BAB IV
IMPLEMENTASI DAN PENGUJIAN

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*.

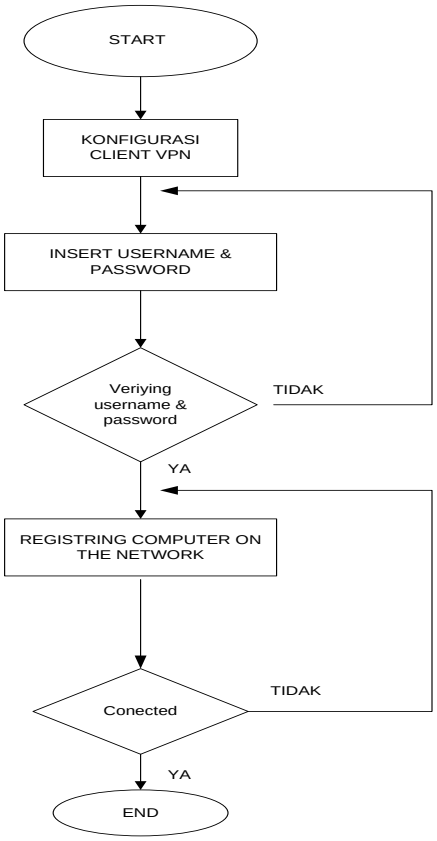
Dalam konfigurasi VPN *Client*, ada beberapa tahapan yang harus dilakukan diantaranya :

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

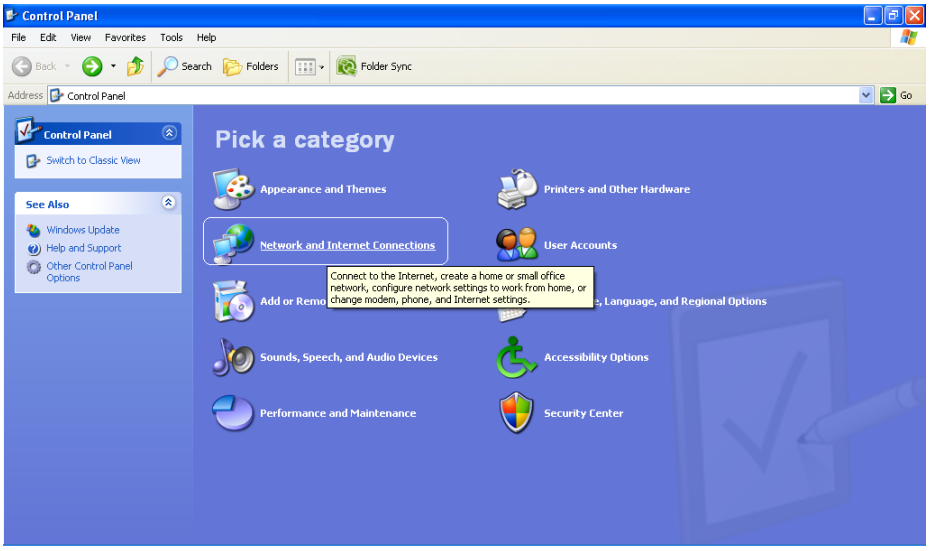
Pengunaan VPN untuk *Client* personal adalah menghubungkan suatu *client* dengan *network* VPN *Server* melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal.

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

Konfigurasi Client OS Windows XP

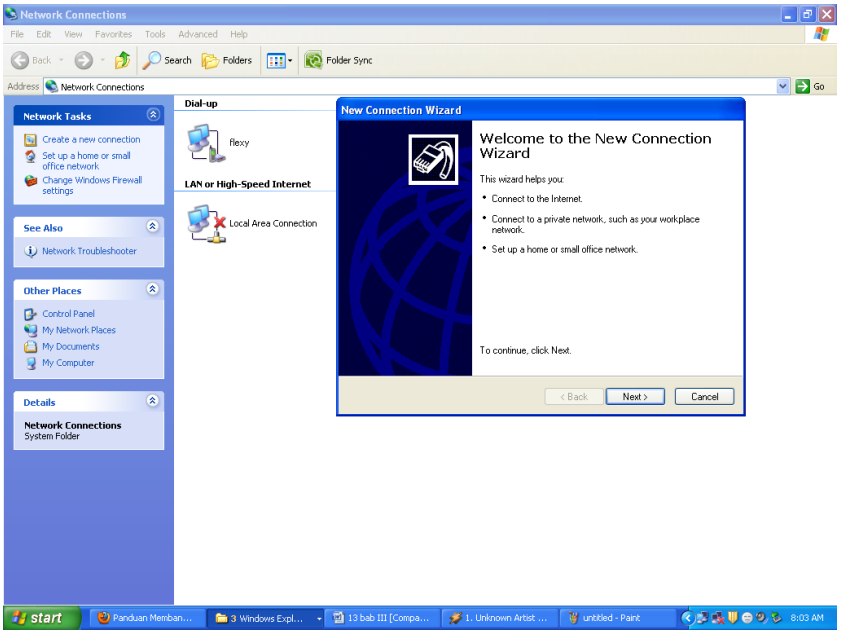
Berikut adalah settingan-setingan *client/user* untuk koneksi ke VPN menggunakan windows xp.

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



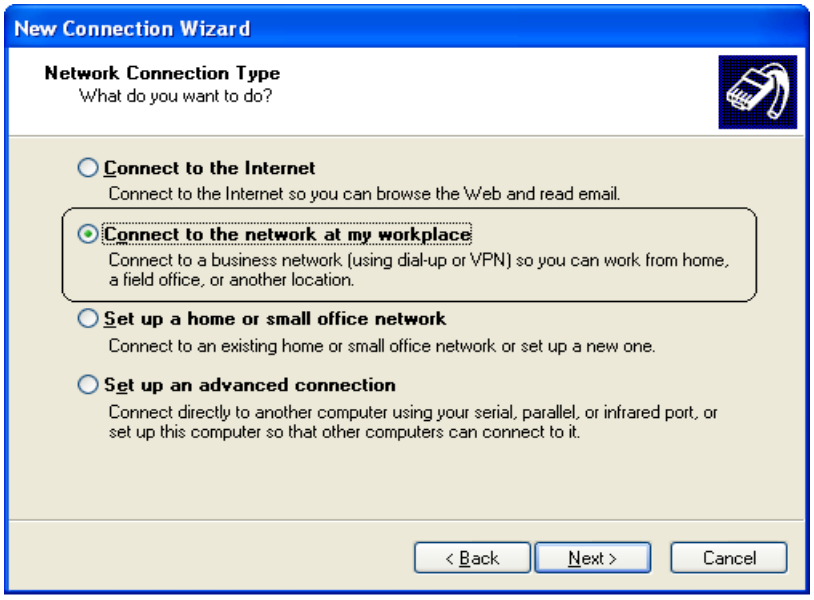
Gambar 4.2 Windows *control panel*

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



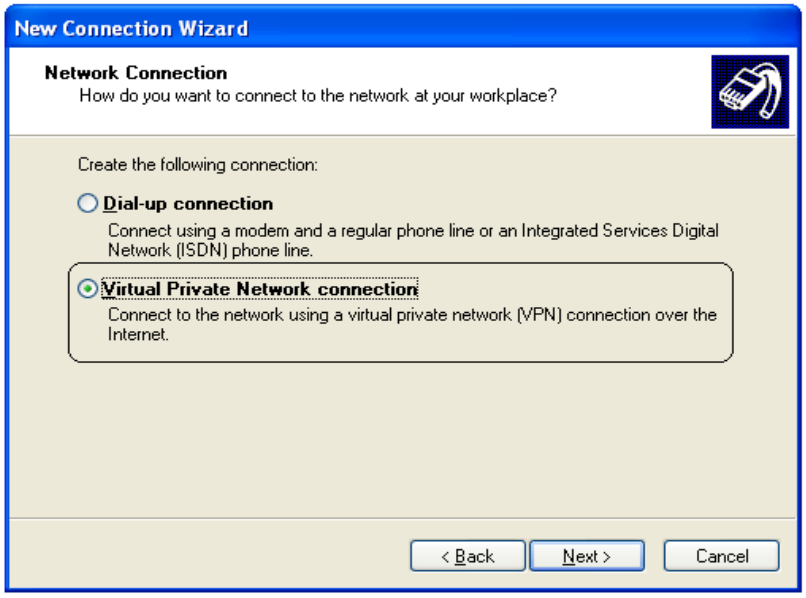
Gambar 4.3 Membuat koneksi baru VPN *client*

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



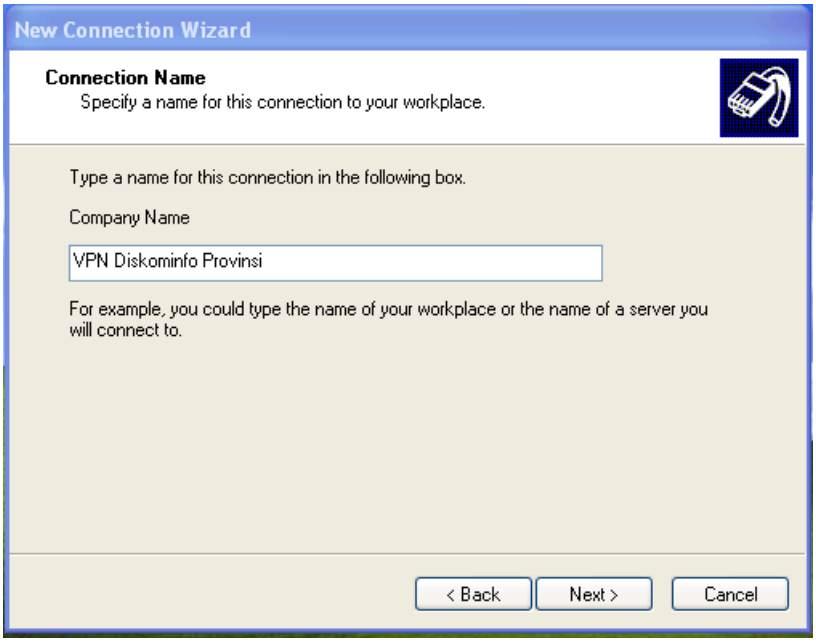
Gambar 4.4 Pemilihan tipe koneksi

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



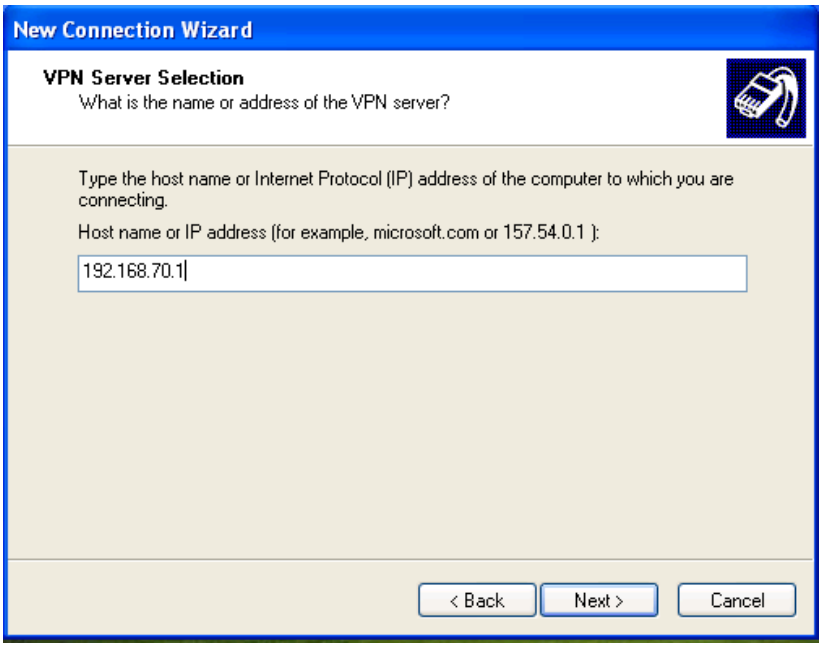
Gambar 4.5 Pemilihan koneksi jaringan

5. Masukan nama untuk sambungan VPN dalam penulisan ini saya masukan nama Diskominfo Provinsi dan klik *next*. Nama untuk sambungan yang dipilih bebas.



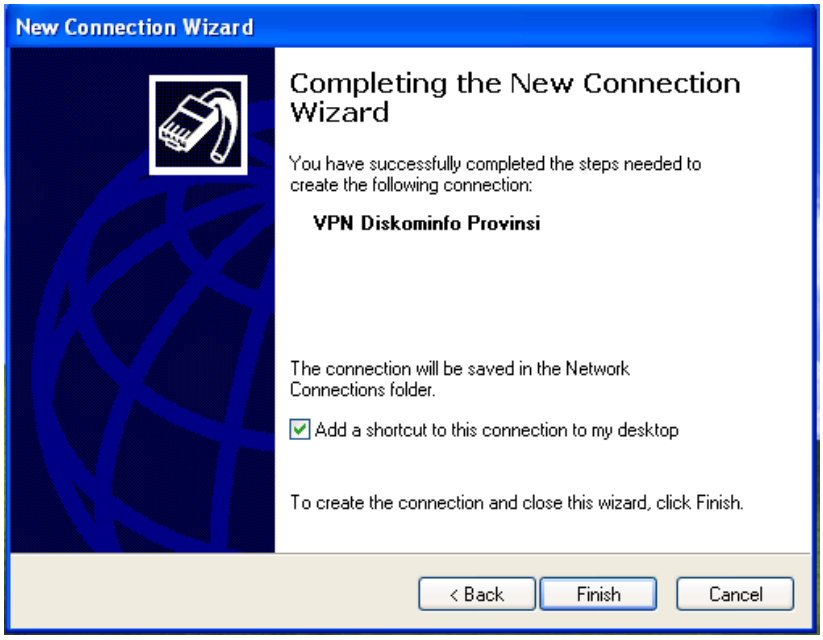
Gambar 4.6 Penamaan koneksi jaringan VPN

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



Gambar 4.7 Memasukan *IP address server* VPN

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



Gambar 4.8 *Finishing* dan Pembuatan *shortcut*

b. Tahap *Dialing* VPN/Koneksi VPN

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

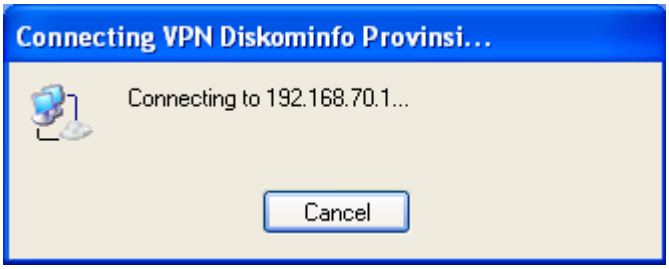
a. *Double* klik pada kotak dialog *network connection* atau pilih *connect* dari menu, akan muncul seperti gambar di bawah



Gambar 4.9 *Dialog Network connection*

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

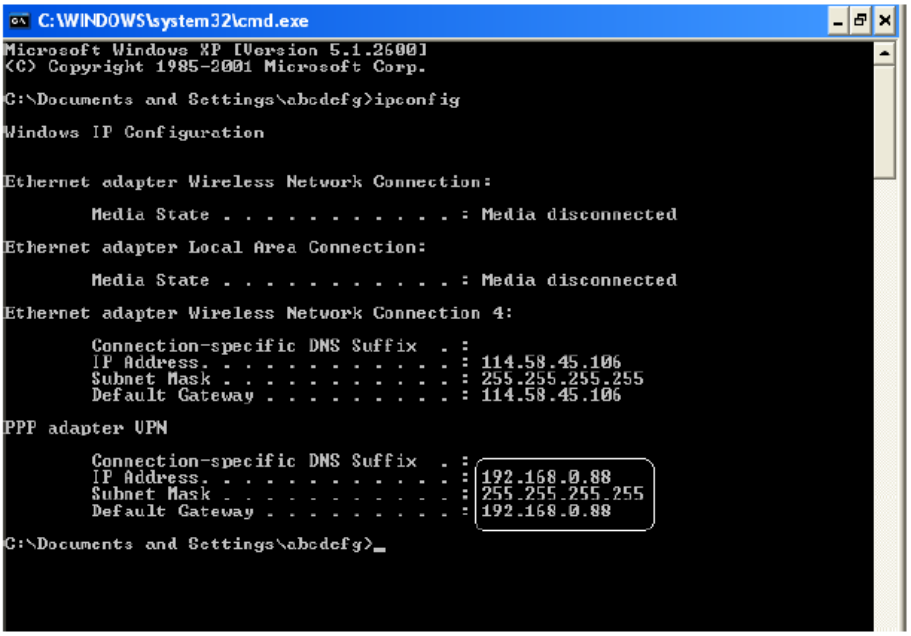
Dari proses *connection* di atas maka proses selanjutnya adalah proses *connection* ke server VPN



Gambar 4.10 *Dialog connection to VPN*

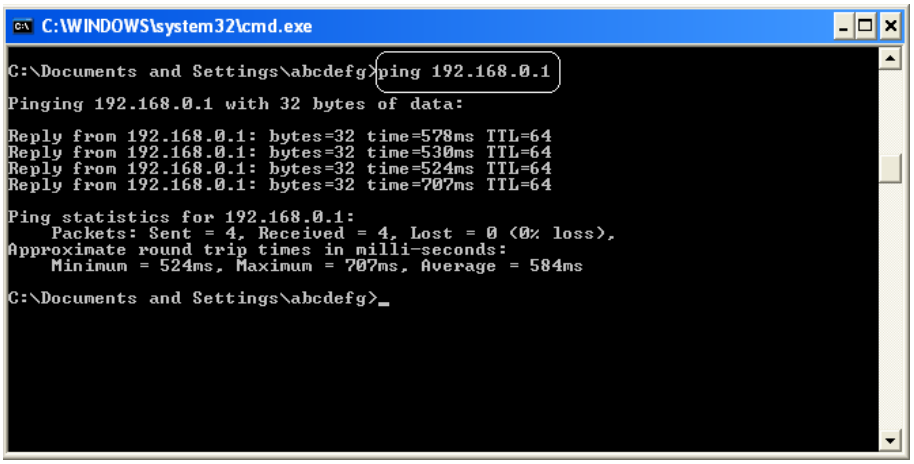
c. Tahap Ping tes dan Kerja VPN

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*.



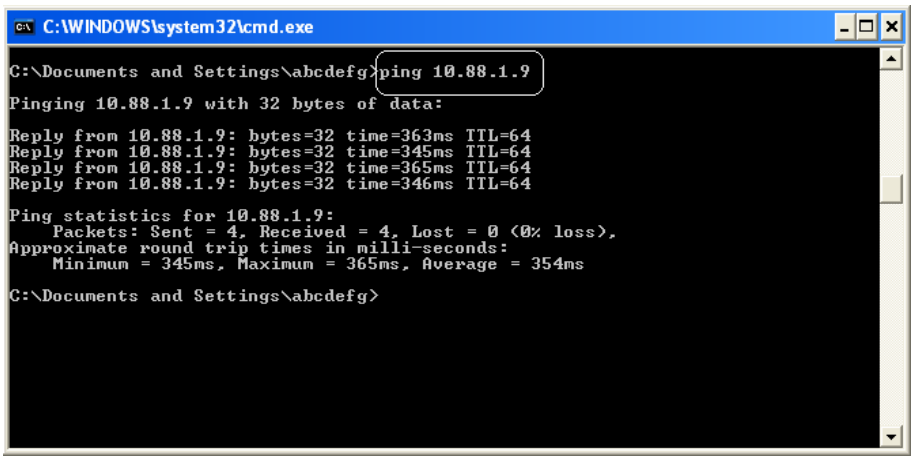
Gambar 4.11 CMD ipconfig

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.



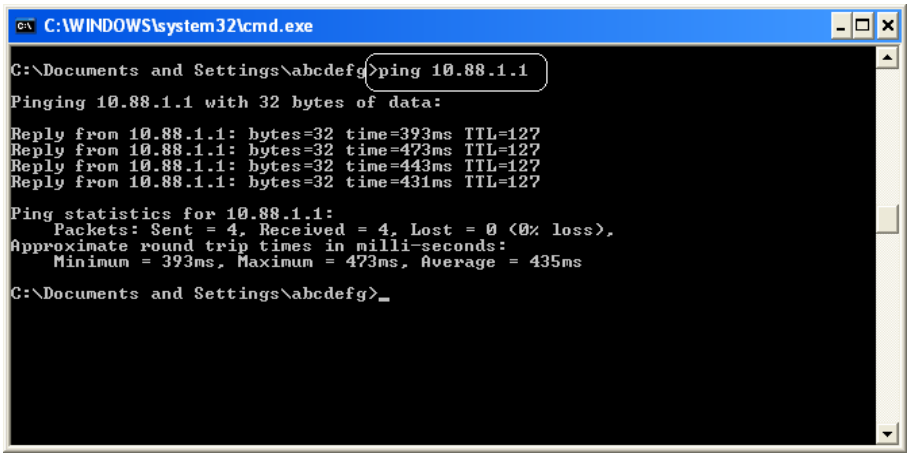
Gambar 4.12 Ping VPN Server

Setelah dilakukan proses ping ke *IP address* VPN *server*, langkah selanjutnya adalah pengujian ke *IP address* lokal VPN yang masuk ke jaringan LAN Diskominfo Provinsi Jawa Barat.



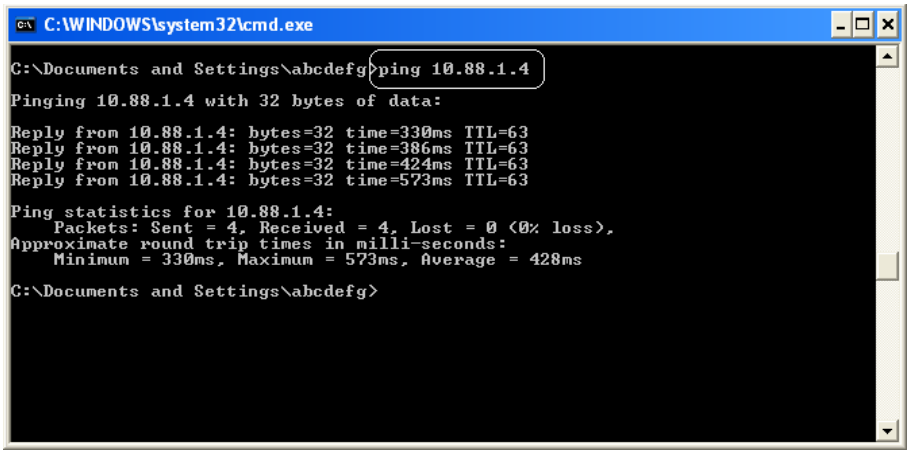
Gambar 4.13 Ping *IP address* lokal VPN

Proses tes ping diatas menandakan *user* VPN sudah terkoneksi ke jaringan lokal Diskominfo Provinsi Jawa Barat 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 Diskominfo Provinsi Jawa Barat. Pertama tes ping ke *IP address file server* 10.88.1.1



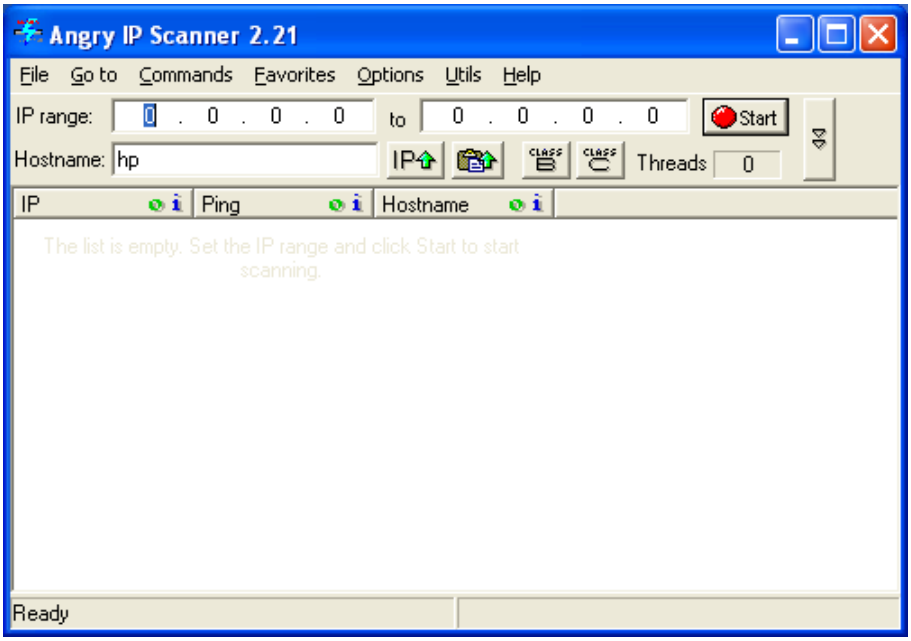
Gambar 4.14 Ping *IP address file server*

Ping *IP address file server* Diskominfo Provinsi Jawa Barat (xserver) terkoneksi. Tahap ping tes selanjutnya *IP address* untuk *mail server* Diskominfo Provinsi Jawa Barat.



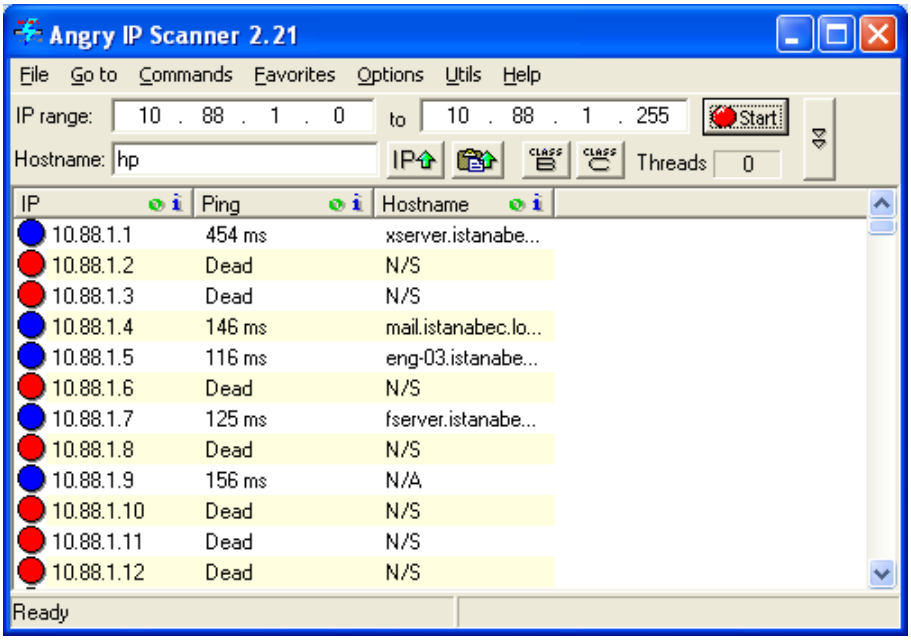
Gambar 4.15 Ping *IP address mail server*

Untuk memastikan bahwa user VPN benar-benar berada di jaringan lokal Diskominfo Provinsi Jawa Barat, maka akan dilakukan pengecekan IP address yang sedang aktif di Diskominfo Provinsi Jawa Barat 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 Diskominfo Provinsi Jawa Barat.



Gambar 4.16 Aplikasi Angry IP Scanner

Masukan *range IP address* Diskominfo Provinsi Jawa Barat mulai dari 10.88.1.0-10.88.1.255 kemudian klik *start* untuk memulai

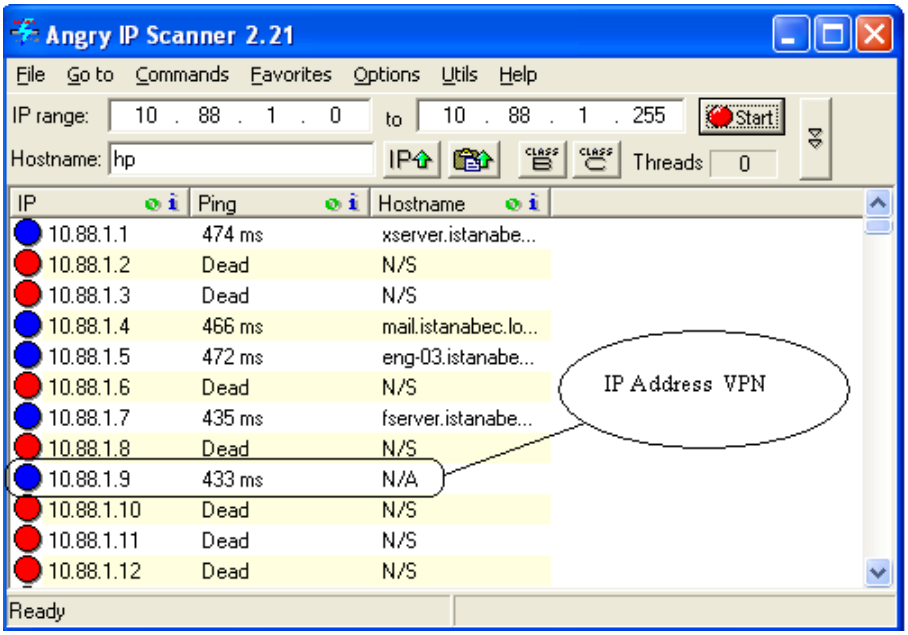


Gambar 4.17 Aplikasi *angry IP Scanner Check User* Diskominfo Provinsi Jawa Barat



Gambar 4.18 *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 Diskominfo Provinsi Jawa Barat.



Gambar 4.19 *IP Address* VPN

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

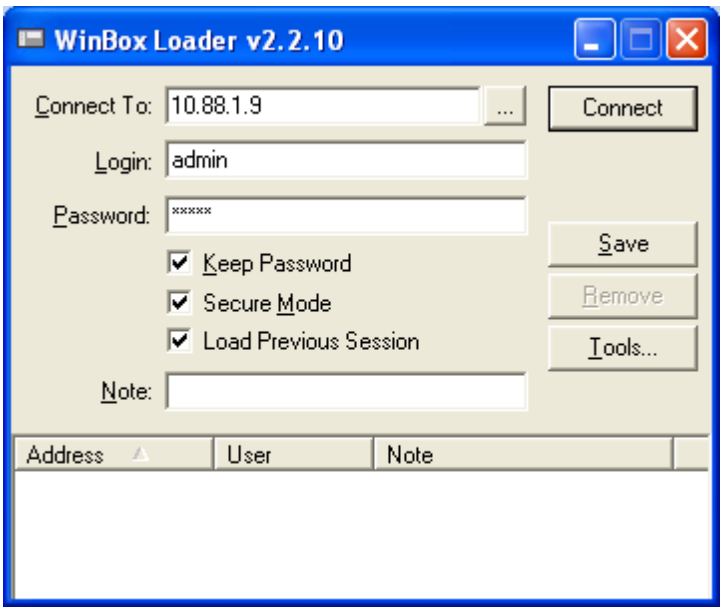
Mikrotik bisa diakses/*remote* menggunakan tool winbox ,Winbox adalah sebuah *utility* untuk melakukan *remote* ke *server* mikrotik dalam mode GUI. Winbox bisa mendeteksi mikrotik yang sudah di install jika masih dalam satu *network*, yaitu dengan mendeteksi MAC address dari *ethernet* yang terpasang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

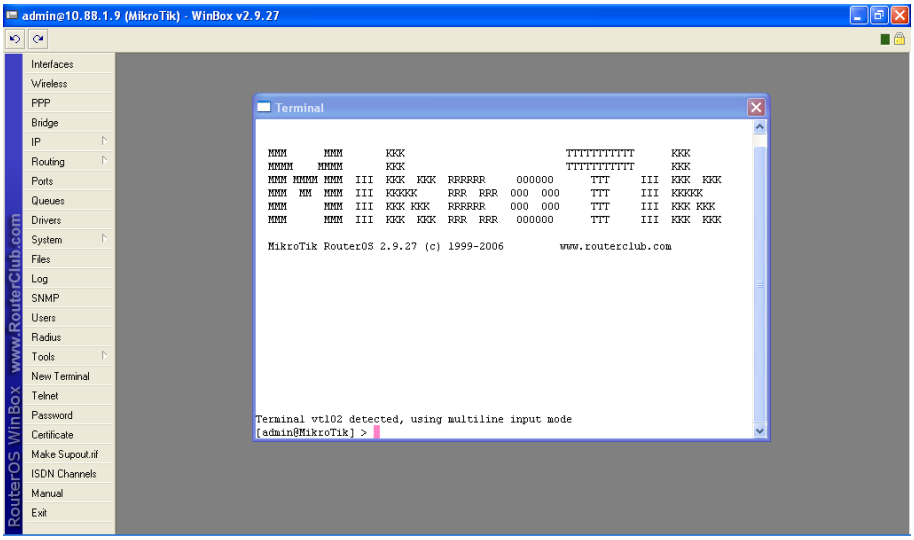
Dalam hal ini pengaksesan Mikrotik *Router*OS akan menggunakan WinBox karena praktis dan mudah digunakan, adapaun cara pengaksesan Mikrotik *Router*OS melalui Winbox adalah sebagai berikut :

a. Buka aplikasi WinBox



Gambar 4.20 *Winbox*

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



Gambar 4.21 *Winbox*

4.3. 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*

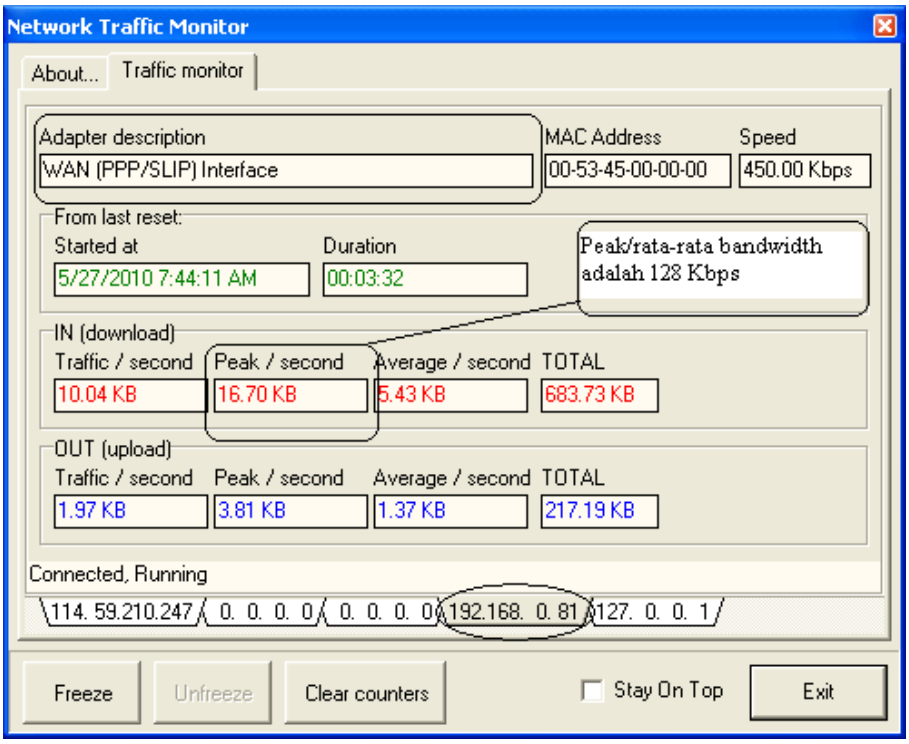
intranet akan menggunakan Microsoft Office Outlok dan Web mail lokal Diskominfo Provinsi Jawa Barat.

4.3.1. 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 Diskominfo Provinsi Jawa Barat menggunaka tunnel PPTP.

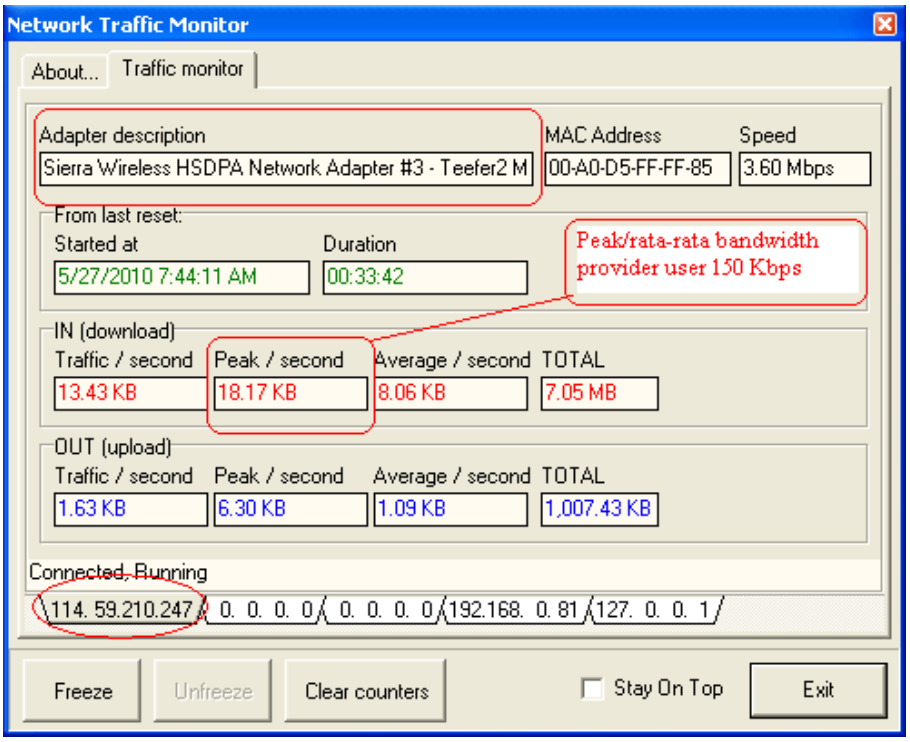


Gambar 4.22 Tampilan aplikasi *Network Traffic Monitor* pada tunnel PPTP

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 4.23 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.