 : Topologi Mesh.....	8
Gambar 2.6 : Metropolitan Area Network.....	8
Gambar 2.7 : Wide Area Network.....	9
Gambar 2.8 : Hotspot.....	10
Gambar 2.9 : Wide Personal Area Networks	10
Gambar 2.10 : Wireless Metropolitan Area Networks	11
Gambar 2.11 : Wireless Wide Area Networks	11
Gambar 2.12 : MAC Filtering	12
Gambar 2.13 : Wired Equivalent Privacy.....	13
Gambar 2.14 : WPA-PSK/WPA2-PSK.....	14
Gambar 2.15 : Captive Portal	15
Gambar 2.16 : Access-Request.....	16
Gambar 2.17 : Access-Accept	16
Gambar 2.18 : Access-Reject	17
Gambar 2.19 : Access-Challenge	17
Gambar 3.1 : Flow Chart Tahapan Penelitian	24
Gambar 3.2 : Timeline Waktu Penelitian	27
Gambar 4.2 : Rancangan Arsitektur Sistem Logika	31
Gambar 4.3 : Rancangan Arsitektur Sistem Fisik	32
Gambar 4.4 : Rancangan Pengujian	33
Gambar 5.1 : Login Web Router Gateway	44
Gambar 5.2 : Menu Captive Portal.....	45
Gambar 5.3 : Formulir Captive Portal	46
Gambar 5.4 : Ubah Back End Captive Portal (1)	47
Gambar 5.5 : Ubah Back End Captive Portal (2)	48
Gambar 5.6 : Ubah Front End Captive Portal (1).....	49
Gambar 5.7 : Ubah Front End Captive Portal (2).....	50
Gambar 5.8 : Ubah Front End Captive Portal (3).....	51
Gambar 5.9 : Ubah Front End Captive Portal (4).....	52
Gambar 5.10 : Simpan Konfigurasi Captive Portal.....	53
Gambar 5.11 : Laptop Terkoneksi Pada Jaringan Nirkabel ESTRADA	56
Gambar 5.12 : Login Page Pada Laptop.....	57
Gambar 5.13 : Verifikasi Status Perangkat Laptop Pada Jaringan Nirkabel ESTRADA	57
Gambar 5.14 : Smartphone Terkoneksi Pada Jaringan Nirkabel ESTRADA	59
Gambar 5.15 : Login Page Pada Smartphone.....	60
Gambar 5.16 : Verifikasi Status Perangkat Smartphone Pada Jaringan Nirkabel ESTRADA.....	61

DAFTAR TABLE

Tabel 2.1 : Penelitian Terkait	22
Tabel 4.1 : Spesifikasi Router HSG.....	29
Tabel 4.2 : Penggunaan Perangkat Lunak	30
Tabel 4.3 : Skenario Pengujian Log In Captive Portal Menggunakan Laptop.....	35
Tabel 4.4 : Skenario Pengujian Log In Captive Portal Menggunakan Smartphone.....	36
Tabel 5.1 : Hasil Pengujian Menggunakan Laptop	58
Tabel 5.2 : Hasil Pengujian Menggunakan Smartphone	61

BAB I PENDAHULUAN

1.1 Latar Belakang

Dewasa ini teknologi mengalami perkembangan yang pesat, berbagai teknologi tengah dikembangkan pada era ini, salah satu yang paling dekat dengan masyarakat adalah teknologi jaringan komputer. Jaringan komputer saat ini sudah menjadi sebuah hal yang sangat dibutuhkan oleh setiap orang hingga sebuah instansi.

Dalam kehidupan sehari – hari, jenis jaringan yang sering digunakan dan paling dekat dengan masyarakat adalah jaringan nirkabel, dimana jaringan nirkabel dapat langsung terhubung ke *smartphone* maupun laptop tanpa perlu menarik kabel dahulu. Dalam penggunaannya, jaringan nirkabel biasa disediakan dalam lingkungan umum untuk memudahkan pengunjung mendapatkan akses *internet*. Dalam lingkungan pekerjaan, jaringan nirkabel juga banyak disediakan oleh sebuah perusahaan sebagai fasilitas yang dapat digunakan oleh karyawannya agar mendapatkan akses *internet* untuk memudahkan pekerjaan. Di balik fasilitas jaringan nirkabel yang disediakan oleh perusahaan, tentu ada yang mengelola agar jaringan nirkabel tetap aman dan berjalan dengan baik, agar kondisi jaringan nirkabel tetap aman dan berjalan dengan baik, dibutuhkan keamanan jaringan nirkabel yang memiliki bentuk keamanan dimana hanya individu yang mempunyai hak saja yang dapat mengakses jaringan nirkabel sehingga performa jaringan nirkabel dapat lebih baik karena individu selain itu tidak dapat mengakses jaringan nirkabel.

Dalam kondisi ini, dibutuhkan *captive portal* sebagai sistem autentikasi jaringan nirkabel, dimana *captive portal* menyediakan *user* dan *password* untuk masing masing pengguna, sehingga seorang pengelola dapat memantau pemakaian bahkan dapat membatasi pemakaian jaringan nirkabel (Aryeh, Asante, & Y Danso, 2016).

Pada studi kasusnya, PT Elang Strategi Adidaya memiliki jaringan nirkabel dimana setiap *access point* sudah terhubung dengan sebuah *controller* namun pada masing – masing *access point* memiliki SSID yang berbeda – beda setiap lantainya sehingga menyulitkan karyawan sebagai pengguna jaringan nirkabel saat berpindah dari lantai 1 ke lantai lainnya karena pengguna akan diminta untuk melakukan autentikasi ulang. Pada kondisi

yang sudah ada, jenis keamanan jaringan nirkabel yang digunakan adalah WPA2-PSK, dimana jika menggunakan keamanan jaringan nirkabel ini siapapun dapat terhubung dengan jaringan nirkabel dengan hanya mengetahui *password* dari jaringan nirkabel. Dalam hal ini, penulis memberikan solusi dengan mengubah seluruh SSID pada setiap *access point* menjadi sama, dan mengubah jenis keamanan jaringan nirkabel dari WPA2-PSK menjadi menggunakan *captive portal*. Dengan adanya *captive portal* memungkinkan jaringan nirkabel yang ada pada PT Elang Strategi Adidaya hanya dapat digunakan oleh karyawan PT Elang Strategi Adidaya karena pengguna diharuskan melakukan autentikasi menggunakan *username* serta *password* yang diberikan oleh seorang *network administrator*. Namun kendala dari instalasi *captive portal* adalah setiap pengguna harus mengingat *username* dan *password* baru yang diberikan oleh *network administrator* sehingga dengan kondisi ini memungkinkan pengguna akan lupa dengan *username* dan *password* yang diberikan. Solusi dari masalah ini adalah *network administrator* melakukan integrasi dengan layanan – layanan yang sering dipakai oleh karyawan PT Elang Strategi Adidaya, salah satu layanan yang sering dipakai adalah zimbra *mail server*. *Network administrator* dapat memanfaatkan zimbra *mail server* sebagai sistem autentikasi karena terdapat *openldap* di dalamnya dan membuat *freeradius* sebagai penghubung antara *router gateway* dengan *openldap* sehingga jaringan nirkabel dengan menggunakan sistem keamanan jaringan *captive portal* memiliki *database* yang sama, dengan itu karyawan sebagai pengguna jaringan nirkabel tidak perlu mengingat banyak *username* dan *password*.

1.2 Perumusan Masalah

Berdasarkan latar belakang sebelumnya, maka dapat dirumuskan permasalahan sebagai berikut.

1. Bagaimana rancangan penerapan integrasi *freeradius* dan *openldap* sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya?
2. Bagaimana efektifitas dari penerapan integrasi *freeradius* dan *openldap* sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya?

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut.

1. Merancang dan menerapkan integrasi freeradius dan openldap sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya.
2. Mengetahui efektifitas dari penerapan integrasi freeradius dan openldap sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya.

1.3.2 Manfaat Penelitian

Manfaat penelitian yang diharapkan dari penelitian ini yaitu.

1. Memberikan kemudahan pengelolaan jaringan nirkabel PT. Elang Strategi Adidaya terkait dengan penerapan autentikasi akses jaringan nirkabel.
2. Memudahkan pengguna jaringan nirkabel dalam melakukan autentikasi dengan cukup mengetahui *user* dan *password* yang sudah terdaftar di *database* terpusat.
3. Menghasilkan karya tulis yang dapat menjadi salah satu referensi di dalam penelitian atau penerapan autentikasi terpusat untuk jaringan nirkabel.

1.2. Batasan Masalah

Batasan masalah dalam penelitian ini yaitu.

1. Dalam penelitian ini penulis hanya menggunakan perangkat *router* dan *access point* dengan merek Ransnet.
2. Pada autentikasi jaringan nirkabel penulis hanya berfokus pada autentikasi menggunakan *captive portal* yang sudah disediakan oleh *router* Ransnet HSG-100.
3. Penulis menggunakan layanan openldap yang sudah ada pada layanan zimbra *mail server* PT Elang Strategi Adidaya.
4. Dalam penelitian ini penulis tidak membahas proses kustomisasi UI/UX dari *login page* pada *captive portal* yang digunakan pada *router* Ransnet HSG-100.
5. Dalam penelitian ini tidak membahas metode enkripsi yang digunakan.

1.3. Sistematika Penulisan

Untuk memberikan kemudahan bagi pembaca dalam penyusunan penelitian ini, penulis menjabarkan penelitian ini secara singkat yang dapat diuraikan sebagai berikut.

A. BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan.

B. BAB II LANDASAN TEORI

Bab ini akan mengkaji hal – hal yang berkaitan dengan topik yang dibahas, dan membahas singkat teori yang diperlukan dalam penelitian ini.

C. BAB III METODELOGI PENELITIAN

Bab ini menjelaskan tentang jenis metode penelitian yang digunakan, tahap – tahapan, lingkungan, alat dan bahan, hingga waktu penelitian.

D. BAB IV RANCANGAN SISTEM

Bab ini membahas tentang rancangan sistem dari penerapan integrasi freeradius dan openldap sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya.

E. BAB V IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi bahasan terkait implementasi beserta rancangan dari penerapan integrasi freeradius dan openldap sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya.

F. BAB VI KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan, serta saran pengembangan terhadap penelitian selanjutnya

BAB II LANDASAN TEORI

2.1 Tinjauan Pustaka

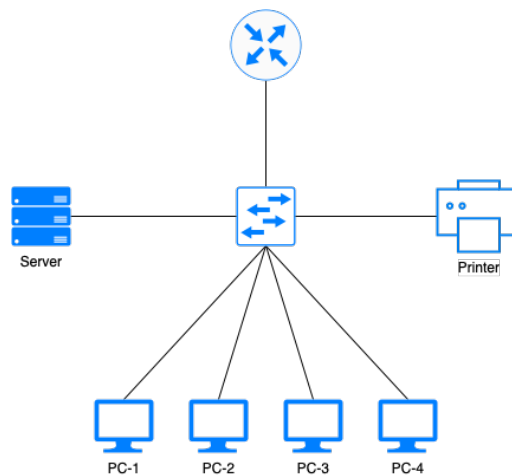
Pada bab ini, penulis akan menjabarkan teori – teori pendukung di dalam perancangan serta implementasi autentikasi jaringan nirkabel terpusat menggunakan freeradius dan openldap.

2.1.1 Jaringan Komputer

Jaringan komputer adalah sistem yang menghubungkan dua perangkat atau lebih untuk melakukan komunikasi dan pertukaran data menggunakan media komunikasi berupa kabel maupun nirkabel (Simargolang, Widarma, & Irawan, 2021).

2.1.1.1 *Local Area Network*

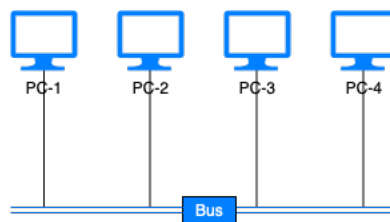
Local Area Networks atau biasa disebut LAN, adalah jaringan komputer dengan ruang lingkup terbatas, jenis jaringan ini banyak digunakan untuk gedung, kampus, pabrik, dan lainnya yang memiliki skala kecil (Simargolang et al., 2021). Di dalam LAN terdapat beberapa jenis topologi jaringan komputer, antara lainnya adalah topologi *bus*, topologi *ring*, topologi *star*, dan topologi *mesh*.



Gambar 2.1 : *Local Area Network*

2.1.1.1.1 Topologi Bus

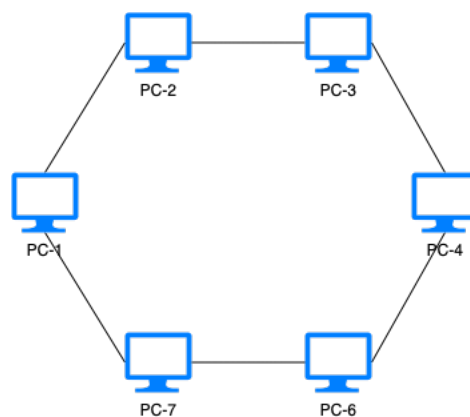
Topologi ini adalah topologi yang sederhana, dimana semua perangkat terhubung pada sebuah kabel (*bus*), dimana kabel tersebut terhubung juga ke perangkat lain, sehingga perangkat dapat menerima maupun mengirim informasi ke perangkat lain sepanjang kabel (*bus*) (Simargolang et al., 2021).



Gambar 2.2 : Topologi Bus

2.1.1.1.2 Topologi Ring

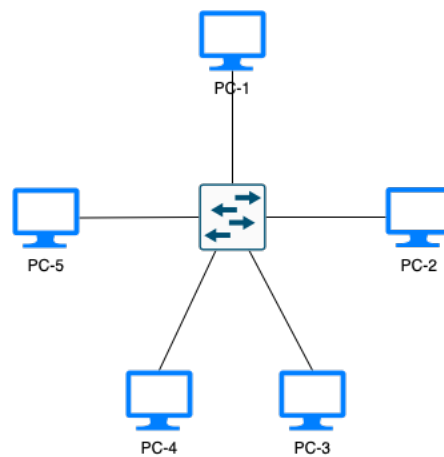
Topologi ini bekerja dengan cara mengirim data secara langsung sepanjang jaringan, setiap data yang dikirim akan diperiksa alamatnya oleh masing masing terminal yang dilewatinya (Simargolang et al., 2021).



Gambar 2.3 : Topologi Ring

2.1.1.1.3 Topologi *Star*

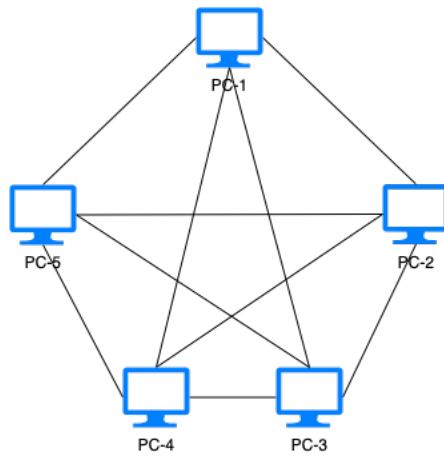
Sesuai dengan namanya, topologi ini berbentuk seperti bintang, setiap komputer dalam jaringan terhubung dengan pusat, terminal pusat tersebut berperan sebagai pengatur dan pengendali semua komunikasi data (Simargolang et al., 2021).



Gambar 2.4 : Topologi *Star*

2.1.1.1.4 Topologi *Mesh*

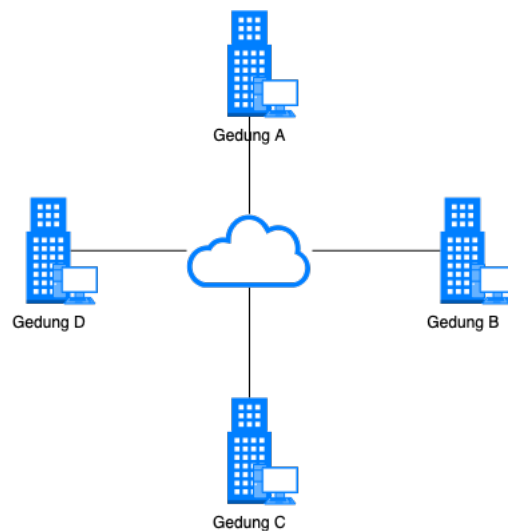
Topologi ini menghubungkan secara fisik masing – masing terminal untuk membentuk jaringan, dalam implementasi topologi *mesh* tingkat kerumitan sebanding dengan jumlah terminal yang akan diimplementasi (Syafrizal, 2005).



Gambar 2.5 : Topologi Mesh

2.1.1.2 Metropolitan Area Network

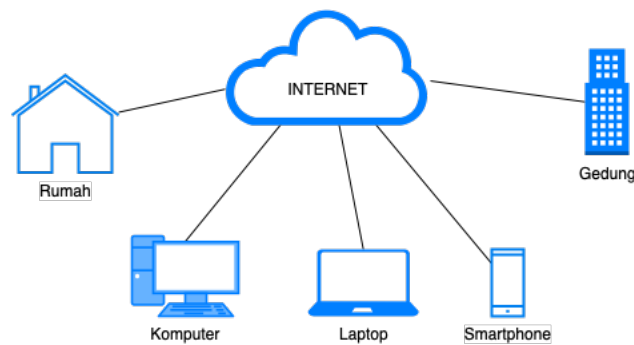
Metropolitan Area Networks (MAN) merupakan jaringan komputer yang mencakup jarak cukup jauh, contoh dari jenis jaringan ini adalah menghubungkan jaringan komputer antargedung dalam satu kota maupun antar kota (Simargolang et al., 2021).



Gambar 2.6 : Metropolitan Area Network

2.1.1.3 *Wide Area Network*

Wide Area Networks (WAN) merupakan jaringan komputer yang memiliki radius tanpa batasan geografis, seperti mencakup antar negara maupun antar benua (Simargolang et al., 2021).



Gambar 2.7 : *Wide Area Network*

2.1.2 Jaringan Nirkabel

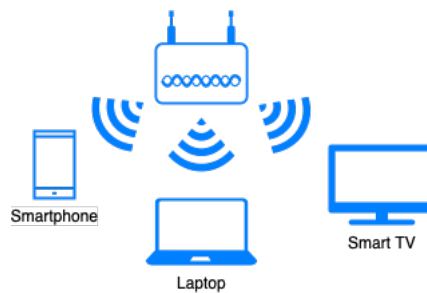
Jaringan nirkabel merupakan mekanisme pertukaran data antar perangkat tanpa memerlukan koneksi fisik, dimana menggunakan frekuensi radio sebagai media untuk mentransmisikan data, saat ini ada 4 tipe jaringan nirkabel, yaitu WLANs (*Wireless Local Area Networks*), WPANs (*Wireless Personal Area Networks*), WMANs (*Wireless Metropolitan Area Networks*), dan WWANs (*Wireless Wide Area Networks*) (Karygiannis & Owens, 2002).

2.1.2.1 *Wireless Local Area Networks*

Wireless Local Area Networks (WLANs) adalah suatu jaringan nirkabel yang mencakup area kecil seperti di dalam area sekolah maupun gedung untuk mendapatkan akses ke *internet*, dalam penggunaan sehari – hari contoh bentuk WLANs adalah *hotspot* (Sharma & Dhir, 2014).

2.1.2.1.1 Hotspot

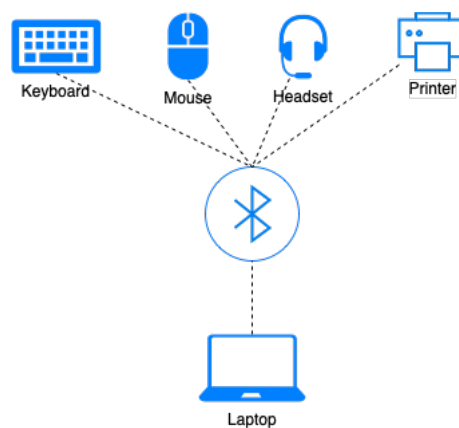
Hotspot merupakan bentuk layanan jaringan WLANs yang disediakan oleh sekolah hingga perusahaan sebagai fasilitas untuk individu sebagai sarana mendapatkan akses *internet* (Sondag & Feher, 2007).



Gambar 2.8 : Hotspot

2.1.2.2 Wireless Personal Area Networks

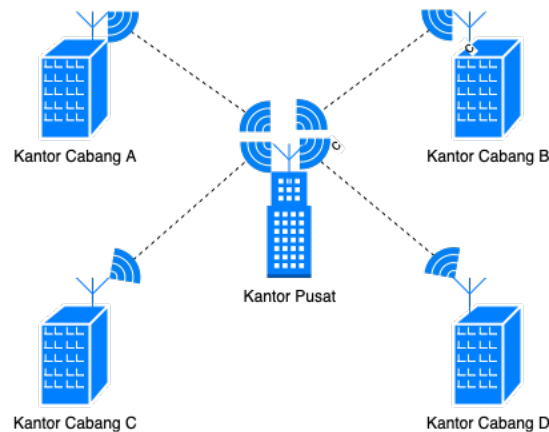
Wireless Personal Area Networks (WPANs) merupakan jaringan nirkabel yang tidak melibatkan infrastruktur atau konektivitas ke jaringan luar, teknologi yang digunakan WPANs adalah *infra red* dan *bluetooth* untuk menghubungkan sebuah gawai ke perangkat periferan (Sharma & Dhir, 2014).



Gambar 2.9 : Wide Personal Area Networks

2.1.2.3 *Wireless Metropolitan Area Networks*

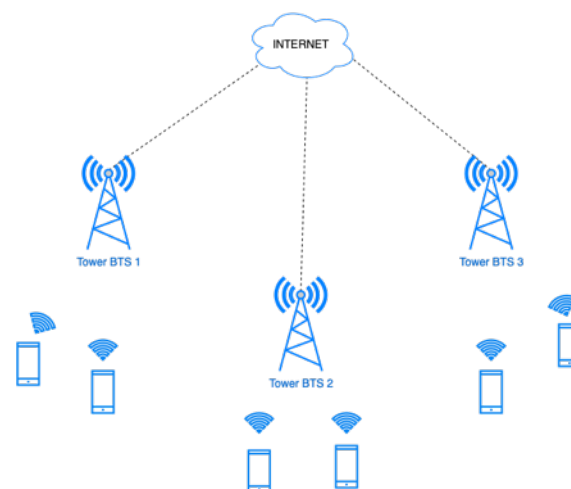
Wireless Metropolitan Area Networks (WMANs) adalah koneksi jaringan nirkabel area dalam kota seperti menghubungkan koneksi antar gedung dalam satu kota, dimana dapat dijadikan sebagai jaringan alternatif dari kabel fiber (Sharma & Dhir, 2014).



Gambar 2.10 : *Wireless Metropolitan Area Networks*

2.1.2.4 *Wireless Wide Area Networks*

Wireless Wide Area Networks (WWANs) adalah jaringan nirkabel yang memiliki skala area terluas, dimana mencakup antar kota, bahkan antar negara, contohnya seperti jaringan seluler yang digunakan pada *smartphone* termasuk ke dalam jaringan nirkabel WWANs (Sharma & Dhir, 2014).



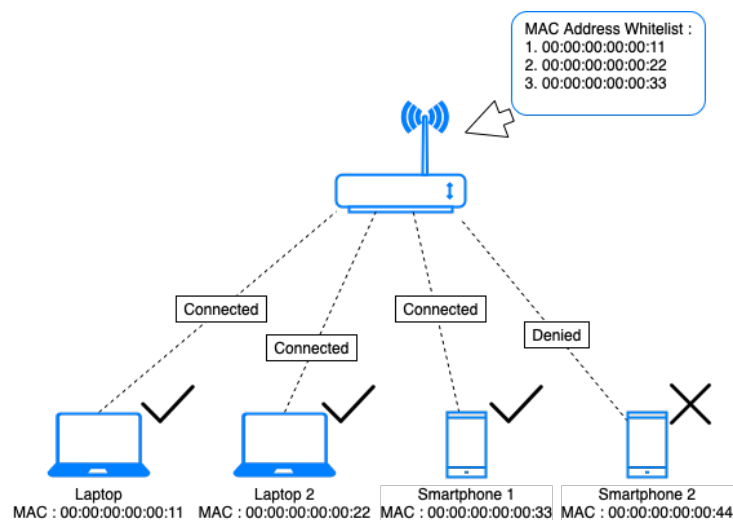
Gambar 2.11 : *Wireless Wide Area Networks*

2.1.3 Keamanan Jaringan Nirkabel

Keamanan jaringan nirkabel merupakan sebuah hal yang perlu diperhatikan oleh seorang pengelola jaringan, karena keamanan jaringan nirkabel menyangkut privasi dimana dapat merugikan penggunanya. Suatu perangkat lebih berpotensi diretas pada jaringan nirkabel dibandingkan LAN, karena tidak perlu menghubungkan secara fisik agar terhubung (Gondohanindijo, 2012).

2.1.3.1 MAC Filtering

Setiap perangkat yang dapat terkoneksi ke sebuah jaringan tentu memiliki sebuah MAC address sehingga dapat terjadinya serangan seperti *spoofing* (Gondohanindijo, 2012). Cara kerja pengamanan ini adalah dengan mendaftarkan masing – masing MAC address perangkat yang ingin terhubung ke sebuah jaringan nirkabel sebagai *white list* (Gondohanindijo, 2012).

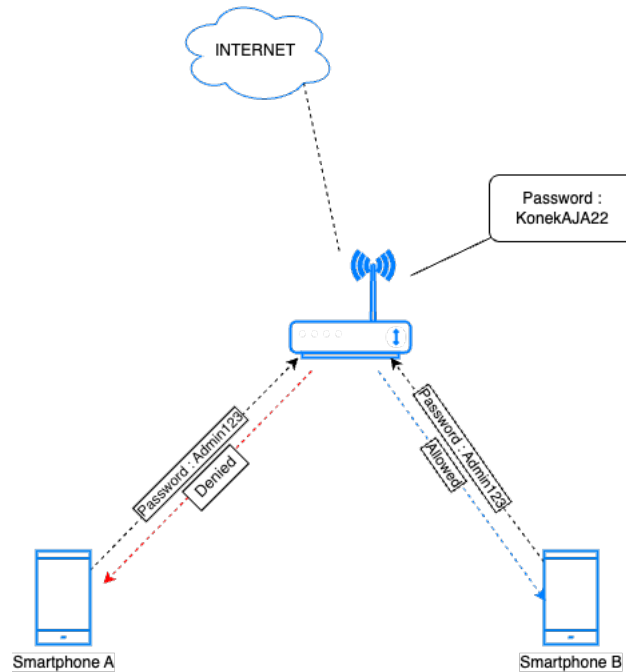


Gambar 2.12 : MAC Filtering

2.1.3.2 WEP (Wired Equivalent Privacy)

WEP (*Wired Equivalent Privacy*) adalah standar keamanan terenkripsi pertama yang digunakan pada jaringan nirkabel (Gondohanindijo, 2012). WEP merupakan sebuah metode pengamanan jaringan nirkabel yang disebut juga *Shared Key Authentication*, metode tersebut adalah metode autentikasi menggunakan kata sandi yang dimasukkan oleh pengelola ke pengguna, dan *access point*, saat pengguna mencoba bergabung dengan

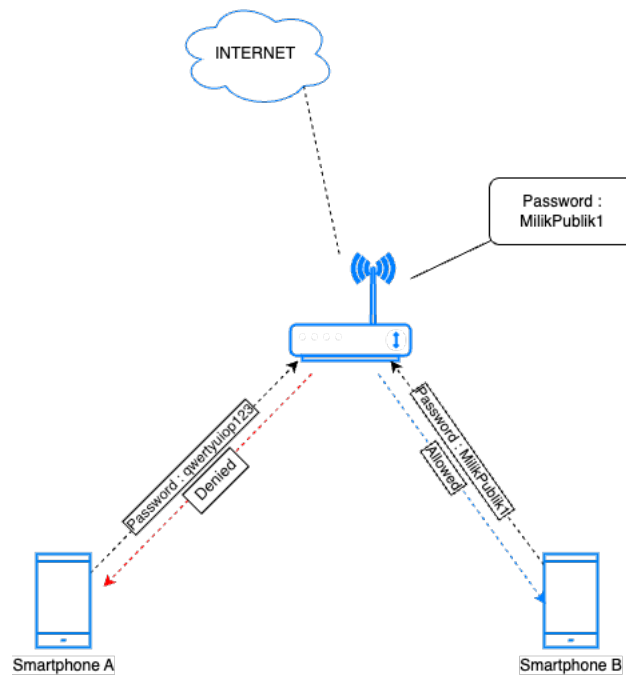
jaringan nirkabel, kata sandi yang dimiliki pengguna harus sama dengan kunci yang dimiliki *access point* (Gondohanindijo, 2012).



Gambar 2.13 : *Wired Equivalent Privacy*

2.1.3.3 WPA-PSK/WPA2-PSK

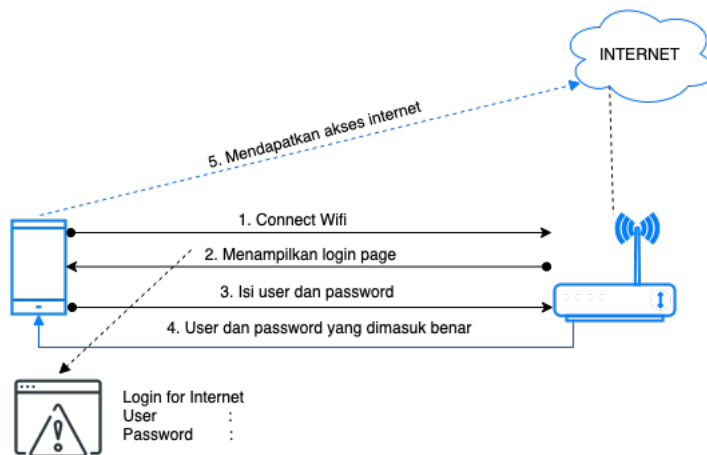
WPA (*Wi-fi Protected Access*) merupakan teknologi keamanan jaringan nirkabel yang dapat diimplementasikan pada pengguna rumahan, perkantoran, maupun publik. WPA-PSK/WPA2-PSK menggunakan *password* statik dengan menggunakan TKIP (*Temporal Key Integrity Protocol*) yang bersifat dinamis dimana dapat berubah setelah 10.000 paket data ditransmisikan (Gondohanindijo, 2012).



Gambar 2.14 : WPA-PSK/WPA2-PSK

2.1.3.4 Captive Portal

Captive portal merupakan teknik autentikasi dan pengamanan data terhadap jaringan internal (Siregar & Prihanto, 2019). *Captive portal* tidak mengizinkan adanya penggunaan jaringan nirkabel sampai pengguna melakukan autentikasi ke dalam sistem, ketika pengguna pertama kali terkoneksi ke jaringan nirkabel, maka pengguna akan diarahkan secara otomatis ke sebuah halaman situs web untuk melakukan autentikasi ataupun registrasi (Siregar & Prihanto, 2019).

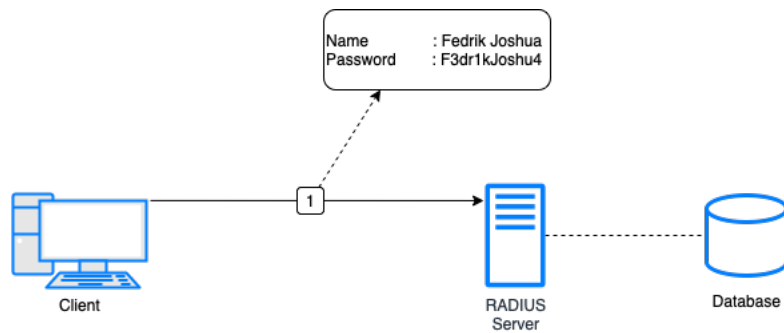


Gambar 2.15 : Captive Portal

2.1.4 RADIUS

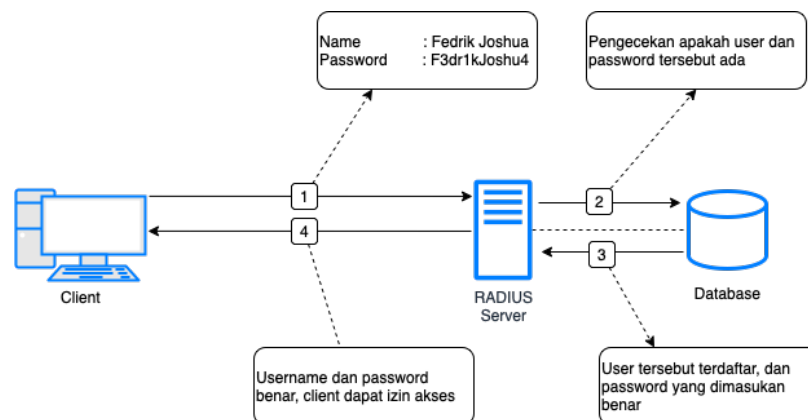
RADIUS adalah protokol kontrol akses yang memverifikasi serta mengautentikasi pengguna berdasarkan metode tanggapan yang umum digunakan (Hassell, 2002). Dalam kehidupan sehari – hari RADIUS sering digunakan untuk autentikasi sebuah situs web atau aplikasi. Dalam penggunaannya, sebuah NAS (*Network Access Server*) berperan sebagai *client* dari RADIUS, dimana *client* tersebut bertanggung jawab sebagai gerbang untuk mengirim informasi ke RADIUS *Server* (Rigney, Rubens, Simpsons, & Willens, 2000). RADIUS digunakan untuk melakukan proses verifikasi identitas bahwa yang mengakses adalah benar seseorang yang mempunyai hak akses. Proses kerja RADIUS dikenal sebagai AAA, yang terdiri dari *Authentication*, *Authorization*, dan *Accounting* (Hassell, 2002). Terdapat 4 paket yang didalam proses autentikasi RADIUS, yaitu sebagai berikut.

- A. *Access-Request*, paket ini dikirimkan kepada RADIUS *server* dengan membawa informasi yang digunakan untuk menentukan apakah pengguna diizinkan untuk mengakses NAS atau layanan lainnya (Rigney et al., 2000).



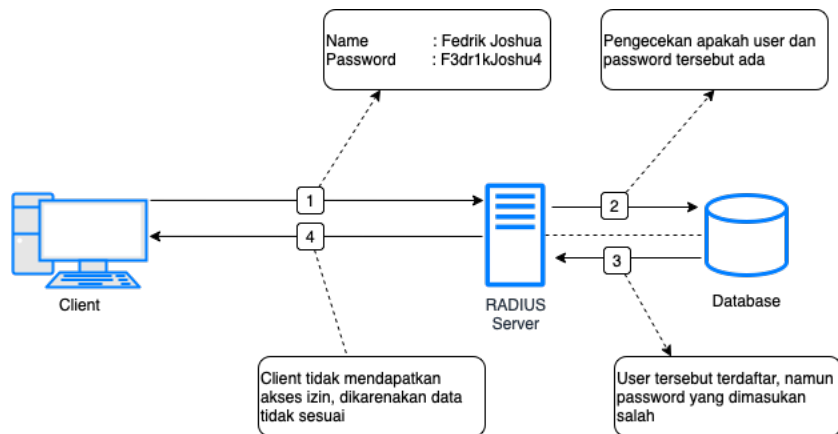
Gambar 2.16 : Access-Request

- B. *Access-Accept*, paket ini dikirimkan oleh RADIUS server kepada NAS untuk memberikan hasil validasi bahwa pengguna memiliki izin dan memberikan informasi yang diperlukan NAS dalam mengirimkan layanannya kepada pengguna (Rigney et al., 2000).



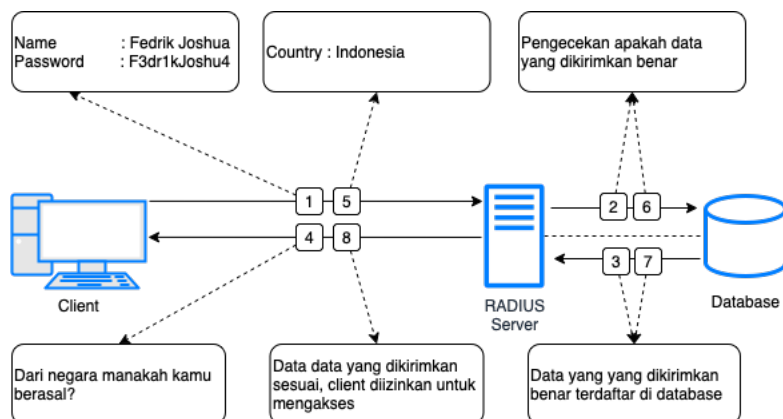
Gambar 2.17 : Access-Accept

- C. *Access-Reject*, paket ini dikirimkan oleh RADIUS kepada NAS untuk memberikan hasil validasi bahwa pengguna tidak memiliki izin untuk menggunakan layanan, dikarenakan RADIUS menerima data – data yang tidak sesuai dengan basis data (Rigney et al., 2000).



Gambar 2.18 : Access-Reject

- D. *Access-Challenge*, paket ini dikirimkan oleh RADIUS kepada NAS untuk diteruskan kepada pengguna untuk memastikan kembali bahwa pengguna adalah seorang yang mempunyai izin untuk mengakses, saat mengirimkan paket ini, RADIUS sekaligus mengirimkan juga pake *access-request* untuk memvalidasi pengguna dengan menanggapi *challenge* yang diberikan RADIUS, jika berhasil pengguna akan mendapatkan izin untuk mengakses layanan (Rigney et al., 2000).



Gambar 2.19 : Access-Challenge

2.1.4.1 Authentication

Authentication adalah proses memverifikasi identitas seseorang (Hassell, 2002). Dalam penggunaannya, biasa ditemukan formulir untuk verifikasi identitas menggunakan *user* dan *password*, dimana *password* tersebut mempresentasikan bahwa *user* yang mencoba akses itu autentik pengguna aslinya.

2.1.4.2 Authorization

Authorization adalah proses dimana melakukan pemberian peraturan hak akses untuk menentukan pengguna yang sudah terautentikasi dapat melakukan apa saja didalam sistem (Hassell, 2002). Contoh penggunaannya, seorang karyawan mengakses situs web ERP kantor menggunakan akunnya, setelah melakukan autentikasi dan terotorisasi, karyawan tersebut tidak dapat mengakses menu yang digunakan HRD untuk menilai kinerja karyawan maupun gaji karyawan.

2.1.4.3 Accounting

Accounting adalah proses yang melakukan dokumentasi terhadap penggunaan layanan yang dimanfaatkan oleh pengguna, hal ini dapat mencakup durasi waktu akses, atau jumlah data yang dikirim maupun diterima pengguna selama sesi masih berlangsung (Hassell, 2002). Dalam kegunaannya, *accounting* ini berguna bagi seorang pengelola untuk menentukan kapasitas serta memprediksi beban sistem dimasa yang akan mendatang (Hassell, 2002).

2.1.5 FreeRADIUS

FreeRADIUS adalah sebuah projek *open source* yang fiturnya banyak diimplementasikan pada protokol RADIUS dengan berbagai perkembangannya (Walt, 2011). FreeRADIUS pertama kali dikembangkan pada tahun 1999 setelah tidak ada kepastian masa depan dari Livingston RADIUS *Server*. FreeRADIUS memiliki reputasi yang bagus dan mampu bersaing dengan RADIUS *server* komersial, dengan moto komunitas ini adalah “*Server* RADIUS paling populer di dunia”, untuk saat ini FreeRADIUS tidak tertandingi dan pernyataan tersebut sangat valid (Walt, 2011). Walt (2011) menulis bahwa terdapat kelebihan dan kekurangan pada FreeRADIUS, diantaranya sebagai berikut.

A. Kelebihan

- a) *Open source*, dalam hal ini FreeRADIUS bukan hanya gratis dalam pemakaian, melainkan dibebaskan untuk mengadaptasi, mengganti, mengembangkan, serta memperbaiki jika dibutuhkan. FreeRADIUS dirilis dengan lisensi GNU (*General Public License*)
- b) Modular, FreeRADIUS datang dengan banyak modul yang sudah terpasang. Pengguna juga dapat membuat modul tersendiri sesuai kebutuhan dalam penggunaan FreeRADIUS.
- c) Banyak *digunakan*, banyaknya penggunaan FreeRADIUS dapat memudahkan pengelola untuk mencari referensi dalam mengelola bahkan mengembangkan FreeRADIUS.
- d) Memiliki komunitas yang aktif, dikarenakan memiliki skala pengguna yang besar, memungkinkan seseorang memiliki masalah yang sama dengan masalah yang sedang dihadapi.
- e) Informasi yang tersedia, karena masifnya pengguna FreeRADIUS dipastikan semua informasi yang dibutuhkan tersedia dari penjuru dunia.
- f) Dukungan berbayar, pengembang inti dari FreeRADIUS memberikan dukungan berbayar.
- g) Ketersediaan perangkat lunak, FreeRADIUS sudah tersedia di berbagai sistem operasi, terutama pada semua distribusi linux yang populer.

B. Kekurangan

- a) Kompleksitas, FreeRADIUS memiliki perangkat lunak dengan pilihan opsi konfigurasi, jika tidak berhati – hati maka dapat terjadi kerusakan pada sistem.
- b) Kerentanan, beberapa kerentanan dilaporkan pada waktu lalu, namun sudah diperbaiki pada versi update selanjutnya.

2.1.6 OpenLDAP

Lightweight Directory Access Protocol atau yang biasa disebut LDAP, LDAP pada awalnya dirancang menjadi protokol jaringan yang menyediakan akses alternatif ke *directory server* yang ada (Butcher, 2007). OpenLDAP pertama kali dikembangkan oleh

Kurt Zeilenga, dan Horward Chu pada tahun 1998, mereka mengembangkan basis kode Universitas Michigan sehingga menghasilkan OpenLDAP dimana saat ini sangat populer dan tersedia di berbagai distribusi linux (Butcher, 2007). Di dalam bukunya yang berjudul *Mastering OpenLDAP*, Butcher (2007) menulis bahwa terdapat struktur teknis yang dipecah sebagai berikut.

- A. *Servers*, *server* utama dari LDAP adalah SLDAP (*Stand-alone Lightweight Access Protocol*). *Server* ini menyediakan *tree information directory*. *Server* dapat menyimpan data direktori secara lokal maupun hanya akses dari jaringan eksternal.
- B. *Clients*, *client* mengakses LDAP *server* menggunakan protokol jaringan LDAP. *Client* meminta *server* untuk melakukan operasi atas nama mereka. Dalam penggunaannya *client* diharuskan terhubung dahulu ke *server* direktori, lalu melakukan autentikasi untuk melakukan operasi lain seperti mencari, memodifikasi, menambahkan, serta menghapus data.
- C. *Utilities*, struktur ini bekerja tidak menggunakan protokol LDAP, melainkan struktur ini melakukan manipulasi data pada *low-level* tanpa membutuhkan mediasi oleh *server*. Dalam penggunaannya, struktur ini digunakan untuk membantu pemeliharaan *server*.
- D. *Libraries*, terdapat *library* OpenLDAP yang dipisahkan antara LDAP. *Library* menyediakan masing – masing fungsi LDAP untuk OpenLDAP, seperti *client*, *utility*, *server* dan semua struktur ini berbagi akses ke *library* menggunakan API (*Application Programming Interface*).

2.2 Penelitian Terkait

Dalam penyusunan tugas akhir ini, penulis melakukan penelitian terhadap kegiatan yang memiliki masalah yang terkait dengan judul penelitian dan memiliki kesamaan dalam membangun jaringan nirkabel menggunakan autentikasi terpusat dengan penggunaan perangkat lunak maupun perangkat keras yang berbeda. Berikut penelitian terkait yang penulis temukan.

No.	Judul Penelitian	Tahun	Kesimpulan
1	<p>Implementasi Jaringan <i>Hotspot</i> dengan <i>Captive Portal</i> Zeroshell dan <i>User Management</i> LDAP</p> <p>Oleh Rofiatul Laily Siregar, dan Agus Prihanto Universitas Negeri Surabaya Fakultas Teknik Jurusan Teknik Informatika</p>	2019	<p>Pada jurnal ini perancangan serta implementasi keamanan jaringan nirkabel menggunakan <i>captive portal</i> dari sistem operasi Zeroshell 3.8.2 dan proses autentikasi menggunakan RADIUS dengan dibantu LDAP sebagai <i>database user</i> dan <i>password</i></p>
2	<p>Sistem Autentikasi <i>Hotspot</i> Menggunakan LDAP dan Radius pada Jaringan <i>Internet Wireless</i> Prodi Teknik Sistem Komputer</p> <p>Oleh Ahmad Herdinal Muttaqin, Adian Fatur Rochim, dan Eko Didik Widiyanto Universitas Diponegoro Fakultas Teknik Program Studi Sistem Komputer</p>	2016	<p>Pada jurnal ini menerapkan keamanan jaringan nirkabel menggunakan <i>captive portal</i> dan proses autentikasi dengan RADIUS serta LDAP, namun dalam jurnal ini <i>captive portal</i> menggunakan perangkat lunak CoovaChilli dan sistem operasi yang digunakan adalah Ubuntu <i>Server</i> 14.04</p>
3	<p><i>Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication</i></p>	2016	<p>Dalam jurnal ini menerapkan keamanan jaringan nirkabel dengan <i>captive portal</i> dimana menggunakan perangkat lunak pfSense yang terinstall pada sistem operasi FreeBSD, dan untuk proses autentikasi</p>

	<p>Oleh F. L. Aryeh, M. Asante, dan A. E. Y. Danso</p> <p><i>University of Mines and Technology, dan Kwame Nkrumah University of Science and Technology</i></p>	<p>menggunakan <i>active directory</i> sebagai <i>database user password</i>, dan NPS (<i>Network Policy Services</i>) berperan sebagai RADIUS local yang sudah terinstall pada <i>Windows Server 2012</i></p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabel 2.1 : Penelitian Terkait

Berdasarkan penelitian terkait di atas, terdapat perbedaan dengan penelitian yang dibuat pada tugas akhir ini, yaitu perangkat keras yang untuk memancarkan jaringan nirkabel menggunakan perangkat Ransnet, sistem operasi yang digunakan adalah centos 7, serta *captive portal* yang digunakan adalah milik produk Ransnet sendiri.

BAB III METODOLOGI PENELITIAN

3.1 Jenis Metode Penelitian

Penelitian adalah salah satu cara paling jitu dalam pengembangan bahkan memajukan sebuah standar tatanan pengetahuan yang telah ada, peneliti dapat mengulik apa saja variabel yang nantinya dapat dimodifikasi agar pengetahuan tersebut berkembang (Sari et al., 2022). Terdapat jenis - jenis metode penelitian, diantaranya.

A. Penelitian Deskriptif

Penelitian deskriptif adalah jenis penelitian terhadap suatu gejala, peristiwa, atau kejadian yang sedang menjadi pusat perhatian.

B. Penelitian Studi Kasus

Penelitian studi kasus merupakan salah satu penelitian yang mempelajari individu ataupun kelompok secara intensif dalam kurun waktu tertentu.

C. Penelitian Survei

Penelitian survei merupakan penelitian yang bertujuan untuk mengumpulkan informasi tentang variabel dari sekelompok objek atau populasi.

D. Penelitian Studi Korelasional

Penelitian studi korelasional merupakan salah metode penelitian yang digunakan untuk mempelajari hubungan antara dua variabel ataupun lebih.

E. Penelitian Eksperimen

Penelitian eksperimen merupakan metode penelitian yang menggunakan penelitian kuantitatif, jenis penelitian ini harus memenuhi 3 syarat yang harus dipenuhi, yaitu kegiatan mengontrol, kegiatan memanipulasi, dan observasi

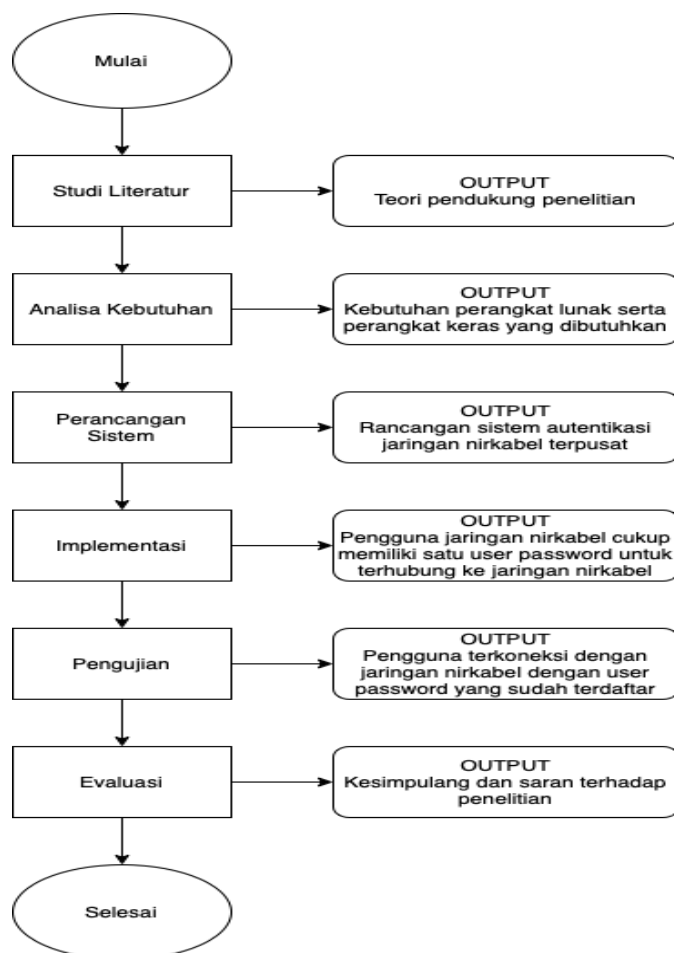
F. Penelitian dan Pengembangan

Penelitian dan pengembangan atau biasa dikenal sebagai *research and development*, merupakan metode penelitian yang melalui serangkaian proses dalam mengembangkan produk baru ataupun menyempurnakan produk yang sudah ada.

Berdasarkan jenis – jenis penelitian yang dijabarkan, dalam penelitian ini penulis menggunakan metode penelitian dan pengembangan, dengan menggunakan perangkat lunak dan perangkat keras yang sudah ada, selanjutnya dilakukan pendalaman untuk mendapatkan hal baru yang nantinya diharapkan dapat menghasilkan suatu hal yang lebih efektif.

3.2 Tahapan Penelitian

Tahapan berikut digunakan penulis sebagai acuan perancangan dan implementasi. Berdasarkan uraian tahapan penelitian pada gambar 3.1, berikut penjelasan terkait masing – masing tahapan yang akan dilakukan dalam penelitian ini.



Gambar 3.1 : Flow Chart Tahapan Penelitian

3.2.1 Studi Literatur

Pada tahap ini, penulis mencari referensi literatur yang terkait dengan radius, ldap, jaringan nirkabel, serta hal – hal lain yang berkaitan dengan penelitian. Penulis meneliti dari berbagai sumber seperti jurnal, artikel, buku elektronik, serta skripsi penelitian, maupun dari situs resmi.

Output dari tahap ini adalah sebuah acuan teori hingga cara kerja bagaimana sebuah komputer dapat memberikan layanan berupa autentikasi terpusat yang dapat diintegrasikan dengan layanan jaringan nirkabel sehingga pengguna hanya memiliki *user* dan *password* yang dapat dipakai untuk berbagai layanan.

3.2.2 Analisa Kebutuhan

Pada tahap ini penulis melakukan analisa hal – hal apa saja yang diperlukan dalam penelitian ini dan pengimplementasian autentikasi terpusat pada jaringan nirkabel.

Output dari tahap ini adalah penulis dapat mengetahui apa saja yang dibutuhkan untuk memperbaiki permasalahan yang ada.

3.2.3 Perancangan Sistem

Pada tahap ini penulis melakukan perancangan sistem yang akan dibuat, perancangan sistem meliputi perangkat keras dan perangkat lunak yang dibutuhkan untuk menerapkan autentikasi terpusat pada jaringan nirkabel.

Output dari tahap ini adalah penulis dapat menentukan rancangan sistem yang dibutuhkan.

3.2.4 Implementasi

Dalam tahapan ini, penulis melakukan proses implementasi, proses implementasi tersebut meliputi instalasi FreeRADIUS, konfigurasi FreeRADIUS agar terintegrasi dengan OpenLDAP hingga melakukan konfigurasi pada *hotpost router gateway* agar melakukan proses autentikasi melalui FreeRADIUS yang sudah dikonfigurasi.

Output dari tahap ini adalah terbentuknya perancangan dan implementasi integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal*.

3.2.5 Pengujian

Setelah melakukan tahap implementasi, masuk ke tahap proses pengujian pada rancangan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal*.

Output dari tahap ini adalah pengguna teruji dapat melakukan proses autentikasi pada jaringan nirkabel menggunakan FreeRADIUS dan OpenLDAP.

3.2.6 Evaluasi

Pada tahap ini melakukan evaluasi terhadap rancangan yang diimplementasikan, sehingga dapat menghasilkan dan saran yang dapat dilakukan oleh pengembangan selanjutnya.

Output dari tahap ini adalah menghasilkan sebuah kesimpulan dari penelitian ini, serta memberikan saran untuk pengembang selanjutnya.

3.3 Lingkungan Penelitian

Penulis melakukan penelitian pada lingkungan jaringan komputer PT. Elang Strategi Adidaya, dan menggunakan sistem virtualisasi dengan perangkat lunak Proxmox.

3.4 Alat dan Bahan Penelitian

Dalam melakukan penelitian ini, penulis menggunakan perangkat sebagai berikut.

- A. Laptop dengan spesifikasi :
 - a) *Processor* : Apple M1
 - b) *RAM* : 8GB
 - c) *Storage* : 512 GB

BAB IV

RANCANGAN SISTEM

Pada bab ini akan menjelaskan perancangan terkait penelitian ini yang meliputi analisis kebutuhan perangkat keras dan perangkat lunak, perancangan sistem fisik, *logic*, pengujian, dan skenario pengujian.

4.1 Analisis Kebutuhan

4.1.1 Analisis Kebutuhan Perangkat Keras

Dalam penelitian ini penulis menggunakan spesifikasi perangkat keras yang optimal terhadap layanan yang akan diimplementasikan, dimana penggunaan perangkat keras ini ditentukan berdasarkan pendekatan studi literatur yang merujuk langsung ke situs resmi FreeRADIUS, dan RansNet. Penulis akan menentukan spesifikasi *server* beserta *router* yang digunakan berdasarkan jumlah pengguna jaringan agar layanan dapat berjalan dengan optimal dan tidak berlebihan dalam menentukan spesifikasi perangkat yang dibutuhkan. Dalam situs dan forum resmi FreeRADIUS, menyebutkan bahwa penggunaan FreeRADIUS untuk skala kecil hingga menengah tidak ditentukan secara spesifik perangkat keras yang dibutuhkan, bahkan untuk instalasi FreeRADIUS dengan skala kecil sudah cukup dengan menggunakan RAM 8 MB, *disk* 100 GB, dan 1 *core* CPU. Dalam penggunaannya, FreeRADIUS mengutamakan spesifikasi CPU untuk proses autentikasi. Dengan ketentuan tersebut, penulis menggunakan spesifikasi *server* untuk FreeRADIUS dalam *virtual machine* sebagai berikut.

- RAM : 8 GB
- CPU : 8 Cores
- Disk : 100GB

Untuk *router* menggunakan merek RansNet dengan jenis HSG (*HotSpot Gateway*) yang berfungsi sebagai gerbang utama (*gateway*) untuk jaringan LAN. Agar layanan berjalan optimal tentu harus menyesuaikan kebutuhan dengan tipe serta spesifikasi *router* yang dibutuhkan, tabel dibawah ini adalah spesifikasi dari masing – masing tipe HSG.

Type	HSG-100	HSG-200	HSG-400	HSG-800	HSG-2000	HSG-5000	HSG-15000	HSG-25000
Maks. hotspot instance (VLAN)	200	200	200	300	500	500	2000	2000
Maks. throughput per hotspot instance	200 Mbps	200 Mbps	200 Mbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Maks. jumlah devices per hotspot instance	200	200	200	500	2000	2000	2000	2000
Processor	Multi-Core	Multi-Core	Multi-Core	Multi-Core	Multi-Core	Multi-Core	Quad-Core	Quad-Core
RAM (GB)	4	4	4	4	16	32	32	64
Gigabit Interface	4xGE	4xGE	4xGE	4xGE	6xGE	8xGE	8xGE	8xGE

Tabel 4.1 : Spesifikasi Router HSG

Untuk melakukan penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya, HSG-100 sudah mencukupi dalam penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* dengan perkiraan jumlah pengguna sebesar 50 – 80 perangkat perhari melakukan koneksi ke jaringan.

4.1.2 Analisis Kebutuhan Perangkat Lunak

Dalam penelitian ini menggunakan perangkat lunak yang berkaitan dengan penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya. Perangkat lunak yang digunakan penulis dipilih berdasarkan analisa penulis terkait stabilitas, serta dukungan teknis yang diberikan baik dari *service desk* resmi oleh perangkat lunak tersebut, maupun komunitas

yang aktif. Semua perangkat lunak yang digunakan dapat diunduh secara gratis melalui *internet*.

Berikut ini adalah perangkat lunak yang akan digunakan dalam penelitian ini.

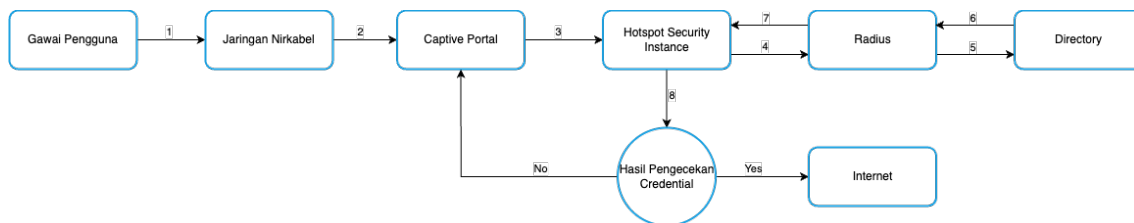
No.	Layanan	Perangkat Lunak	Fungsi
1	Sistem Operasi	CentOS 7.9	Sistem operasi yang digunakan untuk instalasi FreeRADIUS dan Zimbra <i>mail server</i> .
2	Platform Virtualisasi Server	Proxmox VE 5.2-1	<i>Virtual environment</i> yang digunakan dalam membuat <i>virtual machine</i> untuk instalasi sistem operasi
3	<i>Mail Server</i>	Zimbra Collaboration 8.8.15	Layanan yang sudah terpasang di PT Elang Strategi Adidaya untuk dimanfaatkan layanan LDAP di dalamnya.
4	Radius	FreeRADIUS 3.0.13	Layanan yang digunakan untuk mengintegrasikan <i>captive portal</i> dengan OpenLDAP.
5	<i>Web Browser</i>	Safari 15.5	Perangkat lunak yang digunakan untuk menampilkan <i>captive portal</i> pada saat terhubung dengan jaringan nirkabel.

Tabel 4.2 : Penggunaan Perangkat Lunak

4.2 Perancangan Sistem

4.2.1 Perancangan Arsitektur Sistem Logika

Bagian ini akan menjelaskan bagaimana rancangan arsitektur sistem logika dalam penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal*. Gambar di bawah ini akan menggambarkan bagaimana arsitektur sistem logika dari penelitian ini.



Gambar 4.1 : Rancangan Arsitektur Sistem Logika

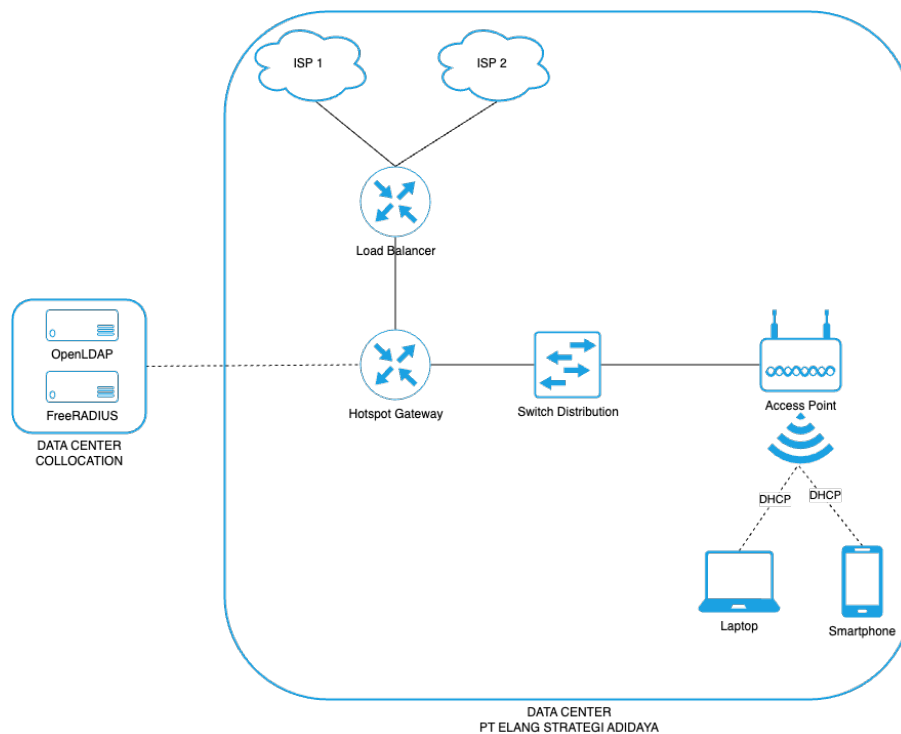
Pada gambar 4.1 adalah gambaran terkait rancangan logika yang akan berjalan pada penelitian ini, dengan penjabaran rancangan sebagai berikut.

1. Pada saat pertama kali pengguna terkoneksi kedalam jaringan nirkabel, secara otomatis pengguna akan arahkan ke dalam *login page captive portal* untuk melakukan autentikasi.
2. Setelah memasukan *username* dan *password* pada *captive portal*, *hotspot security instance* akan menerima credential tersebut lalu mengirimkan pada *radius server* untuk pengecekan kebenaran dari *credential* yang dikirimkan.
3. Setelah *radius server* menerima *credential* dari *hotspot security instance*, *radius server* mengirimkan kembali pada direktori *server* untuk melakukan pengecekan apakah *credential* yang dikirim terdaftar atau tidak di dalam direktori.
4. Lalu setelah direktori *server* melakukan pengecekan *credential* yang ada di dalam direktori, direktori *server* mengirimkan hasil pengecekan kepada *radius server* terkait status *credential* yang dikirimkan.
5. *Radius server* menerima hasil pengecekan *credential* dari direktori *server*, lalu meneruskan kembali hasil pengecekan kepada *hotspot security instance* apakah *credential* yang dikirimkan benar atau salah.

6. Setelah *security hotspot instance* menerima hasil pengecekan dari *radius server*, *security hotspot instance* akan menentukan jika *credential* yang dikirimkan benar maka perangkat tersebut akan mendapatkan akses *internet*, namun jika *credential* yang dikirimkan salah maka perangkat akan dikembalikan kembali ke halaman *captive portal* untuk melakukan autentikasi ulang.

4.2.2 Perancangan Arsitektur Sistem Fisik

Pada bagian ini, akan digambarkan sebuah arsitektur sistem fisik seperti pada gambar dibawah ini.



Gambar 4.2 : Rancangan Arsitektur Sistem Fisik

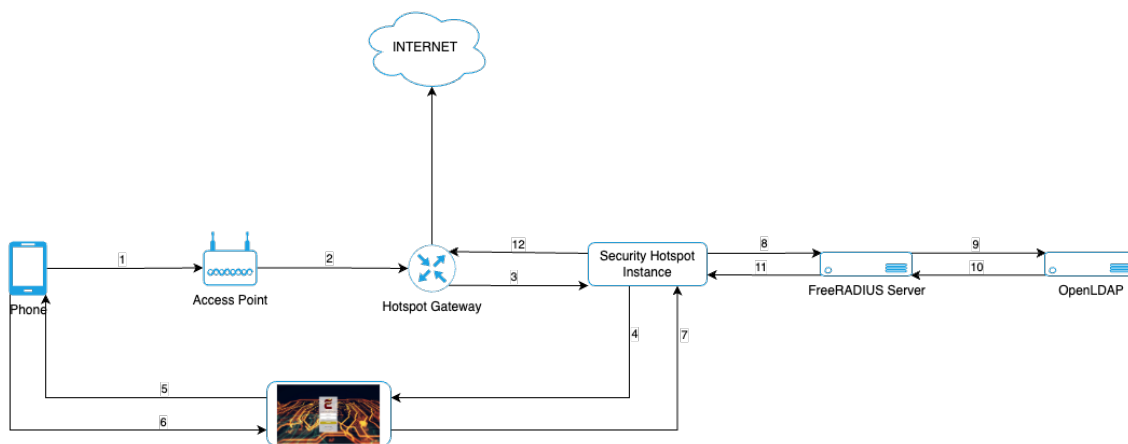
Berdasarkan gambar 4.2 tentang rancangan arsitektus sistem fisik, dapat dijelaskan bahwa.

1. Pada kantor PT Elang Strategi Adidaya, terdapat 2 penyedia layanan *internet* yang terhubung pada jaringan lokal, dimana 1 diantaranya memiliki statik ip *public* dan 1 lainnya merupakan layanan *internet* tanpa statik ip *public*.

2. *Server* OpenLDAP dan FreeRADIUS berada di dalam 1 *data center collocation* dimana lokasinya berada di luar bangunan kantor PT Elang Strategi Adidaya, sedangkan perangkat lainnya berada di dalam bangunan kantor PT Elang Strategi Adidaya.
3. Pengguna dapat terhubung ke dalam jaringan nirkabel PT Elang Strategi Adidaya menggunakan gawainya melalui *access point* yang ada.
4. Terdapat *switch* dimana memungkinkan untuk memasang lebih dari 1 *access point*, dan menjadi penghubung antara *access point* dengan *router*.

4.3 Perancangan Pengujian

Rancangan arsitektur sistem yang akan dibangun pada penelitian harus melewati tahap pengujian rancangan sistem yang sebagaimana sudah dijabarkan sebelumnya. Pada bagian ini akan dibangun sebuah rancangan pengujian integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* dengan sebagai berikut.



13

Gambar 4.3 : Rancangan Pengujian

Pada gambar 4.3 di atas, dapat dijabarkan rancangan pengujian yang akan dilakukan pada penelitian ini adalah sebagai berikut.

1. Gawai dapat berupa *smartphone* maupun laptop dimana terhubung kedalam jaringan nirkabel melalui *access point*.
2. Melalui *access point*, *smartphone* akan mendapatkan IP Address dan terhubung dengan *hotspot gateway*.
3. *Hotpost gateway* dengan fitur *security hotspot instance* akan mengirimkan *captive portal* kepada *smartphone* untuk melakukan autentikasi.
4. *Smartphone* melakukan autentikasi melalui *captive portal* dengan memasukan *username* dan *password*.
5. *Security hotspot instance* melakukan pengecekan *credential* yang dikirimkan oleh *smartphone* menggunakan FreeRADIUS.
6. FreeRADIUS akan mencari *credential* yang didapatkan di dalam OpenLDAP untuk melakukan pengecekan pada direktori apakah *username* dan *password* yang dikirimkan terdaftar di dalam direktori.
7. Setelah itu, FreeRADIUS mengirimkan hasil pengecekannya kepada *security hotspot instance*.
8. Dari *security hotspot instance*, akan memberikan akses *internet* kepada *smartphone* melaluia *hotspot gateway* jika hasil pengecekan *credential* dari FreeRADIUS benar terdaftar pada direktori, dan tidak akan diizinkan untuk mengakses *internet* jika pengecekan *credential* dari FreeRADIUS tidak terdaftar pada direktori.

4.4 Skenario Pengujian

Dalam konfigurasi *default*, implementasi *captive portal* pada perangkat RansNet ini menggunakan *username* serta *password* yang sudah disediakan atau ditambahkan pada perangkat *router gateway* itu sendiri, namun hal tersebut kurang efektif dikarenakan pengguna harus mengingat lebih dari 1 *username* dan *password* untuk mengakses fasilitas yang diberikan, dan jika adanya perubahan *username* serta *password* seorang *administrator* harus melakukan sinkronisasi kembali secara manual agar *username* dan *password* antara masing – masing layanan tetap sama. Untuk itu dalam tahap pengujian, ini penulis melakukan integrasi *captive portal* dengan FreeRADIUS dan OpenLDAP yang sudah tersedia pada layanan zimbra *mail server*.

Skenario pengujian pada penelitian ini adalah perangkat HSG (*HotSpot Gateway*) yang berperan sebagai penyedia *captive portal* serta menjadi *gateway* pada jaringan WLAN di PT Elang Strategi Adidaya akan memberikan IP DHCP serta mengirimkan *captive portal* kepada gawai yang terhubung kedalam jaringan WLAN melalui *access point*, pengguna gawai tersebut diwajibkan untuk memasukkan *username* dan *password* yang mereka miliki dan terdaftar pada OpenLDAP zimbra *mail server* untuk mendapatkan akses *internet* dari jaringan WLAN tersebut.

4.4.1 Skenario Pengujian *Log In Captive Portal* Menggunakan Laptop

Skenario pengujian *log in* pada *captive portal* menggunakan laptop untuk mendapatkan akses *internet* melalui jaringan nirkabel ini dapat digambarkan pada tabel di bawah ini.

No	Username	Status Autentikasi	Status Koneksi
1	User1	Berhasil Login	Terkoneksi Internet
2	User2
3	User3
4	User4
5	User5
6	User6
7	User7
8	User8
9	User9
10	User10

Tabel 4.3 : Skenario Pengujian *Log In Captive Portal* Menggunakan Laptop

4.4.2 Skenario Pengujian *Log In Captive Portal* Menggunakan *Smartphone*

Skenario pengujian *log in* pada *captive portal* menggunakan *smartphone* untuk mendapatkan akses *internet* melalui jaringan nirkabel ini dapat digambarkan pada tabel di bawah ini.

No	Username	Status Autentikasi	Status Koneksi
1	User1	Berhasil Login	Terkoneksi Internet
2	User2
3	User3
4	User4
5	User5
6	User6
7	User7
8	User8
9	User9
10	User10

Tabel 4.4 : Skenario Pengujian Log In Captive Portal Menggunakan Smartphone

BAB V

IMPLEMENTASI DAN PENGUJIAN

Pada bab ini penulis akan membahas implementasi dari rancangan yang telah dibuat pada bab sebelumnya, dan disertai pengujian dari hasil penerapan autentikasi jaringan nirkabel terpusat dengan *captive portal* menggunakan FreeRADIUS dan OpenLDAP. Pada tahap implementasi akan dibahas secara detil mengenai proses instalasi hingga konfigurasi FreeRADIUS dan proses konfigurasi HSG sebagai *gateway* agar terintegrasi dengan FreeRADIUS serta menampilkan *captive portal* bagi pengguna yang ingin terhubung ke jaringan nirkabel PT Elang Strategi Adidaya.

5.1 Implementasi

Pada tahap ini akan dijabarkan secara rinci proses persiapan serta instalasi setiap perangkat lunak yang dibutuhkan dalam penerapan autentikasi jaringan nirkabel terpusat dengan *captive portal* menggunakan FreeRADIUS dan OpenLDAP pada PT Elang Strategi Adidaya.

5.1.1 Persiapan

Pada bagian ini akan menjabarkan proses dalam mempersiapkan hal – hal apa saja yang dibutuhkan dalam implementasi ini.

5.1.1.1 Pembaruan *Repository* CentOS

Sebelum melakukan instalasi FreeRADIUS, diperlukan untuk melakukan pembaruan *repository* pada CentOS. Pembaruan dilakukan pada *server* yang akan dijadikan FreeRADIUS *server*. Untuk melakukan pembaruan *repository* pada CentOS penulis menjalankan perintah berikut.

```
# yum update -y
```

5.1.1.2 Pengecekan *Credential* OpenLDAP pada *Zimbra Mail Server*

Dalam implementasi ini, penulis menggunakan OpenLDAP yang sudah terpasang bersama dengan zimbra. Untuk itu, penulis tidak mengetahui *credential* OpenLDAP yang terpasang pada zimbra dikarenakan *credential* tersebut dibuat secara otomatis oleh zimbra pada saat proses instalasi *zimbra mail server*. Namun *credential* OpenLDAP pada zimbra tersebut dapat dilihat pada konfigurasi *zimbra mail server* dengan perintah berikut di dalam *server* zimbra.

```
# /opt/zimbra/bin/zmlocalconfig -s | grep ldap
```

Hasil dari perintah di atas, akan mengeluarkan *credential* OpenLDAP yang digunakan pada *zimbra mail server* dengan hasil dari perintah tersebut adalah sebagai berikut.

```
ldap_url = ldap://w-mail.estrada.co.id:389
zimbra_class_ldap_client = com.zimbra.cs.ldap.unboundid.UBIDLdapClient
zimbra_class_provisioning = com.zimbra.cs.account.ldap.LdapProvisioning
zimbra_ldap_password = dummypassword
zimbra_ldap_user = zimbra
zimbra_ldap_userdn = uid=zimbra, cn=dummy, cn=zimbra
zimbra_zmprov_default_to_ldap = false
```

Dari hasil di atas dapat dilihat *username*, *password*, url, serta *port* OpenLDAP yang digunakan oleh *zimbra mail server*, dan dapat penulis gunakan untuk diintegrasikan dengan FreeRADIUS *server* yang dirangkum sebagai berikut.

- *URL* : w-mail.estrada.co.id
- *Port* : 389
- *Username* : uid=zimbra, cn=dummy, cn=zimbra
- *Password* : dummypassword

Penulis melakukan sensor terhadap *username* dan *password* di atas karena hal tersebut merupakan rahasia dari perusahaan.

5.1.2 Instalasi dan Konfigurasi

Pada bagian ini akan menjabarkan proses instalasi hingga semua sistem yang sudah terinstal dapat terintegrasi.

5.1.2.1 Instalasi dan Konfigurasi FreeRADIUS

Pada tahap ini akan dijabarkan proses instalasi serta konfigurasi FreeRADIUS hingga terintegrasi dengan OpenLDAP yang terdapat pada zimbra *mail server* dan sudah diketahui *credential* dari OpenLDAP tersebut pada bagian sebelumnya.

Tahap pertama pada bagian ini adalah penulis melakukan instalasi paket – paket yang dibutuhkan untuk layanan FreeRADIUS.

```
# yum install -y freeradius freeradius-utils freeradius-ldap
```

Lalu penulis membuka *file* modul ldap pada FreeRADIUS *server* untuk memodifikasi konfigurasi dari FreeRADIUS.

```
# vi /etc/raddb/mods-available/ldap
```

Setelah itu penulis menambahkan konfigurasi di bawah ini di dalam *blockline* ldap lalu simpan.

```
ldap {
    ...
    server = 'w-mail.estrada.co.id'
    port = 389
    identity = uid=zimbra, cn=dummy, cn=zimbra
    password = dummypassword
    base_dn = 'dc=estrada, dc=co, dc=id'
    ...
}
```

Isi dari data – data di atas didapatkan dari bagian sebelumnya pada saat melakukan pengecekan *credential* OpenLDAP zimbra *mail server*, dan untuk *base_dn* tidak

didapatkan dari pengecekan *credential* sebelumnya, melainkan didapatkan berdasarkan *domain* yang dipakai oleh *mail server*.

Setelah itu penulis menghubungkan *link* pada *file* modul yang sebelumnya sudah ditambahkan konfigurasi dari direktori *mods-available* ke *mod-enabled*.

```
# ln -s /etc/raddb/mods-available/ldap /etc/raddb/mod-enabled/ldap
```

Lalu penulis membuka *file* konfigurasi *default* FreeRADIUS *server* untuk memodifikasi konfigurasi dari FreeRADIUS.

```
# vi /etc/raddb/sites-enabled/default
```

Sehabis itu penulis menghapus simbol komentar (#) pada *blockline* di bawah ini lalu simpan *file*.

```
Auth-Type LDAP {  
    ldap  
}
```

Lalu penulis membuka *file* konfigurasi *inner-tunnel* untuk memodifikasi konfigurasi dari FreeRADIUS

```
# vi /etc/raddb/sites-available/inner-tunnel
```

Penulis menghapus simbol komentar (#) pada baris *ldap* di dalam *blockline authorize* untuk mengaktifkan fitur otorisasi menggunakan *ldap*.

```
authorize {  
    ...  
    ldap  
    ...  
}
```

Tetap di dalam *file* inner-tunnel, penulis menghapus simbol komentar (#) pada *blockline* untuk mengaktifkan autentikasi menggunakan ldap di dalam *blockline authenticate* lalu simpan *file*.

```
authenticate {  
  ...  
    Auth-Type LDAP {  
      ldap  
    }  
  ...  
}
```

Selesai memodifikasi konfigurasi FreeRADIUS di atas, penulis melakukan *restart* pada paket FreeRADIUS untuk mengaktifkan konfigurasi yang sudah diubah.

```
# service radiusd restart
```

Setelah menyesuaikan dan mengaktifkan konfigurasi, penulis melakukan verifikasi bahwa FreeRADIUS sudah terintegrasi dengan OpenLDAP dengan menjalankan tes autentikasi menggunakan *username* dan *password* yang terdaftar pada OpenLDAP, dengan menjalankan perintah berikut.

```
# radtest dummyuser dummpassword 127.0.0.1 1812 testing123
```

Setelah FreeRADIUS sudah berhasil terintegrasi dengan OpenLDAP, maka hasil dari perintah di atas akan mendapatkan balasan *access-accept*.

```
Sent Access-Request Id 96 from 0.0.0.0:45059 to 127.0.0.1:1812 length 76  
User-Name = "dummyuser"  
User-Password = "dummpassword"  
NAS-IP-Address = 103.x.x.x  
NAS-Port = 1812  
Message-Authenticator = 0x00  
Cleartext-Password = "dummpassword"  
Received Access-Accept Id 96 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

IP dari tanggapan *server* openldap diatas penulis sensor untuk menjaga keamanan data dari perusahaan tempat penulis melakukan penelitian.

Lalu penulis menambahkan *port* radius pada *firewall* agar layanan radius dapat diakses dari perangkat lain, setelah itu *restart firewall* agar penambahan *port* tersebut aktif.

```
# firewall-cmd --permanent --add-port=1812/udp
# firewall-cmd --reload
```

Penulis melakukan verifikasi bahwa *port* untuk radius sudah terdaftar pada *firewall*.

```
# firewall-cmd --list-all
```

Setelah *port* radius sudah terdaftar, maka hasilnya akan seperti sebagai berikut.

```
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: ens18
  sources:
  services:
  ports: 1812/udp
  protocols:
  masquerade: no
  forward-ports
  source-ports:
  icmp-blocks:
  rich rules:
```

Setelah FreeRADIUS sudah berhasil terintegrasi dengan OpenLDAP, selanjutnya penulis menambahkan konfigurasi pada FreeRADIUS agar *router gateway* dapat terintegrasi, penulis membuka *file* *clients.conf*

```
# vi /etc/raddb/clients.conf
```

Penulis menambahkan konfigurasi di bawah ini pada bagian terakhir agar *router gateway* dapat terintegrasi dengan FreeRADIUS.

```
client estrada_network {
    ipaddr = 0.0.0.0/0
    secret = estxxx
}
```

Penulis melakukan sensor pada konfigurasi diatas untuk menjaga keamanan data dari perusahaan tempat penulis melakukan penelitian.

Pada konfigurasi yang ditambahkan di atas, penulis menggunakan IP 0.0.0.0/0 agar FreeRADIUS menerima semua IP yang ingin terhubung ke layanan radius, dikarenakan pada PT Elang Strategi Adidaya menggunakan 2 ISP dimana salah satu ISP tersebut tidak memiliki *static IP public*.

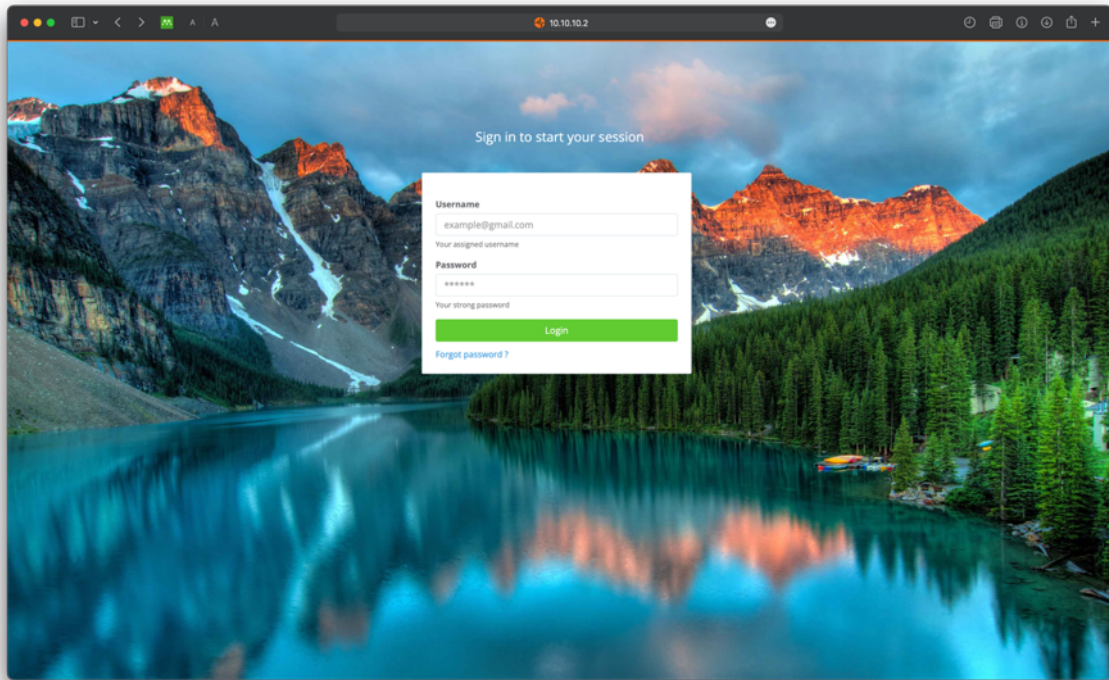
Selesai menyesuaikan konfigurasi, penulis melakukan *restart* kembali pada layanan radius untuk mengaktifkan konfigurasi yang baru ditambahkan.

```
# service radiusd restart
```

5.1.2.2 Konfigurasi Router Gateway

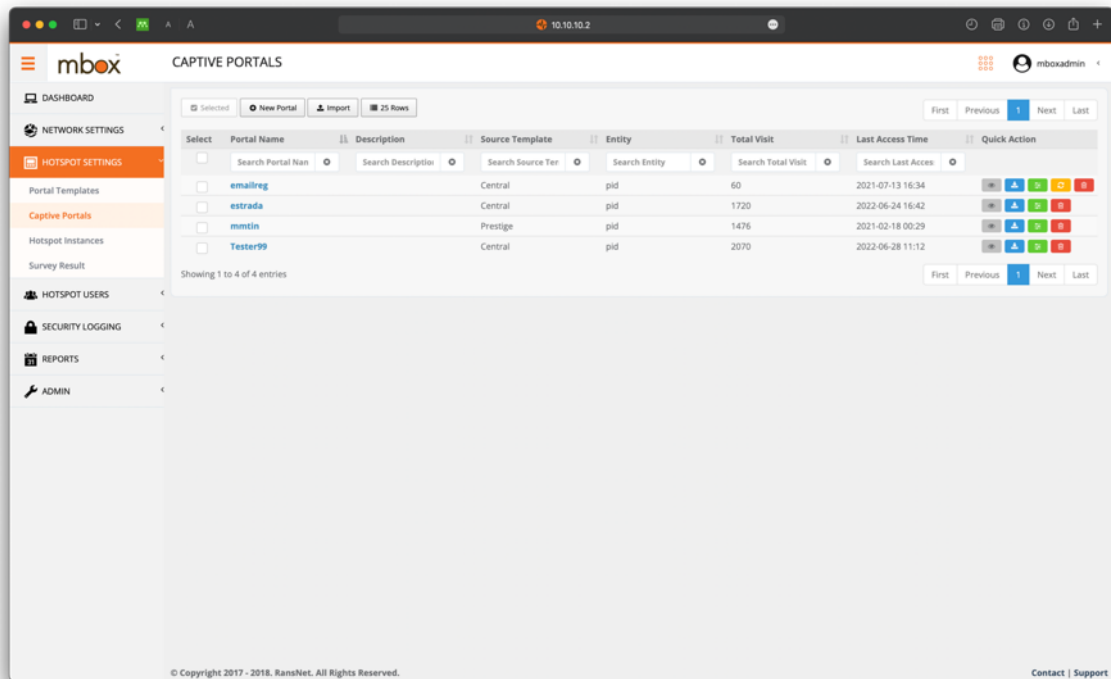
Tahap ini akan menjabarkan proses konfigurasi *router gateway* untuk menampilkan *captive portal* pada jaringan nirkabel hingga terintegrasi dengan FreeRADIUS agar dapat menggunakan *username* dan *password* yang ada pada OpenLDAP.

Penulis membuka halaman situs web pada *router gateway* untuk membuat *captive portal*, lalu *log in* untuk akses dasbor.



Gambar 5.1 : Login Web Router Gateway

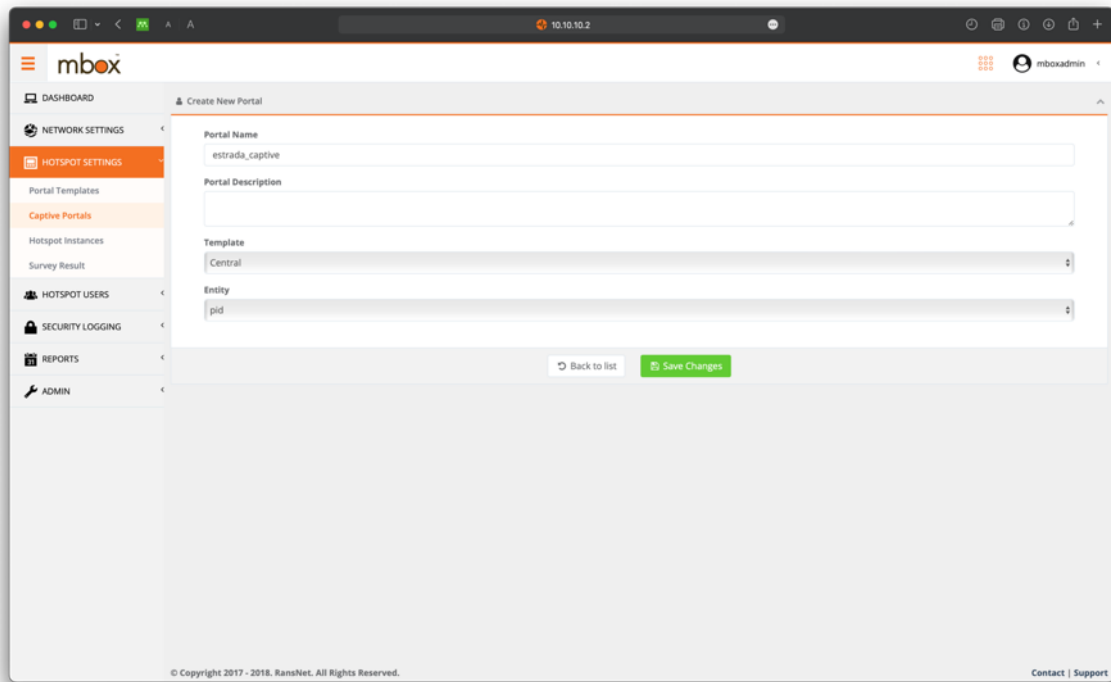
Setelah itu penulis menuju menu “*Hotspot Settings*” lalu “*Captive Portals*”



Gambar 5.2 : Menu Captive Portal

Pada gambar 5.2, penulis menuju “New Portal” untuk menambahkan halaman *captive portal* yang akan ditampilkan saat pengguna terhubung ke jaringan nirkabel.

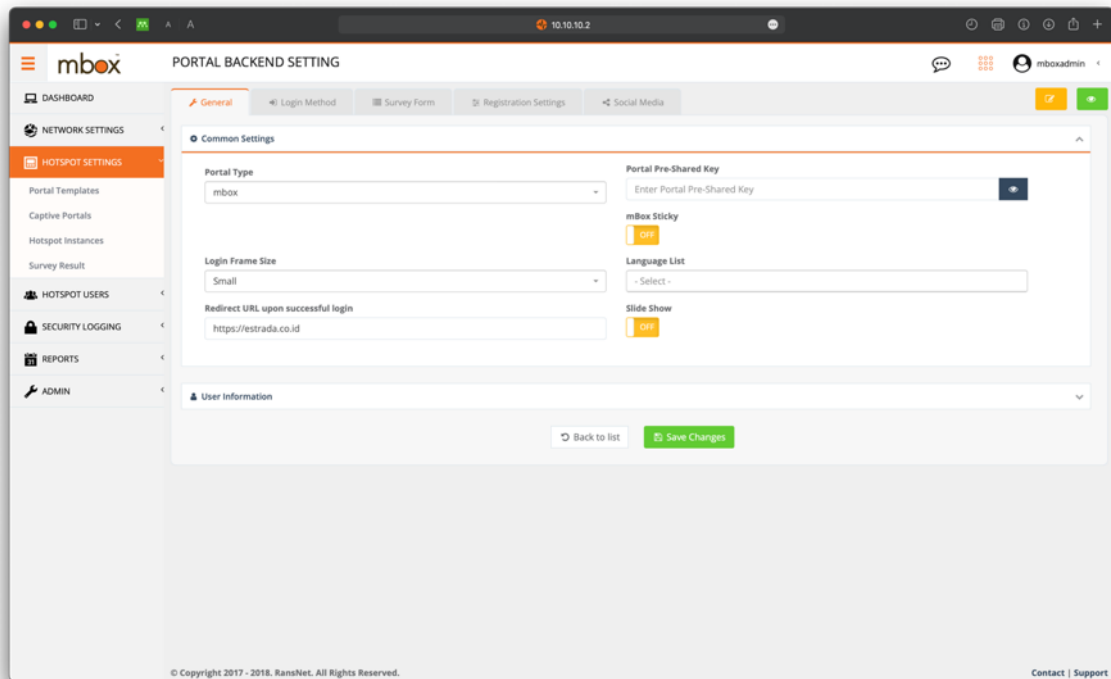
Setelah itu diarahkan kepada formulir untuk membuat *captive portal*.



Gambar 5.3 : Formulir Captive Portal

Pada gambar 5.3, penulis sudah mengisi formulir tersebut sesuai dengan kebutuhan penulis pada implementasi ini, lalu penulis melakukan klik “*Save Changes*” untuk menyimpan konfigurasi.

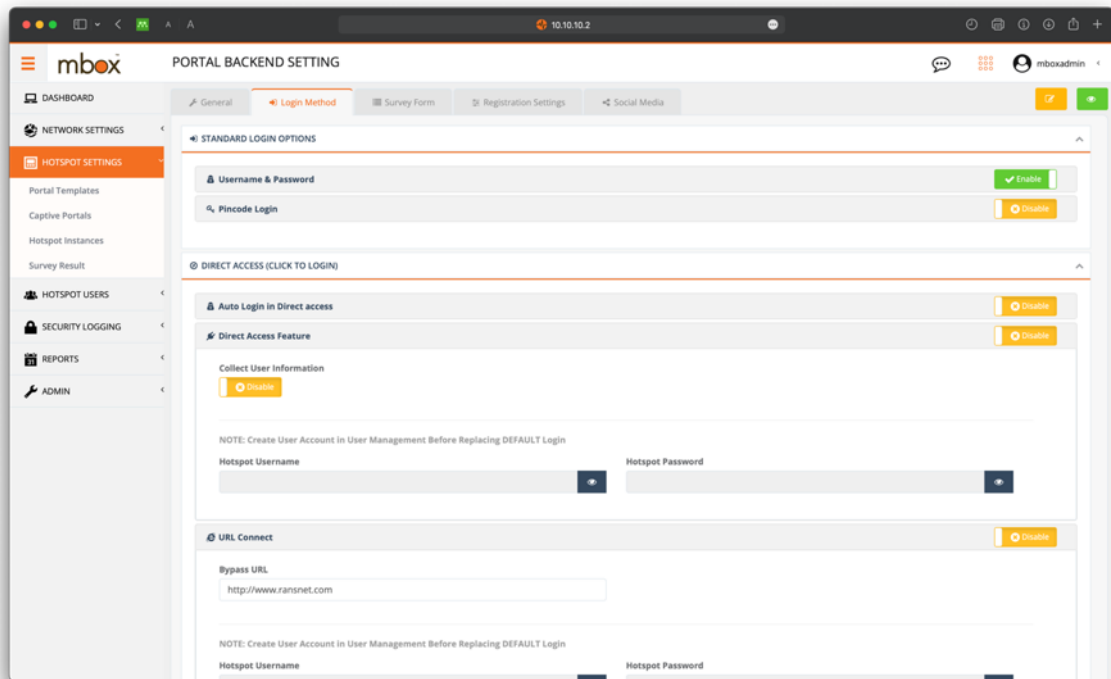
Setelah itu, diarahkan pada halaman untuk mengubah halaman dari *captive portal* yang sudah dibuat sebelumnya.



Gambar 5.4 : Ubah Back End Captive Portal (1)

Pada bagian “*General*” ini, penulis hanya menambahkan tautan *company profile* untuk mengalihkan pengguna jaringan nirkabel ke situs web tersebut setelah berhasil *login*.

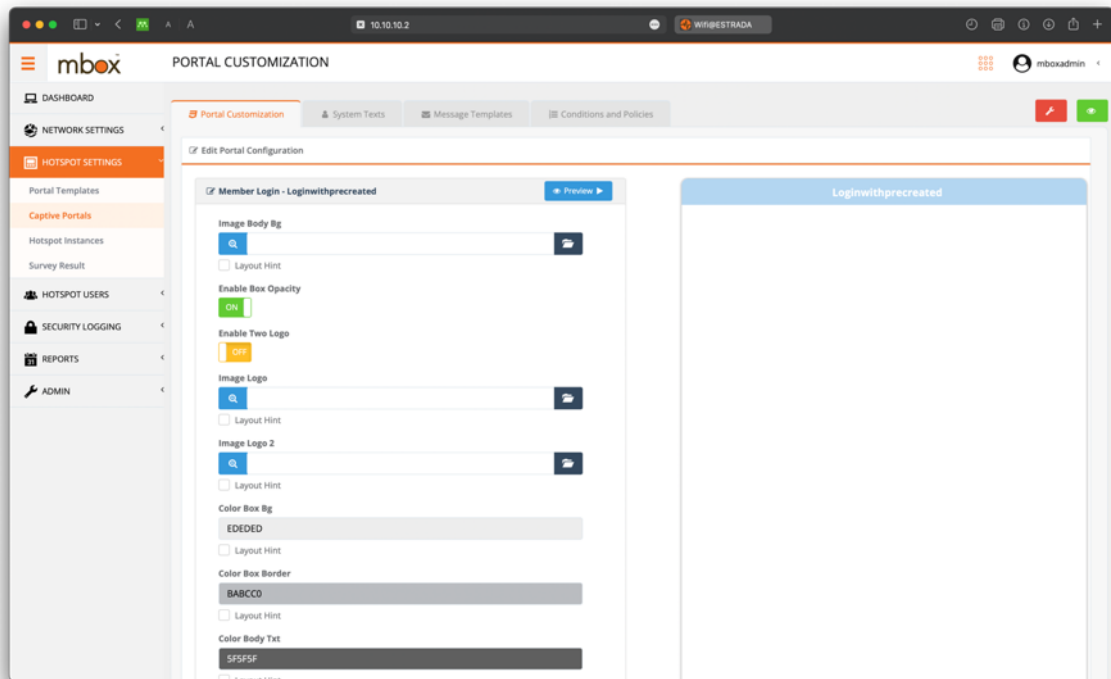
Setelah itu pada bagian “*Login Method*”, penulis menonaktifkan fitur “*Direct Access*” untuk *captive portal* karna untuk konfigurasi awal fitur tersebut aktif, lalu penulis mengaktifkan fitur “*Username & Password*” untuk mewajibkan pengguna jaringan nirkabel melakukan autentikasi menggunakan *username* dan *password* agar dapat mengakses *internet*.



Gambar 5.5 : Ubah Back End Captive Portal (2)

Selanjutnya penulis beralih kepada konfigurasi untuk *front end* halaman *captive portal* dengan klik pada ikon pensil berwarna kuning pada gambar 5.5.

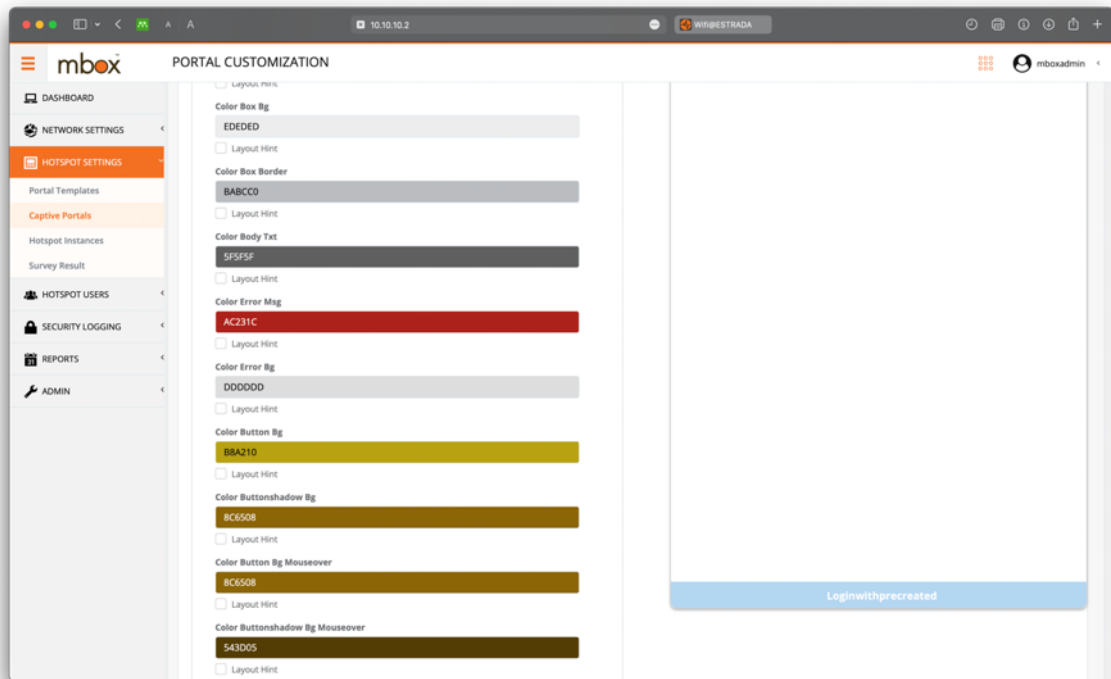
Setelah itu akan diarahkan pada halaman untuk mengubah konfigurasi *front end captive portal*.



Gambar 5.6 : Ubah Front End Captive Portal (1)

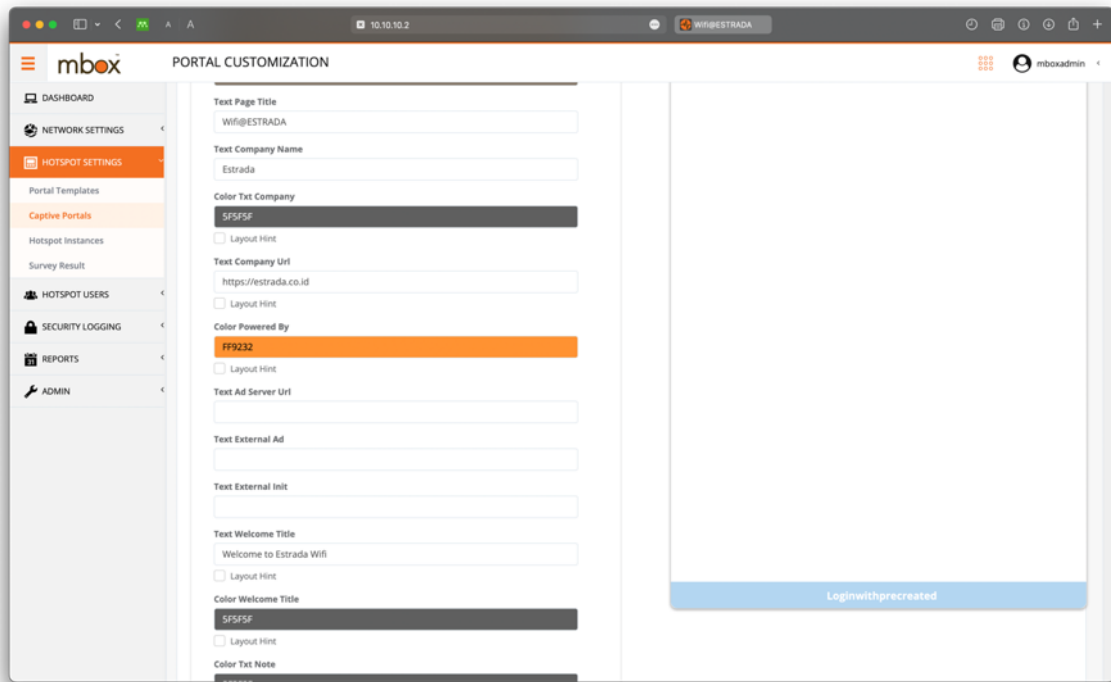
Pada gambar 5.6, penulis sudah mengubah “Image Body Bg” dengan mengunggah gambar yang penulis pilih pada kolom tersebut, lalu penulis juga menunggah logo PT Elang Strategi Adidaya pada kolom “Image Logo”.

Setelah itu penulis mengubah warna masing – masing fungsi tombol pada *captive portal* agar selaras dengan warna logo serta *background* yang penulis pilih sebelumnya.



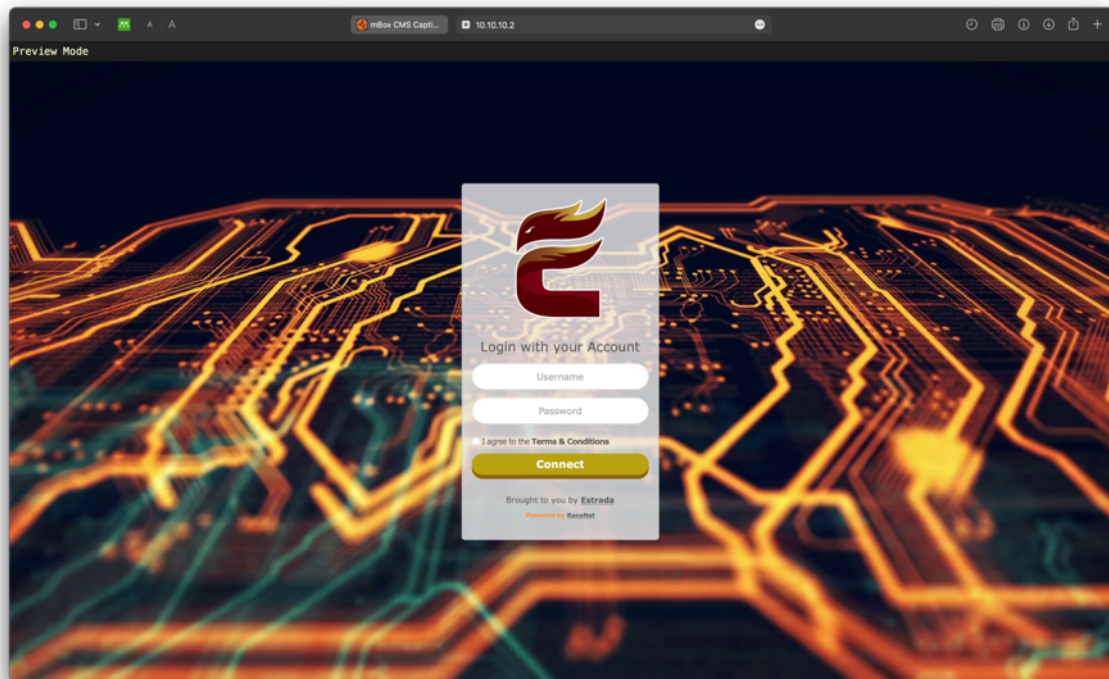
Gambar 5.7 : Ubah Front End Captive Portal (2)

Selanjutnya penulis mengubah *title*, nama perusahaan, serta teks selamat datang pada *captive portal*.



Gambar 5.8 : Ubah Front End Captive Portal (3)

Pada tahap ini penulis sudah selesai untuk konfigurasi *captive portal*, hasil dari konfigurasi tersebut dapat dilihat dengan klik ikon mata berwarna hijau yang ada pada gambar 5.6.

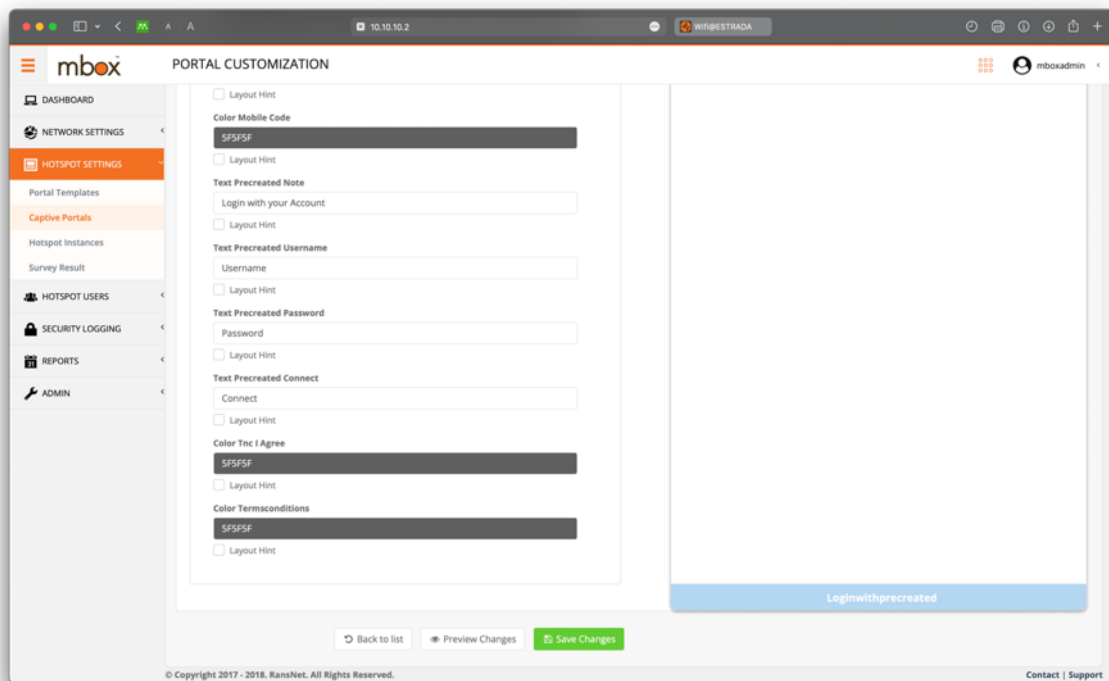


Gambar 5.9 : Ubah Front End Captive Portal (4)

Pada hasil *preview* diatas, salin tautan yang dipakai untuk membuka halaman *preview* tersebut dengan menghapus kata *preview* pada tautan yang didapat. Perubahan pada tautan seperti penulis contohkan dibawah ini.

- Sebelum dihapus : http://10.10.10.2/pid/estrada_captive/login.php?preview=1
- Setelah dihapus : http://10.10.10.2/pid/estrada_captive/login.php

Hasil konfigurasi dari *captive portal* pada gambar 5.9 sudah sesuai dengan kebutuhan, setelah itu klik tombol “*Save Changes*” untuk menyimpan konfigurasi yang sudah dibuat.



Gambar 5.10 : Simpan Konfigurasi Captive Portal

Penulis melakukan verifikasi pada *router* terkait autentikasi menggunakan FreeRADIUS yang sudah dikonfigurasi sebelumnya.

```
# test aaa radius-server 103.x.x.x radius-key estxxx username dummyuser
password dummypassword
```

Setelah berhasil, hasil autentikasi menggunakan RADIUS pada *router* akan mendapatkan balasan dari FreeRADIUS packet "Access-Accept".

```
Sending Access-Request of id 57 to 103.x.x.x port 1812
  User-Name = "dummyuser"
  User-Password = "dummypassword"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 1812
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 103.x.x.x port 1812, id=57,
length=20
```

Setelah integrasi terverifikasi berhasil, penulis masuk ke *mode* konfigurasi pada *router* untuk menambahkan konfigurasi *security hotspot*.

```
# configure
```

Setelah itu penulis menambahkan konfigurasi *security hotspot* pada VLAN untuk lantai 1.

```
security hotspot vlan111
hotspot-server 172.20.1.1 ports 4528 5320
client-network 172.20.1.0 255.255.255.0
client-dhcp 172.20.1.2 255.255.255.0 lease 8600
client-dhcp-server
router 172.20.1.1
dns 172.20.1.1
range 172.20.1.2 172.20.1.254
client-sticky last 7
client-sticky-vlanlist vlan133,vlan222
client-local-dns on
bypass-domain .ransnet.com
bypass-dst macc.ransnet.com,splash.ransnet.com
redirect-url https://estrada.co.id
radius-server 103.x.x.x estxxx
hotspot-portal http://splash.ransnet.com/pid/estrada_captive/login.php
start
```

Lalu penulis menambahkan konfigurasi *security hotspot* pada VLAN untuk lantai 2.

```
security hotspot vlan222
hotspot-server 172.20.2.1 ports 4811 4322
client-network 172.20.2.0 255.255.255.0
client-dhcp 172.20.2.2 255.255.255.0 lease 8600
client-dhcp-server
router 172.20.2.1
dns 172.20.2.1 172.20.2.1
range 172.20.2.2 172.20.2.254
client-sticky last 7
client-sticky-vlanlist vlan111,vlan133
client-local-dns on
bypass-domain .ransnet.com
bypass-dst macc.ransnet.com,splash.ransnet.com
redirect-url https://estrada.co.id
radius-server 103.x.x.x estxxx
hotspot-portal http://splash.ransnet.com/pid/estrada_captive/login.php
start
```

Penulis menambahkan konfigurasi *security hotspot* kembali pada VLAN untuk lantai 3.

```
security hotspot vlan133
hotspot-server 172.20.5.1 ports 5098 5040
client-network 172.20.5.0 255.255.255.0
client-dhcp 172.20.5.2 255.255.255.0 lease 8600
client-dhcp-server
router 172.20.5.1
dns 172.20.5.1 172.20.5.1
range 172.20.5.2 172.20.5.254
client-sticky last 7
client-sticky-vlanlist vlan111,vlan222
client-local-dns on
bypass-domain .ransnet.com
bypass-dst macc.ransnet.com,splash.ransnet.com
redirect-url https://estrada.co.id
radius-server 103.x.x.x estxxx
hotspot-portal http://splash.ransnet.com/pid/estrada_captive/login.php
start
```


5.2 Pengujian Penerapan Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis *Captive Portal* Di PT Elang Strategi Adidaya

Pada bagian ini penulis akan menjabarkan hasil pengujian dari penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* di PT Elang Strategi Adidaya.

5.2.1 Pengujian Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis *Captive Portal* menggunakan perangkat laptop

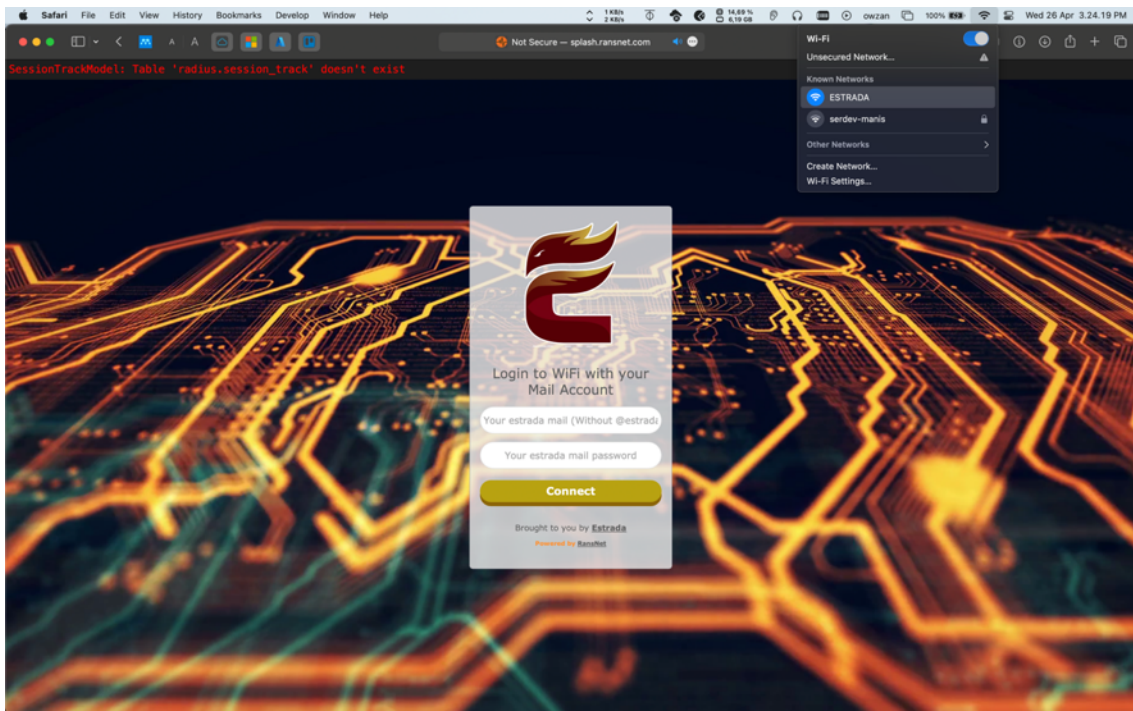
Pada tahap pengujian integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel menggunakan perangkat laptop, penulis akan menghubungkan laptop penulis dengan jaringan nirkabel yang sudah penulis buat sebelumnya dengan cara sebagai berikut.

Penulis terhubung pada jaringan nirkabel dengan SSID “ESTRADA”



Gambar 5.11 : Laptop Terkoneksi Pada Jaringan Nirkabel ESTRADA

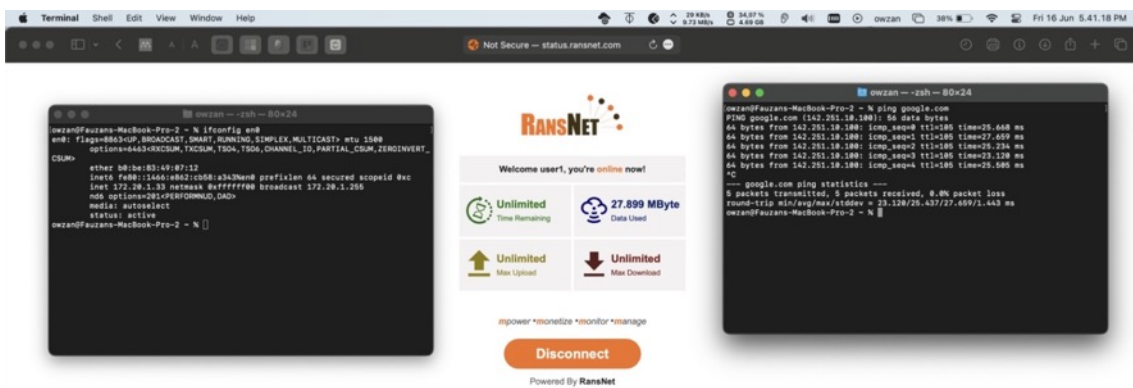
Setelah terhubung pada jaringan nirkabel dengan SSID “ESTRADA”, secara otomatis diarahkan ke dalam *login page* sebelum mendapatkan *internet*.



Gambar 5.12 : Login Page Pada Laptop

Penulis menggunakan *username* serta *password* yang sudah terdaftar di dalam OpenLDAP pada zimbra mail server.

Setelah berhasil terhubung, penulis mengakses halaman web `status.ransnet.com/status` untuk memverifikasi status perangkat dalam jaringan nirkabel.



Gambar 5.13 : Verifikasi Status Perangkat Laptop Pada Jaringan Nirkabel ESTRADA

Selanjutnya penulis mengulangi pengujian di atas menggunakan 10 *username* yang sudah penulis daftarkan dalam OpenLDAP pada *zimbra mail server* sebagai sampel untuk menguji efektivitas integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* menggunakan laptop dengan hasil pengujian sebagai berikut.

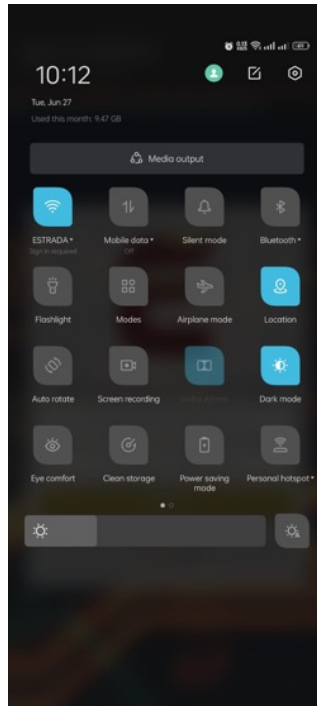
No	Username	Status Autentikasi	Status Koneksi
1	User1	Berhasil Login	Terkoneksi Internet
2	User2	Berhasil Login	Terkoneksi Internet
3	User3	Berhasil Login	Terkoneksi Internet
4	User4	Berhasil Login	Terkoneksi Internet
5	User5	Berhasil Login	Terkoneksi Internet
6	User6	Berhasil Login	Terkoneksi Internet
7	User7	Berhasil Login	Terkoneksi Internet
8	User8	Berhasil Login	Terkoneksi Internet
9	User9	Berhasil Login	Terkoneksi Internet
10	User10	Berhasil Login	Terkoneksi Internet

Tabel 5.1 : Hasil Pengujian Menggunakan Laptop

5.2.2 Pengujian Integrasi FreeRADIUS dan OpenLDAP Sebagai Layanan Autentikasi Jaringan Nirkabel Berbasis *Captive Portal* menggunakan perangkat *smartphone*

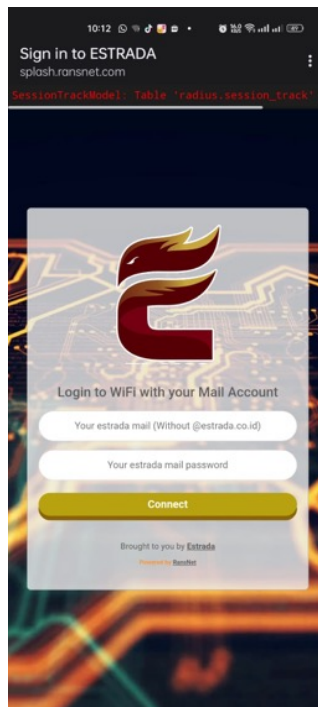
Pada tahap pengujian integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel menggunakan perangkat *smartphone*, penulis akan menghubungkan *smartphone* penulis dengan jaringan nirkabel yang sudah penulis buat sebelumnya dengan cara sebagai berikut.

Smartphone penulis terhubung ke dalam jaringan nirkabel dengan SSID “ESTRADA”



Gambar 5.14 : Smartphone Terkoneksi Pada Jaringan Nirkabel ESTRADA

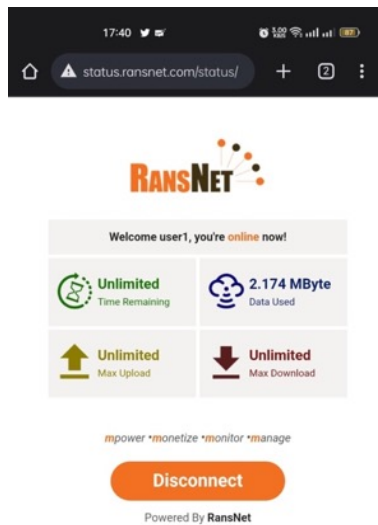
Setelah terhubung ke dalam jaringan nirkabel dengan SSID “ESTRADA”, secara otomatis akan diarahkan ke dalam *login page* untuk melakukan autentikasi sebelum mendapatkan akses *internet*.



Gambar 5.15 : Login Page Pada Smartphone

Penulis menggunakan *username* serta *password* yang sudah terdaftar di dalam OpenLDAP pada *zimbra mail server*.

Setelah berhasil terhubung ke dalam jaringan nirkabel, penulis mengakses halaman web status.ransnet.com/status untuk memverifikasi status perangkat dalam jaringan nirkabel.



*Gambar 5.16 : Verifikasi Status Perangkat Smartphone Pada Jaringan Nirkabel
ESTRADA*

Selanjutnya penulis mengulangi pengujian di atas menggunakan 10 *username* dan *password* yang sudah penulis daftarkan dalam OpenLDAP pada zimbra *mail server* sebagai sampel untuk menguji efektivitas integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* menggunakan *smarthpone* dengan hasil pengujian sebagai berikut.

No	Username	Status Autentikasi	Status Koneksi
1	User1	Berhasil Login	Terkoneksi Internet
2	User2	Berhasil Login	Terkoneksi Internet
3	User3	Berhasil Login	Terkoneksi Internet
4	User4	Berhasil Login	Terkoneksi Internet
5	User5	Berhasil Login	Terkoneksi Internet
6	User6	Berhasil Login	Terkoneksi Internet
7	User7	Berhasil Login	Terkoneksi Internet
8	User8	Berhasil Login	Terkoneksi Internet
9	User9	Berhasil Login	Terkoneksi Internet
10	User10	Berhasil Login	Terkoneksi Internet

Tabel 5.2 : Hasil Pengujian Menggunakan Smartphone

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan pengujian yang telah dilakukan, maka penulis mengambil kesimpulan sebagai berikut.

- a. Hasil rancangan penerapan integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* adalah menyiapkan 2 *server* yang terhubung ke dalam jaringan *internet*, salah satu *server* terpasang layanan *zimbra mail server* dimana sudah terpasang *package* OpenLDAP sebagai direktori *username* dan *password* untuk digunakan sebagai autentikasi ke dalam jaringan nirkabel, 1 *server* lainnya terpasang *package* FreeRADIUS untuk digunakan sebagai penghubung antara *router* HSG-100 dengan OpenLDAP *server* dalam melakukan autentikasi berhasil diimplementasikan.
- b. Integrasi FreeRADIUS dan OpenLDAP sebagai layanan autentikasi jaringan nirkabel berbasis *captive portal* dapat dinyatakan efektif karena penulis sudah melakukan pengujian dengan *laptop* dan *smartphone* dimana masing – masing perangkat menggunakan 10 *user* untuk melakukan autentikasi dengan hasil seluruh *user* pada masing – masing perangkat dapat terkoneksi ke dalam jaringan nirkabel dan mendapatkan akses *internet* setelah melakukan autentikasi pada *captive portal* dengan dukungan FreeRADIUS menggunakan *username* serta *password* yang sudah terdaftar dalam OpenLDAP.

6.2 Saran

Dalam penelitian ini, integrasi antara *router gateway* dengan *server* FreeRADIUS menggunakan jaringan *internet*, penulis menyarankan integrasi tersebut dibangun di dalam jaringan lokal agar koneksi antara perangkat tidak bergantung pada koneksi internet sehingga meningkatkan *availability* pada konektivitasnya.

DAFTAR PUSTAKA

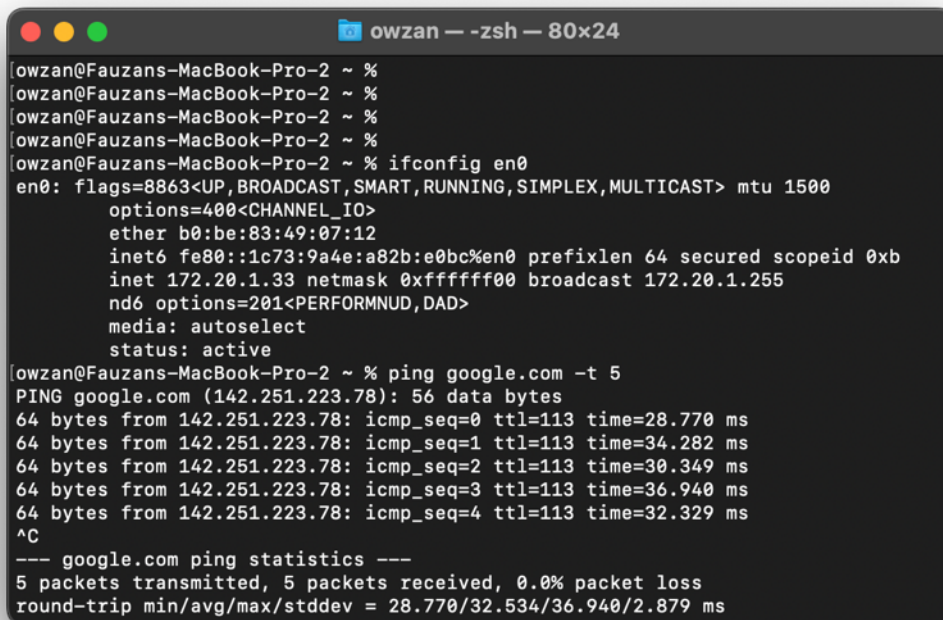
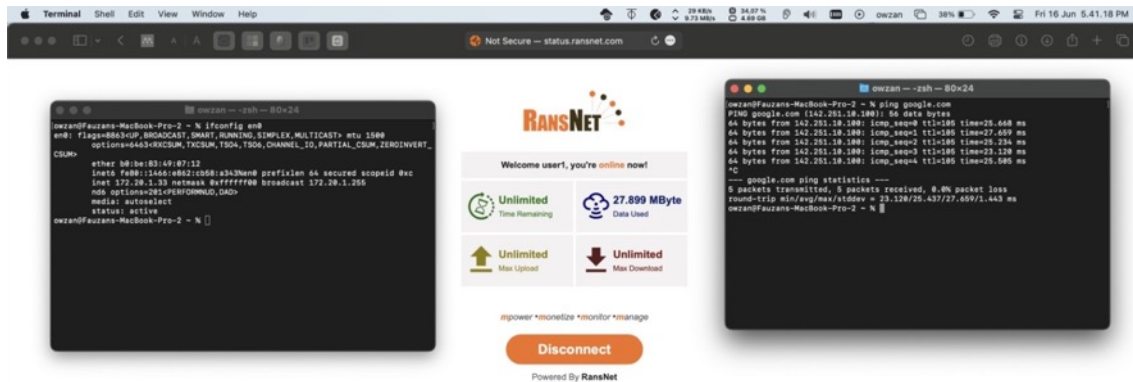
- Aryeh, F. L., Asante, M., & Y Danso, A. E. (2016). *Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication*. Ghana Journal of Technology, 1(1), 40–45.
- Butcher, M. (2007). *Directory Servers and LDAP* (D. Paterson, N. Bangera, V. P. Jha, & D. Chittar, Eds.). Brimingham: Packt Publishing Ltd.
- Gondohanindijo, J. (2012). Sistem Keamanan Jaringan NIRKABEL. *Majalah Ilmiah INFORMATIKA*, 3(2), 141–160.
- Hassell, J. (2002). RADIUS. O'Reilly Media, Inc.
- Karygiannis, T., & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*.
- Rigney, C., Rubens, A. C., Simpsons, W. A., & Willens, S. (2000). *Remote Authentication Dial In User Service (RADIUS)*.
- Sari, M., Siswati, T., Suparto, A. A., Jonata, Ambarsari, I. F., Azizah, N., ... Andalia, N. (2022). *Metodologi Penelitian* (1st ed.; A. Yanto, Ed.). Padang: PT. GLOBAL EKSEKUTIF TEKNOLOGI.
- Sharma, K., & Dhir, N. (2014). *A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison*. (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, 5(6), 7810–7813.
- Simargolang, M. Y., Widarma, A., & Irawan, M. D. (2021). Jaringan Komputer (J. E. Hutagalung & M. Amin, Eds.). Yayasan Kita Menulis.

- Siregar, R. L., & Prihanto, A. (2019). Implementasi Jaringan *Hotspot* dengan *Captive Portal* Zeroshell dan *User Management* LDAP. *Jurnal Manajemen Informatika*, 9(2), 87–96.
- Sondag, T., & Feher, J. (2007). *Open Source Wifi Hotspot Implementation*. *Information Technology and Libraries*, 26(2), 35–43.
- Syafrizal, M. (2005). *Pengantar Jaringan Komputer* (1st ed.; D. Prabantini, Ed.). Yogyakarta: CV. ANDI OFFSET.
- Walt, D. van der. (2011). *FreeRADIUS Beginner's Guide* (C. Apte, K. Pendey, A. Lewis, V. D'souza, & N. Shetty, Eds.). Birmingham: Packt Publishing Ltd.

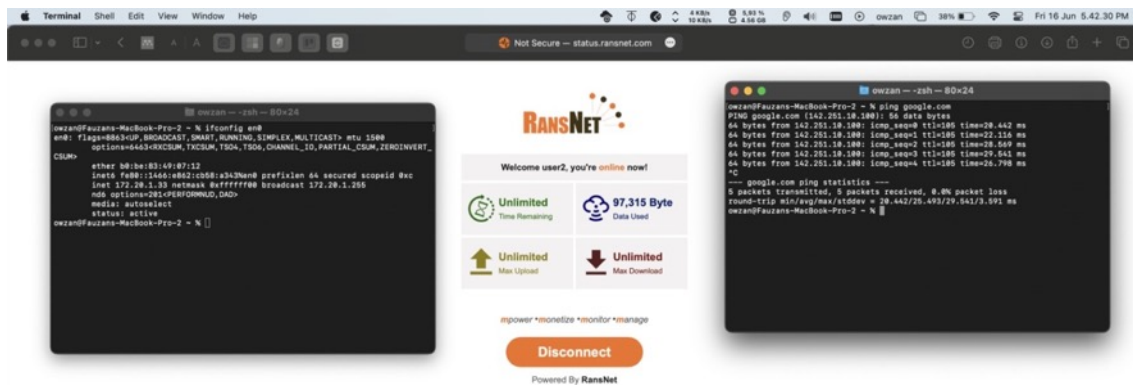
LAMPIRAN

Lampiran 1 – Screenshot status perangkat laptop pada jaringan nirkabel ES-TRADA

Menggunakan user1 untuk autentikasi pada laptop



Menggunakan user2 untuk autentikasi pada laptop

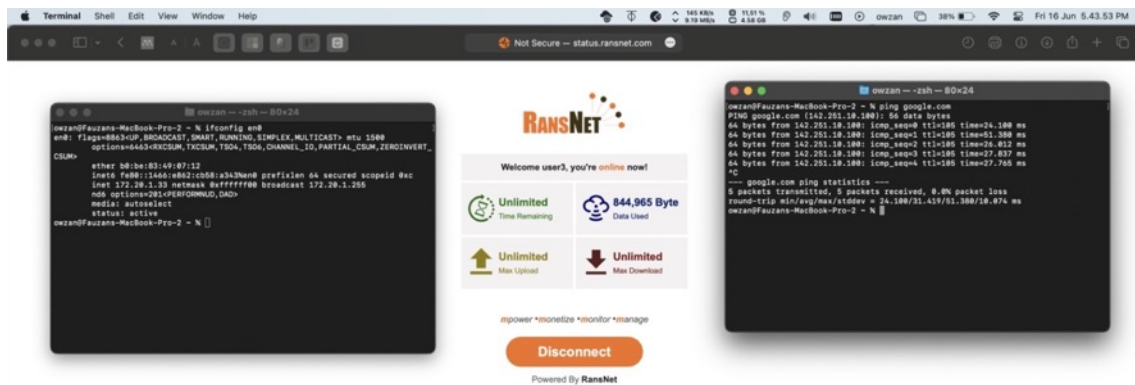


```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether b0:be:83:49:07:12
    inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
    inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=29.580 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=27.875 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=36.302 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=29.664 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=28.471 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.875/30.378/36.302/3.038 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

Menggunakan user3 untuk autentikasi pada laptop

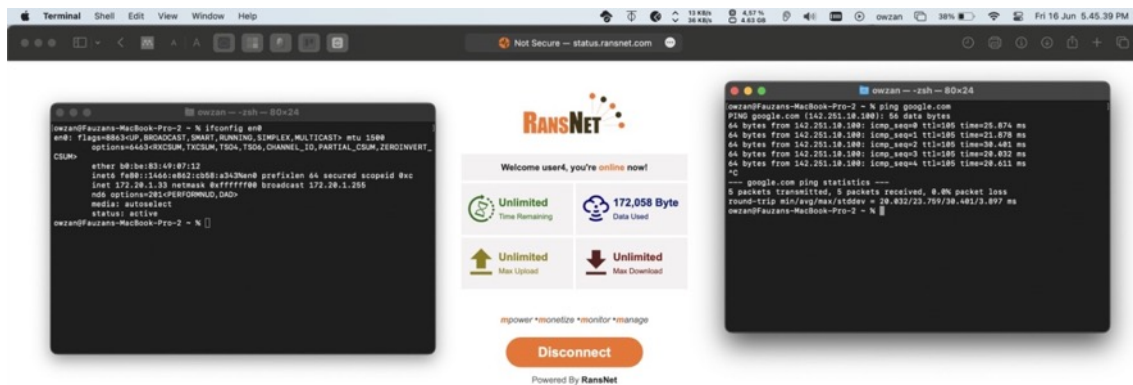


```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether b0:be:83:49:07:12
    inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
    inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=29.314 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=36.341 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=36.670 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=28.906 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=34.336 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 28.906/33.113/36.670/3.367 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

Menggunakan user4 untuk autentikasi pada laptop

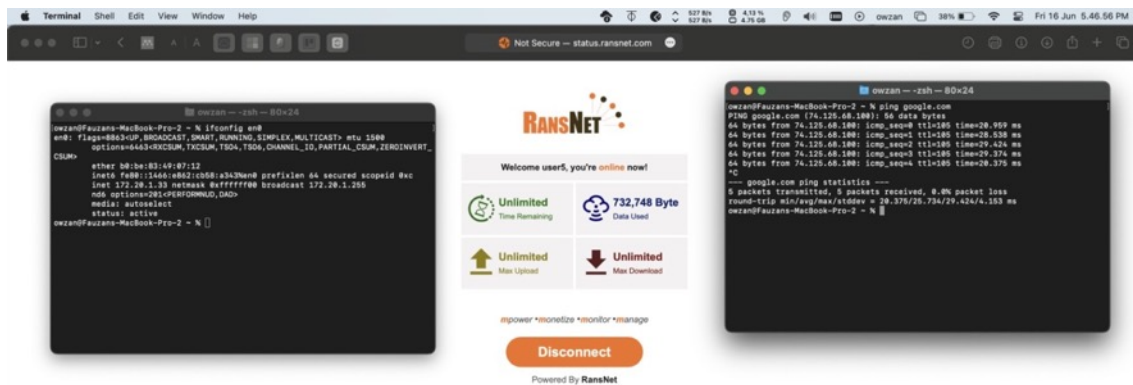


```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_ID>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active

owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=28.822 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=33.506 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=29.962 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=27.723 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=30.242 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.723/30.051/33.506/1.945 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

Menggunakan user5 untuk autentikasi pada laptop

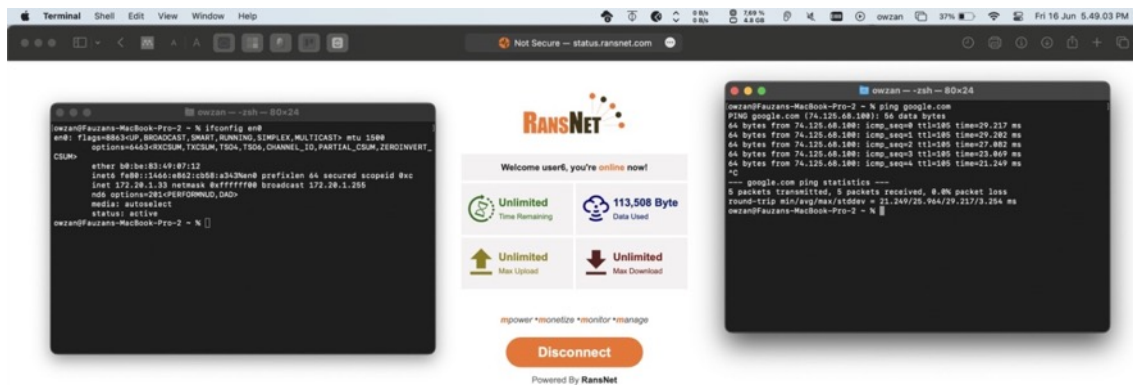


```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether b0:be:83:49:07:12
    inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
    inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=36.539 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=36.014 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=36.563 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=35.396 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=36.120 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 35.396/36.126/36.563/0.426 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

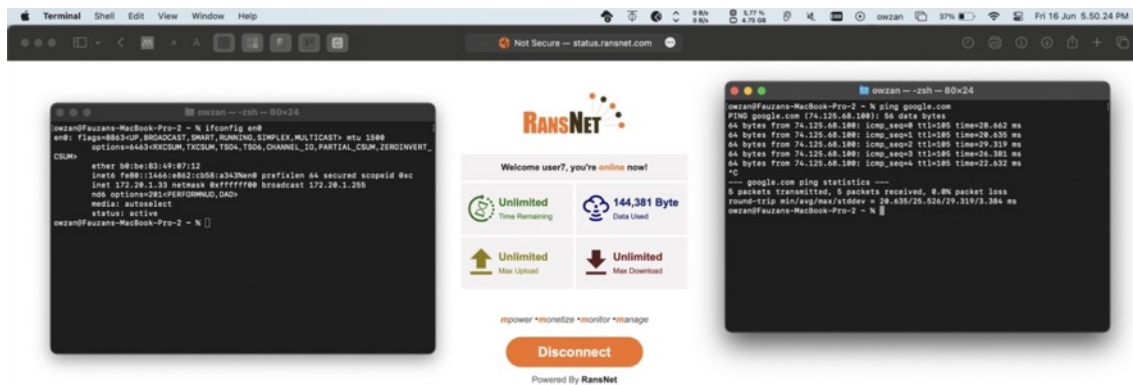

Menggunakan user6 untuk autentikasi pada laptop



```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_ID>
    ether b0:be:83:49:07:12
    inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
    inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=35.838 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=37.230 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=34.694 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=36.945 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=36.172 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 34.694/36.176/37.230/0.896 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

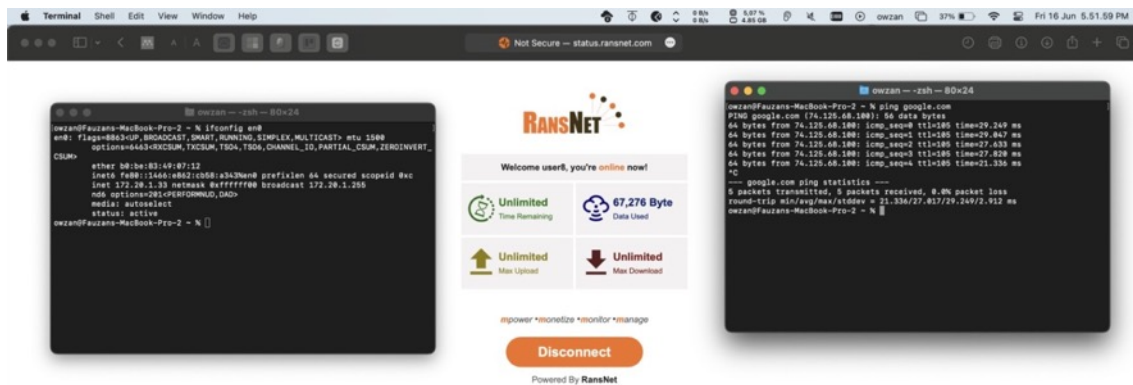
Menggunakan user7 untuk autentikasi pada laptop



```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=28.691 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=28.205 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=36.732 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=28.036 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=35.836 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 28.036/31.500/36.732/3.922 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```


Menggunakan user8 untuk autentikasi pada laptop



The screenshot shows a laptop screen with three windows. On the left is a terminal window with the following output:

```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
owzan@Fauzans-MacBook-Pro-2 ~ %
```

In the center is a RANSNET status page. It features the RANSNET logo, a 'Welcome user8, you're online now!' message, and a dashboard showing 'Unlimited Time Remaining', '67,276 Byte Data Used', and 'Unlimited Max Upload' and 'Unlimited Max Download' options. A 'Disconnect' button is at the bottom.

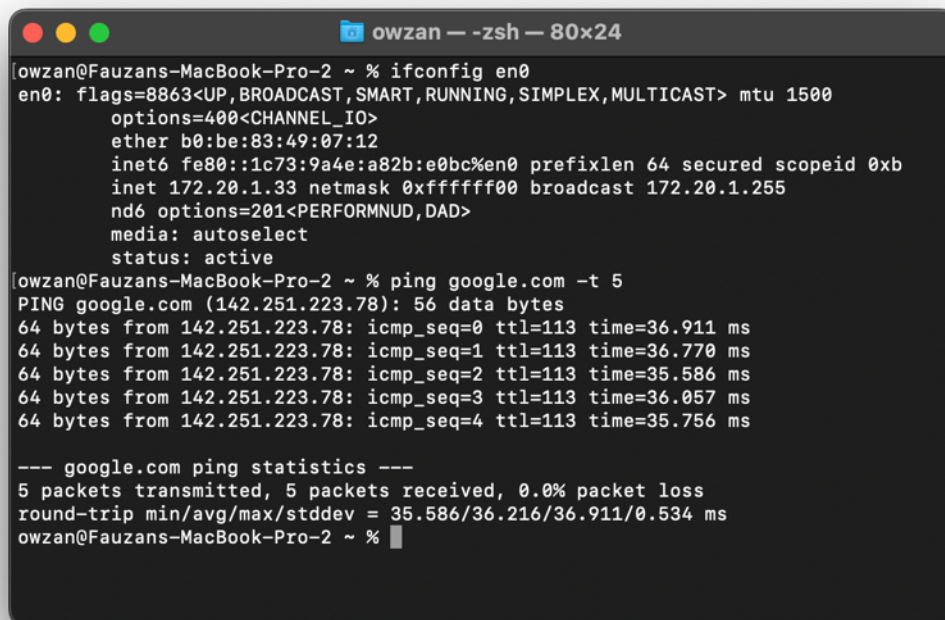
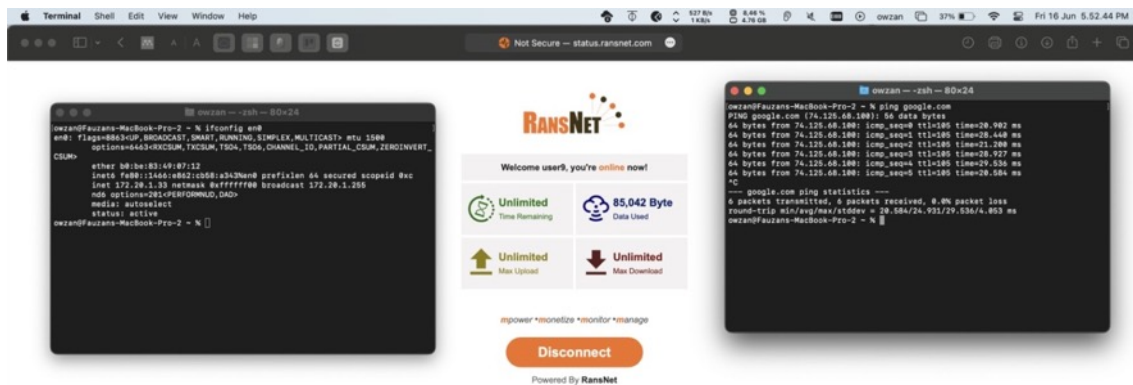
On the right is another terminal window showing the output of a ping command:

```
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com
PING google.com (74.125.68.100): 56 data bytes
64 bytes from 74.125.68.100: icmp_seq=0 ttl=105 time=29.249 ms
64 bytes from 74.125.68.100: icmp_seq=1 ttl=105 time=29.847 ms
64 bytes from 74.125.68.100: icmp_seq=2 ttl=105 time=27.638 ms
64 bytes from 74.125.68.100: icmp_seq=3 ttl=105 time=27.828 ms
64 bytes from 74.125.68.100: icmp_seq=4 ttl=105 time=23.326 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.336/27.817/29.249/2.912 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

```
owzan --zsh -- 80x24
[owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=36.837 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=36.162 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=29.624 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=43.015 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=28.444 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 28.444/34.816/43.015/5.304 ms
owzan@Fauzans-MacBook-Pro-2 ~ % ]
```

Menggunakan user9 untuk autentikasi pada laptop



Menggunakan user10 untuk autentikasi pada laptop

The screenshot shows a terminal window on the left with the following output:

```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
owzan@Fauzans-MacBook-Pro-2 ~ %
```

In the center is the RANSNET dashboard for user10, displaying:

- Welcome user10, you're online now!
- Unlimited Time Remaining
- 97,960 Byte Data Used
- Unlimited Max Upload
- Unlimited Max Download
- Disconnect button
- Powered By RANSNET

On the right is another terminal window showing ping statistics:

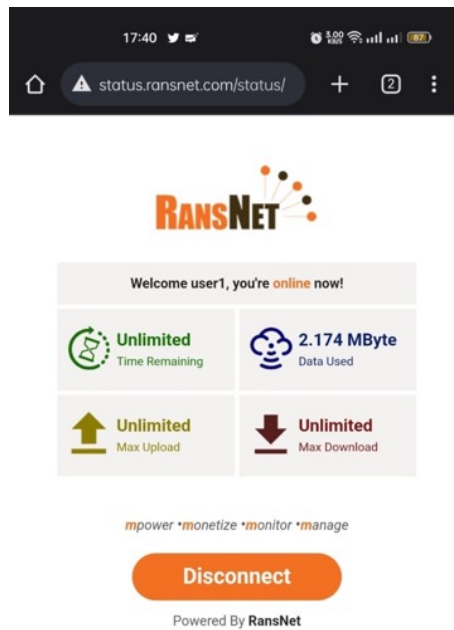
```
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com
PING google.com (142.251.18.138): 56 data bytes
64 bytes from 142.251.18.138: icmp_seq=0 ttl=105 time=28.596 ms
64 bytes from 142.251.18.138: icmp_seq=1 ttl=105 time=28.427 ms
64 bytes from 142.251.18.138: icmp_seq=2 ttl=105 time=29.480 ms
64 bytes from 142.251.18.138: icmp_seq=3 ttl=105 time=28.147 ms
64 bytes from 142.251.18.138: icmp_seq=4 ttl=105 time=27.524 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.488/28.831/28.417/3.948 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

```
owzan@Fauzans-MacBook-Pro-2 ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether b0:be:83:49:07:12
inet6 fe80::1c73:9a4e:a82b:e0bc%en0 prefixlen 64 secured scopeid 0xb
inet 172.20.1.33 netmask 0xfffff00 broadcast 172.20.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
owzan@Fauzans-MacBook-Pro-2 ~ % ping google.com -t 5
PING google.com (142.251.223.78): 56 data bytes
64 bytes from 142.251.223.78: icmp_seq=0 ttl=113 time=36.670 ms
64 bytes from 142.251.223.78: icmp_seq=1 ttl=113 time=27.641 ms
64 bytes from 142.251.223.78: icmp_seq=2 ttl=113 time=28.069 ms
64 bytes from 142.251.223.78: icmp_seq=3 ttl=113 time=27.727 ms
64 bytes from 142.251.223.78: icmp_seq=4 ttl=113 time=37.249 ms

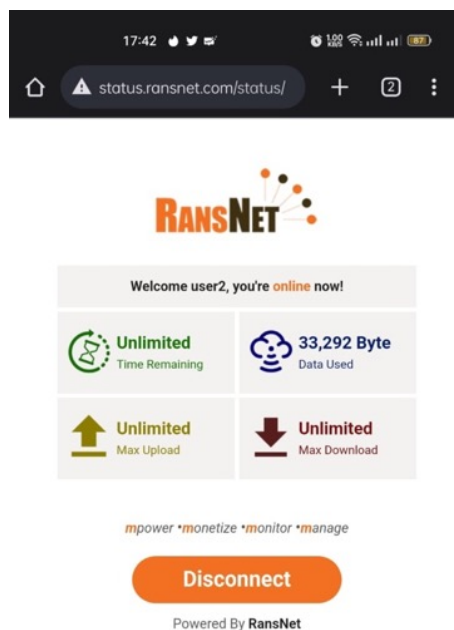
--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.641/31.471/37.249/4.487 ms
owzan@Fauzans-MacBook-Pro-2 ~ %
```

Lampiran 2 – Screenshot status perangkat *smartphone* pada jaringan nirkabel ES-TRADA

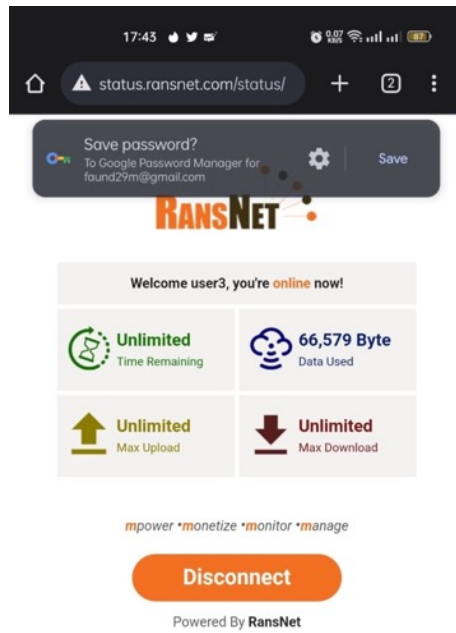
Menggunakan user1 untuk autentikasi pada *smartphone*



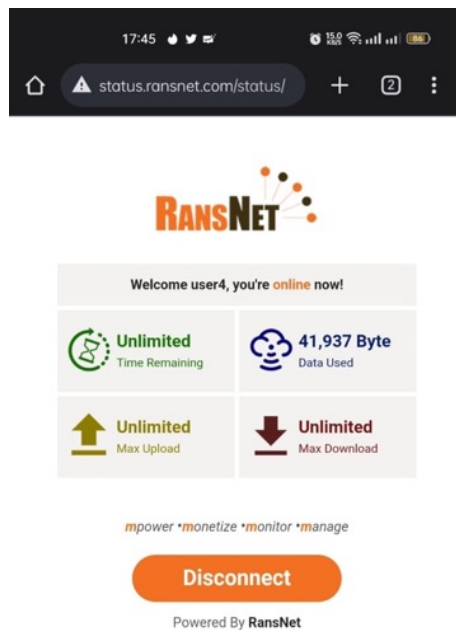
Menggunakan user2 untuk autentikasi pada *smartphone*



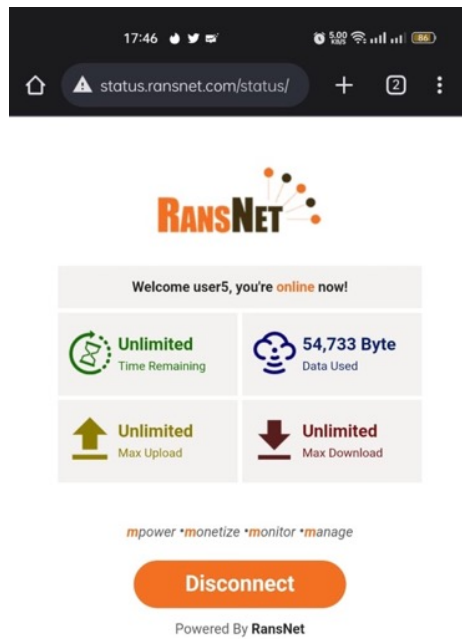
Menggunakan user3 untuk autentikasi pada *smartphone*



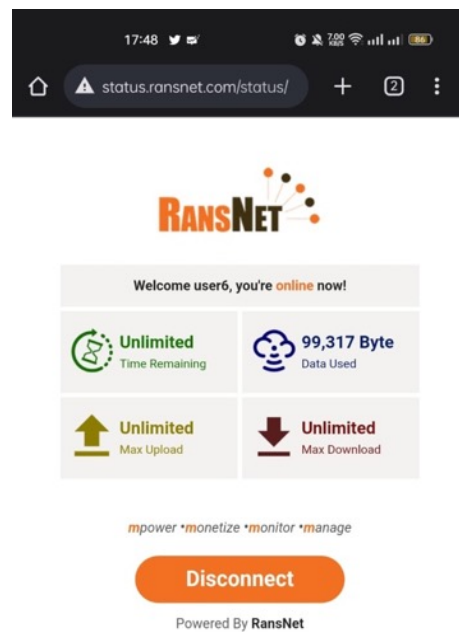
Menggunakan user4 untuk autentikasi pada *smartphone*



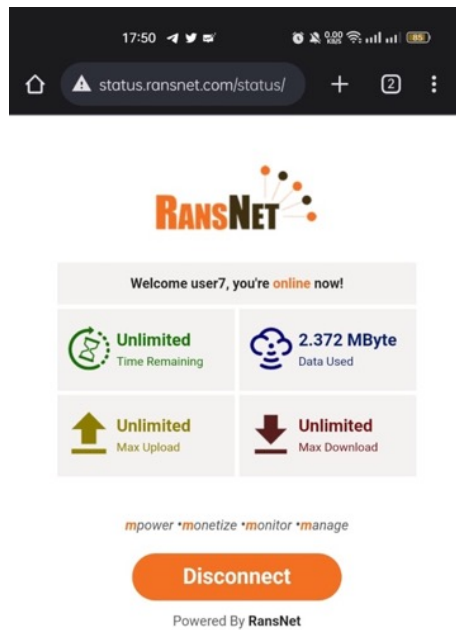
Menggunakan user5 untuk autentikasi pada *smartphone*



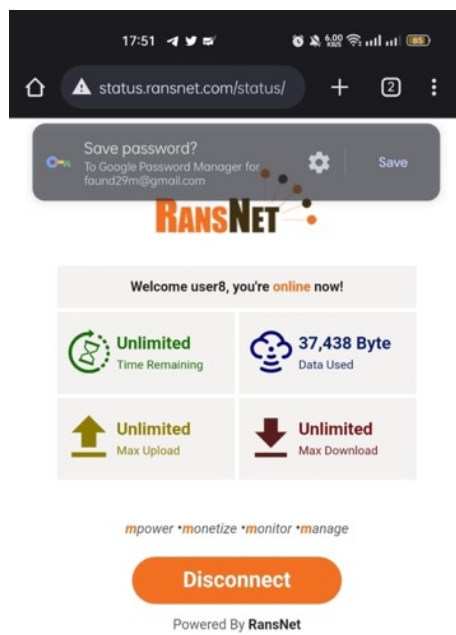
Menggunakan user6 untuk autentikasi pada *smartphone*




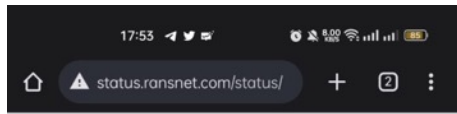
Menggunakan user7 untuk autentikasi pada *smartphone*







Menggunakan user8 untuk autentikasi pada *smartphone*



Menggunakan user9 untuk autentikasi pada *smartphone*



Welcome user9, you're **online** now!


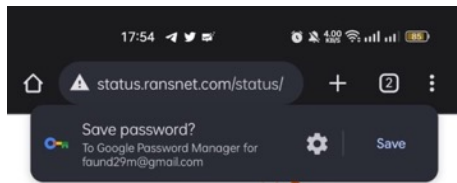
 Unlimited Time Remaining	 42,067 Byte Data Used
 Unlimited Max Upload	 Unlimited Max Download

*m*power • *m*onetize • *m*onitor • *m*anage





Disconnect

Powered By **RansNet**

Menggunakan user10 untuk autentikasi pada *smartphone*



Welcome user10, you're **online** now!

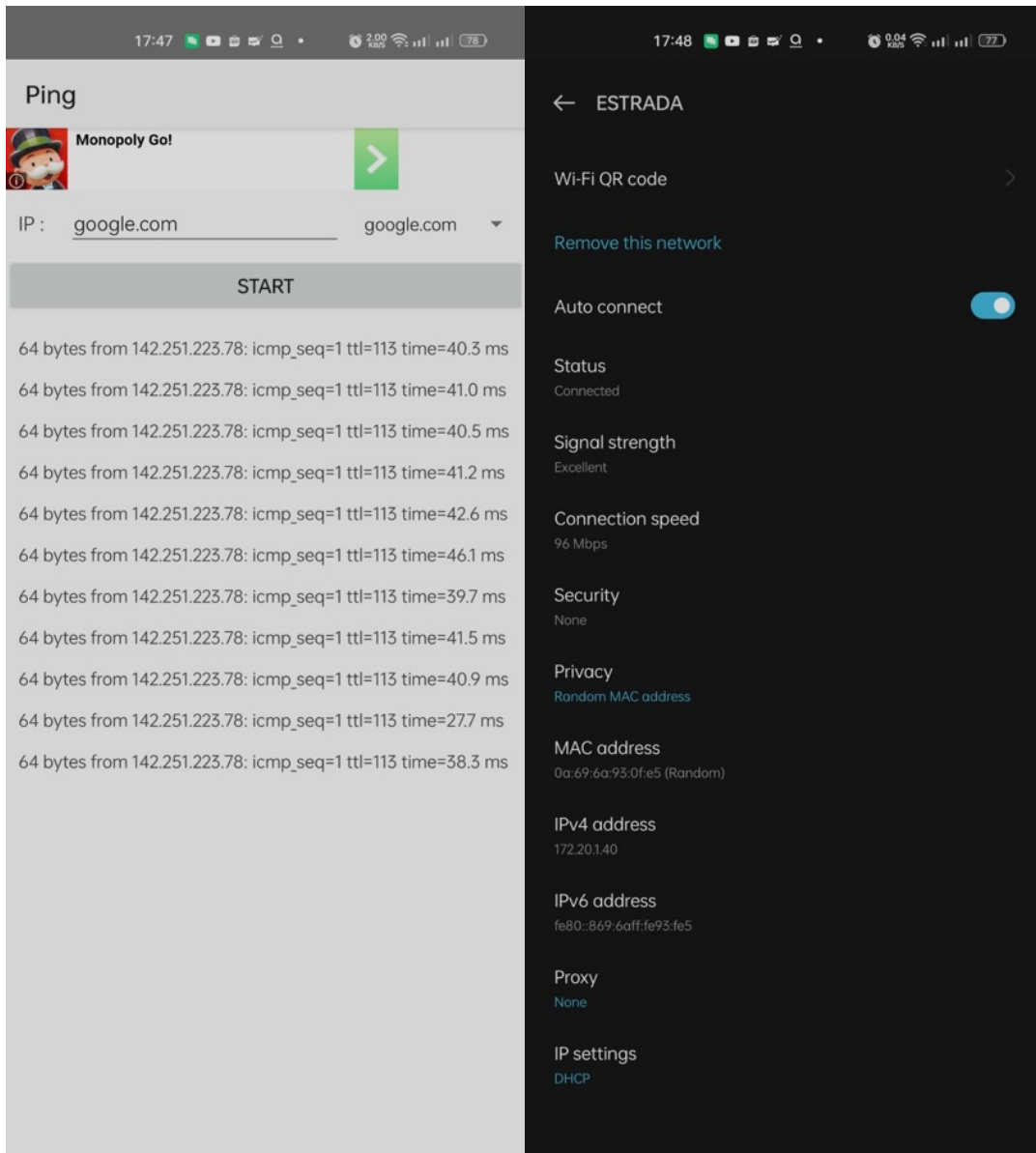
 Unlimited Time Remaining	 70,772 Byte Data Used
 Unlimited Max Upload	 Unlimited Max Download

*m*power • *m*onetize • *m*onitor • *m*anage

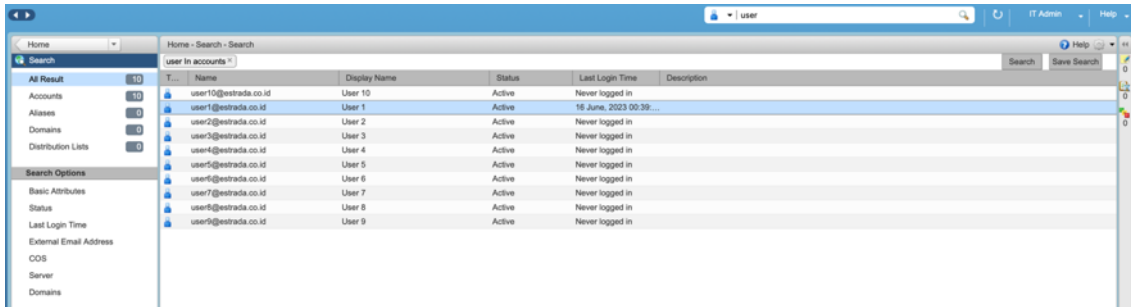
Disconnect

Powered By **RansNet**

Lampiran 3 – Screenshot IP dan hasil ping dari smartphone ke google.com untuk verifikasi koneksi internet



Lampiran 4 – Screenshot username user1 hingga user10 terdaftar dalam openldap pada zimbra mail server



Lampiran 5 – Screenshot daftar username lain yang sudah terhubung ke dalam jaringan nirkabel ESTRADA dan berhasil melakukan log in

