



Certified Network Associate (MTCNA) Preparation

Title	Object
Introduction	About Mikrotik
	First Time Accessing the router
	Initial configuration (Internet access)
	Upgrading RouterOS
	Router identity
	Manage RouterOS logins
	Manage RouterOS services
	Managing configuration backups
	Resetting a RouterOS device
	Reinstalling a RouterOS device (Netinstall)
	RouterOS license levels
DHCP	DHCP server and client
	Address Resolution Protocol (ARP)
Wireless	802.11a/b/g/n/ac Concepts
	Setup a simple wireless link
	Wireless Security and Encryption
Firewall	Firewall principles
	NAT

MODULE 1

INTRODUCTION



*Mikro***Tik**

About Exam

Kriteria Exam

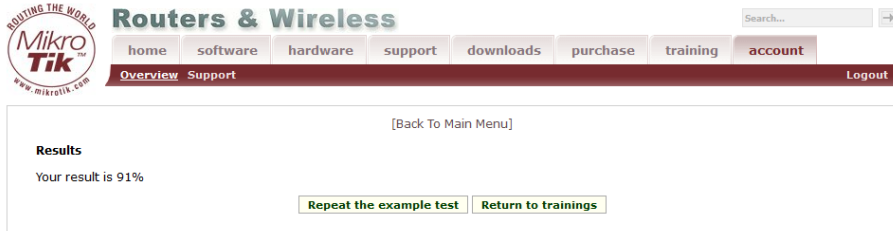
- Soal ujian sertifikasi menggunakan bahasa Inggris.
- Tidak boleh copy paste dan screenshot soal.
- Waktu mengikuti Ujian Online Jika Score Dibawah atau sama dengan 49 maka dinyatakan TIDAK LULUS
- Jika Score Antara 50%-59% akan mendapat kesempatan yg ke 2 dengan Mengikuti Ujian Online sekali lagi (biasanya soalnya lebih rumit).
- Jika Score 60% keatas dinyatakan LULUS
- Dan bagi yg ingin menjadi TRAINER Score Lulus Minimal 75 %
- Masa Berlaku Sertifikat 3 Tahun
- Tipe ujian nya open book, jadi boleh buka buku apa saja, namun tidak boleh tanya dan mencontek siapapun.

Registrasi

- Buka situs resmi mikrotik di <https://www.mikrotik.com/> kemudian masuk ke tab account, pilih register
- Isi informasi dengan lengkap dan benar karena nama account tercetak sebagai nama sertifikat anda.
- Jika sudah mempunyai account silahkan langsung login menggunakan username dan password sesuai dengan tahap registrasi anda.
- Ketika sudah login masuk ke menu my training session dan pilih try example test (20 soal & tidak ada batasan waktu)

Pembahasan Sample Test

Disini saya hanya mendapatkan 91%, jadi silahkan dikoreksi jika terdapat beberap jawaban yang salah.



ROUTING THE WORLD
MikroTik
www.mikrotik.com

home software hardware support downloads purchase training **account**

Overview Support Logout

[Back To Main Menu]

Results
Your result is 91%

[Repeat the example test](#) [Return to trainings](#)

1. Choose all valid hosts address range for subnet 15.242.55.62/27

- 15.242.55.32-15.242.55.63
- 15.242.55.33-15.242.55.63
- 15.242.55.31-15.242.55.62
- 15.242.55.33-15.242.55.62

Pembahasan :

Subnetmask /27 = 255.255.255.224

Jumlah IP = 256 – 224 = 32

Range Network :

Network	Host	Broadcast
0	1 – 30	31
32	33 – 62	63

Karena pertanyaannya adalah semua host yang valid, bukan semua ip pada blok tersebut maka saya pilih jawaban yang hanya terdapat IP hostnya saja yakni :

15.242.55.33 – 15.242.55.62

2. Select valid subnet masks:

- 192.0.0.0
- 255.255.224.0
- 255.192.0.0
- 255.255.192.255

Pembahasan :

Subnetmask didapat dari hasil penerjemahan biner pada IPV4 ke bilangan decimal, dimulai dari /1 - /32 (Sesuai dengan panjangnya IPV4 yakni 32 bit), maka dari itu desimalnya akan berurutan (setelah biner 0 maka tidak ada lagi biner 1), seperti yang terjadi dijawab 255.255.192.255 yang artinya jika diterjemahkan pada biner tidak akan ketemu :

11111111.11111111.11000000.11111111

Maka dapat dipastikan kecuali Subnetmask 255.255.255.192.255

3. Select valid MAC-address

- 00:00:5E:80:EE:B0
- 192.168.0.0/16
- AEC8:21F1:AA44:54FF:1111:DDAE:0212:1201
- G2:60:CF:21:99:H0

Pembahasan :

MAC Address intinya terdiri dari 6 bytes, maka sudah dipastikan jawabannya antara a dan d (anggap saja ada pointnya diurut dari atas), kemudian kriteria lainnya penomorannya adalah dari 0 – F. Jadi sudah dipastikan bahwa point A adalah jawaban yang benar.

4. In MikroTik RouterOS, Layer-3 communication between 2 hosts can be achieved by using an address subnet of:

- /29
- /32
- /31
- /30

Pembahasan :

Subnet yang bisa menghubungkan 2 host adalah ? Ingat patokannya saja :

/28 = 16 (Karena $2 \times 8 = 16$, ini sebagai patokan jika naik dibagi 2, turun $\times 2$)

/29 = 8

/30 = 4

/31 = 2

/32 = 0

Maka dapat disimpulkan bahwa yang bisa menjalin komunikasi 2 host adalah /29 dan /30.

5. Is ARP used in the IPv6 protocol ?

Pembahasan :

Coba lihat perbandingan IPV4 dan IPV6 di situs IBM berikut :

http://www.ibm.com/support/knowledgecenter/ssw_i5_54/rzai2/rzai2compipv4ipv6.htm

Di bagian tabel Address Resolution Protokol terlihat seperti dibawah ini kutipannya :

Address Resolution Protocol is used by IPv4 to find a physical address, such as the MAC or link address, associated with an IPv4 address.	IPv6 embeds these functions within IP itself as part of the algorithms for stateless autoconfiguration and neighbor discovery using Internet Control Message Protocol version 6 (ICMPv6). Hence, there is no such thing as ARP6.
---	--

Bahwasannya IPV6 sudah memiliki fungsi dari ARP yang dimiliki IPV4, jadi IPV6 sudah tidak lagi menggunakan protocol ARP yang digunakan pada IPV4. Jawabannya **false** Atau bisa juga dilihat di :

<http://electronicdesign.com/embedded/whats-difference-between-ipv4-and-ipv6>

IP to MAC resolution	broadcast ARP	Multicast Neighbor Solicitation
-----------------------------	---------------	---------------------------------

Cukup banyak refererensi yang menjelaskan keduanya, untuk lebih jelasnya mengenai IPV4 dan IPV6 akan dijelaskan pada BAB berikutnya.

6. Which of the following are valid IP addresses?

- 192.168.256.1
- 10.10.14.0
- 192.168.13.255
- 1.27.14.254

Pembahasan :

IPV4 terdiri dari 8 bit, jika di desimalkan maka totalnya adalah 256 per oktatnya, itu semua total. Namun, yang perlu diperhatikan adalah IPV4 dimulai dari 0 dan diakhiri sampai 255. Jadi pada pengalamatannya tidak ada yang sampai dengan 256. Selain itu tidak ada juga jika dimulai dari 0 pada oktat pertama. Maka jawabannya adalah selain 192.168.256.1

7. How many IP addresses can one find in the header of an IP packet?

- 1
- 3
- 4
- 2

Pembahasan :

IP Address pada header IP Packet sebanyak 2 buah, yakni Source dan Destination IP Address :

Sumber : <https://en.wikipedia.org/wiki/IPv4>

Offsets	Octet	0				1				2				3																			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP				ECN				Total Length															
4	32	Identification								Flags				Fragment Offset																			
8	64	Time To Live				Protocol				Header Checksum																							
12	96	Source IP Address								Destination IP Address																							
16	128																																
20	160																																
24	192																																
28	224																																
32	256									Options (if IHL > 5)																							

8. The network address is

- The first address of the subnet
- The first usable address of the subnet
- The last address of the subnet

Pembahasan :

Network Address adalah IP Address pertama pada sebuah subnet. Jika dilihat dari pilihan diatas, ada yang menyebutkan IP usable (yang digunakan) pertama dari sebuah subnet (network address tidak dapat digunakan), dan ip terakhir pada sebuah subnet (jika broadcast ip bisa saja ini jawabannya). Jadi kedua argument tersebut merupakan salah. Jawaban : Point A.

9. What protocol does ping use?

- ICMP
- TCP
- ARP
- UDP

Pembahasan :

PING menggunakan protocol ICMP. Protkol icmp dikirimkan melalui paket IP dan digunakan untuk mengirim pemberitahuan yang berhubungan dengan kondisi jaringan.

10. Collisions are possible in full-duplex Ethernet networks

false

Pembahasan :

Full Duplex adalah bentuk komunikasi 2 arah, dimana data dikirimkan dalam 1 waktu. Mempunyai kanal terpisah untuk setiap arahnya. Jadi kecil kemungkinan untuk terjadinya collision.

11. The basic unit of a physical network (OSI Layer 1) is the:

- Byte
- Bit
- Header
- Frame

Pembahasan :

Pada OSI Layer, layer 1 adalah physical yang mempunyai ciri salah satunya adalah bentuk data yang dikirimkan adalah melalui bit-bit. Anda bisa cek di Wikipedia mengenai OSI Layer.

12. How many layers does Open Systems Interconnection model have?

- 12
- 5
- 9
- 7
- 6

Pembahasan :

OSI Layer memiliki 7 Layer yakni :

Application, Presentation, Session, Transport, Network, Data Link, Physical

13. Which of the following is NOT a valid MAC Address?

- EA:BA:AA:EE:FF:CB
- 13:16:86:53:89:43
- 80:GF:AA:67:13:5D
- 95:B5:DD:EE:78:8A
- 88:0C:00:99:5F:EF

Pembahasan :

Sama dengan pembahasan no.3, namun pada kali ini adalah inversnya. Sudah jelas jika salah satu saja terdapat angka atau huruf yang diluar 0 – F maka bukanlah MAC Address / Tidak valid.

14. Which of the following protocols / ports are used for SNMP. (Simple Network Management Protocol)

- TCP 25
- TCP 123
- UDP 162
- TCP 161
- TCP 162
- UDP 161

Pembahasan :

SNMP menggunakan Protokol UDP dan Portnya adalah 161 untuk agent dan 162 untuk manager.

15. How many usable IP addresses are there in a 20-bit subnet?

- 4096
- 2048
- 4094
- 2047
- 2046

Pembahasan :

$/20 = /28 = 16$ Host

Karena berada di oktat ke-3 maka total IP $\times 256 = 4096 - 2$
(Network dan Broadcast) = 4094

16. MAC layer by OSI model is also known as

- Layer 3
- Layer 7
- Layer 6
- Layer 1
- Layer 2

Pembahasan :

MAC Address masuk kedalam Data Link yang merupakan alamat fisik dari sebuah perangkat.

17. Which computers would be able to communicate directly (without any routers involved):

- 192.168.0.5/26 and 192.168.0.100
- 192.168.17.15/29 and 192.168.17.20/28
- 10.5.5.1/24 and 10.5.5.100/25
- 10.10.0.17/22 and 10.10.1.30/23

Pembahasan :

$/26$ memiliki jumlah IP 64, jadi rasanya tidak mungkin karena 5 masuk kedalam blok 1 (0-63), sedangkan 100 masuk kedalam blok ke-2 (64 – 127).

/29 = 8 Host, 15 masuk kedalam kelompok 8 – 15 tetapi 15 tidak bisa digunakan untuk berkomunikasi karena merupakan broadcast address. /28 memiliki 16 host, 20 masuk kedalam blok 16 – 31. Dan sudah dapat dipastikan mereka berbeda network dan broadcast/tidak bisa berkomunikasi secara langsung.

/24 = 256 host, /25 = 128 host. Jadi ip yang menggunakan /25 masih masuk kedalam subnet /24

/22 = 4 host (Oktat ke-3 dari 0-3), /23 = 2 host (Oktat ke-3 dari 0-1), sudah dapat dilihat 0-1 masih dalam 1 blok subnet. Jadi bisa terhubung.

Jadi, pilihan ke-3 dan ke-4 jawabannya adalah bisa saling terhubung langsung.

18. What is term for the hardware coded address found on an interface?

- IP Address
- MAC Address
- FQDN Address
- Interface Address

Pembahasan :

Hardware Coded in Interface = Physical Address = MAC Address

19. Select which of the following are 'Public IP addresses':

- 11.63.72.21
- 10.110.50.37
- 172.28.73.21
- 192.168.0.1
- 172.168.254.2

Pembahasan :

Lihat referensi kembali mengenai IP Private :

RFC1918 name	IP address range	number of addresses
24-bit block	10.0.0.0 - 10.255.255.255	16,777,216
20-bit block	172.16.0.0 - 172.31.255.255	1,048,576
16-bit block	192.168.0.0 - 192.168.255.255	65,536

Selain yang berada di table IP Address range tersebut maka ia adalah IP Public.

20. You have a router with configuration

- Public IP :202.168.125.45/24
- Default gateway:202.168.125.1
- DNS server: 248.115.148.136, 248.115.148.137
- Local IP: 192.168.2.1/24

Mark the correct configuration on client PC to access to the Internet

- IP:192.168.1.223/24 gateway:248.115.148.136
- IP:192.168.2.253/24 gateway:202.168.0.1
- IP:192.168.2.2/24 gateway:202.168.125.45
- IP:192.168.2.115/24 gateway: 192.168.2.1
- IP:192.168.0.1/24 gateway:192.168.2.1

Pembahasan :

Fokuskan pada Local IP Saja dan cari yang satu network dan gateway-nya merupakan Local IP tersebut.

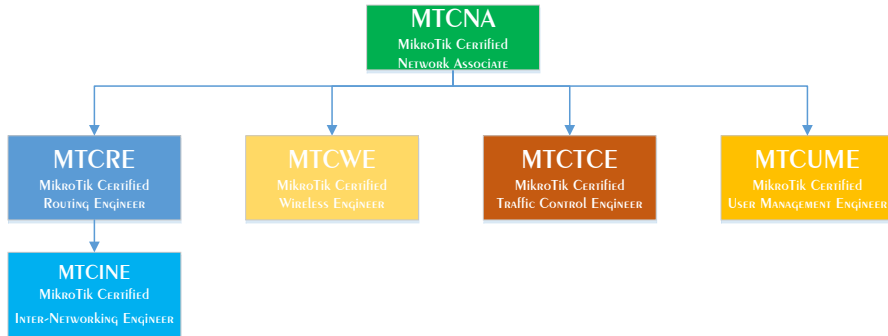
Jawabannya adalah Point ke 3.

Untuk soal Real MTCNA akan saya bahas diakhir modul. Setelah mereview soal MTCNA di website resmi mikrotik, sekarang tulis skor awalmu dibawah ini :

Example Test	Real Test Target

About MikroTik

Mikrotik Certification Program



Masa berlaku sertifikat selama 3 tahun, dan tidak perlu mengulang pada sertifikat sebelumnya boleh lanjut ke level selanjutnya.

MikroTik History



MikroTik adalah software dan hardware berkantor pusat di Latvia(Rusia), didirikan pada tahun 1996 dengan founder John Arnis Reikstins. yang memiliki tujuan untuk menjadikan teknologi internet lebih cepat, lebih luas, terjangkau, dan handal. Sesuai mottonya "Routing The World". Berbasis Linux dan MS DOS + Wirelles Combination Aeronet 2Mbps di Moldova.

Jenis Mikrotik

a) Mikrotik Router OS

- Mengubah PC menjadi router mikrotik yang handal
- Berbasis Linux
- Diinstall sebagai system operasi
- Diinstall pada power PC

b) Mikrotik Routerboard

- Build in hardware yang menggunakan system operasi Mikrotik RouterOS
- Tersedia mulai dari low-end sampai high end router

Fitur Mikrotik

a) Support driver (Ethernet,Wirelles Card, V35, ISDN, USB Mass Storage, USB 3G Modem, E1/T1.

b) Router Plus

- User Management (DHCP,Hotspot,Radius, dll)
- Routing (RIP,RIPng,OSPF,OSPFv3,BGP)
- Firewall (Fully Customized,Linux Based)
- QoS/Bandwith Limiter (Fully Customized,Linux Based)
- Tunnel (EolP, PPTP, L2TP, PPOE, SSTP, OpenVPN)
- Real Time Tools (Torch,Watchdog,MAC-Ping,MRTG,Sniffer)

Routerboard Type

RB	9	5	1
Routerboard	Seri/Kelas Router	N Port Ethernet	N Wireless

Kode lain dibelakang tipe :

Kode	Keterangan
U	Port USB Support
A	Advanced, diatas license level 4
H	High Performance Proessor
R	Embedded Wireless Card
G	Gigabit Ethernet Support
2nD	Dual Channel

Arsitektur Routerboard

Dibedakan berdasarkan jenis dan kinerja processor (arsitektur)

Jenis OS	Support for
MIPSBE	CRS, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx
SMIPS	hAP lite
TILE	CCR
PPC	RB3xx, RB600, RB8xx, RB1xxx
ARM	RB3011
X86	RB230, X86
MIPSLE	RB1xx, RB5xx, Crossroads
Images	Cloud Hosted Router Support (vmdk, vhdx, vdi, img)
SwitchOS	Switches

Microprocessor without Interlocked Pipeline Stages Big Endian, jenis processor yang dikembangkan oleh MIPS Computer Systems, Inc. Ada 2 jenis MIPS yaitu (MIPS – Little Endian) dan MIPSBE (MIPS – Big Endian), endian / endianness adalah istilah yang menggambarkan urutan byte yang disimpan dalam memori computer, misal MikroTik > kiTorkiM.

Mikrotik vs Cisco

FAQ : http://wiki.mikrotik.com/wiki/Manual:RouterOS_FAQ

How does this software compare to using a Cisco router?

You can do almost **everything** that a proprietary router does at a fraction of the **cost** of such a router and have **flexibility in upgrading, ease of management and maintenance.**

First time accessing the router

Overview

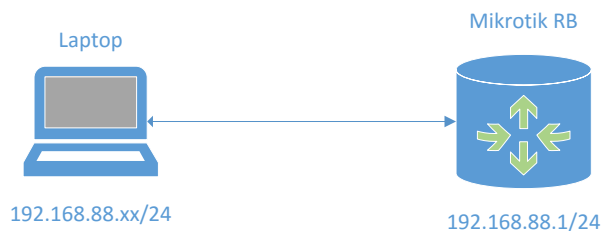
Setelah anda berhasil menginstall routerOS atau menghidupkan routerboard pertama kali, ada banyak cara untuk mengaksesnya, diantaranya adalah :

Access Via	Connection	CLI	GUI	Need IP
Keyboard	Direct via PC	Yes		
Serial Console	Serial Cable Connector	Yes		
Winbox	Using Windows OS	Yes	Yes	
API	Socket Programming			Yes
Web (HTTP)	Layer 3		Yes	Yes
Telnet & SSH	Layer 3	Yes		Yes
FTP	Layer 3	Yes		Yes
MAC-Telnet	Layer 2	Yes		

RB baru / setelah direset default memiliki konfigurasi default :

- IP Address 192.168.88.1/24
- Username "admin" password blank

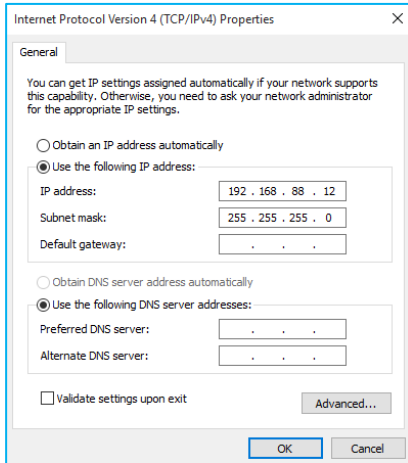
Untuk meremote RB, hubungkan kabel UTP antara Laptop/PC dan RB melalui Ethernet, kemudian set IP Laptop di set 192.168.88.X/24.



Konfigurasi tambahan dapat diatur berdasarkan model dari RB. Hal ini didokumentasikan dalam Wiki Mikrotik :

http://wiki.mikrotik.com/wiki/Manual:Default_Configurations

Connect to Mikrotik RB



Set IP Address Computer :

IP Address : 192.168.88.X

Netmask : 255.255.255.0

Uji koneksi dengan cara Ping ke IP Mikrotik RB

> ping 192.168.88.1

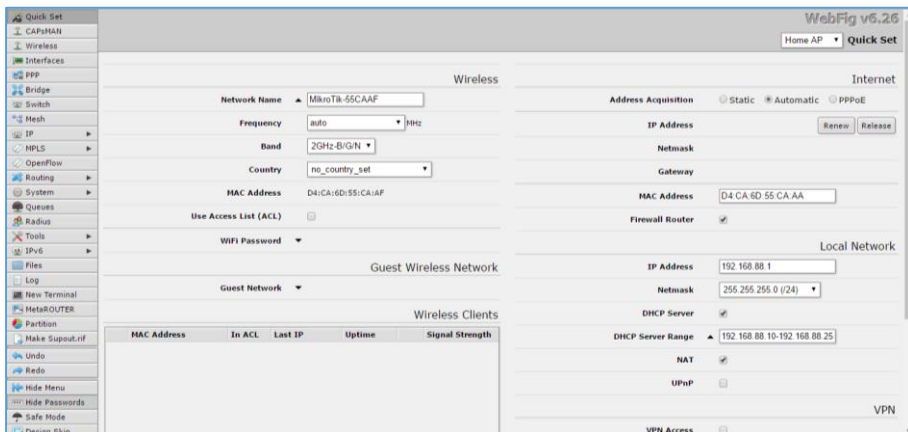
```
C:\Users\andri>ping 192.168.88.1

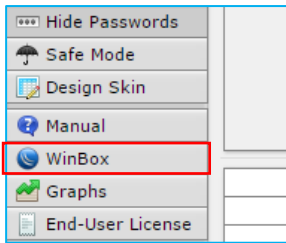
Pinging 192.168.88.1 with 32 bytes of data:
Reply from 192.168.88.1: bytes=32 time=2ms TTL=64
Reply from 192.168.88.1: bytes=32 time=3ms TTL=64
Reply from 192.168.88.1: bytes=32 time=1ms TTL=64
Reply from 192.168.88.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

1. Webfig

Sejak versi 5.0 webfig GUI mirip winbox. Buka URL RB melalui web browser (<http://192.168.88.1>). Webfig berjalan menggunakan service webserver/http dan menggunakan port 80, dengan fitur ini anda bisa mengakses Webfig menggunakan Web Browser (Seperti Chrome, Mozilla, Opera,dls).





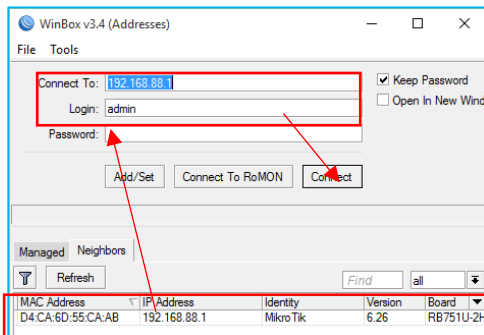
Secara default, untuk pertama kali kita akan langsung dihadapkan dengan dashboard webfig karena autentikasinya belum diset. Anda bisa download Winbox melalui halaman webfig tersebut.

2. Winbox

Adalah sebuah tools konfigurasi yang dapat mengakses router menggunakan IP atau MAC Address.

Bagaimana mendapatkan winbox :

- Web Mikrotik <http://mikrotik.com/download>
- Web service mikrotik yang dapat diakses menggunakan IP atau Domain router
- Copy dari penyimpanan



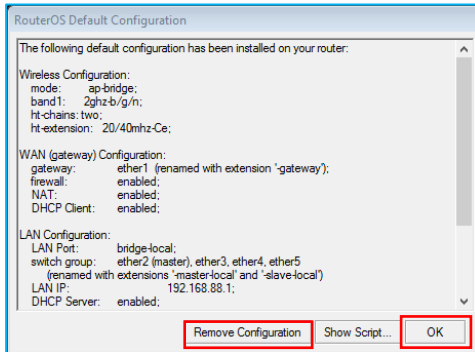
Cara akses menggunakan winbox.

Neighbors

- 1) Klik menu neighborhood atau tanda (...) jika menggunakan winbox versi lama.
- 2) Jika MikroTik terhubung dengan benar maka akan teridentifikasi pada menu neighbors tersebut.
- 3) Klik pada kolom MAC atau IP Address untuk mengisi field connect to secara otomatis. Jika menggunakan MAC Address tidak perlu mengkonfigurasi IP Address, tetapi jika menggunakan IP Address anda perlu mengkonfigurasi IP PC anda supaya bisa terhubung.

Manual

- 1) Isi field secara manual baik menggunakan IP / MAC Address. Rekomendasi IP Address.
- 2) Setelah form diisi semua, lanjutkan dengan menekan tombol connect.

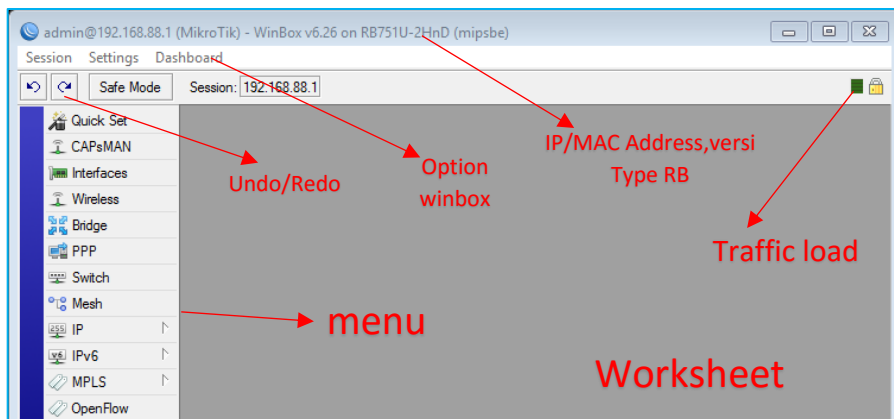


Winbox akan secara otomatis mendownload plugin dari router untuk menyesuaikan versi routerOS yang digunakan. Winbox berjalan menggunakan port 8291.

Setelah itu ada notifikasi mengenai default configuration script mikrotik, jika ingin mengabaikan pilih OK, atau jika ingin menghapus default config nya bisa pilih remove configuration (Blank Configuration).

Interface Winbox v.6.26

WinBox adalah tools yang paling bagus yang digunakan untuk mengkonfigurasi MikroTik, karena terdapat fitur CLI jug ajiaka anda merasa bosan dengan GUI.



Tips

Jika winbox mengalami masalah / tidak bisa menjalin koneksi ke router ada beberapa tips berikut :

- Pastikan PC terkoneksi langsung ke router menggunakan Ethernet Cable atau Wifi jika tersedia. Atau setidaknya dalam 1 switch yang sama.
- Jika menggunakan MAC untuk koneksi yang bekerja pada layer 2 sangat mungkin terjadi tanpa menggunakan IP Address, tetapi tidak stabil karena bersifat broadcast address. Tidak disarankan untuk menggunakan ini, hanya direkomendasikan ketika awal awal konfigurasi karena jika menggunakan IP ketika mengubah konfigurasi IP Address maka RB akan otomatis Disconnected.
- Jika anda menggunakan VBox atau VMware pastikan dinonaktifkan terlebih dahulu, karena dapat mengganggu koneksi ke router menggunakan winbox.

Terminal Configuration

Dalam beberapa kondisi tertentu, konfigurasi melalui GUI tidak dapat dilakukan karena :

Bandwith Limited, Need running script, remote via ...x console, dan lain sebagainya. Remote dan configuration via terminal bisa dilakukan dengan cara :

Service	Port	Security
Telnet (Telecommunication Network)	23	Non Secure
SSH (Secure Shell)	22	Secure
Serial console	Serial Cable	

3. Telnet (Telecommunication Network)

Anda bisa menggunakan CMD/Terminal/putty dan lainnya untuk menjalankan service telnet maupun ssh. Misalkan disini saya menggunakan CMD untuk menjalankan telnet, maka :

Buka CMD kemudian ketikkan perintah >telnet 192.168.88.1, jika fitur telnet belum terinstall silahkan dienable terlebih dahulu fitur telnet di windows. Telnet sendiri menggunakan port default : 23

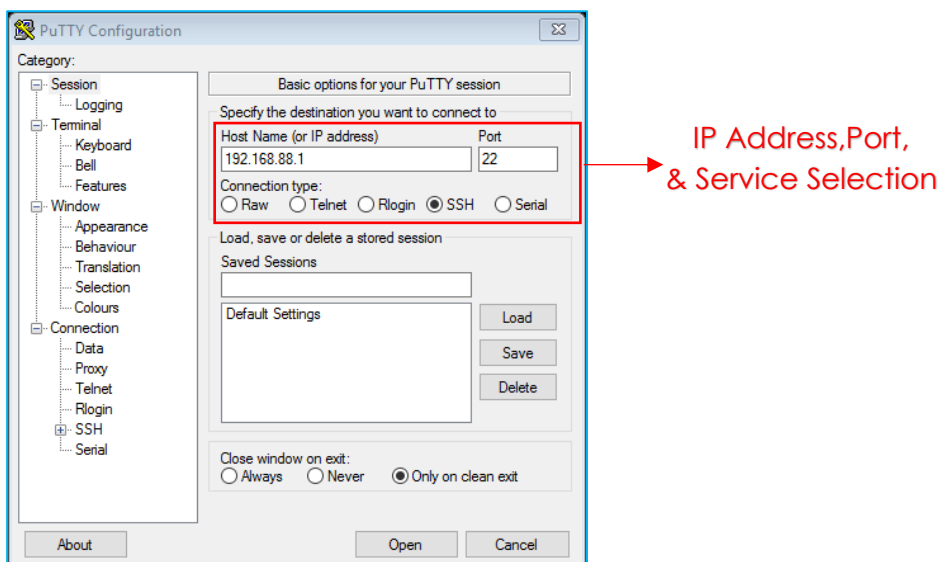
```
C:\> Telnet 192.168.88.1

MikroTik v6.33.3 (stable)
Login:
```

Masukan username : admin, password : "blank". Dan MikroTik siap untuk di configure via CLI.

4. SSH (Secure Shell)

Gunakan aplikasi Telnet/SSH seperti MsDOS Prompt, putty, winSCP, dan sebagainya untuk meremote mikrotik. Port defaultnya adalah 22 dan lebih aman dibanding telnet.



5. Serial Console

Digunakan apabila kita salah mengkonfigurasi seperti mendisable semua port di RB, dan Netinstall. Dibutuhkan juga Cable DB-9 / Converter USB to DB-9, Program Hyper Terminal.

Buka terminal atau putty dan sebagainya dengan parameter berikut (berlaku untuk semua jenis RB kecuali 230) :

```
115200bit/s, 8 data bits, 1 stop bit, no parity, flow  
control=none by default.
```

Jika menggunakan RB 230, gunakan parameter berikut :

```
9600bit/s, 8 data bits, 1 stop bit, no parity, hardware (RTS/CTS)  
flow control by default.
```

Jika parameter benar maka akan tampil login formnya via CLI.

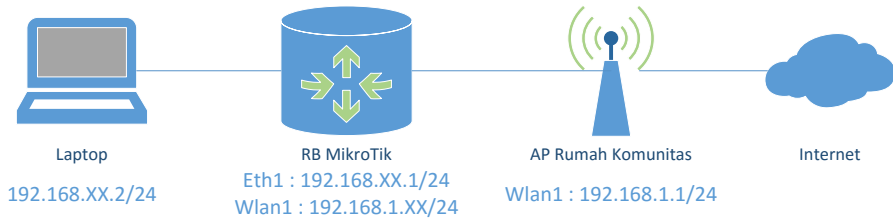
Initial Configuration

Topology

Resource Internet : Access Point Rumah Komunitas

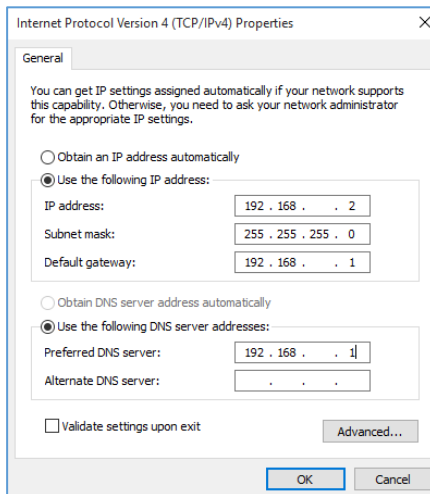
Router : Mikrotik

IP Publik : Dari AP Rumah Komunitas (DHCP)



Langkah Kerja

Setting IP Laptop/PC



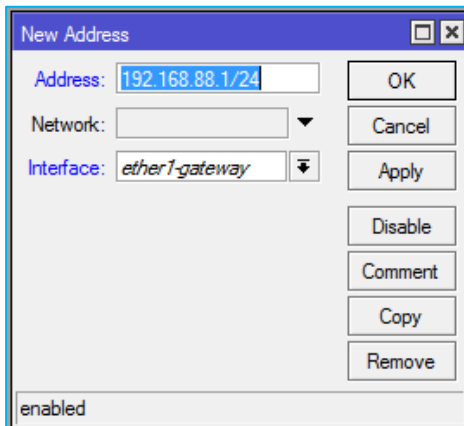
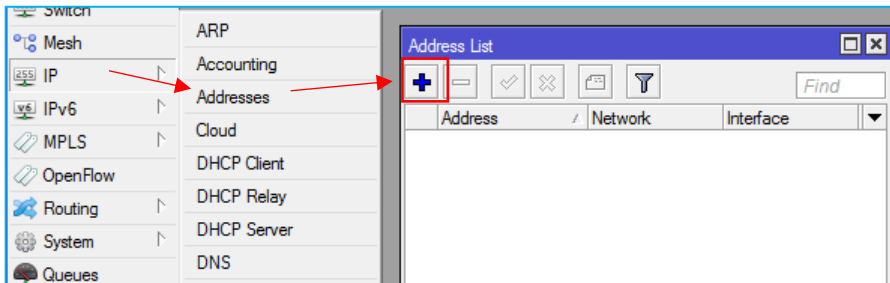
a) Setting IP Laptop 1 range dengan Mikrotik RB interface ether1, misalkan 192.168.xx.2 netmask 255.255.255.0, xx diganti dengan no.peserta masing masing.

b) Setting gateway dan DNS pada laptop (IP Mikrotik RB, 192.168.xx.1), hal ini dimaksudkan agar laptop mereferensikan bahwa Mikrotik adalah jembatan untuk ke jaringan yang lain, seperti ke Internet dan routing ke network lain.

Setting Interface ether1 Mikrotik

c) Setting IP Address pada Ether1 Mikrotik dengan 192.168.XX.1/24, namun bisa juga menggunakan IP Address yang lain dengan syarat 1 range dengan IP Laptop.

Buka menu *IP > Address > Add*



d) Kemudian isikan IP Address dan Subnetmask yang menggunakan prefix, pilih interface yang terhubung ke laptop, lalu *apply > ok*. Misalkan 192.168.88.1 (tetapi sesuaikan dengan no.peserta).

e) Jika ingin menambahkan comment (untuk mempermudah mengingat jalur dari interface) bisa klik comment pada konfigurasi New Address diatas, lalu isikan commentnya > Ok.

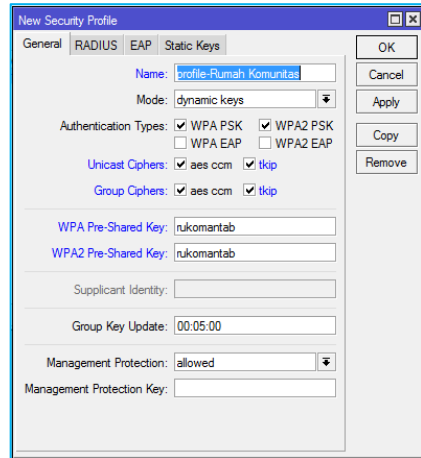
Setting Security Profile

- f) Masuk ke menu *wireless > tab security profile > general*. Setting dengan option sebagai berikut.

Name: *profile-Rumah Komunitas*

Password : *rukomantab*

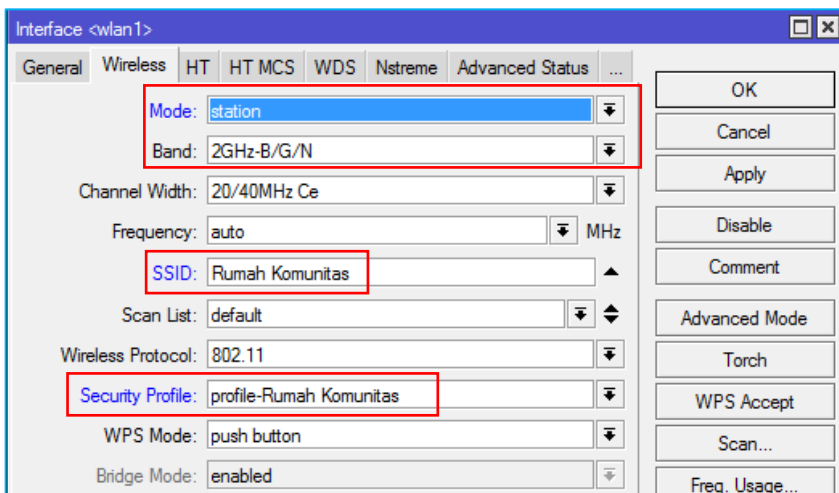
Dan option lainnya seperti gambar disamping.



Settingan diatas disesuaikan dengan password Access Point yang akan digunakan sebagai access internet.

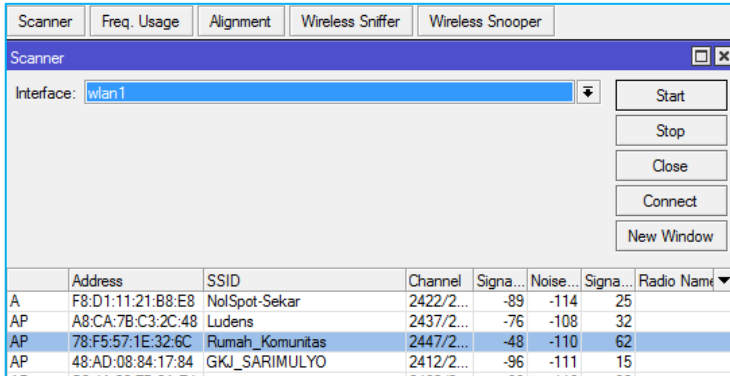
Setting WLAN Mode

- g) WLAN Mode : Station (Untuk menerima Koneksi dari AP/Sebagai Client), Band = 2GHz-B/G/N & SSID = Rumah Komunitas (Optional, bisa disesuaikan dengan nama SSID AP), Security Profile : *profile-Rumah Komunitas* (sesuai dengan profile yang sudah dibuat).



Scanning

Tools untuk mempermudah melakukan Scanning dan Connection ke AP. *Scan > Connect*, namun sebelumnya perlu disesuaikan band dan security profilnya.



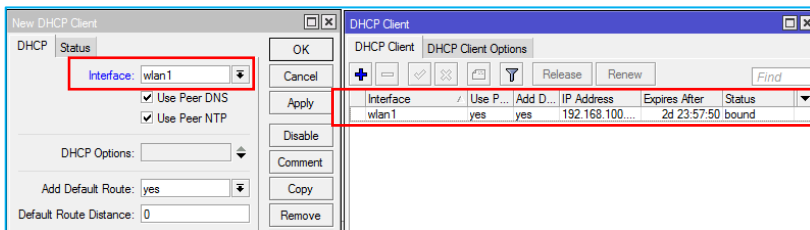
The screenshot shows the 'Scanner' application window with the 'Interface' set to 'wan1'. The main area displays a table of detected wireless networks. The table has columns for Address, SSID, Channel, Signal strength, Noise, Signal-to-Noise ratio, and Radio Name. The detected networks are:

	Address	SSID	Channel	Signa...	Noise...	Signa...	Radio Name
A	F8:D1:11:21:B8:E8	NolSpot-Sekar	2422/2...	-89	-114	25	
AP	A8:CA:7B:C3:2C:48	Ludens	2437/2...	-76	-108	32	
AP	78:F5:57:1E:32:6C	Rumah_Komunitas	2447/2...	-48	-110	62	
AP	48:AD:08:84:17:84	GKJ_SARIMULYO	2412/2...	-96	-111	15	

DHCP Client

Untuk dapat terkoneksi, silahkan set IP DHCP Client untuk mendapatkan IP Address yang sudah disediakan oleh Access Point dengan layanan DHCP Servernya.

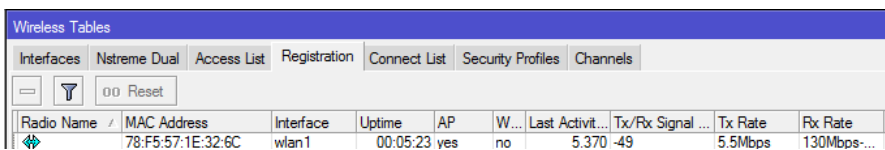
Masuk ke menu IP > DHCP Client > Set Interface = WLAN1 > Apply



The screenshot shows the 'New DHCP Client' dialog box with the 'Interface' dropdown menu set to 'wan1'. The 'DHCP Client' tab is active, showing a table of DHCP clients. The table has columns for Interface, Use Peer DNS, Add D..., IP Address, Expires After, and Status. The table contains one entry:

Interface	Use P...	Add D...	IP Address	Expires After	Status
wan1	yes	yes	192.168.100...	2d 23:57:50	bound

h) Indikasi wireless sudah terkoneksi adalah munculnya huruf "R" (Running) & MAC Address AP pada wireless yang digunakan di kolom *Registration*.



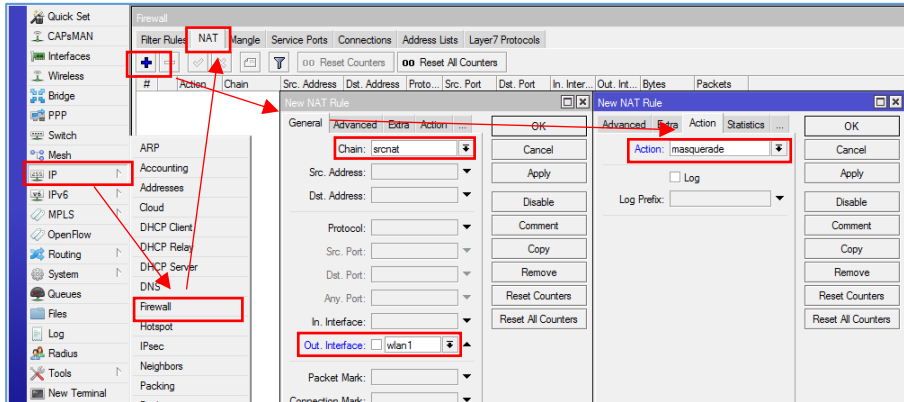
The screenshot shows the 'Wireless Tables' window with the 'Registration' tab selected. The table displays the registration status of the wlan1 interface. The table has columns for Radio Name, MAC Address, Interface, Uptime, AP, W..., Last Activit..., Tx/Rx Signal..., Tx Rate, and Rx Rate. The table contains one entry:

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	78:F5:57:1E:32:6C	wan1	00:05:23	yes	no	5.370	-49	5.5Mbps	130Mbps...

Setting NAT (Network Address Translation)

Fungsi : Agar IP Address Private dapat digunakan untuk Internet Connection dengan mentranslasikan ke IP Public.

Menu : IP > Firewall > NAT



Keterangan

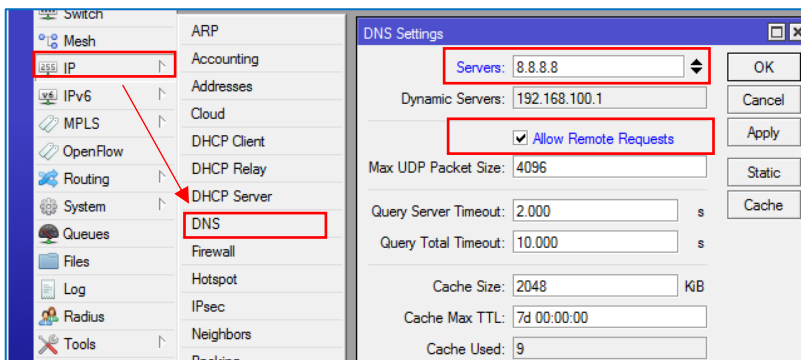
Chain : srcnat

Out Interface: wlan1 (sesuai jalur keluar ke internet)

Action : masquerade

DNS Setting

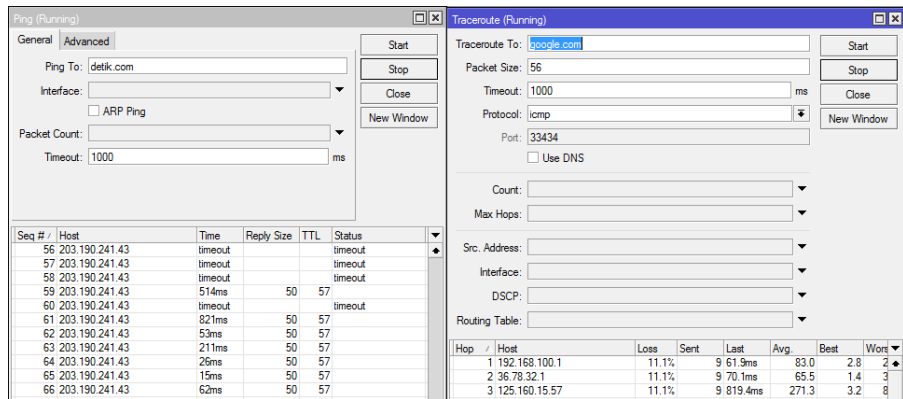
Fungsi : Untuk menerjemahkan IP Address ke Domain, DNS Server yang biasa digunakan adalah milik google yang mempunyai address 8.8.8.8, sedangkan jika AP sudah memberi service DHCP Server, maka akan secara otomatis terisi DNS Server AP.



allow-remote-requests=yes akan menjadikan Router Mikrotik anda sebagai DNS Server juga. Sehingga nantinya konfigurasi DNS pada komputer user cukup diarahkan ke Router Mikrotik, dan tidak lagi diarahkan ke DNS Server milik Google ataupun ISP, atau lainnya. Hal ini dapat menghemat penggunaan Bandwidth karena pertanyaan-pertanyaan DNS hanya akan diberikan ke Router Mikrotik anda.

Test PING & Traceroute

Destination : Internet misalkan domain (yahoo.com atau google.com).



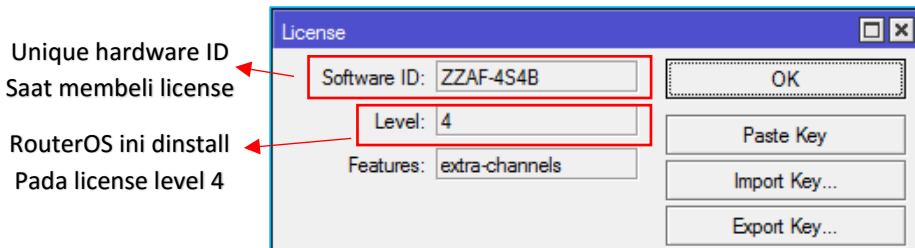
Troubleshoot

1. Router tidak bisa ping ke luar? *Cek apakah wireless sudah terkoneksi, cek dhcp client apakah sudah running dan mendapatkan IP (Bound)*
2. Router bisa ping ke IP Public tapi tidak bisa ping domain ? *Check IP DNS (allow remote request)*
3. Komputer tidak dapat ping ke router ? *cek IP Address pastikan sudah sesuai baik subnet (/24) maupun rangenya*
4. Komputer bisa ping keluar tapi tidak bisa ping domain? *Check IP DNS di PC*

License Mikrotik

- Fitur-fitur RouterOS ditentukan oleh level lisensi yang melekat pada perangkat.
- Level dari lisensi juga menentukan batasan upgrade packet.
- Lisensi melekat pada storage/media penyimpanan (ex. Hardisk, NAND, USB, Compact Flash).
- Bila media penyimpanan diformat dengan non MikroTik, maka lisensi akan hilang

Untuk mengecek level license mikrotik buka menu *System > License* pada winbox.



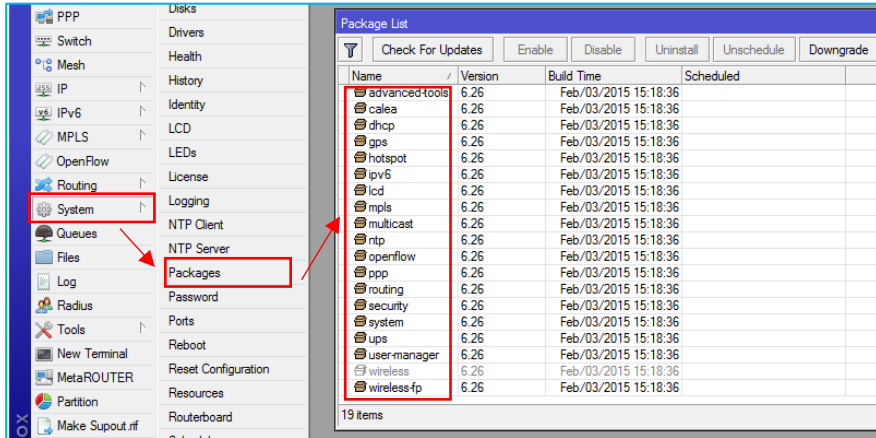
untuk pengetahuan, macam macam level license mikrotik :

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

Versi Mikrotik

Selain license, fitur juga ditentukan oleh versi mikrotik yang diinstall. Pada routerOS fitur yang dimiliki dan disupport, bisa dilihat pada paket apa saja yang diinstall.

Masuk ke menu System > Package



Dapat diidentifikasi bahwa versi yang digunakan adalah 6.26 dan mempunyai banyak fitur karena paket yang diinstall tersebut.

Package & Features

Berikut adalah table fitur dalam setiap paket yang disediakan oleh Mikrotik

Package	Features
advanced-tools (mipsle, mipsbe, ppc, x86)	advanced ping tools, netwatch, ip-scan, sms tool, wake-on-LAN
calea (mipsle, mipsbe, ppc, x86)	data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (mipsle, mipsbe, ppc, x86)	Dynamic Host Control Protocol client and server
gps (mipsle, mipsbe, ppc, x86)	Global Positioning System devices support
hotspot (mipsle, mipsbe, ppc, x86)	HotSpot captive portal server for user management
ipv6 (mipsle, mipsbe, ppc, x86)	IPv6 addressing support
mpls (mipsle, mipsbe, ppc, x86)	Multi Protocol Labels Switching support
multicast (mipsle, mipsbe, ppc, x86)	Protocol Independent Multicast - Sparse Mode; Internet Group Managing Protocol - Proxy
ntp (mipsle, mipsbe, ppc, x86)	Network protocol server, also includes simplistic client. NTP client is also built into the system package and functions well without this package installed.
openflow (mipsle, mipsbe, ppc, x86)	Enables OpenFlow support
ppp (mipsle, mipsbe, ppc, x86)	MPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
routerboard (mipsle, mipsbe, ppc, x86)	accessing and managing RouterBOOT, RouterBOARD specific information.
routing (mipsle, mipsbe, ppc, x86)	dynamic routing protocols like RIP, BGP, OSPF and routing utilities like BFD, filters for routes.
security (mipsle, mipsbe, ppc, x86)	IPSEC, SSH, Secure WinBox
system (mipsle, mipsbe, ppc, x86)	basic router features like static routing, ip addresses, sNTP telnet, API, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EuiP, iPIP, bridging, VLAN, VRRP etc.). Also, for RouterBOARD platform - MetaROUTER Virtualization
ups (mipsle, mipsbe, ppc, x86)	APC ups management interface
user-manager (mipsle, mipsbe, ppc, x86)	MikroTik User Manager server for controlling Hotspot and other service users.
wireless (mipsle, mipsbe, ppc, x86)	wireless interface support. Sometimes sub-types are released, for example wireless-fp introduced FastPath support, wireless-cm2 introduced CAPsMAN v2 and wireless-rep introduced Repeater mode. These packages are occasionally released separately, before the new features get merged into the main wireless package.

arlan (x86)	legacy Aironet Arlan support
isdn (x86)	ISDN modem support
lcd (x86)	LCD panel support for serial/parallel port devices. Not needed for RouterBOARD LCD panels.
radiolan (x86)	RadioLan cards support
synchronous (x86)	FarSync support
xen (discontinued x86)	XEN Virtualization
kvm (x86)	KVM Virtualization
routeros-mipsle (mipsle)	combined package for mipsle (RB100, RB500) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-mipsbe (mipsbe)	combined package for mipsbe (RB400) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-powerpc (ppc)	combined package for powerpc (RB300, RB600, RB1000) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)
routeros-x86 (x86)	combined package for x86 (Intel/AMD PC, RB230) (includes system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing)

Paket dan fitur yang cukup banyak tentunya bisa memakan resource CPU jika semua diaktifkan dan penggunaan tidak sesuai dilapangan. Pada intinya gunakan fitur sesuai dengan kebutuhan dilapangan saja.

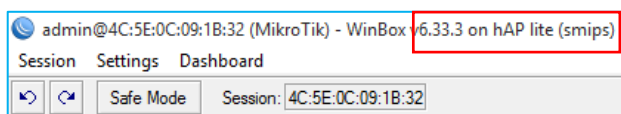
Upgrade/Downgrade Paket

- Upgrade diperlukan jika ingin memperbaiki fitur dan bug, sedangkan downgrade dilakukan apabila hardware kurang support terhadap versi baru atau bahkan bug pada versi latest.
- Upgrade paket harus memperhatikan aturan level dan lisensi yang berlaku, kompatibilitas terhadap jenis arsitektur hardware. Silahkan bisa dicrosscheck di <http://mikrotik.com/download.html>

Langkah Kerja

Manual Upgrade

- Cek versi mikrotik, bisa dicek ketika masuk winbox pada bagian taskbar. Dan upgrade lah RB ke versi yang terbaru. Misalkan disini saya menggunakan MikroTik RB 941-2ND (hAP-Lite). Paket terbaru bisa di cek disitus resmi mikrotik.



- Pilih sesuai dengan series dari RB anda. Download dan simpan di Laptop.

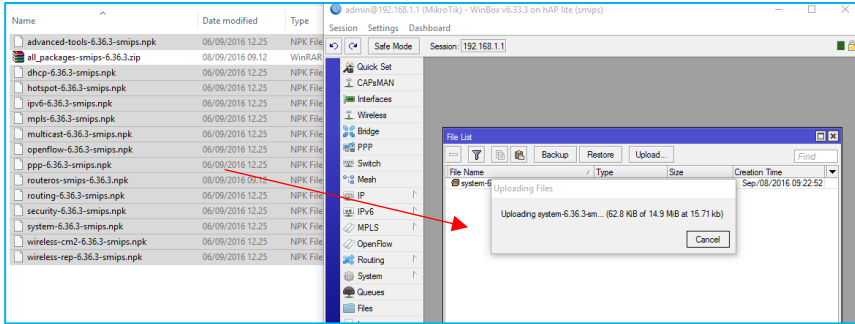
	6.34.6 (Bugfix only)	6.36.3 (Current)	5.26 (Legacy)	6.37rc32 (Release candidate)
MIPSBE	CRS, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, mAP, RB4xx, cAP, HEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package	↓	↓	↓	↓
Extra packages	↓	↓	↓	↓
SMIPS	hAP lite			
Main package	↓	↓	-	↓
Extra packages	↓	↓	-	↓

Misalkan disini saya memilih current, yang lebih stabil dan terbaru. Terdapat 2 package yakni main (Untuk mensupport extra packages) dan extra (berisi paket seperti hotspot, dhcp, routing, dsb), download keduanya.

- Ekstrak extra package terlebih dahulu

advanced-tools-6.36.3-smips.npk	06/09/2016 12.25	NPK File	65 KB
all_packages-smips-6.36.3.zip	08/09/2016 09.12	WinRAR ZIP archive	7.980 KB
dhcp-6.36.3-smips.npk	06/09/2016 12.25	NPK File	137 KB
hotspot-6.36.3-smips.npk	06/09/2016 12.25	NPK File	145 KB
ipv6-6.36.3-smips.npk	06/09/2016 12.25	NPK File	189 KB
mpls-6.36.3-smips.npk	06/09/2016 12.25	NPK File	53 KB
multicast-6.36.3-smips.npk	06/09/2016 12.25	NPK File	37 KB
openflow-6.36.3-smips.npk	06/09/2016 12.25	NPK File	49 KB
ppp-6.36.3-smips.npk	06/09/2016 12.25	NPK File	249 KB
routeros-smips-6.36.3.npk	08/09/2016 09.12	NPK File	7.128 KB
routing-6.36.3-smips.npk	06/09/2016 12.25	NPK File	69 KB
security-6.36.3-smips.npk	06/09/2016 12.25	NPK File	285 KB
system-6.36.3-smips.npk	06/09/2016 12.25	NPK File	5.130 KB
wireless-cm2-6.36.3-smips.npk	06/09/2016 12.25	NPK File	853 KB
wireless-rep-6.36.3-smips.npk	06/09/2016 12.25	NPK File	881 KB

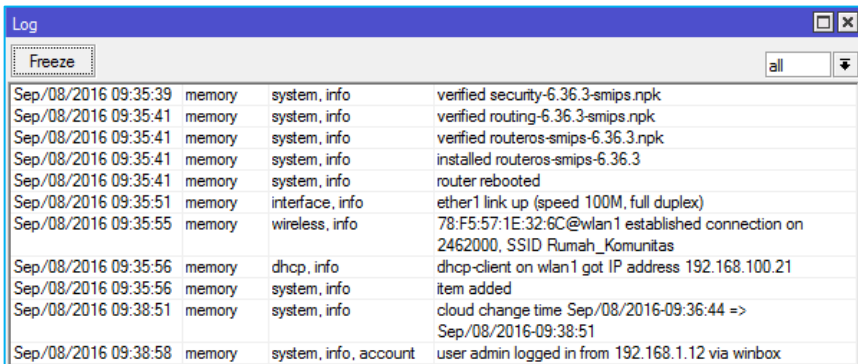
- Upload kedalam file list Mikrotik melalui winbox atau filezilla (ftp) dengan cara drag & drop. Tips, lebih baik login menggunakan IP Address, karena jika menggunakan MAC Address kurang stabil koneksinya.



- Kemudian reboot RB dengan langkah `system > reboot`
- Setelah router kembali ON, maka defaultnya di neighbors versi mikrotik akan terbaca

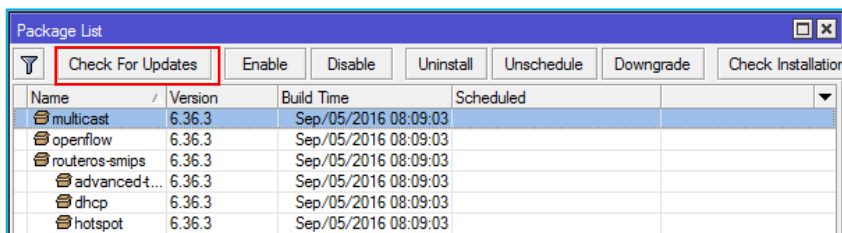
MAC Address	IP Address	Identity	Version
4C:5E:0C:09:1B:31	192.168.1.1	Mikro Tik	6.36.3 (st...

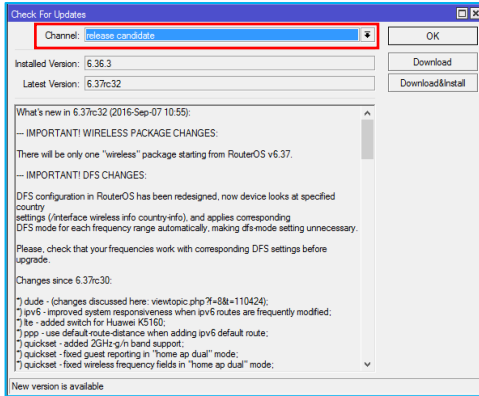
- Cek kembali pada `system > package`, apakah paket paket yang baru berhasil diinstall. Apabila belum cek error message di menu Log.



Upgrade Otomatis (RB must have Internet Access)

- Masuk ke menu `package > Check for Updates`





Pilih versi Upgrade seperti bug fix only, current, dan sebagainya (sama dengan ketika upgrade manual). Perbedaannya adalah kita tidak bisa mengcustom versi paketyang kita inginkan

(yang ada hanya yang terbaru). Jika ingin downgrade otomatis, maka akan kembali ke versi sebelumnya. Pilih download (download saja) atau download & install (selesai download langsung melakukan installasi).

Enable/Disable Paket

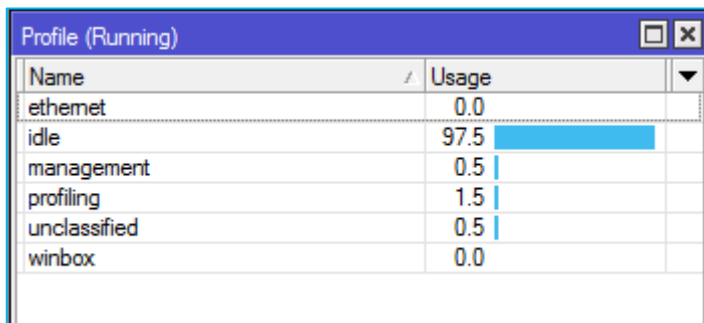
Fitur ini Dibutuhkan jika terdapat paket yang belum terpakai (dapat mengurangi penggunaan resource) maupun akan dipakai. Misalkan IPv6, caranya masuk ke menu System > Packet > pilih paket > Disable / Uninstall.

Package List				
<input type="button" value="Check For Updates"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Uninstall"/> <input type="button" value="Unschedule"/> <input type="button" value="Downgrade"/> <input type="button" value="Check Installation"/>				
Name	Version	Build Time	Scheduled	
multicast	6.36.3	Sep/05/2016 08:09:03		
openflow	6.36.3	Sep/05/2016 08:09:03		
routeros-smips	6.36.3	Sep/05/2016 08:09:03		
advanced-t...	6.36.3	Sep/05/2016 08:09:03		
dhcp	6.36.3	Sep/05/2016 08:09:03		
hotspot	6.36.3	Sep/05/2016 08:09:03		
ipv6	6.36.3	Sep/05/2016 08:09:03	scheduled for disable	
mpls	6.36.3	Sep/05/2016 08:09:03		
ppp	6.36.3	Sep/05/2016 08:09:03		
routing	6.36.3	Sep/05/2016 08:09:03		
security	6.36.3	Sep/05/2016 08:09:03		
system	6.36.3	Sep/05/2016 08:09:03		
wireless-cm2	6.36.3	Sep/05/2016 08:09:03		
routing	6.36.3	Sep/05/2016 08:09:03		
security	6.36.3	Sep/05/2016 08:09:03		
wireless-rep	6.36.3	Sep/05/2016 08:09:03		

Maka akan diberi keterangan Scheduled for disable atau uninstall. Langkah terakhir adalah restart router agar perubahan yang di jadwalkan untuk disable atau uninstall berhasil.

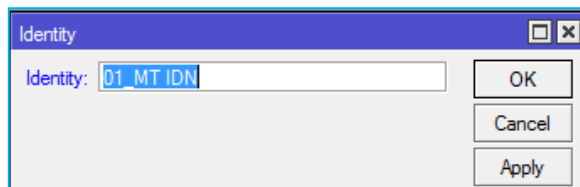
User & Router Management

Mikrotik Profile, digunakan untuk melihat resource pemakaian CPU RB anda, cek Tools > Profile.



Name	Usage
ethernet	0.0
idle	97.5
management	0.5
profiling	1.5
unclassified	0.5
winbox	0.0

Router Identity, berfungsi untuk memberi nama kepada RB, agar kedepannya tidak bingung karena banyaknya router yang saling terhubung. Sehingga dapat dikenali dengan baik antara router 1 dengan yang lain. Masuk ke menu *System > Identity*. Ganti nama router menjadi xx_nama anda. (xx = no.peserta)



Identity: 01_MT IDN

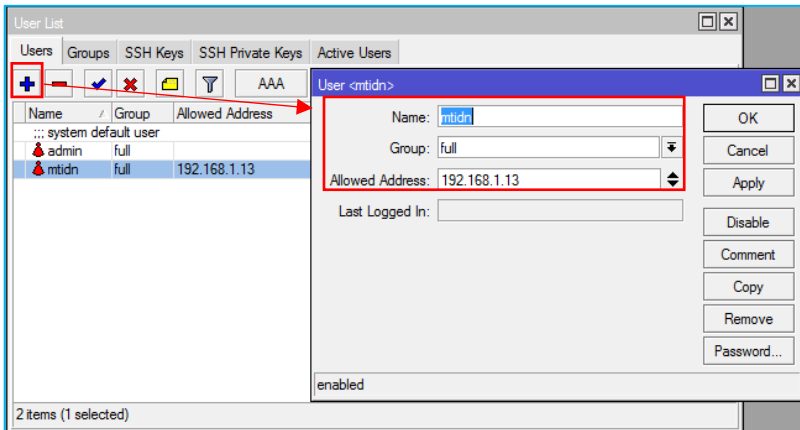
OK
Cancel
Apply

Login Account, mikrotik RB jika tidak dirubah login accountnya akan sangat rentan terhadap pembobolan. Sangat mudah untuk mengaksesnya. Maka dari itu coba rubah account login anda dengan langkah langkah sebagai berikut.

Menu : System > User

Only access from your PC

Buatlah dengan username : nama_anda, only access from IP : 192.168.1.13, group : full



Untuk alasan keamanan silahkan beri password untuk admin maupun user yang baru saja dibuat.

Cobalah login menggunakan user baru dan admin. Dan apa yang terjadi ?

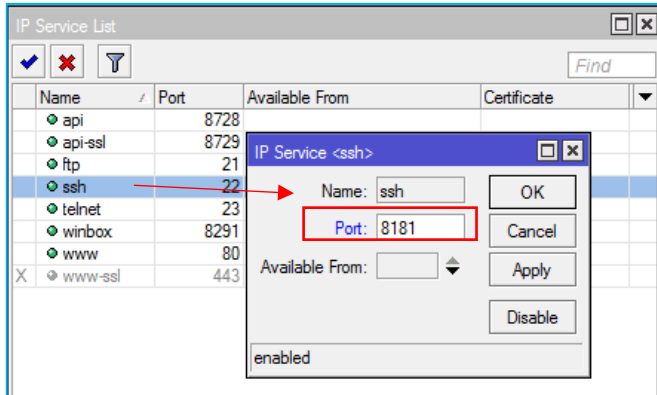
Pada contoh diatas username admin, bisa digunakan dari mana saja yang terhubung dengan RB. Tetapi untuk username baru hanya bisa diakses dari computer yang menggunakan IP tertentu.

Cobalah membuat RB tidak bisa diakses pada PC tertentu, dan selain PC tersebut RB bisa mengaksesnya !

Port & Services, service yang dimiliki mikrotik diantaranya adalah SSH dengan port 22. Gantilah port default tersebut misalkan menjadi port 8181. Perubahan port ini akan mengecoh

seseorang yang tidak berhak mengakses kedalam RB kita dalam aktivitas scanning dan penetration testing.

Menu > IP > Services



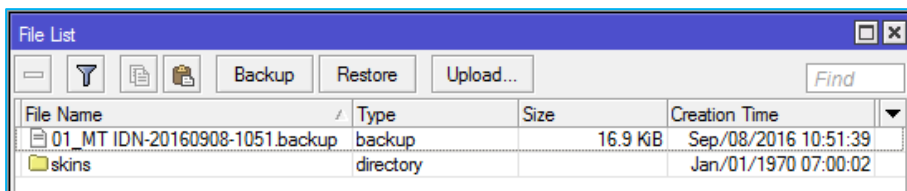
Backup, Export & Restore

Backup bersifat menyeluruh, sedangkan export hanya sebagian konfigurasi saja yang dibackup. Keduanya dapat dikombinasikan dengan tools netwatch, scheduler, dan email untuk keperluan automatic regularly backup dan mengirimkan ke email tertentu.

Backup

Via Winbox, masuk ke menu file > backup

Format default : [RB_ID]-[date][month][year][hour][minute]



Selain format default, kita juga dapat memberi nama file sesuai dengan yang kita inginkan. Bisa dilakukan di Winbox ataupun terminal.

Via Terminal, Command : system backup save name=[nama_file]

```
[admin@01_MT IDN] > system backup save name=backup_tut01
Saving system configuration
Configuration backup saved
[admin@01_MT IDN] > file print
# NAME                                TYPE                                SIZE CREATION-TIME
0 01_MT IDN-20160908-1...             backup                              16.9KiB sep/08/2016 10:51:39
1 skins                                directory                            jan/01/1970 07:00:02
2 01_MT IDN-20160908-1...             backup                              16.9KiB sep/08/2016 10:54:06
3 backup_tut01.backup                 backup                              16.9KiB sep/08/2016 10:55:59
[admin@01_MT IDN] > █
```

File backup dapat disimpan di PC dengan cara drag & drop dari winbox ke PC, atau menggunakan FTP.

Export, export konfigurasi IP Address anda menggunakan perintah export via terminal.

Export semua config : export file=[nama_file]

Only IP Address : /ip address export file=[nama_file]

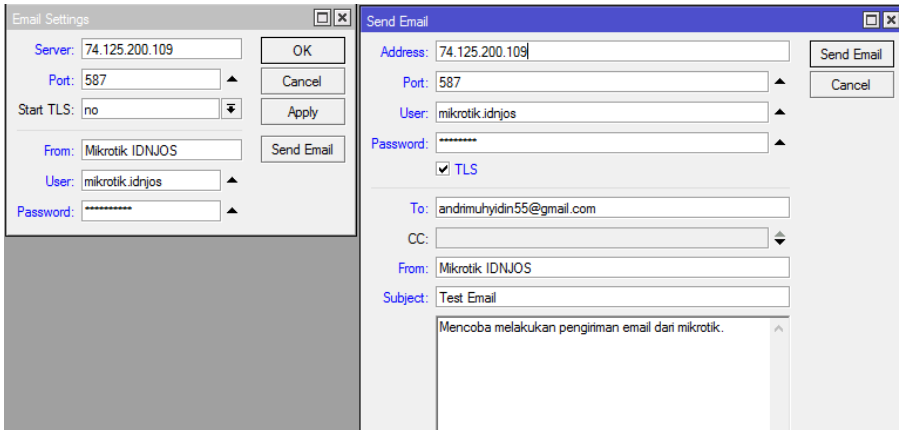
```
[admin@01_MT IDN] > export file=backup_all_config
[admin@01_MT IDN] > /ip address export file=backup-ipaddress
```

Tools Email

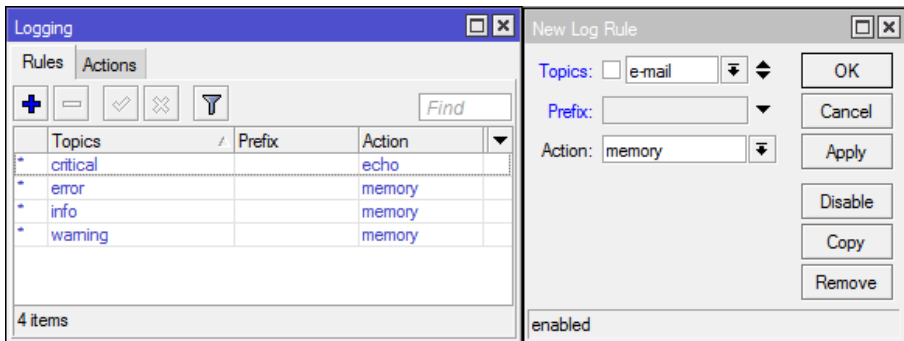
Dapat digunakan untuk Mengirimkan kondisi jaringan, Backup konfigurasi berkala, dan lainnya ke alamat email tertentu.

Tools ini hanya menggunakan enkripsi sederhana (TLS).

- Siapkan account email khusus beserta SMTP Server. Misalkan account google. Tidak disarankan untuk menggunakan email yang biasa anda pakai, karena email dan password akan terlihat jelas di WinBox.
- Cara mendapatkan IP Address dan SMTP google cobalah ping smtp.gmail.com
- Setting pada menu Tools > Email untuk smtp server, port, username dan password. Port SMTP google : 587.



- Untuk mempermudah troubleshoot penggunaan fitur ini dan melihat proses pengiriman email, maka aktifkan fitur logging untuk email di menu /System Logging.



Reset Configuration, untuk mengembalikan router ke konfigurasi default. Apabila konfigurasi sudah terlalu kompleks dan butuh direfresh dari 0, ataupun bisa jadi karena lupa password.

a) System Reset (Soft Reset)

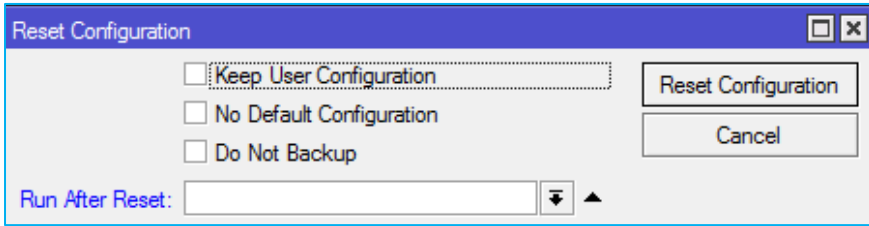
Menghapus semua konfigurasi yang telah dibuat, hanya bisa dilakukan oleh user full access.

Via Terminal

Command : system reset-configuration [option]

```
[admin@01_MT IDN] > system reset-configuration
keep-users no-defaults run-after-reset skip-backup
```


Via Winbox, masuk ke menu system > reset configuration



Terdapat beberapa option :

Options	Descriptions
Keep users	mempertahankan konfigurasi User
No Defaults	setelah direset tidak akan mengembalikan ke konfig default melainkan semua belum terkonfigurasi.
Skip backup	tidak melakukan backup konfig sebelumnya
Run after reset	menjalankan file backup setelah di reset, opsi ini membutuhkan file yang dibackup.

b) Hard Reset

Beberapa RB memiliki rangkaian khusus yang apabila dijumpet bersamaan dengan RB dinyalakan akan mereset semua konfigurasi dan kembali ke default. Dan beberapa RB memiliki tombol reset yang dapat dikenali dengan mudah.



Contohnya adalah RB 751 yang memiliki tombol reset bagian depan diantara kabel power dan LED Power indikasi.

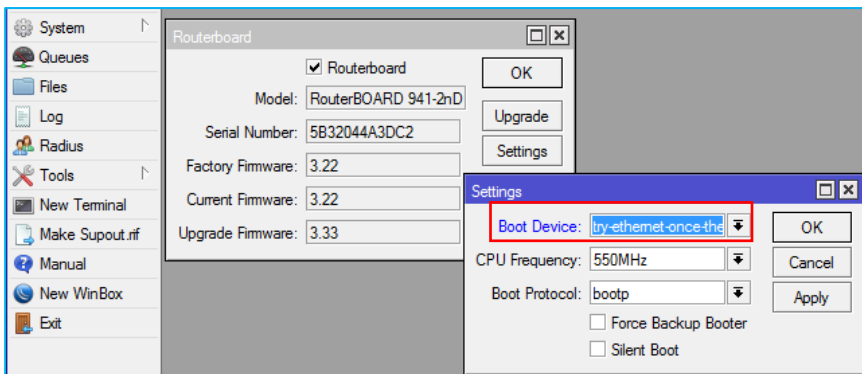
Cara melakukan reset : menahan beberapa detik tombol sembari router dinyalakan atau di reboot.

Netinstall

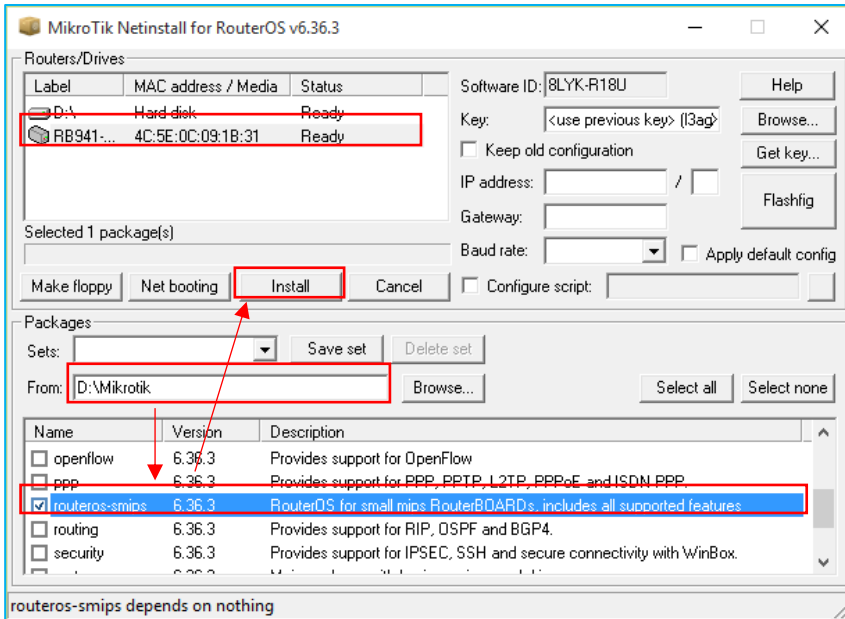
- Pada power PC menggunakan CD/USB Bootable mikrotik
- RB hanya dapat dilakukan dengan Netinstall Software
- Download di web resmi mikrotik, running under windows, dan PC harus terhubung dengan router menggunakan kabel UTP/LAN.

Langkah Kerja

- Setting BIOS pada mikrotik supaya booting melalui Ethernet sebelum NAND. Masuk menu System > Routerboard > Setting



- Masuk ke menu software netinstall. Yang perlu di setting adalah folder tempat paket routers yang akan diinstall ke RB, ekstensinya adalah npk, bukan zip.



- Selain digunakan untuk install ulang, bisa juga digunakan untuk reset password tanpa menghapus konfigurasi sebelumnya dengan cara check pilihan "keep old configuration" pada netinstall.

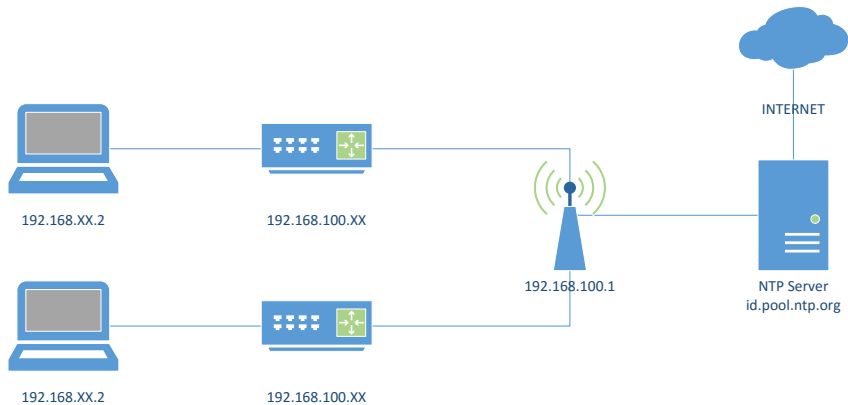
Network Time Protocol (NTP)

Rata rata RB tidak memiliki battery dan clock internal (kecuali RB 230), system clock yang akurat dan actual dibutuhkan terutama untuk log, scheduler, netwatch. NTP akan mensinkronisasi waktu dengan router atau server lainnya dalam jaringan.

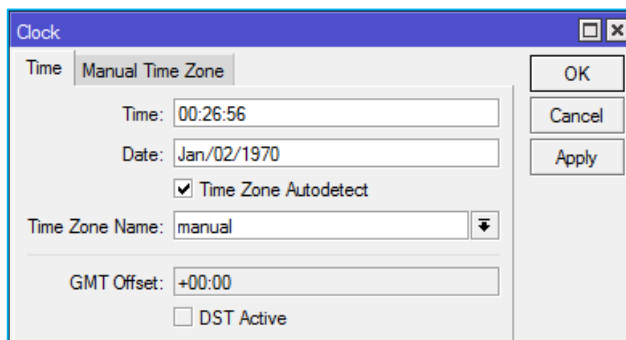
MikroTik support NTP Server dan client. Install NTP Server jika belum terinstall, Karena system hanya membundle NTP Client.

Langkah kerja

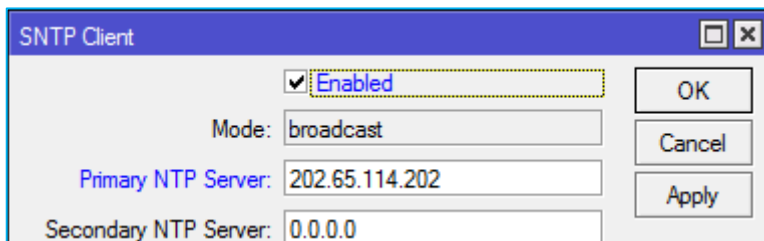
- Setting NTP Client pada RB sehingga waktu mengacu pada standar waktu internasional (GMT+7), misalkan diarahkan ke Public NTP Server **id.pool.ntp.org** atau **asia.pool.ntp.org**



- Cek internal clock router System > Clock, saat pertama ON time 00:00:00 - 1970



- Setting NTP Client System > NTP Client atau SNTP Client. Isi dengan IP Address id.pool.ntp.org atau server yang lain.



Fase sinkronisasi NTP Client adalah :

Started	Start service NTP
Reached	Terkoneksi dengan NTP Server
Synchronized	Sinkronisasi waktu dengan NTP server
Timeset	Mengganti waktu/tanggal local sesuai waktu NTP Server

- Kembali ke menu clock dan amati perubahannya, jika belum ada perubahan pastikan RB terhubung dengan NTP Server (internet atau local), atau IP Address server benar.

NTP Server Lokal

- Install & Jalankan NTP Server disalah satu router peserta, dan arahkan NTP Client peserta lainnya ke RB tersebut.
- Check apakah clock sesuai dengan waktu actual public NTP Server.

MODULE 2

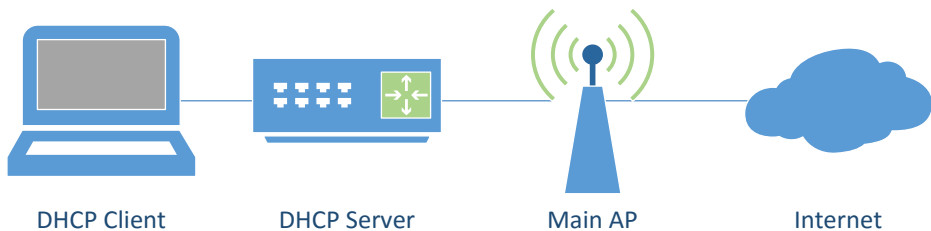
DHCP



DHCP Introduction

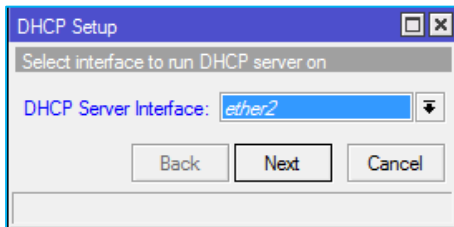
Adalah layanan yang menyediakan space IP Address (DHCP Server) dan memberikan kepada Client yang merequest layanan dari DHCP tersebut (DHCP Client). Mendukung fungsi dasar yakni memberikan client IP Address, Subnetmask, Default Gatewat, DNS & WINS Server (Windows).

Topolgy

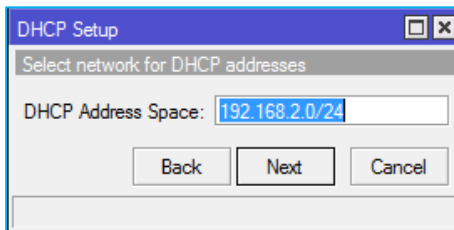


DHCP Server Configuration

Sebelum mengkonfigurasi DHCP, pastikan Interface sudah di set IP Addressnya. Masuk ke menu IP > DHCP Server > DHCP Setup.

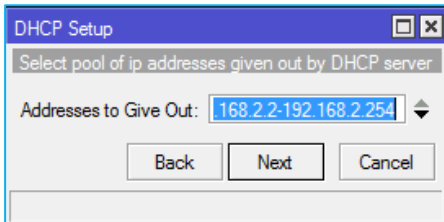
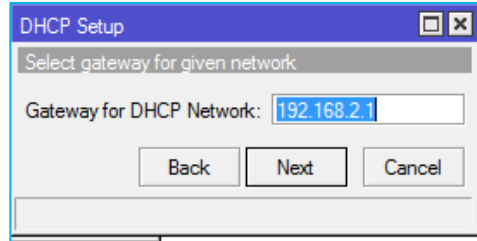


- Pilih interface untuk distribusi IP Address.

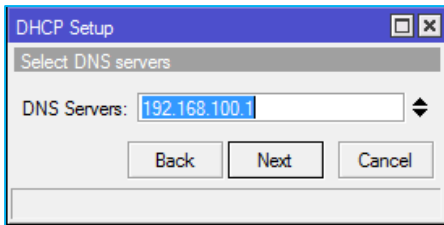


- Masukan IP Address Network beserta subnetmask yang berfungsi untuk menentukan range dari host dalam network tersebut.

- Masukan IP Address router yang digunakan sebagai gateway dari jaringan anda.

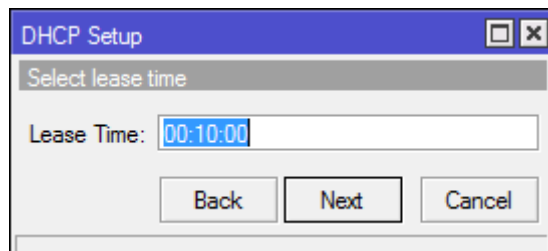


- Kemudian set range host address yang akan di distribusikan ke client.



- Set DNS Server, bisa menggunakan DNS dari internet ataupun IP router sendiri.

Kemudian langkah terakhir adalah set lease time, yakni lama waktu untuk ip address tersebut didistribusikan kedalam perangkat client.



Silahkan cek melalui client yang dihubungkan pada interface ether2 (sesuai dengan konfigurasi yang dilakukan), kemudian set IP di opsi otomatis.

PC Client Automatically Network Setup

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

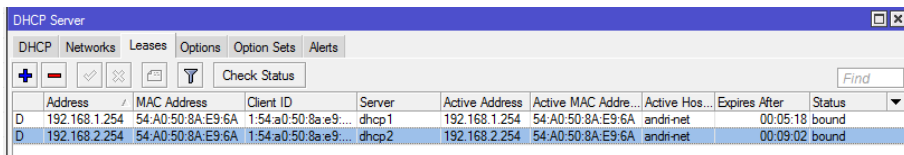
Preferred DNS server:

Alternate DNS server:

Kemudian cek apakah IP Address sudah didapatkan atau belum, bisa cek melalui CMD kemudian ketikkan ipconfig. Setelah itu cobalah akses koneksi internet (jika sudah mengkonfigurasi simple setup pada bab sebelumnya).

DHCP Server Management

Leases (IP > DHCP Server > Leases), digunakan untuk mengecek daftar penerima layanan DHCP yang sudah terkoneksi.



	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Hos...	Expires After	Status
D	192.168.1.254	54:A0:50:8A:E9:6A	1:54:a0:50:8a:e9:...	dhcp1	192.168.1.254	54:A0:50:8A:E9:6A	andri-net	00:05:18	bound
D	192.168.2.254	54:A0:50:8A:E9:6A	1:54:a0:50:8a:e9:...	dhcp2	192.168.2.254	54:A0:50:8A:E9:6A	andri-net	00:09:02	bound

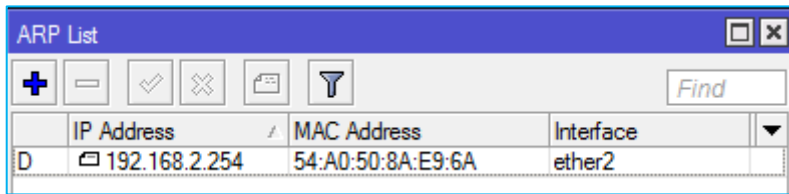
DHCP Static, digunakan untuk membuat suatu IP Address digunakan untuk MAC Address tertentu saja, bersifat tetap. Pilih salah satu MAC Address client yang sudah ter leases kemudian klik kanan dan pilih make static

ARP (Address Resolution Protocol)

Digunakan untuk alasan keamanan, yakni hanya membolehkan client yang terdistribusi IP dari DHCP Server untuk terkoneksi, dan tidak untuk yang secara manual.

ARP Table

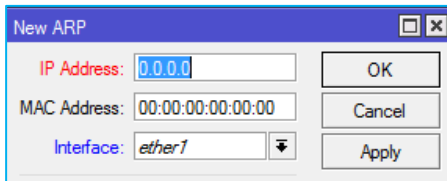
Sebuah router memiliki tabel ARP yang berisi entri ARP yang terdiri dari *IP Address* dan *MAC Address* yang sesuai. Cek pada menu `/ip arp`



	IP Address	MAC Address	Interface
D	192.168.2.254	54:A0:50:8A:E9:6A	ether2

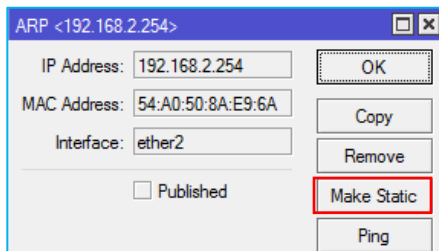
Default Dynamic ARP, entri ARP akan ditambahkan otomatis oleh Router ketika terdapat perangkat yang terkoneksi dengan interface tersebut.

Static ARP, untuk meningkatkan keamanan mode ini diperlukan, yakni dengan menambahkan secara manual Entri ARP.



Caranya klik Add New kemudian masukan kombinasi IP & MAC Address.

Make Static, membuat Dynamic ARP menjadi static

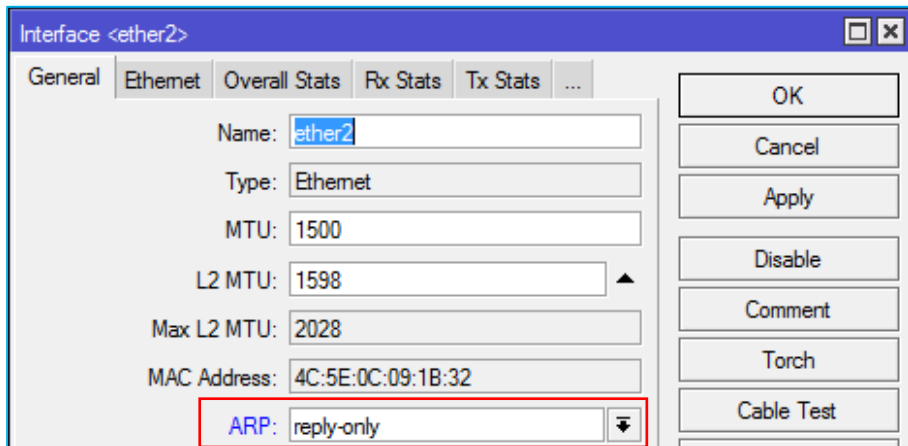


Caranya double klik pada salah satu entri ARP yang akan di set manual, kemudian pilih MAC Static.

ARP Mode pada DHCP Network

Cara ini lebih efektif pada jaringan berskala dibanding dengan IP Manual dan menggunakan ARP Static (Input manual).

Caranya setting pada interface yang mendistribusikan DHCP dan pada menu **ARP = reply-only**



- Add ARP For Leases
- Always Broadcast
- Use RADIUS

Kemudian aktifkan "Add ARP For Leases" untuk mengaktifkan mode ARP pada jaringan yang memiliki DHCP.

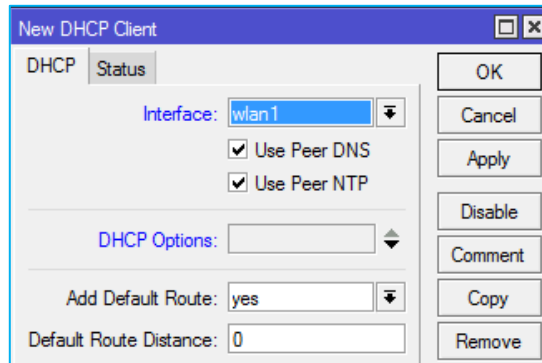
Pada kondisi ini router hanya menerima request client dengan kombinasi IP & MAC Address yang sesuai dengan table ARP. Tanpa menambahkan ARP Secara manual.

Test pada Client

Cobalah rubah IP Laptop secara manual dan koneksikan kembali pada RB Mikrotik.

DHCP Client

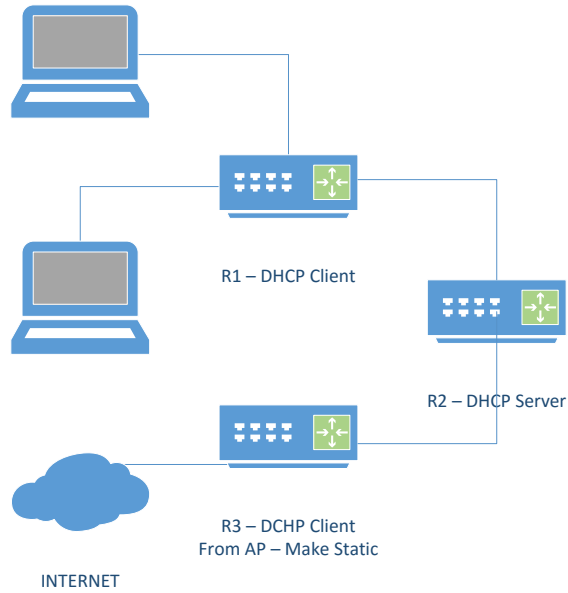
Berfungsi untuk menerima layanan IP Address yang disediakan oleh DHCP Server. Beberapa parameter yang perlu diperhatikan dalam mengkonfigurasi DHCP Client :



Parameter	Keterangan
Interface	Pilih interface yang terkoneksi pada DHCP Server
Hostname (Optional)	Nama host yang akan dikenali oleh dhcp server
Client ID (Optional)	MAC Address yang digunakan apabila proses DHCP Server menggunakan radius.
Add default route	Jika ingin aturan default route mengarah sesuai dengan informasi DHCP Server
Use peer DNS	Mengikuti aturan DNS dari DHCP Server
Use peer NTP	Mengikuti aturan NTP dari DHCP Server
Default route distance	Menentukan prioritas routing jika terdapat lebih dari 1 DHCP Server, routing akan melalui distance yang lebih kecil.

Silahkan di Praktikan

Topology



Keterangan

Options	Values
R2	AP + DHCP Server
R1, R2	Station + DHCP Client
R3	Gateway Internet
Default route R1	IP R3
DHCP Server R2	Make Static R3
ARP	Reply Only

MODULE 3

WIRELESS



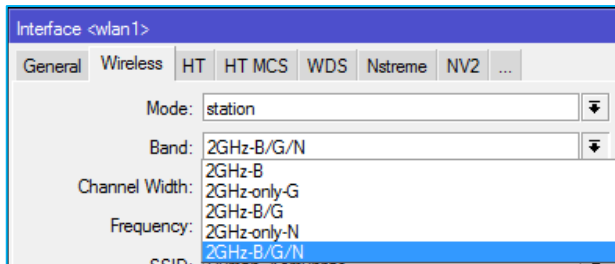
Wireless Concept

Mikrotik mendukung beberapa modul ratio wireless card untuk jaringan wlan menggunakan frekuensi 2,4 GHz dan 5 GHz dengan standard an spesifikasi IEEE 802.11 a/b/g/n.

Spesifikasi	Frekuensi	Speed Up
802.11 a	5 GHz	54 Mbps
802.11 b	2,4 GHz	11 Mbps
802.11 g	2,4 GHz	54 Mbps
802.11 n	2,4 atau 5 GHz	300 Mbps

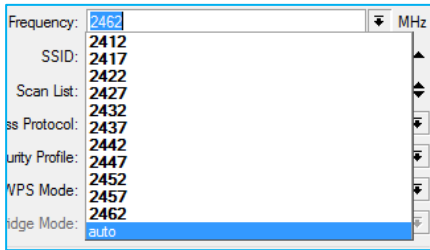
Wirelles Band

Band merupakan mode kerja frekuensi dari suatu perangkat wireless untuk menghubungkan 2 perangkat, keduanya harus bekerja pada band frekuensi yang sama. Band yang ada di list berikut bergantung pada jenis wireless card yang digunakan.



Frekuensi Channel

Adalah pembagian frekuensi dalam suatu band dimana AP beroperasi. Nilai channel bergantung pada band yang dipilih, kemampuan wireless card, dan regulasi frekuensi pada suatu negara.



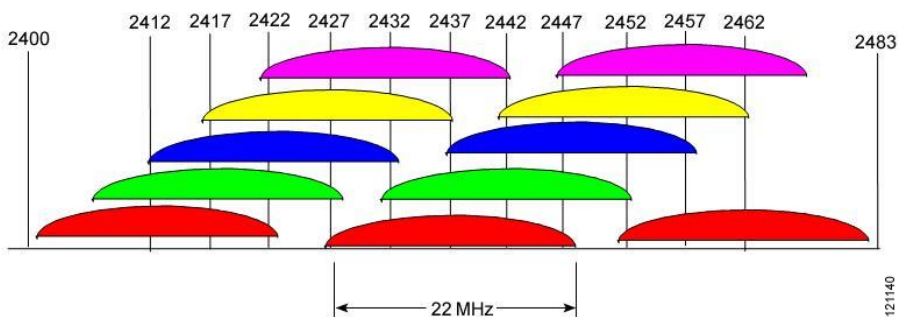
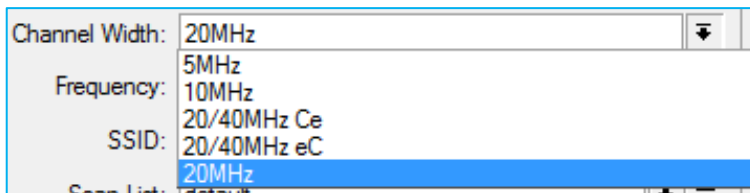
Range frequency channel masing masing band :

- 2,4 GHz = 2312 – 2399 MHz
- 5 GHz = 4920 – 6100 MHz

Channel Width

Rentan frekuensi batas bawah dan batas atas dalam 1 channel/kanal. Mikrotik dapat mengatur beberapa lebar channel yang akan digunakan. Default lebar channel yang akan digunakan adalah : 22 Mhz (ditulis 20 MHz).

Lebar channel dapat dikecilkan 5 MHz untuk meminimalil frekuensi, atau dibesarkan 40 MHz untuk mendapatkan throughput yang lebih besar.



Wireless Connection

Koneksi terjadi antara AP dengan 1 atau lebih station. Syarat terjadi koneksi wireless adalah kesamaan SSID dan Band. Station akan secara otomatis mengikuti channel frekuensi pada AP. Station hanya dapat melakukan scan AP dengan list frekuensi yang di set pada station. Mode interface wireless mikrotik :

AP Mode

- AP Bridge, fungsinya sebagai Access Point
- Bridge, hamper sama seperi AP Bridge, bedanya mode ini hanya bisa dikoneksikan oleh 1 station saja atau dalam mode point to point.

Station Mode

- Station, Scan dan connect AP dengan frekuensi dan SSID yang sama, tidak bisa di bridge
- Station WDS, sama dengan station namun bedanya mode ini dapat membentuk koneksi WDS (Wireless Distribution System) dengan AP yang menjalankan WDS.
- Station Pseudobridge, sama seperti station, dengan tambahan MAC Address Translation untuk fungsi bridge.
- Station Pseudobridge Clone, sama seperti Station Pseudobridge, namun menggunakan Station Pseudobridge Clone address untuk konek ke AP.

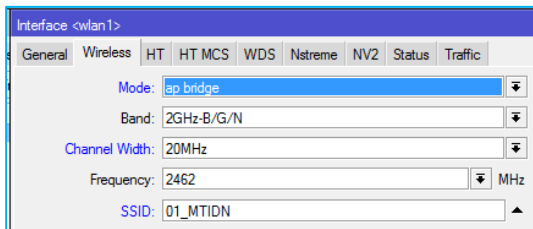
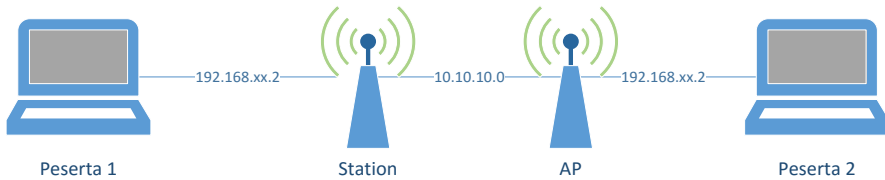
Special Mode

- Alignment Only, mode transmit terus menerus digunakan untuk positioning antena jarak jauh
- Nstreame dual slave, digunakan untuk system nstreame dual slave (dual antenna)

- WDS Slave, sama seperti AP Bridge, namun melakukan scanning ke SSID yang sama dan melakukan koneksi menggunakan WDS, apabila link terputus akan melanjutkan scanning.

Wireless Access Point

Topology



Terdapat 2 RB, buatlah masing masing menjadi AP & Station, samakan SSID, band & Frekuensinya.

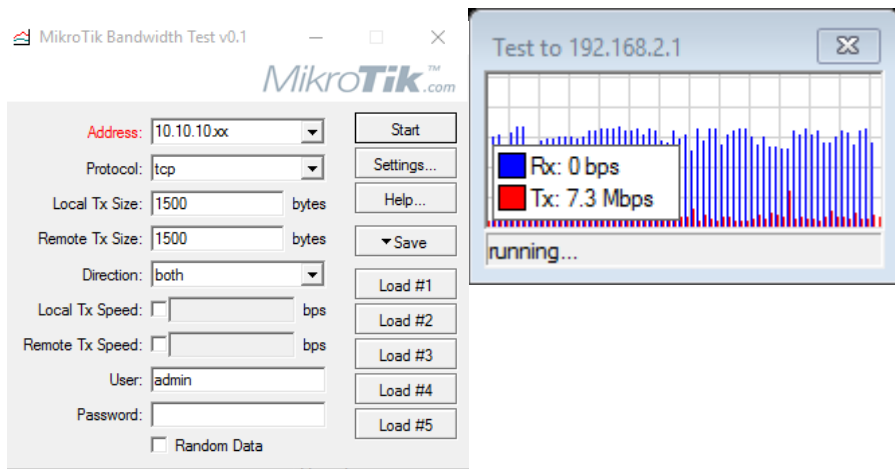
Frequency (MHz)	Usage	Noise F...
2412	4.8	-111
2417	3.5	-115
2422	1.3	-115
2427	3.6	-114
2432	2.0	-113
2437	6.7	-108
2442	4.2	-110
2447	3.3	-110
2452	2.9	-111
2457	2.6	-116
2462	4.5	-117

-Tambahkan IP Address pada masing masing WLAN pada AP dan station, bedakan untuk tiap pasangan.

-Pastikan link sudah terkoneksi dan dapat dilakukan ping ke masing masing address.

-Coba gunakan tool freq usage dan snoopers untuk mencari signal freq yang maksimal (max ccq).

Lakukan test ping & bandwidth menggunakan /tools bandwidth test.

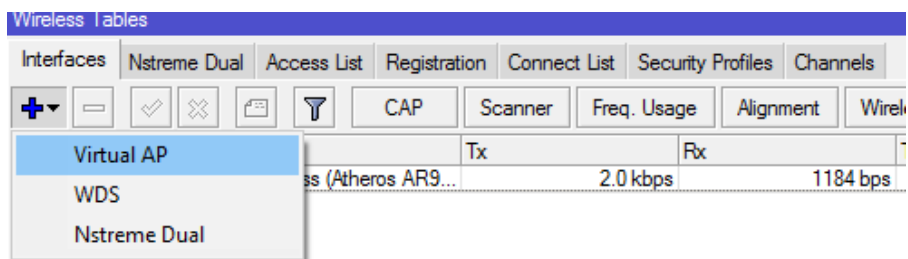


Virtual Access Point

Akan menjadi Child dari real interface wlan dan dapat di set SSID yang berbeda namun menggunakan frequency dan band yang sama dengan wlan induk. Virtual AP bersifat sama seperti AP yaitu :

- Dapat dikoneksikan dengan station atau client
- Sebagai DHCP Server
- Sebagai Hotspot server

Cobalah membuat Virtual AP sebanyak banyaknya dengan SSID yang berbeda beda untuk setiap virtual AP.



Setting SSID, Security, dan option lainnya sesuai dengan kebutuhan, dan pastikan Virtua AP berhasil menjadi list child main AP.

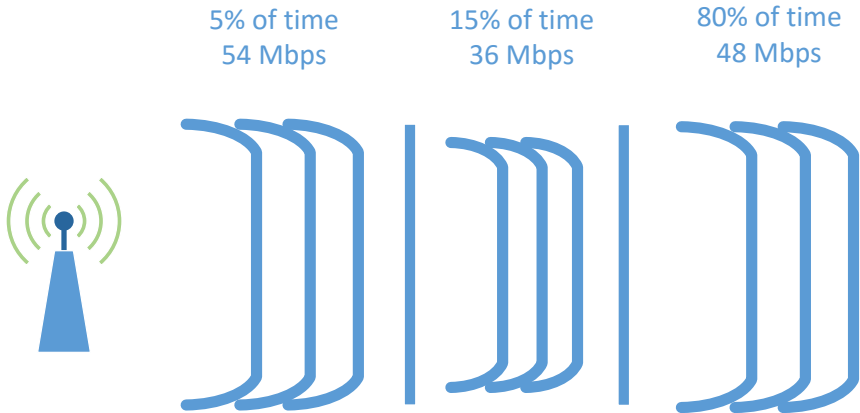
Wireless Tables						
Interfaces						
Nstreme Dual						
Access List						
Registration						
Connect List						
Security Profiles						
Channels						
CAP						
Scanner						
Freq. Usage						
Alignment						
Wireless Sniffer						
Wireless Snooper						
Name	Type	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	
R wlan1	Wireless (Atheros AR9...		336 bps	336 bps	1	
↔MTIDN_01	Virtual AP	0 bps	0 bps	0	0	
↔MTIDN_02	Virtual AP	0 bps	0 bps	0	0	

Dan gunakan tool scanning adan snooper dari router peserta lain untuk mengamatinnya.

Rate Flapping (Rate Jump)

Terjadi karena naik turunnya data rate sehingga link tidak stabil. Hal ini dapat dicegah dengan memilih data rate yang lebih rendah agar link lebih stabil. Menu Wirelles > Registration.

Misalkan untuk contoh dibawah ini, link akan lebih stabil apabila rate diturunkan menjadi 36 Mbps.



Access & Connection List

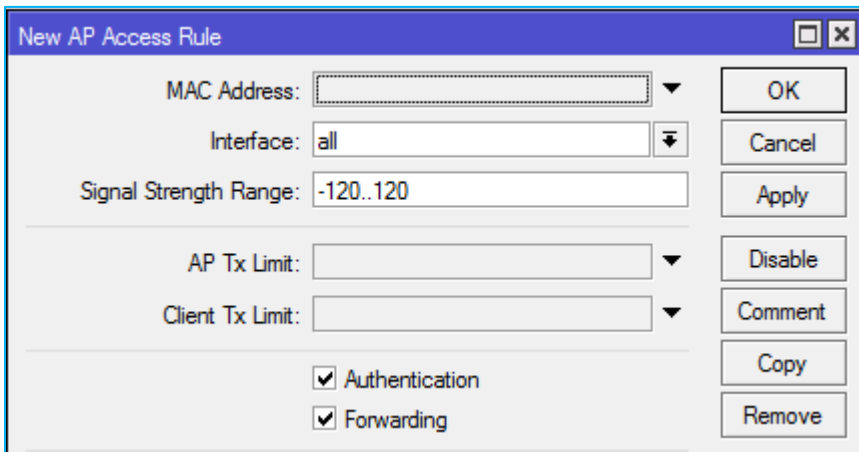
Digunakan untuk fitur keamanan wireless yakni dengan teknik filtering mac-address.

- **Mode Access Point**, pembatasan hak akses dapat dilakukan dimana AP hanya dapat dikoneksikan oleh station yang sudah terdaftar (access list)
- **Mode Station**, agar tidak tertipu oleh SSID AP yang sama, dapat di lock dengan MAC Address Filtering (Connect List)

a) Access List

Mengatur client/station mana saja yang diizinkan untuk terkoneksi dengan interface wireless AP.

Menu */wireless access-list*

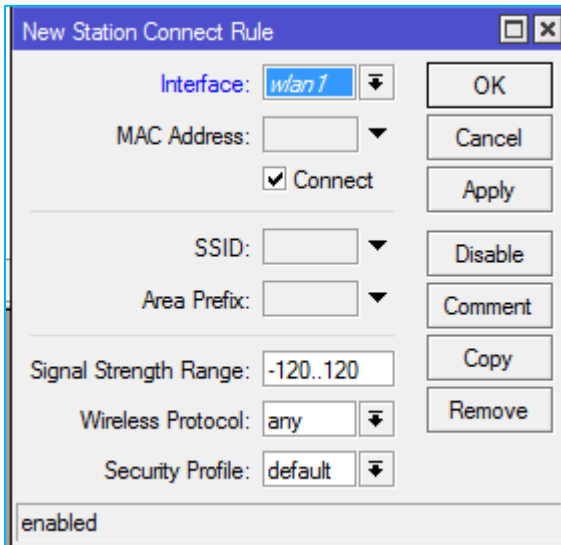


Option	Keterangan
MAC Address	Yakni Alamat MAC yang diizinkan untuk terkoneksi
Signal Strength Range	Batas nilai kekuatan signal station yang diizinkan.

b) Connection List

Membatasi AP mana saja yang diizinkan untuk terkoneksi dengan interface wireless suatu station.

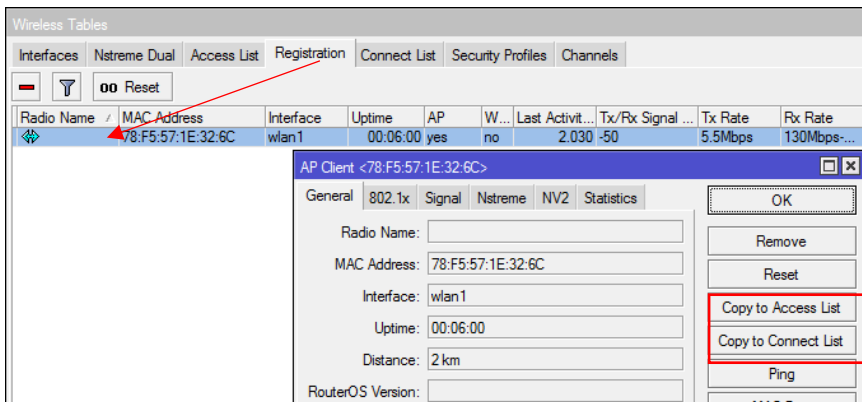
Menu /Wireless connection-list



Options	Keterangan
Interface	Interface radio yang difungsikan sebagai client
MAC Address	MAC Address AP yang akan dikoneksikan
Connect (Y/N)	Boleh atau tidaknya terkoneksi dengan MAC diatas.
SSID	SSID yang ingin dikoneksikan, bila kosong berarti Any AP
Security Profile	Jika menggunakan option ini harus diapply di rule connection list.

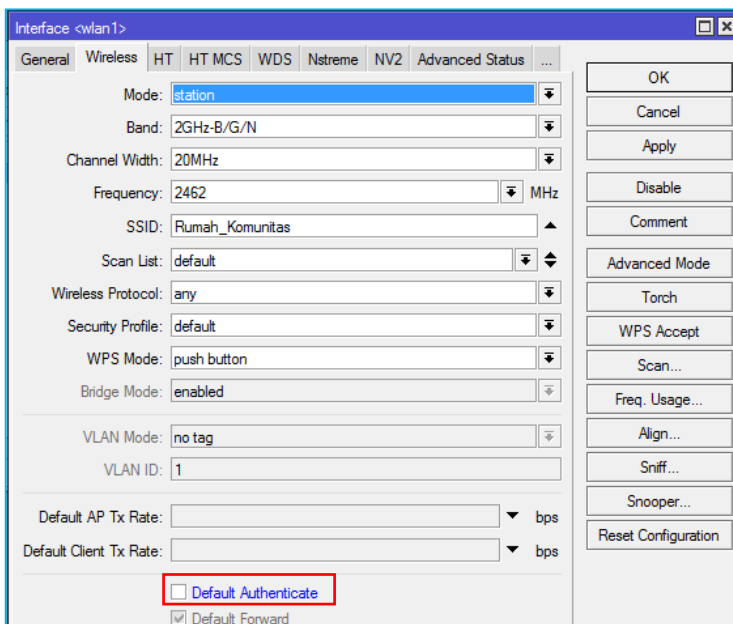
c) Registration List

Berisi data AP/Station yang sedang terkoneksi. Untuk mempermudah entri informasi AP atau Station kedalam Access List maupun Connection List dapat mengambil informasi dari Registered List.



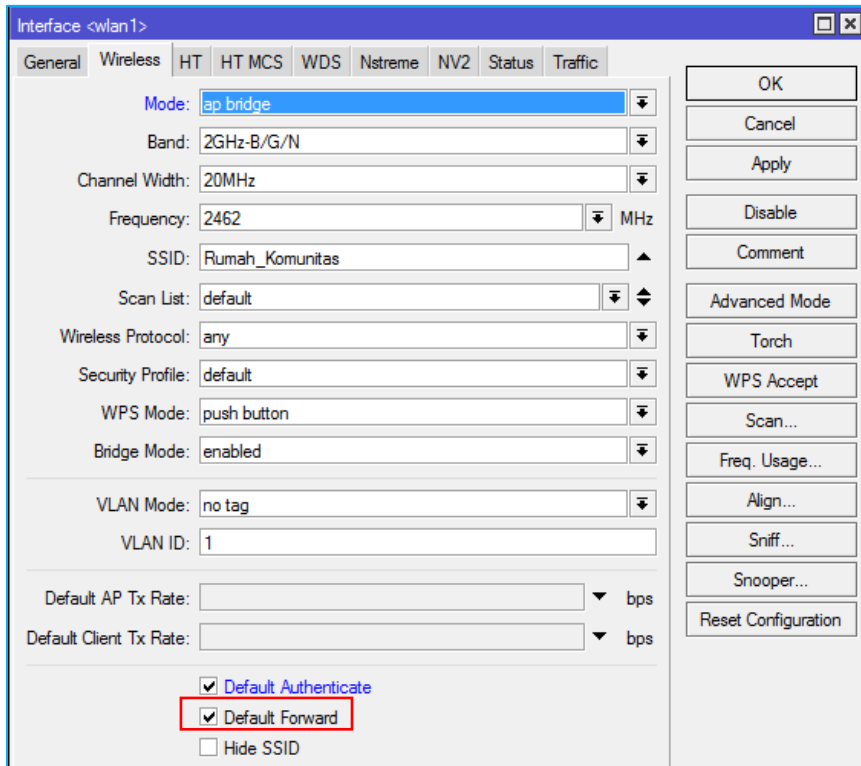
d) Default Authenticated

Uncheck default authenticated untuk menggunakan pilihan Connection List atau Access List baik pada AP atau Station.



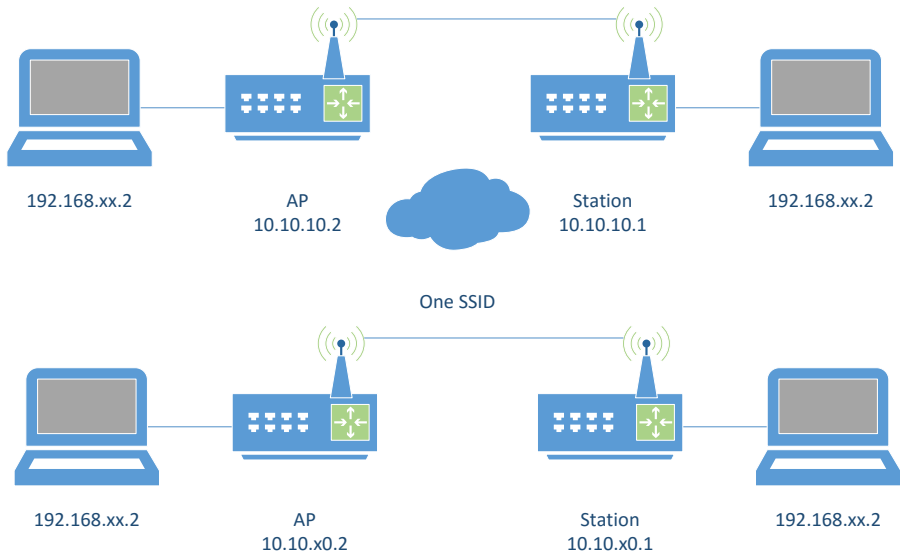
e) Default Forward

Only Access Point mode. Digunakan untuk perizinan komunikasi antar client/station yang terkoneksi dalam 1 AP.



f) MAC Address Filtering Lab

Topolgy



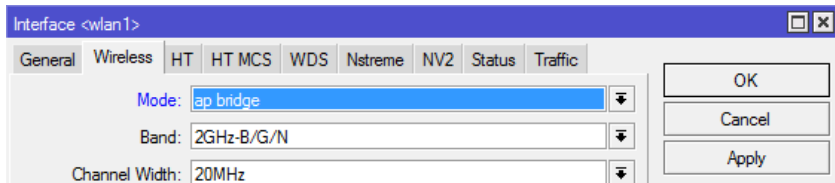
Langkah Kerja

- Cobalah untuk memfilter MAC Address agar koneksi PTP dengan partner anda tidak mudah dikacaukan oleh koneksi lain.
- Masukan data MAC Address wireless partner ke list yang benar. Station ke Connection List, AP ke Access List.

Default Authenticate Setting wireless AP, default authenticate harus di uncheck agar tidak semua client bisa terautentikasi secara otomatis.

Default Forward

Hide SSID



Wireless Encryption & LAB

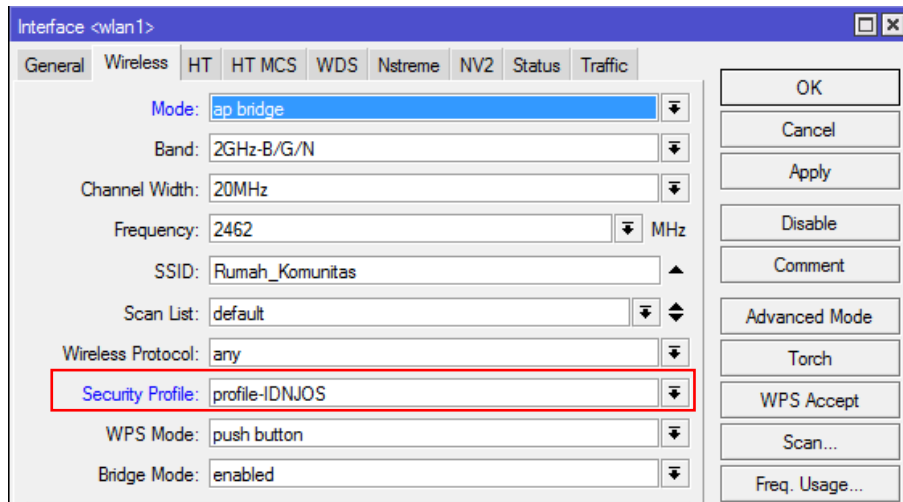
Selain MAC Filtering terdapat metode keamanan lainnya :

- Authentication (WPA-PSK, WPA-AEP)
- Enkripsi (AES, TKIP, WEP)
- Tunnel

Menu /Wireless Security-Profile

Option	Keterangan
Name	Diberi nama tertentu untuk diimplementasikan pada interface wireless.
Mode Dynamic Keys	WPA
Mode Static Keys	WEP (Old Version)
Authentication Types	Jenis Autentikasi
Unicast Ciphers	Jenis enkripsi
Field Key	Kolom untuk mengisi password atau autentikasi.

Kemudian implementasikan pada wireless interface dengan cara double klik pada interface wireless dan ubah security profile ke profil yang sudah dibuat.



Security profile dapat diterapkan pada mode AP ataupun Station. Perbedaannya adalah ketika di *Mode AP*, maka security profile ini digunakan untuk station dalam mengautentikasi password wifi. Sedangkan pada *Mode Station*, digunakan untuk autentikasi ke AP (harus sama dengan AP).

MODULE 4

FIREWALL



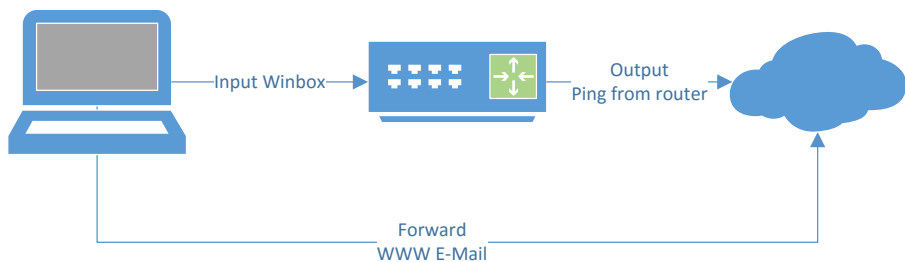
About Firewall

- melindungi router dan jaringan dari akses yang tidak dikehendaki baik dari luar (internet) maupun client (local).
- Filtering access
- Dalam mikrotik firewall diimplementasikan dalam fitur filter rule dan NAT

Firewall Chain

3 default chain yang otomatis dilewati traffic dalam mikrotik router dan tidak dapat dihapus :

- Input, untuk memproses paket yang **memasuki router** melalui salah satu interface dengan Dst IP Address merupakan salah satu IP Address router. Paket tidak bisa melewati router jika bertentangan dengan aturan chain input.
- Forward, untuk memproses paket yang melewati router
- Output, untuk memproses paket berasal dari router dan meninggalkan melalui salah satu interface.



Rule Chain

- Aturan chain dibaca oleh router dari atas kebawah
- Paket dicocokkan dengan kriteria umum dalam suatu chain, apabila cocok paket akan melalui kriteria umum chain berikutnya kecuali di passthrough
- Chain bekerja berdasarkan prinsip IF ... THEN ... (Syarat ... Tindakan ...)

IF Condition

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Source IP (IP Client)
Dst IP (IP Internet)

Protocol (TCP/UDP/ICMP,dll)
Source port (umumnya port dari client)
Dst Port (Service port tujuan)

Interface for traffic
are incoming Atau
outgoing.

Then Condition

Extra Action Statistics ...

Action: accept

Log Prefix:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

```

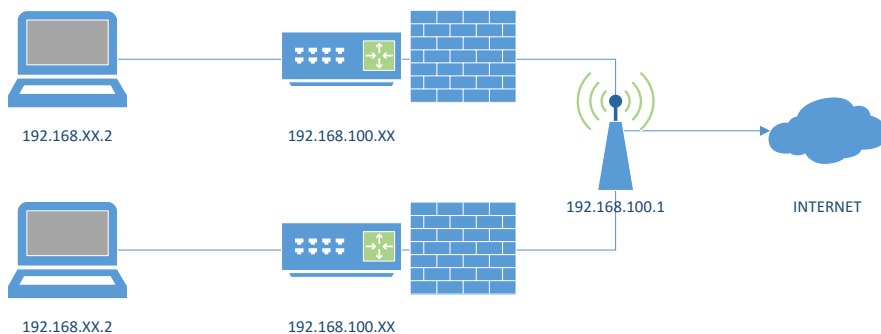
accept - accept the packet. Packet is not passed to next firewall rule.
add-dst-to-address-list - add destination address to address list specified by address-list parameter
add-src-to-address-list - add source address to address list specified by address-list parameter
drop - silently drop the packet
jump - jump to the user defined chain specified by the value of jump-target parameter
log - add a message to the system log containing following data: in-interface, out-interface, src-mac, protocol,
src-ip:port->dst-ip:port and length of the packet. After packet is matched it is passed to next rule in the list,
similar as passthrough
passthrough - ignore this rule and go to next one (useful for statistics).
reject - drop the packet and send an ICMP reject message
return - passes control back to the chain from where the jump took place
tarpit - captures and holds TCP connections (replies with SYN/ACK to the inbound TCP SYN packet)

```

Firewall Strategy

Terdapat 2 metode, yakni :

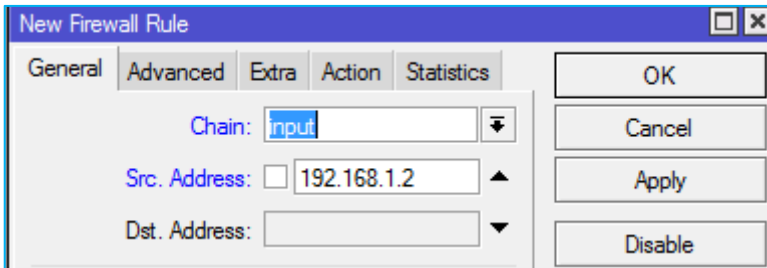
- Drop few, accept any
- Accept few, drop any



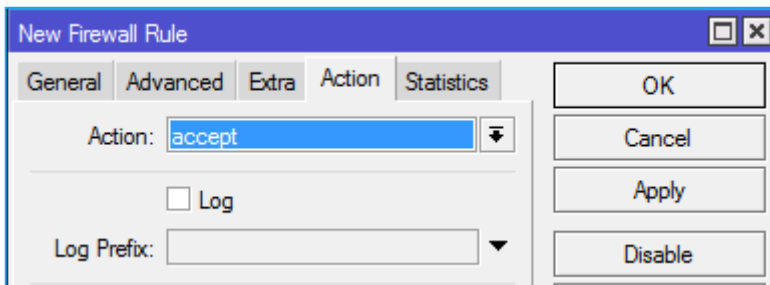
Accept few & Drop Any, hanya IP Laptop yang bisa mengakses router

- Chain input, karena akan melakukan filter traffic ke router
- Buat IF Condition di menu IP > Firewall > Filter Rules > General

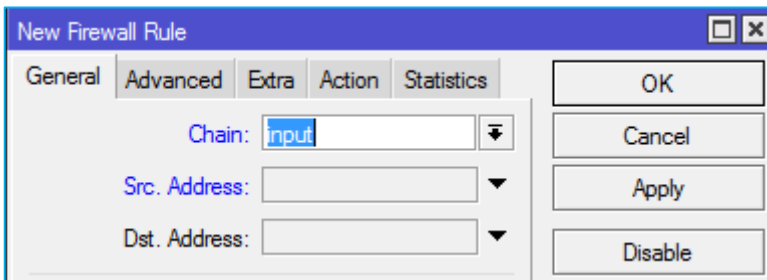
Jika (IF) ada traffic menuju ke router (chain = input) yang berasal dari IP Laptop (src address = 192.168.xx.2)



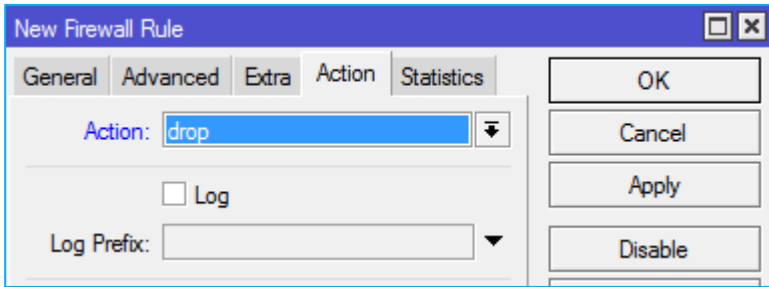
- Buat THEN condition di tab menu action, paket akan di terima "Accept"



- Setelah membolehkan IP Laptop mengakses router, selanjutnya adalah memblok semua IP kecuali IP laptop itu sendiri.
- Buat IF Condition, Jika ada traffic yang masuk siapapun itu



- Then condition, maka akan di drop

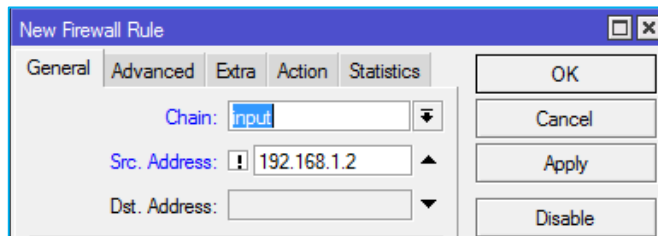


- Akan ada 2 chain rule, perhatikan jumlah bytes pada setiap chain rule ketika melakukan akses ke router, bertambahkah ? Cobalah melakukan akses ping, akses web, atau remote winbox

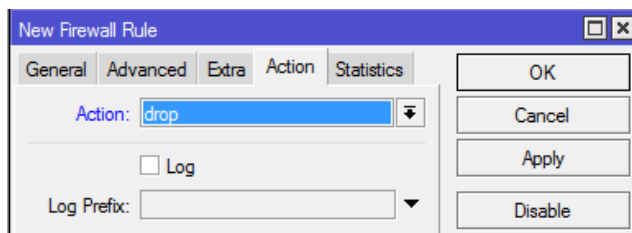
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc...	input	192.168.1.2							58.7 KiB	790
1	✗ drop	input								1107 B	8

Drop Any & Accept Few, drop any paket kecuali dari IP Laptop

- Pada IF Condition tanda seru "!" berarti selain (Selain IP Laptop)



- Maka akan di Drop



Firewall Logging

Adalah fitur untuk mencatat aktifitas yang jaringan inginkan dan ditampilkan pada log.

Log Ping ke IP Interface Router

- Buat filter rule pada IP > Firewall > Filter Rules, untuk tagging semua ICMP yang mengarah ke kedalam router melalui interface ether1. Atau menggunakan script yang dieksekusi di terminal :

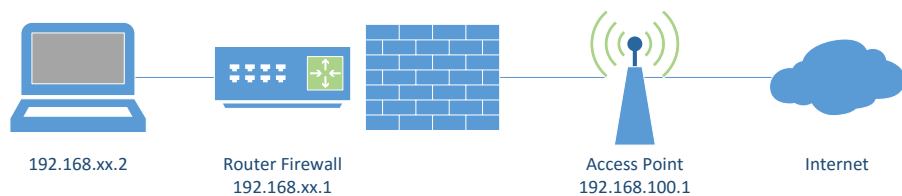
```
chain=input protocol=icmp in-interface=ether1 action=log
log-prefix="pinger"
```

- Coba ping dari laptop menuju interface IP ether 1

Sep/08/2016 15:59:31	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:31	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:32	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:32	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:33	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:33	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:34	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:34	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:35	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60
Sep/08/2016 15:59:35	memory	firewall.info	pinger input: in:ether1 out:(none), src-mac 54:a0:50:8a:e9:6a, proto ICMP (type 8, code 0), 192.168.1.254->192.168.1.1, len 60

Block Situs Tertentu

Topology



Membatasi akses client agar tidak bisa mengakses situs tertentu.

Misalnya situs <http://idn.id>.

Langkah Kerja :

- Cek IP Address suatu domain

Command > ping idn.id

```
C:\>ping idn.id
Pinging idn.id [104.152.168.20] with 32 bytes of data:
```

Berdasarkan informasi yang didapatkan bahwa idn.id memiliki IP Address 104.152.168.20.

- Filter rule

Option	Value
Chain	Forward
Dst Address	104.152.168.20
Action	Drop

Implementasikan rule tersebut pada RB anda.

IF Condition	
Then Condition	

Jika suatu domain memiliki banyak IP seperti youtube, bisa menggunakan langkah ini secara berulang dengan entri IP satu persatu. Atau

Gunakan Address List untuk mendefinisikan beberapa IP Address suatu domain sebelum dibuatkan rule diatas.

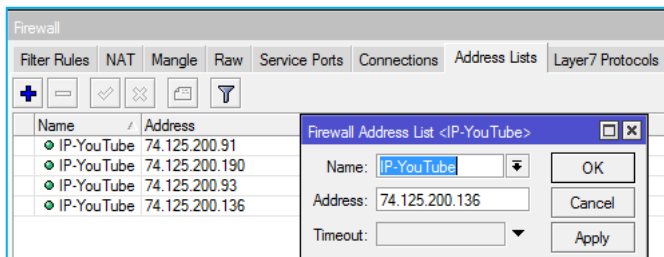
Address List Block

Misalkan disini akan memblok suatu situs yang memiliki banyak IP. Contohnya adalah YouTube. Untuk mencari tahu informasi IP Address youtube bisa menggunakan nslookup.

```
C:\>nslookup youtube.com
Server: 1.2.168.192.in-addr.arpa
Address: 192.168.2.1

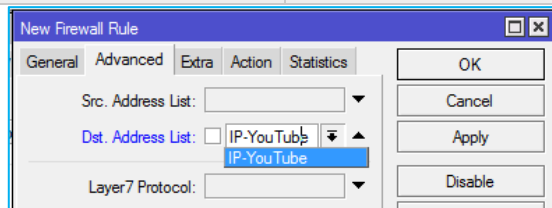
Non-authoritative answer:
Name: youtube.com
Addresses: 2404:6800:4003:c00::5b
           74.125.200.91
           74.125.200.190
           74.125.200.93
           74.125.200.136
```

Masuk ke menu /firewall address-list



Buat filter rule dengan ketentuan sebagai berikut

Option	Value
Chain	Forward
Dst Address List	IP-YouTube
Action	Drop



Kita juga dapat mengatur client mana saja yang diizinkan untuk akses ke YouTube dengan mengatur Src Address pada filter rule atau mendefinisikan dahulu IP Address client pada access list.

Connection Tracking & State

Untuk melihat **Connection Tracking** lihat menu IP > Firewall > Connection.

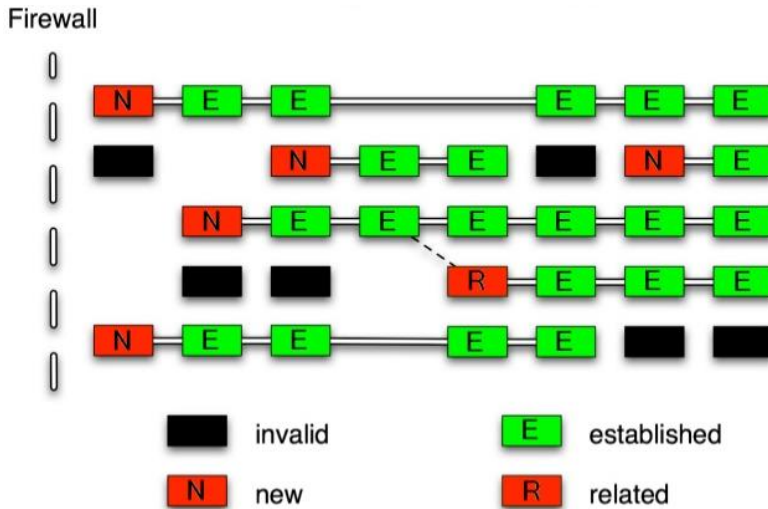
Firewall								
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols								
Tracking								
	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
SACs	192.168.2.254:62040	216.58.196.174:443	17 (u...		00:02:40		0 bps/0 bps	15.6 KiB/5.9 KiB
Cs	192.168.100.8:14943	111.221.29.109:443	6 (tcp)		23:18:56	established	0 bps/0 bps	280 B/0 B
Cs	192.168.100.8:14874	111.221.29.109:443	6 (tcp)		23:07:55	established	0 bps/0 bps	240 B/0 B
SACs	192.168.2.254:50102	172.217.24.78:443	17 (u...		00:02:59		78.2 kbps/1623.5 kbps	10.9 KiB/199.0 KiB
C	192.168.2.254:59161	255.255.255.255:20...	17 (u...		00:00:09		800 bps/0 bps	215.6 KiB/0 B
SACs	192.168.2.254:15089	111.221.29.109:443	6 (tcp)		23:52:17	established	0 bps/0 bps	1471 B/4729 B
SACs	192.168.2.254:15093	74.125.68.188:443	6 (tcp)		23:59:36	established	0 bps/0 bps	2148 B/1870 B
SACs	192.168.2.254:15146	74.125.200.91:443	6 (tcp)		23:59:19	established	0 bps/0 bps	1410 B/738 B
SACs	192.168.2.254:50393	74.125.200.100:443	17 (u...		00:01:02		0 bps/0 bps	2805 B/26.3 KiB
SACs	192.168.2.254:14863	103.253.112.214:80	6 (tcp)		23:06:32	established	0 bps/0 bps	1121 B/46.3 KiB
SACs	192.168.2.254:59554	74.125.68.188:5228	6 (tcp)		23:05:59	established	0 bps/0 bps	14.1 KiB/21.5 KiB

Connection Tracking memiliki kemampuan untuk melihat informasi koneksi yang melewati router seperti source dan destination IP & Port yang sedang digunakan, status koneksi, tipe protocol, dan lain lain.

Setiap paket data memiliki status koneksi (**Connection State**) yang dapat dilihat pada Connection Tracking. Status koneksi :

State	Description
Established	paket ini merupakan bagian dari koneksi yang telah dikenal.
New	Paket baru terkoneksi atau memiliki koneksi yang belum terdapat paket di kedua arah.
Related	paket memulai membuat koneksi baru , tetapi terhubung dengan koneksi yang ada, seperti transfer data FTP atau pesan kesalahan ICMP.
Invalid	paket tidak tergabung dalam koneksi yang dikenal. pada saat yang sama, tidak membuka koneksi baru yang valid.

Gambaran Connection State



Membuat Rule Connection State

Fungsi : menghemat resource & keamanan jaringan.

a) Membuat filter rule untuk connection state valid

Option	Value
Chain	Input
Connection State	Invalid
Action	Drop

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Connection Type:

Connection State: invalid established related new

Connection NAT State:

Dengan cara buatlah untuk connection state yang lain dengan nilai yang berbeda.

Connection State	Action
Established	Accept
Related	Accept
New	Passthrough

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	input								0 B	0
1	✓ acc...	input								1122 B	7
2	✓ acc...	input								6.0 KiB	82
3	📄 pas...	input								28.7 KiB	538

Menghemat resource karena proses filtering selanjutnya akan dilakukan ketika koneksi dimulai (Connection State = New).

Network Address Translation (NAT)

Adalah suatu metode untuk menghubungkan lebih dari satu computer ke jaringan internet dengan menggunakan satu alamat IP Public. NAT digunakan karena ketersediaan IP Public, selain itu digunakan karena alasan keamanan, kemudahan, fleksibilitas dalam administrasi jaringan. 2 Type NAT

- Source NAT, untuk paket yang berasal Network yang di NAT (LAN), action masquerade. Command :

```
ip firewall nat add chain=srcnat action=masquerade out-interface=wlan1
```

Keterangan :

Paket dari interface manapun yang keluar melalui interface public (wlan1) akan di bungkus (masquerade) dan ditranslasikan menjadi IP Public.

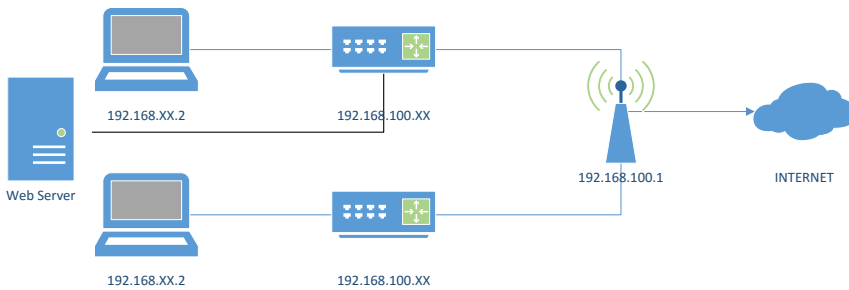
- Destination NAT, untuk paket yang menuju ke jaringan yang di NAT. biasanya digunakan untuk mengakses service local dari luar jaringan, digunakan juga untuk membelokan port dari natted network ke port tertentu pada router atau IP dan port lain diluar router.

Membuat Rule DMZ (DeMilitarized Zone)

adalah suatu servis tertentu dalam zona privat (LAN) yang dapat diakses dari luar (internet) dengan metode port forwarding.

Accessing Web Server Local dari Internet

Fungsikan salah satu client pada LAN 1 sebagai web server yang bisa diakses dari IP luar (WAN)

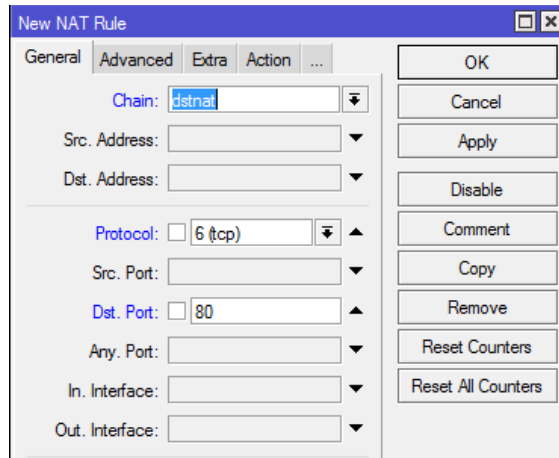


Mengaktifkan Web Server, bisa menggunakan XAMPP, WAMPP, dll

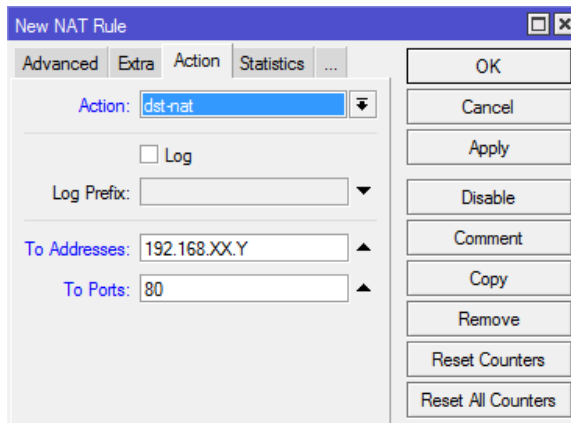


Buat rule firewall nya sebagai berikut (Firewall > NAT)

Chain = dstnat, protocol = tcp, dst-port = 80



action = dstnat, to-address = 192.168.100.2, port = 80



Rule ini dapat diartikan jika kondisi traffic menuju jaringan yang di NAT (LAN 1), pada protocol TCP Port 80 (http), maka akan diarahkan ke IP Web Server pada LAN 1.

Untuk mencoba hasil dstnat coba akses IP WLAN1 router peserta 1 via web browser dari LAN 2. Kemudian coba nonaktifkan rule dan akses kembali.

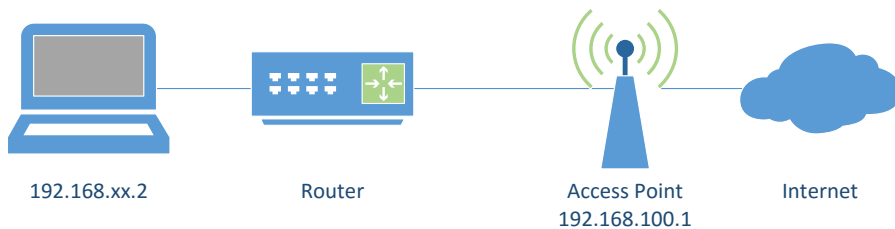
Hotspot Mikrotik

Fungsi : memberikan layanan jaringan di area public dengan media kabel atau nirkabel.

Rule : Ketika user membuka web page maka router akan memeriksa apakah pengguna terautentikasi atau tidak. Jika tidak, maka akan diredirect ke hotspot login page yang memerlukan username dan password. Tapi jika informasi benar, maka router akan menerima user kedalam system dan memberikan akses kedalam jaringannya.

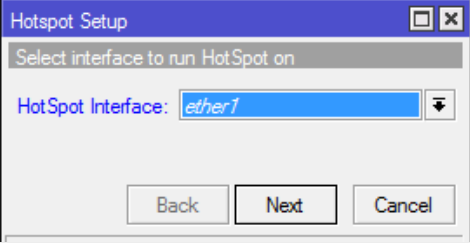
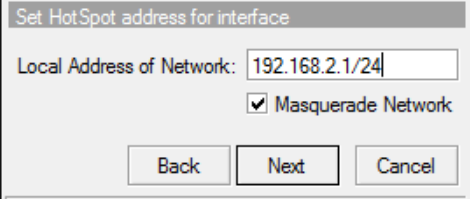
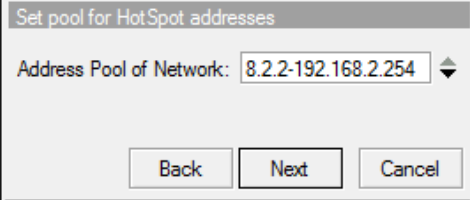
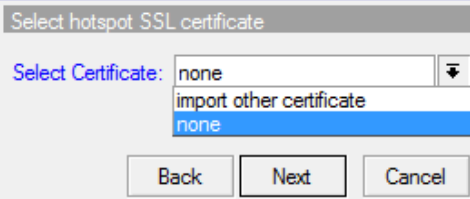
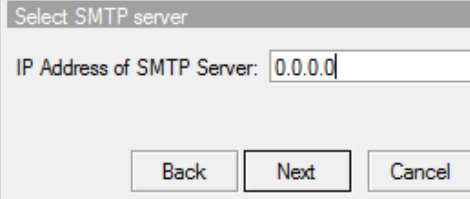
Penggunaan hotspot dihitung berdasarkan Time, Data Up/Down (Volume). Selain itu dapat juga dilakukan limited bandwidth berdasarkan keduanya.

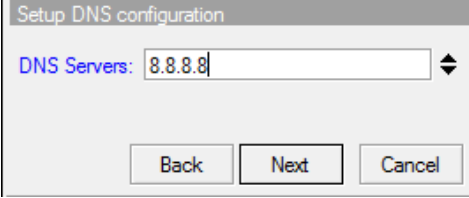
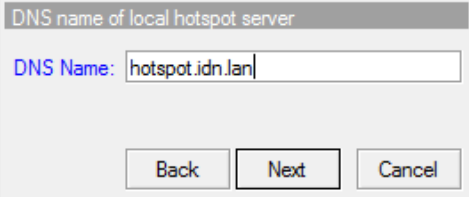
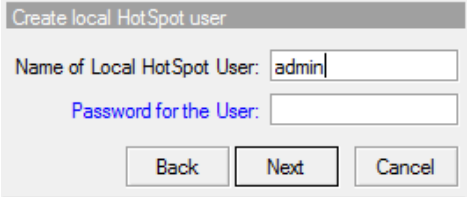
Topology



Setup Hotspot

Menu : IP > Hotspot > Servers > Hotspot Setup

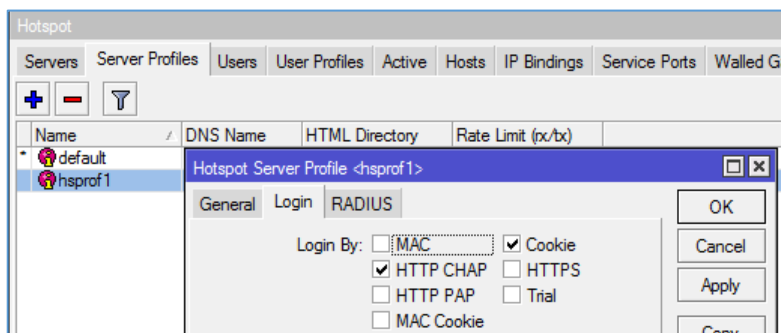
No	Keterangan	Gambar
1	Interface Hotspot, selain kabel dan nirkabel, hotspot juga bisa dipasang pada Virtual AP.	
2	LAN Address (IP Address jaringan LAN) NAT (Jika ingin di NAT otomatis, check opsi Masquerade).	
3	Address Pool (Range IP)	
4	Certificate (None), SSL certificate/https	
5	SMTP Address	

6	DNS Server	
7	DNS Name (Hotspot Domain), bisa dikosongkan jika tidak memiliki FQDN Domain.	
8	Hotspot User Account	

Hotspot sudah bisa running, namun beberapa parameter lain harus kita pelajari untuk memaksimalkan Hotspot di Mikrotik.

Hotspot Server Profile

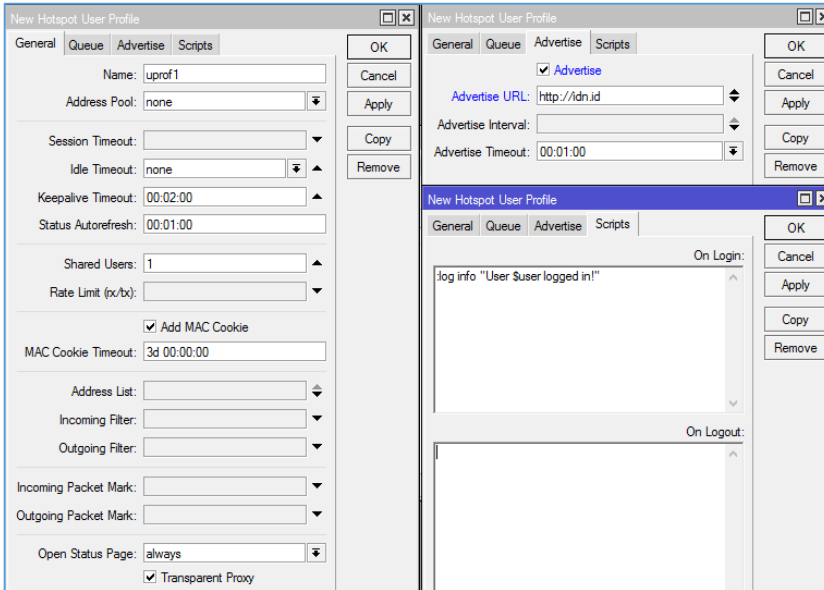
Fungsi : Menyimpan konfigurasi umum dari hotspot server. Profile ini digunakan untuk grouping beberapa hotspot server dalam 1 router juga terdapat konfigurasi yang berpengaruh pada user hotspot seperti Mode Autentikasi. 6 Mode Autentikasi



Mode	Keterangan
HTTP PAP	Menampilkan page hotspot login dan mengirimkan info login berupa plain text.
HTTP-CHAP	Mengintegrasikan proses Challenge Handshake Authentication Protocol pada proses login.
HTTPS	Menggunakan SSL untuk autentikasi.
HTTP Cookie	Setelah user berhasil login data cookie akan dikirimkan ke web browser dan disimpan oleh router di Active HTTP Cookie List yang akan digunakan untuk autentikasi selanjutnya.
MAC Address	Mengautentikasi user mulai dari user tersebut muncul di host list dan menggunakan MAC Address sebagai username dan password.
Trial	Tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.

Hotspot User Profile

Fungsi : Menyimpan konfigurasi umum dari group user yang memiliki pengaturan yang sama.



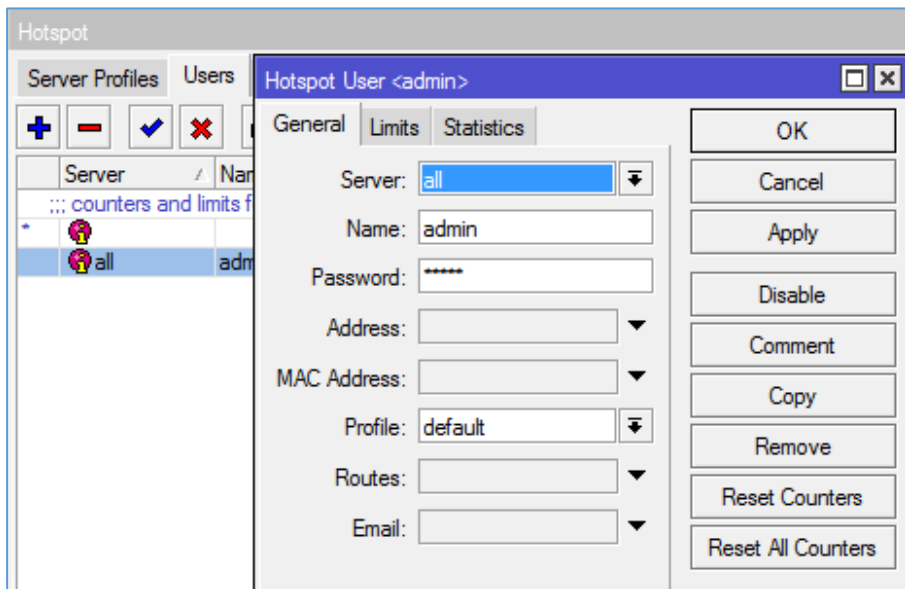
Option	Value
Address List	Nama daftar alamat dimana pengguna IP ditambahkan. Digunakan untuk menandai traffic per group untuk konfigurasi queue tree.
Address Pool	Range IP yang akan diberikan ke user.
Advertise	Otomatis muncul halaman iklan setelah interval tertentu dan selama interval tertentu. Page mungkin akan terblok oleh Popup Blocker pada browser.
Script	Logging / Debug user login, misal pada script on login ditambahkan script :log info "User \$user logged in!"

Coba setting supaya login dan logout tercatat dalam log.

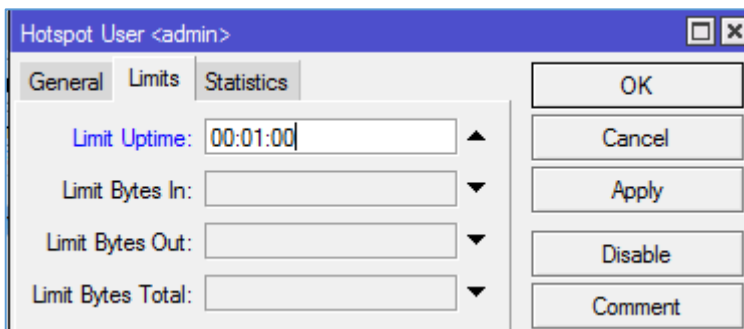
User Profile

Halaman dimana username, password, dan profile disimpan. Beberapa limitasi yang ditentukan di page ini adalah :

- Uptime Limit & Bytes – in /Bytes – Out. Jika telah mencapai limitasi maka user tersebut akan expired dan tidak dapat digunakan lagi.
- IP Address yang spesifik bisa diberikan kepada user tertentu. Selain itu juga bisa dibatasi dengan MAC Address.



Parameter Limits :



Keterangan

Parameter	Keterangan
Limit Uptime	Batas waktu user untuk dapat menggunakan akses hotspot
Limit Bytes In/Out	Batas transfer dan receive data yang bisa dilakukan user.
Limit Byte Total	Total jumlah transfer & receive data

Cobalah

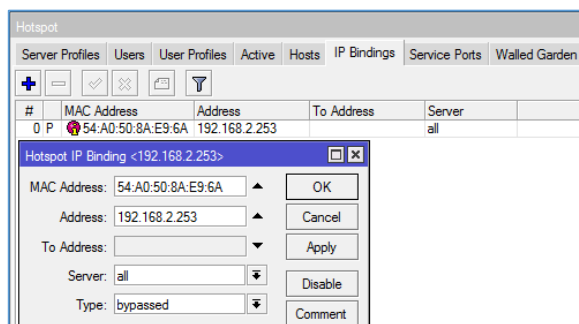
Batasi user1 agar hanya memiliki quota waktu 1 menit, dan coba login menggunakan profile tersebut selama lebih dari 1 menit.

Check pemakaian kuota

<http://<ip/domain>hotspot/status>

IP Bindings

Adalah one to one NAT, digunakan untuk bypass autentikasi user untuk akses all resource. Berdasarkan IP / MAC Address Client atau Keduanya.



Cobalah

Bypass IP/MAC Address laptop anda agar dapat langsung akses internet tanpa autentikasi hotspot.

Walled Garden

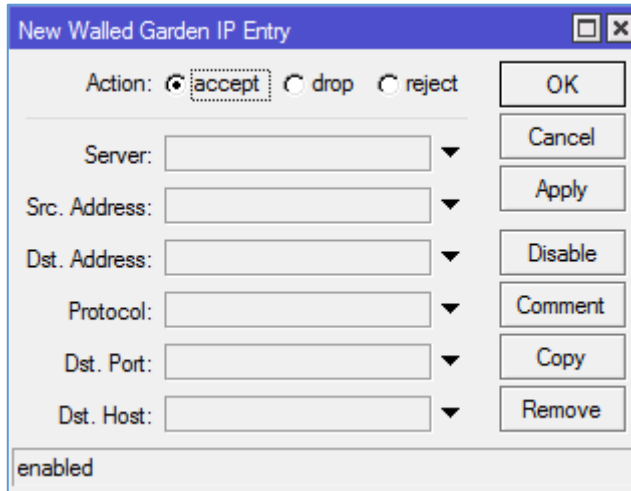
Adalah sebuah system yang memungkinkan untuk user yang belum terautentikasi menggunakan (Bypass!) beberapa resource jaringan, khususnya protocol http dan https, untuk protocol lain dapat juga, namun lebih spesifik diatur dalam walled

garden IP. Walled Garden biasanya digunakan untuk akses web server pada LAN.

Property	Description
action (<i>allow</i> <i>deny</i> ; Default: allow)	Action to perform, when packet matches the rule <ul style="list-style-type: none"> allow - allow access to the web-page without authorization deny - the authorization is required to access the web-page
server (<i>string</i> ; Default:)	Name of the HotSpot server, rule is applied to.
src-address (<i>IP</i> ; Default:)	Source address of the user, usually IP address of the HotSpot client
method (<i>string</i> ; Default:)	HTTP method of the request
dst-host (<i>string</i> ; Default:)	Domain name of the destination web-server
dst-port (<i>integer</i> ; Default:)	TCP port number, client sends request to
path (<i>string</i> ; Default:)	The path of the request, path comes after "http://dst_host/"

Walled Garden IP

Fungsi hampir sama dengan Walled Garden, tetapi fitur ini mampu melakukan bypass terhadap protocol dan port selain http dan https, misalkan telnet, ssh, winbox.



The image shows a dialog box titled "New Walled Garden IP Entry". It contains the following fields and controls:

- Action:** Radio buttons for "accept" (selected), "drop", and "reject".
- Server:** A text input field with a dropdown arrow.
- Src. Address:** A text input field with a dropdown arrow.
- Dst. Address:** A text input field with a dropdown arrow.
- Protocol:** A text input field with a dropdown arrow.
- Dst. Port:** A text input field with a dropdown arrow.
- Dst. Host:** A text input field with a dropdown arrow.
- Buttons:** "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove".
- Status:** A checkbox labeled "enabled" which is checked.

Edit Tampilan Hotspot Login

Folder Script : /hotspot/login.html

- Download file tersebut dengan cara drag & drop ke PC dan edit html sesuai dengan keinginan anda.
- Upload kembali setelah selesai diedit beserta image file yang digunakan (apabila ada).