

# **MODUL MTCNA**

---

MikroTik Certificate Network Associate  
Komunitas IT SMKN 1 Nglegok

**BY: Evan Cristianto**  
**Angkatan XIV**



**Penulis** : Evan Cristianto  
**Design Cover** : Evan Cristianto  
**Pembimbing** : Very Setiawan, S.Kom  
**Support** : Komunitas IT SMKN 1 Nglegok  
**Website** : evancrstian.blogspot.com  
**Terbit** : 21 Februari 2025



## PENGANTAR

Puji syukur atas kehadirat Tuhan yang Maha Esa atas limpah dan Rahmatnya sehingga Buku yang berjudul "For KITS Book: MTCNA" telah selesai ditulis dan disusun dan dapat saya selesaikan dengan tepat waktu. Semogabuku ini dan ilmu yang saya dapat bisa bermanfaat bagi kita semua.

Saya mengucapkan terima kasih banyak kepada seluruh pihak yang telah membantu saya dalam membuat buku ini, dan sekali lagi saya sangat berterima kasih khususnya kepada:

1. Tuhan yang Maha Esa
2. Kedua orang tua yang selalu memberikan semangat
3. Pembina Komunitas IT, Bapak Very Setiawan, S.kom
4. Seluruh Alumni, Kakak kelas, dan teman teman Komunitas IT

Saya berharap buku ini dapat berguna bagi semua orang tanpa terkecuali. Karena buku yang saya tulis masih belum dikatakan sempurna. Saya berharap saran serta kritikan dari anda sekalian agar kedepannya menjadi lebih baik. Jadi bagi kalian yang menemukan kesalahan dalam buku saya, mohon saran dan kritikan kalian kirim ke email saya evancristianto629@gmail.com. Terima Kasih.

Hormat Saya

Evan Cristianto



## DAFTAR ISI

<b>PENGANTAR.....</b>	<b>3</b>
<b>DAFTAR ISI.....</b>	<b>4</b>
<b>Mikrotik Certified Network Associate (MTCNA).....</b>	<b>8</b>
<b>LAB 1 Akses menggunakan Winbox, Webfig dan SSH (PuTTY, CMD).....</b>	<b>9</b>
A. Akses Winbox.....	9
B. Akses ViaWebfig.....	12
C. Selanjutnya Akses Menggunakan SSH, PUTY, dan CMD.....	13
<b>LAB 2 SERVICE &amp; PORT MANAGEMENT.....</b>	<b>18</b>
A. Mengaktifkan dan Menonaktifkan Service.....	18
B. Mengubah Port Pada Service.....	20
<b>LAB 3 UPGRADE dan DOWNGRADE MIKROTIK.....</b>	<b>22</b>
A. Upgrade MikroTik.....	22
B. Downgrade MikroTik.....	26
<b>LAB 4 Disable, Enable, Add Package.....</b>	<b>28</b>
A. Mendisable Packages.....	28
B. Menenable Packages.....	31
C. Add Packages.....	33
<b>LAB 5 Backup (.backup) VS Export (.rsc) &amp; Restore VS Import.....</b>	<b>35</b>
A. Backup.....	35
B. Restore.....	38
C. Export.....	41
D. Import.....	42
<b>LAB 6 Manajemen User and Group.....</b>	<b>43</b>
A. Manajemen User.....	43
B. Management Groub.....	46
<b>LAB 7 MNDP (Mikrotik Neighbour Discovery Protocol).....</b>	<b>48</b>
<b>LAB 8 NTP and Clock.....</b>	<b>50</b>
A.NTP Client.....	50
B. NTP Server.....	51
<b>LAB 9 Soft &amp; Hard Reset Device.....</b>	<b>53</b>
Pada lab ini kita akan melakukan 2 cara untuk melakukan reset pada Mikrotik yaitu Hard & Soft reset. reset adalah reset tanpa menghapus konfigurasi. Hard reset adalah reset dengan menghapus seluruh konfigurasi/mengembalikan ke setelan Pabrik.....	53
A. Soft Reset.....	53
B. Hard Reset.....	54



---

<b>LAB 10 Router Identity &amp; Mikrotik Misc (Trace Route, Torch, Bandwidth Test, Interface Traffic Monitor,Ping Tool, System Logging, Rommon).....</b>	<b>55</b>
A.MikroTik Identity.....	55
B.Trace Route.....	56
C.Torch.....	60
D. Bandwidth Test.....	62
E. Interface Traffic Monitor.....	66
F. Ping Tool.....	67
G. System Logging.....	68
G. Rommon.....	71
<b>LAB 11 Konfigurasi IP , DHCP Server &amp; leases (TimeManagement and Make Static).....</b>	<b>72</b>
A.Konfigurasi IP ADRESS.....	72
B.DHCP Server.....	78
C.Leases.....	82
- Time Management.....	86
<b>LAB 12 Setting router gateway(IP Klien Dynamic).....</b>	<b>87</b>
<b>LAB 13 Creating briges/loopback.....</b>	<b>93</b>
<b>LAB 14 Adding ports to bridges.....</b>	<b>96</b>
<b>LAB 15 Wireless (AP Bridge &amp; Station Bridge).....</b>	<b>100</b>
A. AP Bridge.....	100
B. Station Bridge.....	102
<b>LAB 16 Wireless (Bridge &amp; Station).....</b>	<b>105</b>
A.Bridge.....	105
B.Station.....	107
<b>LAB 17 Security Profile (Authentication and Encryption).....</b>	<b>109</b>
<b>LAB 18 Virtual Access Point (Membuat 2 VAP).....</b>	<b>111</b>
<b>LAB 19 Virtual Access Point + Router Gateway (Repeater).....</b>	<b>114</b>
<b>LAB 20 Tunnel (EoIP, PPTP, L2TP, PPPoE).....</b>	<b>117</b>
A.EoIP.....	117
B.PPPtP.....	122
I Skenario 1.....	122
II. Skenario 2.....	127
C.L2TP Tunnel.....	130
D.PPPoE Tunnel.....	136
I. Skenario 1.....	136
II.Skenario 2.....	139



---

<b>LAB 21 Routing Concepts.....</b>	143
<b>LAB 22 Route Flags.....</b>	144
<b>LAB 23 Static Route 2 Router.....</b>	145
<b>LAB 24 Static Route 3 Router.....</b>	150
<b>LAB 25 Static Routing Default Route.....</b>	154
<b>LAB 26 Prioritas Routing.....</b>	157
<b>LAB 27 SIMPLE QUEUE.....</b>	160
<b>LAB 28 Simple Queue with PCQ.....</b>	162
<b>LAB 29 Simple Queue with Parent and Child.....</b>	166
<b>LAB 30 Firewall principles.....</b>	169
<b>LAB 31 Structure , chains and actions.....</b>	171
<b>LAB 32 Firewall Filter Input , Output dan Forward.....</b>	172
A. Firewall Filter Input.....	172
B. Firewall Filter Output.....	174
C. Firewall Filter Forward.....	176
<b>LAB 33 Firewall Stragety 1 &amp; 2.....</b>	178
A.Firewall Strategy 1 (Drop All Accept Any).....	178
B. Firewall Strategy 2 (Drop Any Accept All).....	180
<b>LAB 34 Firewall Stragety 1 &amp; 2.....</b>	182
<b>LAB 35 Blokir Situs dengan Firewall Filter Forward (TLS).....</b>	183
A.Firewall Filter Forward.....	184
B.TLS.....	186
<b>LAB 36 Destination NAT Action (dst-nat &amp; redirect).....</b>	189
A. DST NAT.....	189
B. Redirect.....	193
<b>LAB 37 Konfigurasi Dasar Hotspot.....</b>	195
<b>LAB 38 Hotspot Login Methods HTTP CHAP/PAP.....</b>	198
<b>LAB 39 Hotspot Profile (Keepalive timeout, shared user,Rate-limit).....</b>	200
<b>LAB 40 Hotspot Users Add User.....</b>	203
<b>LAB 41 Bypass Hotspot Walled Garden.....</b>	204
<b>LAB 42 Bypass Hotspot IP Binding (regular, bypass,blocked).....</b>	207
A. Reguler.....	207
B. Bypass.....	209
C. Blocked.....	210
<b>Daftar Pustaka.....</b>	212
<b>Biografi Penulis.....</b>	213

---



## Mikrotik Certified Network Associate (MTCNA)

MikroTik adalah sistem operasi berbasis perangkat lunak (software) yang digunakan untuk mengubah komputer menjadi jaringan. MikroTik merupakan perangkat lunak open source yang berbasis linux. MikroTik adalah sebuah perusahaan jaringan yang didirikan oleh John Trully dan Arnis Riekstins pada tahun 1996. John dan Arnis memulai MikroTik dengan menggabungkan sistem operasi Linux dan MS DOS dengan teknologi wireless LAN (WLAN) Aeronet di Moldova.

MTCNA atau Mikrotik Certified Network Associate adalah sertifikasi networking pada level dasar (associate) yang diperuntukkan bagi siapapun yang ingin mendalami teknologinya Mikrotik. Tidak hanya mempelajari teknologi dari mikrotik, tapi juga perangkat dari mikrotik yaitu Router Board. MTCNA (Mikrotik Certified Network Associate) merupakan sertifikasi Mikrotik yang paling awal, sehingga ujian dari sertifikasi ini merupakan pengenalan dan perangkat-perangkat mikrotik Router Board dan perangkat lunak mikrotik Router OS. Tujuan adanya setifikasi MTCNA karena MTCNA menjadi salah satu persyaratan bagi engineer yang ingin terjun ke dunia teknologi informasi khususnya networking atau jaringan. Dengan adanya sertifikat MTCNA yang dimiliki engineer, maka akan memiliki prospek pekerjaan yang kompetitif kedepannya.

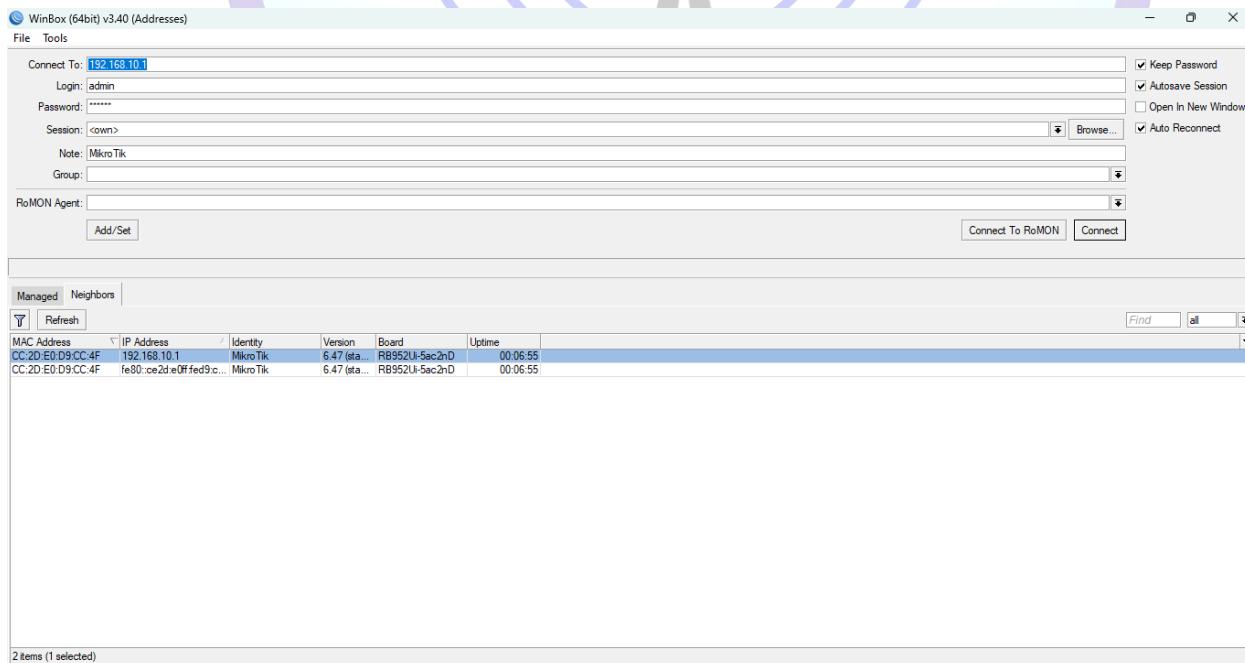


## LAB 1 Akses menggunakan Winbox, Webfig dan SSH (PuTTy, CMD)

Pada LAB pertama ini kita akan mencoba akses MikroTik menggunakan berbagai cara seperti pada judul lab yaitu melalui, Winbox, Webfig, SSH, PuTTy, dan CMD.

### A. Akses Winbox

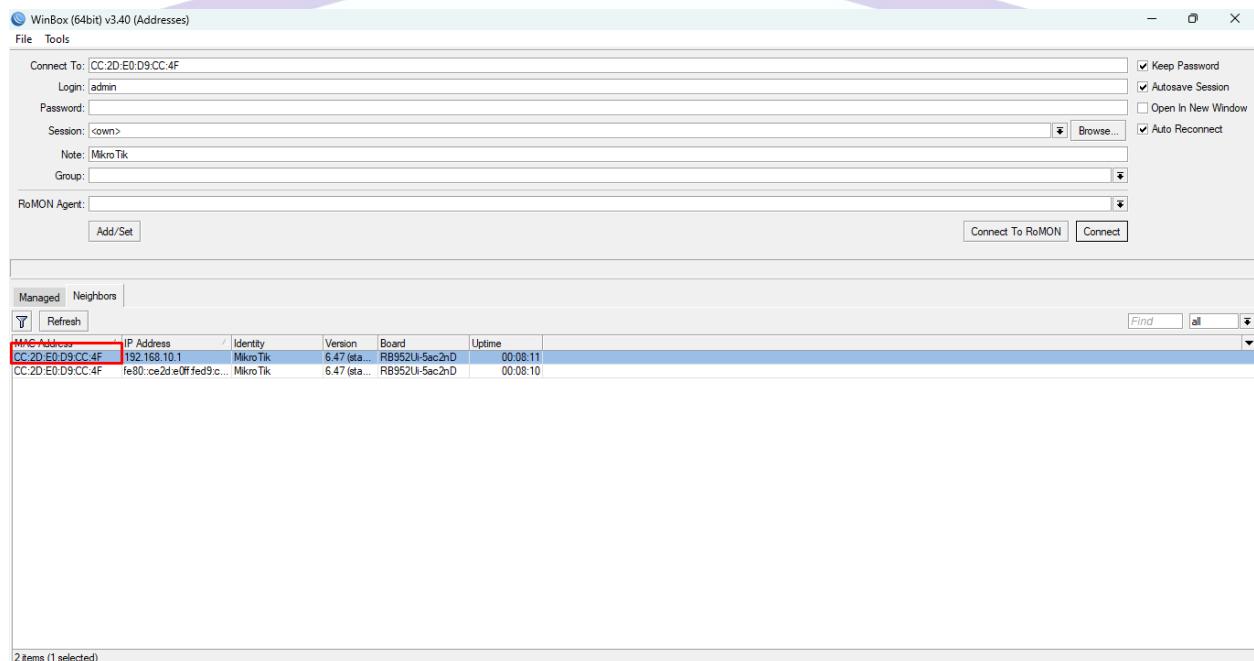
1. Langkah pertama untuk mengakses mikrotik menggunakan winbox adalah menginstall winbox di web resminya mikrotik.
2. Sambungkan router ke pc/laptop ether 2 pada router mengarah ke pc, lalu internet pada ether 1 router
3. Jika kalian sudah menyambungkan maka tampilan akan seperti di bawah ini



4. Disini kalian bisa login menggunakan mac address dan ip dengan cara yang sangat mudah yaitu kalian klik mac/ip sesuai dengan keinginan kalian dan masukkan nama user dan pasword jika ada. Jika sudah klik connect

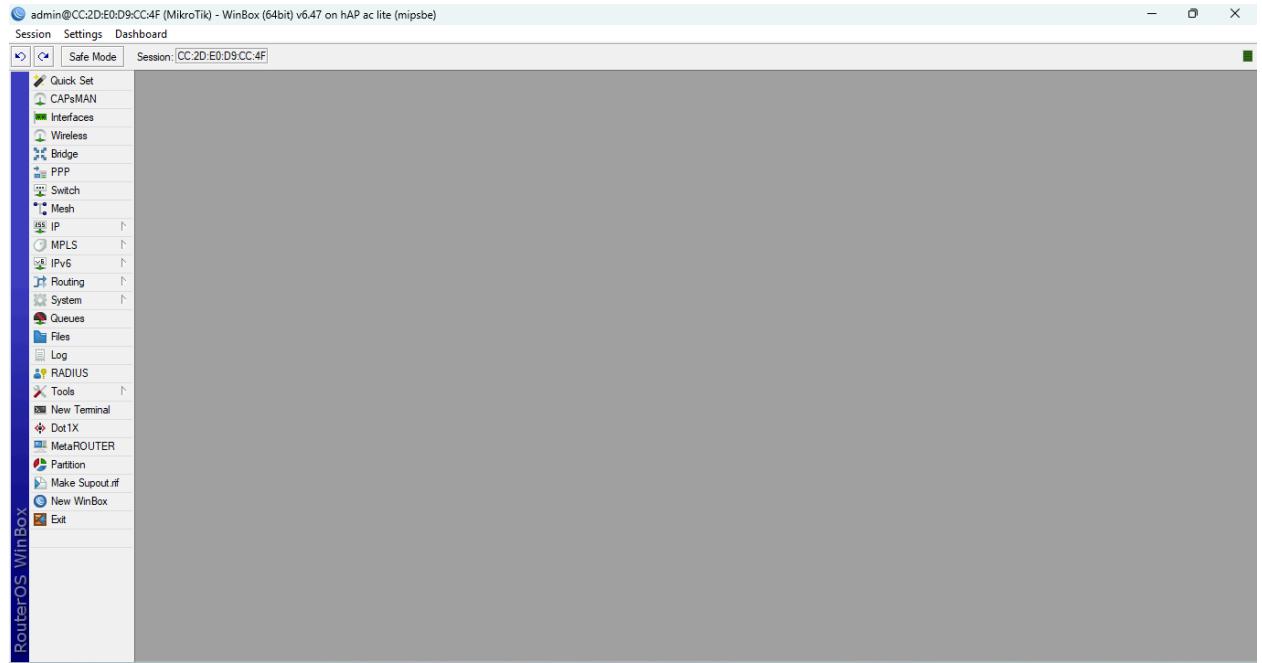


5. Beginilah tampilan jika kita login ke dalam router menggunakan IP
6. Jika kita ingin login menggunakan IP maka ip router dengan IP pc harus dalam satu jaringan yang sama
7. Lalu berikutnya kita akan akses menggunakan Winbox menggunakan MAC Address



8. Kalian klik mac adres lalu connect, maka tampilan kita setelah masuk menggunakan mac address akan seperti ini





9. Perbedaannya terdapat pada nama yang tertera di sebelah kiri atas

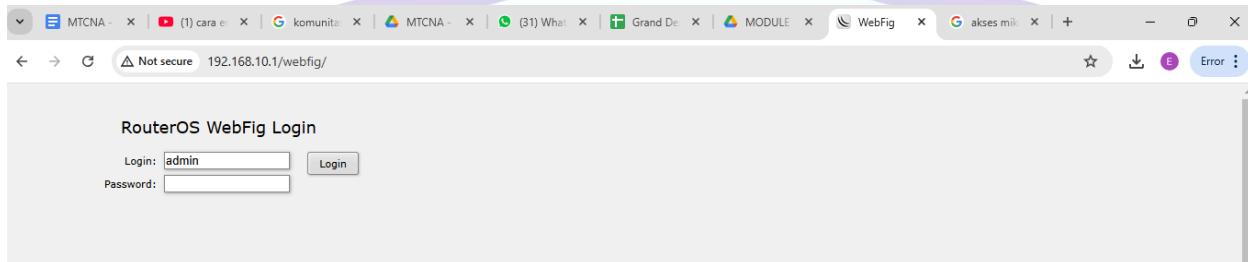




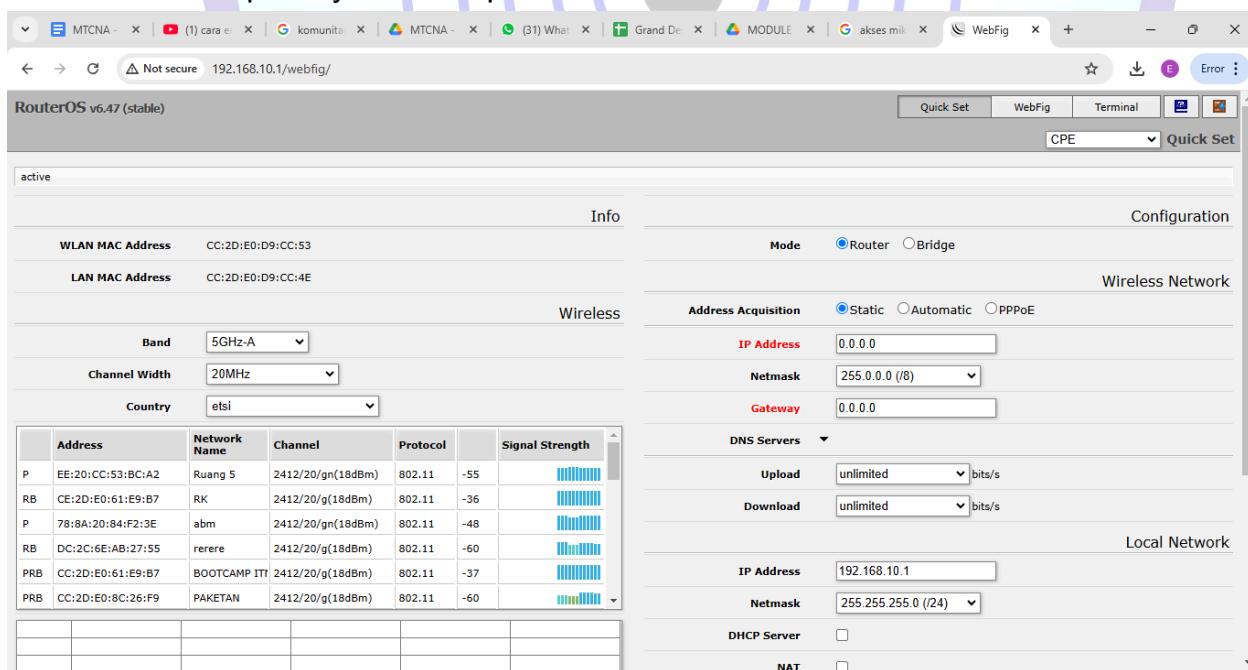
## B. Akses ViaWebfig

Pada via webfig ini kita akan mengakses mikrotik lewat web, cara ini menurut saya adalah cara yang sangat mudah.

1. Langkah Pertama kalian masuk ke dalam Browser
2. Lalu kalian masuk menggunakan IP Address



3. Masukkan Username dan Pasword Router
4. Maka Tampilannya akan seperti ini





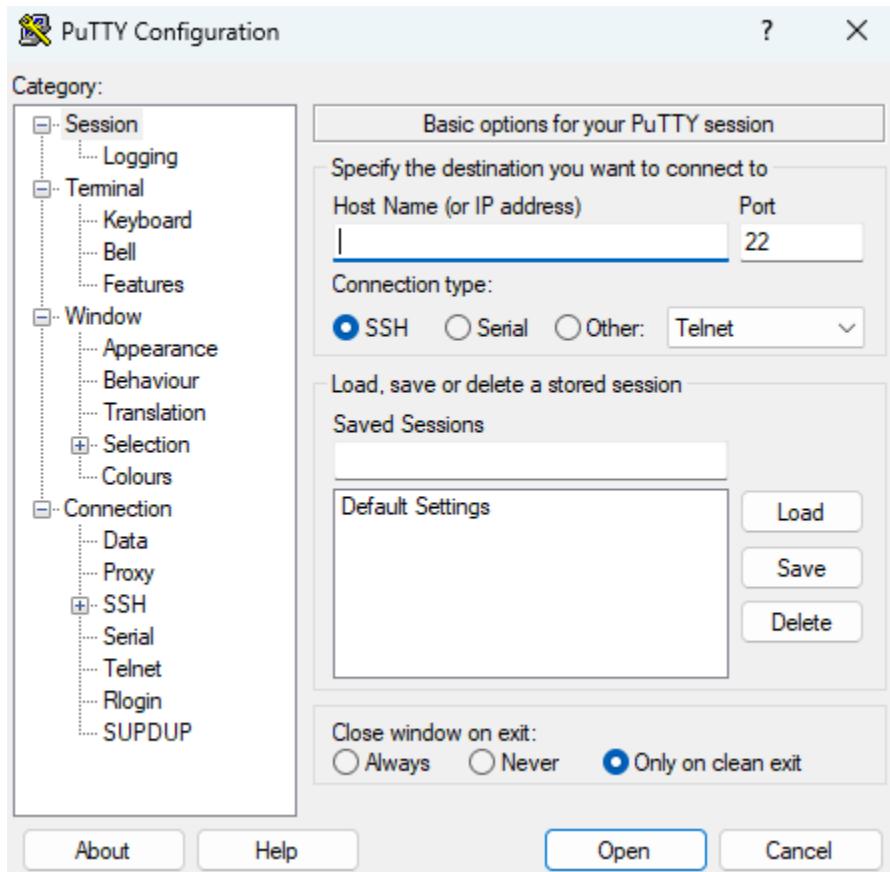
## C. Selanjutnya Akses Menggunakan SSH, PUTY, dan CMD

SSH (Secure Shell) adalah protokol yang digunakan untuk mengakses perangkat atau server secara remote dengan cara yang aman. Dibandingkan dengan Telnet, yang juga digunakan untuk akses remote, SSH lebih aman karena mengenkripsi data yang dikirimkan antara client dan server, sehingga melindungi informasi dari potensi pembobolan.

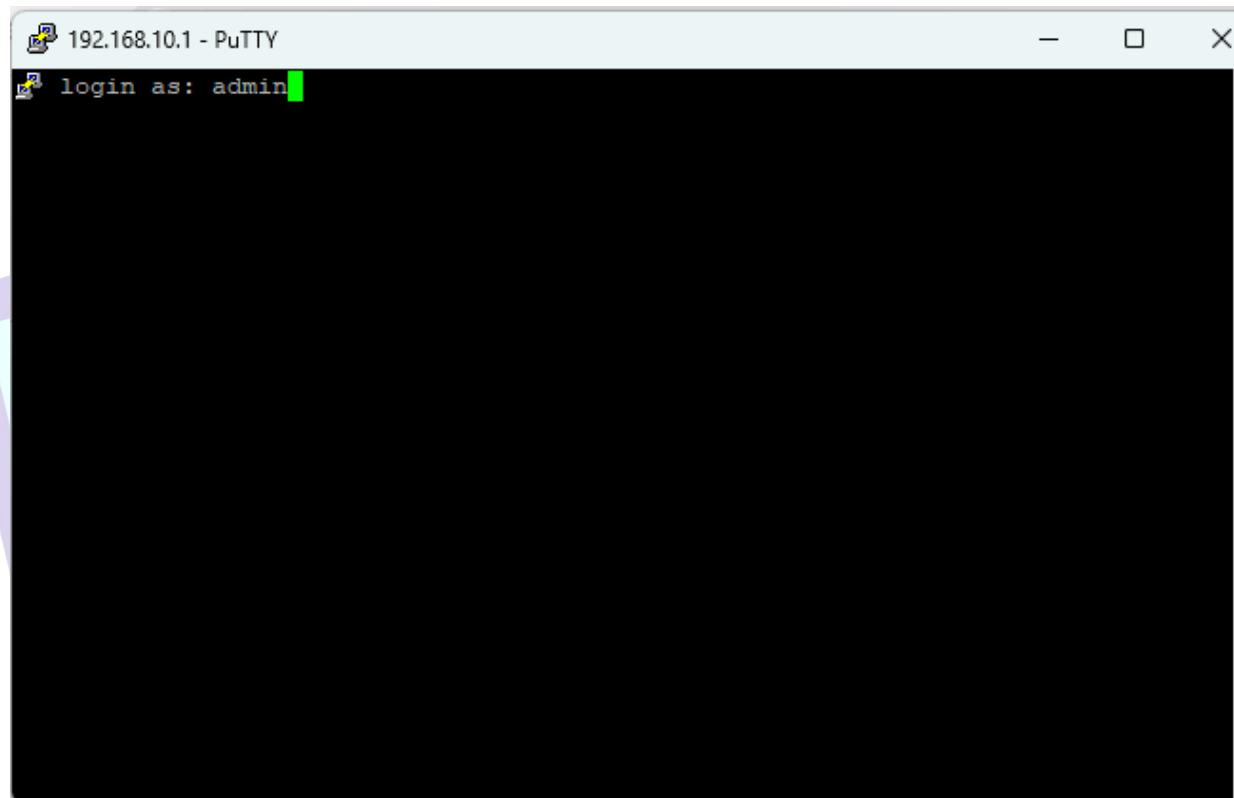
PutTY adalah salah satu aplikasi populer yang digunakan untuk mengakses perangkat secara remote melalui protokol SSH atau Telnet. Dengan PutTY, Anda dapat melakukan konfigurasi atau manajemen perangkat seperti MikroTik dari jarak jauh, baik menggunakan SSH (untuk koneksi aman) maupun Telnet (koneksi yang lebih terbuka namun tidak terenkripsi).

Singkatnya, SSH adalah cara aman untuk remote server, sementara PutTY adalah alat yang digunakan untuk mengaksesnya melalui koneksi tersebut.

1. Pertama akan menggunakan PUTY
  - Langkah pertama kalian install putty di website resminya
  - Berikutnya jika sudah terinstall kalian masuk ke dalam putty



- Tamplannya akan seperti ini
- Jika sudah masuk menggunakan IP sama seperti Viawebfig tadi
- Maka akan seperti ini



```
192.168.10.1 - PuTTY
login as: admin
```

- Kalian login menggunakan admin bisa menggunakan username dan password
- Jika tampilan seperti ini maka arinya kalian sudah berhasil mengakses menggunakan PUTY



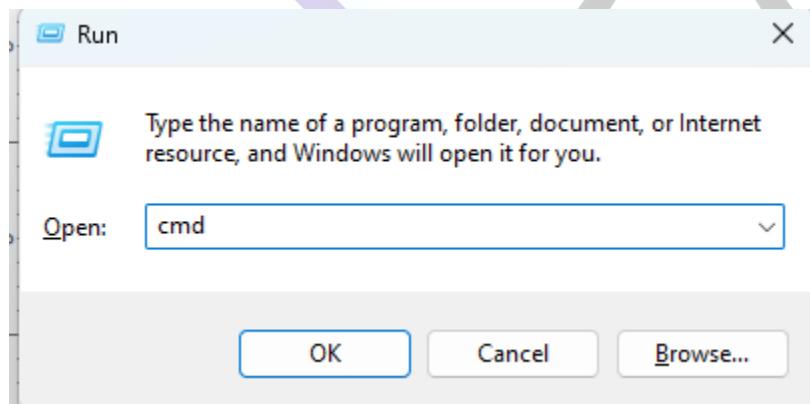
```
192.168.10.1 - PuTTY

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

[admin@evan] >
```

2. Berikutnya kita akan mengakses MikroTik menggunakan CMD

- Langkah pertama kalian klik Windows+R



- Lalu ping menggunakan IP dari router



```
cmd Command Prompt
microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC-LAB ->ping192.168.10.1
'ping192.168.10.1' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\PC-LAB ->ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\PC-LAB ->
```

- Jika TTL maka kalian sudah berhasil menggunakan CMD



## LAB 2 SERVICE & PORT MANAGEMENT

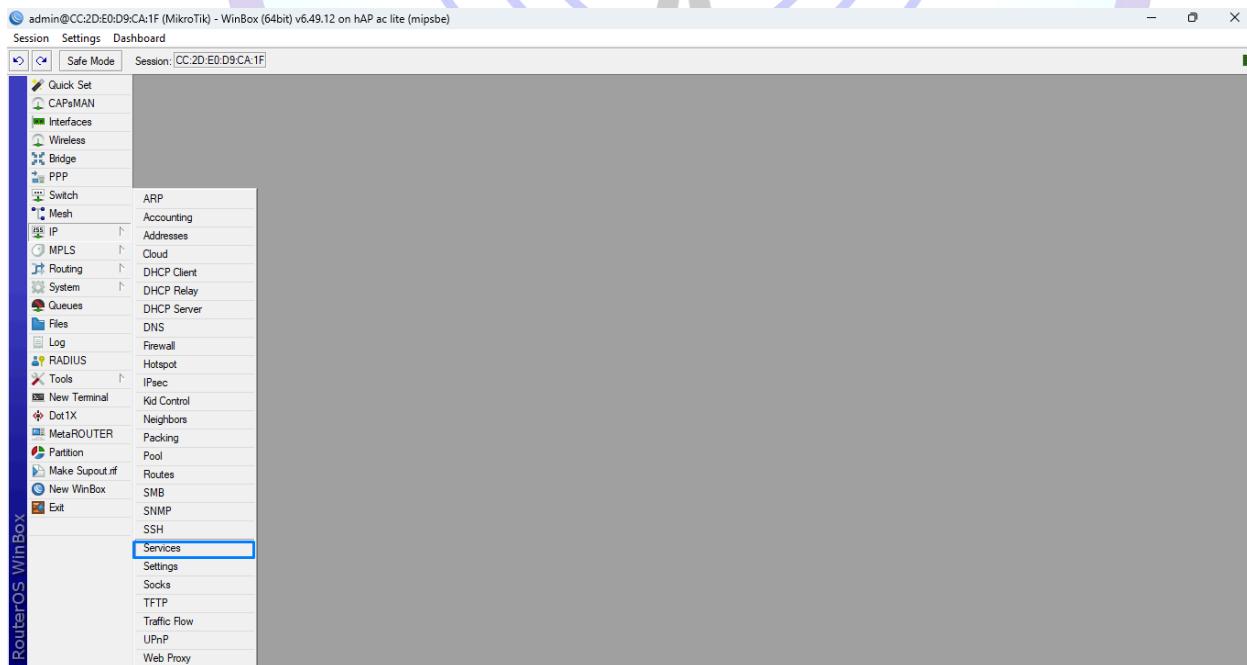
Pada lab ini kita akan belajar mengenai proses pengelolaan layanan-layanan yang berjalan di perangkat jaringan (seperti MikroTik), serta pengaturan port yang digunakan untuk komunikasi jaringan. Tujuannya adalah untuk:

- Meningkatkan Keamanan:** Dengan menonaktifkan layanan yang tidak diperlukan, mengganti port default, dan membatasi akses layanan hanya untuk IP yang diizinkan.
- Mengoptimalkan Kinerja:** Mengatur layanan agar hanya layanan yang penting yang aktif, sehingga perangkat tidak terbebani dengan layanan yang tidak perlu.
- Mengelola Akses:** Mengkonfigurasi firewall dan port forwarding untuk memastikan akses ke layanan sesuai dengan kebutuhan dan menghindari potensi ancaman dari luar.

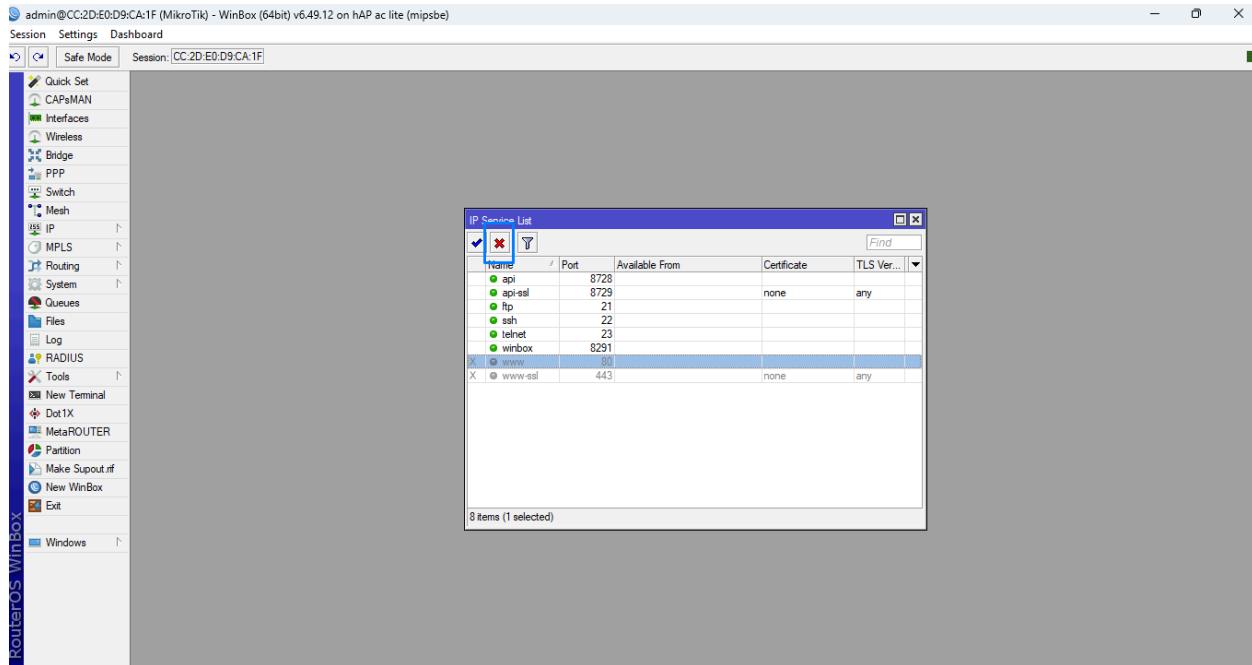
Secara keseluruhan, Service & Port Management adalah langkah penting dalam mengelola jaringan secara efisien dan aman.

### A. Mengaktifkan dan Menonaktifkan Service

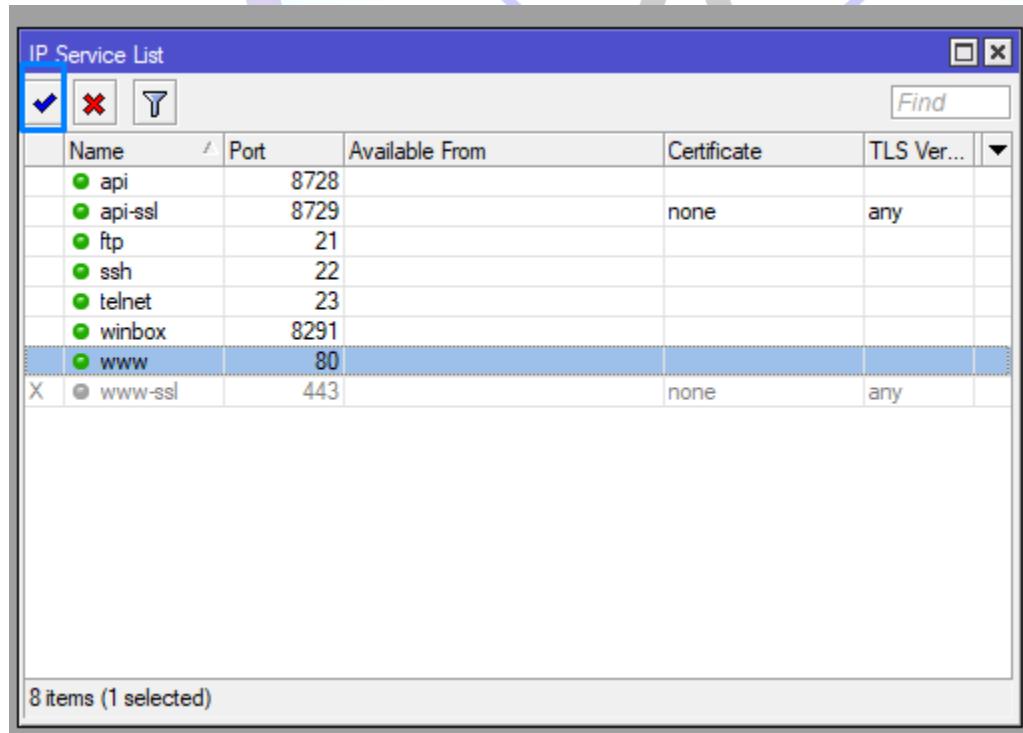
1. Berikut adalah cara untuk mengaktifkan dan menonaktifkan Service
2. Pertama kalian buka winbox lalu klik IP>Service



3. Cara untuk menonaktifkan Service adalah dengan menekan tombol X, sebagai contoh saya akan menonaktifkan Service www



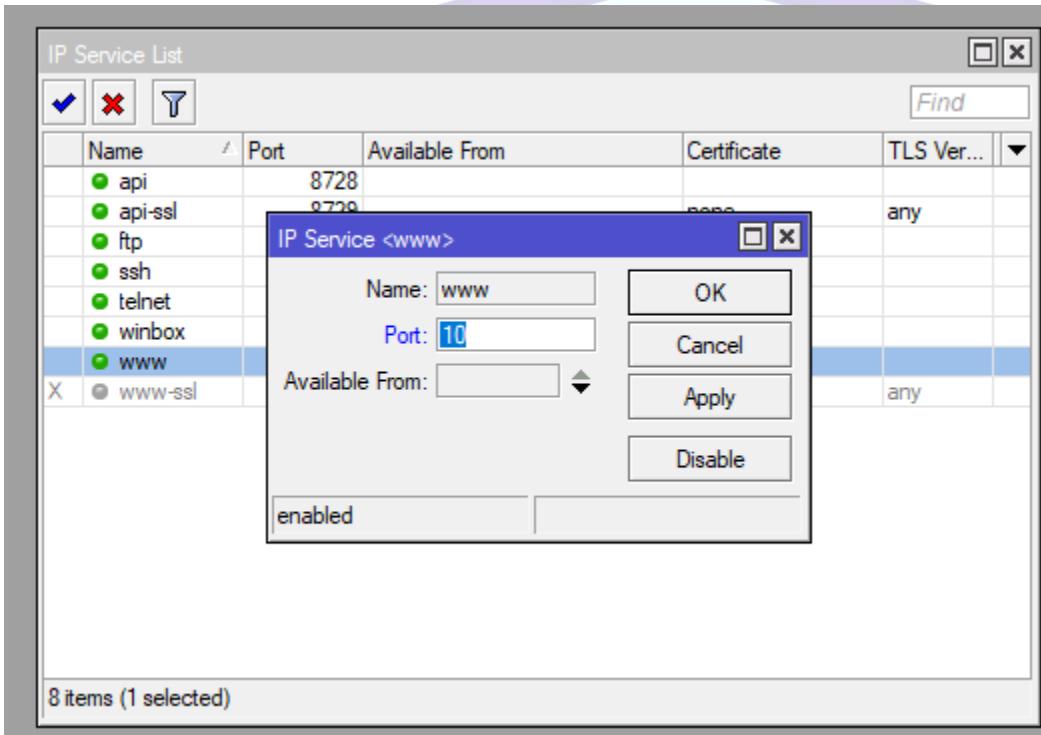
4. Dan cara untuk mengaktifkan kembali caranya sangat mudah kalian hanya klik tombol centang yang terdapat pada sebelah kiri tombol



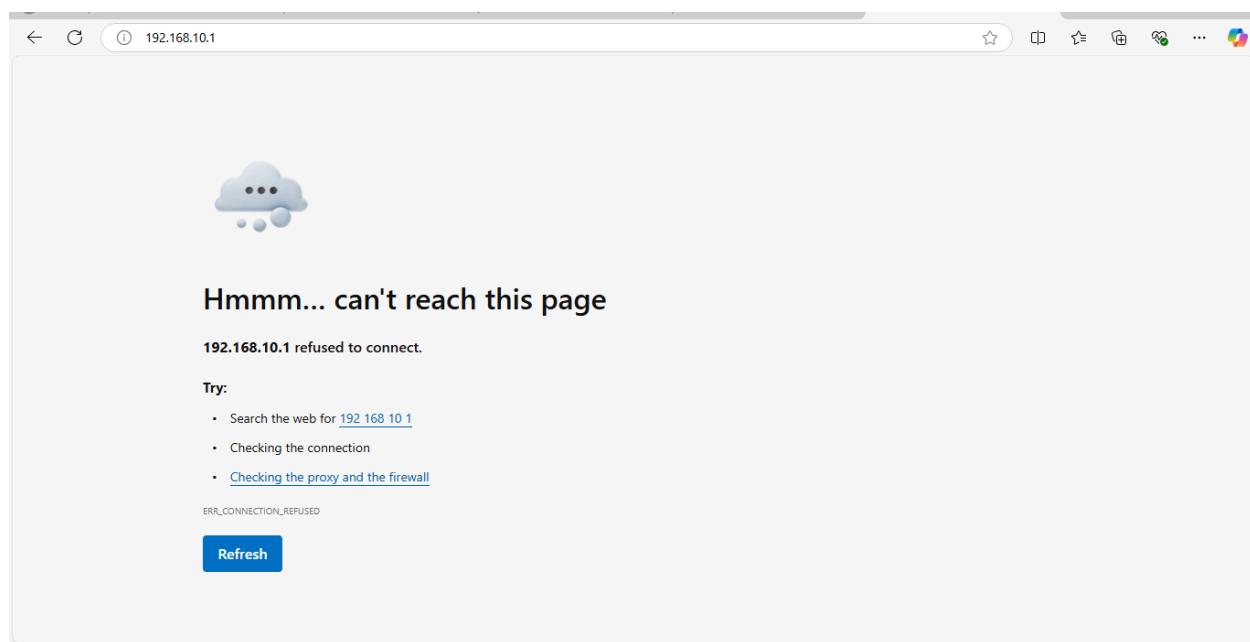


## B. Mengubah Port Pada Service

1. Langkah pertama kalian klik 2 kali pada service yang ingin kalian ubah portnya



2. Jika sudah klik Apply
3. Untuk mencoba kalian masuk MikroTik menggunakan Webfig seperti di lab1 tadi



4. Kita tidak dapat masuk dikarenakan port default pada router telah kita ganti. Untuk mengakses kembali kita hanya perlu menambahkan angka port di paling akhir contoh (192.168.10.1:(port kalian))

RouterOS v6.49.12 (stable) | 192.168.10.1:10/webfig/#Quick\_Set

active

Info		Configuration	
<b>WLAN MAC Address</b>	CC:2D:E0:D9:CA:23	<b>Mode</b>	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
<b>LAN MAC Address</b>	CC:2D:E0:D9:CA:1E	<b>Wireless Network</b>	
<b>Wireless</b> Band: 5GHz-A Channel Width: 20MHz Country: esi		<b>Address Acquisition</b>	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> PPPoE
		<b>IP Address</b>	0.0.0.0
		<b>Netmask</b>	255.0.0.0 (/8)
		<b>Gateway</b>	0.0.0.0
		<b>DNS Servers</b>	unlimited
		<b>Upload</b>	unlimited bits/s
		<b>Download</b>	unlimited bits/s
<b>Local Network</b>			
IP Address: 192.168.10.1 Netmask: 255.255.255.0 (/24) DHCP Server: <input type="checkbox"/> NAT: <input type="checkbox"/>			

5. Kita sudah dapat mengakses kembali melalui Webfig

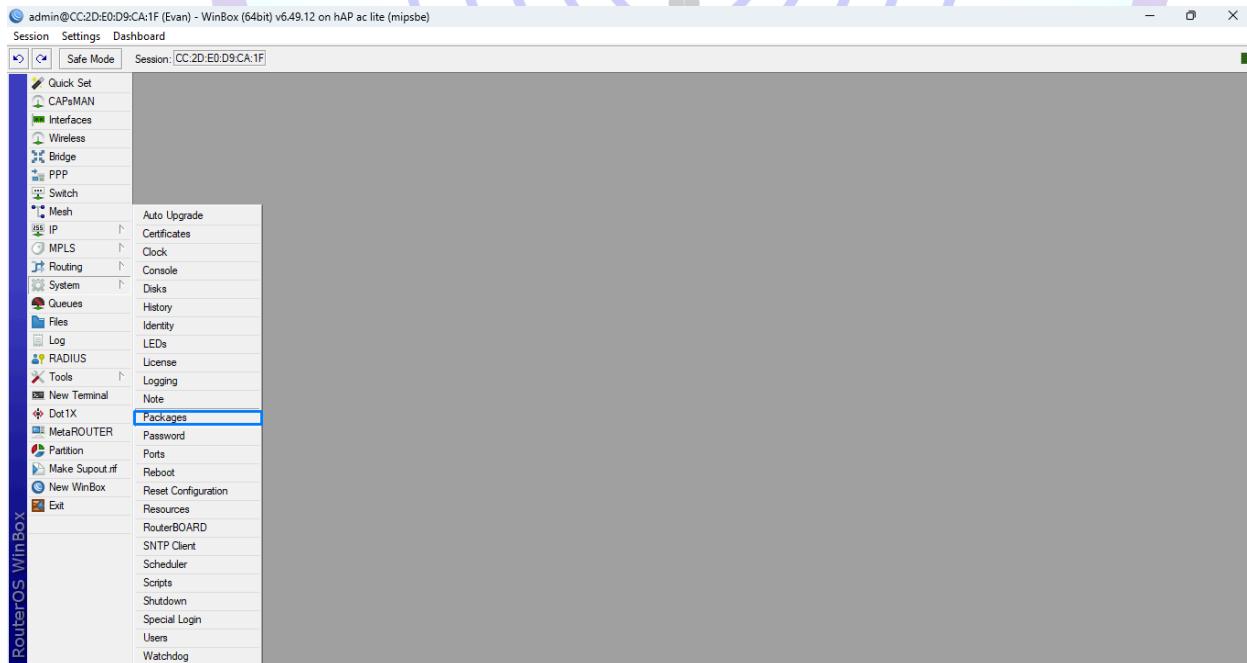


## LAB 3 UPGRADE dan DOWNGRADE MIKROTIK

Pada lab 3 ini kita akan belajar mengenai upgrade dan downgrade mikrotik. Dimana setiap versi terbaru dari mikrotik pasti terdapat sebuah evaluasi dari versi sebelumnya. Upgrade MikroTik adalah proses memperbarui RouterOS ke versi terbaru untuk mendapatkan fitur baru, perbaikan bug, dan peningkatan keamanan. Downgrade MikroTik adalah proses mengembalikan RouterOS ke versi yang lebih lama, biasanya untuk mengatasi masalah kompatibilitas atau kinerja yang muncul setelah upgrade. Secara singkat, Upgrade meningkatkan ke versi terbaru, sedangkan Downgrade menurunkan ke versi yang lebih lama.

### A. Upgrade MikroTik

#### 1. Langkah pertama kalian buka System> Packages



2. Kalian harus mendownload pack terbaru dari MikroTik yaitu di <https://mikrotik.com/download/archive> karena saya menggunakan RB maka download mipsbe



Software

7.16.2

2024-11-27

Architecture	File	Checksum
arm	all_packages-arm-7.16.2.zip	SHA256
arm	routeros-7.16.2-arm.npk	SHA256
arm64	chr-7.16.2-arm64.img.zip	SHA256
arm64	all_packages-arm64-7.16.2.zip	SHA256
arm64	routeros-7.16.2-arm64.npk	SHA256
arm64	chr-7.16.2-arm64.vdi.zip	SHA256
mipsbe	routeros-7.16.2-mipsbe.npk	SHA256
mipsbe	all_packages-mipsbe-7.16.2.zip	SHA256
mmips	routeros-7.16.2-mmips.npk	SHA256
mmips	all_packages-mmips-7.16.2.zip	SHA256
ppc	routeros-7.16.2-ppc.npk	SHA256
ppc	all_packages-ppc-7.16.2.zip	SHA256

### 3. Jika sudah terdownload kalian upload di files

Session Settings Dashboard

Session: [CC.2D:E0:D9:CA:1F]

File List

File Cloud Backup Backup Restore Upload... Find

File Name	Type	Size	Creation Time
flash	disk	18.6 KB	Jan/02/1970 00:02:01
flash/auto-before-reset.backup	backup	18.6 KB	Jan/01/1970 00:00:09
flash/hotspot	directory	1094 B	Feb/16/2024 02:24:33
flash/hotspot/alogin.html	html file	311 B	Feb/16/2024 02:24:33
flash/hotspot/css	directory	4053 B	Feb/16/2024 02:24:33
flash/hotspot/css/style.css	css file	640 B	Feb/16/2024 02:24:33
flash/hotspot/error.html	html file	3719 B	Feb/16/2024 02:24:33
flash/hotspot/errors.txt	txt file	903 B	Feb/16/2024 02:24:33
flash/hotspot/favicon.ico	ico file	644 B	Feb/16/2024 02:24:33
flash/hotspot/img	directory	4423 B	Feb/16/2024 02:24:33
flash/hotspot/img/passw...	svg file	444 B	Feb/16/2024 02:24:33
flash/hotspot/img/user.svg	svg file	1459 B	Feb/16/2024 02:24:33
flash/hotspot/login.html	html file	7.0 KB	Feb/16/2024 02:24:33
flash/hotspot/logout.html	html file	1204 B	Feb/16/2024 02:24:33
flash/hotspot/mdu.js	js file		
flash/hotspot/radvert.html	html file		

### 4. Lalu upload file yang sudah kalian download tadi



File List				
File		Cloud Backup		
<input type="button" value="New"/> <input type="button" value="Filter"/> <input type="button" value="Open"/> <input type="button" value="Save"/> <input type="button" value="Print"/> <input type="button" value="Backup"/> <input type="button" value="Restore"/> <input type="button" value="Upload..."/> <input type="button" value="Find"/>		Type	Size	Creation Time
<input type="checkbox"/>	all_packages-mip...	Uploading Files		2025-02-16 04:37:34
<input type="checkbox"/>	flash	Uploading all_packages-mip...	(3926.8 KiB of 4546.7 KiB at 3.93 Mbps)	2025-02-16 00:02:01
<input type="checkbox"/>	flash			2025-01-16 00:00:09
<input type="checkbox"/>	flash			2024-02-16 02:24:33
<input type="checkbox"/>	flash			2024-02-16 02:24:33
<input type="checkbox"/>	flash			2024-02-16 02:24:33
<input type="checkbox"/>	flash			2024-02-16 02:24:33
<input type="checkbox"/>	flash			2024-02-16 02:24:33
<input type="checkbox"/>	flash/hotspot/css/style.css	.css file	4053 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/error.html	.html file	640 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/errors.txt	.txt file	3719 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/favicon.ico	.ico file	903 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/img	directory		Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/img/passw...	.svg file	644 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/img/user.svg	.svg file	444 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/login.html	.html file	4423 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/logout.html	.html file	1459 B	Feb/16/2024 02:24:33
<input type="checkbox"/>	flash/hotspot/md5.js	.js file	7.0 kB	Feb/16/2024 02:24:33
31 items	12.8 MiB of 16.0 MiB used		19% free	

5. File sudah berhasil terupload



File List

File Cloud Backup

Backup Restore Upload... Find

File Name	Type	Size	Creation Time
all packages-mipsbe-7.16.2.zip	.zip file	4546.7 kB	Jan/06/2025 12:22:21
flash	disk		Jan/02/1970 07:02:01
flash/auto-before-reset.backup	backup	18.6 kB	Jan/01/1970 07:00:09
flash/hotspot	directory		Feb/16/2024 09:24:33
flash/hotspot/alogin.html	.html file	1094 B	Feb/16/2024 09:24:33
flash/hotspot/api.json	json file	311 B	Feb/16/2024 09:24:33
flash/hotspot/css	directory		Feb/16/2024 09:24:33
flash/hotspot/css/style.css	.css file	4053 B	Feb/16/2024 09:24:33
flash/hotspot/error.html	.html file	640 B	Feb/16/2024 09:24:33
flash/hotspot/errors.txt	.txt file	3719 B	Feb/16/2024 09:24:33
flash/hotspot/favicon.ico	.ico file	903 B	Feb/16/2024 09:24:33
flash/hotspot/img	directory		Feb/16/2024 09:24:33
flash/hotspot/img/passw...	.svg file	644 B	Feb/16/2024 09:24:33
flash/hotspot/img/user.svg	.svg file	444 B	Feb/16/2024 09:24:33
flash/hotspot/login.html	.html file	4423 B	Feb/16/2024 09:24:33
flash/hotspot/logout.html	.html file	1459 B	Feb/16/2024 09:24:33
flash/hotspot/md5.js	.js file	7.0 kB	Feb/16/2024 09:24:33

32 items (1 selected) | 13.0 MiB of 16.0 MiB used | 18% free



## B. Downgrade MikroTik

Downgrade adalah cara untuk kita dapat mengakses mikrotik jika RouterBoard tidak support versi terbaru

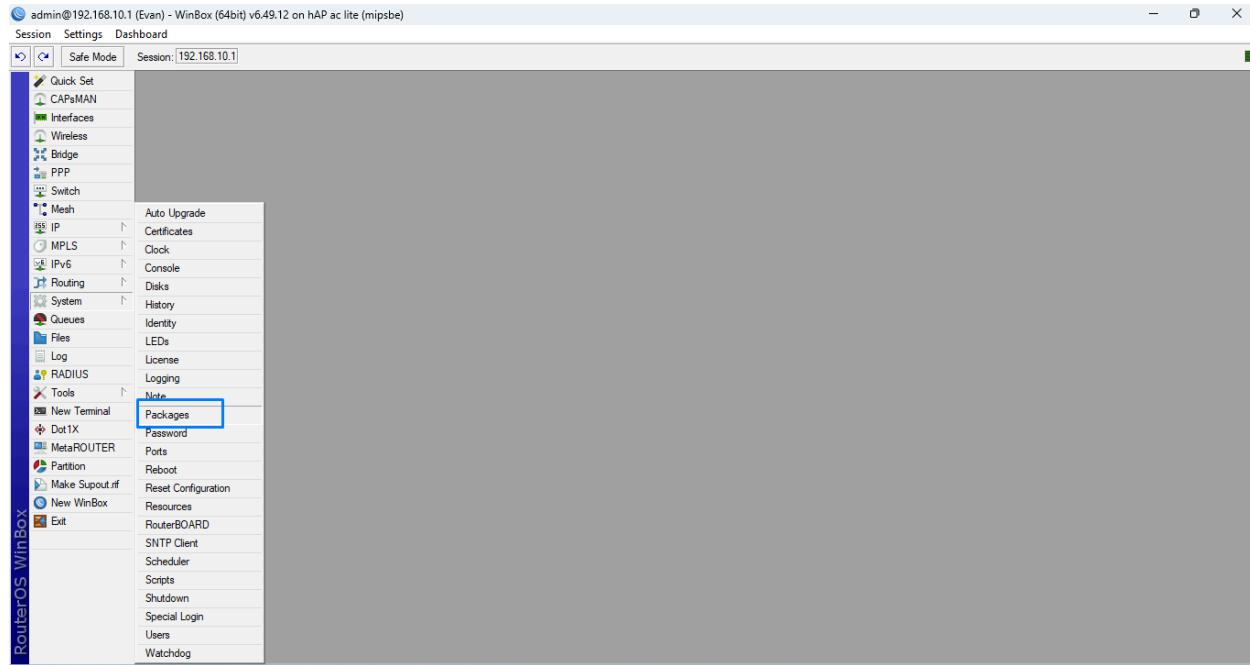
1. Langkah pertama diawali dengan mendownload file pada

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

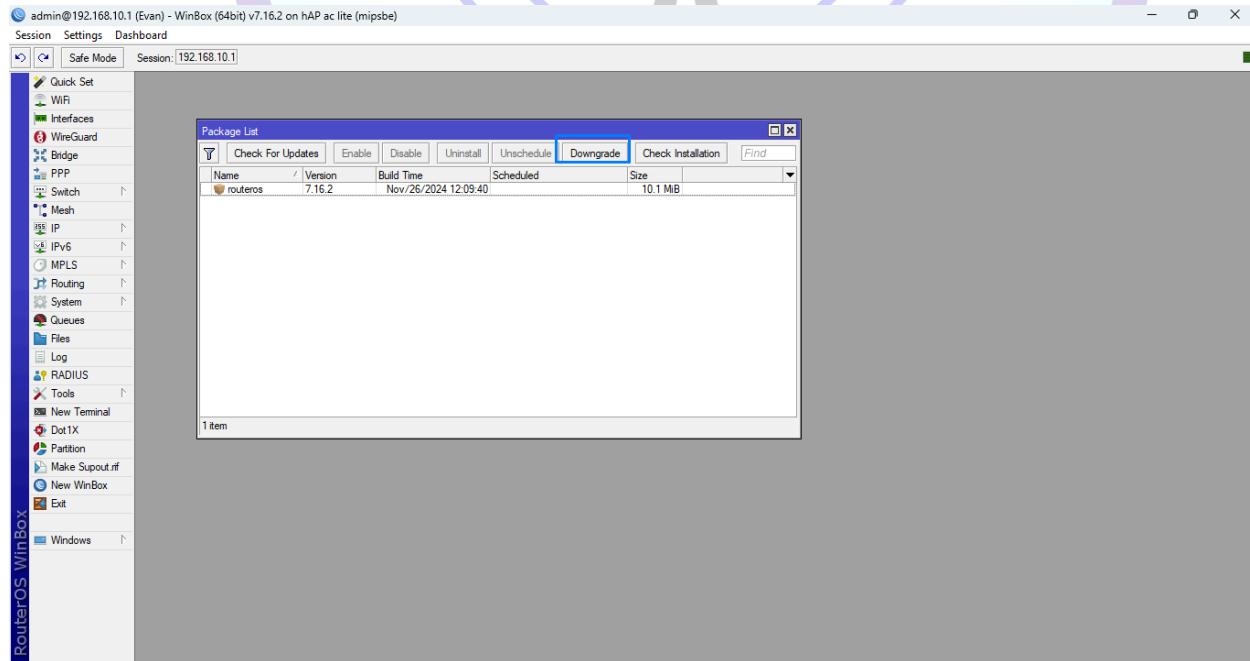
The screenshot shows a web browser displaying the MikroTik Software download page. The URL in the address bar is <https://mikrotik.com/download/archive>. The page has a blue header with the MikroTik logo and navigation links: Home, About, Buy, Jobs, Hardware, Software (which is underlined), Support, Training, and Account. Below the header, there's a blue bar with the word "Software". The main content area shows a table of files for version 7.12.1. The table has columns for Architecture, File, and Checksum. The architectures listed are arm, arm64, mipsbe, mips, mmips, ppc, smips, and tile. Each row contains a file link (e.g., all\_packages-arm-7.12.1.zip) and a SHA256 checksum.

Architecture	File	Checksum
arm	<a href="#">all_packages-arm-7.12.1.zip</a>	SHA256
arm	<a href="#">routeros-7.12.1-arm.npk</a>	SHA256
arm64	<a href="#">routeros-7.12.1-arm64.npk</a>	SHA256
arm64	<a href="#">all_packages-arm64-7.12.1.zip</a>	SHA256
mipsbe	<a href="#">all_packages-mipsbe-7.12.1.zip</a>	SHA256
mipsbe	<a href="#">routeros-7.12.1-mipsbe.npk</a>	SHA256
mmips	<a href="#">all_packages-mmips-7.12.1.zip</a>	SHA256
mmips	<a href="#">routeros-7.12.1-mmips.npk</a>	SHA256
ppc	<a href="#">all_packages-ppc-7.12.1.zip</a>	SHA256
ppc	<a href="#">routeros-7.12.1-ppc.npk</a>	SHA256
smips	<a href="#">all_packages-smips-7.12.1.zip</a>	SHA256
smips	<a href="#">routeros-7.12.1-smips.npk</a>	SHA256
tile	<a href="#">all_packages-tile-7.12.1.zip</a>	SHA256

2. Berikutnya Kalian downgrade pada menu



### 3. Kalian klik downgrade



### 4. Jika sudah Mikrotik sudah di downgrade

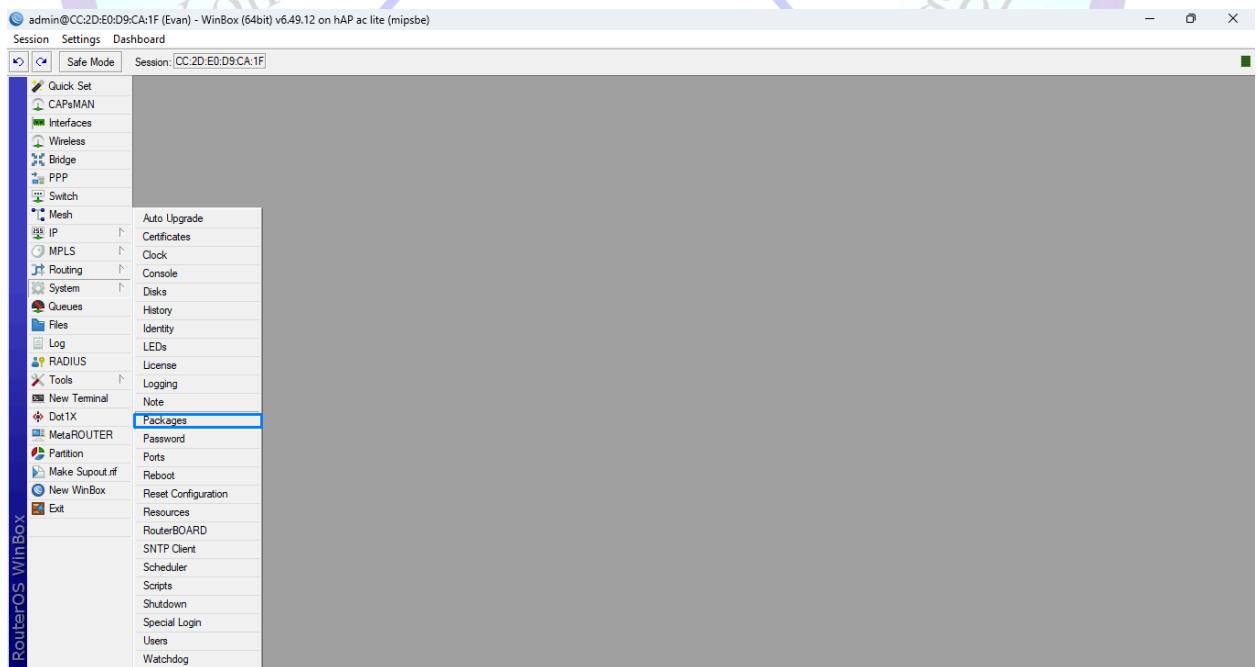


## LAB 4 Disable, Enable, Add Package

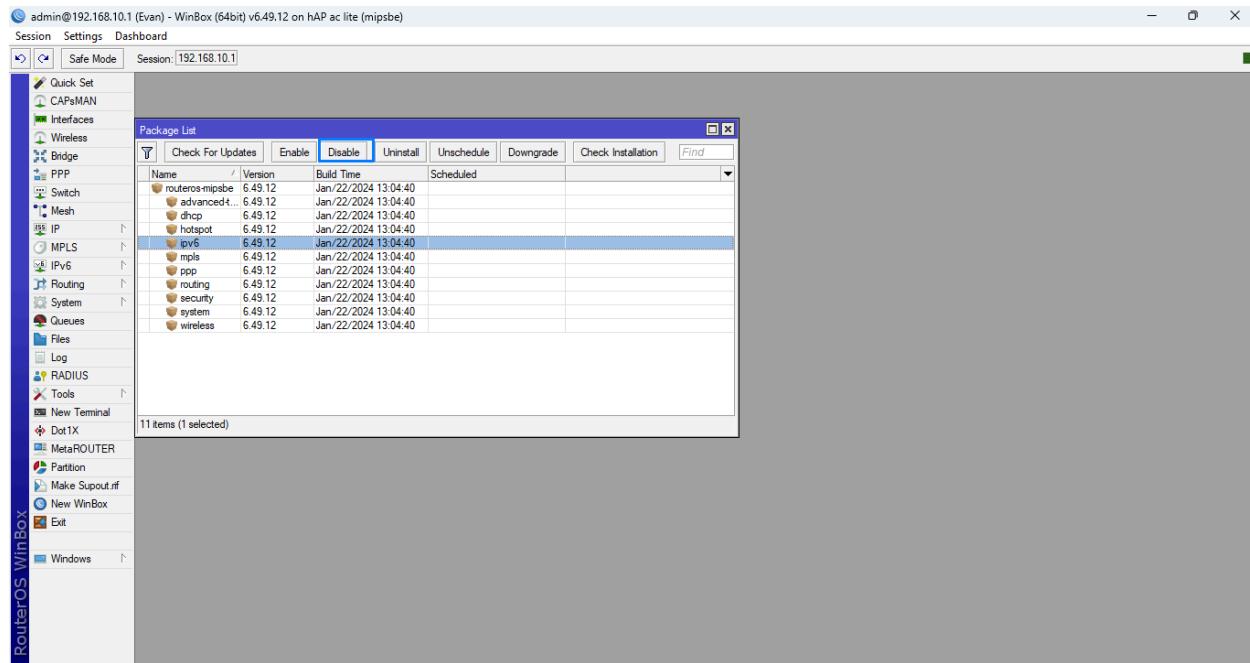
Pada lab 4 ini kita akan mengdisablekan fitur fitur yang tidak digunakan dan mengenablekan fitur yang harus digunakan.

### A. Mendisable Packages

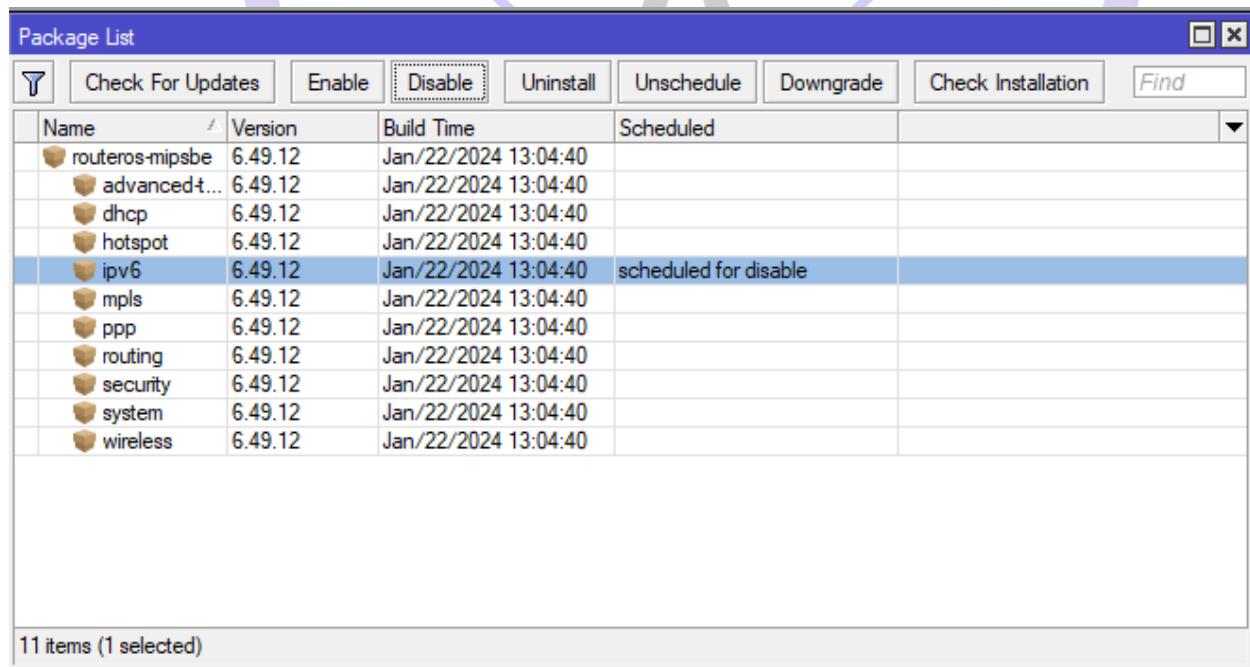
1. Langkah pertama kalian masuk pada system> packages



2. Jika sudah masuk packages kalian klik disable, disini ipv6 akan sebagai contoh mendisablekan.

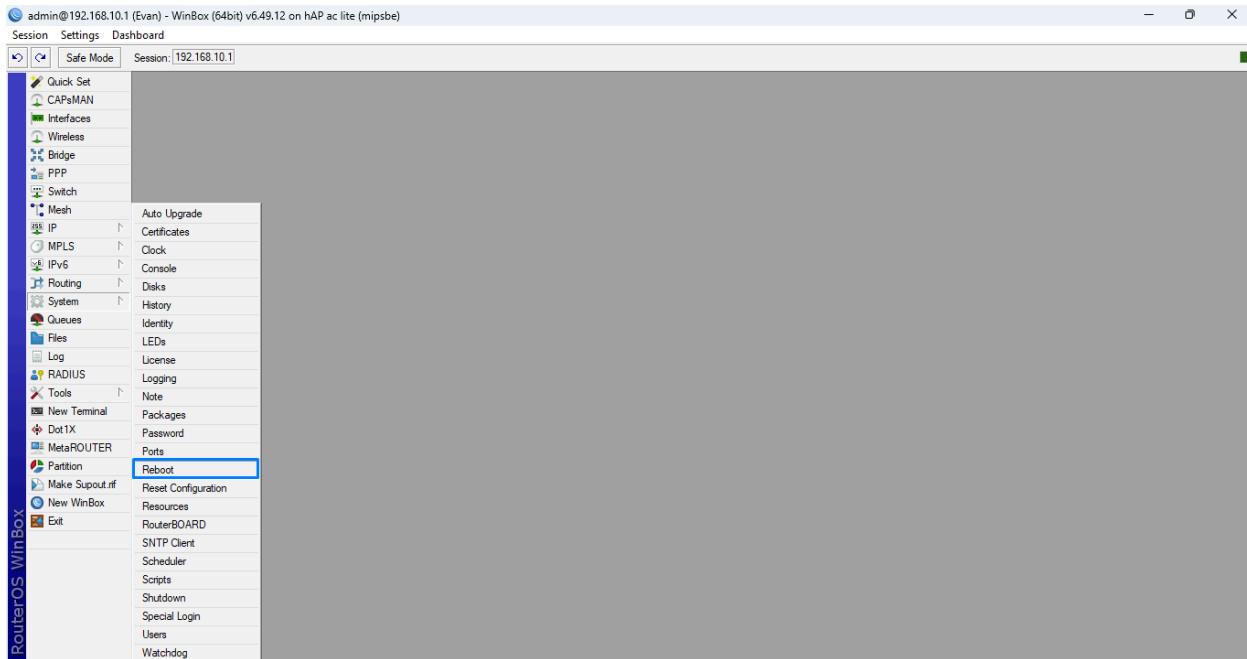


3. Jika kalian pencet disable pada ipv6 maka akan muncul tulisan di sebelah kanannya

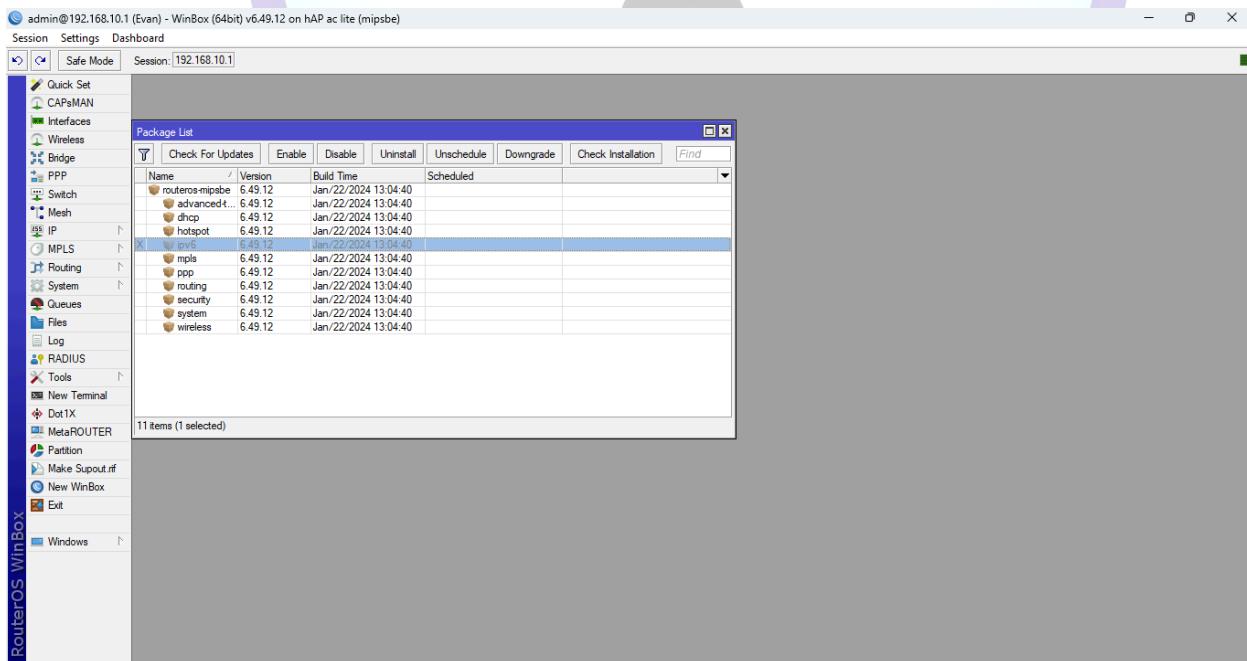




#### 4. Langkah berikutnya masuk ke system>reboot



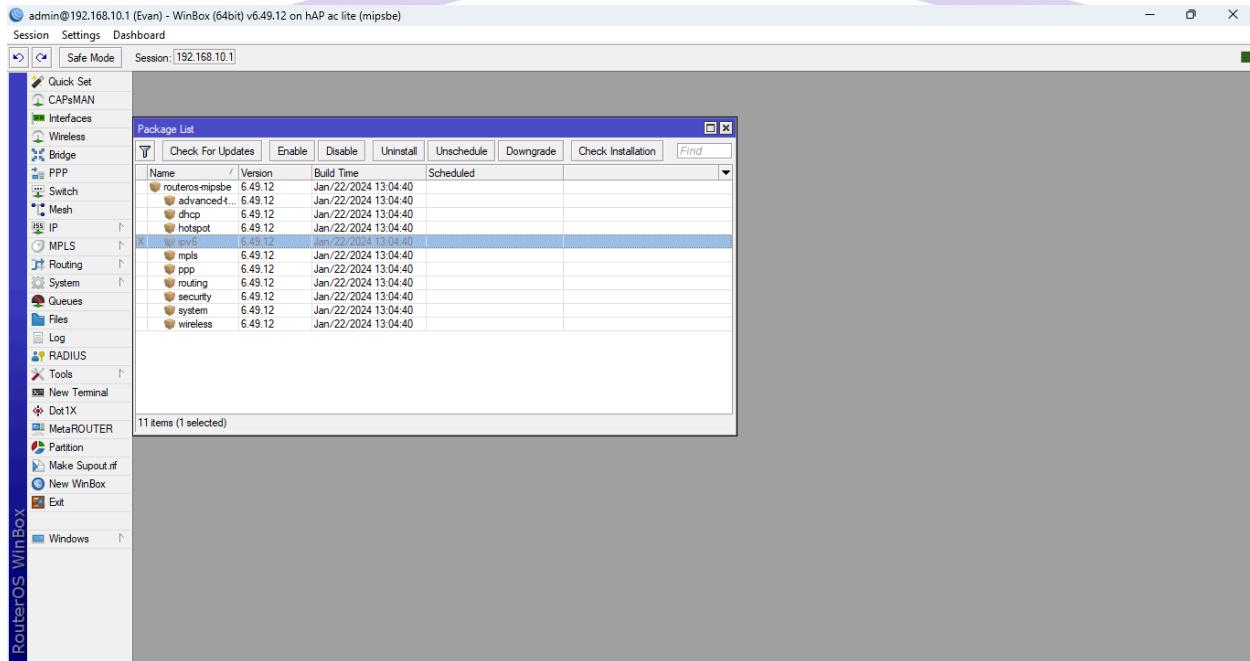
#### 5. Jika sudah di reboot maka ipv6 sudah terdisable



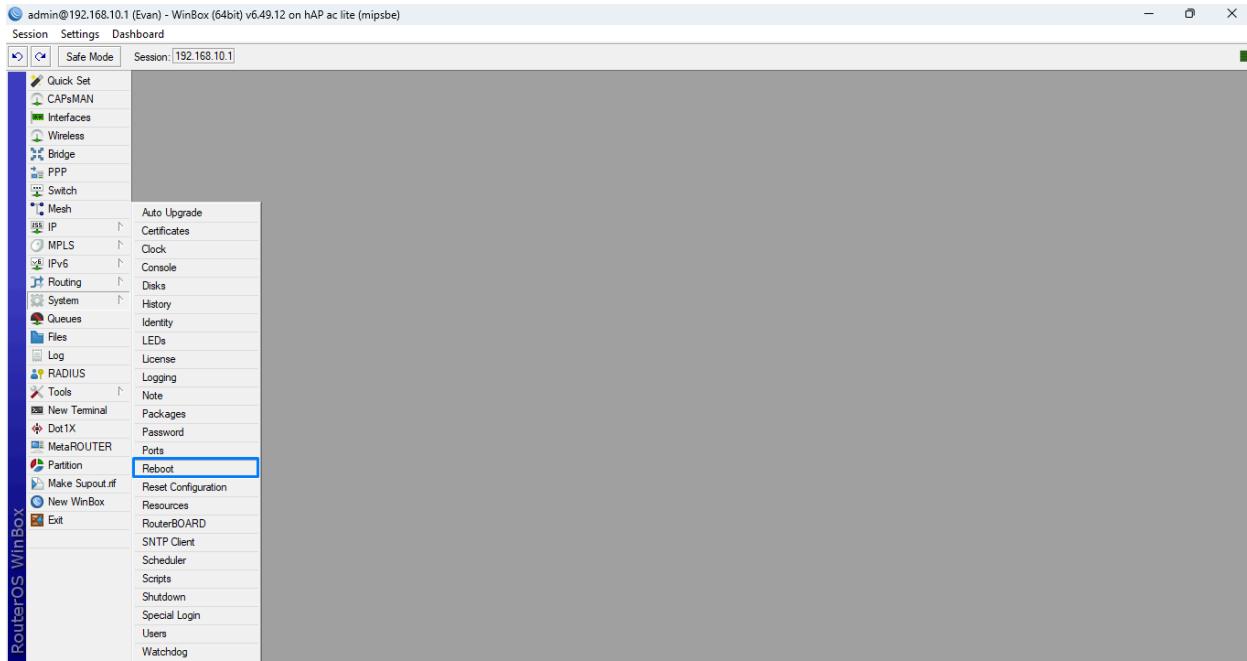


## B. Menenable Packages

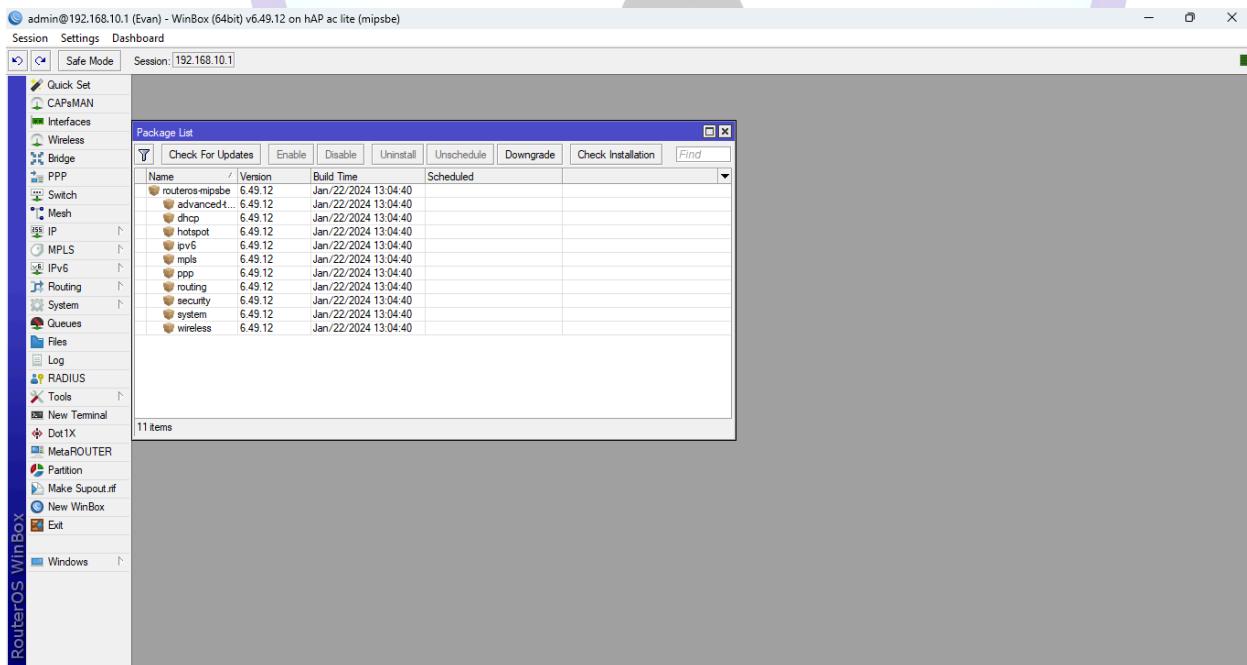
### 1. Kalian klik ipv6 lalu enable



### 2. Jika sudah kalian reboot ulang pada system lalu reboot



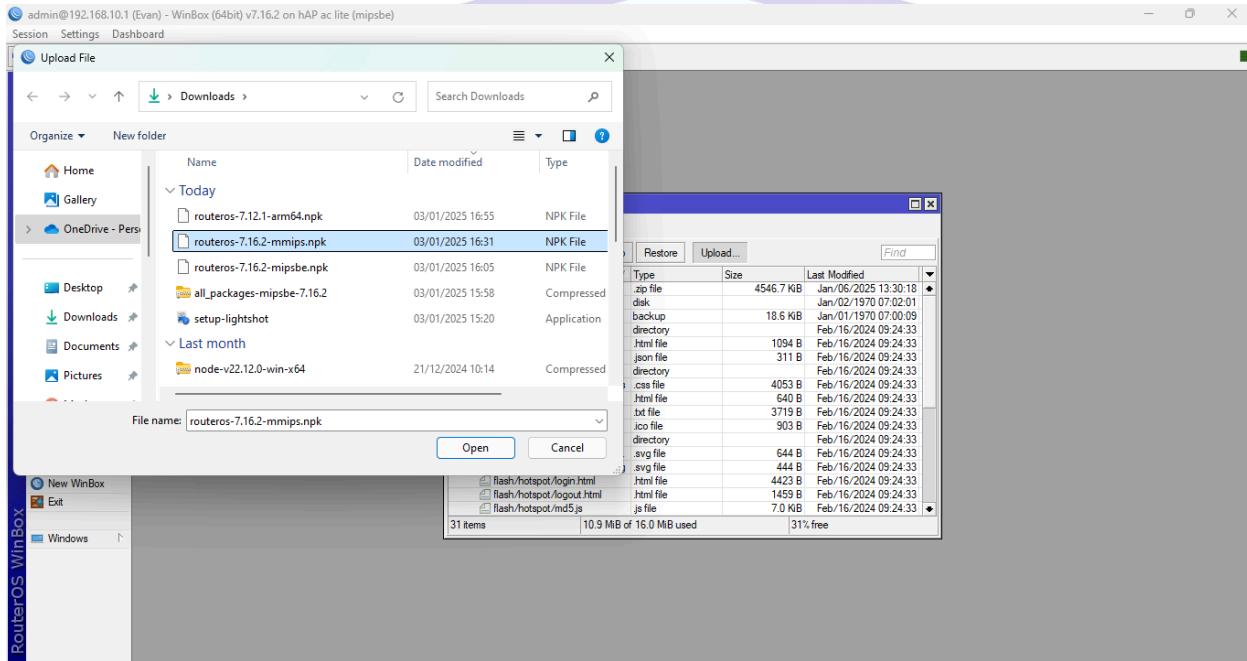
### 3. Jika sudah ter reboot maka ipv6 sudah ter enable kembali





## C. Add Packages

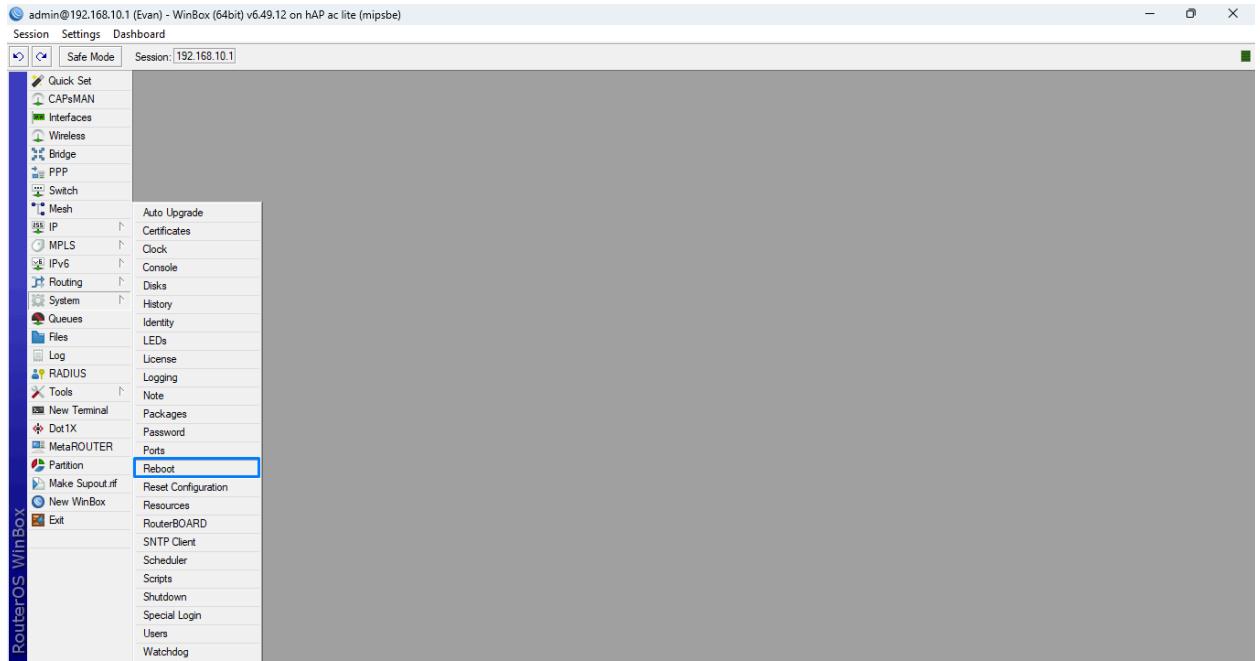
1. Pertama masuk ke winbox seperti biasa
2. Lalu masuk ke file
3. Jika sudah kalian pilih file packages yang ingin kalian tambahkan



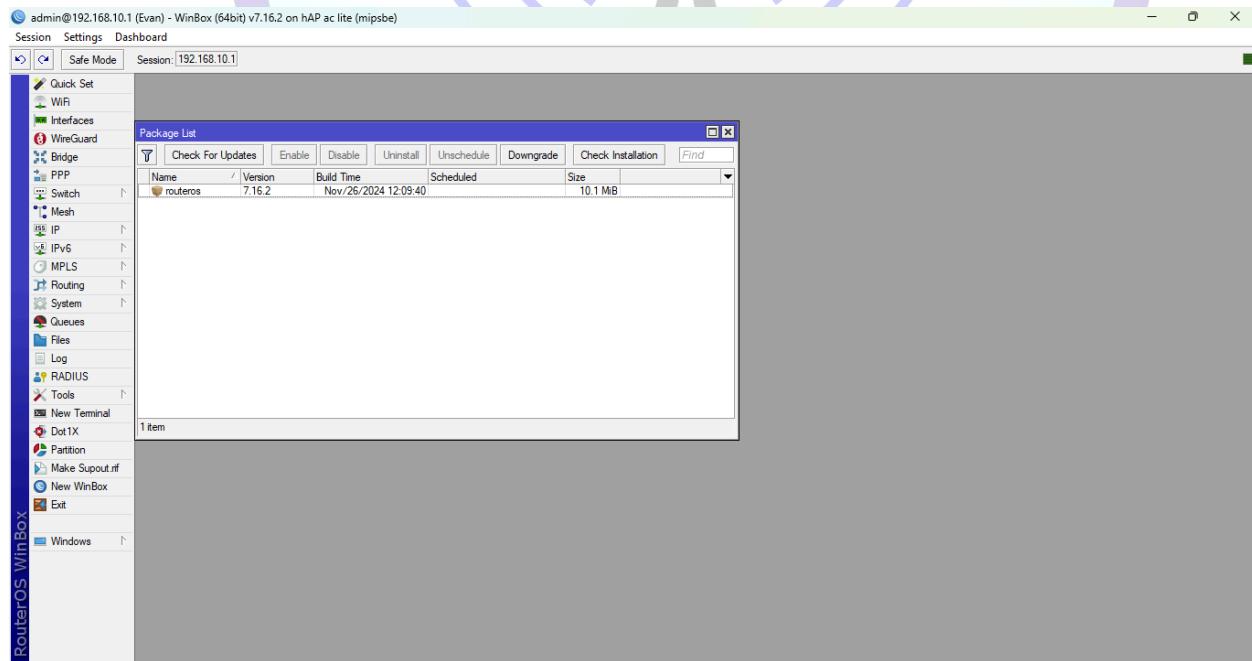
4. File sudah berhasil terupload



5. Berikutnya kalian reboot agar MikroTik dapat menambahkan packages secara otomatis



## 6. Jika sudah di reboot maka sudah berhasil ditambahkan



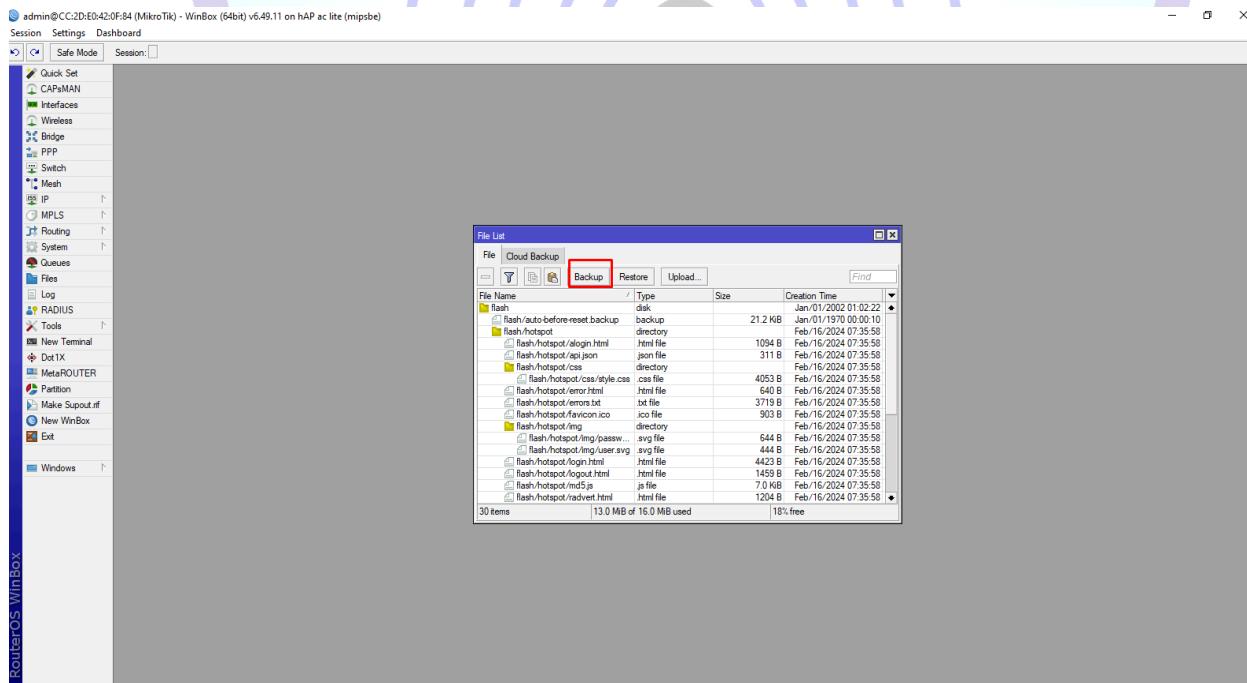


## LAB 5 Backup (.backup) VS Export (.rsc) & Restore VS Import

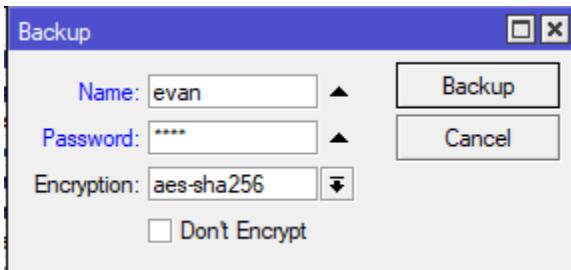
Pada lab 5 ini kita akan belajar mengenai bagaimana cara untuk backup, export, restore dan import file agar konfigurasi kita tidak akan sia sia.

### A. Backup

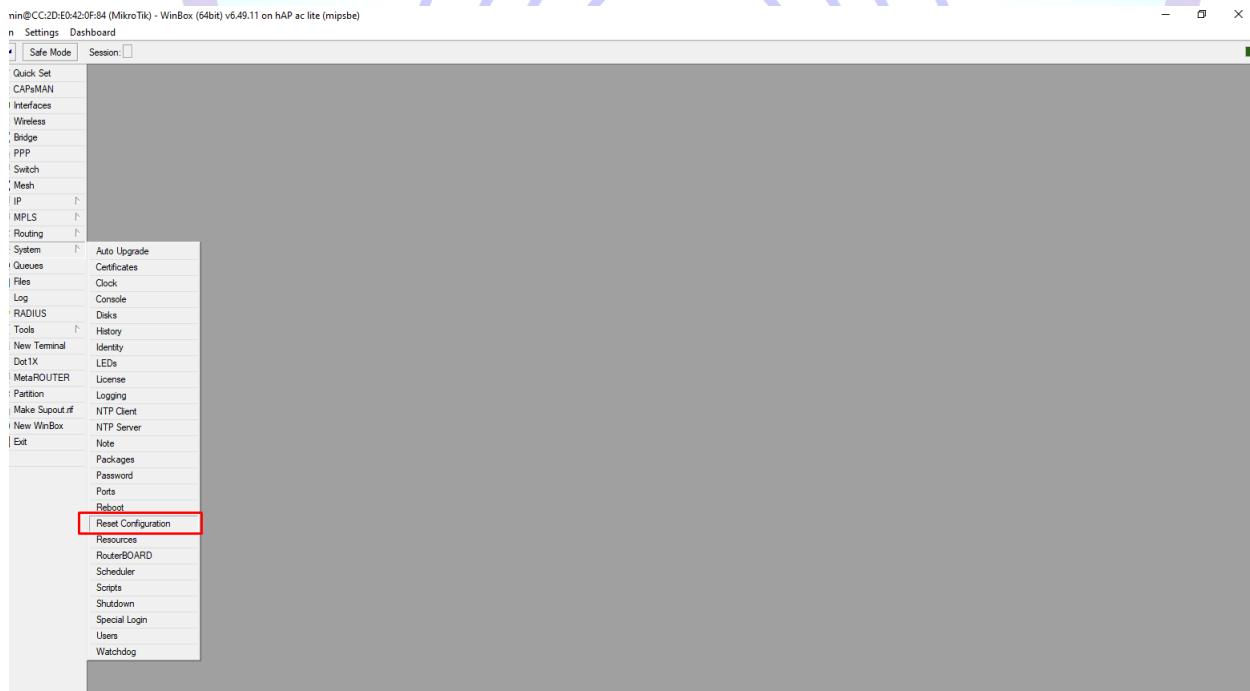
1. Kalian login winbox seperti biasa dengan memasukan username dan pasword
2. Masuk ke dalam file> back up



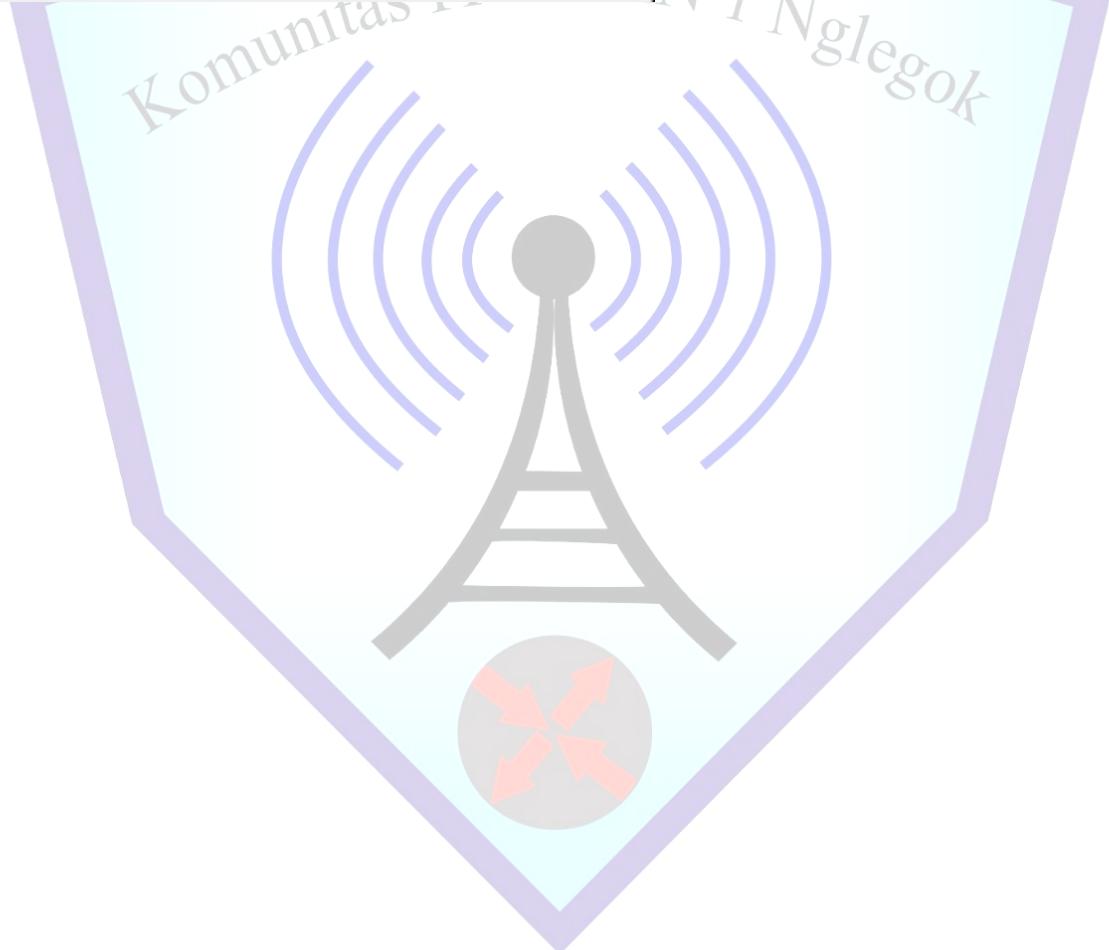
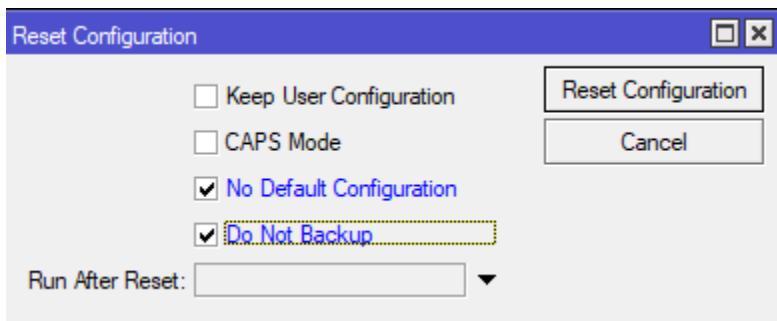
3. Langkah berikutnya kalian Beri nama dan pasword sesuai dengan keinginan kalian sebagai contoh saya akan menggunakan nama evan dan password 1925



4. Jika sudah kalian masuk kedalam system> reset Configuration untuk mencoba back up tadi



5. Pilih sesuai dengan contoh lalu klik reset configuration





## B. Restore

- Untuk merestore konfigurasi kalian masuk ke upload lalu cari dimana kalian menaruh file yang kalian back up tadi

File Name	Type	Size	Creation Time
flash	disk		Jan/01/2002 01:02:22
flash/auto-before-reset.backup	backup	21.2 kB	Jan/01/1970 00:00:10
flash/hotspot	directory		Feb/16/2024 07:35:58
flash/hotspot/alogin.html	html file	1094 B	Feb/16/2024 07:35:58
flash/hotspot/api.json	json file	311 B	Feb/16/2024 07:35:58
flash/hotspot/css	directory		Feb/16/2024 07:35:58
flash/hotspot/css/style.css	.css file	4053 B	Feb/16/2024 07:35:58
flash/hotspot/error.html	html file	640 B	Feb/16/2024 07:35:58
flash/hotspot/errors.txt	txt file	3719 B	Feb/16/2024 07:35:58
flash/hotspot/favicon.ico	ico file	903 B	Feb/16/2024 07:35:58
flash/hotspot/img	directory		Feb/16/2024 07:35:58
flash/hotspot/img/passw...	.svg file	644 B	Feb/16/2024 07:35:58
flash/hotspot/img/user.svg	.svg file	444 B	Feb/16/2024 07:35:58
flash/hotspot/login.html	html file	4423 B	Feb/16/2024 07:35:58
flash/hotspot/logout.html	html file	1459 B	Feb/16/2024 07:35:58
flash/hotspot/md5.js	js file	7.0 kB	Feb/16/2024 07:35:58
flash/hotspot/radvert.html	html file	1204 B	Feb/16/2024 07:35:58

- Jika sudah kalian klik filenya lalu restore



File List				
File		Cloud Backup		
		Backup	Restore	Upload...
File Name	Type	Size	Creation Time	
KITS.backup	backup	22.2 kB	Jan/01/2002 01:01:23	
flash	disk		Jan/01/2002 01:02:22	
flash/auto-before-reset.backup	backup	21.2 kB	Jan/01/1970 00:00:10	
flash/hotspot	directory		Feb/16/2024 07:35:58	
flash/hotspot/alogin.html	.html file	1094 B	Feb/16/2024 07:35:58	
flash/hotspot/api.json	json file	311 B	Feb/16/2024 07:35:58	
flash/hotspot/css	directory		Feb/16/2024 07:35:58	
flash/hotspot/css/style.css	.css file	4053 B	Feb/16/2024 07:35:58	
flash/hotspot/error.html	.html file	640 B	Feb/16/2024 07:35:58	
flash/hotspot/errors.txt	.txt file	3719 B	Feb/16/2024 07:35:58	
flash/hotspot/favicon.ico	ico file	903 B	Feb/16/2024 07:35:58	
flash/hotspot/img	directory		Feb/16/2024 07:35:58	
flash/hotspot/img/passw...	.svg file	644 B	Feb/16/2024 07:35:58	
flash/hotspot/img/user.svg	.svg file	444 B	Feb/16/2024 07:35:58	
flash/hotspot/login.html	.html file	4423 B	Feb/16/2024 07:35:58	
flash/hotspot/logout.html	.html file	1459 B	Feb/16/2024 07:35:58	
flash/hotspot/md5.js	js file	7.0 kB	Feb/16/2024 07:35:58	

3. Masukkan Paswordnya dan tunggu hingga berhasil



File List

File Cloud Backup

Backup Restore Upload... Find

File Name	Type	Size	Creation Time
KITS.backup	backup	22.2 kB	Jan/01/2002 01:01:23
flash	disk		Jan/01/2002 01:02:22
flash/auto-before-reset.backup	backup	21.2 kB	Jan/01/1970 00:00:10

Restore

Backup File: KITS.backup

Password: \*\*

Restore Cancel

flash/hotspot/errors.txt	.txt file	3719 B	Feb/16/2024 07:35:58
flash/hotspot/favicon.ico	.ico file	903 B	Feb/16/2024 07:35:58
flash/hotspot/img	directory		Feb/16/2024 07:35:58
flash/hotspot/img/passw...	.svg file	644 B	Feb/16/2024 07:35:58
flash/hotspot/img/user.svg	.svg file	444 B	Feb/16/2024 07:35:58
flash/hotspot/login.html	.html file	4423 B	Feb/16/2024 07:35:58
flash/hotspot/logout.html	.html file	1459 B	Feb/16/2024 07:35:58
flash/hotspot/md5.js	js file	7.0 kB	Feb/16/2024 07:35:58

31 items (1 selected) | 13.0 MiB of 16.0 MiB used | 18% free



## C. Export

1. Langkah pertama masuk ke dalam new terminal



2. Untuk kita mengembalikan seluruh konfigurasi maka harus mengetikkan perintah  
export file= "nama file"
3. Sebagai contoh adalah file print

```
Terminal <1>
MikroTik RouterOS 6.49.11 (c) 1999-2023          http://www.mikrotik.com/

Do you want to see the software license? [Y/n]: n
[?]           Gives the list of available commands
command [?]   Gives help on the command and list of arguments

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

/             Move up to base level
..            Move up one level
/command      Use command at the base level
nov/25/2024 17:09:58 system,error,critical login failure for user admin from F4:4D
:30:9D:6E:C5 via winbox
[admin@TKJ] > export file="print"
```

4. Berikutnya jika ingin kalian melihat file apa saja yang sudah kalian export dengan menggunakan perintah "file print"



```
Terminal <1>
[admin@TKJ] > file print
# NAME                      TYPE          SIZE CREATION-TIME
0 print.rsc                 script        1465 jan/06/2025 16:27:22
1 flash/pub                  directory     jan/01/2002 08:02:22
2 flash                       disk          jan/01/2002 08:02:22
3 flash/skins                directory     jan/01/1970 07:00:07
4 flash/hotspot               directory     feb/16/2024 14:35:58
5 flash/hotspot/alogin...    .html file    1094 feb/16/2024 14:35:58
6 flash/hotspot/api.json     .json file    311 feb/16/2024 14:35:58
7 flash/hotspot/css          directory     feb/16/2024 14:35:58
8 flash/hotspot/css/st...    .css file    4053 feb/16/2024 14:35:58
9 flash/hotspot/error....   .html file    640 feb/16/2024 14:35:58
10 flash/hotspot/errors...   .txt file    3719 feb/16/2024 14:35:58
11 flash/hotspot/favico...   .ico file    903 feb/16/2024 14:35:58
12 flash/hotspot/img         directory     feb/16/2024 14:35:58
13 flash/hotspot/img/pa...   .svg file    644 feb/16/2024 14:35:58
14 flash/hotspot/img/us...   .svg file    444 feb/16/2024 14:35:58
15 flash/hotspot/login....  .html file    4423 feb/16/2024 14:35:58
16 flash/hotspot/logout...   .html file    1459 feb/16/2024 14:35:58
17 flash/hotspot/md5.js      .js file     7.0KiB feb/16/2024 14:35:58
18 flash/hotspot/radver...   .html file    1204 feb/16/2024 14:35:58
19 flash/hotspot/redire...   .html file    330 feb/16/2024 14:35:58
20 flash/hotspot/rlogin...   .html file    877 feb/16/2024 14:35:58
21 flash/hotspot/status...   .html file    2855 feb/16/2024 14:35:58
```

## D. Import

1. Jika kalian ingin mengimport file kalian maka contoh perintah di bawah ini

```
[admin@TKJ] > import file-name=name-nama filekalian.rsc
```

2. Maka kalian akan mengimport file tanpa melakukan reboot

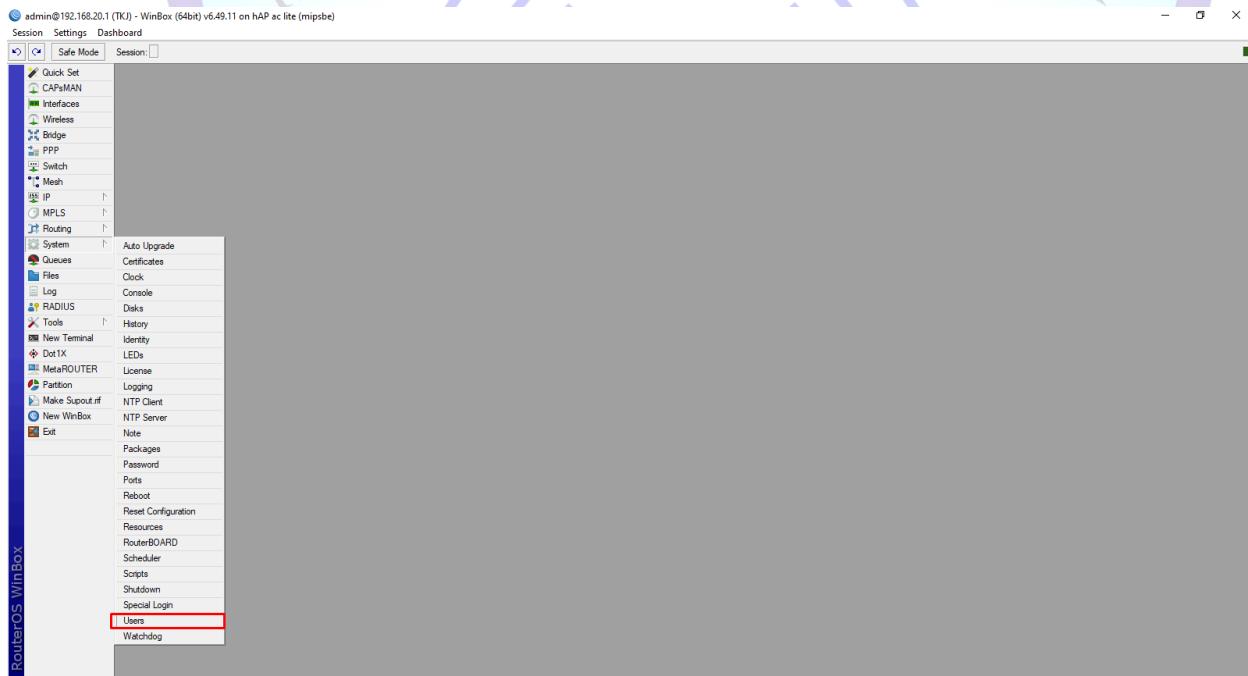


## LAB 6 Manajemen User and Group

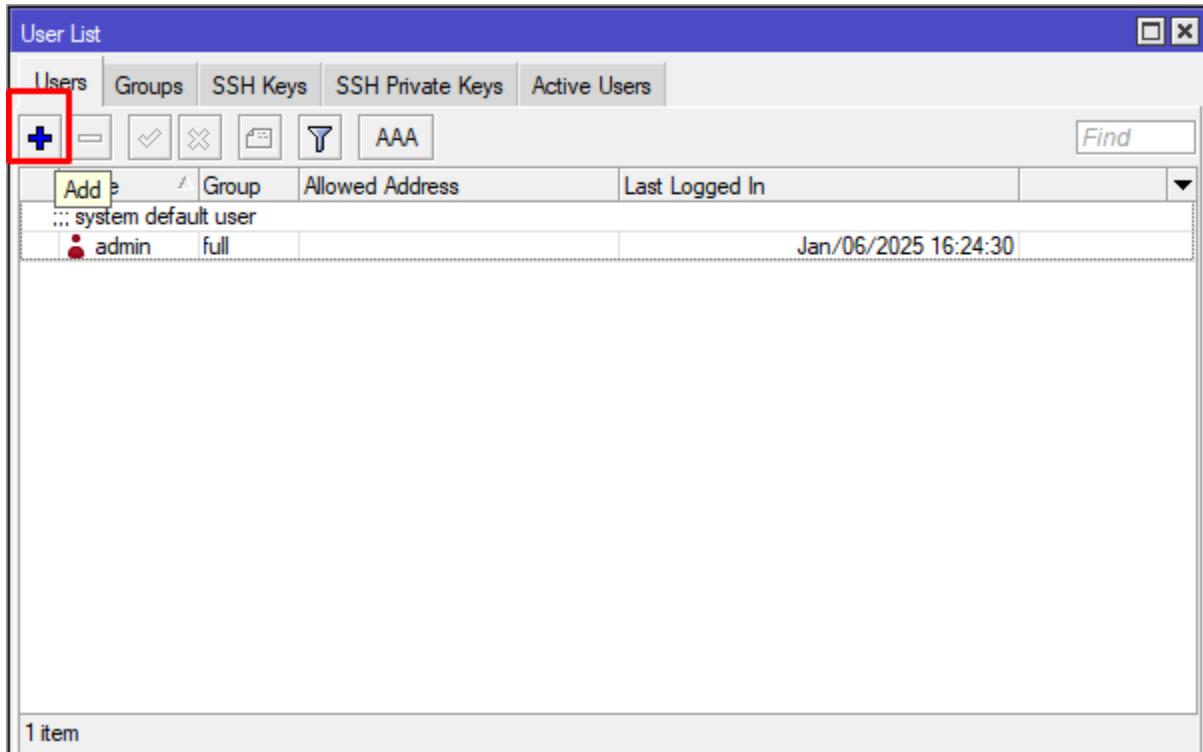
Di lab berikutnya yaitu lab 6 kita akan belajar apa itu dan bagaimana cara melakukan Manajemen User and Group.

### A. Manajemen User

1. Langkah pertama untuk Manajemen User adalah Kalian masuk ke System> Users



2. Disini kita akan menambahkan users kedalam router dengan cara klik tombol +



3. Tambahkan nama dan juga pasword jika kalian ingin menambahkan pasword ke dalam users kalian

New User

Name:	Evan
Group:	Evan
Allowed Address:	
Last Logged In:	
Password:	
Confirm Password:	

enabled      expired

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Expire Password



4. Untuk melihat users yang aktif kalian masuk ke dalam active users dan terlihat users admin yang sedang aktif

The screenshot shows the 'User List' window in Winbox. The title bar says 'User List'. Below it is a navigation bar with tabs: 'Users', 'Groups', 'SSH Keys', 'SSH Private Keys', and 'Active Users'. The 'Active Users' tab is highlighted with a red box. A search bar labeled 'Find' is to the right of the tabs. The main area is a table with columns: Name, At, From, Via, and Group. One row is visible, showing 'admin' with 'Nov/25/2024 17:10:24' in the 'At' column, '192.168.20.254' in the 'From' column, 'winbox' in the 'Via' column, and 'full' in the 'Group' column. At the bottom left of the table area, it says '1 item'.

Name	At	From	Via	Group
admin	Nov/25/2024 17:10:24	192.168.20.254	winbox	full



## B. Management Groups

1. Masuk ke dalam Groups lalu klik tombol + untuk menambahkan group baru

The screenshot shows the 'User List' window with the 'Groups' tab selected. The toolbar at the top has tabs for 'Users', 'Groups' (which is highlighted), 'SSH Keys', 'SSH Private Keys', and 'Active Users'. Below the toolbar is a search bar with a 'Find' button. The main area is a table with columns 'Name', 'Policies', and 'Skin'. There are three rows: 'full' (Policy: local telnet ssh ftp reboot read write policy test winbox password web sniff s... Skin: default), 'read' (Policy: local telnet ssh reboot read test winbox password web sniff s... Skin: default), and 'write' (Policy: local telnet ssh reboot read write test winbox password web ... Skin: default). At the bottom left of the table area, it says '3 items'. The '+' button in the toolbar is highlighted with a red box.

Name	Policies	Skin
S full	local telnet ssh ftp reboot read write policy test winbox password web sniff s...	default
S read	local telnet ssh reboot read test winbox password web sniff s...	default
S write	local telnet ssh reboot read write test winbox password web ...	default

2. Kalian masukkan nama sesuai dengan keinginan kalian lalu kalian bisa memilih akses yang ingin kalian pilih. Disini saya sebagai contoh mencentang semua



New Group

Name:	Evan	OK
Policies:	<input checked="" type="checkbox"/> local <input checked="" type="checkbox"/> telnet <input checked="" type="checkbox"/> ssh <input checked="" type="checkbox"/> ftp <input checked="" type="checkbox"/> reboot <input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> write <input checked="" type="checkbox"/> policy <input checked="" type="checkbox"/> test <input checked="" type="checkbox"/> winbox <input checked="" type="checkbox"/> password <input checked="" type="checkbox"/> web <input checked="" type="checkbox"/> sniff <input checked="" type="checkbox"/> sensitive <input checked="" type="checkbox"/> api <input checked="" type="checkbox"/> romon <input checked="" type="checkbox"/> dude <input checked="" type="checkbox"/> tikapp	Cancel
Skin:	default	Apply
Comment		
Copy		
Remove		

System

3. Jika sudah muncul maka sudah berhasil untuk membuat Group baru

User List

Users	Groups	SSH Keys	SSH Private Keys	Active Users
Evan		local telnet ssh ftp reboot read write policy test winbox passw...	default	
full		local telnet ssh ftp reboot read write policy test winbox passw...	default	
read		local telnet ssh reboot read test winbox password web sniff s...	default	
write		local telnet ssh reboot read write test winbox password web ...	default	

Find

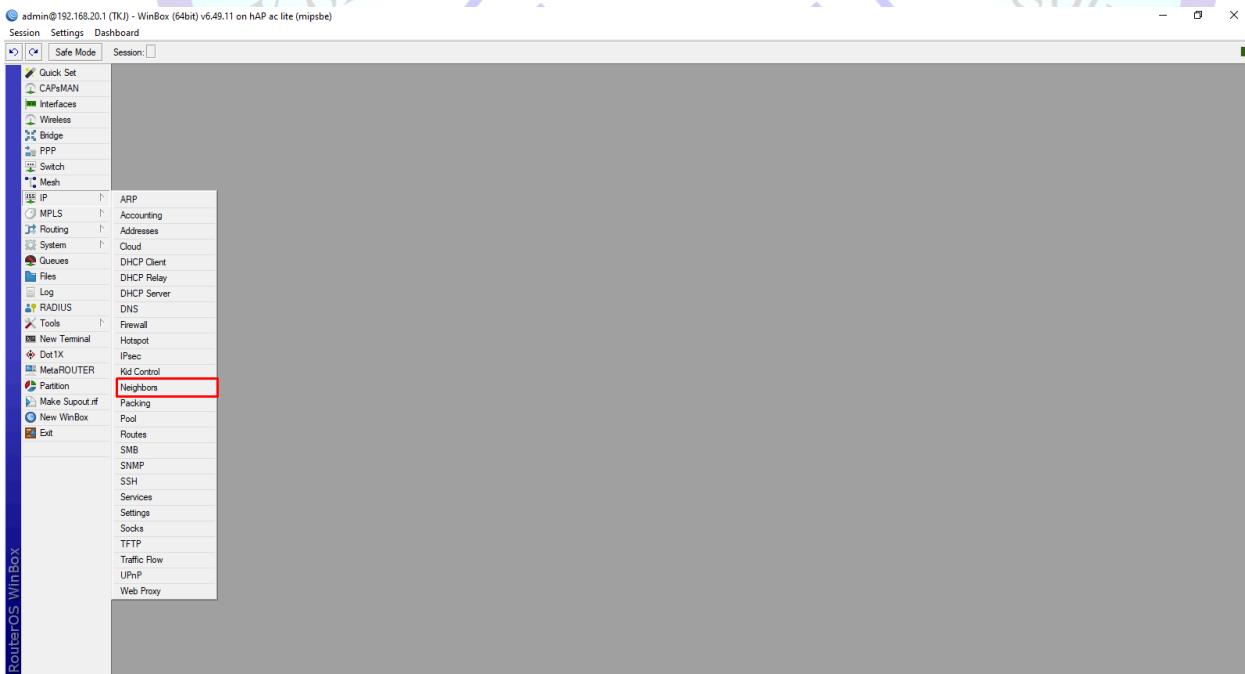
4 items



## LAB 7 MNDP (Mikrotik Neighbour Discovery Protocol)

Pada lab ini kita akan belajar mengenai protokol yang memungkinkan perangkat MikroTik saling mendeteksi dan berbagi informasi seperti nama perangkat, alamat IP, versi RouterOS, dan tipe perangkat di jaringan lokal. Protokol ini bekerja otomatis tanpa konfigurasi manual, memudahkan pengelolaan dan komunikasi antar perangkat MikroTik dalam jaringan yang sama.

1. Login ke dalam winbox
  2. Lalu masuk ke IP > Neighbors



3. Jika sudah masuk ke dalam Neighbors maka tampilannya akan seperti ini



Neighbor List										
Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime	▼
ether1	192.168.103.19	DC:2C:6E:AB:27:50	MikroTik	MikroTik	6.49.12 (...)	RB951Ui-...	no	2	00:46:18	
ether1	192.168.103.42	CC:2D:E0:A4:97:38	deviatul	MikroTik	6.49.12 (...)	RB952Ui-...	no	18	01:38:53	
ether1		00:0C:42:D6:B6:C4	MikroTik	MikroTik	6.49.16 (...)	RB951Ui-...	no	5	00:02:19	
ether1	192.168.103.254	C4:AD:34:CF:ED:0F	Core-TKJ	MikroTik	6.49.7 (st...)	RB1100x4	no	22	4d 06:47:09	
ether1	192.168.103.47	CC:2D:E0:D9:CB:BB	afifatul	MikroTik	6.49.17 (...)	RB952Ui-...	no	23	00:36:01	
ether1		64:00:6A:0D:27:D7					no	2986	00:00:00	
ether1	192.168.103.49	CC:2D:E0:D9:BF:19	MikroTik	MikroTik	6.49.12 (...)	RB952Ui-...	no	26	00:44:18	
ether1	192.168.15.5	6C:3B:6B:DA:62:A0	jihan	MikroTik	6.49.17 (...)	RB951Ui-...	no	57	00:12:37	
ether1		64:00:6A:0C:19:3F					no	133	00:00:00	
ether2		F4:4D:30:9D:6E:C5					no	418	00:00:00	

4. Jika kalian ingin mengatur Neighbors kalian pilih menu Discovery Settings dan sebagai contoh saya akan mengubah interface menjadi static

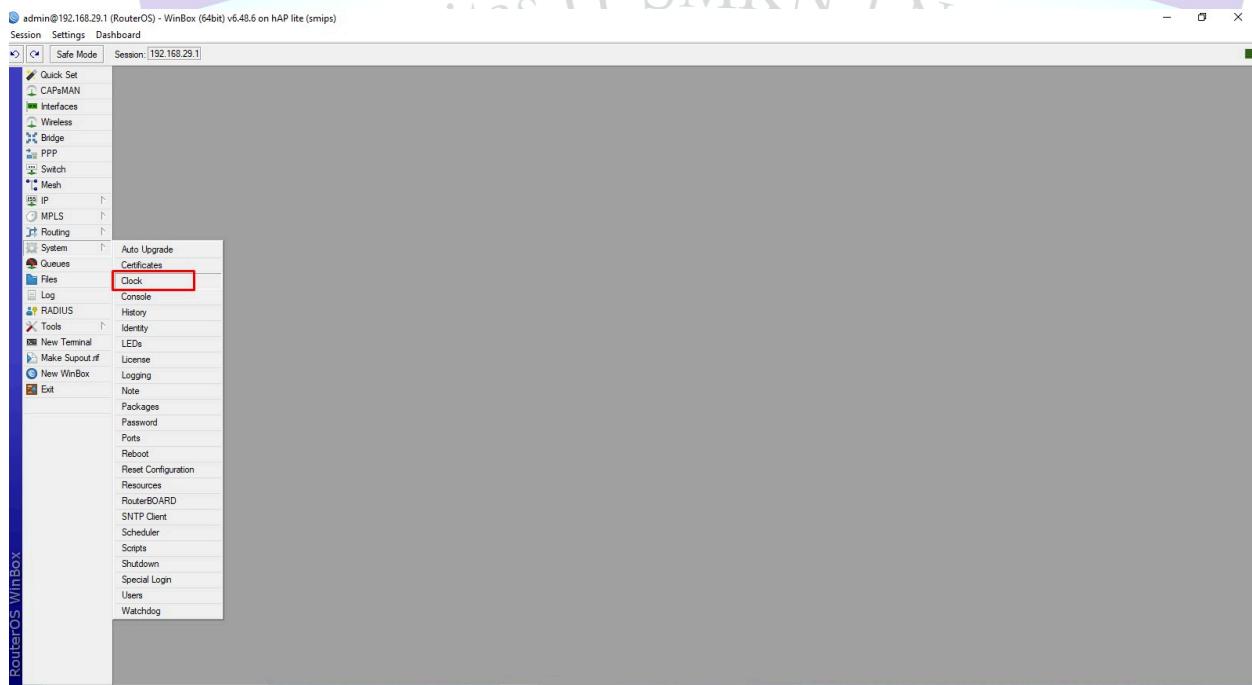
Neighbor List										
Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime	▼
ether1	192.168.103.19	DC:2C:6E:AB:27:50	MikroTik	MikroTik	6.49.12 (...)	RB951Ui-...	no	8	00:47:18	
ether1	192.168.103.42	CC:2D:E0:A4:97:38	deviatul	MikroTik	6.49.12 (...)	RB952Ui-...	no	25	01:39:53	
ether1		00:0C:42:D6:B6:C4	MikroTik	MikroTik	6.49.16 (...)	RB951Ui-...	no	72	00:02:19	
ether1	192.168.103.49	CC:2D:E0:D9:BF:19	MikroTik	MikroTik	6.49.12 (...)	RB952Ui-...	no	29	4d 06:48:09	
ether1	192.168.15.5	6C:3B:6B:DA:62:A0	jihan	MikroTik	6.49.17 (...)	RB951Ui-...	no	30	00:37:01	
ether1		64:00:6A:0C:19:3F					no	3052	00:00:00	
ether1	192.168.103.254	C4:AD:34:CF:ED:0F	Core-TKJ	MikroTik	6.49.7 (st...)	RB1100x4	no	33	00:45:18	
ether1	192.168.103.47	CC:2D:E0:D9:CB:BB	afifatul	MikroTik	6.49.17 (...)	RB952Ui-...	no	3	00:14:37	
ether1		64:00:6A:0D:27:D7					no	199	00:00:00	
ether2		F4:4D:30:9D:6E:C5					no	485	00:00:00	



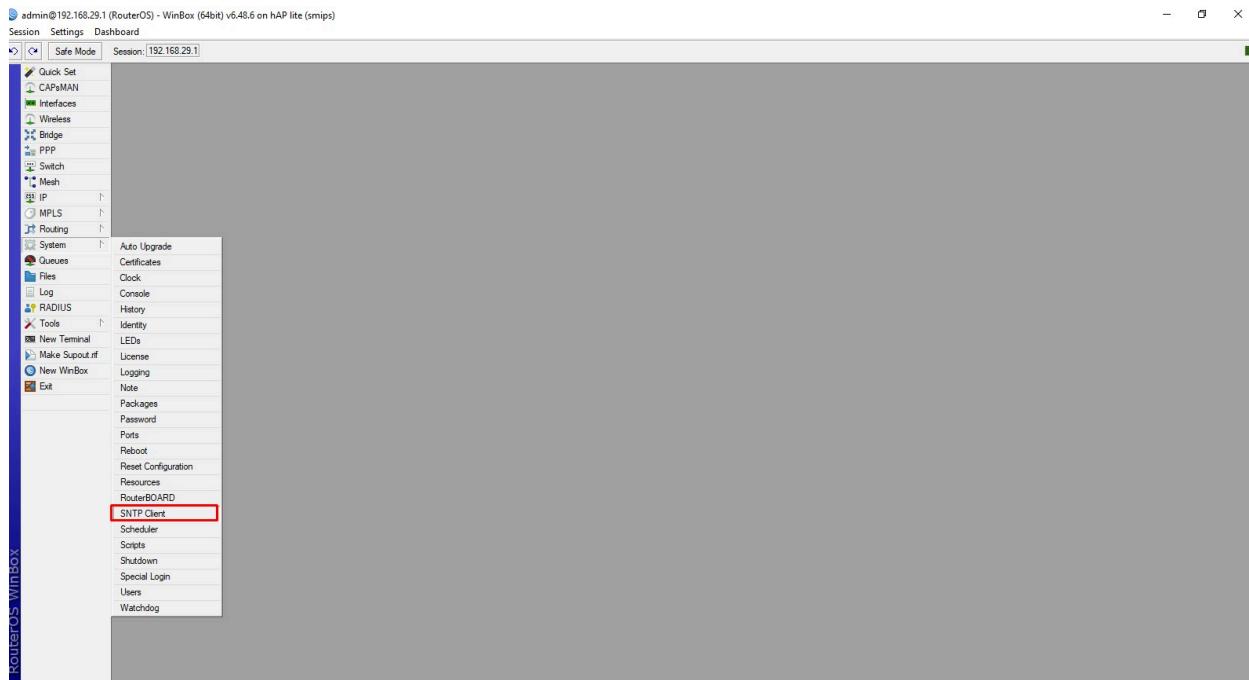
## LAB 8 NTP and Clock

### A.NTP Client

1. Login ke dalam winbox
2. Pilih system lalu clock



3. Sebelum kita melakukan NTP Client kita harus tersambung kedalam internet
4. Setelah itu pilih system>SNTP Client



5. Kemudian kalian Centang pada bagian Enabled. Lalu kalian masukan nama server yang akan kita jadikan NTP Server, disini saya memasukkan server 1.id.pool.ntp.org kemudian Apply > OK.

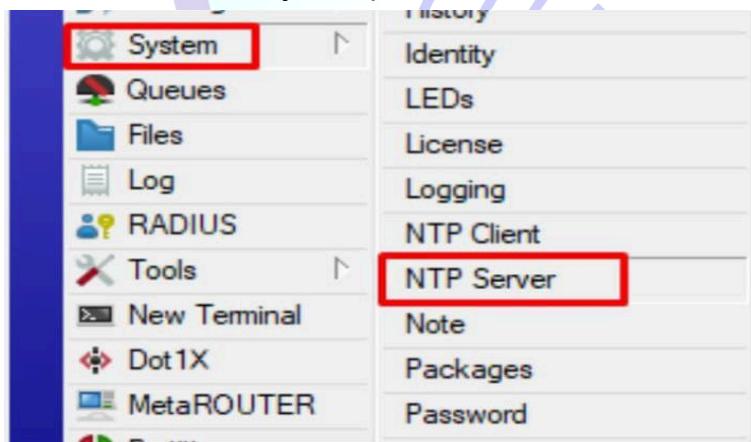
## B. NTP Server

1. Masuk ke dalam winbox
2. Setelah itu kalian buat konfigurasi ntp client dahulu
3. Jika sudah masuk ke system Package

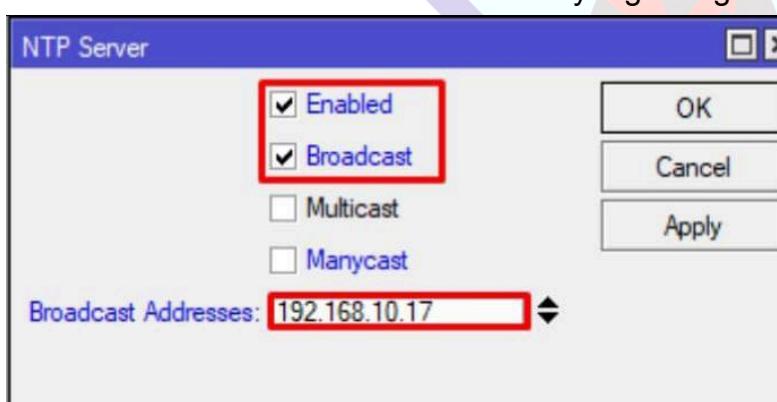


Name	Version	Build Time	Scheduled
ntp	6.49.12	Jan/22/2024 13:04:40	
routeros-mipsbe	6.49.12	Jan/22/2024 13:04:40	
advancedt...	6.49.12	Jan/22/2024 13:04:40	
dhcp	6.49.12	Jan/22/2024 13:04:40	
hotspot	6.49.12	Jan/22/2024 13:04:40	
pv6	6.49.12	Jan/22/2024 13:04:40	
mpls	6.49.12	Jan/22/2024 13:04:40	
ppp	6.49.12	Jan/22/2024 13:04:40	
routing	6.49.12	Jan/22/2024 13:04:40	
security	6.49.12	Jan/22/2024 13:04:40	
system	6.49.12	Jan/22/2024 13:04:40	
wireless	6.49.12	Jan/22/2024 13:04:40	

4. Setelah itu kalian install Package ntp, maka yang tadinya sntp sekarang telah berubah menjadi ntp server



5. Jika kalian sudah masuk ke menu ntp server maka kalian enable dan brodcast. Setelah itu kalian isikan brodcast yang mengarah ke client



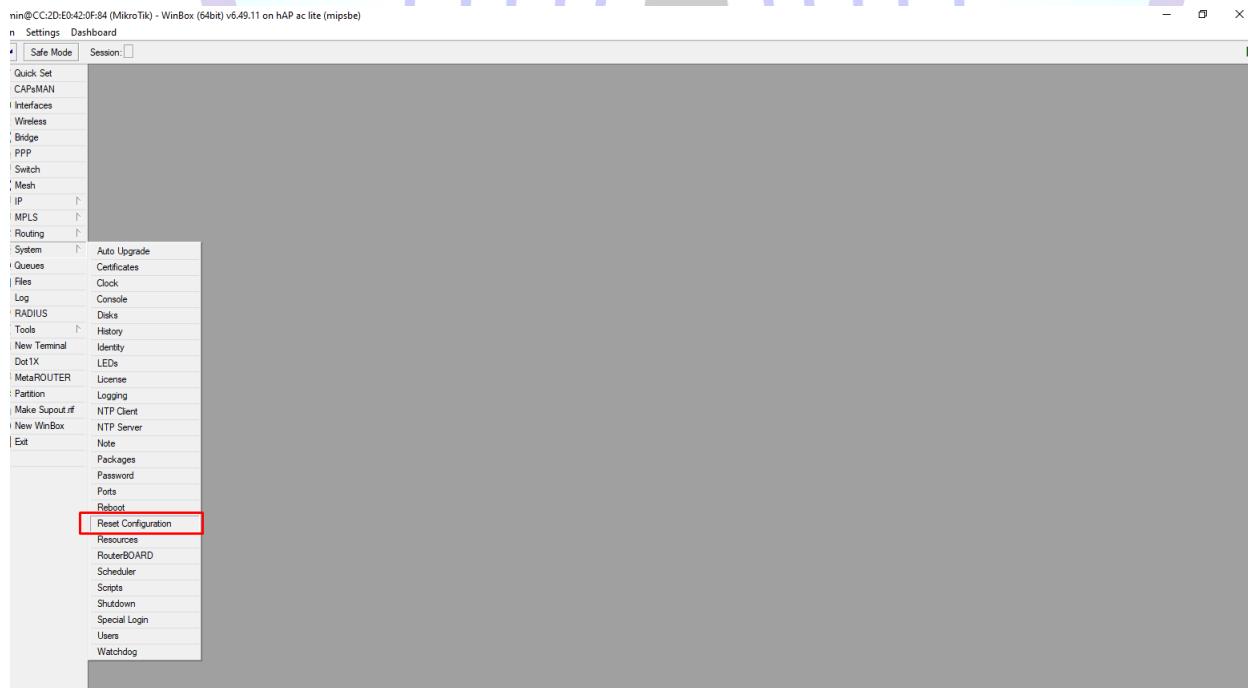


## LAB 9 Soft & Hard Reset Device

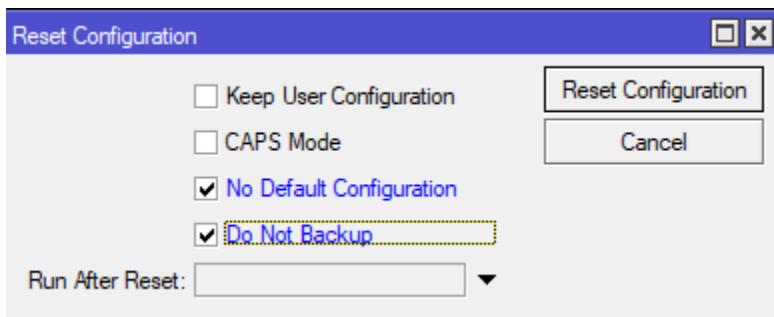
Pada lab ini kita akan melakukan 2 cara untuk melakukan riset pada Mikrotik yaitu Hard & Soft reset. reset adalah reset tanpa menghapus konfigurasi. Hard reset adalah reset dengan menghapus seluruh konfigurasi/mengembalikan ke setelan Pabrik

### A. Soft Reset

1. Langkah pertama seperti biasa kalian login menggunakan Winbox
2. Kalian masuk ke dalam system lalu reset configuration



3. Berikutnya kalian centang 2 terbawah



- Setelah itu maka kalian sudah reset mikrotik dan jika kalian masuk kembali maka akan seperti baru.

## B. Hard Reset

- Langkah pertama kalian lihat pada mikrotik
- Berikutnya lepas semua kabel yang tertancap pada mikrotik
- Setelah itu klik tombol sesuai dengan gambar



- Klik hingga kedip lalu mati kembali

Hard Reset digunakan saat keadaan terdesak, jika kalian tidak dalam kondisi terdesak saran saya kalian menggunakan soft reset karena memiliki sedikit resiko.

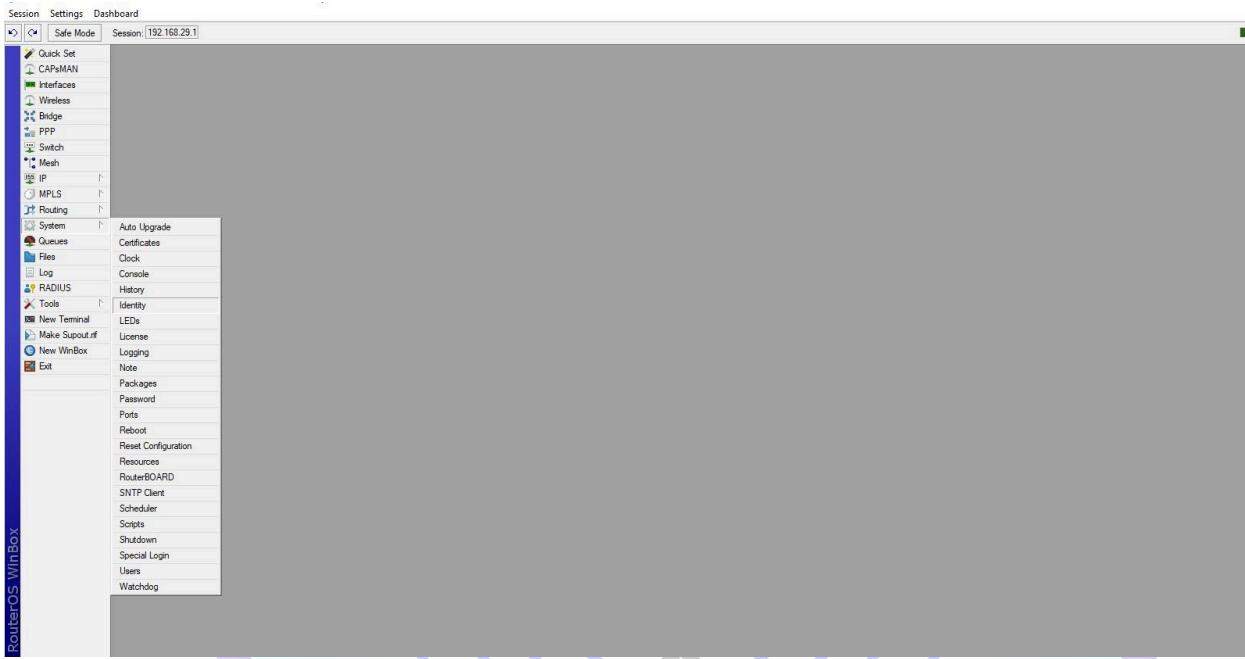


## LAB 10 Router Identity & Mikrotik Misc (Trace Route, Torch, Bandwidth Test, Interface Traffic Monitor,Ping Tool, System Logging, Rommon)

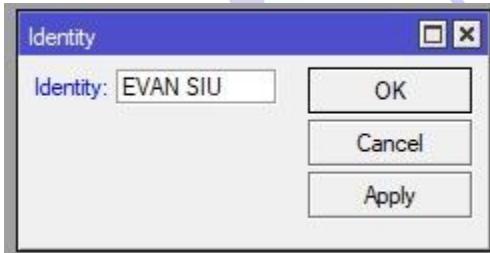
### A.MikroTik Identity

Disini kita akan belajar cara untuk mengubah nama identitas di mikrotik

1. Langkah pertama login winbox
2. Lalu berikutnya system>identity



3. Ubah nama mikrotik kalian sesuai dengan keinginan kalian



## B.Trace Route

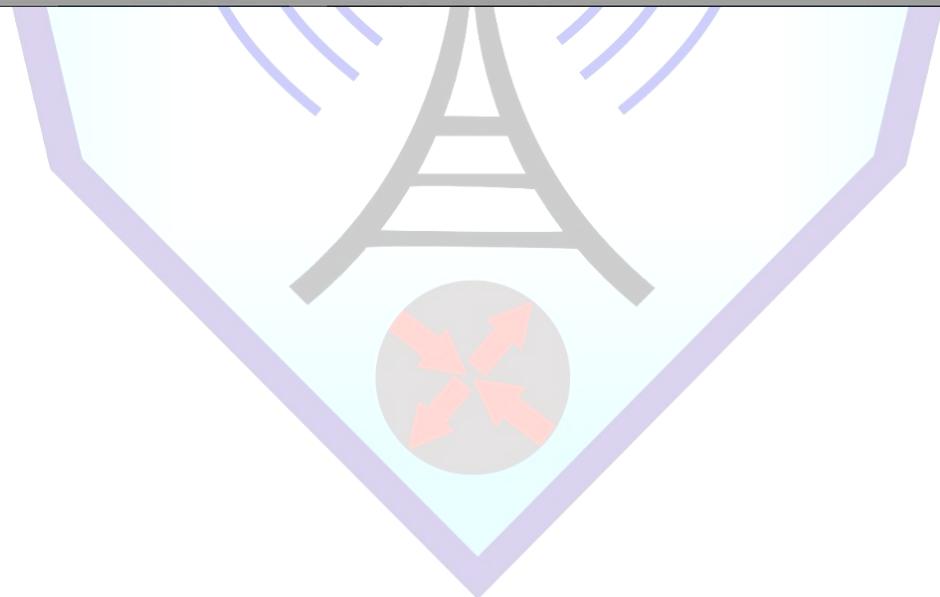
Traceroute di MikroTik digunakan untuk melacak jalur paket data menuju tujuan, menunjukkan setiap hop yang dilalui dan waktu tempuhnya. Ini membantu mendiagnosis masalah jaringan, seperti keterlambatan atau gangguan.



Disini saya mencoba ping ke blog saya

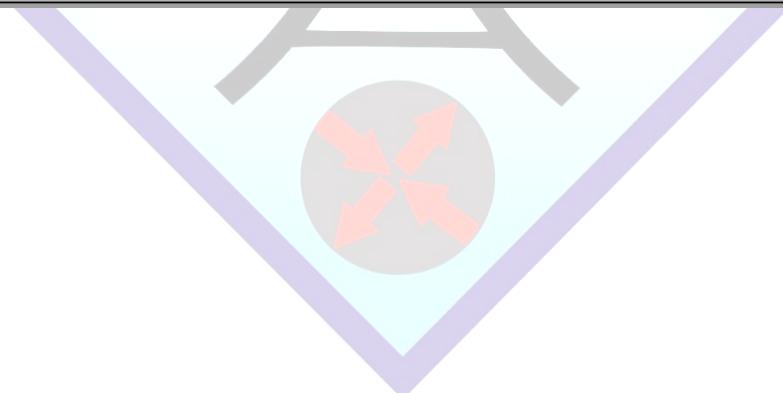
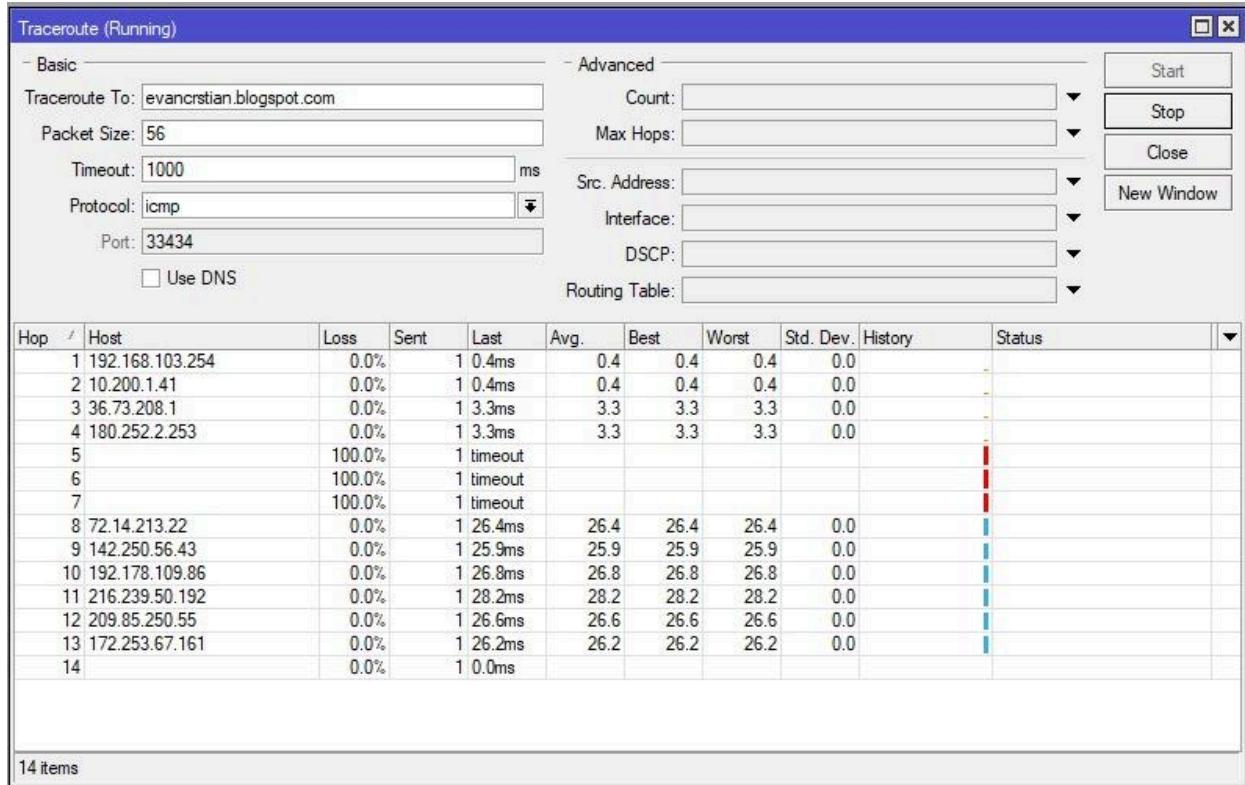
```
Terminal <1>
jan/02/1970 00:00:27 system,error,critical login failure for user admin from 88:AE :DD:84:C1:63 via winbox
jan/02/1970 00:00:54 system,error,critical login failure for user admin from 88:AE :DD:84:C1:63 via winbox
jan/09/2025 09:15:56 system,error,critical router was rebooted without proper shutdown
[admin@EVAN SIU] > tool traceroute address=evancrstian.blogspot.com
# ADDRESS           LOSS SENT LAST AVG BEST WORST
1 192.168.103.254      0%   1  0.4ms  0.4  0.4  0.4
2 10.200.1.41          0%   1  0.5ms  0.5  0.5  0.5
3 36.73.208.1          0%   1  2.4ms  2.4  2.4  2.4
4 180.252.2.253        0%   1  3.1ms  3.1  3.1  3.1
5                      100%  1 timeout
6                      100%  1 timeout
7 180.240.204.194      0%   1  26.4ms 26.4 26.4 26.4
8 72.14.195.48          0%   1  28.1ms 28.1 28.1 28.1
9 172.253.77.225        0%   1  28.8ms 28.8 28.8 28.8
10 192.178.109.208       0%   1  27ms   27   27   27
11                     100%  1 timeout
12 108.170.226.83        0%   1  27.4ms 27.4 27.4 27.4
13 142.251.52.243        0%   1  26.9ms 26.9 26.9 26.9
14                     100%  1 timeout
15                      0%   1  0ms
```

Jika kalian ingin menggunakan mode gui kalian masuk ke dalam tools lalu traceroute





Jika kalian masuk menggunakan mode gui maka kalian tinggal isi parameter umtuk melakukan traceroute yang spesifik seperti pada contoh dibawah ini



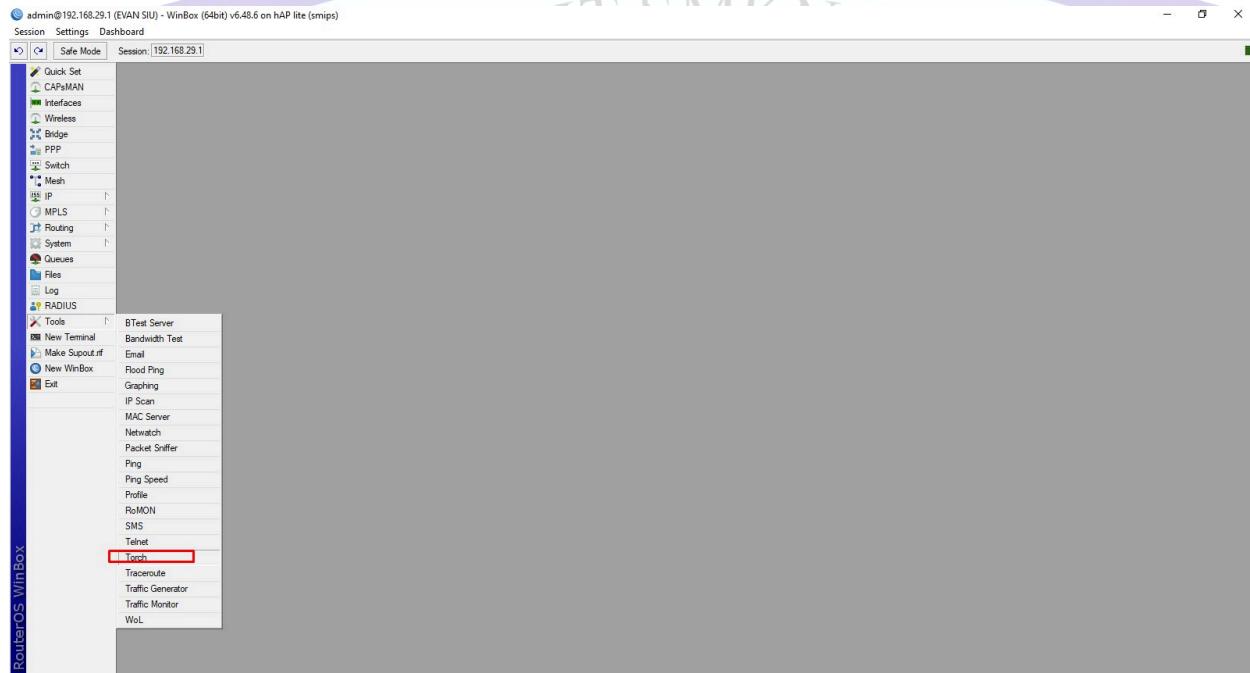


## C.Torch

Torch adalah tool yang tersedia dalam MikroTik yang digunakan untuk mempermudah monitoring Trafic jaringan secara real time.

Jika kalian ingin melihat cara kerjanya sebagai berikut

1. Kalian masuk ke dalam tool lalu pilih torch



2. Selanjutnya kalian konfigurasikan sesuai dengan contoh dibawah ini



Torch (Running)

- Basic -

Interface: ether2

Entry Timeout: 00:00:03 s

- Collect -

Src. Address  Src. Address6

Dst. Address  Dst. Address6

MAC Protocol  Port

Protocol  VLAN Id

DSCP

- Filters -

Src. Address: 0.0.0.0/0  
Dst. Address: 0.0.0.0/0  
Src. Address6: ::/0  
Dst. Address6: ::/0  
MAC Protocol: all  
Protocol: any  
Port: any  
VLAN Id: any  
DSCP: any

Start Stop Close New Window

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.168.29.254	192.168.29.1			4.0 kbps	1968 bps	1	2
800 (ip)		192.168.29.254	74.125.24.95			2.0 kbps	1736 bps	3	3
800 (ip)		192.168.29.254	172.217.194.139			0 bps	0 bps	0	0
800 (ip)		192.168.29.254	157.240.15.60			1440 bps	480 bps	2	1
800 (ip)		192.168.29.254	8.8.8.8			1784 bps	1200 bps	2	2
800 (ip)		192.168.29.254	142.251.12.94			39.6 kbps	29.4 kbps	11	8

6 items Total Tx: 49.0 kbps Total Rx: 34.7 kbps Total Tx Packet: 19 Total Rx Packet: 16

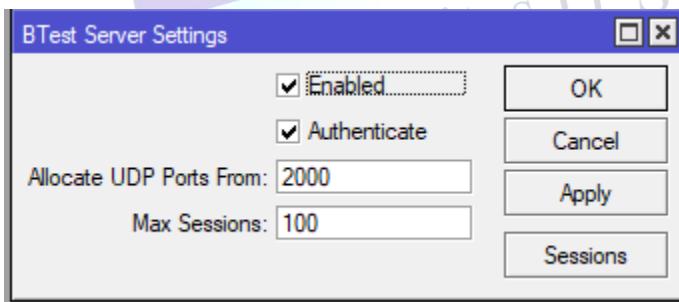
Kalian bisa memantau Traffic yang sedang berlangsung



## D. Bandwidth Test

Bandwidth Test di MikroTik adalah alat untuk mengukur kapasitas traffic yang dapat dilewatkan pada suatu koneksi atau jalur antara perangkat yang terhubung ke router. Terdapat dua jenis Bandwidth Test di MikroTik: Bandwidth Test Server (BTest Server) dan Bandwidth Test Client. Dari keduanya, yang paling sering digunakan adalah Bandwidth Test Client.

1. Login Ke dalam winbox
2. Lalu masuk ke dalam tools dan Btest



Bandwidth Test di MikroTik memungkinkan perangkat berfungsi sebagai **Bandwidth Test Client**. Beberapa parameter yang sering digunakan adalah:

**Test To:** Alamat IP Bandwidth Test Server.

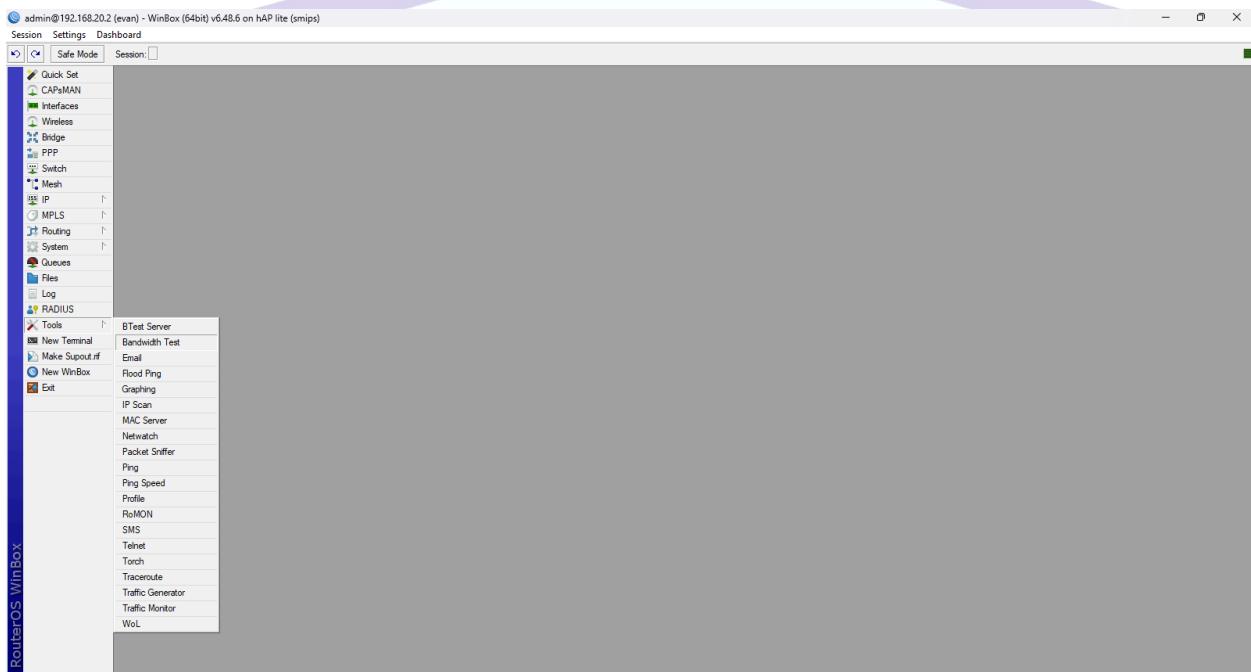
**Protocol:** Pilih protokol yang digunakan, bisa UDP atau TCP.

**Direction:** Menentukan arah lalu lintas (Send/Upload, Receive/Download, atau Both).

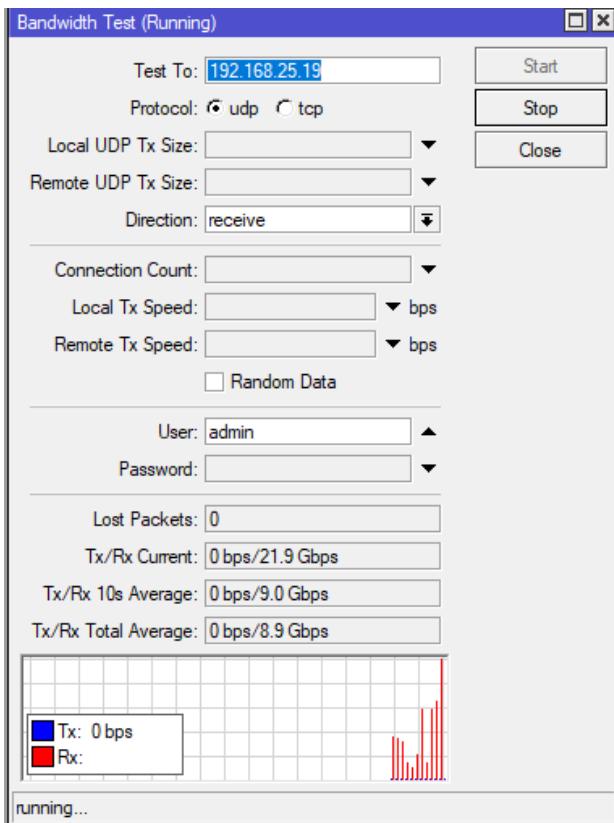
**Local TX Speed & Remote TX Speed:** Menentukan kecepatan transfer data dalam bps (bit per second).



### 3. Jika sudah kalian masuk ke dalam tools badwidth test

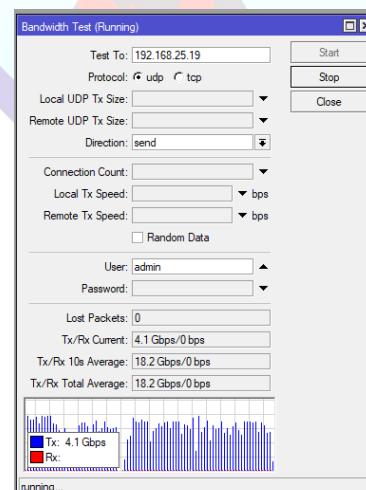
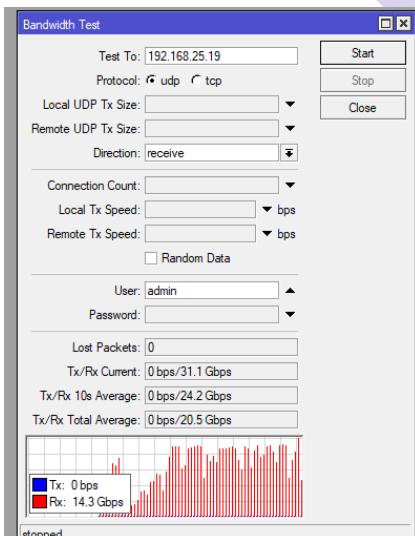


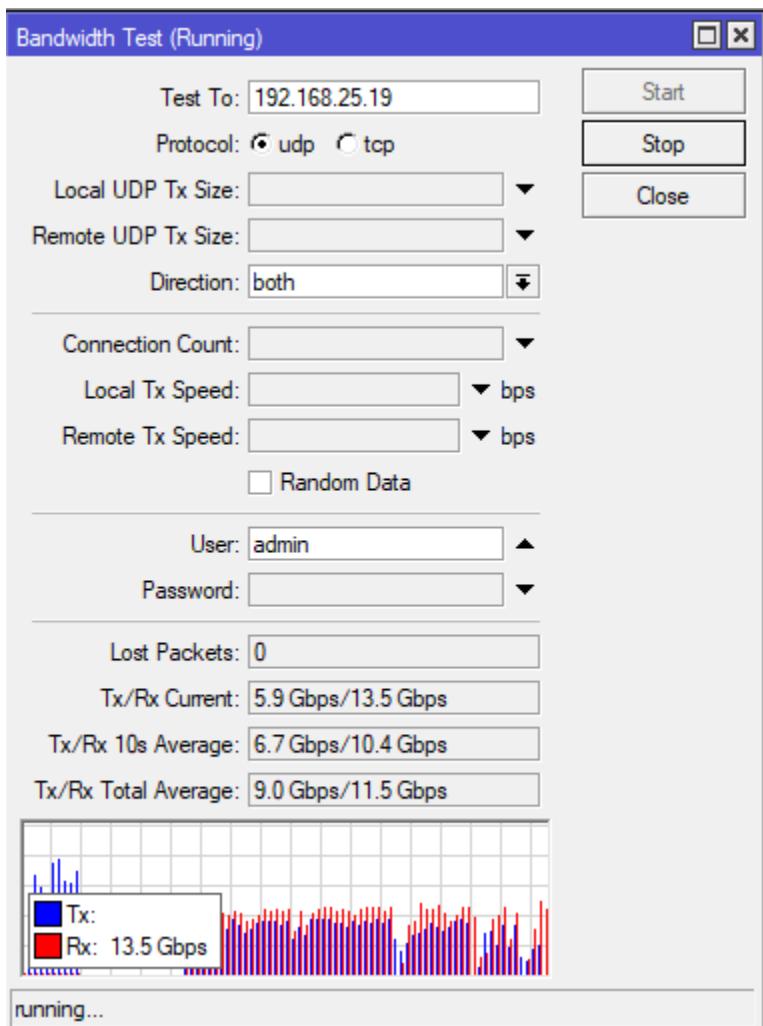
### 4. Setelah itu kalian lakukan sesuai dengan contoh



Dan tunggu

### 5. Kalian lakukan test sebagai Direction receive, send dan both



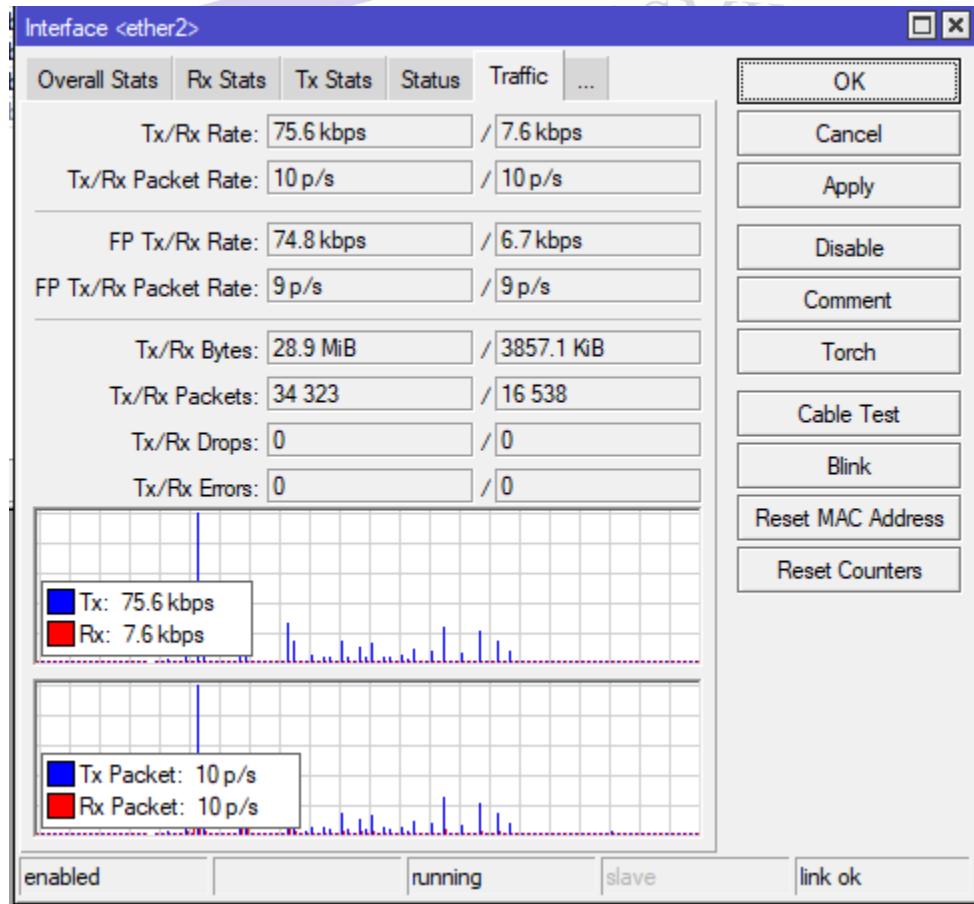




## E. Interface Traffic Monitor

Interface Traffic Monitor di MikroTik menampilkan informasi real-time mengenai traffic jaringan pada setiap interface, baik itu Ethernet maupun WLAN. Fitur ini berguna untuk memantau aktivitas dan kinerja trafik pada masing-masing interface.

Interface Traffic Monitor sangat penting karena beberapa informasi sangat berguna dalam monitoring traffic pada suatu interface.

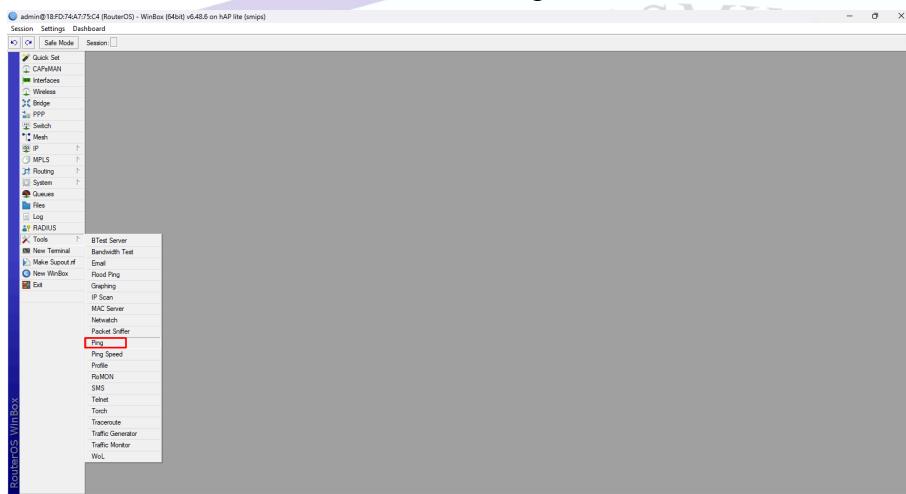




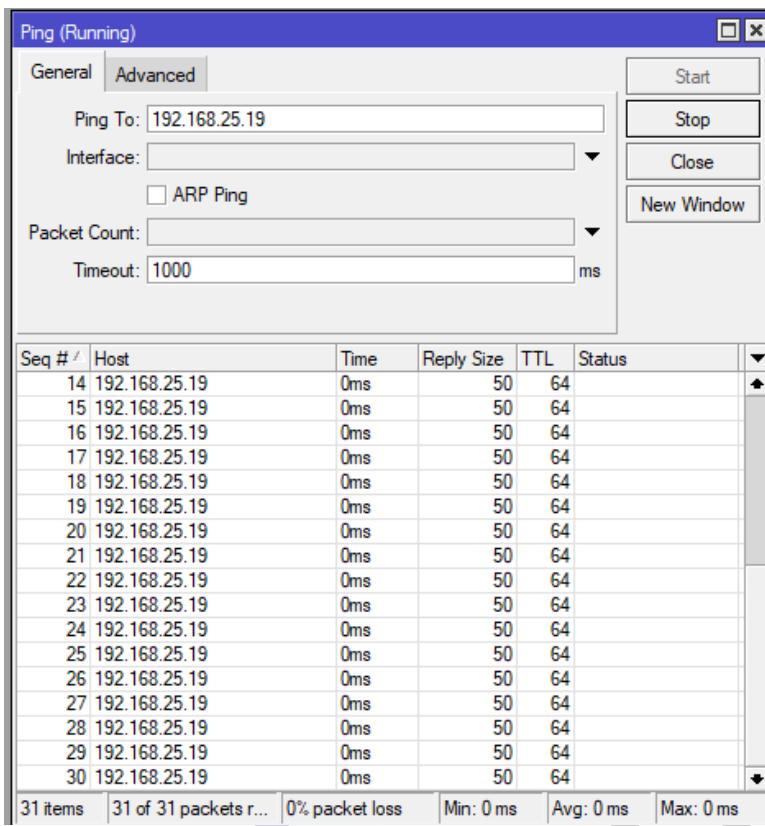
## F. Ping Tool

Ping Tool di MikroTik digunakan untuk menguji koneksi antara perangkat dan alamat tujuan. Proses ini memeriksa apakah host tujuan aktif dan mengukur waktu respons (latency). Ping, yang merupakan singkatan dari Packet Internet Groper, digunakan untuk mengecek koneksi antara dua perangkat di jaringan.

### 1. Masuk ke dalam Tools lalu Ping



### 2. Kemudian menu yang akan muncul seperti ini



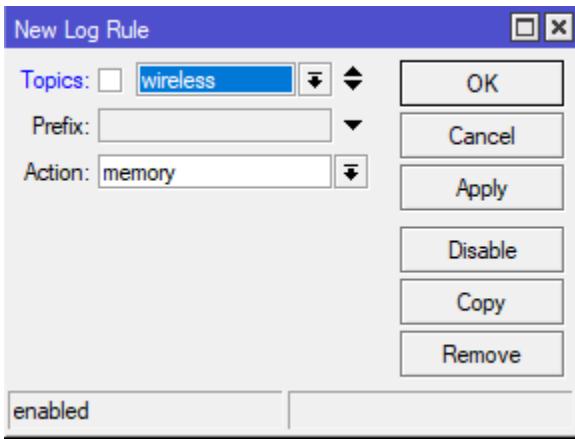
N1 Nglelok

## G. System Logging

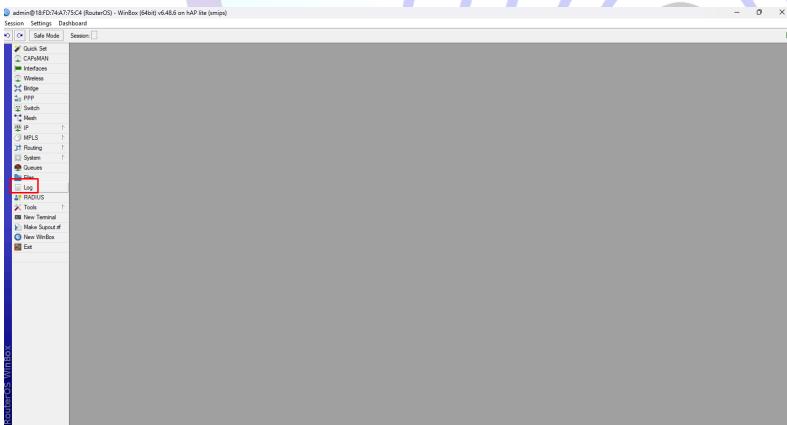
Pertama tama kalian masuk ke dalam system lalu logging



Setelah itu Klik tombol +



Tambahkan wireless  
Untuk mengeceknya kalian masuk ke dalam Log

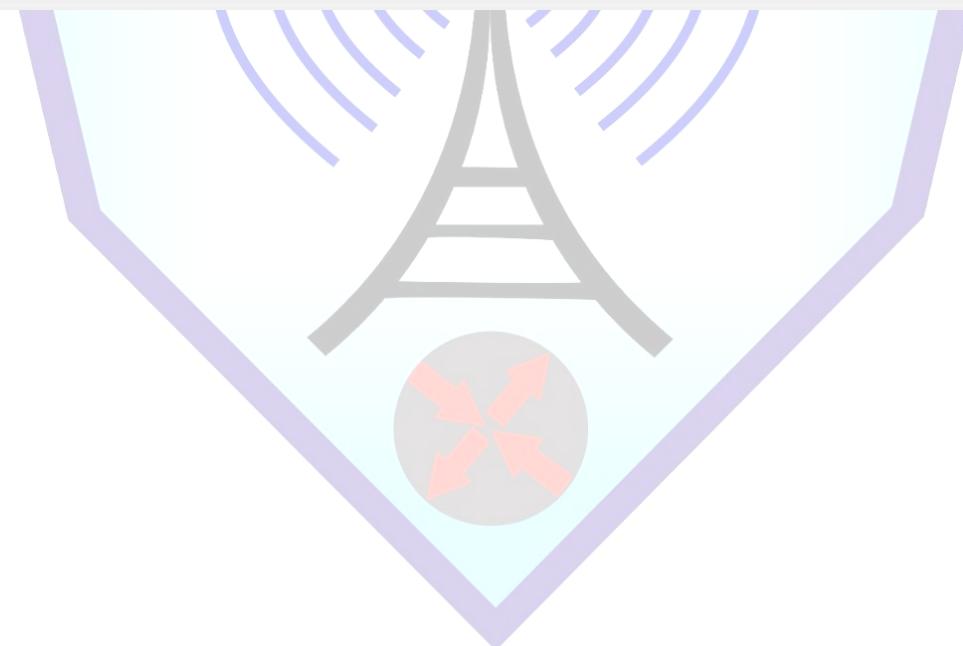


Maka Tampilannya akan seperti ini



#	Time	Buffer	Topics	Message
0	Jan/02/1970 00:00:15	memory	system, info	router rebooted
1	Jan/02/1970 00:00:17	memory	interface, info	ether1 link up (speed 100M, full duplex)
2	Jan/02/1970 00:00:17	memory	interface, info	ether2 link up (speed 100M, full duplex)
3	Jan/02/1970 00:00:41	memory	system, info, account	user admin logged in from 70:B5:E8:62:51:95 via winbox
4	Jan/02/1970 00:00:46	memory	system, info	dhcp client added by admin
5	Jan/02/1970 00:00:46	memory	dhcp, info	dhcp-client on ether1 got IP address 10.201.10.51
6	Jan/02/1970 00:00:59	memory	system, info	address added by admin
7	Jan/02/1970 00:01:32	memory	system, info	address changed by admin
8	Jan/02/1970 00:01:38	memory	system, info	pool dhcp_pool0 added by admin
9	Jan/02/1970 00:01:38	memory	system, info	dhcp network added by admin
10	Jan/02/1970 00:01:38	memory	system, info	dhcp server dhcp1 added by admin
11	Jan/18/2025 03:04:09	memory	dhcp, info	dhcp1 assigned 192.168.25.18 to 70:B5:E8:62:51:95
12	Jan/18/2025 03:04:34	memory	system, info	nat rule added by admin
13	Jan/18/2025 03:07:45	memory	system, info, account	user admin logged out from 70:B5:E8:62:51:95 via winbox
14	Jan/18/2025 03:07:47	memory	system, info, account	user admin logged in from 70:B5:E8:62:51:95 via winbox
15	Jan/18/2025 03:38:32	memory	system, info	log rule added by admin

16 items





## H. Rommon

RoMON (Router Management Overlay Network) adalah sebuah protokol berbasis Layer 2 yang dikembangkan oleh MikroTik untuk mempermudah manajemen dan remote akses ke perangkat MikroTik dalam sebuah jaringan. Dengan RoMON, administrator dapat mengakses perangkat MikroTik lainnya di dalam jaringan, bahkan jika perangkat tersebut berada di belakang NAT atau tidak memiliki akses IP langsung.

### Keunggulan RoMON

1. Dapat mengakses perangkat MikroTik tanpa IP
  - o RoMON bekerja di Layer 2 (Data Link Layer), sehingga tidak memerlukan alamat IP untuk menghubungkan perangkat MikroTik.
2. Mampu melewati NAT dan firewall
  - o Karena bekerja di bawah Layer 3 (Network Layer), RoMON dapat digunakan untuk mengakses perangkat yang berada di balik NAT atau firewall yang membatasi komunikasi berbasis IP.
3. Mempermudah pengelolaan jaringan besar
  - o Sangat berguna dalam jaringan berskala besar, di mana banyak perangkat MikroTik tersebar di berbagai lokasi.
4. Mendukung koneksi multi-hop
  - o RoMON memungkinkan akses ke perangkat yang berada di belakang perangkat MikroTik lain, tanpa perlu konfigurasi routing tambahan.
5. Keamanan yang lebih baik
  - o RoMON dapat dilindungi dengan password atau key, sehingga hanya pengguna yang memiliki izin dapat mengaksesnya.

### Cara Kerja RoMON

RoMON bekerja dengan membuat jaringan overlay berbasis Layer 2. Setiap perangkat MikroTik yang diaktifkan RoMON akan bertindak sebagai node dalam jaringan tersebut.

Komunikasi antar perangkat terjadi melalui RouterOS MAC Layer, sehingga tidak bergantung pada IP. Dengan fitur ini, administrator dapat mengakses semua perangkat MikroTik dalam jaringan dari satu titik pusat, bahkan jika perangkat-perangkat tersebut tidak memiliki IP yang dapat dijangkau secara langsung.

### Komponen Utama RoMON

1. RoMON ID
  - o Setiap perangkat yang menggunakan RoMON memiliki RoMON ID, yang bisa berupa MAC Address atau angka unik lainnya untuk mengidentifikasi perangkat dalam jaringan.
2. RoMON Agent
  - o Perangkat MikroTik yang berperan sebagai penghubung utama untuk mengakses perangkat lain dalam jaringan RoMON.



3. RoMON Link
  - o Koneksi antar perangkat yang membentuk jaringan overlay RoMON.
4. RoMON Discovery
  - o Proses otomatis untuk mendeteksi perangkat MikroTik lain yang terhubung melalui RoMON.

#### Cara Mengaktifkan RoMON di MikroTik

1. Masuk ke MikroTik melalui WinBox atau Terminal

Aktifkan RoMON dengan perintah berikut di terminal:

shell

SalinEdit

/tool romon set enabled=yes

2.

(Opsional) Tambahkan password untuk keamanan

shell

SalinEdit

/tool romon set secret=YourPassword

3.

Cek status RoMON

shell

SalinEdit

/tool romon print

4.

5. Gunakan WinBox untuk mengakses perangkat lain melalui RoMON

- o Buka WinBox → Pilih RoMON pada tab Connect To → Klik Connect.

#### Contoh Penggunaan RoMON

Misalkan terdapat 5 perangkat MikroTik yang terhubung dalam jaringan, tetapi hanya satu yang memiliki akses IP publik (gateway utama). Dengan mengaktifkan RoMON:

- Administrator dapat mengakses semua perangkat MikroTik lainnya melalui gateway utama tanpa perlu mengkonfigurasi IP atau routing tambahan.
- Jika ada perangkat di belakang NAT atau firewall, RoMON tetap bisa digunakan untuk menghubungkannya.
- Memudahkan monitoring dan troubleshooting jaringan secara lebih cepat.

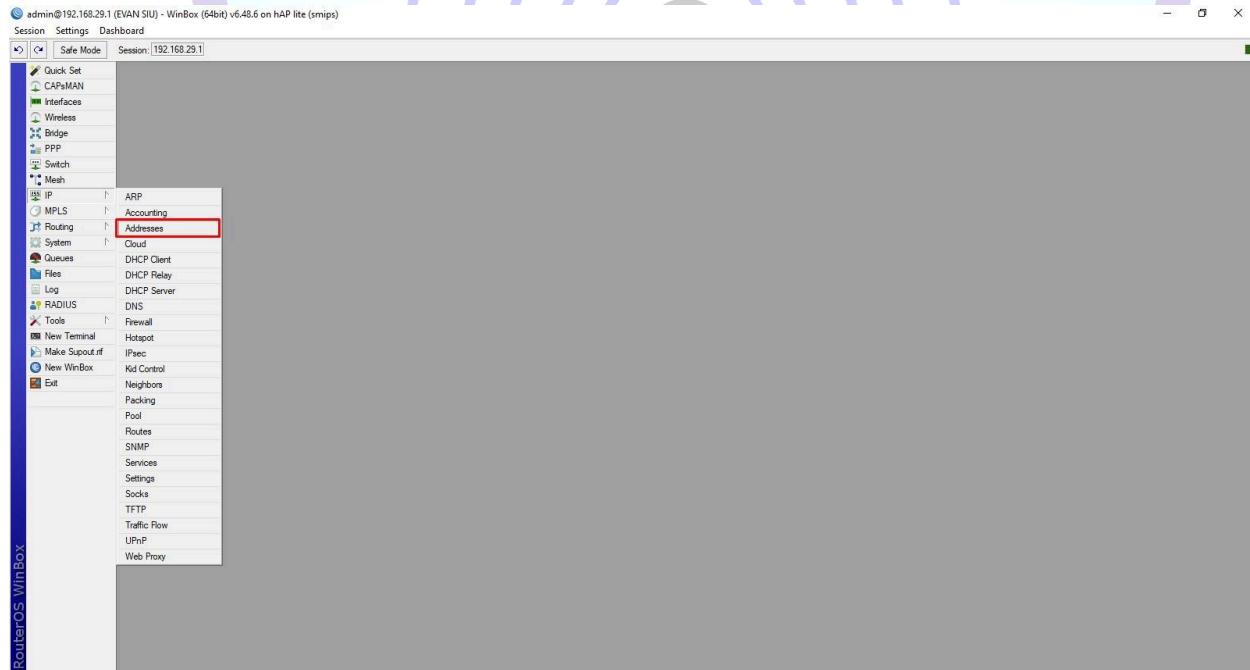


## LAB 11 Konfigurasi IP , DHCP Server & leases (TimeManagement and Make Static)

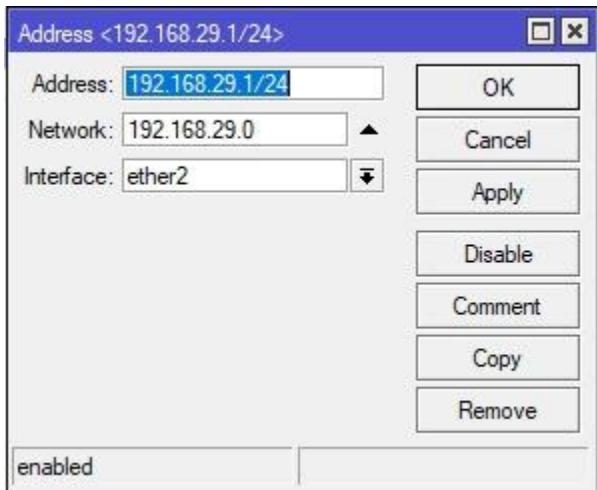
Pada lab ini, saya akan membahas cara konfigurasi IP pada MikroTik menggunakan Winbox. Konfigurasi IP yang salah bisa menyebabkan router tidak terhubung ke internet, jadi pemahaman yang baik tentang IP Address, khususnya IPv4, sangat penting sebelum mengikuti lab ini. Saya juga akan menggunakan topologi tertentu dalam konfigurasi ini.

### A.Konfigurasi IP ADDRESS

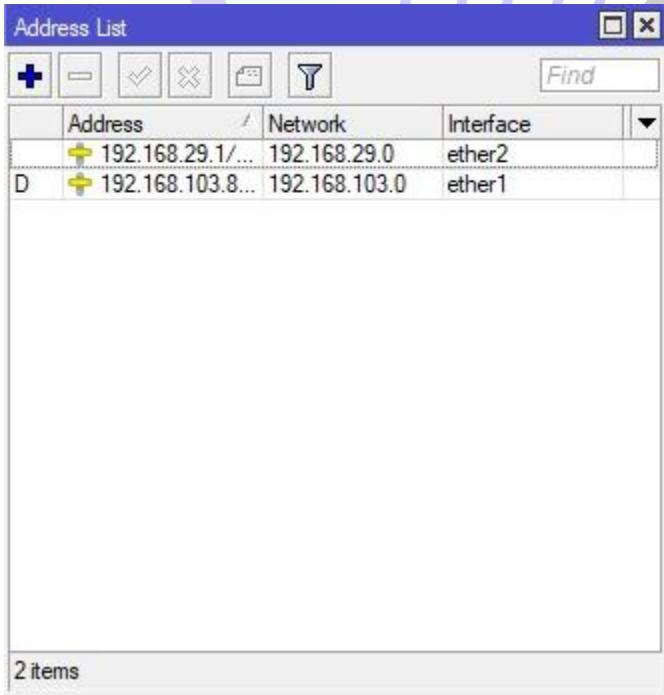
1. Masuk ke dalam winbox
2. IP lalu address



3. Klik tombol + untuk menambahkan
4. Jika sudah tambahkan ip sesuai dengan keinginan sebagai contoh saya akan menambahkan 192.168.29.1/24 dan interface pada ether 2



5. Dan IP sudah berhasil ditambahkan

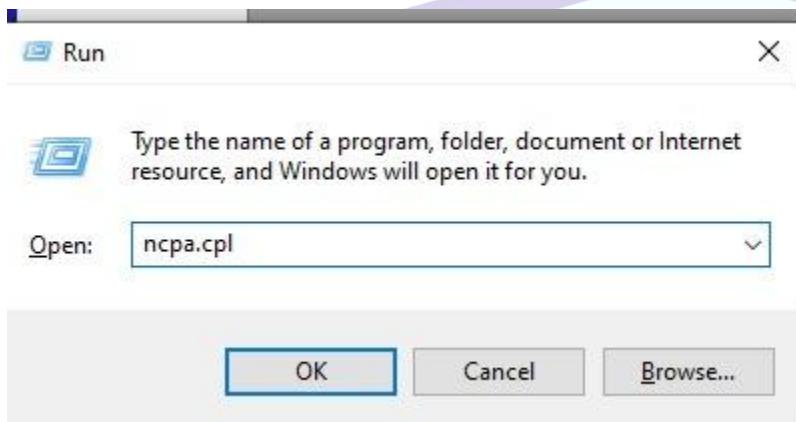


6. IP pada mikrotik juga akan otomatis mengganti

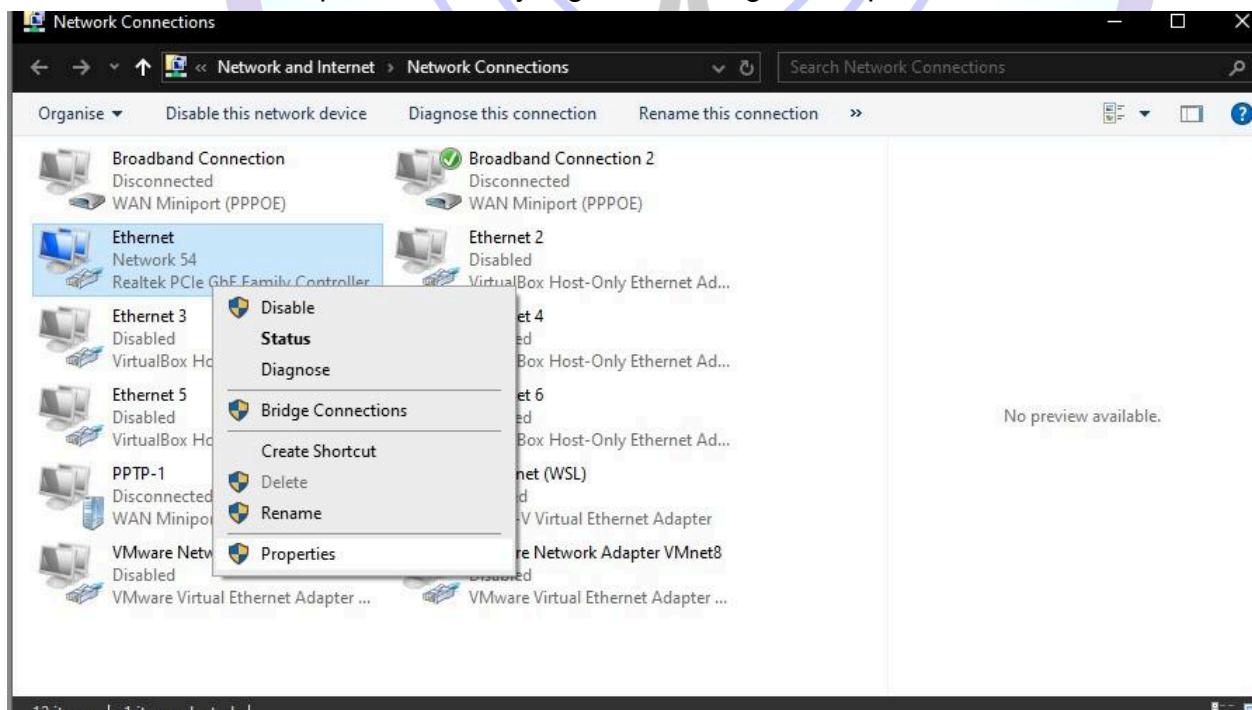
admin@192.168.29.1 (EVAN SIU) - WinBox (64bit) v6.48.6 on hAP lite (smips)



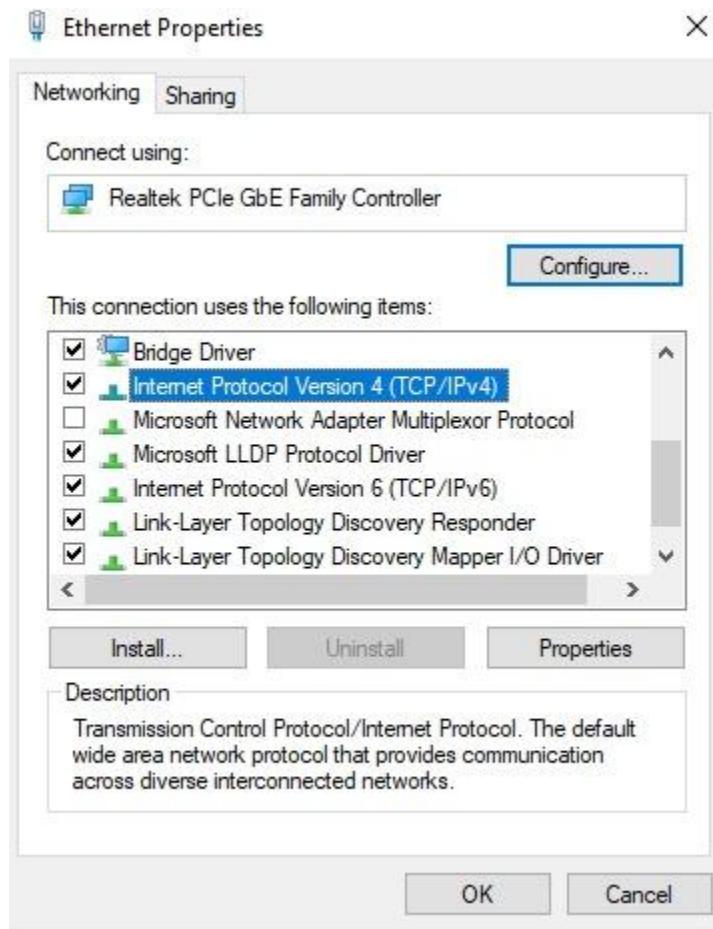
7. Setelah itu lakukan pengujian dengan ping Client ke MikroTik
8. Jika ingin melakukan pengujian maka ip dari client harus satu jaringan dengan ip dari MikroTik
9. Klik Windows+R
10. Lalu ketikkan ncpa.cpl



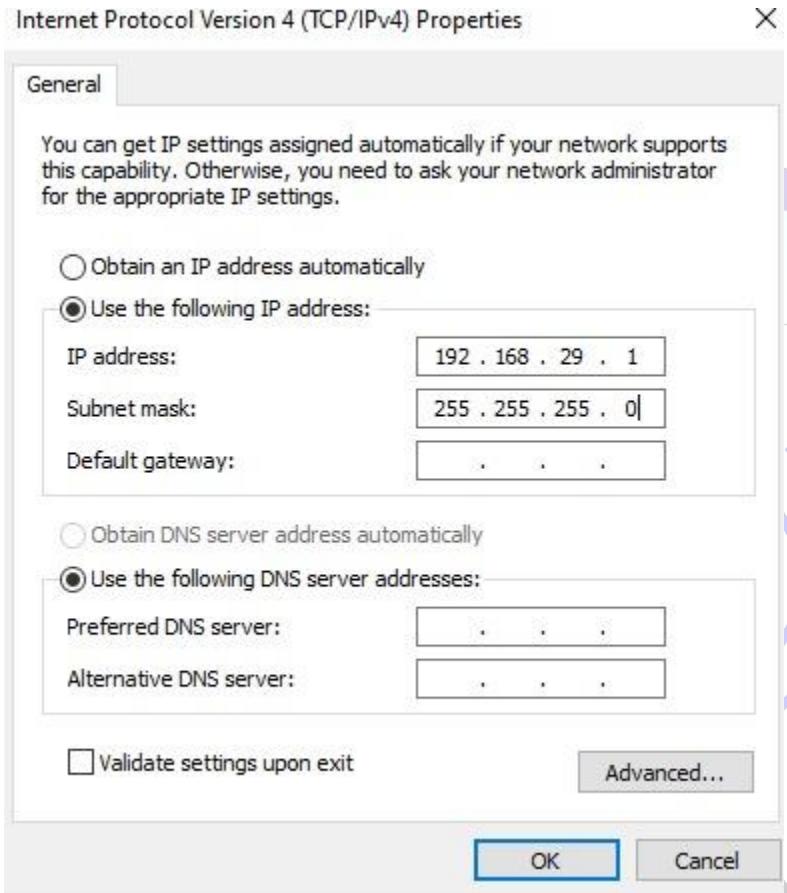
11. Lalu klik kanan pada internet yang tersambung dalam pc kalian



12. Pilih internet protocol version 4



13. Ganti ip yang satu jaringan dengan ip si Mikrotik kalian tadi



14. Terakhir kalian ping menggunakan CMD



```
Command Prompt
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC-TKJ-LAB-4>192.168.29.1
'192.168.29.1' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\PC-TKJ-LAB-4>ping 192.168.29.1

Pinging 192.168.29.1 with 32 bytes of data:
Reply from 192.168.29.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

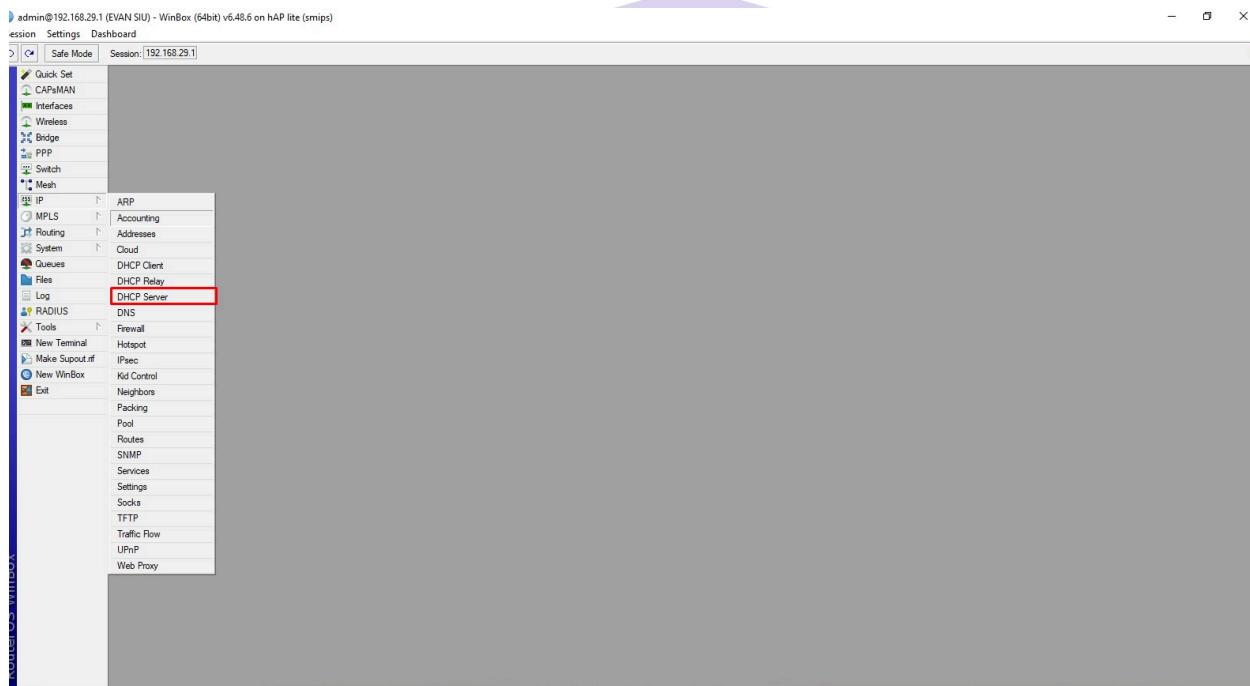
C:\Users\PC-TKJ-LAB-4>
```

15. Dan kita sudah berhasil ping. Ada banyak cara yang bisa dilakukan selain pada tutorial di atas

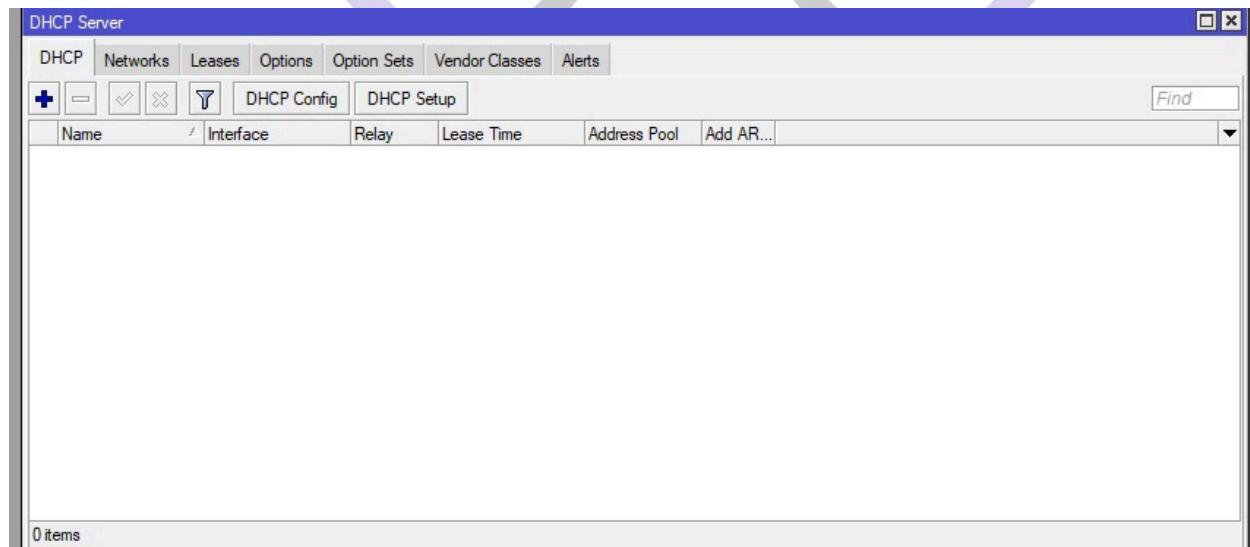


## B.DHCP Server

1. Login Winbox
2. Lalu pilih IP DHCP Server

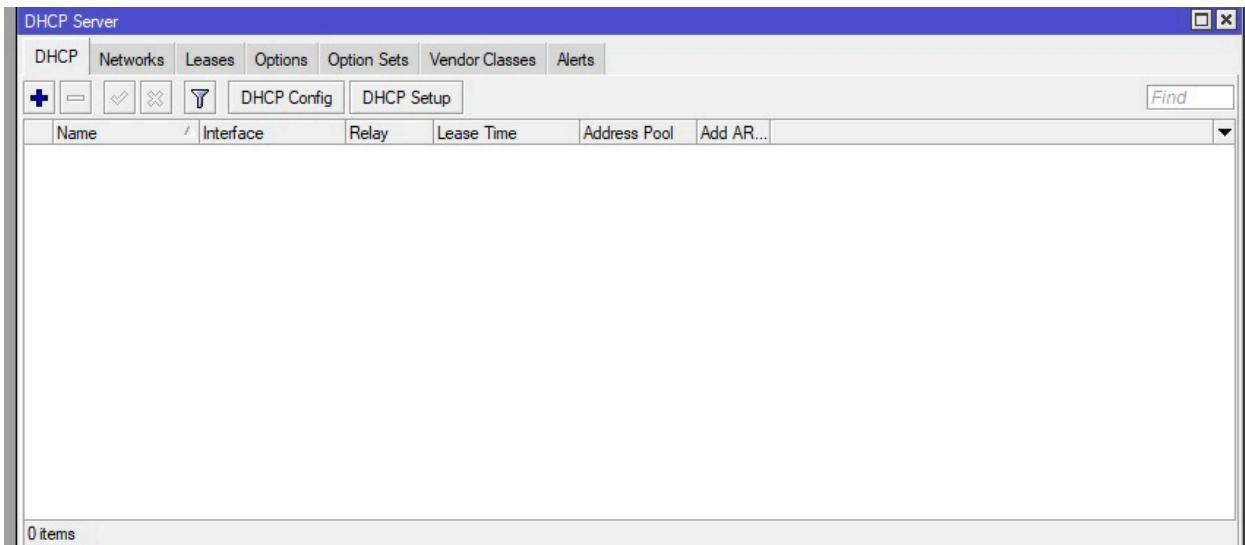


3. Disini masih kosong karena belum ada konfigurasi dan kita akan melakukannya caranya sangat mudah

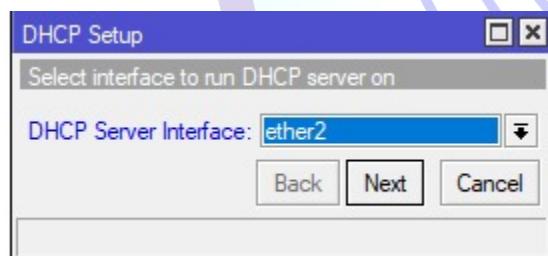




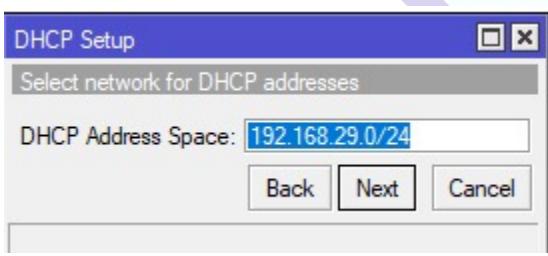
#### 4. Pilih Dhcp Setup



5. Setelah itu pilih interface yang mengarah pada client dan disini saya menggunakan interface ether 2

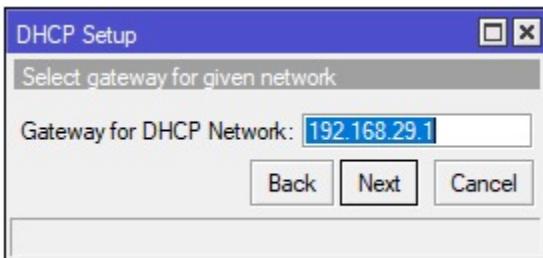


6. Kalian next

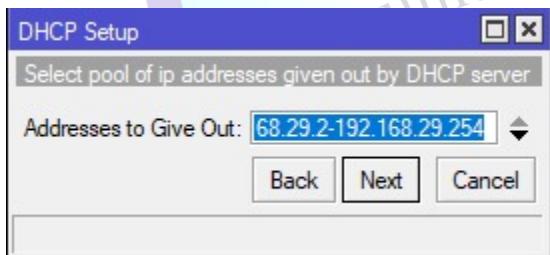




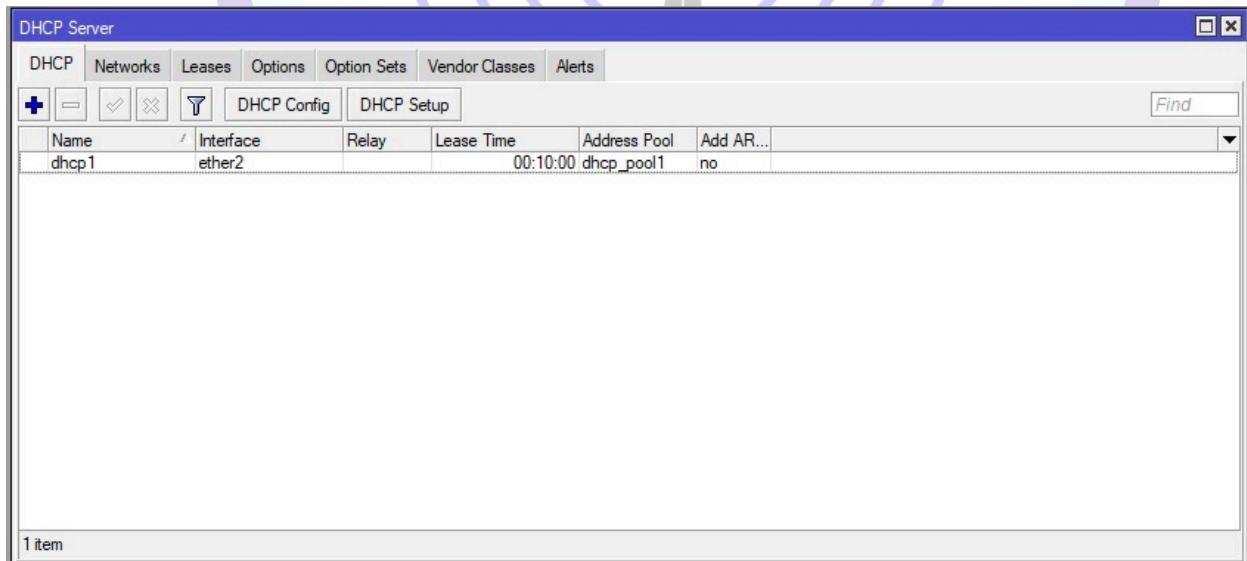
7. Next lagi



8. Kalian Masukkan IP range pada client



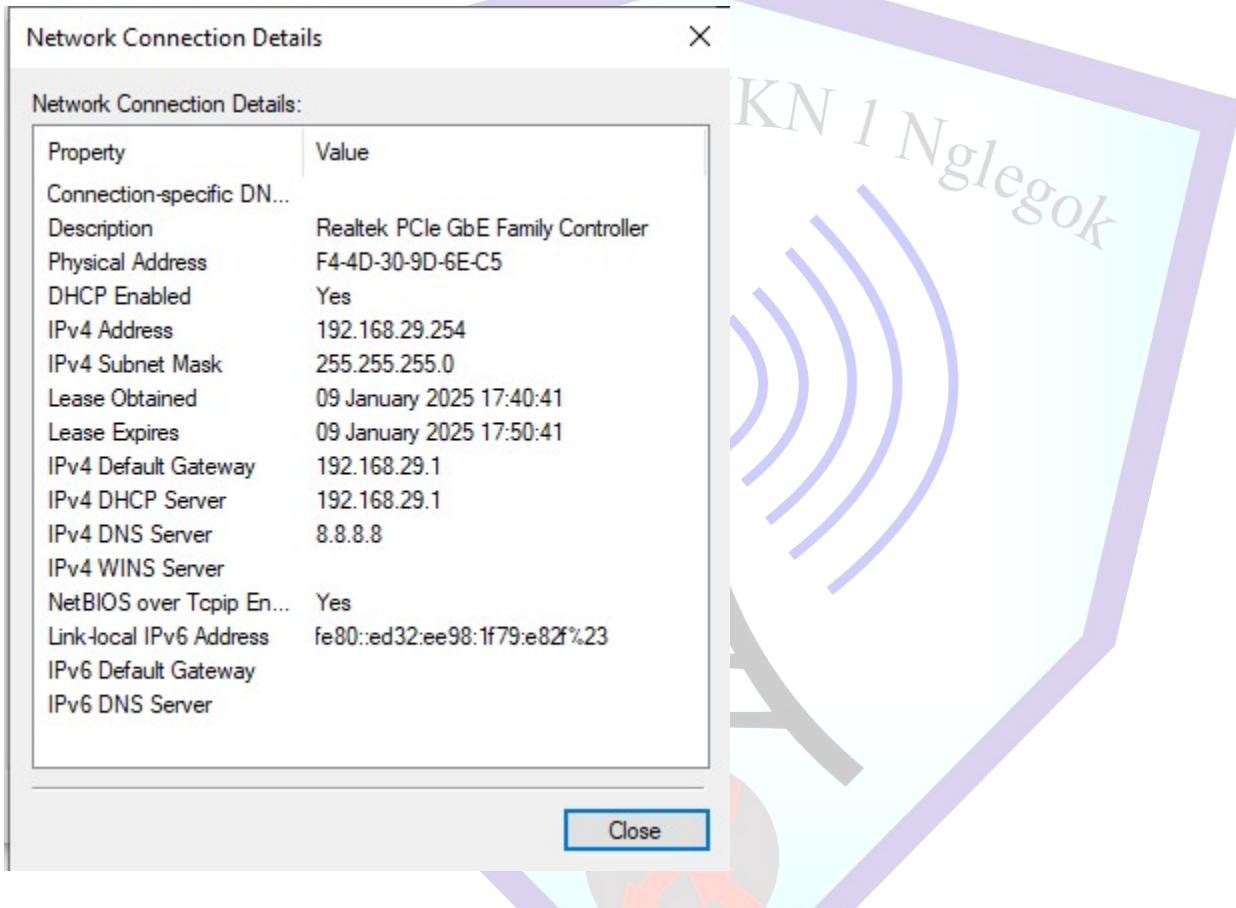
9. Lalu next hingga successful





Setelah kalian melakukan konfigurasi DHCP server kita chek apakah berhasil sebagai mana mestinya

1. Klik Windows+R
2. Lalu klik pada internet yang sedang tersambung ke pc kalian
3. Lalu klik details

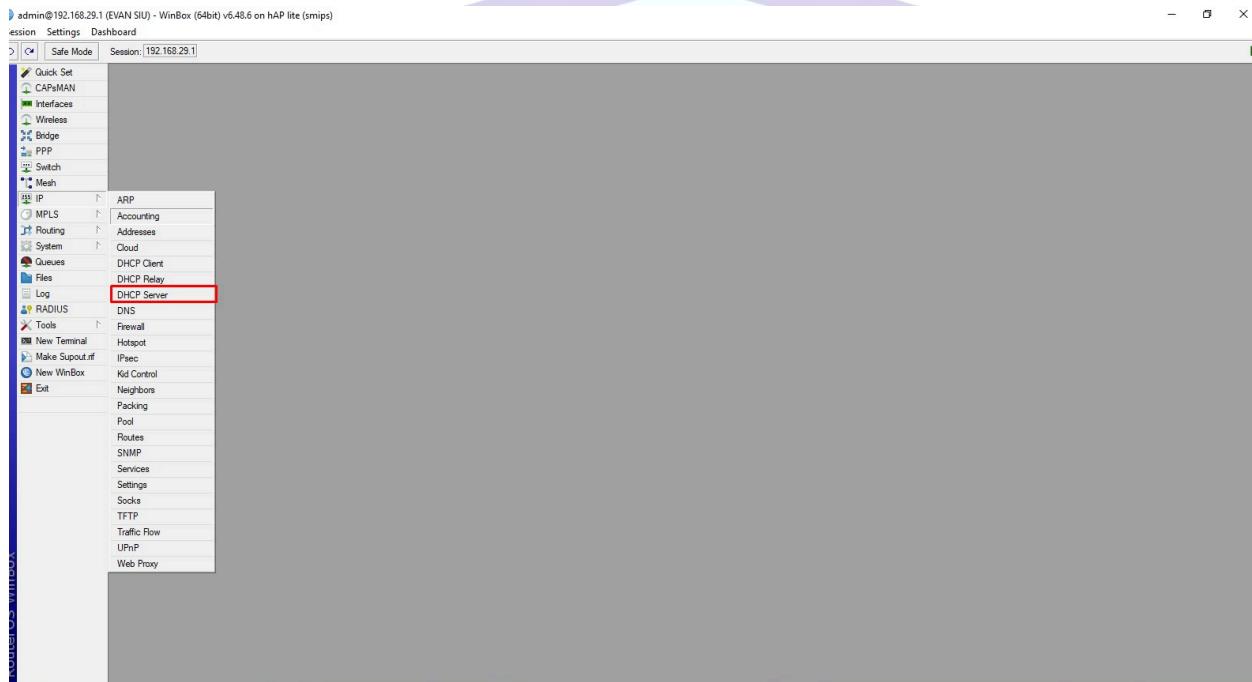




## C.Leases

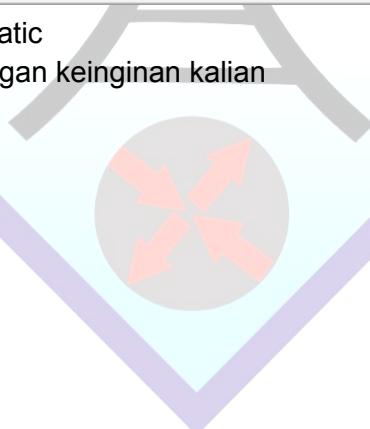
### - MAKE STATIC

1. Login Winbox
2. Lalu masuk ke IP DHCP Server



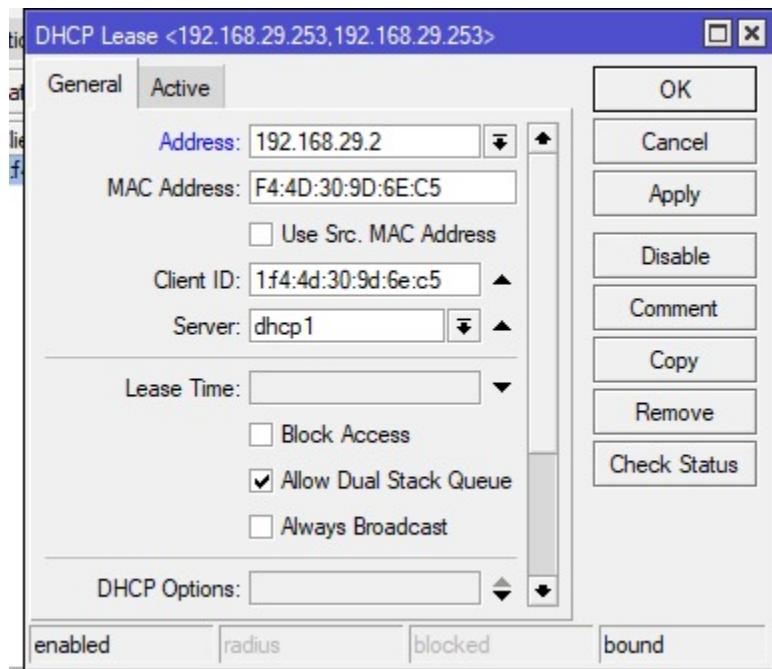


### 3. Lalu masuk ke Leasses



DHCP Server						
	DHCP	Networks	Leases	Options	Option Sets	Vendor Classes
<input style="width: 100px; height: 20px;" type="button" value="+"/> <input style="width: 100px; height: 20px;" type="button" value="-"/> <input style="width: 100px; height: 20px;" type="button" value="✓"/> <input style="width: 100px; height: 20px;" type="button" value="✗"/> <input style="width: 100px; height: 20px;" type="button" value="..."/> <input style="width: 100px; height: 20px;" type="button" value="Filter"/> Check Status <input type="text" value="Find"/>						
D	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre... DE
	192.168.29.254	F4:4D:30:9D:6E:C5	1f4:4d:30:9d:6e:c5	dhcp1	192.168.29.254	F4:4D:30:9D:6E:C5 DE
<input style="width: 100px; height: 20px;" type="button" value="Back"/> <input style="width: 100px; height: 20px;" type="button" value="Forward"/>						
1 item						

4. Jika sudah kalian klik Make Static
5. Lalu kalian ganti ip sesuai dengan keinginan kalian



6. Langkah terakhir kita melakukan pengujian dengan cara
7. Masuk ke dalam Windows+R lalu disable dan enable kembali internet yang tersambung ke dalam pc kalian
8. Jika sudah klik detail



Network Connection Details X

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek PCIe GbE Family Controller
Physical Address	F4-4D-30-9D-6E-C5
DHCP Enabled	Yes
IPv4 Address	192.168.29.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	09 January 2025 17:48:07
Lease Expires	09 January 2025 17:58:07
IPv4 Default Gateway	192.168.29.1
IPv4 DHCP Server	192.168.29.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::ed32:ee98:1f79:e82f%23
IPv6 Default Gateway	
IPv6 DNS Server	

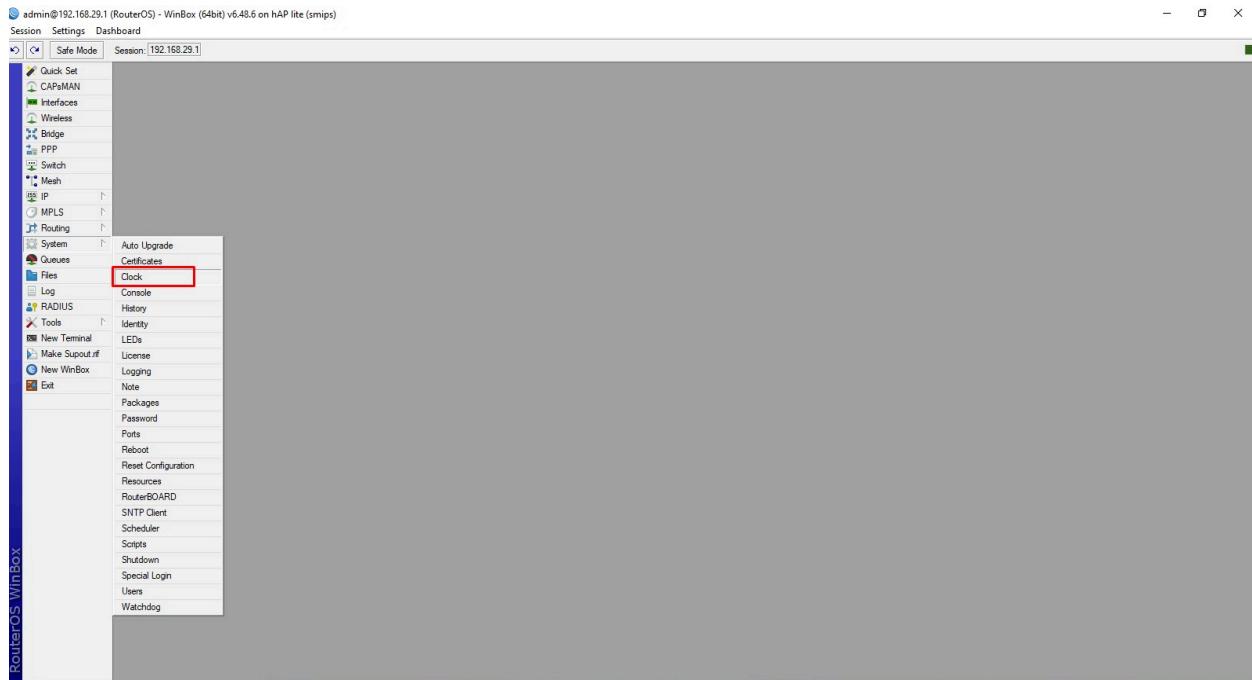
Close

Dan berhasil

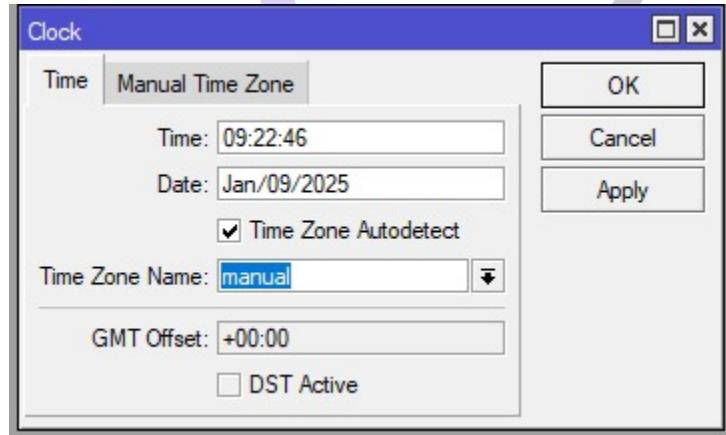


## - Time Management

### 1. Masuk kedalam System Clock



### 2. Lalu Setting sesuai dengan waktu di tempat kalian

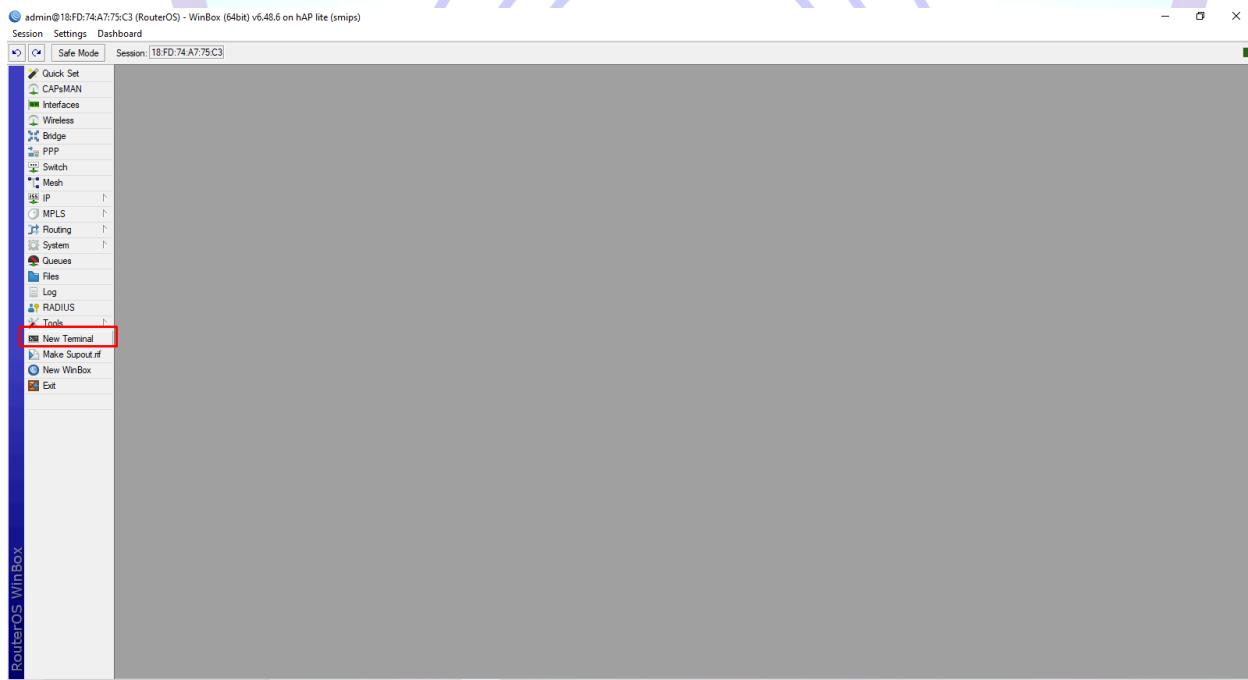




## LAB 12 Setting router gateway(IP Klien Dynamic)

Pada lab ini, kita akan membahas tentang Router Gateway. Fungsi router adalah agar komputer client yang terhubung dengan MikroTik dapat mengakses internet. Setelah mengonfigurasi DHCP Client di MikroTik, seharusnya MikroTik bisa terhubung ke internet. Cobalah untuk melakukan ping ke Google melalui terminal untuk menguji koneksi.

1. Pertama Kalian masuk Ke winbox
2. Lalu new terminal



3. Kita coba ping google.com jika ttl kita berhasil mendapat internet dari router



```
Terminal <1>

MikroTik RouterOS 6.48.6 (c) 1999-2021          http://www.mikrotik.com/

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

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

/             Move up to base level
..            Move up one level
/command      Use command at the base level
jan/02/1970 00:00:13 system,error,critical router was rebooted without proper shut
down
[admin@RouterOS] > system identity set name=evam
[admin@evam] > system identity set name=evan
[admin@evan] > ping google.com
  SEQ HOST                               SIZE TTL TIME  STATUS
    0 64.233.170.106                      56 103 27ms
    1 64.233.170.106                      56 103 27ms
    2 64.233.170.106                      56 103 27ms
sent=3 received=3 packet-loss=0% min-rtt=27ms avg-rtt=27ms max-rtt=27ms

[admin@evan] >
```

#### 4. TTL berikutnya kita akan coba ping menggunakan CMD

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5371]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC-TKJ-LAB-4>ping 8.8.8.8

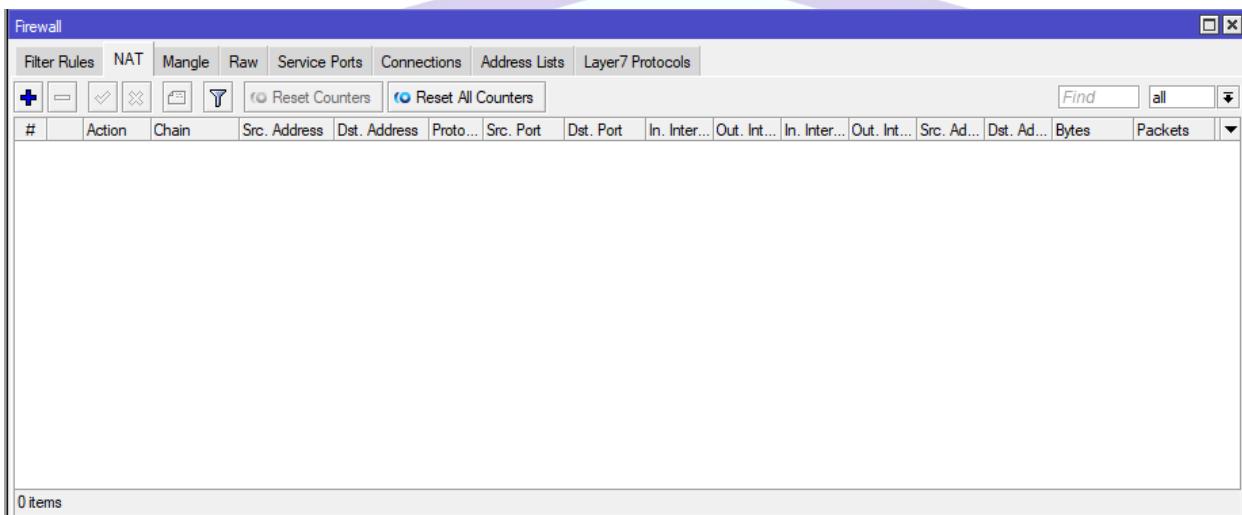
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
  Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\Users\PC-TKJ-LAB-4>
```



Dan disini RTO untuk mengatasinya kita akan melakukan konfigurasi router gateway caranya sebagai berikut

1. Login ke dalam winbox
2. Lalu masuk ke ip>firewall dan pilih NAT



3. Lalu klik menu tambah
4. Setting sesuai dengan contoh di bawah ini



New NAT Rule

General Advanced Extra Action ...

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:  ether1

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

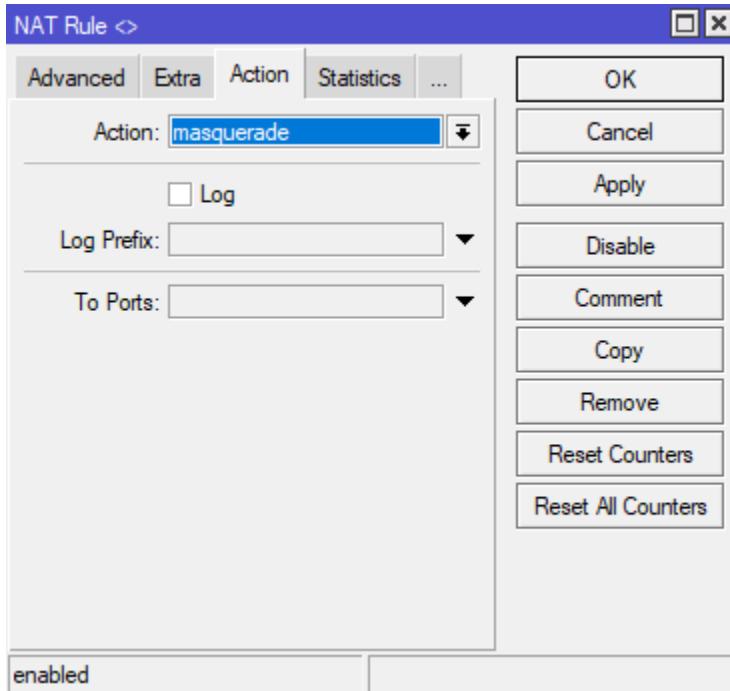
Connection Type:

enabled

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

Kalian ganti chainnya menjadi srcnat dan Out interface kalian masukkan interface yang mengarah ke internet, disini saya akan menggunakan interface 1

5. Berikutnya kalian masuk ke dalam Action lalu ganti



Masquerade sendiri berguna untuk memungkinkan perangkat di jaringan lokal mengakses internet dan menjaga keamanan jaringan



## 6. Jika sudah kita akan uji ping kembali menggunakan cmd

```
Command Prompt      X + ▾
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pc-lab-1>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=26ms TTL=112
Reply from 8.8.8.8: bytes=32 time=26ms TTL=112
Reply from 8.8.8.8: bytes=32 time=27ms TTL=112
Reply from 8.8.8.8: bytes=32 time=26ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 27ms, Average = 26ms

C:\Users\pc-lab-1>
```

Dan Sudah berhasil / TTL sebagai tanda bahwa client sudah bisa mendapat internet

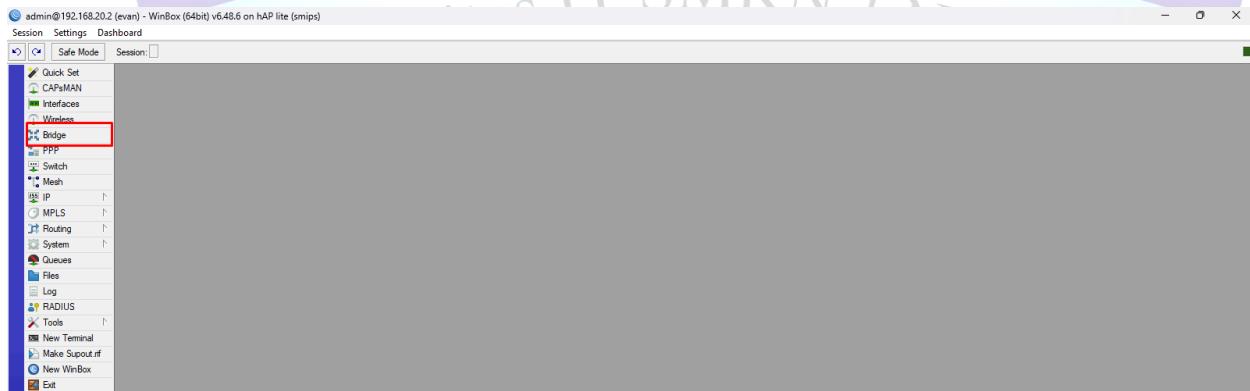




## LAB 13 Creating briges/loopback

Pada lab ini, kita akan membahas tentang Loopback. Loopback adalah IP yang digunakan pada interface virtual (logikal), yang tidak terkait dengan perangkat fisik. Interface loopback sangat penting dalam routing, terutama pada OSPF, karena memberikan alamat yang stabil dan dapat digunakan untuk identifikasi router.

1. Login Winbox
2. Lalu masuk ke dalam Bridge



3. Kalian Klik +



#### 4. Setelah itu saya akan menambahkan Bridge 1- Evan

New Interface

General	STP	VLAN	Status	Traffic
Name: bridge1 -evan				
Type: Bridge				
MTU:				
Actual MTU:				
L2 MTU:				
MAC Address:				
ARP: enabled				
ARP Timeout:				
Admin. MAC Address:				
Ageing Time: 00:05:00				
<input type="checkbox"/> IGMP Snooping				
<input type="checkbox"/> DHCP Snooping				
<input checked="" type="checkbox"/> Fast Forward				
enabled		running	slave	

OK Cancel Apply Disable Comment Copy Remove Torch



5. Dan bridge evan sudah berhasil ditambahkan

R	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)
R	bridge1 -evan	Bridge	65535	1976 bps	0 bps	2

6. Berikutnya kita masuk ke dalam IP>Address

7. Disini kita menambahkan ip sesuai dengan keinginan kita harus perfic /24

New Address

Address: 192.168.19.25

Network:

Interface: bridge1 -evan

OK Cancel Apply Disable Comment Copy Remove

enabled

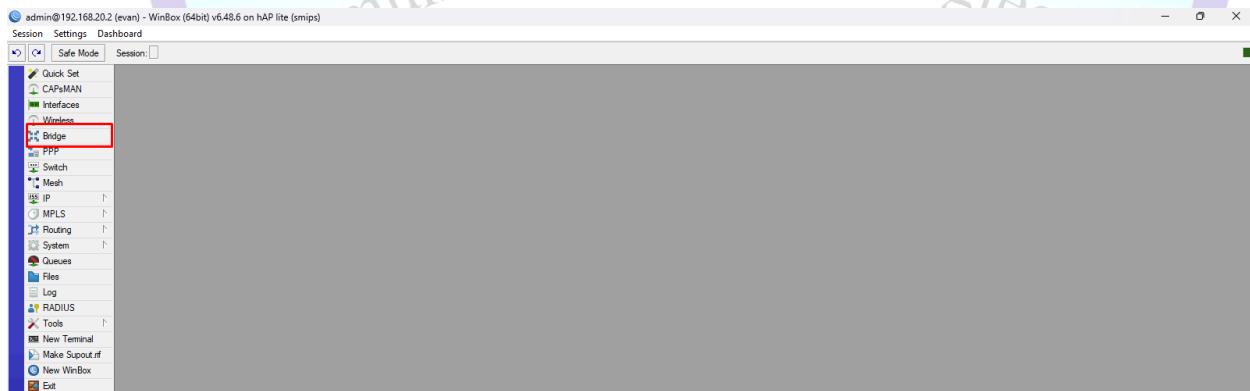
8. Lalu Apply Ok



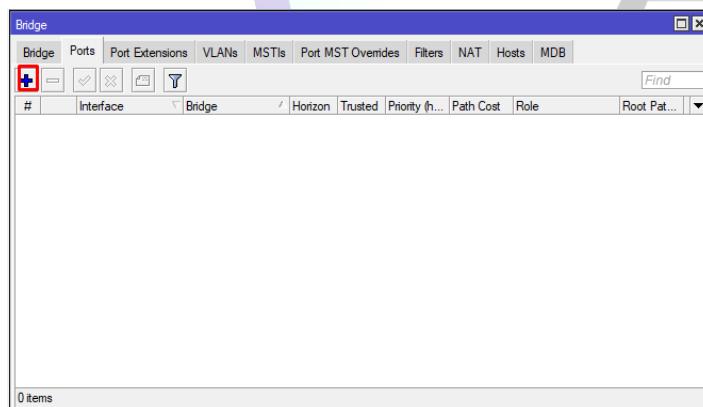
## LAB 14 Adding ports to bridges

Bridge berfungsi Membuat beberapa interface seolah-olah menjadi satu artinya adalah tidak ada perbedaan segmen jaringan didalamnya.

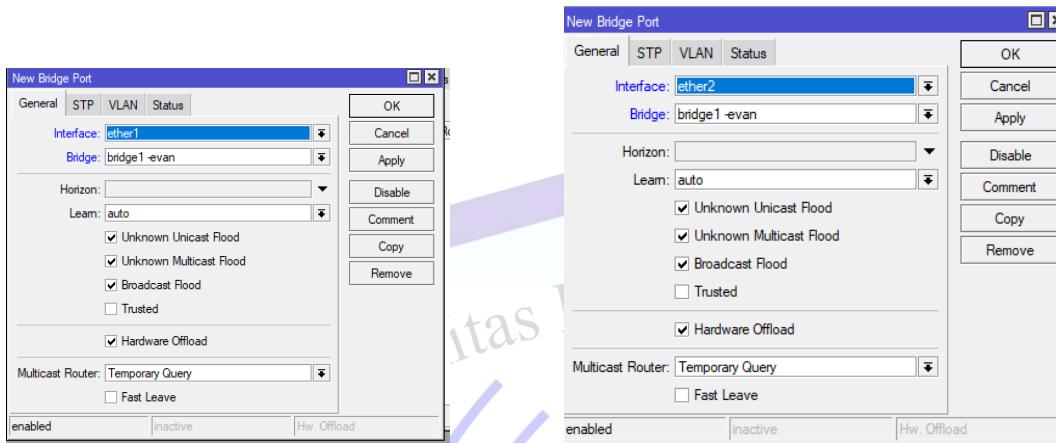
1. Login Winbox
2. Masuk kedalam Bride



3. Berikutnya kalian masuk ke ports dan klik tombol +



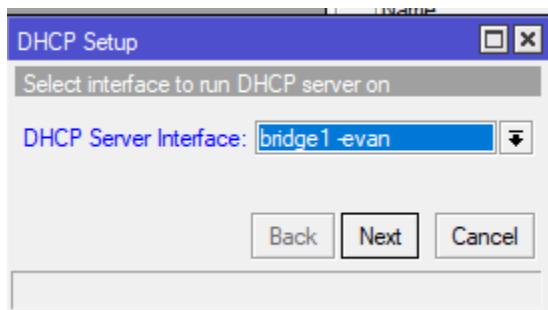
4. Kalian tambahkan ether 1 dan ether 2



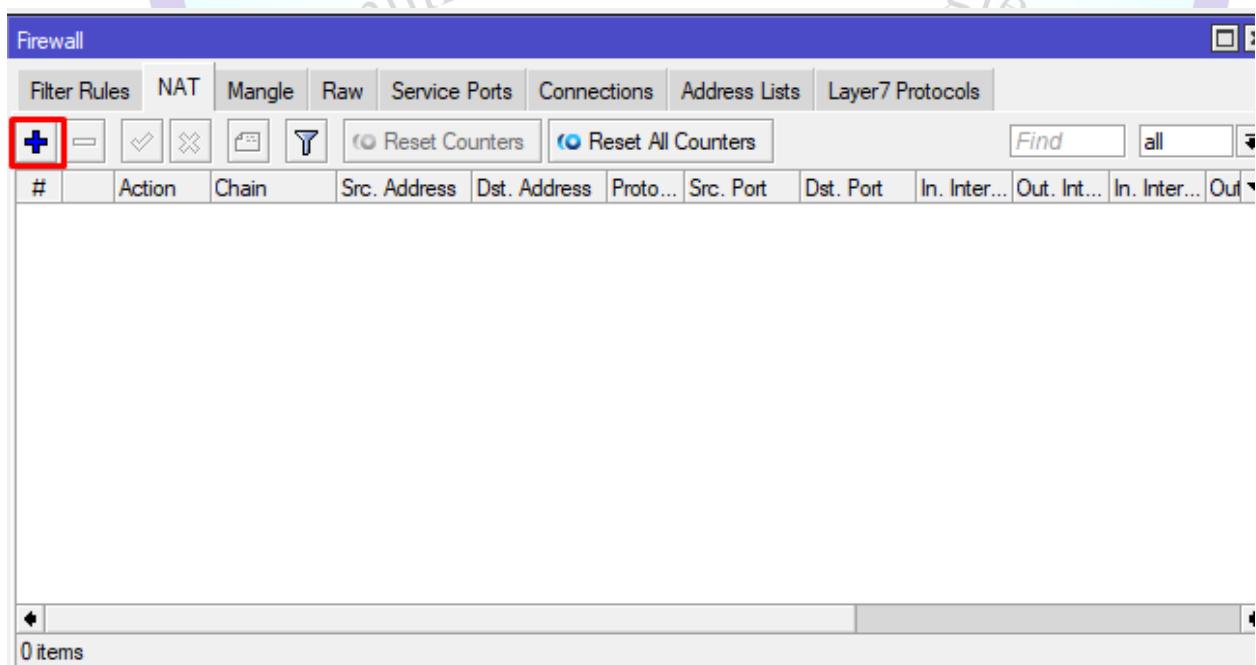
5. Jika sudah maka akan seperti ini

Bridge											
Bridge		Ports		Port Extensions		VLANs		MSTIs		Port MST Overrides	
#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	Role	Root Pat...			
1 H	ether2	bridge1-evan		no	80	10	designated port				
0 H	ether1	bridge1-evan		no	80	10	designated port				

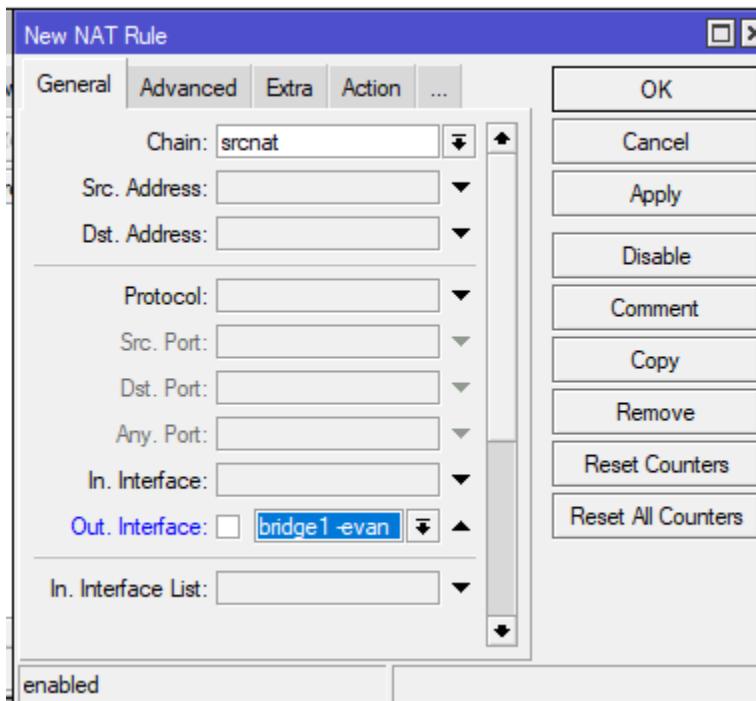
6. Masuk ke dalam IP DCP Server lalu dhcp setup lagi tetapi interface kalian pilih sesuai bridge yang kalian buat tadi dan next hingga sukses



7. Masuk ke dalam NAT dan klik +



8. Ganti out interface dengan bridge kalian dan src nat dan masquerade seperti pada lab 12 tadi



9. Dan Kita berhasil mendapat internet kembali  
Dari sini kita bisa simpulkan saat kita ingin menbridge suatu interface kedalamnya maka bisa menjadi satu artinya adalah tidak ada perbedaan segmen jaringan di dalamnya



## LAB 15 Wireless (AP Bridge & Station Bridge)

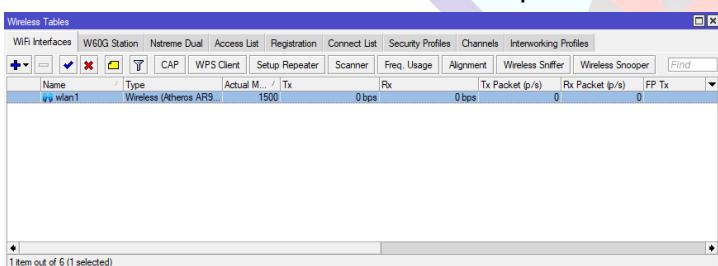
### A. AP Bridge

Pada lab ini, kita akan membahas tentang Wireless AP Bridge. Wireless AP Bridge memungkinkan koneksi antara client dan router tanpa kabel (nirkabel). Mode AP Bridge memungkinkan satu access point terhubung dengan banyak client, yang kemudian dapat mengakses internet. Untuk menghubungkan client ke internet, konfigurasi Router Gateway perlu dilakukan. Berikut adalah topologi yang akan digunakan.

1. Login ke dalam Winbox
2. Masuk ke dalam Wireless



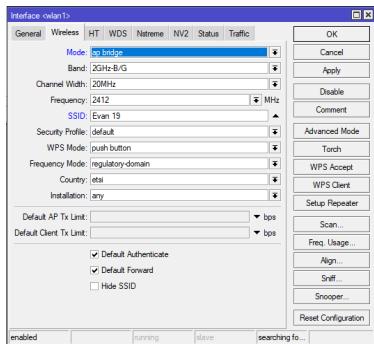
3. Kalian enabled lalu Klik 2 kali pada wlan1



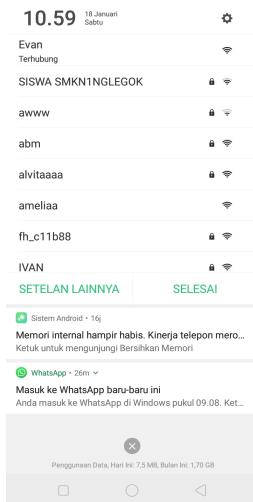
4. Kalian ubah mode menjadi ap bridge dan ssd menjadi nama sesuka kalian Setelah itu, atur IP dan DHCP server pada WLAN1 agar client dapat menerima IP secara dinamis. Jika kalian melihat WLAN1 dengan teks miring, itu menandakan bahwa interface belum aktif, meskipun sudah di-enable. Interface tersebut akan tetap miring jika belum ada client yang terhubung ke access point. Jangan lupa juga untuk mengkonfigurasi Router Gateway agar client dapat terhubung ke internet. Setelah konfigurasi selesai, coba



sambungkan perangkat (misalnya HP atau laptop) dan pastikan client mendapatkan IP dari DHCP Server.



Kita lakukan pengujian bisa menggunakan hp ataupun laptop, disini saya akan mencoba menggunakan hp dan akan mencoba akses internet sebagai client

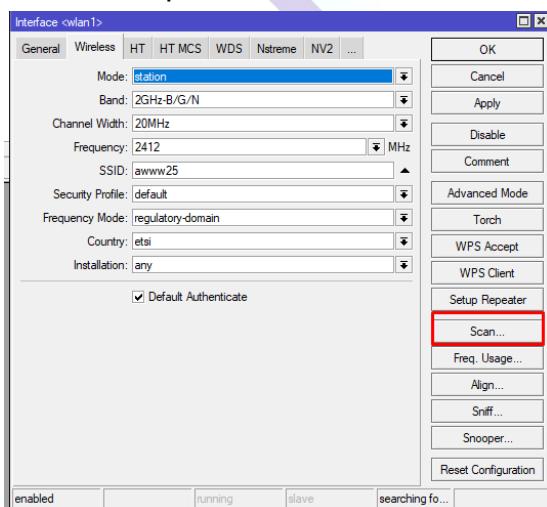




## B. Station Bridge

Pada lab ini, kita akan membahas tentang Wireless Station Bridge. Wireless Station Bridge adalah mode pada MikroTik yang memungkinkan router menjadi penerima layanan wireless dari router lain yang menggunakan mode Wireless Bridge atau AP Bridge. Mode ini hanya dapat menerima layanan dari router dengan vendor yang sama, berbeda dengan Wireless Station yang bisa menerima layanan dari router dengan vendor berbeda, seperti TP-Link. Untuk konfigurasi Station Bridge, kita akan menggunakan topologi berikut.

1. Klik 2 kali pada wlan1
2. Lalu pilih scan



3. Kalian start lalu pilih wifi kalian dan connect



Scanner

Interface: **wlan1**

Background Scan

**Connect** (highlighted with a red arrow)

New Window

	Address	SSID	Channel	Signal...	Noise...	Signa...	Radio Name	RouterO...
AP	52:C2:E8:77:D7:07	DIRECT...	2412/2...	-82	-115	33		
AP	3E:C5:33:7F:91:EF	<b>awww</b>	2412/2...	-51	-115	64		
APRB	6C:3B:6B:2E:58:96	IVAN	2412/2...	-61	-115	54	6C3B6B2E5896	6.49.13
ARB	CE:2D:E0:79:97:98	KITS-am...	2412/2...	-54	-115	61	CC2DE0799798	6.49.12
APRB	CE:2D:E0:D1:FC:89	GURU S...	2412/2...	-81	-115	34	LAB 5	6.49
ARB	CC:2D:E0:79:97:98	ameliaa	2412/2...	-55	-115	60	CC2DE0799798	6.49.12
APRB	CC:2D:E0:D1:FC:89	SISWA S...	2412/2...	-82	-115	33	LAB 5	6.49
APRB	CC:2D:E0:61:E9:B7	IVAN	2412/2...	-60	-115	55	CC2DE061E9B7	6.39.3
APRB	DC:2C:6E:70:AF:C9	CC-2025	2412/2...	-85	-115	30	DC2C6E70AF:C9	6.49.17
APRB	CE:2D:E0:A4:91:F0	afifjeyi	2412/2...	-87	-115	28	CC2DE0A491F0	6.49.11
APRB	CC:2D:E0:A4:91:F0	LAB J1	2412/2...	-90	-115	25	CC2DE0A491F0	6.49.11
APRB	DC:2C:6E:AB:48:...	rot	2412/2...	-90	-115	25	DC2C6EAB489D	6.49.12
APRB	CC:2D:E0:DE:01:...	alfin	2412/2...	-88	-115	27	CC2DE0DE012A	6.49.12
APRB	4A:8F:5A:D8:68:71	GURU S...	2412/2...	-95	-115	20	LAB 8	6.49.2
APRB	18:FD:74:A7:F6:31	coky	2412/2...	-95	-115	20	18FD74A7F631	6.48.6
APRB	DC:2C:6E:AB:58:6A	taufiqsuk...	2412/2...	-94	-115	21	DC2C6EAB586A	6.49.11
AP	30:1F:48:96:AE:48	SEMEN	2437/2...	-58	-115	57		

30 items

#### 4. Maka SSD akan berubah otomatis sesuai dengan Internet si pemancar

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme NV2 ...

Mode: station

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: **awww**

Security Profile: default

Frequency Mode: regulatory-domain

Country: etsi

Installation: any

Default Authenticate

OK Cancel Apply Disable Comment Advanced Mode Torch WPS Accept WPS Client Setup Repeater Scan... Freq. Usage... Align... Sniff... Snooper... Reset Configuration

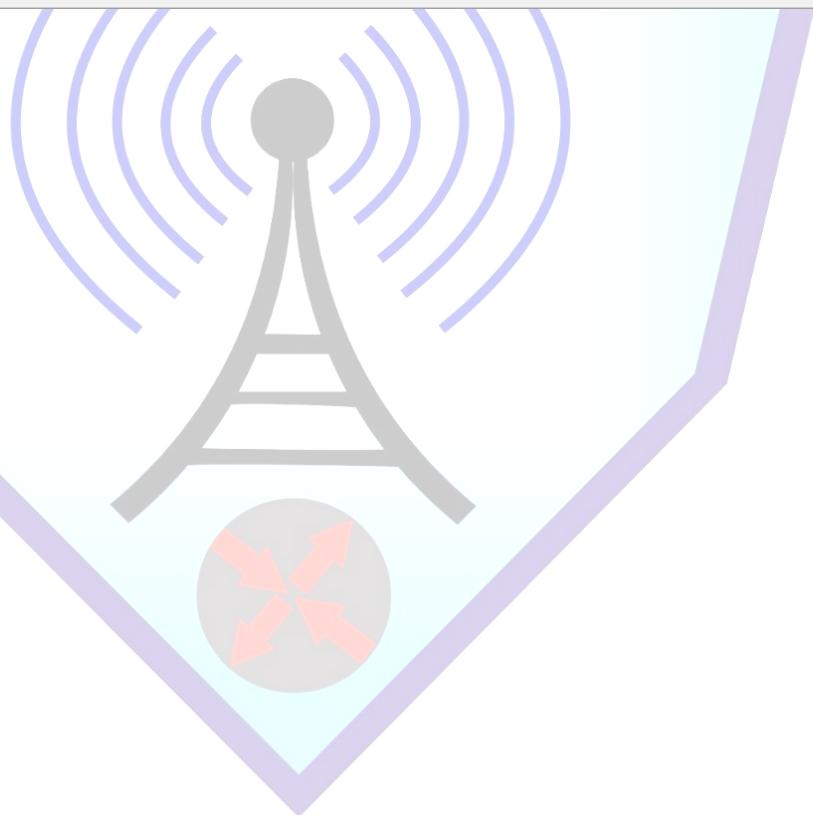
enabled | running | slave | searching fo...

Apabila Ada tanda R atau Running maka sudah berhasil



Wireless Tables								
WiFi Interfaces		W60G Station	Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Channels
+	-	✓	✗	CAP	WPS Client	Setup Repeater	Scanner	Freq. Usage
R	wlan1	Wireless (Atheros AR9...)	1500	0 bps	0 bps	0	Rx Packet (p/s)	FP Tx

1 item out of 6 (1 selected)



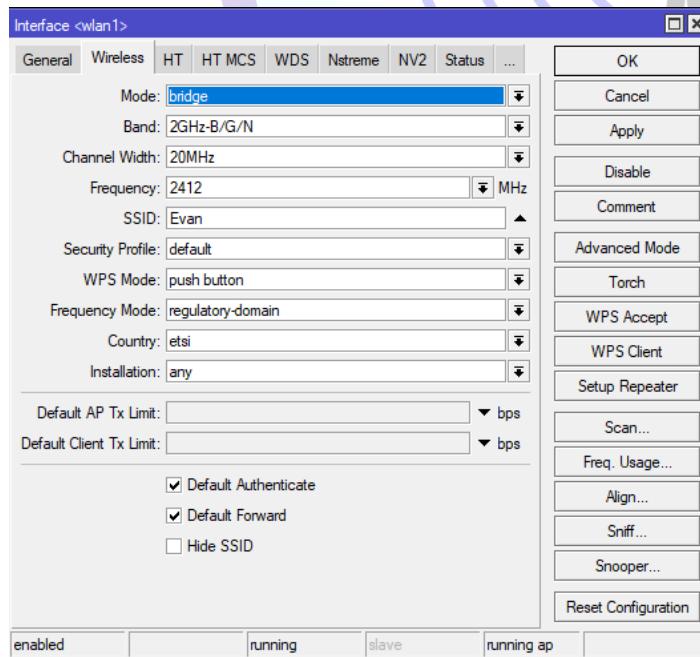


## LAB 16 Wireless (Bridge & Station)

### A.Bridge

Pada lab ini, kita akan membahas tentang Wireless Bridge. Wireless Bridge memungkinkan perangkat atau client terhubung dengan router tanpa menggunakan kabel LAN, atau bisa disebut jaringan nirkabel. Wireless Bridge biasanya digunakan untuk koneksi Point to Point dan mendukung jarak yang jauh, bahkan hingga puluhan kilometer, tergantung pada router yang digunakan. Karena Wireless Bridge memancarkan jaringan secara terpusat, ia dapat mencakup area yang lebih luas.

1. Masuk kedalam Winbox
2. Lalu wireless dan klik 2 kali pada wlan1
3. Lalu pilih bridge dan SSD menjadi nama sesuai dengan nama kalian bebas



4. Langkah Berikutnya kalian atur IP pada wlan1
5. Masuk ke dalam IP Address dan tambahkan Wlan 1



Address <192.168.19.8/24>

Address:	192.168.19.8/24	OK
Network:	192.168.19.0	Cancel
Interface:	wlan1	Apply
		Disable
		Comment
		Copy
		Remove
enabled		

6. Dan kalian DHCP server> lalu dhcp setup menggunakan interface wlan1

DHCP Server

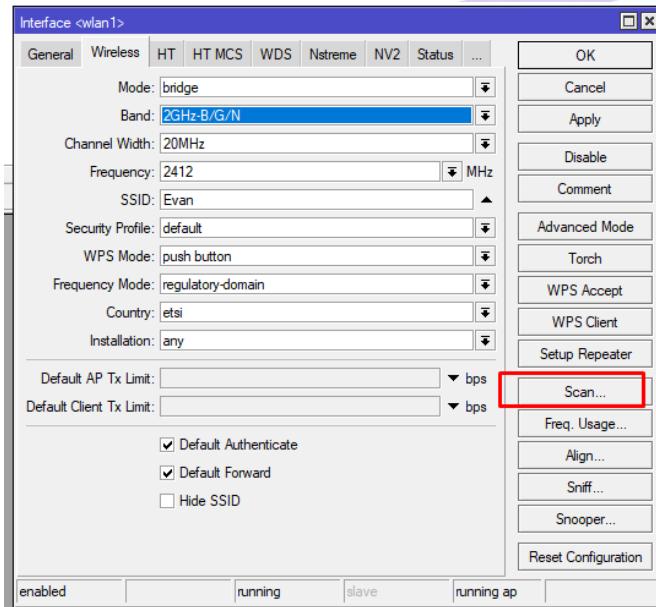
DHCP							Networks	Leases	Options	Option Sets	Vendor Classes	Alerts
+/-		✓	✗	✖	✖	✖	DHCP Config	DHCP Setup	Find			
X		dhcp1	ether2				00:10:00	dhcp_pool1	no			
		dhcp2	wlan1				00:10:00	dhcp_pool3	no			

2 items



## B.Station

1. Masuk ke dalam Winbox
2. Lalu Wireless dan klik 2 kali wlan 1
3. Berikutnya klik scan



Pastikan terdapat pemancar lain, disini saya akan menggunakan Hospot saya



Scanner (Running)

Interface: wlan1

Background Scan

**Connect**

37 items (1 selected)

	Address	SSID	Channel	Signa...	Noise...	Signa...	Radio Name	RouterO...
APRB	CC:2D:E0:D9:BF:57	MikroTik	2412/2...	-48	-116	68	CC2DE0D9BF57	6.45.6
APRB	48:8F:5A:66:3C:C9	Sambel	2412/2...	-63	-116	53	488F5A663CC9	6.49.12
ARB	DC:2C:6E:70:AF:...	Johan Si...	2412/2...	-58	-116	58	DC2C6E70AFBD	6.49.12
PRB	DC:2C:6E:AB:48:...	gesangg...	2412/2...	-80	-116	36	DC2C6EAB489D	6.49.12
APRB	DC:2C:6E:70:AF:C9	CC-2025	2412/2...	-83	-116	33	DC2C6E70AFC9	6.49.17
AP	52:C2:E8:77:7D:07	DIRECT...	2412/2...	-78	-116	38		
ARB	CE:2D:E0:DE:01:...	KITS HE...	2412/2...	-86	-116	30	CC2DE0DE012A	6.49.12
APRB	DC:2C:6E:AB:58:6A	taufiqsuk...	2412/2...	-95	-116	21	DC2C6EAB586A	6.49.11
APRB	CE:2D:E0:D1:FC:89	GURU S...	2412/2...	-82	-116	34	LAB 5	6.49
APRB	CC:2D:E0:DE:01:...	alfin	2412/2...	-85	-116	31	CC2DE0DE012A	6.49.12
APRB	CE:2D:E0:23:FB:64	GURU S...	2412/2...	-82	-116	34	LAB 6	6.49
APRB	CC:2D:E0:A4:91:F0	affjeyi	2412/2...	-92	-116	24	CC2DE0A491F0	6.49.11
AP	30:1F:48:96:AF:48	SEMEN	2422/2...	-48	-116	68		
ARB	CC:2D:E6:65:2B:07	rom aww	2437/2...	-47	-115	68	CC2DE0652B07	6.49.12
AP	52:4F:34:61:71:B2	Aula	2437/2...	-77	-115	38		
APRB	00:0C:42:D6:B4:59	AP-TKRO	2437/2...	-88	-115	27	AP-TKRO	6.47
AP	DE:44:F9:F6:9B:87	valda	2447/2...	-51	-116	65		

Disini pasti akan berubah secara otomatis

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme NV2 ...

Mode: station bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2437 MHz

SSID: rom aww

Security Profile: default

Frequency Mode: regulatory-domain

Country: etsi

Installation: any

Default Authenticate

OK Cancel Apply Disable Comment Advanced Mode Torch WPS Accept WPS Client Setup Repeater Scan... Freq. Usage... Align... Sniff... Snooper... Reset Configuration

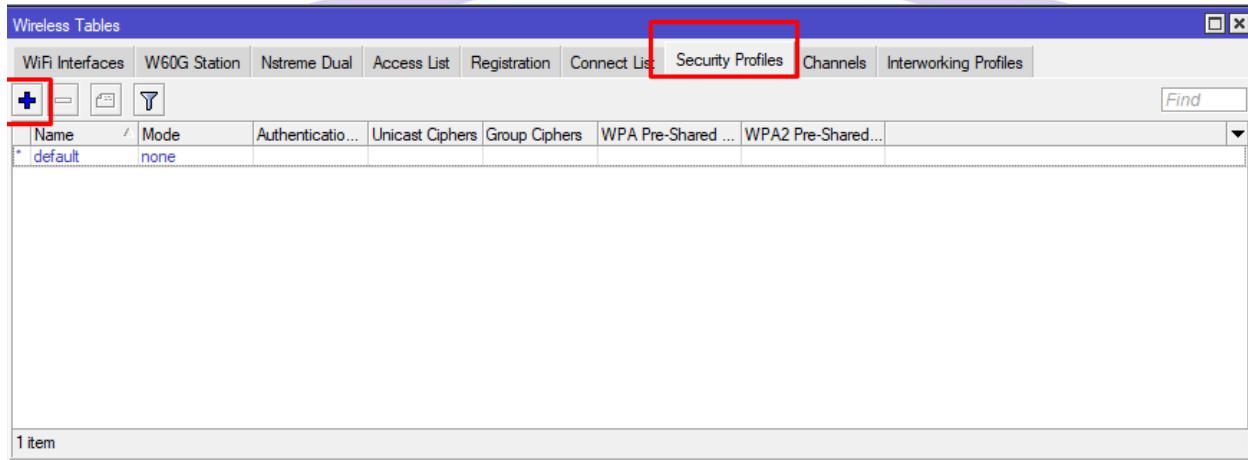
enabled running slave searching fo...



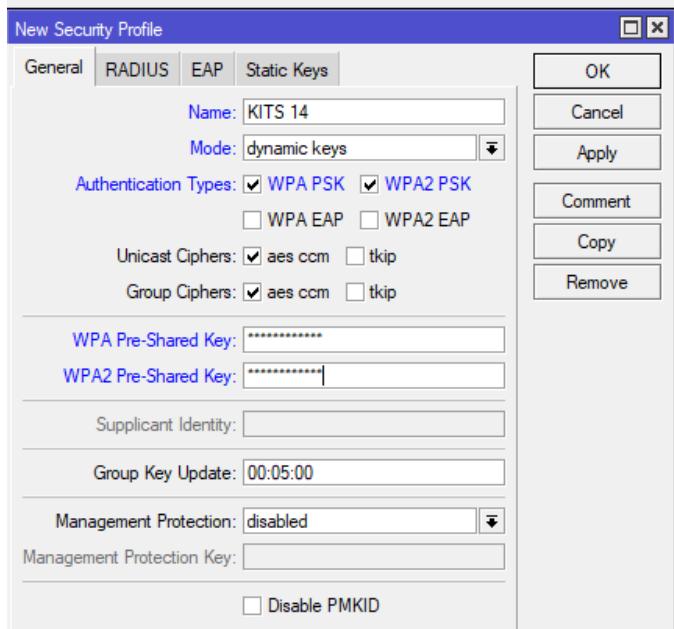
## LAB 17 Security Profile (Authentication and Encryption)

Pada lab ini kita akan membahas tentang yaitu security profile yaitu salah satu fitur untuk keamanan wireless

1. Masuk ke dalam Winbox
2. Lalu wireless dan kalian pilih security profile dan klik +

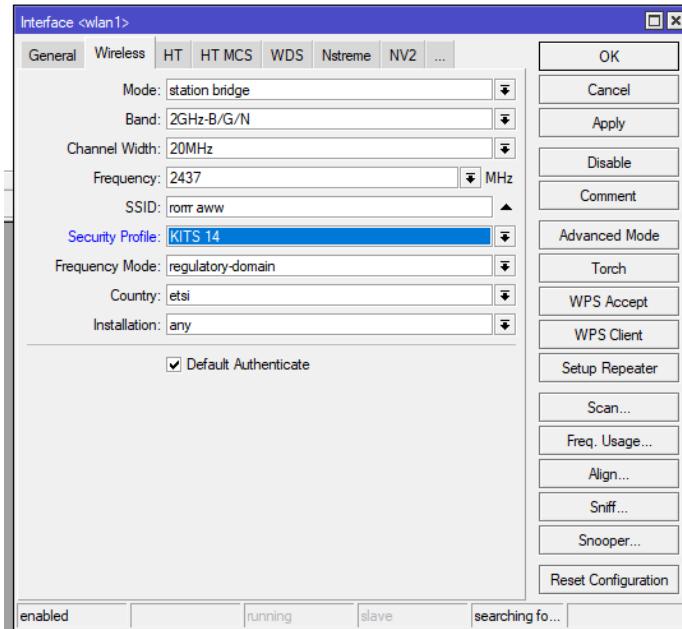


3. Berikutnya kalian ganti menjadi dynamic keys dan setting sesuai di bawah dan minimal untuk password adalah 8 huruf

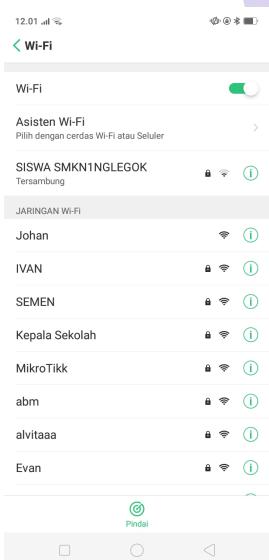




4. Masuk kembali ke wifi interface
5. Dan masukkan security profile yang sudah kalian buat tadi



### Lakukan Pengetesan



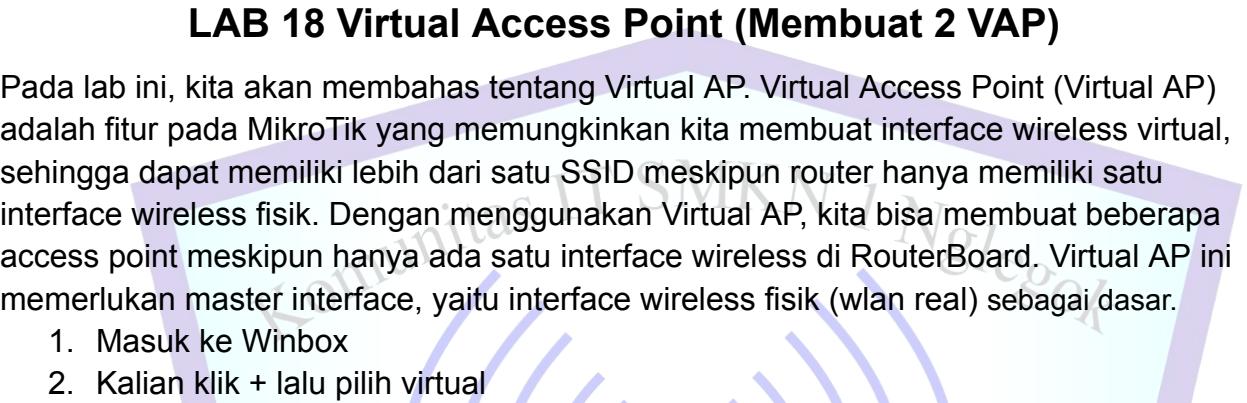
Dan disini sudah terdapat Password pada Wifi Evan



## LAB 18 Virtual Access Point (Membuat 2 VAP)

Pada lab ini, kita akan membahas tentang Virtual AP. Virtual Access Point (Virtual AP) adalah fitur pada MikroTik yang memungkinkan kita membuat interface wireless virtual, sehingga dapat memiliki lebih dari satu SSID meskipun router hanya memiliki satu interface wireless fisik. Dengan menggunakan Virtual AP, kita bisa membuat beberapa access point meskipun hanya ada satu interface wireless di RouterBoard. Virtual AP ini memerlukan master interface, yaitu interface wireless fisik (wlan real) sebagai dasar.

1. Masuk ke Winbox
2. Kalian klik + lalu pilih virtual



A screenshot of the Winbox Wireless Tables window. The title bar says "Wireless Tables". The menu bar includes WiFi Interfaces, W60G Station, Nstreme Dual, Access List, Registration, Connect List, Security Profiles, Channels, and Interworking Profiles. Below the menu is a toolbar with icons for adding (+), deleting (-), selecting (checkmark), deleting (cross), creating (file), filtering (magnifying glass), CAP, WPS Client, Setup Repeater, Scanner, Freq. Usage, Alignment, Wireless Sniffer, and Wireless Snooper. A "Find" button is also present. The main table has columns for Interface, Actual M..., Tx, Rx, Tx Packet (p/s), Rx Packet (p/s), and FP Tx. There are three rows: "Virtual" (selected), "WDS", and "Nstreme Dual". The status bar at the bottom left shows "1 item out of 6 (1 selected)".

Interface	Actual M...	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
Virtual	ess (Atheros AR9...)	1500	72.2 kbps	36.4 kbps	17	14
WDS						
Nstreme Dual						

3. Kalian Pilih SSD sesuai keinginan lalu master interface kalian pilih wlan 1



New Interface

General Wireless WDS Status Traffic

Mode: ap bridge

Secondary Channel:

SSID: KITS 14 HEBAT

Master Interface: wlan1

Security Profile: KITS 14

Interworking Profile: disabled

WPS Mode: disabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Advanced Mode Torch

Dan Virtual Ap sudah dilakukan

Wireless Tables

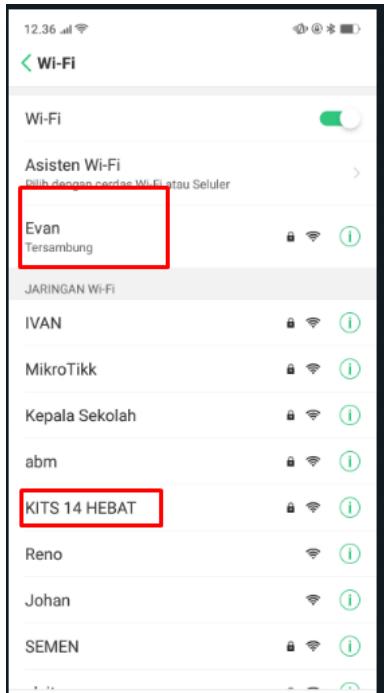
WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels Interworking Profiles

+ - ✓ ✘ 🔍 CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper Find

Name	Type	Actual M...	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
wlan1	Wireless (Atheros AR9...)	1500	458.0 kbps	0 bps	50	0	0
wlan2	Virtual	1500	0 bps	0 bps	0	0	0

2 items out of 7 (1 selected)

Kita lakukan Pengetesan Pada hanphone saya

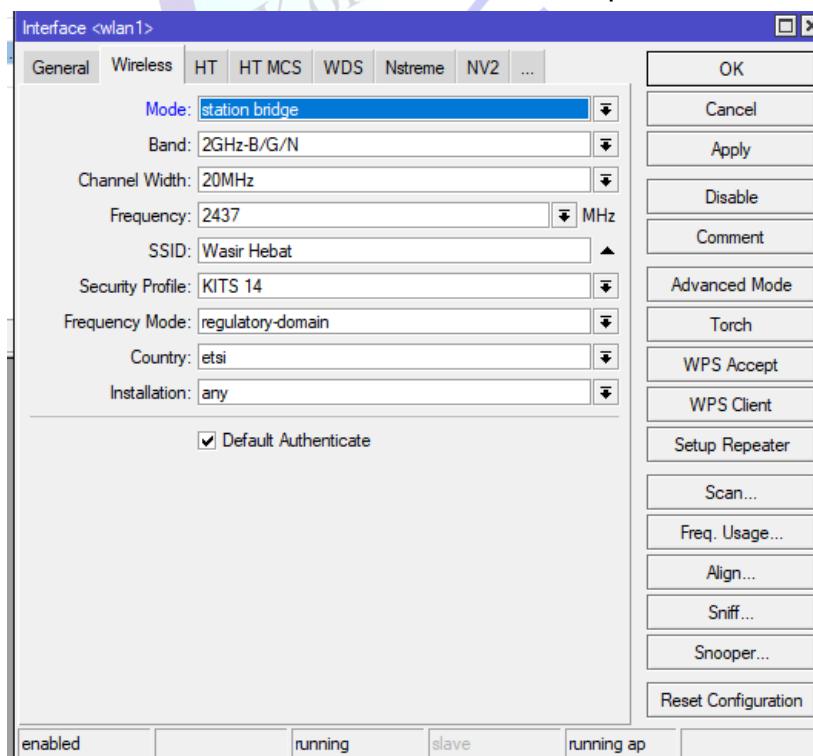




## LAB 19 Virtual Access Point + Router Gateway (Repeater)

Pada lab ini, kita akan menggunakan dua mode WLAN, yaitu Station dan AP Bridge, dengan hanya satu interface WLAN. MikroTik akan berfungsi sebagai repeater, yang menangkap sinyal Wi-Fi yang ada di sekitar dan mengubahnya menjadi layanan ISP, kemudian membagikannya kembali ke pengguna di sekitarnya. Dalam lab ini, saya menggunakan routerboard RB951Ui-2nD. Berikut adalah topologi jaringan yang digunakan.

1. Masuk ke dalam winbox
2. Lalu Kalian Masuk ke Interface dan pilih wlan1



3. Berikutnya kalian buat interface baru dengan cara klik tombol + lalu pilih virtual



Wireless Tables							
	Virtual	Actual M...	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
	Virtual	Actual M...	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
	WDS	Address (Atheros AR9...)	1500	72.2 kbps	36.4 kbps	17	14
	Nstreme Dual						

4. Seperti pada contoh di bawah ini

New Interface

General Wireless WDS Status Traffic

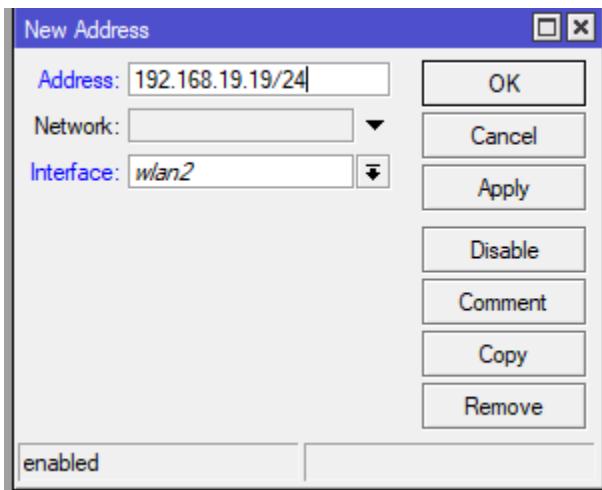
Mode: ap bridge  
Secondary Channel:  
SSID: Evan 2  
Master Interface: wlan1  
Security Profile: KITS 14  
Interworking Profile: disabled  
WPS Mode: disabled  
VLAN Mode: no tag  
VLAN ID: 1  
Default AP Tx Rate:  
Default Client Tx Rate:  
 Default Authenticate  
 Default Forward  
 Hide SSID

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Advanced Mode Torch

5. Berikutnya kita setting ip pada wlan 2

6. Masuk kedalam IP lalu address dan pilih tombol +



7. Step berikutnya masuk ke IP DHCP server dan DHCP setup wlan 2 next hingga sukses



## LAB 20 Tunnel (EoIP, PPTP, L2TP, PPPoE)

Pada lab kali ini, saya akan membahas tentang **Tunnel**. Tunnel adalah protokol yang memungkinkan perpindahan data secara aman antara satu jaringan dengan jaringan lainnya. Tunneling memungkinkan komunikasi jaringan pribadi atau koneksi point-to-point untuk dikirim melalui jaringan publik, seperti internet, melalui proses yang disebut **encapsulation**. Proses ini memungkinkan paket data terlihat seperti data publik saat melewati jaringan publik, padahal sebenarnya itu adalah data pribadi, sehingga bisa melewati tanpa terdeteksi.

Secara sederhana, Tunnel adalah sebuah "terowongan" yang dibangun di dalam jaringan publik. Ibaratnya, kita membuat terowongan di tengah jalan raya metropolitan, dan data (ibarat orang) yang melewati terowongan tersebut tidak akan diganggu oleh orang lain (data) yang berada di jalan raya umum. Tunneling adalah dasar dari **VPN (Virtual Private Network)** yang memungkinkan pembuatan jaringan pribadi melalui internet global.

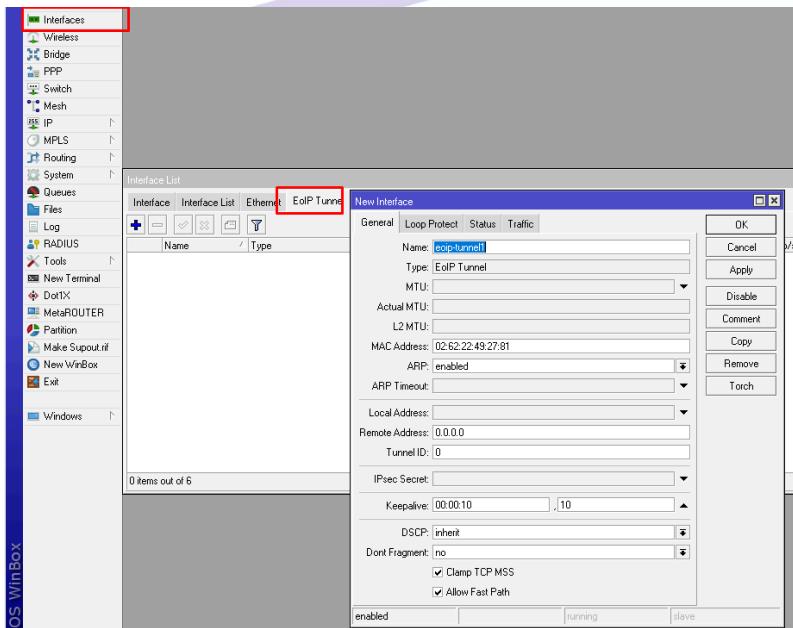
Pada beberapa jenis Tunnel, proses Tunneling juga meliputi **enkapsulasi** dan **enkripsi data** untuk menjamin keamanan data saat pengiriman. Dalam Tunnel, data hanya melewati satu jalur, sehingga hanya ada satu lompatan (hop). Untuk Tunnel pada VPN, enkripsi digunakan untuk melindungi data pengguna. Syarat dasar untuk membuat Tunnel adalah kedua perangkat harus memiliki IP publik dan terhubung ke internet.

### A.EoIP

EoIP Tunnel (Ethernet over IP) adalah fitur di MikroTik yang memungkinkan pengguna mengirimkan lalu lintas Ethernet antar jaringan melalui koneksi IP. EoIP Tunnel menciptakan sebuah "terowongan" di atas IP antara dua MikroTik, memungkinkan dua jaringan lokal yang terpisah oleh jaringan publik untuk terhubung. Konsep EoIP Tunnel adalah dengan membungkus lalu lintas Ethernet dalam paket IP dan mengirimkannya melalui jaringan publik atau koneksi IP yang ada.



1. Langkah pertama kalian masuk ke winbox seperti biasa
2. Langlah selanjutnya kalian konfigurasikan agar client mendapatkan internet, lalu kalian konfigurasikan ip pada ether 1 dengan cara kalian masuk ke interface >EoLP lalu klik tombol + pada kolom nama isikan seperti pada contoh yaitu eoip pc 1. Untuk remot address kalian bisa isikan dengan ip public router 2, dan pada tunnel id saya isikan 7.





New Interface

General Loop Protect Status Traffic

Name: **e0ip-tunnel1 R1**

Type: EoIP Tunnel

MTU:

Actual MTU:

L2 MTU:

MAC Address: 02:88:D9:C0:2B:0A

ARP: enabled

ARP Timeout:

Local Address:

Remote Address: 192.168.87.3

Tunnel ID: 7

IPsec Secret:

Keepalive: 00:00:10 , 10

DSCP: inherit

Dont Fragment: no

Clamp TCP MSS

Allow Fast Path

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Torch

### 3. Setelah itu kalian buat interface bridge pada kedua router

New Interface

General STP VLAN Status Traffic **R1**

Name: **bridge1 R1**

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP: enabled

ARP Timeout:

Admin. MAC Address:

Ageing Time: 00:05:00

IGMP Snooping

DHCP Snooping

Fast Forward

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Torch

New Interface

General STP VLAN Status Traffic

Name: **bridge1R2**

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP: enabled

ARP Timeout:

Admin. MAC Address:

Ageing Time: 00:05:00

IGMP Snooping

DHCP Snooping

Fast Forward

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Torch



#### 4. Setelah itu kita Assign Interface Eoip Tunnel dan Interface yang mengarah ke router

Bridge										
#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	Role	Root Pat...		
0 H	ether2	bridge1 R1		no	80	10	designated port			
1	eoip-tunnel7 R1	bridge1 R1		no	80	10	disabled port			

Bridge										
#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	Role	Root Pat...		
0 H	ether2	bridge1 R2		no	80	10	designated port			
1	eoip-tunnel1 R2	bridge1 R2		no	80	10	designated port			

#### 5. Dan jika sudah maka interface last akan seperti dibawah ini, Eoip Tunnel dan ether akan menjadi RS(Running Sealve) dan Bridgenya adalah R(Running)

Interface List															
Interface		Interface List		Ethernet		EoIP Tunnel		IP Tunnel		GRE Tunnel		VLAN		VRP	
Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx	Packet (p/s)	Rx	Packet (p/s)	FP Tx	FP Rx	FP Tx	FP Rx	FP Tx	FP Rx
R	bridge1 R1	Bridge	1458	1598	0 bps	5.9 kbps	0	12	0 bps	498 bps	0	0	0	1	0
S	eoip-tunnel1 R1	EoIP Tunnel	1458	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0	0	0	0
R	ether1	Ethernet	1500	1598	512 bps	1072 bps	1	2	480 bps	1008 bps	1	2	0	0	0
RS	ether2	Ethernet	1500	1598	98.5 kbps	7.5 kbps	12	12	98.1 kbps	7.1 kbps	12	12	0	0	0
R	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	0	0	0
R	ether4	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	0	0	0
R	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	0	0	0
R	wlan1	Wireless (Atheros AR9...	1500	1600	336 bps	0 bps	1	0	0 bps	0 bps	0	0	0	0	0

Interface List															
Interface		Interface List		Ethernet		EoIP Tunnel		IP Tunnel		GRE Tunnel		VLAN		VRP	
Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx	Packet (p/s)	Rx	Packet (p/s)	FP Tx	FP Rx	FP Tx	FP Rx	FP Tx	FP Rx
R	bridge1 R2	Bridge	1458	1598	0 bps	4.8 kbps	0	10	0 bps	0 bps	0	0	0	0	0
RS	eoip-tunnel1 R2	EoIP Tunnel	1458	65535	14.6 kbps	0 bps	14	0	0 bps	0 bps	0	0	0	0	0
R	ether1	Ethernet	1500	1598	19.7 kbps	0 bps	18	0	19.1 kbps	0 bps	0	0	18	0	0
RS	ether2	Ethernet	1500	1598	79.6 kbps	6.8 kbps	12	11	79.2 kbps	6.4 kbps	12	12	0	0	0



6. Dan dibawah ini adalah ip last yang berada pada setiap interface

Address List		
Address	Network	Interface
192.168.10.1/...	192.168.10.0	bridge1 R1

Address List		
Address	Network	Interface
192.168.10.2	192.168.10.2	bridge1R2
192.168.19.19...	192.168.19.0	ether2
D 192.168.87.73...	192.168.87.0	ether1

7. Setelah itu kita setting ip pada client

8. Jika sudah kita akan melakukan uji coba dengan cara ping antar kedua router

```
C:\Users\pc-lab-3>ping 192.168.10.5  
Pinging 192.168.10.5 with 32 bytes of data:  
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.10.5:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

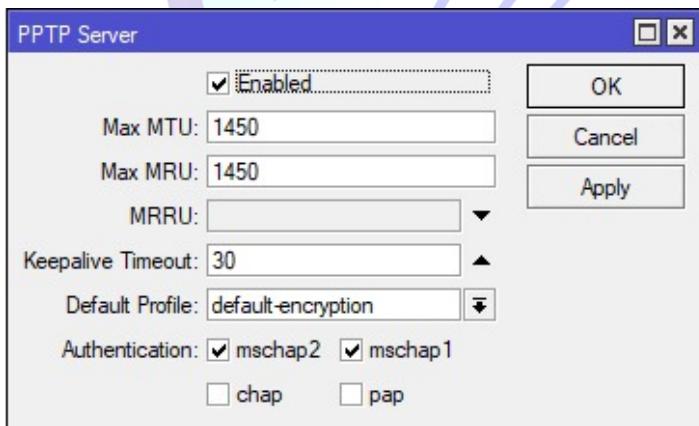
```
C:\> C:\WINDOWS\system32\cmd. +   
Microsoft Windows [Version 10.0.22631.4317]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\pc-lab-3>ping 192.168.10.6  
Pinging 192.168.10.6 with 32 bytes of data:  
Reply from 192.168.10.6: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.10.6:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



## B.PPtP

### I Skenario 1

1. Langkah pertama kalian login dan remote Mikrotik, lalu buat konfigurasi agar router dapat mengakses internet. Jika sudah kita akan membuat konfigurasi PPTP Server pada R1
2. Masuk ke PPP> interface > dan pptp server lalu kalian enabled kan



3. Masuk ke secret lalu klik tombol + untuk membuat baru, disini sebagai contoh saya membuat dengan nama evan dan paswordnya adalah Evan2008, dan service yang saya gunakan adalah any. Untuk local address dan remote address kalian isikan ip yang akan di berikan interface pptp pada Client, dan ingat bahwa ip harus 1 jaringan.

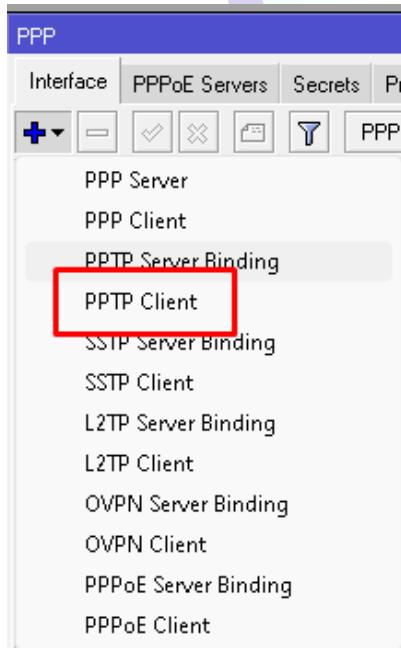


PPP Secret <Evan>

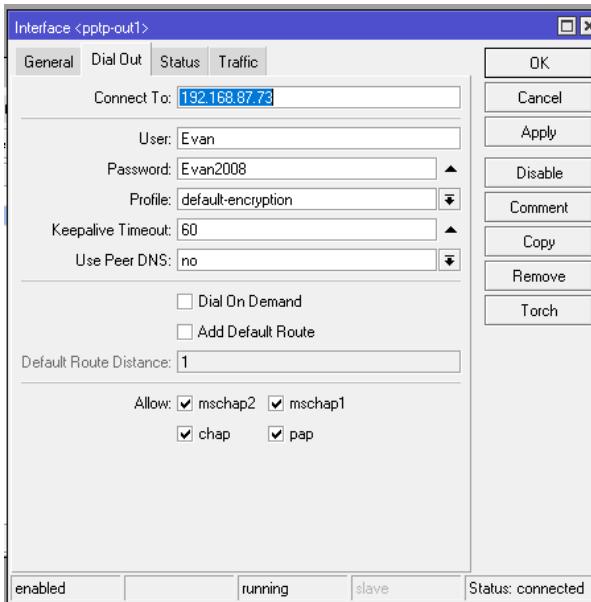
Name:	Evan
Password:	Evan2008
Service:	any
Caller ID:	
Profile:	default
Local Address:	10.10.10.1
Remote Address:	10.10.10.2
Remote IPv6 Prefix:	
Routes:	
IPv6 Routes:	
Limit Bytes In:	
Limit Bytes Out:	
Last Logged Out:	Jan/01/2002 03:14:03
Last Caller ID:	192.168.87.95
Last Disconnect Reason:	nas request
enabled	

OK Cancel Apply Disable Comment Copy Remove

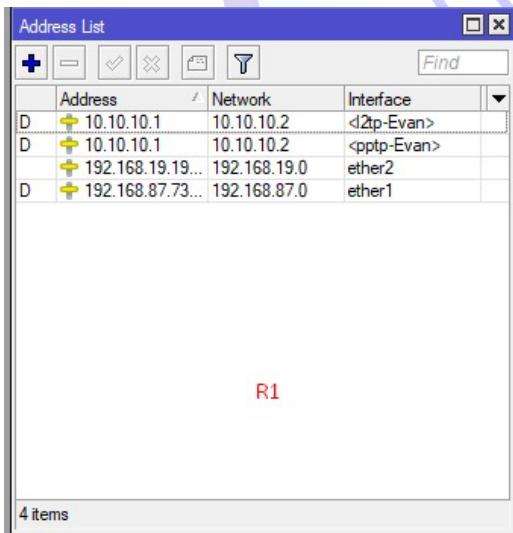
4. Jika sudah kita setting pada sisi client, kalian masuk ke ppp interface dan kalian pilih pptp client



5. Kalian setting yang dial out. Untuk connectnya kalian isikan ip public dari router 1 yang kalian dapat secara otomatis dari dhcp client, lalu untuk user dan passwordnya kalian isi sebagai mana yang telah kalian buat tadi. Pastikan statusnya connected.



6. Untuk mengeceknya kalian masuk ke ip address dan sini kita sudah sejaringan dengan server dan ip akan terisi secara dynamic





Address List			
	Address	Network	Interface
D	10.10.10.2	10.10.10.1	l2tp-out1
D	10.10.10.2	10.10.10.1	pptp-out1
D	192.168.25.19...	192.168.25.0	ether2
D	192.168.25.19...	192.168.25.0	wlan7
D	192.168.87.95...	192.168.87.0	ether1

R2

7. Untuk melakukan ping kalian harus membuat konfigurasi routing static. Untuk dst address kalian isikan ip network dari ether 2 lawan sedangkan untuk gateway isikan ip dari lawan yang diperoleh secara dynamic tadi

Route <192.168.25.0/24>

General Attributes

Dst. Address: 192.168.25.0/24

Gateway: 10.10.10.2 reachable <pptp-Evan>

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

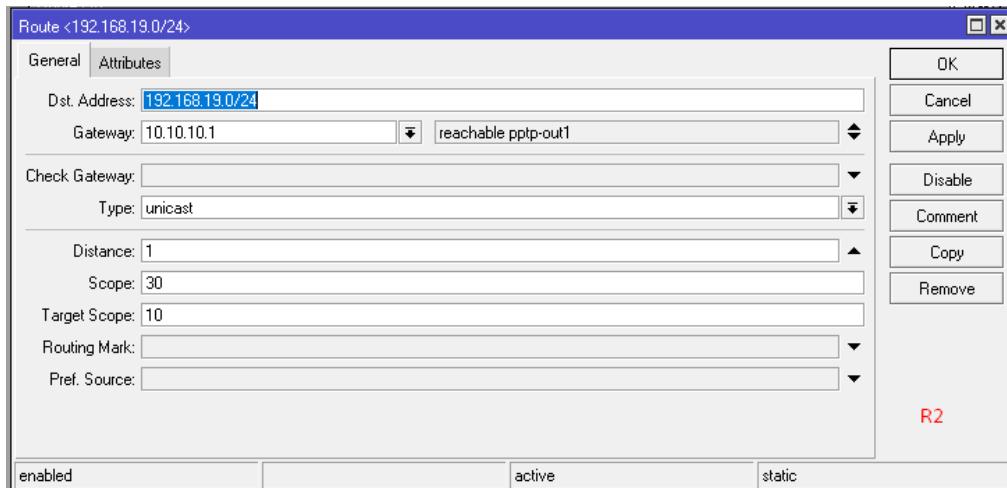
Routing Mark:

Pref. Source:

OK Cancel Apply Disable Comment Copy Remove

enabled active static

R1



8. Langkah terakhir masuk ke cmd lalu kalian coba ping antar router, jika ttl maka konfigurasinya sudah benar

```
C:\Users\pc-lab-3>ping 192.168.25.19

Pinging 192.168.25.19 with 32 bytes of data:
Reply from 192.168.25.19: bytes=32 time<1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.25.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

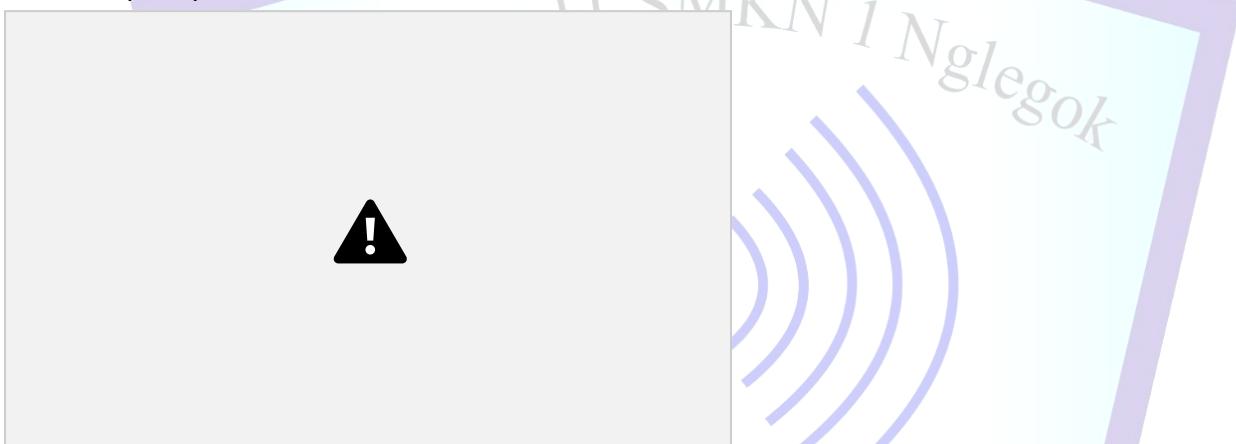
```
B C:\Users\pc-lab-3>ping 192.168.25.19
F
S Pinging 192.168.25.19 with 32 bytes of data:
M Reply from 192.168.25.19: bytes=32 time<1ms TTL=64
M Reply from 192.168.25.19: bytes=32 time<1ms TTL=64
M Reply from 192.168.25.19: bytes=32 time<1ms TTL=64
F Reply from 192.168.25.19: bytes=32 time<1ms TTL=64
S
G Ping statistics for 192.168.25.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
L Approximate round trip times in milli-seconds:
F     Minimum = 0ms, Maximum = 0ms, Average = 0ms
T
```



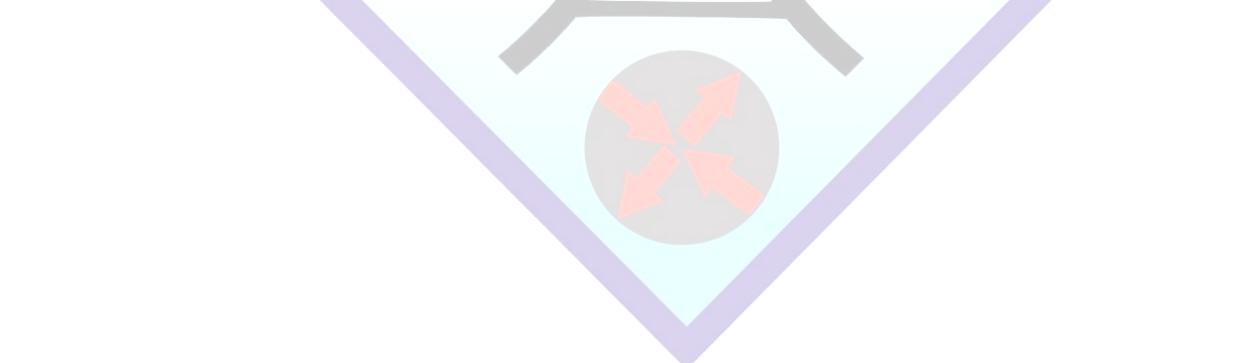
## II. Skenario 2

Untuk skenario 2 kita akan mengakses dengan cara yang berbeda mari kita lihat konfigurasinya.

1. Langkah pertama kalian remote dan login terlebih dahulu ke Mikrotik. Lalu kalian buat agar mikrotik mendapatkan internet. Jika sudah kalian aktifkan pptp server pada router seperti pada skenario 1 tadi



2. Masuk ke secret lalu klik tombol + untuk membuat baru, disini sebagai contoh saya membuat dengan nama evan dan paswordnya adalah Evan2008, dan service yang saya gunakan adalah any. Untuk local address dan remote address kalian isikan ip yang akan di berikan interface pptp pada Client, dan ingat bahwa ip harus 1 jaringan.





PPP Secret <Evan>

Name:	Evan	OK
Password:	Evan2008	Cancel
Service:	any	Apply
Caller ID:		Disable
Profile:	default	Comment
Local Address:	10.10.10.1	Copy
Remote Address:	10.10.10.2	Remove
Remote IPv6 Prefix:		
Routes:		
IPv6 Routes:		
Limit Bytes In:		
Limit Bytes Out:		
Last Logged Out:	Jan/01/2002 03:55:59	
Last Caller ID:	192.168.87.95	
Last Disconnect Reason:	peer request	
enabled		

3. Jika sudah masuk ke setting lalu pilih network and internet  
[Back up and Restore \(Windows 7\)](#)



**Network and Internet**  
[View network status and tasks](#)



**Hardware and Sound**

4. Jika sudah klik yang set up a new connection or network.

Change your networking settings



[Set up a new connection or network](#)

Set up a broadband, dial-up or VPN connection, or set up a ro...

5. Pilih yang connect to a workplace



- Connect to the Internet  
Set up a broadband or dial-up connection to the Internet.
- Set up a new network  
Set up a new router or access point.
- Connect to a workplace  
Set up a dial-up or VPN connection to your workplace.

6. Dan klik yang use my internet connection (VPN)

← Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)  
Connect using a virtual private network (VPN) connection through the Internet.



→ Dial directly  
Connect directly to a phone number without going through the Internet.



7. Kalian masukkan nama secret yang telah kalian buat tadi

Windows Security

### Sign in

Username

Evan

Password

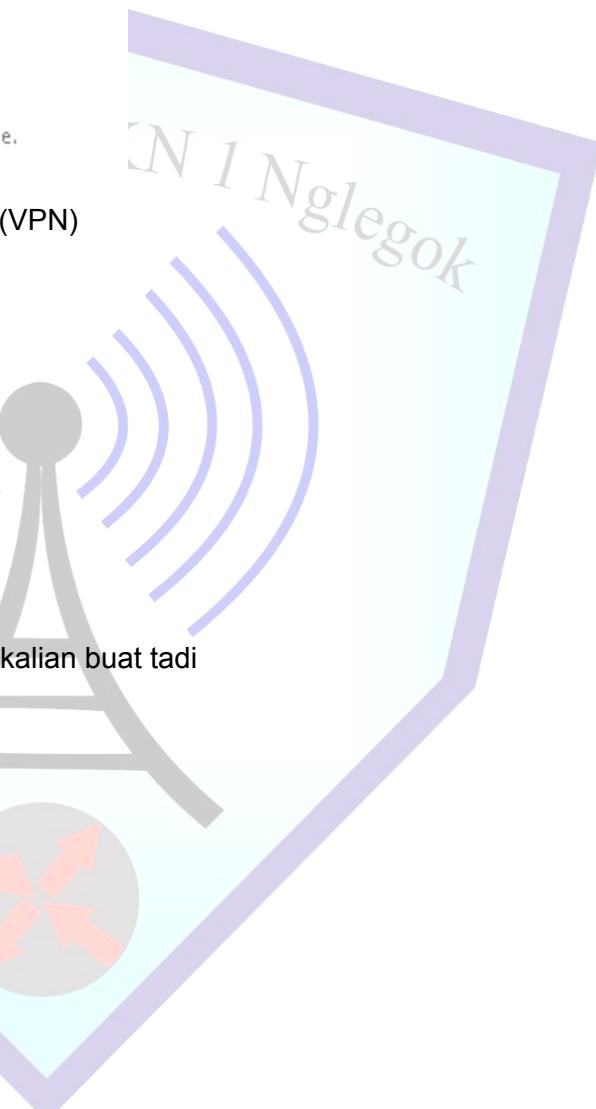
\*\*\*\*\*

The username or password is incorrect.

OK

Cancel

8. Bisa dililah di bawah ini adalah bagian network yang semula terisi ethernet yang menyambung dengan internet, sekarang muncul pptp yang telah kita buat konfigurasinya tadi.

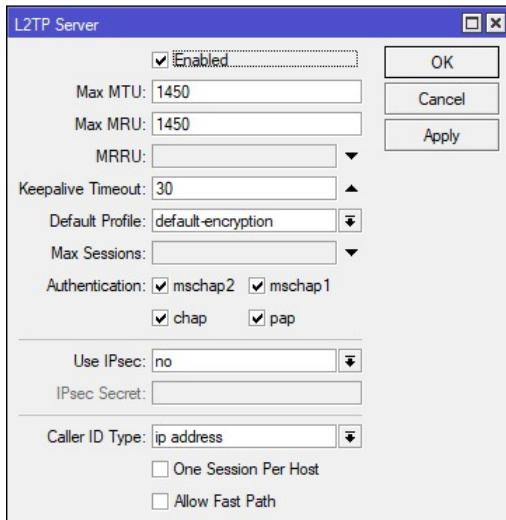




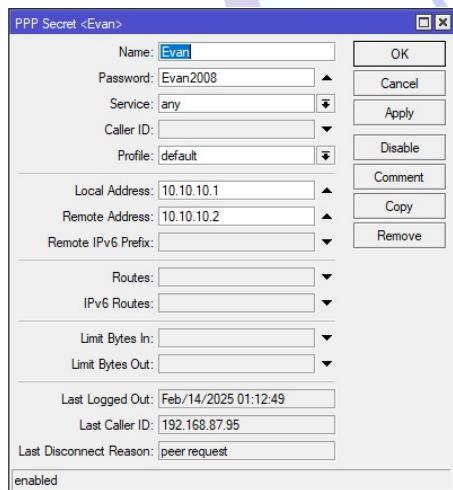
## C.L2TP Tunnel

L2TP (Layer Two Tunneling Protocol) adalah protokol jaringan yang digunakan untuk membuat koneksi tunneling yang aman antar perangkat melalui jaringan publik, seperti internet. L2TP bekerja pada layer 2 (data link layer) dan sering dipasangkan dengan protokol keamanan seperti IPsec untuk memastikan data yang dikirimkan terlindungi dengan enkripsi. Tujuan utama L2TP adalah untuk menghubungkan dua jaringan atau perangkat secara virtual seolah-olah berada dalam satu jaringan lokal meskipun mereka terpisah secara fisik.

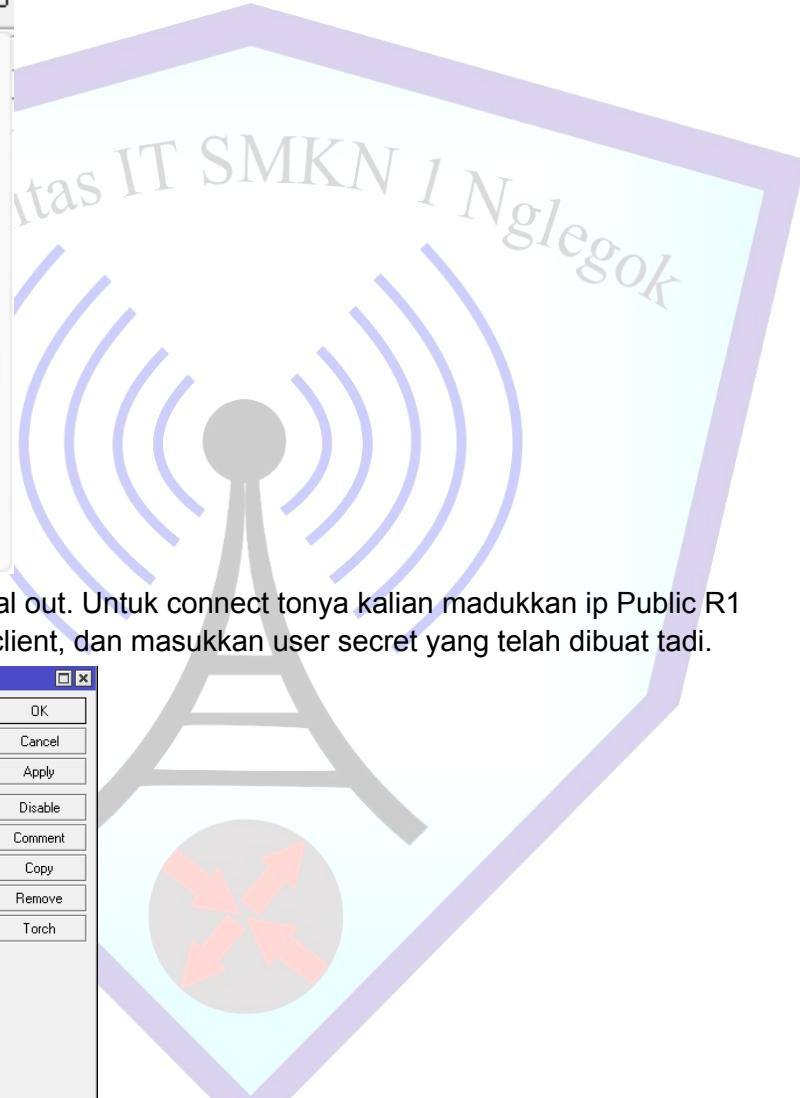
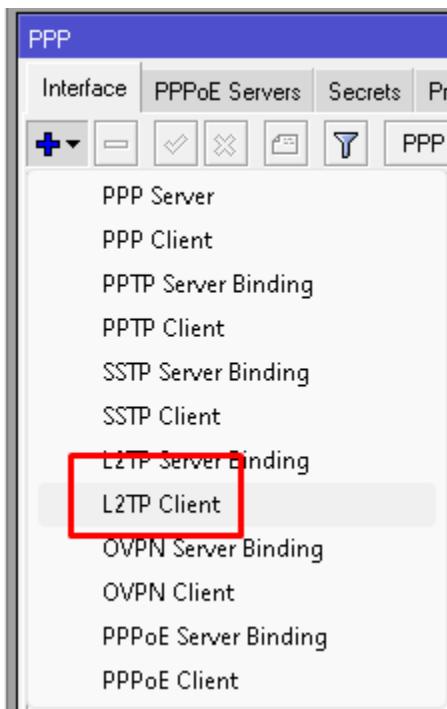
1. Langkah pertama pada konfigurasi L2TP kali ini kalian login lalu remote mikrotik serta konfigurasikan agar semua perangkat mendapat akses internet. Untuk R1 sebagai l2tp server dan R2 sebagai l2tp client. Masuk ke dalam PPP> lalu interface dan l2tp server kalian enabledkan.



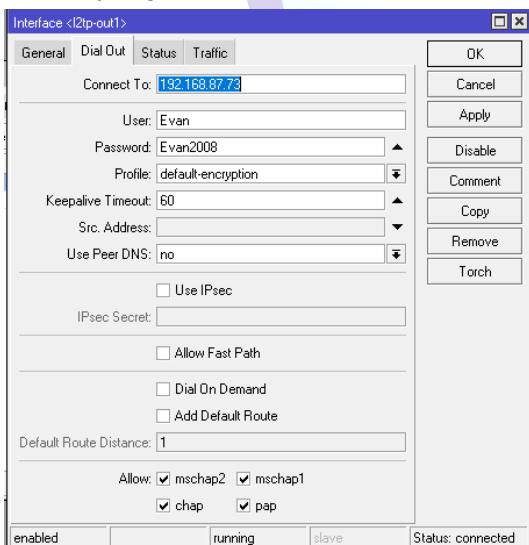
2. Masuk ke secret lalu klik tombol + untuk membuat baru, disini sebagai contoh saya membuat dengan nama evan dan paswordnya adalah Evan2008, dan service yang saya gunakan adalah any. Untuk local address dan remote address kalian isikan ip yang akan di berikan interface pptp pada Client, dan ingan bahwa ip harus 1 jaringan.



3. Kita konfigurasikan l2tp pada sisi client. Kalian klik tombol + lalu pilih l2tp client.



4. Kalian masuk ke dalam dial out. Untuk connect tonya kalian madukkan ip Public R1 yang diperoleh dari dhcp client, dan masukkan user secret yang telah dibuat tadi.



5. Jika semua sudah dilakukan kita lakukan pengecekan pada ip.

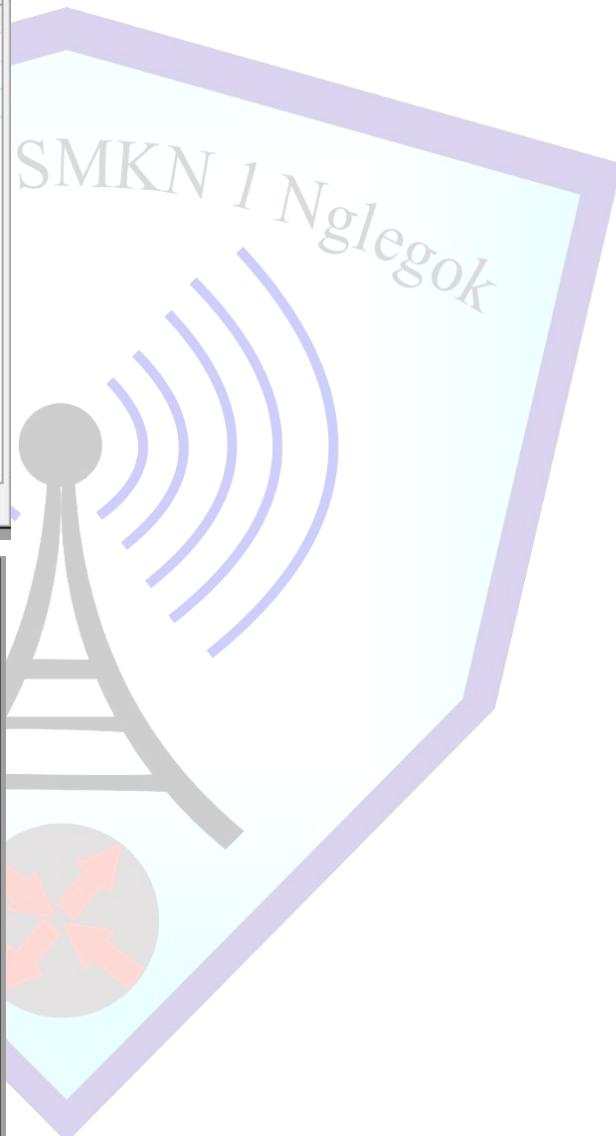


	Address	Network	Interface
D	10.10.10.1	10.10.10.2	<l2tp-Evan>
D	10.10.10.1	10.10.10.2	<pptp-Evan>
D	192.168.19.19...	192.168.19.0	ether2
D	192.168.87.73...	192.168.87.0	ether1

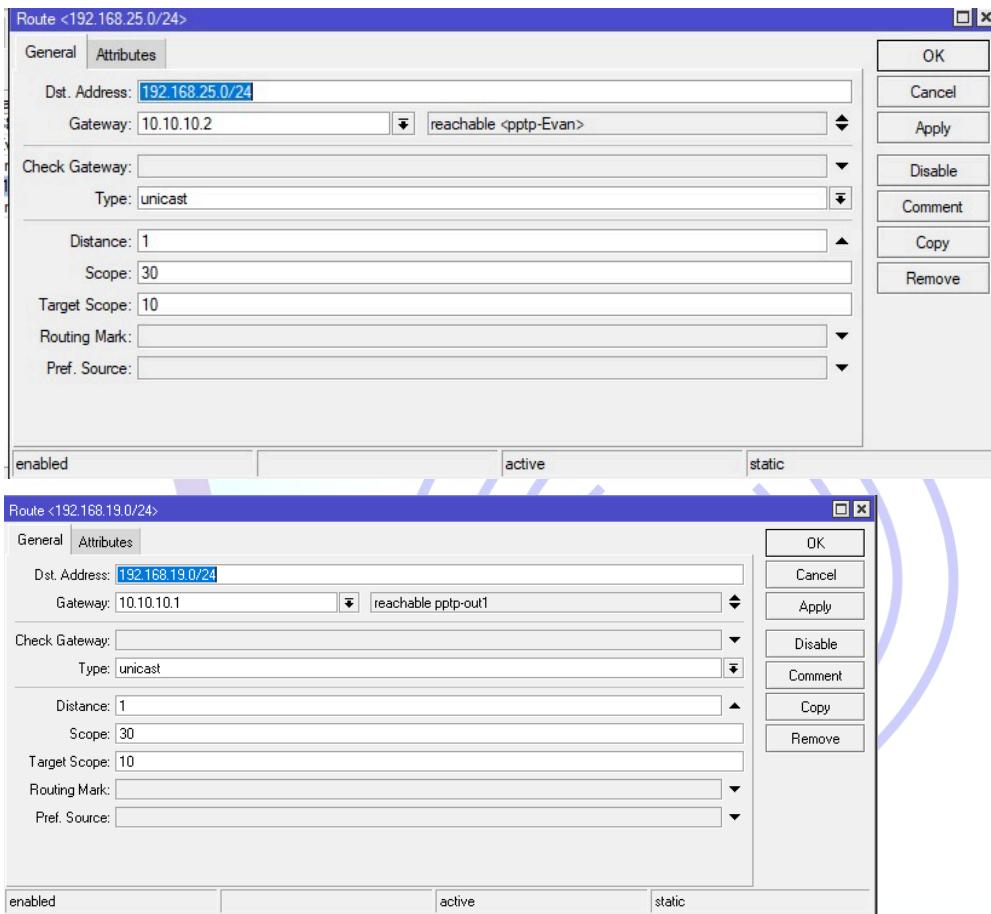
4 items

	Address	Network	Interface
D	10.10.10.2	10.10.10.1	l2tp-out1
D	10.10.10.2	10.10.10.1	pptp-out1
D	192.168.25.19...	192.168.25.0	ether2
D	192.168.25.19...	192.168.25.0	wlan1
D	192.168.87.95...	192.168.87.0	ether1

5 items



6. Langkah selanjutnya masuk ke ip route dan kita buat konfigurasi router static. Untuk dst add kalian isikan ip ether 2 dari lawan dan gateway ether 1 dari lawan.



7. Langkah terakhir kalian ping antar pc dan jika hasilnya ttl maka konfigurasi kalian sudah benar.

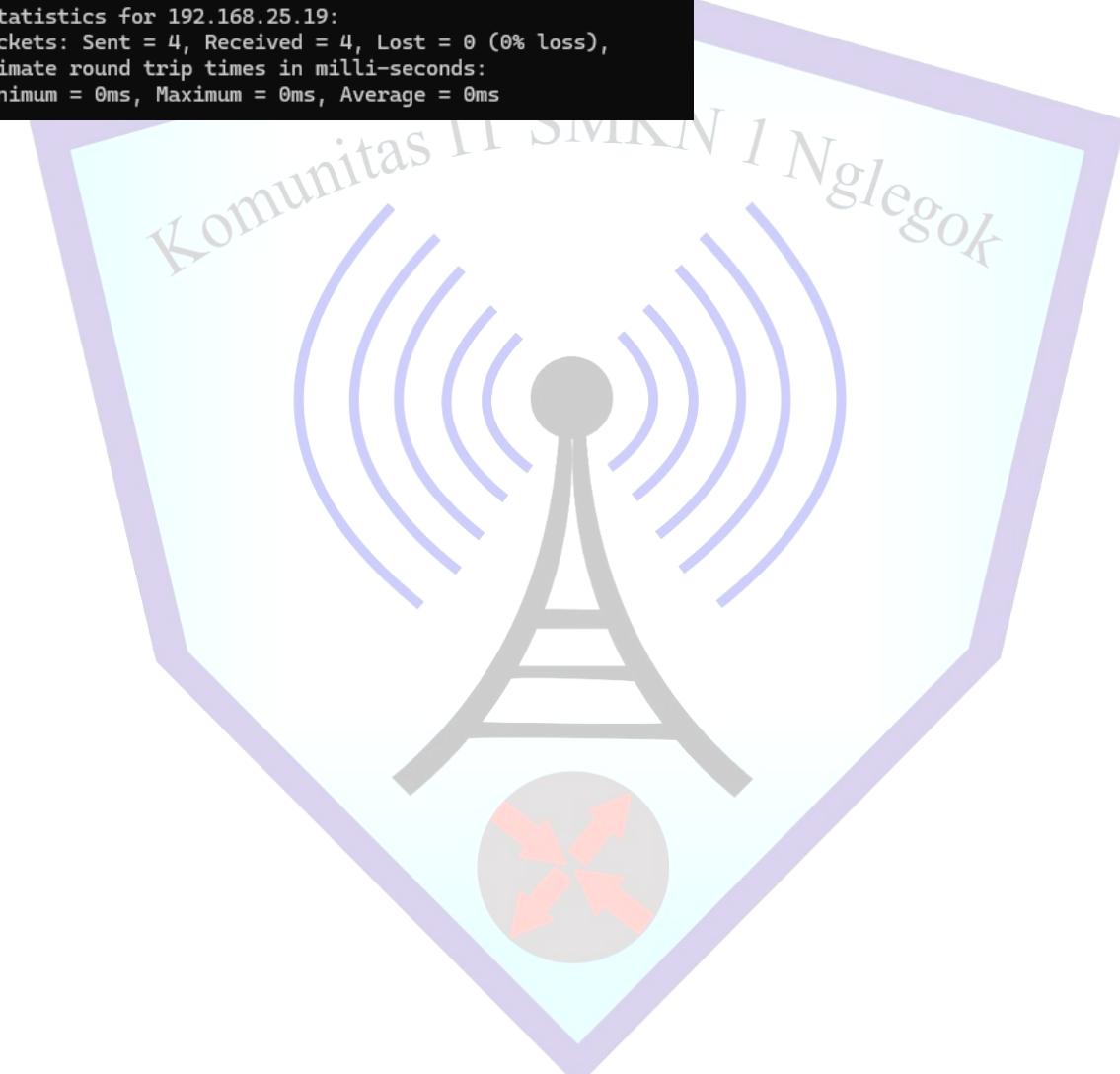
```
C:\Users\pc-lab-3>ping 192.168.25.19

Pinging 192.168.25.19 with 32 bytes of data:
Reply from 192.168.25.19: bytes=32 time<1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63
Reply from 192.168.25.19: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.25.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
Pinging 192.168.25.19 with 32 bytes of data:  
Reply from 192.168.25.19: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.25.19:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



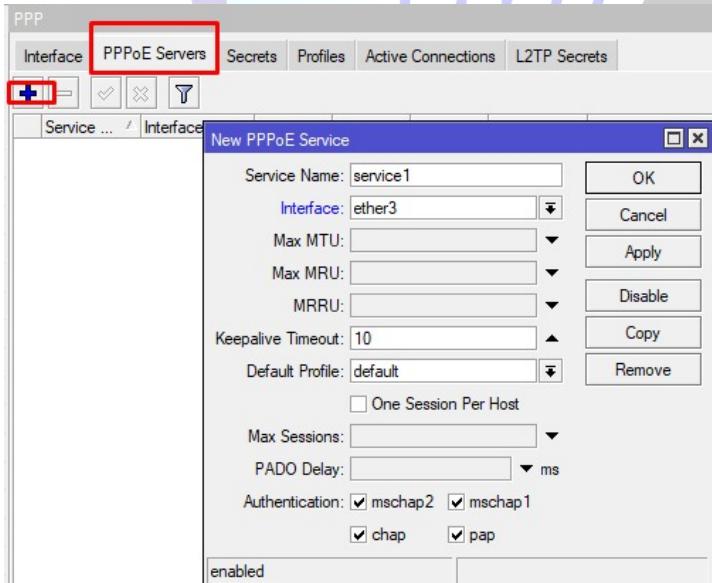


## D.PPoE Tunnel

Pada lab ini kita akan belajar mengenai PPPoE (Point-to-Point Protocol over Ethernet) adalah protokol yang digunakan untuk menghubungkan perangkat ke jaringan melalui sambungan broadband Ethernet. PPPoE membuat "tunnel" yang memungkinkan pengiriman data antara pengguna dan penyedia layanan internet (ISP) secara aman. Protokol ini digunakan untuk autentikasi, pengaturan sesi, dan pemantauan penggunaan bandwidth. Dalam PPPoE, setiap koneksi pelanggan diidentifikasi dan dikelola secara terpisah, sering kali digunakan pada layanan DSL atau koneksi broadband berbasis Ethernet.

### I. Skenario 1

1. Langkah pertama kalian login dan remote serta konfigurasikan seperti biasa. Masuk ke dalam PPoE Servers lalu klik tombol +, untuk interfacenya kalian pilih ke router client disini saya menggunakan ether 3.



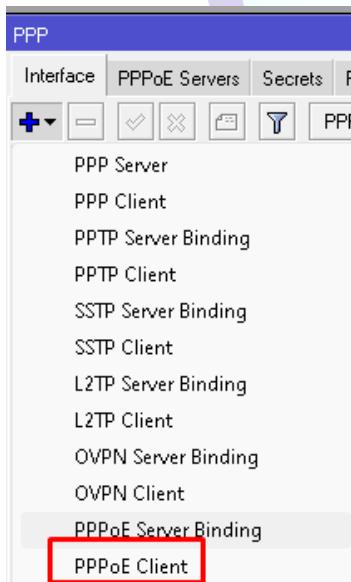
2. Masuk ke secret lalu klik tombol + untuk membuat baru, disini sebagai contoh saya membuat dengan nama evan dan paswordnya adalah Evan2008, dan service yang saya gunakan adalah any. Untuk local address dan remote address kalian isikan ip yang akan di berikan interface pptp pada Client, dan ingat bahwa ip harus 1 jaringan.



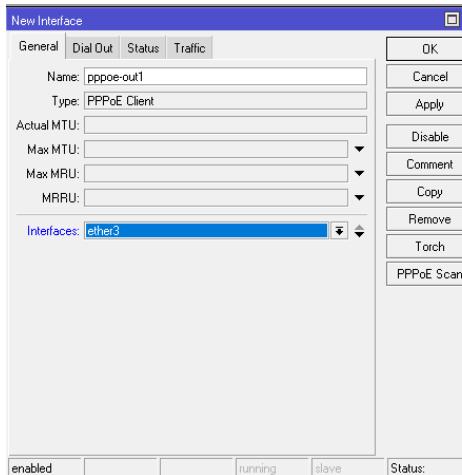
PPP Secret <Evan>

Name:	Evan	OK
Password:	Evan2008	Cancel
Service:	any	Apply
Caller ID:		Disable
Profile:	default	Comment
Local Address:	10.10.10.1	Copy
Remote Address:	10.10.10.2	Remove
Remote IPv6 Prefix:		
Routes:		
IPv6 Routes:		
Limit Bytes In:		
Limit Bytes Out:		
Last Logged Out:	Feb/14/2025 01:12:49	
Last Caller ID:	192.168.87.95	
Last Disconnect Reason:	peer request	
enabled		

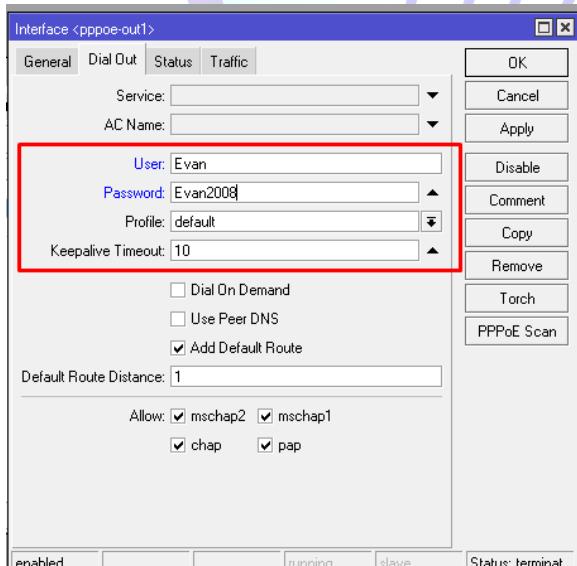
3. Berikutnya kita konfigurasi dari sisi client, masuk ke PPP lalu pilih interface dan klik + pilih yang PPoE Client.



4. Pada menu interface kalian plih yang mengarah ke router service.



5. Berikutnya masuk ke dial out kalian masukkan user dan password secret kalian



6. Jika status sudah connect mala kalian chek di ip address masing" router kalian akan mendapatkan ip secara dynamic.



Address List

	Address	Network	Interface
D	10.10.10.1	10.10.10.2	<l2tp-Evan>
D	10.10.10.1	10.10.10.2	<pptp-Evan>
D	10.10.10.1	10.10.10.2	<pppoe-Evan>
D	192.168.19.19...	192.168.19.0	ether2
D	192.168.87.73...	192.168.87.0	ether1

5 items

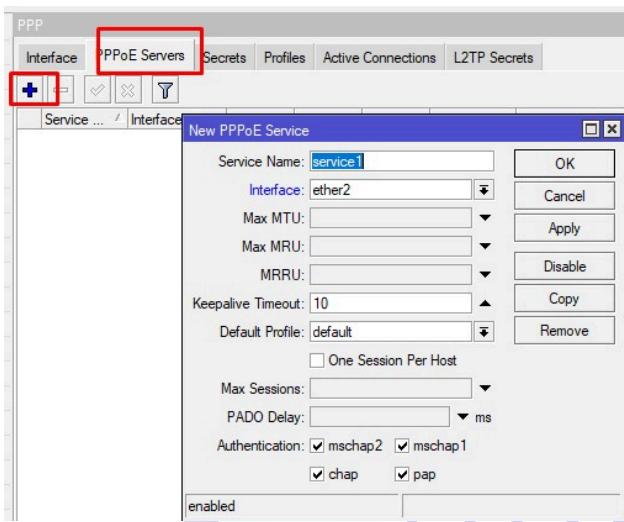
Address List

	Address	Network	Interface
D	10.10.10.2	10.10.10.1	l2tp-out1
D	10.10.10.2	10.10.10.1	pptp-out1
D	10.10.10.2	10.10.10.1	pppoe-out1
D	192.168.25.19...	192.168.25.0	ether2
D	192.168.25.19...	192.168.25.0	wlan7
D	192.168.87.95...	192.168.87.0	ether1

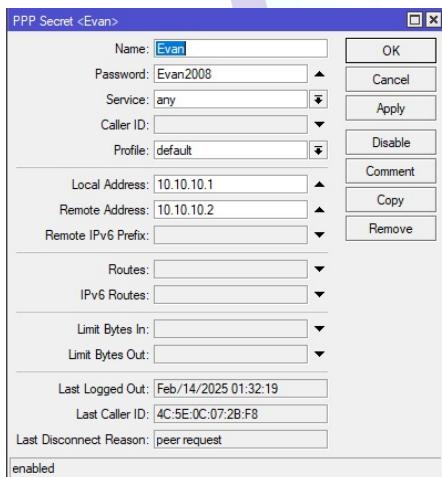
6 items

## II.Skenario 2

1. Langkah pertama kalian login dan remote serta konfigurasikan seperti biasa. Masuk ke dalam PPoE Servers lalu klik tombol +, untuk interfacenya kalian pilih ke router client disini saya menggunakan ether 3.



2. Masuk ke secret lalu klik tombol + untuk membuat baru, disini sebagai contoh saya membuat dengan nama evan dan paswordnya adalah Evan2008, dan service yang saya gunakan adalah any. Untuk local address dan remote address kalian isikan ip yang akan di berikan interface pptp pada Client, dan ingat bahwa ip harus 1 jaringan.



3. Kalian masuk ke Settings, lalu pilih network and internet.



**Network and Internet**

[View network status and tasks](#)

**Hardware and Sound**

4. Lalu pilih yang connect to the internet



- Set Up a Connection or Network

Choose a connection option

Connect to the Internet  
Set up a broadband or dial-up connection to the Internet.

Set up a new network  
Set up a new router or access point.

Connect to a workplace  
Set up a dial-up or VPN connection to your workplace.

5. Klik set up a new connection or network

Change your networking settings



[Set up a new connection or network](#)

Set up a broadband, dial-up or VPN connection,

6. Pilih Broadband (PPPoE)

Connect to the Internet

How do you want to connect?

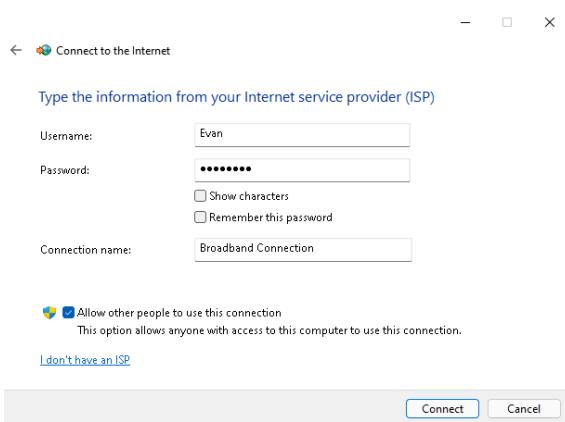
Broadband (PPPoE)

Connect using DSL or cable that requires a username and password.

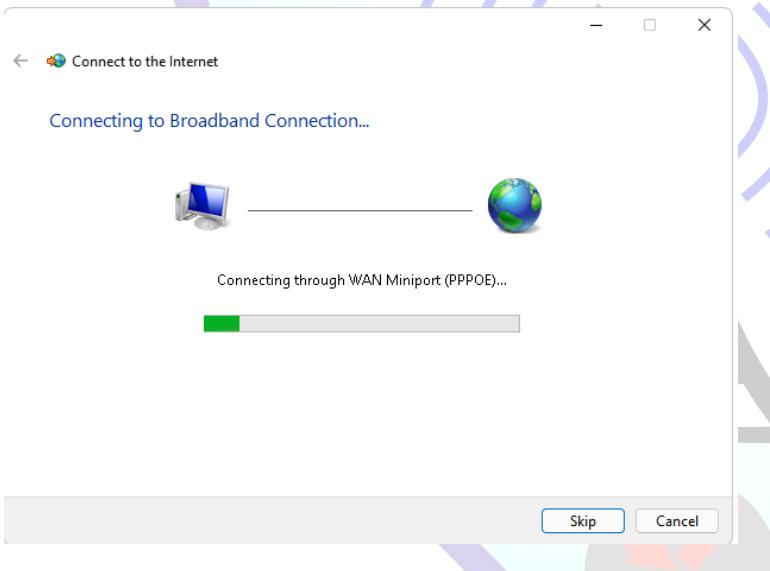
Show connection options that this computer is not set up to use

Cancel

7. Masukkan Username dan passwordnya



8. Maka akan seperti ini dan akan terkoneksi.



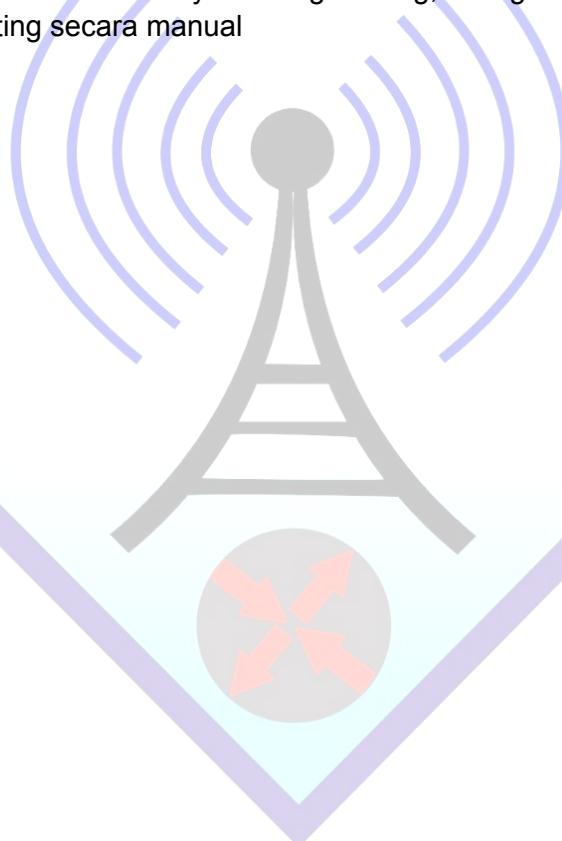


## LAB 21 Routing Concepts

Routing merupakan suatu protokol yang digunakan untuk mendapatkan rute dari satu jaringan ke jaringan yang lain. Device dari routing adalah Router (perangkat yang menjembatani dua network).

Tujuan utama dari routing protokol adalah untuk membangun dan memperbaiki table routing. Dimana tabel ini berisi jaringan-jaringan dan interface yang berhubungan dengan jaringan tersebut.

Router menggunakan protokol routing ini untuk mengatur informasi yang diterima dari router-router lain dan interfacenya masing-masing, sebagaimana yang terjadi di konfigurasi routing secara manual





## LAB 22 Route Flags

S: Static Route

D: Dynamic

A: Active

C: Connect

DAS: Dynamic Active Static, suatu routing bersifat static yang dibuat secara dynamic atau otomatis

DAC: Dynamic Active Connect, konfigurasi terhubung yang dibuat secara otomatis.

AS: Active Static, konfigurasi dari router yang bisa kita konfigurasikan sendiri

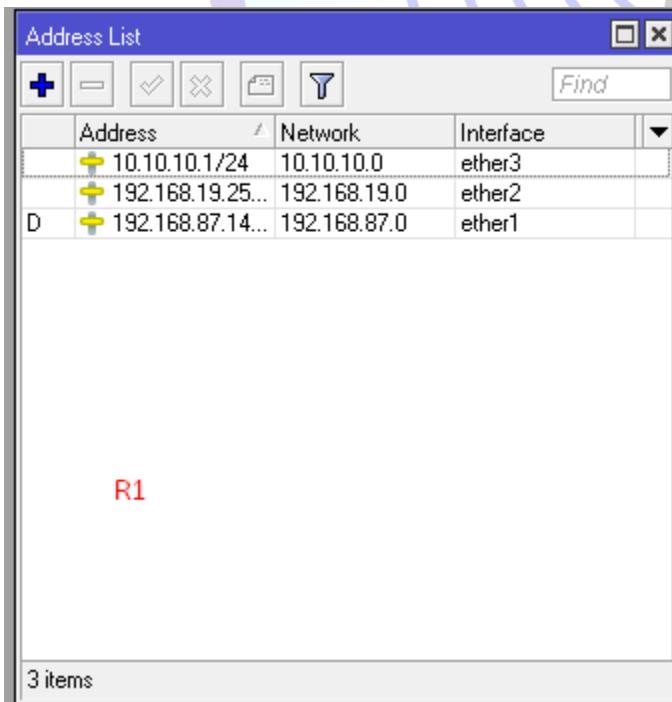


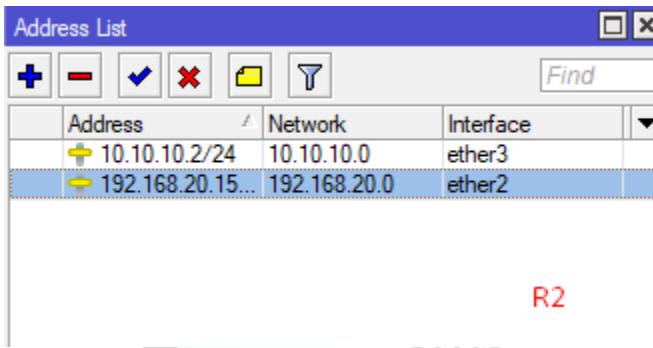


## LAB 23 Static Route 2 Router

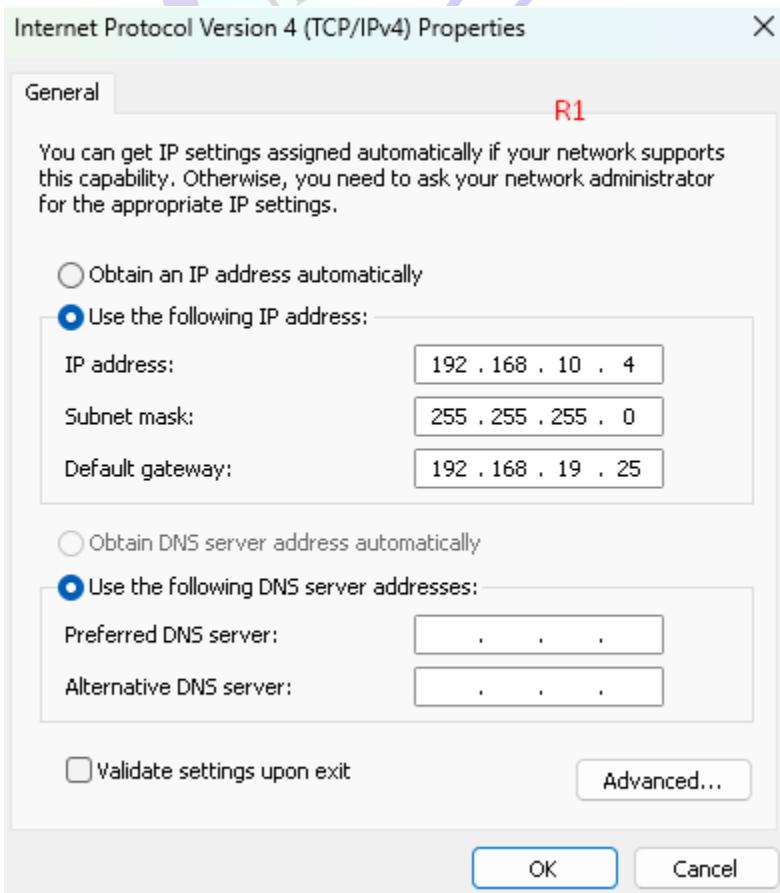
Pada lab kali ini, saya akan membahas tentang Routing pada Mikrotik. Routing adalah metode dalam jaringan untuk menghubungkan Router 1 ke jaringan lainnya, sehingga perangkat-perangkat dalam jaringan tersebut dapat saling berkomunikasi. Sebelum membahas lebih jauh tentang Routing Static, penting untuk memahami apa itu Routing Static. Routing Static adalah jenis routing pada Mikrotik yang memungkinkan konfigurasi informasi tentang tujuan jaringan dilakukan secara manual. Semua pengaturan rute dan konfigurasinya diatur oleh administrator jaringan, tanpa adanya pembaruan otomatis seperti pada routing dinamis.

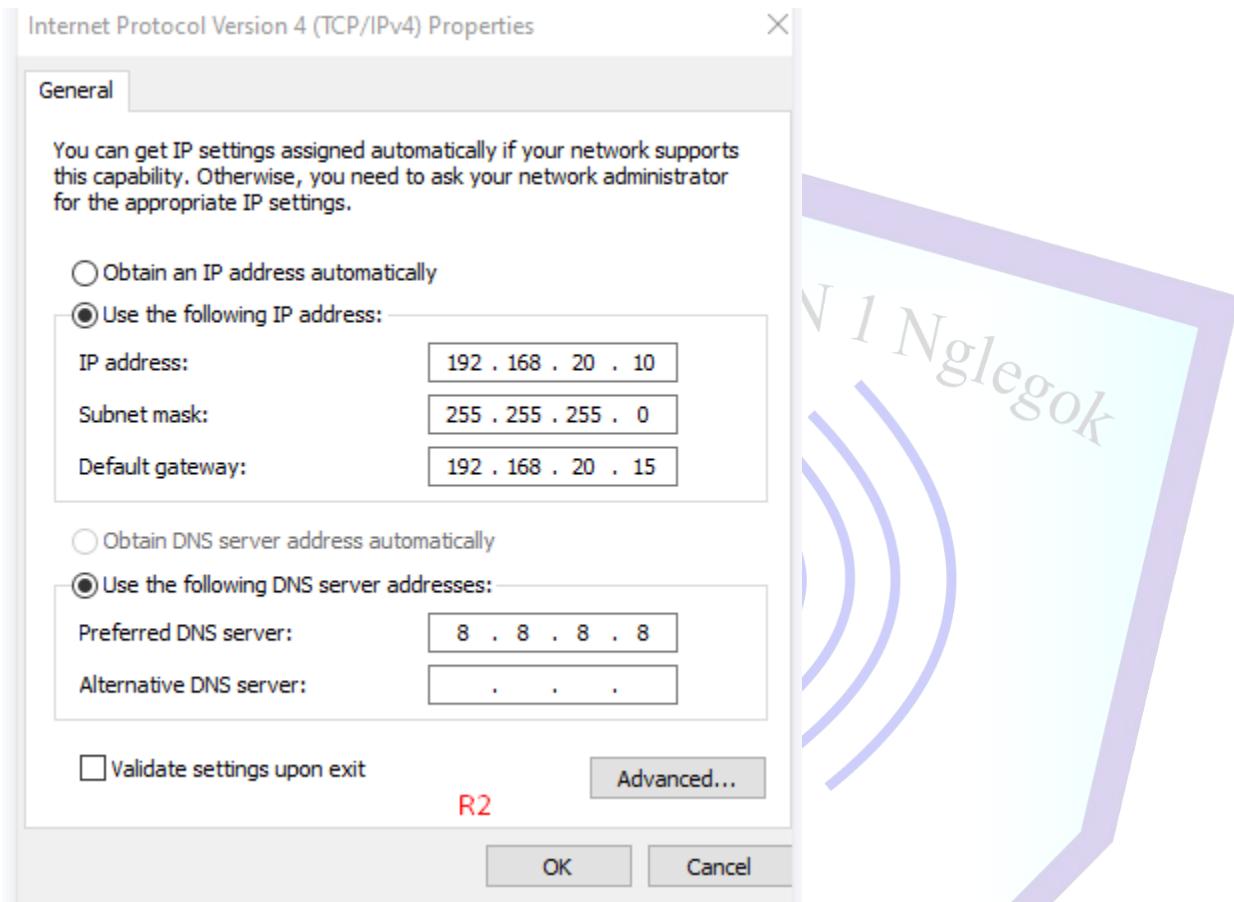
1. Langkah pertama yang kita lakukan untuk melakukan router static adalah setting ip pada ether 2 setiap router, dan untuk ip ether 1 kita akan gunakan sebagai router gatewaynya





2. Langkah berikutnya kita konfigurasikan ip static pada setiap pc, disini saya menggunakan 192.169.10.0/24 dan juga 192.168.20.0/24





3. Masuk ke ip route lalu konfigurasikan ip static pada setiap pc, untuk ketentuannya sebagai berikut. Untuk r1 dts addressnya kalian isikan ip ether 2 dari r2 dan untuk gatewaynya kalian isikan ip ether 1 dari router r2. Begitu juga untuk router 2



Route <192.168.20.0/24>

General	Attributes
Dst. Address: <input type="text" value="192.168.20.0/24"/>	R1
Gateway: <input type="text" value="10.10.10.2"/> <input type="button" value="reachable ether3"/>	
Check Gateway: <input type="text"/>	
Type: <input type="text" value="unicast"/>	
Distance: <input type="text" value="1"/>	
Scope: <input type="text" value="30"/>	
Target Scope: <input type="text" value="10"/>	
Routing Mark: <input type="text"/>	
Pref. Source: <input type="text"/>	
<input checked="" type="radio" value="enabled"/> enabled <input type="radio" value="active"/> active <input type="radio" value="static"/> static	

Route <192.168.19.0/24>

General	Attributes
Dst. Address: <input type="text" value="192.168.19.0/24"/>	R2
Gateway: <input type="text" value="10.10.10.1"/> <input type="button" value="reachable ether3"/>	
Check Gateway: <input type="text"/>	
Type: <input type="text" value="unicast"/>	
Distance: <input type="text" value="1"/>	
Scope: <input type="text" value="30"/>	
Target Scope: <input type="text" value="10"/>	
Routing Mark: <input type="text"/>	
Pref. Source: <input type="text"/>	
<input checked="" type="radio" value="enabled"/> enabled <input type="radio" value="active"/> active <input type="radio" value="static"/> static	

4. Dan langkah terakhir kita ping antar pc. Jika hasilnya ttl maka kita sudah berhasil melakukan routing static



```
C:\Users\pc-lab-3>ping 192.168.19.25          R1
Pinging 192.168.19.25 with 32 bytes of data:
Reply from 192.168.19.25: bytes=32 time=1ms TTL=63
Reply from 192.168.19.25: bytes=32 time<1ms TTL=63
Reply from 192.168.19.25: bytes=32 time<1ms TTL=63
Reply from 192.168.19.25: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.19.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\pc-lab-3>
```

```
C:\Users\pc-lab-3>ping 192.168.20.15          R2
Pinging 192.168.20.15 with 32 bytes of data:
Reply from 192.168.20.15: bytes=32 time<1ms TTL=64

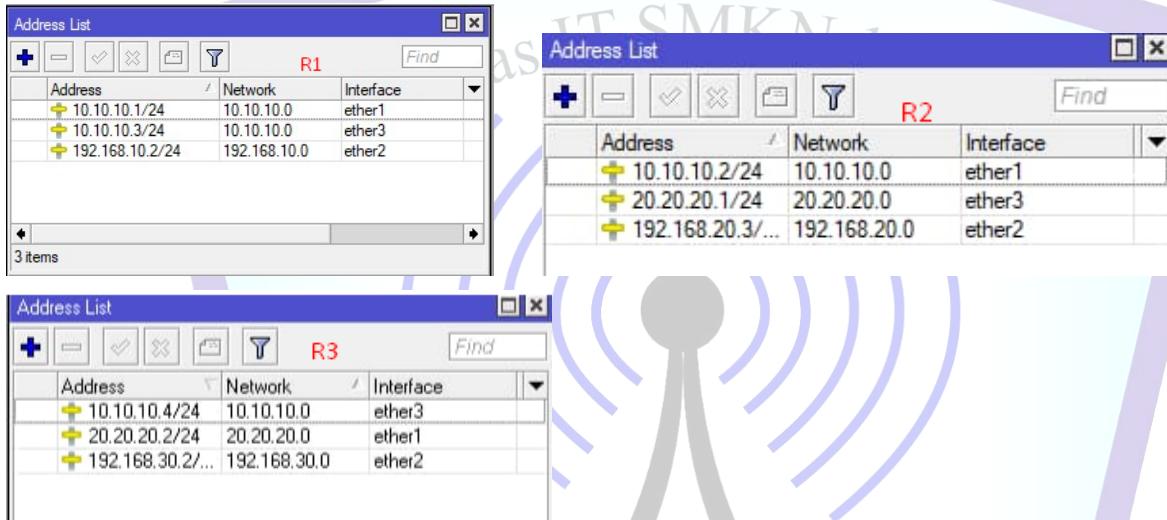
Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



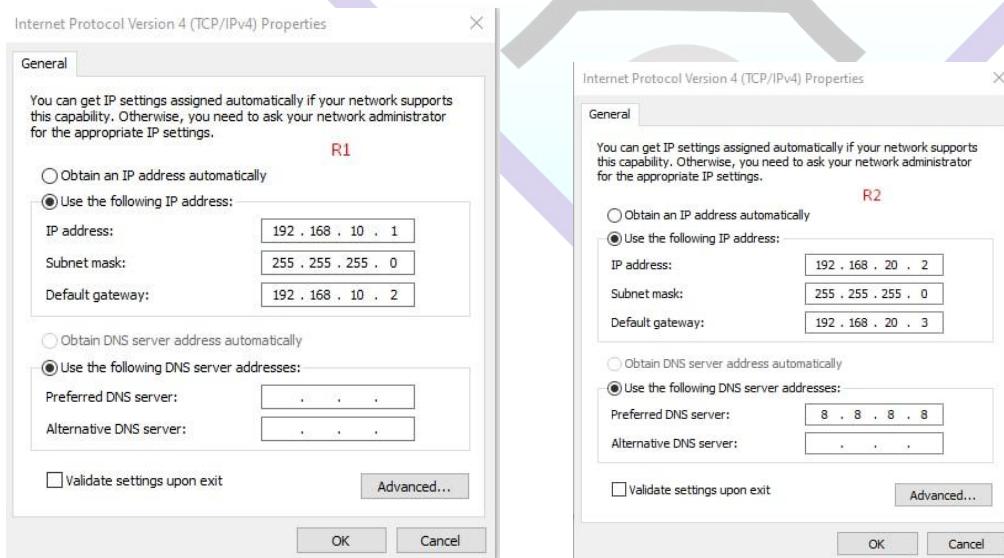
## LAB 24 Static Route 3 Router

Pada lab kali ini kita akan belajar mengenai router static lagi yaitu dengan menggunakan 3 pc,Mari kita belajar bersama sama

1. Pertama kita akan membuat konfigurasi IP terlebih dahulu sesuai dengan topologi yang telah kalian buat pada setiap router.



2. Selanjutnya akan setting IP static, dengan cara masuk ke control panel dan isikan ip. Pada pc 1 saya isikan 192.168.10.1 gatewaynya 192.168.10.2 . Untuk pc 2 saya isikan 192.168.20.2 gatewaynya 192.168.20.3





3. Kemudian masuk ke ip route dan klik tombol +, untuk dst addressnya kalian isikan ip tujuan kalian sedangkan untuk gateway isikan dengan ip terdekat.

The image shows three separate windows for configuring routes on routers R1, R2, and R3. Each window has tabs for 'General' and 'Attributes'. The 'General' tab is selected in all three windows. The 'Attributes' tab is visible at the bottom of each window. A vertical toolbar on the right side of each window contains buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. A large purple arrow points from the text '1 Nglegok' towards the windows.

**R1 Route <192.168.20.0/24>**

General	Attributes
Dst. Address: 192.168.20.0/24	reachable ether3
Gateway: 10.10.10.2	
Check Gateway:	
Type: unicast	
Distance: 1	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

**R2 Route <192.168.10.0/24>**

General	Attributes
Dst. Address: 192.168.10.0/24	reachable ether1
Gateway: 20.20.20.1	
Check Gateway:	
Type: unicast	
Distance: 1	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

**R3 Route <192.168.20.0/24>**

General	Attributes
Dst. Address: 192.168.20.0/24	reachable ether1
Gateway: 20.20.20.1	
Check Gateway:	
Type: unicast	
Distance: 1	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

4. Kita coba ping telerlebih dahulu di new terminal dan jika hasilnya ttl maka konfigurasi kalian sudah berhasil.



```
[admin@RouterOS] > ping 192.168.30.2
SEQ HOST R1 SIZE TTL TIME STATUS
0 192.168.30.2 56 64 0ms
1 192.168.30.2 56 64 0ms
2 192.168.30.2 56 64 0ms
3 192.168.30.2 56 64 0ms
4 192.168.30.2 56 64 0ms
5 192.168.30.2 56 64 0ms
6 192.168.30.2 56 64 0ms
7 192.168.30.2 56 64 0ms
sent=8 received=8 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

```
[admin@mikrotik] > ping 192.168.10.2
SEQ HOST R3 SIZE TTL TIME STATUS
0 192.168.10.2 56 64 0ms
1 192.168.10.2 56 64 0ms
2 192.168.10.2 56 64 0ms
sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

5. Langkah terakhir kita akan ping antar pc dan hasilnya sama yaitu TTL maka berhasil dalam melakukan konfigurasi pada lab ini.

```
C:\Users\pc-lab-3>ping 192.168.20.2 R1
Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\pc-lab-3>
```

```
C:\Users\pc-lab-3>ping 192.168.30.2 R2
Pinging 192.168.30.2 with 32 bytes of data:
Reply from 192.168.30.2: bytes=32 time<1ms TTL=64

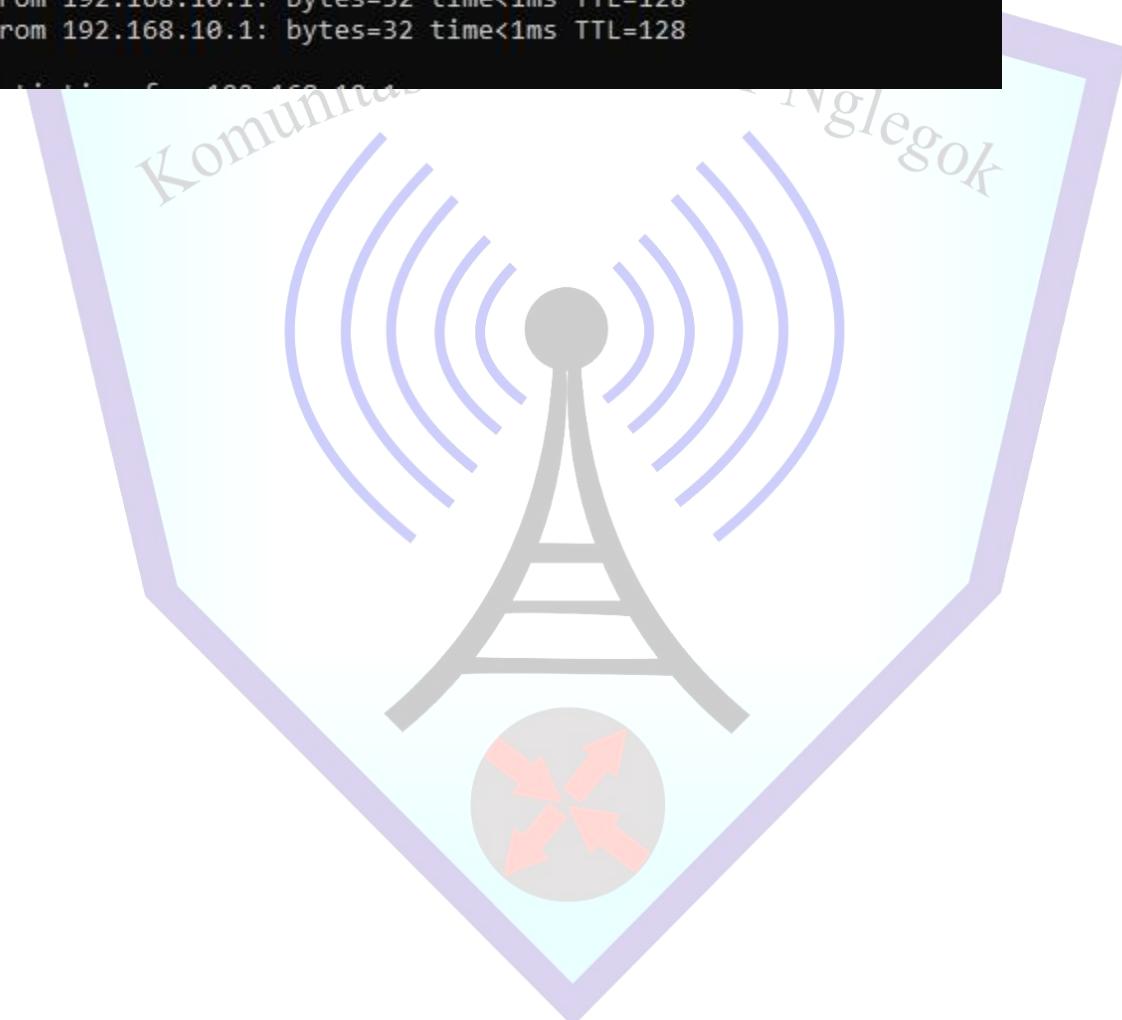
Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\pc-lab-3>
```



```
C:\Users\pc-la>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
```

R3

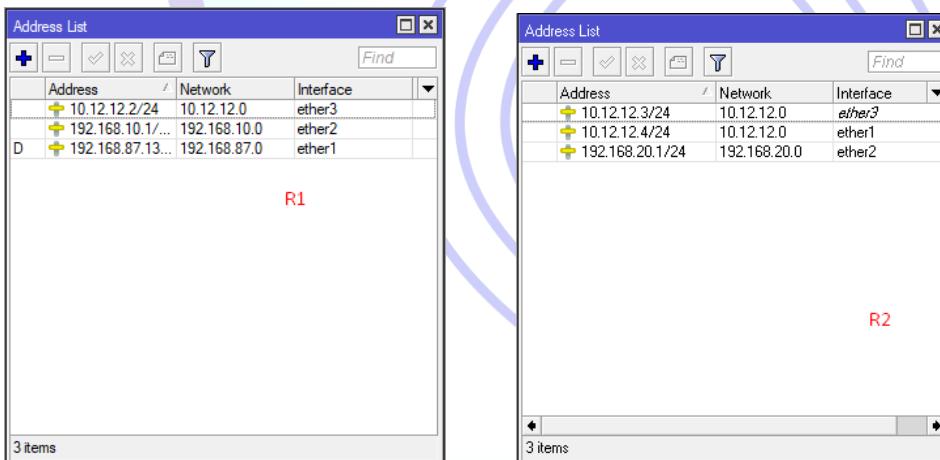




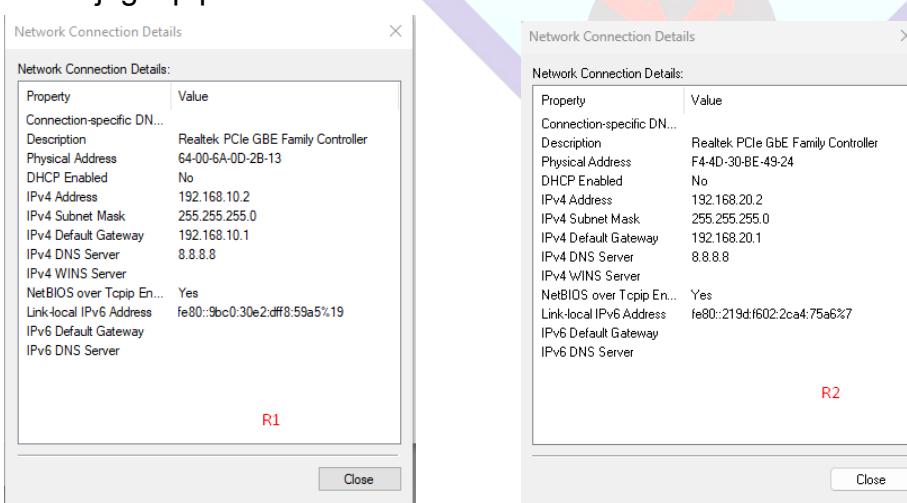
## LAB 25 Static Routing Default Route

Pada lab kali ini, saya akan membahas tentang Routing pada Mikrotik. Routing adalah metode dalam jaringan yang digunakan untuk menghubungkan Router 1 ke jaringan lainnya, sehingga perangkat-perangkat dalam jaringan tersebut dapat saling berkomunikasi. Sebelum membahas lebih jauh tentang Routing Static, penting untuk memahami apa itu Routing Static. Routing Static adalah jenis routing pada Mikrotik di mana konfigurasi rute menuju jaringan tujuan dilakukan secara manual oleh administrator. Semua pengaturan rute dan konfigurasinya diatur secara tetap, tanpa pembaruan otomatis seperti pada routing dinamis.

1. Disini kita akan melakukan default route yang konfigurasinya hampir sama dengan router static mari kita belajar.



2. Jika ip kalian sudah kalian konfigurasikan,maka selanjutnya kita konfigurasikan juga ip pc





3. Masuk ke ip route lalu klik +, Disini kita tidak akan menggunakan dst address/default route, untuk gatewaynya isikan ip Public dari router lawan.

The screenshot shows two separate windows for route configuration:

- R1 Configuration:** Dst. Address: 0.0.0.0, Gateway: 10.12.12.4 (reachable ether3), Type: unicast, Distance: 1, Scope: 30, Target Scope: 10, Routing Mark: (empty), Pref. Source: (empty).
- R2 Configuration:** Dst. Address: 0.0.0.0, Gateway: 10.12.12.2 (reachable ether1), Type: unicast, Distance: 1, Scope: 30, Target Scope: 10, Routing Mark: (empty), Pref. Source: (empty).

4. Jika sudah maka statusnya akan menjadi AS(Autonomous System)

Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
0.0.0.0/0	10.12.12.4 reachable ether3	1		
10.12.12.0/24	ether3 reachable	0	10.12.12.2	
192.168.10.0/24	ether2 reachable	0	192.168.10.1	
192.168.87.0/24	ether1 reachable	0	192.168.87.139	



5. Dan terakhir kalian coba pingkan antar pc jika hasilnya TTL maka kalian sudah berhasil melakukan default

```
C:\Users\pc-lab-3>ping 192.168.20.2          R1

Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\pc-lab-3>ping 192.168.10.2          R2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

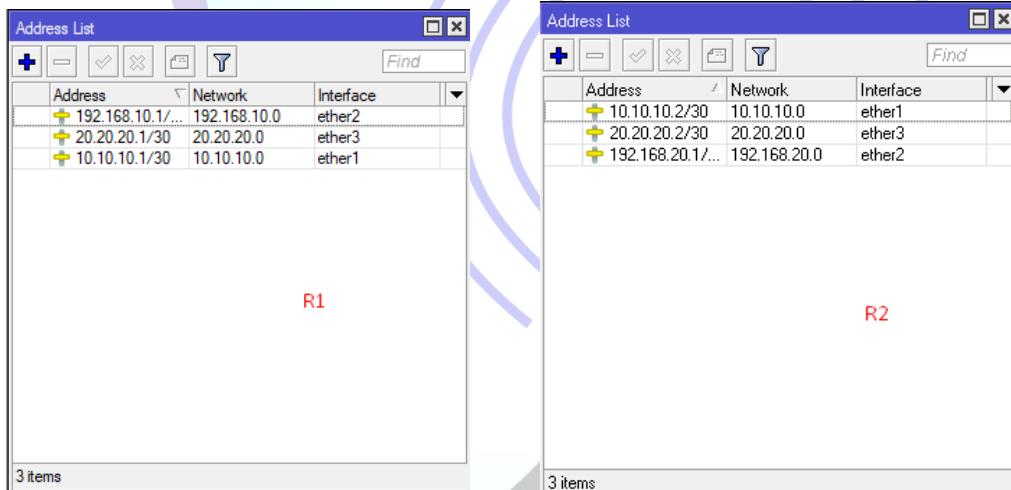
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```



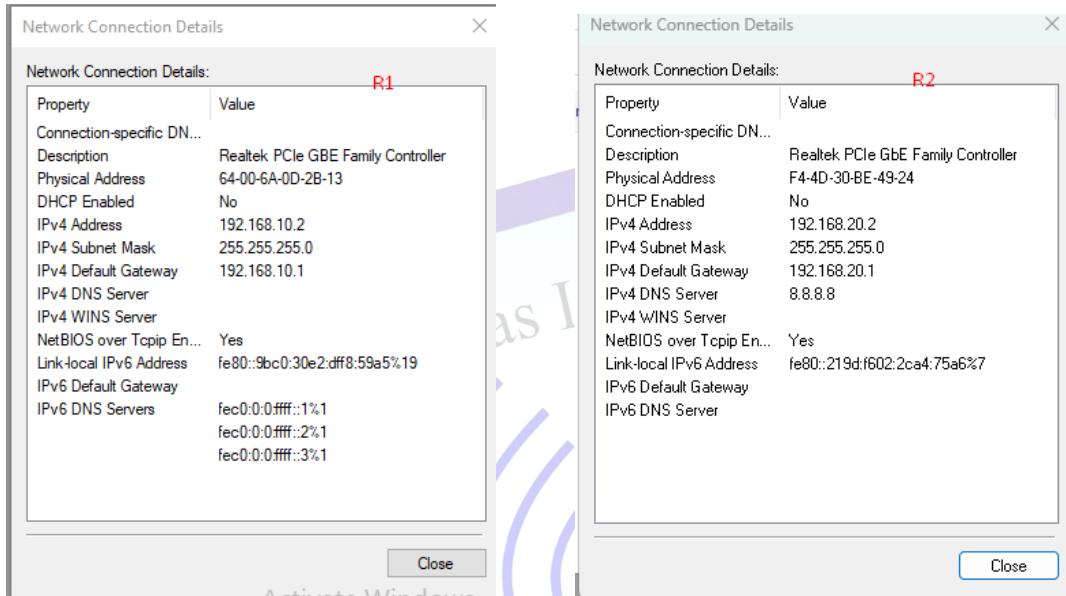
## LAB 26 Prioritas Routing

Pada lab kali ini, saya akan membahas tentang Routing pada Mikrotik. Routing adalah metode dalam jaringan yang digunakan untuk menghubungkan Router 1 ke jaringan lain, sehingga perangkat-perangkat dalam jaringan tersebut dapat saling berkomunikasi. Sebelum membahas lebih lanjut tentang Routing Static, penting untuk memahami apa itu Routing Static. Routing Static adalah jenis routing pada Mikrotik di mana pengaturan rute menuju jaringan tujuan dilakukan secara manual oleh administrator. Semua konfigurasi rute ditentukan secara tetap, tanpa adanya pembaruan otomatis seperti pada routing dinamis.

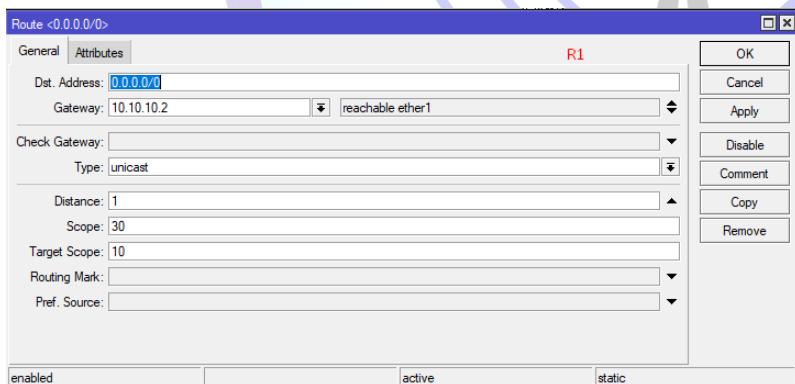
1. Pertama tama kita akan setting op di ether 2, ether 1 dan ether 3 yang akan kita gunakan untuk jembatan penghubung.



2. Kalian juga harus setting ip pada setiap pc sesuai dengan ip router kalian tadi



3. Masukk ke Ip route, lalu kita buat 2 konfigurasi. Dstnya kita isikan default dan untuk gateway r1 ip ether 1 dan r2 ip ether 3



4. Jika sudah maka tampilannya akan seperti ini. AS dan S terjadi karena router list yang dibaca adalah posisi atas dan yang dibawah hanya bertuliskan S



Route List				
Routes		Nexthops	Rules	VRF
R1				
AS	► 0.0.0.0/0	10.10.10.2 reachable ether1	Distance	1
	► 0.0.0.0/0	20.20.20.2 reachable ether3		1
DAC	► 10.10.10.0/30	ether1 reachable		0
DAC	► 20.20.20.0/30	ether3 reachable		0
DAC	► 192.168.10.0/...	ether2 reachable		0

5. Kemudian kita masuk ke new terminal ketikkan tool traceroute 192.168.20.2 dan akan melewati jalan gateway ether 1 dari lawan terlebih dahulu.

```
[admin@MikroTik] > tool traceroute 192.168.20.2
# ADDRESS          LOSS SENT LAST AVG BEST WORST
1 10.10.10.2          0%   8    0.4ms  0.4  0.3  0.6
2 192.168.20.2          0%   8    0.8ms  0.7  0.4  0.9
```

Route List						
Routes		Nexthops	Rules	VRF	Find	all
R2						
AS	► 0.0.0.0/0	10.10.10.1 reachable ether1	Distance	1		
S	► 0.0.0.0/0	20.20.20.1 reachable ether3		1		
DAC	► 10.10.10.0/30	ether1 reachable		0	10.10.10.2	
DAC	► 20.20.20.0/30	ether3 reachable		0	20.20.20.2	
DAC	► 192.168.20.0/...	ether2 reachable		0	192.168.20.1	

Route <0.0.0.0/0>

General	Attributes	
Dst. Address:	0.0.0.0/0	
Gateway:	10.10.10.1 reachable ether1	
Check Gateway:		
Type:	unicast	
Distance:	2	
Scope:	30	
Target Scope:	10	
Routing Mark:		
Pref. Source:		
enabled	active	static



## LAB 27 SIMPLE QUEUE

Simple Queue pada Mikrotik adalah fitur untuk mengatur dan membatasi bandwidth pada jaringan. Dengan Simple Queue, Anda dapat mengontrol aliran data antara perangkat atau antarnetwork, mengatur kecepatan upload dan download, serta menetapkan prioritas trafik tertentu. Fitur ini memungkinkan pengaturan pembatasan bandwidth secara sederhana dan efektif tanpa memerlukan konfigurasi yang kompleks.

1. Login winbox
2. Lalu masuk ke Queues



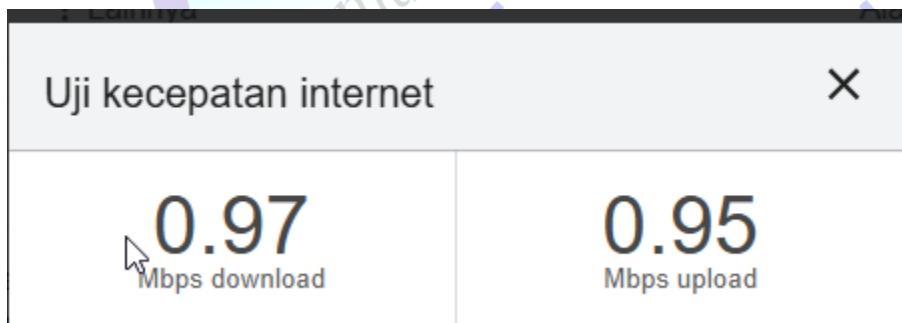
3. Kemudian kalian setting IP dari client yang ingin dibatasi kecepatannya

New Simple Queue

General	Advanced	Statistics	Traffic	Total	Total Statistics		
Name: <input type="text" value="queue1"/>							<input type="button" value="OK"/>
Target: <input type="text" value="192.168.21.23"/>							<input type="button" value="Cancel"/>
Dst: <input type="text"/>							<input type="button" value="Apply"/>
Target Upload		Target Download					
Max Limit: <input type="text" value="1M"/>	<input type="button" value="▼"/>	<input type="text" value="1M"/>	<input type="button" value="▼"/>	bits/s			
Burst							
Burst Limit: <input type="text" value="unlimited"/>	<input type="button" value="▼"/>	<input type="text" value="unlimited"/>	<input type="button" value="▼"/>	bits/s			
Burst Threshold: <input type="text" value="unlimited"/>	<input type="button" value="▼"/>	<input type="text" value="unlimited"/>	<input type="button" value="▼"/>	bits/s			
Burst Time: <input type="text" value="0"/>	<input type="button" value="▼"/>	<input type="text" value="0"/>	<input type="button" value="▼"/>	s			
Time							
enabled <input type="checkbox"/>							
<input type="button" value="Comment"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/> <input type="button" value="Reset Counters"/> <input type="button" value="Reset All Counters"/> <input type="button" value="Torch"/>							



4. Jika sudah kalian chek menggunakan speedtest di google





## Komunitas IT SMKN 1 Nglegok

### LAB 28 Simple Queue with PCQ

1. Login ke Winbox
2. Setelah itu kalian masuk ke Queues



3. Kalian settingkan IP client dan kalian masukkan max limit yang kalian ingin tentukan. Disini max limit saya membatasi limit upload dan limit Download 1 M



Simple Queue <Limitasi-PCQ>

General Advanced Statistics Traffic Total Total Statistics

Name: Limitasi-PCQ

Target: 192.168.20.0/24

Dst: [dropdown menu]

Target Upload Target Download

Max Limit: 1M bits/s

Burst

Burst Limit: unlimited bits/s

Burst Threshold: unlimited bits/s

Burst Time: 0 s

Time

enabled

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

4. Berikutnya kalian masuk ke Queue Types lalu klik tombol + dan kita akan membuat konfigurasi pcq dan namanya saya berikan Upload pcq dan Download pcq. Untuk Classifier Upload kalian centang yang src address sedangkan yang download kalian centang dst address



New Queue Type

Type Name:	Upload-PCQ	OK
Kind:	pcq	Cancel
Rate:	256k bits/s	Apply
Queue Size:	50 KiB	Copy
Total Queue Size:	2000 KiB	Remove
Burst Rate:		
Burst Threshold:		
Burst Time:	00:00:10	
Classifier:	<input checked="" type="checkbox"/> Src. Address <input type="checkbox"/> Dst. Address	
	<input type="checkbox"/> Src. Port <input type="checkbox"/> Dst. Port	
Src. Address Mask:	32	
Dst. Address Mask:	32	
Src. Address6 Mask:	128	
Dst. Address6 Mask:	128	

New Queue Type

Type Name:	Download-PCQ	OK
Kind:	pcq	Cancel
Rate:	256k bits/s	Apply
Queue Size:	50 KiB	Copy
Total Queue Size:	2000 KiB	Remove
Burst Rate:		
Burst Threshold:		
Burst Time:	00:00:10	
Classifier:	<input type="checkbox"/> Src. Address <input checked="" type="checkbox"/> Dst. Address	
	<input type="checkbox"/> Src. Port <input type="checkbox"/> Dst. Port	
Src. Address Mask:	32	
Dst. Address Mask:	32	
Src. Address6 Mask:	128	
Dst. Address6 Mask:	128	

Dan ini tampilan jika kita sudah menambahkan pcq download dan upload



Type Name	Kind
Download-PCQ	pcq
Upload-PCQ	pcq
* default	pfifo
* default-small	pfifo
* ethernet-default	pfifo
* hotspot-default	sfq
* multi-queue-ethernet-default	mq pfifo
* only-hardware-queue	none
* pcq-download-default	pcq
* pcq-upload-default	pcq
* synchronous-default	red
* wireless-default	sfq

5. Setelah itu kita kembali ke konfigurasi simple Queue lalu masuk ke tab advanced, disini kita hanya mengubah Queue Type kalian gantikan sesuai dengan contoh

Simple Queue <Limitasi-PCQ>

General		Advanced		Statistics		Traffic		Total		Total Statistics	
Packet Marks:											
Target Upload		Target Download									
Limit At: unlimited		unlimited									
Priority: 8		8									
Bucket Size: 0.100		0.100		ratio							
Queue Type: Upload-PCQ		Download-PCQ									
Parent: none											
enabled											

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

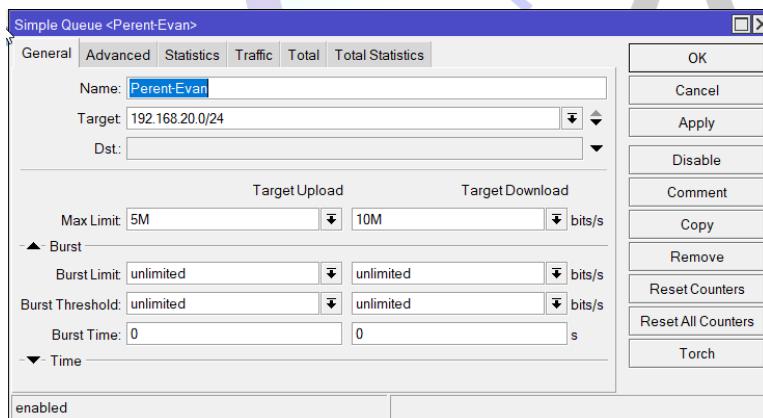
Untuk mengetesnya kita bisa masuk ke tool torch



# Komunitas IT SMKN 1 Nglelok

## LAB 29 Simple Queue with Parent and Child

1. Login ke winbox
2. Lalu kita buat parent dahulu, berikutnya kita Masukkan ip network dari client dan kita isi max limit upload dan download disini saya masukkan maxlimit dengan 5M



3. Setelah itu kita buat Childnya disini saya namakan PC 1 dan pada target kita isikan ip spesifik dari client, dan untuk maxnya saya masukkan 10M



Simple Queue <PC 1>

General	Advanced	Statistics	Traffic	Total	Total Statistics
Name: PC 1					
Target: 192.168.20.254					
Dst:					
Target Upload		Target Download			
Max Limit:	10M	▼	5M	▼	bits/s
▲ Burst					
Burst Limit:	unlimited	▼	unlimited	▼	bits/s
Burst Threshold:	unlimited	▼	unlimited	▼	bits/s
Burst Time:	0	▼	0	▼	s
▼ Time					
enabled					

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

4. Berikutnya masuk ke dalam advance dan parent kalian masukkan yang telah kalian buat tadi dan tambahkan limitnya

Simple Queue <PC 1>

General	Advanced	Statistics	Traffic	Total	Total Statistics
Packet Marks:					
Target Upload		Target Download			
Limit At:	128k	▼	128k	▼	bits/s
Priority:	8	▼	8	▼	
Bucket Size:	0.100	▼	0.100	▼	ratio
Queue Type:	default-small	▼	default-small	▼	
Parent:	Parent-Evan				
enabled					

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

5. Begitu juga untuk PC 2



Simple Queue <PC 2>

General Advanced Statistics Traffic Total Total Statistics

Name: PC2  
Target: 192.168.20.255  
Dst:

Target Upload Target Download

Max Limit: 5M bits/s  
Burst Limit: unlimited bits/s  
Burst Threshold: unlimited bits/s  
Burst Time: 0 s

Time

enabled

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

Simple Queue <PC 2>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Target Upload Target Download

Limit At: 128k bits/s  
Priority: 8  
Bucket Size: 0.100 ratio  
Queue Type: default-small

Parent: Parent-Evan

enabled

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

6. Dan berikut adalah Queue listnya

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✎ Filter Reset Counters Reset All Counters Find

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
0	Parent-Evan	192.168.20.0/24	5M	10M	
1	PC 1	192.168.20.254	10M	5M	
2	PC 2	192.168.20.255	5M	5M	



## LAB 30 Firewall principles

Pada kesempatan ini, saya akan menjelaskan mengenai Prinsip Firewall. Firewall adalah teknologi penting dalam Keamanan Sistem Informasi (IS Security) yang digunakan untuk melindungi jaringan dan sistem organisasi dari ancaman yang datang dari luar. Cara kerja firewall melibatkan pengaturan aturan dan kebijakan yang mengontrol akses ke jaringan serta membatasi jenis data yang diperbolehkan masuk dan keluar dari jaringan. Selain itu, firewall juga dapat memantau lalu lintas jaringan dan memberikan peringatan jika terdeteksi adanya aktivitas yang mencurigakan.

Berikut adalah beberapa prinsip yang perlu diterapkan saat membangun firewall dan menetapkan kebijakan keamanan:

### 1. Segregasi Jaringan (Network Segmentation)

Prinsip pertama adalah membagi jaringan Anda menjadi zona-zona yang berbeda untuk meningkatkan keamanan. Zona-zona ini bisa mencakup:

- Jaringan Internal: Jaringan yang digunakan untuk mengelola data dan sistem penting organisasi.
- DMZ (Demilitarized Zone): Zona antara jaringan internal dan publik, tempat server yang dapat diakses oleh pengguna luar seperti web server dan email server.
- Jaringan Publik: Bagian jaringan yang dapat diakses oleh pihak luar, seperti internet.

Segregasi jaringan ini membantu membatasi potensi serangan dan mencegahnya untuk menyebar ke seluruh jaringan organisasi, sekaligus melindungi aset yang lebih penting.

### 2. Pemeriksaan Lalu Lintas Jaringan (Traffic Inspection)

Firewall berfungsi untuk memeriksa dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan Anda. Proses ini meliputi:

- Penyaringan Berdasarkan Alamat IP: Memastikan hanya perangkat dengan alamat IP yang sah yang diizinkan untuk mengakses jaringan.
- Penyaringan Berdasarkan Port: Mengontrol komunikasi melalui port tertentu, hanya mengizinkan port yang dibutuhkan dan menutup port lainnya untuk mencegah potensi ancaman.



- Penyaringan Berdasarkan Protokol: Memeriksa jenis protokol yang digunakan (misalnya TCP, UDP, HTTP) untuk memastikan hanya protokol yang sah yang diperbolehkan.
- Stateful Inspection: Firewall memeriksa status koneksi dan hanya mengizinkan paket yang sah yang sesuai dengan status koneksi tersebut.

Dengan pemeriksaan ini, firewall dapat mencegah serangan yang dilakukan melalui berbagai cara, seperti spoofing, port scanning, atau Denial-of-Service (DoS).

### 3. Pemantauan dan Pelaporan (Monitoring and Logging)

Untuk menjaga keamanan jaringan secara berkelanjutan, firewall harus dilengkapi dengan kemampuan pemantauan dan pelaporan yang baik. Aspek penting yang harus diperhatikan adalah:

- Pemantauan Aktivitas Jaringan: Mengawasi lalu lintas data secara real-time untuk mendeteksi adanya aktivitas yang mencurigakan atau anomali.
- Pencatatan Log: Menyimpan log untuk setiap peristiwa yang terjadi dalam jaringan, yang dapat digunakan untuk analisis lebih lanjut dan forensik keamanan.
- Peringatan dan Tanggap Cepat: Memberikan notifikasi saat terdeteksi potensi serangan, memungkinkan tim keamanan untuk segera merespons dan mengurangi dampak dari insiden yang terjadi.



## LAB 31 Structure , chains and actions

### Struktur Firewall: Chains dan Actions

Dalam konfigurasi firewall, terdapat dua komponen utama yang menentukan bagaimana lalu lintas data diproses, yaitu Chains dan Actions.

#### 1. Chains

Chains adalah urutan atau rangkaian aturan filter yang diterapkan pada lalu lintas data.

Terdapat tiga jenis Chains utama yang digunakan dalam pengelolaan trafik:

- Input Chain: Chain ini digunakan untuk memproses paket data yang masuk ke dalam router melalui salah satu interface yang ada di router dan memiliki tujuan IP Address yang sesuai dengan IP router itu sendiri. Jenis trafik yang diproses di sini bisa berasal dari jaringan publik maupun jaringan lokal, dengan tujuan akhir router itu sendiri.
- Forward Chain: Chain ini digunakan untuk memproses paket data yang melewati router tanpa diarahkan langsung ke router itu sendiri. Artinya, trafik ini tidak dimaksudkan untuk mencapai router, tetapi hanya melalui router untuk diteruskan ke tujuan lainnya. Trafik ini berasal dari jaringan lain yang melewati router tersebut.
- Output Chain: Chain ini digunakan untuk memproses paket data yang keluar dari router. Ini berlaku untuk trafik yang dikirim oleh router itu sendiri ke jaringan lain atau luar.

#### 2. Actions

Actions atau tindakan adalah keputusan yang diambil untuk menentukan apa yang harus dilakukan dengan paket data yang sesuai dengan kriteria di dalam Chain. Terdapat beberapa jenis aksi yang bisa diterapkan pada paket data:

- Accept: Paket data diterima dan diproses lebih lanjut. Setelah paket diterima, tidak ada aturan lainnya yang perlu diperiksa lagi pada chain berikutnya, karena paket tersebut dianggap sah.
- Drop: Paket data ditolak tanpa memberikan tanggapan apapun. Paket yang dijatuhkan tidak diberi informasi lebih lanjut, dan tidak ada indikasi bahwa paket tersebut ditolak.
- Reject: Paket data ditolak dan firewall mengirimkan pesan penolakan kepada pengirim paket, memberi tahu bahwa paket tersebut tidak diterima.



## LAB 32 Firewall Filter Input , Output dan Forward

### A. Firewall Filter Input

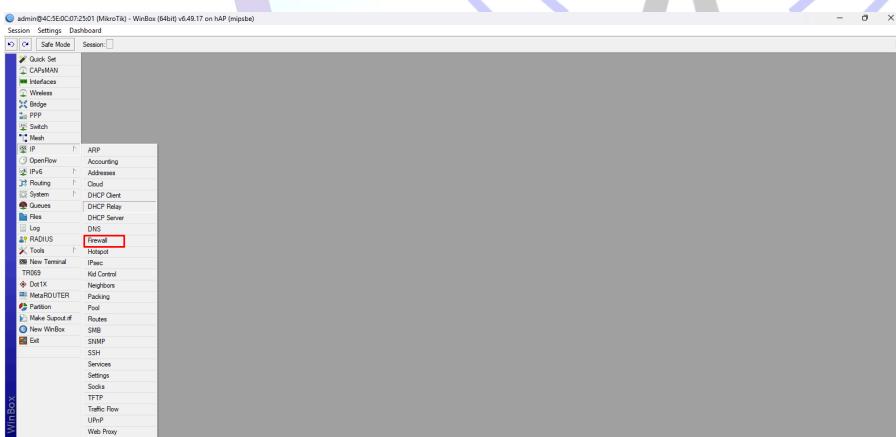
Pada lab kali ini, saya akan membahas tentang Firewall Filter Input. Fungsi dari Firewall Filter Input adalah untuk memfilter atau mengatur paket yang masuk ke router. Contoh paket yang masuk adalah permintaan ping dari client ke router. Dalam lab ini, kita akan mencoba untuk memblokir paket ping yang berasal dari client menuju router. Berikut adalah topologi yang saya gunakan.

1. Langkah pertama kalian harus memastikan Client dengan router bisa saling ping

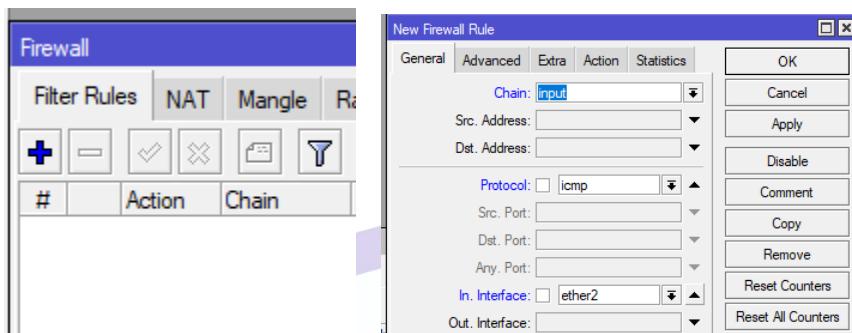
```
C:\Users\pc-lab-1>ping 192.168.19.25

Pinging 192.168.19.25 with 32 bytes of data:
Reply from 192.168.19.25: bytes=32 time<1ms TTL=64
Reply from 192.168.19.25: bytes=32 time=10ms TTL=64
Reply from 192.168.19.25: bytes=32 time<1ms TTL=64
Reply from 192.168.19.25: bytes=32 time=1ms TTL=64
```

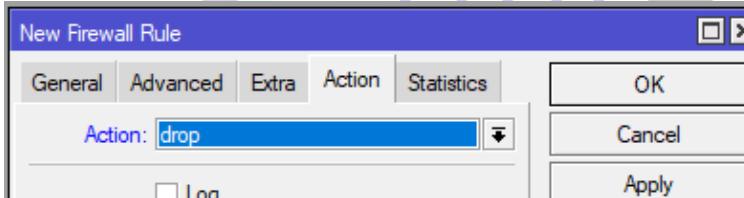
2. Masuk ke Winbox
3. Lalu IP> Firewall



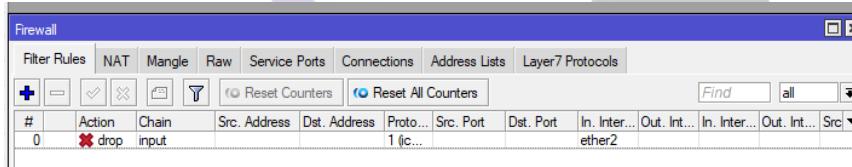
4. Kalian tambahkan filter Rules dengan ketentuan Chain input, Protocol icmp dan in interface Ether 1



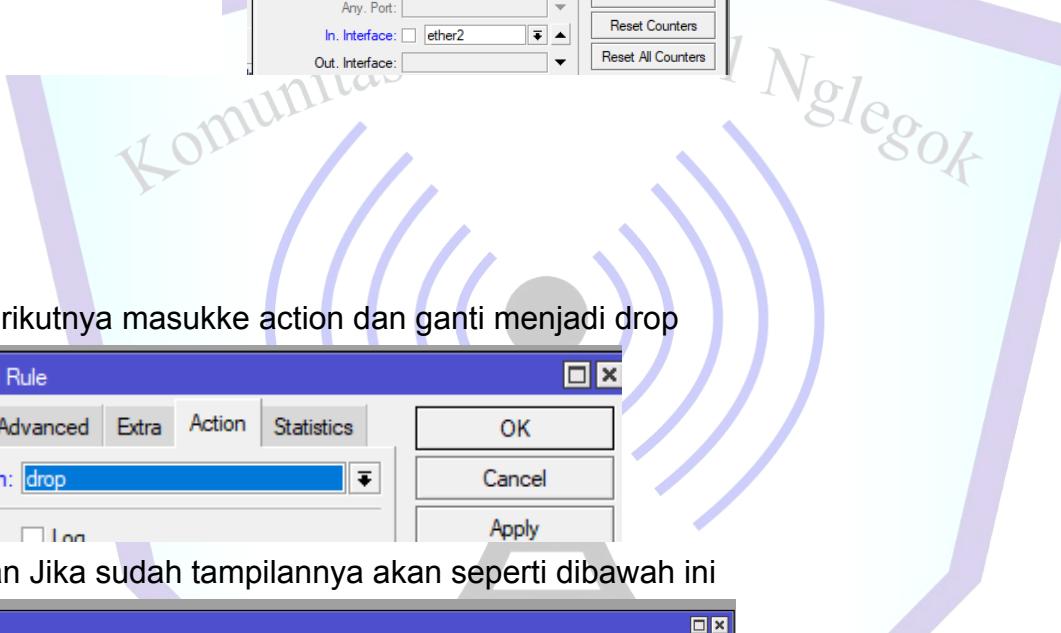
5. Berikutnya masukke action dan ganti menjadi drop



6. Dan Jika sudah tampilannya akan seperti dibawah ini



7. Untuk mengetesnya kalian ping kembali client dengan router dan hasilnya akan rto



```
Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(C) Microsoft Corporation. All rights reserved.

C:\Users\pc-lab-1>ping 192.168.19.25

Pinging 192.168.19.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```



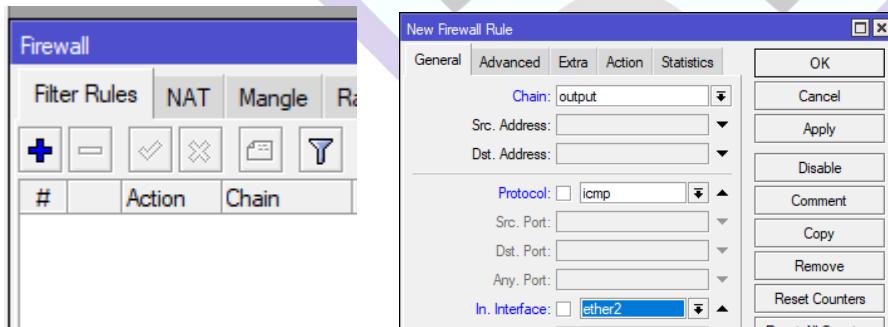
## B. Firewall Filter Output

Pada lab sebelumnya, saya membahas tentang Firewall Filter Input, dan sekarang saya akan membahas tentang Firewall Filter Output. Firewall Filter Output berfungsi kebalikan dari Firewall Filter Input; jika Firewall Filter Input mengatur paket yang masuk ke router, maka Firewall Filter Output mengatur paket yang keluar dari router. Dalam lab kali ini, kita akan mencoba untuk memblokir paket ping yang keluar dari router. Berikut adalah topologi yang saya gunakan.

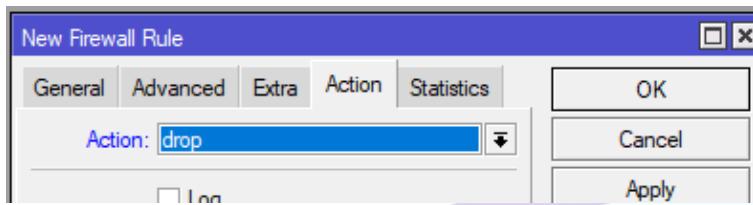
1. Login ke winbox
2. Lalu Maasuk ke IP firewall



3. Klik tombol +, lalu kalian buat dengan Chain output protocol icmp dan in interface ether 2



4. Lalu ganti action menjadi drop



## 5. Untuk mengetesnya kalian masuk ke new terminal lalu ping route ke client

```
Terminal <1>
[admin@MikroTik] > ping 192.168.19.25
SEQ HOST          SIZE TTL TIME STATUS
 0 192.168.19.25      56 64 0ms
 1 192.168.19.25      56 64 0ms
 2 192.168.19.25      56 64 0ms
 3 192.168.19.25      56 64 0ms
sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik] > ping 192.168.19.24
SEQ HOST          SIZE TTL TIME STATUS
 0              packet rejected
 1              packet rejected
 2              packet rejected
 3              packet rejected
 4              packet rejected
 5              packet rejected
sent=6 received=0 packet-loss=100%
```

[admin@MikroTik] > |



## C. Firewall Filter Forward

1. Langkah pertama kalian harus memastikan client bisa mengakses

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

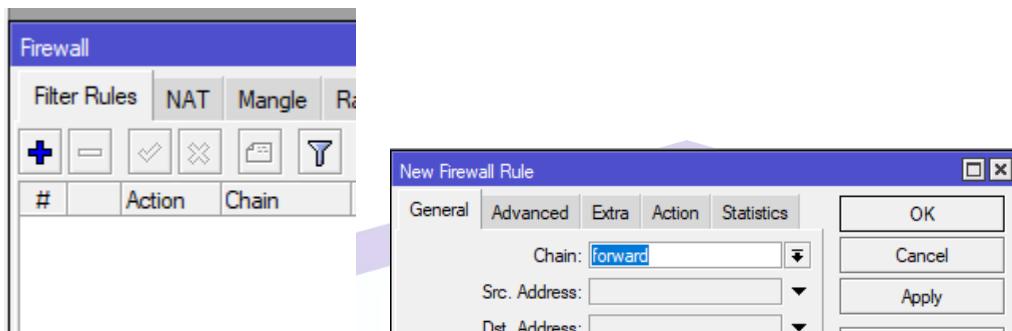
C:\Users\pc-lab-1>ping google.com

Pinging google.com [142.251.12.104] with 32 bytes of data:
Reply from 142.251.12.104: bytes=32 time=27ms TTL=102
Reply from 142.251.12.104: bytes=32 time=27ms TTL=102
Reply from 142.251.12.104: bytes=32 time=29ms TTL=102
Reply from 142.251.12.104: bytes=32 time=34ms TTL=102
```

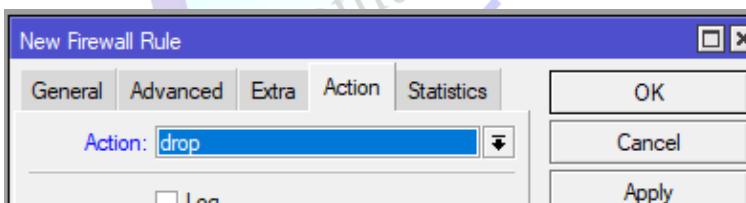
2. Masuk ke IP firewall



3. Lalu kalian buat filter rules baru dan ganti chain menjadi forward



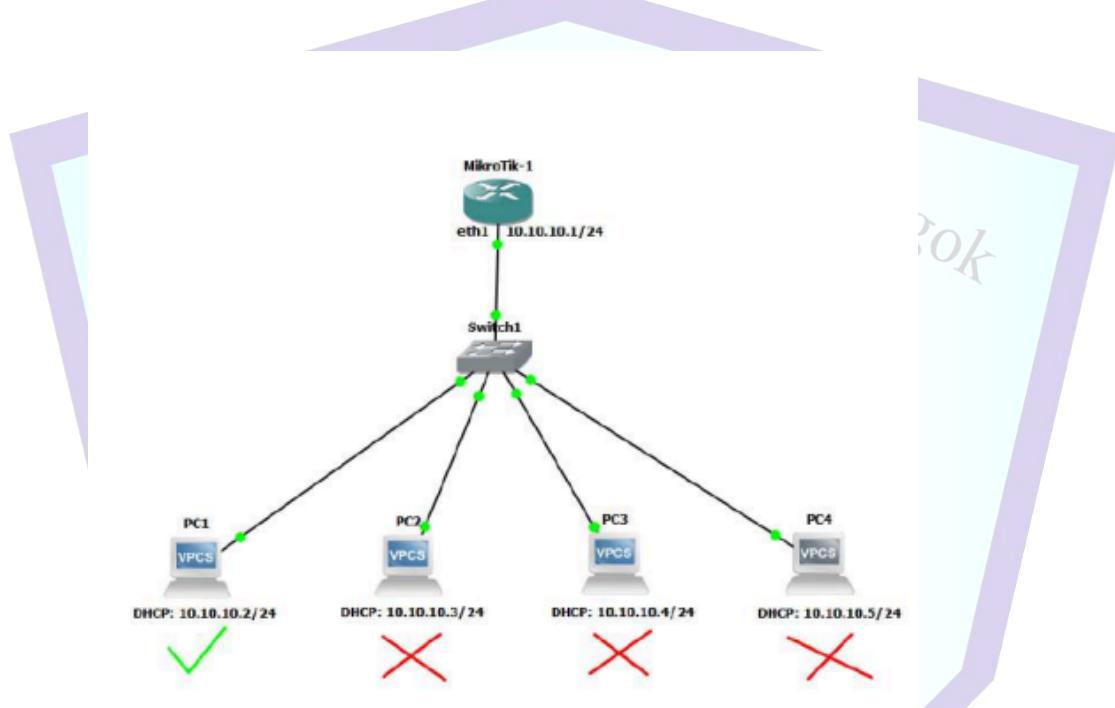
4. Dan kita ubah Actionnya menjadi drop



5. Untuk pengujinya kalian ping 8.8.8.8 pada client dan hasilnya akan berubah menjadi rto

## LAB 33 Firewall Strategy 1 & 2

### A.Firewall Strategy 1 (Drop All Accept Any)



Pada topologi ini, terdapat 4 client, dan kita akan melakukan konfigurasi untuk memblokir 3 client serta mengizinkan hanya 1 client agar dapat mengakses jaringan. Implementasi ini akan dilakukan menggunakan RouterOS di GNS3.

1. Langkah pertama adalah kalian buat topologi sama seperti diatas yaitu di GNS3
2. Kemudian kita akan menambahkan IP pada interface yang menuju ke client, bisa juga menggunakan DHCP Server

```
[admin@mikroTik] > [admin@mikroTik] > ip address add address=10.10.10.1/24 interface=ether1
```

```
[admin@mikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  10.10.10.1/24    10.10.10.0      ether1
```



3. Setelah itu kalian buat 2 rule firewall seperti contoh dibawah ini

Rule 1 : chain=input, src-address=10.10.10.2 (IP yang di Accept) , action=Accept. Rule 2 : chain=input, action=drop

4. Untuk rule yang pertama kita gunakan untuk mengujikan koneksi dengan client yang mempunyai ip 10.10.10.2, dan sedangkan untuk rule kedua kita gunakan untuk memblokir client yang lain. Untuk perintah yang akan gunakan sebagai berikut.

```
[admin@mikrotik] > ip firewall filter add chain=input src-address=10.10.10.2 action=accept
[admin@mikrotik] > ip firewall filter add chain=input action=drop
[admin@mikrotik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0  chain=input action=accept src-address=10.10.10.2
  1  chain=input action=drop
```

5. Jika sudah kita akan melakukan pengujian dengan cara kita akan ping. Untuk yang pertama hasilnya akan TTL

```
PC1> ip 10.10.10.2/24
Checking for duplicate address...
PC1 : 10.10.10.2 255.255.255.0

PC1> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=64 time=11.231 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=64 time=1.682 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=64 time=1.566 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=64 time=6.278 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=64 time=15.644 ms
```

6. Sedangkan ping pada client yang telah kita blokir tadi maka hasilnya akan berubah menjadi RTO (Request Time Out)

```
PC2> ping 10.10.10.1
10.10.10.1 icmp_seq=1 timeout
10.10.10.1 icmp_seq=2 timeout
10.10.10.1 icmp_seq=3 timeout
10.10.10.1 icmp_seq=4 timeout
10.10.10.1 icmp_seq=5 timeout
```



```
PC3> ip 10.10.10.4/24
Checking for duplicate address...
PC1 : 10.10.10.4 255.255.255.0

PC3> ping 10.10.10.1
10.10.10.1 icmp_seq=1 timeout
10.10.10.1 icmp_seq=2 timeout
10.10.10.1 icmp_seq=3 timeout
10.10.10.1 icmp_seq=4 timeout
10.10.10.1 icmp_seq=5 timeout
```

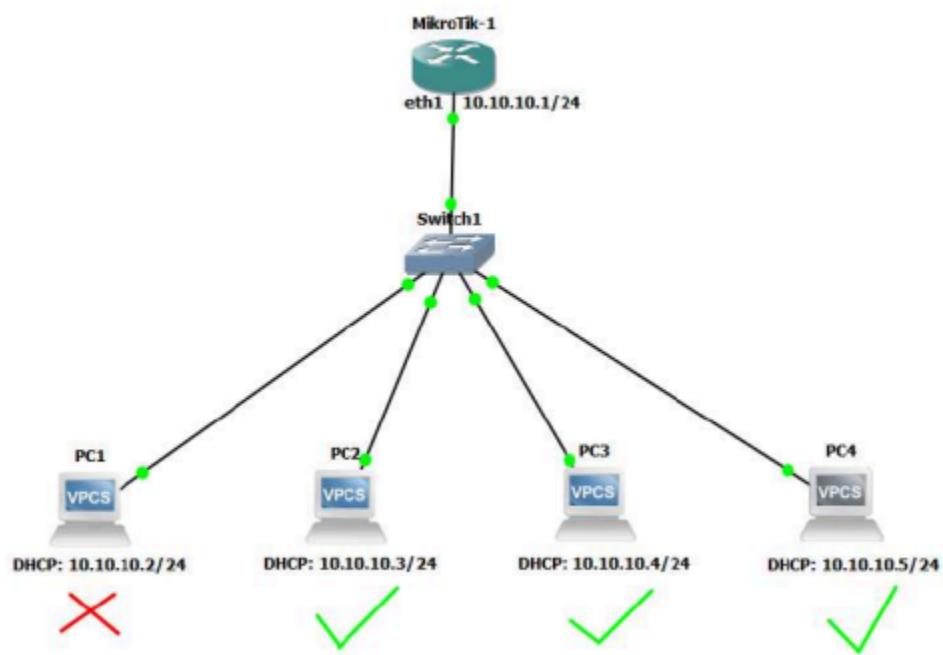
```
PC4> ip 10.10.10.5/24
Checking for duplicate address...
PC1 : 10.10.10.5 255.255.255.0

PC4> ping 10.10.10.1
10.10.10.1 icmp_seq=1 timeout
10.10.10.1 icmp_seq=2 timeout
10.10.10.1 icmp_seq=3 timeout
10.10.10.1 icmp_seq=4 timeout
10.10.10.1 icmp_seq=5 timeout
```

komunitas IT SMKN 1 Nglegok



## B. Firewall Strategy 2 (Drop Any Accept All)





Pada topologi ini, terdapat 4 client, di mana 1 client akan diblokir, sementara 3 client lainnya diizinkan untuk berkomunikasi dengan router. Konfigurasi ini tetap menggunakan dua aturan utama, yaitu Rule Accept dan Rule Drop, tetapi dengan perbedaan dalam penempatan aksi (action).

Aturan pertama digunakan untuk mengizinkan akses bagi 3 client, memastikan mereka dapat berkomunikasi dengan router tanpa kendala. Sementara itu, aturan kedua diterapkan untuk memblokir 1 client tertentu, sehingga perangkat tersebut tidak dapat mengakses router.

1. Pertama tama kalian buat sesuai dengan topologi diatas di GNS3
2. Lalu kalian tambahkan IP pad interface yang mengarah ke client, bisa juga jika kalian menggunakan DHCP Client. Comandnya seperti pada gambar dibawah

```
[admin@MikroTik] > ip address add address=10.10.10.1/24 interface=ether1
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK          INTERFACE
0   10.10.10.1/24    10.10.10.0    ether1
```

3. Setelah itu kalian setting ip yang mengarah ke client
4. Kemudian kita akan membuat 2 Rule baru lagi yaitu

Rule 1 : chain=input, src-address=10.10.10.2 (IP yang di Accept) , action= Drop.Rule 2 : chain=input, action=Accept

5. Untuk rule yang pertama kita akan menggunakan untuk memblokir komunikasi client yang menggunakan IP 10.10.10.2, dan untuk rule yang kedua kita akan mengizinkan Client lain. Perintahnya seperti dibawah ini

```
[admin@MikroTik] > ip firewall filter add chain=input src-address=10.10.10.2 action=drop
[admin@MikroTik] > ip firewall print
bad command name print (line 1 column 13)
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0   chain=input action=drop src-address=10.10.10.2
```



6. Jika kita sudah melakukan konfigurasi maka kita akan mencobanya dengan ping.  
Pada sisi client yang kita blokir tadi maka hasilnya akan rto

```
PC1> ip 10.10.10.2/24
Checking for duplicate address...
PC1 : 10.10.10.2 255.255.255.0

PC1> ping 10.10.10.1
10.10.10.1 icmp_seq=1 timeout
10.10.10.1 icmp_seq=2 timeout
10.10.10.1 icmp_seq=3 timeout
10.10.10.1 icmp_seq=4 timeout
10.10.10.1 icmp_seq=5 timeout
```

7. Dan untuk Client yang lain hasilnya akan menjadi TTL karena bisa berkomunikasi

```
PC2> ip 10.10.10.3/24
Checking for duplicate address...
PC1 : 10.10.10.3 255.255.255.0

PC2> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=64 time=6.535 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=64 time=4.260 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=64 time=3.759 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=64 time=3.166 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=64 time=1.165 ms
```

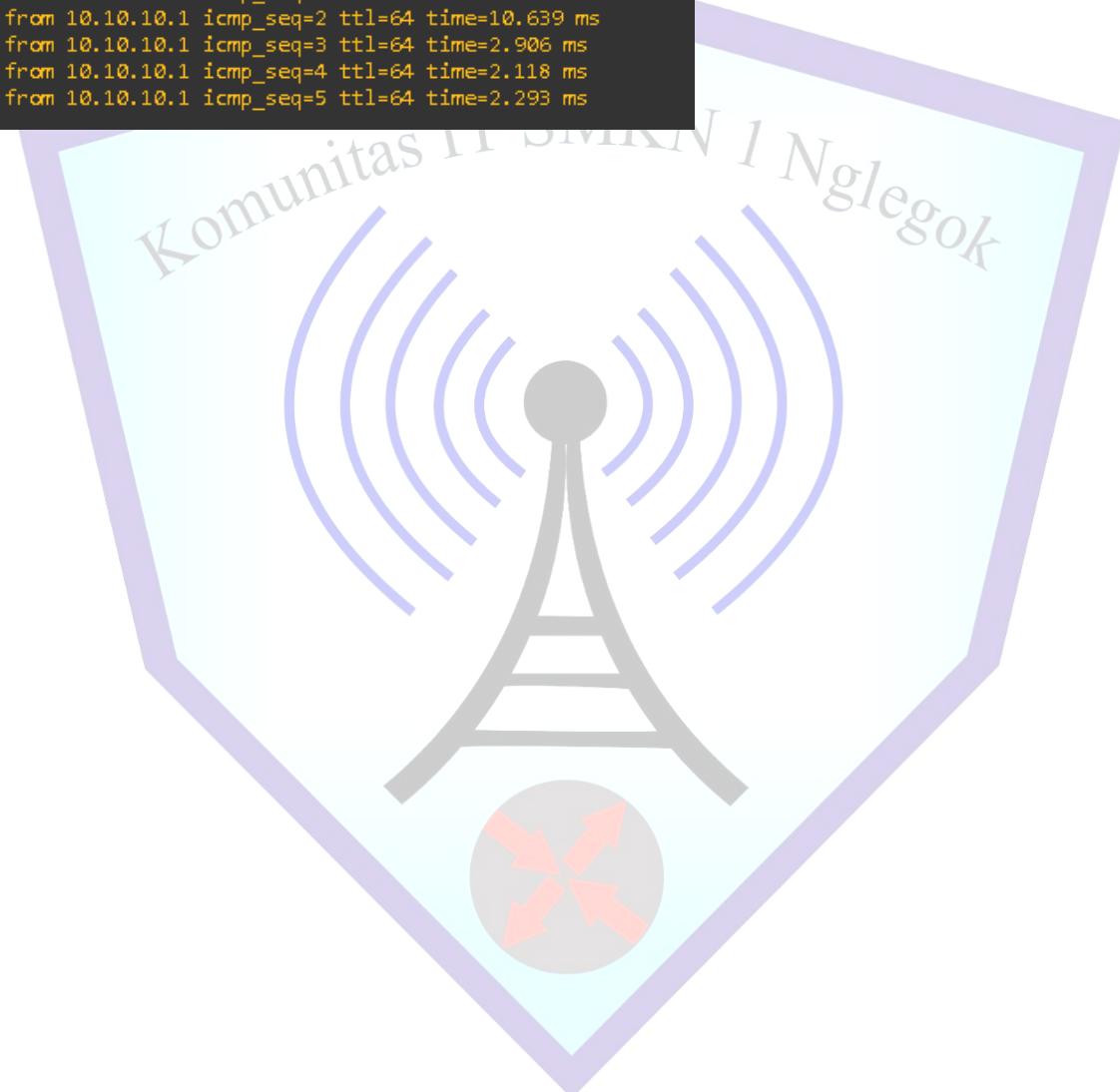
```
PC3> ip 10.10.10.4/24
Checking for duplicate address...
PC1 : 10.10.10.4 255.255.255.0

PC3> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=64 time=1.573 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=64 time=4.136 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=64 time=1.196 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=64 time=1.314 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=64 time=1.399 ms
```



```
PC4> ip 10.10.10.5/24
Checking for duplicate address...
PC1 : 10.10.10.5 255.255.255.0

PC4> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=64 time=1.134 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=64 time=10.639 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=64 time=2.906 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=64 time=2.118 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=64 time=2.293 ms
```

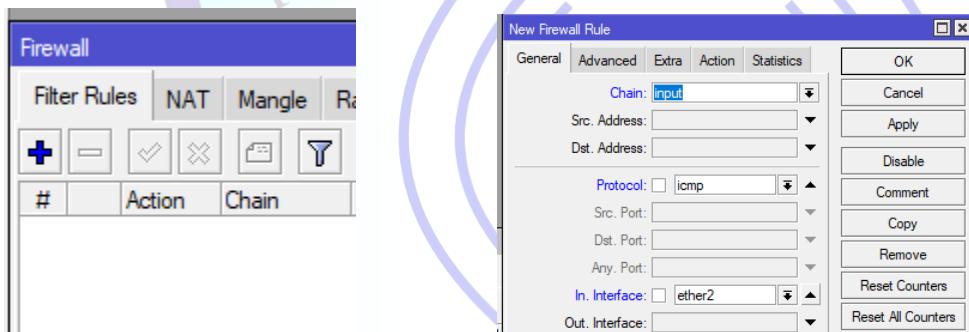




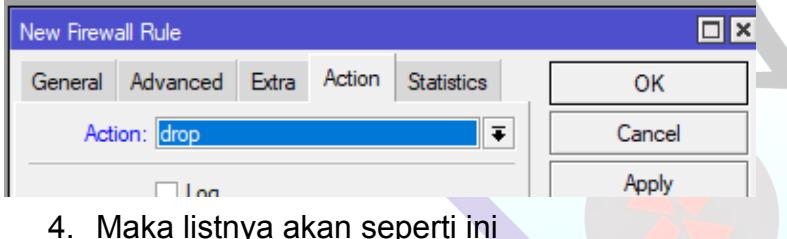
## LAB 34 Firewall Strategy 1 & 2

Pada lab kali ini, saya akan membahas mengenai Action Drop. Action Drop berfungsi untuk menolak paket tanpa memberi tahu pengirim bahwa paket tersebut ditolak. Contohnya, seperti seorang kurir pos yang mengantarkan paket ke suatu rumah, namun paket tersebut dibuang tanpa sepengertian pengirim. Agar lebih jelas, langsung saja kita lihat konfigurasi yang dapat digunakan, yaitu dengan memilih Chain: input dan in.Interface: ether2.

1. Login ke winbox
2. Lalu ip firewall nat dan ubah chain menjadi input protocol icmp dan in interfaceanya adalah ether2



3. Ubah juga action menjadi drop



4. Maka listnya akan seperti ini

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src...
0	drop	input			1 (c...							

5. Sebagai pengujinya kalian masuk ke cmd dan ping ip routernya jika hasilnya rto maka konfigurasi sudah berhasil



---

```
Administrator: Command Prompt + 
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pc-lab-1>ping 192.168.19.25

Pinging 192.168.19.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```



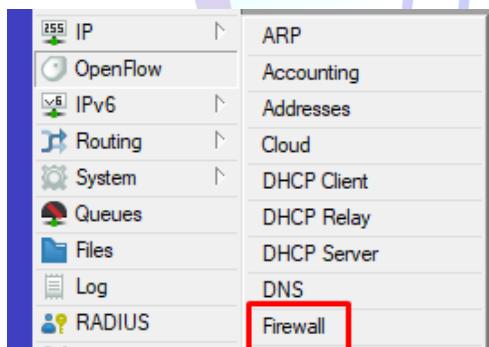


## LAB 35 Blokir Situs dengan Firewall Filter Forward (TLS)

### A.Firewall Filter Forward

Pada lab kali ini, saya akan membahas tentang cara memblokir situs menggunakan Firewall Filter Forward. Firewall Filter Forward berfungsi untuk memfilter paket-paket yang melewati router, seperti contoh paket ping dari client ke Google. Namun, kali ini kita akan fokus pada cara memblokir situs dengan memanfaatkan Firewall Filter Forward. Untuk melakukannya, mari kita ikuti langkah-langkah konfigurasi di bawah ini.

1. Login ke winbox
2. Lalu masuk ke IPfirewall



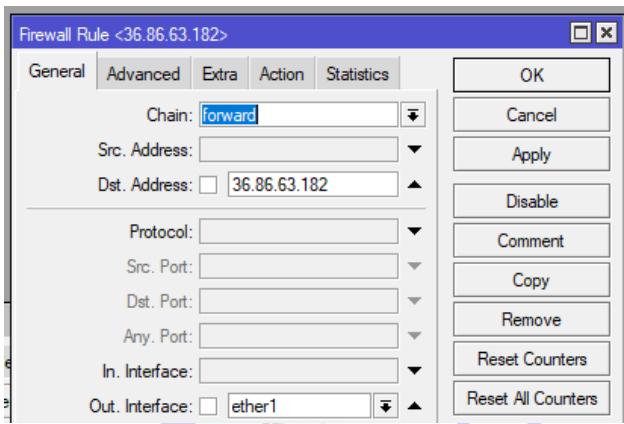
3. Lalu untuk melihat ip dari web yang ingin kita blokir dengan cara masuk ke dalam cmd dan ketikkan nslookup

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

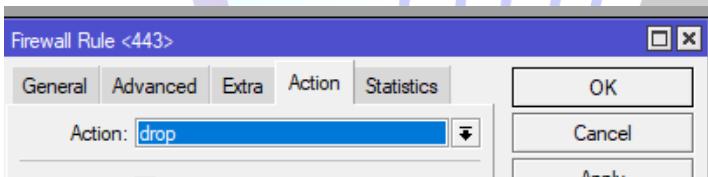
C:\Users\pc-lab-1>nslookup smkn1nglegok.sch.id
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: 10.10.3.1

DNS request timed out.
    timeout was 2 seconds.
Name: smkn1nglegok.sch.id
Address: 36.86.63.182
```

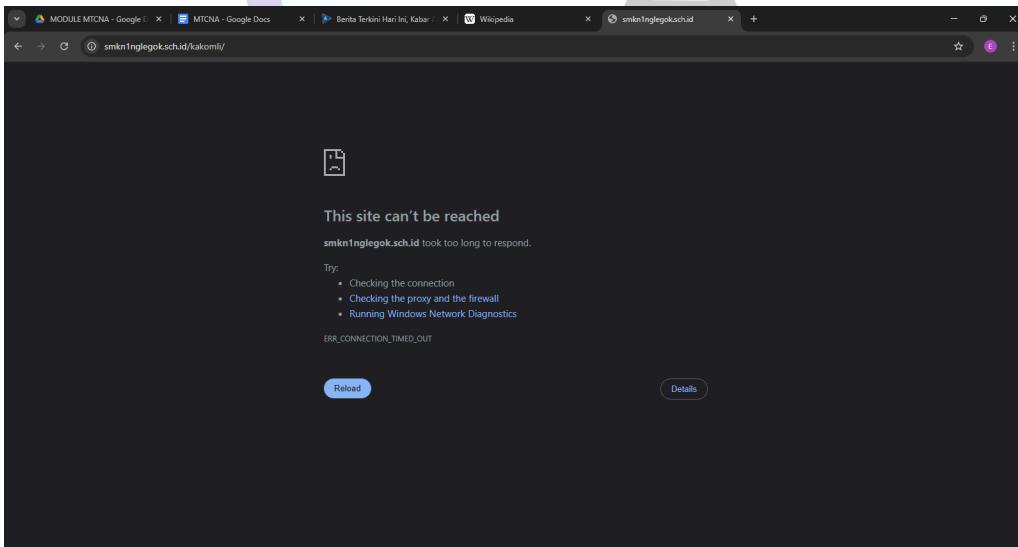
4. Lalu klik + dan ganti chain menjadi forward dan dst address kalian masukkan ip dari web yang ingin kalian blokir tadi



5. Lalu ganti actionnya menjadi drop



6. Dan jika sudah kalian kunjungi web yang kalian blokir tadi

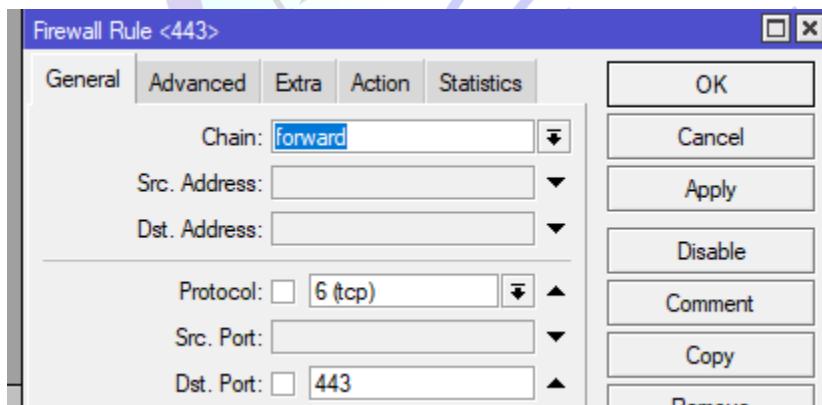




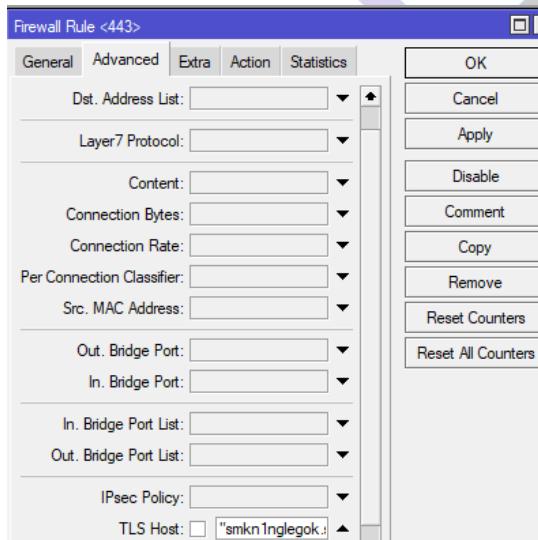
## B.TLS

Pada lab kali ini, saya akan membahas cara memblokir situs menggunakan Firewall Filter Forward. Firewall Filter Forward berfungsi untuk memfilter paket-paket yang melewati router, seperti contoh paket ping dari client menuju Google. Kali ini, kita akan fokus pada cara memblokir akses ke situs tertentu dengan memanfaatkan Firewall Filter Forward. Untuk melakukannya, mari kita ikuti langkah-langkah konfigurasi yang ada di bawah ini.

1. Buat Firewall rule baru lagi dengan ketentuan Chain forward Protocol 6 dan Dst Port 443

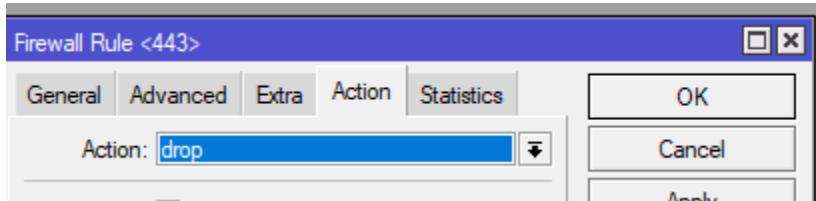


2. Berikutnya masuk ke Advance dan masukkan TLS host/ nama domain dari web yang ingin kalian blokir

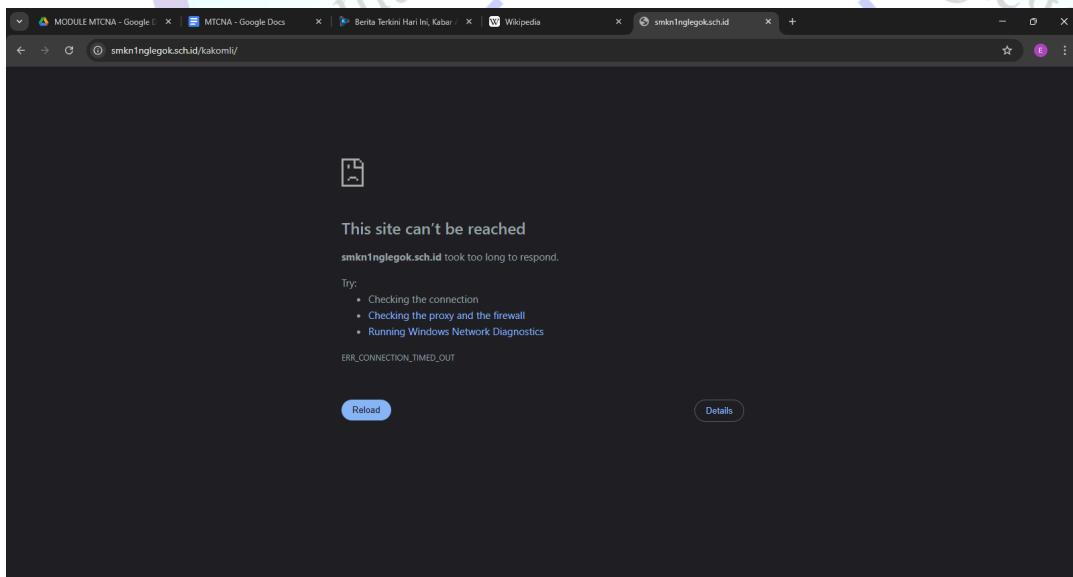




3. Setelah itu ke Action dan ganti menjadi Drop



4. Jika sudah kalian uji dengan cara masuk ke dalam web yang sudah kalian blokir tadi



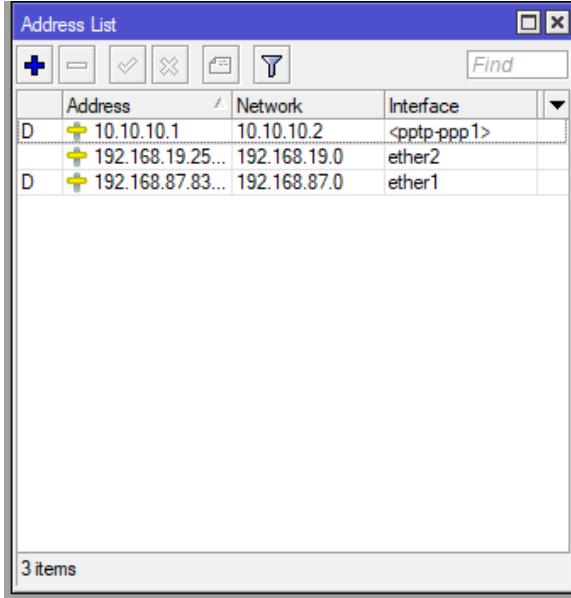
## LAB 36 Destination NAT Action (dst-nat & redirect)

Pada lab kali ini, saya akan membahas cara memblokir situs menggunakan Firewall Filter Forward. Firewall Filter Forward berfungsi untuk memfilter paket-paket yang melewati router, seperti halnya paket ping dari client menuju Google. Pada lab ini, kita akan fokus pada cara memblokir akses ke situs tertentu dengan memanfaatkan Firewall Filter Forward. Untuk melakukannya, mari ikuti langkah-langkah konfigurasi berikut ini.

### A. DST NAT



1. Login ke dalam winbox seperti biasa
2. Langkah selanjutnya ip address ether 2 dan saya akan menggunakan 192.168.19.25 nantinya akan di bridge ke dalam VMnya



3. Langkah selanjutnya kita akan menginstall apache2 pada VM debian kita. Comanndnya adalah apt install apache2

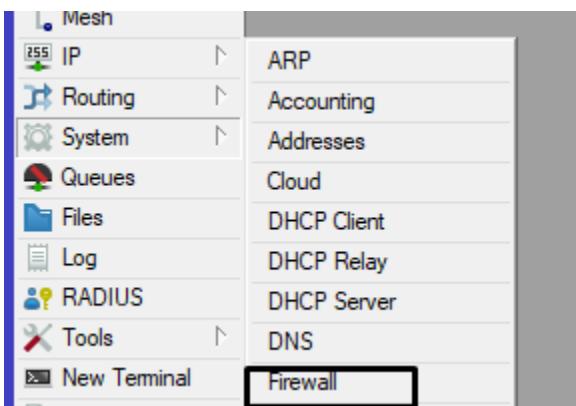
```
root@vbox:~# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.62-1~deb12u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

4. Setelah itu kita lihat ip yang kita peroleh dari router, comanndnya adalah ip a

```
inet6 :1/128 scope host noPreferredIface
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
      link/ether 08:00:27:3b:f6:8f brd ff:ff:ff:ff:ff:ff
      inet 192.168.19.23/24 brd 192.168.19.255 scope global dynamic enp0s3
          valid_lft 430sec preferred_lft 430sec
      inet6 fe80::a00:27ff:fe3b:f68f/64 scope link
          valid_lft forever preferred_lft forever
```



5. Setelah itu kita kembali ke winbox, lalu masuk ke IP > Firewall NAT dan kalian klik tombol +



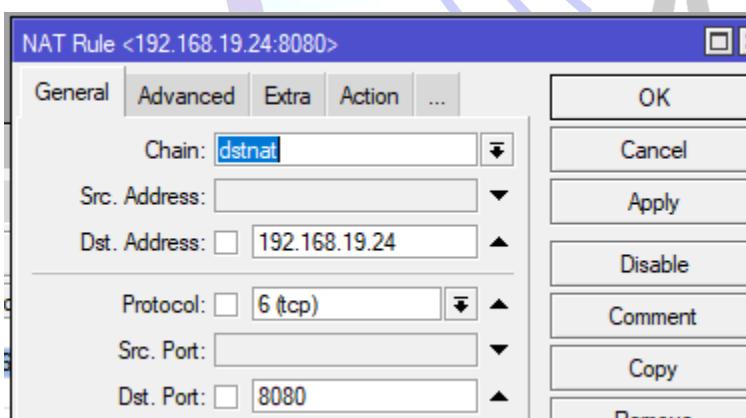
6. Kita buat NAT baru dengan ketentuan sebagai berikut ini

Chain : dstnat

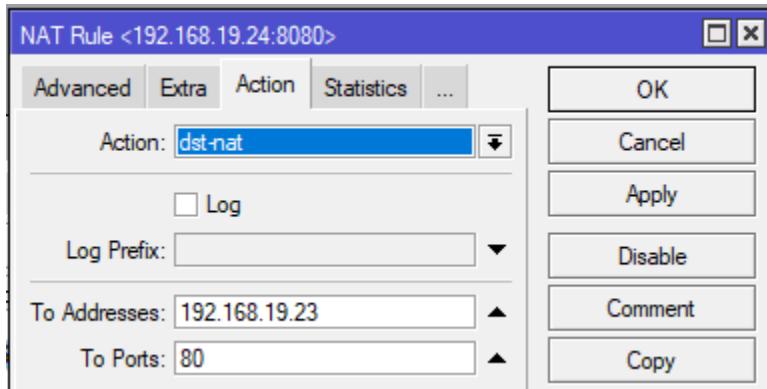
Dst Address kalian isikan IP dari PC kalian

Protocol : 6(tcp)

Dst Port : 8080



7. Selanjutnya kita masuk ke menu Action ganti menjadi dst-nat, To addressnya kalian isikan ip dari VM kalian, dan untuk To portsnya isikan 80.



8. Langkah terakhir kita akan akses apache 2 di web dengan cara kalian search menggunakan IP dari VM kalian



## Apache2 Debian Default Page

 It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.Load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain



The diagram features a central grey tower with three curved blue lines radiating from its top, representing signal transmission. Below the tower is a light blue circle containing four orange arrows pointing inwards towards a central point, symbolizing data flow or connectivity.



## B. Redirect

1. Langkah pertama kita masuk ke IP > Service dan pastikan port pada service www adalah 80

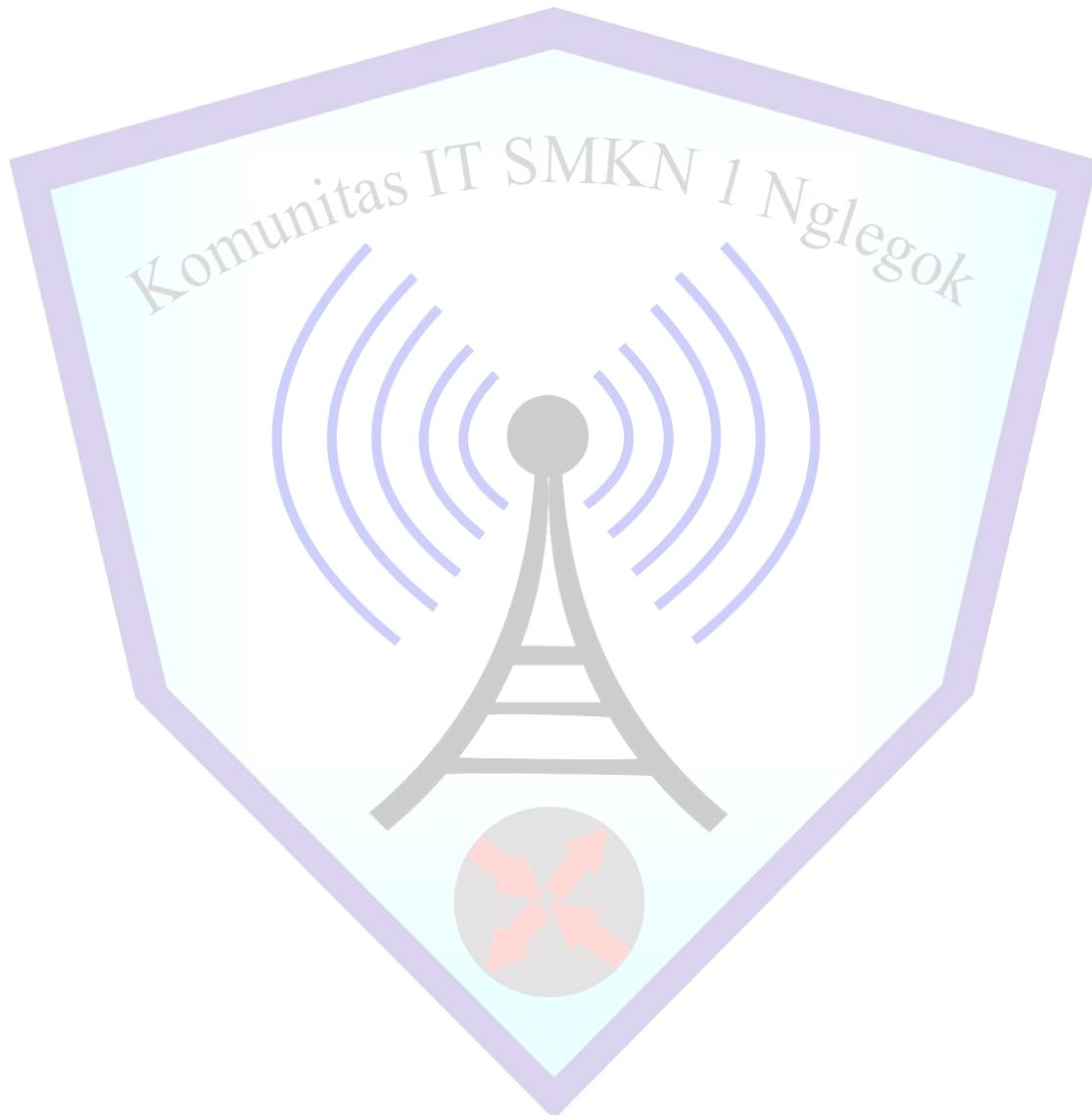
IP Service List					
	Name	Port	Available From	Certificate	TLS Ver...
●	api	8728			
●	api-ssl	8729		none	any
●	ftp	21			
●	ssh	22			
●	telnet	23			
●	winbox	8291			
●	www	80			

2. Berikutnya kalian masuk kedalam IP Firewall NAT dan buat nat baru. Untuk chainnya kalian isikan dstnat, protocolnya adalah 6(tcp) dan src portnya adalah 81

3. Berikutnya Masuk ke menu action dan ubah menjadi redirect, to portnya kalian masukkan 80



- 
4. Langkah terakhir kalian akses mikrotik menggunakan Webfig di chrome

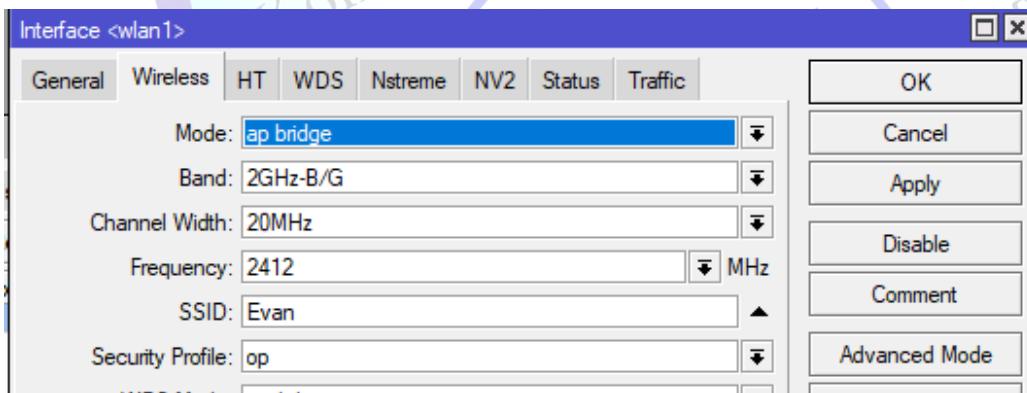




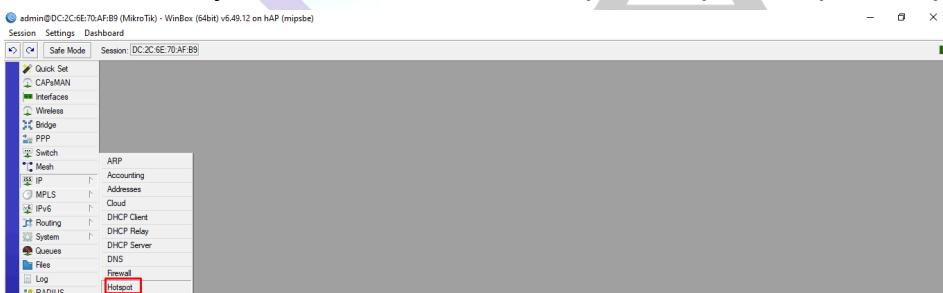
## LAB 37 Konfigurasi Dasar Hotspot

Pada lab kali ini, saya akan membahas tentang Hotspot yang disebarluaskan melalui jaringan wireless. Agar pengujian nanti lebih mudah, pastikan terlebih dahulu sudah memahami tentang lab Router Gateway dan Wireless AP (Access Point). Berikut adalah langkah-langkah konfigurasi yang perlu dilakukan.

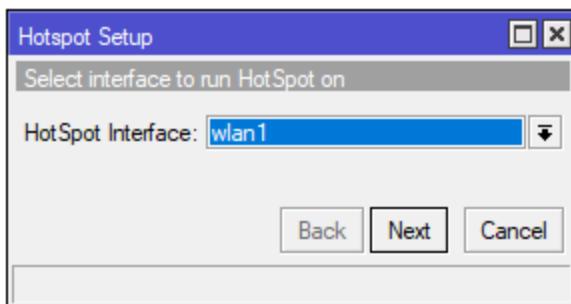
1. Masuk ke dalam winbox
2. Lalu ke interface aktifkan wlan 1 dan klik 2 kali. Kalian ubah modenya menjadai ap bridge



3. Berikutnya kalian masuk ke IP hospot dan pilih hospot setup



4. Pilih wlan 1





5. Kalian Masukkan nama domain sesuai dengan keinginan kalian

Hotspot Setup □ X

DNS name of local hotspot server

DNS Name:

Back Next Cancel

6. Lalu tambahkan nama user dan passwordnya

Hotspot Setup □ X

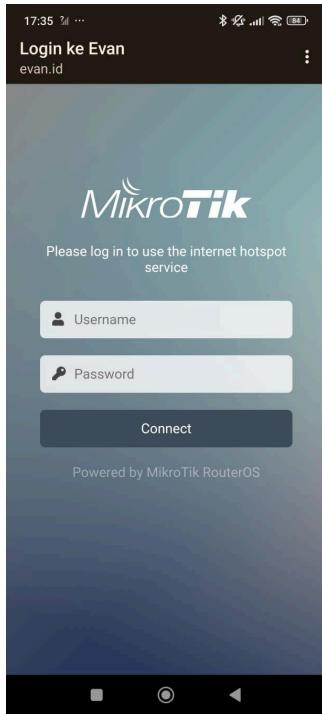
Create local HotSpot user

Name of Local HotSpot User:

Password for the User:

Back Next Cancel

7. Jika sudah maka tampilannya akan seperti di bawah ini

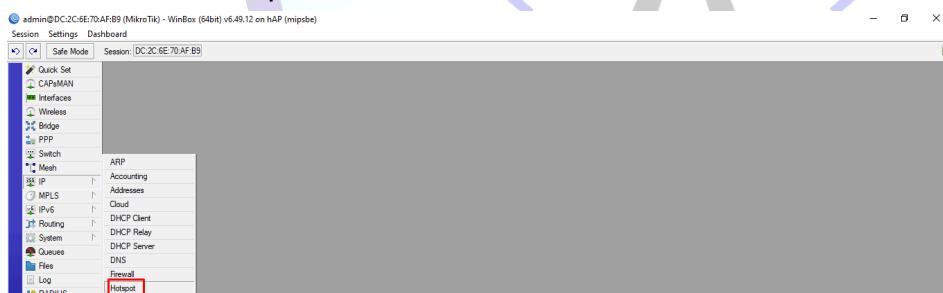




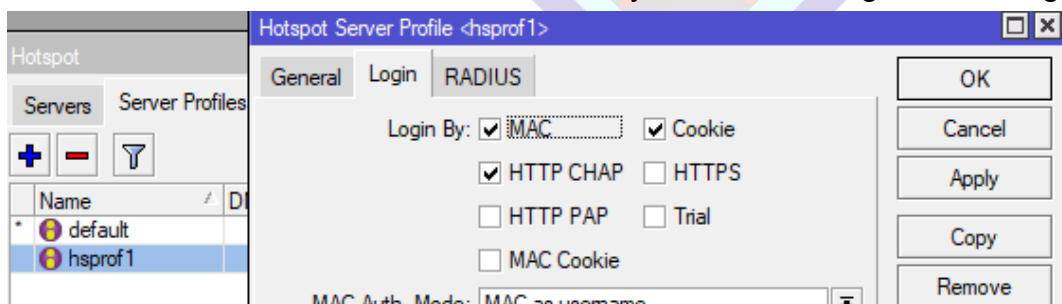
## LAB 38 Hotspot Login Methods HTTP CHAP/PAP

Pada lab kali ini, saya akan membahas tentang metode login Hotspot HTTP CHAP/PAP. Sebelum melanjutkan, kita perlu memahami bahwa HTTP CHAP/PAP adalah metode login default dan dasar pada hotspot Mikrotik. Ketika Hotspot dikonfigurasi di Router Mikrotik, metode login HTTP CHAP akan diaktifkan secara otomatis. HTTP PAP mengirimkan nama pengguna dan kata sandi dalam bentuk teks biasa melalui jaringan, yang menjadikannya tidak aman untuk digunakan di jaringan publik. Namun, HTTP PAP lebih cepat dan bisa digunakan di jaringan pribadi di mana keamanan tidak menjadi prioritas utama.

1. Masuk ke winbox
2. Lalu IP hotspot



3. Pilih server dan klik tombol + berikutnya kalian centang sesuai dengan contoh



4. Lalu untuk generalnya kalian ganti servernya menjadi all



Hotspot User <Evan>

General   Limits   Statistics

Server: all

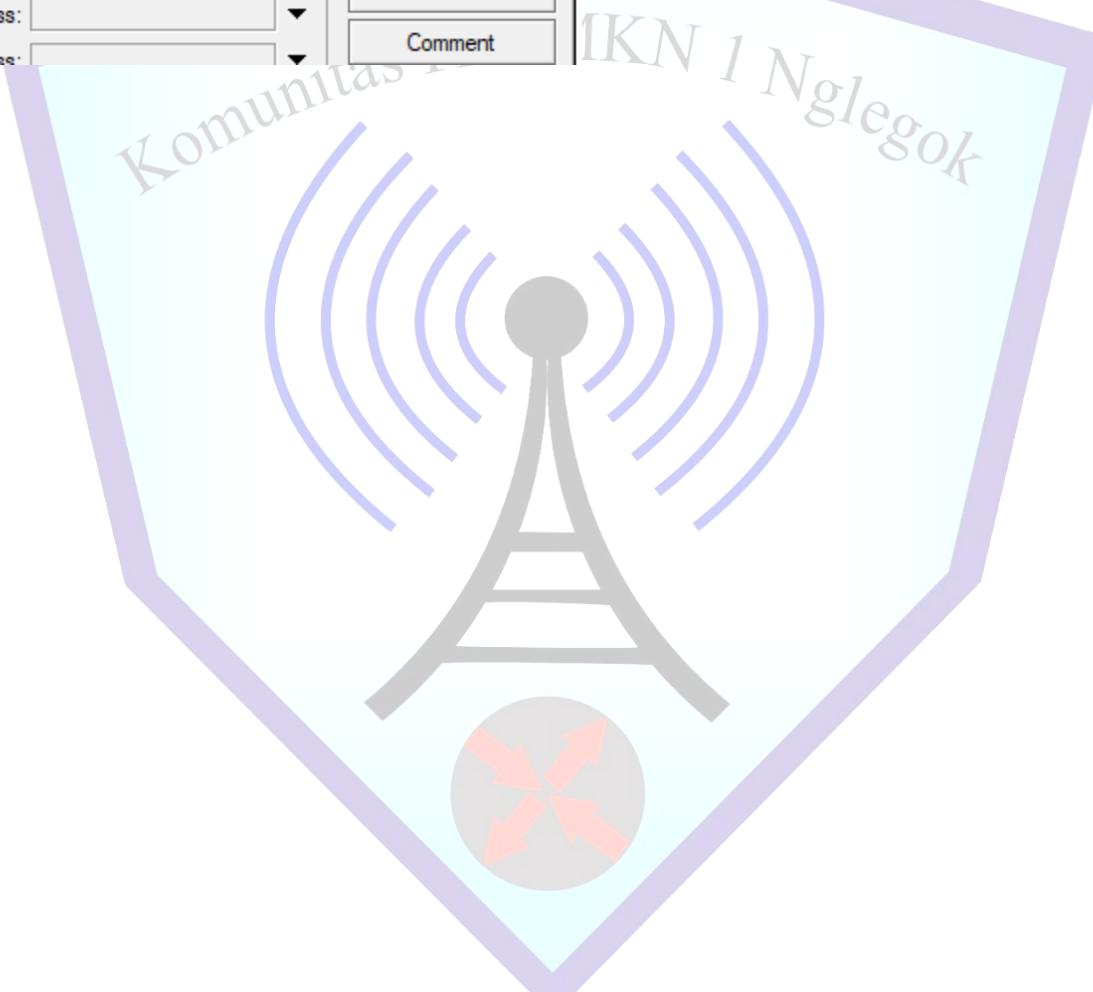
Name: Evan

Password: evancris

Address:

MAC Address:

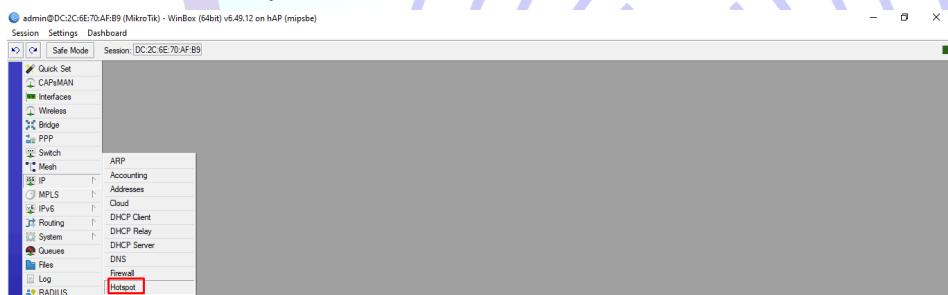
OK Cancel Apply Disable Comment





## LAB 39 Hotspot Profile (Keepalive timeout, shared user, Rate-limit)

1. Login ke winbox
2. Lalu IP hotspot



3. Pilih user Profiles dan klik tombol +



4. Disini kita setting kecepatan badwith, Waktu akses dan maksimal user



New Hotspot User Profile

General	Queue	Scripts
Name: Evan	OK	
Address Pool: none	Cancel	
Session Timeout:	Apply	
Idle Timeout: none	Copy	
Keepalive Timeout: 00:02:00	Remove	
Status Autorefresh: 00:01:00		
Shared Users: 7		
Rate Limit (rx/tx): 512k/512k		

5. Kita Bikin Users baru lagi dan disini daya menambahkan nama dan pasword lalu server kalian ganti menjadi all

New Hotspot User

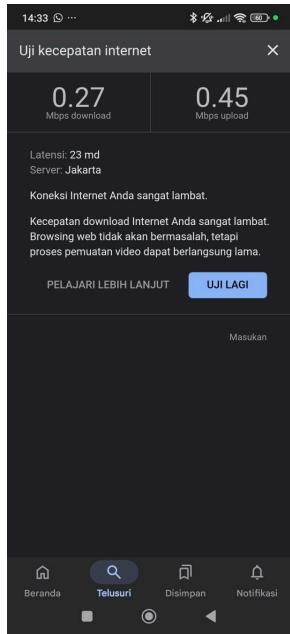
General	Limits	Statistics
Server: all	OK	
Name: evan	Cancel	
Password: 1925keren	Apply	
Address:	Disable	
	Comment	

6. Untuk melihat userss yanh sedang menggunakan hospot kita masuk ke host

Hotspot

Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	Cookies	...
A H	72:54:6F:D1:F0:32	192.168.80.252	192.168.80.252	hotspot1	00:00:08	0 bps	0 bps		

7. Langkah terakhir kita lakukan pengetesan

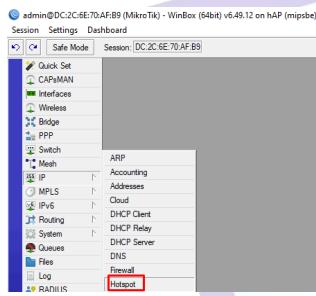




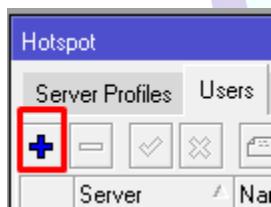
## LAB 40 Hotspot Users Add User

Pada kali ini kita akan membahas tentang fitur hotspot yang berada dalam mikrotik yaitu add user, berikut pembahasannya

1. Login ke winbox
2. Lalu IP hotspot



3. Masuk ke users dan klik tombol +



4. Dan kalian buat users sesuai dengan keinginan kalian

Hotspot User <Evan>

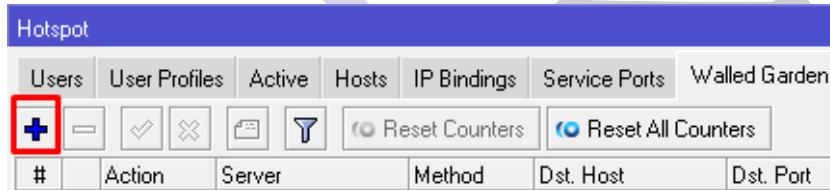
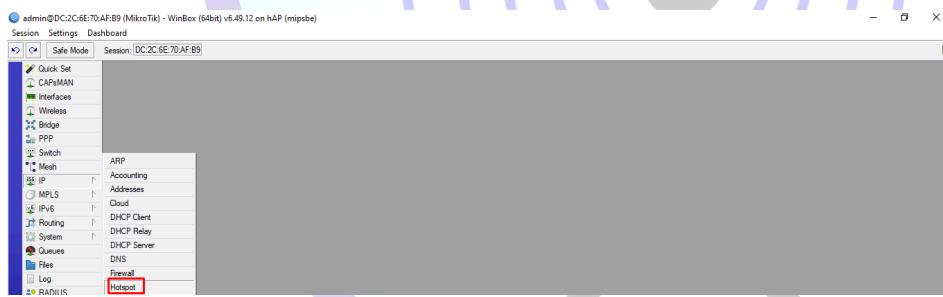
General	Limits	Statistics
Server: all		OK
Name: Evan		Cancel
Password: 199		Apply
Address:		Disable
MAC Address:		Comment
Profile: Evan		Copy
Routes:		Remove
Email:		Reset Counters
enabled		



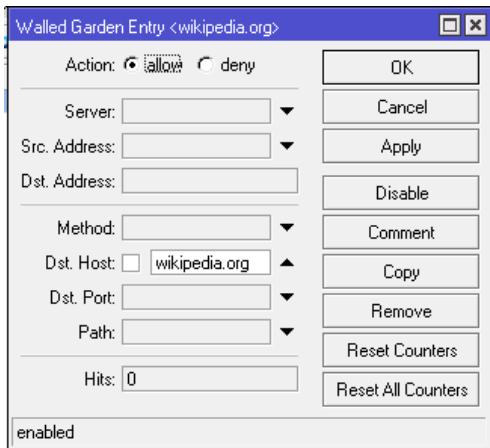
## LAB 41 Bypass Hotspot Walled Garden

Pada lab kali ini, saya akan membahas salah satu fitur Hotspot pada MikroTik, yaitu Walled Garden. Sebelum melanjutkan, apakah kalian tahu apa itu Walled Garden? Walled Garden adalah fitur pada Hotspot MikroTik yang memungkinkan administrator jaringan untuk mengonfigurasi akses terbatas bagi client. Dengan fitur ini, client dapat mengakses beberapa situs web atau layanan tertentu meskipun mereka belum login, sementara akses ke layanan lain dibatasi. Sebagai contoh, saya akan membuat client yang belum login dapat mengakses situs mikrotik.com, tetapi tidak bisa mengakses situs atau layanan lainnya.

1. Langkah pertama buat konfigurasi Hotspot, setelah itu masuk ke IP Hotspot Kalian pilih Tab Walled Garden dan klik tombol +



2. Disini karena kita mengizinkan Client bisa mengakses suatu layanan maka kita pilih Actionnya Allow dan Dst hosts kita isikan dengan alamat web tujuan kita



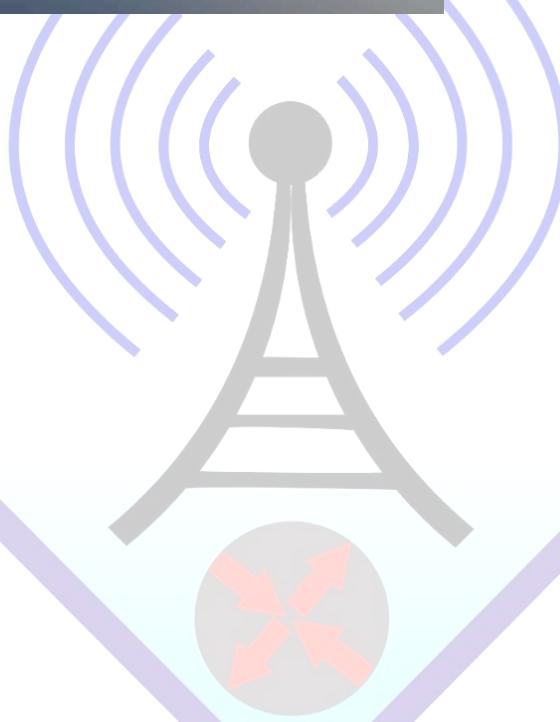
3. Lalu kita akan melakukan pengujian dengan menyambungkan perangkat hotspot, lalu akses web yang telah kita pilih tadi



4. Hasilnya jika kita mengunjungi web lain maka akan diarahkan menuju login kembali.



1 Nglegok

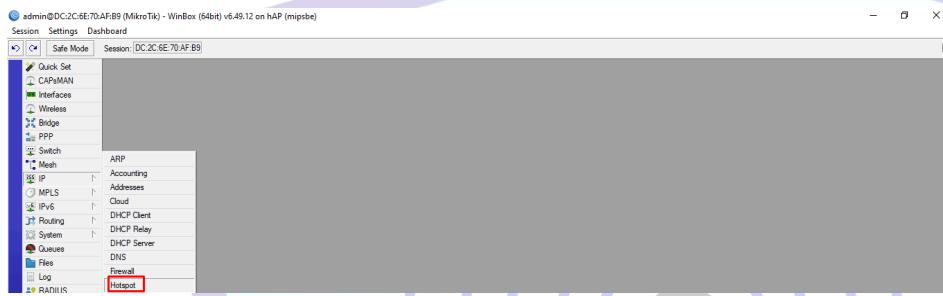




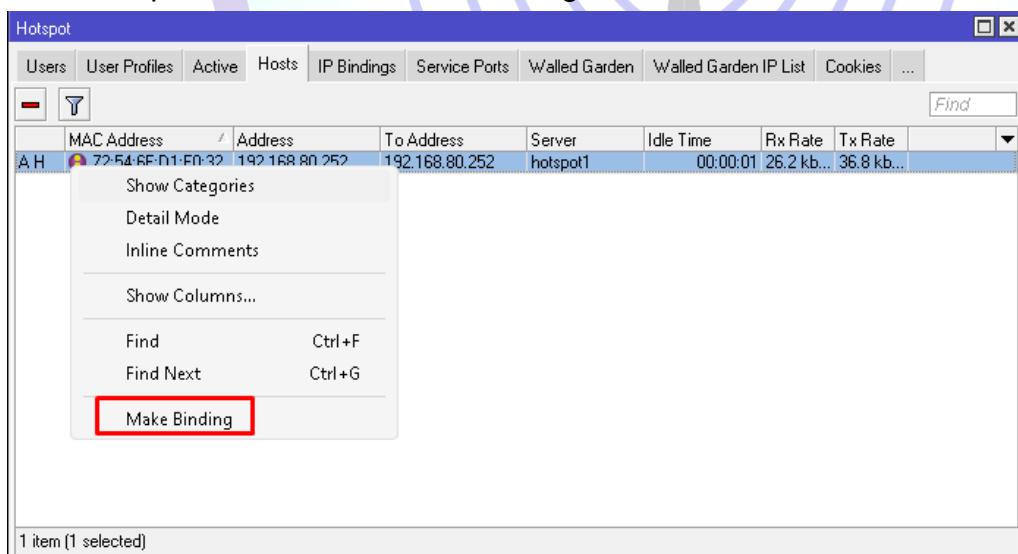
## LAB 42 Bypass Hotspot IP Binding (regular, bypass,blocked)

### A. Reguler

1. Masuk ke winbox
2. Lalu kalian ke IP hospot



3. Masukke Host dan kalian klik 2 kali pada salah satu client yang tersambung hospot kita, lalu klik Make Binding.



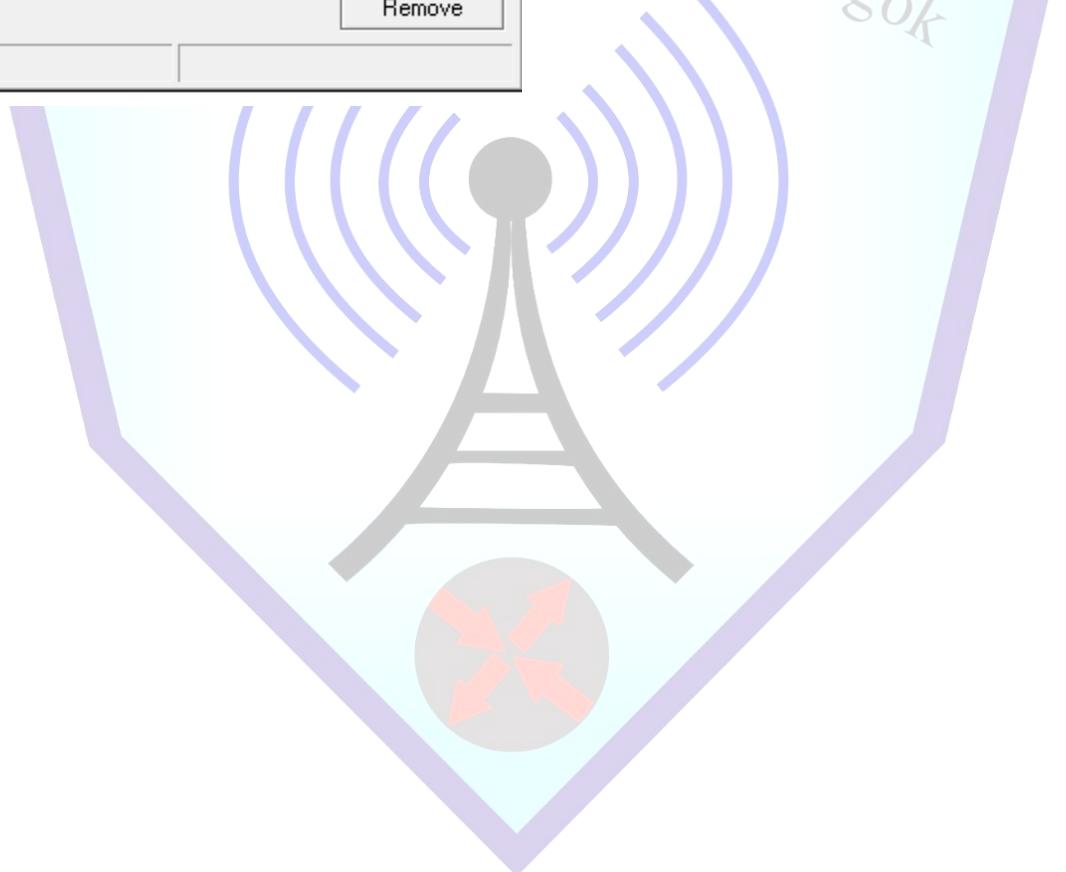
4. Setelah itu kita akan mengubah type pada IP bindinh menjadi regulae



New Hotspot IP Binding

MAC Address:	72:54:6F:D1:F0:32	OK
Address:	192.168.80.252	Cancel
To Address:	192.168.80.252	Apply
Server:	hotspot1	Disable
Type:	regular	Comment
		Copy
		Remove

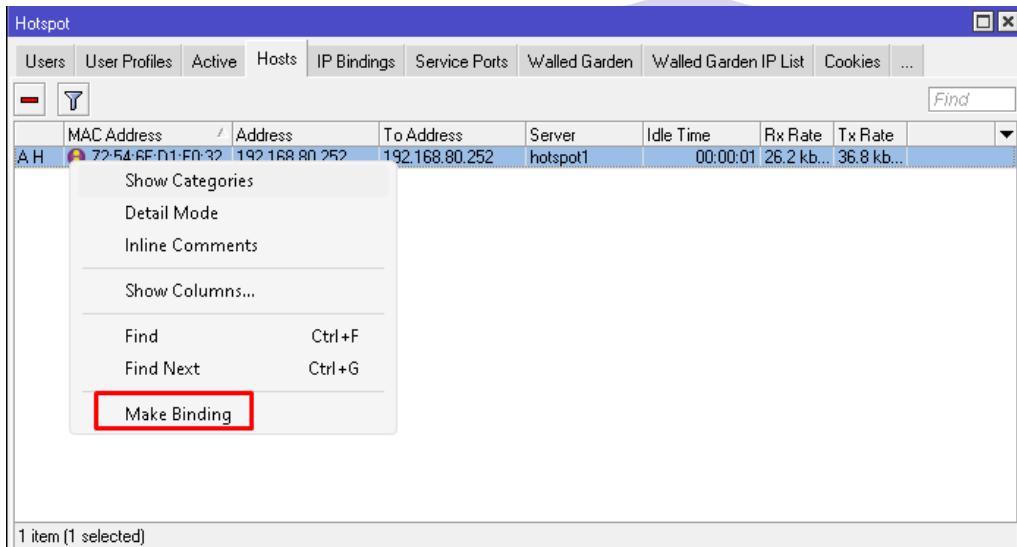
enabled



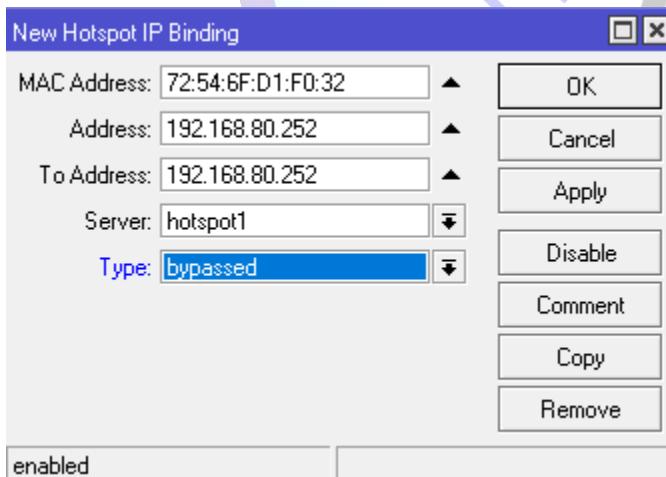


## B. Bypass

1. Masuk winbox, lalu ke IP hotspot> Host dan klik 2 kali pada client setelah itu kalian klik Make Binding



2. Kita akan merubah typenya menjadi bypassed



3. Kita lakukan pengetesan dengan mengakses internet tanpa login pada client.



## WIKIPEDIA

Ensiklopedia bebas

Bahasa Indonesia

718,000+ artikel

English

6,949,000+ articles

日本語

1,447,000+ 文章

Русский

2,023,000+ статьи

Deutsch

2,984,000+ Artikel

Español

2,006,000+ artículos

Français

2,662,000+ articles

Italiano

1,903,000+ articoli

中文

1,461,000+ 条目 / 條目

فارسی

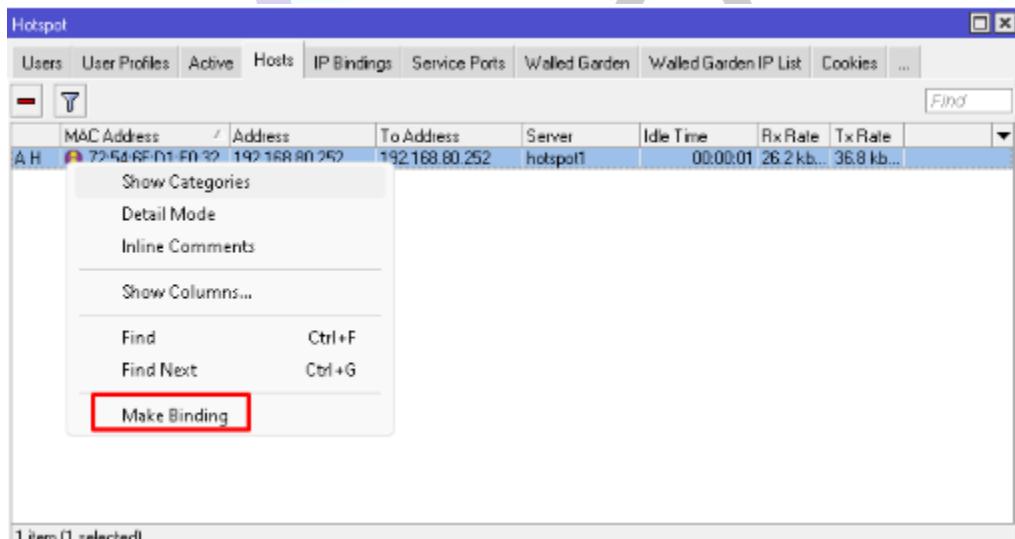
۱,۴۶۱,۰۰۰+ مقاله +۳۷۸,۰۰۰+

ID

XA Baca Wikipedia dalam bahasa Anda ▾

## C. Blocked

1. Masuk winbox, lalu ke IP hotspot> Host dan klik 2 kali pada client setelah itu kalian klik Make Binding



2. Kita ubah typenya menjadi blocked



Hotspot IP Binding <192.168.19.24>

MAC Address:	BE:97:3E:1F:08:08	▲	OK
Address:	192.168.19.24	▲	Cancel
To Address:	192.168.19.24	▲	Apply
Server:	hotspot1	▼	Disable
Type:	blocked	▼	Comment
			Copy
			Remove

enabled      blocked

3. Untuk pengujian kita akan mencoba dari sisi client dan hasilnya client kita tidak akan mengakses internet.

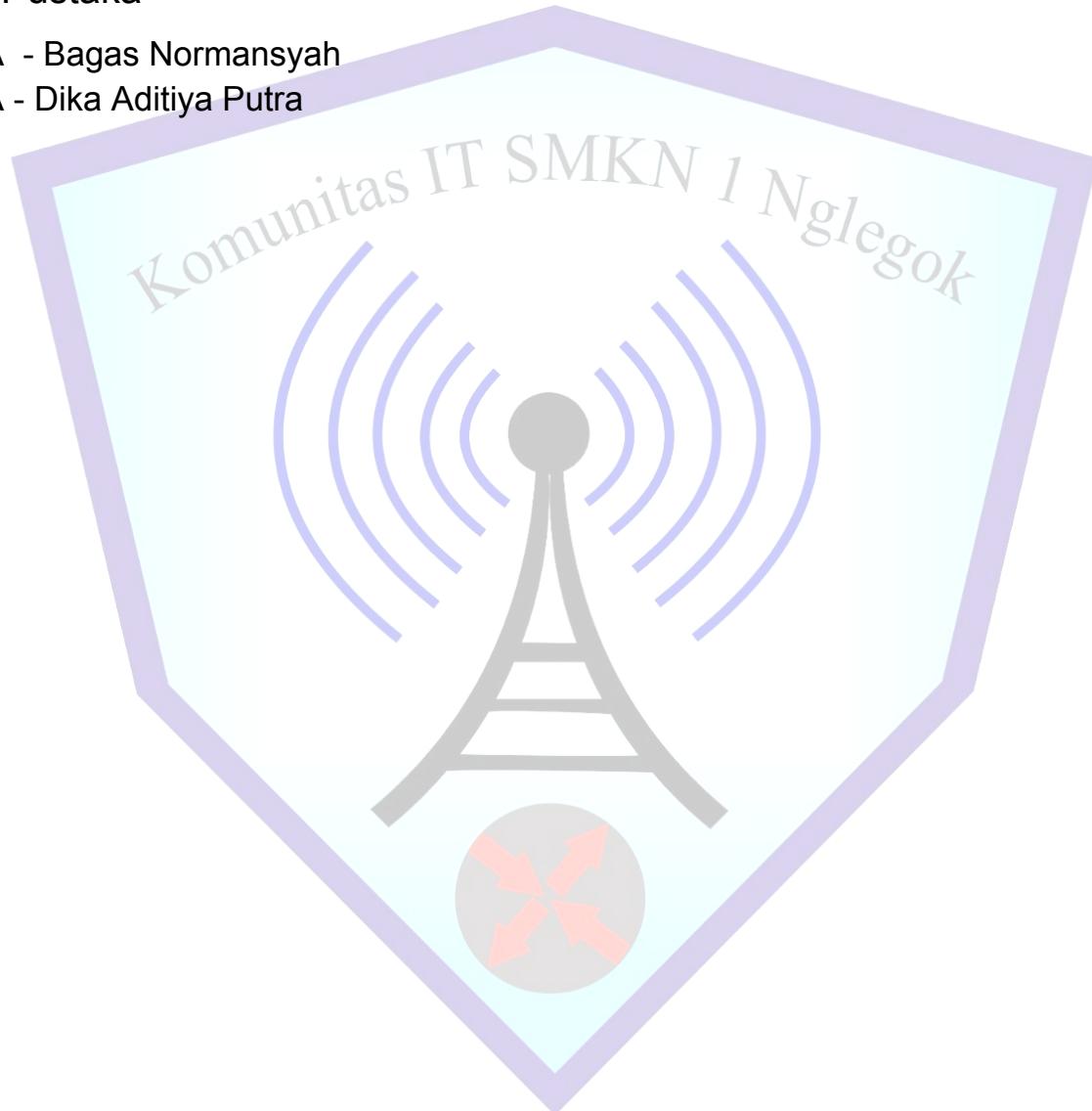
#	MAC Address	Address	To Address	Server	
0 B	BE:97:3E:1F:08:08	192.168.19.24	192.168.19.24	hotspot1	



## Daftar Pustaka

MTCNA - Bagas Normansyah

MTCNA - Dika Aditya Putra





## Biografi Penulis



Perkenalkan nama saya Evan Cristianto, saya biasanya dipanggil evan. Saya lahir di Blitar 25 Oktober 2008. Saya membuat buku ini saat berusia 16 tahun. Saya mempunyai orang tua yang terus memberi semangat serta dukungan sehingga dapat menyelesaikan buku dengan tepat waktu. Ayah saya bernama Edi Susanto dan Ibu saya bernama Desiati.

Sebelum saya bersekolah di SMKN 1 Nglegok saya terlebih dahulu sekolah di SMPN 2 Gandusari dan melanjutkan di SMKN 1 Nglegok Jurusan Teknik Komputer dan jaringan. Alasan saya memilih TKJ karena saya dari kecil sudah menyukai computer. Karena keinginan saya untuk menjadi IT

yang handal saya bergabung dengan Komunitas IT SMKN 1 Nglegok agar saya dapat berkembang tidak hanya skil tapi seluruhnya.

Semoga buku yang saya buat ini serta semua ilmu dapat berguna, serta bermanfaat bagi semua orang tanpa terkecuali. Terima Kasih.