

MODUL MIKROTIK MTCNA



MUHAMMAD FAHRIZUR RIFQI
PESANTREN NETWORKERS

DAFTAR ISI

DAFTAR ISI.....	1
Bab 1. KONFIGURASI DASAR MIKROTIK	
Lab 1. Akses ke Routerboard Mikrotik	5
Lab 2. Akses ke Routerboard Via Terminal (Telnet/SSH).....	5
Lab 3. Akses ke Routerboard Via Web Browser (Webfig).....	7
Lab 4. Akses ke Routerboard Via Winbox	8
Lab 5. Versi dan Spesifikasi Routerboard	9
Lab 6. Management MNDP.....	9
Lab 7. Enable / Disable Paket Mikrotik.....	10
Lab 8. Uninstall Paket Mikrotik	10
Lab 9. Merubah Identitas (nama) routerboard.....	11
Lab 10. Upgrade / Downgrade versi OS Routerboard Mikrotik	12
Lab 11. Hard Reset.....	14
Lab 12. Soft Reset.....	15
Lab 13. User Login Management	16
- User Management Akses	17
Lab 14. Merubah Identity (nama) Routerboard.....	17
Lab 15. Merubah Tanggal dan Waktu.....	18
Lab 16. Backup dan Restore	19
Lab 17. Backup Binary.....	20
Lab 18. Export & Import	20
Lab 19. Install Ulang Routerboard (Netinstall)	22
Lab 20. Konfigurasi DNS	26
Lab 21. Konfigurasi NTP Client	27
Lab 22. Konfigurasi NTP Server.....	28
Lab 23. Menghubungkan PC ke Internet dengan Routerboard Mikrotik.....	30
Lab 24. Konfigurasi IP Address Pada Routerboard	30
- Konfigurasi IP Address Pada PC/Laptop	35
Bab 2. NETWORK MANAGEMENT	
Lab 25. Konfigurasi DHCP-Server	35

Lab 26. Konfigurasi DHCP-IP Static	38
Lab 27. Konfigurasi DHCP-Mac Static.....	41
Lab 28. IP Service	43
Bab 3. FIREWALL	
Lab 29. Membatasi akses IP ke routerboard dengan (drop few, accept any)	46
Lab 30. Membatasi akses IP ke routerboard dengan (accept few, drop any)	48
Lab 31. Firewall Logging	50
Lab 32. Blok website dengan (Konten) pada Mikrotik	51
Lab 33. Blok website dengan Address List	54
Lab 34. Connection Tracking & Connection State.....	56
Lab 35. Konfigurasi NAT	58
Lab 36. Blok Situs dengan DNS Nawala.....	60
Lab 37. Blok Situs dengan Transparent DNS Nawala	62
Bab 4. WIRELESS	
Lab 38. Konfigurasi Wireless AP & Station	65
Lab 39. Wireless Tool	69
Lab 40. Virtual Access Point	70
Lab 41. Wireless Mac Filtering (Default Authenticated)	73
Lab 42. Wireless Mac Filtering (Default Forwarding).....	78
Lab 43. Konfigurasi Wireless Nstream.....	79
Bab 5. BRIDGE	
Lab 44. Konfigurasi Wireless Bridging	84
Bab 6. ROUTING	
Lab 45. Konfigurasi Static Route.....	90
Lab 46. Konfigurasi Default Route.....	94
Bab 7. Tunnel	
Lab 47. Konfigurasi EoIP Tunnel.....	97
Lab 48. Konfigurasi PPTP Tunnel (Skenario 1).....	101
Lab 49. Konfigurasi PPTP Tunnel (Skenario 2)	105
Lab 50. Konfigurasi L2TP Tunnel (Skenario 1).....	109
Lab 51. Konfigurasi L2TP Tunnel (Skenario 2).....	112
Lab 52. Konfigurasi PPPoE Tunnel (Skenario 1).....	115

Bab 8. QoS

Lab 53. Konfigurasi Simple Queue.....	120
Lab 54. Konfigurasi Simple Queue with PCQ	122

Konfigurasi

Dasar Mikrotik



Bab 1. Konfigurasi Dasar Mikrotik

Lab 1. Akses ke Routerboard Mikrotik

Akses ke perangkat mikrotik dapat dilakukan dengan berbagai cara dan aplikasi yg digunakan untuk mengakses mikrotik pun berbeda beda, diantaranya:

Akses Via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung pada PC	Yes		
Serial Console	Konektor Kabel Serial	Yes		
Telnet & SSH	Layer 3	Yes		Yes
Winbox	Menggunakan OS Windows/Mac OS	Yes	Yes	
FTP	Layer 3	Yes		Yes
API	Socket Programming			Yes
WEB (HTTP)	Layer 3		Yes	Yes
MAC-Telnet	Layer 2	Yes		

Pada Routerboard (RB) baru atau setelah dilakukan reset default configuration, router akan memiliki konfigurasi default dari pabrikannya yaitu:

- IP address pada Ether 2-5: 192.168.88.1/24
- Username “admin” password blank (kosong)

Untuk mengakses routerboard tersebut kita harus menyamakan network ip laptop kita dengan routerboard dengan mengatur ip address pada laptop kita dengan IP 192.168.88.0/24.

Secara umum ada 3 cara yang bisa dilakukan untuk mengakses routerboard

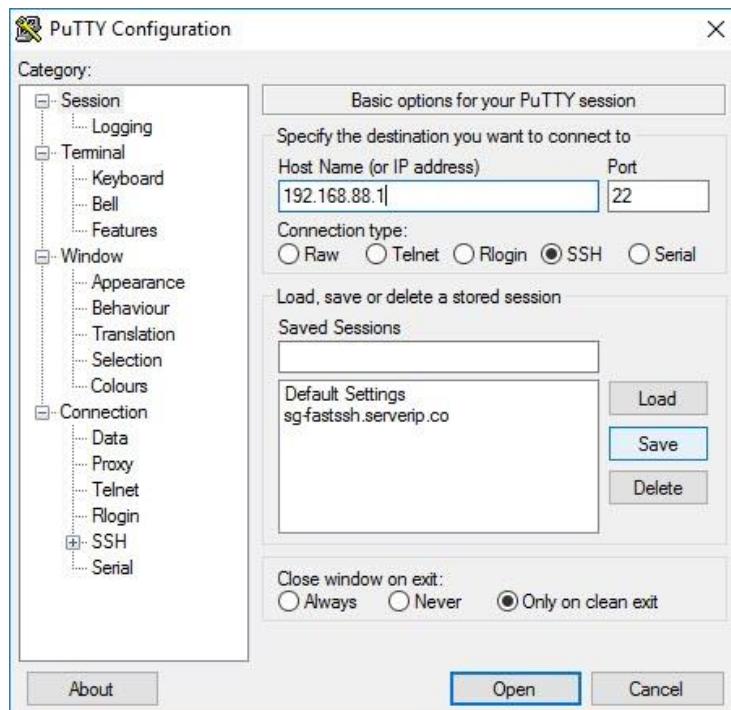
Lab 2. Akses ke Routerboard Via Terminal (Telnet/SSH)

Untuk akses via Terminal kita bisa melakukan remote dengan menggunakan kabel serial jika tidak dimungkinkan untuk mengakses router melalui kabel utp pada ethernet routerboard. Remote & konfigurasi secara terminal bisa dilakukan dengan cara:

- Telnet (via IP port 23, non secure connection)
- SSH (via IP port 22, lebih aman (secure) dari telnet)
- Serial console (kabel serial)

Akses via terminal bisa menggunakan aplikasi ssh/console menggunakan PUTTY bisa di didownload <http://www.putty.org/>.

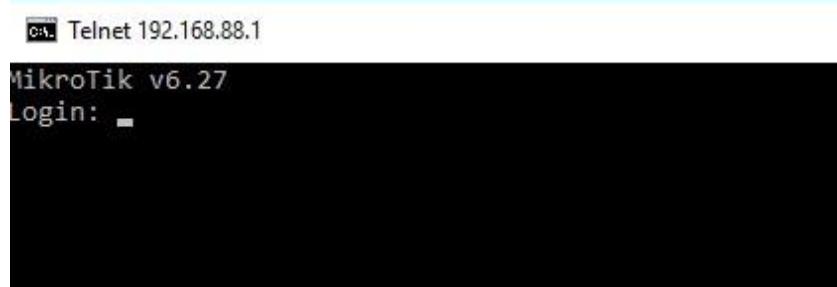
Untuk aksesnya tinggal masukkan IP address dari interface mikrotik yang terhubung ke pc kita ke kolom hostname pada putty, sekaligus port yang kita gunakan untuk remote



Klik open dan isi user & passwordnya maka tampilan selanjutnya seperti berikut

A screenshot of a terminal window titled '192.168.88.1 - PuTTY'. The window displays a command-line interface for MikroTik RouterOS 6.27. It starts with a decorative banner of letters (M, K, T) and then shows the RouterOS version and a URL. Below that, it lists several commands with their descriptions: '?', 'command ?', '[Tab]', '/', '..', and '/command'. A command-line prompt shows '[admin@MikroTik] > ip address print'. The output of this command is displayed, showing network configuration details. The interface includes standard window controls (minimize, maximize, close) and scroll bars.

Untuk akses mikrotik via telnet, caranya hampir sama dengan SSH, tinggal memasukkan ip address dan user name & password routerboardnya

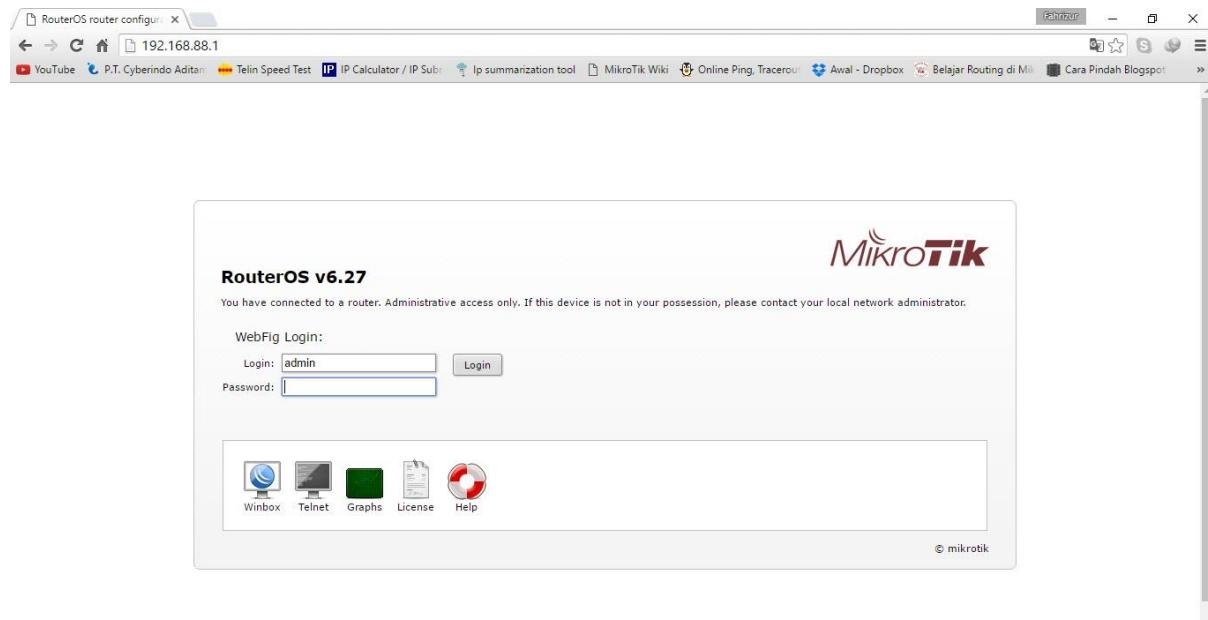


```
Telnet 192.168.88.1
MikroTik v6.27
Login: ■
```

Lab 3. Akses ke Routerboard Via Web Browser (Webfig)

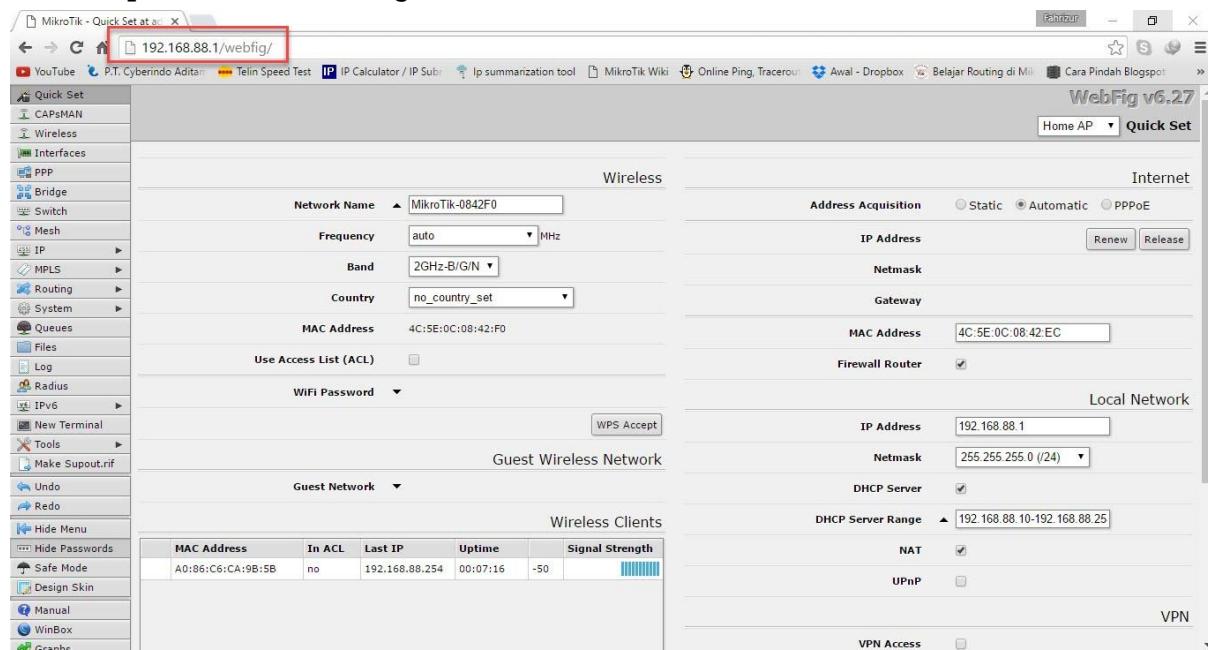
Pada routerboard, mikrotik juga menyediakan akses remote melalui web, akses via remote web memiliki fitur yang sama dengan winbox, jadi kemudahan aksesnya sama ketika kita akses melalui winbox. Cara penggunannya sebagai berikut:

1. Tambahkan IP pada interface ethernet router



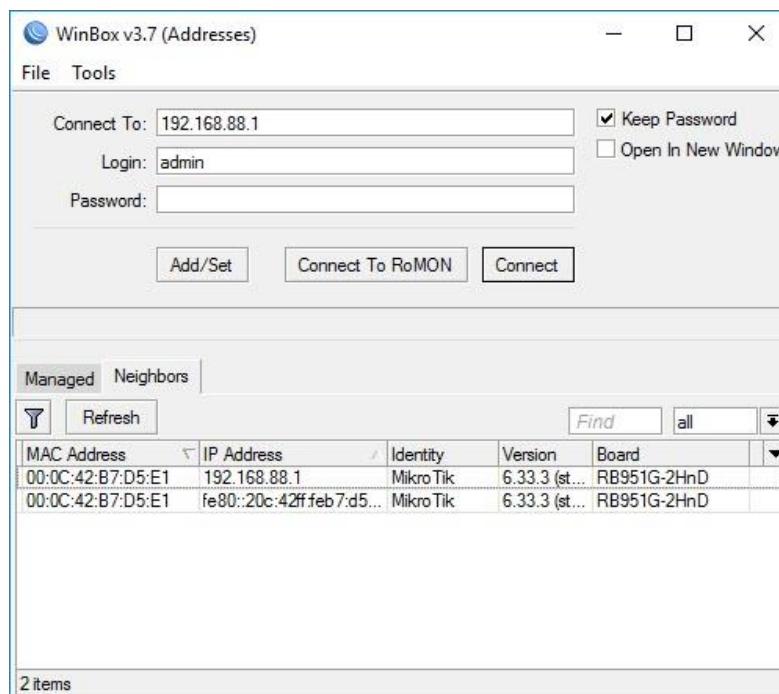
2. Akses IP address router via browser dengan mengetikkan <http://<ip>> router>
3. Masukkan Username dan Password routerboard

4. Tampilan menu webfig



Lab 4. Akses ke Routerboard Via Winbox

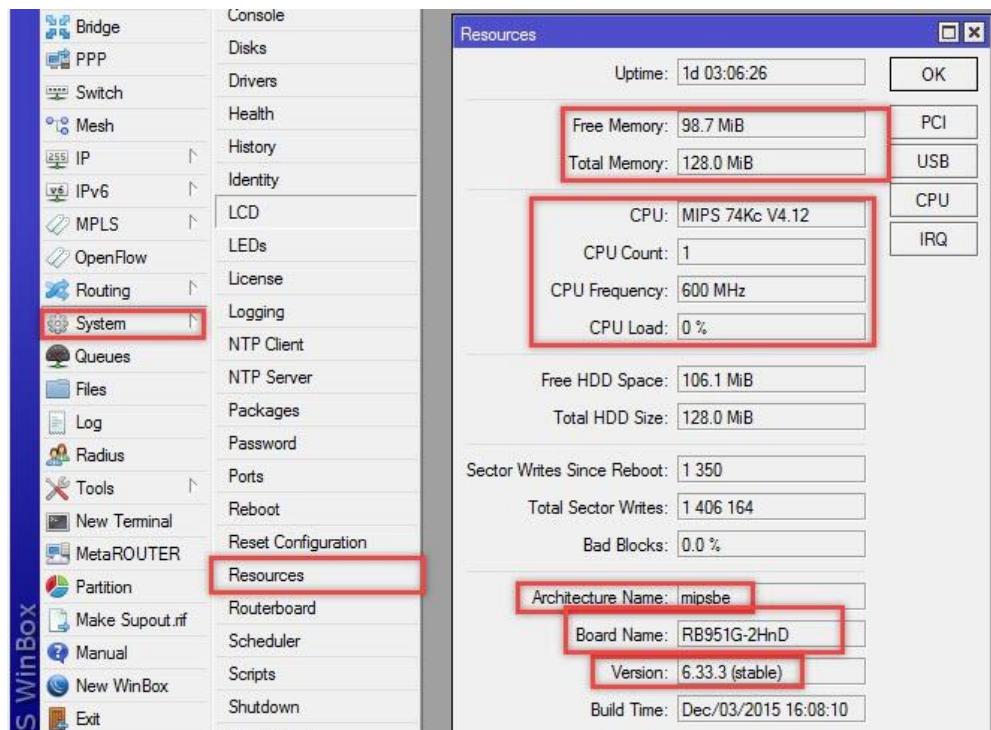
Secara umum akses remote yang mudah dan sangat populer digunakan untuk akses routerboard adalah winbox, winbox manawarkan fitur kemudahan konfigurasi karena berbasis Gui. winbox sendiri adalah software propetary dari mikrotik, bisa didownload pada <http://www.mikrotik.com/download>,



Akses winbox bisa menggunakan ip address router ataupun mac address router (yg masih dalam satu network ip) dari pc kita. Winbox jug amenyediakan fitur CLI (Terminal), jadi kalau nanti bosen pakai fitur GUInya bisa menggunakan fitur CLI nya

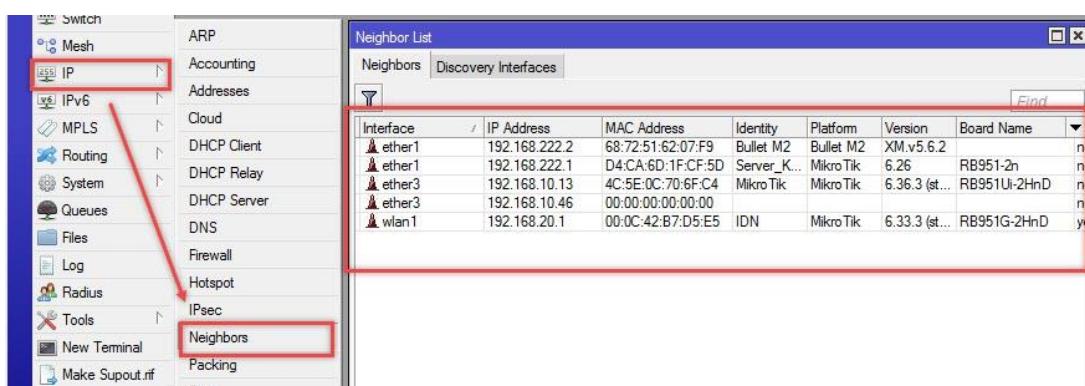
Lab 5. Versi dan Spesifikasi Routerboard

Untuk melihat versi dan spesifikasi routerboard mikrotik bisa dilakukan pada menu, **System > resource**

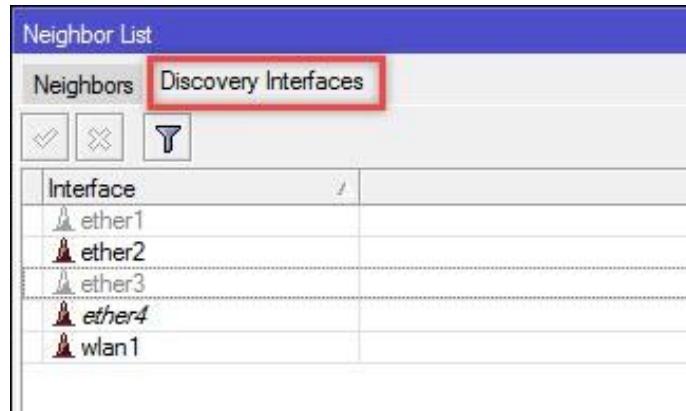


Lab 6. Management MNDP

MNDP (Mikrotik Neighbour Discovery Protocol) pada mikrotik merupakan fitur yang digunakan untuk menemukan device yang menggunakan device mikrotik, secara default MNDP aktif pada semua perangkat mikrotik. Pada perangkat yang menggunakan MNDP bisa dilihat pada menu IP > Neighbours

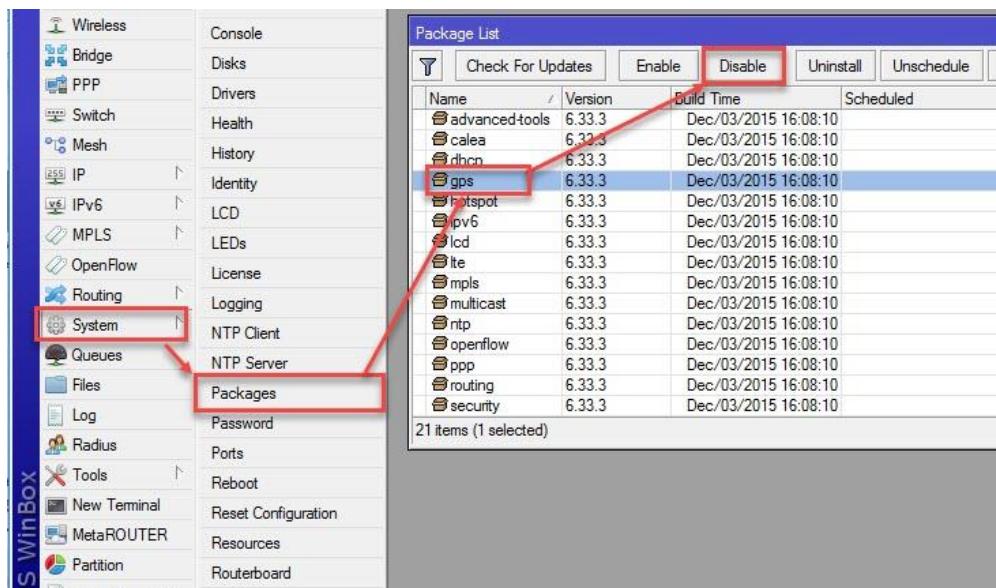


Untuk mendisable/menonaktifkan mndp tiap interface bisa dilakukan pada menu IP > Neighbours > Discovery Interfaces



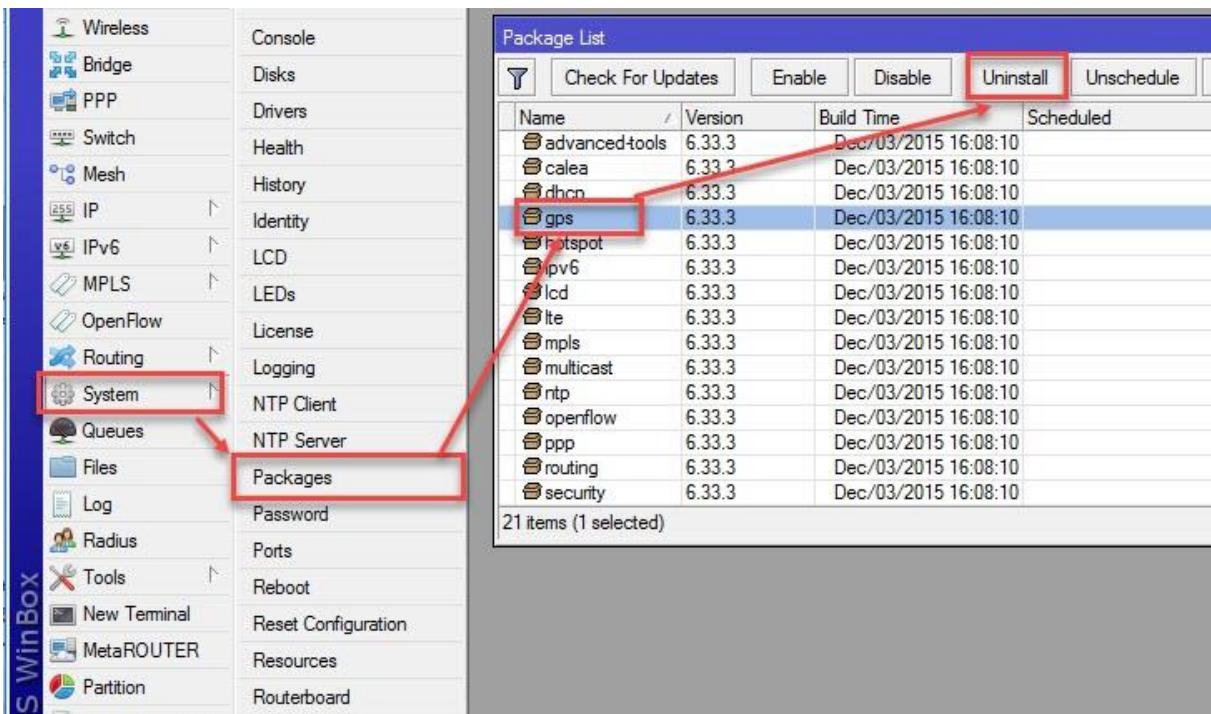
Lab 7. Enable / Disable Paket Mikrotik

Jika kita tidak menginginkan suatu paket aktif dalam routerboard kita, cukup kita disable paket tersebut



Lab 8. Uninstall Paket Mikrotik

Karena routerboard juga membutuhkan performa yg stabil dan memiliki ruang space yg cukup, kita bisa menghapus paket paket yg tidak digunakan dalam routerboard.



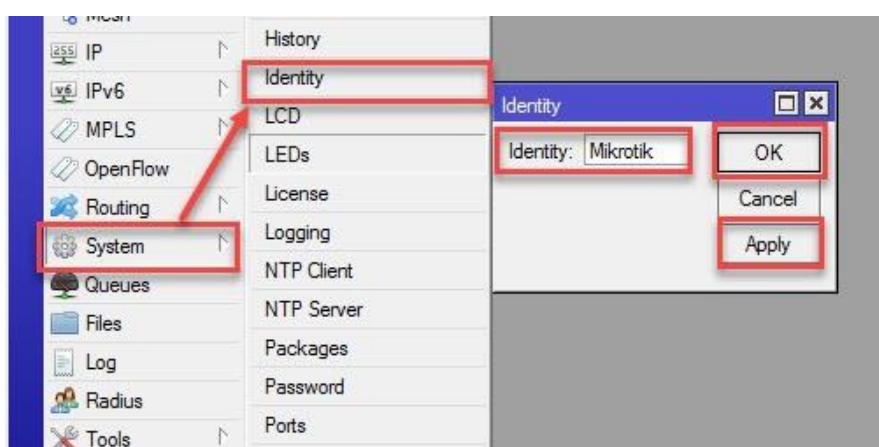
Lab 9. Merubah Identitas (nama) routerboard

Identitas dari suatu device dalam jaringan adalah suatu hal penting, karena apa? Coba bayangkan jika dalam satu jaringan kita memiliki banyak device yang sama semua judul penamaannya, karena itu kita harus mengganti identitas agar tidak salah dalam konfigurasinya.

Pada router os mikrotik, untuk mengganti identitas suatu router kita bisa lakukan pada menu **System > Identity >**

Untuk via cli konfigurasinya sebagai berikut:

```
[admin@IDN] > system identity set name=IDN
```



Lab 10. Upgrade / Downgrade versi OS Routerboard Mikrotik

Upgrade os mikrotik digunakan agar routerboard kita selalu up to date untuk memperbaiki bugs, ataupun adanya penambahan fitur fitur baru dari mikrotik. Dalam upgrade yg harus diperhatikan adalah aturan level dan lisensi pada routerboard tersebut. Untuk versi upgrade kita bisa memilih yg versi stable (stabil) karena versi ini adalah versi yg sudah stabil dalam performanya.

Untuk melakukan upgrade / downgrade kita harus mengetahui terlebih dahulu arsitektur dari routerboard kit, apakah mipsbe, smips, arm, ataupun X86. Untuk paket upgrade atau downgrade bisa didownload pada <http://www.mikrotik.com/download>,

The screenshot shows the MikroTik Downloads page. At the top, there are tabs for Home, Purchase, Software, Downloads (which is selected), Products, Support, Training, and Account. Below the tabs, there are links for RouterOS, Download archive, and Changelogs. The main content area is titled "RouterOS" and shows a table of packages for different architectures:

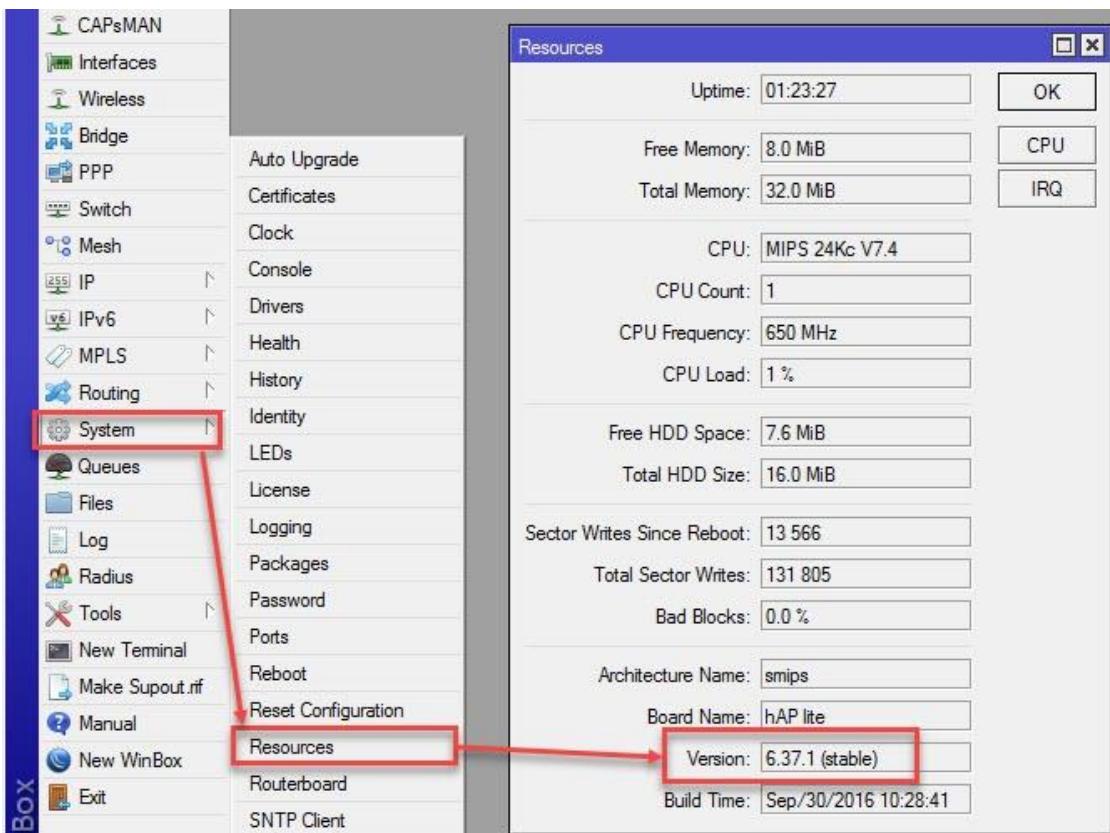
	6.34.6 (Bugfix only)	6.37.1 (Current)	5.26 (Legacy)	6.38rc15 (Release candidate)
MIPSBE	CRS, NetBox, NetMetal, PowerBox, QRT, RB0xx, IAP, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDisk, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package	[Download]	[Download]	[Download]	[Download]
Extra packages	[Download]	[Download]	[Download]	[Download]
SMIPS				
Main package	[Download]	-		[Download]
Extra packages	[Download]	-		[Download]
TILE	CCR			
Main package	[Download]	[Download]	-	[Download]
Extra packages	[Download]	[Download]	-	[Download]
The Dude server	[Download]	[Download]	-	[Download]

A red arrow points from the "SMIPS" section to the "Main package" download link for version 6.37.1.

Ekstrak file .zip yang tadi sudah didownload dan drag and drop paket .npk tersebut ke dalam winbox pada menu file

The screenshot shows the WinBox interface. On the left, there's a file explorer window titled "all_packages-smips-6.37.1" showing a list of NPK files. A red box highlights the list of files. On the right, there's a session window titled "jkb@192.168.10.1 (seven) - WinBox v6.37.1 on hAP lite (smips)". Inside this window, a file upload dialog is open, showing the progress of uploading the selected files. A red box highlights the "File List" and the upload progress bar.

Kemudian **reboot** routerboard tersebut. Kemudian buka kembali winbox pada menu **System -> Resource**, untuk mengecek versi paket apakah sudah terupdate atau belum.



Untuk downgrade, caranya hampir sama yaitu drag & drop packet, perbedannya terdapat pada peket yang kita upload ke routerboard adalah paket yg versi terdahulu dari versi paket yg digunakan. Terakhir jangan lupa reboot routerboard agar packet tadi langsung dieksekusi.

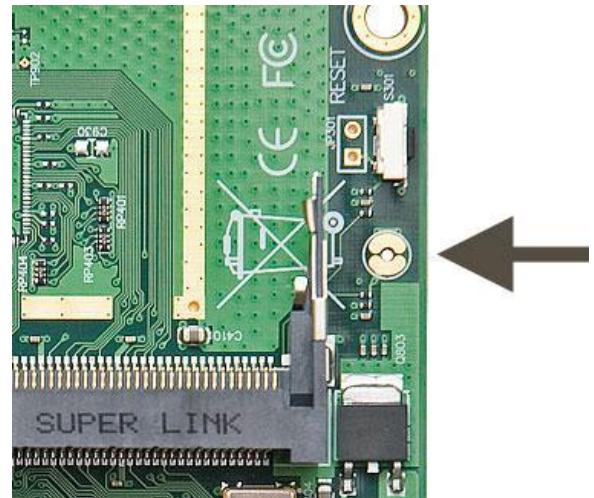
Reset Konfigurasi Mikrotik

Reset konfigurasi digunakan untuk menghapus dan mereset ulang semua konfigurasi menjadi default, tergantung reset apa yang kita pilih. Reset konfigurasi ada 2 cara yang bisa dilakukan, yaitu **Hard Reset** dan **Soft Reset**.

Lab 11. Hard Reset

Seperti penjelasan sebelumnya, hard reset digunakan dengan cara menjumper tombol reset (fisik) pada routerboard sambil menyalakan RB, cara ini digunakan ketika kita tidak bisa mengakses routerboard baik melalui winbox / terminal console Caranya sebagai berikut:

1. Sebelumnya kondisi mikrotik pada kondisi off (mati),
2. Cari tombol reset pada routerboard, tekan tombol reset dengan jarum / ujung bolpoin secara perlahan (jangan terlalu keras) sambil memasukkan power injector ke RB
3. Tahan beberapa saat sampai routerboard berkedip beberapa kali
4. Jika sudah selesai konfigurasinya akan kembali ke pengaturan pabrik dengan memiliki IP 192.168.88.1 pada interfacenya



Lab 12. Soft Reset

Di bab sebelumnya kita sudah membahas tentang **Hard Reset**, pada bab ini kita akan membahas tentang **Soft Reset**. Soft Reset bisa digunakan ketika kita masih bisa mengakses Routerboard kita. Jadi soft reset ini kita lakukan ketika kita bisa mengakses routerboard baik melalui Winbox ataupun terminal console (ssh/telnet). Jadi tidak perlu melakukan reset pakai jarum / ujung bolpoin lagi.

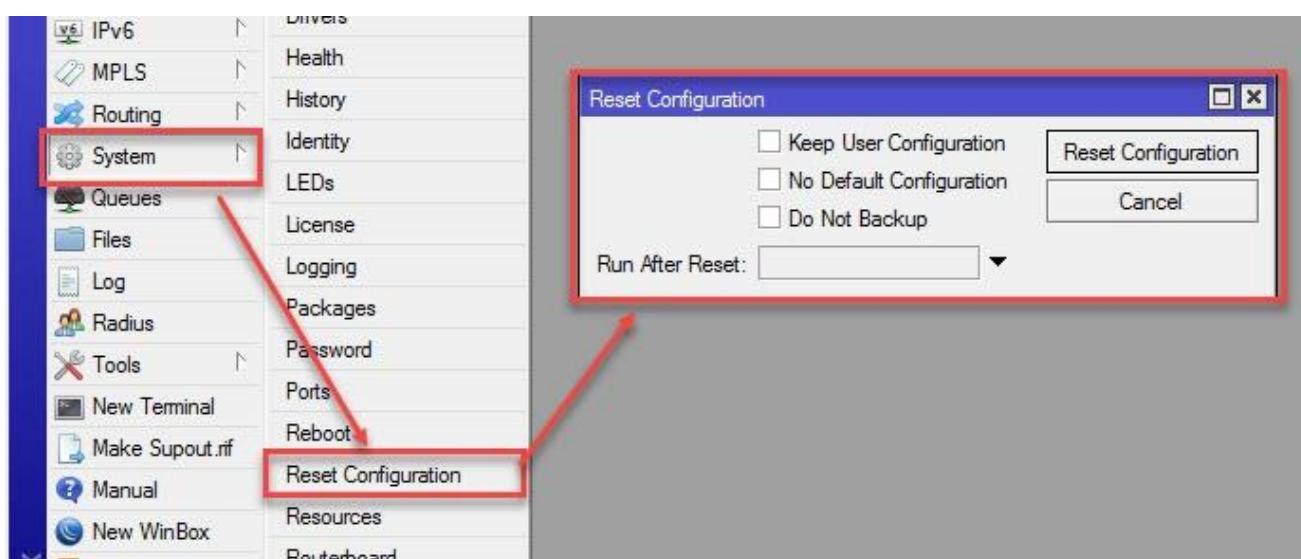
Pada Soft reset ini ada 3 mode reset yang bisa dilakukan yaitu:

- **Keep User Configuration** = Semua user dan Password yang kita tambahkan tidak akan terhapus, jadi selain user dan Password semua akan terhapus
- **No-Defaults Configuration** = semua konfigurasi akan direset / dihapus tanpa terkecuali, dan tidak akan membuat router menjadi settingan default pabrik
- **(Do Not Backup** = semua konfigurasi akan direset termasuk file back up

Ketika kita mereset RB secara soft reset kita bisa memilih salah satu dari ketiga type soft reset tersebut, maka nanti hasilnya semua konfigurasi akan keserupaan dan sama hasilnya ketika kita menggunakan Hard reset, yaitu akan mengembalikan settingan router menjadi pengaturan pabrik.

Untuk perintah soft reset secara CLI sebagai berikut:

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



Untuk perintah GUInya bisa diklik pada menu **System > Reset-Configuration**, kemudian pilih type soft resetnya kemudian klik **Reset Configuration**

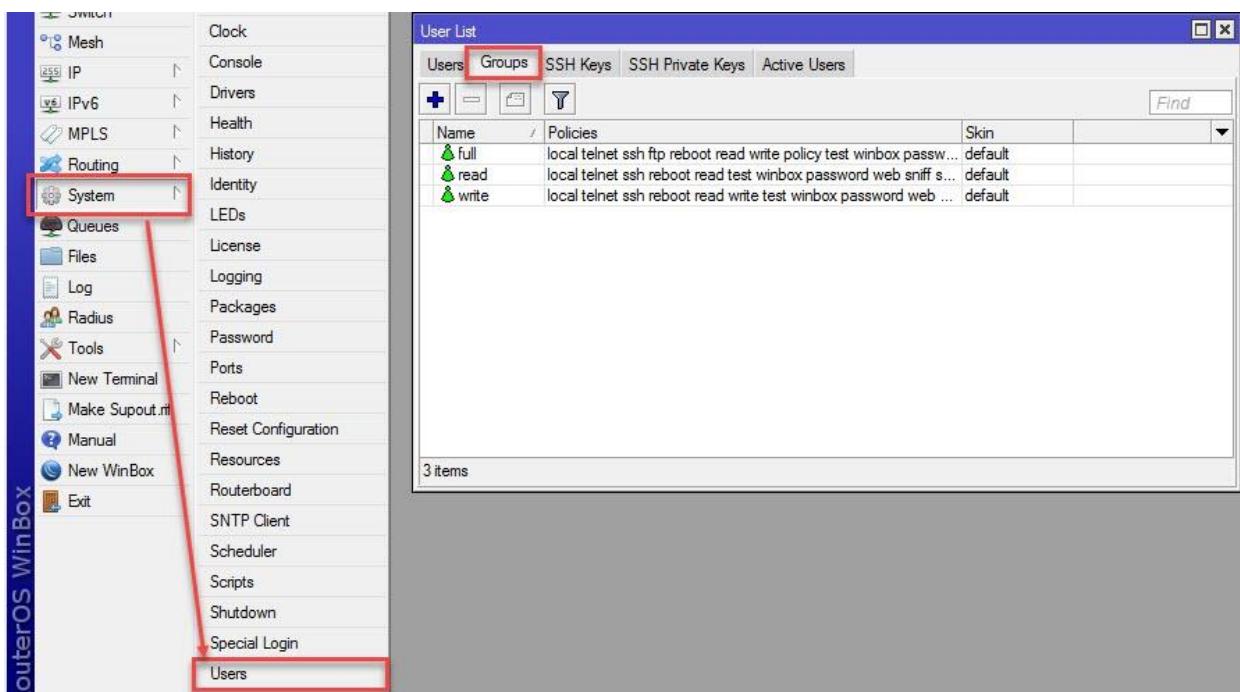
Jika sudah secara otomatis routerboard akan mereboot

Lab 13. User Login Management

User login management log in digunakan pengguna sebagai aturan untuk mengakses routerboard. Menu yang digunakan untuk mengatur User Login terdapat pada Menu **System > Users**. Manajemen User dapat dikelompokkan menjadi 2 kelompok yaitu:

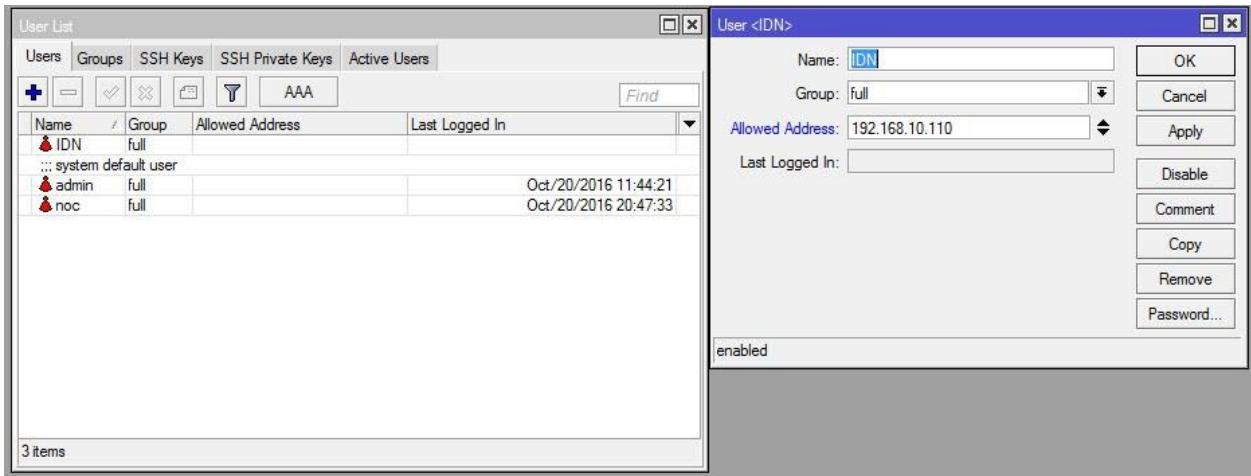
- **USER** = Pengguna yang berisi (username & password) dari suatu user
- **GROUP** = profil pengelompokan user berdasarkan penentuan privilege yang didapat dari suatu user. Jadi kita bisa tentukan privilege dari user tersebut.
Dalam hal ini terdapat 3 privilege yang bisa kita setting sesuai keinginan kita (costumize),
 - a. **Full** : User dapat melihat, menulis konfigurasi dan dapat melakukan konfigurasi dengan bebas
 - b. **Read** : User hanya dapat melihat isi menu dalam routerboard tersebut dan tidak dapat melakukan konfigurasi
 - c. **Write** : User hanya dapat mengkonfigurasi saja dan tidak bisa melihat hasil konfigurasi tersebut

Untuk bisa mengkonfigurasi mode GROUP bisa dilakukan pada menu **System > User > Groups**:

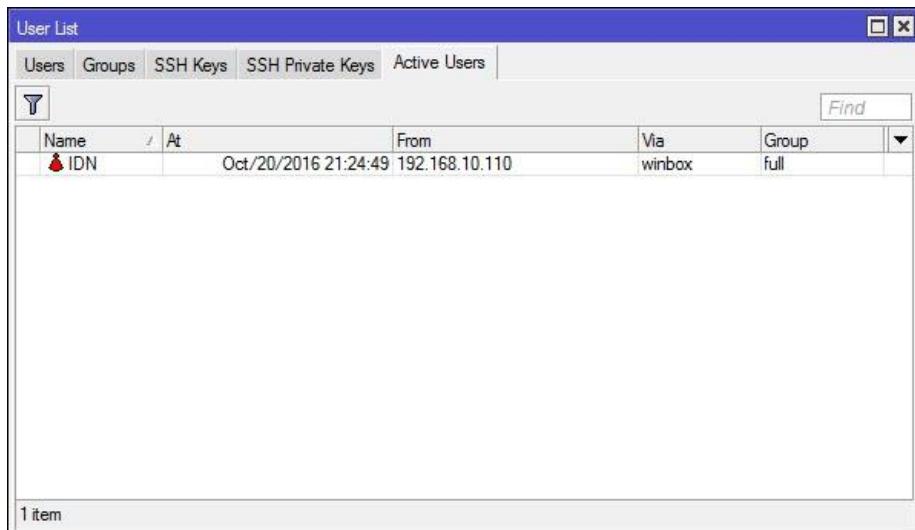


- User Management Akses

Pada tiap tiap user dibatasi hak aksesnya menggunakan group, dan juga tiap tiap user dibatasi berdasarkan IP address / network yang kita tentukan, jadi hanya ip address / network yang hanya bisa menggunakan user tersebut tersebut.



Untuk melihat user yang sedang aktif, bisa dilihat pada menu **System > User > Active Users**



Management user digunakan untuk memproteksi routerboard kita berdasarkan user/ pengguna dan ini bermanfaat agar akses routerboard kita tidak diotak atik & disalah gunakan oleh sembarang orang.

Lab 14. Merubah Identity (nama) Routerboard

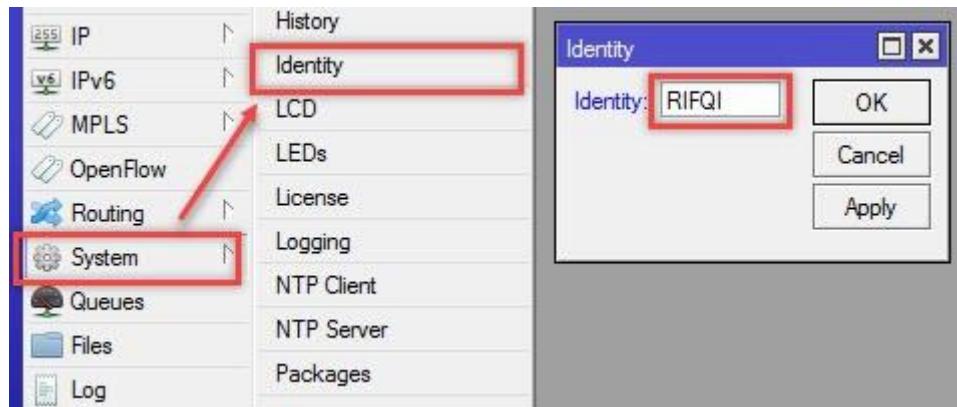
Secara default dari mikrotiknya, routerboard kita memiliki identity berupa **Mikrotik**, akan tetapi kita diberi kebebasan untuk mennganti Identity tersebut sesuai dengan keinginan kita.

Tujuan merubah identity pada routerboard supaya kita tidak salah meremote dalam mengkonfigurasi suatu router, karena jika identity sama antar router maka akan memungkinkan kita ketika akan meremote routerboard.

Untuk CLI bisa dikonfigurasi dengan perintah:

```
[admin@MikroTik> System Identity set name=[Identity yang akan digunakan]
```

Untuk yang GUI dapat dikonfigurasi seperti berikut



Lab 15. Merubah Tanggal dan Waktu

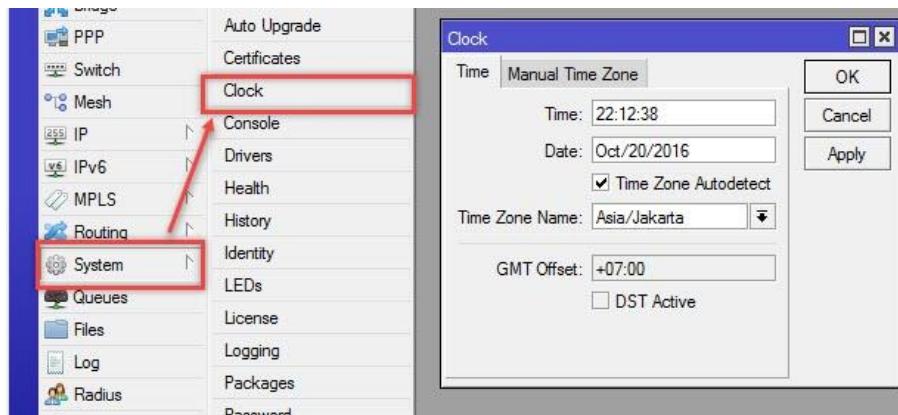
Merubah tanggal dan waktu pada mikrotik, merupakan lab dasar tapi sangat berpengaruh sangat besar kepada kita, kenapa? Karena waktu pada routerboard bisa menunjukkan suatu kejadian yang terjadi pada routerboard. Oleh karena itu merubah tanggal dan waktu pada routerboard menjadi up to date sesuai dengan pengaturan waktu yang berlaku adalah saatu keharusan yg harus dilakukan.

Untuk pengaturan via CLI perintah yang bisa dilakukan sebagai berikut:

```
[admin@rifqi> system clock set time=21:59:00 date=oct/20/2016 time-zonename=Asia/Jakarta
```

Penjelasan perintah diatas sebagai berikut, bisa dilihat pada pengisian time kita harus mengisikannya secara lengkap yaitu **Jam:menit:detik** kemudian pada bagian date kita harus mengisikannya dengan format **Bulan/Tanggal/Tahun**. Untuk bagian bulan tidak dapat diisi dengan nominal angka, jadi harus menggunakan 3 kata depan bulannya dalam format Inggris. Kemudian sesuaikan Zona Waktu yang berlaku

Untuk mode GUI bisa pada menu **system > clock**, kemudian isikan waktu, tanggal dan juga zona waktunya



Lab 16. Backup dan Restore

Pada lab ini kita akan membahas mengenai backup dan restore konfigurasi pada routerboard, maksud dari backup adalah menyimpan seluruh konfigurasi dari routerboard. nah kenapa kita harus melakukan backup? Why? Karena kita harus mengamankan (menyimpan) seluruh konfigurasi, jika terjadi sesuatu pada routerboard kita.

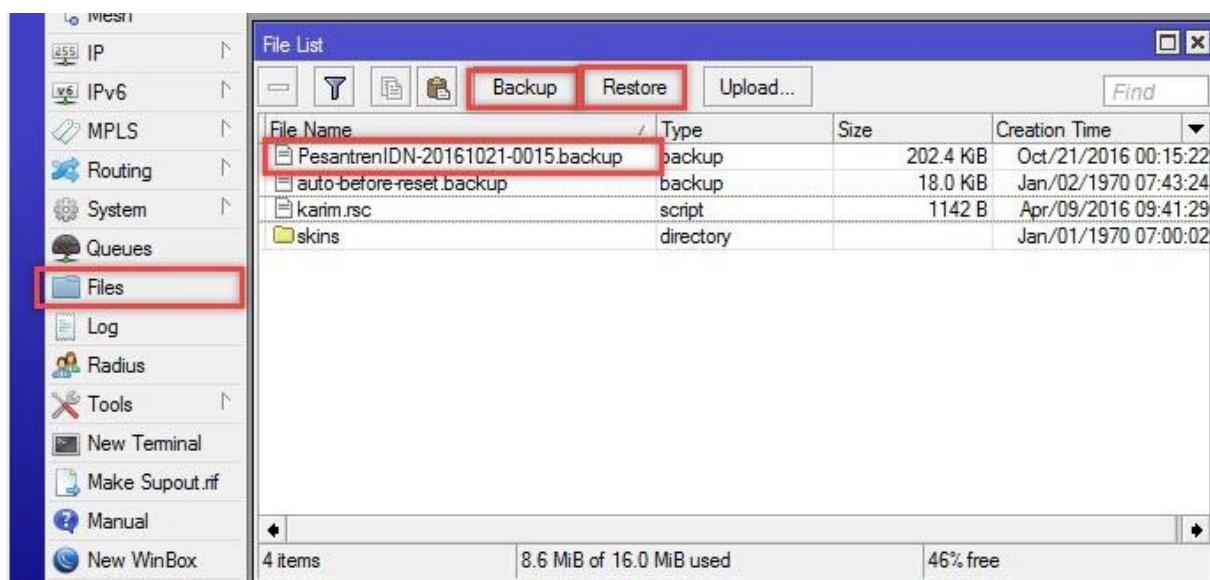
Jadi ketika routerboard kita eror atau kita melakukan kesalahan dalam konfigurasi, kita bisa merestor hasil backup yang sudah dibuat / disimpan sebelumnya.

Mode Backup sendiri ada 2 type, yaitu:

Binary file (.backup)	Script file (.rsc)
Tidak dapat dibaca oleh text editor	Hasil berupa script, dapat dibaca oleh text editor
Membacup seluruh konfigurasi router	Dapat membackup sebagian atau seluruh konfigurasi yang ada dalam routerboard
Hasil dari file backup ketika direstore akan kembali ke konfigurasi backup (semula)	Hasil dari file backup script ketika direstore tidak akan mengembalikan seperti konfigurasi semula, malainkan hanya penambahan script pada konfigurasi utama
Perintah (command) berupa: backup / restore	Perintah (command) berupa: Export / Import
Membutuhkan reboot ketika direstore	Tidak membutuhkan reboot ketika direstore

Lab 17. Backup Binary

Untuk perintah backup binary dapat dilakukan pada menu **File > Backup**, dengan mengklik submenu **Backup**. Untuk memindahkan file hasil backup bisa dengan ftp ataupun dengan melakukan drag & drop file binary ke folder PC kita



sedangkan untuk restore bisa dilakukan dengan mengklik submenu **Restore** pada menu file, untuk file yang masih ada dalam folder pc kita bisa dilakukan dengan mengklik submenu **Upload** dan cari file backup binary yang tadi kita simpan, atau bisa juga dengan melakukan drag & drop file .binary ke winbox pada menu file, kemudian klik file .binary backup tadi dan klik restore, selanjutnya jangan lupa **reboot** routerboard.

Lab 18. Export & Import

Untuk lab kali ini, kia akan melanjutkan materi lab pada bab sebelumnya, untuk materi export & import terdapat pada lab sebelumnya. Pada backup script kita hanya bisa menggunakan fasilitas CLI untuk melakukan perintah export dan import. Pada lab ini saya akan mencontohkan export seluruh konfigurasi routerboard dan sebagian konfigurasi pada routerboard. Sebelum nya buka terlebih dahulu menu **new terminal** pada winbox.

Untuk perintah Export keseluruhan konfigurasi sebagai berikut:

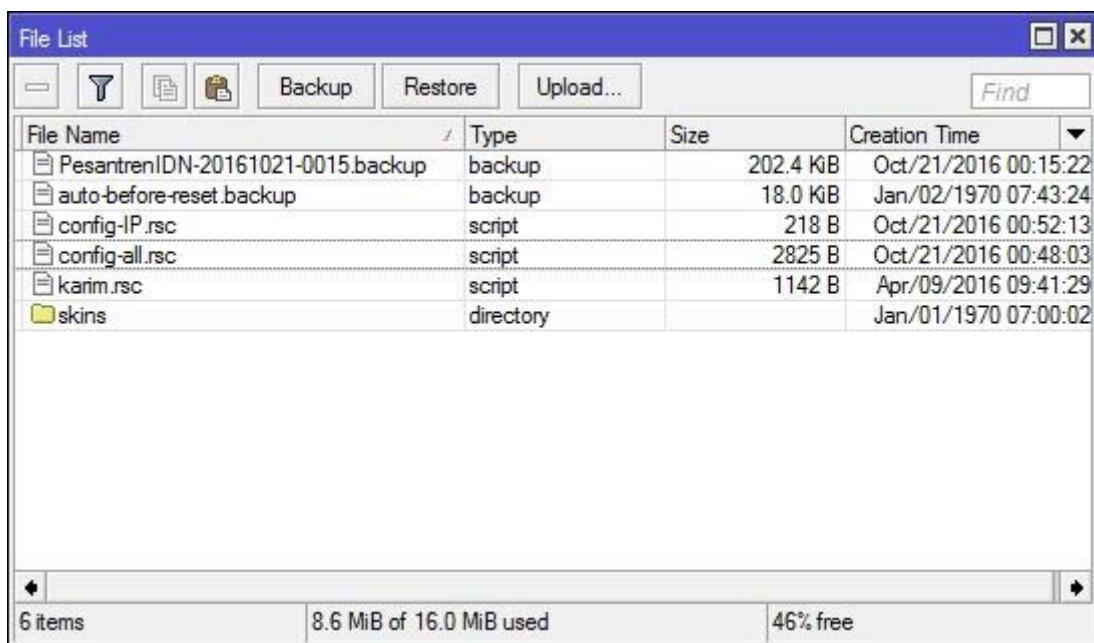
```
[admin@IDN] > export file=config-ALL
```

Sedangkan sebagian konfigurasi sebagai berikut:

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

Kemudian check hasil file export tadi menu file, bisa melalui GUI atauapun CLI

```
[IDN@PesantrenIDN] > file print
# NAME          TYPE          SIZE CREATION-TIME
0 skins         directory
1 PesantrenIDN-2016102... backup      202.4KiB oct/21/2016 00:15:22
2 config-IP.rsc script        218 oct/21/2016 00:52:13
3 config-all.rsc script       2825 oct/21/2016 00:48:03
4 karim.rsc    script        1142 apr/09/2016 09:41:29
5 auto-before-reset.ba... backup      18.0KiB jan/02/1970 07:43:24
[IDN@PesantrenIDN] >
```



Untuk import bisa dilakukan dengan perintah sebagai berikut:

```
[admin@IDN] > import (file script yang tadi disimpan)
```

```
[admin@MikroTik] > import config-all.rsc
Script file loaded and executed successfully
[admin@RIFQI] >
```

Lab 19. Install Ulang Routerboard (Netinstall)

Install ulang routerboard mikrotik dapat dilakukan dengan berbagai macam cara, salah satunya adalah **Netinstal**, netinstall sendiri adalah software yang digunakan untuk menginstal routerboard melalui jaringan ethernet yang ada pada routerboard. Netinstall digunakan ketika routerboard yang kita miliki, mengalami eror berupa lupa username dan password, gagal melakukan upgrade, kerusakan os, rusak.

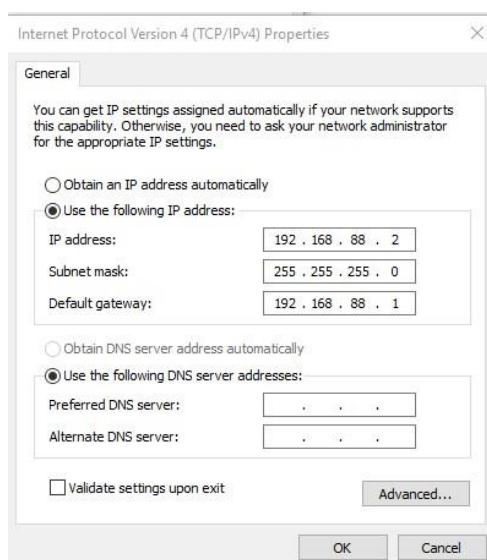
Syarat netinstall adalah, perangkat routerboard kita harus mendukung boot melalui ethernet dan harus ada link ethernet routerboard yang terhubung ke ethernet yang ada pada pc / laptop kita. Intinya pada netinstall system routerboard kita akan terlihat seperti routerboard yang masih baru.

Software & hardware yang dibutuhkan:

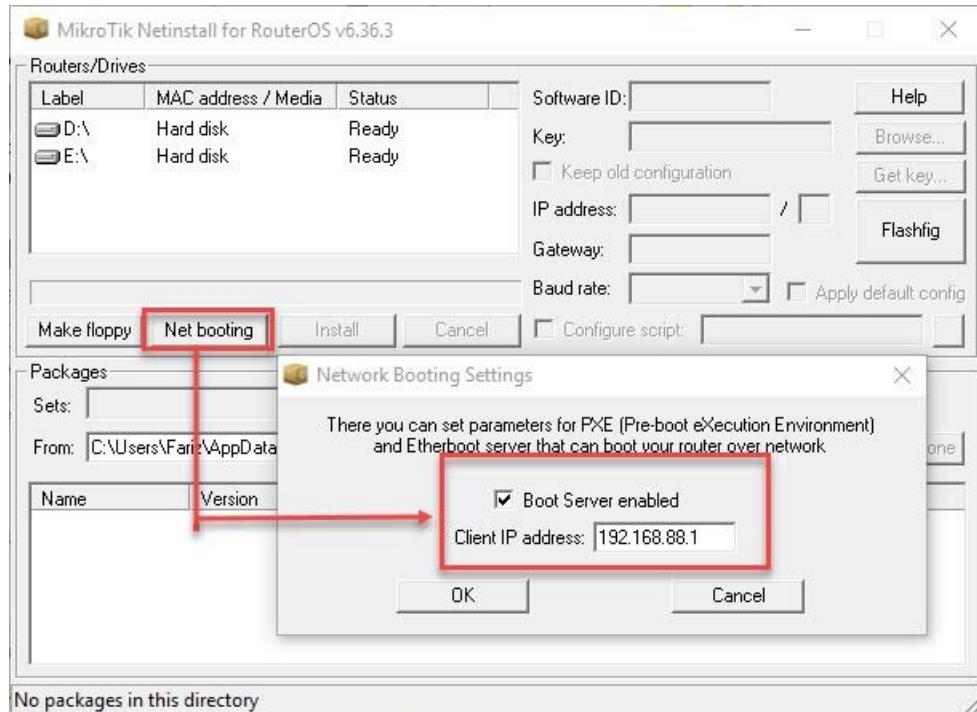
1. Softwae Netinstall dapat didownload di website (<http://www.mikrotik.com/download/>)
2. Paket software router os, sesuai dengan arsitektur yang dipakai, seperti x86, mipsbe, smips, tile, ppc, arm, mipsle dll pada situs (<http://www.mikrotik.com/download/>)
3. Kabel UTP

Untuk eksekusi instalasi dengan netsinstall sebagai berikut:

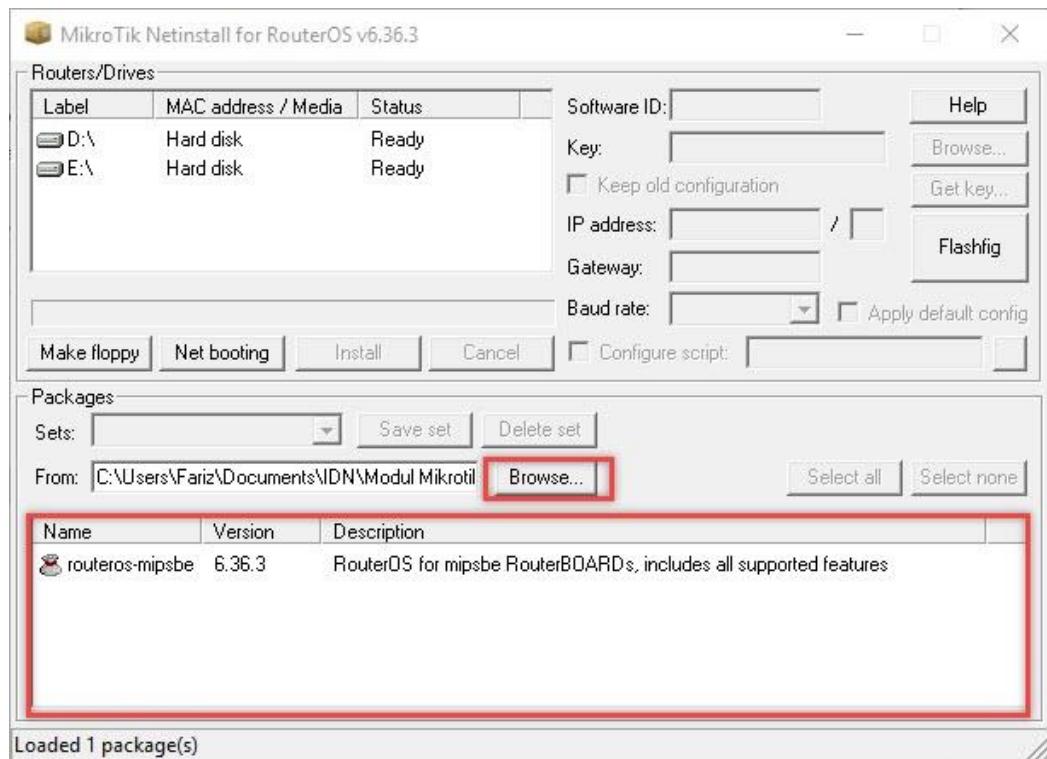
1. Setelah semua software dan paket os sudah didownload, ekxtrak dan tempatkan pada suatu folder yang mudah kita temukan
2. Konfigurasikan static ip address pada laptop kita yang satu network dengan ip address yang ada pada salah satu interface router kita. Misalnya pada laptop kita ip address 192.168.88.2 netmask 255.255.255.0



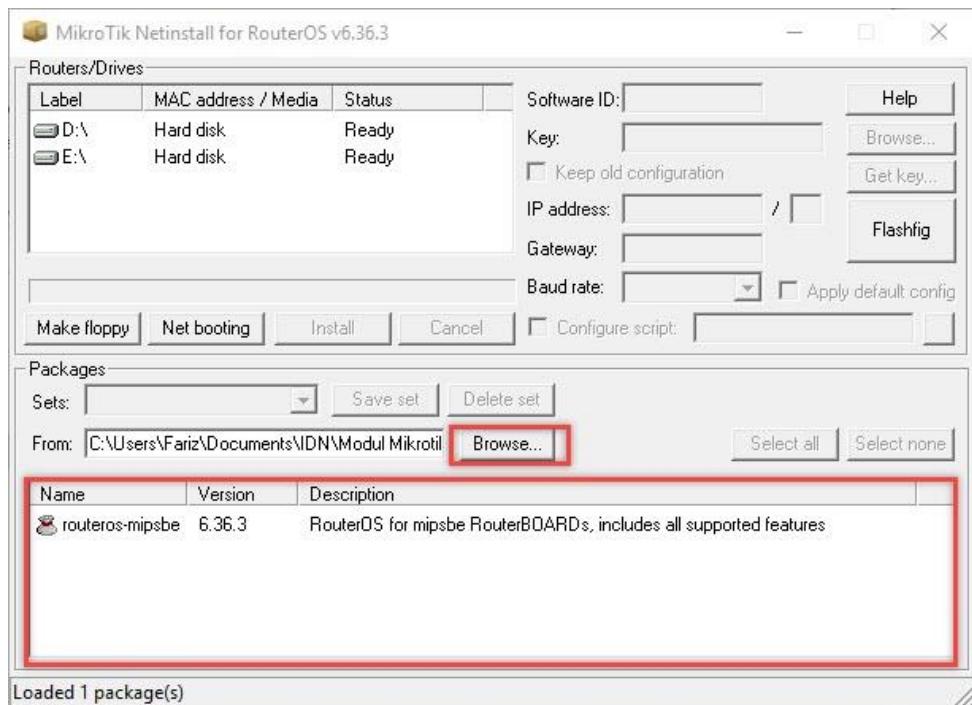
3. Tancapkan kabel utp antara ethernet laptop kita dan ethernet pada routerboard
4. Jalankan program netinstall dan tekan tombol **Net booting**, kemudian centang pada pilihan Boot Server enable untuk mengaktifkannya, lalu sisikan client ip address (ip address pada ethernet router, yaitu 192.168.88.1)



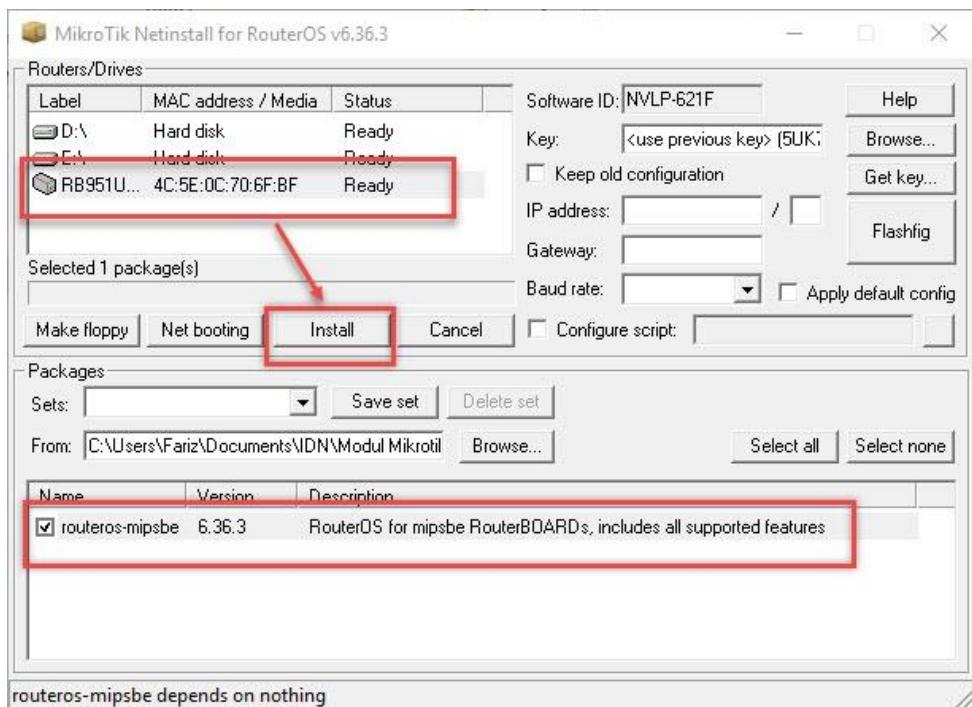
5. Pada menu packages tekan tombol browse, lalu pilih folder dimana tadi kita menyimpan file paket os .npk yang tadi sudah didownload. Contoh: karena saya menggunakan Routerboard Series 951Ui-2HnD, maka arsitektur paket yang saya download adalah arsitektur jenis **MIPSBE**. Sesuaikan saja arsitektur mikrotik yang anda miliki dengan paket routerboard yang akan diinstal



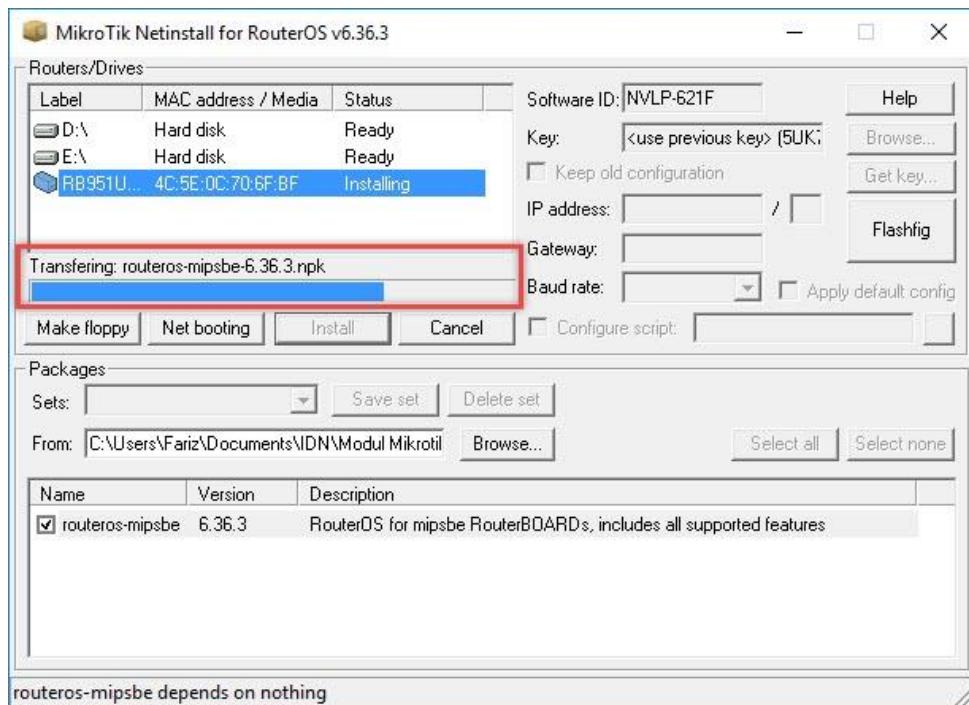
6. Pastikan routerboard dalam kondisi off dan kabel utp sudah tertancap pada ethernet routerboard dan laptop
7. Gunakan metode **Hard reset**, dengan menekan tombol reset yang ada pada router dan tahan
8. Ketika menekan & menahan tombol reset, nyalakan router dengan menancapkan power adaptornya
9. Tunggu beberapa saat sampai mac-address router terdeteksi pada netinstall, lalu lepaskan tombol reset, dan klik paket yang akan digunakan untuk instalasi



10. Kilik pada mac-address routerboard, dan tekan tombol install,



11. Tunggu sebentar sampai proses instalasi selesai



12. Setelah muncul keterangan Finished pada netinstall, routerboard secara otomatis akan mereboot dan tunggu hingga proses reboot selesai.

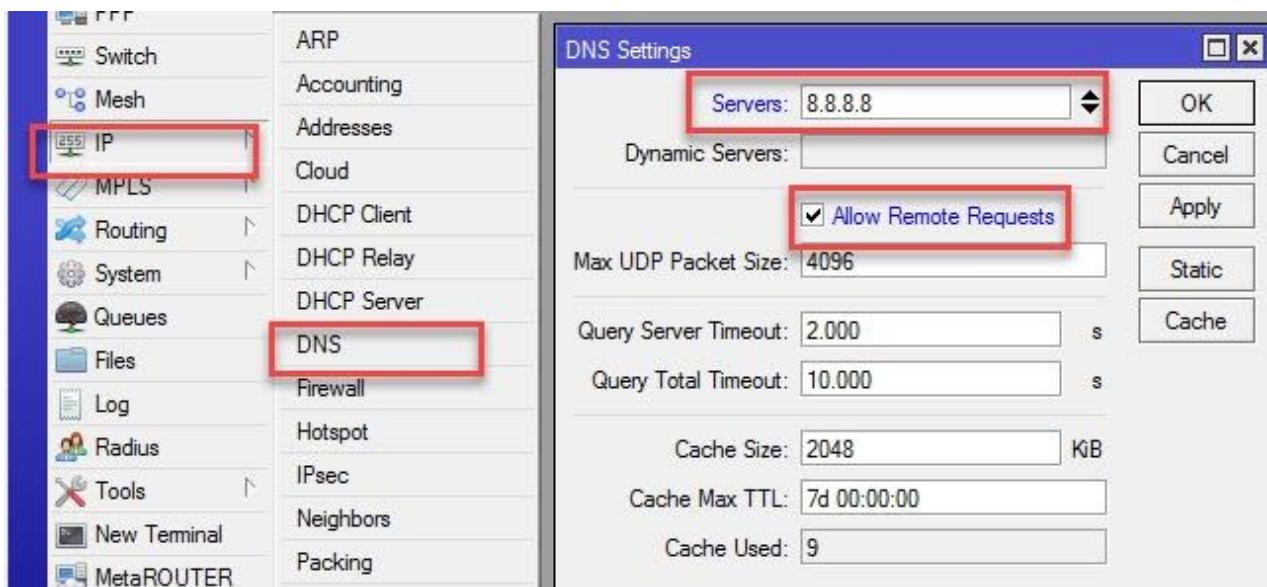
Perlu diingat, proses instalasi dengan menggunakan netinstall akan menghapus semua konfigurasi yang ada didalam router, untuk default aksesnya **usernmae=admin password=(kosong,tidak perlu diisi)**.

Lab 20. Konfigurasi DNS

DNS (Domain Name System) adalah system yang memetakan IP address menjadi sebuah domain ataupun sebaliknya. Jadi kita tidak perlu menghafal tiap tiap ip address dari suatu situs, bayangkan saja kalau kita mengakses suatu website memakai ip address, kalau 1 website sekiranya masih bisa, jika sangat banyak?? Maka DNS berperan penting disini karena dns mentranslasikan ip address menjadi sebuah name.

Pada mikrotik kita akan menambahkan IP dari DNS server, kita bisa menggunakan dns dari isp tempat kita langganan atau bisa juga melalui DNS public, contohnya milik google (8.8.8.8 dan 8.8.4.4). pada pembahasan kali ini kita akan menambahkan ip dns google

Untuk menambahkan dns bisa dilakukan pada menu **IP > DNS**



Ketika kita mengaktifkan **Allow Remote Request**, yang berarti client yang terhubung ke routerboard kita tidak perlu lagi menggunakan DNS sebelumnya, cukup menggunakan dns yang ada pada routerboard kita

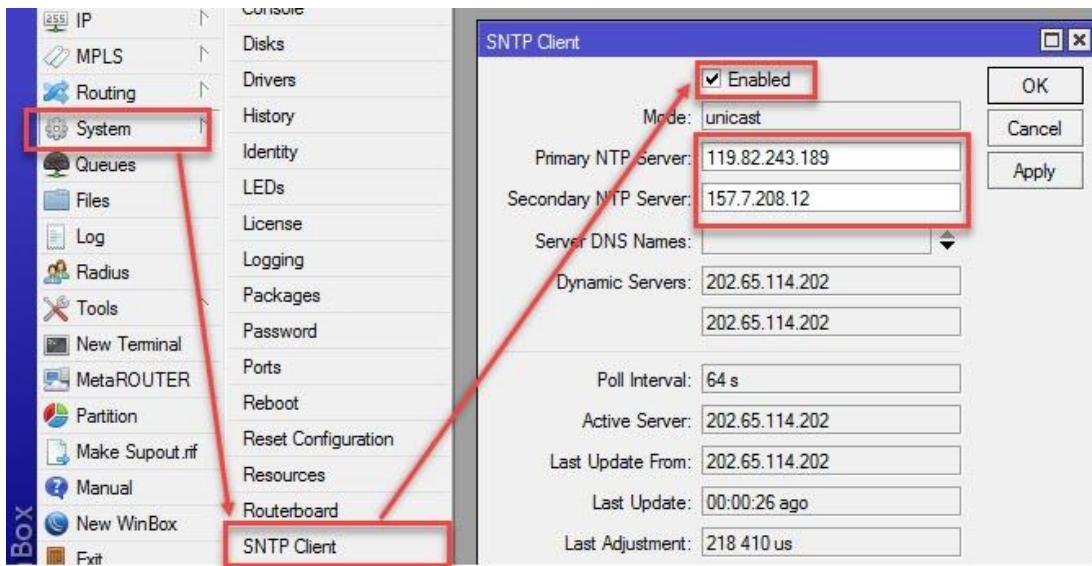
Lab 21. Konfigurasi NTP Client

Dalam lab kali ini kita akan membahas mengenai NTP (Network Time Protocol), NTP adalah sebuah mekanisme atau protokol yang digunakan untuk sinkronasi terhadap time secara online. NTP sendiri menggunakan port 123 UDP. Kenapa kita menggunakan NTP? Terkadang pada routerboard yang tidak memiliki baterai cmos, atau battery cmosnya rusak, kejadiannya router setelah direboot waktu dalam routerboardnya akan kembali ke waktu pengaturan default yaitu pada tahun 1970. Untuk menhindari ketidakpastian akan akurasi waktunya makanya kita akan mengkonfigurasi NTP client pada routerboard kita.

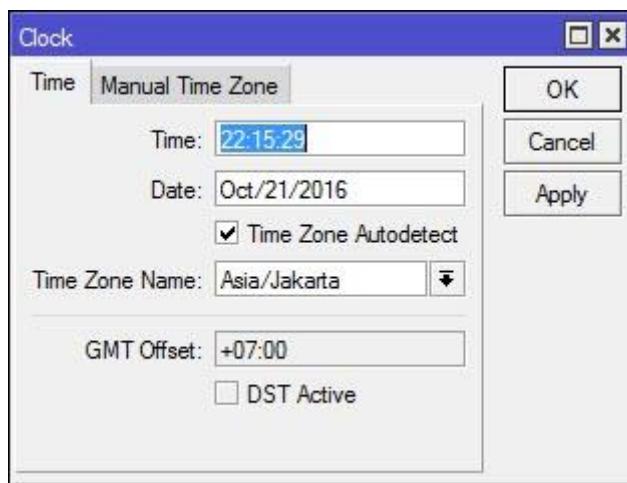
Sebelumnya kita harus tahu ip address dari server NTP yang akan kita pakai, berikut saya bagikan ip address ntp yang bisa dipakai:

- 119.82.243.189
- 157.7.208.12
- 103.18.128.60

Untuk menu konfigurasi NTP client terdapat pada menu **System > SNTP Client**, aktifkan sntp client dengan mencentang tanda enable dan mengisi form ntp server yang tersedia



Pengujiannya bisa dicheck pada menu **System > Clock**, sekarang kita tidak perlu risau lagi tentang akurasi waktu pada routerboard kita.



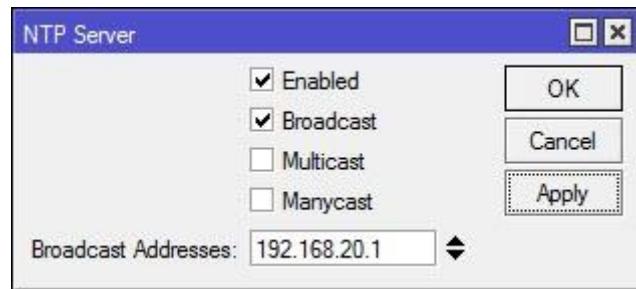
Lab 22. Konfigurasi NTP Server

Untuk menggunakan fitur NTP server pada routerboard, secara default dalam routerboard tidak terdapat paket **NTP Server**, jadi kita harus melakukan instalasi sendiri packet ntp servernya. Untuk paketnya bernama **ntp.npk** bisa didownload pada website www.mikrotik.com/download pilih yang extra package. Sesuaikan juga arsitektur yang digunakan

Fungsi ntp server sendiri adalah kita bisa membuat server ntp ini agar bisa digunakan oleh ntp client yang masih dalam satu network, jadi cukup mencari update informasi time pada jaringan lokal saja

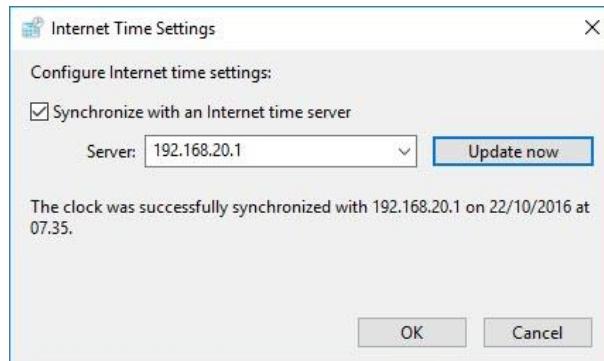
Metode penyebaran informasi waktu pada NTP Sever kita bisa menggunakan mode **Broadcast**, **Multicast**, **Manycast**. NTP server dapat dikonfigurasi pada menu **System > NTP Server**.

Berikut contoh konfigurasi NTP Server pada network 192.168.20.0/24, konfigurasikan ip 192.168.20.1 sebagai ip ntp server, lalu type yang dipakai adalah **Broadcast**.



Pada sisi client pengguna ntp server, ntp client tinggal memasukkan ip ntp server yang sudah kita buat sebelumnya dengan type yang sama dengan yang ada pada ntp server.

Untuk client yang menggunakan OS windows cukup tambahkan ip ntp server saja pada Internet Time Setting



Lab 23. Menghubungkan PC ke Internet dengan Routerboard Mikrotik

Pada lab-lab sebelumnya kita telah banyak membahas tentang konfigurasi dasar dari mikrotik, pada materi berikut kita akan menghubungkan routerboard kita ke internet dan memberikan akses internet ke PC/Laptop kita. Karena fungsi utama dari router adalah menghubungkan jaringan yang berbeda.

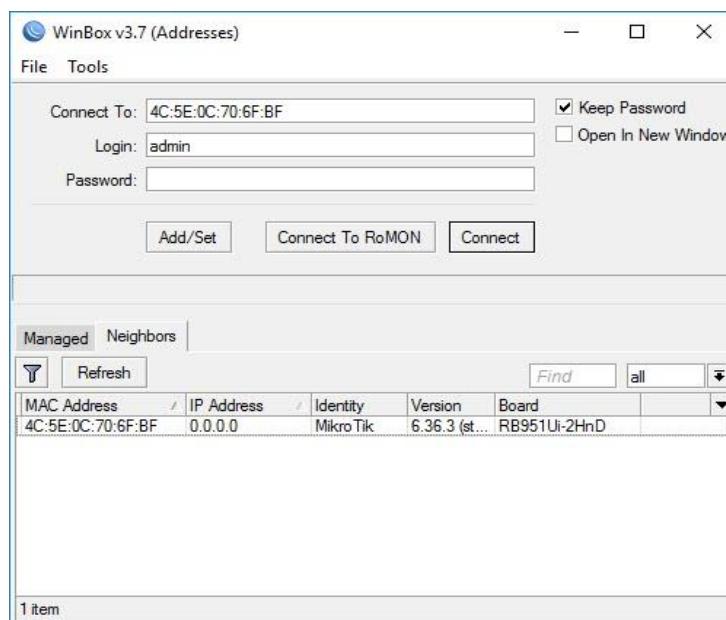
Sebelum konfigurasi kita pahami dahulu topologi berikut:



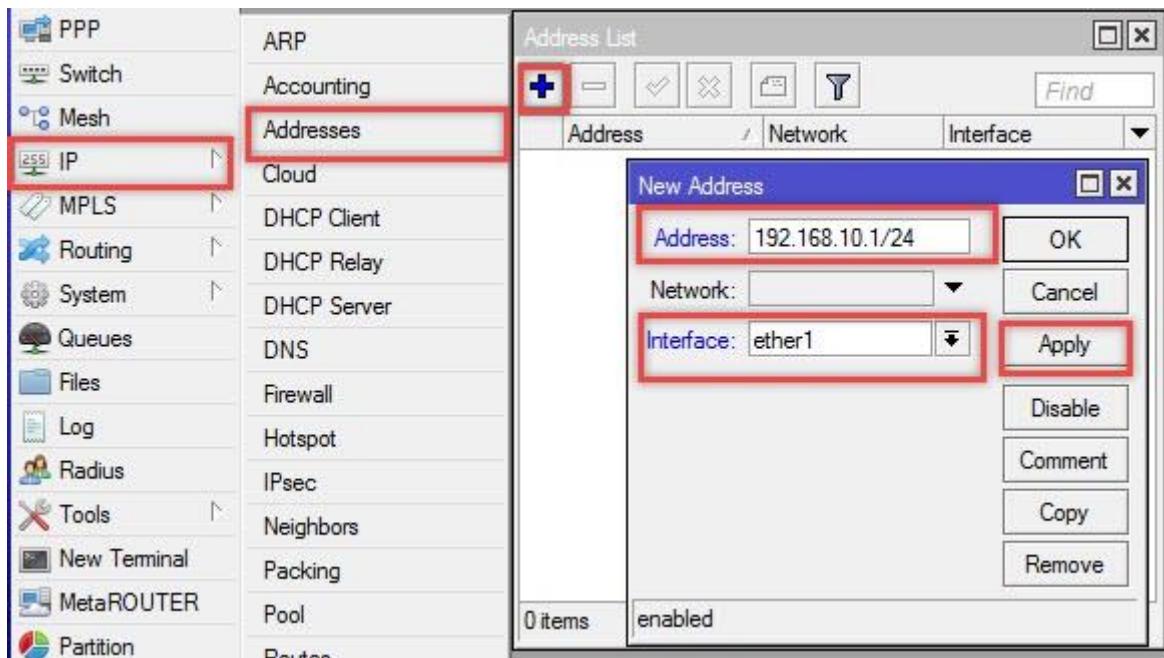
Pada lab ini saya akan mengkonfigurasi menggunakan Routerboard **951Ui-2HnD**, untuk akses ke mikrotiknya saya menggunakan winbox agar lebih mudah diikuti dan dipahami.

Lab 24. Konfigurasi IP Address Pada Routerboard

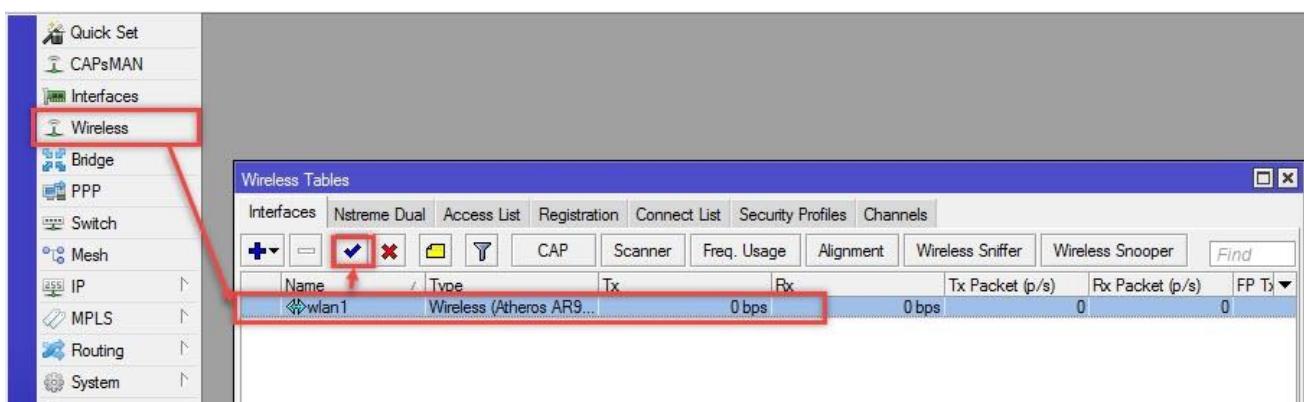
1. Akses routerboard Melalui winbox



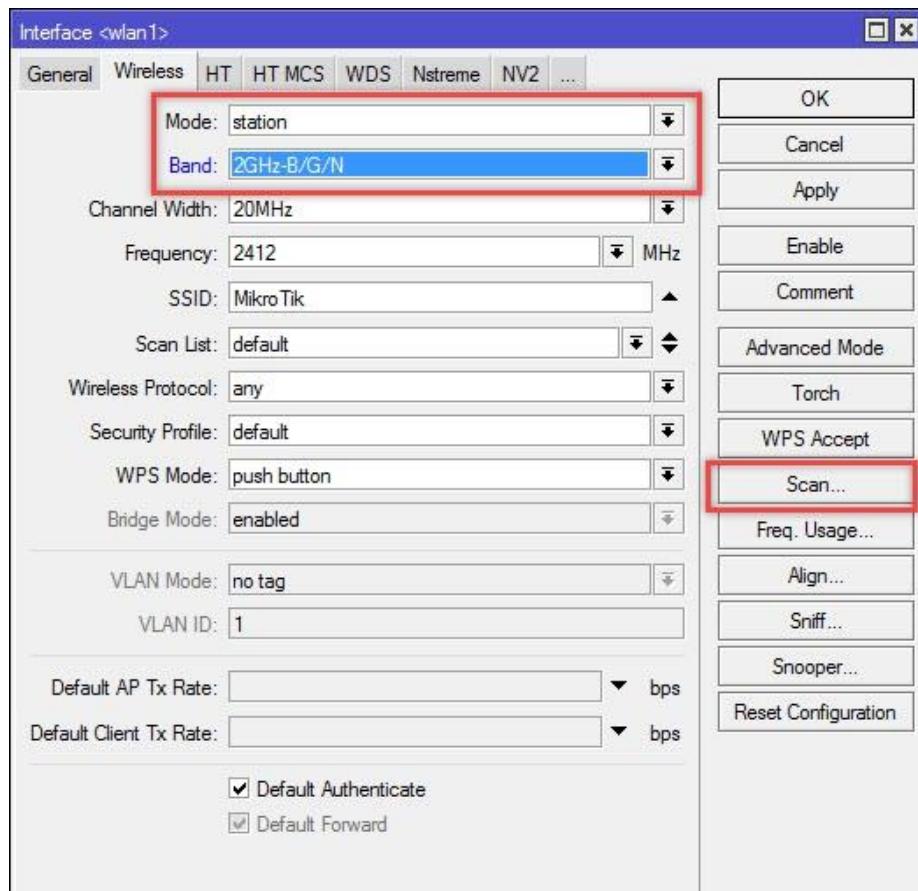
2. Masuk ke menu IP > Address untuk menambahkan IP address pada interface ethernet yang terhubung ke laptop/pc kita. Parameter yang kita set adalah **IP Address= 192.168.10.1/24** dan **interface= ether1**



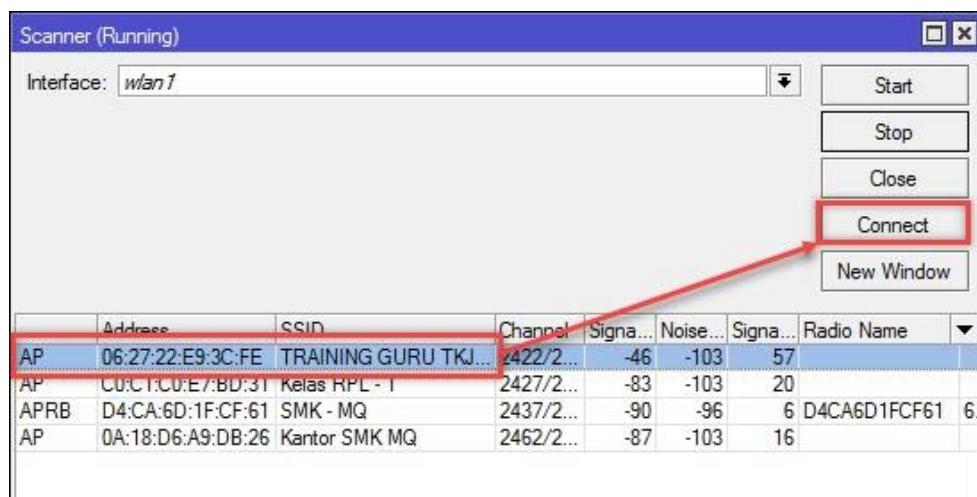
3. Kemudian aktifkan fitur wireless, pada menu **Wireless > Interfaces**. Aktifkan wlan1 dengan mengklik tombol enable.

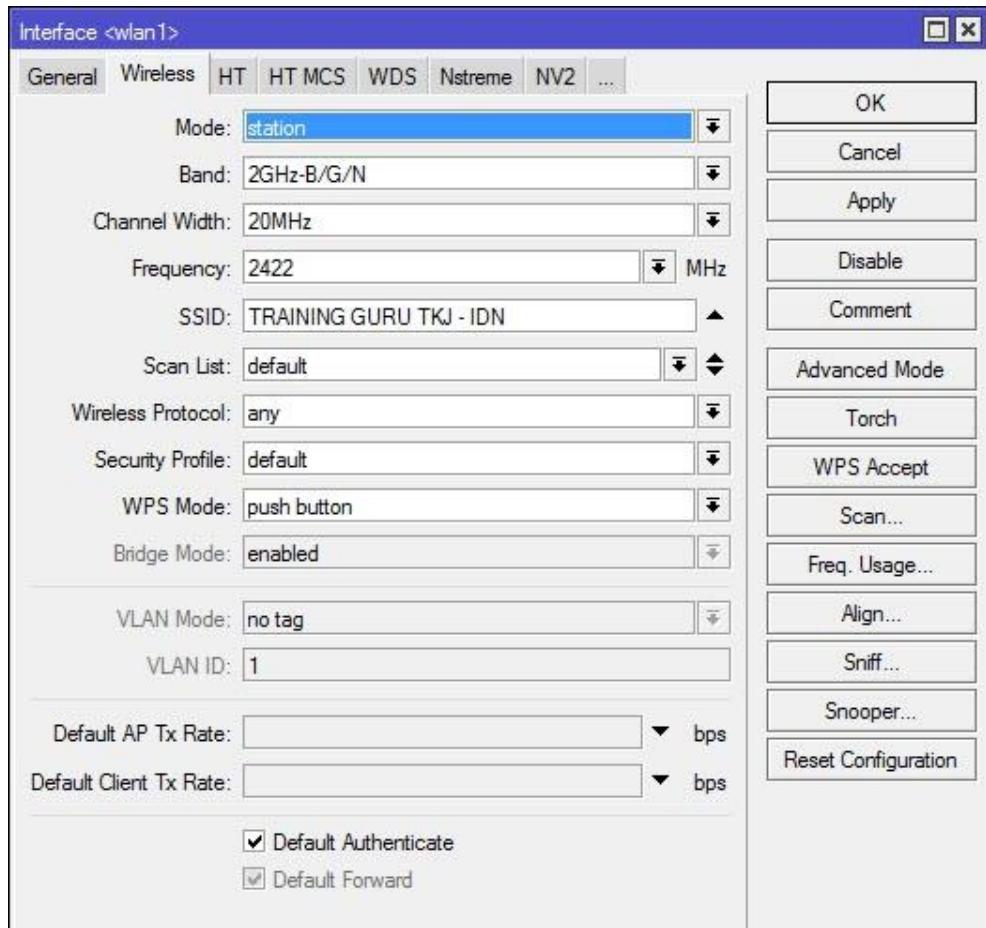


4. Kemudian double klik pada wlan1, untuk mengkonfigurasi wireless menjadi mode station (client) agar bisa terhubung ke Access Point. Untuk parameter yang kita konfigurasi sebagai berikut: Mode: **Station**, Band=2GHzB/G/N (bisa berubah ubah otomatis sesuai band yang ada pada Access Point).

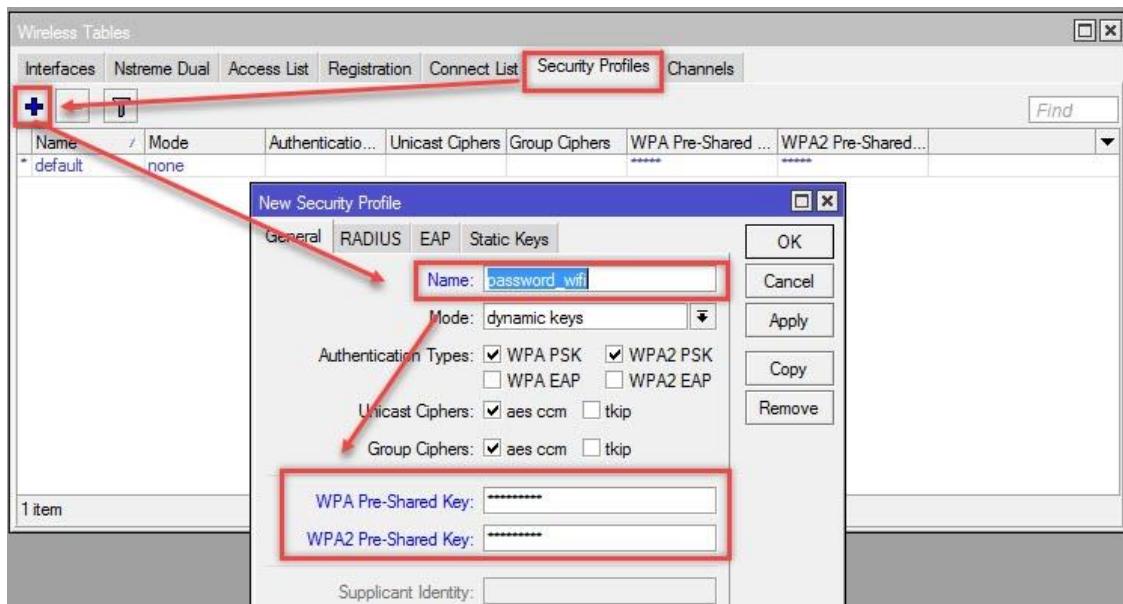


5. Kemudian klik tombol **scan** untuk mencari access point yang akan hubungkan, lalu klik name access point yang akan kita hubungkan, kemudian klik tombol **connect**

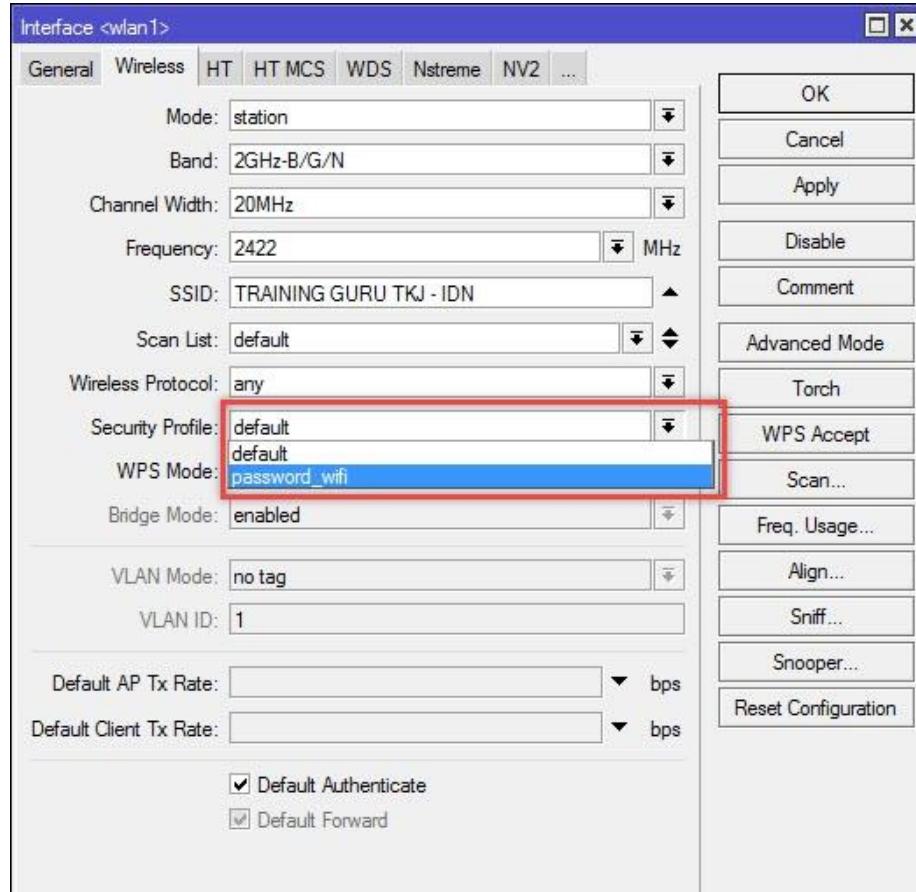




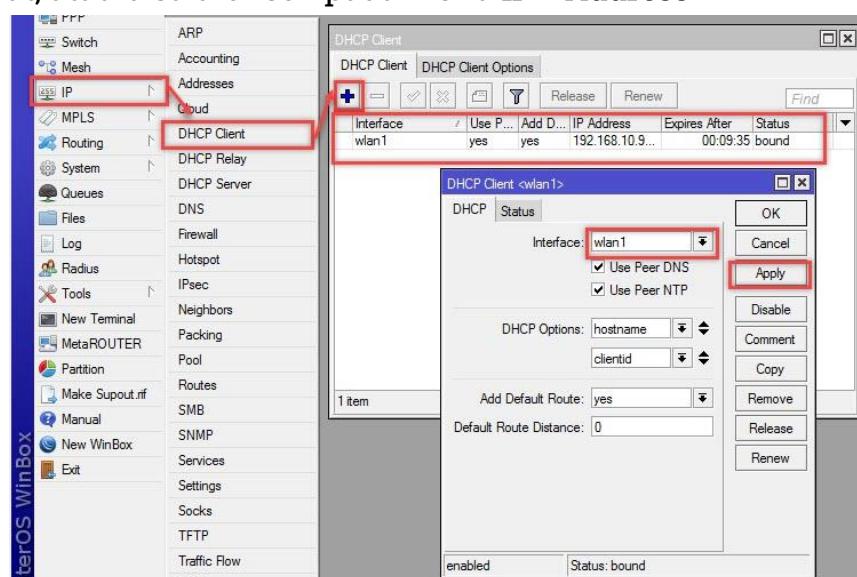
6. Karena access point yang kita hubungkan terdapat authentifikasi password, maka kita sebagai sisi client (station) kita harus menambahkan password pada **Security Profile** agar routerboard kita bisa terhubung ke Access Point. Untuk menambahkan password, bisa dilakukan pada menu: **Wireless > Security Profile**. Password access point bisa ditambahkan pada kolom yang disediakan



7. Masuk lagi pada tab Wireless > Interface, untuk memasukkan security profile yang tadi kita buat



8. Kemudian konfigurasikan **DHCP-Client**, pada interface wlan1. Parameter yang dikonfigurasi pada dhcp client adalah **interface=wlan1**. Kemudian tunggu sampai status berubah menjadi **bound** dan terdapat keterangan ip dhcp-client yang didapat, atau bisa dicheck pada menu IP > Address



9. Kemudian test koneksi internet apakah sudah bisa terhubung ke internet atau belum, bisa dites melalui ping google.com pada terminal.

```
[admin@MikroTik] > ping google.com
SEQ HOST SIZE TTL TIME STATUS
0 74.125.68.101 56 43 32ms
1 74.125.68.101 56 43 47ms
2 74.125.68.101 56 43 154ms
3 74.125.68.101 56 43 104ms
4 74.125.68.101 56 43 41ms
5 74.125.68.101 56 43 75ms
6 74.125.68.101 56 43 32ms
7 74.125.68.101 56 43 42ms
```

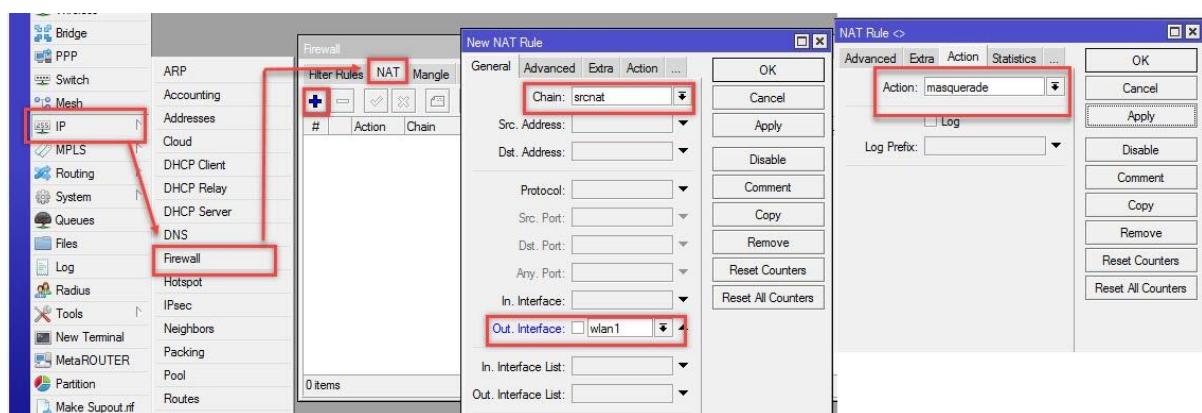
10. Konfigurasikan NAT (Network Address Translation) agar pc/ laptop kita juga bisa terhubung ke internet. NAT ini berfungsi menterjemahkan alamat ip private ke dalam ip public. NAT digunakan karena keterbatasan akses internet kita menggunakan IP Public.

Untuk Konfigurasinya bisa dilakukan pada menu IP > Firewall > NAT. Untuk parameter pada menu NAT berupa:

Chain: srcnat

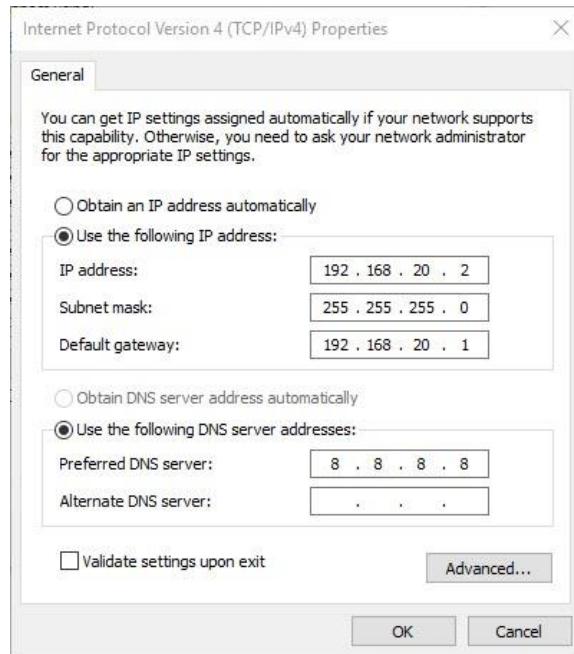
out interface: wlan1 (tergantung dari mana sumber internet)

Action: Masquerade



- Konfigurasi IP Address Pada PC/Laptop

Konfigurasikan Ip address beserta dns pada interface ethernet laptop/ pc agar bisa terhubung ke internet



Lakukan test ping internet dengan mengakses menggunakan ping ke google.com

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

C:\Users\Fariz>ping google.com

Pinging google.com [216.58.221.78] with 32 bytes of data:
Reply from 216.58.221.78: bytes=32 time=33ms TTL=51
Reply from 216.58.221.78: bytes=32 time=52ms TTL=51
Reply from 216.58.221.78: bytes=32 time=33ms TTL=51
Reply from 216.58.221.78: bytes=32 time=34ms TTL=51

Ping statistics for 216.58.221.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 52ms, Average = 38ms

C:\Users\Fariz>
```

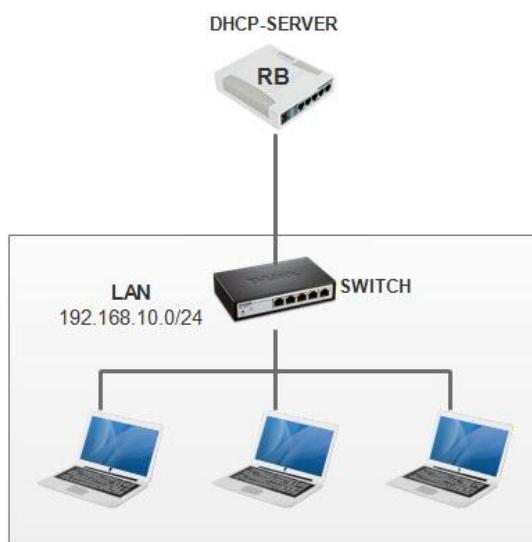
NETWORK MANAGEMENT

Bab 2. Network Management

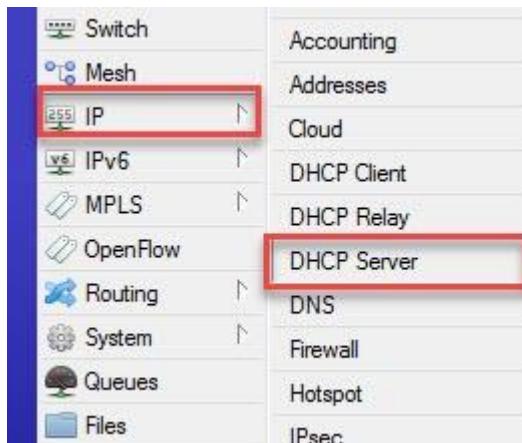
Lab 25. Konfigurasi DHCP-Server

DHCP adalah suatu paket yang mendistribusian ip address secara otomatis. Pada lab ini kita akan mengkonfigurasikan Routerboard mikrotik sebagai DHCP-Server, jadi nantinya client tidak perlu lagi mensest manual ip address pada devicenya.

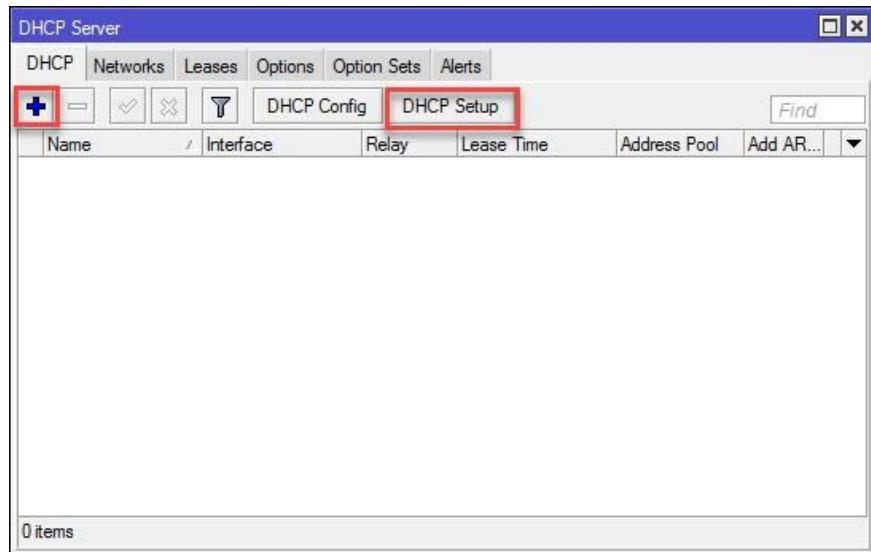
Topologi yang digunakan sebagai berikut:



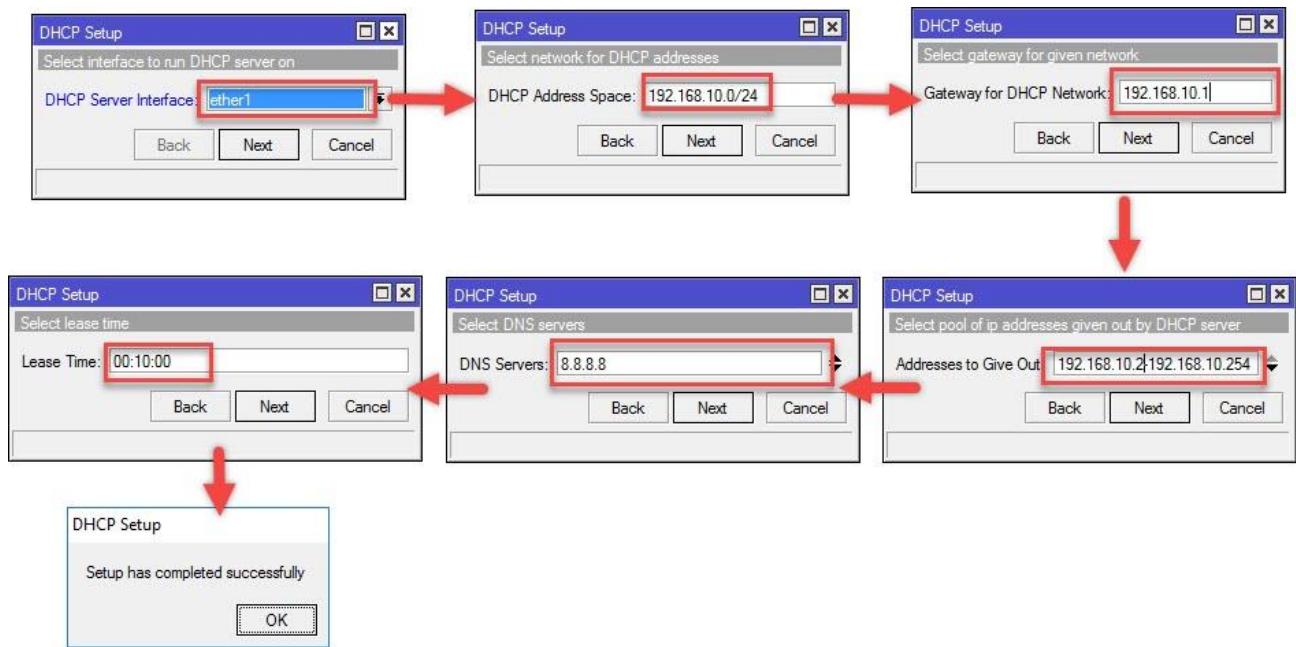
1. Pastikan sudah mengkonfigurasi ip address pada interface yang terhubung ke interface switch
2. Masuk pada menu IP > DHCP Server untuk mengkonfigurasi DHCP-Server



3. Kemudian klik pada menu DHCP-Setup



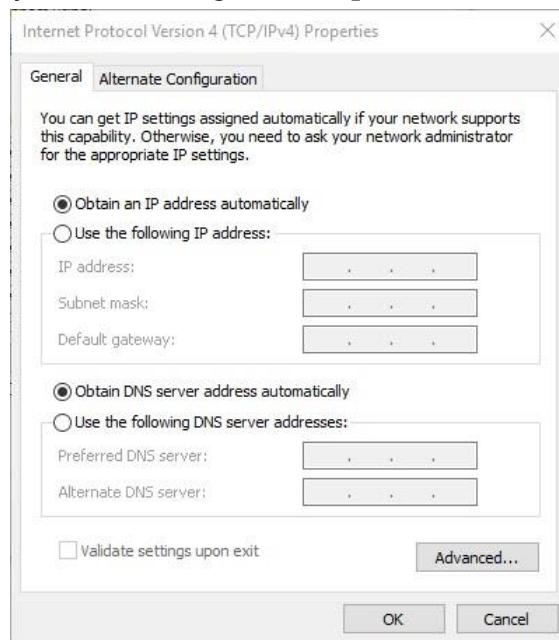
4. Kemudian ikuti arahan berikut



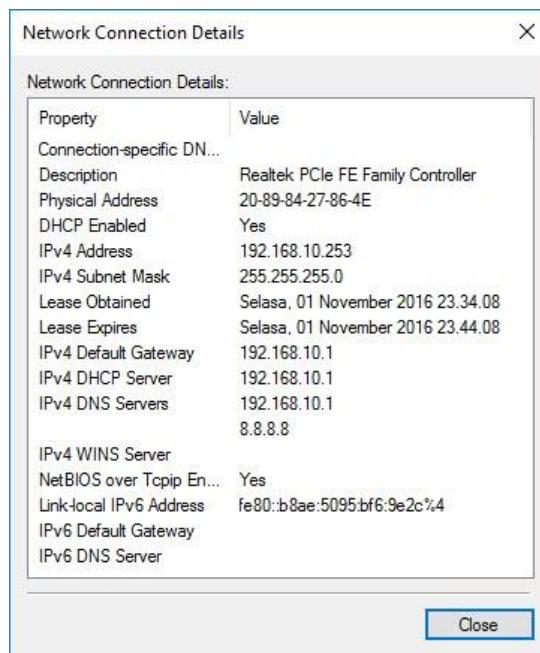
Keterangan:

- Pertama kita memilih interface mana yang ingin kita jadikan sebagai DHCP Server interface
- Kita memilih ip network yang akan digunakan untuk dhcp server
- Pemilihan gateway yang akan diberikan ke client
- Rentang ip address yang akan didistribusikan ke client
- DNS yang akan dipakai untuk client
- Lease time adalah waktu lamanya IP address yang diberikan ke client. Jika batas waktu lease time habis maka client akan mendapatkan IP DHCP yang baru dari DHCP Server

5. Untuk pengujinya, atur konfigurasi IP pada client menjadi Obtain (automatic)



6. Check pada interface ethernet laptop apakah sudah mendapatkan ip dari dhcp-server yang ada di router atau belum, kalau sudah tadiadnya seperti berikut



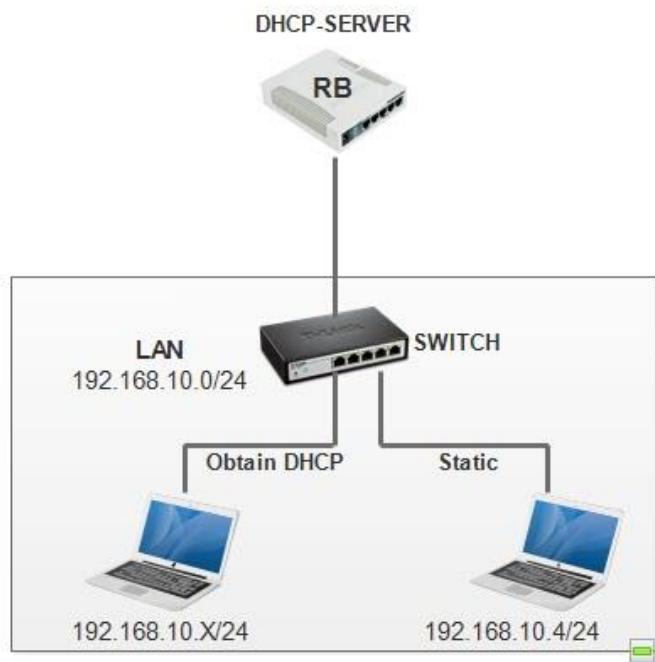
7. Untuk melihat daftar ip / client mana saja yang sudah menggunakan ip address bisa pada menu IP > DHCP Server > Leases

DHCP Server								
DHCP		Networks		Leases		Options		Alerts
<input type="button" value="New"/>		<input type="button" value="Edit"/>		<input type="button" value="Delete"/>		<input type="button" value="Check Status"/>		<input type="button" value="Find"/>
Address	/	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Host Name	Expires After
D					192.168.10.253	20-89-84-27-86-4E	DESKTOP-K3HMVE5	00:05:35 bound

Lab 26. Konfigurasi DHCP-IP Static

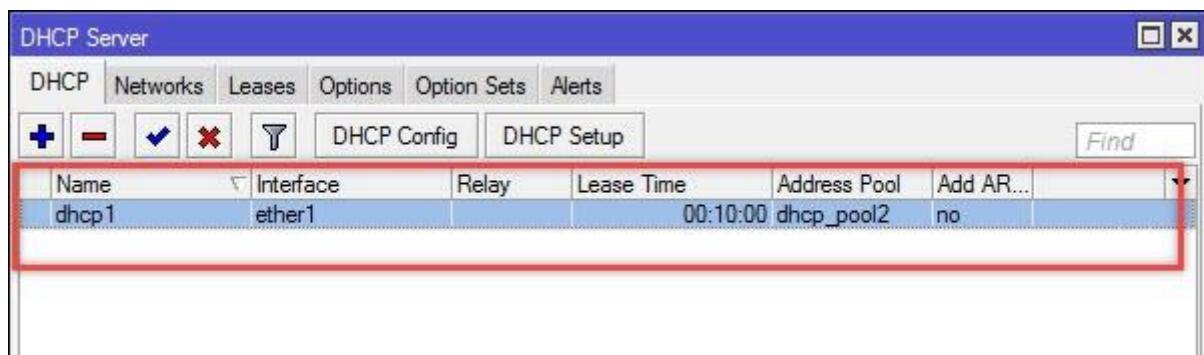
Pada lab sebelumnya kita telah membahas tentang DHCP-Server, pada pembahasan kali ini kita akan membahas tentang pengelolalaan DHCP-Server menggunakan mac static. Salah satunya dengan membuat client tidak dapat mengubah IP menjadi statik

Kenapa harus kita set agar client tidak bisa mengubah ipnya menjadi ip statik? Alsannya karena keamaanan pada DHCP-Server, jadi ini akan mempermudah kita dalam monitoring ke client. Untuk membuat client tidak bisa memakai IP secara statik kita akan juga akan menggunakan fitur ARP. Sebelumnya apa itu ARP? ARP (address resolution protocol) adalah sebagai pemetaan antara ip address dan mac-address yang dimiliki oleh suatu device. Perhatikan topologi berikut:

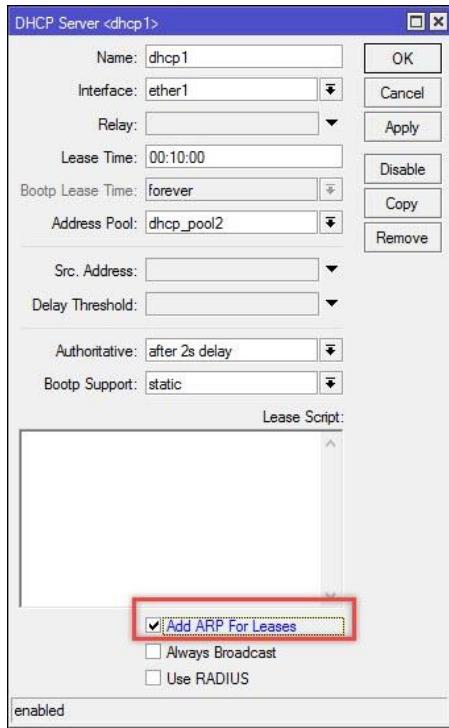


Untuk konfigurasinya sebagai berikut:

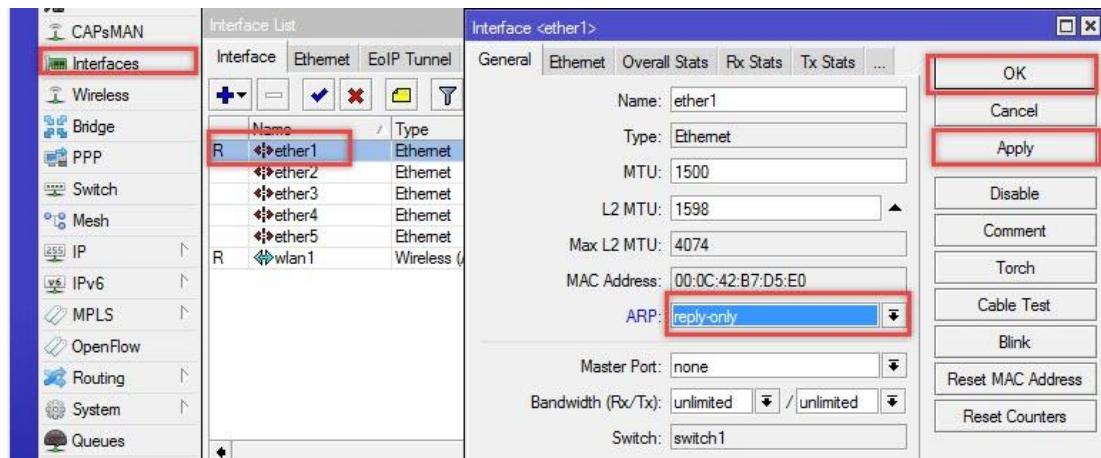
1. Pastikan sebelumnya sudah mengkonfigurasi DHCP-Server pada router board,



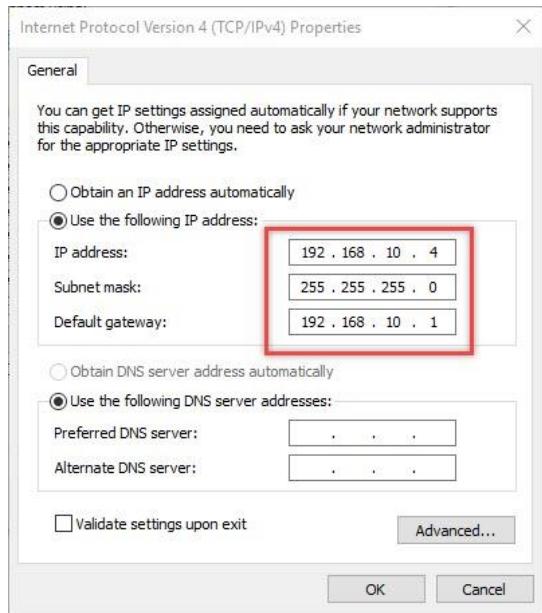
2. Double klik pada dhcp server tersebut, lalu centang (✓) pada Add ARP for leases



3. Kemudian kita masuk pada menu Interface, untuk membuat ARP mrnjadi mode read only, Masuk Interface > PilihInterface yang digunakan untuk DHCP- Server >ARP=Read Only



4. Untuk pengujinya, coba ganti ip address yang ada pada laptop/pc menjadi 192.168.10.4,



5. Coba akses ping ke ip yang ada pada interface router yang terhubung ke pc/laptop, hasilnya pc/laptop tidak bisa ping ke ip yang ada pada router

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

C:\Users\Fariz>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.35: Destination host unreachable.
Reply from 192.168.10.35: Destination host unreachable.
Request timed out.
Reply from 192.168.10.35: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
C:\Users\Fariz>
```

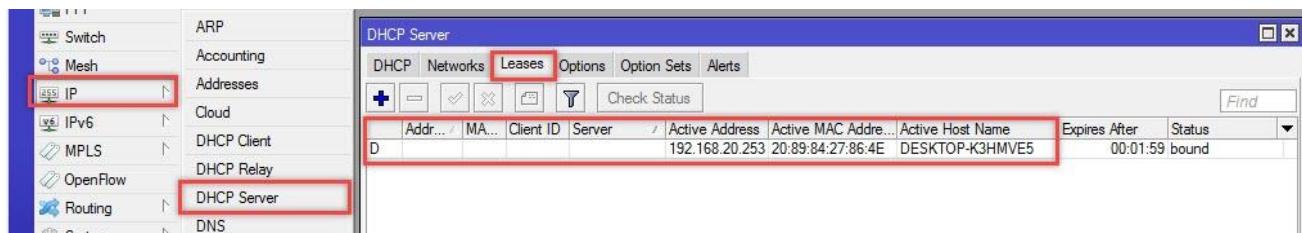
Lab 27. Konfigurasi DHCP-Mac Static

Melanjutkan pembahasan tentang pengelolaan DHCP-Server, pada pembahasan ini kita akan membuat ip dhcp yang dimiliki oleh salah satu client kita akan jadikan menjadi static, lok kok dibuat static? Pada dhcp-server ada yang namanya leases time, yaitu batas waktu habis menggunakan ip yang diberikan ke client, setalah leases time itu habis maka ip yang diberikan ke client sebelumnya akan diberikan lagi ke client yang berbeda.

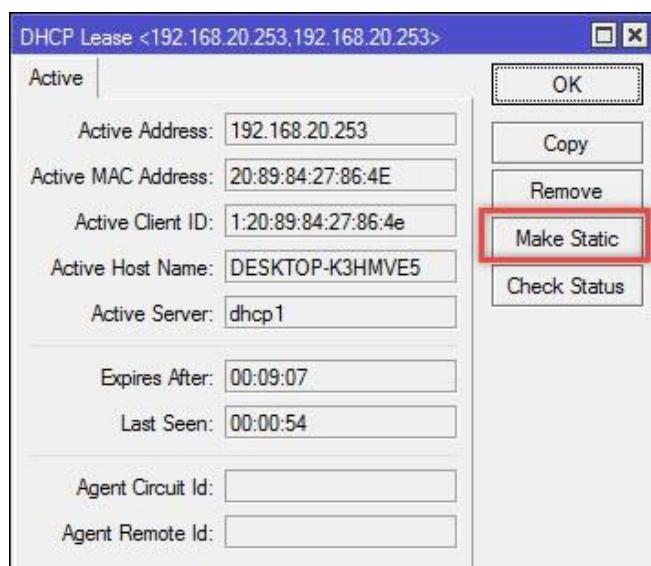
Pada pengelolaan dhcp kali ini kita akan mengkonfigurasi bagaimana salah satu client tersebut bisa menggunakan ip address yang sama terus menerus tanpa adanya bergantian ip dhcp

Untuk konfigurasinya sebagai berikut:

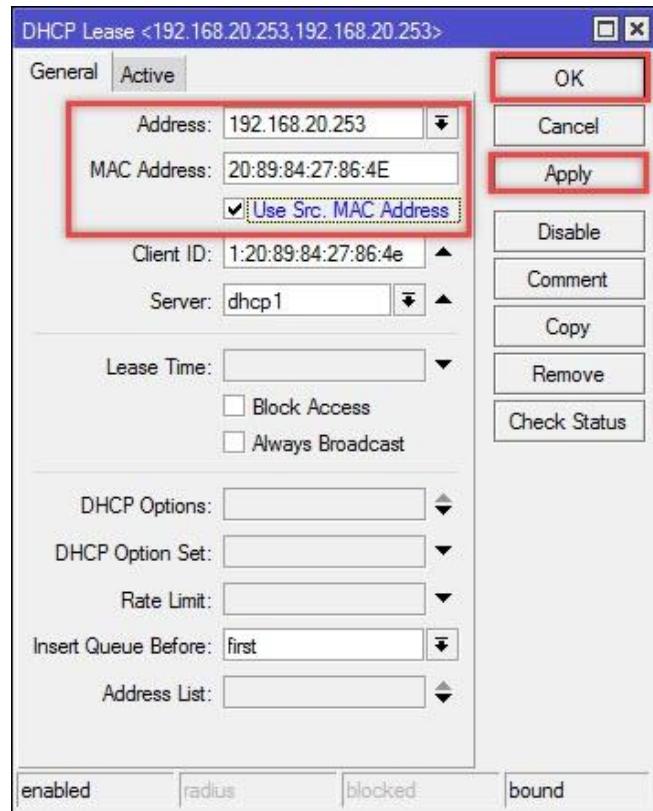
1. Masuk pada menu DHCP Server, IP > DHCP Server > Leases



2. Double klik pada salah satu hasil leases yang ada, lalu klik **Make Static**



3. Setelah itu buka kembali hasil leases tadi, akan muncul tab tambahan yaitu **General**, klik pada tab **General** lalu masukkan IP untuk client tersebut, setelah itu klik centang (✓) pada **Use Src Mac Address**, klik apply dan ok



4. Hasil konfigurasi mac-static tdi sebagai berikut

DHCP Server								
DHCP		Networks		Leases		Options		Alerts
<input style="width: 20px; height: 20px; border: none;" type="button" value="+"/>		<input style="width: 20px; height: 20px; border: none;" type="button" value="X"/>		<input style="width: 20px; height: 20px; border: none;" type="button" value="X"/>		<input style="width: 20px; height: 20px; border: none;" type="button" value="F"/>		<input style="width: 50px; height: 20px; border: none;" type="button" value="Find"/>
Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Host Name	Expires After	
192.168.20.253	20:89:84:27:86:4E	1:20:89:84:27:86:4e	dhcp1	192.168.20.253	20:89:84:27:86:4E	DESKTOP-K3HMVE5	00:03:12	

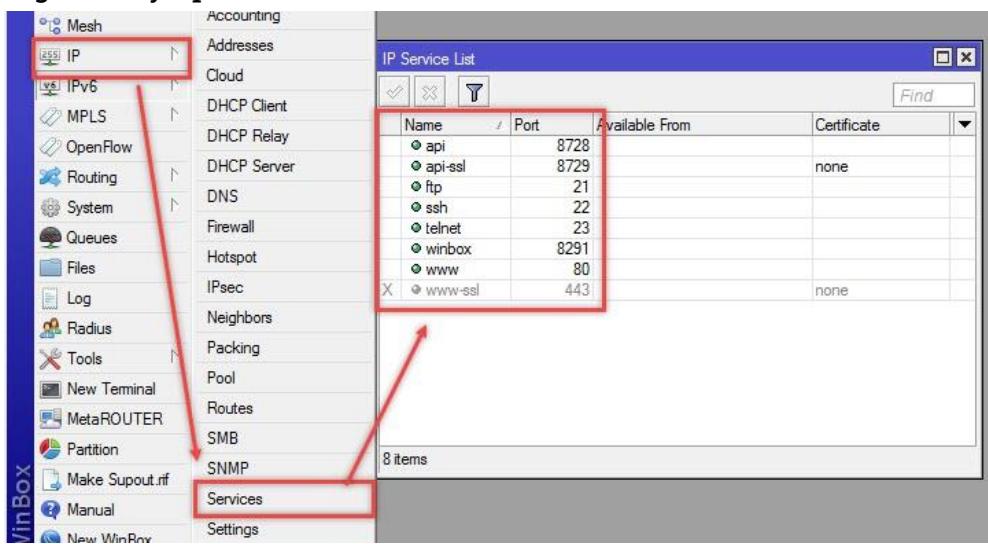
5. Jadi untuk konfigurasi diatas akan membuat client akan terus-menerus mendapatkan ip dhcp **192.168.20.253**
6. selesai

Lab 28. IP Service

Router Mikrotik menyediakan layanan service untuk memudahkan akses ke routerboard, secara default service ini akan berjalan terus menerus kecuali kita menonaktifkan service tersebut. Kita bisa mendisable service atau mengganti port port service demi keamanan routerboard kita.

Bayangkan jika servie service tersebut terbuka bebas pada jaringan publik? Pasti akan sering mengalami yang namanya percobaan untuk menghack routerboard kita. Maka kita bisa disable/ mengganti port service yang digunakan

Untuk konfigurasinya pada menu IP > Service



FIREWALL

Bab 3. Firewall

Pada Mikrotik fitur firewall adalah suatu fitur yang penting terlebih fungsi utama dari sebuah router adalah menghubungkan network yang berbeda, firewall dalam mikrotik berfungsi untuk melindungi router dari ancaman-serangan yang berasal dari luar (internet) maupun dari sisi client. Begitu juga untuk melindungi network dari network yang lain yang masih dalam satu router. Dalam mikrotik banyak sekali fitur-fitur yang tersedia dalam menu Firewall.

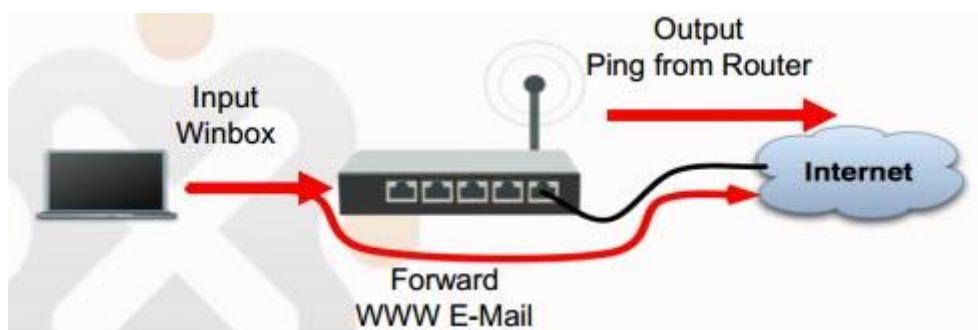
Untuk Firewall basic yang ada didalam mikrotik terdapat pada menu IP > Firewall > Filter Rule. Oke mari kita bahas sekilas mengenai Firewall Filter Rule

Setiap Firewall Filter rule diorganisir dalam chain (rantai) yang berurutan, pada chain terdapat 3 aturan chain (**input**, **forward**, dan **output**). Router akan membaca aturan chain dari atas ke bawah sesuai dengan chain mana dulu yang dibuat

Ketika paket diproses oleh router, paket akan dicocokkan dengan kriteria/syarat dalam suatu chain, ketika paket cocok dengan syarat chain maka paket akan melalui kriteria / prasarat chain berikutnya / dibawahnya.

Untuk aturan chain gambarannya sebagai berikut:

- INPUT – **ke** Router
- OUTPUT – **dari** Router
- FORWARD – **melewati** router



Konsep dari Firewall Filter Rule adalah **IF THEN**

- **IF** (jika) paket yang memenuhi syarat kriteria yang kita buat
- **Then** (maka) action apapun yang akan diproses pada packet tersebut

Protecting Routerboard with Filter Rule

Pada real praktik dilapangan pasti akan adanya serangan atau ancaman dari dalam maupun dari luar router, untuk menghindari hal hal yang tidak diinginkan dengan router kita, kita bisa menggunakan fitur Firewall Filter Rule di konfigurasi router kita. Kita akan memfilter paket apa saja yang boleh (accept) dan menolak/membuang (drop) paket yang tidak diperbolehkan masuk ke router

Ada 2 metode yang bisa digunakan yaitu:

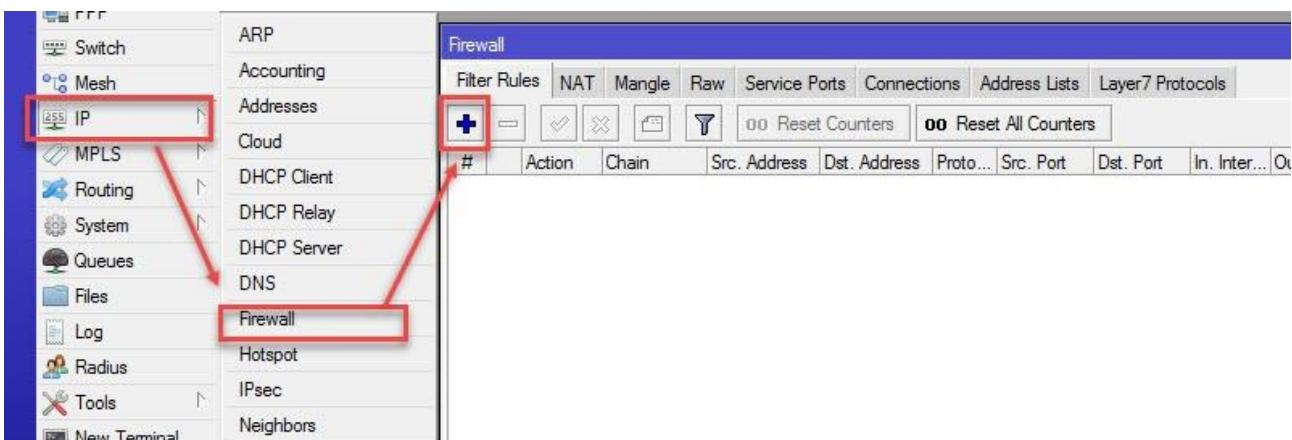
- Drop beberapa paket, dan menerima paket lainnya (*drop few, accept any*)
- Terima beberapa paket, dan membuang paket lainnya (*accept few, drop any*)

Untuk secara default pada rule pada firwall, semua traffic pakcet akan diaccepr oleh router.

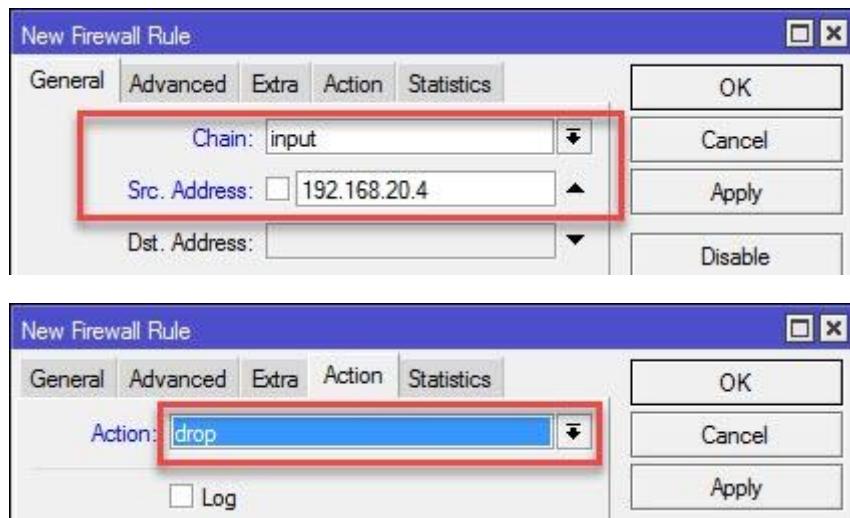
Lab 29. Membatasi akses IP ke routerboard dengan (drop few, accept any)

Pada lab ini kita akan menolak beberapa ip address agar tidak bisa akses ke routerboard dan mengijinkan semua ip address yang tidak blok bisa mengaskses routerboard

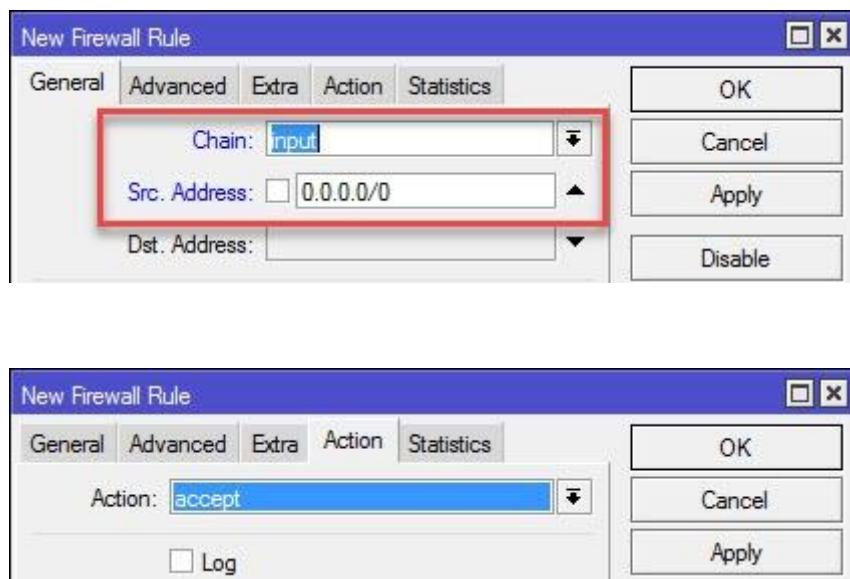
Untuk konfigurasinya terdapat pada menu IP > Firewall > Filter Rules



Klik tombol (+) dan konfigurasi parameter berikut: chainnya: Input ,kemudian yang drop adalah ip address **192.168.20.4**, untuk actionnya adalah **drop**



Lalu untuk rule acceptnya, tambahkan sebagai berikut:



Inilah hasil dari konfigurasi yang telah tadi kita buat, perlu diingat kembali routerboard membaca rule dari **atas ke bawah** jadi rule yang akan diproses dahulu adalah yang bereada diatas kemudian turun ke rule selanjutnya

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte
0	drop	input	192.168.20.4					
1	acc...	input	0.0.0.0/0					

Kemudian set ip laptop kita menjadi 192.168.20.4/24 dan test ping dari pc/laptop kita ke ip ethernet routerboard (192.168.20.1)

```

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

C:\Users\Fariz>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Fariz>

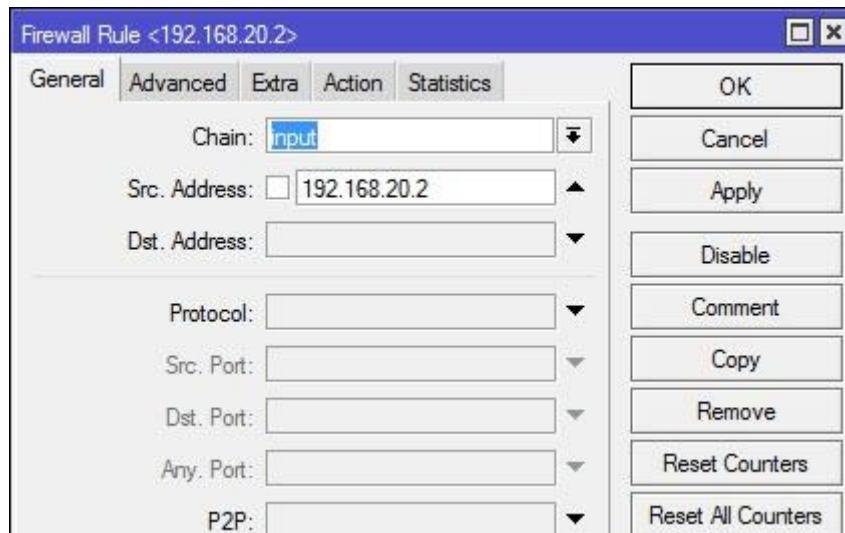
```

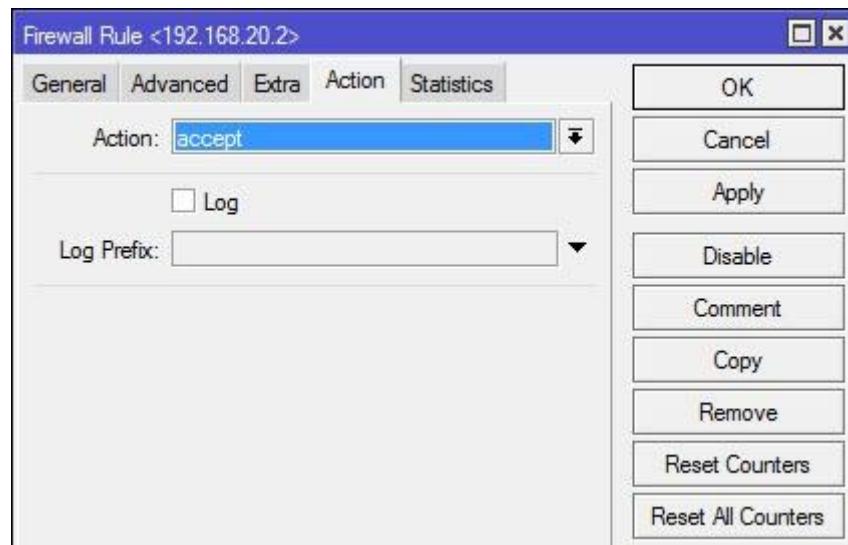
Lab 30. Membatasi akses IP ke routerboard dengan (accept few, drop any)

Kita akan melanjutkan mode lab selanjutnya yaitu (accept few, drop any), intinya kita akan mengijinkan hanya ip tertentu yang bisa digunakan untuk akses routerboard dan memblok semua ip selain yang diijinkan.

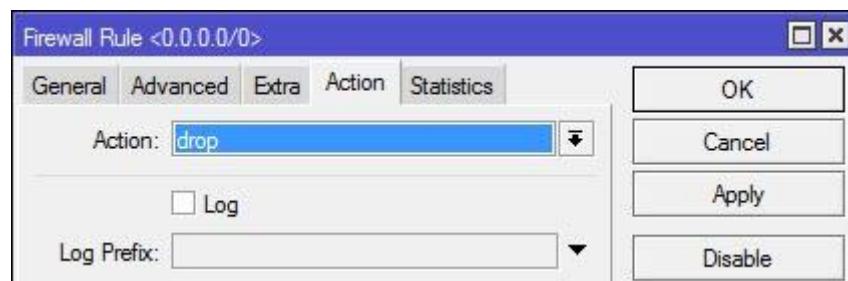
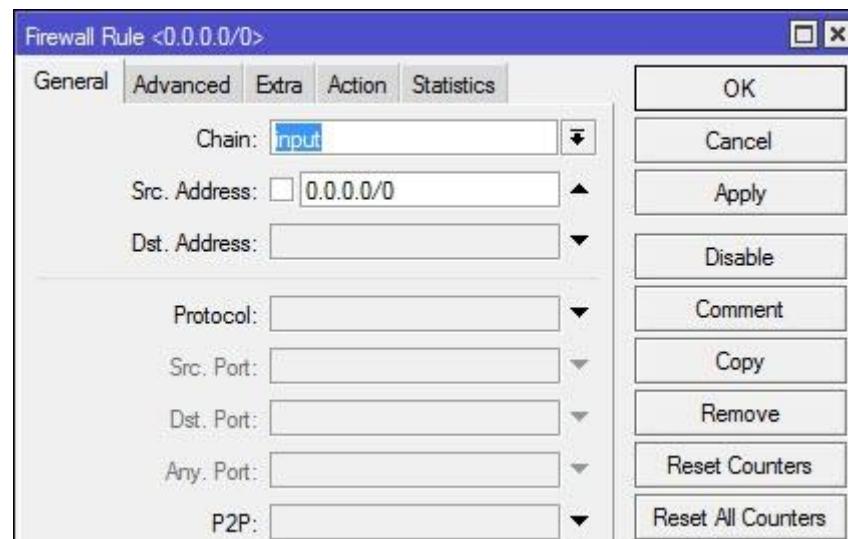
Sebelumnya hapus terlebih dahulu konfigurasi sebelumnya, Konfigurasinya sebagai berikut:

Buat rule accept. Untuk chainnya pilih **input**, dan src addressnya (ip yang diijinkan): **192.168.20.2**, untuk actionnya adalah **accept**





Kemudian buat rule untuk yang drop, untuk chainnya: **input**, src address: 0.0.0.0/0 (karena semua ip yang akan kita blok) dan untuk actionnya: **drop**

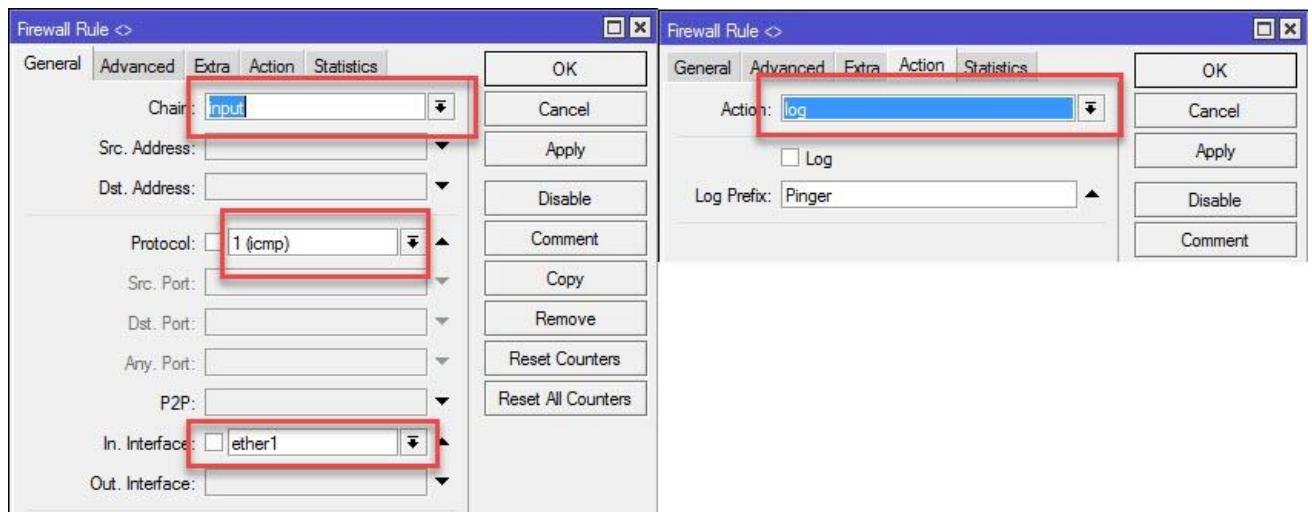


Pengujian, coba gunakan ip address dalam satu network dari (192.168.20.0/24) selain ip address 192.168.2.2 pada ethernet laptop/pc kita.

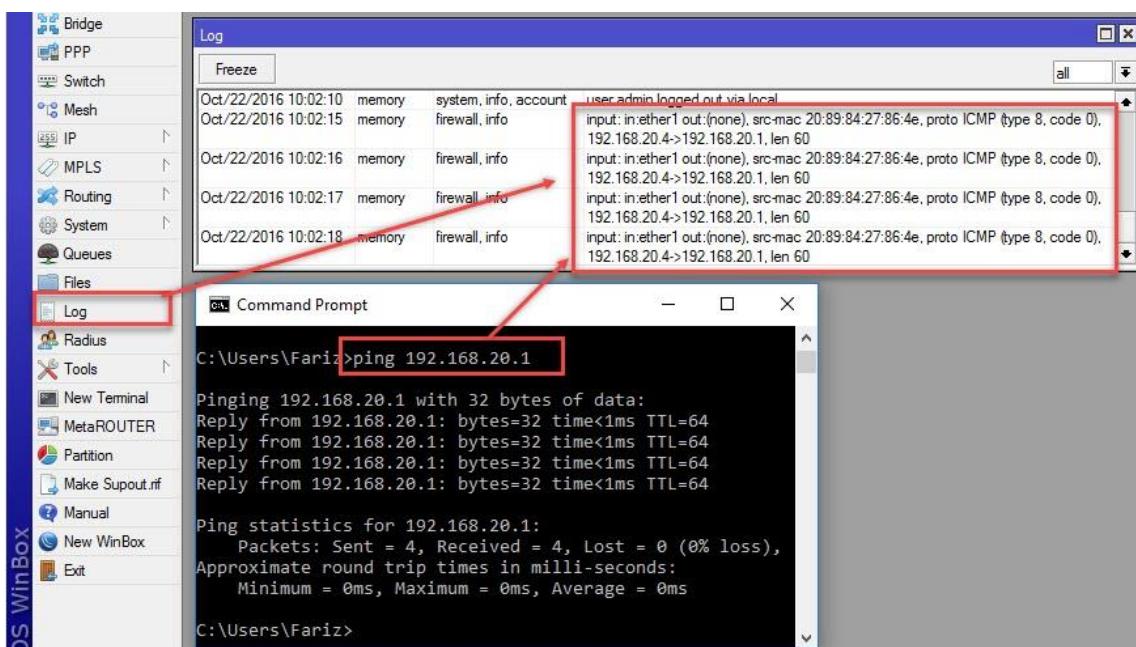
Lab 31. Firewall Logging

Firewall logging pada mikrotik berfungsi untuk mencatat kejadian (log) pada aktifitas di routerboard kita. Router akan mencatat segala aktifitas yang terjadi dan menampilkannya pada menu log. Fungsi ini memudahkan kita untuk melihat kejadian apa saja yang terjadi pada routerboard kita.

Kita akan membuat log dari interface routerboard kita yaitu pada **ether1**, konfigurasikan pada menu IP > Firewall > Filter Rules. Buat rule dengan parameter sebagai berikut: Chain: **input**, Protocol: **icmp**, In Interfaces: **ether1** dan actionnya: **log**



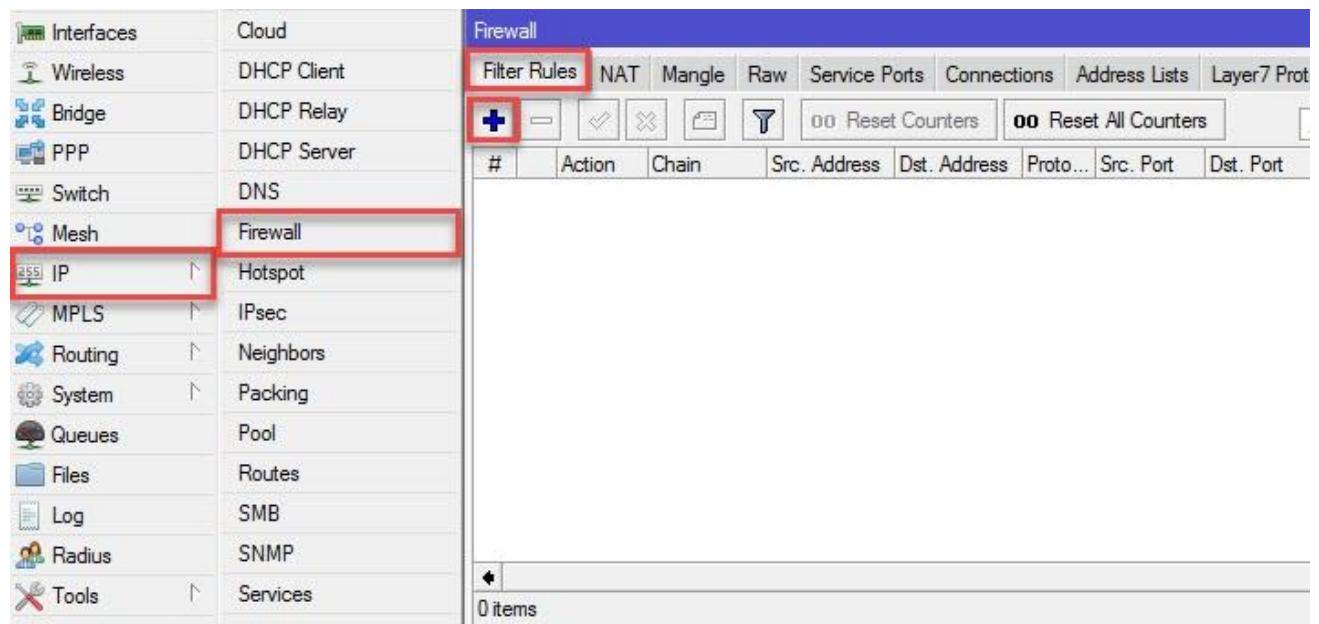
Untuk pengujinya kita coba ping dari laptop kita ke ip address yang ada apada eth1 pda router



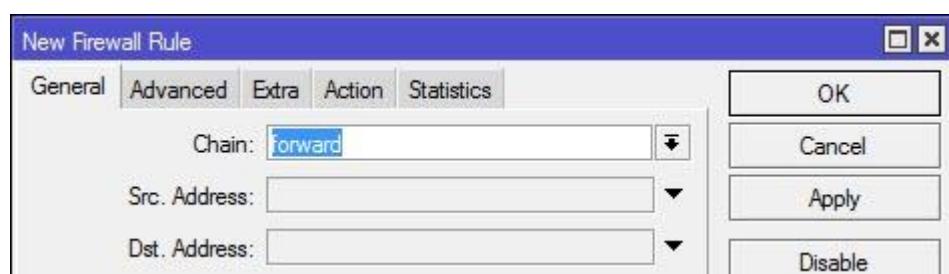
Lab 32. Blok website dengan (Konten) pada Mikrotik

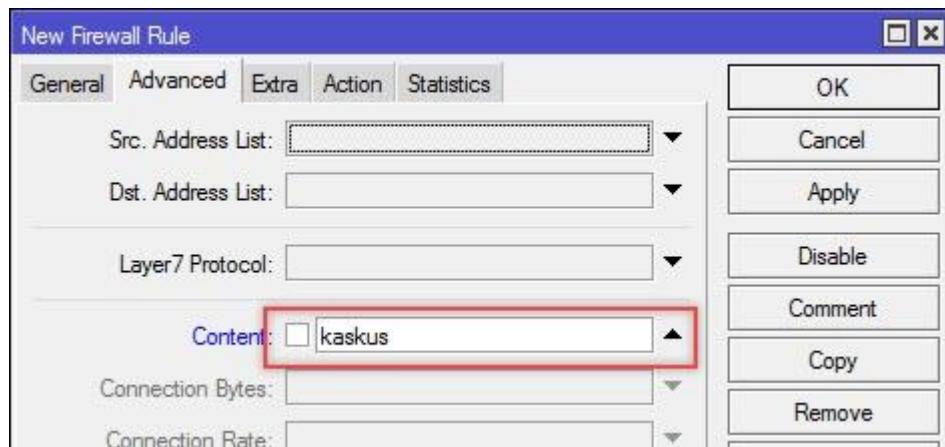
Mikrotik memiliki banyak fitur dalam urusan firewall. Contohnya adalah blocking. Pada pembahasan ini, kita akan membahas bagaimana caranya membuat blocking berdasarkan **Konten (kata)**. Bloking sendiri bertujuan untuk membatasi hak akses kepada client terhadap situs tertentu. Konfigurasi dapat dilakukan pada menu IP > Firewall > Filter Rules >

Untuk konten yang kita blok sebagai berikut: **kaskus, detik, bukalapak** dan parameter yang dikonfigurasi adalah chain: **forward**, Content: **kaskus** dan action: **drop**



Pada Sub menu General, konfigurasikan untuk Chain: **Forward**, pada tab advanced konfigurasikan content: **kaskus** dan untuk tab Action: **drop**



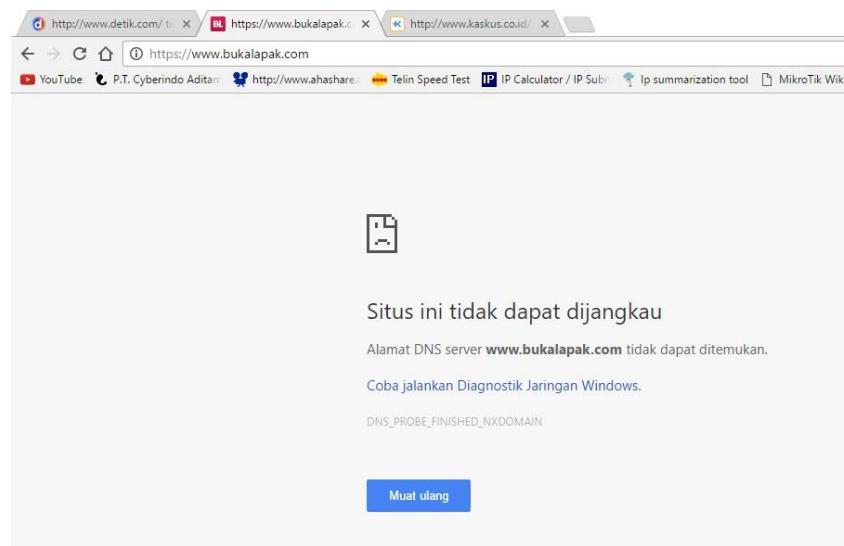
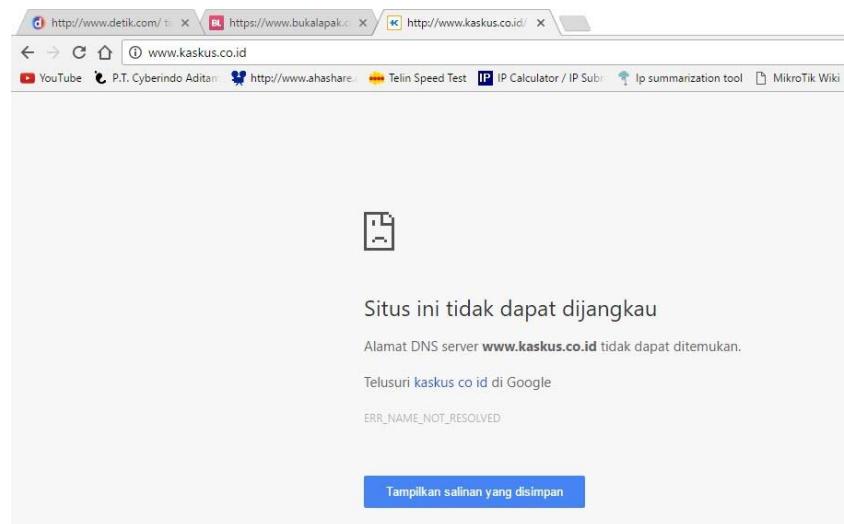
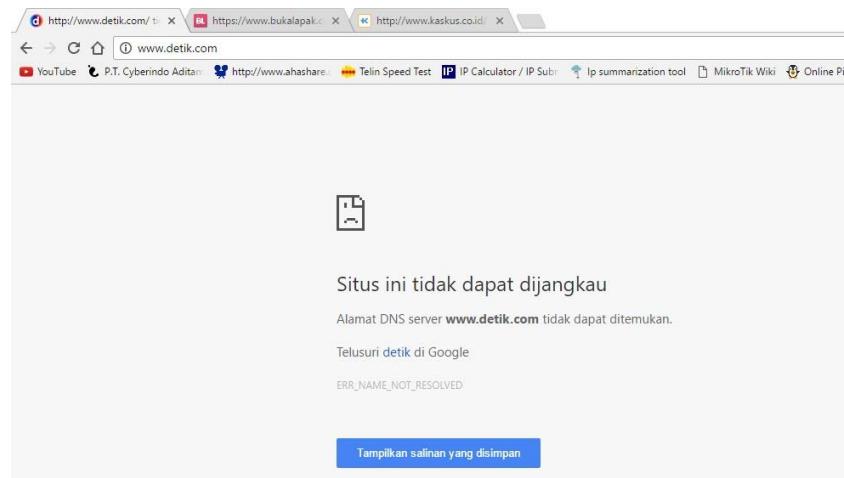


Untuk konten detik dan bukalapak buat rule yang sama untuk masing masing rule, sehingga pada filter rule terdapat 3 rule konten yang di blok/tolak

Firewall					
Filter Rules		NAT	Mangle	Raw	Service Ports
#					
0	✗ Action:	drop	Chain:	forward	
	Content:	kaskus	Log:	no	
	Bytes:	3410 B	Packets:	55	
	Rate:	0 bps	Packet Rate:	0	
1	✗ Action:	drop	Chain:	forward	
	Content:	detik	Log:	no	
	Bytes:	3335 B	Packets:	55	
	Rate:	234 bps	Packet Rate:	0	
2	✗ Action:	drop	Chain:	forward	
	Content:	bukalapak	Log:	no	
	Bytes:	5.5 KB	Packets:	90	
	Rate:	0 bps	Packet Rate:	0	

3 items

Untuk pengujinya, kita bisa akses konten tersebut satu per satu



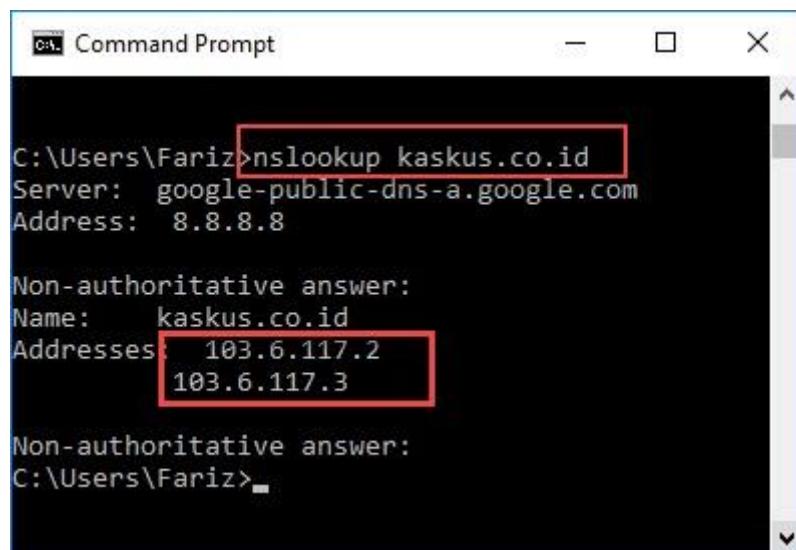
Lab 33. Blok website dengan Address List

Blokir website bisa juga dilakukan dengan metode address list, address list sendiri adalah metode untuk memfilter banyak IP yang dijadikan 1 group dengan 1 rule firewall. Satu line address-list bisa berupa subnet, range atau hanya 1 host Ip address.

Pada lab ini kita akan melakukan bloking menggunakan address list? Kenapa address list? Karena dalam suatu website terdapat lebih dari 1 IP server yang digunakan jadi kita akan memblokir semua ip server dari suatu website. Untuk mengetahui berapa ip server pada suatu website bisa kita menggunakan nslookup

Untuk menu **Address List** terdapat pada menu **IP > Firewall > Address List**

Kita akan memblokir situs **www.kaskus.co.id**, gunakan nslookup untuk mengetahui ip server dari website tersebut. Kita bisa menggunakan fitur CMD dengan mengetikkan **nslookup kaskus.co.id** , lalu enter (untuk lab ini kita harus terkoneksi dengan internet)

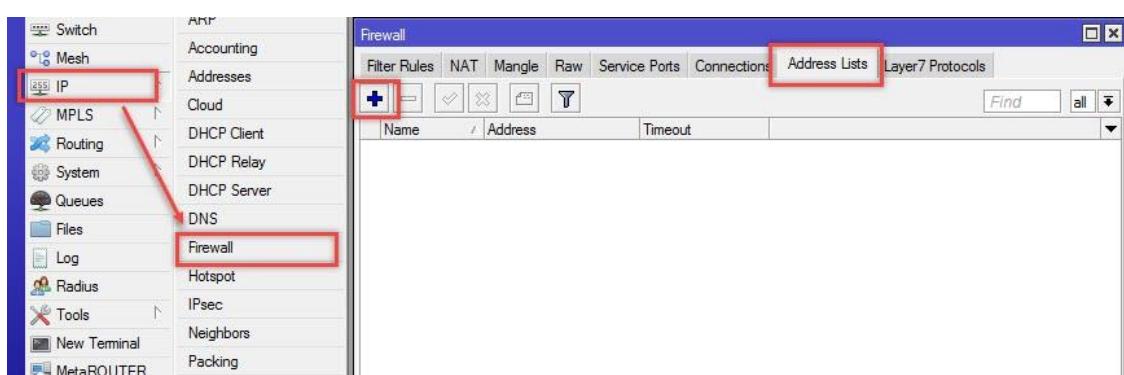


```
C:\Users\Fariz>nslookup kaskus.co.id
Server:  google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name:   kaskus.co.id
Addresses:  103.6.117.2
          103.6.117.3

Non-authoritative answer:
C:\Users\Fariz>
```

Tanda kotak merah ditas dalam gambar nslookup, menunjukkan ada 2 ip address dari website tokopedia.com, tinggal nanti kita masukkan saja pada address list. Kemudian masukkan kedua ip tersebut pada address list. Dengan cara masuk pada menu **IP > Firewall > Address List**

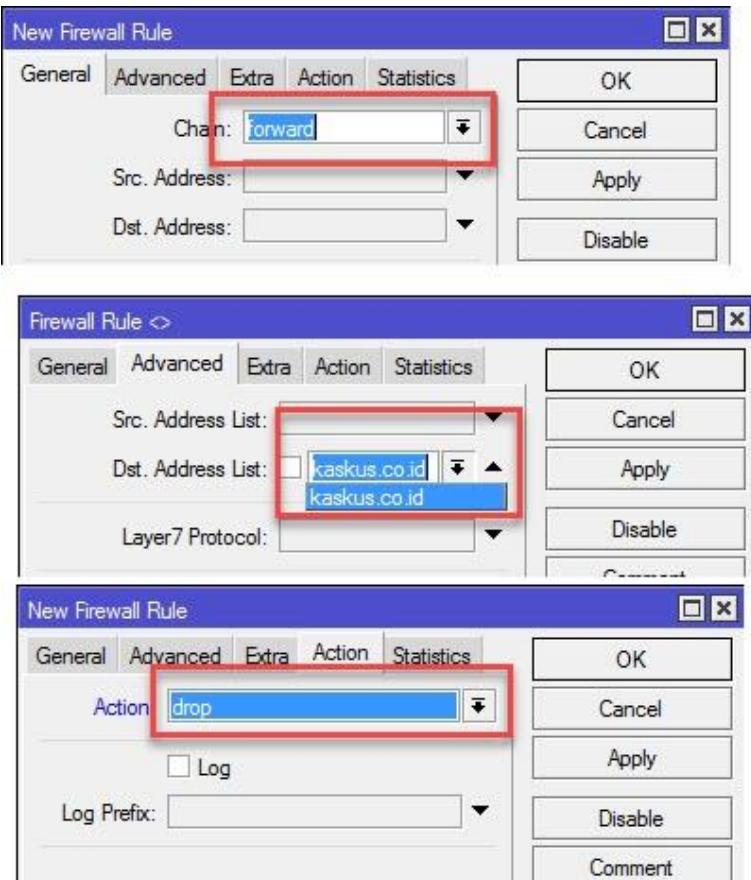


Masukkan name dengan diisi dengan nama situsnya, dan masukkan IP server dari situs tersebut. Karena tokopedia.com memiliki 2 IP serve maka kita harus menambahkan 2 rule pada address list.

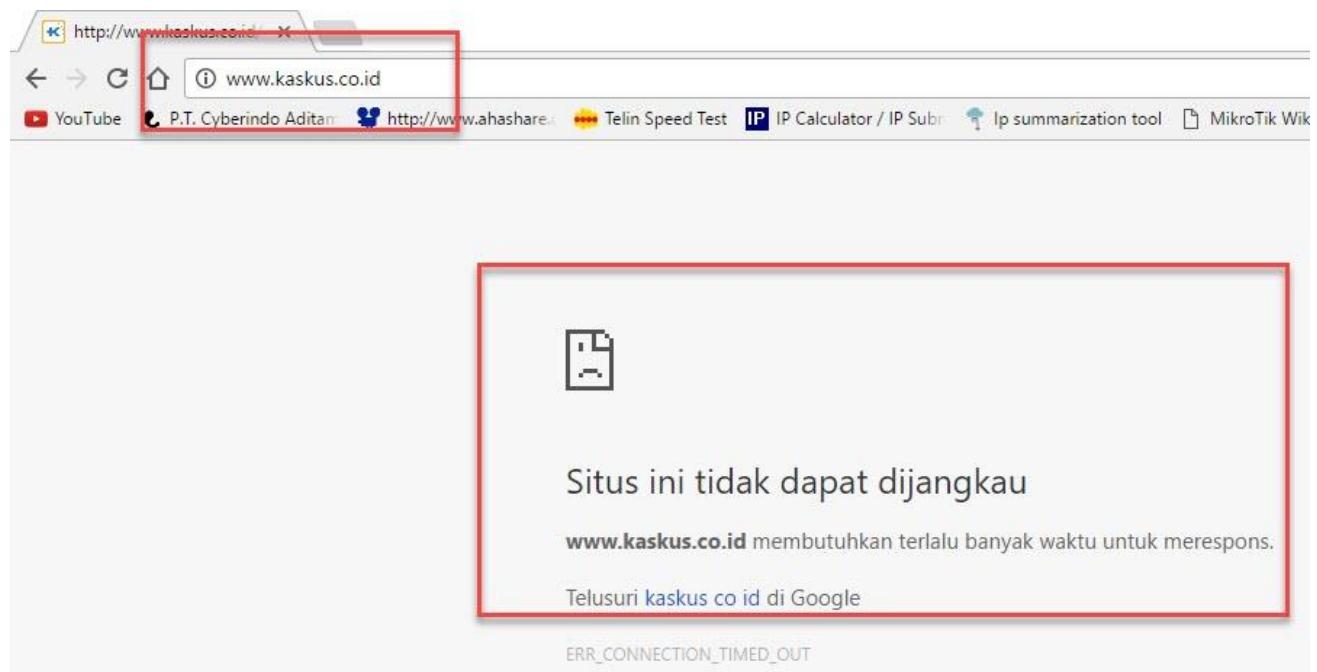


Setelah selesai membuat rule pada address list, kita konfigurasikan ke **filter rule**, pada menu IP > Firewall > Filter Rules

Untuk parameter yang dikonfigurasi yaitu Chain= **Forward** kemudian ke tab advanced pilih Dst.Address= **kaskus.co.id** kemudian pada tab action pilih action= **drop**



Kemudian ujicoba test dengan mengakses website tokopedia.com pada browser di pc/laptop kita



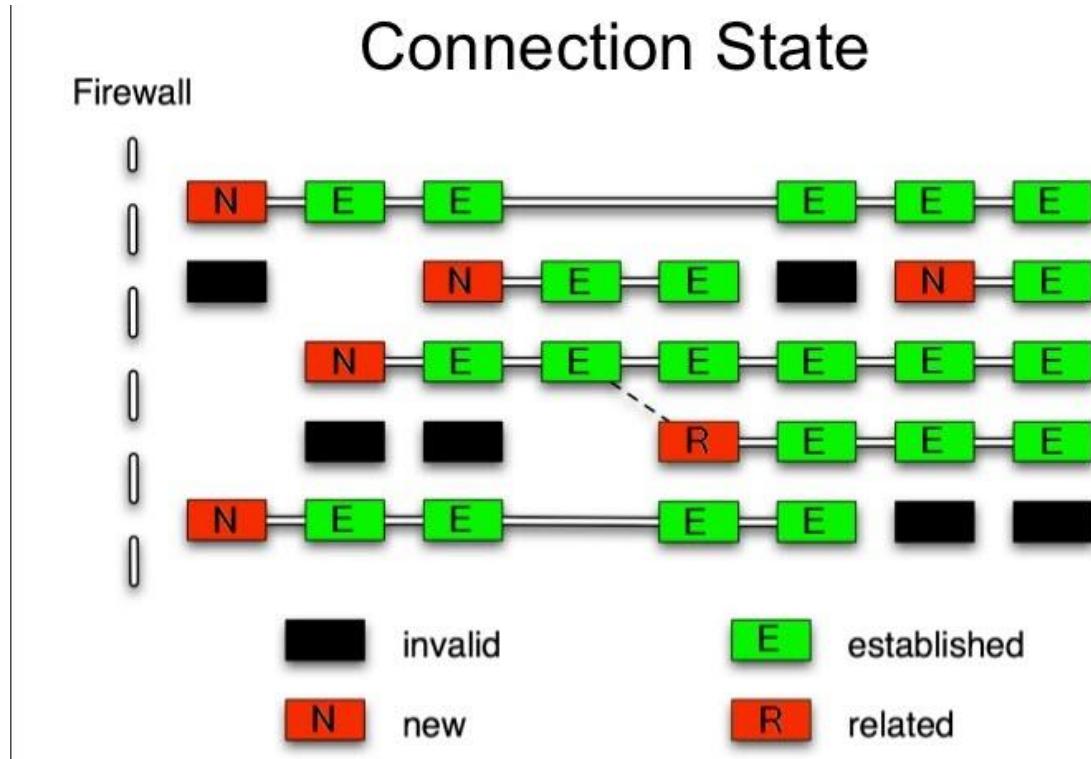
Lab 34. Connection Tracking & Connection State

Pada Firewall terdapat fitur yang bernama **Connection Tracking**, fitur tersebut berfungsi untuk melihat aktifitas koneksi pada jaringan yang sedang digunakan, Informasi yang kita dapat pada connection tracking berupa source & destination IP dan port yang digunakan, status koneksi, type protocol dan banyak hal lainnya.

Setiap paket data pasti mempunyai status koneksi (connection state) yang dapat kita lihat informasi pada connection tracking. Untuk status koneksinya akan saya jelaskan sebagai berikut:

- **Established** = paket yang termasuk bagian dari koneksi yang sudah ada atau sudah dikenali
- **New** = paket memulai sebuah koneksi baru, atau tergolong menjadi koneksi paket yang belum sempurna dalam pengiriman paket di dua arah, antara client & server, jadi masih setengah dalam pengirimannya. hanya client yang mengirim request paket
- **Related** = peket memuli sebuah koneksi baru, tetapi masih terkait dengan sebuah koneksi yang masih ada, seperti transfer data pada FTP atau pesan eror ICMP

- **Invalid** = paket tidak termasuk koneksi dari manapun yang sudah diketahui dan pada saat yang sama, paket tidak membuat sebuah koneksi baru



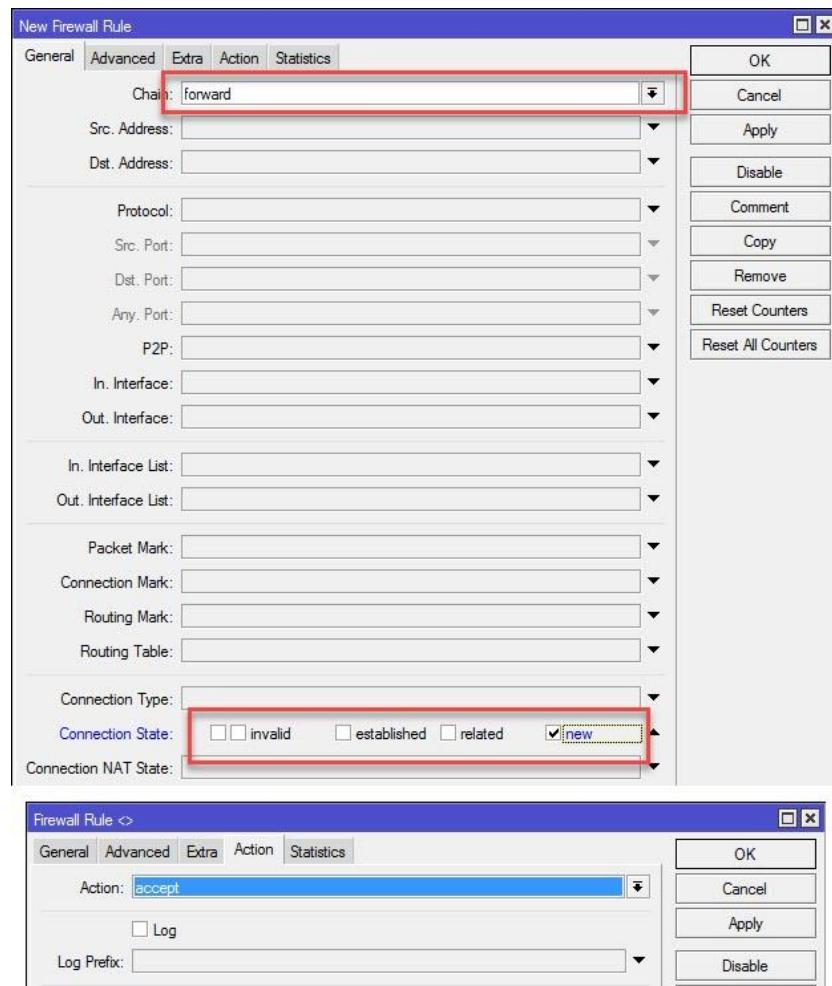
- Implementasi Connection Tracking

Pada lab ini kita akan membuat rule untuk status koneksi, masing masing 1 rule. Rule ini akan berfungsi untuk menghemat resource dari routerboard, karena proses filtering selanjutnya akan dilakukan ketika ada sebuah koneksi dimulai (connection = new).

Untuk rulennya dapat dikonfigurasi pada **IP > Firewall > Filter Rule**, untuk masing masing rule chain yang dipakai adalah **forward**, dan connection statenya sebagai berikut:

- Connection state Invalid > action= **drop**
- Connection state established > action= **Accept**
- Connection state related > action= **Accept**
- Connection state new > action= **Pass-through**

1. Buat masing-masing 1 rule per connection state yang digunakan



2. Sehingga nanti akan terbentuk koneksi rule sebagai berikut:

#	Action	Chain	Connection State	Bytes	Packets
3	✓ accept	forward	established	7.7 MiB	9 856
1	✓ accept	forward	related	160 B	2
2	✗ drop	forward	invalid	280 B	7
0	passthrough	forward	new	41.2 kB	361

Lab 35. Konfigurasi NAT

NAT (Network Address Translation), suatu metode untuk menghubungkan banyak komputer (lokal) ke jaringan internet dengan menggunakan satu atau lebih alamat ip public. NAT digunakan karena keterbatasan akses internet kita

menggunakan IP Public. NAT juga digunakan untuk keamanan dan kemudahan administrasi jaringan yang kita bangun.

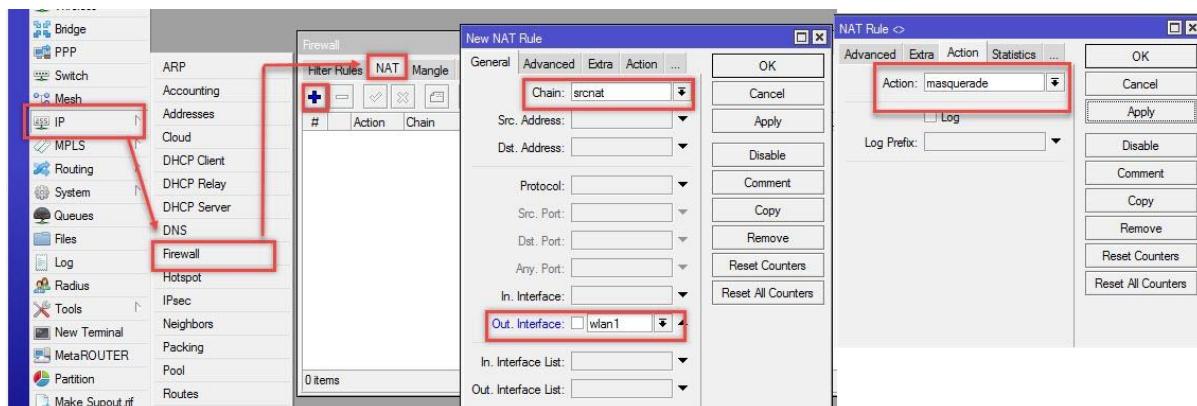
Pada Firewall mikrotik, NAT dibedakan menjadi 2 chain yaitu:

1. Srcnat, untuk action yang bisa digunakan yaitu:
 - Masquerade : menghubungkan subnet LAN ke 1 dynamic ip internet
 - Src-nat: menterjemahkan subnet LAN ke 1 static ip internet
2. Dstnat (port forwarding), untuk action yang bisa digunakan yaitu:
 - Dst-nat : memperbolehkan traffic ke luar router
 - Redirect: membelokkan traffik ke router itu sendiri

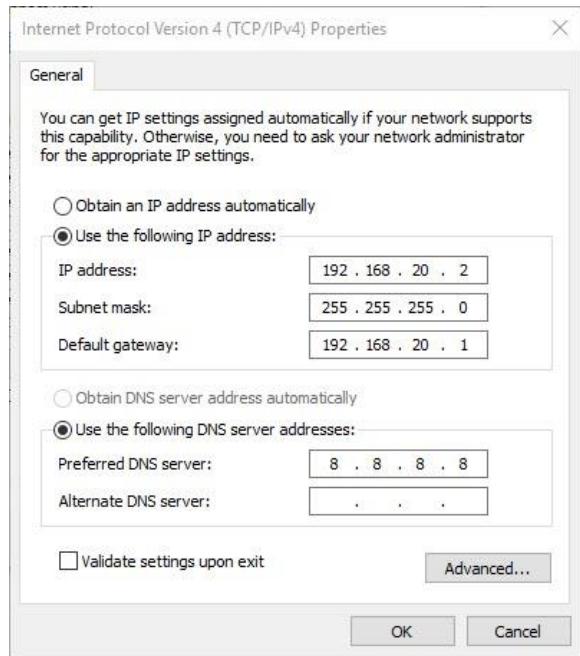
Pada kab ini kita akan menghubungkan ip private kita ke internet, dengan menggunakan NAT (**srcnat**) pada mikrotik. Untuk sumber internetnya kita menggunakan akses via wifi (**wlan1**) di mikrotik (station). Untuk perintah CLI nya sebagai berikut:

```
[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=wlan1  
| action=masquerade  
|  
|  
| datang dari source (sumber) dan ingin keluar melalui interface wlan1, maka paket  
akan diterjemahkan oleh masquerade
```

Untuk konfigurasinya dapat dilakukan pada menu **IP > Firewall > NAT**, sebagai berikut;



Konfigurasikan Ip address beserta dns pada interface ethernet laptop/ pc agar bisa terhubung ke internet



Lakukan test ping internet dengan mengakses menggunakan ping ke google.com atau akses website tertentu misal akses website idn.id



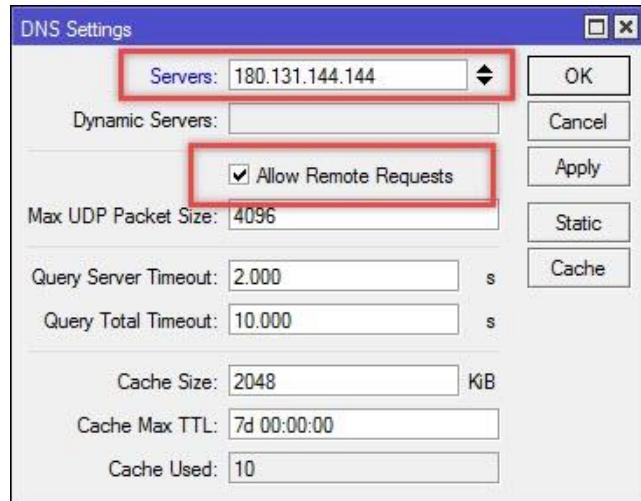
Lab 36. Blok Situs dengan DNS Nawala

Internet adalah dunia yang tanpa batas, banyak hal yang bisa temukan di internet. Kita bisa mencari soal materi pelajaran, berita, kejadian terkini, bahkan informasi yang sangat jauh dari lokasi kita tinggal. Namun internet juga memiliki situs-situs atau website yang tidak seharusnya kita buka, apalagi buat anak-anak. Misalnya pornografi, kekerasan dll. Maka dari itu harus dilakukan filter terhadap website mana saja yang tidak kita perbolehkan untuk diakses.

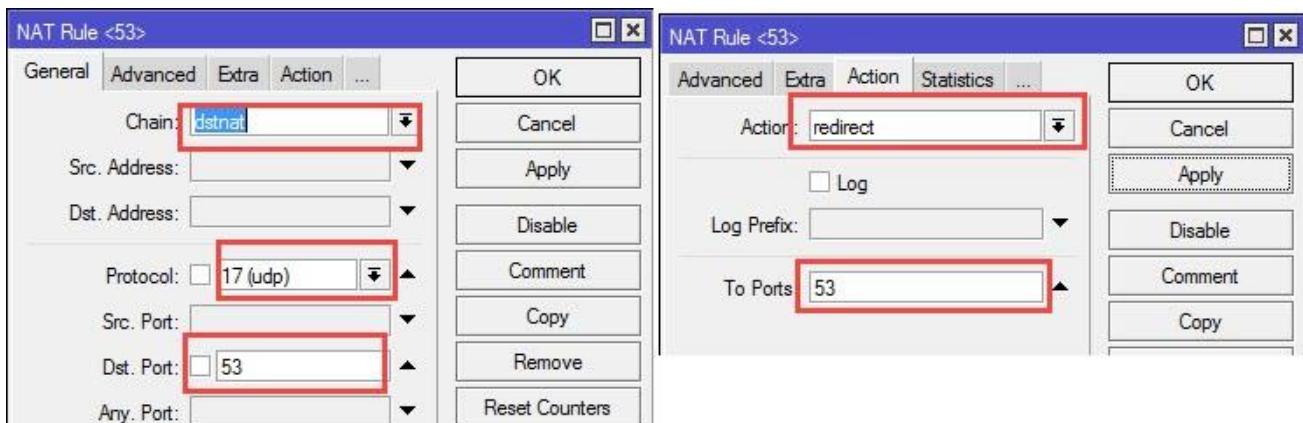
Tujuan dari dilakukannya transparent dns dengan NAWALA, supaya internet yang kita akses bersih dan aman dari situs-situs seperti pornografi dan perjudian.

Metode ini dikonfigurasikan pada menu Firewall dan juga pada DNS.

- Masuk pada menu DNS, untuk menambahkan IP DNS Nawala (**180.131.144.144**) pada router os, IP > DNS

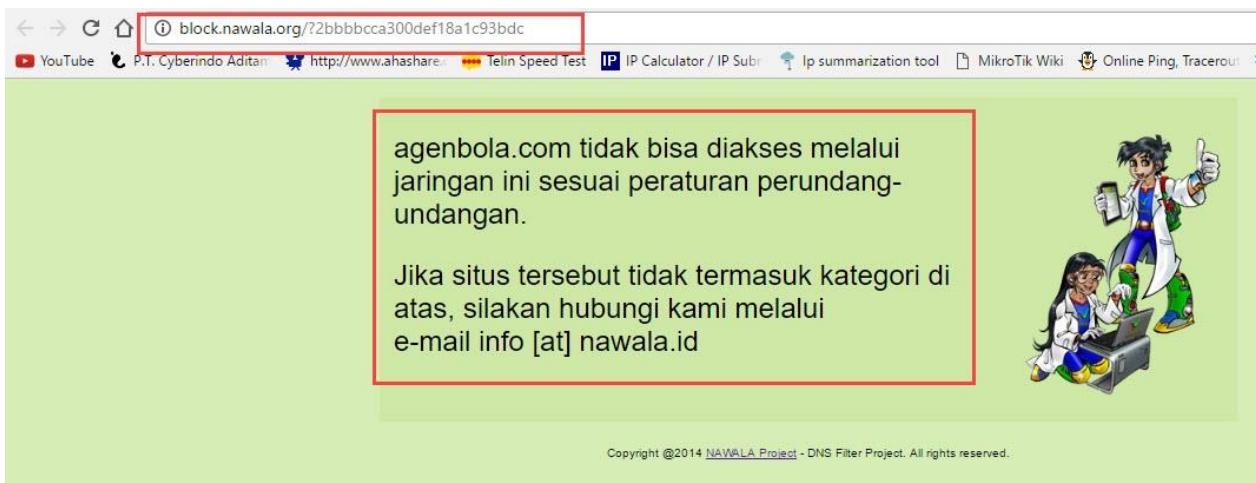


- Masuk pada menu IP > Firewall > NAT, tambahkan rule dstnat dengan parameter yang dikonfigurasi yaitu Tab General, chain=**dstnat**, protocol=**udp** dan **Dst.port=53**,



Kemudian pada tab action, isi action=**redirect**, to port=**53**, klik **apply** dan **ok**

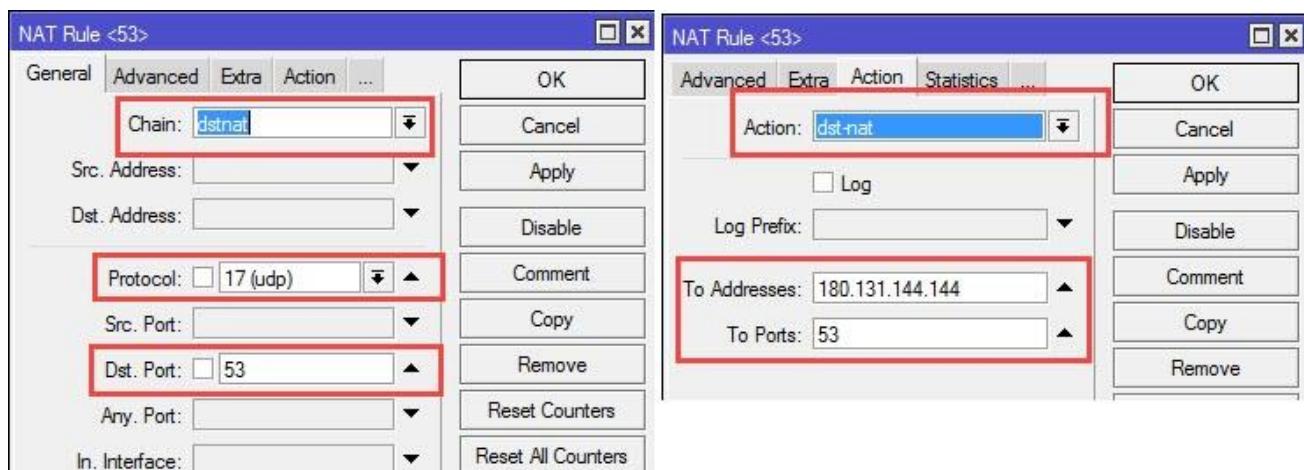
Lalu uji coba test dengan mengakses browser dan coba akses website



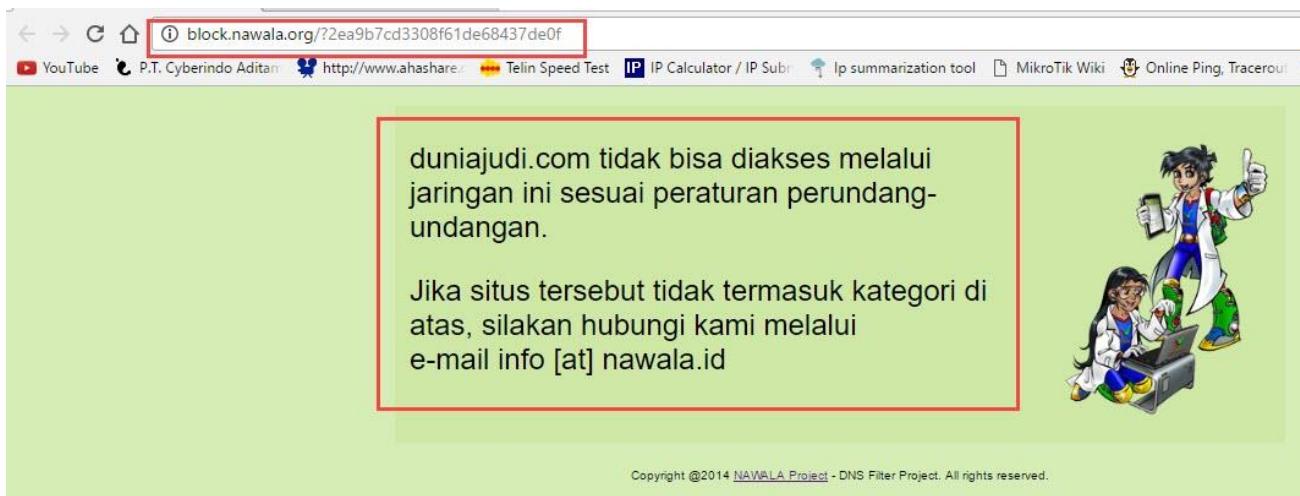
Lab 37. Blok Situs dengan Transparent DNS Nawala

Pada lab ini kita akan mengkonfigurasi Transparent DNS Nawala, kenapa kok transparat ? jadi kita tidak perlu set dns manual secara manual dnsnya pada client, cukup diset pada routerboard nantinya jika ada traffic situs yang diblokir nanti akan langsung diredirect ke dnsnya milik nawala.

1. Konfigurasi Transparent DNS dapat dilakukan pada menu IP > Firewall > NAT, dengan parameter yang dikonfigurasi yaitu: chain: **dstnat** protocol: **udp**, dst port:53 untuk tab actionnya, action: **dst-nat** to addresses: **180.131.144.144** , to ports: 53



2. Kemudian uji coba dengan membuka browser dan mencoba mengakses situs togel (judi), contohnya www.duniajudi.com, check apakah bisa diakses? Atau malah muncul blocking page dari nawala?



Jika muncul page bloking dari nawala berarti website tersebut sudah terblokir oleh dns nawala.

WIRELESS



Bab 4. Wireless

Mikrotik dengan RouterOSnya sudah mendukung fitur wireless dengan standart **IEEE 802.11**. Secara lengkapnya standart wireless yang disupportnya sebagai berikut: **802.11a, 802.11b, 802.11g, 802.11n and 802.11ac**. Mikrotik juga menyertakan fitur tambahan pada Menu wirelessnya,

Untuk fitur tambahan pada wireless mikrotik yaitu WPA, WEP, AES encryption, Wireless Distribution System (WDS), Dynamic Frequency selection (DFS), Virtual Access Point, Nstreme and NV2 proprietary protocols dan banyak lagi feature fatur tambahan.

Wireless pada mikrotik dapat beroprasi pada beberapa mode yaitu: Access point, Client (station), wireless bridge dll.

Lab 38. Konfigurasi Wireless AP & Station



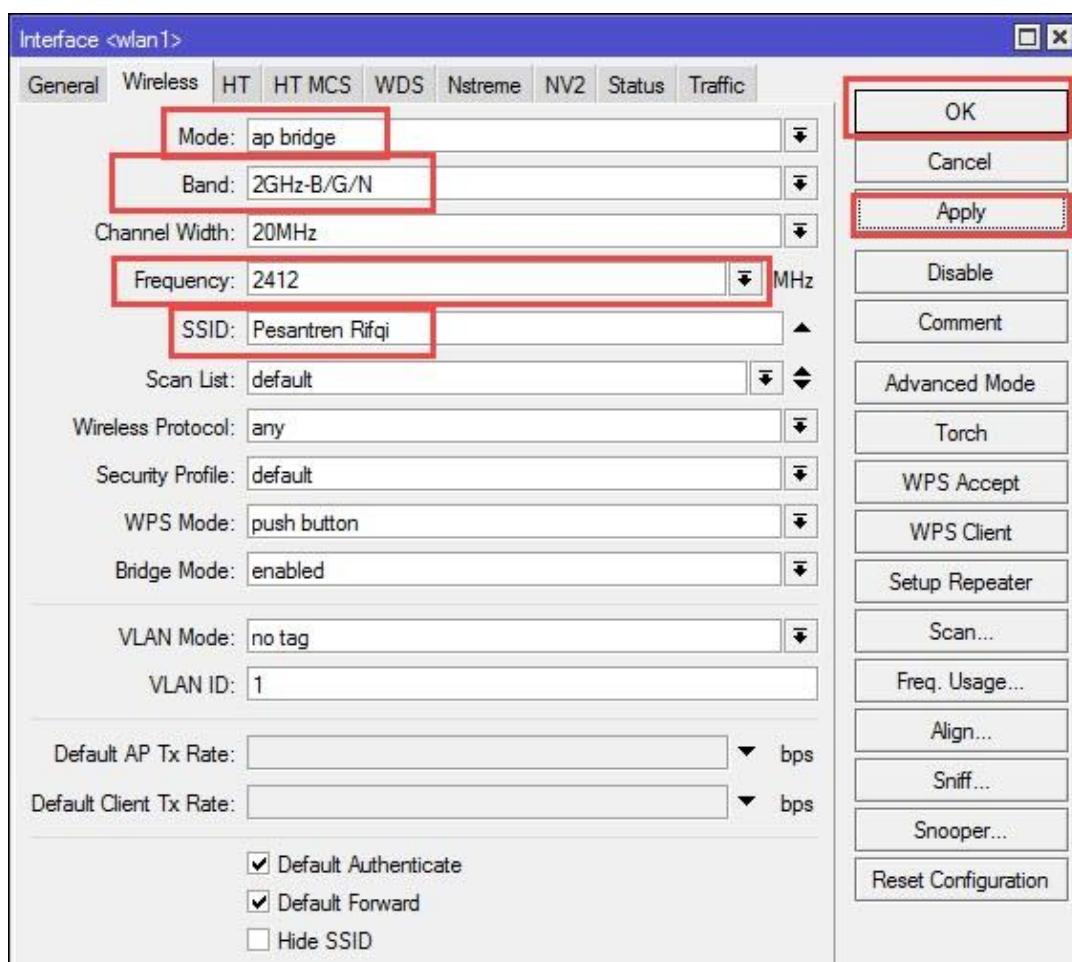
Pada lab ini kita akan mengelabkan bagaimana konfigurasi wireless mikrotik dengan 2 Routerboard yang memiliki fitur wireless. Perlu diperhatikan bahwa lab ini kita membutuhkan 2 routerboard yang memiliki fitur wireless. 1 Routerbord akan bertindak sebagai **Access point**, 1 routerboard lagi akan bertindak sebgai **client (station)** . Langsung saja kita praktekan bersama-sama

1. Ubah identity pada masing masing router, beri nama pada **router1=AP** dan pada **router2=station**, bisa dikonfigurasikan pada **System > Identity**
2. Konfigurasikan Parameter dibawah pada menu **Wireless > Interfaces**
 - A. Router AP
 1. Jika interface **wlan1** masih dalam kondisi off, aktifkan dengan mengenable terlebih dahulu



2. Kemudian Konfigurasikan Parameter sebagai berikut

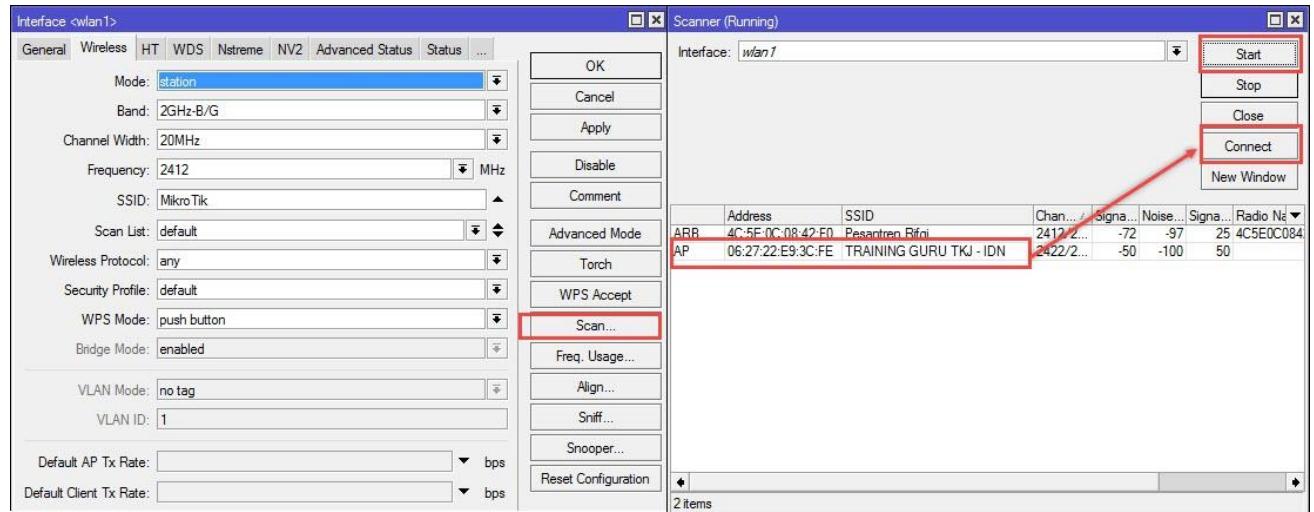
- Mode= ap bridge
- Band= 2Ghz-B/G/N
- Frequency= 2412
- SSID= Pesantren Rifqi (nama ssid bebas, bisa diatur sesuka kita)
- Jangan lupa klik apply dan ok



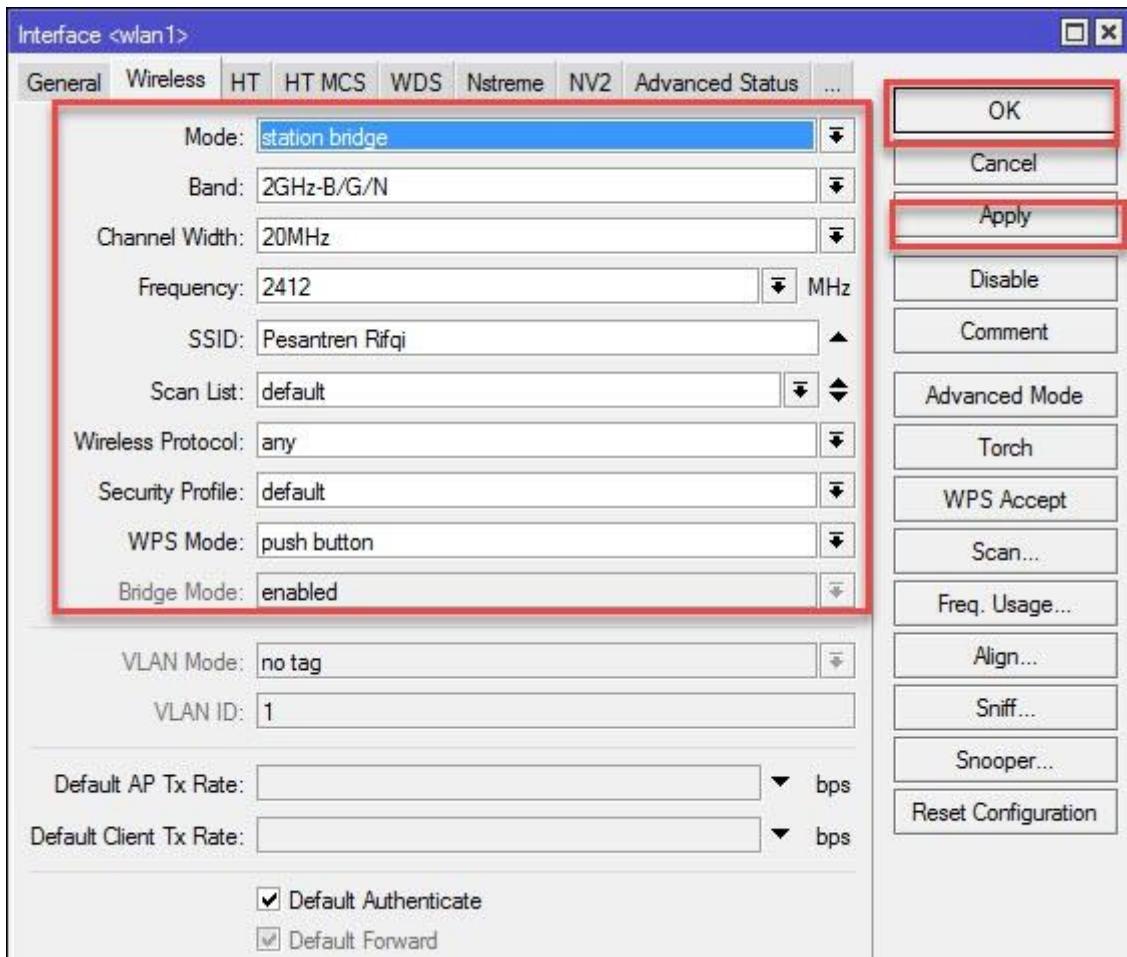
B. Station Mode

1. Konfiguraskan pada wireless client parameter sebagai berikut;
 - Lakukan scan wireless AP pada menu **scan**, klik tombol **start** dan

- Hubungkan dengan SSID yang ada pada router 1 yaitu: Pesantren rifqi



- Secara otomatis parameter yang ada pada client, parameternya akan sama dengan yang ada pada konfigurasi pada AP, perbedannya hanya modenya yang berubah menjadi **station bridge**.

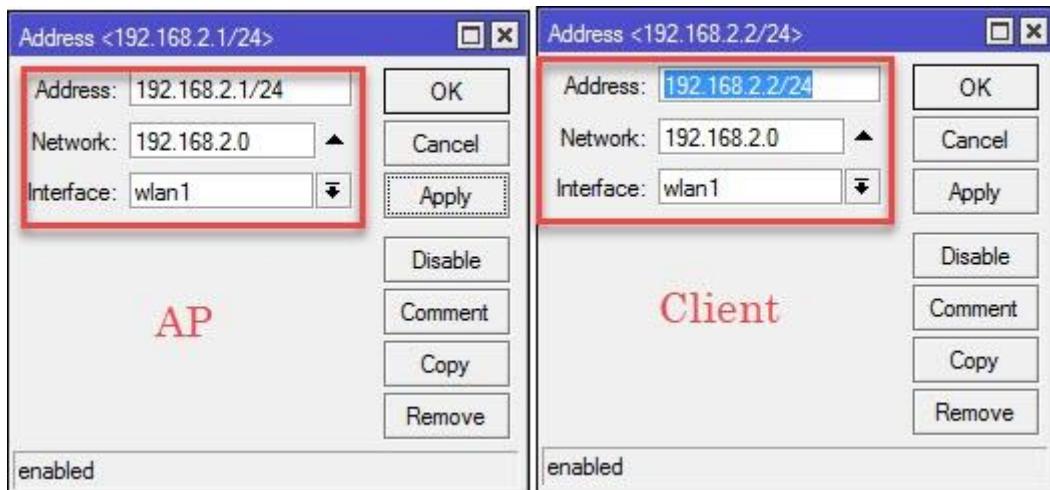


- Jangan lupa klik apply dan ok

3. Kemudian konfigurasikan IP address pada masing-masing interface **wlan1**, yaitu pada sisi AP maupun Client. Pada menu **IP > address**

a. Router AP: 192.168.2.1/24 klik apply dan ok

b. Router Client: 192.168.2.2/24 klik apply dan ok



4. Kemudian test ping koneksi untuk memastikan kedua routeboard tersebut sudah terhubung

```
[noc@PesantrenIDN] > ping 192.168.2.2
SEQ HOST SIZE TTL TIME STATUS
0 192.168.2.2 56 64 2ms
1 192.168.2.2 56 64 0ms
2 192.168.2.2 56 64 0ms
3 192.168.2.2 56 64 10ms
```

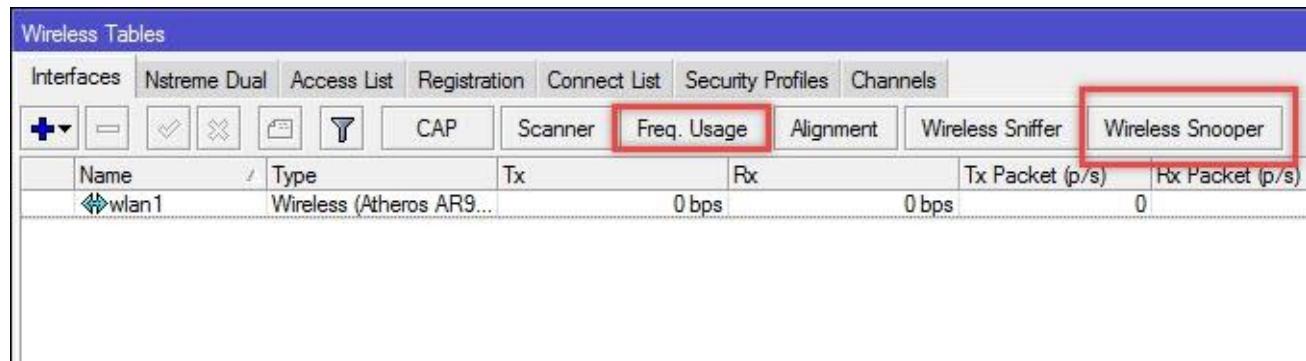
AP


```
[admin@MikroTik] > ping 192.168.2.1
SEQ HOST SIZE TTL TIME STATUS
0 192.168.2.1 56 64 7ms
1 192.168.2.1 56 64 0ms
2 192.168.2.1 56 64 0ms
3 192.168.2.1 56 64 1ms
```

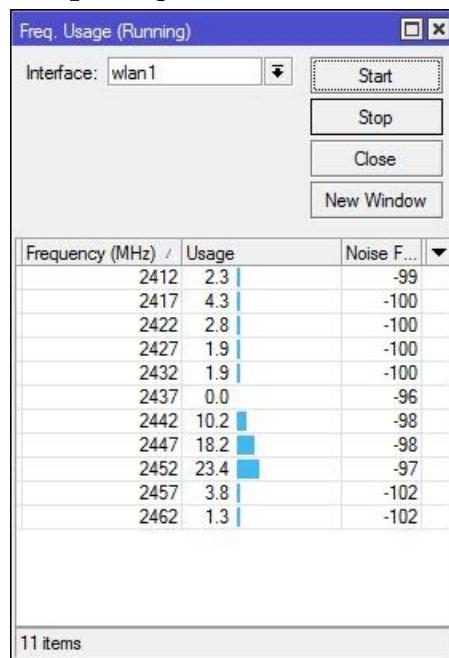
Client

Lab 39. Wireless Tool

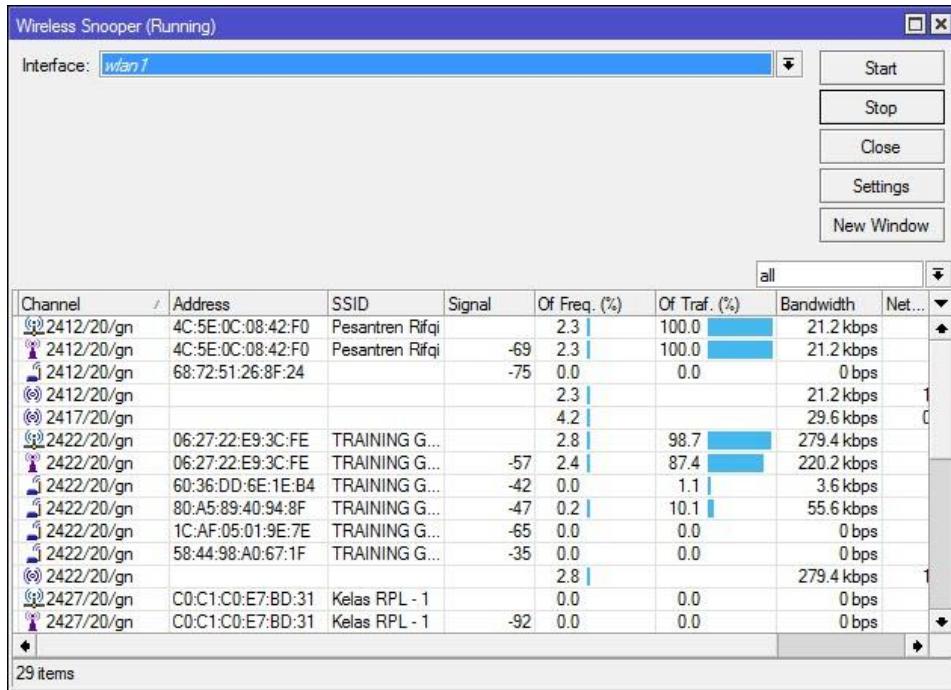
Pada Wireless mikrotik terdapat tool yang berfungsi untuk pemilihan channel yang lebih optimal dan untuk menghindari adanya interverensi. Pada la ini kita kan mencoba menggunakan 2 tool wireless yang ada pada mikrotik. Yaitu **Freqency Usage** dan **Snooper**. Untuk toolnya terdapat pada menu **wireless**. Saat menggunakan tool ini semua aktivitas dari wireless sementara akan terputus untuk beberapa saat.



- Freq. Usage



- Wireless Snooper



Lab 40. Virtual Access Point

Virtual Access Point adalah interface virtual wireless yang digunakan untuk membuat beberapa Access Point Virtual dari satu interface wireless fisik. Jadi hanya dengan menggunakan satu wireless interface fisik saja kita dapat membuat banyak virtual Access Point dengan **SSID**, **Network**, dan **Mac Address**, yang berbeda pada masing-masing AP. Namun **menggunakan frekuensi dan band yang sama** dengan wlan induknya (real). Berikut keterangan pada Virtual Access Point:

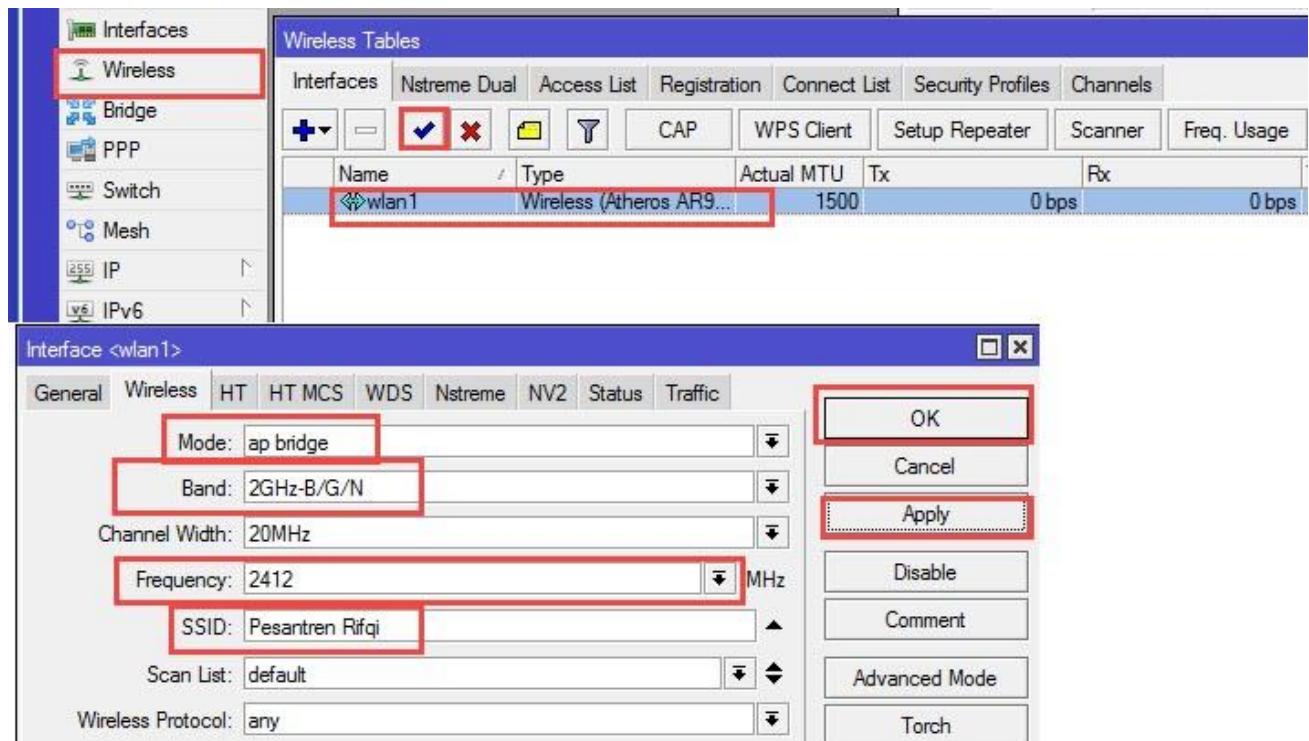
- Virtual AP akan menjadi child dari wlan yang ada (interface real)
- Satu Interface wlan dapat digunakan untuk membuat virtual AP dengan batas maksimum VAP sebanyak 128 VAP
- Virtual AP dapat dikonfigurasi dengan SSID, Network, security profile dan access list yang berbeda, namun frekuensi dan band yang digunakan sama dengan yang digunakan pada wlan induk (interface real)
- Virtual AP bersifat sama seperti AP pada umumnya seperti:
 - Dapat dihubungkan dengan station/client
 - Dapat mendistribusikan IP address dengan fitur DHCP Server
 - Dapat difungsikan sebagai Hotspot Server

Virtual AP pada mikrotik juga bisa dikonfigurasikan pada firewall. Fitur Virtual AP ini sama halnya seperti yang ada pada Virtual LAN (VLAN) pada jaringan kabel.

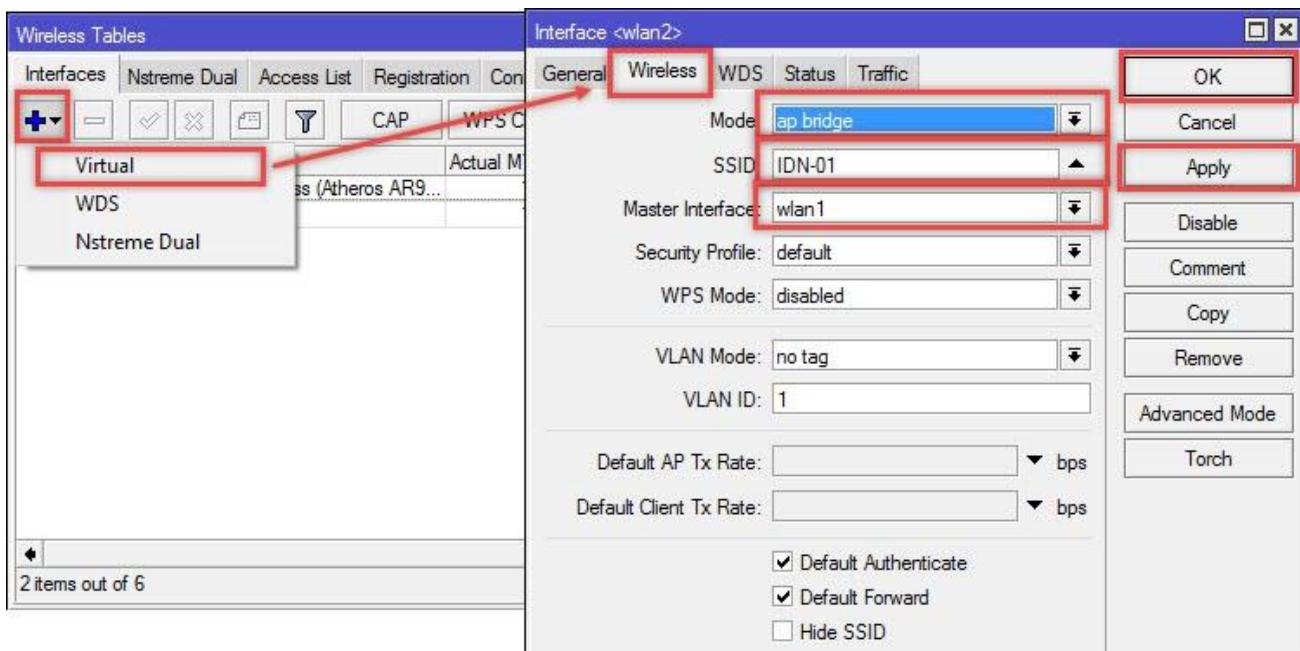
Contoh penggunaan Virtual AP pada real prakteknya bisa digunakan pada Wifi sekolah, dimana ada satu hotspot hanya digunakan untuk Guru dan satu hotspot digunakan untuk Siswa. Kita dapat membuat hal tersebut dengan menggunakan sebuah device mikrotik yang hanya memiliki satu interface wireless fisik, dengan menggunakan fitur VAP ini. Konfigurasi VAP dapat dikonfigurasikan pada menu: **Wireless > add > Virtual**.

Konfigurasi Virtual AP pada mikrotik:

1. Masuk pada menu wireless, kemudian aktifkan interface wlannya
2. Konfigurasikan wlan dengan mode **AP Bridge**
3. Set SSID sesuai dengan keinginan kita, jangan lupa klik apply dan ok



4. Selanjutnya, pada window wireless klik tombol (+)/Add dan pilih **Virtual**



5. Pada Tab General kita bisa mengubah nama virtual & Mac Addressnya, sedangkan pada tab Wireless kita bisa mengkonfigurasi SSID, Security Profile, dll
6. **Master interface** adalah wireless interface fisik yang dimiliki oleh routrboard,
7. Kemudian kita akan membuat VAP sebanyak 5 buah, konfigurasikan 5 buah VAP

Wireless Tables										
Interfaces		Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels			
R	wlan1	Wireless (Atheros AR9...)	1500	0 bps	2.7 kbps					
	↳ wlan2	Virtual	1500	0 bps	0 bps					
	↳ wlan3	Virtual	1500	0 bps	0 bps					
	↳ wlan4	Virtual	1500	0 bps	0 bps					
	↳ wlan5	Virtual	1500	0 bps	0 bps					
	↳ wlan6	Virtual	1500	0 bps	0 bps					

8. Pastikan Virtual AP yang tadi kita buat sudah bisa tersedia



Lab 41. Wireless Mac Filtering (Default Authenticated)

Masih dalam materi wireless pada mikrotik, pembahasan kali ini kita akan mengbahas mengenai konfigurasi Wireless Mac Address Filtering. Maksudnya adalah kita akan memfilter suatu mac address suatu koneksi jaringan agar tidak diganggu oleh yang lain, walaupun memiliki SSID yang sama. Mac Filtering dapat dikonfigurasikan pada sisi Access Point Maupun pada sisi Station,

Keterangan Wireless Mac Filtering pada Access Point & Station:

- Pada **Access Point**, access point dapat melakukan pembatasan hak akses dimana AP hanya bisa terhubung oleh station sudah kita tentukan.
- Pada **Station**, station juga bisa kita lock agar hanya bisa terhubung dengan AP yang sudah ditentukan

Untuk konfigurasi Mac Filtering pada AP bisa dikonfigurasikan di **Access List**, sedangkan untuk Station bisa dikonfigurasikan di **Connect List**. Untuk Lab nya perhatikan topologi berikut:

Jaringan A

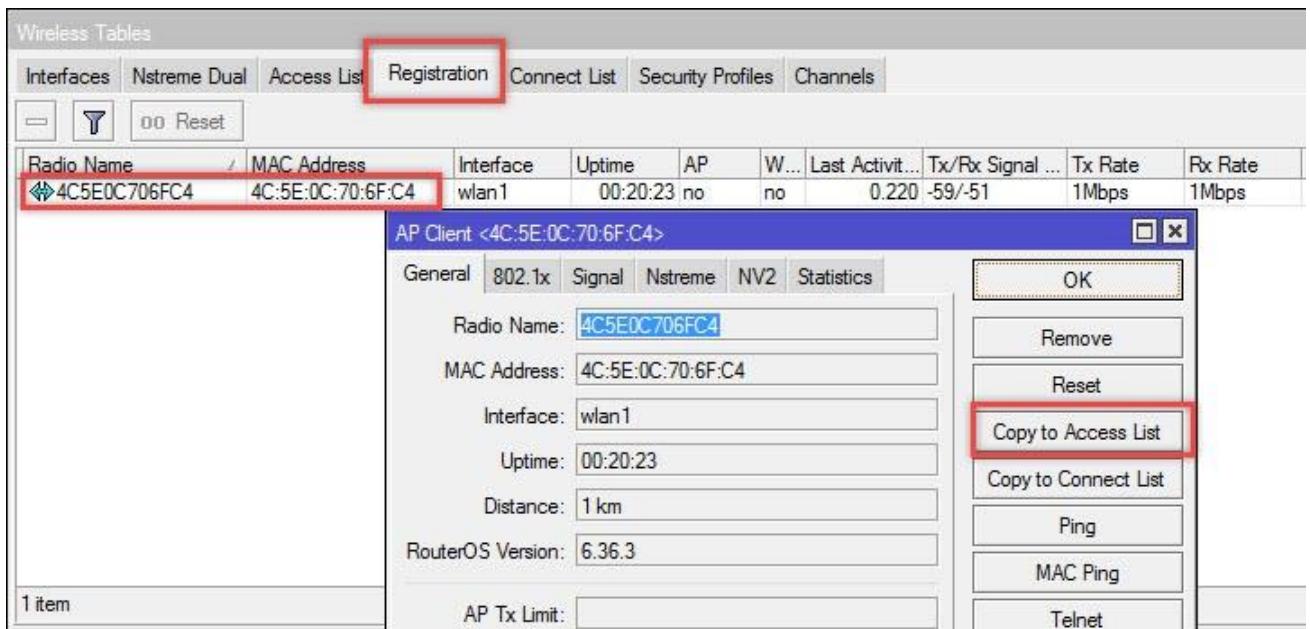


Jaringan B

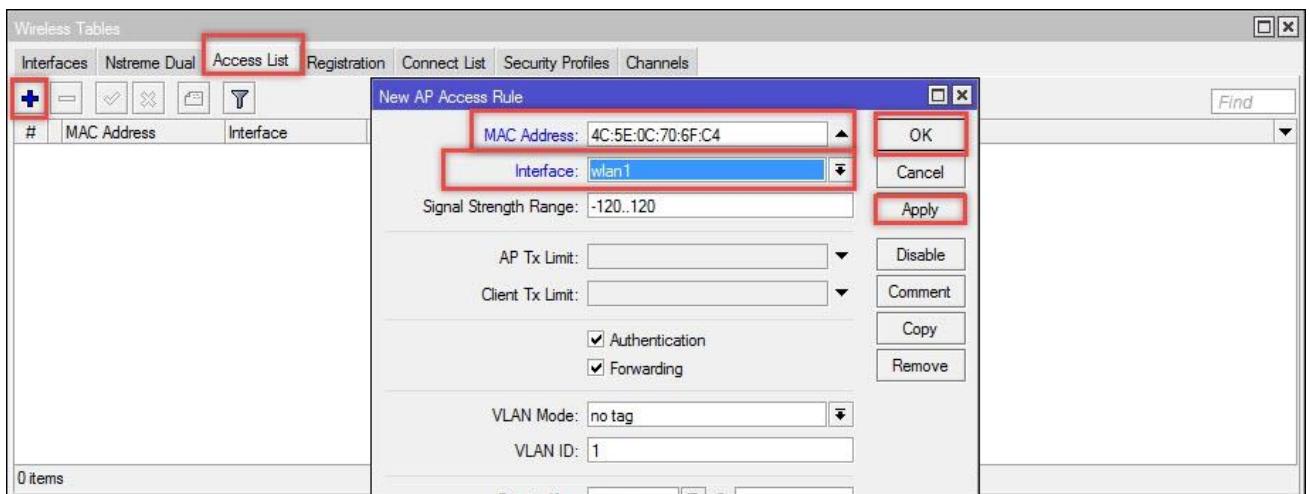


Untuk lab ini kita membutuhkan 4 Routerboard, dan juga kita harus mengkonfigurasikan setiap 2 router ke dalam jaringan Peer to peer, sehingga nantinya kita akan memiliki 2 jaringan peer to peer. Untuk topology diatas semua konfigurasi AP menggunakan SSID yang sama.

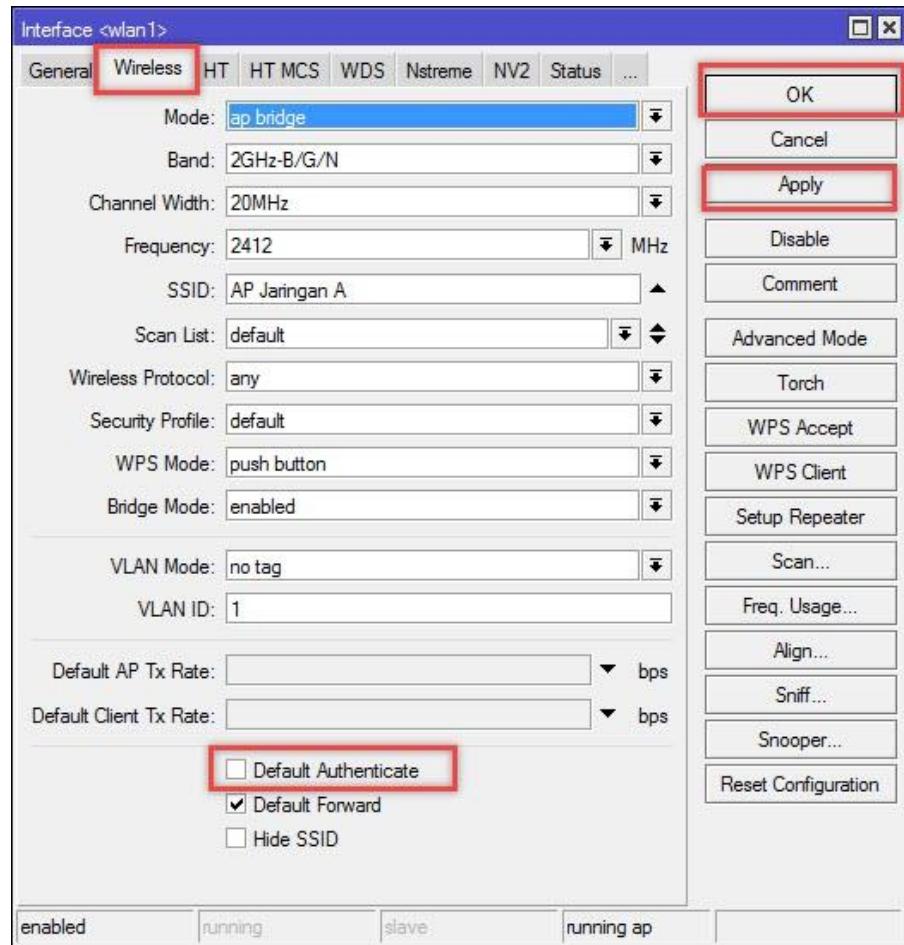
1. Konfigurasikan Jaringan A dan B sesuai dengan topology diatas.
2. Konfigurasikan IP wlan pada masing masing router sesuai dengan topologi diatas.
3. Konfigurasikan pada Jaringan A maupun B pada sisi AP seperti berikut:
4. Sebelumnya pastikan client dan access point bisa terhubung terlebih dahulu agar lebih mudah dalam melakukan filtering
5. Masuk pada menu **Registration**, terlihat bahwa ada 1 client yang sudah terhubung ke AP, copykan mac address tersebut pada menu **Access List** atau secara mudahnya lagi klik pada **copy to access list** (untuk sisi AP)



6. Masuk pada menu **Access List**, klik add (+), daftarkan mac client yang tadi kita copy pada kolom mac address yang disediakan, untuk interfacenya pilih **wlan1**, jangan lupa klik apply lalu ok



7. Pada Menu Interface wireless, un-check pada **Default Authenticate** jangan lupa untuk di apply dan Ok .



8. Konfigurasikan pada Jaringan A maupun B pada sisi client seperti berikut:
9. Karena client sudah terhubung ke Access Point, Masuk pada menu **Registration**, terlihat bahwa ada 1 Access Point yang sudah terhubung ke client, copykan mac address tersebut pada menu **Connect List** atau secara mudahnya lagi klik pada **copy to connect list** (untuk sisi client)

Wireless Tables

Interfaces	Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels			
—	—	—	oo Reset	—	—	—			
Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
4C5E0C0...	4C:5E:0C:08:42:F0	wlan1	00:09:38	yes	no	0.850	-56/-61	11Mbps	1Mbps

AP Client <4C:5E:0C:08:42:F0>

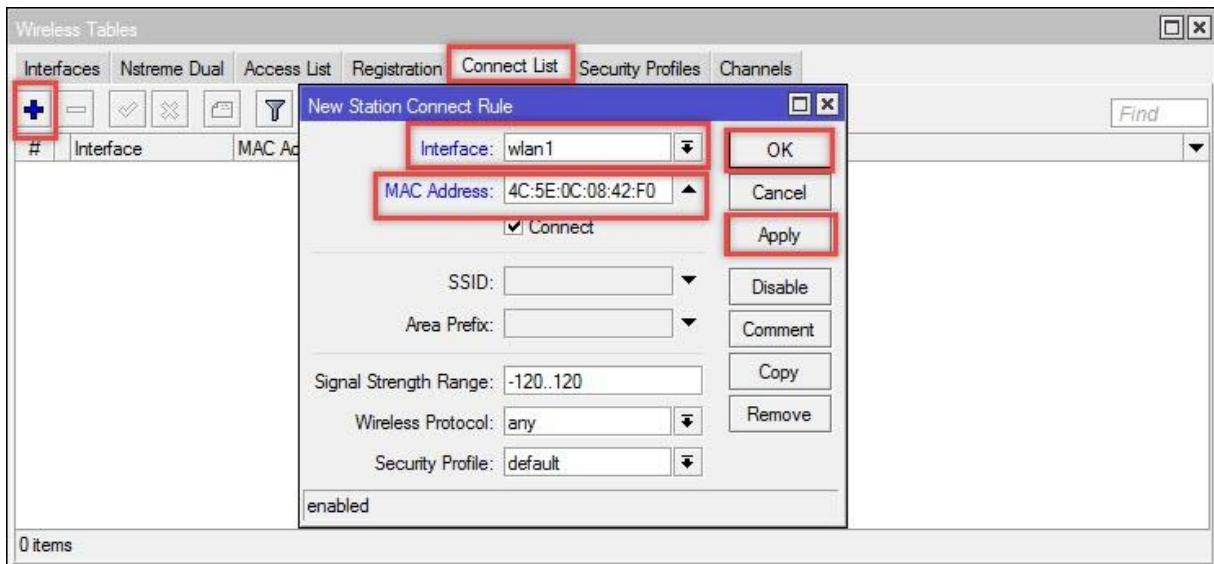
General	802.1x	Signal	Nstreme	NV2	Statistics
Radio Name: 4C5E0C0842F0	MAC Address: 4C:5E:0C:08:42:F0	Interface: wlan1	Uptime: 00:09:38	Distance: 23 km	RouterOS Version: 6.37.1
AP Tx Limit:					

Context menu on the right side of the client table row:

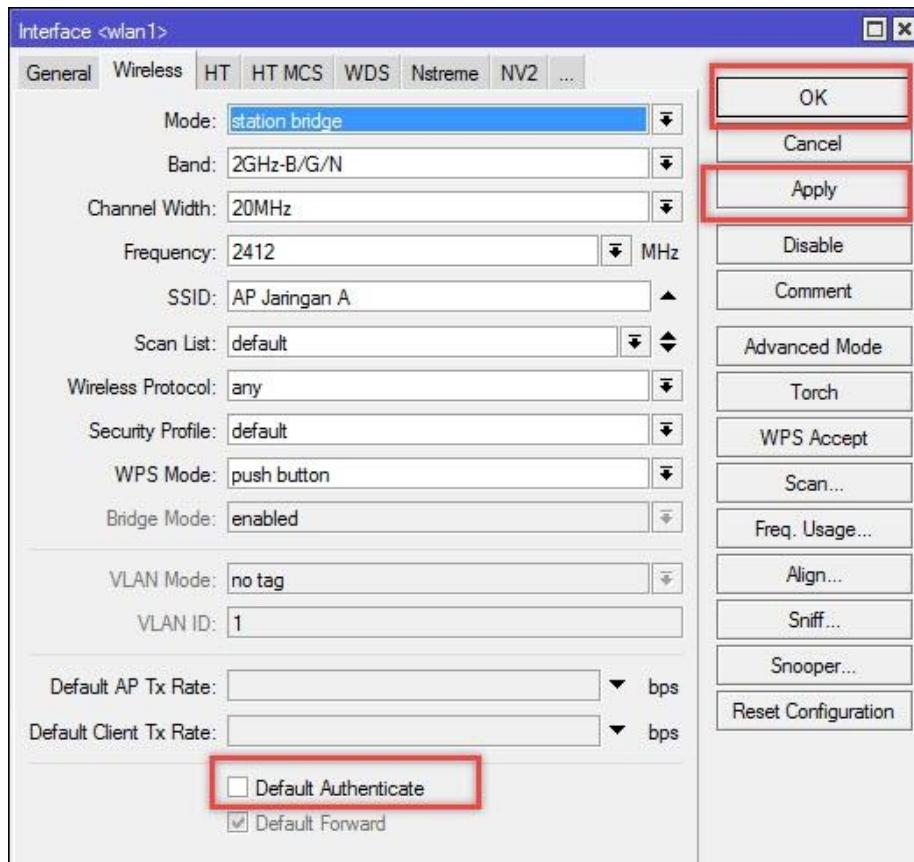
- OK
- Remove
- Reset
- Copy to Access List**
- Copy to Connect List**
- Ping
- MAC Ping
- Telnet

1 item (1 selected)

10. Masuk pada menu **Connect List**, klik add (+), daftarkan mac client yang tadi kita copy pada kolom mac address yang disediakan, untuk interfacenya pilih **wlan1**, jangan lupa klik apply lalu ok



11. Pada Menu Interface wireless, un-check pada **Default Authenticate** jangan lupa untuk di apply dan Ok .

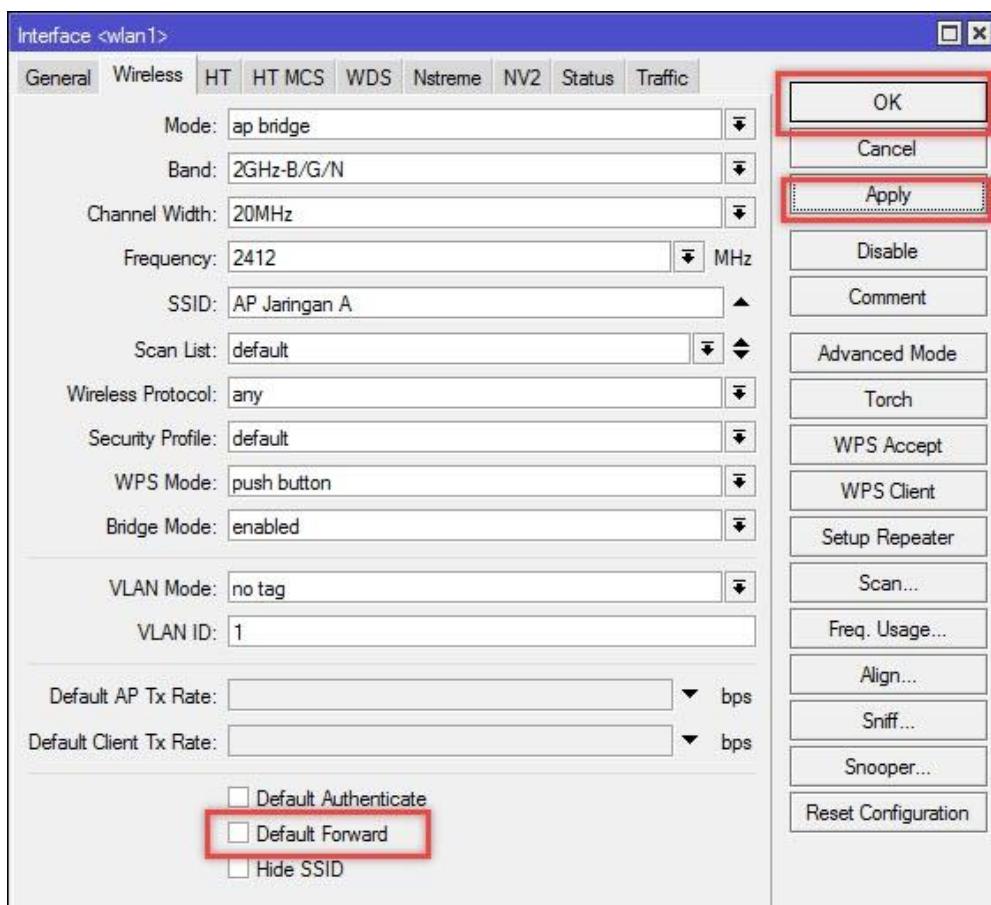


12. Uji coba dengan cara mencoba client untuk terkoneksi ke access point yang bukan pada jaringannya

Lab 42. Wireless Mac Filtering (Default Forwarding)

Melanjutkan lab pada pembahasan sebelumnya, fitur default forwarding ini berfungsi untuk mengijinkan / tidak mengijinkan komunikasi antar client/station yang terkoneksi dalam 1 access point. Ketika default forward ini diun-check maka sesama station yang terhubung tidak dapat saling berkomunikasi. Default forward didisable karena untuk alasan keamanan. Untuk Konfigurasinya, default forward hanya bisa dikonfigurasikan pada **Access Point**. Konfigurasinya sebagai berikut:

1. Buka menu Interface wireless, double klik pada **wlan1**, klik pada tab **wireless**, un-check **default forward**



2. Uji coba ping antar client yang masih dalam satu access point, apakah bisa ngeping atau tidak?

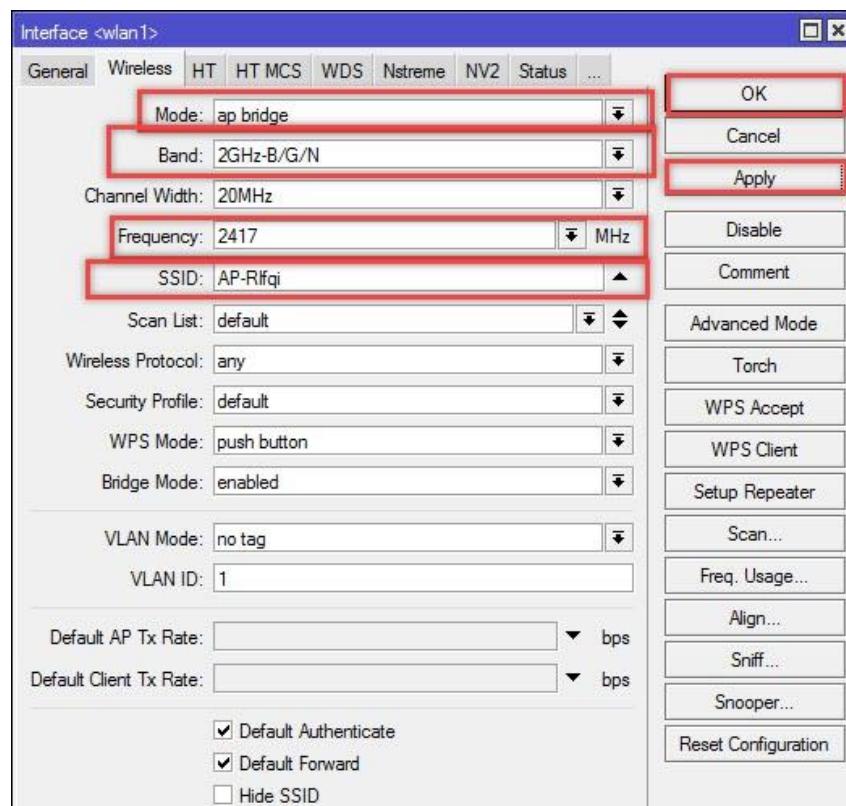
Lab 43. Konfigurasi Wireless Nstream

Nstream adalah fitur wireless yang ada pada mikrotik yang digunakan untuk meningkatkan perfomance link wireless untuk skala koneksi jarak jauh. Juga sebagai penguat sinyal dan meingkatkan throughput bandwith wireless, namun juga tergantung dengan hardware device wireless, slot frekuensi pada tempat tersebut, dan kondisi lapangan

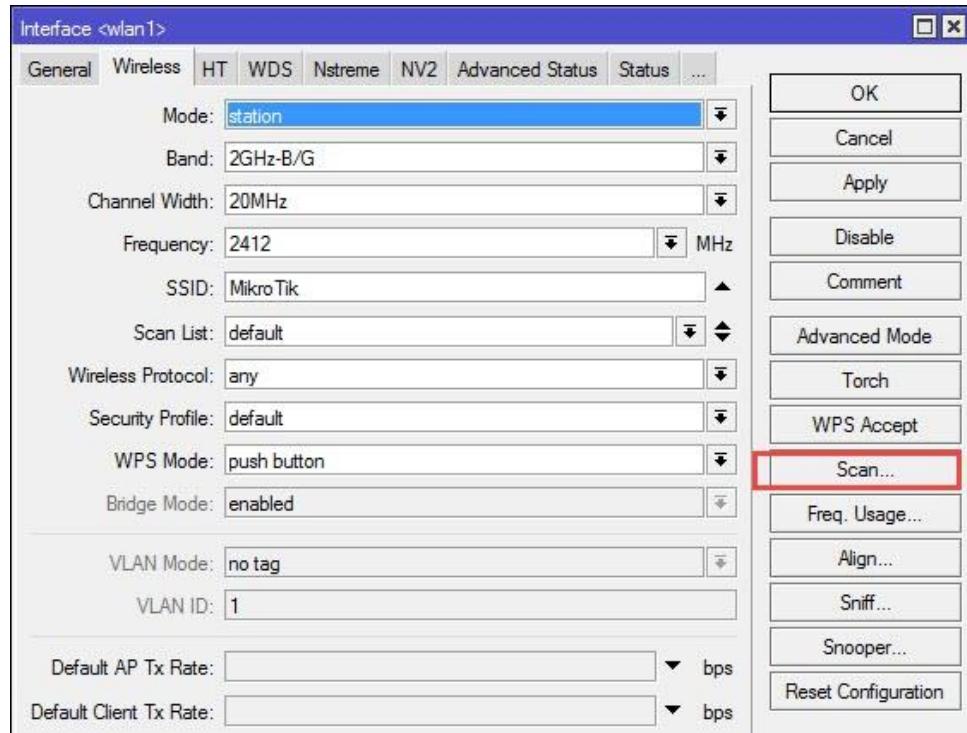
Untuk konfigurasinya terdapat pada menu **Wireless > Interface**

Pada lab berikut kita akan menggunakan topologi point to point antara **AP** dan **Client**, yang berarti kita membutuhkan 2 routerboard dengan fasilitas wireless. Konfigurasinya sebagai berikut:

1. Pertama ubah terlebih dahulu identity pada masing-masing router, untuk router1=AP dan router2=Station, konfigurasikan pada **System > Identity**
2. Kemudian konfigurasi pada sisi **AP** dengan parameter sebagai berikut:
 - Masuk ke menu Wireless
 - Pilih mode=**ap bridge**
 - Pilih band=**2ghz-B/G/N**
 - Pilih Frequency=**2417**
 - Pada SSID=**AP-Rifqi**
 - Klik apply dan ok



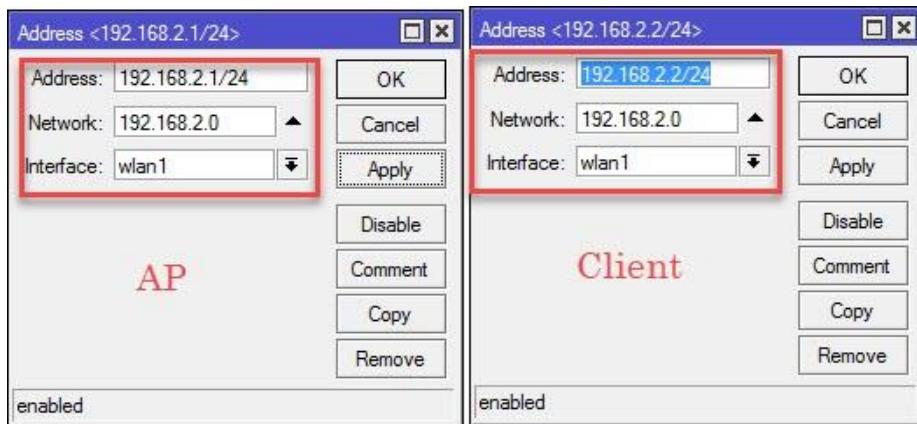
3. Pada sisi client, lakukan scan wireless dan hubungkan dengan AP yang memiliki SSID=AP-Rifqi, untuk scan bisa dilakukan pada menu **Wireless > Interface > Scanner**



Scanner (Running)

Address	SSID	Channel	Signa...	Noise...	Signa...	Radio Name	...
ARB 4C:5E:0C:08:42:F0	AP-Rifqi	2417/2...	-61	-100	39	4C5E0C0842F0	6.
AP 06:27:22:E9:3C:FE	TRAINING GURU TKJ...	2422/2...	-50	-101	51		
AP C0:C1:C0:E7:BD:31	Kelas RPL - 1	2427/2...	-92	-100	8		
AP 42:A5:89:37:62:CB	Sk55k-WmFyc2xhbW...	2427/2...	-91	-100	9		
AP C0:C1:C0:25:01:82	Kelas RPL - 2	2437/2...	-88	-96	8		
AP 0A:18:D6:A9:DB:26	Kantor SMK MQ	2462/2...	-85	-103	18		

4. Kemudian konfigurasikan masing masing ip address pada tiap-tiap interface wlan di AP dan Client

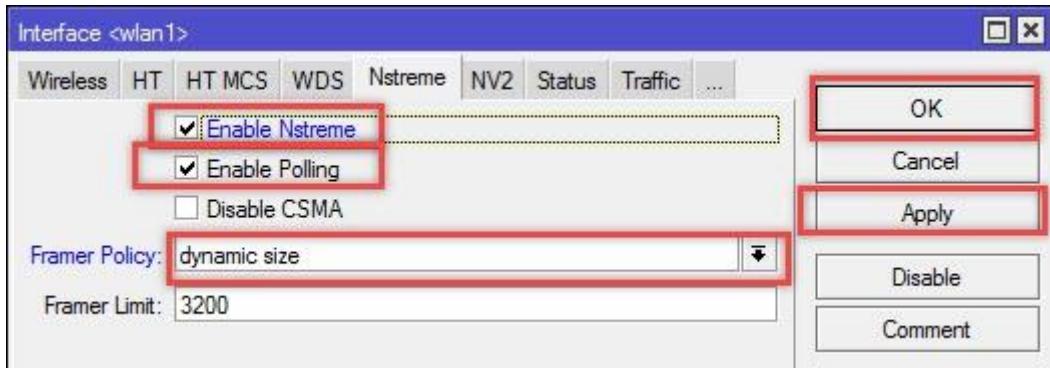


5. Tes ping untuk memastikan koneksi antara AP dan Client sudah terhubung

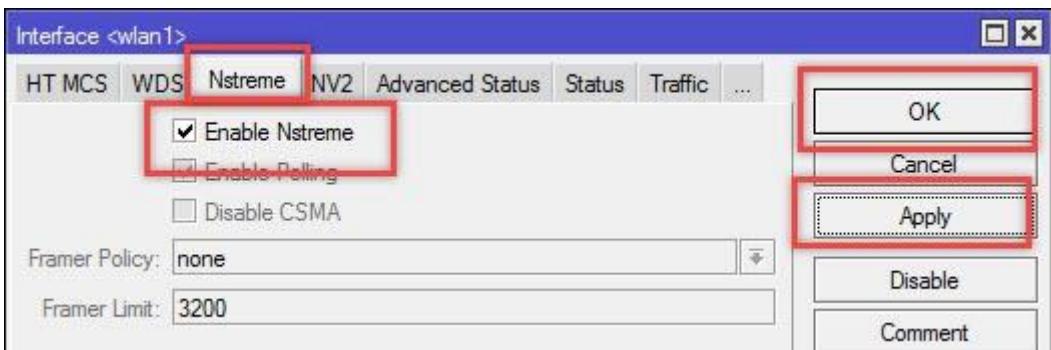
```
[noc@PesantrenIDN] > ping 192.168.2.2
SEQ HOST SIZE TTL TIME STATUS
0 192.168.2.2 56 64 2ms
1 192.168.2.2 56 64 0ms
2 192.168.2.2 56 64 0ms
3 192.168.2.2 56 64 10ms
AP

[admin@MikroTik] > ping 192.168.2.1
SEQ HOST SIZE TTL TIME STATUS
0 192.168.2.1 56 64 7ms
1 192.168.2.1 56 64 0ms
2 192.168.2.1 56 64 0ms
3 192.168.2.1 56 64 1ms
Client
```

6. Pada router AP, masuk pada **interface wlan1 > Nstream**, aktifkan fitur dengan mencentang pada () **Enable Nstream**, untuk Frame Policy= **dynamic size**, jangan lupa klik apply dan ok

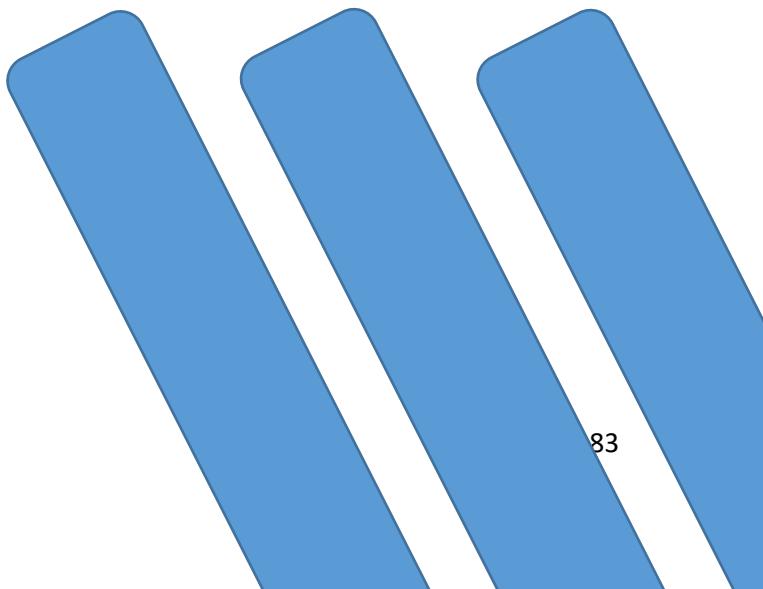


7. Untuk router client, masuk pada **interface wlan1 > Nstream** dan mengaktifkan **nstream** dengan mencentang pada () **Enable Nstream**



8. Test pada sisi station menggunakan bandwith test saat menggunakan nstream dan tidak menggunakan nstream

BRIDGE



Bab 5. Bridge

Bridge pada mikrotik adalah penggabungan 2 atau lebih interface seolah-olah berada dalam 1 segmen network yang sama. Bridge juga bisa dijalankan pada jaringan wireless. Interface bridge adalah interface virtual, karena virtual kita bisa membuat interface bridge sebanyak yang kita inginkan.

Secara teknikal pembuatan bridge baru dengan cara membuat interface bridge & menambahkan interface fisik ke dalam port bridge. Jika kita hanya membuat interface bridge tanpa menambahkan interface fisik pada port bridgenya, maka bridge tersebut akan dianggap sebagai interface loopback.

Penggunaan bridge juga memiliki kelemahan, kelemahan bridge sebagai berikut:

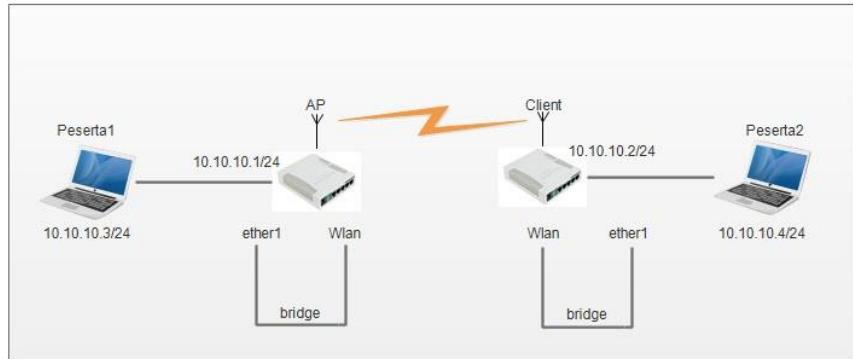
- Sulit untuk mengatur traffik broadcast karena terlalu banyaknya traffic broadcast yang ada
- Permasalahan pada satu port/segmen akan mengakibatkan masalah pada port/segmen yang ada pada bridge yang sama
- Peningkatan beban traffik akibat terjadi karena terlalu banyaknya traffic broadcast yang ada

Wireless Bridge

Untuk wireless bridge, mikrotik mendukung semua mode wireless untuk dilakukan bridging, kecuali hanya pada mode station. Karena mode station tidak bisa digunakan untuk bridge akhirnya mikrotik menciptakan mode station dengan baru yaitu station bridge. Station bridge bisa bekerja pada koneksi antar mikrotik.

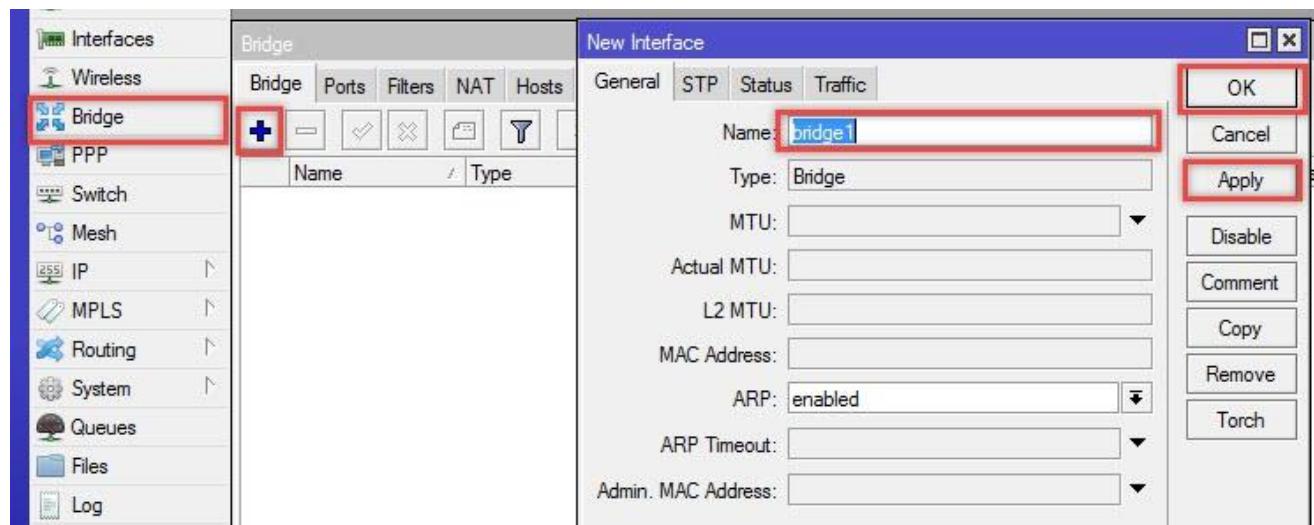
Lab 44. Konfigurasi Wireless Bridging

Untuk konfigurasi bridging pada wireless konfigurasinya hampir sama dengan konfigurasi pada media kabel, perbedaannya hanya interface **wlan** juga dimasukkan pada port bridge. Pada lab kita juga akan membuat koneksi wireless antara AP & Client terlebih dahulu, untuk lebih jelasnya Perhatikan topologi berikut:

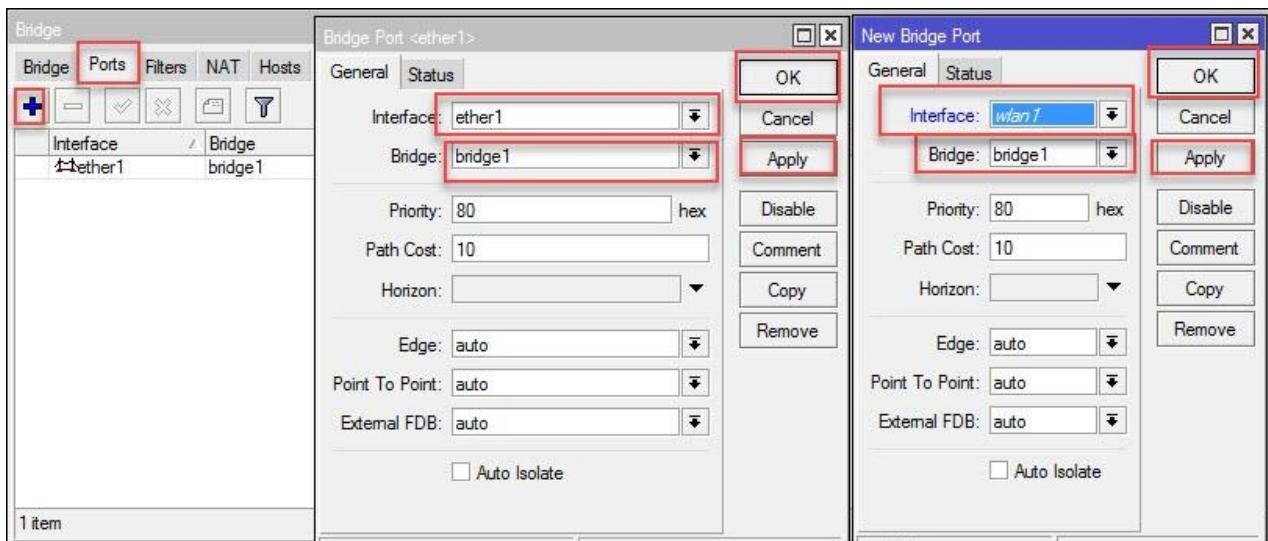


Konfigurasinya sebagai berikut:

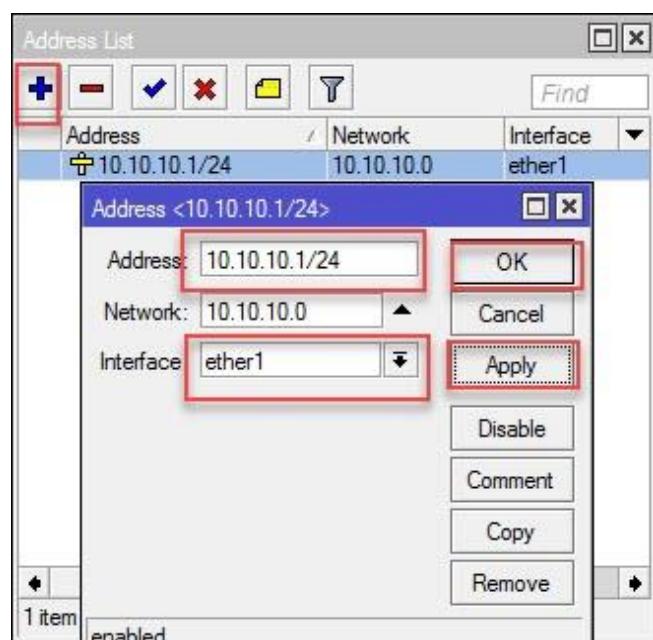
1. Pastikan antara kedua router tersebut sudah saling terhubung via wireless
2. Lalu buat interface **bridge** untuk router 1, masuk ke menu **Bridge > add (+)**, beri nama interface bridge dengan nama **bridge1**, jangan lupa klik apply dan ok



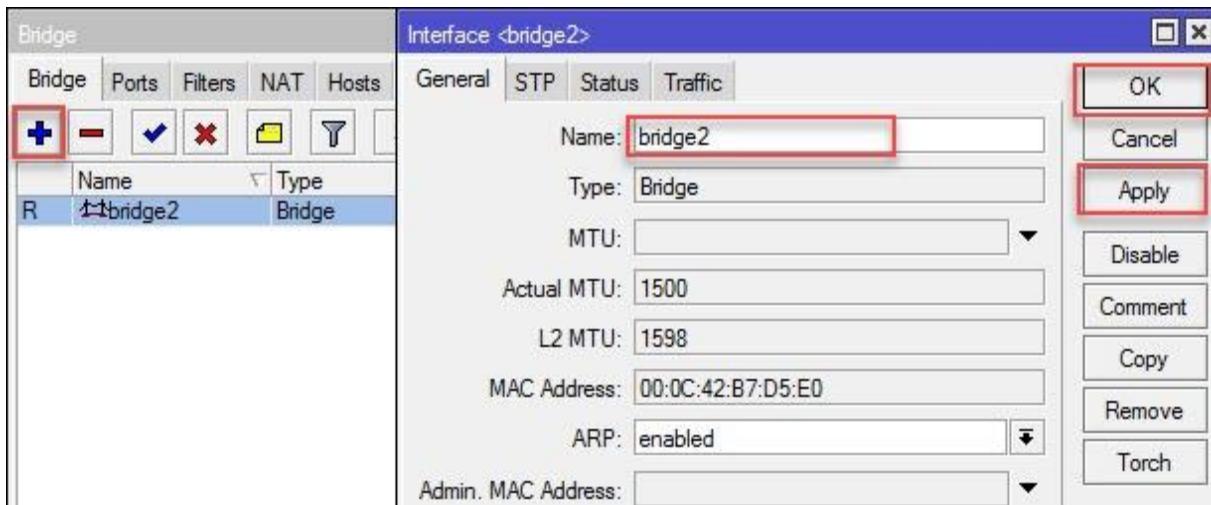
3. Klik pada tab **Ports**, tambahkan interface **wlan1** dan **ether1** pada port **bridge**



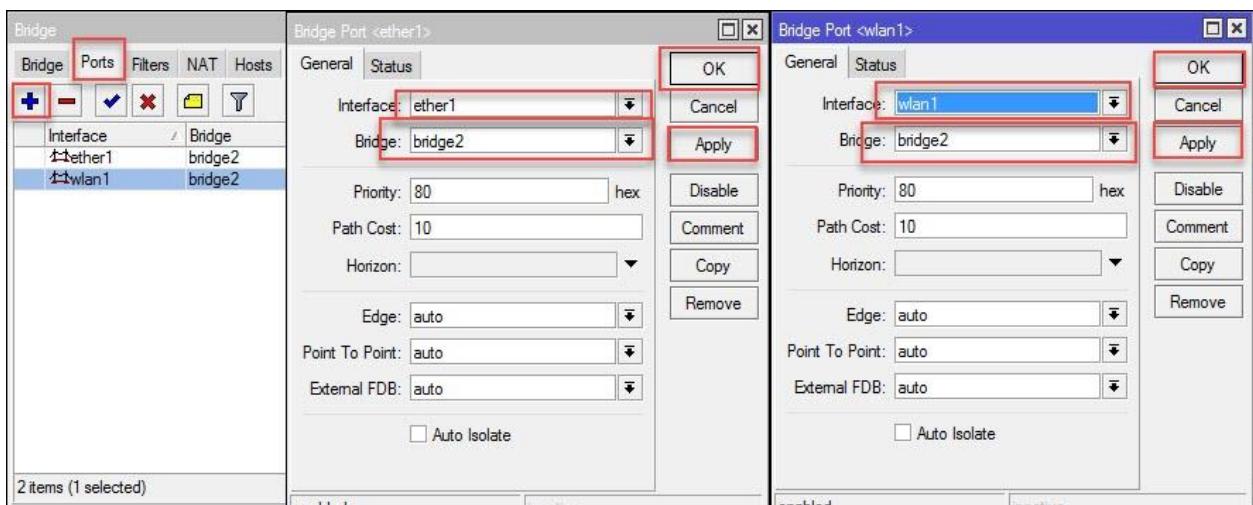
4. Setelah itu tambahkan ip address pada interface **ether1** karena interface tersebut yang terhubung ke pc/laptop peserta, dengan IP Address **10.10.10.1/24**



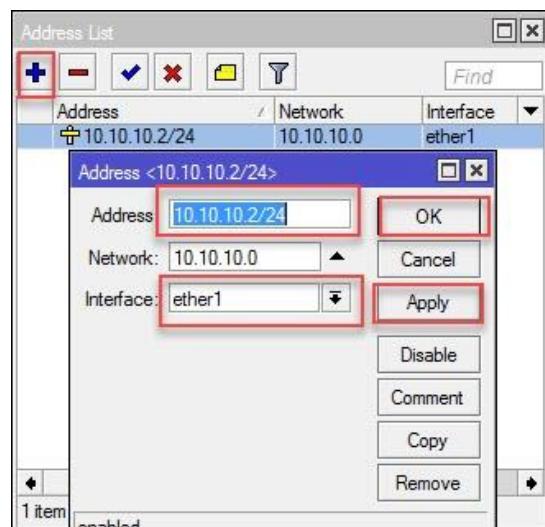
5. Kemudian konfigurasikan bridge pada sisi client, dengan hal yang sama seperti pada konfigurasi bridge di AP, masuk ke menu **Bridge > add (+)**, beri nama interface bridge dengan nama **bridge2**, jangan lupa klik apply dan ok



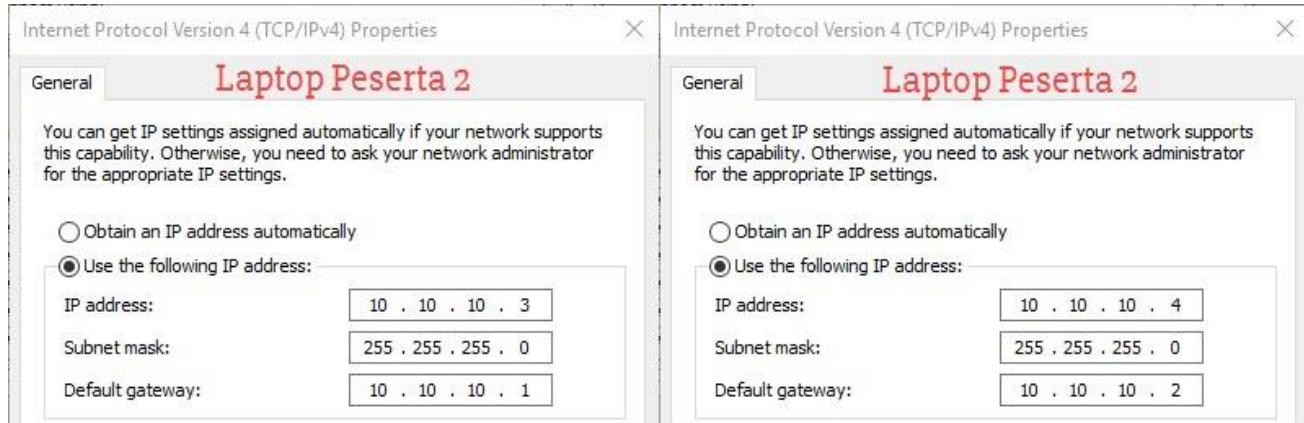
6. Klik pada tab Ports, tambahkan interface **wlan1** dan **ether1** pada port bridge



7. Setelah itu tambahkan ip address pada interface **ether1** karena interface tersebut yang terhubung ke pc/laptop peserta, dengan IP Address **10.10.10.2/24**



8. Setting IP address pada masing masing pc/laptop yang terhubung ke routerboard,seperti berikut



9. Kemudian coba tes ping dari peserta dengan mencoba ping ke ip address router1 dan ip address laptop peserta1

```
C:\ Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Fariz>ping 10.10.10.1 → Router1
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Fariz>ping 10.10.10.3 → Pc client1
Pinging 10.10.10.3 with 32 bytes of data:
Reply from 10.10.10.3: bytes=32 time=1ms TTL=64
Reply from 10.10.10.3: bytes=32 time<1ms TTL=64
Reply from 10.10.10.3: bytes=32 time<1ms TTL=64
Reply from 10.10.10.3: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Fariz>
```

10. Coba tes kembali pada sisi peserta 1, ping ke ip router & laptop peserta 2

röütig

Bab 6. Routing

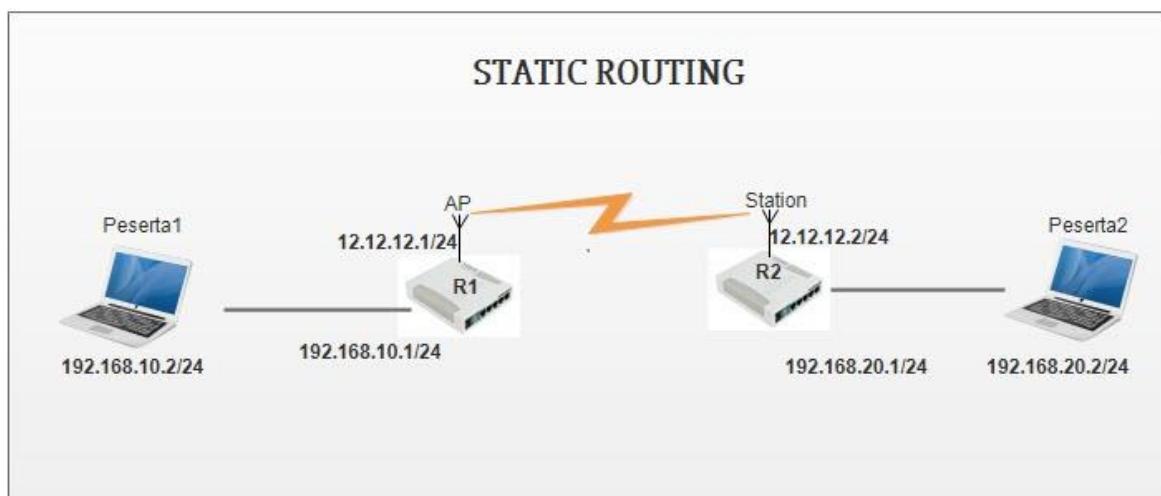
Pada bab ini kita akan membahas tentang fungsi dari sebuah router yaitu **Routing**, apa itu routing? **Routing** adalah metode untuk menghubungkan beberapa network yang berbeda, nah pada bab ini kita akan membahas salah satu jenis dari routing yaitu routing static.

Routing Static adalah proses routing yang dilakukan dengan menambahkan network tujuan secara manual, jadi kita menambahkan network tujuan yang akan kita tuju secara manual (dilakukan oleh administrator). Pada static route parameter yang perlu kita tambahkan secara manual yaitu **network tujuan & gateway**.

Konsep yang digunakan untuk static route adalah "**Mau ke network mana?, lewat gateway mana?**

Biar lebih paham akan static route, mari kita lab kan saja biar ndak pada penasaran lagi, perhatikan topology lab berikut:

Lab 45. Konfigurasi Static Route



Pada lab ini saya tidak membahas mengenai cara menghubungkan router via wireless, dan cara penambahan ip address pada interface, untuk konfigurasi-konfigurasi diatas bisa dicari pada bab & lab lab sebelumnya, saya mulai langsung tentang konfigurasi static route.

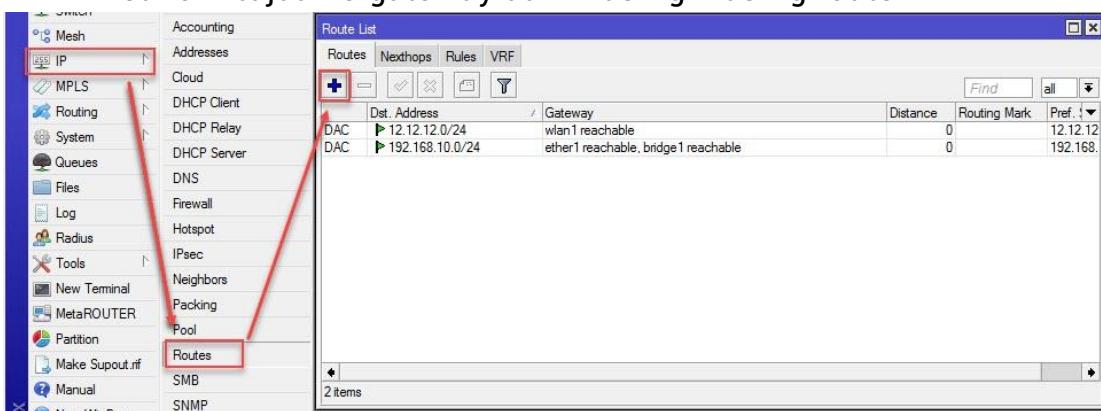
1. Tujuan lab berikut adalah kita akan menghubungkan Laptop **peserta1** (network **192.168.10.0/24**) bisa terhubung dengan Laptop **peserta2** (network **192.168.20.0/24**)

2. Pastikan Konfigurasi pada masing masing router sudah terkonfigurasi dengan benar

Address	Network	Interface
12.12.12.2/24	12.12.12.0	wlan1
192.168.20.1/24	192.168.20.0	ether1

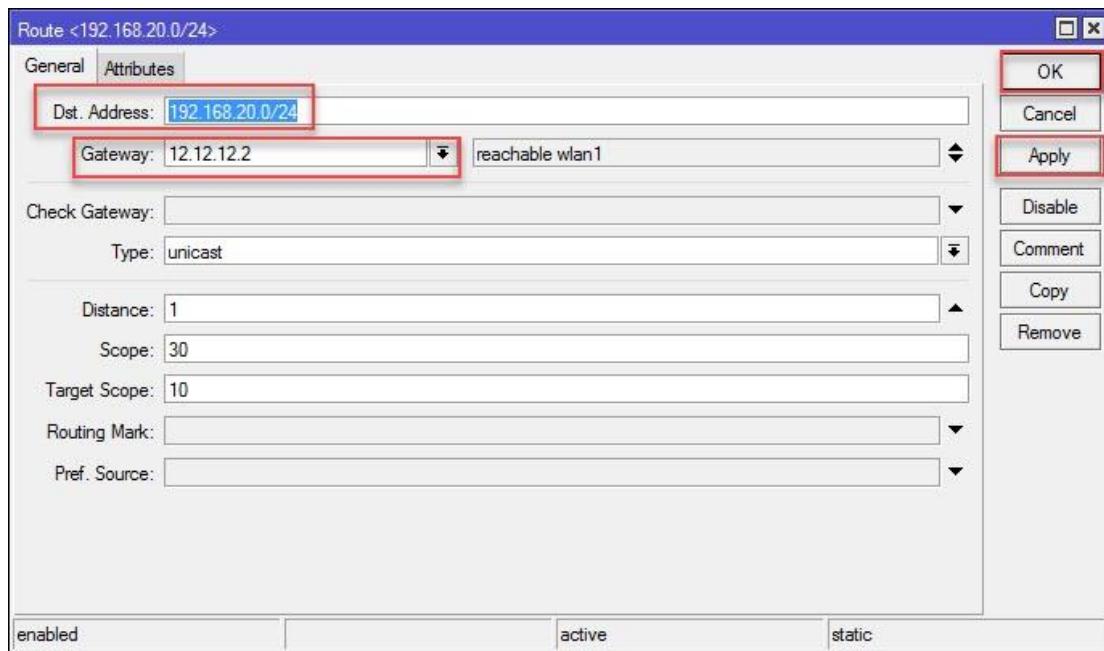
Address	Network	Interface
12.12.12.1/24	12.12.12.0	wlan1
192.168.10.1/24	192.168.10.0	ether1

3. Konfigurasikan Static Route Pada menu IP > Route > Add (+), masukkan network tujuan & gateway dari masing masing router



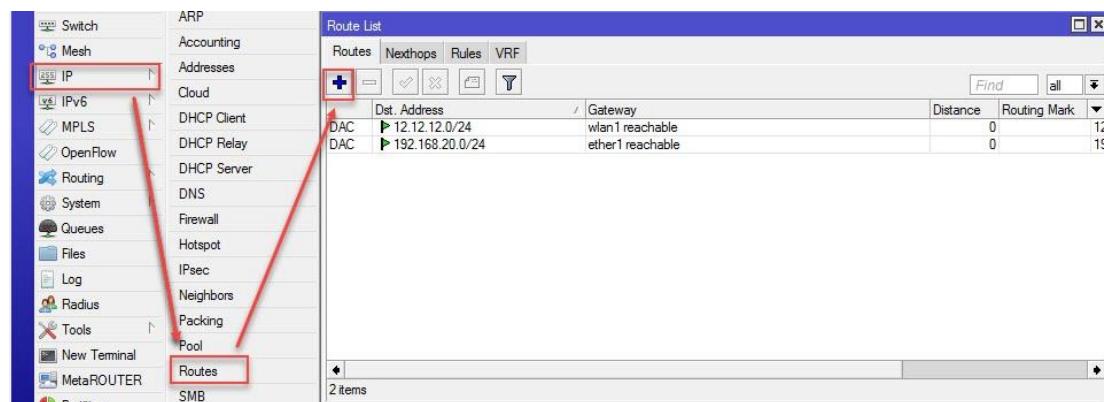
Pada Router R1

Tujuan network dari Router R1 adalah network **(192.168.20.0/24)**, maka network tersebut yang akan kita isikan pada kolom **Dst Address**, sedangkan untuk **Gateway** kita isikan ip address **wlan** dari router client, yaitu **12.12.12.2** karena ip address tersebutlah yang terhubung langsung dengan network **(192.168.20.0/24)**



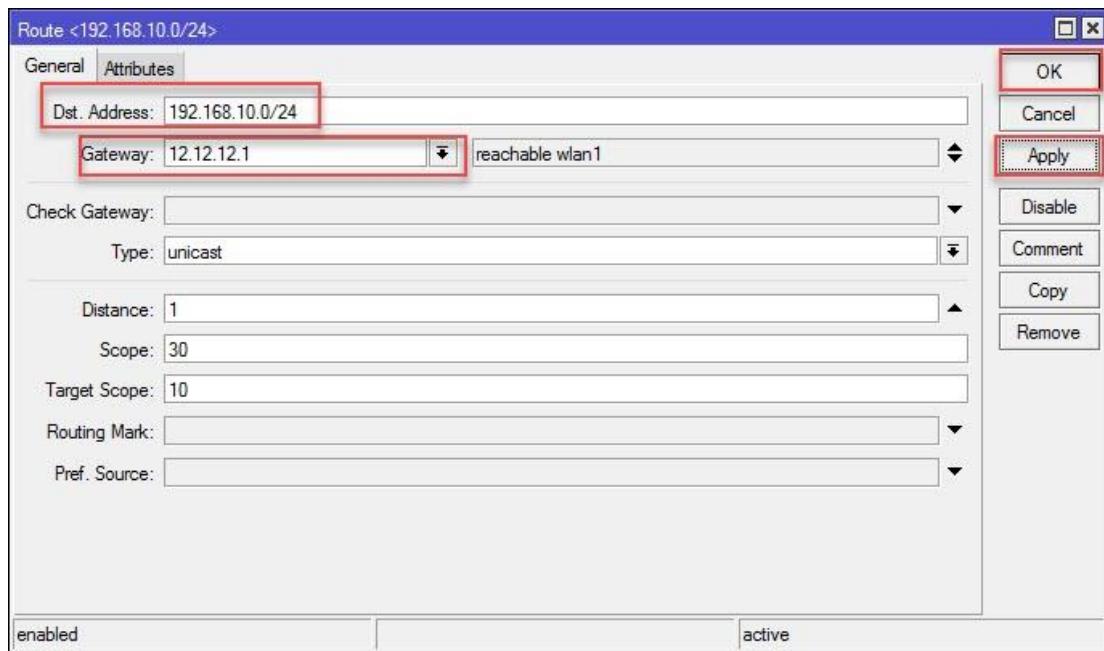
Jangan Lupa klik apply dan ok

4. Sedangkan untuk sisi Router R2 konfigurasikan Static Route Pada menu IP > Route > Add (+),



Pada Router R2

Tujuan network dari Router R2 adalah network (192.168.10.0/24), maka network tersebut yang akan kita isikan pada kolom Dst Address, sedangkan untuk Gateway kita isikan ip addrees wlan dari router client, yaitu 12.12.12.1 karena ip address tersebutlah yang terhubung langsung dengan network (192.168.10.0/24)



5. Kemudian setting Ip address dan gateway masing masing laptop, sesuai dengan topology diatas,
6. Tes ping antara Laptop Peserta R1 dan laptop Peserta R2, begitu juga sebaliknya. Untuk Laptop1 default gatewaynya yaitu **192.168.10.1**, sedangkan Laptop2 default gatewaynya yaitu **192.168.20.1**

```

C:\ Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Fariz>ping 12.12.12.1 → Ping ke Interface
                                         wlan Router R1
Pinging 12.12.12.1 with 32 bytes of data:
Reply from 12.12.12.1: bytes=32 time<1ms TTL=63
Reply from 12.12.12.1: bytes=32 time=8ms TTL=63
Reply from 12.12.12.1: bytes=32 time=57ms TTL=63
Reply from 12.12.12.1: bytes=32 time=1ms TTL=63

Ping statistics for 12.12.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 57ms, Average = 16ms

C:\Users\Fariz>ping 192.168.10.2 → Ping ke laptop
                                         peserta 1
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time<1ms TTL=63
Reply from 192.168.10.2: bytes=32 time=9ms TTL=63
Reply from 192.168.10.2: bytes=32 time<1ms TTL=63
Reply from 192.168.10.2: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

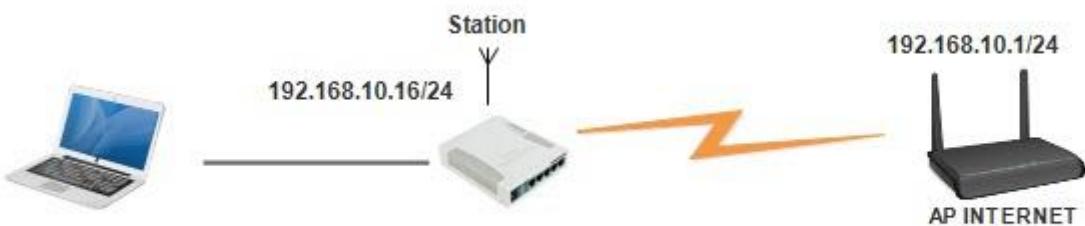
C:\Users\Fariz>

```

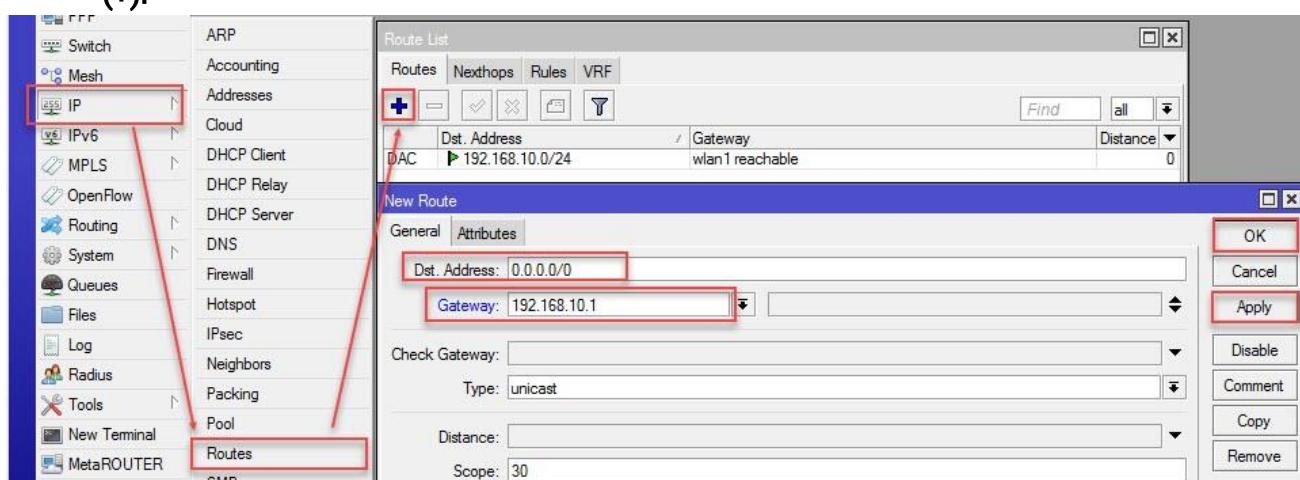
Lab 46. Konfigurasi Default Route

Default Route digunakan ketika network yang akan kita tuju sudah terlalu banyak, jika kita konfigurasi network tujuan kita satu persatu nanti akan membebani pada tabel routing. Default route digunakan pada routing untuk akses ke internet.

Untuk Konfigurasinya perhatikan topology berikut



1. Konfigurasikan routerboard ke access point yang tersedia, jika AP menggunakan security konfigurasikan juga pada routerboard
2. Set IP address secara static pada routerboard, sesuaikan juga network yang ada pada jaringan tersebut
3. Konfigurasi Default Route dapat dikonfigurasikan pada menu IP > Route > Add (+).



4. Masukkan Pada kolom Dst. Address= 0.0.0.0/0 dan pada Gateway= 192.168.10.1. 0.0.0.0/0 maksudnya adalah semua network, karena kita akan terhubung internet dan kita tidak tahu tentang network network apa saja yang ada diinternet maka cukup masukkan network tersebut agar kita bisa terhubung ke internet.
5. Sedangkan Gateway= 192.168.10.1, adalah ip gateway untuk terhubung ke internet
6. Klik Apply dan Ok

7. Untuk default route memiliki keterangan **AS**, karena dibuat manual oleh sang administrator, **A=Active** dan **S=static**

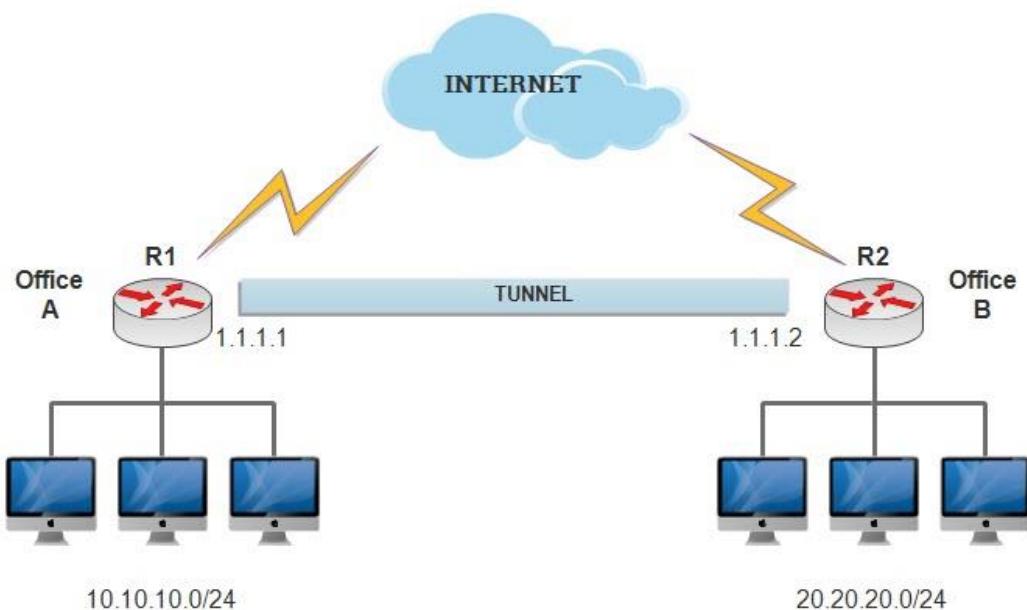
	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	192.168.10.1 reachable wlan1	1
DAC	192.168.10.0/24	wlan1 reachable	0

A - active, S - static

TUNNEL

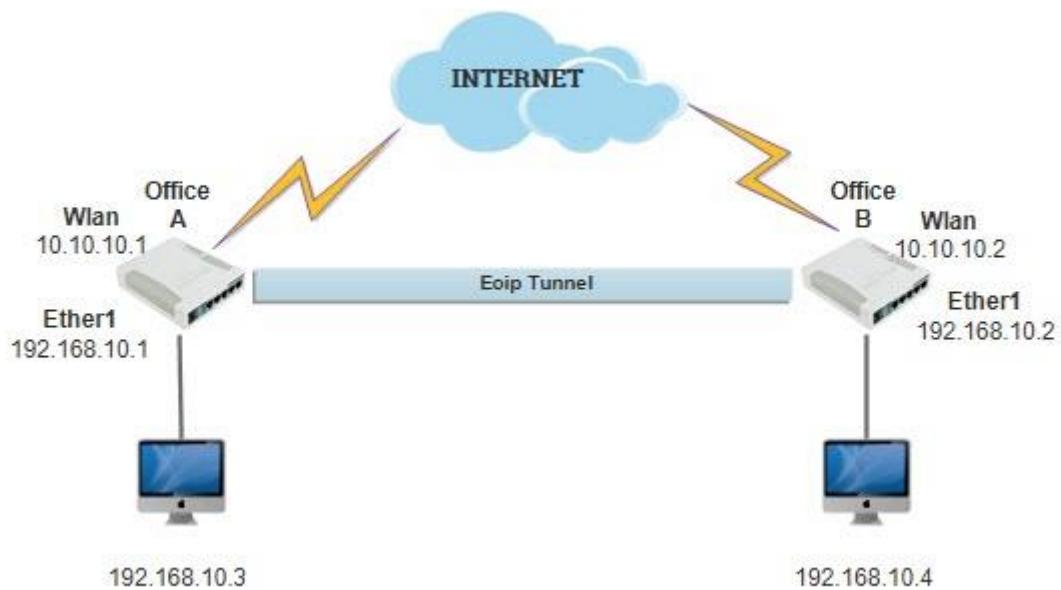
Bab 7. Tunnel

Setelah pada bab sebelumnya kita telah membahas mengenai bab Routing pada bab ini kita akan mengulas sedikit tentang tunnel, apa itu toh tunnel? Tunnel jika diterjemahkan ke bahasa indonesia artinya adalah **terowongan**, loh kok terowongan ? oke, kita akan bahas disini **Tunnel** adalah jalur khusus yang ada pada internet yang digunakan untuk menghubungkan 2 jaringan atau lebih. Atau secara singkatnya kita membuat jaringan private dalam internet



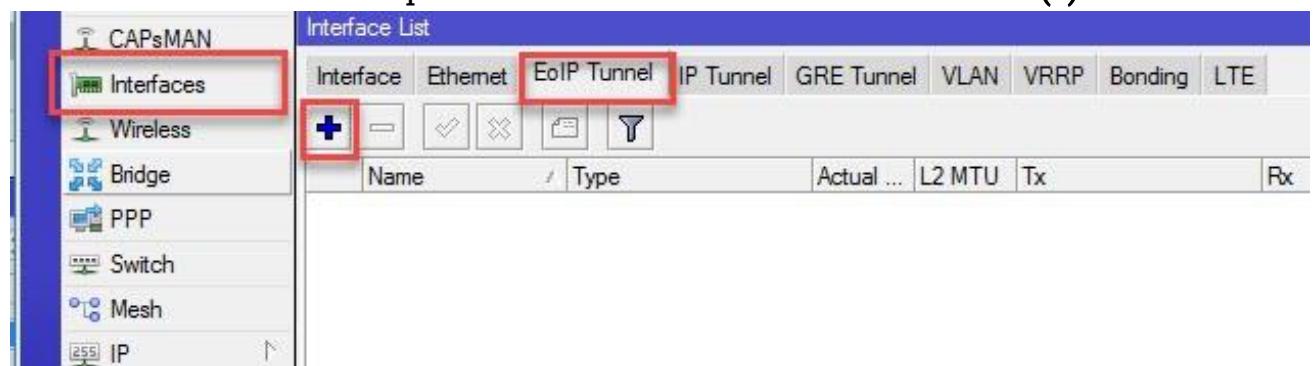
Lab 47. Konfigurasi EoIP Tunnel

EOIP Tunnel adalah program tunnel yang hanya ada pada perangkat mikrotik (Mikrotik Proprietary) yang digunakan untuk membangun network tunnel. EOIP tunnel tidak menggunakan enkripsi dalam pengiriman paket datanya, tidak disarankan menggunakan EOIP tunnel untuk transfer data yang memiliki keamanan yang tinggi. Oke langsung saja pada labnya biar tidak penasaran lagi, perhatikan topology berikut:



Untuk Konfigurasinya sebagai berikut

1. Konfigurasikan IP Address sesuai pada topology diatas
2. Hubungkan tiap tiap router ke Akses Point (internet), agar setiap pc nantinya bisa mengakses internet
3. Buat interface EoIP pada menu **Interface > EoIP Tunnel > Add (+)**



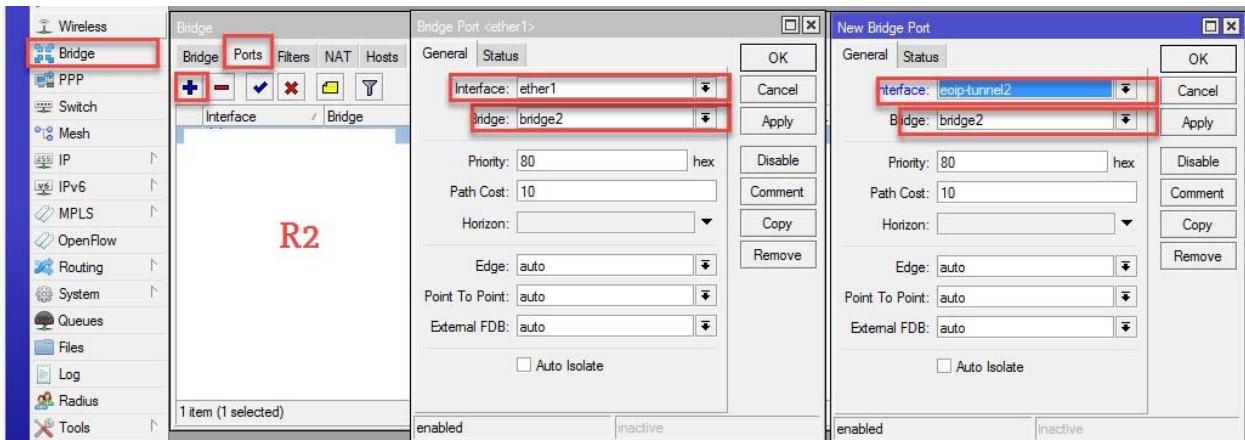
4. Untuk parameter yang dikonfigurasi pada eoip tunnel yaitu, **remote address = IP Address Publik lawan, Tunnel ID = ID antara router EoIP harus sama**, jangan lupa klik apply dan ok

R1

R2

5. Kemudian buat interface bridge dan tambahkan interface ether1 dan interface eoip-tunnel pada port bridge, jangan lupa klik apply dan ok

R1



6. Jangan lupa set ip pada masing masing laptop/pc, kemudian uji coba ping antar laptop dan router. Berikut contoh hasil ping dari pc router1 ke pc yang ada pada router 2

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

C:\Users\Fariz>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time=3ms TTL=64
Reply from 192.168.10.4: bytes=32 time=6ms TTL=64
Reply from 192.168.10.4: bytes=32 time=6ms TTL=64
Reply from 192.168.10.4: bytes=32 time=10ms TTL=64

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 6ms

C:\Users\Fariz>
```

7. Hasil ping dari pc router2 ke pc yang ada pada router1

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

C:\Users\Fariz>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=8ms TTL=64

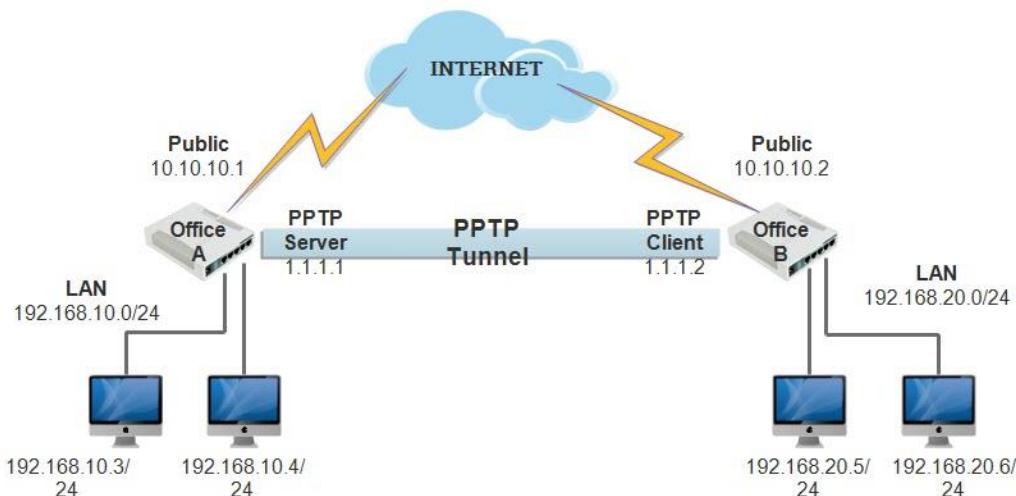
Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms

C:\Users\Fariz>
```

Lab 48. Konfigurasi PPTP Tunnel (Skenario 1)

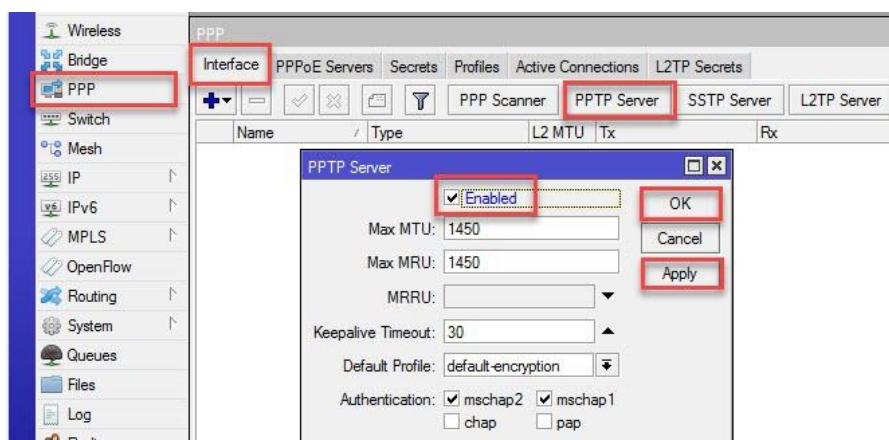
Melanjutkan pembahasan mengenai tunnel, pada lab sebelumnya kita sudah membahas mengenai EoIP tunnel, pada pembahasan kali ini kita akan membahas mengenai PPTP, PPTP (Point To Point Tunneling Protocol) adalah salah satu protocol yang digunakan untuk membuat jaringan tunnel VPN, sedangkan VPN itu sendiri apa?

VPN (Virtual Private Network) adalah metode untuk menghubungkan jaringan lokal melalui internet dengan cara membuat tunnel didalam internet. PPTP ini banyak digunakan, karena hampir disemua OS dapat menjalankan PPTP client, Untuk dapat menjalankan PPTP Server, sebelumnya kita harus mengkonfigurasi terlebih dahulu PPP Secret dan PPP Profiles, biar tidak penasaran lagi perhatikan topologi berikut:

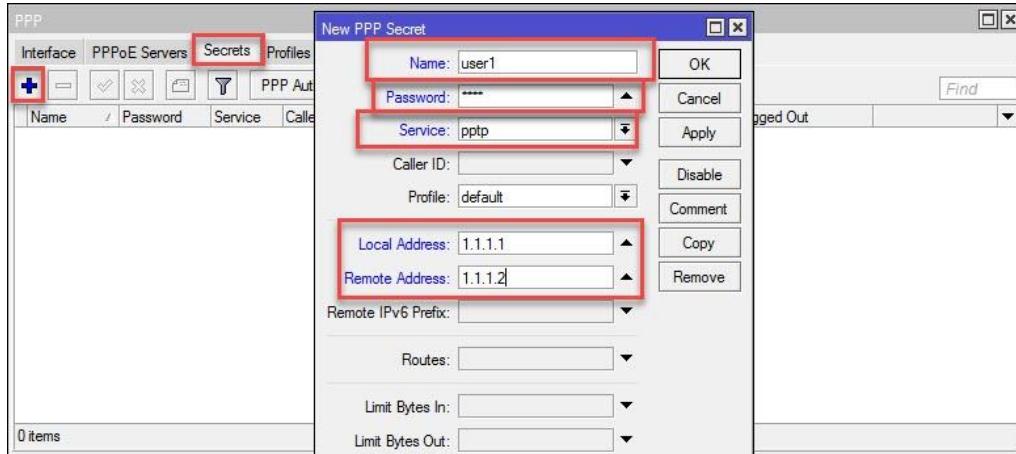


Pada Skenario lab ini, kita akan menghubungkan antara kantor A (PPTP Server) dan Kantor B (PPTP Client) menggunakan PPTP Tunnel. Konfigurasi berikut adalah konfigurasi dari PPTP Server.

1. Sebelumnya Aktifkan Telebih dahulu **PPTP Server** pada rb Kantor A di menu **PPP > Interface > PPTP Server** > Centang () pada kotak enable, klik apply dan ok

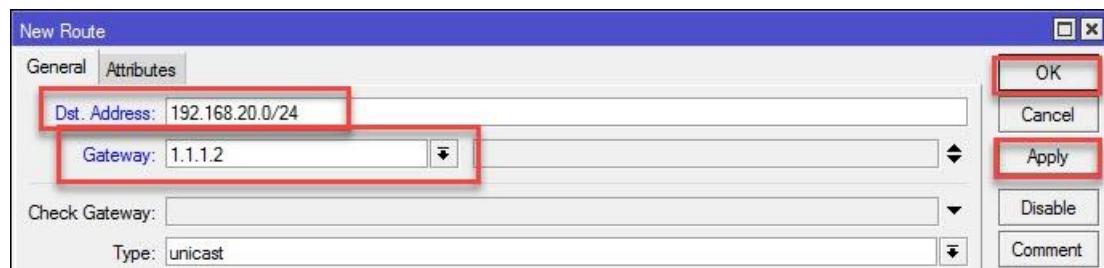


2. Kemudian masuk pada submenu **Secret** pada PPP Menu, untuk membuat profile username, password dll yang digunakan untuk PPTP Client



Keterangan:

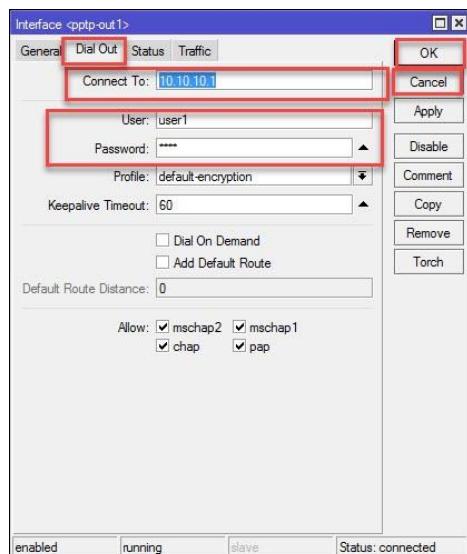
- **Name:** username yang digunakan client
 - **Password:** password dari username tersebut
 - **Service:** Layanan tunnel yang digunakan untuk ppp secret ini, karena kita menggunakan PPTP maka pilih PPTP
 - **Local Address:** IP yang digunakan router untuk komunikasi point to point ke client
 - **Remote Address:** IP point to point yang diberikan ke client
3. Karena dalam topology, jaringan LAN kantor A dan Kantor B berbeda maka kita tambahkan static route agar kedua jaringan LAN tersebut bisa terhubung



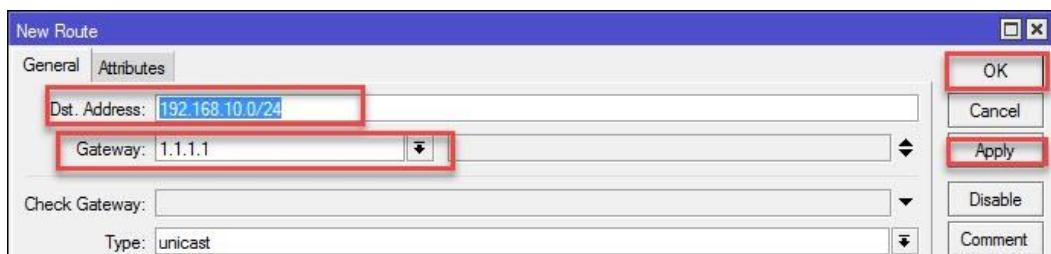
4. Kemudian Konfigurasikan pada router kantor B, kita konfigurasikan PPTP-Client dengan menambahkan interface pptp-client pada menu **Interface > (+) > PPTP-Client**



5. Kemudian masukkan IP (publik) dari router kantor 1, username & password pada submenu Dial Out



6. Lalu konfigurasikan static route agar bisa terhubung ke jaringan lokal router kantor A



7. Kemudian konfigurasikan IP address pada masing masing pc/laptop per kantor, sesuaikan konfigurasi dengan topologi diatas, lalu ping antar pc/laptop dari kantor B ke Kantor A,

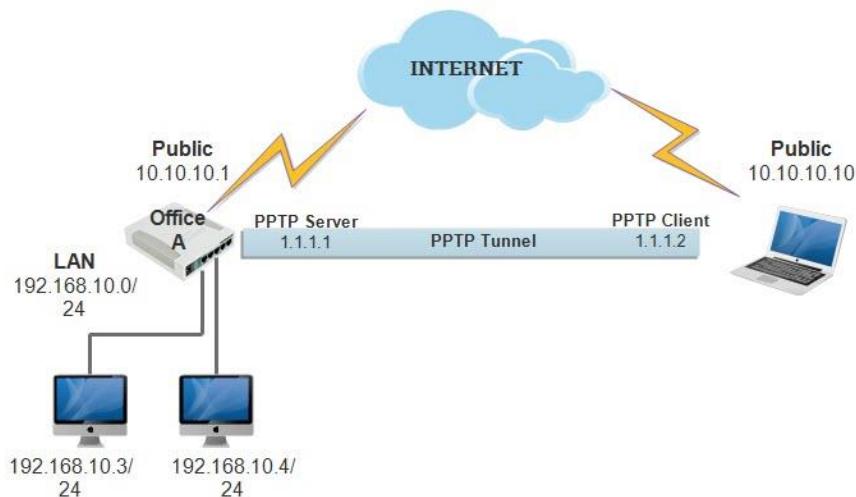
```
Windows Command Prompt  
Microsoft Windows [Version 10.0.10586]  
(c) 2015 Microsoft Corporation. All rights reserved.  
C:\Users\Fariz>ping 192.168.10.3  
Pinging 192.168.10.3 with 32 bytes of data:  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=8ms TTL=64  
  
Ping statistics for 192.168.10.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 8ms, Average = 2ms  
  
C:\Users\Fariz>
```

8. Hasil ping dari pc kantor B ke pc kantor A

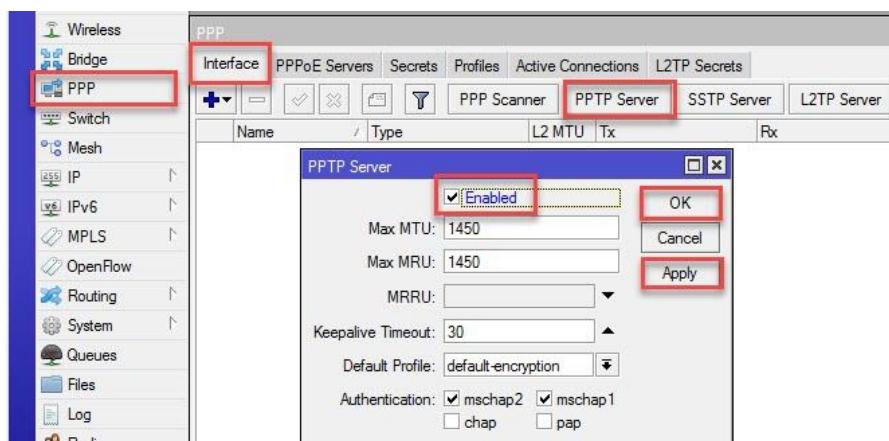
```
Windows Command Prompt  
Microsoft Windows [Version 10.0.10586]  
(c) 2015 Microsoft Corporation. All rights reserved.  
C:\Users\Fariz>ping 192.168.20.6  
Pinging 192.168.20.6 with 32 bytes of data:  
Reply from 192.168.20.6: bytes=32 time=1ms TTL=63  
Reply from 192.168.20.6: bytes=32 time=2ms TTL=63  
Reply from 192.168.20.6: bytes=32 time=1ms TTL=63  
Reply from 192.168.20.6: bytes=32 time=25ms TTL=63  
  
Ping statistics for 192.168.20.6:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 25ms, Average = 7ms  
  
C:\Users\Fariz>
```

Lab 49. Konfigurasi PPTP Tunnel (Skenario 2)

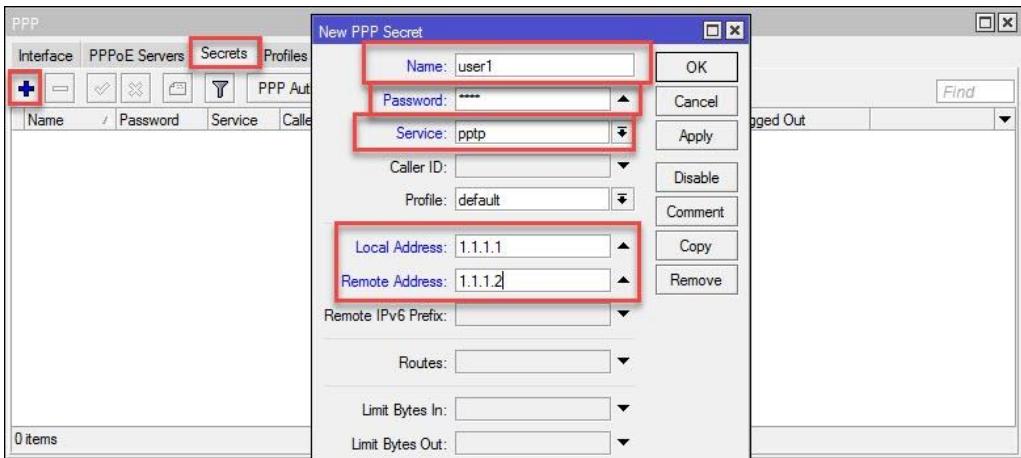
Pada lab sebelumnya kita sudah mengkonfigurasi dan menghubungkan 2 kantor dengan 2 RB pada masing masing kantor, pada lab berikut kita akan menghubungkan Kantor A dengan Laptop/windows (tanpa RB), untuk konfigurasinya kita bisa menggunakan konfigurasinya pada Lab sebelumnya,



1. Sebelumnya Aktifkan Terlebih dahulu **PPTP Server** pada rb Kantor A di menu **PPP > Interface > PPTP Server** > Centang () pada kotak enable, klik apply dan ok

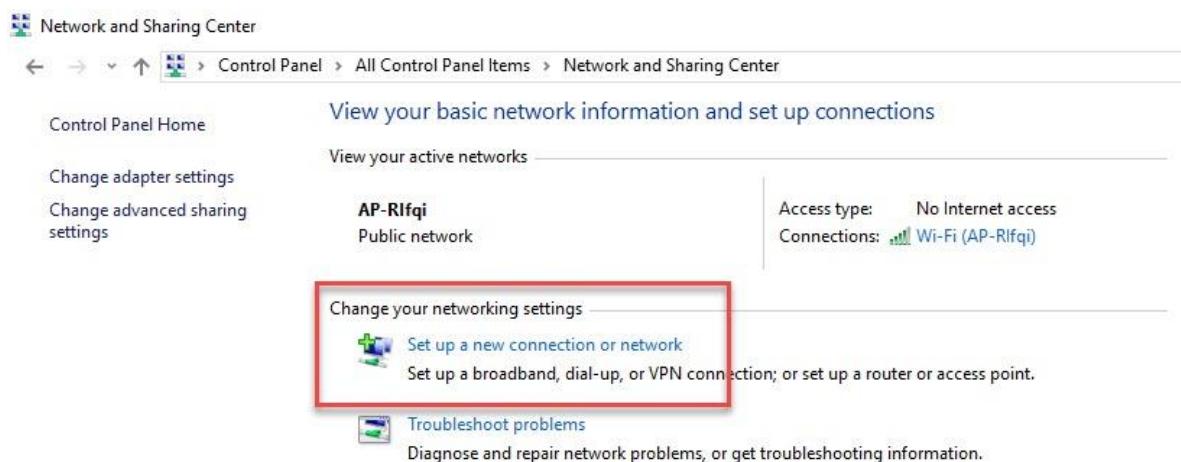


2. Kemudian masuk pada submenu **Secret** pada **PPP** Menu, untuk membuat profile username, password dll yang digunakan untuk PPTP Client

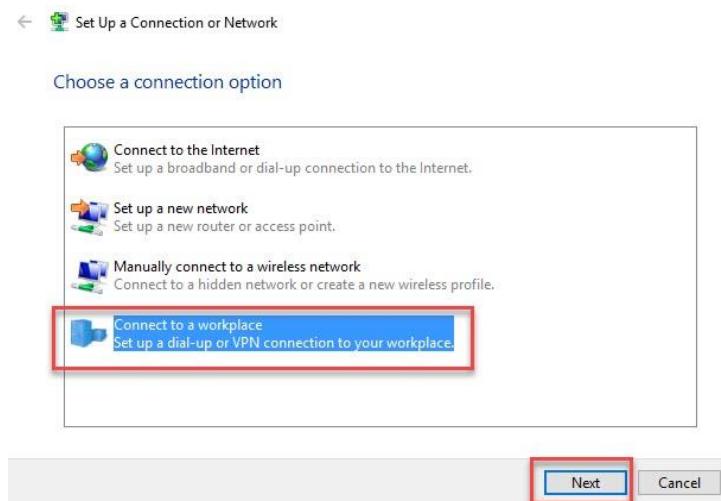


Keterangan:

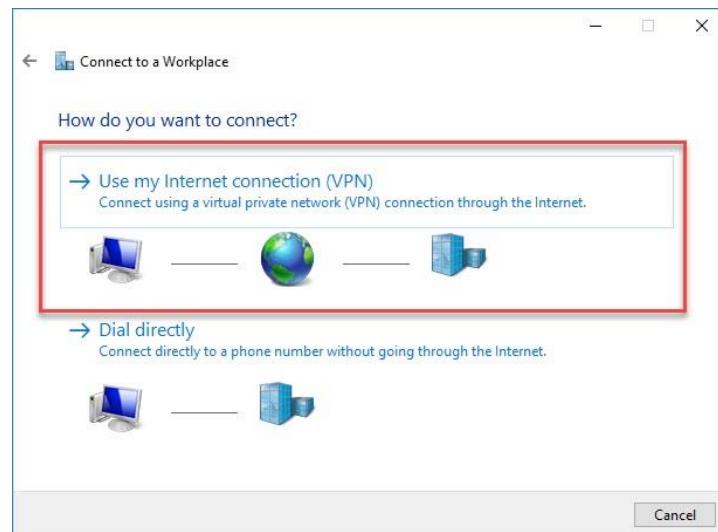
- **Name:** username yang digunakan client
 - **Password:** password dari username tersebut
 - **Service:** Layanan tunnel yang digunakan untuk ppp secret ini, karena kita menggunakan PPTP maka pilih PPTP
 - **Local Address:** IP yang digunakan router untuk komunikasi point to point ke client
 - **Remote Address:** IP point to point yang diberikan ke client
3. Kemudian konfigurasi IP pada laptop sesui dengan topology diatas, kemudian buat VPN Profile Connection pada windows, masuk pada **Control Panel > Network and Sharing center**, kemudian pilih yang **Setup a new connection or network**



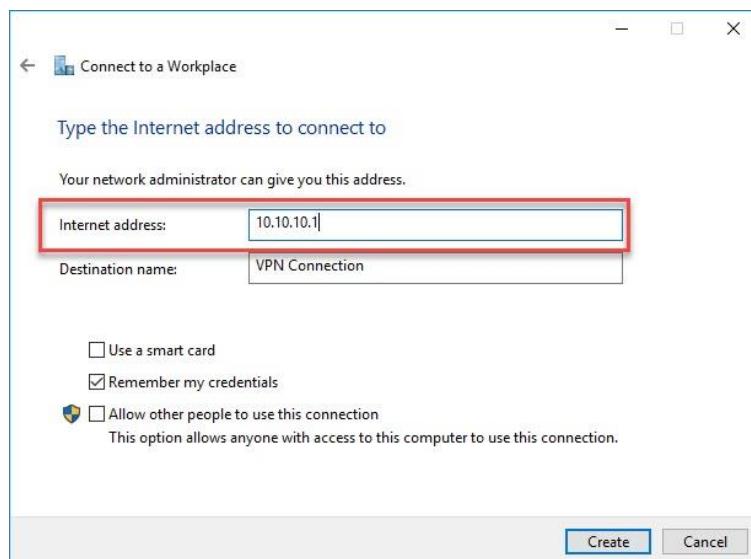
4. Kemudian Pilih Connect to a workplace, klik Next



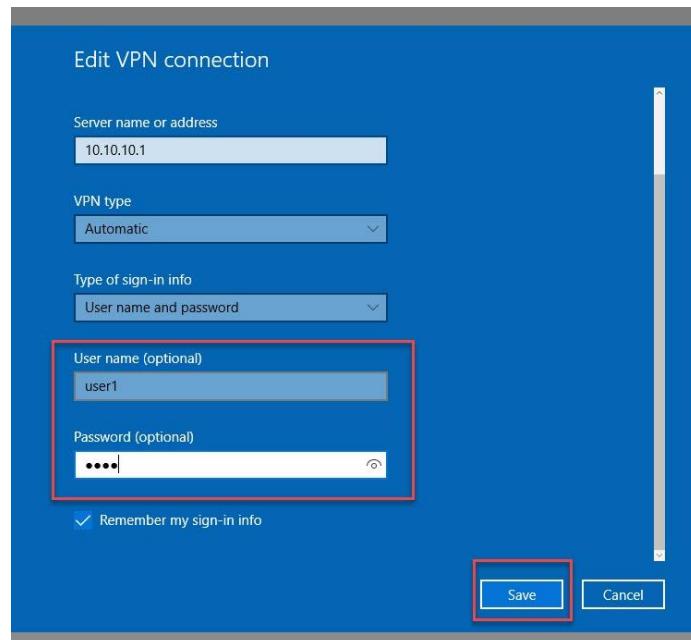
5. Lalu pilih Use my Internet connection (VPN)



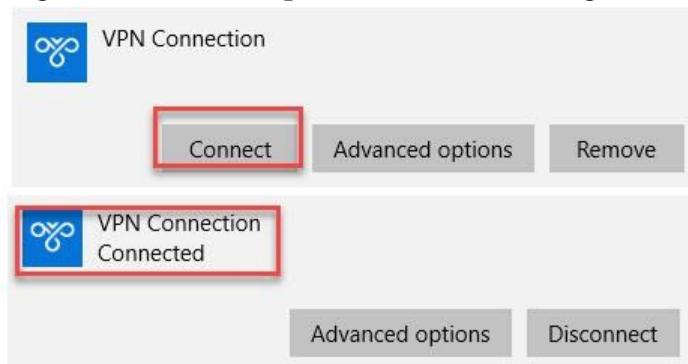
6. Kemudian isikan alamat ip publik dari PPTP Server Router Kantor A



7. Kemudian isikan Username dan Password PPTP-Server yang tadi dibuat



8. Klik Connect, tunggu sebentar sampai muncul keterangan Connected



9. Kemudian Tes ping ke ip salah satu pc yang ada pada jaringan lokal router kantor A

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

C:\Users\Fariz>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms

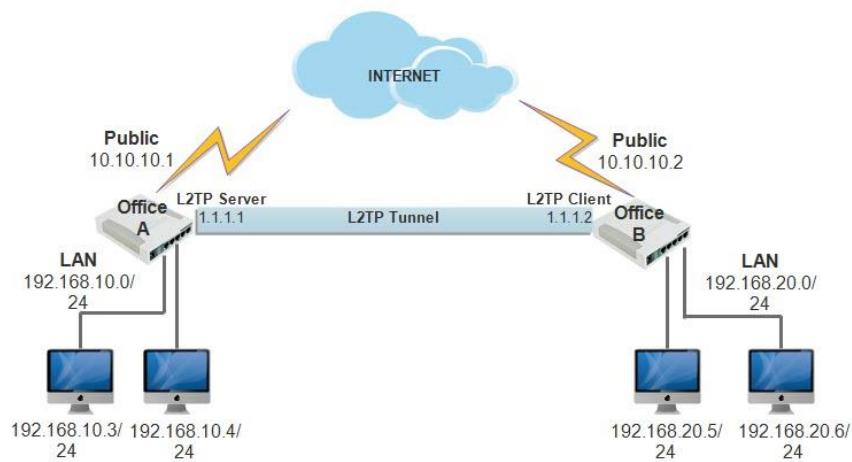
C:\Users\Fariz>
```

10. Done, selesai

Lab 50. Konfigurasi L2TP Tunnel (Skenario 1)

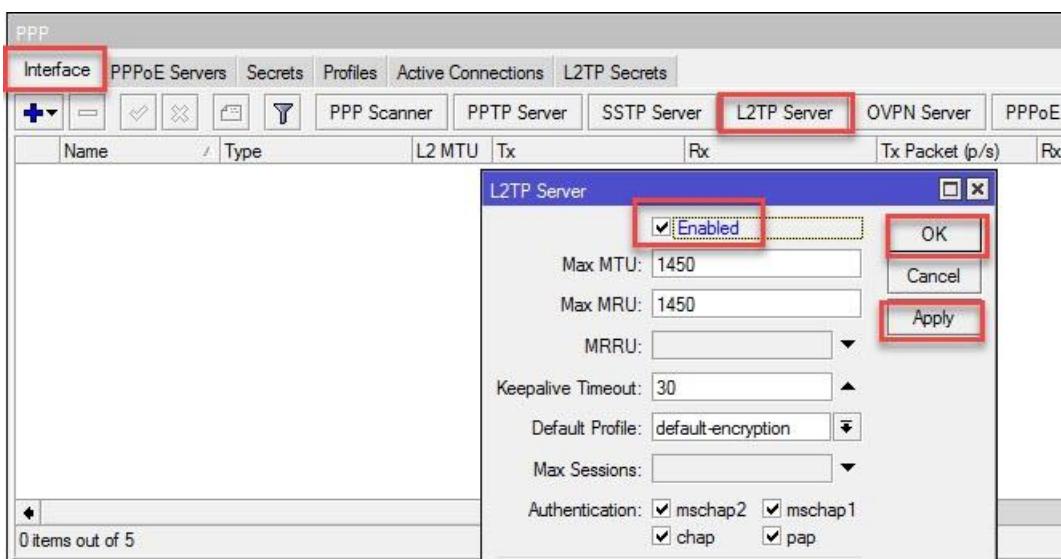
L2TP (Layer 2 Tunneling Protocol) adalah jenis protokol tunneling & encapsulation yang digunakan untuk tunnel, perbedaan dengan tunnel lainnya L2TP ini mendukung nonTCP/IP protocol (frame relay, ATM & dll), jadi bisa berkerja tanpa menggunakan protocol TCP/IP. Pada L2TP ini juga tidak adanya fitur enkripsi pada paket yang ditransferkan, untuk enkripsi biasanya L2TP dikombinasikan dengan Ipsec

Untuk konfigurasinya hampir sama dengan konfigurasi pada PPTP-Server, bedanya hanya layanan yang digunakannya yaitu L2TP, perhatikan topology berikut:

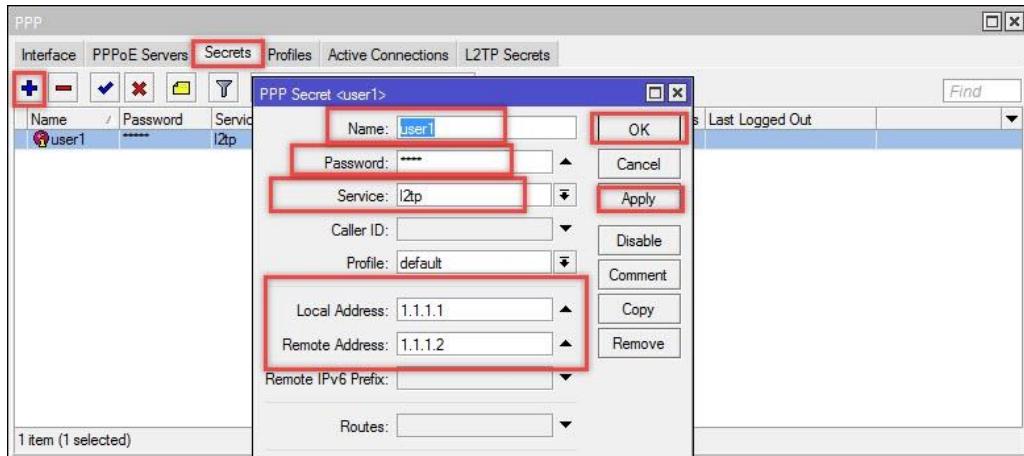


Pada Skenario lab ini, kita akan menghubungkan antara kantor A (L2TP Server) dan Kantor B (L2TP Client) menggunakan PPTP Tunnel. Konfigurasi berikut adalah konfigurasi dari **L2TP Server**

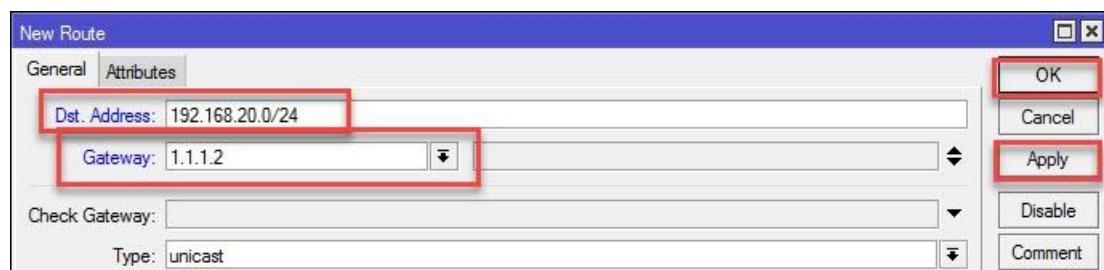
1. Sebelumnya Aktifkan Terlebih dahulu **L2TP Server** pada rb Kantor A di menu PPP > Interface > L2TP Server > Centang (✓) pada kotak enable, klik apply dan ok



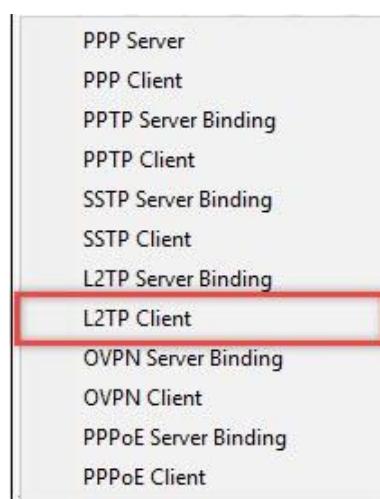
2. Kemudian masuk pada submenu **Secret** pada PPP Menu, untuk membuat profile username, password dll yang digunakan untuk PPTP Client



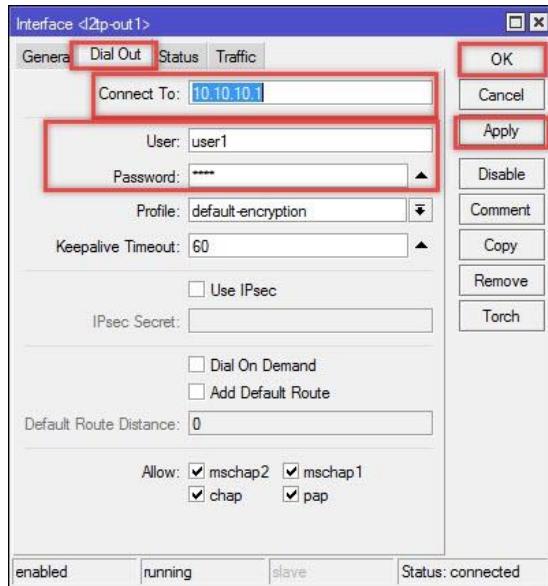
3. Untuk keterangannya bisa dibaca pada bab PPTP, karena isi keterangannya sama
 4. Karena dalam topology, jaringan LAN kantor A dan Kantor B berbeda maka kita tambahkan static route agar kedua jaringan LAN tersebut bisa terhubung



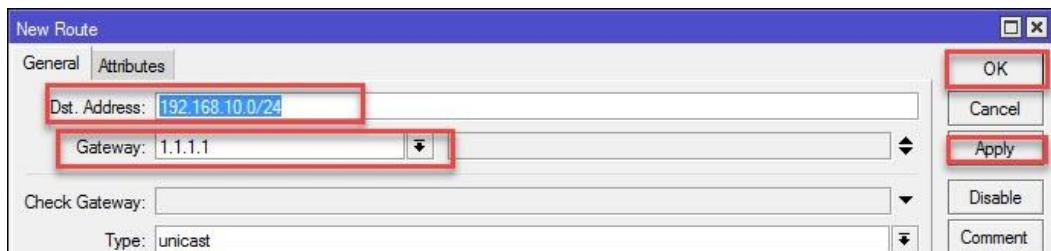
5. Kemudian Konfigurasikan pada router kantor B, kita konfigurasikan L2TP-Client dengan menambahkan interface pptp-client pada menu **Interface > (+) > L2TP-Client**



6. Kemudian masukkan IP (publik) dari router kantor 1, username & password pada submenu Dial Out



7. Lalu konfigurasikan static route agar bisa terhubung ke jaringan lokal router kantor A



8. Kemudian konfigurasikan IP address pada masing masing pc/laptop per kantor, sesuaikan konfigurasi dengan topologi diatas, lalu ping antar pc/laptop dari kantor B ke Kantor A,

```
C:\ Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Fariz> ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64
Reply from 192.168.10.3: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms

C:\Users\Fariz>
```

9. Hasil ping dari pc kantor B ke pc kantor A

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

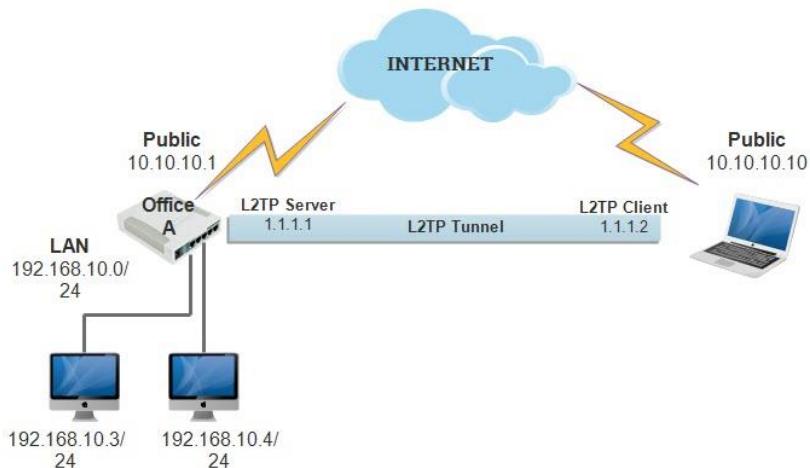
C:\Users\Fariz>ping 192.168.20.6

Pinging 192.168.20.6 with 32 bytes of data:
Reply from 192.168.20.6: bytes=32 time=1ms TTL=63
Reply from 192.168.20.6: bytes=32 time=2ms TTL=63
Reply from 192.168.20.6: bytes=32 time=1ms TTL=63
Reply from 192.168.20.6: bytes=32 time=25ms TTL=63

Ping statistics for 192.168.20.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 25ms, Average = 7ms

C:\Users\Fariz>
```

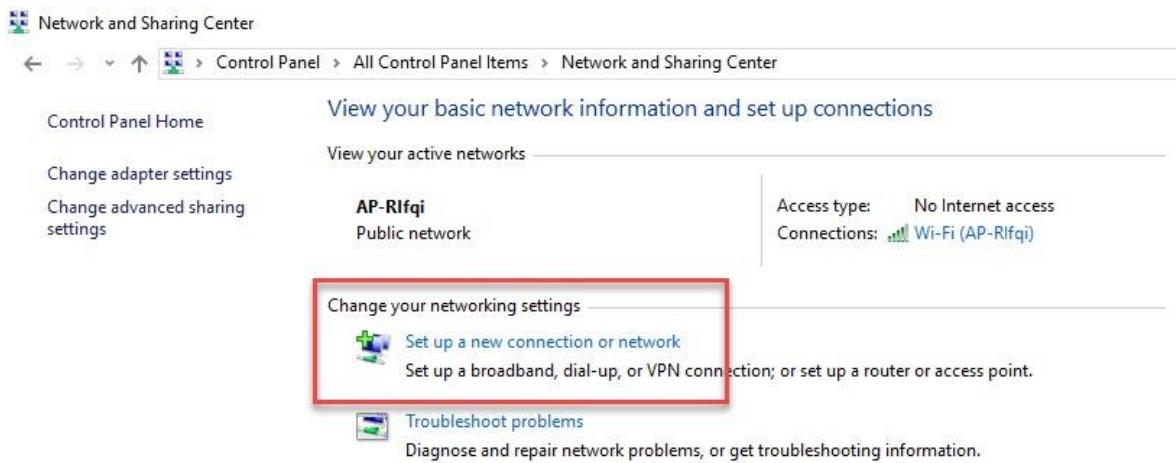
Lab 51. Konfigurasi L2TP Tunnel (Skenario 2)



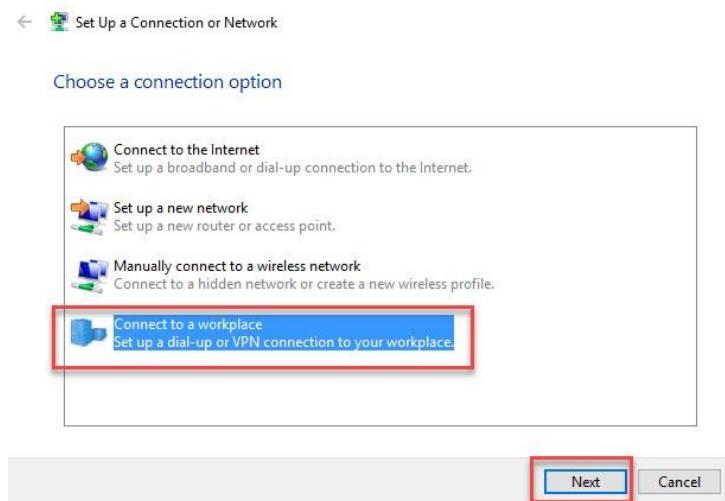
Pada lab sebelumnya kita sudah mengkonfigurasi dan menghubungkan 2 kantor dengan 2 RB pada masing masing kantor, pada lab berikut kita akan menghubungkan Kantor A dengan Laptop/windows (tanpa RB), untuk konfigurasinya kita bisa menggunakan konfigurasi pada Lab sebelumnya, disini saya hanya akan membahas bagaimana konfigurasi yang ada pada sisi client (windows).

Untuk konfigurasi L2TP-client pada windows sebagai berikut:

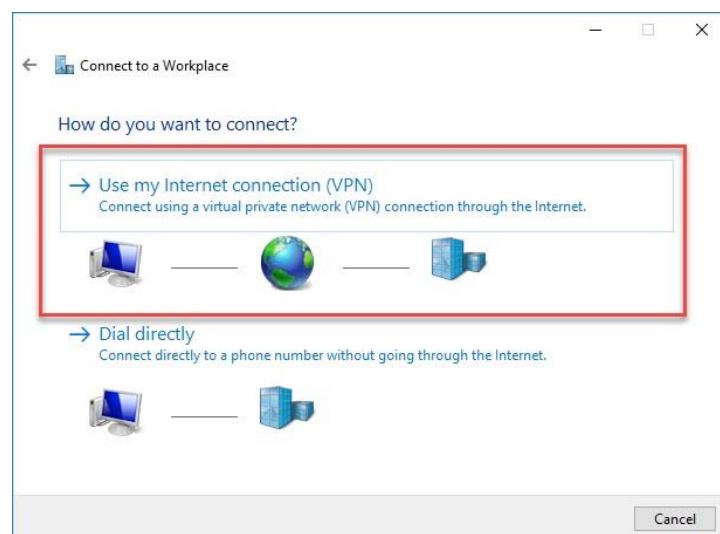
1. Konfigurasikan IP Address pada laptop sesuai dengan topology diatas, kemudian buat VPN Profile Connection pada windows, masuk pada **Control Panel > Network and Sharing center**, kemudian pilih yang **Setup a new connection or network**



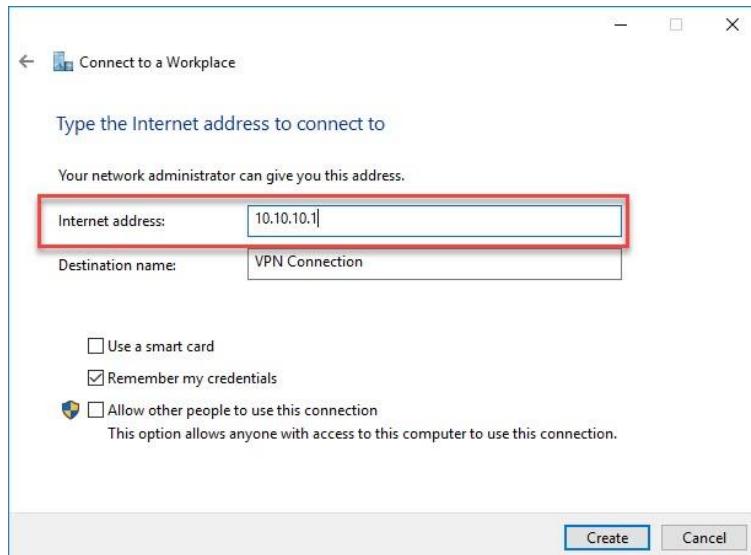
2. Kemudian Pilih Connect to a workplace, klik Next



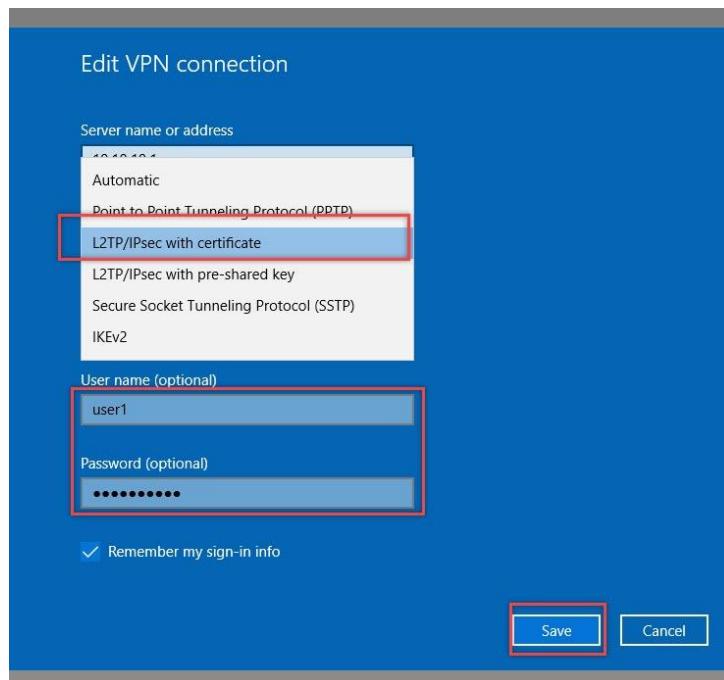
3. Lalu pilih Use my Internet connection (VPN)



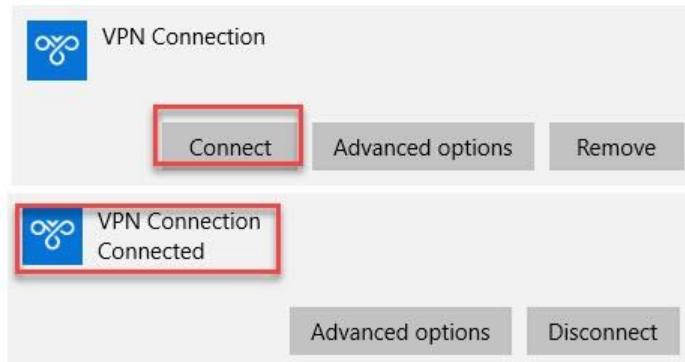
4. Kemudian isikan alamat ip publik dari PPTP Server Router Kantor A



5. Kemudian isikan Username dan Password L2TP-Server yang tadi dibuat, pilih L2TP/Ipsec with certificate, jangan lupa klik save



10. Klik Connect, tunggu sebentar sampai muncul keterangan Connected



11. Kemudian Tes ping ke ip salah satu pc yang ada pada jaringan lokal router kantor A

```
C:\> Command Prompt  
Microsoft Windows [Version 10.0.10586]  
(c) 2015 Microsoft Corporation. All rights reserved.  
C:\Users\Fariz>ping 192.168.10.3  
  
Pinging 192.168.10.3 with 32 bytes of data:  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=1ms TTL=64  
Reply from 192.168.10.3: bytes=32 time=8ms TTL=64  
  
Ping statistics for 192.168.10.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 8ms, Average = 2ms  
  
C:\Users\Fariz>
```

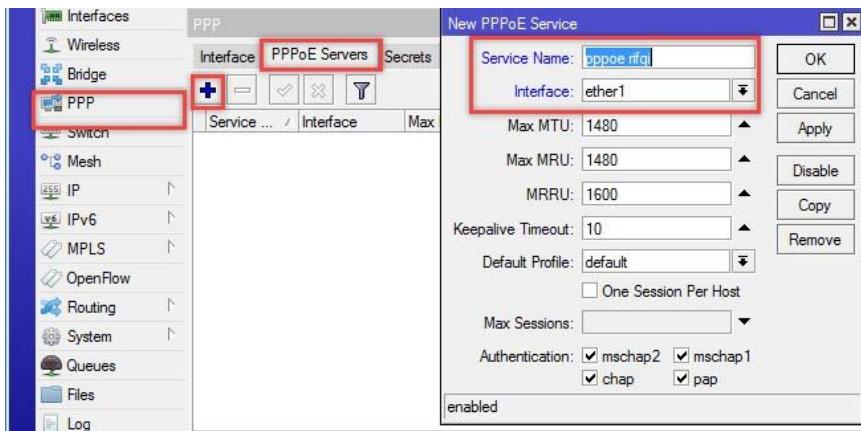
Lab 52. Konfigurasi PPPoE Tunnel (Skenario 1)

Pada lab berikut kita akan membahas mengenai PPPoE, apa lagi itu PPPoE? PPPoE adalah protokol tunneling yang digunakan untuk mengenkapsulasi paket PPP pada frame ethernet, gampangnya paket data yang ditransfer pada PPPoE akan mengalami proses engkapsulasi pada saat data ditransfer. PPPoE ini biasanya dipakai pada layanan ADSL, untuk menghubungkan modem ADSL (kabel modem telfon) pada jaringan Ethernet (TCP/IP),

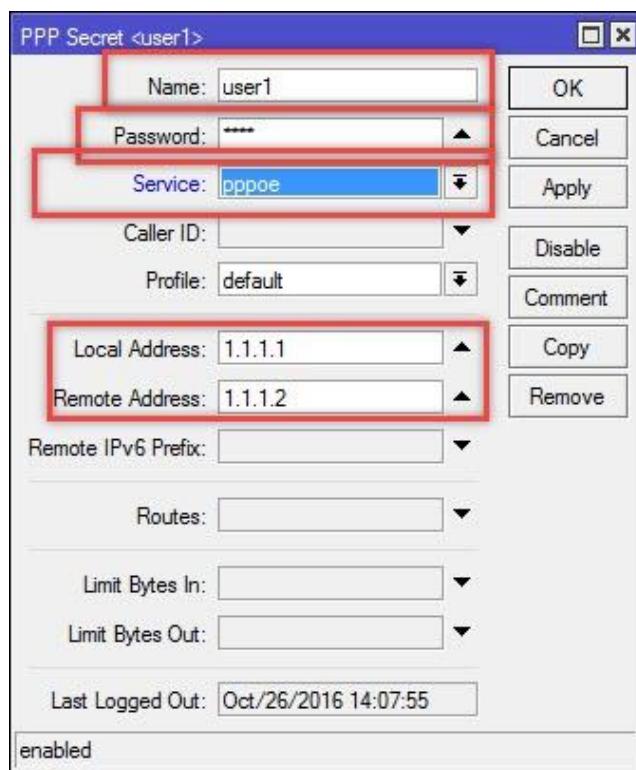


Untuk topologynya cukup mudah yaitu kita hanya menggunakan 2 Routerboard saja, untuk konfigurasinya sebagai berikut:

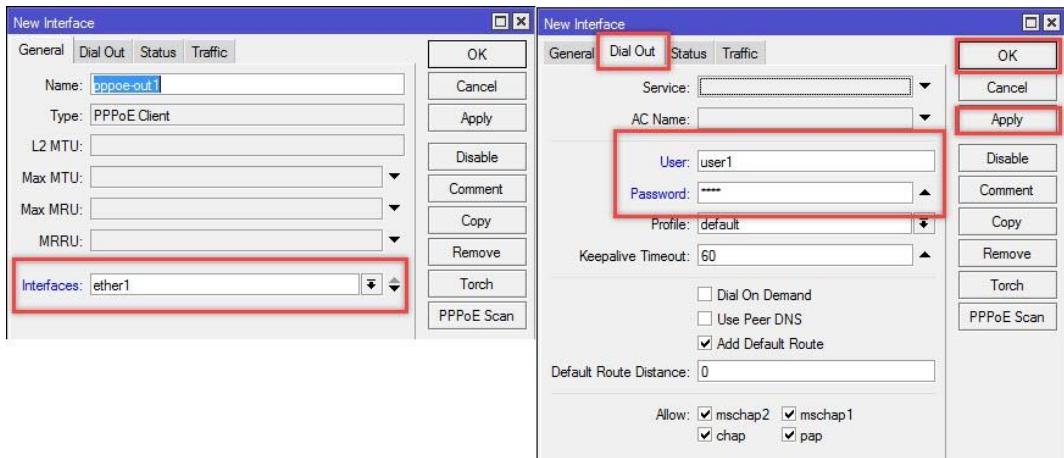
1. Pertama kita harus mengaktifkan terlebih dahulu layanan PPPoE Server pada Router R1, pada menu **PPP > PPPoE Servers > add (+)**, kemudian pada bagian interfaces kita pilih interface yang terhubung ke router R2



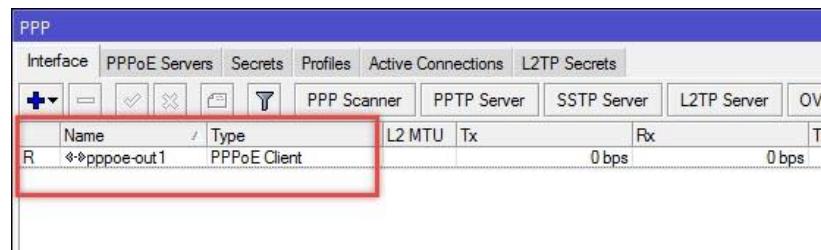
2. Kemudian masuk pada submenu **Secret** pada **PPP** Menu, untuk membuat profile username, password dll yang digunakan untuk PPPoE Client, pada Service pilih **pppoe**, klik tombol (+) untuk menambahkan profile



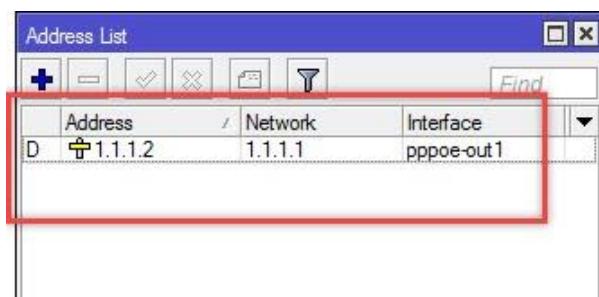
3. Kemudian Konfigurasikan pada router kantor B, kita konfigurasikan **PPPoE-Client** dengan menambahkan interface **pppoe-client** pada menu **Interface > (+) > PPPoE-Client**



4. Kemudian check koneksi apakah sudah **connected** atau belum, jika muncul keterangan seperti dibawah berikut, tandanya sudah **connected**



5. Bisa kita check juga apakah pppoe-client yang tadi sudah terhubung mendapatkan ip dari pppoe-server atau tidak



6. Done, Selesai

QoS

Bab 8. QoS

QoS (Quality of Service) adalah metode untuk mengatur bandwidth yang bertujuan agar tidak terjadinya monopoly penggunaan bandwidth sehingga semua client atau client yang kita prioritaskan bisa mendapatkan jatah bandwidth masing-masing.

Pada router OS QoS dikenal dengan Bandwidth Management, untuk paket yang digunakan adalah **Queue**. Terdapat 2 macam metode yang digunakan pada Queue yaitu:

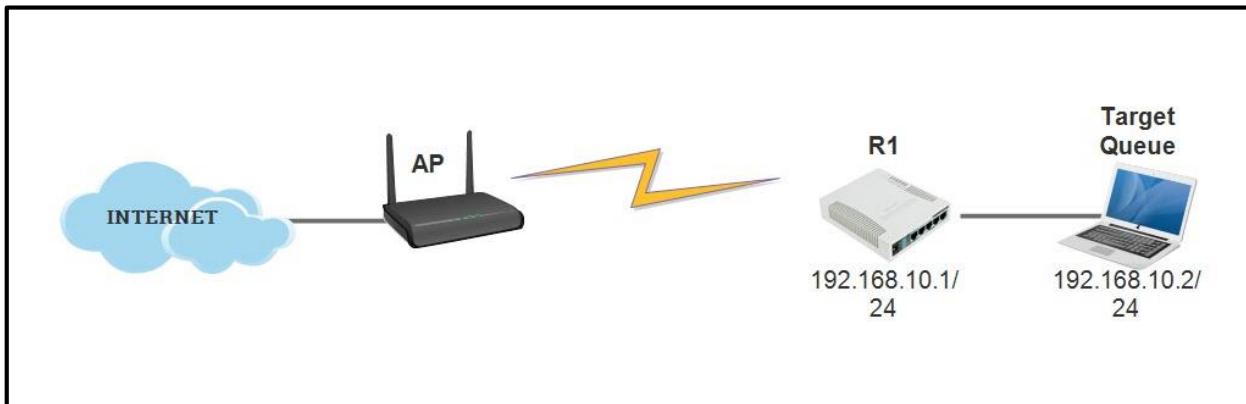
1. **Simple Queue** : merupakan jenis bandwidth management yang mudah dan simple dalam konfigurasinya. Simple Queue digunakan untuk management trafik upload & download pada masing-masing client. Simple Queue ini bisa diimplementasikan pada jaringan skala kecil dan menengah
2. **Queue Tree** : merupakan jenis bandwidth management yang mengelompokkan bandwidth management ke dalam grup /parent sehingga nanti akan terlihat seperti sebuah hierarki. Untuk fungsinya hampir sama dengan Simple Queue namun untuk Queue tree ini kita harus mengaktifkan mangle untuk traffic paket pada menu firewall, sehingga kita dapat melakukan limitasi/prioritas pada traffic paket apapun semisal browsing, streaming, game, email dan lain-lain.

Pada saat menerapkan Queue pada suatu jaringan, ada 2 jenis batasan alokasi bandwidth (**rate limit**), yaitu:

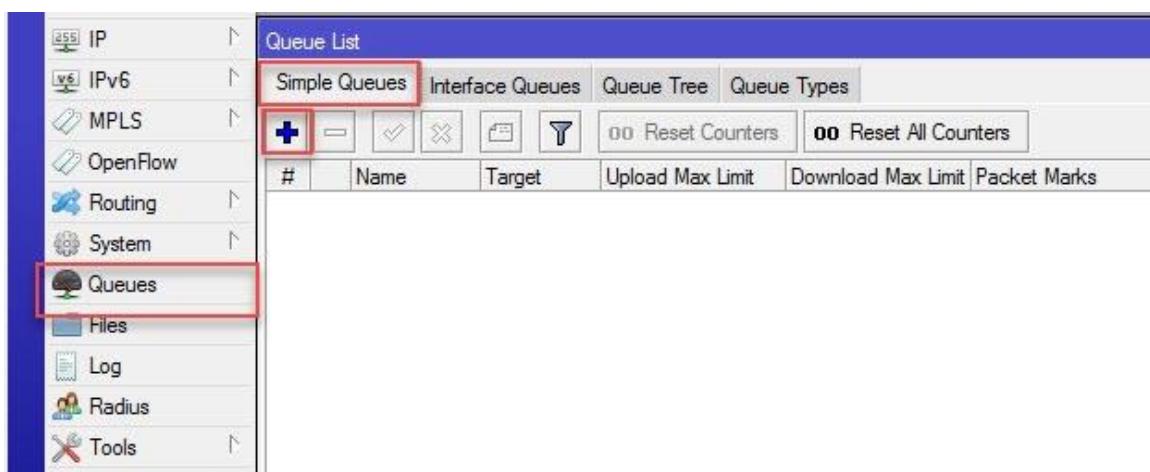
1. **CIR (Committed Information Rate)**: alokasi bandwidth pada suatu keadaan terburuk dimana client akan mendapatkan bandwidth sesuai dengan "limit-at" (dengan asumsi bandwidth yang tersedia cukup untuk mendapatkan CIR pada semua client)
2. **MIR (Maximal Information Rate)**: alokasi bandwidth maksimum dimana client bisa mendapatkan bandwidth tambahan sesuai dengan "max-limit". MIR bisa berjalan jika masih terdapat sisa bandwidth setelah semua client mencapai "limit-at"

Lab 53. Konfigurasi Simple Queue

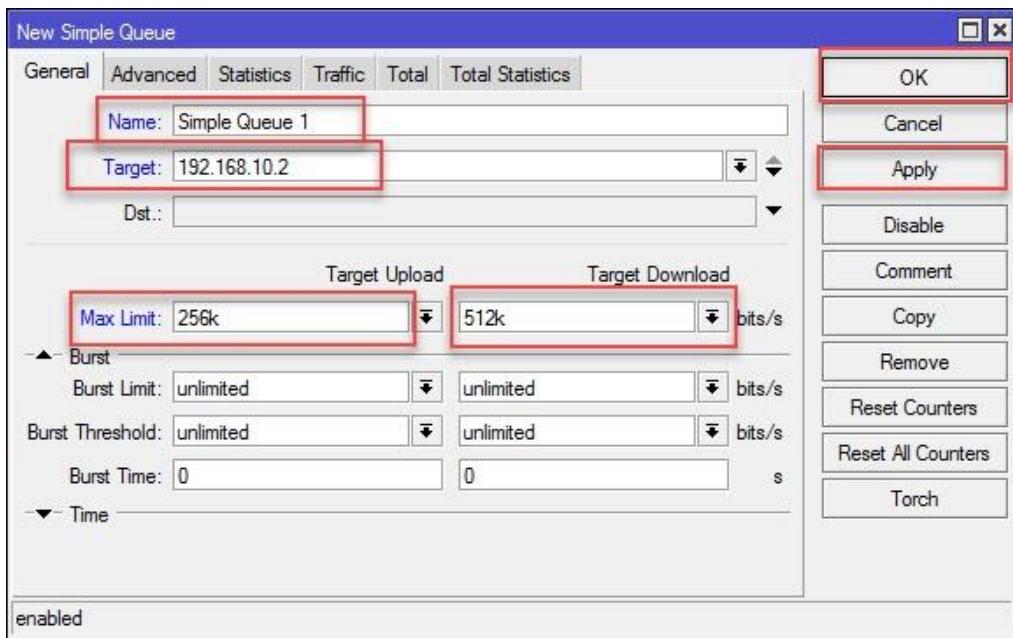
Tadi sudah dijelaskan tentang overview dari QoS dan Queue, simple queue ini bisa digunakan untuk bandwidth management pada (wireless access list, ethernet, ppp secret, dan hotspot user) untuk kali ini kita langsung saja uji coba lab tentang konfigurasi Simple Queue pada mikrotik, perhatikan topology berikut:



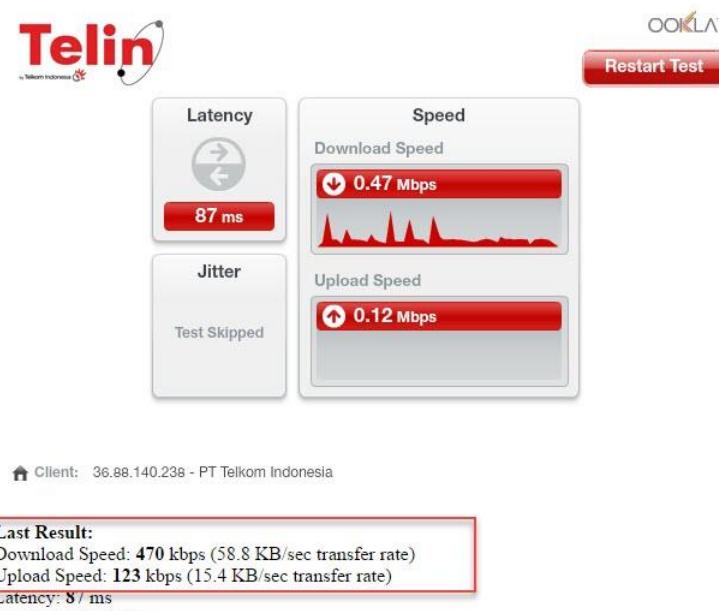
1. Pertama koneksi laptop ke internet melalui router yang terhubung ke Wifi/AP, untuk konfigurasinya bisa dibaca pada lab lab sebelumnya
2. Konfigurasi ini, kita akan membatasi koneksi laptop pada IP 192.168.10.2/24 dengan bandwidth **Download=512kb** dan **Upload=256kb**
3. Untuk konfigurasinya masuk pada menu Queue > Simple Queue > add (+)



4. Untuk tab General, isikan Name: Simple Queue 1, Target=192.168.10.2 (IP Laptop), lalu Max limit (target upload)=256k dan Max limit (target download)=512k, jangan lupa klik apply dan ok



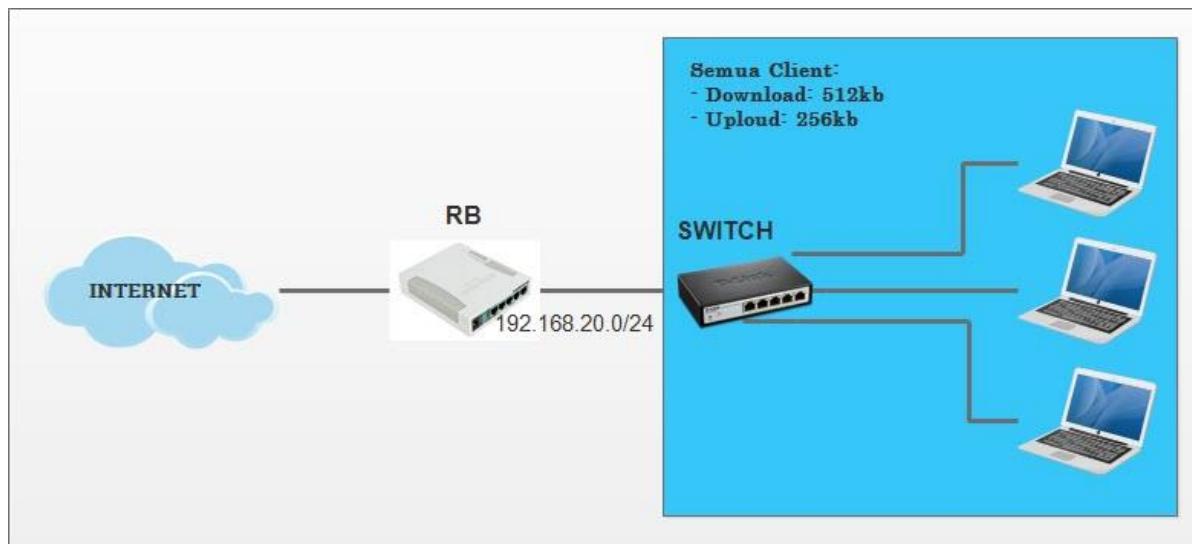
5. Kemudian uji coba speedtest pada situs <http://speedtest.telin.co.id/>



6. Terlihat bahwa traffic upload dan download tidak melebihi batas target yang tadi telah dikonfigurasikan

Lab 54. Konfigurasi Simple Queue with PCQ

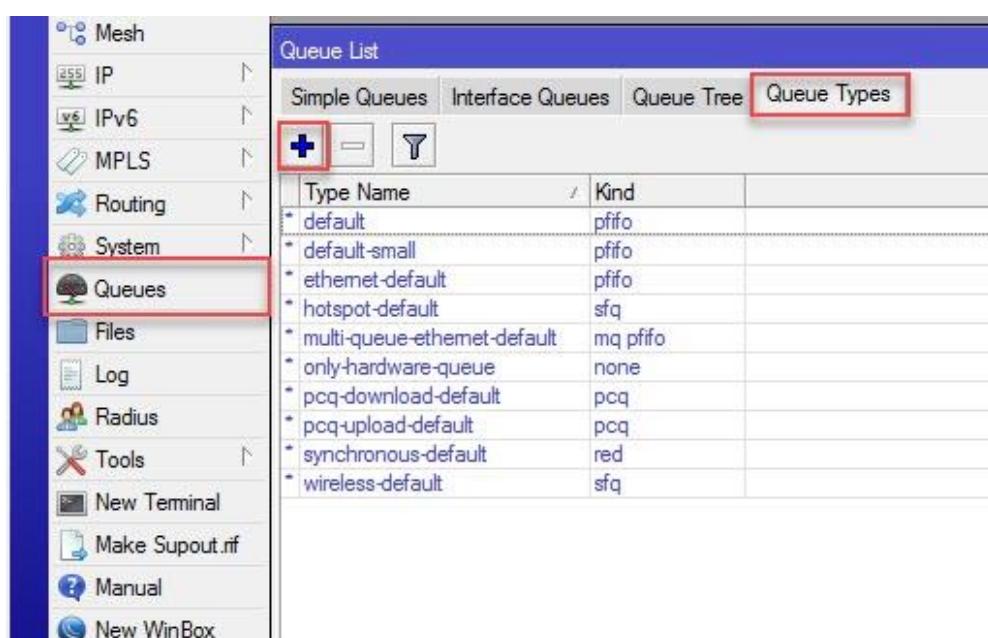
PCQ merupakan suatu metode alokasi bandwidth dengan memberikan bandwidth sama kesemua client yang ada pada suatu jaringan serta membagi total bandwidth yang ada, gambarannya perhatikan topology berikut:



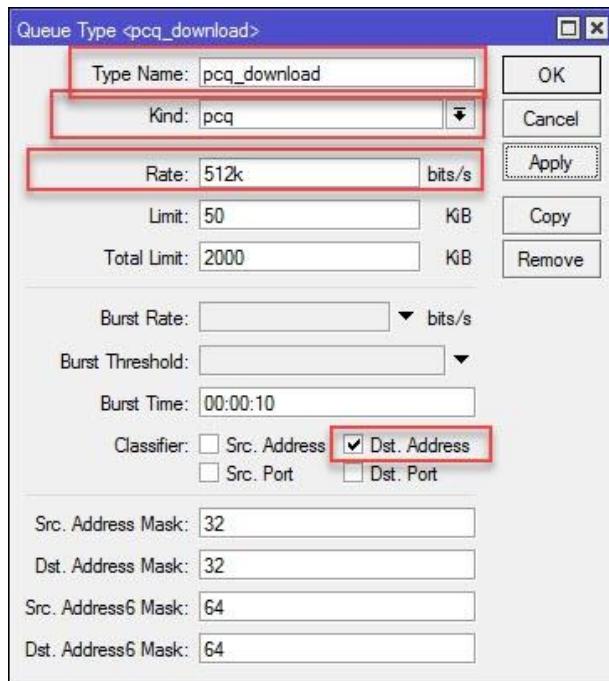
Jadi nantinya semua client akan mendapatkan bandwidth Download= 512kb dan Upload= 256kb, metode ini akan membagikan bandwidth merata ke semua client yang aktif. PCQ ini sangat ideal jika kita kesulitan dalam membagi rata bandwidth ke klient.

Untuk konfigurasinya sebagai berikut:

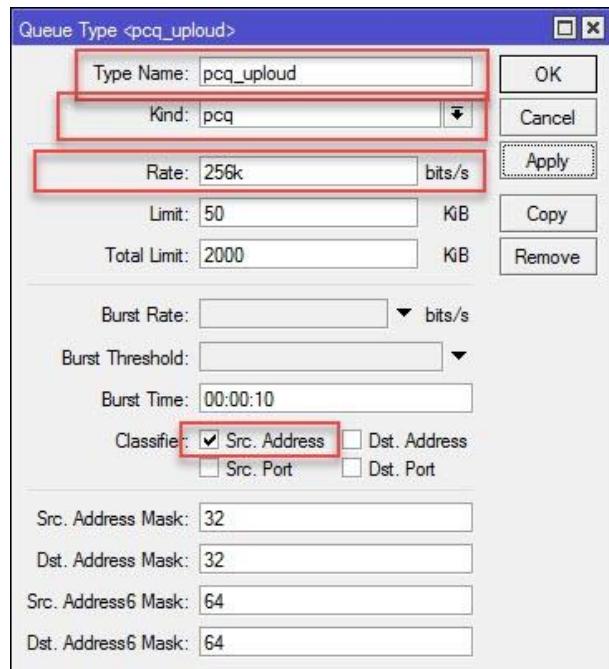
1. Pertama kita buat dahulu profile pcq baru, buat profile pcq download dan profile pcq upload, masuk pada menu **Queue > Queue Types > (+)**



2. Isikan parameter berikut pada profil pcq download, **Type name=pcq_download**, **Kind= pcq**, **Rate= 512k**, centang (✓) pada **Dst.Address**, klik apply dan ok



3. Lalu buat satu lagi untuk profile pcq upload, isikan sebagai berikut **Type name=pcq_upload**, **Kind=pcq**, **Rate=256k**, centang (✓) pada **Src.Address**, klik apply dan ok



4. Terlihat ada 2 pcq yang tadi kita buat

Queue List	
Simple Queues	
<input style="margin-right: 10px;" type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="T"/>	
Type Name	Kind
* wireless-default	sfq
* synchronous-default	red
pcq_upload	pcq
pcq_download	pcq
* pcq-upload-default	pcq
* pcq-download-default	pcq
* only-hardware-queue	none
* multi-queue-ethernet-default	mq pfifo
* hotspot-default	sfq
* ethernet-default	pfifo
* default-small	pfifo
* default	pfifo

12 items

5. Kemudian buat satu rule simple queue, pada tab General isikan name=queue_PCQ, target 192.168.20.0/24 dan pada tab Advanced masukkan profile pcq yang tadi kita buat pada Queue Type

New Simple Queue	
General	
Name:	queue_PCQ
Target:	192.168.20.0/24
Dst.:	
Target Upload	Target Download
Max Limit:	unlimited
Burst	
Burst Limit:	unlimited
Burst Threshold:	unlimited
Burst Time:	0
Time	
enabled	

New Simple Queue	
Advanced	
Packet Marks:	
Target Upload	Target Download
Limit At:	unlimited
Priority:	8
Bucket Size:	0.100
Queue Type:	pcq_upload
	pcq_download
Parent:	none
enabled	

6. Untuk melihat trafik data dari pcq yang tadi kita buat, masuk pada tab traffic

