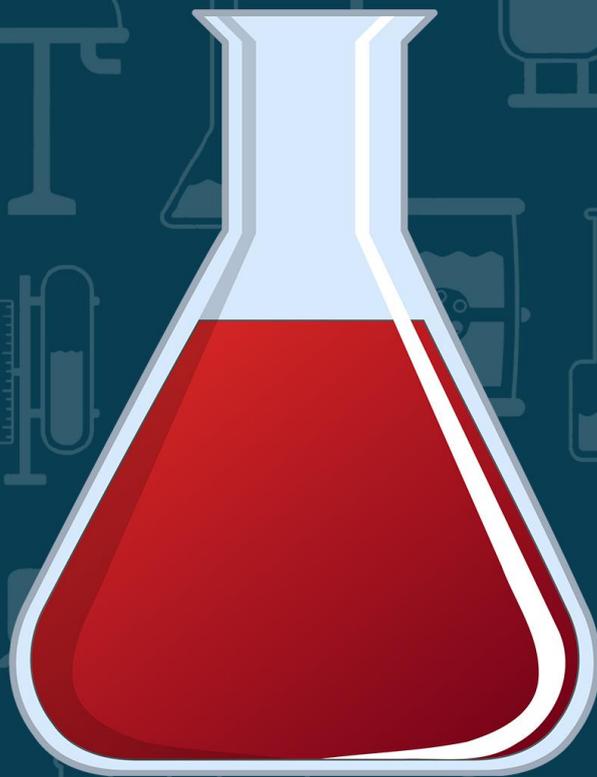


EDISI 2

ngeLab mikrotik



Arief Wahyudin

KATA PENGANTAR

Syukur alhamdulillah Allah SWT masih memberikan nikmat kepada kita semua, sehingga saat ini masih dapat menikmati belajar dan berbagi ilmu.

Ngelab MikroTik Edisi Ke-2 adalah modul yang digunakan untuk kegiatan Ngebar MikroTik Ke-2 pada tanggal 26 dan 27 Maret 2017. Ngelab MikroTik mengacu pada *Outline MTCNA* dan *MTCRE* yang ada di web resmi MikroTik (www.mikrotik.com).

Tujuan dari dibuatnya modul ini adalah untuk memudahkan peserta Ngebar MikroTik Ke-2 dalam memahami teori dan konsep dari materi *MTCNA* dan *MTCRE*, seperti materi *Model OSI Layer*, *Model TCP/IP*, *Subnetting*, *IP Address*, *Subnetting*, *Firewall*, *Wireless*, *Bridging*, *Routing*, *Tunnel*, dan *Network Management*.

Modul ini masih sangat jauh dari kata sempurna karena penyusunannya adalah hasil praktik secara mandiri, oleh karena itu saya selaku penulis modul ini sangat mengharapkan masukan untuk meningkatkan bobot dari modul ini agar kedepannya dapat diperbaiki menjadi lebih baik dan dapat membantu bagi siapa saja yang ingin belajar MikroTik.



Jombang, 26 Maret 2017

Arief Wahyudin

DAFTAR ISI

| | | |
|--------------|--|------------|
| I. | NETWORKING FUNDAMENTALS | 1 |
| | L1.1. 7 Layer OSI | 2 |
| | L1.2. 5 Layer TCP/IP | 3 |
| | L1.3. IPv4 | 4 |
| | L1.4. Subnetting IPv4 | 7 |
| II. | MIKROTIK FUNDAMENTALS | 10 |
| | L2.1. Mengakses Mikrotik | 11 |
| | L2.2. System Identity Mikrotik..... | 17 |
| | L2.3. Versi Mikrotik | 19 |
| | L2.4. Fitur Mikrotik..... | 20 |
| | L2.5. Enable dan Disable Fitur Mikrotik..... | 20 |
| | L2.6. User Management | 21 |
| | L2.7. Backup dan Restore | 23 |
| | L2.8. Export dan Import Konfigurasi Mikrotik | 24 |
| | L2.9. Reset Mikrotik | 26 |
| | L2.10. IP Address Mikrotik..... | 26 |
| III. | FIREWALL | 30 |
| | L3.1. NAT | 31 |
| | L3.2. Firewall Logging Mikrotik..... | 34 |
| | L3.3. Filter Rule | 35 |
| | L3.4. Content | 39 |
| | L3.5. Address List | 43 |
| | L3.6. Layer 7 Protocols..... | 48 |
| | L3.7. Transparent DNS | 52 |
| | L3.8. Transparent Web Proxy..... | 54 |
| | L3.9. Redirect..... | 60 |
| IV. | WIRELESS..... | 61 |
| | L4.1. Access Point Bridge (Pemancar) | 63 |
| | L4.2. Station (Penerima)..... | 68 |
| | L4.3. Station Bridge (Penerima) | 72 |
| | L4.4. Virtual Access Point Bridge | 73 |
| V. | BRIDGE..... | 76 |
| | L5.1. Wired Bridge | 77 |
| | L5.2. Wireless Bridge | 80 |
| VI. | ROUTING | 82 |
| | L6.1. Static Routing..... | 83 |
| | L6.2. Dinamic Routing (RIPv2) | 86 |
| VII. | TUNNEL..... | 89 |
| | L7.1. PPPoE Tunnel..... | 90 |
| VIII. | NETWORK MANAGEMENT | 96 |
| | L8.1. Wireless Mac Address Filtering..... | 97 |
| | L8.2. Wireless Nstreame | 99 |
| | L8.3. Hotspot..... | 100 |
| IX. | NETWORK SIMULATION | 104 |
| | L9.1. Instalasi Loopback Adapter GNS3 di Windows | 105 |

LABORATORIUM 1



NETWORKING FUNDAMENTALS

L1.1. 7 LAYER OSI

Open System Interconnection atau disingkat OSI adalah sebuah model yang digunakan untuk membantu desainer jaringan dalam memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. *Layer OSI* adalah model arsitektural jaringan yang dikembangkan oleh Badan *International Organization of Standardization* (ISO) di wilayah Eropa pada tahun 1977.

| NO | NAMA | DATA | DEVICE |
|----|--------------|--------|----------|
| 7 | APPLICATION | DATA | SOFTWARE |
| 6 | PRESENTATION | DATA | SOFTWARE |
| 5 | SESSION | DATA | SOFTWARE |
| 4 | TRANSPORT | SEGMEN | SOFTWARE |
| 3 | NETWORK | PAKET | ROUTER |
| 2 | DATA LINK | FRAME | SWITCH |
| 1 | PHYSICAL | BIT | HUB |

Layer OSI

Model OSI secara konseptual terbagi ke dalam tujuh lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik.

Berikut adalah tujuh *layer* OSI :

- **Layer 7 Application**
Layer ini menyediakan layanan untuk aplikasi pengguna, selain itu *layer* ini bertanggungjawab terhadap pertukaran informasi antara program komputer. Data pada *layer* ini berbentuk data.
- **Layer 6 Presentation**
Layer ini menyediakan layanan pengkonversian dan pemformatan data sebelum di transfer. *Layer* ini membentuk kode konversi, kode translasi, dan enkripsi. Data pada *layer* ini berbentuk data.
- **Layer 5 Session**
Layer ini menentukan bagaimana dua terminal menjaga, memelihara, dan mengatur koneksi agar saling berhubungan satu sama lain. Data pada *layer* ini berbentuk data
- **Layer 4 Transport**
Layer ini membagi data menjadi segmen, menjaga koneksi logika “*end-to-end*” antar terminal, dan menyediakan penanganan *error*. *Layer* ini juga bertanggung jawab mencari jalur (*routing*) yang

kosong untuk transmisi data. Data pada *layer* ini berbentuk segmen.

- **Layer 3 Network**

Layer ini menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, dan menjaga antrian trafik di jaringan. Data pada layer ini berbentuk paket dan perangkat yang ada pada layer network adalah router. Pada Layer ini pengalamatan yang digunakan dalam bentuk desimal seperti 192.168.1.0.

- **Layer 2 Data Link**

Layer ini menyediakan link untuk data, memaketkan data menjadi *frame* yang berhubungan dengan hardware, komunikasinya dengan kartu jaringan, mengatur komunikasi *layer physical* antara sistem koneksi dan penanganan *error*. Data pada *layer* ini berbentuk *frame* dan perangkat yang ada pada *layer* ini adalah switch. Pada *layer* ini pengalamatan yang digunakan dalam bentuk heksadesimal seperti A1-B2-C3-D3-E4-88.

- **Layer 1 Physical**

Leyer ini bertanggung jawab terhadap proses data menjadi bit dan mentransfernya melalui media dan menjaga koneksi fisik antar sistem. Data pada layer ini berbentuk bit dan perangkat yang ada pada layer ini adalah hub kabel kabel jaringan. Pada layer ini pengalamatan yang digunakan dalam bentuk biner seperti 11110000.

L1.2. 4 LAYER TCP/IP

Transmission Control Protocol/Internet Protocol atau disingkat TCP/IP adalah standar komunikasi data atau protocol yang digunakan dalam internet dalam proses tukar-menukar data dari satu komputer ke komputer lainnya. Protokol TCP/IP dikembangkan pada tahun 1970 hingga 1980 oleh *Defense Advance Research projects Agency* (DARPA).

| NO | NAMA |
|----|-------------|
| 5 | APPLICATION |
| 4 | TRANSPORT |
| 3 | NETWORK |
| 2 | DATA LINK |
| 1 | PHYSICAL |

Layer TCP/IP

Menurut dokumen RFC 1122 model lapisan protocol TCP/IP terdiri dari empat lapisan. Tidak seperti model OSI model TCP/IP bukan standar internasional sehingga banyak sumber yang menambahkan lapisan fisik di dalam model TCP/IP. Model TCP/IP antara lain sebagai berikut :

- **Layer 5 Application**
Layer ini bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan.
- **Layer 4 Transport**
Layer ini bertanggung jawab menjamin data akan sampai dan berurutan ke tujuan. Jika ada data yang hilang, maka layer ini menyediakan mekanisme untuk meminta dan mengirim data ulang.
- **Layer 3 Network**
Layer ini bertanggung jawab mengatur perjalanan paket dari melewati banyak jaringan dengan berbagai media fisik yang berbeda. Informasi yang diberikan hanya IP address sumber dan tujuan.
- **Layer 2 Data Link**
Layer ini bertanggung jawab mengatur komunikasi antara dua komputer yang menggunakan saluran fisik yang sama.
- **Layer 1 Physical**
Layer ini bertanggung jawab menyalurkan data dari satu titik ke titik lain secara fisik.

L1.3. IPv4

IP Address versi 4 (IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IPv4. IPv4 memiliki panjang 32 bit dan dibagi menjadi 4 blok. Masing-masing blok berukuran 8 bit dan ditulis

dalam bilangan desimal dengan nilai berkisar antara 0 hingga 255. IPv4 ditulis dalam notasi desimal bertitik yang dibagi ke dalam empat buah oktet dengan masing-masing berukuran 8 bit. Format notasi tersebut dikenal dengan *dotted-decimal format*.

IP Address adalah deretan bilangan biner (32 bit atau 128 bit) yang unik dan digunakan sebagai identitas untuk host dalam jaringan komputer



| | | | | | | | | |
|---------|---|----------|---|----------|---|----------|---|----------|
| OKTET | : | OKTET 1 | . | OKTET 2 | . | OKTET 3 | . | OKTET 4 |
| BINER | : | 11111111 | . | 11111111 | . | 11111111 | . | 00000000 |
| DESIMAL | : | 255 | . | 255 | . | 255 | . | 0 |

IP Address versi 4

a. Jenis IP versi 4 berdasarkan identitasnya

IPv4 yang dimiliki oleh sebuah *host* dapat dibagi dengan menggunakan *subnet mask* jaringan ke dalam dua buah bagian, yakni:

1) Network Identifier (NetID) atau Network Address.

NetID adalah alamat yang digunakan khusus untuk mengidentifikasi alamat jaringan di mana *host* berada.

2) Host Identifier (HostID) atau Host address.

HostID adalah alamat yang digunakan khusus untuk mengidentifikasi alamat *host*.

b. Jenis IP versi 4 berdasarkan ketentuan penggunaannya

Berdasarkan ketentuan penggunaannya IPv4 terbagi menjadi beberapa jenis, yakni sebagai berikut:

1) Alamat Unicast

Alamat *unicast* merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah *internetwork* IP. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one*. Alamat *unicast* menggunakan kelas A, B, dan C dari kelas-kelas alamat IPv4. Sebuah alamat *unicast* dibedakan dengan alamat lainnya dengan menggunakan *subnet mask*.

Alamat *unicast* dibagi menjadi dua, yaitu alamat publik dan alamat privat

- Alamat Publik

Alamat publik adalah alamat-alamat yang telah ditetapkan dan berisi beberapa buah *network identifier* yang telah

dijamin unik jika *intranet* tersebut telah terhubung ke *Internet*.

- **Alamat Privat**

Alamat Privat adalah alamat IP yang berada di dalam ruangan alamat pribadi. Sebuah jaringan yang menggunakan alamat IP privat disebut juga dengan jaringan privat atau *private network*.

2) **Alamat Multicast**

Alamat *multicast* merupakan alamat IPv4 yang didesain agar diproses oleh satu atau beberapa *node* dalam segmen jaringan yang sama atau berbeda. Alamat multicast digunakan dalam komunikasi *one-to-many*. Alamat-alamat *multicast* IPv4 didefinisikan dalam ruang alamat kelas D dalam kelas IPv4.

3) **Alamat Broadcast**

Alamat *broadcast* merupakan alamat IPv4 yang didesain agar diproses oleh setiap *node* dalam segmen jaringan yang sama. Alamat *broadcast* digunakan dalam komunikasi *one-to-everyone*. Jenis-jenis alamat *broadcast* antara lain sebagai berikut :

- *Network Broadcast*

Network broadcast IPv4 adalah alamat yang dibentuk dengan cara mengkonfigurasi semua *bit host* menjadi 1 dalam sebuah alamat yang menggunakan kelas (*classful*).

- *Subnet Broadcast*

Subnet broadcast adalah alamat yang dibentuk dengan cara mengeset semua *bit host* menjadi 1 dalam sebuah alamat yang tidak menggunakan kelas (*classless*)

- *All Subnets Directed Broadcast*

All subnets directed broadcast adalah alamat *broadcast* yang dibentuk dengan mengkonfigurasi semua *bit-bit network identifier* yang asli yang berbasis kelas menjadi 1 untuk sebuah jaringan dengan alamat tak berkelas (*classless*).

- *Limited Broadcast*

Limited broadcast adalah alamat yang dibentuk dengan mengkonfigurasi 32 bit alamat IPv4 menjadi 1. Alamat ini digunakan ketika sebuah *node* IP harus melakukan penyampaian data secara *one-to-everyone* di dalam sebuah jaringan lokal tetapi ia belum mengetahui *network identifier*-nya.

c. **Jenis IP versi 4 berdasarkan kelasnya**

Dalam RFC 791 alamat IPv4 dibagi ke dalam lima kelas.

| Kelas Alamat IP | Oktet Pertama | | Untuk |
|-----------------|---------------|------------|------------------------|
| | Desimal | Biner | |
| Kelas A | 1 s.d 126 | 0xxxxxxxx | Unicast skala besar |
| Kelas B | 128 s.d 191 | 10xxxxxxxx | Unicast skala menengah |
| Kelas C | 192 s.d 223 | 110xxxxxx | Unicast skala kecil |
| Kelas D | 224 s.d 239 | 1110xxxxx | Multicast |
| Kelas E | 240 s.d 255 | 1111xxxxx | Eksperimen |

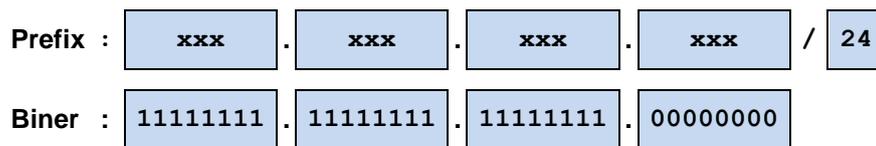
d. Format Prefix IP versi 4

Dalam IPv4 sebuah alamat dapat direpresentasikan dengan menggunakan angka prefiks yang merujuk kepada *subnet mask* yang digunakan. *Prefix* adalah sebuah bagian dari IP yang memiliki nilai-nilai tetap dan menjadi bagian dari sebuah rute atau *subnet identifier*.



Format *Prefix* IPv4

Panjang *prefix* menentukan jumlah bit terbesar paling kiri yang membuat *prefix subnet*. Jika dalam sebuah IPv4 menggunakan *prefix /24* maka jumlah bit 1 dari 32 bit deretan bilangan biner berjumlah 24.



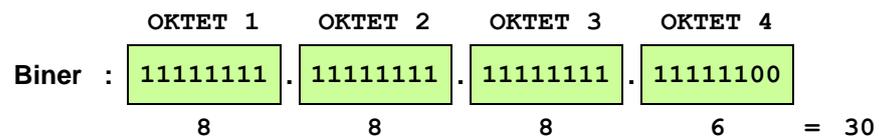
Jumlah bit 1 berdasarkan *prefix*

L1.4. SUBNETTING (IPv4)

Subnetting adalah cara untuk menentukan jumlah penggunaan *IP Address* yang paling sesuai dengan kebutuhan atau jumlah *host* yang ada dalam jaringan. Ketika mendengar *subnetting* umumnya yang ditanyakan atau dicari adalah jumlah *host per subnet*, jumlah *ip address per subnet*, jumlah blok *subnet, network, host, dan broadcast*. Untuk menjawab pertanyaan tersebut umumnya yang digunakan adalah *prefix* atau *netmask* yang digunakan.

| PREFIX | NETMASK | PREFIX | NETMASK |
|--------|---------------|--------|-----------------|
| /8 | 255.0.0.0 | /20 | 255.255.240.0 |
| /9 | 255.128.0.0 | /21 | 255.255.248.0 |
| /10 | 255.192.0.0 | /22 | 255.255.252.0 |
| /11 | 255.224.0.0 | /23 | 255.255.254.0 |
| /12 | 255.240.0.0 | /24 | 255.255.255.0 |
| /13 | 255.248.0.0 | /25 | 255.255.255.128 |
| /14 | 255.252.0.0 | /26 | 255.255.255.192 |
| /15 | 255.254.0.0 | /27 | 255.255.255.224 |
| /16 | 255.255.0.0 | /28 | 255.255.255.240 |
| /17 | 255.255.128.0 | /29 | 255.255.255.248 |
| /18 | 255.255.192.0 | /30 | 255.255.255.252 |
| /19 | 255.255.224.0 | | |

Perlu diketahui netmask diperoleh dari prefix, misal IP Address 192.168.1.0 dengan prefix 30 atau umumnya ditulis dengan 192.168.1.0/30 maka netmasknya adalah hasil dari penghitungan nilai biner dari prefix. Prefix /30 memiliki arti jumlah bit 1 dari total 32 bit IPv4 ada 30 dan jika ditulis sebagai berikut



Setelah total bit 1 tiap-tiap oktet diketahui maka dapat dilakukan konversi bilangan dari biner ke desimal

| | | | | | | | | | |
|----------------|----------|------------|-----------|-----------|-----------|----------|----------|----------|----------|
| Bit ke | : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Biner | : | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Desimal | : | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

| | OKTET 1 | OKTET 2 | OKTET 3 | OKTET 4 |
|----------------|------------|------------|------------|------------|
| Biner | : 11111111 | . 11111111 | . 11111111 | . 11111100 |
| Desimal | : 255 | . 255 | . 255 | . 252 |

Dari tahapan tersebut dapat diketahui bahwa netmask dari 192.168.1.0/30 adalah 255.255.255.252

Setelah mengetahui prefix dan Netmask maka dapat digunakan untuk mengetahui jumlah *ip address*, jumlah *host address*, *network*, dan *broadcast*. Berikut adalah cara untuk menentukan ip address, jumlah host, network, dan host pada IPv4 kelas C

IP Address 192.168.1.1/30
 Netmask 255.255.255.0

Jumlah IP Address adalah 256 dikurangi nilai desimal oktet ke-4
 $256 - 252 = 4$ IP Address

Jumlah Host Address adalah jumlah IP Address dikurangi 2, 2 adalah IP Address Network dan dan IP Address Broadcast.
 $4 - 2 = 2$ Host Address

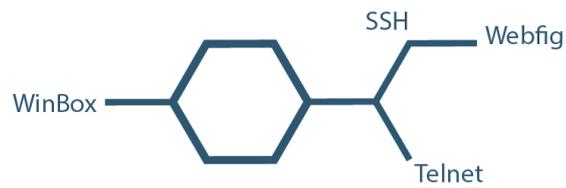
Blok subnet adalah urutan IP Address sesuai jumlah IP Address, Blok Subnet Ke-1nya adalah

IP Address Ke-1 192.168.1.0
 IP Address Ke-2 192.168.1.1
 IP Address Ke-3 192.168.1.2
 IP Address Ke-4 192.168.1.3

Network Address adalah IP Address yang paling atas atau pertama, jadi Network Address adalah 192.168.1.0

Broadcast Address adalah IP Address yang paling bawah atau terakhir, jadi Broadcast Address adalah 192.168.1.3

LABORATORIUM 2



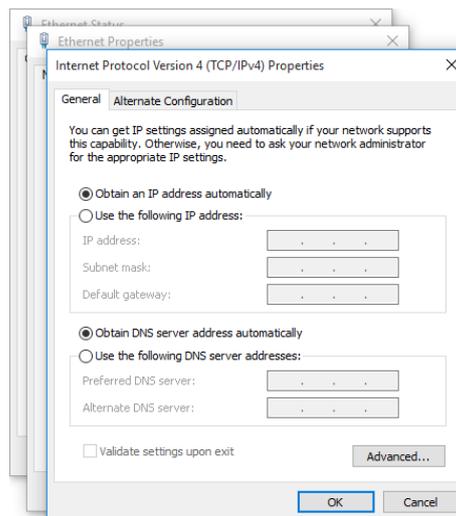
MIKROTIK FUNDAMENTALS

L2.1. MENGAKSES MIKROTIK

Perlu Anda ketahui ada banyak cara untuk mengakses Mikrotik, berikut adalah daftar cara mengakses MikroTik,

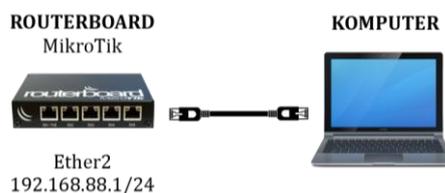
| NO | VIA | KONEKSI | TEXT | GUI | IP |
|----|--------------------|----------------|------|-----|----|
| 1 | WinBox | Sistem Operasi | ✓ | ✓ | ✓ |
| 2 | WinBox (MAC) | Layer 2 | ✓ | ✓ | - |
| 3 | Web | Layer 3 | ✓ | ✓ | ✓ |
| 4 | Telnet (CMD/PuTTY) | Layer 3 | ✓ | - | ✓ |
| 5 | Telnet (MAC) | Layer 2 | ✓ | - | - |
| 6 | SSH (PuTTY) | Layer 3 | ✓ | - | ✓ |

Yang perlu Anda lakukan sebelum menghubungkan *Routerboard* (RB) Mikrotik ke Komputer adalah memastikan *IP Address* pada Komputer Anda dalam keadaan kosong atau *obtain*.



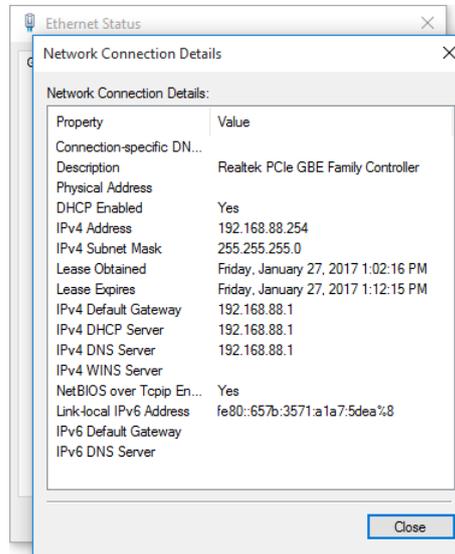
Ethernet Properties dalam kondisi *obtain*

Setelah itu Anda hubungkan komputer ke RB (*Ether 2*) seperti topologi berikut ini dengan menggunakan kabel UTP tipe *straight*.



Topologi Konfigurasi Mikrotik

Secara otomatis atau *default configuration ether 2* pada RB sudah dikonfigurasi menjadi DHCP Server. IP Pool yang diberikan kepada *client* atau komputer yang terhubung dengan RB mulai 192.168.88.2 hingga 192.168.88.254.



IP Address Ethernet Komputer
Yang diperoleh dari RB MikroTik

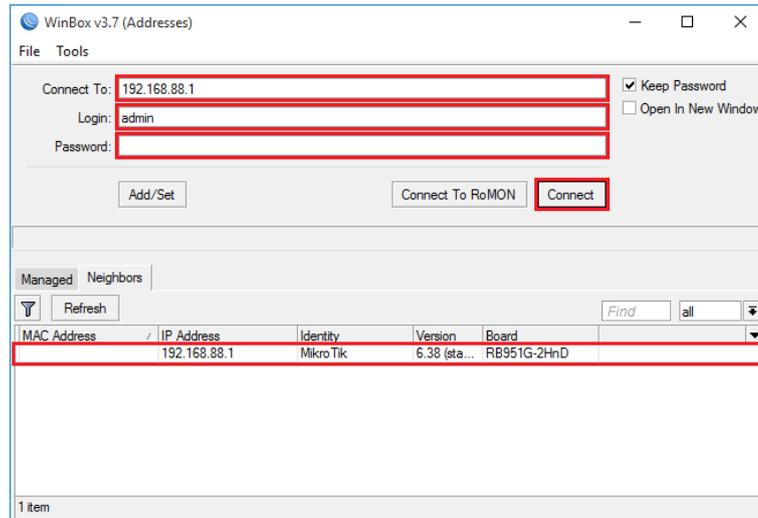
Selain itu *IP Address Ether 2* pada RB juga memiliki *IP Address default* yang juga menjadi *Gateway* yaitu 192.168.88.1

Pertama Anda dapat mengakses Mikrotik dengan menggunakan Aplikasi WinBox. Aplikasi WinBox dapat diperoleh langsung dari situs mikrotik.com atau dapat juga diperoleh dari RB MikroTik.



Icon Aplikasi *WinBox*

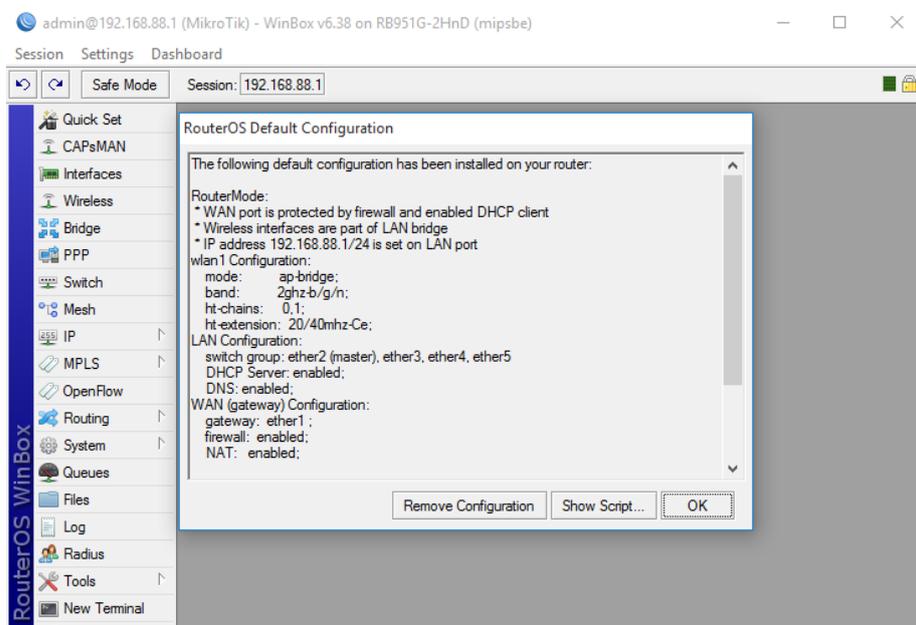
Selanjutnya Anda jalankan Aplikasi WinBox dan masukkan *IP Address, login, dan password default* yang digunakan Mikrotik.



Winbox Mikrotik

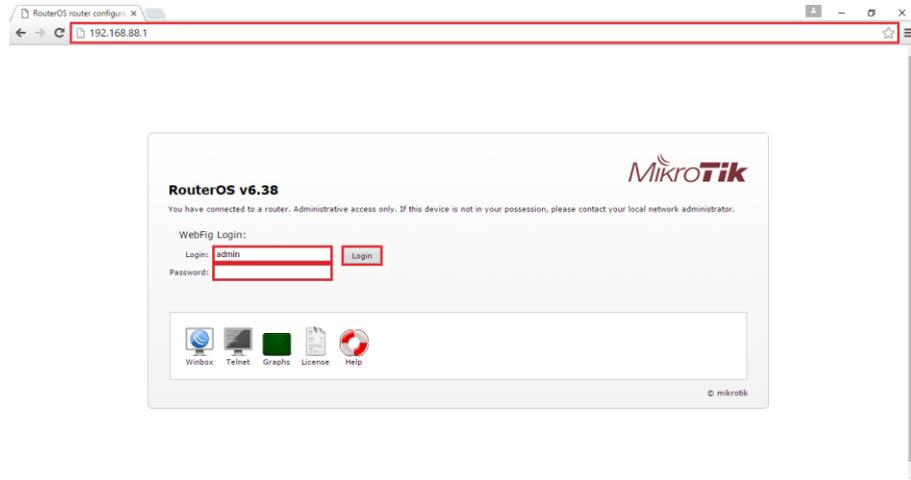
Secara default *username* yang digunakan pada Mikrotik adalah “admin” dan password yang digunakan adalah kosong atau tanpa password.

Setelah *ip address*, *username*, dan *password* dimasukkan langkah selanjutnya menekan tombol *Connect*.

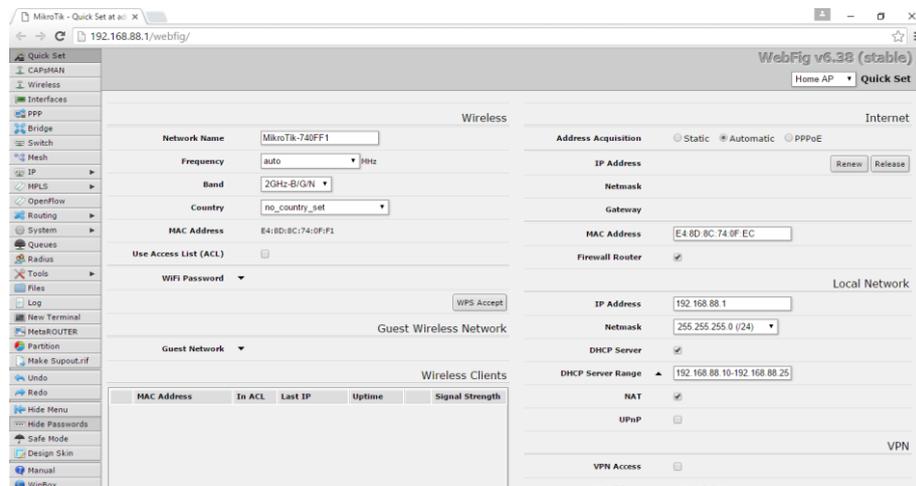


Jendela Konfigurasi Mikrotik melalui WinBox

Anda juga dapat mengakses MikroTik menggunakan *web browser* atau dikenal dengan *webfig (web configuration)*. Caranya dengan memasukkan *IP Address* MikroTik pada *browser* dan memasukkan *username* dan *password* lalu menekan tombol *Login*.



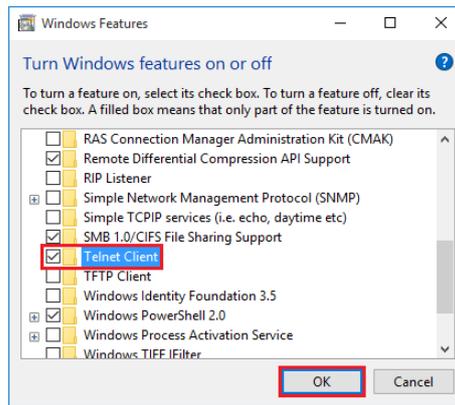
Halaman *Login* MikroTik pada *Browser*



Jendela konfigurasi MikroTik via *Browser*

Anda juga dapat mengakses MikroTik menggunakan Telnet. Telnet sendiri dapat diakses menggunakan **Command Prompt** pada Sistem Operasi Windows dan juga aplikasi **PuTTY**.

Sebelum mengakses MikroTik menggunakan Telnet melalui *Command Prompt* pastikan terlebih dahulu aplikasi telnet sudah aktif dengan cara masuk ke *Windows Features* dan memastikan *Folder Telnet (Client/Server)* dalam kondisi centang.

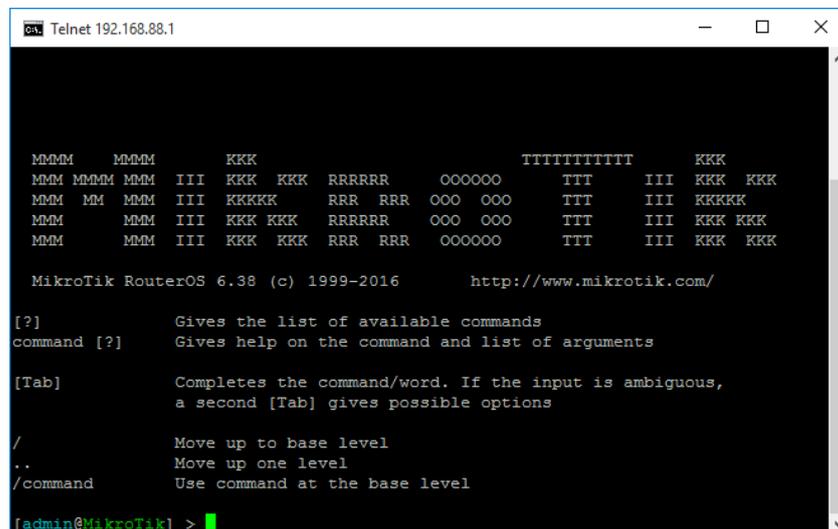


Jendela Windows Features

Selanjutnya buka *Command Prompt* dan menuliskan “telnet 192.168.88.1” dan menekan *enter*.

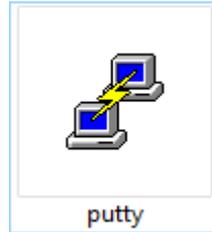


Telnet pada *Command Prompt*



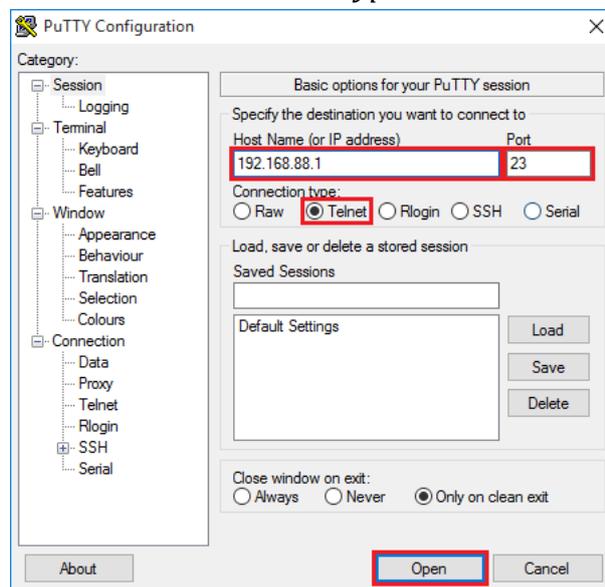
Jendela konfigurasi Mikrotik dengan Telnet

Sedangkan aplikasi selain *Command Prompt* yang dapat digunakan untuk mengkonfigurasi Mikrotik via Telnet dapat menggunakan aplikasi PuTTY

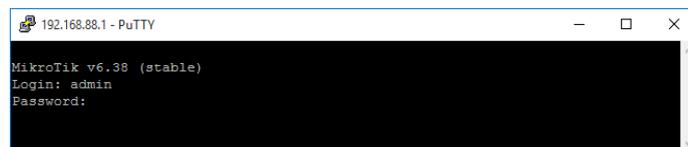


Icon Aplikasi **PuTTY**

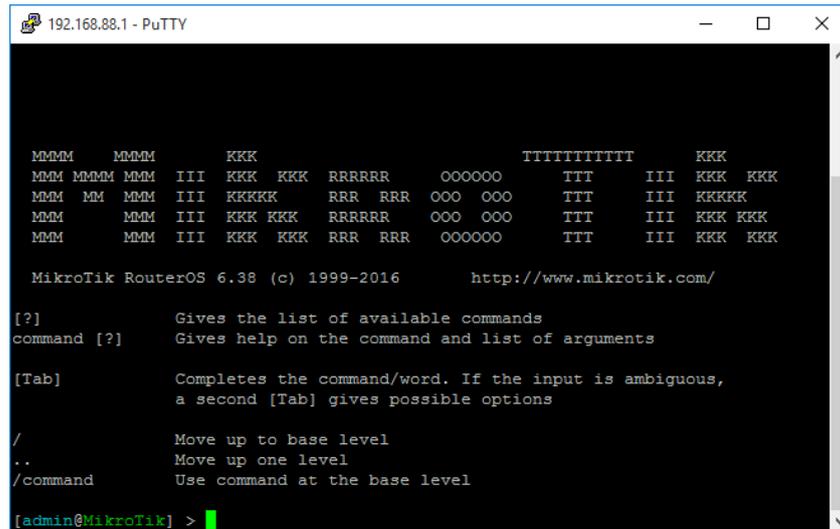
Anda cukup menjalankan Aplikasi **PuTTY** lalu memasukkan **IP Address** yang digunakan Mikrotik pada **Hostname** dan memilih **Telnet** pada **radio button Connection type** dan menekan tombol **Open**.



Mengakses Mikrotik via Telnet dengan PuTTY

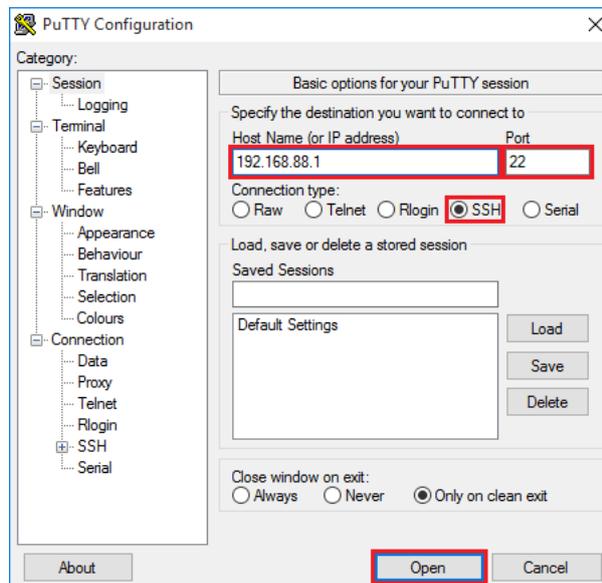


Telnet pada PuTTY



Jendela konfigurasi Mikrotik dengan Telnet

Anda juga dapat mengakses Mikrotik melalui SSH menggunakan *PuTTY*. Caranya hampir sama dengan *Telnet* hanya mengganti *Connection Type* dari *Telnet* menjadi *SSH*.

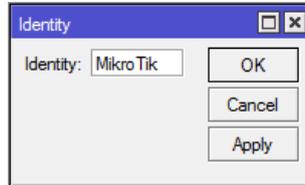


Mengakses MikroTik via Telnet dengan PuTTY

L2.2. SYSTEM IDENTITY MIKROTIK

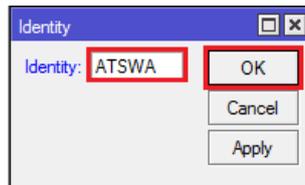
System Identity atau lebih umum dikenal dengan *hostname* adalah nama dari perangkat MikroTik. *System Identity* pada MikroTik dapat digunakan sebagai pembeda perangkat satu dengan perangkat lainnya. Perlunya untuk mengubah *default system identity* agar ketika

melakukan konfigurasi RB dengan jumlah banyak tidak terjadi kesalahan konfigurasi RB satu dengan RB lainnya.
 Jika Anda ingin mengubah *hostname* Mikrotik melalui WinBox caranya klik **System** lalu klik **Identity**.



Hostname default dari Mikrotik

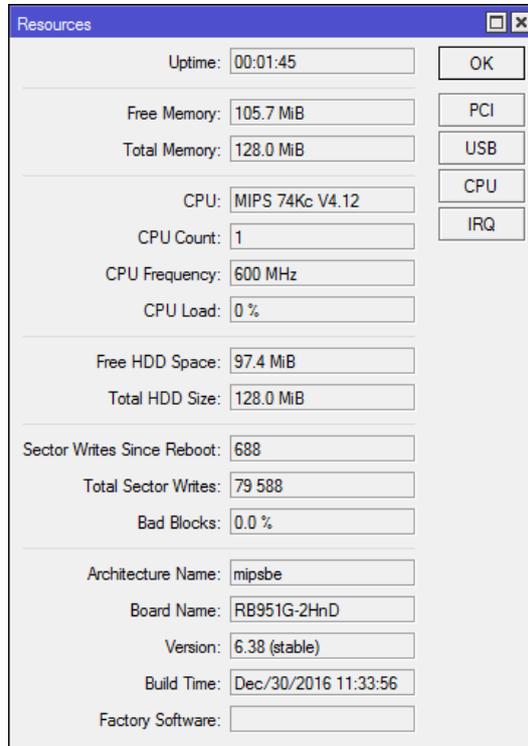
Setelah mengubah *hostname default* dengan *hostname* yang baru klik **OK**.



Hostname diubah menjadi ATSWA

L2.3. VERSI MIKROTIK

Anda dapat mengetahui versi MikroTik dengan cara klik **System** lalu klik **Resource**.

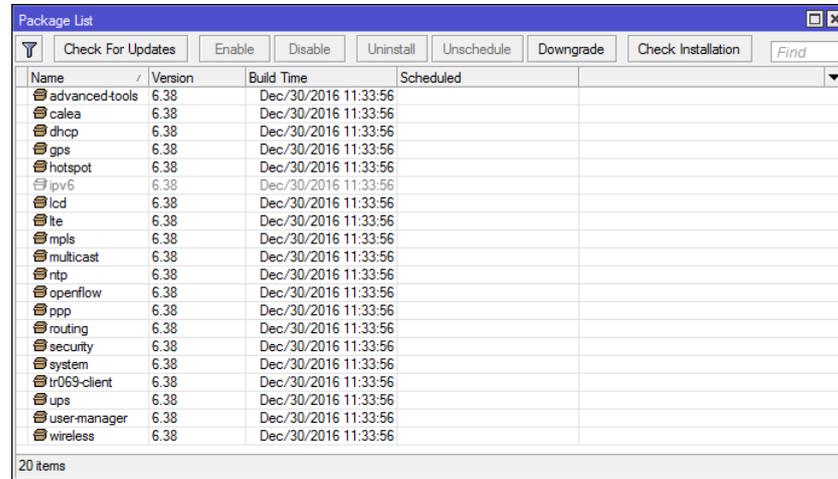


Jendela *Resources* pada WinBox Mikrotik

Selain dapat melihat versi dari sistem operasi Anda juga dapat melihat konsumsi system yang berjalan terhadap memory dan processor, kapasitas storage, arsitektur yang digunakan sistem operasi, serta seri motherboard.

L2.4. FITUR MIKROTIK

Anda dapat melihat fitur atau paket yang ada pada Mikrotik pada jendela *Package List*. Caranya klik menu **System** lalu klik **Packages**.



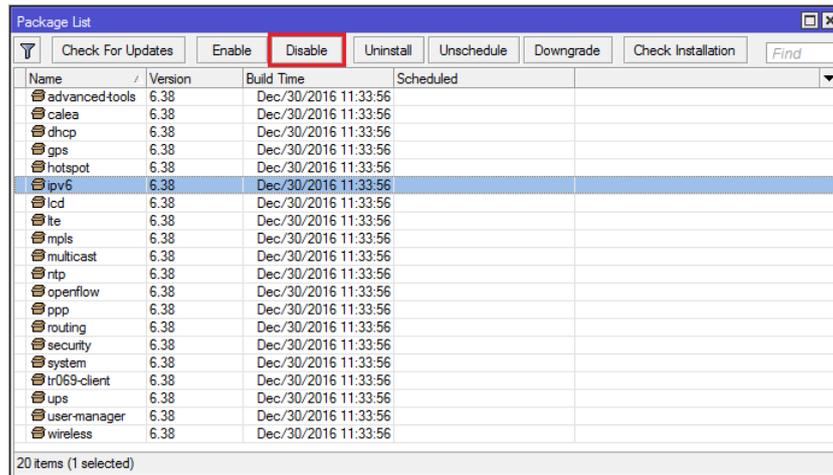
| Name | Version | Build Time | Scheduled |
|----------------|---------|----------------------|-----------|
| advanced-tools | 6.38 | Dec/30/2016 11:33:56 | |
| calea | 6.38 | Dec/30/2016 11:33:56 | |
| dhcp | 6.38 | Dec/30/2016 11:33:56 | |
| gps | 6.38 | Dec/30/2016 11:33:56 | |
| hotspot | 6.38 | Dec/30/2016 11:33:56 | |
| ipv6 | 6.38 | Dec/30/2016 11:33:56 | |
| lcd | 6.38 | Dec/30/2016 11:33:56 | |
| lte | 6.38 | Dec/30/2016 11:33:56 | |
| mpls | 6.38 | Dec/30/2016 11:33:56 | |
| multicast | 6.38 | Dec/30/2016 11:33:56 | |
| ntp | 6.38 | Dec/30/2016 11:33:56 | |
| openflow | 6.38 | Dec/30/2016 11:33:56 | |
| ppp | 6.38 | Dec/30/2016 11:33:56 | |
| routing | 6.38 | Dec/30/2016 11:33:56 | |
| security | 6.38 | Dec/30/2016 11:33:56 | |
| system | 6.38 | Dec/30/2016 11:33:56 | |
| tr069-client | 6.38 | Dec/30/2016 11:33:56 | |
| ups | 6.38 | Dec/30/2016 11:33:56 | |
| user-manager | 6.38 | Dec/30/2016 11:33:56 | |
| wireless | 6.38 | Dec/30/2016 11:33:56 | |

Jendela *Package List* pada WinBox Mikrotik

Pada jendela *Package List* Anda dapat melihat paket yang aktif dan terinstal pada sistem operasi Mikrotik, versi paket, serta tanggal paket tersebut di install.

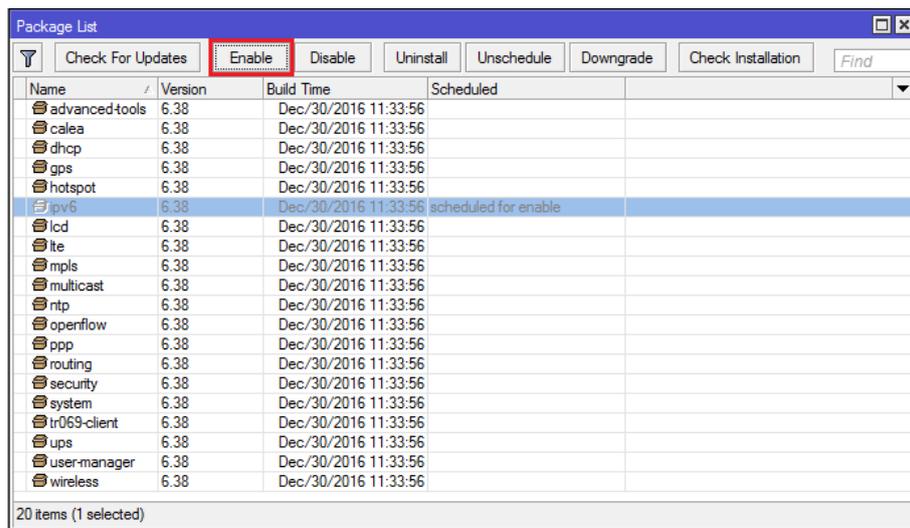
L2.5. ENABLE DAN DISABLE FITUR MIKROTIK

Anda dapat mengaktifkan dan menonaktifkan Fitur dalam Mikrotik sesuai kebutuhan. Selain itu tujuannya agar mengurangi konsumsi dari sistem operasi terhadap *memory* dan *processor*. Cara menonaktifkan atau *disable* fitur dengan cara masuk ke **Package List** terlebih dahulu lalu memilih paket yang akan di *disable* dan klik menu **Disable**. Setelah di *disable* *reboot* Mikrotik dengan cara klik **System** lalu klik **Reboot**.



Disable paket ipv6

Untuk mengaktifkan atau *enable* paket caranya kurang lebih sama hanya saja menu yang dipilih adalah **Enable**. Setelah itu **reboot** kembali mikrotik sama seperti seperti proses sebelumnya.

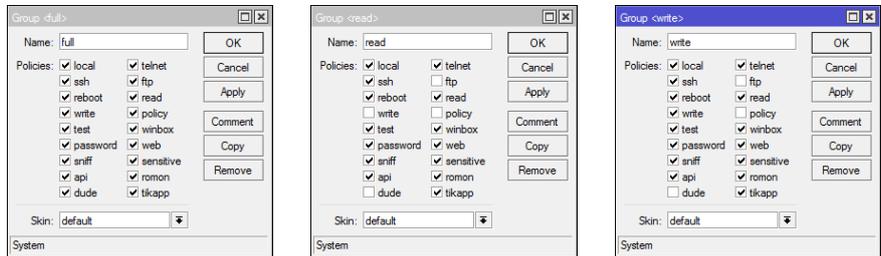


Enable paket ipv6

L2.6. USER MANAGEMENT

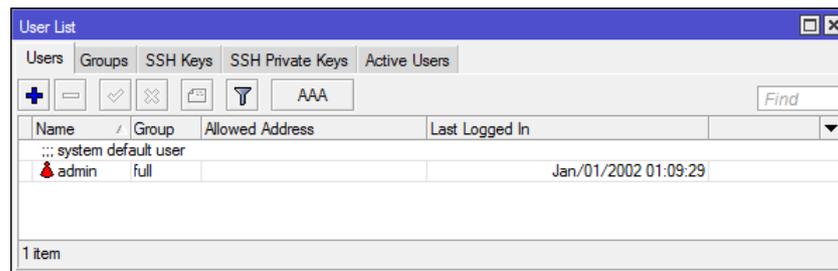
Mikrotik *User Manager* digunakan untuk mengatur hak akses bagi siapa saja yang ingin melihat dan memodifikasi konfigurasi MikroTik. MikroTik menyediakan pengaturan *user* serta *profile* hak akses. Secara *default* Mikrotik menyediakan tiga profil yaitu **read** (*hanya dapat melihat tanpa dapat mengubah*), **write** (*hanya dapat memodifikasi konfigurasi tanpa dapat melihat hasil*), dan **full** (*dapat*

melihat dan memodifikasi konfigurasi). MikroTik juga menyediakan satu user dengan nama **Admin** dengan profil **full**.



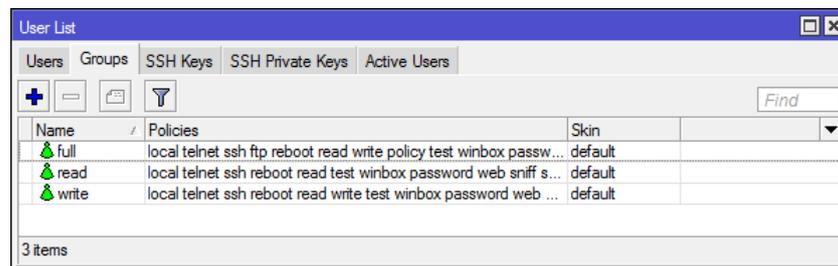
Daftar profil yang disediakan MikroTik

Anda dapat melihat atau memodifikasi pengaturan *user manager* dalam MikroTik dengan cara klik **System** lalu klik **User**.



Daftar User pada User List

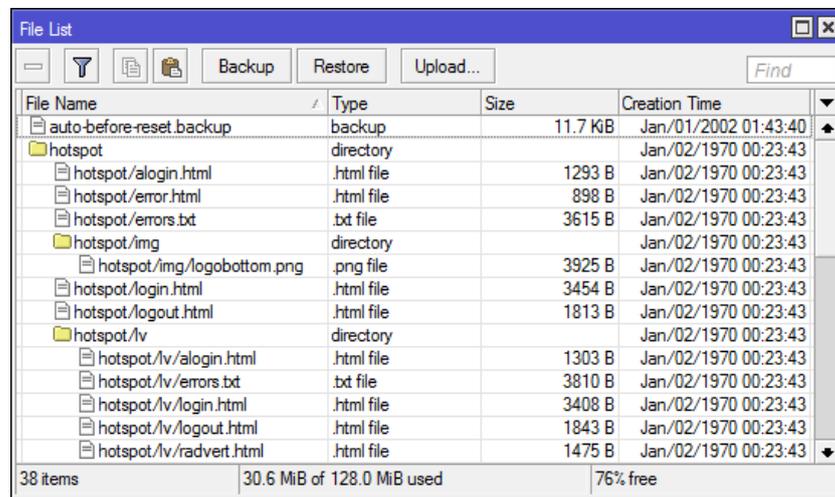
Pada bagian menu **User** terdapat daftar pengguna yang tersedia dan pada menu **Groups** terdapat profil user.



Daftar Group pada User List

L2.7. BACKUP DAN RESTORE KONFIGURASI

Mikrotik menyediakan fitur untuk melakukan *backup* dan *restore* konfigurasi yang ada dalam sistem operasi MikroTik. Manfaat dari *Backup* dan *Restore* adalah ketika terjadi kondisi dimana RB harus dikembalikan ke pengaturan awal atau *reset* maka seluruh konfigurasi yang sudah dilakukan otomatis akan hilang dan perlu dilakukan konfigurasi lagi dari awal hingga akhir. Jika *user* sudah melakukan *backup* konfigurasi maka meringankan ketika terjadi kondisi tersebut dan tidak perlu melakukan konfigurasi dari awal cukup dengan *restore* seluruh konfigurasi kembali seperti semula. Untuk melakukan Backup konfigurasi yang harus dilakukan adalah masuk ke **File List** dengan cara klik **Files**.



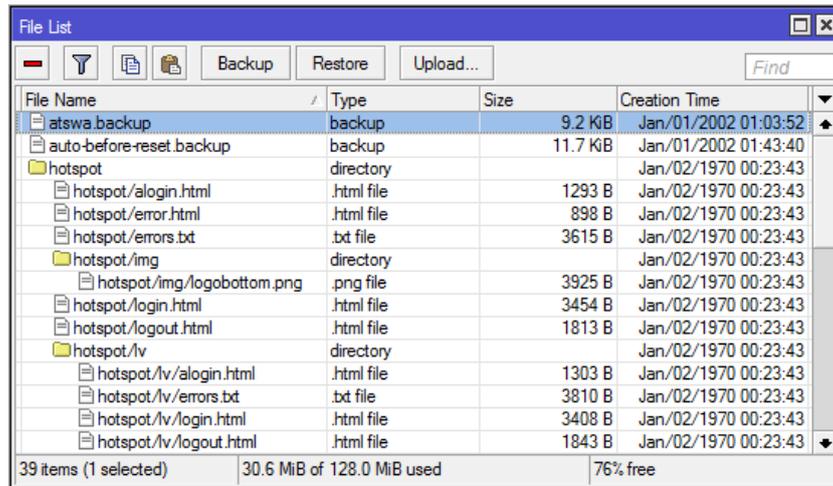
Jendela File List MikroTik

Setelah masuk ke **File List** klik **Backup** dan isi nama file pada **name** dan **password** pada **password**.



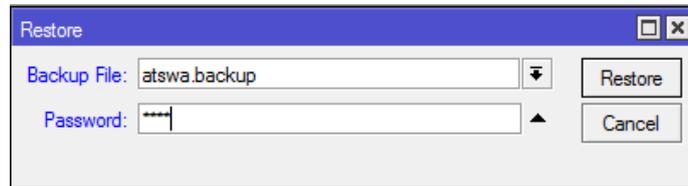
Pemberian nama dan password file backup

Setelah langkah tersebut dilakukan secara otomatis file backup akan tersimpan pada **File List** dengan ekstensi file **backup**.

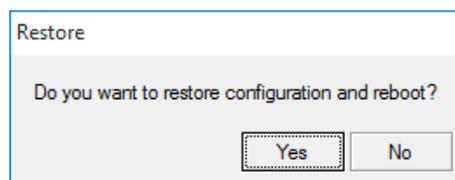


File backup pada File List

Untuk mengembalikan file cukup dengan klik **Restore** lalu pilih file backup dan masukkan password sesuai dengan yang dikonfigurasi sebelumnya lalu klik **Restore**. Jika nama file dan password sesuai akan muncul peringatan untuk *reboot* mikrotik lalu pilih **Yes**.



Nama file dan password dari file backup



Permintaan *reboot* MikroTik

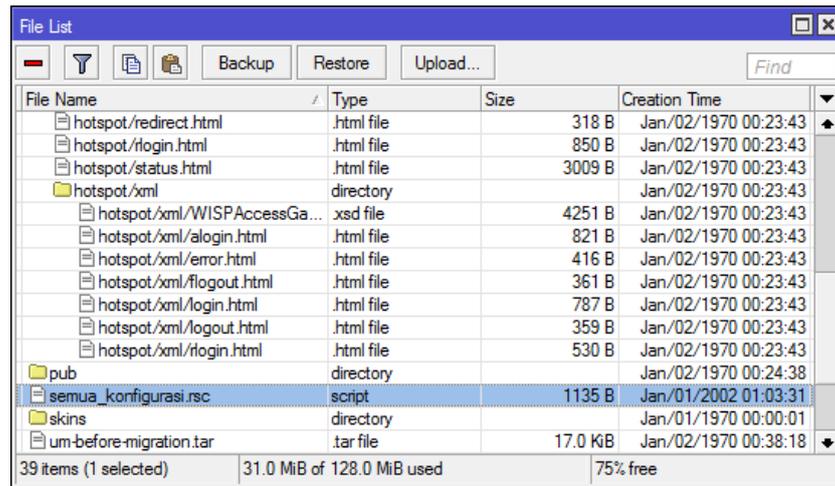
L2.8. EXPORT DAN IMPOR KONFIGURASI MIKROTIK

Export dan *import* adalah salah satu layanan untuk menyimpan file konfigurasi seperti *backup* dan *restore* namun *export* dan *import* dapat digunakan untuk konfigurasi tertentu atau tidak keseluruhan. Proses *export* dan *import* tanpa melalui proses enkripsi jadi *file* yang tersimpan dapat menunjukkan apa saja yang di konfigurasi. Selain itu proses *import* tidak memerlukan *reboot* seperti proses *restore*.

Untuk melakukan *export file* masuk ke **New Terminal** MikroTik lalu ketikkan perintah *export* berikut

```
[admin@rb] > export file=semua_konfigurasi
```

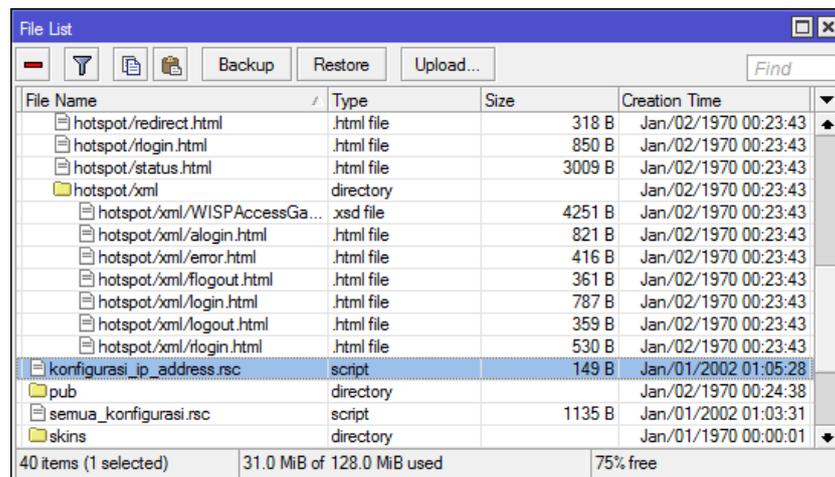
Perintah tersebut digunakan untuk *export* seluruh konfigurasi yang ada pada MikroTik



Hasil *export* pada *file list*

Sedangkan untuk *export* konfigurasi tertentu seperti hanya *export* konfigurasi *IP Address* pada MikroTik perintahnya sebagai berikut

```
[admin@rb] /ip address > export file=konfigurasi_ip_address
```



Hasil *export* pada *file list*

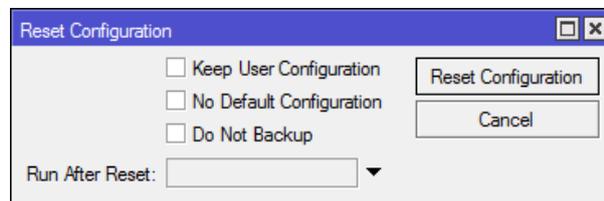
Untuk melakukan import perintah yang digunakan adalah

```
[admin@rb] > import file-name=konfigurasi_ip_address
```

L2.9. RESET MIKROTIK

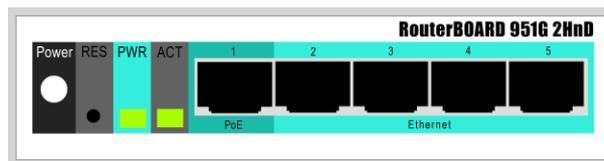
Untuk melakukan *reset* RB dapat dilakukan dengan 2 cara, yaitu dengan *soft reset* dan *hard reset*. *Soft reset* adalah cara melakukan *reset* MikroTik menggunakan *software* dan *hard reset* adalah cara melakukan *reset* mikrotik dengan cara menekan tombol *reset* pada RB.

Untuk melakukan *soft reset* caranya dengan klik **System** lalu klik **Reset Configuration** lalu klik **Reset Configuration**.



Jendela *Reset Configuration*

Untuk melakukan *hard reset* caranya dengan melepas kabel *power* dari RB, lalu menekan tombol *reset* pada RB dan menancapkan kembali kabel *power*, tunggu hingga led ACT berkedip setelah itu lepas kembali tombol *reset* yang ditekan.



Bagian belakang RB 951

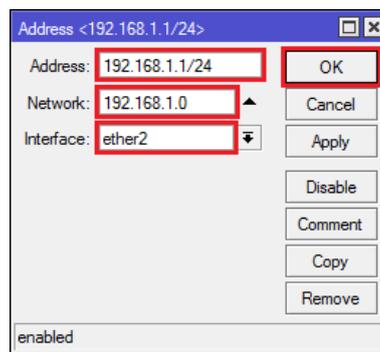
L2.10. IP ADDRESS MIKROTIK

IP Address yang dapat dikonfigurasi pada MikroTik ada dua yaitu IP Statis dan IP Dinamis. IP Statis adalah *IP Address* yang dikonfigurasi secara manual sedangkan IP Dinamis adalah IP Address yang diperoleh secara otomatis (*DHCP Client*) atau dikonfigurasi untuk memberikan IP Address secara otomatis (*DHCP Server*) kepada host yang terhubung dengan RB

Dynamic Configuration Protocol (DHCP) adalah layanan yang secara otomatis memberikan IP Address kepada komputer yang memintanya



Konfigurasi IP Statis dilakukan dengan cara klik IP lalu klik **Addresses** lalu klik **+** atau **Add** lalu masukkan *IP Address (Host)* beserta *Prefix (Contoh : 192.168.1.1/24)* pada kolom **Address**, *IP Network* pada kolom **Network**, serta pilih *Ethernet* yang diinginkan pada menu **Interface** lalu klik **OK**.

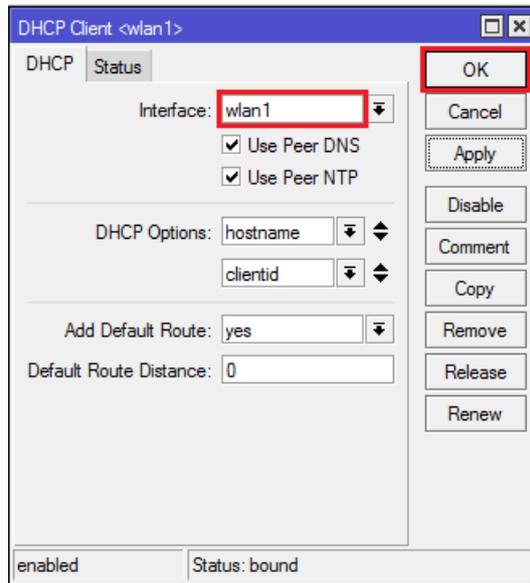


Jendela Address pada menu *Address List*

perangkat yang memberikan IP Address disebut DHCP server, sedangkan perangkat yang meminta atau mendapatkan IP Address disebut sebagai DHCP Client.

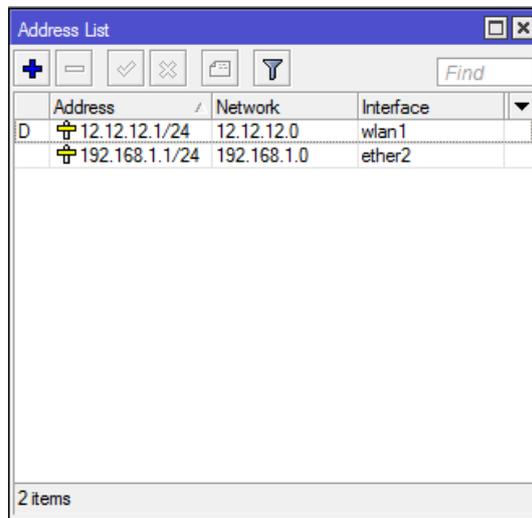


Untuk konfigurasi *IP Address* Dinamis ada dua, *DHCP Client* dan *DHCP Server*. *DHCP Client* dikonfigurasi ketika *Ethernet* pada RB terhubung dengan perangkat lain yang menyediakan *IP Address* dari *DHCP Server*. Konfigurasi *DHCP Client* pada RB dengan cara klik **IP** lalu klik **DHCP Client** lalu klik **Add** lalu pilih *Ethernet* yang akan mendapatkan *IP Address* dari *DHCP Server* pada menu *Interface*, lalu klik **OK**.



Jendela DHCP Client

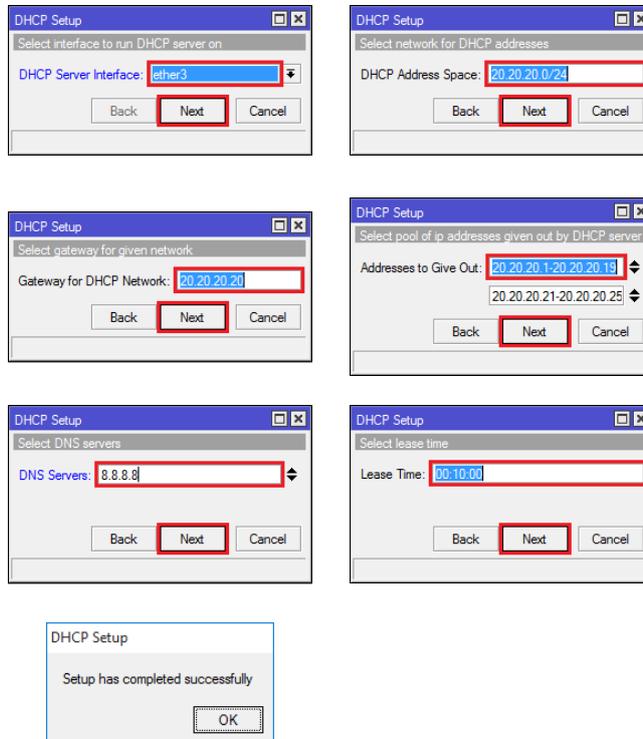
Setelah itu IP Address yang diperoleh dapat dilihat di *Address List* dan pada bagian depan IP Dinamis akan muncul huruf D sebagai informasi bahwa IP tersebut adalah IP Dinamis



IP Address yang diperoleh dari DHCP Server

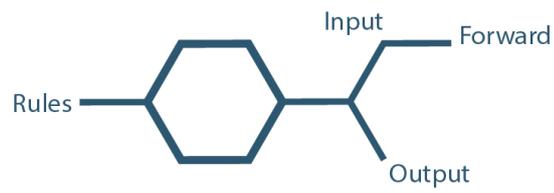
Untuk membuat DHCP Server langkah yang dilakukan adalah melakukan konfigurasi IP Address yang digunakan *Ethernet* yang terhubung dengan perangkat penerima atau DHCP Client. Setelah siap langkah selanjutnya klik **IP** lalu klik **DHCP Server** lalu klik **DHCP**

Setup, pilih **Interface**, dan masukkan **IP Address** sesuai yang di inginkan



Langkah-Langkah konfigurasi DHCP Server

LABORATORIUM 3



MIKROTIK FIREWALL

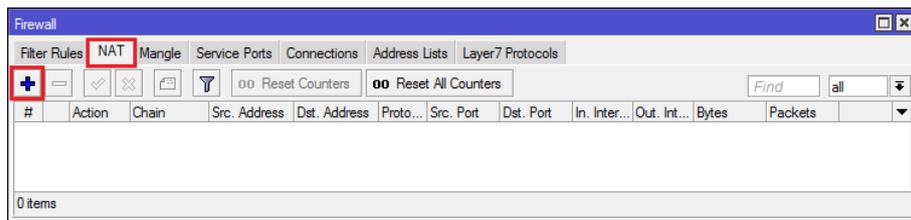
L3.1. NAT

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan banyak komputer ke jaringan internet dengan menggunakan satu atau lebih alamat IP



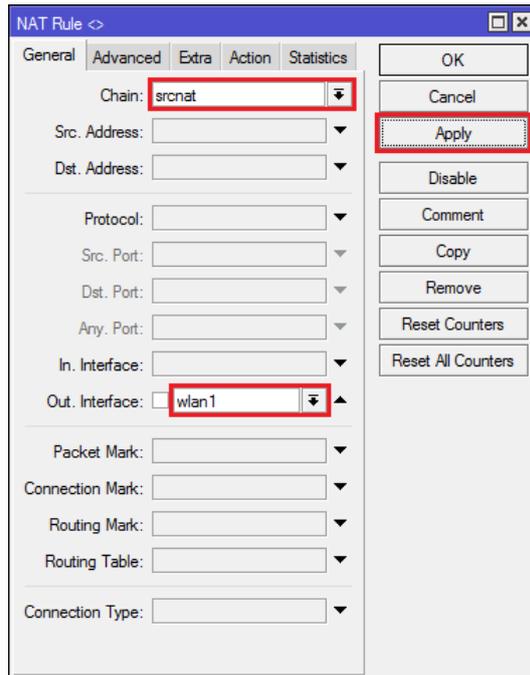
Pada *IP Firewall* NAT terdapat dua Chain, **srcnat** dan **dstnat**, **srcnat** mengijinkan action **masquerade** (*layanan jaringan LAN mendapatkan 1 alamat dinamis yang berasal dari IP Address WAN*) dan **srcnat** (*layanan jaringan LAN mendapatkan 1 alamat static yang berasal dari IP Address WAN*).

Untuk melakukan konfigurasi NAT pada RB dengan cara klik **IP** lalu klik **Firewall** lalu klik **NAT** lalu klik “+” atau **Add**.



Jendela NAT pada *Firewall*

Setelah masuk *NAT Rule* pada bagian **General** pilih “srcnat” pada **Chain** dan pilih ethernet yang terhubung dengan internet atau publik pada *Out Interface* lalu **Apply**.

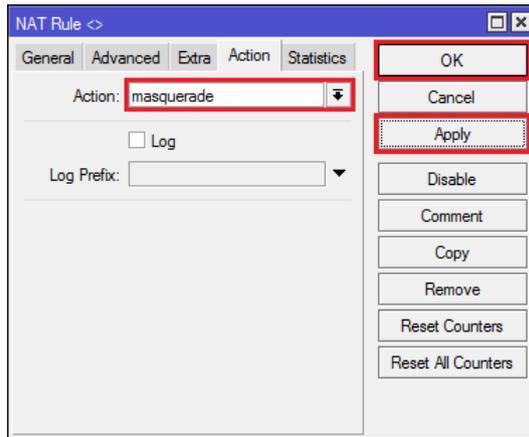


Jendela *General* pada NAT Rule



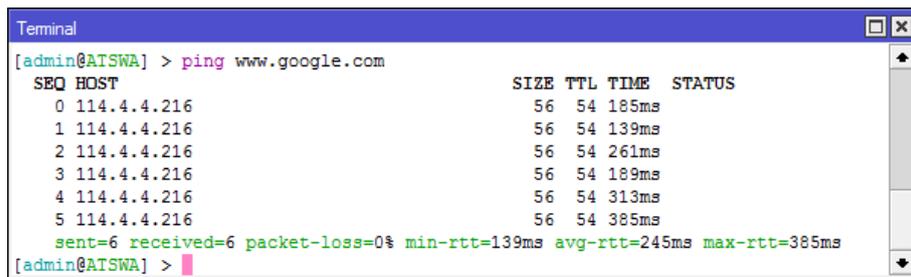
Penerapan Out dan In pada Router MikroTik

Setelah itu masuk ke **Action** dan pilih *masquerade* pada Action lalu klik **Apply** lalu klik **OK**.



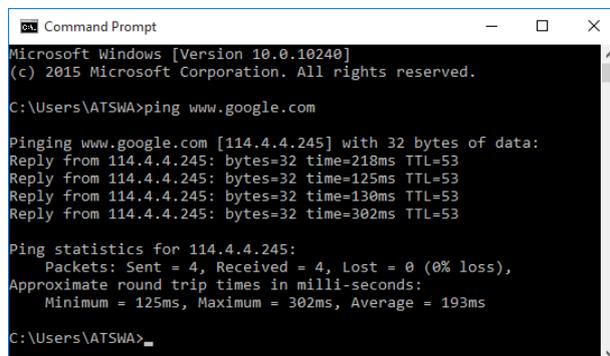
Jendela Action pada NAT Rule

Setelah itu masuk ke Terminal pada MikroTik lalu test ping ke *www.google.com* dan pastikan *reply*.



Hasil ping *www.google.com* melalui terminal

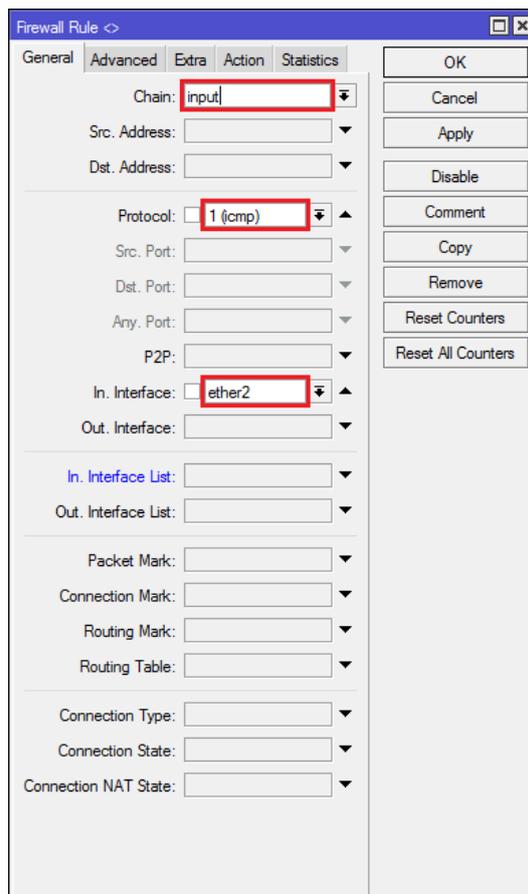
Selain itu lakukan tes ping pula menggunakan *Command Prompt* pada komputer untuk memastikan komputer sudah mendapatkan akses *internet*.



Hasil ping *www.google.com* melalui cmd

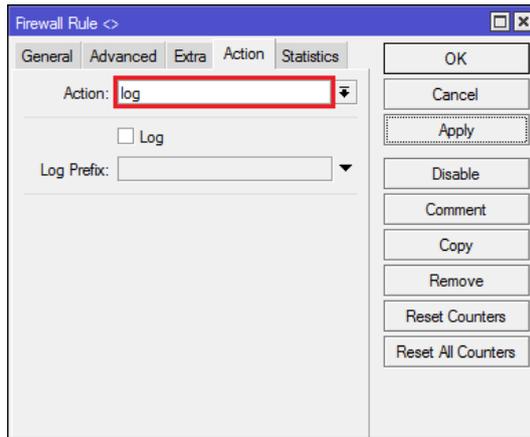
L3.2. FIREWALL LOGGING MIKROTIK

Firewall Logging adalah layanan pada *firewal* yang digunakan untuk mencatat aktifitas jaringan pada *Log MikroTik*. Untuk mengaktifkannya klik IP lalu klik **Firewall** lalu klik **Filter Rule** lalu klik **General** lalu tentukan *Chain* setelah itu pilih protokol ICMP pada menu **Protocol** dan pilih *interface* yang terhubung dengan komputer.



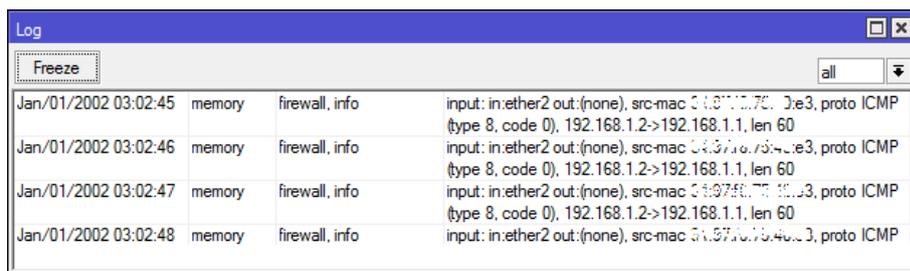
Jendela General pada *Firewall Rule*

Setelah itu masuk ke menu **Action** dan pilih *Log* pada menu **Action** lalu klik **OK**.



Jendela Action pada Firewall Rule

Setelah itu lakukan ping dari komputer ke IP Address yang berada pada RB atau komputer lain dan masuk ke **Log** pada Mikrotik untuk melihat hasilnya.



Log pada Mikrotik

L3.3. FILTER RULE

Filter Rule atau aturan penyaringan adalah salah satu fitur pada firewall MikroTik yang digunakan untuk melakukan penyaringan trafik yang menuju ke router, keluar dari router, dan melewati router. Dalam *Filter Rule* terdapat tiga pilihan *Chain* yaitu *Input*, *Forward*, dan *Output*. Masing-masing *Chain* memiliki pengaturan trafik yang berbeda, antara lain sebagai berikut



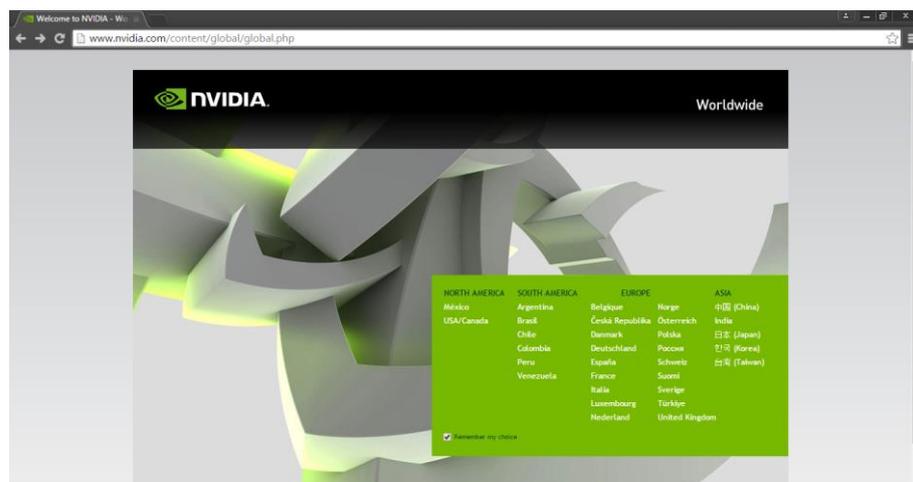
Chain Filter Rules pada MikroTik



Penerapan *Source* (Src) dan *Destination* (Dst) pada MikroTik

Jika *Chain* dengan mode *Input* Anda dapat mengatur trafik yang berasal dari komputer dan menuju *router* atau sebaliknya, jika *Chain* dengan mode *Forward* Anda dapat mengatur trafik yang melewati *router* dari komputer menuju Internet atau sebaliknya, dan jika *Chain* dengan mode *Output* Anda dapat mengatur trafik yang berasal dari *router* menuju ke Internet atau sebaliknya.

Anda dapat memanfaatkan *Filter Rule* untuk memblokir situs menggunakan *Filter Rule* pada firewall dengan cara klik **IP** lalu klik **Firewall** lalu klik **Filter Rule** lalu klik “+” atau **Add**. Pastikan terlebih dahulu situs yang akan Anda blokir dapat diakses dengan normal.



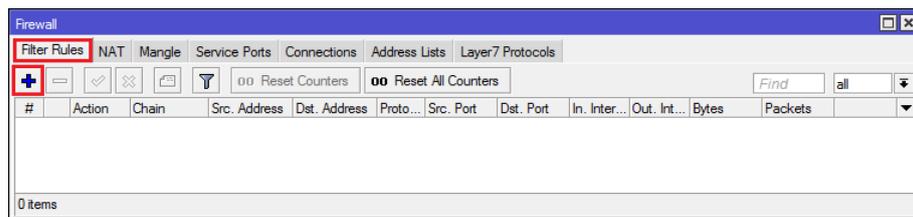
Situs www.nvidia.com sebelum diblokir

Setelah dipastikan situs yang akan diblokir dapat diakses langkah selanjutnya adalah mengetahui *IP Address* yang digunakan situs tersebut. Jika menggunakan *Command Prompt* dapat menggunakan perintah *nslookup*.



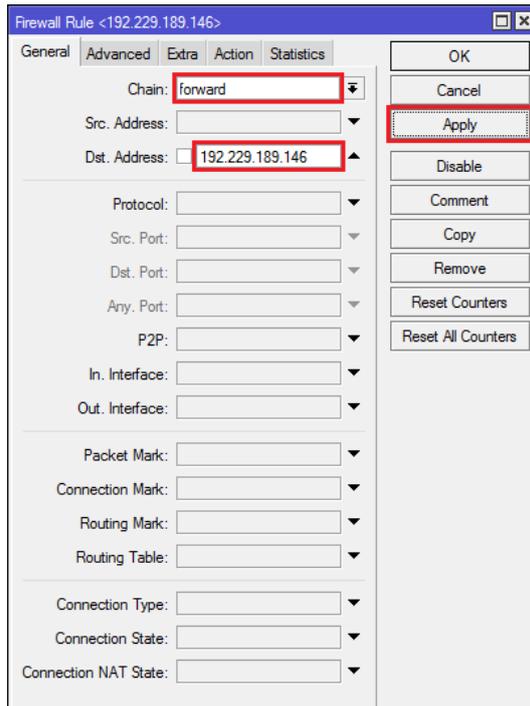
IP Address dari www.nvidia.com

Setelah Anda mengetahui *IP Address* langkah selanjutnya kembali ke menu *Filter Rule* pada *Firewall*



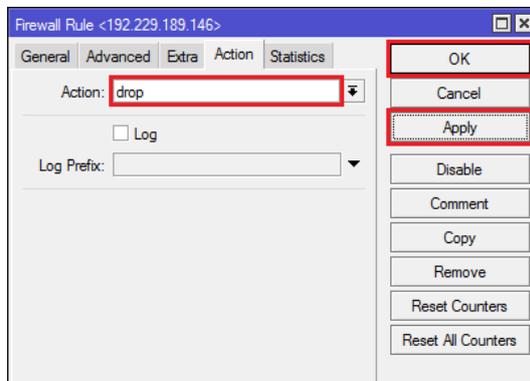
Jendela *Filter Rule* pada *Firewall*

Pada menu *General* pastikan *Chain* dengan mode *Forward* karena yang akan dilakukan adalah melakukan pemblokiran trafik yang melewati *Router* yaitu dari Komputer ke Internet. Setelah itu masukkan *IP Address* dari situs yang akan diblokir pada bagian *Dst Address* lalu klik *Apply*.



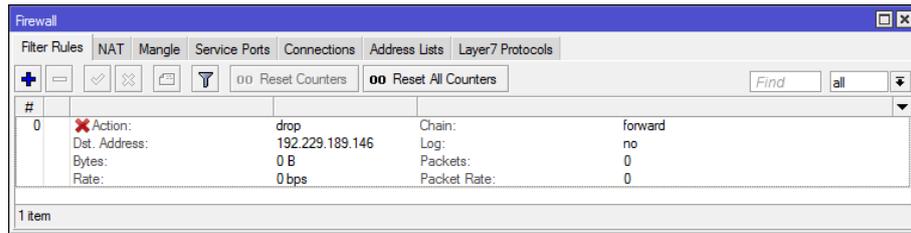
Jendela **General** pada **Firewall Rule**

Setelah itu masuk ke menu **Action** pada **Firewall Rule** lalu pilih **“drop”** lalu klik **Apply** lalu klik **OK**.



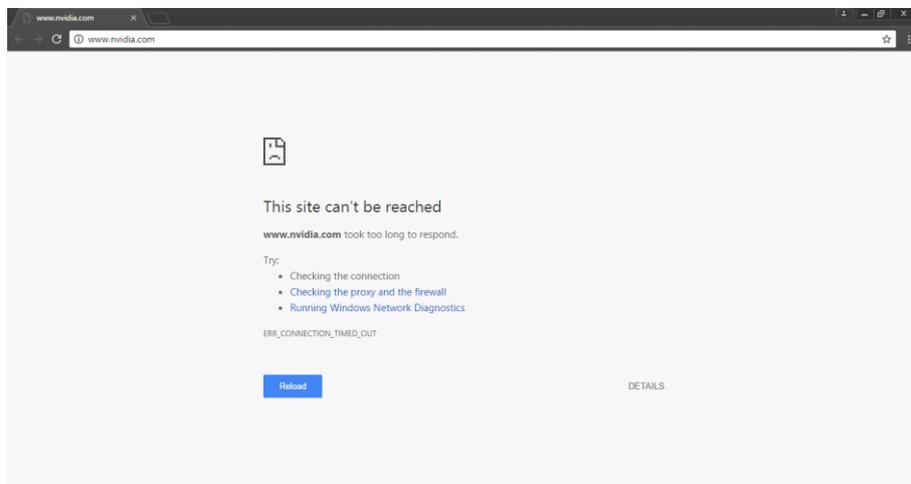
Jendela **Action Firewall Rule**

Anda dapat melihat *rule* yang telah dibuat pada menu **Firewall Rule**.



Filter Rule yang sudah dibuat

Jika semua langkah tersebut sudah sesuai lakukan pengujian terhadap situs yang diblokir untuk melihat apakah sudah berhasil atau belum.



halaman www.nvidia.com setelah berhasil diblokir

L3.4. *CONTENT*



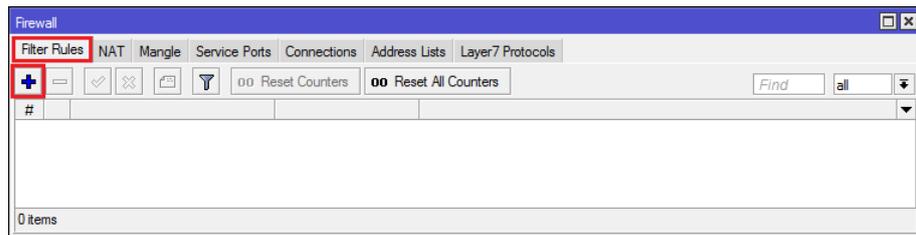
Topologi Jaringan

Dalam firewal Anda juga dapat melakukan penyaringan berdasarkan konten atau informasi yang ada di halaman sebuah situs. Sebelum Anda melakukan pemblokiran uji terlebih dahulu terhadap web tersebut untuk memastikan bahwa web tersebut masih dapat diakses.



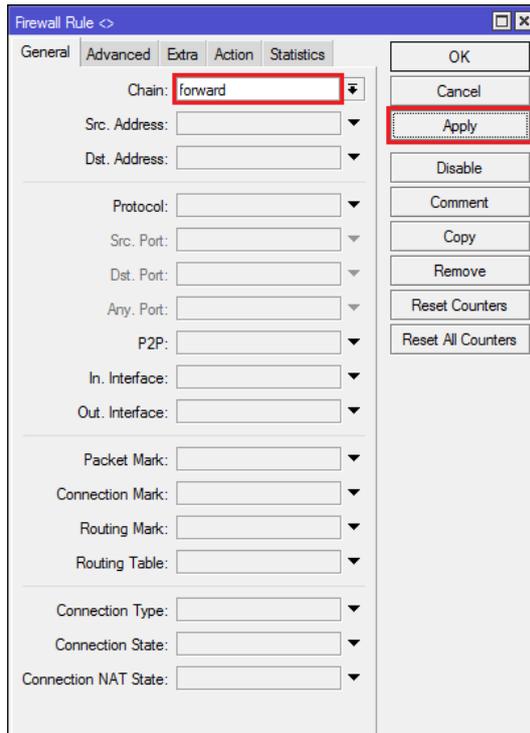
Halaman www.amd.com sebelum diblokir

Setelah itu klik **IP** lalu klik **Firewall** lalu klik **Filter Rule** lalu klik “+” atau **Add**.



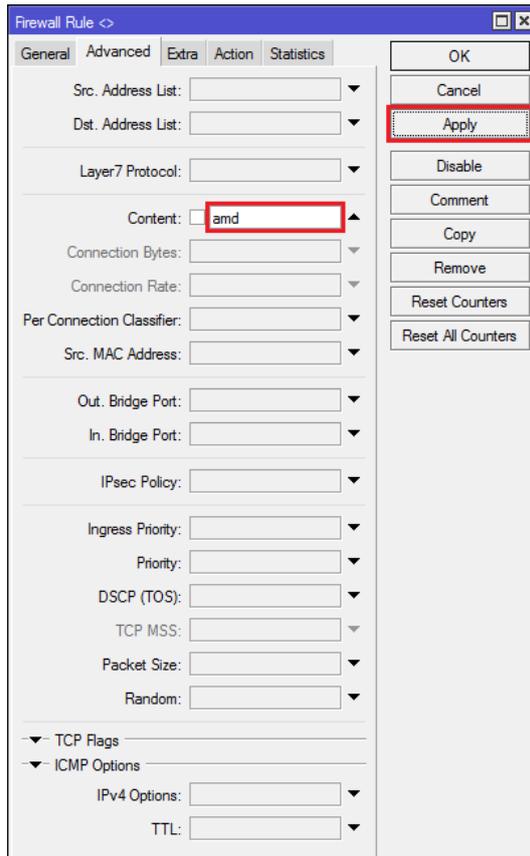
Jendela **Filter Rule**

Masuk ke menu **General** pada **Firewall Rule** dan pilih mode **Forward** pada **Chain** lalu klik **Apply**.



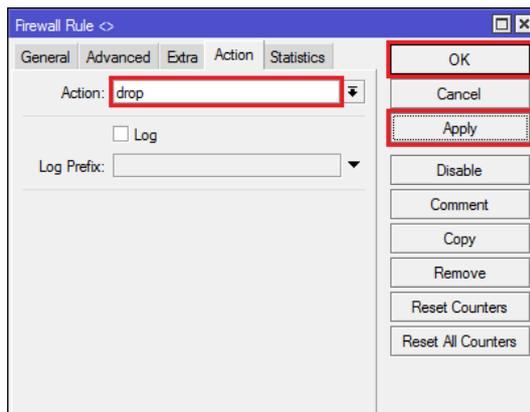
Jendela **General** pada **Firewall Rule**

Klik **Advanced** dan pada bagian **content** masukkan kata yang akan diblokir lalu klik **Apply**.



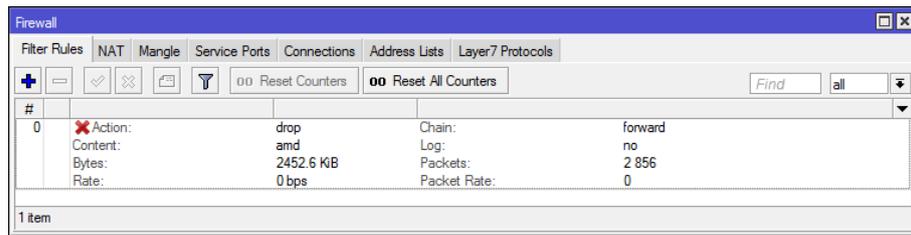
Jendela **Advanced** pada **Firewall Rule**

Klik **Action** lalu pilih **drop** pada daftar pilihan **Action** lalu klik **Apply** lalu klik **OK**.



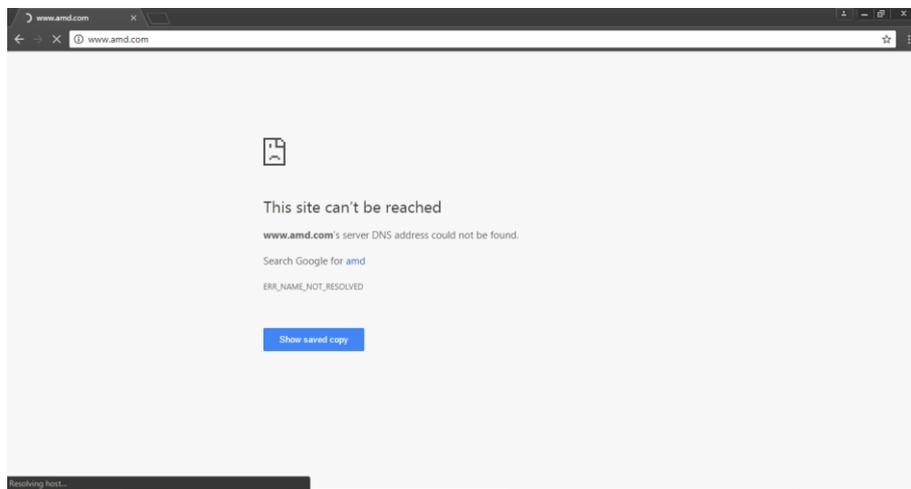
Jendela **Action** pada **Firewall Rule**

Untuk melihat **rule** yang telah dibuat masuk ke menu **Filter Rule** pada **Firewall**.



Filter Rule yang dibuat

Setelah semua selesai lakukan pengujian apakah konten tersebut sudah berhasil diblokir atau belum.



halaman www.amd.com setelah diblokir

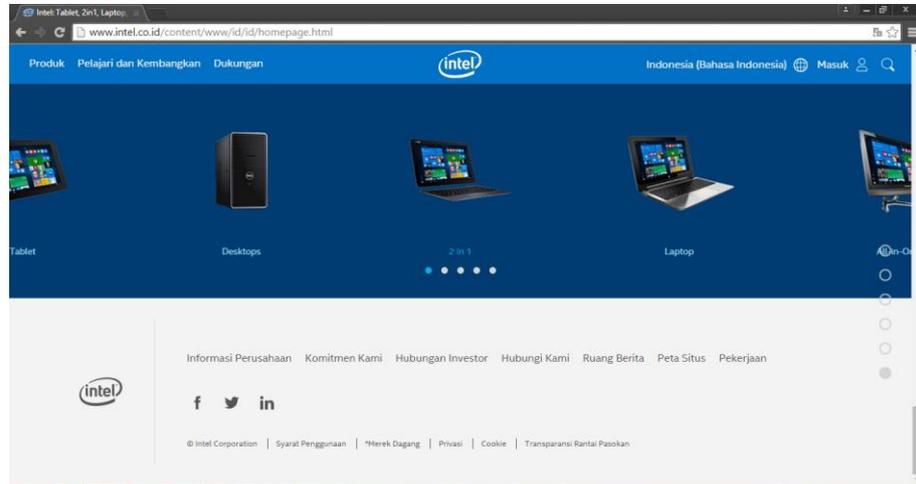
L3.5. ADDRESS LIST



Topologi Jaringan

Jika Anda ingin melakukan pemblokiran terhadap situs yang memiliki **IP Address** lebih dari satu dapat menggunakan **Address List**. **Address List** adalah fitur yang digunakan untuk melakukan pemfilteran terhadap **Grup IP Address** menjadi **1 Rule Firewall**.

Seperti sebelumnya lakukan pengujian terlebih dahulu terhadap situs atau *web* yang akan diblokir masih dapat diakses sebelum dilakukan pemblokiran.



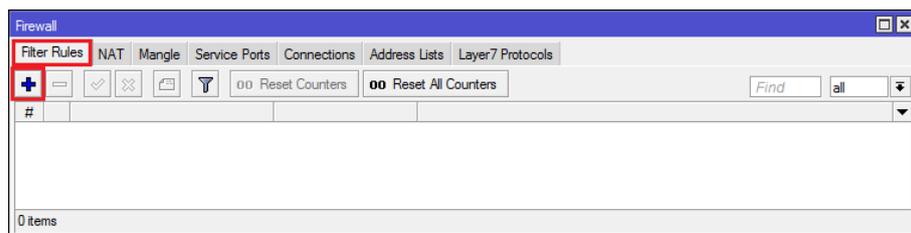
Halaman www.intel.com sebelum diblokir

Selanjutnya adalah melihat **IP Address** dari domain yang akan diblokir menggunakan **nslookup**.



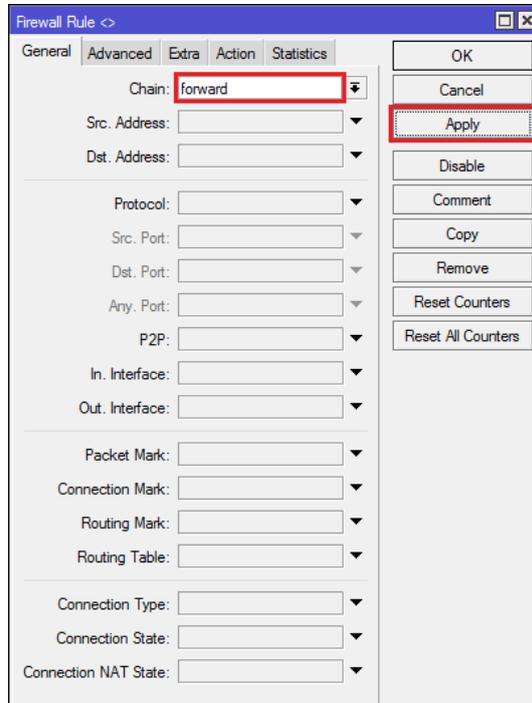
IP Address dari www.intel.com

Setelah mengetahui **IP Address** langkah selanjutnya adalah masuk ke **Filter Rule Firewall** dengan cara klik **IP** lalu klik **Firewall** lalu klik **Filter Rule**



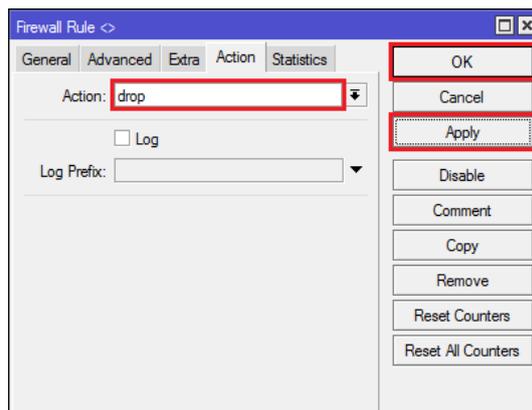
Jendela Filter Rule Firewall

Masuk ke menu **General** lalu pilih **Forward** pada pengaturan **Chain** lalu klik **Apply**.



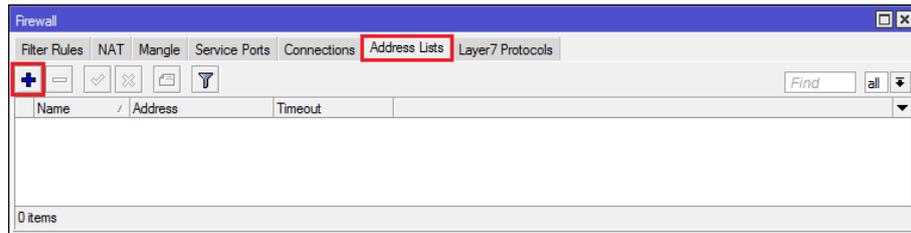
Jendela **General** pada **Firewall Rule**

Masuk ke menu **Action**, pada **Action** pilih **drop** lalu klik **Apply**.



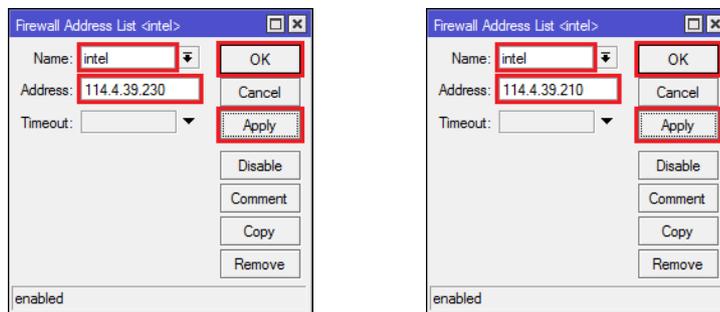
Jendela **Action** pada **Firewall Rule**

Masuk ke menu **Address List** lalu klik “+” atau **Add**.



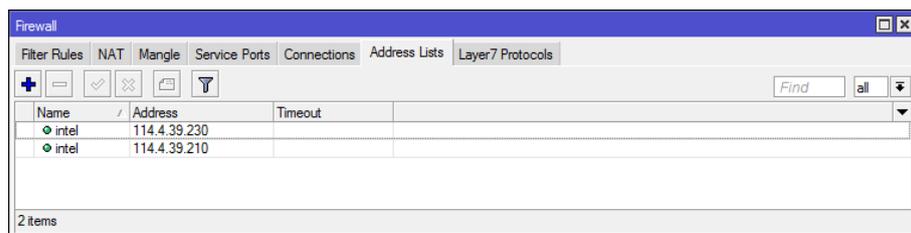
Jendela *Address List* pada *Firewall*

Pada *Firewall Address List* masukkan semua *IP Address* dari domain yang akan diblokir.



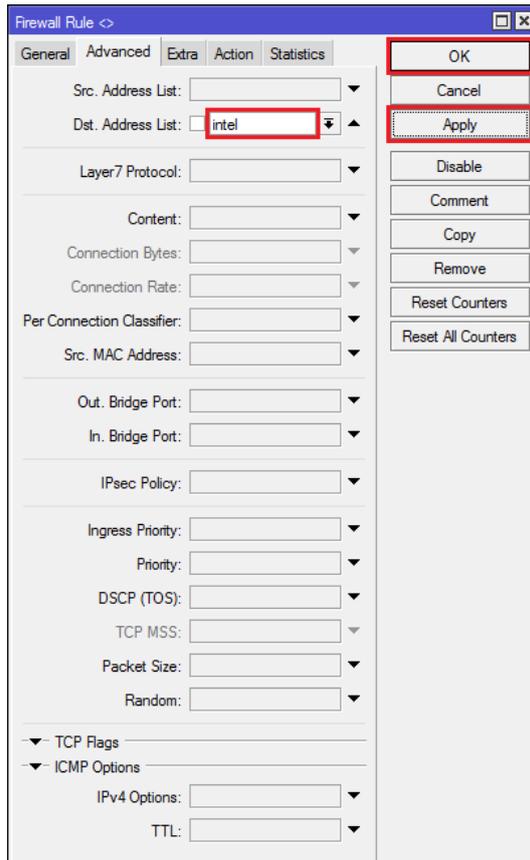
Jendela *Firewall Address List*

Untuk melihat *Address List* yang telah dibuat dapat dilihat di menu *Address List*.

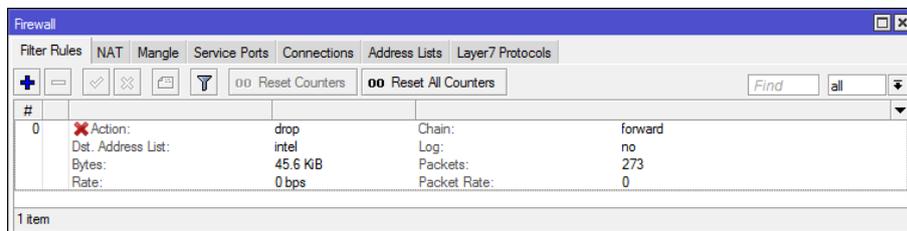


Address List yang sudah jadi

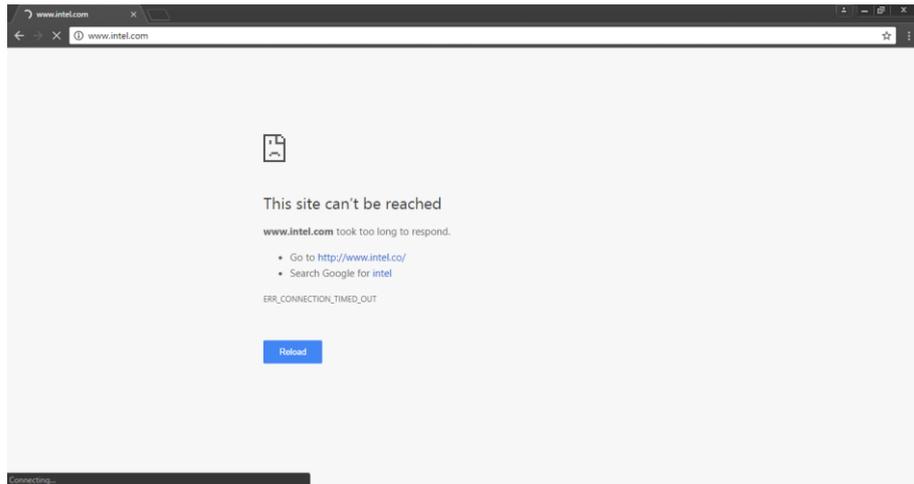
Masuk kembali ke menu *Advanced* pada *Firewall Rule*, pada bagian *Dst. Address List* pilih daftar *IP Address* yang telah dibuat sebelumnya lalu klik *Apply* lalu klik *OK*.



Jendela *Advanced* pada *Firewall Rule*



Lakukan pengujian terhadap domain dari *web* yang telah diblokir menggunakan *Address List* apakah sudah berhasil diblokir atau belum.



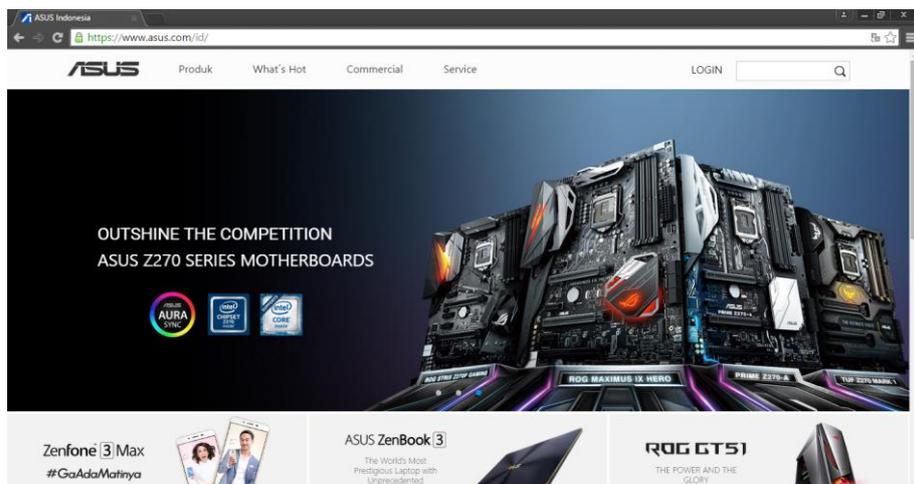
Halaman web www.intel.com setelah diblokir

L3.6. LAYER 7 PROTOCOLS



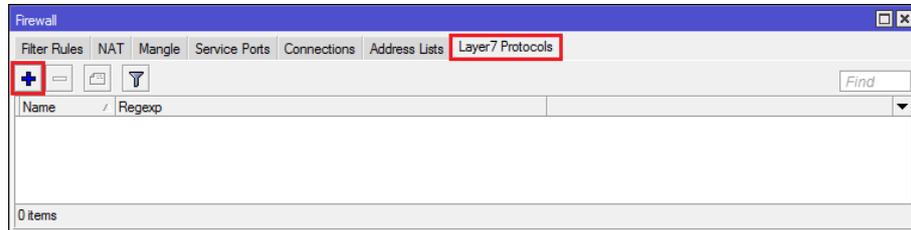
Topologi Jaringan

Anda juga dapat melakukan pemblokiran menggunakan **Regex** melalui **Layer 7 Protocols** pada **Firewall**. Pastikan **web** yang akan diblokir sebelum dilakukan pemblokiran masih dapat diakses.



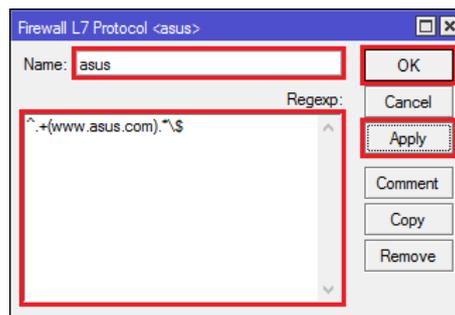
Halaman www.asus.com sebelum diblokir

Masuk ke **Firewall** dengan cara klik **IP** lalu klik **Firewall** lalu klik **Layer 7 Protocols**. Setelah masuk ke menu **Layer 7 Protocols** klik “+” atau **Add**.



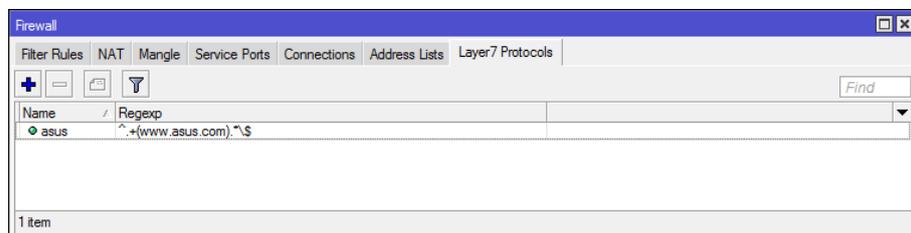
Jendela **Layer 7 Protocol** pada **Firewall**

Masuk di jendela **Firewall L7 Protocol** lalu masukkan domain dari situs yang akan diblokir dengan menuliskan “**^(nama_domain).***” lalu klik **Apply** lalu klik **OK**.



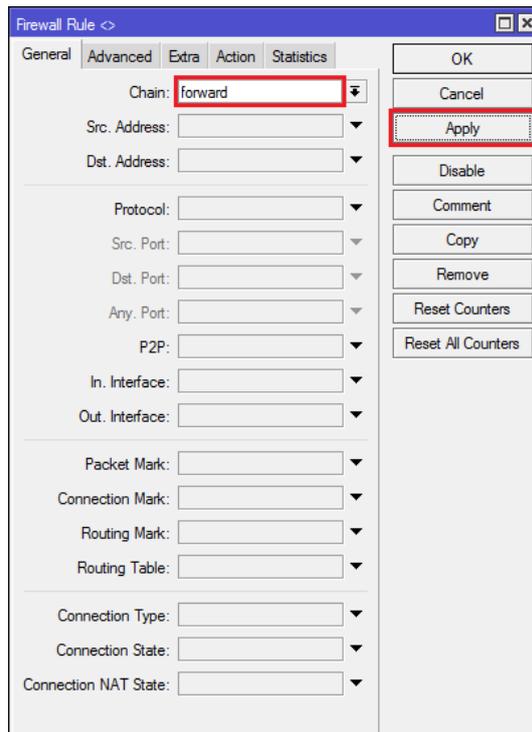
Jendela **Firewall L7 Protocol**

Daftar dari **domain** yang diblokir menggunakan **Layer 7 Protocol** dapat dilihat pada menu **Layer 7 Protocols** pada **Firewall**.



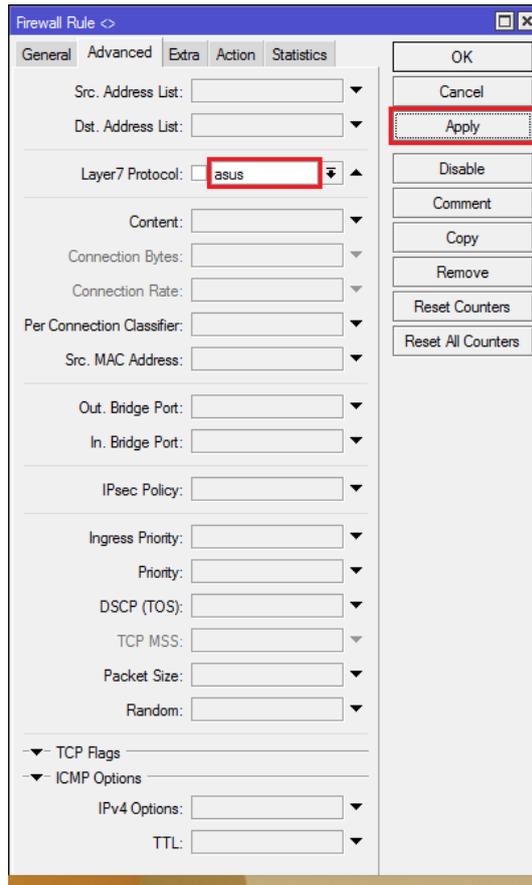
Daftar **rule** pada jendela **Layer 7 Protocol**

Setelah itu masuk ke menu **Filter Rule** lalu klik “+” atau **Add**. Setelah masuk ke jendela **Firewall Rule** klik menu **General** dan pada daftar **Chain** pilih **Forward** lalu klik **Apply**.



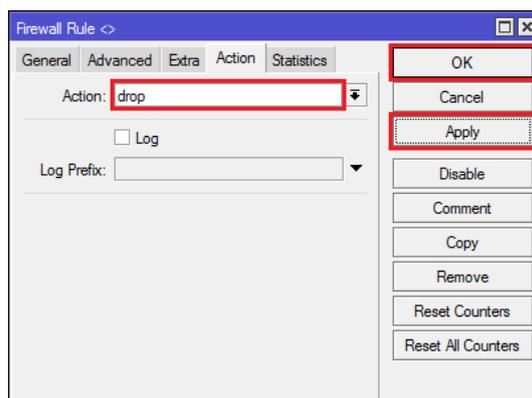
Jendela **General** pada **Firewall Rule**

Setelah itu masuk ke menu **Advanced** lalu pada daftar **Layer 7 Protocol** pilih daftar yang sudah dibuat lalu klik **Apply**.



Jendela *Advanced* pada *Firewall Rule*

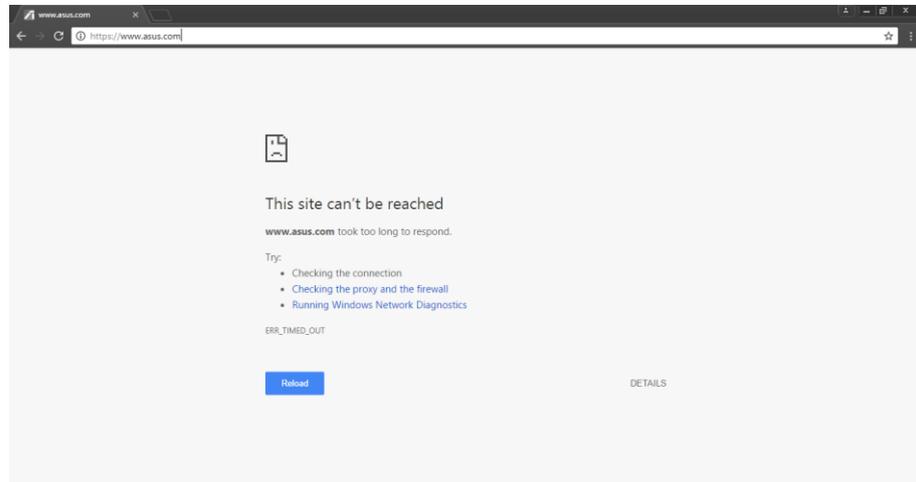
Setelah itu masuk ke menu **Action** dan pada daftar *Action* pilih **drop** lalu klik **Apply** lalu klik **OK**.



Jendela *Action* pada *Firewall Rule*

Untuk melihat *rule* yang telah dibuat dapat dilihat pada *Filter Rule* pada menu *Firewall*.

Langkah terakhir adalah melakukan pengujian terhadap domain situs yang telah diblokir untuk memastikan apakah sudah berhasil diblokir atau belum.



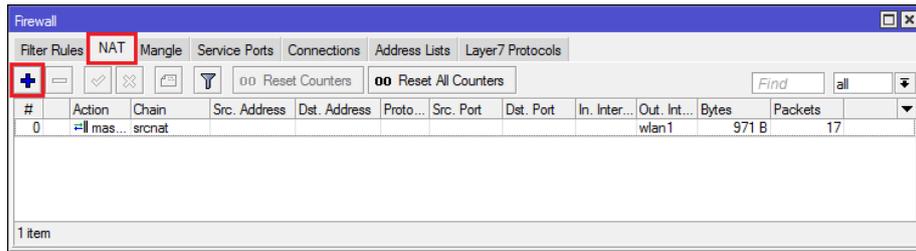
Halaman www.asus.com yang telah diblokir

L3.7. *TRANSPARENT DNS*



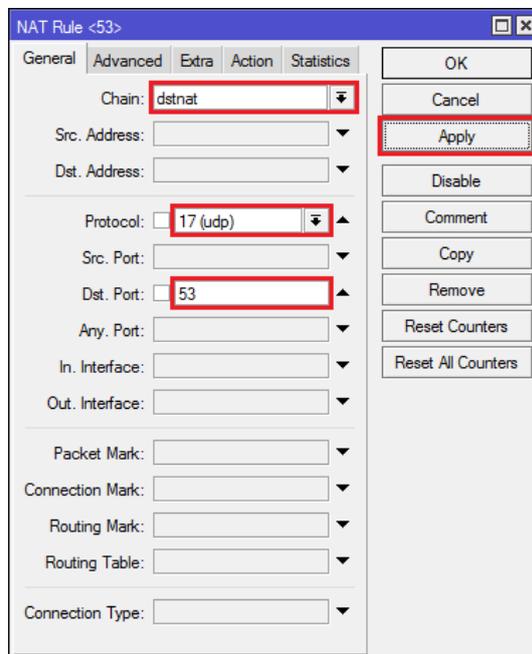
Topologi Jaringan

Untuk melakukan pemblokiran menggunakan *Transparent DNS* pastikan terlebih dahulu *IP Address* dari *DNS* yang akan digunakan. Di Indonesia ada *DNS* yang cukup terkenal adalah *DNS* dari *Nawala Project*. Alamat *DNS* dari *Nawala Project* adalah 180.131.144.144. Langkah pertama yang dilakukan adalah masuk *NAT* pada *Firewall* dengan cara klik *IP* lalu klik *Firewall* lalu klik *NAT* lalu klik “+” atau *Add*.



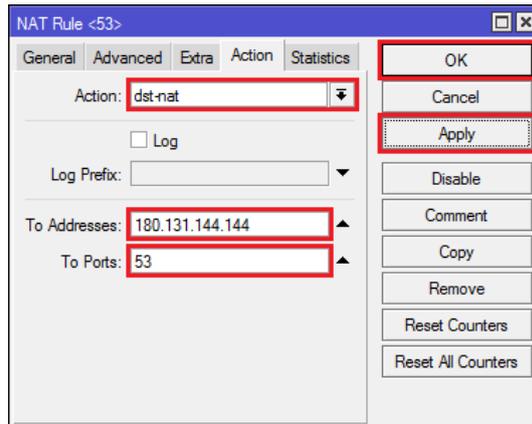
Jendela NAT pada *Firewall*

Setelah masuk NAT masuk ke menu **General** dan pada **Chain** pilih *dstnat*, pada **Protocol** pilih **UDP**, pada **dst Port** masukkan 53 (53 adalah port dari DNS), lalu klik **Apply**.



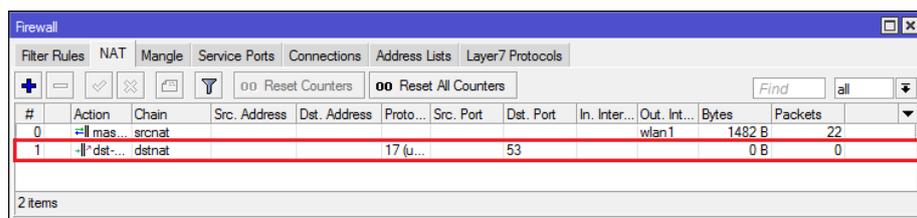
Jendela **General** pada **NAT Rule**

Setelah itu masuk ke menu **Action** pada **Action** pilih **dst port**, pada **to address** masukkan **IP Address** dari **Nawala Project**, lalu pada **to port** masukkan **port** dari DNS yaitu 53, lalu klik **Apply** lalu klik **OK**.



Jendela *Action* pada *NAT Rule*

Setelah itu untuk melihat *NAT Rule* yang telah dibuat dapat melihat pada menu *NAT* pada *Firewall*.



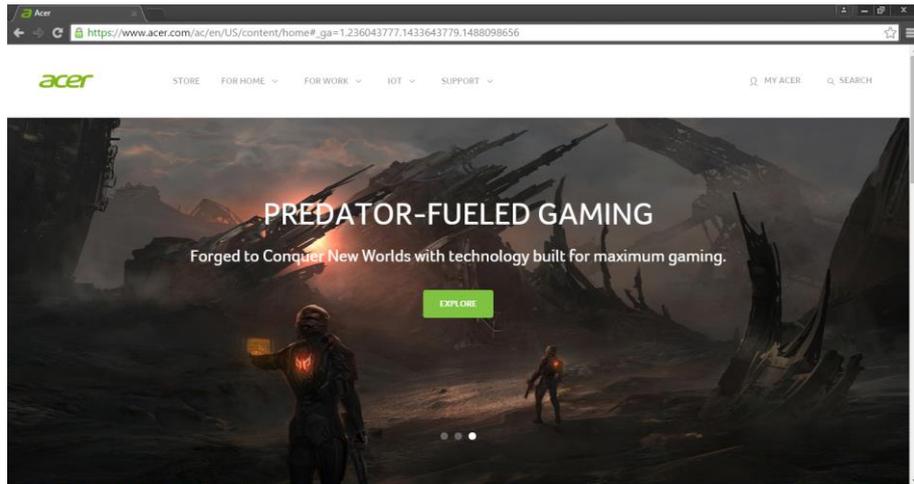
Daftar *NAT Rule* pada jendela *NAT Firewall*

L3.8. *TRANSPARENT WEB PROXY*



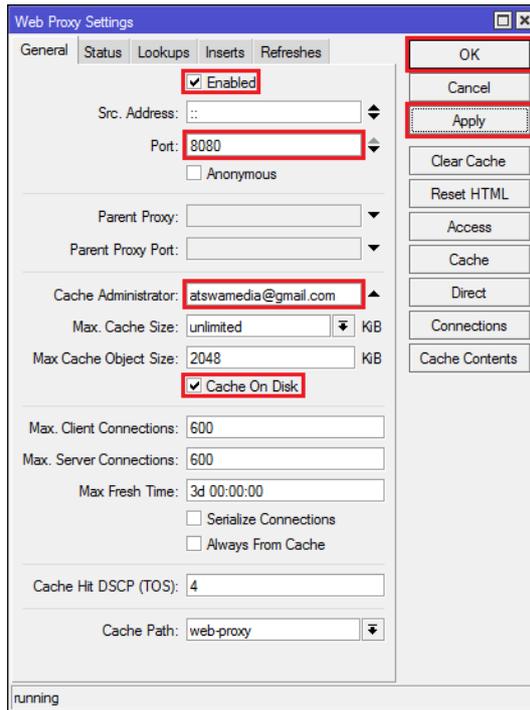
Topologi Jaringan

Untuk melakukan pemblokiran menggunakan *Transparent Web Proxy* pastikan terlebih dahulu domain dari web yang akan diblokir masih dapat diakses.



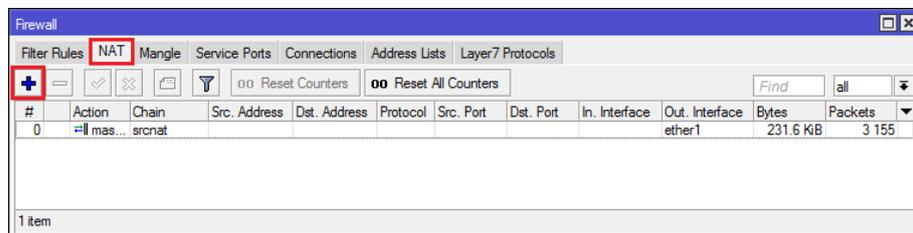
Halaman www.acer.com sebelum diblokir

Setelah itu masuk ke menu **Web Proxy Settings** dengan cara klik **IP** lalu klik **Web Proxy**. Setelah masuk di menu **Web Proxy Setting** aktifkan *web proxy* dengan cara memberikan ceklist pada **Enabled** lalu pada **port** masukkan **8080** (*8080 adalah port dari web proxy*), lalu pada **Cache Administrator** masukkan identitas yang ditampilkan dapat berupa *email* nomer telpon atau lain sebagainya, lalu beri ceklist pada **Cache On Disk** agar penyimpanan *cache web proxy* disimpan pada *harddisk* bukan *memory*.



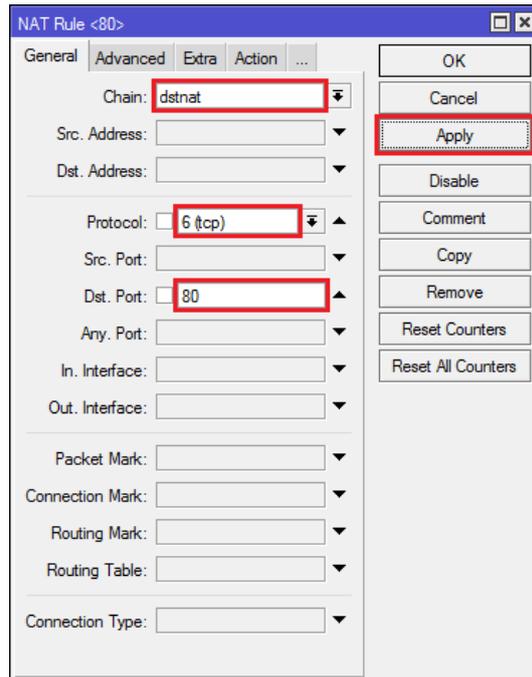
Jendela *Web Proxy Settings*

Setelah itu masuk ke **NAT** pada **Firewall** lalu klik “+” atau **Add**.



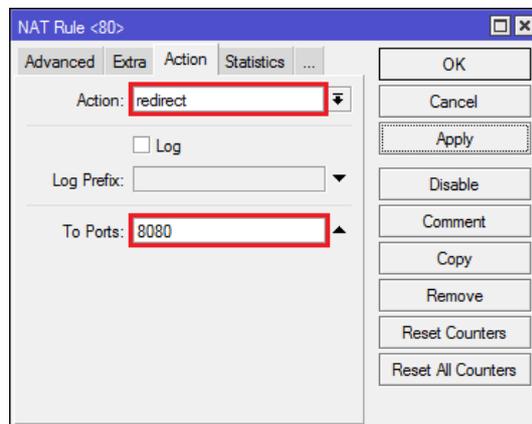
Jendela **NAT** pada **Firewall**

Setelah itu masuk ke menu **General** pada **NAT Rule** lalu pada **Chain** pilih **forward**, lalu pada **Protocol** pilih **TCP**, lalu pada **Dst Port** masukkan **80** (*80 adalah port dari www atau web*), lalu klik **Apply**.



Jendela **General** pada **NAT Rule**

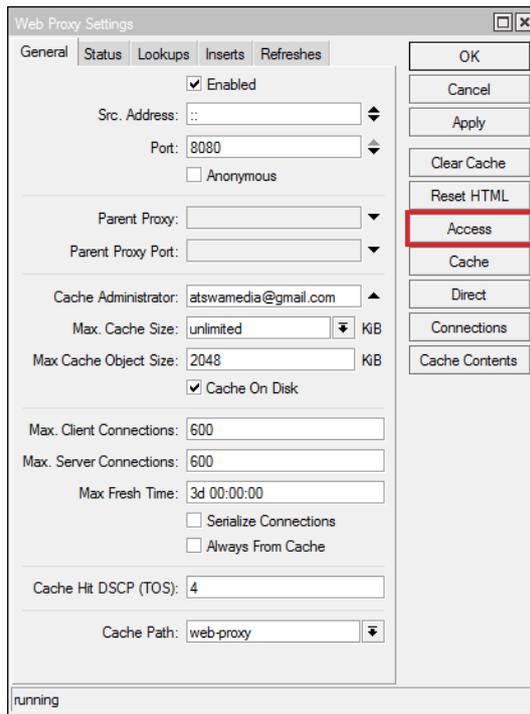
Setelah itu masuk ke menu **Action** pada **NAT Rule** lalu pada **Action** pilih **redirect** lalu pada **To Ports** masukkan 8080, lalu klik **Apply**, lalu klik **OK**.



Jendela **Action** pada **NAT Rule**

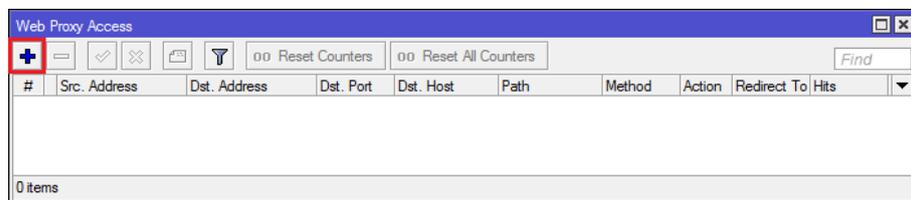
Untuk melihat **NAT Rule** yang sudah dibuat dapat dilihat pada menu **NAT Firewall**.

Setelah itu masuk kembali ke jendela **Web Proxy Setting** lalu masuk menu **Access** untuk masuk ke **Web Proxy Access**.



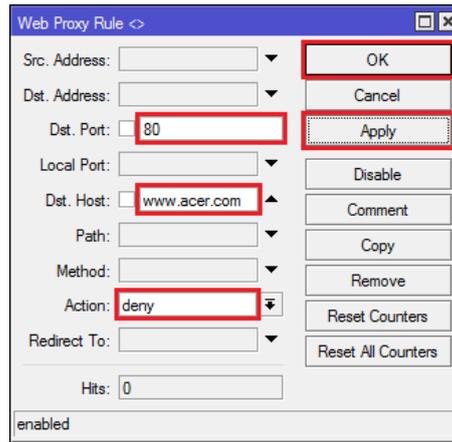
Jendela **General** pada **Web Proxy Setting**

Pada **Web Menu Access** klik “+” atau **Add**.



Jendela **Web Proxy Access**

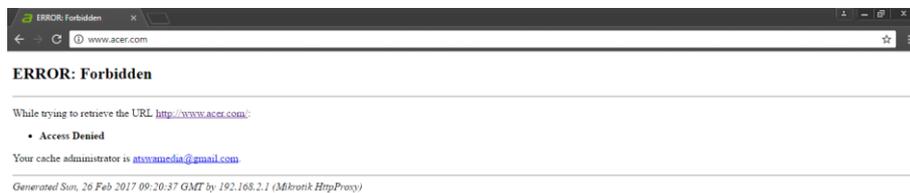
Setelah itu pada **Dst Port** masukkan 80, lalu pada **Dst Host** masukkan domain dari **web** yang akan diblokir, dan pada bagian **Action** pilih **deny**, lalu klik **Apply**, lalu klik **OK**.



Jendela *Web Proxy Rule*

| # | Src. Address | Dst. Address | Dst. Port | Dst. Host | Path | Method | Action | Redirect To | Hits |
|---|--------------|--------------|-----------|--------------|------|--------|--------|-------------|------|
| 0 | | | 80 | www.acer.com | | | deny | | 1 |

Daftar *Web Proxy Rule* pada *Web Proxy Access*



Halaman www.acer.com yang telah diblokir

L3.9. REDIRECT



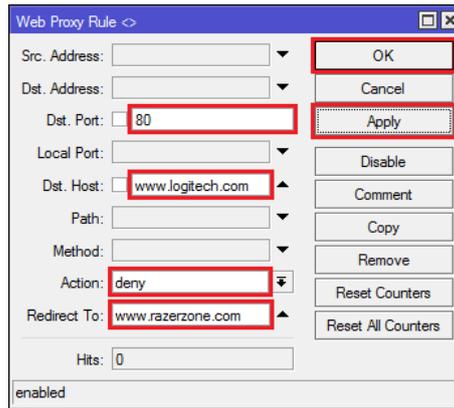
Topologi Jaringan

Sebelum Anda mengalihkan situs pastikan terlebih dahulu situs yang akan dialihkan tersebut masih dapat diakses.



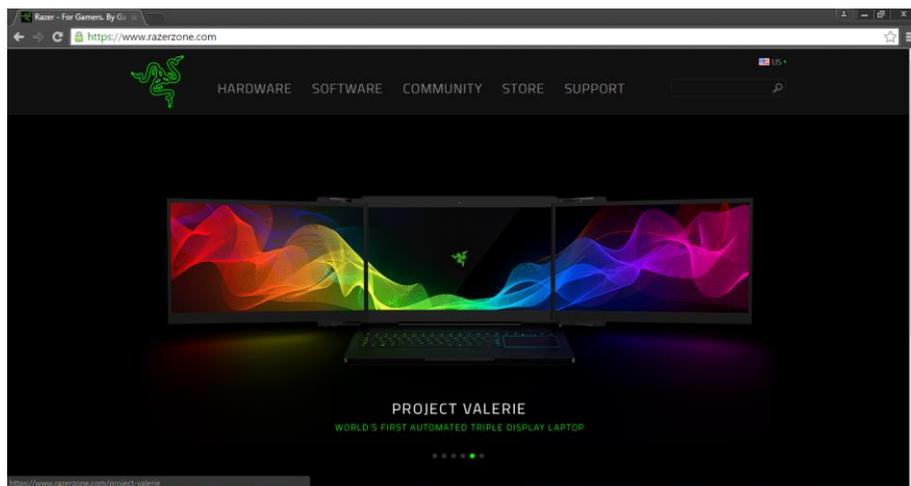
Halaman www.logitech.com sebelum dialihkan

Setelah itu lakukan konfigurasi **Web Proxy** seperti sebelumnya, dan pada pengaturan **Web Proxy Rule** masukkan alamat situs yang akan dialihkan pada **Dst. Host** dan masukkan alamat situs tujuan pada **Redirect To**



Jendela *Web Proxy Rule*

Anda dapat melakukan pengujian dengan cara memasukkan situs yang di alihkan dan pastikan sudah berhasil mengakses ke situs tujuan.



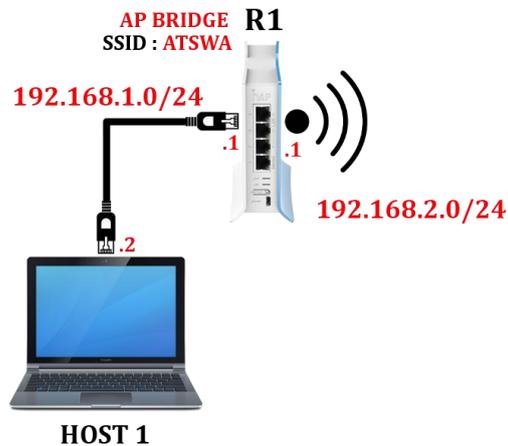
Halaman www.razerzone.com

LABORATORIUM 4



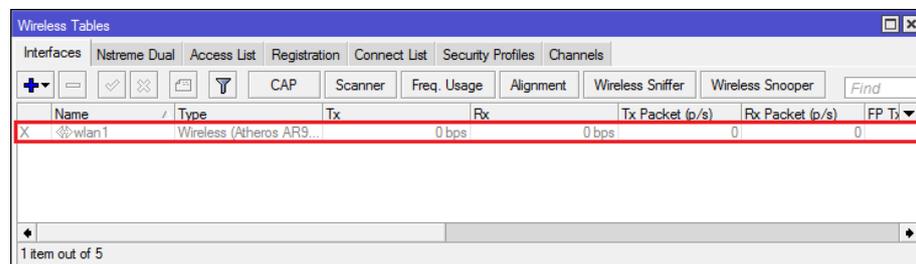
MIKROTIK WIRELESS

L4.1. ACCESS POINT BRIDGE (PEMANCAR)



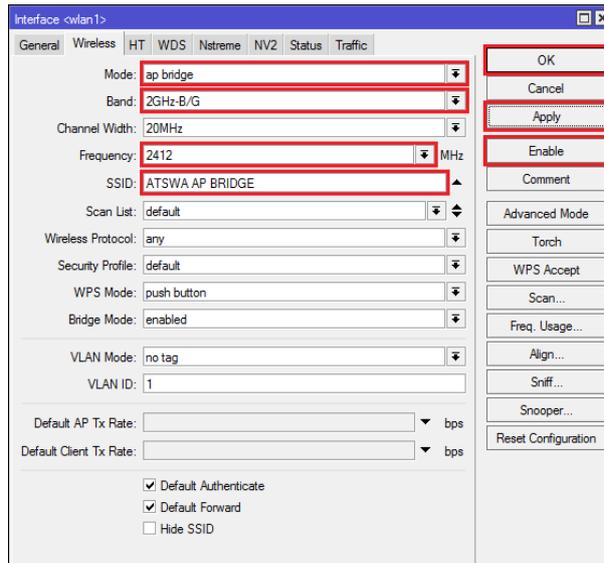
Topologi *Wireless AP Bridge*

Access Point adalah istilah yang digunakan untuk perangkat wireless yang dikonfigurasi sebagai pemancar atau pemberi koneksi. Untuk membuat *Access Point* pada perangkat MikroTik pertama masuk ke **Wireless Tables** dengan cara klik **Wireless** lalu double klik **Wireless** yang ada pada *Interface List*.



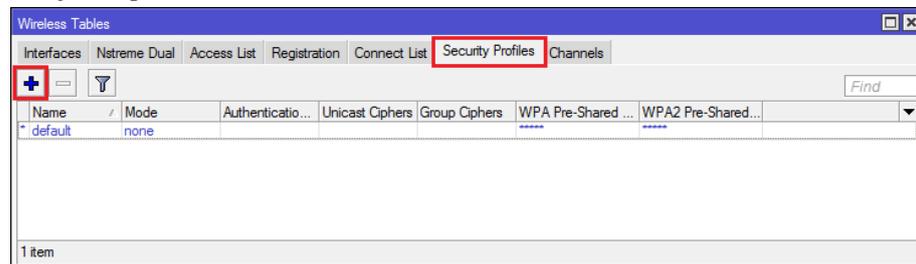
Jendela *Wireless Tables*

Setelah Anda masuk di jendela **Wireless Interface** lakukan konfigurasi dengan memilih **AP Bridge** pada bagian **mode** lalu pilih **band** yang diinginkan lalu pilih **frequency** yang diinginkan lalu beri nama **AP Bridge** pada bagian **SSID** lalu aktifkan dengan cara klik **Enable** lalu klik **Apply** lalu klik **OK**.



Jendela *Wireless* pada *Interface Wireless Tables*

Anda dapat memberikan password pada Access Point untuk memberikan fasilitas keamanan agar hanya pihak-pihak tertentu saja yang dapat terhubung. Caranya masuk ke menu **Security Profiles** pada **Wireless Tables** lalu klik “+” atau **Add**.

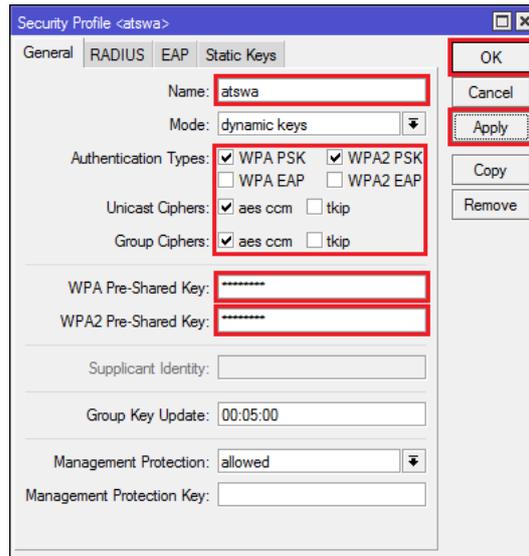


Jendela *Security Profiles* pada *Wireless Tables*

Metode keamanan pada perangkat wireless umumnya menggunakan metode authentication (WPA-PSK, WPA-AEP) dan Enkripsi (AES, TKIP, WEP)

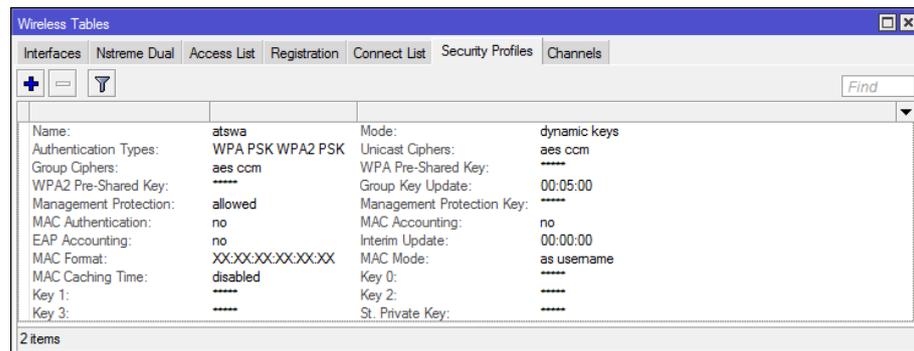


Setelah masuk di jendela pengaturan *Security Profile* masukkan nama atau identitas *password* pada *name* lalu pilih enkripsi yang diinginkan pada **Authentication Types** lalu masukkan **Password** pada **Shared Key** lalu klik **Apply** lalu klik **OK**.



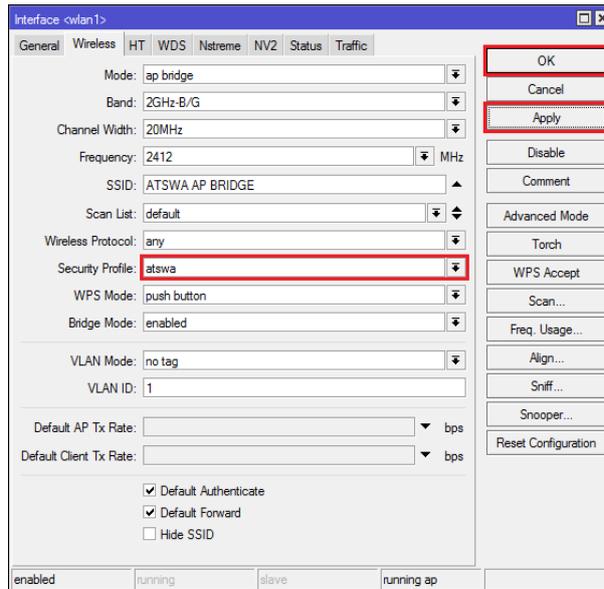
Jendela *General* pada *Security Profile*

Untuk melihat *Security Profile* atau *Password* yang telah dibuat dapat dilihat pada menu *Security Profiles Wireless Tables*.



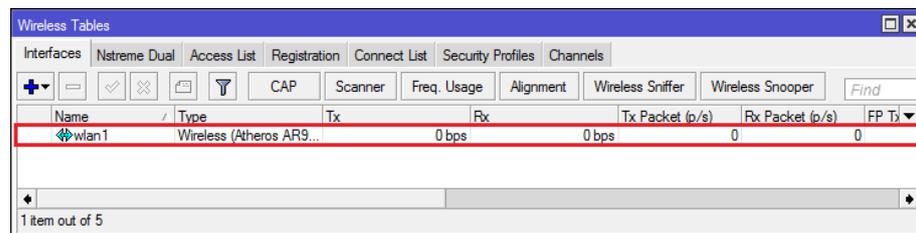
Jendela *Security Profiles* pada *Wireless Tables*

Selanjutnya adalah memasukkan *Security Profile* ke *Wireless Interface* dengan cara masuk kembali ke jendela pengaturan *Wireless Interface* dan pada bagian *Security Profile* mengubah dari konfigurasi *default* ke *profile* yang telah dibuat.



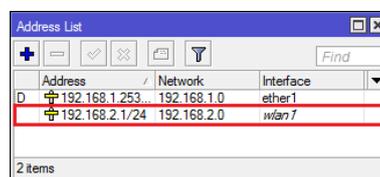
Jendela *Wireless* pada *Interface Wireless Tables*

Hasil konfigurasi pada *Interface List* dapat dilihat pada *Wireless Tables*.



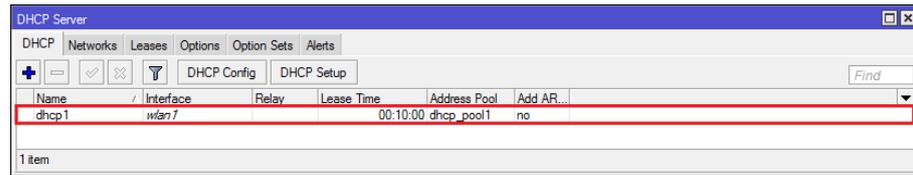
Jendela *Interface* pada *Wireless Tables*

Setelah itu konfigurasi *IP Address* untuk *Wireless Interface*.



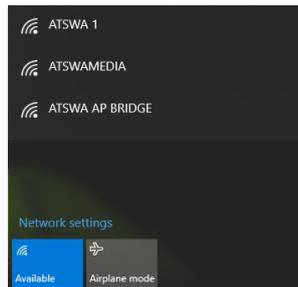
Jendela *Address List*

Agar *host* mendapatkan *IP Address* secara otomatis dari *Wireless Interface* maka konfigurasi *Wireless Interface* menjadi *DHCP Server*.



Jendela DHCP Server

Lakukan pengujian pada komputer dengan cara melihat *Access Point* yang sudah dibuat.



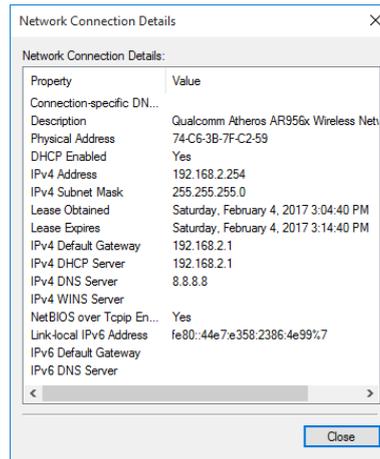
Daftar *Access Point* pada Komputer

Masukkan *Password* sesuai dengan *Security Profile* yang sudah dibuat.



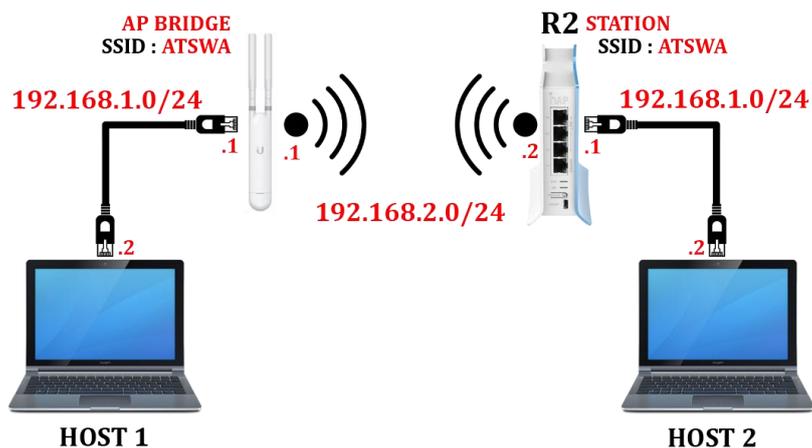
Menu untuk memasukkan *Password*

Setelah itu periksa pada komputer apakah sudah mendapatkan *IP Address* dari *AP Bridge*.



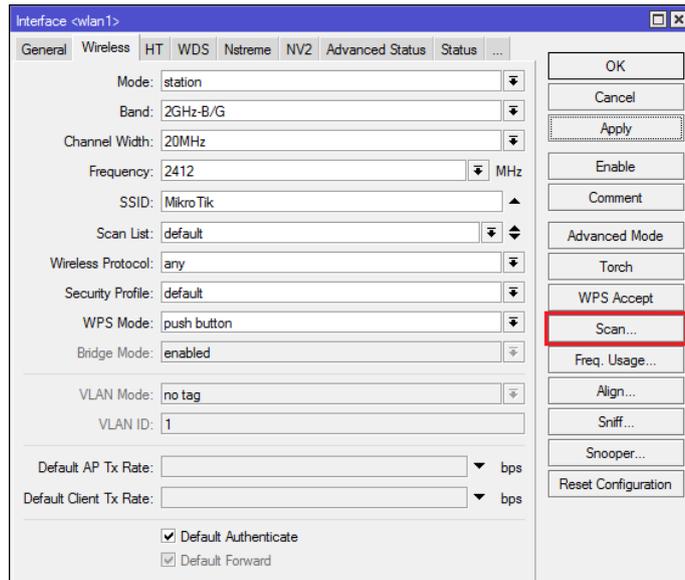
Jendela *Network Connection* pada Komputer

L4.2. STATION (PENERIMA)



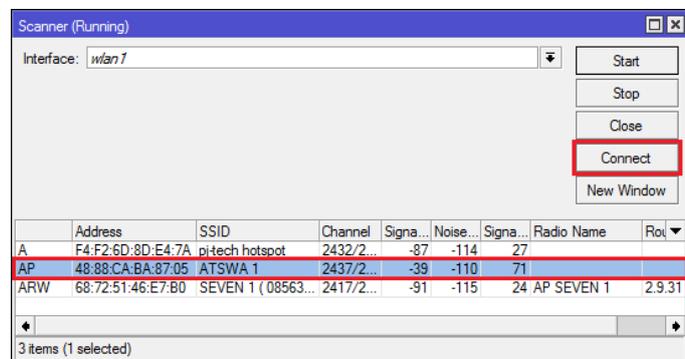
Topologi *Wireless Station*

Untuk membuat penerima atau *Station Bridge* pada Mikrotik caranya masuk ke jendela konfigurasi **Wireless Interface** dengan cara klik **Wireless** lalu double klik **Wireless** yang ada pada **Interface List Wireless Tables**. Setelah masuk di jendela konfigurasi **Wireless Interface** klik **Scan**.



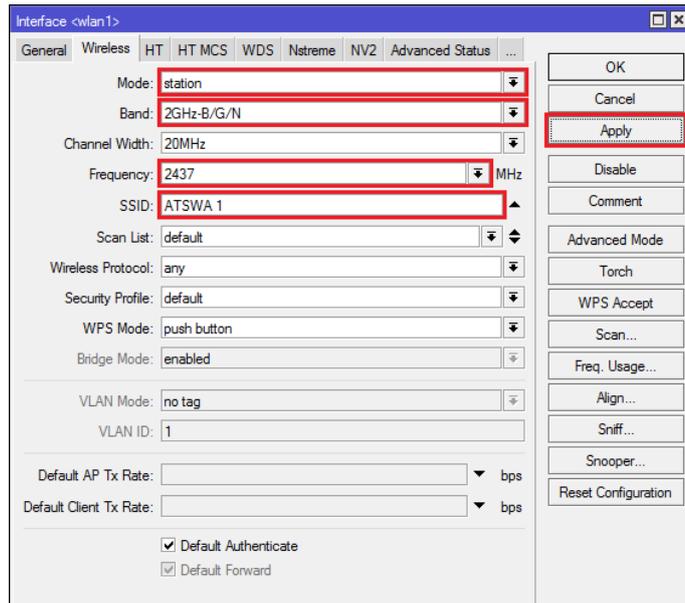
Jendela *Wireless* pada *Interface Wireless Tables*

Setelah itu klik **Start** lalu pilih **Access Point** yang akan dihubungkan lalu klik **Connect**. Pilih **Access Point** yang bukan MikroTik karena **Station** adalah konfigurasi untuk terhubung dengan **Access Point** perangkat selain MikroTik.



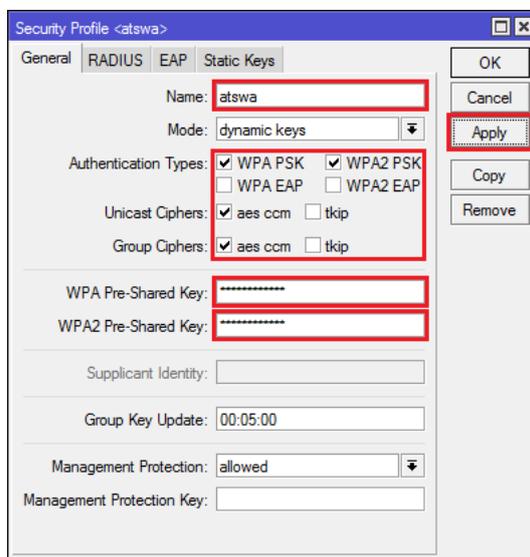
Jendela *Wireless Scanner*

Setelah itu pada jendela konfigurasi **Wireless Interface** akan muncul konfigurasi sesuai dengan konfigurasi pada **Access Point** terutama pada bagian band, *ferquency*, dan SSID. Setelah itu klik **Apply** lalu klik **OK**.



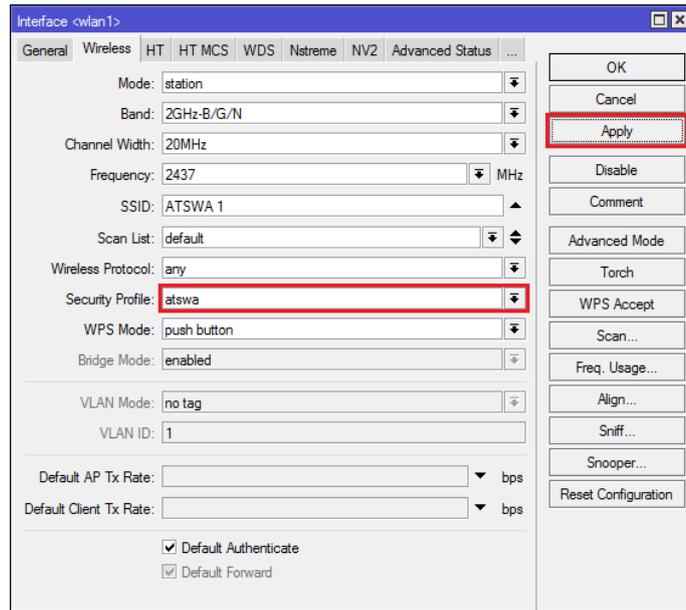
Jendela *Wireless* pada *Interface Wireless Tables*

Jika *Access Point* yang sudah terhubung menggunakan **password**, buat terlebih dahulu **password** pada **Security Profile** yang sama agar dapat terhubung dengan cara klik “+” atau **Add** pada menu **Security Profiles**.



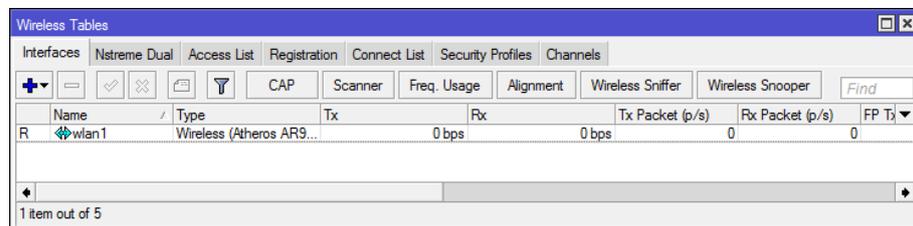
Jendela *Security Profile* pada *Wireless Tables*

Setelah itu masukkan **profile** yang telah dibuat pada jendelan pengaturan **Wireless Interface** lalu klik **Apply** lalu klik **OK**.



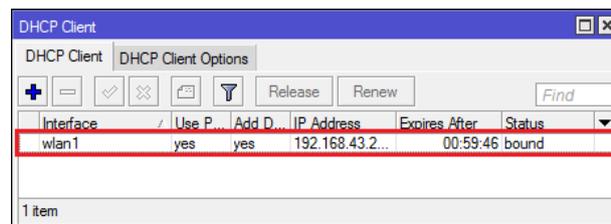
Jendela *Wireless* pada *Interface Wireless Tables*

Pastikan **Wireless Interface** pada **Interface List** sudah dalam kondisi **R** atau **Running** atau berjalan.



Jendela *Interface* pada *Wireless Tables*

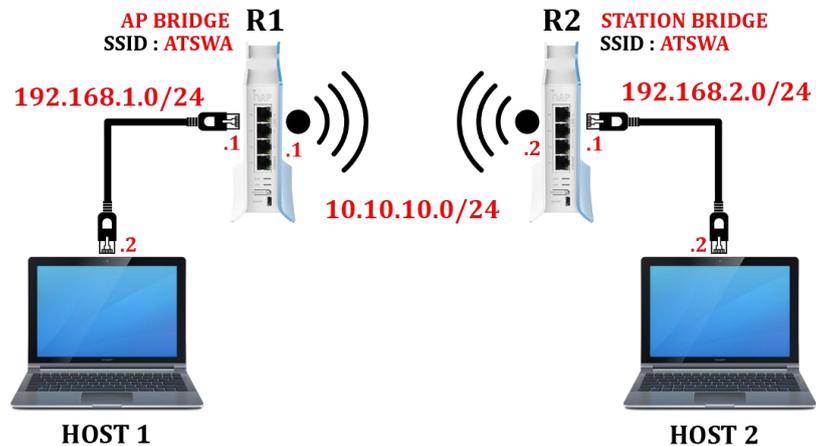
Jika **Access Point** tersebut menggunakan konfigurasi **DHCP Server** lakukan konfigurasi **DHCP Client** pada **Wireless Interface**.



DHCP Client List pada *DHCP Client*

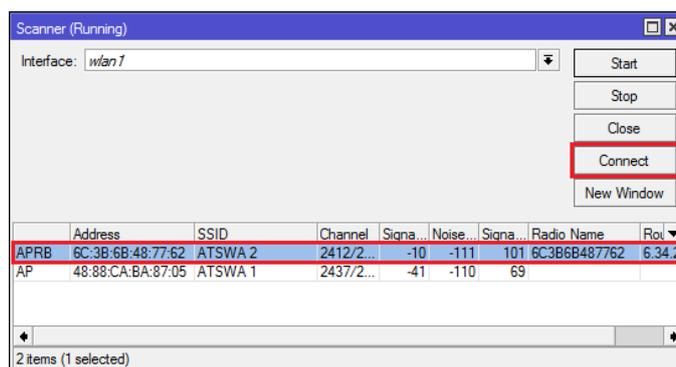
Lakukan pengujian terhadap **Access Point** dengan menggunakan perintah **ping** atau periksa pada **Address List** untuk memastikan **Wireless Interface** sudah mendapatkan **IP Address**.

L4.3. STATION BRIDGE (PENERIMA)



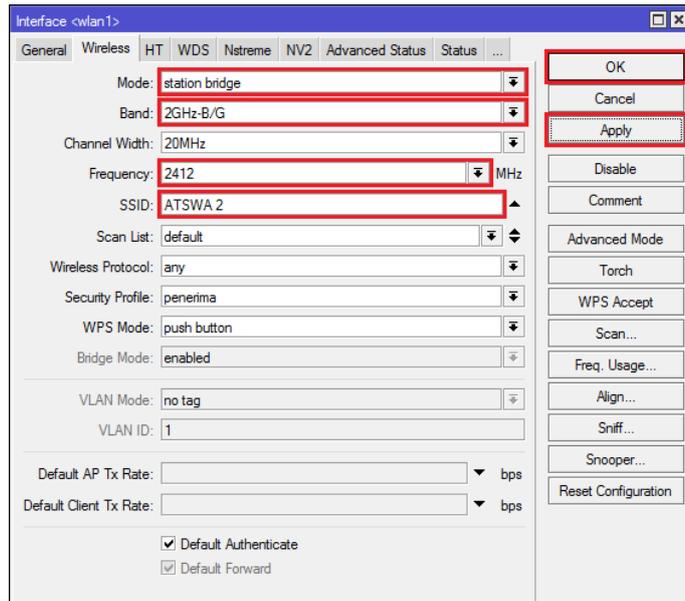
Topologi *Wireless Station Bridge*

Station Bridge adalah mode penerima khusus untuk menerima dari perangkat **Access Point** MikroTik. Untuk tahap konfigurasi tidak berbeda dengan konfigurasi sebelumnya hanya saja pastikan perangkat yang akan dihubungkan benar-benar perangkat MikroTik, umumnya perangkat MikroTik muncul dengan ID **APRB** atau **Access Point Routerboard**.



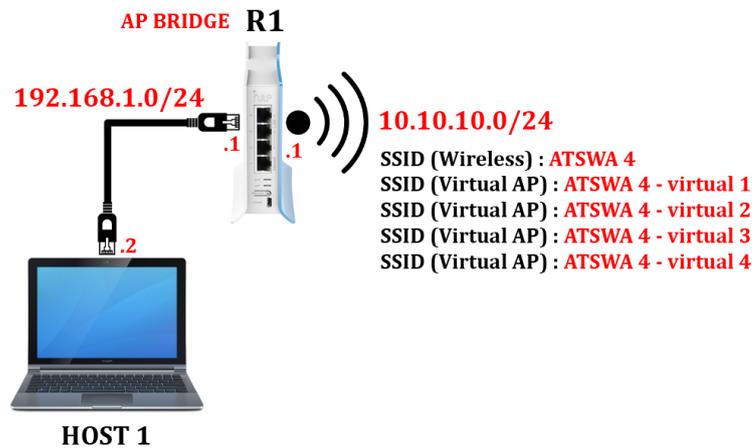
Jendela *Wireless Scanner*

Setelah itu pastikan pada jendela pengaturan **Wireless Interface** mode yang aktif adalah **Station Bridge**.



Jendela *Wireless* pada *Interface Wireless Tables*

L4.4. VIRTUAL ACCESS POINT BRIDGE



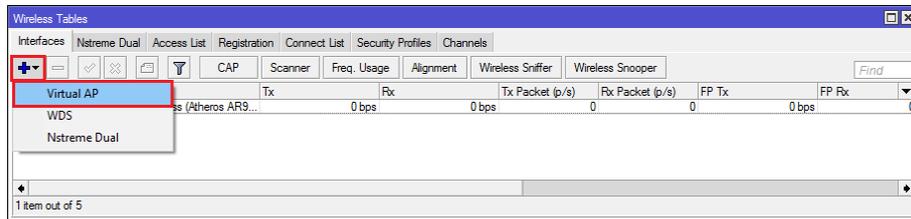
Topologi *Virtual AP Bridge*

virtual access point adalah fitur untuk membuat access point lebih dari satu menggunakan satu wireless interface



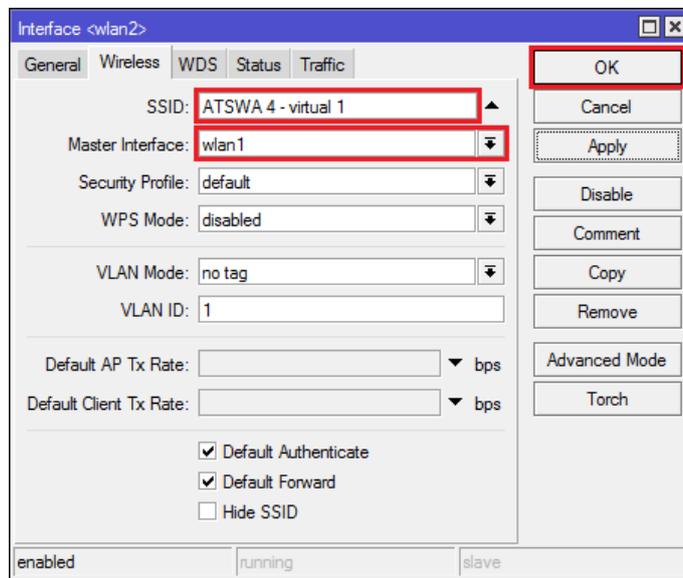
Anda dapat membuat lebih dari 1 *Access Point* menggunakan MikroTik, istilah umumnya *Virtual Access Point*. Langkah membuat

Virtual Access Point adalah dengan cara masuk ke **Wireless Tables** lalu masuk ke menu **Interface** dan klik “+” atau **Add**.



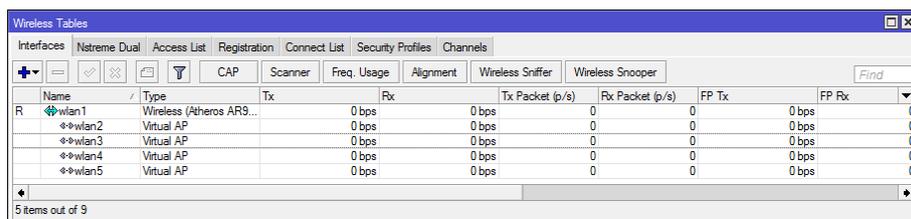
Menu *Create Virtual AP* pada *Interface Wireless Tables*

Seperti pada jendela **Wireless Interface** yang perlu dikonfigurasi adalah SSID serta **Master Wireless Interface** yang digunakan.



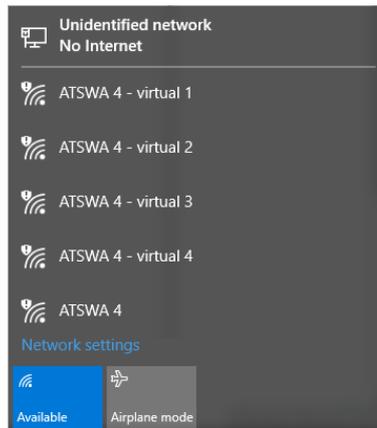
Jendela *Wireless Interface*

Virtual Access Point yang telah dibuat dapat dilihat di menu **Interface** pada **Wireless Tables**.



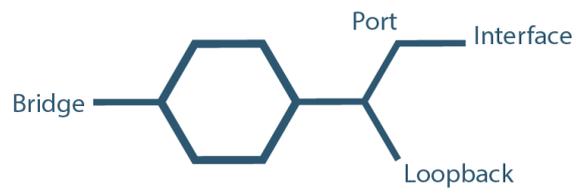
Daftar *Virtual Access Point* pada *Wireless Interface*

Selain itu dapat dilihat pada komputer



Tampilan *Access Point* pada Komputer

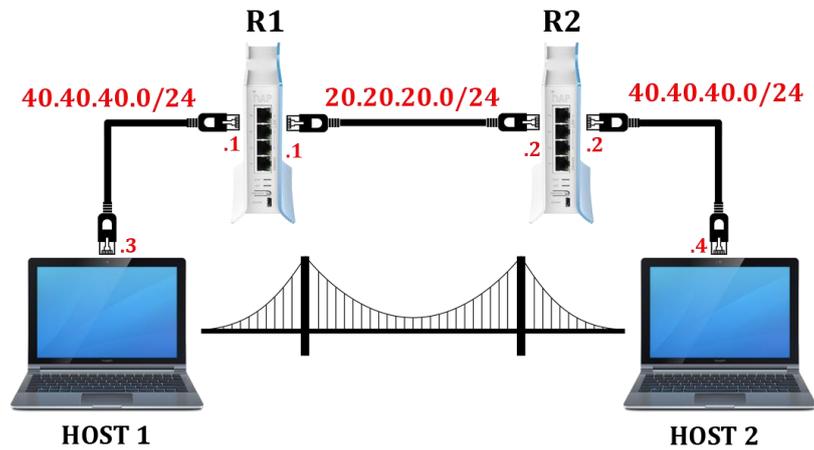
LABORATORIUM 5



MIKROTIK BRIDGE

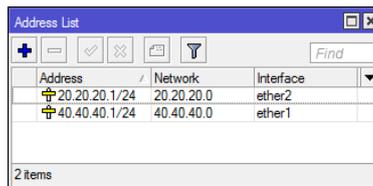
L5.1. WIRED BRIDGE

Bridge adalah layanan yang menghubungkan dua atau lebih interface agar seolah-olah berada dalam satu segmen jaringan yang sama



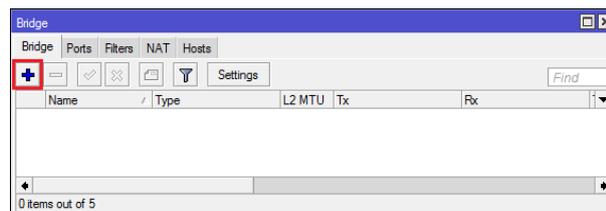
Topologi *Wired Bridge*

Jika Anda ingin menggabungkan dua jaringan menggunakan fasilitas **Bridge** pada **MikroTik** seperti topologi tersebut yang perlu dilakukan adalah konfigurasi **IP Address interface** yang menghubungkan komputer dan juga **router**.



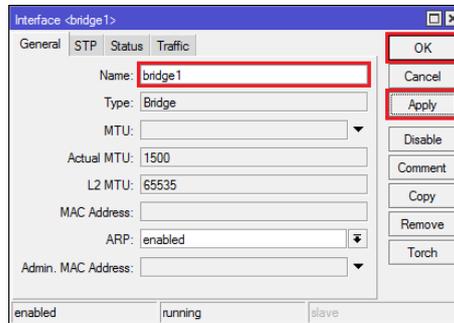
IP Address pada Router 1

Setelah itu masuk ke menu **Bridge** lalu klik “+” atau **Add**



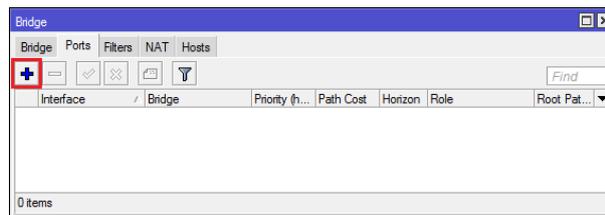
Jendela Bridge List pada Bridge

Setelah itu buat **Interface Bridge** dengan cara memberikan nama **Bridge** lalu klik **Apply** lalu klik **OK**.



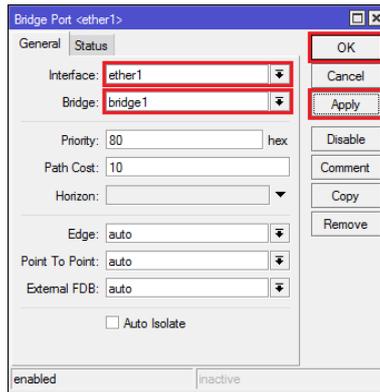
Jendela General pada Bridge

Setelah itu masuk ke menu **Port** pada **Bridge** dan buat **Port** baru dengan cara klik “+” atau **Add**.



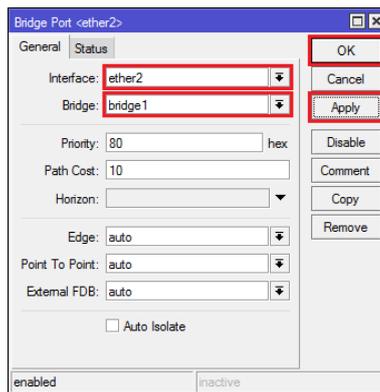
Jendela Port pada Bridge

Port yang pertama dibuat adalah **Port** yang menghubungkan **Ethernet** ke **Router** dengan **Bridge**. Pada **Interface** pilih **Ethernet** yang terhubung dengan **Router** dan pada **Bridge** pilih **Interface Bridge** yang dibuat sebelumnya lalu klik **Apply** lalu klik **OK**.



Jendela konfigurasi *Bridge Port* pada *Bridge*

Port yang pertama dibuat adalah **Port** yang menghubungkan **Ethernet** ke Komputer dengan **Bridge**. Pada **Interface** pilih **Ethernet** yang terhubung dengan komputer dan pada **Bridge** pilih **Interface Bridge** yang dibuat sebelumnya lalu klik **Apply** lalu klik **OK**.



Jendela konfigurasi *Bridge Port* pada *Bridge*

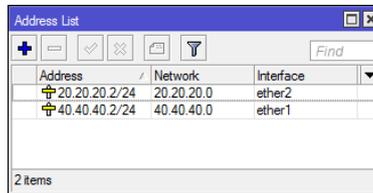
Setelah itu **port** yang telah dibuat dapat dilihat di **Port List** pada **Bridge**.

| Interface | Bridge | Priority (h...) | Path Cost | Horizon | Role | Root Pat... |
|-----------|---------|-----------------|-----------|---------|-----------------|-------------|
| ether1 | bridge1 | 80 | 10 | | designated port | |
| ether2 | bridge1 | 80 | 10 | | designated port | |

2 items

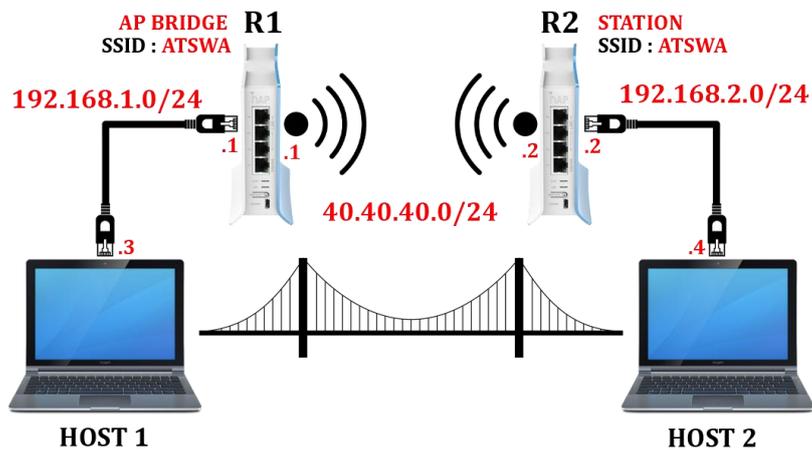
Daftar *Port Bridge* yang telah dibuat pada *Ports Bridge*

Untuk menghubungkan *router* sisi lainnya lakukan langkah yang sama dimulai dengan memberikan *IP Address* pada *Ethernet* yang terhubung dengan *Router* dan *Ethernet* yang terhubung dengan Komputer. Dan membuat *Interface Bridge* serta *Port Bridge*.



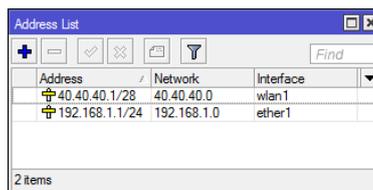
IP Address pada *Router 2*

L2.11. WIRELESS BRIDGE



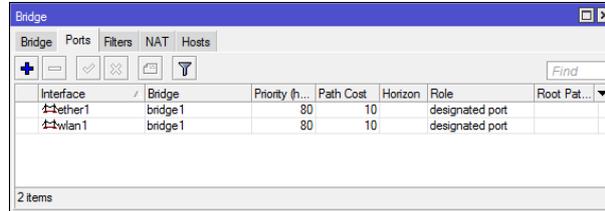
Topologi *Wireless Bridge*

Jika Anda ingin menerapkan menggunakan media *Wireless* langkah yang dilakukan tidak jauh berbeda, Anda hanya perlu mengganti *Interface* yang digunakan saja dari *ethernet* ke *wireless ethernet*. Langkah pertama memberikan *IP Address* pada *Ethernet* yang akan dihubungkan ke komputer dan ke *Router Bridge*.



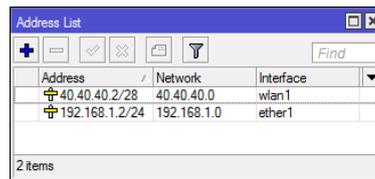
IP Address Pada *Router 1*

Setelah itu membuat **Interface Bridge** dan membuat **Port** yang menghubungkan **Ethernet** ke **Interface Bridge**.



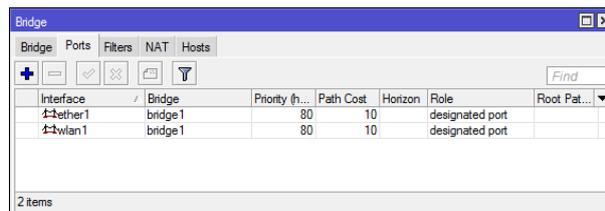
Daftar *Bridge* pada *Ports Bridge Router 1*

Pada sisi *Router* yang lainnya juga dilakukan konfigurasi yang sama yaitu memberikan *IP Address* pada *Ethernet* yang akan dihubungkan ke *Komputer* dan ke *Router Bridge*.



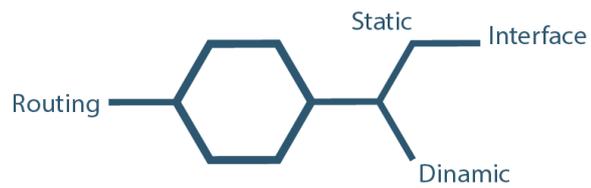
IP Address pada *Router 2*

Setelah itu membuat **Interface Bridge** dan membuat **Port** yang menghubungkan **Ethernet** ke **Interface Bridge**.



Daftar *Bridge* pada *Ports Bridge Router 2*

LABORATORIUM 6



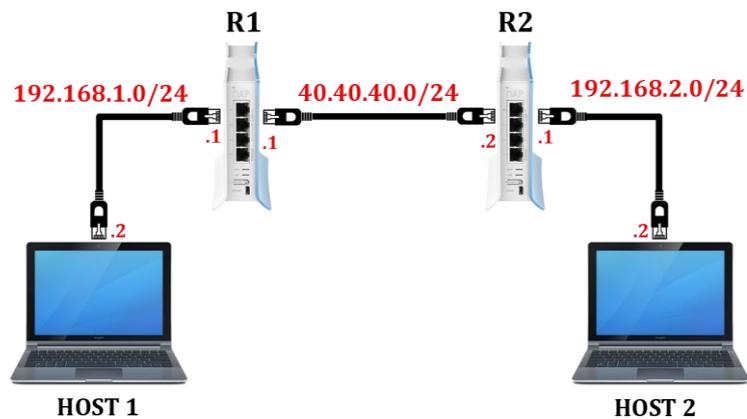
MIKROTIK ROUTING

L6.1. STATIC ROUTING

Routing adalah suatu proses pengiriman dan pengambilan paket dari jaringan yang berbeda



Static Routing adalah konfigurasi *router* untuk menghubungkan jaringan berbeda dengan menggunakan alamat **network** dari jaringan dengan **gateway** dari **router** tersebut.



Topologi *Static Routing*

Jika Anda ingin menerapkan *static routing* sesuai topologi tersebut konfigurasi *Ethernet* yang terhubung dengan jaringan lokal dengan *ethernet* yang terhubung dengan *router* lainnya.

| Address | Network | Interface |
|----------------|-------------|-----------|
| 40.40.40.1/29 | 40.40.40.0 | ether1 |
| 192.168.1.1/24 | 192.168.1.0 | ether2 |

IP Address pada Router 1

| Address | Network | Interface |
|----------------|-------------|-----------|
| 40.40.40.2/29 | 40.40.40.0 | ether1 |
| 192.168.2.1/24 | 192.168.2.0 | ether2 |

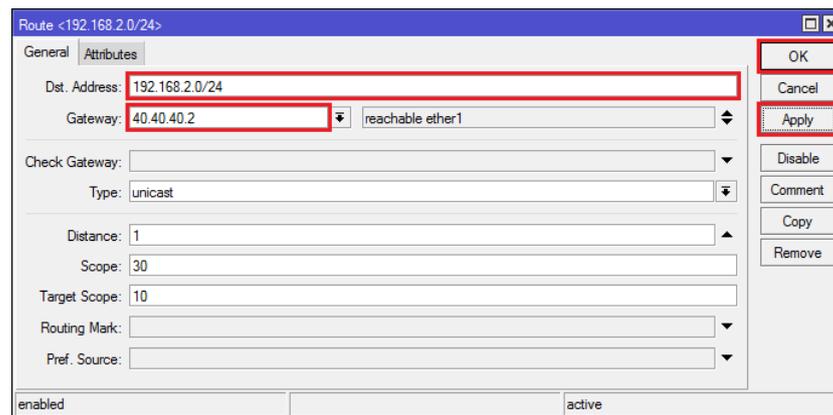
IP Address pada Router 2

Setelah *IP Address* pada masing-masing *Router* dikonfigurasi selanjutnya membuat *Static Routing* dengan cara klik **IP** lalu klik **Router** lalu klik “+” atau **Add**.



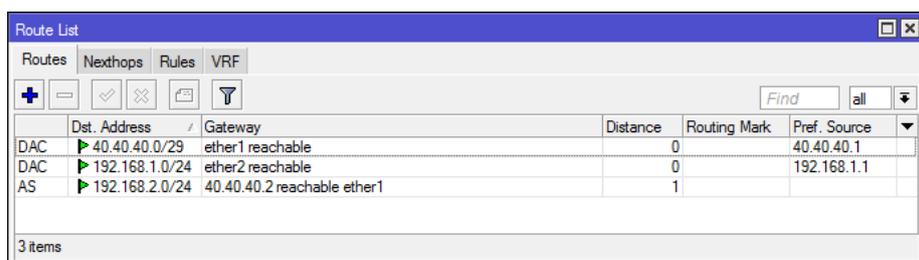
Router List pada Router 1

Masukkan **Network Address** beserta **Prefix** dari Jaringan tujuan pada **Dest. Address** dan memasukkan **Gateway** pada **Gateway**.



Jendela untuk membuat Routing Statis

Setelah itu periksa pada **router list** dan pastikan sudah dalam Status **AS** dan **reachable**.

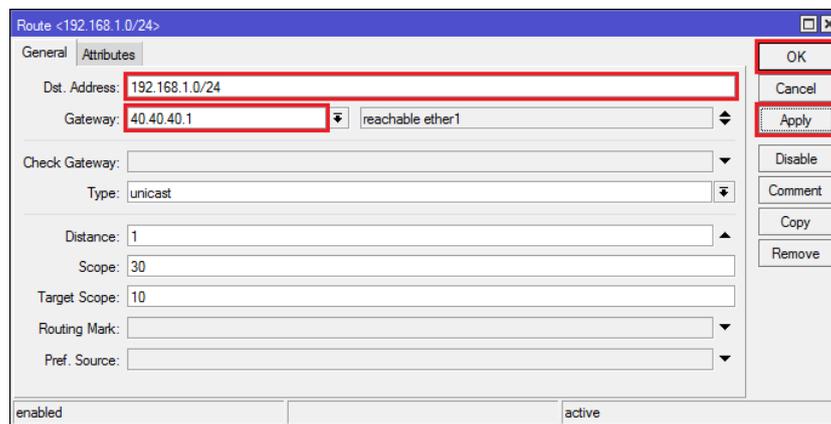


Router List pada Router 1

Untuk *router* sisi lainnya lakukan hal yang sama dengan masuk ke **Router List** lalu membuat list baru dan memasukkan **Network Address** serta **Prefix** dari **Network** tujuan dan **Gateway** dari **Router** tujuan.

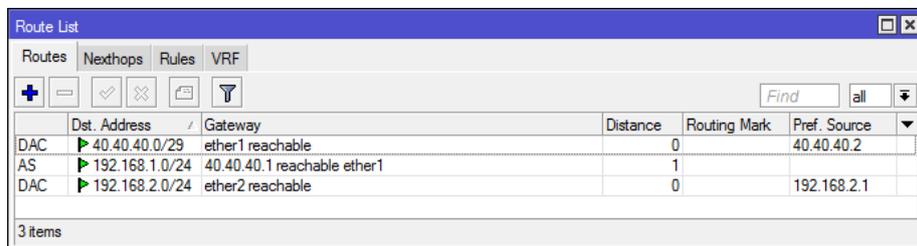


Router List pada *Router 2*



Jendela untuk membuat *Routing* Statis

Setelah itu periksa hasil konfigurasi pada **Router List** bahwa kondisi sudah **AS** dan **reacable**.

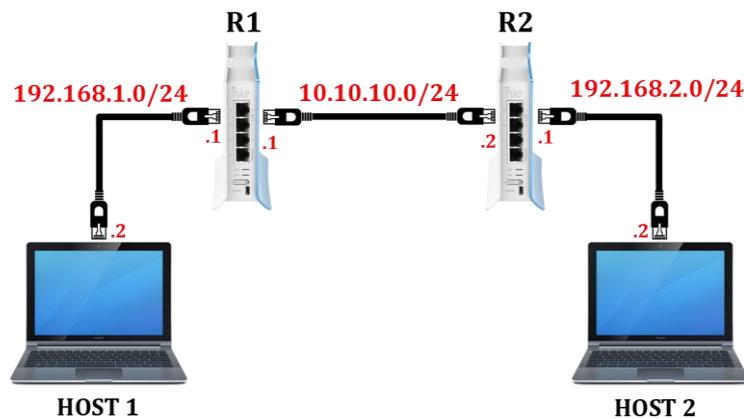


Router List pada *Router 2*

Untuk menguji apakah jaringan yang berbeda sudah saling terhubung lakukan pengujian dengan perintah *ping* dari komputer yang berada pada jaringan satu ke jaringan lainnya

L6.2. DINAMIC ROUTING (RIPv2)

Dinamic Routing adalah konfigurasi *router* untuk menghubungkan jaringan berbeda menggunakan alamat *network* dari jaringan yang terhubung dengan *router* tersebut



Topologi *Dinamic Routing RIPv2*

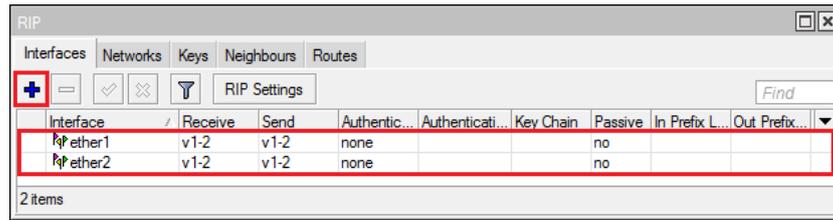
Pertama lakukan konfigurasi *IP Address* pada masing-masing *router* sesuai topologi tersebut.

| Address | Network | Interface |
|----------------|-------------|-----------|
| 10.10.10.1/24 | 10.10.10.0 | ether1 |
| 192.168.1.1/24 | 192.168.1.0 | ether2 |

| Address | Network | Interface |
|----------------|-------------|-----------|
| 10.10.10.2/24 | 10.10.10.0 | ether1 |
| 192.168.2.1/24 | 192.168.2.0 | ether2 |

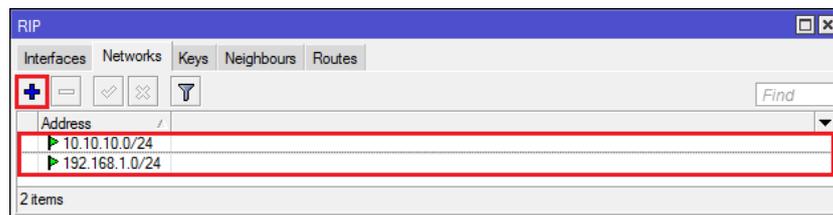
IP Address pada *Router 1* dan *Router 2*

Setelah itu klik menu *Router* lalu klik *RIPv2* lalu klik *Interface* lalu klik *Add* atau "+" lalu pilih interface yang terhubung dengan jaringan yang akan di *routing*. Sesuai dengan topologi yang digunakan maka *interface* yang digunakan adalah *interface ether1* da *ether2*.

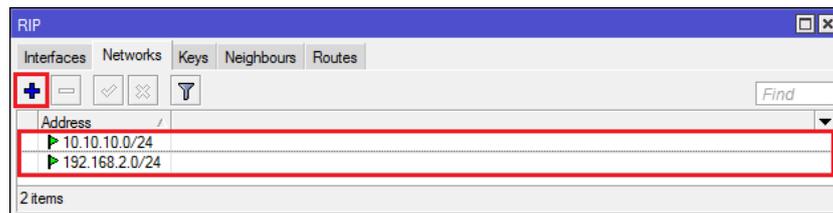


Daftar *Interface* yang digunakan pada *R1*

Setelah itu klik **Networks** klik **Add** atau “+” lalu masukkan *Network Address* tujuan yang akan di *routing*.

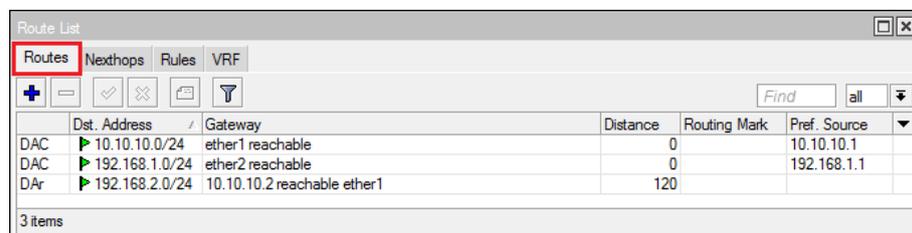


Network Address pada *R1*



Network Address pada *R2*

Untuk melihat konfigurasi *routing* yang telah dibuat Anda dapat melihat di *Router List*. Pastikan *ethernet* dalam kondisi **DAr** dan **reachable**.



Route List pada *R1*

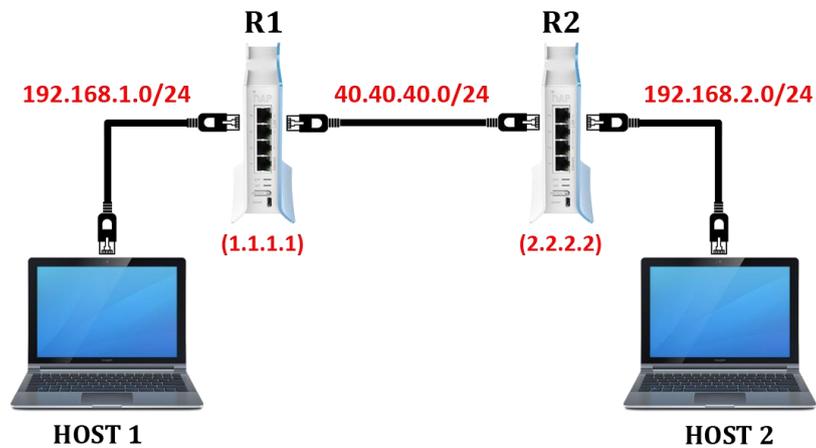
| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|----------------|-----------------------------|----------|--------------|--------------|
| DAC | 10.10.10.0/24 | ether1 reachable | 0 | | 10.10.10.2 |
| DAr | 192.168.1.0/24 | 10.10.10.1 reachable ether1 | 120 | | |
| DAC | 192.168.2.0/24 | ether2 reachable | 0 | | 192.168.2.1 |

3 items

Route List pada R2

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan router R1 dengan R2 menggunakan ping.

L6.3. DINAMIC ROUTING (OSPF)



Topologi *Dinamic Routing OSPF*

Pertama konfigurasi *IP Address* masing-masing *router* sesuai topologi tersebut.

| Address | Network | Interface |
|----------------|-------------|-----------|
| 40.40.40.1/24 | 40.40.40.0 | ether1 |
| 192.168.1.1/24 | 192.168.1.0 | ether2 |

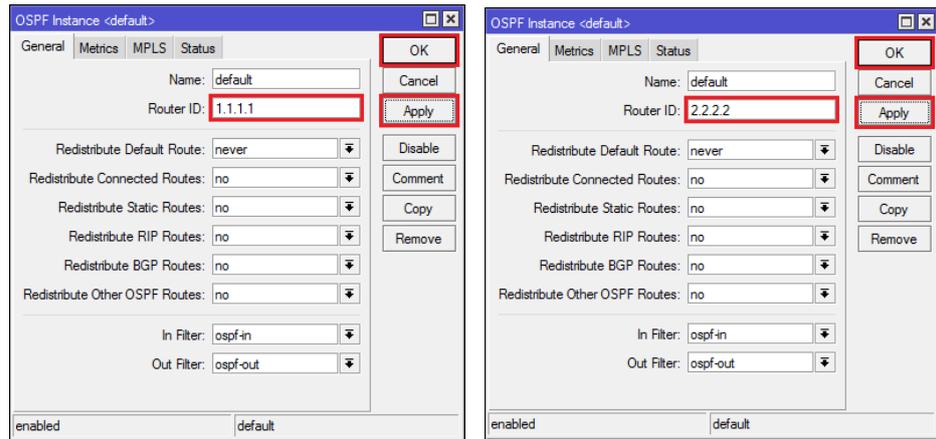
2 items

| Address | Network | Interface |
|----------------|-------------|-----------|
| 40.40.40.2/24 | 40.40.40.0 | ether1 |
| 192.168.2.1/24 | 192.168.2.0 | ether2 |

2 items

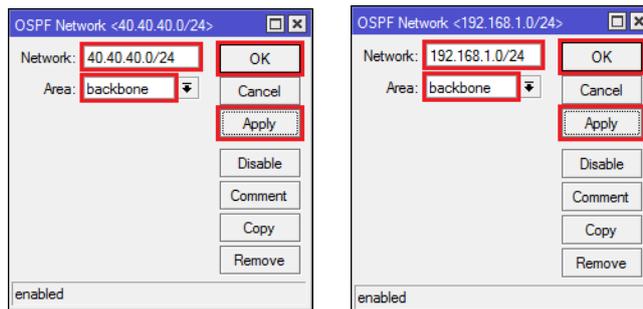
Konfigurasi *IP Address* R1 dan R2

Setelah itu klik **Routing** klik **OSPF** klik **Instances** double klik rules **default** pada **Instances list** lalu ubah Router ID. Router ID R1 1.1.1.1 dan R2 2.2.2.2

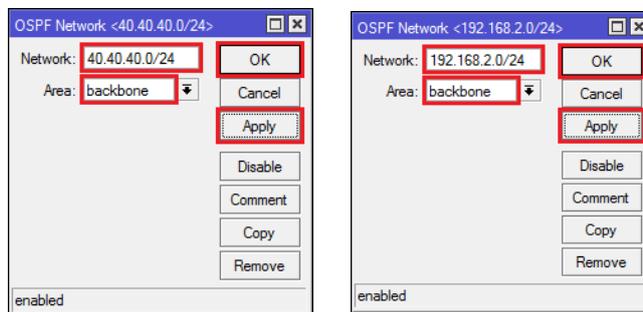


Konfigurasi Router ID pada R1 dan R2

Setelah itu masuk klik menu **Network** lalu klik “+” atau **Add** lalu masukkan **Network Address** yang ada pada **network** dan pada **Area** pilih **backbone**.

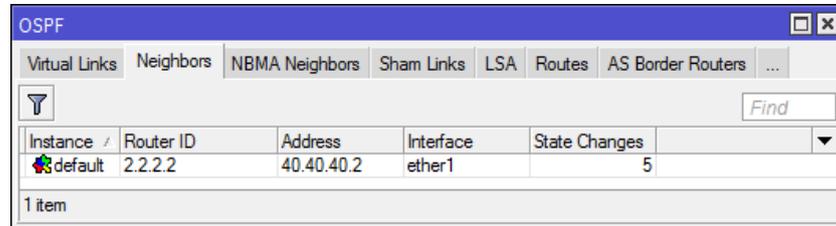


Konfigurasi pada R1

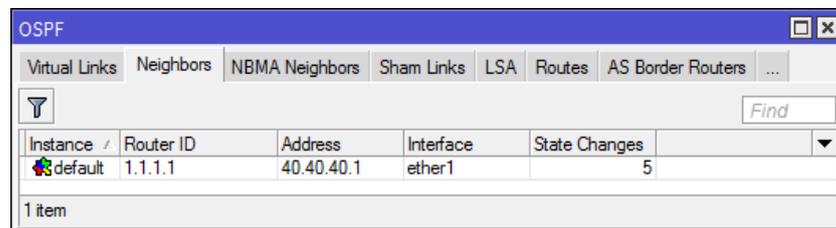


Konfigurasi pada R2

Setelah itu periksa menu *Neighbors* pada **R1** dan pastikan **Router ID R2** sudah muncul dan juga sebaliknya pastikan pada *Neighbors R2* **Router ID R1** sudah muncul.

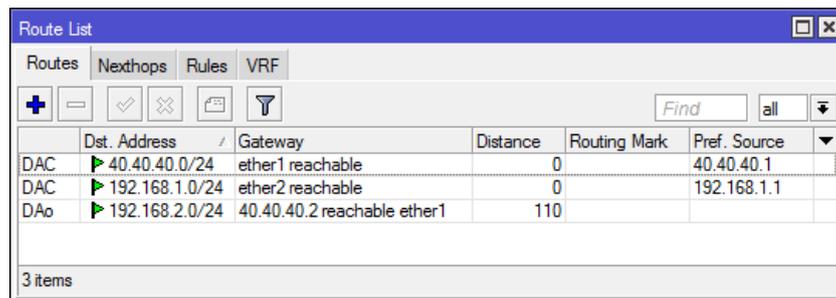


Neighbors pada Router R1



Neighbors pada Router R2

Setelah itu masuk ke *Router List* untuk melihat konfigurasi routing sudah berhasil atau belum



Router List pada R1

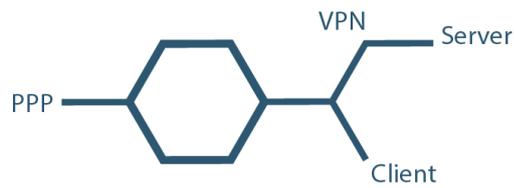
| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|----------------|-----------------------------|----------|--------------|--------------|
| DAC | 40.40.40.0/24 | ether1 reachable | 0 | | 40.40.40.2 |
| DAo | 192.168.1.0/24 | 40.40.40.1 reachable ether1 | 110 | | |
| DAC | 192.168.2.0/24 | ether2 reachable | 0 | | 192.168.2.1 |

3 items

Router List pada R2

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan router R1 dengan R2 menggunakan ping.

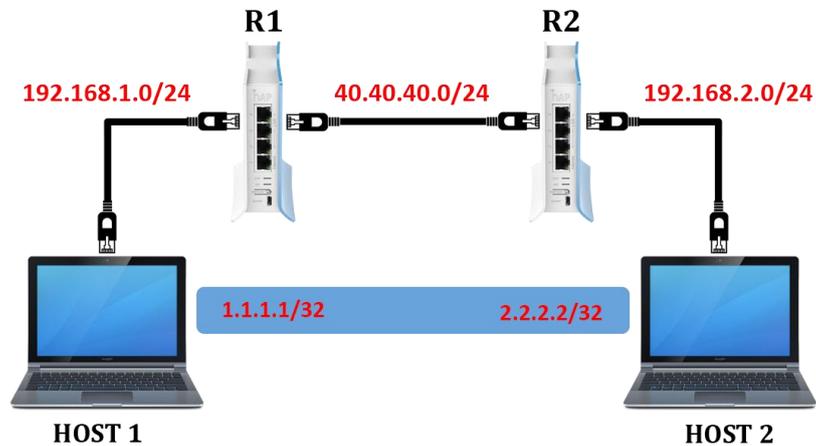
LABORATORIUM 7



MIKROTIK TUNNEL

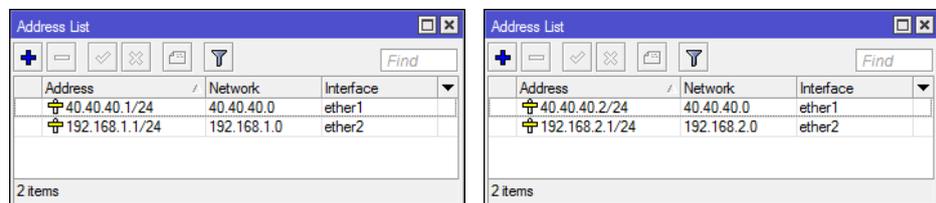
L7.1. IPIP TUNNEL

IPIP bekerja dengan melakukan enkapsulasi paket data dari suatu ip ke ip lainnya dan membentuk sebuah tunnel



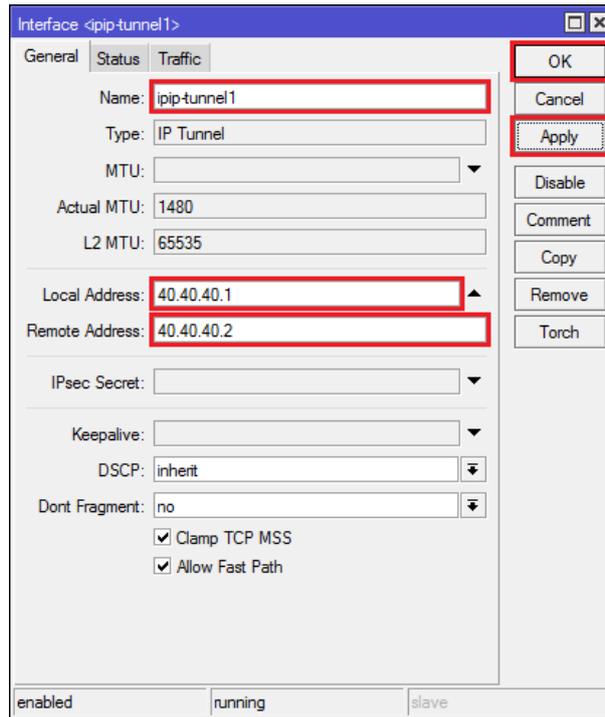
Topologi *IPIP Tunnel*

Pertama konfigurasi *IP Address* pada *Router R1* dan *R2* sesuai dengan topologi tersebut.

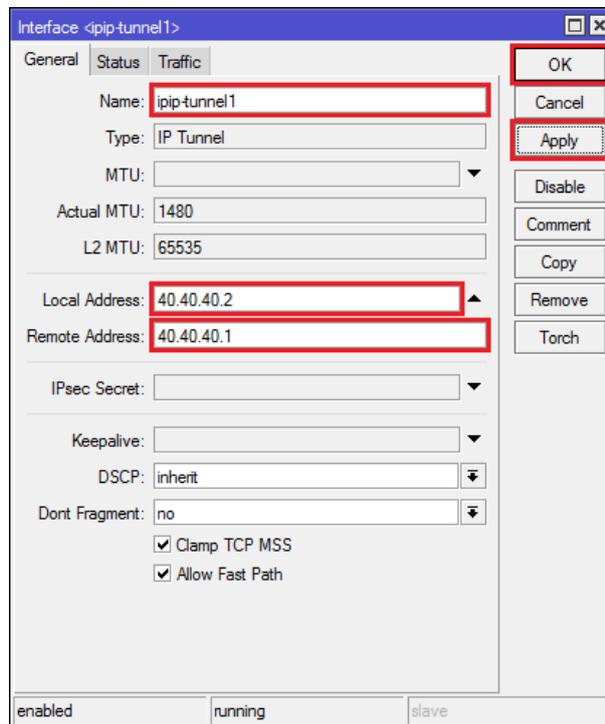


IP Address pada *Router R1* dan *R2*

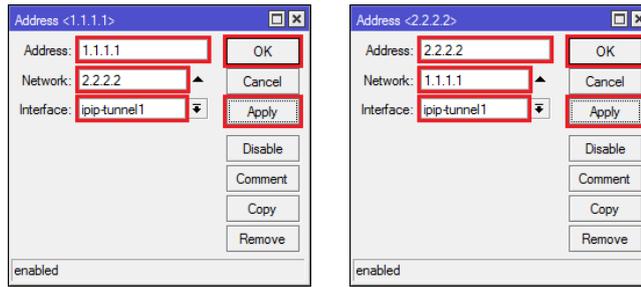
Setelah itu klik **Interface** lalu klik “+” atau **Add** dan masukkan *IP Address (Local/Asal dan Remote/Tujuan)* sesuai dengan Topologi lalu klik **Apply** klik **OK**.



Konfigurasi *IPIP Tunnel* pada Router **R1**

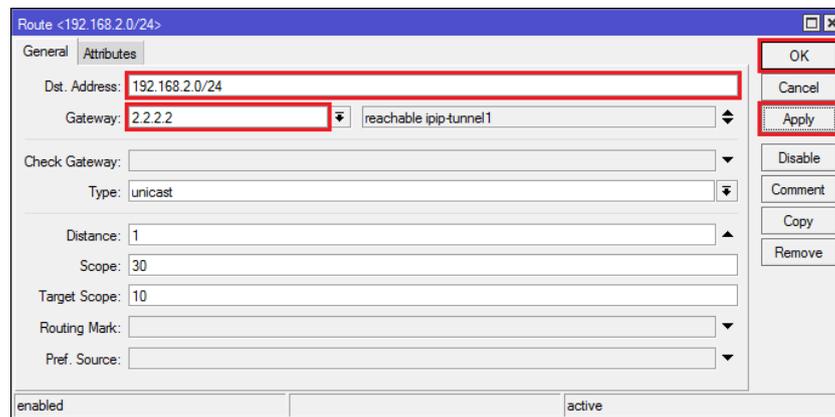


Konfigurasi *IPIP Tunnel* pada Router **R2**

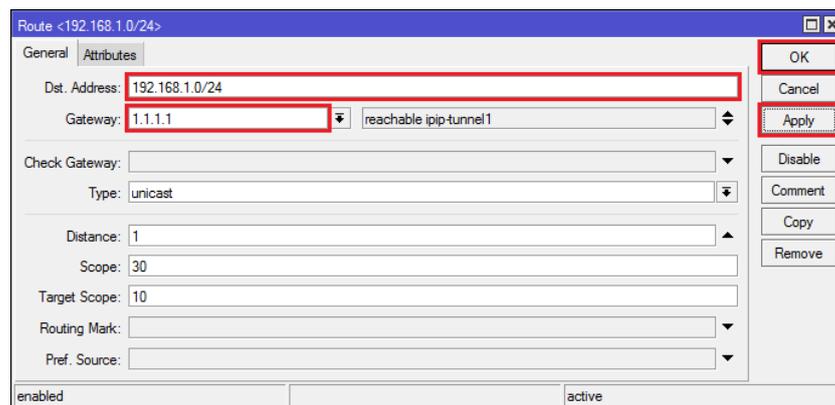


IP Address (IPIP Tunnel) pada R1 dan R2

Setelah itu masuk ke *Route List* dan tambahkan *routing* pada **R1** dan **R2**. Pada Router **R1** masukkan *IP Network Address* tujuan (**R2**) pada **Dst Address** dan *IP Tunnel* pada **Gateway** dan pada Router **R2** juga sebaliknya. Setelah itu klik **Apply** dan klik **OK**.



Konfigurasi di Router R1



Konfigurasi di Router R2

Pastikan hasil *routing* pada router **R1** dan **R2** dalam kondisi AS.

| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|----------------|--------------------------------|----------|--------------|--------------|
| DAC | 2.2.2.2 | ipip-tunnel1 reachable | 0 | | 1.1.1.1 |
| DAC | 40.40.40.0/24 | ether1 reachable | 0 | | 40.40.40.1 |
| DAC | 192.168.1.0/24 | ether2 reachable | 0 | | 192.168.1.1 |
| AS | 192.168.2.0/24 | 2.2.2.2 reachable ipip-tunnel1 | 1 | | |

Route List Router R1

| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|----------------|--------------------------------|----------|--------------|--------------|
| DAC | 1.1.1.1 | ipip-tunnel1 reachable | 0 | | 2.2.2.2 |
| DAC | 40.40.40.0/24 | ether1 reachable | 0 | | 40.40.40.2 |
| AS | 192.168.1.0/24 | 1.1.1.1 reachable ipip-tunnel1 | 1 | | |
| DAC | 192.168.2.0/24 | ether2 reachable | 0 | | 192.168.2.1 |

Route List Router R2

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan router R1 dengan R2 menggunakan ping

L7.2. PPPoE TUNNEL

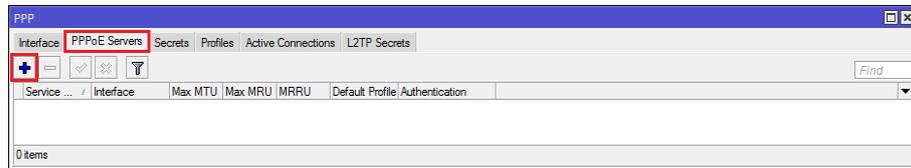
Point-to-Point Protocol over Ethernet atau PPPoE adalah protokol yang digunakan untuk mengenkapsulasi Point-to-Point Protocol Frame dalam Ethernet Frame



Topologi PPPoE Server dan Client

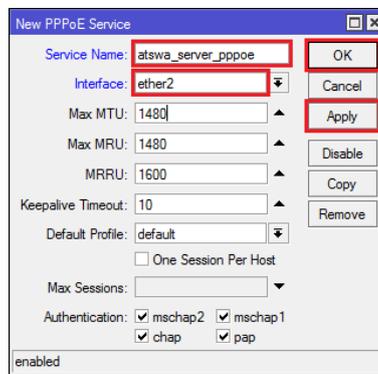
Langkah pertama yang dilakukan dalam membuat jaringan PPPoE adalah membuat Server PPPoE lalu membuat PPPoE Client. PPPoE Client dapat berupa Router atau Komputer. Langkah membuat

PPPoE Server dengan klik **PPP** lalu klik **PPPoE Servers** lalu klik **Add** atau “+”.



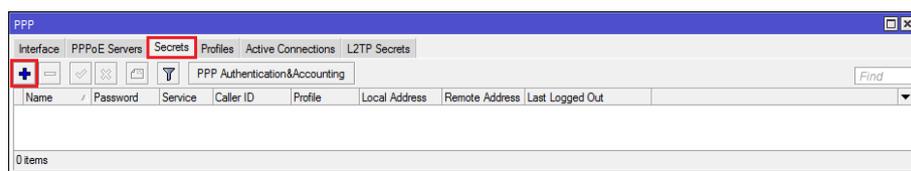
Jendela *PPPoE Server* pada *PPP*

Setelah itu buat nama *PPPoE Server* pada **Service Name** dan pilih **Interface** yang digunakan lalu klik **Apply** klik **OK**.



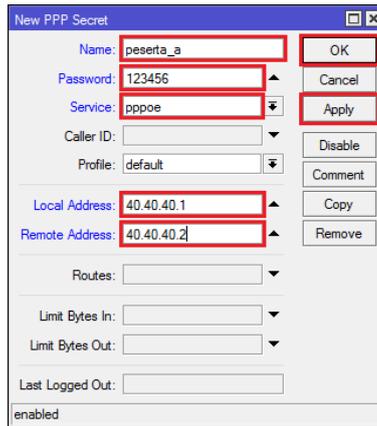
Jendela *PPPoE Service*

Setelah itu klik **Secrets** klik **Add** atau “+”



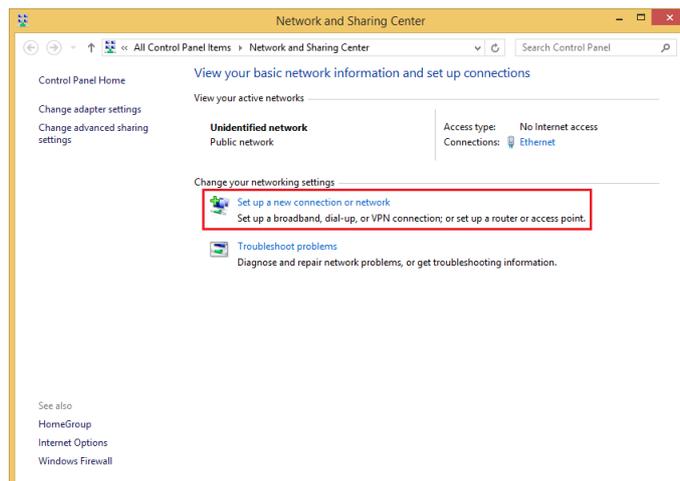
Jendela *Secrets* pada *PPP*

Pada jendela pengaturan *PPP Secret* buat **User** dengan memasukkan **name**, **password**, **service**, **local address**, dan **remote address** lalu klik **Apply** klik **OK**.



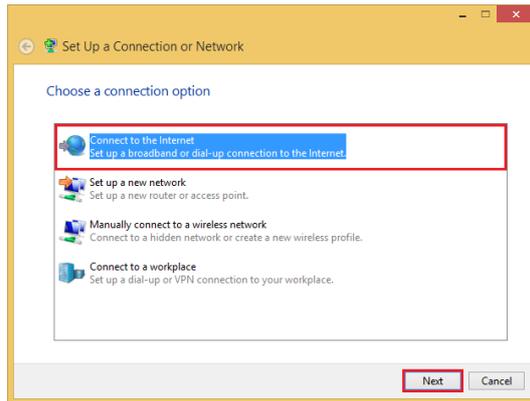
Jendela *PPP Secret*

Setelah selesai membuat *PPPoE Server* selanjutnya melakukan konfigurasi pada sisi *Client*. Jika sisi *Client* yang Anda inginkan adalah Komputer caranya ke ***Network and Sharing Center*** lalu klik ***Set up a new connection or network***.



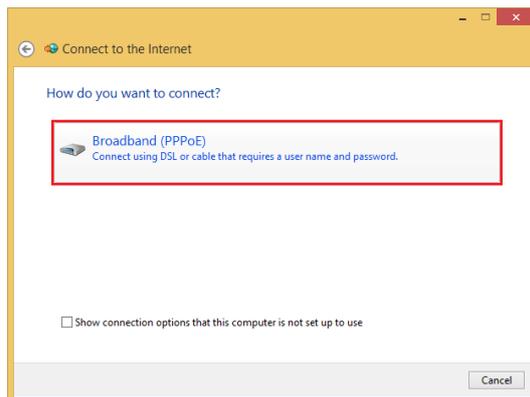
Jendela *Network and Sharing Center*

Lalu klik ***Connect to the Internet*** lalu klik ***Next***.

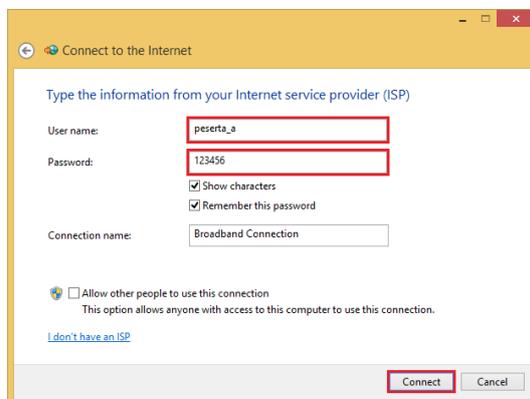


Jendela *Connection or Network*

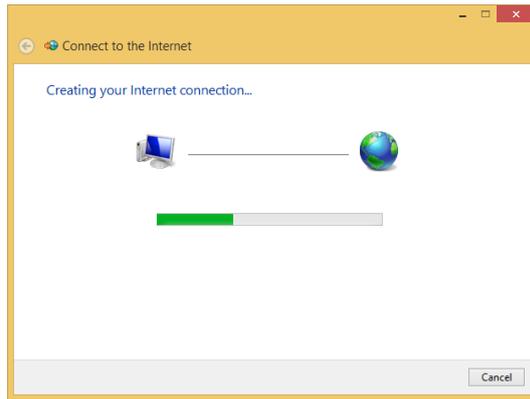
Klik **Broadband (PPPoE)** dan masukkan **username** dan **password** sesuai dengan **user** yang telah dibuat pada **PPP Secrets** lalu klik **Connect** dan tunggu hingga terhubung.



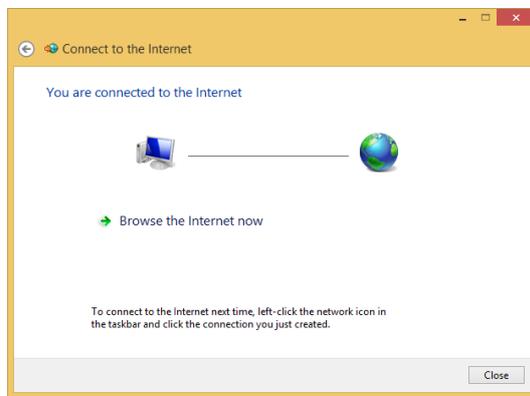
Jendela *Connection or Network*



Jendela *Connection or Network*

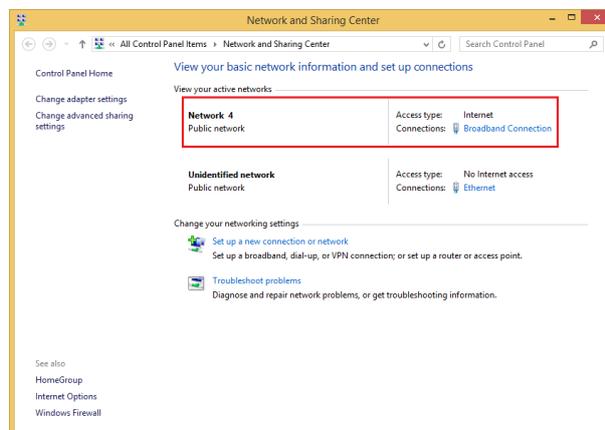


Proses terhubung dengan *PPPoE Server*

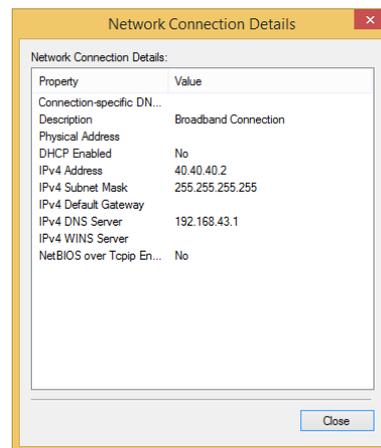
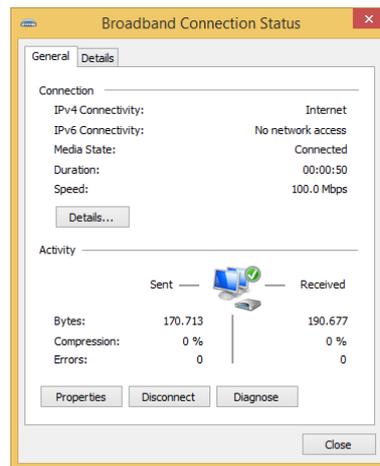


Pemberitahuan koneksi *PPPoE* berhasil

Untuk memastikan koneksi berhasil dan sesuai dengan konfigurasi yang dilakukan pada *PPPoE Server* periksa *IP Address* yang diperoleh pada *Ethernet* Komputer.

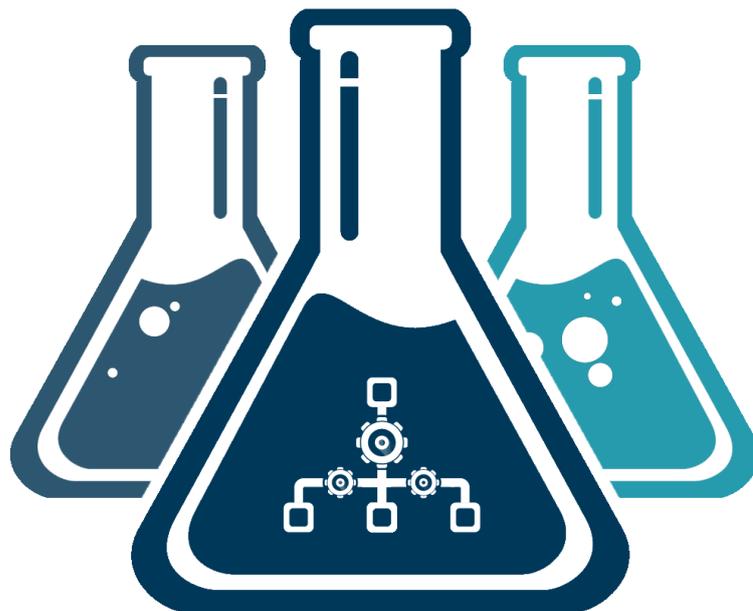
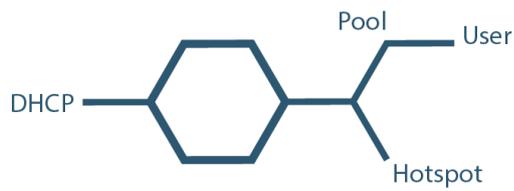


Jendela *Network and Sharing Center*



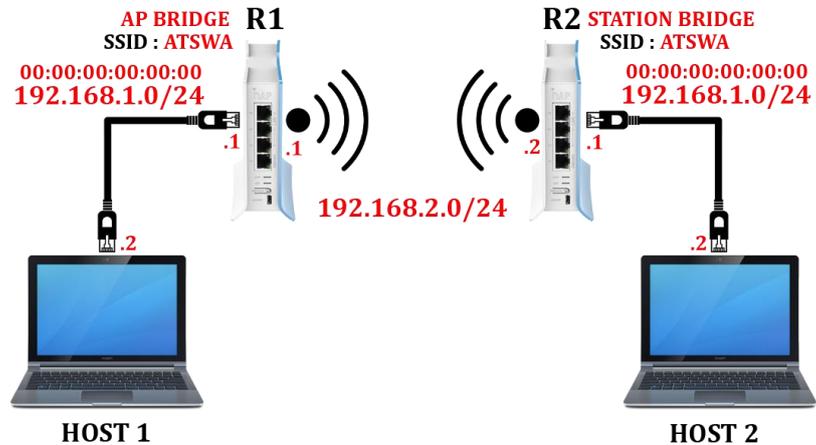
Connection Status pada Network Connection

LABORATORIUM 8



NETWORK MANAGEMENT

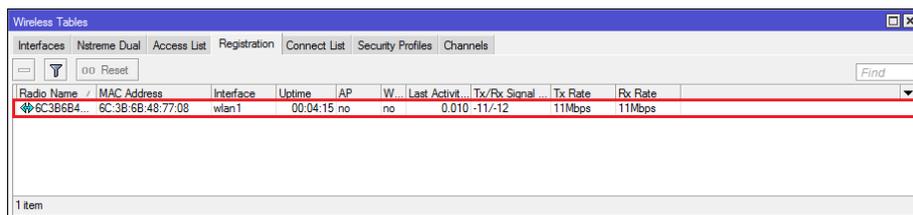
L8.1. WIRELESS MAC ADDRESS FILTERING



Topologi *Wireless MAC Address Filtering*

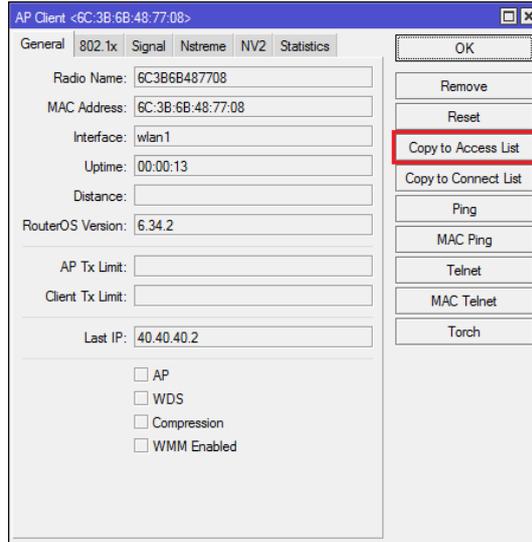
Untuk mencegah perangkat lain terhubung dapat memanfaatkan fitur MAC Filtering dengan cara masuk ke menu **Registration Wireless Tables** pada *Router AP Bridge* dan *Router Station Bridge*. Setelah itu double klik Wireless interface yang akan digunakan.

Media Access Control (MAC) Address adalah alamat fisik suatu interface jaringan yang bersifat unik dan berfungsi sebagai identitas perangkat tersebut



Jendela *Registration* pada *Wireless Tables Router AP Bridge*

Pada *AP Bridge* pilih **Copy to Access List**.

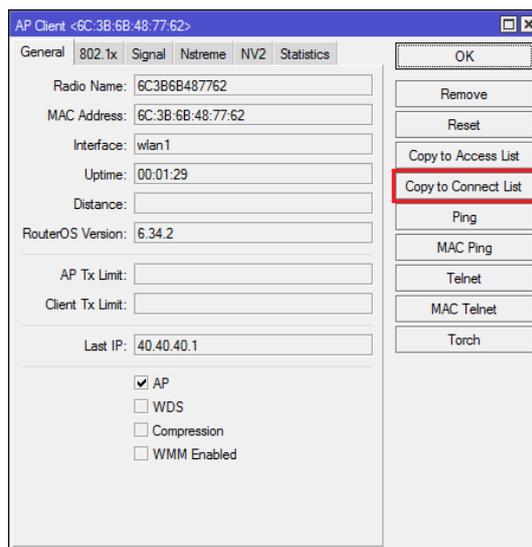


Jendela *General AP Client* pada *Router AP Bridge*



Jendela *Registration* pada *Wireless Tables Router Station Bridge*

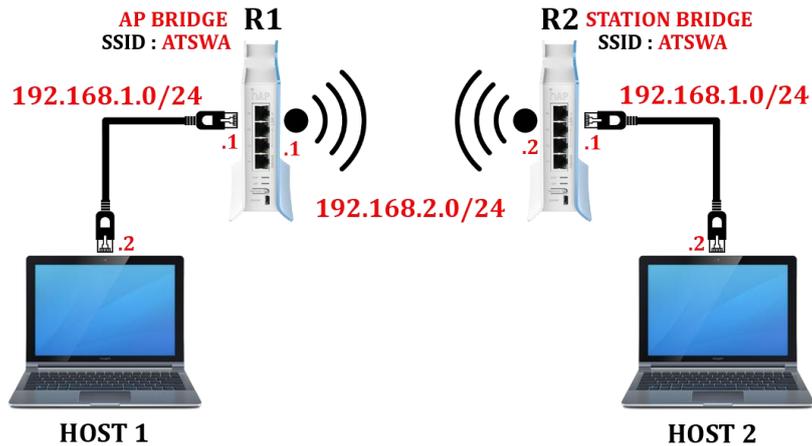
Pada *Station Bridge* pilih **Copy to Connect List**.



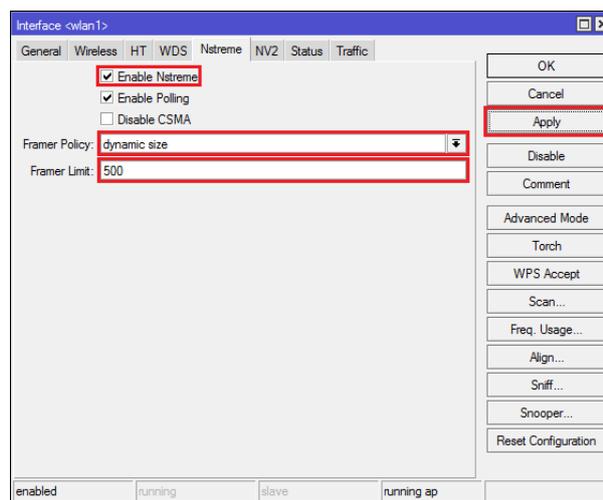
Jendela *General AP Client* pada *Router Station Bridge*

L8.2. WIRELESS NSTREME

Nstreme adalah protocol wireless MikroTik yang digunakan untuk meningkatkan performa link wireless jarak jauh

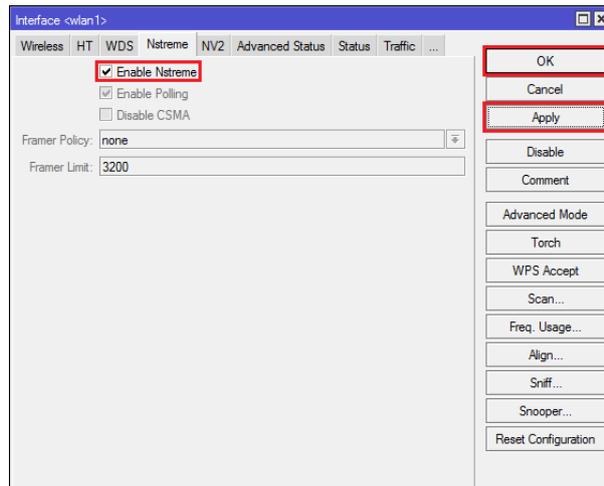


Untuk mengkonfigurasi *Nstreme* pada bagian *AP Bridge* masuk ke menu *Nstreme* pada *Wireless Interface*. Aktifkan *ceklis* pada **Enable Nstreme** pada *Framer Policy* pilih *dynamic size* dan pada *frame limit* masukkan nilai 500 lalu klik **Apply** lalu **OK**.



Jendela *Nstreme* pada Router *AP Bridge*

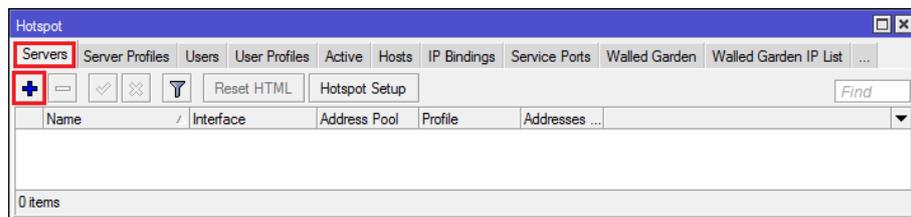
Pada bagian *Station Bridge* cukup mengaktifkan dengan cara *ceklis* **Enable Enstreme** lalu klik **Apply** lalu klik **OK**.



Jendela *Nstreme* pada Router *Station Bridge*

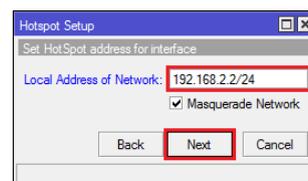
L8.3. HOTSPOT

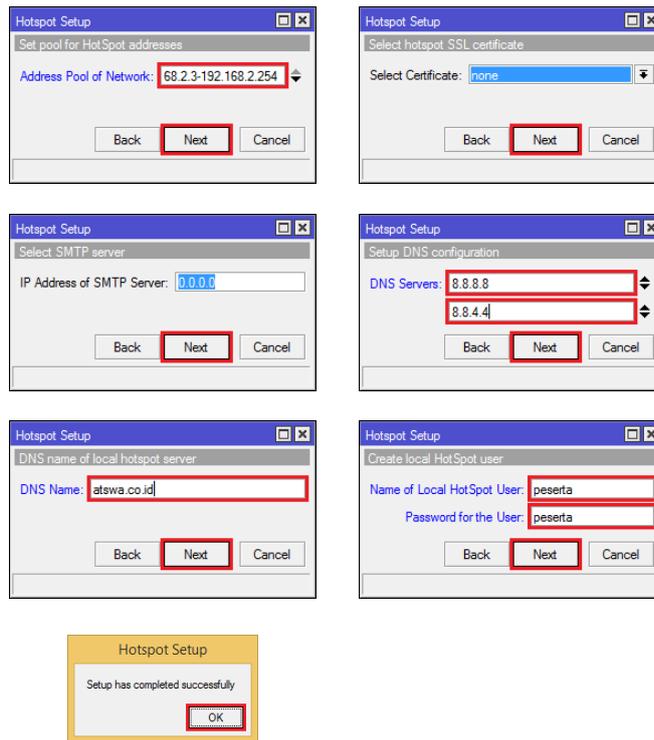
Untuk membuat *hotspot* caranya klik IP klik *Hotspot* klik *Server* klik *Add* atau “+”.



Menu *Hotspot Server*

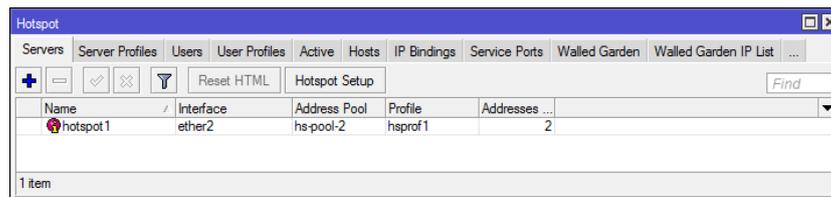
Lalu klik *Hotspot Setup* tentukan *interface* yang akan digunakan pada *Hotspot Interface*, masukkan IP Address yang digunakan pada *Local Address of Network*, tentukan IP Address yang diberikan kepada *User* pada *Address Pool of Network*, tentukan DNS Server yang digunakan pada *DNS Servers*, tentukan domain yang digunakan pada *DNS Name*, dan buat satu *User* yang digunakan untuk masuk ke *Hotspot*.



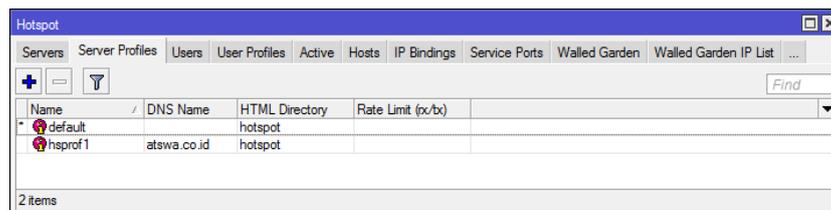


Pengaturan *Hotspot Setup*

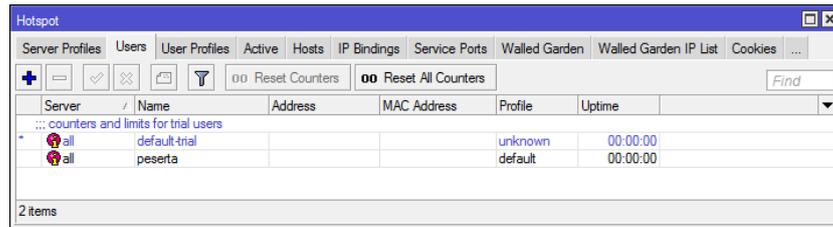
Hotspot Server yang dibuat dapat dilihat di *Server List* pada menu *Servers*, *Profile* yang dibuat dapat dilihat pada menu *Server Profiles*, dan *User* yang dibuat dapat dilihat di menu ***Users***.



Menu *Servers* pada *Hotspot*

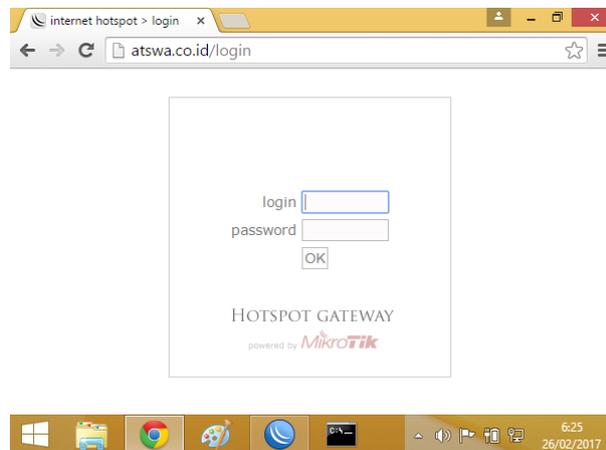


Menu *Server Profile* pada *Hotspot*



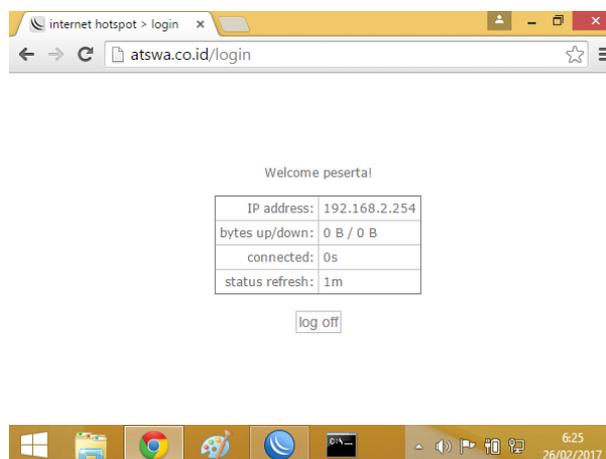
Menu *User* pada *Hotspot*

Hubungkan Komputer dan lakukan pengujian dengan cara mengakses *internet* melalui *web browser*, jika konfigurasi *hotspot* sudah benar maka *browser* akan langsung masuk ke *hotspot gateway* yang sudah dibuat dan menampilkan menu untuk memasukkan user name dan password yang telah dibuat.



Halaman *Hotspot Gateway*

Setelah *user* melakukan *login*,



Halaman yang muncul setelah user berhasil login

LABORATORIUM 9



NETWORK SIMULATION

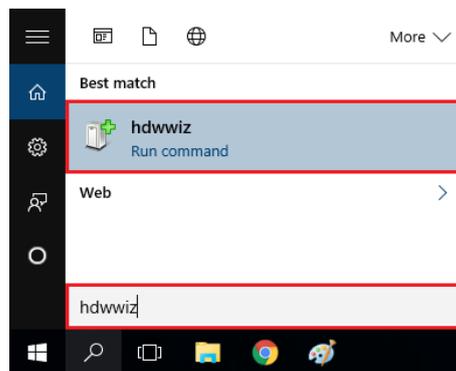
L9.1. INSTALASI LOOPBACK ADAPTER GNS3 DI WINDOWS

Jika Anda ingin menghubungkan GNS3 dengan Komputer maka perlu dibuat loopback adapter.

loopback adapter adalah sebuah perangkat virtual yang diimplementasikan dalam perangkat lunak dan tidak terhubung ke perangkat keras, namun terintegrasi dalam jaringan komputer

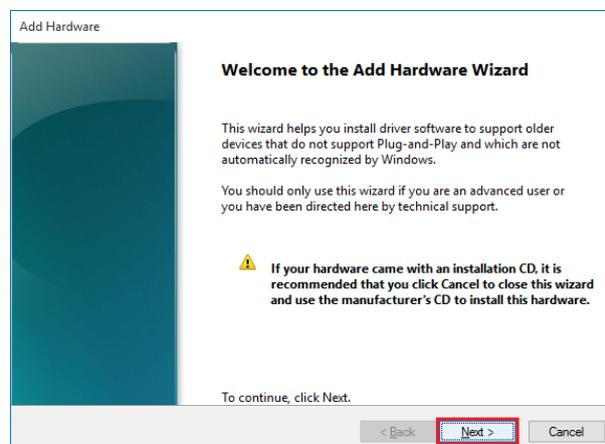


Dengan adanya loopback adapter Anda dapat melakukan konfigurasi atau pengujian menggunakan aplikasi seperti command prompt, winbox, dan lain sebagainya. Untuk membuat loopback adapter pada sistem operasi windows caranya dengan masuk ke **Hardware Wizard** dengan cara mengetikkan **hdwwiz** pada run.



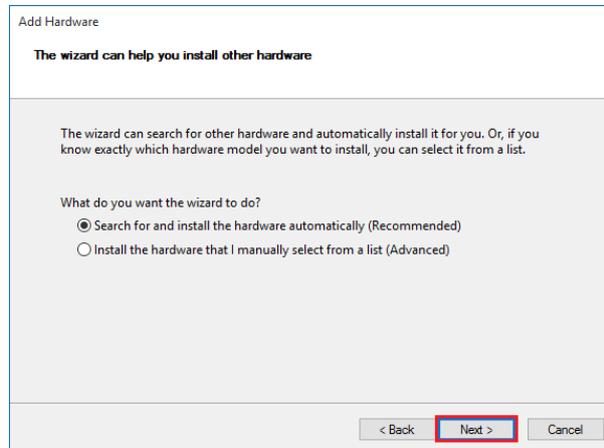
Jendela run pada windows

Setelah muncul jendela **Add Hardware Wizard** lalu klik **Next**



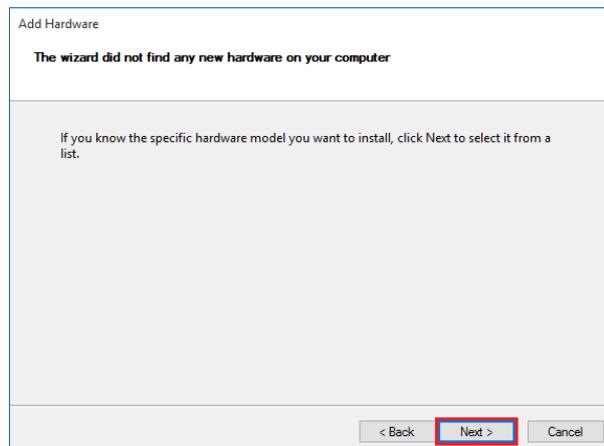
Jendela pengaturan

Setelah itu pilih ***Search for and install the hardware automatically*** lalu klik ***Next***.



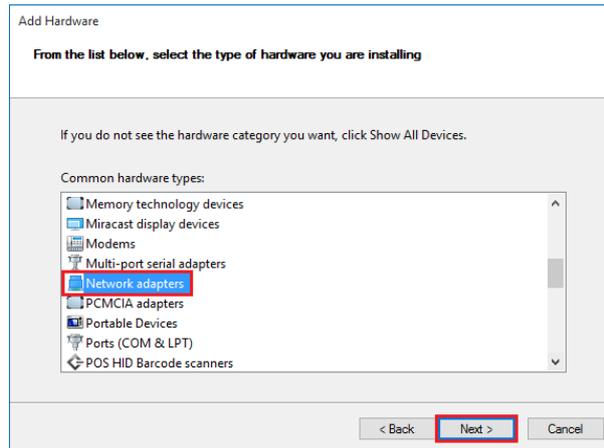
Jendela pengaturan

Klik ***Next***.



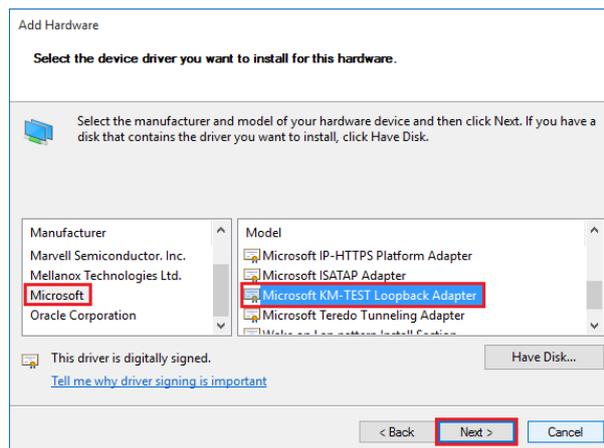
Jendela pengaturan

Setelah itu pilih ***Network Adapter*** pada ***Hardware Category*** lalu klik ***Next***.



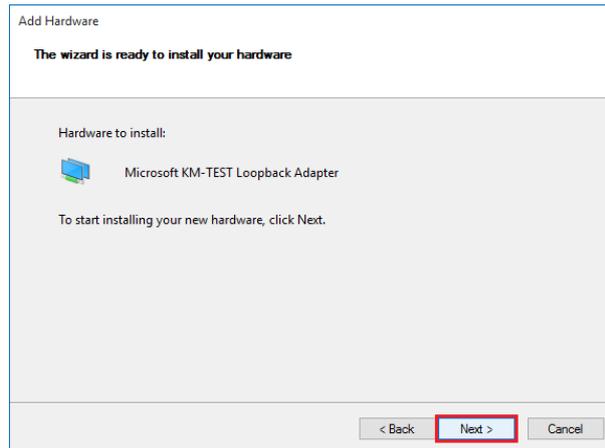
Pengaturan

Setelah itu pilih **Microsoft** pada **Manufacture** dan pilih **Microsoft KM-TEST Loopback Adapter** pada **Model** lalu klik **Next**.

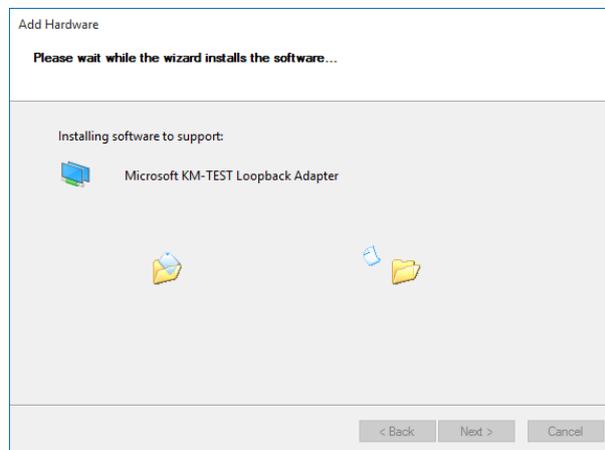


Jendela pengaturan

Setelah proses instalasi berhasil lalu klik **Next**.

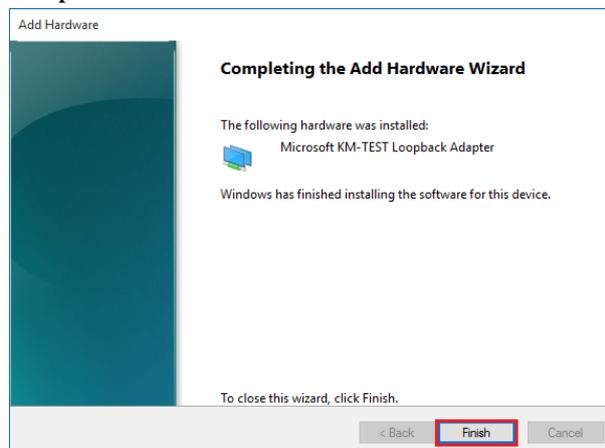


Jendela instalasi KM-TEST Loopback Adapter



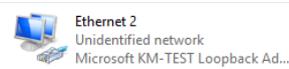
Proses instalasi *software*

Setelah seluruh proses selesai klik ***Finish***.



Jendela pemberitahuan bahwa instalasi sudah berhasil

Adapter loopback dapat dilihat di Network Interface, secara default adapter loopback yang dibuat umumnya muncul dengan nama Ethernet dan ada keterangan Microsoft KM-TEST Loopback Adapter.



Icon Adapter Loopback

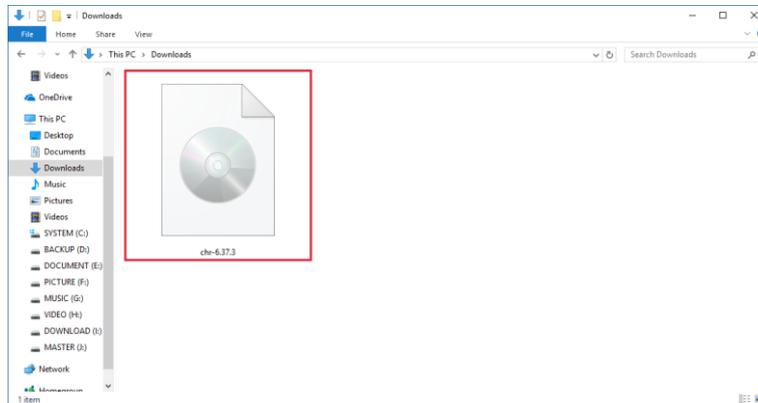
L9.2. INSTALASI MIKROTIK DENGAN QEMU GNS3

Anda dapat menjalankan MikroTik OS di dalam GNS3 menggunakan fasilitas Qemu yang ada pada GNS3.

Qemu adalah aplikasi yang digunakan untuk menjalankan emulasi suatu sistem operasi

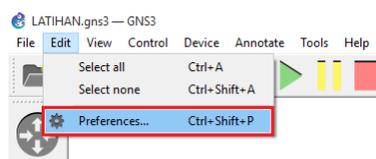


Untuk membuat emulasi MikroTik OS pada GNS3 pertama persiapan terlebih dahulu file Image MikroTik, file image dapat di download di situs mikrotik dengan ekstensi CHR.



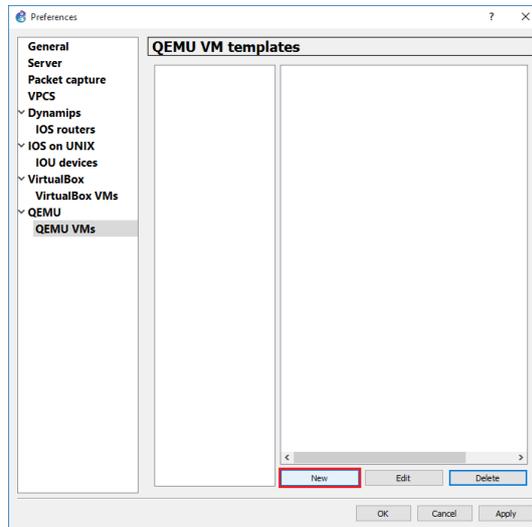
File Image CHR Mikrotik OS

Setelah itu buka aplikasi GNS3 lalu klik **Edit** dan klik **Preferences**.



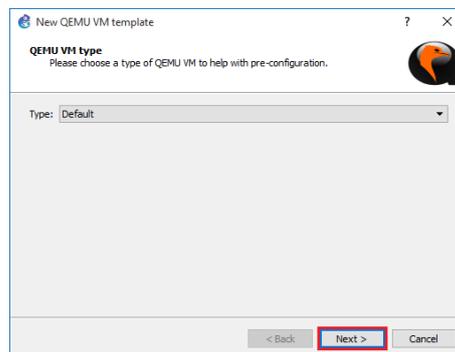
Menu Preference

Setelah itu klik **QEMU** lalu klik **New**.



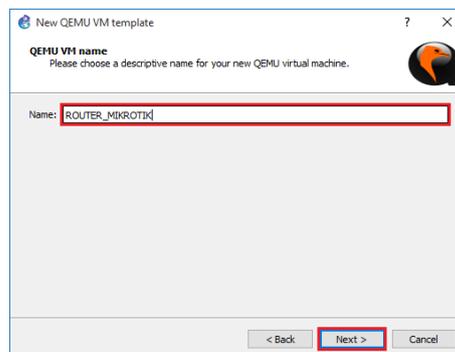
Jendela pengaturan Qemu

Klik **Next**.



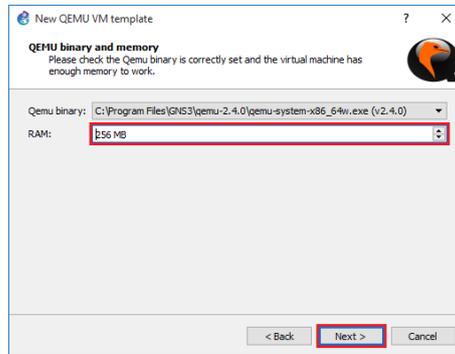
Jendela pengaturan Qemu

Beri nama **QEMU** yang akan dibuat pada bagian **Name** lalu klik **Next**.



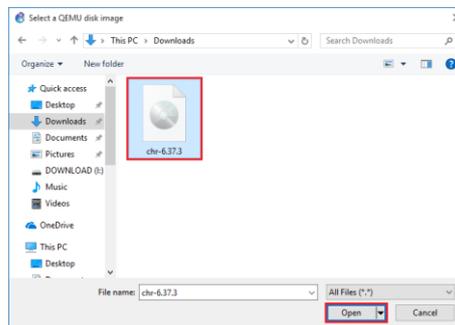
Jendela pengaturan Qemu

Tentukan kapasitas RAM yang digunakan pada bagian RAM lalu klik **Next**.



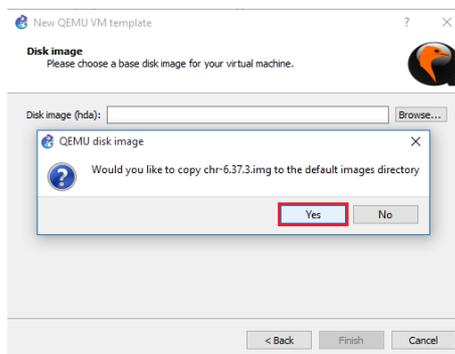
Jendela pengaturan Qemu

Pilih file image yang sudah dipersiapkan sebelumnya lalu klik **Open**.



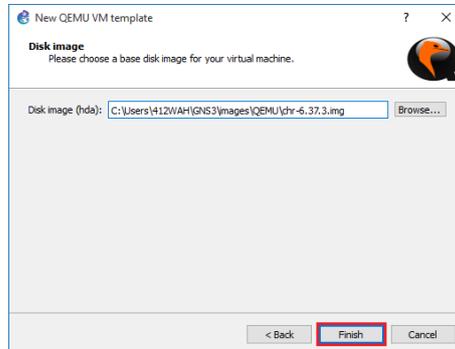
Jendela pengaturan Qemu

Klik **Yes**.

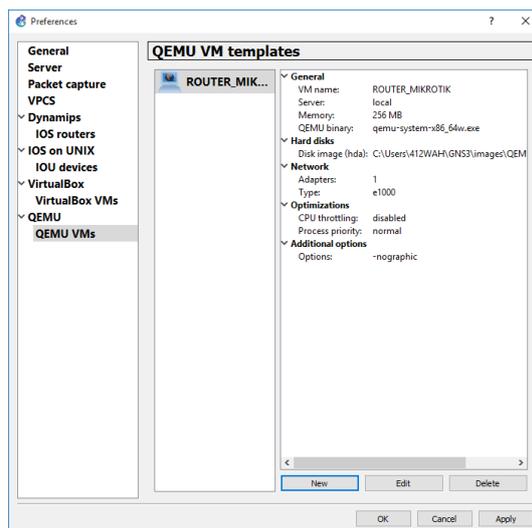


Jendela pengaturan Qemu

Klik Finish.

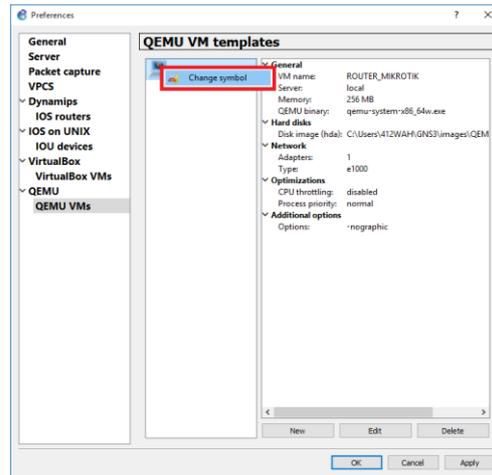


Jendela pengaturan Qemu



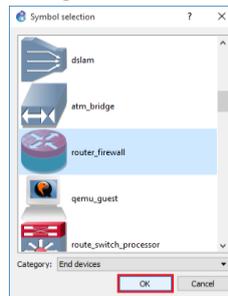
Jendela pengaturan Qemu

Anda dapat merubah Icon default agar menjadi icon router yang telah dibuat dengan cara klik icon lalu klik *Change Symbol*



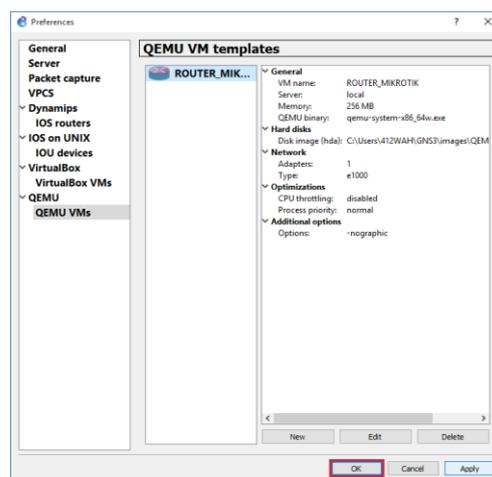
Jendela pengaturan Qemu

Setelah itu klik icon yang di inginkan lalu klik OK.



Memilih Icon untuk Qemu

Klik OK



Jendela pengaturan Qemu

*Jika seseorang meninggal dunia, maka terputuslah amalannya
kecuali tiga perkara (yaitu): sedekah jariyah, ilmu yang dimanfaatkan,
atau do'a anak yang sholeh"*

-: HR. Muslim :-

DAFTAR PUSTAKA

Mikrotik. 2016. *MikroTik Certified Network Associate Training Outline*.
https://www.mikrotik.com/download/pdf/MTCNA_Outline.pdf

Mikrotik. 2015. *Mikrotik Certified Routing Engineer Training Outline*.
https://www.mikrotik.com/download/pdf/MTCRE_Outline.pdf

Purbo, Onno W. 2017. *Model Protocol TCP/IP di Internet*. bit.ly/2nXPPer