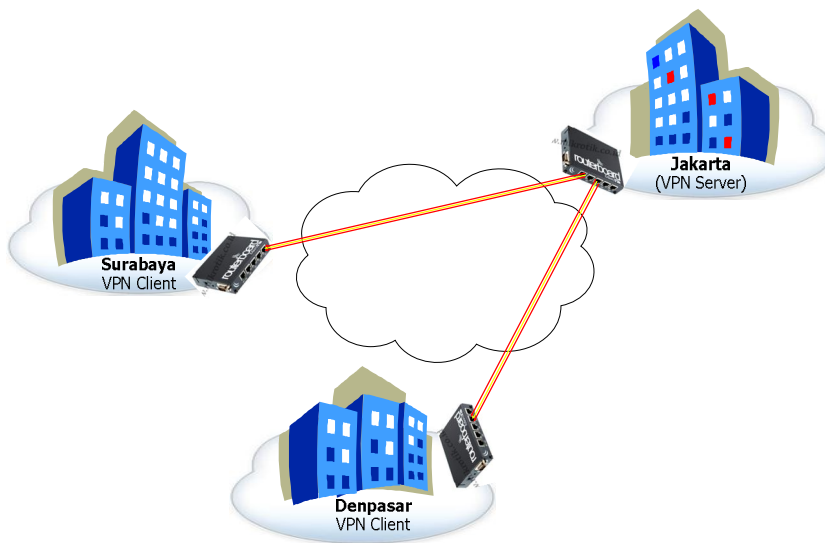


B u k u P a n d u a n

“MEMBANGUN VPN SERVER & CLIENT Dengan Mikrotik”

Untuk menggabungkan 2 Jaringan
LAN Yang beda Lokasi via Internet



Oleh :

Nathan Gusti Ryan



XP Solution

We give you Solution with our eXPerience

IT Training – Software – Hardware – Technical Support
Networking Server System - Security Protection System
MRP & ERP Application

Surabaya – Jawa Timur – 081-357-661-007

Websites : www.xp-solution.com Email : xp.solution@yahoo.com



XP Solution
We give you Solution with our eXPerience

IT Training – Software – Hardware – Technical Support – Networking Server System
Security Protection System – MRP & ERP Application
Surabaya – Jawa Timur – 081-357-661-007
Websites : www.xp-solution.com Email : xp.solution@yahoo.com

Silabus Workshop MIKROTIK

“MEMBANGUN VPN SERVER & CLIENT Dengan Mikrotik”

**Untuk menghubungkan 2 Jaringan LAN
Yang beda Lokasi via Internet**

- 1. Introduction to Mikrotik.**
- 2. Introduction to Virtual Private Network (VPN).**
- 3. Teknik Konfigurasi Modem ADSL untuk VPN Dial Up.**
- 4. Teknik Konfigurasi Mikrotik Router.**
- 5. Teknik Konfigurasi VPN Server Mikrotik.**
- 6. Teknik Konfigurasi VPN Client (PC).**
- 7. Teknik Konfigurasi VPN Client Mikrotik.**
- 8. Teknis Backup & Recovery Mikrotik.**
- 9. User Manajemen & FTP Server.**

TRAINING INSTALLASI MIKROTIK PC ROUTER MEMBANGUN VPN MIKROTIK ANTAR JARINGAN LAN

BAB 1 PENGANTAR MIKROTIK PC ROUTER

Pendahuluan

Mikrotik RouterOS adalah salah satu Distro Linux yang didesain khusus untuk fungsi Routing System. Produk Mikrotik berupa **RouterBoard** yang berbentuk seperti Hardware Router pada umumnya dan berupa **RouterOS** yang di Install ke sebuah PC.

Kehandalan Mikrotik sudah terbukti dan tidak diragukan lagi, baik dari segi keamanan atau proteksinya maupun kemudahan dalam menggunakannya. Karena itulah hampir semua ISP bisa dipastikan mengenal dan menggunakan Mikrotik dalam layanan kepada pelanggan maupun dalam melakukan Manajemen Networknya serta Mikrotik mampu melejit sebagai Router masa depan yang sangat handal. **Jadi apapun ISP-nya, router dan bandwidth manajemen menggunakan Mikrotik.**

Pada Training / Workshop ini khusus mengangkat materi Bandwith Manajemen menggunakan **SPEEDY** karena layanan akses Internet saat ini di Indonesia yang paling murah dan paling banyak digunakan masyarakat maupun Corporate adalah **TELKOM SPEEDY**.

Lisensi Mikrotik

Sebelum melakukan instalasi hal yang perlu diperhatikan adalah level lisensi, perhatikan manual lisensi atau daftar list harga software. Level tertinggi adalah level 6 yang memiliki semua modul yang bisa kita gunakan secara maksimum. Perbedaan dari tiap lisensi adalah pada harga dan kelengkapan paket, informasi untuk hal ini dapat di tanyakan langsung ke keysupport@mikrotik.com atau dapat kita baca di website resminya www.mikrotik.com atau www.mikrotik.co.id.

Metode Implementasi Mikrotik

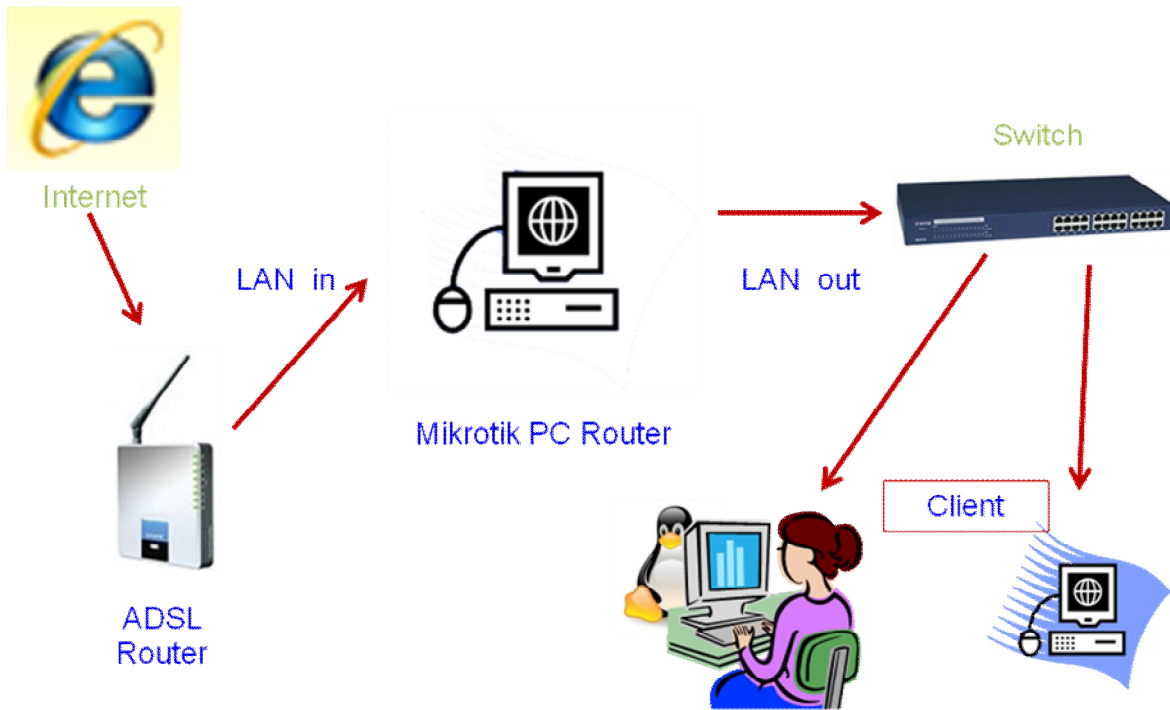
Implementasi Mikrotik ada 2, yaitu:

1. **Mikrotik PC Router**; menggunakan PC biasa dengan 2 LAN Card yang di install dengan Mikrotik RouterOS.
2. **Mikrotik RouterBoard**; menggunakan RouterBoard Mikrotik / produk jadi router yang sudah siap pakai (RB-450, RB-433, RB-750, RB-1000, dll).

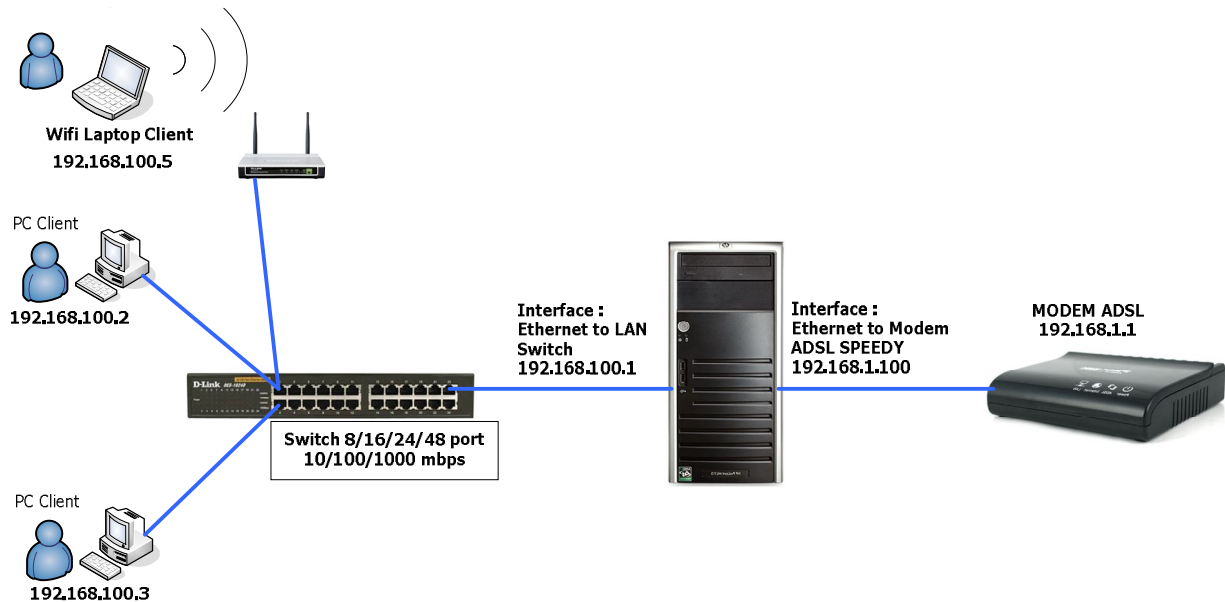


Mikrotik Basic Desain

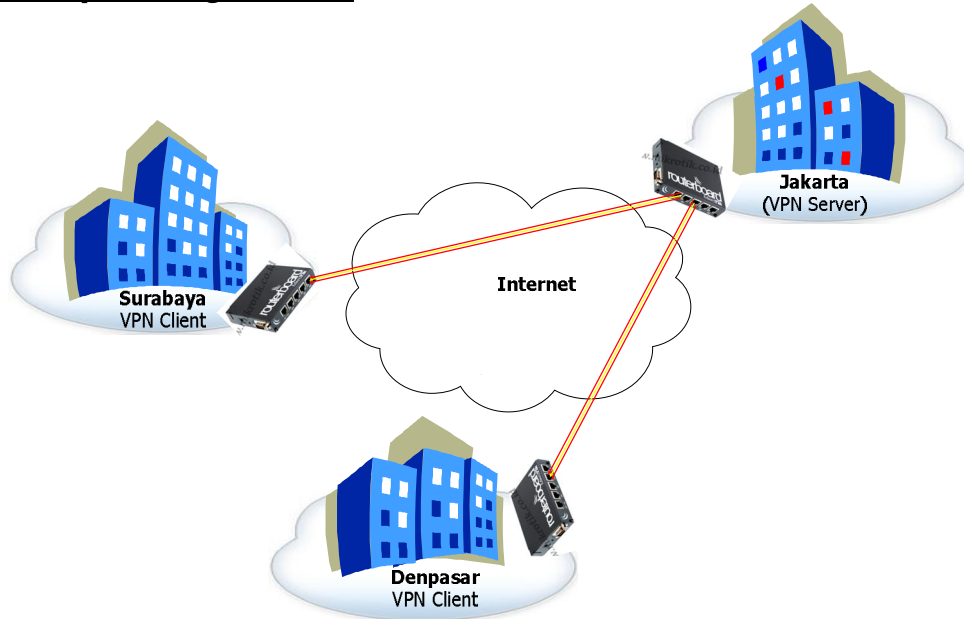
Berikut ini ada desain dasar / Basic Concept penggunaan Mikrotik RouterOS :



Atau gambar konsepnya seperti dibawah ini :



Basic Concept Design VPN :



HARDWARE untuk Mikrotik PC Router :

PC atau komputer yang dapat difungsikan sebagai Mikrotik PC Router adalah sebagai berikut :

1. Menggunakan processor minimal 100 MHz atau direkomendasikan menggunakan PC Built up atau PC rakitan minimal Pentium II – 400 Mhz.
2. Memori (RAM) minimal 64 Mb dan disarankan menggunakan 512 Mb atau 1 Gb, besar memory sangat berpengaruh pada, yang berpengaruh terhadap kemampuan kecepatan proses dari routing dan kapasitas Cache Proxy.
3. Media penyimpanan (Hard Drive) menggunakan sistem standar Kontroler IDE dan ATA. Sisa media penyimpanan kita adalah minimal sebesar 64 Mb. Sangat disarankan untuk mengalokasikan space penyimpanan yang besar, karena akan berpengaruh terhadap paket yang akan dipilih dan nantinya akan membantu sebagai cache pada saat menggunakan fungsi web proxy serta diperlukan jika Mikrotik kita fungsikan sebagai FTP Server.
4. CDRom atau DVD Jika instalasi menggunakan media CD, pastikan standar kontrolernya adalah ATA/ATAPI.
5. LAN Card atau Network Interface / ethernet tipe PCI.

Catatan :

- Direkomendasikan menggunakan **CPU Built Up** karena memiliki Power Supply yang kuat dan System Board yang handal, sebab Mikrotik yang kita buat ini nantinya akan difungsikan sebagai Router secara Dedicated 1 x 24 x 31.
- Setelah Mikrotik di Install dan dapat di akses via remote (Winbox / WebBox / Telnet), maka penggunaan Monitor sudah tidak diperlukan lagi.
- Menggunakan PCI LAN Card segala macam Merk dan Type dapat dikenali secara langsung oleh Mikrotik (Dlink DFE 528/538, TPLink, Realtek, Intel, Atheros, 3Com, SMC, dll).
- Onboard LAN sebaiknya tidak digunakan, karena hanya merk tertentu saja bisa terdeteksi otomatis oleh Mikrotik.
- Sebaiknya menggunakan harddisk **IDE**, karena harddisk SATA atau SCSI tidak terdeteksi oleh Mikrotik versi < 3. Kapasitas harddisk IDE hingga 160 GB IDE dapat berfungsi dengan baik.
- Dapat juga menggunakan Media Storage berupa **Compact Flash (CF)** dengan memanfaatkan peripheral **PCI CF to IDE**.

PAKET INSTALLASI MIKROTIK

Paket standar Mikrotik yang sudah kita install minimal akan berisi paket sistem (system package) saja. Termasuk dasar Routing IP dan Administrasi Router. Untuk menambah paket lainnya seperti wireless, OSPF, IP Telephony dan sebagainya silakan download terlebih dahulu paket-paketnya. Penting untuk diperhatikan adalah saat memilih paket tambahan yaitu harus sama versinya dengan RouterOS yang kita gunakan. Jika tidak maka paket tambahan tersebut tidak dapat diinstallasi. Mikrotik yang baru saja didownload dan di install adalah versi shareware yang hanya bisa dipergunakan sementara dan akan bisa dipergunakan lebih lanjut bila melakukan registrasi terlebih dahulu.

```

Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

[X] system          [X] lcd          [X] telephony
[X] ppp             [X] ntp           [X] ups
[X] dhcp            [X] radiolan       [X] user-manager
[X] advanced-tools  [X] routerboard    [X] web-proxy
[X] arlan            [X] routing         [X] webproxy-test
[X] calea           [X] routing-test    [X] wireless
[X] gps             [X] rstp-bridge-test [X] wireless-crd
[X] hotspot         [X] security        [X] wireless-legacy
[X] isdn            [X] synchronous

system (depends on nothing):
Main package with basic services and drivers

Do you want to keep old configuration? [y/n]:

```

Sebaiknya paket Installasi ini di Install semua dan jika ada paket yang tidak kita butuh dapat di REMOVE nantinya setelah Mikrotik kita konfigurasi lebih lanjut.

```

MikroTik Login: admin
Password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM  MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM     MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 2.9.51 (c) 1999-2008      http://www.mikrotik.com/

Terminal linux detected, using multiline input mode
[admin@MikroTik] > setup_

```

Tahapan Instalasi Awal Mikrotik telah selesai kita lakukan dan konfigurasi lebih lanjut dapat kita lakukan dengan perintah **/setup** melalui System Konsole ataupun kita lakukan melalui **Winbox**.

Tips yang dapat anda gunakan, khususnya bagi Newbie agar tidak bingung saat pertama kali melakukan Instalasi dalam menentukan **INTERFACE** dari LAN Card yang kita pasang di PC Router maka sebaiknya kita pasang 1 buah LAN Card saja lebih dulu. Dan selanjutnya kita lakukan /Setup dengan menentukan Interface LAN Card tersebut sebagai koneksi ke jaringan Local / LAN kita.

Setelah pada **fisik LAN Card pertama** tersebut itu kita **tandai** atau kita beri nama sebagai Interface **“LAN”** dan selanjutnya kita pasang **LAN Card** yang **kedua** untuk kita sambungkan ke **Modem ADSL**. LAN Card kedua ini kita tandai atau kita beri nama dengan **“SPEEDY”**. Penandaan dan Penamaan Interface LAN Card ini sangat membantu kita jika ada perubahan dalam penataan kabel UTP kita.

Jika pada saat pertama kali konfigurasi kita lakukan dari PC atau Laptop via LAN Card secara **direct** (langsung atau **Peer To Peer**), maka kita harus menggunakan **Cross Cable UTP**. Tapi jika koneksi dari Mikrotik ke Switch lalu kabel UTP ke PC atau Laptop maka kita gunakan **Stright Cable UTP**.

BAB 2

INTRODUCTION TO VPN

Virtual Private Network (VPN) adalah sebuah jaringan komputer yang berlapis-lapis (jaringan yang ada di atas jaringan komputer yang lain). Sifat pribadi VPN berarti bahwa traffic data VPN umumnya tidak terlihat, atau di enkapsulasi, lalu lintas jaringan yang mendasarinya. Demikian pula, lalu lintas dalam VPN muncul untuk jaringan yang mendasarinya hanya sebagai arus lalu lintas lain untuk diundangkan.

Dalam istilah yang lebih teknis, di link lapisan protokol jaringan virtual dikatakan terowongan melalui jaringan transportasi yang mendasarinya. Istilah VPN dapat digunakan untuk menggambarkan berbagai macam konfigurasi jaringan dan protokol. Dengan demikian, hal itu dapat menjadi rumit ketika mencoba generalisasi tentang karakteristik VPN. Beberapa yang lebih umum penggunaan VPN dijelaskan di bawah ini, bersama dengan lebih rinci tentang berbagai skema klasifikasi dan VPN model.

Common yang digunakan VPN

VPN dapat digunakan untuk mengamankan komunikasi melalui Internet publik. VPN sering dipasang oleh organisasi untuk menyediakan akses remote kepada jaringan organisasi yang aman, atau untuk menghubungkan dua lokasi jaringan bersama dengan menggunakan jaringan yang tidak aman untuk membawa lalu lintas.

VPN dapat digunakan untuk menyembunyikan alamat IP dari komputer-komputer di Internet, misalnya, untuk menjelajahi World Wide Web secara anonim atau untuk mengakses Pembatasan lokasi layanan, seperti Internet TV ataupun semacam IP Proxy.

Sebuah VPN tidak perlu eksplisit fitur keamanan seperti otentikasi atau enkripsi lalu lintas. Sebagai contoh, penyedia layanan jaringan VPN dapat digunakan untuk memisahkan lalu lintas dari beberapa pelanggan melalui jaringan yang mendasarinya.

Klasifikasi VPN

Teknologi VPN tidak mudah dibandingkan, karena berbagai protokol, terminologi dan pengaruh pemasaran yang telah ditetapkan mereka. Sebagai contoh, teknologi VPN dapat berbeda:

- * Dalam protokol yang mereka gunakan untuk terowongan lalu lintas melalui jaringan yang mendasari;
- * Dengan lokasi terowongan penghentian, seperti pelanggan atau penyedia jaringan tepi tepi;
- * Apakah mereka menawarkan untuk situs-situs atau konektivitas akses sites yang jauh;
- * Dalam tingkat keamanan yang diberikan;
- * Oleh lapisan OSI yang mereka hadir untuk jaringan penghubung, seperti rangkaian Layer 2 atau Layer 3 konektivitas jaringan.

Beberapa skema klasifikasi dibahas dalam bagian berikut :

➤ Secure VPN vs Trusted VPN

Kelompok industri '**Virtual Private Networking Konsorsium**' telah menetapkan dua jenis klasifikasi **VPN Aman (Secure VPN)** dan **VPN Terpercaya (Trusted VPN)**. Termasuk anggota konsorsium seperti Microsoft, Cisco, Juniper dan banyak lainnya.

Secure VPN secara eksplisit menyediakan mekanisme autentikasi terowongan terowongan endpoint selama setup, dan enkripsi lalu lintas dalam perjalanan. Aman VPN sering digunakan untuk melindungi lalu lintas ketika menggunakan Internet sebagai tulang punggung yang mendasar, tapi juga dapat digunakan dalam lingkungan ketika tingkat keamanan jaringan yang mendasarinya berbeda dari lalu lintas dalam VPN.

Secure VPN dapat diimplementasikan oleh organisasi yang ingin menyediakan fasilitas akses remote kepada karyawan atau dengan organisasi-organisasi yang ingin menghubungkan beberapa jaringan bersama-sama dengan aman menggunakan Internet untuk membawa lalu lintas. Yang umum digunakan untuk VPN aman

dalam akses remote skenario, di mana perangkat lunak klien VPN pada sebuah sistem pengguna akhir digunakan untuk menyambung ke jaringan kantor remote dengan aman. Protokol Secure VPN mencakup IPSec, SSL atau PPTP (dengan MPPE / Microsoft Point to Point Encryption).

Trusted VPN biasanya dibuat oleh operator dan organisasi-organisasi besar dan digunakan untuk segmentasi lalu lintas pada jaringan inti yang besar. Mereka sering menyediakan layanan kualitas dan jaminan carrier-grade lainnya fitur. VPN dipercaya bisa diimplementasikan oleh operator jaringan yang ingin multipleks beberapa sambungan pelanggan secara transparan melalui jaringan inti yang sudah ada atau dengan organisasi-organisasi besar yang ingin memisahkan arus lalu lintas dari satu sama lain dalam jaringan. Trusted VPN protokol termasuk MPLS, ATM atau Frame Relay.

Secure VPN dan **Trusted VPN** berbeda dari dalam bahwa mereka tidak menyediakan fitur keamanan seperti kerahasiaan data melalui enkripsi. VPN aman akan tetapi tidak menawarkan tingkat kontrol aliran data yang terpercaya VPN dapat memberikan jaminan seperti bandwidth atau routing.

Dari perspektif pelanggan, terpercaya VPN dapat bertindak sebagai kawat logis menghubungkan dua jaringan. Pembawa yang mendasari jaringan tidak dapat dilihat oleh pelanggan, dan tidak ada pelanggan menyadari kehadiran pelanggan lain melintasi tulang punggung yang sama. Gangguan antara pelanggan, atau gangguan pada tulang punggung itu sendiri, tidak mungkin dilakukan dari dalam VPN yang terpercaya.

Beberapa penyedia layanan Internet yang dikelola menawarkan layanan VPN untuk pelanggan bisnis yang menginginkan keamanan dan kenyamanan VPN tetapi memilih untuk tidak melakukan pemberian server VPN sendiri. Dikelola aman lagi VPN adalah campuran dari dua model VPN utama, dan merupakan solusi keamanan yang dikontrak dapat mencapai ke host. Selain menyediakan pekerja dengan secure remote akses ke jaringan internal perusahaan, keamanan lainnya dan jasa manajemen kadang-kadang dimasukkan sebagai bagian dari paket. Contoh-contoh termasuk membuat anti-virus dan anti-spyware program diperbaharui di setiap menghubungkan komputer atau perangkat lunak tertentu memastikan patch sambungan diinstal sebelum diperbolehkan.

Kategorisasi berdasarkan hubungan administratif user

The Internet Engineering Task Force (IETF) telah dikategorikan berbagai VPN, beberapa di antaranya, seperti Virtual LAN (VLAN) adalah tanggung jawab standardisasi organisasi lain, seperti Institute of Electrical and Electronics Engineers (IEEE) Proyek 802, PI 802,1 (arsitektur).

Awalnya, Wide Area Network (WAN) link dari penyedia layanan telekomunikasi node jaringan yang saling berhubungan dalam satu perusahaan. Dengan munculnya LAN, perusahaan bisa interkoneksi node mereka dengan link yang mereka miliki. Sedangkan yang asli yang digunakan WAN jalur khusus dan lapisan 2 multiplexing layanan seperti Frame Relay, berbasis IP lapisan 3 jaringan, seperti ARPANET, internet, militer jaringan IP (NIPRNET, SIPRNET, JWICS, dll), menjadi media interkoneksi umum. VPN mulai didefinisikan melalui jaringan IP. Pihak militer sendiri jaringan mungkin dilaksanakan sebagai VPN pada peralatan transmisi yang umum, tetapi dengan enkripsi terpisah dan mungkin router.

Ini menjadi pertama berguna untuk membedakan antara berbagai jenis IP VPN berdasarkan pada hubungan administratif (bukan teknologi) interkoneksi node. Begitu hubungan itu didefinisikan, teknologi yang berbeda dapat digunakan, tergantung pada persyaratan seperti keamanan dan kualitas layanan.

Ketika sebuah perusahaan interkoneksi satu set node, semua di bawah kontrol administratif, melalui sebuah LAN, yang disebut sebagai intranet. Ketika saling berhubungan beberapa node berada di bawah kewenangan administratif tetapi tersembunyi dari internet publik, hasil set node disebut extranet. Seorang pengguna baik organisasi dapat mengelola intranet dan extranet itu sendiri, atau menegosiasikan pelayanan sebagai kontraksi (dan biasanya disesuaikan) penawaran dari penyedia layanan IP. Dalam kasus terakhir, organisasi pengguna lapisan 3 kontrak untuk layanan - sebanyak mungkin lapisan 1 kontrak untuk layanan seperti garis khusus, atau lapisan 2 multiplexing layanan seperti frame relay.

Dokumen IETF membedakan antara penyedia-ditetapkan dan diatur pelanggan VPN. Hanya sebagai saling berhubungan dan mengatur penyedia layanan dapat menyediakan layanan WAN konvensional, jadi satu operator selular dapat pasokan ditetapkan penyedia-VPN (PPVPNs), mempresentasikan satu titik yang sama - of-kontak ke organisasi pengguna.

Internet Protocol Tunnels

Tunnelling protocol

Beberapa pelanggan dikelola virtual jaringan mungkin tidak menggunakan enkripsi untuk melindungi isi data. Jenis jaringan overlay tidak rapi sesuai dalam kategorisasi aman atau terpercaya. Salah satu contoh jaringan lapisan bisa menjadi GRE terowongan, menetapkan di antara dua host. Tunnelling ini akan tetap menjadi suatu bentuk jaringan pribadi virtual namun bukan aman atau VPN yang terpercaya.

Contoh native teks-jelas termasuk protokol tunnelling GRE, L2TP dan PPTP (ketika MPPE tidak digunakan).

Security Mechanisms / Mekanisme Keamanan

Secure VPN menggunakan **kriptografi protokol tunneling** dimaksudkan untuk menyediakan kerahasiaan (pemblokiran mencegah dan dengan demikian paket sniffing), pengirim otentikasi (pemblokiran identitas spoofing), dan pesan integritas (pemblokiran pesan perubahan) untuk mencapai privasi.

Secure VPN Protokol adalah sebagai berikut:

- * IP Security (Internet Protocol Security) - Sebuah standar protokol keamanan berbasis awalnya dikembangkan untuk IPv6, di mana dukungan adalah keharusan, tetapi juga digunakan secara luas dengan IPv4.
- * Transport Layer Security (SSL / TLS) digunakan baik untuk tunneling seluruh lalu lintas jaringan (SSL VPN), seperti dalam OpenVPN proyek, atau untuk mengamankan sambungan individu. SSL telah menjadi fondasi oleh sejumlah vendor untuk menyediakan kemampuan akses remote VPN. Keuntungan praktis dari suatu SSL VPN adalah bahwa hal itu dapat diakses dari lokasi yang membatasi akses eksternal untuk SSL-based e-commerce website tanpa IP Security implementasi. SSL VPN berbasis mungkin rentan terhadap serangan Denial of Service (DOS) terhadap koneksi TCP karena mereka secara inheren tidak terautentikasi terakhir.
- * DTLS, digunakan oleh Cisco untuk generasi berikutnya disebut produk VPN AnyConnect Cisco VPN. DTLS memecahkan masalah-masalah yang ditemukan saat TCP melalui TCP tunneling seperti halnya dengan SSL / TLS.
- * Secure Socket Tunneling Protocol (SSTP) oleh Microsoft yang diperkenalkan pada Windows Server 2008 dan Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or L2TP traffic through an SSL 3.0 channel. Terowongan SSTP Point-to-Point Protocol (PPP) atau L2TP lalu lintas melalui saluran SSL 3,0 .
- * MPVPN (Multi Path Virtual Private Network). Pengembangan Sistem Ragula Perusahaan yang terdaftar memiliki merek dagang "MPVPN". [5]
- * SSH VPN - OpenSSH menawarkan VPN tunneling untuk mengamankan koneksi remote ke jaringan (atau antar-network link). Fitur ini (opsi-w) tidak boleh dikacaukan dengan port forwarding (option-L). OpenSSH server menyediakan jumlah terbatas bersamaan terowongan dan fitur VPN itu sendiri tidak mendukung otentikasi pribadi.

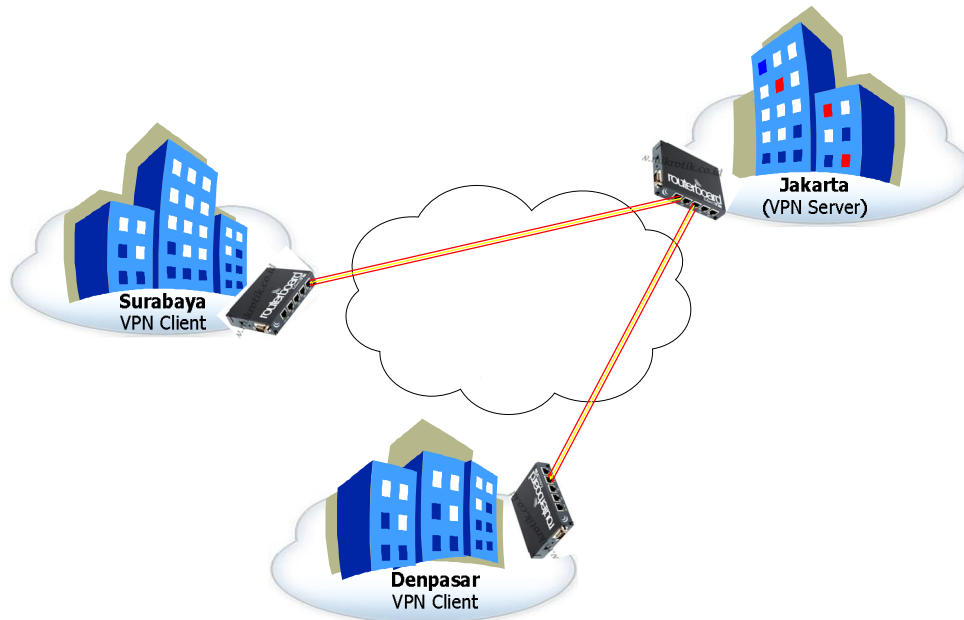
Authentication / Otentikasi

Tunnel endpoints diharuskan untuk mengotentikasi diri sebelum terowongan aman VPN dapat dibangun. Terowongan diciptakan pengguna akhir, seperti akses remote VPN dapat menggunakan sandi, biometrik, dua-faktor otentikasi atau kriptografi metode. Jaringan-untuk-jaringan terowongan, password atau sertifikat digital sering digunakan, sebagai kunci harus disimpan secara permanen dan tidak memerlukan campur tangan untuk terowongan yang akan didirikan secara otomatis.

Model Jaringan VPN (PPTP)

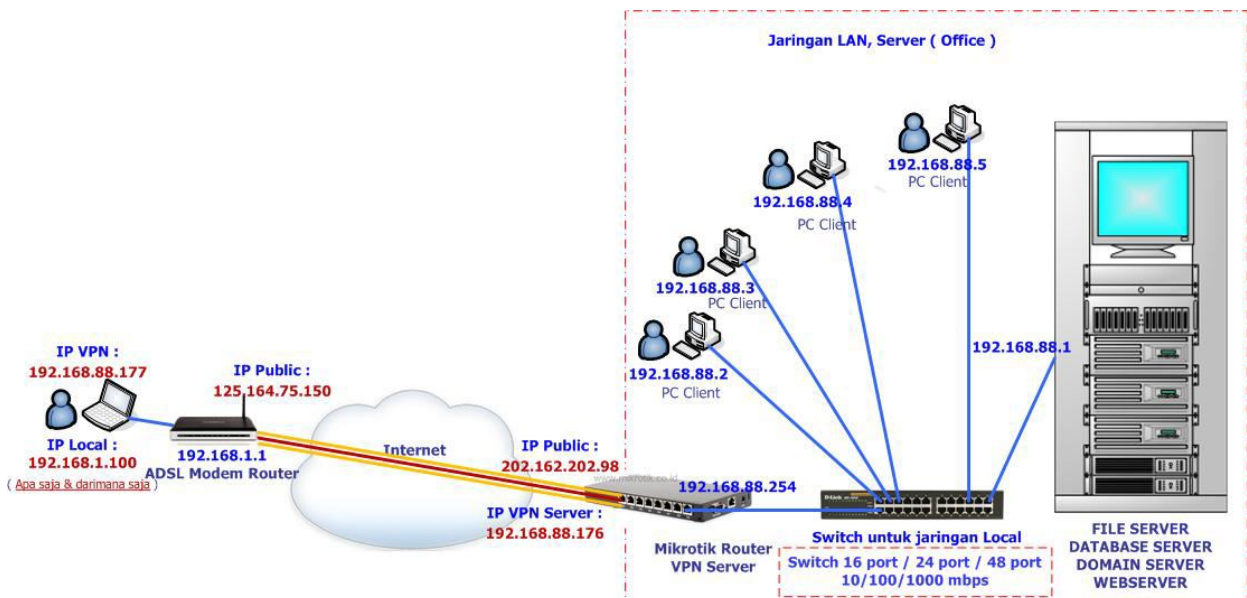
A. VPN --> LAN to LAN

Adalah Teknik Komunikasi VPN yang menghubungkan 2 jaringan LAN atau lebih via internet. Sehingga dengan VPN ini kedua jaringan LAN seolah-olah berada dalam 1 tempat atau 1 jaringan LAN yang sama.



B. VPN --> PC Client to LAN

Adalah Teknik Komunikasi VPN yang menghubungkan sebuah PC atau Laptop Client ke jaringan LAN via internet. Sehingga kita dapat mengakses semua resource yang ada dalam jaringan atau server di kantor. Sehingga dengan VPN ini seolah-olah PC / Laptop Client berada dalam 1 tempat atau 1 jaringan LAN yang sama dengan resource Server tersebut.



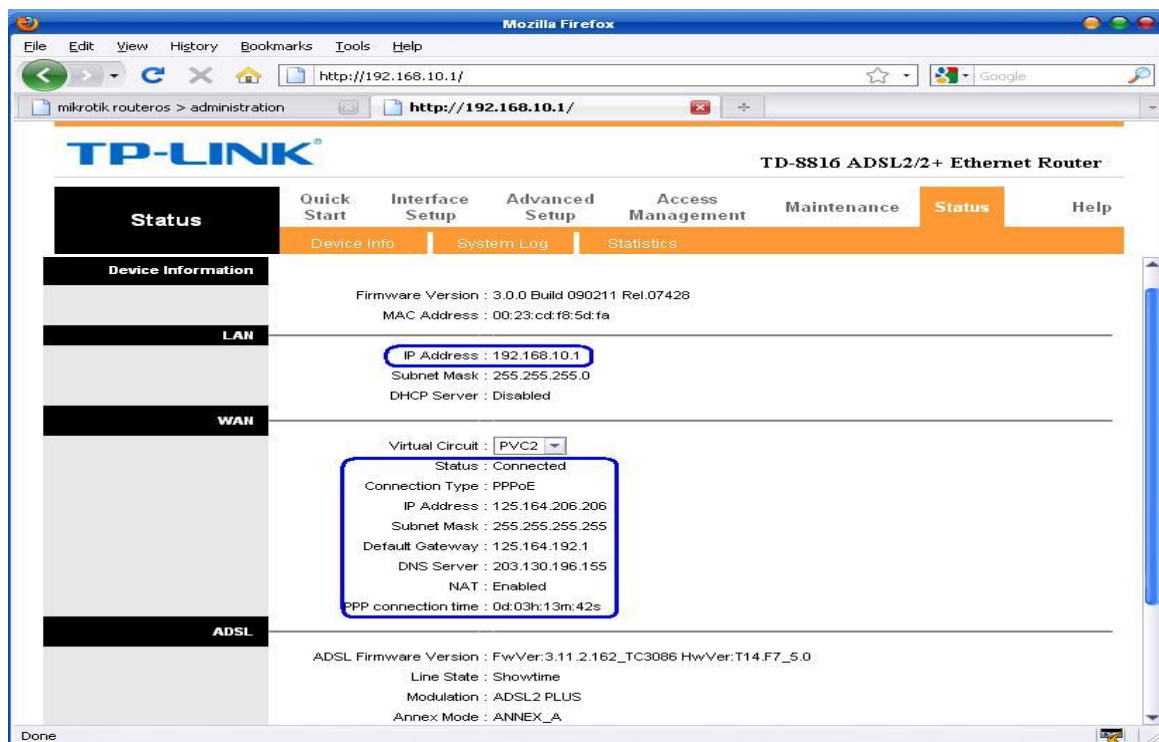
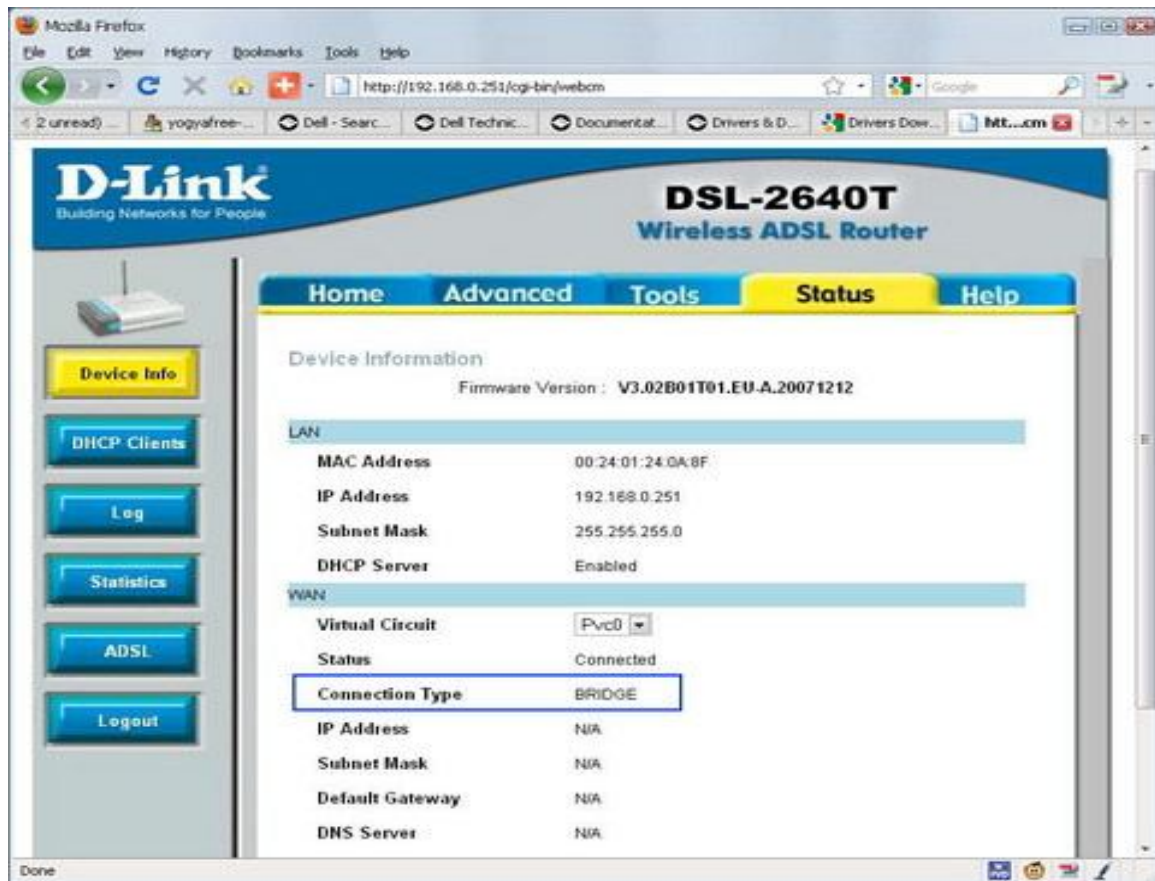
BAB 3

TEKNIK KONFIGURASI MODEM ADSL UNTUK VPN

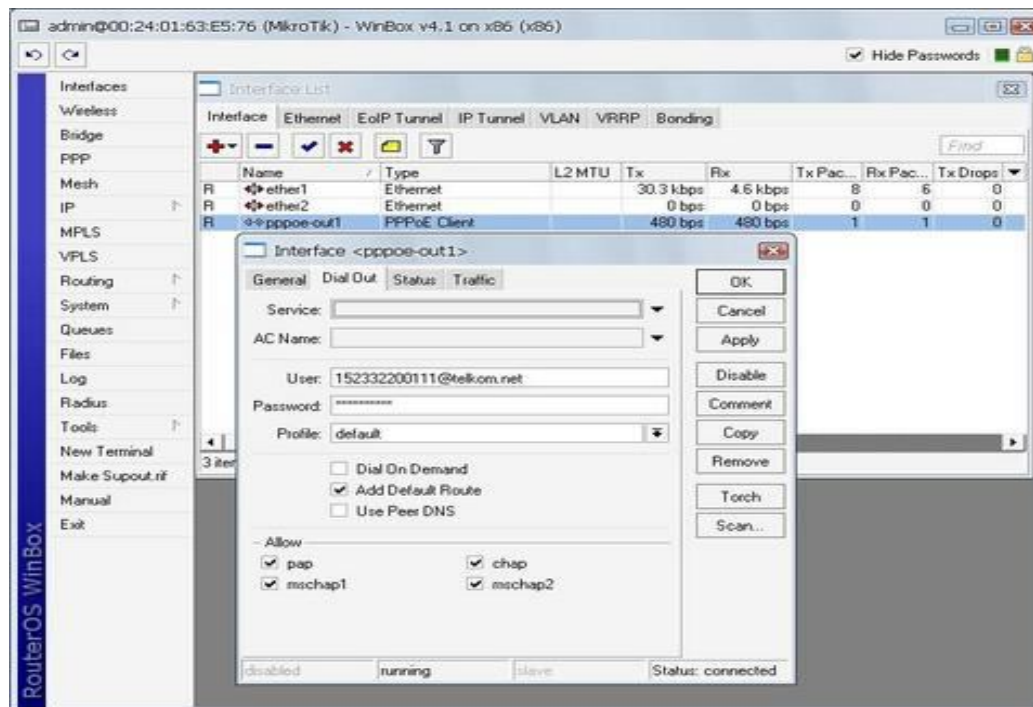
Supaya kita dapat melakukan konfigurasi Mikrotik sebagai VPN Server maka Mikrotik kita tersebut harus kita setting dengan IP Public. Jika kita menggunakan koneksi dari ISP baik menggunakan Cabling Routing System maupun menggunakan Wireless Routing System maka IP Public dapat di langsung di setting pada Interface WAN / interface yang di koneksikan ke Gateway ISP.

Namun jika kita menggunakan ISP Speedy, maka kita harus melakukan setting pada Modem ADSL kita menjadi BRIDGE. Tidak semua modem support fitur Bridge, jadi kita harus memilih Modem ADSL yang tepat agar kita dapat memanfaatkan koneksi dari Speedy ini sehingga dapat kita fungsikan sebagai VPN Server – Client.





Selanjutnya kita harus setting pada Mikrotik kita dengan menambahkan Interface PPPoE Dial Out. Setelah Create interface ini berhasil, maka Mikrotik kita akan memperoleh IP Public dari Telkom Speedy. Berikutnya kita dapat melakukan setting Mikrotik VPN Server / VPN Client.



BAB 4

MEMBUAT VPN CLIENT (PC)

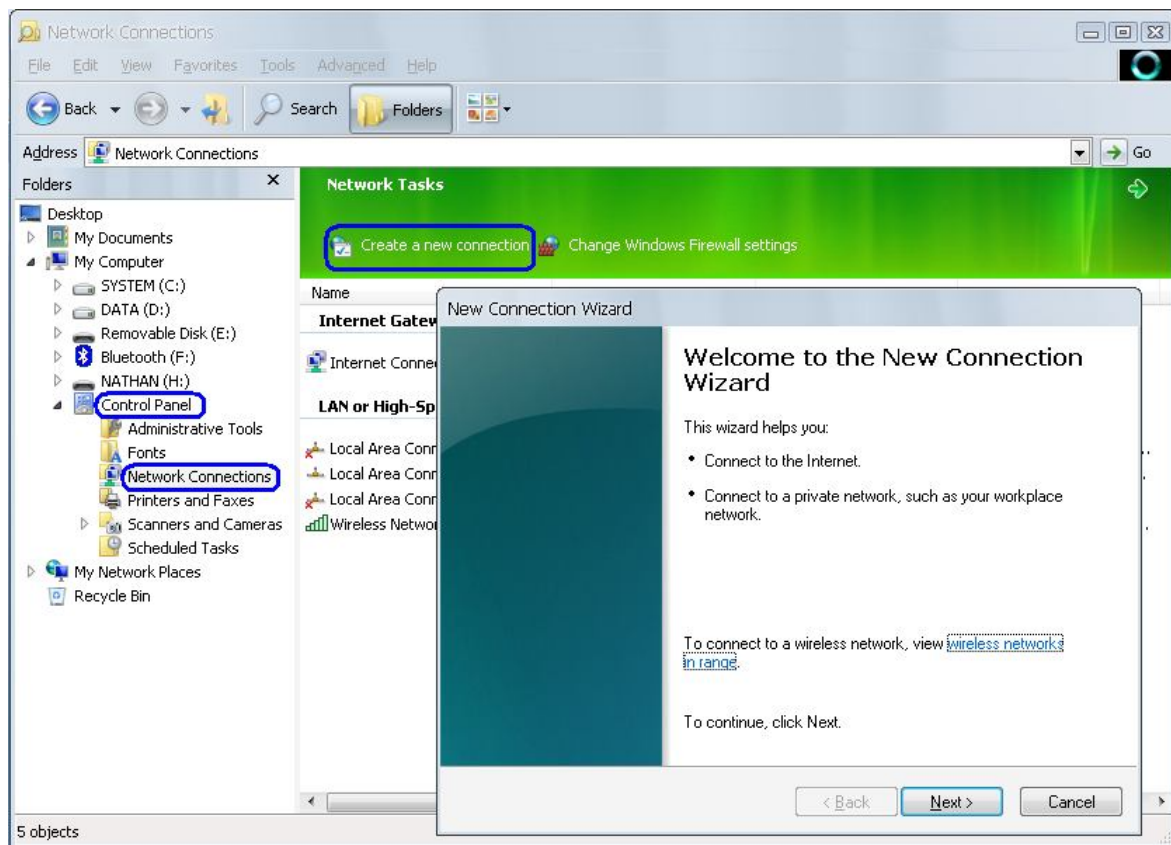
VPN / Virtual Private Network adalah jaringan pribadi yang aman (*tunneling encryption data*) melalui jalur internet (*public*) sehingga kita dapat menggunakan Resource yang ada diseluruh jaringan **LAN** kita layaknya kita berada dalam jaringan LAN tersebut secara langsung.

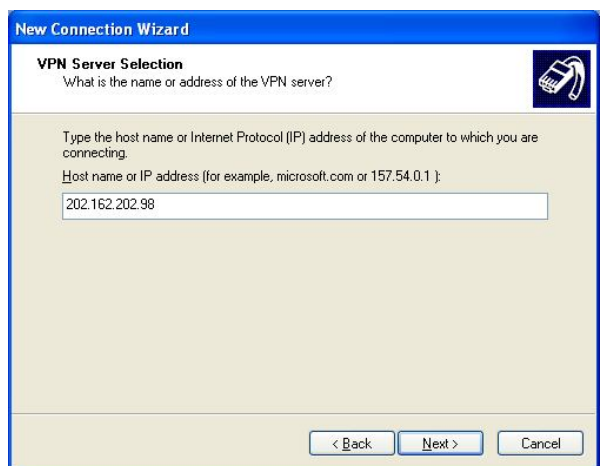
Dalam membuat setting Mikrotik VPN Client, tahapan-tahapan yang akan kita lakukan, yaitu :

1. **Step VPN Client Configuration.**
2. **Step Dialing VPN / Connecting VPN.**
3. **Step Ping Test & Working.**

Berikut ini Step by Step membuat **VPN Client** di PC / Laptop kita secara lengkap :

- Dari menu "**Control Panel -> Network**", buat satu koneksi baru.
- Pilih Create koneksi VPN (lihat step by step dibawah ini).



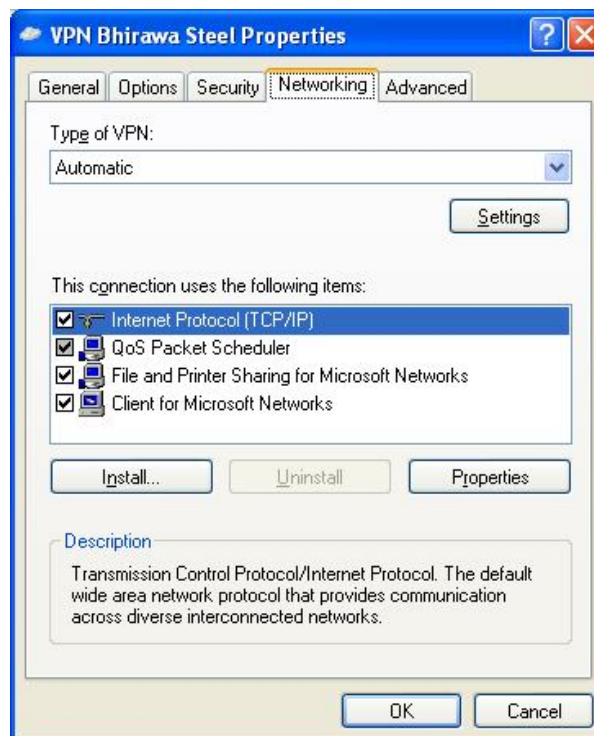
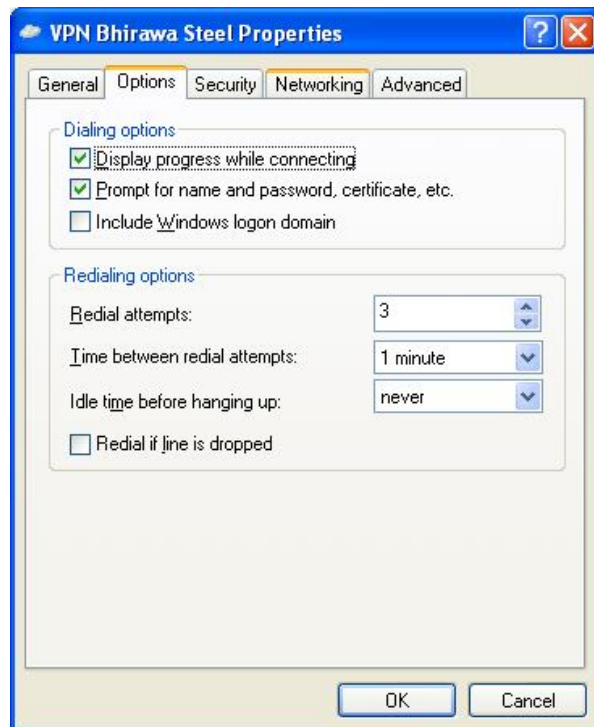
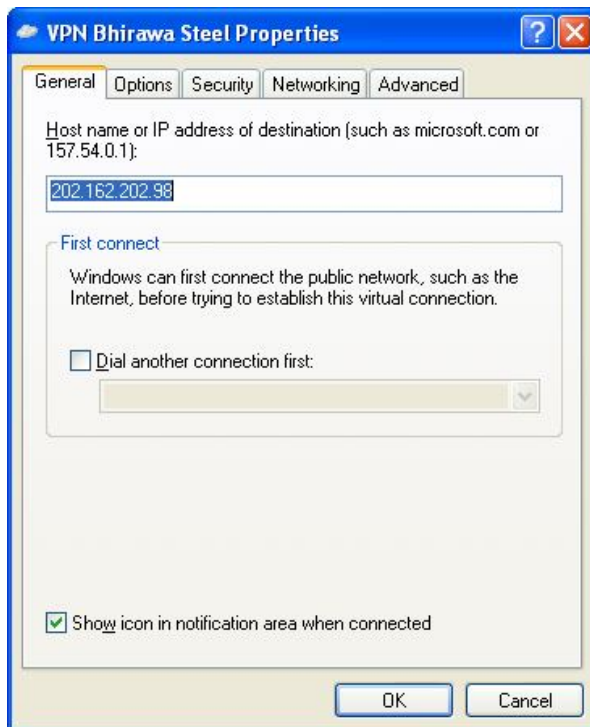


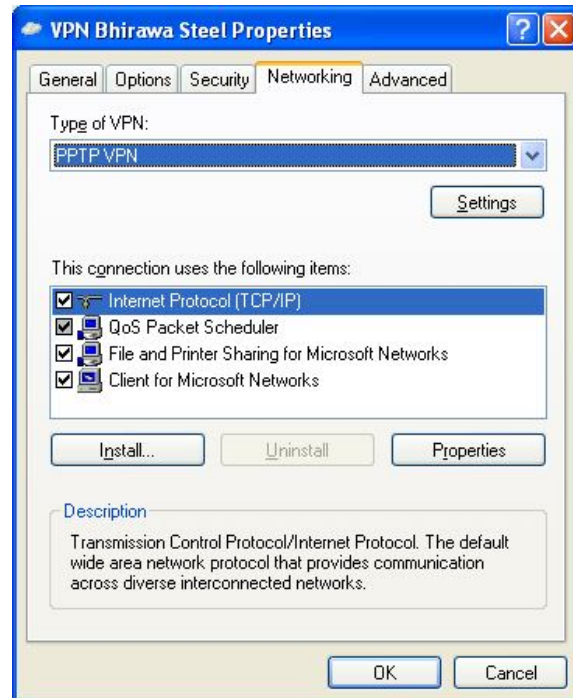
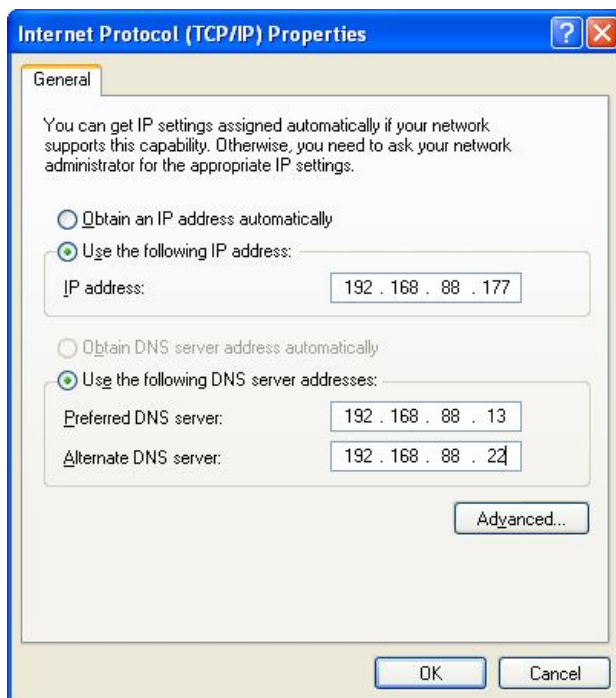


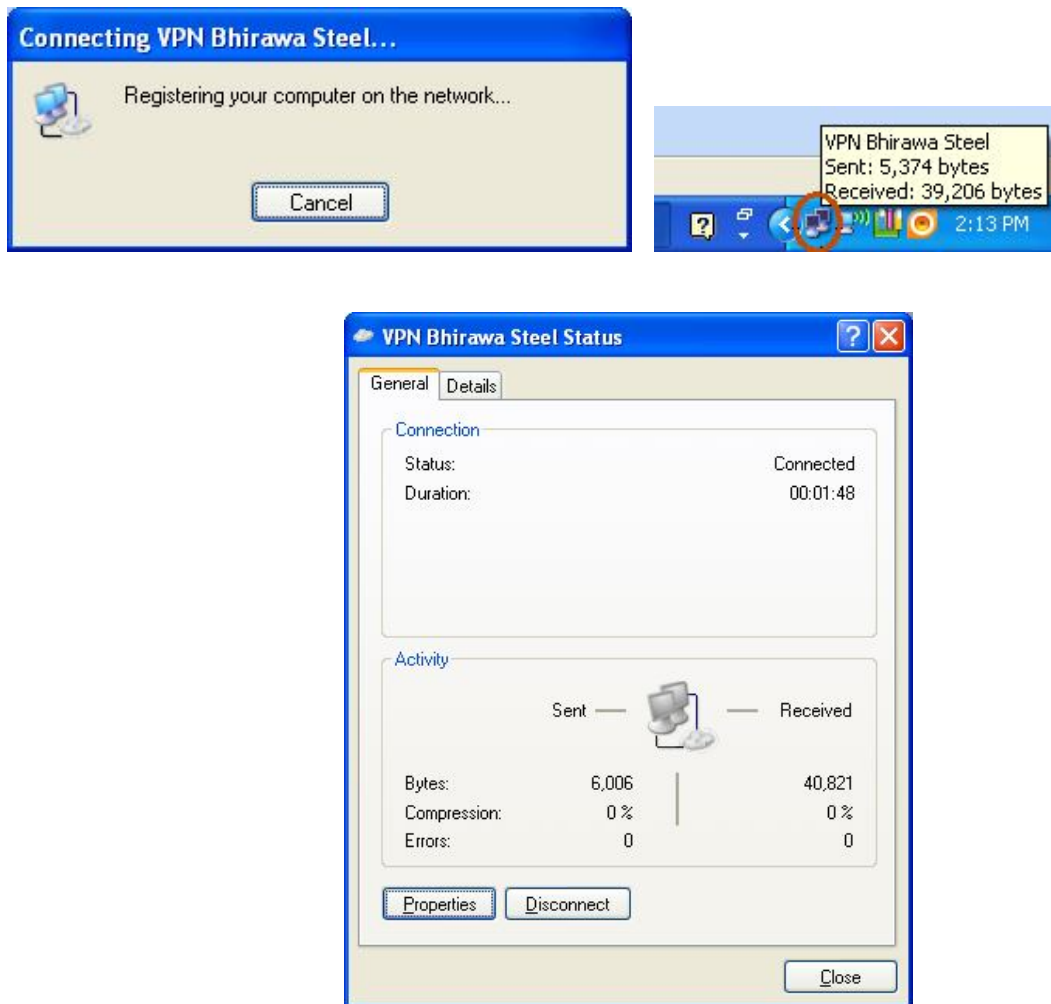
Username : vpn01
Password : nathan01

Username : vpn02
Password : nathan02

Username : vpn10
Password : nathan10

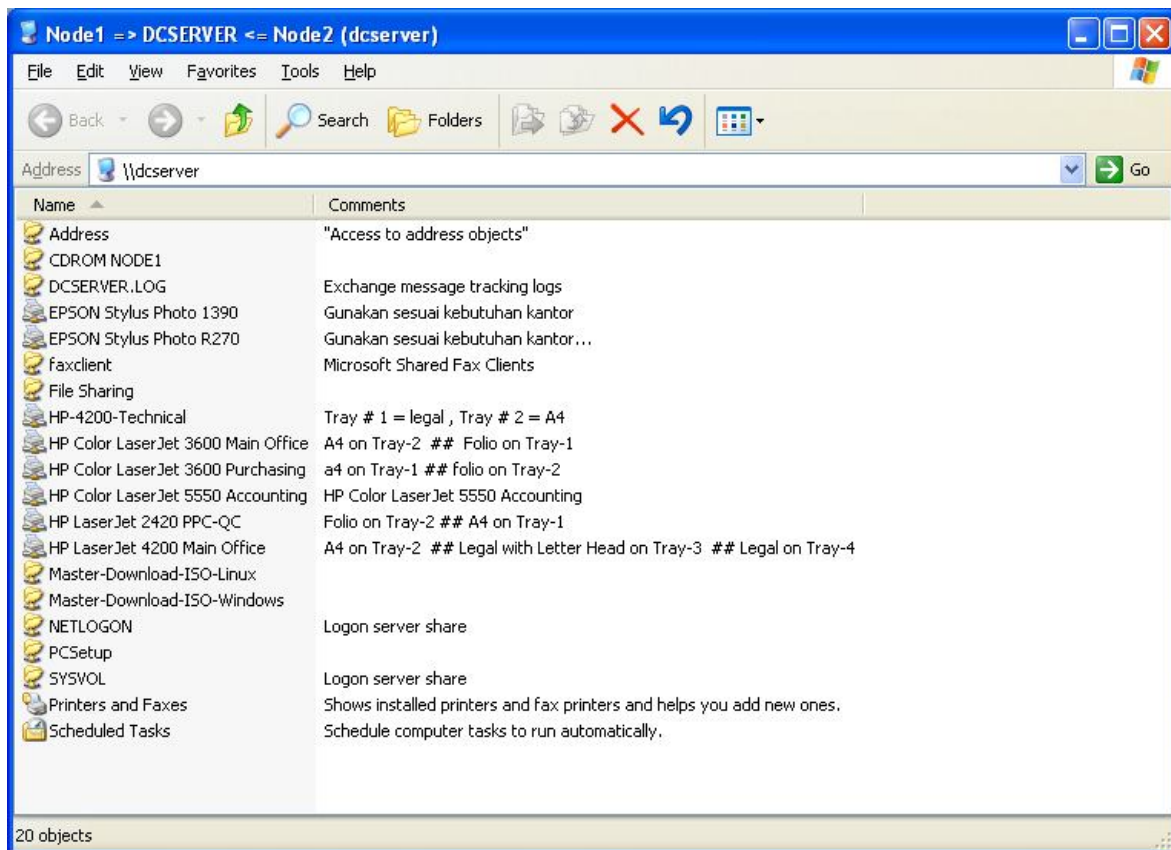
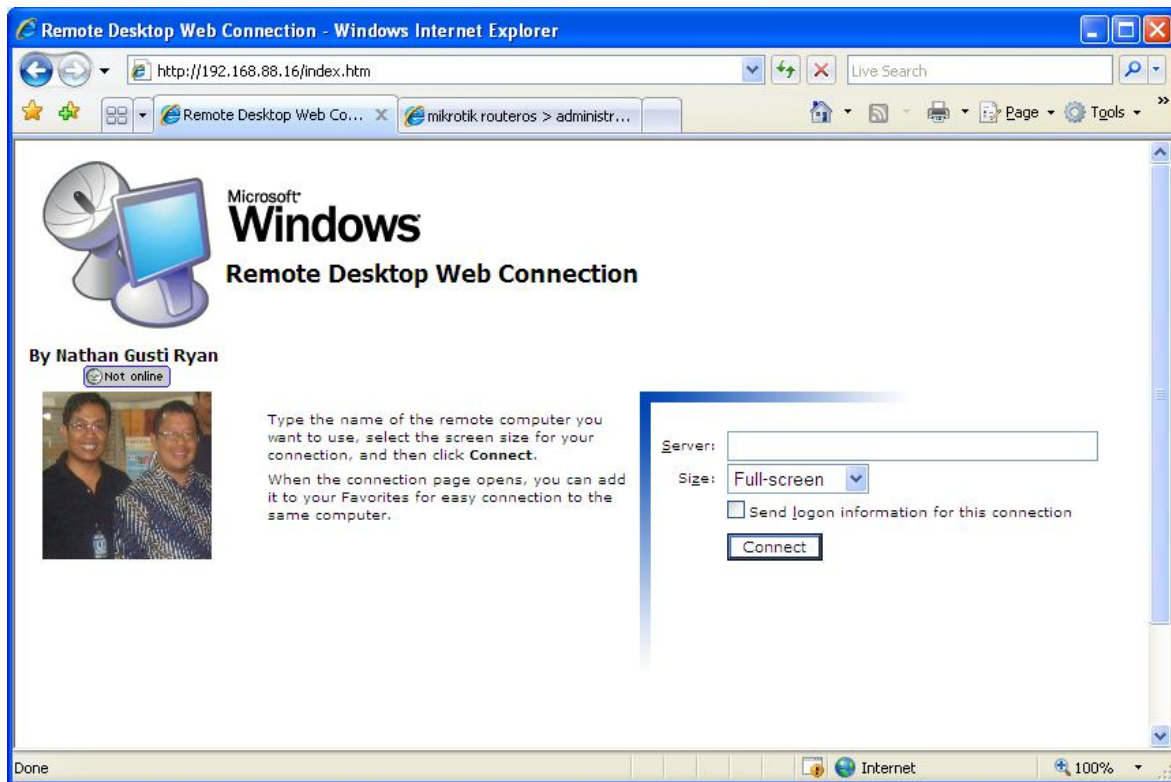






Setelah VPN Connection ini berjalan, maka selanjutnya kita dapat menggunakan Resource yang ada diseluruh jaringan LAN kita layaknya kita berada dalam jaringan LAN tersebut secara langsung. Disini saya sudah mencoba berbagai Resource atau fasilitas yang ada dalam jaringan lokal seperti : **Remote Desktop**, **Akses Peripheral yang Web Base akses** (Printer Network, Switch, Router, Modem ADSL, Mikrotik, Web Server, dll), **Akses Fileserver**, **Akses Email Server** (Microsoft Outlook), **Akses Domain Server**, dll.





BAB 4

KONFIGURASI MIKROTIK ROUTER-OS Menggunakan VMWare Workstation

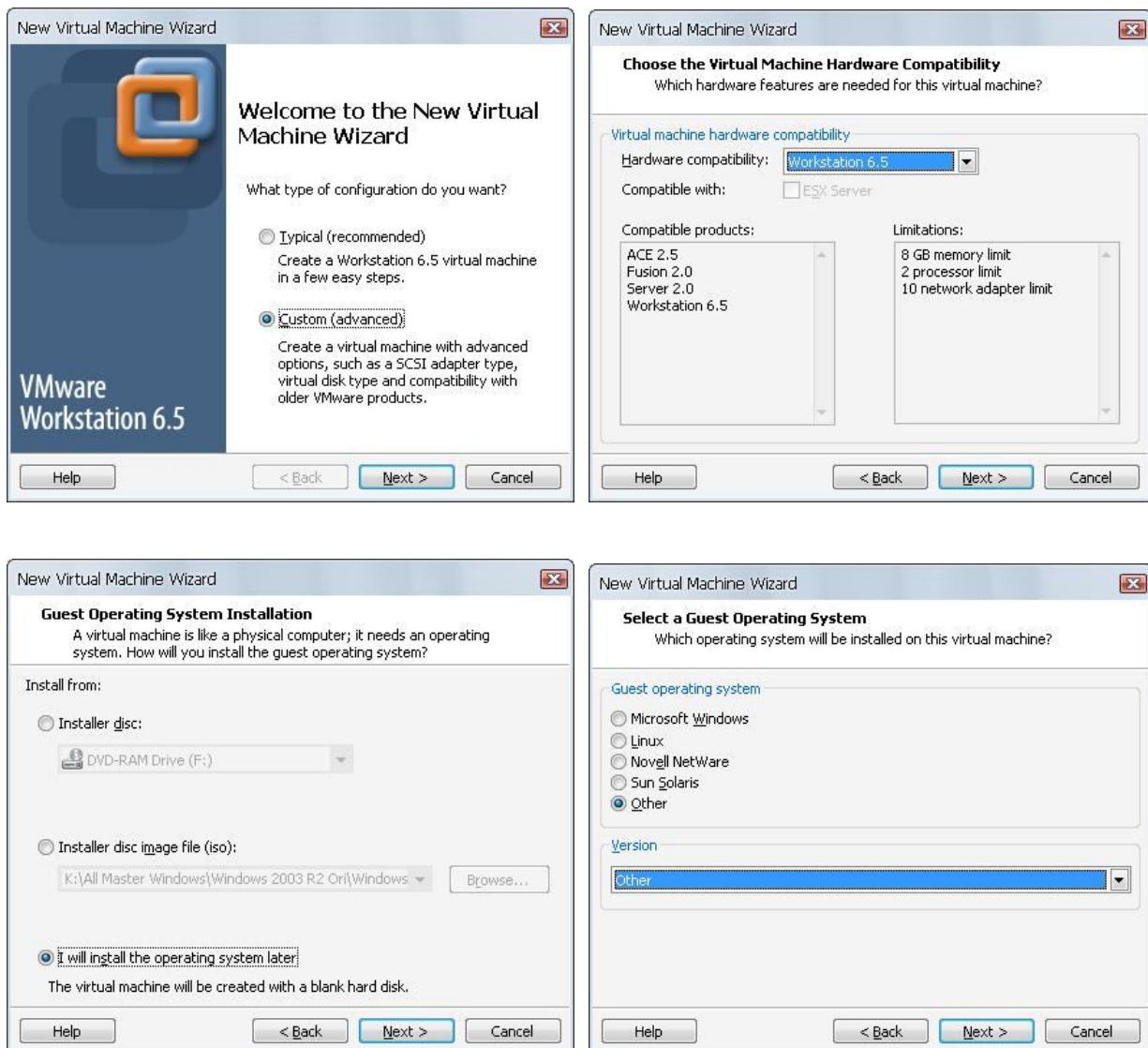
Pendahuluan VMWare Workstation

Mikrotik RouterOS adalah salah satu Distro Linux yang didesain khusus untuk fungsi Routing System. Produk Mikrotik berupa **RouterBoard** yang berbentuk seperti Hardware Router pada umumnya dan berupa **RouterOS** yang di Install ke sebuah PC.

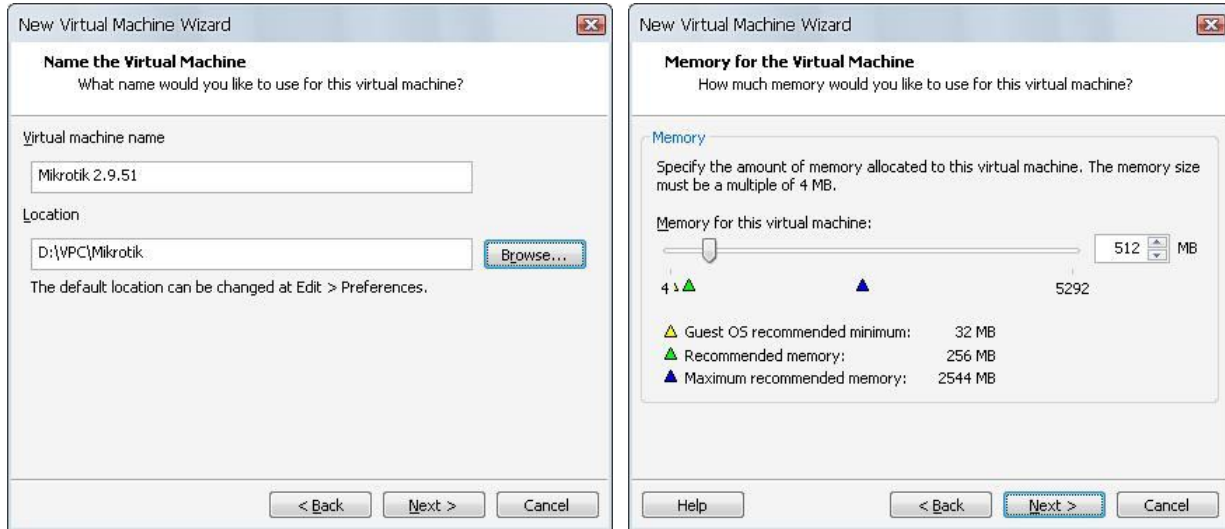
Pada materi Training ini, kita gunakan Metode menggunakan **VMWare Workstation** agar setiap peserta Training dapat memiliki, mengkonfigurasi dan menggunakan Mikrotik masing - masing. Virtual PC ini selain digunakan untuk Training juga dapat digunakan pada pemakain Mikrotik sehari - hari.

Langkah pertama yang kita lakukan adalah membuat sebuah Virtual PC dengan **VMWare 6.5** ataupun **Microsoft Virtual PC** yang sudah dinyatakan **Free License** oleh **Microsoft**.

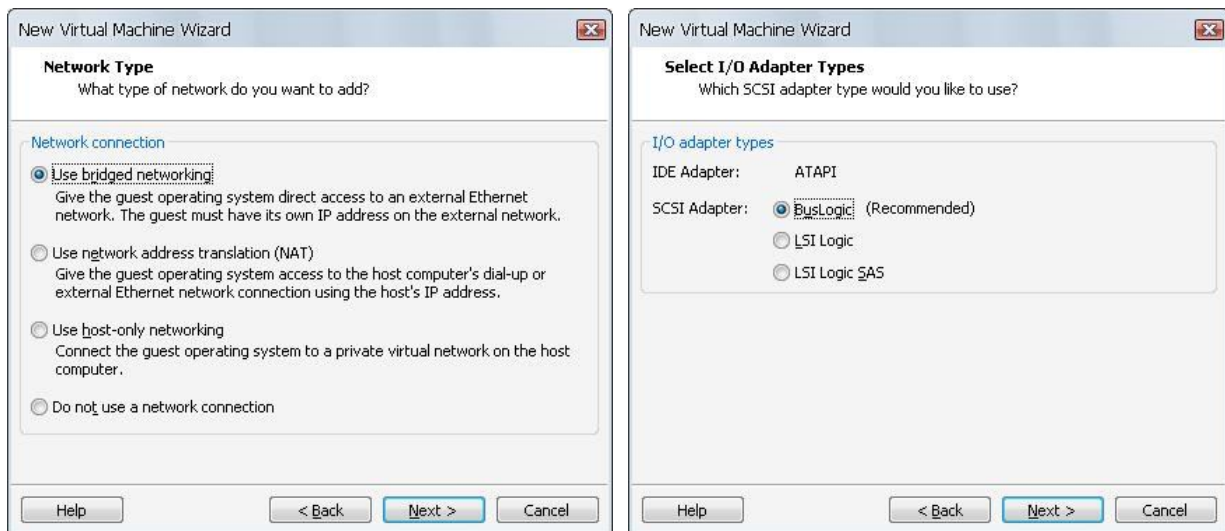
Ikuti Step by Step Wizard-nya seperti pada gambar capture ini :

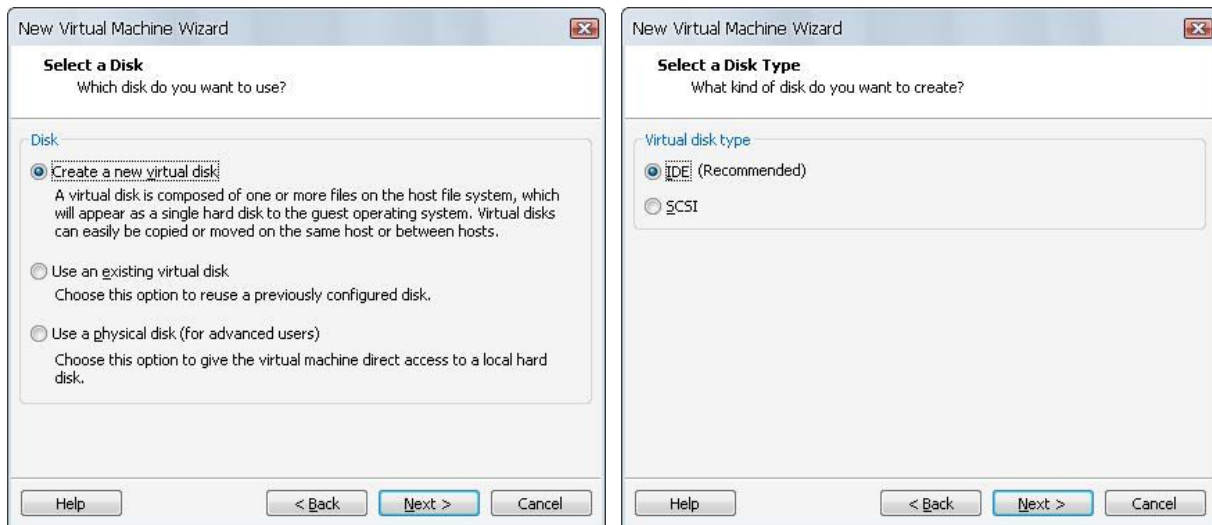


Jika Real PC anda menggunakan memory 512 GB dengan OS Windows XP, maka anda dapat gunakan Memory untuk Virtual PC sebesar 64 MB atau 128 MB. Tapi jika Real PC kita menggunakan

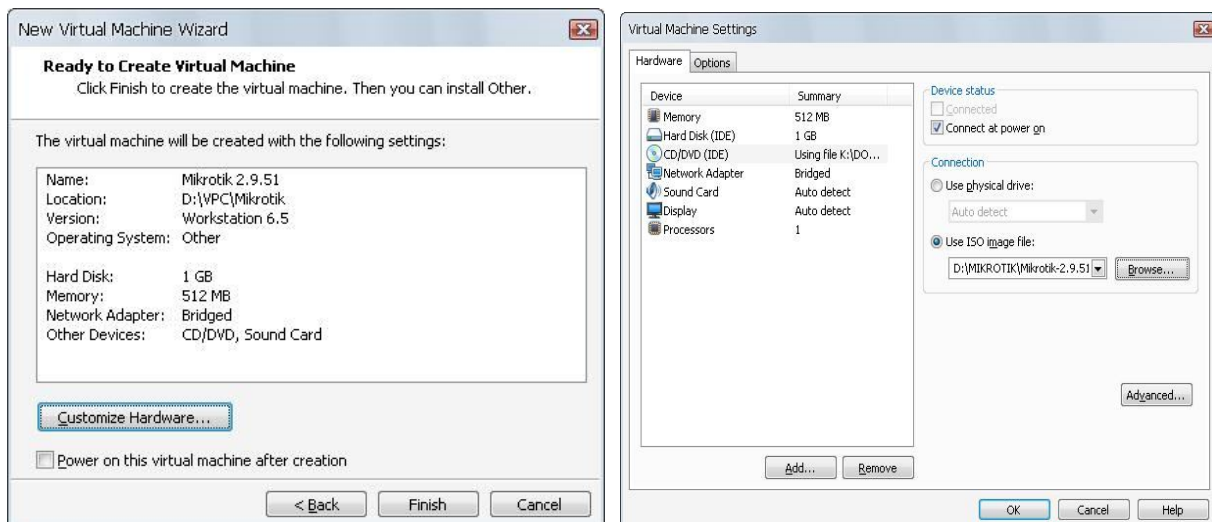
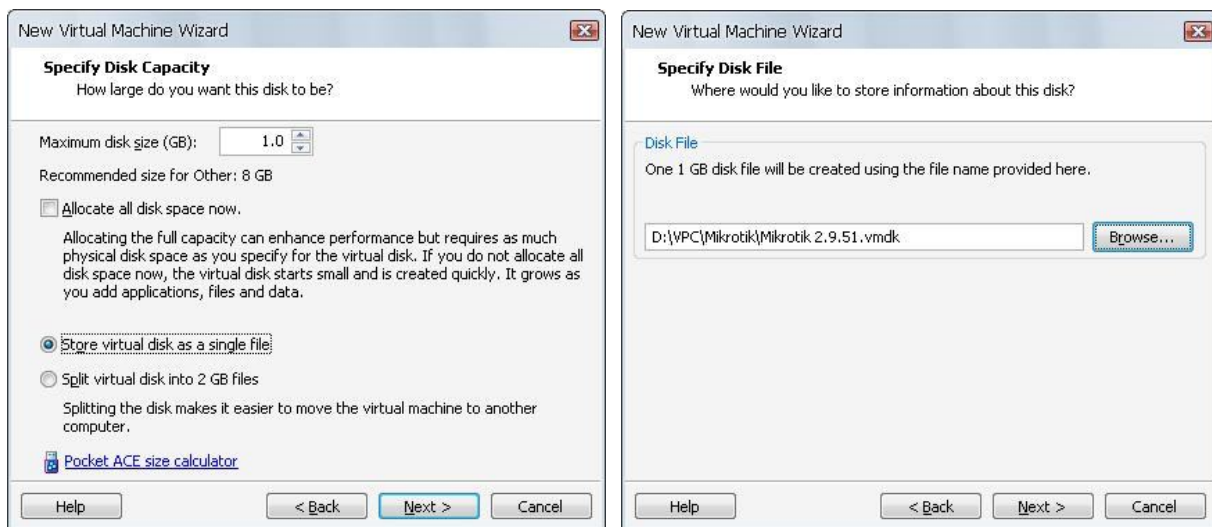


Pada Wizard selanjutnya kita buat 1 buah Network Adapter, pilihlah mode “**BRIDGE Networking**”. Sedangkan I/O Adapter kita setting default.

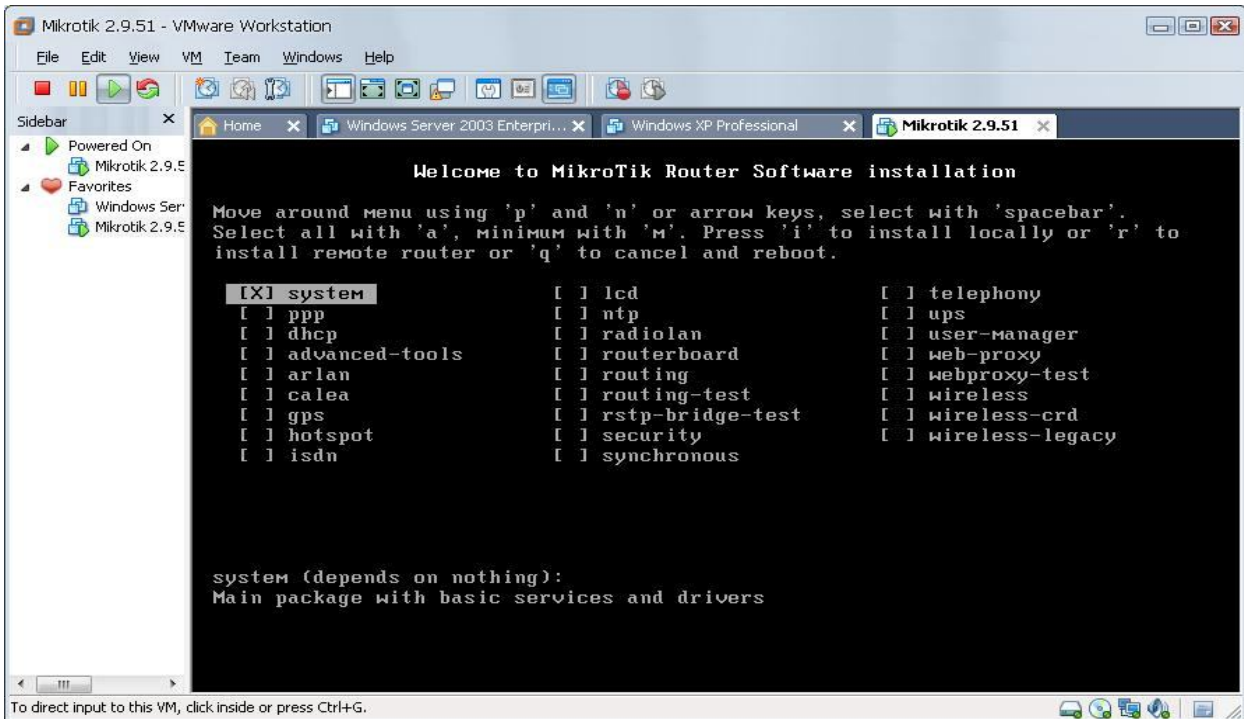




Pada Wizard selanjutnya kita buat 1 buah Virtual Harddisk, pilihlah type harddisk “IDE”. Lalu tentukan lokasi penyimpanan harddisk tersebut.



Untuk pilihan jenis **CDRom**, kita bisa menggunakan **Real CD** yang telah disediakan ataupun menggunakan **File ISO** yang disimpan di harddisk local maupun di dalam CD tersebut. Selanjutnya hidupkan Virtual PC tersebut dan lakukan setting **Boot Order** dengan **Boot from CDRom First**.



```
install remote router or 'q' to cancel and reboot.

[X] system      [X] lcd          [X] telephony
[X] ppp         [X] ntp          [X] ups
[X] dhcp        [X] radiolan     [X] user-manager
[X] advanced-tools [X] routerboard [X] web-proxy
[X] arlan       [X] routing      [X] webproxy-test
[X] calea       [X] routing-test [X] wireless
[X] gps         [X] rstp-bridge-test [X] wireless-crd
[X] hotspot     [X] security     [X] wireless-legacy
[X] isdn        [X] synchronous

system (depends on nothing):
Main package with basic services and drivers

Do you want to keep old configuration? [y/n]:n
Warning: all data on the disk will be erased!
Continue? [y/n]:
```

Tekan **"a"** untuk menginstall semua package. Lalu tekan **"i"** untuk memulai proses install. Karena konfigurasi Router baru, jawab **"n"** untuk mengabaikan konfigurasi yang lama (jika harddisk sdh ada installasi Mikrotik). Lalu **"y"** to continue installation.

```

[X] system          [X] lcd             [X] telephony
[X] ppp             [X] ntp             [X] ups
[X] dhcp            [X] radiolan        [X] user-manager
[X] advanced-tools  [X] routerboard     [X] web-proxy
[X] arlan            [X] routing          [X] webproxy-test
[X] calea            [X] routing-test    [X] wireless
[X] gps              [X] rstp-bridge-test [X] wireless-crd
[X] hotspot          [X] security         [X] wireless-legacy
[X] isdn             [X] synchronous

```

system (depends on nothing):
Main package with basic services and drivers

Do you want to keep old configuration? [y/n]:n

Warning: all data on the disk will be erased!

Continue? [y/n]:y

Creating partition.....

Selanjutnya tunggu Mikrotik melakukan proses Instalasi hingga selesai.

```

installed isdn-2.9.51
installed lcd-2.9.51
installed ntp-2.9.51
installed ppp-2.9.51
installed radiolan-2.9.51
installed routerboard-2.9.51
installed routing-2.9.51
disabled routing-2.9.51
installed routing-test-2.9.51
installed rstp-bridge-test-2.9.51
installed security-2.9.51
installed synchronous-2.9.51
installed telephony-2.9.51
installed ups-2.9.51
installed user-manager-2.9.51
installed web-proxy-2.9.51
installed (disabled) webproxy-test-2.9.51
installed wireless-2.9.51
installed (disabled) wireless-crd-2.9.51
installed (disabled) wireless-legacy-2.9.51
Checking disk integrity...

Software installed.
Press ENTER to reboot

```

Setelah muncul tampilan seperti di atas ini, instalasi telah selesai dalam waktu yang relatif cepat lalu tekan **ENTER** dan keluarkan CD Installer Mikrotik.

```

MikroTik 2.9.51
MikroTik Login: admin
Password: _

```

Setelah itu akan muncul tampilan seperti di atas ini. Masukkan Username : **Admin** dan kosongkan password / langsung tekan enter.

```

MikroTik v2.9.51
Login: admin
Password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III   KKK KKK RRRRRR      000000      TTT      III   KKK KKK
MMM MM  MMM III   KKKKK RRR RRR 000 000      TTT      III   KKKKK
MMM      MMM III   KKK KKK RRRRRR      000 000      TTT      III   KKK KKK
MMM      MMM III   KKK KKK RRR RRR 000000      TTT      III   KKK KKK

MikroTik RouterOS 2.9.51 <c> 1999-2008      http://www.mikrotik.com/

Terminal ansi detected, using single line input mode
[admin@MikroTik] >
root level

log/ -- System logs
quit -- Quit console
certificate/ -- Certificate management
special-login/ -- Special login users
radius/ -- Radius client settings
redo -- Redo previously undone action
driver/ -- Driver management
ping -- Send ICMP Echo packets
setup -- Do basic setup of system
interface/ -- Interface configuration
password -- Change password
undo -- Undo previous action
port/ -- Serial ports
import --
snmp/ -- SNMP settings
user/ -- User management
file/ -- Local router file storage.
system/ -- System information and utilities
queue/ -- Bandwidth management
ip/ -- IP options
tool/ -- Diagnostics tools
isdn-channels/ -- ISDN channel status info
ppp/ -- Point to Point Protocol
routing/ --
mikrotik/ --
export --

[admin@MikroTik] > _

```

Tekan “?” / [tanda tanya](#) untuk menampilkan help command. Untuk memulai setting Mikrotik, dari Konsol ini kita ketikkan “**setup**”, lalu ikuti Wizard seperti contoh dibawah ini.

```

MikroTik Login: admin
Password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III   KKK KKK RRRRRR      000000      TTT      III   KKK KKK
MMM MM  MMM III   KKKKK RRR RRR 000 000      TTT      III   KKKKK
MMM      MMM III   KKK KKK RRRRRR      000 000      TTT      III   KKK KKK
MMM      MMM III   KKK KKK RRR RRR 000000      TTT      III   KKK KKK

MikroTik RouterOS 2.9.51 (c) 1999-2008      http://www.mikrotik.com/

Terminal linux detected, using multiline input mode
[admin@MikroTik] > setup_

```

```

/ip address add address=192.168.1.1/24 interface=LAN comment="added by setup"
+ a - add ip address
* g - setup default gateway
x - exit menu
your choice [press Enter to setup default gateway]: g
gateway: 192.168.10.1
#Adding default route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="added by \
setup"
+ a - add ip address
* g - setup default gateway
x - exit menu
your choice [press Enter to setup default gateway]: x
r - reset all router configuration
+ l - load interface driver
+ a - configure ip address and gateway
d - setup dhcp client
* s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
your choice [press Enter to setup dhcp server]: x

[Safe Mode released]

Setup completed successfully.
Following commands were executed during this setup:
#Enabling interface
/interface enable LAN
#Adding IP address
/ip address add address=192.168.1.1/24 interface=LAN comment="added by setup"
#Adding default route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="added by \
setup"
[admin@MikroTik] > system
[admin@MikroTik] system> reboot
Reboot, yes? [y/N]: _

```

Setup uses Safe Mode. It means that all changes that are made during setup are reverted in case of error, or if Ctrl-C is used to abort setup. To keep changes exit setup using the 'x' key.

```

[Safe Mode taken]
Choose options by pressing one of the letters in the left column, before
dash. Pressing 'x' will exit current menu, pressing Enter key will select the
entry that is marked by an '*'. You can abort setup at any time by pressing
Ctrl-C.
Entries marked by '+' are already configured.
Entries marked by '-' cannot be used yet.
Entries marked by 'X' cannot be used without installing additional packages.
r - reset all router configuration
+ l - load interface driver
* a - configure ip address and gateway
d - setup dhcp client
s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
your choice [press Enter to configure ip address and gateway]: a
+ a - add ip address
* g - setup default gateway
x - exit menu
your choice [press Enter to setup default gateway]: _

```

changes exit setup using the 'x' key.

[Safe Mode taken]

Choose options by pressing one of the letters in the left column, before dash. Pressing 'x' will exit current menu, pressing Enter key will select the entry that is marked by an '*'. You can abort setup at any time by pressing Ctrl-C.

Entries marked by '+' are already configured.

Entries marked by '-' cannot be used yet.

Entries marked by 'X' cannot be used without installing additional packages.

```
r - reset all router configuration
+ l - load interface driver
* a - configure ip address and gateway
d - setup dhcp client
s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
```

your choice [press Enter to configure ip address and gateway]: a

```
+ a - add ip address
* g - setup default gateway
x - exit menu
```

your choice [press Enter to setup default gateway]: a

enable interface: LAN

ip address/netmask: 192.168.8.1/24

changes exit setup using the 'x' key.

[Safe Mode taken]

Choose options by pressing one of the letters in the left column, before dash. Pressing 'x' will exit current menu, pressing Enter key will select the entry that is marked by an '*'. You can abort setup at any time by pressing Ctrl-C.

Entries marked by '+' are already configured.

Entries marked by '-' cannot be used yet.

Entries marked by 'X' cannot be used without installing additional packages.

```
r - reset all router configuration
+ l - load interface driver
* a - configure ip address and gateway
d - setup dhcp client
s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
```

your choice [press Enter to configure ip address and gateway]: a

```
+ a - add ip address
* g - setup default gateway
x - exit menu
```

your choice [press Enter to setup default gateway]: a

enable interface: LAN

ip address/netmask: 192.168.1.1/24

Entries marked by 'X' cannot be used without installing additional packages.

```
r - reset all router configuration
+ l - load interface driver
* a - configure ip address and gateway
d - setup dhcp client
s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
```

your choice [press Enter to configure ip address and gateway]: a

```
+ a - add ip address
* g - setup default gateway
x - exit menu
```

your choice [press Enter to setup default gateway]: a

enable interface: LAN

ip address/netmask: 192.168.1.1/24

#Enabling interface

/interface enable LAN

#Adding IP address

/ip address add address=192.168.1.1/24 interface=LAN comment="added by setup"

```
+ a - add ip address
* g - setup default gateway
x - exit menu
```

your choice [press Enter to setup default gateway]: g

gateway: 192.168.10.1

```

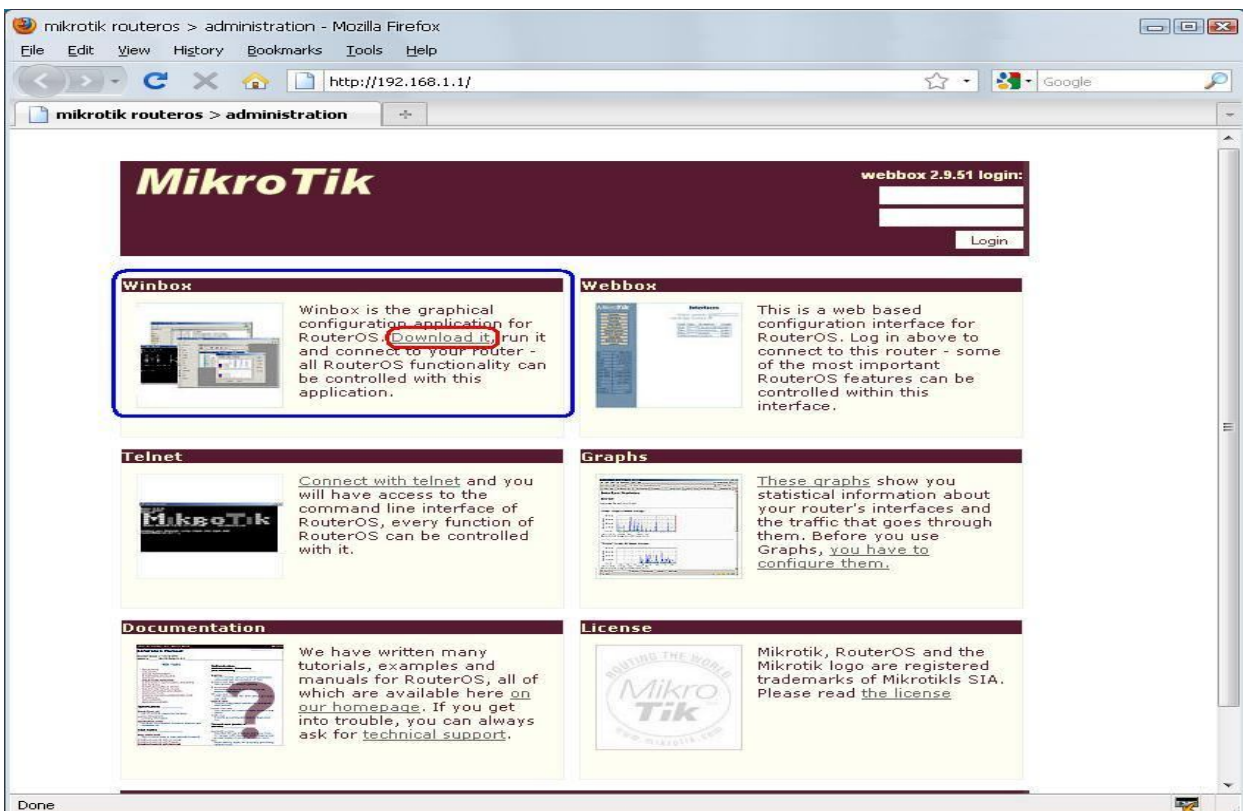
x - exit menu
your choice [press Enter to setup default gateway]: g
gateway: 192.168.10.1
#Adding default route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="added by \
setup"
+ a - add ip address
* g - setup default gateway
x - exit menu
your choice [press Enter to setup default gateway]: x
r - reset all router configuration
+ l - load interface driver
+ a - configure ip address and gateway
d - setup dhcp client
* s - setup dhcp server
p - setup pppoe client
t - setup pptp client
x - exit menu
your choice [press Enter to setup dhcp server]: x

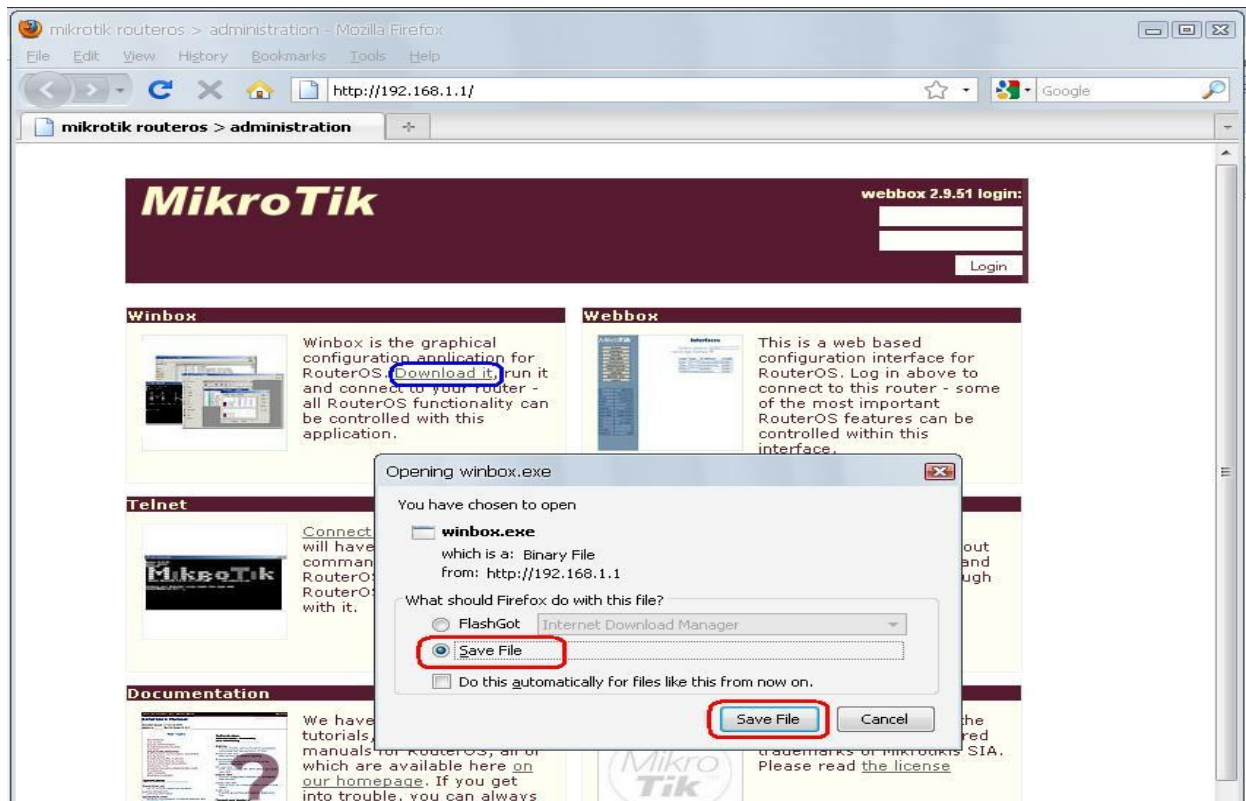
[Safe Mode released]

Setup completed successfully.
Following commands were executed during this setup:
#Enabling interface
/interface enable LAN
#Adding IP address
/ip address add address=192.168.1.1/24 interface=LAN comment="added by setup"
#Adding default route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="added by \
setup"
[admin@MikroTik] >

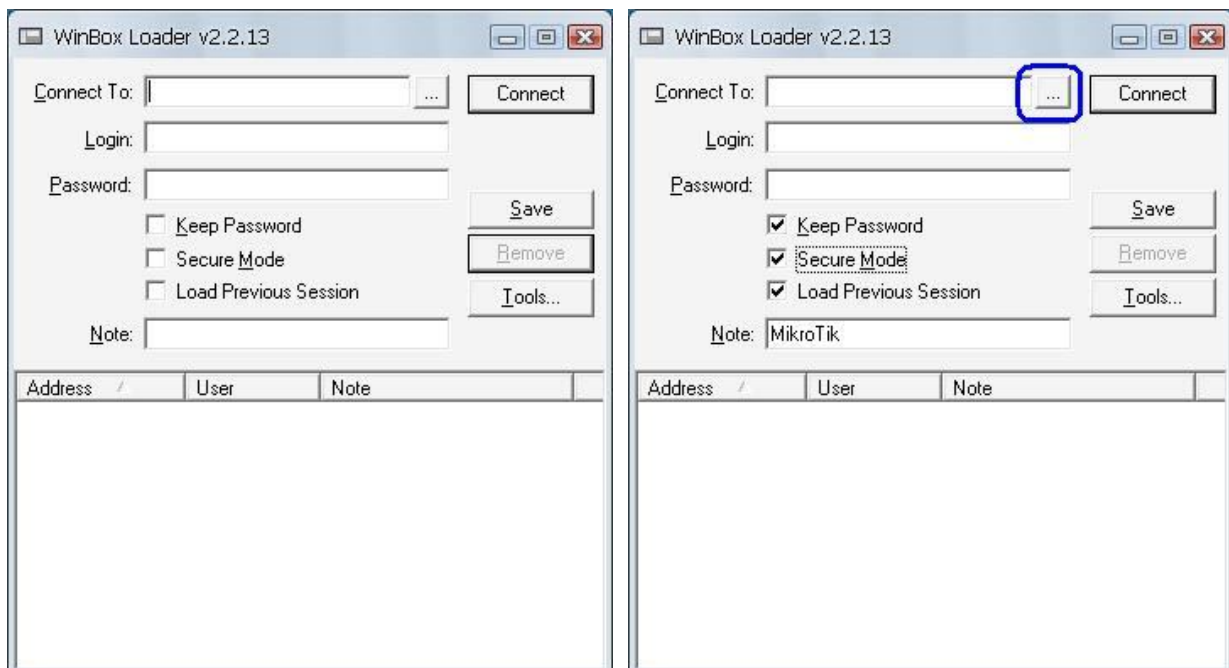
```

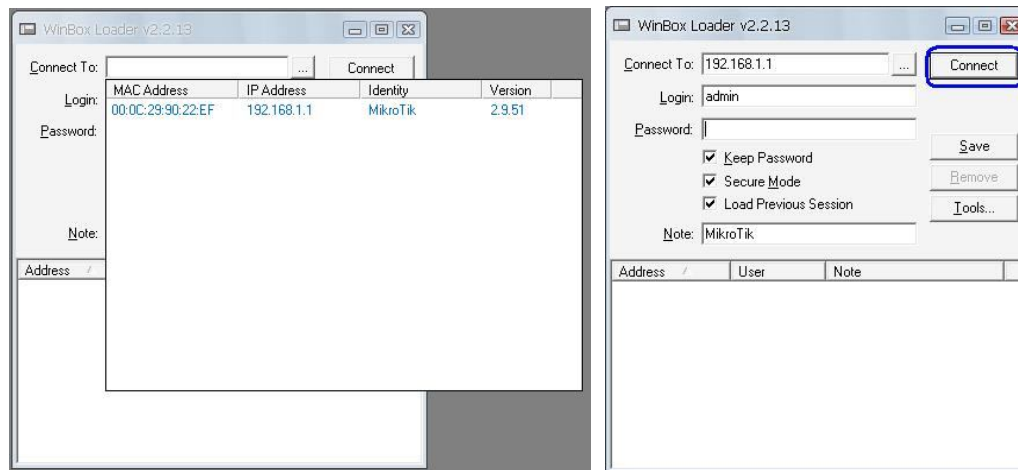
Setelah Setup Wizard ini selesai dan IP Address PC kita telah kita setting se-level dengan LAN Mikrotik, maka selanjutnya kita buka WebBrowser kita IP Address Mikrotik tersebut : **192.168.1.1**. Lalu akan muncul tampilan seperti dibawah ini dan dari **WebBox** inilah kita bisa konfigurasi lebih lanjut, diantaranya kita bisa download **Winbox** yang telah disediakan.



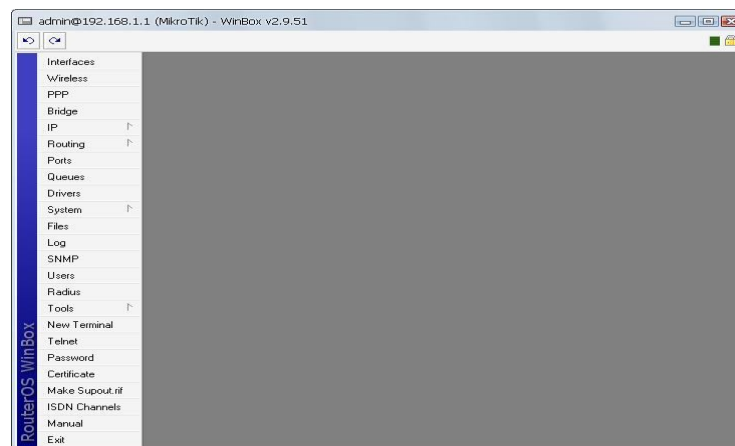


Lakukan download Winbox tersebut dan simpan di Local harddisk kita, lalu jalankanlah aplikasi Winbox tersebut. Selanjutnya setelah muncul tampilan seperti dibawah ini maka selanjutnya kita bisa lakukan browsing Mikrotik seperti tampilan dibawah ini ataupun dengan cara mengetikkan IP Address Mikrotik kita : **192.168.1.1**.

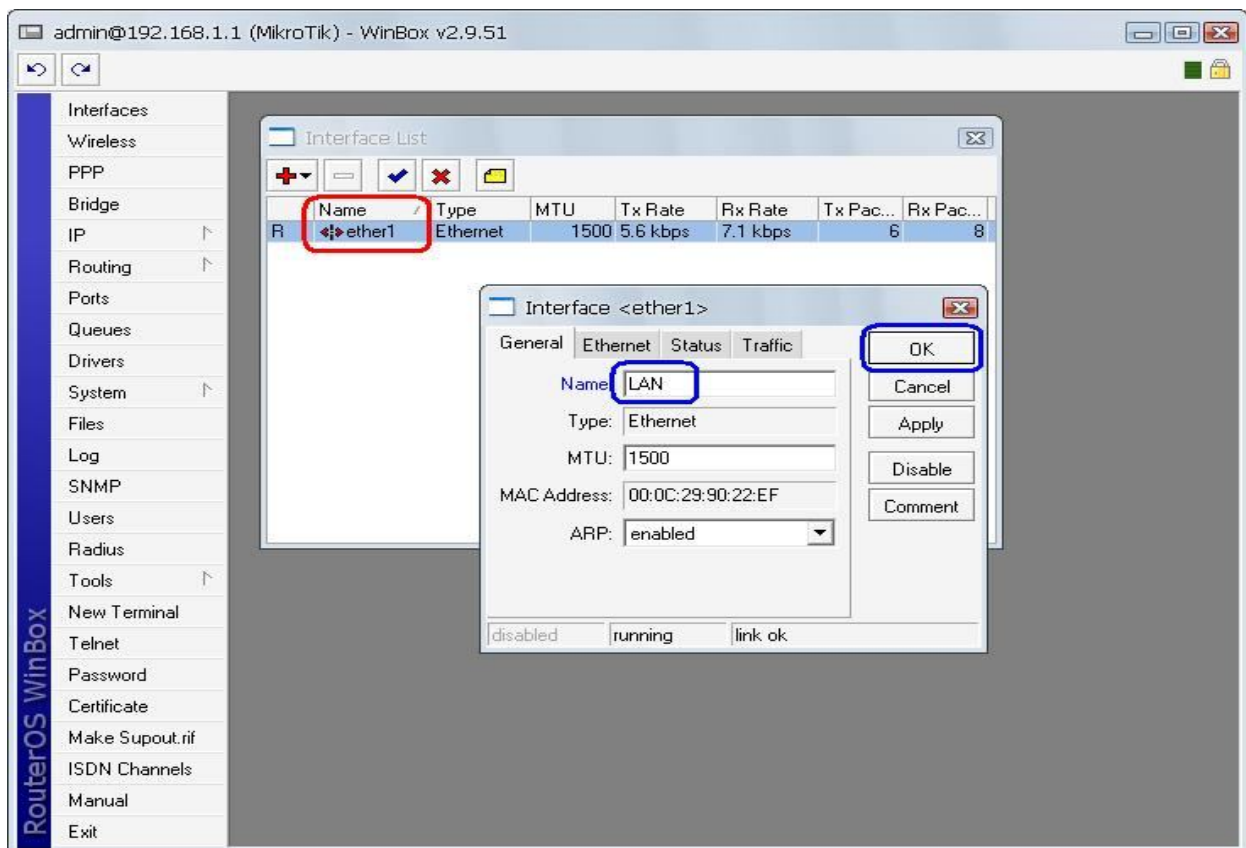
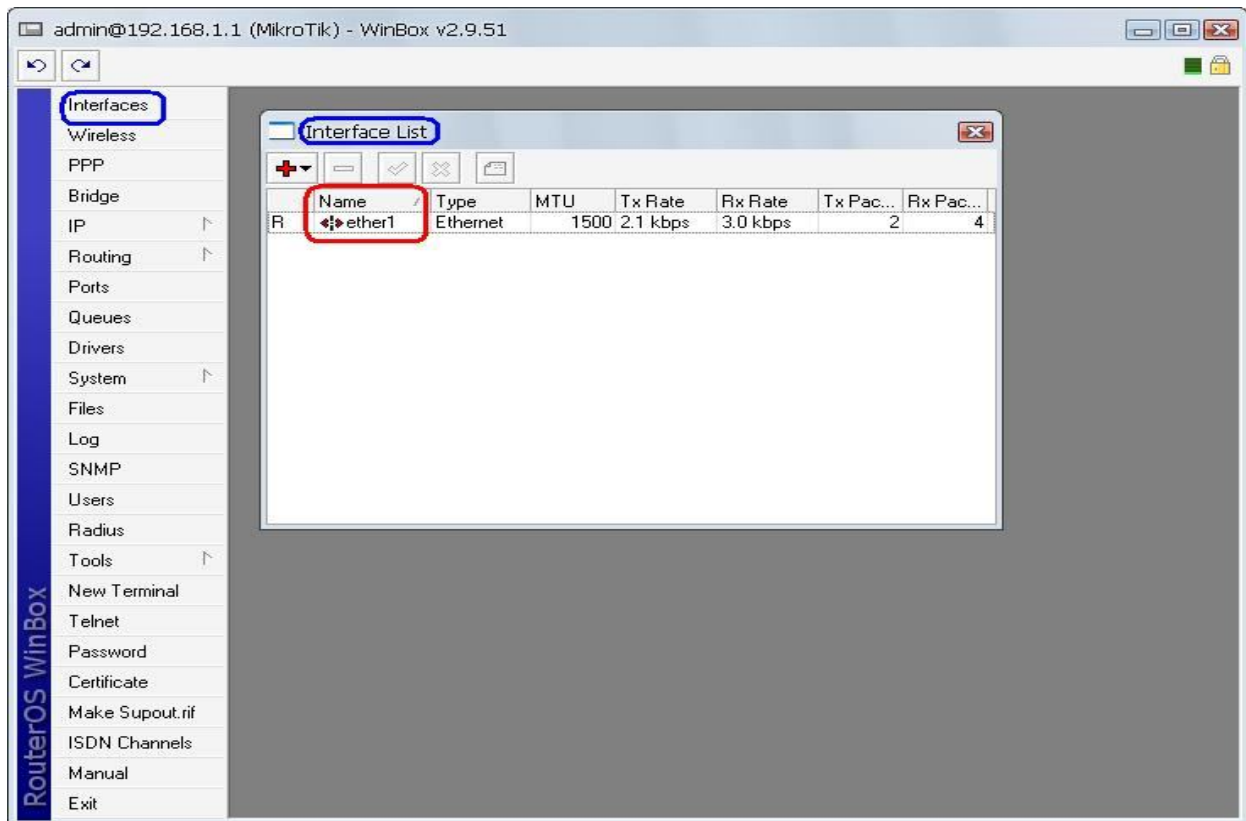


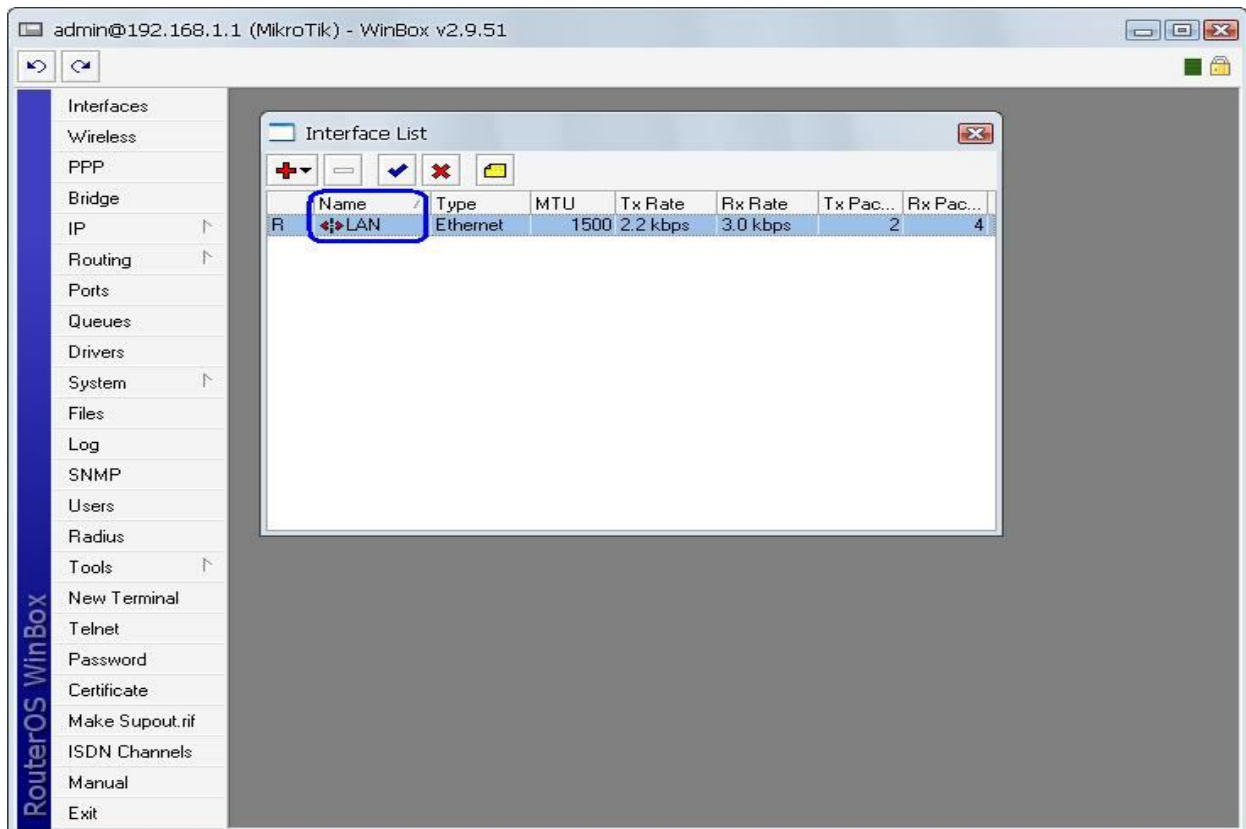


Disini kita juga bisa menyimpan koneksi beserta password-nya agar memudahkan kita Login di waktu berikutnya. Penyimpanan Account ini hanya disarankan pada penggunaan komputer pribadi...

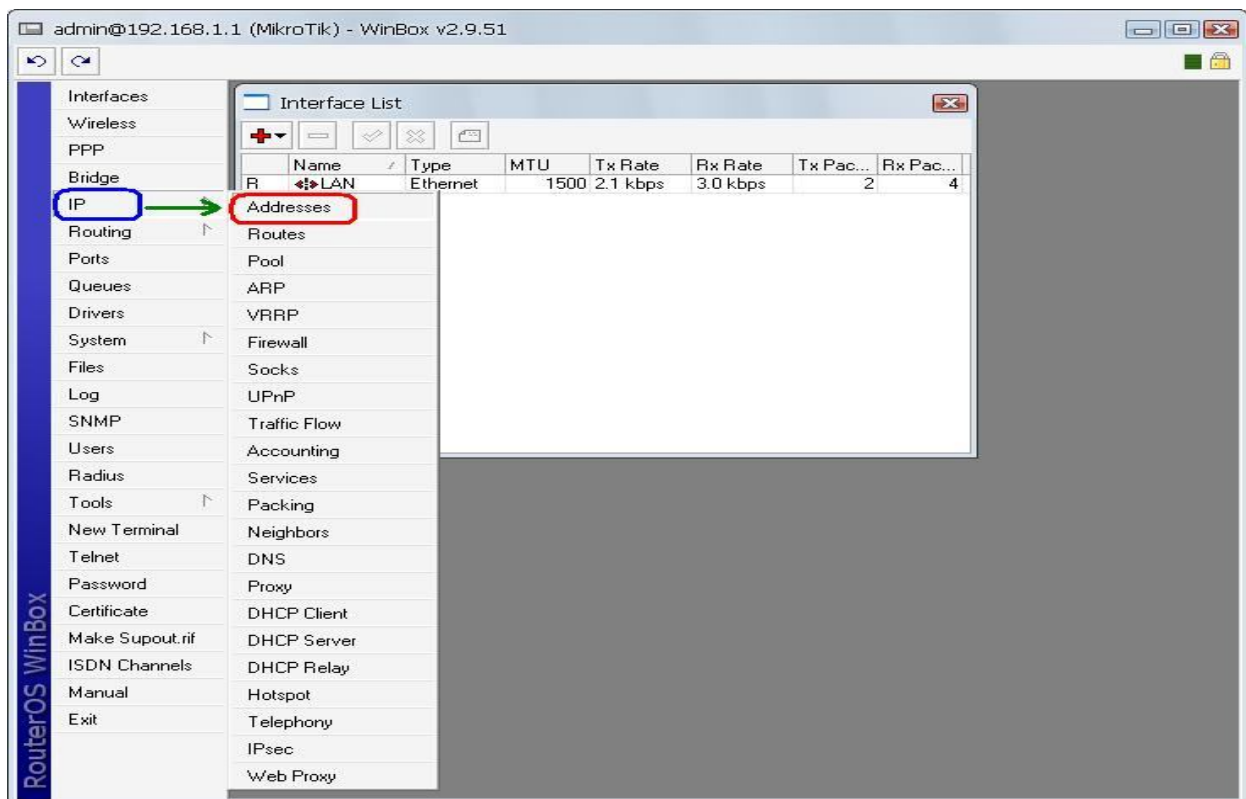


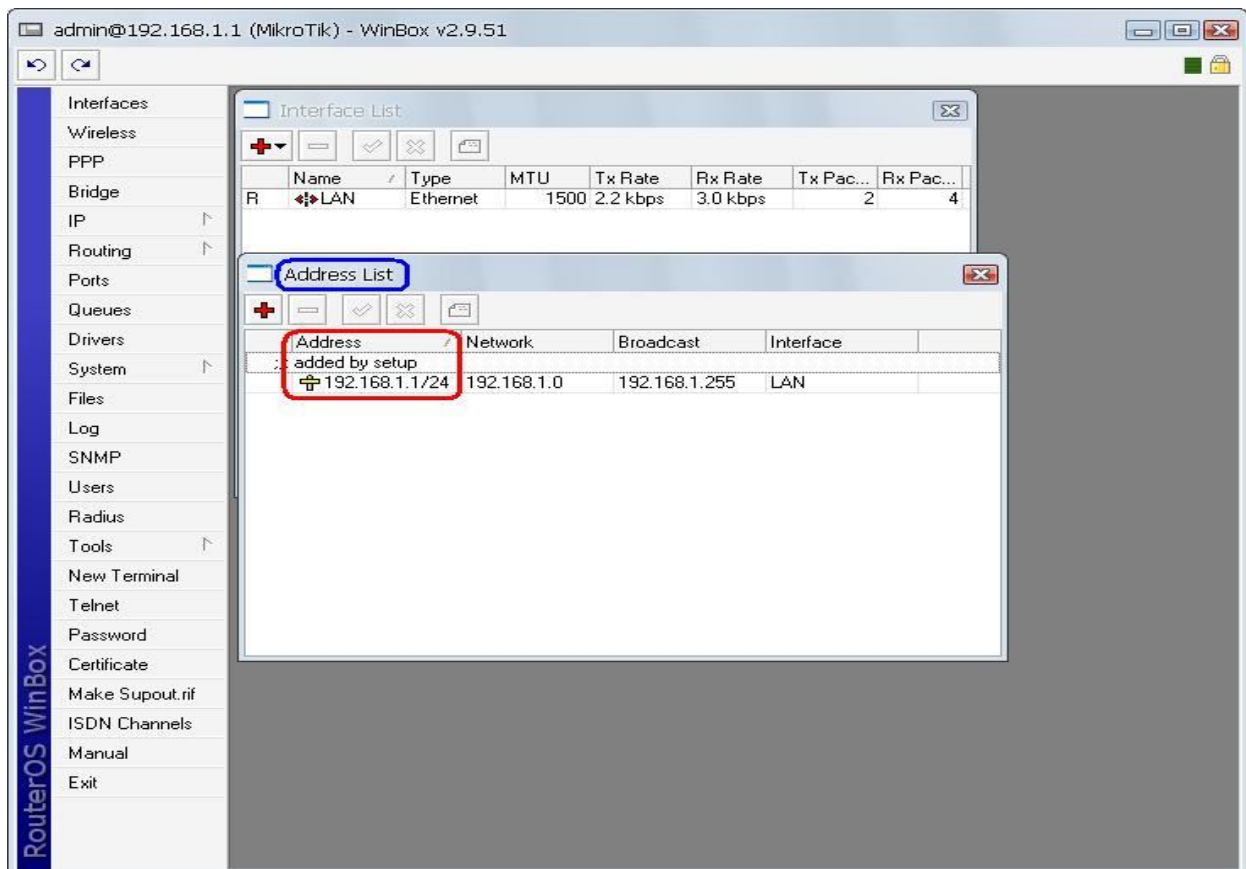
Selanjutnya akan muncul tampilan Winbox seperti diatas dan kita bisa melakukan konfigurasi lebih lanjut. Klik menu Interface untuk menampilkan Interface LAN Card yang telah kita pasang. Kita berikan nama **“LAN”** pada interface ini, double klik Interface Name “ether1” tersebut dan ganti dengan nama **“LAN”**.



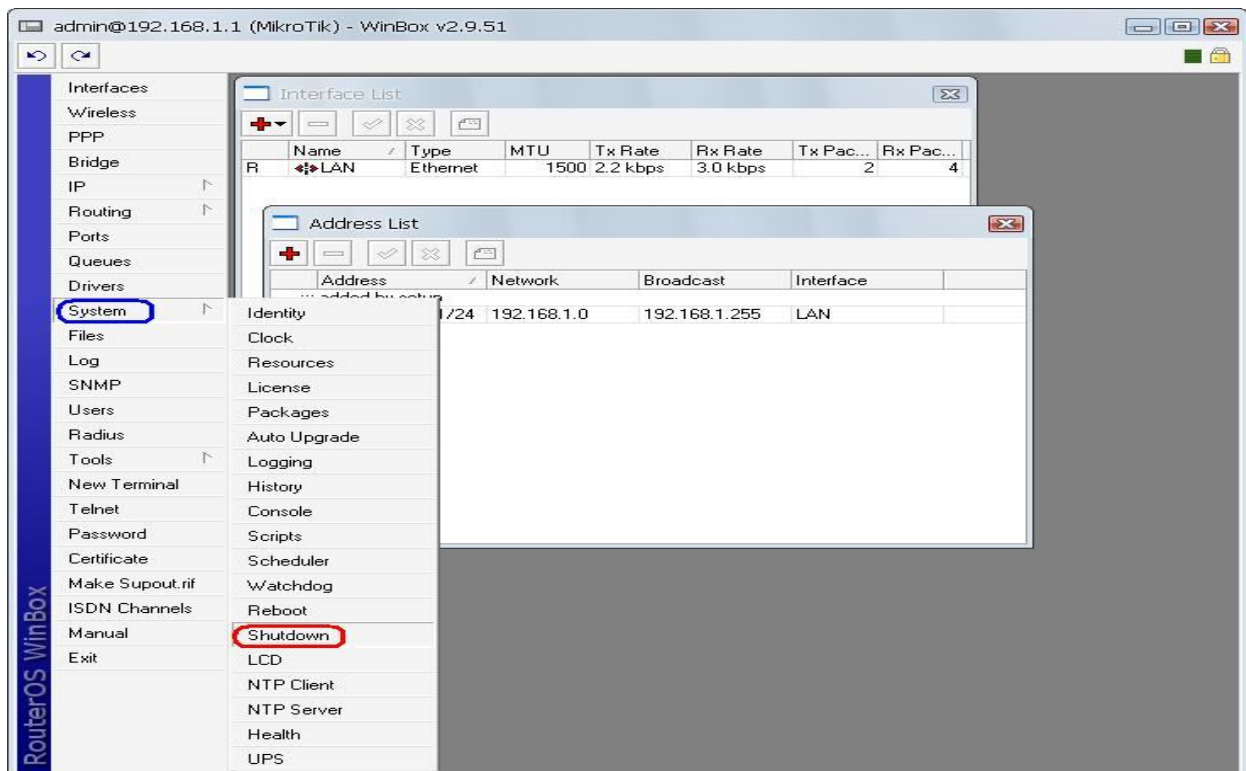


Setelah memberi nama Interface **LAN**, kita selanjutnya memberikan IP Address : **192.168.1.1** pada interface tersebut. Dari **Winbox**, kita pilih menu "**IP**" -> "**Addresses**".



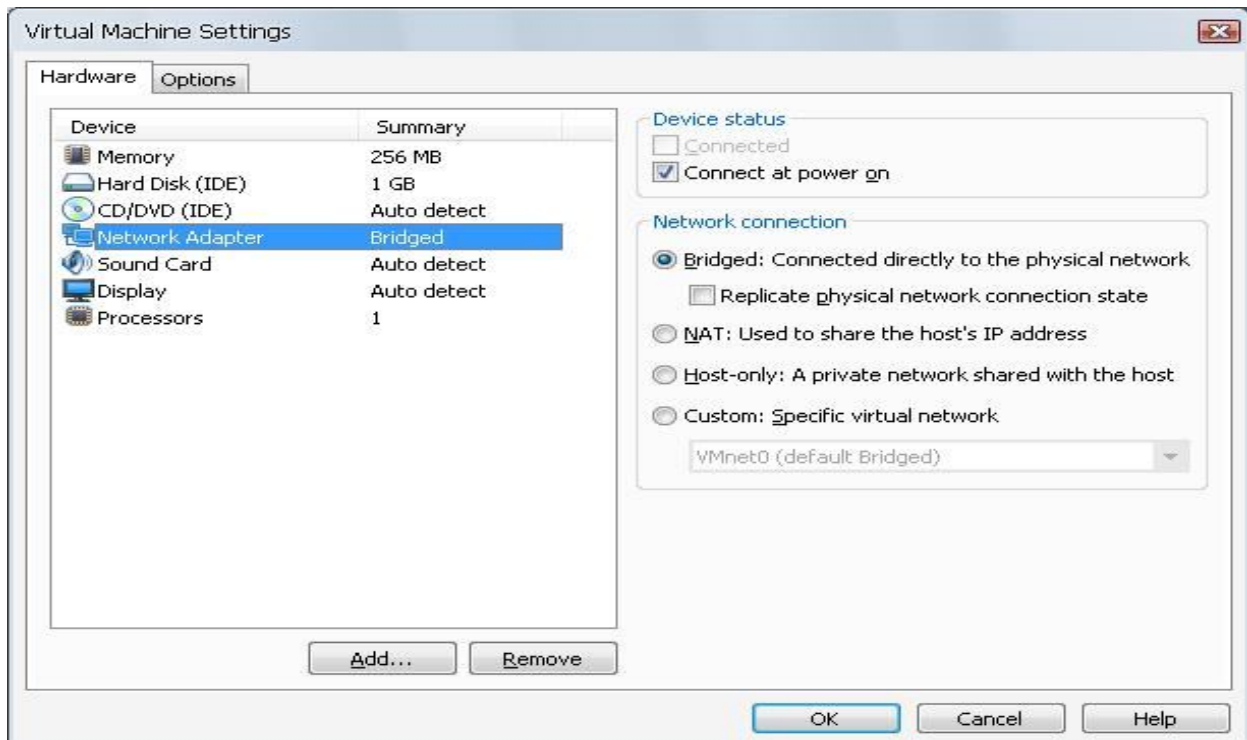
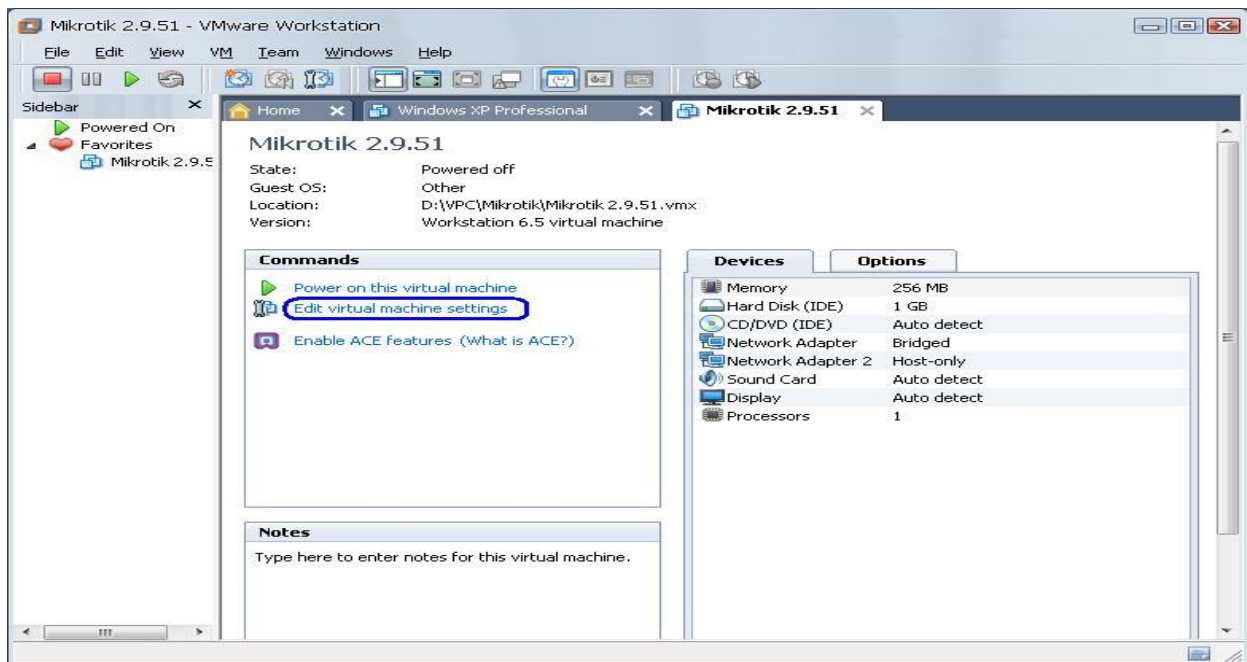


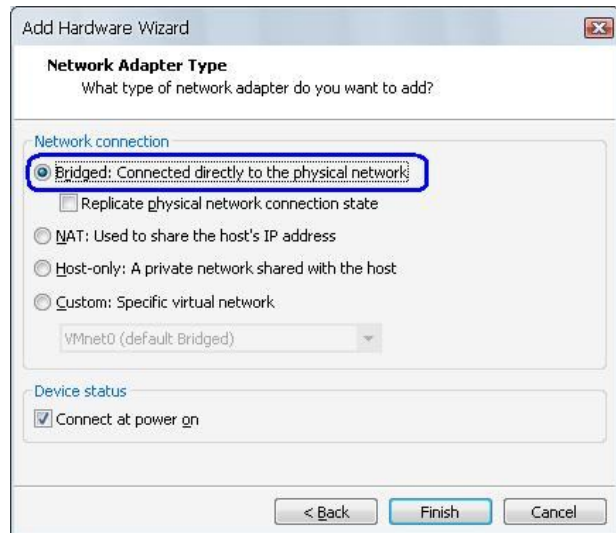
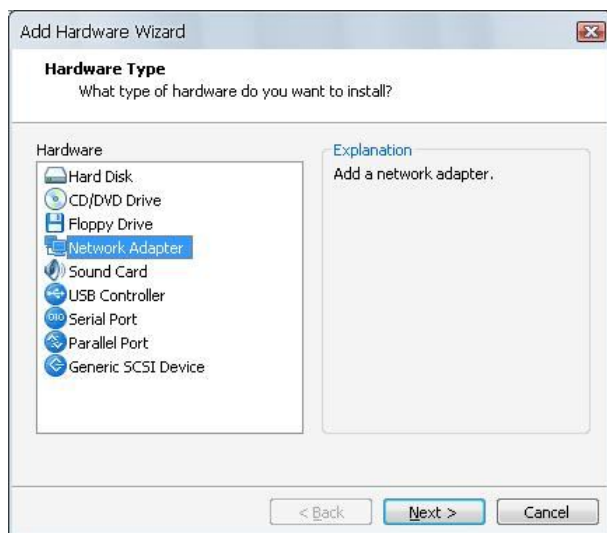
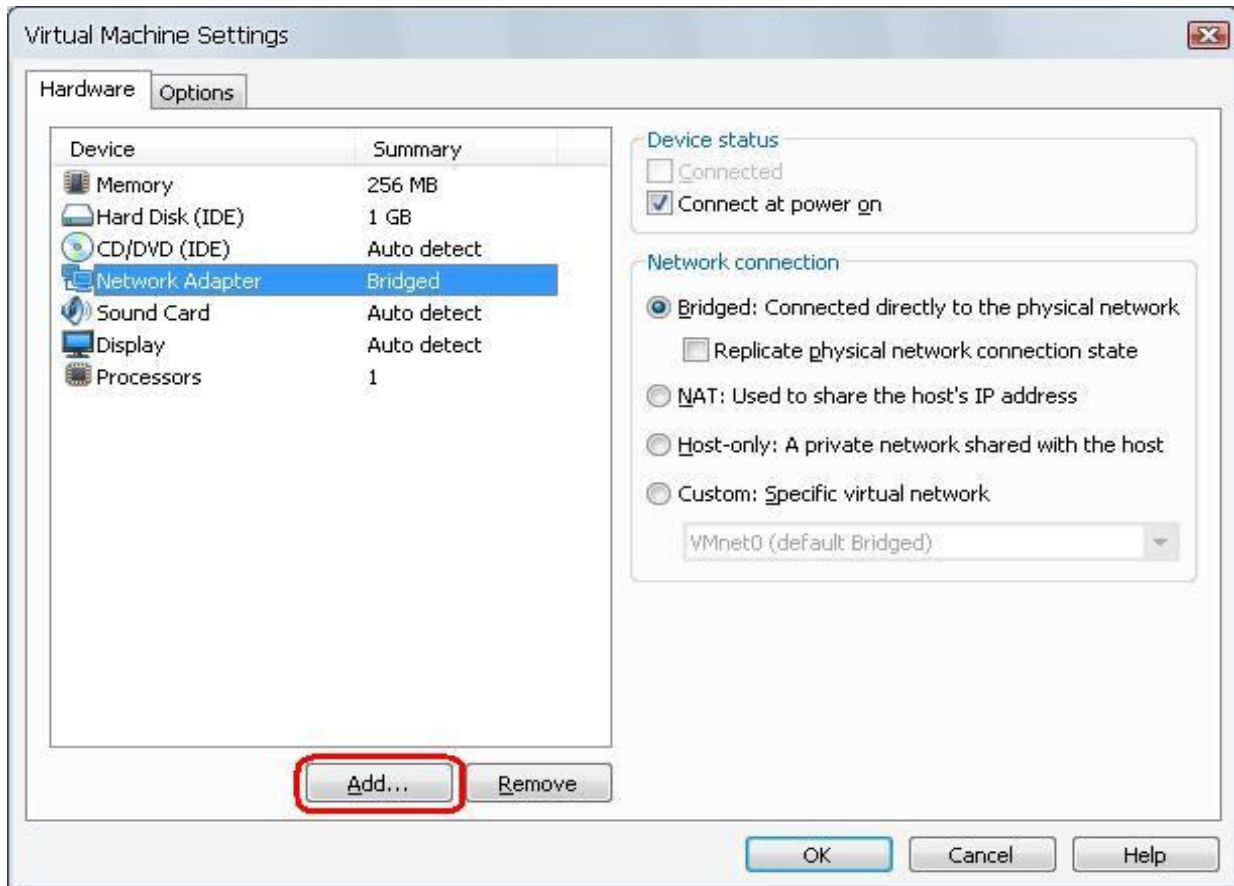
Kita lihat IP Address **192.168.1.1/24** merupakan IP address yang kita input dari Setup di Konsol tadi. Oke, selanjutnya Mikrotik kita **Shutdown** untuk menambahkan sebuah interface lagi untuk koneksi ke Modem ADSL.

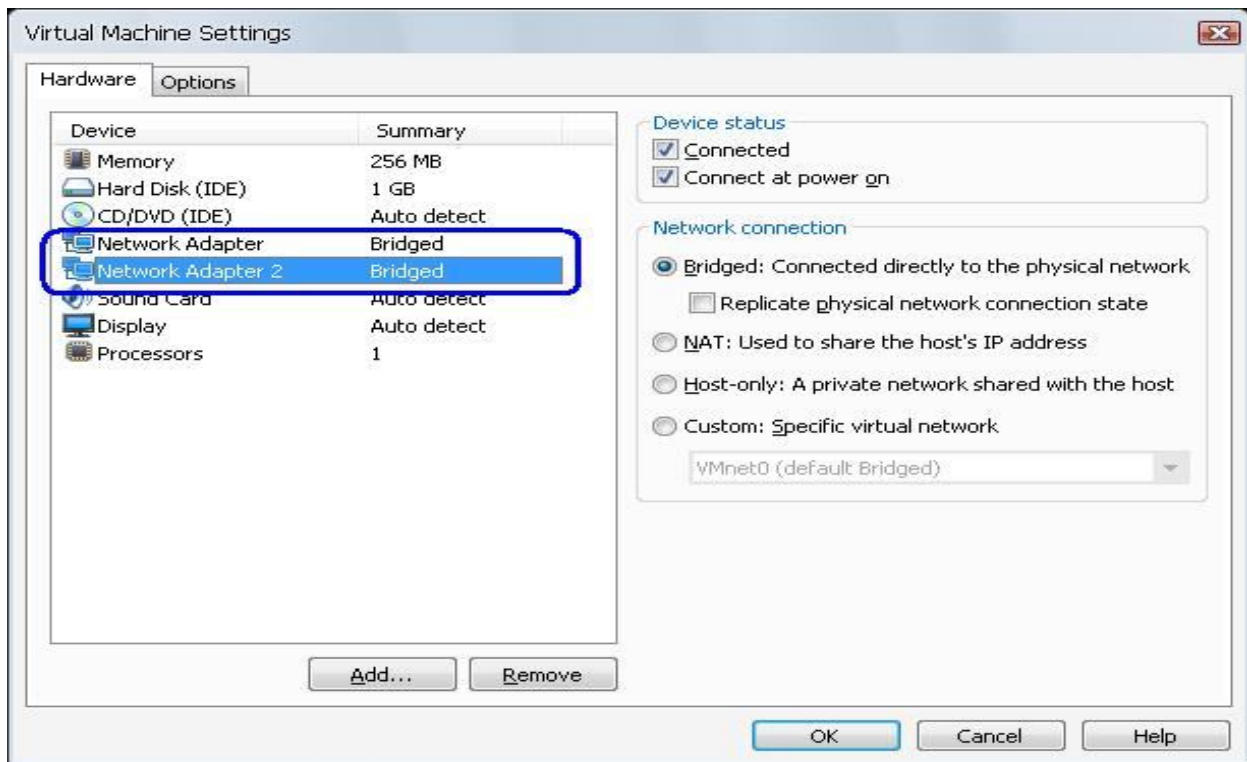




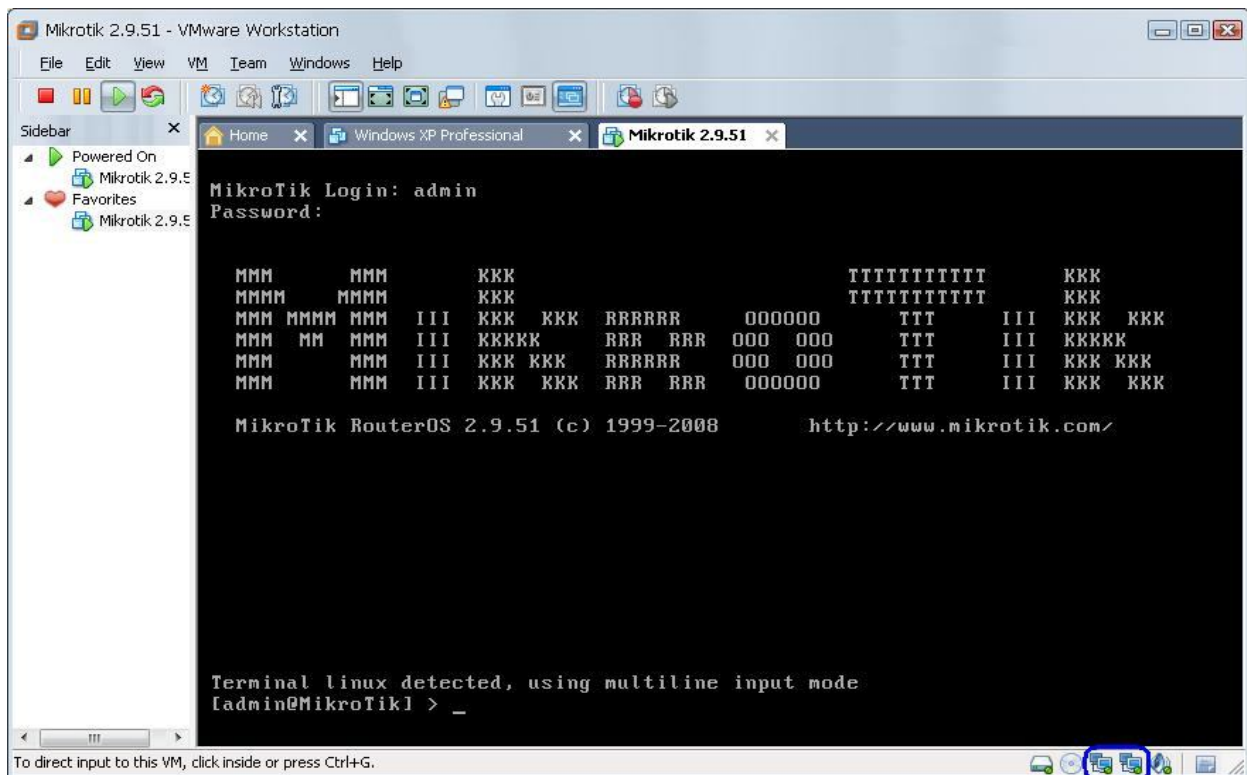
Dari VMWare kita masuk ke menu "Edit Virtual Machine Setting", kita **Add** sebuah **interface Network Adapter** pada mode **Bridge Network**.



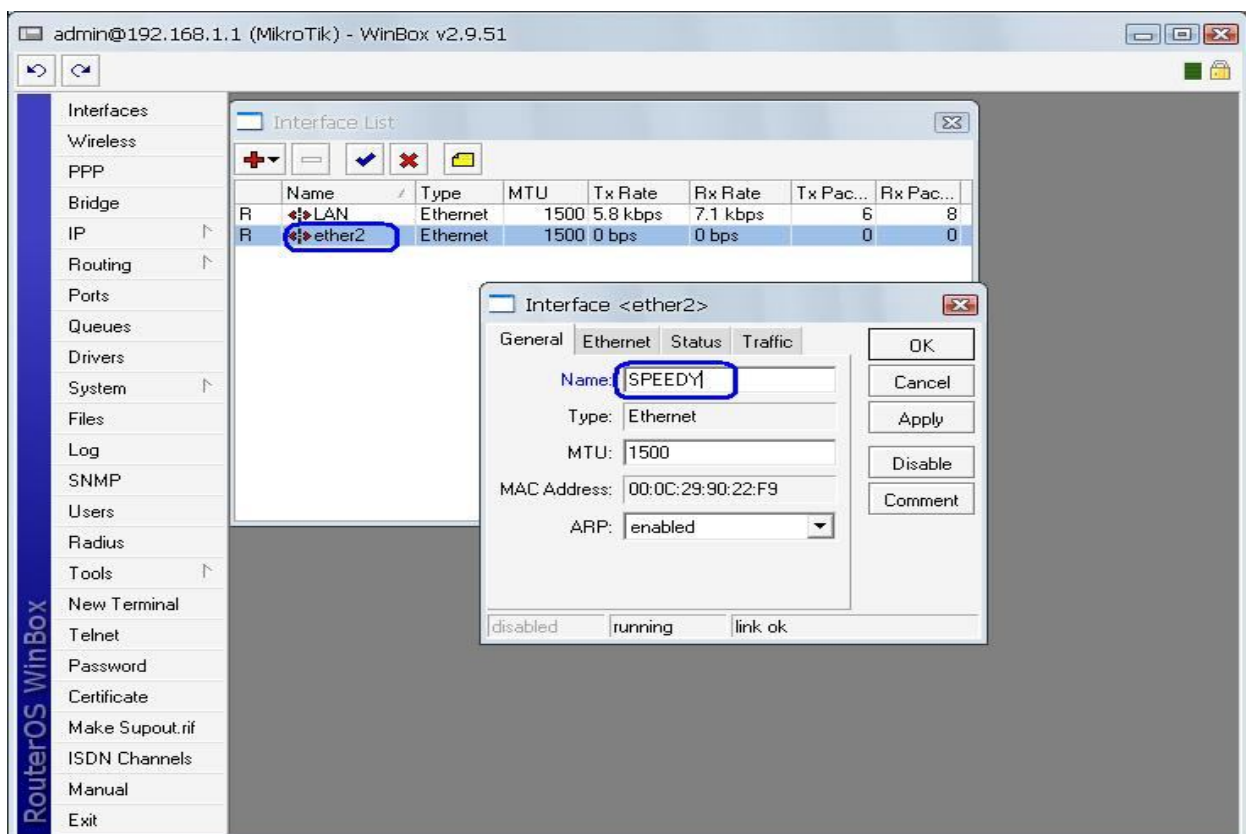
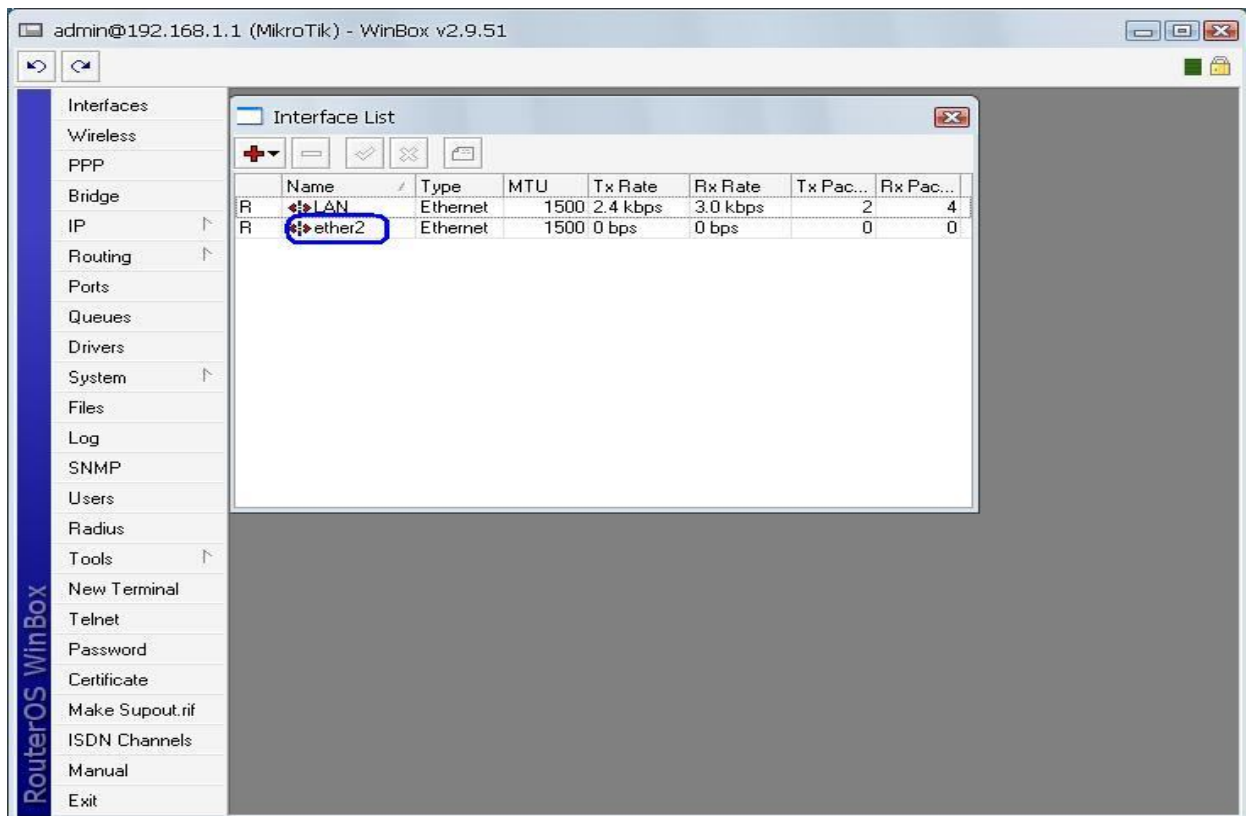




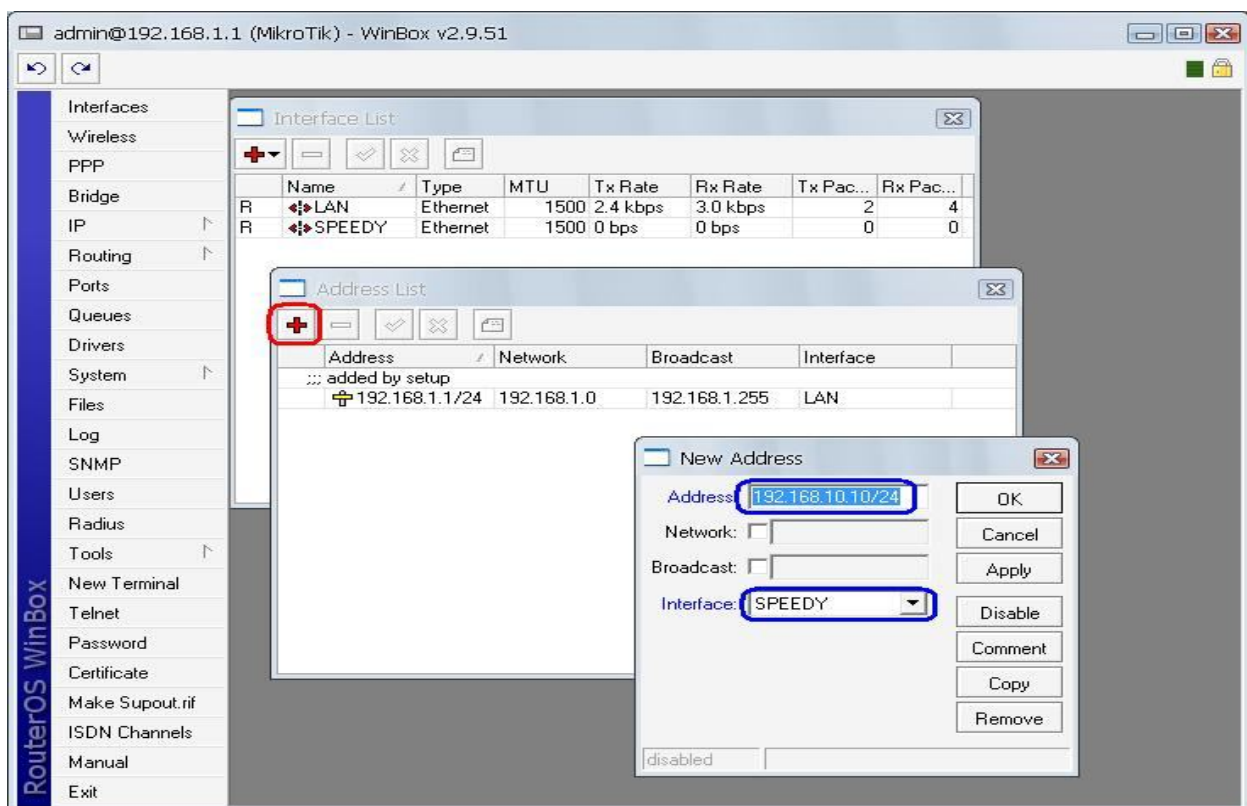
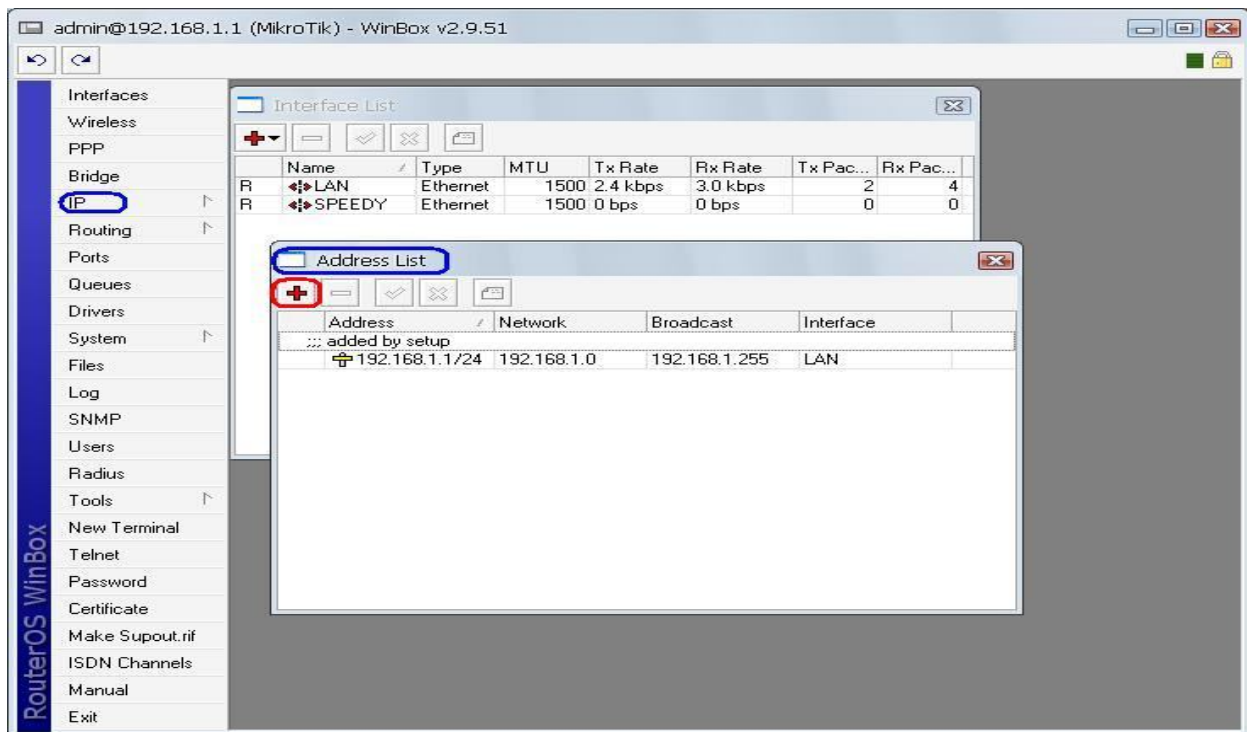
Setelah network adapter selesai kita buat, selanjutnya kita jalankan / kita hidupkan lagi Mikrotik kita.



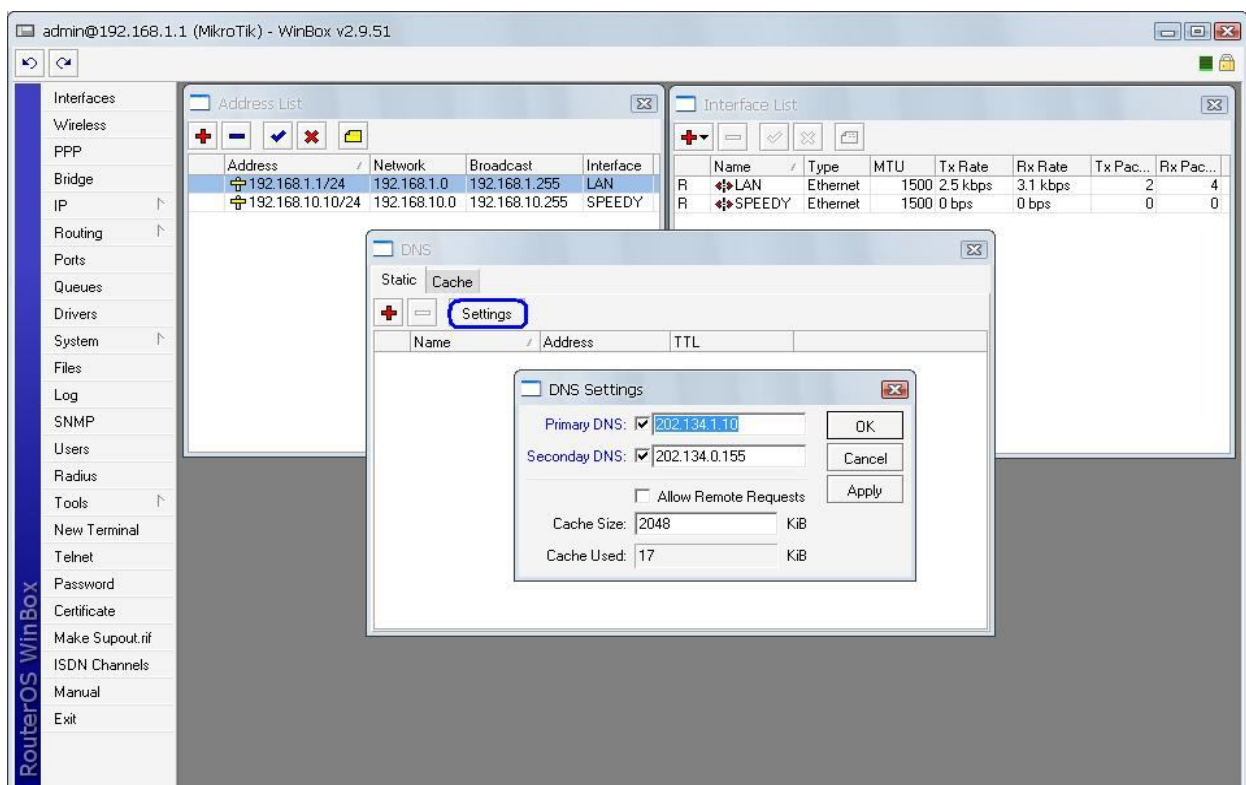
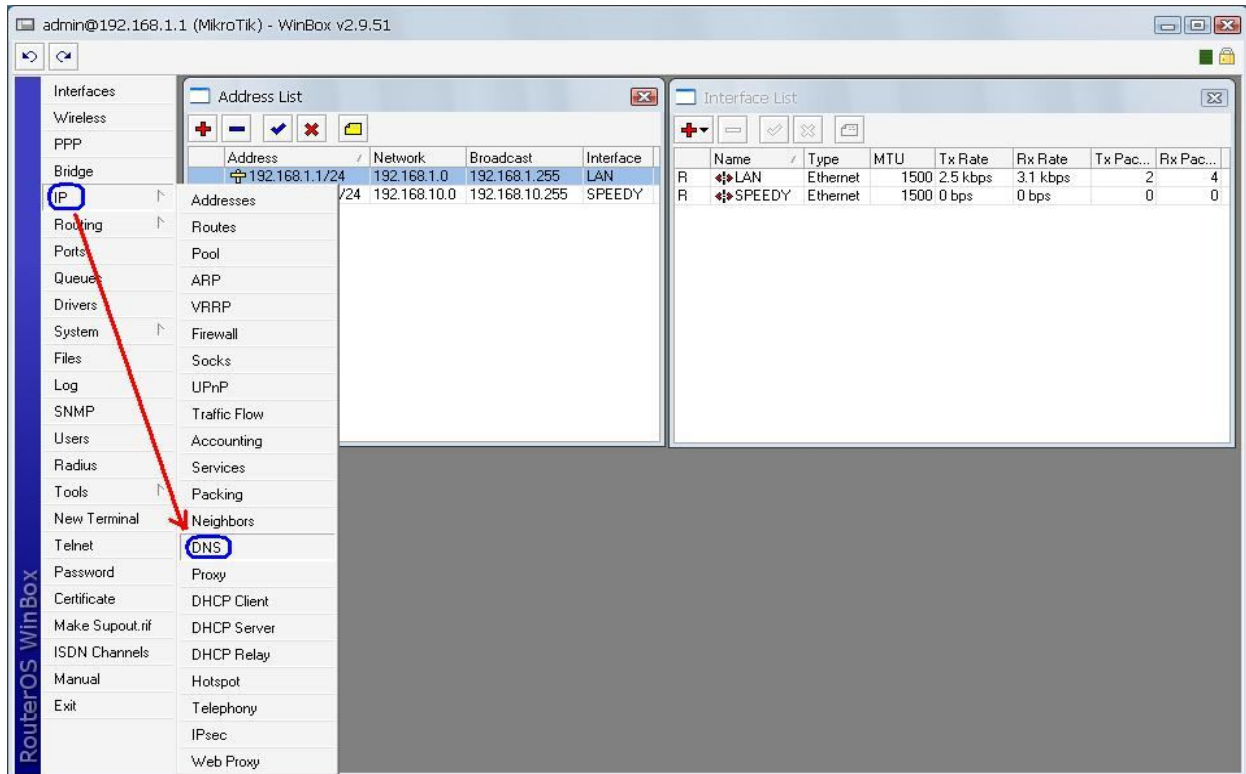
Selanjutnya kita lihat interface Mikrotik kita sudah ada **"ether2"** yang baru kita pasangkan, ganti nama interface ini dengan nama **"SPEEDY"**.



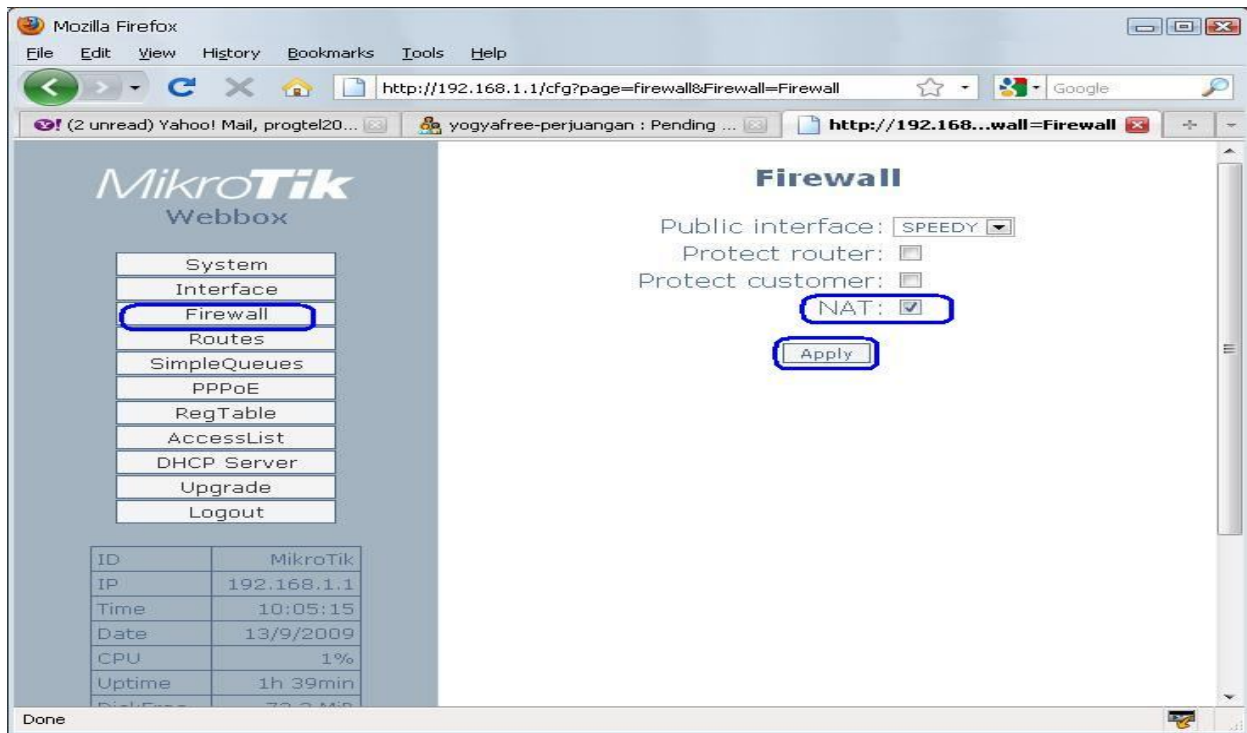
Langkah selanjutnya adalah kita berikan IP Address pada interface **Speedy** dengan IP Address : **192.168.10.10/24**.



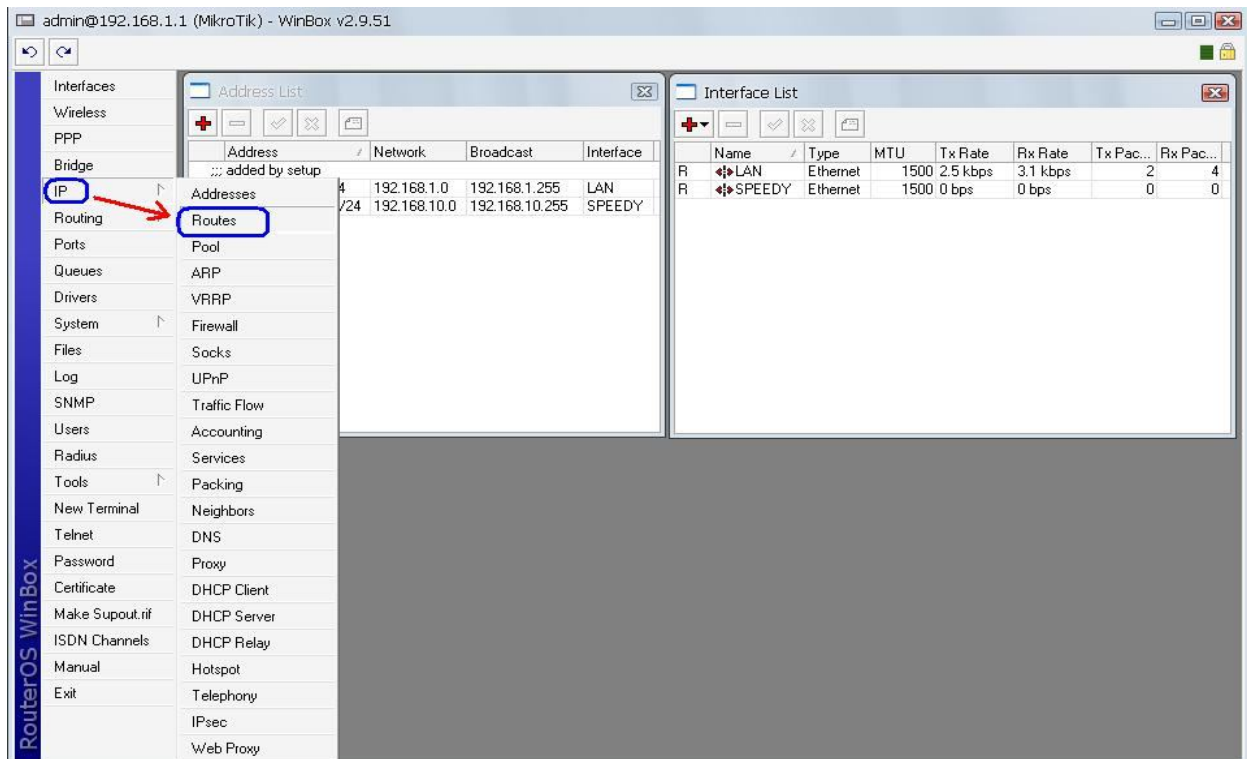
Selanjutnya kita masukkan IP DNS Speedy dari Winbox, lalu pilih menu **“IP”** -> **“DNS”**.

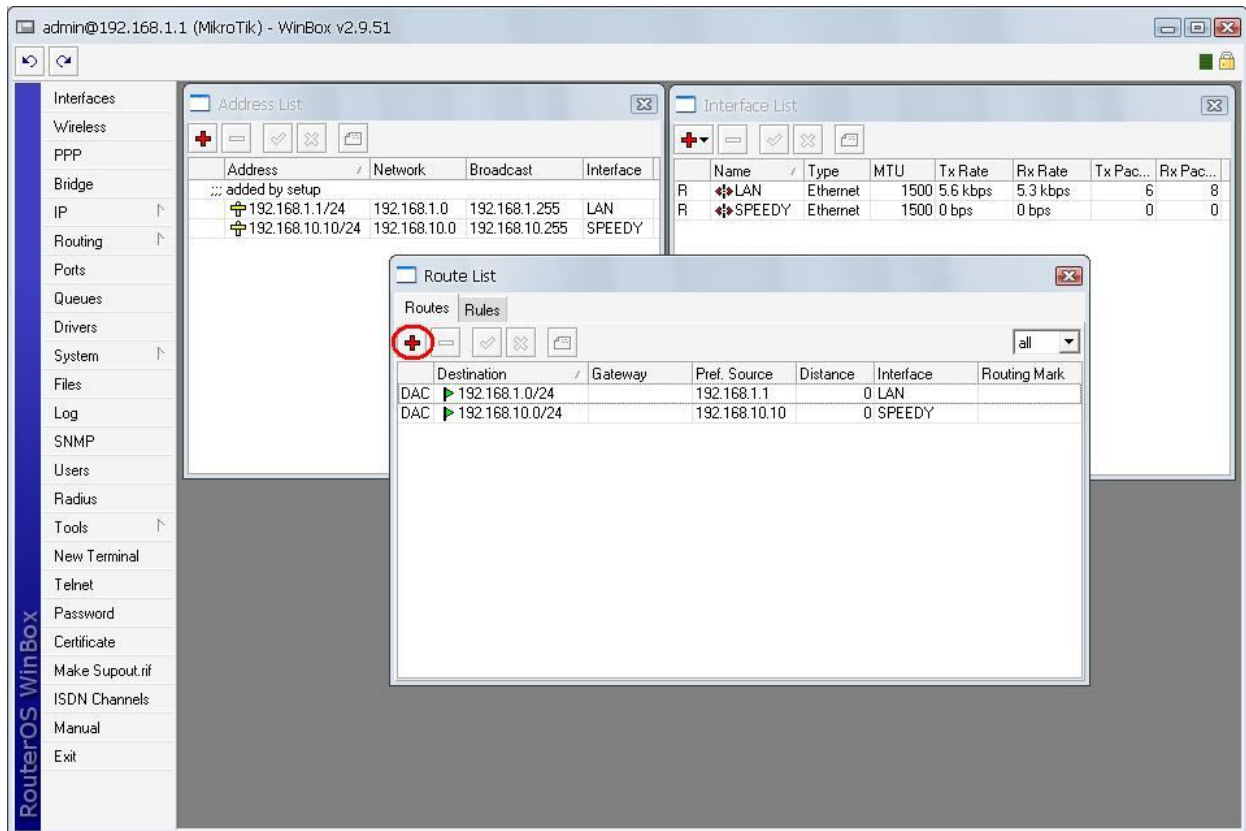


Selanjutnya kita NAT dari **Webbox** -> **Firewall**. Tujuan atau maksud pengaturan NAT ini adalah mengatur Interface Mikrotik sebagai Network Address Tranlastor sehingga IP Address **LAN** dapat mengakses IP Address **WAN / Internet**. Memang kita bisa setting dari Winbox, tapi dari WebBox ini sangat lebih mudah, khususnya bagi Newbie.

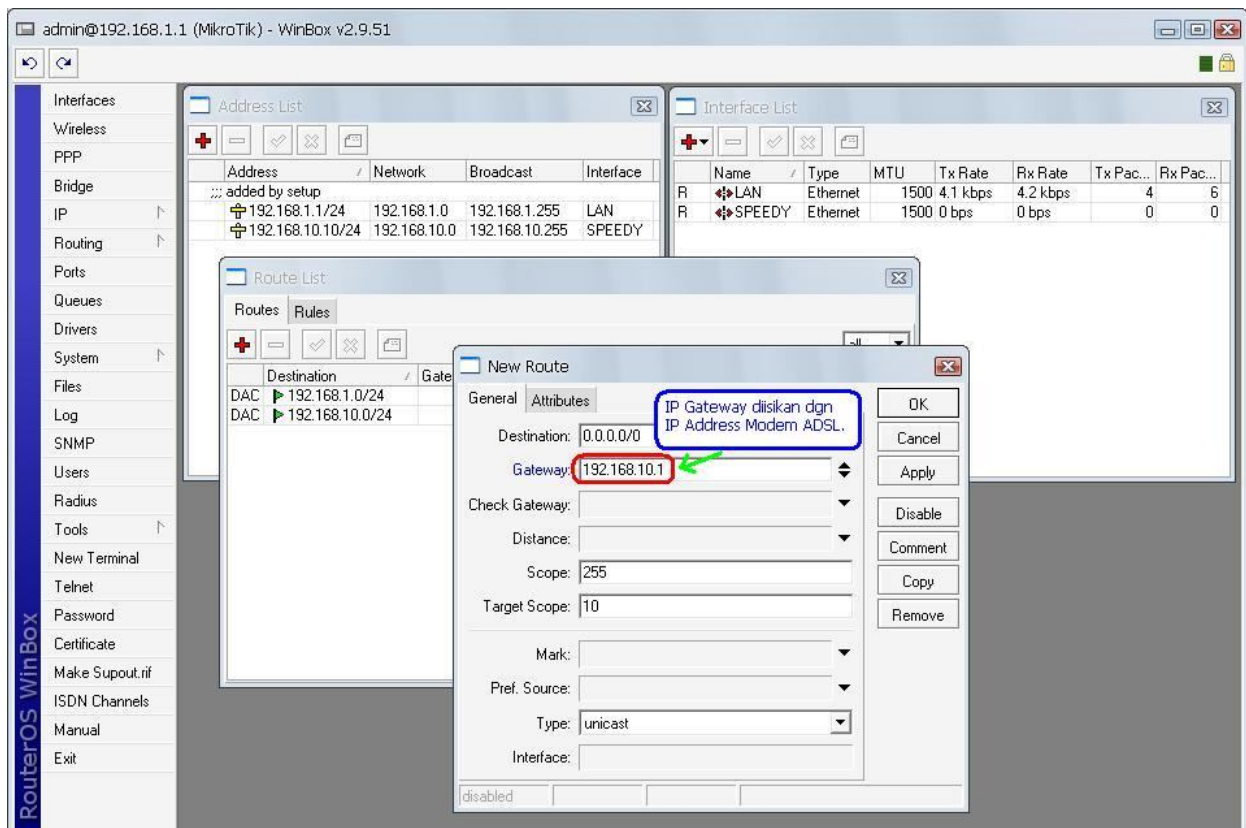


Selanjutnya kita setting "IP" -> "Routes".

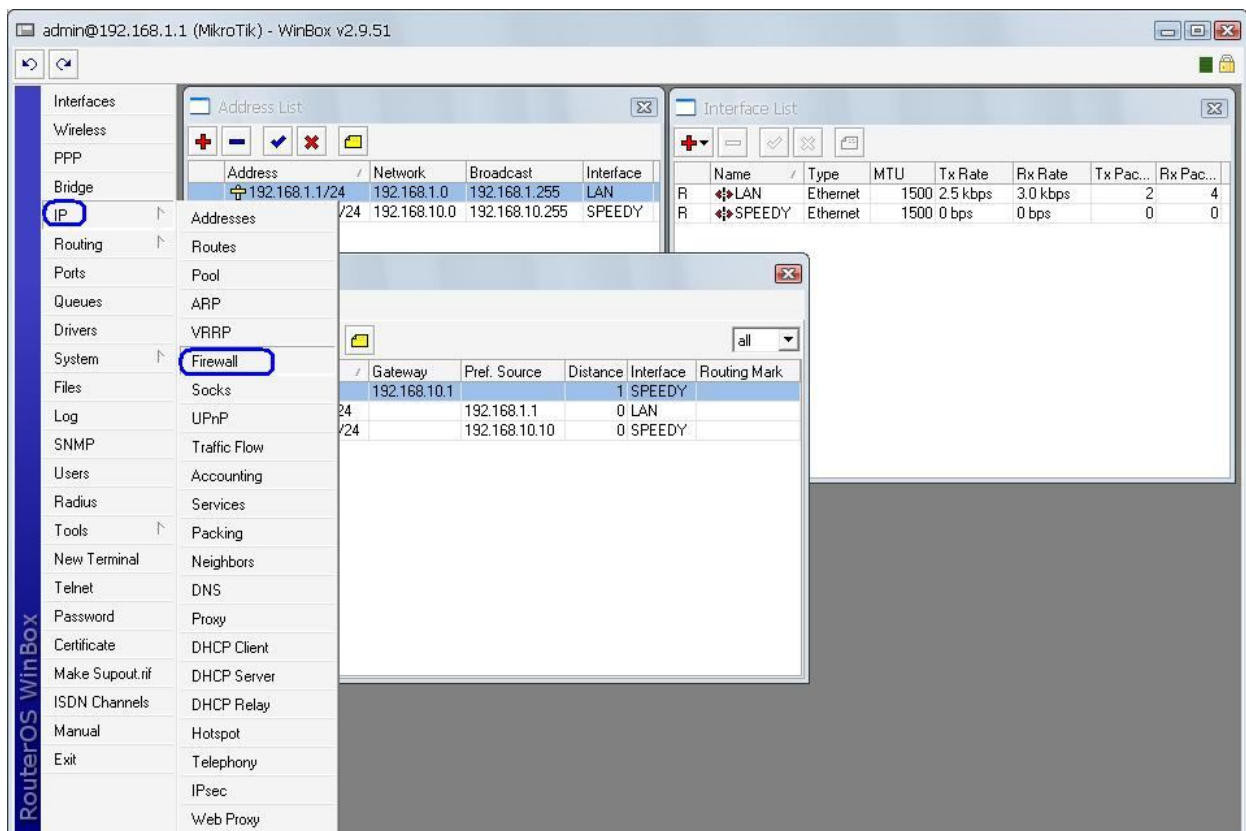
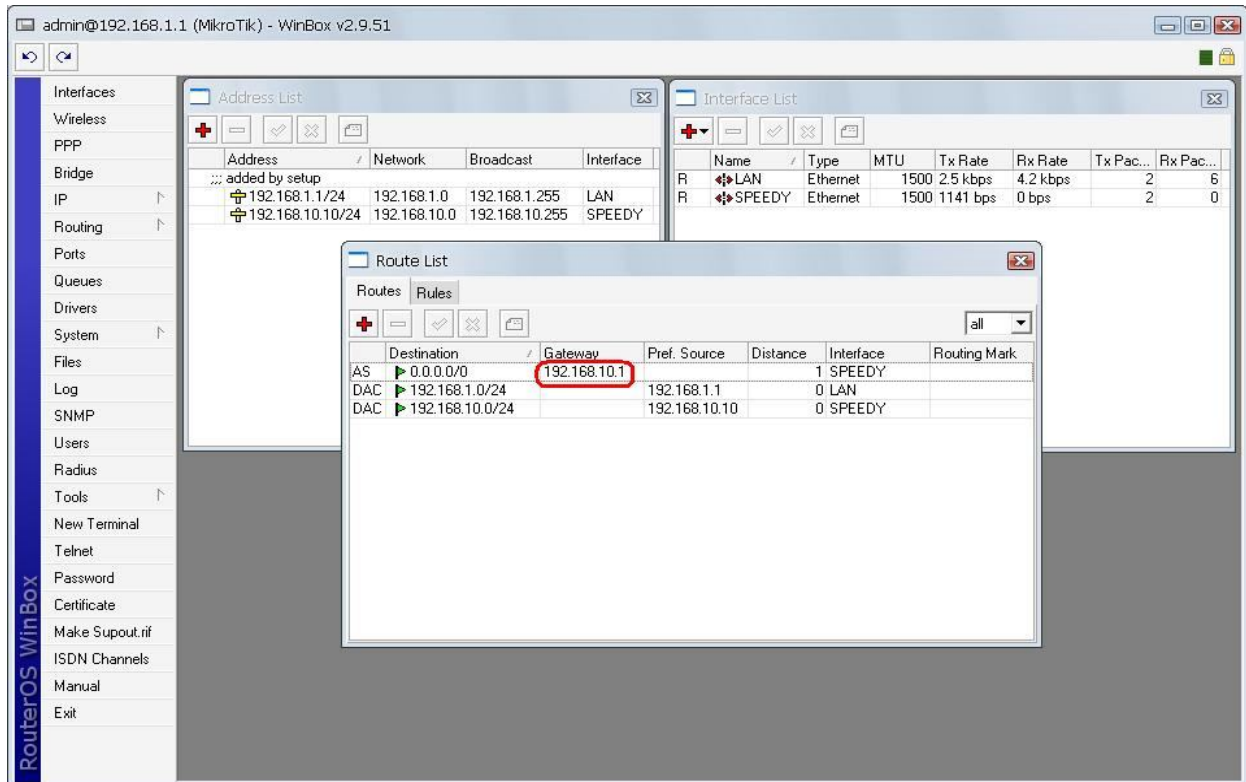




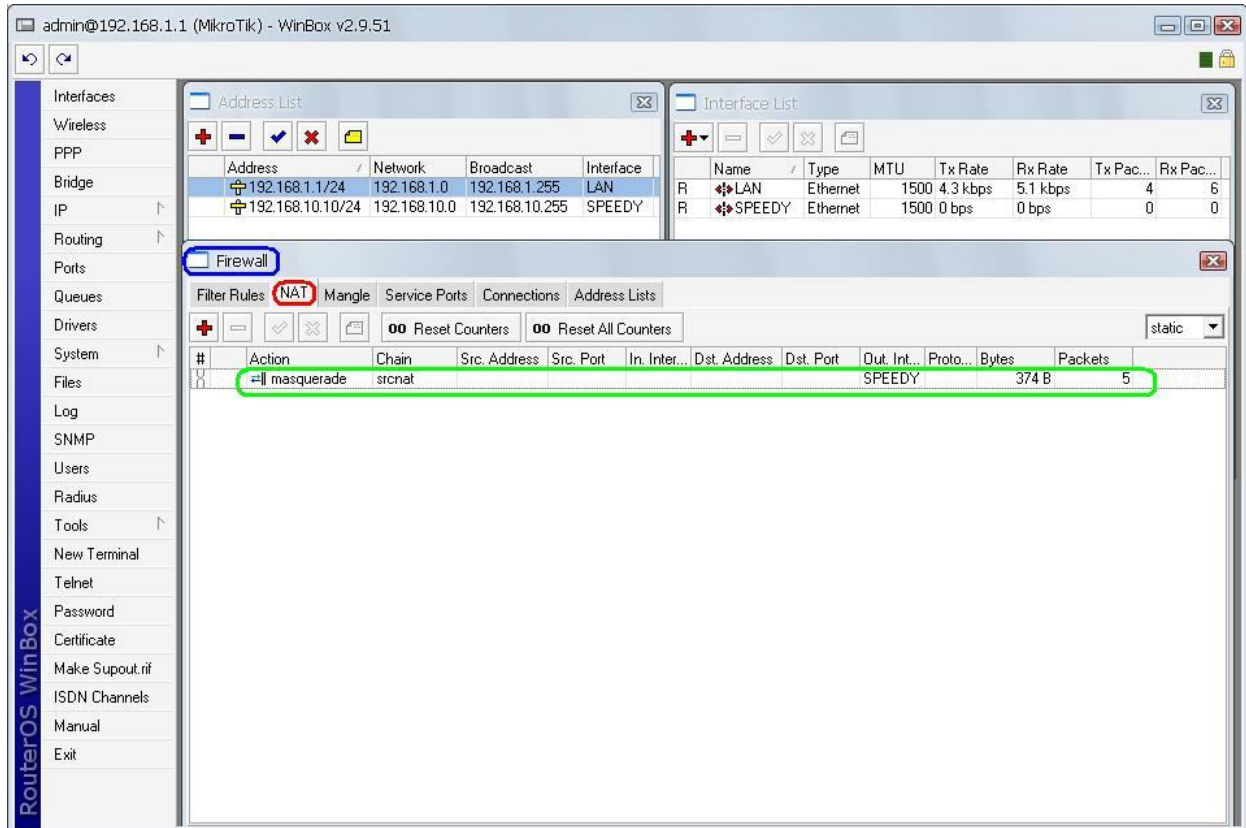
Pada menu **Routes** kita klik symbol **Plus** (New Route) lalu pada kolom input “Gateway” kita isikan dengan IP Address Modem ADSL kita, yaitu IP : **192.168.10.1**.



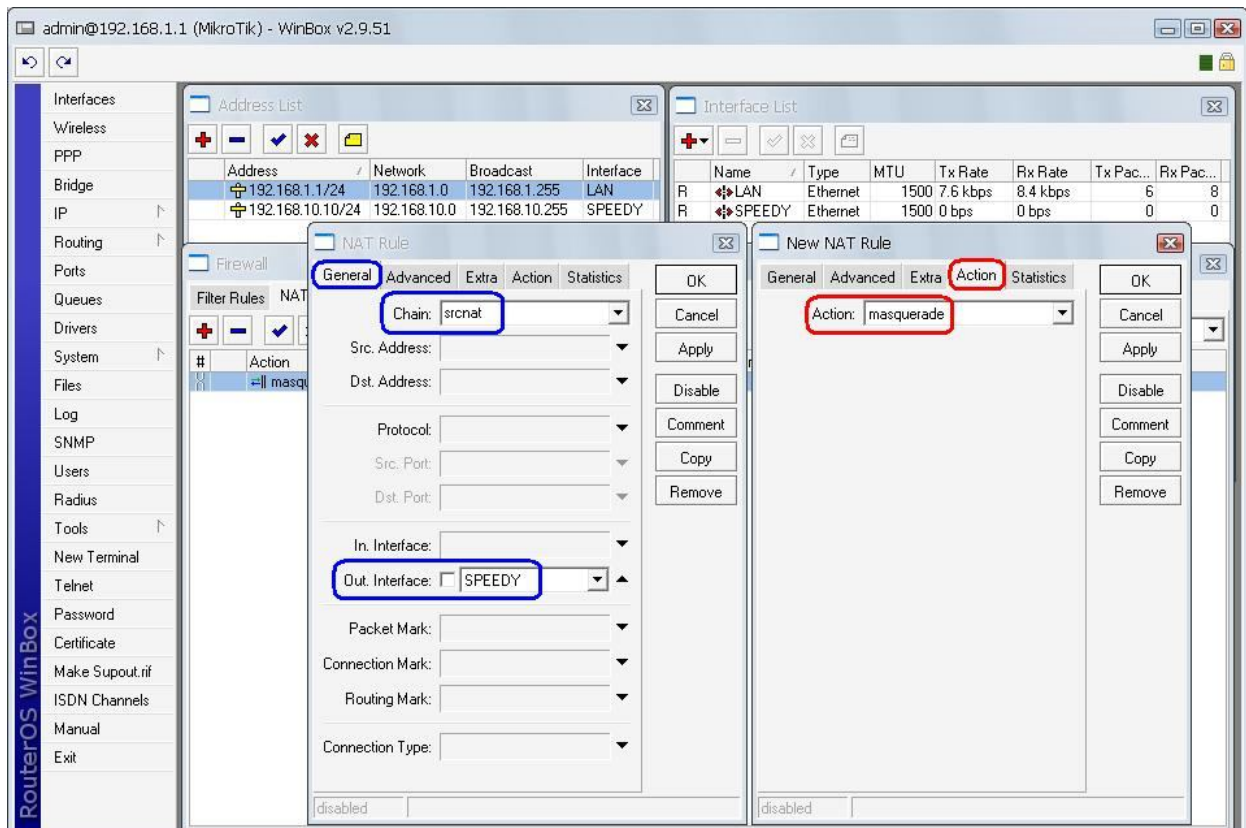
Dan hasilnya seperti pada gambar dibawah ini :

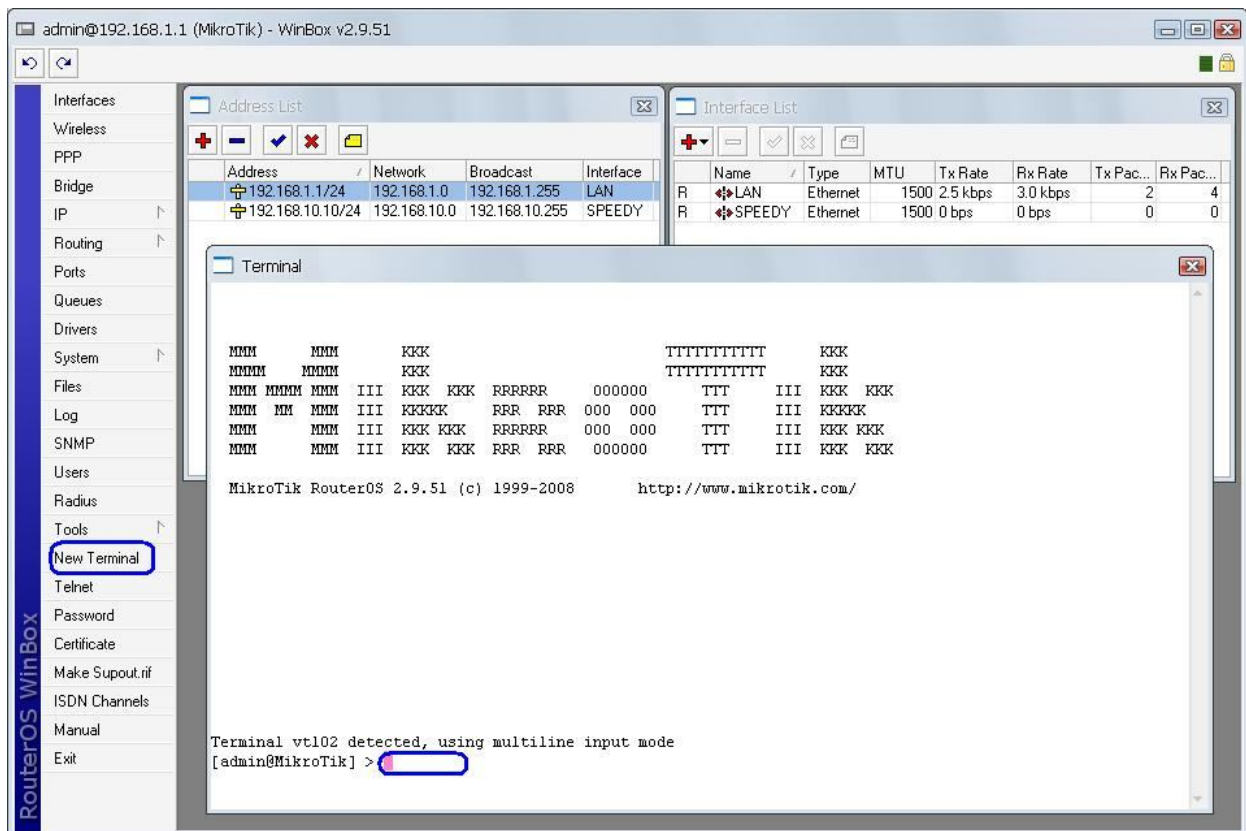


Selanjutnya kita cek setting **"Firewall"** -> **"NAT"**. Setting ini telah kita lakukan dari WebBox.

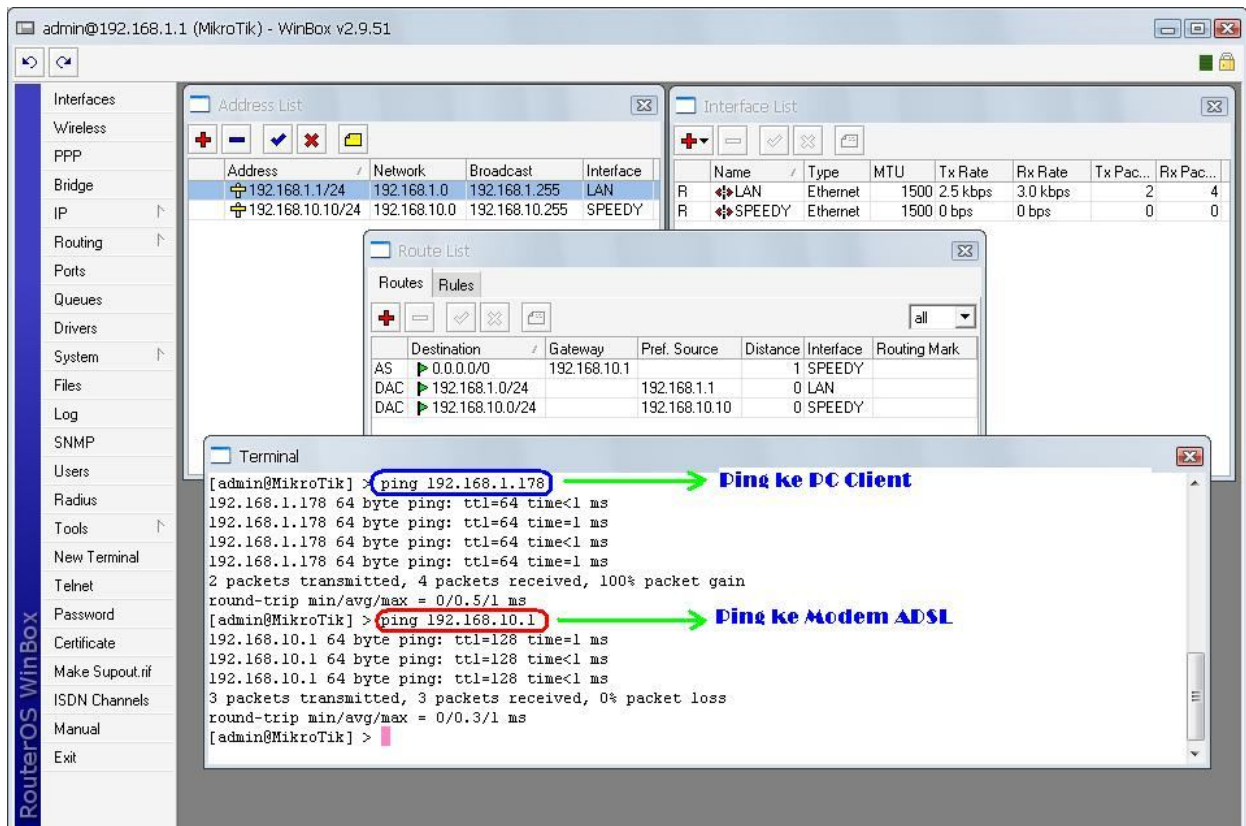


Jika kita lakukan setting dari Winbox, maka settingnya seperti pada gambar dibawah ini.

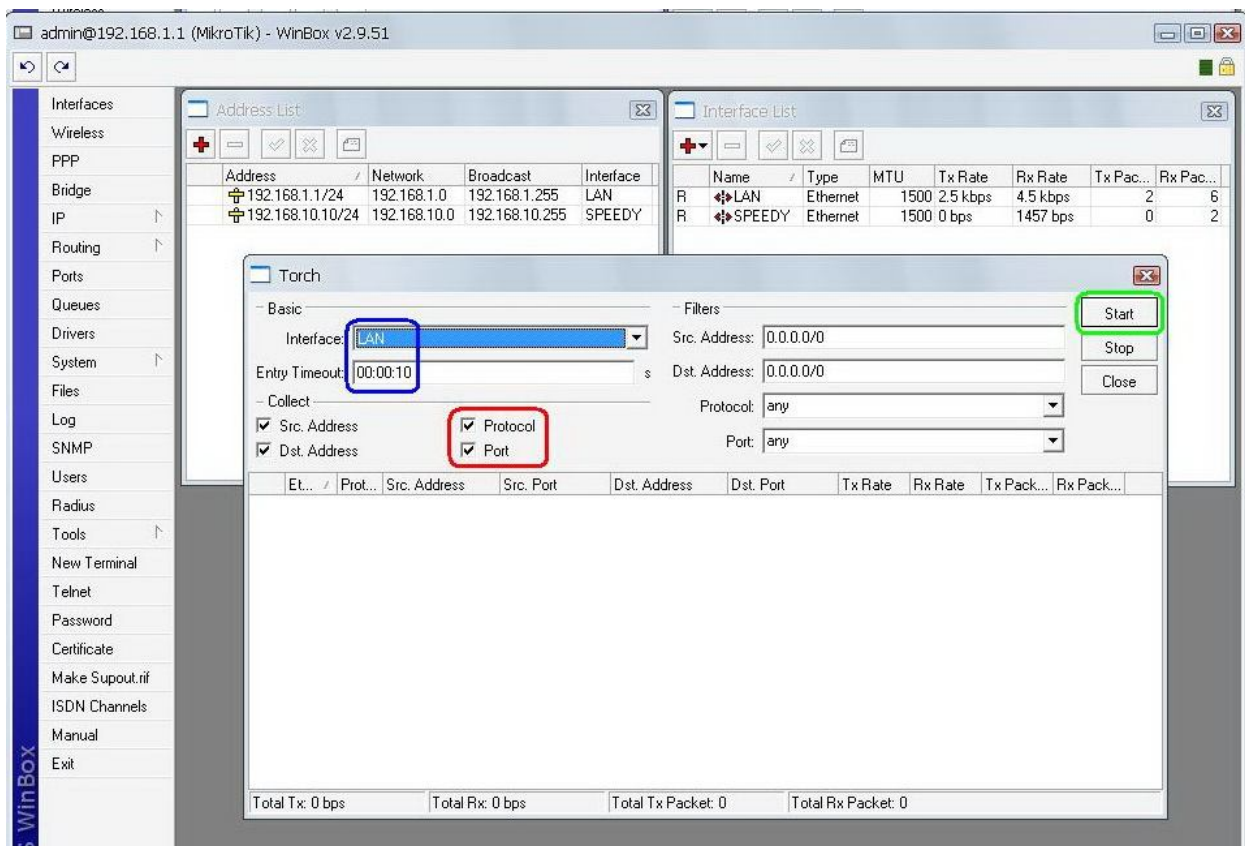
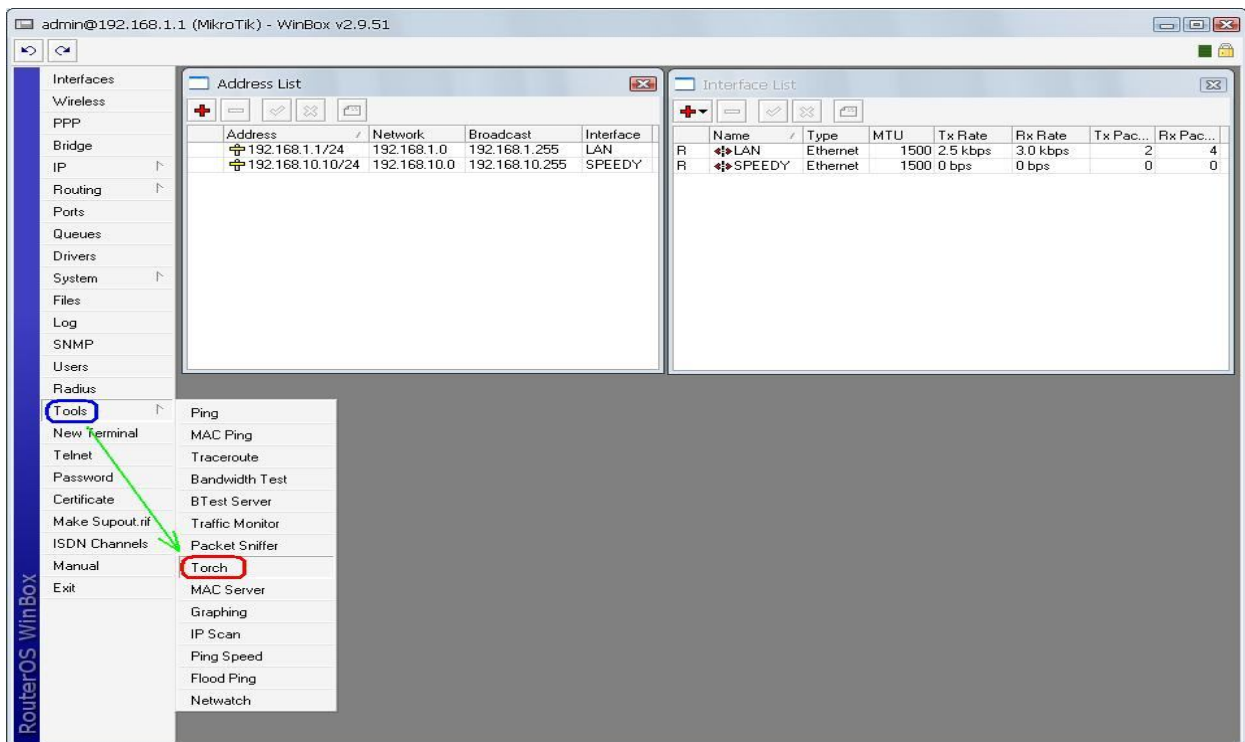


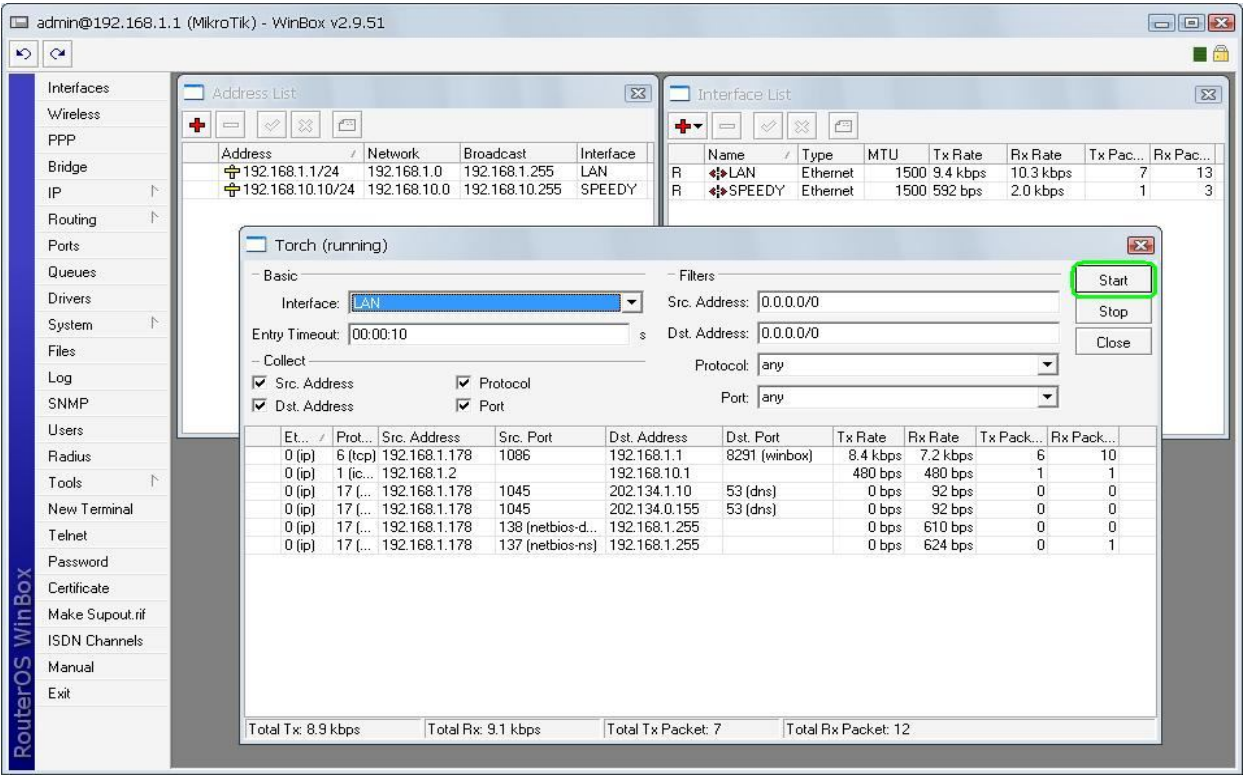


Langkah selanjutnya kita lakukan test Ping koneksi dari **Winbox** -> **Terminal**. Test Ping juga kita lakukan untuk menguji koneksi dari PC Client jaringan LAN ke kedua interface Mikrotik maupun ke IP Address Modem.



Selanjutnya kita dapat menggunakan menu **"Tools"** -> **"Torch"** untuk Trafik / lalu lintas data jaringan kita yang melewati Mikrotik....



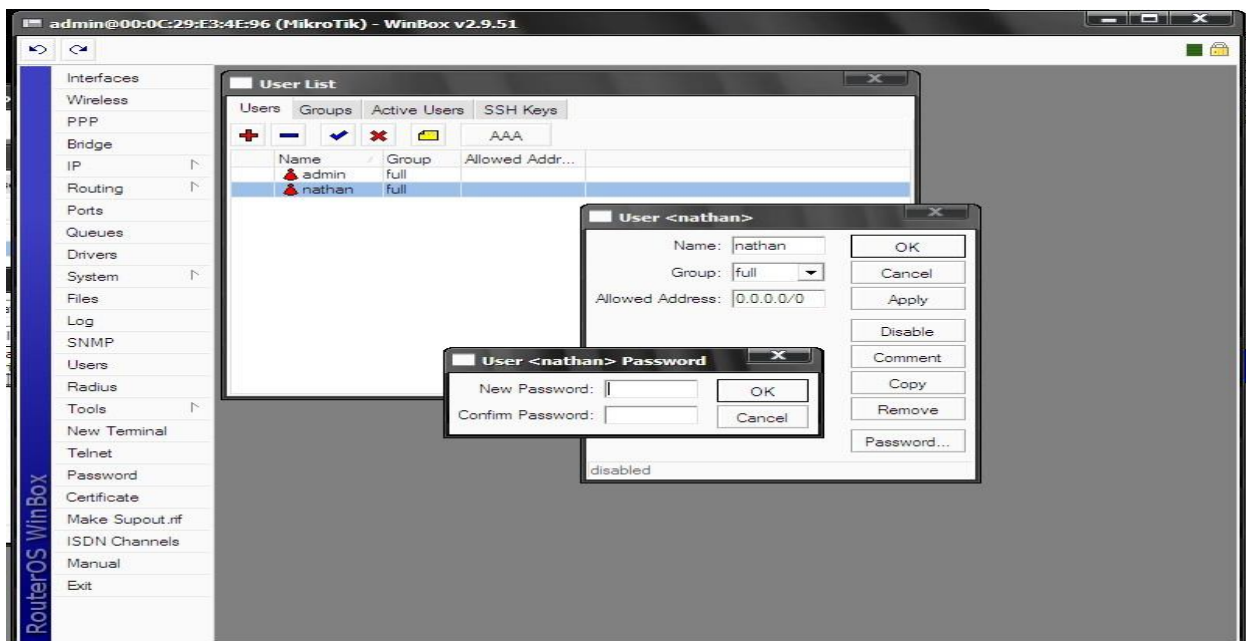
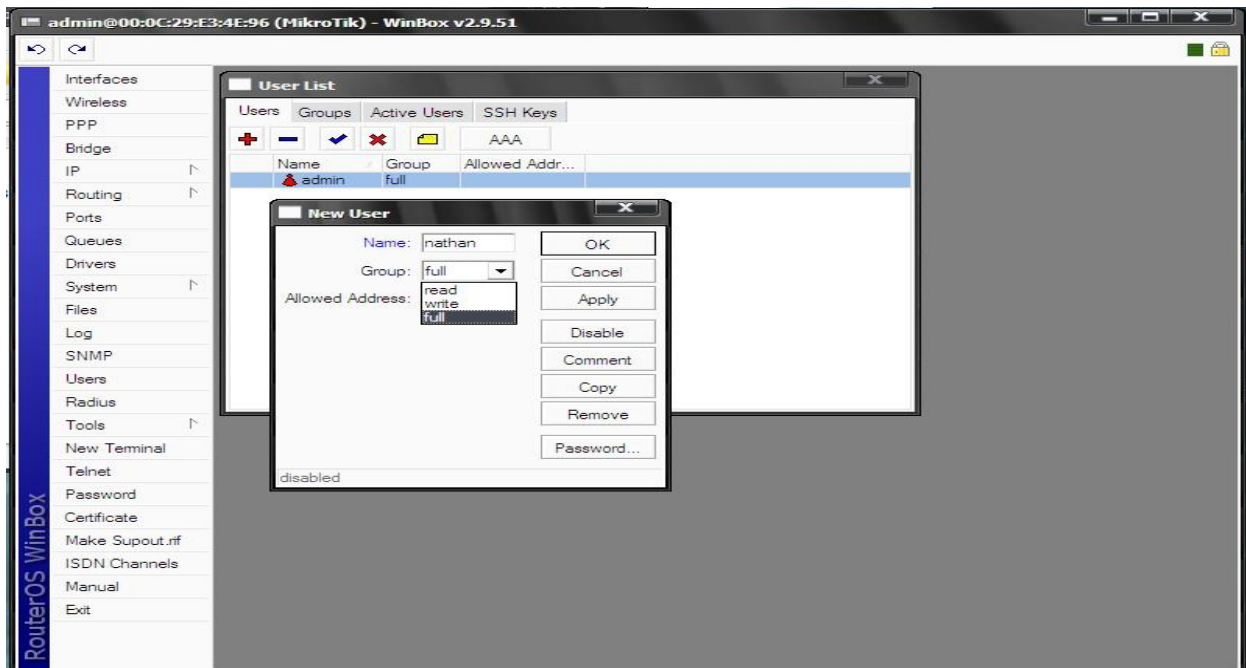


BAB 5

MANAGING USER MIKROTIK

Tentang Firewall Mikrotik

Pengaturan User dalam **Mikrotik** sangat mudah, akses ke Mikrotik dapat dari IP Address mana saja maupun dari IP Address tertentu saja. Pengaturan atau Rule-nya dibagi menjadi Full Akses, Read only dan write only. Manajemen User ini



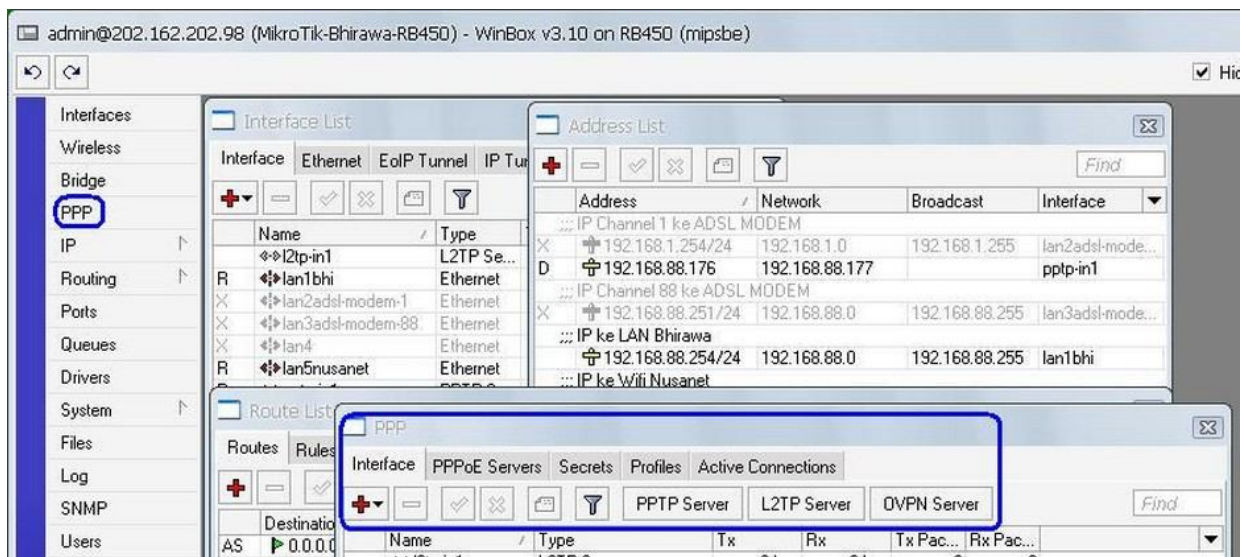
BAB 6

KONFIGURASI MIKROTIK VPN SERVER

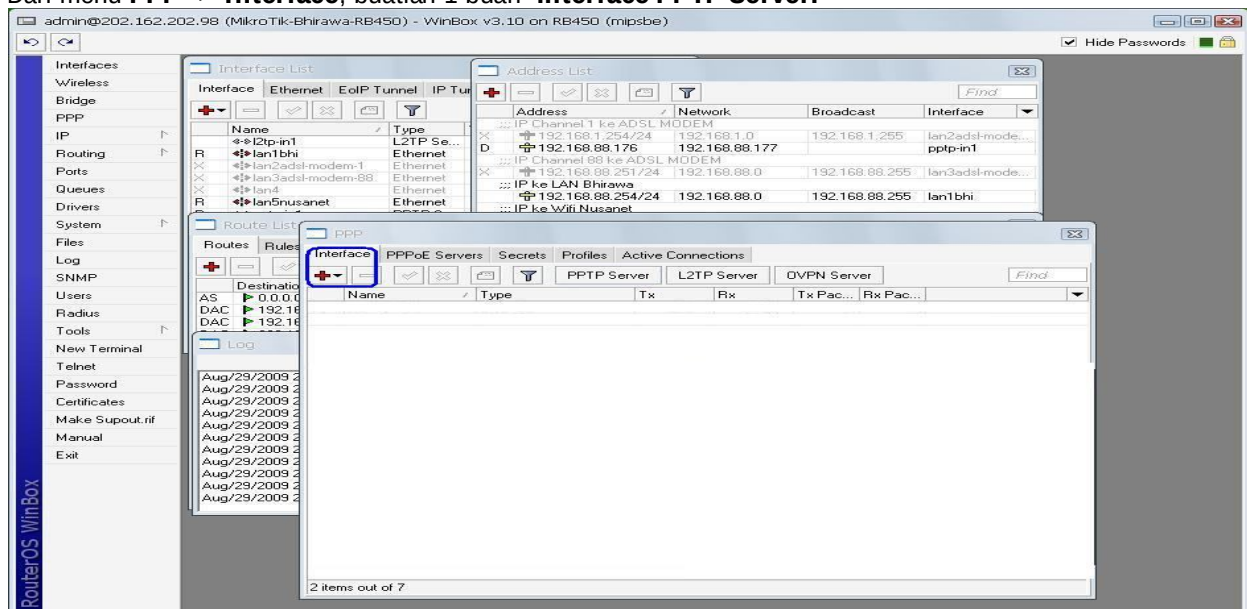
Dalam pembuatan Mikrotik VPN Server ini, tahapan-tahapan yang akan kita lakukan, yaitu :

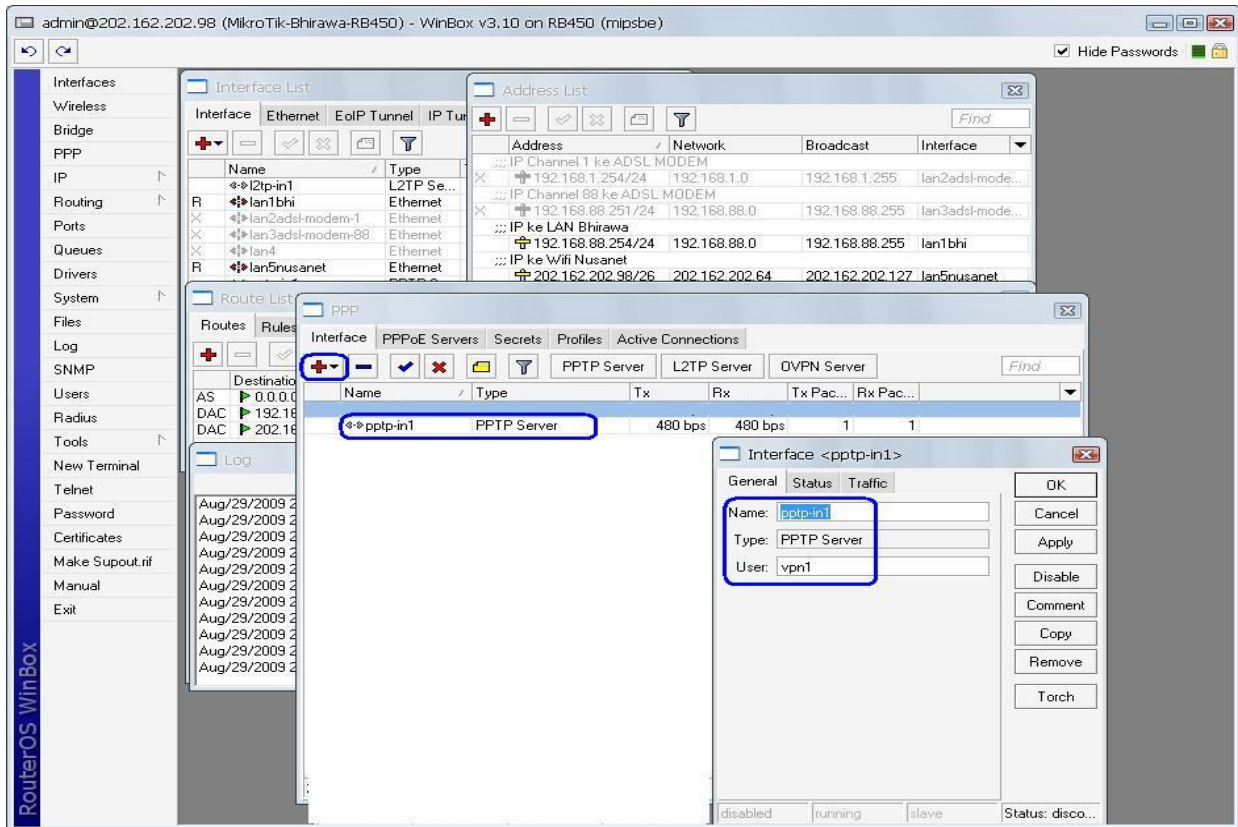
1. Step Mengaktifkan Fitur PPTP Server.
2. Step Membuat Interface PPTP in.
3. Step Membuat Authenticated User / VPN User.

Langkah – langkah pertama untuk membuat **VPN Server Mikrotik** adalah dari Winbox lalu masuk ke menu **PPP**, lihat gambar dibawah ini :

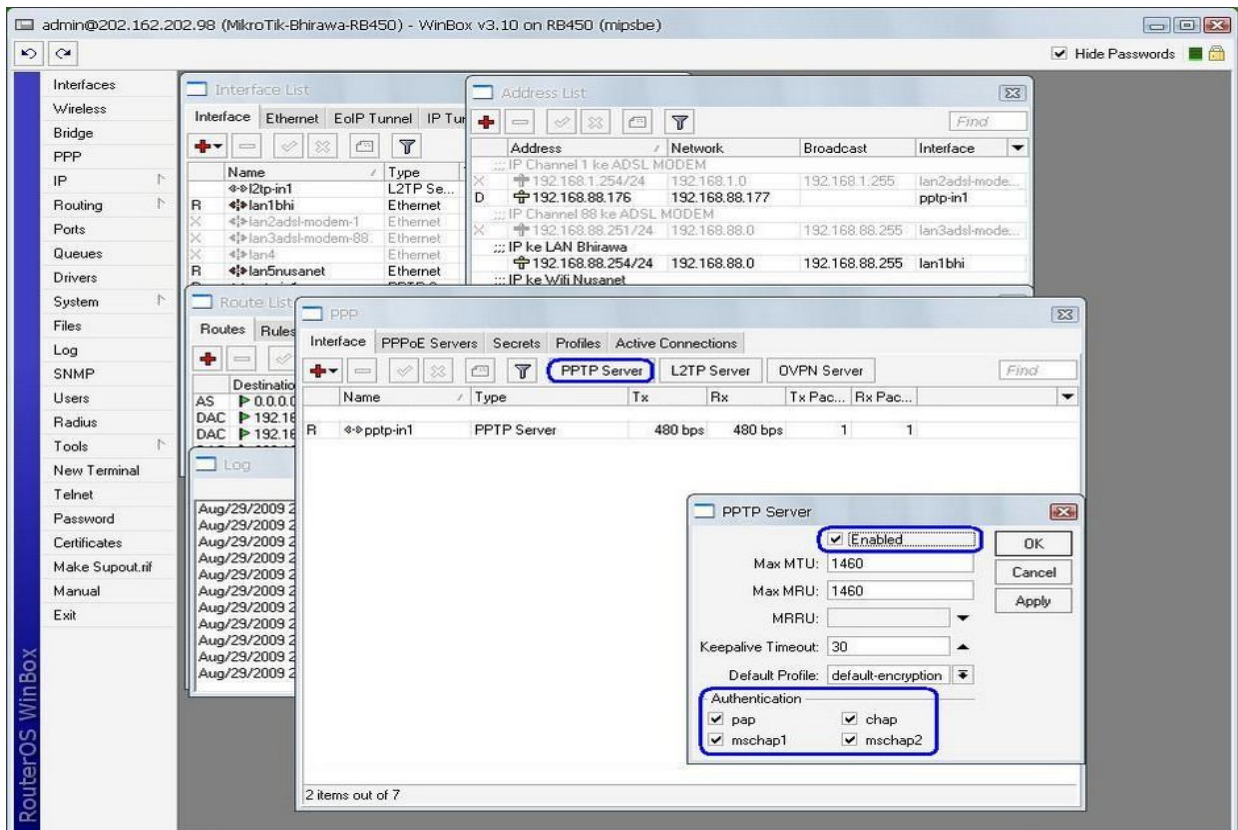


Dari menu **PPP -> Interface**, buatlah 1 buah **interface PPTP Server**.

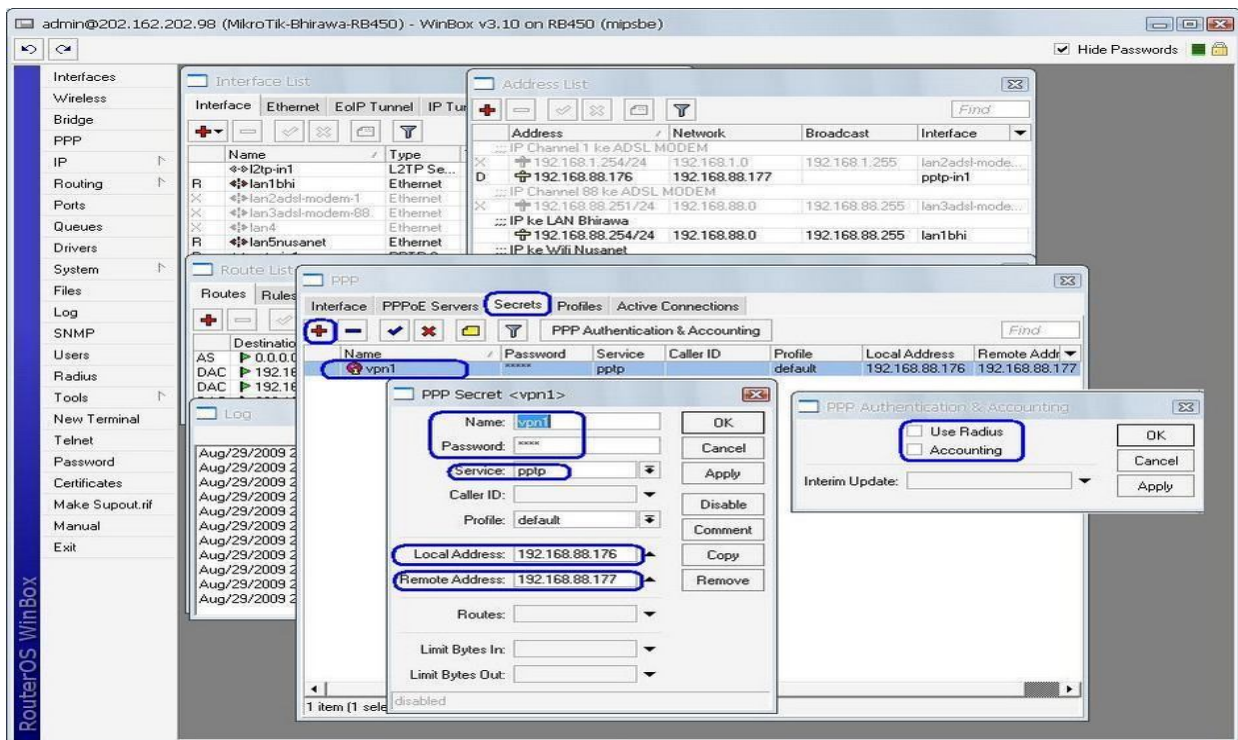




Selanjutnya kita aktifkan fitur **PPTP Server** dengan memberikan Checkmark "ENABLED".



Langkah selanjutnya kita buat sebuah Account User yang di autentikasi untuk koneksi ke VPN Server kita.



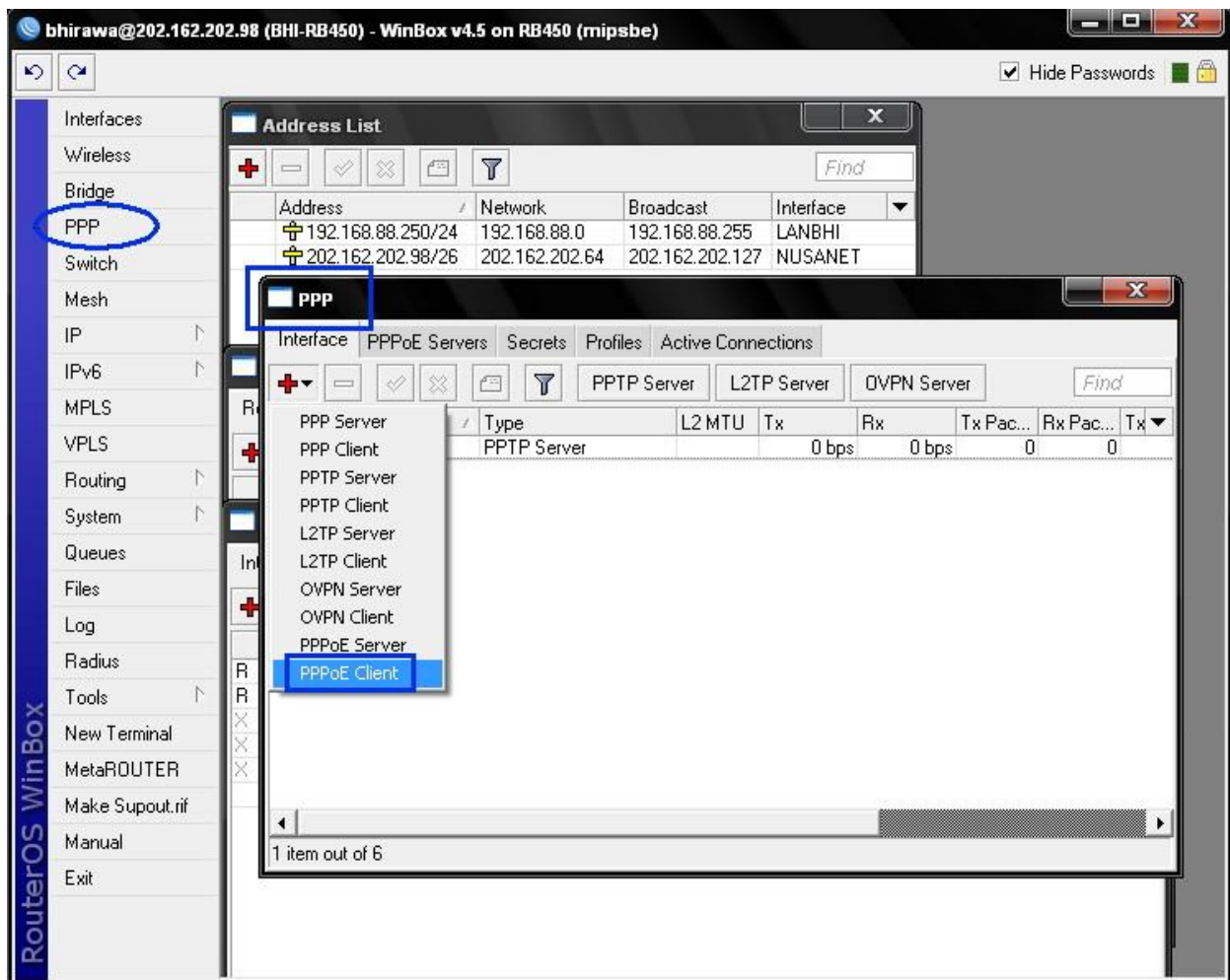
BAB 7

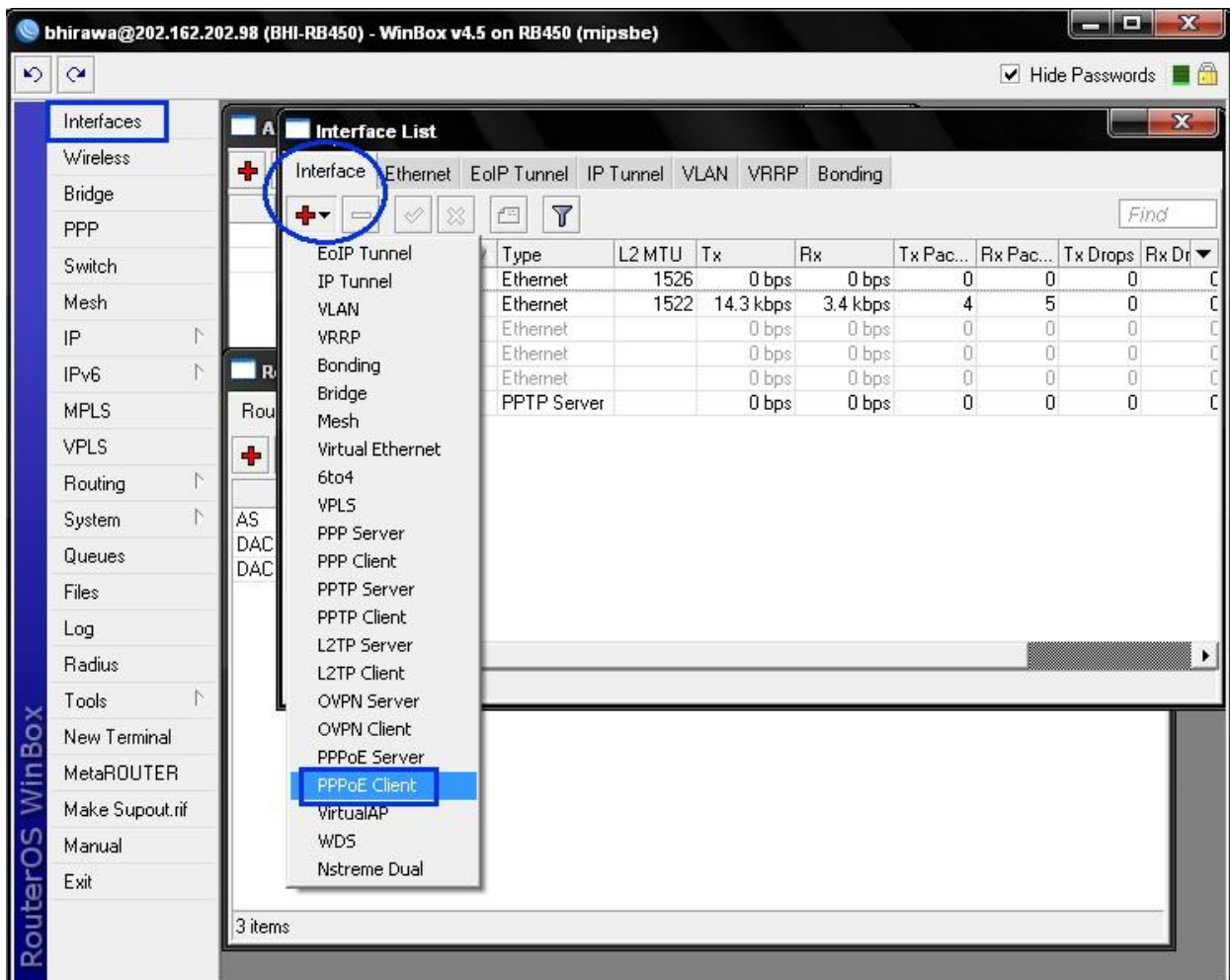
KONFIGURASI MIKROTIK VPN CLIENT

Setelah **Mikrotik VPN Server** telah selesai kita buat dan berfungsi dengan baik, maka selanjutnya kita akan melakukan konfigurasi **Mikrotik VPN Client**. Tahapan yang harus kita lakukan ada 2 yaitu :

1. Prepare **Dial Out PPPoE Client** (untuk mendapatkan IP Public pada VPN Mikrotik VPN Client kita)
2. Konfigurasi **VPN Client / PPTP Client**.

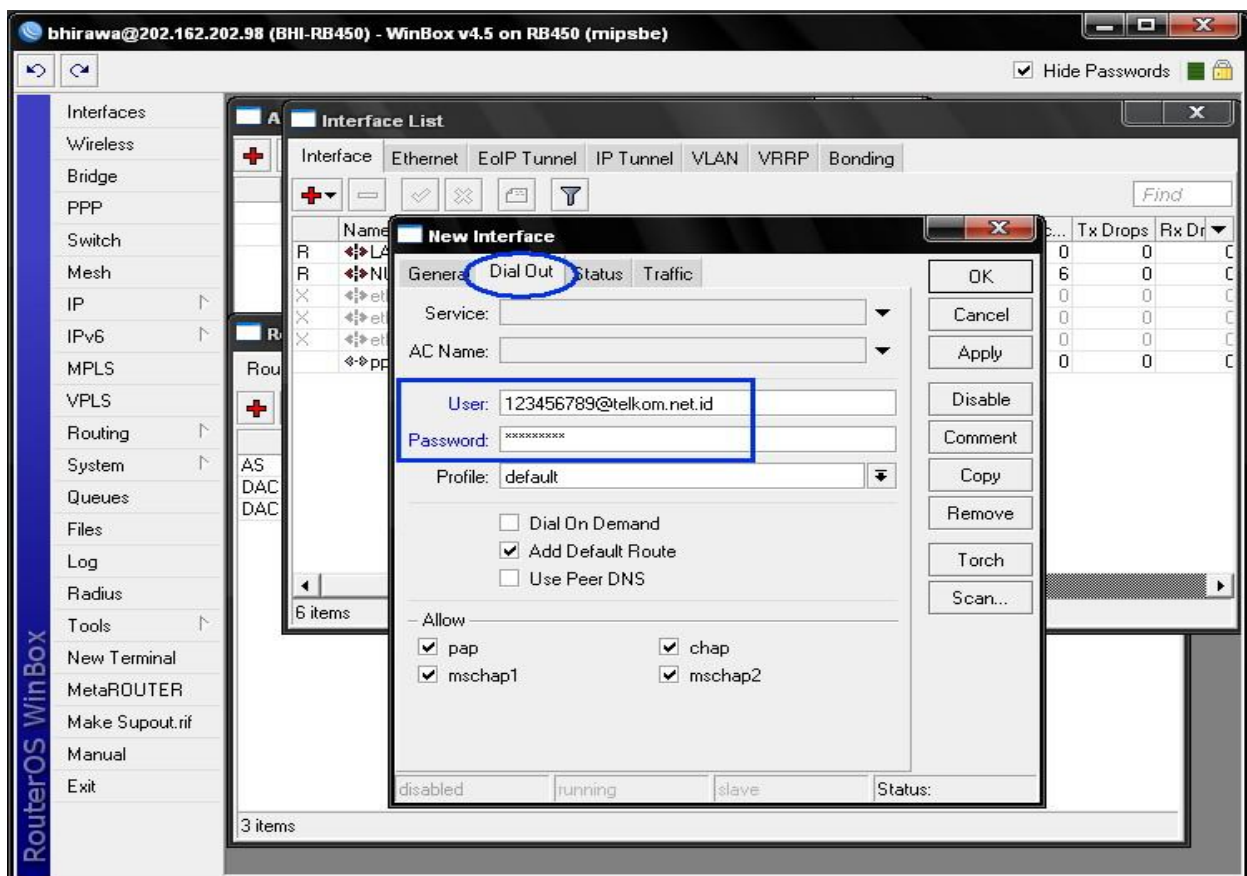
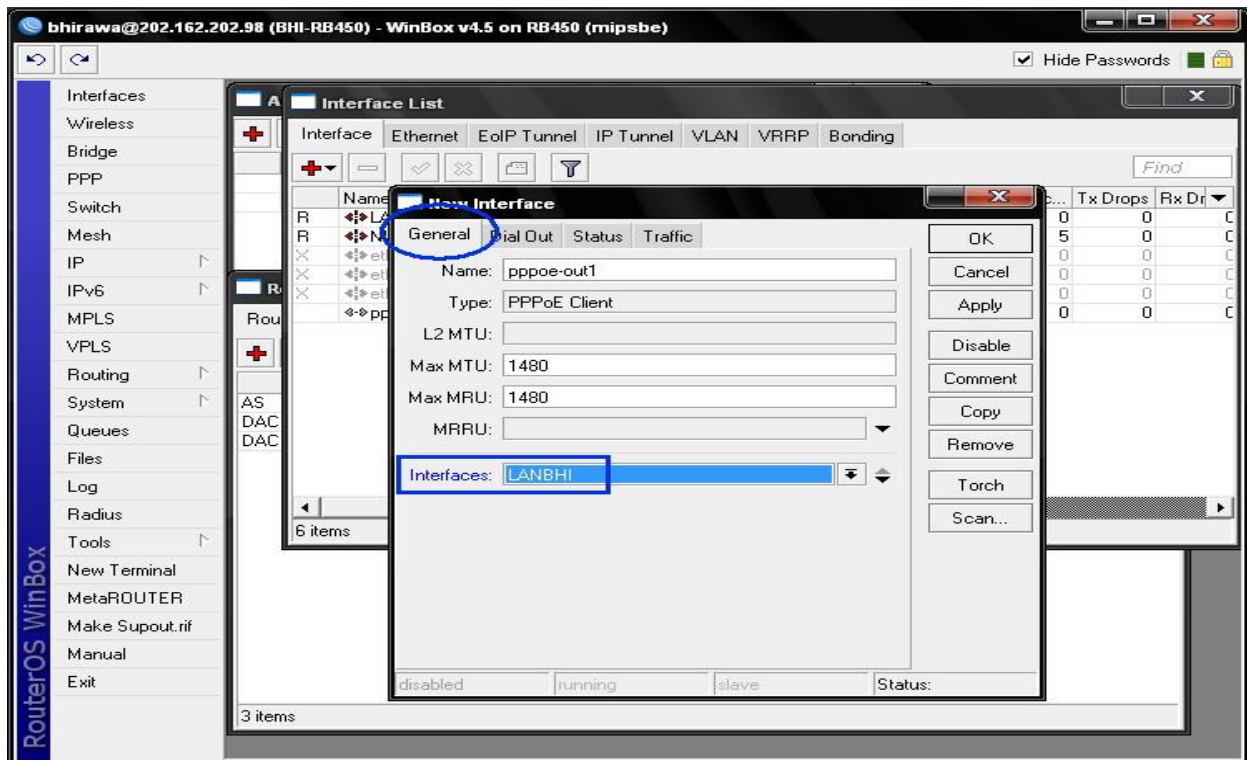
Caranya membuat **Dial Out PPPoE Client** adalah melalui menu **Interface** lalu pilih **Add New Interface PPPoE Client** atau melalui menu **PPP Interface** lalu pilih **Add New Interface PPPoE Client**.





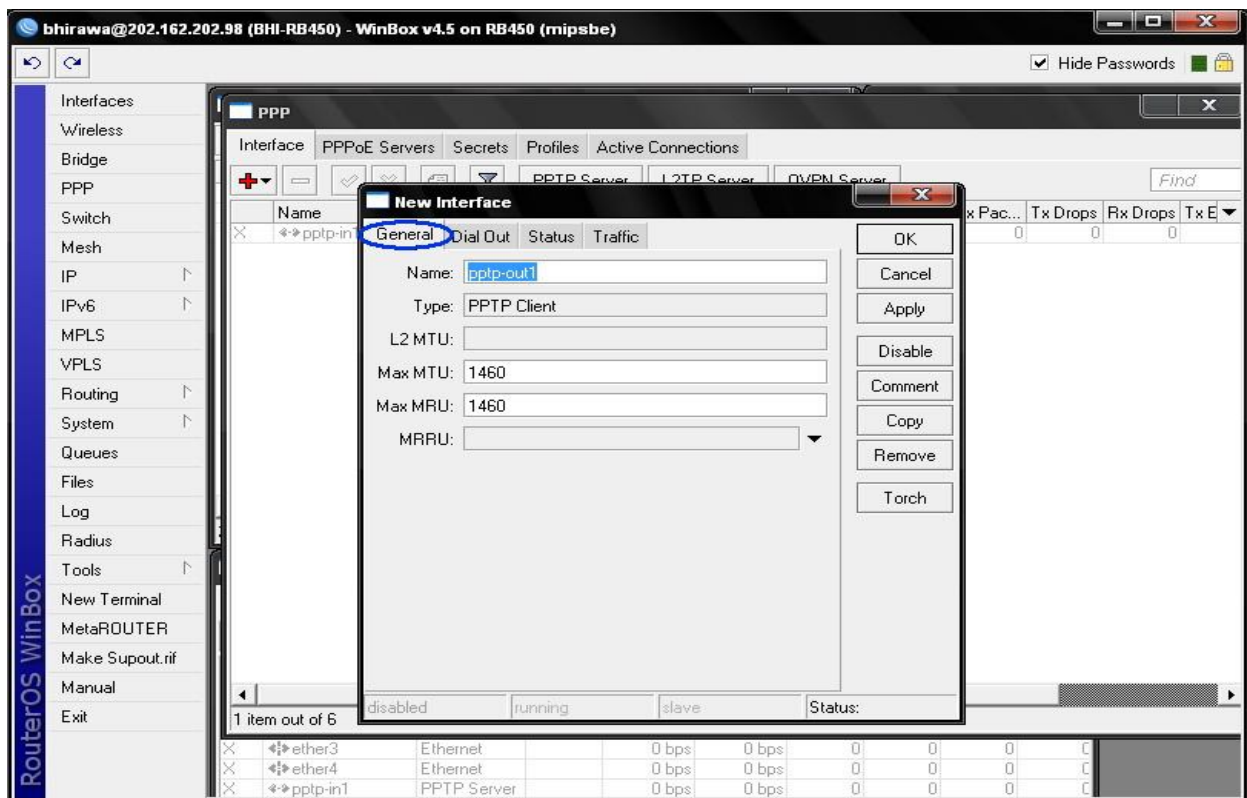
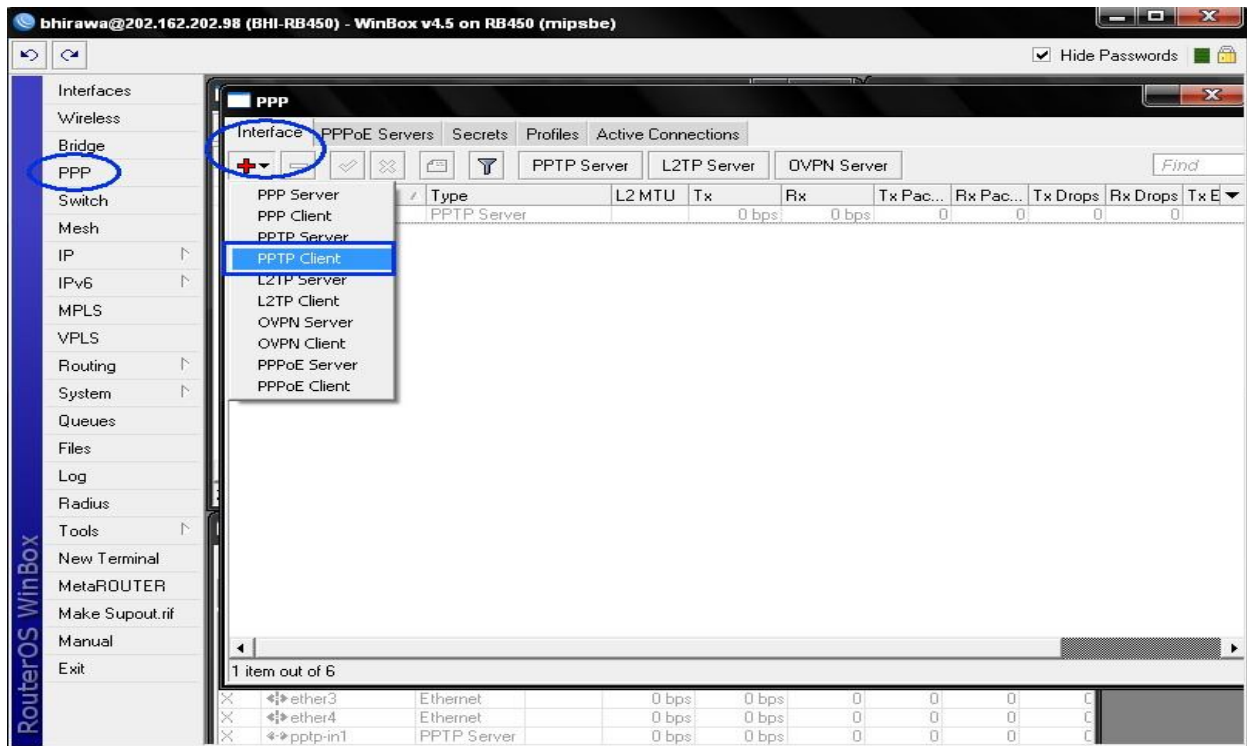
Selanjutnya pada Option **General**, kita tentukan **Nama Interface PPPoE Client** dan menentukan **Interface Ethernet** mana yang kita gunakan utk mengakses Modem ADSL Bridge yang telah kita konfigurasi sebelumnya.

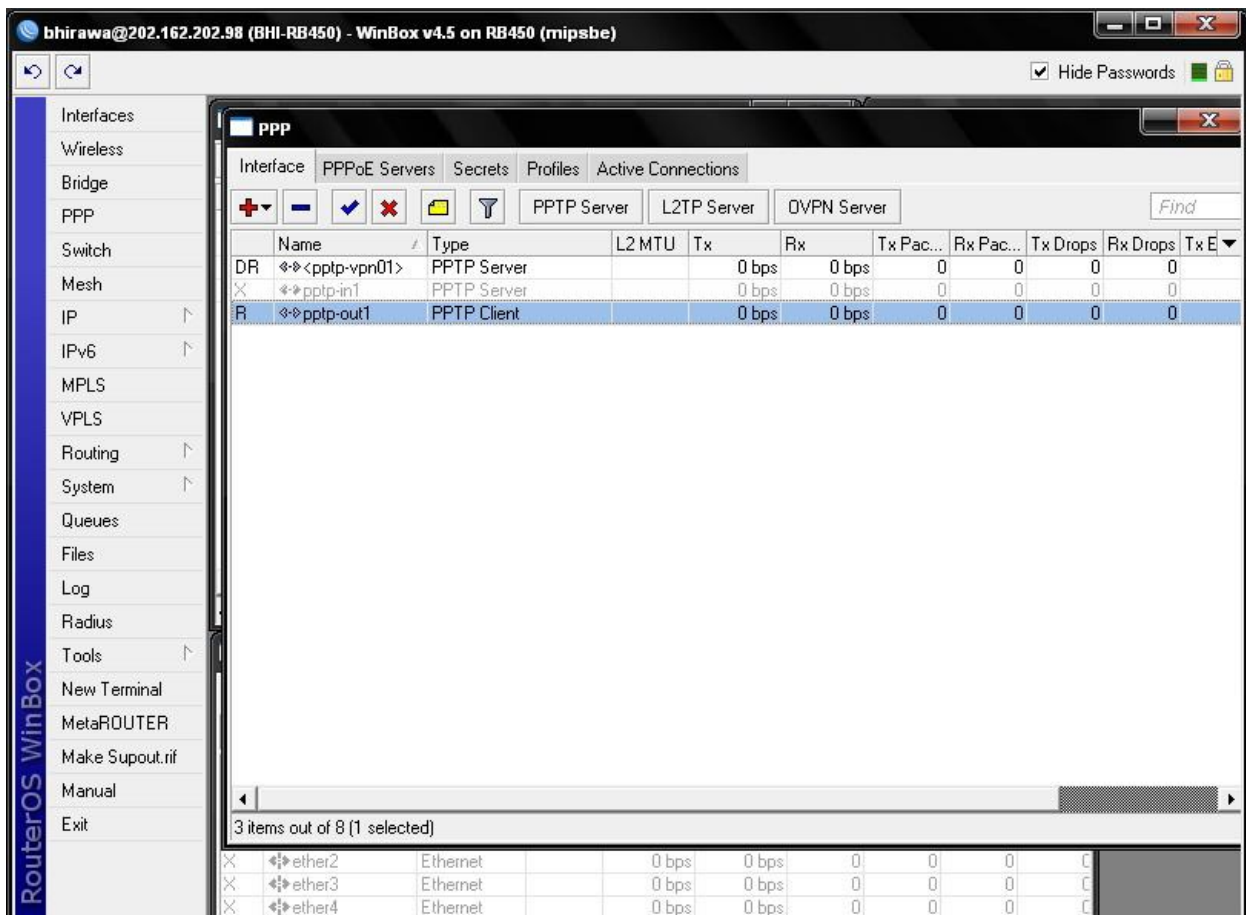
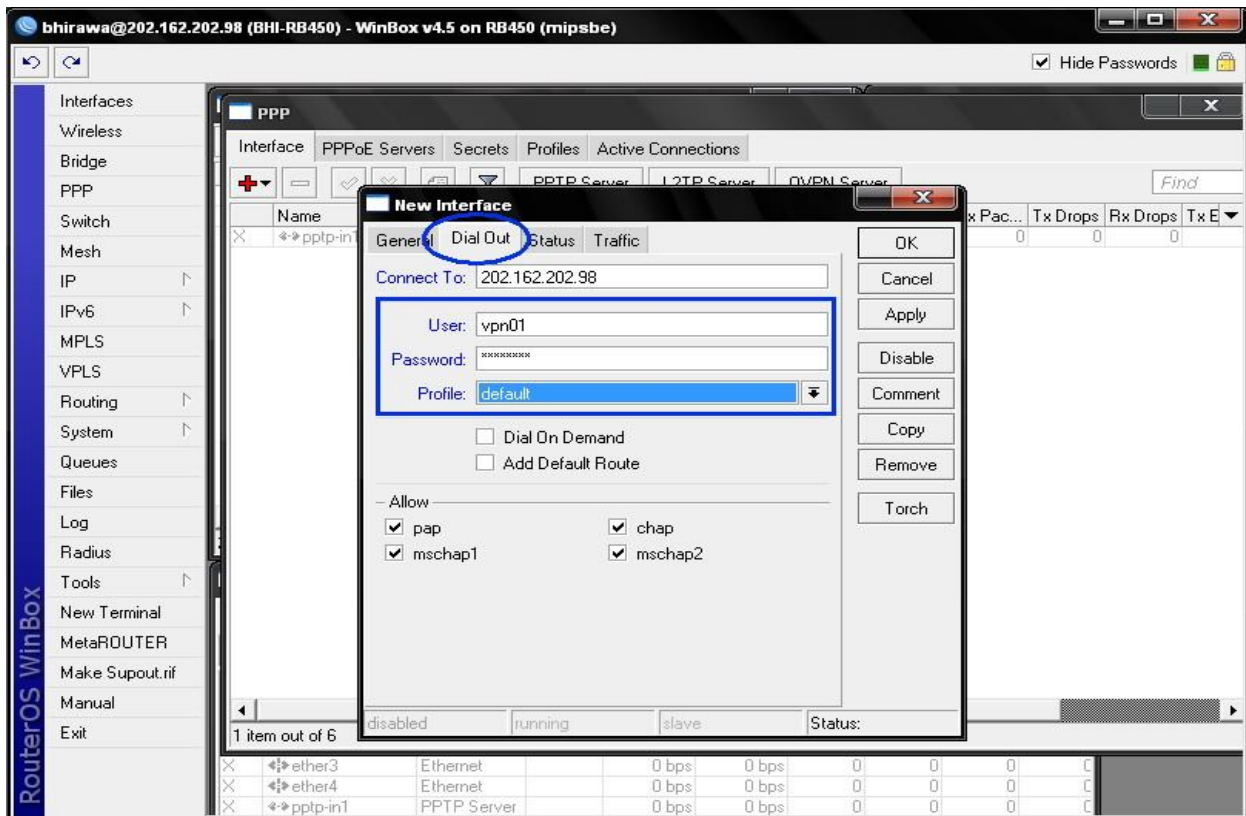
Setelah itu, pada Option **Dial Out** kita harus memasukkan **Username** dan **Password Speedy** kita. Jika Username dan Password kita benar, begitu kita klik OK maka koneksi akan langsung di lakukan dan selanjutnya Mikrotik akan mendapatkan IP Public Speedy.



Sampai sini tahap **Prepare VPN Client** telah selesai selanjutnya tahap konfigurasi **VPN Client / PPTP Client**.

Pada tahap konfigurasi **VPN Client / PPTP Client** ini kita akan membuat sebuah **Interface PPTP Client**. Caranya adalah melalui menu **PPP Interface** lalu pilih **Add New Interface PPTP Client** seperti gambar dibawah ini.





BAB 8

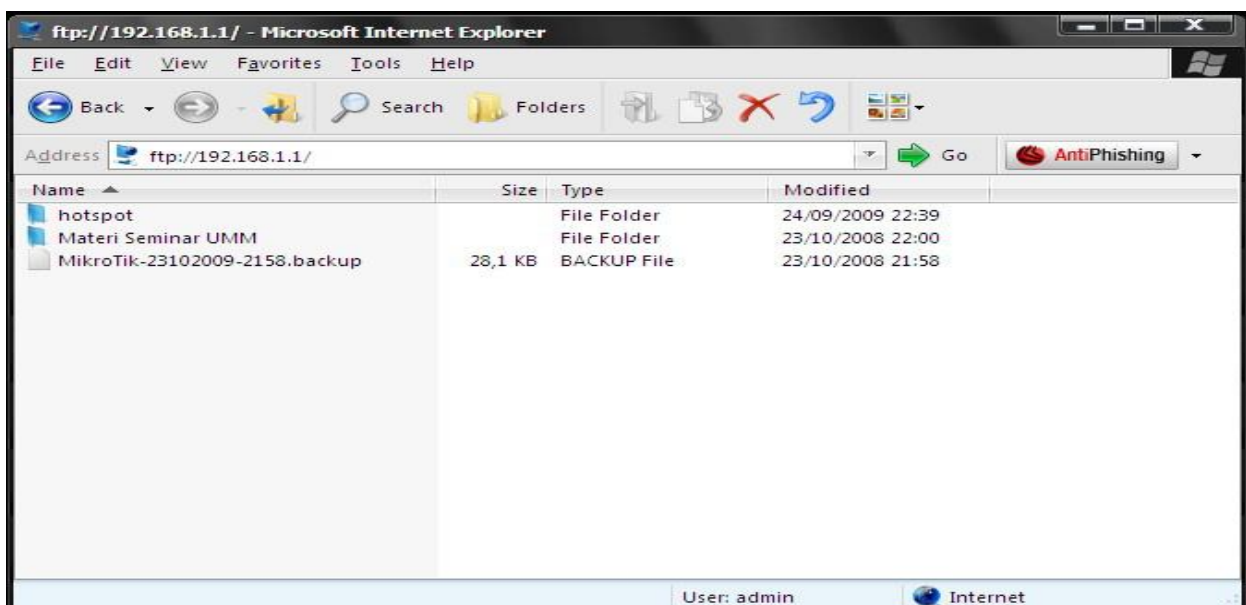
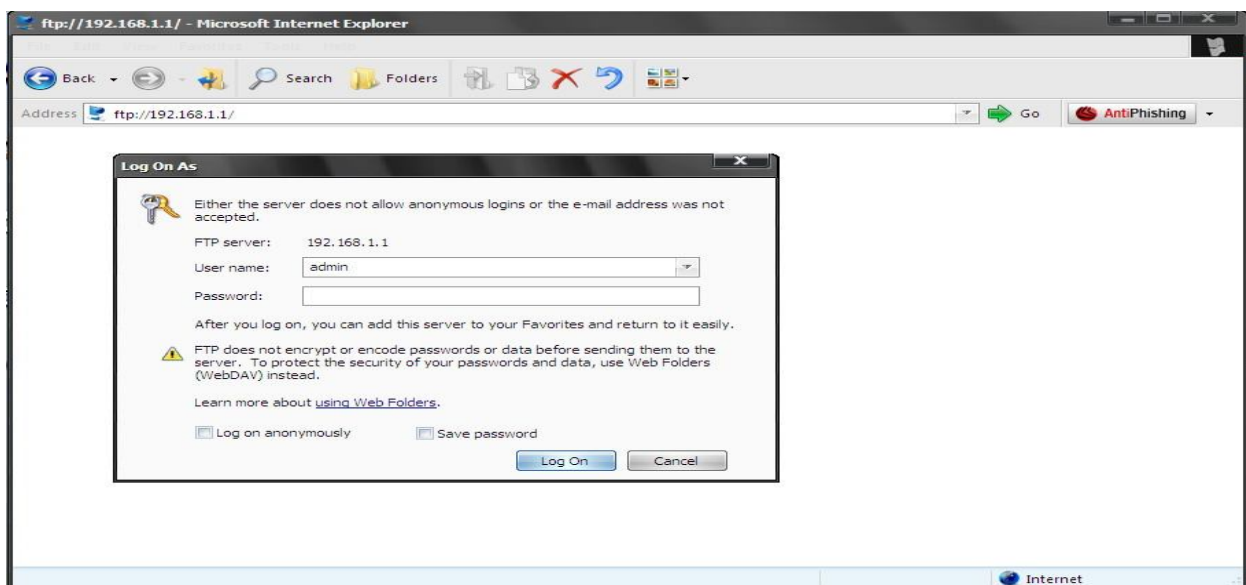
KONFIGURASI MIKROTIK FTP SERVER

Tentang FTP Server

FTP adalah Protocol yang digunakan untuk transfer file yang dapat diakses dengan mudah menggunakan Windows Explorer, Internet Explorer maupun dengan aplikasi **FTP Client**. Jika sewaktu instalasi awal **Mikrotik** kita install semua paket / modul maka secara otomatis Fitur FTP Server juga sudah aktif. User Authentikasi untuk mengakses FTP Server ini kita setting dari menu **Winbox -> User**.

Selanjutnya kita bisa coba akses menggunakan Internet Explorer dengan mengetikkan alamat akses :

ftp://ip-address-mikrotik-kita

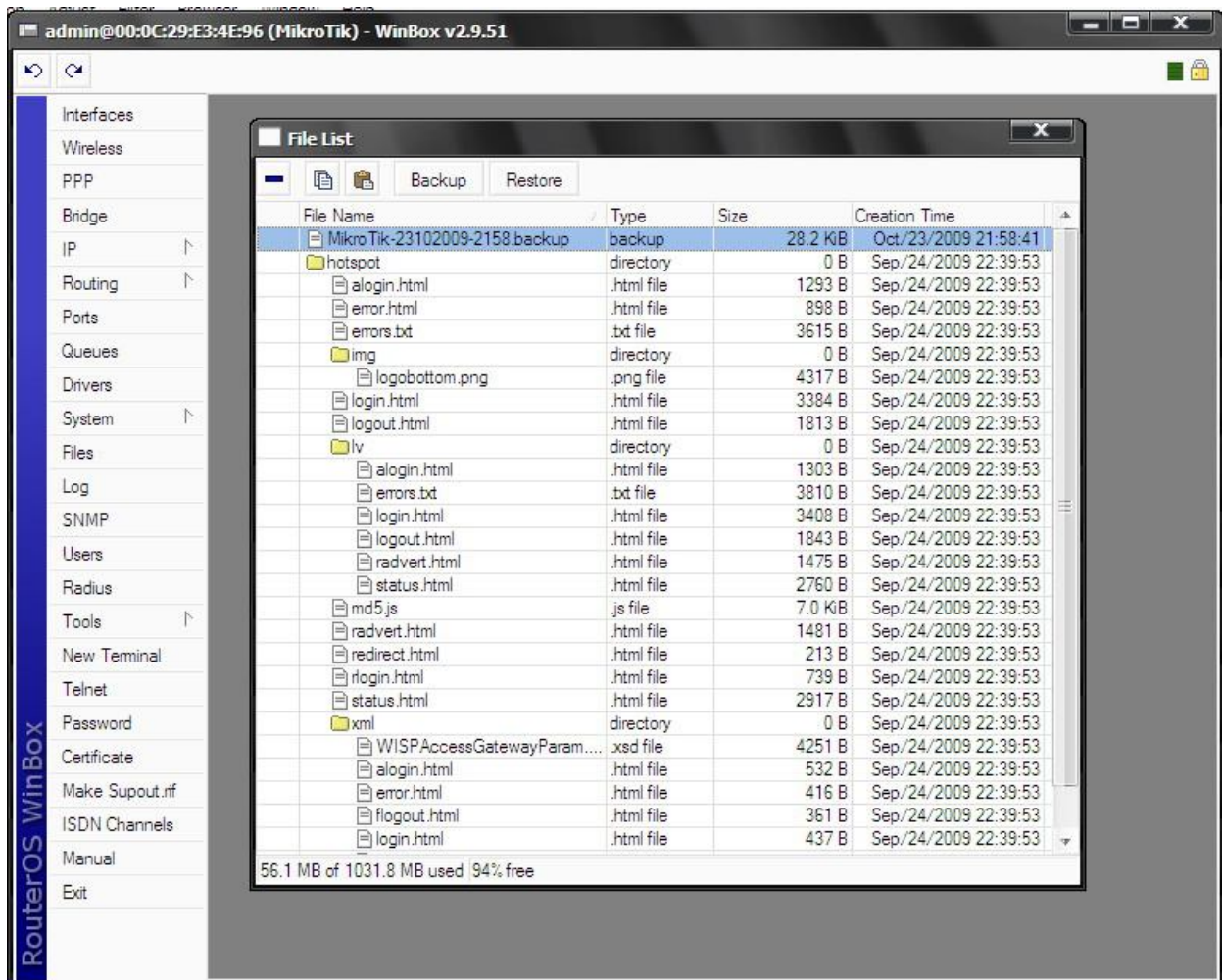


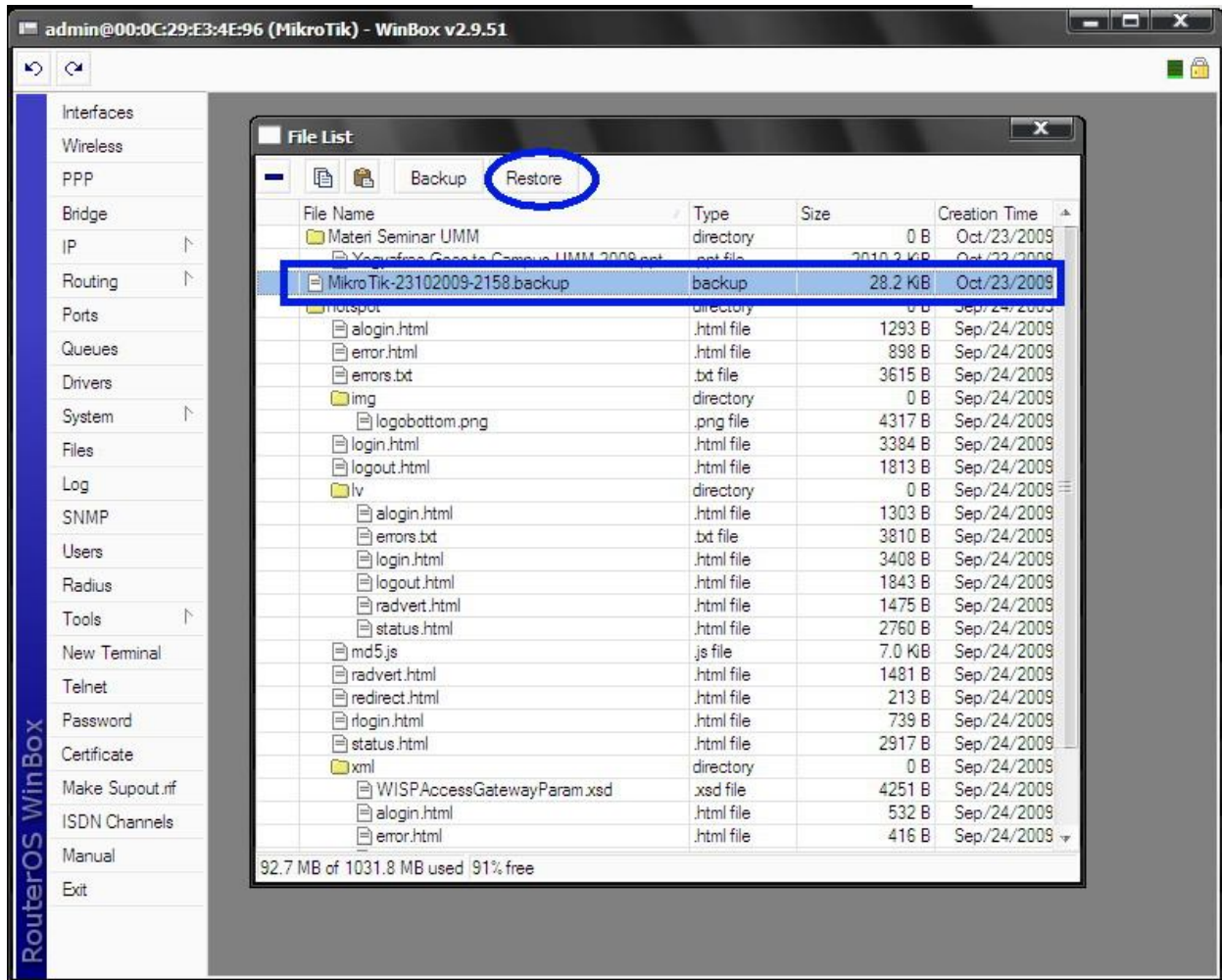
BAB 9

BACKUP DAN RESTORE KONFIGURASI MIKROTIK

Backup konfigurasi **Mikrotik** kita sangat bermanfaat jika suatu saat Mikrotik kita mengalami kerusakan sehingga kita harus Install Ulang System Mikrotik. Atau juga kita ingin melakukan Restore dari Backup konfigurasi Mikrotik kita untuk me-refresh konfigurasi setelah kita lakukan berbagai perubahan atau terjadi kesalahan konfigurasi. Begitu juga jika ingin membuat Mikrotik lain dengan konfigurasi yang Identik sehingga kita bisa membuat Mikrotik Router dalam waktu yang cepat.

Untuk melakukan Backup konfigurasi ini dari **Winbox** -> **Files**. Setelah kita klik Backup maka akan terlihat sebuah file baru dengan identifikasi **nama file dan tanggal + waktu** proses backup. Selanjutnya kita bisa menyimpan file backup konfigurasi ini dengan cara meng-copy file tersebut dari Mikrotik ke Disk local PC kita. Caranya bisa menggunakan copy via FTP ataupun menggunakan Winbox (gunakan Drag 'n Drop).





~~~~~oo00000#00000o~~~~~