

BIODATA PENULIS

Nama : Faris Jawad
TTL : Cikarang, 06 April 2001
Alamat : Perumahan Mutiara Bekasi Jaya blok B7 no 7
Email : farisjwd@gmail.com
Sosmed : Fb = facebook.com/zawad97
Ig = @javad_zawad
Blog : farisjwd.wordpress.com
Cita-cita : Network Engineer
Karya : Buku "10 SuperLab Cisco" - Desember 2016
Buku "MI-8291" - Maret 2017
Sertifikasi : MTCNA (Mikrotik Certified Network Associate) - 1609NA865
MTCRE (Mikrotik Certified Routing Engineer) - 1611RE160

✓ SEJARAH MIKROTIK



MikroTik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentuknya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang Amerika yang berimigrasi ke Latvia. Di Latvia ia berjumpa dengan Arnis seorang sarjana Fisika dan Mekanik sekitar tahun 1995. John dan Arnis mulai me-routing dunia pada tahun 1996, misi MikroTik sendiri yaitu me-routing seluruh dunia. Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.



Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah

membantu negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna. Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staff Research and Development (R&D) MikroTik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka juga merekrut tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan MikroTik secara marathon. Router MikroTik didesain dengan system modular, sehingga dimungkinkan untuk menambah interface wireless sesuai dengan kebutuhan, hingga sebanyak jumlah slot minipci yang tersedia. Processor dan memori yang tersedia sebanding dengan kemampuan routerboard untuk mengalirkan koneksi data, baik sesuai dengan bps (bit per second) maupun pps (packet per second) nya.

✓ Jenis, Arsitektur dan Tipe MikroTik

• Jenis MikroTik

» MikroTik RouterOS™

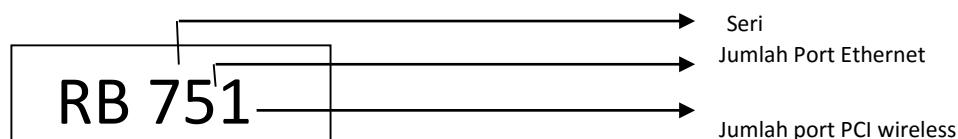
- Software untuk mengubah PC biasa menjadi sebuah Router yang handal.
- Berbasis Linux
- Diinstall sebagai Sistem Operasi

» MikroTik RouterBoard

- Built in hardware (board) yang menggunakan RouterOS sebagai Operating Sistemnya.
- Tersedia mulai low-end s/d high-end Router.

• Tipe RouterBoard

RouterBoard memiliki sistem kode tertentu



Kode Lain ada di belakang tipe

U - dilengkapi port USB

A - Advanced, biasanya diatas lisensi level 4

H - Hight Performance, processor lebih tinggi

R - dilengkapi wireless card embedded.

G - dilengkapi port ethernet Gigabit

RB 751U 2HnD = RouterBoard Seri 7, dengan 5 port ethernet, 1 port wireless, USB, Hight Performance, Dual Chain

Seri sebuah router ditentukan oleh arsitektur hardwarenya

» Arsitektur RouterBoard

Arsitektur RouterBoard dibedakan berdasarkan jenis dan kinerja processor, software/OS untuk setiap arsitektur berbeda

routeros-mipsle (<i>mipsle</i>)	combined package for mipsle (RB100, RB500) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-mipsbe (<i>mipsbe</i>)	combined package for mipsbe (RB400) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-powerpc (<i>ppc</i>)	combined package for powerpc (RB300, RB600, RB1000) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-x86 (<i>x86</i>)	combined package for x86 (Intel/AMD PC, RB230) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
mpls-test (<i>mipsle, mipsbe, ppc, x86</i>)	Multi Protocol Labels Switching support improvements
routing-test (<i>mipsle, mipsbe, ppc, x86</i>)	routing protocols (RIP, OSPF, BGP) improvements

Mips (Microprocessor without Interlocked Pipeline Stages), adalah jenis processor yang dikembangkan oleh MIPS Computer Systems, Inc. Pada Mikrotik ada 2 jenis mips yaitu mipsle (mips - little endian) dan mipsbe (mips - big endian), endian / endianness adalah istilah yang menggambarkan urutan urutan byte yang disimpan dalam memori komputer, misal MikroTik disimpan dengan urutan kiTorkiM.

✓ Fitur MikroTik

1. **Address List:** merupakan kumpulan kelompok IP Address yang berdasarkan nama
2. **Bridge:** seperti namanya yang ini mempunyai fungsi untuk bridge spinning' tree dan multiple bridge interface bisa juga untuk bridging firewalling
3. **Data Rate Management:** merupakan QoS yang memiliki dasar HTB yang menggunakan:

- burst
- PCQ
- RED
- SFQ
- FIFO queue
- CIR
- MIR
- limit antar peer to peer

4. Asynchronous : mempunyai dukungan untuk serial PPP dial-in atau dial-out, memiliki otentikasi CHAP,PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.

5. Bonding: mengkombinsaikan beberapa ethernet dalam satu pipa pada koneksi yang sangat cepat.

6. DHCP: support DHCP tiap antarmuka :

- DHCP Relay
- DHCP Client,
- multiple network DHCP
- static and dynamic DHCP leases.
- Monitoring penghitungan: mampu menghitung Traffic IP, log, statistik graph

7. NTP: kepanjangan NTP adalah Network Time Protokol yang berguna didalam server dan clients atau bisa juga untuk menganalisis menggunakan GPS system.

8. Point to Point Tunneling Protocol

9. Proxy: kemampuannya untuk Cache FTP dan HTTP proxy server, HTTPS proxy bisa juga untuk transparent proxy DNS dan HTTP, sangat support protokol SOCKS, parent proxy, static DNS.

10. Routing: RIP v1/v2, OSPF v2, BGP v4

11. SDSL: support Single Line DSL, mampu memutuskan suatu jalur koneksi dan jaringan, artinya kita berkuasa jika kita yang pegang settingan ini..

12. Simple Tunnel: Ethernet over IP, untuk konsep EOIP anda bisa lihat di sini.

13. SNMP: Simple Network Monitoring Protocol untuk read only

14. Synchronous:

Firewall dan NAT: support untuk filterisasi koneksi peer to peer, source NAT dan destination NAT. Keunggulan nya adalah kemampuannya dalam memfilter berdasarkan:

- MAC address
- IP address
- Range port
- Protokol IP
- Pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS

15. Hotspot: bagian ini semua sudah tahu, didalamnya memiliki Hotspot gateway dengan otentikasi RADIUS. support untuk limit data, SSL ,HTTPS.

16. IPSec: Fitur yang ada adalah :

- Protokol AH dan ESP untuk IPSec
- MODP Diffie Hellmann groups 1,2,5
- MD5 dan algoritma SHA1 hashing;
- mampu mengalgoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256;
- Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5

17. M3P: merupakan MikroTik Protokol Paket Packer yang digunakan dalam wireless links dan ethernet.

18. ISDN: support untuk ISDN dial in dan dial out. dengan beberapa otentikasi dibawah ini : PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius.

supporting 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.

19. MNDP: merupakan MikroTik Discovery Neighbour Protokol, seperti kebanyakan mempunyai dukungan untuk Cisco Discovery Protokol (CDP).

20. Tool: seperti pada umumnya sebuah router biasa, disini juga dapat test Ping, Trace route, bandwidth test, ping flood, telnet, SSH, packet sniffer, Dinamik DNS update.

21. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.

22. WinBox: sebuah aplikasi untuk remote dan mengkonfigurasi MikroTik itu sendiri

✓ Level MikroTik

Mikrotik bukanlah perangkat lunak yang gratis jika anda ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari MikroTikls untuk dapat menggunakanya alias berbayar. Mikrotik dikenal dengan istilah Level pada lisensinya. Tersedia mulai dari Level 0 kemudian 1, 3 hingga 6, untuk Level 1 adalah versi Demo Mikrotik dapat digunakan secara gratis dengan fungsi-fungsi

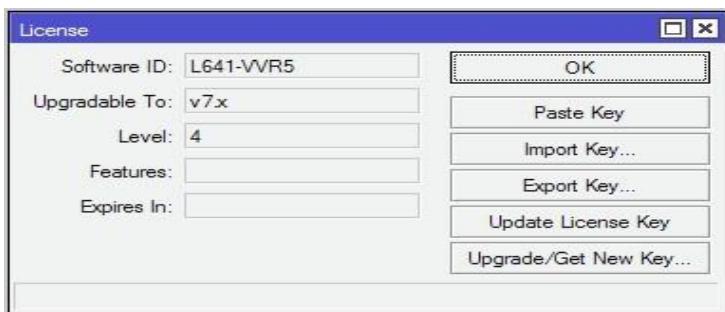
yang sangat terbatas. Tentunya setiap level memiliki kemampuan yang berbeda-beda sesuai dengan harganya, Level 6 adalah level tertinggi dengan fungsi yang paling lengkap.

»Berikut Adalah Jenis Level Lisensi Dalam Mikrotik:

- **Level 0 (gratis):** tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- **Level 1 (demo):** pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
- **Level 3:** sudah mencakup level 1 ditambah dengan kemampuan untuk menajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau Ethernet dan pengelolan perangkat wireless tipe klien.
- **Level 4:** sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe akses poin.
- **Level 5:** mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
- **Level 6:** mencakup semua level dan tidak memiliki limitasi apapun.

Pada MikroTik RouterOS, Lisensi dapat dilihat pada menu License

- Klik System > License



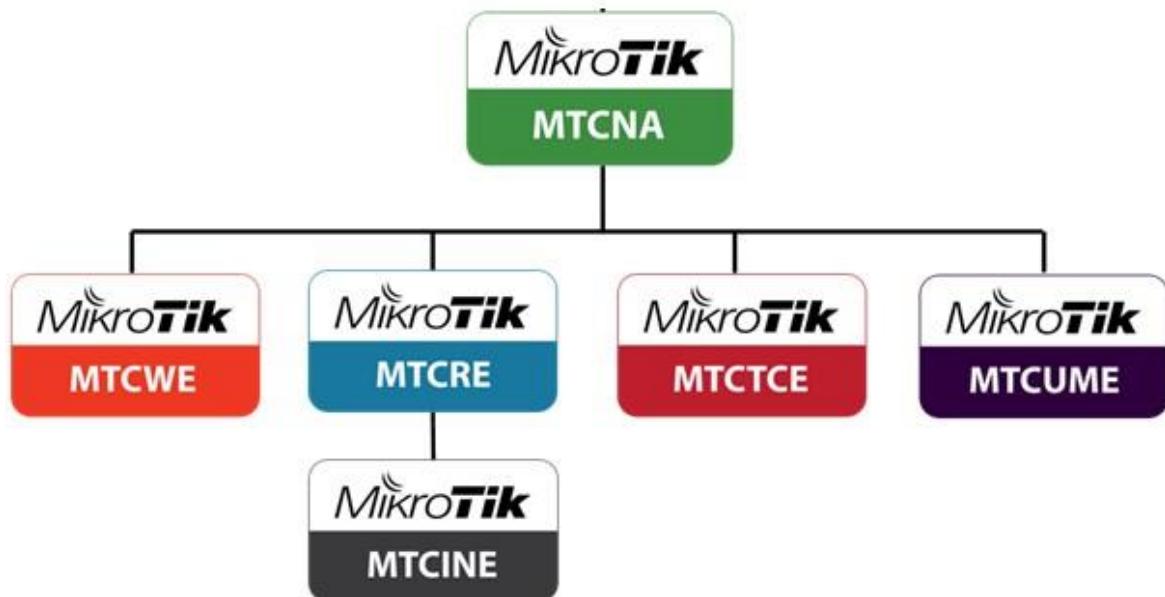
Level Licensi MikroTik dapat dilihat pada table berikut:

Level number	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key ↗	registration required ↗	volume only ↗	\$45	\$95	\$250
Upgradable To	-	no upgrades	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes(*)	yes	yes	yes
EoIP tunnels	24h limit	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200	200	500	unlimited
PPTP tunnels	24h limit	1	200	200	500	unlimited
L2TP tunnels	24h limit	1	200	200	500	unlimited
OVpn tunnels	24h limit	1	200	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
Synchronous interfaces	24h limit	-	-	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Misal untuk lisensi FREE, dapat didownload langsung dari website resminya namun mikrotik hanya bisa digunakan selama 24 jam, setelah itu fitur-fiturnya

tidak dapat digunakan lagi. Apabila ingin memperpanjang maka harus upgrade ke versi diatasnya. Sedangkan untuk lisensi DEMO hanya dapat diakses melalui website demo.mt.lv.

JENJANG SERTIVIKASI MIKROTIK



- Mikrotik Certified Network Associated (MTCNA)
- Mikrotik Certified Wireless Engineer (MTCWE)
- Mikrotik Certified Routing Engineer (MTCRE)
- Mikrotik Certified Traffic Control Engineer (MTCTCE)
- Mikrotik Certified User Management Engineer (MTCUME)
- Mikrotik Certified Inter-Networking Engineer (MTCINE)

Dari Beberapa Sertifikat Di atas, Alhamdulillah saya Telah Mendapatkan Dua Sertifikat: MTCNA dan MTCRE

MTCNA



Sertifikat **MTCNA** adalah Sertifikat Pertama yang saya dapatkan Di SMK ini,Sertifikat **MTCNA** ini Saya dapatkan dengan Nilai 69 ketika saya telah Belajar 3 bulan Di SMK MadinatulQuran,Untuk Belajar **MTCNA** saya di beri waktu oleh guru saya hanya 3 hari...

Ketika Exam **MTCNA** jumlah soal nya adalah 25 soal dan diberi waktu hanya 60 menit

Alhamdulillah walaupun waktu untuk belajar nya tidak terlalu banyak saya bisa lulus sertifikasi MTCNA 😊

MTCRE



Ini adalah Sertifikat **MTCRE**, Sertifikat **MTCRE** adalah Sertifikat ke dua yang saya dapatkan di SMK MadinatulQuran

Exam **MTCRE** berisikan Soal tentang Routing ,Jumlah Soal **MTCRE** adalah 25 soal dan diberi waktu 60 menit..

Alhamdulillah Saya bisa lulus sertifikasi **MTCRE** nilai 71 ,saya sangat bersyukur bisa mendapatkan Dua sertifikasi Tersebut, karena saat itu saya sedang dalam Proses belajar Cisco bukan MikroTik.....Semoga saya bisa Meraih Sertifikasi **MTCINE** (Mikrotik Certified Inter Networking Engineer)

BAB 1. BASIC

Lab 1. Akses Mikrotik

Di Lab ini saya akan menjelaskan cara meng-akses RouterBoard yang masih Default (Stelan Pabrik), Di dalam RouterBoard Memiliki setiangan Default Konfigurasi, Yaitu IP Interface Ethernet 1 adalah = 192.168.88.1 dan User Loginnya adalah = User:admin , Password: (Kosong)

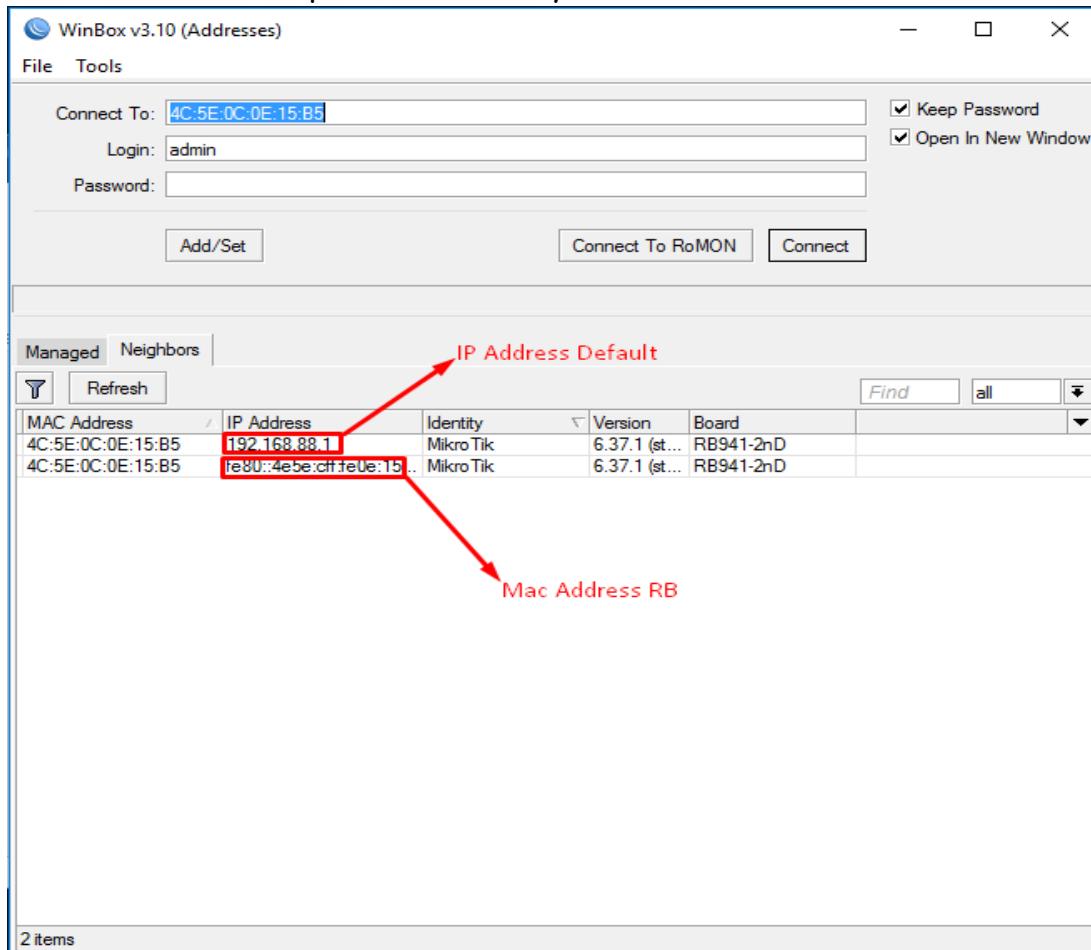
Ada banyak cara untuk meng-Akses Router Mikrotik,Bisa Menggunakan Winbox,SSH,Telnet,WebFig. Ke-Empat Ini adalah cara yang biasa di gunakan untuk Meng-Akses Mikrotik ,Kita juga bisa Mengakses Mikrotik lewat Android dengan Menggunakan aplikasi Tik-App yang bisa di Download di Play Store..

❖ Via Winbox

Pertama saya akan Memberikan Contoh Meng-Akses RouterBoard dengan Winbox..Apa itu Winbox? Winbox adalah sebuah aplikasi yang di luncurkan resmi oleh mikrotik,winbox adalah sebuah utility yang digunakan untuk melakukan remote ke Device mikrotik kita dalam mode GUI (Graphical User Interface), GUI adalah antarmuka pada sistem operasi yang menggunakan tampilan grafis, dapat dikendalikan menggunakan beberapa macam alat input. Jadi cara paling untuk mudah meng-akses mikrotik adalah menggunakan Winbox ,karna winbox merupakan sebuah aplikasi jadi kita hanya tinggal meng-Klik Klik saja ..Jika yang Belum Memiliki winbox Kita bisa mendownload nya Di www.mikrotik.com

Oke sekarang kita akan mulai Lab..

Pertama kita buka Aplikasi Winbox nya



Jika Menggunakan Winbox kita bisa Meng-akses Mikrotik dgn IP Address dan Mac-Address

- Kita klik Neighbors,lalu kita refresh
- Kita pilih kita ingin meng-akses melalui ip address/mac-address

Disini saya akan menggunakan mac-address

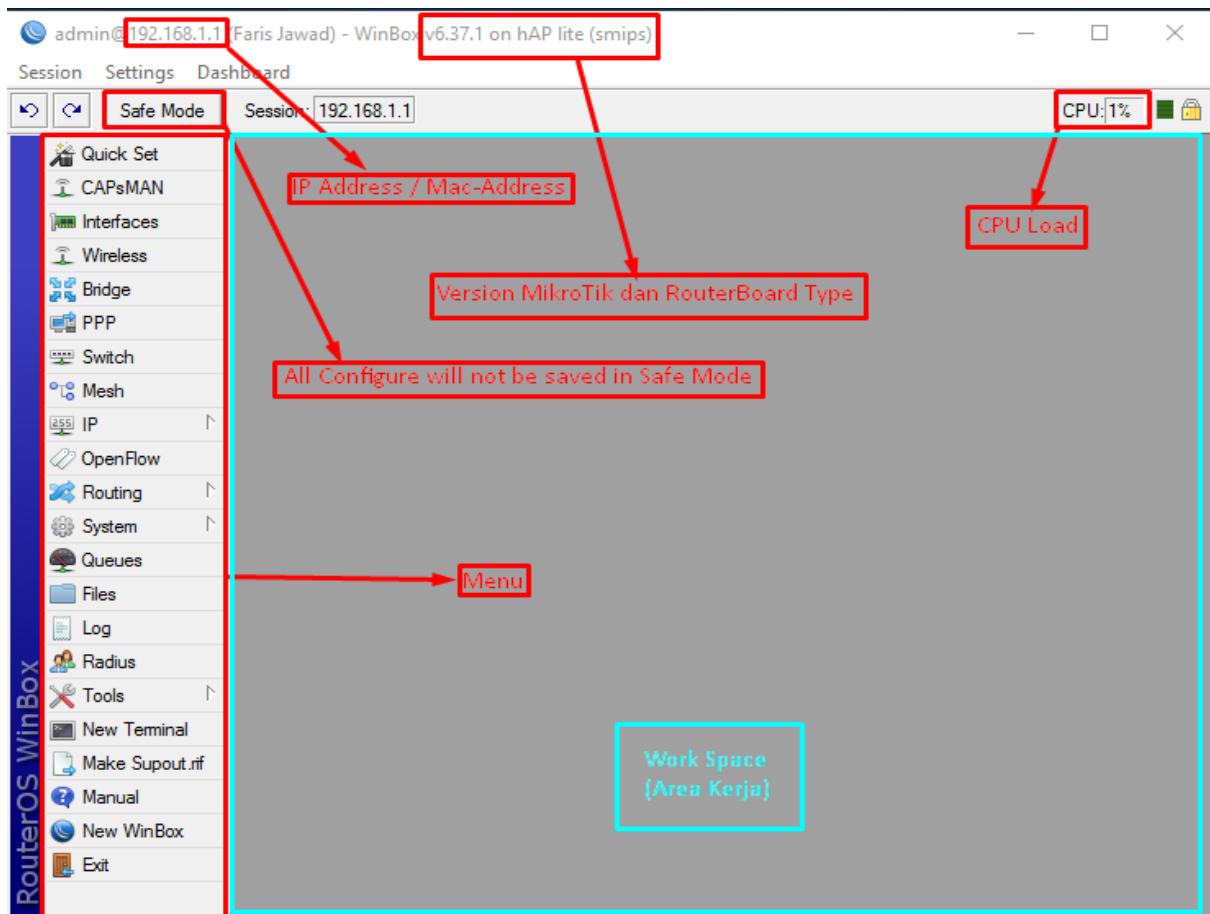
User Loginnya Kita isi dgn Konfigurasi Default

Login:admin

Password: (Kosong)

- Lalu Kita klik Connect

Lalu Tampilan Winbox akan Berubah seperti ini:



Setelah Masuk Ke Winbox Kita bisa Mengonfig perangkat MikroTik kita..

❖ Via Webfig

WebFig adalah tools/utility untuk meng-konfigurasi Mikrotik Router via Web browser. WebFig dapat diakses langsung dari router dan tidak memerlukan software atau aplikasi tambahan [kecuali browser].

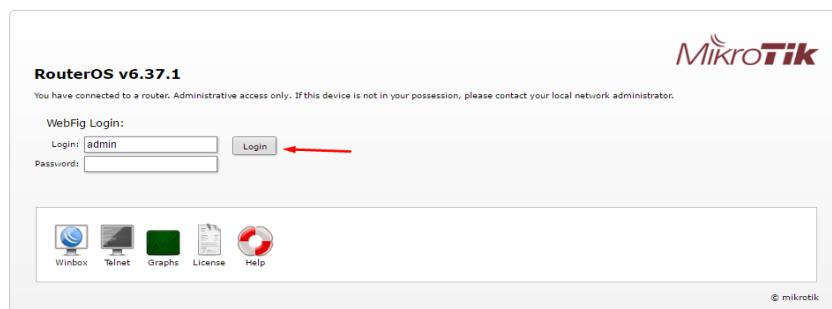
Karena WebFig bersifat independent maka memungkinkan untuk mengkonfigurasi router langsung menggunakan beragam mobile device tanpa membutuhkan software yang spesific.

WebFig di desain sedemikian rupa sebagai alternatif pengganti WinBox, dengan kemampuan mengakses fitur router yang sama dengan menggunakan WinBox.

WebFig dapat dijalankan dari homepage Browser yang dapat diakses dengan cara memasukan IP Address router yang di URL pada browser.

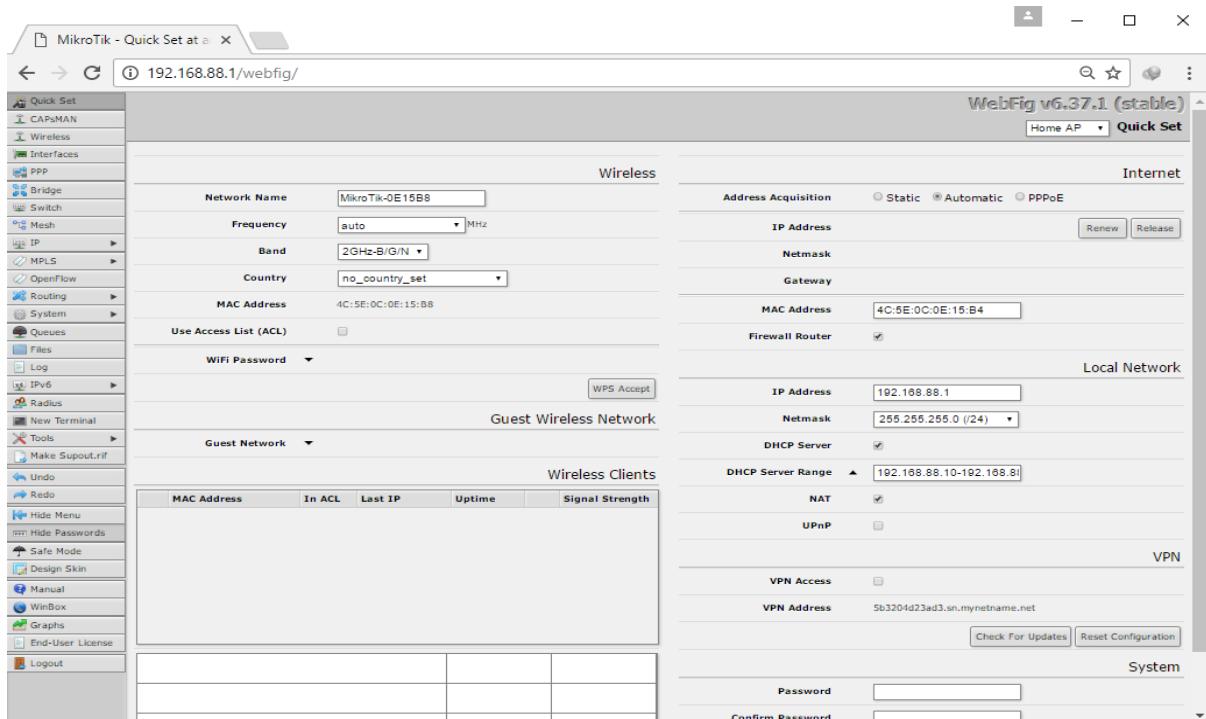
Kita Lanjut Ke lab nya.. di sini saya menggunakan Chrome.

Pertama Kita Buka Chrome nya:



-
- Lalu di tempat Url kita isikan dengan IP router kita (192.168.88.1)
 - Isi webfig loginnya dengan= Login:admin password: (kosong) <- (default)
 - Lalu Klik Login

Setelah Klik Login tampilan webfig akan berubah seperti ini:



Setelah masuk Kita bisa mengonfig Device mikrotik Sesuai Kebutuhan kita . tampilan webfig hampir sama dengan winbox

- **Via Telnet**

Telnet adalah singkatan dari Telecommunications Network Protocol, merupakan remote login yang terjadi pada jaringan internet disebabkan karena adanya service dari protocol Telnet. Dengan adanya Telnet dapat memungkinkan pengguna dapat mengakses Route MikroTik secara remote melalui jaringan internet, telnet menggunakan protocol Transmission Control Protocol (TCP) Port nya 23.

Oke Kita lanjut Ke Lab nya.

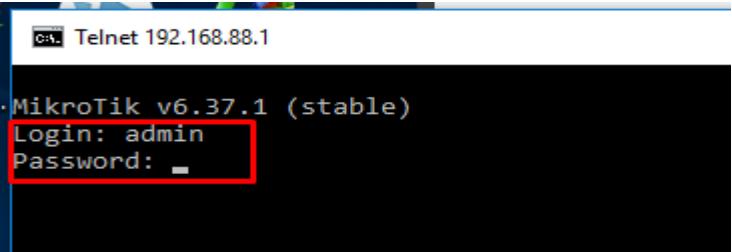
Pertama Kita Buka Command Prompt

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420>telnet 192.168.88.1
```

- Lalu kita masukan Perintah=telnet 192.168.88.1 (IP Router Default)
- Lalu tekan Enter

Setelah tekan Enter maka akan keluar User Login Seperti Berikut



```
Telnet 192.168.88.1
MikroTik v6.37.1 (stable)
Login: admin
Password: -
```

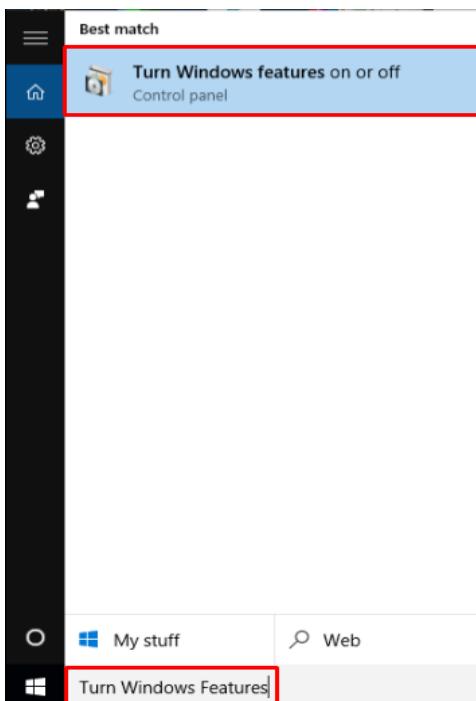
- User Login kita isikan= Login=admin Password= (kosong) <- (default)

Setelah masuk Ke CLI (Command Line Interface) Mikrotik kalian bisa mengonfig nya sesuai kebutuhan kalian,

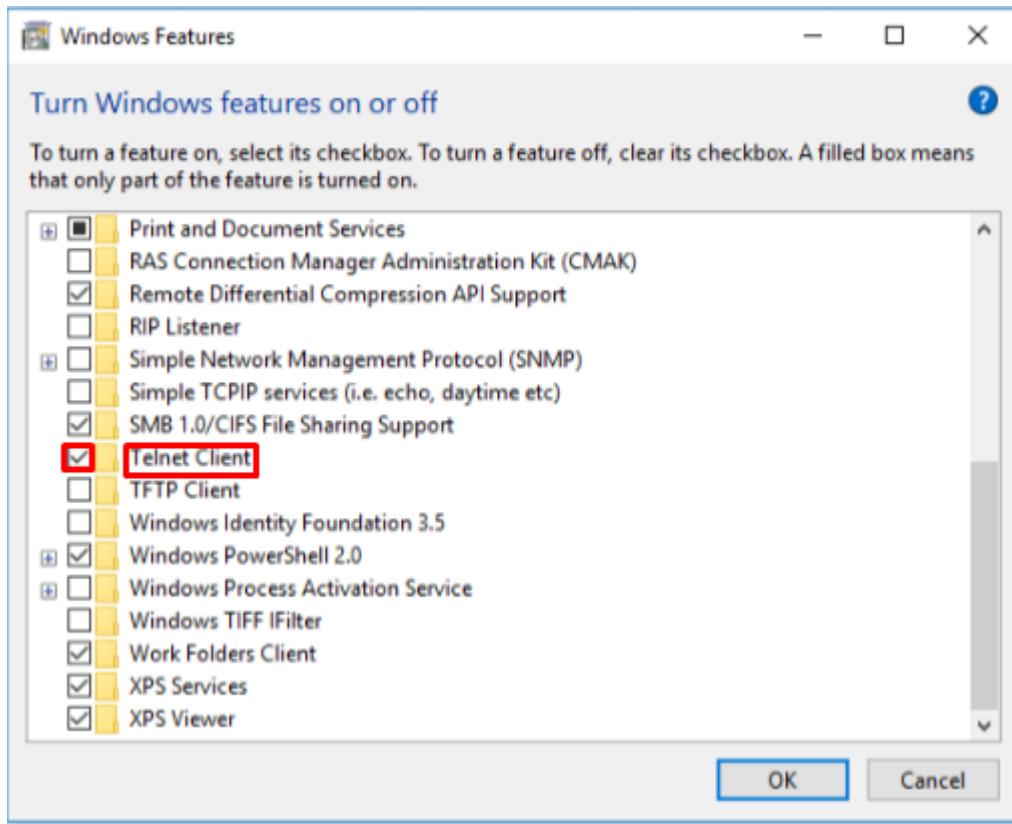
Tidak semua PC windows bisa Melakukan akses telnet ke mikrotik,Terkadang Fitur telnet di PC tersebut perlu di aktifkan terlebih dahulu agar bisa meng-Akses Router melalui Telnet

Selanjutnya saya akan menjelaskan bagaimana cara meng-Aktifkan fitur telnet pada Windows..

- Klik Menu Start 
- Lalu masukan kata "Turn Windows Features On or Off"



- Lalu Klik Menu tersebut
- Kita cari Fitur “Telnet Client”
- Lalu Kita Ceklis



Jika kita sudah Melakukan Step tersebut maka akan muncul Instalasi Telnet Fitur,lalu kita hanya tinggal Klik Klik Next saja...jika sudah selesai maka Fitur telnet Di PC anda telah aktif/alias bisa telnet Ke Router MikroTik... ☺

Berikut adalah Perintah yang biasa digunakan di CLI (Command Line Interface)

1. **INTERFACE PRINT** = digunakan untuk melihat informasi interface yang ada pada mikrotik
2. **IP ADDRESS PRINT** = digunakan untuk melihat informasi IP Address pada masing-masing Interface Mikrotik
3. **IP SERVICE PRINT** = digunakan untuk melihat informasi service yang ada pada mikrotik
4. **SYSTEM SHUTDOWN** = digunakan untuk men-shutdown mesin mikrotik
5. **SYSTEM REBOOT** = digunakan untuk merestart mesin mikrotik
6. **SYSTEM BACKUP SAVE** = digunakan untuk Membackup Settingan Mikrotik
7. **IP DNS PRINT** = digunakan untuk menampilkan informasi DNS pada mikrotik
8. **IP ROUTE PRINT** = digunakan untuk menampilkan informasi tabel routing pada mikrotik
9. **PASSWORD** = digunakan untuk mengganti password Mikrotik
10. **USER PRINT** = digunakan untuk melihat informasi user yang ada di mikrotik
11. **SYSTEM IDENTITY SET NAME** = digunakan untuk mengganti nama mesin mikrotik
12. **IP ADDRESS ADD ADDRESS=192.168.x.x/24 INTERFACE=ether** = digunakan untuk menambahkan IP Address pada interface mikrotik
12. **INTERFACE SET NAME=nama Nomor** = digunakan untuk merubah nama interface Mikrotik
13. **SYSTEM PACKAGE PRINT** = digunakan untuk melihat informasi package yang ada di mikrotik
14. **USER ADD NAME=USER GROUP=FULL PASSWORD=PASSUSER** = digunakan untuk menambahkan user baru pada mesin mikrotik
15. **IP ROUTE ADD GATEWAY=192.xx.x.x** = digunakan untuk menambahkan gateway
16. **IP DNS SET SERVERS=x.x.x.x,x.x.x.x** = digunakan untuk menambahkan informasi DNS server pada mikrotik
17. **SYSTEM RESOURCE PRINT** = digunakan untuk melihat informasi resource perangkat
18. **IP ADDRESS REMOVE Nomor** = digunakan untuk menghapus IP Address pada interface mikrotik
19. **FILE PRINT** = digunakan untuk melihat informasi file yang ada pada mesin mikrotik
20. **IP POOL PRINT** = digunakan untuk melihat informasi IP POOL pada mesin mikrotik

Dan masih banyak yang lainnya 😊

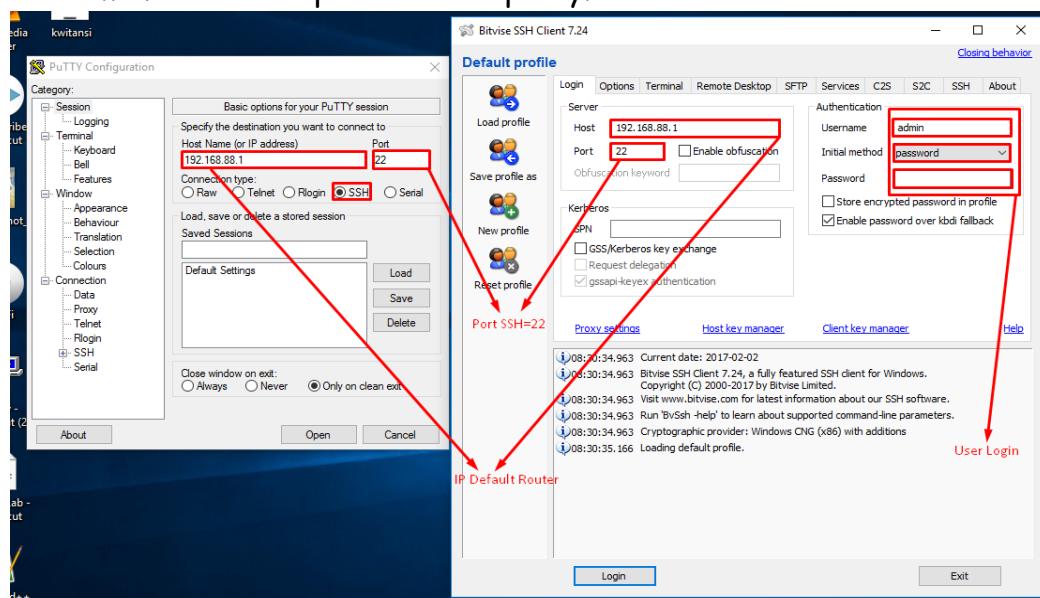
- **Via SSH**

Apa sih SSH itu ?

SSH adalah akronim dari Secure Shell yang merupakan sebuah protokol jaringan yang memanfaatkan kriptografi untuk melakukan komunikasi data pada perangkat jaringan agar lebih aman. Fungsi SSH dapat digunakan untuk menggantikan telnet, rlogin, ftp, dan rsh, salah satu fungsi utamanya adalah untuk menjamin keamanan dalam melakukan transmisi data pada suatu jaringan. SSH Menggunakan Protocol TCP Port nya 22

Di lab SSH ini saya menggunakan dua aplikasi yang biasa digunakan Untuk SSH: putty dan Bitvise SSH Client..

Pertama Kita buka Aplikasi SSH: putty/bitvise ssh client



- Host / Host Name (IP Address) kita isi dengan 192.168.88.1 (IP router Default)
- Dan Port kita isi dengan 22 karena port SSH adalah 22
- Authentication (bitviseSSH) kita isikan Username=admin Password=(kosong)
- Lalu Kita klik Login (bitviseSSH) / Open (Putty)
- Jika Menggunakan putty, user loginnya muncul ketika kita telah Klik Open

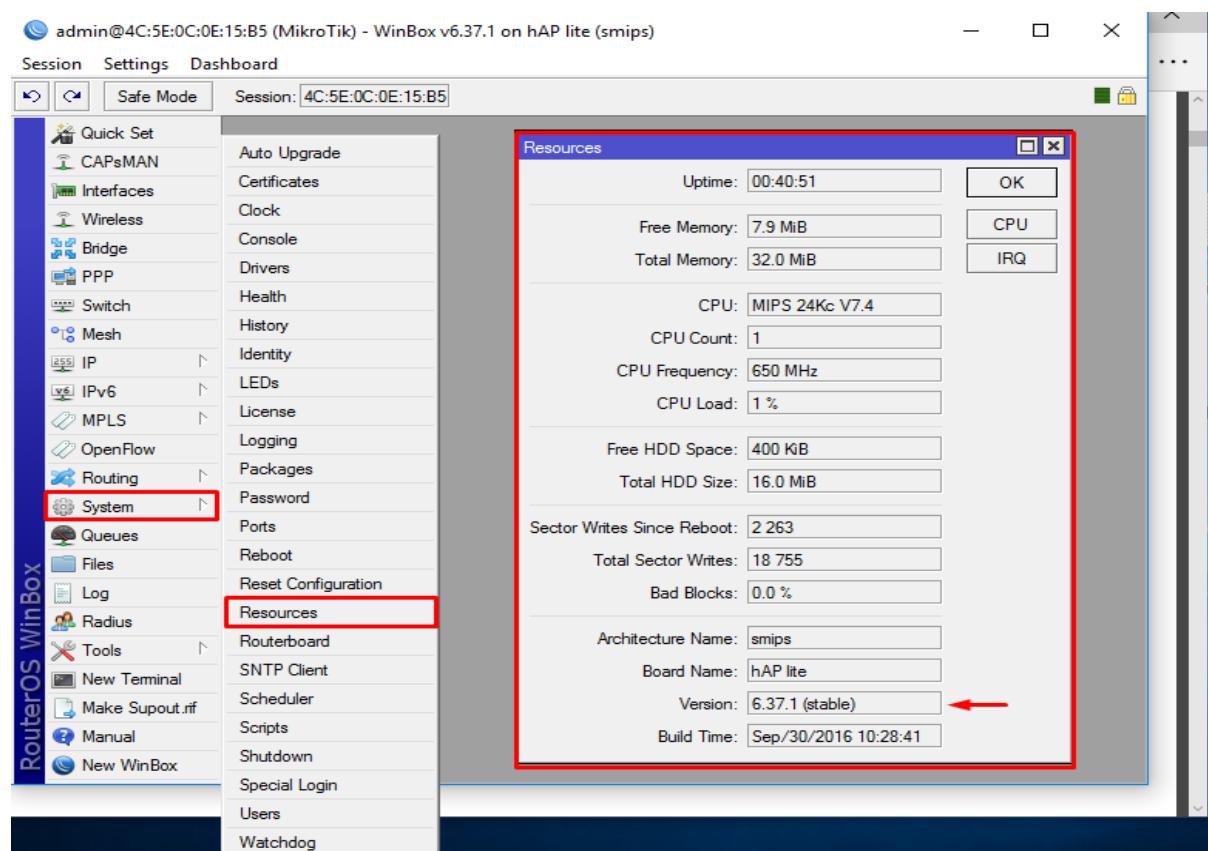
Jika Kita sudah Masuk tampilan nya akan sama seperti Telnet karna telnet dan SSH menggunakan CLI (Command Line Interface).. Setelah Itu Kita bisa mengonfig sesuai Kebutuhan kita

Lab 2. Melihat Versi MikroTik

Oke di lab ini saya akan menjelaskan cara melihat Versi MikroTik, Untuk melihat Versi MikroTik ada dua cara, cara yang paling mudah adalah menggunakan Winbox (GUI) karna kita hanya klik klik saja , dan cara satu lagi adalah menggunakan CLI (Telnet,SSH atau Terminal)

Oke langsung saja kita nge-lab...

- Via Winbox



- Masuk Ke Winbox
- Klik System > Resources

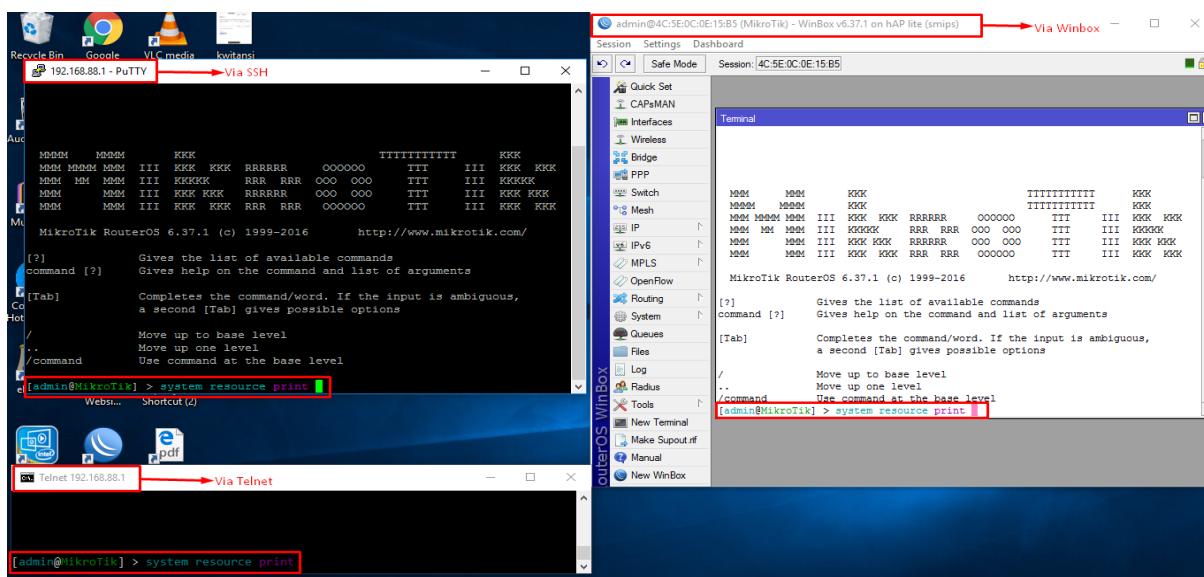
Setelah Mengikuti Step Tersebut maka kita bisa melihat Versi MikroTik

- **Via CLI (Command Line Interface)**

Untuk melihat versi MikroTik melalui CLI ada 3 cara yaitu :

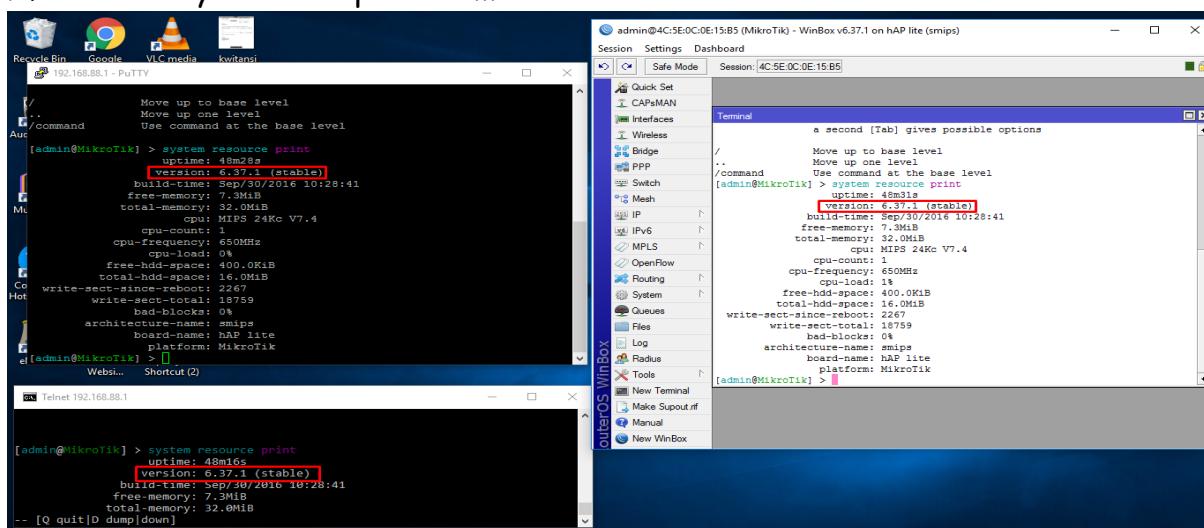
- **Telnet**
- **SSH**
- **Terminal (Winbox)**

Oke Kita lanjut ke lab nya...



Untuk Melihat Versi MikroTik melalui Telnet / SSH maka kita harus Login terlebih dahulu..

- **Klik New Terminal > Ketikan " System Resource Print"**
- Maka Hasil nya akan Seperti ini...



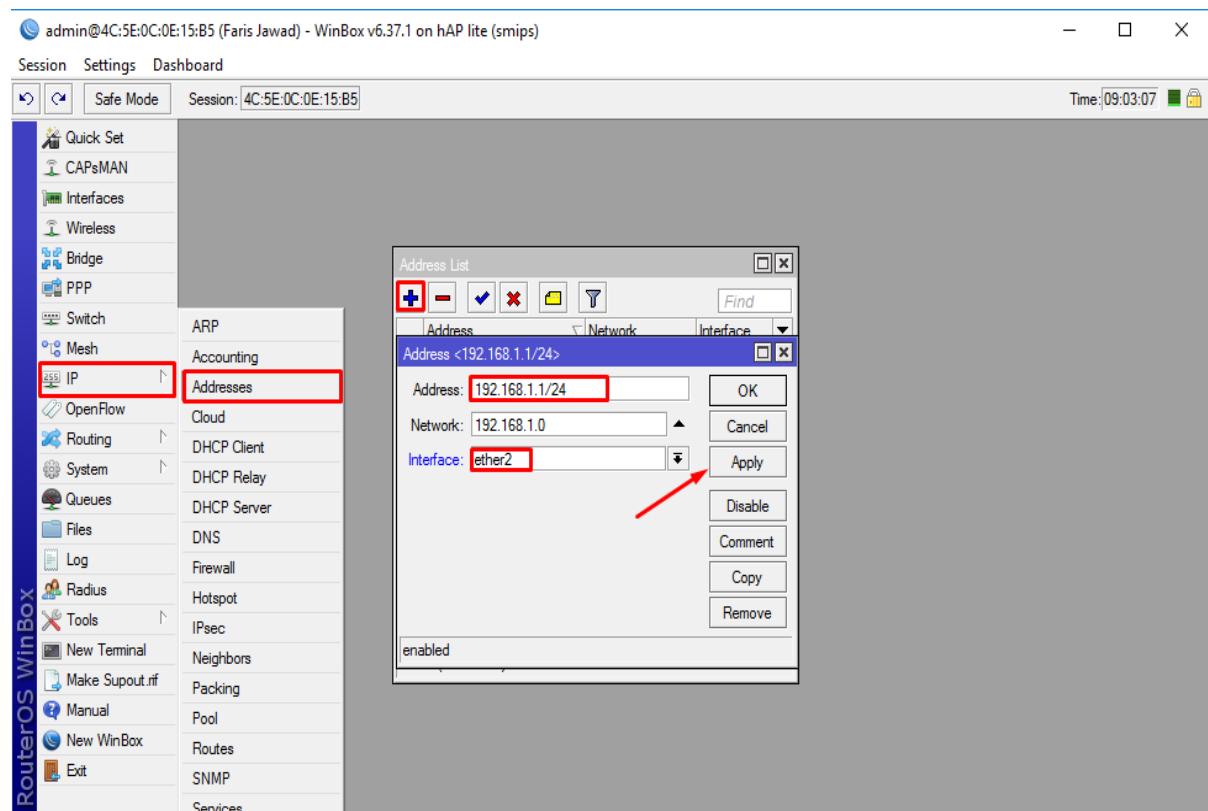
Lab 3. Menghubungkan Router Ke Internet (NAT)

Oke di lab ini saya akan menjelaskan bagaimana cara agar router MikroTik dapat terhubung ke Internet ,Untuk bisa terhubung ke internet kita harus menggunakan IP Public..karna IP client (kita) adalah IP Private maka kita Perlu Menerjemahkan IP Private ke IP Public untuk terhubung ke internet, untuk menerjemahkan IP tersebut kita harus menggunakan Fitur NAT (Network Address Translation) . Di lab ini saya akan memberikan contoh Membuat NAT (Network Address Translation) agar PC kita dapat terhubung ke Internet.

Oke di lab ini saya akan mencontohkan bagaimana cara nya Router kita dapat Terhubung ke Access point (TKJ Satuu) (Sumber Internet)

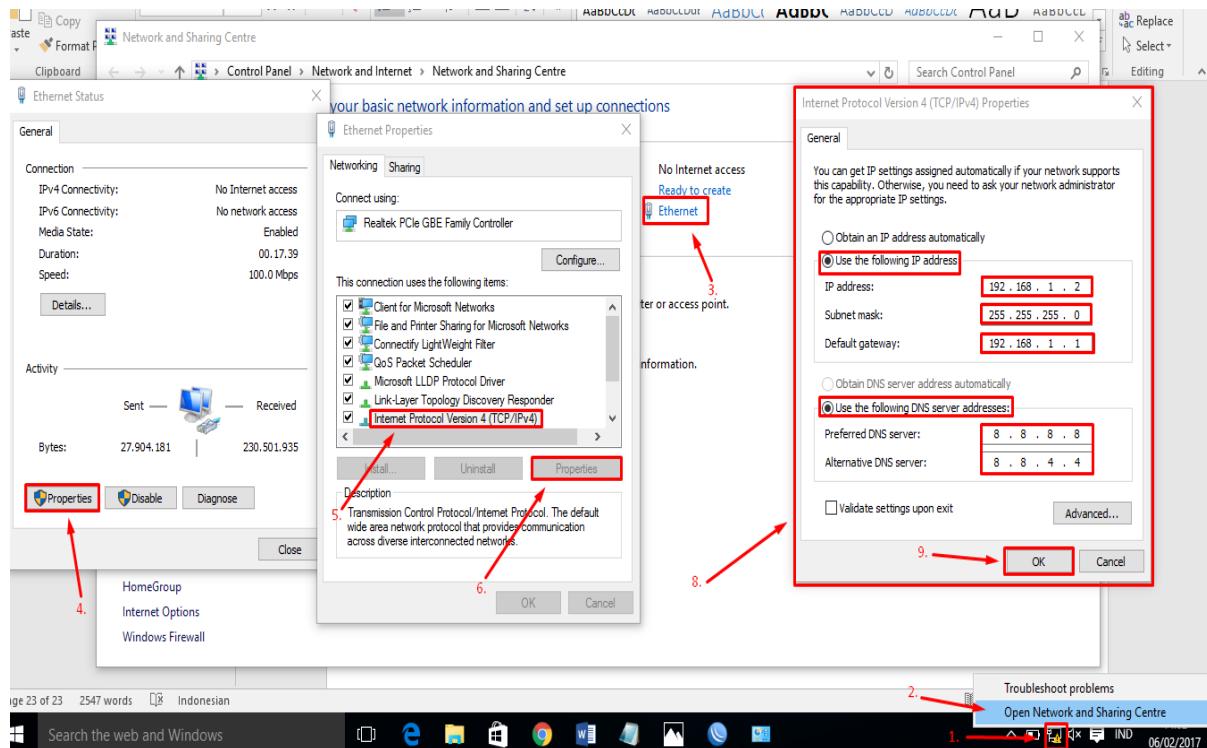
Oke langsung saja kita nge-Lab...

- Pertama Kita harus Membuat IP address agar Client (PC) dapat terhubung ke Router



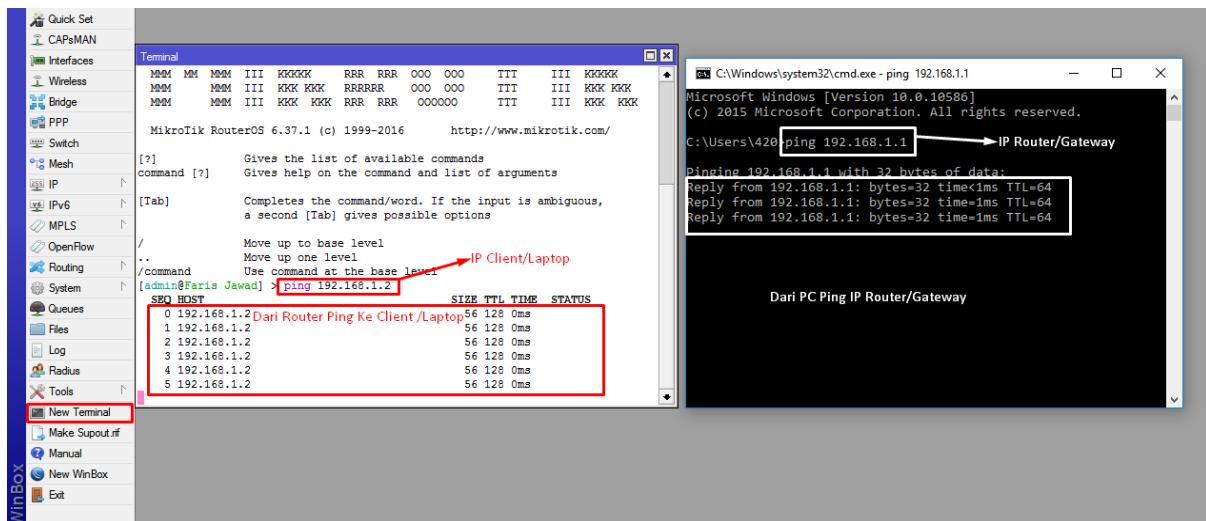
- Kita Klik IP > Addresses > add (+) > address=192.168.1.1/24 > interface=ether2 lalu apply dan ok

IP yang telah kita buat tadi akan berfungsi Sebagai Gateway Client.. selanjutnya kita harus mengkonfigurasikan IP address di Client (PC) agar Client (PC) dapat terhubung ke router..



- Kita Buka Open Network And Sharing Centre
- Lalu klik Properties
- Lalu Kita pilih Internet Protocol Version 4 (TCP/Ipv4) > Properties
- Lalu Kita isikan IP secara Static isi gateway dengan IP router =192.168.1.1
- Lalu Klik OK

Step selanjutnya adalah Kita harus Mengetest apakah Client dan Router sudah saling terhubung atau belum,cara nya kita PING dari Client (PC) ke router dan Router PING ke Client (PC)

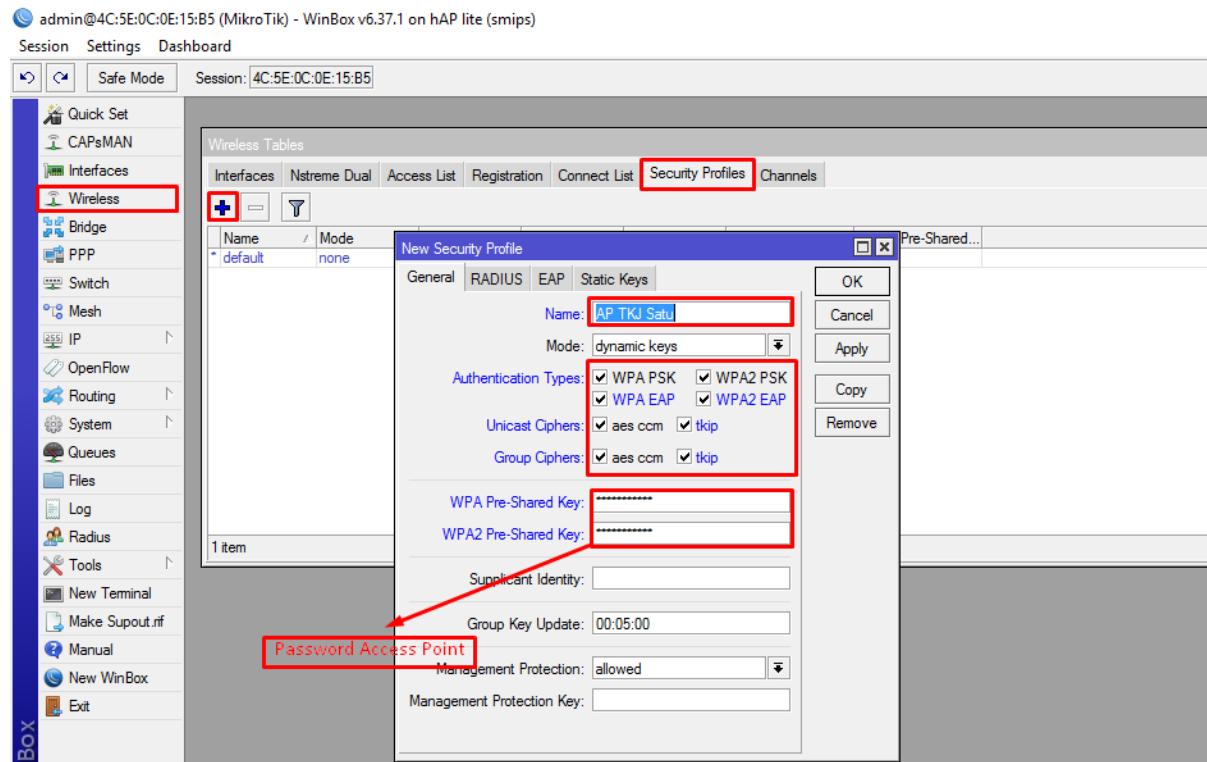


Setelah Berhasil...Kita lanjut ke Step Selanjutnya..

Step selanjutnya adalah kita membuat Security Profil, Sebelum kita buat Security Profile kita harus mengetahui kenapa kita harus membuat security Profile? Fungsi di Security Profile di sini berfungsi agar Router kita bisa masuk ke access point (TKJ Satuu) sebagai Client karna Access Point (TKJ Satuu) di lindungi oleh Password..

Kita harus Masuk Ke menu Wireless

- Pertama Kita Nyalakan dahulu Interface WLAN nya
- Lalu yang kita harus buat Security Profile sesuai dgn password Access point

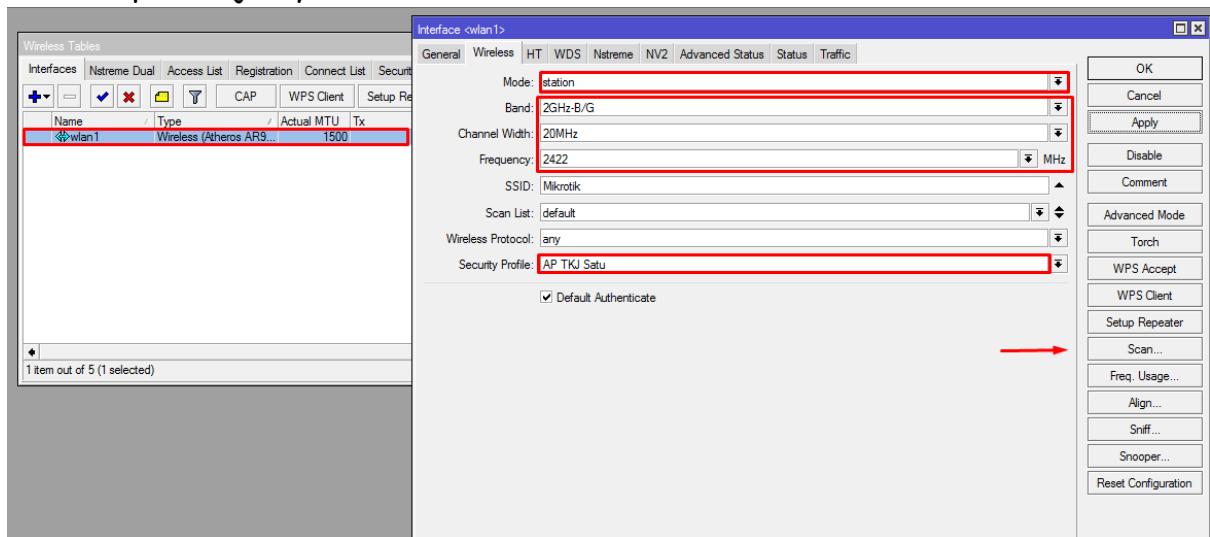


- Kita masuk Menu Wireless > Security Profiles > Add (+)
- Kita isi name=AP TKJ Satu (bebas)
- Lalu Kita Ceklis Semua List (WPA PSK/EAP,WPA2 PSK/EAP) ,(Aes com,tkip)
- Lalu Isi WPA/WPA2 Sharred Key=masukaja (password AP TKJ Satu)
- Klik Apply dan Ok

Setelah Kita Membuat Security Profile Kita harus Men-Setting Wireless kita sebagai Mode Station..Untuk apa Mode Station? Wireless dengan Mode station ini digunakan sebagai wireless client/ Penerima ,Mode Station Di gunakan jika Access Point Bukan MikroTik

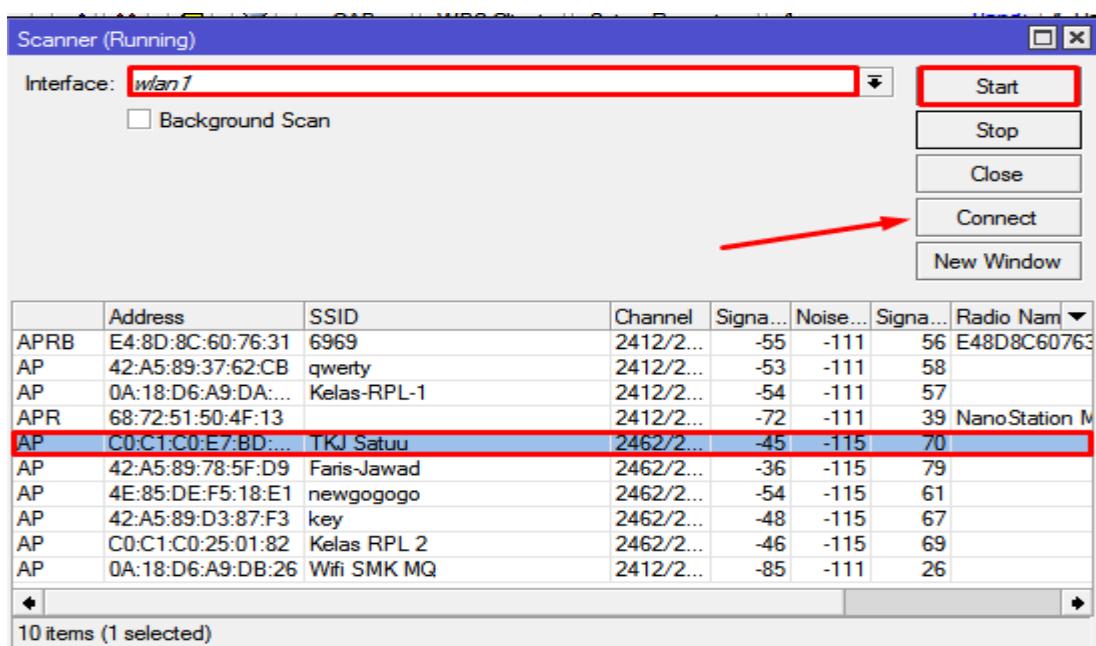
Tetapi jika Acces Point nya Mikrotik Juga maka Mode nya Station Bridge
Oke Itu Sedikit penjelasan tentang Station Dan Station Bridge

Oke Step selanjutnya kita masuk Ke Wireless Menu...



- Kita Setting Mode=Station Band,channel dan Frekuensi bebas
- Lalu kita Setting Security Profile nya
- Selanjutnya Kita Klik Scan
- Interface =Wlan 1 >Start

Lalu akan Ada List SSID yang ada di Sekitar Router kita..



- Lalu Kita Pilih SSID Tkj Satuu lalu Klik Connect

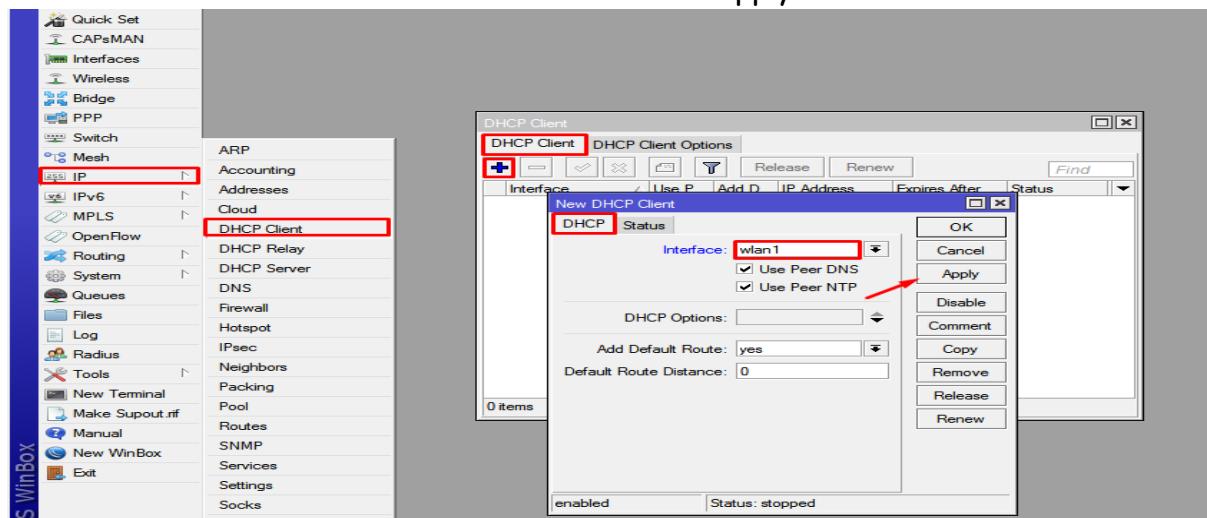
Jika Step ini sudah Selasai maka Wireless kita sudah terhubung ke Internet (access point)

Wireless Tables											
Interfaces		Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels				
	Name	Type	Actual MTU	Tx	Rx		Tx Packet (p/s)	Freq. Usage	Alignment	Wireless Sniffer	Wireless Snooper
R	wlan1	Wireless (Atheros AR9...)	1500	0 bps	54.6 kbps		0	23	0 bps		0 bps
1 item out of 5 (1 selected)											

Jika sudah terhubung maka status nya Running (R)..

Step selanjut nya adalah kita membuat DHCP Client....Apa sih fungsi DHCP client? Disini DHCP client berfungsi agar interface WLAN kita mendapat IP Address secara otomatis karna Access Point yang kita tuju adalah DHCP Server...

- Pertama Kita harus masuk Ke Menu DHCP Client = IP > DHCP Client > Add(+)
- Setelah itu Interface Kita isikan Wlan1 lalu Apply dan OK



Jika Interface Wlan Kita telah mendapatkan IP Address dari DHCP Server (AP) maka maka akan muncul IP address nya dan status nya Bound..

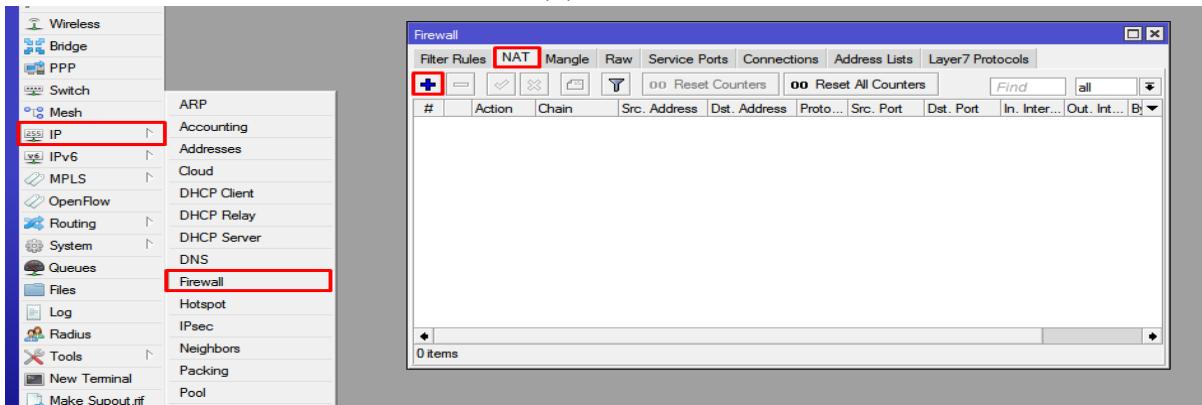
DHCP Client						
DHCP Client		DHCP Client Options				
Interface		Use P...	Add D...	IP Address	Expires After	Status
wlan1		yes	yes	192.168.123.97/24	2d 23:59:59	bound
1 item						

IP DHCP Client

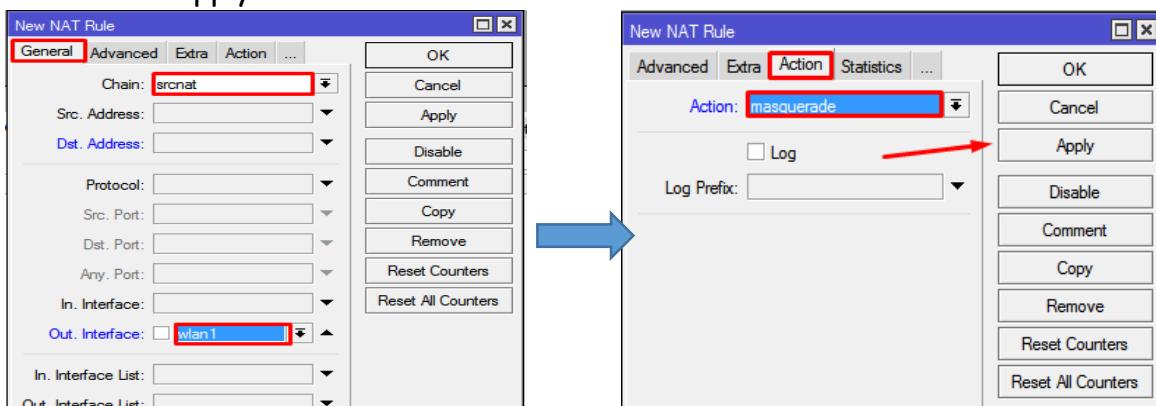
Step Selanjutnya adalah Membuat NAT (Network Address Translation) untuk Menerjemahkan IP Private ke IP Public...

Untuk membuat NAT kita harus masuk Ke Menu NAT..

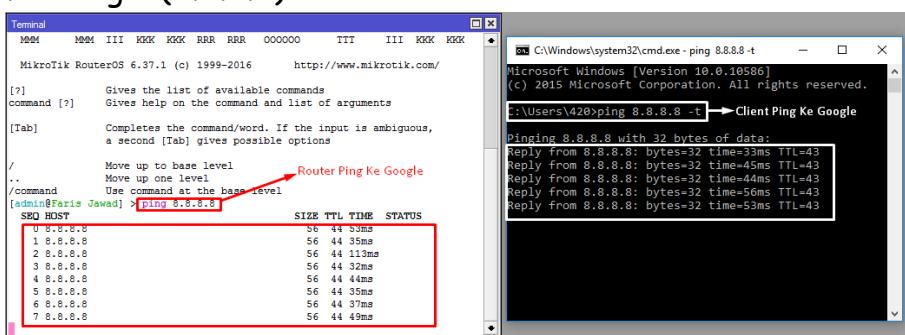
- Klik IP > Firewall > Nat > Add (+)



- Lalu kita isi Chain=Srcnat Out.Interface=Wlan1 dan action=masquerade
- Lalu Apply dan Oke



Jika Step ini sudah selasai maka Router dan seluruh Client yang terhubung ke Router Bisa Mendapatkan acces Internet .Untuk pengetesan maka Kita Test Ping Ke Google (8.8.8.8)



Oke cara di atas menjelaskan cara membuat Nat agar semua Client yang terhubung ke Router bisa terkoneksi ke internet..Selanjut nya saya akan memberikan LAB Tambahan...

Yaitu cara membuat Nat Untuk satu network / satu Range IP... apakah Nat Seperti ini berguna?semua tergantung kebutuhan kita,misalkan routerboard yang kita punya di gunakan untuk SERVER Kelas dan setiap kelas memeliki Network yang berbeda.Contoh:

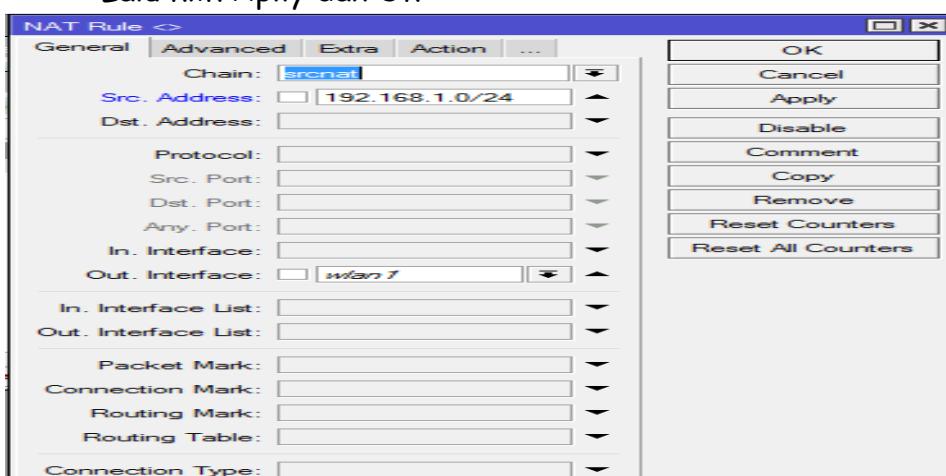
Kelas TKJ 1=192.168.1.0/24 Interface=Ethernet3

Kelas TKJ 2=192.168.2.0/24 Interface=Ethernet4

Kelas RPL 1=192.168.3.0/24 Interface=Ethernet5

Di lab tambahan ini saya mencontohkan bagaimana caranya agar Nat hanya di gunakan untuk Kelas TKJ 1 (192.168.1.0/24) jadi artinya hanya kelas TKJ 1 yang bisa terhubung ke internet dan Kelas TKJ 2 tidak bisa terhubung ke internet karna IP kelas TKJ 2 tidak di Nat.. Sebenarnya kita hanya perlu merubah settingan Nat nya Seperti Ini..

- Kita isi Chain=srcnat Src.Address=192.168.1.0/24 Out.Interface=wlan 1 Action=masquerade
- Lalu klik Apply dan Ok

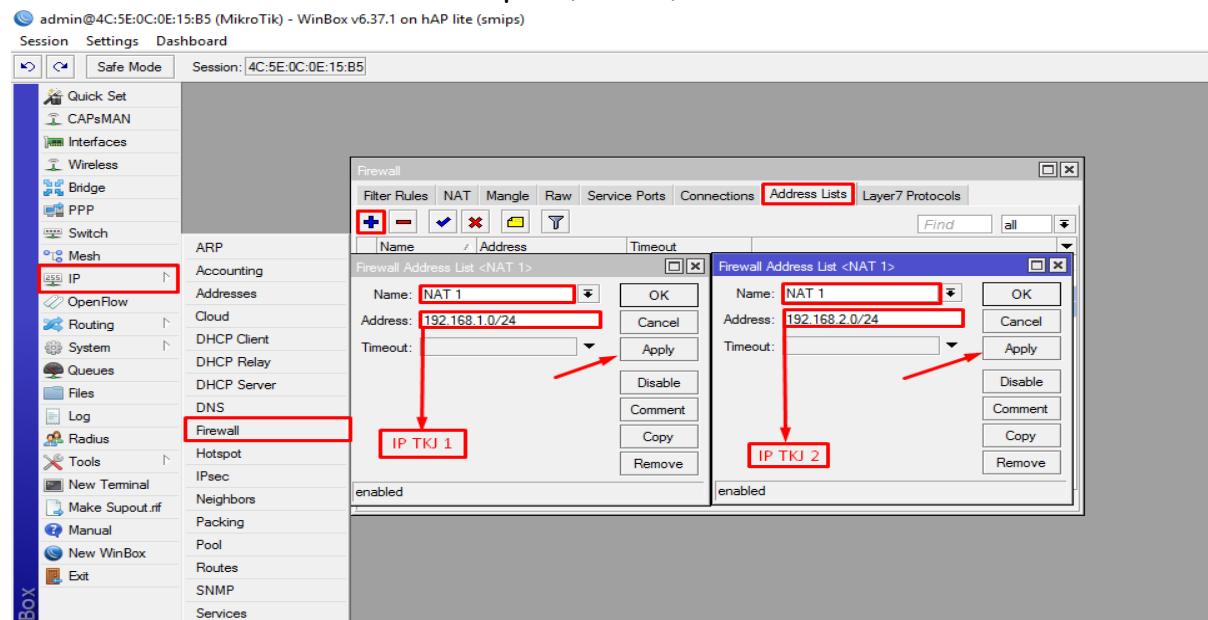


Setelah kita Setting seperti ini,maka IP yang di NAT hanya 192.168.1.0/24 (kelas tkj 1) dan IP 192.168.2.0/24 dan 192.168.3.0/24 tidak di NAT (tdk terhubung ke internet) maka kelas TKJ 2 dan RPL 1 tidak mendapatkan acces internet dari router.

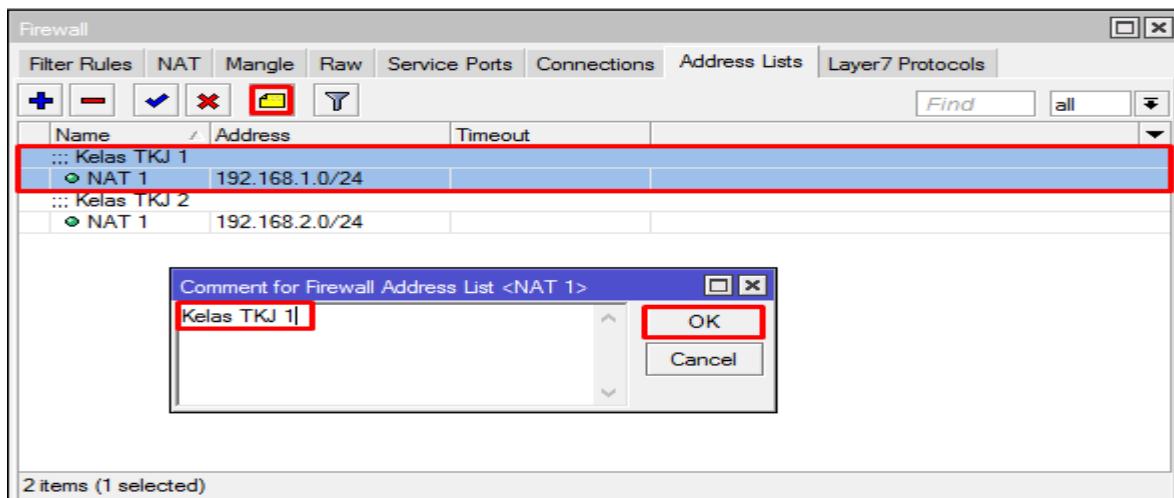
Kita juga bisa Meng-Costum IP yang akan Kita Nat dengan Address List. Apa Fungsi Address List? Address list berguna untuk mengelompokan Banyak IP/Domain ke dalam satu Kelompok.. Apakah Address List Berguna untuk NAT ? jelas berguna jika lab sebelum nya kita hanya membuat 1 list NAT yang hanya di bisa gunakan oleh network 192.168.1.0/24 maka dengan address list kita bisa membuat 1 list nat yang bisa di gunakan untuk banyak network.. nah di lab ini kita akan membuat 1 list NAT dengan Address list yang berguna agar hanya 2 network saja yang di NAT yaitu 192.168.1.0/24 (TKJ 1) dan 192.168.2.0/24 (TKJ 2) jadi kita perlu mengelompokan IP 192.168.1.0/24 dan 192.168.2.0/24 dalam satu kelompok (address list)...

Untuk Mengelompokan IP TKJ 1 dan TKJ 2 kita perlu masuk ke menu address list

- Klik IP > Firewall > Address List > Add (+)
- Lalu Kita buat Nama Kelompok (NAT 1) dan masukan IP TKJ 1 Dan TKJ 2

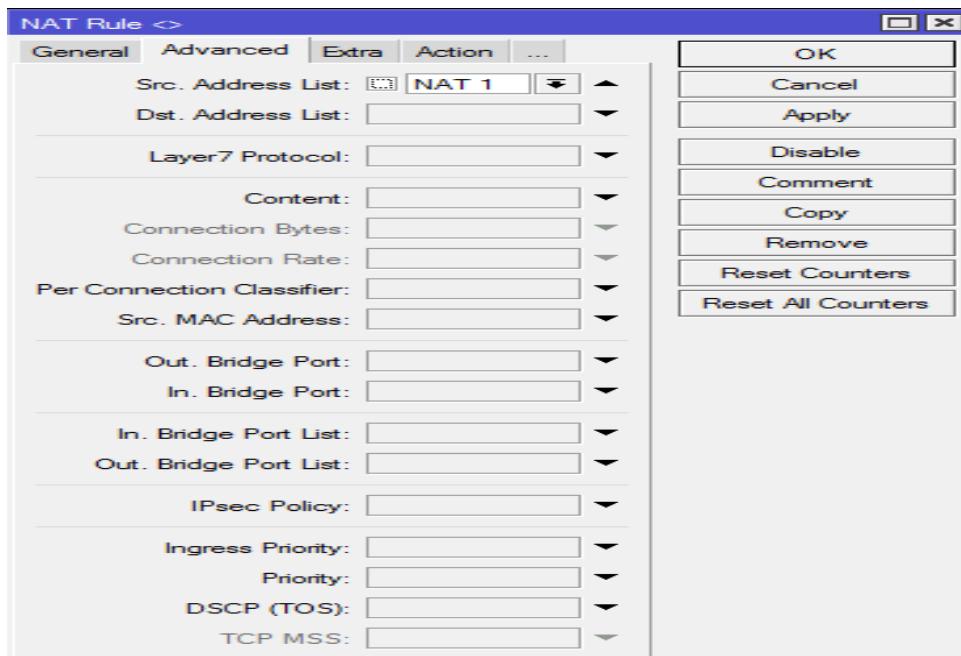


Setelah Step Ini sudah Selesai maka IP 192.168.1.0/24 dan IP 192.168.2.0/24 sudah menjadi satu kelompok (NAT 1)



Untuk menandai List kita bisa menambahkan Comment agar kita bisa membedakan yang mana IP TKJ 1 dan IP TKJ 2

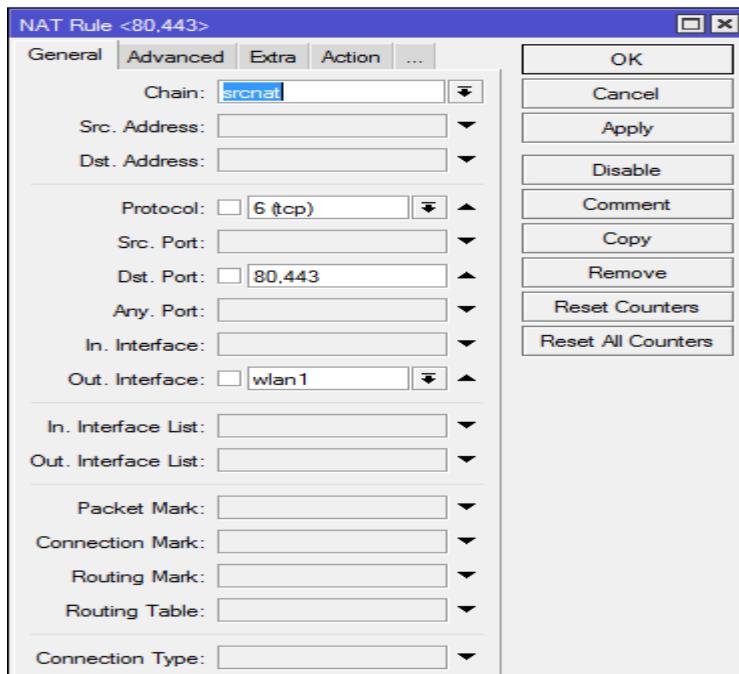
Setelah Step Ini selesai kita kembali ke Menu NAT ... Untuk Memasukan Address list (NAT 1) yang telah kita buat kita perlu memasukan nya di src.address list yang ada di Tab Advanced



- Isi Chain=srcnat Out.Interface=wlan1 Src.Address list=NAT 1
- Action=Masquerade
- Lalu Apply dan Ok

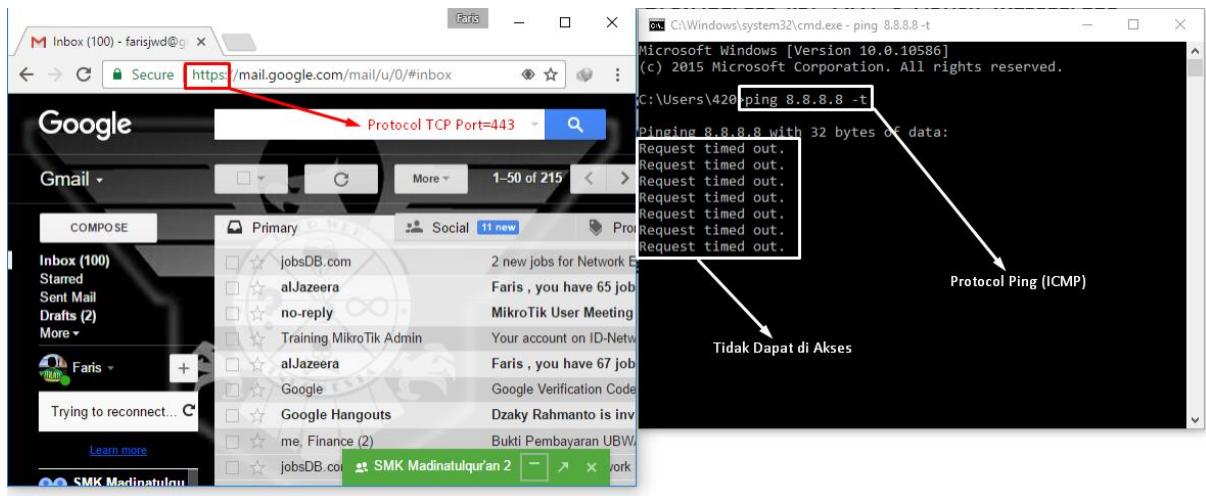
Setelah Step ini selesai maka hanya Network TKJ 1 dan TKJ 2 saja yang di NAT (terhubung ke internet) dan Network RPL 1 tdk dapat terhubung ke internet karna tdk kita NAT.. Oke saya akan memberikan 1 lab tambahan yang terakhir ..yaitu kita membuat NAT untuk Network 192.168.1.0/24 dan kita membatasi Protocol apa saja yang bisa di akses ke internet oleh client...di sini saya akan mencontohkan bagaimana cara nya network 192.168.1.0/24 hanya bisa mengakses Protocol HTTP dan HTTPS. Maka artinya clien tdk bisa ping ke internet dan client hanya bisa mengakses browser karna kita hanya mengizinkan TCP HTTP dan HTTPS (80,443)

Oke langsung saja kita lanjut ke Lab nya.... kita hanya perlu meng-edit Nat yang telah kita buat....



- Isi Chain=srcnat Protocol=tcp Dst.port=80,443 Out.Interface=wlan1 Action=masquerade
- Lalu Apply dan Ok

Setelah Step ini selesai semua client yang mengakses internet melewati router kita hanya bisa meng-Akses HTTP (80) dan HTTPS (443) karna kita hanya meng-izinkan Protocol TCP port=80,443 saja yang bisa di akses ke internet,Contoh di sini saya akan meng-akses Protocol Ping (ICMP) ke internet,bisakah client meng-akses protocol ping ?



Disini saya mencoba Ping Ke google.com (8.8.8.8) Ternyata Protocol Ping (ICMP) tidak bisa di akses oleh Client dan Protocol HTTPS tetap bisa di akses oleh Client karna kita hanya mensetting Client hanya bisa meng-akses Protocol HTTP(80) dan HTTPS(443).....

Masih banyak lagi Lab tentang NAT mungkin dan di sini saya hanya menjelaskan sedikit saja..

Lab 4. Melihat Fitur Fitur Mikrotik (Package)

Router MikroTik memiliki banyak Fitur yang mungkin biasa kita gunakan seperti: Wireless, Hotspot, DHCP dll untuk melihat beberapa fitur yang di miliki MikroTik kalian bisa melihat nya di halaman awal karna saya menaruh penjelasan tentang fitur fitur yang di miliki MikroTik dan kegunaannya..

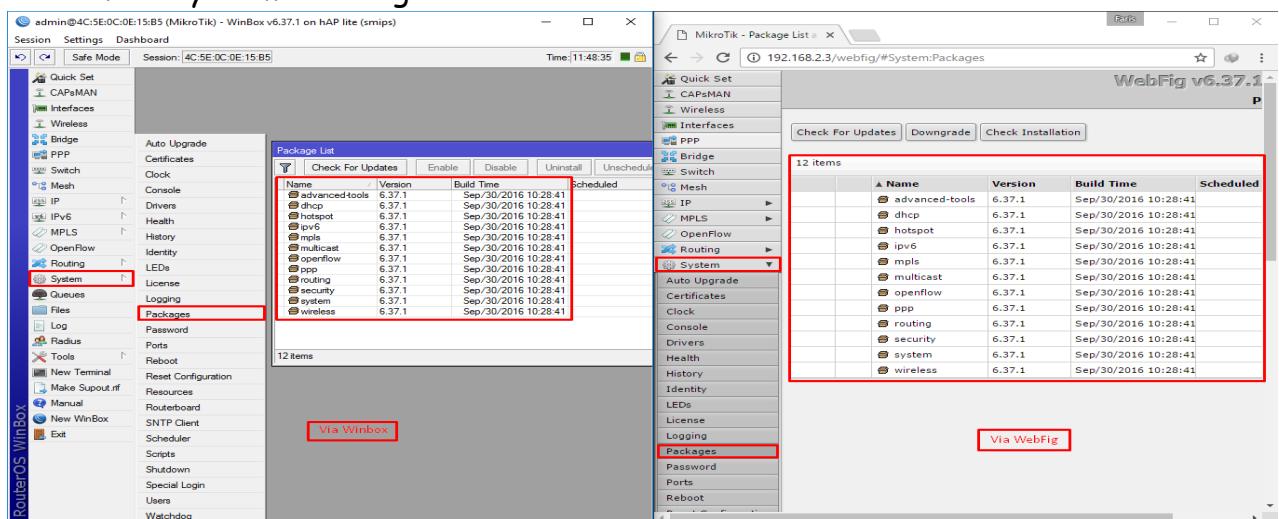
Ada dua cara untuk melihat Fitur MikroTik, Yaitu:

- **GUI (Winbox dan Webfig)**
- **Terminal (Telnet dan SSH)**

Oke kita langsung ke Lab bagaimana cara melihat Fitur Fitur yang di miliki MikroTik...

Pertama saya akan menjelaskan cara Melihat Fitur MikroTik menggunakan GUI (Graphical User Interface)...

- **Klik System > Package**



Berikut Hasil nya jika mengeCheck Fitur MikroTik Lewat GUI (Winbox/WebFig)

Selanjutnya saya akan menjelaskan cara MengCheck Fitur MikroTik Lewat Terminal (Telnet/SSH)

- Login Terlebih dahulu (Telnet/SSH)
- Ketik "System Package Print" > enter

The image shows two terminal windows side-by-side. Both windows are titled '192.168.2.3 - PuTTY'. The left window is labeled 'Via Telnet' and the right window is labeled 'Via SSH'. Both windows display the same command-line interface output. The command entered in both is '[admin@MikroTik] > system package print'. The output lists various system packages with their names and versions. The 'Via SSH' window also shows a help menu for the Tab key.

#	NAME	VERSION
0	ppp	6.37.1
1	openflow	6.37.1
2	advanced-tools	6.37.1
3	dhcp	6.37.1
4	ipv6	6.37.1
5	mpls	6.37.1
6	multicast	6.37.1
7	security	6.37.1
8	wireless	6.37.1
9	hotspot	6.37.1
10	routing	6.37.1
11	system	6.37.1

Nah Keluarkah Fitur Fitur MikroTik Beserta Versi Fitur nya ..

Dan Disini saya akan memberikan List Fitur Fitur Mikrotik:

Pengelompokan fitur mikrotik:

- a. Firewall and NAT
- b. Routing-Static Routing
- c. Data Rate Management
- d. Hotspot
- e. Point to point tunneling protocol
- f. Simple tunnels
- g. IpSec
- h. Web proxy
- i. Caching DNS Client
- j. DHCP
- k. Universal client
- l. VRRP
- m. UPNP

- n. NTP
- o. Monitoring/Accounting
- p. SNPM
- q. M3P
- r. MNDP
- s. Tools

2.Layer Dua Konektivitas

- a. Wireless
- b. Bridge
- c. Virtual Lan
- d. Synchronous
- e. Asynchronous
- f. ISDN
- g. SDSL

Adapun Fitur-Fitur Mikrotik Router OS

1. Address List: Pengelompokan IP Address berdasarkan nama.
2. Asynchronous: Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3. Bonding: Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
4. Bridge: Mendukung fungsi bridge spanning tree, multiple bridge interface, bridging firewalling.
5. Data Rate Management: QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.
6. DHCP: Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.

7. Firewall dan NAT: Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot: Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. IPSec: Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5
10. ISDN: mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
11. M3P: MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
12. MNDP: MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
13. Monitoring / Accounting: Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
14. NTP: Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
15. Point to Point Tunneling Protocol: PPTP, PPPoE dan L2TP Access Concentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.
16. Proxy: Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
17. Routing: Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
18. SDSL: Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
19. Simple Tunnel: Tunnel IPIP dan EoIP (Ethernet over IP).
20. SNMP: Simple Network Monitoring Protocol mode akses read-only.

21. Synchronous: V.35, V.24, E1/T1, X21, DS3 (T3) media types; sync-PPP, Cisco HDLC; Frame Relay line protocol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
22. Tool: Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
23. UPnP: Mendukung antarmuka Universal Plug and Play.
24. VLAN: Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
25. VoIP: Mendukung aplikasi voice over IP.
26. VRRP: Mendukung Virtual Router Redundant Protocol.

Sebenarnya sih saya telah Menaruh penjabaran tentang Fitur Fitur MikroTik di halaman Awal Buku ini,tetapi penjelasan Tentang Fitur MikroTik yang Di awal Halaman Berbeda Dgn yang di sini....Dan agar Lebih Mudah,saya Menaruh lagi di sini,Sekalian Untuk Membantu Menebalkan Buku saya ☺

Lab 5. Men-Enable/Disable dan Uninstall Package

MikroTik Memiliki Banyak Fitur Fitur Yang bisa Kita gunakan atau yang biasa di sebut Package..Di lab ini saya akan menjelaskan cara Men-Enable/Disable dan Uninstal Package.Untuk Apa Kita Men-Disable / Uninstal Package ? Untuk Mengurangi Beban Router..Karna Tidak semua Package Mikrotik di gunakan oleh kita itu semua tergantung Kebutuhan kita..Contoh:jika kita setting RouterBoard sebagai Server Kelas ,kita harus Men-Disable / Uninstall Package yang Tidak di gunakan sebagai server:Wireless,IPv6,MPLS dll...Kita hanya menggunakan Package yang di butuhkan Router Untuk Menjadi Server Kelas.

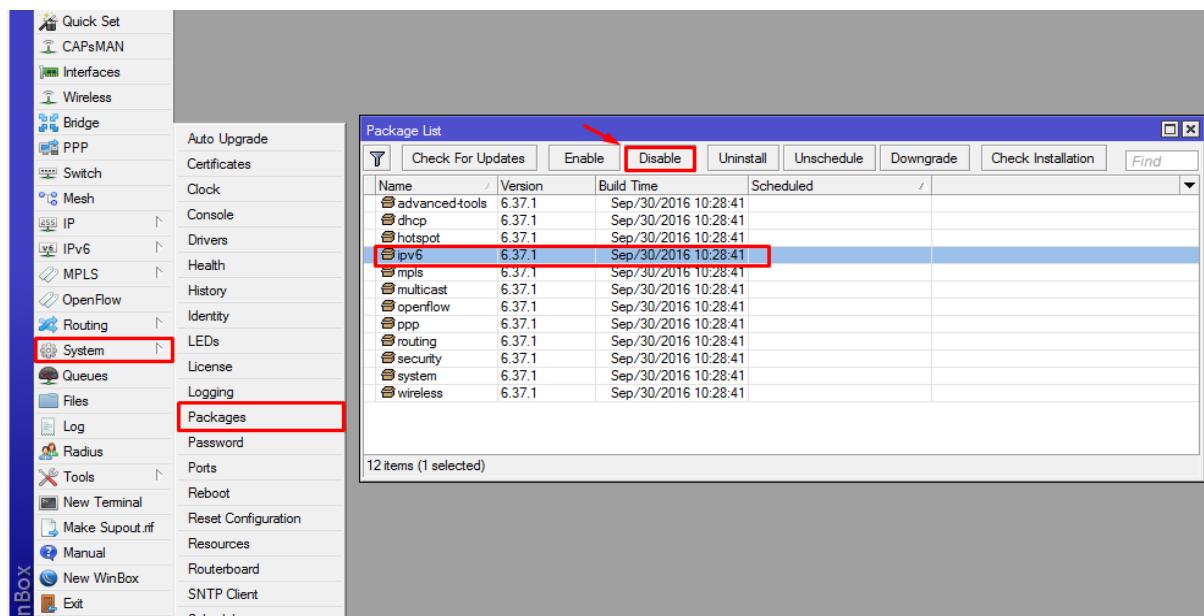
Pada Lab Ini Kita Bisa Menggunakan 2 Cara :

- **GUI (Winbox dan Webfig)**
- **Terminal (Telnet dan SSH)**

Oke kita Lanjut Ke Lab nya... Pertama saya akan Menjelaskan Menggunakan GUI (Winbox)

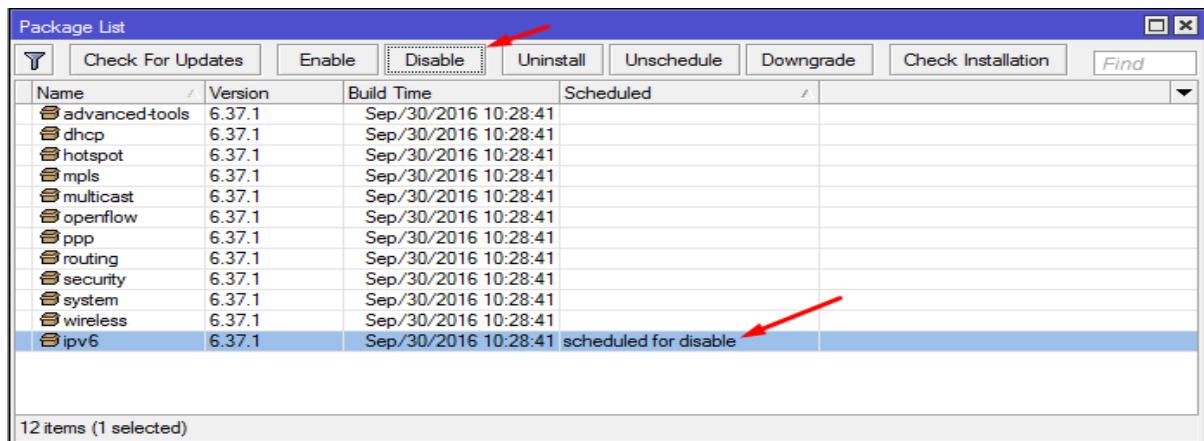
Pertama Kita Harus Masuk Ke Winbox dahulu..Disini saya akan Mencontoh kan Men-Disable Package IPv6..

- Klik System > Package



- Pilih Package yang akan di Disable (IPv6)
- Lalu klik Disable

Setelah Berhasil Maka Tampilan akan Berubah seperti ini..

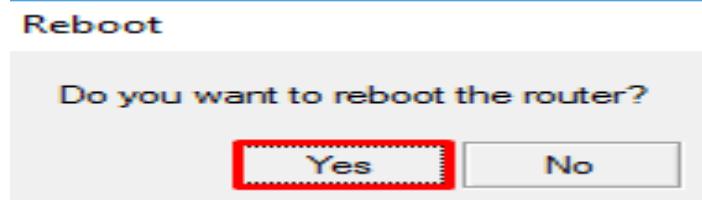


Package List				
	Name	Version	Build Time	Scheduled
	advanced-tools	6.37.1	Sep/30/2016 10:28:41	
	dhcp	6.37.1	Sep/30/2016 10:28:41	
	hotspot	6.37.1	Sep/30/2016 10:28:41	
	mpls	6.37.1	Sep/30/2016 10:28:41	
	multicast	6.37.1	Sep/30/2016 10:28:41	
	openflow	6.37.1	Sep/30/2016 10:28:41	
	ppp	6.37.1	Sep/30/2016 10:28:41	
	routing	6.37.1	Sep/30/2016 10:28:41	
	security	6.37.1	Sep/30/2016 10:28:41	
	system	6.37.1	Sep/30/2016 10:28:41	
	wireless	6.37.1	Sep/30/2016 10:28:41	
	ipv6	6.37.1	Sep/30/2016 10:28:41	scheduled for disable

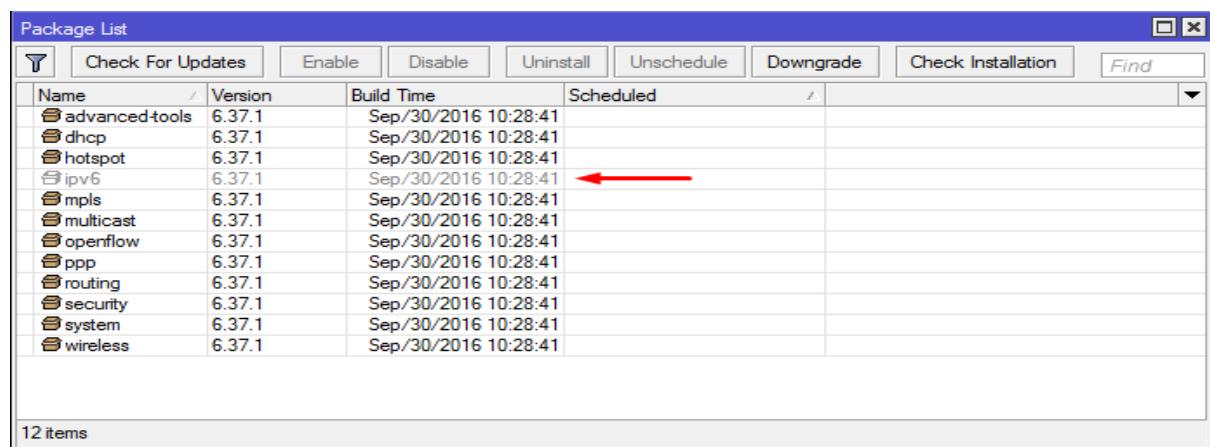
Setelah Step ini.. IPv6 akan ada Status Scheduled for disable yang artinya dijadwalkan untuk menonaktifkan.. jadi IPv6 akan dinonaktifkan Ketika router telah di Reboot/Restart.

Maka step selanjutnya Kita harus Me-Reset RouterBoard..

- Klik System > Reboot > Yes



Jika Router sudah Di restart kita bisa melihat Package IPv6 sudah di di Disable



Package List				
	Name	Version	Build Time	Scheduled
	advanced-tools	6.37.1	Sep/30/2016 10:28:41	
	dhcp	6.37.1	Sep/30/2016 10:28:41	
	hotspot	6.37.1	Sep/30/2016 10:28:41	
	ipv6	6.37.1	Sep/30/2016 10:28:41	disabled
	mpls	6.37.1	Sep/30/2016 10:28:41	
	multicast	6.37.1	Sep/30/2016 10:28:41	
	openflow	6.37.1	Sep/30/2016 10:28:41	
	ppp	6.37.1	Sep/30/2016 10:28:41	
	routing	6.37.1	Sep/30/2016 10:28:41	
	security	6.37.1	Sep/30/2016 10:28:41	
	system	6.37.1	Sep/30/2016 10:28:41	
	wireless	6.37.1	Sep/30/2016 10:28:41	

Untuk Men-Disable banyak Package sekaligus Kita bisa menekan CTRL untuk menandai beberapa Package yang akan kita Disable/Uninstall

Selanjutnya saya akan menjelaskan cara Men-Disable lewat Terminal (Telnet/SSH)

Di sini saya akan mencontohkan bagaimana Men-Disable Package lewat terminal (Telnet)

Pertama kita harus terkoneksi ke Router lewat Telnet...

- Ketik System Package Print=Untuk Melihat List Package MikroTik

Untuk Men-Disable melalui Terminal kita harus tau List Number Package yang akan kita disable..

The screenshot shows a Telnet session connected to 192.168.2.3. The user is navigating through the system package configuration. In the first part, the user runs `/system package print`, which lists various packages with their names and versions. The `ipv6` package is highlighted with a red box. In the second part, the user runs `/system package disable 4`, where `4` corresponds to the number of the `ipv6` package. In the final part, the user runs `/system package print` again, and the `ipv6` package now has a status of "scheduled for disable", indicated by a red box.

```
[admin@MikroTik] > system package
[admin@MikroTik] /system package> print
Flags: X - disabled
# NAME VERSION SCHEDULED
0 PPP 6.37.1
1 openflow 6.37.1
2 advanced-tools 6.37.1
3 dhcp 6.37.1
4 ipv6 6.37.1
5 mpls 6.37.1
6 multicast 6.37.1
7 security 6.37.1
8 wireless 6.37.1
9 hotspot 6.37.1
10 routing 6.37.1
11 system 6.37.1
[admin@MikroTik] /system package> disable 4
[admin@MikroTik] /system package> print
Flags: X - disabled
# NAME VERSION SCHEDULED
0 PPP 6.37.1
1 openflow 6.37.1
2 advanced-tools 6.37.1
3 dhcp 6.37.1
4 ipv6 6.37.1 scheduled for disable
5 mpls 6.37.1
6 multicast 6.37.1
7 security 6.37.1
8 wireless 6.37.1
9 hotspot 6.37.1
10 routing 6.37.1
11 system 6.37.1
[admin@MikroTik] /system package>
```

Di sini saya akan Men-Disable Package IPv6

- Kita Ketik Disable 4 (4 adalah number list IPv6)

Setelah kita memberikan perintah tersebut .kita perlu melihat status Package nya =System Package Print... IPv6 akan ada Status Scheduled for disable yang artinya dijadwalkan untuk menonaktifkan..jadi IPv6 akan dinonaktifkan Ketika router telah di Reboot/Restart.

Lab 6. Meng-Upgrade Paket MikroTik

Oke di lab ini saya akan menjelaskan cara meng-Upgrade Paket Mikrotik.....Untuk apa Paket MikroTik di Upgrade? Paket MikroTik di Upgrade untuk mengatasi/mengganti Bug (kerusakan/kehilangan) pada Versi sebelumnya..untuk meng-Upgrade paket mikrotik kita harus memiliki Paket (package) terbaru,untuk memiliki paket terbaru mikrotik kita bisa men-download nya di <http://www.mikrotik.com/download>....Pertama kita perlu mendownload paket terbaru mikrotik di [mikrotik.com/download](http://www.mikrotik.com/download)...

MikroTik Indonesia - Up: MikroTik Routers and WiFi

Secure <https://mikrotik.com/download>

MikroTik Home Buy About Jobs Hardware Software Support Training Account

Software Downloads Changelogs Download archive RouterOS The Dude

Check For Updates in QuickSet or System > Packages menu in WebFig or WinBox.

You can find more information about version changes in Changelogs page.

RouterOS

	6.37.4 (Bugfix only)	6.38.1 (Current)	5.26 (Legacy)	6.39rc26 (Release candidate)
MIPSBE	CRS, D10C, LDF, LHD, Merlin, Merlin+, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, eAP, HEX, wAP, BaseBox, DynaDisk, RB2011, SXT, Omnitil, Groove, Metal, Sentair, RB750r			
Main package	Download	Download	Download	Download
Extra packages	Download	Download	Download	Download
SMIPS	hAP lite			
Main package	Download	Download	-	Download
Extra packages	Download	Download	-	Download
TILE	CCR			
Main package	Download	Download	-	Download
Extra packages	Download	Download	-	Download

Versi Terbaru

<https://mikrotik.com>

Oke di sini saya akan men-download package/paket SMIPS versi 6.38.1(Current) yaitu versi paling baru saat ini, Kenapa saya mendownload paket SMIPS? Karna di lab ini saya menggunakan RouterBoard Hap-Lite dan Hap-Lite itu memakai RouterOS SMIPS,dan di sini saya akan mendownload MAIN PACKAGE..apa perbedaan Main Package dan Extra Package? Kalo kita men-Download Main Package maka hasil download-an nya adalah 1 file yang berformat (.NPK) jadi kesimpulannya Main package adalah sebuah file yang mewakili semua package dalam 1 file ...dan jika kita men-Download Extra Package hasil Download-an nya akan berformat (.zip) /sebuah RAR setelah itu kita perlu meng-Extract nya agar semua kita bisa melihat semua package Mikrotik yang ada di dalam File tersebut,di dalam file tersebut ada 12 package Mikrotik yang format nya (.NPK) file tersebut terpisah sesuai kegunaanya masing masing ,Contoh:ada file Wireless,DHCP,System,Security dan lain lain...

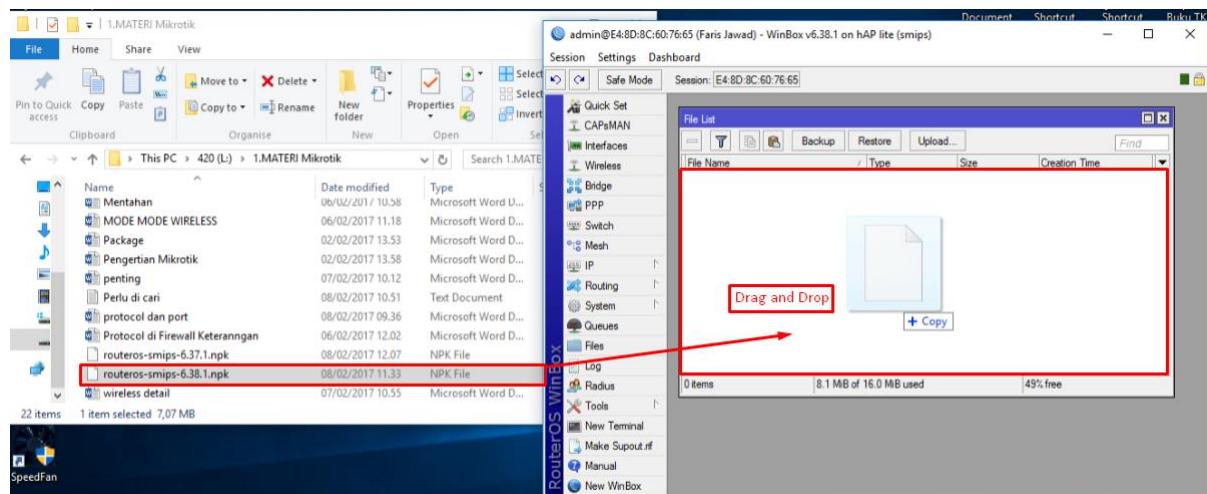
Oke cara pertama adalah cara Drag and Drop dari folder ke Files(Winbox)

*Catatan: sebelum kita men-Drag and Drop pastikan Meng-Kosongkan/Mem-Backup Files Yang ada di Penyimpanan (Disk) RouterBoard,karna berasa Jika Disk RouterBoard Kepenuhan maka Paket Kita Tidak bisa masuk/Masuk tapi tidak Sempurna,karna Disk yang di miliki RouterBoard biasanya Kecil,dan itu sering membuat Kita gagal Meng-Upgrade Paket Mikrotik..

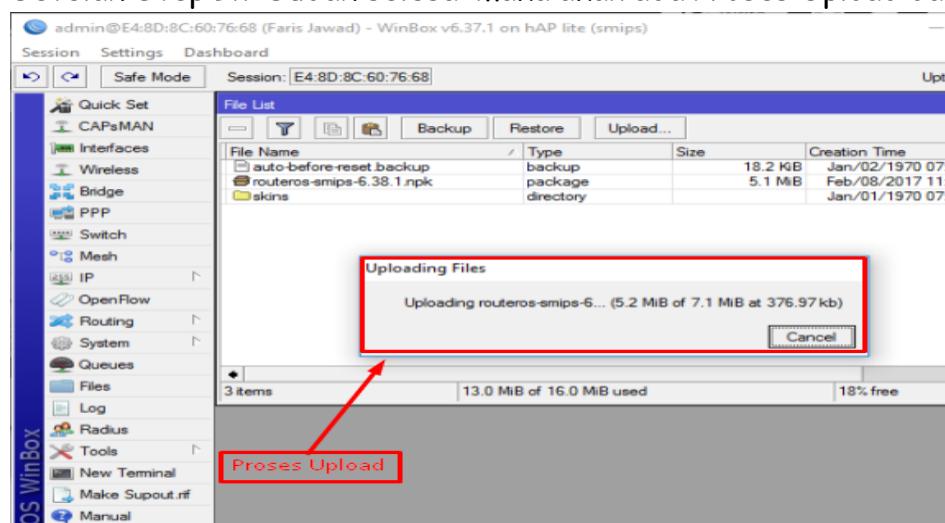
Di Lab ini saya Akan Mencoba Meng-Upgrade Paket MikroTik Dari Versi 6.37.1 ke Versi 6.38.1 (terbaru)

Oke kita lanjut ke Lab nya ...

- Pertama kita cari file paket yang telah kita Download
- Lalu kita Drag and Drop ke Files (winbox)



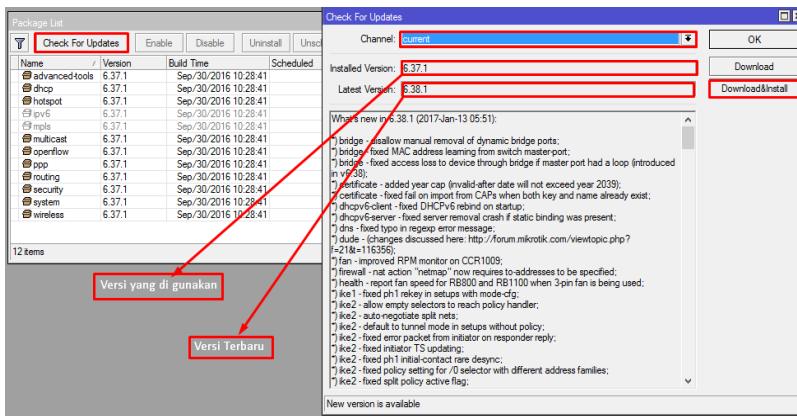
Setelah Step Ini Sudah selesai maka akan ada Proses Upload dari PC ke Router nya



Cara kedua.. kita akan mendownload paket nya langsung dari RouterBoard...Jika Kita menggunakan cara ini,RouterBoard kita harus Terkoneksi ke Internet

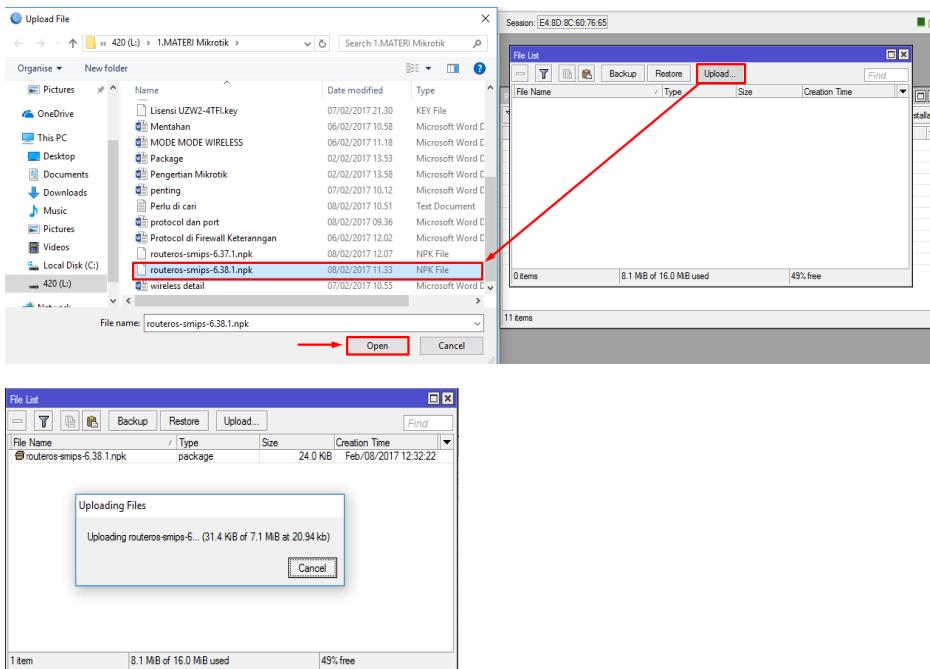
Oke langsung saja kita lanjut Ke Lab nya

- Klik System > Package > Check For Updates
- Kita Isi Channel=Current
- Klik Download&Install



Cara Ketiga...Cara ketiga ini kita akan Meng-Upload langsung paket dari winbox

- Klik Files > Upload
- Lalu kita cari hasil download Paket terbaru yang telah kita Download
- Lalu Open



Lab 7. Downgrade Paket Mikrotik

Oke di lab ini saya akan Menjelaskan bagaimana cara nya Men-Downgrade Paket Mikrotik..

Apakah Kita perlu Men-Downgrade Paket Mikrotik ? Jelas Kita Perlu ... karna terkadang ada aja problem seperti: RouterBoard Kita Tidak Kompatible dgn Paket MikroTik yang terbaru jadi kita perlu men-Downgrade Paket Mikrotik Kita

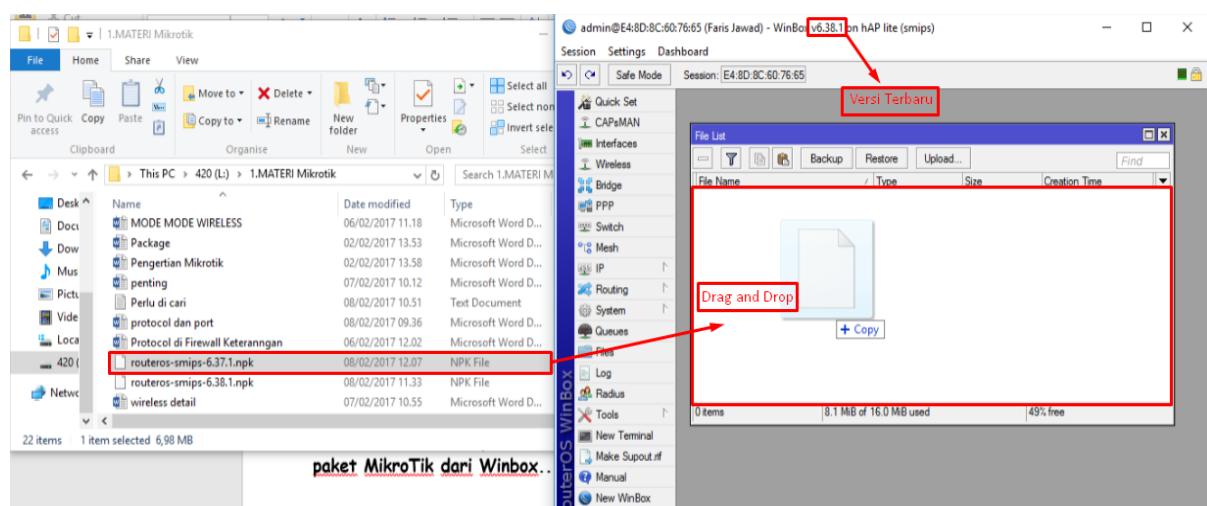
Cara Men-Downgrade paket MikroTik hampir sama dengan Meng-Upgrade...

Untuk Men-Downgrade Kita Juga perlu Men-Drag and Drop Ke files (winbox)/ mengupload paket dari Winbox langsung.cara nya telah saya contohkan di lab sebelum nya...

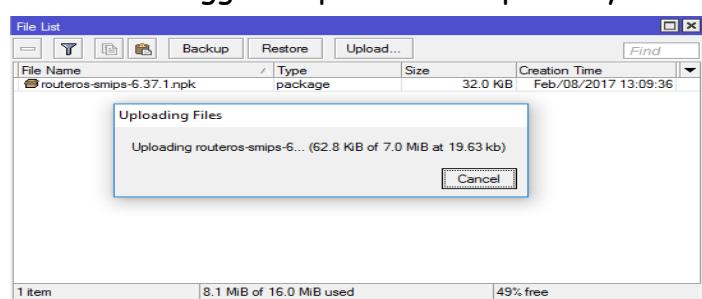
Di lab ini saya akan Mencoba Men-Downgrade paket MikroTik dari Versi 6.38.1 ke 6.37.1

OKe langsung saja Kita ke Lab nya...

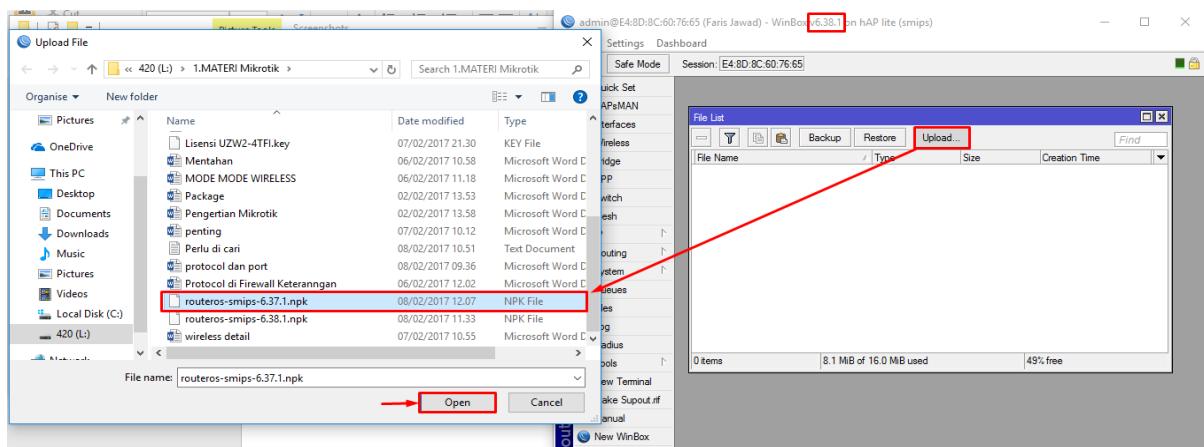
- Pertama Kita Drag and Drop dari file ke Files (winbox)



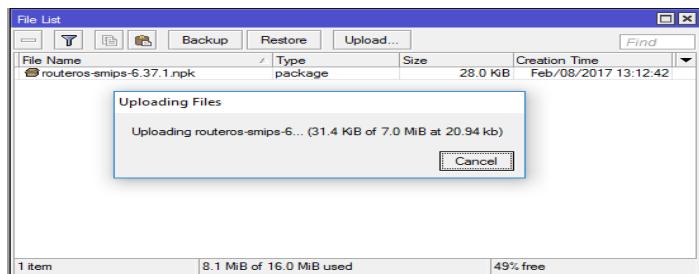
Lalu kita Tunggu sampai Proses Upload nya selesai..



atau kita bisa langsung meng-Upload paket MikroTik dari Winbox..

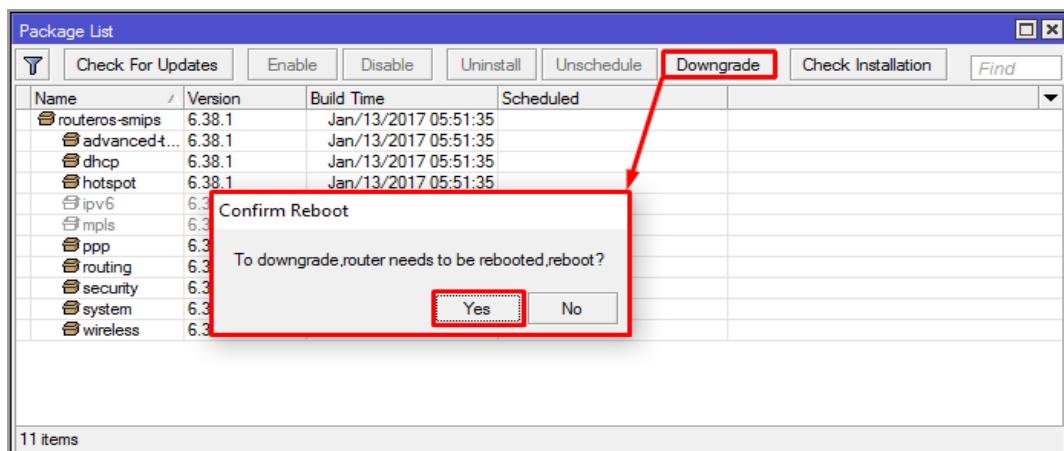


Tunggu sampai Proses Upload nya selesai...



Step Selanjutnya adalah Proses Men-Downgrade nya ...

- Klik System > Package
- Klik Downgrade > Yes



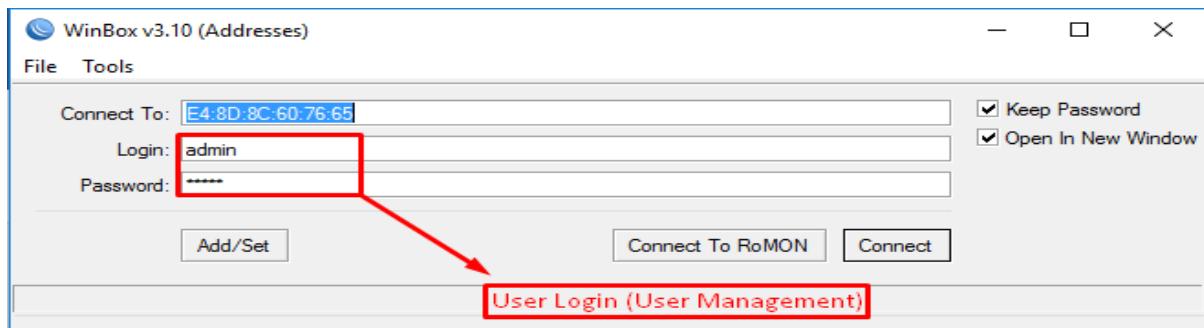
Setelah RouterBoard di Restart maka Versi paket akan Menurun Ke versi 6.37.1
😊



Lab 8. User Management

Oke di lab ini saya akan Menjelaskan Tentang User management..Apa Fungsi User Management? Fungsi utama dari User Management adalah Melindungi Router MikroTik Kita, agar tidak semua orang bisa meng-config router kita sembarangan ...karna Untuk masuk dan Meng-Config Router MikroTik Kita perlu menggunakan User Management.User Management bisa dibilang sama dengan User Login atau User yang kita gunakan Untuk masuk Ke system Mikrotik..

Pada dasar nya RouterBoard Mikrotik Memiliki User Management (User Login) Default yaitu: User (Login)=admin ,Password=(kosong)



Kita bisa Membuat Banyak User Management di MikroTik,Misalnya Kita bisa Membuat User Untuk Rekan Kita yang sama sama meng-Handle jaringan di daerah kita,kta bisa membuatkan dia Usermanagement dengan hak akses Full/Write,atau kita bisa membuat user untuk Teman kita yang hanya ingin melihat/Memonitoring jaringan Kita,

Oke ini adalah sedikit penjelasan Tentang Akses Full,Write dan Read:

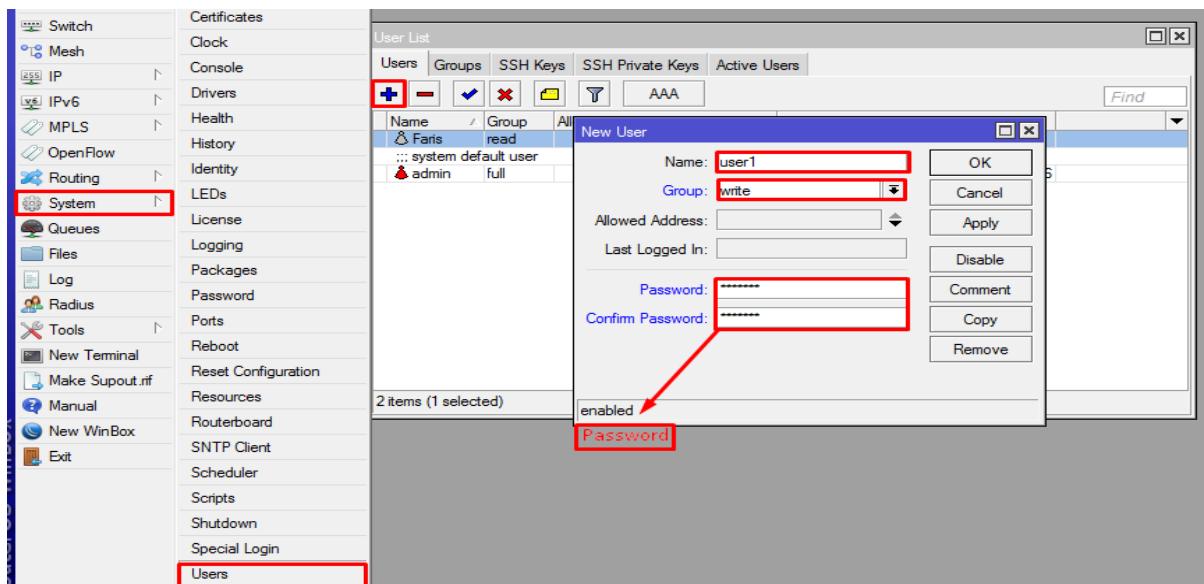
Full --> user yang memiliki akses ini merupakan user dengan pangkat paling tinggi, yang dapat melakukan konfigurasi seperti menghapus konfigurasi, menambahkan konfigurasi, sampai dengan menambahkan user baru ke dalam sistem Mikrotik.

Write --> user ini memiliki akses ini hampir sama seperti user yang memiliki akses Full, namun bedanya Akses Write tidak dapat menambahkan user baru, dan juga tidak dapat melakukan proses backup konfigurasi.

Read --> user dengan akses ini hanya mampu melakukan monitoring pada sistem, tidak mampu melakukan konfigurasi seperti pada user dengan memiliki akses Write maupun Full.

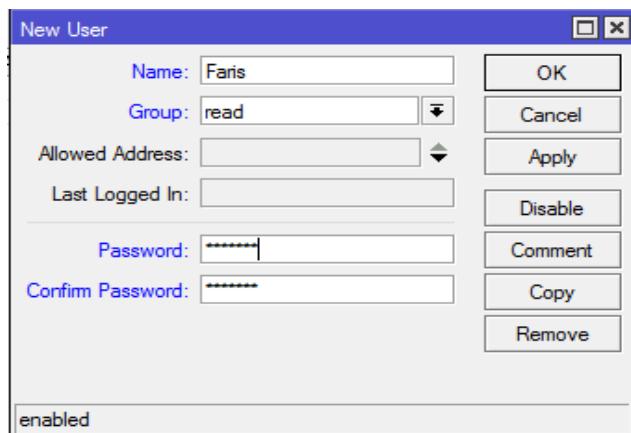
Oke pertama Kita akan mencoba membuat User dengan Akses Write dan Read..

- Klik System > User > add (+)
- Kita isikan name=User1 (terserah kita) Group=Write Password=(terserah)



Selanjutnya Kita buat User dengan akses Read...

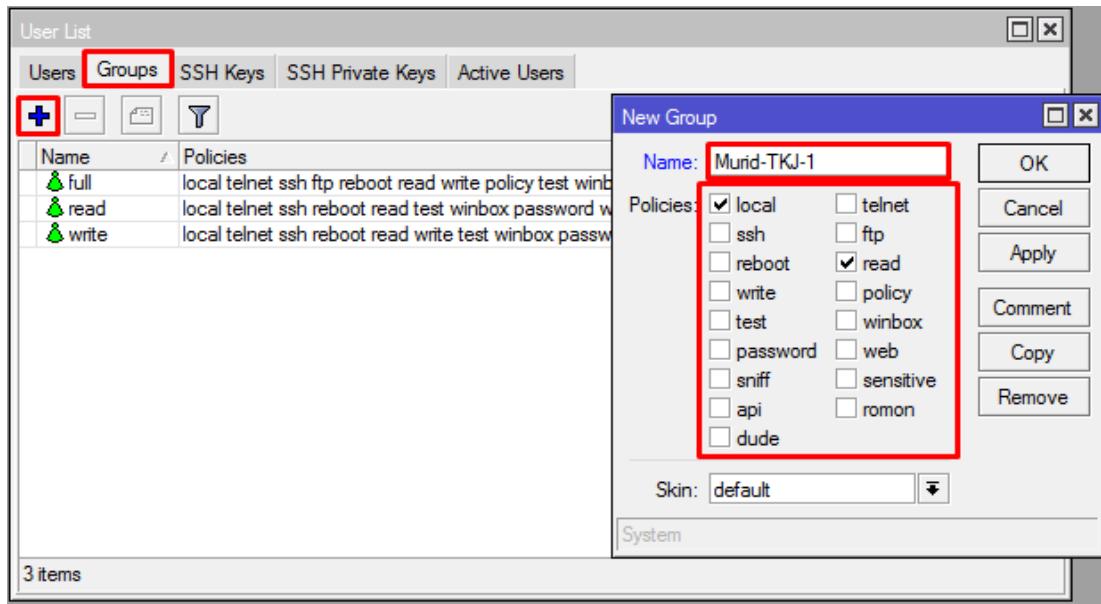
- Klik System > User > add (+)
- Kita isikan name=Faris (terserah kita) Group=Read Password=(terserah)



Untuk Akses User nya kita juga bisa Meng-Costum nya dgn cara membuat Group...di sana kita bisa meng-Costum sesuai keinginan kita....

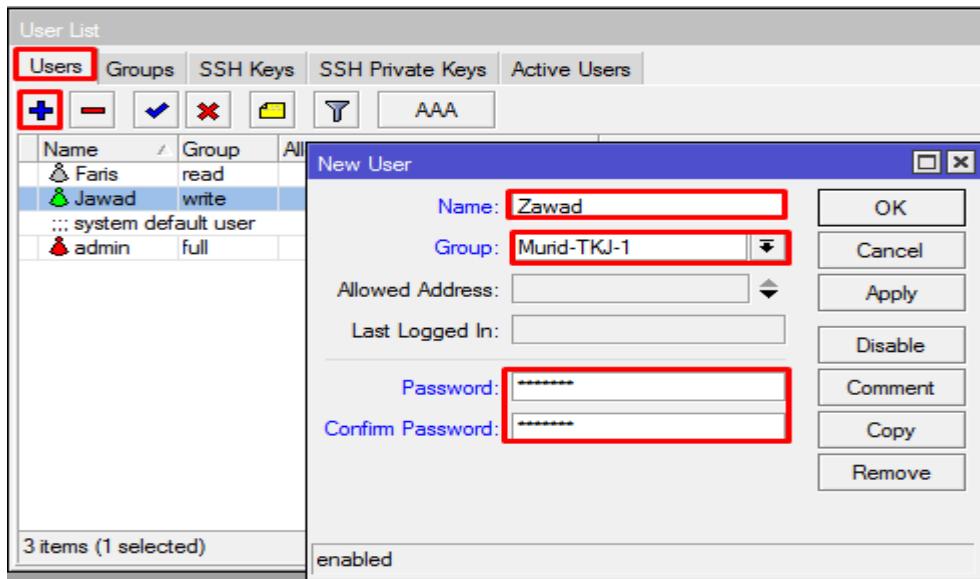
Oke di Langsung saja Kita Coba,Pertama kita Kita harus membuat Group Untuk user..

- Klik System > User > Group > Add (+)
- Isi name=Murid-TKJ-1 (Terserah kita), Policies Kita Ceklis Sesuai Kebutuhan User..



- Lalu Apply dan OK

Selanjut nya kita akan Membuat user dengan Group akses Murid-TKJ-1,cara nya sama seperti membuat user sebelumnya,hanya bedanya Group kita isi dengan Group yang telah kita buat (Murid-TKJ-1)..



Nah selanjutnya saya akan sedikit menjelaskan Tentang Policies beserta Keterangannya:

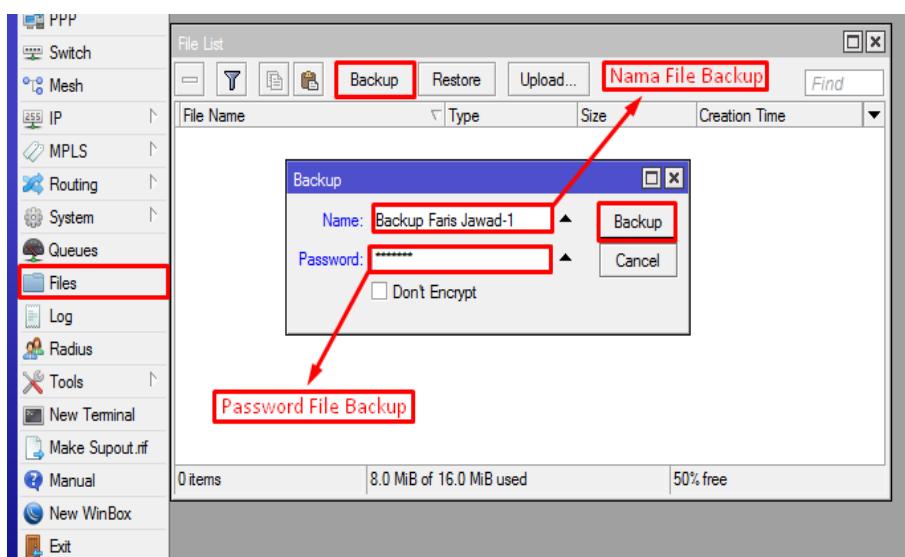
- telnet : kebijakan yang mengijinkan user login secara remote via telnet
- ssh : kebijakan yang mengijinkan user login secara remote via secure shell protocol
- ftp : Kebijakan yang mengijinkan hak penuh login via FTP, termasuk transfer file dari/menuju router. User dengan kebijakan ini memiliki hak read, write, dan menghapus files.
- reboot : Kebijakan yang mengijinkan user me-restart router.
- read : Kebijakan yang mengijinkan untuk melihat Konfigurasi router. Semua command console yang tidak bersifat konfigurasi bisa diakses.
- write : Kebijakan yang mengijinkan untuk melakukan konfigurasi router, kecuali user management. Policy ini tidak mengijinkan user untuk membaca konfigurasi router, user yang diberikan policy write ini juga disarankan juga diberikan policy read.
- policy : Kebijakan yang memberikan hak untuk management user. Should be used together with write policy. Allows also to see global variables created by other users (requires also 'test' policy).
- test : Kebijakan yang memberikan hak untuk menjalankan ping, traceroute, bandwidth-test, wireless scan, sniffer, snooper dan test commands lainnya.
- web : Kebijakan yang memberikan hak untuk remote router via WebBox
- winbox : Kebijakan yang memberikan hak untuk remote router via WinBox
- password : Kebijakan yang memberikan hak untuk mengubah password
- sensitive : Kebijakan yang memberikan hak untuk melihat informasi sensitif router, misal secret radius, authentication-key, dll.
- api : Kebijakan yang memberikan hak untuk remote router via API.
- sniff : Kebijakan yang memberikan hak untuk menggunakan tool packet sniffer.

Lab 9. Backup, Export dan Import Settingan Mikrotik

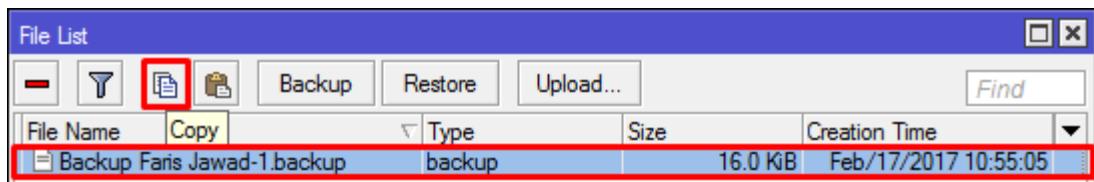
Di lab ini saya akan menjelaskan Tentang Backup,Export dan Import Konfigurasi Mikrotik, Apa Fungsi Backup Konfigurasi? Backup Konfigurasi berguna ketika router kita tiba tiba eror kita hanya meng-Upload konfigurasi Router yang telah kita backup..jadi kita tidak perlu men-Setting ulang RouterBoard kita..Lalu Apa perbedaan Backup dan Export Konfigurasi ? Jika Mem-Backup Konfigurasi artinya kita mem-Backup semua Konfigurasi yang ada di RouterBoard dan format nya .backup dan hasil backup tidak bisa di buka notepad dan tidak bisa di edit,berbeda dengan Export,kalau kita ingin meng-Export konfigurasi kita hanya bisa menggunakan CLI/Terminal dan format hasil Export adalah .rsc dan file hasil backup bisa di lihat dan di edit di notepad dan salah satu keunggulan Export adalah bisa menyimpan konfigurasi Per-Fitur yang ingin di Export (Tidak semua Konfigurasi di Export) contoh kita bisa meng-Export Konfigurasi Wireless/Firewall dll.... Dan yang terakhir adalah Import.. Import adalah kita memasukan Konfigurasi yang telah kita Backup/Export ke dalam Router..

Oke Pertama saya akan menjelaskan cara Backup seluruh Konfigurasi Router..

- Klik Menu File lalu Klik Backup
- Lalu Kita isikan Name dan password sesuai keinginan kita



Jika Sudah Maka File Konfigurasi Akan ada di File List

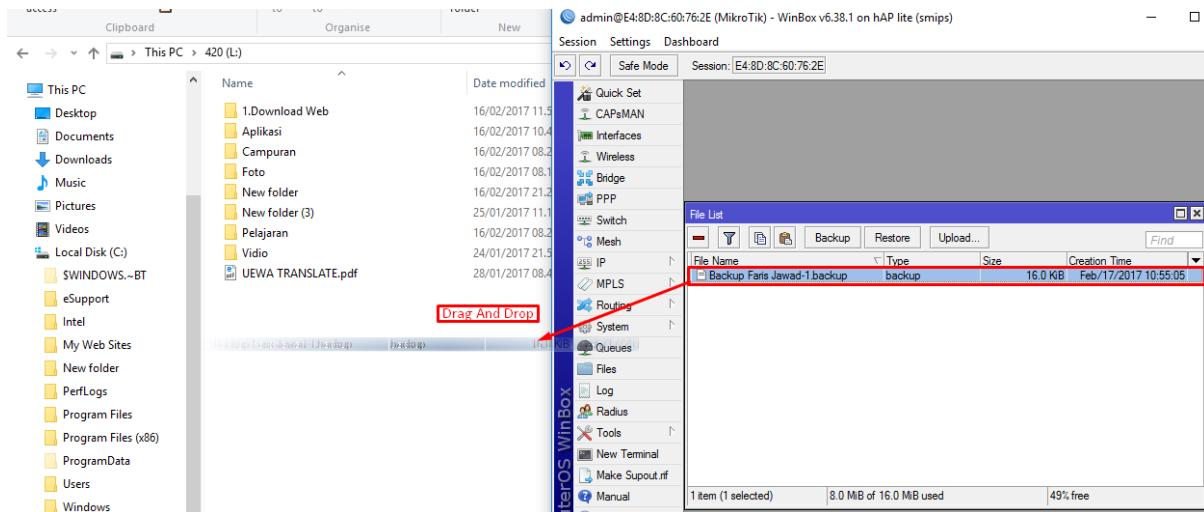


Setelah Step ini kita bisa mengambil hasil backup tersebut untuk di simpan di Pc kita, ada dua cara Untuk mengambil hasil Backup nya..Car pertama adalah cara Drag And Drop dan cara kedua Adalah Dengan Menggunakan Protocol FTP

Pertama saya akan menjelaskan Cara mengambil konfigurasi dengan cara Drag And Drop...

Oke cara ini adalah cara paling mudah untuk meng-Copy hasil backup ke PC kita ..

- Kita pilih File Backup yang ingin Di-Copy
- Lalu kita Drag And Drop ke folder



Lalu kita hanya tinggal menunggu saja sampai proses Drag and Drop nya selesai...

Cara ke dua untuk mengambil Konfigurasi dari RouterBoard adalah menggunakan FTP.....

Apa Itu FTP? FTP adalah File Transfer Protocol yang Berfungsi untuk transfer File Dari Komputer Ke Device yang lain,FTP Menggunakan Protocol TCP Port 20,di pembahasan ini Router akan di fungsikan sebagai FTP server dan Pc kita Sebagai FTP Client jadi intinya FTP client meminta data Hasil Konfigurasi yang ada di FTP Server (RouterBoard).Cara Menggunakan Protocol FTP untuk mengambil Konfigurasi dari Router adalah FTP client cukup membuka Web Browser dan memasukan [ftp://\(ip-router\)](ftp://(ip-router)) lalu klik enter...

- Masuk Web Browser dan Masukan <ftp://192.168.97.1> (Ip router/Gateway) di URL



Index of /

Name	Size	Date Modified
Backup Faris Jawad-1.backup	16.0 kB	2/17/17, 10:55:00 AM

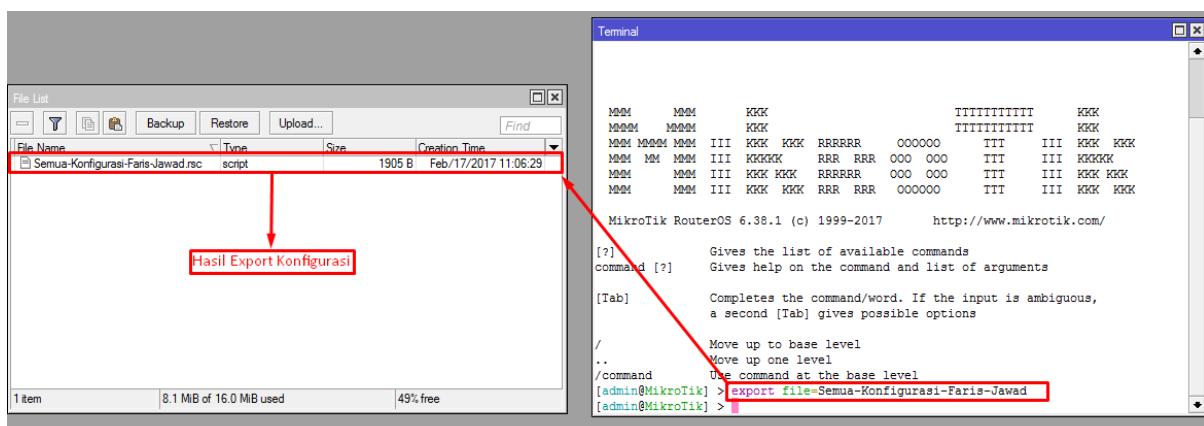
- Lalu di kita Klik hasil backup nya maka akan Otomatis Ter-Download

Lalu Kita hanya perlu mencari hasil download tersebut ...

Oke Selanjutnya saya menjelaskan cara Meng-Export konfigurasi, Export hanya bisa di lakukan lewat CLI (terminal,SSH/Telnet) oke di lab ini saya akan mencoba meng-Export seluruh konfigurasi dan Meng-Export konfigurasi Per-Fitur (Routing)...

Pertama saya akan mencoba meng-Export seluruh Konfigurasi..

- Masukan Perintah "Export File: (Nama-Hasil-Konfigurasi)"
- Lalu Enter



Lalu di menu File List akan keluar Hasil Export seluruh konfigurasi kita...

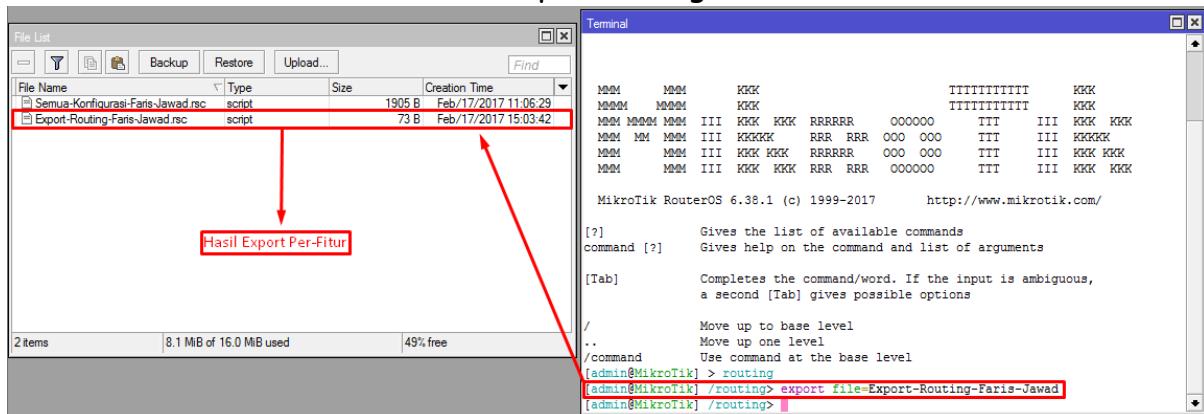
Selanjutnya saya Meng-Export Konfigurasi Per-Fitur (routing)..

- Masukan perintah "Routing" lalu Enter

Setelah kita masuk Ke menu Routing melalui CLI perintah selanjutnya adalah

- Masukan Perintah "Export File: (Nama-Hasil-Konfigurasi)"

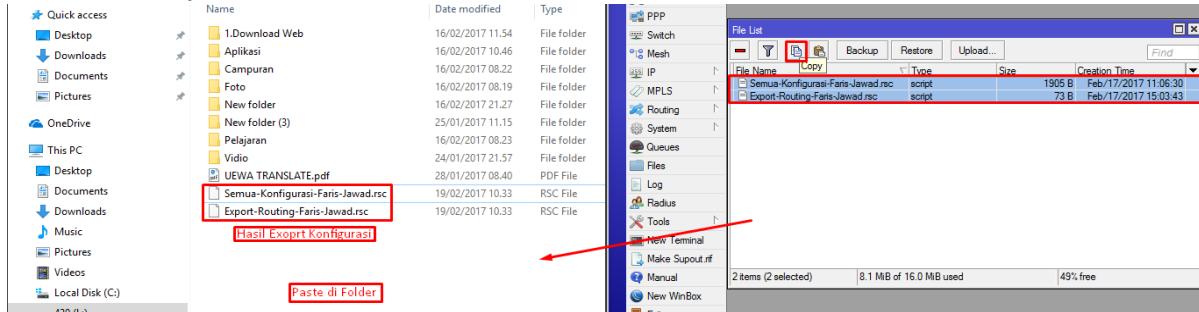
Lalu akan muncul di File list hasil Export Konfigurasi Per-Fitur tersebut,



Oke setelah kita men-Export seluruh Konfigurasi dan meng-Export konfigurasi Per-Fitur selanjutnya kita perlu memindahkan File tersebut ke PC kita ,ada dua cara untuk memindahkan Hasil Export ke PC kita,cara pertama adalah cara Copy paste dan cara kedua dgn cara Drag and Drop.....

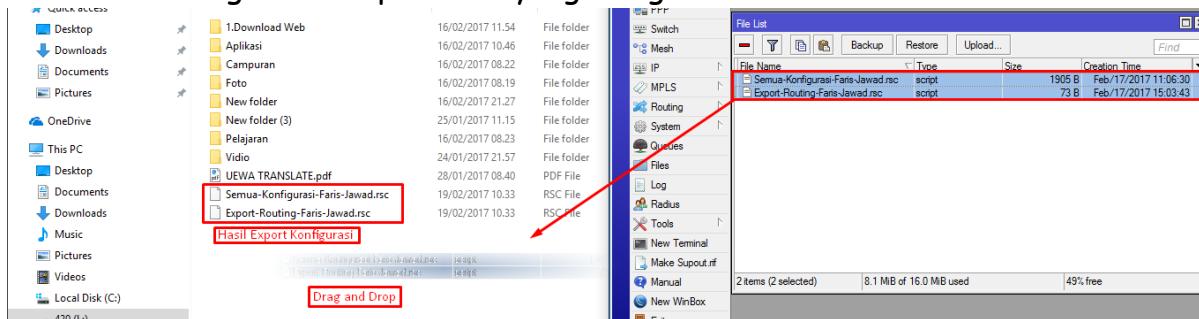
Pertama saya akan menggunakan cara Copy paste

- Kita pilih File yang ingin di Copy di File List Lalu klik Icon Copy 
- Selanjutnya kita hanya perlu mem-Paste di File yang diinginkan



Itu adalah cara memindahkan hasil Export ke PC dengan cara Copy Paste ,selanjutnya saya akan Menggunakan cara ke dua yaitu Drag And Drop,cara nya sama seperti memindahkan Backup dengan cara Drag And Drop....

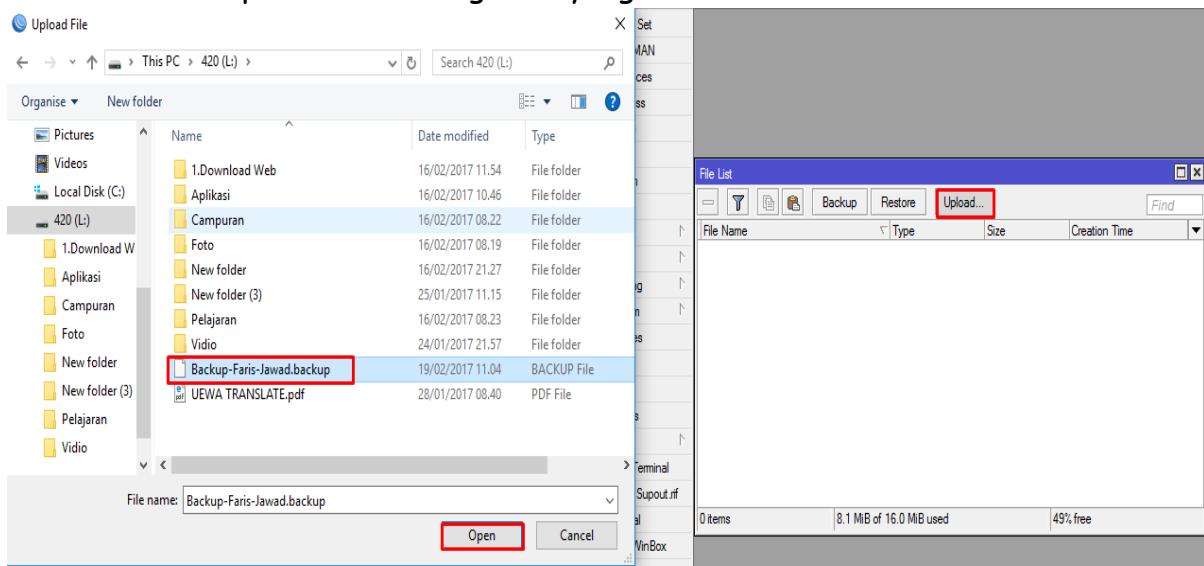
- Pilih File yang ingin di pindahkan
- Lalu Drag And Drop Ke File yang Diinginkan



Selanjutnya saya Menjelaskan Tentang Import Konfigurasi ,Import Konfigurasi Berguna Untuk Memasukan File Konfigurasi dari PC (External) ke Router , cara Untuk Men-Import Konfigurasi adalah dengan cara Upload...

Oke langsung saja kita Upload file Konfigurasi ,cara upload Konfigurasi sama seperti Meng-Upgrade Package bedanya file yang di upload adalah Hasil Konfigurasi Bukan File Package ...

- Klik Upload **Upload...** di Menu File List
- Lalu Kita pilih hasil Konfigurasi yang ada di File



Lab 10. Reset Konfigurasi

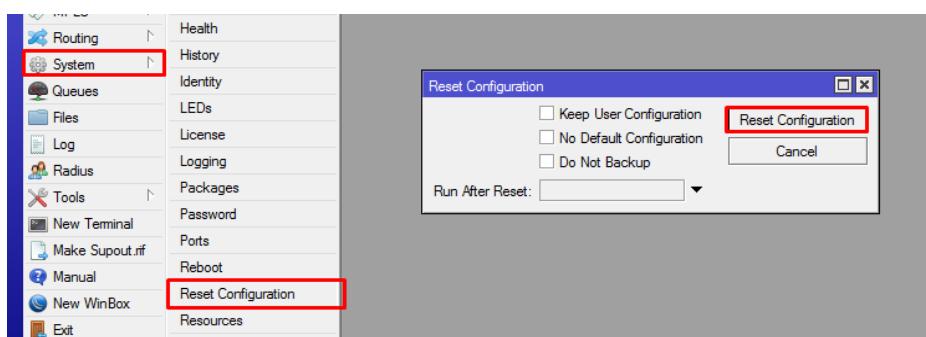
Oke di lab ini saya akan menjelaskan bagaimana cara Mereset Konfigurasi Dengan Soft Reset ,Hard Reset dan Net-Install

❖ Soft Reset..

Soft reset adalah Menghapus semua Konfigurasi router menjadi Settingan Pabrik (default) ,Soft Reset bisa di lakukan Melalui GUI/Terminal..

OKe pertama saya mencontohkan bagaimana cara nya Soft Reset Melalui GUI (winbox).

- Klik System > Reset Configuration > Reset Configuration



Setelah Step Ini Router Akan Merestart sendiri,Waktu Booting setelah Restart adalah 30 detik,Setelah Selesai maka Router akan Kembali Seperti baru/kembali Ke settingan Pabrik (default)

Ketika Kita ingin mereset Router Kita,kita juga bisa Meng-Costum,Berikut Adalah Menu yang ada di Reset Configuration Beserta keterangannya-

- Keep User Configuration=Konfigurasi User Tidak akan Di Reset / User Tdk hilang
- No Default Configuration=Router Tidak Akan Menggunakan Konfigurasi Default/Router Tidak Memiliki Konfigurasi apapun
- Do Not Backup=Konfigurasi Tidak Akan Di backup

Nah Itu ada beberapa Keterangan Untuk Meng-Costum Ketika kita Ingin Mereset Konfigurasi Di router...

Selanjutnya saya akan Menjelaskan Bagaimana cara Untuk Mereset Konfigurasi Melalui CLI (Telnet)..

- Masukan Perintah "System Reset Configuration"

```
[admin@Faris-Jawad] > system reset-configuration
```

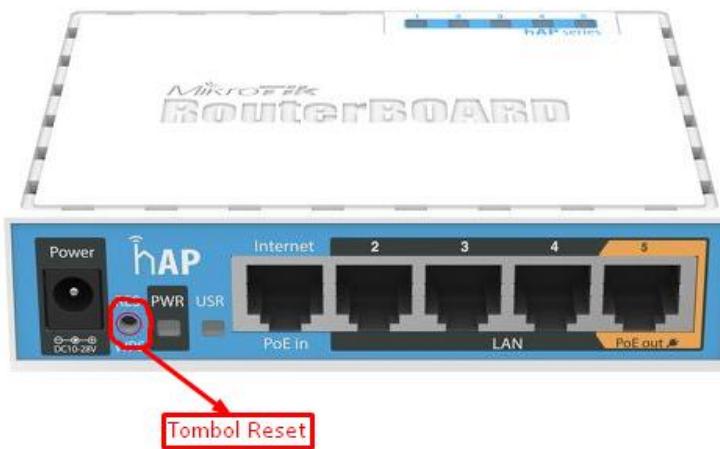
Kita Juga Bisa Meng-Costum Reset Konfigurasi Di CLI

```
keep-users --
no-defaults --
run-after-reset --
skip-backup --
```

<-Menu Costum Reset Konfigurasi

❖ Hard Reset

Selanjutnya saya akan Menjelaskan bagaimana cara Me-Reset Konfigurasi dengan cara Hard Reset..Maksud dari Hard Reset adalah kita me-Reset Router Lewat External (Luar)..



Di atas adalah contoh gambar sebuah RouterBoard.Untuk Hard Reset Kita Memerlukan Sebuah benda yang bisa masuk ke Tombol Hard Reset (Pulpen)

Oke langsung saja Kita Nge-Lab..

- Router Harus Dalam Keadaan Mati (Kabel Power Tidak Tersambung ke Router)
- Lalu Kita Masukan Benda (Pulpen) Ke dalam Tombol Power sampai terasa menekan suatu Tombol..
- Lalu kita colokan Kabel Power Ke Router
- Tunggu sampai Lampu Act (Kuning) Ber-Kedip kedip

Setelah lampu ACT selesai ber-kedip kedip itu tanda nya Router Sudah Di Reset..kita hanya perlu menunggu 30 detik maka Router siap digunakan Kembali...

❖ Net Install

Apa itu Net Install..????

Net Install adalah salah satu program yang berjalan di computer berbasis windows dengan protocol Bootp yang digunakan untuk menginstall routerOS melalui PC ke routerboard melalui Ethernet

Kapan kita menggunakan Net Install..???

Net Install biasa digunakan disaat:

1. Instalasi sebelumnya gagal
2. Os dalam router rusak
3. Password akses hilang
4. Apabila ingin mereset password/lupa password

Yang perlu kita miliki saat ingin melakukan Net Install adalah:

1. Software Net Install
2. Package MikroTik

Untuk memiliki Software tersebut kita bisa mendownload nya di Mikrotik.com..

-Download Software Net Install

Useful tools and utilities

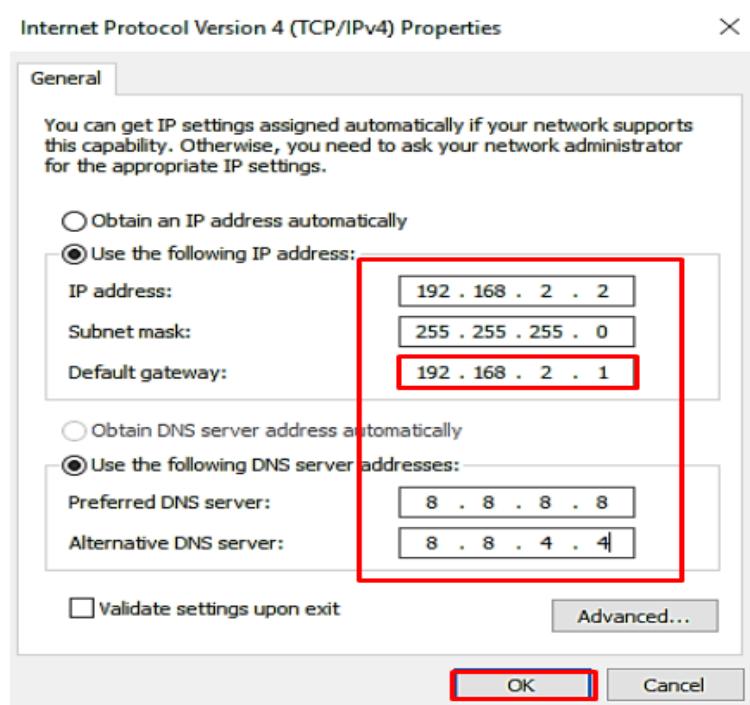
Winbox version 3.11	Configuration tool for RouterOS
Netinstall	RouterOS Installation tool
v3.30 mipsle	All packages for version 3.30 mipsle
Wireless link calculator	Wireless link probability calculator
Trafr	Traffic sniffer reader for Linux distributions
BTest	Bandwidth test tool for Windows
Neighbour	Neighbour viewer for Windows
Atheros	RouterBOARD wireless card drivers

Selanjutnya Kita download Package nya ..

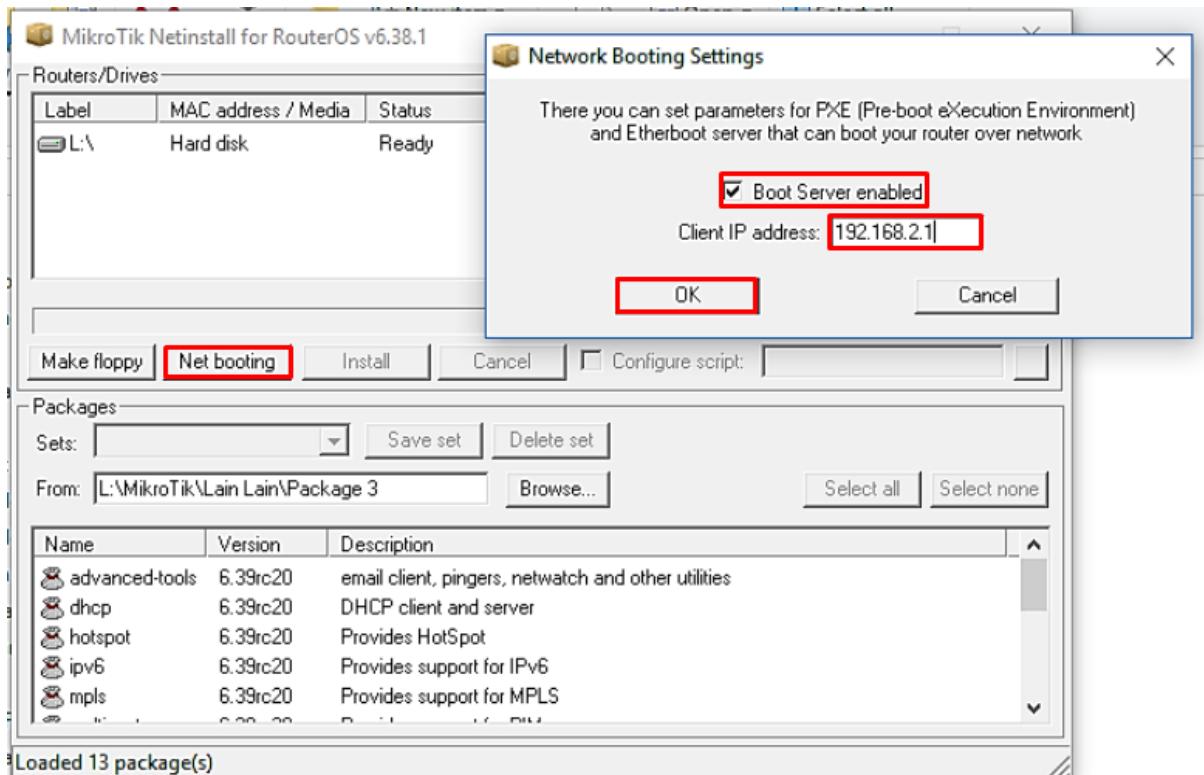
The screenshot shows the MikroTik Software download page. The URL in the address bar is <https://mikrotik.com/download>. The 'Software' tab is active. In the main content area, there's a table for the TILE package. The 'Download' button for the package is highlighted with a red box.

Untuk menggunakan Net-Install,Pertama kita Perlu men-Setting Ip addrees dan Gateway di PC kita ...

- Setting Ip address :192.168.2.2 dan Gateway :192.168.2.1
- Lalu Klik Ok

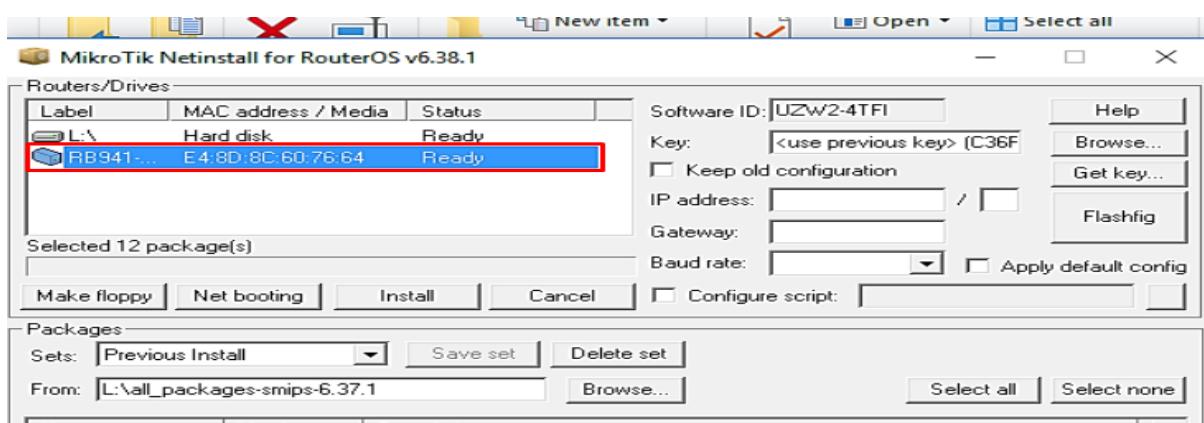


- Kita masuk Ke App Net Install
- Klik Net Booting > Ceklis Boot Server Enable
- Isi Client IP Address:192.168.2.1 (IP Gateway PC)



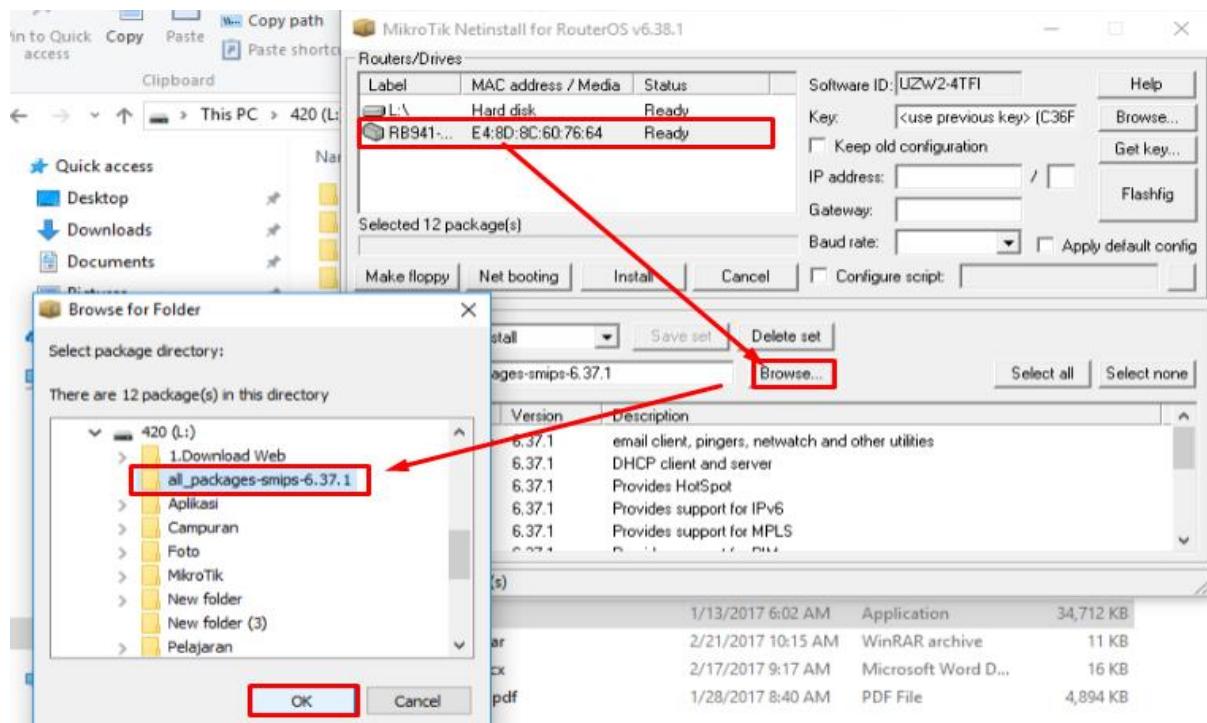
Jika step tersebut sudah selesai , Step selanjutnya adalah Me-Hard reset RouterBoard..

- Cabut Kabel Power dari RouterBoard
- Masukan Benda Ke Tombol Reset
- Colokan Kabel Power Ke RouterBoard
- Tunggu sampai Router Kita ter-Detec Oleh Net Install (15 Detik)

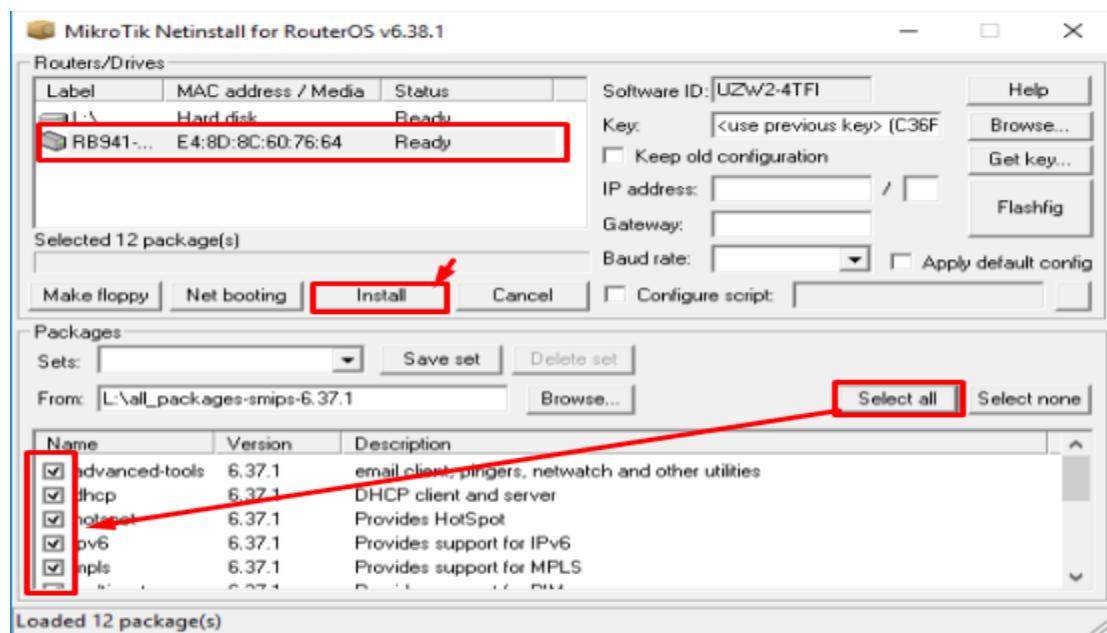


Setelah Step ini Maka RouterBoard akan ter-Detec di Net Install,...

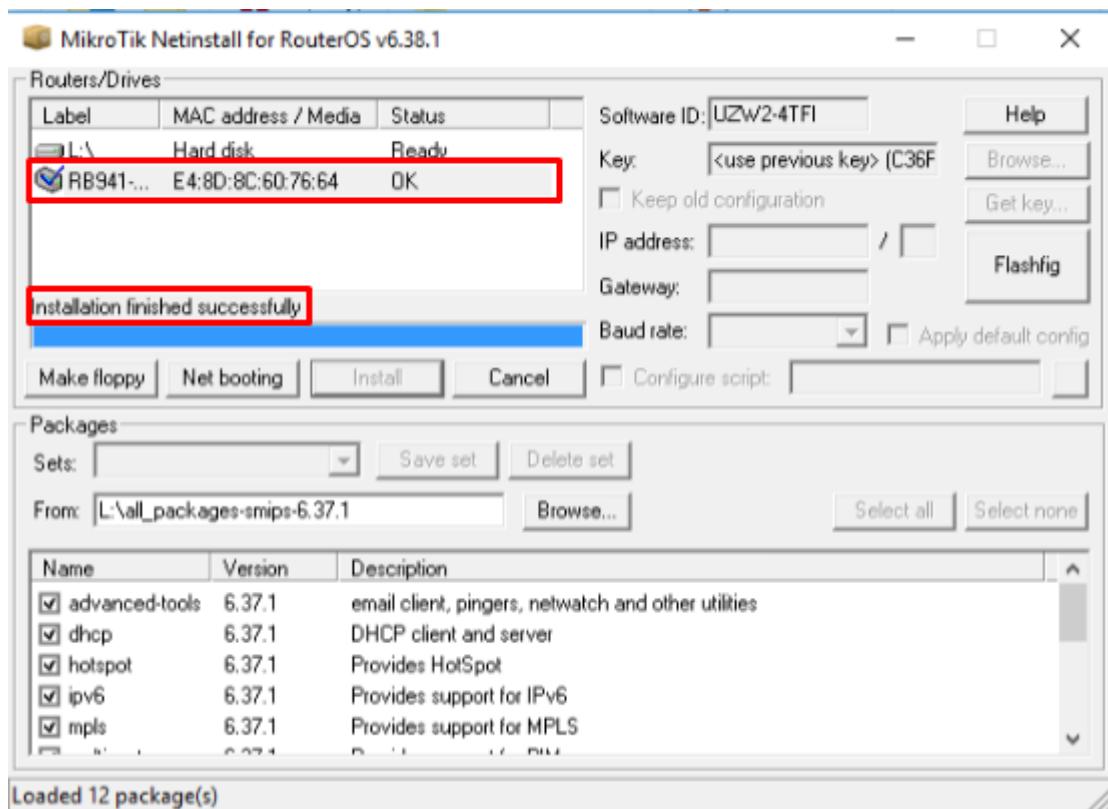
- Kita Klik Browse
- Lalu Pilih Package yang akan di Install Di RouterBoard
- Lalu Klik OK



- Selanjutnya adalah Klik Select all Untuk menandai Semua Package
- Lalu Klik Install



Setelah itu Kita hanya perlu menunggu sampai Peng-Instalan OS di RouterBoard Selesai...



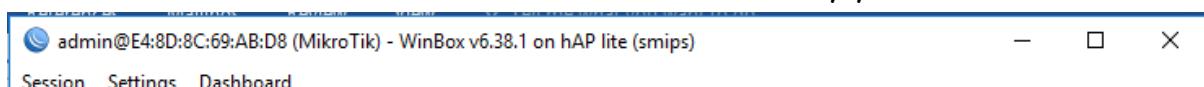
Jika sudah selesai maka RouterBoard akan kembali ke settingan Default..

Kata kata Motivasi

Lab 11. Router Identity

Oke di lab ini saya akan menjelaskan Tentang Router Identity..

Apa sih guna nya Router Identity ? Router Identity berfungsi Untuk Menamai Router/Memberi Identitas Router, Router Identity ini sangat Bermanfaat ketika kita menghandle jaringan besar yang kebanyakan router nya menggunakan MikroTik dengan Router Identity kita bisa menamai mana yang Router 1 dan 2 dst.. RouterBoard MikroTik Memiliki Default Router Identity yaitu:MikroTik



Untuk Mengganti Router Identity ada dua cara :

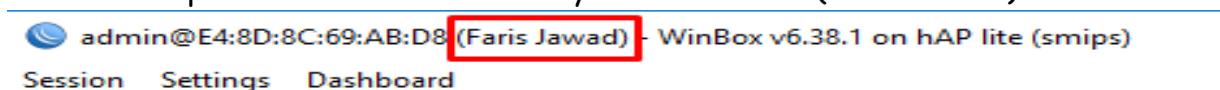
- GUI (Winbox/WebFig)
- CLI (Telnet,SSH,Terminal)

Di sini saya akan menjelaskan cara mengganti Router Identity Menggunakan GUI (Winbox), cara nya cukup mudah 😊

- Klik System > Identity
- Lalu Identity Kita isi sesuai keinginan kita (Faris Jawad)
- Lalu Apply dan OK



Setelah Step Ini maka Router Identity Akan Berubah (Faris Jawad)



Oke Selanjutnya saya akan menjelaskan bagaimana cara nya mengganti Router Identity menggunakan CLI (Telnet)

Oke di lab Ini saya akan mencoba mengganti Router Identity Faris Jawad Menjadi Zawad97

Pertama Kita harus Melihat Router Identity dlu dengan menggunakan Perintah: "System Identity Print"

```
[admin@Faris Jawad] > system identity print  
name: Faris Jawad
```

Lalu Kita akan mengganti Router Identity nya sesuai Keinginan Kita (Zawad97)

- Ketik "System Identity set name=Zawad97"

```
[admin@Faris Jawad] > system identity set name=Zawad97
```

Setelah Step ini Router Identity telah berubah Menjadi Zawad97

```
[admin@Zawad97] > system identity print  
name: Zawad97
```

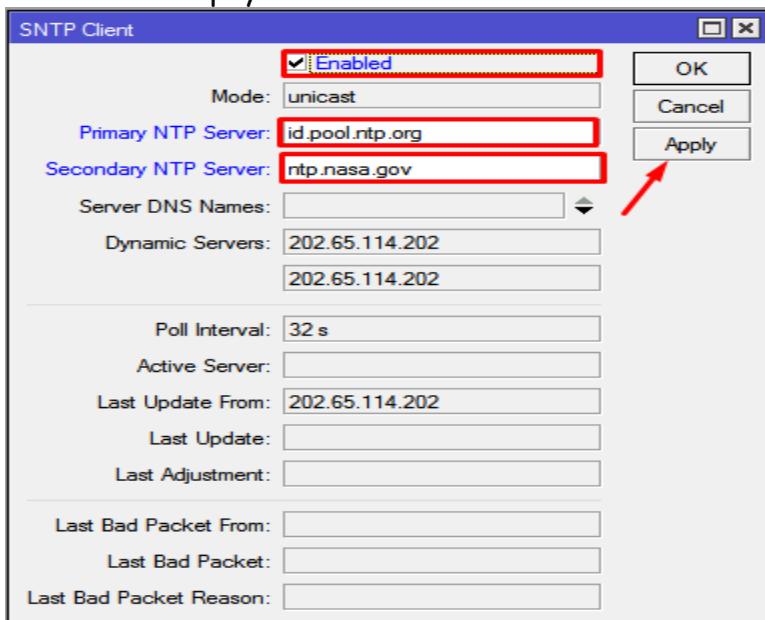
Lab 12. NTP (Network Time Protocol)

Di Lab Ini saya akan membahas tentang NTP (Network Time Protocol)...Apa itu NTP ? NTP adalah Suatu Protocol yang digunakan Untuk Sinkronisasi Waktu di Internet.. NTP menggunakan port komunikasi UDP dengan nomor Port 123. Protokol ini memang didesain untuk dapat bekerja dengan baik agar Device dapat mensinkronisasi waktu dengan Internet,karna terkadang ada Website yang tdk bisa di buka jika waktu kita tdk sinkron dengan waktu yang di internet...Dalam kondisi tertentu Router Mikrotik harus bekerja berdasarkan waktu, baik tanggal, hari, maupun jam.

Untuk daftar NTP server yang bisa kita gunakan dapat kita lihat di <http://www.pool.ntp.org/> .

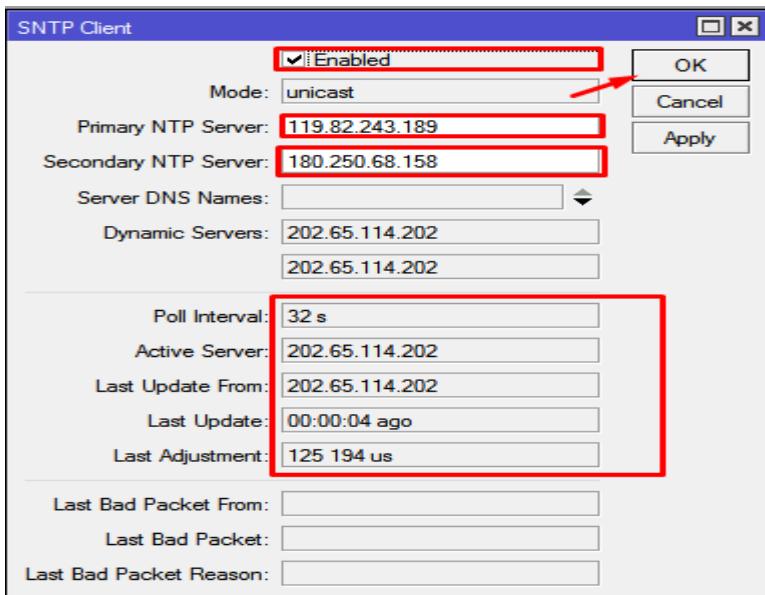
Oke selanjutnya saya akan menejelaskan bagaimana cara nya agar Router dan Client bisa men-Sinkronisasi dgn waktu yang ada di internet..

- Klik System > SNTP Client
- Ceklis Enable
- Isi Primary NTP Server=id.pool.ntp.org ,dan Isi Secondary NTP Server=ntp.nasa.gov
- Lalu Klik Apply



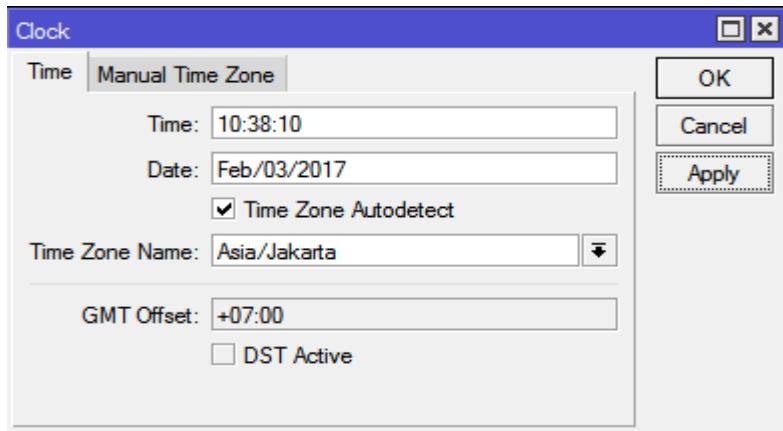
Jika Kita telah klik Apply maka Primary NTP Server dan Secondary NTP Server akan berubah Menjadi IP address

- Lalu Klik OK



Jika sudah selesai kita bisa mengecheck Waktu Kita Sinkron dengan internet atau tidak..

- Klik System > Clock



Biasanya Jika Router kita telah terhubung Internet Router akan Men-Sinkronosasi Otomatis/Kita tidak perlu men-Setting Manual lagi,Tetapi kita juga perlu tau Cara Manual..

Bab 2. Wireless

> About Wireless <

Wireless adalah teknologi tanpa kabel, dalam hal ini adalah melakukan telekomunikasi dengan menggunakan gelombang elektromagnetik sebagai media perantara pengganti kabel. Sekarang ini teknologi wireless berkembang sangat pesat sekali, secara kasat mata dapat kita lihat dengan semakin banyaknya penggunaan telepon seluler, disamping itu berkembang juga teknologi wireless yang digunakan untuk akses internet.

Sejarah Wireless

Pada akhir 1970-an IBM mengeluarkan hasil percobaan mereka dalam merancang WLAN dengan teknologi IR, perusahaan lain seperti Hewlett-Packard (HP) menguji WLAN dengan RF. Kedua perusahaan tersebut hanya mencapai data rate 100 Kbps. Karena tidak memenuhi standar IEEE 802 untuk LAN yaitu 1 Mbps maka produknya tidak dipasarkan. Baru pada tahun 1985, (FCC) menetapkan pita Industrial, Scientific and Medical (ISM band) yaitu 902-928 MHz, 2400-2483.5 MHz dan 5725-5850 MHz yang bersifat tidak terlisensi, sehingga pengembangan WLAN secara komersial memasuki tahapan serius. Barulah pada tahun 1990 WLAN dapat dipasarkan dengan produk yang menggunakan teknik spread spectrum (SS) pada pita ISM, frekuensi terlisensi 18-19 GHz dan teknologi IR dengan data rate >1 Mbps.

Pada tahun 1997, sebuah lembaga independen bernama IEEE membuat spesifikasi/standar WLAN pertama yang diberi kode 802.11. Peralatan yang sesuai standar 802.11 dapat bekerja pada frekuensi 2,4GHz, dan kecepatan transfer data (throughput) teoritis maksimal 2Mbps.

Pada bulan Juli 1999, IEEE kembali mengeluarkan spesifikasi baru bernama 802.11b. Kecepatan transfer data teoritis maksimal yang dapat dicapai adalah 11 Mbps. Kecepatan transfer data sebesar ini sebanding dengan Ethernet tradisional (IEEE 802.3 10Mbps atau 10Base-T). Peralatan yang menggunakan standar 802.11b juga bekerja pada frekuensi 2,4Ghz. Salah satu kekurangan peralatan wireless yang bekerja pada frekuensi ini adalah kemungkinan terjadinya interferensi dengan cordless phone, microwave oven, atau peralatan lain yang menggunakan gelombang radio pada frekuensi sama.

Pada saat hampir bersamaan, IEEE membuat spesifikasi 802.11a yang menggunakan teknik berbeda. Frekuensi yang digunakan 5Ghz, dan mendukung kecepatan transfer data teoritis maksimal sampai 54Mbps. Gelombang radio yang dipancarkan oleh peralatan 802.11a relatif sukar menembus dinding atau penghalang lainnya. Jarak jangkau gelombang radio relatif lebih pendek dibandingkan 802.11b. Secara teknis, 802.11b tidak kompatibel dengan 802.11a. Namun saat ini cukup banyak pabrik hardware yang membuat peralatan yang mendukung kedua standar tersebut.

Pada tahun 2002, IEEE membuat spesifikasi baru yang dapat menggabungkan kelebihan 802.11b dan 802.11a. Spesifikasi yang diberi kode 802.11g ini bekerja pada frekuensi 2,4Ghz dengan kecepatan transfer data teoritis maksimal 54Mbps. Peralatan 802.11g kompatibel dengan 802.11b, sehingga dapat saling dipertukarkan. Misalkan saja sebuah komputer yang menggunakan kartu jaringan 802.11g dapat memanfaatkan access point 802.11b, dan sebaliknya.

Pada tahun 2006, 802.11n dikembangkan dengan menggabungkan teknologi 802.11b, 802.11g. Teknologi yang diusung dikenal dengan istilah MIMO (Multiple Input Multiple Output) merupakan teknologi Wi-Fi terbaru. MIMO dibuat berdasarkan spesifikasi Pre-802.11n. Kata "Pre-" menyatakan "Prestandard versions of 802.11n". MIMO menawarkan peningkatan throughput, keunggulan reabilitas, dan peningkatan jumlah klien yg terkoneksi. Daya tembus MIMO terhadap penghalang lebih baik, selain itu jangkauannya lebih luas sehingga Anda dapat menempatkan laptop atau klien Wi-Fi sesuka hati. Access Point MIMO dapat menjangkau berbagai perlatalan Wi-Fi yg ada disetiap sudut ruangan. Secara teknis MIMO lebih unggul dibandingkan saudara tuanya 802.11a/b/g. Access Point MIMO dapat mengenali gelombang radio yang dipancarkan oleh adapter Wi-Fi 802.11a/b/g. MIMO mendukung kompatibilitas mundur dengan 802.11 a/b/g. Peralatan Wi-Fi MIMO dapat menghasilkan kecepatan transfer data sebesar 108Mbps.

Itu sedikit Penjelasan Tentang Wireless dan Sejarahnya..

Sebelum kita masuk ke Lab-Lab tentang Wireles Kita perlu sedikit mengetahui Tentang Fitur Fitur yang ada di menu Wireless...

❖ Mode Wireless

Mode wireless digunakan untuk menentukan interface wireless akan kita jadikan apa.. bisa jadi station, access point dan lain lain...

Sedikit penjelasan tentang Mode wireless dan fungsinya

- Mode Alignment Only

Mode Alignment only, biasa digunakan untuk membantu pada saat pointing dengan indikator beeper pada RouterBoard, sebagai contoh kita bisa menambahkan script dimana ketika mendapatkan sinyal bagus maka beeper akan berbunyi..

- Mode AP-Bridge

Mode AP-bridge digunakan sebagai Access point atau pemancar sinyal yang bisa melayani banyak client atau disebut juga dengan PTMP (Point To Multi Point), mode ini bisa kita gunakan untuk network yang sifatnya Routing ataupun Bridging. Untuk menggunakan mode AP-Bridge ini perangkat Routerboard minimal harus memiliki lisensi level 4

- Mode Bridge

Mode bridge digunakan sebagai Access point atau pemancar akan tetapi hanya bisa melayani satu client atau disebut juga dengan PTP (Point To Point), mode ini juga bisa kita gunakan untuk network yang sifatnya Routing ataupun Bridging. Untuk menggunakan mode ini perangkat Routerboard minimal memiliki lisensi level 3..

- Mode Nstreme dual slave

Pada dasarnya mekanisme kerja pada interface wireless adalah half duplex, akan tetapi dengan menggunakan mode ini kita dapat mengaktifkan mekanisme kerja full duplex, mode ini merupakan proprietary didalam wireless mikrotik, tentunya kita juga membutuhkan 2 wireless card dan 2 antenna pada masing-masing wireless router mikrotik

- Mode Station

Wireless dengan Mode station ini digunakan sebagai wireless client/ penerima pada topologi PTP (Point To Point) atau PTMP (Point To Multi Point), wireless Mode

station hanya bisa digunakan untuk membentuk network yang sifatnya routing, sehingga mode ini merupakan salah satu mode yang efektif dan efisian jika pada sisi wireless client/station tidak dibutuhkan bridging

- Mode Station-Bridge

Mode Station-Bridge merupakan mode pada interface wireless yang berfungsi sebagai penerima / client dan support untuk bridge network, perlu di ketahui bahwa untuk mode ini hanya bisa digunakan apabila perangkat AP dan stationnya sama sama Mikrotik..

- Mode Station-Pseudobridge

Mode Station-Pseudobridge merupakan pengembangan dari Mode Station standar, sama-sama menjadikan wireless sebagai penerima/client, perbedaannya adalah pada Mode Station-Pseudobridge support untuk membuat network yang sifatnya Bridge Network, Di dalam penggunaan mode ini terdapat konsekuensi dimana untuk bridging pada L2 tidak bisa dilakukan secara penuh, dalam artian mac-address sebuah perangkat yang berada di bawah perangkat wireless (PC end user) tidak terbaca pada sisi Access Point.

- Mode Station-Pseudobridge-Clone

Mode Station-Pseudobridge-Clone hampir sama dengan Mode Station-Pseudobridge yang membedakan adalah didalam mode ini bisa melakukan cloning mac-address, umumnya pada sebuah link wireless, yang terbaca pada sisi Access point adalah mac-address dari interface wireless client, tetapi jika menggunakan Mode Station-Pseudobridge-Clone yang terbaca adalah mac-address dari perangkat yang terhubung ke station (end user), Secara default yang terbaca adalah mac-address pada frame header yang pertama di teruskan, atau bisa ditentukan pada "station-bridge-clone-mac"

- Mode Station-WDS

Mode Station-WDS berfungsi sebagai penerima/client dari sebuah Access Point yang mengaktifkan protocol WDS,jika Di router Station Sudah di aktifkan mode WDS maka Router akan berfungsi Sebagai Reapeter, Kekurangan protokol WDS adalah penurunan throughput wireless hingga 50%, perlu diketahui bahwa antara vendor yang satu dengan vendor yang lain fungsi WDS belum tentu compatible, begitu juga dengan WDS pada mikrotik.

- Mode WDS-Slave

Mode WDS-Slave ini berfungsi sebagai pemancar (Access Point) sekaligus sebagai penerima (Station) atau disebut juga dengan repeater, Mode ini merupakan salah satu solusi apabila ingin membangun sebuah repeater tetapi perangkat yang dimiliki hanya menggunakan 1 card wireless card.

❖ Band Wireless

Selanjutnya yang perlu kita perhatikan kita men-setting Wireless adalah Band Wirelessnya

Menentukan Band Wireless merupakan cara untuk menentukan standart protokol yang akan digunakan oleh wireless interface kita. Selain menentukan standart protokol, band juga menentukan data rates yang bisa dilewatkan, channel frequencies dan lebar channel nya,

Mikrotik memiliki banyak Band yang dapat digunakan Interface Wireless...Band yang support di Indonesia hanya Band Yang yang berkerja di di Frekuensi 2,4Ghz jadi tidak sembarang band bisa kita gunakan,karna band yang bekerja di 5Ghz masih sedikit yang menggunakannya/atau band tersebut tidak dapat kita gunakan di Negri Indonesia ini ☺ Selanjutnya saya akan menjelaskan Jenis-jenis Band Beserta Keterangannya..

- 2Ghz-b, bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b dengan data rate maksimum 11 Mbit/s.
- 2Ghz-b/g, juga bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b dan 802.11g. protokol 802.11g hampir sama seperti 802.11b akan tetapi melakukan transmisi dengan basis OFDM seperti 802.11a sehingga protokol 802.11g bisa mencapai 54 Mbit/s.

- 2.4ghz-g-turbo - IEEE 802.11g menggunakan double channel yang kecepatan teoritisnya adalah hingga 108 Mbit
- 2ghz-10mhz - variasi dari IEEE 802.11g dengan menggunakan setengah dari lebar band standard (air rate of up to 27Mbit)
- 2ghz-5mhz - variasi dari IEEE 802.11g dengan menggunakan seperempat dari lebar band standard (air rate of up to 13.5Mbit)
- 2Ghz-b/g/n, bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b, 802.11g dan 802.11n. Pengembangan dari standart protokol 802.11, ditambah dengan kemampuan multiple-input multiple-output (MIMO). Dengan tambahan fitur MIMO ini, secara teori maksimal data rate yang bisa dicapai adalah 300 Mbit/s.
- 2Ghz-only G, bekerja di frekuensi 2,4Ghz, hanya menggunakan protokol 802.11g.
- 2Ghz-only N, bekerja di frekuensi 2,4Ghz, hanya menggunakan protokol 802.11n.
- 5ghz - menggunakan standard IEEE 802.11a 54Mbit
- 5ghz-turbo - IEEE 802.11a menggunakan double channel yang kecepatan teoritisnya adalah hingga 108 Mbit.
- 5Ghz-a, bekerja di frekuensi 5 Ghz. Menggunakan protokol 802.11a, maximum data rate yang bisa dicapai adalah 54 Mbit/s.
- 5Ghz-a/n, bekerja di frekuensi 5 Ghz. Menggunakan protokol 802.11a dan 802.11n.
- 5Ghz-only N, bekerja di frekuensi 5 Ghz dan hanya menggunakan protokol 802.11n.
- 5ghz-10mhz - variasi dari IEEE 802.11a dengan menggunakan setengah dari lebar band standard (air rate of up to 27Mbit)
- 5ghz-5mhz - variasi dari IEEE 802.11a dengan menggunakan seperempat dari lebar band standard (air rate of up to 13.5Mbit)

#Catatan:

1. Turbo channel hanya support di card non-N dan hanya ada di ROS versi 2.xx, 3.xx dan 4.xx.
2. Penggunaan Band 5GHz ini harus seizin dept. kominfo, jadi kita kita boleh asal pakai Band 5Ghz

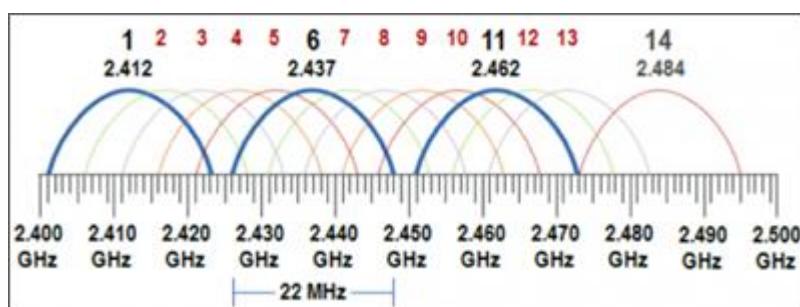
Jika kita telah Membaca Sedikit penjelasan tentang band Wireless, ada beberapa pilihan band yang menggunakan lebih dari satu protokol. Maka Jika kita Men-Setting sebuah interface wireless dengan band yang menggunakan lebih dari satu protokol, maka interface wireless tersebut memberikan pilihan beberapa Protocol kepada client, maka Client akan memilih Protocol mana yang support dengan Perangkat Client tersebut.....

❖ Frekuensi

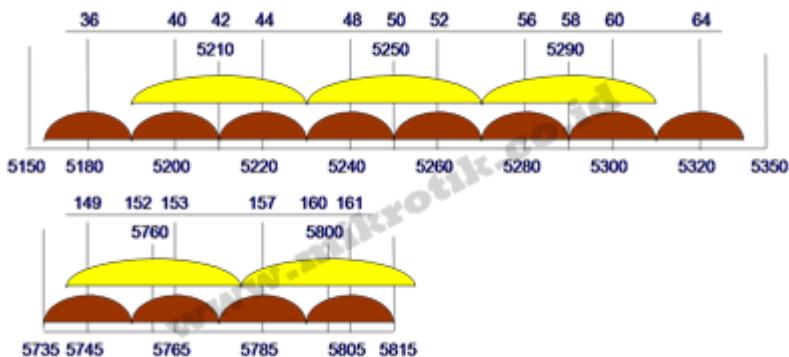
Interface Wireless menggunakan Radio Frekuensi yang berfungsi sebagai Media Rambat Wireless tersebut, yang perlu kita perhatikan adalah jenis Frekuensi yang kita gunakan harus bersih atau tidak ada gangguan. Gangguan Wireless bisa berupa halangan seperti Pohon, Gunung, Gedung, Tembok, Kaca atau karna ada perangkat Wireless yang lain yang menggunakan Frekuensi yang sama dengan Interface Wireless kita.. itu adalah beberapa masalah yang dapat mengganggu Media Rambat Interface Wireless

Agar kita bisa membentuk link wireless yang Baik kita perlu menghindari gangguan tersebut. hal pertama yang harus dilakukan dilakukan adalah site survey terlebih dahulu untuk mengetahui kondisi lapangan secara fisik maupun penggunaan frekuensi yang sudah ada. Misalnya, adanya halangan berupa bukit, gedung, pohon, tembok, kaca dsb yang harus dihindari. Kita harus mengetahui juga frekuensi - frekuensi yang ada disekitar. jadi nantinya bisa dihindari penggunaanya agar tidak interferensi/overlapping.

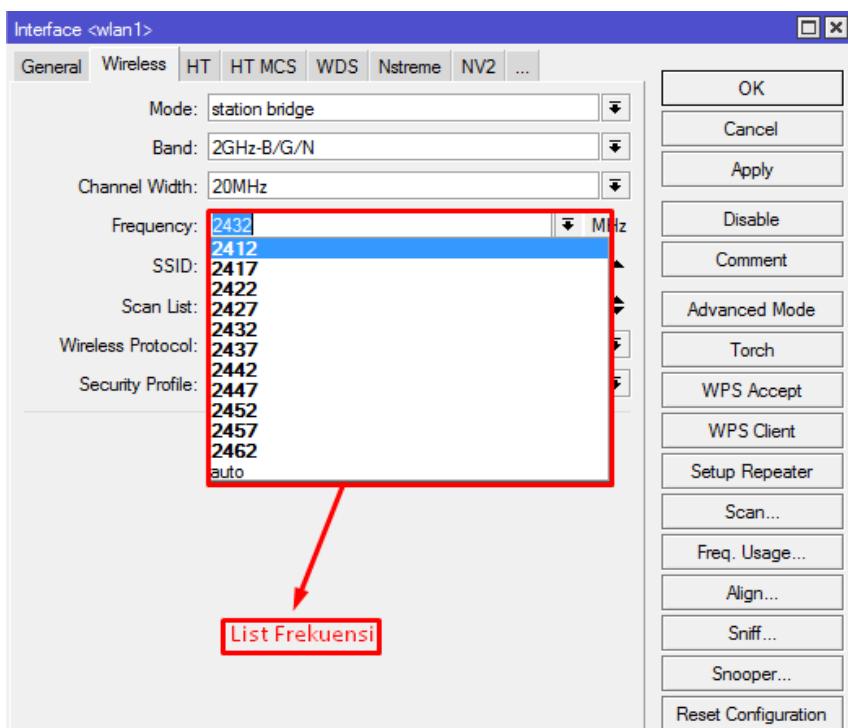
Alokasi frekuensi sudah diatur dalam regulasi di setiap wilayah dan negara. Di Indonesia, untuk keperluan wireless LAN sudah dalokasikan dalam ISM Band pada frekuensi 2,4GHz dan 5,8GHz. Lebih detail nya, untuk 2,4GHz dibagi dalam beberapa channel dengan lebar channel masing - masing 22MHz.



Begitu juga dengan yang 5GHz. Frekuensi 5Ghz juga dibagi menjadi beberapa channel.



Di mikrotik, tiap channel ditampilkan dengan nilai tengah frekuensi-nya. Misal pada band 2,4GHz, channel1 di wakili dengan angka=2412 ,dan seterusnya...



Kembali ke masalah Radio Frekuensi ,MikroTik menyediakan beberapa Tools yang bisa kita gunakan untuk scanning Frekuensi yang kosong/tidak ada halangan apapun yang berfungsi untuk memaksimalkan kinerja Wireless tersebut..

❖ SSID

SSID (Service Set Identifier) merupakan identifikasi atau nama untuk jaringan Wireless. Setiap peralatan Wi-Fi harus menggunakan SSID (Service Set Identifier) tertentu. Peralatan Wi-Fi dianggap satu jaringan jika menggunakan SSID (Service Set Identifier) yang sama. Agar dapat berkomunikasi, setiap peralatan Wireless haruslah menggunakan SSID (Service Set Identifier) bersifat case-sensitive, penulisan huruf besar dan huruf kecil akan sangat berpengaruh

- Hide-SSID (default value: no) :

yes - jika diaktifkan maka AP tidak akan memasukkan informasi SSID pada beacon frame dan tidak akan memberikan frame balasan berisi informasi SSID jika ada permintaan informasi SSID.

no - AP akan memasukkan informasi SSID pada frame beacon dan akan memberikan informasi SSID jika ada permintaan informasi SSID.

Setting ini hanya berpengaruh jika menggunakan mode AP, sebenarnya tidak berpengaruh banyak pada security karena informasi SSID tetap dimasukkan pada frame yang lain (bukan beacon frame).

❖ Scan List

Scan List adalah nilai default adalah channel ISM (standard channel) sesuai dengan band yang digunakan, Scan list bisa berupa range, list dari channel yang dipisahkan dengan tanda comma atau bisa juga gabungan dari keduanya.

❖ Parameter Tx Rate

- default-ap-tx-limit (integer; default: 0) - adalah limit traffic rate untuk pengiriman data dari AP ke tiap client (bps). , 0 - berarti tanpa limit
- default-client-tx-limit (integer; default: 0) - adalah limit traffic rate untuk pengiriman data dari tiap client ke AP (bps). Hanya bekerja jika client sama-sama menggunakan mikrotik., 0 - berarti tanpa limit

❖ Parameter Checklist

- Default-Authentication (default value: yes) :

Jika digunakan mode AP maka semua client yang tidak dibatasi di access-list akan diautentikasi dan bisa terkoneksi.

Jika digunakan di mode station maka wireless bisa terkoneksi ke AP manapun yang tidak dibatasi di connect-list.

- Default-Forwarding (default value: yes) :

Adalah parameter yang digunakan untuk forwarding traffic dari client ke client yang lain dalam AP yang sama. Bisa dibatasi lebih spesifik per clientnya di access-list.

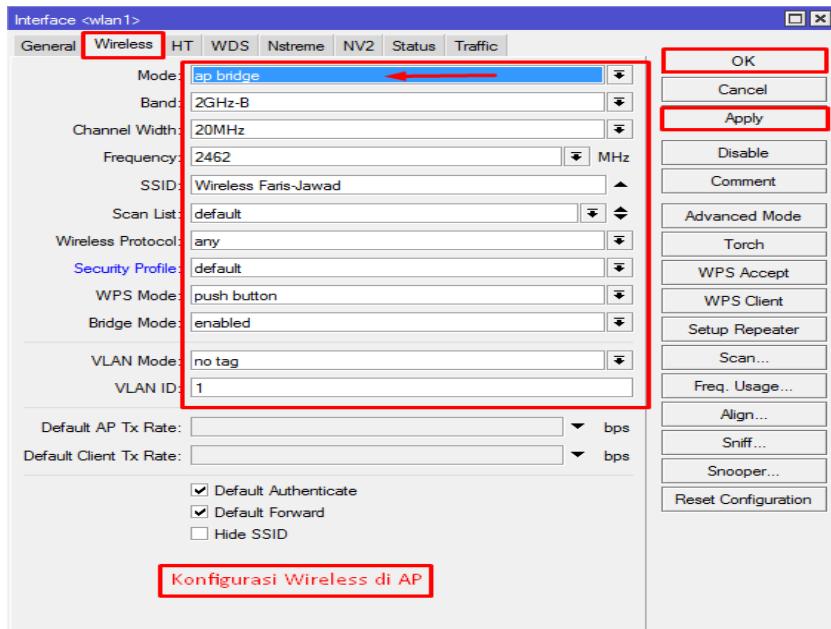
Lab 13. Menghubungkan Router dengan Wireless



Oke di lab ini kita akan memulai Lab tentang Wireless...di lab ini kita akan mencoba menghubungkan dua RouterBoard dengan menggunakan Wireless, sebenarnya Konsep nya sama dengan cara mengkoneksikan Router ke Internet tapi beda nya adalah si Access Point juga menggunakan perangkat MikroTik juga...oke langsung saja kita coba... jangan lupa Tiap router di beri router identity sesuai kegunaannya ..

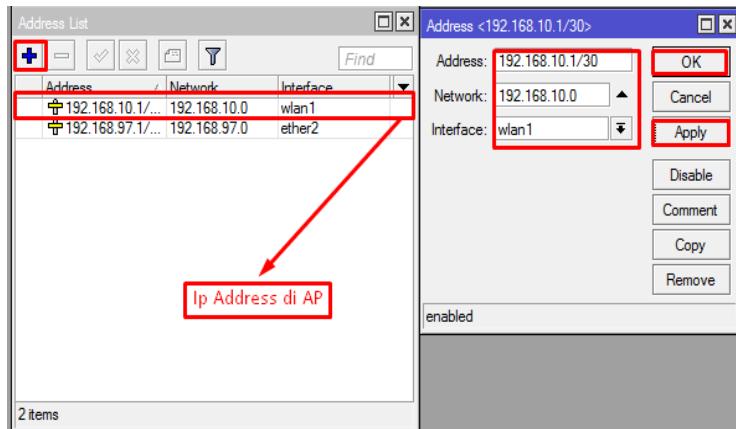
Pertama Kita harus Men-Setting Router yang kita fungsikan sebagai Access Point..

- Klik Menu Wireless > Masuk Ke Interface Wireless
- Masuk ke Tab Wireless
- Pilih Mode=Ap Bridge , Band=(terserah)2GHz-B , Channel Width=20MHz , Frekuensi=2462 SSID=(terserah)Wireless Faris-Jawad , Security Profile=di isi jika Access Point ingin di beri Security Wireless..



Selanjutnya Kita perlu Men-Setting Ip Address untuk Wireless yang berfungsi Sebagai alamat bagi Access Point/Gateway bagi Client...

- Klik Menu IP > Address > Add (+)
- Isi Address=(terserah)192.168.10.1/30 ,Interface=Wlan1
- Lalu Apply dan OK

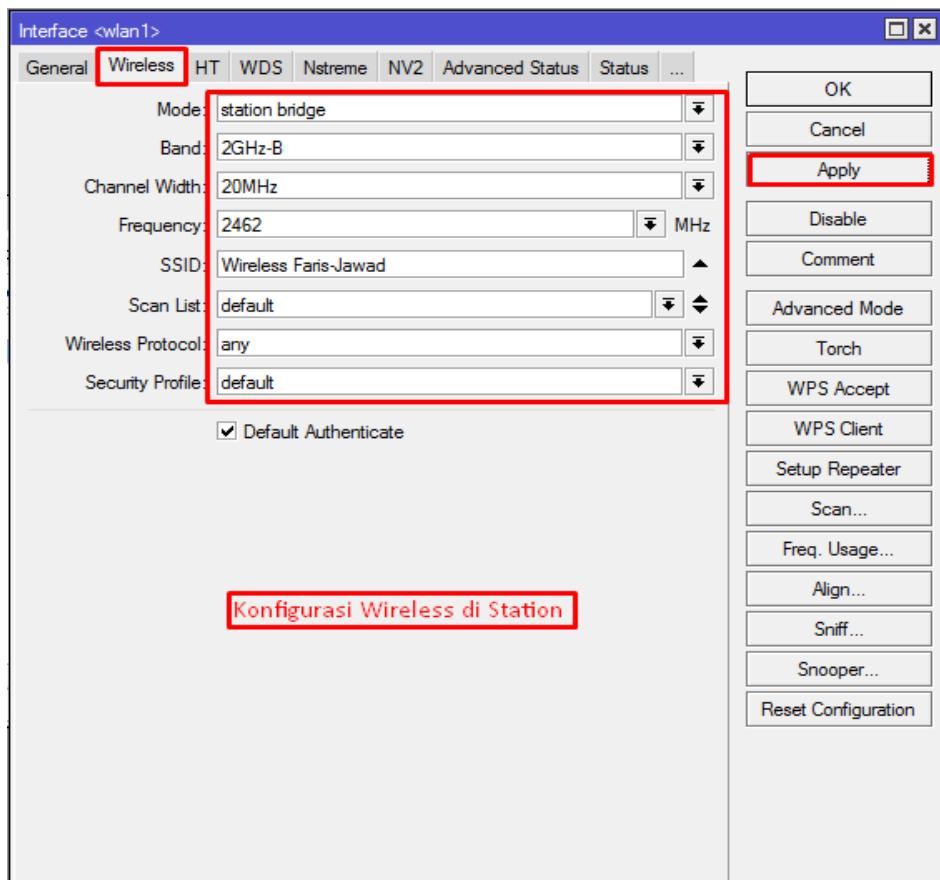


Di sini saya menggunakan /30 karna saya hanya ingin 1 Access Point dan 1 Wireless Client yang bisa menggunakan Network tersebut (Point To Point),di sini saya Tidak men-Setting DHCP server yang berfungsi agar membagikan Ip adrees secara Otomatis ke Client...

Selanjutnya kita perlu men-Setting Interface Wireless yang digunakan Station...

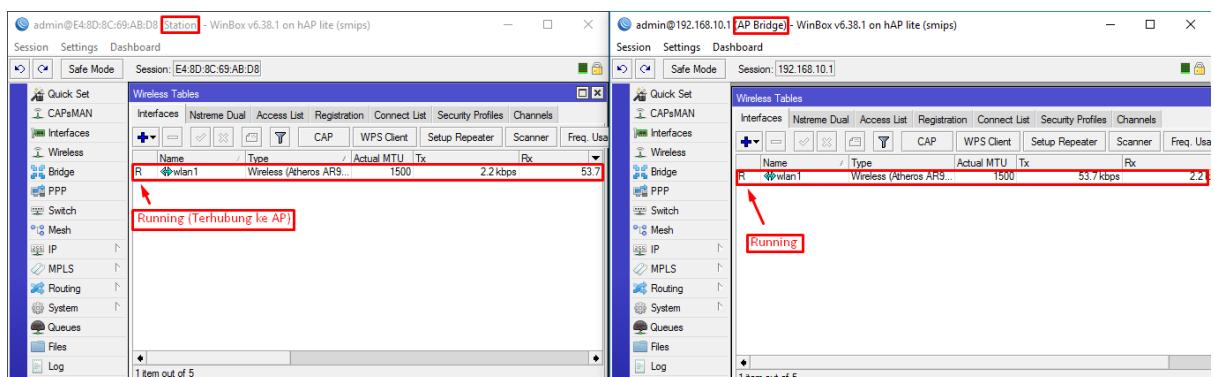
- Klik Menu Wireless > Masuk Ke Interface Wireless
- Masuk ke Tab Wireless
- Pilih Mode=Station Bridge ,Band=2GHz-B ,Channel Width=20MHz ,Frekuensi=2462 SSID=Wireless Faris-Jawad ,Security Profile=di isi jika Access Point di Password

Band,Channel dan Frekuensi Mengikuti Access Point... saat mencari access point kita bisa gunakan Tools Scan / kita bisa langsung isikan nama SSID Access Point...,Jika Access Point dan Station sama sama Mikrotik maka mode yang di pakai Oleh Station adalah Station Bridge...dan jika Access Point bukan MikroTik maka mode yang di pakai Station adalah Station..... Intinya Mode Station Bridge hanya bisa di pakai ketika Kedua perangkat Wireless sama sama MikroTik...



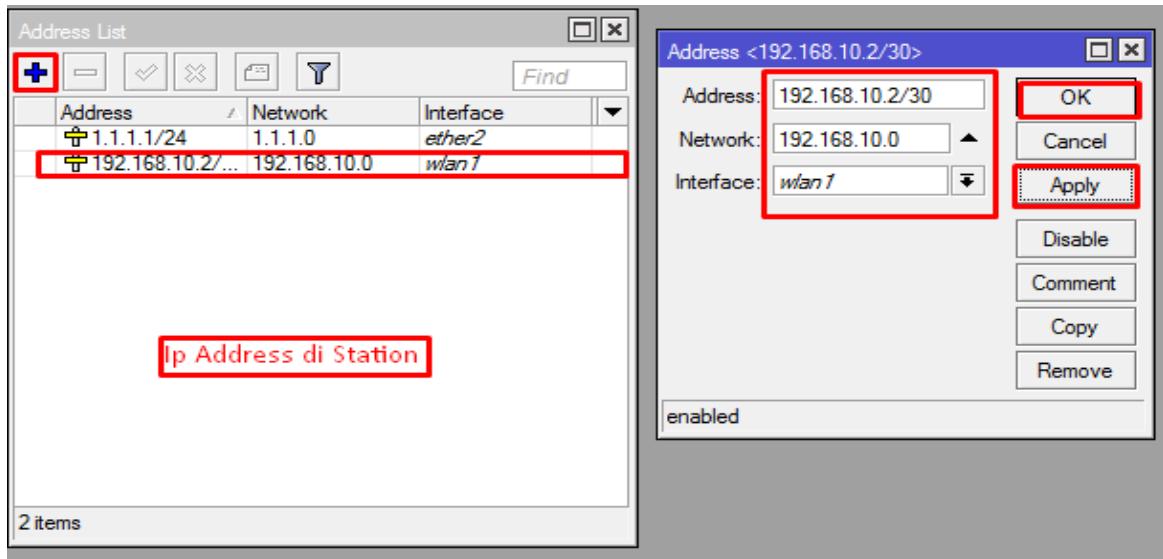
Step Selanjutnya kita akan meng-Konfigurasikan IP address untuk Interface Wireless secara Static,saya men-Setting IP di Station secara Static karna Access Point tidak menggunakan Fitur DHCP Server,Jika AP menggunakan DHCP Server maka di station tidak Perlu Setting Ip secara Static,Tetapi Station hanya perlu menggunakan Fitur IP DHCP Client yang berfungsi meminta Ip dari DHCP Client...

Jika Sudah Selesai maka Status ke dua Interface Wireless adalah R (Running)

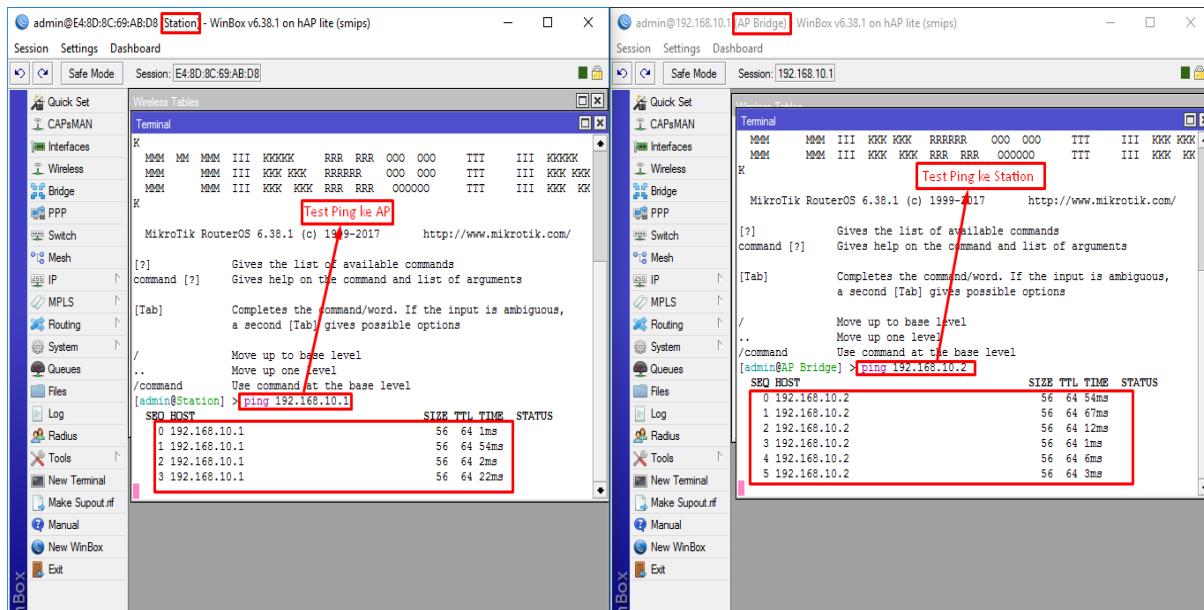


Oke kita lanjutkan Setting IP address di Station...

- Klik Menu IP > Address > Add (+)
- Isi Address=192.168.10.2/30 ,Interface=Wlan1
- Lalu Apply dan OK



Jika sudah Step ini, Step selanjutnya adalah Kita test Ping dari AP ke Station dan dari Station ke AP...

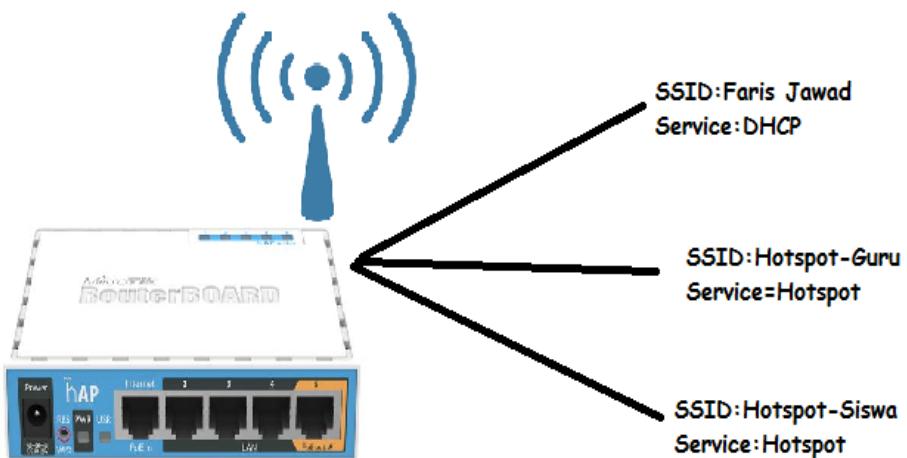


Lab 14. Virtual Access Point

Multiple SSID adalah salah satu fitur yang sering digunakan dalam distribusi akses jaringan melalui media nirkabel/wireless. Metode ini memungkinkan sebuah perangkat yang secara fisik hanya memiliki satu interface wireless dapat memancarkan lebih dari 1 SSID dengan service yang berbeda pula.

Fitur tersebut kerap diimplementasikan pada jaringan kantor, kampus, dsb yang berguna untuk memenuhi kebutuhan akses wireless yang berbeda jadi Kita bisa membuat Lebih dari 2 SSID dengan 1 Interface Wireless,Kita juga bisa men-Setting Service Per-SSID ,IP address dan Mac Address di setiap SSID.

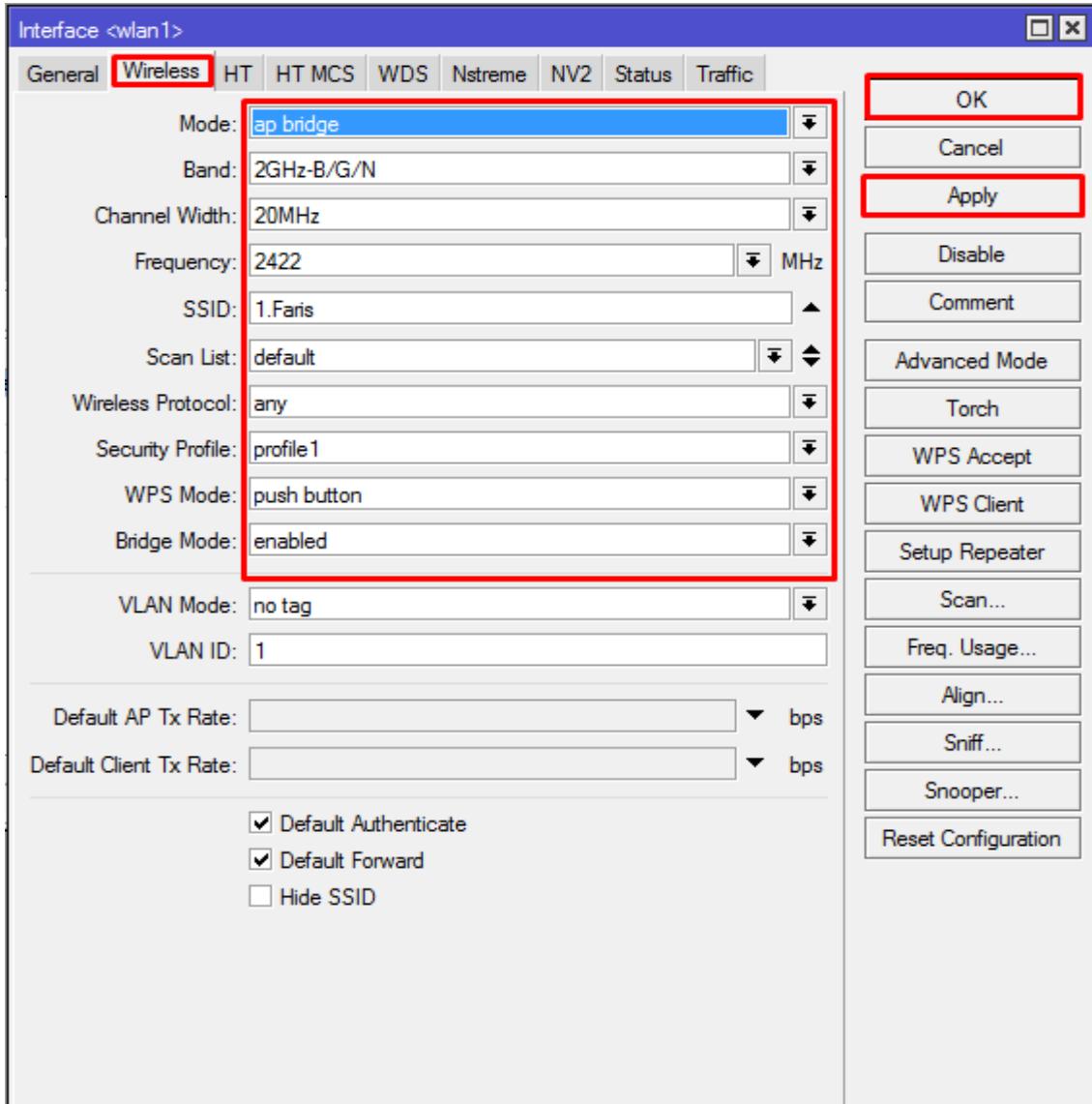
Gambarannya seperti ini..



Oke jika sudah mengerti konsep dari Virtual AP kita langsung Lab kan...

Pertama Kita Setting Interface Wireless Kita sebagai Access Point..

- Klik Wireless > Klik Interface Wireless
- Setting Interface Wireless sesuai Kebutuhan (Bebas)
- Mode: AP Bridge , Band: 2GHz-B/G/N , Channel: 20MHz , Frekuensi: 2422
SSID: 1.Faris (Bebas)

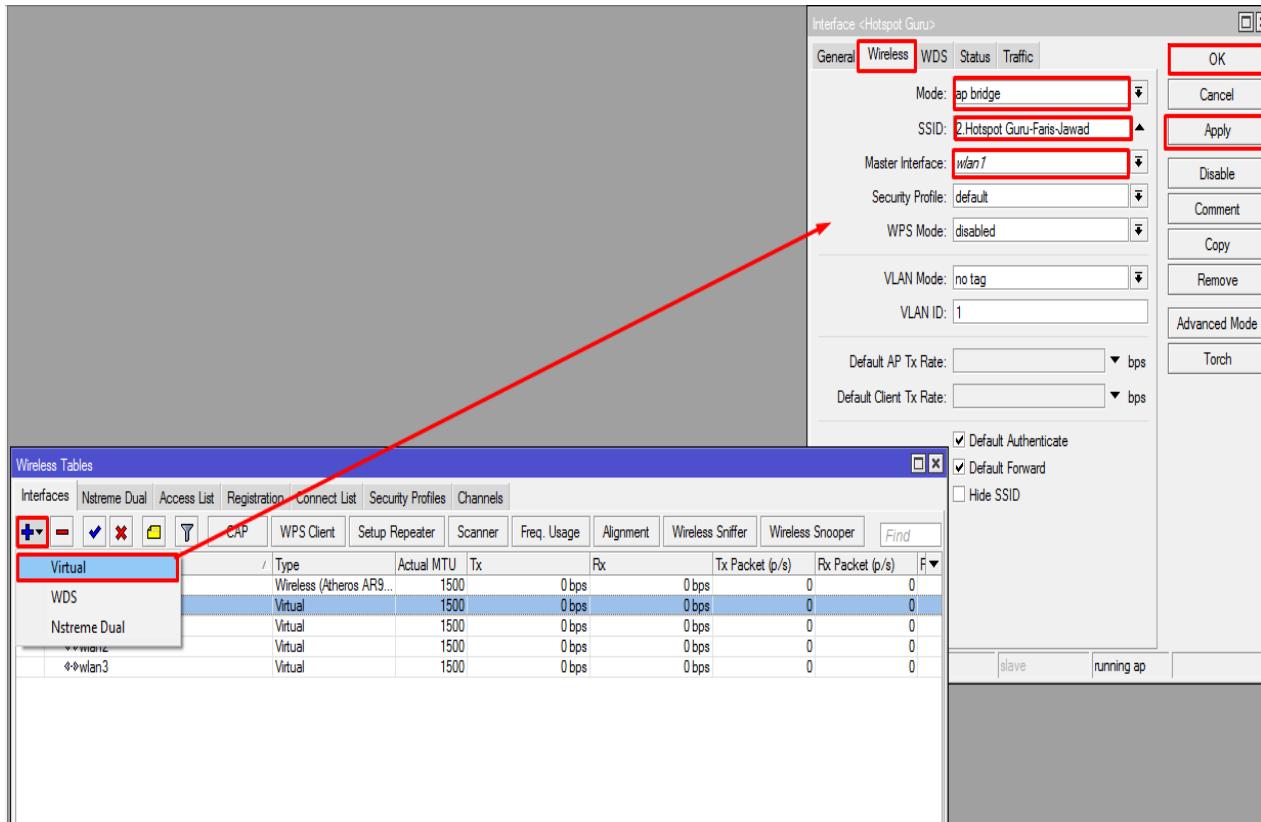


Step selanjutnya adalah Membuat Virtual Access Point ,pada Virtual Access Point Settingan Band,Channel,Frekuensi dll akan mengikuti Master Interface Wireless...

Oke saya akan Membuat 4 Virtual Access Point

Pertama saya akan Membuat Virtual Access Point yang berfungsi sebagai Hotspot dengan SSID:2.Hotspot Guru-Faris-Jawad

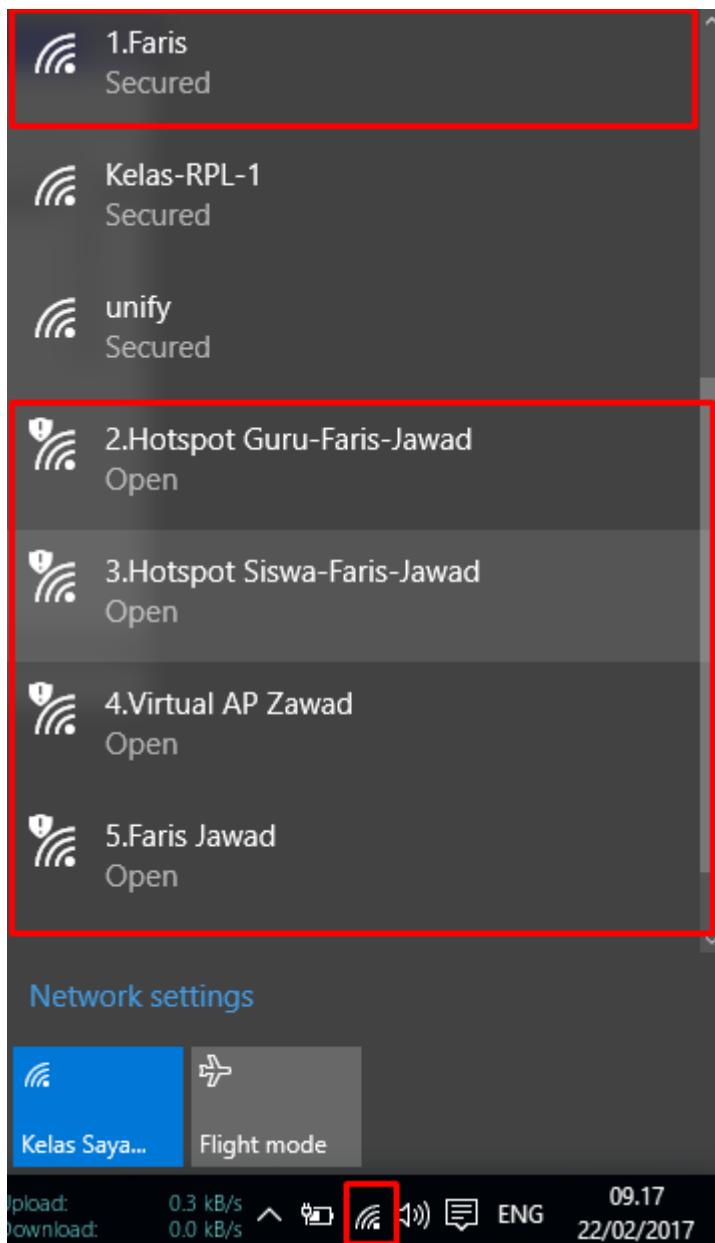
- Klik Menu Wireless > Interface > Add > Virtual
- Isi Mode:Ap Bridge , SSID:2.Hotspot Guru-Faris-Jawad ,Master Interface:Wlan1



Jika kita sudah bisa membuat 1 VAP maka kita bisa membuat VAP yang lebih banyak..

Catatan: Semakin Banyak Virtual AP yang kita buat akan semakin padat Trafic yang ada di Frekuensi Tersebut,karna Frekuensi VAP mengikuti Frekuensi Master Interface Wireless... jika sudah membuat VAP kita bisa membuat IP address yang berbeda setiap Virtual Access Point

Untuk Melihat Hasil Virtual Access Point Yang Telah kita buat kita bisa melihat menggunakan Wifi Adapter yang ada di laptop kita



Lab 15. Wireless Nstreme



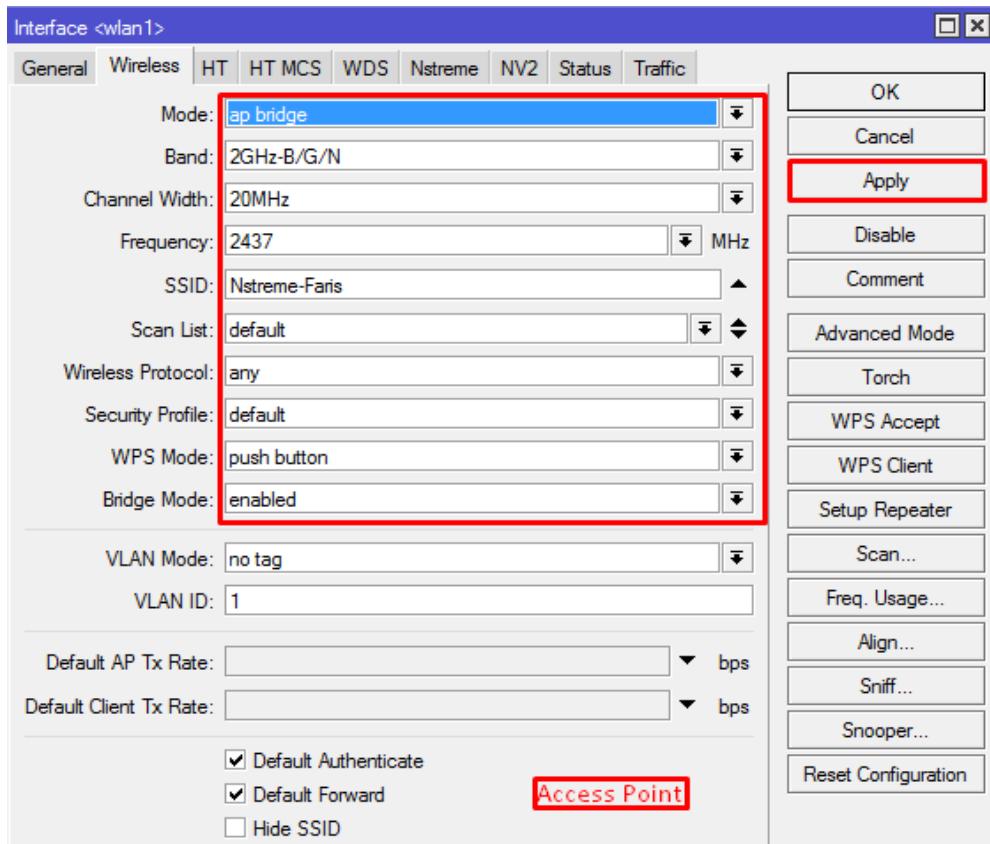
Nstreme adalah MikroTik proprietary, protokol nirkabel dibuat untuk mengatasi keterbatasan kecepatan dan jarak IEEE 802.11 standar dan untuk memperpanjang point-to-point dan point point-to-multi kinerja wireless link. Protokol Nstreme-dual baru yang dirancang untuk menyediakan komunikasi real full-duplex pada wireless dengan sepasang kartu nirkabel - satu untuk transmisi data dan satu untuk menerima. Bisa di bilang Nstreme berfungsi untuk memfokuskan Sinyal ke beberapa Device..

Oke langsung saja kita Mulai Lab nya...

Jangan Lupa beri Router Identity pada Yang menjadi Access Point dan Station

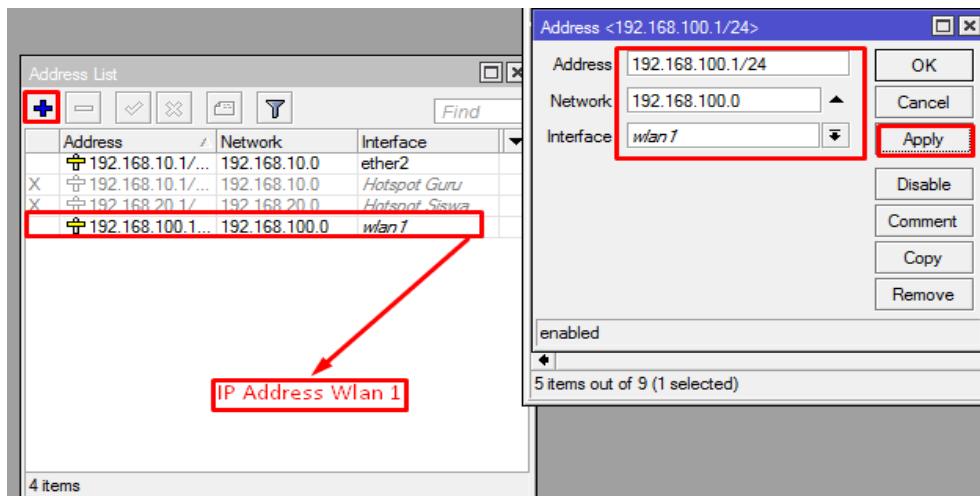
Pertama kita perlu Setting Wireless yang digunakan Sebagai Access Point..

- Klik Menu Wireless > Wireless
- Isi Mode=Ap Bridge , Band=(terserah)2GHz-B/G/N ,Channel=20MHz ,Frekuensi=(terserah)2473 ,SSID=(terserah)Nstreme-Faris
- Lalu Klik Apply dan OK



Step selanjutnya adalah Men-Setting IP Address untuk Interface Wlan..

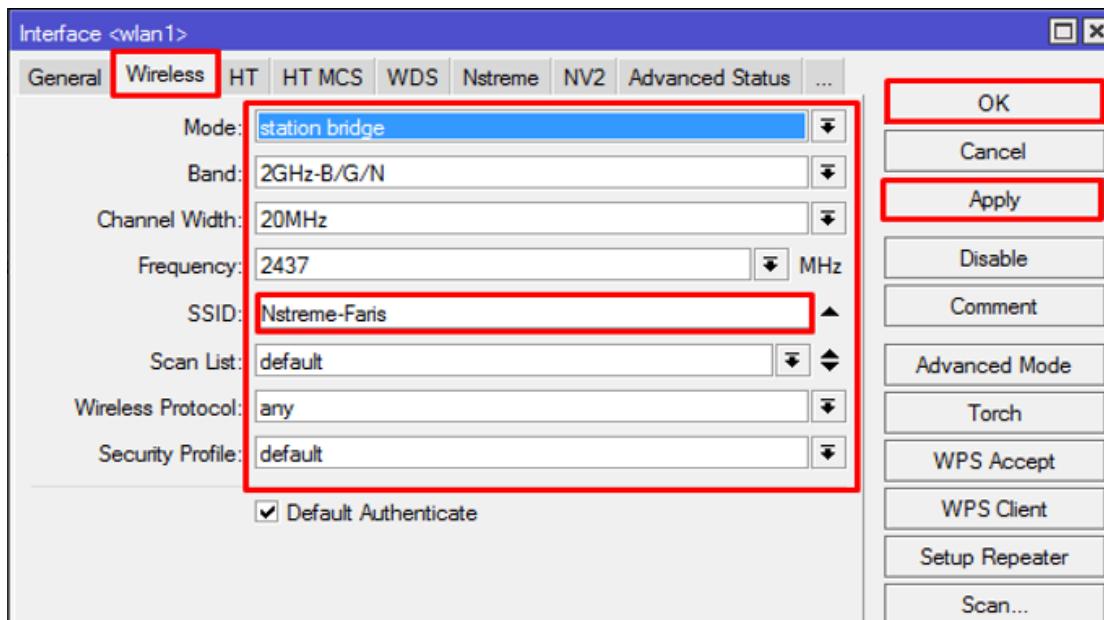
- Isikan IP Address=192.168.100.1/24 ,Interface=Wlan1
- Lalu Apply dan OK



Di sini saya Men-Setting IP Secara Static, Jika ingin Menggunakan DHCP Bisa saja, agar Si station lebih mudah mendapatkan IP Address...

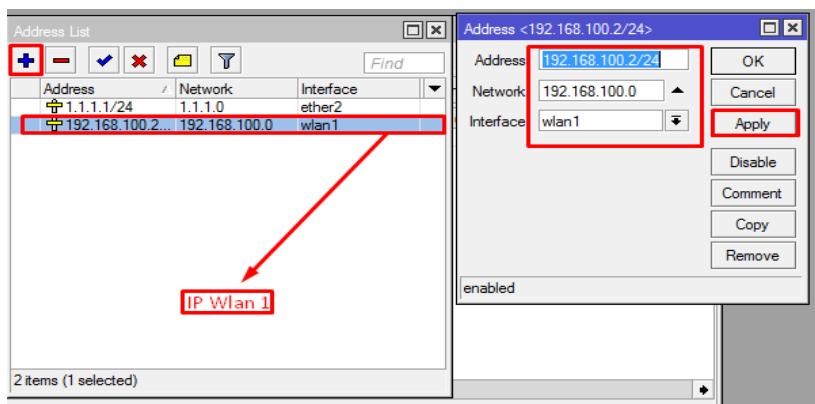
Step selanjutnya adalah kita setting Wireless yang ada pada station...

- Klik Menu Wireless > Wireless
- Isi Mode=Station Bridge , Band=2GHz-B/G/N ,Channel=20MHz ,Frekuensi=2473 ,SSID=Nstreme-Faris
- Lalu Klik Apply dan OK

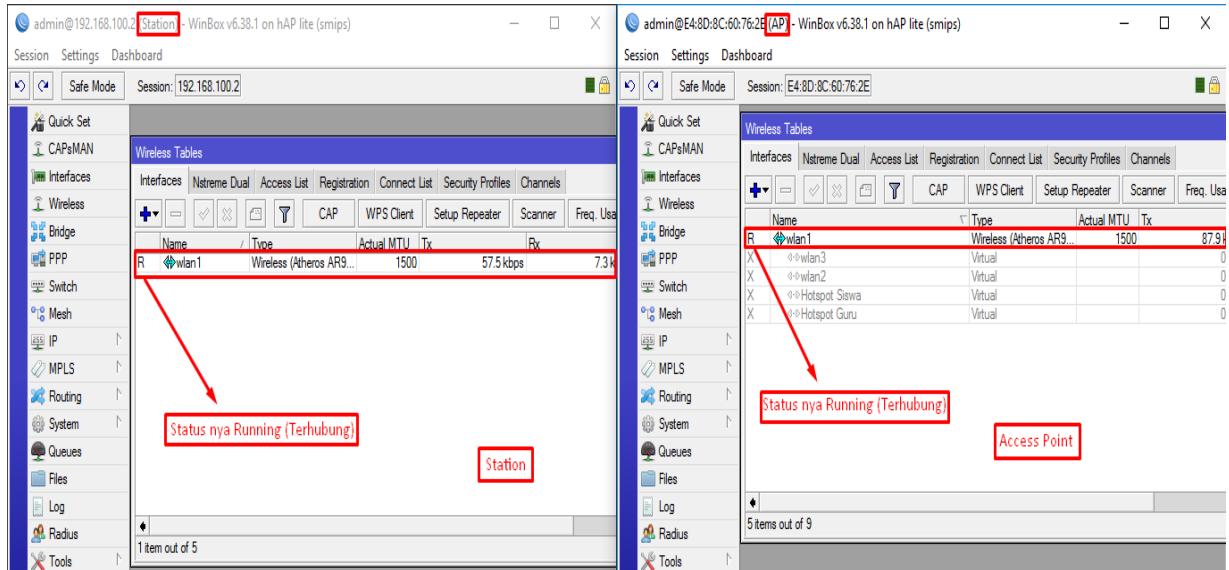


Selanjutnya kita perlu men-Setting Ip address di Station agar Access Point dan Station bisa terhubung,jika access point menggunakan Fitur DHCP Server maka Station hanya perlu membuat DHCP Client di Interface=Wlan 1,tapi di sini saya akan men-Setting Ip Address Secara Static....

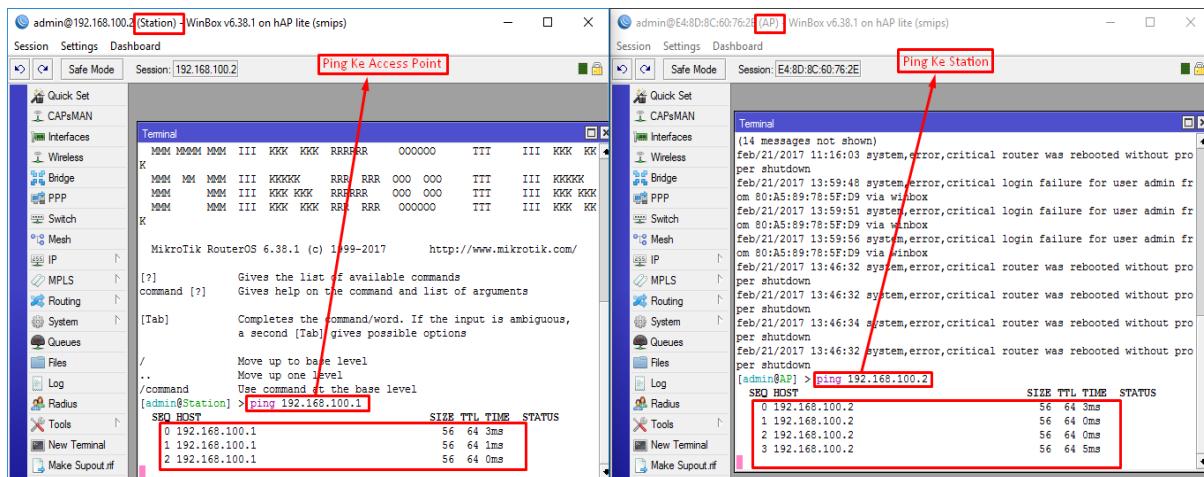
- Isikan IP Address=192.168.100.2/24 ,Interface=Wlan1
- Lalu Apply dan OK



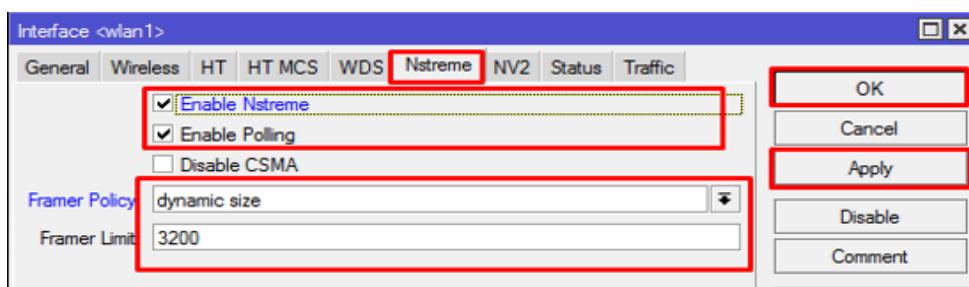
Jika kedua Router tersebut telah terhubung maka Status di kedua Interface Wireless tersebut adalah R (Running)..



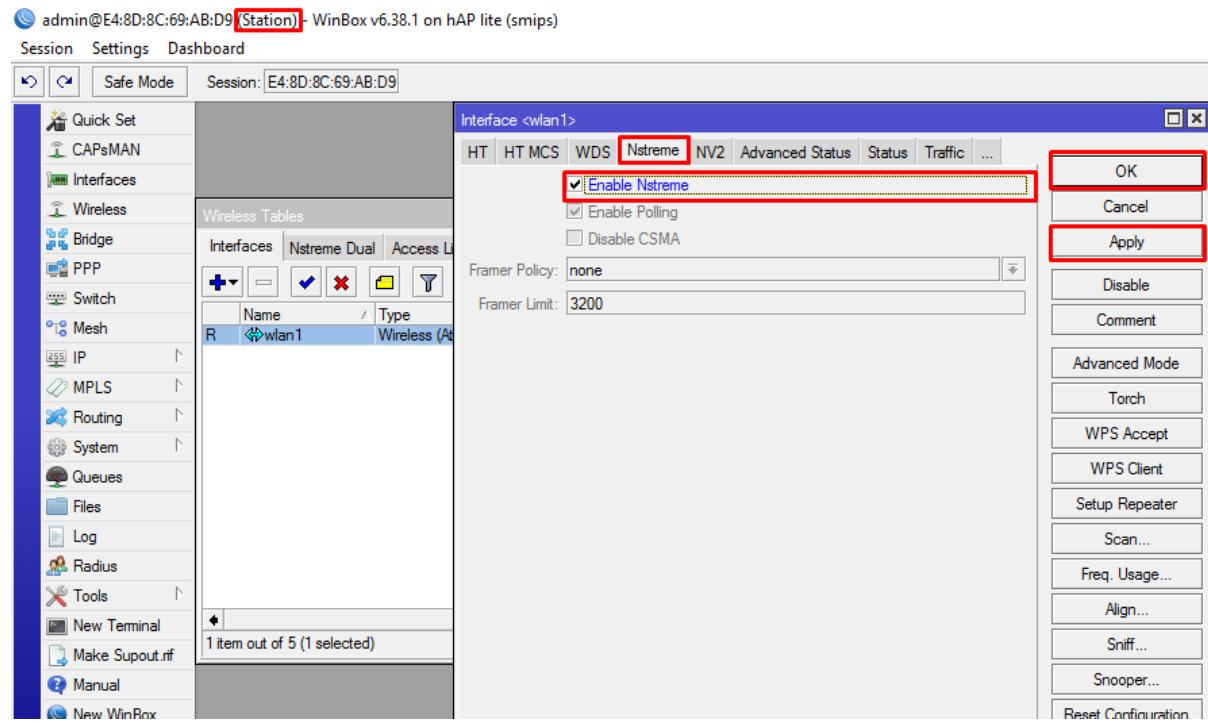
Dan Untuk Menguji Apakah sudah saling terhubung bisa,Kita ping dari Station ke Access Point dan Access Point ke Station...



Jika kedua Router telah terhubung,Selanjutnya adalah meng-Aktifkan Fitur Nstreme di kedua Router,Pertama Kita Setting Nstreme di Access Point...



Selanjutnya Kita setting Nstreme Juga di Router yang di gunakan sebagai Station.



Selesai.... 😊

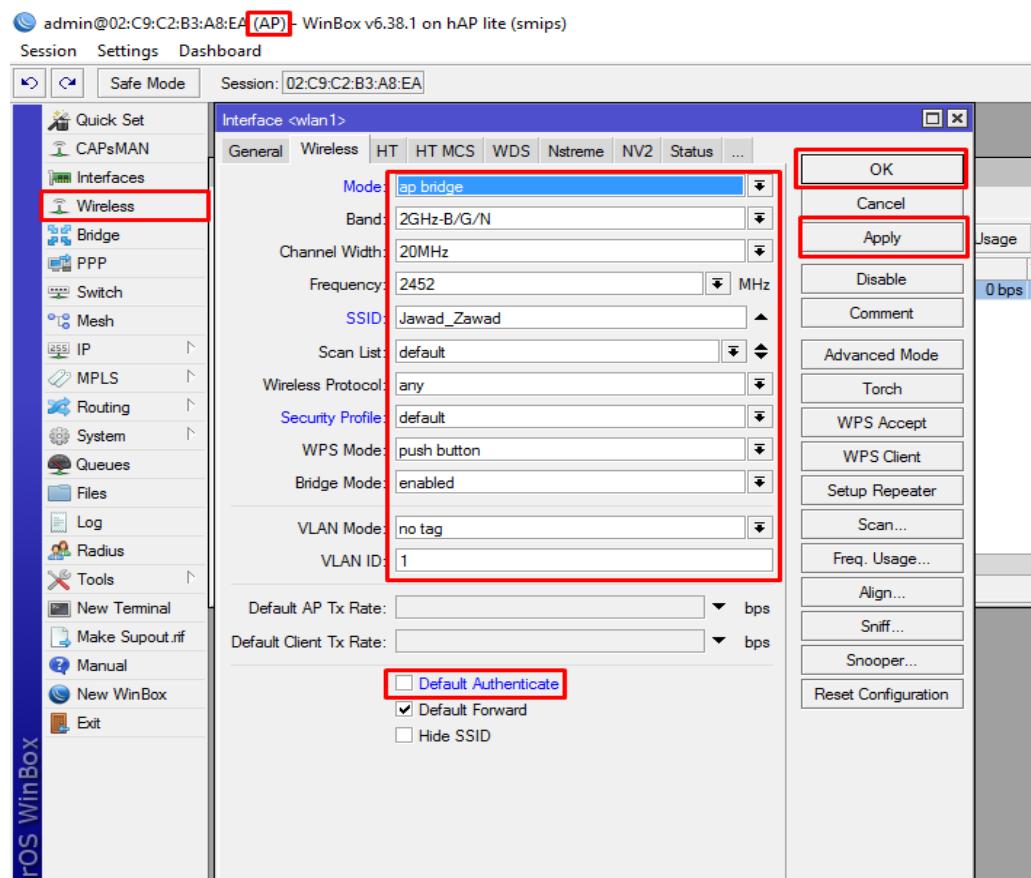
Lab 16. Mac-Address Filtering

Apa Fungsi Mac Address Filtering ? Mac-Address Filtering Berfungsi untuk Mem-Filter Mac-Address mana saja yang bisa terkoneksi (Access Point). Mac-Address Filtering berfungsi ketika kita sedang Menseetting Station dan kita ingin station tehubung Ke SSID=Jawad_Zawad, sedangkan ada dua router yang menggunakan SSID=Jawad_Zawad, Bagaimana cara kita menentukan target (Access Point) kita? Sedangkan Access Point Yang menggunakan SSID=Jawad_Zawad ada 2 ? Mac-Address Filtering adalah Solusi dari masalah ini..

Mari Kita coba Lab kan...

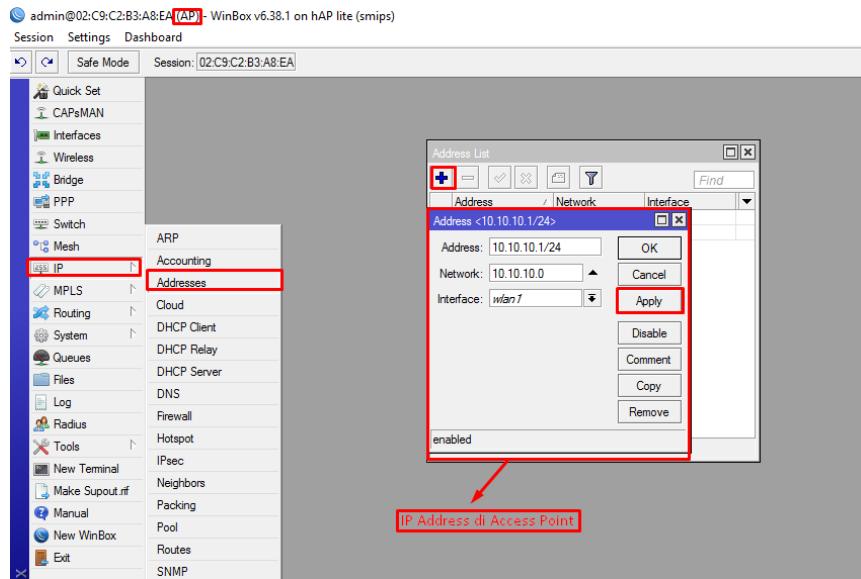
Pertama Setting Interface Wireless yang di gunakan Sebagai Access Point..

- Isi Mode=AP Bridge , Band, Channel, Frekuensi=Terserah
SSID=Jawad_Zawad
- Lalu Apply OK



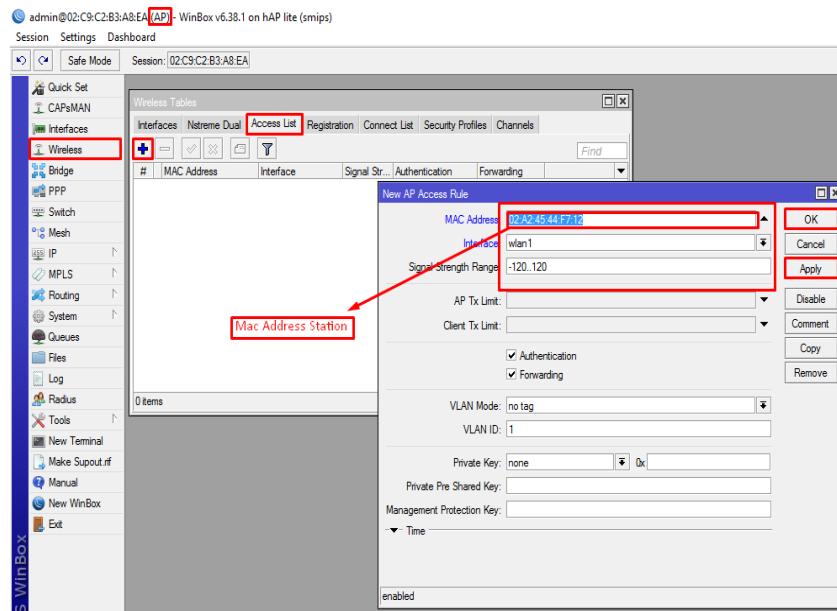
Step selanjutnya adalah membuat IP Address untuk interface Wireless..

- Isi IP address 10.10.10.1/24 dan Interface=Wlan1
- Lalu Apply dan OK

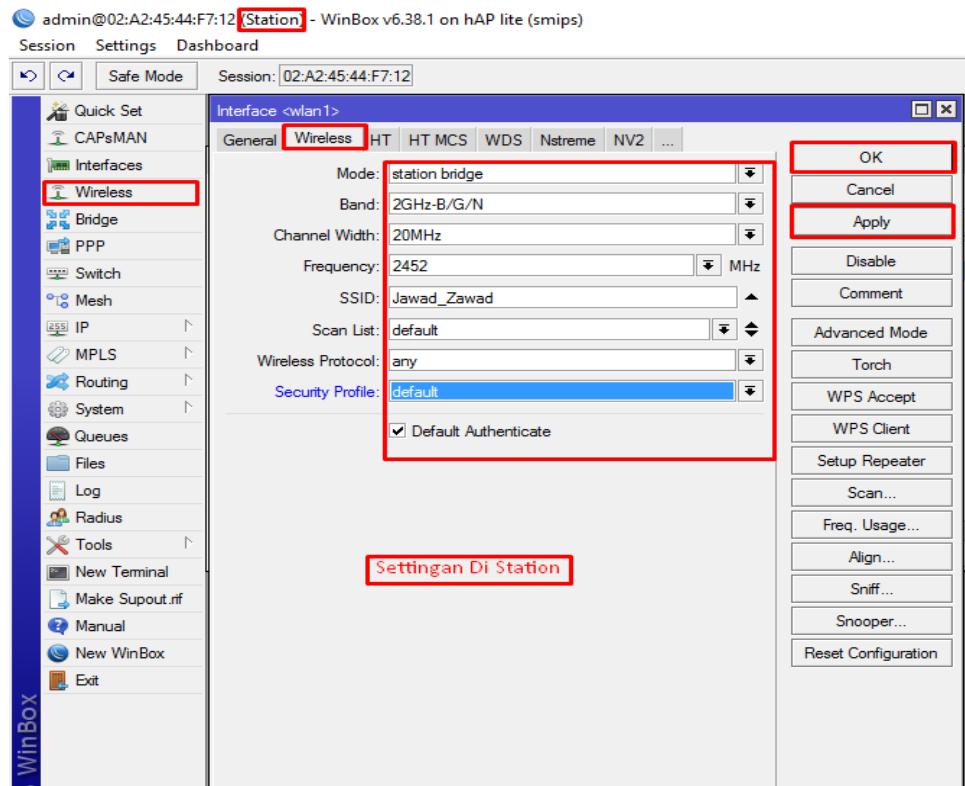


Step selanjutnya adalah memasukan Mac-Address station di access list yang berfungsi untuk meng-Izinkan Router station terhubung ke access point

- Klik Access List di menu Wireless > Add (+)
- Isi Mac-Address=02:A2:45:44:F7:12 (Mac-Address Station)
- Isi Interface=Wlan 1 ,karna kita menggunakan Wlan 1
- Lalu Apply OK



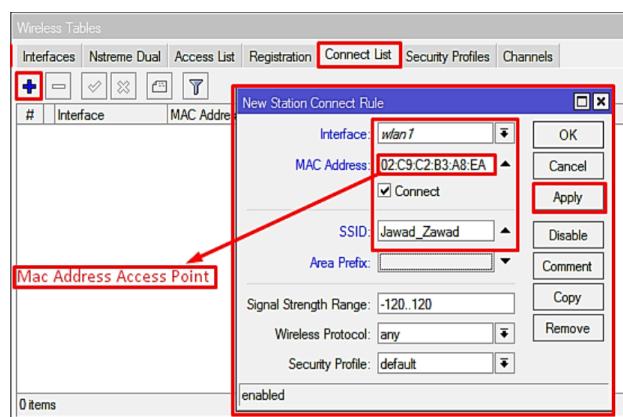
Selanjutnya Kita perlu men-Setting Wireless yang ada di station,



Yang wajib di isi adalah SSID nya,selain SSID kita bisa memilih bebas...

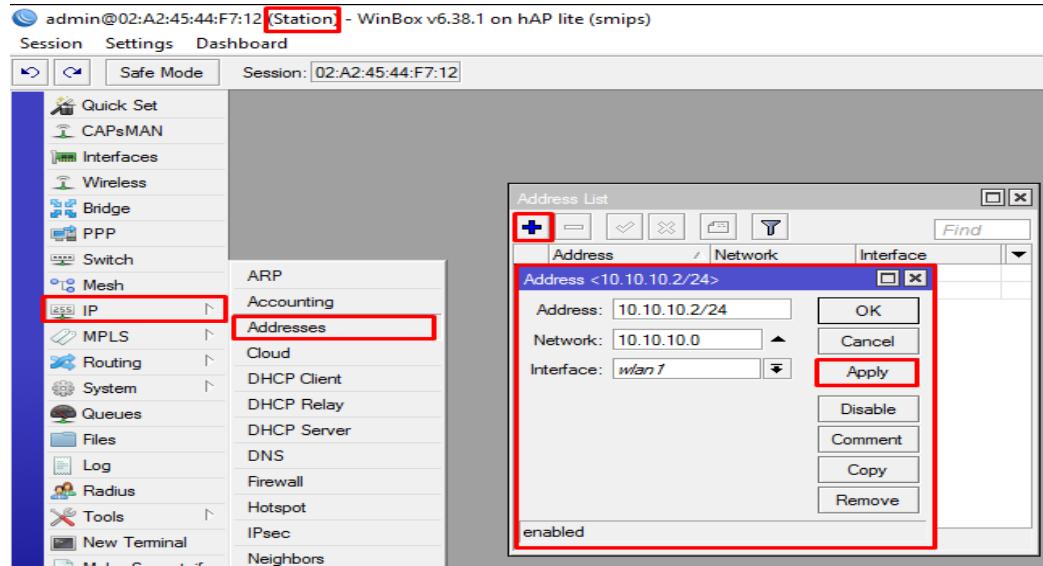
Selanjutnya kita perlu memasukan Mac-Address Access Point Di Connect List yang berfungsi agar Station mengarah langsung ke Access Point...

- Klik Connect List di menu Wireless > Add (+)
- Isi Mac-Address=02:C9:C2:B3:A8:EA (Mac-Address Access Point)
- Isi Interface=Wlan 1 ,karna kita menggunakan Wlan 1
- Dan Isi SSID=Jawad_Zawad
- Lalu Apply OK



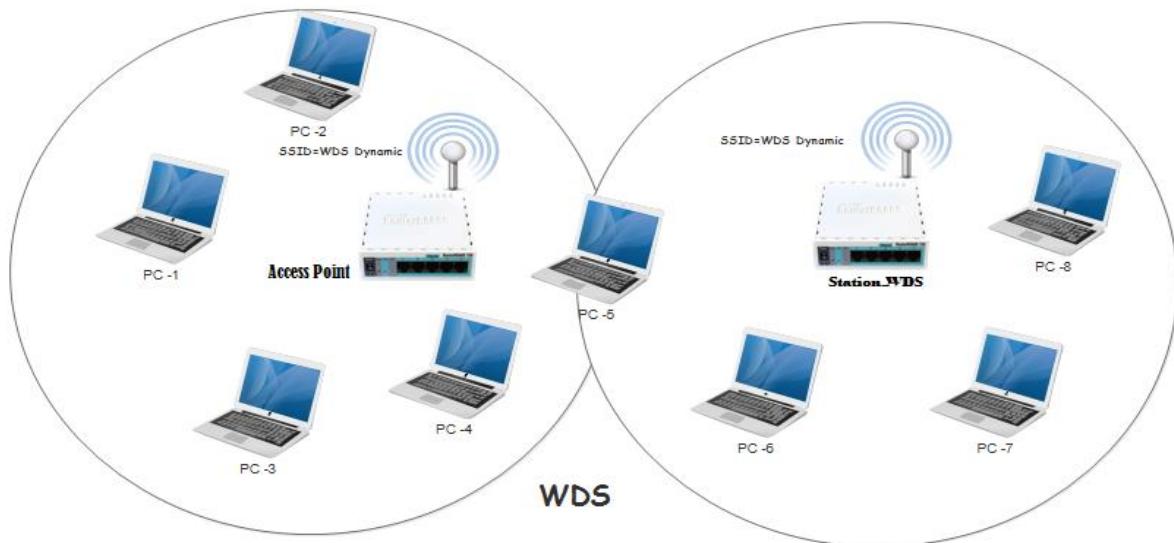
Step selanjutnya adalah memberi IP address Untuk interface Wlan 1..

- Isi Ip Address=10.10.10.2/24 dan interface=Wlan1
- Lalu Apply dan OK



Jika step ini sudah selesai maka Access Pont dan Station aka terhubung secara Otomatis walaupun ada dua Router yang menggunakan SSID=Jawad_Zawad

Lab 17. WDS Dynamic

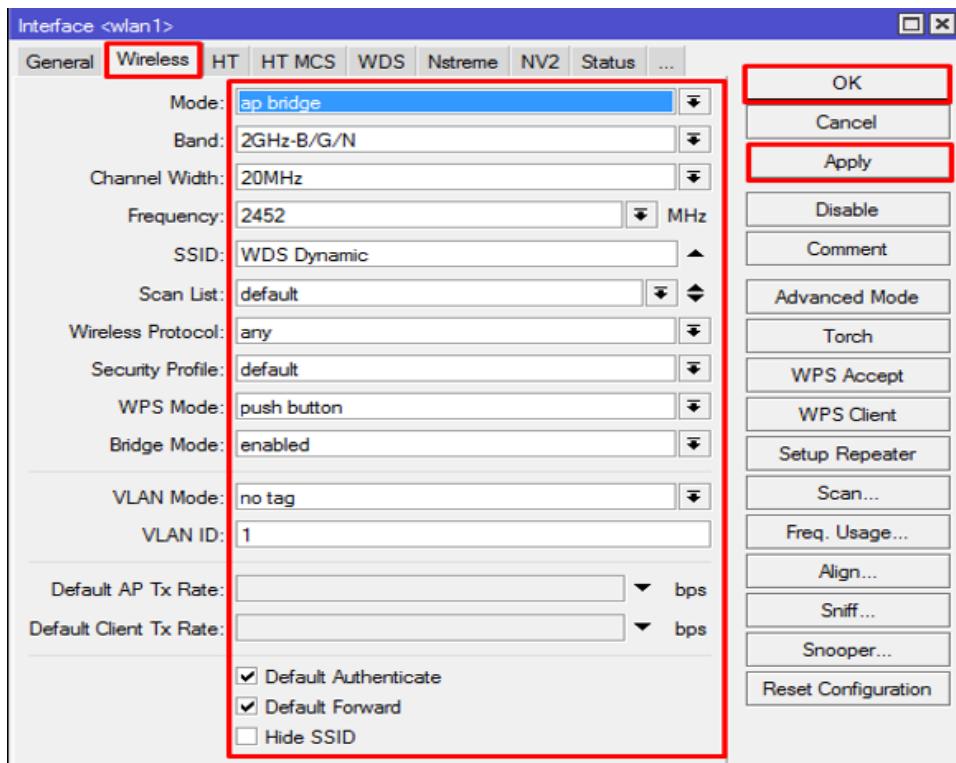


Apa Fungsi dari WDS ? WDS (Wireless Distribution System) adalah sistem yang memungkinkan interkoneksi antar Access point (AP). Sistem ini digunakan untuk memperluas jangkauan area wireless, dengan menggunakan beberapa perangkat AP Untuk Menjadi satu kesatuan, tanpa membangun backbone jaringan atau WDS itu bisa di fungsikan sebagai Repeater yang berfungsi untuk memperluas Jangkauan sinyal Sebuah Jaringan Wireless... Di lab ini kita akan mencoba membuat WDS secara Dynamic , karna WDS juga bisa di setting secara Static...

Pertama kita perlu men-Setting Wireless yang di gunakan Sebagai Access Point..

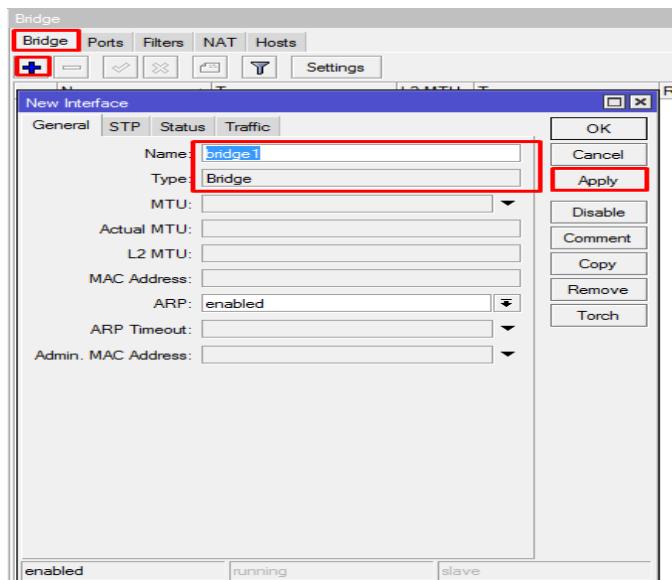
Setting Access Point dgn SSID=WDS Dynamic

- Isi Mode Ap Bridge , Band, Channel, Frekuensi=Terserah ,
- isi SSID=WDS Dynamic
- Lalu Apply dan OK



Selanjutnya kita perlu Membuat Bridge yang berfungsi agar Access Point dan Station-WDS terhubung...

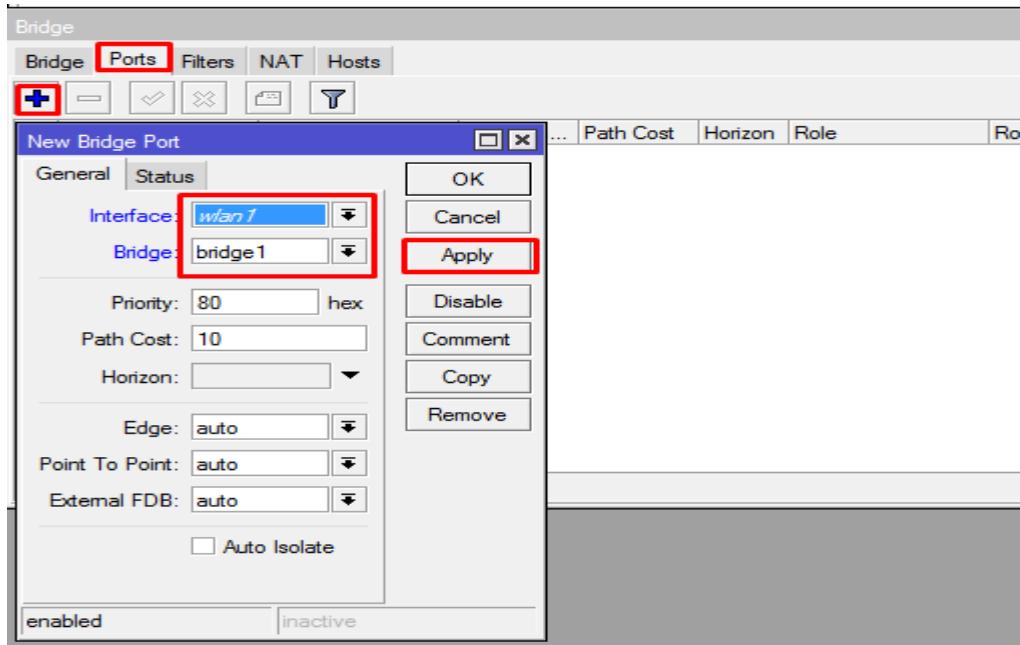
- Klik Menu Bridge > Add (+)
- Isi Name=Bebas (Bridge1)



Step selanjutnya adalah, Memasukan Interface Wireless ke Dalam Bridge1

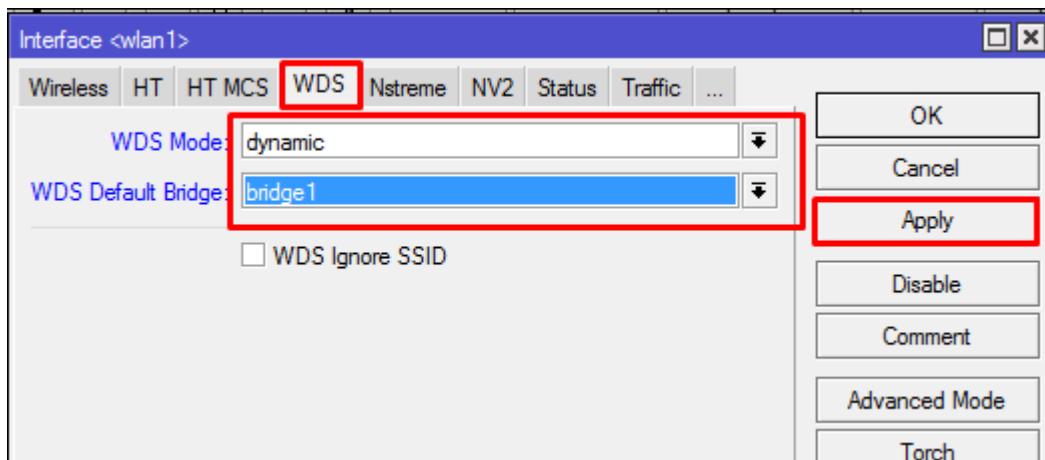
- Klik Port di menu Bridge > Add (+)

- Isi Interface=Wlan1 dan Bridge=Bridge1
- Lalu Apply dan OK



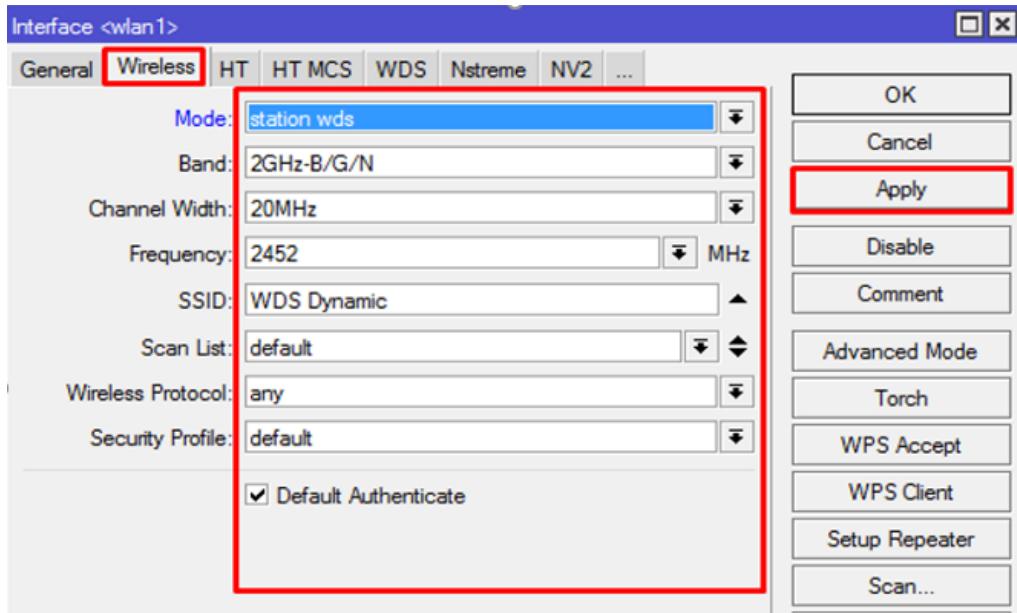
Selanjutnya kita perlu men-Setting WDS dynamic di menu Wireless..

- Klik WDS yang ada di menu Wireless
- Isi WDS Mode=Dynamic dan WDS Default Bridge=Bridge1
- Lalu Apply dan OK

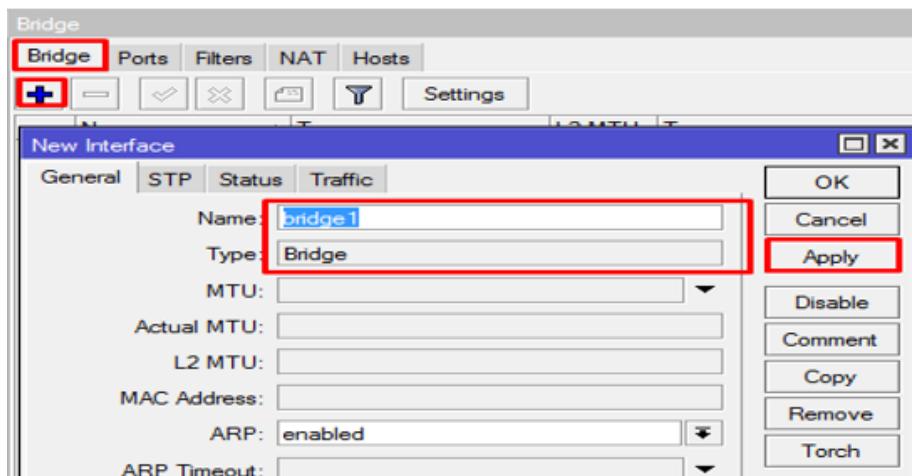


Step selanjutnya adalah emn-Setting Wireless yang di gunakan sebagai Station WDS...Setting Wireless Seperti Biasa (Station) Hanya Mode nya saja yang Diaganti dengan Station-Wds

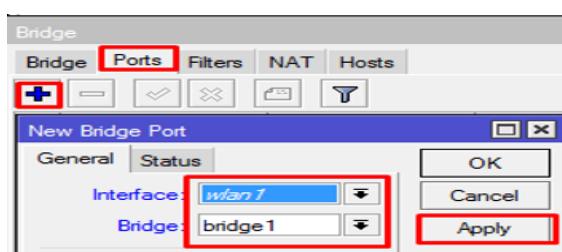
- isi Mode=Station Wds , Band, Channel, Frekuensi, SSID=Di sesuaikan dengan Access Point
- Lalu Apply dan OK



Step selanjutnya adalah Membuat Bridge dan memasukan Interface Wlan 1 ke Bridge yang telah kita buat..

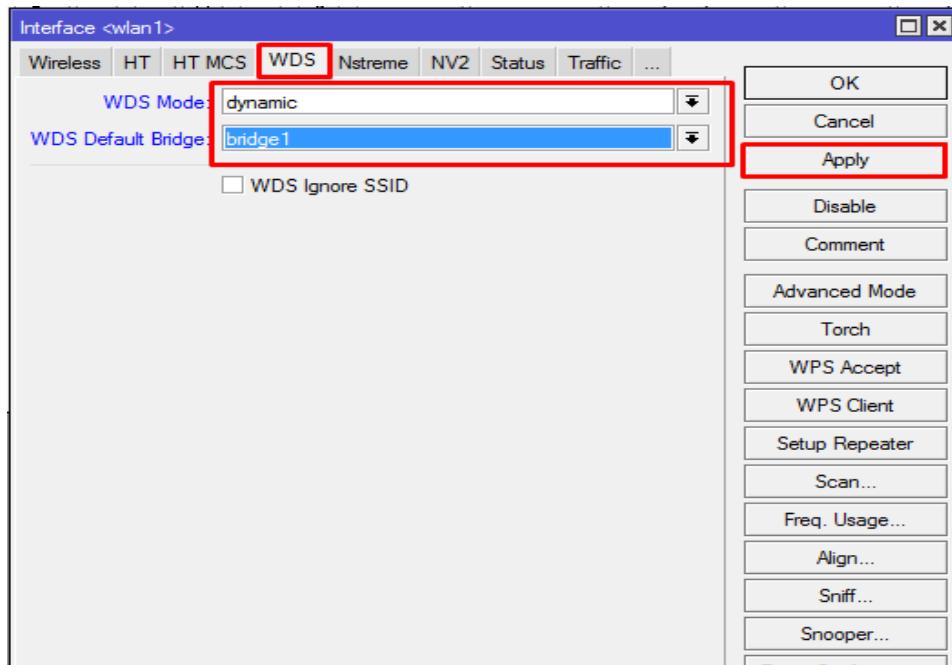


Masukan Interface Wlan1 Ke Bridge 1



Step yang terakhir adalah men-Setting Wds di station.. cara nya sama seperti men-Setting WDS di Access Point..

- Klik WDS yang ada di menu Wireless
- Isi WDS Mode=Dynamic dan WDS Default Bridge=Bridge1
- Lalu Apply dan OK



Jika step ini sudah Selasai maka akan terbentuk Interface WDS di Router yang berfungsi sebagai Access Point....

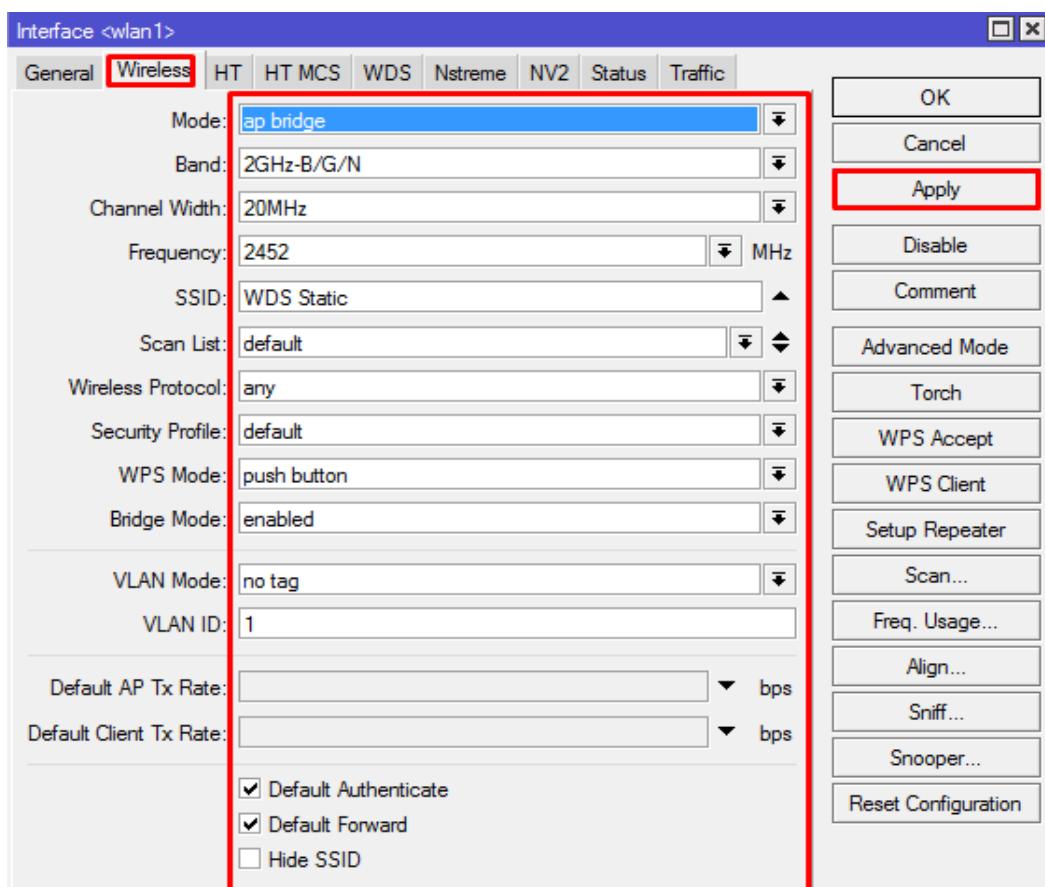
Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
RS wlan1	Wireless (Atheros AR9...)	1500	0 bps	0 bps	0	0
DRS & wds6	WDS	1500	0 bps	0 bps	0	0

Lab 18. WDS Static

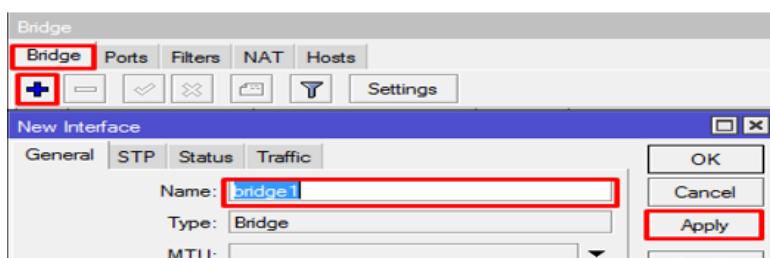
Jika di Lab sebelumnya Kita membuat WDS secara Dynamic, Di Lab ini kita akan Membuat WDS secara Static..

Setting Access Point Dgn SSID=WDS Static

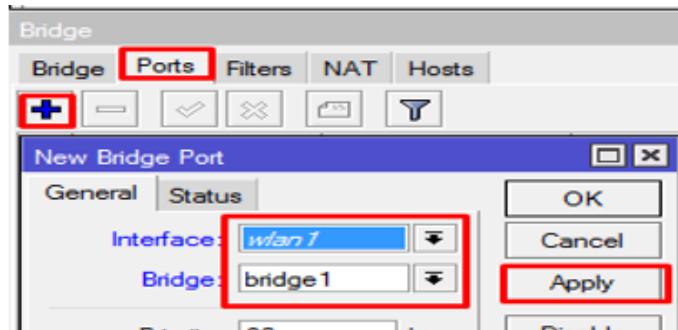
- Isi Mode Ap Bridge , Band, Channel, Frekuensi=Terserah ,
- isi SSID=WDS Static
- Lalu Apply dan OK



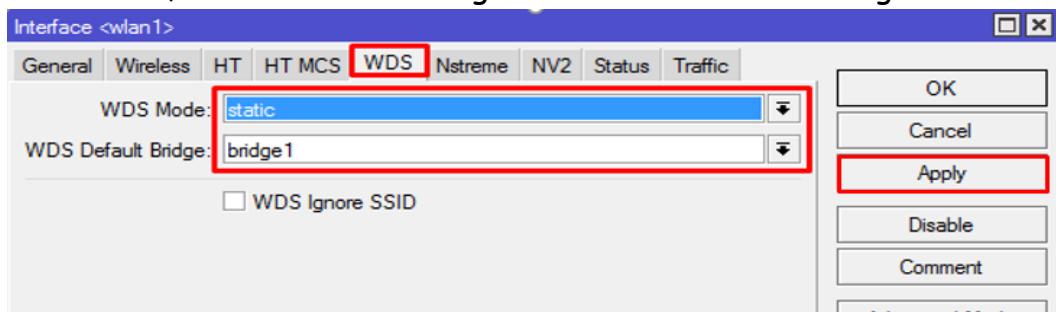
Selanjutnya Kita Perlu Membuat Bridge dan memasukan Inteface Wlan1 ke dalam Bridge yang telah kita buat..



Masukan Interface Wlan1 Ke Bridge tersebut

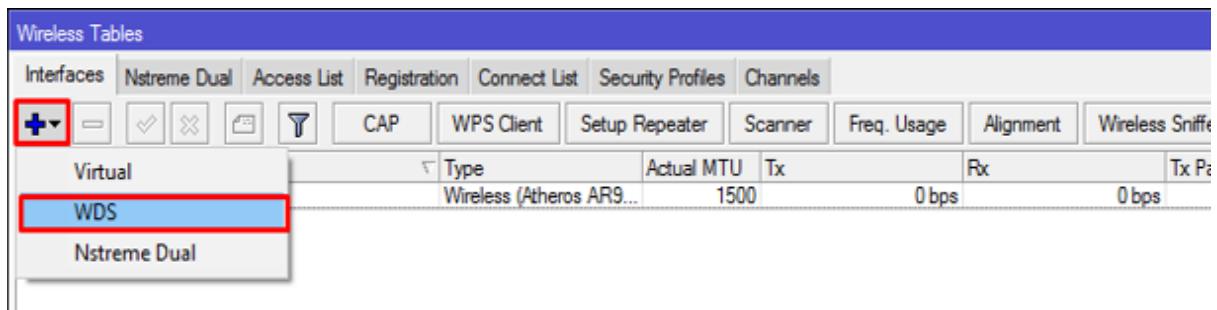


Jika sudah,Kita akan Mensetting WDS di Access Point dengan WDS Static

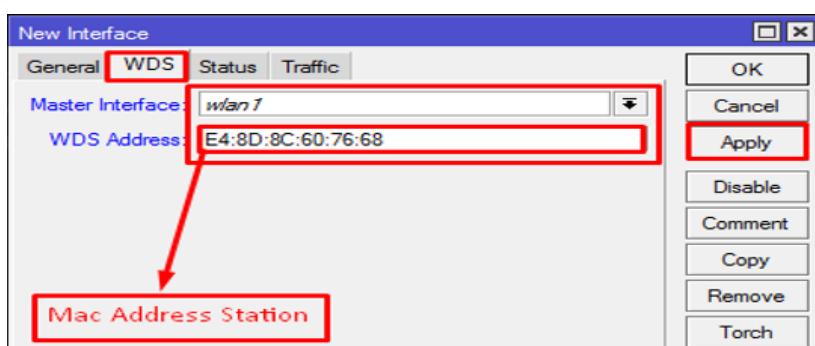


Step Selanjutnya adalah,Kita Buat Interface WDS secara manual...

- Klik Menu Wireless > Add (+) > WDS

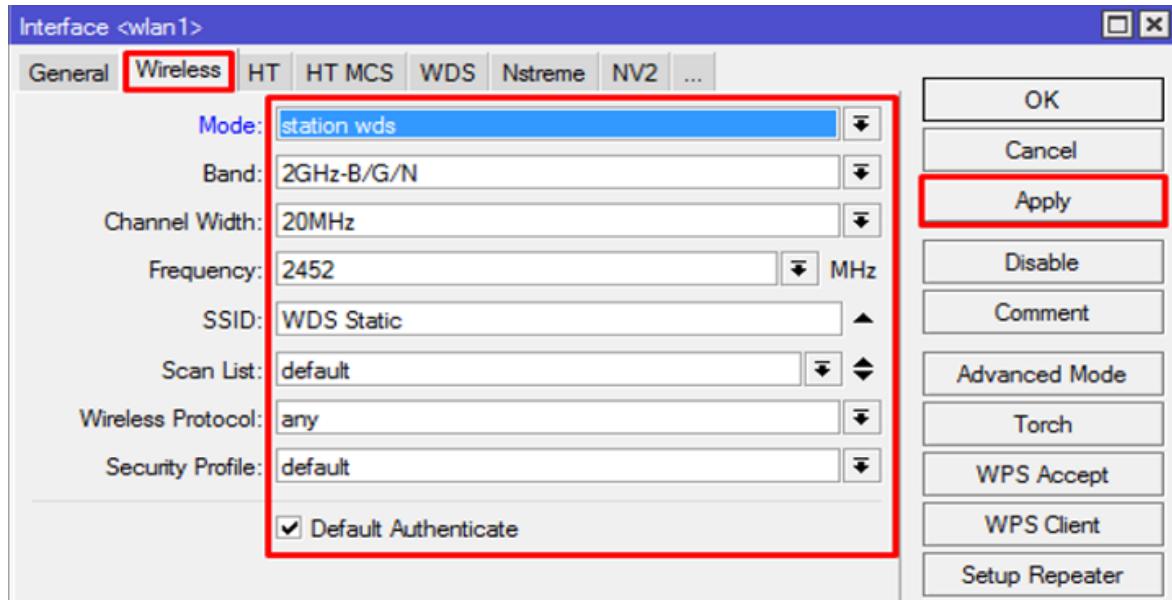


- Klik WDS > Isi Master Interface=Wlan 1
- Isi Mac Address=E4:8D:8C:60:76:68 (Mac Address Station)

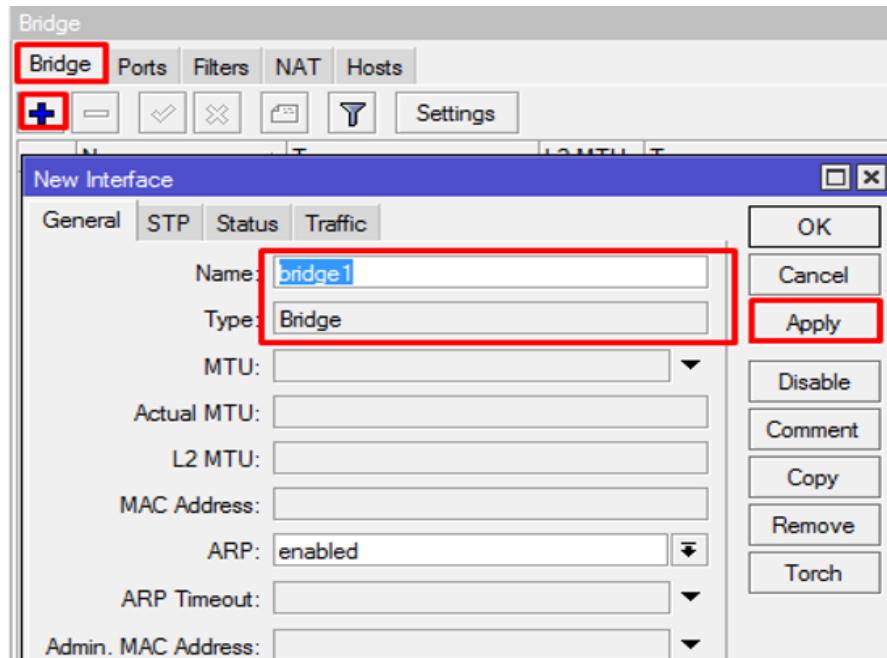


Settingan Wireless dan WDS di Access Point Telah Selesai, Selanjutnya kita akan men-Setting Di Station.

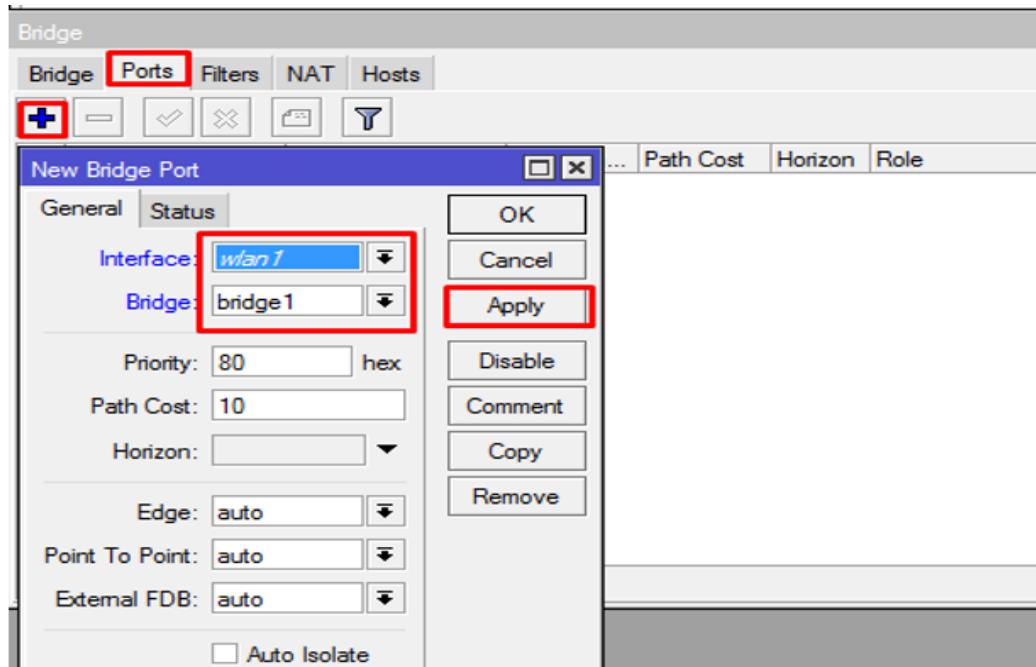
Setting Wireless Dengan Mode=Station WDS , band dan yanng lainnya di sesuaikan dengan Access Point...



Step Selanjutnya adalah Membuat Bridge dan Memasukan Interface Wlan 1 ke Bridge tersebut..



Dan masukan Interface Wlan 1 Ke Bridge yang telah kita buat.



Jika Step Ini sudah Selesai Maka Interface WDS yang ada di Access Poit akan Berstatus (RSA) yang artinya Fungsi dari WDS telah Berfungsi..

Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/c)	Rx Packet (p/c)
RS wlan1	Wireless (Atheros AR9...)	1500	848 bps	0 bps	2	0
RSA wds1	WDS	1500	424 bps	0 bps	1	0

2 items out of 8

Status di AP

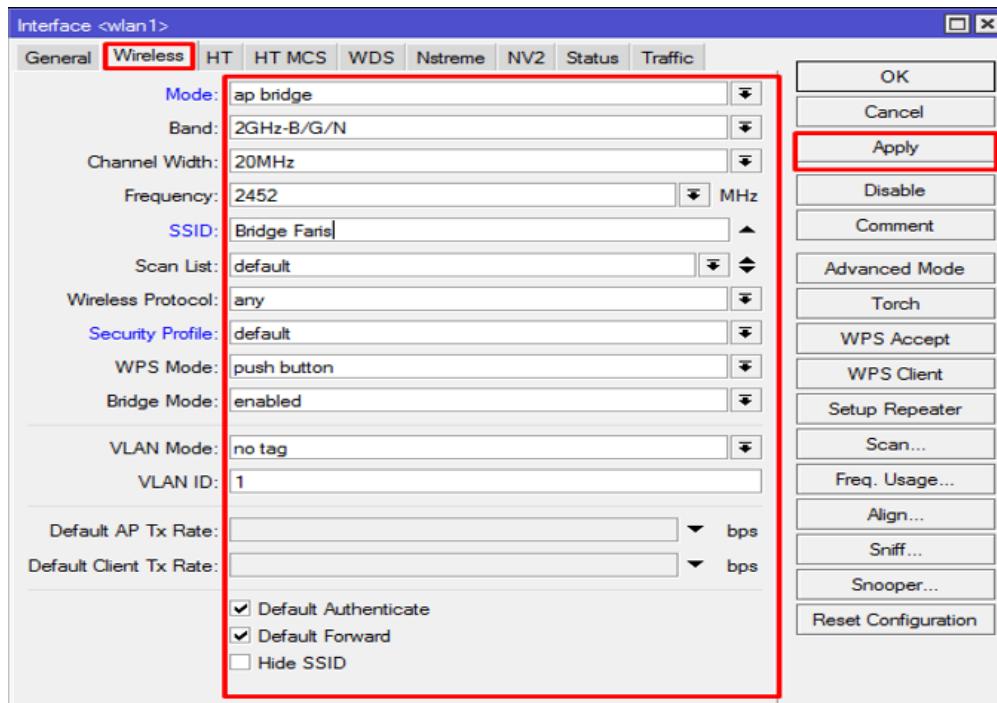
Lab 19. Wireless Bridge

Bridge adalah Fitur yang berfungsi menghubungkan beberapa jaringan terpisah agar menjadi Satu Segmen Jaringan. dan Bridge bisa menghubungkan tipe jaringan yang Berbeda-beda



Pertama Kita Setting Access Point Menggunakan SSID=Bridge Faris

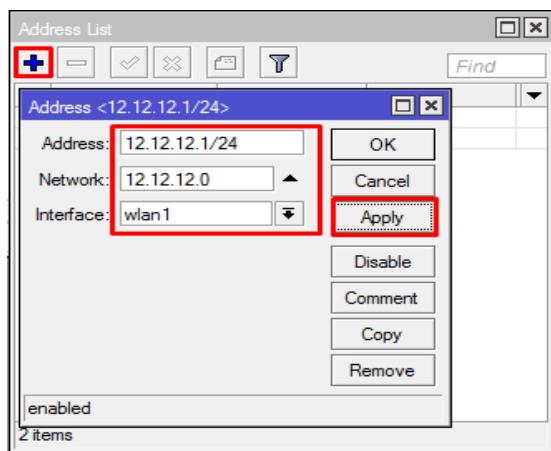
- Isi Mode Ap Bridge , Band, Channel, Frekuensi=Terserah ,
- isi SSID=Bridge Faris (Terserah)
- Lalu Apply dan OK



Langkah Selanjutnya adalah Membuat IP Address Untuk Interface Wireless dan Untuk Interface Ethernet 2 (LAN)

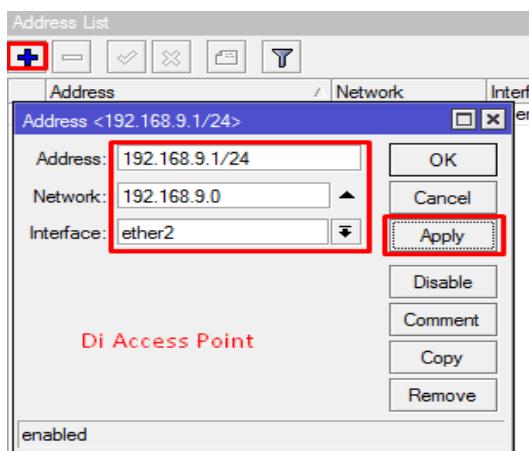
Buat IP Address Untuk Interface Wlan terlebih dahulu...

- Klik IP > Address > Add (+)
- Isi Address=12.12.12.1/24 dan isi Interface=Wlan1
- Lalu Apply dan OK



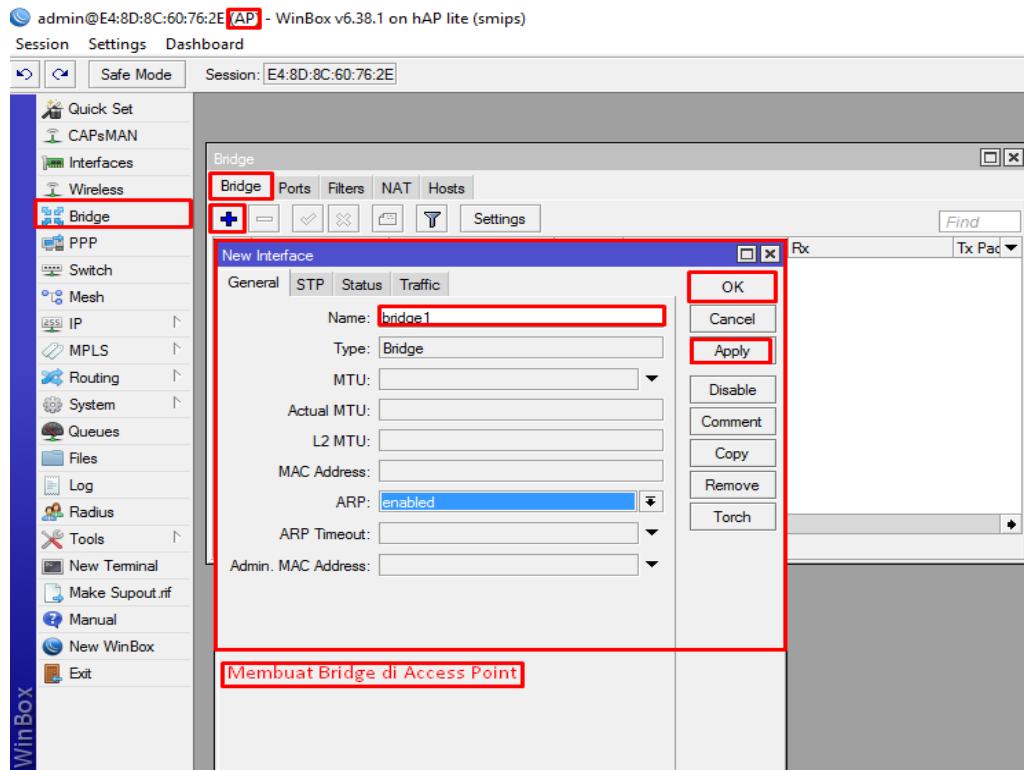
Selanjutnya Kita buat IP address lagi Untuk Ethernet 2 (LAN)

- Klik IP > Address > Add (+)
- Isi Address=192.168.9.1/24 dan isi Interface=Ether2
- Lalu Apply dan OK

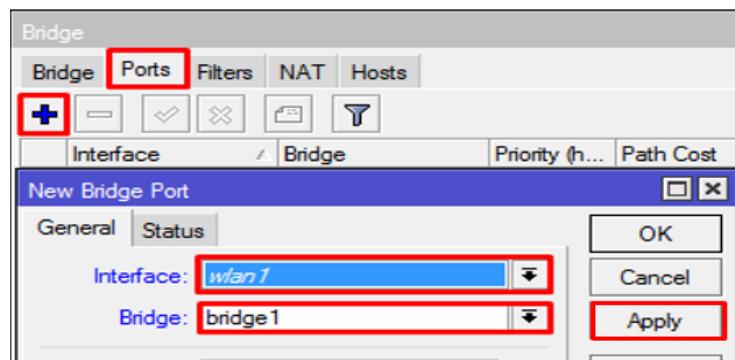


Lalu kita setting IP PC yang terhubung ke Access Point dengan IP Address 192.168.9.2/24 dan gateway nya 192.168.9.1

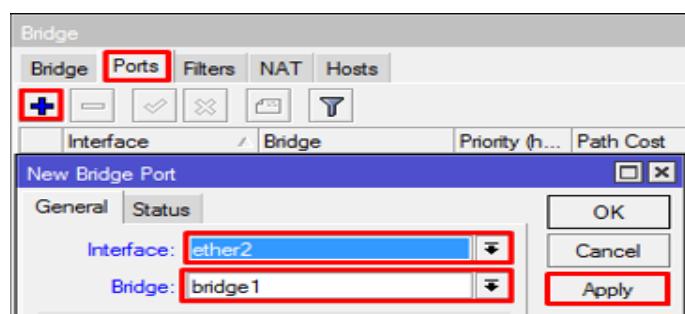
Step Selanjutnya adalah Membuat Bridge, dan Memasukan Interface Wlan 1 dan Ethernet 2 ke Bridge yang telah kita buat..



Selanjutnya Kita masukan Interface Wlan 1 Ke Bridge Tersebut



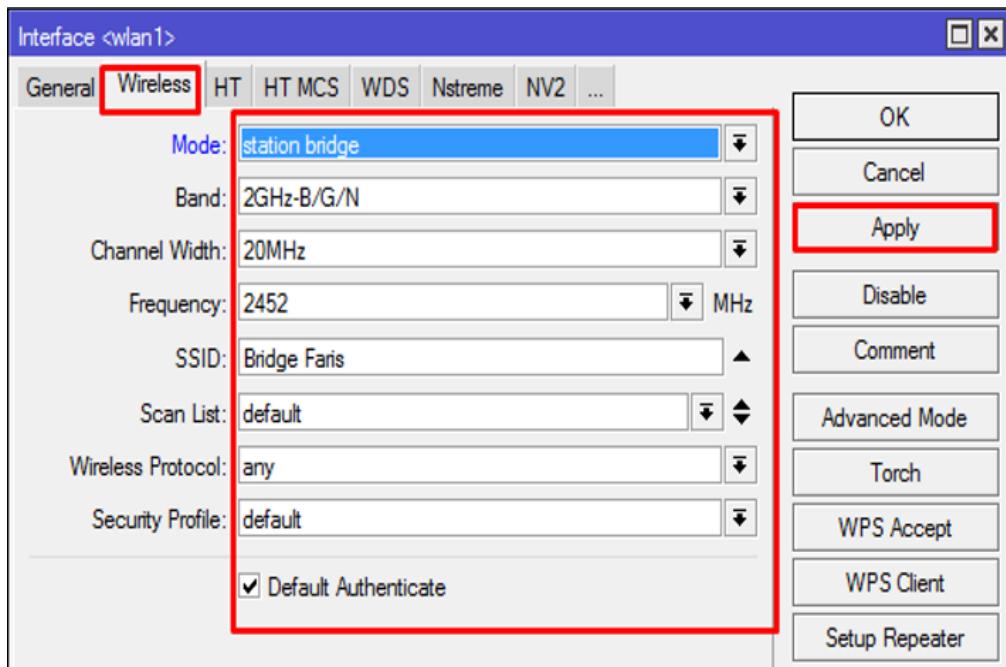
Selanjutnya masukan Juga Interface Ethernet 2 Ke Bridge tersebut..



Step selanjutnya adalah Men-Setting Router Yang di gunakan Sebagai Station..

Setting Wireless Mode=Station Bridge Dan Tujuan SSID=Bridge Faris

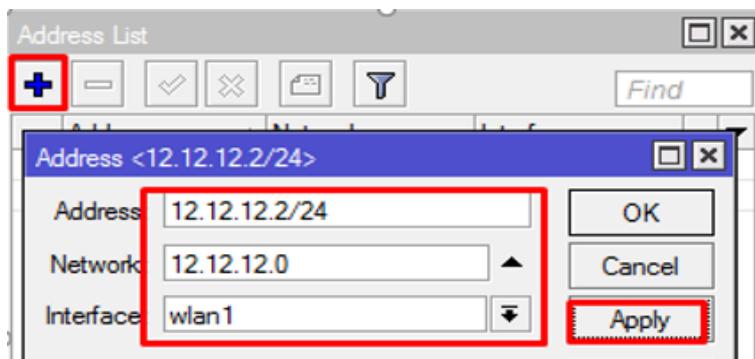
- Isi Mode Station Bridge , Band,Channel,Frekvensi=Mengikuti AP
- isi SSID=Bridge Faris
- Lalu Apply dan OK



Step Selanjutnya adalah membuat IP address Untuk Interface Wlan 1 dan Ethernet 2 (LAN)

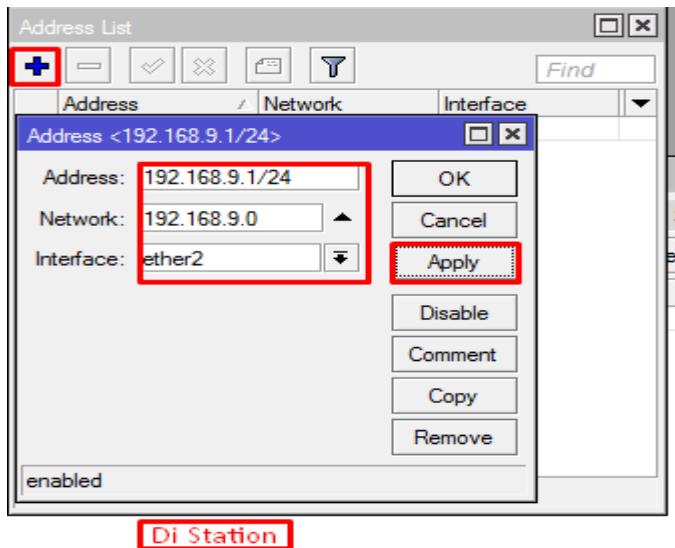
Buat IP Address Untuk Interface Wlan terlebih dahulu...

- Klik IP > Address > Add (+)
- Isi Address=12.12.12.1/24 dan isi Interface=Wlan1
- Lalu Apply dan OK



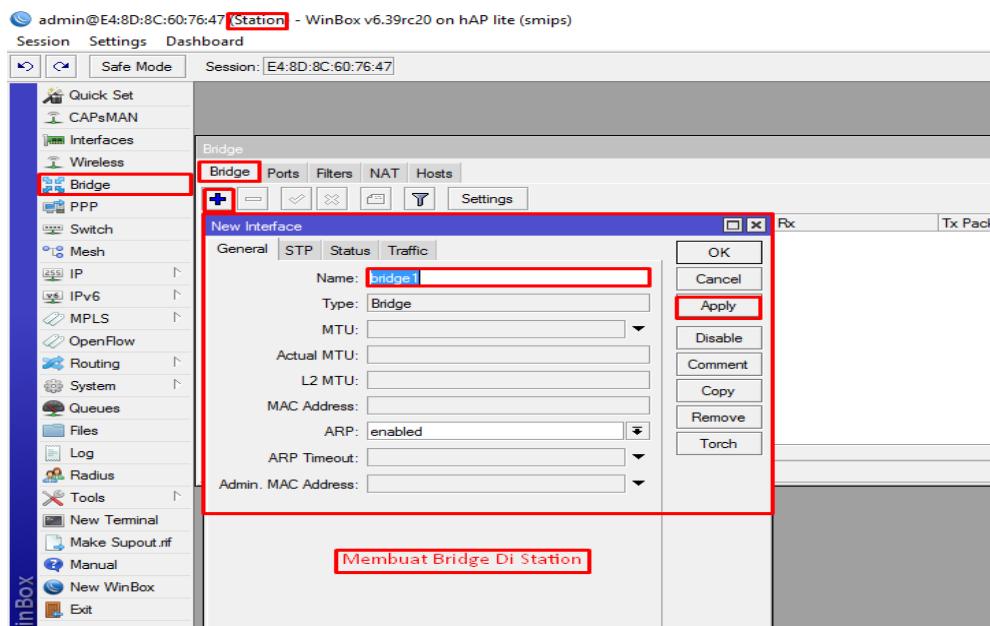
Selanjutnya Kita buat IP address lagi Untuk Ethernet 2 (LAN)

- Klik IP > Address > Add (+)
- Isi Address=192.168.9.1/24 dan isi Interface=Ether2
- Lalu Apply dan OK

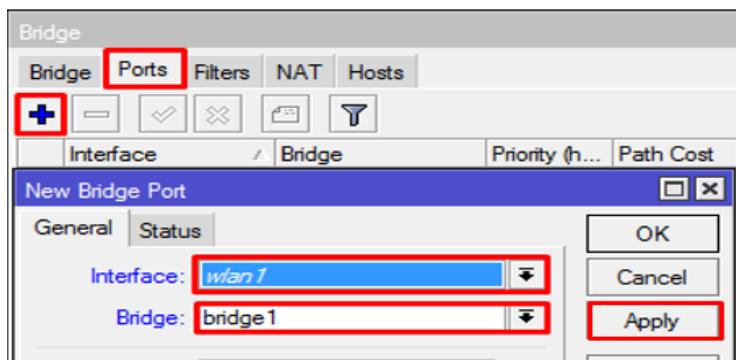


Lalu kita setting IP PC yang terhubung ke Station dengan IP Address 192.168.9.3/24 dan gateway nya 192.168.9.1

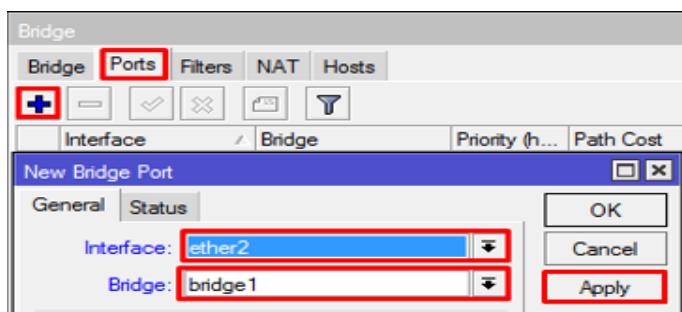
Step Selanjutnya adalah Membuat Bridge,dan Memasukan Interface Wlan 1 dan Ethernet 2 ke Bridge yang telah kita buat..



Selanjutnya Kita masukan Interface Wlan 1 Ke Bridge Tersebut

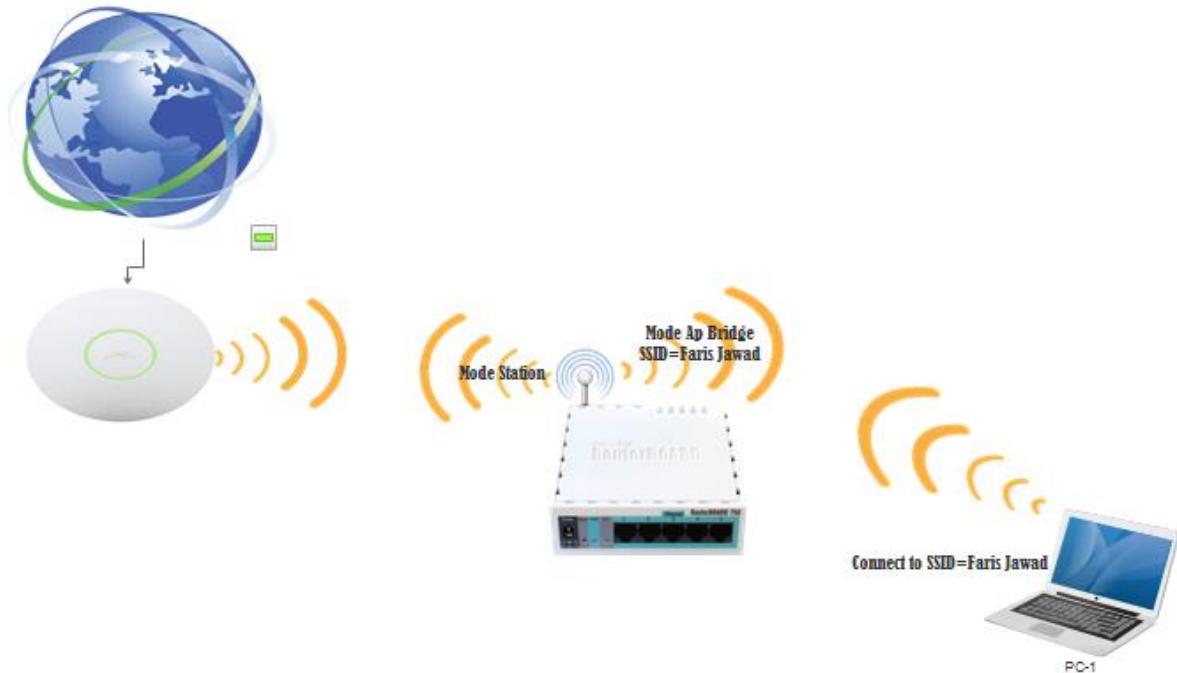


Selanjutnya masukan Juga Interface Ethernet 2 Ke Bridge tersebut..



Setelah Step Ini selesai Maka PC 1 yang terhubung Ke Access Point(192.168.9.2) akan menjadi satu segmen jaringan dengan PC 2 yang terhubung dengan Station(192.168.9.3)... dengan demikian PC 1 bisa melakukan Test Ping ke PC 2 karna sekarang Kedua PC tersebut telah Menjadi satu Segmen Jaringan..

Lab 20. Wireless Multi Fungsi

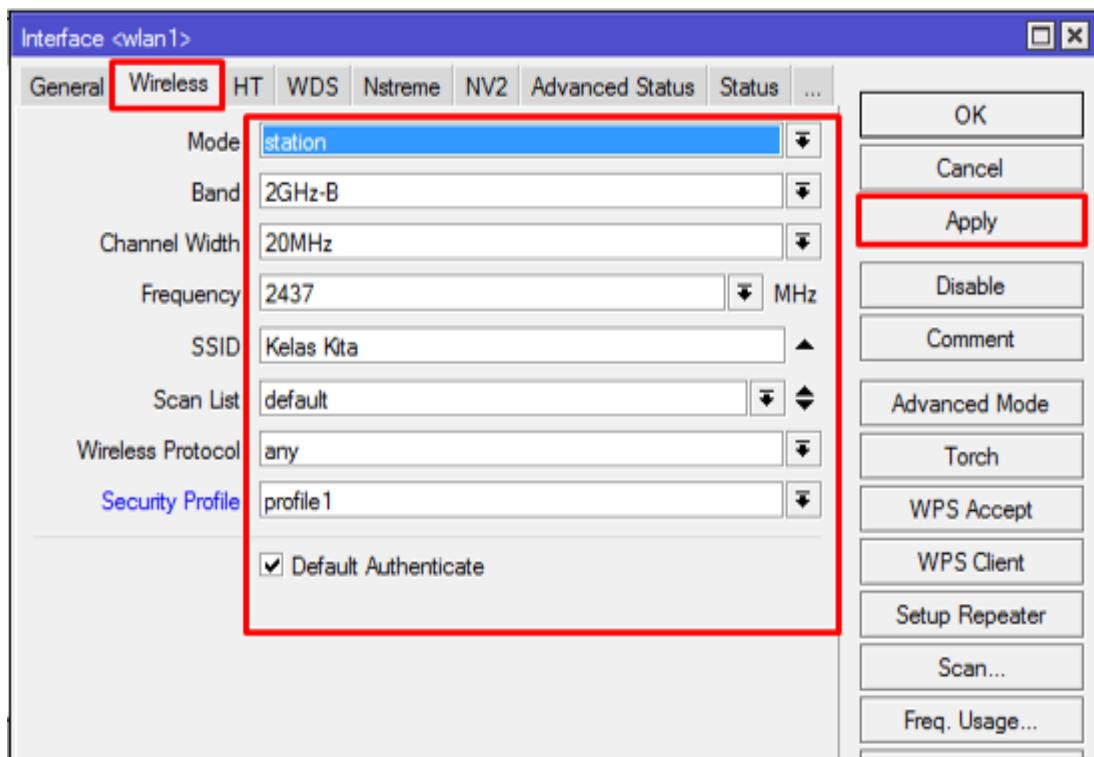


Yang di maksud dengan Wireless Multi Fungsi adalah adalah menggunakan 1 interface wireless untuk 2 fungsi yang berbeda,jadi jika kita mempunyai router yang hanya memiliki 1 interface Wireless kita bisa menggunakan 1 Interface wireless Tersebut menjadi 2 fungsi (Station dan AP Bridge)

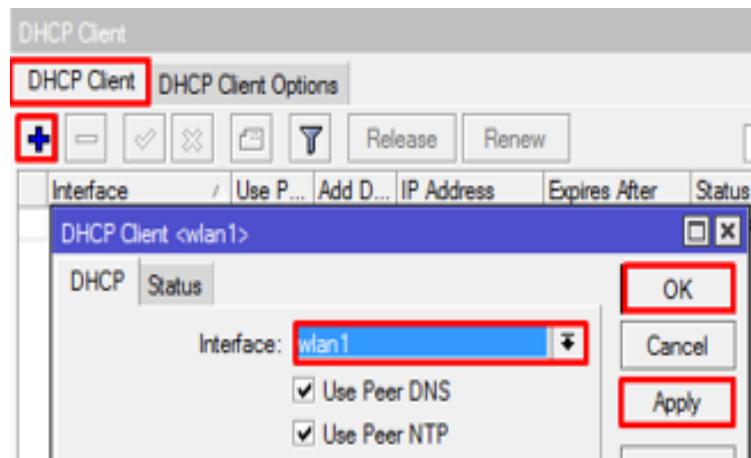
Di lab ini saya menggunakan Router Hap Lite yang hanya memiliki 1 interface Wireless dengan 1 interface Wireless, saya akan menggunakan Master Interface Sebagai Station untuk terhubung ke internet dan saya akan membuat Virtual Access Point agar Router bisa di fungsikan sebagai Access Point...

Pertama Kita setting Master Interface sebagai Wireless Client untuk terhubung ke Internet....

- Pertama Kita buat Security Profile Di Wireless
- Lalu Kita setting Wireless agar bisa terkoneksi ke Access Point
- Lalu Apply dan OK



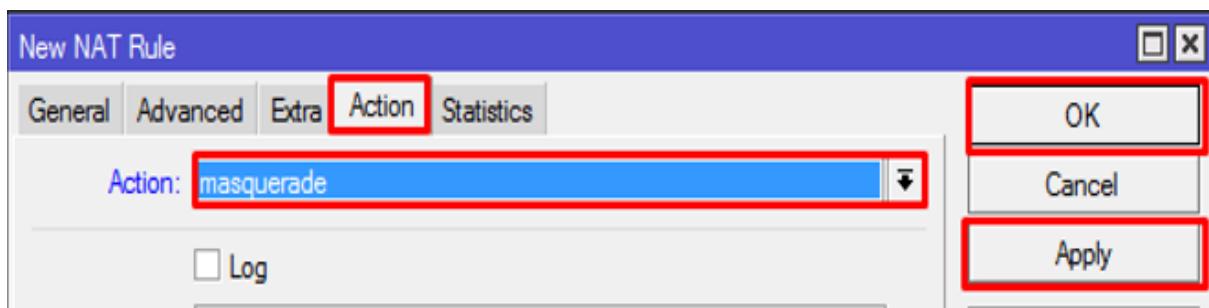
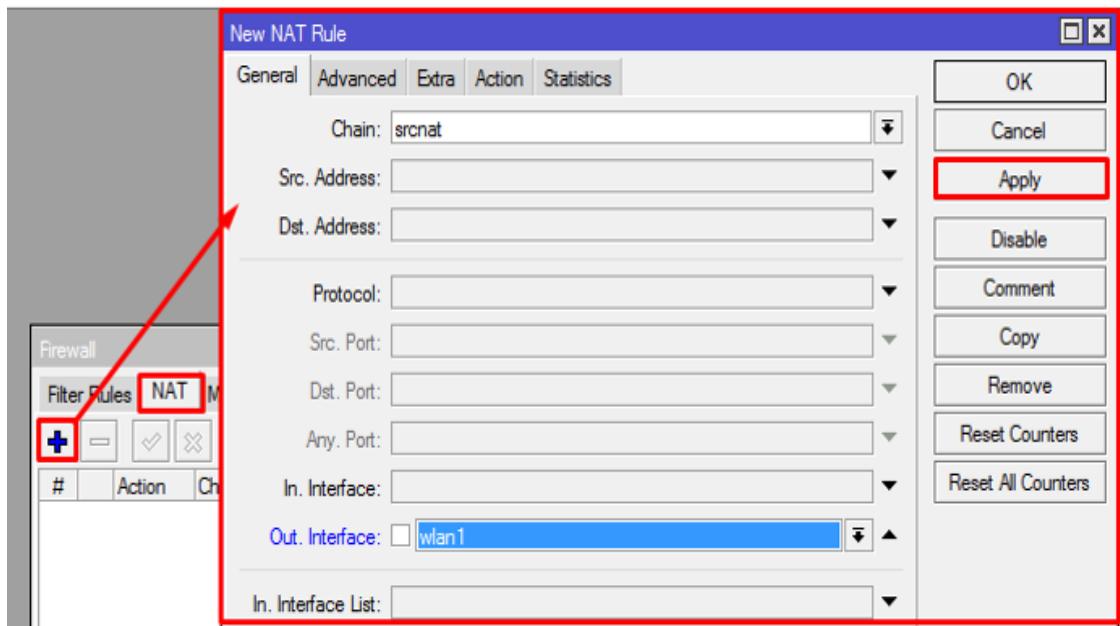
Step Selanjutnya adalah membuat DHCP Client agar Router Mendapatkan IP Address dari Access Point...



Jika sudah Mendapatkan IP DHCP Client dari Router, Step Selanjutnya adalah Membuat NAT agar Router Beserta LAN yang terhubung bisa meng-Akses Internet..

Setting NAT

- Isi Chain=SrcNat ,Out Interface=Wlan1 dan Action=Masquerade
- Lalu Apply dan OK

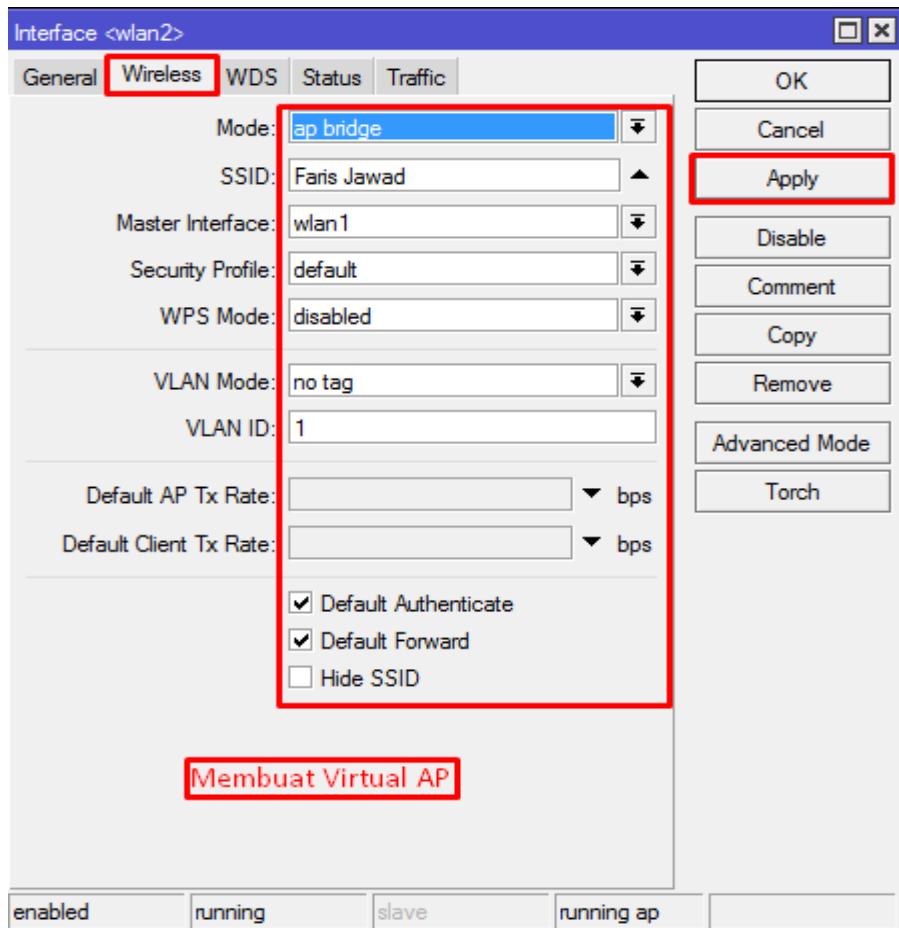


Setelah Step ini sudah selesai maka Router sudah terhubung ke internet...

Selanjutnya Kita akan membuat Virtual Access Point agar Router dapat di fungsikan sebagai Access Point...

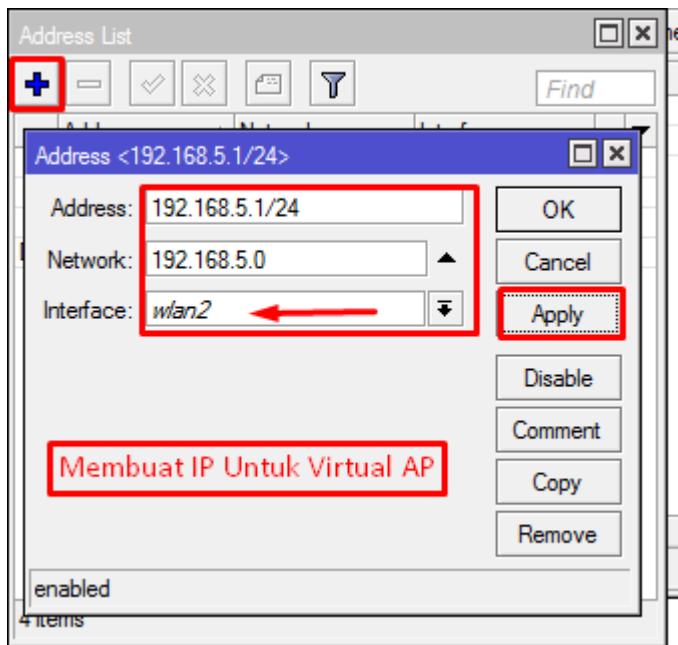
Membuat Virtual Access Point

- Klik Menu Wireless > Add (+) > Virtual
- Isi Mode=AP Bridge SSID=Faris Jawad ,Master Interface=Wlan1



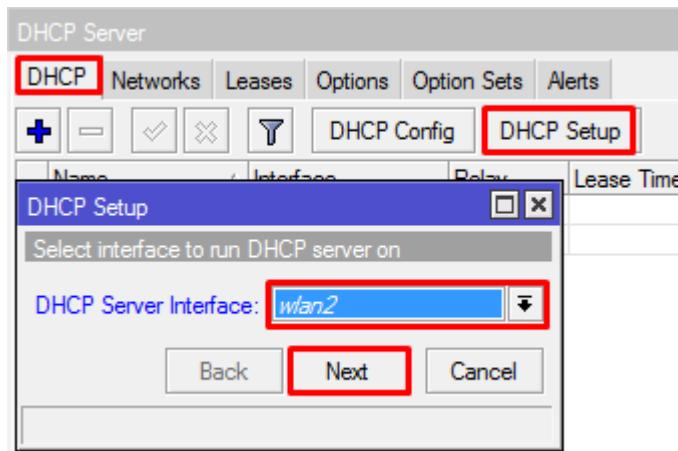
Maksud dari Master-Interface=Wlan 1 adalah Band, Channel, Frekuensi mengikuti Interface Wlan 1, Di virtual AP ini kita bisa membuat Security Profile juga yang berfungsi agar access Point kita memiliki Password....

Step Selanjutnya Adalah membuat IP address Untuk Wlan2 (Virtual AP)



Di sini saya memberikan IP address 192.168.5.1/24

Jika Kita sudah membuat IP address Kita perlu membuat DHCP Server yang berfungsi untuk Memberikan IP Address secara Otomatis Ke Client yang terhubung ke SSID=Faris Jawad (VAP)

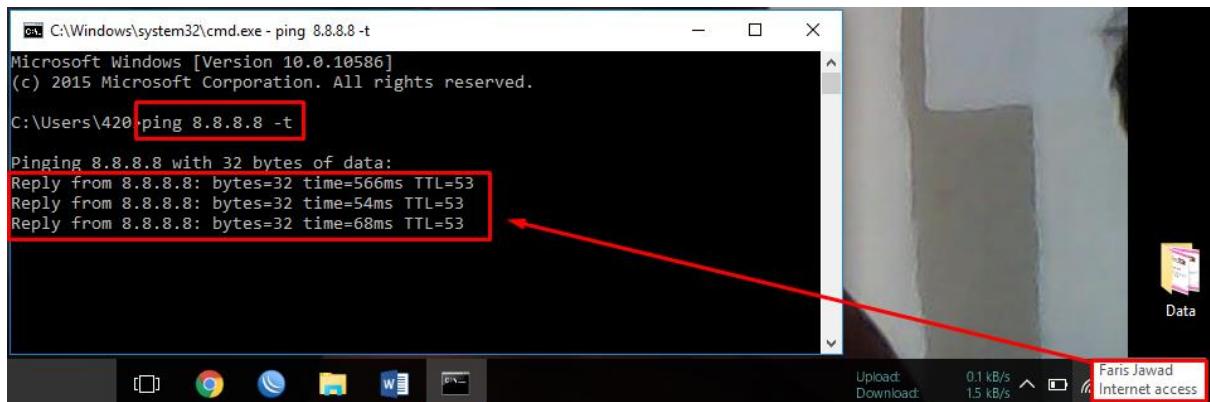


- Klik IP > DHCP Server > DHCP Setup
- Isi Interface=Wlan2 (Virtual Access Point)...

Lalu Next Next saja Hingga Selesai.....

Setelah Step ini selesai maka 1 Interface Wireless yang dimiliki oleh Memiliki 2 Fungsi yaitu menjadi Station dan Menjadi Access Point...

Untuk Pengetesan Coba kita masuk ke VAP tersebut dan Coba untuk meng-Akses Internet..



Lab 21. Wireless Repeater

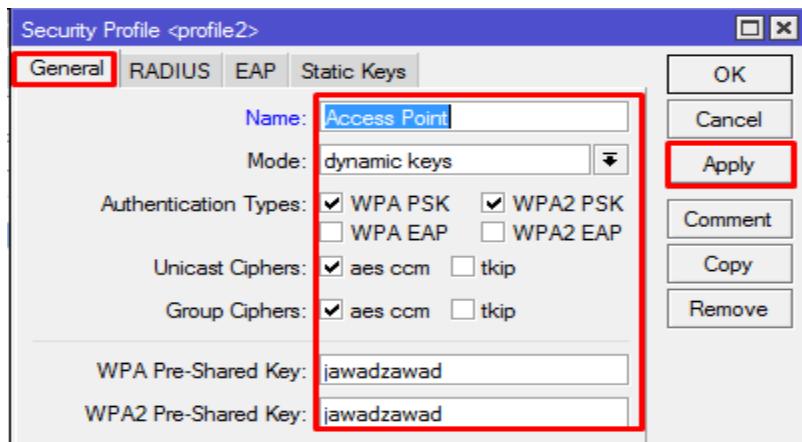
Di lab ini kita akan membahas bagaimana cara nya agar Router kita bisa di gunakan sebagai Repeater yang berguna untuk memperluas jangkauan area Wireless,dan di lab sebelumnya kita telah mencoba Membuat WDS yang fungsi nya sama seperti Repeater ,Fitur Wireless Repeater ini adalah Fitur yang baru di keluarkan oleh mikrotik,Fitur ini hanya support pada perangkat yang menggunakan RouterOS 6.35 ke atas,Dan Fitur ini di perkenalkan pada saat event MUM Europe 2016.



Di sini RouterBoard Kiri Akan berfungsi sebagai Pusat Access Point dan RouterBoard Kanan Akan di fungsikan sebagai Repeater...

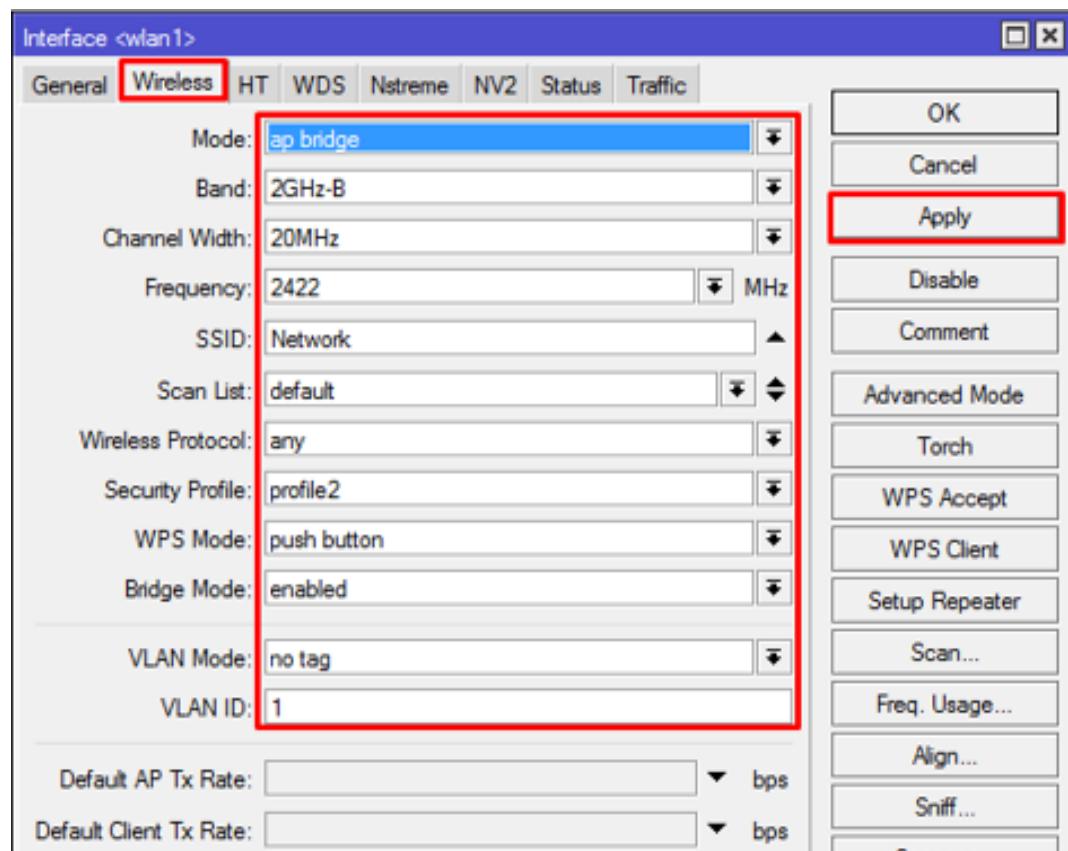
Pertama Kita Perlu Men-Setting RouterBoard kiri sebagai Access Point..

- Pertama Kita buat Security Profile Di Wireless



Lalu Kita setting Wireless sebagai Access Point

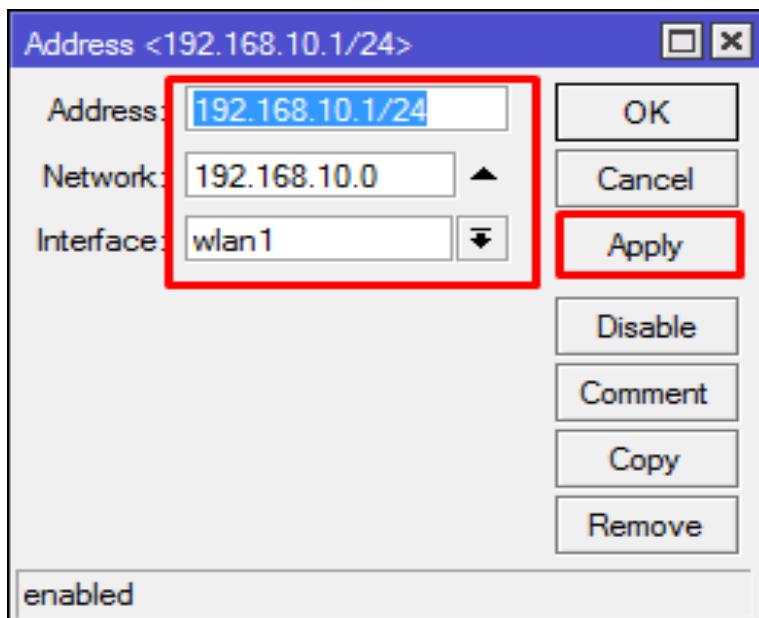
- Isi SSID=Network , Channel,Frekvensi,Band=Terserah



- Lalu Apply dan OK

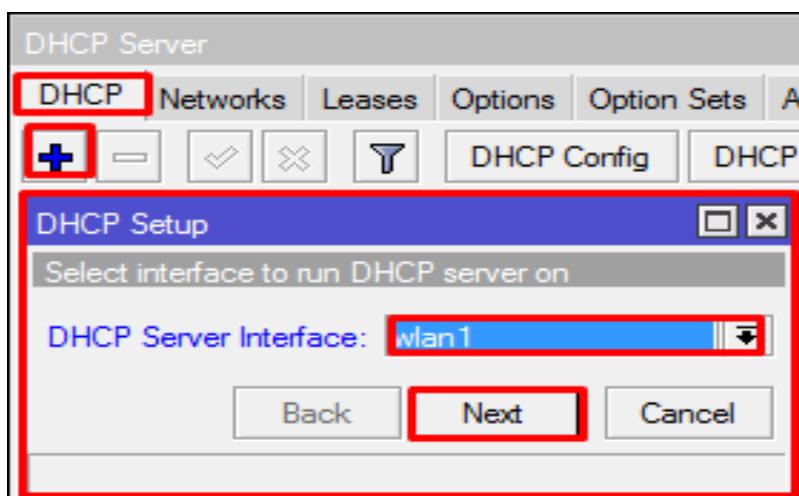
Selanjutnya Kita perlu membuat IP Address dan DHCP Server Untuk Wlan agar Client bisa mendapatkan IP Address Secara Otomatis...

- Buat Ip Address=192.168.10.1 ,Interface=Wlan 1



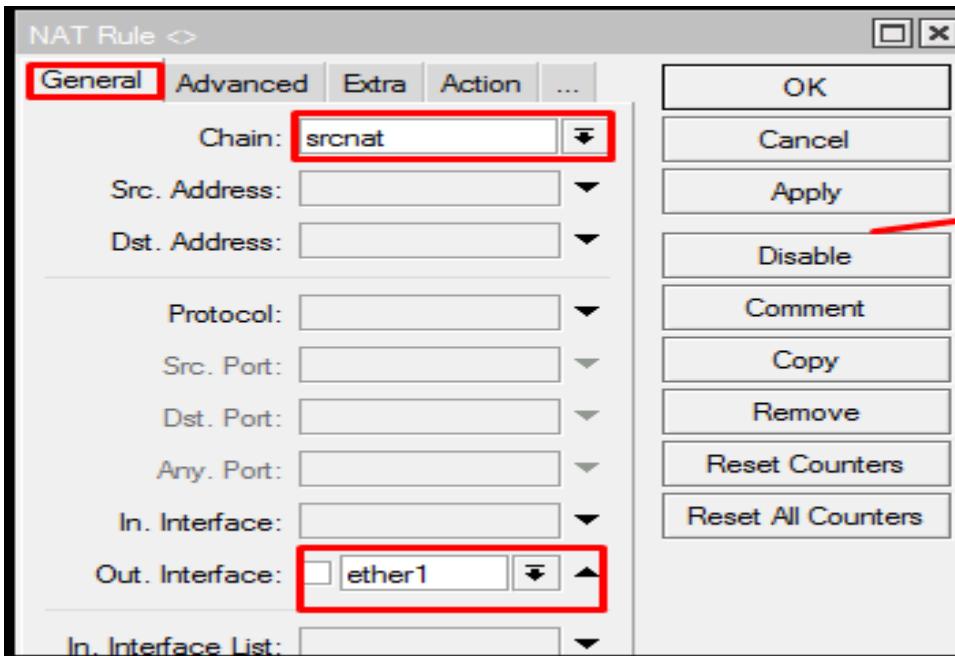
Lalu Buat DHCP Server Untuk Interface Wlan 1

- Klik IP > DHCP Server > Add (+)
- Isi Interface=Wlan 1 , Lalu Next Next saja..

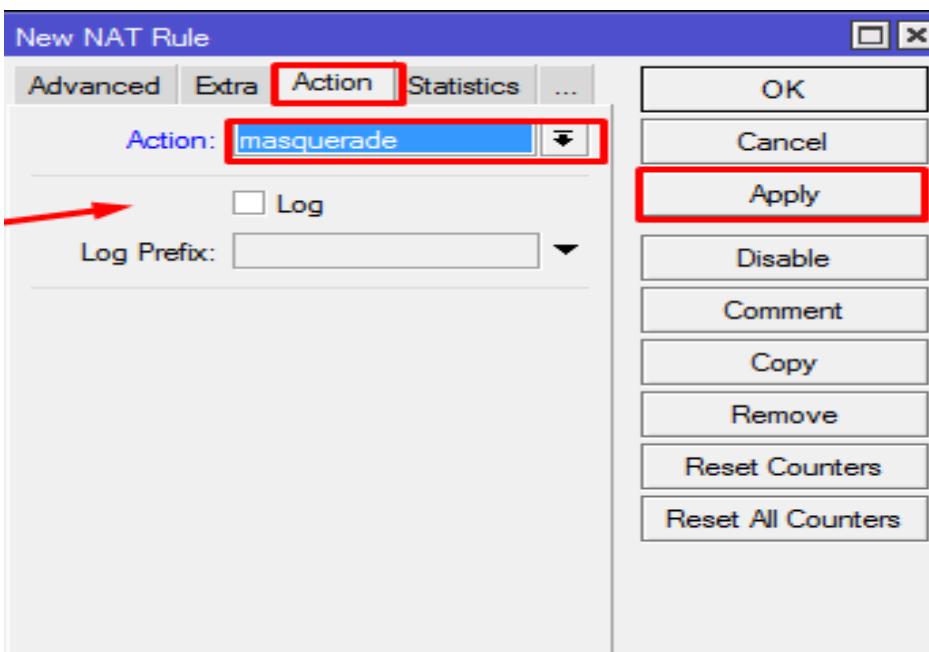


Selanjutnya Kita perlu Men-Setting NAT agar Client Bisa terhubung ke Internet

- Klik IP > Firewall > NAT > Add (+)
- Isi Chain=SrcNat ,Out.Interface=Ether1



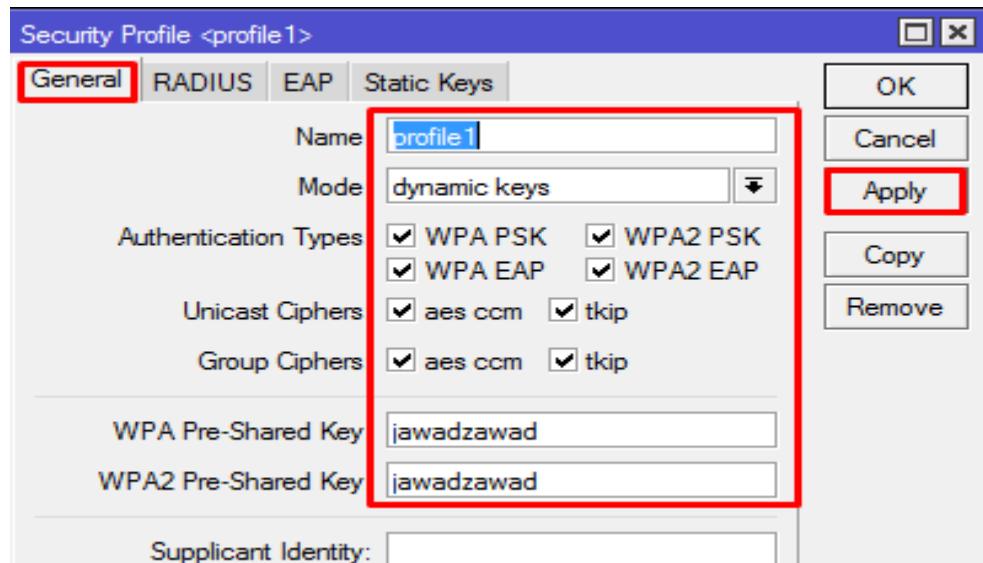
- Dan Isi Action=Masquerade
- Lalu Apply dan OK



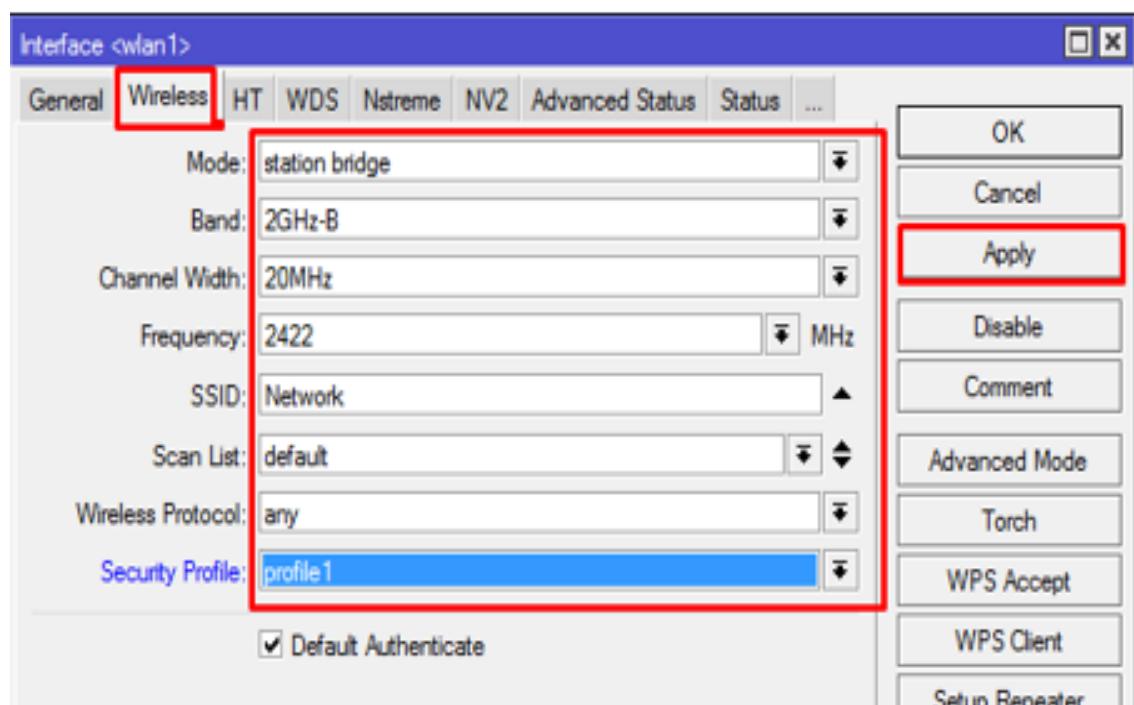
Jika Sudah melewati Step Ini maka Konfigurasi Di Access Point Sudah Selesai..

Selanjutnya kita Perlu mengkonfigurasi RouterBoard kanan yang di fungsikan sebagai Repeater..

- Buat Security Profile Sesuai dengan Password Access Point
- Lalu Apply dan OK



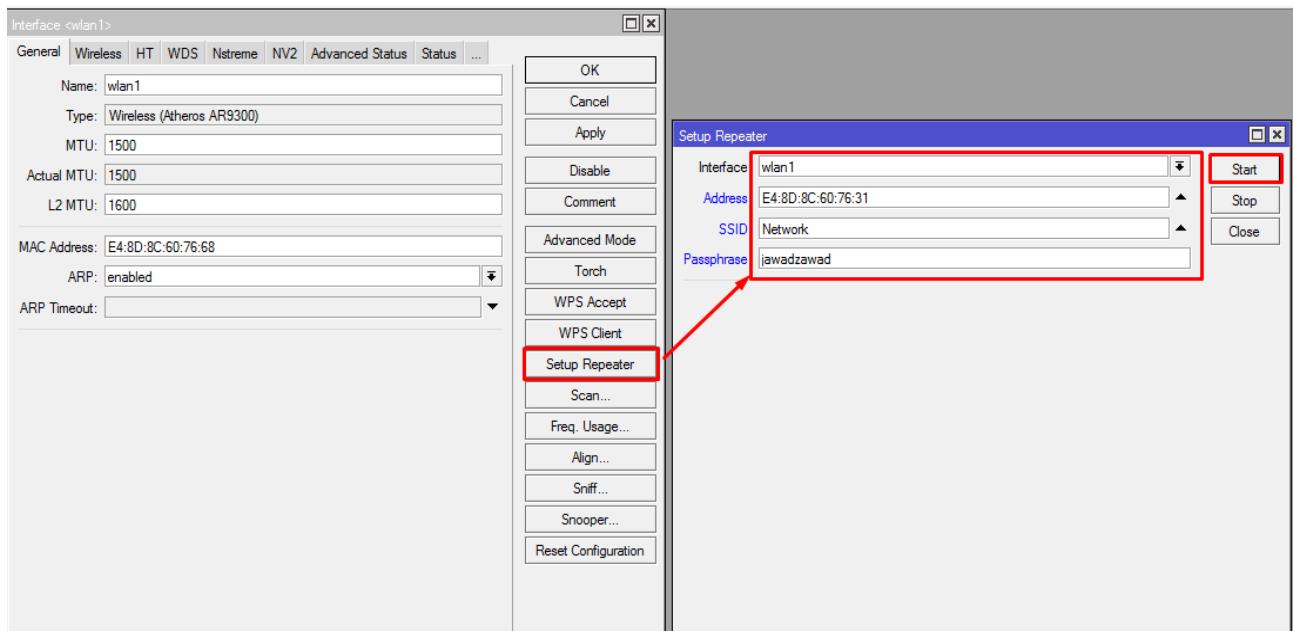
Selanjutnya Setting Interface Wireless Sebagai Station Bridge agar terhubung ke Access Point..



- Lalu Apply dan OK

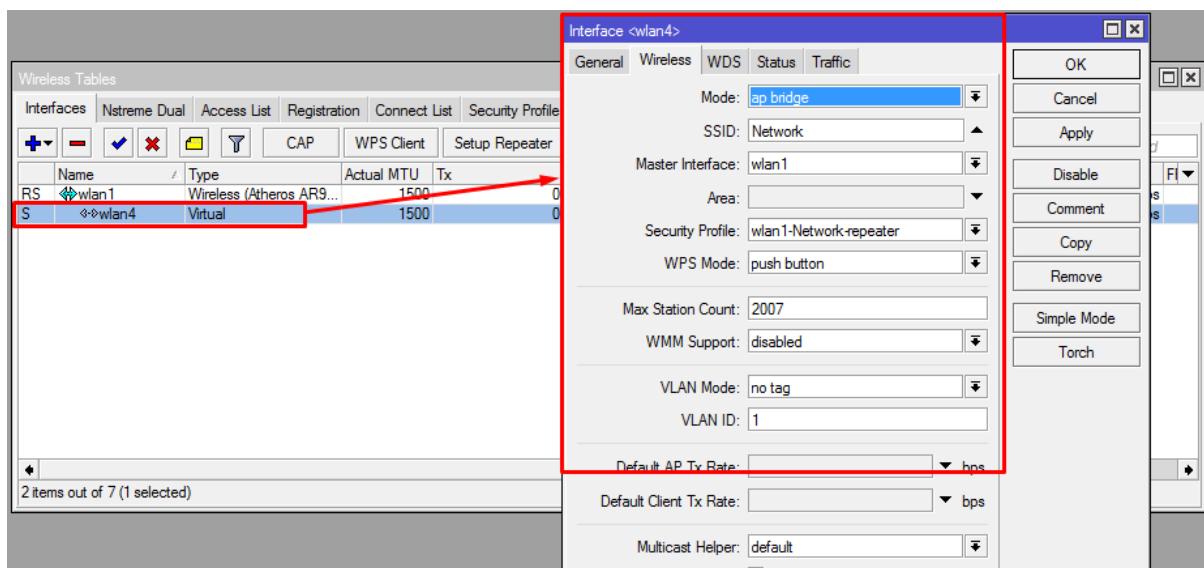
Selanjutnya Kita akan men-Setting Station sebagai Repeater...

- Klik Interface Wlan 1 > Setup Repeater
- Isi Interface=Wlan1 ,Isi Address=E4:8D:8C:60:76:31 (Mac-Address AP) ,SSID=Network (Sesuaikan) ,Passphrase=jawadzawad (Password AP)
- Lalu Klik Start

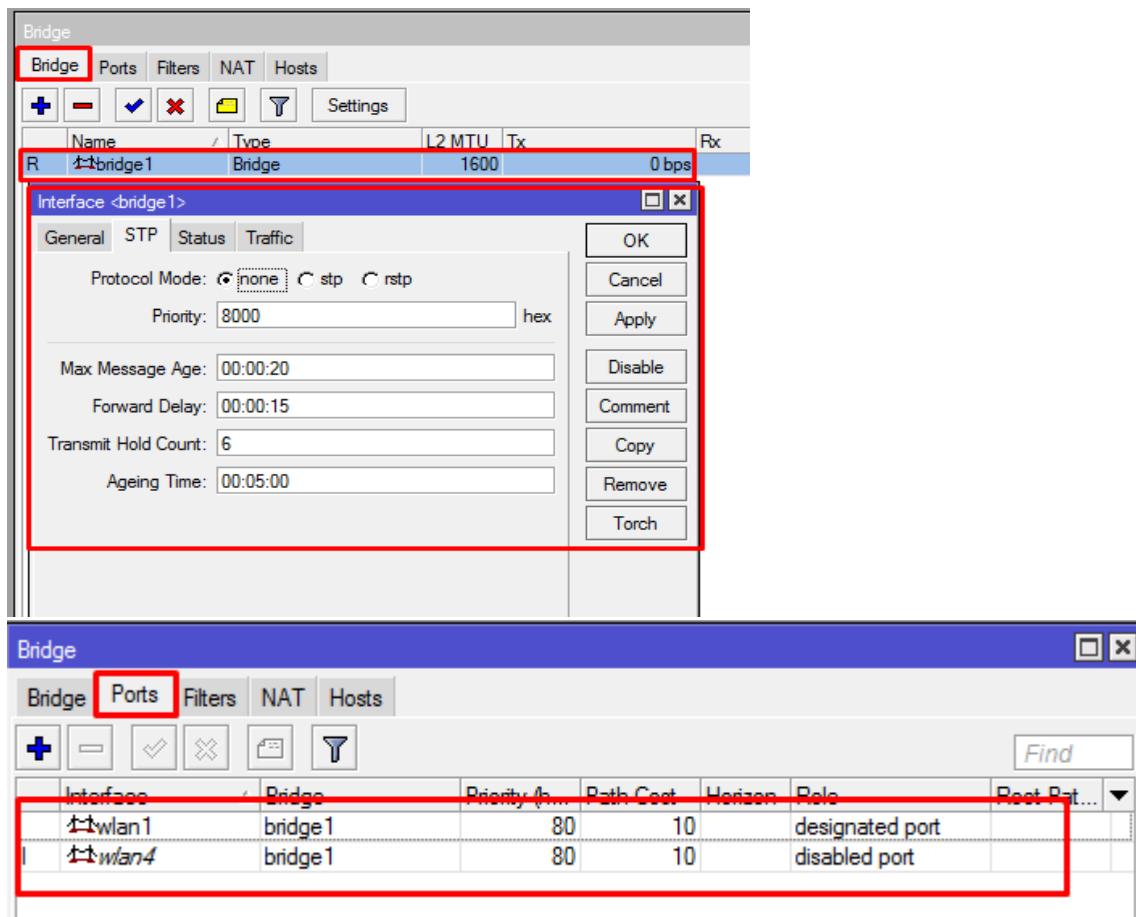


Jika sudah Melewati Step ini maka RouterBoard Kanan sudah menjadi Repeater... Nantinya di RouterBoard kanan akan terbentuk otomatis Virtual AP dan Bridge...

Virtual Access Point



Interface Bridge



Catatan=SSID dan Password Untuk Repeater bisa di ganti sesuai keinginan kita..

#Catatan:jika Access Point bukan menggunakan Mikrotik,maka Fitur ini tetap bisa di gunakan,yang perlu di perhatikan adalah saat memasukan Mac-Address Access Point ke Repeater..

Bab 3. Firewall

Fungsi Firewall

Firewall digunakan untuk membatasi akses antara dua jaringan yang saling terhubung, yaitu antara jaringan internal dengan jaringan global (internet). Firewall diletakkan diantara kedua jaringan internal dan global, sehingga semua informasi yang keluar maupun masuk harus melewati firewall. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain Alamat IP dari komputer sumber :

- Alamat IP dari komputer tujuan.
- Port TCP/UDP sumber dari sumber.
- Port TCP/UDP tujuan data pada komputer tujuan.
- Informasi dari header yang disimpan dalam paket data.

Tujuan utama firewall adalah menjaga agar akses internel maupun eksternal dari orang yang tidak berwenang atau tidak mempunyai akses. Firewall merupakan suatu cara yang efektif untuk melindungi jaringan dari ancamana gangguan lewat internet. Membatasi dan menjaga kerusakan pada satu bagian jaringan agar tidak menyebar ke bagian yang lain pada jaringan.

Manfaat Firewall

Berikut ini beberapa manfaat apabila dalam pemasangan jaringan menggunakan firewall :

- Seluruh akses dalam jaringan dapat kita kontrol melalui firewall.
- Dapat menjaga informasi rahasia berharga yang menyali keluar tanpa sepengetahuan.
- Dapat mengawasi semua service berjalan.
- Dapat mencatat dan merekam semua kegiatan berjalan melewatinya.
- Dapat menerapkan suatu kebijakan keamanan (Security Policy).
- Dapat mencegah suatu paket yang dirasa mencurigakan oleh sistem.
- Dapat menghambat pergerakan para penyerang yang mencoba memasuki sistem.

Cara Kerja Firewall

Komputer memiliki ribuan port yang dapat diakses untuk berbagai keperluan. Cara Kerja Firewall dari komputer adalah menutup port kecuali untuk beberapa port tertentu yang perlu tetap terbuka. Firewall di komputer bertindak sebagai garis pertahanan terdepan dalam mencegah semua jenis hacking ke dalam jaringan, karena, setiap hacker yang mencoba untuk menembus ke dalam jaringan komputer akan mencari port yang terbuka yang dapat diaksesnya.

Dalam Jaringan firewall terdapat dua buah cara yang dapat kita gunakan agar komunikasi jaringan dapat berjalan sesuai dengan fungsinya, yaitu menggunakan **packet filtering** dan **sistem proxy**, berikut penjelasnya.

- **Packet Filtering**

Packet filtering biasa juga disebut dengan screening router, yaitu suatu roter yang melakukan routing paket antara jaringan internal dan jaringan eksternal sesuai dengan kebijakan keamanan yang digunakan pada suatu jaringan. Dengan kata lain, packet filtering hanya dapat dipakai untuk menyaring paket-paket yang digunakan dengan paket-paket yang tidak digunakan dan mempunyai resiko keamanan yang lebih besar. Informasi yang digunakan untuk menyalin paket-paket antara lain alamat IP address asal dan tujuannya, Protokol yang digunakan (TCP, UDP, atau ICMP), dan alamat port asal dan tujuannya.

- **Sistem Proxy**

Proxy merupakan suatu program server atau aplikasi spesifik yang dijalankan pada mesin firewall. Setiap komunikasi yang terjadi antara dua buah jaringan dilakukan melalui suatu operator (Proxy Server). Firewall akan menggunakan kombinasi antara packet filtering dan sistem proxy, karena tidak semua kinerja protokol jaringan dapat berjalan secara maksimal sesuai dengan salah satu dari kedua teknik tersebut.

Proxy dalam melakukan tugasnya mengambil user request untuk internet service seperti HTTP, FTP dan meneruskannya pada host yang menjadi tujuannya. Dapat disimpulkan, proxy merupakan perantara antara jaringan internal dengan jaringan global (internet).

Cara Kerja Firewall Filter Rule

Prinsip IF....THEN....

- IF (jika) packet memenuhi syarat kriteria yang kita buat.
- THEN (maka) action apa yang akan dilakukan pada packet tersebut

IF (Jika)

The screenshot shows the 'New Firewall Rule' configuration window with several fields highlighted by a red border:

- Src. Address:** Source IP (IP client)
- Dst. Address:** Destination IP (IP internet)
- Protocol:** Protocol (TCP/UDP/ICMP, dll)
- Src. Port:** Source port (biasanya port dari client)
- Dst. Port:** Destination port (service port tujuan)
- Any. Port:**
- P2P:**
- In. Interface:** Interface (traffik masuk atau keluar)
- Out. Interface:**
- Packet Mark:**
- Connection Mark:**
- Routing Mark:**
- Routing Table:**
- Action:** Connection Type:

THEN (maka)

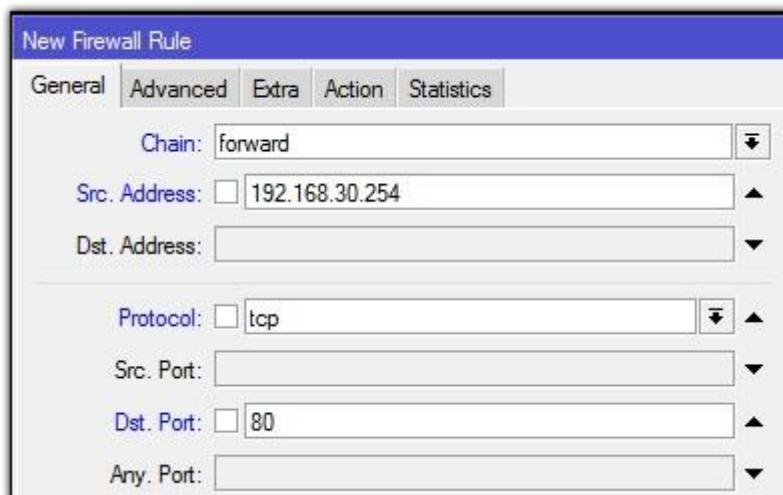
The screenshot shows the 'Action' dropdown menu with several options listed:

- accept** - accept the packet. Packet is not passed to next firewall rule.
- add-dst-to-address-list** - add destination address to [address list](#) specified by address-list parameter
- add-src-to-address-list** - add source address to [address list](#) specified by address-list parameter
- drop** - silently drop the packet
- fasttrack connection**
- jump**
- log**
- passthrough**
- reject**
- return**
- tarpit**

Selanjutnya saya akan Sedikit menjelaskan Parameter Parameter yang bisa kita gunakan di Firewall

Protokol dan Port

Penggunaan port dan protocol ini biasa di kombinasikan dengan IP address. Misalkan Anda ingin client tidak bisa browsing, namun masih bisa FTP, maka Anda bisa buat rule firewall yang melakukan blok di protocol TCP port 80. Ketika Anda klik tanda drop down pada bagian protocol, maka akan muncul opsi protocol apa saja yang akan kita filter. Parameter ini akan kita butuhkan ketika kita ingin melakukan blok terhadap aplikasi dimana aplikasi tersebut menggunakan protocol dan port yang spesifik.



Interface

Interface secara garis besar ada 2, input interface dan output interface. Cara menentukannya adalah dengan memperhatikan dari interface mana traffick tersebut masuk ke router, dan dari interface mana traffick tersebut keluar meninggalkan router. Misalkan Anda terkoneksi ke internet melalui router mikrotik, kemudian Anda ping ke www.mikrotik.co.id dari laptop Anda, maka input interface adalah interface yang terkoneksi ke laptop Anda, dan output interface adalah interface yang terkoneksi ke internet. Contoh penerapannya adalah ketika Anda ingin menjaga keamanan router, Anda tidak ingin router bisa diakses dari internet. Dari kasus tersebut Anda bisa lakukan filter terhadap koneksi yang masuk ke router dengan mengarahkan opsi in-interface pada interface yang terkoneksi ke internet .



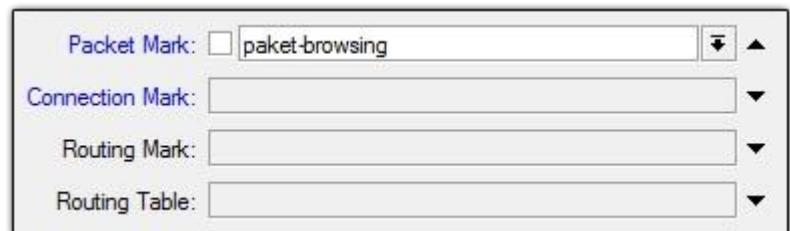
Parameter P2P

Sebenarnya ada cara yang cukup mudah dan simple untuk melakukan filtering terhadap traffick P2P seperti torrent atau edonkey. Jika sebelumnya Anda menggunakan banyak rule, Anda bisa sederhanakan dengan menentukan parameter P2P pada rule firewall filter. Jika Anda klik bagian drop down, akan muncul informasi program p2p yang dapat di filter oleh firewall.



Mangle

Kita biasanya membuat mangle untuk menandai paket/koneksi, kemudian kita gunakan untuk bandwidth management. Akan tetapi kita juga bisa membuat mangle untuk melakukan filtering. Firewall filter tidak dapat melakukan penandaan pada paket atau koneksi, akan tetapi kita bisa kombinasikan mangle dan firewall filter. Pertama, kita tandai terlebih dahulu paket atau koneksi dengan mangle, kemudian kita definisikan di firewall filter dan fitur yang lainnya.



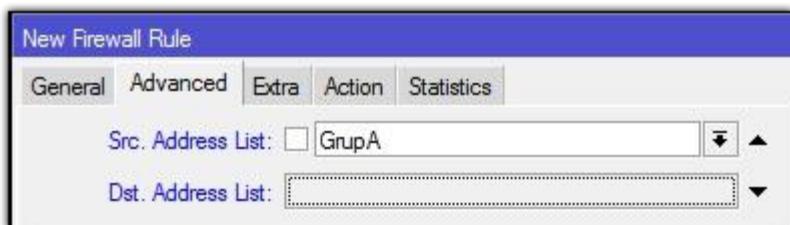
ConnectionState

Jika Anda tidak ingin ada paket - paket invalid lalu lalang di jaringan Anda, Anda juga bisa melakukan filtering dengan mendefinisikan parameter connection state. Paket invalid merupakan paket yang tidak memiliki koneksi dan tidak berguna sehingga hanya akan membebani resource jaringan. Kita bisa melakukan drop terhadap paket - paket ini dengan mendefinisikan parameter connection state.



Address List

Ada saat dimana kita ingin melakukan filtering terhadap beberapa ip yang tidak berurutan atau acak. Apabila kita buat rule satu per satu, tentu akan menjadi hal yang melelahkan. Dengan kondisi seperti ini, kita bisa menerapkan grouping IP membuat "address list". Pertama, buat daftar ip di address list, kemudian terapkan di filter rule Anda. Opsi untuk menambahkan parameter "Address List" di firewall ada di tab Advanced. Ada 2 tipe address list, "Src. Address List" dan "Dst. Address List. Src Address List adalah daftar sumber ip yang melakukan koneksi, Dst Address List adalah ip tujuan yang hendak diakses.



Layer 7 Protocol

Jika Anda familiar dengan regexp, Anda juga bisa menerapkan filtering pada layer7 menggunakan firewall filter. Di mikrotik, penambahan regexp bisa dilakukan di menu Layer 7 Protocol. Setelah Anda menambahkan regexp, Anda bisa melakukan filtering dengan mendefinisikan Layer 7 Protocol pada rule filter yang Anda buat. Perlu diketahui bahwa penggunaan regexp, akan membutuhkan resource CPU yang lebih tinggi dari rule biasa.



Content

Saat kita hendak melakukan blok terhadap website, salah satu langkah yang cukup mudah untuk melakukan hal tersebut adalah dengan melakukan filter berdasarkan content. Content merupakan string yang tertampil di halaman website. Dengan begitu, website yang memiliki string yang kita isikan di content akan terfilter oleh firewall. Misalkan kita ingin block www.facebook.com maka cukup isi parameter content dengan string "facebook" dan action drop, maka website facebook baik HTTP maupun HTTPS tidak dapat diakses.

Content: facebook

Mac address

Ketika kita melakukan filter by ip address, terkadang ada user yang nakal dengan mengganti ip address. Untuk mengatasi kenakalan ini, kita bisa menerapkan filtering by mac-address. Kita catat informasi mac address yang digunakan user tersebut, kemudian kita tambahkan parameter Src. Mac Address di rule firewall kita. Dengan begitu selama user tersebut masih menggunakan device yang sama, dia tetap ter-filter walaupun berganti ip.

Src. MAC Address: D0:DF:9A:01:36:D4

Time

Salah satu solusi alternatif selain kita harus repot membuat scheduler dan script, kita bisa memanfaatkan fitur time di firewall filter. Fitur ini akan menentukan kapan rule firewall tersebut dijalankan. Bukan hanya untuk menentukan jam saja, fitur ini juga bisa digunakan untuk menentukan hari apa saja rule tersebut berjalan. Misalkan kita ingin melakukan block facebook di jam kerja, maka kita bisa buat rule firewall yang melakukan block facebook yang dijalankan dari jam 08:00 sampai jam 16:00 selain hari Sabtu dan Minggu. Sebelum anda membuat rule firewall dengan parameter "time", pastikan Anda sudah set NTP di router Anda agar waktu router sesuai dengan waktu real.

Time
Time: 08:00:00 - 16:00:00
 sun mon tue wed thu fri sat

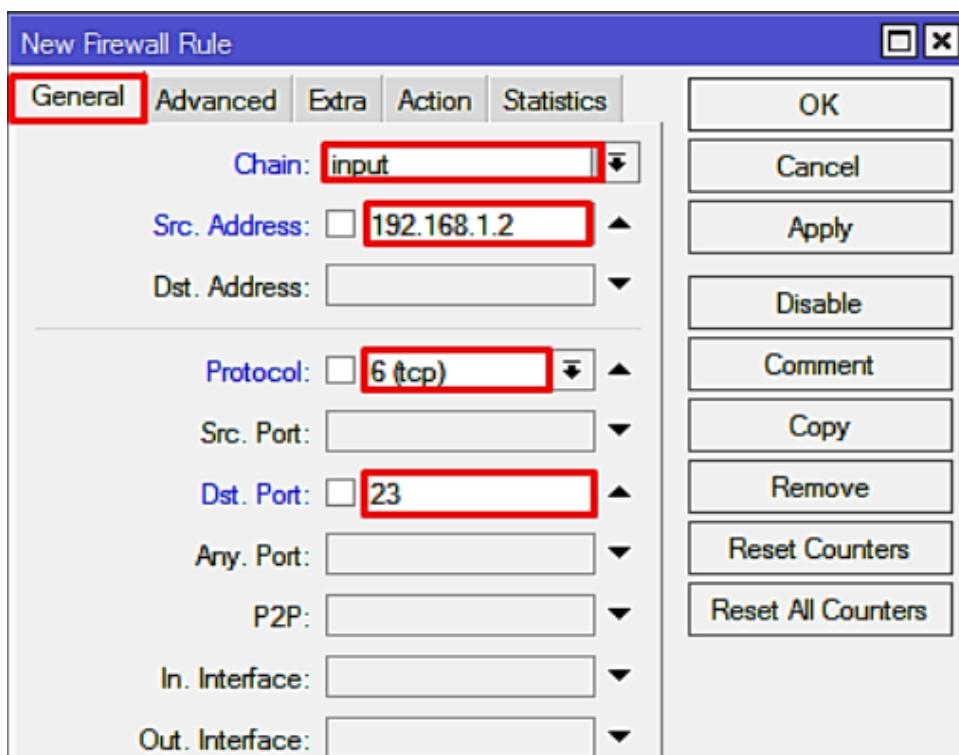
Saat Anda membuat rule firewall, usahakan untuk membuat rule yang spesifik. Semakin spesifik rule yang kita buat, maka semakin optimal pula rule tersebut akan berjalan.

Lab 22. Melindungi Router Dengan Filter Rule

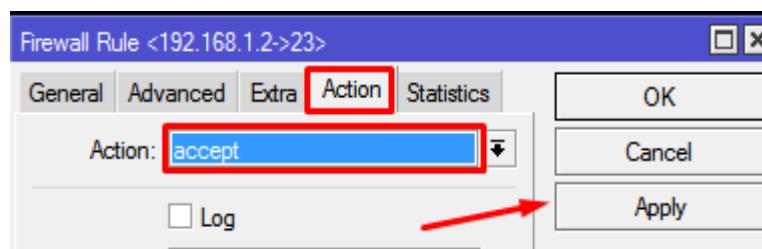
Di lab ini kita akan membahas bagaimana cara melindungi Router dengan Filter Rule, fungsi Filter rule di sini adalah Membuat izin akses masuk ke Router, di lab ini kita akan mencoba membuat Rule agar IP 192.168.1.2 bisa melalakukan akses telnet ke router dan selain IP 192.168.1.2 tidak bisa akses telnet ke router

Pertama kita akan mencoba cara Accept few and Drop Any, yang artinya Terima beberapa dan Tolak Semua..

- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Input ,Src.Address=192.168.1.2 (IP PC) ,Protocol=TCP ,Dst.Port=23 (Port Telnet)



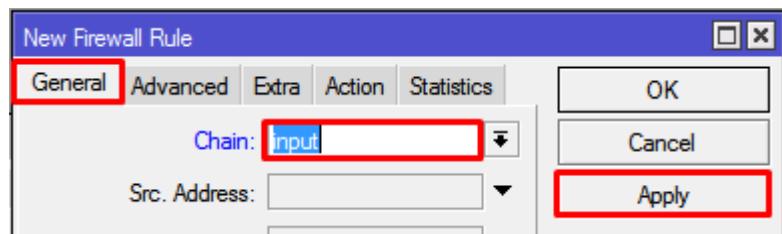
- Dan Pilih Action=Accept
- Lalu Apply dan OK



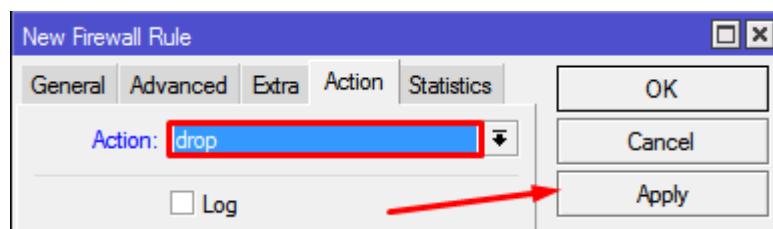
Jika Kita sudah Membuat Rule seperti itu maka Artinya "Jika ada yang masuk dengan IP 192.168.1.2 menggunakan Protocol TCP port 23 di perbolehkan"

Selanjutnya adalah membuat Rule untuk menolak semua akses yang masuk ke router...

- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Input



- Dan isi action=Drop
- Lalu Apply dan OK



Rule

Firewall									
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols	
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	(▼)
::: special dummy rule to show fasttrack counters									
0	D	pas...	forward						
1	✓ acc...	input	192.168.1.2		6 (tcp)		23		
2	✗ drop	input							

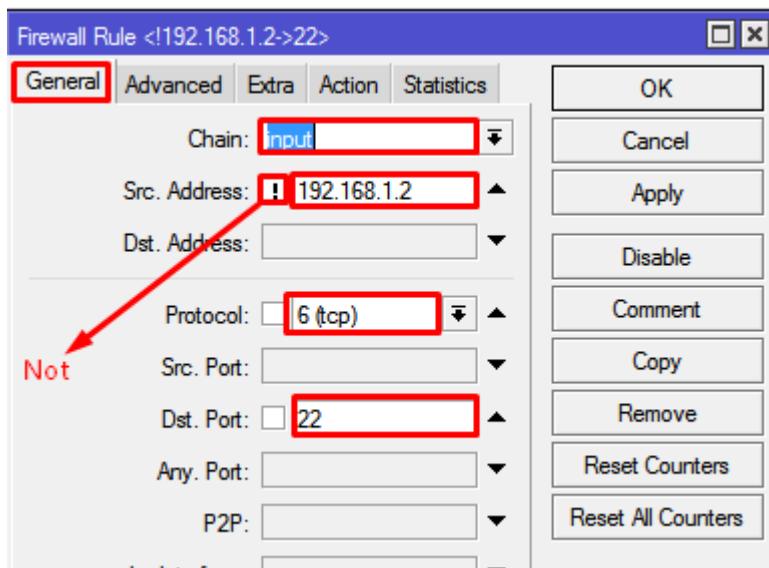
Untuk pengetesan coba setting IP PC=192.168.1.2 jika kita menggunakan Ip tersebut maka kita tetap bisa meng-akses telnet ke Router,Tetapi jika kita menggunakan IP lain maka kita tidak bisa meng-Akses Router lewat telnet..

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420\telnet 192.168.1.1
Connecting To 192.168.1.1...Could not open connection to the host, on port 23: Connect failed
```

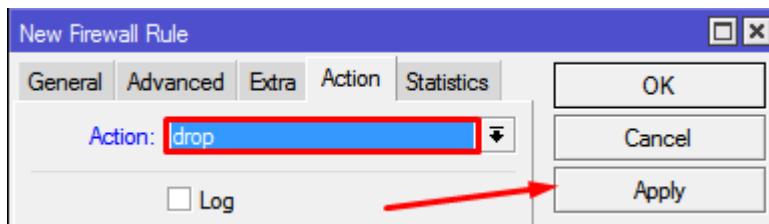
Ada cara yang lebih mudah dari Accept few and Drop any.....

- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Input ,Src.Adreess=(Not)192.168.1.2 (IP PC) ,Protocol=TCP ,Dst.Port=23 (Port Telnet)



Kita harus meng-Klik fitur Not (■)

- Dan isi action=Drop
- Lalu Apply dan OK



Jika sudah membuat Rule tersebut maka artinya "jika ada yang masuk selain IP 192.168.1.2 maka akan di tolak"

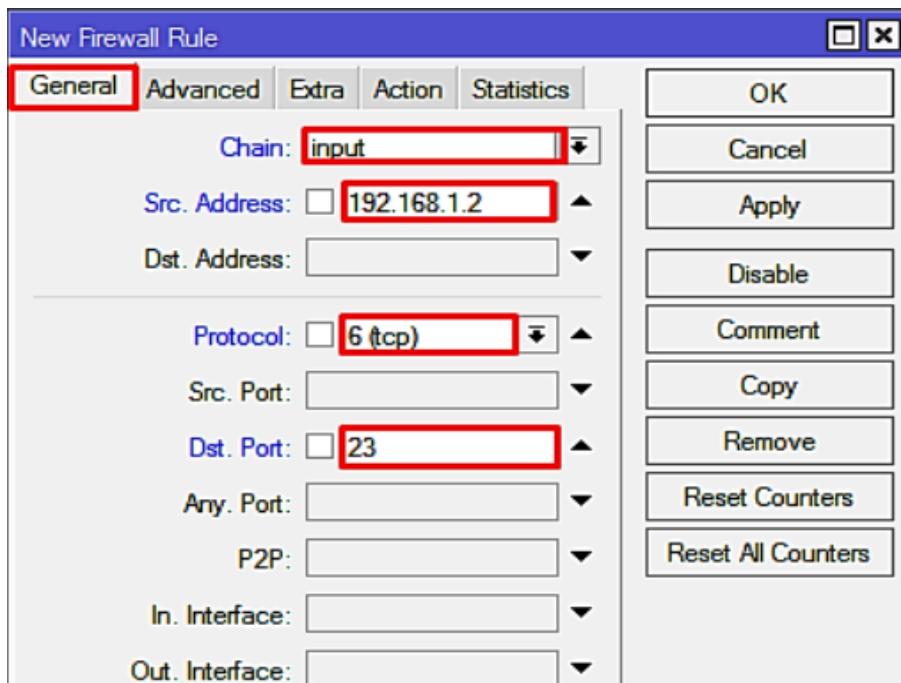
Nah itu adalah cara mudah nya untuk membatasi akses telnet ke router...

Lab 23. Firewall Logging

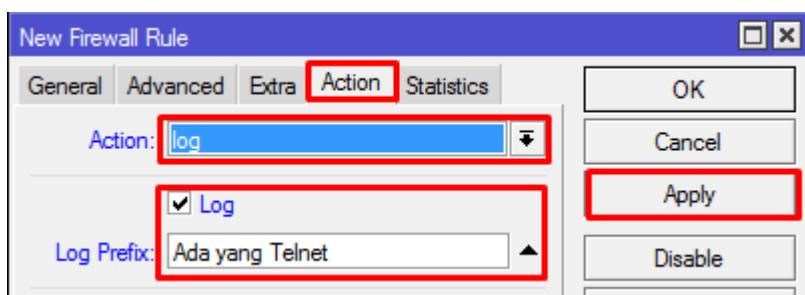
Fungsi dari Firewall Logging adalah mencatat kegiatan yang masuk,keluar dan melewati router sesuai kebutuhan,Hasil dari dari Firewall Logging bisa di lihat di menu Log

Di sini kita akan mencoba mencatat aktivitas Telnet yang masuk Ke router..

- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Input ,Src.Adreess=192.168.1.2 (IP PC) ,Protocol=TCP ,Dst.Port=23 (Port Telnet)

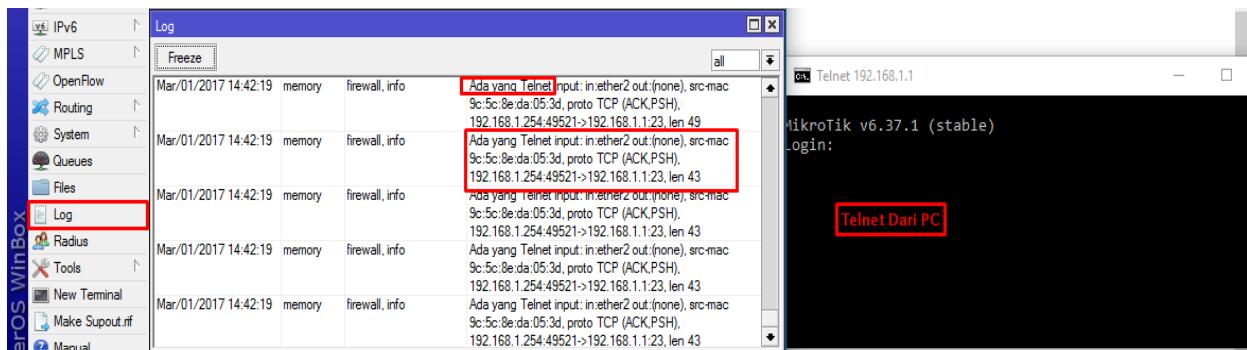


- Isi Action LOG dan checklist LOG ,isi LOG=Ada yang Telnet (Keterangan)
- Lalu Apply dan OK



Untuk Pengecekan Coba kita melakukan Akses Telnet ke router..

Maka aktivitas Telnet kita akan tercatat di Router.



Lab 24. Blok situs dengan Filter Rule

Di lab ini kita akan memulai Mem-Blok Situs,pertama kita akan mencoba mem-Blok situs menggunakan Filter Rule...untuk Mem-Blokir suatu situs menggunakan Filter Rule Kita perlu tau Ip address website yang ingin di Blokir.....

Di lab ini kita akan mencoba mem-Blokir website 1cak.com..

Pertama kita perlu mengetahui IP address dari Website 1cak.com..

- Masuk CMD dan masukan Perintah "nslookup 1cak.com"

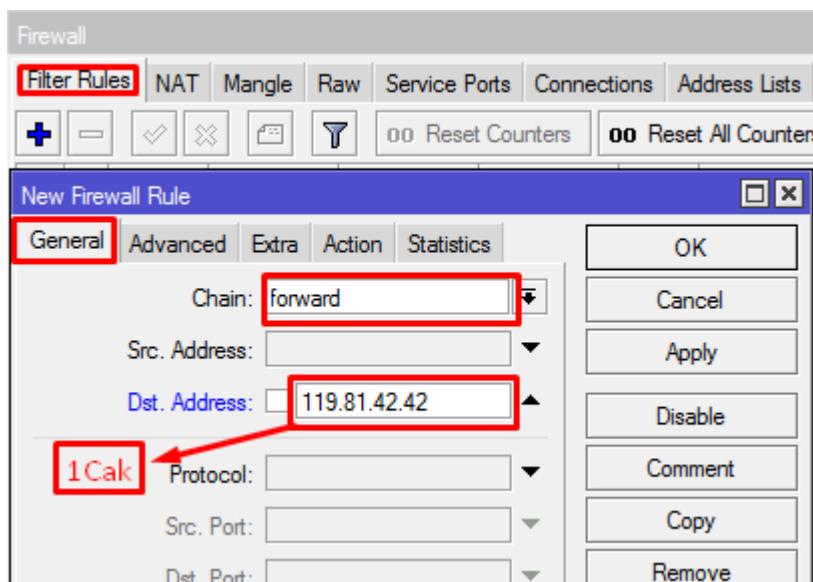
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420>nslookup 1cak.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

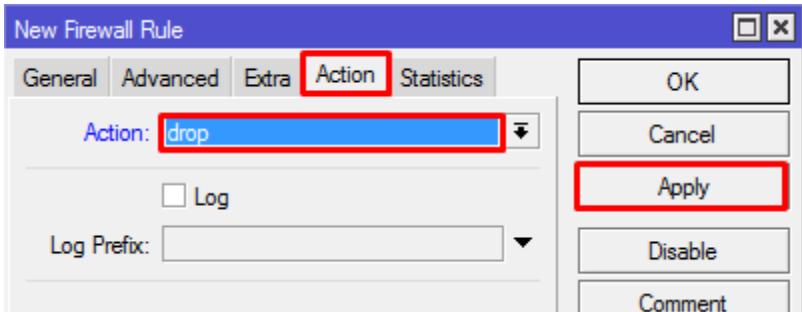
Non-authoritative answer:
Name: 1cak.com
Address: 119.81.42.42
```

Jika sudah mendapatkan IP address yang di gunakan 1cak.com,selanjutnya kita buat Rule untuk mem-Blokir website tersebut...

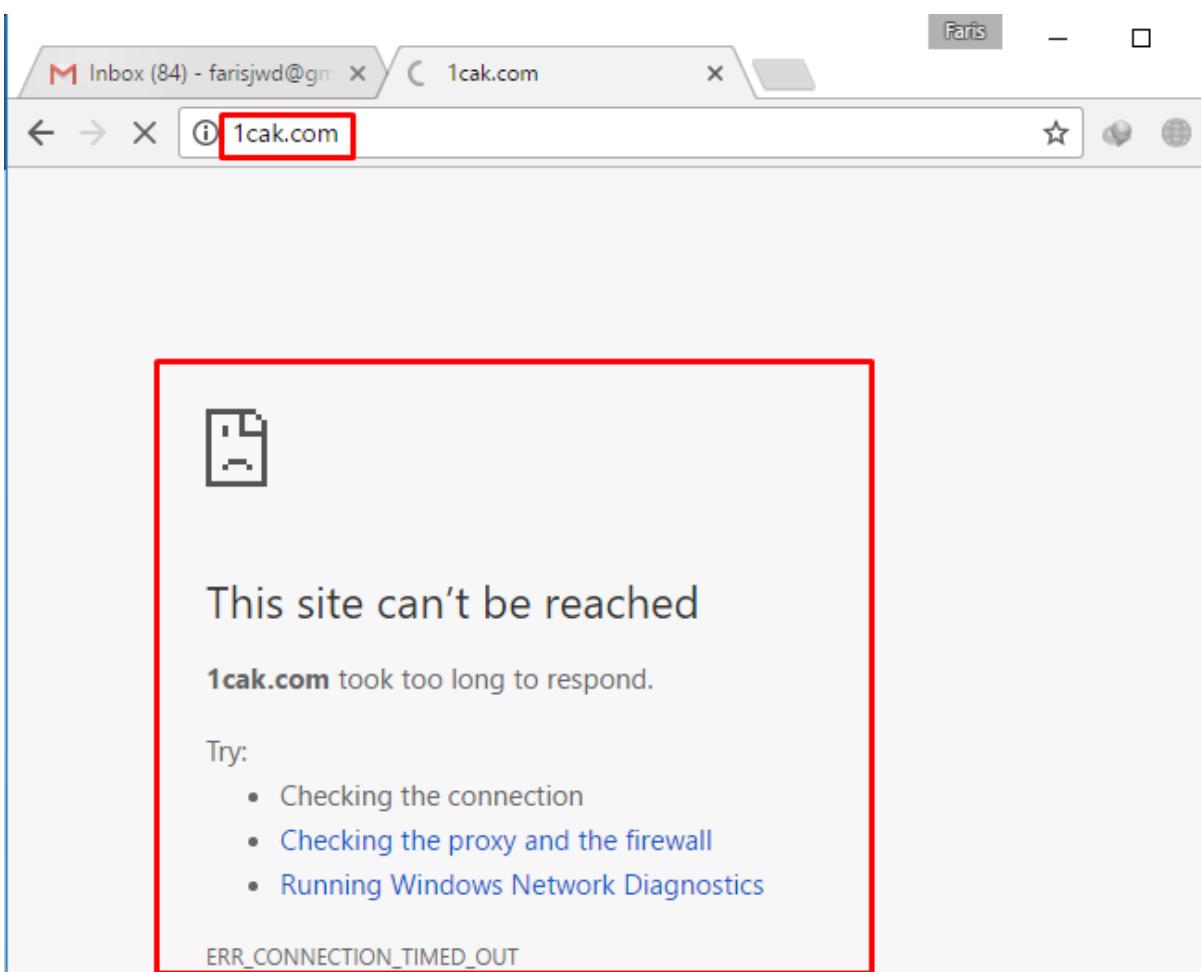
- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Forward ,Dst.Address= 119.81.42.42 (IP 1cak.com)



- Isi action=Drop
- Lalu Apply dan OK



Jika sudah melalukan Step tersebut maka 1cak.com tidak bisa di akses lagi..untuk vertifikasi coba kunjungi website 1cak.com



Eror ☺

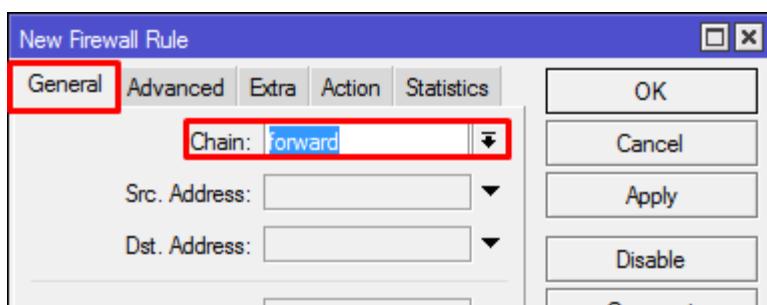
Lab 25. Blok Konten dalam MikroTik

Jika pada lab sebelumnya kita mem-Blokir menggunakan IP address Website (Dst.Address) maka di lab ini kita akan mencoba memblokir situs menggunakan Konten,konsep memblokir website menggunakan Konten adalah memblokir Webiste yang mengandung Konten tersebut,Contoh kita memblokir facebook,maka jika ada website yang menggunakan/mencantumkan Facebook pun akan ikut terblokir oleh Firewall...

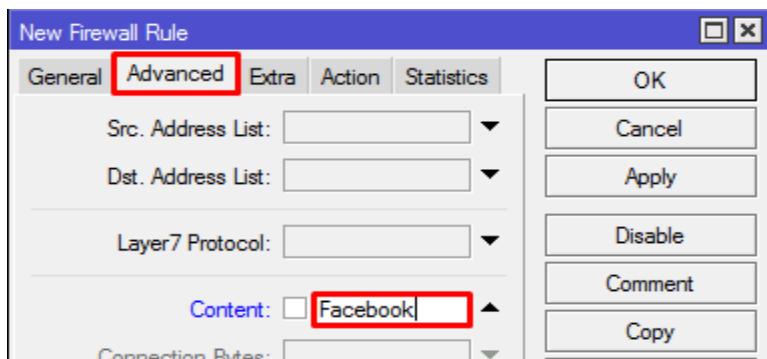
Di lab ini kita akan mencoba Memblokir Facebook,Instagram dan Youtube..

Pertama kita buat Rule Firewall untuk memblokir Konten Facebook

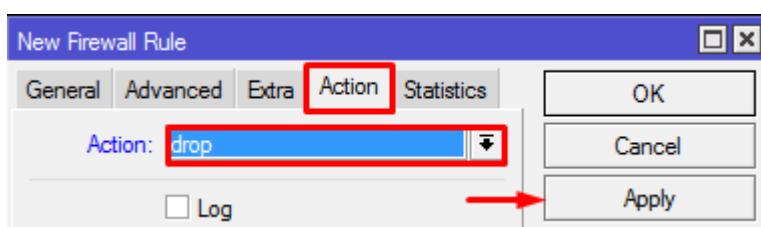
- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain=Forward



- Isi content=Facebook



Dan Action nya Drop



Buat Rule untuk Konten Youtube dan Instagram,cara sama seperti membuat Rule untuk facebook, bedanya hanya mengganti Konten dengan Instagram dan Youtube..



Jika sudah membuat semua Rule maka akan jadi seperti gambar di bawah ini..

#		Action:	Chain:	forward	Log:	Rate:
0	D	::: special dummy rule to show fasttrack counters				
		Action: passthrough	Chain: Packets:	0	Rate: 0 bps	
		Bytes: 0 B				
		Packet Rate: 0				
1		Action: drop	Chain: forward		Content: facebook	
		Log: no	Bytes: 9.7 kB		Packets: 58	
		Rate: 0 bps	Packet Rate: 0			
2		Action: drop	Chain: forward		Content: instagram	
		Log: no	Bytes: 1414 B		Packets: 21	
		Rate: 0 bps	Packet Rate: 0			
3		Action: drop	Chain: forward		Content: youtube	
		Log: no	Bytes: 427 B		Packets: 7	
		Rate: 0 bps	Packet Rate: 0			

4 items

Coba Kunjungi Web Facebook,Instagram dan Youtube..

The screenshot shows a web browser with three tabs open:

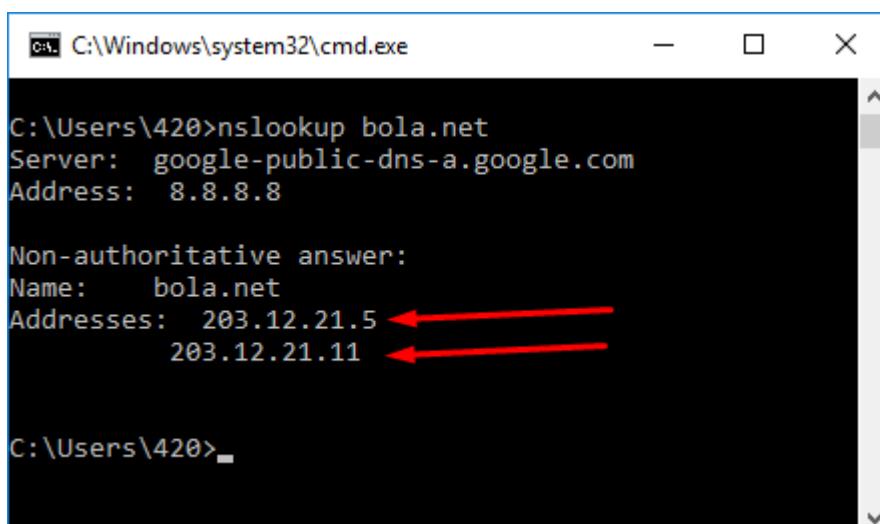
- Tab 1: www.facebook.com - Error message: "This site can't be reached" and "www.facebook.com's server DNS address could not be found. Try running Windows Network Diagnostics."
- Tab 2: www.instagram.com - Error message: "This site can't be reached" and "www.instagram.com's server DNS address could not be found. Try running Windows Network Diagnostics." A red arrow points to this tab.
- Tab 3: www.youtube.com - Error message: "This site can't be reached" and "www.youtube.com's server DNS address could not be found. Try running Windows Network Diagnostics."

Below the browser, there is a summary message: "This site can't be reached" and "www.youtube.com's server DNS address could not be found. Try running Windows Network Diagnostics."

Lab 26. Blok Situs dengan Address List

Jika pada lab sebelumnya kita mencoba mem-Blokir situs menggunakan Content, di lab ini kita akan mencoba mem-Blokir situs menggunakan Address List. Apa Fungsi dari Address List? Address list berfungsi untuk mengelompokan Banyak IP/Domain ke dalam satu Kelompok, address list akan digunakan untuk mem-Blokir suatu situs ketika situs tersebut menggunakan banyak IP address (Lebih dari satu), jika kita mem-Blokir suatu website yang menggunakan banyak IP Address dengan Filter Rule maka kita akan membuat banyak Rule dan itu Ribet... berbeda jika kita mem-Blokir suatu website yang menggunakan banyak IP Address dengan Address List, Kita hanya perlu membuat satu address list dan 1 Rule Firewall... di lab ini kita akan mencoba memblokir website bola.net..

Pertama kita lihat ip address yang digunakan Website bola.net



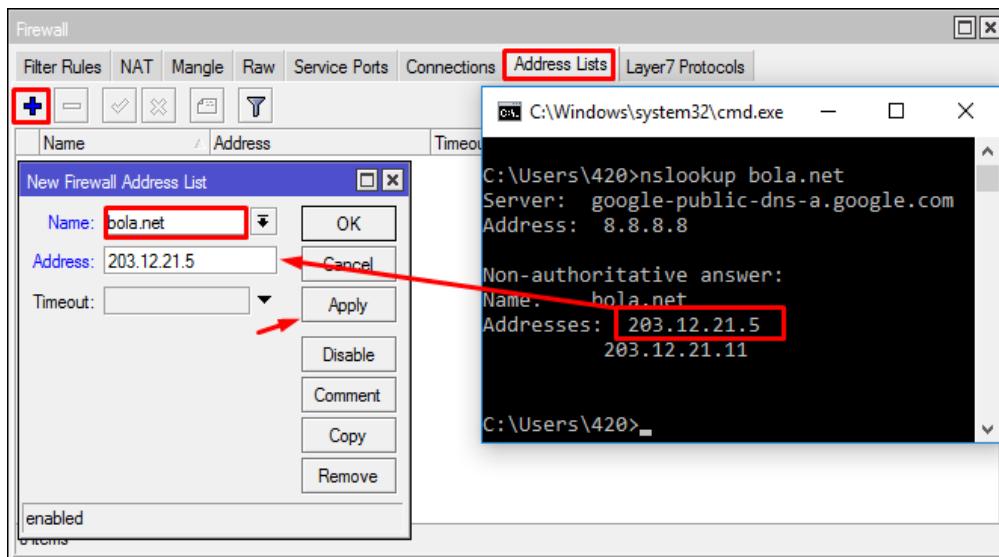
```
C:\Windows\system32\cmd.exe
C:\Users\420>nslookup bola.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: bola.net
Addresses: 203.12.21.5
          203.12.21.11

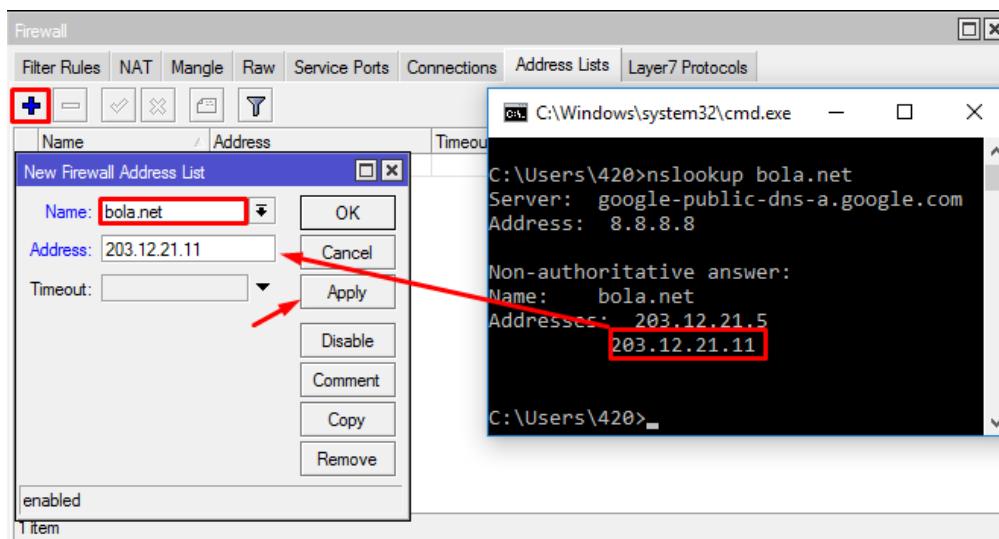
C:\Users\420>
```

Website bola.net memakai 2 IP Address.. Setelah kita mengetahui IP Address yang digunakan oleh website bola.net kita perlu membuat address list untuk website tersebut..

- Klik IP > Firewall > Address List > Add(+)
- Isi Nama=Bola.net (Bebas)
- Masukan salah satu IP yang digunakan Website Bola.net
- Lalu Apply dan OK



Ulangi cara di atas dan masukan IP address kedua yang di gunakan Bola.net



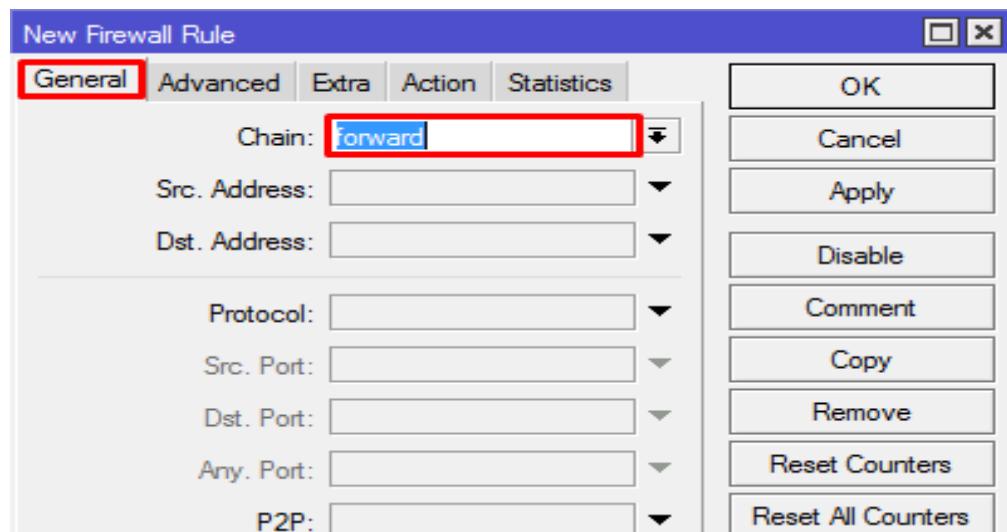
Step selanjutnya adalah membuat Filter rule dan memasukan Address list ke Filter rule tersebut...

Address List Bola.net

Name	Address	Timeout
bola.net	203.12.21.5	
bola.net	203.12.21.11	

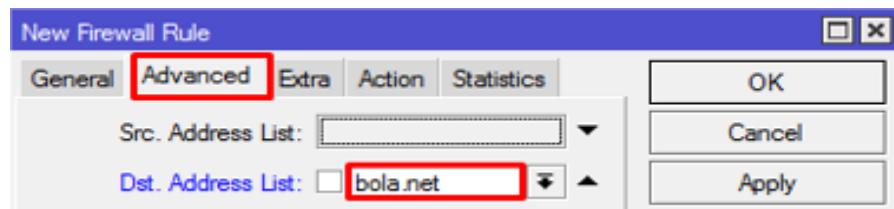
Masuk Ke Menu Filter Rule terlebih dahulu..

- Klik IP > Firewall > Filter Rule > Add (+)
- Klik General dan isi Chain=Forward



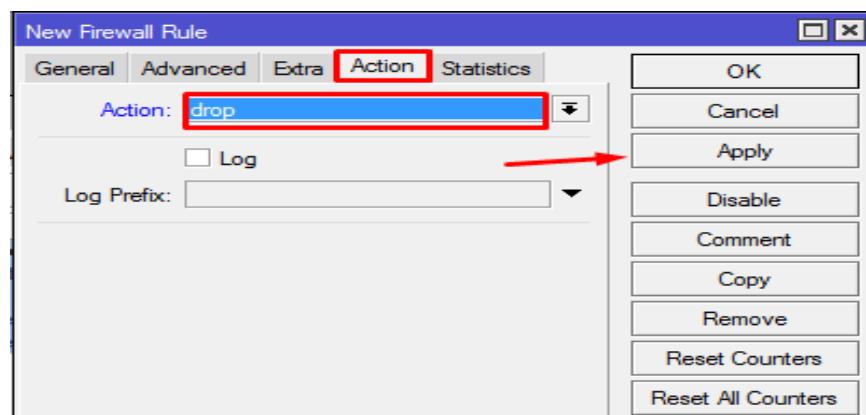
Selanjutnya isi kita masukan Address list ke Filter Rule...

- Klik Advance > Isi Dst.Address List=Bola.net



Selanjutnya adalah memilih action=Drop untuk filter rule tersebut

- Klik Action > Isi Action=Drop
- Lalu Apply dan OK



Setelah step ini maka Website Bola.net sudah terblokir...☺

Untuk Src.Address/Client yang ingin di blokir bisa di isi dengan IP Network,IP Range /Kita bisa menggunakan Fitur Not (!),Isi Src.Address sesuai Kebutuhan kita...

Address list juga bisa kita gunakan untuk memblokir beberapa Website sekaligus..Contoh saya akan mencoba memblokir beberapa situs belanja Online=Mataharimall.com,OLX.co.id,Tokopedia.com...

Peratama kita cari IP address yang di gunakan oleh ketiga website tersebut...

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420>nslookup mataharimall.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: mataharimall.com
Address: 139.255.59.18 ←

C:\Users\420>nslookup olx.co.id
Server: google-public-dns-a.google.com
Address: 8.8.8.8

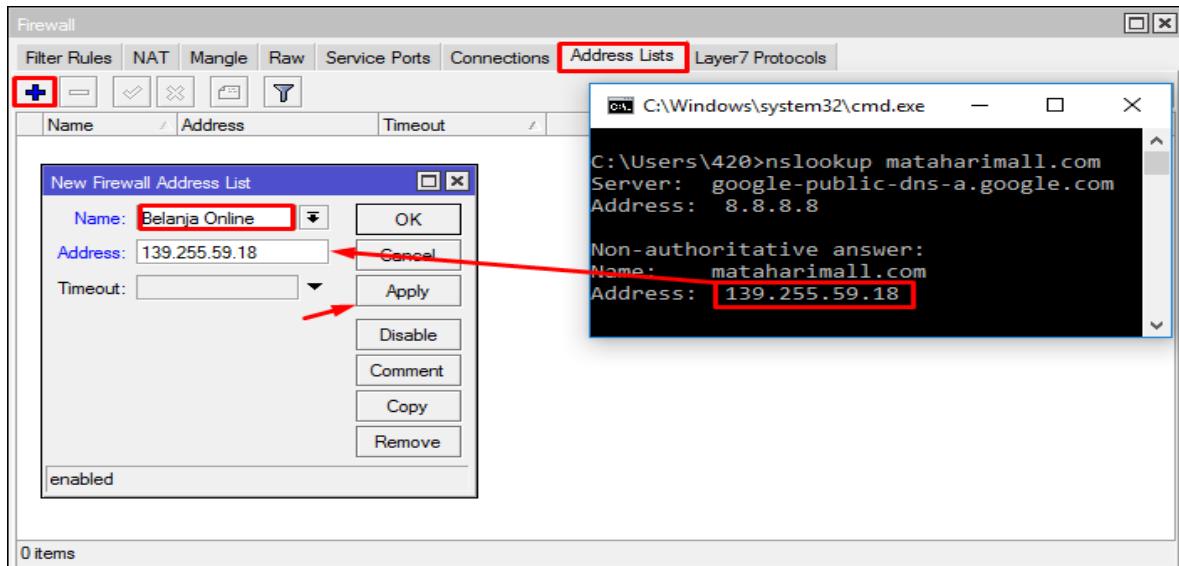
Non-authoritative answer:
Name: olx.co.id
Addresses: 210.210.179.84 ←
           210.210.179.94 ←
           210.210.179.104 ←

C:\Users\420>nslookup tokopedia.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: tokopedia.com
Addresses: 182.253.224.184 ←
           182.253.224.188 ←
```

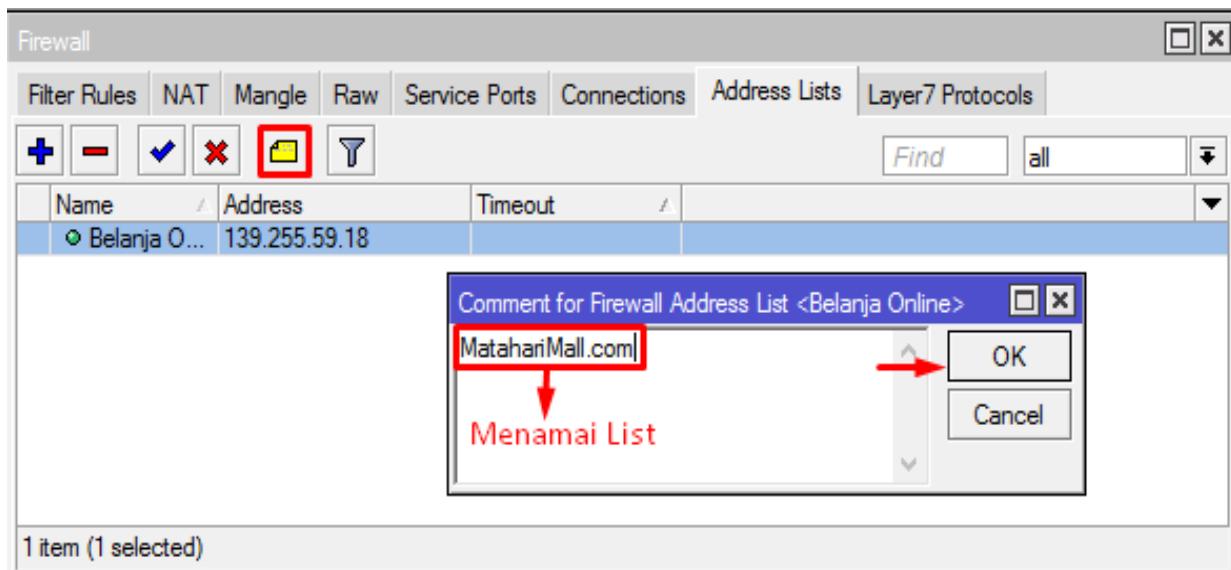
Website Mataharimall menggunakan 1 IP address, OLX.co.id menggunakan 3 IP Address ,dan Tokopedia.com menggunakan 2 IP Address....

Selanjutnya kita hanya perlu mengelompokan ke-Enam IP tersebut ke dalam 1 Address List yang di beri nama Belanja Online....



Lakukan Berulang kali dan Masukan IP Address yang di gunakan OLX.co.id dan Tokopedia.com ke dalam Address List=Belanja Online...

Jika sudah Memasukan Semua IP Address ke Address List=Belanja Online kita perlu Memberi Comment di List yang telah kita buat yang berfungsi untuk menamai/menandai mana IP Address Mataharimall dan yang mana IP Address OLX.co.id,



Jika kita memberi Comment di setiap List maka Hasil nya akan Seperti Ini

Name	Address	Timeout
::: MatahariMall.com		
• Belanja Online	139.255.59.18	
::: OLX.co.id		
• Belanja Online	210.210.179.84	
::: OLX.co.id		
• Belanja Online	210.210.179.94	
::: OLX.co.id		
• Belanja Online	210.210.179.104	
::: Tokopedia.com		
• Belanja Online	182.253.224.184	
::: Tokopedia.com		
• Belanja Online	182.253.224.188	

Jika sudah membuat address list, selanjutnya kita akan membuat Filter Rule dan memasukan Address list ke Filter Rule...

- Filter Rule > Add (+)
- Isi Chain=Forward

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

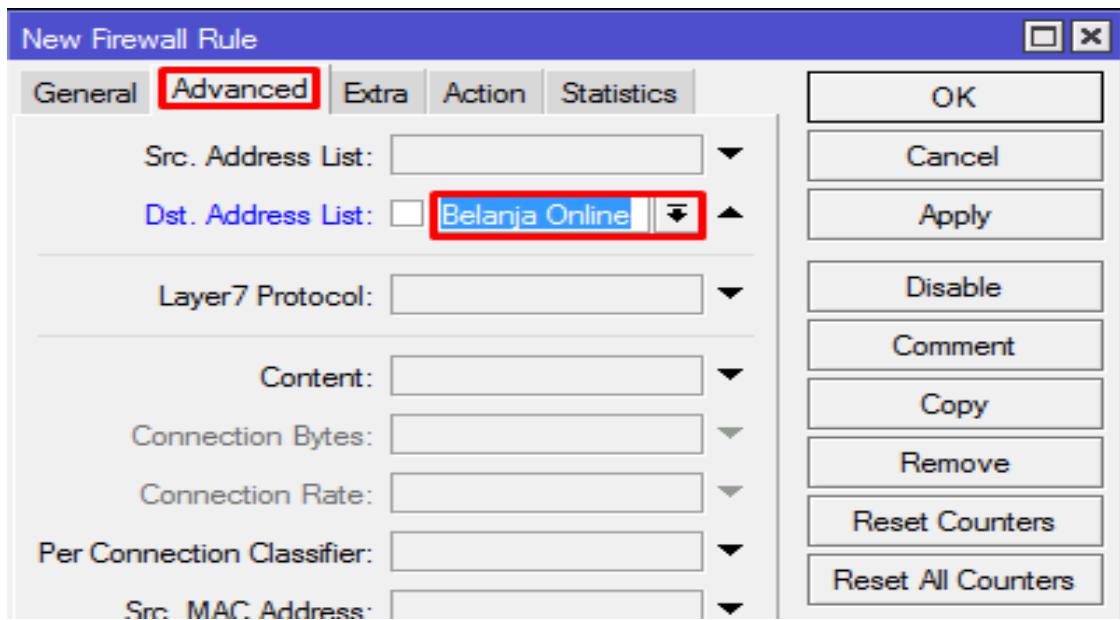
Dst. Port:

Any. Port:

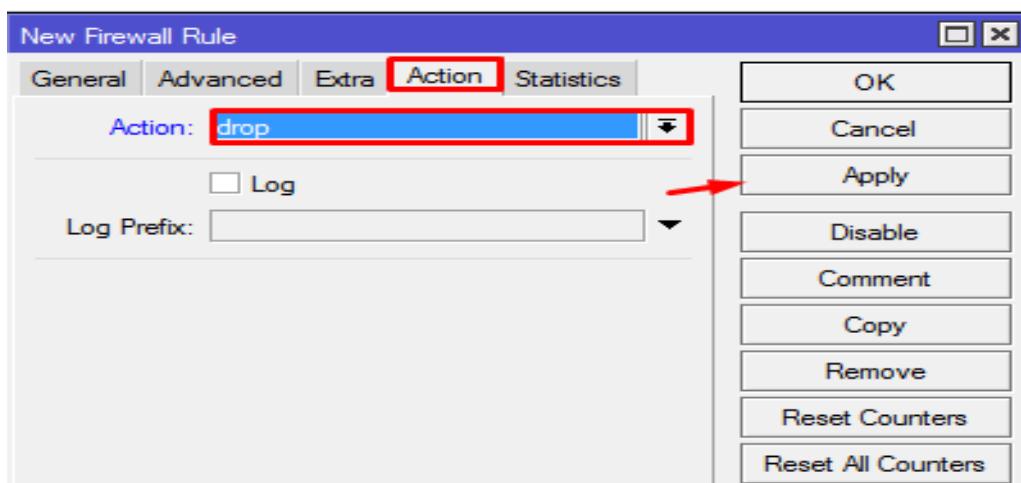
P2P:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

- Dan Isi Dst.Address List=Belanja Online



- Dan isi Action=Drop
- Lalu Apply dan OK



Firewall					
		Filter Rules	NAT	Mangle	Raw
		Service Ports	Connections	Address Lists	Layer7 Protocols
		Reset Counters	Reset All Counters	<input type="button" value="Find"/>	<input type="text" value="all"/>
#					
0	D	...; special dummy rule to show fasttrack counters			
	Action:	passthrough	Chain:	forward	
	Log:	no	Bytes:	0 B	
	Packets:	0	Rate:	0 bps	
	Packet Rate:	0			
1		Action: drop	Chain: forward		
	Dst. Address List:	Belanja Online	Log: no		
	Bytes:	3344 B	Packets: 66		
	Rate:	0 bps	Packet Rate: 0		

Coba test masuk ke 3 Webiste tersebut.. maka hasil nya akan Eror 😊

Lab 27. Blok Situs dengan Layer 7 Protocol

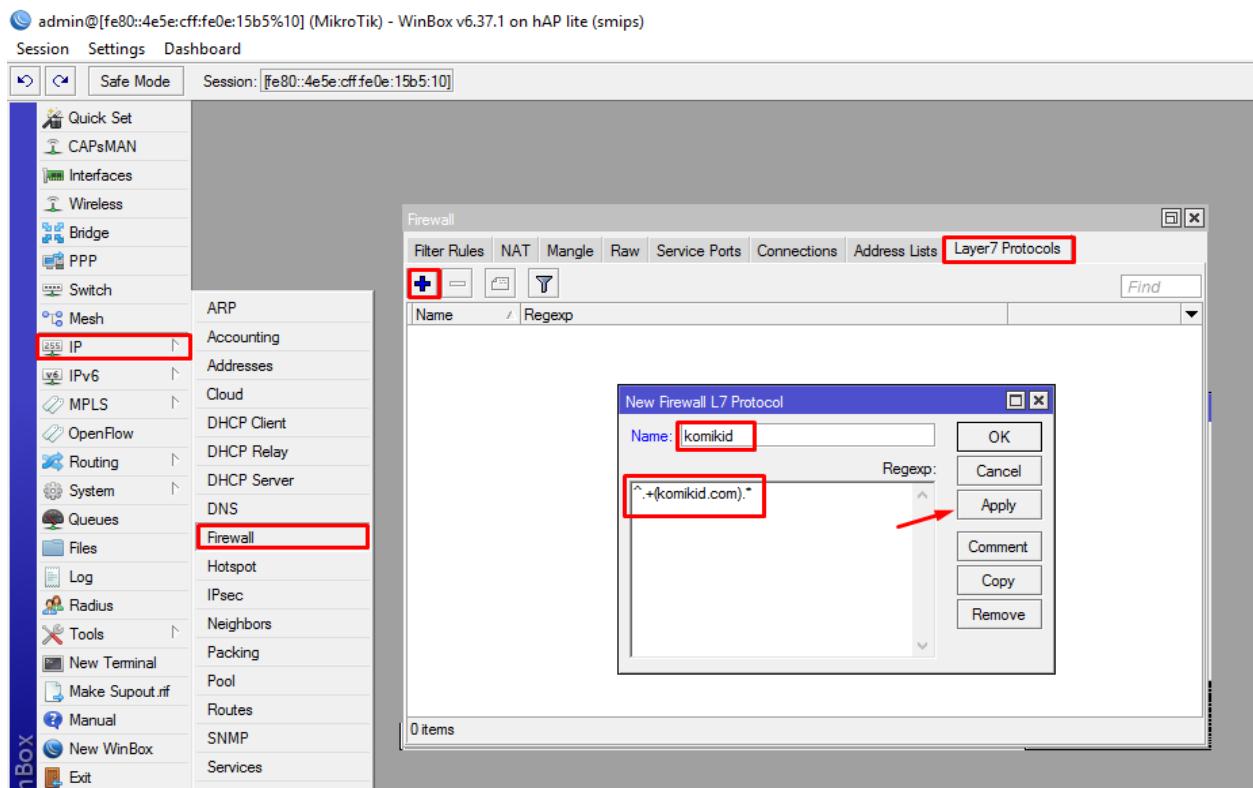
Protokol Layer7 adalah metode untuk mencari pola dalam ICMP/TCP/UDP stream, atau istilah lainnya regexp pattern. Dengan Layer 7 Protocol IP Packet akan di periksa secara detail.

Cara kerja L7 adalah mencocokkan (mathcer) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/pattern data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, matcher tidak memeriksa lebih lanjut. Dan akan dianggap unknown connections. Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada Resource RouterBoard maupun PC Router anda. Untuk menghindari hal tersebut, maka tambahkan regular firewall matchers (pattern) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

Layer 7 matcher harus melihat kedua arah lalu lintas (masuk dan keluar). Untuk memenuhi persyaratan ini rule L7 harus diatur dalam chain Forward. Jika rule pada chain input/prerouting, maka aturan yang sama juga harus diatur dalam chain output/postrouting, jika tidak, maka data mungkin dianggap tidak lengkap sehingga pola/pattern dianggap tidak benar/cocok. Layer 7 Protocol Bekerja dengan Menggunakan Regexp.

Di Lab ini kita akan mencoba mem-Blokir situs www.Komikid.com dengan Layer 7 Protocol...

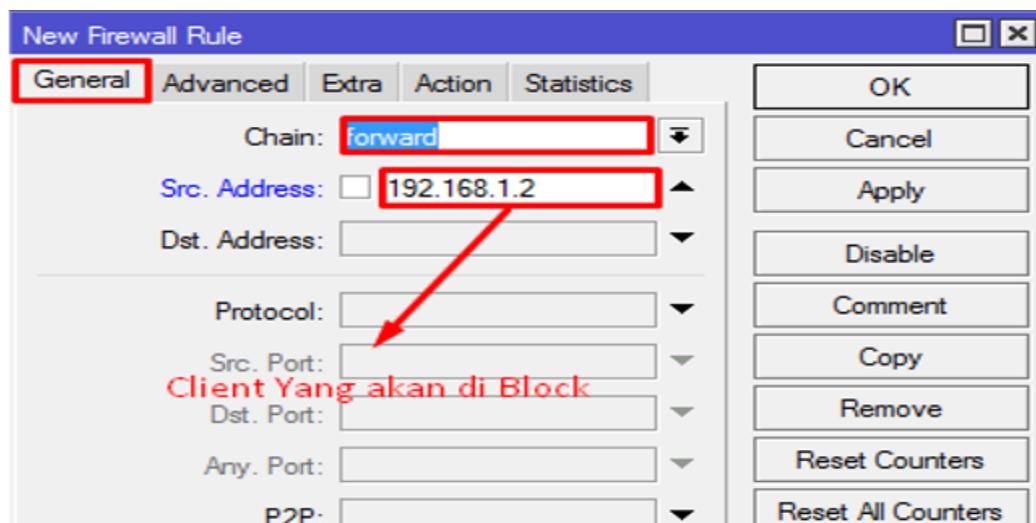
- Klik IP > Firewall > Layer 7 Protocol > Add
- Isi name=Komikid dan Isi Regexp ^.+**(komikid.com)**.*
- Lalu Apply dan OK



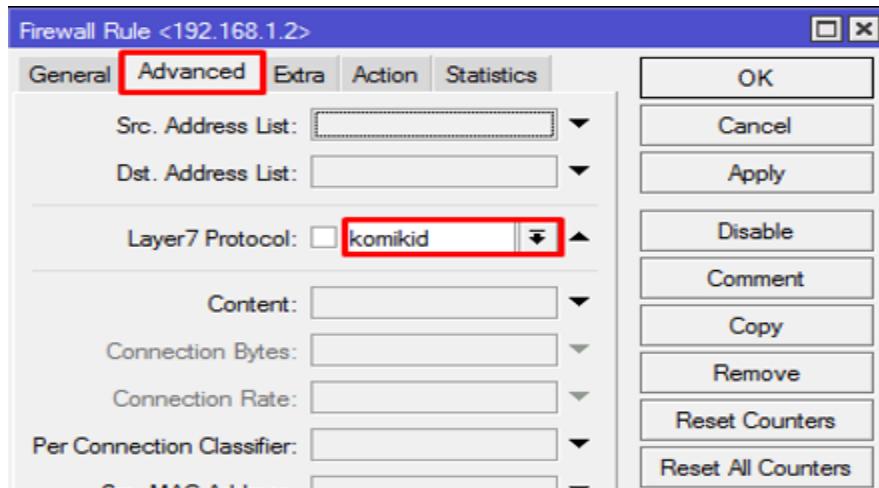
Regexp Adalah suatu Script yang di gunakan di Layer 7 Protocol untuk Mem-Blokir suatu situs...

Setelah membuat Rule layer 7 Protocol kita perlu membuat Filter Rule dan memasukan layer 7 Protocol ke Filter Rule Tersebut ...

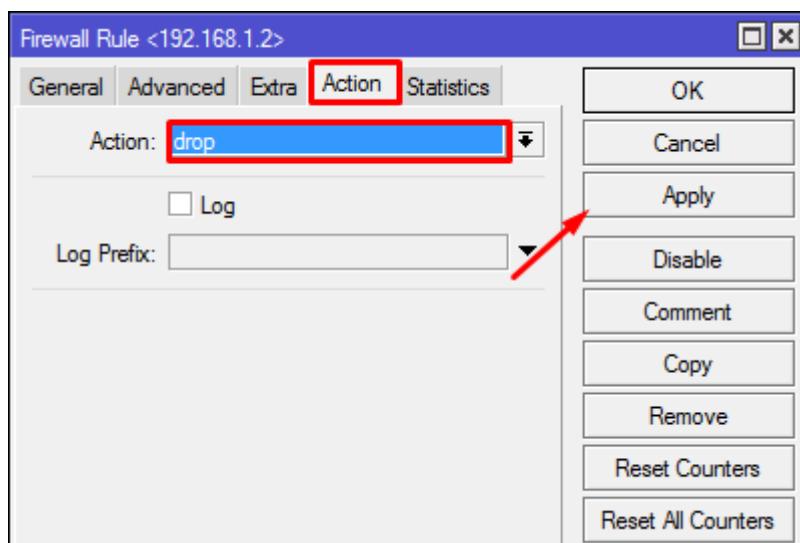
- Klik IP > Firewall > Filter Rule > Add (+)
- Isi Chain Forward dan Isi Src.Address=192.168.1.2 (Client)



- Klik Advanced > Isi Layer7 Protocol=Komikid



- Klik Action > Pilih Action=Drop
- Lalu Apply dan OK



Jika Step Ini sudah selesai maka Website www.Komikid.com sudah Ter-Blokir

Lab 28. Connection Traking & State MikrotikOS

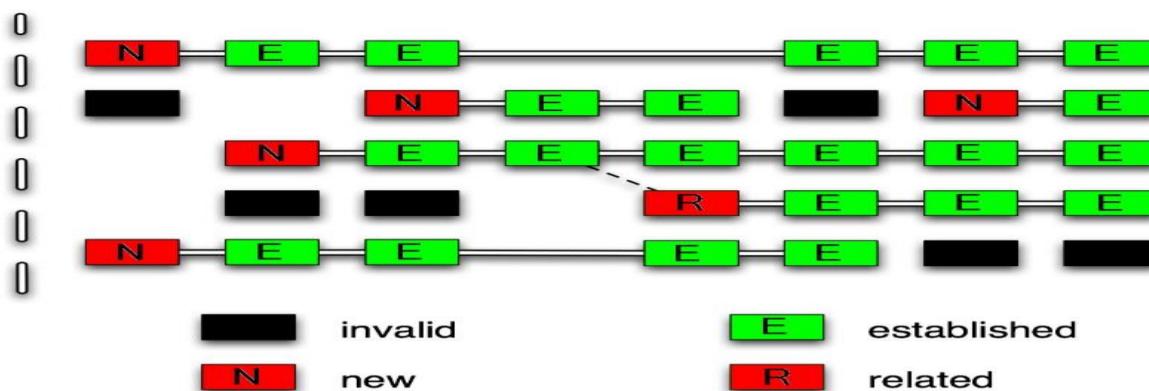
Dalam firewall, ada yang disebut dengan Connection Tracking yang merupakan fitur baru di dalam firewall yang ditambahkan sejak kernel 2.4.x. Kemampuan dari connection tracking adalah untuk menyimpan dan menjaga informasi koneksi seperti koneksi baru atau koneksi yang sudah ada yang disertai dengan jenis protokol, alamat IP asal dan alamat IP tujuan. Dengan menggunakan fitur ini, para administrator dapat menolak atau mengijinkan berbagai macam koneksi. Connection tracking mempunyai beberapa keadaan: Dalam mikrotik, bisa dilihat di Menu: Ip > Firewall > Connections

Firewall								
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols
		Tracking						
Src. Address	/	Dst. Address	Proto	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C 0.0.0.0:5678		255.255.255.255:5678	17 (u...)		00:00:03	0 bps/0 bps	465 B/0 B	
C 192.168.1.1:41386		255.255.255.255:5678	17 (u...)		00:00:01	0 bps/0 bps	152 B/0 B	
C 192.168.10.1:51424		255.255.255.255:5678	17 (u...)		00:00:03	0 bps/0 bps	450 B/0 B	
SCs 192.168.10.254		8.8.8.8	1 (ic...)		00:00:09	960 bps/960 bps	18.8 kB/18.5 kB	
C 192.168.10.254:5678		255.255.255.255:5678	17 (u...)		00:00:01	0 bps/0 bps	96 B/0 B	
SACs 192.168.10.254:49154		216.58.203.242:443	6 (tcp)		23:59:57 established	0 bps/0 bps	3864 B/6.1 kB	
SACs 192.168.10.254:49155		74.125.68.181:443	6 (tcp)		23:59:21 established	0 bps/0 bps	2652 B/5.3 kB	
SACs 192.168.10.254:49164		172.217.24.110:443	6 (tcp)		23:59:52 established	0 bps/0 bps	31.3 kB/584.9 kB	
SACs 192.168.10.254:49178		54.194.99.187:443	6 (tcp)		23:59:34 established	0 bps/0 bps	82 B/80 B	
SACs 192.168.10.254:49179		54.194.99.187:443	6 (tcp)		23:59:24 established	0 bps/0 bps	82 B/80 B	
SACs 192.168.10.254:49180		202.154.59.183:80	6 (tcp)		23:59:29 established	0 bps/0 bps	3835 B/44.5 kB	
SACs 192.168.10.254:49181		202.154.59.183:80	6 (tcp)		23:59:28 established	0 bps/0 bps	6.1 kB/58.4 kB	
SACs 192.168.10.254:49185		202.154.59.183:80	6 (tcp)		23:59:28 established	0 bps/0 bps	4157 B/15.3 kB	
SACs 192.168.10.254:49186		202.154.59.183:80	6 (tcp)		23:59:28 established	0 bps/0 bps	8.6 kB/184.2 kB	
SACs 192.168.10.254:49187		202.154.59.183:80	6 (tcp)		23:59:28 established	0 bps/0 bps	4309 B/32.9 kB	
SACs 192.168.10.254:49188		52.9.56.132:443	6 (tcp)		23:59:26 established	0 bps/0 bps	82 B/40 B	
SACs 192.168.10.254:49194		74.125.68.94:443	6 (tcp)		23:59:52 established	0 bps/0 bps	1345 B/792 B	
SACs 192.168.10.254:49197		74.125.200.148:443	6 (tcp)		23:59:52 established	0 bps/0 bps	3422 B/5.5 kB	
SACs 192.168.10.254:49199		216.58.203.238:443	6 (tcp)		23:59:53 established	0 bps/0 bps	3088 B/37.8 kB	
SACs 192.168.10.254:49204		192.0.72.28:80	6 (tcp)		23:59:23 established	0 bps/0 bps	1751 B/1188 B	
SACs 192.168.10.254:49205		192.0.72.28:80	6 (tcp)		23:59:23 established	0 bps/0 bps	1032 B/675 B	
SACs 192.168.10.254:49206		192.0.72.28:443	6 (tcp)		23:59:26 established	0 bps/0 bps	940 B/6.7 kB	
SACs 192.168.10.254:49207		192.0.72.28:443	6 (tcp)		23:59:48 established	0 bps/0 bps	7.1 kB/189.5 kB	
SACs 192.168.10.254:49208		192.0.72.28:80	6 (tcp)		23:59:24 established	0 bps/0 bps	976 B/671 B	
SACs 192.168.10.254:49209		192.0.72.28:80	6 (tcp)		23:59:23 established	0 bps/0 bps	1711 B/638 B	
SACs 192.168.10.254:49210		192.0.72.28:80	6 (tcp)		23:59:23 established	0 bps/0 bps	990 B/605 B	
SACs 192.168.10.254:49211		202.154.59.183:80	6 (tcp)		23:59:52 established	0 bps/0 bps	5.5 kB/65.4 kB	
SACs 192.168.10.254:49212		192.0.72.28:443	6 (tcp)		23:59:24 established	0 bps/0 bps	903 B/507 B	
SACs 192.168.10.254:49213		192.0.72.28:443	6 (tcp)		23:59:26 established	0 bps/0 bps	1083 B/6.7 kB	
SACs 192.168.10.254:49214		192.0.72.28:443	6 (tcp)		23:59:24 established	0 bps/0 bps	772 B/6.7 kB	
SACs 192.168.10.254:49215		192.0.72.28:443	6 (tcp)		23:59:27 established	0 bps/0 bps	1098 B/564 B	
SACs 192.168.10.254:49218		192.168.10.1:8291	6 (tcp)		00:04:59 established	17.0 kbps/111.5 kbps	6.9 kB/70.8 kB	
SACs 192.168.10.254:53410		74.125.200.138:443	17 (u...)		00:00:29	0 bps/0 bps	7.6 kB/5.3 kB	
SACs 192.168.10.254:53958		52.229.116.205:3544	17 (u...)		00:02:31	0 bps/0 bps	1246 B/1644 B	
SACs 192.168.10.254:55120		172.217.24.110:442	17 (u...)		00:00:05	0 bps/0 bps	7.8 kB/16.3 kB	

Connection tracking memiliki Fungsi untuk melihat semua informasi koneksi yang melewati router, seperti source dan destination IP dan Port yang sedang digunakan, status koneksi,tipe protocol dan lain-lain. Setiap paket data itu memiliki status koneksi (connection started) yang dapat dilihat pada connection tracking, dan ini adalah Jenis-jenis status koneksi nya :

- established = Sebuah koneksi yang merupakan bagian dari koneksi yang sudah ada. Maksudnya server 1 menerima paket SYN-ACK dan kemudian merespon dengan paket ACK (Acknowledgment). Intinya, paket tersebut adalah bagian dari koneksi yang telah dikenal.
- New = Sebuah klien merequest koneksi melalui firewall. Maksudnya server1 menghubungi server2 dengan mengirimkan paket SYN (Synchronize), intinya, paket tersebut memulai koneksi baru atau memiliki koneksi yang belum melihat paket di kedua arah.
- related = Sebuah koneksi yang mereques sebuah reques baru tetapi masih merupakan bagian dari koneksi yang sudah ada. Maksudnya server2 menerima paket SYN dari server 1 dan kemudian merespon dengan sebuah paket SYN-ACK (Synchronize-Acknowledgment), intinya, paket tersebut memulai koneksi baru, tetapi yang berhubungan dengan koneksi yang ada, seperti FTP transfer data atau pesan icmp yang error.
- invalid = Sebuah keadaan dimana tidak ada keadaan seperti 3 keadaan di atas , intinya, paket tersebut tidak tergabung dalam connetion yang dikenal dan pada saat yang sama,paket tersebut tidak membuka koneksi baru yang valid.

Ini adalah gambaran connection state /status koneksi:



Lab 29. Membuat Rule untuk Connection State

Jika di Lab sebelumnya menjelaskan tentang Connection state,Maka di Lab ini kita akan membuat Rule untuk Connection State tersebut yang berfungsi untuk mengurangi Resource dari RouterBoard kita..

Kita mulai Membuat Rule Connection State,Pertama Kita akan membuat Rule Untuk Connection State Invalid dengan Action=Drop

- Klik menu IP > Firewall > Filter Rule > Add (+)
- Di General Isi Chain=Input dan Connection State=Invalid

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: invalid established related new untracked

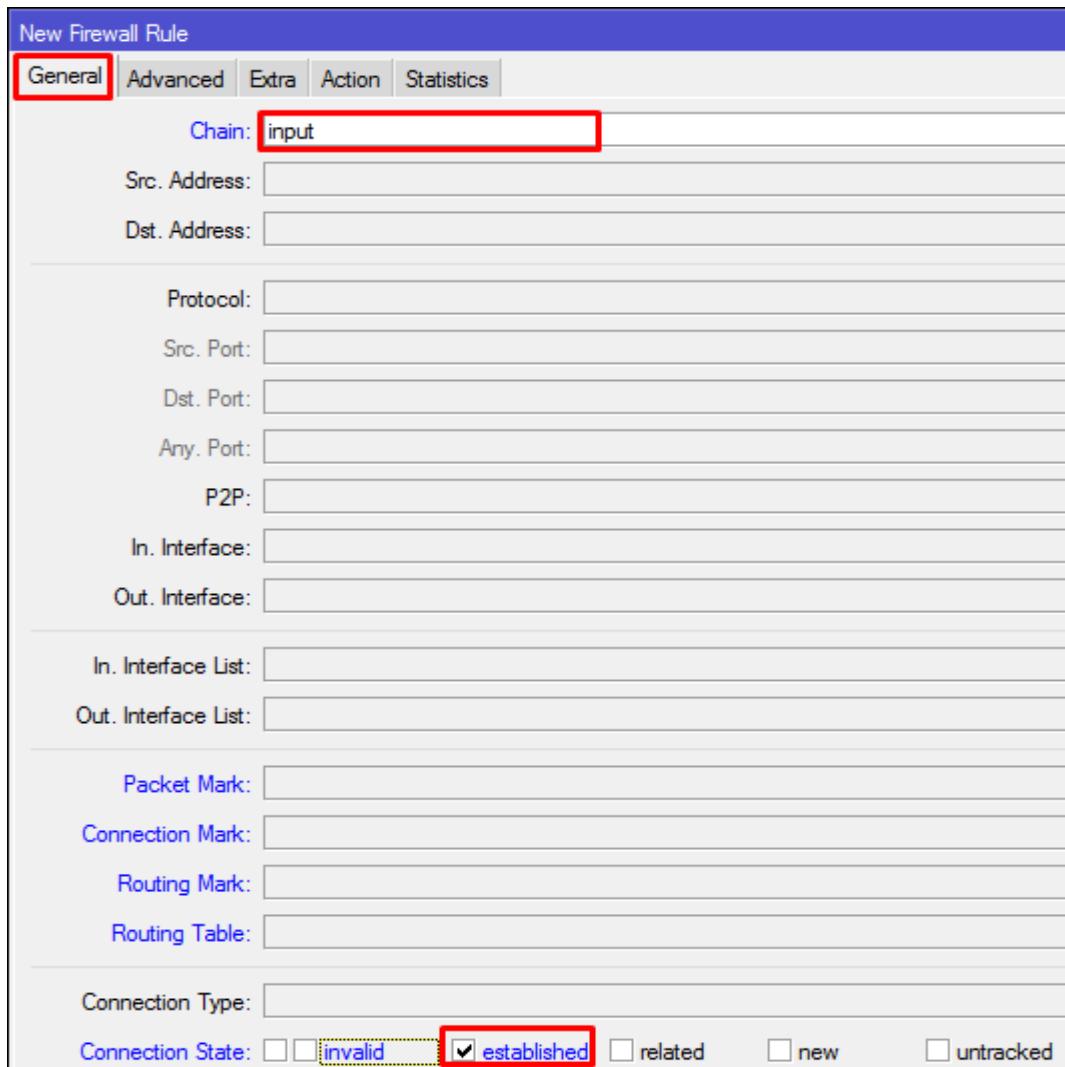
- Lalu Isi Action=Drop

- Lalu Apply dan OK



Selanjutnya kita akan membuat Rule Untuk Connection State Estabilized dengan Action=Accept

- Klik menu IP > Firewall > Filter Rule > Add (+)
- Di General Isi Chain=Input dan Connection State=Estabilized



- Lalu Isi Action=Accept

- Lalu Apply dan OK



Selanjutnya kita akan membuat Rule Untuk Connection State Related dengan Action=Accept

- Klik menu IP > Firewall > Filter Rule > Add (+)
- Di General Isi Chain=Input dan Connection State=Related

The screenshot shows the 'New Firewall Rule' dialog box with the 'General' tab selected. The 'Chain' dropdown is set to 'input'. In the 'Connection State' section at the bottom, the 'related' checkbox is checked and highlighted with a red box. Other options like 'invalid', 'established', 'new', and 'untracked' are also present but not checked.

- Lalu Isi Action=Accept

- Lalu Apply dan OK



Dan yang terakhir kita akan membuat Rule untuk Connection State New dengan Action=Passthrough

- Klik menu IP > Firewall > Filter Rule > Add (+)
- Di General Isi Chain=Input dan Connection State>New

The screenshot shows the 'New Firewall Rule' dialog box with the 'General' tab selected. The 'Chain:' dropdown is set to 'input' and is highlighted with a red box. Below it are fields for Src. Address, Dst. Address, Protocol, Src. Port, Dst. Port, Any. Port, P2P, In. Interface, Out. Interface, In. Interface List, Out. Interface List, Packet Mark, Connection Mark, Routing Mark, and Routing Table. At the bottom, the 'Connection Type:' dropdown is shown with several options: invalid, established, related, new (which is checked and highlighted with a red box), and untracked.

- Lalu Isi Action=Passthrough

- Lalu Apply dan OK



Setelah kita membuat 4 Rule untuk Setiap Connection State Maka akan Ada 4 Rule yang berfungsi Untuk Mengurangi Resource RouterBoard

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State
0	✗ drop	input								invalid
1	✓ accept	input								established
2	✓ accept	input								related
3	✗ passthrough	input								new

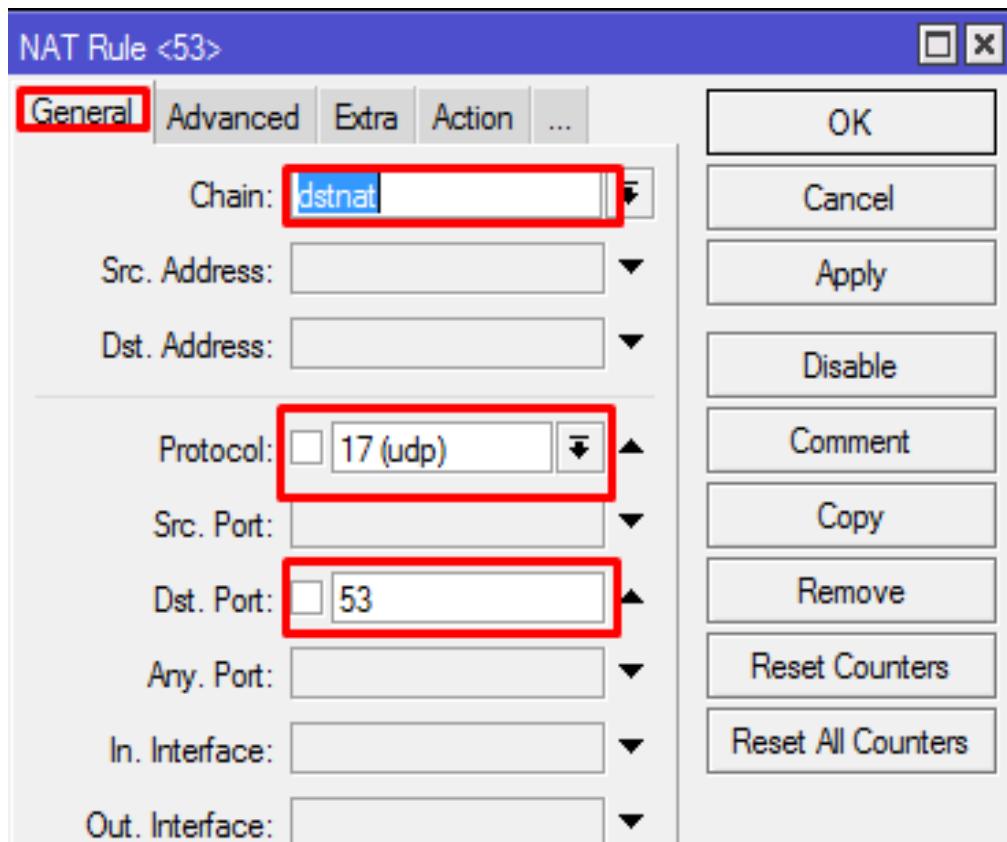
Selesai 😊

Lab 30. Blokir Situs Porno dengan Transparent DNS

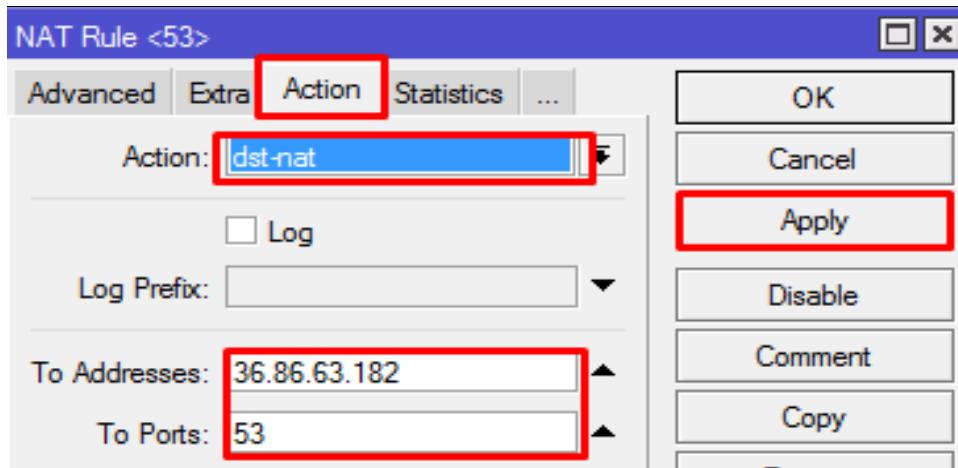
Jika di lab-lab sebelumnya kita memblokir situs dengan cara membuat Filter Rule di RouterBoard maka di lab ini kita akan Mem-Blokir situs dengan menggunakan DNS. Pada lab sebelumnya kita bisa men-Costum Website apa saja kita yang kita blokir,tetapi dengan DNS ini yang blokir situs adalah DNS tersebut,Router hanya Meng-Alihkan semua Akses Client ke DNS tersebut,lalu DNS akan mem-Blokir Website jika Client Meng-Akses situs Porno dan lain lain,di karnakan DNS tersebut memiliki BlackList Website terlarang,jika client meng-Akses website yang terdaftar di BlackList DNS maka maka Website akan Di Blokir Oleh DNS tersebut...di sini kita akan Menggunakan <http://dnsbersih.id/>...

Pertama Kita akan membuat Rule NAT Untuk Meredirect semua akses client ke <http://dnsbersih.id/>..

- Klik IP > Firewall > NAT > Add (+)
- Klik General > Isi Chain=Dstnat , Protocol=17 (Udp) ,Dst.Port=53



- Klik Action > Isi Action=Dst-Nat , To Address=36.86.63.182 ,To Port=53
- Lalu Apply dan OK

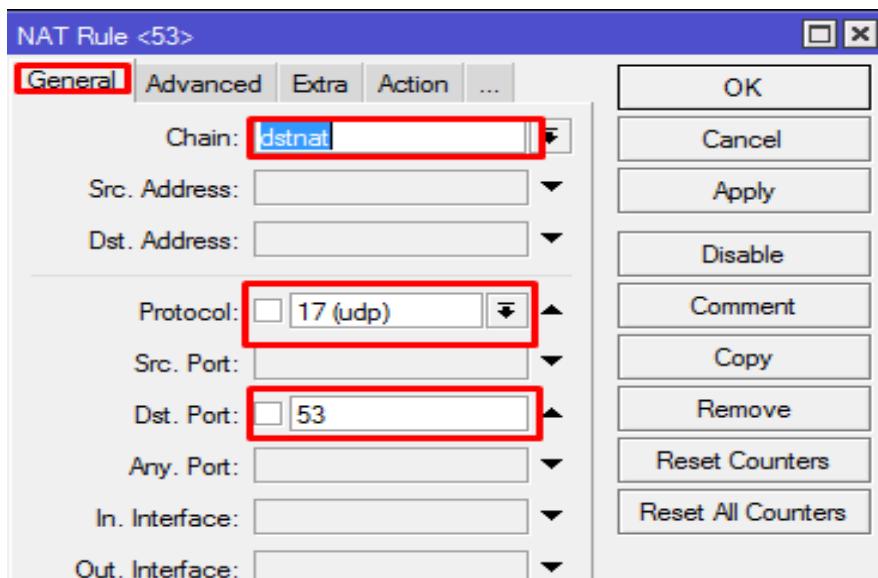


To Address di isi dengan IP dari <http://dnsbersih.id/> dan port 53 karna Protocol DNS adalah UDP port Number=53

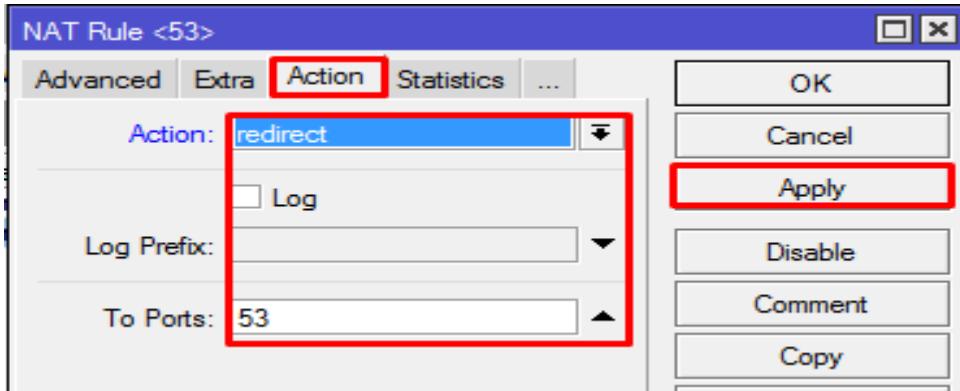
Jika sudah membuat Rule seperti ini yang akan memfilter Situs Situs terlarang adalah DNS tersebut bukan RouterBoard kita

Selanjutnya saya akan menjelaskan bagaimana Membuat Rule untuk DNS yang lebih mudah..

- Klik IP > Firewall > NAT > Add (+)
- Klik General > Isi Chain=Dstnat , Protocol=17 (Udp) ,Dst.Port=53

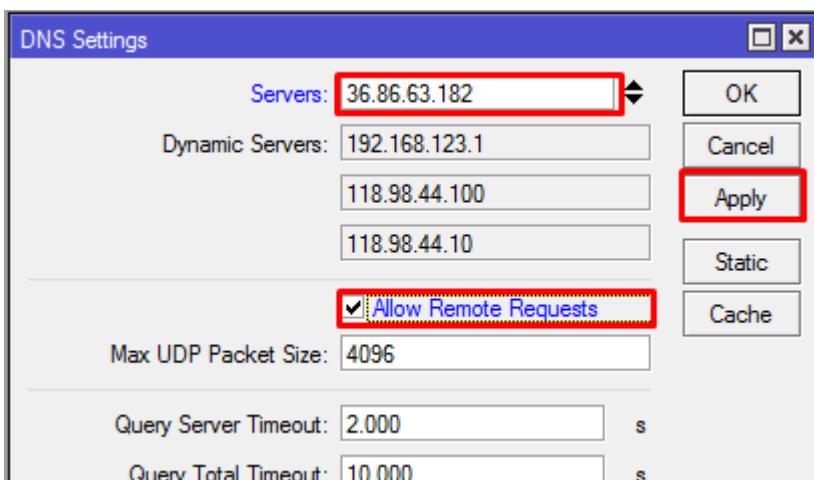


- Klik Action > Isi Action=Redirect , To Port=53
- Lalu Apply dan OK



Jika sudah membuat Rule NAT ,Selanjutnya kita perlu mensetting DNS.

- Klik IP > DNS
- Isi Servers=36.86.63.182 ,Checklist Allow Remote Request
- Lalu Apply dan OK



Cara pertama dan cara ke dua sama saja,hanya berbeda cara..

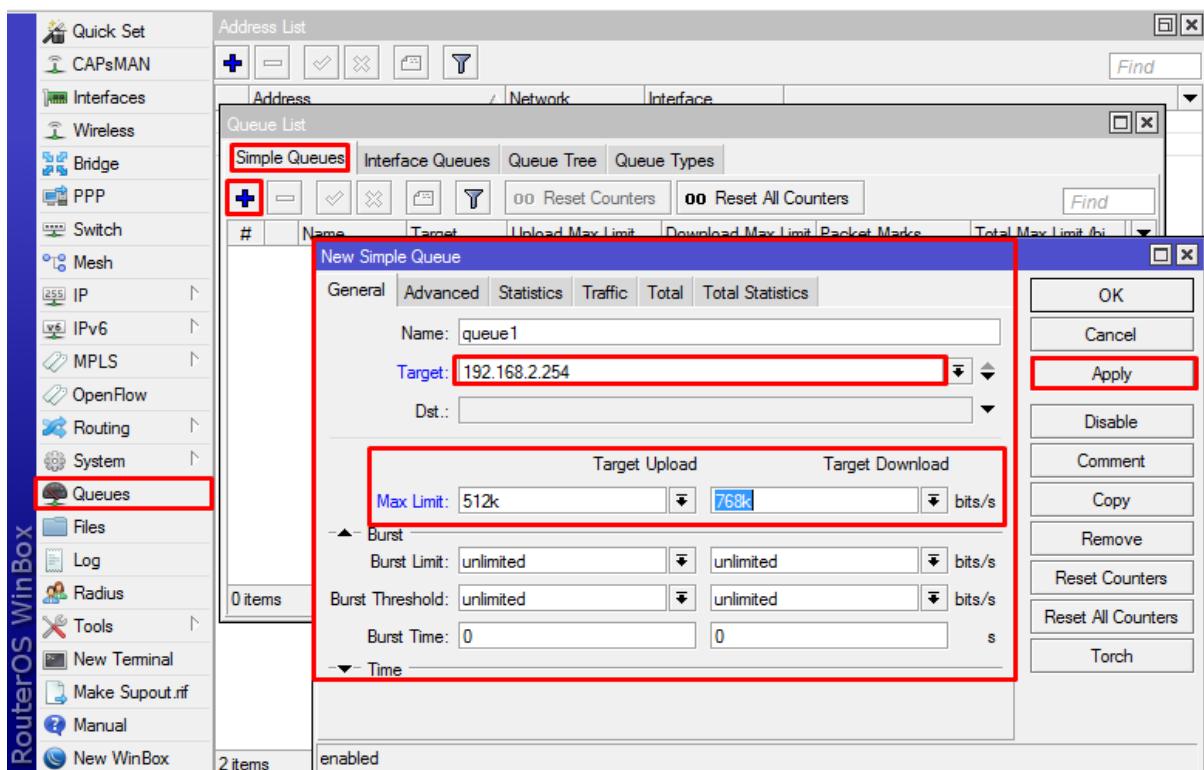
Bab 4 .QoS

Lab 31. Simple Queue

Simple Queue adalah Membuat pengaturan bandwidth secara sederhana berdasarkan IP Address client dengan menentukan kecepatan upload dan download maksimum yang bisa dicapai oleh client, jadi menggunakan Simple queue adalah cara paling mudah untuk melakukan limitasi bandwidth terhadap Client.

Konfigurasi:

- Klik Queue > Simple Queue > Add
- Isi Name=queue1
- Target 192.168.2.254 (IP PC/Client) ,Max Limit (Upload)=512kb ,Max Limit(Download)=768kb
- Lalu Apply dan OK

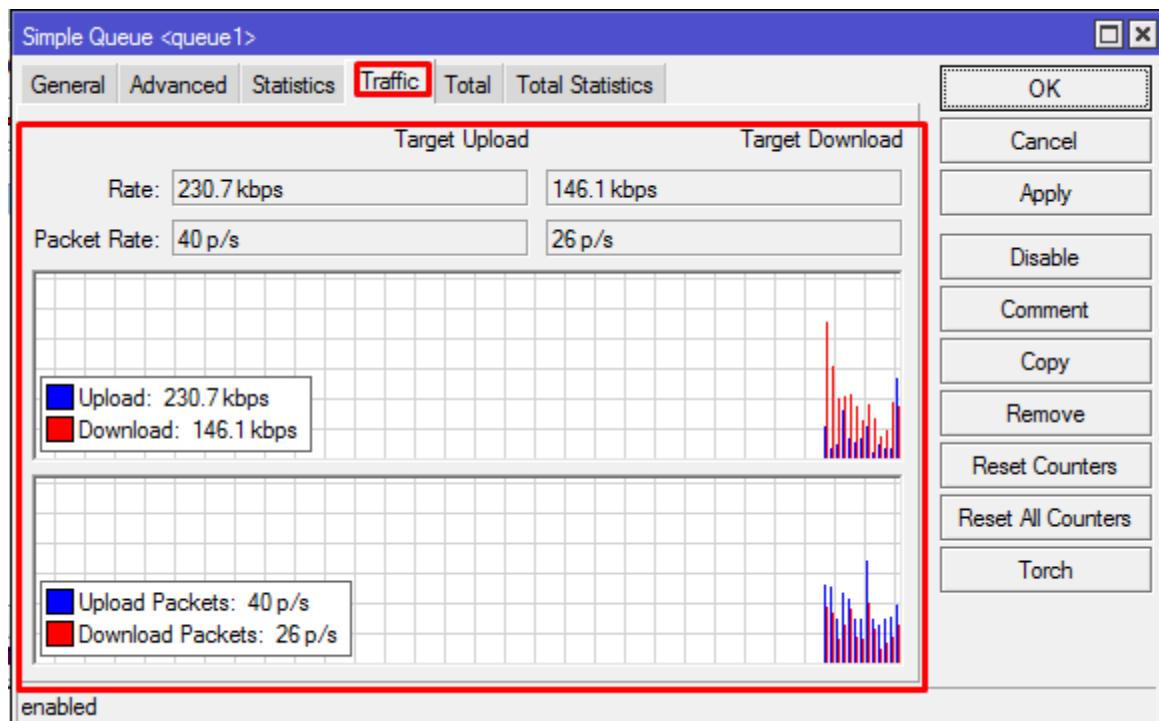


Jika sudah melewati Step ini maka Bandwidth client tidak akan melebihi batas telah ditentukan oleh Simple Queue

Rule Simple Queue

Queue List							
Simple Queues		Interface Queues		Queue Tree		Queue Types	
+/-	Checkmark	X	File	Filter	Reset Counters	Reset All Counters	Find
#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Lim	▼
0	queue1	192.168.2.254	512k	768k			

Trafic Simple Queue



Lab 32. Simple Queue with Burst Limit

Jika simple Queue menggunakan Burst Limit maka Client Akan mendapatkan Bandwidth yang lebih besar dari pada max limit,brust adalah batasan bandwith yang dapat dipakai dalam waktu yang telah ditentukan oleh server tersebut. Burst limit biasa di gunakan bersama burst treshold, burst limit, dan juga burst time. Fungsi dari burst limit ini pun sangat diperlukan untuk network administrator yang berguna agar bandwith yang dipakai saat jam kerja tersebut tidak habis secara sia - sia, oleh sebab itu kita menambahkan burst limit di queue kita.

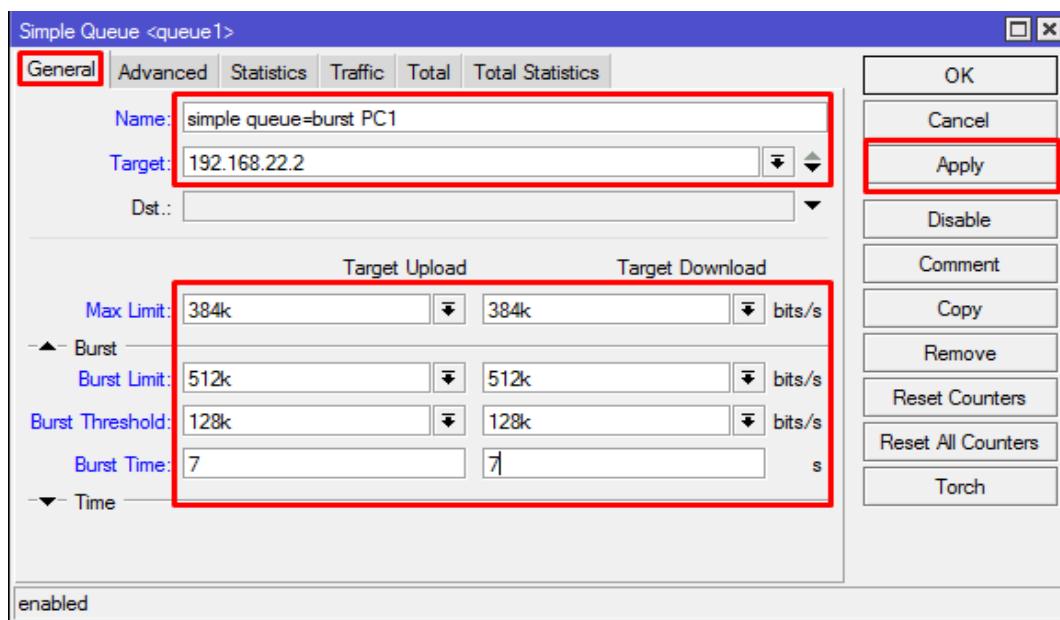
Contoh penerapannya seperti berikut :

1. contoh komputer A, kita ingin mengatur bandwith yang dia pakai. Max bandwith=384kb, burst limit=512kb, burst thersholt=128kb, burst time=7s(detik).

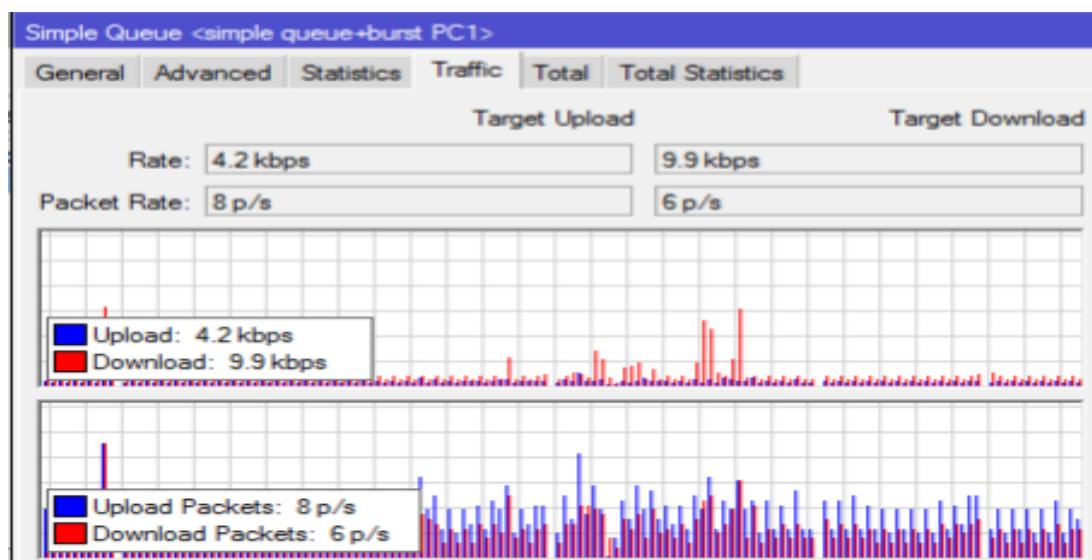
- Artinya
- Saat komputer A terhubung ke wifi kita, dia akan mendapatkan bandwith sebesar 384kb
- Pada suatu waktu bandwith tersebut akan ditambah hingga 512kb selama 7 detik(burst limit).
- Dan akan diturunkan lagi bandwithnya setelah 7 detik ke 128kb(burst thersholt)
- Setelah turun maka bandwithnya akan naik lagi ke 384kb
- Kemudian dinaikkan lagi pada waktu tertentu ke 512kb selama 7 detik
- Setelah itu diturunkan kembali ke 128kb, dan balik lagi ke 384kb.
- Dan selanjutnya akan begitu terus.
- Dengan di burst maka akan menghasilkan pergantian bandwith secara otomatis oleh router kita, dan itu tentunya bisa menghemat bandwith kita juga. Burst limit ini sering kita jumpai pada kartu GSM, disaat kita mengunduh sebuah file awal - awal kita akan mendapatkan bandwith maksimal, dan setelah itu diturunkan(burst thersholt) dan dikembalikan kembali ke bandwith awalnya

Konfigurasi:

- Klik Queue > Simple Queue > Add
- Isi Name simple queue burst PC1
- Target 192.168.22.2 (IP PC/Client) ,Max Limit (Upload)=384kb ,Max Limit(Download)=384kb
- Isi Burst Limit (Upload)=128kb ,Burst Limit Threshold=128kb
- Isi Burst time Upload=7 ,Burst time download=7
- Lalu Apply dan OK

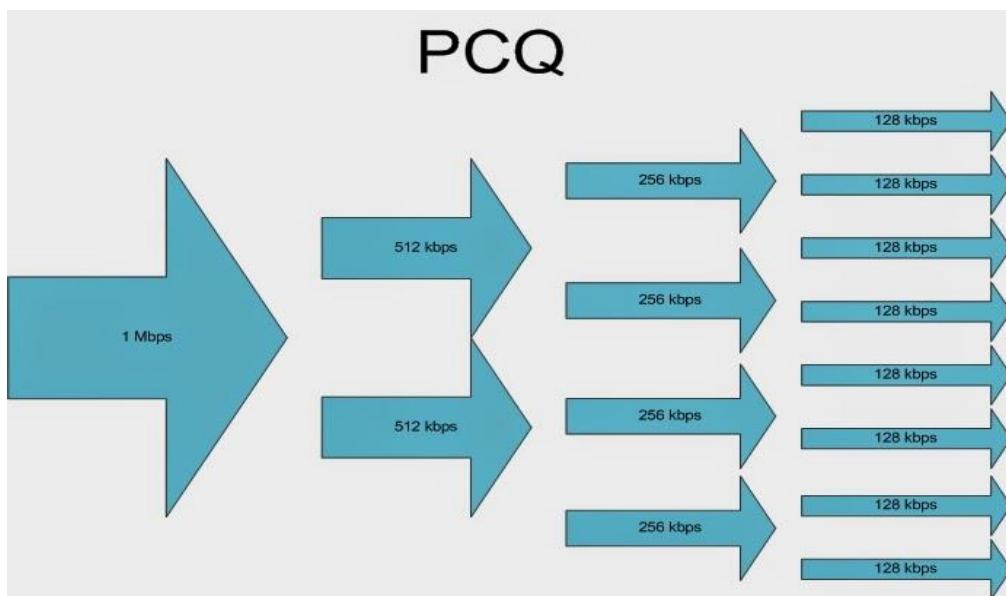


Jika sudah Coba Lihat Trafic di Simple Queue tersebut



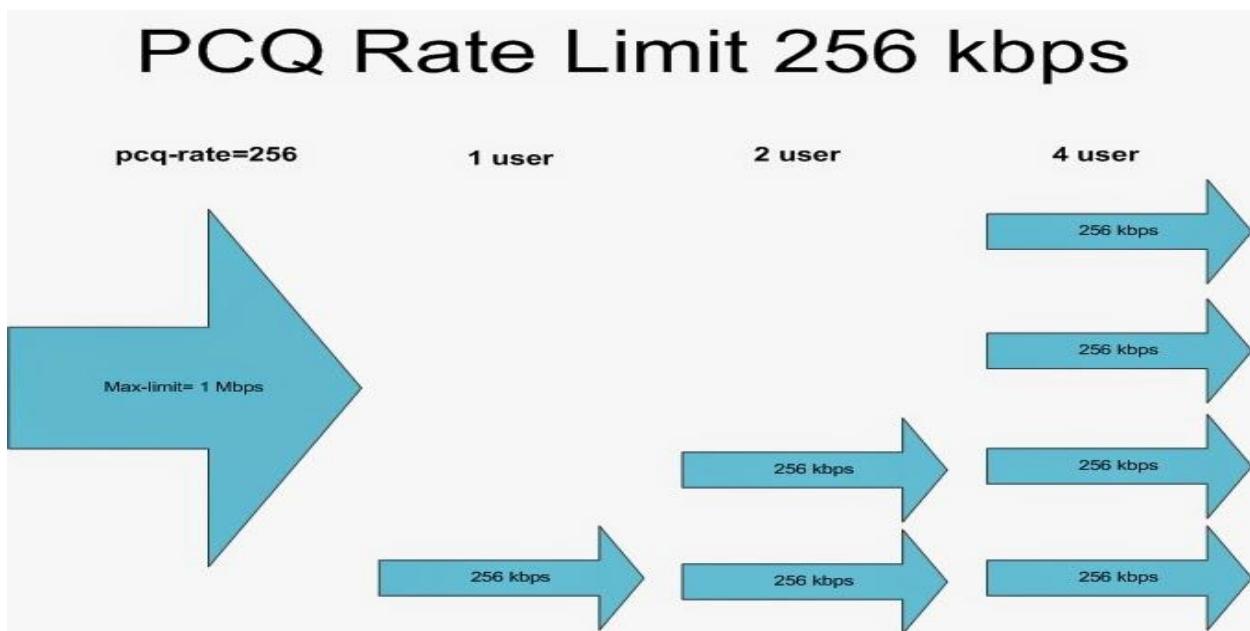
Lab 33. Simple Queue with PCQ

PCQ atau Per Connection Queue merupakan pengaturan manajemen bandwidth bersifat massive. Dengan menggunakan PCQ walaupun jumlah komputer client sejumlah puluhan atau bahkan ratusan, hanya diperlukan satu atau dua konfigurasi queue ,PCQ berfungsi untuk membagi Bandwidth ke client secara merata, PCQ bekerja dengan membuat sub-stream berdasarkan parameter pcq-classifier yang dapat berupa IP Address pengirim berdasarkan pengirim (src-address), IP Address tujuan (dst-address), Port pengirim (src-port) maupun Port tujuan (dst-port). Gambar di bawah ini adalah contoh ilustrasi dari PCQ



Dalam PCQ kita juga bisa menggunakan Parameter PCQ Rate, Parameter pcq-rate dapat digunakan untuk membatasi bandwidth maksimum yang bisa didapatkan oleh tiap sub-stream. Jika parameter yang digunakan adalah pcq-rate=0 maka setiap sub-stream bisa saja mendapatkan bandwidth maksimum yang nantinya diberikan oleh Simple Queue.

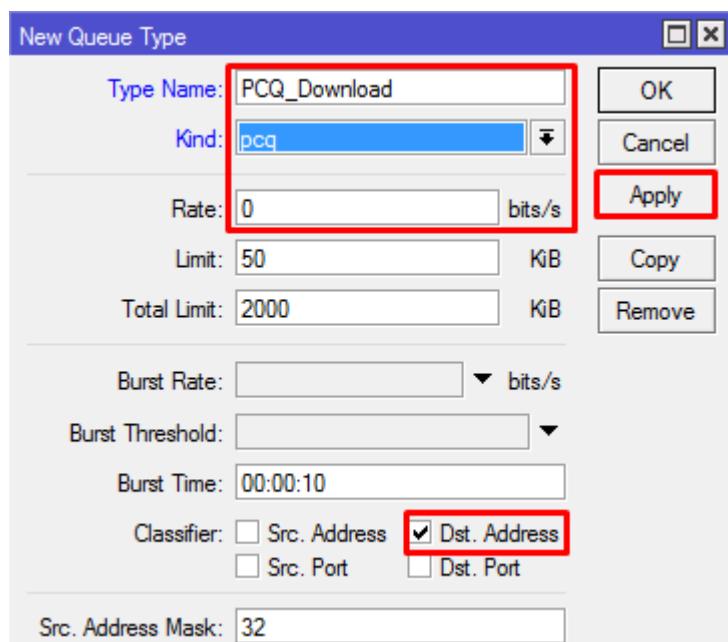
Lebih detailnya bisa di lihat gambar di bawah ini yang menggunakan pcq-rate=256



selanjutnya kita akan mencoba meng-konfigurasikan PCQ:

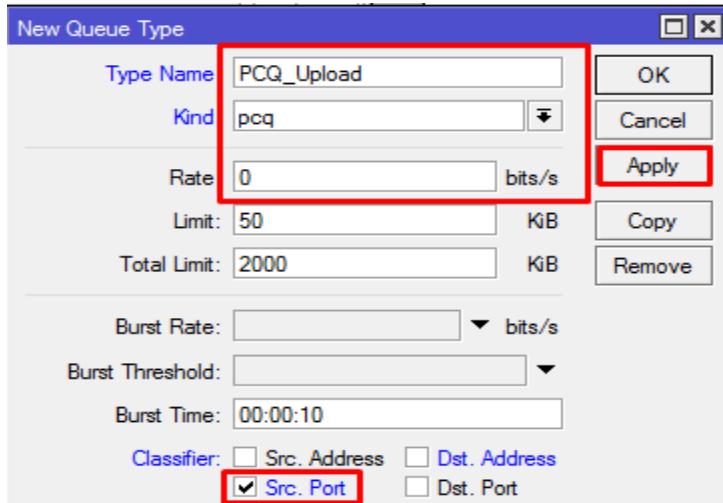
Peratama kita akan membuat Queue Type terlebih dahulu.

- Klik Queue > Queue Type > Add (+)
- Isi Type Name=PCQ_Download ,Kind=Pcq ,Rate=0 ,Classifier=Dst.Address
- Lalu Apply dan OK

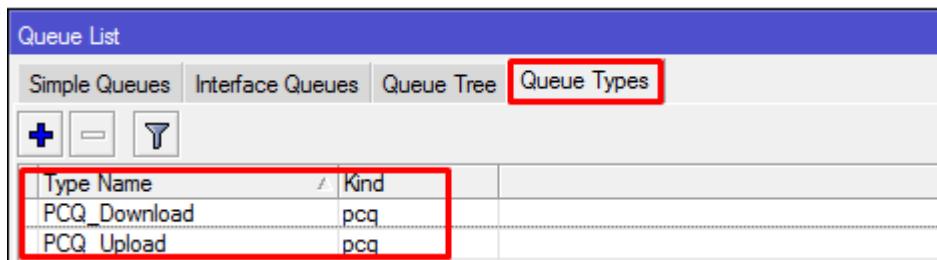


Selanjutnya Kita akan Membuat Queue Type untuk Upload nya..

- Klik Queue > Queue Type > Add (+)
- Isi Type Name=PCQ_Uplod ,Kind=Pcq ,Rate=0 ,Classifier=Src.Address
- Lalu Apply dan OK

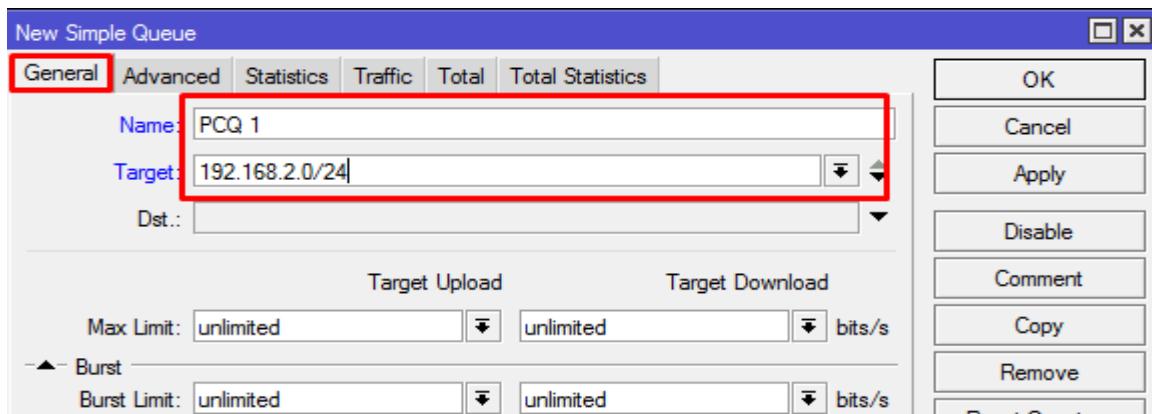


Jika sudah selesai maka urutan Rule nya akan seperti ini.

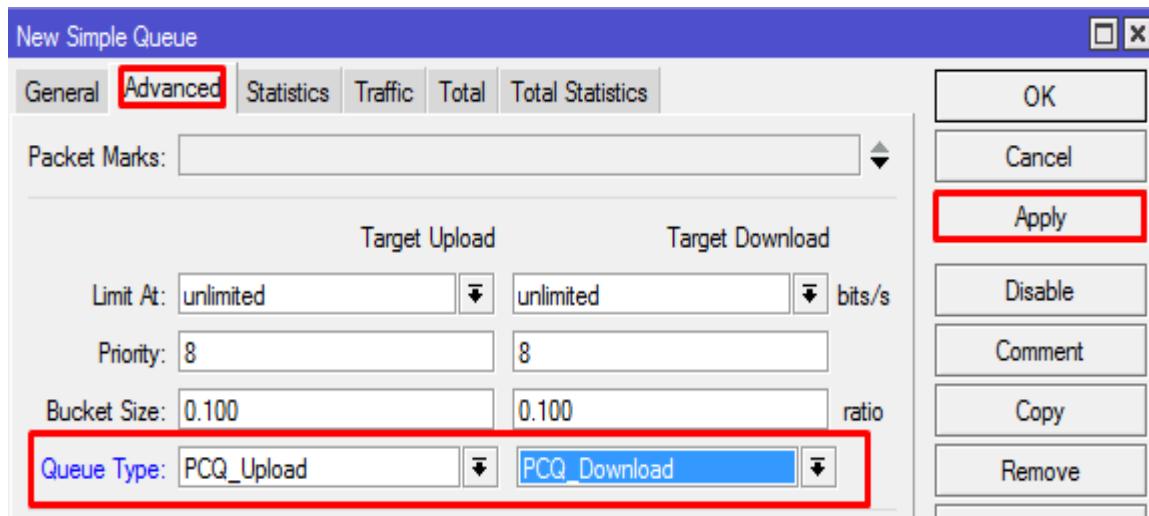


Selanjutnya Kita akan membuat Simple Queue dan memasukan Parameter Queue Type yang telah kita buat.

- Klik Queue > Simple Queue > Add (+)
- Isi Name= PCQ 1 (terserah) ,Target=192.168.2.0/24 (Network Client)



- Klik Advanced > Isi Queue Type
- Target Upload=PCQ_Uplod , Target Download=PCQ_Download
- Lalu Apply dan OK



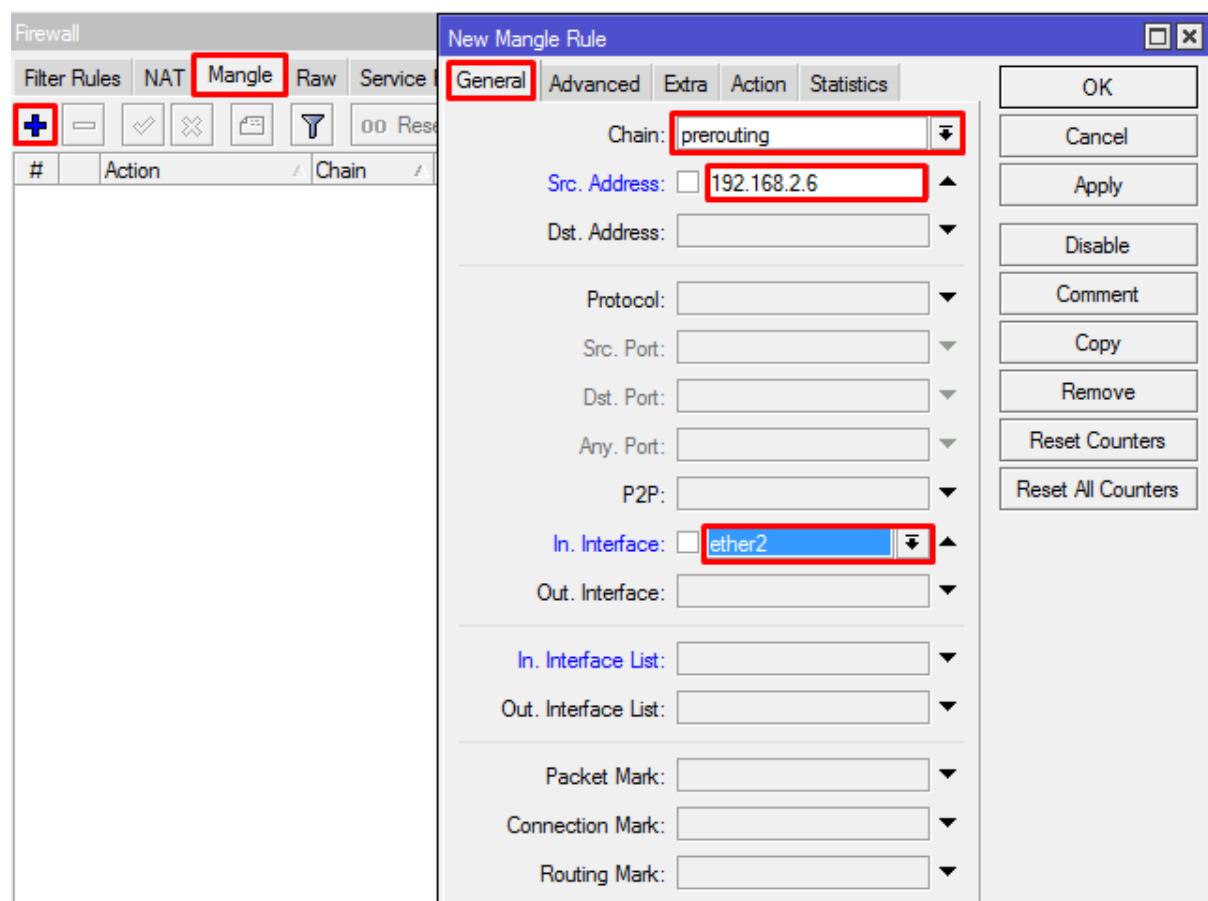
Jika sudah membuat Rule seperti ini maka Bandwidth di network 192.168.2.0/24 akan terbagi secara rata ke masing masing Client..

Lab 34. Membuat Rule Mangle Untuk Queue

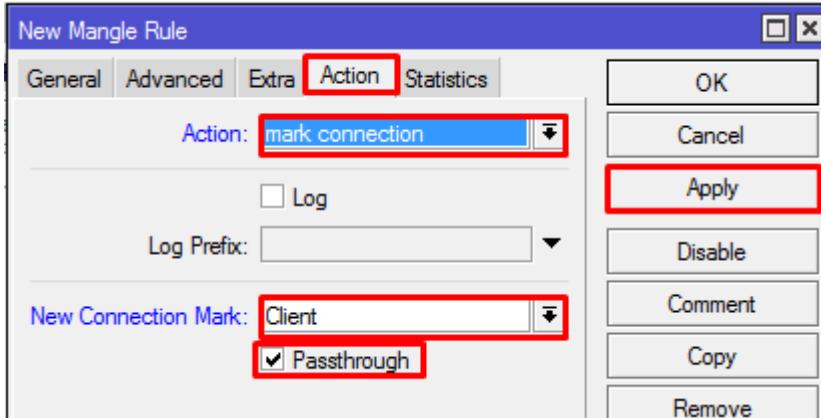
Di Lab kita akan membuat Rule Mangle untuk Queue, Rule Mangle berfungsi untuk menandai Paket (Marking) yang keluar masuk Router.. jika kita menggunakan Mangle untuk Queue maka Kita bisa membatasi bandwidth Upload dan Download, dan kita juga bisa membatasi Bandwidth Per-Extensi (.MP3, .MKV) artinya jika kita melakukan Queue dengan menambahkan mangle maka kita bisa membatasi bandwidth secara Detail.. di lab ini kita akan mencoba membuat Mangle untuk traffic Upload dan Download...

Pertama kita akan membuat 1 rule mangle dengan menggunakan Action mark Connection yang berfungsi untuk menandai koneksi baru yang di buat oleh Client..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting ,Src.Adress=192.168.2.6 (IP Client) , In.Interface=Ethenet2 (Mengarah ke Client)



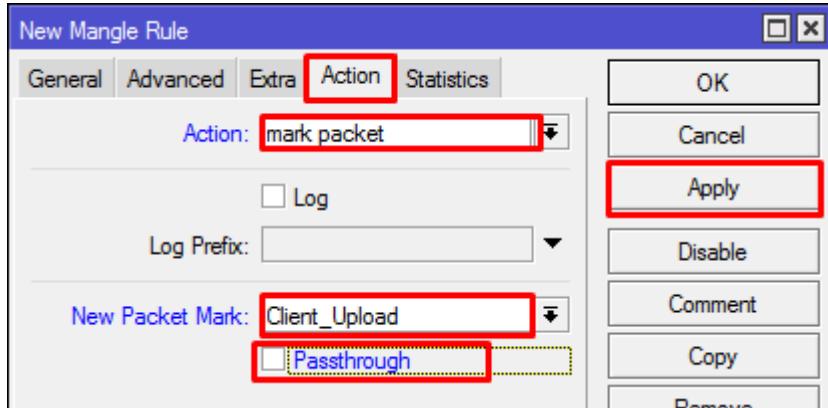
- Lalu Klik Action
- Isi Action=Mark Connection ,New Connection Mark=Client (bebas) , Checklist Passthrough
- Lalu Apply dan OK



Jika kita sudah menandai koneksi koneksi baru yang di buat Oleh Client ,selanjutnya kita akan membuat rule mangle untuk Menandai Packet Upload dan Download..

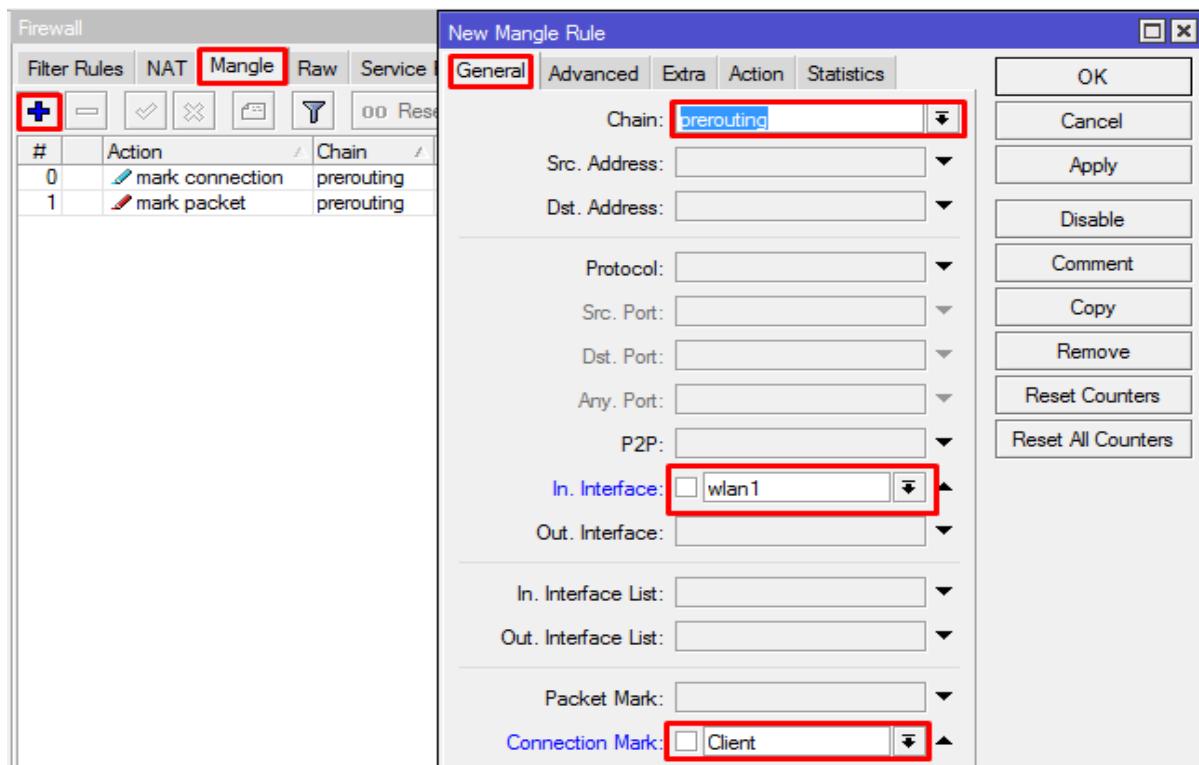
- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting , Connection Mark=Client In.Interface=Ethenet2 (Mengarah ke Client)

- Lalu Klik Action
- Isi Action=Mark Packet, New Connection Mark=Client_Upload (bebas), Unchecklist Passthrough
- Lalu Apply dan OK

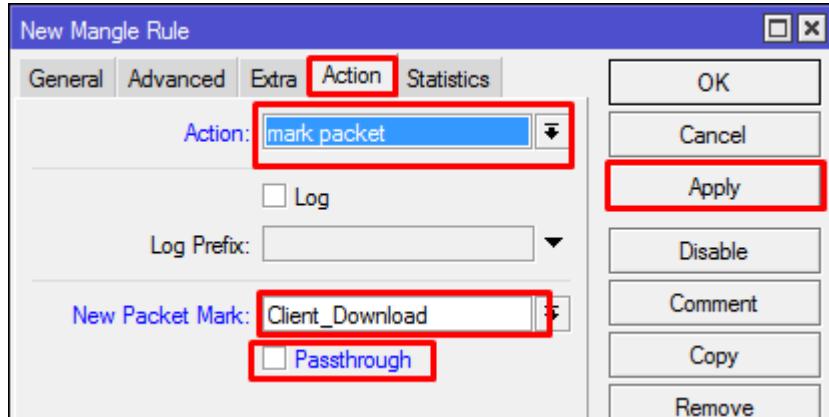


Rule di atas adalah Rule untuk Upload Client, selanjutnya kita akan membuat Rule mangle untuk Download Client..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting , Connection Mark=Client, In.Interface=Wlan1 (mengarah ke Internet)



- Lalu Klik Action
- Isi Action=Mark Packet, New Connection Mark=Client_Download (bebas), Unchecklist Passthrough
- Lalu Apply dan OK



Jika sudah Membuat 3 Rule tersebut maka Trafic Upload dan Download Client akan tercatat...

Lab 35. Queue Tree

Queue Tree berfungsi untuk mengimplementasikan fungsi yang lebih kompleks dalam limit bandwidth pada mikrotik dimana penggunaan packet mark nya memiliki fungsi yang lebih baik. Digunakan untuk membatasi satu arah koneksi saja baik itu download maupun upload. Secara umum Queue Tree ini tidak terlihat berbeda dari Simple Queue.

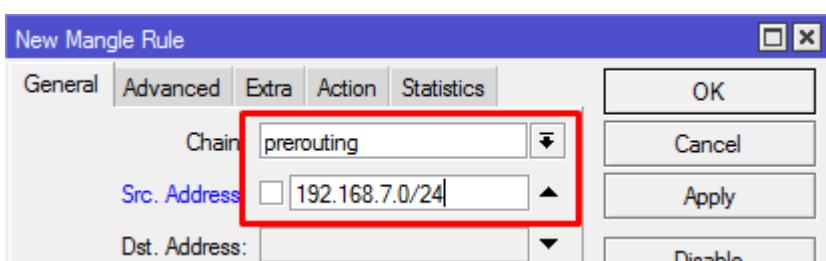
Perbedaan yang bisa kita lihat langsung yaitu hanya dari sisi cara pakai atau penggunaannya saja. Dimana Queue Simple secara khusus memang dirancang untuk kemudahan konfigurasi sementara Queue Tree dirancang untuk melaksanakan tugas antrian yang lebih kompleks dan butuh pemahaman yang baik tentang aliran trafik. ,membatasi bandwidth untuk client menggunakan Queue Tree lebih baik karna Queue Tree akan membagi rata bandwidth kepada seluruh Client dan Queue Tree juga dapat mencatat Trafic yang keluar masuk Router karna Queue Tree menggunakan Mangle..

Pertama Kita Setting Router agar dapat terkoneksi ke Internet,di sini router saya terkoneksi ke internet melalui Wireless (Wlan1)..

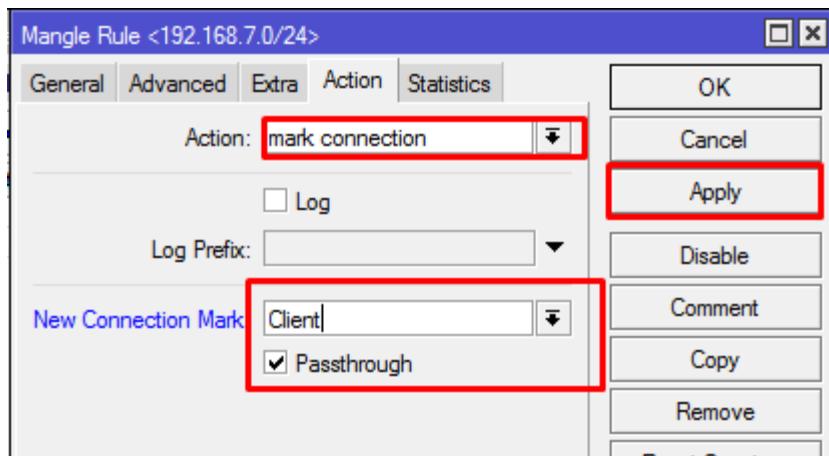
Jika Router kita telah terkoneksi ke Internet ,Selanjutnya kita akan membuat Mangle yang berfungsi untuk mencatat Trafic dari Queue Tree..

Pertama Kita buat Mangle Mark-Connection yang berfungsi untuk mencatat Koneksi baru yang di buat oleh Client ..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting Src.Address 192.168.7.0/24 (Network Client)

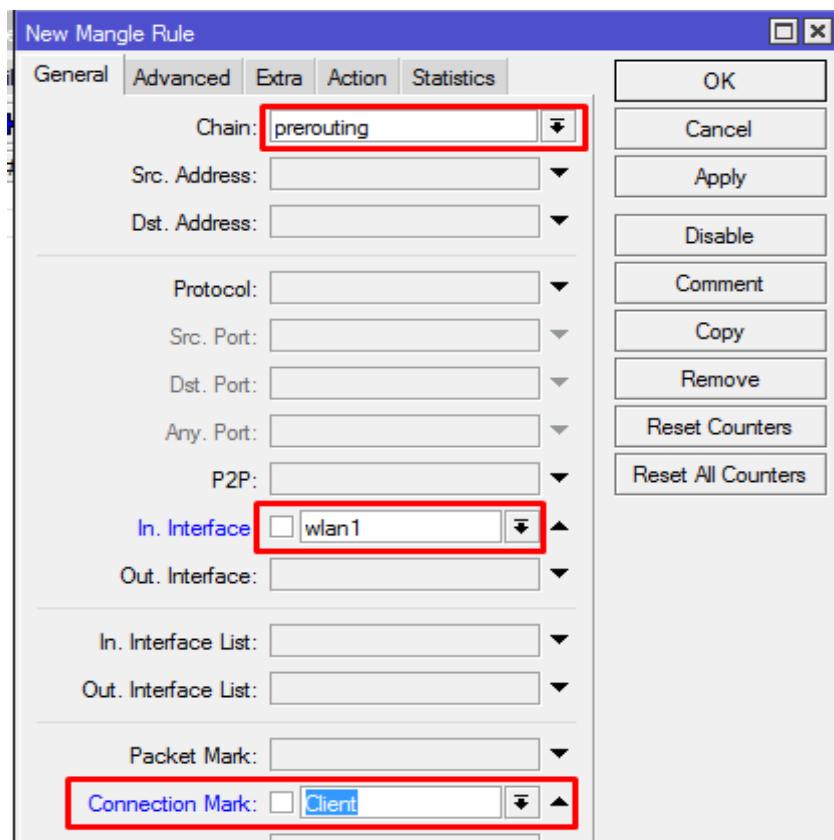


- Pilih Action=Mark Connection ,Isi New Connection Mark=Client dan Checklist Passthrough
- Lalu Apply dan OK

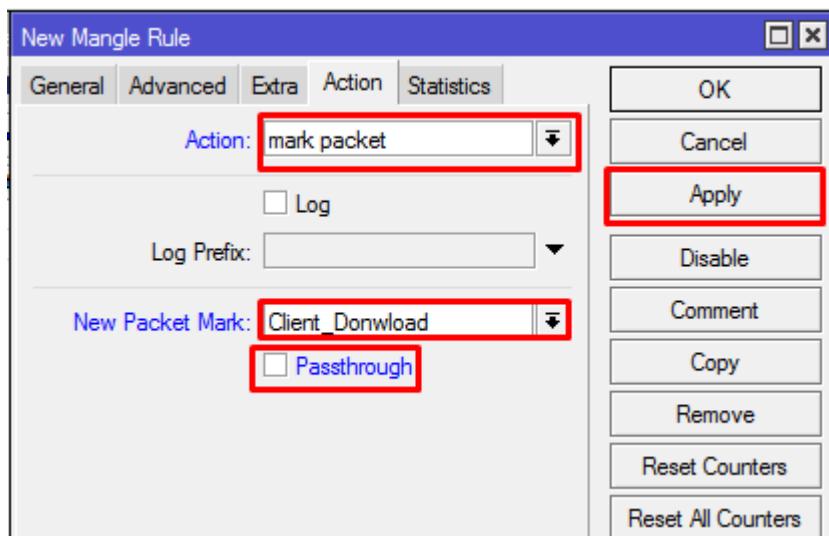


Jika sudah Kita akan membuat Rule Mangle Untuk Mencatat Trafic Download dari Client..

- Klik Mangle > Add (+)
- Isi Chain=Prerouting ,In.Interface=Wlan1 (Public) ,Connection Mark=Client

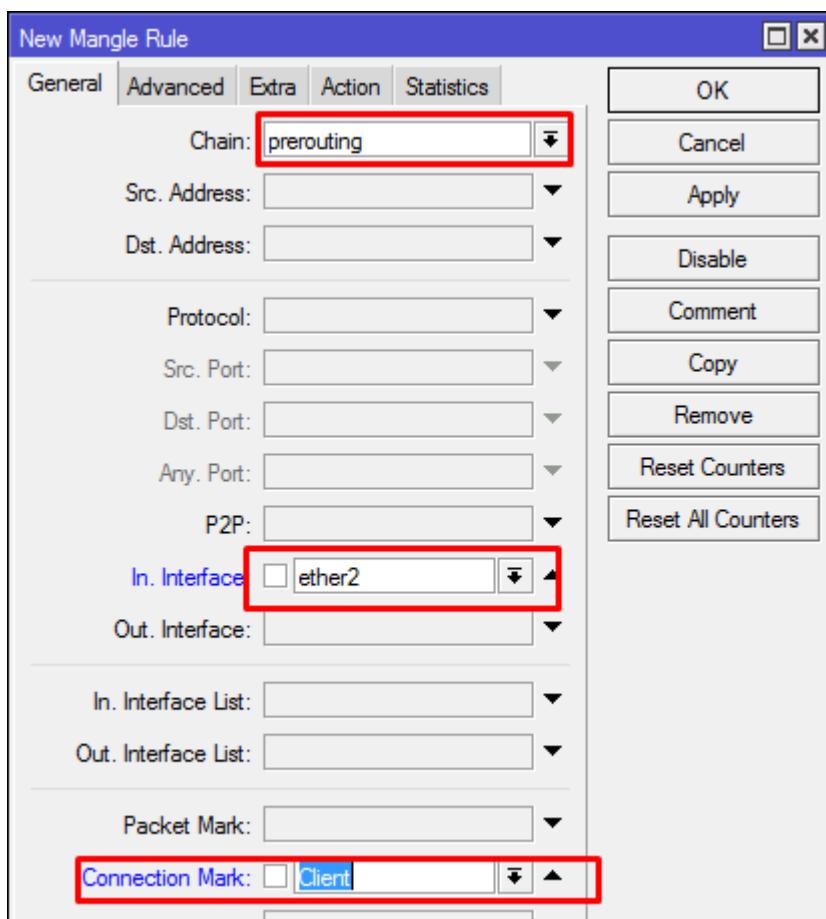


- Pilih Action=Mark Packet ,New=Packet Mark =Client_Download ,Dan Unchecklist Passthrough
- Lalu Apply dan OK

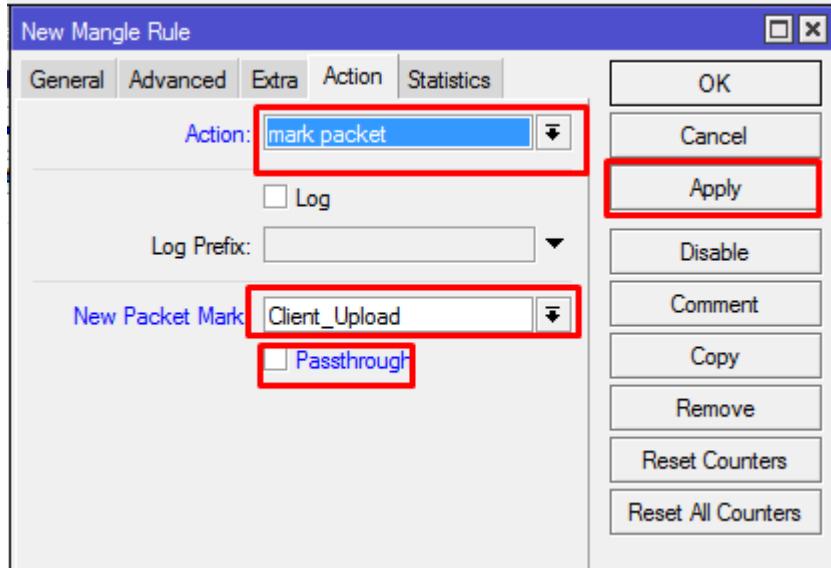


Jika sudah kita akan membuat Rule mangle untuk mencatat Aktivitas Upload dari Client ...

- Klik Add (+) Pada menu Mangle
- Isi Chain=Prerouting ,In.Interface=Ether2 ,Connection Mark=Client



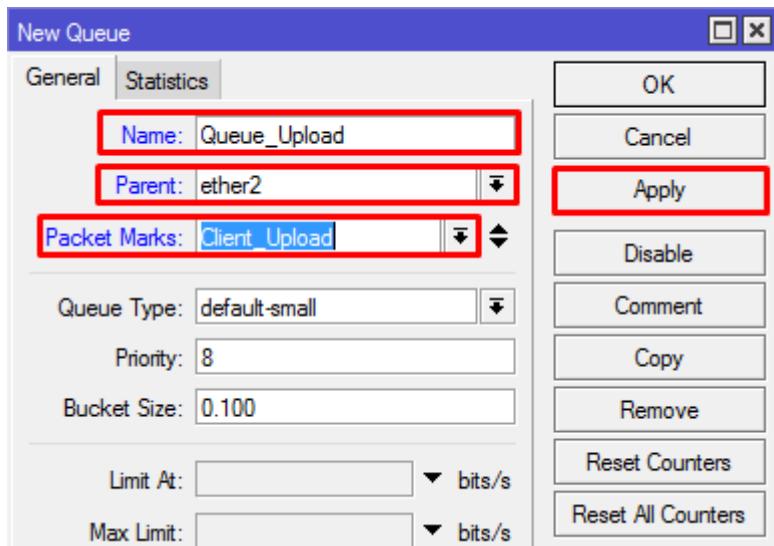
- Isi Action=Mark Packet dan Isi New Packetmark=Client_Upload dan Uncheck Passthrough
- Lalu Apply dan OK



Jika sudah melewati Step ini maka Konfigurasi Mangle Sudah selesai,Maka kita lanjut ke lab selanjutnya yaitu membuat Queue Tree..

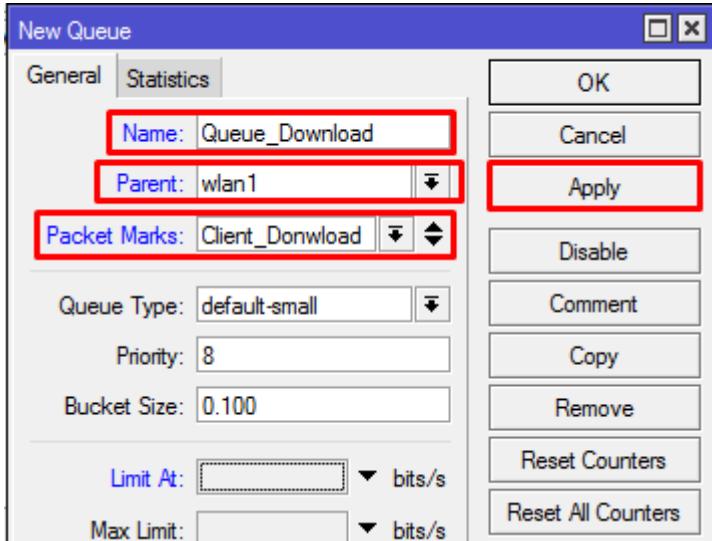
Pertama kita kan membuat Queue Tree Untuk Trafic Upload Terlebih dahulu..

- Klik Menu Queue > Queue Tree > Add (+)
- Isi Name=Queue_Upload ,Isi Parent=Ether2 ,Mark Packet=Client_Upload
- Lalu Apply dan OK



Selanjutnya kita akan membuat Queue Tree Untuk Trafic Download.

- Klik Menu Queue > Queue Tree > Add (+)
- Isi Name=Queue_Download ,Isi Parent=Wlan1 ,Mark Packet=Client_Download
- Lalu Apply dan OK



Jika sudah maka Konfigurasi Queue Tree telah selesai,Maka Semua Client akan mendapatkan Bandwidth secara merata dan semua traffic upload dan download akan tercatat di Mangle dan Queue..

Bab 5. Network Management

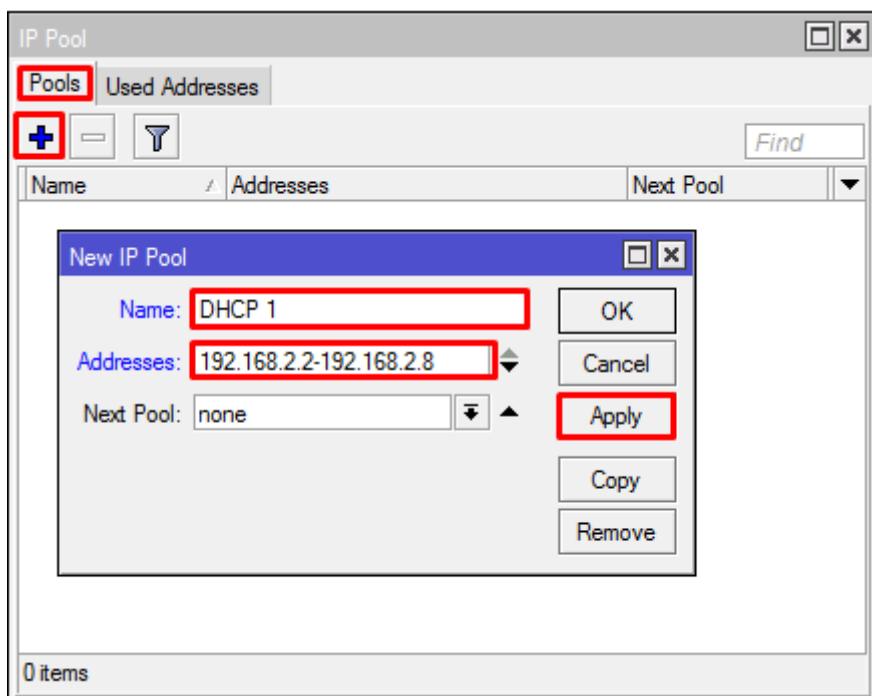


Lab 36. Setting DHCP

Di lab ini saya akan menjelaskan Cara Setting DHCP, di Lab ini saya akan menjelaskan bagaimana cara setting DHCP Server secara Manual, Jika pada lab lab sebelumnya kita membuat DHCP server menggunakan cara Wizard , pada lab ini kita akan Membuat DHCP secara Manual...

Pertama beri IP address 192.168.2.1/24 untuk WLAN1, selanjutnya kita akan membuat IP Pool, IP Pool adalah sekumpulan IP Address yang akan di bagikan kepada Client, IP Pool biasa di gunakan Untuk DHCP dan PPTP

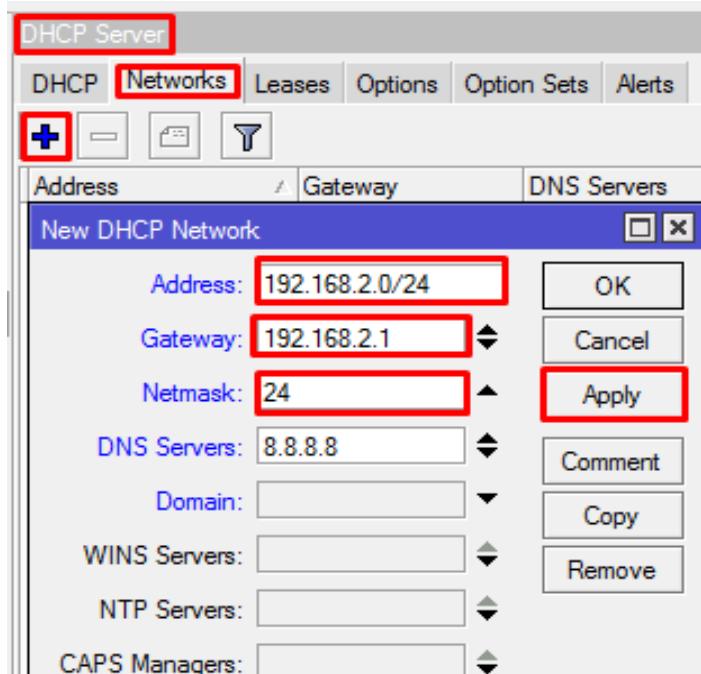
- Klik IP > Pool > Add (+)
- Isi Name=DHCP 1 , Addresses=192.168.2.2-192.168.2.8
- Lalu Apply dan OK



Jika sudah melewati Step Ini maka Artinya IP Address yang akan di berikan kepada Client adalah 192.168.2.2 sampa 192.168.2.8 , Selain IP Address tersebut maka IP Address tidak akan di berikan kepada Client...

Langkah selanjutnya adalah Membuat DHCP Network..

- Klik IP > DHCP Server > Networks > Add (+)
- Isi Address=192.168.2.0/24 ,Gateway=192.168.2.1 ,Netmask=24 , DNS Server=8.8.8.8 (Di sesuaikan)
- Lalu Apply dan OK

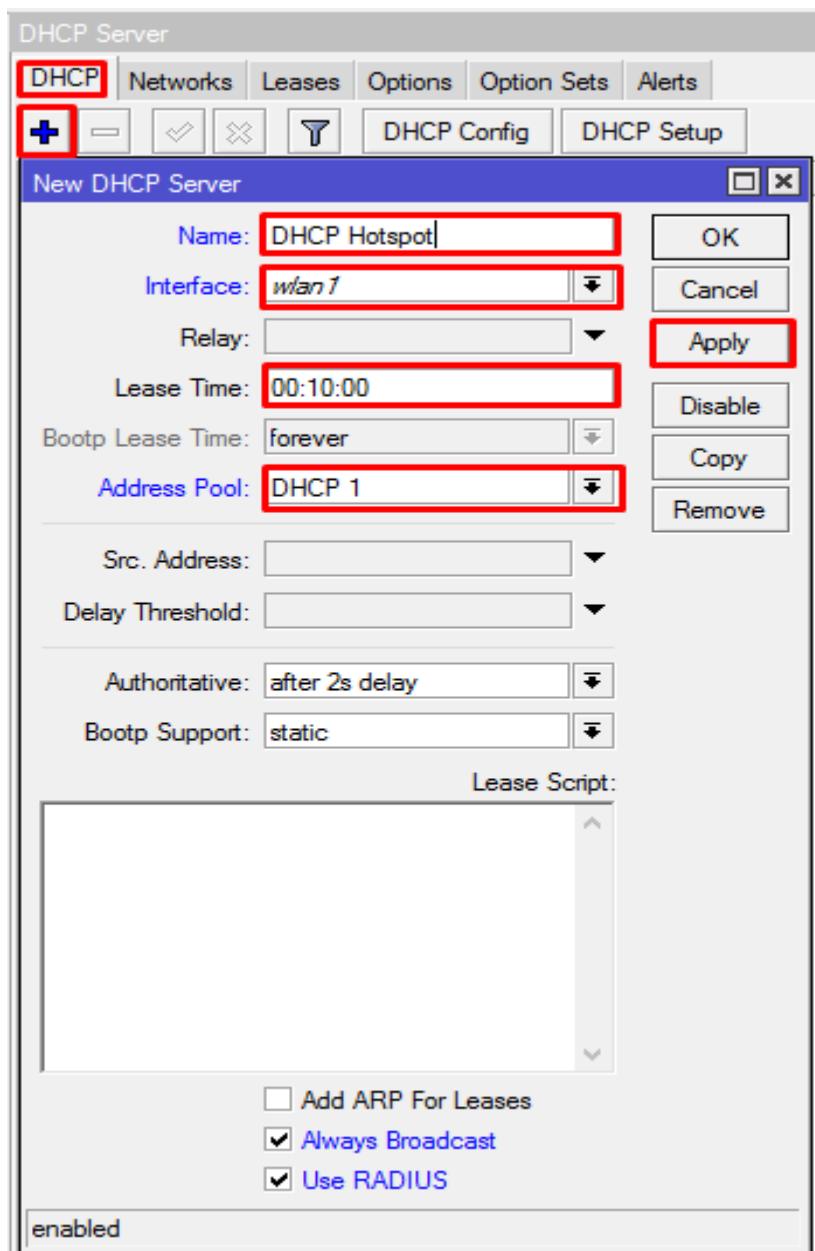


Jika sudah Selesai maka hasil nya akan seperti ini...

DHCP Server					
DHCP	Networks	Leases	Options	Option Sets	Alerts
				Address 192.168.2.0/24	Gateway 192.168.2.1

Langkah selanjutnya adalah Membuat DHCP Server...

- Klik IP > DHCP Server > DHCP > Add (+)
- Isi Name=DHCP Hotspot , Interface=Wlan1 ,Lease Time=00:10:00 ,Address Pool=DHCP 1 (IP Pool yang telah kita buat) ,Checklist Always Broadcast dan Use RADIUS
- Lalu Apply dan OK



Jika Sudah Melewati Step ini,Maka Setting DHCP server Secara manual telah selesai..

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
DHCP Hotspot	wlan1		00:10:00	DHCP 1	no

Jika Ada Client yang menggunakan DHCP,maka Status dari Client tersebut bisa di lihat **Leases** ,Di Leases akan terlihat IP Address yang digunakan oleh Client,Mac Address Client ,Host Name ,Dan Lain Lain,

Dan Used Address di IP Pool juga akan bertambah karna Ada Client yang menggunakan IP Pool tersebut..

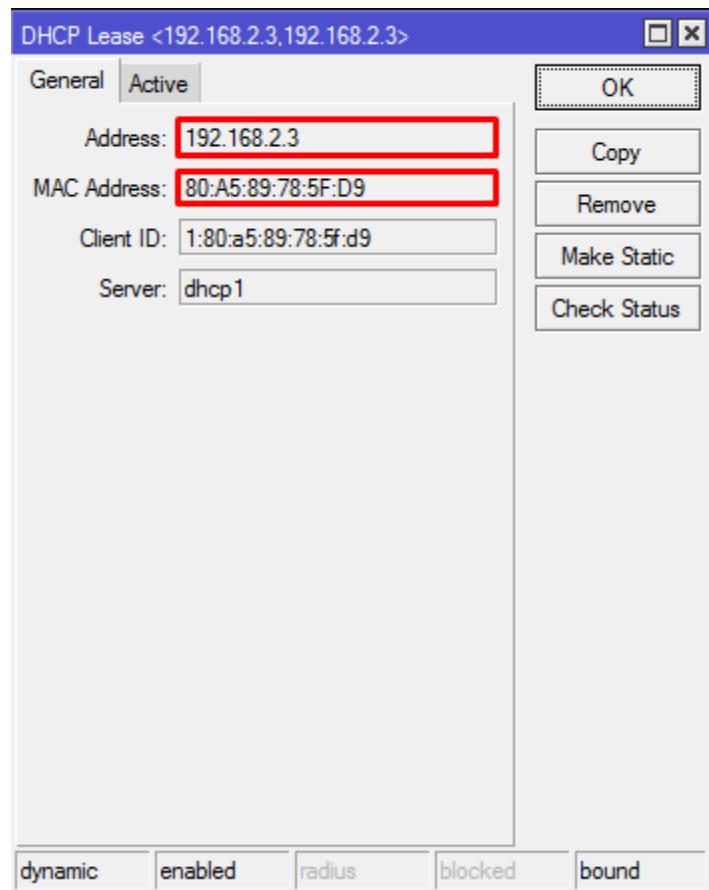
Pool	Address	Owner	Info
Unknown	192.168.2.254	DHCP	9C:5C:8F:DA:05:3D
DHCP 1	192.168.2.8	DHCP	80:A5:89:78:5F:D9

Selesai..

Lab 37. Management DHCP Server

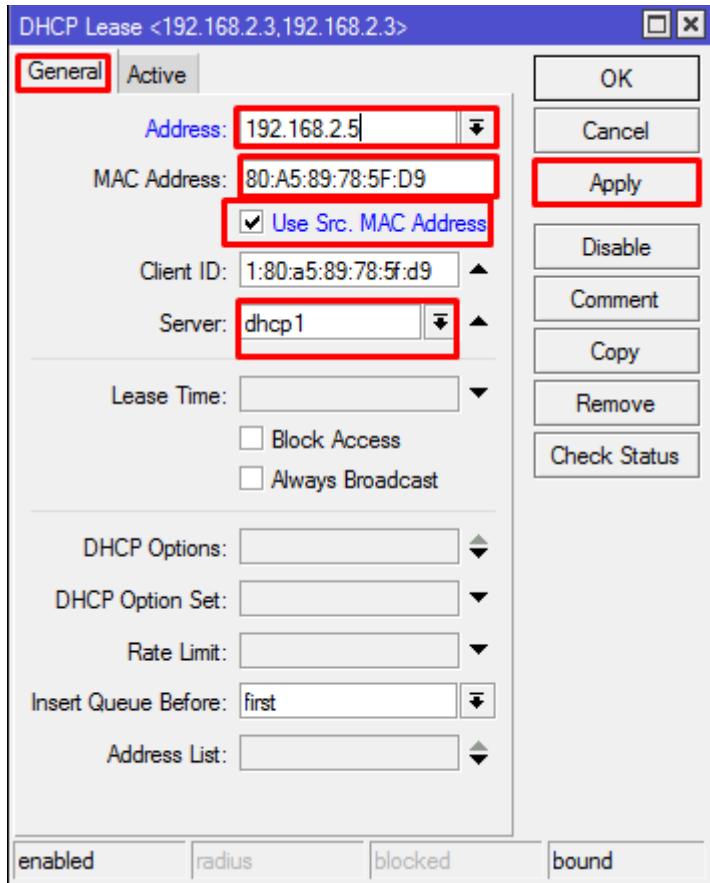
di lab ini kita akan mencoba untuk me-management DHCP Server,Pertama kita akan mencoba Untuk Memberikan IP Static Untuk Client,Contoh Jika Kita memiliki Jaringan Wireless dengan Network 192.168.2.0/24 dan kita ini PC dengan Mac-Address (80:A5:89:78:5F:D9) akan di berikan IP 192.168.2.5 secara static dari Router,maka artinya setiap PC dengan Mac-Address (80:A5:89:78:5F:D9) terhubung ke jaringan Wireless tersebut maka PC tersebut akan selalu mendapatkan IP 192.168.2.5 ,dan Untuk menggunakan Fitur tersebut kita akan menggunakan Parameter ARP

Pada Umum nya DHCP Server akan memberikan IP Secara Random/tidak beraturan

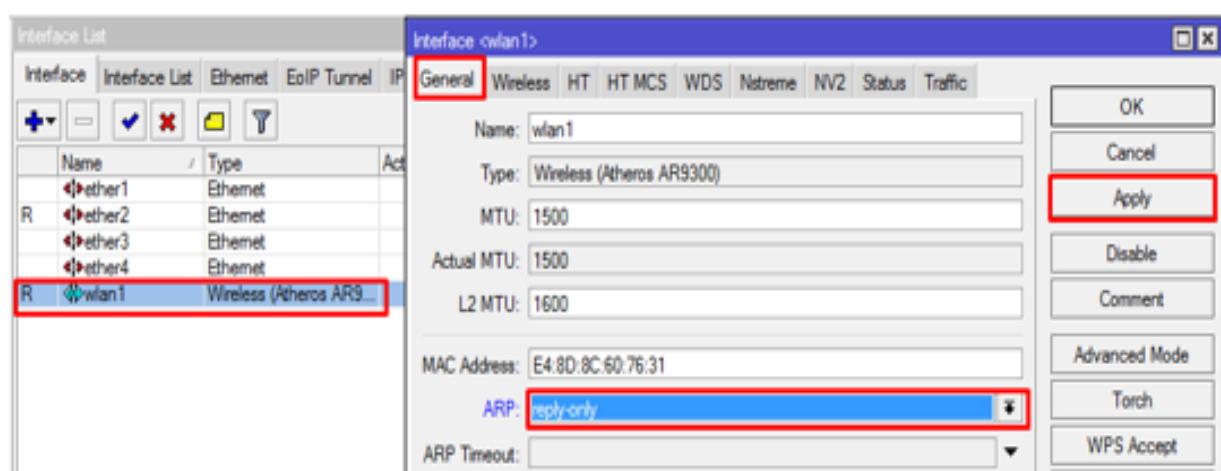


Jika Pertama PC tersebut mendapatkan IP 192.168.2.3 (IP Random) maka di sini kita akan men-Setting Static agar PC tersebut mendapatkan IP 192.168.2.5

- Klik Client DHCP Leases > Pilih salah satu Client > Klik Make Static
- Di General , Isi Address=192.168.2.5 , Checklist Use Src.MAC Address
- Lalu Apply dan OK



Selanjutnya kita akan Meng-Setting Parameter ARP=Replay-Only di Interface Wlan1.

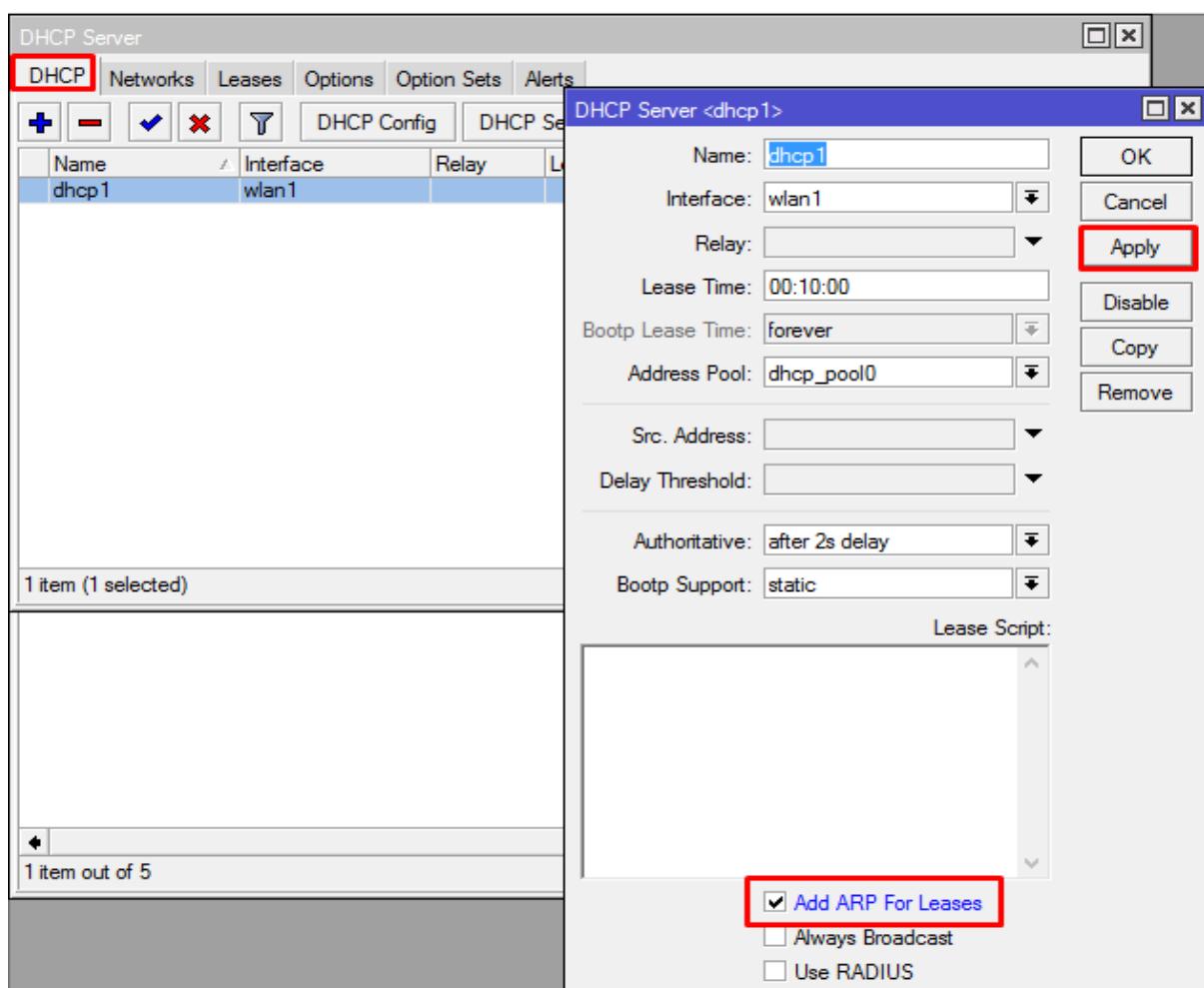


Jika sudah Coba Check IP Address pada PC tersebut, IP Address pada PC tersebut akan berubah menjadi 192.168.2.5

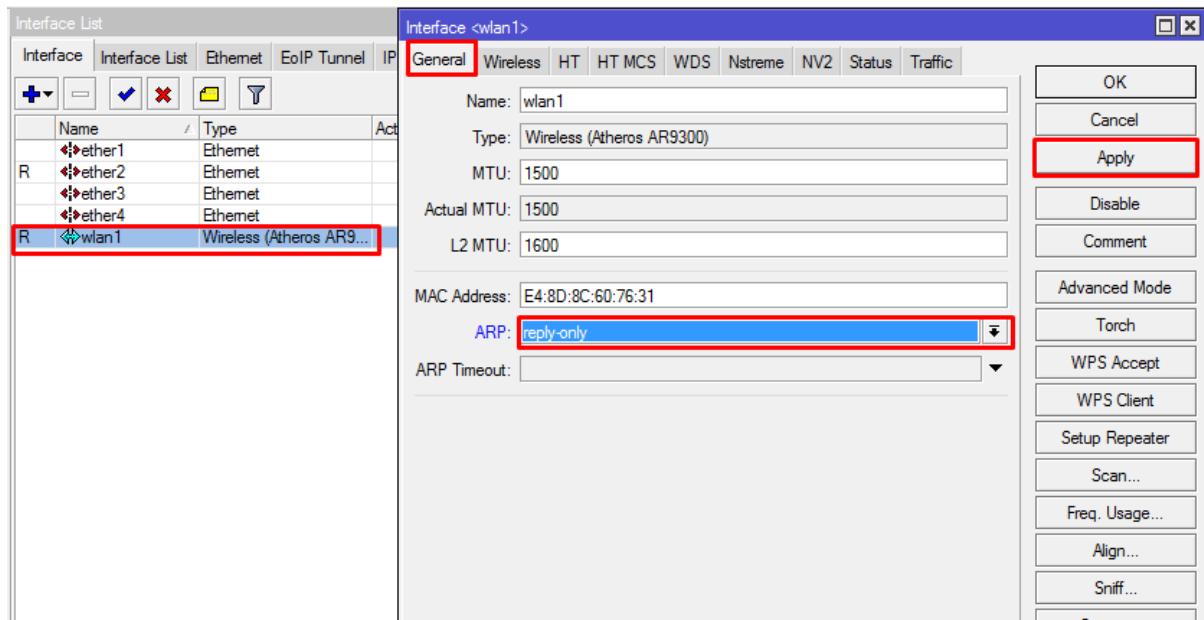
Adapter name: WiFi
SSID: Faris Jawad
Connection type: 802.11n
IPv4 address: 192.168.2.5
IPv6 address: fe80::e4b0:e10a:c271:8abb%8
Signal strength:

Selanjutnya kita akan mencoba Untuk Mensetting DHCP agar Client tidak dapat men-Setting IP Secara Static, jadi jika ada Client yang terhubung ke wireless kita dengan Menggunakan IP Static maka IP tersebut tidak Valid.

- Masuk Ke Rule DHCP Server yang telah kita buat
- Lalu Checklist Add ARP For Leases



Selanjutnya Kita akan meng-Setting Parameter ARP=Reply-Only di interface Wlan1



- Lalu Appy dan OK

Selesai

Lab 38. Membuat Web Proxy di Mikrotik

Di lab ini kita akan mencoba Membuat Web Proxy, Proxy adalah suatu aplikasi yang menjadi perantara antara client dengan server, sehingga client tidak akan berhubungan langsung dengan server-server yang ada di Internet. Mikrotik memiliki fitur Web proxy yang bisa digunakan sebagai proxy server yang nantinya akan menjadi perantara antara browser user dengan web server di Internet...

Keuntungan menggunakan Web Proxy

Fungsi dari proxy secara umum adalah sebagai Caching, Filtering, dan Connection Sharing. Semua fungsi ini dapat anda temui pada Web Proxy Mikrotik.

1. Caching

Web Proxy Mikrotik dapat melakukan caching content yaitu menyimpan beberapa konten web yang disimpan di memori Mikrotik. Konten tersebut akan digunakan kembali apabila ada permintaan pada konten itu lagi.

2. Filtering

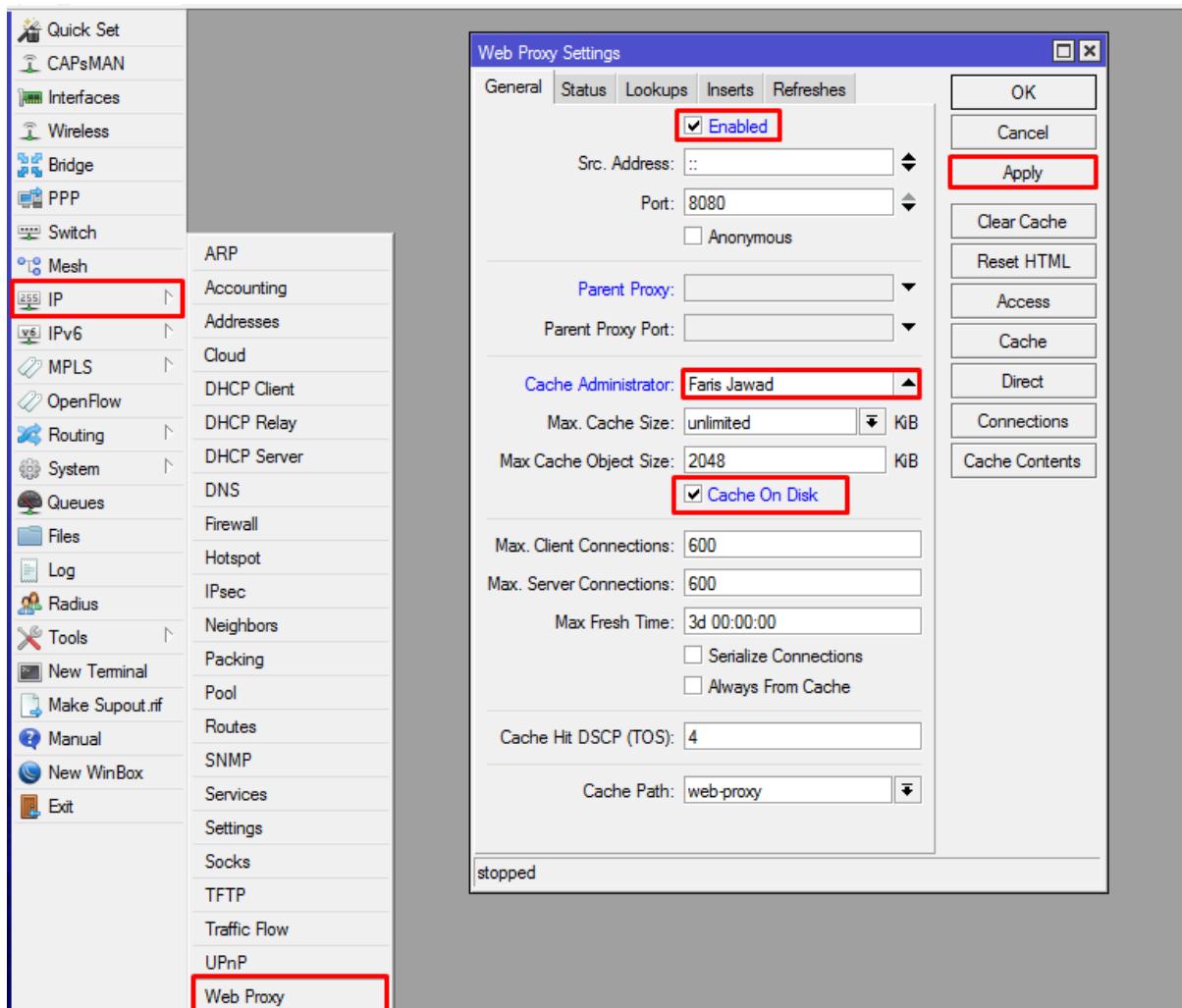
Dengan menggunakan Web Proxy anda dapat membatasi akses konten-konten tertentu yang di-request oleh client. Anda dapat membatasi akses ke situs tertentu, ekstensi file tertentu, melakukan redirect (pengalihan) ke situs lain, maupun pembatasan terhadap metode akses HTTP. Hal tersebut tidak dapat anda lakukan jika hanya menggunakan NAT.

3. Connection Sharing

Web Proxy meningkatkan level keamanan dari jaringan anda, karena computer user tidak berhubungan langsung dengan web server yang ada di Internet.

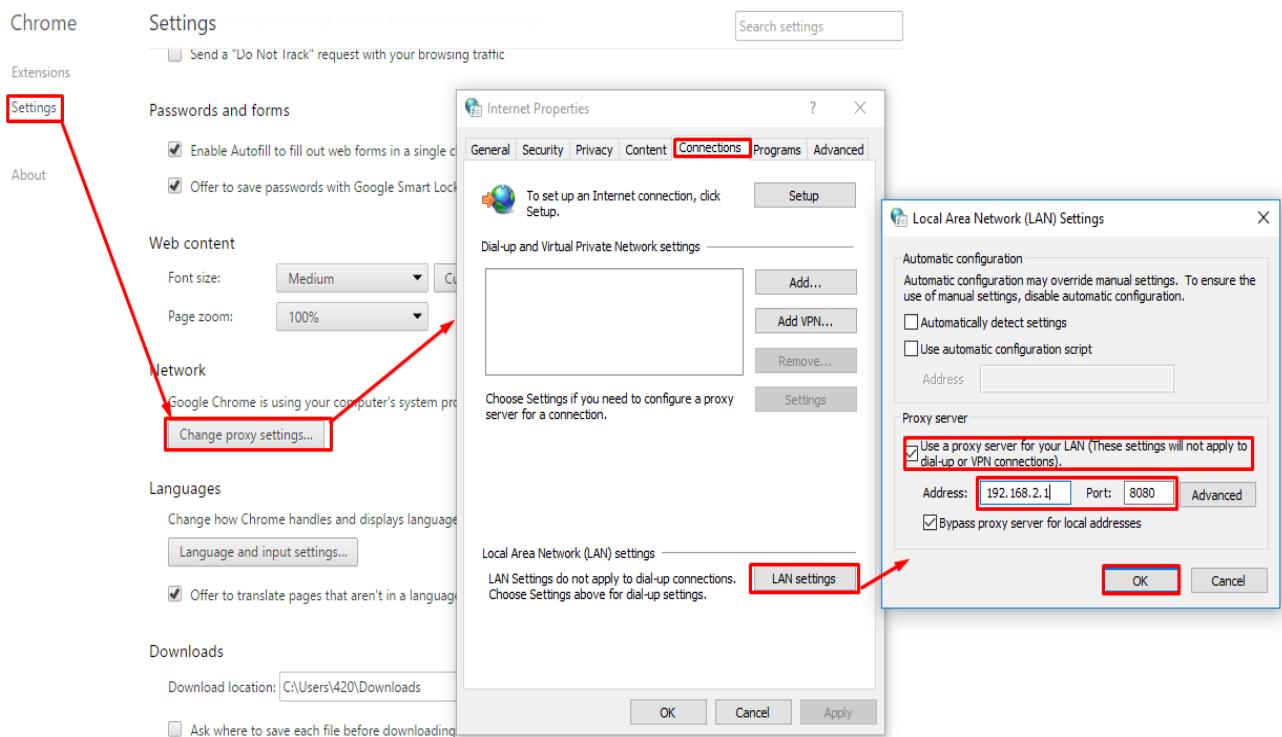
Selanjutnya buat Web Proxy terlebih dahulu..

- Klik IP > Web Proxy
- Checklist **Enable**, Isi Cache Administrator=Faris Jawad (Bebas), dan Checklist Cache On Disk
- Lalu Apply dan OK



Jika sudah maka Kita perlu men-Setting Proxy di Browser yang ada PC..

Isi Address=192.168.2.1(IP Router) dan Isi Port=8080



Jika sudah melewati step ini maka Web Proxy telah selesai..

Untuk pengetesan Coba kita Masukan 192.168.10.2 (IP Asal) di URL.

Maka Hasil nya adalah Halaman yang di blokir Oleh Web Proxy



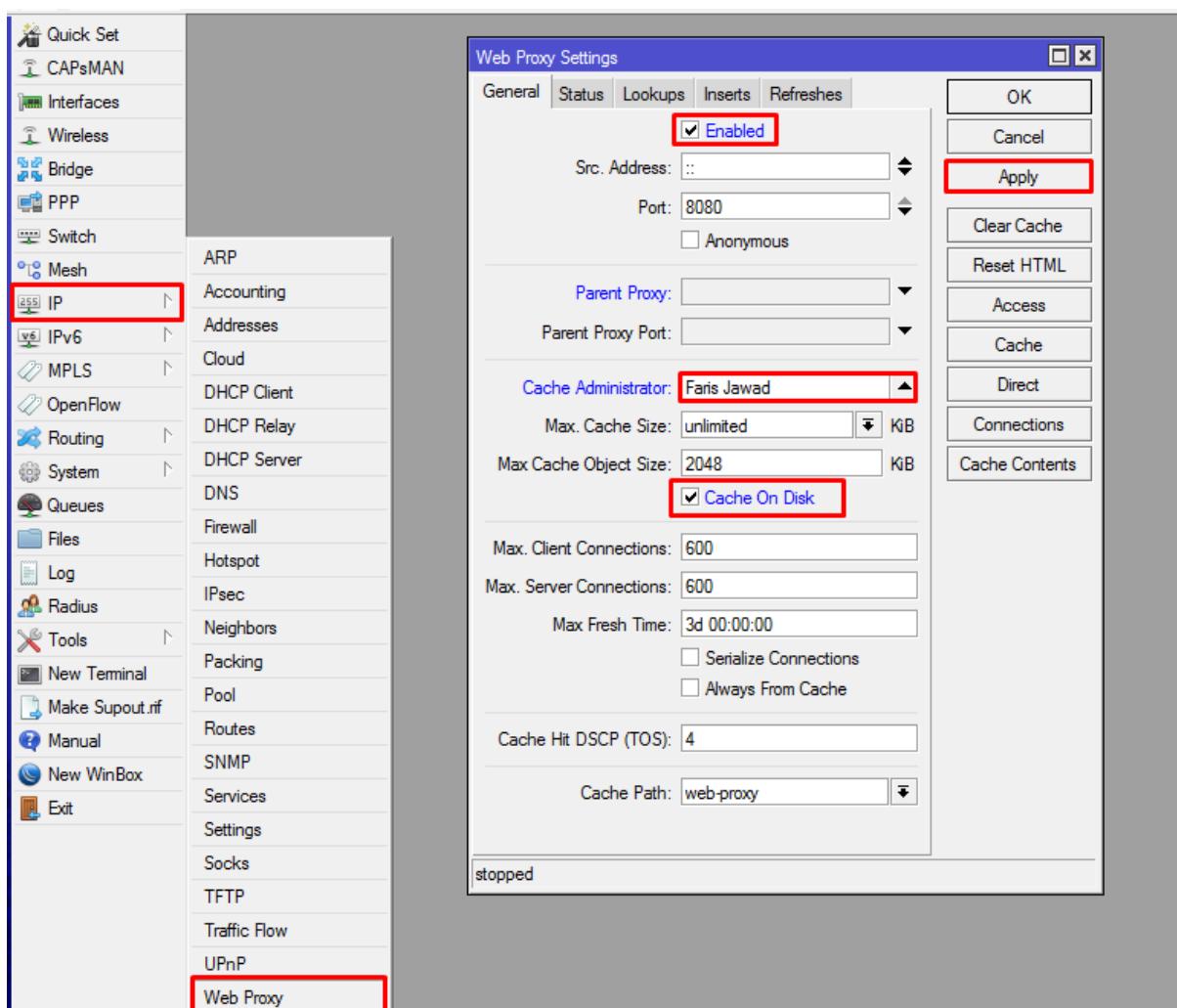
Selesai... ☺

Lab 39. Membuat Transparent Proxy di Mikrotik

Jika di lab sebelumnya kita telah membuat Web Proxy, di lab ini kita akan membuat Transparent Proxy yang berfungsi agar Client tidak perlu men-setting Proxy secara manual.. kita hanya perlu menambahkan Konfigurasi Nat agar traffic dari Internet di arahkan ke Web Proxy sebelumnya baru menuju Client..

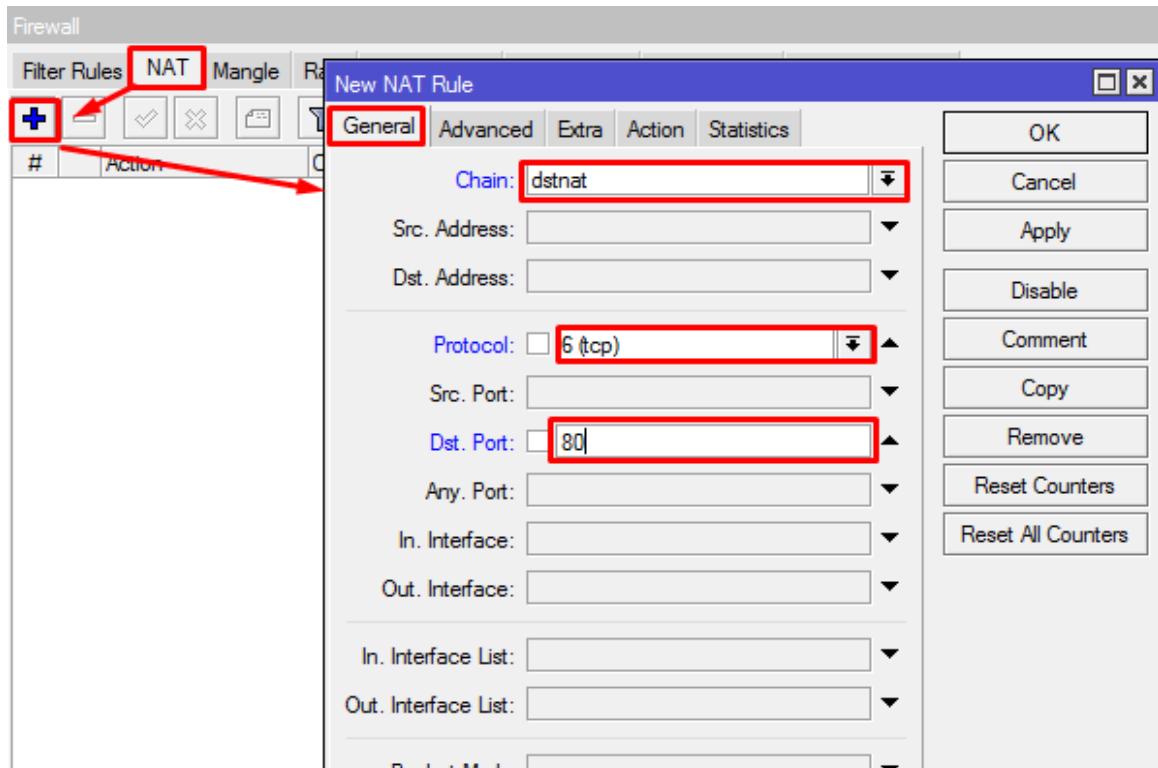
Pertama Kita perlu men-setting Web Proxy..

- Klik IP > Web Proxy
- Checklist **Enable**, Isi Cache Administrator=Faris Jawad (Bebas), dan Checklist Cache On Disk
- Lalu Apply dan OK



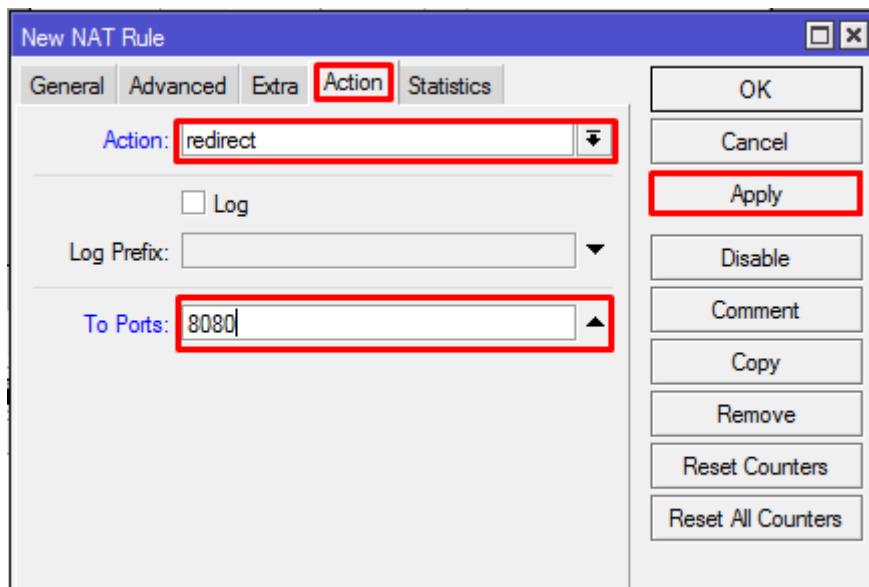
Selanjutnya kita akan membuat konfigurasi NAT..

- Klik IP > Firewall > NAT
- Isi Chain=DstNat ,Protocol=TCP ,Dst.Port=80



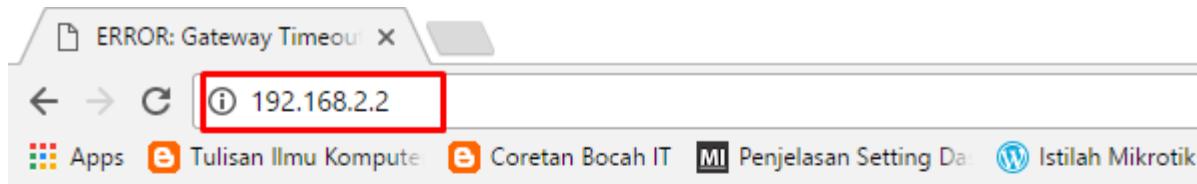
Selanjutnya Pindah ke Tab Action

- Pilih Action=Redirect ,dan Isi To Ports=8080
- Lalu Apply dan OK



Jika sudah membuat konfigurasi NAT tersebut maka Client tidak perlu mensetting Proxy di Browsernya

Hasil dari untuk Lab ini dan Lab yang sebelumnya akan sama .. Coba Isikan IP asal di URL browser..



ERROR: Gateway Timeout

While trying to retrieve the URL <http://192.168.2.2/>:

- No route to host

Your cache administrator is [Faris Jawad](#).

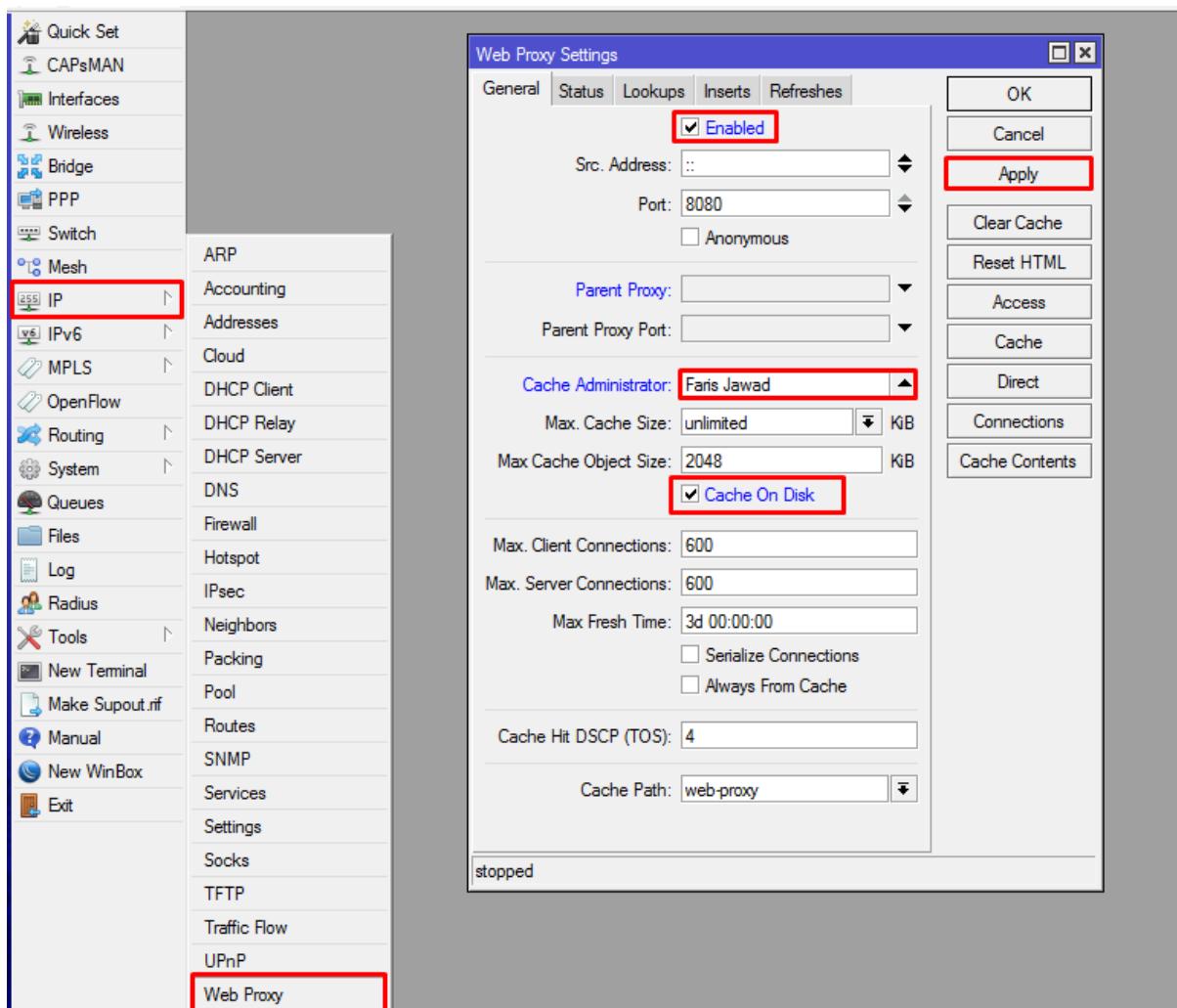
Generated Fri, 10 Mar 2017 03:14:05 GMT by :ffff:192.168.2.1 ([Mikrotik HttpProxy](#))

Lab 40. Meredirect Situs dengan Proxy

Jika di lab sebelumnya Web Proxy di gunakan untuk memblokir ke IP address yang tidak Valid,maka di lab ini Web Proxy akan di gunakan Untuk meredirect suatu situs ke situs yang lain..Contoh di sini saya akan Mencoba untuk mem-Blokir situs 1cak.com dan meredirect nya ke blog saya (farisjwd.wordpress.com)..

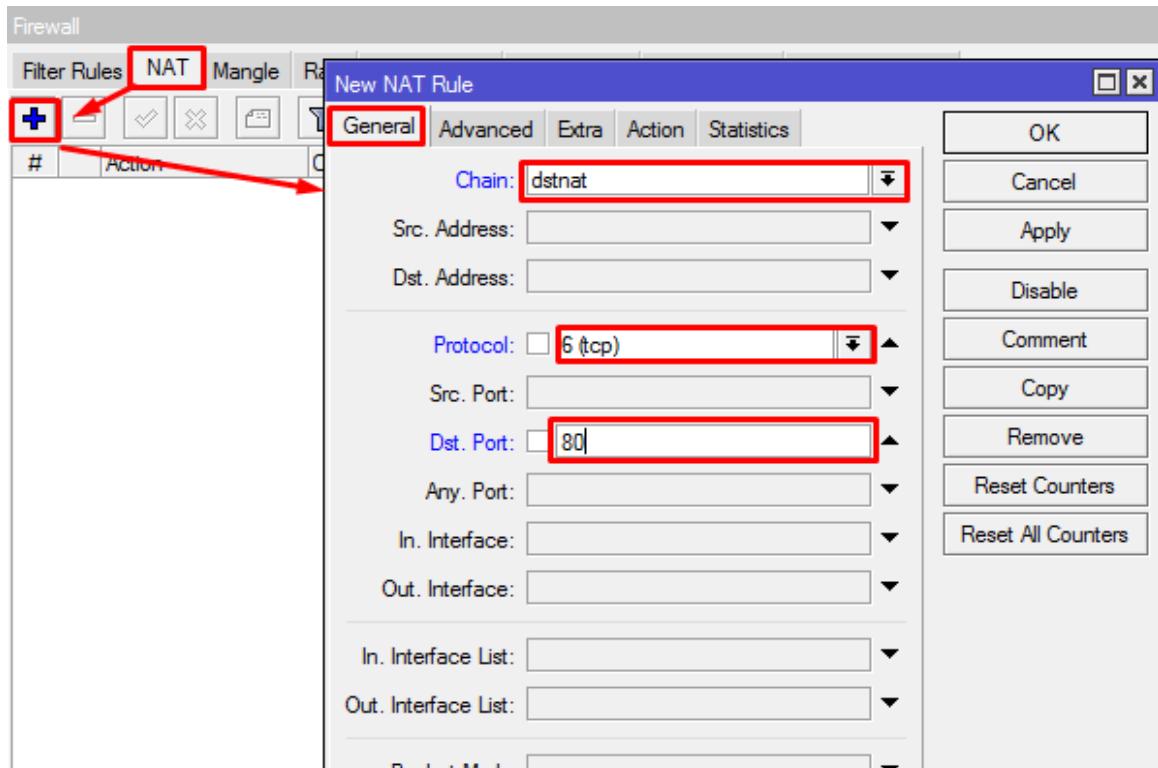
Buat Web Proxy terlebih dahulu..

- Klik IP > Web Proxy
- Checklist **Enable** ,Isi Cache Administrator=Faris Jawad (Bebas) ,dan Checklist Cache On Disk
- Lalu Apply dan OK



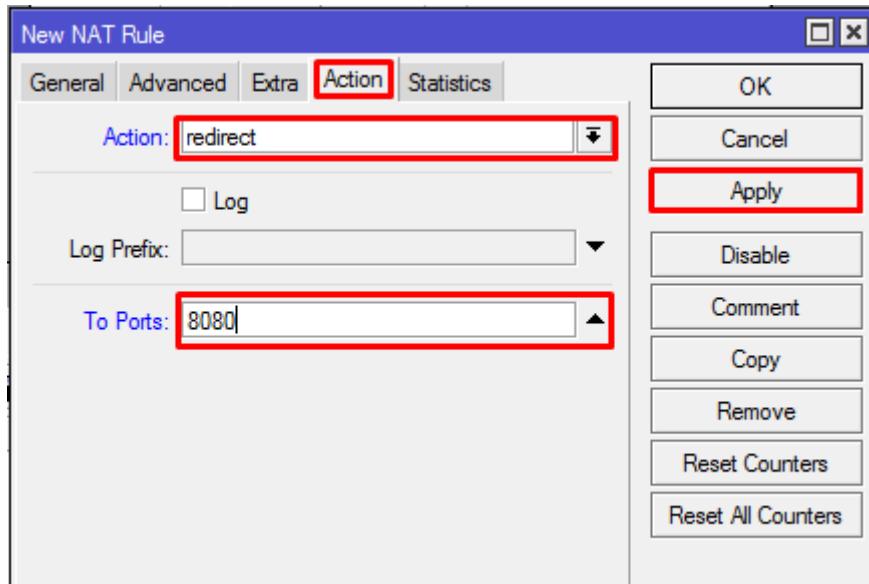
Selanjutnya kita akan membuat konfigurasi NAT..

- Klik IP > Firewall > NAT
- Isi Chain=DstNat ,Protocol=TCP ,Dst.Port=80



Selanjutnya Pindah ke Tab Action

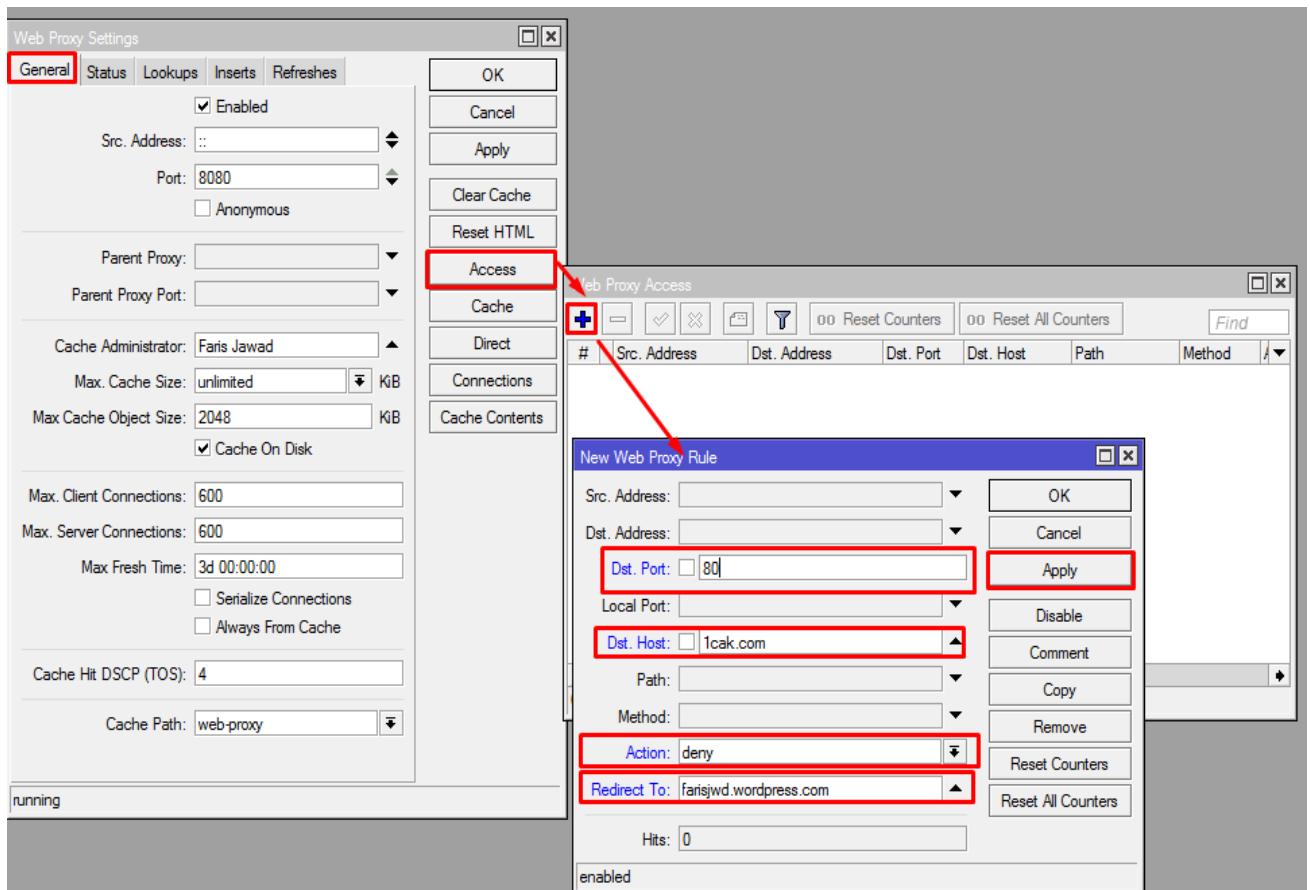
- Pilih Action=Redirect ,dan Isi To Ports=8080
- Lalu Apply dan OK



Selanjutnya kita akan membuat suatu Rule di Web Proxy yang berfungsi untuk memblokir situs 1cak.com tersebut dan meredirect nya ke situs farisjwd.wordpress.com,

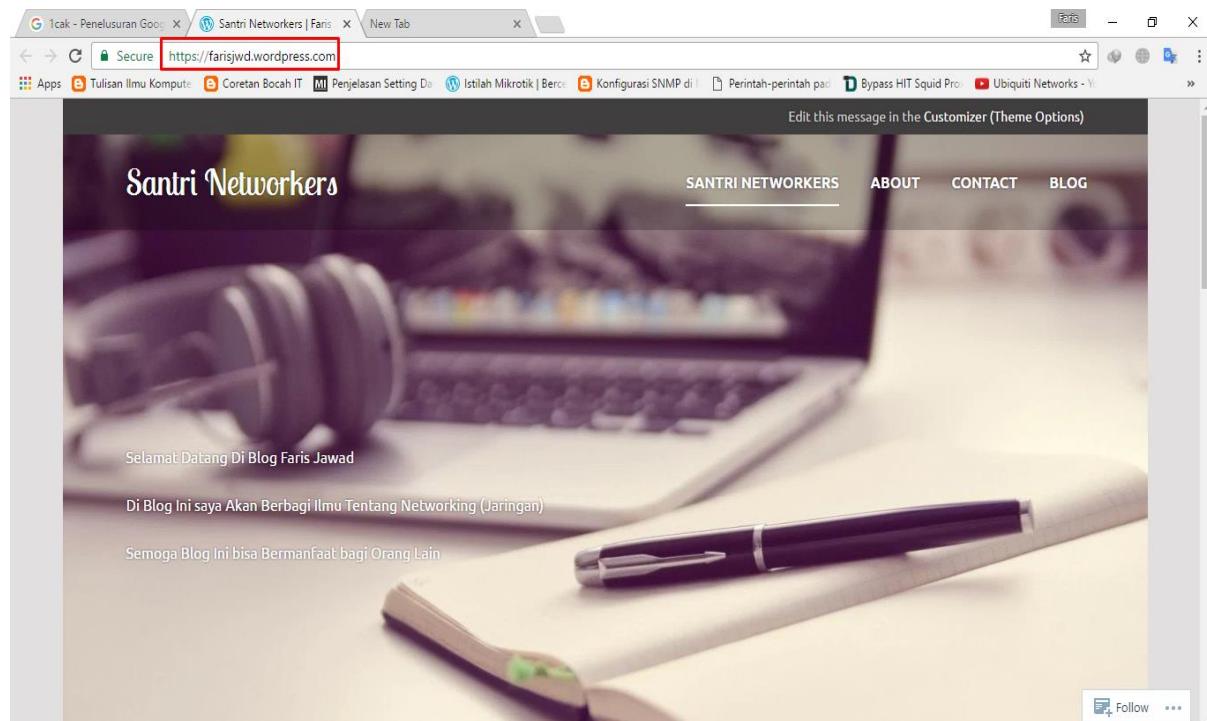
Buka Web Proxy yang telah kita buat.

- Pada Tab General ,lalu Klik menu Access
- Klik Add (+) > Isi Dst.Port=80 ,Dst.Host=1cak.com (Website yang akan di Redirect) ,Action=Deny , Redirect To=farisjwd.wordpress.com (Website Untuk Redirect)
- Lalu Apply dan OK



Jika kita telah membuat Rule di Web Proxy tersebut ,Maka Rule Tersebut bisa dibaca: Jika ada yang mengunjungi 1cak.com dengan menggunakan Protocol TCP Port 80 maka akan di Tolak dan akan di Redirect ke farisjwd.wordpress.com

Untuk Pengetesan Coba buka Website 1cak.com ,maka hasil nya akan terbuka website farisjwd.wordpress.com ☺

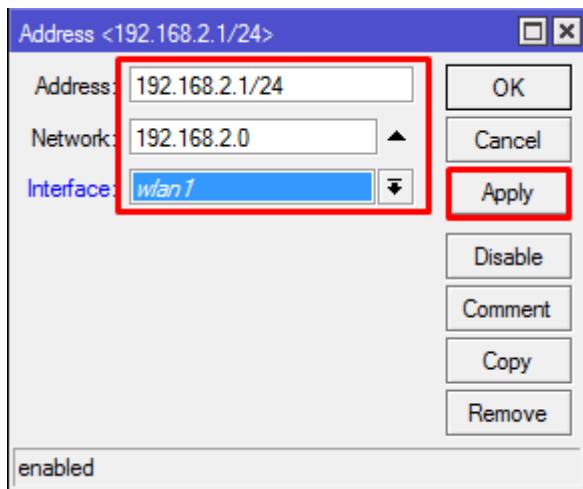


Lab 41. Mengatasi NetCut dengan Mikrotik

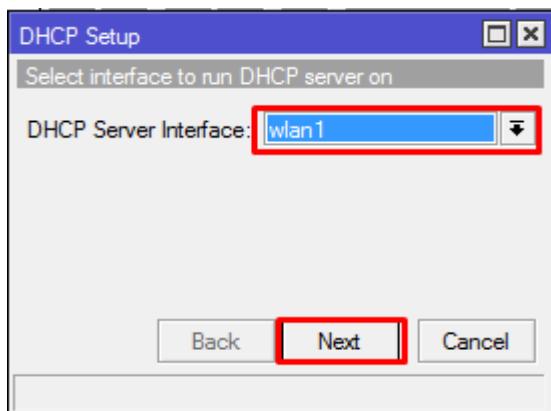
NetCut adalah aplikasi yang dapat memutuskan jaringan Client yang terhubung dalam satu jaringan LAN, di jaman sekarang sangat banyak orang yang menggunakan aplikasi ini di karenakan mereka ingin mendapatkan bandwidth dengan kecepatan yang tinggi, Router Mikrotik Memiliki cara untuk mengatasi NetCut tersebut...

Contoh: di lab ini kita akan mencoba membuat jaringan Wireless yang aman dari NetCut..

Pertama buat IP Address untuk interface Wlan 1,



Selanjutnya kita buat DHCP server untuk Wlan 1 tersebut

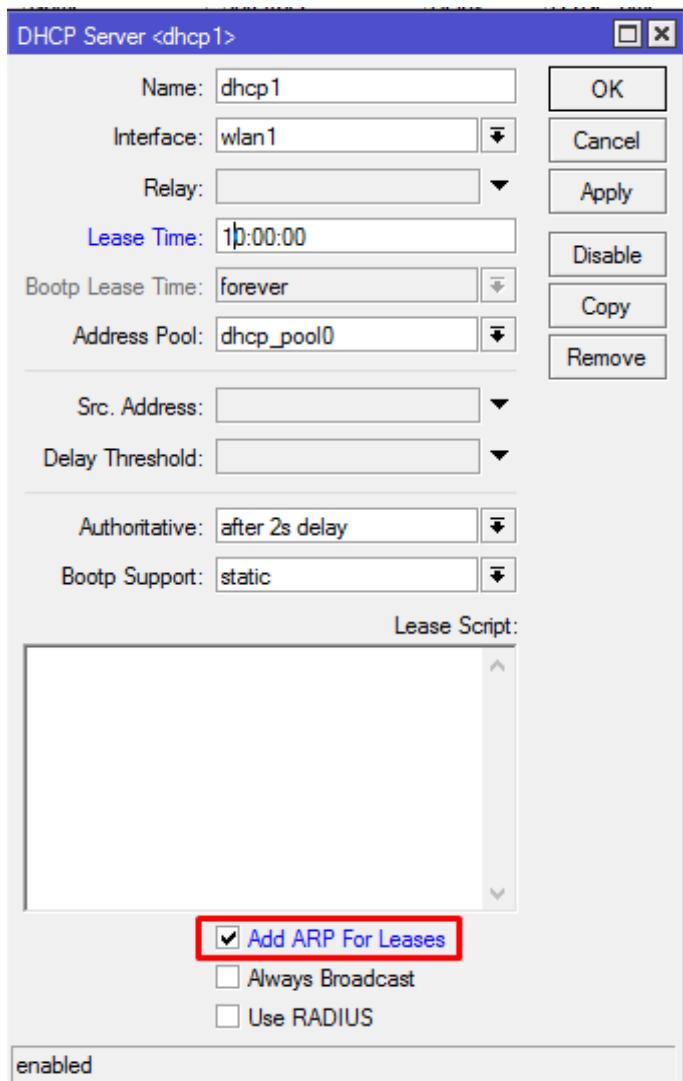


Lalu next next saja sampai selasai proses pembuatan DHCP server..

Name	/	Interface	/	Relay	Lease Time	Address Pool	Add AR...	▼
dhcp1		wlan1			00:10:00	dhcp_pool2	no	

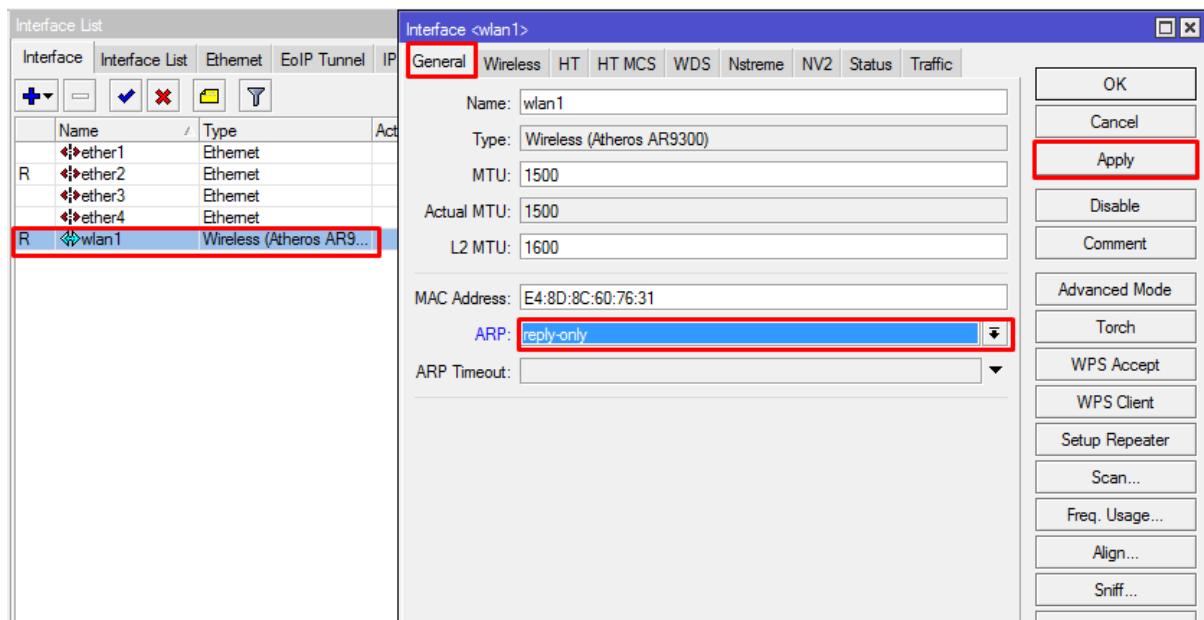
Selanjutnya kita akan meng-Aktive kan Fitur ARP Pada DHCP Tersebut dan Pada Interface Wlan 1..

Mensetting ARP di DHCP Server



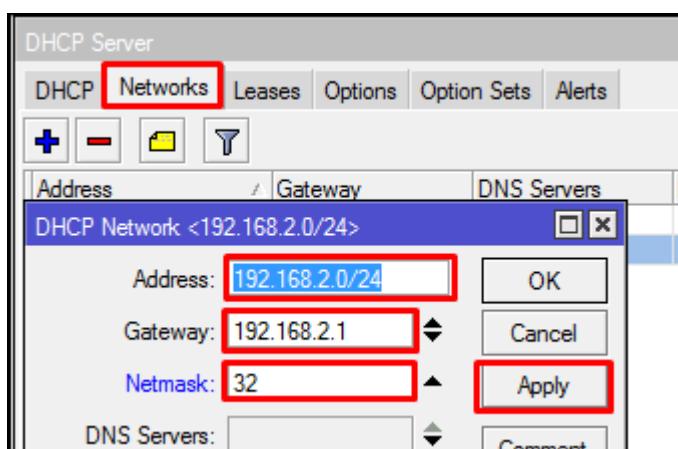
Jika sudah Apply dan OK

Step selanjutnya adalah mensetting ARP=Reply-Only di Interface Wlan1



Jika sudah Maka Kita akan meng-Edit lagi Network pada DHCP tersebut..

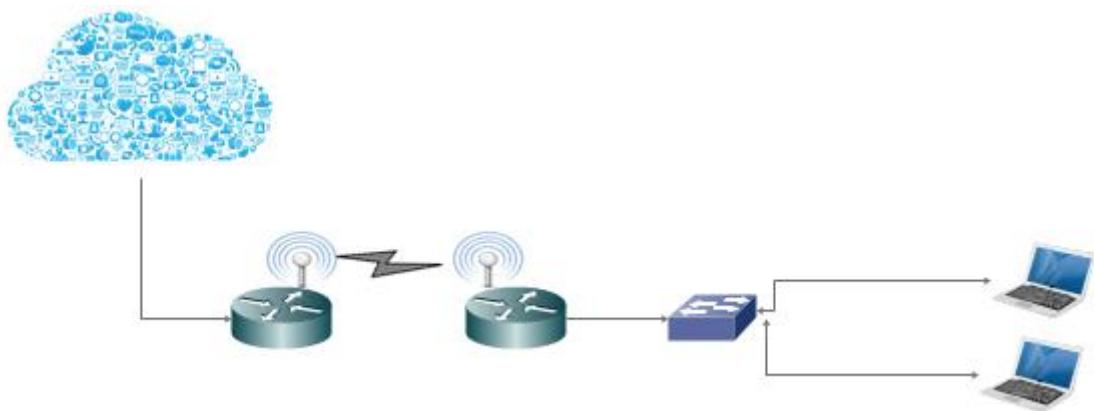
Pada DHCP Network Kita isi Netmask=32



Jika sudah Melewati Step ini maka jaringan kita akan aman dari serang NetCut,Jika ingin lebih aman lagi Drop Packet Ping yang masuk ke dalam router,karna NetCut menggunakan Protocol ICMP..

Selesai..

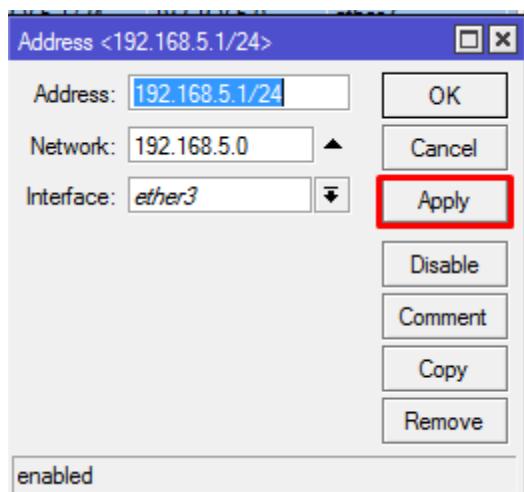
Lab 42. Hotspot Via Ethernet



Di lab ini kita akan mencoba membuat Hotspot Via Ethernet, Hotspot berfungsi untuk mempermudah management client, jika ada client yang ingin terhubung dengan internet maka client tersebut harus login terlebih dahulu dengan username dan password yang telah di tentukan .. Biasanya Hotspot di setting untuk Wireless , Tetapi di lab ini kita akan mencoba Untuk mensetting hotspot dengan menggunakan Ethernet..

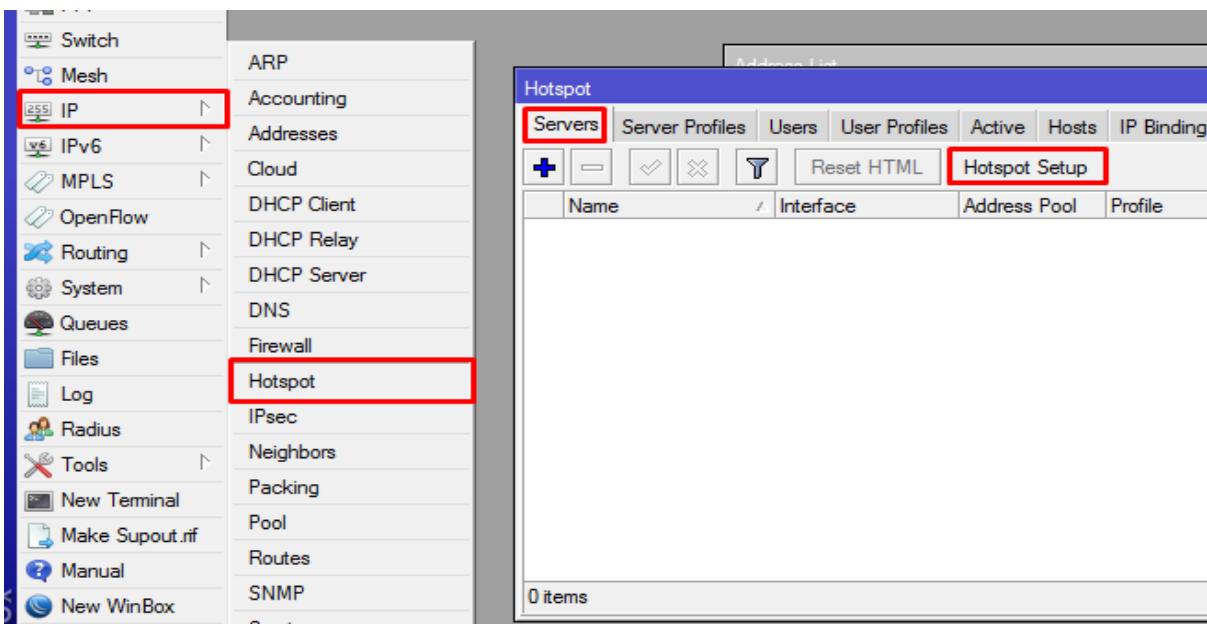
Setting Wireless agar Router dapat terhubung ke internet Setting NAT dan Lain-Lain.. dan Setting IP Address 192.168.5.1/24 untuk interface=Ether3 (mengarah ke Client).

Setting IP Address Ethernet 3



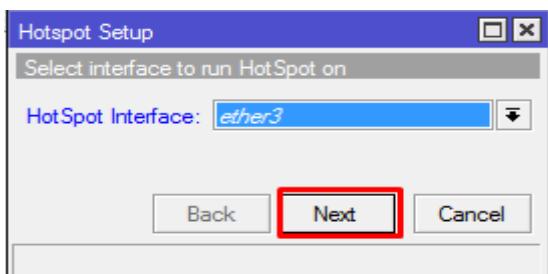
Selanjutnya kita Akan Membuat Hotspot..

- Klik IP > Hostpot > Server > Hotspot Setup

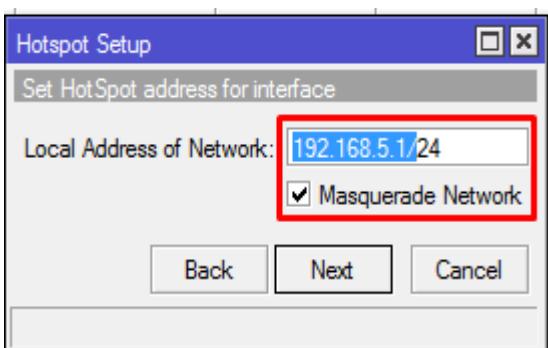


Seanjutnya akan keluar sebuah Box Hotspot Setup. Kita hanya tinggal menyesuaikan..

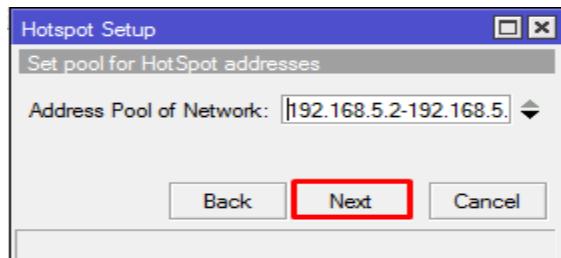
- Pilih Interface=Ether3
- Lalu Next



- Isi IP Ether 3 dan Checklist Masquerade Network
- Lalu Next



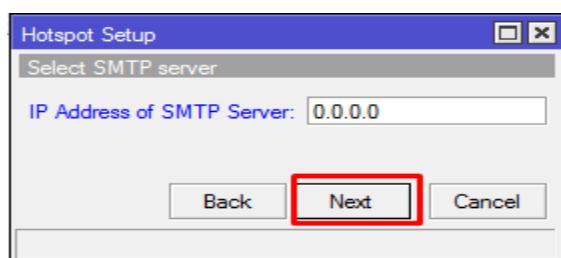
- Isi IP Range Sesuai Keinginan kita, IP Address yang akan di berikan kepada Client.
- Lalu Next



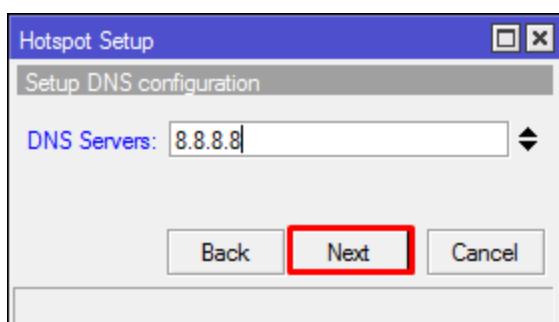
- Isi Certificate=None
- Lalu Next



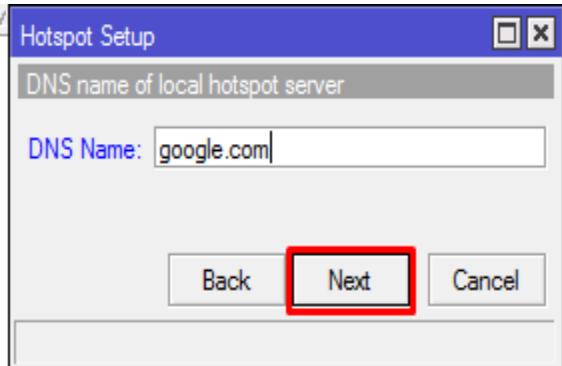
- Isi SMTP Server 0.0.0.0
- Lalu Next



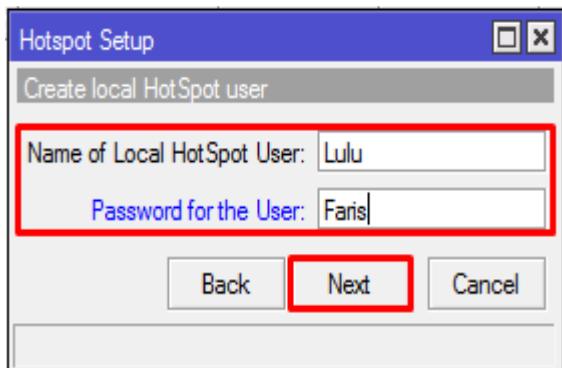
- Isi DNS Server=8.8.8.8
- Lalu Next



- Isi DNS Name=google.com
- Lalu Next



- Isi Name=Lulu dan Password=Faris
- Lalu Next



Setelah Step Ini maka User untuk hotspot telah selesai di buat...

User ini di buat agar Client dapat melewati proses autentikasi,karna pada saat Proses autentikasi clien perlu memasukan User yang telah di tentukan ..jika tidak memasukan User maka Client tidak akan mendapatkan akses Internet dari Router..

Selanjutnya kita akan mencoba menggunakan User tersebut agar Client bisa mendapatkan akses internet..

Kita bisa mencobanya di Browser ,Coba ketik apa saja di URL, maka Otomatis Url akan di redirect ke halam login Hotspot,selanjutnya masuk User yang telah kita buat.



Isi Login=Lulu dan Password=Faris

Lalu Ok..

Setelah Kita login maka akan keluar Text Box yang ber-Isikan tentang User yang kita gunakan..

Welcome Lulu!	
IP address:	192.168.5.254
bytes up/down:	1378 B / 0 B
connected:	0s
status refresh:	1m

Jika sudah Login ,maka Client sudah mendapatkan Akses Internet.. 😊

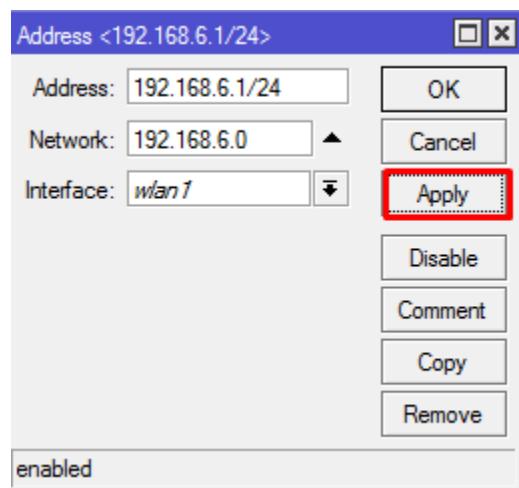
Lab 43. Hotspot Via Wireless



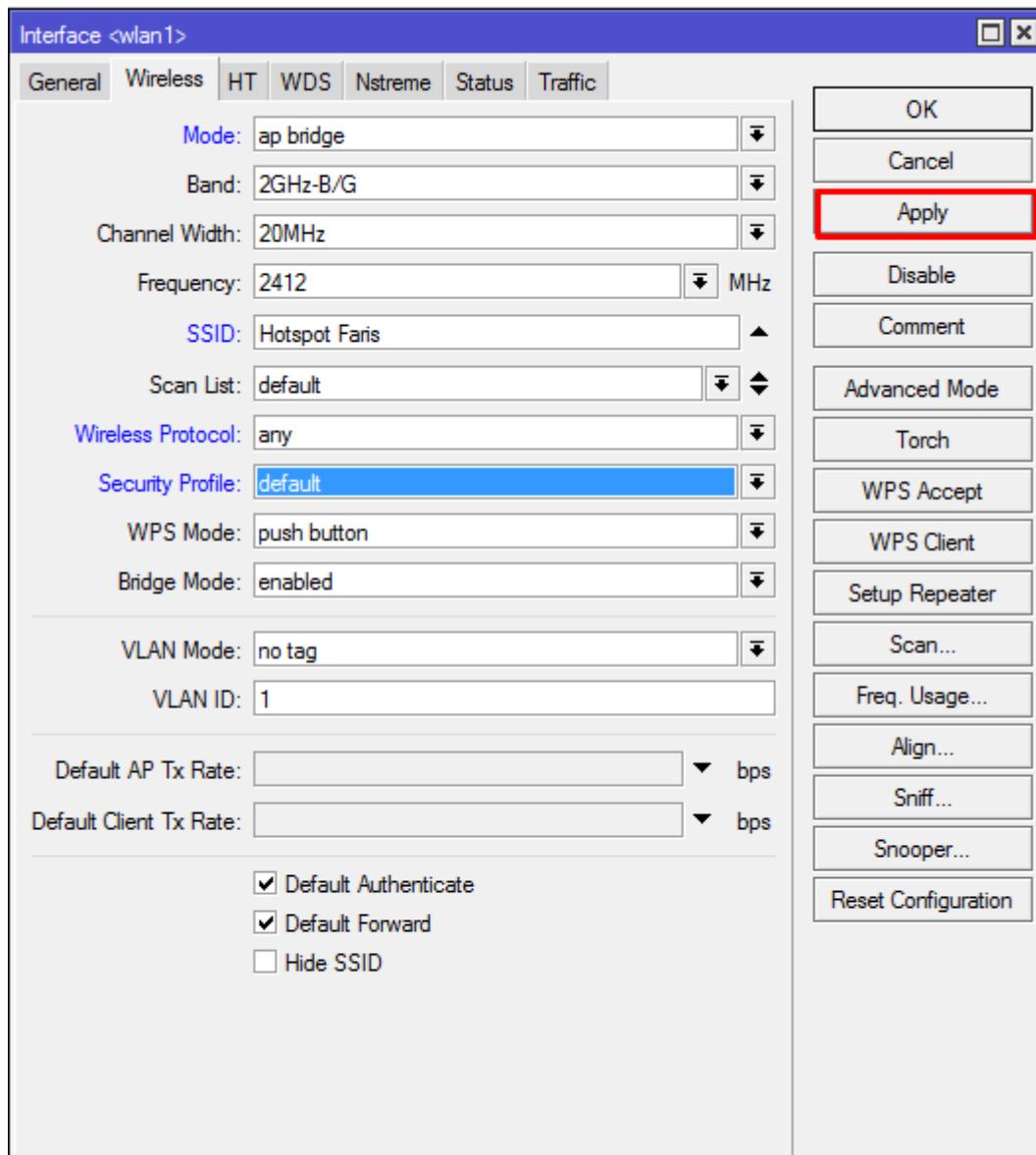
Jika pada lab sebelumnya Client terhubung dengan router dengan menggunakan ethernet maka di lab ini client terhubung dengan Router dengan Wireless dan router terhubung ke Internet melalui Ether 1

Setting Ether1 agar Router dapat terhubung ke internet Setting NAT dan lain lain dan Setting IP Address 192.168.6.1/24 untuk interface=Wlan1 (mengarah ke Client).

Setting IP Address

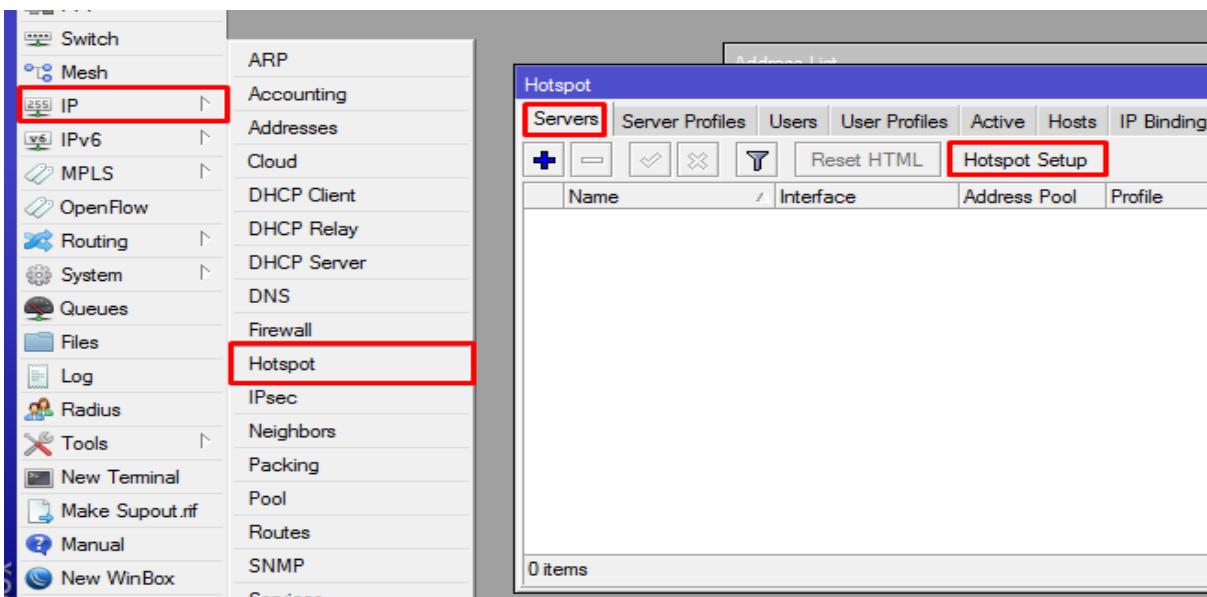


Selanjutnya Kita Setting Wireless denag Mode Access Point Untuk Agar Client dapat terkoneksi ke Router..



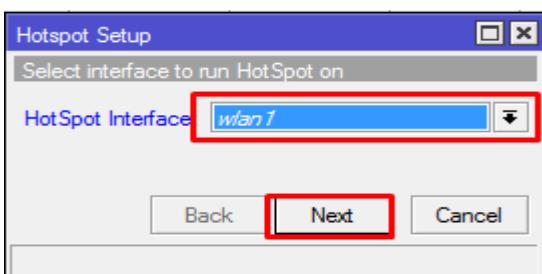
Jika Sudah Kita akan membuat Hostpot menggunakan Inteface Wlan1..

- Klik IP > Hostpot > Server > Hotspot Setup

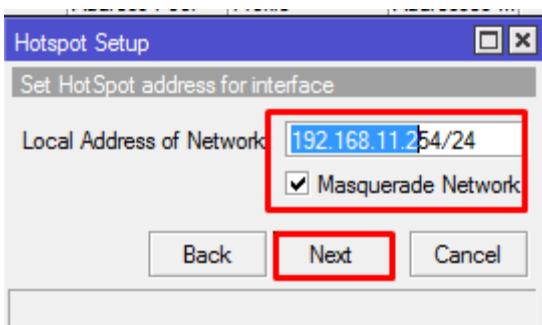


Seanjutnya akan keluar sebuah Box Hotspot Setup. Kita hanya tinggal menyesuaikan Sesuai Keinginan kita..

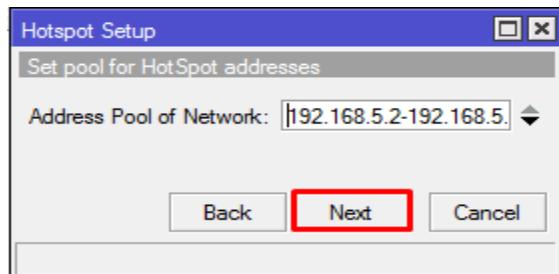
- Pilih Interface=Wlan1
- Lalu Next



- Isi IP Wlan1 dan Checklist Masquerade Network
- Lalu Next



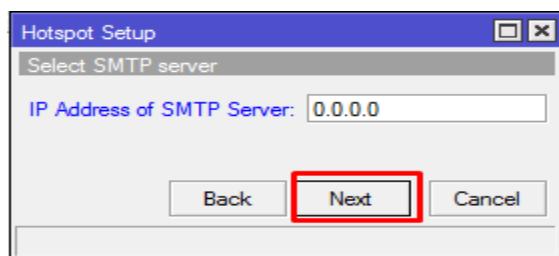
- Isi IP Range Sesuai Keinginan kita, IP Address yang akan di berikan kepada Client.
- Lalu Next



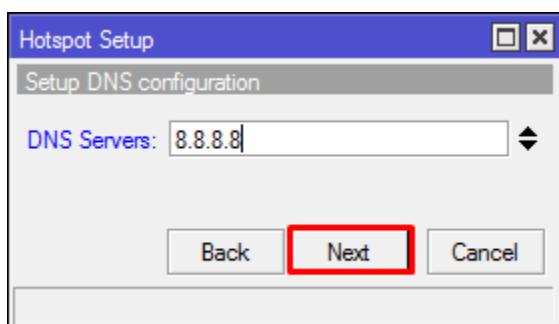
- Isi Certificate=None
- Lalu Next



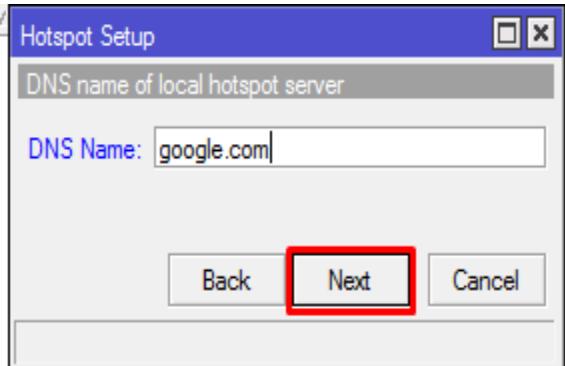
- Isi SMTP Server 0.0.0.0
- Lalu Next



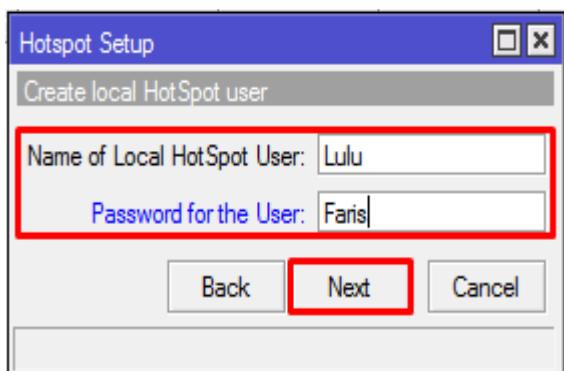
- Isi DNS Server=8.8.8.8
- Lalu Next



- Isi DNS Name=google.com
- Lalu Next



- Isi Name=Lulu dan Password=Faris
- Lalu Next



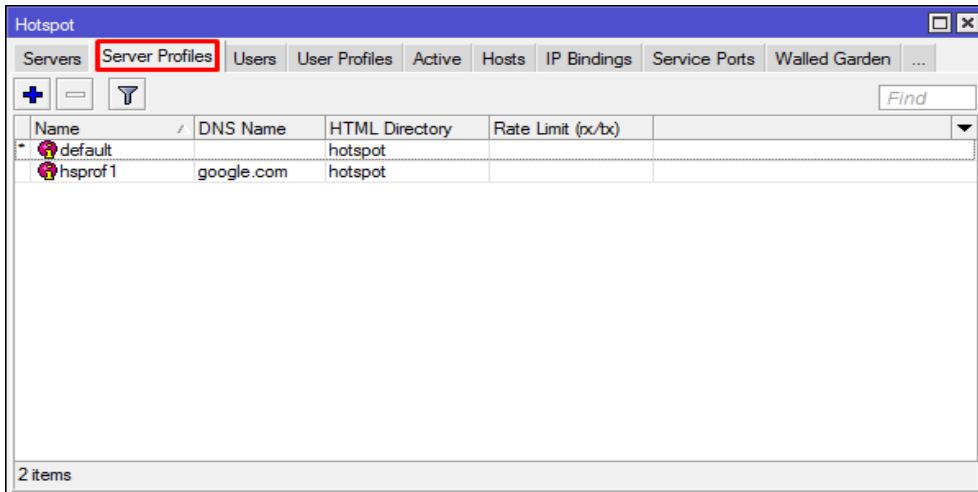
Jika sudah melewati step ini maka User bisa di gunakan Client untuk login hotspot..



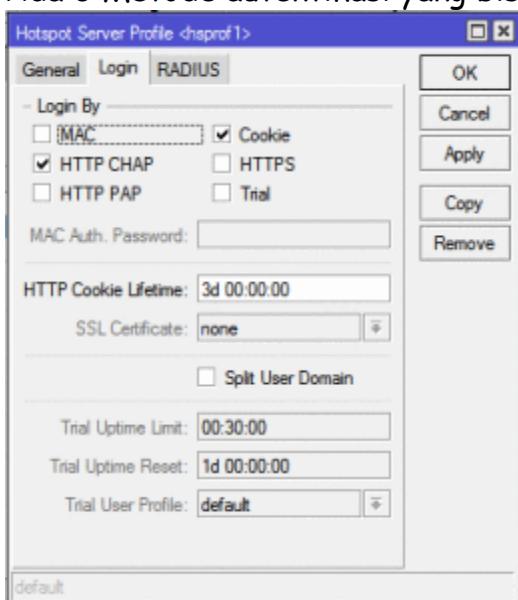
Lab 44. Fitur Hotspot

Jika kita mensetting Hotspot Kita bisa menggunakan Fitur yang telah di sediakan oleh mikrotik untuk melakukan management Hotspot ,Fitur Fitur Hotspot untuk management Hotspot

- Server Profile



Hotspot Server Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari beberapa hotspot server. Profile ini digunakan untuk grouping beberapa hotspot server dalam satu router. Pada server profile terdapat konfigurasi yang berpengaruh pada user hotspot seperti : Metode Autentikasi. Ada 6 Metode autentifikasi yang bisa digunakan di Server Profile.



Pada menu Server Profile ini terdapat fitur-fitur yang ada dalam Hotspot MikroTik yaitu :

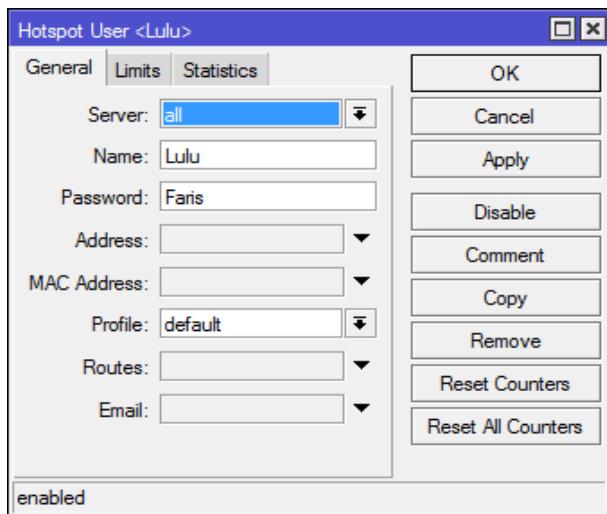
- *MAC Address* : metode ini akan mengautentikasi user mulai dari user tersebut muncul di 'host-list', dan menggunakan *MAC address* dari client sebagai username dan password.
- *HTTP CHAP* : metode standard yang mengintegrasikan proses *CHAP* pada proses login.
- *HTTP PAP* : metode autentikasi yang paling sederhana, yaitu menampilkan halaman login dan mengirimkan info login berupa plain text.
- *HTTPS* : menggunakan Enkripsi Protocol SSL untuk Autentikasi.
- *HTTP Cookie* : setelah user berhasil login data cookie akan dikirimkan ke web-browser dan juga disimpan oleh router di 'Active HTTP cookie list' yang akan digunakan untuk autentikasi login selanjutnya.
- *Trial* : User tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.

- **Users**

Server	Name	Address	MAC Address	Profile	Uptime
::: counters and limits for trial users					
all	Lulu			default	00:39:55
					00:00:00

2 items

Pada menu ini digunakan untuk mengelola User yaitu untuk mengelola Client yang terkoneksi dengan Hotspot kita. Pada menu ini juga mempunyai fitur untuk melimitasi penggunaan yang dilakukan oleh User.



Gambar tersebut adalah submenu yang ada didalam Users, pada submenu tersebut terdapat 3 menu yaitu :

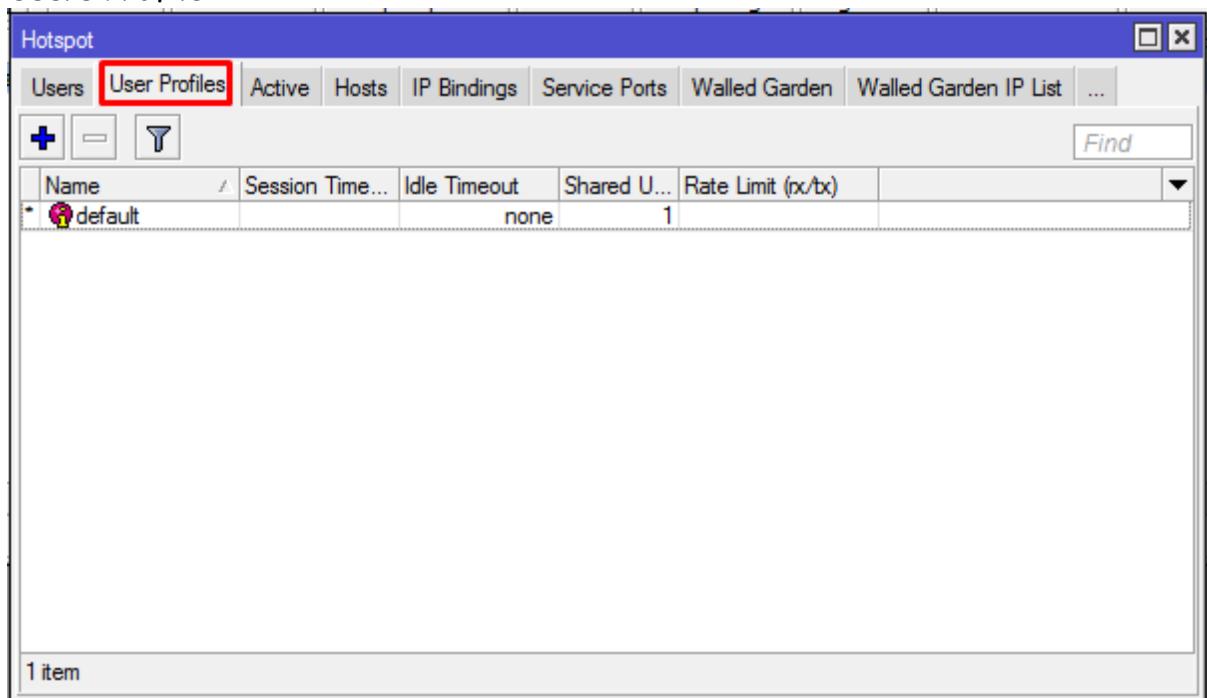
- General

- Limits : pada menu ini terdapat fitur yang digunakan untuk limitasi berdasarkan berapa lama user akses jaringan (*uptime*), kecepatan akses (*data rate*), banyak data yang sudah digunakan (*quota based*), bahkan kebijakan *policy firewall*.

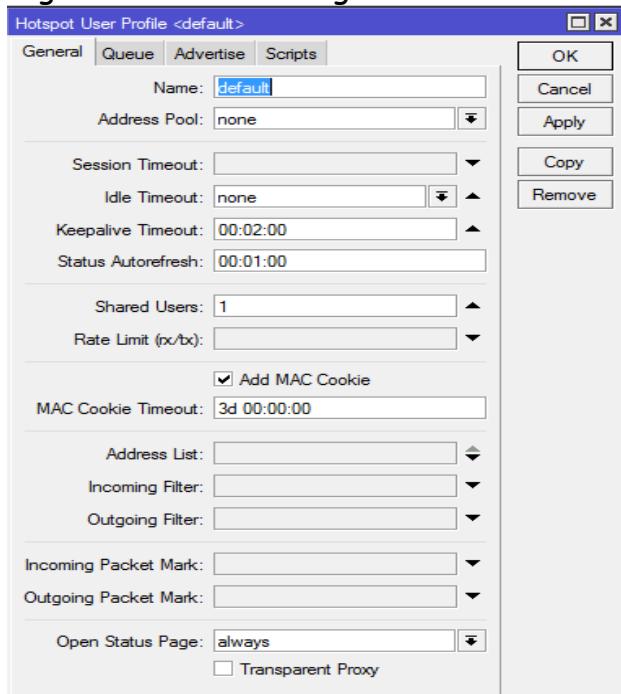
Limitasi ini bisa diterapkan per user atau mungkin per group dari jaringan.

- Statistics : digunakan untuk melihat data statis dari user.

- **Users Profile**



Digunakan untuk konfigurasi umum dari user Hotspot



Pada submenu tersebut juga terdapat menu :

- General : digunakan untuk mengkonfigurasi User
- Assign poolip pada group user
- Time-out(untuk mencegah monopoli oleh user)
- Data rate (kecepatan akses)
- Session time (sesi akses)
- Shared Users : mensharing banyak user yang dapat menggunakan Hotspot tersebut dengan satu akun
- Address List : IP user akan ditambahkan ke dalam firewall addresslist sesuai list yang ditentukan
- Incoming Filter : Nama chain baru untuk trafik yang berasal dari IP user (trafik upload)
- Outgoing Filter : Nama chain baru untuk trafik yang menuju IP user (trafik download)
- Incoming Packet Mark : Nama packet-mark untuk trafik yang berasal dari IP user (trafik upload)
- Outgoing Packet Mark : Nama packet-mark untuk trafik yang menuju IP user (trafik download)
- Advertise : Dengan menggunakan fitur advertisement pada Hotspot server, berfungsi untuk menampilkan popup halaman sebuah web ke user dan popup-popup yang akan muncul bisa anda atur intervalnya.

- Active

Server	User	Domain	Address	Uptime	Idle Time	Session Time	Rx Rate	Tx Rate
hotspot1	admin		10.5.50.254	00:42:59	00:00:29		0 bps	0 bps

Pada menu ini digunakan untuk memonitoring user siapa saja yang sedang aktif saat ini.

- Hosts

MAC Address	Location	To Address	Server	Idle Time	Rx Rate	Tx Rate

Hosts ini digunakan untuk memonitoring semua perangkat yang terhubung dengan hotspot server baik yang sudah login ataupun belum

Flag yang tersedia didalam tabel Host :

S : User sudah ditentukan IP nya didalam IP binding

H : User menggunakan IP DHCP

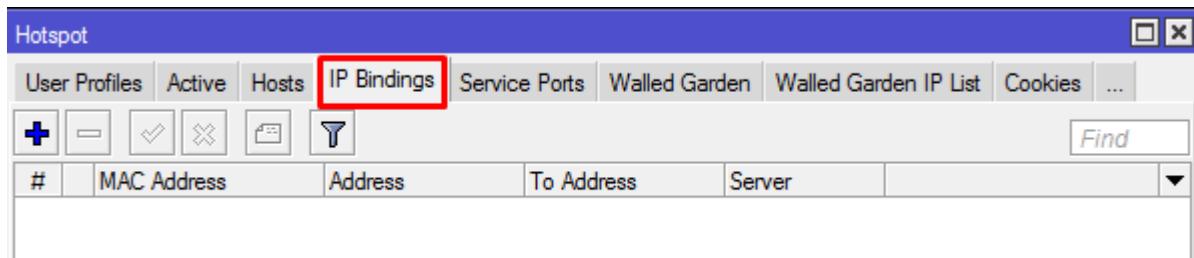
D : User menggunakan IP statik

A : User sudah melakukan login / Autentikasi

P : User di bypass pada IP binding

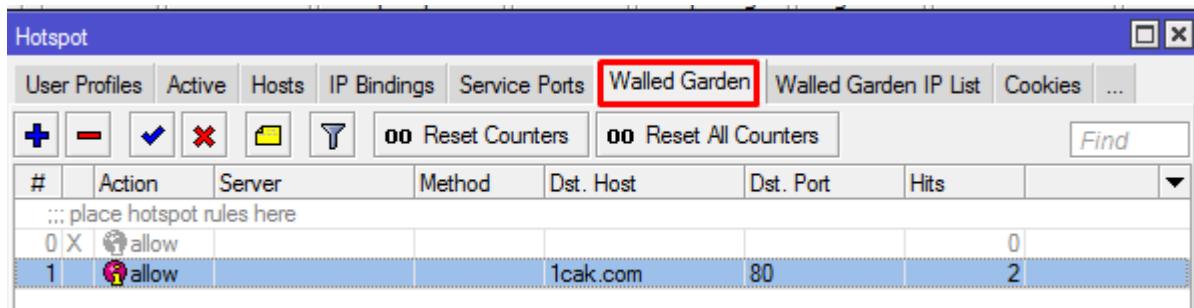
- IP Bindings

Ip bindings bisa untuk bypass host terhadap authentication, block akses dari host tertentu berdasarkan mac address/ip address asli



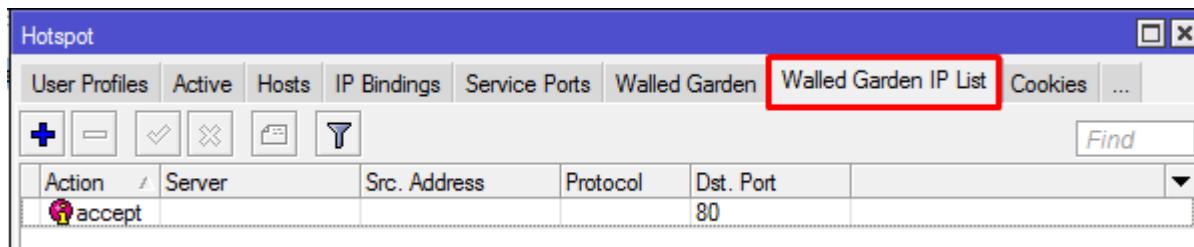
- Walled Garden

Walled garden itu sebuah sistem yang memungkinkan untuk user yang belum terautentikasi menggunakan bypass beberapa resource jaringan tertentu tetapi tetap memerlukan autentikasi jika ingin menggunakan resource yang lain



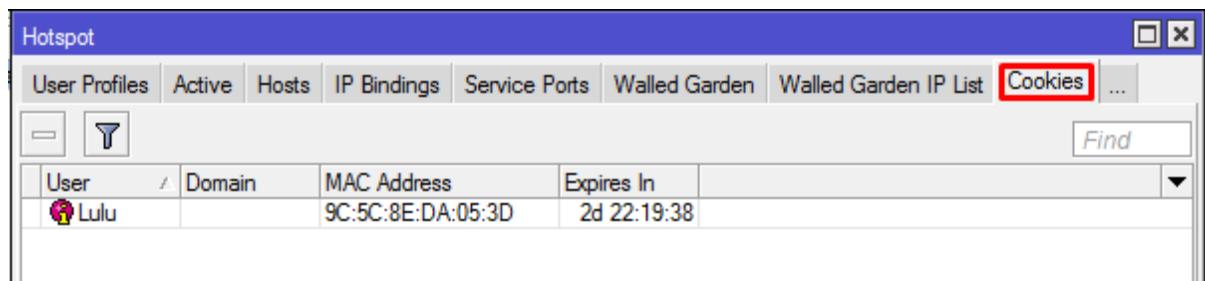
- Walled IP Garden IP-List

Walled garden ip-list mampu melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu. Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi



- *Cookies*

Cookies digunakan untuk mengetahui daftar dinamis dari semua http cookies yang valid.



The screenshot shows a Windows application window titled "Hotspot". The top menu bar includes "User Profiles", "Active", "Hosts", "IP Bindings", "Service Ports", "Walled Garden", "Walled Garden IP List", "Cookies" (which is highlighted with a red box), and "...". Below the menu is a toolbar with a search icon and a "Find" button. The main area is a table with columns: "User", "Domain", "MAC Address", and "Expires In". A single row is visible, showing "Lulu" in the User column, "9C:5C:8E:DA:05:3D" in the MAC Address column, and "2d 22:19:38" in the Expires In column. There is also a small user icon next to the "Lulu" entry.

User	Domain	MAC Address	Expires In
Lulu		9C:5C:8E:DA:05:3D	2d 22:19:38

Menget Itu adalah beberapa Fitur yang bisa kita gunakan untuk me-management Hotspot Mikrotik..

Lab 45. IP Binding

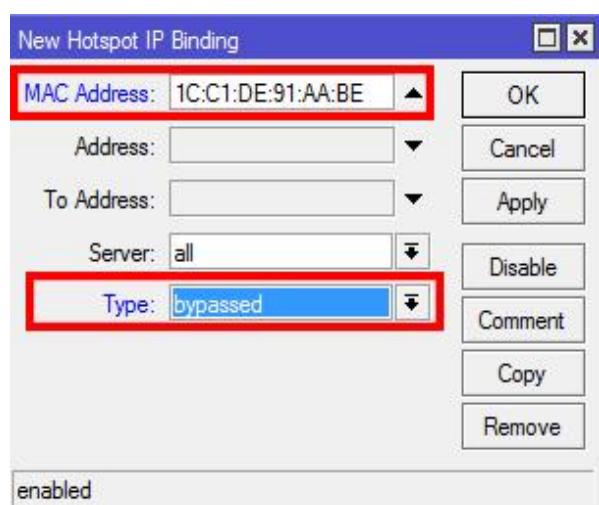
Biasanya kalau kita membuat hotspot mikrotik dan ingin browsing,pastinya kita akan dihadapkan dengan login hotspot pada web browser sebelum kita dapat membuka alamat yang kita tuju. Nah,bypass ini bisa di bilang fungsinya untuk menonaktifkan/meniadakan login hotspot. Sehingga kita bisa browsing tanpa harus login hotspot mikrotik terlebih dahulu. Di mikrotik terdapat berbagai fitur untuk melakukan bypass,salah satunya menggunakan IP Binding.

IP-Binding adalah menu HotSpot yang memungkinkan untuk setup statis One-to-One NAT translation, memungkinkan untuk memotong klien HotSpot tertentu tanpa otentikasi apapun, dan juga memungkinkan untuk memblokir host tertentu dan subnet dari jaringan HotSpot,

Buat Hotspot terlebih dahulu,Setelah selesai membuat Hotspot selanjutnya kita akan men-Setting IP Binding..

Misalkan "Mac Address 1C:C1:DE:91:AA:BE" akan di-bypass, sehingga user yang memiliki mac address tersebut jika ingin terkoneksi ke internet tidak akan melewati proses autentikasi dari hotspot login yang telah kita buat,karna pada default nya setiap Client yang ingin berselancar ke internet melalui Hostpot harus login terlebih dahulu.

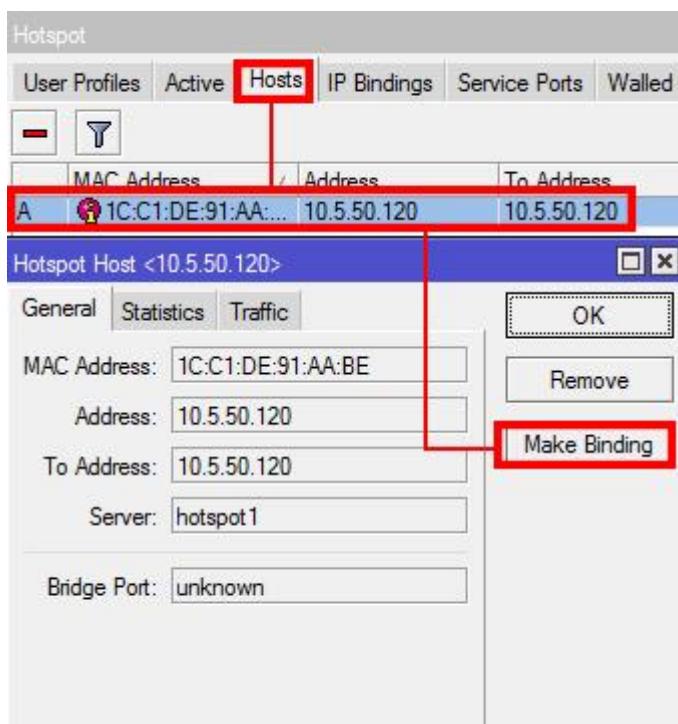
- Klik IP > Hotspot > IP Binding > Add
- Lalu Isi Mac-Address Client (Yang Ingin d Bypass)
- Lalu Pilih Type=Bypassed
- Lalu Apply dan OK



Pada opsi type terdapat 3 macam parameter yaitu :

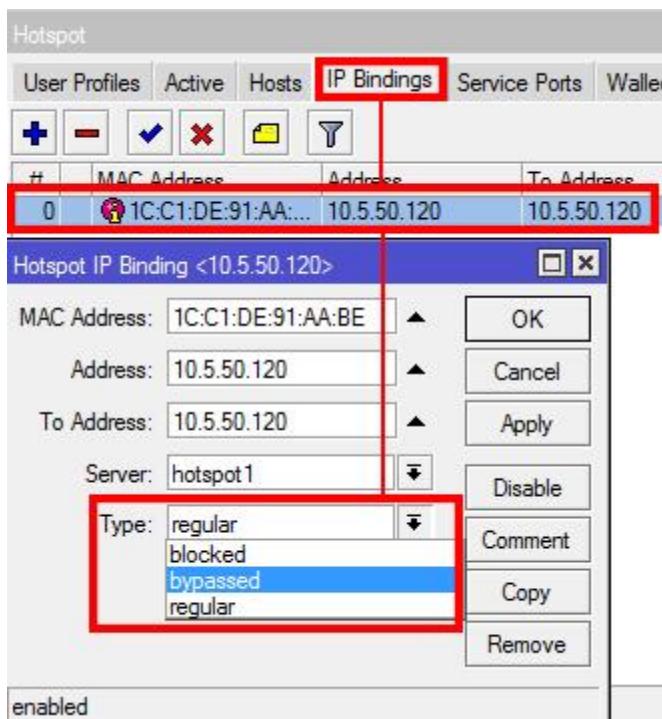
- Blocked = Mac address yang didaftarkan dengan type ini otomatis tidak akan mendapatkan layanan hotspot.
- Bypassed = Mac address yang didaftarkan dengan type ini akan dibypass sehingga tidak perlu melewati proses autentikasi.
- Regular = Mac address yang didaftarkan dengan type ini akan melewati proses autentikasi seperti user biasa, misalkan digunakan hanya untuk mengalokasikan ip address khusus ke host tertentu.

Kita juga bisa melakukan IP-Bindings terhadap host yang aktif. Caranya cukup mudah yaitu pilih host yang akan dilakukan IP-bindings, kemudian klik dua kali dan pilih "Make Binding"



Selanjutnya akan muncul Hotspot IP Bindings, pada parameter type pilih bypassed.

Lalu Kita hanya perlu men-Setting Client tersebut di menu IP Binding dan Memilih Type untuk Client tersebut..



Lalu Apply dan OK....

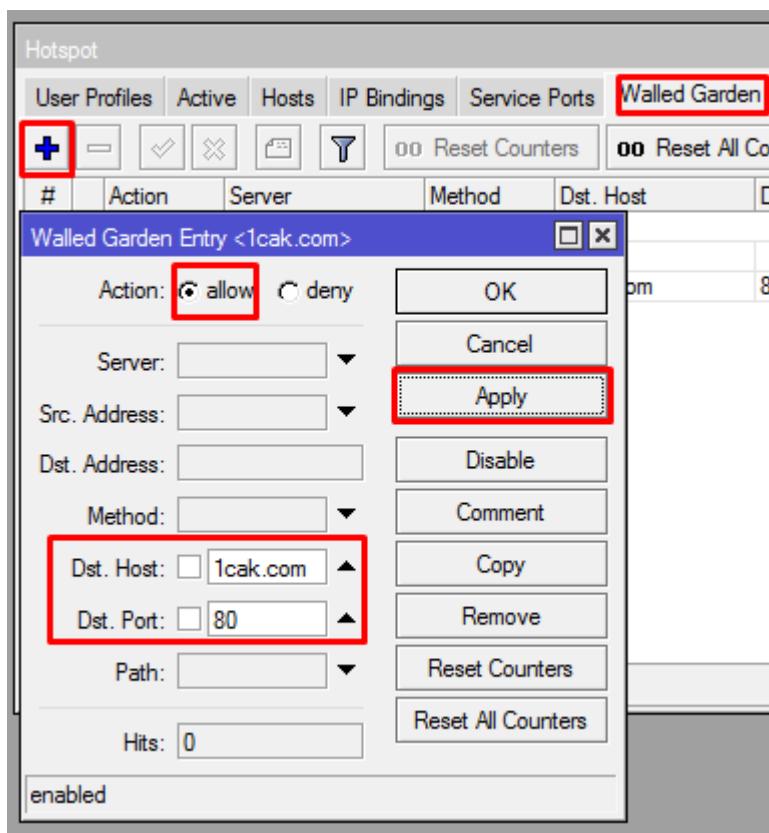
Jika sudah melewati Step ini maka Client tersebut tidak perlu Login lagi karna Client tersebut telah kita setting IP Binding..

Lab 46. Walled Garden

Jika pada Lab sebelumnya, user yang belum melakukan proses autentikasi tidak bisa berselancar di internet, maka di lab ini saya akan membahas bagaimana cara nya agar User yang belum melewati proses autentikasi tapi bisa mengakses website tertentu, dalam hal ini bisa menggunakan Fitur Walled Garden. Misal, user yang belum terautentikasi bisa membuka website www.1cak.com

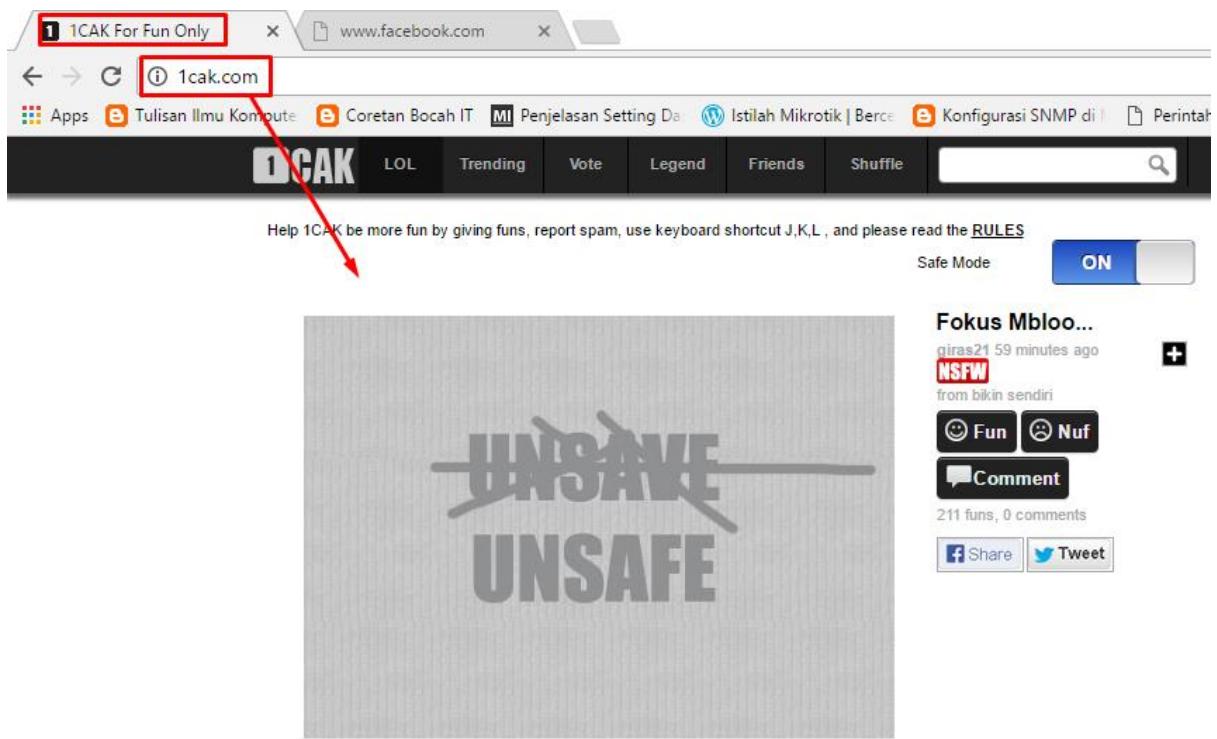
Di lab ini kita akan menggunakan Konfigurasi Hotspot yang telah kita buat di lab sebelumnya..

- Masuk ke Menu Hotspot Lalu Klik Walled Garden
- Lalu Klik Add (+)
- Pilih Action=Allow dan Isi Dst.Host=1cak.com
- Lalu Apply dan OK



Jika sudah melewati Step ini maka Website 1cak.com bisa di buka oleh Client yang belum melakukan Login..

Untuk Pengetesan,buka situs 1cak.com dalam keadaan belum login ke hotspot..

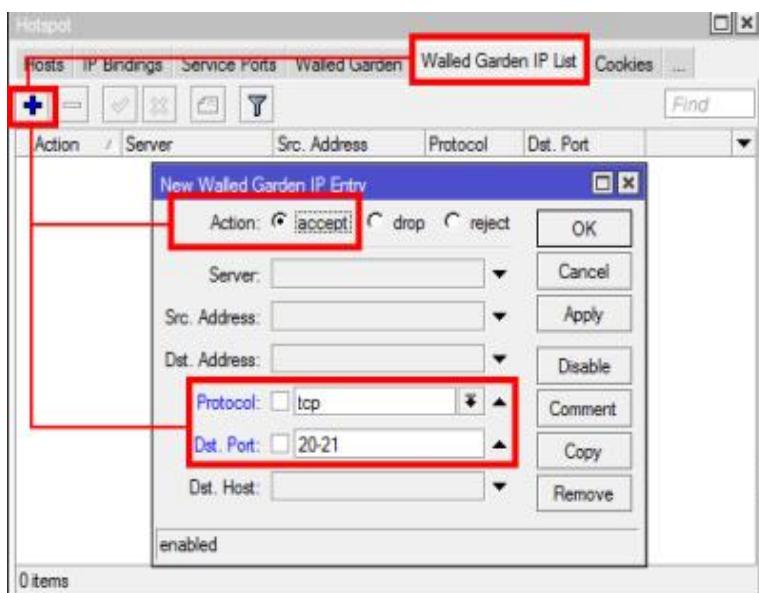


Maka hasil nya 1cak.com dapat di buka walaupun client belum login ke hotspot..

Lab 47. IP-Walled Garden

Jika Pada Lab sebelum nya kita membahas tentang Walled Garden di lab ini kita akan membahas IP-Walled Garden, IP-Walled Garden Fungsinya hampir sama seperti Walled Garden tetapi dapat melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu. Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi. Misalnya kita akan melakukan bypass terhadap trafik dengan protokol tcp dan tujuan port 20-21 (FTP)

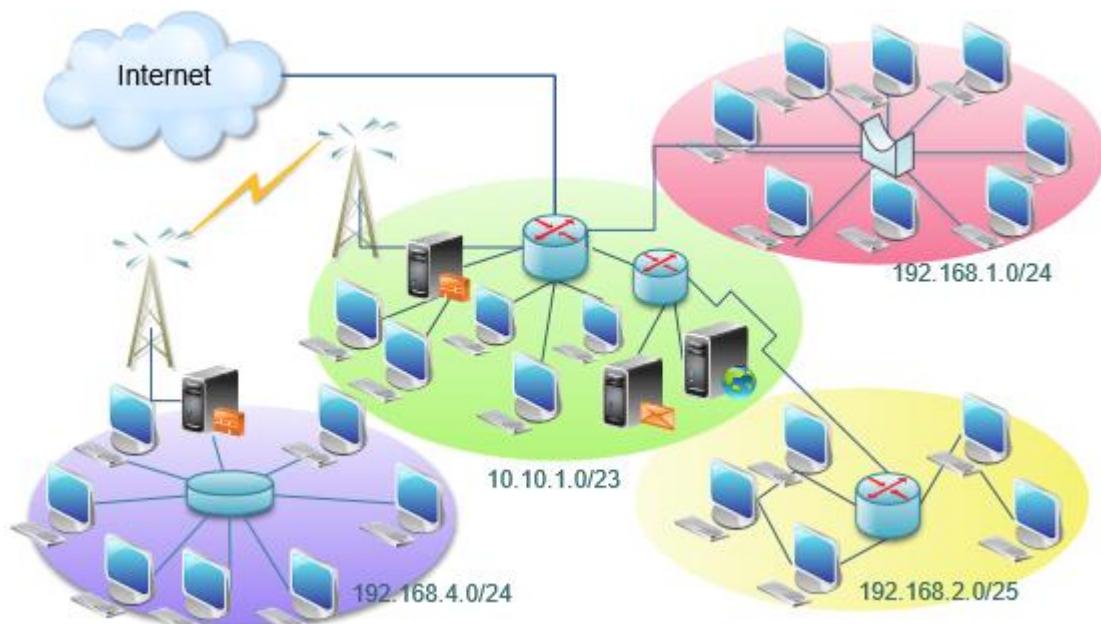
- Klik IP > Hotspot > Walled Garden IP List
- Pilih Action=Accept ,Isi Protocol=Tcp dan Dst.Port=20-21
- Lalu Apply dan OK



Selesai...

Bab 6. Routing

Routing adalah sebuah proses untuk pemilihan jalur untuk meneruskan paket-paket dari satu jaringan ke jaringan lainnya. Routing juga dapat diartikan sebagai metode penggabungan beberapa jaringan sehingga paket-paket data dapat dikirimkan dari satu jaringan ke jaringan selanjutnya. Jenis routing terbagi menjadi dua: yang pertama adalah Routing static, jika kita menggunakan Routing static maka kita (Administrator) yang akan menetukan secara manual jalur yang digunakan oleh router untuk mengirimkan paket untuk mencapai tujuan, dan jika menggunakan Dynamic Routing maka Router akan saling bertukar table routing dengan router yang lainnya agar Router tersebut dapat mengenali Remote address (Network yang tidak terhubung langsung).



Type routing pada MikroTik RouterOS:

- **Dynamic routes** = informasi routing yang secara otomatis ditambahkan saat penambahan IP address pada interface, dynamic route juga didapat dari informasi routing yang didapat dari protokol routing dinamik seperti RIP, OSPF, dan BGP. -
- **static routes** = informasi routing yang dibuat secara manual oleh user untuk mengatur ke arah mana trafik tertentu akan disalurkan. Default route adalah salah satu contoh static routes.

Protocol Routing:

Routing protocol akan digunakan oleh router jika router tersebut menggunakan Routing Dynamic. Routing protocol merupakan Protocol yang digunakan oleh Router router untuk saling bertukar informasi Routing, pertukaran inrformasi akan dilakukan secara Dynamic, sehingga jika terjadi perubahan pada jaringan, maka Protocol tersebut akan memberihtahukan perubahan tersebut kepada router router lain yang ada di dalam jaringan tersebut, dan ini adalah beberapa jenis Protocol Routing.

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)
- Border Gateway Protocol (BGP)

Dan Protocol Routing dibagi menjadi dua:

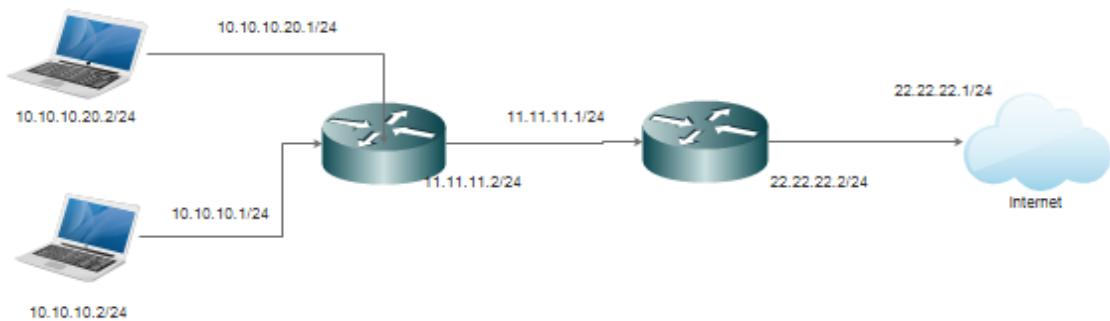
- Interior Gateway Protocol(IGP)

Interior gateway protocol adalah protocol routing yang digunakan pada router router yang berada dalam satu Autonomous System, Routing Protocol yang termasuk IGP adalah RIP, OSPF, IS-IS

- Exterior Gateway Protocol (EGP)

Exterior Gateway Protocol adalah protocol routing yang digunakan pada router router yang berasal dari Autonomous System yang berbeda, Routing protocol yang digunakan untuk EGP adalah BGP

Prinsip Dasar Routing



- IP Address Gateway harus merupakan IP Address yang subnetnya sama dengan salah satu IP Address yang terpasang pada router (connect directly).
- Pada Router R1 terdapat 3 interface dengan 3 IP address.
- Default gateway pada router R1 adalah router R2
- IP Address yang menjadi default gateway router R1 adalah 11.11.11.1, karena IP Address tersebut berada dalam subnet yang sama dengan salah satu IP Address pada R1 (11.11.11.2/24)
- Setting static default route pada R1 adalah Dst-address=0.0.0.0/gateway=11.11.11.1

Untuk pemilihan Routing, router akan memilih berdasarkan

1. Rule routing yang paling spesifik tujuannya Contoh: destination 192.168.0.128/26 lebih spesific dari 192.168.0.0/24
2. Router akan memilih yang distance nya paling kecil, apabila tidak disetting, nilai defaultnya adalah:

- Connected Routes: 0
- Static Routes: 1
- eBGP: 20
- OSPF: 110
- RIP: 120
- MME: 130
- iBGP: 200

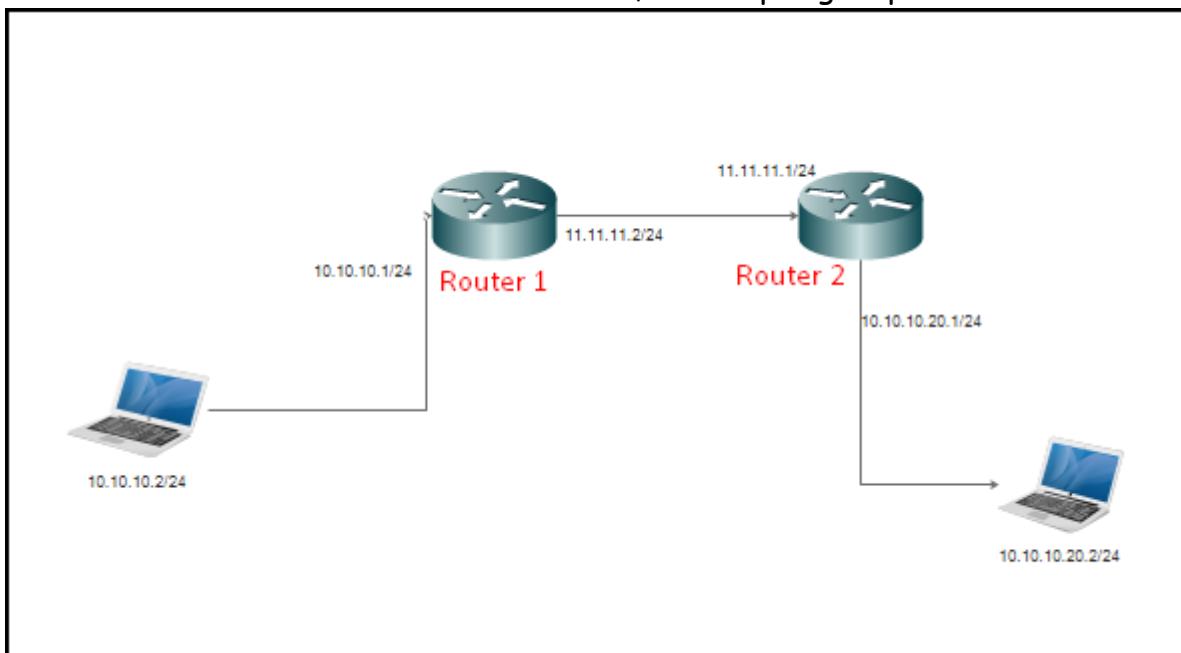
3. Apabila spesifikasi dan distancenya sama, router akan memilih secara random menggunakan algoritma Round Robin

Lab 48. Static Route

Pada Lab ini kita akan mencoba Me-Routing secara Static/Manual,jika kita menggunakan Static Route maka kita harus tau **Ingin kemana dan lewat mana?**,Itu adalah konsep dari Static Route,

Kita akan membuat sebuah topologi sederhana..

Kita Akan Mencoba Static Route di GNS 3,Buat Topologi seperti di bawah ini



Setiap PC terhubung ke router lewat Ether 1 ,dan Router terhubung ke Router lainnya melalui Ether 2. Dan Pasang IP Static Pada Setiap PC

Konfigurasi IP Address pada Router 1

```
R1
[admin@MikroTik] > ip address add address=10.10.10.1/24 interface=ether1
[admin@MikroTik] > ip address add address=11.11.11.2/24 interface=ether2
[admin@MikroTik] >
```

Setelah melakukan Step maka Interface ether1 dan ether2 pada router 1 sudah memiliki IP Address..

Selanjutnya kita akan meng-Konfigurasikan IP Address pada Router2

```
R2
[admin@MikroTik] > ip address add address=10.10.20.1/24 interface=ether1
[admin@MikroTik] > ip address add address=11.11.11.1/24 interface=ether2
[admin@MikroTik] >
```

Jika kedua Router telah di beri IP Address Maka langkah selanjutnya adalah Me-Routing agar semua Router, agar Router 1 dapat mengenali jaringan LAN yang ada di router 2, dan Router 2 dapat mengenali jaringan LAN yang ada di router 1, Ini berfungsi ketika PC yang terhubung pada router 1 (PC 1) ingin Mengirimkan data ke PC yang yang terhubung ke Router 2 (PC 2), Jika kita tidak me-Routing kedua Router tersebut maka kedua PC tersebut tidak bisa saling terhubung..

Kongfigurasi Routing Pada Router 1

```
[admin@MikroTik] > ip route add dst-address=10.10.20.0/24 gateway=11.11.11.1
[admin@MikroTik] >
```

Admin@Mikrotik> Ip route add dst-address=10.10.20.0/24 gateway=11.11.11.1

Konfigurasi diatas berfungsi untuk menambahkan Tabel Routing pada Router 1 , Tabel Routing routing yang di tambahkan adalah Network 10.10.20.0/24 melewati 11.11.11.1 , maka Artinya jika PC 1 ingin mengirim data ke PC 2 , data tersebut sudah bisa terkirim , karena ketika PC 1 akan mengirim data Ke PC 2 (10.10.20.2/24) Router 1 telah mengetahui jalur mana yang akan di gunakan untuk mengirimkan data ke PC 2, Tetapi ketika PC 2 ingin mengirimkan data kembali ke PC 1 maka data tidak akan terkirim di karnakan Router 2 belum tau jalur yang di gunakan untuk mengirim data ke PC 1, itu di karnakan Router 2 belum di Routing atau Router 2 belum Memiliki table Routing untuk Network 10.10.10.0/24

Konfigurasi Routing pada Router 2

```
[admin@MikroTik] >
[admin@MikroTik] > ip route add dst-address=10.10.10.0/24 gateway=11.11.11.2
[admin@MikroTik] >
```

Admin@Mikrotik> Ip route add dst-address=10.10.10.0/24 gateway=11.11.11.2

Jika sudah melakukan Konfigurasi tersebut maka Network 10.10.10.0/24 sudah ada pada Table Routing yang ada di Router 2, dan Artinya Jika PC 2 ingin mengirimkan data ke PC 1, Router 2 telah mengetahui jalur untuk mengirim data ke PC 1.. jadi Ke dua PC tersebut sudah saling terhubung..

Tabel routing Pada Setiap Router dapat kita lihat dengan menggunakan Perintah: **Ip Route Print**

Coba Kita Cek Tabel Routing pada Router 1

```
[admin@MikroTik] >
[admin@MikroTik] > Table Routing pada Router 1
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 ADC 10.10.10.0/24 10.10.10.1 ether1 0
1 A S 10.10.20.0/24 11.11.11.1 1
2 ADC 11.11.11.0/24 11.11.11.2 ether2 0
[admin@MikroTik] >
```

Selanjutnya Cek Tabel Routing di Router 2

```
[admin@MikroTik] >
[admin@MikroTik] > Table Routing pada Router 2
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 A S 10.10.10.0/24 11.11.11.2 1
1 ADC 10.10.20.0/24 10.10.20.1 ether1 0
2 ADC 11.11.11.0/24 11.11.11.1 ether2 0
```

Jika sudah Coba test Ping antar PC tersebut..

Teknik Routing dapat di lakukan Menggunakan CLI maupun Menggunakan GUI,di lab ini saya menggunakan CLI karna menggunakan CLI lebih mudah dari pada menggunakan GUI ,GUI cenderung lebih rumit untuk melakukan Teknik Routing..

Lab 49. RIP

Pertama Kita Perlu tau Penjelasan RIP, apa itu RIP? RIP adalah sebuah protokol routing dynamic yang digunakan dalam jaringan LAN (Local Area Network) dan WAN (Wide Area Network). Oleh karena itu protokol ini diklasifikasikan sebagai Interior Gateway Protocol (IGP). Protokol ini menggunakan algoritma Distance-Vector Routing

cara kerja Protocol RIP adalah memilih jalur yang paling cepat sampai ke network tujuan. dan maksimal loncatan pada RIP adalah 16 loncatan.

Nah, sekarang kita akan mencoba mengkonfigurasi routing rip pada GNS3. berikut topologinya.



Kita coba memakai 3 router terlebih dahulu.

- Konfigurasi router1

Kita Lihat Ether1 Terhubung ke Area 12.12.12.0/24, maka kita buat yang satu subnet dengan network 12.12.12.0/24 misalnya 12.12.12.1

```
[admin@MikroTik] > ip address add address=12.12.12.1/24  
interface: ether1  
[admin@MikroTik] >
```

kita lihat interface berapa yang terhubung ke router2 yaitu ether1. maka kita tulis routing rip interface ad interface=ether1.

```
[admin@MikroTik] >  
[admin@MikroTik] > routing rip interface add interface=ether1
```

dan disinilah perbedaan static routing dan dynamic routing kalau di dynamic routing. Yang dimasukkan adalah network yang terhubung ke kita tapi kalau static route yang. Dimasukkan adalah network yang tidak terhubung ke kita. maka kita ketik **routing rip network add network=12.12.12.0/24**

```
> routing rip network add network=12.12.12.0/24  
>
```

Nah konfigurasi di router 1 sudah selesai, sekarang coba langkah yang sama pada router 2 dan 3. dan ingat buat ip yang satu segmen dengan network yang terhubung.

Jika sudah selesai, coba lihat Tabel Routing pada router 1, 2 dan 3..

Ketik **IP Route Print**

Tabel Routing Router 1

[admin@MikroTik] > ip route print				
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r B - blackhole, U - unreachable, P - prohibit				
#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADC 12.12.12.0/24	12.12.12.1	ether1	0
1	ADR 23.23.23.0/24		12.12.12.2	120

Jalurnya sudah terbuat secara otomatis.

Tabel Routing di Router2

[admin@MikroTik] > ip rou pr				
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r B - blackhole, U - unreachable, P - prohibit				
#	DST-ADDRESS	PREF-SRC	GATEWAY	
0	ADC 12.12.12.0/24	12.12.12.2	ether1	
1	ADC 23.23.23.0/24	23.23.23.1	ether2	

Dikarenakan router2 terhubung secara langsung dengan ke 2 networknya maka router2 sudah bisa terhubung walaupun tidak dibuat dynamic routing karena terhubung secara langsung.

Tabel Routing pada Router3

[admin@MikroTik] > ip route print				
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - nme, B - blackhole, U - unreachable, P - prohibit				
#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADR 12.12.12.0/24		23.23.23.1	120
1	ADC 23.23.23.0/24	23.23.23.2	ether1	0

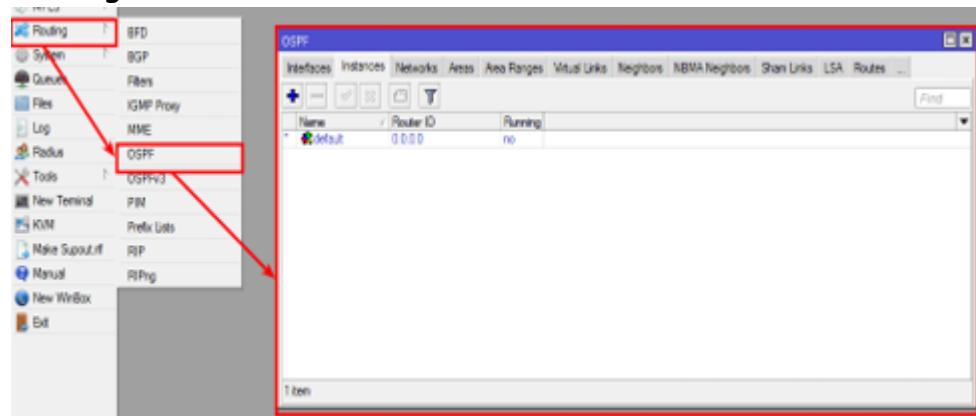
Lab 50. OSPF

Routing ospf adalah salah satu dari beberapa routing dinamic yang dapat kita gunakan. Apa itu routing dinamik? Routing dinamik adalah routing yang diaman dalam penentuan rutennya dilakukan secara otomatis.

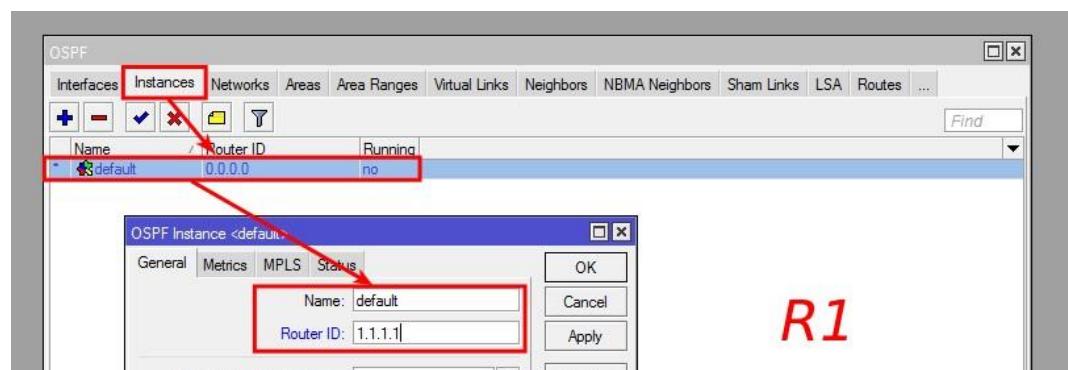
Bayangkan jika anda harus mengkonfigurasi 100 router dengan routing static. Tentu akan menyusahkan bukan. Oleh karena itu kita dapat menggunakan routing static yaitu routing yang dimana router akan mencari sendiri rute nya.

Untuk mengkonfigurasi routing ospf kita akan menggunakan topologi sebelumnya yaitu pada lab 48. Tetapi jangan lupa untuk menghapus routing static yang ada terlebih dahulu.

Untuk masuk kedalam konfigurasi routing ospf anda dapat membukanya pada menu Routing > OSPF

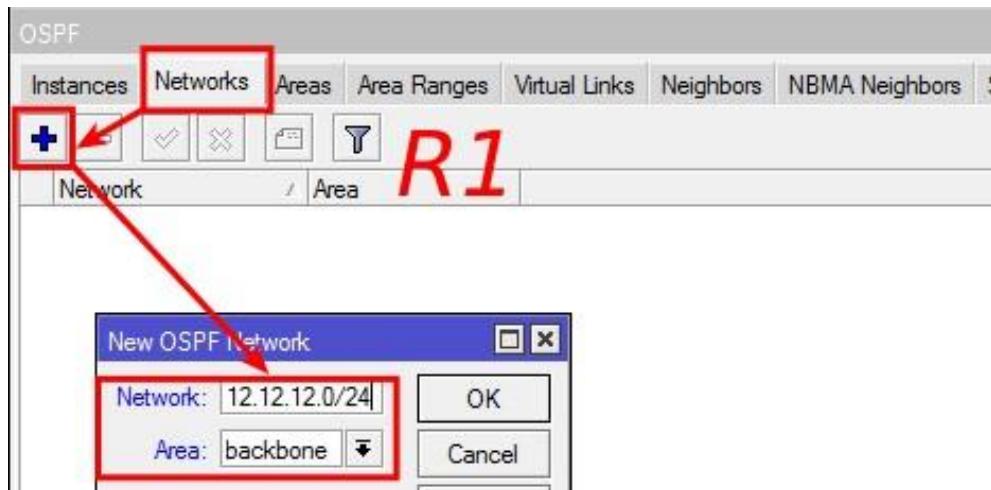


Pertama set router id router ospf pada Menu Routing > OSPF > Instances. Router-id ini akan berfungsi sebagai penamaan pada router Ospf

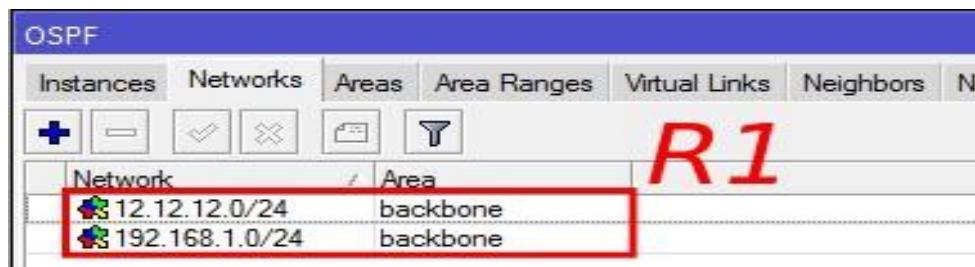


Selanjutnya adalah menambahkan network yang akan dimasukkan kedalam routing ospf caranya yaitu pada Menu Routing > OSPF > Network kemudian tambahkan network yang ingin ditambahkan pada Router R1

kita akan menambahkan network 12.12.12.0/24 dan network 192.168.1.0/24.

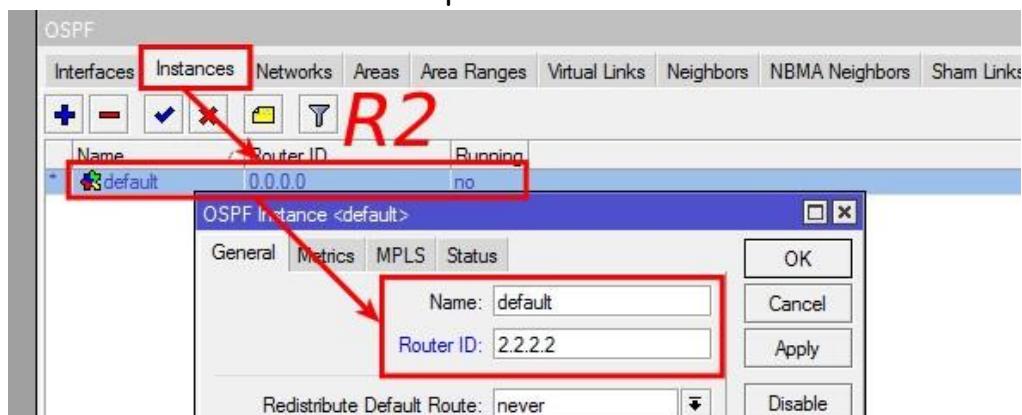


Setelah itu tambahkan juga network 192.168.1.0/24 sehingga hasil dari routing ospf network akan seperti berikut ini.



Konfigurasi OSPF Router R2

Tambahkan router id sama seperti router R1



Kemudian tambahkan network dengan cara yang sama pada router R1 sehingga hasil dari routing ospf network akan seperti ini

OSPF		Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBM
								R2
	Network	/	Area					
	12.12.12.0/24			backbone				
	192.168.2.0/24			backbone				

Untuk memeriksa konfigurasi kita akan menggunakan ip --> route pada Router R1 dan router R2. Dengan Ip route kita akan melihat apakah kedua router sudah saling berbagi rute yang dimilikinya satu sama lain.

Router R1

Route List					
Routes		Nexthops	Rules	VRF	
DAC	► 12.12.12.0/24	ether1 reachable			Distance
DAC	► 192.168.1.0/24	ether2 reachable			0
DAo	► 192.168.2.0/24	12.12.12.2 reachable ether1			110

Route List					
Routes		Nexthops	Rules	VRF	
DAC	► 12.12.12.0/24	ether1 reachable			Distance
DAo	► 192.168.1.0/24	12.12.12.1 reachable ether1			0
DAC	► 192.168.2.0/24	ether2 reachable			110
					Pref. Source
					12.12.12.2
					192.168.2.1

Tes terakhir dan tes yang paling penting kita dapat menggunakan tes ping antar Laptop yaitu disini saya mencoba ping dari laptop1 menuju laptop2.

```
C:\Windows\system32\cmd.exe
^C
C:\Users\Irpan>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=62
Reply from 192.168.1.2: bytes=32 time=1ms TTL=62
Reply from 192.168.1.2: bytes=32 time=1ms TTL=62
Reply from 192.168.1.2: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\Irpan>
```