

DAFTAR ISI :

1. Konfigurasi Dasar

Lab 1. Mengakses RouterBoard
Lab 2. Menginstall Mikrotik RouterOS
Lab 3. Mengkoneksikan RouterBoard dengan PC
Lab 4. Manajemen User di Mikrotik
Lab 5. Merubah Router Identity
Lab 6. Merubah Tanggal dan Waktu
Lab 7. Disable , Enable , Uninstall Packet
Lab 8. Upgrade dan Downgrade Packet
Lab 9. Hard Reset Configuration
Lab 10. Soft Reset Configuration
Lab 11. Koneksi Internet
Lab 12. NTP Client
Lab 13. NTP Server
Lab 14. ARP (Address Resolution Protocol) Static
Lab 15. Backup & Restore
Lab 16. Export & Import
Lab 17. Install Ulang Routerboard dengan Netinstall

2. Manajemen Network

Lab 18. DHCP Server
Lab 19. Pengelolaan DHCP Server 1
Lab 20. Pengelolaan DHCP Server 2
Lab 21. DHCP Client

3. FIREWALL

Penjelasan
A. Firewall NAT
Lab 22. Masquerade IP Address Tertentu
B. Firewall Filter Rule
1. Firewall INPUT
Lab 23. Blok Akses dengan Firewall Input

Lab 24. Membatasi IP Untuk mengakses Router (Firewall Tactic)
Lab 25. Membatasi Port Untuk mengakses Router

2. Firewall FORWARD

Lab 26. Memblok Akses Forward
Lab 27. Blok Situs dengan Firewall Forward
Lab 28. Blok Situs berdasarkan Konten
Lab 29. Address List
Lab 30. Blok Situs dengan Address List
Lab 31. Blok Situs dengan Layer 7 Protocol
Lab 32. Blok Situs Porno dengan DNS Nawala
Lab 33. Transparent DNS Nawala

C. Firewall Logging

Lab 34. Firewall Logging

4. WEB PROXY

Penjelasan

Lab 35. Mengaktifkan Web Proxy
Lab 36. Transparent Proxy
Lab 37. Blok Situs dengan Proxy
Lab 38. Blok Situs berdasarkan Kata
Lab 39. Blok Situs berdasarkan Konten
Lab 40. Me-Redirect Website

5. Routing

Lab 41. Routing Static

6. Wireless Network

Lab 42. Membuat Routerboard menjadi Access Point
Lab 43. Point to Point Via Wireless
Lab 44. Mac Address Filtering
Lab 45. Hotspot
Lab 46. Bypass IP di Hotspot
Lab 47. Virtual Access Point
Lab 48. Virtual Access Point + DHCP Server

Lab 49. Bridging Via Wireless

7. Tunnel

Lab 50. EOIP Tunnel

Lab 51. PPPOE Server

Lab 52. PPPOE Client

Lab 53. PPTP Server

KONFIGURASI DASAR

LAB 1. Mengakses RouterBoard

Assalamualaikum wr.wb

Alhamdulillah di malam yang cerah ini saya punya kesempatan untuk membuat Jobsheet tentang Mikrotik. Oke langsung aja buat pembukaannya saya akan memberikan tutorial dasar yaitu tentang Cara Meremote RouterBoard. Untuk sebagian orang yang baru kenal dengan Mikrotik mungkin hanya tau cara meremote RouterBoard menggunakan Winbox , tetapi sebenarnya banyak cara untuk meremote RouterBoard tersebut , yang beberapa akan dibahas di dalam Lab ini.

Untuk meremote sendiri kita harus tau dengan apa kita akan login kedalam Router itu , untuk itu RouterBoard yang kita beli itu memiliki Konfigurasi Bawaan (default) dari Pabrik , konfigurasi default itu sendiri adalah

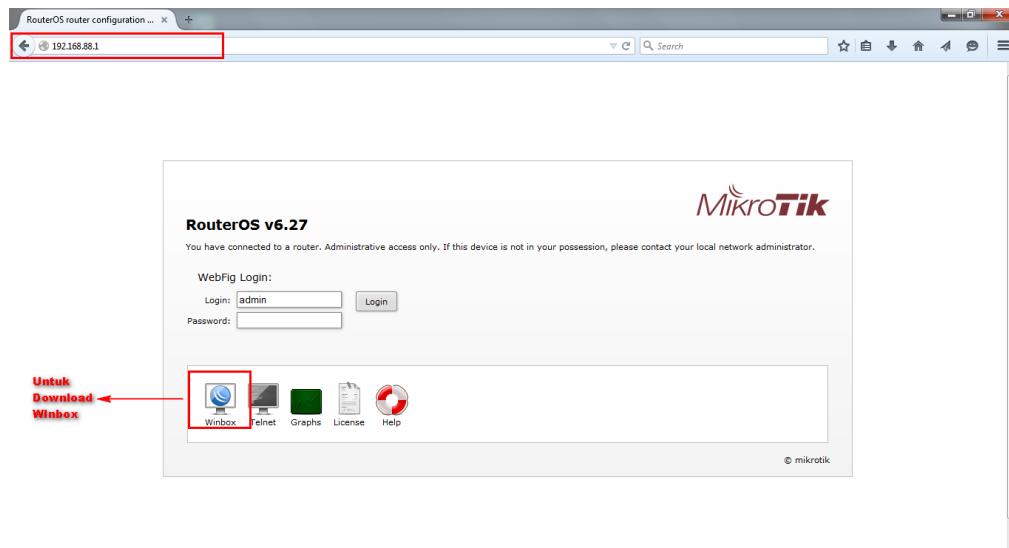
IP : 192.168.88.1/24

User Login : Admin

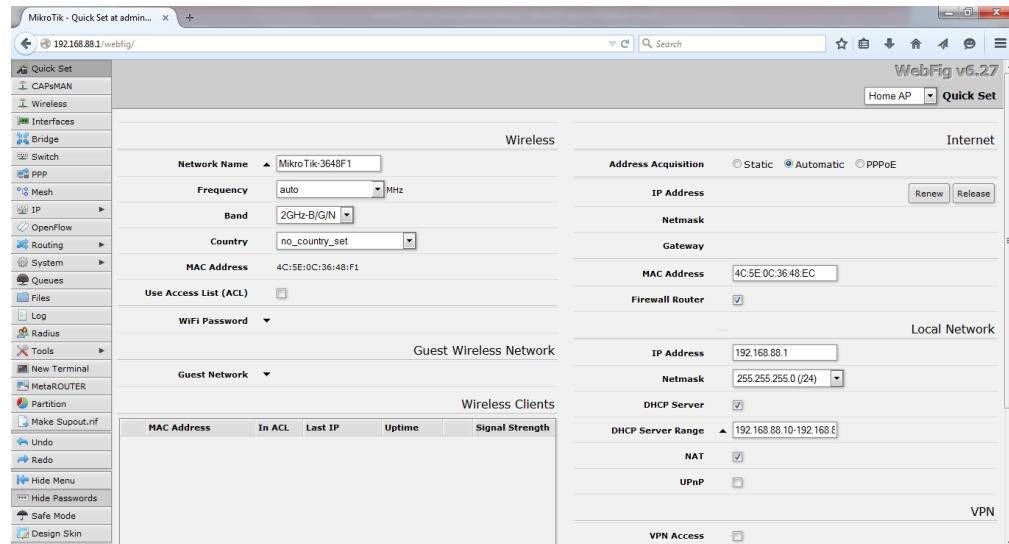
Password : <Tidak Usah di Isi>

1. WebFig

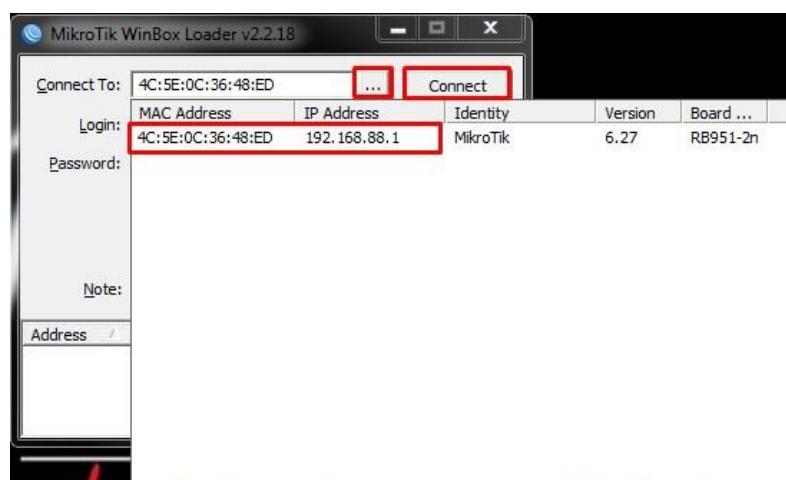
Yang pertama adalah dengan menggunakan WebFig atau Web Configuration , WebFig ini berjalan di Port 80. Jadi dengan menggunakan fitur ini kita bisa meremote melalui Web Browser seperti Mozilla atau Chrome. Untuk meremotnya cukup mudah tinggal masukkan saja IP dari RouterBoard di web browser.



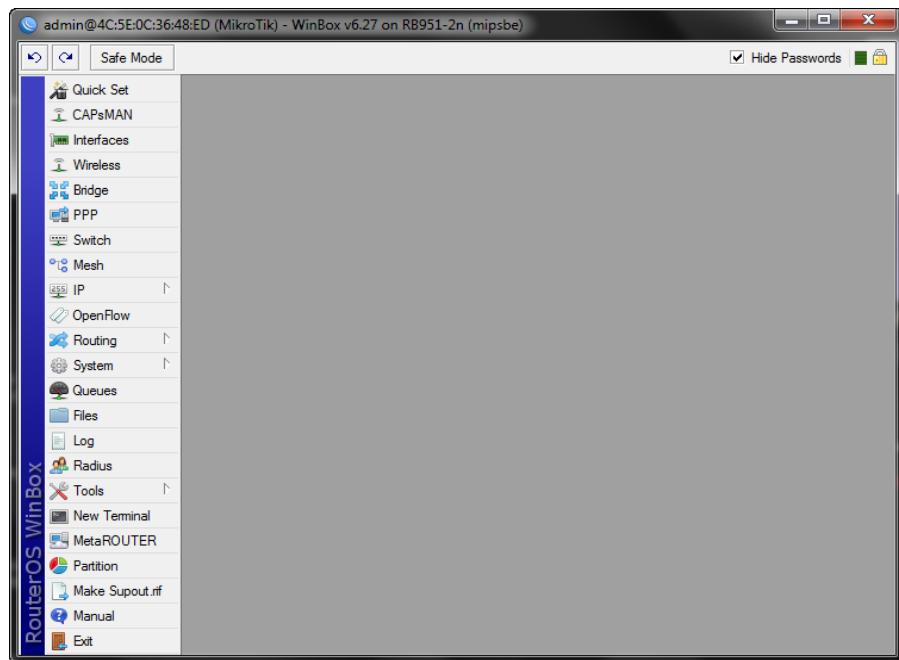
Kemudian silahkan login dengan menggunakan User Admin dan Password dikosongkan. Didalam WebFig kita juga bisa mendownload aplikasi Winbox , dengan mengklik Icon Winbox. Kemudian inilah tampilan dari WebFig itu sendiri.



2. Kemudian yang kedua adalah WinBox. Untuk para pengguna Mikrotik pasti sudah tidak asing dengan software bawaan Mikrotik ini. WinBox ini berjalan di Port 8291. Untuk mendapatkan WinBox kita bisa download di WebFig yang sebelumnya dibahas atau bisa juga dengan mendownload di situs resmi MikroTik yaitu di www.Mikrotik.com/download. Untuk meremotnya silahkan buka Winbox yang sudah didownload. Kemudian klik tombol “...” untuk mengecek Network Discovery nya.



Untuk awal meremote disarankan meremote menggunakan MAC Address , karena jika meremote menggunakan IP kemudian kita melakukan konfigurasi IP Address maka secara otomatis Router akan disconnect dari PC. Jika sudah terremote maka seperti inilah tampilan Winbox.

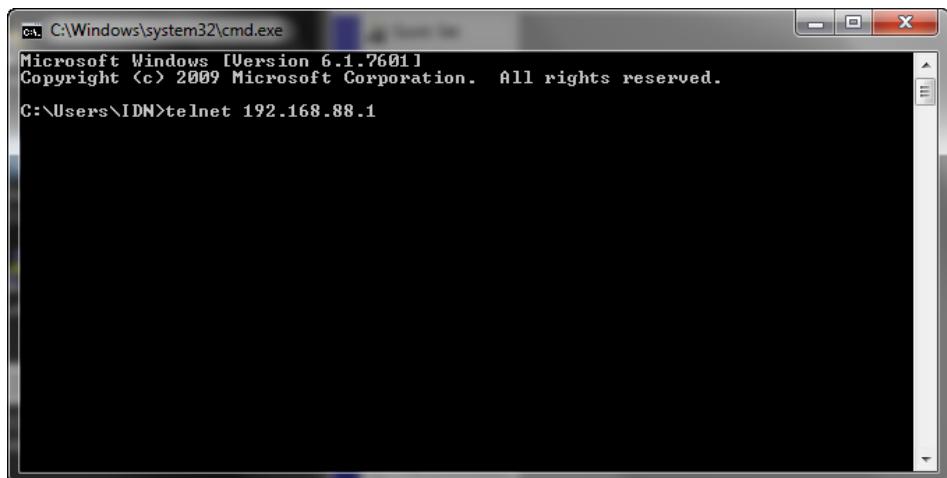


Menurut saya meremote menggunakan Winbox adalah cara meremote yang paling bagus , karena tampilannya yang menarik dan gak ngebosenin , Winbox juga menyediakan Fitur GUI dan juga CLI , jadi kalo bosen Klak klik menu , bisa ganti ke mode ketak ketik sintaks.

3. Telnet

Yang ketiga ada Telnet , telnet itu sendiri kepanjangan dari Telecommunication Network , telnet ini berbasis text dan berjalan di port 23. Untuk menjalankan di Windows caranya cukup mudah yaitu tinggal buka CMD atau Command Prompt kemudian ketikkan perintah

telnet [IP ROUTER]



Nah inilah tampilan dari Remote Via Telnet , kalo kalian udah pernah nyoba Mikrotik RouterOS tampilannya gak jauh beda sama telnet ini. Dia berupa clear text dan agak ngebosenin diliatnya ☺.

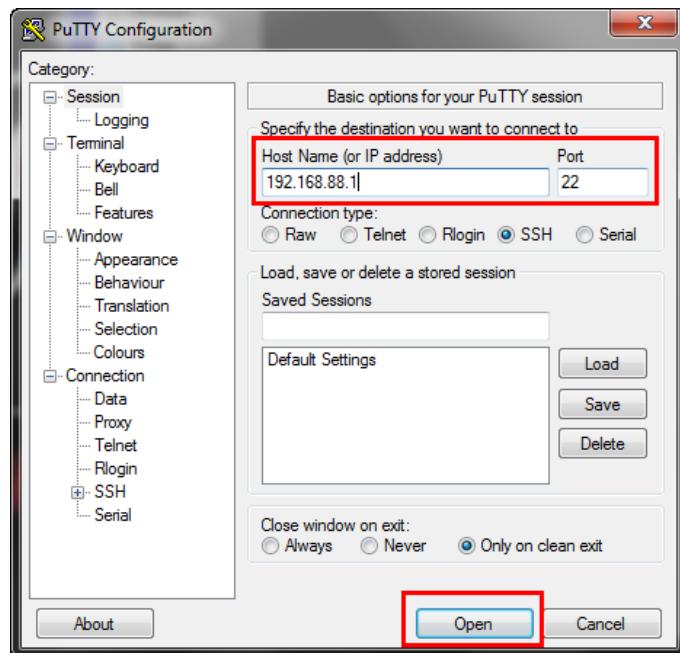
```
    MMM      MMM      KKK          TTTTTTTTTT      KKK
    MMMM     MMMM     KKK          TTTTTTTTTT      KKK
    MMM MMMM MMMM III KKK KKK RRRRRR 00000000 TTT III KKK KKK
    MMM MM MM MM III KKKKKK RRR RRR 000 000 TTT III KKKKKK
    MMM MM MM MM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
    MMM MM MM MM III KKK KKK RRR RRR 00000000 TTT III KKK KKK

MikroTik RouterOS 6.27 <c> 1999-2015      http://www.mikrotik.com/

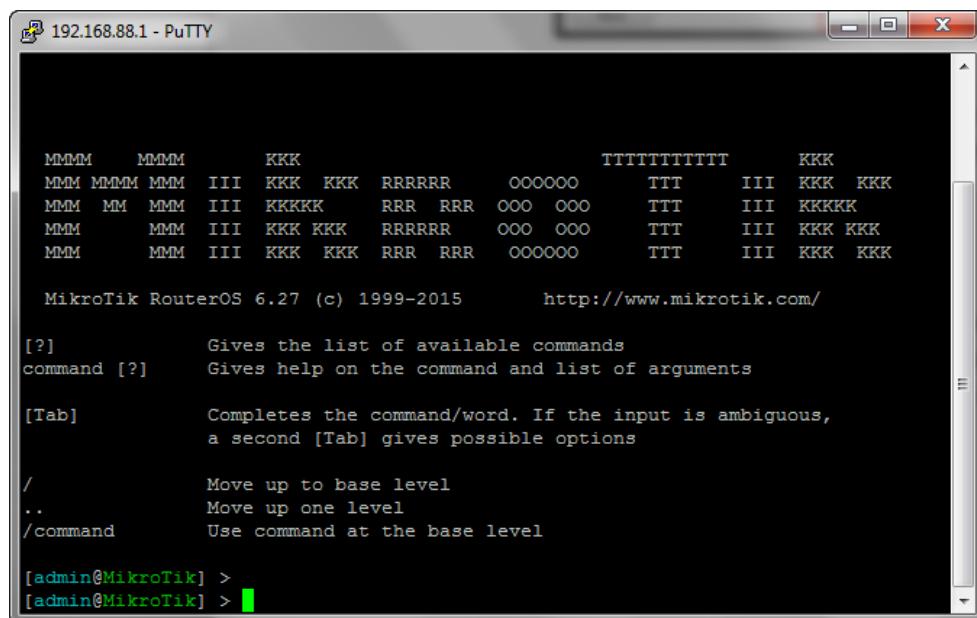
[?]      Gives the list of available commands
command [?]  Gives help on the command and list of arguments
[Tab]    Completes the command/word. If the input is ambiguous,
         a second [Tab] gives possible options
/
/..      Move up to base level
/..command  Move up one level
Use command at the base level
```

4. SSH

Untuk yang ke 4 sekaligus yang terakhir dibahas di Lab ini ada yang namanya SSH atau Secure Shell. SSH ini merupakan aplikasi remote login yang hampir sama seperti Telnet, cuman bedanya di SSH ini lebih aman karena adanya proses Enkripsi data. Untuk menggunakan SSH kita menggunakan aplikasi pihak ketiga yaitu Putty. Pertama buka Puttynya kemudian masukkan IP Router dan klik bagian SSH dan pilih portnya sesuai Port SSH yaitu port 22



Kemudian inilah tampilan dari SSH , sebenarnya gak beda jauh malah bisa dibilang MIRIP dengan meremote lewat Telnet. Seperti dibilang sebelumnya bedanya hanya di proses enkripsi nya saja.



Oke masbroo demikian dulu pembahasan tentang Cara Meremote RouterBoard. Dan juga mohon maaf kalo cuma beberapa aja yang dimasukin , kalo misalkan pengen tau cara lain meremotennya silahkan googling aja , di sini Cuma yang saya tau aja yang dimasukin.

LAB 2. Menginstall Mikrotik RouterOS

Assalamualaikum wr.wb

Setelah di lab awal kita sudah membahas cara meremote Mikrotik RouterBoard selanjutnya di lab ini akan membahas cara menginstall Mikrotik RouterOS.

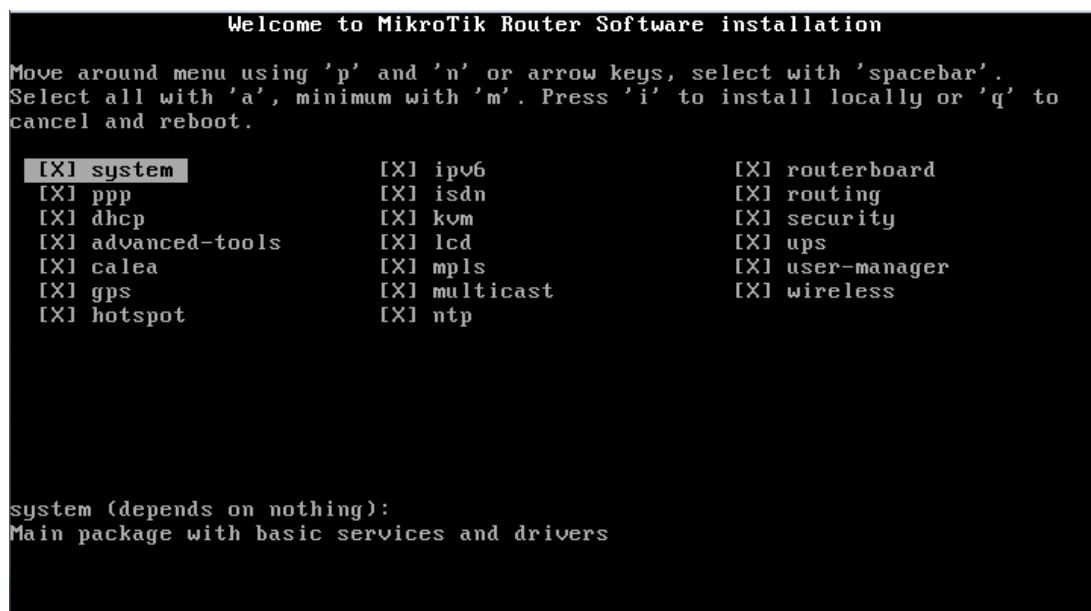
Tentu saja kita akan menginstall nya di PC. RouterOS ini nantinya akan membuat PC kita sebagai Router. Dan untuk spesifikasi PC nya pun tidak terlalu besar bahkan pentium 2 pun mampu untuk menginstall ini. Namun saat kita menginstall RouterOS maka seluruh hardisk kita akan dihapus.

Untuk menginstall Mikrotik siapkan terlebih dahulu alat dan bahannya yaitu

- CD yang sudah di Burn ISO Mikrotik
- PC yang akan dijadikan RouterOS

Langkah Install :

pertama masukkan CD kedalam PC , kemudian tunggu hingga layar instalasi muncul. Kemudian inilah tampilan instalasinya , dibagian kita kita harus memilih Fitur apa saja yang akan diinstall nantinya. Untuk memilih semua tekan "A". Setelah memilih paket kemudian Tekan tombol "I" pada keyboard untuk memulai instalasi.



Kemudian setelah menekan tombol I maka kita akan ditanya apakah sudah yakin dengan paket yang akan diinstall , tekan saja "Y" untuk melanjutkan

```
system (depends on nothing):  
Main package with basic services and drivers  
  
Do you want to keep old configuration? [y/n]:_
```

Kemudian akan muncul peringatan , seperti dibahas sebelumnya bahwa mikrotik akan menghapus semua isi hardisk kita. Tekan "Y" untuk memulai proses instalasi

```
Warning: all data on the disk will be erased!  
  
Continue? [y/n]:_
```

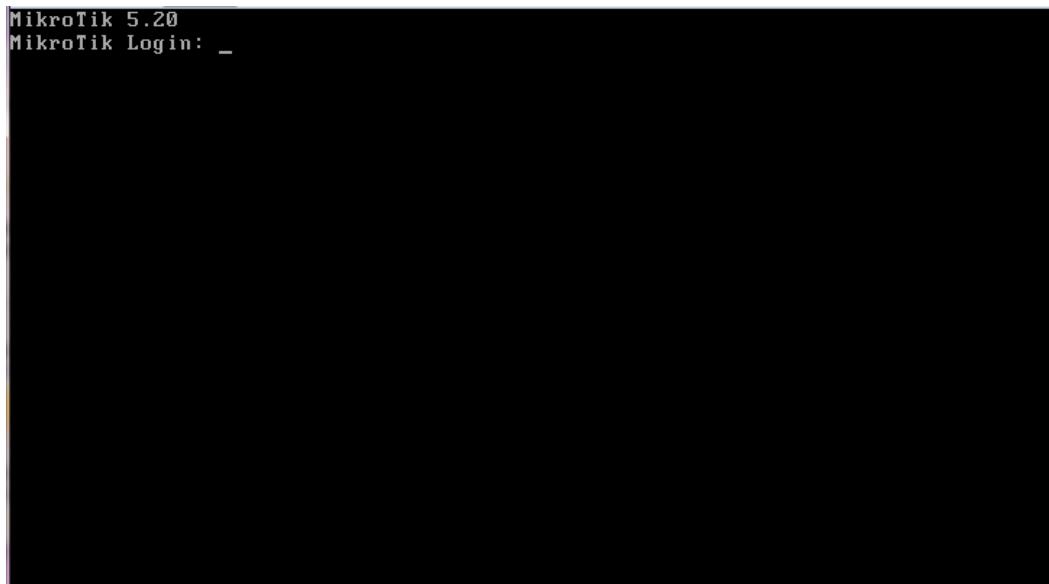
Kemudian mikrotik akan mulai melakukan pemformatan terhadap hardisk kita.

```
WARNING: couldn't keep config - current license does not allow that  
Creating partition.....  
Formatting disk....
```

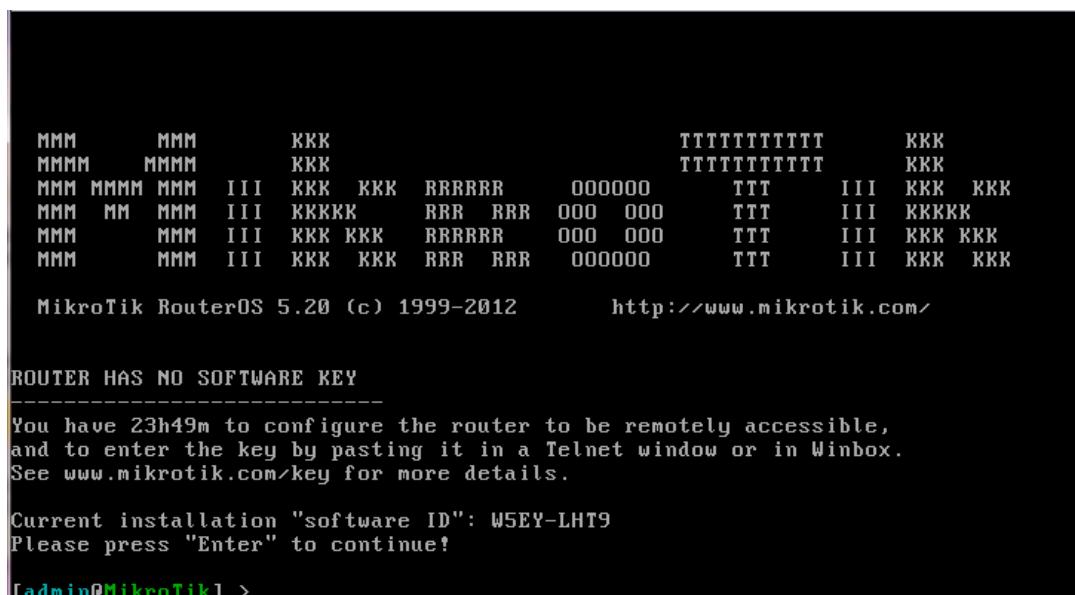
Setelah semua paket terinstall kita diminta untuk mereboot PC kita , tekan Enter untuk mereboot nya.

```
installed system-5.20  
installed wireless-5.20  
installed user-manager-5.20  
installed ups-5.20  
installed security-5.20  
installed routing-5.20  
installed routerboard-5.20  
installed ntp-5.20  
installed multicast-5.20  
installed mpls-5.20  
installed lcd-5.20  
installed kvm-5.20  
installed isdn-5.20  
installed ipv6-5.20  
installed hotspot-5.20  
installed gps-5.20  
installed calea-5.20  
installed advanced-tools-5.20  
installed dhcp-5.20  
installed ppp-5.20  
  
Software installed.  
Press ENTER to reboot
```

Setelah tereboot maka inilah tampilan login Mikrotik. Secara Default Mikrotik memiliki satu user yaitu **Admin** dengan password <Kosong>



Selanjutnya inilah tampilan awal MikrotikRouterOS. Sama kan seperti meremote Routerboard lewat SSH atau telnet.



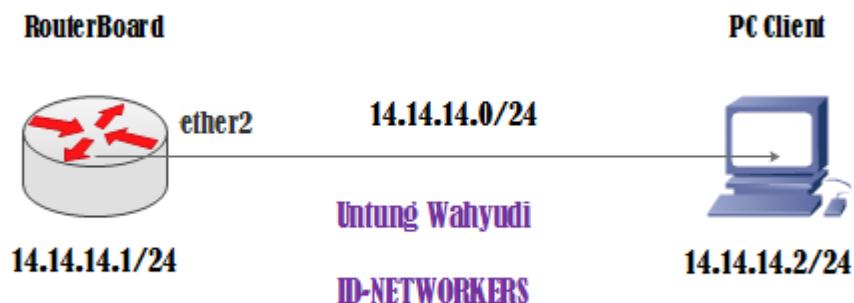
Oke mas dan Mba Broo , karena sudah selesai diinstall itu artinya sudah berhasil. Untuk konfigurasi kedepannya silahkan baca saja tutorial tutorial selanjutnya

Wassalam !

LAB 3. Mengkoneksikan RouterBoard dengan PC.

Assalamualaikum Wr. Wb

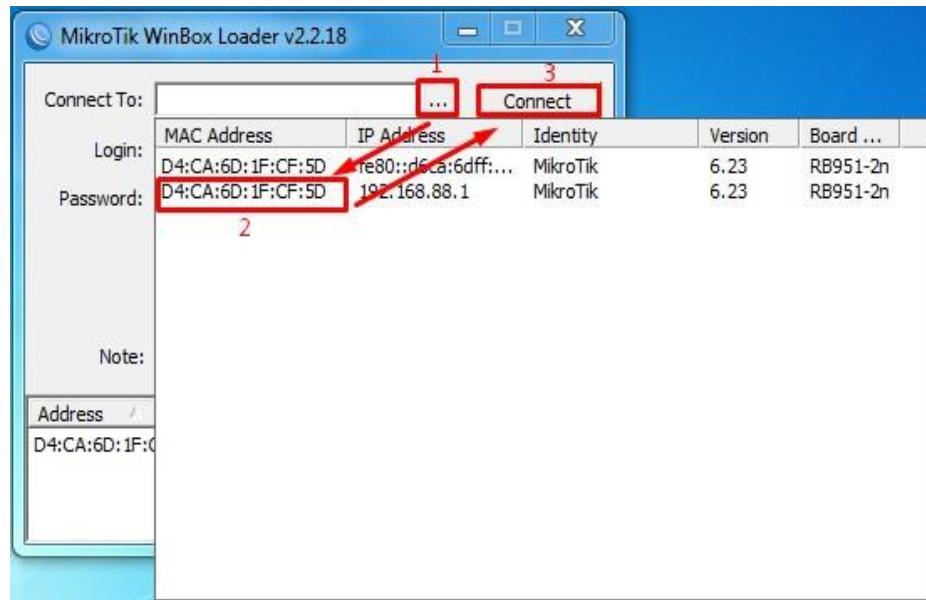
Masih lanjut dari pembahasan Lab sebelumnya , di Lab ini saya ingin membahas tentang cara mengkoneksikan RouterBoard dengan PC. Maksudnya adalah gimana caranya sebuah PC bisa melakukan komunikasi dengan RouterBoard. Sekaligus saya mau ngasih tau cara menambahkan IP di Routerboard Mikrotik. Kurang lebih topologinya seperti ini.



Langkah Konfigurasi :

1. Remote Via Winbox

Yang pertama harus dilakukan adalah kita remote RouterBoard lewat Winbox , seperti dibilang sebelumnya untuk awal meremote winbox sebaiknya meremote menggunakan MAC Address sehingga ketika kita mengubah IP dari Interface RouterBoard maka router tidak akan ter-Disconnect.

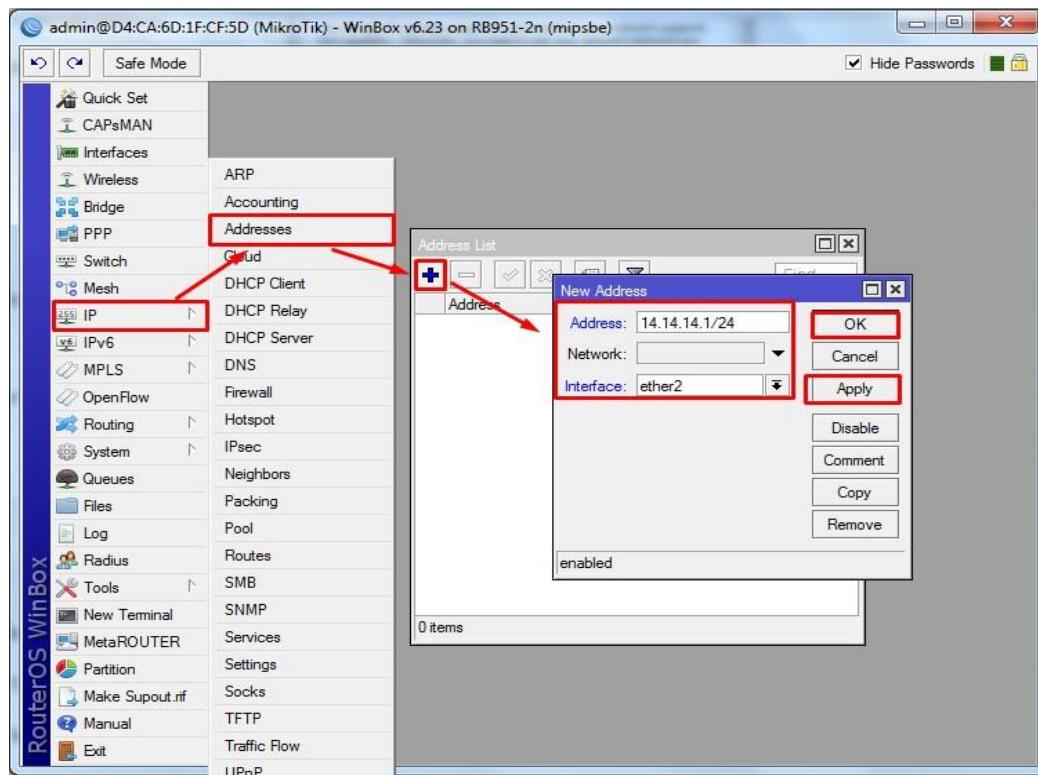


2. Menambahkan IP Address.

Setelah terremote , kemudian kita tambahkan IP address untuk interface RouterBoard nya. Untuk CLI bisa gunakan perintah:

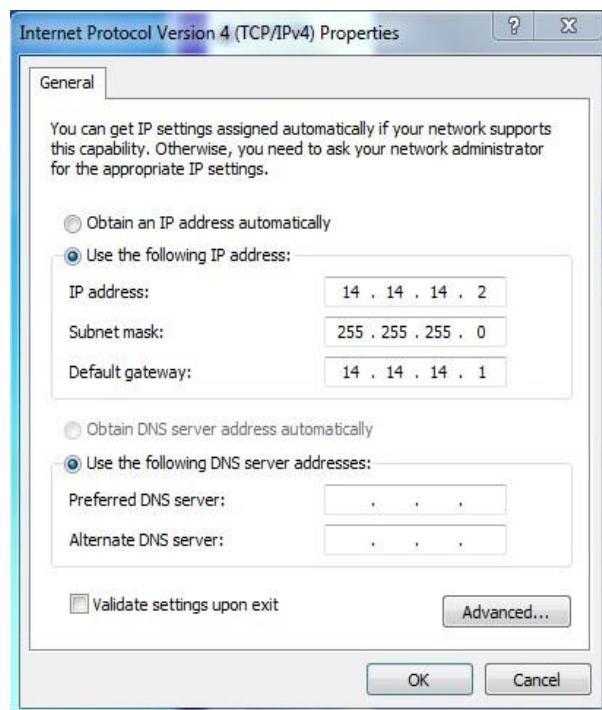
```
[admin@Untung > ip address add address=[IPAddress]]
```

Kemudian untuk GUI nya kita bisa klik menu IP > Addresses > + kemudian masukkan IP Address sesuai keinginan kita , lalu pilih interface nya , karena disini saya ngehubungin PC ke Ether2 jadi saya pilih nya interface Ether2.

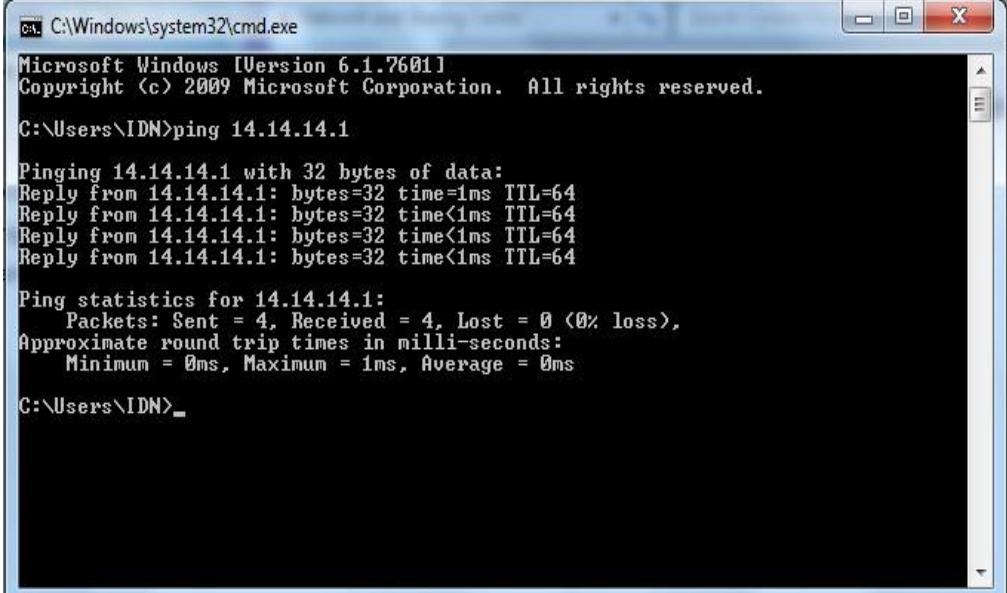


3. Pengujian di Client.

Selanjutnya kita lakukan pengujian di Client , sebelumnya kita ubah dulu IP dari client menjadi 1 network dengan IP RouterBoard .



Setelah itu coba test Ping dari Client ke IP Router. Jika sudah reply itu tandanya berhasil.



```
ca C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\IDN>ping 14.14.14.1

Pinging 14.14.14.1 with 32 bytes of data:
Reply from 14.14.14.1: bytes=32 time=1ms TTL=64
Reply from 14.14.14.1: bytes=32 time<1ms TTL=64
Reply from 14.14.14.1: bytes=32 time<1ms TTL=64
Reply from 14.14.14.1: bytes=32 time<1ms TTL=64

Ping statistics for 14.14.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\IDN>
```

Oke karena sudah reply maka itu artinya sudah berhasil. Gimana mudahkan cara mengkoneksikan RB dengan PC. Yailah mudah ini kan masih dasar. Kedepannya mungkin akan selalu meningkat kesulitannya jadi waspadalah waspadalah ☺.

Oke sekian dulu tentang Lab Mengkoneksikan RB ke PC.

Wassalam !

LAB 4. Management User di Mikrotik.

Assalamualaikum Wr. Wb

Lanjut lagi dari materi sebelumnya , di Lab ini saya mau ngasih sedikit tutorial tentang Management User di Mikrotik. Dilab ini gak akan dibahas terlalu jauh tentang management user karena management user nanti adanya di materi MTCUME , dan saya belum paham masalah itu , jadi disini Cuma basicnya aja yaitu bagaimana cara menambahkan User dengan Group (Hak Akses) yang berbeda.

Oke langsung aja ke topik pembahasan , di pembahasan kali ini saya akan membuat 2 user dengan Group yang berbeda , group inilah yang nantinya menentukan Hak Akses dari setiap user. Secara default Mikrotik sudah menyediakan 1 user yaitu **user Admin** dengan **Group Full**. Untuk group sendiri ada 3 group secara default yaitu :

Full = Bisa melihat dan melakukan konfigurasi , dan juga bisa mengubah dan menghapus user

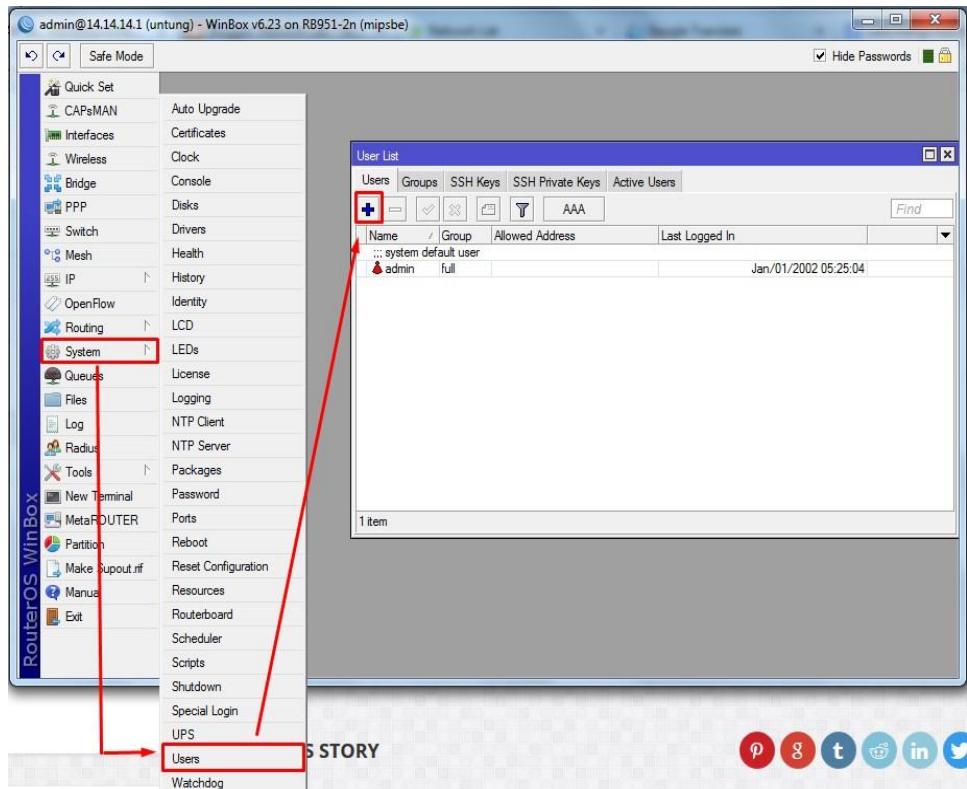
Write = Bisa melakukan konfigurasi tapi **TIDAK BISA** mengubah/menghapus User lain

Read = Hanya bisa melihat - lihat saja.

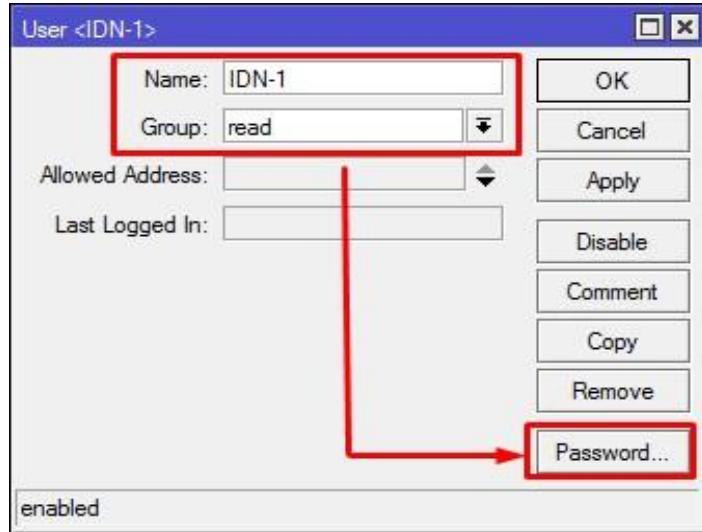
Langkah Konfigurasi :

1. Membuat User IDN-1

Seperti saya bilang sebelumnya saya bakal bikin 2 user , di sini saya bikin user pertama dengan nama IDN-1. Untuk membuat user kita bisa klik menu **System > Users > +** ,



Kemudian masukkan Nama dan Group dari User yang akan kita buat. Disini saya buat Group atau hak aksesnya adalah **Read**. Untuk memberikan password bisa klik bagian passwordnya.



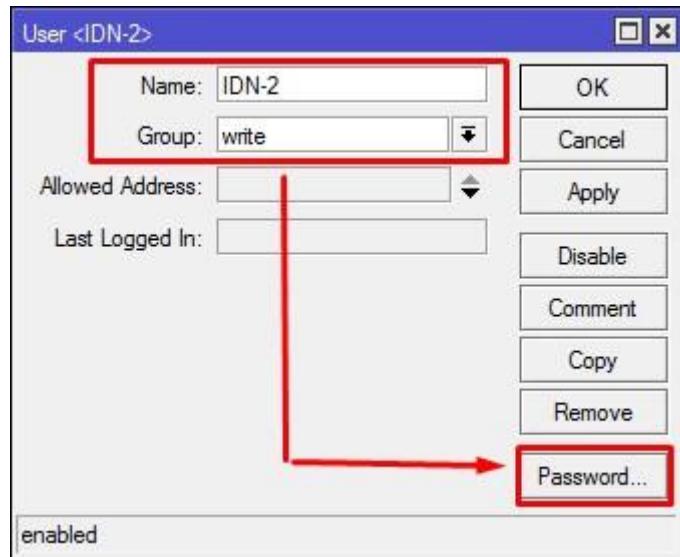
Jika sudah klik **Apply** dan **OK** , maka user IDN-1 sudah terbuat.

2. Membuat User IDN-2.

Setelah selesai membuat User IDN-1 selanjutnya saya buat user yang kedua yaitu user IDN-2 , caranya masih sama seperti sebelumnya Cuma nama dan Group nya saja yang dibedakan. Untuk IDN-2 saya kasih group atau hak aksesnya adalah **Write**.

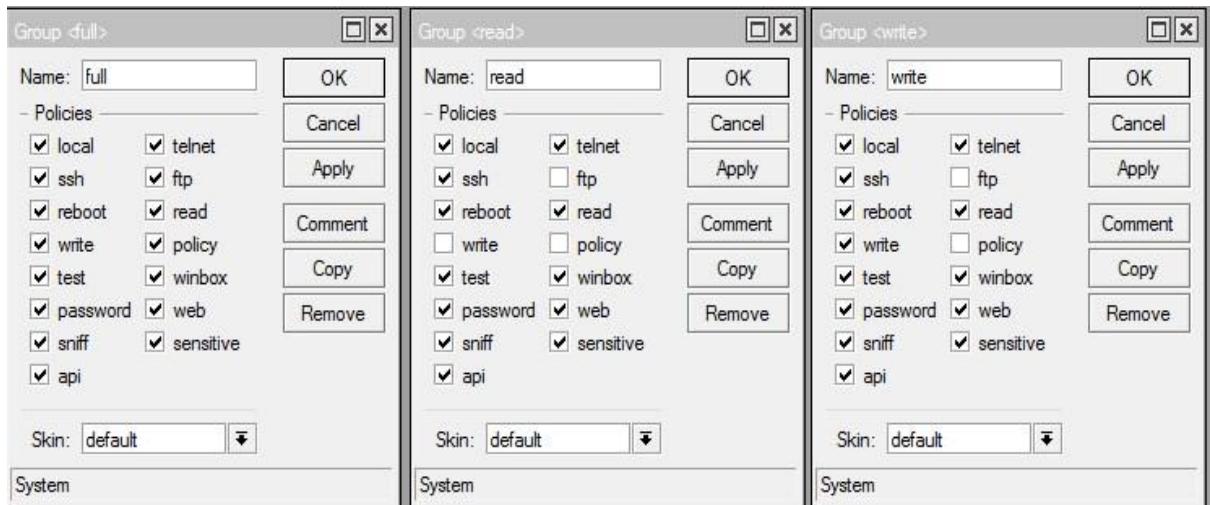
IDN-1 = Read = Hanya bisa melihat - lihat saja.

IDN-2 = Write = Bisa melakukan konfigurasi tetapi tidak bisa mengubah atau menghapus User.



3. Melihat Hak Akses Group

Agar lebih paham tentang Group atau Hak Akses dari setiap user kita bisa melihatnya , berikut gambar dari hak akses setiap group secara default. Sebenarnya kita bisa mengubah sendiri hak akses setiap group sesuai dengan yang kita inginkan.



4. Pengujian Hak Akses.

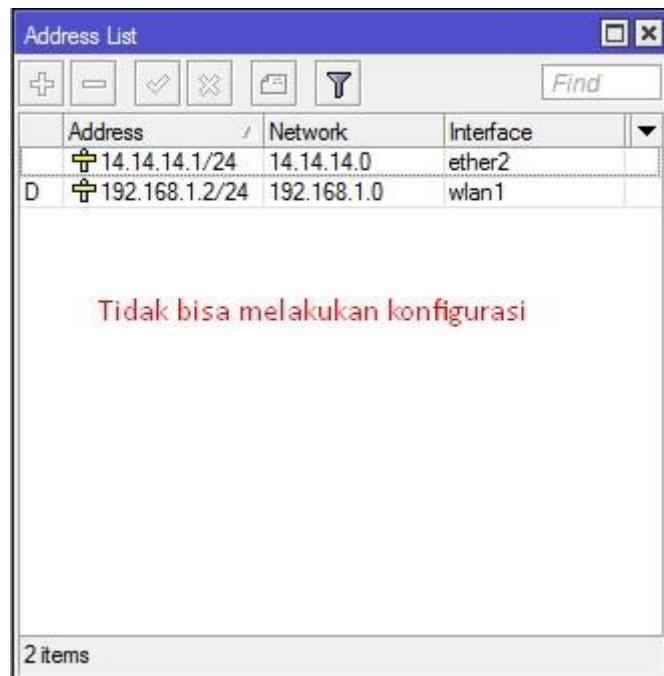
Setelah selesai membuat user dengan hak akses yang berbeda beda selanjutnya kita akan mencoba hak akses dari setiap user. Untuk mengingatkan kembali tentang hak akses dan user yang tadi kita buat berikut ringkasannya.

5. Hak Akses User IDN-1

Pertama kita kan mengetes hak akses dari user IDN-1 , pertama kita login sebagai User IDN-1 di Winbox.



Kemudian coba melakukan konfigurasi , contohnya kita akan menambahkan IP address dengan menggunakan user IDN-1 , karena hak aksesnya adalah Read maka User IDN-1 tidak bisa melakukan konfigurasi apapun.

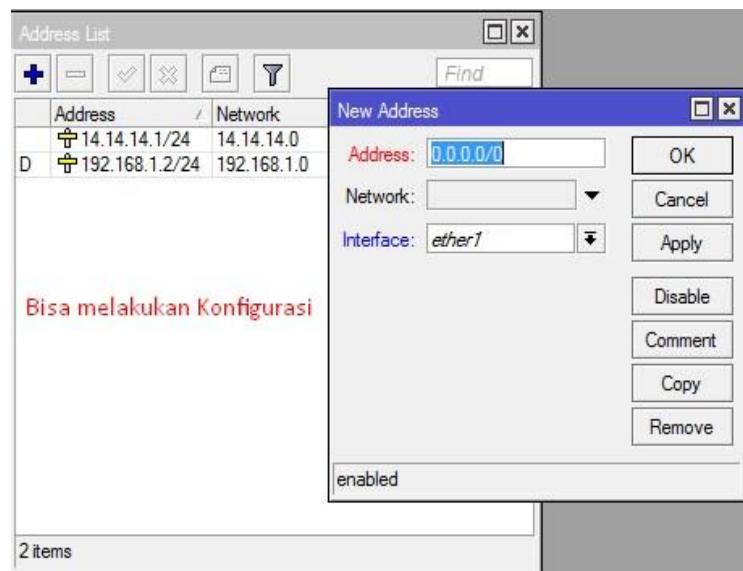


6. Hak Akses User IDN-2

Selanjutnya kita akan menguji hak akses dari User IDN-2 , pertama logout user IDN-1 kemudian login kembali menggunakan User IDN-2.



Selanjutnya coba lakukan konfigurasi IP address. Karena User IDN-2 memiliki Hak Akses Write maka dia bisa melakukan konfigurasi IP address namun dia tidak bisa mengubah atau menghapus user lain.



Oke mas dan mba broo sekian dulu tentang Basic User management di Mikrotik.
Wassalam

LAB 5. Merubah Router Identity

Assalamualaikum wr.wb

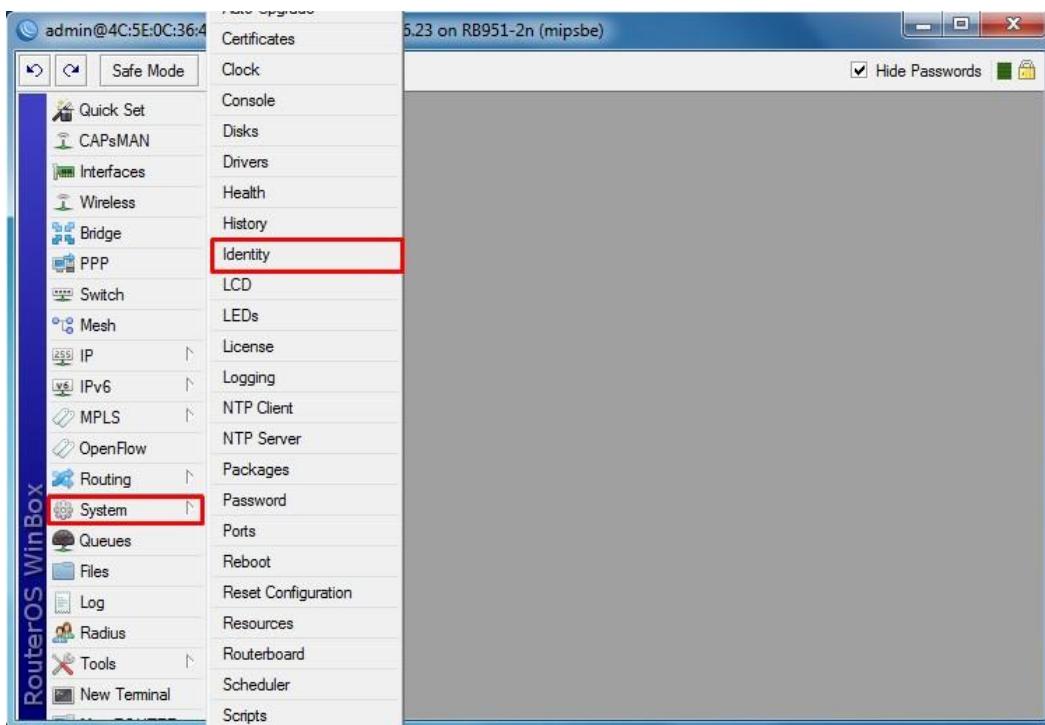
Di Lab kali ini agak menyimpang dari lab sebelumnya , di lab ini saya ingin membahas tentang merubah Router Identity , atau nama dari RouterBoard. Secara default Router Mikrotik memiliki identity **Mikrotik** namun kita bisa mengubah nya sesuai keinginan kita. Sebenarnya ini Cuma lab dasar tapi sangat bermanfaat. Jangan sampe kita salah konfig hanya karena salah meremote Router yang Identitas nya sama. Kan bahaya kalo salah router. Makanya ini lumayan bermanfaat menurut saya

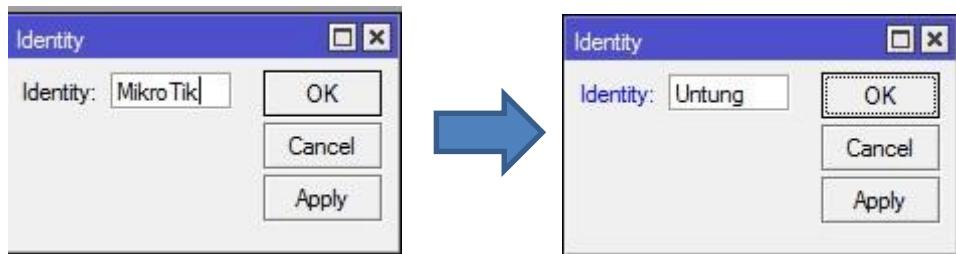
Oke langsung aja ke Langkah konfigurasi :

Untuk merubah identity router di CLI kita bisa gunakan perintah :

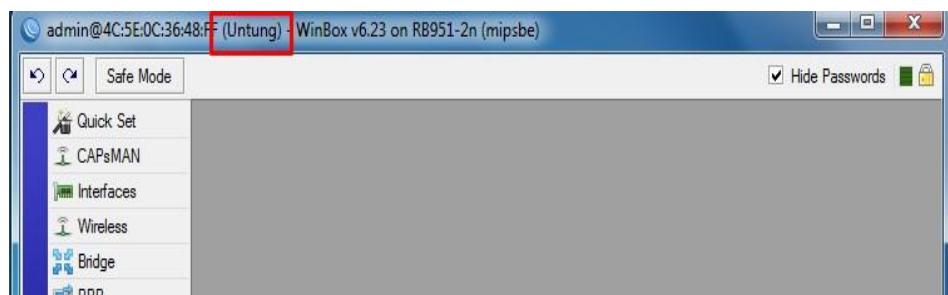
[admin@MikroTik> System Identity set name=[Identitas]

Kemudian untuk mode GUI kita bisa klik menu **System > Identity** kemudian ubah namanya sesuai keinginan kita.





Jika sudah maka identitas dari router akan terubah menjadi nama yang tadi kita buat.



Jika di CLI maka dari yang mikrotik akan berubah menjadi Untung

```

[?]           Gives the list of available commands
command [?]   Gives help on the command and list of arguments

[Tab]         Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/             Move up to base level
..            Move up one level
/command      Use command at the base level
[admin@Untung] >
[admin@Untung] >

```

Oke mas dan mba broo sekian dulu tentang konfigurasi dasar yaitu merubah Identitas Router. Meskipun sangat dasar tapi itu sangat membantu kita dalam mengelola jaringan. Oke semoga bermanfaat.

Wassalam !

LAB 6. Merubah Tanggal dan Waktu

Assalamualaikum wr.wb

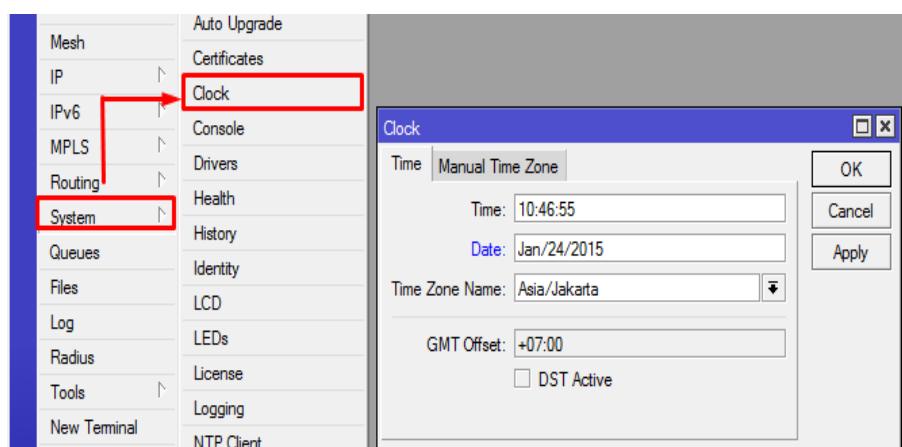
Oke masih lanjut di konfigurasi dasar , di lab ini saya akan menjelaskan tentang cara merubah tanggal dan waktu di Router Mikrotik. Secara default waktu di Mikrotik adalah **jam 00:00:00 dan tanggal Jan/02/1970**. Tentunya kita gak mau dong kalo waktu di mikrotik *ngawur* alias gak tepat. Maka dari itu lab ini saya masukin kedalam modul.

Oke untuk mengatur Tanggal dan Waktu di mikrotik caranya cukup mudah untuk CLI bisa gunakan perintah

```
[admin@untung> system clock set time=10:41:00 date=Jan/24/2015 time-zone-name=Asia/Jakarta
```

Saya jelaskan lagi perintah diatas , bisa diliat di Time kita harus mengisikan nya secara lengkap yaitu **Jam:Menit:Detik** , kemudian di bagian Date kita harus isikannya dengan format **Bulan/tanggal/tahun**. Dan untuk bagian bulan **tidak dapat diisikan dengan angka** , jadi harus dengan **3 kata depannya**. Kemudian sesuaikan juga tentang zona waktunya.

Untuk mode GUI kita klik menu **system > clock** kemudian isikan waktu dan tanggallnya.



Oke karena sudah diatur waktunya berarti lab kita kali ini sudah selesai yeaaay !

LAB 7. Disable , Enable dan Uninstall Packet.

Assalamualaikum wr.wb

Setelah sebelumnya sudah ngebahas tentang Management User selanjutnya saya akan membahas masalah Management Packet di Mikrotik. Kalo denger kata management Packet pasti udah paham kan maksudnya , kalo belom paham saya kasih sedikit ringkasan. Yang namanya management itu artinya mengelola jadi disini kita akan mengelola packet packet yang ada di Mikrotik.

Di Lab ini saya Cuma mau ngebahas tentang Cara Men-Disable , Enable dan Uninstall Packet saja. Berikut penjelasan dari ketiga kata tersebut

Disable = Menonaktifkan paket yang dipilih

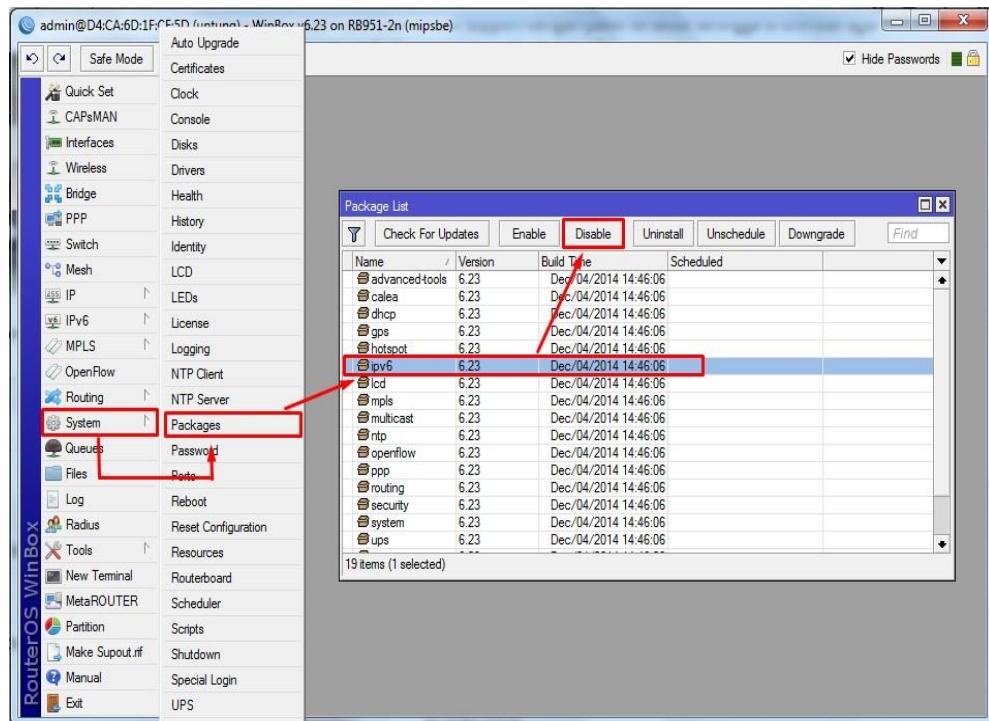
Enable = Mengaktifkan kembali paket yang telah di-Disable

Uninstall = Menghapus Paket yang tidak kita gunakan.

Langkah Konfigurasi :

1. Disable Paket.

Untuk mendisable paket kita bisa klik menu **System > Packages** kemudian kita pilih packet yang akan kita disable , lalu klik bagian **Disable** untuk mendisable packet. Sebagai contoh saya akan mendisable packet **ipv6**.



Setelah kita klik bagian command atau perintah nya maka akan muncul kalimat "**scheduled for ...**" yang artinya perintah itu akan dijalankan ketika kita mereboot Router. Sebagai contoh karena saya memilih bagian **disable** maka akan muncul kalimat "**scheduled for disable**".

Package List				
	Check For Updates	Enable	Disable	Uninstall
Name	/ Version	Build Time	Scheduled	
advanced-tools	6.23	Dec/04/2014 14:46:06		
calea	6.23	Dec/04/2014 14:46:06		
dhcp	6.23	Dec/04/2014 14:46:06		
gps	6.23	Dec/04/2014 14:46:06		
hotspot	6.23	Dec/04/2014 14:46:06		
ipv6	6.23	Dec/04/2014 14:46:06	scheduled for disable	
lcd	6.23	Dec/04/2014 14:46:06		
mpls	6.23	Dec/04/2014 14:46:06		
multicast	6.23	Dec/04/2014 14:46:06		
ntp	6.23	Dec/04/2014 14:46:06		
openflow	6.23	Dec/04/2014 14:46:06		
ppp	6.23	Dec/04/2014 14:46:06		
routing	6.23	Dec/04/2014 14:46:06		
security	6.23	Dec/04/2014 14:46:06		
system	6.23	Dec/04/2014 14:46:06		
ups	6.23	Dec/04/2014 14:46:06		

19 items (1 selected)

2. Meng-Uninstall Paket

Selanjutnya kita akan coba menguninstall paket. Seperti dibahas sebelumnya menguninstall paket akan menghapus paket dari Router Mikrotik. Sebagai contoh saya akan menghapus paket **MPLS**.

Package List				
	Check For Updates	Enable	Disable	Uninstall
Name	/ Version	Build Time	Scheduled	
advanced-tools	6.23	Dec/04/2014 14:46:06		
calea	6.23	Dec/04/2014 14:46:06		
dhcp	6.23	Dec/04/2014 14:46:06		
gps	6.23	Dec/04/2014 14:46:06		
hotspot	6.23	Dec/04/2014 14:46:06		
ipv6	6.23	Dec/04/2014 14:46:06	scheduled for disable	
lcd	6.23	Dec/04/2014 14:46:06		
mpls	6.23	Dec/04/2014 14:46:06	scheduled for uninstall	
multicast	6.23	Dec/04/2014 14:46:06		
ntp	6.23	Dec/04/2014 14:46:06		
openflow	6.23	Dec/04/2014 14:46:06		
ppp	6.23	Dec/04/2014 14:46:06		
routing	6.23	Dec/04/2014 14:46:06		
security	6.23	Dec/04/2014 14:46:06		
system	6.23	Dec/04/2014 14:46:06		
ups	6.23	Dec/04/2014 14:46:06		

19 items (1 selected)

3. Pengujian

Selanjutnya kita akan melakukan pengujian terhadap paket yang tadi kita disable dan uninstall , caranya adalah dengan cara mereboot Router Mikrotik kita yaitu dengan cara klik **System > Reboot** atau dengan menggunakan perintah

```
[admin@untung] > system reboot  
Reboot, yes? [y/N]:  
Y  
system will reboot shortly
```

Setelah selesai ter-reboot buka kembali menu **System > Packages** dan lihat paket yang tadi kita disable dan uninstall. Paket yang didisable akan berwarna pudar yang artinya sedang nonaktif , sedangkan paket yang di Uninstall akan hilang dari Paket Mikrotik.

Package List					
	Check For Updates	Enable	Disable	Uninstall	Unschedule
advanced-tools	6.23				
alea	6.23				
dhcp	6.23				
gps	6.23				
hotspot	6.23				
ipv6	6.23				
lcd	6.23				
multicast	6.23				
ntp	6.23				
openflow	6.23				
ppp	6.23				
routing	6.23				
security	6.23				
system	6.23				
ups	6.23				
user-manager	6.23				
18 items (1 selected)					

Untuk mengaktifkan kembali paket yang didisable kita gunakan perintah **Enable** , caranya sama seperti sebelumnya tinggal klik paketnya kemudian klik enable lalu reboot Router nya.

Package List

Name	Version	Build Time	Scheduled
advanced-tools	6.23	Dec/04/2014 14:46:06	
alea	6.23	Dec/04/2014 14:46:06	
dhcp	6.23	Dec/04/2014 14:46:06	
gps	6.23	Dec/04/2014 14:46:06	
hotspot	6.23	Dec/04/2014 14:46:06	
inet	6.23	Dec/04/2014 14:46:06	
lcd	6.23	Dec/04/2014 14:46:06	
mpls	6.23	Dec/04/2014 14:46:06	
multicast	6.23	Dec/04/2014 14:46:06	
ntp	6.23	Dec/04/2014 14:46:06	
openflow	6.23	Dec/04/2014 14:46:06	
ppp	6.23	Dec/04/2014 14:46:06	
routing	6.23	Dec/04/2014 14:46:06	
security	6.23	Dec/04/2014 14:46:06	
system	6.23	Dec/04/2014 14:46:06	
ups	6.23	Dec/04/2014 14:46:06	

19 items (1 selected)

Oke masbroo sekian dulu yaa tentang Enable Disable dan Uninstallnya. DiLab selanjutnya InshaAllah saya bakal ngebahas tentang Upgrade dan Downgrade Paket.

Wassalam !

LAB 8. Upgrade dan Downgrade Packet.

Assalamualaikum wr.wb

Sesuai janji saya di Lab sebelumnya , kali ini saya akan membahas tentang Upgrade dan Downgrade Packet. Sebelum masuk ke konfigurasi saya jelasin dulu sedikit tentang Upgrade dan Downgrade.

Jadi **Upgrade** adalah kita "*memperbarui paket yang ada dimikrotik dari versi sebelumnya ke versi terbaru. Fungsi nya adalah untuk mengatasi BUG atau kekurangan yang ada di versi sebelumnya.*"

Sedangkan **Downgrade** adalah *menurunkan versi mikrotik ke versi sebelumnya. Jadi fungsi dari downgrade adalah apabila Router kita tidak cocok dengan versi mikrotik terbaru , atau bahkan versi terbaru memiliki bug.*" Maka dari itu perlu namanya Downgrade.

Dalam hal upgrade dan downgrade kita harus memperhatikan Seri dari Routerboard dan juga Arsitekturnya. Lisensi juga mempengaruhi upgrade Downgrade. Untuk itu kita tidak boleh salah download paket.

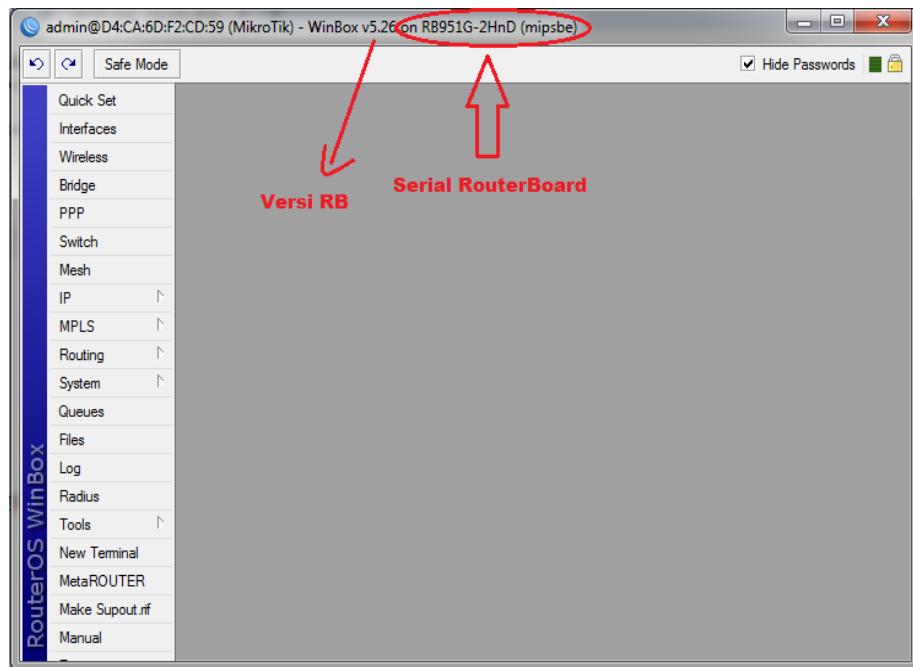
Langsung aja yoo ke langkah konfigurasi.

UPGRADE PACKET :

Disini saya punya RouterBoard dengan seri 951G dan arsitekturnya itu mipsbe terus mau saya upgrade **versi 5.2 ke Versi 6.23** , (Sebenarnya sih itu punya sekolah , bukan punya sendiri ☺).

1. Cek Versi dan Seri RouterBoard

Langkah pertama yang harus dilakukan adalah kita lihat dulu versi dan seri dari RouterBoard.



2. Download Packet

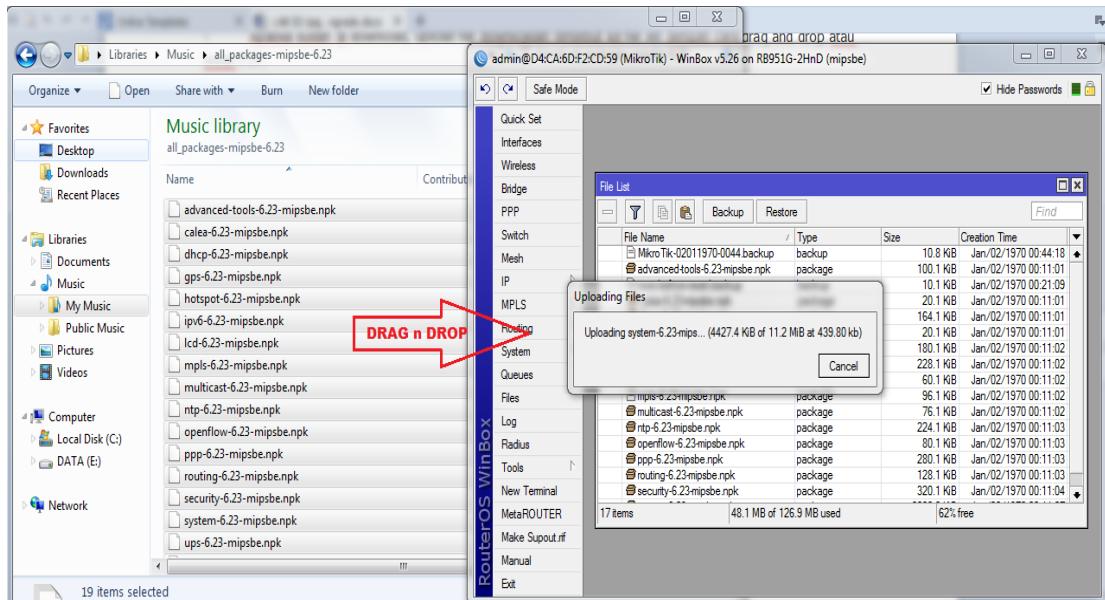
Selanjutnya kita download paket mikrotik nya di www.Mikrotik.com/download, karena kita ingin mengupgrade paket jadi kita download versi terbaru yaitu versi 6.23. Di Mikrotik.com kita sudah dimudahkan untuk pemilihan paket karena sudah dikelompokkan berdasarkan seri dan arsitekturnya.

The screenshot shows the Mikrotik download page for RouterOS v6.23. It asks to choose an instruction set: 'mipsbe' (selected), 'CRS series, RB4xx series, RB7xx series, RB9xx series, RB2011 series, SXT, OmniTik, Groove, METAL, SEXTANT'. It also lists other download options: 'Upgrade package' (selected), 'All packages' (highlighted with a red box), 'Wireless CAPsMANv2', 'Netinstall', 'Torrent', 'Changelog', and 'MD5'. To the right, there are comparison tables for 'v5.26' and 'v4.17' showing file sizes and download links for each category.

	v5.26	v4.17
All packages	Download	Download
Upgrade package	Download	Download
Wireless CAPsMANv2	Download	Download
Netinstall	Download	Download
Torrent	Download	Download
Changelog	Download	Download
MD5	Download	Download

3. Upgrade Packet

Setelah dipilih kemudian download yang All Packages. File download akan berupa extensi .Zip , jadi kita extract terlebih dahulu file tersebut. Setelah terextrak kemudian Drag n Drop File tersebut kedalam **Menu Files** Mikrotik.

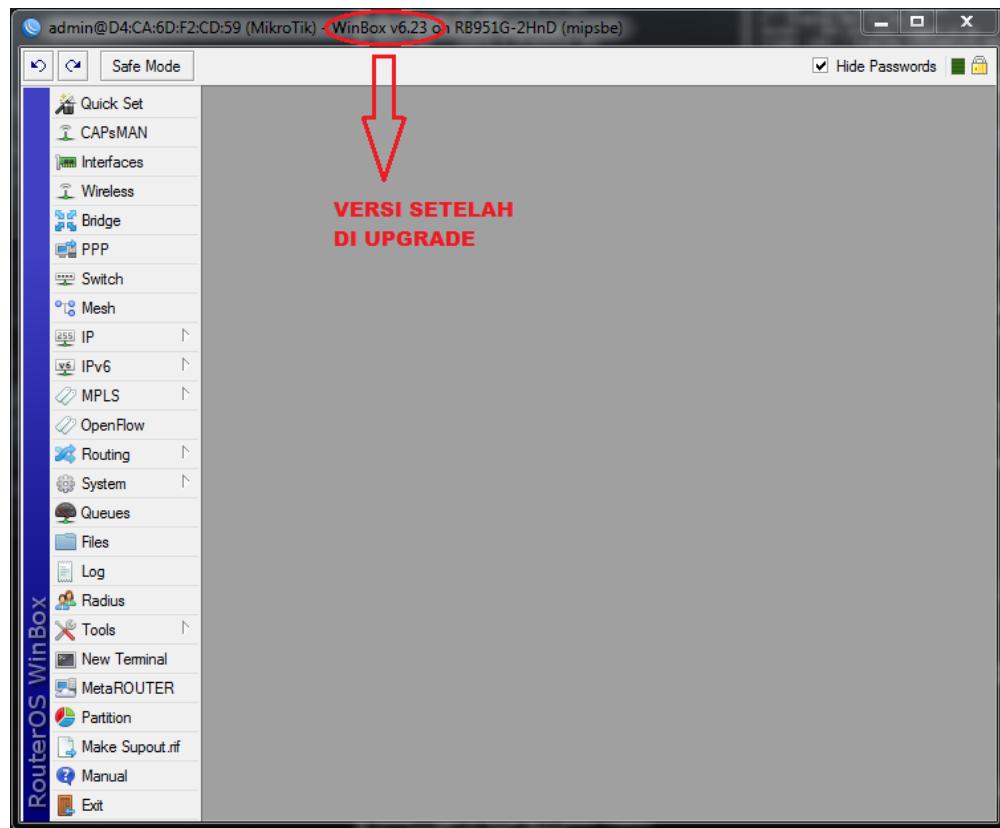


4. Pengecekan

Setelah semua file terupload, selanjutnya kita kan melakukan pengecekan apakah paket sudah terupgrade atau belum , caranya adalah kita reboot terlebih dahulu Router Mikrotik kita.

```
[admin@untung] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

Setelah selesai mereboot , kita bisa langsung melihat apakah versinya sudah berubah tau belum , karena ditampilkan awal winbox sudah terlihat versi dari Mikrotiknya , yang sebelumnya 5.26 sekarang menjadi 6.23

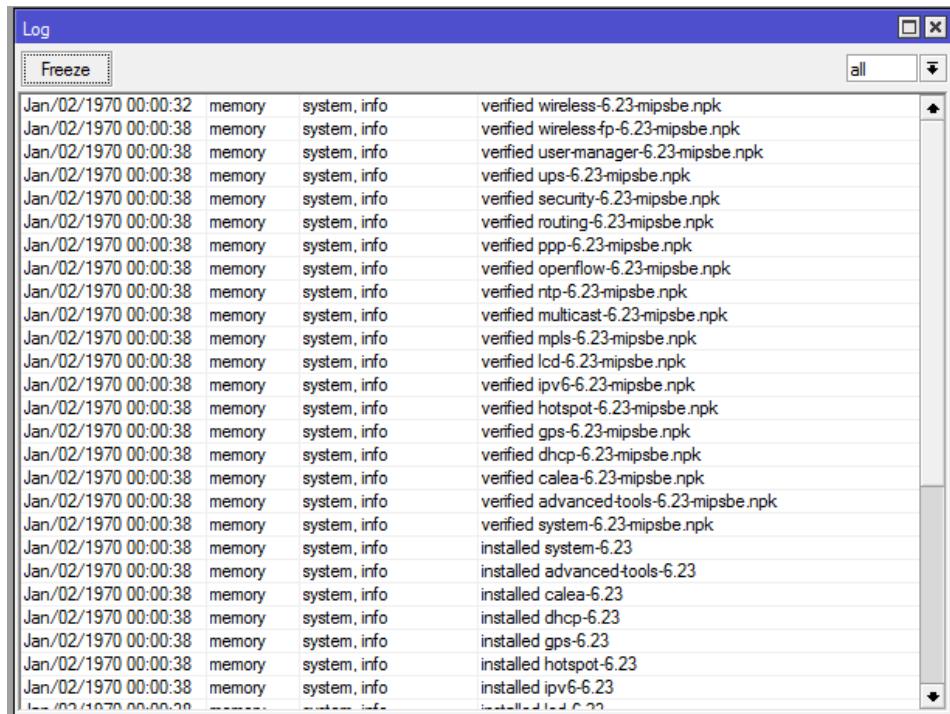


Kita juga bisa melihat paket dari mikrotik yang sudah ter-upgrade , caranya adalah dengan mengklik menu System > Packages. Maka akan terlihat versi dari paket mikrotik akan berubah menjadi versi 6.23

Name	Version	Build Time	Scheduled
advanced-tools	6.23	Dec/04/2014 14:46:06	
calea	6.23	Dec/04/2014 14:46:06	
dhcp	6.23	Dec/04/2014 14:46:06	
gps	6.23	Dec/04/2014 14:46:06	
hotspot	6.23	Dec/04/2014 14:46:06	
ipv6	6.23	Dec/04/2014 14:46:06	
lcd	6.23	Dec/04/2014 14:46:06	
mpls	6.23	Dec/04/2014 14:46:06	
multicast	6.23	Dec/04/2014 14:46:06	
ntp	6.23	Dec/04/2014 14:46:06	
openflow	6.23	Dec/04/2014 14:46:06	
ppp	6.23	Dec/04/2014 14:46:06	
routing	6.23	Dec/04/2014 14:46:06	
security	6.23	Dec/04/2014 14:46:06	
system	6.23	Dec/04/2014 14:46:06	
ups	6.23	Dec/04/2014 14:46:06	

19 items

Kemudian kita lihat apakah terjadi kesalahan/error pada saat mengupgrade paket , untuk melihatnya klik menu Log



The screenshot shows a window titled "Log" with a "Freeze" button. The log entries are as follows:

Date	Type	Category	Message
Jan/02/1970 00:00:32	memory	system, info	verified wireless-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified wireless-fp-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified user-manager-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified ups-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified security-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified routing-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified ppp-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified openflow-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified ntp-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified multicast-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified mpls-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified lcd-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified ipv6-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified hotspot-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified gps-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified dhcp-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified calea-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified advanced-tools-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	verified system-6.23-mipsbe.npk
Jan/02/1970 00:00:38	memory	system, info	installed system-6.23
Jan/02/1970 00:00:38	memory	system, info	installed advanced-tools-6.23
Jan/02/1970 00:00:38	memory	system, info	installed calea-6.23
Jan/02/1970 00:00:38	memory	system, info	installed dhcp-6.23
Jan/02/1970 00:00:38	memory	system, info	installed gps-6.23
Jan/02/1970 00:00:38	memory	system, info	installed hotspot-6.23
Jan/02/1970 00:00:38	memory	system, info	installed ipv6-6.23

Ternyata tidak ada paket yang gagal terupload, berarti proses pengupgrade an sudah selesai . Selanjutnya adalah Downgrade.

DOWNGRADE :

Untuk downgrade caranya hampir sama hanya saja yang berbeda adalah paket yang diupload , jika dalam Upgrade kita upload versi terbaru maka di Downgrade kita upload versi sebelumnya. Jadi kita download versi sebelumnya lalu kita upload. Jika sudah Kita klik tab **Downgrade** , maka Router akan langsung terdowngrade.

Untuk downgrade saya gak masukin Gambarnya karena intinya sama aja. Mohon maaf yaa

Oke sekian dulu tentang Upgrade dan Downgrade Paket di Mikrotik. Semoga tutorial yang singkat ini bermanfaat.

Wassalam !

Reset Configuration

Assalamualaikum wr.wb

Oke sob selanjutnya di Lab ini saya mau ngebahas tentang cara Reset Configuration di Mikrotik. Reset ini digunakan jika kita ingin mereset semua konfigurasi yang sudah dibuat sebelumnya. Didalam reset configuration ini nantinya semua konfigurasi akan tereset tergantung jenis reset yang dipilih , kecuali Username **Admin** dan Password <kosong>. Reset configuration ini ada 2 cara untuk melakukannya yaitu dengan Hard Reset dan juga Soft Reset yang akan saya bahas di 2 lab yang berbeda.

Lab 9. Hard Reset Configuration

Seperti yang saya jelaskan sebelumnya bahwa didalam mereset konfigurasi ada 2 cara yaitu Hard dan Soft Reset. Di Lab ini saya bakal jelasin cara Reset Configuration secara Hard Reset atau secara Hardware. Jika kita melakukan reset secara Hardware maka Router akan kembali ke pengaturan Pabrik.

Cara untuk meresetnya adalah cari bagian lubang kecil yang ada di RouterBoard, kemudian gunakan benda kecil seperti lidi atau ujung pulpen untuk menekan tombol yang ada didalemnya. Kalo saya biasanya pakai pulpen (*maklum pelajar rajin jadi kemana-mana harus bawa pulpen ☺*)



Jadi pertama kita tekan tombol reset yang ada didalam lubang kecil itu dengan lidi atau pulpen kemudian colokkan kabel power ke RouterBoard , nanti lampu ACT akan berkedip dan tunggu sampai matang dan tiriskan *eeehh salah*. Maksudnya tunggu sampai lampu ACT berhenti berkedip.

Kalo kurang jelas begini langkahnya :

1. Colokkan Lidi/Ujung pulpen ke lubang reset ,
2. Tekan tombol reset secara perlahan (jangan terlalu keras) , sampai terasa tertekan saja.
3. Colokkan kabel Power ke Routerboard
4. Tunggu sampai lampu ACT berhenti Berkedip

Oke jika sudah selesai berkedip maka RB akan kembali kepengaturan pabrik dengan **IP 192.168.88.1**.

Oke sekian dulu masbroo tentang Hard Reset , di Lab berikutnya bakal ngebahas cara Soft Resetnya.

Wassalam !

Lab 10. Soft Reset Configuration

Assalamualaikum wr.wb

Setelah dilab sebelumnya saya ngabahas cara Hard Reset , di lab ini saya mau ngebahas cara ngerest yang satu lagi , yaitu dengan cara Soft Reset. Maksud dari Soft Reset adalah kita meresetnya melalui Winbox atau alat remote yang lain. Jadi tidak perlu lagi colok menyolok pake pulpen atau lidi.

Di Soft Reset ini kita bisa memilih jenis reset nya. Ada 3 jenis resetnya yaitu :

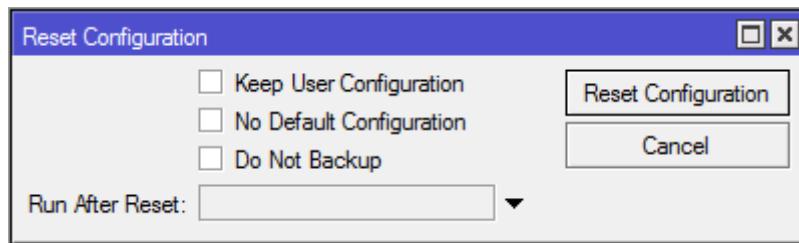
- **Keep User Configuration** = Artinya semua user dan password yang kita tambahkan tidak akan terhapus.
- **No-Defaults** = artinya semua konfigurasi akan di reset/dihapus tanpa terkecuali.
- **Do Not Backup** = Artinya semua konfigurasi akan di reset termasuk file backupan.

Kemudian jika kita hanya memilih Reset-configuration biasa maka hasilnya akan sama seperti Hard Reset , yaitu akan kembali ke pengaturan pabrik.

Oke karena sudah tau teorinya sekarang langsung ke langkah konfigurasinya , untuk CLI bisa gunakan perintah

```
[admin@Untung] > System reset-configuration [jenisresetnya]
```

Kemudian untuk GUI nya kita bisa klik menu **System > Reset-Configuration** , lalu pilih jenis resetnya kemudian klik Reset Configuration



Jika sudah maka mikrotik akan ter-Reboot secara otomatis.

Oke sekian dulu pembahasan tentang Reset-Configuration di Mikrotik.

Reset-configuration ini sangat bermanfaat buat orang-orang yang baru belajar seperti saya, jadi kalo misalkan ada kesalahan dan gak mau ribet mending direset aja ahaha 😊.

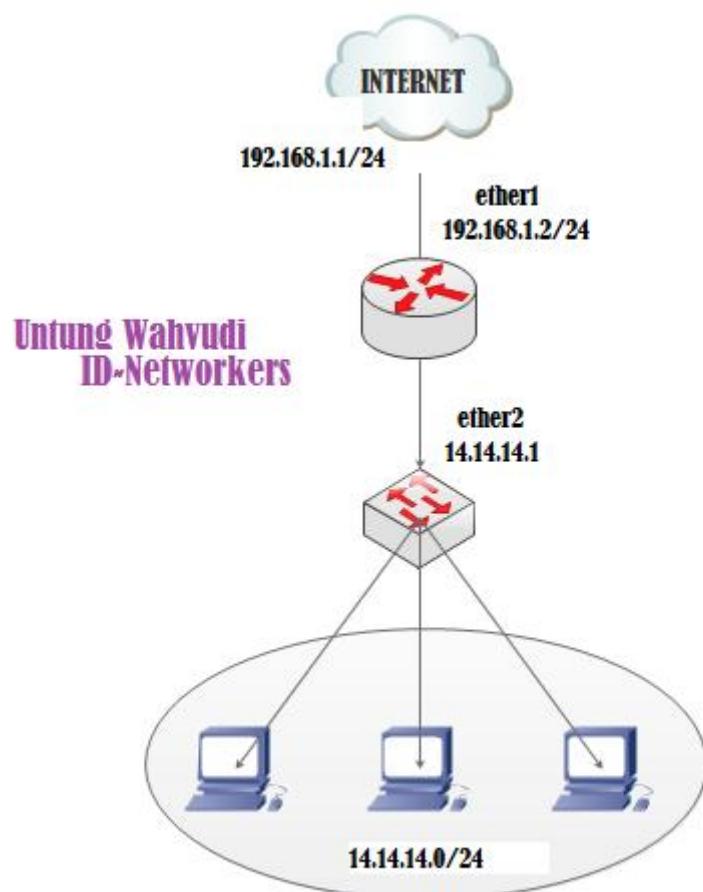
Wassalam !

LAB 11. Koneksi Internet.

Assalamualaikum wr.wb

Setelah beberapa lab sebelumnya masih ngebahas tentang konfigurasi dasar , di Lab ini saya mau naikin lagi tingkatannya yaitu tentang fungsi utama dari sebuah router , apalagi kalo bukan ngehubungin jaringan yang berbeda. Disini Router Mikrotik akan ngehubungin jaringan lokal kita ke jaringan Internet. Menarik bukan ???

Sebelum ke konfigurasi kita bahas dulu skenarionya , kurang lebih topologinya seperti ini.



Langkah Konfigurasi :

1. Menambahkan IP Address

Yang pertama kali harus kita lakukan adalah menambahkan IP address untuk **ether1 yang ke Internet** dan **ether2 yang ke jaringan local**.

Untuk menambahkan IP address melalui CLI bisa gunakan perintah

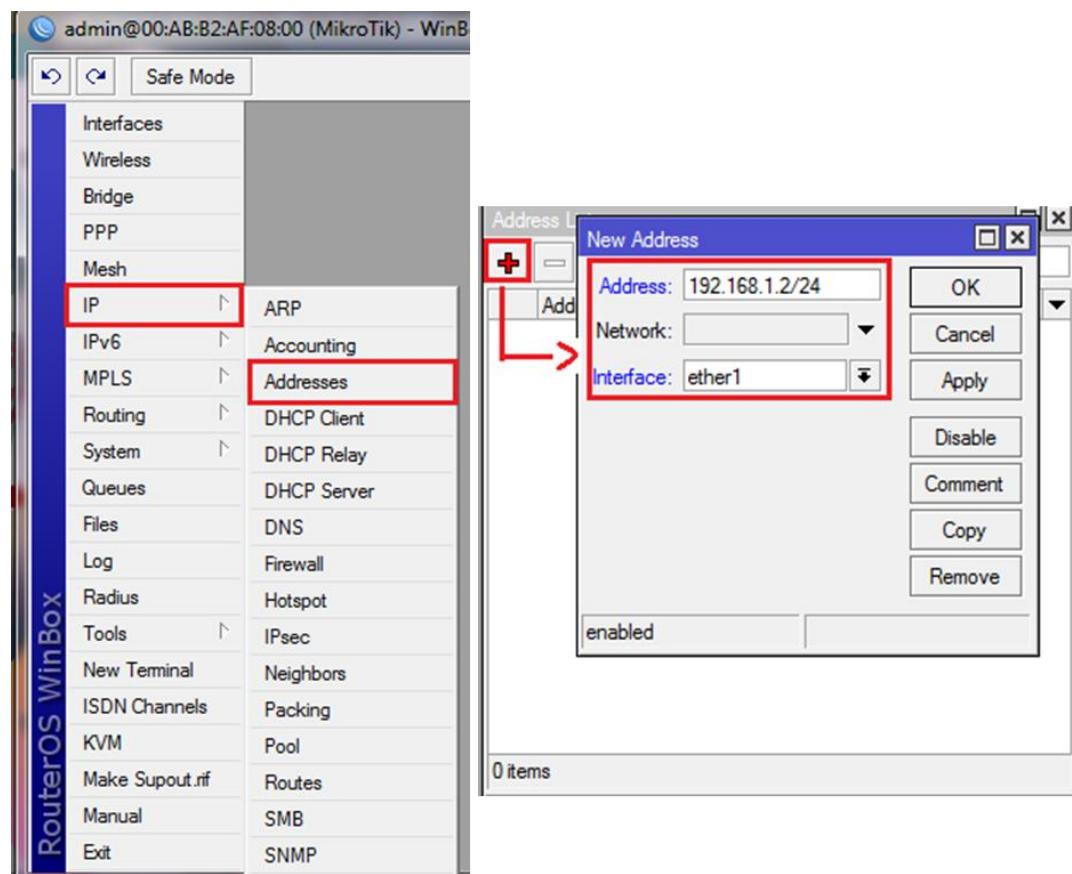
(Untuk IP address Public)

```
[admin@untung> ip address add address=192.168.1.2/24 interface=ether1
```

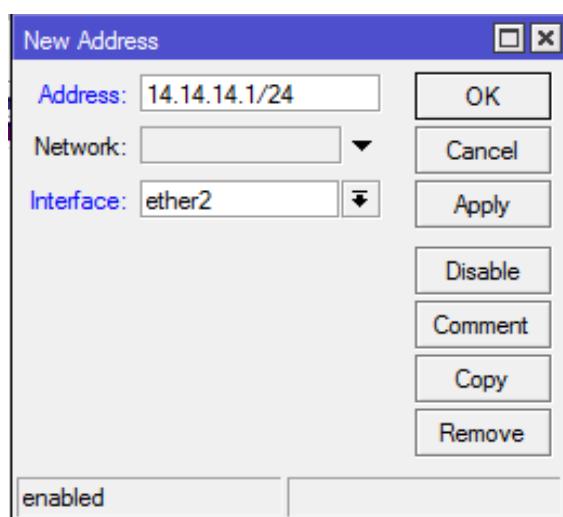
(Untuk IP address Lokal)

```
[admin@untung> ip address add address=14.14.14.1/24 interface=ether2
```

Untuk GUI klik menu **IP > Addresses > +**, kemudian masukkan IP address untuk ke internet (public). Jangan lupa pilih interfacenya yang mengarah ke Internet.



Kemudian masukkan pula untuk IP localnya. IP local ini nantinya akan digunakan client sebagai gateway untuk ke Internet.



Jika sudah maka hasilnya akan seperti ini :

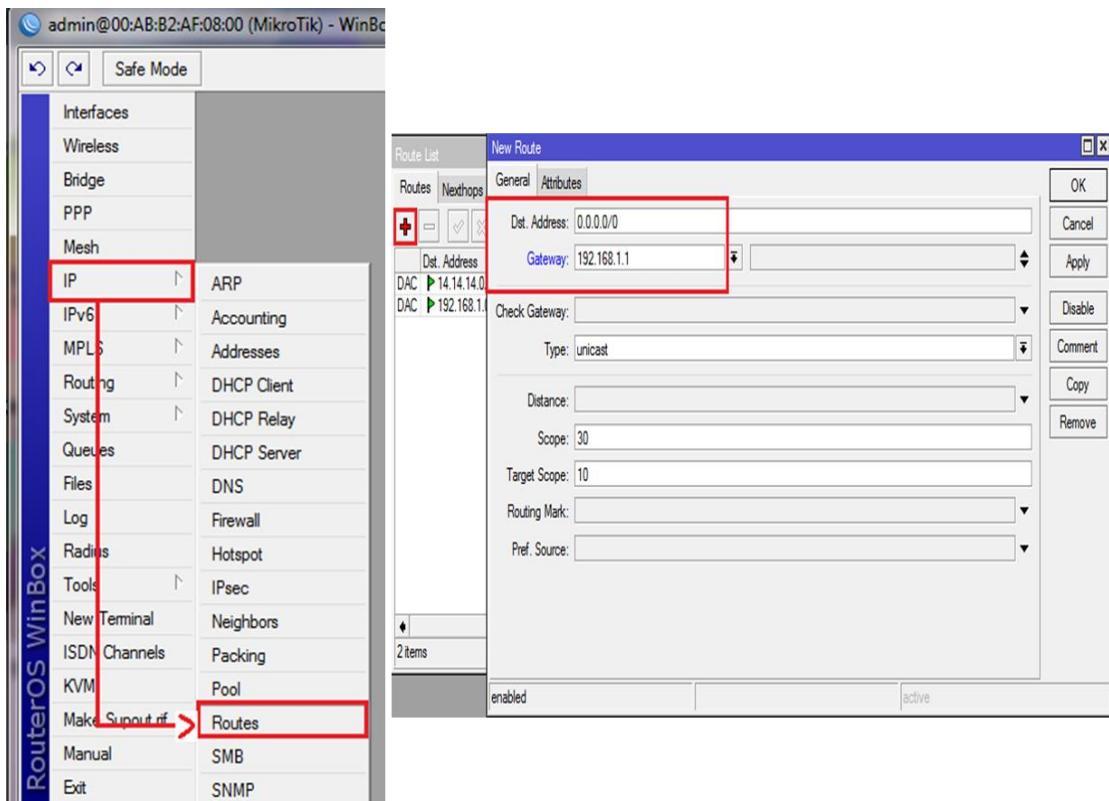
Address List			
	Address	Network	Interface
+	14.14.14.1/24	14.14.14.0	ether2
+	192.168.1.2/24	192.168.1.0	ether1
2 items			

2. Menambahkan Default Gateway

Karena fungsi utama router adalah menghubungkan jaringan maka diperlukan yang namanya proses Routing. Proses Routing ini adalah proses dimana router menghubungkan beberapa jaringan yang berbeda menjadi satu segmen. Disini kita akan melakukan proses Routing menggunakan Routing Static jadi kita harus memasukkan sendiri Alamat tujuan dan jalur yang akan dilewati. (*Untuk pembahasan mendalam mengenai Static Routing nanti bakal di Bahas di Lab yang lain*). Karena disini Router ingin menghubungkan jaringan Lokal dengan Jaringan Internet maka dari itu tujuan (dst-address) nya adalah 0.0.0.0/0 yang artinya mewakili berjuta-juta IP yang berada di internet. Dan gatewanya adalah IP dari ISP itu sendiri. Untuk konfigurasi CLI nya bisa gunakan perintah :

```
[admin@untung> ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1
```

Untuk mode GUI nya kita klik menu **IP > Routes > +** kemudian masukkan **dst-addressnya=0.0.0.0/0 gateway=192.168.1.1**



3. Konfigurasi DNS

Selanjutnya kita akan mengatur DNS , DNS adalah singkatan dari Domain Name Server , yang berfungsi untuk pemetaan alamat IP menjadi sebuah nama atau sebaliknya. Sebagai contoh ketika kalian browsing , apakah kalian pernah mengetikkan IP dari server website tersebut ??

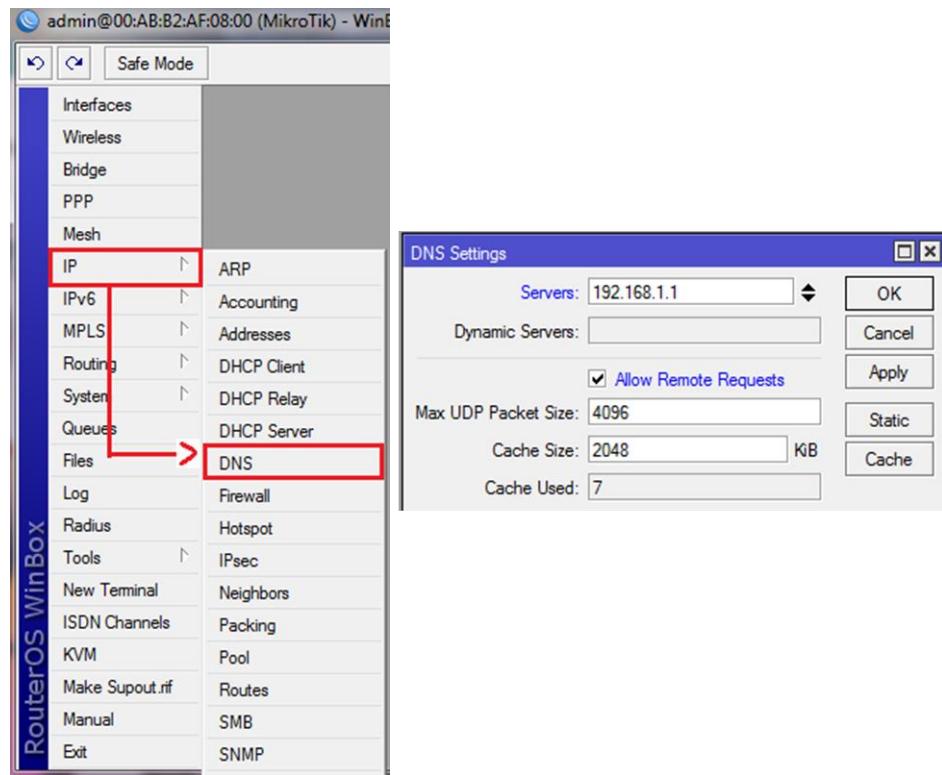
contoh ketika mengakses google , anda pasti selalu mengetikkan www.google.com atau google.com saja kan. Dan anda mungkin tidak tau berapa alamat IP dari google. Nah itulah fungsi dari DNS yang mengubah alamat IP menjadi sebuah nama , jadi kita akan lebih mudah mengakses Website di Internet. Untuk konfigurasi DNS di Mikrotik caranya cukup mudah , kita hanya perlu **memasukkan alamat IP dari DNS Server**, kita bisa menggunakan DNS dari ISP atau juga bisa menggunakan DNS google (8.8.8.8 / 8.8.4.4).

Untuk konfigurasi melalui CLI bisa gunakan perintah

```
[admin@untung> ip dns set servers=192.168.1.1 allow-remote-requests=yes
```

*Maksud dari **Allow-remote-request=yes** adalah agar client nantinya tidak perlu menggunakan DNS dari ISP lagi , cukup menggunakan DNS Mikrotik yaitu IP yang kejaringan **local (ether2)**.*

Untuk mode GUI kita klik menu IP > DNS kemudian masukkan alamat IP DNS Servernya lalu centang bagian Allow-remote-request.



Sekarang coba test ping ke google dari Router , jika konfigurasinya benar maka hasilnya pasti sudah bisa ping ke Google.com

```
[admin@MikroTik] > ping google.com
HOST                                         SIZE TTL TIME STATUS
111.94.248.46                                56  58 95ms
111.94.248.46                                56  58 69ms
111.94.248.46                                56  58 65ms
111.94.248.46                                56  58 93ms
111.94.248.46                                56  58 54ms
sent=5 received=5 packet-loss=0% min-rtt=54ms avg-rtt=75ms max-rtt=95ms

[admin@MikroTik] >
```

4. Konfigurasi NAT

Sekarang router kita sudah bisa terhubung ke internet. Nah untuk membuat PC client juga bisa melakukan koneksi Internet maka dibutuhkan yang Namanya **NAT atau Network Address Translation** , NAT ini berfungsi untuk menterjemahkan/menyamarkan alamat IP Lokal kita menjadi alamat IP Public kita. Coba bayangan berapa banyak jaringan lokal yang memiliki IP Private sama seperti kita , jika kita tidak translate ke IP public maka website akan susah merespons permintaan karena banyaknya alamat IP lokal yang sama. Maka dari itu NAT sangat dibutuhkan di jaringan Internet.

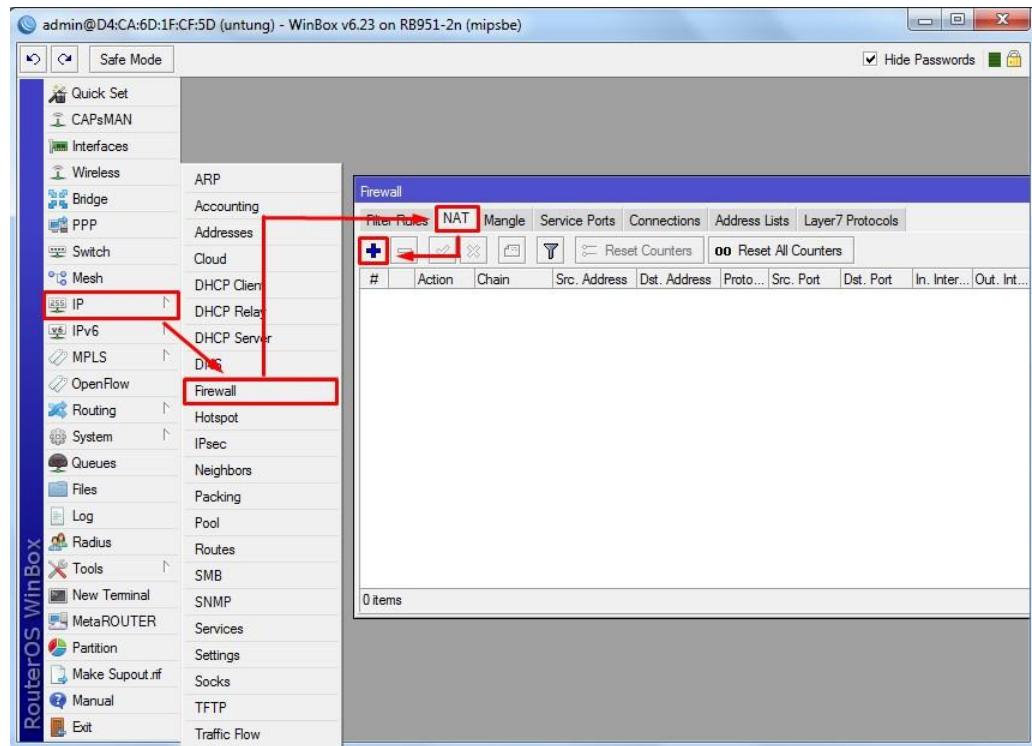
Untuk konfigurasi di Mikrotik caranya adalah sebagai berikut

```
[admin@untung> ip firewall nat add chain=srcnat out-interface=ether1  
action=masquerade
```

Yuk kita coba terjemahin perintah diatas , kalo saya nerjemahinnya kurang lebih seperti ini gan :

*"Jika ada paket yang lewat berasal dari **Source (sumber)** dan ingin keluar melalui **ether1** maka akan di samarkan (masquerade)"*

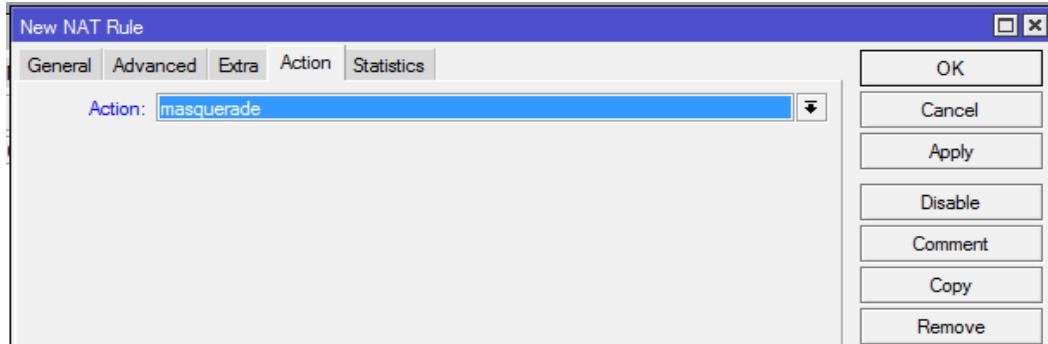
Untuk mode GUI kita klik menu IP > Firewall > NAT > +



Setelah itu masukkan isikan bagian **Chain** dan **Out-interface** , untuk Out-interface masukkan interface yang mengarah ke ISP (Internet)

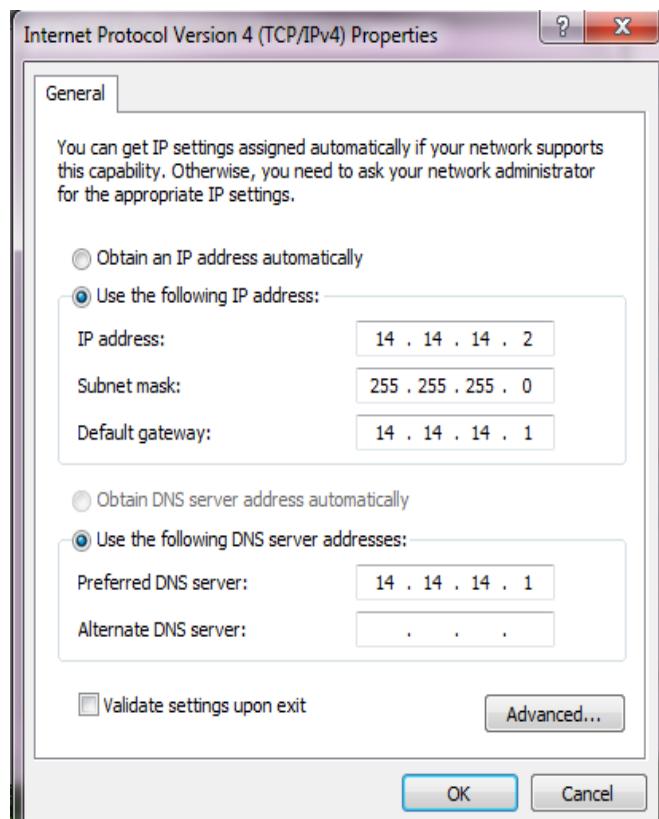
This screenshot shows the 'New NAT Rule' dialog box. It has several tabs: General (which is selected and highlighted with a red box), Advanced, Extra, Action, and Statistics. The 'General' tab contains fields for 'Chain' (set to 'srcnat'), 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'Any. Port', 'In. Interface' (set to 'ether1'), and 'Out. Interface' (set to 'ether1'). To the right of the dialog box is a vertical toolbar with buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Jangan lupa di tab action , isikan dengan **action = masquerade**

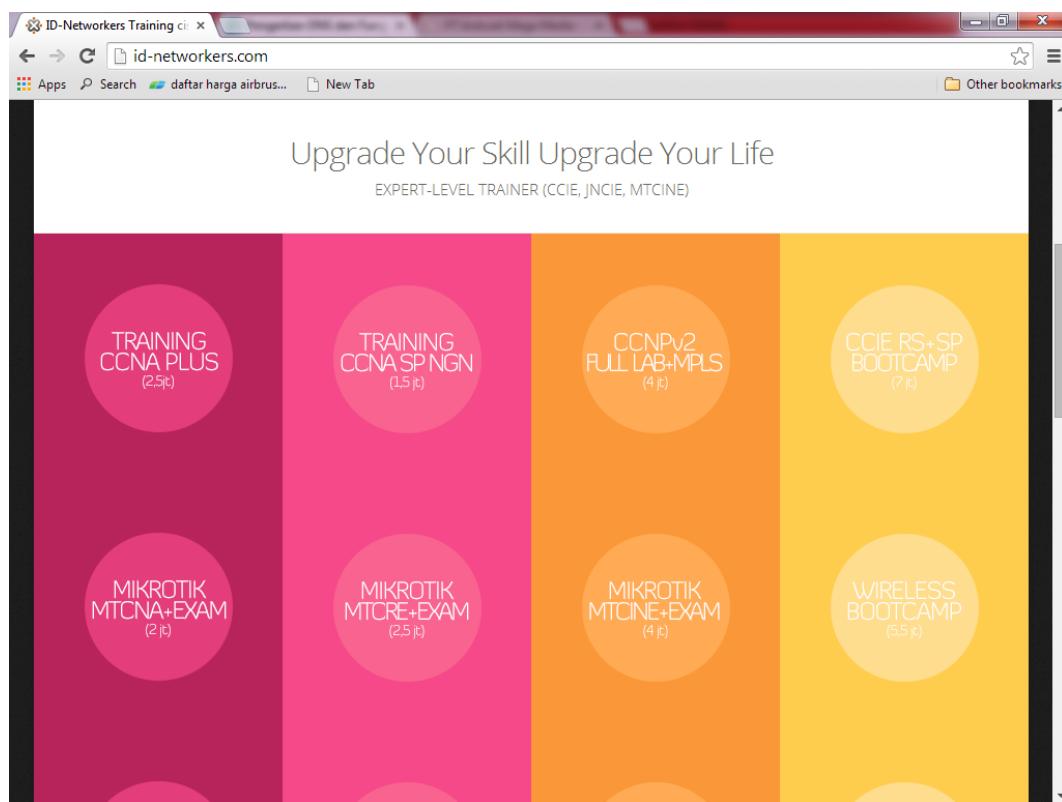


4. Pengujian di Client.

Setelah konfigurasi NAT telah selesai tiba saatnya kita untuk mengetest nya di sisi client. Yang pertama harus dilakukan adalah ganti IP Client menjadi 1 Network dengan IP interface ether2.



Kemudian silahkan test browsing. InshaAllah pasti berhasil



Oke karena client sudah bisa internetan maka artinya sudah berhasil. Seengganya kalian udah bisa buat jaringan warnet dengan mikrotik setelah membaca tutorial ini. Kalo untuk pembahasan lebih kompleksnya bakal dijelasin di lab lab berikutnya. Oke sekian dulu

Wassalam !

LAB 12. Network Time Protocol Client.

Assalamualaikum wr.wb

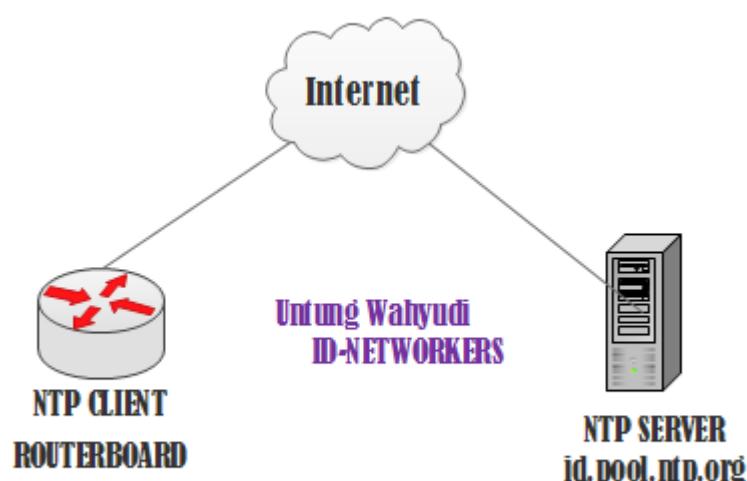
Karena sebelumnya saya sudah ngebahas tentang cara koneksi RouterBoard dengan Internet , selanjutnya di Lab ini saya mau ngebahas tentang waktu di Mikrotik. Waktu di Mikrotik ini sangat penting keberadannya , karena dibeberapa kondisi Router membutuhkan konfigurasi Waktu yang tepat. Karena router Mikrotik tidak memiliki baterai CMOS seperti di PC makanya setiap saat router di reboot waktu di RouterBoard akan kembali ke tahun 1970.

Untuk menghindari ketidakjelasan dan ketidakakuratan dari Waktu Routerboard kita harus mengkonfigurasikan sebuah fitur yang bernama NTP atau Network Time Protocol. NTP adalah sebuah protocol yang digunakan untuk melakukan sinkronisasi waktu terhadap perangkat jaringan (NTP Server).

Untuk mengkonfigurasi NTP , kita harus tau IP dari NTP Server yang nantinya kita akan menyesuaikan Waktunya dengan NTP Server tersebut. Di Indonesia ada NTP Server khusus yaitu www.id.pool.ntp.org . dan untuk itu tentunya Router kita harus terhubung ke internet seperti di Lab sebelumnya.

Langkah Konfigurasi :

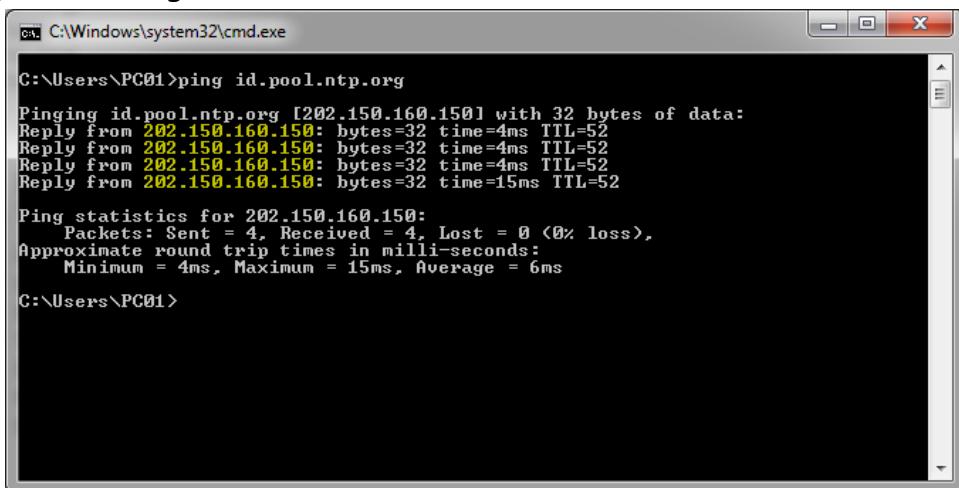
Kita akan buat topologinya kurang lebih menjadi seperti ini



1. Cek IP NTP Server

Yang pertama harus dilakukan adalah melihat IP dari NTP Server nya yaitu **id.pool.ntp.org**, untuk melihatnya bisa menggunakan 2 cara yaitu dengan cara ping dan nslookup.

Dengan Cara Ping :



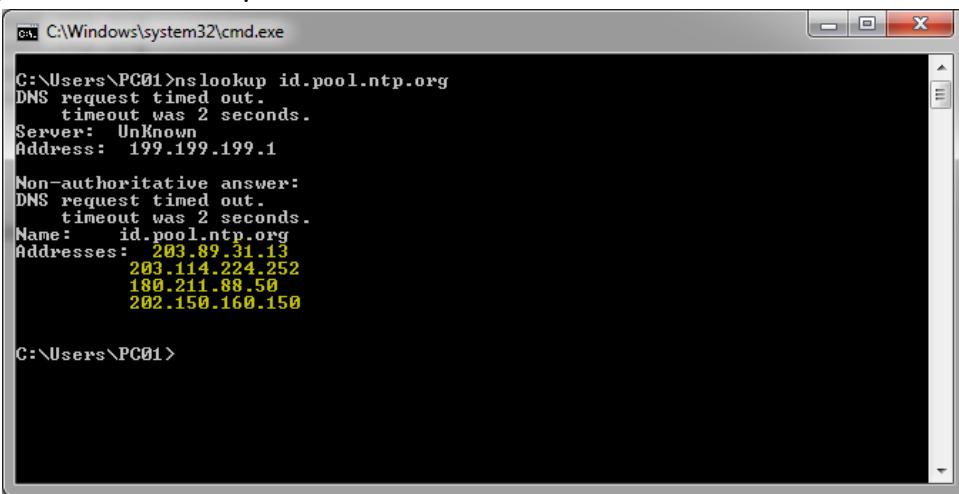
```
C:\Windows\system32\cmd.exe
C:\Users\PC01>ping id.pool.ntp.org

Pinging id.pool.ntp.org [202.150.160.150] with 32 bytes of data:
Reply from 202.150.160.150: bytes=32 time=4ms TTL=52
Reply from 202.150.160.150: bytes=32 time=4ms TTL=52
Reply from 202.150.160.150: bytes=32 time=4ms TTL=52
Reply from 202.150.160.150: bytes=32 time=15ms TTL=52

Ping statistics for 202.150.160.150:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 15ms, Average = 6ms

C:\Users\PC01>
```

Dengan Cara Nslookup:



```
C:\Windows\system32\cmd.exe
C:\Users\PC01>nslookup id.pool.ntp.org
DNS request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  199.199.199.1

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:   id.pool.ntp.org
Addresses:  203.89.31.13
          203.114.224.252
          180.211.88.50
          202.150.160.150

C:\Users\PC01>
```

2. Konfigurasi NTP Client

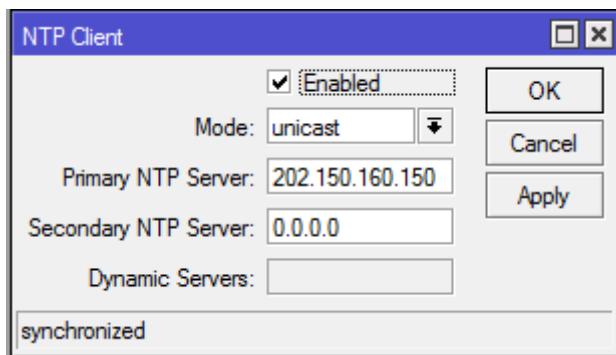
Setelah tau alamat IP dari NTP Server selanjutnya kita configurasi NTP Client di Mikrotik. Untuk CLI bisa gunakan perintah

```
[admin@untung> system ntp client set enable=yes primary-
ntp=202.150.160.150 mode=unicast
```

Atau bisa juga primary-ntp kita isi dengan alamat website NTP Server , menjadi

```
[admin@untung> system ntp client set enable=yes primary-ntp=id.pool.ntp.org  
mode=unicast
```

Untuk mode GUI nya klik menu **System > NTP Client** kemudian isikan alamat ntp servernya dan modenya



3. Pengaturan Zona Waktu

Selanjutnya kita harus mengkonfigurasikan Time Zone sesuai dengan tempat tinggal kita , Misalnya Asia/Jakarta untuk WIB , Asia/Makassar untuk WITA dan Asia/Jayapura untuk WIT.

Untuk mengatur Waktu melalui CLI bisa gunakan perintah

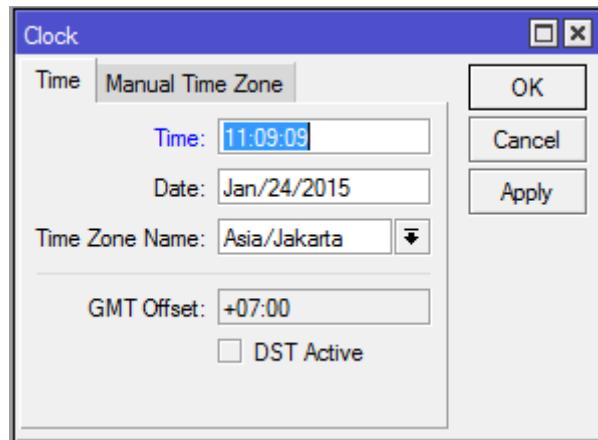
```
[admin@untung> system clock set time-zone-name=Asia/Jakarta
```

4. Pengujian

Kemudian kita cek apakah waktunya sudah sinkron atau belum, dengan perintah

```
[admin@untung> system clock print
```

Atau bisa dilihat lewat GUI dengan cara klik Menu **System > Clock**.



Sekarang waktu di RB kita tidak akan kembali ke Tahun 1970 , selama masih sinkron dengan NTP id.pool.ntp.org

Oke karena sudah berhasil saatnya saya untuk bilang "*sempoaaa!*"

Oke sekian dulu mas dan mba broo , lanjut lagi nanti di lab lab yang menarik untuk dibaca.

Wassalam !

LAB 13. Network Time Protocol Server.

Assalamualaikum warahmatullahi wabarakatuh

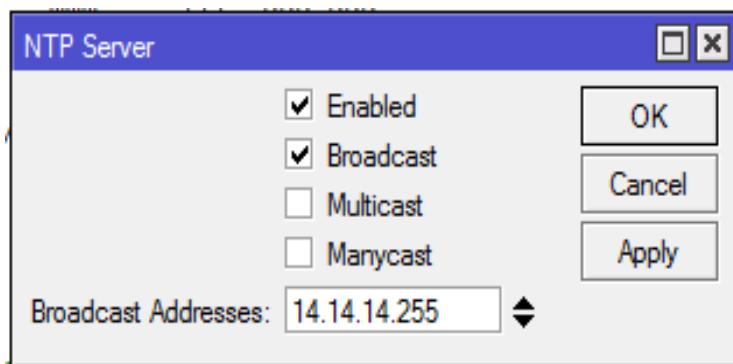
Melanjutkan lab yang sebelumnya , kalo dilab sebelumnya Mikrotik kita sebagai NTP Client maka di sini mikrotiknya akan kita buat menjadi NTP Server.

Untuk konfigurasinya itu sangat mudah mas broo. Kita hanya tinggal mengaktifkan fitur NTP Servernya kemudian kita pilih jenis nya lalu kemudian taraa selesai. Karena kita disini sebagai NTP Server untuk para client yang membutuhkan maka kita setting NTP Servernya dengan mode **Broadcast** , karena kita memiliki lebih dari satu client. Oke dari pada penasaran langsung aja ke konfigurasinya

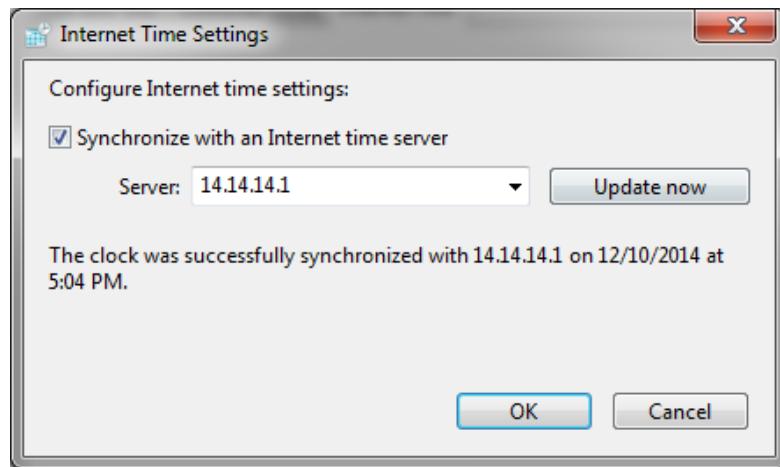
Untuk mode CLI bisa gunakan perintah

```
[admin@untung> system ntp server set enable=yes multicast=no broadcast=yes  
broadcast-addresses=14.14.14.255
```

Untuk mode GUI nya tinggal klik System > NTP Server kemudian isikan seperti dibawah ini , tinggal IP Broadcastnya saja yang disesuaikan.



Kemudian silahkan ditest diclient ,jika clientnya menggunakan PC maka caranya adalah klik dibagian pojok kanan bawah (waktu dan tanggal) kemudian klik date and time setting kemudian pilih yang bagian Internet Time lalu masukkan IP Routernya.



Oke karena sudah berhasil maka saya tutup lab kali ini dengan mengucap Alhamdulillah.

Kurang lebihnya mohon maaf gan

Wassalam !

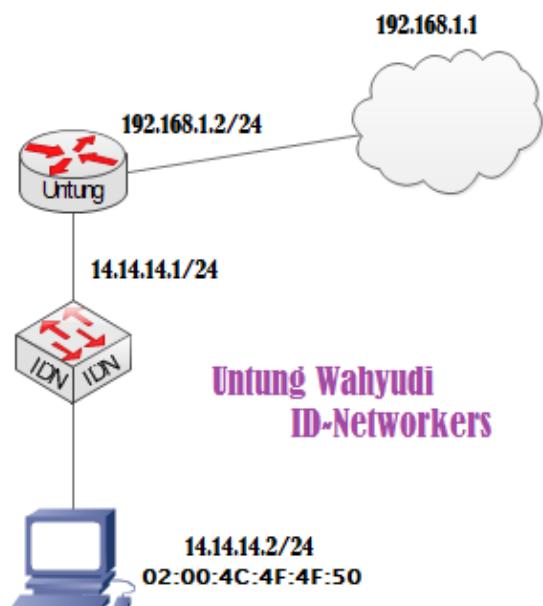
LAB 14. Address Resolution Protocol Static

Assalamualaikum wr.wb

Masih lanjut lagi ke konfigurasi yang masih dibilang dasar tapi bermanfaat. Di lab ini saya mau ngebahas sedikit tentang **ARP** atau **Address Resolution Protocol**. Jadi ARP ini digunakan untuk membuat pemetaan antara IP address dengan MAC Address yang dimiliki suatu komputer. Didalam Mikrotik pemetaan ARP ini dilakukan secara dinamik atau otomatis oleh Router. Namun bisa saja kita buat pemetannya menjadi Static. Tujuan dibuat pemetaan secara static adalah **Agar Komputer client tidak dapat mengubah IP Address sesukanya**. Jika client merubah IP nya maka IP tersebut tidak valid dan akhirnya tidak akan terhubung ke Router bahkan ke Internet.

Langkah Konfigurasi :

Setelah sudah paham tentang konsep ARP selanjutnya kita akan coba membuat ARP di Router menjadi Static. Topologinya kurang lebih seperti ini.



Mari kita bahas kasus diatas, jadi kasusnya saya ingin client dengan IP **14.14.14.2** dan Mac Address **02:00:4C:4F:4F:50** tidak bisa mengganti IP address nya dengan IP address lain. Dan jika dia mengubah IP nya menjadi **14.14.14.3** atau yang lainnya meskipun satu network dia tidak bisa terkoneksi ke Routerboard dan yang pasti gak bisa koneksi internet juga.

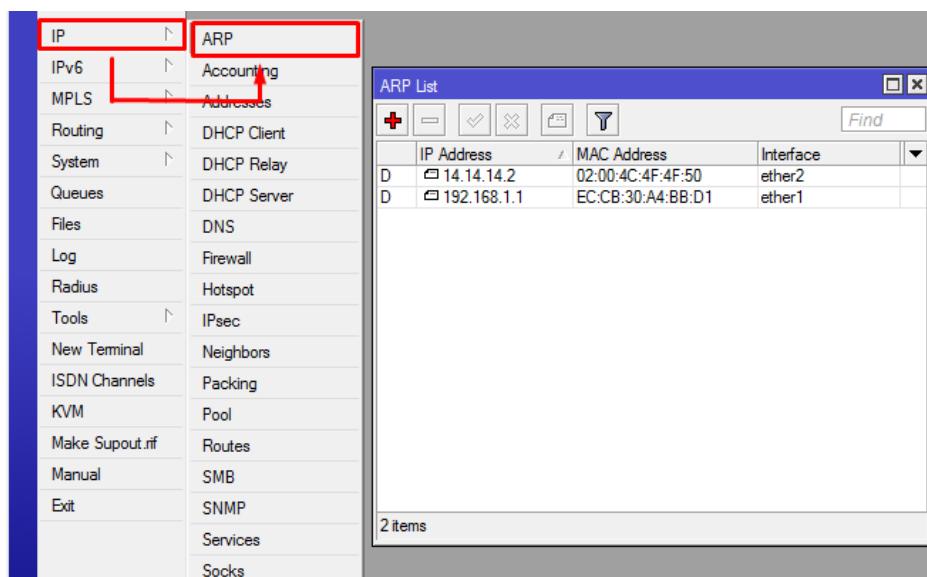
Berikut Langkah konfigurasi nya :

1. Mengecek tabel ARP

Yang pertama harus dilakukan adalah , kita cek dulu tabel ARP yang sudah dibuat oleh router secara otomatis. Sekalian untuk mengecek Mac Address dari IP tersebut. Untuk CLI bisa gunakan perintah

```
[admin@untung] > ip arp print
Flags: X - disabled, I - invalid, H - DHCP, D - dynamic
# ADDRESS MAC-ADDRESS INTERFACE
0 D 14.14.14.2 02:00:4C:4F:4F:50 ether2
1 D 192.168.1.1 EC:CB:30:A4:BB:D1 ether1
[admin@untung] >
```

Untuk mode GUI lakukan dengan cara klik menu **IP > ARP** .



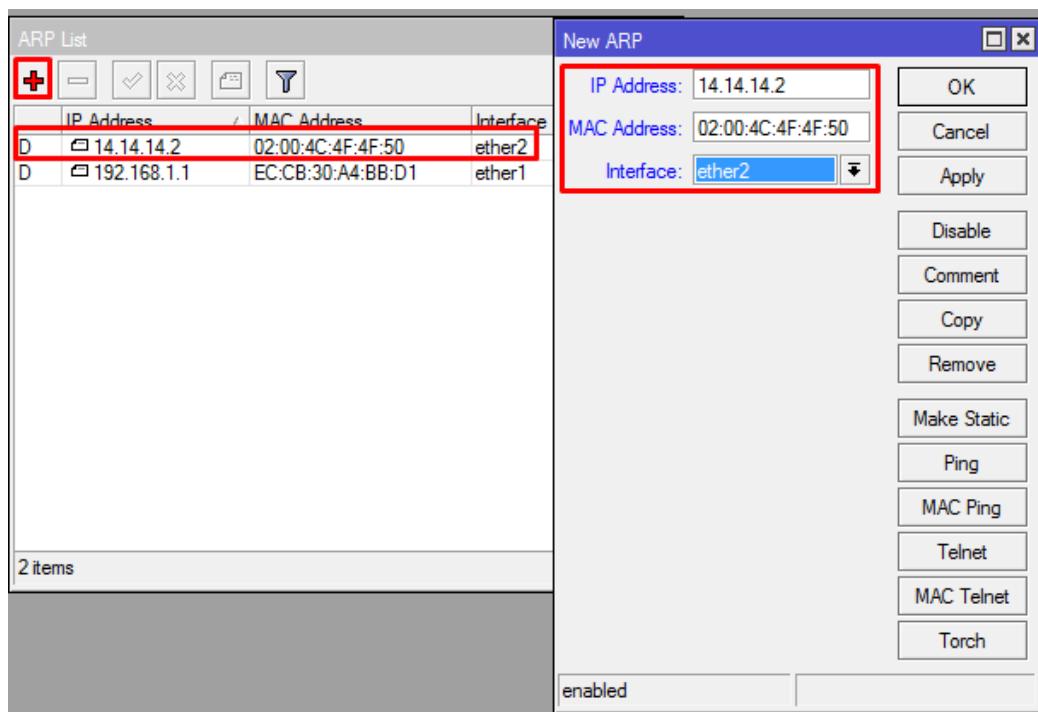
Dari tabel diatas bisa dilihat bahwa IP **14.14.14.2** memiliki Mac address sekian. Dan yang perlu diperhatikan juga huruf “D” didepannya yang berarti **Dynamic**.

2. Pemetaan IP dengan Mac Address

Setelah kita mengetahui MAC Address dari host (komputer) selanjutnya kita akan melakukan pemetaan alamat IP dengan Mac Addressnya. Untuk CLI bisa gunakan perintah

```
[admin@untung> ip arp add address=14.14.14.2 interface=ether2
```

Untuk lewat Winboxnya mudah , setelah di tabel ARP , kita klik tombol Add (+) , lalu masukkan IP address , Mac Address dan Interfacenya.



3. Pengecekan

Untuk melihatnya silahkan lihat kembali tabel ARP nya , huruf "D" yang tadi muncul sekarang sudah tidak ada , itu artinya tabel tersebut sudah bukan Dynamic .

	IP Address	MAC Address	Interface
D	14.14.14.2	02:00:4C:4F:4F:50	ether2
D	192.168.1.1	EC:CB:30:A4:BB:D1	ether1

2 items

Oke mas broo sekian dulu tentang ARP static di Mikrotik. Mohon maaf bila ada kekurangan

Wassalam !

LAB 15. Backup and Restore

Assalamualaikum wr.wb

Setelah diatas membahas banyak tentang konfigurasi konfigurasi , di Lab ini saya mau ngebahas tentang Backup dan Restore. Kalian pasti udah gak asing kan dengan bahasa ini , dan saya yakin kalian pasti tau maksud dari kedua kata tersebut. Jadi saya jelaskan sedikit aja yaa , jadi backup digunakan untuk menyimpan hasil konfigurasi kita. Jadi ketika kita buat kesalahan dalam konfigurasi kita bisa merestore file backupan yang sudah dibuat sebelumnya.

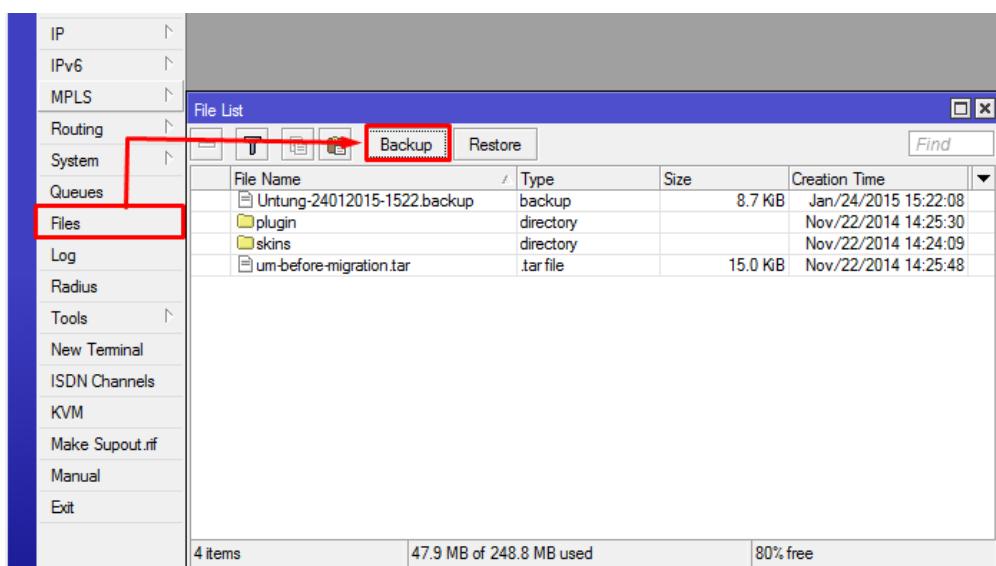
Konfigurasi yang di Backup nantinya akan berupa File , jadi kita bisa pindahkan dan merestorenya di Router Lain. Oke tanpa basa basi langsung aja ke langkah konfigurasinya

BACKUP :

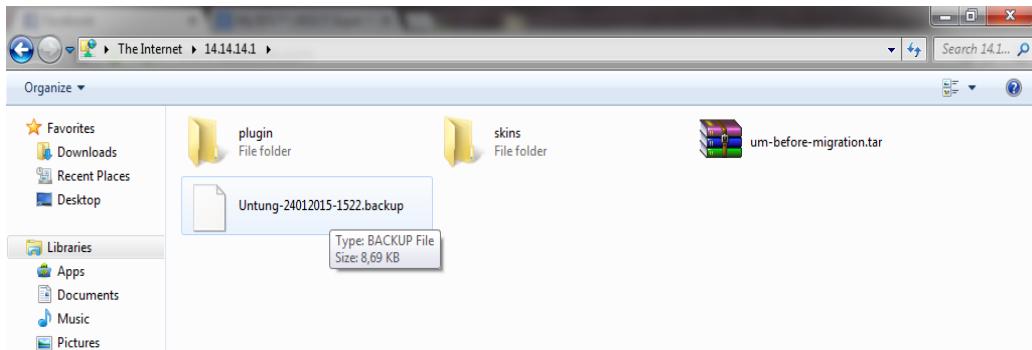
Untuk CLI kita bisa gunakan perintah

```
[admin@Untung] > system backup save name=Untung-backup
Saving system configuration
Configuration backup saved
[admin@Untung] >
```

Kemudian hasil backup dapat dilihat di menu Files , untuk melakukan backup melalui GUI caranya mudah tinggal klik menu Files kemudian klik Backup , maka secara otomatis file backup akan terbuat.



Kita bisa mendownload File backupannya dengan cara *Copy paste* atau *drag n drop* ke PC kita. Namun jika bosan dengan copas atau *drag n drop* dari winbox , kita bisa mendownload filenya di FTP Router tersebut. Caranya adalah ke Windows Explorer kemudian ketikkan **ftp://IPROUTER** , lalu silahkan copy pasti dari FTP tersebut.



RESTORE :

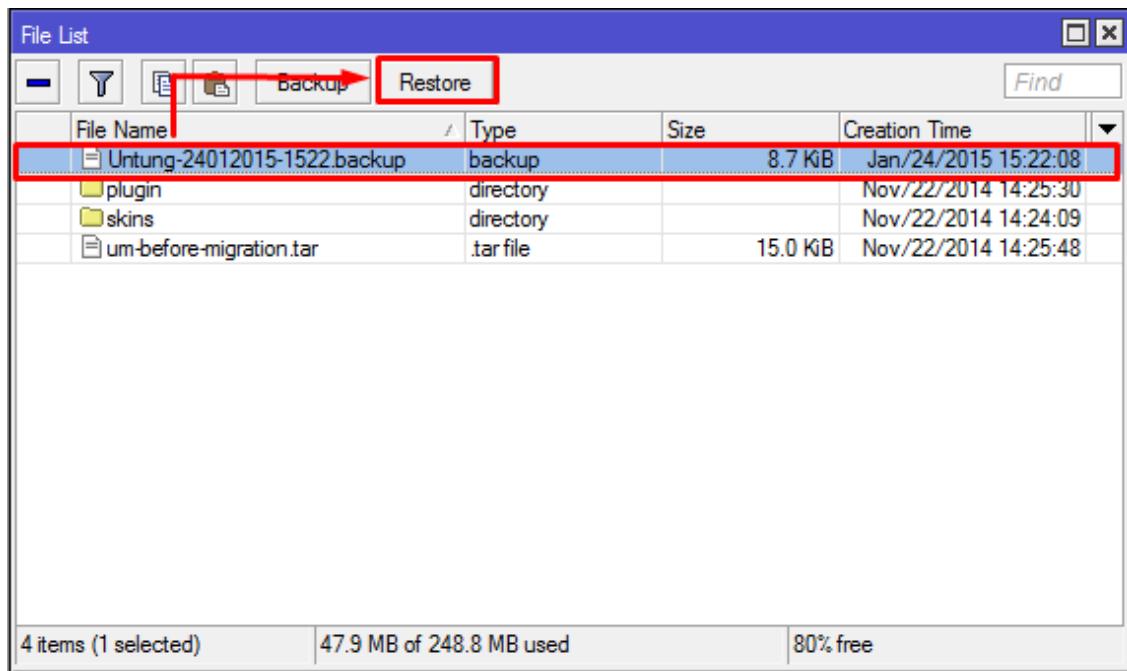
Setelah File di backup , tentu saja kita ingin mengembalikan file backupan tersebut kedalam Router Mikrotik , maka dari itu ada yang namanya fitur **Restore**. Untuk me-restore file backupan tersebut caranya adalah sebagai berikut

Mode CLI :

```
[admin@Untung] > system backup load name=Untung-24012015-1522.backup
Restore and reboot? [y/N]:
```

Saat kita merestore maka kita diminta untuk mereboot Router Mikrotik , ikutin aja kemauan si Router , daripada nanti ngambek ☺

Untuk Mode GUI tinggal klik menu **Files** kemudian pilih file backup-an yang tadi dibuat lalu klik bagian **Restore**. Kemudian reboot Routernya seperti biasa.



Oke sekian dulu ya tentang cara Backup dan Restore konfigurasi di Mikrotik.

Semoga hal yang sederhana ini bermanfaat untuk kita semua.

Wassalam !

LAB 16. Export Import

Assalamualaikum wr.wb

Lanjut lagi pembahasan dari lab sebelumnya , di Lab ini sebenarnya gak beda jauh dengan lab sebelumnya yaitu untuk membackup konfigurasi juga , namun bedanya disini dengan menggunakan fitur yang lain yaitu dengan menggunakan perintah Export Import. Ada beberapa perbedaan antara Backup Restore dan Export Import. Diantaranya yang saya tau adalah :

1. **Backup**, membackup seluruh konfigurasi , sedangkan **Export** kita bisa memilih konfigurasi apa saja yang akan di backup.
2. **Backup restore** , bisa dilakukan dengan mode GUI dan CLI sedangkan **Export Import** hanya bisa dengan mode CLI atau terminal saja.

Cuma itu yang saya tau perbedaannya. Kalo kurang jelas monggo di googling. Di sini Cuma ngebahas yang pernah saya Lab-in aja jadi gak saya bahas lebih mendalam.

Langsung aja ke langkah konfigurasinya.

Untuk melakukan export import kita hanya bisa melakukannya di mode CLI saja, berikut konfigurasi nya

EXPORT :

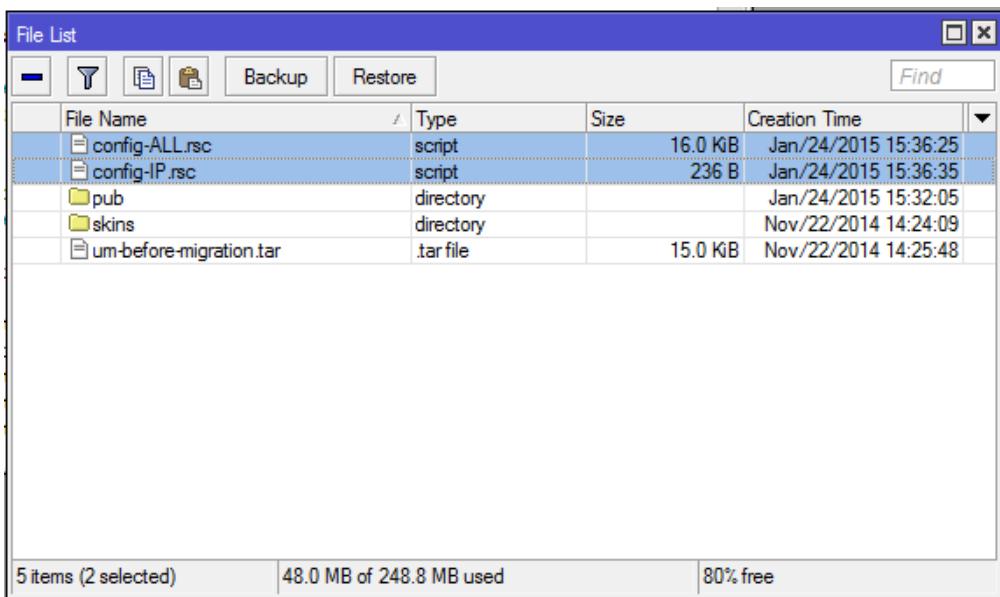
Untuk export kita bisa menggunakan perintah seperti dibawah ini, sebelumnya saya udah bilang kalo export ini bisa membackup konfigurasi yang kita inginkan saja , jadi gambar dibawah ini saya kasih 2 contoh yaitu backup keseluruhan dan backup konfigurasi IP.

```
[admin@Untung] > export file=config-ALL
[admin@Untung] > ip address export file=config-IP
[admin@Untung] >
```

Kemudian file nya bisa langsung dilihat di menu Files , untuk melihat nya di mode CLI bisa dengan cara mengetikkan perintah dibawah ini. File hasil Export akan berupa ekstensi .rsc

```
[admin@Untung] > file print
# NAME          TYPE
0 skins         directory
1 um-before-mi... .tar file
2 config-ALL.rsc script
3 config-IP.rsc script
4 pub           directory
[admin@Untung] >
```

Untuk mengecek di GUI bisa klik menu Files nya. Disana bisa dilihat file hasil Export kita yang memiliki ekstensi .rsc. besarnya file dan tanggal peng-export-annya.



IMPORT :

Import ini digunakan untuk mengembalikan file Export. Untuk melakukan export bisa gunakan perintah berikut

```
[admin@Untung] > import file-name=config-ALL.rsc
Opening script file config-ALL.rsc
Script file loaded successfully
```

Dan Yap , file sudah ter-import.

Oke mas broo sekian dulu tentang Export Import nya

Wassalam !

LAB 17. Install Ulang RouterBoard dengan Netinstall

Assalamualaikum wr.wb

Oke mas broo lanjut lagi ke lab berikutnya. Di Lab ini saya mau ngebahas menyenggung hardware lagi nih , yaitu bagaimana cara menginstall ulang RouterBoard kita. Salah satu cara menginstall Mikrotik adalah dengan cara Netinstall. *Apaa itu Netinstall ??*. Bagi yang belum tau saya jelasin secara singkat aja yaa , jadi Netinstall adalah sebuah software yang digunakan untuk menginstall ulang RouterBoard ataupun RouterOS , yang perantaranya melalui ethernet.

Nah di lab kali ini saya mau ngebahas cara install ulang Routerboard pake aplikasi itu. Oke tanpa bertele-tele langsung aja ke konfigurasinya yuuk , cuusss !

Oh maaf sebelum ke konfigurasinya pertama tama siapin dulu alat tempurnya

ALAT TEMPUR :

- Software Netinstall
- Paket Mikrotik dengan versi sesuka kalian
- Kabel UTP
- Dan yang paling penting RouterBoard nya.

Oke pertama tama saya jelasin dulu cara download software Netinstallnya. Kita bisa download softwarenya di www.mikrotik.com/download , sesuaikan juga arsitektur dan seri dari RouterBoard. Mendownload Netinstall sama seperti kita mendownload packet mikrotik yang sudah dibahas di Lab sebelumnya.

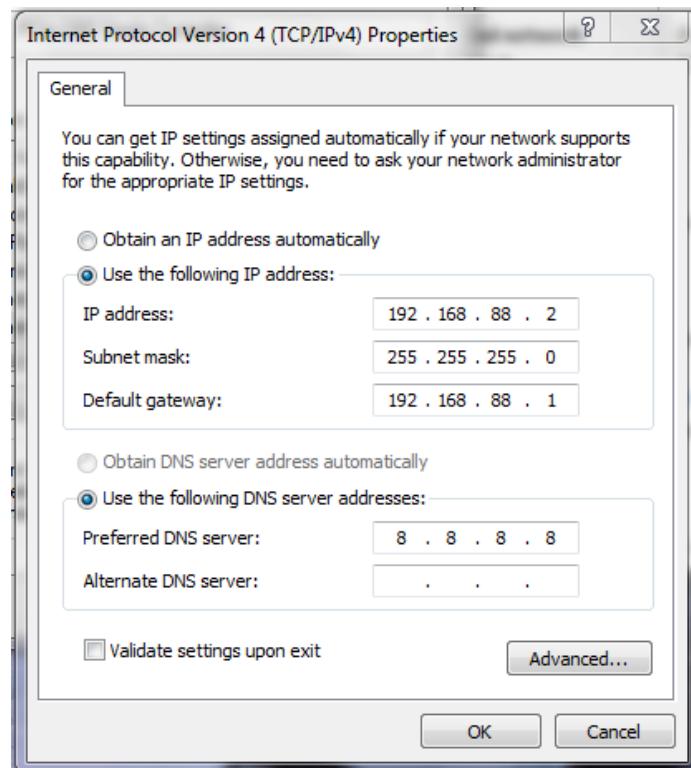
Download MikroTik software products

RouterOS
Please choose your instruction set:

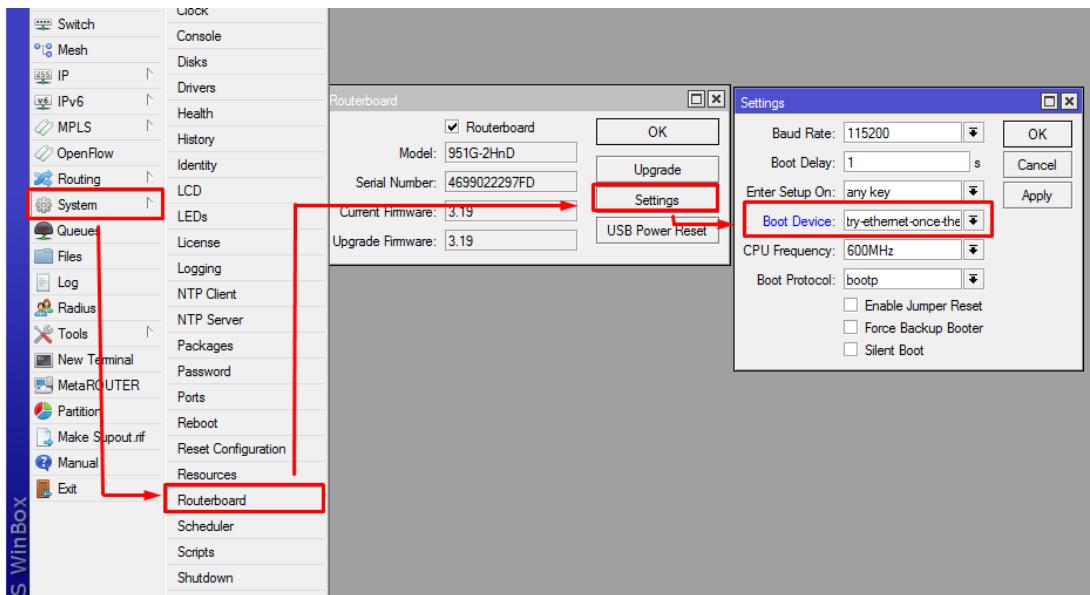
mipsbe CRS series, RB4xx series, RB7xx series, RB9xx series, RB2011 series, SXT, OmniTik, Groove, METAL, SEXTANT

v6.25	2015-Jan-19	v5.26	v4.17
	Upgrade package	Standard upgrade package. Can also be used for Netinstall.	
	All packages	Package with all features including less used ones.	
	Wireless CAPsMANv2	Wireless test package which includes the new CAPsMAN feature (Controlled AP system manager).	
	Netinstall	Utility for installation from network. <small>(Utility for installations from network)</small>	
	Torrent	Downloadable content with Bit-Torrent client.	
	Changelog	View changes in current version.	
	MD5	View MD5 hashes to confirm file validity.	

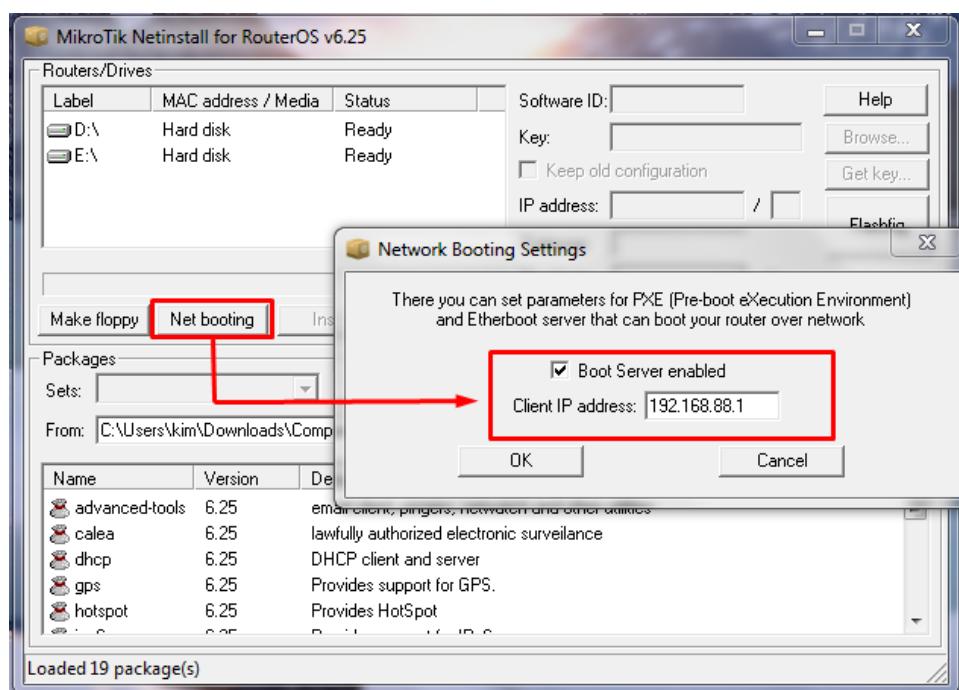
Kemudian sekalian juga download paket mikrotiknya versi berapapun. Jika sudah terdownload. Pastikan RouterBoard telah terpasang ke PC/Laptop kita. Colokkan kabel UTP nya ke Port ether1 (PoE). Jangan lupa masukkan IP PC kita menjadi 1 network dengan RouterBoard.



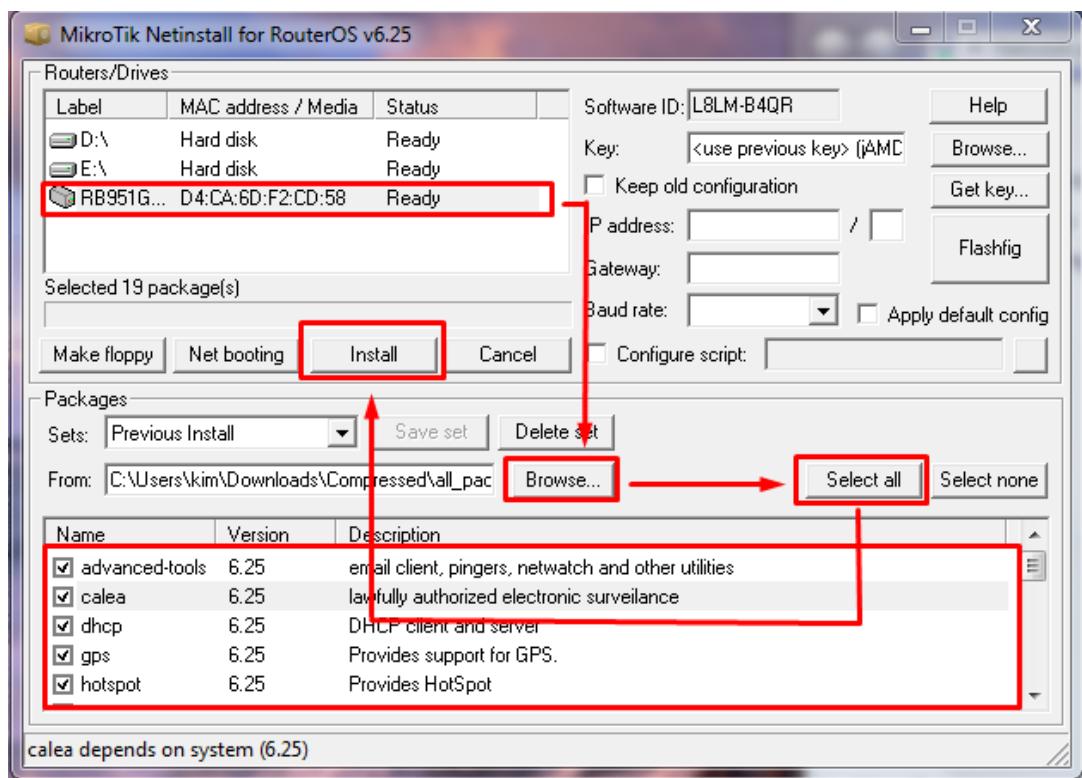
Sama halnya ketika kita ingin menginstall ulang PC , kita juga harus mengatur boot priority di RouterBoard. Untuk mengaturnya silahkan remote RouterBoard lewat winbox kemudian klik menu **System > Routerboard > Settings** kemudian dibagian Boot Device pilih yang “try-ethernet-once-then-nand” artinya kita akan mengatur boot yang pertama adalah lewat ethernet.



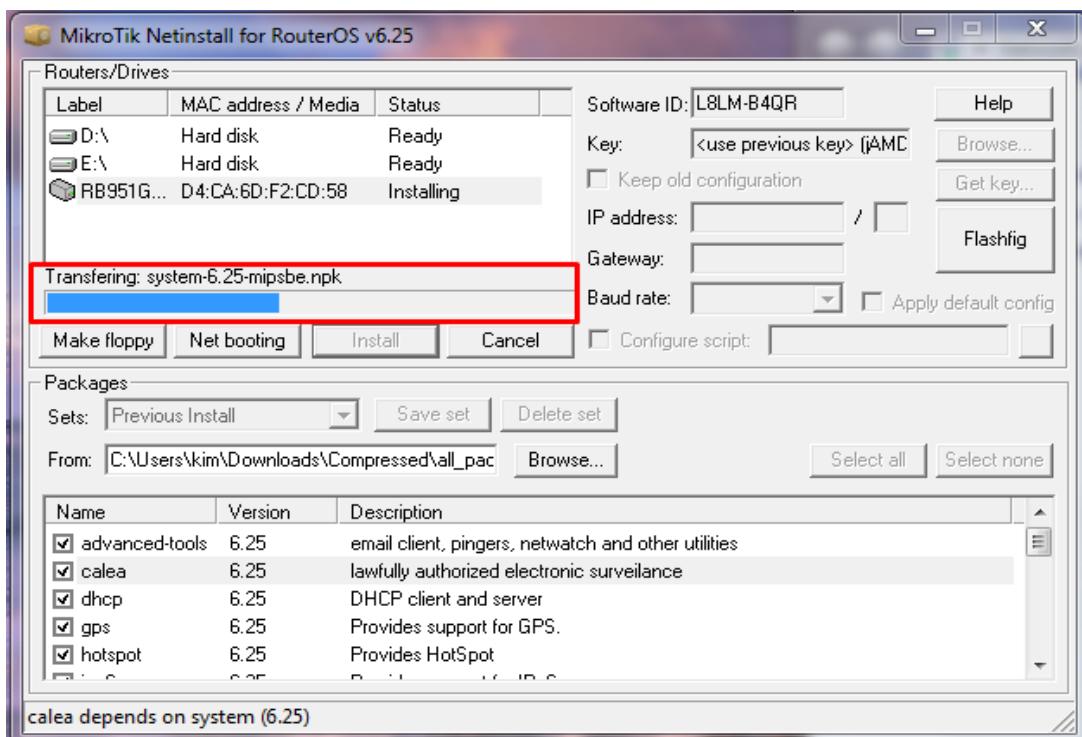
Selanjutnya jalankan program Netinstall , kemudian klik bagian Netbooting lalu masukkan IP dari Router. Karena di sini IP Router saya adalah 192.168.88.1 maka saya masukkan secara default , yaitu ip sekian.



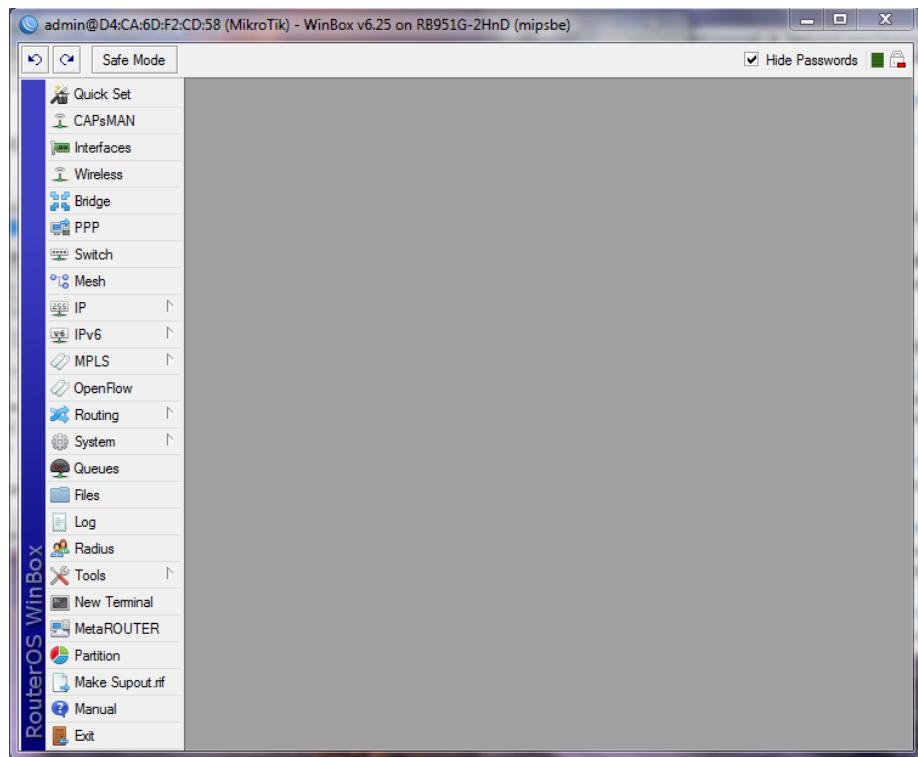
Setelah itu reset RouterBoard dengan cara Hard Reset , dan tunggu sampai Routerboard terdeteksi oleh Netinstall. Jika sudah terdeteksi selanjutnya klik di bagian RouterBoardnya lalu klik bagian **Browse** untuk memasukkan paket yang akan di install di RouterBoard , lalu klik **select All** kemudian klik **install**.



Kemudian proses instalasi akan berjalan , tunggu hingga proses instalasi selesai



Setelah proses instalasi selesai silahkan test login dengan menggunakan winbox, maka hasilnya adalah seperti dibawah ini , RouterBoard telah kembali menjadi Baru yeaaay !



Oke mas dan mba broo karena sudah berhasil saatnya saya untuk bilang *sempoaal* , Oh ya ada tambahan lagi nih , hati hati ketika memilih device yang akan diinstall , jangan sampe salah klik malah menginstall di partisi harddisk Laptop/PC anda.

Oke sekian dulu

Wassalam !

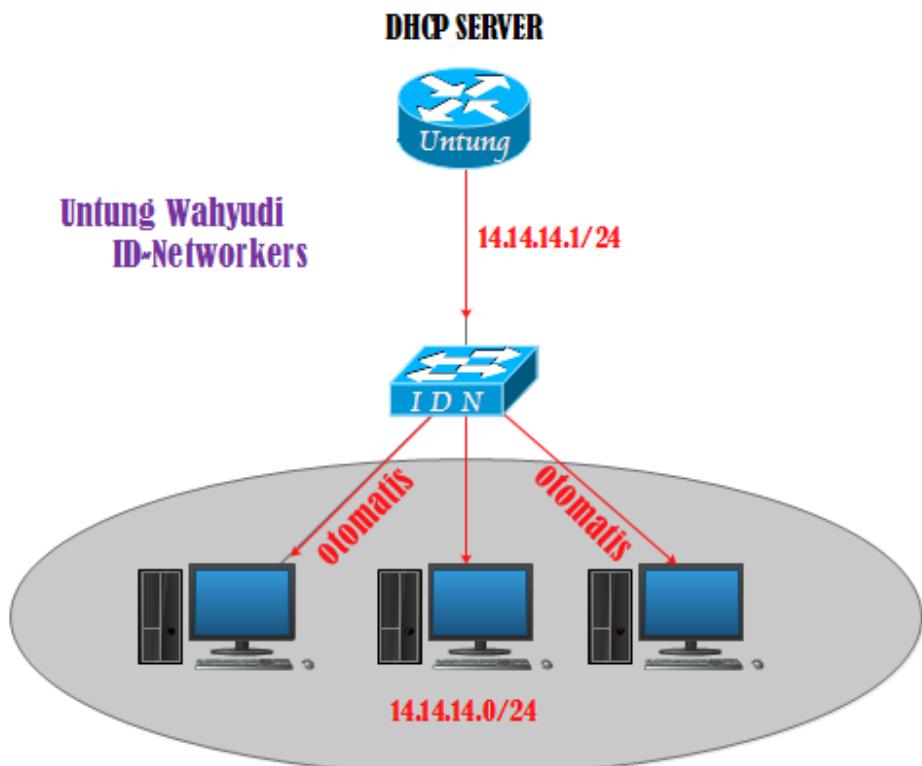
MANAJEMEN NETWORK

LAB 18. DHCP Server

Assalamualaikum wr.wb

Masih lanjut lagi dengan lab lab yang menarik buat di pelajari , di lab ini saya mau ngebahas sedikit tentang management Network , setelah di lab sebelumnya saya sudah kasih tau cara ngasih IP static untuk client, di lab kali ini saya mau ngasih tau cara Menjadikan Router sebagai DHCP Server. Oh ya sebelum ke sana saya ingin memberi pengetahuan sedikit tentang DHCP , jadi DHCP itu sebuah protocol yang digunakan untuk memberikan IP secara otomatis. Nah karena disini pembahasannya tentang DHCP Server berarti Router kita nantinya akan memberikan IP secara otomatis kepada client, jadi client gak perlu ngubah IP secara static/manual.

Oke dari pada ribet langsung aja ke konfigurasinya mas broo. Kurang lebih topologi yang bakal dibuat itu seperti ini , monggo disimak yoo.

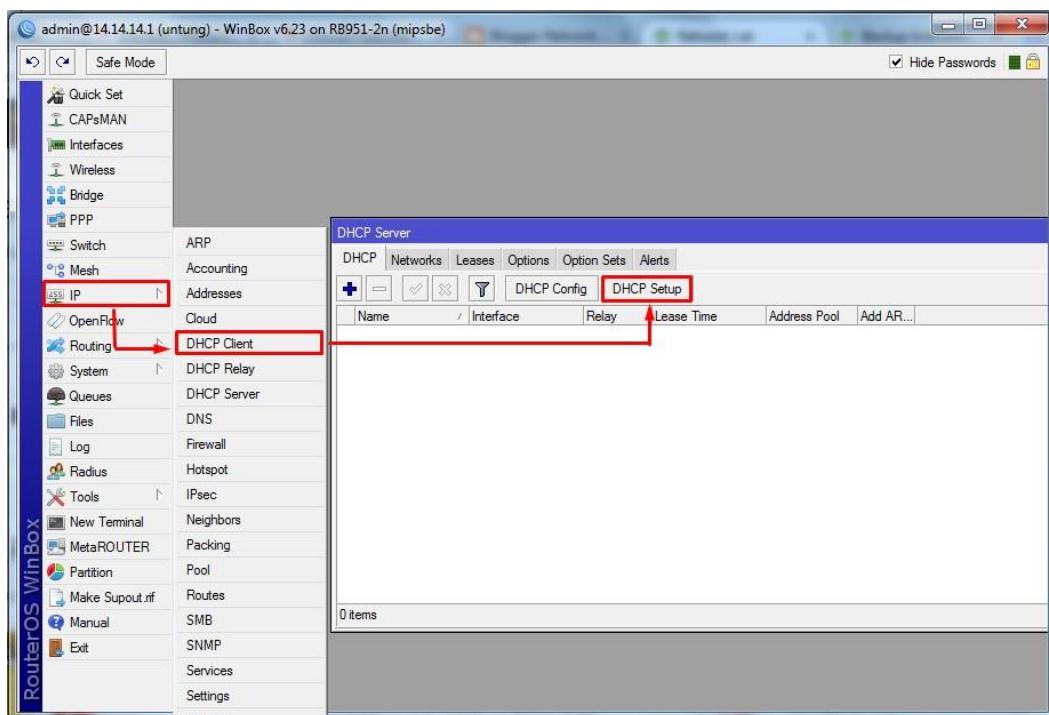


Oke setelah menyimak topologi diatas , saya harap kalian udah paham tentang konsep DHCP ini. Jadi sekarang tinggal ke konfigurasinya aja deh.

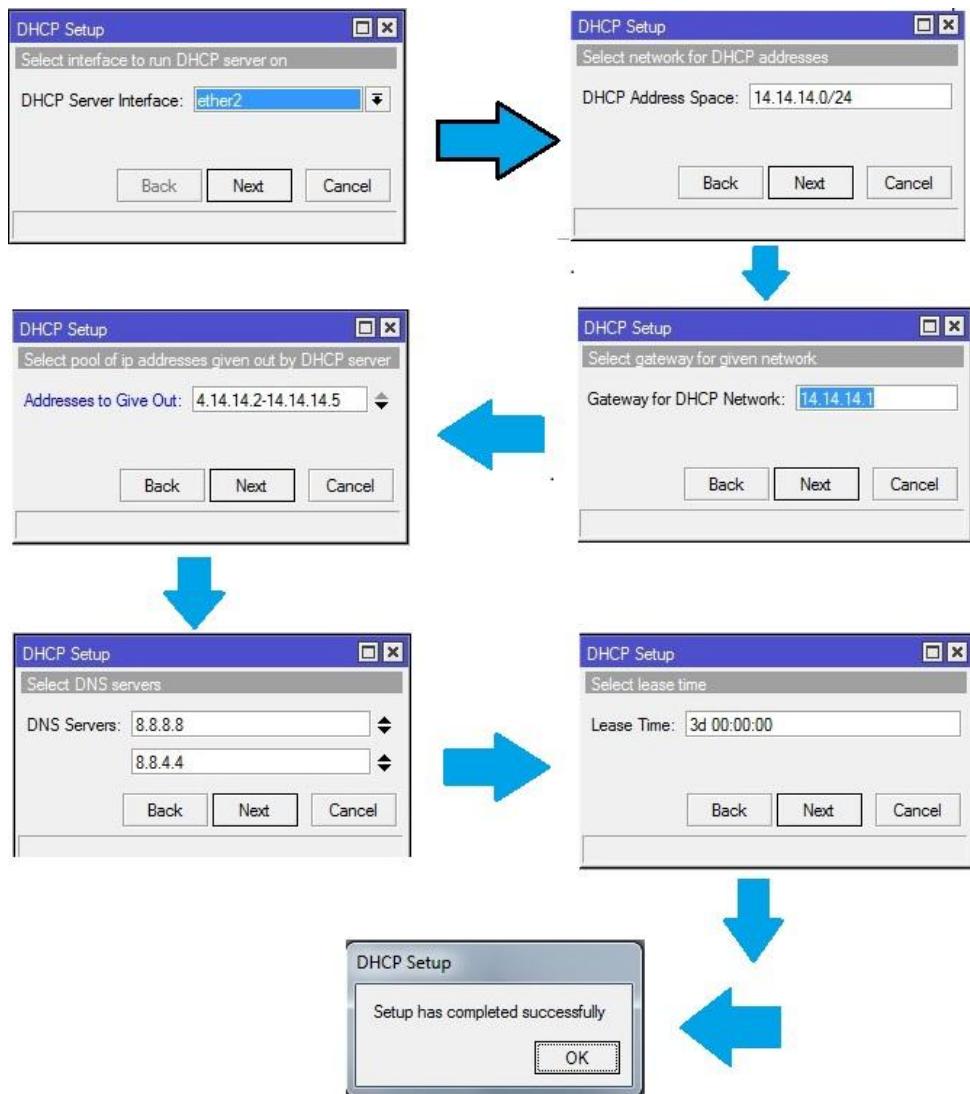
Langkah Konfigurasi :

Sebelumnya pastikan dulu kalian sudah mengatur IP di interface yang akan diberikan ip DHCP , di sini saya bakal ngatur di Interface ether2 dengan IP 14.14.14.1 , setelah diatur IP nya sekarang saatnya masuk ke tahapan pembuatan DHCP Server.

Untuk mengkonfigurasi DHCP Server caranya cukup mudah , pertama klik menu **IP > DHCP Server > DHCP Setup**.



Kemudian tinggal ikuti prosedur selanjutnya , saya buat singkat menjadi satu gambar seperti dibawah ini

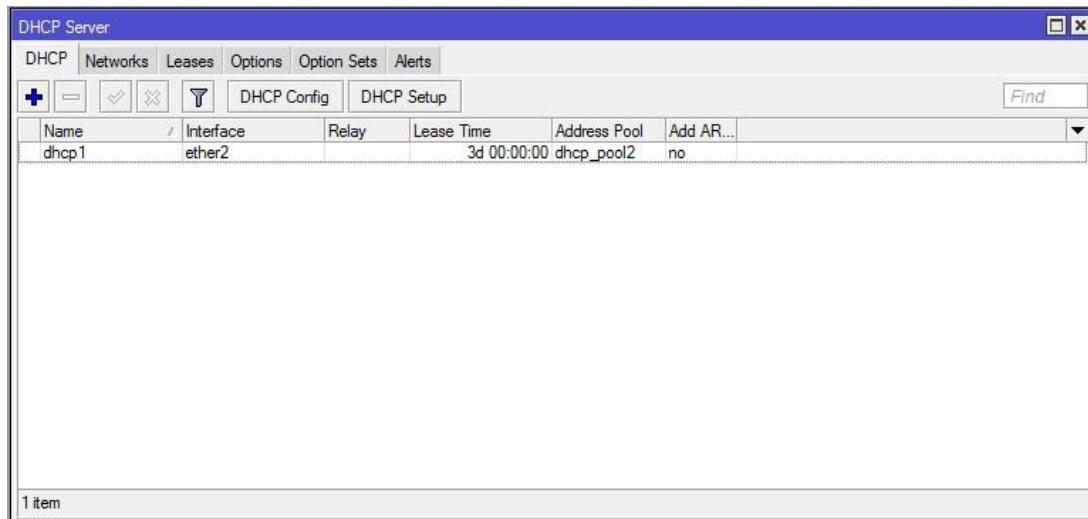


Keterangan :

1. Yang pertama adalah kita mengatur Interface mana yang akan diberikan IP DHCP
2. Pemilihan IP Network dari DHCP tersebut
3. Gateway dari IP yang nantinya diberikan ke client
4. Jumlah IP yang diberikan ke client.

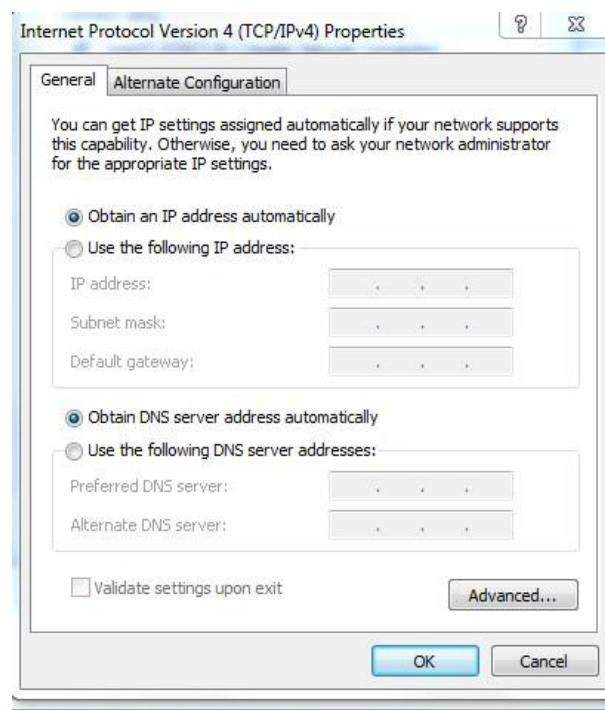
5. DNS yang akan dipakai oleh client
6. Lease time adalah lamanya IP tersebut diberikan ke client. Jika batas waktu itu habis maka client akan diberikan IP DHCP yang baru.

Jika sudah berhasil maka tampilan di Menu DHCP Server adalah sebagai berikut

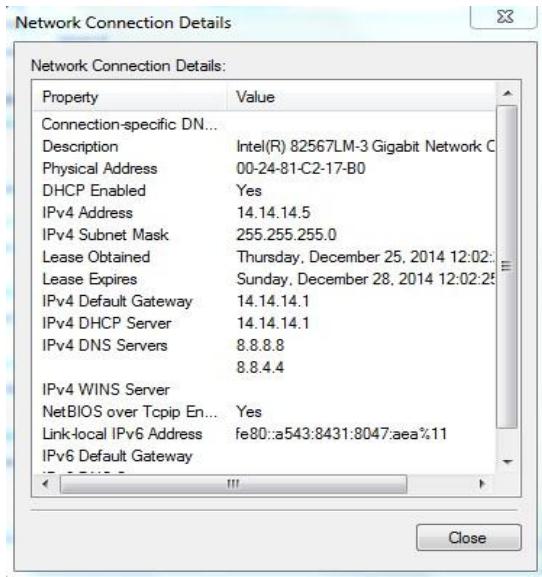


Pengujian di Client :

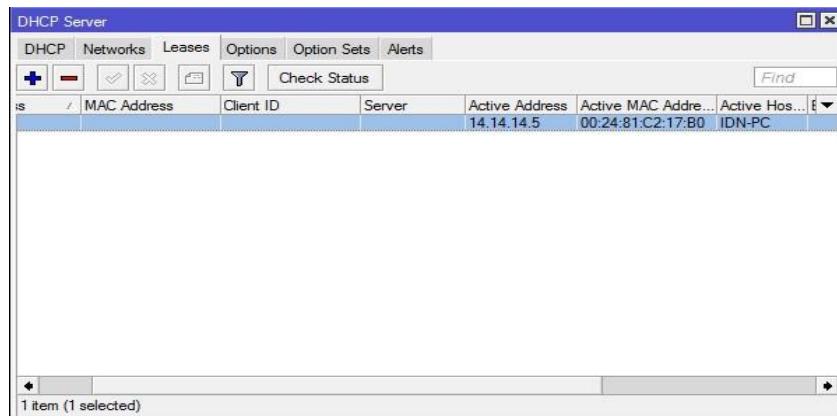
Selanjutnya kita coba test di client . kita atur IP di Client menjadi Automatic atau otomatis.



Kemudian silahkan di cek apakah client sudah dapat IP DHCP Dari router Mikrotik atau belum. Jika sudah dapat tandanya kita sudah berhasil membuat DHCP Server.



Kita juga bisa mengecek client mana saja yang telah menggunakan IP DHCP , klik menu **IP > DHCP Server > Leases**



Oke karena sudah berhasil maka saya sudahi dulu lab kali ini , saya tutup dengan mengucap , Alhamdulillah .

Oke sekian dulu

Wassalam !

LAB 19. Pengelolaan DHCP Server

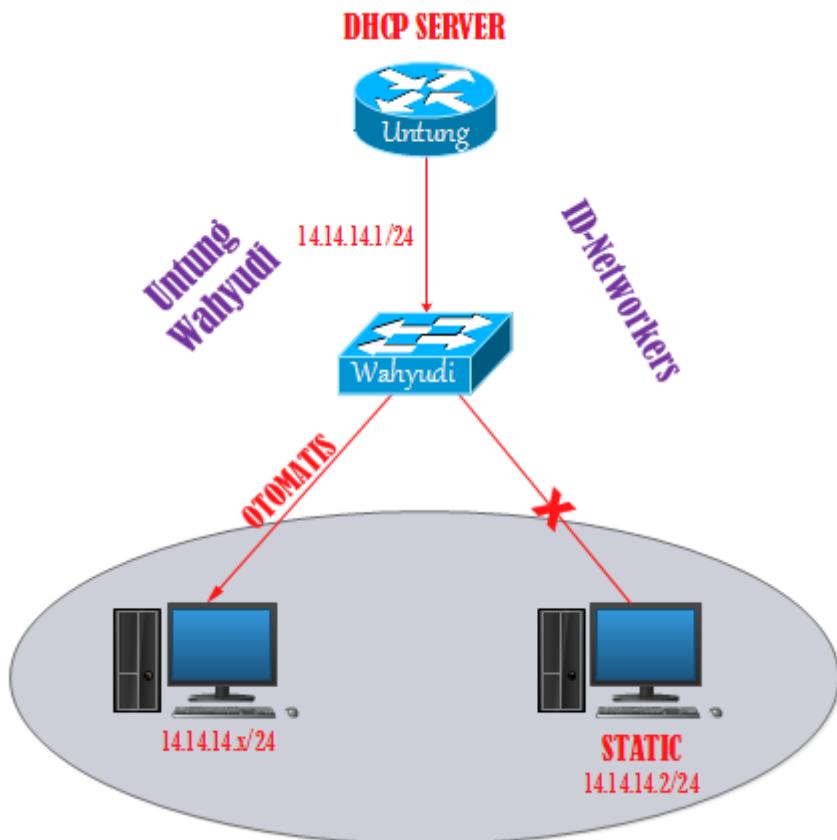
(Membuat client tidak bisa merubah IP menjadi Static)

Assalamualaikum wr.wb

Melanjutkan pembahasan di lab sebelumnya tentang DHCP Server, dilab ini saya mau ngebahas tentang pengelolaannya , salah satu diantara pengelolaan tersebut adalah membuat client tidak bisa mengubah IP menjadi Static. Terkadang walaupun kita sudah memberikan IP secara DHCP ke client tapi ada aja client yang *bandel* dan merubah IP nya menjadi static , ini membuat kita jadi susah monitoring. Maka dari itu kita harus membuat kemanan didalam DHCP Server.

Untuk membuat Client tidak bisa memakai IP secara static kita bisa menggunakan fitur ARP yang sudah dibahas sebelumnya , namun agak sedikit berbeda disini , kita menggunakan fitur ARP=reply-only , jadi dia hanya akan memberikan layanan terhadap IP DHCP.

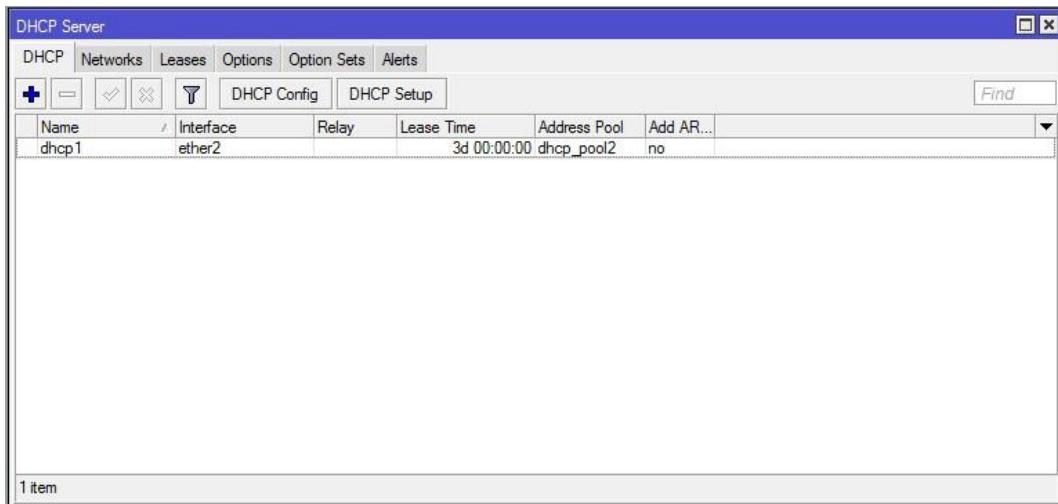
Dari pada pusing mending langsung aja ke konfigurasinya , kurang lebih topologinya begini gan



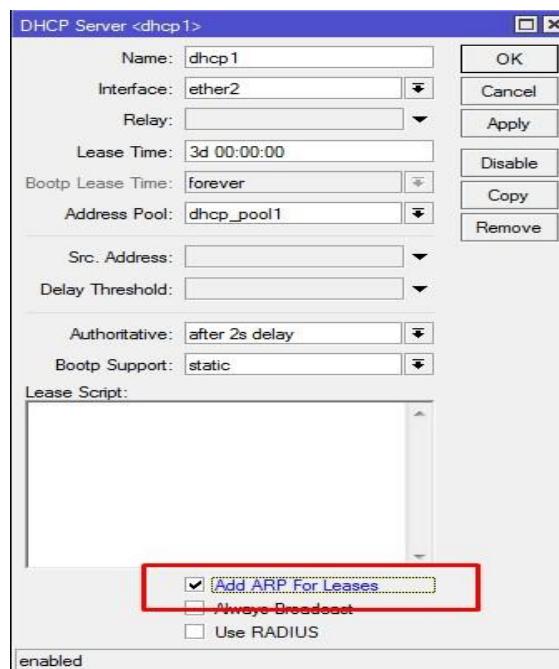
Silahkan disimak gambar tersebut , penjelasannya gini , jika ada client yang mencoba merubah IP Static maka hasilnya tidak akan diterima oleh router , dan si router akan menganggap bahwa client tersebut bukan di jaringannya.

Langkah konfigurasi :

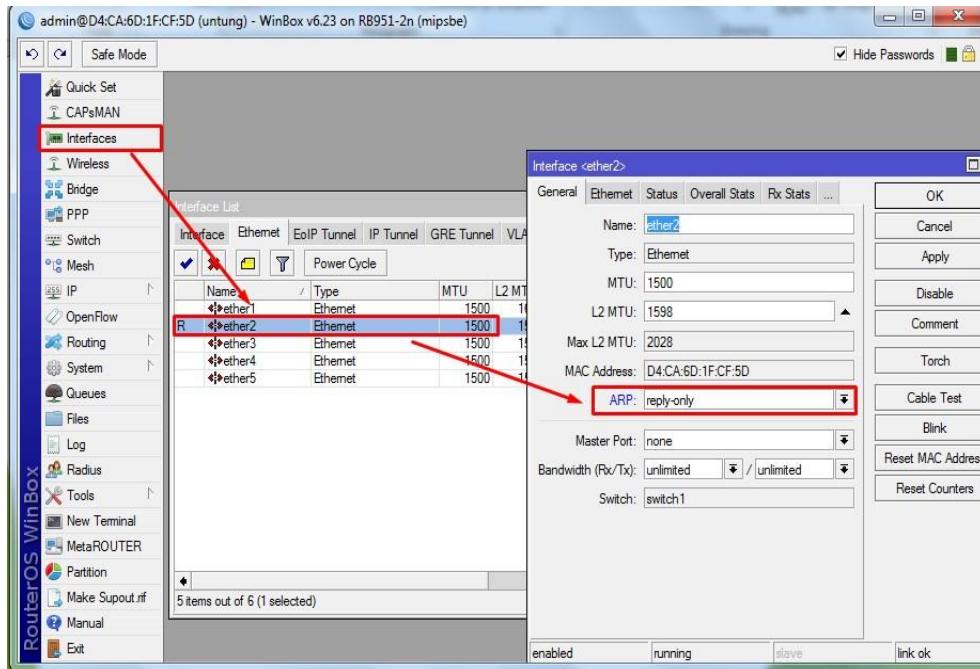
Pertama pastikan kalian sudah buat konfigurasi DHCP server seperti di lab sebelumnya



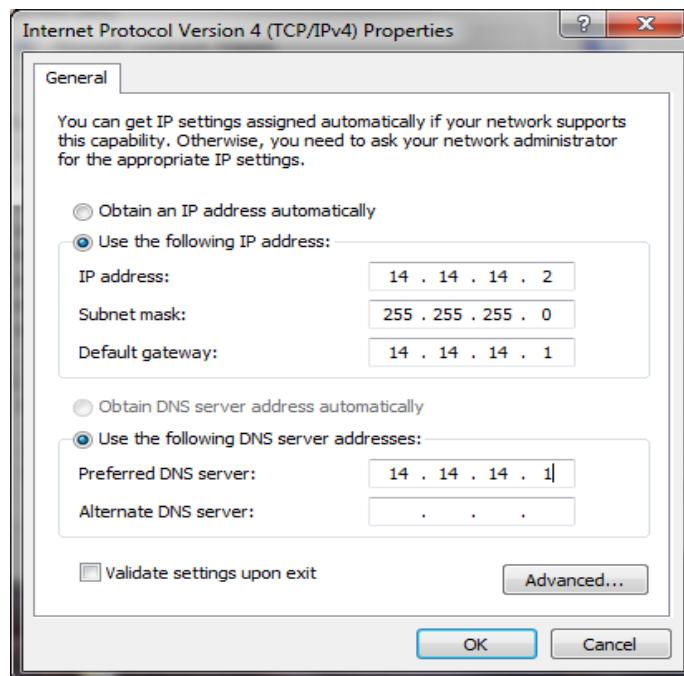
Kemudian double klik dihasil DHCP tersebut. Lalu dibagian paling bawah klik bagian "**Add ARP for Leases**".

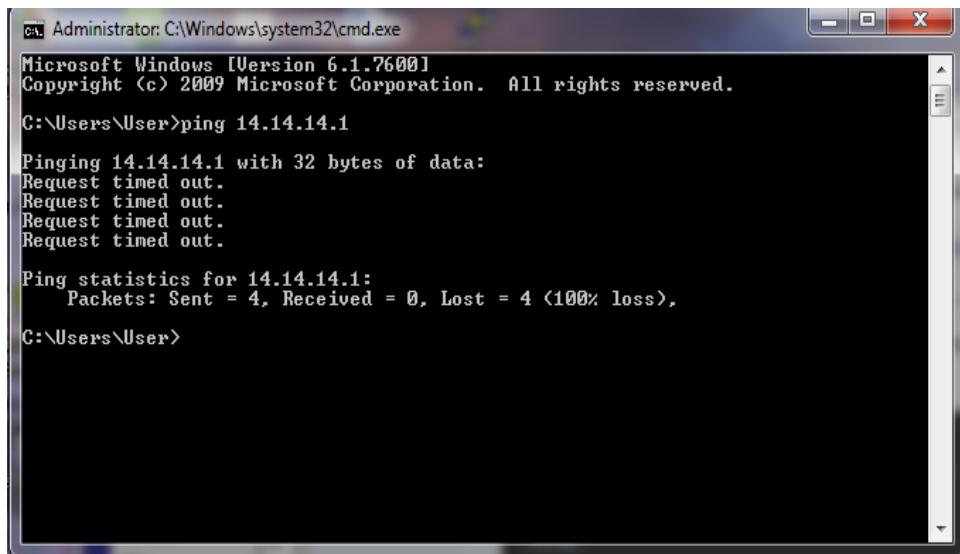


Setelah itu kita ke menu Interface untuk membuat nya menjadi ARP=Reply only. Caranya kita klik menu **Interface** > Pilih Interface yang diberikan IP DHCP > **ARP=Reply-Only**



Kemudian silahkan coba ganti IP di client menjadi static, contoh disini menjadi 14.14.14.2 , maka hasil nya client tersebut tidak bisa terhubung ke Router.





```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 14.14.14.1

Pinging 14.14.14.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 14.14.14.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\User>
```

Oke karena sudah berhasil jadi sekian dulu lab kali ini

Kurang lebih nya mohon maaf

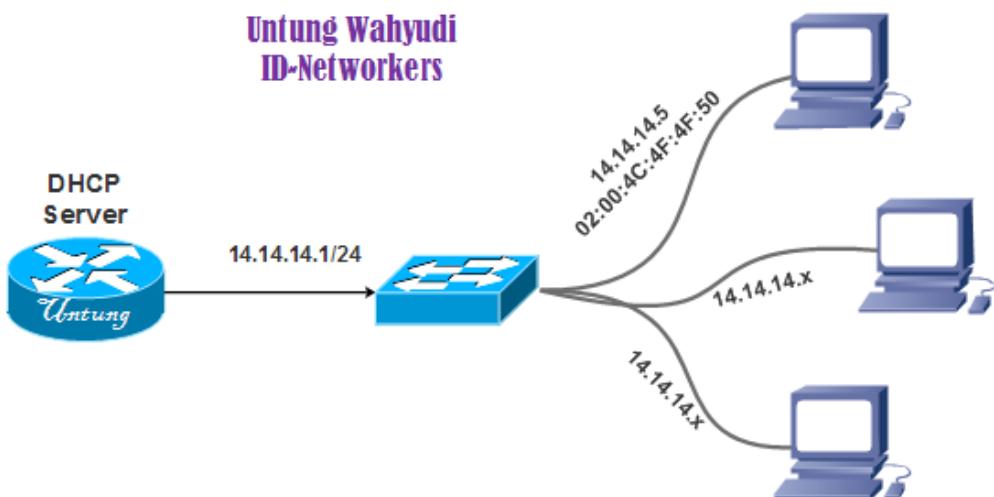
Wassalamualaikum

LAB 20. Pengelolaan DHCP Server

(Memberikan IP Khusus ke Client)

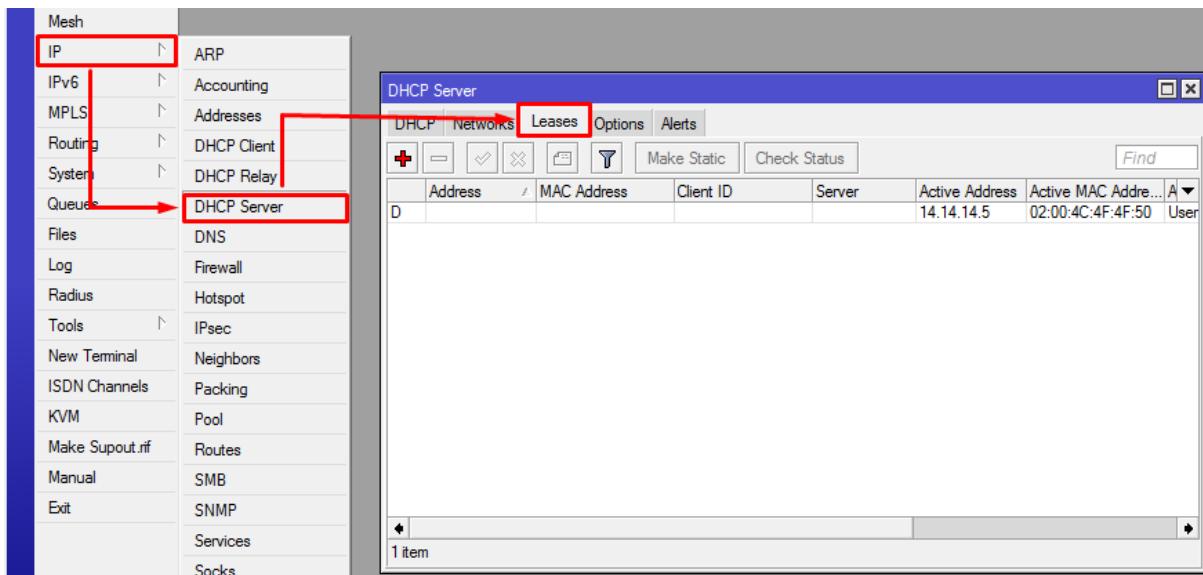
Assalamualaikum wr.wb

Masih mengenai pengelolaan DHCP Server , kalo dibaca dari judul mungkin agak bingung yaa . Saya jelaskan dari awal deh , jadi di DHCP Server kan ada yang namanya lease time , jadi itu menentukan berapa lama sebuah IP diberikan ke Client , setelah lease time itu habis maka client akan diberikan IP yang lagi yang baru dan berbeda tentu nya. Nah di pengelolaan ini saya mau bikin kondisi dimana client bakal dapat IP yang sama secara terus menerus.

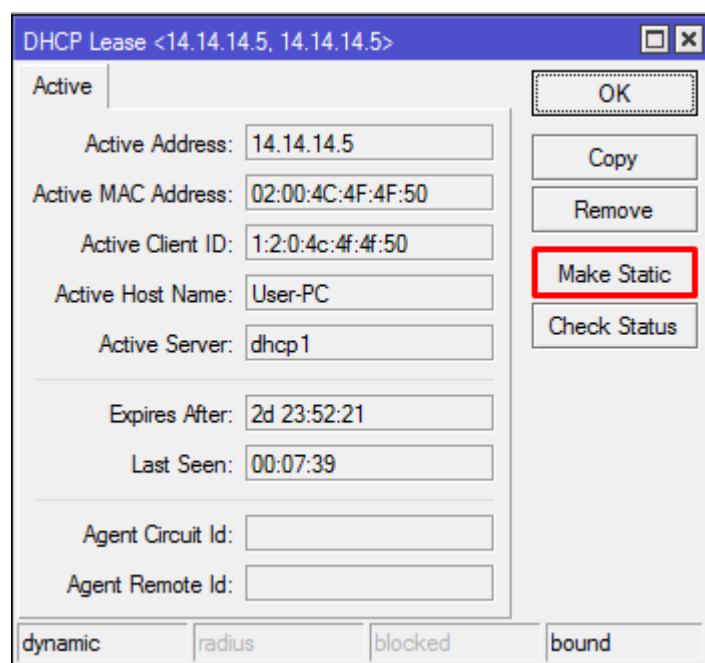


Oke langsung aja kekonfigurasinya

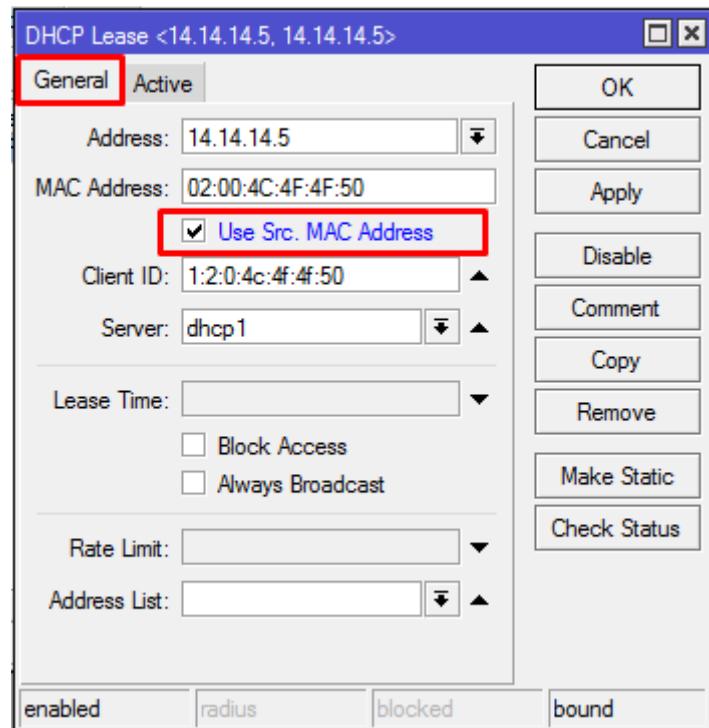
Pertama , klik menu **IP > DHCP Server > Leases** , disana akan terlihat user yang menerima layanan DHCP Server



Kemudian double klik , di bagian List nya. Setelah itu klik dibagian menu **Make Static** , lalu **OK**



Setelah itu buka kembali list yang tadi maka akan muncul menu tambahan yaitu **General** , klik menu General tersebut lalu masukan IP untuk client tersebut setelah itu klik bagian “**Use Src.Mac Address**” ,



Setelah itu apply dan OK , maka inilah hasilnya dibagian MAC Address dan Client ID akan terdaftar Mac Address dan Client ID dari PC tersebut.

DHCP Server						
DHCP		Networks		Leases		Options
<input style="width: 20px; height: 20px; border: none;" type="button" value="+"/>		<input style="width: 20px; height: 20px; border: none;" type="button" value="X"/>		<input style="width: 20px; height: 20px; border: none;" type="button" value="Check"/>		<input type="button" value="Find"/>
Address	/	MAC Address	Client ID	Server	Active Address	Active MAC Addre... A
14.14.14.5		02:00:4C:4F:4F:50	1:2:0:4c:4f:4f:50	dhcp1	14.14.14.5	02:00:4C:4F:4F:50 User

Dengan rule diatas maka PC tersebut akan terus mendapatkan IP **14.14.14.5** sebagai IP DHCP nya.

Oke karena sudah berhasil maka saya tutup lab kali ini dengan mengucap Alhamdulillah

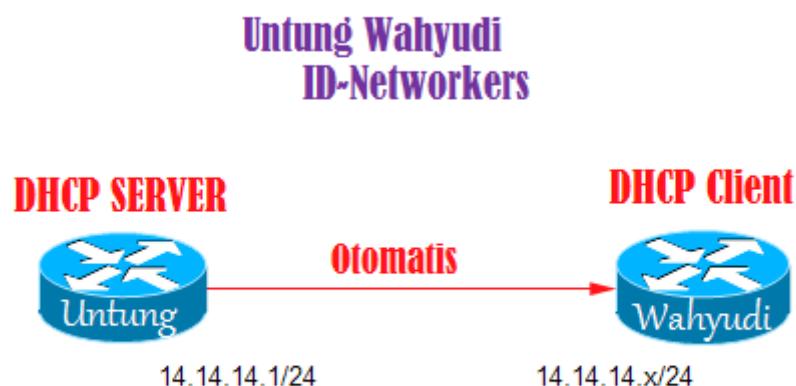
Wassalam !

LAB 21. DHCP Client

Assalamualaikum wr.wb

Masih lanjut lagi di lab DHCP , kalo di lab sebelumnya Router Mikrotik kita dijadikan sebagai DHCP Server , maka dilab ini saya mau bikin Router nya menjadi DHCP Client. Kalo server yang memberikan layanan DHCP , berarti kalo client yang menerima IP DHCP nya.

Nih saya kasih lagi topologinya

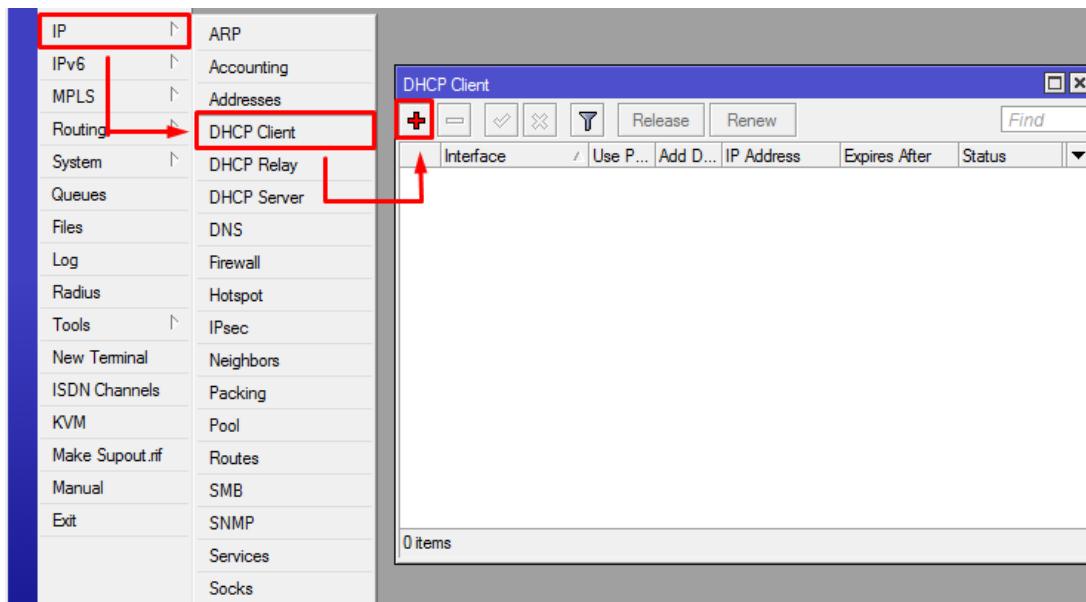


Sebelum mengatur DHCP Client , ada beberapa hal yang harus diperhatikan , yang pertama adalah

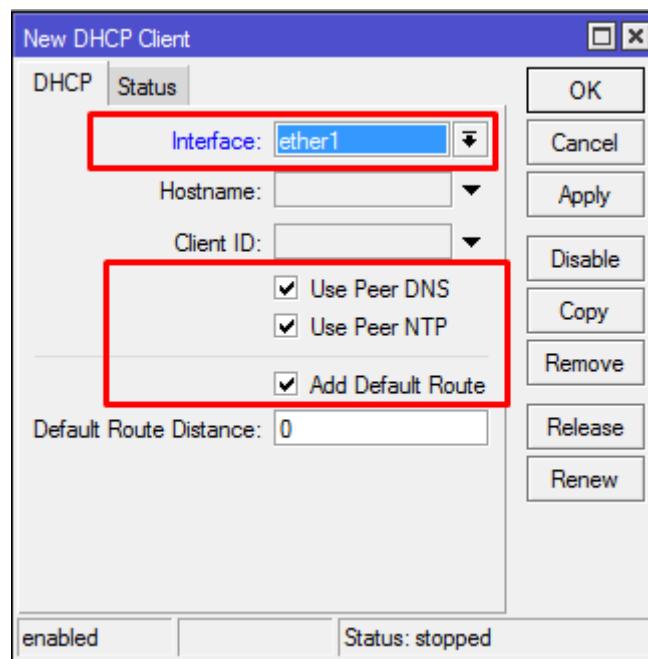
- Harus adanya DHCP Server atau penyedia layanan DHCP nya ,
- Lalu pastikan kita terhubung dengan DHCP Server tersebut. Entah itu kita terhubung lewat kabel ataupun wireless , intinya kita harus terhubung dengan Penyedia tersebut.

Oke kalo sudah paham langsung aja ke konfigurasinya

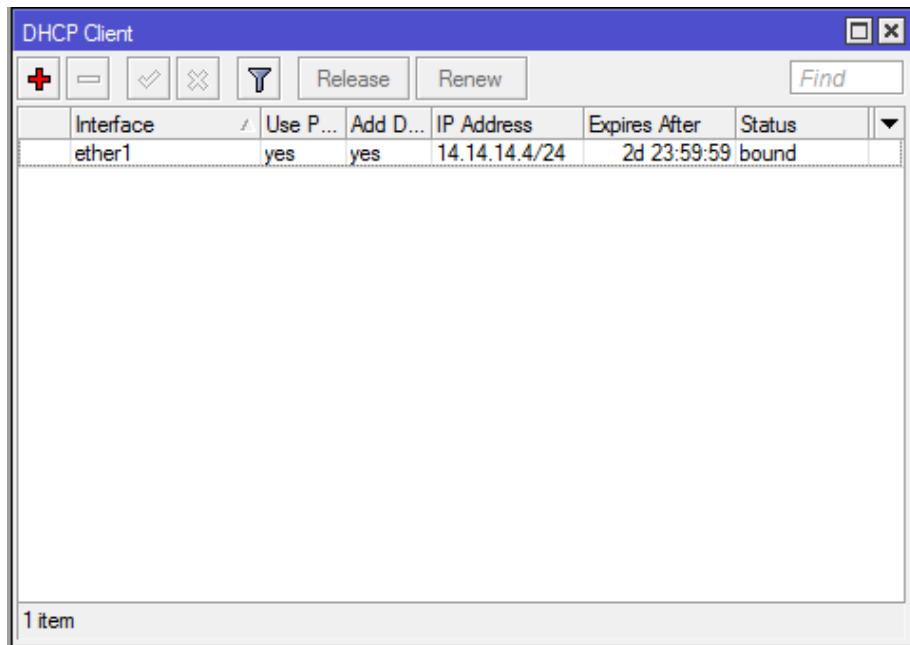
Pertama klik menu **IP > DHCP Client > Add**



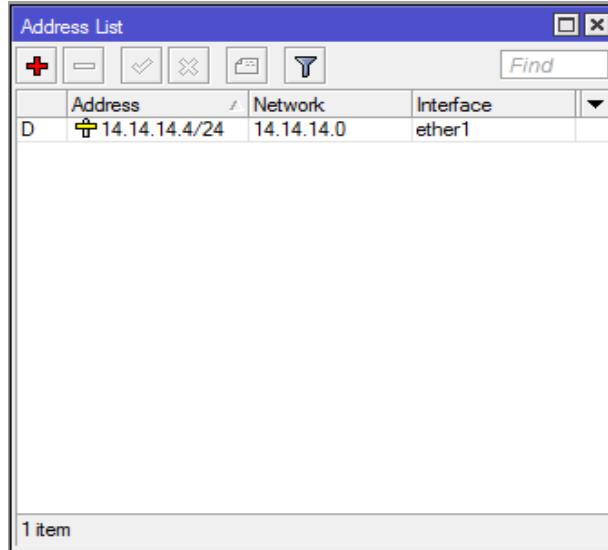
Kemudian kita pilih interface yang akan dijadikan sebagai DHCP Client , disana ada kata kata **“Use Peer DNS dan NTP”** itu artinya kita mengikuti aturan DNS dan NTP dari DHCP Server tersebut.



Jika sudah maka hasilnya akan terlihat seperti gambar berikut , dibagian kanan ada kata “**Bound**” , yang artinya berhasil 😊.



Kemudian bisa dicek IP yang didapat dengan melihat IP address nya , lalu coba lakukan ping ke DHCP severnya. Jika ada reply artinya berhasil



```
[admin@wahyudi] > ping 14.14.14.1
HOST                               SIZE TTL TIME STATUS
14.14.14.1                         56  64 13ms
14.14.14.1                         56  64 3ms
14.14.14.1                         56  64 2ms
14.14.14.1                         56  64 2ms
14.14.14.1                         56  64 1ms
sent=5 received=5 packet-loss=0% min-rtt=1ms avg-rtt=4ms max-rtt=13ms

[admin@wahyudi] >
```

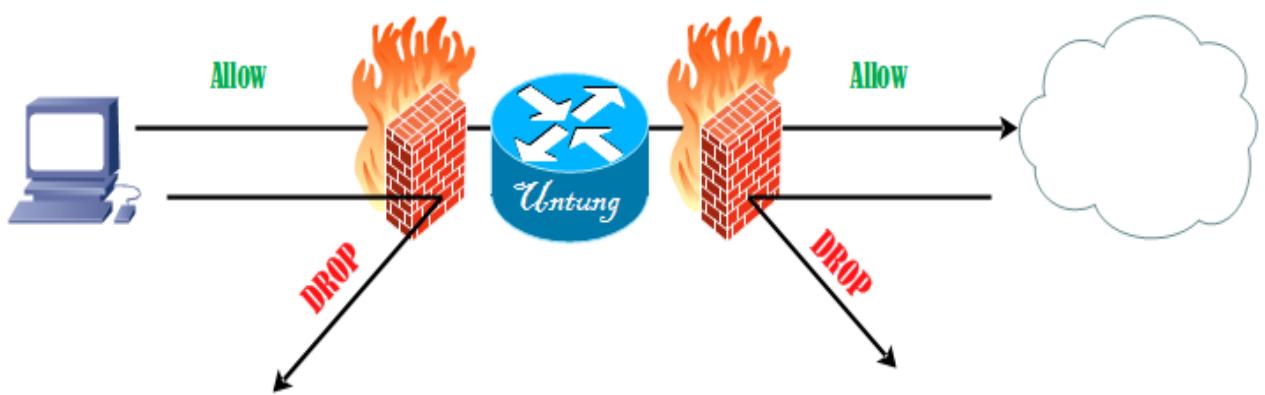
Oke karena sudah reply itu artinya berhasil , sekian dulu pembahasan di lab ini , kurang lebihnya mohon maaf

Wassalamualaikum !

FIREWALL

Firewall merupakan sebuah sistem keamanan yang berfungsi untuk memeriksa paket yang keluar ataupun masuk. Dengan adanya firewall kita bisa melindungi jaringan kita terhadap serangan dari luar maupun dari jaringan lokal kita sendiri. Nah untuk di Mikrotik sendiri kita bisa membuat Router Mikrotik sebagai firewall yang melindungi jaringan lokal dari serangan yang berasal dari luar (internet). Karena nantinya Router Mikrotik akan memilih mana paket yang boleh masuk atau keluar dan mana paket yang akan dibuang. Ada beberapa jenis firewall yang ada di Mikrotik , yang beberapa akan saya bahas di Lab lab berikutnya.

Untung Wahyudi
ID-Networkers



A. Firewall NAT

NAT atau Network Address Translation adalah sebuah firewall yang berfungsi untuk merubah IP address pengirim seolah olah menjadi IP address dari Router. NAT ini biasanya digunakan disaat Router berada diantara 2 jaringan yang berbeda. Di Lab sebelumnya tentang koneksi internet saya udah sempet ngabahas tentang NAT , dan jika dilihat dari topologi sebelumnya Router Mikrotik berada diantara 2 jaringan yang berbeda , yaitu **Jaringan Lokal atau LAN dengan Jaringan Internet**. Di lab 10 tersebut saya membuat sebuah rule firewall yang berfungsi untuk menyembunyikan (masquerade) IP jaringan lokal yang akan menuju Internet melalui **ether1**. Firewall NAT ini dibagi menjadi 2 Yaitu Srcnat dan Dstnat. Namun di Bab ini saya bakal lebih ngebahas tentang **srcnat**.

Untuk mengingatkan kembali , di Lab 10 saya buat rule dengan perintah

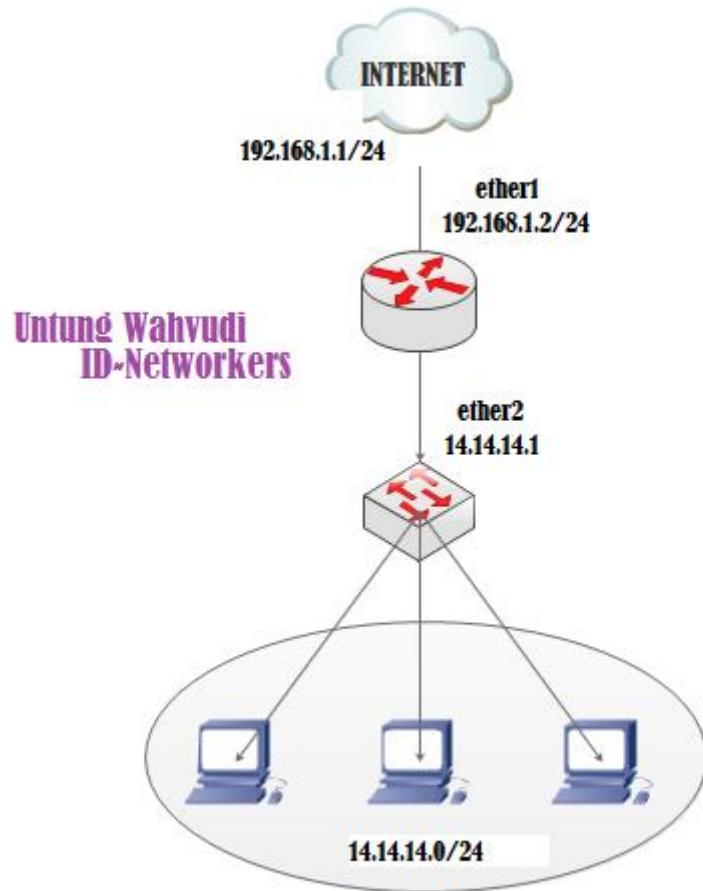
```
[admin@untung> ip firewall nat add chain=srcnat out-interface=ether1  
action=masquerade
```

Yang artinya kurang lebih begini :

*"Jika ada paket yang lewat berasal dari **Source (sumber)** dan ingin keluar melalui **ether1** maka akan di samarkan*

LAB 22. Firewall NAT (Masquerade IP Address Tertentu)

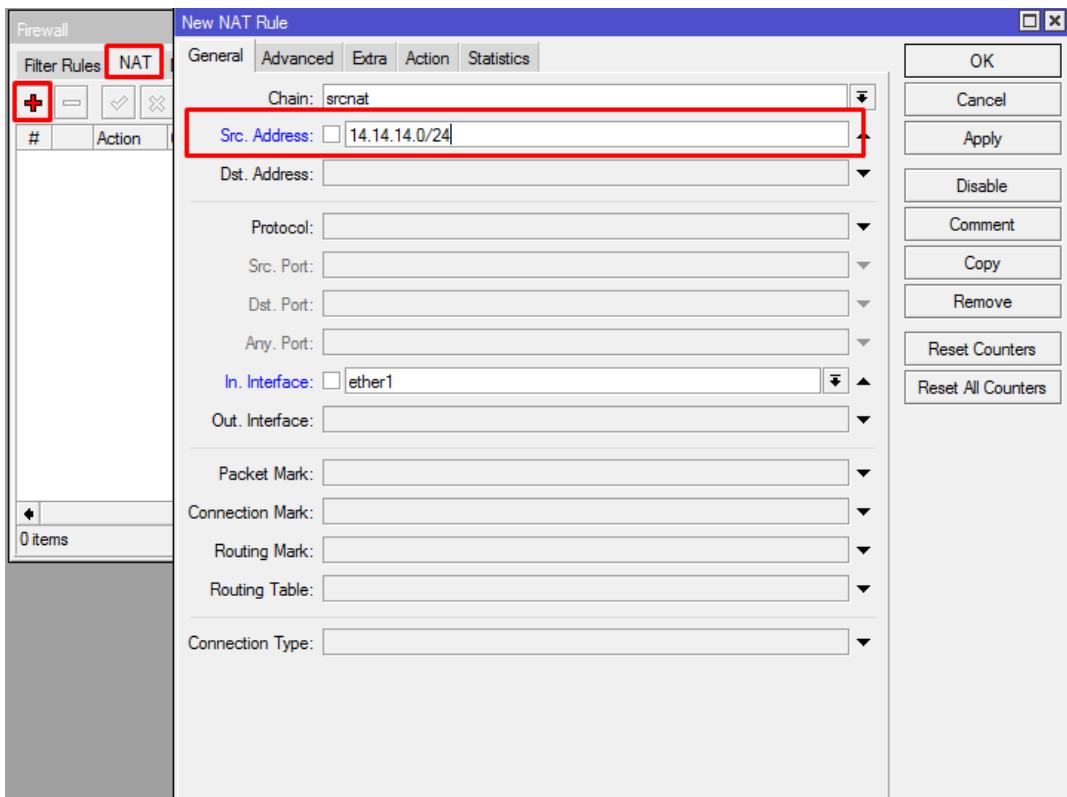
Perintah masquerade sebelumnya tidak mencantumkan IP address lokal yang berhak untuk mengakses internet. Jadi agak susah untuk membatasi komputer mana saja yang bisa terkoneksi ke internet. Untuk menyegarkan kembali ingatan kita , saya kasih topologi nya lagi di Lab sebelumnya.



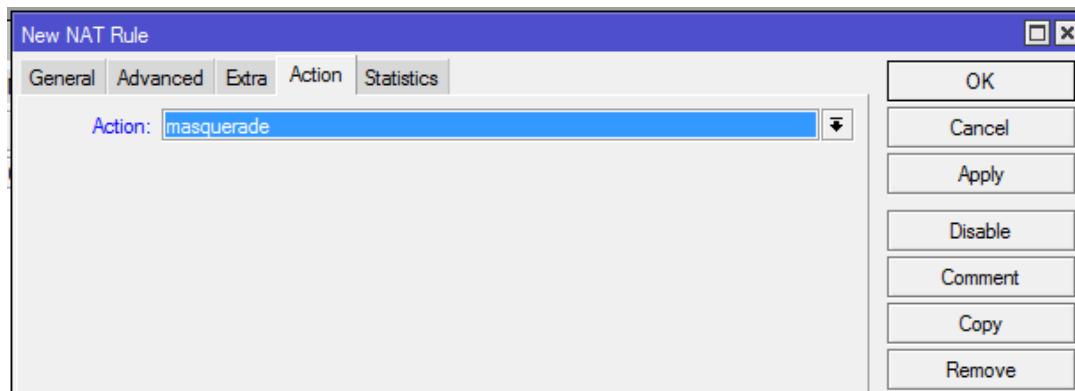
Berikut ini adalah perintah konfigurasi masquerade dengan menggunakan perintah **src-address** didalamnya

```
[admin@untung> ip firewall nat add chain=srcnat src-address=14.14.14.0/24 out-interface=ether1 action=masquerade
```

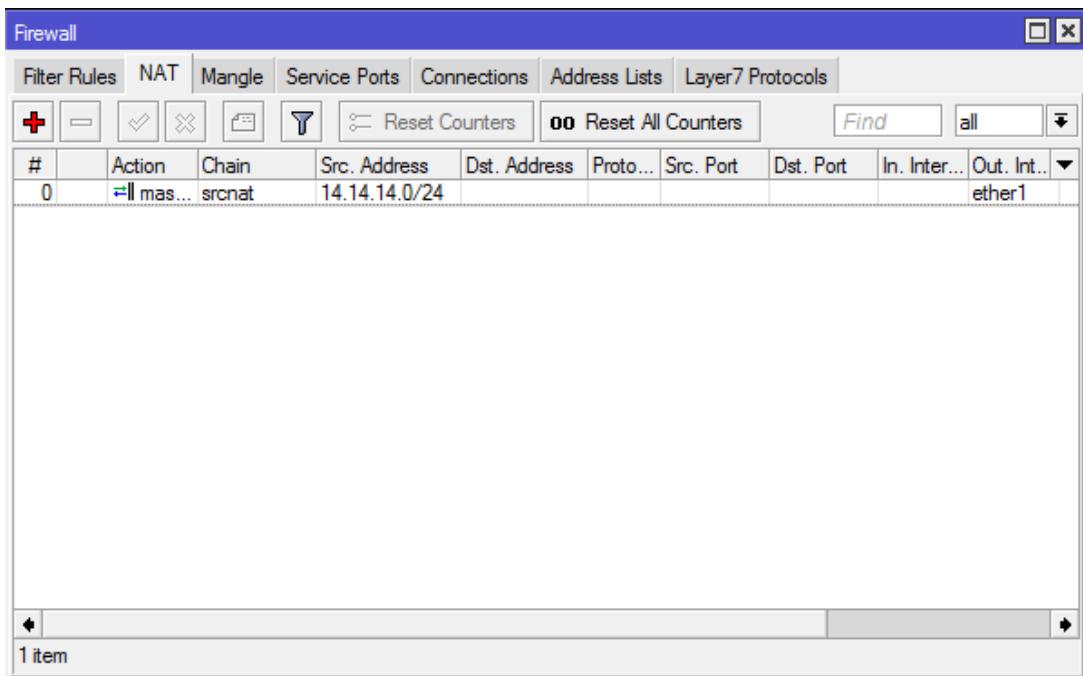
Untuk cara GUI nya bisa klik menu **IP > Firewall > NAT > +** , kemudian isikan seperti gambar dibawah ini



Jangan lupa action nya mas bro , **action = masquerade**.



Beginilah hasil akhir rule nya.



Jika kita menggunakan perintah diatas artinya kita hanya membolehkan IP address dengan network **14.14.14.0/24 (14.14.14.1 - 14.14.14.254)** yang bisa terkoneksi ke internet.

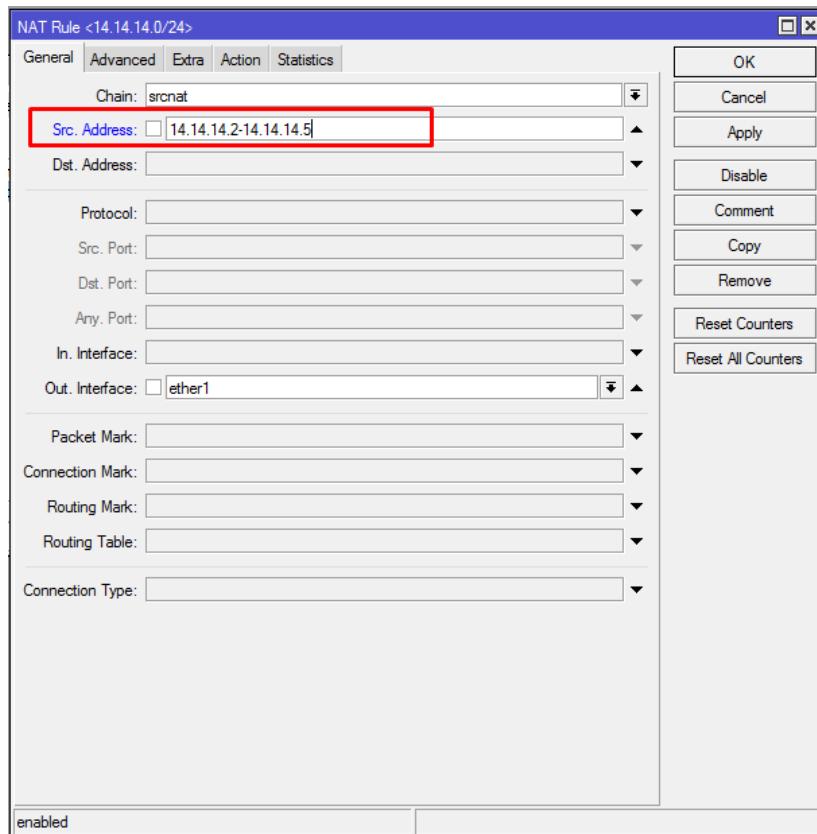
Terus gimana misalnya kita Cuma pengen 3 user aja yang bisa koneksi ke internet , yaitu user yang menggunakan IP 14.14.14.2 , 14.14.14.3 dan 14.14.14.4. Selain dari IP itu tidak bisa koneksi ke internet. Caranya mudah yaitu dengan menggunakan perintah **src-address (IP address asal)**. Dengan topologi yang sama seperti diatas kita buat hanya IP address 14.14.14.2 , 14.14.14.3 dan 14.14.14.4 aja yang bisa koneksi ke internet.

Yang pertama harus dilakukan adalah kita hapus dulu rule yang sebelumnya , **kenapa mesti dihapus ??** karena Router Mikrotik membaca rule dari atas kebawah , jika di rule pertama dia membolehkan IP dengan network 14.14.14.0/24 maka hasilnya IP 14.14.14.5 ~ 14.14.14.254 akan dapat terkoneksi ke internet. Bukannya kita pengen Cuma IP 14.14.14.2 - 14.14.14.4 aja yang koneksi internet ???

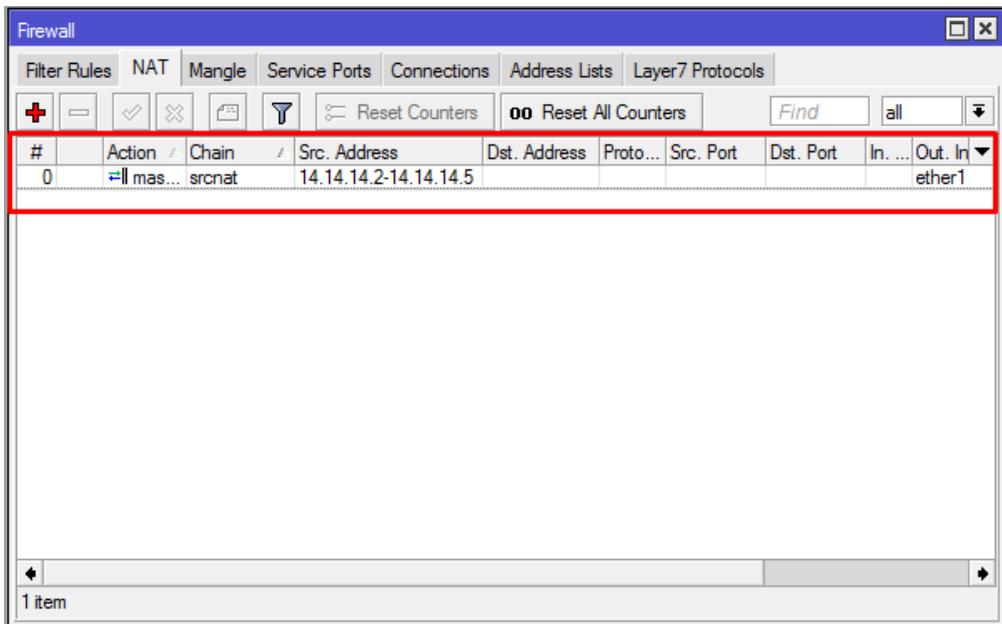
```
[admin@untung> ip firewall nat remove number=0
```

```
[admin@untung> ip firewall nat add chain=srcnat src-address=14.14.14.2-14.14.14.4  
out-interface=ether1 action=masquerade
```

Untuk GUI nya kita bisa langsung mengedit saja rule yang sebelumnya dengan cara **double klik** kemudian edit menjadi seperti dibawah ini



Kemudian bisa dilihat hanya ada **SATU** rule saja , artinya hanya ada rule yang membolehkan IP 14.14.14.2-14.14.14.5 saja yang bisa koneksi internet.



Dengan membuat rule seperti diatas maka hanya IP 14.14.14.2-14.14.14.5 saja yang bisa koneksi ke internet. Dengan begitu berhasil lah keinginan kita untuk membuat rule masquerade IP tertentu

Jika diterjemahkan kurang lebih artinya seperti dibawah ini

Jika ada paket yang berasal dari IP 14.14.14.2-14.14.14.5 ingin keluar melalui ether1 maka akan disamarkan (masquerade)

Oke dengan berakhirnya pembuatan rule diatas maka berakhir pula lab kita kali ini yang membahas masquerade IP tertentu. Kayaknya dibeberapa lab kedepan akan banyak ngebahas tentang Firewall , yaiyalaah namanya juga BAB firewall -_- .

Oke sekian dulu

Wassalam !

B. FIREWALL FILTER

Oke lanjut lagi masih di BAB Firewall , setelah di lab sebelumnya membahas tentang Firewall NAT , di lab selanjutnya bakal ngebahas tentang Firewall Filter. Apa sih firewall Filter itu ???

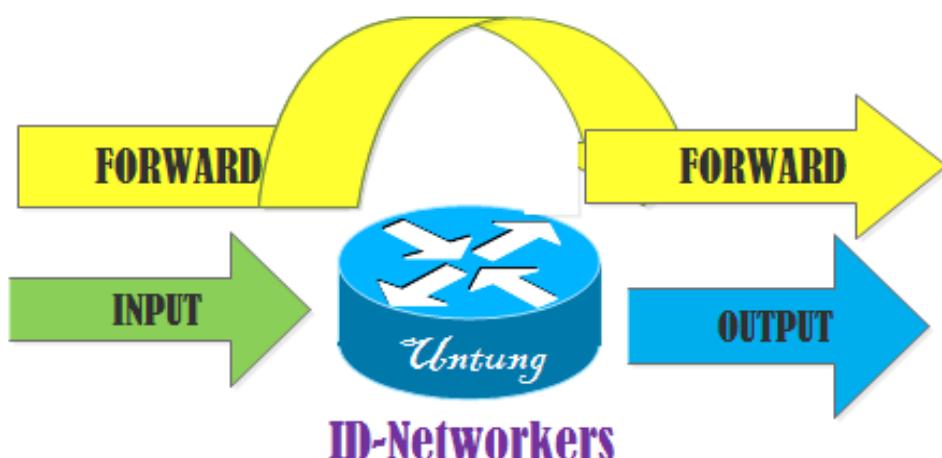
Firewall filter digunakan untuk membatasi suatu paket yang dapat masuk atau melewati sebuah sistem Router. Namanya juga filter artinya *disaring* . jadi setiap paket yang mau masuk atau keluar nantinya bakal disaring/dipilih oleh Router.

Ada 3 jenis atau chain di firewall filter , yaitu :

- **INPUT** = Menangani paket data yang **MASUK** kedalam Router
- **FORWARD** = Menangani paket data yang **MELINTASI** Router
- **OUTPUT** = Menangani paket data yang **KELUAR** dari Router.

Cuma di modul ini saya Cuma ngebahas chain INPUT dan FORWARD aja , untuk yang OUTPUT saya gak bahas , karena rada susah praktekinnya kalo di rumah dikarenakan kekurangan alat ☺.

Biar lebih paham mengenai Firewall Filter , monggo disimak gambar berikut



Firewall INPUT

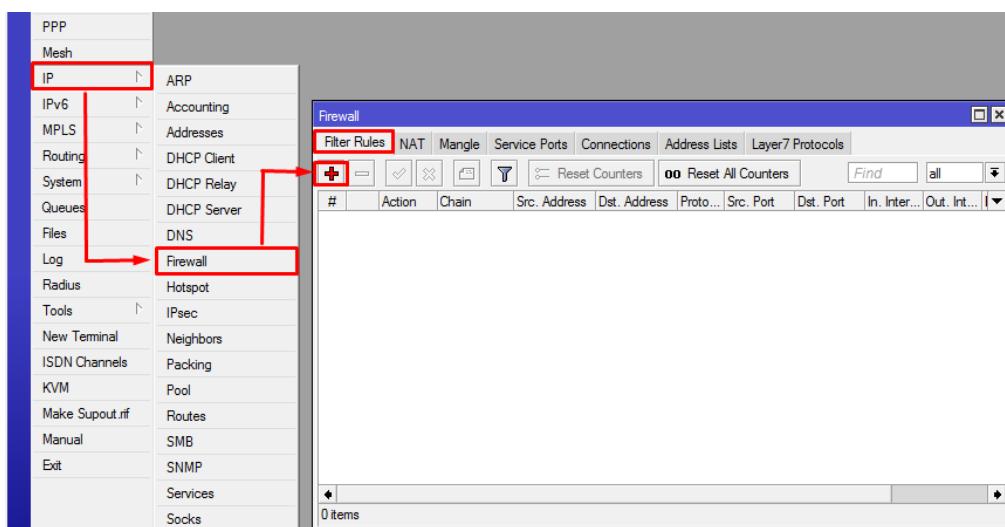
Yang pertama saya bahas di firewall filter adalah Firewall dengan Chain INPUT , Chain Input pada firewall ini menangani paket paket yang ditujukan atau diarahkan ke interface si Router. Chain ini berguna untuk memberikan perlindungan terhadap akses yang ditujukan untuk router , baik dari jaringan lokal atau pun dari internet , baik dari dalam ataupun dari luar. Jadi dengan chain ini router akan aman secara jasmani dan rohani 😊 lhooo ngaco.

LAB 23. Blok Akses dengan Firewall INPUT

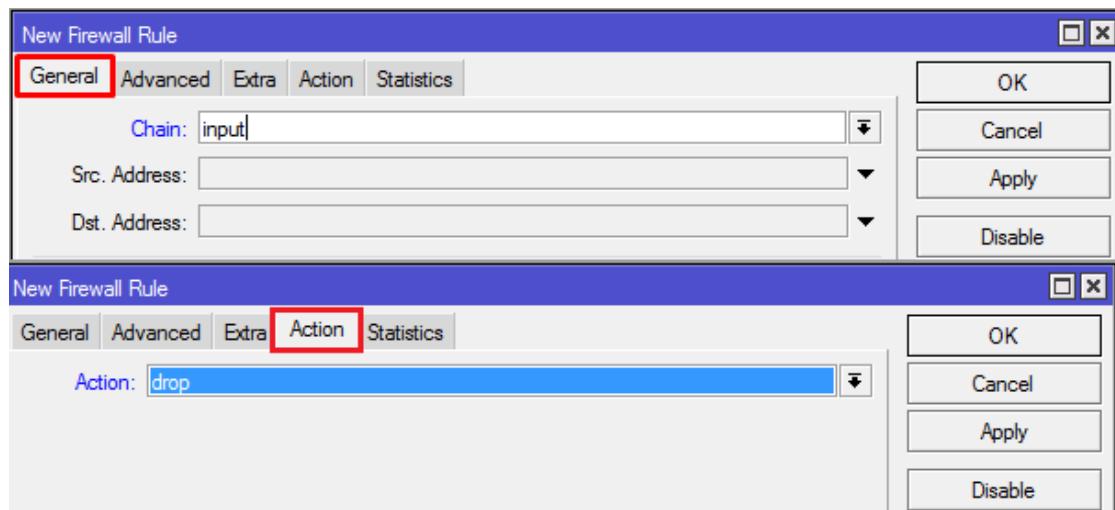
Assalamualaikum wr.wb

setelah paham tentang konsep firewall INPUT , kita akan membuat sedikit percobaan , yaitu kita akan coba memblok semua traffic yang akan masuk ke dalam router dengan menggunakan **chain input**. Jadi **SEMUA** traffic yang masuk akan **DI BLOK**. Caranya adalah sebagai berikut.

Klik menu IP > Firewall > Filter Rules > Add



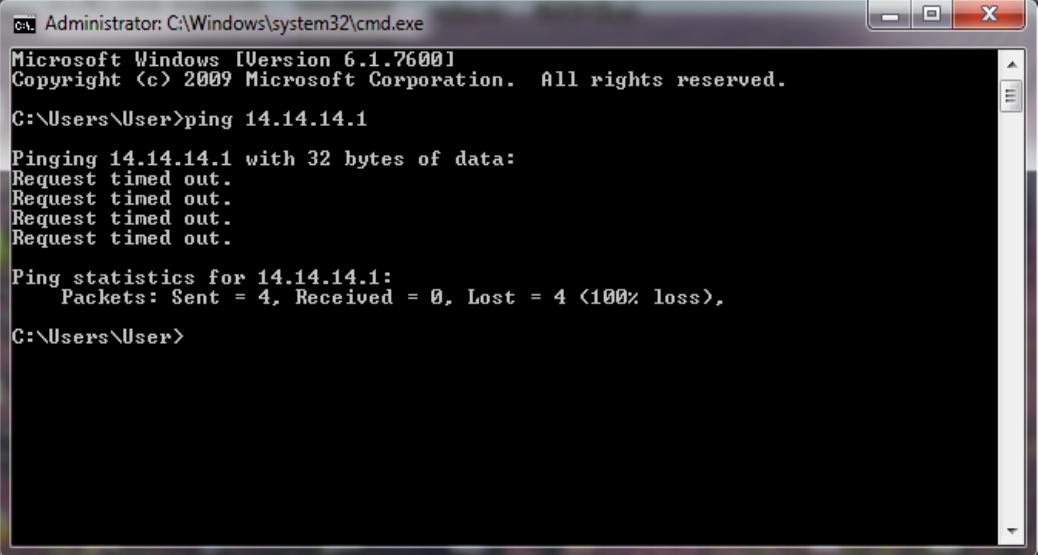
Kemudian kita buat rule untuk memblok semua Traffic Input , caranya pilih chain=input kemudian di tab Action pilih Drop !



Kemudian inilah hasil rule yang tdi kita buat.

Firewall										
Filter Rules		NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols			
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	
0	drop	input								
1 item										

Kemudian coba lakukan test ping dari client menuju Router.



```
c:\ Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 14.14.14.1

Pinging 14.14.14.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 14.14.14.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\User>
```

Dengan rule yang kita buat tadi , maka semua traffic yang menuju ke Router akan di blok , Kita tidak bisa melakukan ping termasuk kita **tidak bisa mengakses RouterBoard** kita , jadi cara diatas tidak terlalu efektif. Untuk menanganinya kita akan gunakan cara **drop any , accept few** atau sebaliknya di Lab selanjutnya

Oke sekian dulu ,

Wassalam !

Lab 24. Firewall Filter INPUT (Membatasi IP untuk mengakses Router)

Assalamualaikum wr.wb

Oke lanjut setelah penjelasan tentang Firewall INPUT saya harap kalian para pembaca udah paham pengertian dari firewall INPUT ini. Sedikit menambahkan lagi , di firewall ini nantinya akan ada taktik dalam pembuatannya.

Firewall Tactic :

- **Accept few , Drop any** (Terima beberapa , Buang semuanya) artinya , kita menerima beberapa paket yang dibutuhkan , kemudian membuang semua paket.
- **Drop few , Accept any** (Buang beberapa , Terima semuanya) artinya , kita membuang paket yang tidak dibutuhkan , kemudian menerima semua paket.

Oke dilab ini bakal dibahas mengenai taktik yang pertama saja , jadi untuk taktik yang kedua mungkin akan langsung paham bila sudah mempraktekan yang ini.

Accept Few , Drop Any (Terima beberapa , Buang Semuanya)

Kasusnya begini :

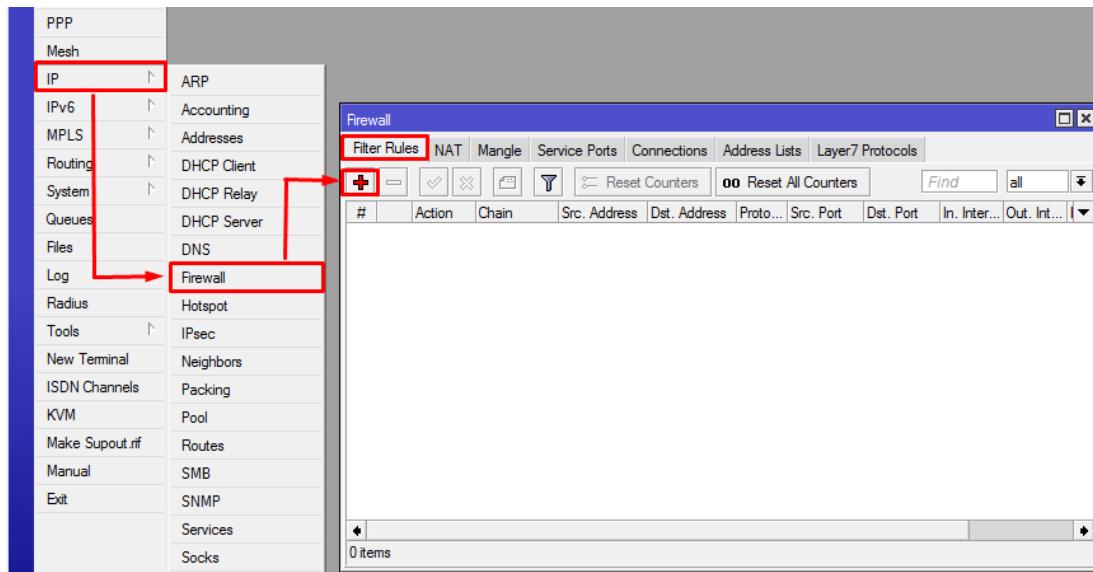
Kita pengen hanya IP dari Admin saja yang bisa mengakses si Router. Jadi **selain IP dari Administrator** akan kita **drop**. Disini IP yang digunakan Admin adalah 14.14.14.2

Udah dibaca baik baik kasusnya ???

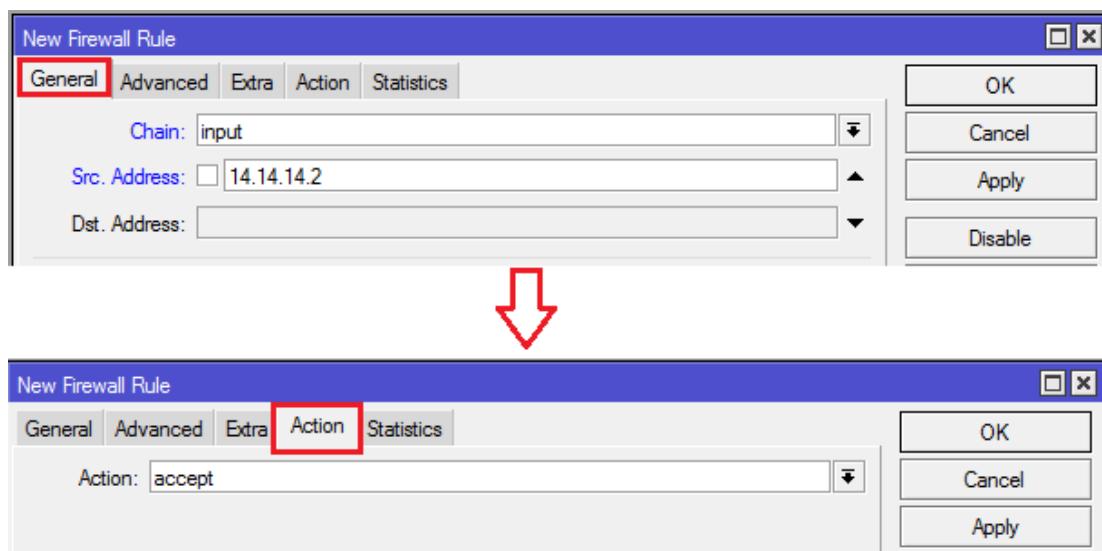
Kalo udah sekarang kita langsung aja ke langkah konfigurasi nya

Ini hampir sama seperti lab sebelumnya , jika kalian masih ngelanjutin dari lab sebelumnya , saya harap **konfigurasi tadi dihapus** dulu , kita akan mulai dari awal

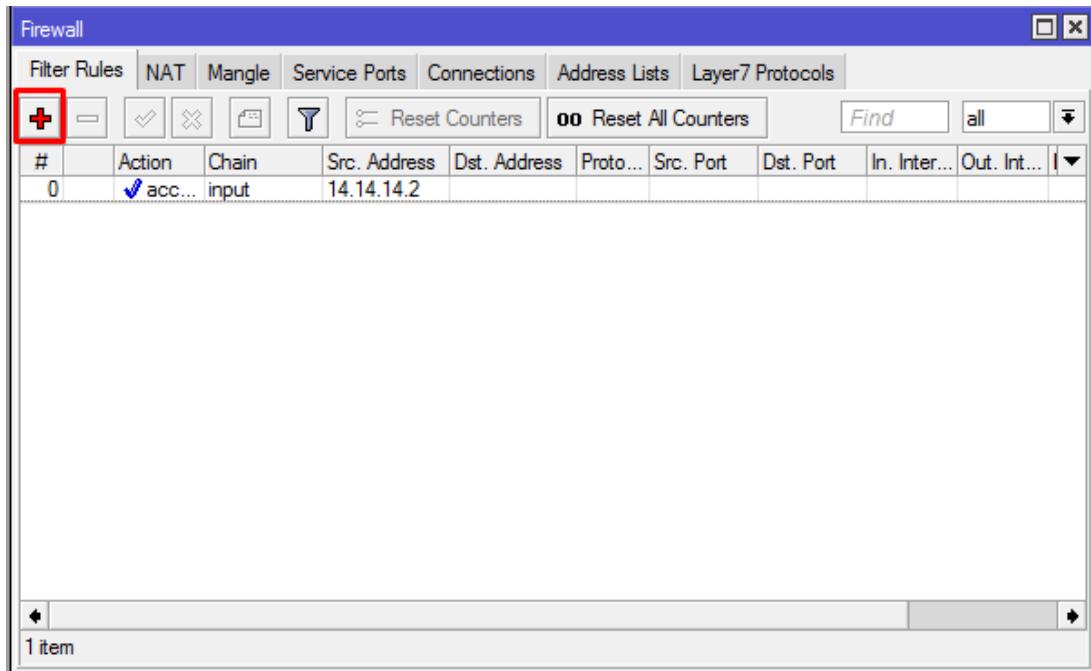
Oke , pertama klik IP > Firewall > Filter Rules > Add



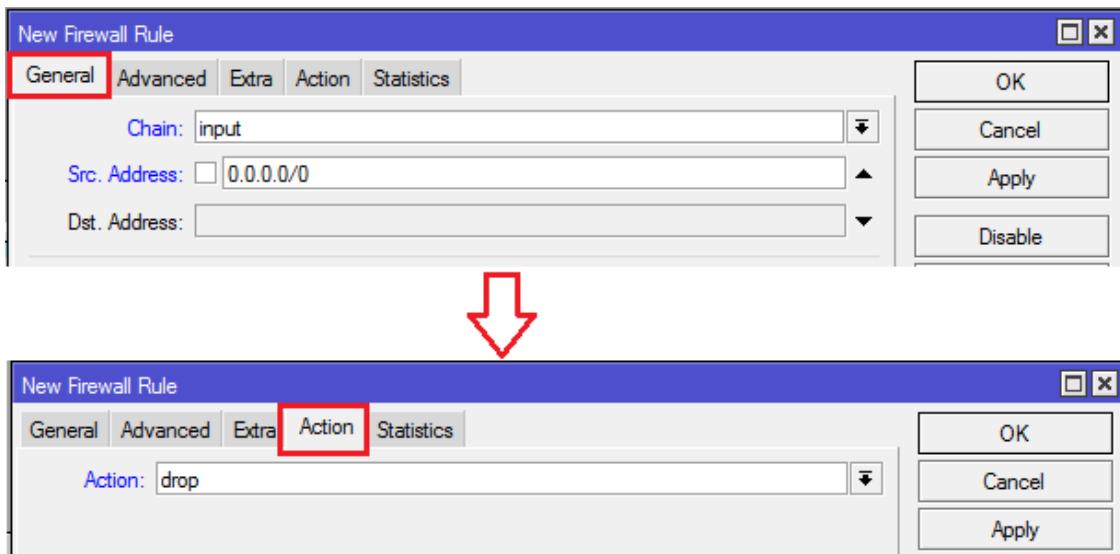
Kemudian kita buat Rule untuk **Accept Few** (Terima beberapa). Kita masukkan chain=input lalu di bagian src-address kita masukkan IP dari admin atau ip kita sendiri, kemudian di tab **action=accept**.



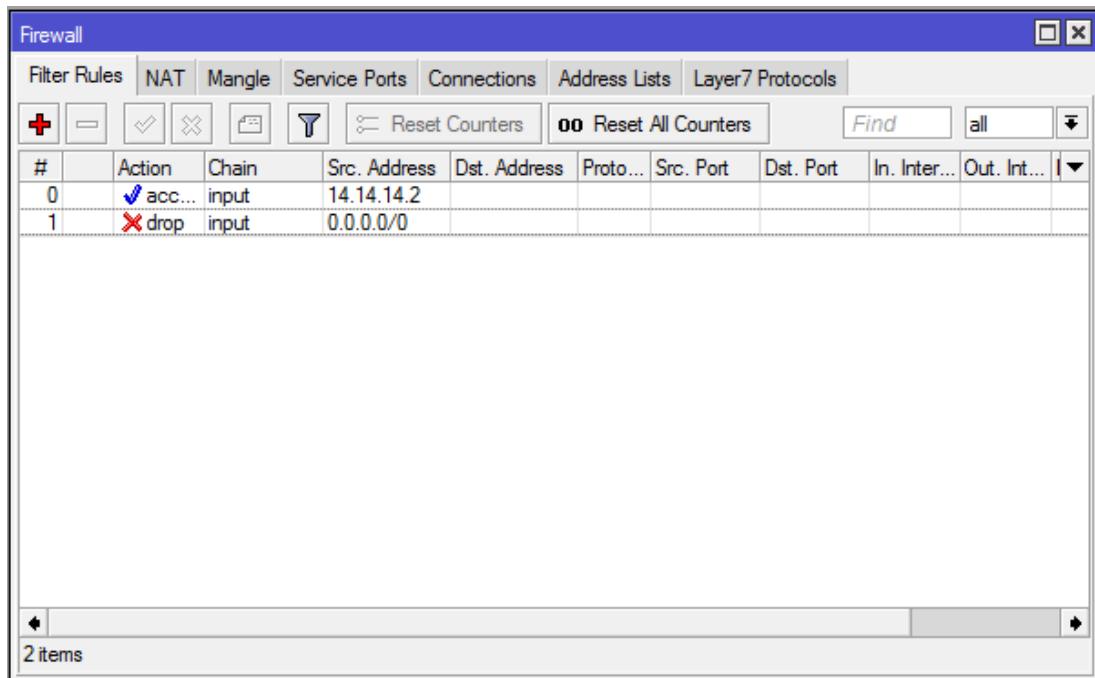
Dengan rule diatas kita sudah membuat yang **accept few** , bisa dilihat hasil rule dibawah ini. selanjutnya kita akan buat rule untuk mendrop semua paket lainnya. Caranya klik tombol add lagi



Kemudian masukkan seperti rule sebelumnya hanya saja IP nya yang dibedakan , ubah menjadi **0.0.0.0/0** ini menandakan berjuta juta IP lainnya. Kemudian Actionnya kita buat menjadi **drop**.



Kemudian inilah hasil rule yang telah kita buat tadi , Ingat Mikrotik membaca rule **Top to Bottom atau dari atas ke bawah**.



Kemudian coba test Ping dari IP 14.14.14.2 , pasti berhasil

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

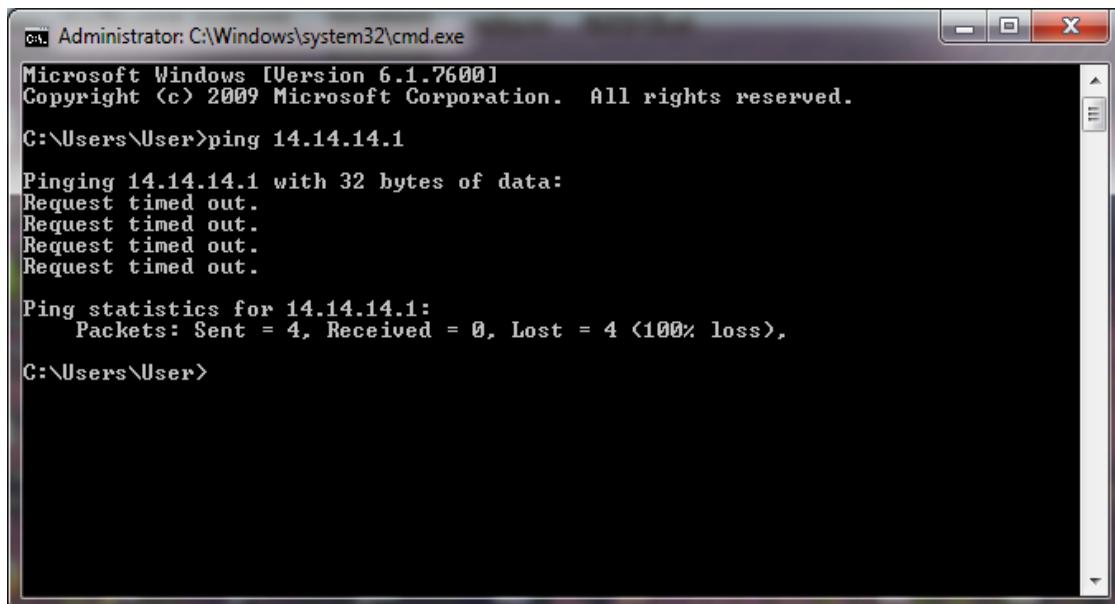
C:\Users\User>ping 14.14.14.1

Pinging 14.14.14.1 with 32 bytes of data:
Reply from 14.14.14.1: bytes=32 time<1ms TTL=64
Reply from 14.14.14.1: bytes=32 time<1ms TTL=64
Reply from 14.14.14.1: bytes=32 time=1ms TTL=64
Reply from 14.14.14.1: bytes=32 time=1ms TTL=64

Ping statistics for 14.14.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```

Lalu coba ganti IP nya bebas , asal jangan **14.14.14.2** , contoh disini saya pakai **IP 14.14.14.90** , lalu coba test ping kembali bagaimana hasilnya ?? Pasti gagal lah , karena yang bukan IP 14.14.14.2 akan di drop



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 14.14.14.1

Pinging 14.14.14.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 14.14.14.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\User>
```

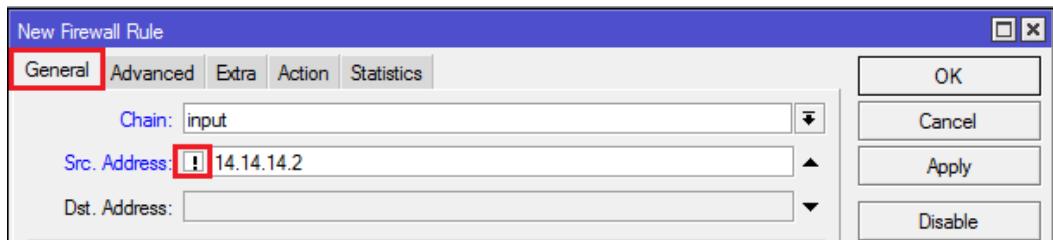
Oke ternyata sudah berhasil , sesuai dengan yang diharapkan yakni hanya IP admin saja yg bisa mengakses RouterBoard. Selain IP itu maka akan di drop.

Sebenarnya ada cara lain yang lebih simple gan , yaitu hanya dengan membuat 1 rule aja cukup untuk semuanya.

Daripada bingung langsung aja ke konfigurasinya.

Sebelum itu kita **HAPUS** dulu semua konfigurasi sebelumnya.

Kemudian kita buat rule baru seperti dibawah ini. Kemudian kita klik kotak kecil dibagian depan **src-address**.



Bisa dilihat perbedaannya adalah di Tanda “!” di depan Src.Address. tanda “!” artinya adalah “**selain**”. Jadi kita terjemahkan rule diatas.

*Jika ada yang mencoba masuk **selain** IP 14.14.14.2 maka akan di **drop***

Kemudian inilah hasil dari rule yang kita buat , jadi hanya ada satu rule saja. Dan hasilnya pun sama

Firewall										
Filter Rules		NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols			
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	I▼
0	drop	input	!14.14.14.2							

1 item

Oke karena sudah berhasil maka lab kali ini saya tutup dengan mengucap Alhamdulillah.

Sekian dulu yaaa

Wassalam !

Lab 25. Firewall Filter INPUT (Membatasi Port untuk mengakses Router)

Assalamualaikum wr.wb

Lanjut lagi dari lab sebelumnya , jika di lab sebelumnya kita memblok IP yang mengakses Router maka di Lab ini akan dibahas mengenai membatasi Port untuk mengakses Router. Maksud port disini adalah port port fitur remote yang digunakan mikrotik. Untuk masalah port yang digunakan untuk mengakses mikrotik sudah saya bahas di lab pertama jadi saya buat simple aja , adapun port yang dapat meremote mikrotik diantaranya , **port 8291 (Winbox) , 22 (ssh) , 23 (telnet) , 80 (WebFig)**

Kalo di lab sebelumnya saya Cuma bahas satu taktik , di lab ini saya bakal praktekan dengan 2 taktik.

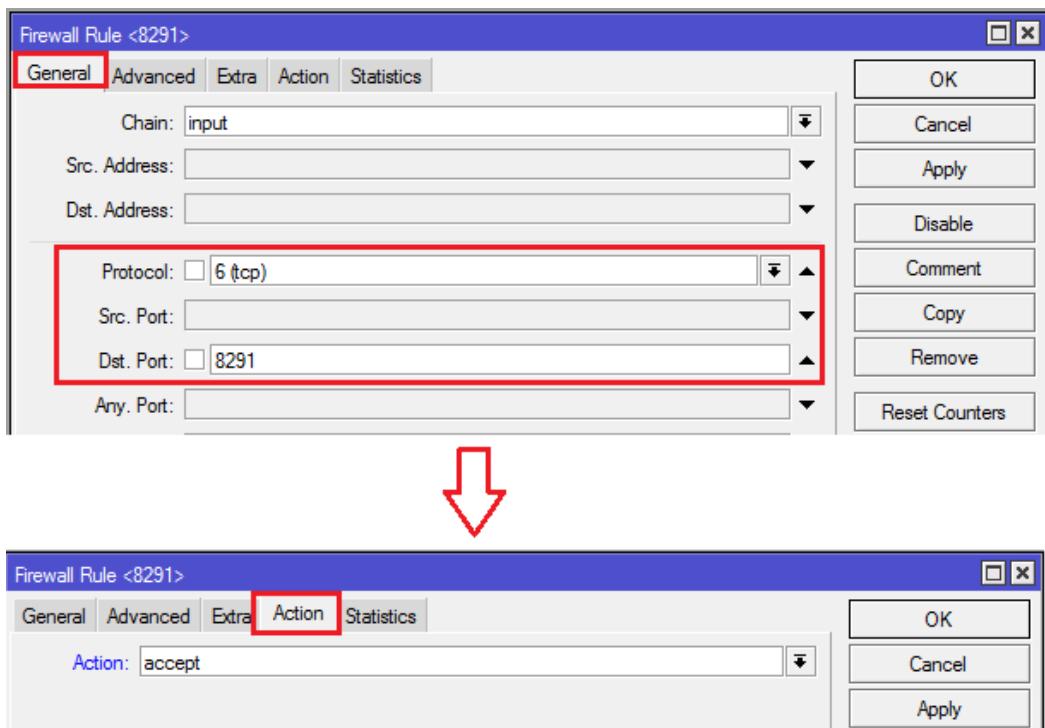
Accept Few , Drop Any (Terima beberapa , Buang Semuanya)

Untuk konfigurasi taktik diatas artinya kita akan membolehkan beberapa port lalu mendrop yang lainnya , begini kasusnya

"Kita akan memblok semua port kecuali Port Winbox (8291). "

Langkah konfigurasinya :

Klik menu IP > Firewall > Filter Rule > Add , kemudian buat rule seperti gambar dibawah ini , kita akan buat rule untuk meng-**accept** terlebih dulu , kita masukkan protocol **tcp** , dan port nya **8291**.

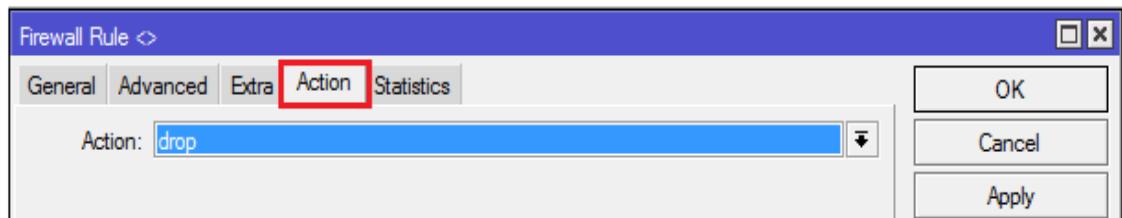
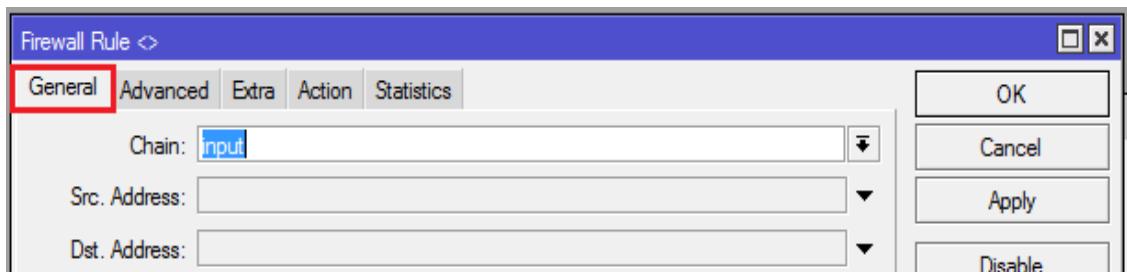


Maka hasilnya akan seperti ini ,

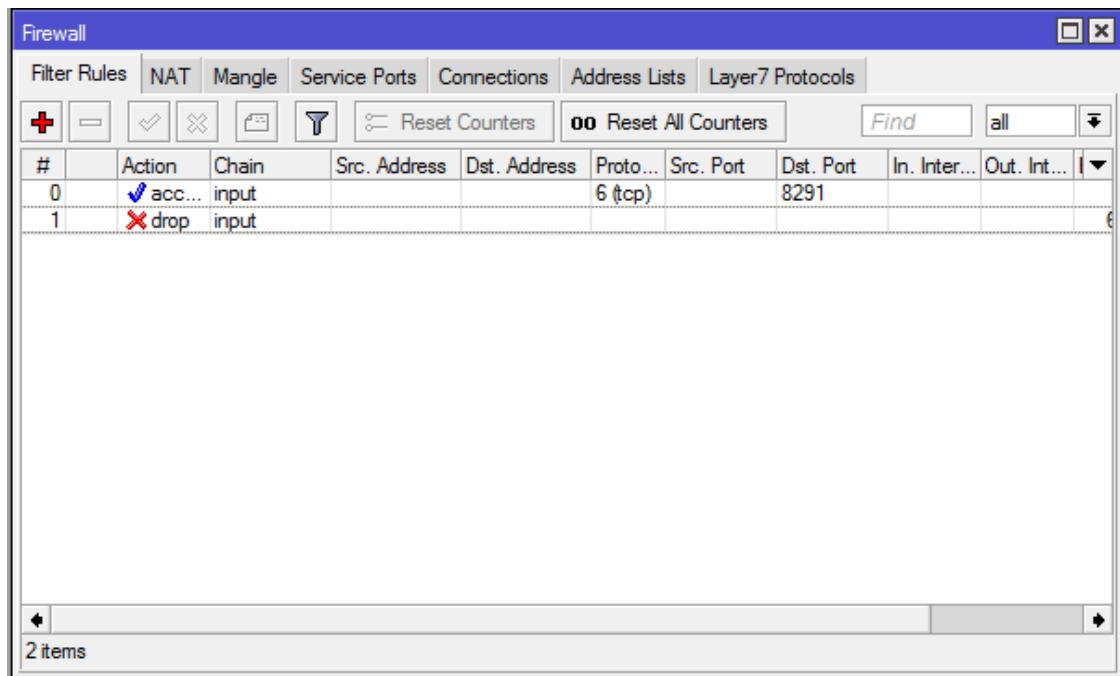
Firewall										
Filter Rules		NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols			
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Interface
0	✓ acc...	input			6 (tcp)		8291			

1 item

Lalu kita buat rule lagi dengan cara mengklik **Add** , kemudian kita buat rule untuk mendrop semua port, caranya adalah sebagai berikut dengan **action=drop**



Kemudian inilah hasil akhir dari rule yang kita buat , dengan rule seperti ini maka router hanya bisa diakses melalui winbox



Sekarang silahkan coba remote lewat telnet atau port yang tadi diblok , hasilnya pasti gagal.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>telnet 14.14.14.1
Connecting To 14.14.14.1...Could not open connection to the host, on port 23: Connect failed

C:\Users\User>
```

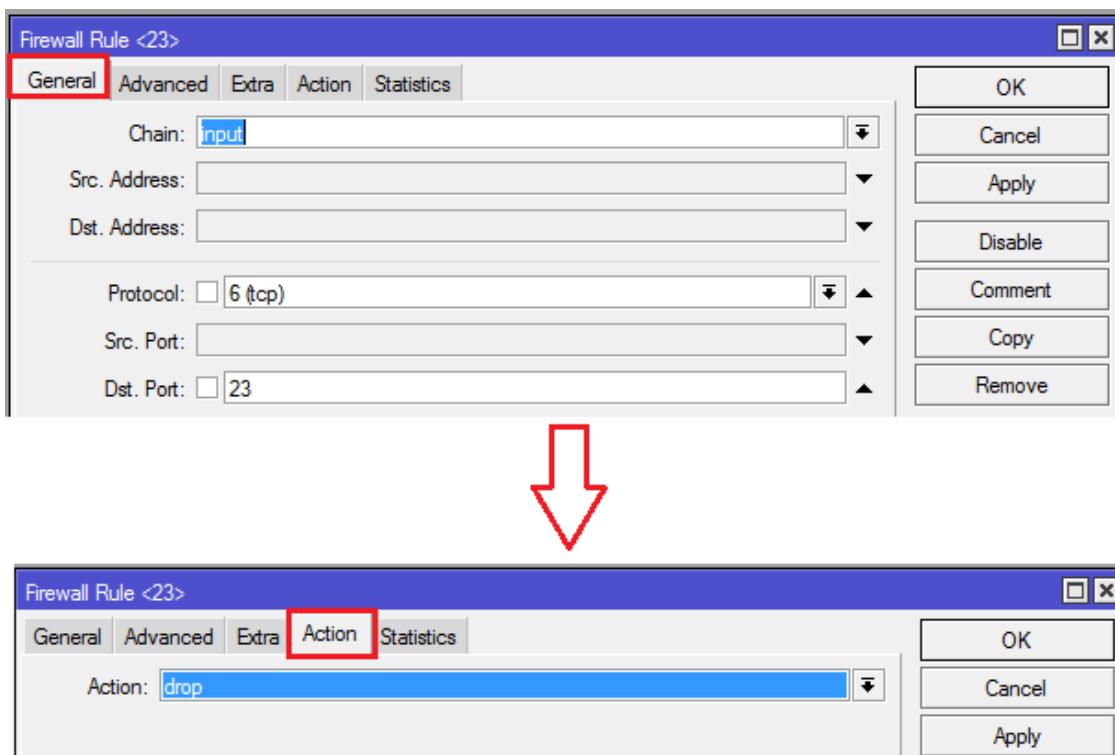
Drop Few , accept Any (Buang beberapa , Terima Semuanya)

Oke sekarang kita pakai taktik yang kedua jadi kita akan membuang port yang tidak digunakan kemudian membolehkan semua port , kasusnya begini

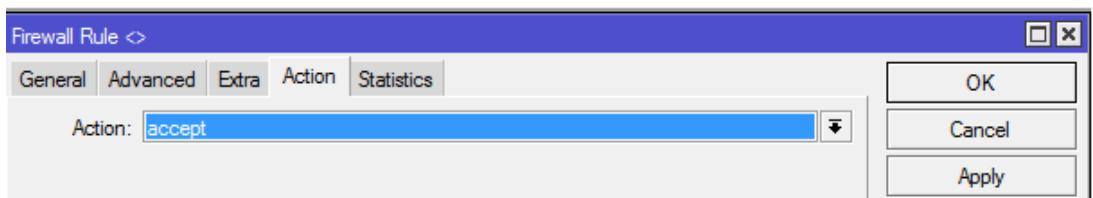
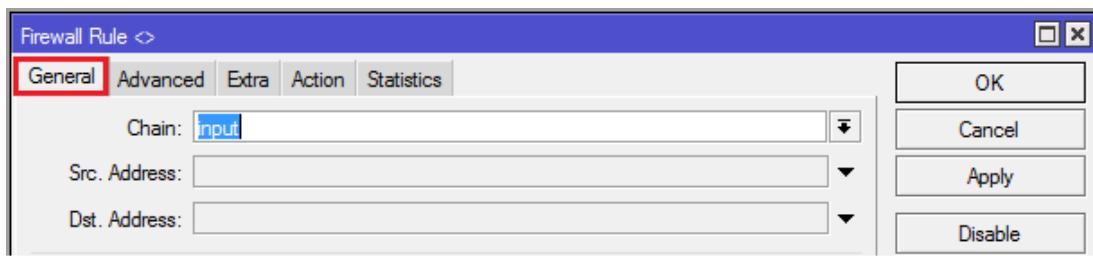
"Kita ingin Router Kita tidak bisa diakses melalui telnet , namun tetap bisa diakses melalui cara yang lain"

Langsung aja ke konfigurasinya , disini saya Cuma nampilin pembuatan rule nya yaa. Pertama **hapus dulu semua rule sebelumnya** , jadi pastikan tidak ada rule di firewall Filter

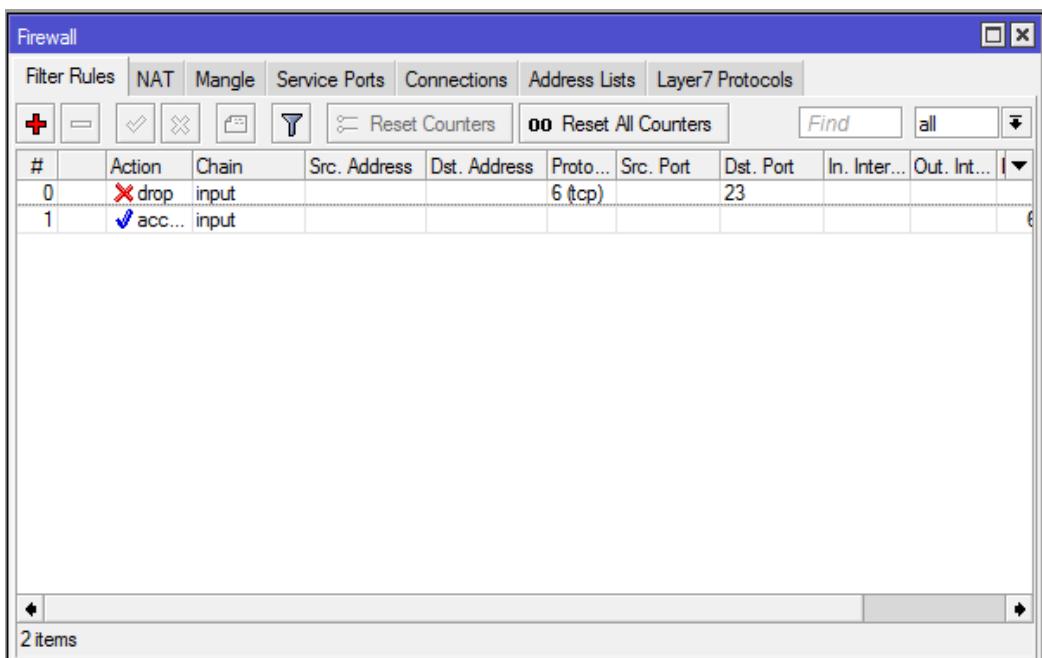
Kita buat rule untuk mendrop port telnet (23)



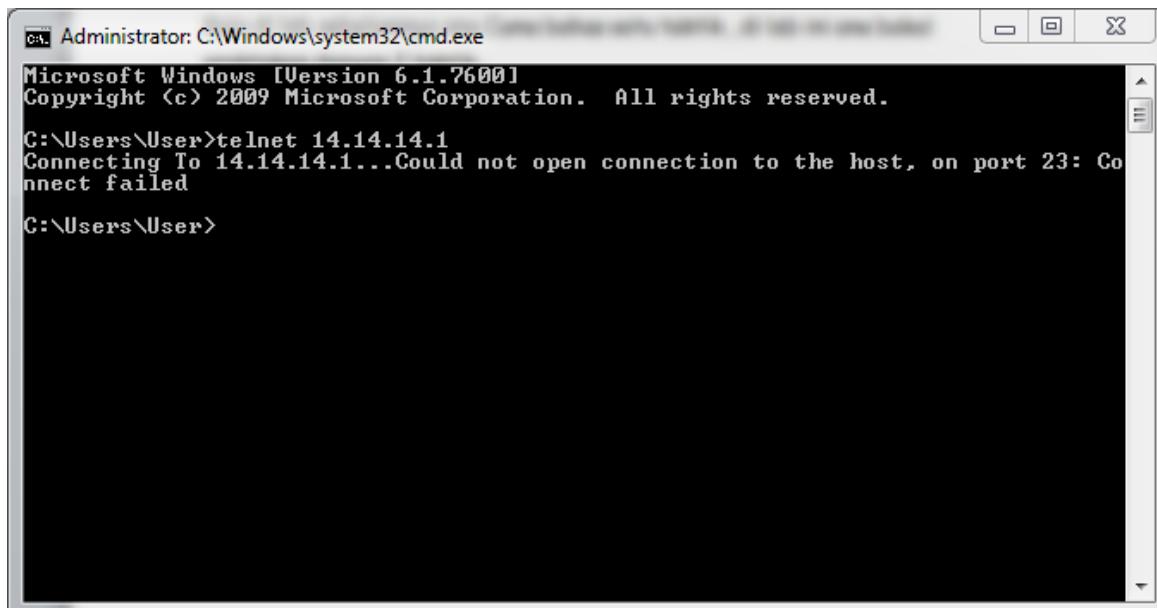
Selanjutnya kita buat lagi rule untuk membolehkan semua port masuk , dengan rule seperti ini.



Maka seperti ini lah hasil akhir pembuatan rule kita. Rule ini akan membuat router tidak bisa diakses melalui telnet.



Maka hasilnya adalah seperti ini , ketika akan diakses melalui telnet hasilnya tidak akan terbuka.



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the following text:

```
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>telnet 14.14.14.1
Connecting To 14.14.14.1...Could not open connection to the host, on port 23: Connect failed

C:\Users\User>
```

Oke karena sudah berhasil maka saya tutup lab kali ini , mohon maaf bila ada kekurangan

Wassalam !

Firewall FORWARD.

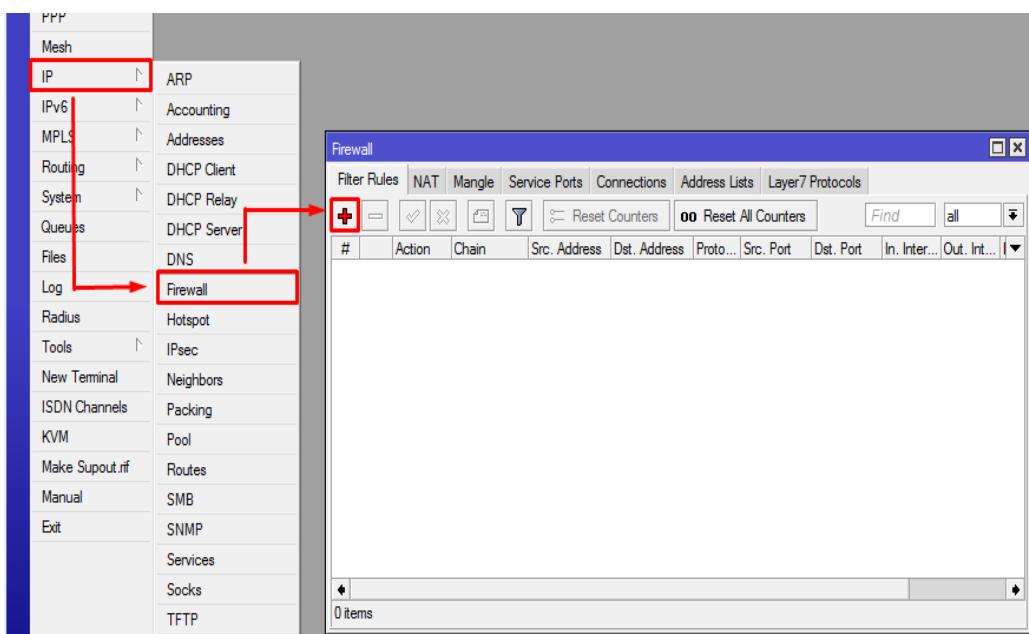
Setelah selesai materi Firewall Input , sekarang masuk pembahasan Forward. Firewall ini lah yang menangani paket yang melewati Router , baik dari jaringan lokal maupun dari jaringan luar . Firewall ini juga yang menentukan boleh tidaknya sebuah paket menuju internet ataupun menuju jaringan lokal. Karena berhubungan dengan internet maka Firewall ini menentukan **website apa saja yang bisa diakses oleh client**.

Lab 26. Blok Akses Forward

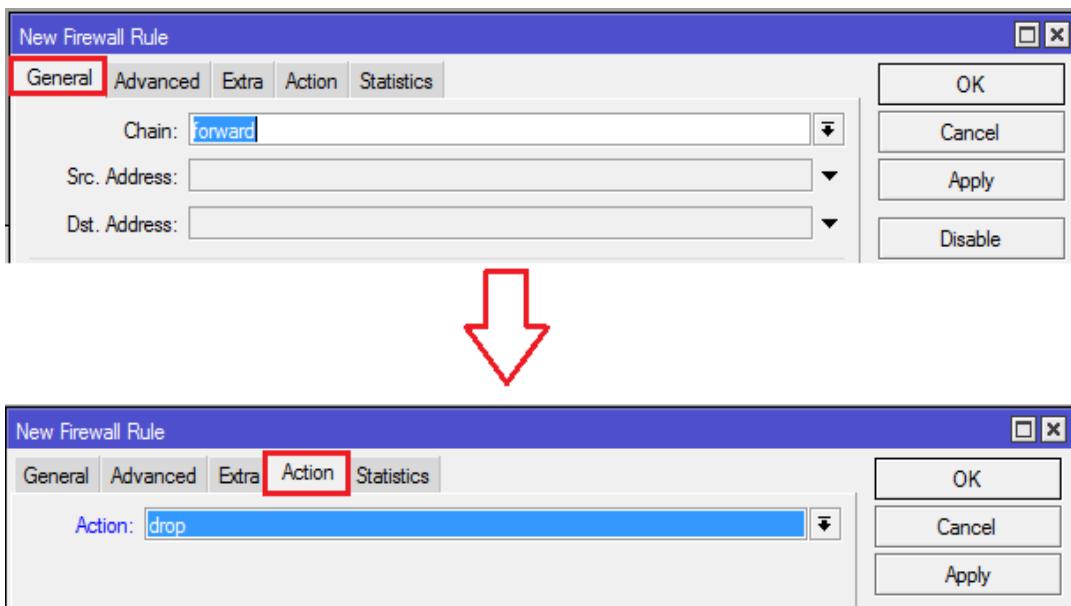
Assalamualaikum wr. Wb

Oke biar kalian lebih paham tentang Firewall Forward ini , dilab kali ini saya bakal ngasih percobaan yaitu kita akan memblok Akses yang melewati Router. Jadi dalam kasus ini Client **tidak akan bisa melakukan koneksi ke internet** , yaitu dengan cara memblok Akses Forward nya.

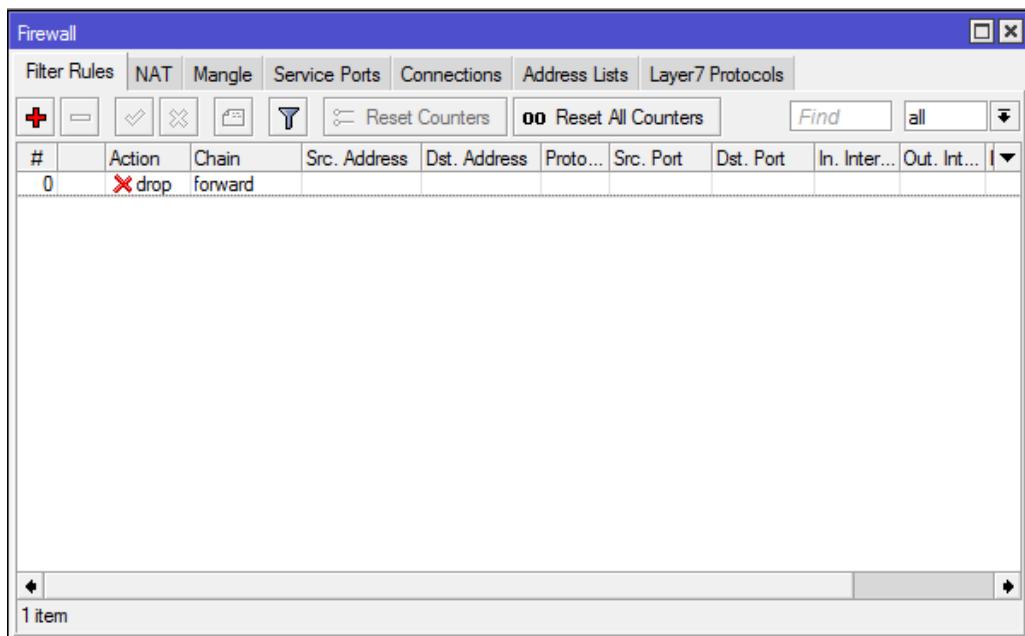
Oke berikut caranya , pertama klik IP > Firewall > Filter Rules > Add ,



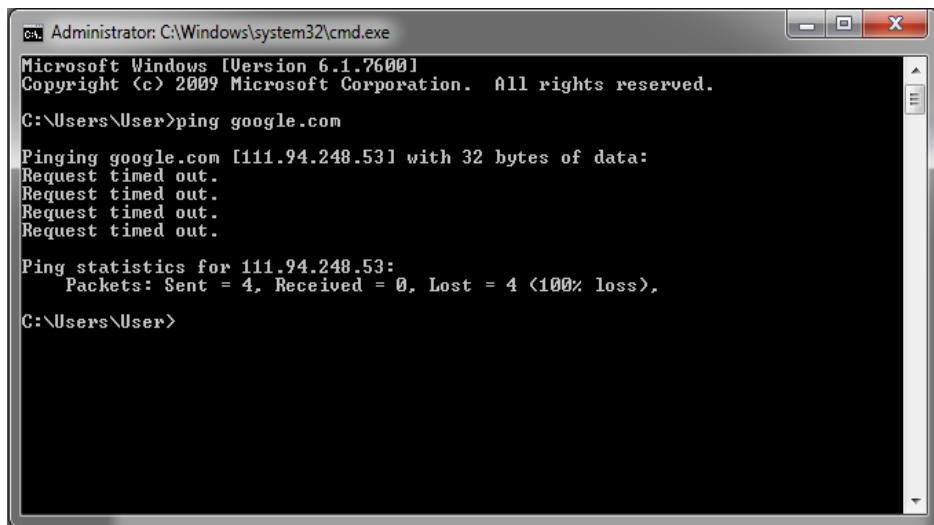
Selanjutnya kita buat rule untuk mendrop semua paket yang melewati Router. Monggo di cek gambarnya , kita buat **chain=forward , action=drop**.



Setelah itu inilah hasil dari pembuatan rule kita . Dengan rule ini maka paket yang melewati Router baik dari client maupun dari luar akan di **drop**.



Kemudian kita coba test ping dari client menuju internet , hasilnya pasti RTO seperti gambar dibawah ini



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping google.com
Pinging google.com [111.94.248.53] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 111.94.248.53:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\User>
```

Nah kan di drop paketnya . Kalian pasti bingung kenapa harus di drop ??
Lab ini Cuma buat menambah pemahaman dari konsep Firewall Forward aja. Jadi
saya harap setelah memahami lab ini maka kalian para pembaca akan memahami
konsep dari Firewall Forward ini.

Oke sekian dulu yaa

Wassalam !

Lab 27. Blok Situs Menggunakan Firewall Forward

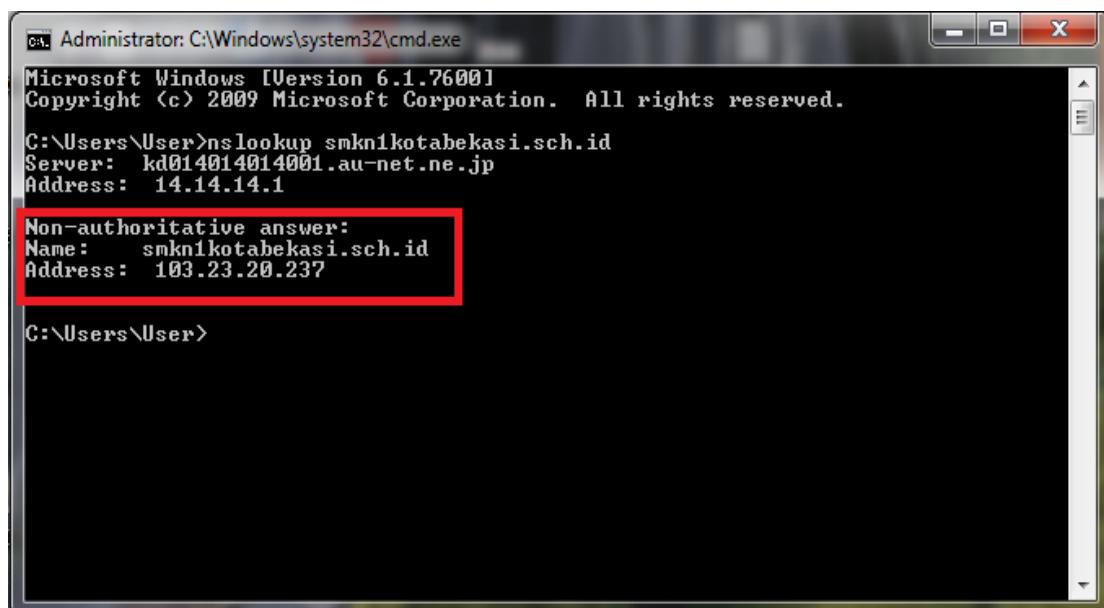
Assalamualaikum wr.wb

Lanjut lagi yaa , setelah kalian mulai paham konsep Firewall Forward sekarang saatnya masuk ke tahap sedikit lebih lanjut. Sebelumnya saya udah bilang kan , kalo Firewall Forward ini menentukan website apa saja yang dapat dinikmati oleh client. Nah di lab ini saya bakal ngebahas cara memblok situs menggunakan Firewall Forward. Pasti seruu kaan nge blok blok situs gitu 😊.

Oke langsung aja study case nya .

*saya mau ngeblok situs sekolah saya sendiri yaitu
www.smkn1kotabekasi.sch.id , entah kenapa rasanya pengen banget blok tuh
situs 😊.*

Oke langsung aja ke langkah konfigurasinya , yang pertama harus dilakukan adalah kita harus mencari tau IP dari website target kita, dengan cara menggunakan nslookup.



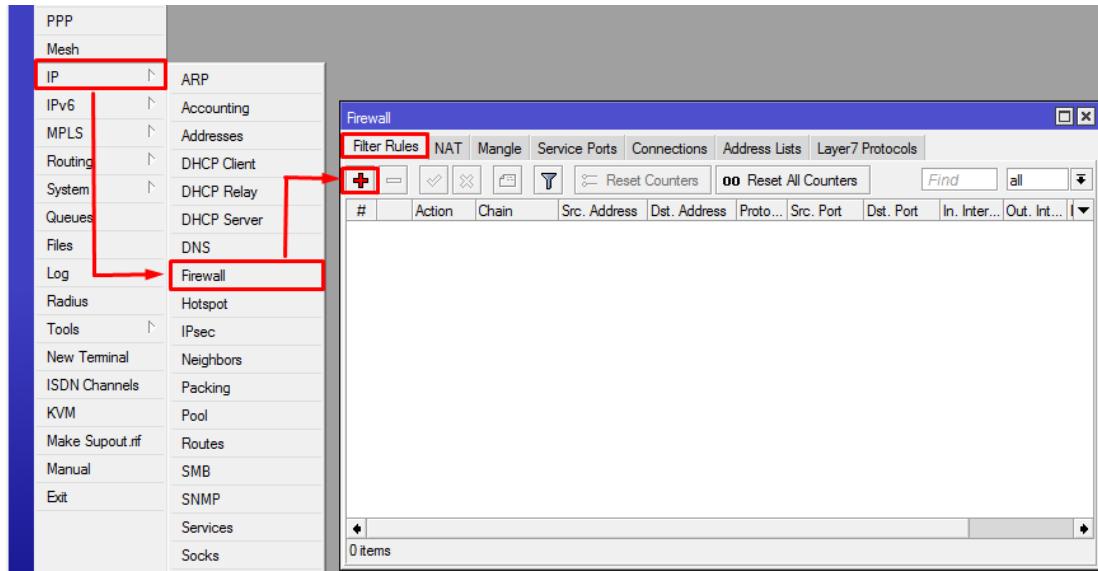
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>nslookup smkn1kotabekasi.sch.id
Server: kd014014014001.au-net.ne.jp
Address: 14.14.14.1

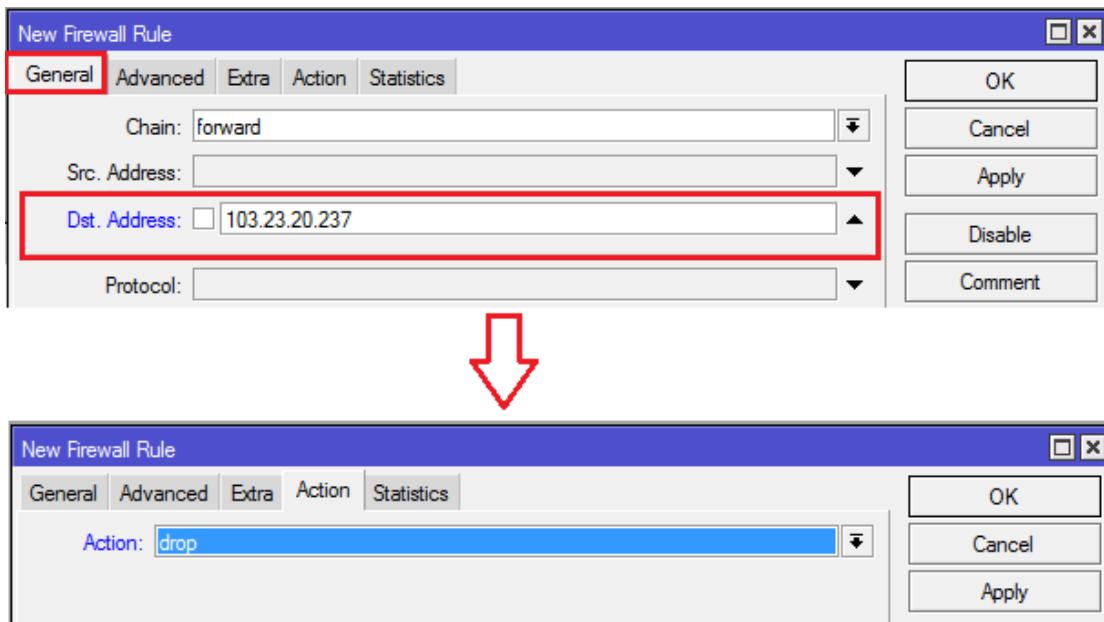
Non-authoritative answer:
Name: smkn1kotabekasi.sch.id
Address: 103.23.20.237

C:\Users\User>
```

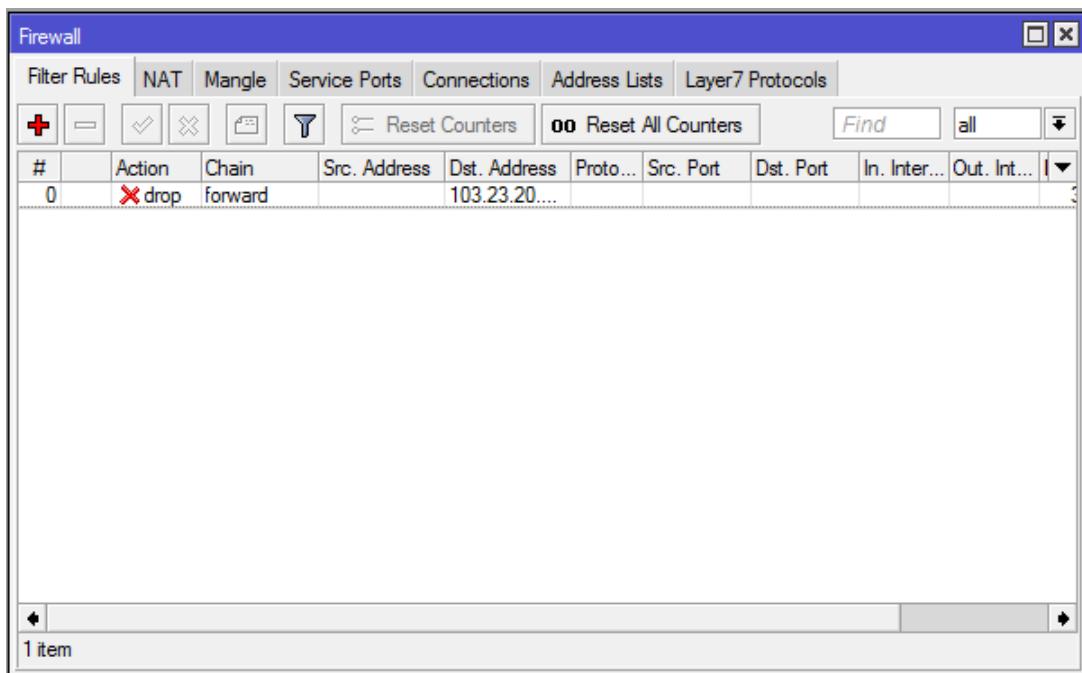
Selanjutnya kita buka menu firewall , dengan cara klik IP > Firewall > Filter Rules > Add



Kemudian kita buat rule forward nya , oh ya pastikan Konfigurasi di lab sebelumnya dihapus yaaa. Kemudian inilah rule yang akan kita buat , masukkan IP address target di bagian dst-address



Kemudian inilah hasil rule yang tdi kita buat. Dengan rule ini maka situs smkn1kotabekasi.sch.id tidak bisa dibuka



Silahkan coba buka situs yang tadi diblok , maka hasilnya tidak akan berhasil



Oke karena sudah berhasil saatnya saya untuk bilang *sempoaal* , tolong di ingat bijaklah dalam memblok situs, dengan rule ini kita juga bisa memblok **situs yang tidak baik**.

Oke sekian dulu yaa

Wassalam !

Lab 28. Blok Situs berdasarkan Konten.

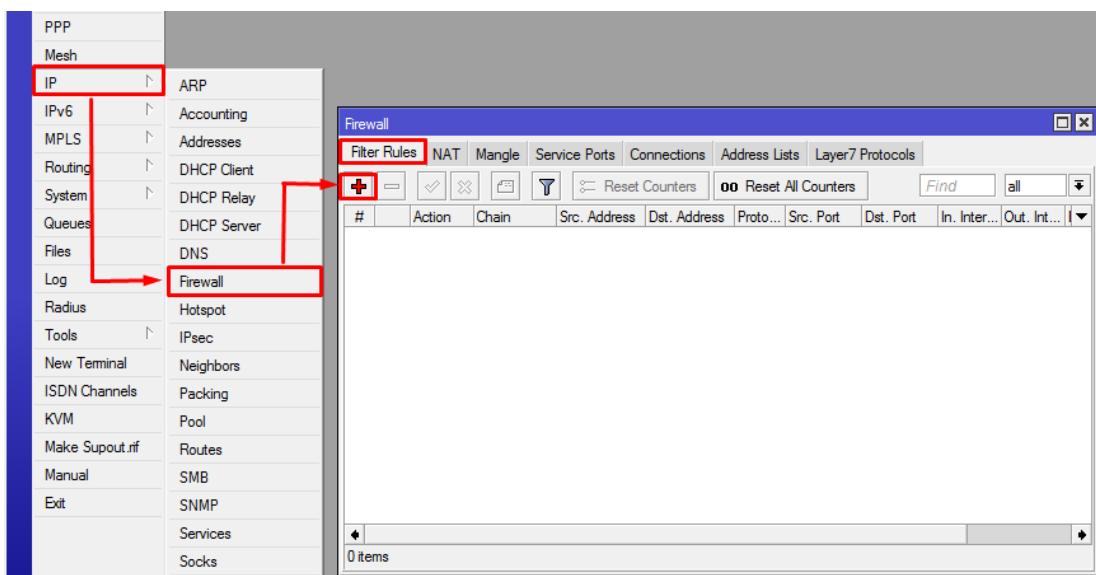
Assalamualaikum wr.wb

Melanjutkan dari lab sebelumnya tentang blokir situs , cuman cara diatas kurang efektif , karena kita harus memasukan IP dari situs target kita. Di lab ini saya mau bahas cara yang lebih ringkas yaitu berdasarkan **Konten atau Kata** .

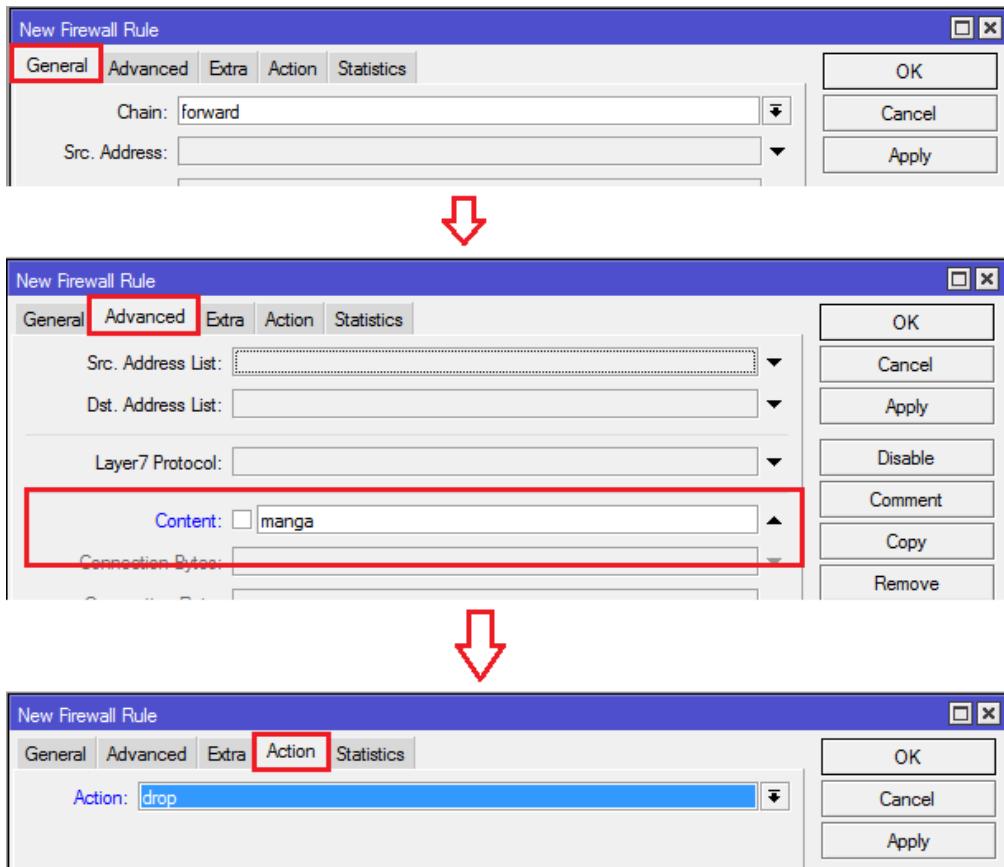
Penasaraan ???

Yok laah lanjut aja ke konfigurasinya

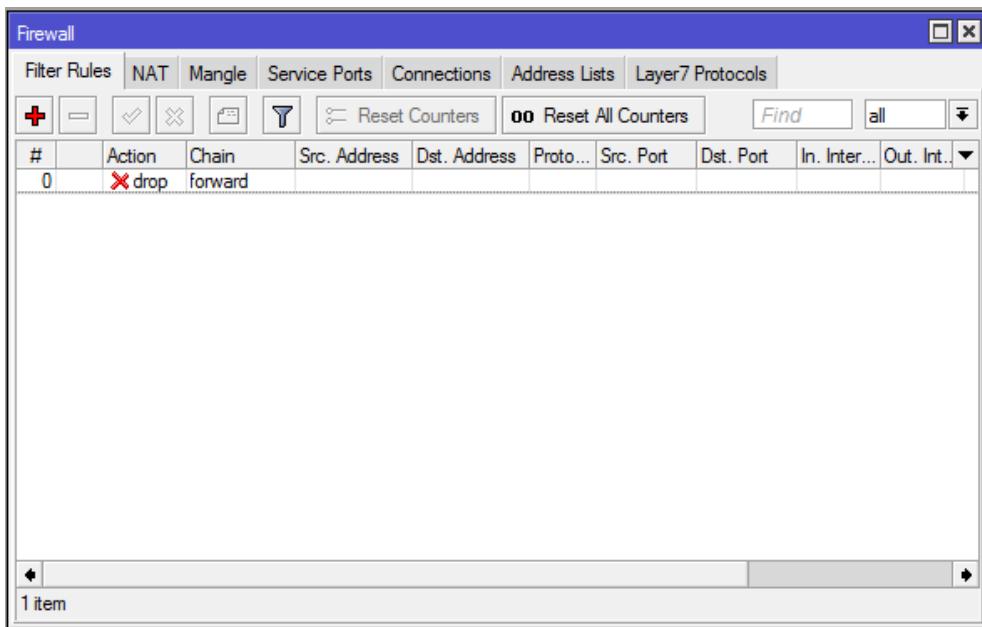
Pertama kita klik menu **IP > Firewall > Filter Rules > Add**



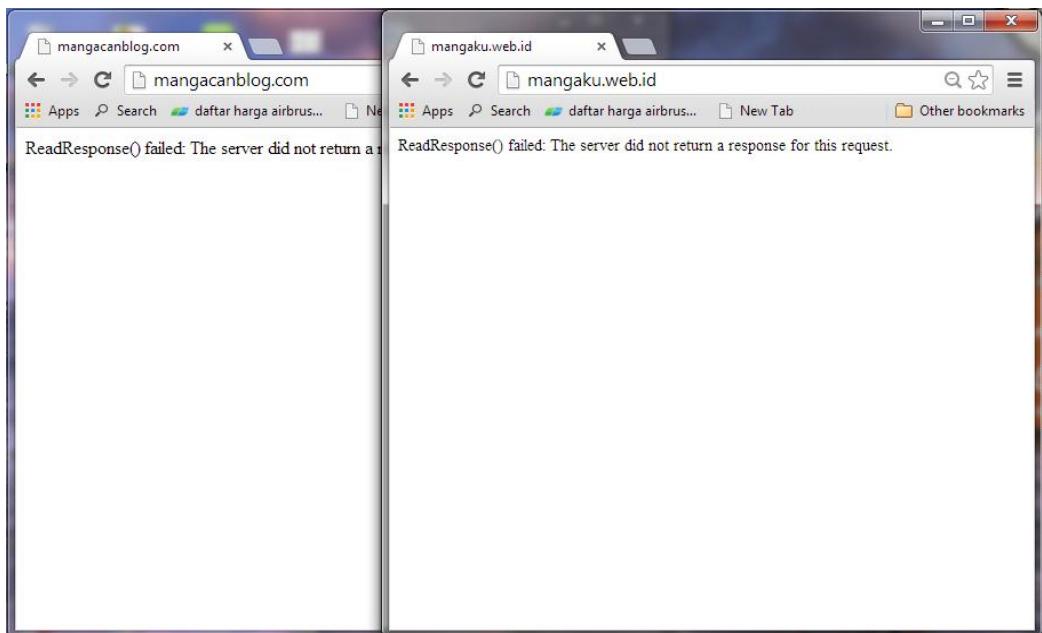
Selanjutnya kita buat rule seperti dibawah ini , dibagian **advanced > content** kita isikan content yang akan kita blok , jangan lupa **action=drop**. Lalu klik **Apply** dan **OK**.



Selanjutnya inilah rule yang sudah kita buat.



Setelah itu silahkan coba situs atau website dengan kata **manga** , maka hasilnya akan seperti ini , alias tidak bisa dibuka .



Bisa dilihat gambar diatas adalah bukti bahwa situs yang memiliki kata Manga , tidak bisa terbuka. Itu artinya rule yang kita buat sudah berhasil

Oke sekian dulu mas broo

Wassalam !

Lab 29. Address List

Assalamualaikum wr.wb

Yuk lanjut lagi , setelah sedikit membahas tentang firewall Forward sekarang kita keluar dulu dari forward , tapi masih nyangkut di materi Firewall kok. Di Lab kali ini saya mau ngebahas tentang Address List.

Opo itu Address List ??

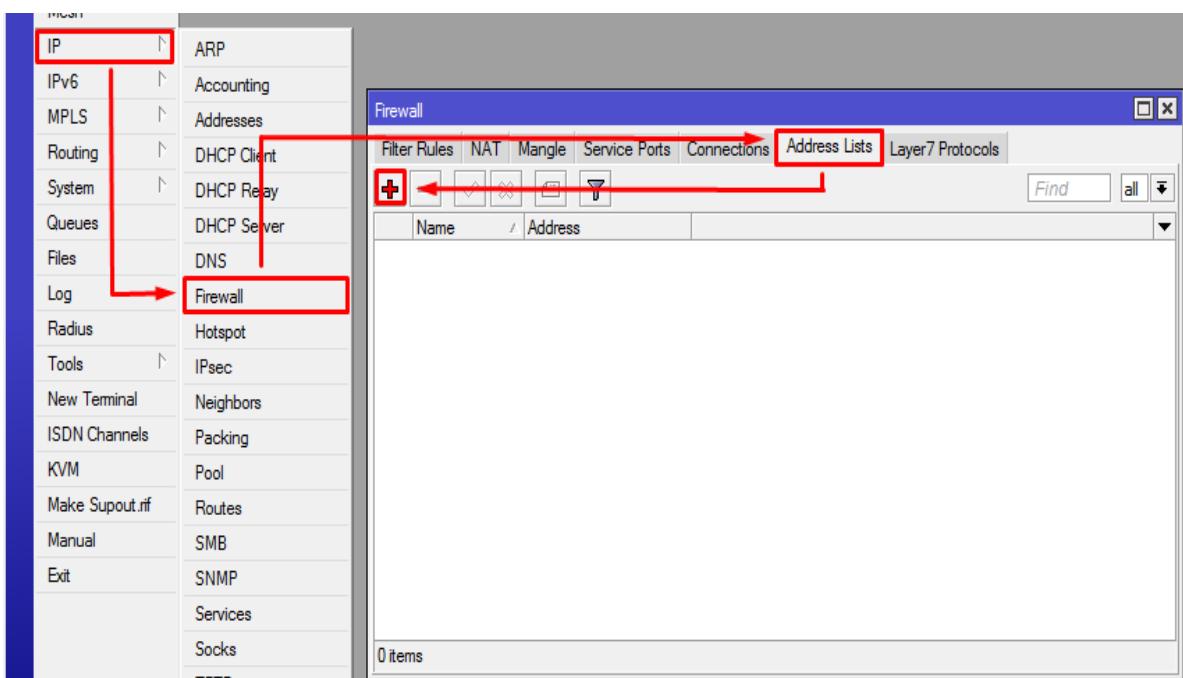
Jadi Address List itu salah satu fitur mikrotik yang digunakan untuk membuat IP tertentu menjadi sebutan nama. Jadi nantinya kita gak perlu lagi berurusan sama angka angka , jadi kita Cuma urusan sama huruf-huruf ☺.

Oke langsung aja di Lab-in yuk ,

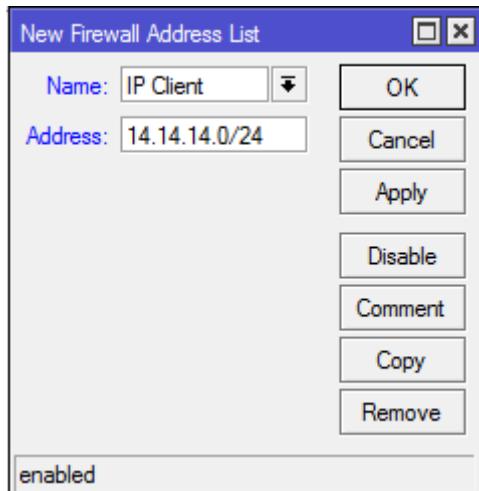
Study Case :

*Disini saya ingin membuat IP lokal saya yaitu **14.14.14.0/24** dengan sebutan **IP Client**. Sedangkan untuk **IP 14.14.14.2** yaitu IP saya sendiri disebut dengan **IP Untung**.*

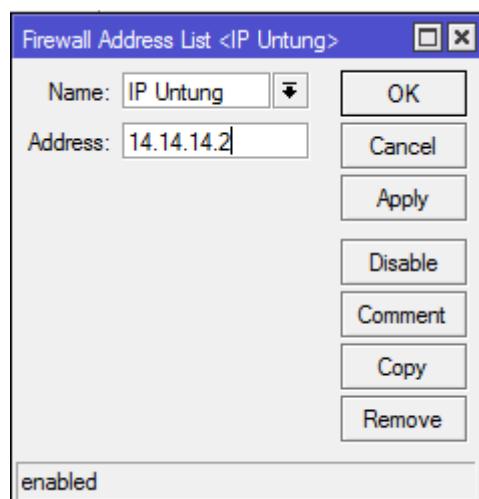
Oke langsung aja ke konfigurasinya , pertama klik menu **IP > Firewall > Address List > Add**



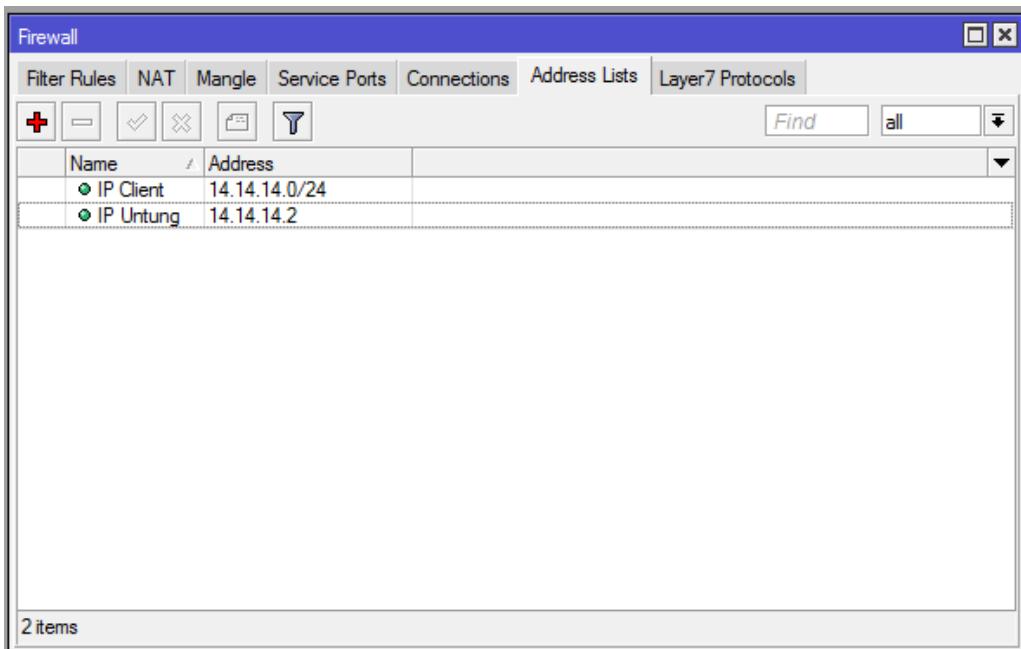
Kemudian kita masukkan Nama/Sebutan dan IP address nya , pertama kita buat untuk **IP Client** yaitu **14.14.14.0/24**



Kemudian kita buat lagi dengan nama **IP Untung** dan **IP nya 14.14.14.2**



Maka hasil akhirnya adalah seperti ini , akan terbentuk 2 Address List , yaitu untuk **IP Client** dan untuk **IP untung**



Oke sekian dulu tentang Lab Address List ini. Oh iya sebagai tambahan Address List ini bisa kita gunakan untuk memanajemen Jaringan kita , sebagai contoh kita bisa memblok situs berdasarkan Address List ini yang akan saya bahas di Lab Selanjutnya.

Wassalam !

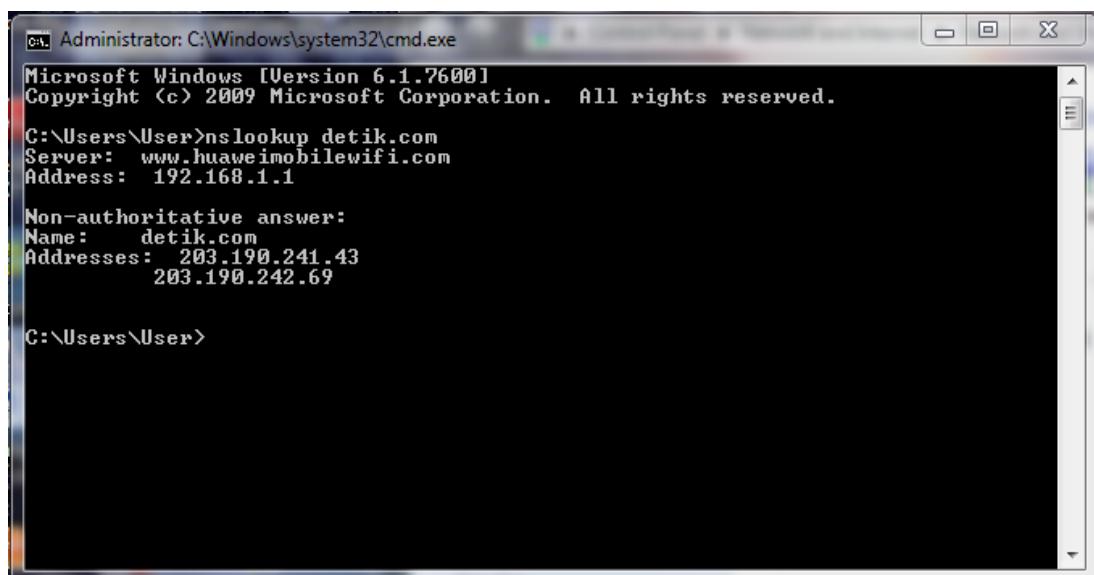
Lab 30. Blok Situs dengan Address List

Assalamualaikum wr.wb

Melanjutkan dari lab sebelumnya tentang address list , di lab ini saya bakal mencoba salah satu manfaat dari Address List tersebut. Yaitu kita akan memblok situs menggunakan Address List.

Langsung aja yoo , saya mau ngeblok situs Detik.com , yang mana detik.com ini memiliki beberapa IP. Nah konfigurasinya seperti berikut

Pertama kita cari tau terlebih dahulu IP dari target kita , caranya masih sama yaitu dengan nslookup



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

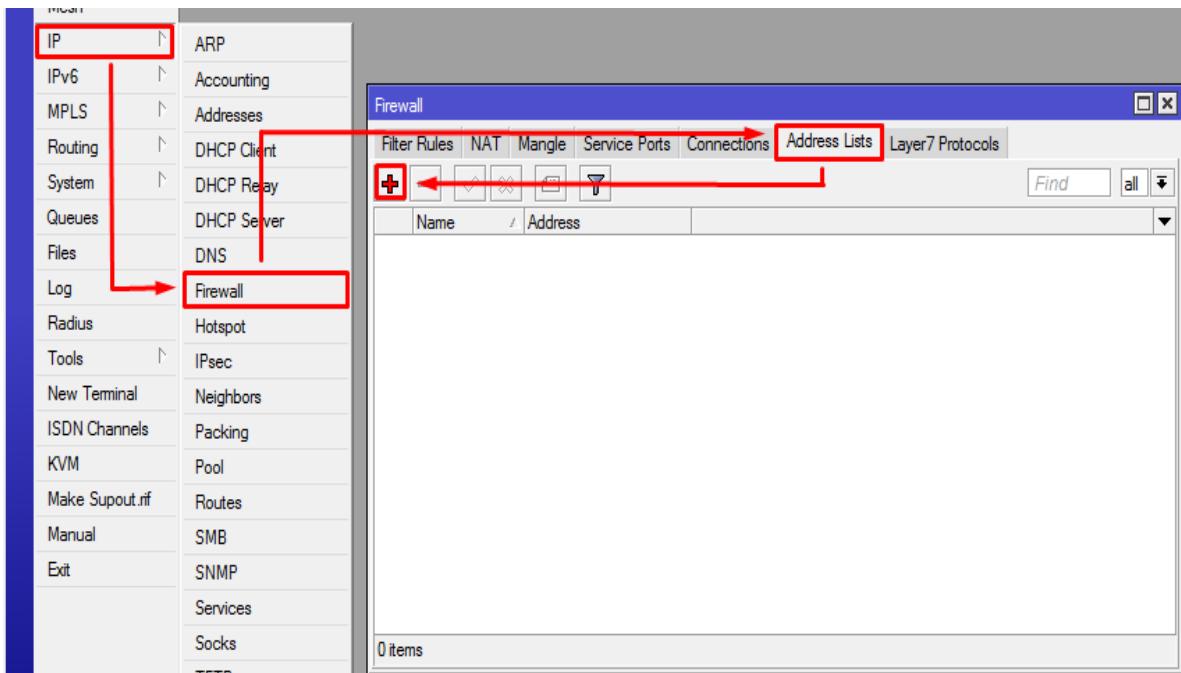
C:\Users\User>nslookup detik.com
Server: www.huaweiimobilewifi.com
Address: 192.168.1.1

Non-authoritative answer:
Name: detik.com
Addresses: 203.190.241.43
          203.190.242.69

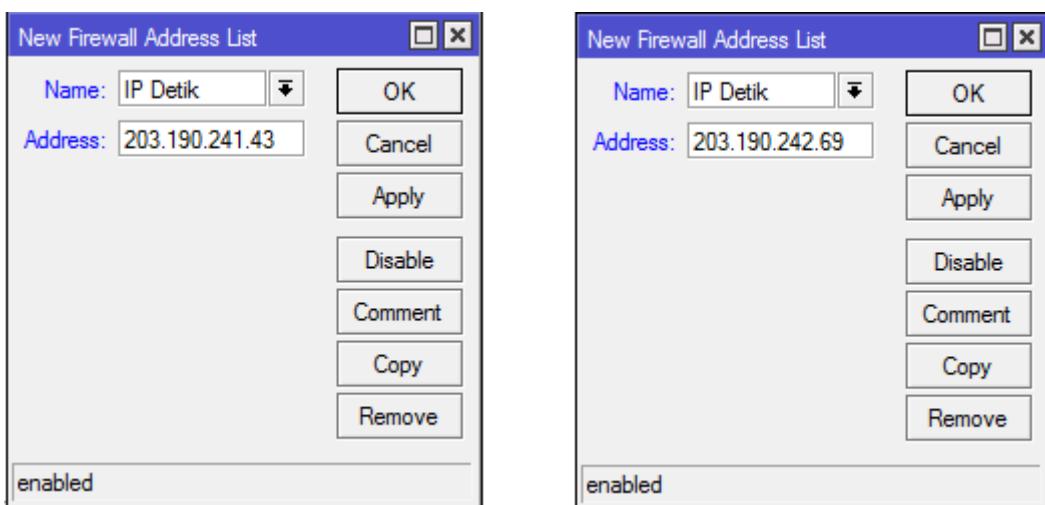
C:\Users\User>
```

Bisa dilihat di gambar diatas , bahwa detik.com mempunyai 2 IP address.

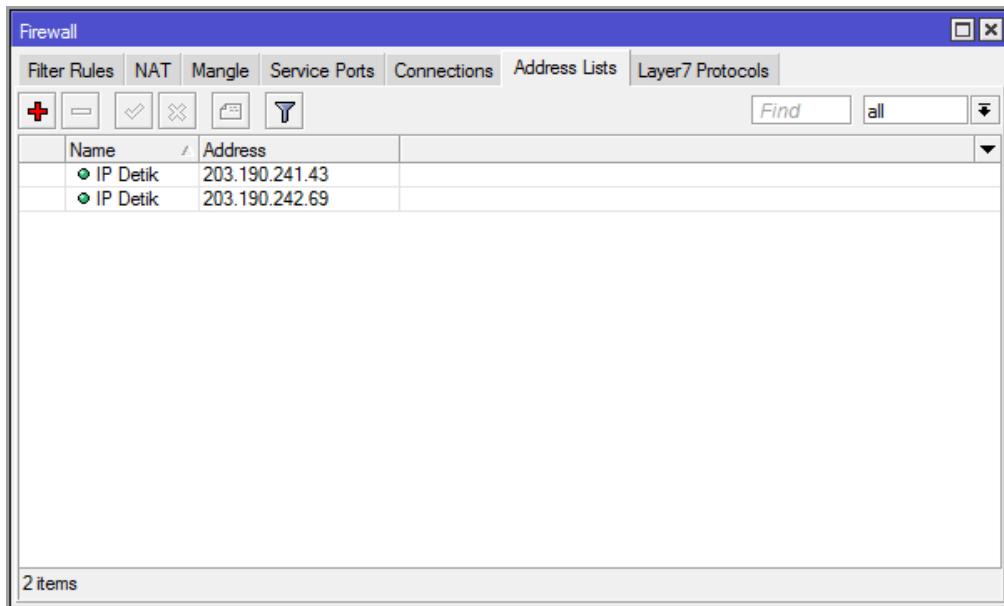
Selanjutnya kita masukkan IP tersebut kedalam address List , caranya klik **IP > Firewall > Address List > Add**



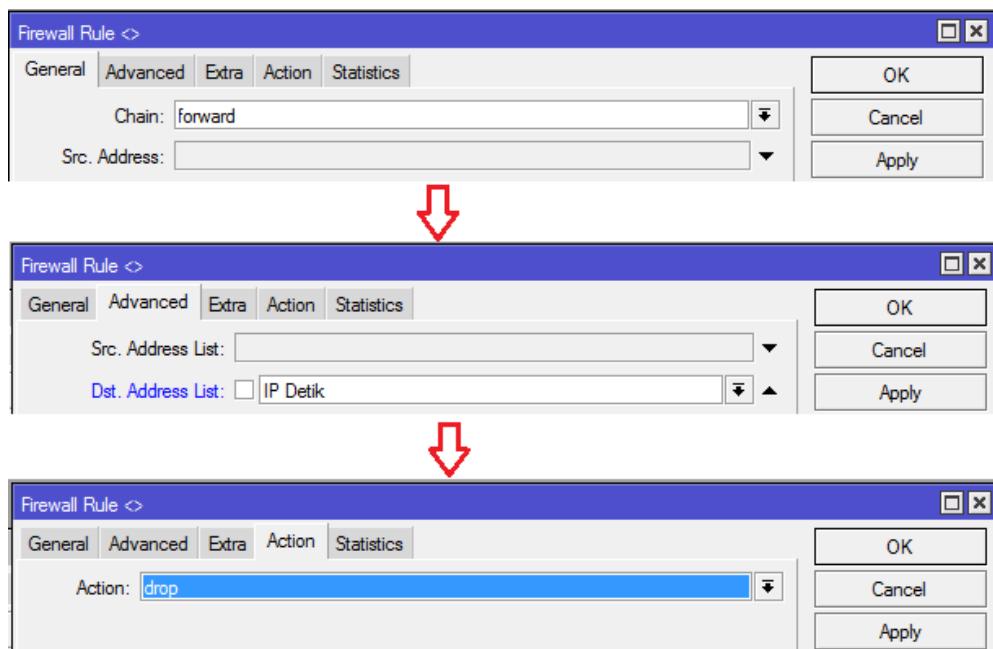
Setelah itu kita masukkan kedua IP dari detik.com itu kedalam address List.



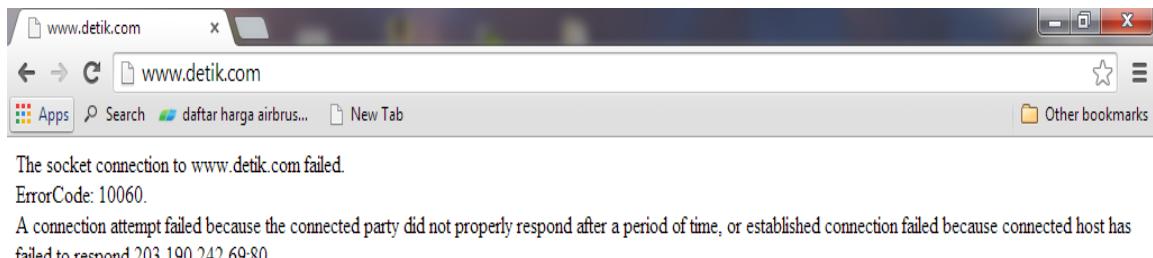
Setelah itu inilah hasil dari Address List yang kita buat tadi. Akan terbentuk 2 address list dengan IP yang berbeda namun Nama yang sama.



Setelah itu kita buat rule untuk memblok akses ke Website Detik.com , yaitu dengan firewall Forward. Pasti masih tau kan caranya. Klik menu IP > Firewall > Filter Rules > Add , kemudian buat rule seperti dibawah ini



Setelah itu apply dan ok . Jika sudah terbentuk rule nya selanjutnya kita coba akses Detik.com dari client, maka hasilnya situs detik.com tidak bisa diakses.



Dan Taraaaaa , situs detik.com tidak bisa diakses. Oke karena sudah berhasil maka saatnya saya untuk bilang *Sempoaal!*

Oke sekian dulu tentang blokir situs dengan Address List.

Kurang lebih nya mohon maaf

Wassalam !

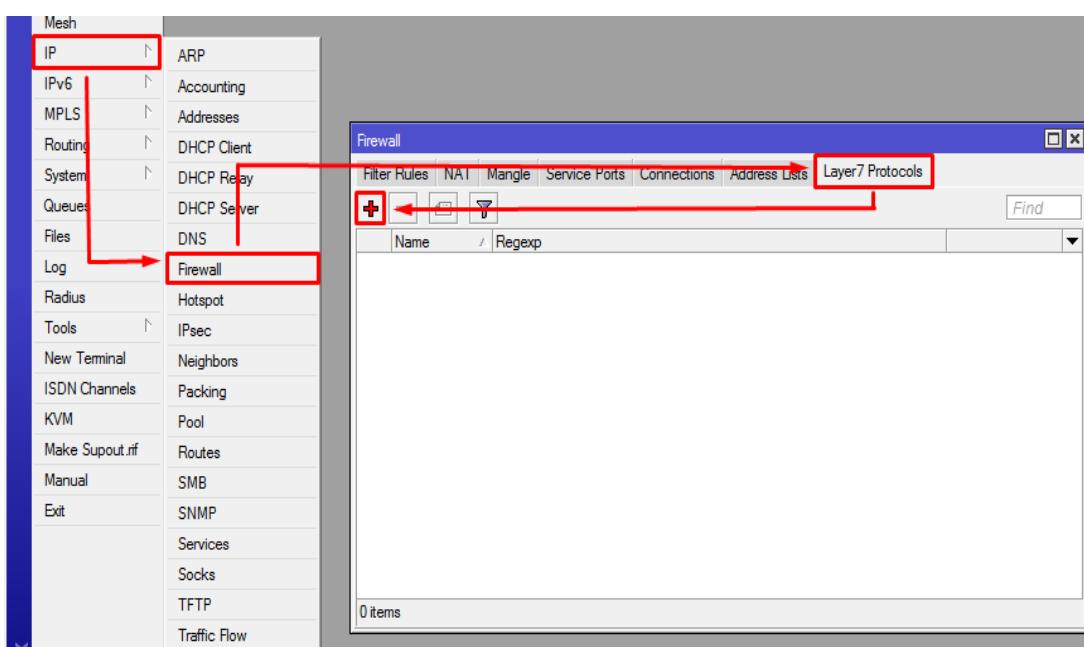
Lab 31. Blok Situs dengan Layer 7 Protocol

Assalamualaikum wr.wb

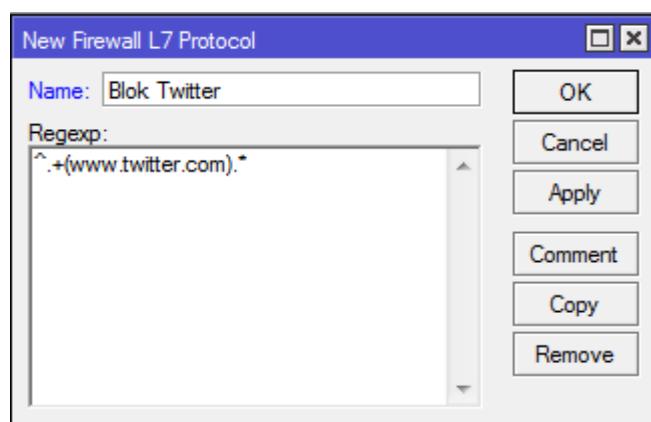
Masih di materi yang sama yaitu tentang blokir situs sana sini. Di Lab kali ini saya mau bahas satu cara lagi blokir situs , yaitu dengan Layer 7 Protocol.

Sebenarnya intinya sama yaitu memblok situs/website yang tidak kita inginkan.

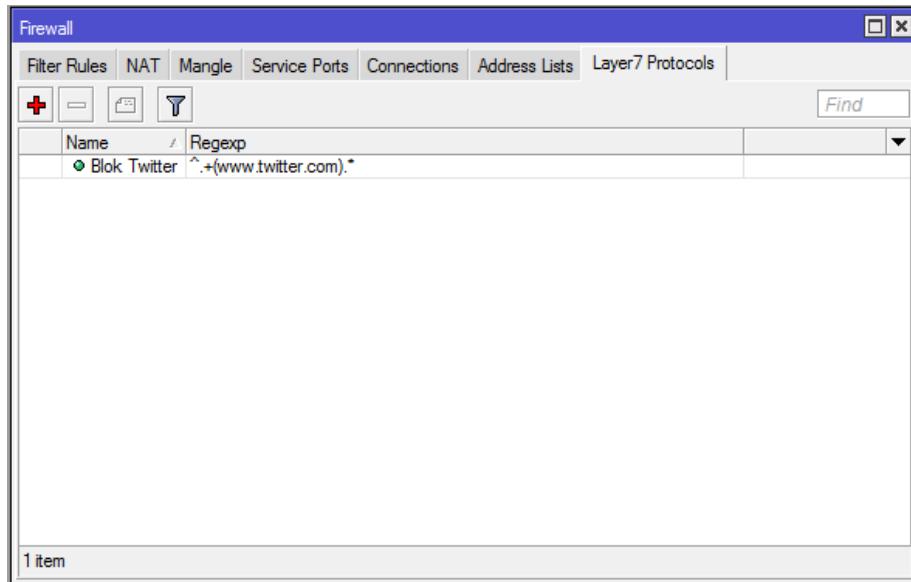
Oke daripada bingung langsung aja kekonfigurasinya. Yang pertama harus dilakukan adalah kita membuat rule Layer 7 Protocolnya , Caranya adalah klik menu IP > Firewall > Layer 7 Protocol > Add



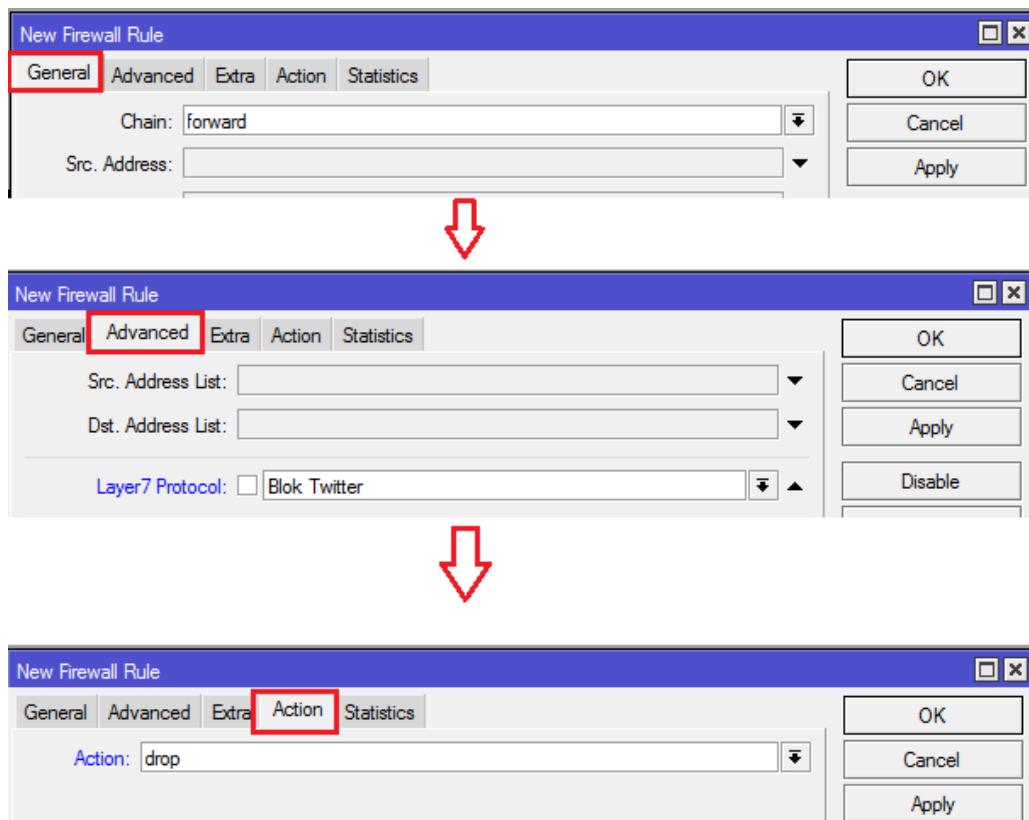
Kemudian kita buat rule nya , disini saya mau ngeblok Situs Twitter , lalu di regexp kita buat syntak seperti ini ^.+(www.namasitus.com).^* , bisa dilihat sesuai contoh



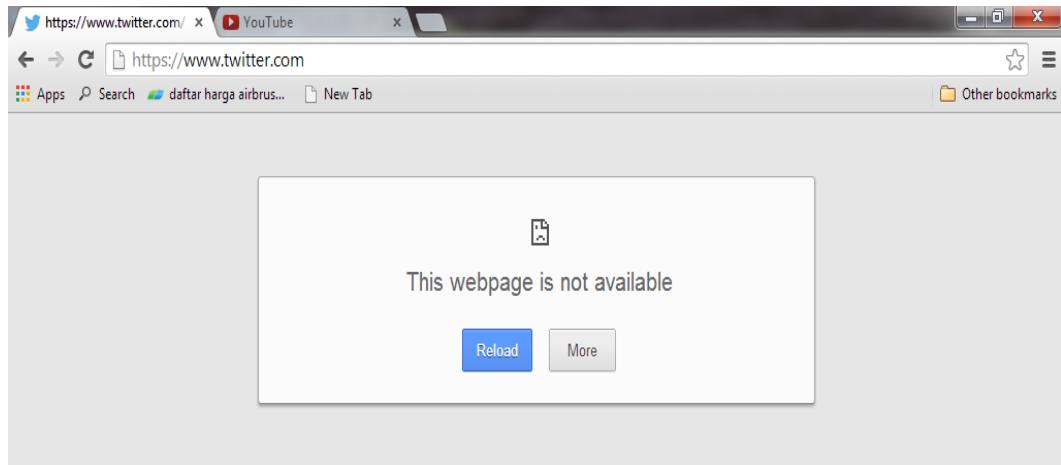
Setelah itu klik Apply lalu oke , kemudian hasilnya akan terlihat di bagian menu layer 7 protocol itu.



Selanjutnya kita buat rule untuk memblokir berdasarkan Layer 7. Tentunya di Firewall Filter Rule. Kemudian kita buat rule nya seperti ini , masukkan layer 7 protocol yang tadi dibuat di bagian **Advanced**.



Setelah itu apply dan oke , selanjutnya kita coba buka situs yang tadi diblokir, maka hasilnya adalah Seperti ini , tidak akan berhasil dibuka , atau hanya akan berputar putar (loading terus menerus)



Oke karena sudah berhasil , saya sudahi dulu lab kali ini.

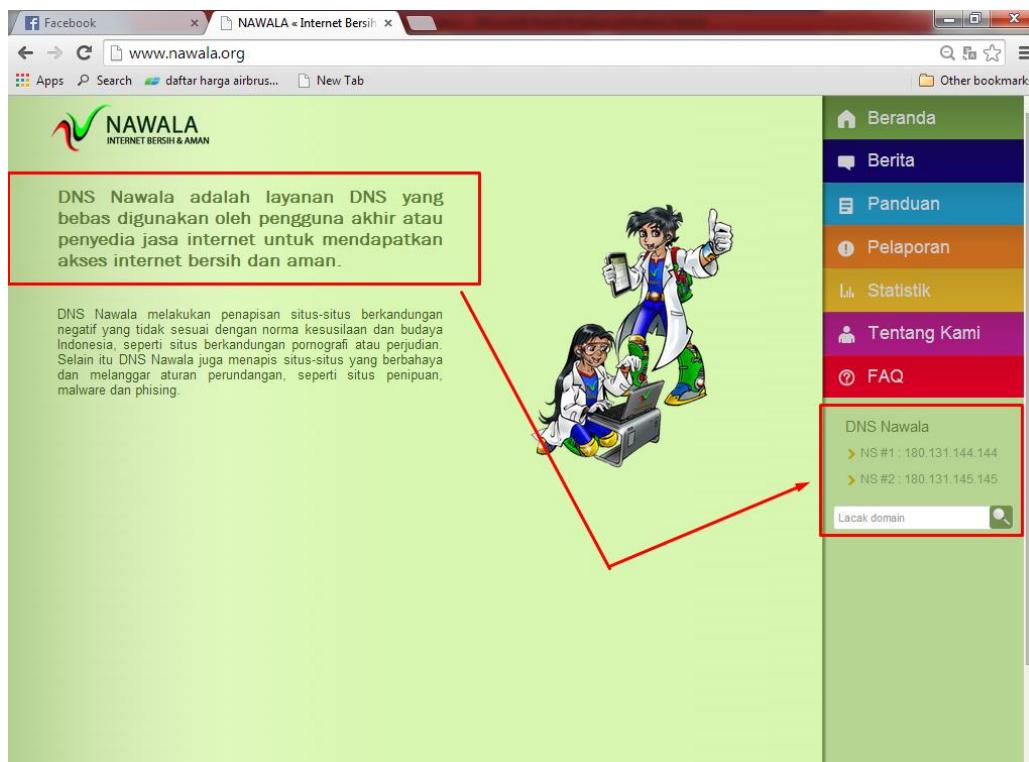
Kurang lebih nya mohon maaf,

Wassalamualaikum wr.wb !

Lab 32. Blok Situs Porno dengan DNS Nawala

Assalamualikum wr.wb

Setelah berbagai cara memblok situs sekarang kita masuk lagi ke materi yang bisa dibilang mungkin saangaaat bermanfaat , yaitu memblok situs **porn*** , sebenarnya kita bisa saja memblok situs porno melalui cara cara sebelumnya hanya saja kurang efektif karena kita harus mengetahui dahulu IP atau nama website situs tidak baik ini. Nah disini saya mau ngasih tau cara simple buat blok situs porno yaitu dengan menggunakan DNS nawala , buat yang belum tau apa itu DNS nawala nih saya kasih SS an nya , sekalian diliat **IP dari DNS Nawala**. Karena nantinya kita akan mengubah DNS di Router menjadi DNS Nawala ini.

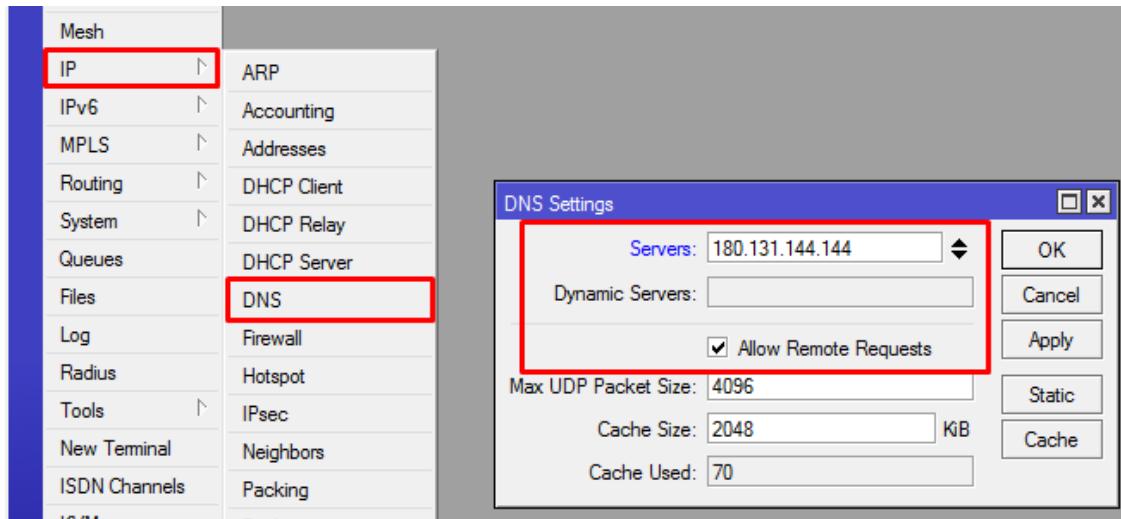


Kalo yang IP nya gak kebaca saya kasih tau aja yaaa ,

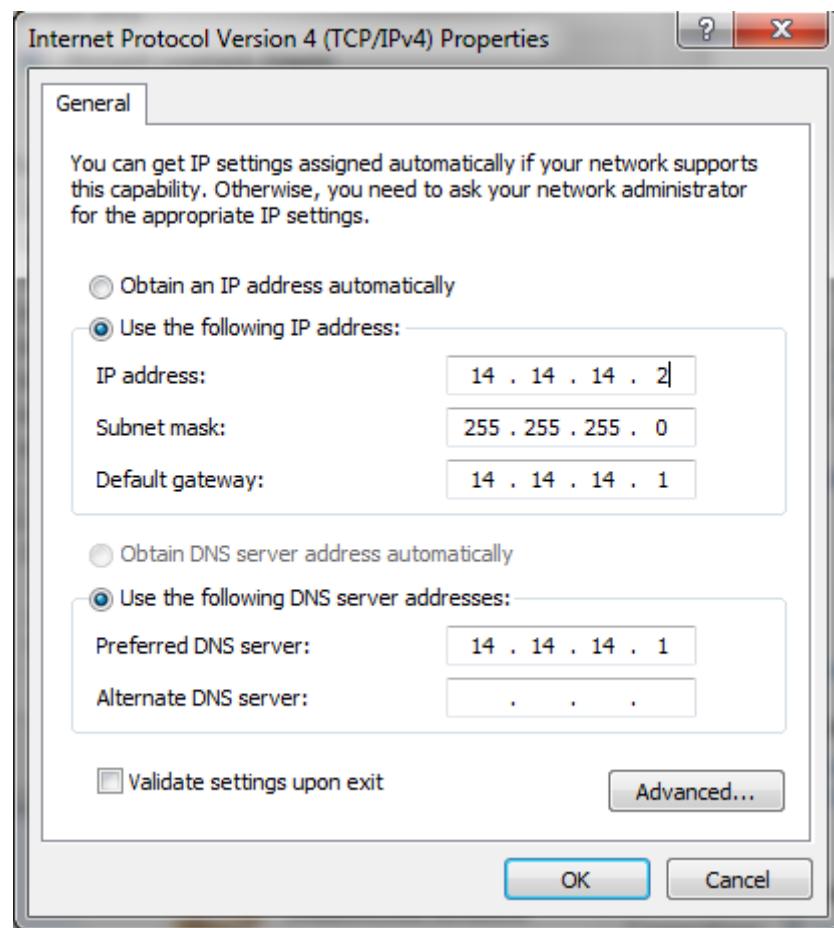
DNS NAWALA :

NS 1 : 180.131.144.144
NS 2 : 180.131.145.145

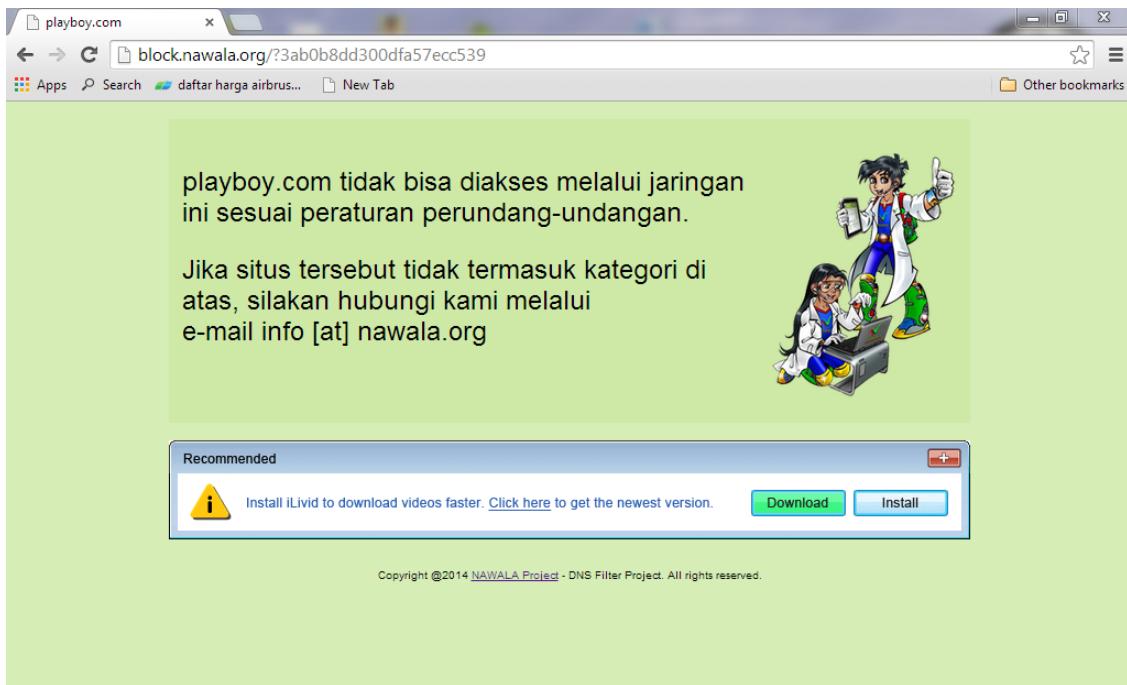
Oke langsung aja kekonfigurasinya , seperti yang saya bilang sebelumnya bahwa konsepnya adalah kita akan mengatur DNS dari Router menjadi DNS Nawala ini. Caranya sama seperti di Lab koneksi internet sebelumnya , Pertama kita klik menu **IP** > **DNS** kemudian ubah menjadi **IP DNS Nawala**



Setelah itu dibagian client kita bisa gunakan IP dari DNS nawala atau IP dari ether Routerboard itu sendiri, hasilnya akan sama saja.



Selanjutnya silahkan buka situs porn* apa saja , sebagai contoh saya buka situs www.playboy.com , maka hasilnya akan situs tersebut tidak bisa dibuka dan akan muncul tampilan berikut



Oke karena situs porno nya tidak bisa dibuka , itu artinya lab kita sudah berhasil.
Dan karena sudah berhasil saatnya saya untuk bilang "**Alhamdulillah , akhirnya
situs itu terblokir ☺**"

Oke sekian dulu ya mas dan mba broo

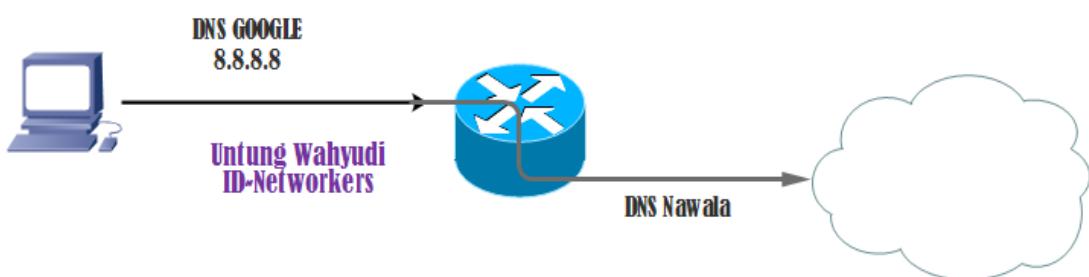
Wassalam !

Lab 33. Transparent DNS Nawala

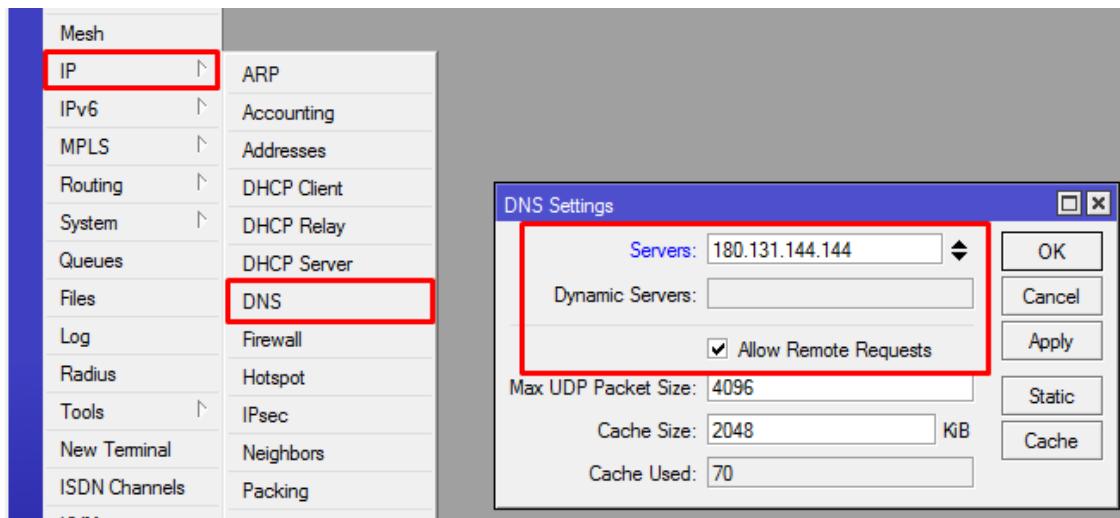
Assalamualaikum wr.wb

Masih melanjutkan dari Lab sebelumnya , saya mau kasih bocoran nih , ternyata lab sebelumnya itu masih memiliki kekurangan. Apa kekurangannya ??
Jadi jika client mengganti DNS nya menjadi DNS Google atau DNS lain yang bukan DNS Nawala maka hasilnya client tetap dapat membuka situs porn* tersebut. Nah Ihooooo bahayaa kan. Lalu gimana cara menangkalnya ?

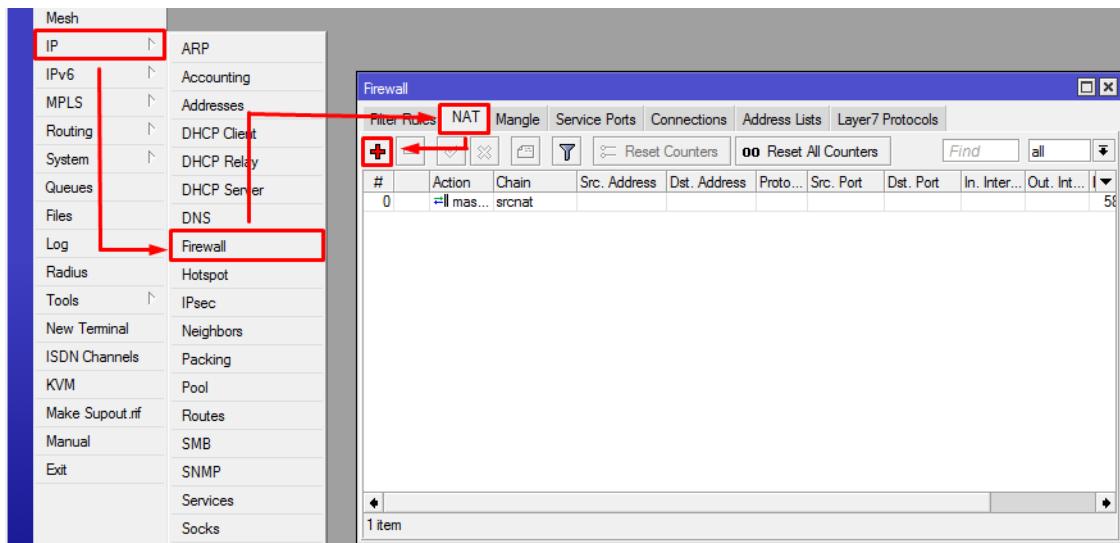
Nah untuk alasan itu lah saya buat Lab ini. Jadi di Lab ini saya bakal buat Transparent DNS , artinya kita akan memaksa client untuk memakai DNS Nawala ini , walaupun dia mencoba ganti ke DNS google tetap saja seolah olah dia menggunakan DNS nawala ini. Penasaran ?? Langsung aja yuuk cuuuus.



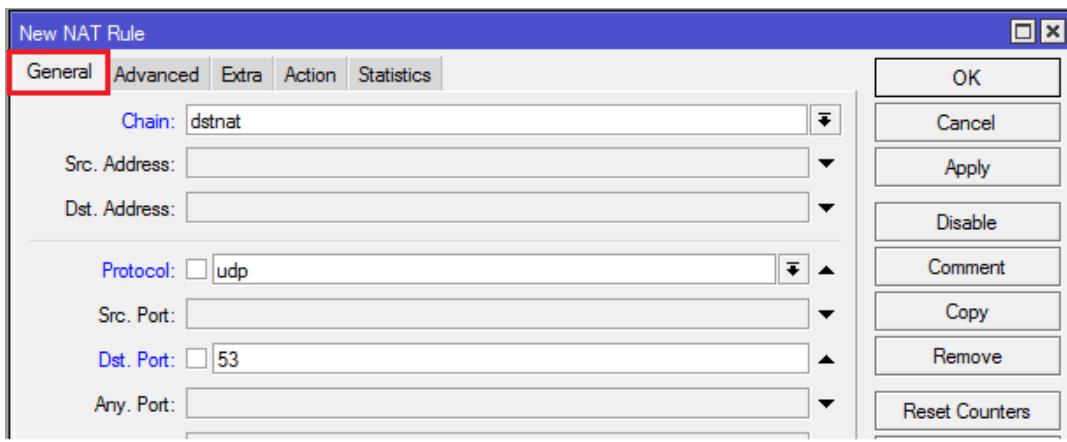
Pertama pastikan kita sudah mengatur DNS Router menjadi DNS Nawala



Setelah itu kita masuk ke menu Firewall NAT , dengan cara klik menu IP > Firewall NAT > Add

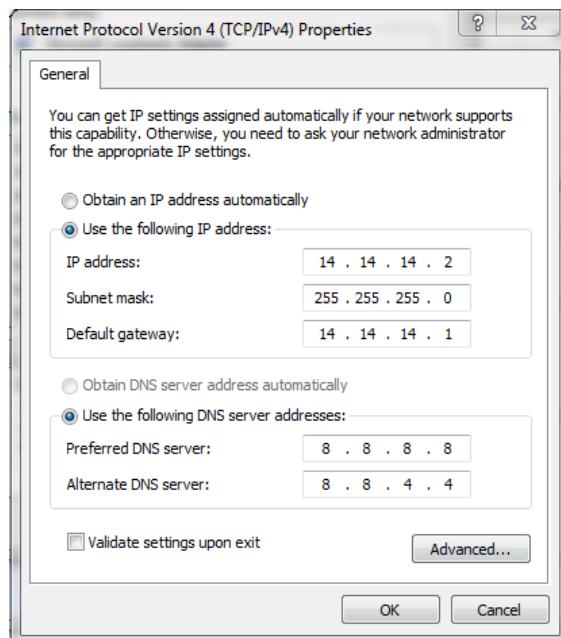


Setelah itu kita buat rule dengan **chain=dstnat** , **protocol=udp** , **port=53** , kemudian di tab **action** kita pilih **action=redirect** , **to-port=53**. (*Keterangan : Port 53 adalah Port DNS*)



Maksud dari perintah diatas adalah , kita akan me-redirect atau mengarahkan segala jenis DNS (port 53) menuju DNS yang digunakan oleh Router.

Selanjutnya silahkan ganti DNS di client menjadi DNS google , lalu buka situs playboy.com , maka hasilnya akan sama , yaitu tidak bisa dibuka





Oke ternyata sama sama gak bisa dibuka meskipun client udah ganti DNS. Oke mas broo sekian dulu yaa lab kali ini

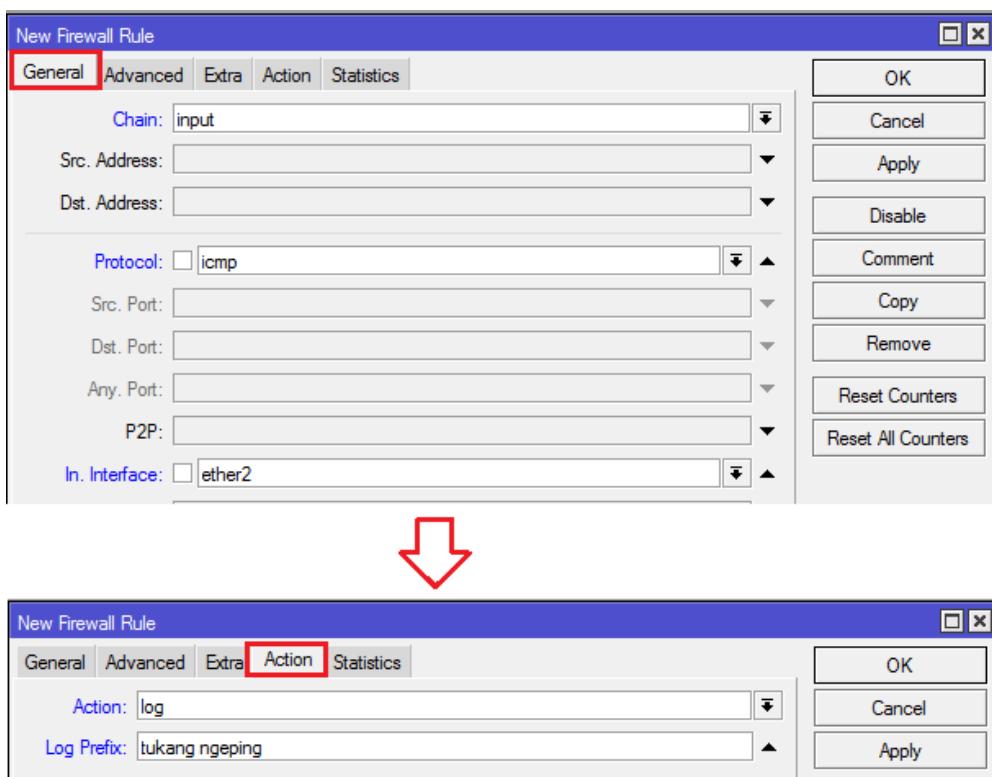
Wassalam !

Lab 34. Firewall Logging

Assalamualaikum wr.wb

Setelah bosen berurusan sama masalah blokar blokir situs sekarang refreshing dulu sedikit. Di lab ini saya mau ngebahas masalah Firewall Logging. Jadi firewall Logging ini salah satu fitur mikrotik yang digunakan untuk mencatat aktifitas jaringan yang dilakukan router. Jadi kita hanya perlu memilih kegiatan apa yang akan kita masukkan ke Logging (catatan) nantinya.

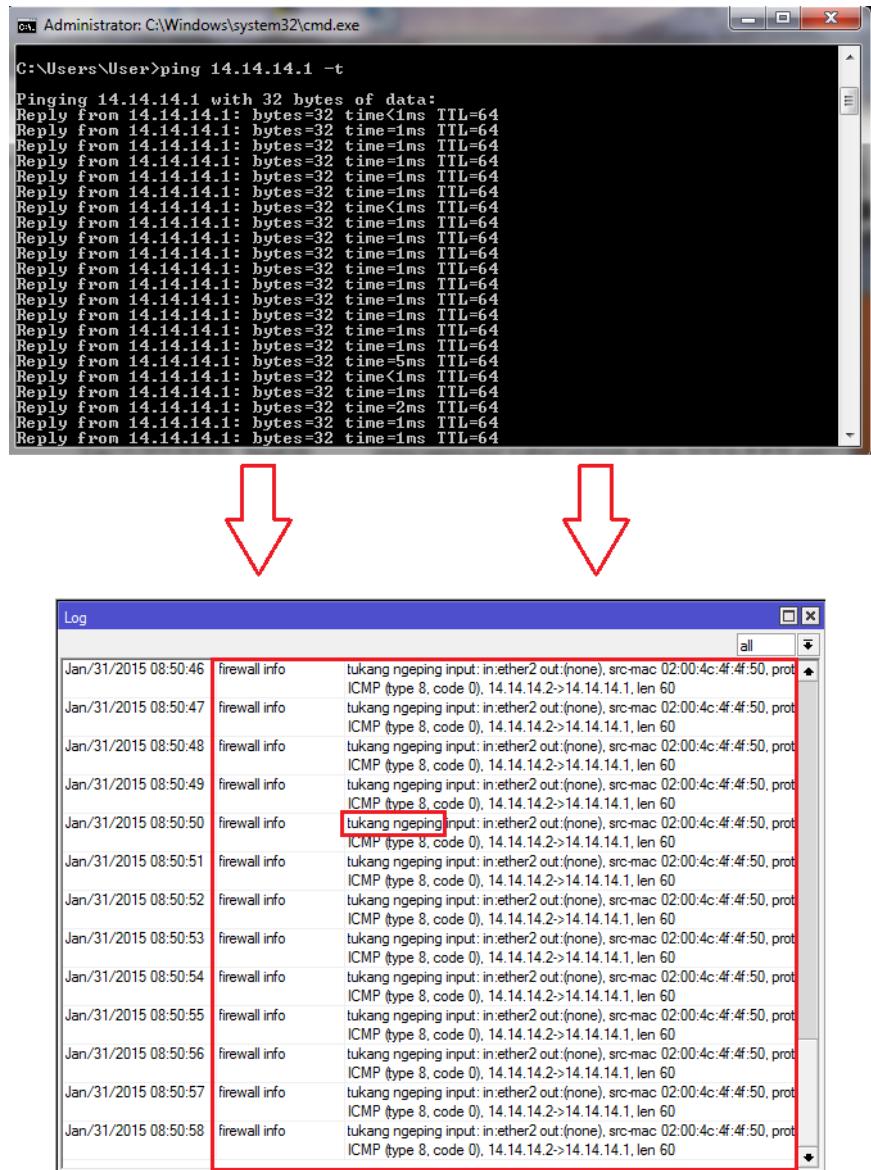
Oke langsung aja , sebagai contoh saya mau mencatat kegiatan **Ping** yang masuk kedalam Router melalui ether2. Pertama klik menu **IP > Firewall > Filter Rules > Add** , kemudian buat rule seperti dibawah ini



Keterangan :

Dibagian protocol saya pilih **ICMP** , karena ingin mencatat kegiatan **PING** Lalu dibagian action kita pilih **log** , dibagian **log prefix** adalah sebutan atau nama yang akan masuk di log nantinya

Setelah itu silahkan coba ping dari client ke Router , maka hasilnya akan di catat di log. Seperti gambar dibawah ini



Oke karena sudah tercatat itu artinya sudah berhasil.

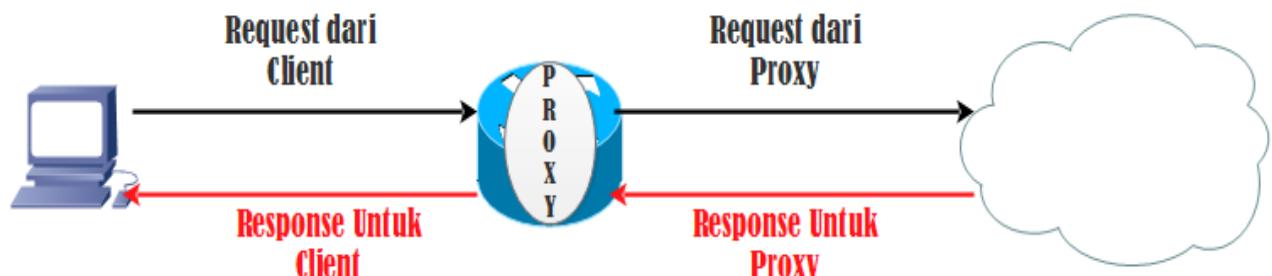
Sekian dulu yoo

Wassalam !

Web Proxy

Alhamdulillah sekarang udah masuk ke materi Proxy. Apa itu proxy ???
Proxy adalah suatu aplikasi yang menjadikan perantara antar client dengan server (website) , sehingga nantinya client tidak berhubungan secara langsung dengan server server yang ada diinternet. Proxy akan membuat request dari client ke web server di internet menjadi atas permintaan dari Proxy Server. Sehingga website akan mengetahui bahwa yang mengakses adalah Proxy Server dan bukannya dari client. Jadi website akan memberikan response nya kepada Proxy , dan bukannya ke client. Barulah nanti akan diteruskan oleh proxy ke client. Untuk lebih paham monggo disimak gambar nya

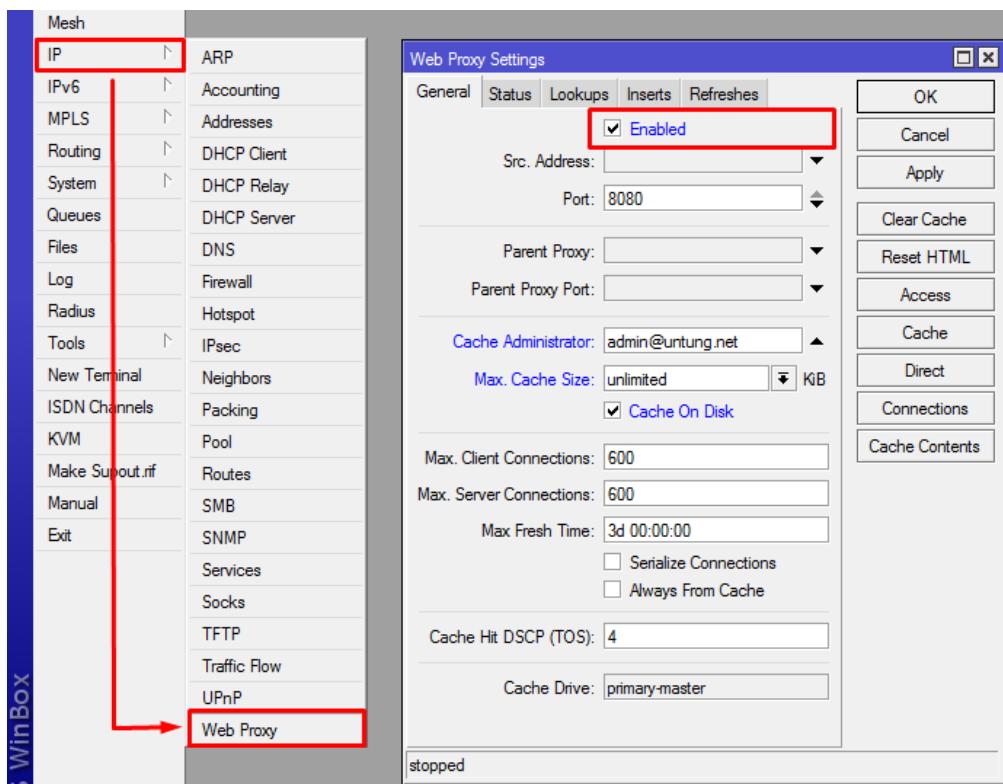
Untung Wahyudi
ID-Networkers



Lab 35. Mengaktifkan Web Proxy

Assalamualaikum wr.wb

Langsung aja ke pembahasan pertama yaitu cara mengaktifkan Web Proxy di Mikrotik , caranya adalah klik menu **IP > Web Proxy** , kemudian klik bagian enable dan isi seperti dibawah ini



Keterangan :

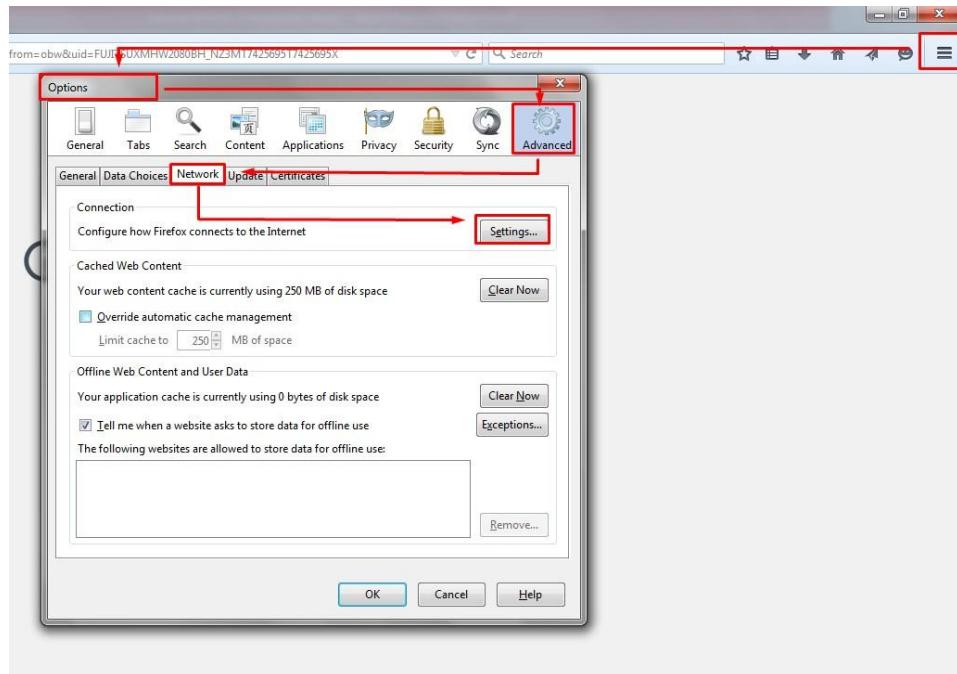
Port : Port yang akan digunakan Proxy

Cache Administrator : Admin yang bertanggung jawab , isikan saja email anda

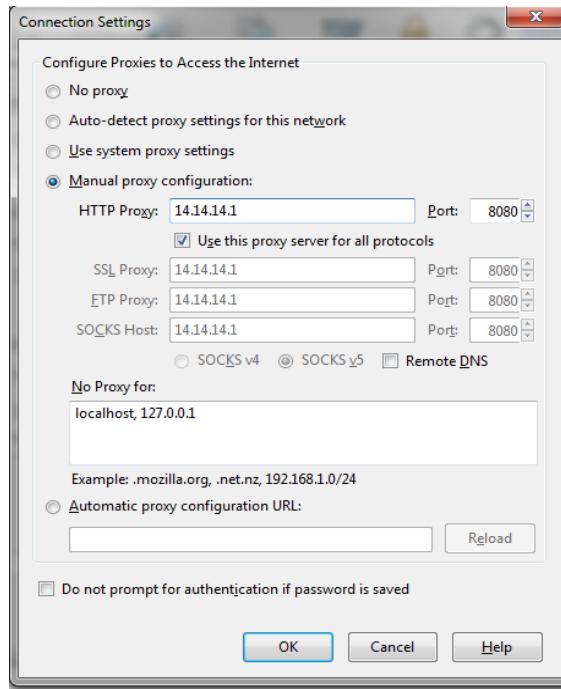
Max.Cache Size : Menentukan ukuran hardisk router yang akan digunakan untuk menyimpan cache

Cache-on-Disk : bila kita pilih **yes** maka **Penyimpanan Cache** akan disimpan di **Harddisk** , sedangkan bila kita pilih **No** , maka cache akan disimpan di **RAM**

Dengan begitu maka Proxy kita sudah diaktifkan , sekarang tinggal aktifkan Proxy di Web Browser client. Pasti udah pada tau doong caranya. Disini saya pake browser Mozilla , caranya Klik bagian pojok kanan atas , tapi bukan tanda close lhoo , yaitu tanda open menu , kemudian pilih Option > Advanced > Setting ,



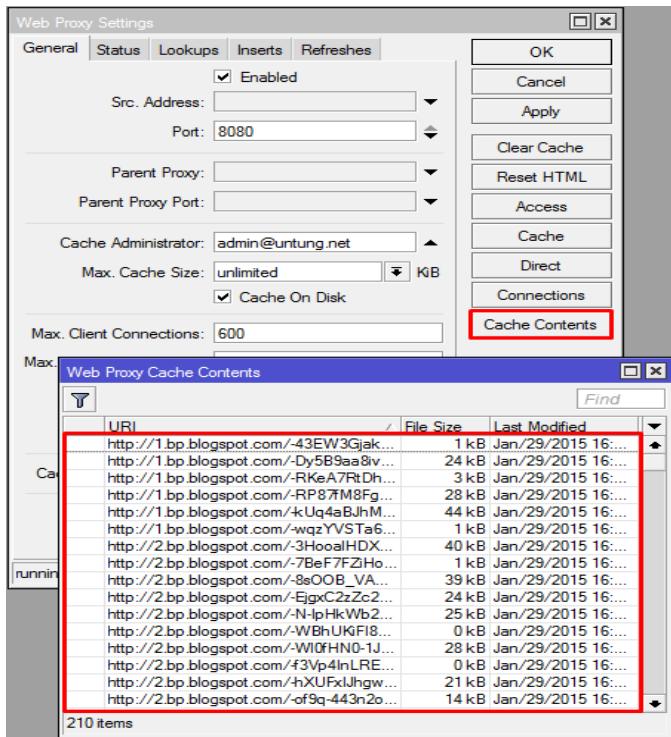
Kemudian kita arahkan proxy nya menuju IP Proxy kita , seperti gambar dibawah ini .



Kemudian silahkan lakukan aktifitas Browsing dari client , setiap kali client mengunjungi situs maka akan terlihat koneksi yang dilakukan oleh client kita. Untuk melihatnya klik saja menu **connection** di web proxy mikrotik

Src. Address	Dst. Address	Protocol	State	Tx Bytes	Rx Bytes
C 14.14.14.5	54.69.181.33	HTTP/1.1	rx body	3393 B	1169 B
C 14.14.14.5	31.13.90.2	HTTP/1.1	rx body	18.8 kB	3076 B
C 14.14.14.5	0.0.0	idle		3240.9 kB	6.0 kB
S 31.13.90.2	14.14.14.5	HTTP/1.1	rx body	2867 B	18.8 kB
S 54.69.181.33	14.14.14.5	HTTP/1.1	rx body	940 B	3374 B
S 117.102.125.139	0.0.0	idle		484 B	293.5 kB
S 202.169.45.240	54.149.1.51	HTTP/1.1	idle	2420 B	1467.3 kB

Kita juga bisa melihat situs yang pernah dikunjungi oleh client yang telah ter-cache di Web Proxy. Dengan cara klik bagian **Cache Contents**



Oke mas broo karena sudah ter-cache di Web Proxy , itu artinya sudah berhasil.
Untuk beberapa lab kedepan mungkin akan membahas tentang Web Proxy ini.
Jadi nikmatin yoo

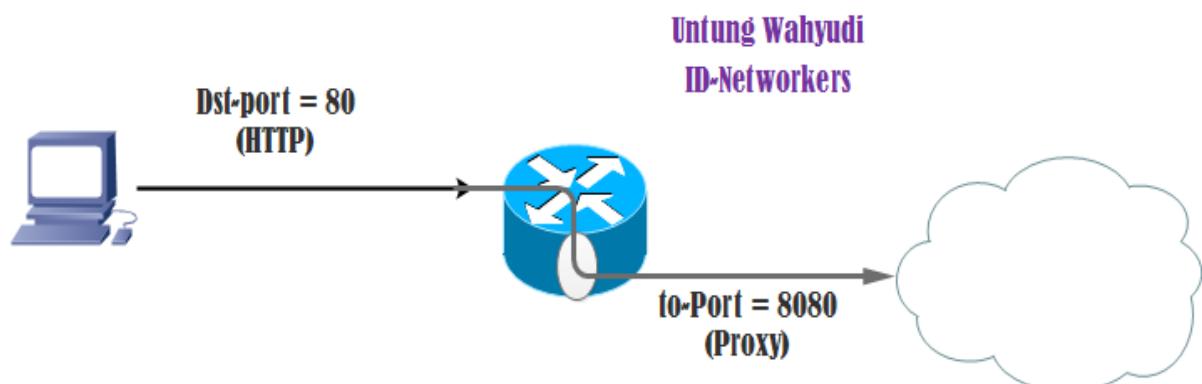
Oke sekian dulu
Wassalamualaikum wr.wb

Lab 36. Transparent Proxy

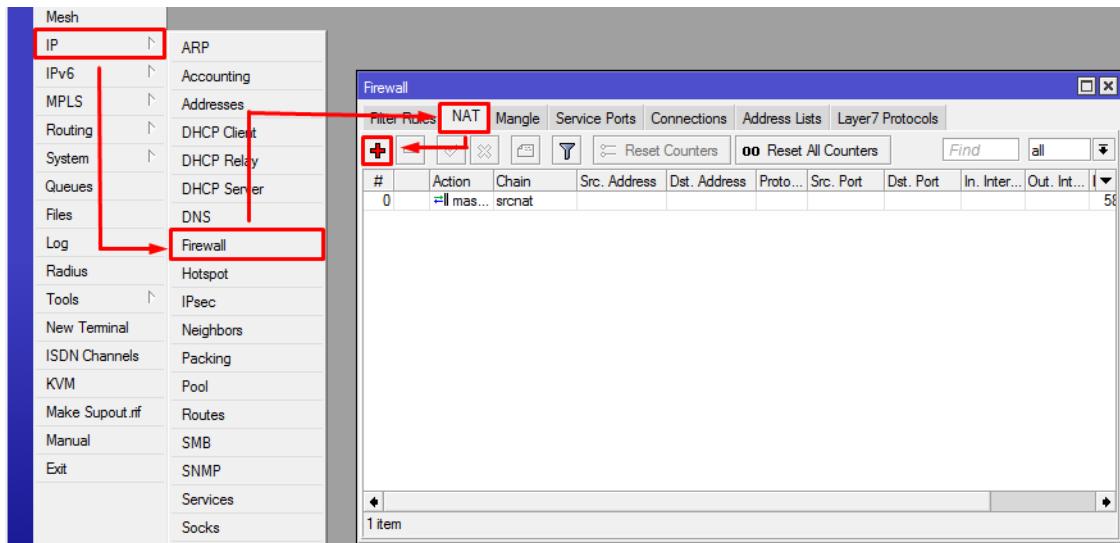
Assalamualaikum wr.wb

Setelah di lab sebelumnya kita sudah tau cara mengaktifkan web proxy baik dari sisi Router maupun dari sisi client , saatnya untuk mengevaluasi. Di Lab sebelumnya ada kekurangan yang sangat mendalam , apa itu ??

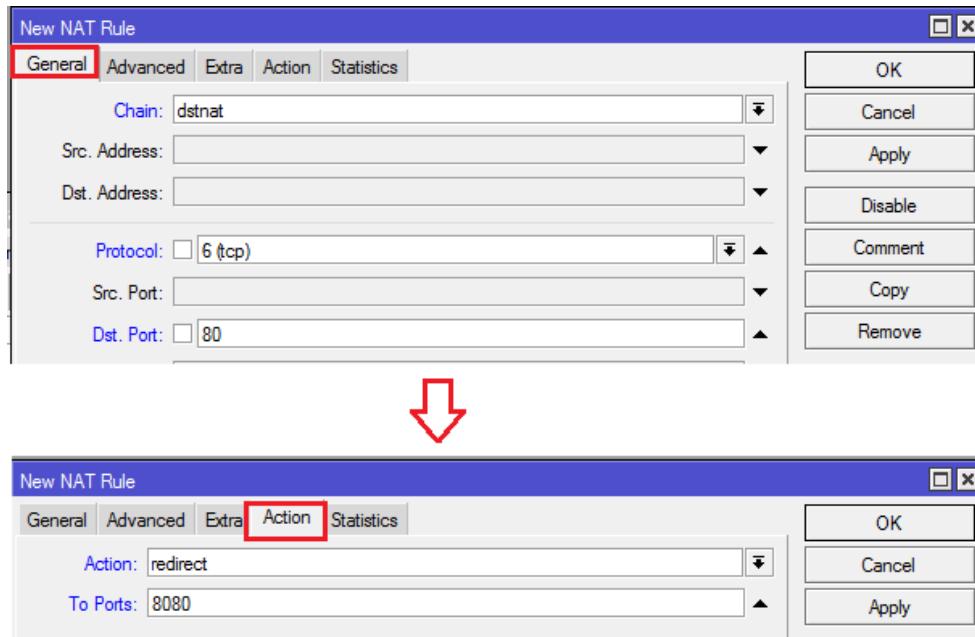
Yaitu kita harus setting manual di Web Browser client. Laah terus kalo ada 100 PC gimana ?? Kan jadi memakan waktu buat setting manual belom lagi kalo client gonta ganti IP Proxy yang gratisan dari internet. Nah untuk mengatasinya kita bisa menggunakan **Transparent Proxy**. Udah tau kan maksud dari Transparent. Kan udah saya jelaskan di lab DNS Nawala. Oke langsung aja yuu cuss



Untuk mengaktifkan transparent proxy caranya adalah klik menu IP > Firewall > NAT > Add



Kemudian buat rule seperti ini , dibagian general kita isi **action=dstnat** , **protocol=tcp** , **dst-port=80** , kemudian ditab **action** , kita pilih **action=redirect** , **to-port=8080**



Coba terjemahin artinya yuuk , jadi artinya kurang lebih begini

"Jika ada traffic HTTP (port 80) maka akan di redirect/diarahkan menuju Web Proxy (Port 8080)"

Selanjutnya client tidak perlu lagi konfigurasi IP Proxy di browser nya. Secara otomatis akan diarahkan ke Proxy Router kita.

Oke mas dan mba broo sekian dulu yaa

Wassalam !

Lab 37. Blok Situs menggunakan Proxy

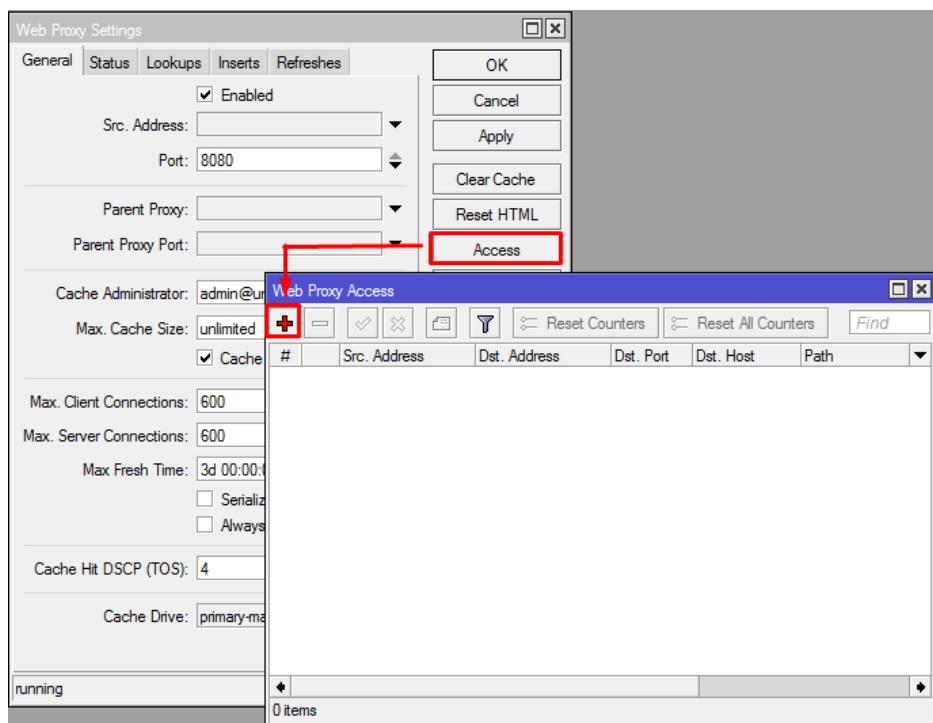
Assalamualaikum wr.wb

Ahaha ternyata materinya gak jauh jauh nih dari yang satu ini. Kita balik lagi ke materi blokir situs , namun ada bedanya yaitu menggunakan Web Proxy.

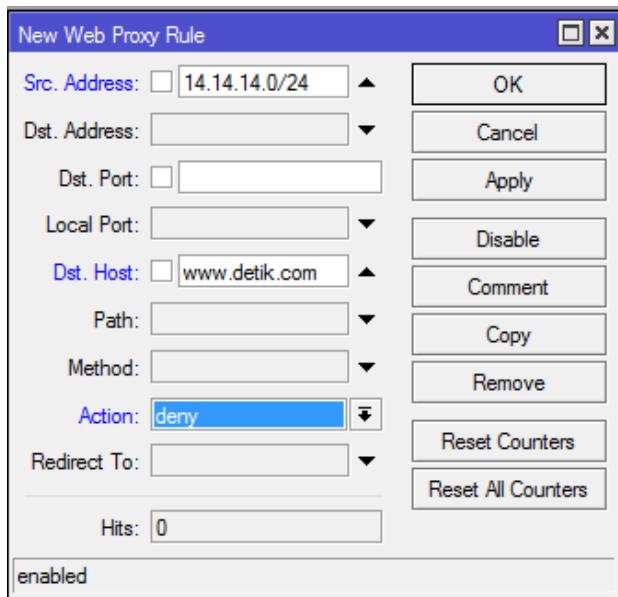
Diterangin sedikit yoo , jadi intinya ketika client ingin mengakses sebuah situs yang di blok di proxy maka request tersebut Cuma nyampe di proxy , tapi web proxy tidak meneruskan ke internet.

Oke langsung aja kekonfigurasinya

Pertama kita buka menu IP > Web Proxy , kemudian klik bagian Access , lalu kita klik tombol Add di menu Access tersebut



Setelah itu kita buat rule seperti gambar dibawah ini , masukkan src-address=IP Network Local kita , dst-host= situs yang ingin diblok , action=deny , Setelah itu apply dan OK.



Setelah selesai membuat rule , silahkan buka situs yang tadi diblok , sebagai contoh saya blok detik.com. Maka hasilnya adalah seperti berikut ini.



Dan hasilnya adalah situs tidak dapat dibuka , dan ada pemberitahuan bahwa situs itu terlarang dan di blok oleh administrator nya.

Oke karena sudah berhasil maka saya tutup dengan mengucap Alhamdulillah

Sekian dulu yaa

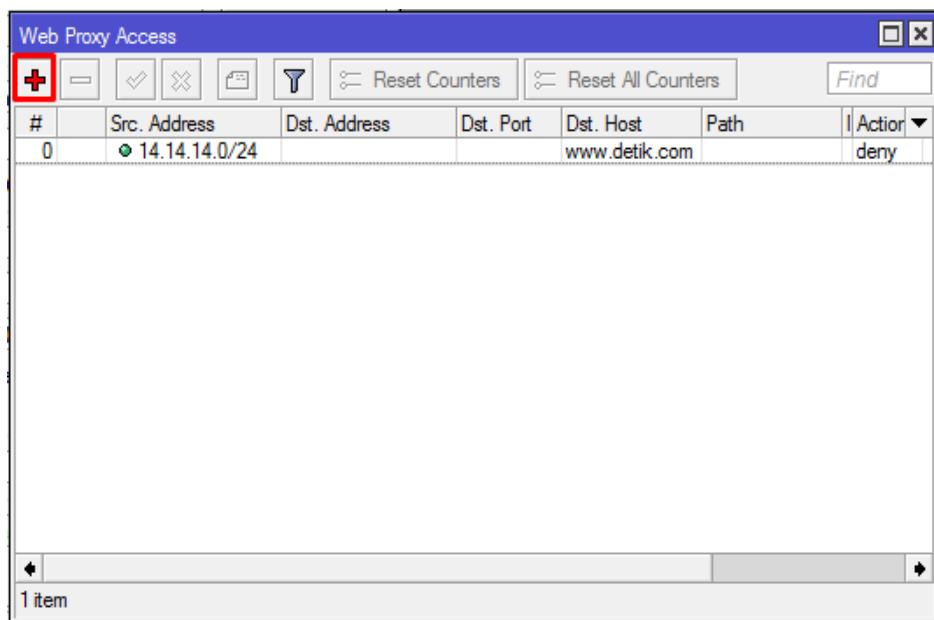
Wassalam !

Lab 38. Blok Situs di Proxy (Berdasarkan Kata)

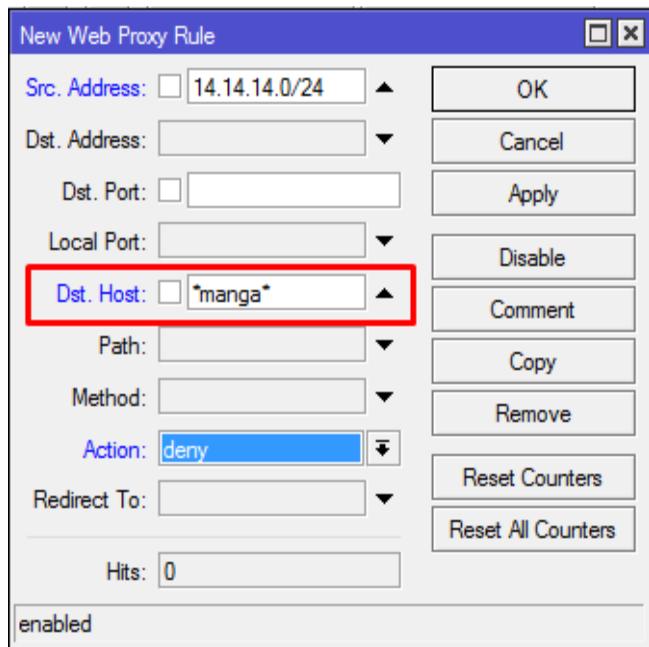
Assalamualaikum wr.wb

Melanjutkan dari lab sebelumnya , disini juga masih sama yaitu memblok situs dengan web proxy hanya saja ada yang berbeda. Kalo di lab sebelumnya kita memblokir berdasarkan URL atau alamat dari website di lab ini saya mau jelasin cara singkat memblokir situs. Misalnya kita ingin memblokir situs Porn* sedangkan kita gak tau alamat lengkap dari websitenya kita bisa gunakan cara ini. Jadi kita akan memblokir setiap website yang mengandung kata yang kita tentukan. Bingung ???

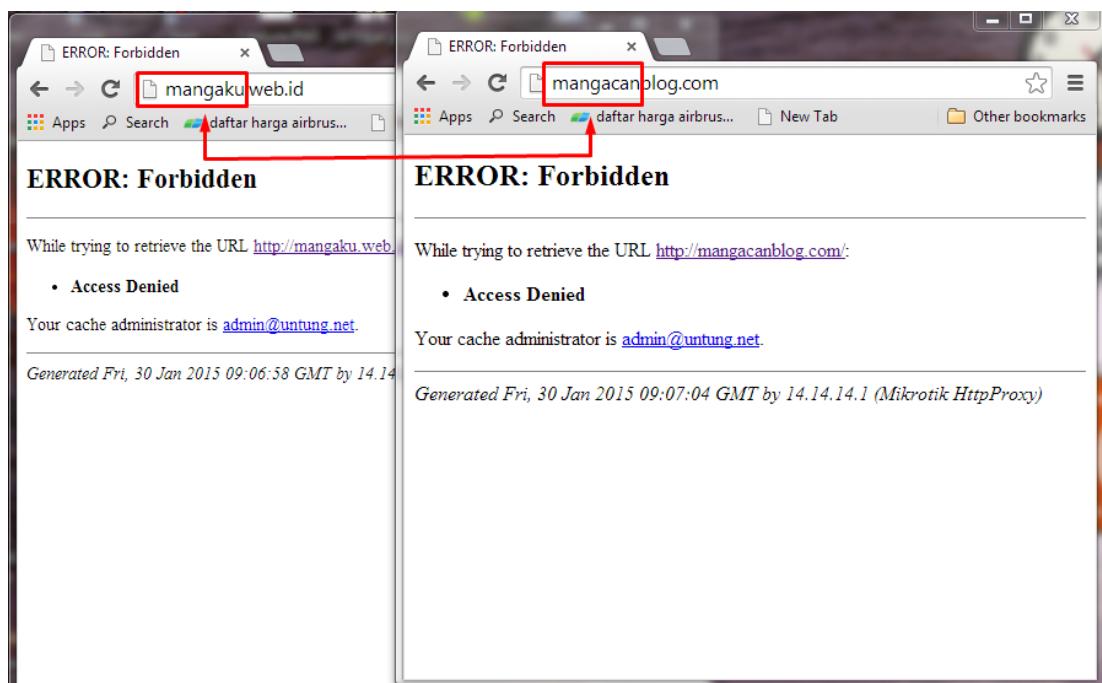
Langsung aja yuk , disini sebagai contoh saya mau blokir situs yang mengandung kata "**Manga**" , berikut caranya. Buka menu Access yang ada di Web Proxy , kemudian klik **Add**



Setelah itu tambahkan rule seperti dibawah ini, dibagian **dst-host** kita masukan kata ***KataYangInginDiblokir*** , sebagai contoh saya masukin ***manga***.



Selanjutnya apply dan OK. Kemudian silahkan buka situs yang mengandung kata tersebut. Sebagai bukti saya buka 2 situs yang mengandung kata Manga , maka hasilnya adalah sebagai berikut



Dan sudah terblokir. Kalo sudah tidak bisa dibuka artinya konfigurasi kita berhasil

Oke sekian dulu mas dan mba broo

Wassalam !

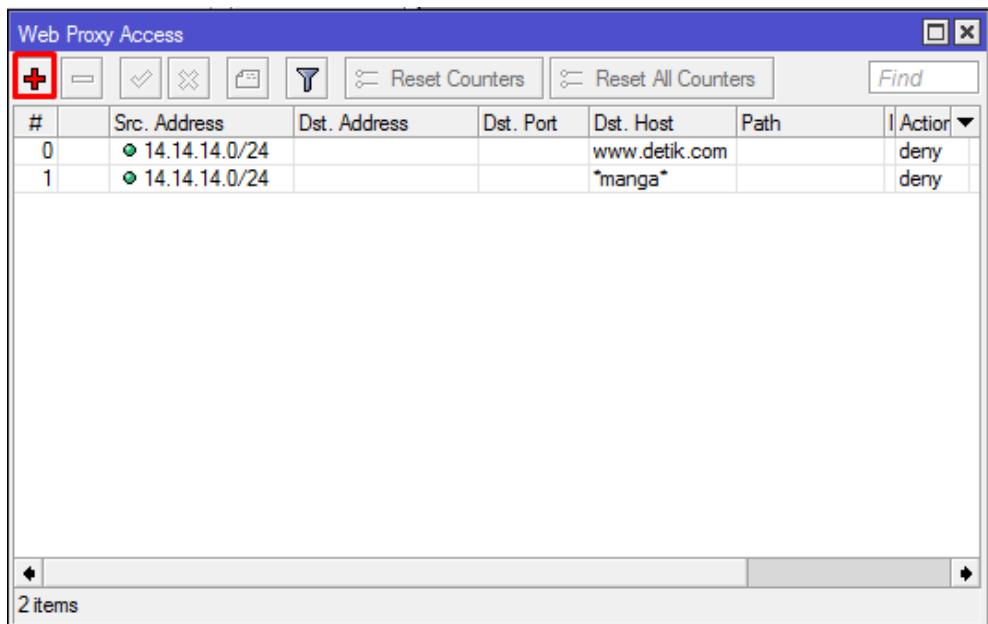
Lab 39. Blok File berdasarkan Ekstensi

Assalamualaikum wr.wb

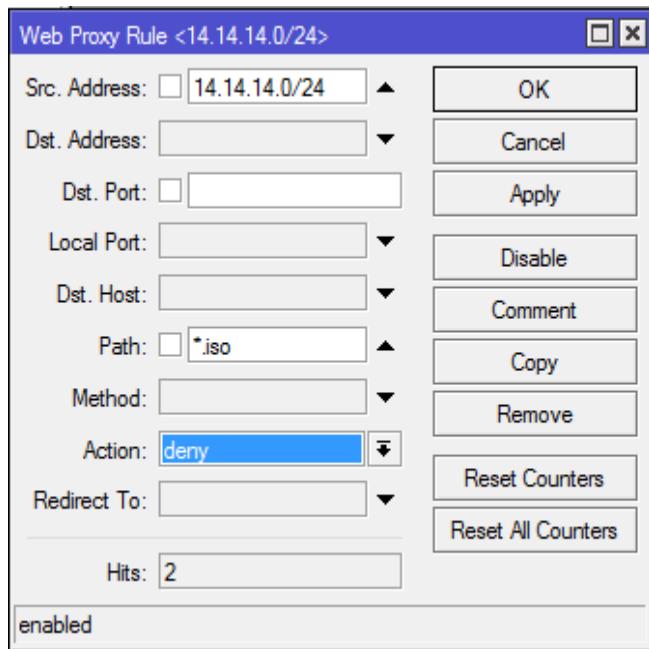
Masih kuat ???

Yuk lanjut lagi , masih seputar hal yang sama yaitu masalah blok sana blok sini. Setelah sebelumnya kita udah blok berdasarkan kata , sekarang kita akan memblok aktifitas **download** berdasarkan ekstensi di **proxy mikrotik**. Kan bahaya tuh kalo client main download download file yang kapasitasnya gede. Seperti contoh file dengan extensi .iso , rata rata pasti gede. Maka dari itu saya buat lab ini , tujuannya untuk mengatasi masalah diatas

Oke langsung aja tanpa basa basi kita ke konfigurasinya , pertama kita klik menu **Access** yang ada di **Web Proxy** , lalu klik **add**



Kemudian kita buat rule seperti ini , dibagian Path kita isikan ekstensi filenya, Ohya penulisan harus benar mas broo jadi begini **path=*.ekstensi** ingaat tanda bintang yoo. Sebagai contoh **path=*.iso**



Setelah pembuatan rule itu , kita klik Apply lalu OK. Setelah itu coba kita download file yang ber-ekstensi .iso , maka hasilnya akan seperti ini

ERROR: Forbidden

While trying to retrieve the URL <http://download2.mikrotik.com/routeros/5.26/mikrotik-5.26.iso>:

- Access Denied

Your cache administrator is admin@untung.net.

Generated Fri, 30 Jan 2015 09:40:09 GMT by 14.14.14.1 (Mikrotik HttpProxy)

OKE ternyata sudah berhasil di blokir , ingat yaa mas broo bijaklah dalam membuat rule . Sesuaikan dengan kebutuhan masing-masing

Oke sekian dulu

Wassalam !

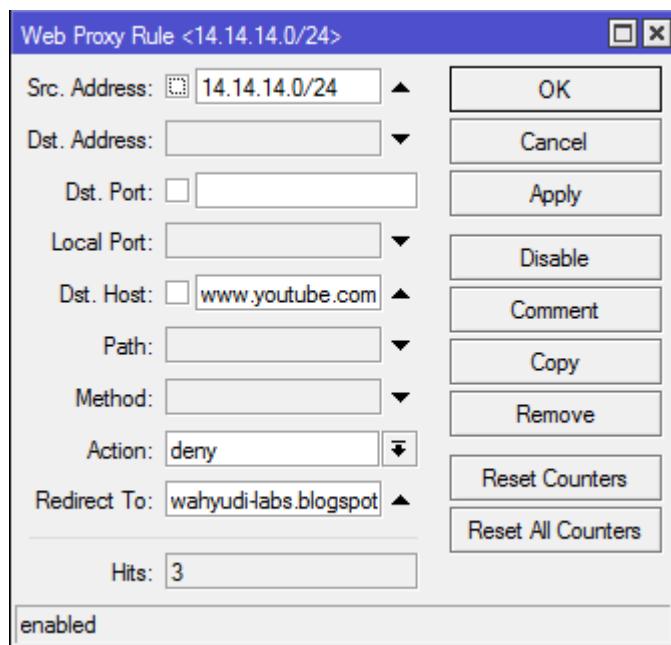
Lab 40. Me-Redirect sebuah Website

Assalamualaikum wr.wb

Udah ah capek blok blok situsnya , kalo gak suka sama situs itu jangan asal maen blok laah , gak baik. Pake cara lain aja , yaitu cara Redirect. Jadi ketika client mengakses suatu website nantinya akan di arahkan (redirect) ke website lain. Asiik kan ??

Langsung aja yuk , disini saya mau meredirect traffic ke **youtube.com** menjadi **ke wahyudi-labs.blogspot.com**. Sekalian ajang promosi blog ^_^. Oke tanpa basa basi langsung aja , di bagian Proxy Access kita buat rule seperti dibawah ini.

Di bagian **dst-host**:isikan situs yang akan diredirect, **action=deny** , lalu **Redirect To** : kita ubah menjadi tujuannya.



Kemudian Apply dan OK. Selanjutnya silahkan coba buka situs yang diredirect tersebut. Yaitu situs **www.youtube.com** dan hasilnya adalah akan teredirect ke **wahyudi-labs.blogspot.com**

The screenshot shows a web browser window with the title bar "Network Lab". The address bar displays "wahyudi-labs.blogspot.com". Below the address bar, there are links for "Apps", "Search", "daftar harga airbus...", and "New Tab". On the right side of the browser, there are icons for "Other bookmarks", "RSS", "Twitter", "Facebook", and "Email".

The main content area of the browser shows a blog post titled "[Lab 5] Basic Manajemen User" by Untung Wahyudi. The post has a timestamp of "On 23.17" and categories "Manajemen User, Mikrotik, MTCNA, TKJ". It includes a comment icon with "No comments".

The post content starts with "Assalamualaikum wr.wb Ketemu lagi dengan ane , dalam acara "bincang pagi tak bermutu". Oke Jadi di perbincangan ini ane mau ngebahas sedikit tentang Manajemen User di Mikrotik. Kalo kalian udah baca postingan ane tentang manajemen User di Linux pasti kalian akan mudah memahami postingan ini. Soalnya..." and ends with a "Read More" link.

To the right of the post, there is a sidebar with a "Search" section containing a search bar labeled "Search this site...". Below the search bar, there are two recommended posts: "Mampir Juga ke Blog Teman Saya" by Alfa Farhan and "NightLabs" by NightLabs.

Dan taaraaa telah berhasil ter-redirect. Itu tandanya kita sudah berhasil membuat rule yang benar.

Oke sekian dulu ya mas broo

Wassalam !

Lab 41. Routing Static

Assalamualaikum wr.wb

Setelah selesai dengan materi Proxy , saatnya masuk ke tahap lebih lanjut , ciaelaah gayaa kan. Di Lab ini saya mau ngebahas masalah Routing???. Apa itu routing ??

Buat yang belum tau , routing itu sebuah teknik yang digunakan untuk menghubungkan beberapa jaringan yang memiliki Network yang berbeda. Pahaam?? . Kalo belom paham disimak aja dulu lab ini , InshaAllah setelah ini pasti , makin gak ngerti hehehe.

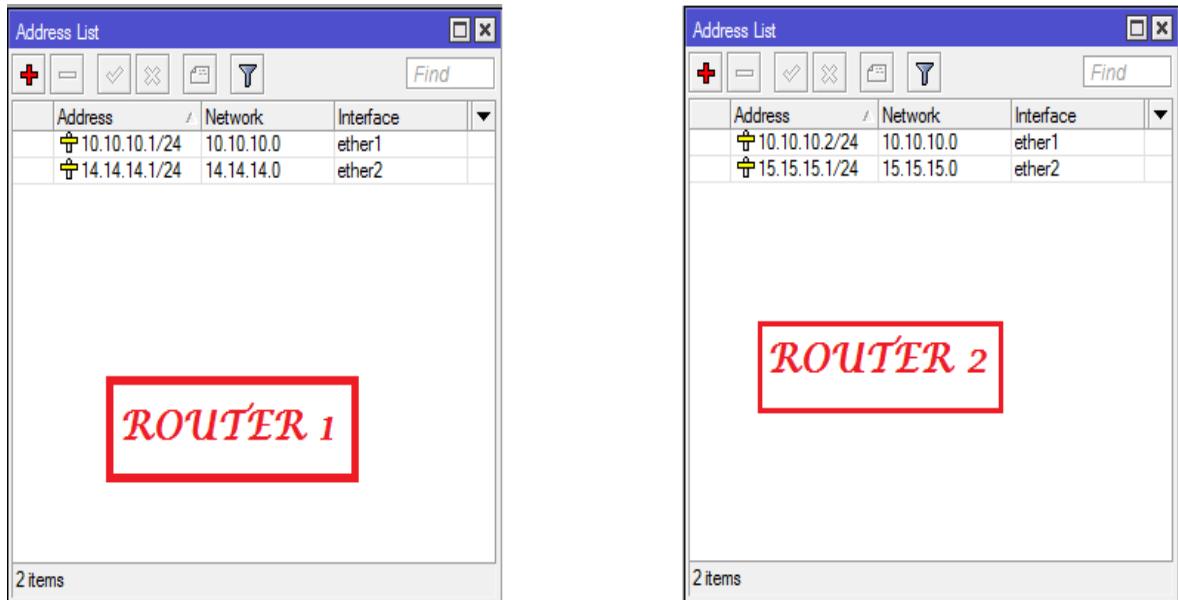
Oke jadi di lab ini saya mau ngebahas salah satu jenis dari Routing , yaitu Routing Static. Jadi routing static ini adalah proses routing yang dilakukan secara manual. Maksudnya manual , kita sebagai admin harus mengetahui betul tujuan dan jalur yang dilewati paket.

OM Rendra Towidjojo (Pengarang Buku Mikrotik Kungfu Kitab) , Berkata :

Prinsip dari Routing Static adalah **"Mau Kemana ?"** dan **"Lewat Mana ?"**. Dengan berpatokan dengan prinsip itu maka akan mudah untuk kita melakukan konfigurasi nantinya.

Oke langsung aja ke langkah konfigurasinya. Topologi nya kurang lebih begini. Saya pengen semua network bisa saling komunikasi , Network 14.14.14.0/24 bisa terhubung dengan Network 15.15.15.0/24.

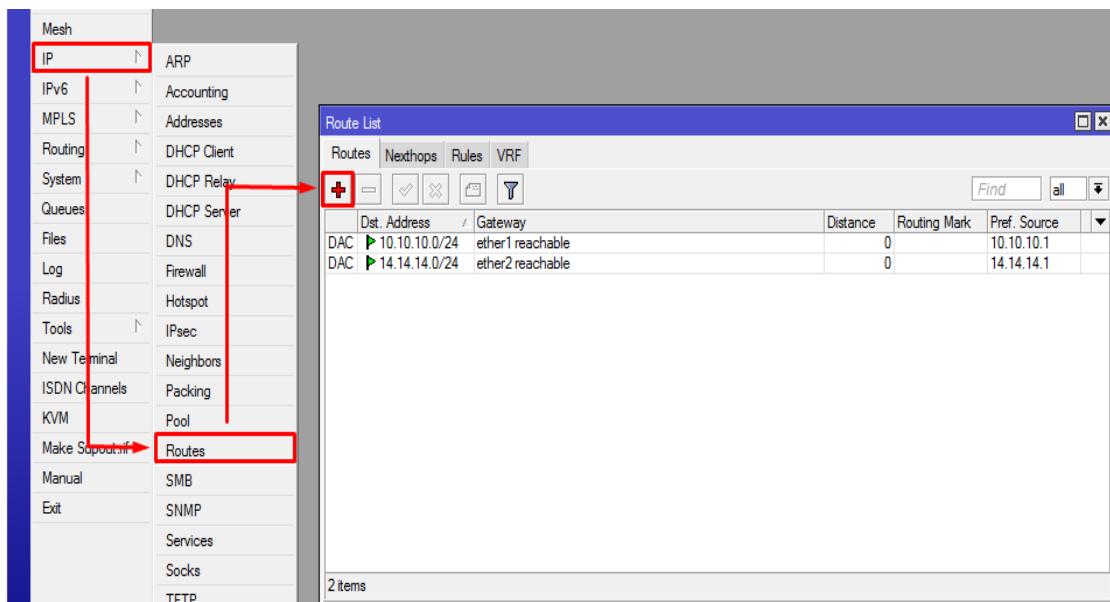
Oke langsung aja ke konfigurasinya , Saya gak ngebahas mulai dari cara menambahkan IP , disini saya langsung ke proses routing nya. Bisa dilihat IP address dari Router 1 dan Router 2



Selanjutnya kita akan mulai mengkonfigurasikan Routing Staticnya

Pada Router 1 :

Pertama kita klik menu IP > Routes > Add

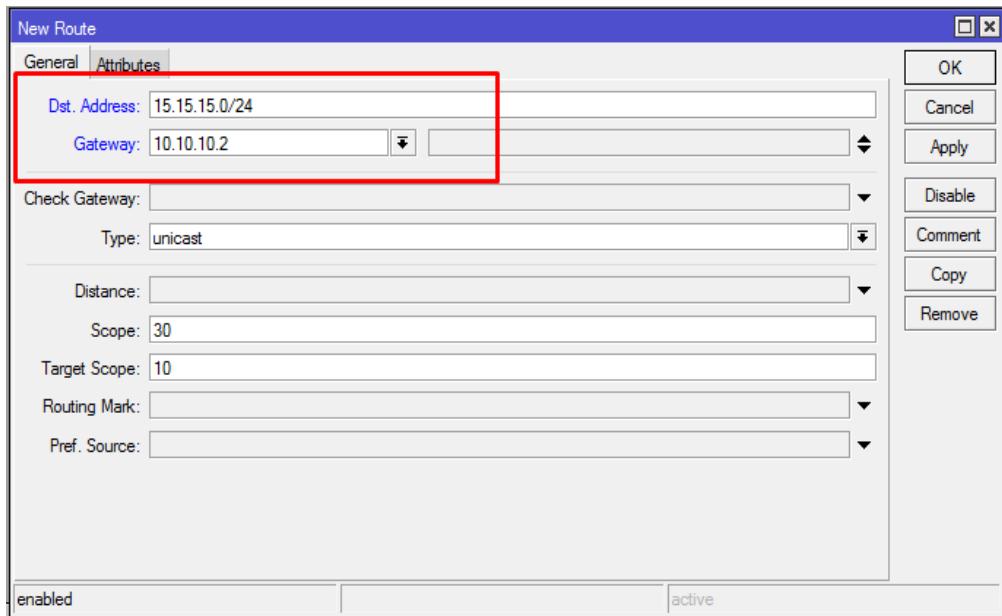


Kemudian tambahkan rule seperti gambar dibawah ini , Kita akan mendaftarkan

network 15.15.15.0/24 dengan gateway 10.10.10.2 , karena IP 10.10.10.2 lah yang terhubung langsung dengan network 15.15.15.0/24 .

Dst-Address = Tujuannya

Gateway = Jalur yang dilewati

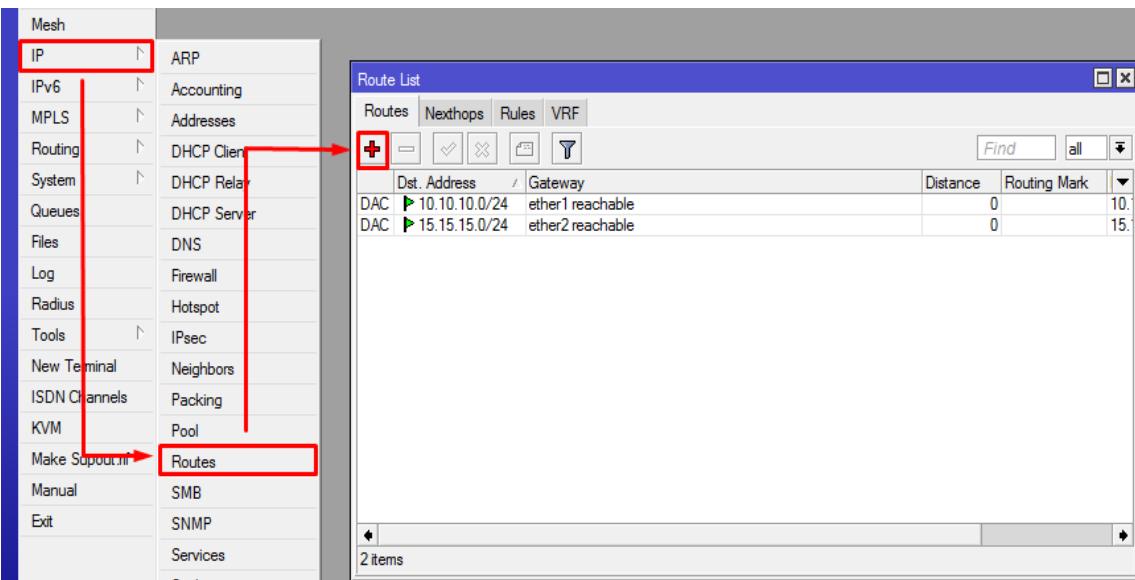


Jika sudah maka akan terbentuk tabel Routing yang mendaftarkan network 15.15.15.0/24. Yang bertanda "AS" artinya **Active Static**.

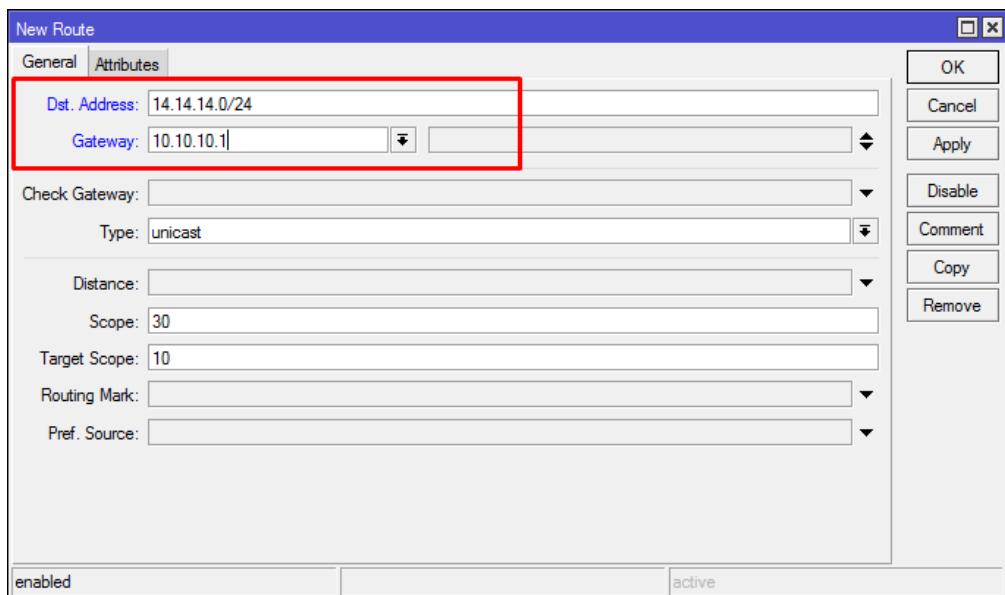
Route List					
	Routes	Nexthops	Rules	VRF	
	Find	all			
	Dst. Address	/	Gateway	Distance	Routing Mark
DAC	▶ 10.10.10.0/24		ether1 reachable	0	10.10.10.1
DAC	▶ 14.14.14.0/24		ether2 reachable	0	14.14.14.1
AS	▶ 15.15.15.0/24		10.10.10.2 reachable ether1	1	
3 items					

Pada Router 2 :

Sama halnya dengan router 1 , pertama kita klik **IP > Routes > Add**



Kemudian kita buat tabel routing nya , kita daftarkan Network 14.14.14.0/24 , dengan gateway 10.10.10.1



Setelah selesai maka akan muncul tabel Routing yang mendaftarkan network 14.14.14.0/24

Route List				
	Routes	Nexthops	Rules	VRF
			<input type="text" value="Find"/> all	
DAC	▶ 10.10.10.0/24	ether1 reachable	0	10.1
AS	▶ 14.14.14.0/24	10.10.10.1 reachable ether1	1	
DAC	▶ 15.15.15.0/24	ether2 reachable	0	15.1

3 items

Kemudian silahkan test ping antar client , kalo konfigurasinya bener maka hasilnya pasti berhasil.

Oke sekian dulu yaa pembahasan di Lab ini

Wassalam !

WIRELESS NETWORK

Lab 42. Membuat RouterBoard menjadi Access Point

Assalamualaikum wr.wb

Alhamdulillah sekarang kita sudah masuk materi Wireless , sebagai pembukaan di bab wireless ini saya mau buat lab yang istimewa , yaitu bagaimana cara membuat RouterBoard menjadi Access Point. *Emang harus ya dijadiin Access Point , kenapa gak pake kabel aja semua ??*. Kalo misalkan kita Cuma pake kabel dan colok di ether aja rasanya kurang lengkap , lalu gimana kalo client kita laptop dan rasanya aneh kalo harus dicolok dan diem disuatu tempat. Makanya dibuatlah interface khusus yaitu interface wlan di RouterBoard. Tapi gak semua jenis RB itu memiliki interface wlan jadi gak semuanya bisa dibuat menjadi access point. Sebagai contoh saya pakai jenis RB951 , nah itu ada interface wlan nya.

Oke tanpa basa- basi langsung aja yoo , melanjutkan lab koneksi internet , disini kita menambah network/jaringan yang menggunakan wireless , jadi kurang lebih topologinya begini



Oke jika sudah amati Topologi sekarang kita ke konfigurasinya , pertama kita aktifkan terlebih dahulu interface wlan-nya. Klik menu Wireless kemudian klik dibagian **wlan1** lalu klik tanda ceklis.

Wireless Tables								
Interfaces		Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels	
[+]	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx	[▼]
X	wlan1	Wireless (Atheros AR9...)	2290	0 bps	0 bps	0	0	[▼]

1 item out of 6 (1 selected)

Jika sudah , buka interface wlan1 nya kemudian klik tab Wireless lalu buat seperti gambar dibawah ini :

Interface <wlan1>

General	Wireless	HT	HT MCS	WDS	Nstreme	...	OK
	Mode: ap bridge						Cancel
	Band: 2GHz-B/G/N						Apply
	Channel Width: 20MHz						Disable
	Frequency: 2412	MHz					Comment
	SSID: Wifi Untung						Torch
	Scan List: default						Scan...
	Wireless Protocol: any						Freq. Usage...
	Security Profile: default						Align...
	Bridge Mode: enabled						Sniff...
	Default AP Tx Rate:	bps					Snooper...
	Default Client Tx Rate:	bps					Reset Configuration
	<input checked="" type="checkbox"/> Default Authenticate						Advanced Mode
	<input checked="" type="checkbox"/> Default Forward						
	<input type="checkbox"/> Hide SSID						
enabled	running	slave	searching for...				

Keterangan :

Mode = **ap bridge** , artinya kita membuat RB menjadi Access Point.

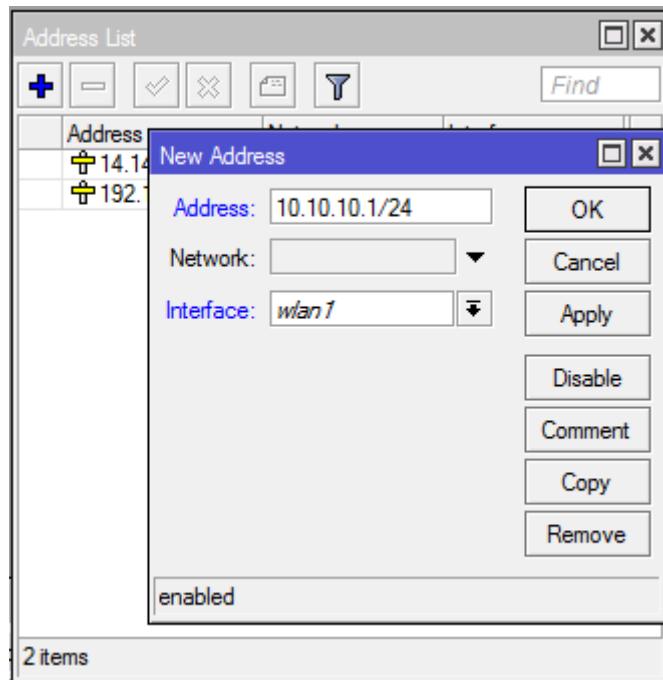
Band = Disesuaikan dengan client , jika kita memilih 2GHz-B/G/N , maka RB akan terhubung dengan perangkat yang memiliki frekuensi 2,4 GHz dengan spesifikasi 802.11b , 802.11g , 802.11n.

SSID = Ini tanda pengenal dari wireless yang kita buat. Ini opsional aja mas broo , isikan sesuai keinginan

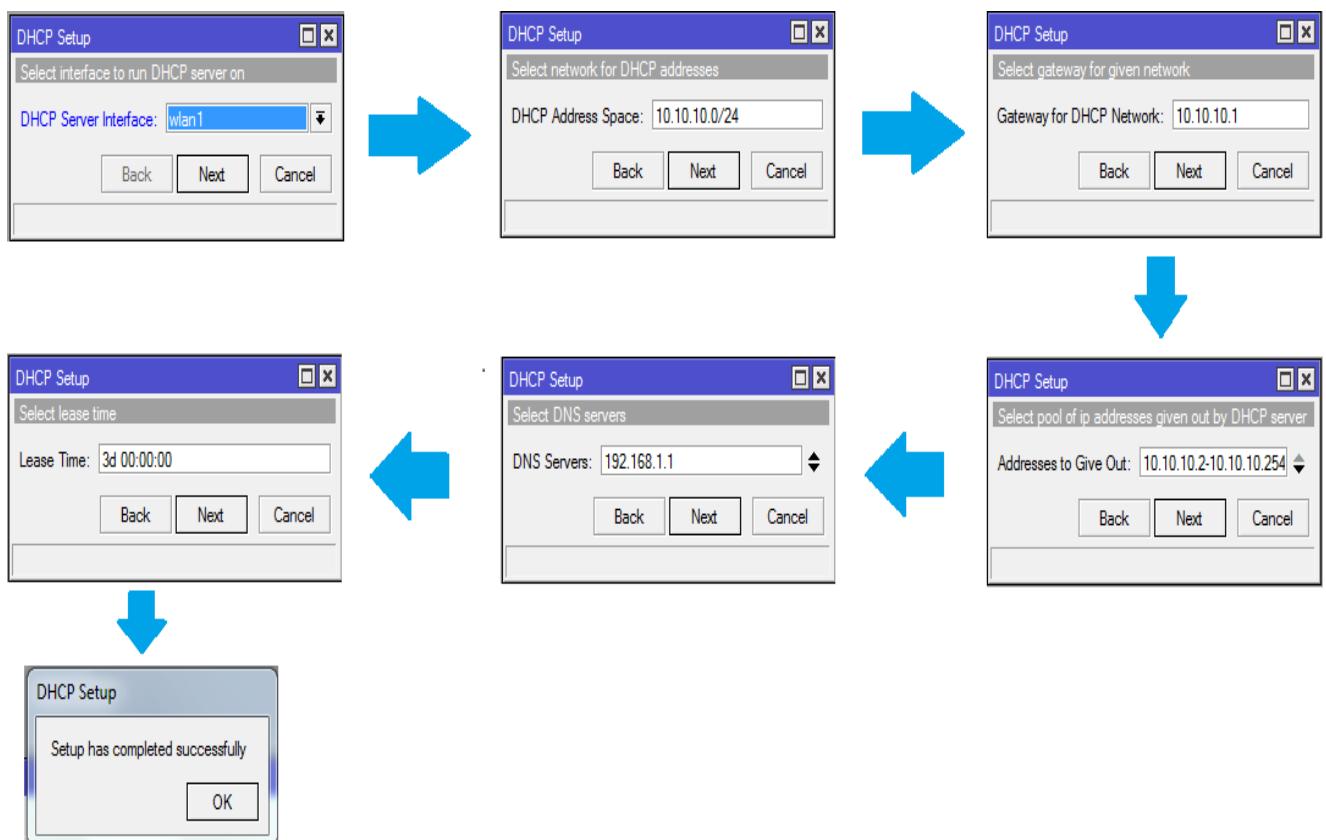
Jika sudah, seharusnya AP kita sudah terdeteksi di Laptop yang menggunakan wireless card.



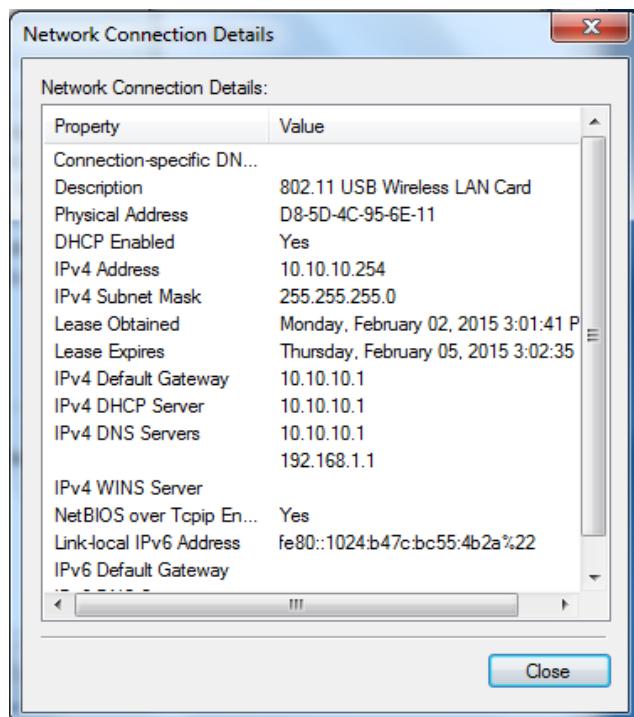
Jika sudah kedetect , selanjutnya kita akan memberikan IP untuk interface wlan nya , kan gak mungkin buat Access Point tapi gak dikasih IP. Caranya masih sama kok kayak di lab awal.



Kita juga bisa menambahkan DHCP untuk Access Point kita , ini berguna untuk meningkatkan kenyamanan dari client.



Jika sudah silahkan client koneksi ke RB tersebut , InshaAllah pasti ter-koneksi dengan lancar. Dan silahkan di cek IP nya , apakah sudah diberikan secara DHCP atau belum



Oke karena sudah terkoneksi artinya kita sudah sukses membuat RouterBoard kita menjadi Access Point.

Oke sekian dulu yaa

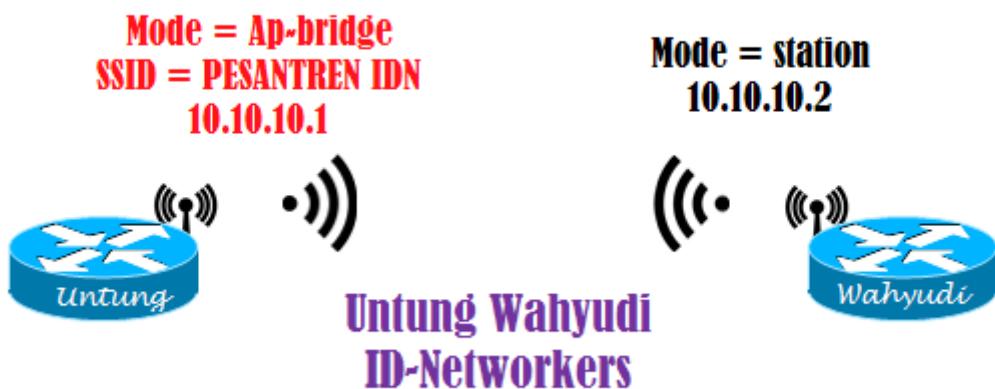
Wassalam !

Lab 43. Point to Point via Wireless

Assalamualaikum wr.wb

Lanjut lagi materi wireless nya , sekarang kita akan membuat point to point antar RouterBoard melalui media Wireless. Simple kok , intinya Cuma gimana caranya 2 Router bisa saling terkoneksi melalui media wireless. Setelah di lab sebelumnya kita sudah membuat RB menjadi Wireless maka lab tersebut masih dipake di lab ini. Disini kita membutuhkan 2 RB , ya iyalaah namanya juga *point to point*. Jadi yang satu sebagai Access Point nah yang satu lagi sebagai client. Yuk capcuss

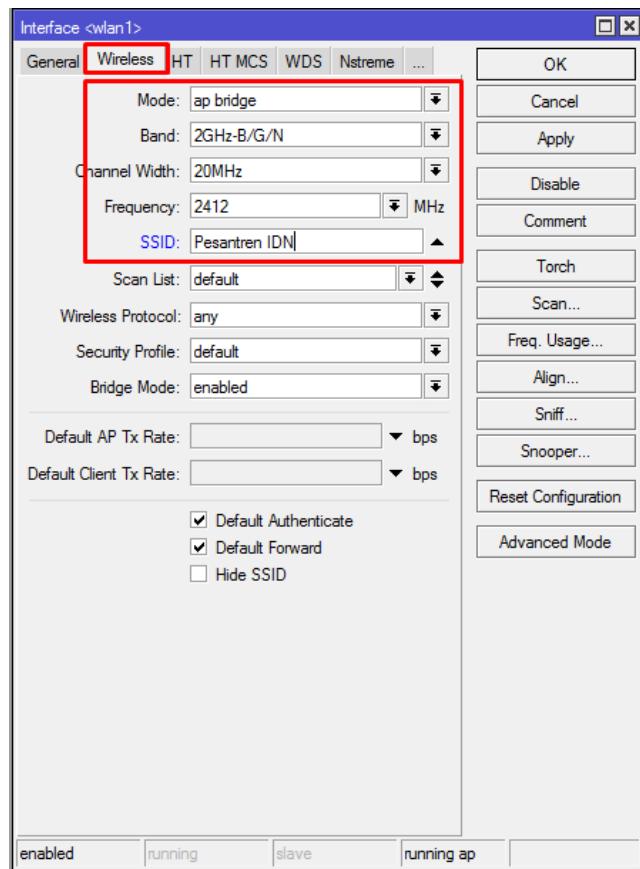
Kurang lebih topologinya begini



Oke langsung ke konfigurasinya :

Pada Router 1 :

Karena router 1 sebagai Access Point maka langkahnya masih sama dilab sebelumnya, kita buat mode nya menjadi ap-bridge , kemudian isikan SSID nya , sebagai contoh saya isi **Pesantren IDN** .



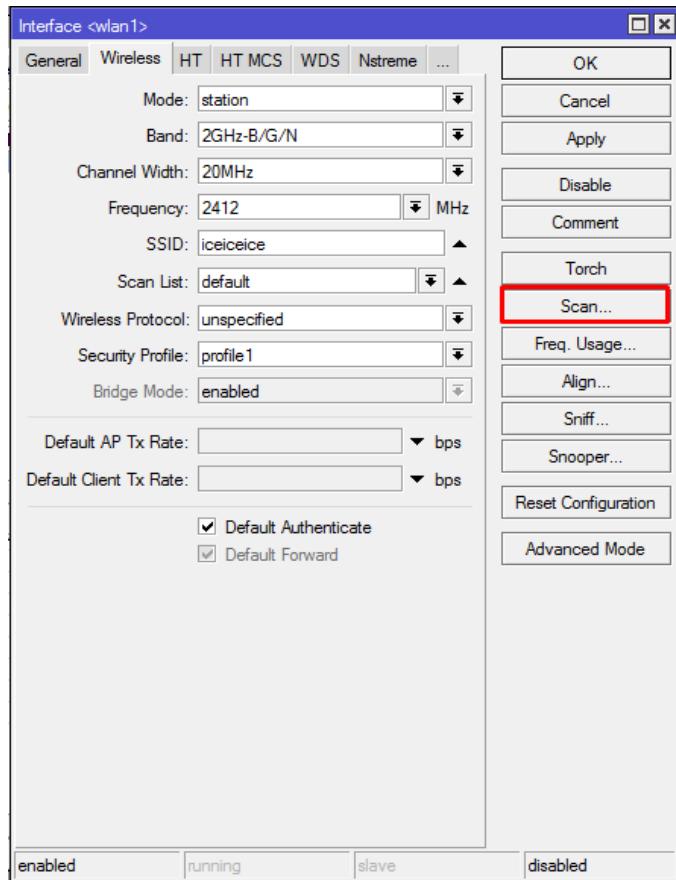
Setelah itu kita tambahkan IP untuk wlan1 , sebagai contoh saya pakai
10.10.10.1/24

Address List		
Address	Network	Interface
10.10.10.1/24	10.10.10.0	wlan1
1 item		

Sampai sini konfigurasi Router 1 sudah selesai , sekarang lanjut di konfigurasi Router 2 .

Pada Router 2 :

Selanjutnya kita konfigurasi Router 2 sebagai client , caranya adalah kita aktifkan interface wlan1 kemudian kita buat menjadi **mode station atau station bridge**. Kemudian klik tab Scan untuk men-scan Wireless



Kemudian pilih SSID wireless yang akan dikoneksikan , kita koneksi ke Wifi **Pesantren IDN** , setelah itu klik **Connect**.

Scanner (Running)

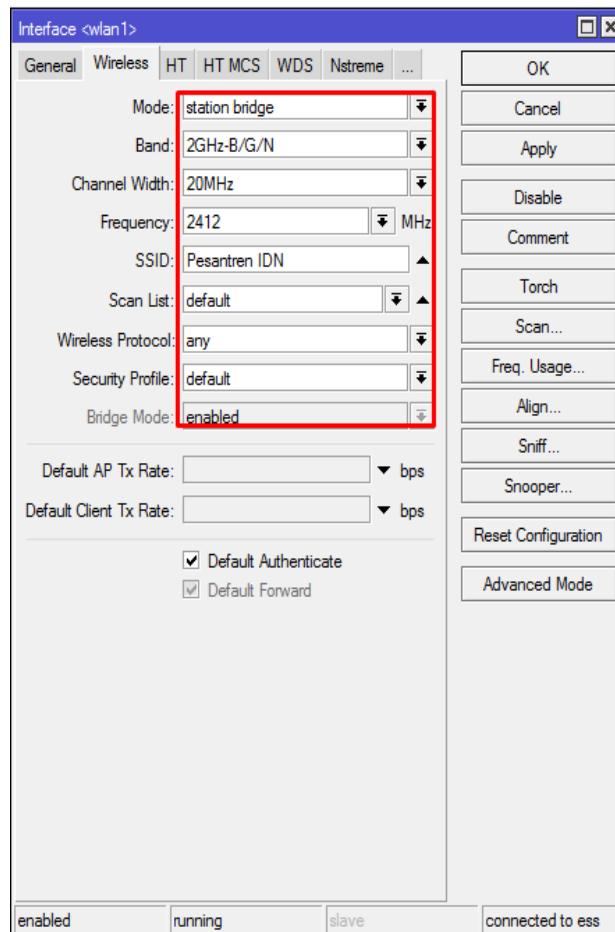
Interface: **wlan1**

Connect (button highlighted with a red box)

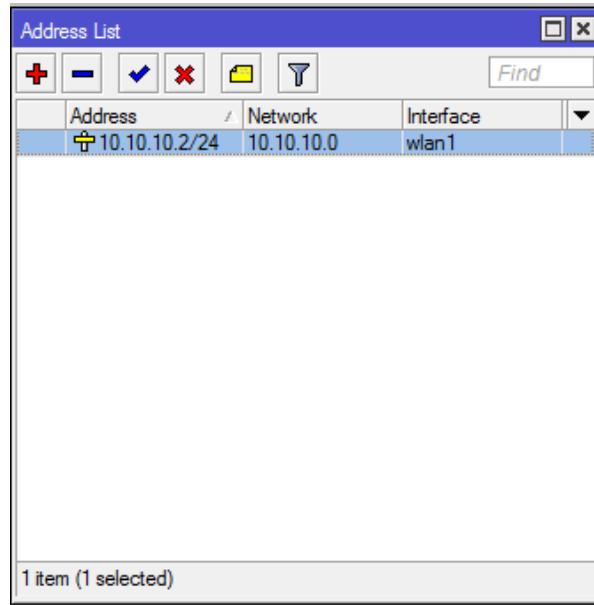
	Address	SSID	Band	Chan...	Frequ...	Signa...	Noise...	Signa...	Radio Name	▼
AP	BC:F6:85:40:A9:BA	TKJ GURU	2GHz...	20MHz	2412	-83	-99	16		
APR	D4:CA:6D:05:D1:69	Pesantren IDN	2GHz...	20MHz	2412	-45	-99	54	D4CA6D05D169	
AP	02:18:60:7B:F9:3A	[REDACTED]	2GHz...	20MHz	2412	-81	-99	18		
A	A0:F3:C1:74:34:50	LAB TKJ TEORI	2GHz...	20MHz	2427	-48	-103	55		
A	B0:48:7A:BD:81:28	LAB TKJ	2GHz...	20MHz	2432	-49	-103	54		
AP	02:18:60:59:CD:B7	J's Network	2GHz...	20MHz	2437	-72	-97	25		
ARB	4C:5E:0C:C3:D1:81	daynet.net	2GHz...	20MHz	2447	-41	-99	58	4C5E0CC3D181	
	00:23:69:D5:43:90	AP-GURU	2GHz...	20MHz	2457	-87	-102	15		
	00:27:22:C2:3A:77	AP-SMKN1	2GHz...	20MHz	2427	-93	-103	10		
P	E0:3F:49:8B:F1:A8	RPL HOTSPOT	2GHz...	20MHz	2462	-89	-104	15		
	00:1F:1F:0F:84:F5	ictnode2	2GHz...	20MHz	2462	-94	-104	10		

11 items (1 selected)

Jika sudah connect maka hasilnya akan seperti ini.



Jika sudah sekarang kita tambahkan IP untuk interface wlannya , kita buat menjadi 1 network dengan Router 1. Disini kita berikan IP **10.10.10.2/24**.



Jika sudah selanjutnya kita test ping antar Router.

Router 1 ke Router 2

```
[admin@R1] > ping 10.10.10.2
HOST                                SIZE TTL TIME   STATUS
10.10.10.2                           56   64 13ms
10.10.10.2                           56   64 5ms
10.10.10.2                           56   64 6ms
10.10.10.2                           56   64 6ms
10.10.10.2                           56   64 4ms
10.10.10.2                           56   64 8ms
sent=6 received=6 packet-loss=0% min-rtt=4ms avg-rtt=7ms max-rtt=13ms

[admin@R1] >
```

Router 2 ke Router 1

```
Terminal

      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  KKKKKK  RRR  RRR  000  000  TTT  III  KKKKK
      MMM  MM  III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
      MMM  MM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 5.26 (c) 1999-2013      http://www.mikrotik.com/

[admin@R2] > ping 10.10.10.1
HOST          SIZE TTL TIME STATUS
10.10.10.1    56  64  4ms
10.10.10.1    56  64  6ms
10.10.10.1    56  64  7ms
10.10.10.1    56  64  9ms
sent=4 received=4 packet-loss=0% min-rtt=4ms avg-rtt=6ms max-rtt=9ms

[admin@R2] >
```

Oke karena sudah koneksi dan sukses Ping nya maka artinya lab ini sudah berhasil
Oke mas dan mba broo sekian dulu yaa

Wassalam !

Lab 44. Mac Address Filtering

Assalamualaikum wr.wb

Lanjut lagi dari lab sebelumnya , di lab ini saya mau ngebahas ke tingkat yang berikutnya. Jadi kasusnya begini , gimana kalo kita buat point to point tapi di daerah itu ada banyak Wifi dan SSID nya sama dengan SSID yang kita buat. Naah kalo Router nya salah konek gimana tuuh ??? . Maka dari itu kita buat kemananya yaitu dengan Mac Address Filtering. Jadi baik si Router AP maupun Router Client tidak akan salah konek dan salah dikonekin. *Apaan coba dikonekin??.* Maksudnya ada client yang salah konek ke Wifi nya. Nih saya kasih topologinya

Oh ya ada satu tambahan lagi sebelum konfigurasi , sebaiknya kita harus tau dulu mac address dari 2 Router tersebut. Karena nantinya Mac Adress tsb akan dimasukkan di Access List dan Connect List

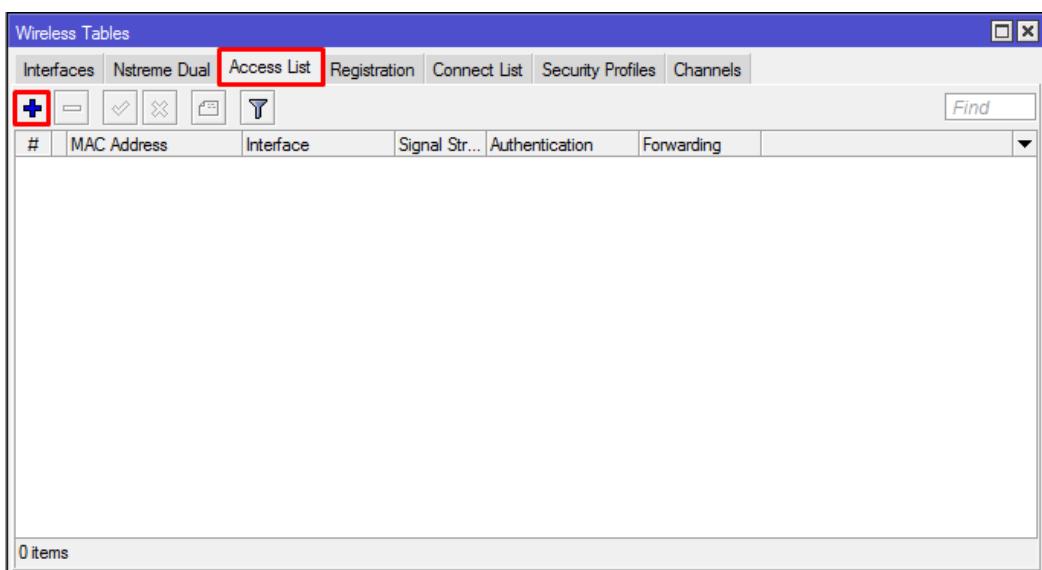
Access List (Di Router AP) = Daftar client yang terkoneksi di AP

Connect List (Di Router Client) = Daftar AP/Server yang bisa dikoneksikan

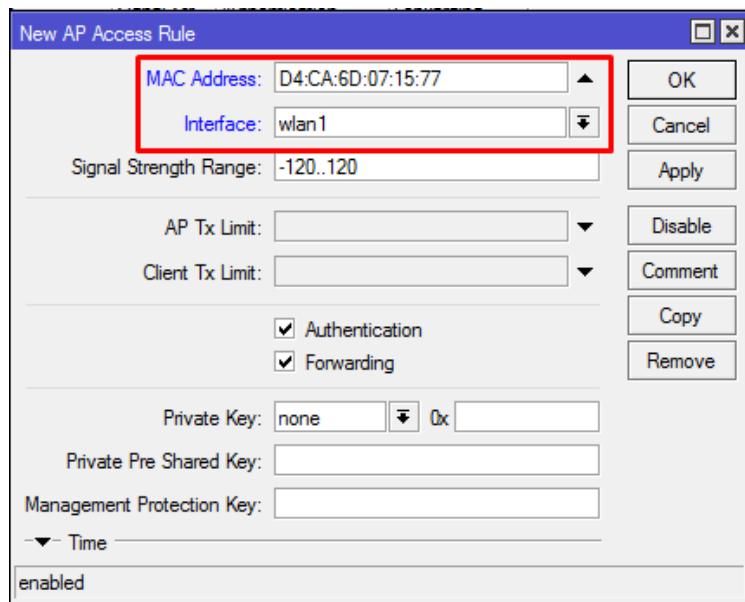
Yuk langsung aja kekonfigurasi nya.

Pada Router 1 (AP)

Kita klik menu Access List , kemudian klik Add



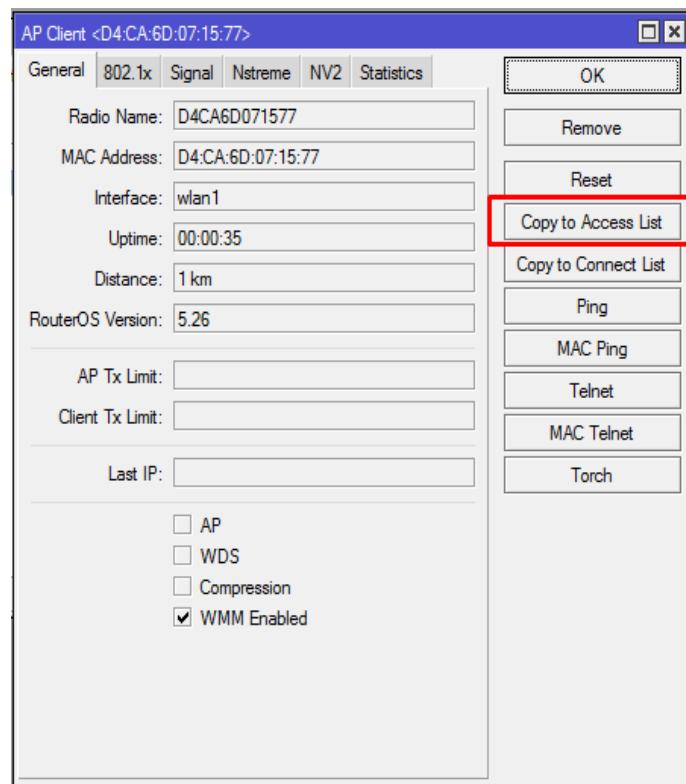
Setelah itu kita tambahkan Mac Address dari client yang terkoneksi ke RB kita.



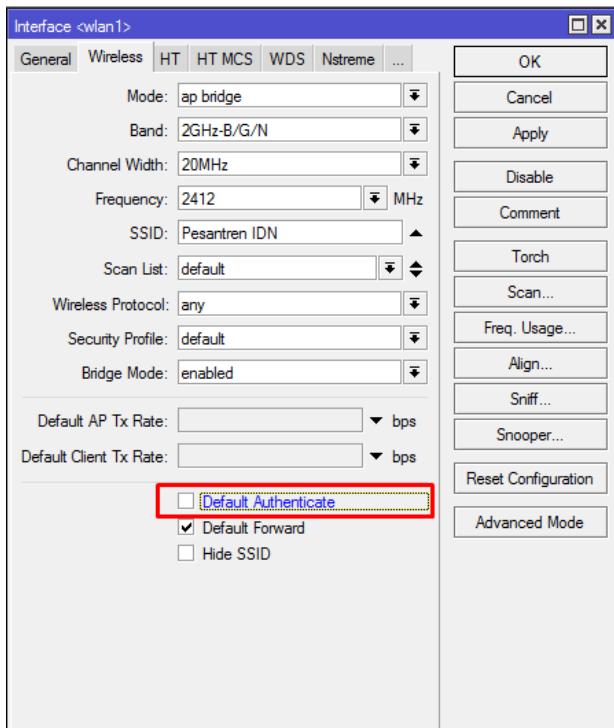
Setelah konfigurasi diatas maka konfigurasi di Router AP sudah selesai. Ohya sebenarnya ada cara lebih mudah , daripada pusing pusing ngapal Mac Address client , kita bisa gunakan cara simple yaitu dengan cara klik tab Registration , disana ada daftar client yang sedang terhubung ke AP kita

Wireless Tables								
Interfaces	Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels		
1 item								

Kemudian double klik di daftar nya , lalu kita pilih tab "Copy to Access List"



Aahaha , ternyata ada cara simple nya . Jika sudah selanjutnya kita klik menu interface wireless nya , kemudian hilangkan tanda centang di bagian Default Authentication.



Keterangan :

Default Authentication , artinya kita memberikan autentikasi secara default , jadi semua perangkat dapat terkoneksi. Jika kita hilangkan maka autentikasi nya tidak secara default melainkan melalui autentikasi MAC Address yang tadi kita buat.

Pada Router 2 (Client)

Caranya masih sama hanya saja kita daftarkan Mac Address dari Router AP nya, klik tab **Connect List** kemudian klik add.

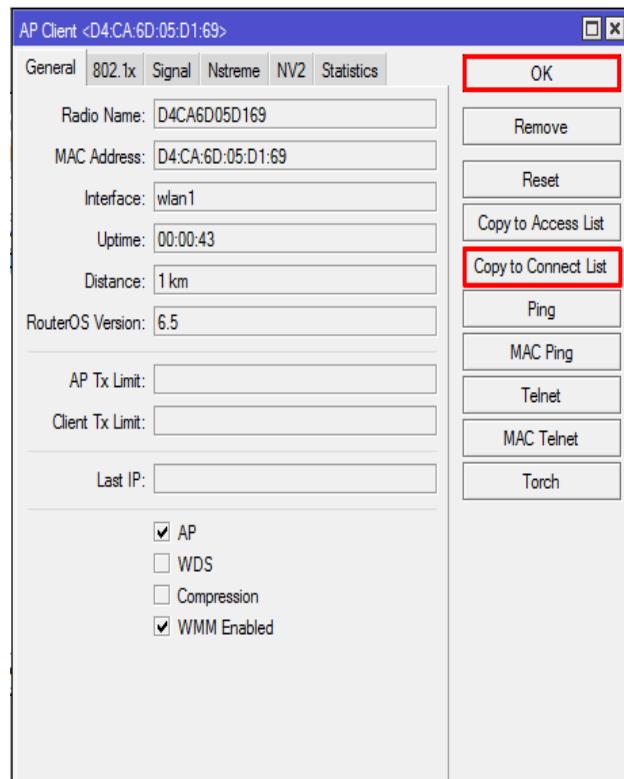
Wireless Tables						
Interfaces	Nstreme Dual	Access List	Registration	Connect List	Security Profiles	
#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0 items						

Setelah itu kita daftarkan MAC Address dari Router AP nya

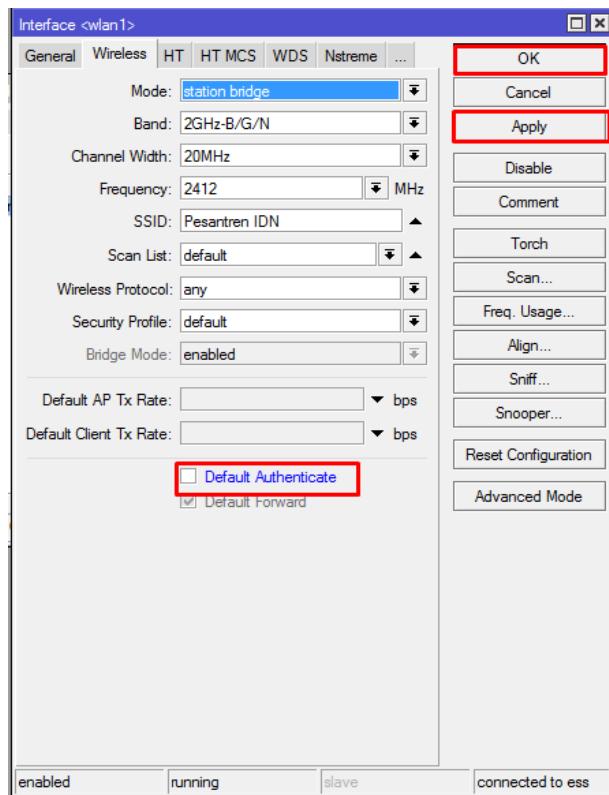
New Station Connect Rule

Interface:	wlan1	OK
MAC Address:	D4:CA:6D:05:D1:69	Cancel
<input checked="" type="checkbox"/> Connect		Apply
SSID:		Disable
Area Prefix:		Comment
Signal Strength Range:	-120..120	Copy
Wireless Protocol:	any	Remove
Security Profile:	default	
enabled		

Kita juga bisa membuat cara yang lebih mudah , yaitu dengan menggunakan tab Registration seperti sebelumnya , tinggal pilih "Copy to Connect List"



Jika sudah , kita buat default authentication nya di nonaktifkan. Sama seperti sebelumnya kan.



Nah sekarang 2 Router tersebut sudah tidak bisa koneksi ke Router atau Access Point lain. Istilahnya gak bisa selingkuh dengan Router lain hahaha

Oke mas broo sekian dulu yaa, kurang lebih nya mohon maaf

Wassalam !

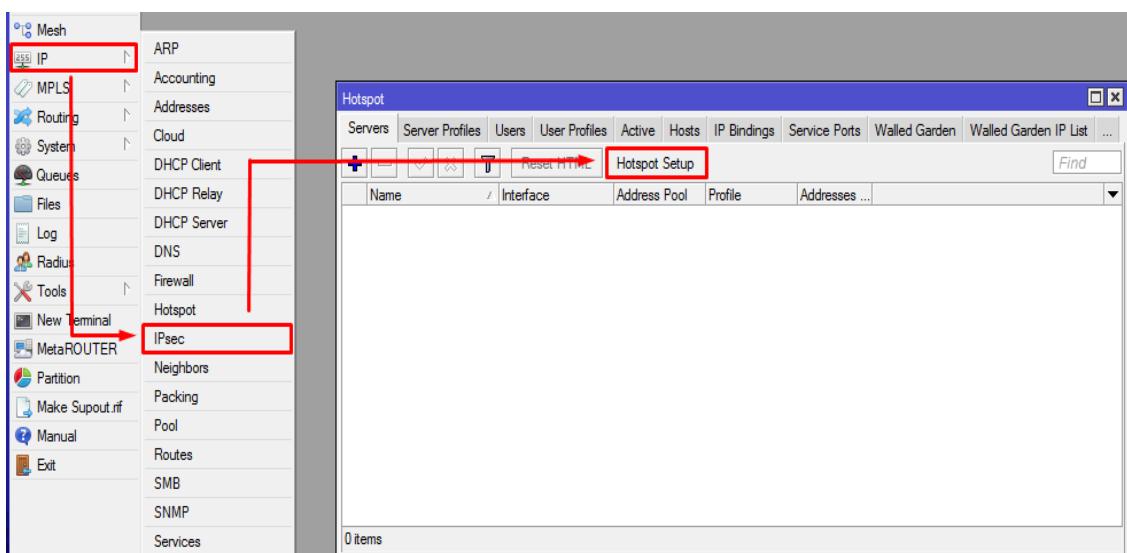
Lab 45. Membuat Hotspot

Assalamualaikum wr.wb

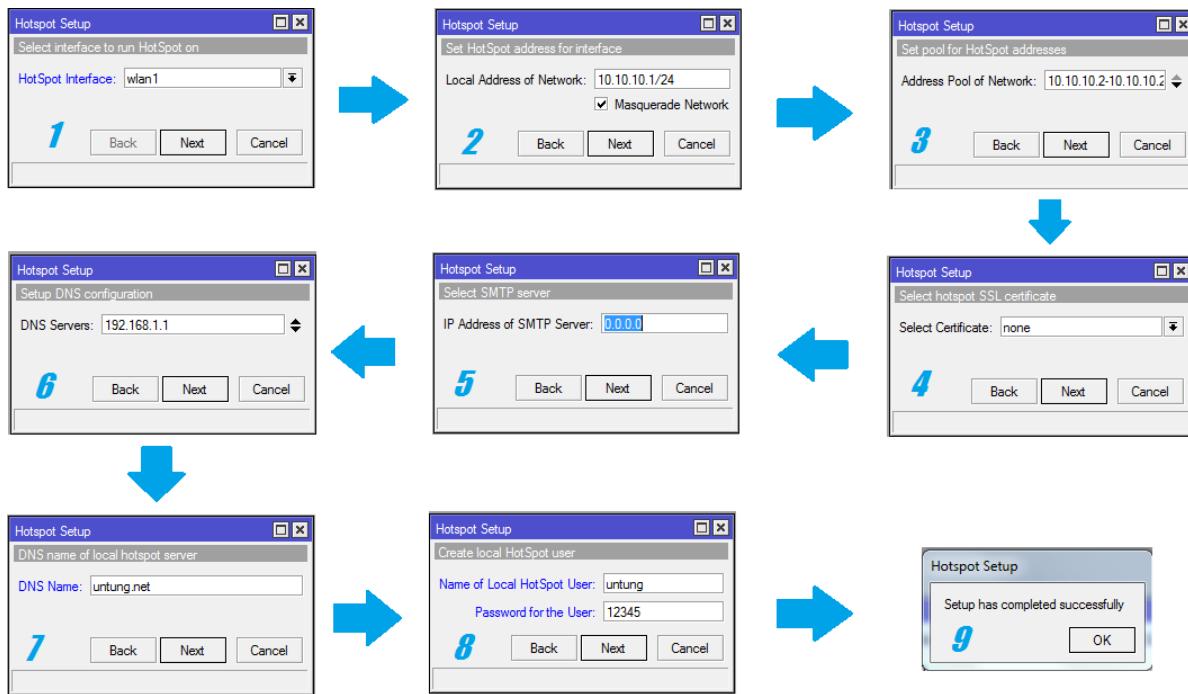
Yuk lanjut lagi lab wireless network nya , di lab ini sangaaaat spesial karena kita akan membuat layanan Hotspot dengan Mikrotik kita. Dengan hotspot ini nantinya client yang ingin melakukan aktifitas browsing akan dimintai authentikasi berupa username dan password. Yuk langsung aja kekonfigurasinya

Sebelum ke konfigurasi hotspot ini , sebaiknya interface wlan kita sudah dikonfigurasikan dengan benar , seperti di Lab Membuat RouterBoard menjadi AP , sekaligus sudah bisa terkoneksi ke internet dengan NAT. Yuk cuuuuss langsung aja

Pertama kita klik menu IP > Hotspot > Hotspot Setup



Kemudian silahkan simak gambar berikut ini.



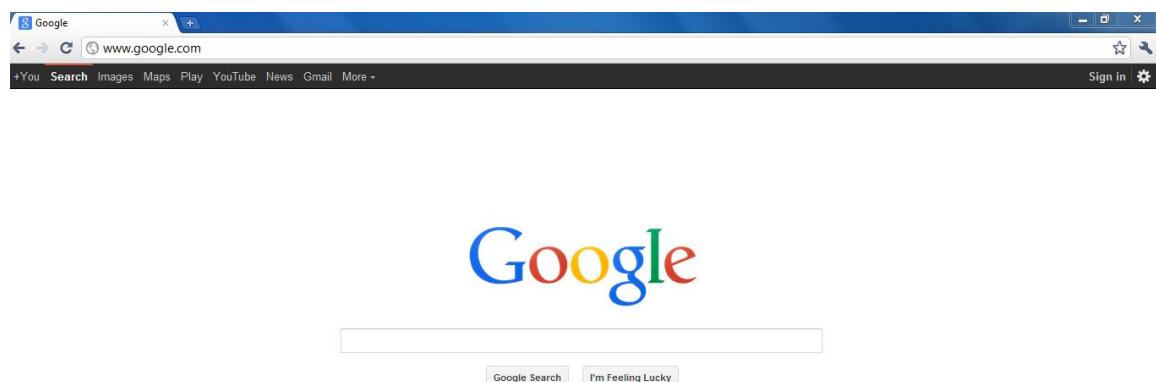
Keterangan :

- 1 = Pilih interface yang akan dijadikan hotspot
- 2 = IP Gateway/ IP dari interface tersebut
- 3 = Jumlah IP yang akan diberikan ke client , tergantung jumlah client
- 4 = Sertifikat SSL , jika kita mempunya sertifikat SSL silahkan di import , sertifikat ini untuk membuat browser hotspot kita menjadi HTTPS.
- 5 = IP SMTP Server , pilih saja 0.0.0.0
- 6 = IP DNS Server nya
- 7 = Nama DNS local nya , atau nama jaringan hotspotnya
- 8 = Pembuatan user pertama , kita bisa saja menambah usernya nanti
- 9 = Pembuatan telah selesai

Jika sudah , coba koneksi client ke Wifi yang tadi sudah kita buat di Lab membuat RouterBoard menjadi Access Point , pastikan sudah terhubung ke internet , lalu silahkan buka browser nya , maka hasilnya akan muncul authentikasi seperti ini



Coba login dengan user yang tadi sudah dibuat untuk dapat melakukan browsing. Jika sudah maka hasilnya seperti ini



Kita bisa melakukan monitoring terhadap user yang menggunakan layanan hotspot kita , cara nya tinggal klik tab Host di bagian menu Hotspot.

Hotspot							
	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List
AH	D8:5D:4C:95:6E:11	10.10.10.254	10.10.10.254	hotspot1	00:00:00	477 bps	477

Oke mas bro karena sudah berhasil maka saya tutup lab ini dengan mengucap Alhamdulillah

Sekian dulu yoo , kurang lebih nya mohon maaf

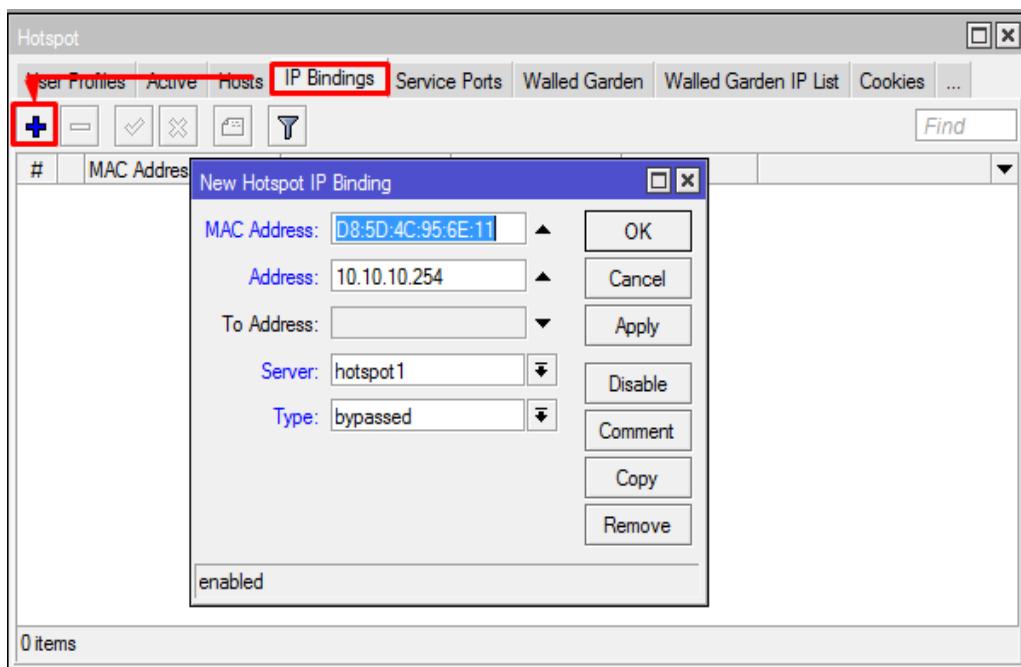
Wassalam !

Lab 46. Mem-Bypass IP Tertentu

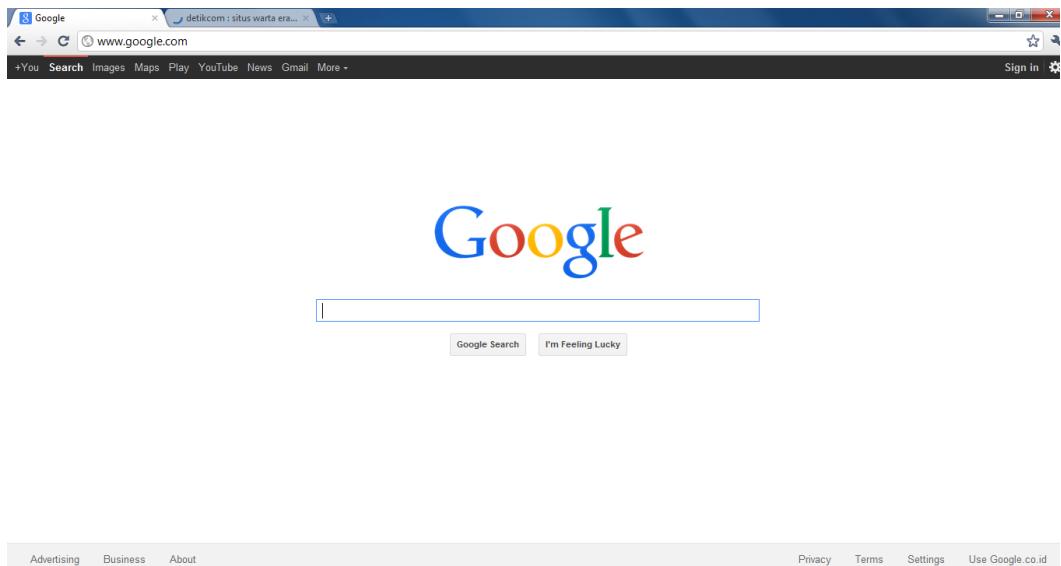
Assalamualaikum wr.wb

Melanjutkan dari lab hotspot sebelumnya , di sini kita akan membahas sedikit lebih dalam tentang Hotspot. Karena hotspot melakukan authentikasi ketika ingin melakukan browsing maka akan rada ribet untuk admin si router itu sendiri , karena ketika ingin browsing si admin akan tetap ditanyakan authentikasi dan password. Nah untuk mengatasi itu kita bisa menggunakan fitur **IP Binding** pada Hotspot. IP Binding ini memiliki beberapa 3 fitur yaitu **blocked** , **regular** dan **bypass**. Nah di lab ini Cuma akan dibahas yang bypass aja , jadi IP tertentu tidak akan ditanya authentikasinya ketika browsing

Pertama klik menu **IP Binding** , di hotspot. Kemudian klik add , lalu isikan Mac Address dan IP Address target nya , lalu pilih type nya bypassed , karena kita ingin mem-bypass IP si Admin



Jika sudah silahkan test browsing , maka hasilnya tidak akan ditanya authentikasinya , melainkan langsung bisa berselancar di dunia internet.



Oke karena sudah berhasil maka saatnya saya untuk bilang , Alhamdulillah.

Oke sekian dulu mas broo , kurang lebih nya mohon maaf yaa

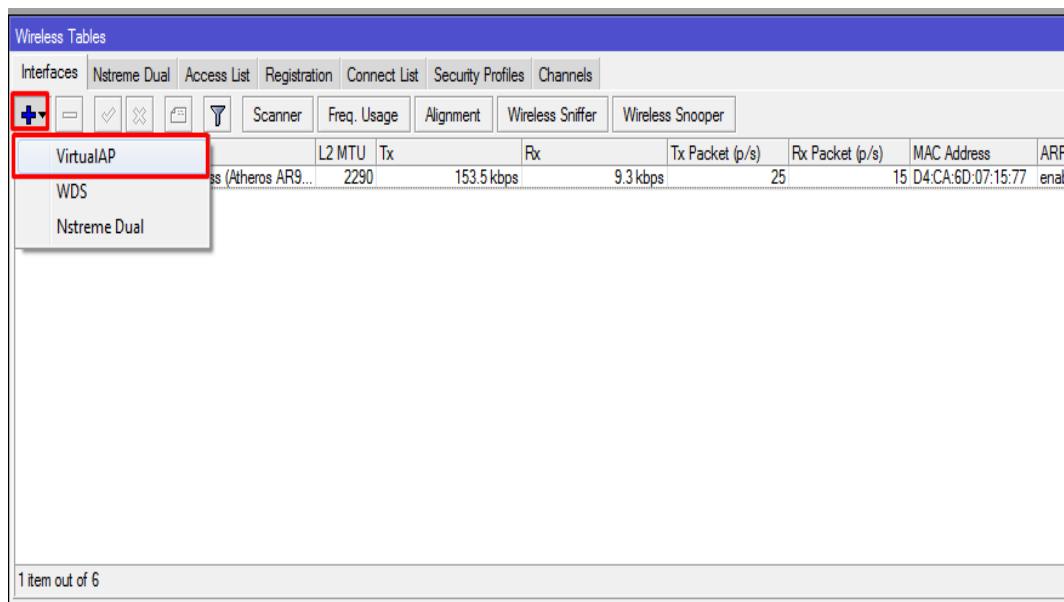
Wassalamualaikum !

Lab 47. Virtual Access Point

Assalamualaikum wr.wb

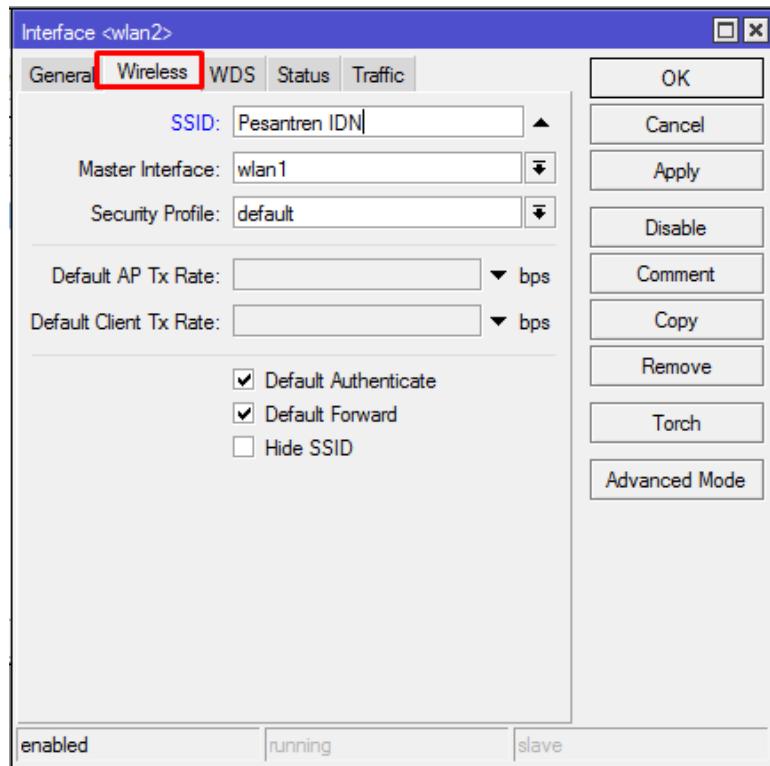
Masih lanjut di lab network , sekarang materinya agak beda yaitu Membuat Virtual Access Point (VAP). Jadi VAP ini adalah salah satu fitur mikrotik yang memungkinkan kita membuat beberapa Access Point hanya berbekal/ menggunakan 1 interface wlan. Jadi ini bisa digunakan untuk menghemat uang kita mas broo. Virtual Access Point ini nantinya akan memiliki IP address yang berbeda-beda , Mac Address yang berbeda dan juga SSID yang berbeda. VAP ini juga bisa kita gunakan sebagai DHCP server dan Hotspot dimasing masing VAP nya. Maksimal dari VAP ini adalah 128 VAP setiap 1 interface wlan. Woaaaa cukup banyak yaa. Bayangkan kita bisa membuat 128 jaringan hotspot hanya dengan 1 interface wlan . Tapi harus diperhatikan juga spesifikasi Routernya yoo , jangan asal buat 128 hotspot tadi spesifikasinya standar , ntar malah masuk rumah sakit tuh RB hehehe.

Oke langsung aja , untuk percobaan pertama kita akan buat 3 Virtual AP dengan menggunakan interface wlan1. Pertama kita klik menu **wireless** , kemudian klik menu Add lalu pilih Virtual AP. (*Oh ya karena nantinya VAP ini menginduk kepada interface asli , maka konfigurasi di interface wlan 1 harus mode AP-Bridge.*)



Wireless Tables									
Interfaces	Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels			
<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="+"/>		<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Delete"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Edit"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="X"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Scanner"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Freq. Usage"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Alignment"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Wireless Sniffer"/>	<input style="width: 20px; height: 20px; border: 1px solid black;" type="button" value="Wireless Snooper"/>
VirtualAP	WDS	WDS	WDS	WDS	WDS	WDS	L2 MTU	Tx	
	WDS	WDS	WDS	WDS	WDS	WDS	2290	153.5 kbps	
	WDS	WDS	WDS	WDS	WDS	WDS	9.3 kbps	25	
	WDS	WDS	WDS	WDS	WDS	WDS	15	D4:CA:6D:07:15:77	
	WDS	WDS	WDS	WDS	WDS	WDS	enat		
Nstreme Dual									
1 item out of 6									

Selanjutnya kita buat SSID yang berbeda , sebagai contoh kita buat SSID nya Pesantren IDN.



Oh ya karena saya udah janji buat 3 VAP , nah tinggal dibuat 2 lagi dengan cara yang sama , maka hasilnya akan terdeteksi 3 Access Point yang tadi kita buat



Bisa dilihat kan , akan muncul 3 SSID yang tadi kita buat , padahal RB kita Cuma memiliki 1 Interface wlan.

Oke karena sudah berhasil , maka saatnya saya untuk bilang Alhamdulillah.

Sekian dulu yaa

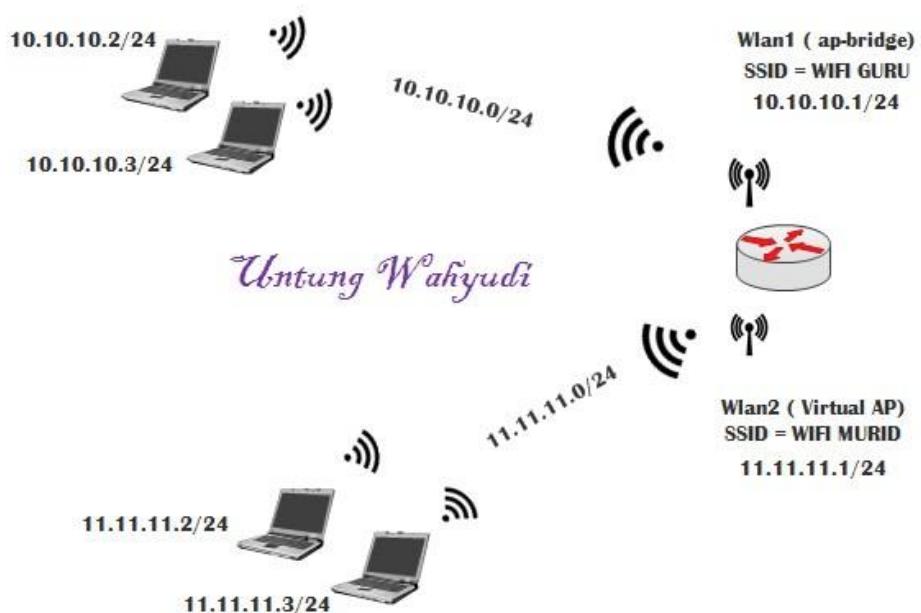
Wassalam !

Lab 48. Virtual Access Point + DHCP Server

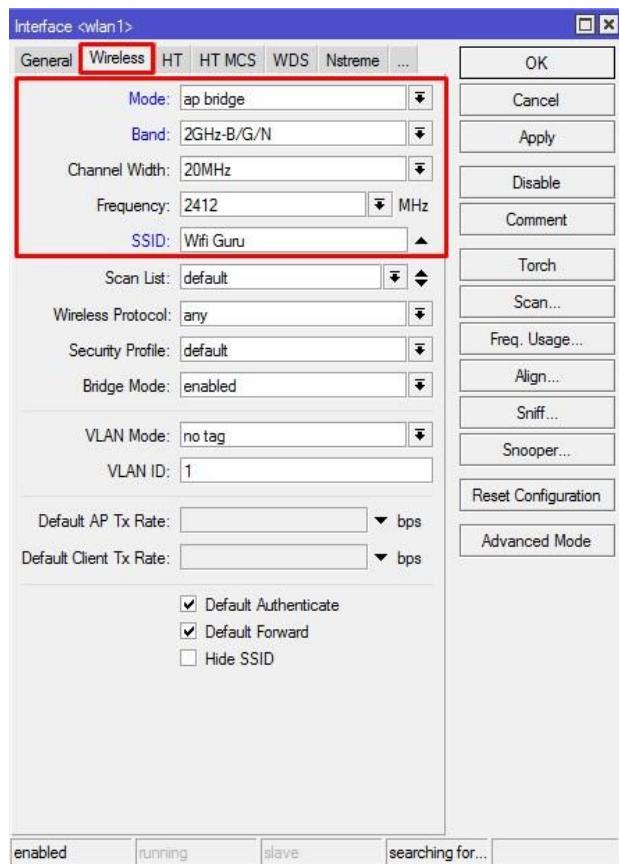
Assalamualaikum wr.wb

Masih melanjutkan tentang Virtual Access Point , sebelumnya saya udah bahas tentang kelebihan VAP ini , dan VAP ini bisa digunakan sebagai DHCP Server dan Hotspot. Nah di Lab ini saya mau bahas tentang cara membuat VAP dengan DHCP Server. Oke langsung aja study case nya

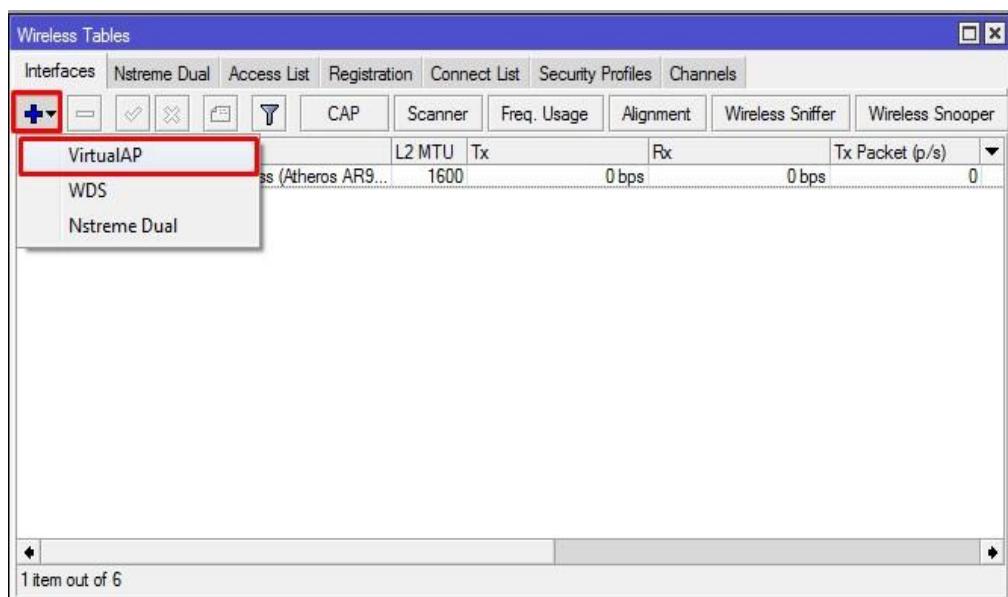
Di sebuah sekolah ingin memisahkan jaringan Wireless , yaitu Wifi untuk para guru dan Wifi untuk Murid. Nah nantinya IP nya juga berbeda untuk masing masing Wifi tersebut. Nih topologinya. Jadi kita buat interface asli untuk Wifi guru , dan Virtual AP nya untuk wifi murid.



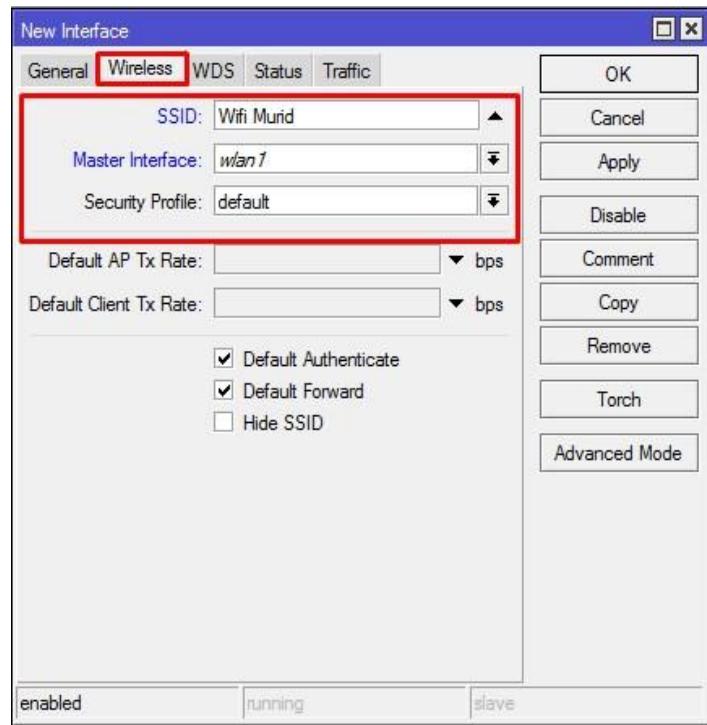
Yuk langsung aja kekonfigurasi nya , pertama kita setting untuk Wifi guru (wlan1) . Kita buat mode nya menjadi Ap-bridge dan SSID nya Wifi Guru



Selanjutnya kita buat juga Virtual AP untuk para murid. Cara nya tinggal klik add lalu pilih Virtual AP



Kemudian kita buat SSID nya menjadi Wifi Murid. Seperti dibawah ini

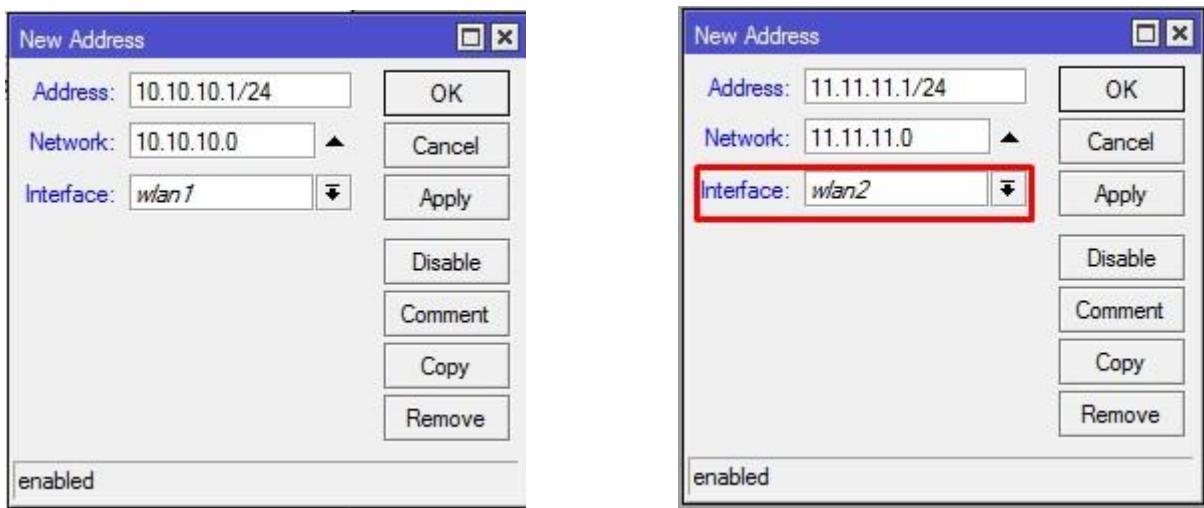


Maka hasilnya akan seperti ini , interface wlan2 akan meng-induk ke wlan1

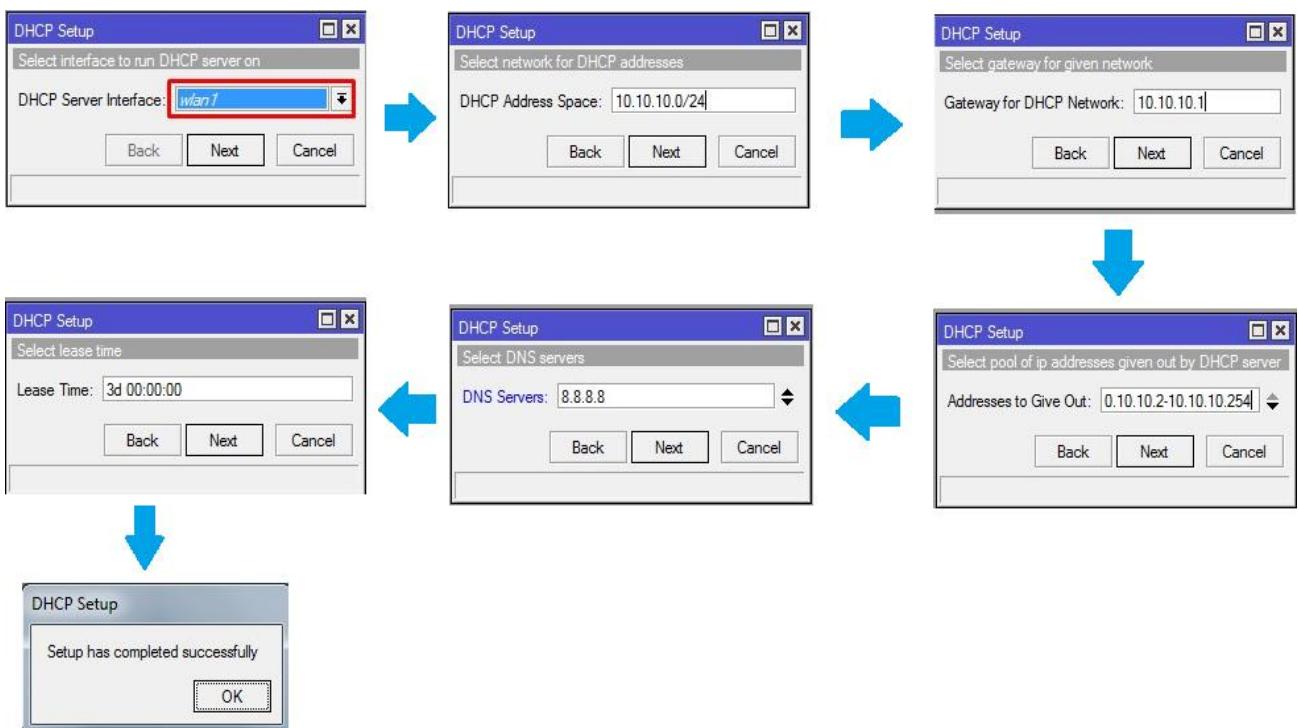
Wireless Tables							
Interfaces		Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)		
wlan1	Wireless (Atheros AR9...)	1600	0 bps	0 bps	0		
↳ wlan2	VirtualAP	1600	0 bps	0 bps	0		

2 items out of 7

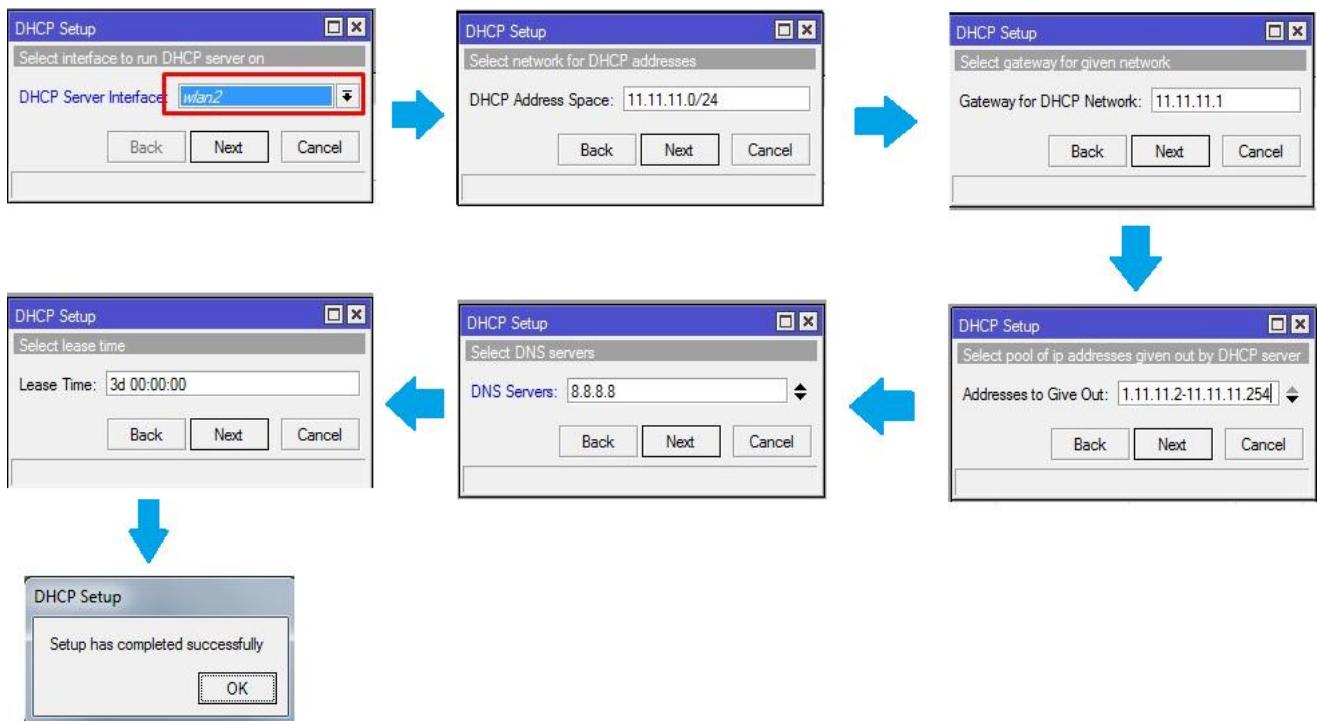
Setelah itu kita berikan IP untuk masing-masing AP , 10.10.10.1/24 untuk Wifi Guru (wlan1) dan 11.11.11.1/24 untuk Wifi Murid (wlan2/VAP)



Kemudian kita buat DHCP Server untuk masing masing interface ,
Untuk wlan1 (Wifi Guru)



Kemudian kita buat juga untuk interface wlan2 (Wifi Murid)



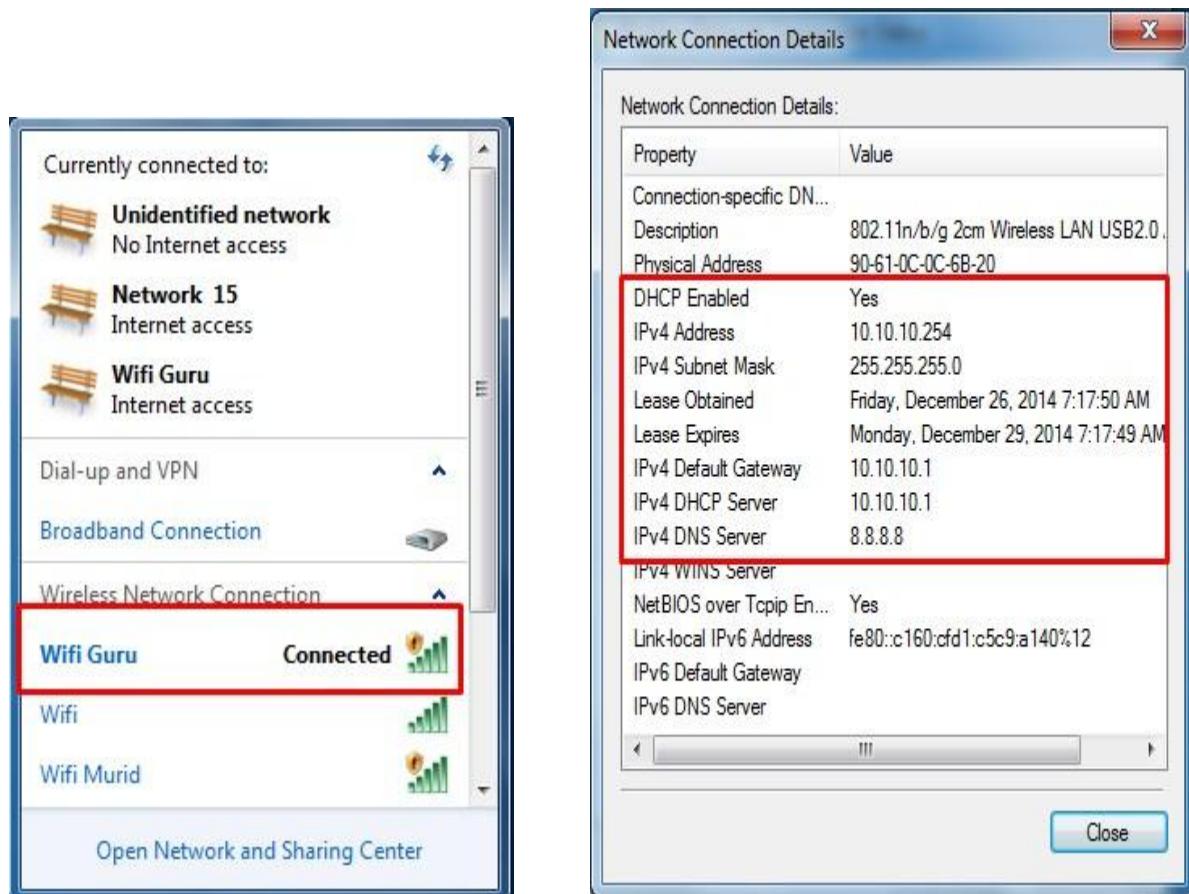
Jika sudah maka begini hasil nya , akan ada 2 DHCP , yang satu untuk guru dan yang satu untuk murid

DHCP Server					
DHCP Networks Leases Options Option Sets Alerts					
		DHCP Config	DHCP Setup		
Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	wlan1		3d 00:00:00	dhcp_pool1	no
dhcp2	wlan2		3d 00:00:00	dhcp_pool2	no

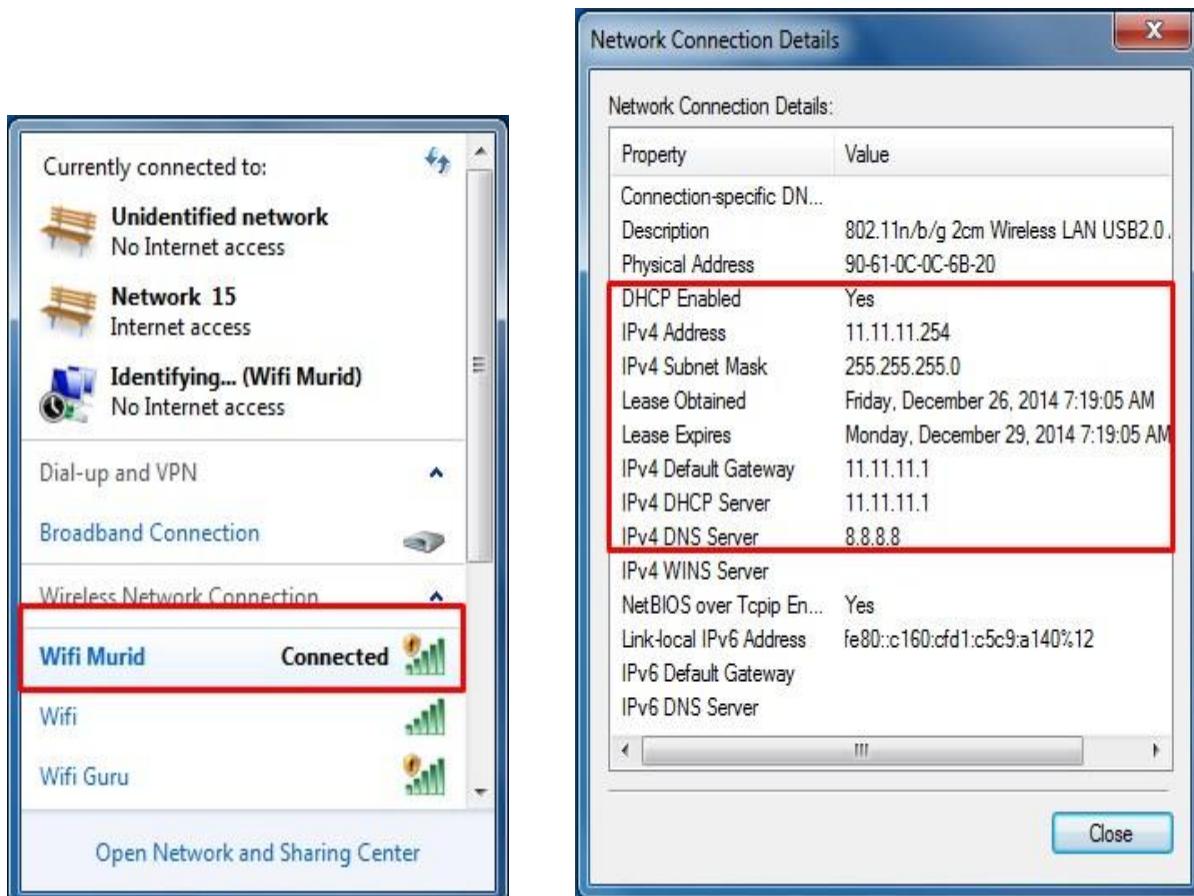
2 items

A red bracket on the left side of the table groups the two rows. Two red arrows point from this bracket to the right, each pointing to a red box containing text: 'DHCP Wlan 1 (WIFI GURU)' and 'DHCP Virtual AP (WIFI MURID)'.

Selanjutnya silahkan koneksi ke 2 Wifi tersebut , pertama koneksi ke Wifi Guru dan cek IP address nya



Kemudian coba koneksi ke Wifi Murid , dan cek IP nya



Oke mas dan mba bro , karena 2 jaringan tersebut sudah terpisah maka artinya lab kita sudah berhasil, saatnya kita mengucapkan Alhamdulillah

Sekian dulu yoo , kurang lebih nya mohon maaf

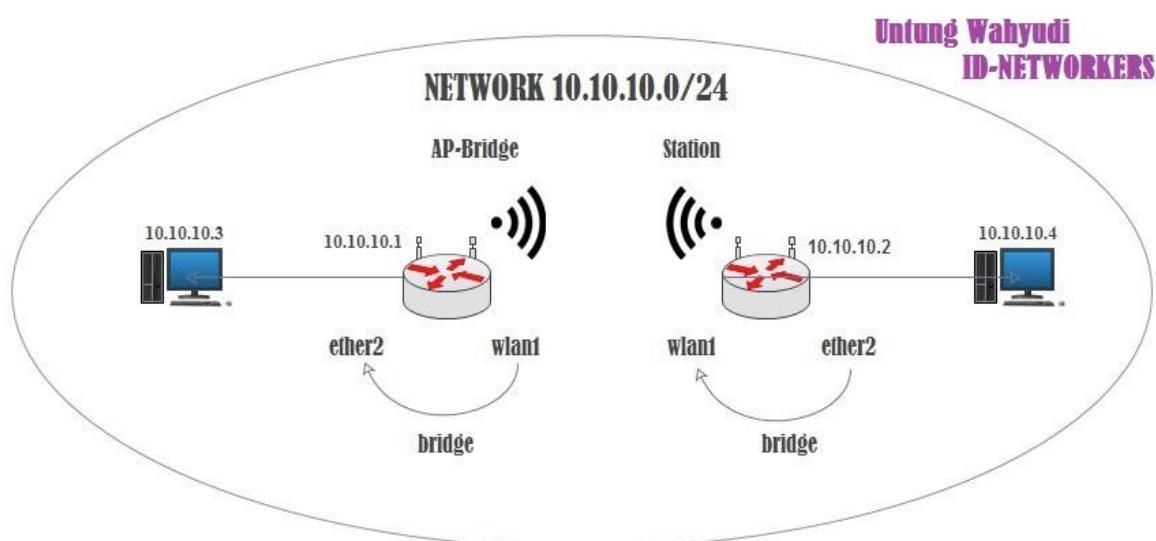
Wassalam !

Lab 49. Bridging

Assalamualaikum wr.wb

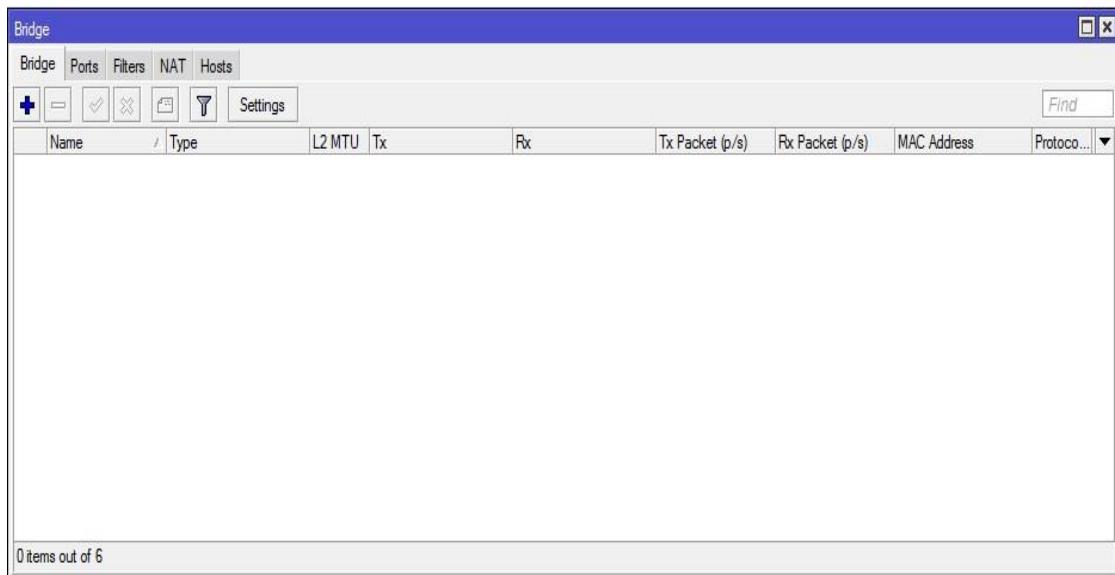
Sekarang kita sudah meninggalkan materi wireless dan masuk ke materi Bridging. *Apa itu bridging ???*, jadi bridging adalah sebuah teknik yang menggabungkan beberapa interface dari router menjadi satu , sehingga interface interface tersebut akan menjadi satu segmen jaringan. Bridging ini mengacu pada OSI layer 2 (Data Link). Bisa diibaratkan nantinya router kita menjadi sebuah switch.

Oke untuk meningkatkan pemahaman tentang Bridging kita langsung nge-lab saja. Jadi kita akan buat topologinya menjadi seperti ini. Oh ya disini saya bridging nya menggunakan media wireless , sebenarnya sama aja konfigurasinya seperti di media kabel.

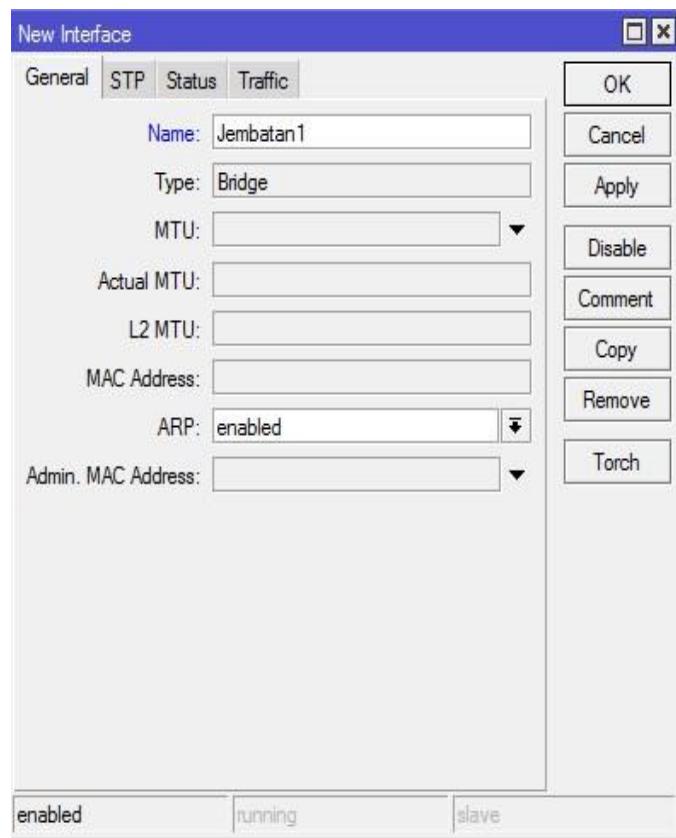


PADA ROUTER 1 :

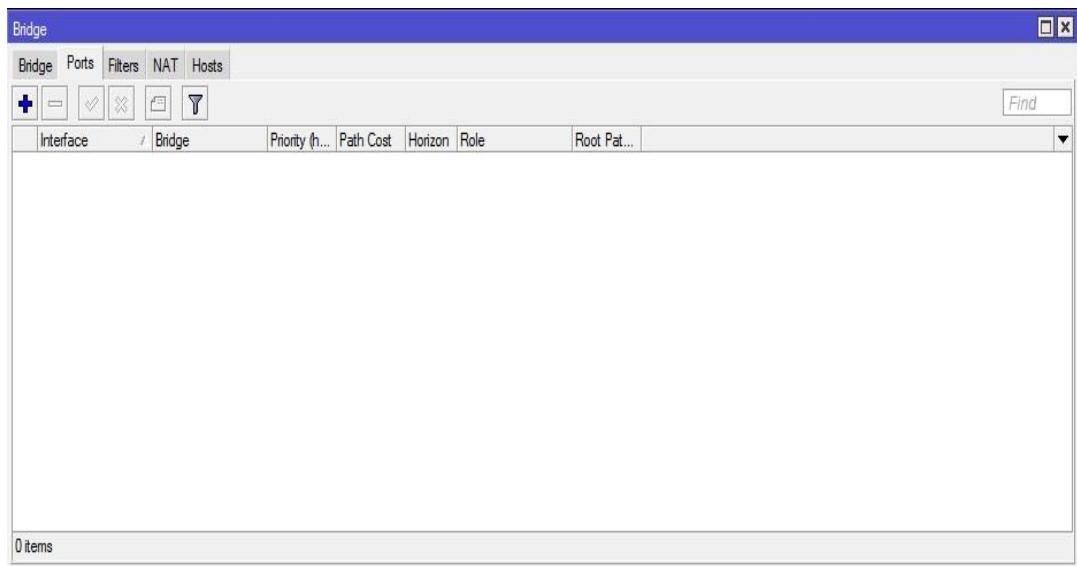
Pertama pastikan kedua router sudah saling terkoneksi. Antar bridge dan station nya seperti di lab sebelumnya. Kemudian kita akan menambahkan interface bridge , caranya tinggal klik menu **Bridge** , kemudian klik tombol add.



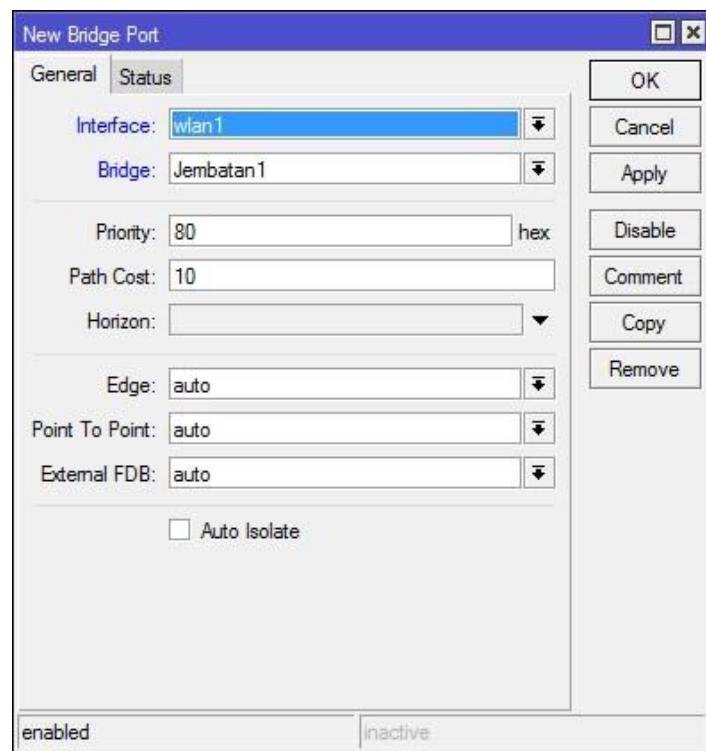
Setelah itu , kita buat interface bridge-nya dengan nama opsional sesuka kalian.



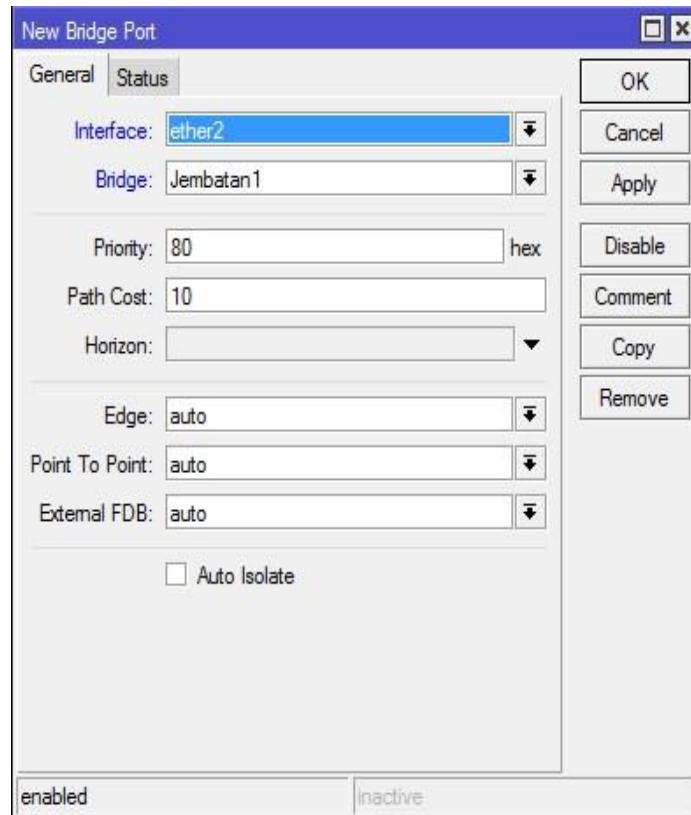
Setelah itu kita masukkan interface yang akan kita bridge kedalam interface "Jembatan1". Karena ditopologi diatas kita akan menghubungkan jaringan wireless dan ether2 , maka kita masukkan interface wlan1 dan ether2 , caranya klik **tab Port** di menu Bridge , kemudian klik **add**.



Kemudin kita masukkan interface wlan1 kedalam jembatan1



Kita masukkan juga interface ether2 kedalamnya

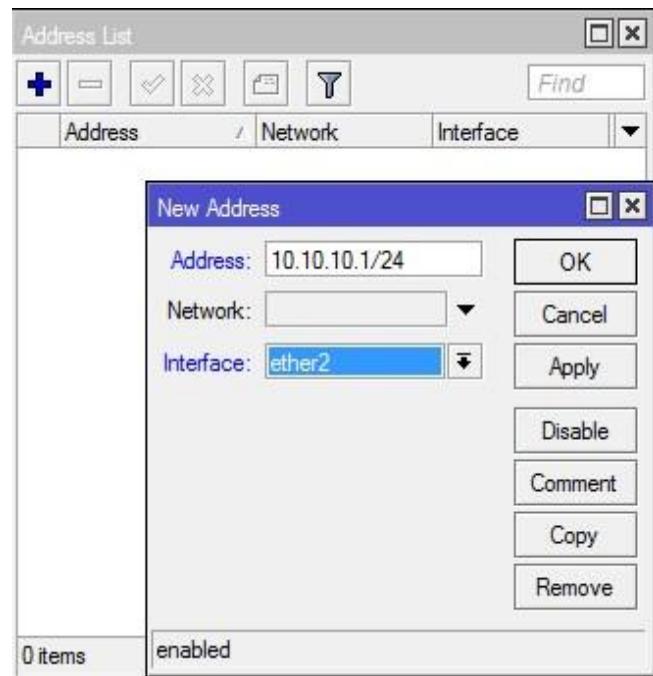


Kemudian hasilnya akan menjadi seperti ini .

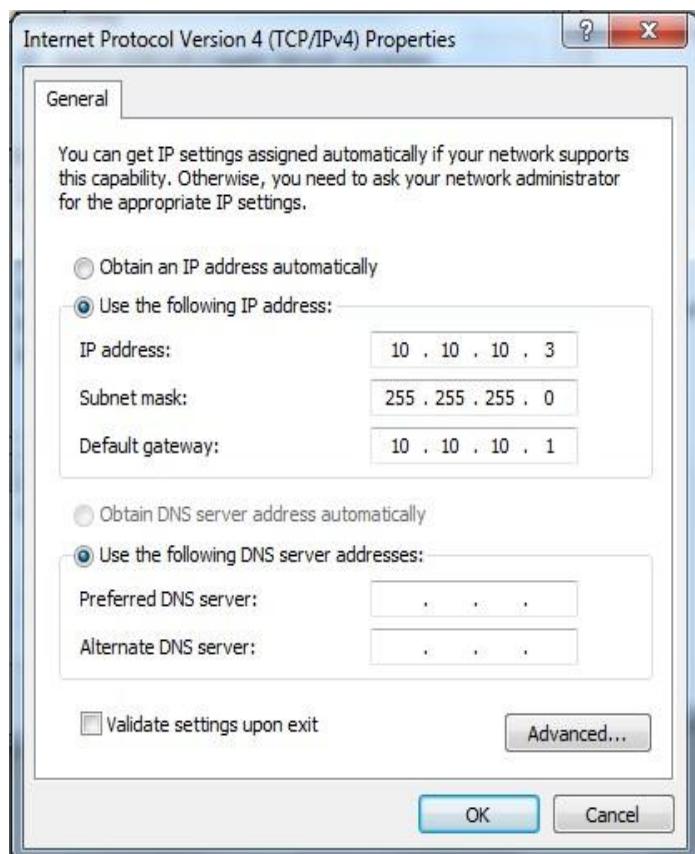
Bridge						
Bridge	Ports	Filters	NAT	Hosts		
ether2	Jembatan1	80	10	designated port	Root Pat...	
wlan1	Jembatan1	80	10	designated port		

2 items

Setelah itu kita tambahkan IP untuk interface nya , terserah kita interface mana yang akan kita berikan IP , bisa interface wlan1 ataupun ether2. Kita bisa saja tidak memberikan IP untuk interface tersebut , karena layaknya switch kita tidak perlu memberikan IP address untuk interfacenya.

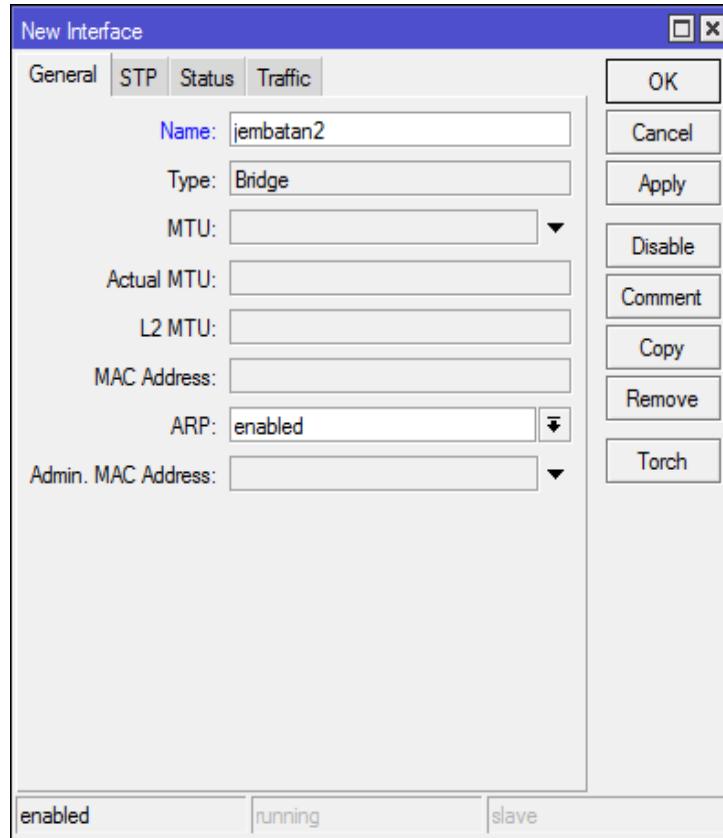


Setelah itu kita masukan juga IP di client kita , ingat harus 1 Network .

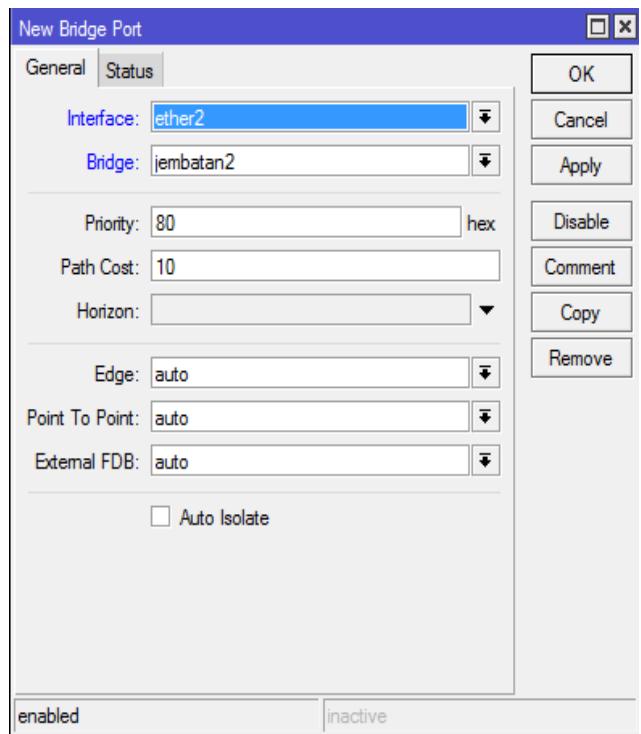


PADA ROUTER 2 :

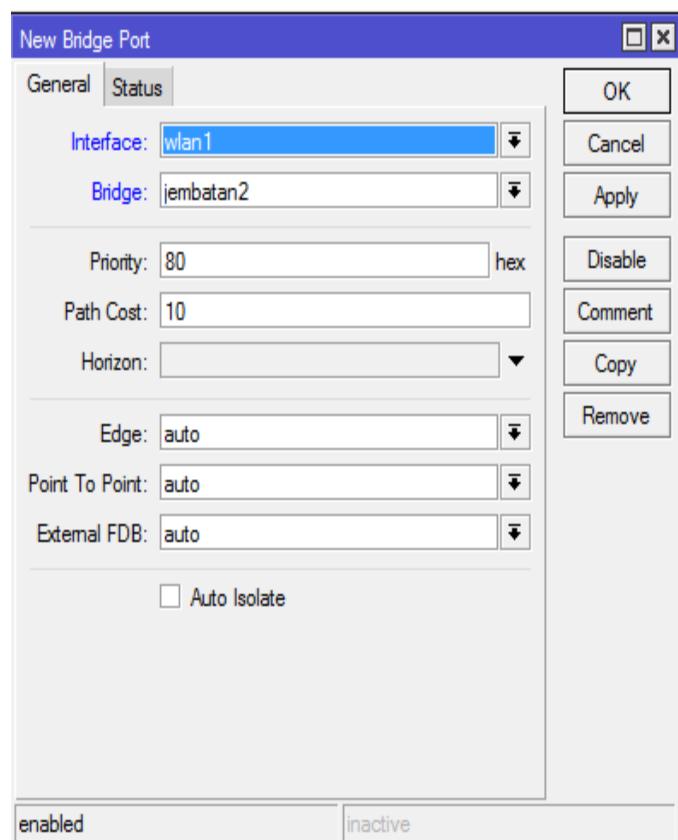
Konfigurasi di router 2 sebenarnya sama saja seperti di Router 1. Tinggal mengulang saja seperti router 1. Pertama kita buat interface bridge nya



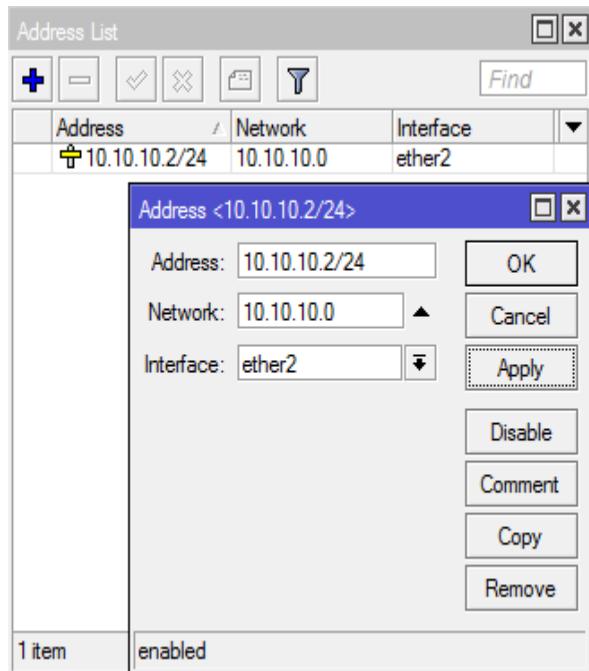
Kemudian kita masukkan interface wlan1 dan ether 2 kedalam interface bridge



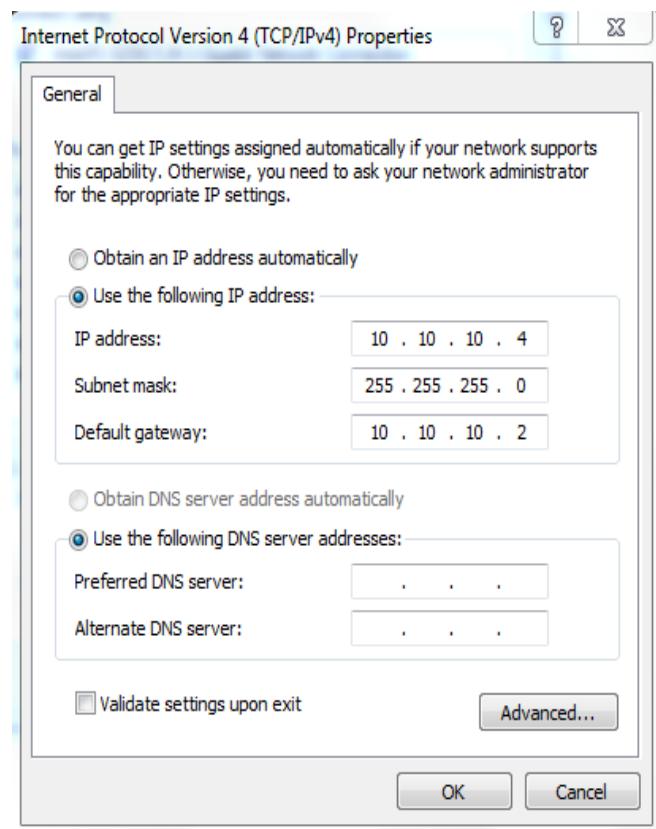
Kemudian masukkan pula interface wlan nya



Setelah itu kita berikan IP address juga untuk interface ether2 nya , harus satu network dengan Router 1 , tapi jangan sampai sama , karena akan bentrok. Ingat di mode Bridge ini kita akan membuat seolah olah Router menjadi Switch



Kemudian konfigurasi IP juga di client nya ,



Selanjutnya coba test ping antar client dan router, pasti akan berhasil. Di sini saya coba ping dari client di Router 1

C:\Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.
C:\Users\IDN>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time=2ms TTL=64
Reply from 10.10.10.2: bytes=32 time<1ms TTL=64
Reply from 10.10.10.2: bytes=32 time<1ms TTL=64
Ping statistics for 10.10.10.2:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
Control-C
^C
C:\Users\IDN>ping 10.10.10.4
Pinging 10.10.10.4 with 32 bytes of data:
Reply from 10.10.10.4: bytes=32 time=3ms TTL=16
Reply from 10.10.10.4: bytes=32 time=1ms TTL=16
Ping statistics for 10.10.10.4:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 2ms
Control-C
^C
C:\Users\IDN>

The screenshot shows a Windows Command Prompt window with two ping sessions. The first session, 'Ke Router 2', pings the IP 10.10.10.2. The second session, 'Ke Client 2', pings the IP 10.10.10.4. Both sessions show successful responses with low latency. Red boxes highlight the output of each session, and arrows point from these boxes to the respective labels 'Ke Router 2' and 'Ke Client 2'.

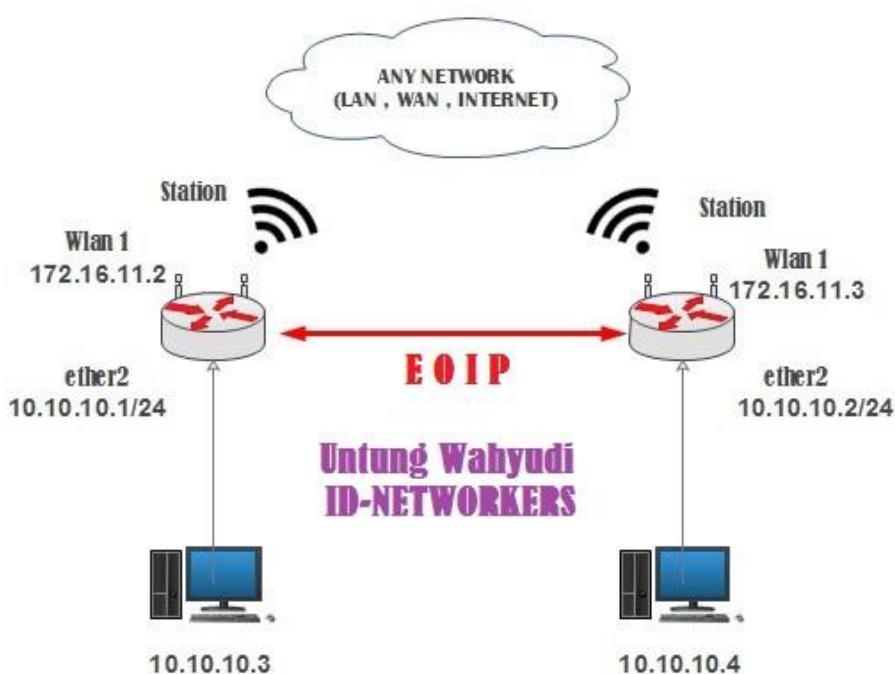
Oke karena sudah berhasil maka saya tutup lab ini dengan mengucap Alhamdulillah

Oke sekian dulu ya mas broo

Wassalam !

Lab 50. EoIP (Ethernet Over IP)

Di Lab sebelumnya kita sudah membahas tentang teknik bridging , yaitu menghubungkan jaringan lokal kita dan router lain menjadi 1 segmen. Namun bagaimana jika yang ingin di bridge adalah 2 jaringan lokal yang terpisah dengan internet ?? Kan gak mungkin kita minta tolong pihak ISP nya buat membridge 2 jaringan kita. Nah maka dari itu kita bisa memanfaatkan fitur EoIP ini. EoIP ini nantinya akan membuat tunnel (terowongan) yang melewati jaringan internet untuk menghubungkan 2 jaringan ini. Biar lebih paham monggo di simak topologi ini



PADA ROUTER 1 :

Oke langsung aja kekonfigurasinya yuk , pastikan router tersebut sudah terkoneksi ke Internet dengan baik , dan sudah diberikan IP ke clientnya

Address List		
<input type="button" value="+"/>	<input type="button" value="-"/>	<input type="button" value="✓"/>
<input type="button" value="✗"/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>
<input type="button" value="Filter"/>	<input type="text" value="Find"/>	
Address	Network	Interface
10.10.10.1/24	10.10.10.0	ether2
172.16.11.2/24	172.16.11.0	wlan1
2 items		

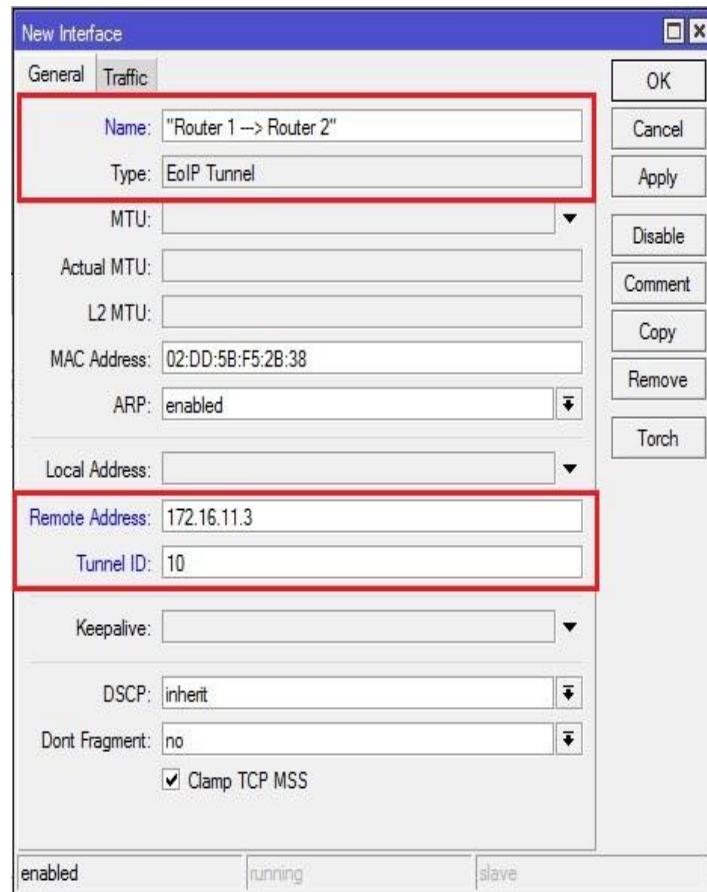
Selanjutnya kita buat Interface EoIP nya. Caranya klik menu **Interface > EoIP Tunnel > Add**

Interface List								
Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	
0 items out of 6								

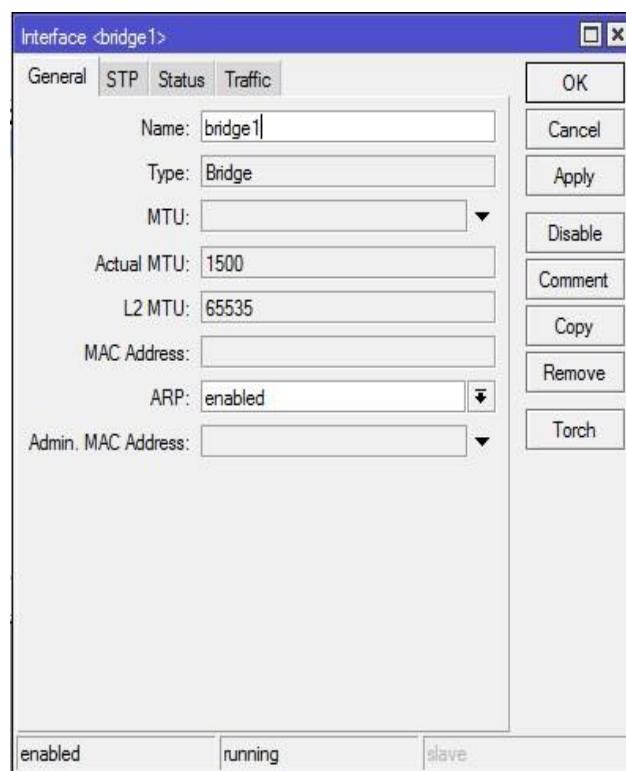
Kemudian isikan namanya bebas. Yang perlu diperhatikan adalah dibagian Remote Address dan Tunnel id.

Remote Address = IP Address Lawan

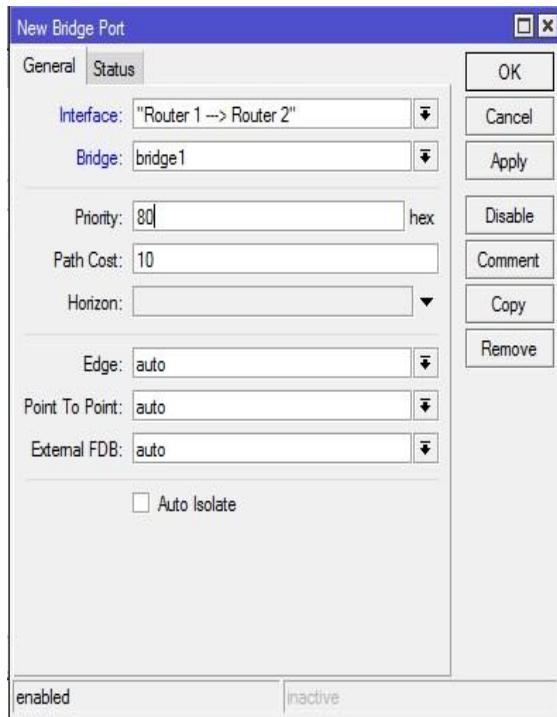
Tunnel ID = harus disamakan dengan Tunnel ID lawan



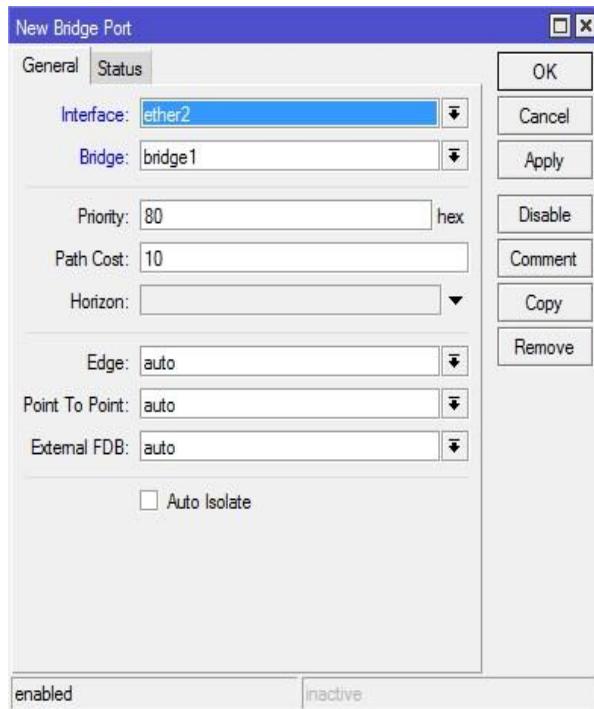
Setelah itu apply dan OK. Kemudian kita akan buat interface bridge nya.



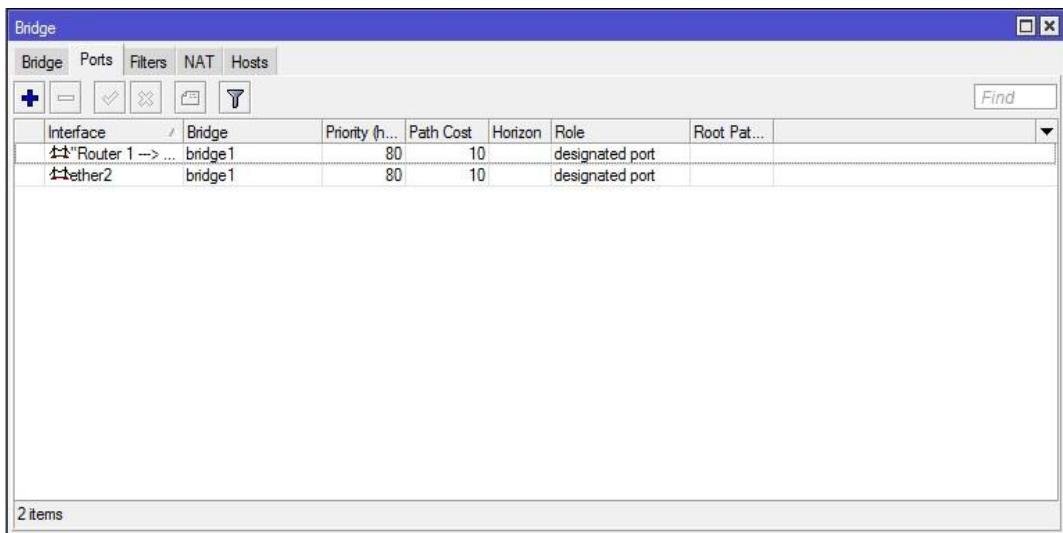
Selanjutnya kita masukkan interface EoIP dan ether2 kedalam interface bridge tersebut. Ini hampir sama seperti lab sebelumnya hanya saja interface yang dimasukan yang berbeda. Klik tab **Ports** > **Add**, kemudian masukkan interface EoIP yang tadi.



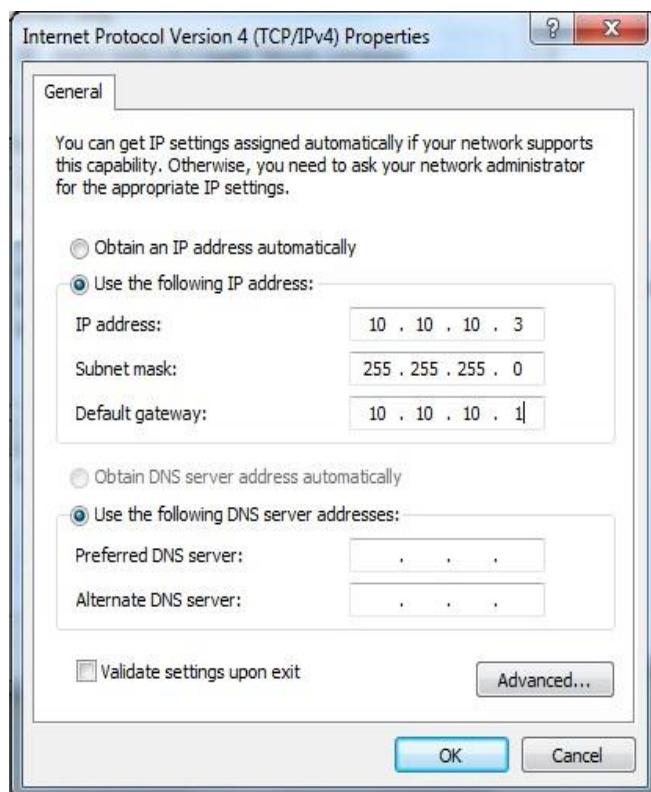
Lalu masukkan juga interface ether2 nya.



Maka hasilnya akan seperti ini .

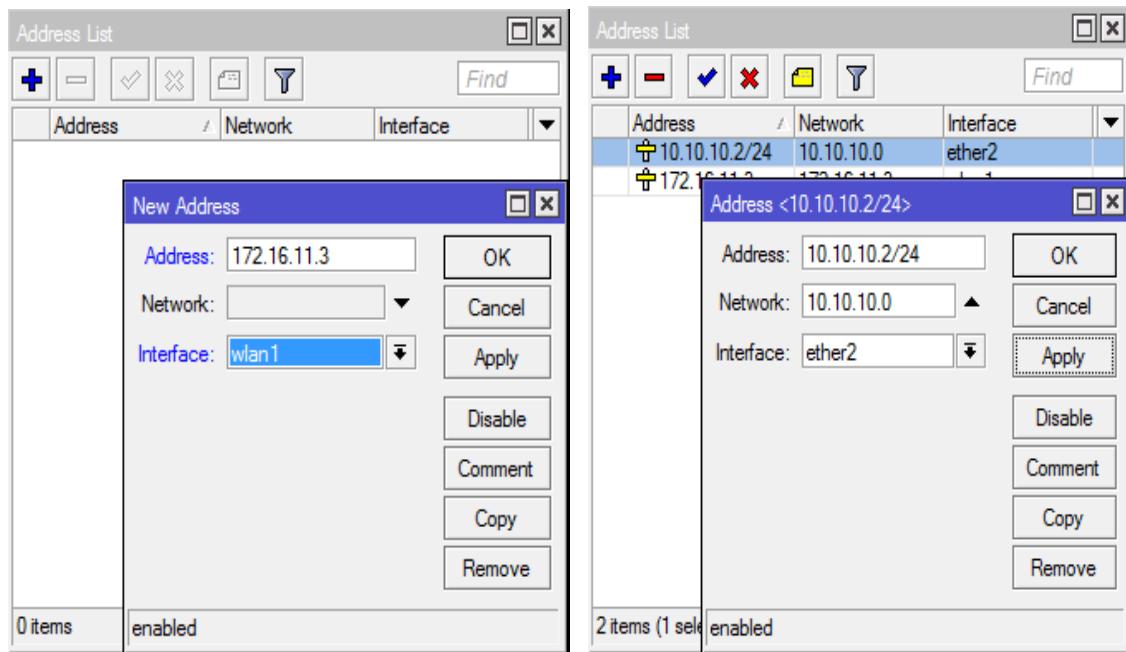


Kemudian di sisi client , isikan IP nya menjadi 1 network , sama halnya seperti lab sebelumnya.

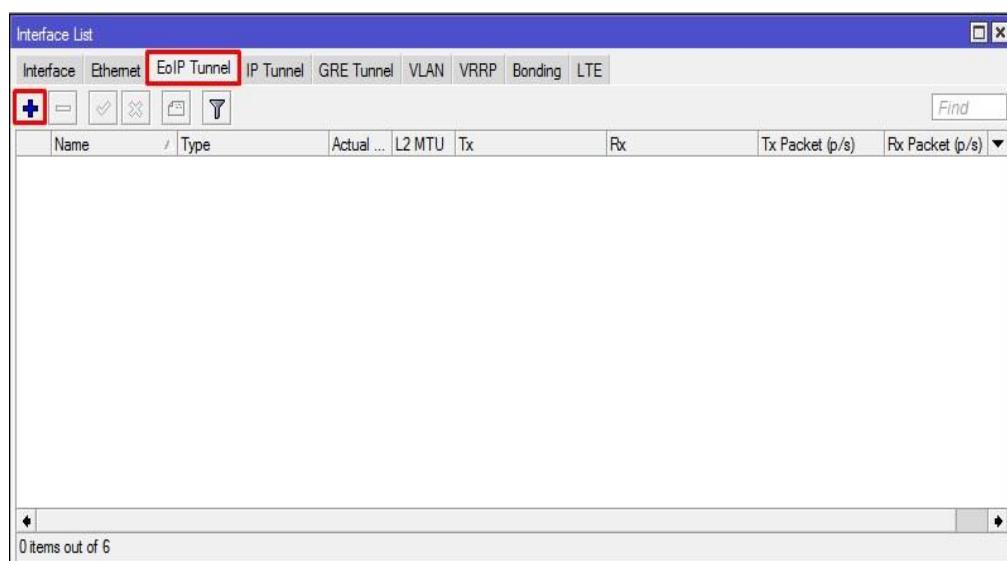


PADA ROUTER 2 :

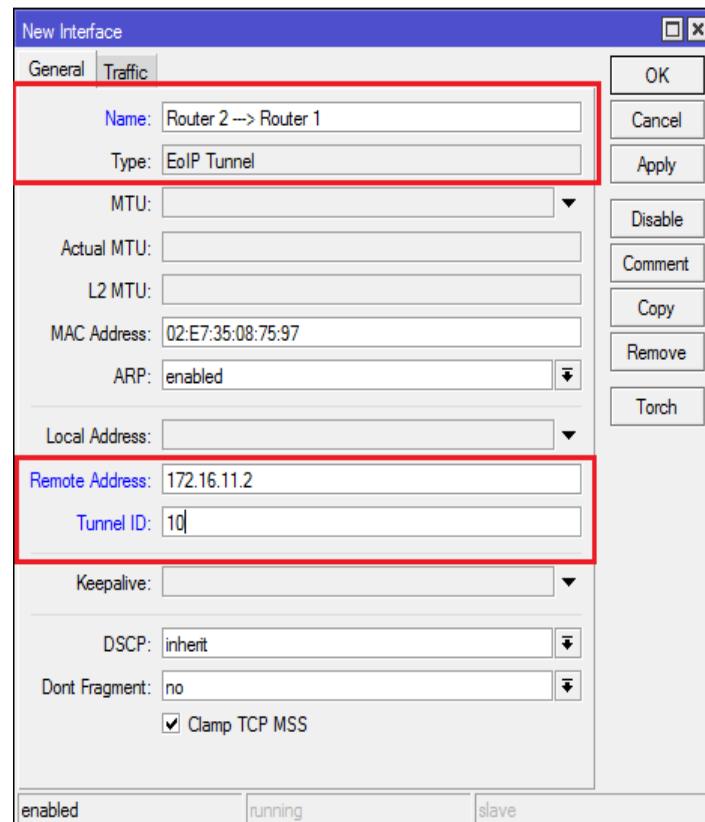
Di router 2 konfigurasinya masih sama seperti di Router 1. Inilah IP address di Router 2



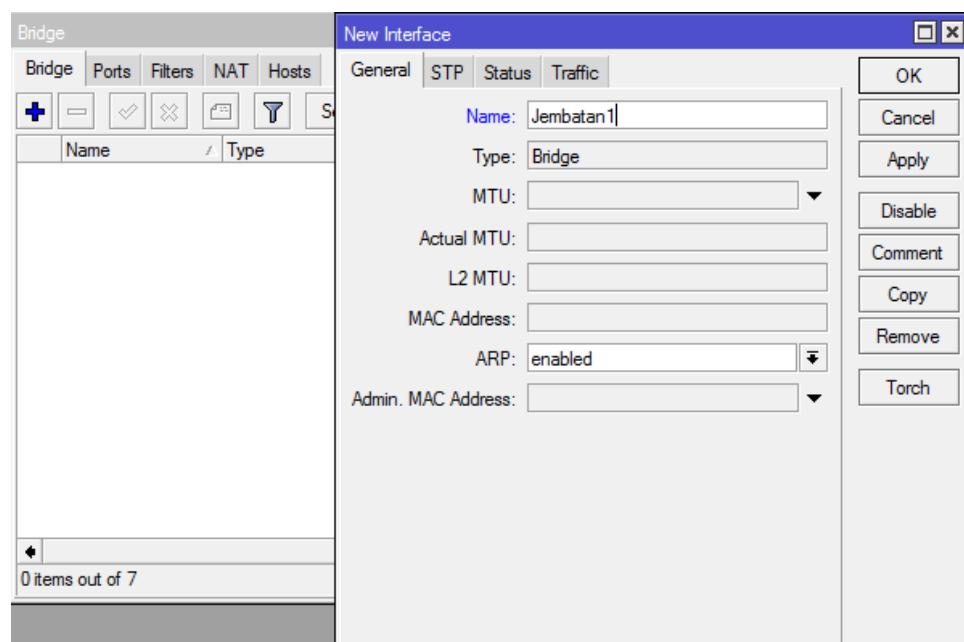
Selanjutnya kita buat interface EoIP nya , seperti di router 1. klik menu
Interface > EoIP Tunnel > Add



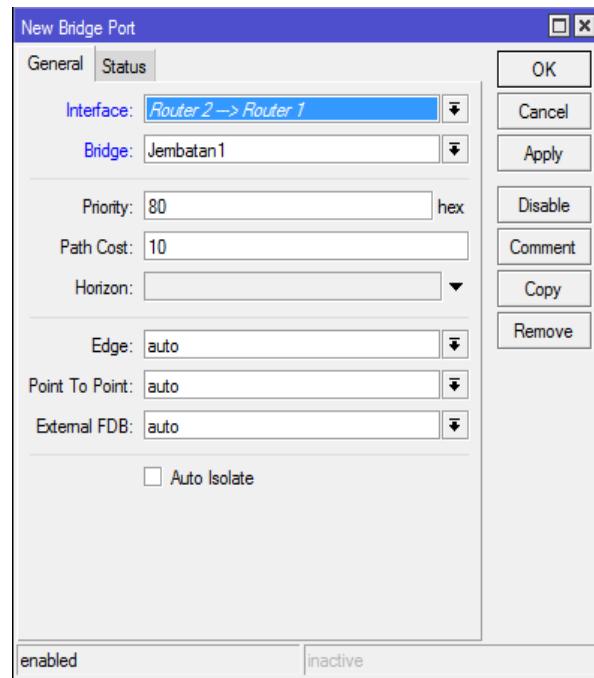
Kemudian masukkan rule nya seperti sebelumnya , di bagian Remote Address isikan alamat IP Router 1. Tunnel Id nya pun disamakan dengan tunnel id di router 1



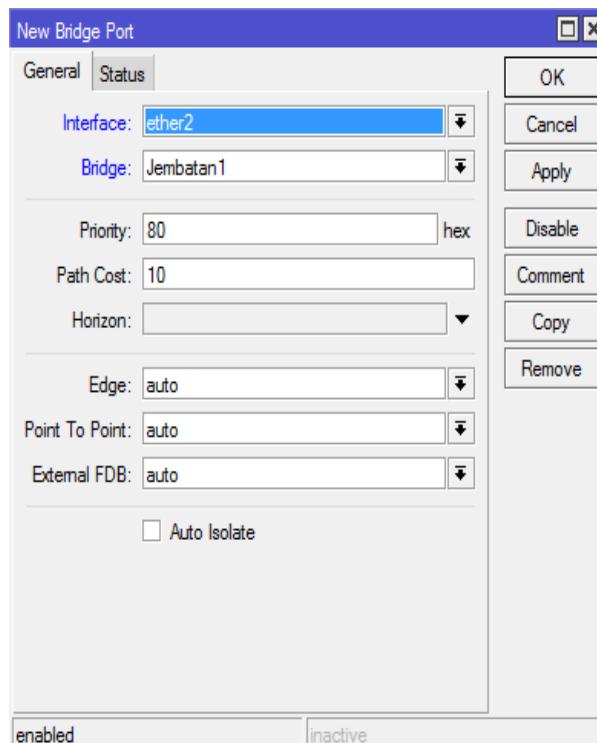
Selanjutnya buat interface bridge nya , klik menu bridge > add , lalu buat dengan nama bebas



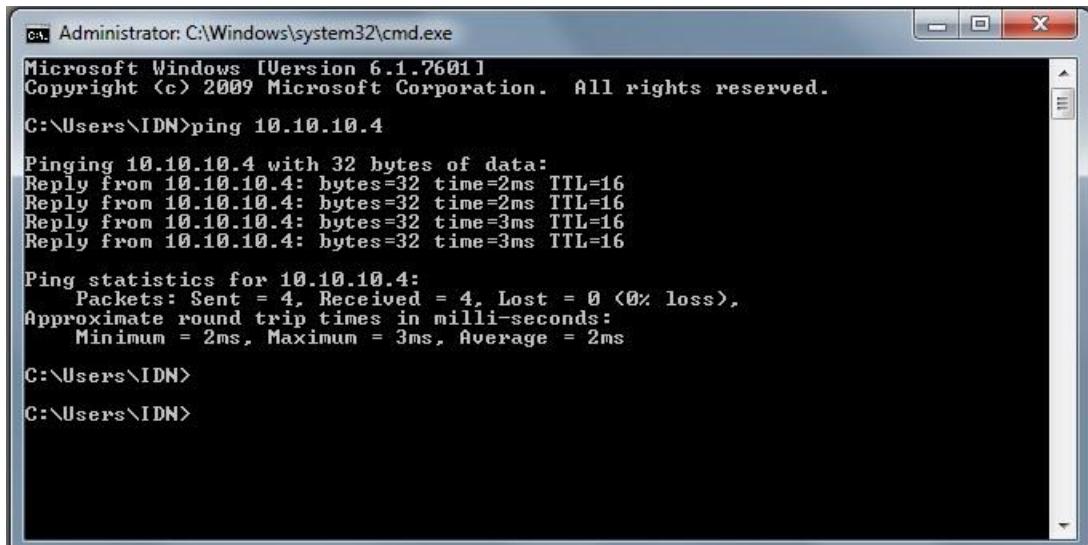
Kemudian masukkan interface EoIP kedalam interface bridge , klik tab Port , kemudian masukkan interface EOIP nya



Masukkan pula interface ether2 nya



Sampai sini maka konfigurasi EoIP sudah selesai. Selanjutnya tinggal test ping antar client dan router. Maka hasilnya 2 jaringan lokal tersebut sudah bisa terkoneksi satu sama lain. Test ping dari client di Router 1 ke client di router 2



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IDN>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:
Reply from 10.10.10.4: bytes=32 time=2ms TTL=16
Reply from 10.10.10.4: bytes=32 time=2ms TTL=16
Reply from 10.10.10.4: bytes=32 time=3ms TTL=16
Reply from 10.10.10.4: bytes=32 time=3ms TTL=16

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\IDN>
C:\Users\IDN>
```

Oke karena sudah berhasil maka saatnya saya bilang , Alhamdulillah

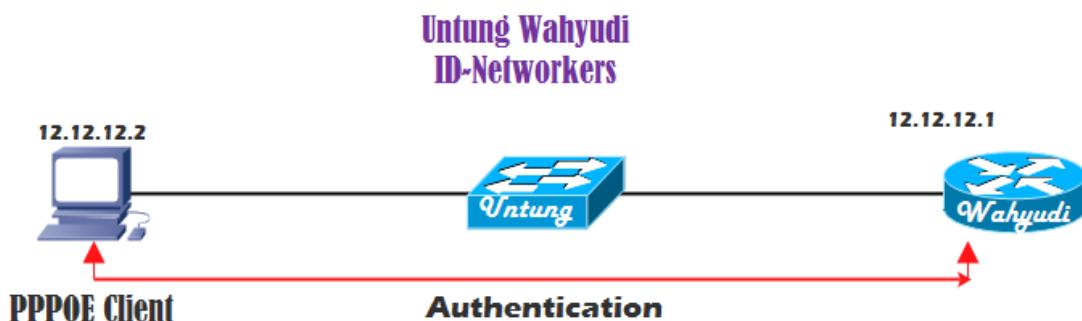
Oke mas dan mba bro sekian dulu yaa

Wassalam !

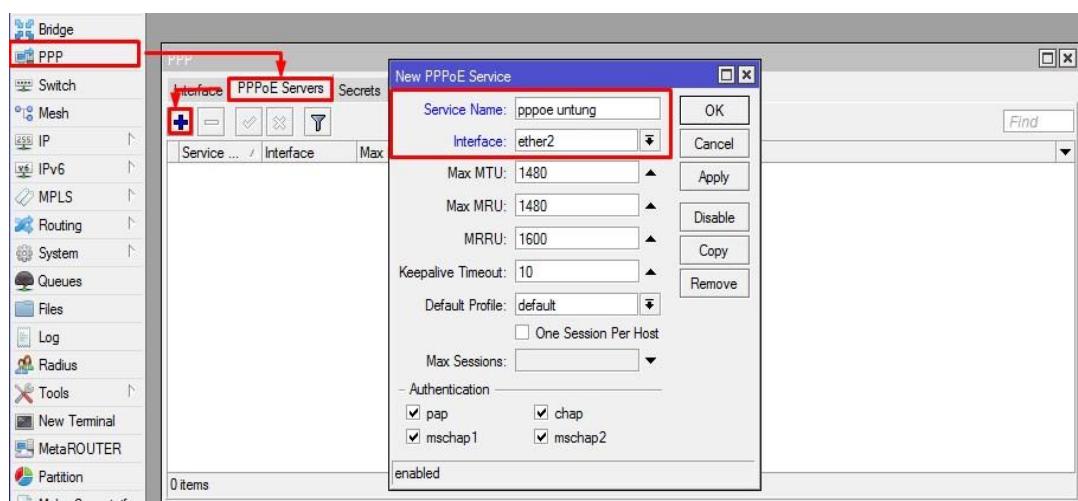
Lab 51. PPPoE (Point to Point Over Ethernet)

Assalamualaikum wr.wb

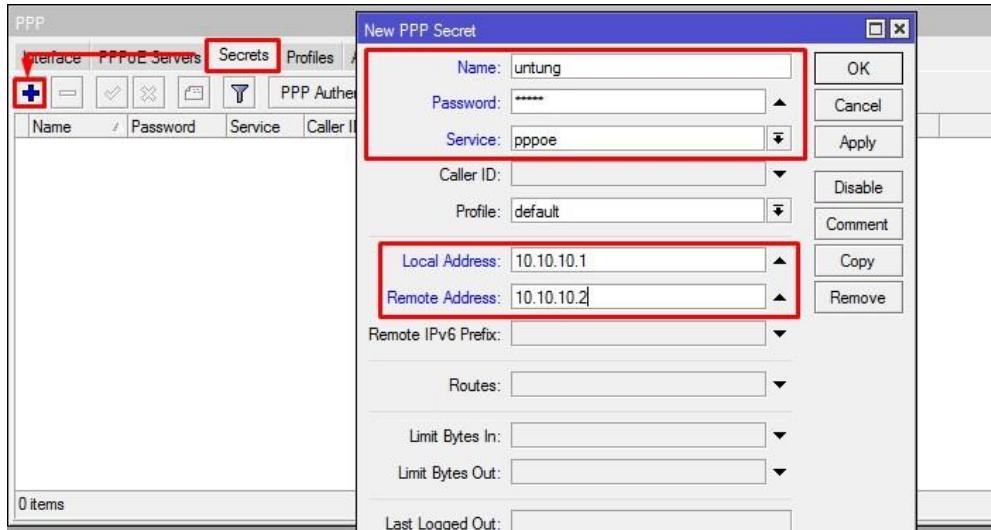
Masih lanjut lagi ternyata materinya masih ada , di lab ini saya mau ngebahas masalah PPPoE. PPPoE ini adalah pengembangan dari PPP (Point to Point Protocol) , jika PPP biasanya menggunakan serial modem , maka PPPOE ini melalui media Ethernet. Jadi dengan PPPoE ini , nantinya setiap client yang terhubung ke router harus memiliki authentikasi. Jadi paket data yang dikirim akan di enkapsulasi , jadi paket tersebut akan susah diketahui oleh client lain , karena setiap client yang akan berkomunikasi harus melewati router terlebih dahulu. Kurang lebih topologi nya seperti ini.



Oke karena sudah tau topologinya sekarang ke konfigurasinya saja , yang pertama harus dilakukan adalah menaktifkan layanan PPPoE server , caranya klik menu **PPP > PPPoE Servers > Add** , kemudian dibagian **interface** kita arahkan menuju **ether** yang terhubung ke client.



Selanjutnya kita akan buat ppp secret , ppp secret ini berisi username dan password yang nantinya digunakan oleh client. Caranya klik tab **Secrets** di menu PPP tadi



Keterangan :

Name : username yang akan digunakan client

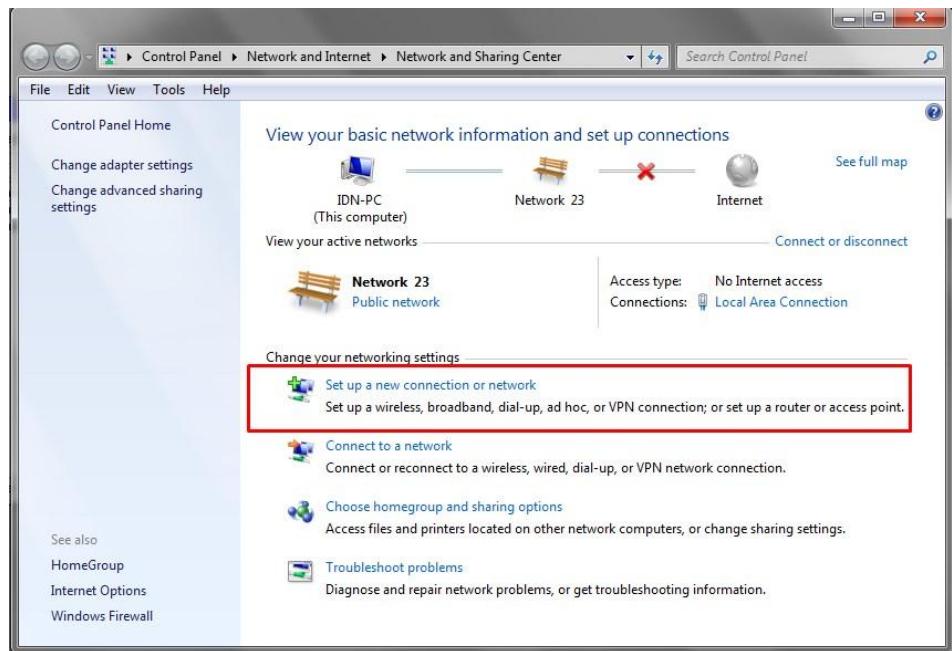
Password : Password dari user tersebut

Service : Layanan yang digunakan untuk ppp secret ini , kita bisa saja isikan **any**

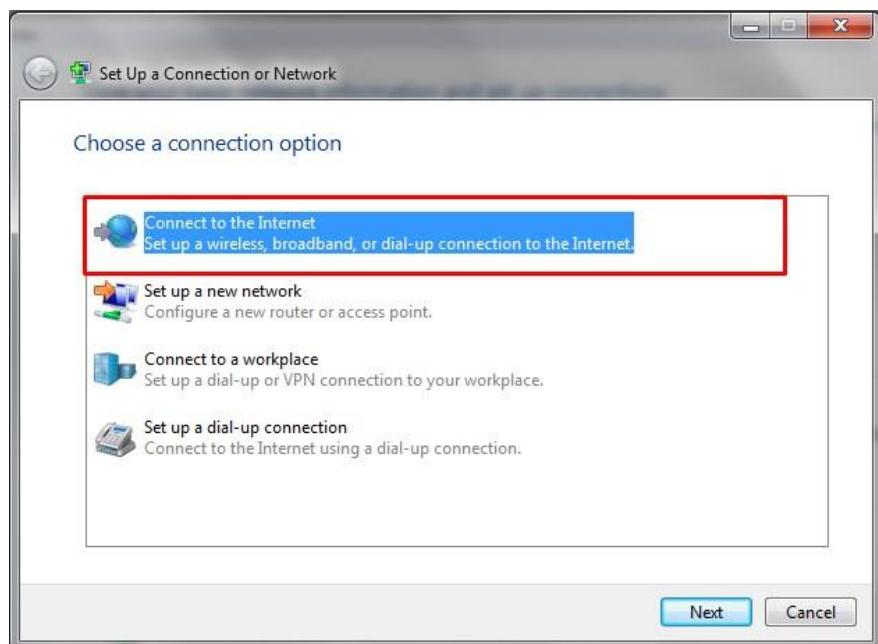
Local Address : IP yang digunakan router untuk Point to Point nya

Remote Address : IP yang diberikan ke client

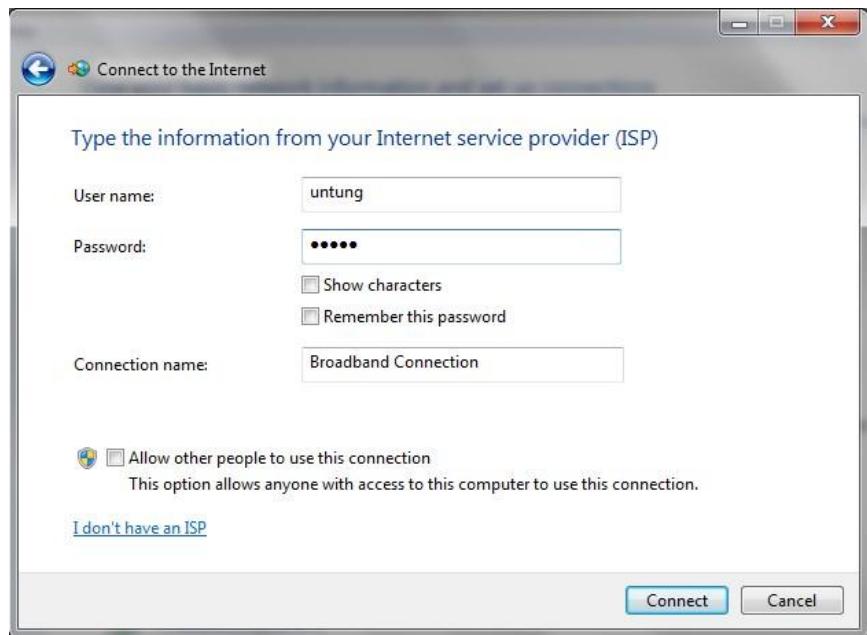
Selanjutnya kita lakukan pengetasan di sisi client , di sini saya menggunakan OS Windows 7 , caranya adalah kita ke bagian **Network And Sharing Center** , kemudian klik **Setup a new connection or network**.



Lalu akan muncul tampilan seperti dibawah ini , kita pilih Broadband(PPPOE)



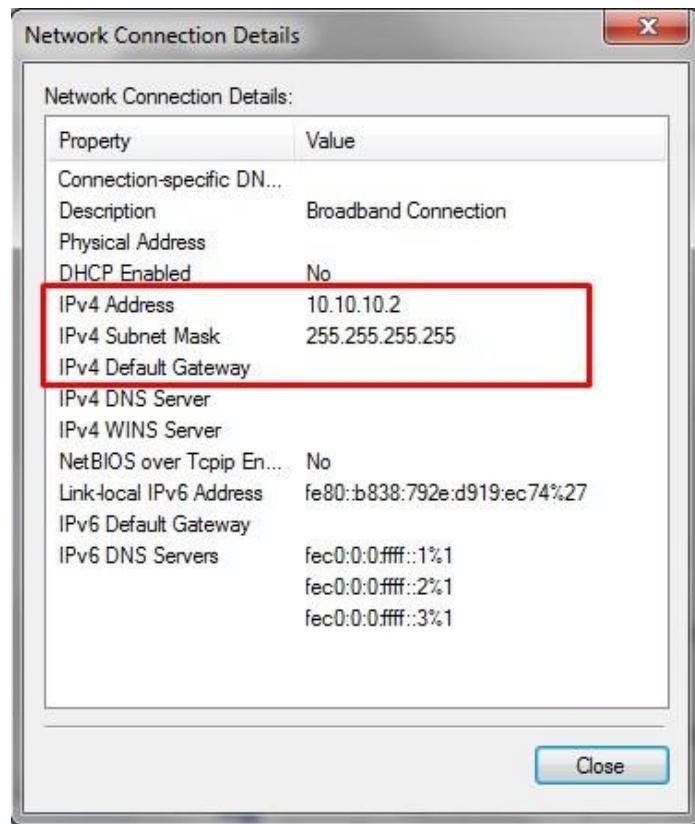
Kemudian akan muncul tampilan Authentication , isikan username dan password nya sesuai yang sudah dibuat di PPP Secrets,



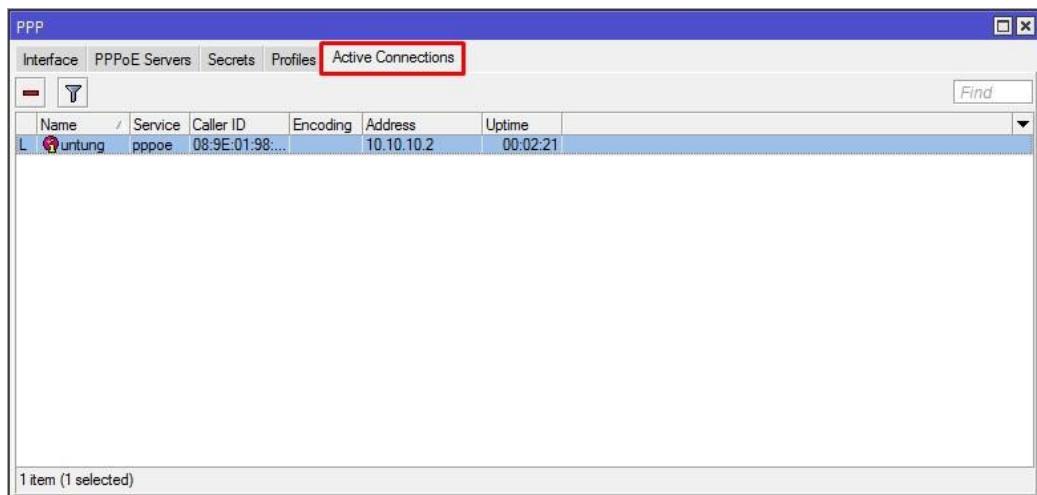
Setelah selesai maka akan muncul adapter **Broadband Connection** baru di **Network Connection**



Kemudian bila kita cek IP nya maka akan mendapat IP **10.10.10.2** , sesuai yang tadi sudah dibuat di **Remote Address**



Kita bisa juga memonitor client mana saja yang terkoneksi ke Broadband kita dari Router , caranya klik tab **Active Connections**



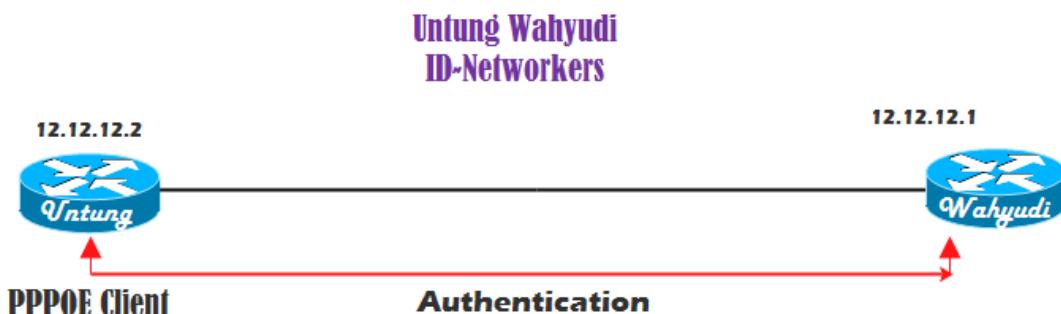
Oke sekian dulu yaa mas bro tentang PPPOE nya , oh ya sedikit tambahan karena ini namanya Point to Point jadi untuk setiap client yang terhubung kita buat PPP Secret untuk masing masing client , begitu juga **Remote Address** nya , meskipun kita bisa saja menggunakan fitur ip pool.

Oke semoga bermanfaat
Wassalam !

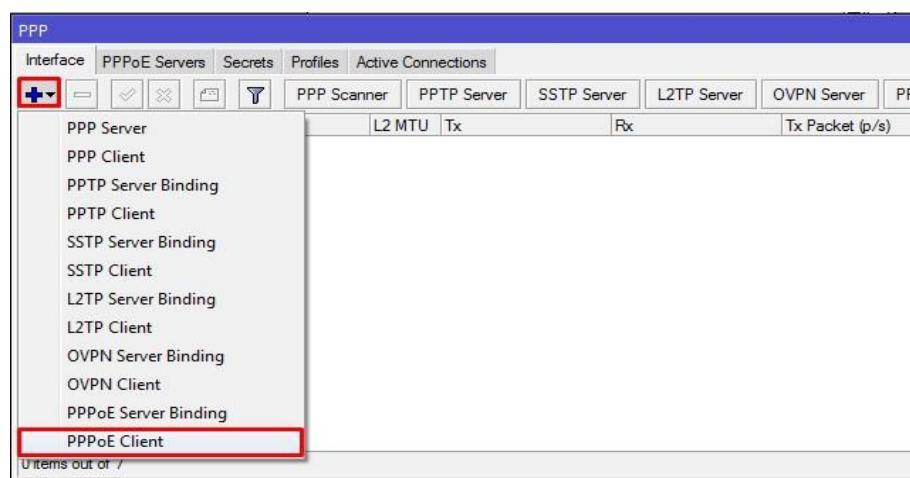
Lab 52. Mikrotik sebagai PPPOE Client

Assalamualaikum wr.wb

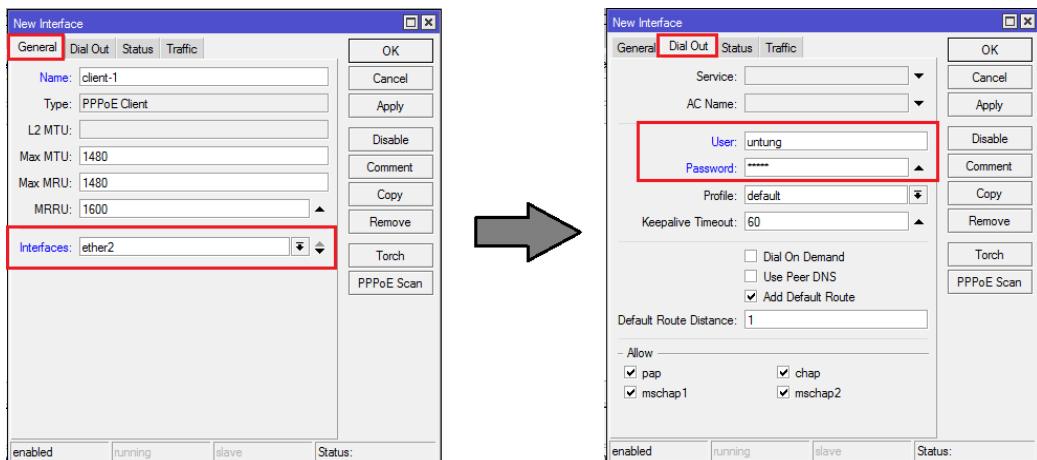
Masih lanjut yoo tentang PPPOE nya , kalo di lab sebelumnya client nya itu berupa PC atau Laptop , maka di Lab ini kita akan membuat Mikrotik sebagai client PPPOE nya, Ini masih melanjutkan dari lab sebelumnya yoo , kurang lebih topologi nya seperti ini



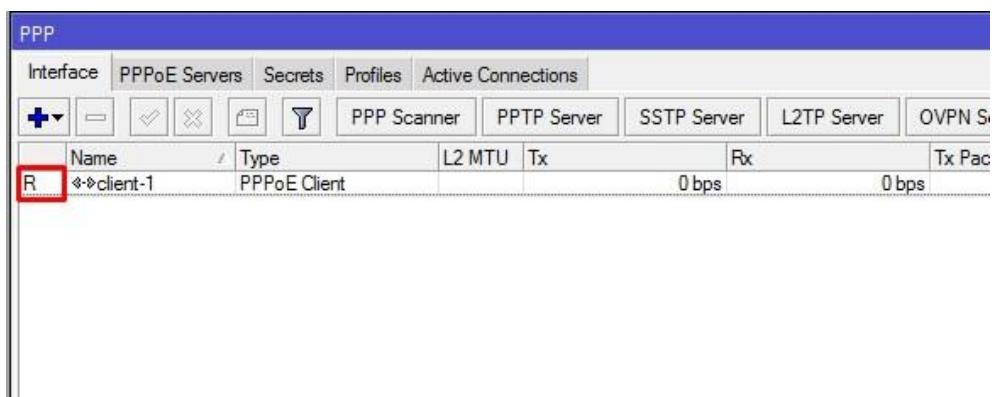
Untuk masalah konfigurasi server kita masih menggunakan konfigurasi sebelumnya , jadi disini hanya konfigurasi Client nya saja. Untuk konfigurasi client pertama kita klik menu **PPP > Interface > Add** kemudian pilih yang **PPPOE Client**



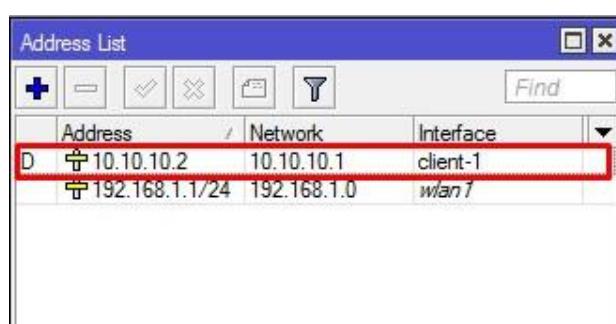
Setelah itu di tab general kita isikan name nya bebas , lalu di bagian **interface** , pilih interface yang terhubung ke Server. Lalu di tab **Dial Out** kita masukkan username dan password yang tadi dibuat di PPPOE Server (*Di lab sebelumnya*)



Jika sudah maka hasilnya akan seperti ini , akan muncul lambang R , yang artinya Running



Kemudian silahkan cek IP nya , maka akan mendapat IP PPPOE di interface pppoe client



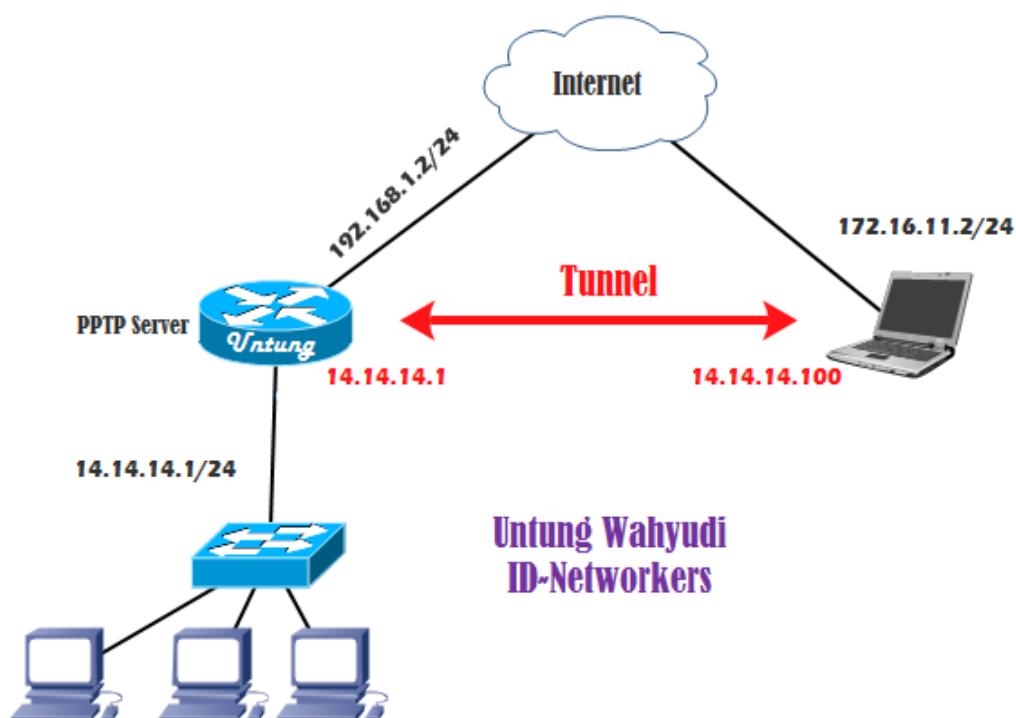
Oke karena sudah mendapat IP artinya sudah berhasil
Sekian dulu yoo

Wassalam !

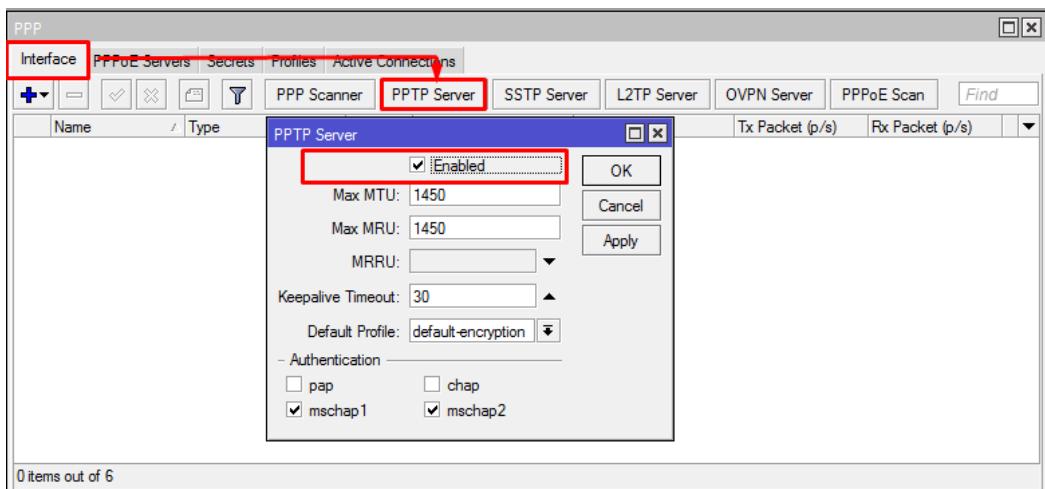
Lab 53. PPTP (Point to Point Tunneling Protocol)

Assalamualaikum wr.wb

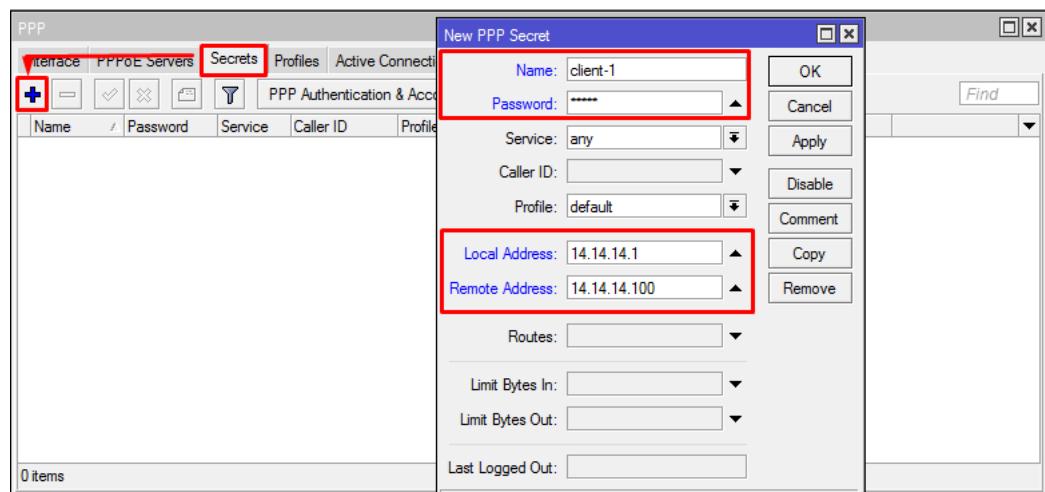
Di lab sebelumnya saya sudah menjelaskan mengenai teknik tunnel. Yang mana jika kita menerapkan teknik ini maka nantinya paket data akan di enkapsulasi. Di Lab ini akan membahas lagi masalah Tunnel , yaitu PPTP (Point to Point Tunneling Protocol. PPTP ini adalah salah satu protocol yang digunakan untuk membuat VPN (Virtual Private Network). Sedangkan VPN itu sendiri adalah teknik menghubungkan beberapa jaringan local melalui internet dengan cara membuat Tunnel (Terowongan). Di lab ini saya akan membuatnya kurang lebih seperti ini



Oke langsung aja kekonfigurasi nya , pertama kita aktifkan terlebih dahulu layanan atau service PPTP , caranya klik menu **PPP > Interface** kemudian klik di bagian **PPTP Server** , lalu klik **enable**



Setelah itu kita buat ppp secret nya , sama seperti di lab PPPOE , klik tab secret lalu buat seperti ini.



Keterangan :

Name : username yang akan digunakan client

Password : Password dari user tersebut

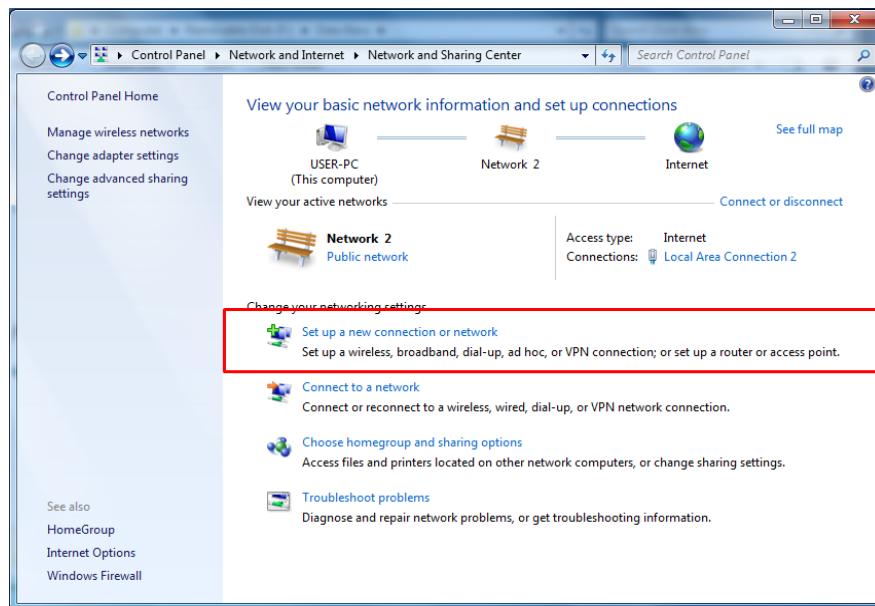
Service : Layanan yang digunakan untuk ppp secret ini , kita bisa saja isikan pptp

Local Address : IP yang digunakan router untuk Point to Point nya

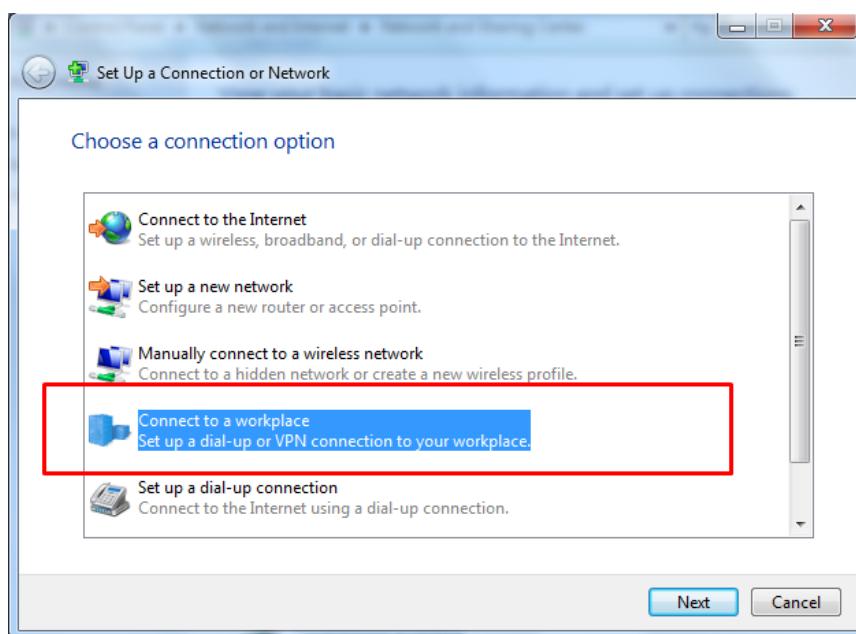
Remote Address : IP yang diberikan ke client

(Disini saya menggunakan IP Jaringan local , bisa saja diganti menjadi IP yang lain)

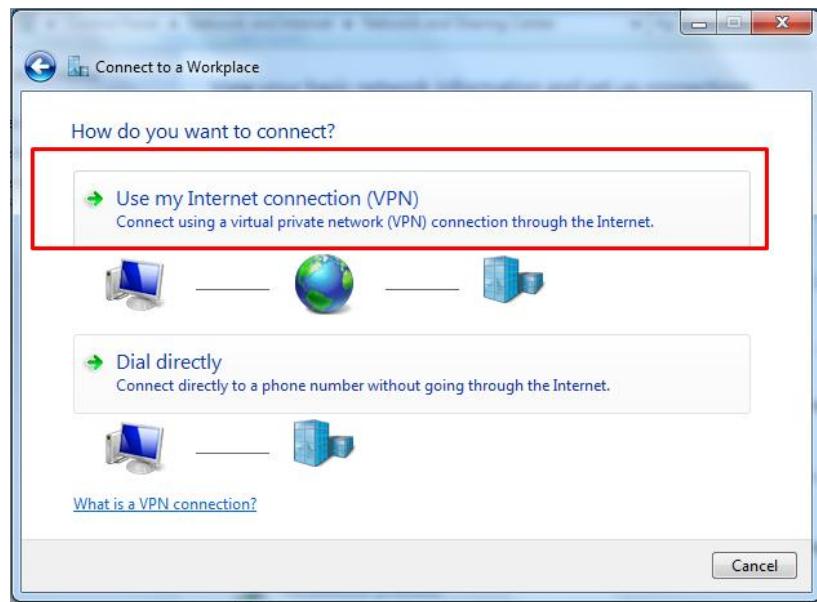
Selanjutnya kita lakukan pengetesan di client , caranya hampir sama seperti di Lab PPPOE , pertama kita ke **Network and Sharing center** , kemudian pilih yang **Setup a new connection or network**.



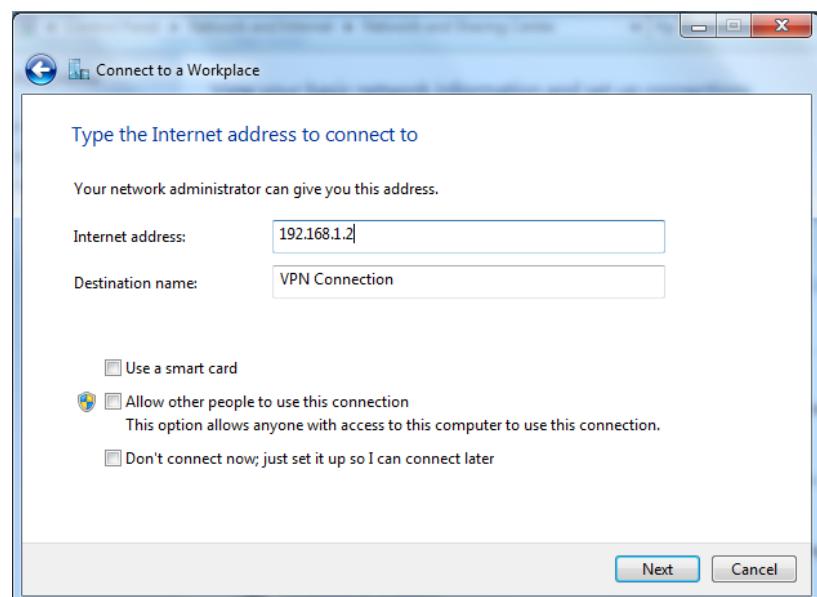
Kemudian kita pilih yang **Connect to a workplace**



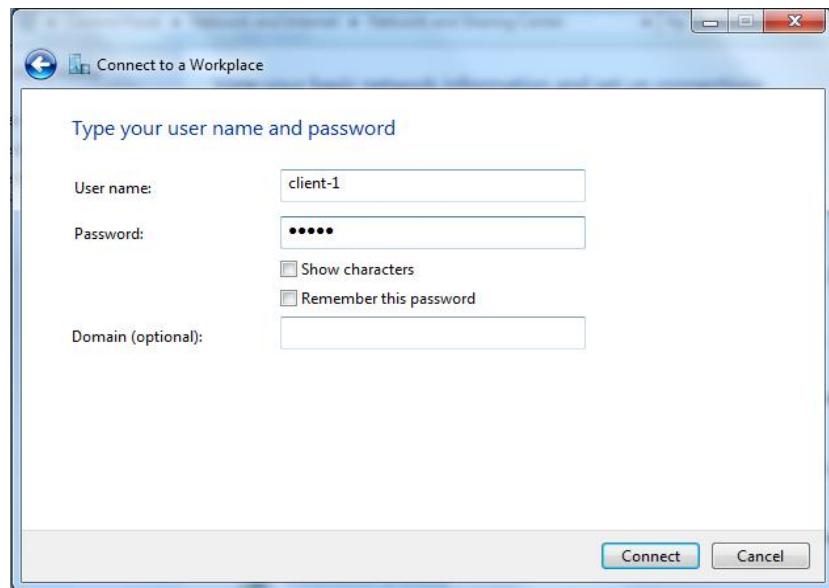
Setelah itu pilih bagian yang **No, Create a New Connection**, sehingga akan muncul bagian berikut , kita pilih yang **Use my Internet Connection (VPN)**



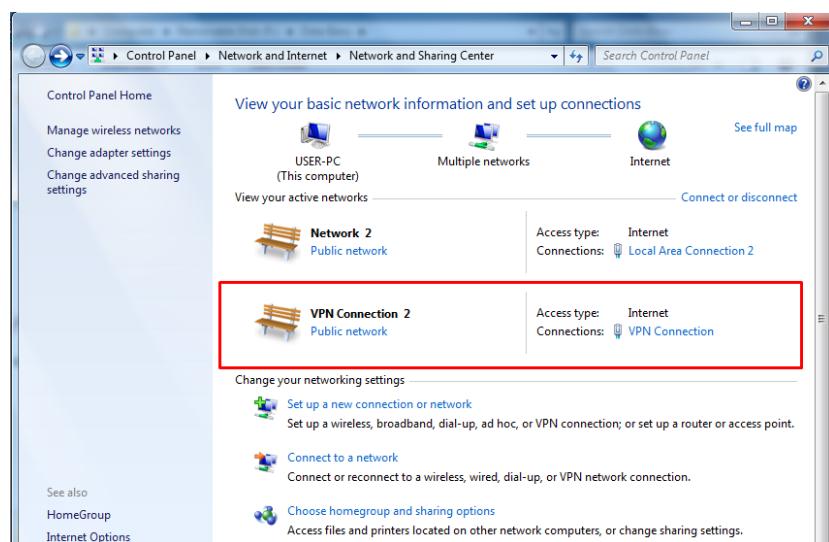
Setelah itu kita masukkan IP Public dari PPTP Server , yaitu 192.168.1.2



Setelah itu akan muncul tab Authentication , kita isikan username dan password yang tadi sudah kita buat di ppp secrets



Setelah selesai maka akan muncul adapter VPN Connection.



Oke kalau sudah muncul gambar diatas artinya sudah berhasil, karena sudah berhasil maka saatnya saya untuk bilang Alhamdulillah

Oke sekian dulu yaa , semoga bermanfaat

Wassalam !