BAB III
ANALISIS DAN PERANCANGAN SISTEM

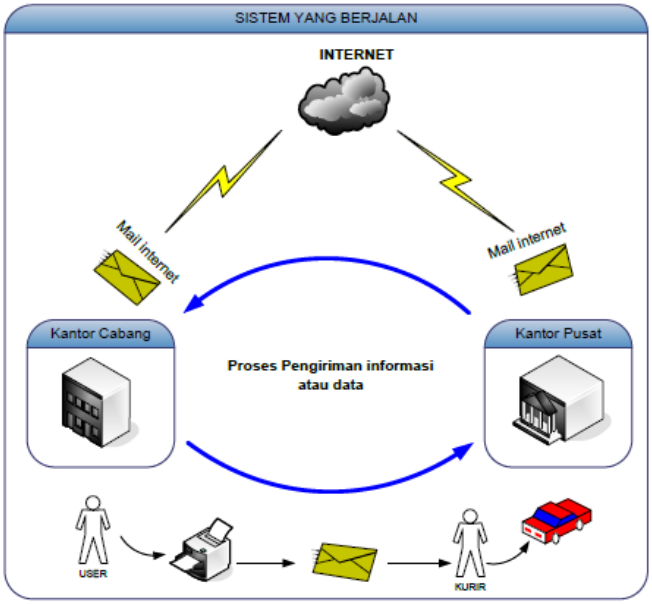
3.1. Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentangobyek yang akan diteliti. Bab ini akan menguraikan proses analisis pembangunansistem Point-to-Point protocol VPN dan perancangan sistem Point-to-Point VPN. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakananalisis kebutuhan – kebutuhan pokok sistem Point-to-Point VPN yang akandibangun.

3.1.1. Analisis Sistem yang berjalan

Bagian ini menggambarkan sistem yang sedang berjalan di PT.Padjadjaran Mitra Berdasarkan hasil penelitian, sistem yang sedang berjalan sekarang masih bersifat manual, antara lain :

1. Data absensi antara kantor pusat dan kantor cabang tidak bisa di share secara langsung
2. User yang akan mengirim, sharing atau akses data berupa file sharing, ke relasi atau kantor pusat, dikirim lewat pos-el (e mail internet).
3. Program aplikasi antara kantor cabang dan kantor pusat berdiri sendiri.
4. Semua laporan yang dibutuhkan di-print dan dikirim melalui jasa kurir.



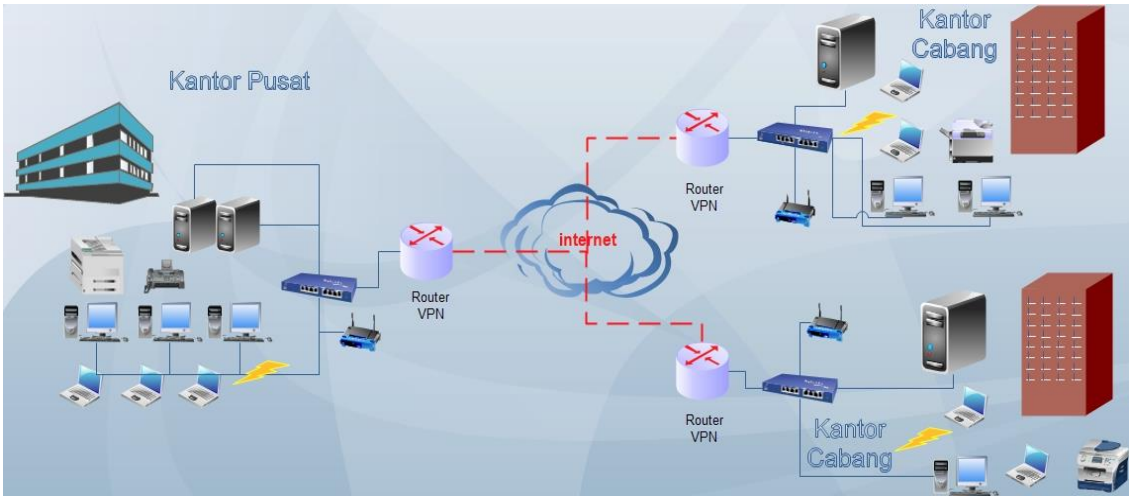
Gambar 3.1 Sistem yang berjalan di PT.Padjadjaran Mitra

Dari gambaran prosedur tersebut terdapat kelemahan- kelemahan sebagai berikut :

1. Lamanya proses penarikan absensi dikarenakan kantor sub devisi yang berjauhan.
2. Peroses pengolahan data memerlukan waktu yang lama .
3. Kurang efektif system penarikan data absensi yang berjalan.
4. Rendahnya tingkat keamanan data.

3.1.2. Solusi yang diusulkan

Dari permasalahan sebelumnya dapat diambil kesimpulan bahwa salah satualternatif solusi yang bisa diusulkan untuk mengatasi hal-hal tersebut adalahdengan jaringan VPN. VPN adalah sebuah teknologi komunikasi yangmemungkinkan suatu jaringan dapat terkoneksi ke jaringan publik dan dapatdigabungkan dengan jaringan lokal. Dengan cara tersebut akan didapatkan hakdan pengaturan yang sama seperti halnya berada di dalam kantor atau jaringanLAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.



Gambar 3.2 Jaringan VPN

3.1.3. Analisa kebutuhan sistem *Point-to-Point VPN*

VPN merupakan perpaduan dari teknologi tunneling dengan teknologi enkripsi. Teknologi tunneling bertugas untuk manangani dan menyediakankoneksi point-to-point dari sumber ke tujuannya. Sedangkan teknologi enkripsi menjamin kerahasiaan data yang berjalan di dalam tunnel.

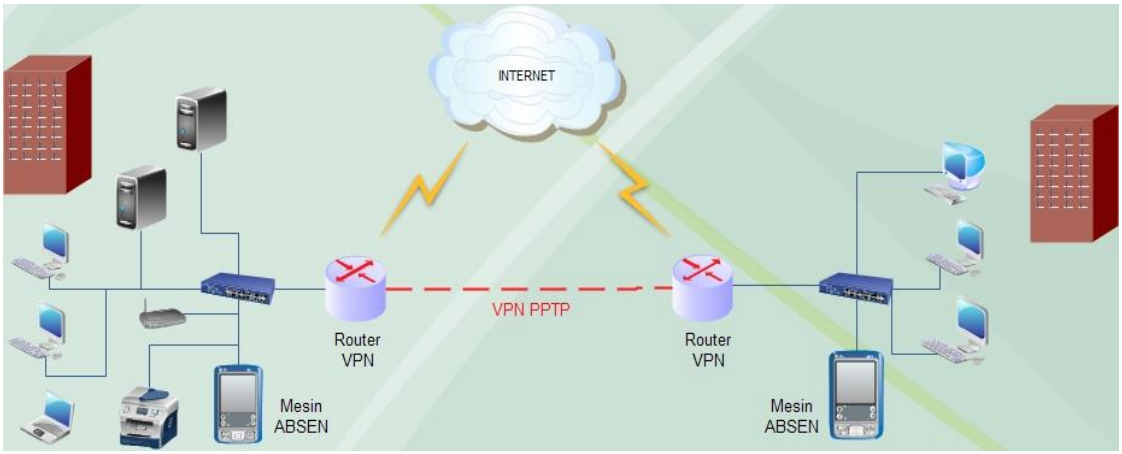
Untuk membangun VPN, ada beberapa tahap yang harus dilakukan :

1. Pemilihan jenis implementasi VPN
2. Pemilihan protokol VPN
3. Pemilihan server VPN

3.1.4. Jenis Implementasi VPN

Dilihat dari jenis implementasi VPN yang ada, dalam penelitian ini termasukdalam kategori *point-to-point* VPN. *point-to-point* VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang suatu perusahaan disebut *intranet point-to-point* VPN. Sedangkan bila VPN digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan), implementasi ini termasuk jenis *ekstranet*.

Dalam implementasinya, untuk dapat menghubungkan kantor pusat dengan kantor cabang, pada masing-masing kantor dibutuhkan sebuah router (*gateway)* sebagai PC router kantor cabang dan PC router sekaligus *server* VPN di kantor pusat. Berikut merupakan gambar topologi jaringan *site-to-site* VPN :



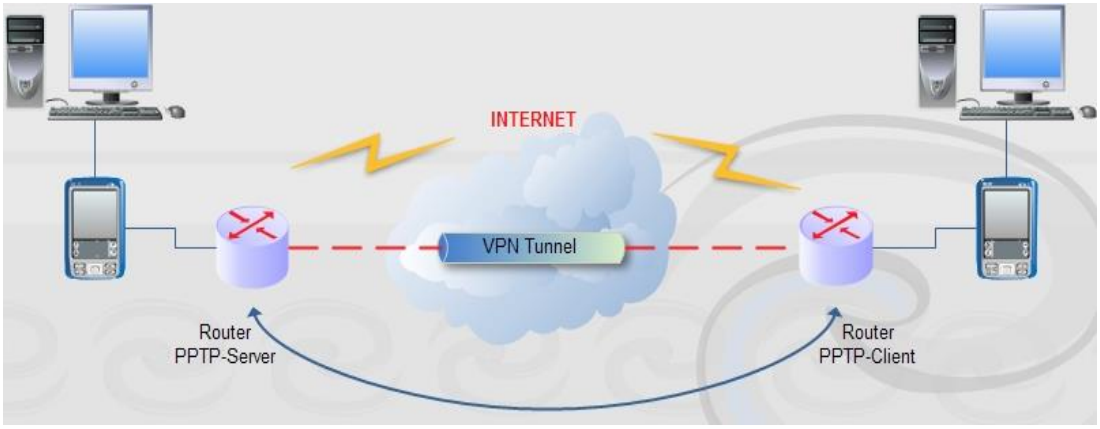
Gambar 3.3Point to Point VPN

3.1.5. Protokol yang digunakan dalam VPN

Untuk membangun site-to-site VPN, dibutuhkan protokol yang berfungsi mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan,aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metodemengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transferdata.

Protokol yang digunakan pada VPN menekankan pada authentikasi danenkripsi. Adanya sistem authentikasi akan mengijinkan klien dan server untukmenempatkan identitas orang yang berbeda di dalam jaringan secara benar.Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saatmelewati jaringan publik.

Dalam penelitian ini protokol yang digunakan adalah PPTP. PPTP yang diimplementasikan kedalam site-to-site VPN menggunakan mekanisme networkto-network, sehingga perlu dilakukan konfigurasi PPTP pada masing-masing gateway. Untuk dapat terkoneksi, masing-masing gateway melakukan sinkronisasi.Dibawah ini merupakan gambar dari cara kerja IP Security pada site-to-siteVPN:



Gambar 3.4 Cara kerja PPTP *Network-to-Network*

Komunikasi yang aman dibuat dengan menggunakan protokol PPTP secara tipikal terdiri dari tiga proses, dimana membutuhkan keberhasilan penyelesaian dari proses sebelumnya. Ketiga proses tersebut adalah :

1. PPP Connection and Communication

Suatu client PPTP menggunakan PPP untuk koneksi ke sebuah ISP dengan memakai line telepon standar atau line ISDN. Koneksi ini memakai protokol PPP untuk membuat koneksi dan mengenkripsi paket data.

2. PPTP Control Connection

Penggunaan koneksi ke internet dibuat oleh protokol PPP, protokol PPTP membuat control connection dari client PPTP ke server PPTP pada internet. Koneksi ini memakai TCP untuk membuat koneksi yang disebut dengan PPTP tunnel.

3. PPTP Data Tunneling

Terakhir, protokol PPTP membuat IP datagram yang berisi paket PPP yang terenkripsi dan kemudian dikirim melalui PPTP tunnel ke server PPTP. Server PPTP memeriksa IP datagram dan mendekripsi paket PPP, dan kemudian mengarahkan paket yang terdekripsi ke jaringan private.

3.1.6. Keamanan PPTP

PPTP secara luas memberikan layanan keamanan otentikasi dan enkripsi yang kuat dan tersedia pada computer yang menjalankan RAS dari server Windows NT versi 4.0 dan Windows NT Workstation versi 4.0 ke client PPTP di internet. PPTP juga dapat melindungi server PPTP dan jaringan private dengan mengabaikan semuanya kecuali PPTP traffic. Walaupun kemanannya kuat, PPTP sangat mudah digunakan dengan adanya firewalls.

1. Otentikasi

Otentikasi dibutuhkan server network access ISP dalam initial dial-in. Jika otentikasi ini dibutuhkan maka sangat sulit untuk log on ke server network access ISP; otentikasi ini tidak berhubungan dengan otentikasi berbasis Windows NT. Dengan kata lain, jika server windows NT versi 4.0 sebagai server PPTP, maka server tersebut yang akan mengendalikan semua akses ke jaringan private. Dengan kata lain, server PPTP merupakan gateway menuju jaringan private. Server PPTP membutuhkan proses logon berbasis Windows NT standar. Semua client PPTP harus memiliki user name dan password. Oleh karena itu keamanan logon akses terbatas dengan menggunakan komputer dengan Windows NT server atau windows NT workstation versi 4 harus sama dengan keamanan saat logging pada komputer berbasis windows NT yang terkoneksi ke LAN lokal. Otentikasi client remote PPTP dilakukan dengan menggunakan metode otentikasi PPP yang sama dimana client RAS langsung terhubung dengan server RAS. User account terletak dalam directory service windows NT server versi 4.0 dan diatur melalui user manager untuk domain. User

manager ini menyediakan pengaturan terpusat yang terintegrasi dengan user account jaringan private yang tersedia. Hanya account yang diakui saja yang bisa mengakses jaringan. Memiliki password yang sulit ditebak akan mengurangi resiko terhadap brute force attack karena proses otentikasi tersebut rentan terhadap brute force attack.

2. Access Control

Setelah proses otentikasi, semua akses ke private LAN diteruskan dengan memakai model keamanan berbasis windows NT. Akses ke sumber pada drive NTFS atau sumber jaringan lainnya membutuhkan ijin yang sesuai. Direkomendasikan bahwa sistem file NTFS digunakan untuk sumber file yang diakses oleh client PPTP.

3. Enkripsi Data

Untuk enkripsi data, PPTP menggunakan proses enkripsi RAS "shared-secret". Disebut "shared-secret" karena pada awal dan akhir koneksi PPTP membagi kunci enkripsi. Dalam implementasi Microsoft dari RAS, shared secret disebut user password. (metode enkripsi lainnya berbasis enkripsi pada tersedianya kunci untuk public; metode enkripsi kedua ini dikenal sebagai public key encryption). PPTP menggunakan skema PPP encryption dan PPP compression. CCP (Compression Control Protocol) digunakan PPP untuk enkripsi. User name dan password PPTP client tersedia untuk PPTP server dan diberikan oleh PPTP client. Kunci enkripsi dihasilkan dari penyimpanan password yang telah di-hash yang terdapat di client dan server. RSA RC4 standar digunakan untuk menghasilkan session key 40 bit berdasarkan pada password client. Kunci ini dipakai untuk mengenkripsi semua data yang melewati internet, untuk melindungi koneksi private agar aman.

Data pada paket-paket PPP dienkripsi. Paket PPP yang berisi blok data terenkripsi kemudian dibungkus hingga manjadi IP datagram yang besar untuk routing melalui internet ke server PPTP. Jika hacker internet melakukan intercept IP datagram, ia hanya akan mendapatkan media header, IP header dan paket PPP berisi blok data yang terenkripsi bukan data yang terdekripsi.

4. PPTP Packet Filtering

Keamanan jaringan dari aktivitas kejahatan dapat meningkat dengan memakai PPTP filtering pada server PPTP. Ketika PPTP filtering digunakan, PPTP server pada

jaringan private menerima dan mengarahkan paket-paket PPTP dari user yang terotentikasi. Hal ini akan melindungi semua paket yang berasal dari server PPTP dan jaringan private. Berhubungan dengan enkripsi PPP, maka hal ini akan menjamin hanya data terenkripsi yang berhak masuk dan keluar private LAN..

3.1.7. Infrastruktur Sistem *point-to-point* VPN

Infrastruktur sistem point-to-point terbagi menjadi dua macam, yaitu perangkatkeras dan perangkat lunak, yang kedua bagian infrastruktur tersebut salingmendukung satu sama lain.

Dalam pembangunan point-to-point VPN, terdapat beberapa kebutuhan hardware dan software di sisi server dan client yang harus dipenuhi, yaitu sebagaiberikut :

1. Router VPN Server

   Adapun spesifikasi hardware yang digunakan sebagai Router server VPN yang dilakukan memiliki spesifikasi sebagai berikut :

3.1 Tabel Mikrotik RB 450

Product Code	RB450
Architecture	MIPS-BE
CPU	AR7130 300MHz
Current Monitor	No
Main Storage/NAND	64MB
RAM	32MB
SFP Ports	0
LAN Ports	5
Gigabit	No
Switch Chip	1
MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
SIM Card Slots	No
USB	No
Memory Cards	No
Power Jack	10-28V
802.3af Support	No

POE Input	10-28V
POE Output	No
Serial Port	DB9/RS232
Voltage Monitor	No
Temperature Sensor	No
Dimentions	150mm x 105mm
Operating System	RouterOS
Temperature Range	-30C .. +60C
RouterOS License	Level5

b. Client VPN

Adapun spesifikasi hardware yang digunakan sebagai Router client VPN yang dilakukan memiliki spesifikasi sebagai berikut :

1. Router VPN Client (Mikrotik RB 750)

Tabel 3.2 Router VPN Client (Mikrotik RB 750)

Product Code	RB750
Architecture	MIPS-BE
CPU	AR7241 400MHz
Current Monitor	No
Main Storage/NAND	64MB
RAM	32MB
SFP Ports	0
LAN Ports	5
Gigabit	No
Switch Chip	1
MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
SIM Card Slots	No
USB	No
Memory Cards	No
Power Jack	10-28V
802.3af Support	No
POE Input	10-28V
POE Output	No
Serial Port	No
Voltage Monitor	No
Temperature Sensor	No

Dimentions	113x89x28mm
Operating System	RouterOS
Temperature Range	-40C .. +55C
RouterOS License	Level4

2. Software

   Spesifikasi perangkat lunak yang digunakan pada komputer penggunasistem VPN adalah Microsoft Windows XP dan aplikasi Absensi Time Attendance yang merupakan aplikasi yang digunakan untuk penarikan absensi.

3.1.8. Analisis Penggunaan

Sistem site-to-site VPN yang di bangun akan digunakan untuk penggunayang memiliki kualifikasi sebagai berikut :

Tabel 3.3 Karakteristik Pengguna

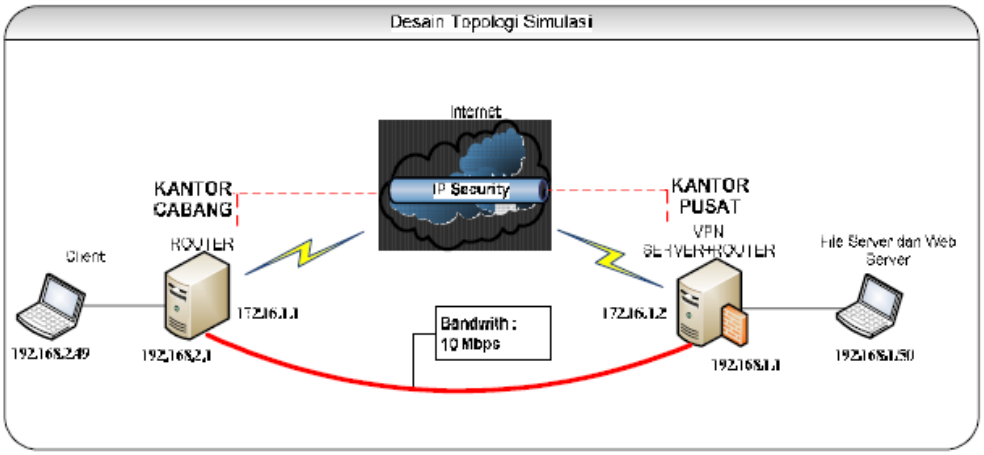
Nama Pengguna	Kualifikasi
Administrator Jaringan	Kualifikasi yang harus dimiliki administrator jaringan yaitu memiliki keahlian di bidang jaringan komputer, menangani LAN, mengkonfigurasi jaringan (khususnya VPN)
HRD dan Assisten	Kualifikasi yang harus dimiliki karyawan yaitu memiliki kemampuan dasar di bidang pengelolaan karyawan, dapat mengoperasikan aplikasi Absensi Time Attendance.

3.2. Perancangan Sistem

Pada bagian ini akan dibahas mengenai perencanaan infrastruktur VPN, konfigurasi, dan instalasi dari perangkat keras maupun perangkat lunak yang dipergunakan pada jaringan untuk implementasi VPN tersebut. Infrastruktur yang mendukung untuk jaringan ini terdiri dari server dan client yang berupa PC, hub/switch, dan perangkat lunak pendukung.

3.3. Arsitektur Simulasi

Dalam simulasi sistem point-to-point VPN akan dilakukan melalui jaringan LAN,dan adapun desain topologi jaringan yang digunakan adalah sebagai berikut :



Gambar 3.5 Desain Topologi Simulasi

Perangkat pendukung pada simulasi point-to-point VPN terdiri dari beberapa hardware dan software yang tertera dalam tabel di bawah ini :

Tabel 3.4 Perangkat pendukung infrastruktur simulasi

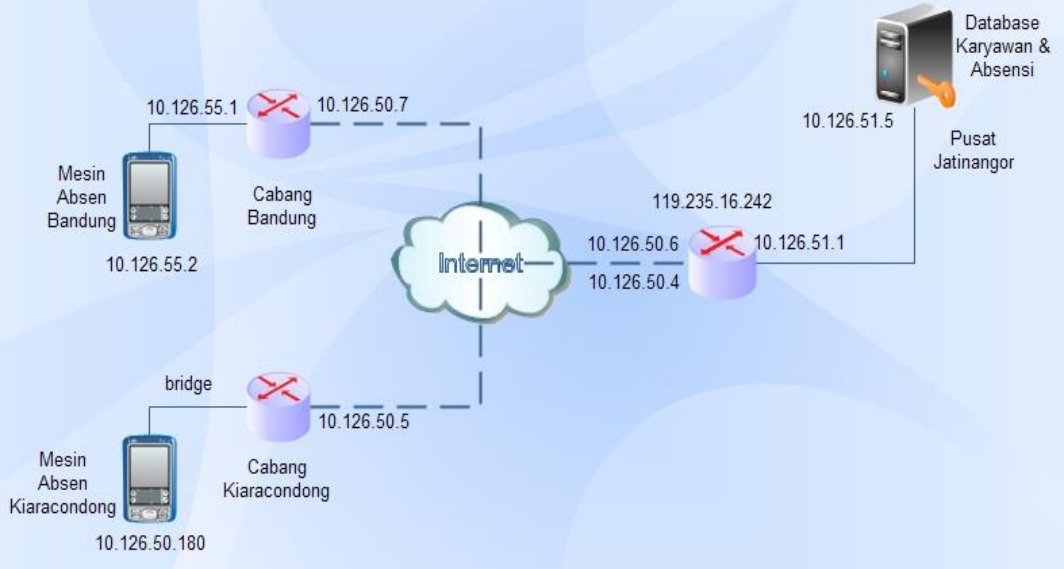
Hardware	Mikrotik RB450
	Mikrotik RB750
	Switch D-link 16 port
	Mesin Absen Finger Print Icon Plus
	Kabel UTP category 5e dan konektor RJ-45.
Software	Windows Xp
	Aplikasi Absensi Time Attendance

Selain kebutuhan hardware dan software yang tertera pada tabel di atas,terdapat pembagian alokasi IP address yang akan digunakan pada saat simulasi.Pada server VPN telah dilakukan konfigurasi DHCP, sehingga IP Address clientakan bersifat dinamis. Dibawah ini merupakan tabel alokasi IP Address pada saatsimulasi:

Tabel 3.5 Alokasi IP address untuk Router

Device	IP Address	Interface
Router VPN PPTP-Server	10.126.50.6	pptp-out
	10.126.50.4	pptp-out
	119.235.16.242	Publik
	10.126.51.1	Ether1

Router PPTP-Client Bandung	10.126.50.7	Pptp-out
	10.126.55.1	Ether 5
Mesin Absen Bandung	10.126.55.2	Eth1
Router PPTP-Client Kiaracondong	10.126.50.5	pptp-out
	bridge	Ether 3
Mesin Absen Kiaracondong	10.126.50.180	Eth1
Database Karyawan (Aplikasi Time Attendance)	10.126.51.5	Eth1



Gambar 3.6 Desain Alokasi IP

3.4. Konfigurasi sistem *point-to-point* VPN

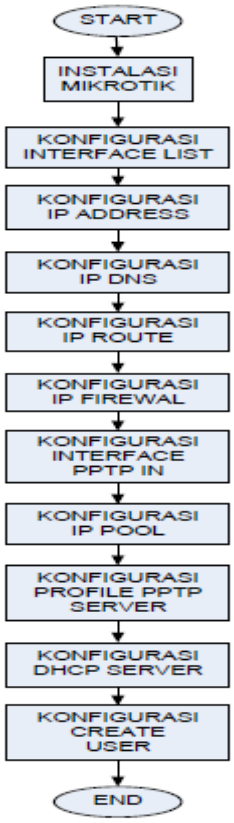
Konfigurasi VPN server dan client adalah tahap dimana dilakukannya pengaturan-pengaturan parameter yang terdapat pada sebuah perangkat lunak.Adapun parameter-parameter yang akan kita setting pada komputer server,router dan client adalah :

3.4.1. Router yang digunakan sebagai server VPN

Tahapan konfigurasi yang harus di lakukan dalam tahap perancangan serveradalah:

a. Tahap konfigurasi IP Pool
b. Tahap konfigurasi IP Routes
c. Tahap konfigurasi PPP sebagai server VPN
d. Tahap konfigurasi DHCP server
e. Tahap konfigurasi firewall NAT Masquerade dan NAT bypass
f. Tahap konfigurasi PPTP

Untuk lebih memperjelas, tahap konfigurasi akan ditampilkan denganFlowchart seperti pada gambar dibawah ini :



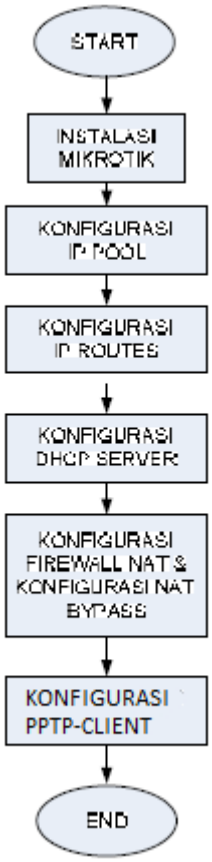
Gambar 4.1 Flowchart Konfigurasi Server

3.4.2. Router yang digunakan sebagai PPTP-Client

Tahapan konfigurasi yang harus di lakukan dalam tahap perancangan server adalah:

a. Tahap konfigurasi IP Pool
b. Tahap konfigurasi IP Routes
c. Tahap konfigurasi DHCP server
d. Tahap konfigurasi firewall NAT Masquerade dan NAT bypass
e. Tahap konfigurasi PPTP-Client
f. Tahap konfigurasi DNS

Untuk lebih memperjelas, tahap konfigurasi akan ditampilkan denganFlowchart seperti pada gambar dibawah ini :



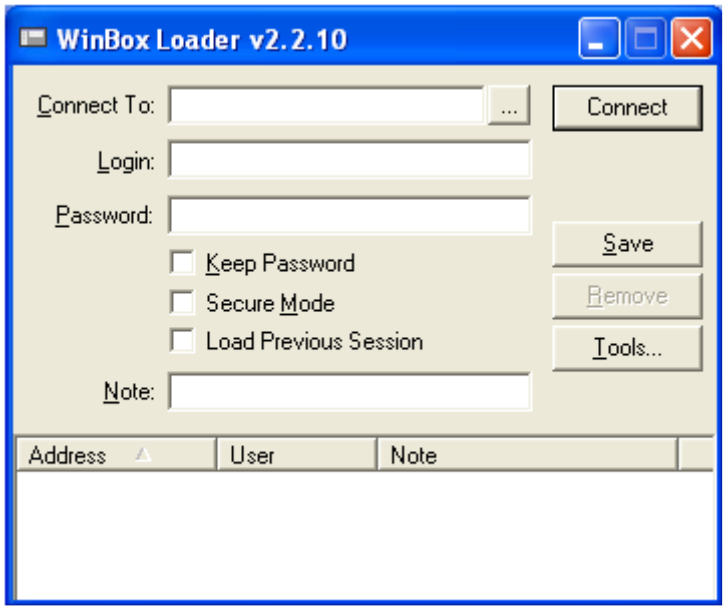
Gambar 4.2 Flowchart Konfigurasi Di Router

3.5. Perancangan dan Konfigurasi *server* VPN

Berikut ini akan dijelaskan tahap-tahap pengkonfigurasian VPN dengan pptp-server. konfigurasi, dan instalasi dari perangkat keras maupun perangkat lunak yang dipergunakan pada jaringan untuk implementasi VPN tersebut. Infrastruktur yang mendukung untuk jaringan ini terdiri dari server dan client yang berupa PC, hub/switch, dan perangkat lunak pendukung.

3.5.1. Tahap membuat interface PPTP in dan mengaktifkan fitur PPTP server

Mikrotik Sudah bisa di-remote baik dengan telenet maupun dengan winbox. Winbox adalah sebuah utility untuk melakukan remote ke server mikrotik dalam mode GUI (Grapihcal User Interface). Dalam pembangunan server VPN, untuk mengaktifkan fitur PPTP server dan membuat interface PPTP in, kita menggunakan utility winbok.



Gambar 4.3 WinBox Loader

Dalam mengaktifkan Fitur PPTP server ada beberapa tahapan. Parameter-parameter yang di setting :

1. Pembuatan interface pptp in

   Setelah proses instalasi server, tahapan selanjutnya akan dilakukan konfigurasi PPTP Server. (Point To Point Tunneling Protocol), atau pembuatan interface PPTP in.



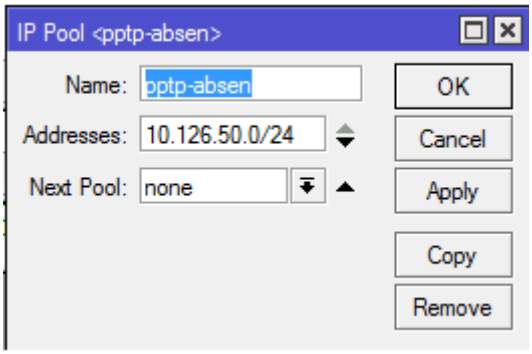
Gambar 4.4 Pembuatan Interface PPTP in

Pembuatan interface pptp-in menggunakan console diterminal

[admin@MikroTik] > interface pptp-server add name=pptp-in1 user=vpn disable=no

2. Setting IP address untuk Client

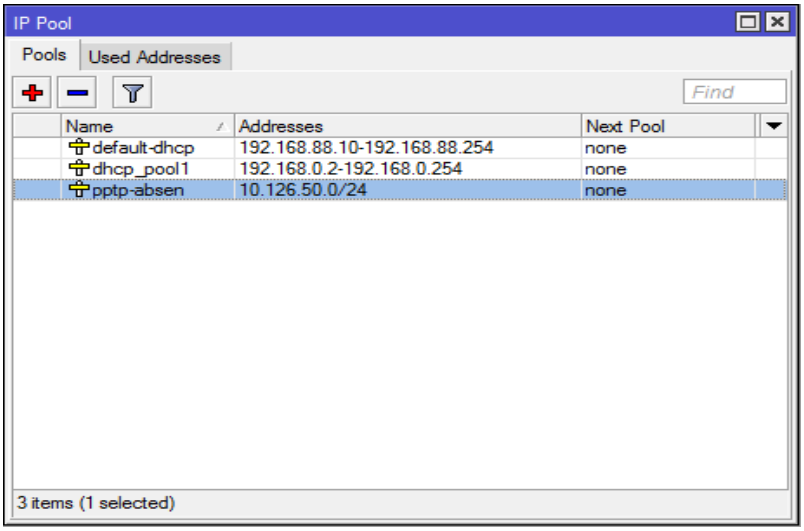
Dalam pembuatan sekelompok IP Address yang akan kita buat untuk mengalokasikan sejumlah IP Address untuk VPN Client per-user yang nanti akan terkoneksi ke Mikrotik VPN Server. Selain mengunakan IP Pool, kita juga bisa memberikan IP Address per-user satu per satu. Tapi jumlah VPN Client di PT Bandung Arta Mas banyak, cara yang tepat untuk pembuatanya adalah dengan menggunakan IP Pool. Setting ip address untuk client di PT Padjadjaran Mitra dimulai dari IP 10.126.50.0/24



Gambar 4.5 Pembuatan IP Pool

Pembuatan IP Pool menggunakan console diterminal

[admin@MikroTik] > ip pool add name=pptp-absen next-pool=none ranges=10.126.50.0/24

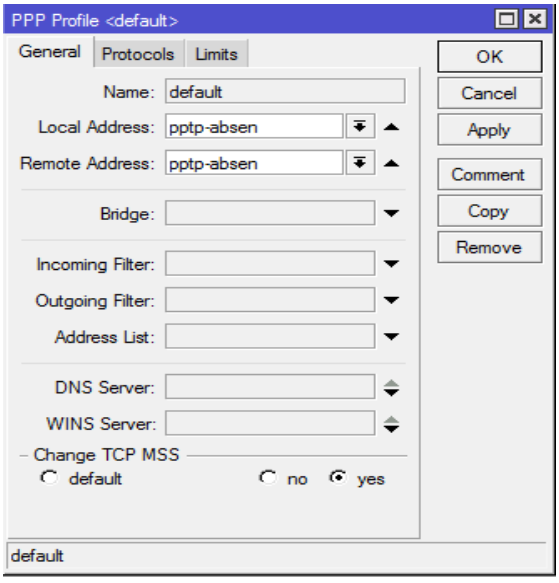


Gambar 4.6 IP address untuk client

Menampilkan IP address untuk client di IP Pool menggunakan console diterminal
[admin@MikroTik] > ip pool print

3. Pembuatan Profile PPTP Server

Local Address adalah IP Address yang digunakan sebagai VPN Gateway oleh Mikrotik. Remote Address adalah IP Address yang akan diberikan kepada masing-masing VPN Client dan IP Address inilah yang dikenali dan berkomunikasi dengan PC yang lain.



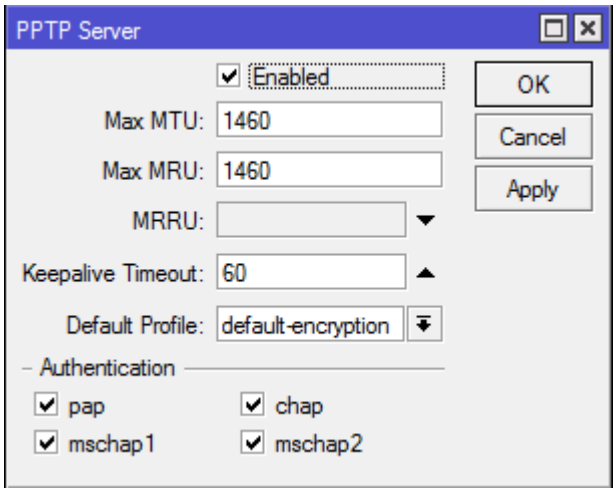
Gambar 4.7 Pembuatan profile PPTP

Pembuatan profile PPTP menggunakan console diterminal

[admin@MikroTik] > ppp profile add name=default local-address =pptp-absen remote-address=pptp-absen use-compression= default use-vj-compression=default use-encryption=yes change-tcp-mss=default

4. Mengaktifkan Fitur PPTP Server

Option inilah yang menentukan Fitur PPTP SERVER berfungsi apa tidak pada Mikrotik kita. Aktifkan / centang tanda checkmark “ENABLE” lalu pilih Default Profile yang telah kita buat.



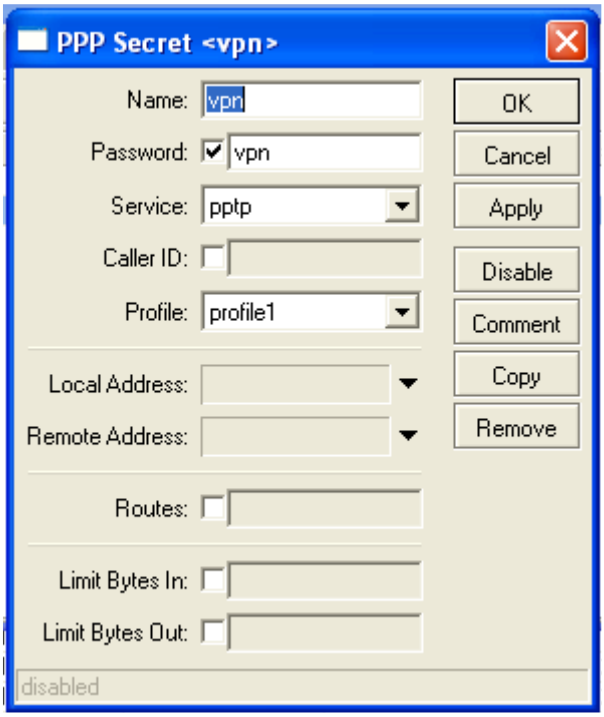
Gambar 4.8 Mengaktifkan PPTP server

Mengaktifkan PPTP server menggunakan console diterminal

[admin@MikroTik] > interface pptp-server enable pptp-in1

5. Membuat Authenticated User / VPN User.

Tahapan membuat User VPN ada dimenu tab “SECREET”. Setting Username, Password, Service dan Profile seperti gambar dibawah ini :



Gambar 4.9 Membuat User VPN client

Membuat user VPN menggunakan console diterminal

[admin@MikroTik] > ppp secret add name=vpn password=vpn service=pptp profile=profile1 disable=no

3.6. Perancangan dan Konfigurasi PPTP-CLIENT

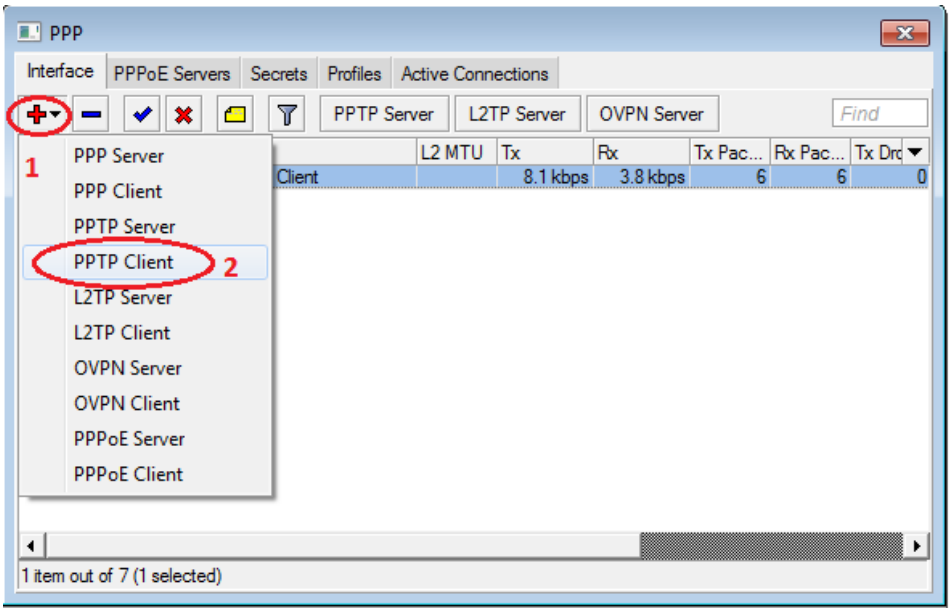
Berikut ini akan di jelaskan tahap-tahap pengkonfigurasian pptp-client yang berada pada tiap-tiap router kantor cabang. Mulai dari tahap pembuatan konfigurasi pppt- client

3.6.1. Tahap Pembuatan Konfigurasi pptp-client

Setelah router terkoneksi dengan internet.Terlebih dahulu harus melakukan pengaktifan pptp-client dengan melakukan login sesuai dengan autentikasi user yang telah diberikan oleh server.

1.Pilih menu ppp pada menu sebelah kiri,

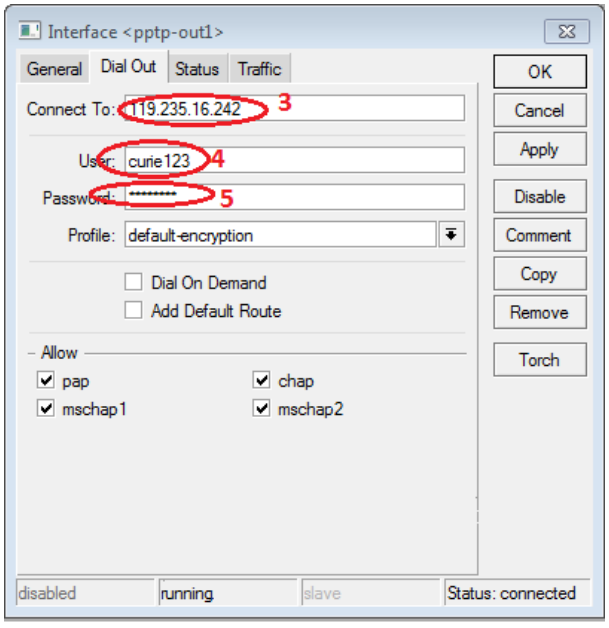
> Klik + pada tab interface >pilih PPTP-Client



Gambar 4.10 Mengaktifkan pptp-client

2.Dial out.

Isi alamat server > isi user > isi password

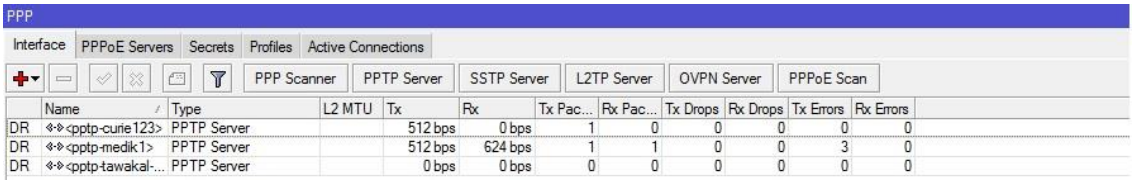


Masukkan pengaturan PPTP disini
Connect to:alamat ip VPN server
User:nama: pengguna VPN Server
password:Password untuk VPN server)

Gambar 4.11 Dial Out

3.7. Perancangan dan Konfigurasi Mesin Absen

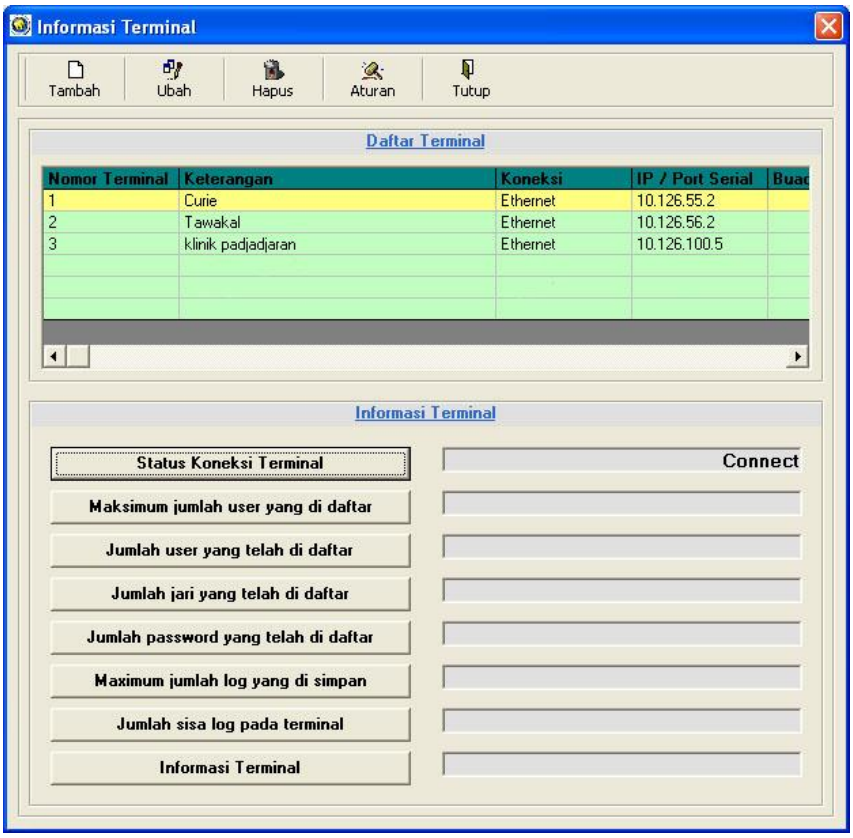
Setelah mengaktifkan pptp-client pada tiap-tiap cabang, tahap selanjutnya



memastikan tiap-tiap mesin absen tersebut sudah terhubung dengan server.

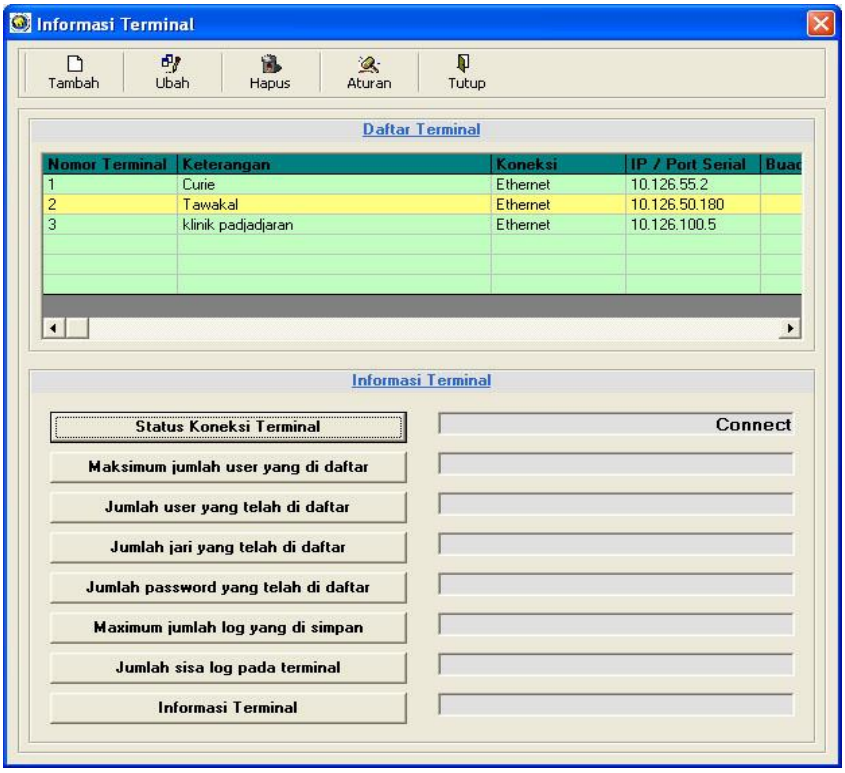
Gambar 4.12 running interface

1. Masuk ke Aplikasi Mesin absen, pastikan terminal mesin absen sudah ter connected

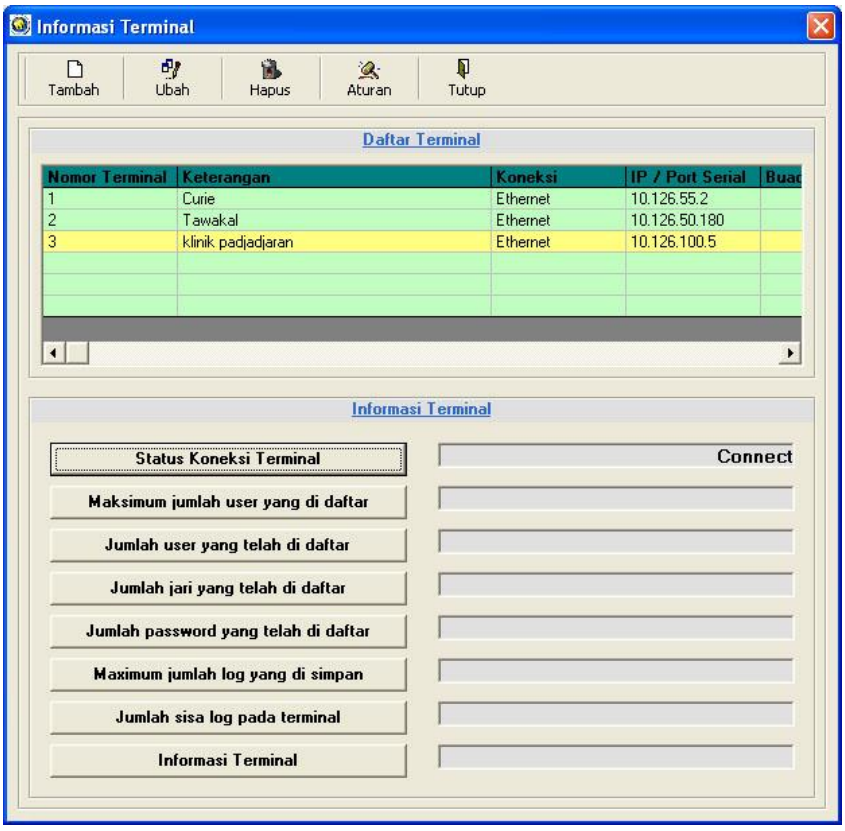


Gambar 4.13 informasi terminal Curie

2. Cek terminal absensi yang lain nya, pastikan agar terminal terhubung.

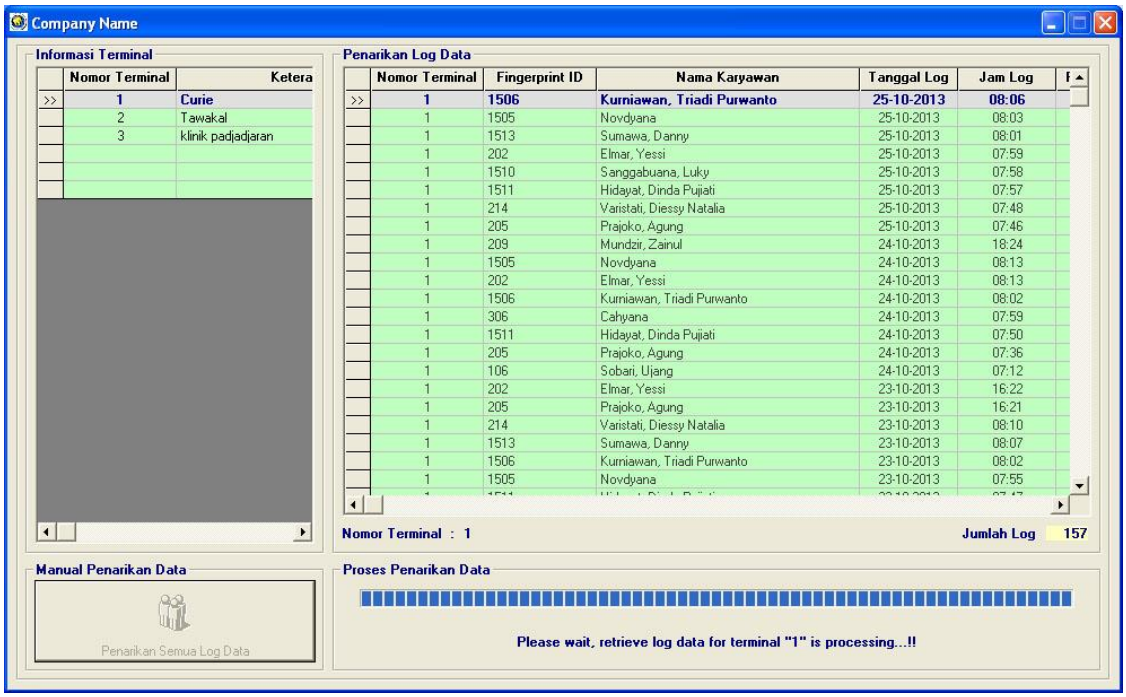


Gambar 4.14 informasi terminal tawakal



Gambar 4.15 informasi terminal Klinik Padjadjaran

3. Setelah semua absensi terminal sudah terhubung, tahap selanjutnya proses penarikan data absesnsi karyawan



Gambar 4.16 proses penarikan data absensi