BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem VPN yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat. Setelah implementasi selesai, maka selanjutnya akan dilakukan pengujian pada kinerja dari jaringan VPN yang telah dibangun.

4.1 Konfigurasi Client

Konfigurasi VPN *client* adalah untuk mempermudah pengaksesan suatu jaringan intranet (lokal area) di manapun *user* berada selama ada koneksi dengan internet melalui koneksi VPN *srver*.

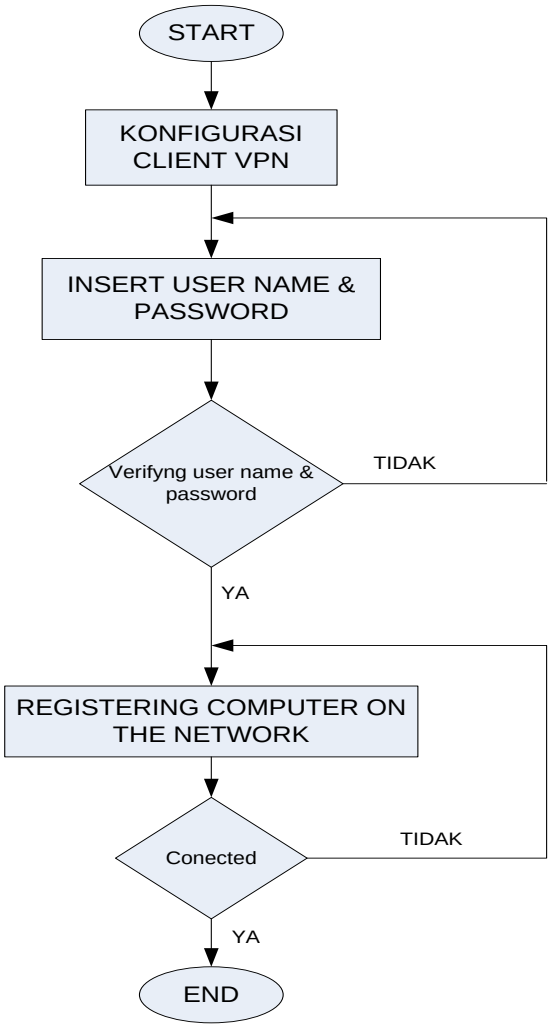
Dalam konfigurasi VPN *Client*, ada beberapa tahapan yang harus dilakukan diantaranya :

a. Tahap VPN *Client Configuration*.

b. Tahap *Dialing* VPN / *Connecting* VPN.

c. Tahap Ping Test & *Working*.

Untuk lebih memperjelas mengenai tahapan konfigurasi di sisi *client,* berikut akan disertakan gambar flowchart



Gambar 4.1 Flowchart Konfigurasi *Client*

a. Tahap Konfigurasi *Client*

Pengunaan VPN untuk *Client* personal adalah menghubungkan suatu *client* dengan *network* VPN *Server* melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal.

Dalam mengkoneksikan *client* dengan VPN server dibutuhkan beberapa tahapan settingan pada komputer *client.*

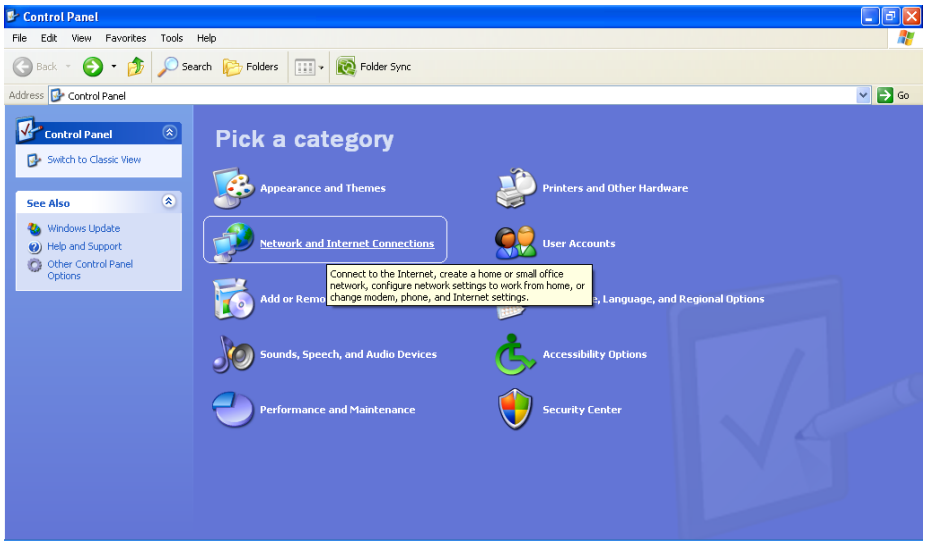
Ada tiga sekenario koneksi *client/user* pada komputer dengan beberapa operating system yang berbeda diantaranya :

1. Konfigurasi *client* menggunakan *Operating Syetem* Windows XP
2. Konfigurasi *client* menggunakan Mac OS X 10.5 (Leopard)
3. Konfigurasi *client* menggunakan Linux ubuntu

1. Konfigurasi *Client OS* Windows XP

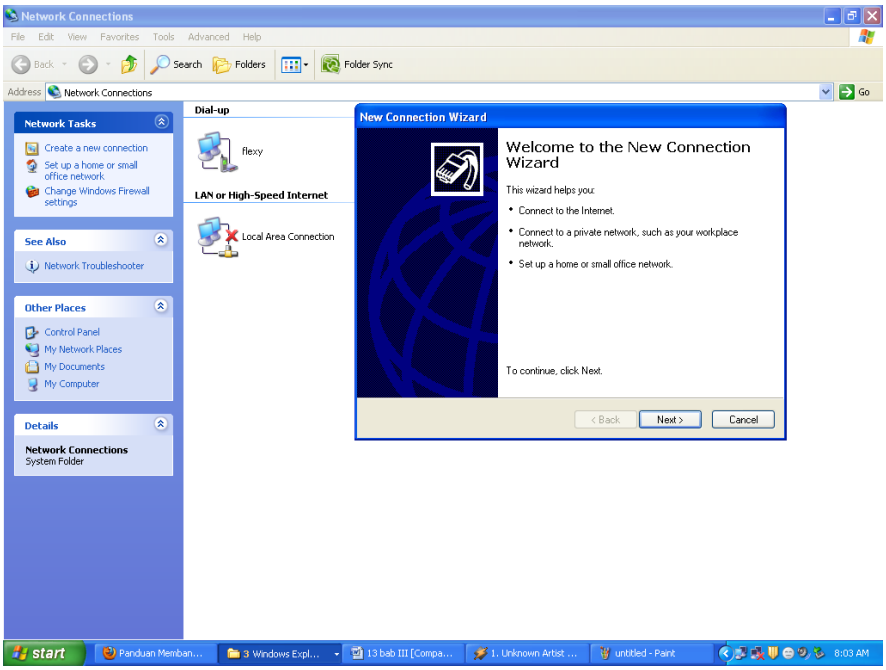
Berikut adalah settingan-setingan *client/user* untuk koneksi ke VPN menggunakan windows xp.

1. Masuk ke windows *control panel* kemudian klik *network and internet connections* seperti gambar dibawah.



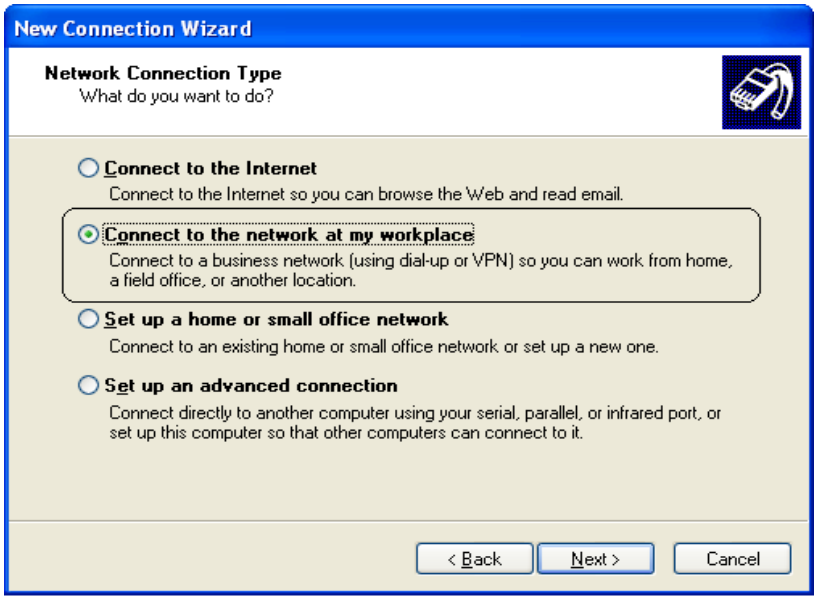
Gambar 4.2 Windows *control panel*

2. Klik *network conecctions* kemudian Pilih “ Buat koneksi baru dari sisi kiri jendela windows xp *new connection wizard* seperti gambar dibawah :



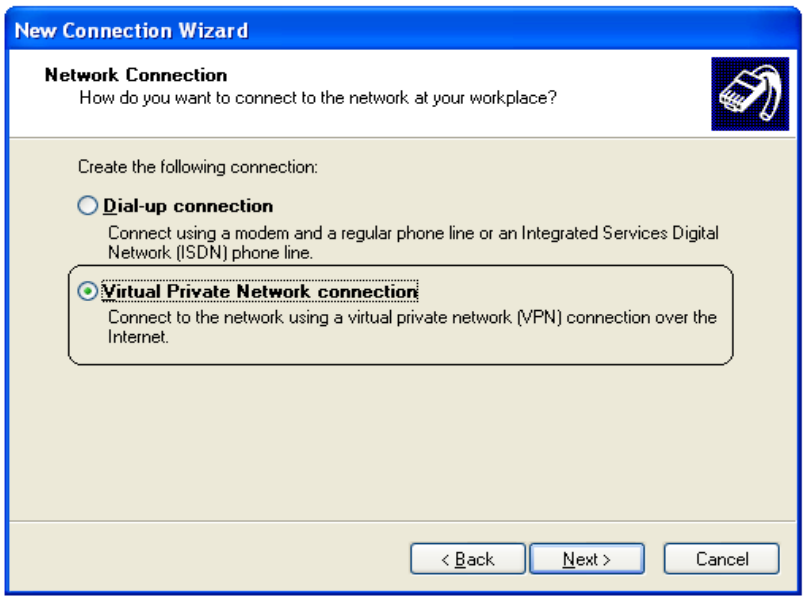
Gambar 4.3 Membuat koneksi baru VPN *client*

3. Tekan tombol *next* untuk memulai *wizard*, lalu pilih ‘*Connect to the at my workplace*’ dari daftar dan klik *next.*



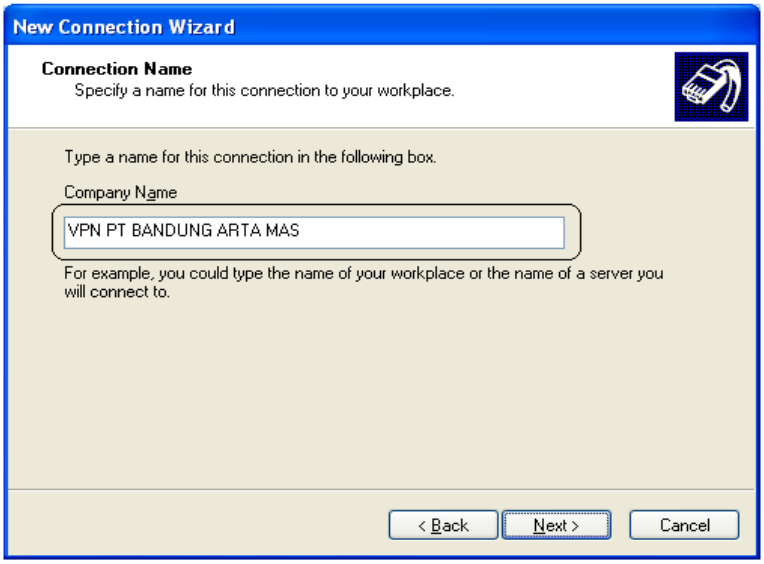
Gambar 4.4 Pemilihan tipe koneksi

4. Pada halaman koneksi jaringan *wizard*, pilih pilihan ‘koneksi *virtual private network*’ dan klik *next.*



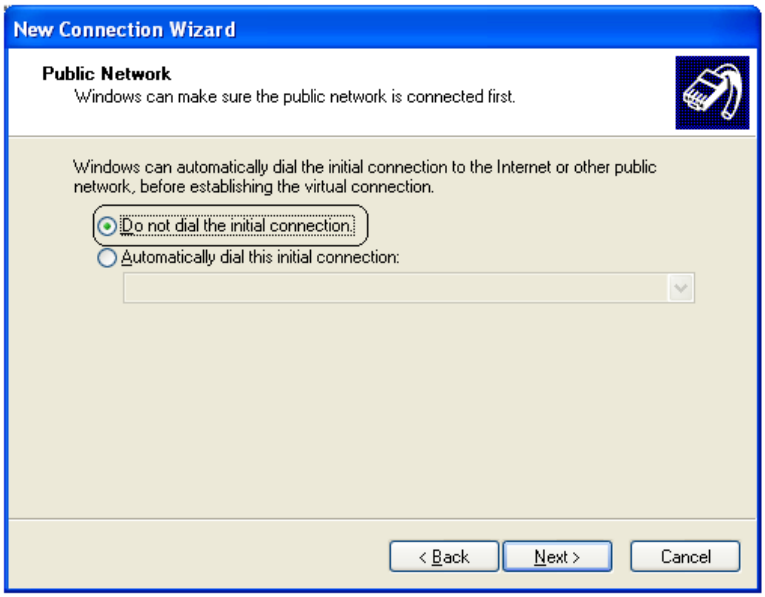
Gambar 4.5 Pemilihan koneksi jaringan

5. Masukan nama untuk sambungan VPN dalam penulisan ini saya masukan nama perusahaan (PT Bandung Arta Mas) dan klik *next*. Nama untuk sambungan yang dipilih bebas.



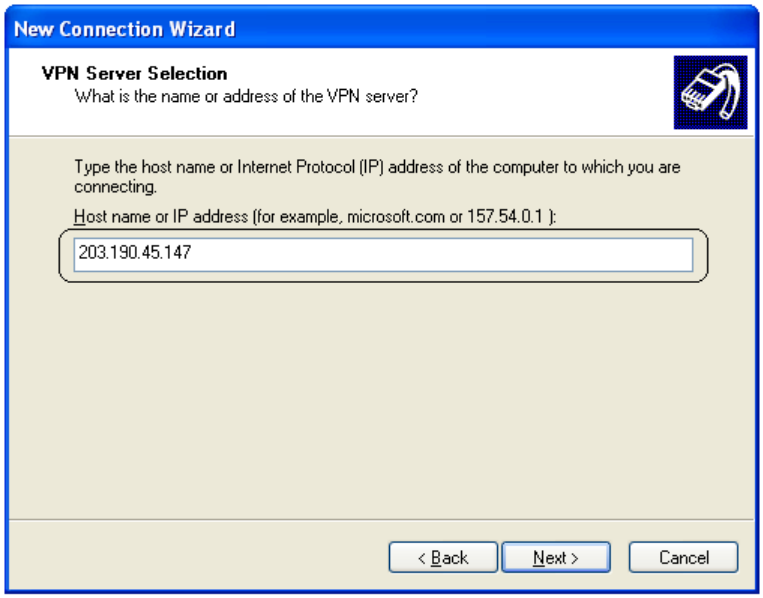
Gambar 4.6 Penamaan koneksi jaringan VPN

6. Kemudian pada ‘layar jaringan publik’ pilih *do not dial the initial connection* dan klik *next*. Pilihan *default automatically dial this initial connection,* dapat digunakan jika koneksi VPN akan dimulai pada saat komputer terhubung ke internet. Jika tidak, pilih opsi *do not dial the initial connection*. Pilihan ini mengharuskan terbentuk koneksi internet pertama, sebelum koneksi VPN baru akan dimulai.



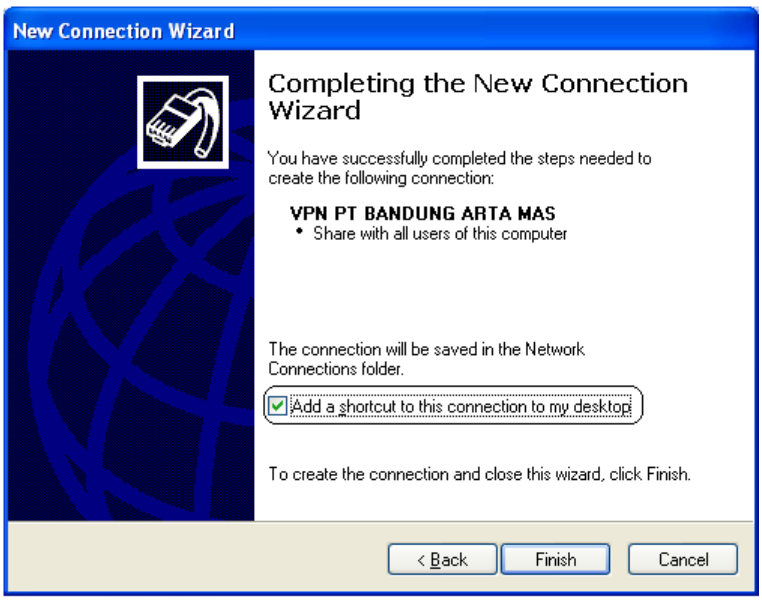
Gambar 4.7 Pemilihan jaringan *public*

7. Masukan *IP address* (*IP Public*) dari *server remote accsess* VPN untuk terhubung, dan klik *next*.



Gambar 4.8 Memasukan *IP address server* VPN

8. Klik *finish* untuk menyelesaikan *wizard*. Informasi koneksi VPN baru telah disimpan.



Gambar 4.9 *Finishing* dan Pembuatan *shortcut*

2. Konfigurasi *Client* Mac OS X 10.5 (Leopard)

Berikut adalah settingan-setingan *client/user* untuk koneksi ke VPN menggunakan Mac OS 10.5 (Leopard)

1. Buka Sistem Preferences di menu Apple Preferensi > Sistem.



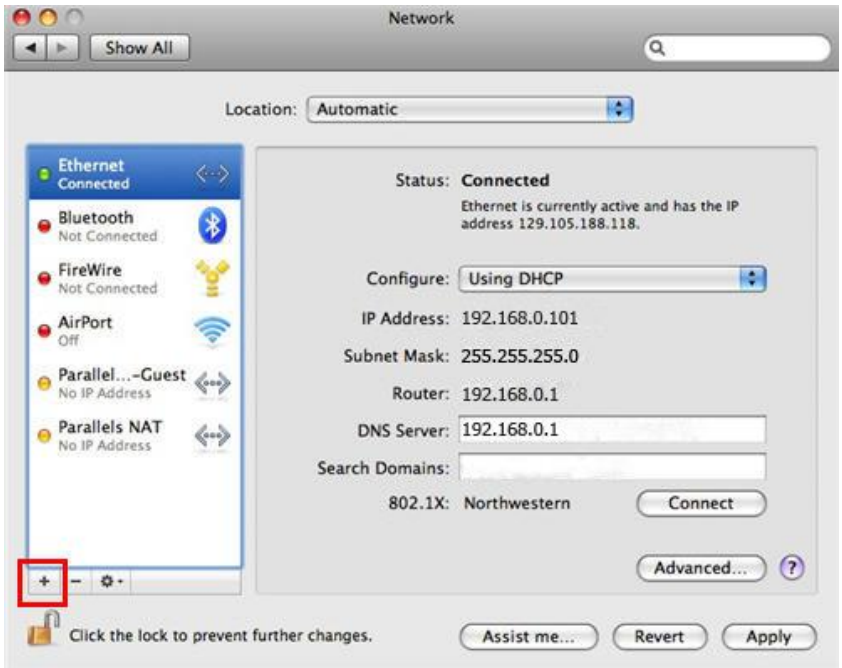
Gambar 4.10 ***Menu bar dekstop mac***

2. Pilih ikon *Network* pada jendela *Syistem Preferences*.



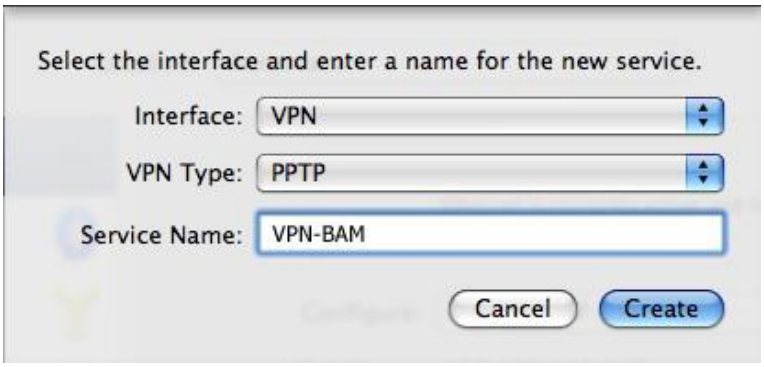
Gambar 4.11 *Menu System Preferences*

3. Pilih tombol + di kiri bawah layar untuk menambahkan koneksi baru.



Gambar 4.12 Pembuatan koneksi baru

4. Langkah selanjutnya pilih *interface*, tipe VPN, dan pembuatan *service name* untuk koneksi baru



Gambar 4.13 Pemilihan interface dan pengisian *service name*

5. Klik panah ke konfigurasi klik kanan dan pilih tambah konfigurasi dari menu *drop down*.



Gambar 4.14 Pembuatan *konfigurasi* baru

6. Masukkan VPN-BAM di dialog nama dan klik *create.*



Gambar 4.15 ***Create new configuration***

7. Selanjutnya isi alamat server dan *acount name* untuk *ecryption* isi automatis **.**



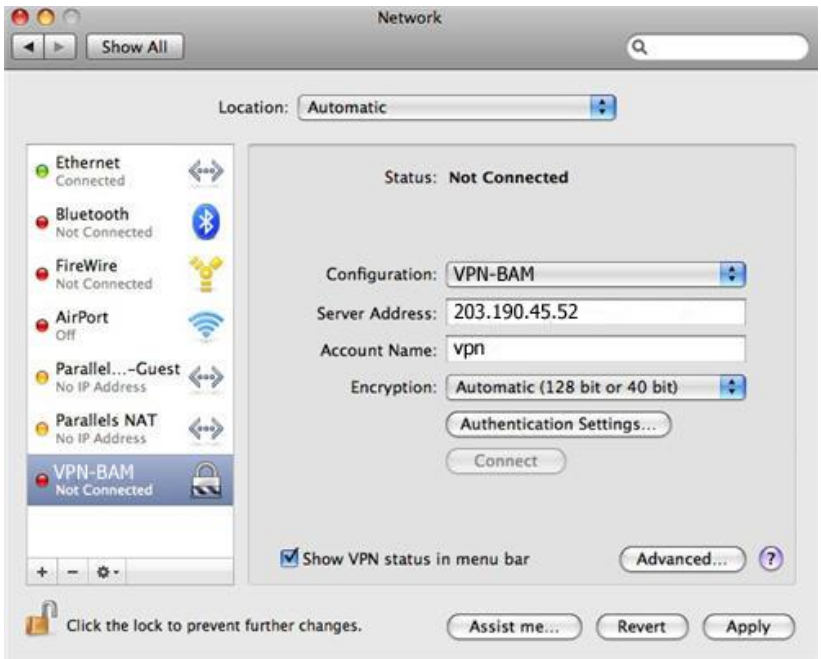
Gambar 4.16 Pembuatan ***account*** **VPN**

8. Klik tombol Advanced.
9. Pilih Pilihan Kirim. Pastikan semua lalu lintas melalui koneksi VPN diperiksa.



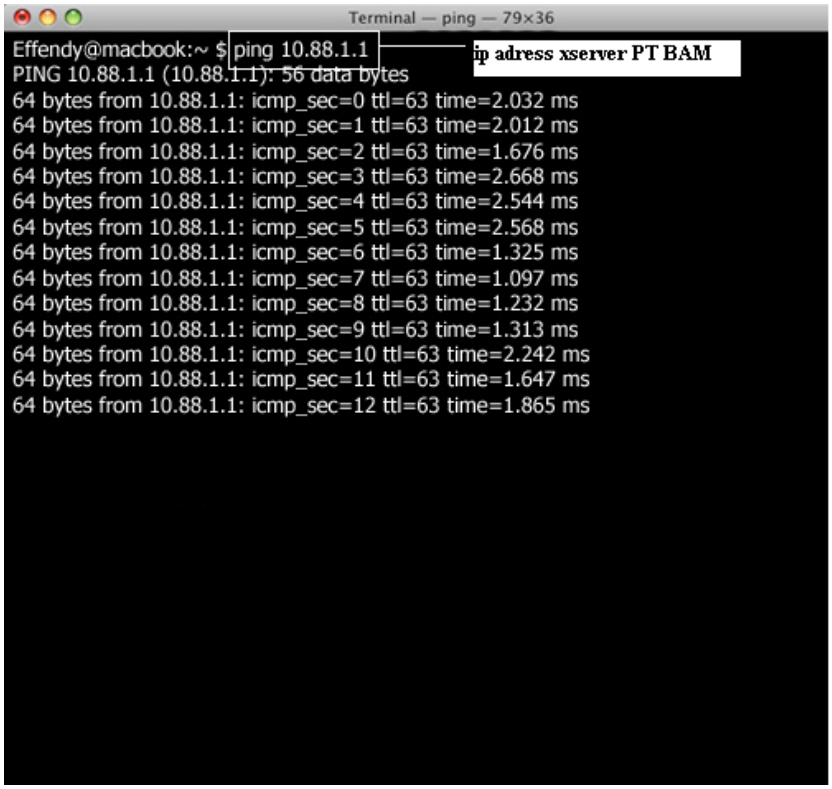
Gambar 4.17 ***Session option***

10. Klik tombol OK.
11. Klik tombol Apply.



Gambar 4.18 ***Finishing*** **dan** ***conection***

Hasil ujicoba ping ip adress xserver PT Bandung Arta Mas di terminal macinthos

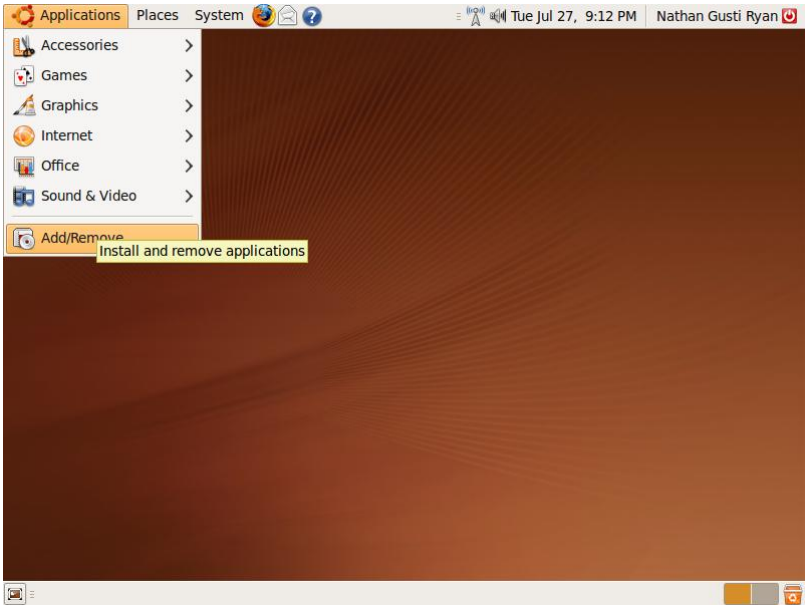


Gambar 4.19 Terminal *Ping IP adress*

3. Konfigurasi *Client* Linux Ubuntu 9

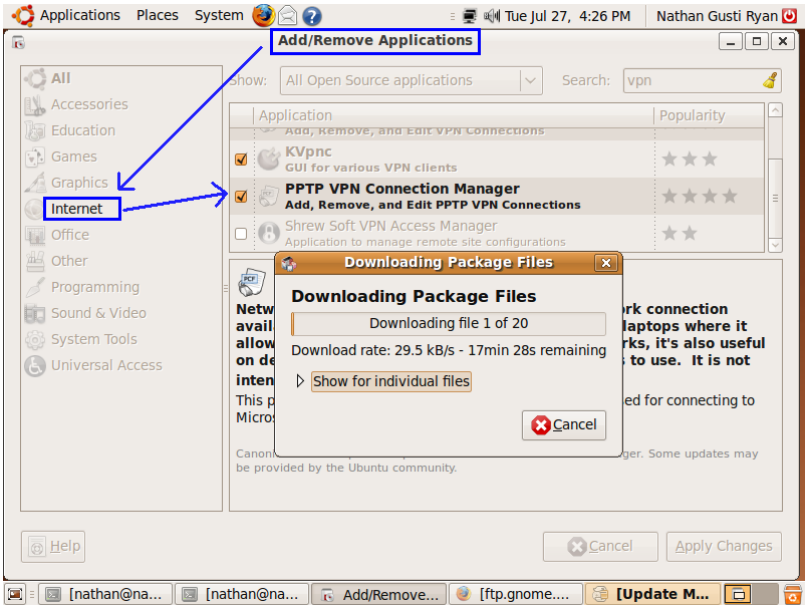
Berikut adalah settingan-setingan *client/user* untuk koneksi ke VPN menggunakan Linux ubuntu 9

1. Mulai dengan melakukan konfigurasi *network*, sebelum melakukan konfigurasi jika belum ada ***Plugin PPTP VPN Client***, harus *install* lebih dulu dari menu ***APPLICATION*** lalu kita pilih ***ADD/REMOVE***.



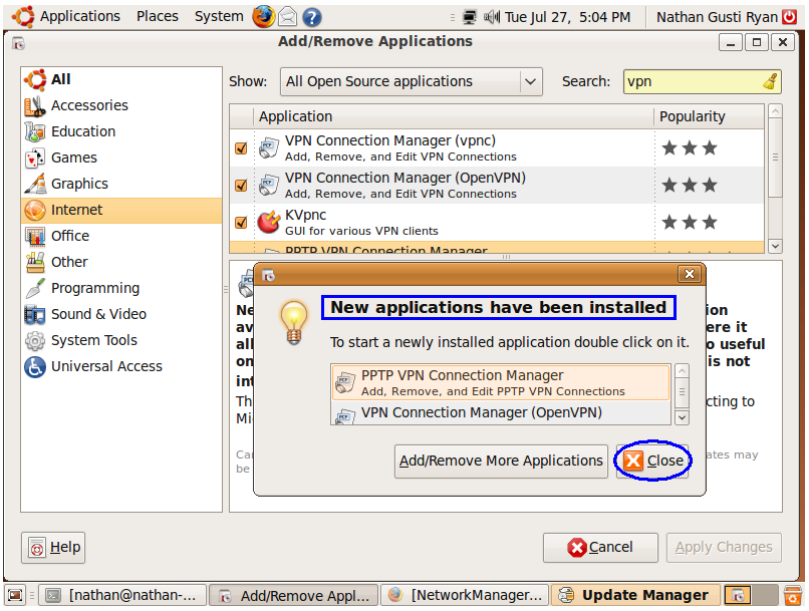
Gambar 4.20 ***Menu bar dekstop linux ubuntu***

2. Selanjutnya setelah muncul gambar seperti dibawah, kita pilih ***Option Internet*** dan lalu pilih tambah aplikasi ***VPN Connection Manager*** terus klik ***Apply Changes***. Selanjutnya **Ubuntu** akan melakukan download paket-paket yang dibutuhkan.



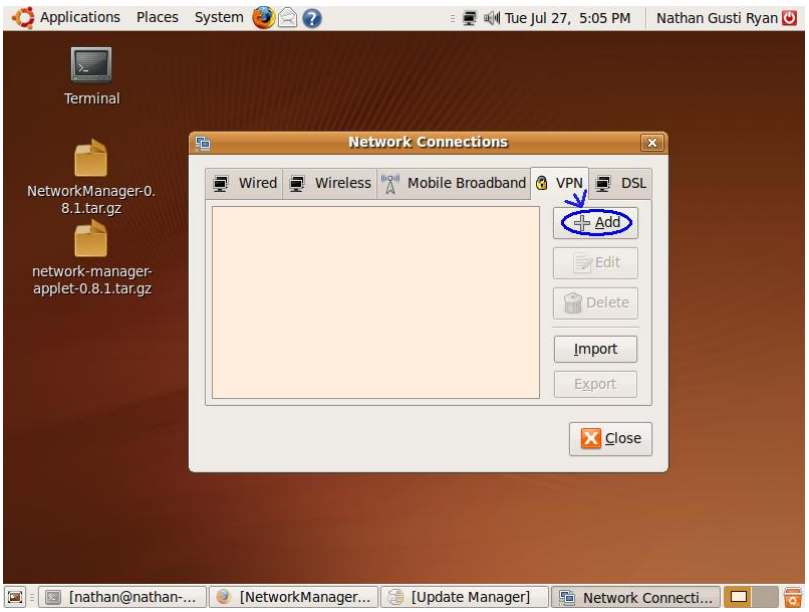
Gambar 4.21 ***Form add/remove aplications***

3. Setelah sukses dan selesai installasi paket ***VPN Connection Manager*** akan muncul tampilan seperti dibawah ini lalu kita klik ***Close***.



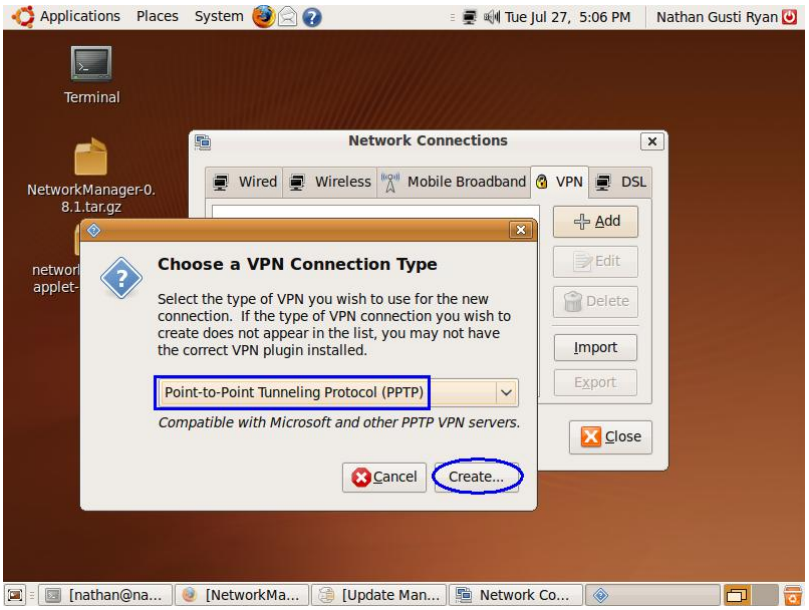
Gambar 4.22 ***New application***

4. Selanjutnya kita klik menu ***System*** lalu pilih ***Preferences*** kemudian pilih ***Network Connections***. Lalu kita bisa ***Add VPN Connection***.



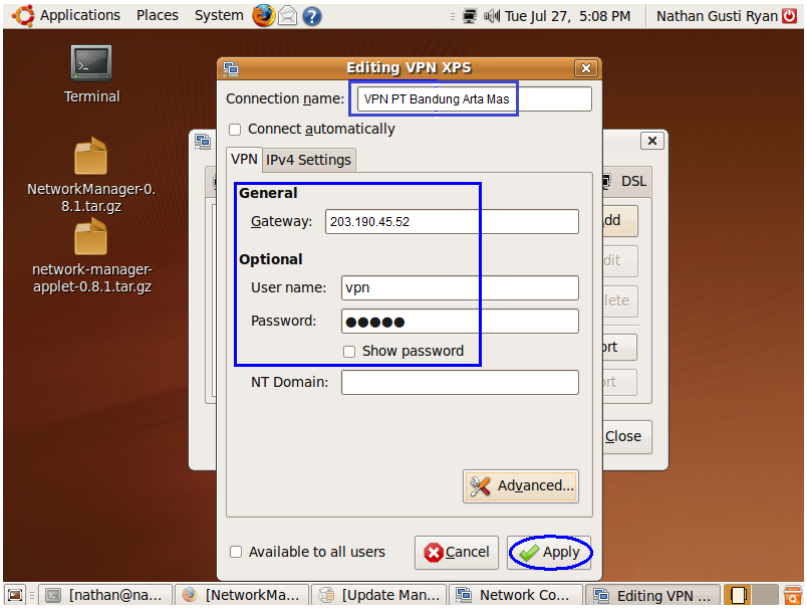
Gambar 4.23 ***Form Network Connection***

5. Selanjutnya muncul pilihan jenis VPN yang akan di buat, pilih ***PPTP VPN Client***, lalu klik ***Create.***



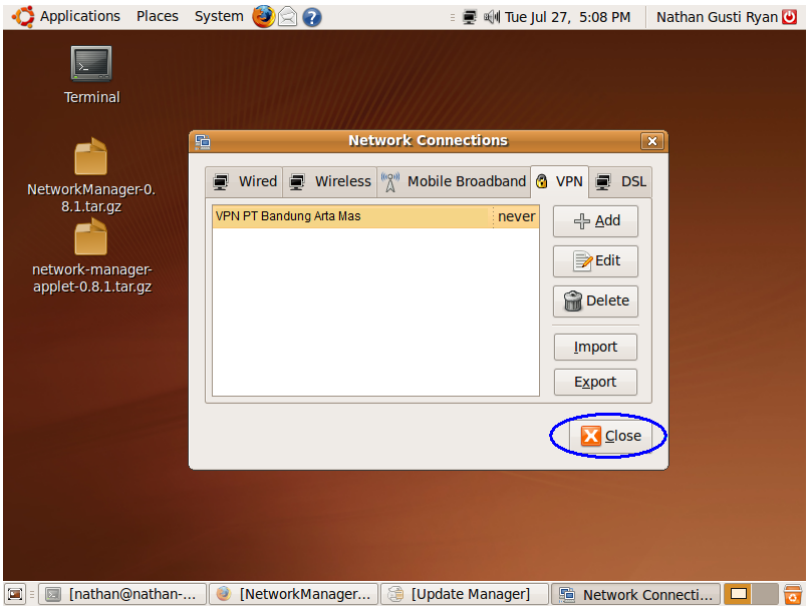
Gambar 4.24 Pemilihan tipe koneksi VPN

6. Selanjutnya setting ***IP Public VPN Server*** pada input **Gateway**, masukkan ***Username*** dan ***Password***. Jika PC Client ini selalu kita gunakan koneksi VPN maka *Option* ***Connect Automatically*** dapat kita aktifkan. Artinya jika PC ini mendapat akses internet maka akses VPN juga akan secara otomatis diaktifkan. Untuk nama koneksi VPN dapat kita berikan secara bebas dan setelah selesai kita klik ***APPLY***.



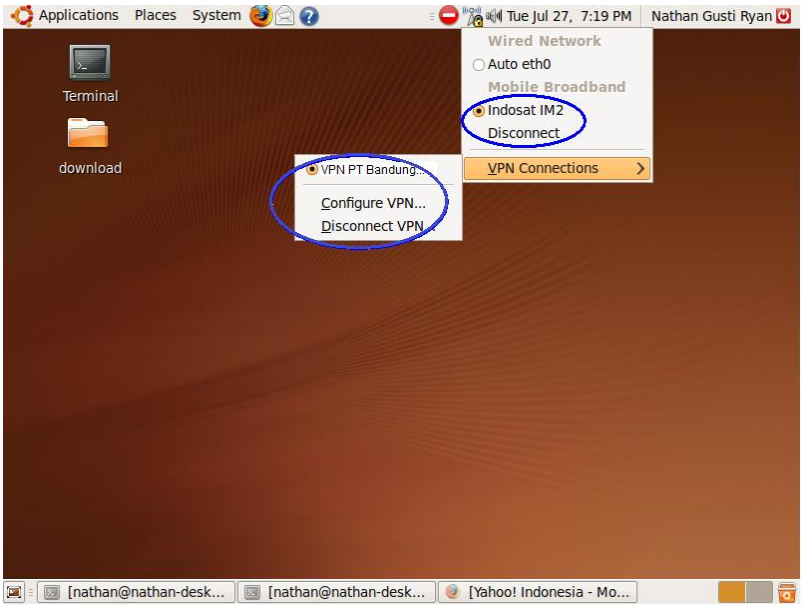
Gambar 4.25 Setting *Ip public*

7. Selanjutnya muncul koneksi VPN yang telah kita buat dan kita bisa klik ***Close***.



Gambar 4.26 *Network Connection*

8. Selanjutnya untuk melihat status *Network*, seperti gambar dibawah ini, menunjukan **VPN** telah terkoneksi.



Gambar 4.27 Status koneksi VPN

b. Tahap *Dialing* VPN / koneksi VPN

Langkah selanjutnya adalah koneksi ke akses *remote* atau server VPN yang sudah dibangun di PT Bandung arta Mas. Untuk menggunakan sambungan sederhana maka langkah-langkahnya adalah sebagai berikut :

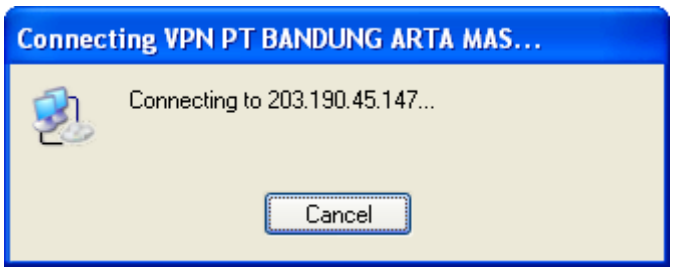
1. *Double* klik pada kotak dialog *network connection* atau pilih *connect* dari menu, akan muncul seperti gambar di bawah



Gambar 4.28 ***Dialog Network cnnection***

2. Masukan *user name* dan *password* yang sudah terdaftar di VPN server, kemudian klik *connect*.

Dari proses *connection* di atas maka proses selanjutnya adalah proses *connection* ke server VPN



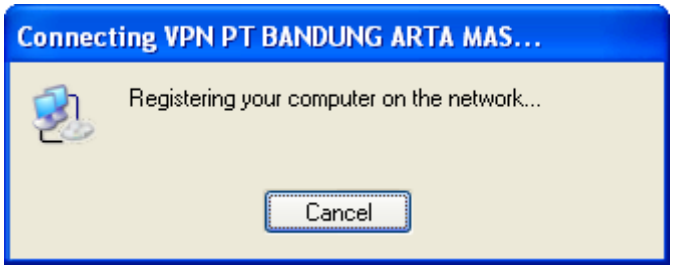
Gambar 4.29 ***Dialog cnnection to VPN***

Proses *verifying username* dan *password*



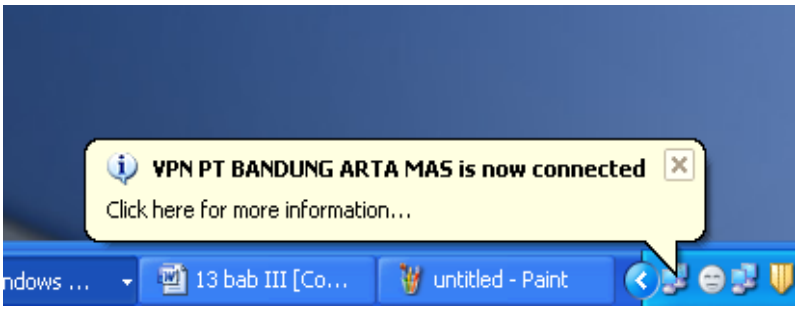
Gambar 4.30 ***Dialog verifying username and password***

Proses *Registering* komputer pada jaringan



Gambar 4.31 Dialog ***registering computer***

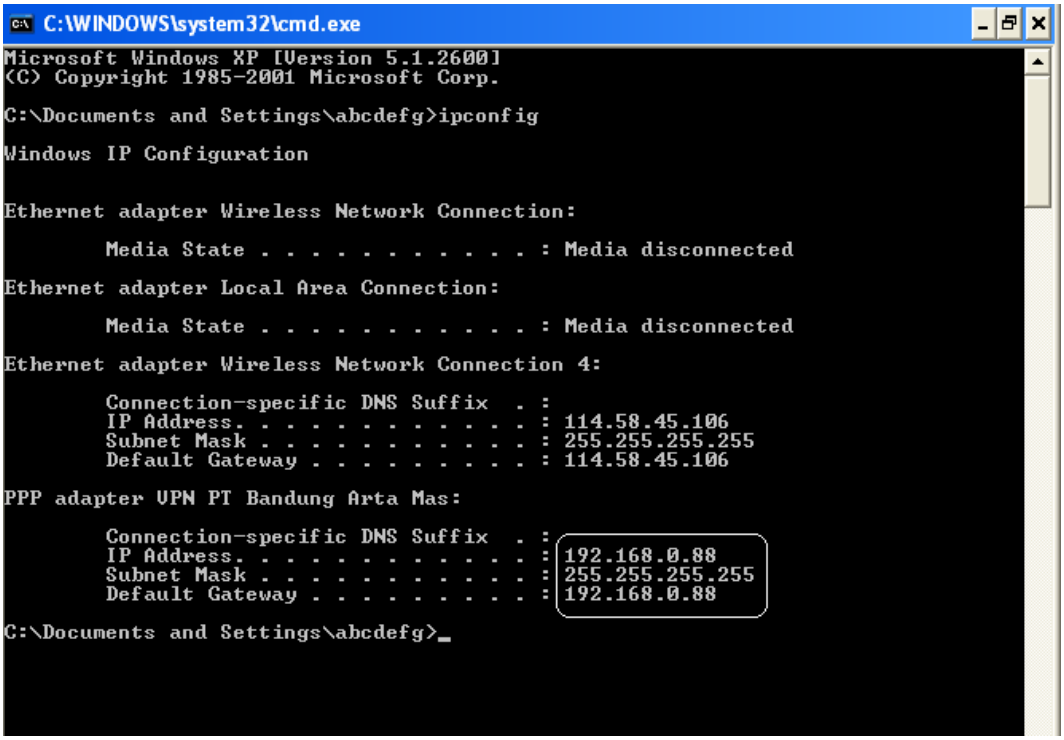
Setelah proses *Authentication* sukses, maka VPN PT Bandung Arta Mas sudah terkoneksi dan muncul ikon seperti dibawah.



Gambar 4.32 Informasi koneksi VPN

a. Tahap Ping tes dan Kerja VPN

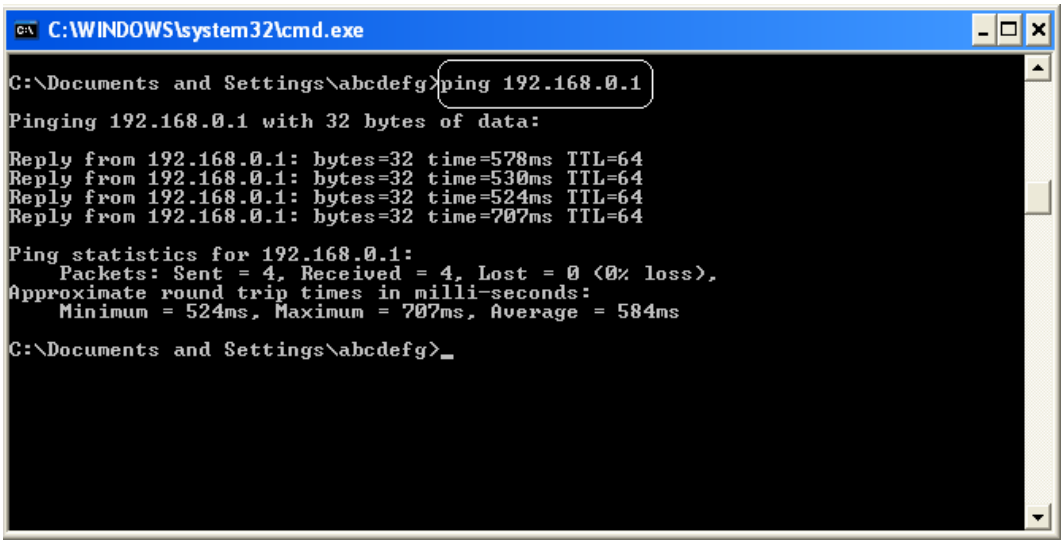
Setelah proses *dial* atau *connect* ke VPN untuk membuktikan koneksi VPN berjalan, maka selanjutnya akan dilakukan pengujian koneksi. Pertama kita chek *IP address* yang didapat dengan cara ketik ipconfig di *command promt*.



Gambar 4.33 CMD ipconfig

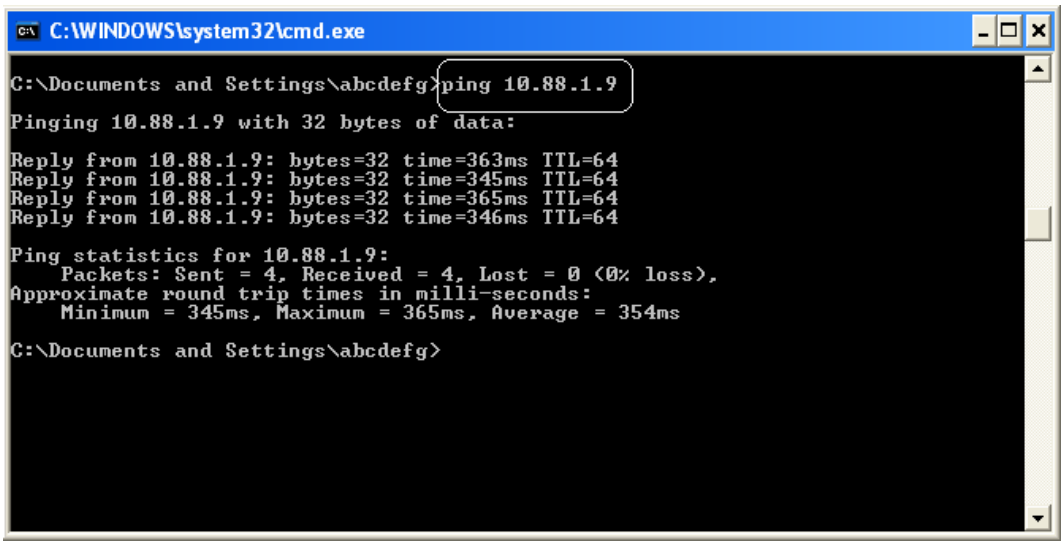
Setelah proses ipconfig, dapat diketahui bahwa *ip address* yang didapat adalah 192.168.0.88 untuk koniksi saat ini, ip address yang didapat bisa berubah – ubah karena VPN server mempunyai DHCP server. *Range IP address* untuk VPN adalah 192.168.0.20-192.168.0.100

Tahap selanjutnya pengujian koneksi dengan tes ping ke *IP adress server* VPN yang mempunyai IP address 192.168.0.1 seperti gambar di bawah.



Gambar 4.34 Ping VPN Server

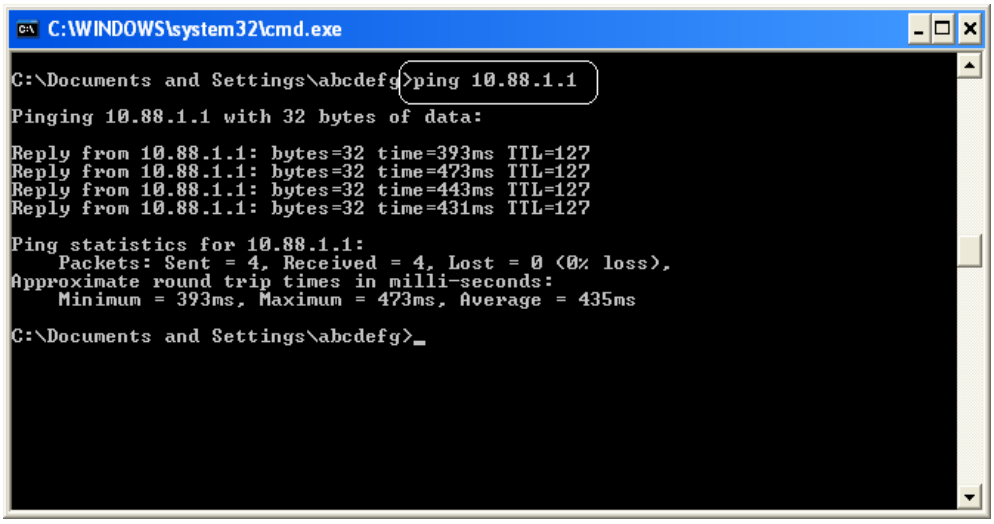
Setelah dilakukan proses ping ke *IP address* VPN *server*, langkah selanjutnya adalah pengujian ke *IP address* lokal VPN yang masuk ke jaringan LAN PT Bandung Arta Mas.



Gambar 4.35 Ping *IP address* lokal VPN

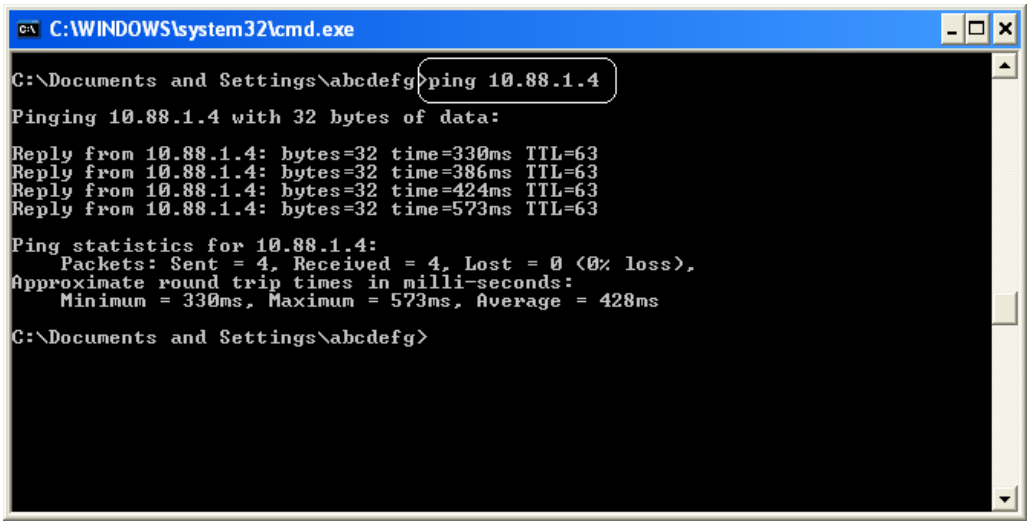
Proses tes ping diatas menandakan *user* VPN sudah terkoneksi ke jaringan lokal PT Bandung Arta Mas melalui VPN server. Untuk memastikan lebih lanjut

koneksi VPN ke jaringan lokal maka akan dilakukan tes ping ke *IP address server-server* yang ada di PT Bandung Arta Mas. Pertama tes ping ke *IP address file server* 10.88.1.1



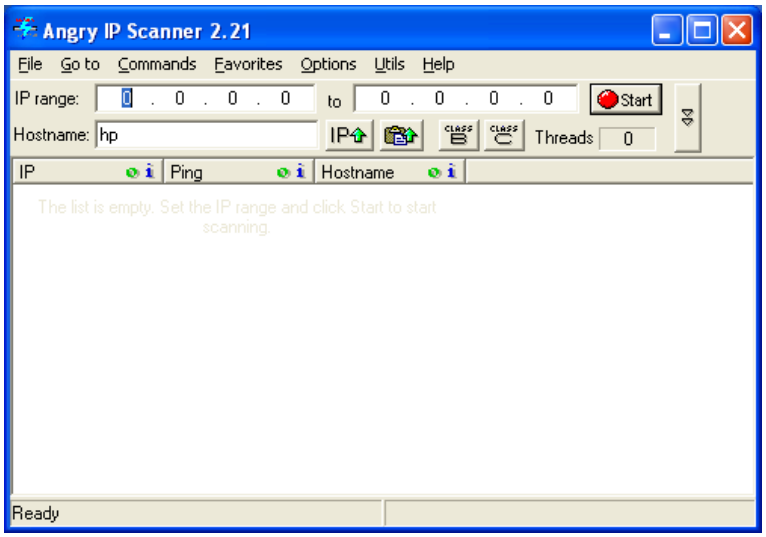
Gambar 4.36 Ping *IP address file server*

Ping *IP address file server* PT Bandung Arta Mas (xserver) terkoneksi. Tahap ping tes selanjutnya *IP address* untuk *mail server* PT Bandung Arta Mas.



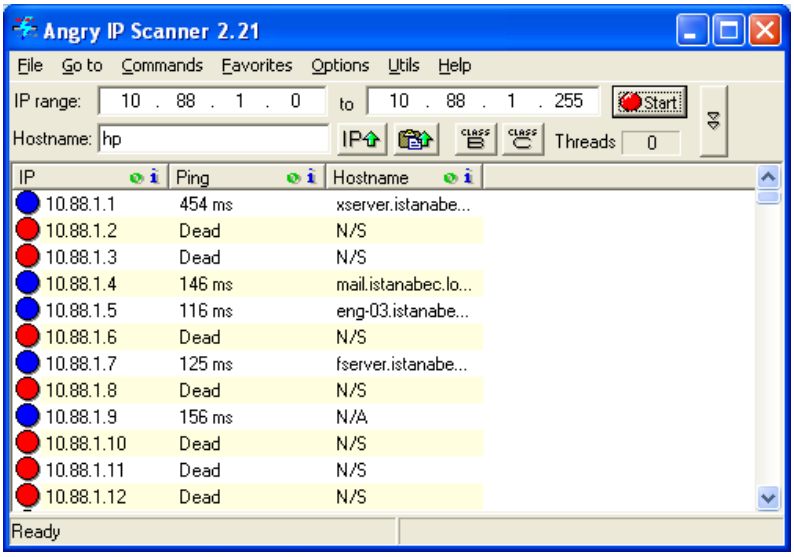
Gambar 4.37 Ping IP address mail server

Untuk memastikan bahwa user VPN benar-benar berada di jaringan lokal PT Bandung Arta Mas, maka akan dilakukan pengecekan IP address yang sedang aktif di PT Bandung Arta Mas dengan menggunakan bantuan aplikasi Angry IP Scanner yang dapat di akses di http://www.angryip.org. Berfungsi untuk ping *IP addres* dan mengetahui user yang aktif di jaringan lokal PT Bandung Arta Mas.



Gambar 4.38 Aplikasi Angry IP Scanner

Masukan *range IP address* PT Bandung Arta Mas mulai dari 10.88.1.0-10.88.1.255 kemudian klik *start* untuk memulai

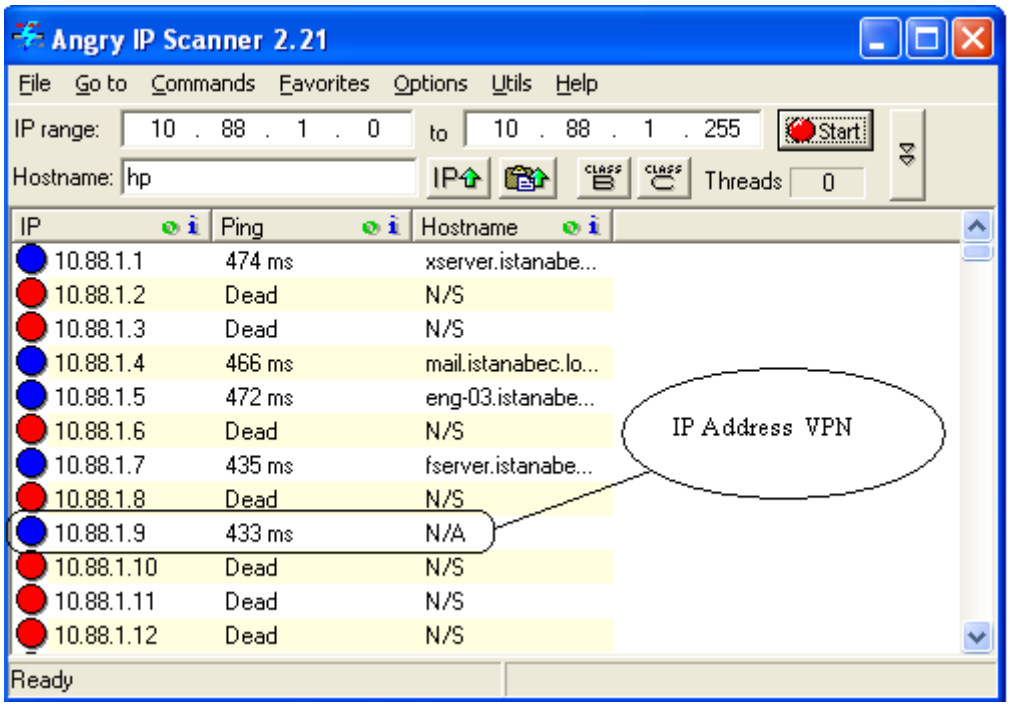


Gambar 4.39 Aplikasi *angry IP Scanner Check User* PT Bandung Arta Mas



Gambar 4.40 *Scanning* berhasil dan *finished*

Scanning berhasil, *IP address* yang di *scane* sebanyak 256 dan yang aktif sebanyak 11 unit termasuk *user* VPN yang terkoneksi ke jaringan lokal PT Bandung Arta Mas.



Gambar 4.41 *IP Address* VPN

Akses *server* VPN atau *remote server* VPN bisa dilakukan beberapa cara diantaranya :

4.2 Akses Mikrotik *Router*OS

Ada 4 cara pengaksesan Mikrotik *Router*OS, antara lain :

a. *Via Console/Command Mikrotik*

Jenis *router board* maupun PC bisa di akses langsung *via console/shell* maupun remote akses menggunakan PUTTY (www.putty.nl)

b. Via *Web Browser*

Mikrotik bisa diakses via *web/port* 80 pada *browser*. Contoh : ketik di *browser* dengan IP Address dari Mikrotik *Router*OS : 10.88.1.9

c. Via WinBox

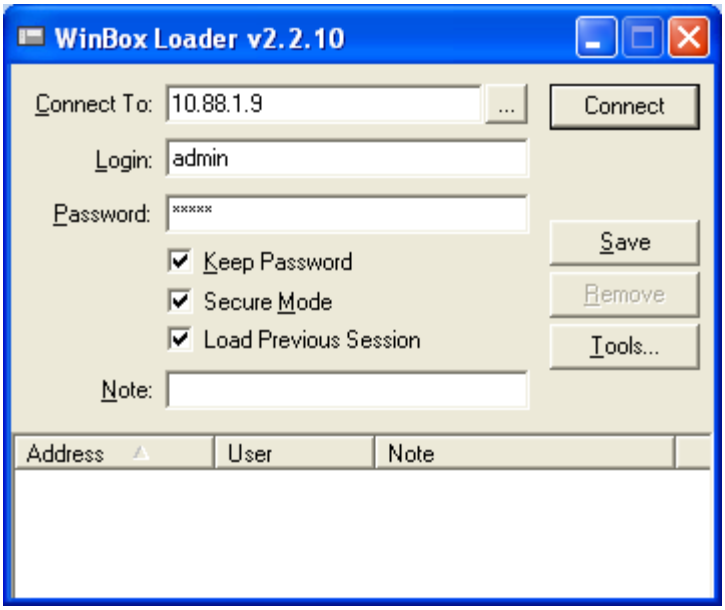
Mikrotik bisa diakses/*remote* menggunakan tool winbox ,Winbox adalah sebuah *utility* untuk melakukan *remote* ke *server* mikrotik dalam mode GUI. Winbox bisa mendeteksi mikrotik yang sudah di install jika masih dalam satu *network*, yaitu dengan mendeteksi MAC address dari *ethernet* yang terpasang di Mikrotik *Router*OS.

d. Via Telnet

Mikrotik dapat di*remote* menggunakan *telnet* melalui program aplikasi ”*command prompt*” (cmd) yang ada pada *windows*. Namun, penggunaan *telnet* tidak dianjurkan dalam jaringan karena masalah keamanannya. Contoh : c:\>telnet 10.88.1.9

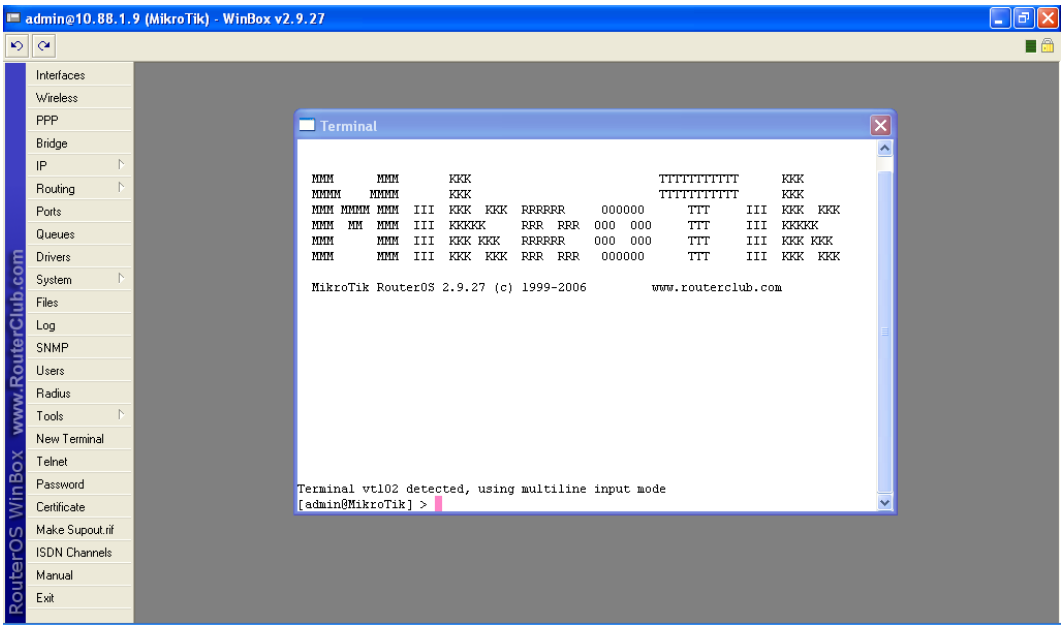
Dalam hal ini pengaksesan Mikrotik *Router*OS akan menggunakan WinBox karena praktis dan mudah digunakan, adapaun cara pengaksesan Mikrotik *Router*OS melalui Winbox adalah sebagai berikut :

a) Buka aplikasi WinBox



Gambar 4.42 Menu utama winbox

Masukan *IP address server*, masukan *username* dan *password* kemudian klik *connect*



Gambar 4.43 Tampilan awal mikrotik *router*OS pada winbox

4.3 Sekenario Pengujian Alpha

Pada pengujian alpah akan dilakukan sekenario pengujian yang terdiri atas dua pengujian diantaranya.

1. Pengujian login sebagai Admin
2. Pengujian login sebagai user vpn

1. Login Admin

Tabel 4.1 Pengujian Verifikasi Data Login Admin

Kasus dan Hasil Uji (Data Normal)	
Data Masukan	*User ID*: admin dan *Password*: admin
Yang Diharapkan	User ID dan *password* yang dimasukkan benar sehingga dapat masuk kedalam menu utama.
Pengamatan	*User ID* dan *password* yang dimasukkan diterima dan masuk ke menu utama
Kesimpulan	Diterima
Kasus dan Hasil Uji (Data Salah)	
Data Masukan	*Username*: a atau kosong *Password*: b atau kosong
Yang Diharapkan	Setelah klik tombol *login* maka muncul pesan *accsess was denide login invalid*
Pengamatan	Muncul pesan bahwa *Login Invalid*
Kesimpulan	Diterima

2. Login *User* VPN

Tabel 4.2 Pengujian Verifikasi Data Login *Client*

Kasus dan Hasil Uji (Data Normal)	
Data Masukan	*User ID*: vpn dan *Password*: vpn
Yang Diharapkan	User ID dan *password* yang dimasukkan benar sehingga dapat masuk kedalam menu utama.
Pengamatan	*User ID* dan *password* yang dimasukkan diterima dan masuk ke menu utama
Kesimpulan	Diterima
Kasus dan Hasil Uji (Data Salah)	
Data Masukan	*Username*: a atau kosong, *Password*: b atau kosong
Yang Diharapkan	Setelah klik tombol *login* maka muncul pesan *accsess was denide login invalid*
Pengamatan	Muncul pesan bahwa *Login Invalid*
Kesimpulan	Diterima

4.4 Pengujian pada Sistem VPN

Pada penelitian ini akan dilakukan beberapa skenario ujicoba dengan tujuan untuk mendapatkan beberapa perbandingan data hasil pengukuran, adapun skenario ujicoba yang akan dilakukan adalah sebagai berikut :

a. Pengujian *Bandwidth* Sistem VPN

Sistem akan diujicoba menggunakan aplikasi bantuan *Network Traffic*

Monitor, lalu akan diketahui kapasitas bandwidth yang di pakai oleh VPN server dan *user* yang mengakses VPN server.

b. Pengujian Sistem dengan *File Server*

Sistem akan diujicoba pada koneksi dengan *file server*, lalu akan mengambil data dari file sharing server. Kemudian *traffic bandwidth* akan diukur menggunakan *Network Traffic Monitor.*

c. Pengujian Sistem dengan *email Intranet* (lokal)

Sistem akan diujicoba pada email *intranet* mulai dari konfigurasi email sampai pengetesean pengiriman mail *intranet* (lokal) untuk membuktikan bahwa *user* seolah-olah berada di lokal area *network email intranet* akan menggunakan Microsoft Office Outlok dan Web mail lokal PT Bandung Arta Mas.

d. Pengujian Sistem dengan Aplikasi *client server*

Sistem akan diujicoba menggunakan aplikasi berbasis *client server* yang ada di PT Bandung Arta Mas yaitu aplikasi searching dan aplikasi checklist KWH meter listrik.

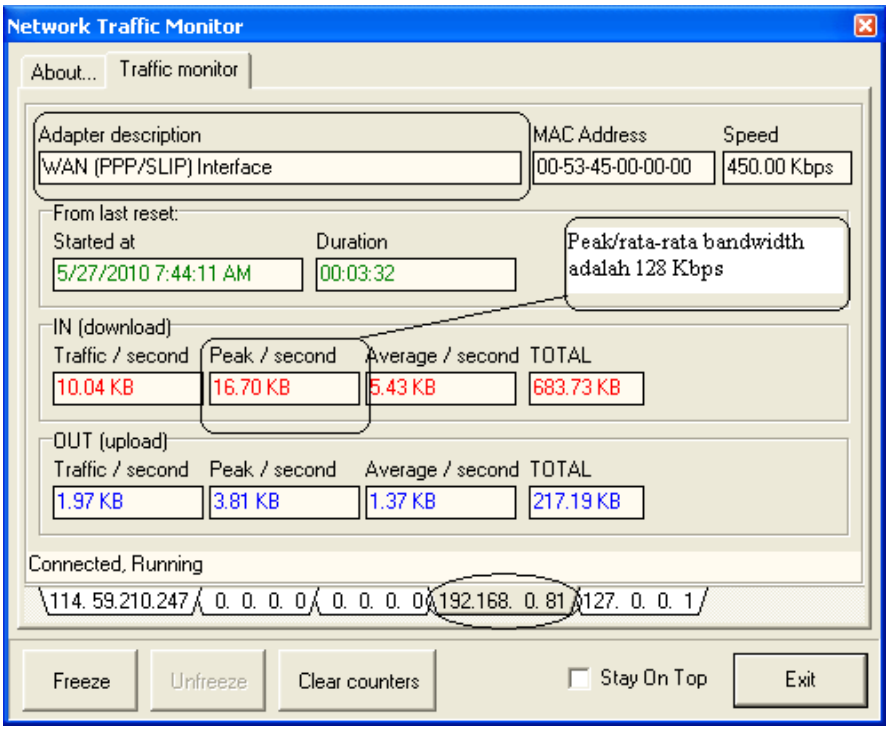
4.4.1 Pengujian *Bandwidth*

Pada pengujian *bandwidth* analisa yang dilakukan meliputi pengukuran parameter-parameter berikut :

1. Pengukuran *bandwidth server* VPN

Sistem akan diuji dan diamati dengan tujuan untuk mengetahui kecepatan

dan paket data yang di peroleh ketika koneksi dengan area lokal PT Bandung Arta Mas menggunaka tunnel PPTP.

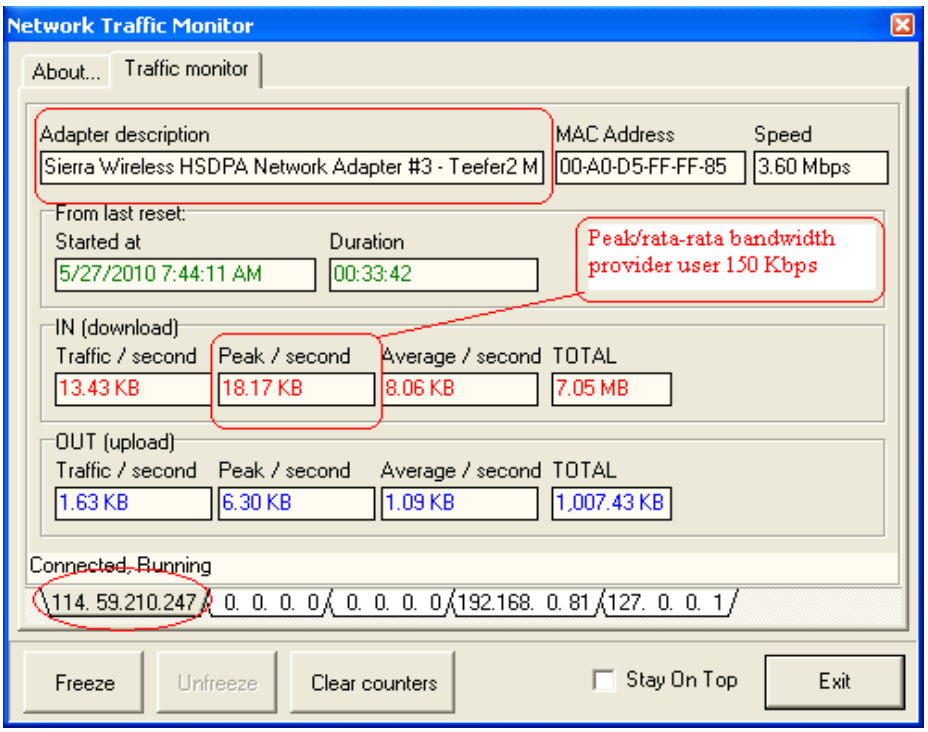


Gambar 4.44 Tampilan aplikasi *Network Traffic Monitor* pada tunnel PPTP

Dari data di atas dapat diketahui bahwa pemakaian rata-rata *bandwidth* saat pengujian adalah maksimal sebesar 128 Kbps karena selain faktor dari *bandwidht* yang digunakan untuk koneksi tunnel PPTP *server* maksimal sebesar 128 Kbps, faktor internet yang digunakan oleh user sangat berpengaruh juga pada koneksi PPTP *server*.

2. Pengukuran *Bandwidth* pada User

Pada pengujian *bandwidth* user akan diuji kecepatan dari provider yang digunakan. Karena kecepatan internet *user* sangat berpengaruh pada *bandwidth* yang diberikan oleh VPN *server*.

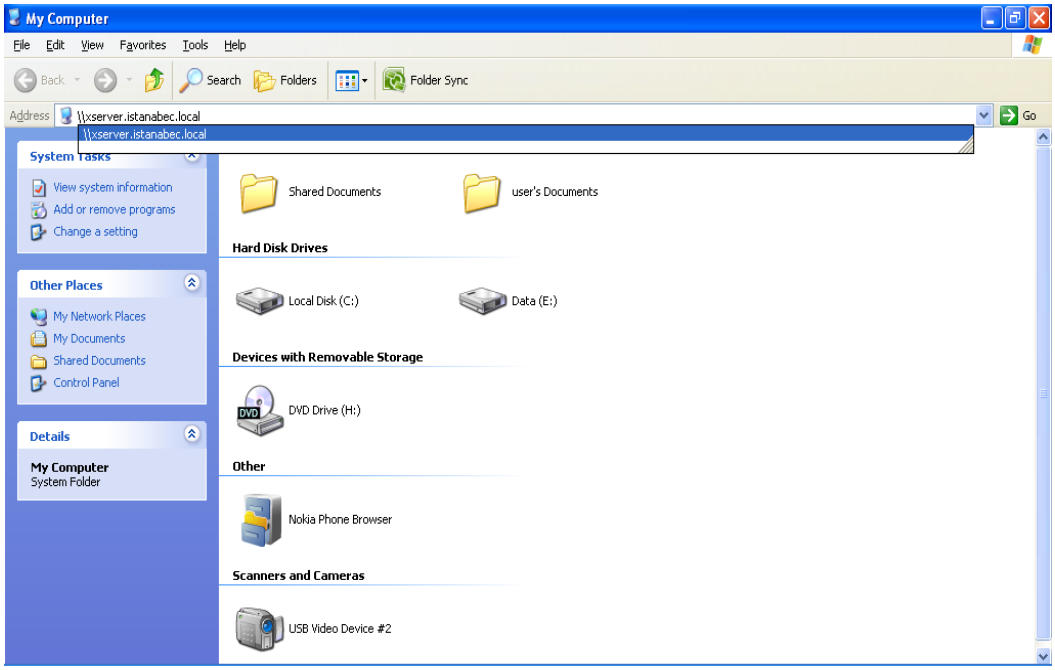


Gambar 4.45 Tampilan aplikasi *Network Traffic Monitor* pada ISP user

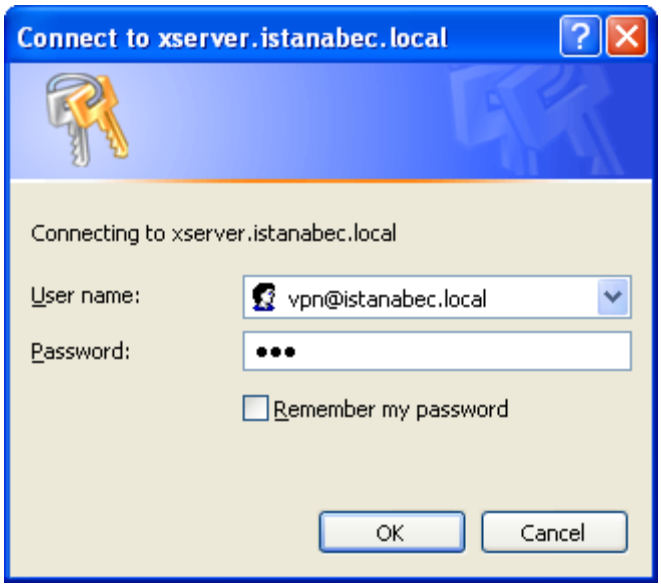
Dari data diatas dapat diketahui bahwa pemakaian rata-rata *bandwidth* dari user sebesar 150 Kbps. Meskipun *bandwidth user* lebih besar dari kapasitas tunnel PPTP *server* maka VPN *server* tetap memberikan *bandwidth* 128 Kbps. Karena maksimal yang diberikan oleh VPN *server* sebesar 128 Kbps begitupun sebaliknya apabilaa *bandwidth* yang di gunakan *user* kurang dari 128 Kbps VPN server akan mengikuti rata-rata dari *bandwidth* isp *user* yang digunakan

4.4.2 Pengujian Sistem pada *File Server*

Pada pengujian *file server* akan dilakukan pengambilan data dari *file sharing* yang berada di *file server* PT Bandung Arta Mas. Pertama masukan alamat *server* dari *file server* PT Bandung Arat Mas pada kolom *address* windows explorer

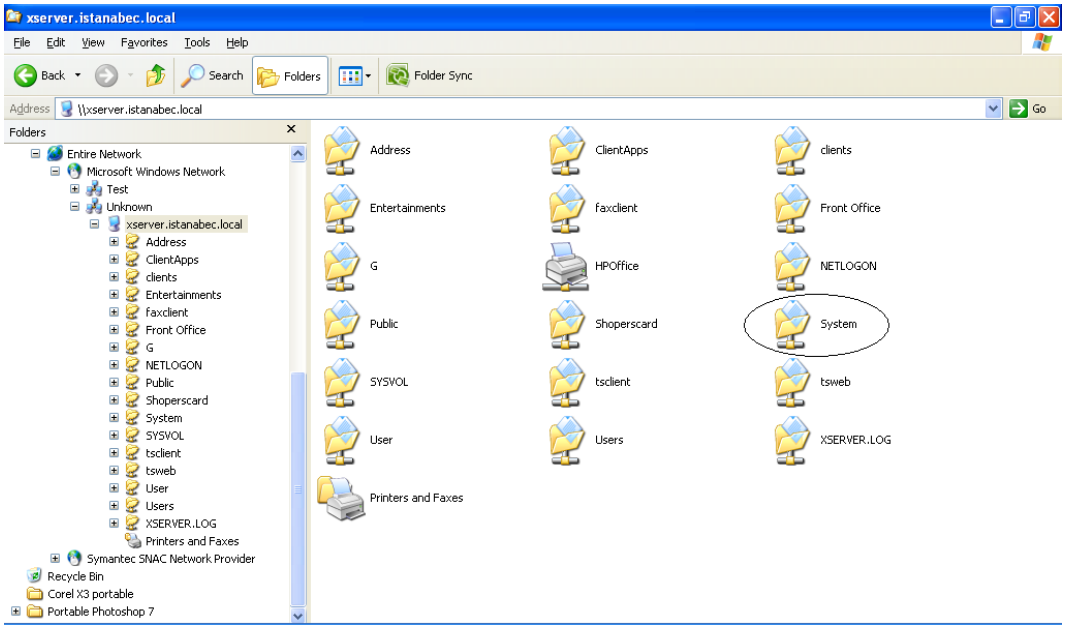


Gambar 4.46 Tampilan windows *explorer*

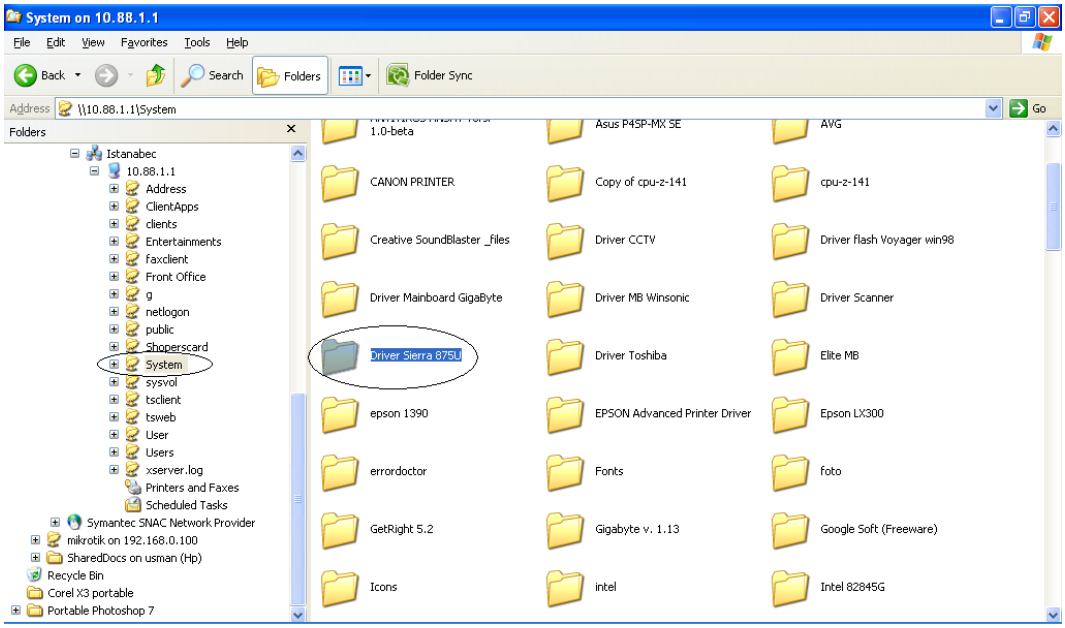


Gambar 4.47 Dialog *Connecttion* windows

Masukan *user name* dan *password* yang sudah terdaftar di *domain controller* PT Bandung Arta Mas. *Autehentikasi* user yang akses ke *file* xserver PT Bandung Arta Mas tingkat hak aksesnya berbeda-beda.

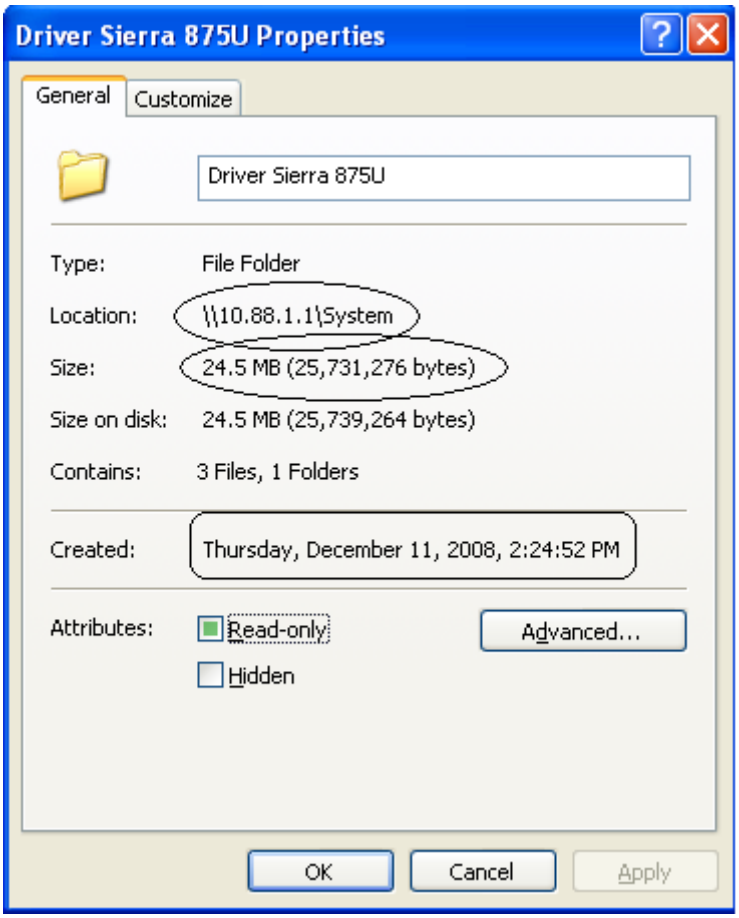


Gambar 4.48 *File sharing* PT Bandung Arta Mas

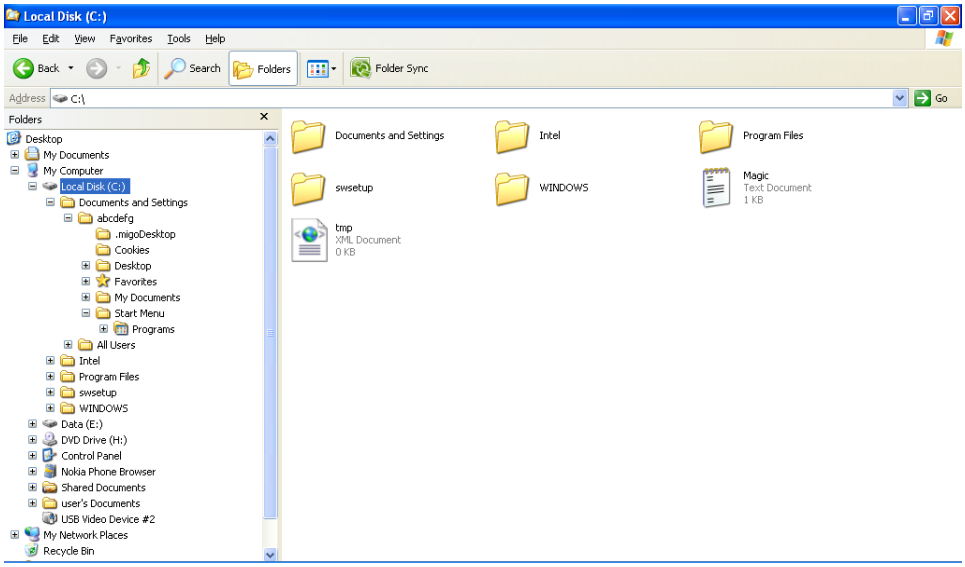


Gambar 4.49 *File sharing* di *folder system*

Pada gambar di atas akan diuji *copy file* dari *folder system* yang berada di *file server* ke *local disc drive C computer user* sebesar 24,5 Mb.

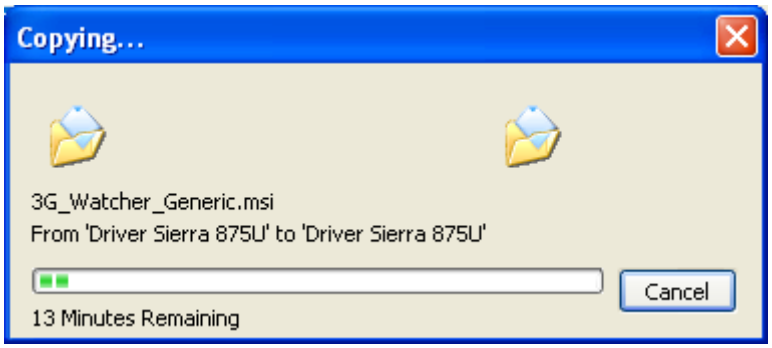


Gambar 4.50 *Propertis file dirver* sierra 875U di *file server*



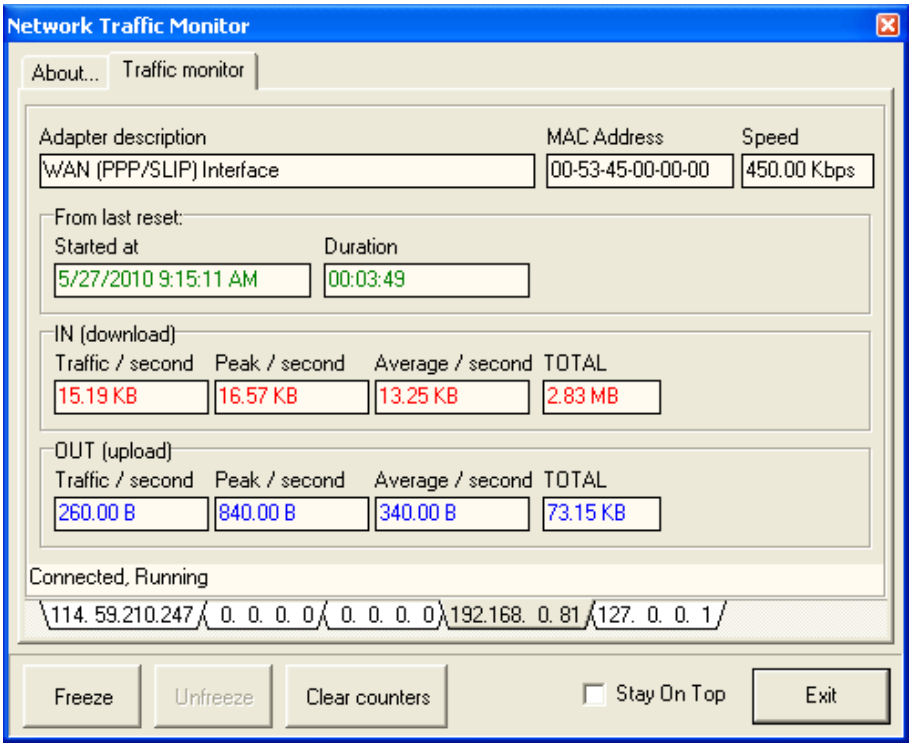
Gambar 4.51 *Local Disk drive [C:]*

Gambar diatas belum dilakukan *copy file*.

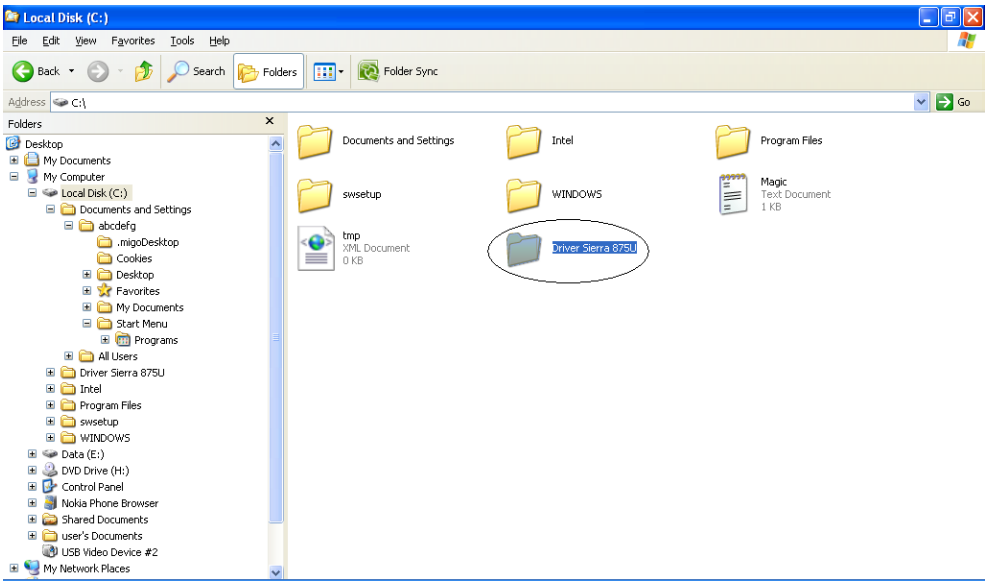


Gambar 4.52 Proses *copy file*

Pada proses *copy file* akan dilaksanakan *check bandwidth* menggunakan *Network Traffic Monitor* pada gambar di bawah terlihat rata-rata pemakaian *bandwidth* sebesar 128 Kbps jadi pemakaian maksimal adalah sebesar 128 Kbps

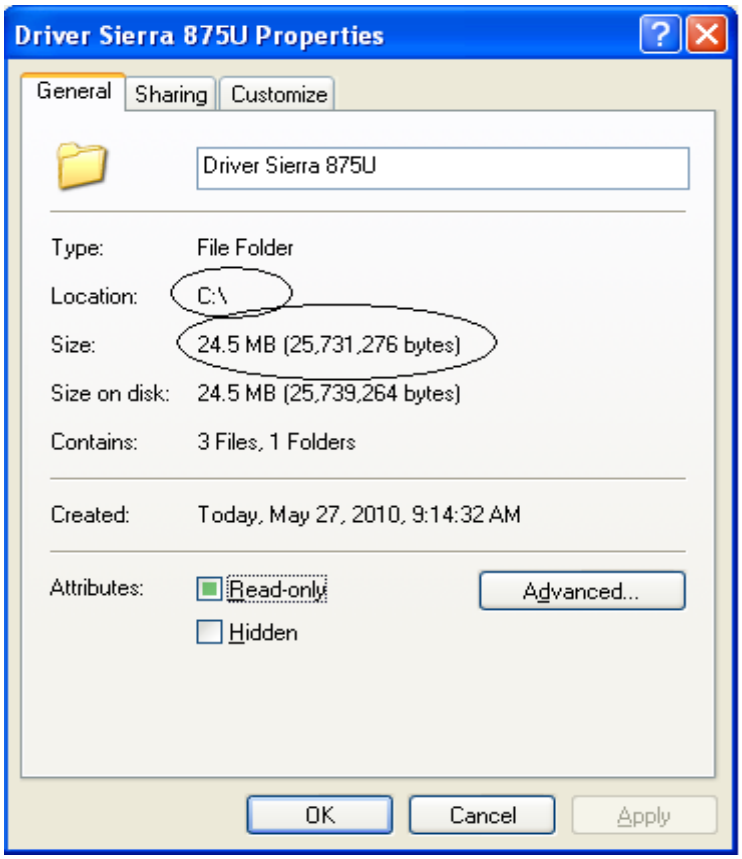


Gambar 4.53 Pengukuran *bandwidth* pada saat proses *copy file*



Gambar 4.54 *Local Disk drive [C:]*

Gambar diatas menunjukan *file* yang sudah *tercopy* ke *local disc drive* C



Gambar 4.55 *Propertis file diver* sierra 875U di lokal *disc dive* C

4.4.3 Pengujian Sistem pada Mail Intranet

Pengujian pada *email server* akan diuji dengan menggunakan dua *acount user* yang berbeda dan masing-masing *user* menggunakan aplikasi yang berbeda untuk akses emailnya. Aplikasi yang akan di gunakan diantaranya :

1. Aplikasi microsoft office outlook
2. Webmail (Qmail)

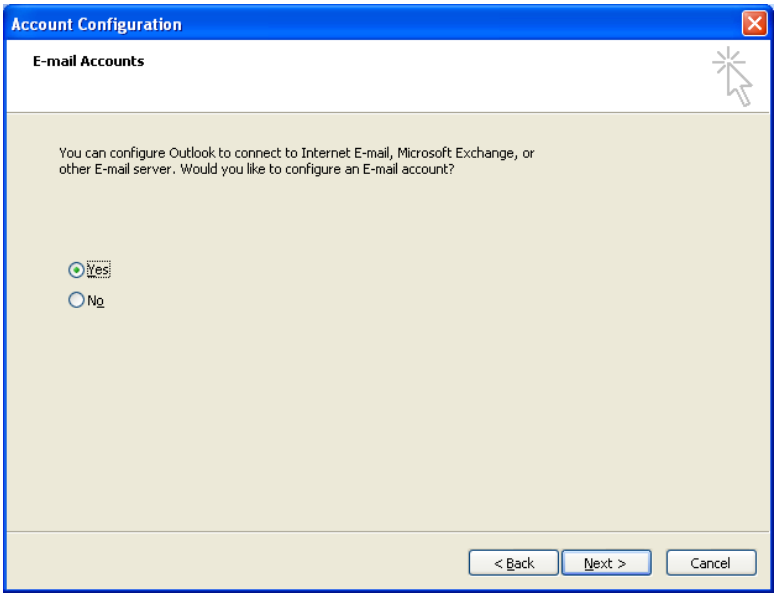
Selanjutnya akan dilakukan pengiriman email pada masing-masing *acount* yang sudah terdaftar diserver mail intranet PT Bandung Arta Mas.

4.4.3.1 Aplikasi Microsoft Office Outlook

Konfigurasi *Microsoft Office Outlook* menggunakan *versi office outlook* 2007 Pertama masuk ke start menu klik *Microsoft Office Outlook* akan muncul gambar seperti dibawah kemudian klik *next*

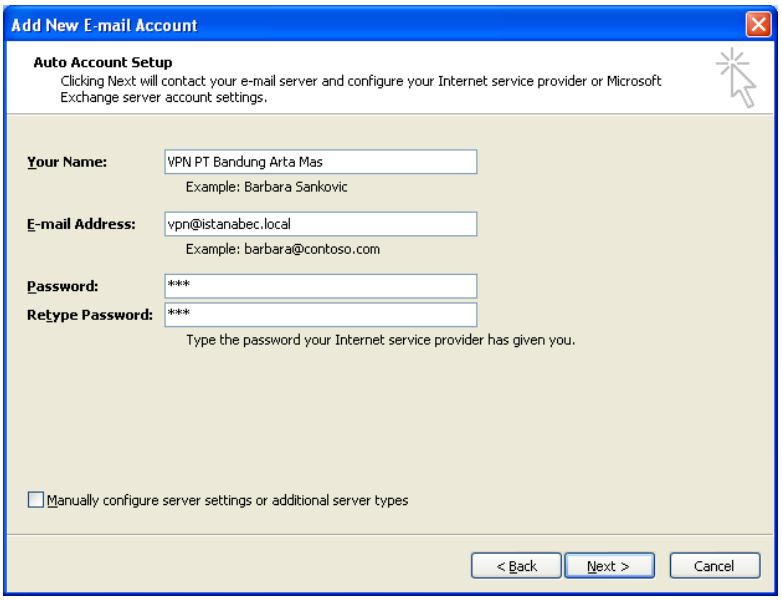


Gambar 4.56 Outlook 2007 Startup Wizard



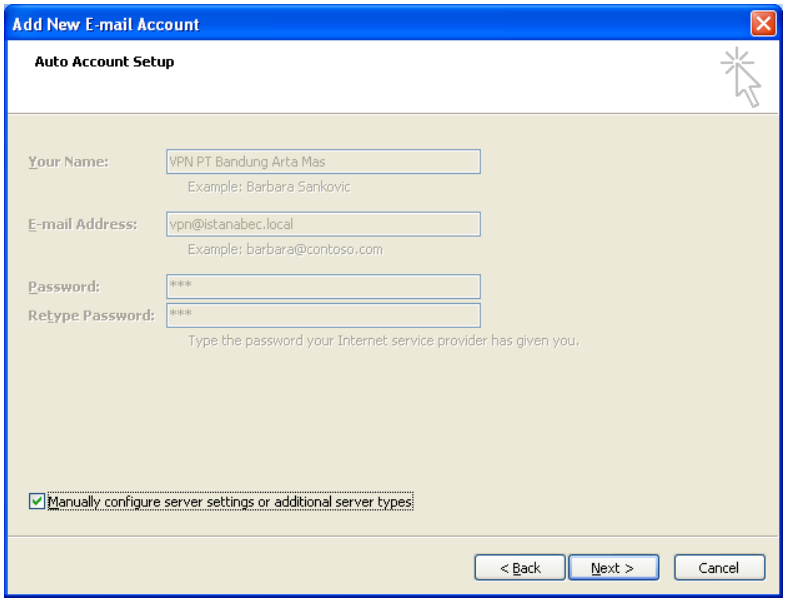
Gambar 4.57 *Konfigurasi Account*

Pilih *yes* pada gambar di atas untuk melanjutkan konfigurasi *account*, lalu klik *next* kemudian isi kolom-kolom yang telah tersedia seperti gambar di bawah.

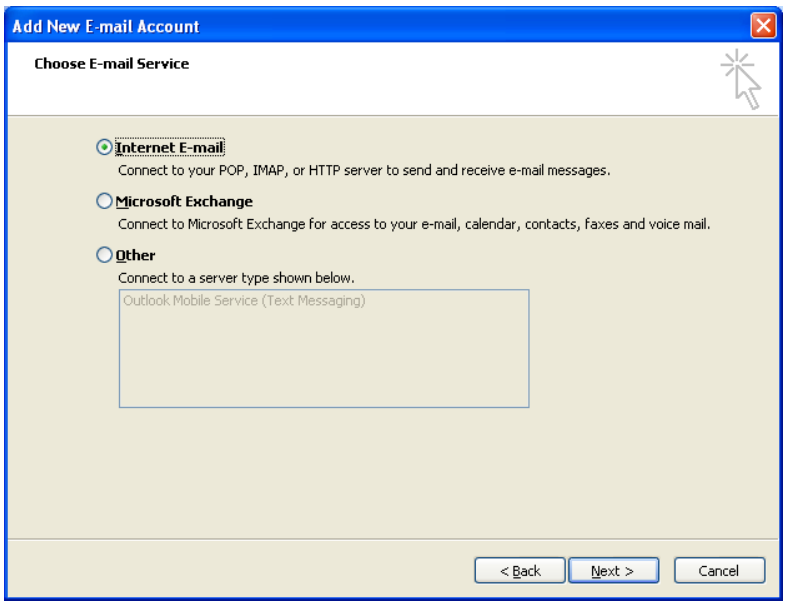


Gambar 4.58 Auto *Setup Account*

Setelah selesai melakukan pengisian nama beserta alamat *email*, untuk kofigur settingan *server* diisi manual centang kolom *Manually configure server setting or additional server type*, seperti gambar di bawah kemudian klik *next* untuk melanjutkan settingan *server*

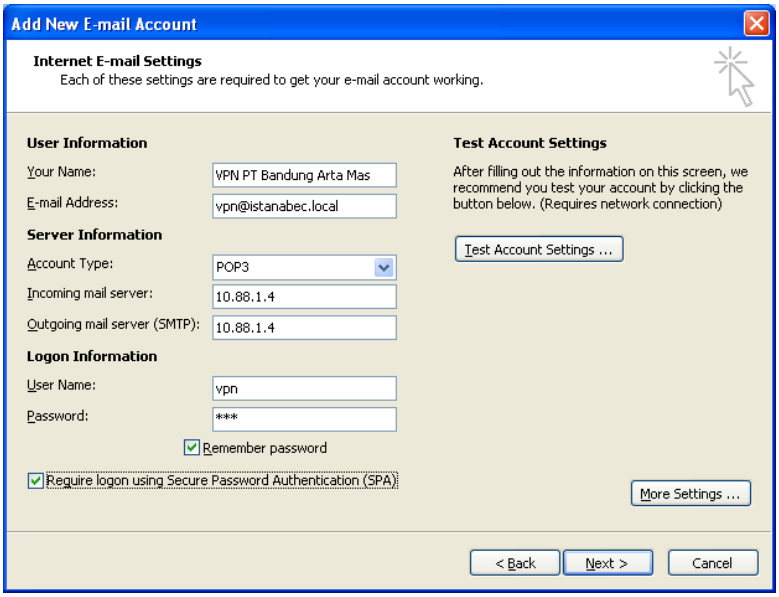


Gambar 4.59 Auto *Setup Account*



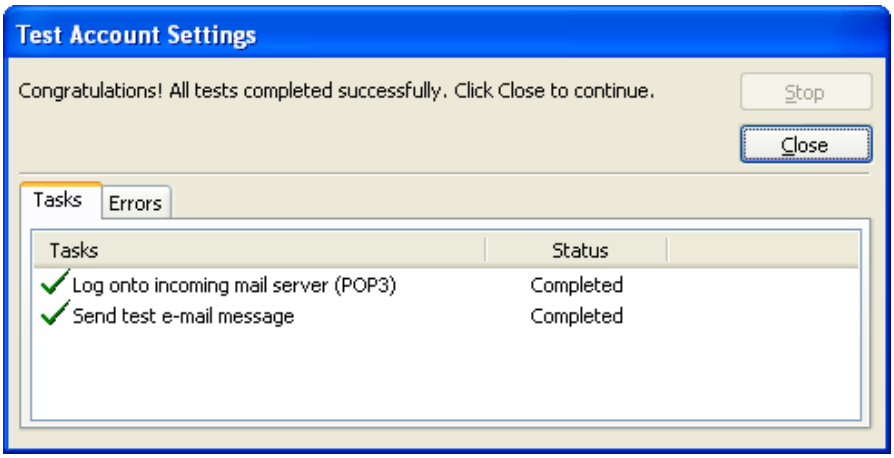
Gambar 4.60 Pemilihan E-mail *service*

Pada gambar diatas pemilihan *email service* menggunakan *email internet* untuk *configure manual server*, lalu klik *next*



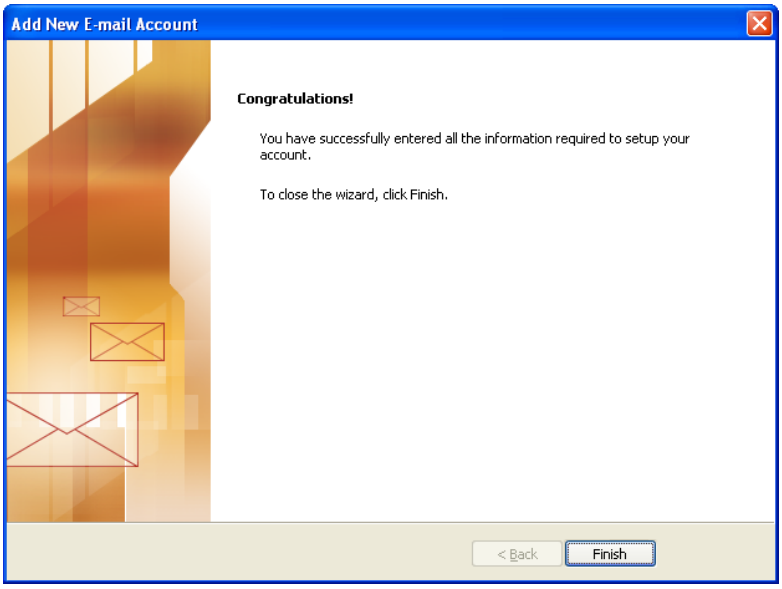
Gambar 4.61 Internet E-mail setting

Masukan *IP address mail server intranet* PT Bandung Arta Mas untuk *Incoming mail server* dan *Outgoing mail server* IP addressnya sama, *acount* tipe *mail server* menggunakan POP3



Gambar 4.62 *Test Account Setting*

Untuk membuktikan bahwa *account user* benar-benar terdaftar di email *server* PT Bandung Arta Mas, lakukan tes *account* setting dengan cara seperti gambar diatas.



Gambar 4.63 *Konfigurasi account finish*

Account berhasil di konfigurasi dan *email intranet* sudah terhubung dengan *server email intranet* PT Bandung Arta Mas.

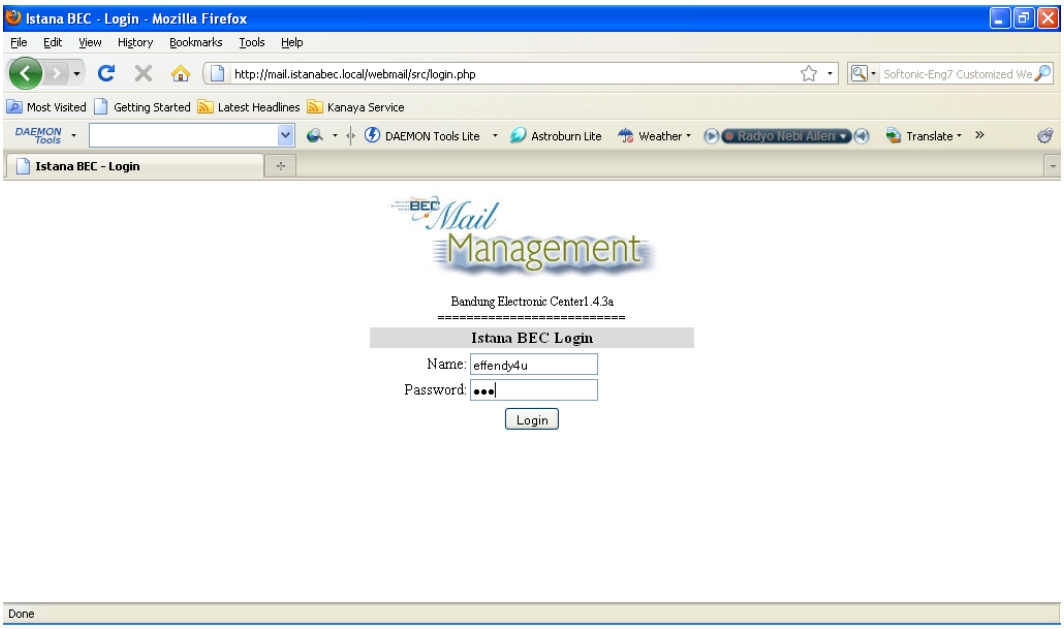
4.4.3.2 Web Mail (Qmail)

Langkah pertama buka *web browser* disini pengujian menggunakan *web browser* mozilla firefox. Masukan alamat *mail server*



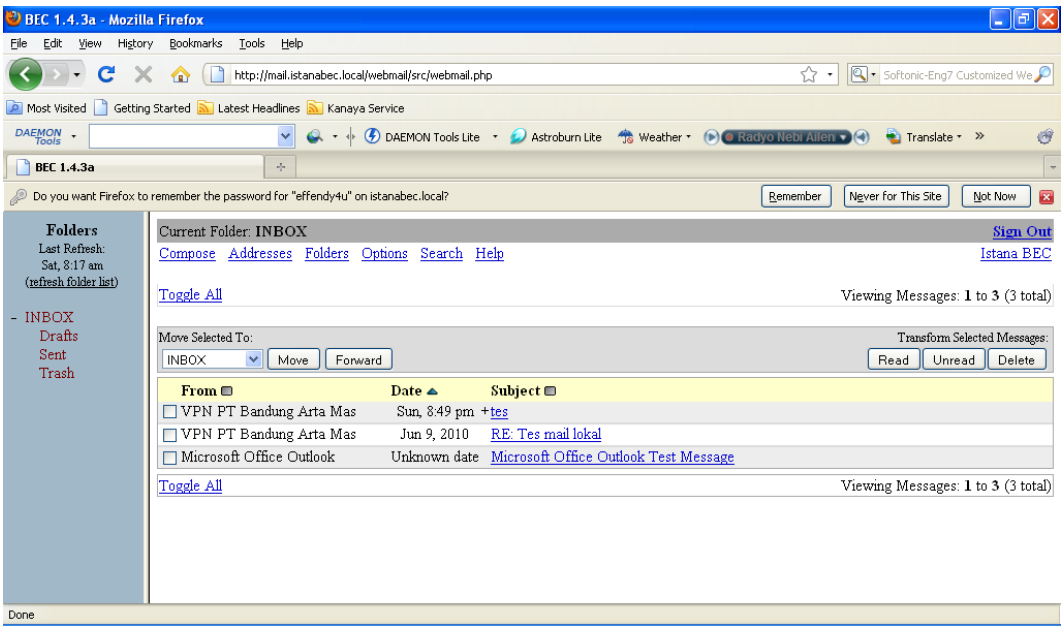
Gambar 4.64 Webmail PT Bandung Arta Mas

Klik *Webmail* kemudian masukan *user name* dan *password* seperti gambar di bawah :

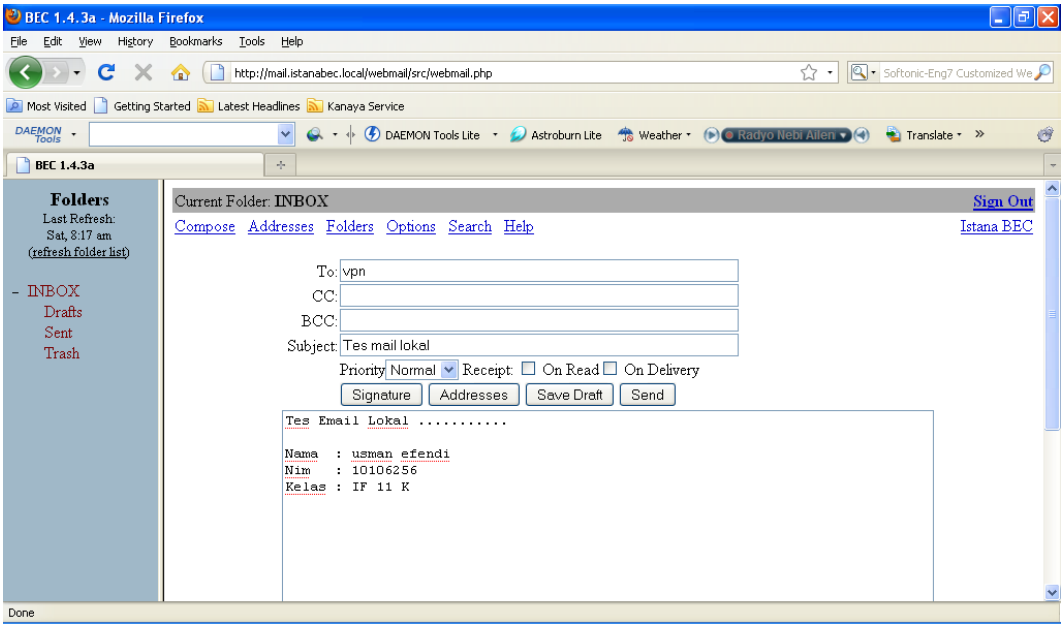


Gambar 4.65 Tampilan Menu login

Setelah melakukan *log in* maka akan masuk ke menu *inbox*

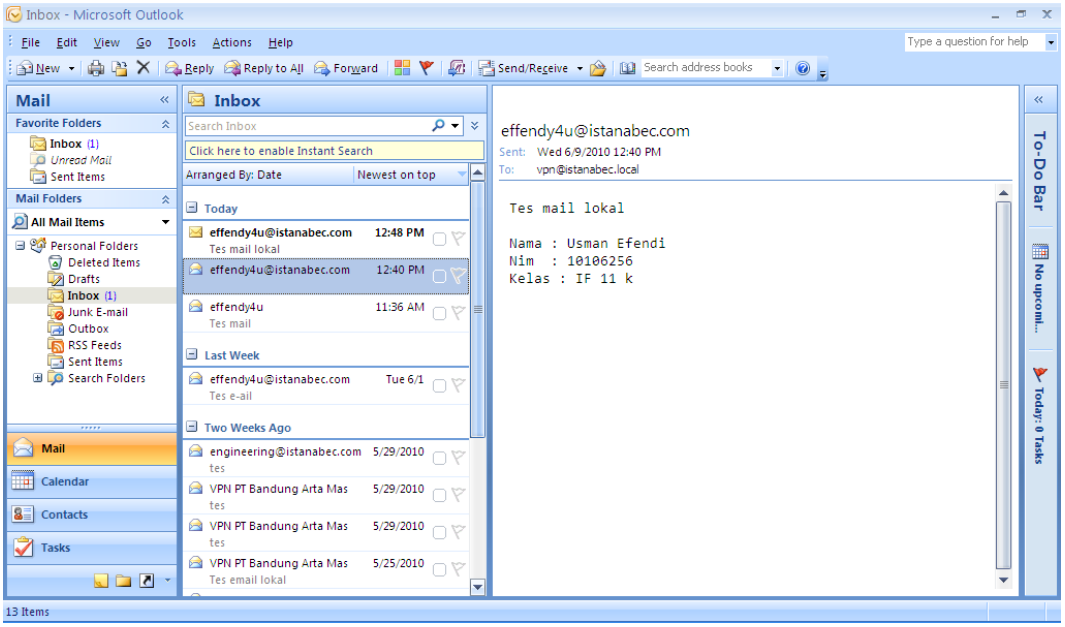


Gambar 4.66 Tampilan *Menu inbox*



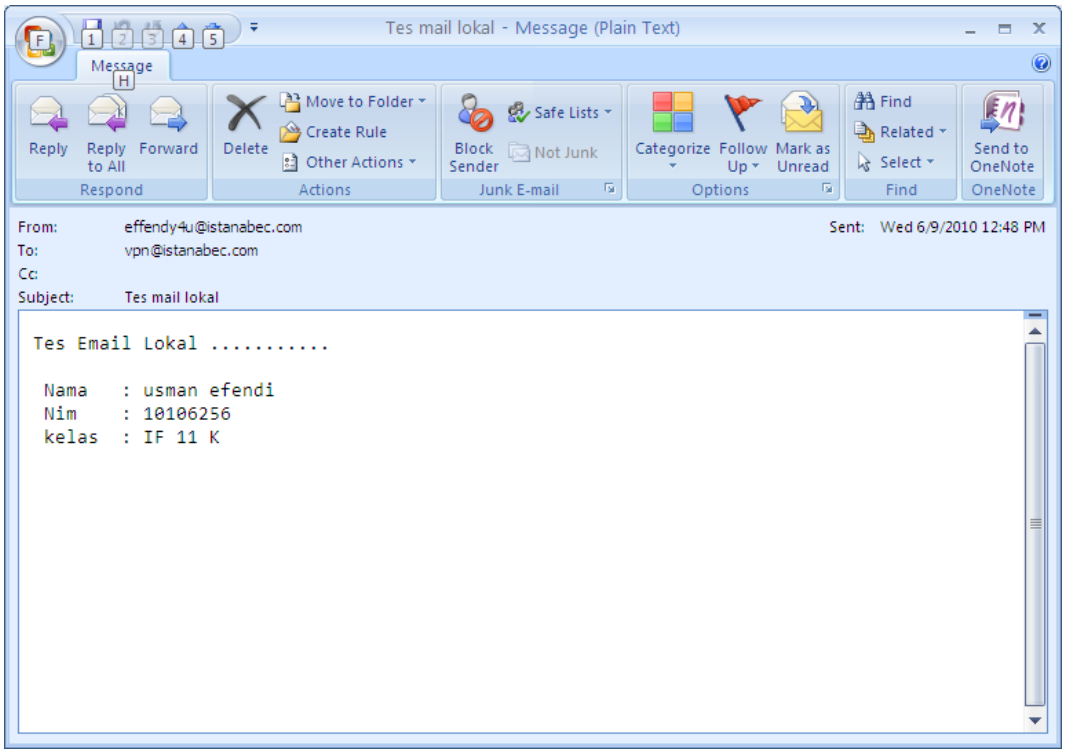
Gambar 4.67 Tampilan *menu create message*

Pada gambar di atas akan dilakukan pengujian *email intranet* dengan mengirim pesan ke *account* yang sudah di buat di mocfrosoft office outlook yaitu *account* VPN. Lalu klik *send.* Kemudian saya akan buka *email* yang sudah dikirim melalui *webmail* tersebut dengan menggunakan Microsoft office outlook.



Gambar 4.68 Menu *Inbox* Microsoft Office Outlook

Pada gambar diatas mail yang dikirim sudah diterima dan bisa diakses seperti gambar dibawah.



Gambar 4.69 Tampilan *message* Microsoft office outlook

4.4.4 Pengujian Sistem Pada Aplikasi Berbasis *Client Server*

Tahap pengujian sistem pada aplikasi *client server* akan membuktikan bahwa pengambilan *database* bias dilakukan pada koneksi jaringan VPN. Pada pengujian ini akan dilakukan menggunakan dua aplikasi berbasis *client server*.

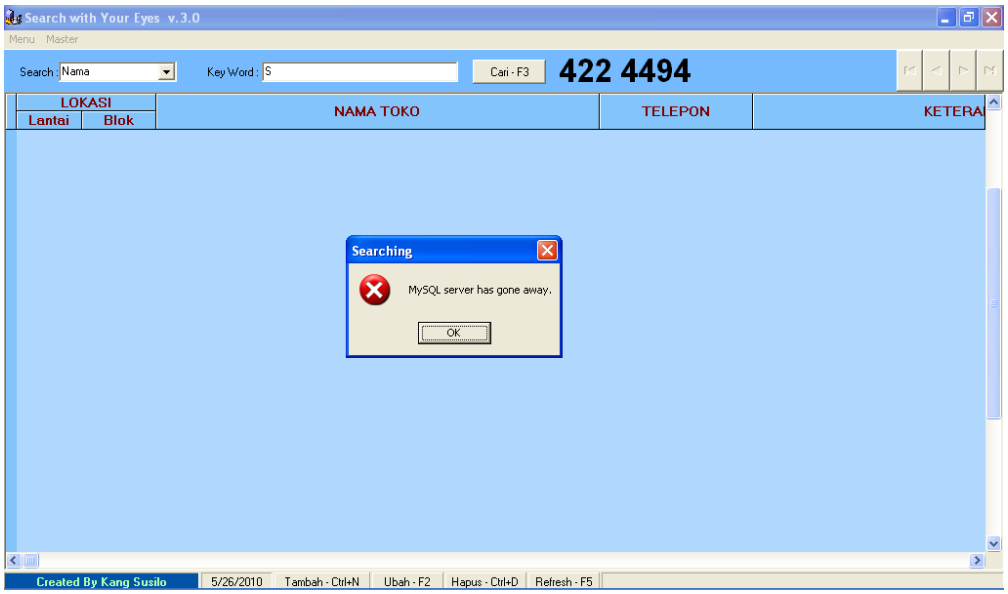
4.4.4.1 Aplikasi *Searching*

Aplikasi *searching* yang ada di PT Bandung Arta Mas berfungsi untuk membantu mempermudah *customer service* untuk mencari no *telephone* kios-kios yang ada di PT Bandung arta mas. Aplikasi *searching* ini berbasis *client server*.



Gambar 4.70 Tampilan Aplikasi Searching

Pada gambar di atas pengujian dengan koneksi VPN dan melakukan penencarian no telp untuk salahsatu kios yang sudah terdaftar no *telphone* nya di aplikasi tersebut.

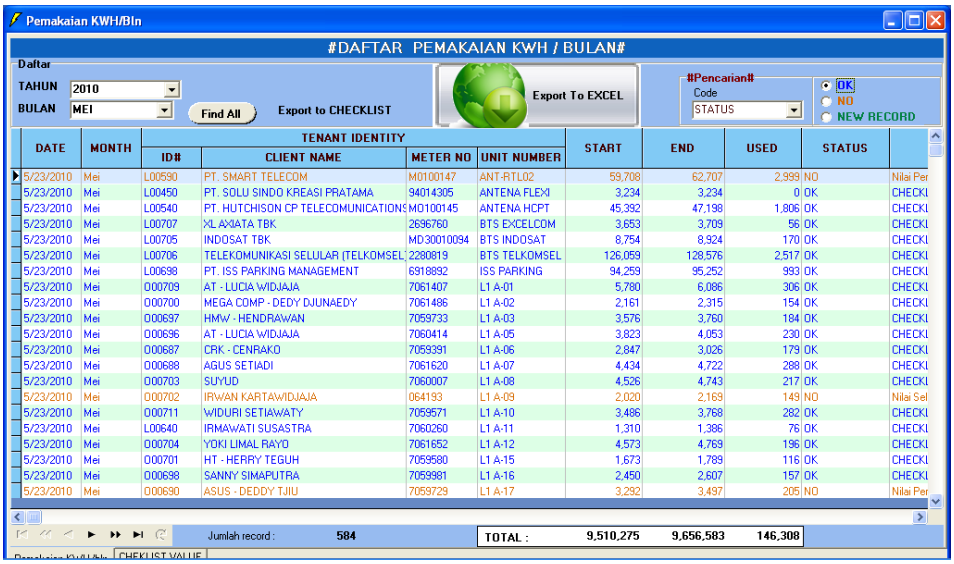


Gambar 4.71 Tampilan Aplikasi *Searching* Tanpa Koneksi VPN

Pada gambar diatas diuji apabila koneksi VPN di-*disconek*, maka dalam aplikasi akan muncul peringatan *database* tidak ditemukan.

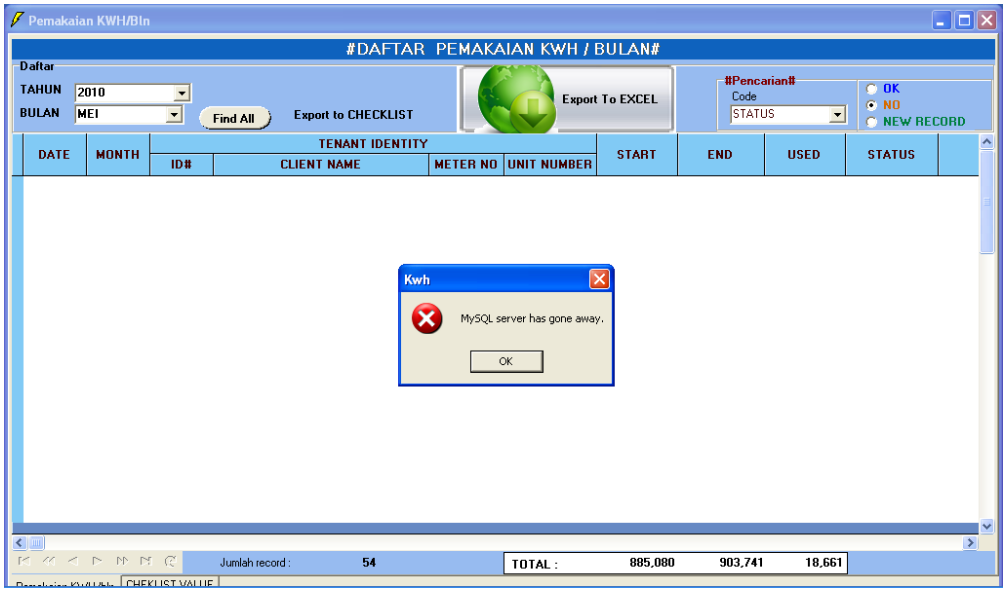
4.4.4.2 Aplikasi *Checklist* KWH Meter Listrik

Aplikasi *checklist* KWH meter adalah sebuah aplikasi yang berfungsi untuk membantu mengurangi tingkat kesalahan pada pencatatan KWH meter listrik di PT Bandung Arta Mas.



Gambar 4.72 Tampilan Aplikasi KWH Meter Listrik

Pada Gambar diatas terdapat *record-record* yang menunjukan nama *client*, no meter, alamat *client*, pencatatan awal, pencatatan akhir status dan keterangan. *Record* tersebut akan di *check* satatus nya untuk mengurangi tingkat kesalahan pada pencatataan KWH meter listrik di PT Bandung Arta Mas. Data gambar di atas bisa dii tampilkan *record-record* karena aplikasi dihubungkan oleh VPN ke *database server*.



Gambar 4.73 Tampilan Aplikasi KWH Meter Listrik Tanpa Koneksi VPN

Pada gambar diatas adalah pengujian tanpa koneksi VPN dan gambar menunjukan aplikasi tidak bias mengambil database karena koneksi VPN diputus.

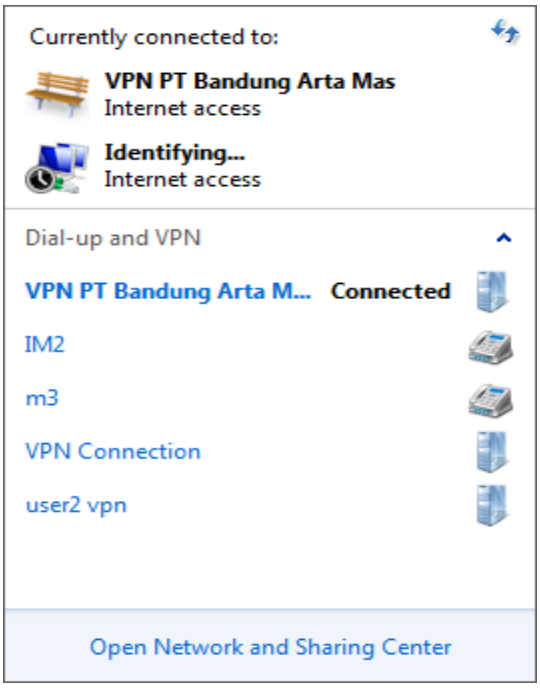
4.4.5 Pengujian pada Session User

Tahap pengujian pada session user akan membuktikan bahwa pemakaian username dan password yang terdaftar tidak bisa digunakan untuk mengakses jaringan vpn pada waktu yang bersamaan dengan menggunakan username dan pasword yang sama.

Pada pengujian session user menggunakan dua unit komputer yang berbeda, pertama user memasukan username dan passwoerd yang akan di ujicoba dan terkoneksi ke jaringan VPN



Gambar 4.74 ***Dialog Network cnnection***



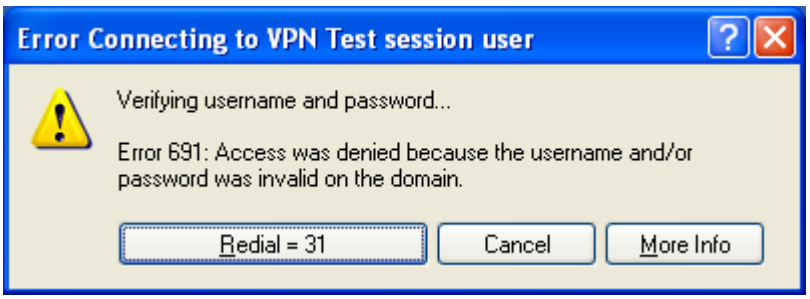
Gambar 4.75 ***View network conecction***

Dari gambar di atas jaringan VPN sudah terkoneksi, kemudian melakukan koneksi ke jaringan vpn di kkomputer yang berbeda dengan melakukan username dan password yang sama.



Gambar 4.76 ***Dialog Network cnnection***

Setelah proses memasukan username dan password yang sama maka akan muncul peringatan seperti gambar dibawah



Gambar 4.77 ***Message error connection***

4.5 Pengujian Beta

Pengujian beta merupakan pengujian yang dilakukan secara objektif untuk memastikan apakah sistem yang telah dibuat diterima atau tidak diterima oleh pihak instansi, melalui kuisioner yang dibagikan kepada responden. Kuesioner yang dibagikan terdiri atas dua bagian diantaranya.

a. Kuesioner untuk admin

b. kuesioner untuk User VPN

Khusus kuesioner untuk admin hanya diberikan kepada pihak yang nantinya akan memegang penuh tanggung jawab untuk sistem yang dibangun yaitu Dept. Head IT PT Bandung Arta Mas. Berikut kuesioner yang diberikan kepada beberapa responden.

a. Kuesioner untuk admin

1. Apakah penggunaan jaringan VPN dapat menjamin keamanan data pada saat transfer data ?
    a. Sangat setuju
    b. Setuju
    c. Kurang setuju
    d. Tidak setuju

2. Apakah jaringan VPN yang di bangun mudah untuk menambah dan menghapus user ?
    a. Sangat setuju
    b. Setuju

c. Kurang setuju

d. Tidak setuju

3. Apakah prformansi jaringan VPN yang dibangun sangat baik ?

    a. Sangat setuju

    b. Setuju

    c. Kurang setuju

    d. Tidak setuju

4. Apakah bandwidth yang digunakan sangat cukup untuk jaringan VPN PT Bandung Arta Mas ?

    a. Sangat setuju

    b. Setuju

    c. Kurang setuju

    d. Tidak setuju

5. Apakah sistem VPN yang dibangun mudah dipelajari ?

    a. Sangat setuju

    b. Setuju

    c. Kurang setuju

    d. Tidak setuju

Hasil kuesioner admin VPN

Tabel 4.3 Jawaban Pertanyaaan Kuesioner Admin

No	Pertanyaan	Jawaban
1	Apakah penggunaan jaringan VPN dapat menjamin keamanan data pada saat transfer data ?	**A (Sangat setuju)**
2	Apakah jaringan VPN yang di bangun mudah untuk menambah dan menghapus user ?	**A (Sangat setuju)**
3	Apakah prformansi jaringan VPN yang dibangun sangat baik ?	**B (Setuju)**
4	Apakah bandwidth yang digunakan sangat cukup untuk jaringan VPN PT Bandung Arta Mas ?	**C (Kurang setuju)**
5	Apakah sistem VPN yang dibangun mudah dipelajari ?	**B (Setuju)**

Dari hasil kuesioner yang ditujukan untuk admin dapat ditarik kesimpulan bahwa sistem VPN yang dibangun di PT Bandung Arta Mas bisa diterima dengan baik oleh pihak perusahaan dan tujuan dari pembangunan jarinagn VPN tercapai.

b. Kuesioner untuk user VPN

1. Apakah implementasi VPN yang diterapkan mudah digunakan?
    a. Sangat setuju
    b. Setuju
    c. Kurang setuju
    d. Tidak setuju
2. Apakah sistem VPN yang diterapkan mempermudah komunikasi data dengan kantor pusat atau kantor-kantor cabang?
    a. Sangat setuju

b. Setuju
c. Kurang setuju
d. Tidak setuju

3. Apakah dengan adanya sistem VPN dapat meningkatkan efektivitas dan efisiensi kerja?
    a. Sangat setuju
    b. Setuju
    c. Kurang setuju
    d. Tidak setuju
4. Apakah jaringan VPN yang dibangun membantu perluasan konektivitas dengan kantor cabang yang lain ?
    a. Sangat setuju
    b. Setuju
    c. Kurang setuju
    d. Tidak setuju
5. Apakah sistem VPN yang dibangun di PT Bandung Arta Mas berjalan optimal ?
    a. Sangat setuju
    b. Setuju
    c. Kurang setuju
    d. Tidak setuju

Pada pengujian ini, perhitungan kuisioner adalah berdasarkan bobot nilai setiap item pilihan. Bobot nilai tersebut adalah :

Bobot nilai pengujian : A = 4

: B = 3

: C = 2

: D = 1

Hasil kuesioner User VPN

1. Untuk pertanyaan No. 1 “Apakah implementasi VPN yang diterapkan mudah digunakan?”

Tabel 4.4 Jawaban Pertanyaaan no 1

Kategori Jawaban	Sangat Setuju	Setuju	Kurang Setuju	Tidak Setuju
Frekuensi Jawaban	2	3	0	0

2. Untuk pertanyaan No. 2 “mempermudah komunikasi data dengan kantor pusat atau kantor-kantor cabang?”

Tabel 4.5 Jawaban Pertanyaaan no 2

Kategori Jawaban	Sangat Setuju	Setuju	Kurang Setuju	Tidak Setuju
Frekuensi Jawaban	4	1	0	0

3. Untuk pertanyaan No. 3 “Apakah dengan adanya sistem VPN dapat meningkatkan efektivitas dan efisiensi kerja?”

Tabel 4.6 Jawaban Pertanyaaan no 3

Kategori Jawaban	Sangat Setuju	Setuju	Kurang Setuju	Tidak Setuju
Frekuensi Jawaban	4	1	0	0

4. Untuk pertanyaan No. 4 “Apakah jaringan VPN yang dibangun membantu perluasan konektivitas dengan kantor cabang yang lain?”

Tabel 4.7 Jawaban Pertanyaaan no 4

Kategori Jawaban	Sangat Setuju	Setuju	Kurang Setuju	Tidak Setuju
Frekuensi Jawaban	3	2	0	0

5. Untuk pertanyaan No. 5 “Apakah sistem VPN yang dibangun di PT Bandung Arta Mas berjalan optimal?”

Tabel 4.8 Jawaban Pertanyaaan no 5

Kategori Jawaban	Sangat Setuju	Setuju	Kurang Setuju	Tidak Setuju
Frekuensi Jawaban	3	2	0	0

Dari tabel di atas kemudian dibuat tabel persentase jawaban yang diberikan oleh responden untuk setiap kategori pertanyaan dan jawaban yang diberikan. Persentase nilai dibuat dengan rumus umum ***(P/n) * 100%***, dimana ***P*** adalah jumlah jawaban pada satu kategori pertanyaan dan jawaban, sedangkan ***n*** adalah jumlah total responden, yaitu lima orang. Tabel dibawah ini memperlihatkan penghitungannya:

Tabel 4.9 Hasil Pengujian Pertanyaan no. 1

No	Keterangan	Responden	Persentase %
1	Sangat Setuju	2	40
2	Setuju	3	60
3	Kurang Setuju	0	0
4	Tidak Setuju	0	0
Jumlah		5	100

Berdasarkan hasil prosentase diatas maka dapat disimpulkan sebanyak tiga orang atau 60% menyatakan setuju sistem VPN yang diterapkan mudah digunakan dan dua orang atau 40% menyatakan sangat setuju bahwa sistem VPN yang diterapkan mudah digunakan.

Tabel 4.10 Hasil Pengujian Pertanyaan no. 2

No	Keterangan	Responden	Persentase %
1	Sangat Setuju	4	80
2	Setuju	1	20
3	Kurang Setuju	0	0
4	Tidak Setuju	0	0
Jumlah		5	100

Berdasarkan hasil prosentase diatas maka dapat disimpulkan sebanyak empat orang atau 80% menyatakan sangat setuju VPN yang diterapkan mempermudah komunikasi data dengan kantor pusat atau kantor-kantor cabang dan satu orang atau 20% menyatakan setuju bahwa sistem VPN yang diterapkan mempermudah komunikasi data dengan kantor pusat atau kantor-kantor cabang.

Tabel 4.11 Hasil Pengujian Pertanyaan no. 3

No	Keterangan	Responden	Persentase %
1	Sangat Setuju	4	80
2	Setuju	1	20
3	Kurang Setuju	0	0
4	Tidak Setuju	0	0
Jumlah		5	100

Berdasarkan hasil prosentase diatas maka dapat disimpulkan sebanyak empat orang atau 80% menyatakan sangat setuju jaringan VPN meningkatkan efektifitas dan efisiensi kerja dan satu orang atau 20% menyatakan setuju bahwa jaringan VPN meningkatkan efektivitas dan efisiensi kerja.

Tabel 4.12 Hasil Pengujian Pertanyaan no. 4

No	Keterangan	Responden	Persentase %
1	Sangat Setuju	3	60
2	Setuju	2	40
3	Kurang Setuju	0	0
4	Tidak Setuju	0	0
Jumlah		5	100

Berdasarkan hasil prosentase diatas maka dapat disimpulkan sebanyak tiga orang atau 60% menyatakan sangat setuju jaringan VPN membantu perluasan konektivitas dengan kantor cabang yang lain dan dua orang atau 40% menyatakan setuju bahwa dengan adanya jaringan VPN membantu perluasan konektivitas dengan kantor cabang yang lain.

Tabel 4.13 Hasil Pengujian Pertanyaan no. 6

No	Keterangan	Responden	Persentase %
1	Sangat Setuju	3	60
2	Setuju	2	40
3	Kurang Setuju	0	0
4	Tidak Setuju	0	0
Jumlah		5	100

Berdasarkan hasil prosentase diatas maka dapat disimpulkan sebanyak tiga orang atau 60% menyatakan sangat setuju sistem VPN yang di bangun di PT Bandung Arta Mas berjalan sesuai tujuan dan dua orang atau 40% menyatakan bahwa sistem VPN yang dibangun di PT Bandung Arta Mas berjalan sesuai tujuan.

Kesimpulan Hasil Pengujian *Beta* pada *User* VPN

Dari hasil kuesioner yang telah dibagikan kepada responden yang nantinya akan menggunakan sistem yang dibangun yaitu karyawan PT Bandung Arta Mas yang telah terdaftar dalam tabel user VPN dan diisi dimana hal tersebut merupakan prosedur pengujian *beta,* dapat disimpulkan bahwa sistem yang dibuat telah sesuai dengan yang diharapkan dan mencapai tujuan.