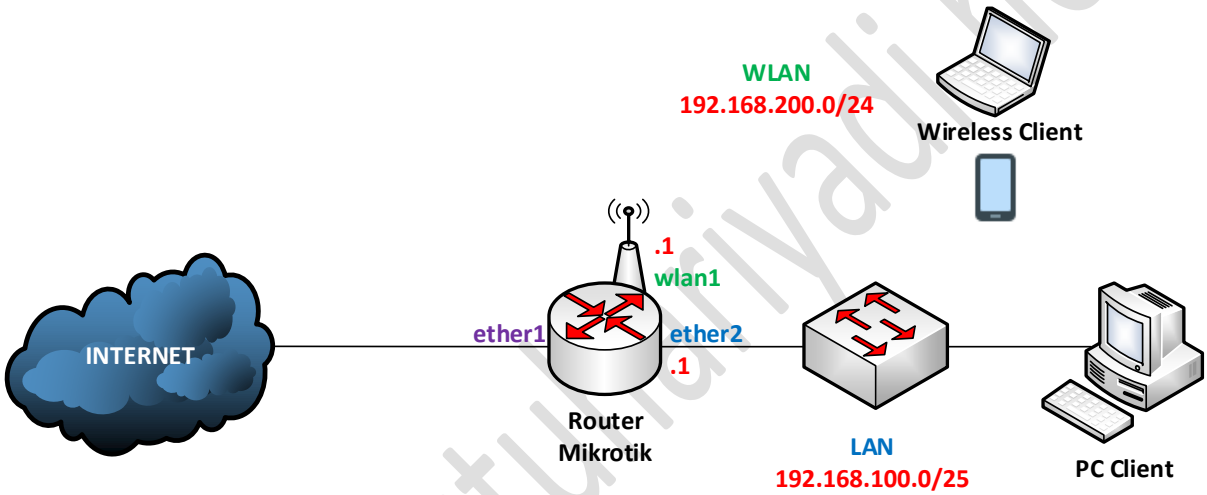
PEMBAHASAN SOLUSI SOAL UJI KOMPETENSI KEAHLIAN (UKK) SMK TKJ PAKET 4 KURIKULUM 2013 TAHUN 2020 TENTANG TROUBLESHOOTING KEAMANAN JARINGAN PADA JARINGAN WAN

Oleh I Putu Hariyadi < admin@iputuhariyadi.net >

A. RANCANGAN TOPOLOGI JARINGAN DAN ALOKASI PENGALAMATAN IP



Alokasi Pengalamatan IP

No.	Network Address	Subnetmask	Deskripsi
1.	192.168.100.0	255.255.255.128 (/25)	Dialokasikan untuk pengalamatan IP pada jaringan lokal (LAN) berkabel.
2.	192.168.200.0	255.255.255.0 (/24)	Dialokasikan untuk pengalamatan IP pada jaringan nirkabel (wireless).
3.	**192.168.19.0**	**255.255.255.0 (/24)**	Dialokasikan untuk pengalamatan IP pada interface jaringan yang terhubung ke Internet **(SESUAIKAN DENGAN ALAMAT IP DARI INTERNET SERVICE PROVIDER (ISP))**.

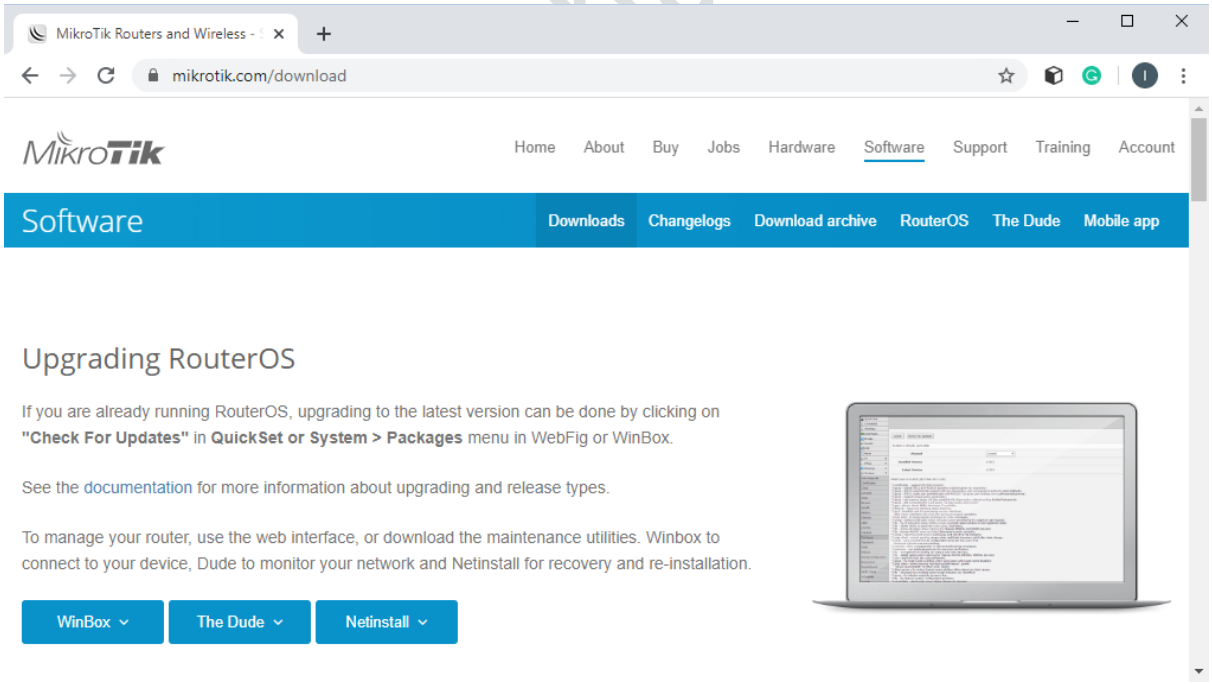
Tabel Pengalamatan IP Perangkat Jaringan

Nama Perangkat	Interface	Alamat IP	Subnetmask	Gateway
Router Mikrotik	Ether1	**192.168.19.254**	**255.255.255.0 (/24)**	**192.168.19.1**
		Sesuaikan dengan alamat IP yang ditentukan oleh Internet Service Provider (ISP)		
	Ether2	192.168.100.1	255.255.255.128 (/25)	
	Wlan1	192.168.200.1	255.255.255.0 (/24)	

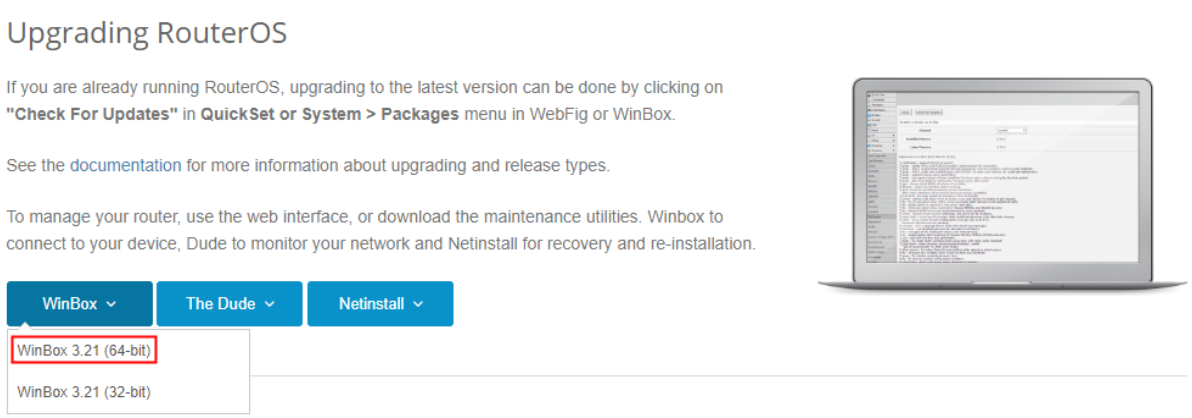
B. MENGAKSES ROUTER MIKROTIK MELALUI WINBOX

Adapun langkah-langkah untuk mengakses *router Mikrotik* melalui aplikasi *Winbox* adalah sebagai berikut:

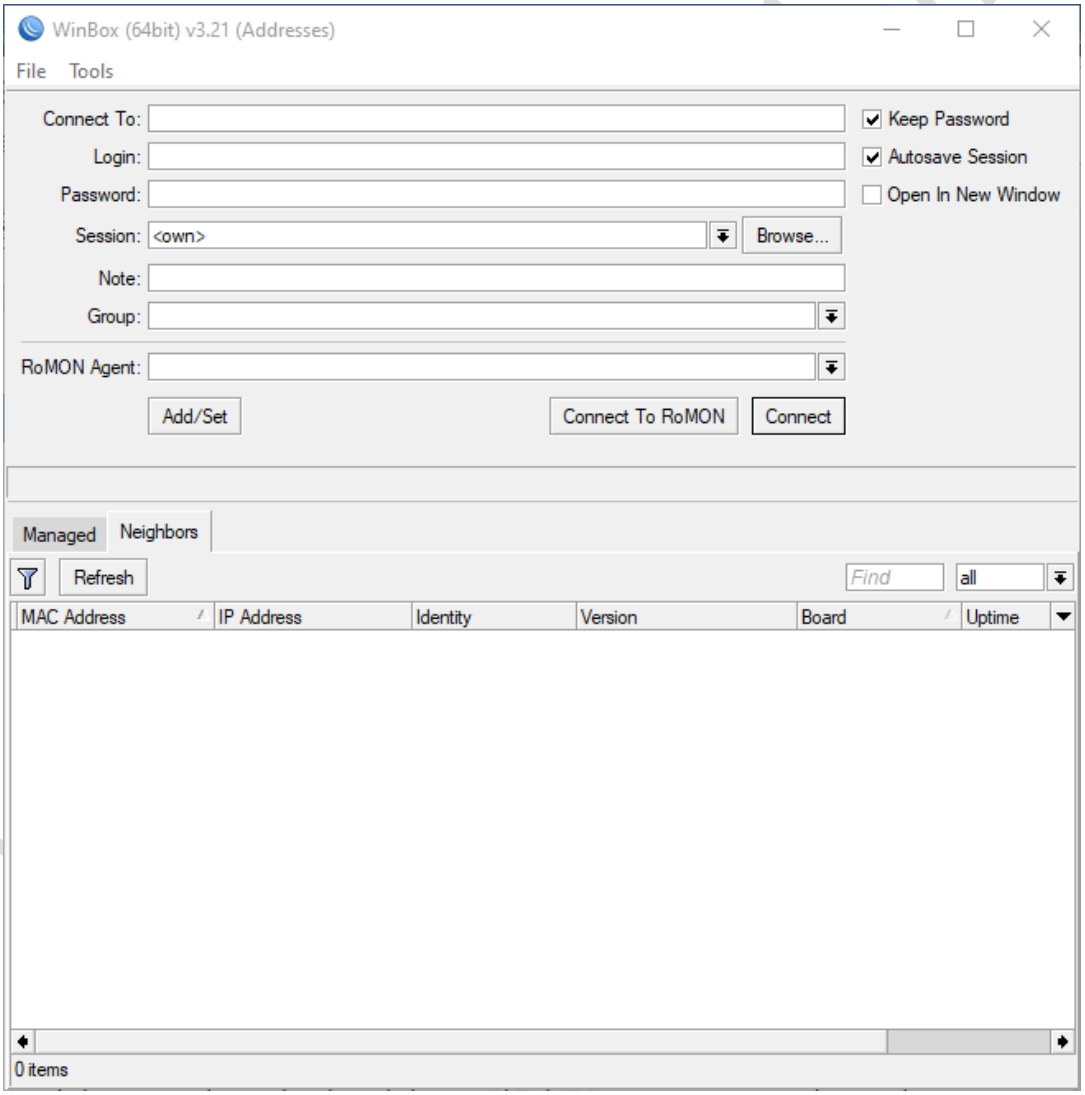
1. Mengunduh aplikasi Winbox dari situs Mikrotik pada alamat https://mikrotik.com/download, seperti terlihat pada gambar berikut:



Pilih **Winbox** > **Winbox 3.21 (64-bit) atau Winbox 3.21 (32-bit)** untuk mengunduh aplikasi tersebut ke komputer yang digunakan, seperti terlihat pada gambar berikut:



2. Jalankan aplikasi **Winbox** yang telah diunduh.
3. Tampil kotak dialog aplikasi **Winbox**, seperti terlihat pada gambar berikut:



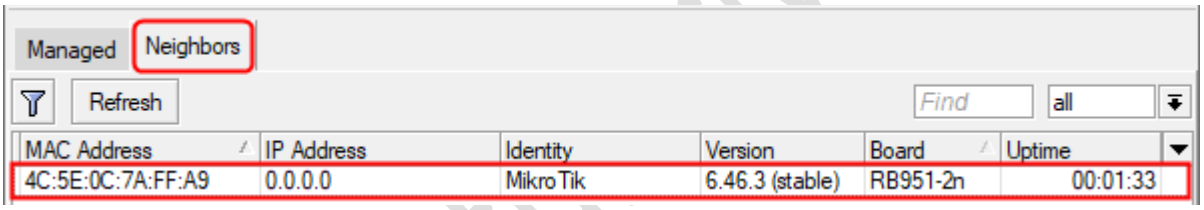
Untuk dapat mengakses Mikrotik maka terdapat 3 (tiga) parameter yang harus dilengkapi pada kotak dialog login dari aplikasi *Winbox* yaitu:

a) ***Connect to*** (digunakan untuk memasukkan alamat IP atau alamat MAC dari router Mikrotik yang akan diakses),

b) ***Login*** (nama login pengguna yang digunakan untuk mengakses router Mikrotik), dan

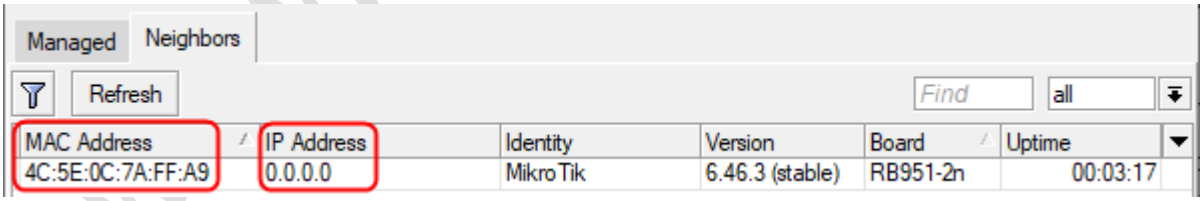
c) ***Password*** (sandi login pengguna yang digunakan untuk mengakses router Mikrotik). Secara default Mikrotik telah membuatkan satu user untuk tujuan administrasi yaitu dengan nama login "**admin**" dengan password kosong (**tanpa sandi**).

Inputan ***Connect to*** dapat diisi secara otomatis melalui pemanfaatan *Mikrotik Neighbor Discovery Protocol (MNDP)* yang dapat mendeteksi router Mikrotik yang terhubung secara langsung dengan komputer yang digunakan yaitu dengan cara memilih tab **Neighbors** di bagian bawah dari *Winbox*, seperti terlihat pada gambar berikut:

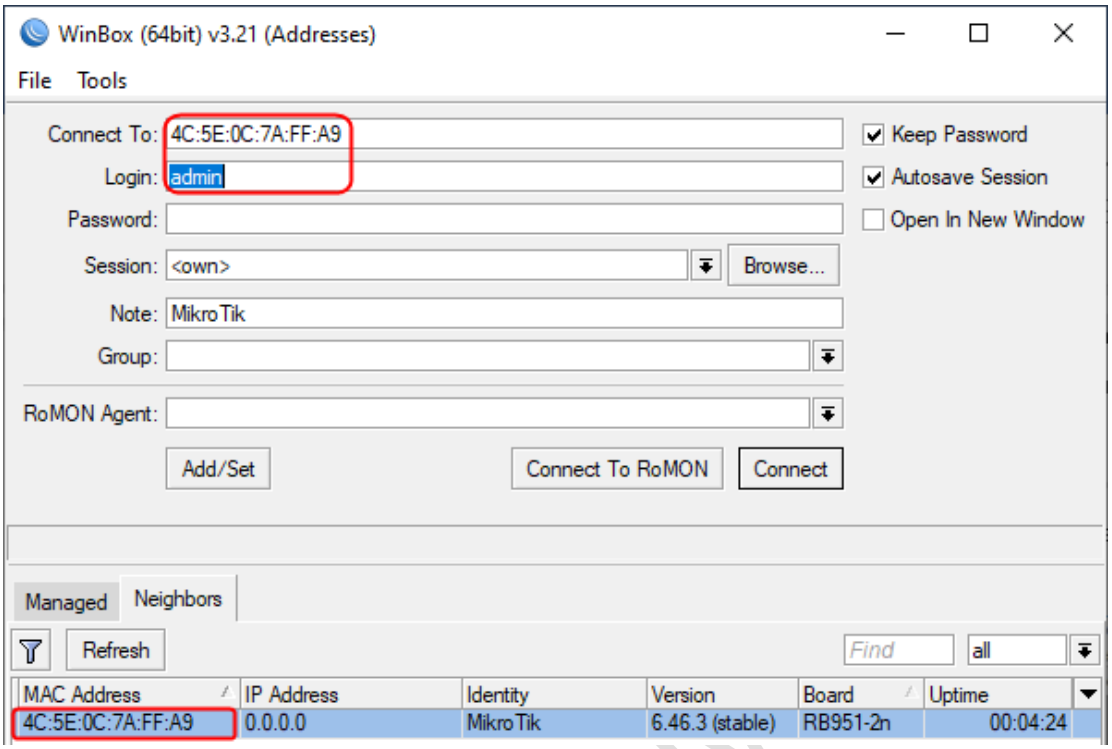


Terdeteksi satu router **Mikrotik RB951-2n**. Apabila belum terdeteksi atau terlihat informasi daftar router Mikrotik maka klik tombol **Refresh**.

Dari daftar *router* yang ditemukan, pilih isian kolom *MAC Address* atau *IP* untuk terkoneksi ke router Mikrotik tersebut, seperti terlihat pada gambar berikut:

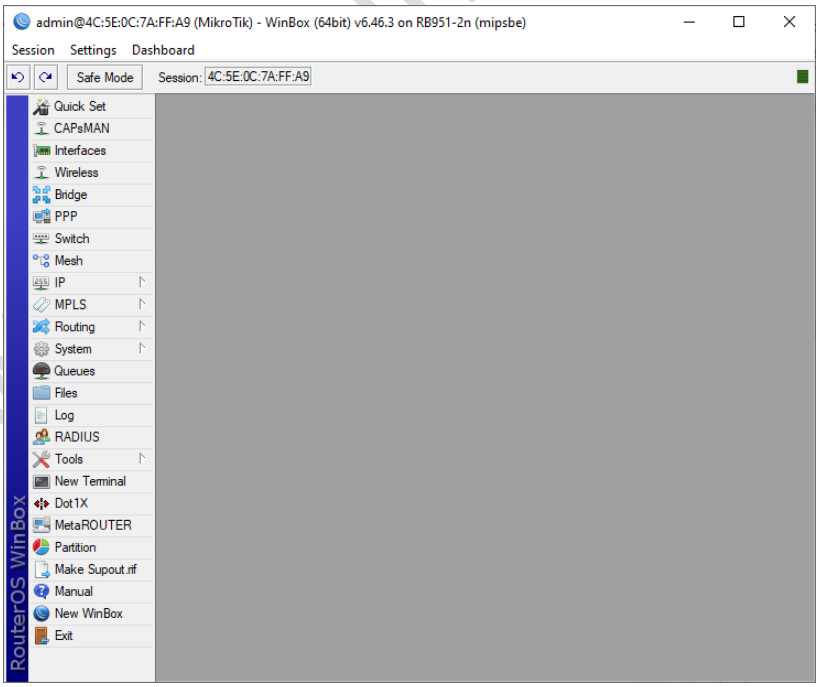


Karena Mikrotik belum memiliki alamat IP maka Pilih **alamat MAC** yang tampil, dan lengkapi parameter *Login* dengan isian "**admin**", seperti terlihat pada gambar berikut:



Selanjutnya tekan tombol "**Connect**" untuk menghubungkan ke router Mikrotik.

4. Tampil kotak dialog yang menampilkan panel menu untuk mengkonfigurasi router Mikrotik, seperti terlihat pada gambar berikut:



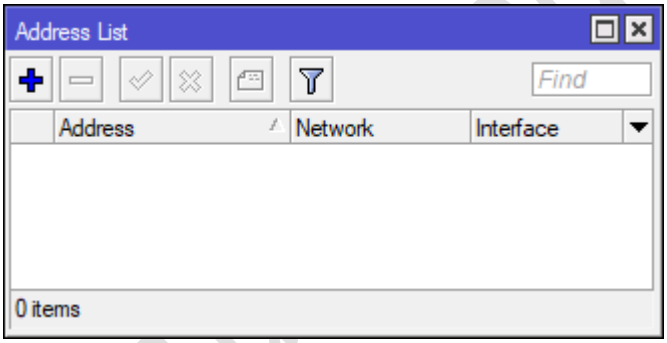
Selanjutnya Anda dapat mengkonfigurasi Mikrotik dengan mengakses panel menu sebelah kiri dan memilih salah satu menu sesuai dengan fitur-fitur yang akan di manajemen.

C. KONFIGURASI DASAR ROUTER MIKROTIK

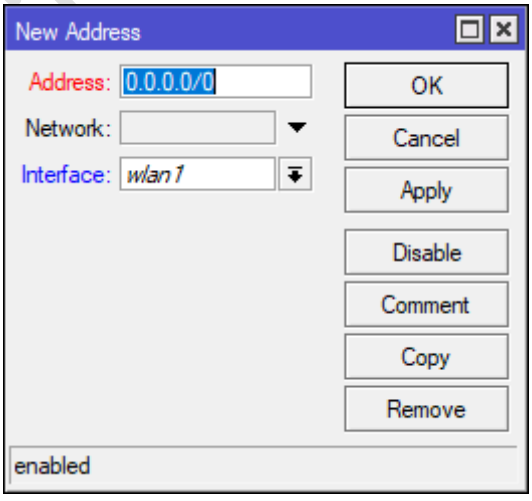
Adapun langkah-langkah konfigurasi dasar yang dilakukan di **router MikroTik** yang meliputi pengalamatan IP, *wireless access point*, *routing*, *Domain Name System (DNS)*, *Network Time Protocol (NTP)*, *Web Proxy*, *Dynamic Host Configuration Protocol (DHCP)*, *Firewall Filter* dan *Internet Connection Sharing (ICS)* serta *Transparent Proxy* adalah sebagai berikut:

1. Mengatur pengalamatan IP pada masing-masing *interface* yaitu **ether1** untuk koneksi ke Internet, **ether2** untuk koneksi ke **LAN** dan **wlan1** untuk koneksi ke jaringan **nirkabel (*wireless*)**.

   Pada panel sebelah kiri dari **Winbox** pilih **IP > Address**, maka akan tampil kotak dialog **Address List**.



   Untuk menambahkan alamat IP pada interface **ether1**, pilih tombol  pada toolbar dari kotak dialog **Address List** maka akan tampil kotak dialog **New Address** seperti terlihat pada gambar berikut:



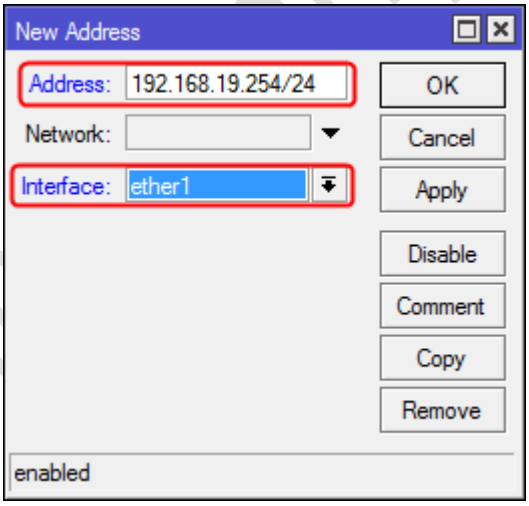
   Terdapat beberapa parameter yang harus diisi pada kotak dialog ini yaitu:

a) **Address**, digunakan untuk menentukan alamat IP dan *subnetmask* dalam format *bit count*, yaitu **192.168.19.254/24** merupakan alamat IP untuk interface **ether1** yang digunakan untuk menghubungkan ke *Internet* melalui ISP.

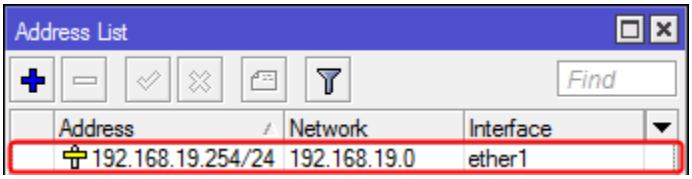
b) **Network**, digunakan untuk menentukan alamat *network* dari alamat IP yang digunakan. Isian untuk alamat ini dapat dikosongkan, karena dapat ditentukan secara langsung oleh router Mikrotik sesuai dengan nilai alamat IP dan *subnetmask* dalam format *bit count* pada parameter **Address**.

c) **Interface**, digunakan untuk menentukan nama *interface* yang akan diberikan alamat IP dengan nilai yang tercantum pada parameter *Address*, yaitu pilih **ether1**.

Isian dari masing-masing parameter dengan nilai yang telah ditentukan, terlihat seperti pada gambar berikut:

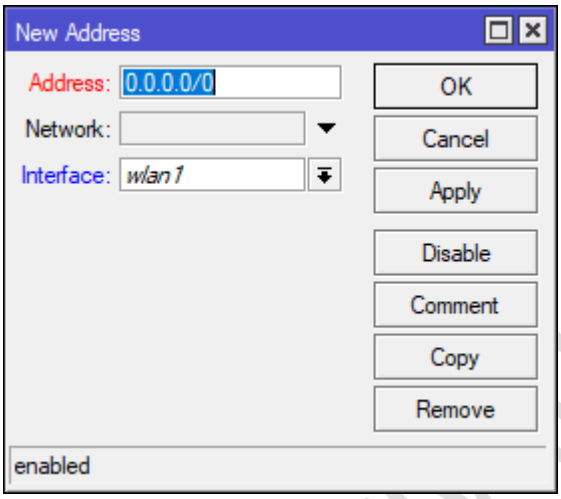


Untuk menyimpan perubahan klik tombol **OK**. Hasil dari penambahan alamat IP terlihat seperti pada gambar berikut:



Selanjutnya dengan cara yang sama, lakukan penambahan alamat IP pada *interface* **ether2**.

Pilih tombol  pada *toolbar* dari kotak dialog **Address List** maka akan tampil kotak dialog **New Address**, seperti terlihat pada gambar berikut:



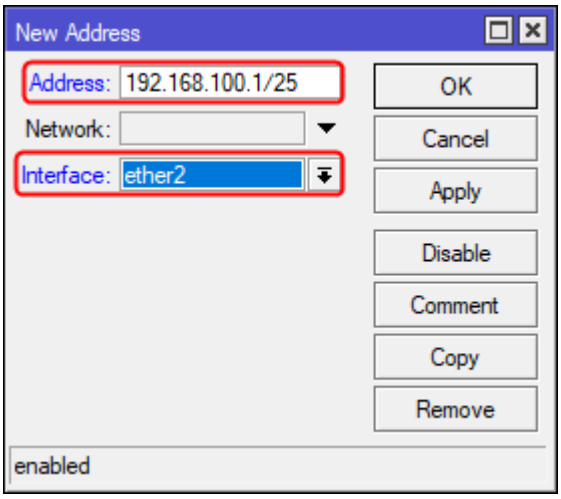
Terdapat beberapa parameter yang harus diisi pada kotak dialog ini yaitu:

a) **Address**, digunakan untuk menentukan alamat IP dan subnetmask dalam format bit count, yaitu **192.168.100.1/25** merupakan alamat IP untuk interface **ether2** yang digunakan untuk menghubungkan ke *LAN*.

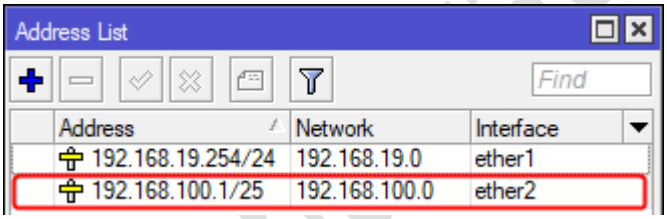
b) **Network**, digunakan untuk menentukan alamat network dari alamat IP yang digunakan. Isian untuk alamat ini dapat dikosongkan, karena dapat ditentukan secara langsung oleh router Mikrotik sesuai dengan nilai alamat IP dan subnetmask dalam format bit count pada parameter **Address**.

c) **Interface**, digunakan untuk menentukan nama interface yang akan diberikan alamat IP dengan nilai yang tercantum pada parameter Address, yaitu pilih **ether2**.

Isian dari masing-masing parameter dengan nilai yang telah ditentukan, terlihat seperti pada gambar berikut:

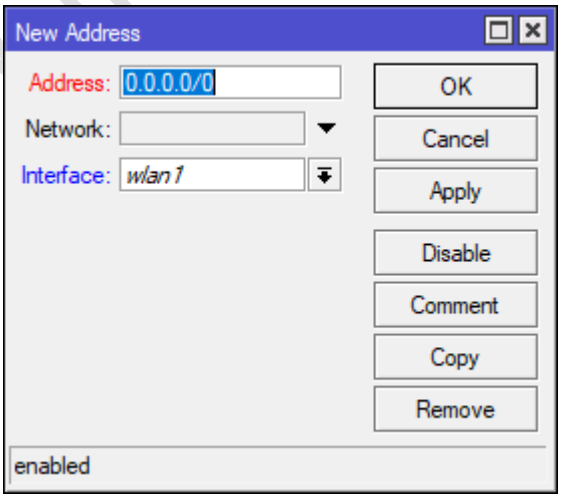


Untuk menyimpan perubahan klik tombol **OK**. Hasil dari penambahan alamat IP terlihat seperti pada gambar berikut:



Selanjutnya dengan cara yang sama, dilakukan pengaturan pengalamatan untuk interface **wlan1** yang terhubung ke jaringan nirkabel ***(wireless)***.

Pilih tombol  pada *toolbar* dari kotak dialog **Address List** maka akan tampil kotak dialog **New Address**, seperti terlihat pada gambar berikut:



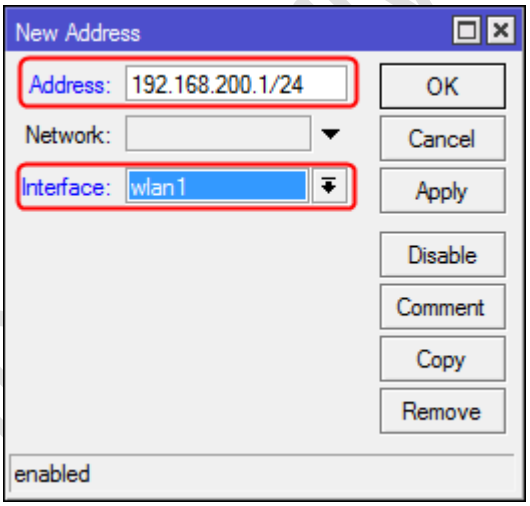
Terdapat beberapa parameter yang harus diisi pada kotak dialog ini yaitu:

a) **Address**, digunakan untuk menentukan alamat IP dan *subnetmask* dalam format *bit count*, yaitu **192.168.200.1/24** merupakan alamat IP untuk *interface* **wlan1** yang digunakan untuk menghubungkan ke *LAN*.

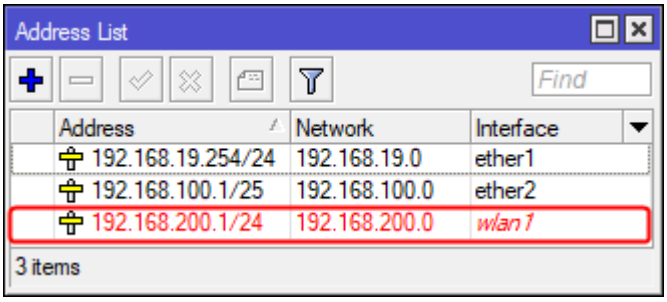
b) **Network**, digunakan untuk menentukan alamat *network* dari alamat IP yang digunakan. Isian untuk alamat ini dapat dikosongkan, karena dapat ditentukan secara langsung oleh *router Mikrotik* sesuai dengan nilai alamat IP dan subnetmask dalam format *bit count* pada parameter **Address**.

c) **Interface**, digunakan untuk menentukan nama *interface* yang akan diberikan alamat IP dengan nilai yang tercantum pada parameter *Address*, yaitu pilih **wlan1**.

Isian dari masing-masing parameter dengan nilai yang telah ditentukan, terlihat seperti pada gambar berikut:



Untuk menyimpan perubahan klik tombol **OK**. Hasil dari penambahan alamat IP terlihat seperti pada gambar berikut:

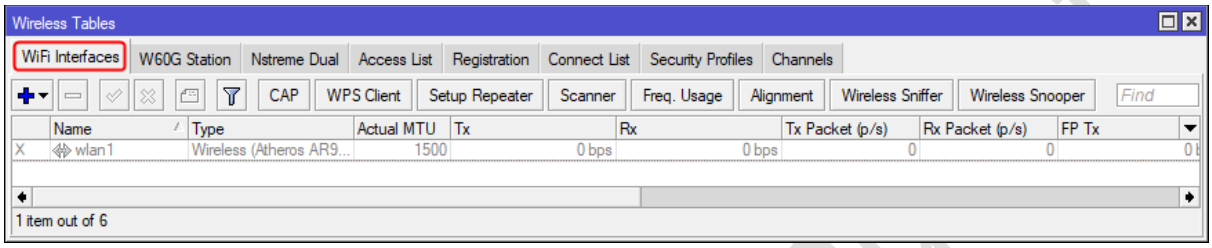


Terlihat nilai dari parameter pada interface **wlan1** berwarna **merah**. Hal ini dikarenakan interface **wlan1** belum diaktifkan.

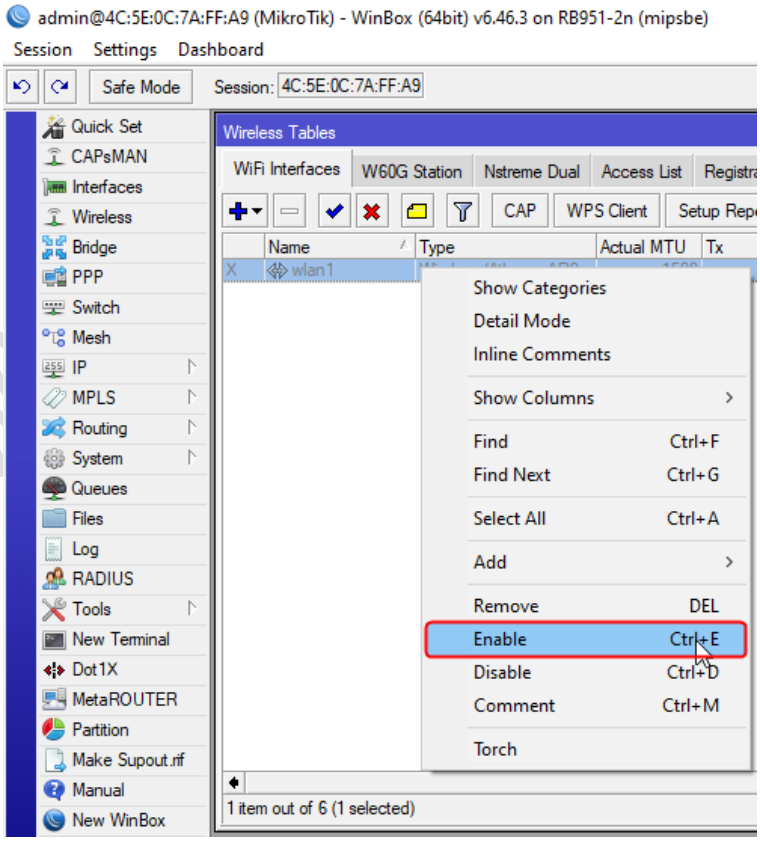
Tutup kotak dialog **Address List**.

2. Mengaktifkan **interface wireless**.

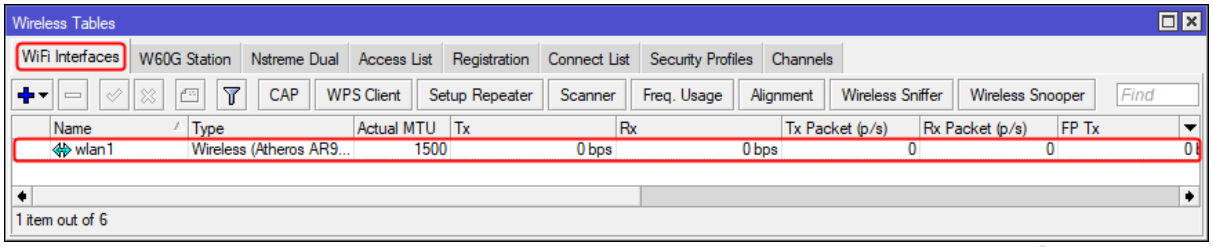
   Pada panel sebelah kiri dari Winbox pilih **Wireless**, maka akan tampil kotak dialog **Wireless Tables**, seperti terlihat pada gambar berikut:



Terlihat terdapat satu interface wireless dengan nama "**wlan1**" dengan status tidak aktif, yang ditandai dengan simbol **X** di awal baris dari interface tersebut. Untuk mengaktifkan interface tersebut, pilih interface "**wlan1**" **>** klik kanan dan pilih **Enable** seperti terlihat pada gambar berikut:

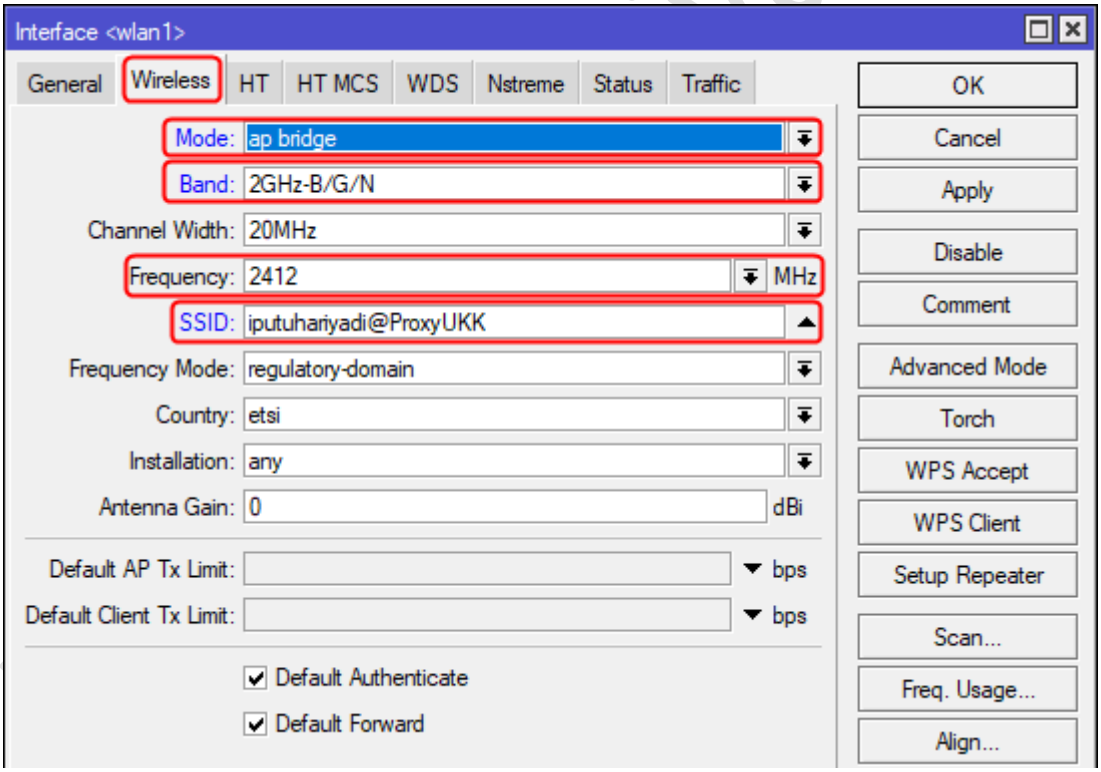


Hasil dari proses pengaktifan interface "**wlan1**" tersebut akan terlihat seperti pada gambar berikut:



3. Mengatur **Service Set Identifier (SSID)** untuk jaringan nirkabel.

   Klik dua kali pada interface "**wlan1**" yang terdapat pada tab **WiFi Interfaces** dari kotak dialog **Wireless Tables**, maka akan tampil kotak dialog properties dari **Interface <wlan1>**. Pada kotak dialog **Interface <wlan1>** tab **Wireless**, lakukan pengaturan parameter *mode, band, frequency,* dan *SSID* untuk jaringan nirkabel yang dibuat, seperti terlihat pada gambar berikut:



Keterangan parameter:

a) *Mode*, digunakan untuk menentukan mode interface wireless yang diaktifkan, pastikan terpilih "**ap-bridge**" agar bertindak sebagai *access point* dengan kemampuan *bridge*.

b) Band, digunakan untuk menentukan *band* yang akan digunakan, sebagai contoh dipilih "**2Ghz-B/G/N**".

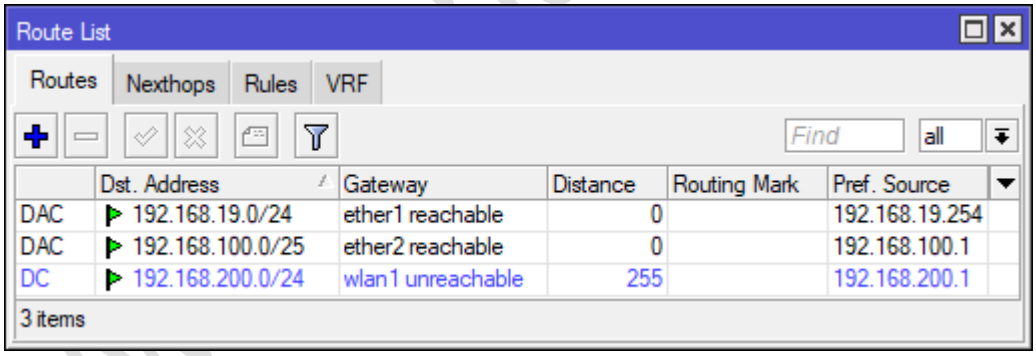
c) *Frequency*, digunakan untuk menentukan *channe*l yang digunakan, sebagai contoh "**2412**". Mohon untuk menyesuaikan nilai ini dengan kondisi jaringan *wireless* di sekitar lokasi Anda. Anda dapat menggunakan fitur *Frequency Usage* dari *router Mikrotik* atau aplikasi seperti **insider** untuk mengetahui *channel* yang belum terpakai sehingga dapat meminimalkan dari *interferensi*.

d) *SSID*, digunakan untuk menentukan nama pengenal *hotspot* mengikuti ketentuan soal yaitu **nama_peserta@ProxyUKK**, sebagai contoh "**iputuhariyadi@ProxyUKK**".

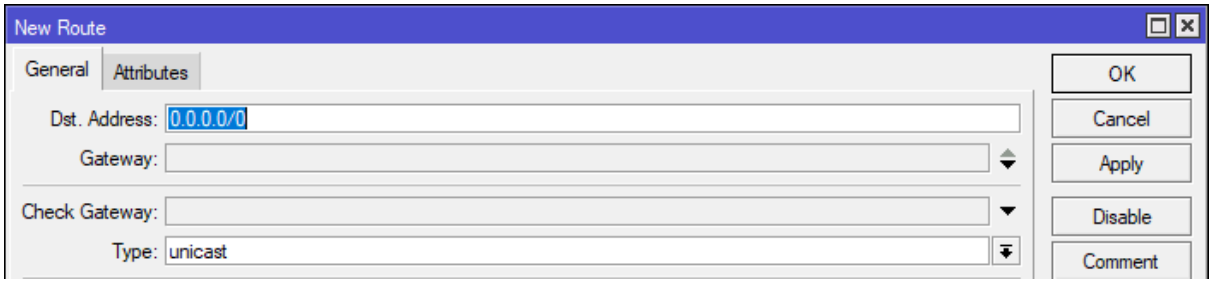
Klik tombol **OK** untuk menyimpan perubahan.

4. Mengatur **Default Route** untuk koneksi ke Internet.

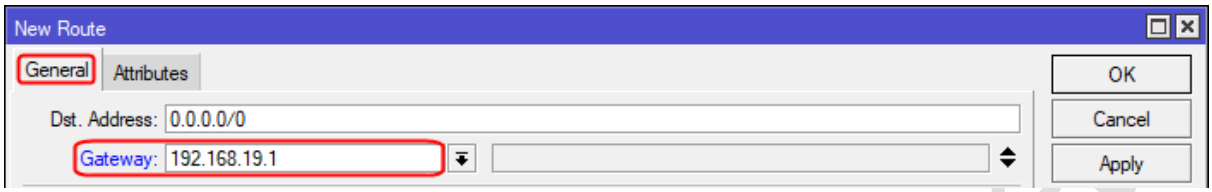
   Pada panel sebelah kiri dari Winbox pilih **IP > Routes**, maka selanjutnya akan tampil kotak dialog **Route List** seperti terlihat pada gambar berikut:



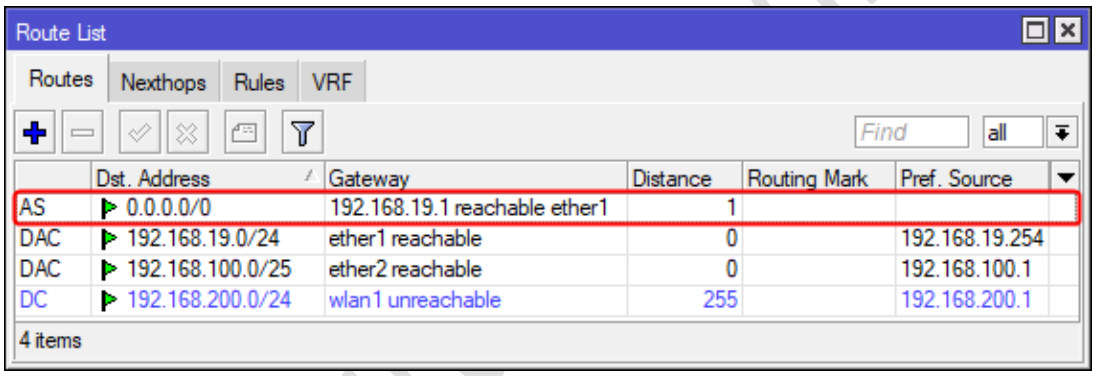
   Untuk menambahkan alamat **default route** untuk koneksi Internet, pilih tombol  pada *toolbar* dari kotak dialog **Route List** maka akan tampil kotak dialog **New Route**, seperti terlihat pada gambar berikut:



Pada tab **General** dari kotak dialog **New Route** yang tampil, lakukan pengaturan parameter **Gateway:** dengan memasukkan alamat IP **192.168.19.1** **(SESUAIKAN DENGAN ALAMAT IP GATEWAY YANG DIBERIKAN OLEH ISP)** , seperti terlihat pada gambar berikut:



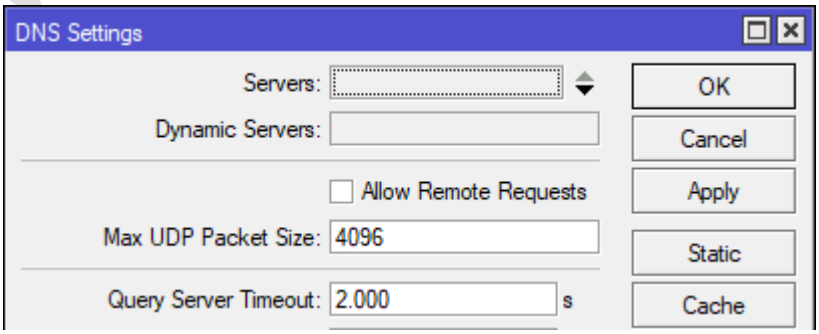
Untuk menyimpan perubahan ketika tombol **OK**. Hasil dari penambahan *default route* ini, terlihat seperti pada gambar berikut:



Tutup kotak dialog **Route List**.

5. Mengatur **Domain Name System (DNS)** untuk memetakan nama domain ke alamat IP menggunakan alamat IP *Server DNS* dari **ISP** atau **Google**.

   Pada panel sebelah kiri dari Winbox, pilih **IP > DNS**, maka selanjutnya akan tampil kotak dialog **DNS Settings**, seperti terlihat pada gambar berikut:

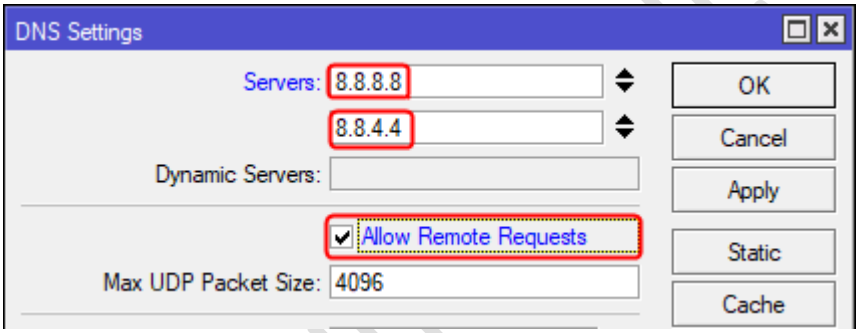


Terdapat beberapa parameter yang diatur pada kotak dialog ini yaitu:

a) **Servers**, digunakan untuk menentukan alamat IP dari *Server DNS* yaitu **8.8.8.8**. Klik tombol ⬍ untuk menambahkan alamat IP untuk *Server DNS* berikutnya yaitu dengan nilai **8.8.4.4**.

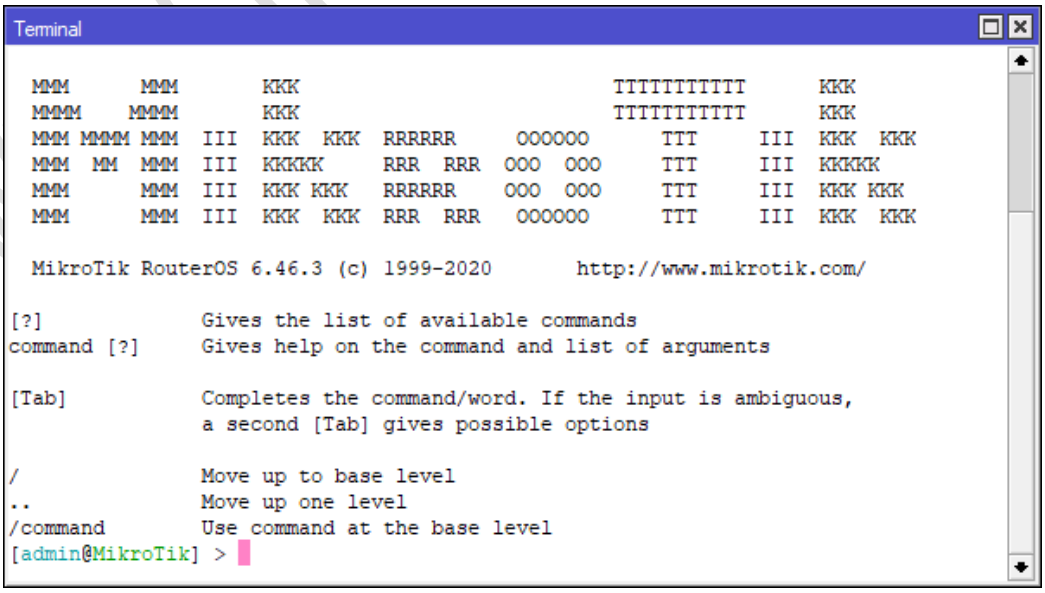
b) **Allow Remote Requests**, digunakan untuk mengaktifkan *router MikroTik* sebagai *DNS server* sehingga mengijinkan permintaan resolusi DNS dari client di LAN dan WLAN. Tandai atau centang pilihan ini dengan dengan memilih inputan *checkbox* yang terdapat diawal keterangan parameter ini.

Isian dari masing-masing parameter dengan contoh nilai diatas, terlihat seperti pada gambar berikut:



Klik tombol **OK** untuk menyimpan perubahan dan menutup kotak dialog **DNS Settings**.

6. Memverifikasi koneksi ke ISP menggunakan perintah **ping** ke alamat IP yang digunakan sebagai *gateway*. Pada panel sebelah kiri dari **Winbox** pilih **New Terminal**, maka akan tampil kotak dialog **New Terminal**, seperti terlihat pada gambar berikut:



Pada *prompt* dari *terminal Mikrotik,* masukkan perintah **ping 192.168.19.1 (SESUAIKAN ALAMAT IP GATEWAY DENGAN ALAMAT YANG DIBERIKAN OLEH ISP)**, seperti terlihat pada gambar berikut:

```
[admin@MikroTik] > ping 192.168.19.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.19.1                               56  64 0ms
    1 192.168.19.1                               56  64 0ms
    sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Tekan **CTRL+C** untuk menghentikan *ping*.

7. Memverifikasi resolusi DNS menggunakan perintah **ping** ke salah satu situs di Internet, sebagai contoh ke **google.com**, seperti terlihat pada gambar berikut:

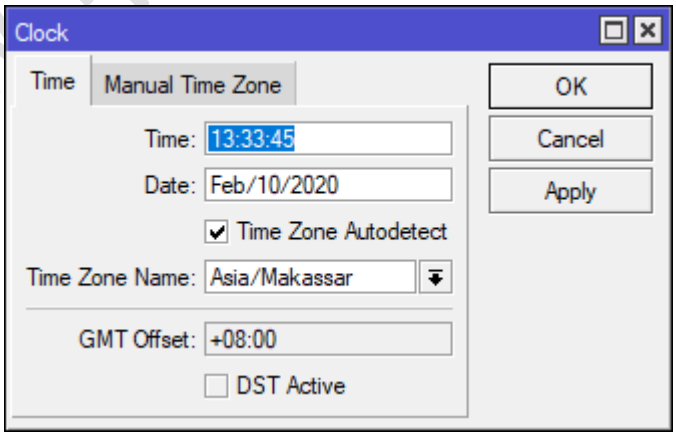
```
[admin@MikroTik] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 216.239.38.120                             56  48 101ms
    1 216.239.38.120                             56  48 73ms
    2 216.239.38.120                             56  48 57ms
    sent=3 received=3 packet-loss=0% min-rtt=57ms avg-rtt=77ms max-rtt=101ms
```

Tekan **CTRL+C** untuk menghentikan *ping*.

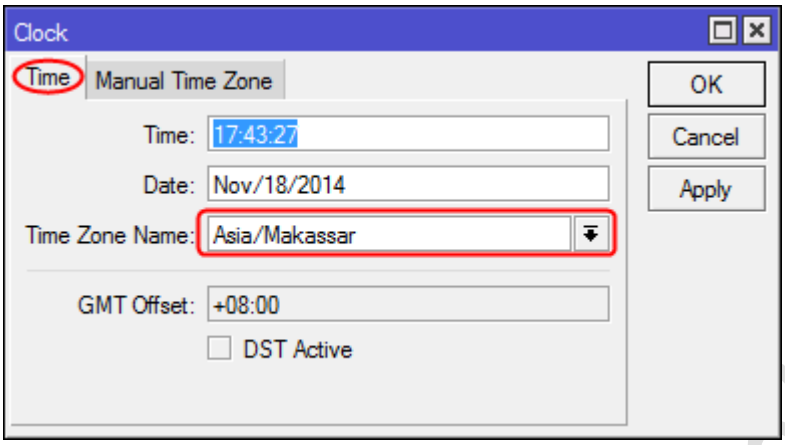
Tutup kotak dialog **Terminal**.

8. Mengatur **System Clock** dan **SNTP Client** untuk sinkronisasi waktu **router Mikrotik** dengan **Server NTP** di *Internet*. Sinkronisasi waktu ini diperlukan agar pembatasan akses *Internet* bagi client WLAN yang menggunakan akun *hotspot* dapat bekerja sesuai dengan waktu yang telah ditentukan yaitu pada pukul 07:00-16:00.

   a) Pada panel sebelah kiri pilih **System > Clock**, maka akan tampil kotak dialog **Clock** seperti terlihat pada gambar berikut:



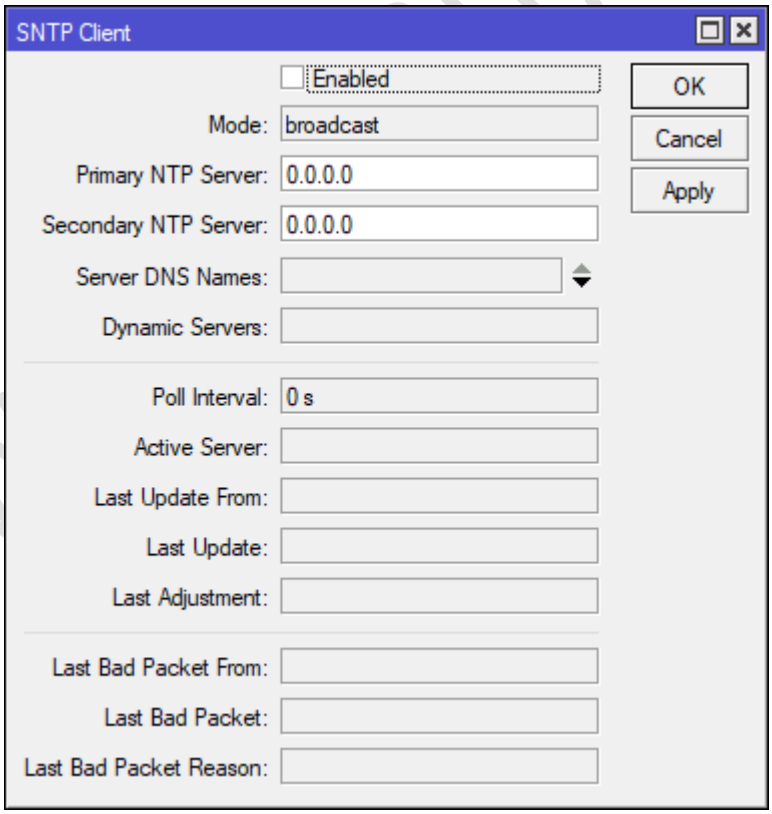
Pada kotak dialog **Clock** tab **Time**, lakukan pengaturan parameter **Time Zone Name** dengan memilih pilihan "**Asia/Makassar**" bagi zona **Waktu Indonesia Tengah (WITA)**, seperti terlihat pada gambar berikut:



Bagi yang berada di zona **Waktu Indonesia Barat (WIB)** dapat memilih **Time Zone Name "Asia/Jakarta"**. Sedangkan bagi yang berada di zona **Waktu Indonesia Timur (WIT)** dapat memilih Time Zone Name "**Asia/Jayapura**".

Klik tombol **OK** untuk menyimpan pengaturan.

b) Pada panel sebelah kiri pilih **System > SNTP Client**, maka akan tampil kotak dialog SNTP Client seperti terlihat pada gambar berikut:

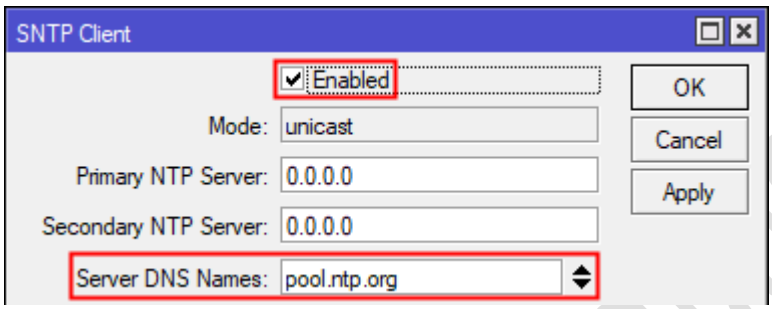


Terdapat beberapa parameter yang diatur yaitu:

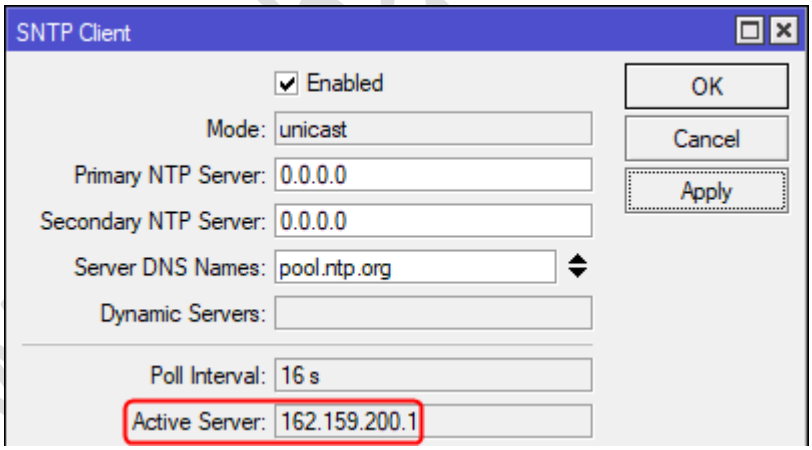
- **Enabled**, pilih untuk mengaktifkan fitur *SNTP Client* untuk sinkronisasi waktu.

- **Server DNS Names**, digunakan untuk mengatur server NTP menggunakan nama domain dimana nama domain akan ditranslasi setiap kali permintaan NTP dikirim yaitu **pool.ntp.org**.

Hasil dari pengaturan parameter terlihat seperti pada gambar berikut:



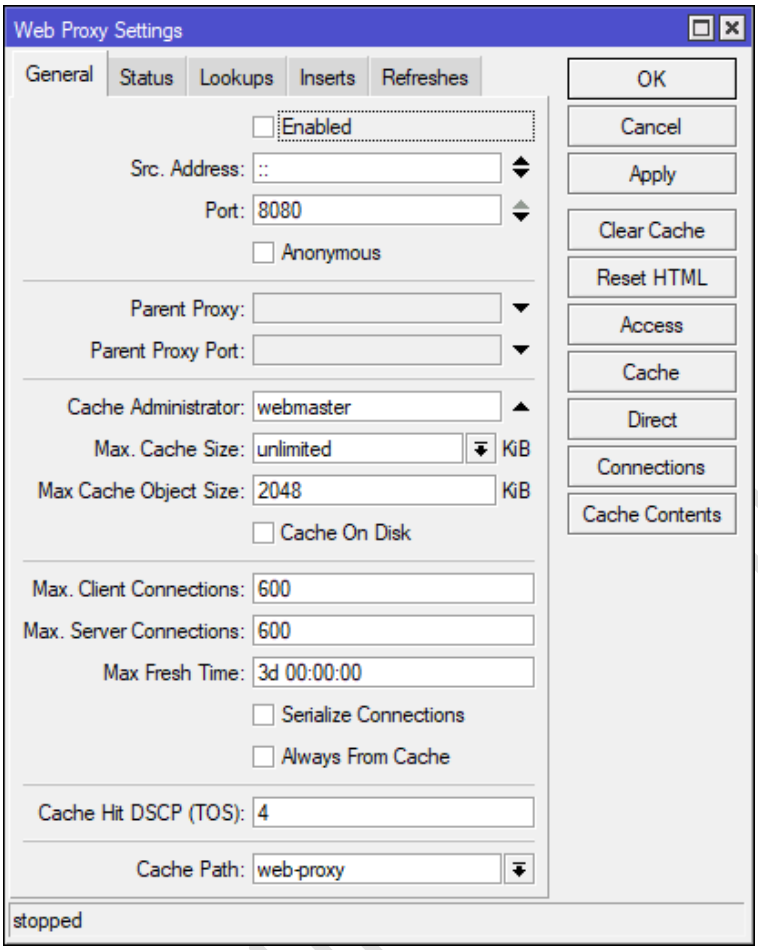
Klik tombol **Apply** untuk menyimpan perubahan. Apabila komunikasi ke *NTP Server* telah berhasil dilakukan maka pada parameter **Active Server** akan menampilkan informasi alamat IP dari *NTP Server* aktif, sebagai contoh **162.159.200.1**, seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menutup kotak dialog *SNTP Client*.

9. Membuat **Web Proxy Server** dengan **Cache Administrator** menggunakan format penulisan **namapeserta@sekolah.sch.id**.

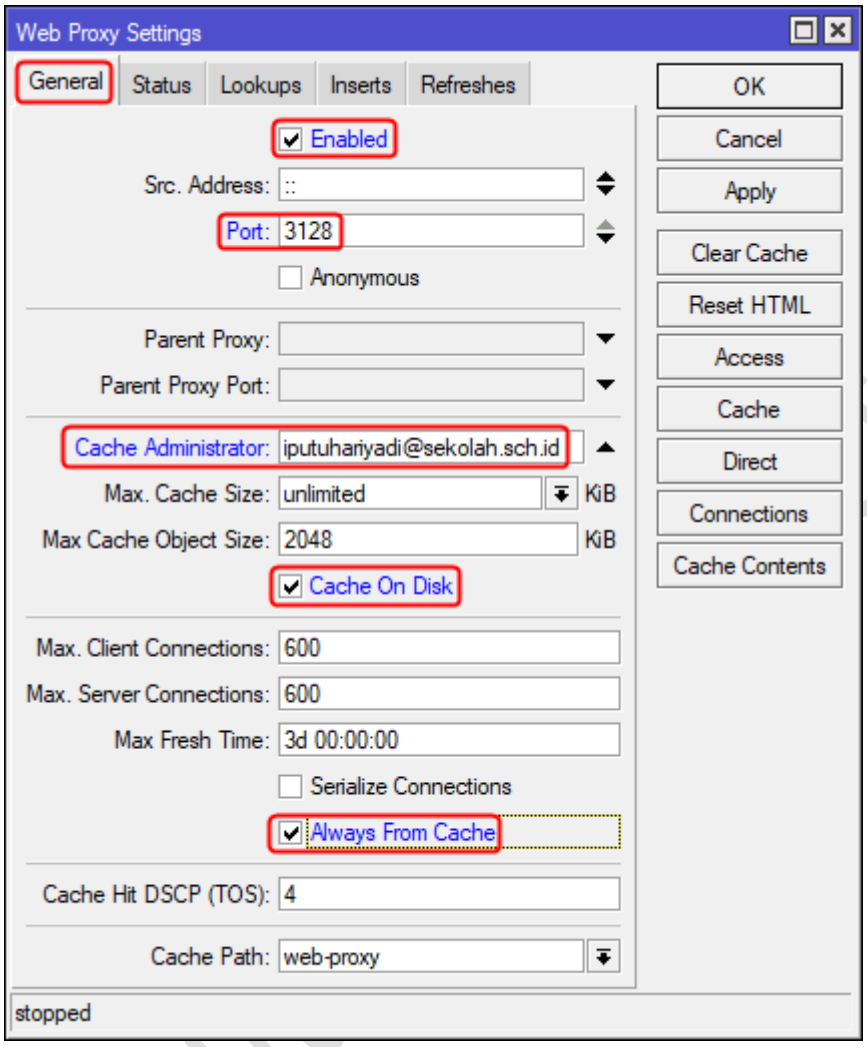
   Pada panel sebelah kiri dari Winbox pilih **IP > Web Proxy**, maka akan tampil kotak dialog **Web Proxy Settings**, seperti terlihat pada gambar berikut:



Terdapat beberapa parameter yang harus diatur yaitu:

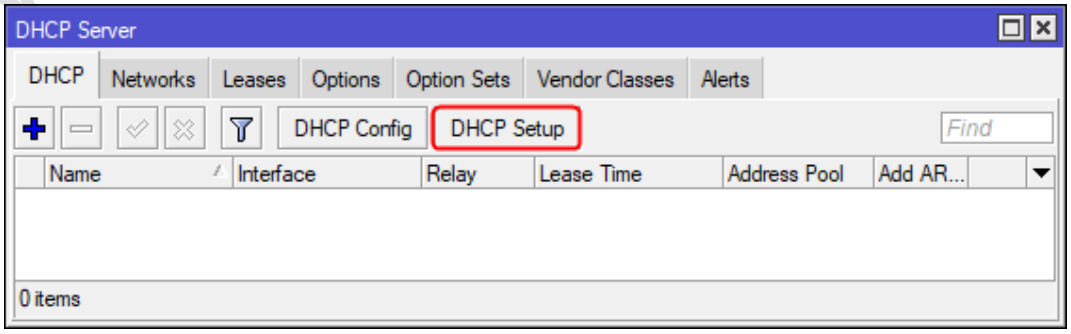
a. **Enabled** digunakan untuk mengaktifkan *web proxy*.
b. **Port** digunakan untuk menentukan port TCP yang digunakan oleh *server proxy*, sebagai contoh **3128**.
c. **Cache Administrator** digunakan untuk menentukan alamat email dari *administrator* yang akan ditampilkan pada halaman *proxy* ketika terjadi kegagalan (*error*), sebagai contoh *iputuhariyadi@sekolah.sch.id*.
d. **Cache On Disk** digunakan untuk menyimpan *cache* pada media penyimpanan (*disk*).
e. **Always From Cache** digunakan untuk menentukan agar selalu menggunakan *cache*.

Hasil pengaturan parameter tersebut akan terlihat seperti pada gambar berikut:

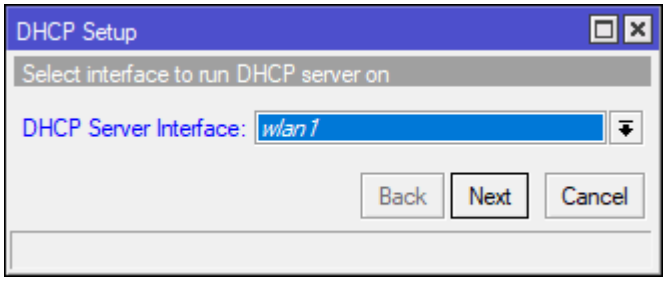


Klik tombol **OK** untuk menyimpan pengaturan.

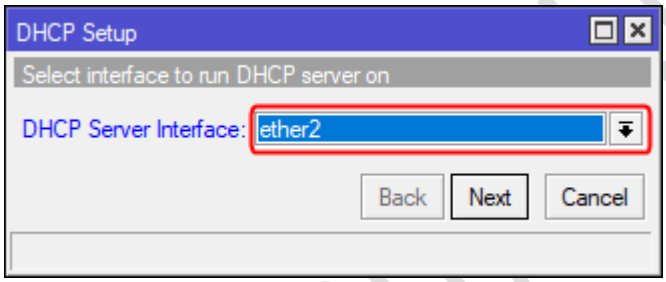
10. Membuat **DHCP Server** untuk mengalokasikan pengalamatan IP secara dinamis ke computer client yang terhubung baik melalui LAN berkabel maupun nirkabel (WLAN). Pada panel sebelah kiri dari Winbox pilih **IP > DHCP Server**, maka akan tampil kotak dialog **DHCP Server.** Pada kotak dialog ini klik tombol **DHCP Setup** untuk membuat DHCP Server secara *wizard*, seperti terlihat pada gambar berikut:



Selanjutnya akan tampil kotak dialog **DHCP Setup** untuk memilih interface yang akan menjalankan server DHCP, seperti terlihat pada gambar berikut:

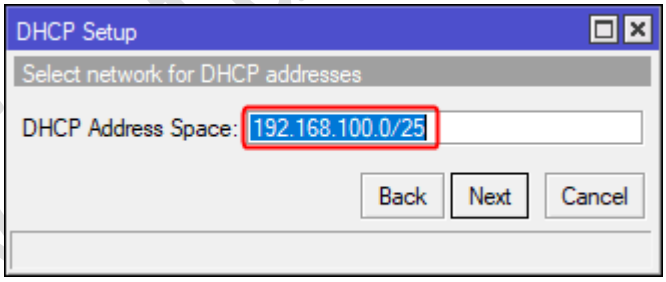


Pilih **ether2** untuk pembuatan *DHCP Server* bagi LAN, seperti terlihat pada gambar berikut:



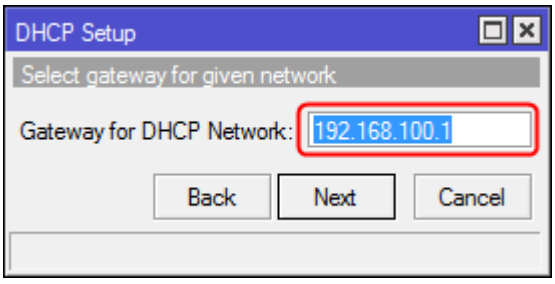
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat jaringan yang dialokasikan untuk alamat DHCP, seperti terlihat pada gambar berikut:



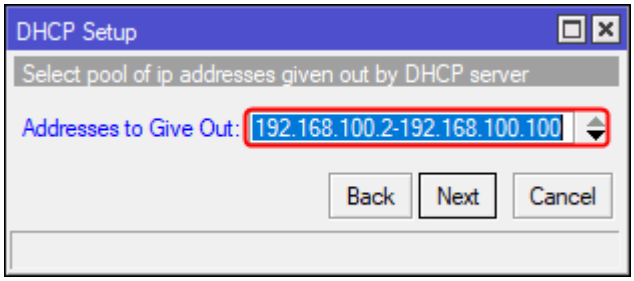
Masukkan alamat jaringan **192.168.100.0/25** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat gateway untuk jaringan DHCP, seperti terlihat pada gambar berikut:



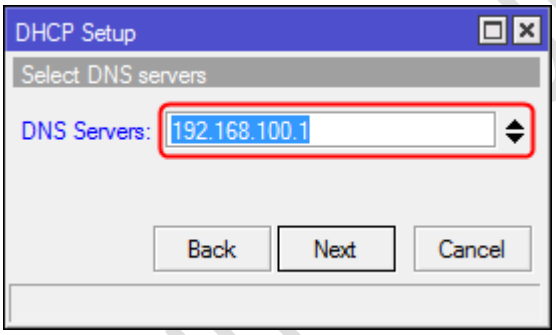
Masukkan alamat IP **192.168.100.1**, dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan rentang alamat IP yang didistribusikan ke client, seperti terlihat pada gambar berikut:



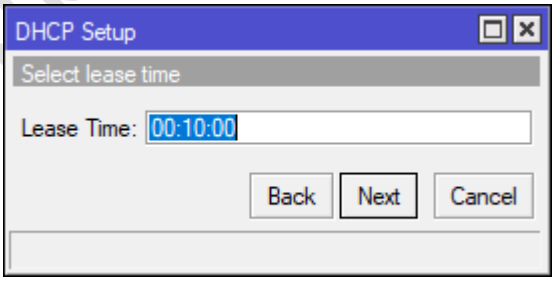
Masukkan alamat IP **192.168.100.2-192.168.100.100** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat DNS Servers, seperti terlihat pada gambar berikut:

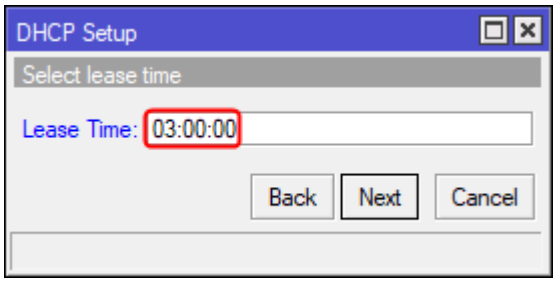


Masukkan alamat IP dari router Mikrotik **192.168.100.1** sebagai *DNS Server* dan klik tombol **Next**.

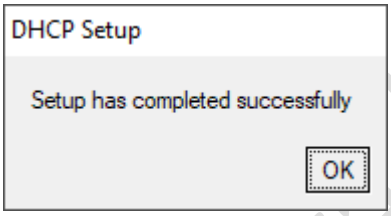
Tampil kotak dialog **DHCP Setup** untuk menentukan waktu sewa alamat IP ke client DHCP, seperti terlihat pada gambar berikut:



Masukkan nilai **03:00:00** agar masa sewanya adalah **3 jam** sehingga akan terlihat seperti pada gambar berikut:

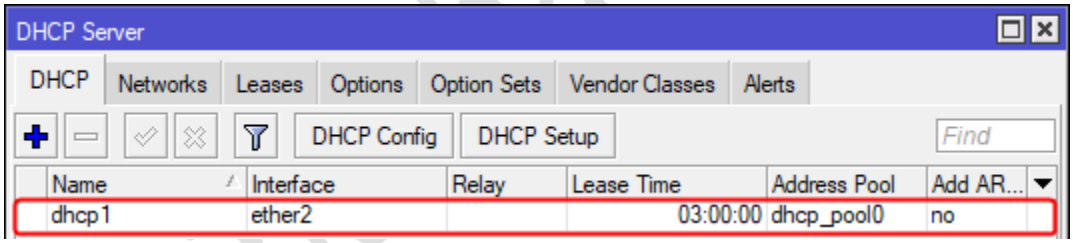


Klik tombol **Next** untuk melanjutkan. Selanjutnya tampil kotak dialog yang menyatakan bahwa *DHCP Setup* telah berhasil diselesaikan, seperti terlihat pada gambar berikut:



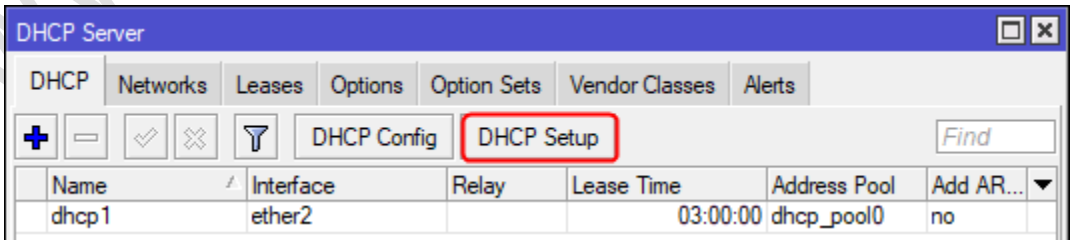
Klik tombol **OK**.

Hasil dari pembuatan *DHCP Server* pada *interface* **ether2**, seperti terlihat pada gambar berikut:

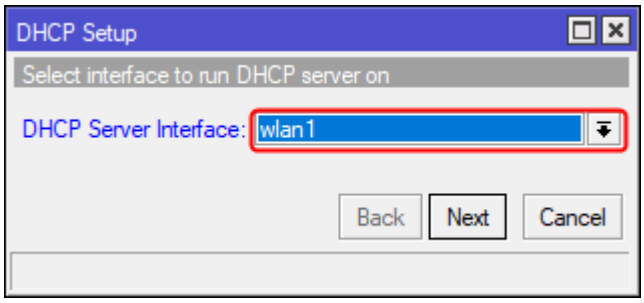


Selanjutnya dengan cara yang sama seperti diatas lakukan pembuatan **Server DHCP** untuk **WLAN**.

Pada kotak dialog **DHCP Server,** klik tombol **DHCP Setup** untuk membuat **DHCP Server** secara *wizard*, seperti terlihat pada gambar berikut:

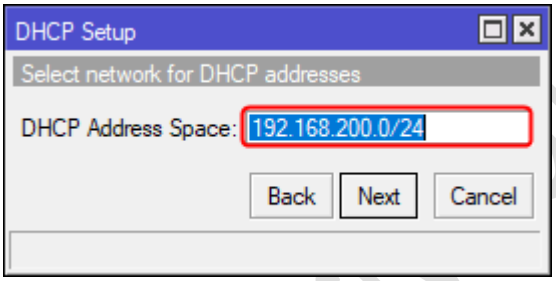


Selanjutnya akan tampil kotak dialog **DHCP Setup** untuk memilih *interface* yang akan menjalankan *server DHCP*, seperti terlihat pada gambar berikut:



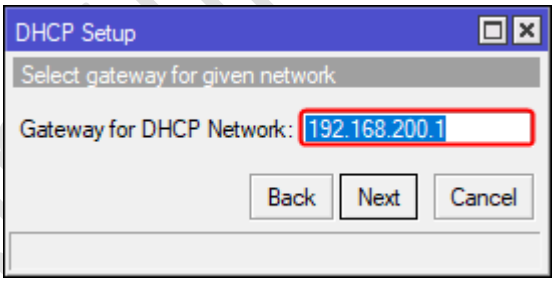
Pilih **wlan1** untuk pembuatan *DHCP Server* bagi **WLAN** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat jaringan yang dialokasikan untuk alamat DHCP, seperti terlihat pada gambar berikut:



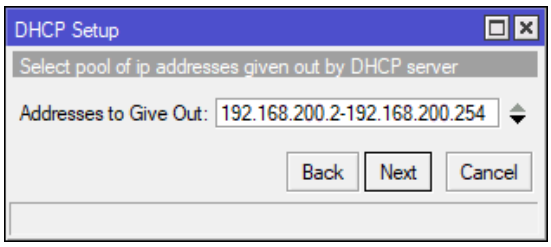
Masukkan alamat jaringan **192.168.200.0/24** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat *gateway* untuk jaringan DHCP, seperti terlihat pada gambar berikut:

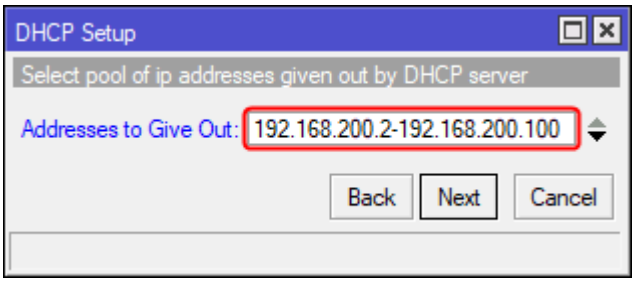


Masukkan alamat IP **192.168.200.1** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan rentang alamat IP yang didistribusikan ke client, seperti terlihat pada gambar berikut:

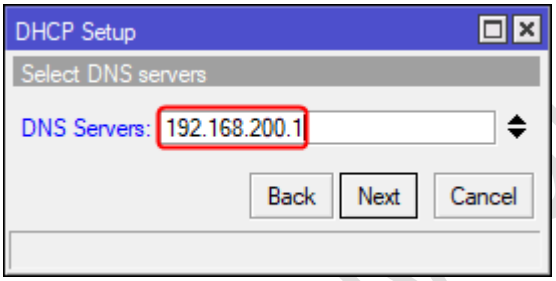


Masukkan alamat IP **192.168.200.2-192.168.200.100**, seperti terlihat pada gambar berikut:



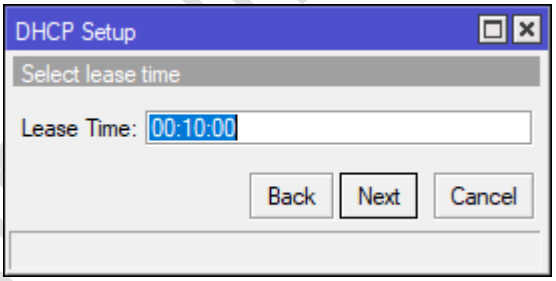
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog **DHCP Setup** untuk menentukan alamat *DNS Servers*, seperti terlihat pada gambar berikut:

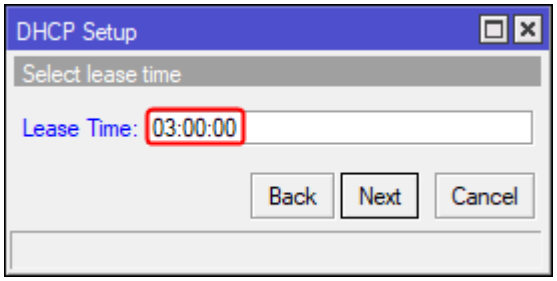


Masukkan alamat IP dari *router Mikrotik* yaitu **192.168.200.1** dan klik tombol **Next**.

Tampil kotak dialog **DHCP Setup** untuk menentukan waktu sewa alamat IP ke *client DHCP*, seperti terlihat pada gambar berikut:

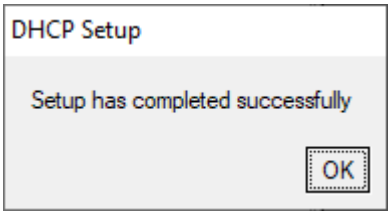


Masukkan nilai **03:00:00** agar masa sewanya adalah **3 jam**, seperti terlihat pada gambar berikut:

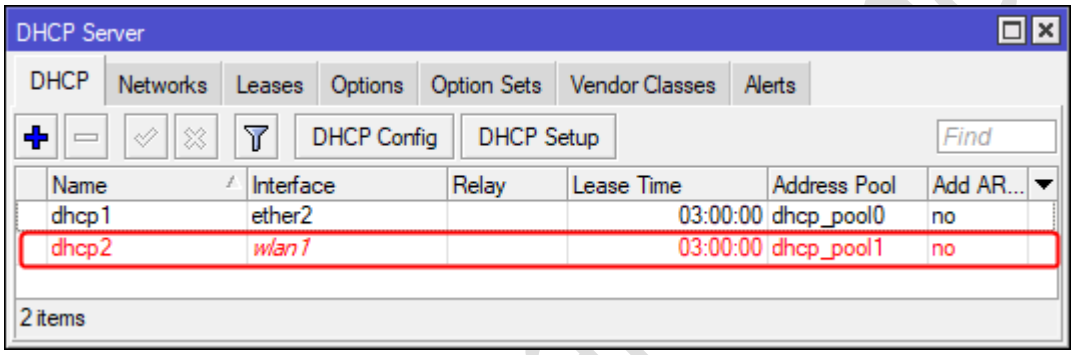


Klik tombol **Next** untuk melanjutkan.

Selanjutnya tampil kotak dialog yang menyatakan bahwa **DHCP Setup** telah berhasil diselesaikan, seperti terlihat pada gambar berikut:



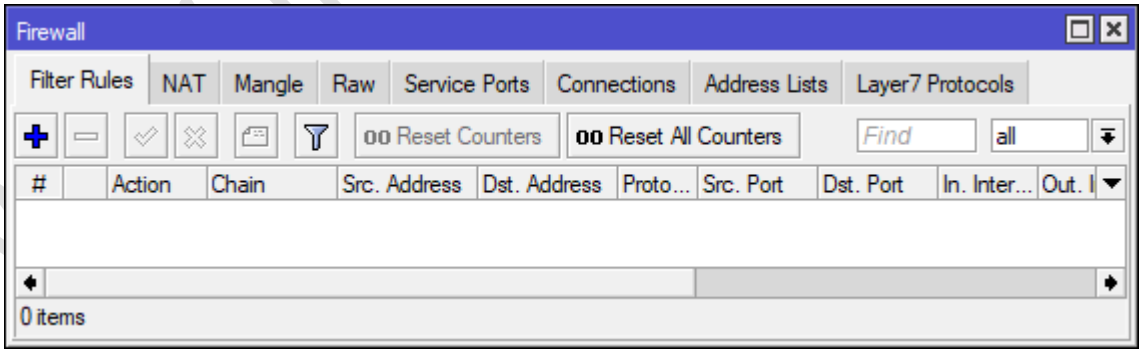
Klik tombol **OK**. Hasil dari pembuatan **DHCP Server** pada **interface wlan1**, terlihat seperti pada gambar berikut:



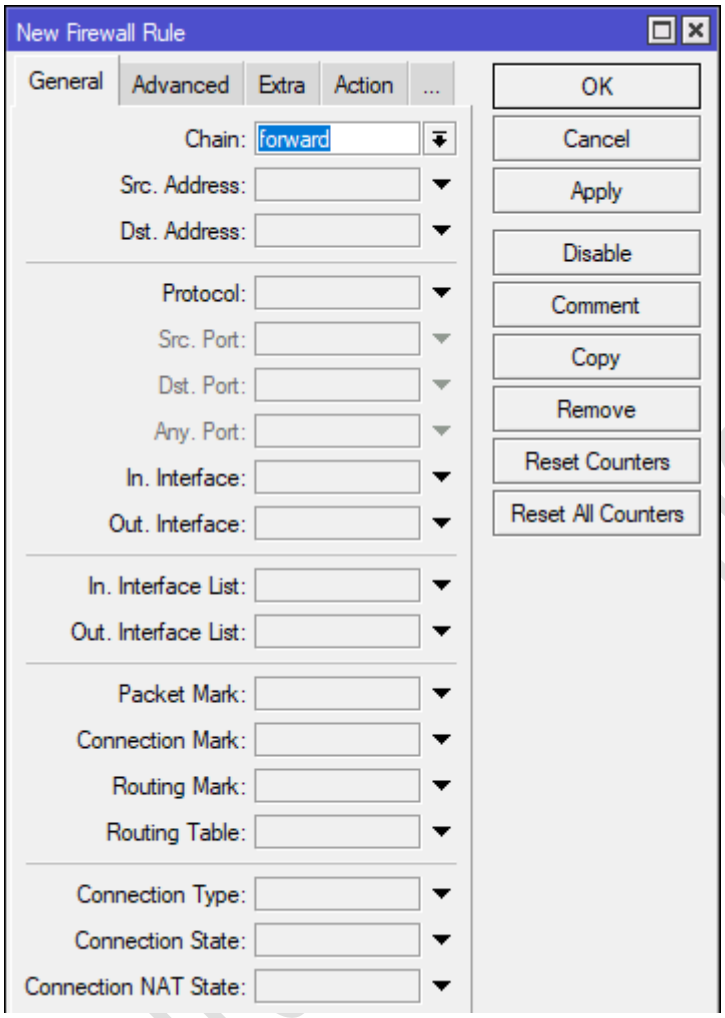
Tutup kotak dialog **DHCP Server**.

11. Mengatur **Firewall** agar **router Mikrotik menolak ping yang diterima pada interface ether2** dari **client LAN** dengan alamat IP **192.168.100.2-192.168.100.50**.

    Pada panel sebelah kiri *Winbox*, pilih **IP > Firewall**, maka akan tampil kotak dialog **Firewall**, seperti terlihat pada gambar berikut:



Untuk menambahkan **Filter Rules** agar menolak *ping* ke *router Mikrotik* dari *client* dengan rentang alamat IP tertentu, pilih tombol  pada toolbar dari kotak dialog *Firewall* maka akan tampil kotak dialog **New Firewall Rule**, seperti terlihat pada gambar berikut:



Pada tab **General** terdapat beberapa parameter yang diatur yaitu:

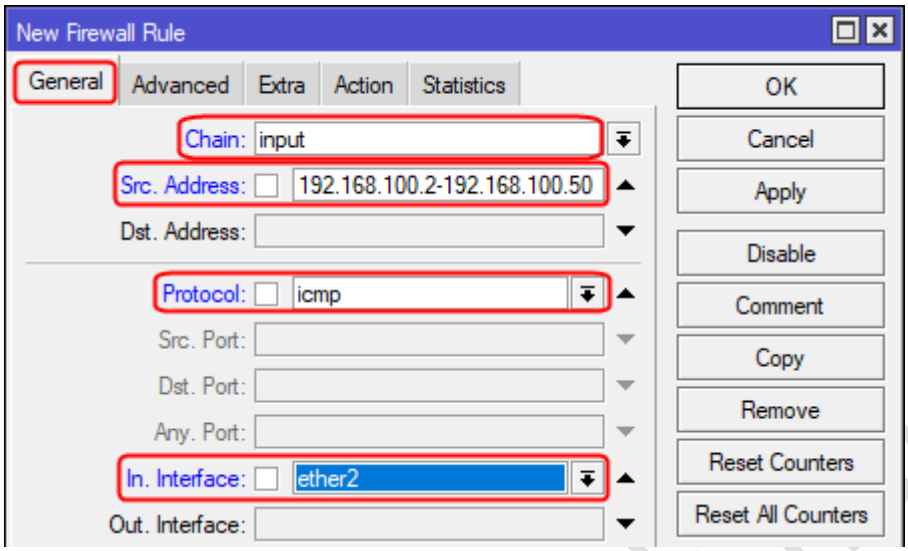
a) **Chain**, digunakan untuk menentukan jenis *chain* yang dibuat rulenya yaitu **input** agar memfilter paket yang masuk ke *router*.

b) **Src. Address**, digunakan untuk menentukan alamat IP sumber yang ditolak akses pingnya yaitu alamat IP **192.168.100.2-192.168.100.50**.

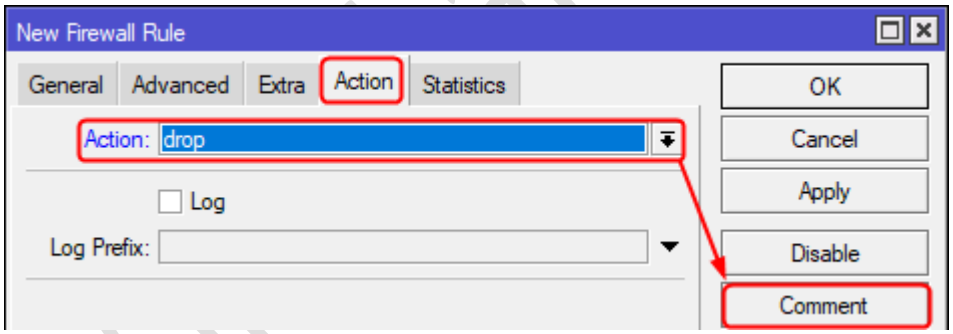
c) **Protocol**, digunakan untuk menentukan protocol yang difilter yaitu **icmp**.

d) **In. Interface**, digunakan untuk menentukan *interface* dimana *router* menerima paket yang akan di *filter* yaitu **ether2**.

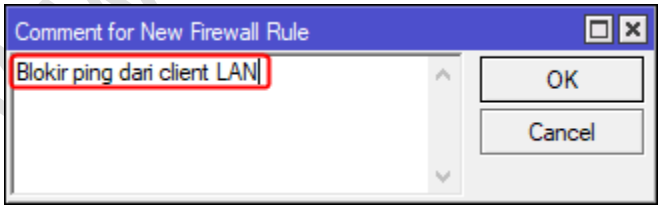
Hasil dari pengaturan pada tab **General** akan terlihat seperti pada gambar berikut:



Selanjutnya pindah ke tab **Action** dan atur parameter **Action** dengan pilihan **drop** agar menolak atau membuang paket yang sesuai dengan kriteria yang ditentukan yaitu menolak paket terkait *ping* serta lakukan penambahan deskripsi terkait *firewall rule* yang dibuat dengan menekan tombol **Comment**, seperti terlihat pada gambar berikut:



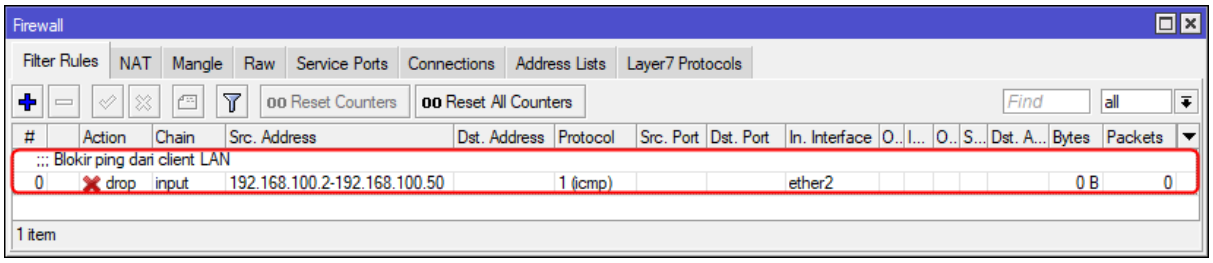
Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Blokir ping dari client LAN**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

Hasil dari penambahan **Filter Rule**, seperti terlihat pada gambar berikut:



12. Mengatur **Firewall** agar **router Mikrotik menolak ping yang berasal dari alamat IP sumber 192.168.100.51-192.168.100.100 dengan tujuan ke client WLAN 192.168.200.0/24**.

Pada *toolbar* dari kotak dialog **Firewall** tab **Filter Rules**, pilih tombol  untuk menambahkan **rule** sehingga *router* menolak meneruskan *ping* yang bersumber dari alamat IP **192.168.100.51-192.168.100.100** ke **client WLAN**.

Pada tab **General** dari kotak dialog **New Firewall Rule** yang tampil, terdapat beberapa parameter yang diatur yaitu:

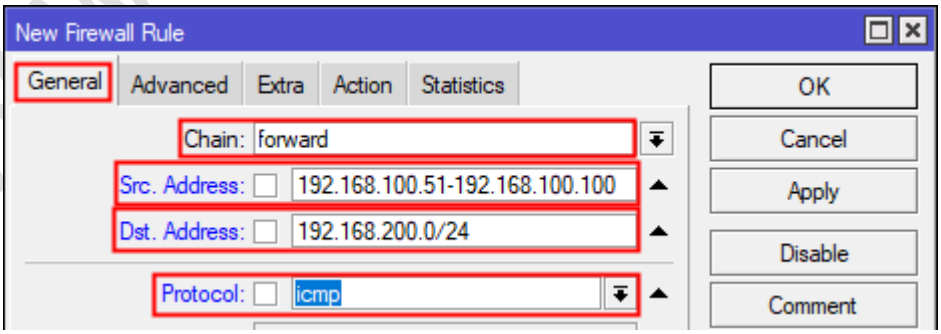
a) **Chain**, digunakan untuk menentukan jenis *chain* yang dibuat *rule*nya yaitu **forward** agar memfilter paket yang melewati *router*.

b) **Src. Address**, digunakan untuk menentukan alamat **IP sumber** yang ditolak akses *ping*nya yaitu alamat IP **192.168.100.51-192.168.100.100**.

c) **Protocol**, digunakan untuk menentukan protocol yang di *filter* yaitu **icmp**.

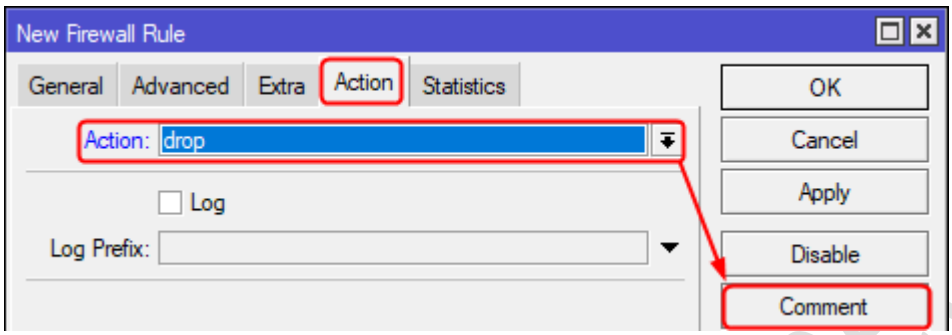
d) **Dst. Address**, digunakan untuk menentukan alamat **IP tujuan** dari *ping* yang akan di *filter* yaitu **client WLAN** dengan alamat *network* **192.168.200.0/24**.

Hasil dari pengaturan pada tab **General** akan terlihat seperti pada gambar berikut:

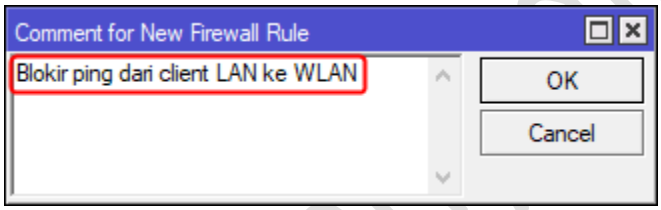


Selanjutnya pindah ke tab **Action** dan atur parameter **Action** dengan pilihan **drop** agar menolak atau membuang paket yang sesuai dengan kriteria yang ditentukan yaitu

menolak paket terkait *ping* serta lakukan penambahan deskripsi terkait *firewall rule* yang dibuat dengan menekan tombol **Comment**, seperti terlihat pada gambar berikut:



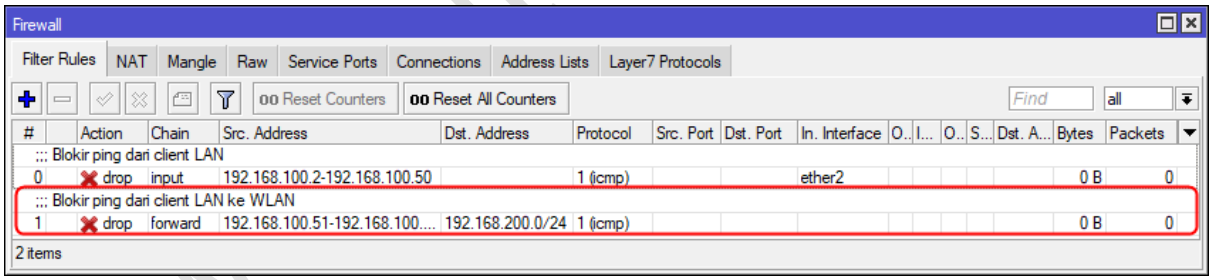
Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Blokir ping dari client LAN ke WLAN**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

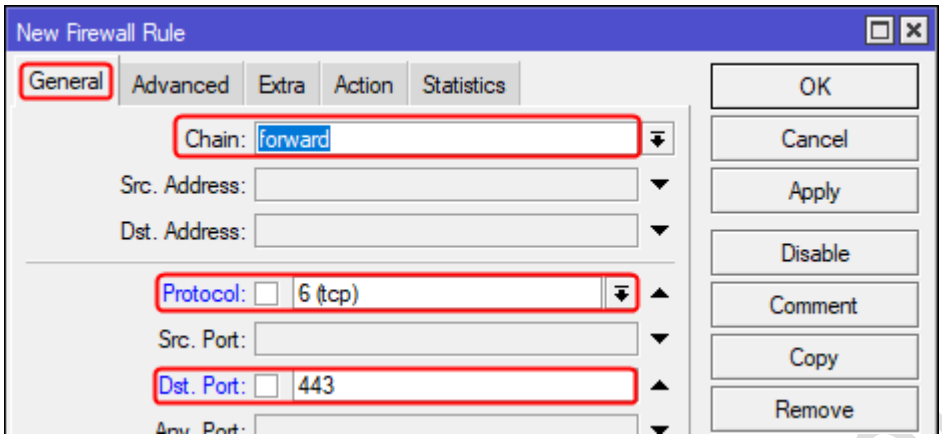
Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

Hasil dari penambahan **Filter Rule**, seperti terlihat pada gambar berikut:



13. Memblokir situs https://www.linux.org menggunakan **TLS-Host**.

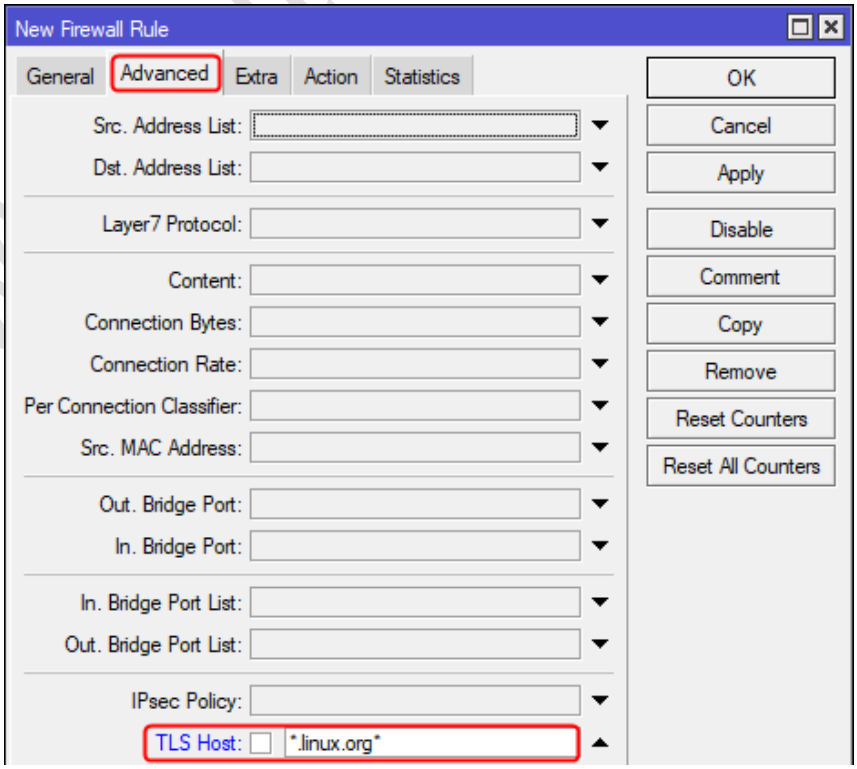
Pada *toolbar* dari kotak dialog **Firewall** tab **Filter Rules**, pilih tombol  untuk menambahkan **rule** sehingga dapat memblokir situs https://www.linux.org. Selanjutnya akan tampil kotak dialog **New Firewall Rule**. Pada tab **General** dari kotak dialog **New Firewall Rule**, terdapat beberapa parameter yang harus diatur, seperti terlihat pada gambar berikut:



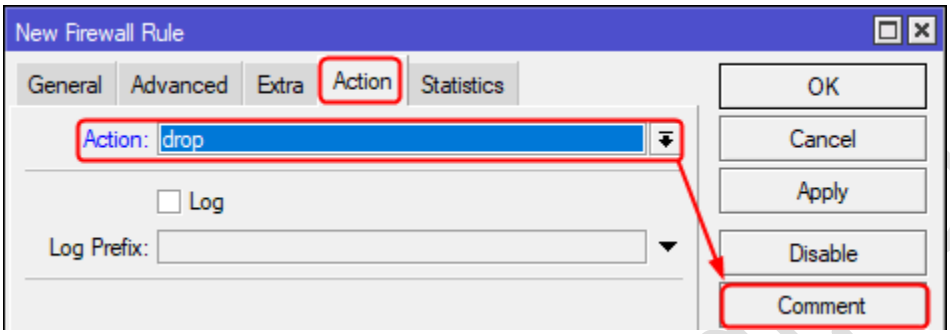
Penjelasan parameter:

- **Chain**, menentukan chain yang digunakan yaitu **forward** agar memproses paket yang melewati *Mikrotik***.**
- **Protocol**, menentukan protokol *transport* yang digunakan oleh *HTTPS* yaitu **6 (tcp)**.
- **Dst. Port**, menentukan nomor port tujuan yaitu **443** untuk protokol HTTPS.

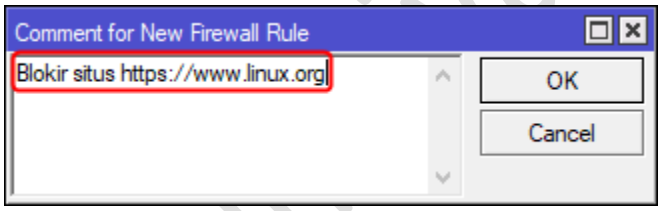
Selanjutnya pindah ke tab **Advanced** dan lakukan pengaturan pada parameter **TLS host** dengan nilai **"*.linux.org*"**, seperti terlihat pada gambar berikut:



Terakhir pindah ke tab **Action.** Pastikan pilihan parameter **Action** adalah **drop** untuk menolak paket yang cocok dengan rule yang ditentukan serta lakukan penambahan deskripsi terkait *firewall rule* yang dibuat dengan menekan tombol **Comment**, seperti terlihat pada gambar berikut:



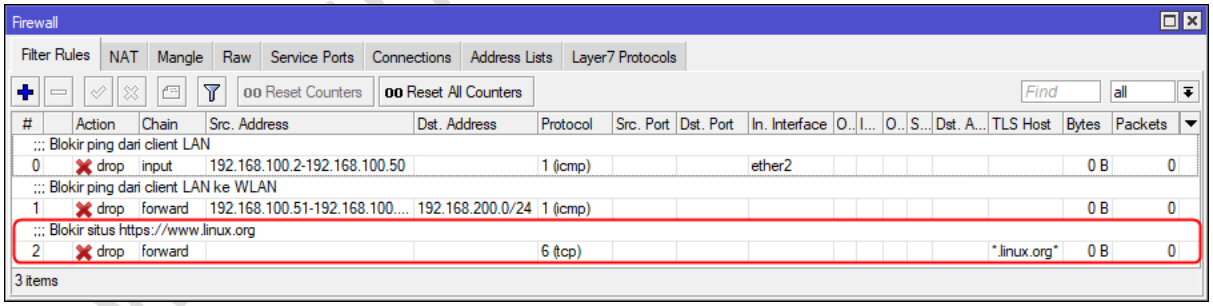
Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Blokir situs https://www.linux.org**", seperti terlihat pada gambar berikut:



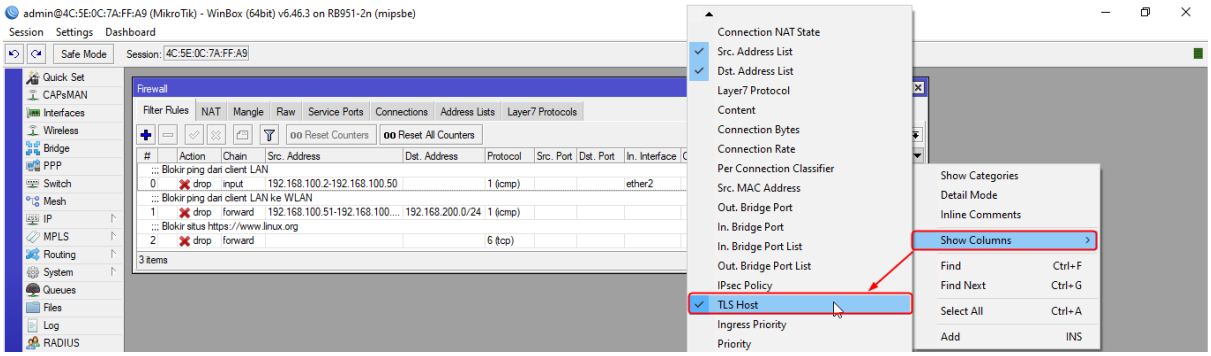
Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



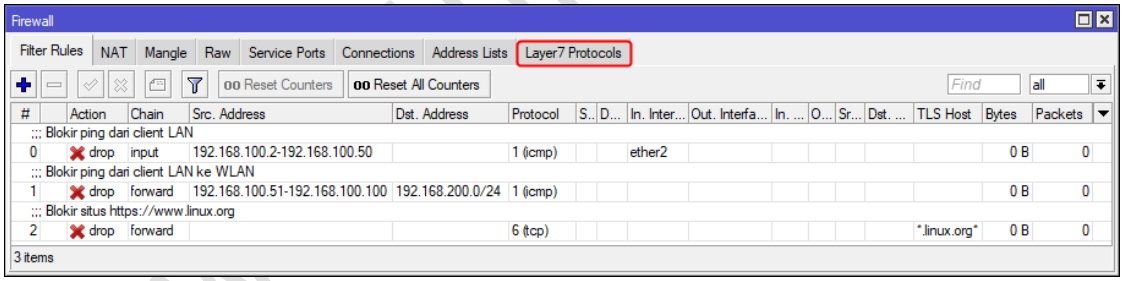
Untuk menampilkan kolom **TLS Host** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **TLS Host**, seperti terlihat pada gambar berikut:



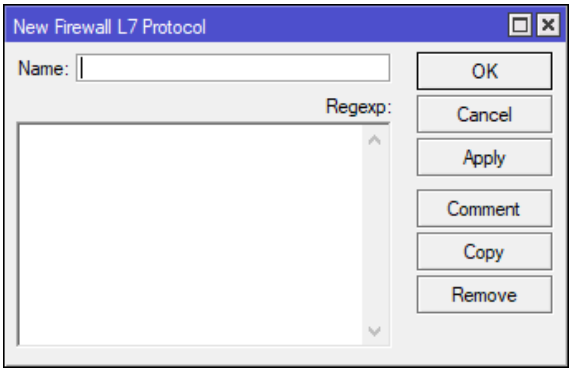
14. Memblokir **file** dengan ekstensi .**mp3** dan .**mkv** menggunakan **IP Firewall Filter Rules**, dan **IP Firewall Mangle** serta **Layer7 Protocols**. *IP Firewall Layer 7 Protocols* digunakan untuk melakukan pencocokan pola (*pattern*) menggunakan *regular expression (regex)* terkait *file* dengan ekstensi **.mp3** dan **.mkv**. *IP Firewall Mangle* digunakan untuk menandai koneksi dan paket terkait file berekstensi **.mp3** dan **.mkv** yang telah dibuat **L7 Protocol**-nya. Sedangkan **IP Firewall Filter Rules** digunakan untuk memblokir *packet* yang telah ditandai tersebut.

a) Membuat **Layer7 Protocols** untuk pencocokan **file** dengan ekstensi **mp3**.

Pilih tab **Layer7 Protocols** pada kotak dialog **Firewall** yang tampil, seperti terlihat pada gambar berikut:



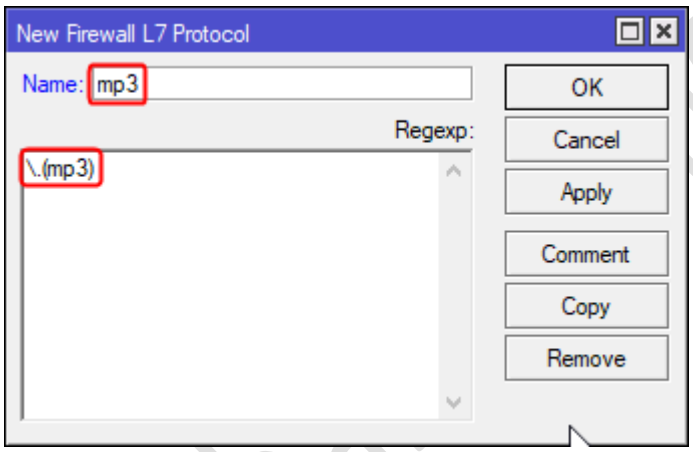
Untuk menambahkan *rule* baru, pilih tombol  pada *toolbar* dari kotak dialog **Firewall tab Layer7 Protocols** maka akan tampil kotak dialog **New Firewall L7 Protocol,** seperti terlihat pada gambar berikut:



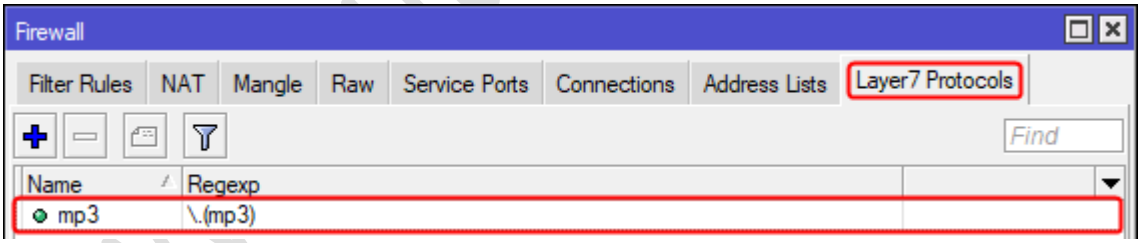
Terdapat beberapa parameter yang harus diatur yaitu:

- **Name**, digunakan untuk menentukan nama pengenal *L7 Protocol* yang dibuat, sebagai contoh **mp3**.
- **Regexp**, digunakan untuk menentukan pola pencocokan *regular expression* terkait *file* dengan ekstensi *mp3*, yaitu **\.(mp3)**

Hasil dari pengaturan parameter tersebut, seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan. Hasil dari penambahan *rule* akan terlihat seperti gambar berikut:



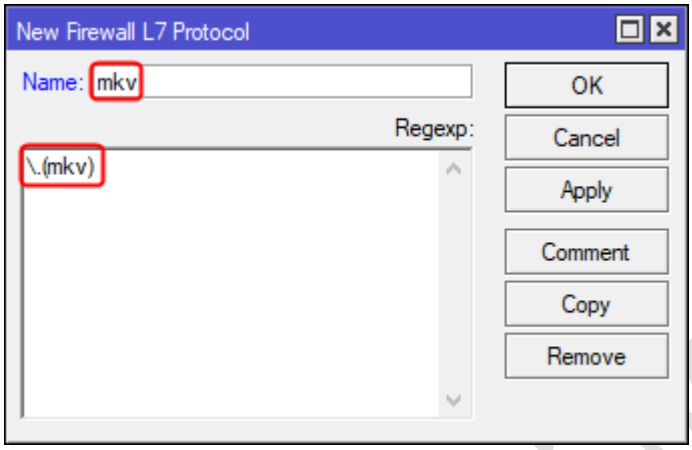
b) Membuat **Layer7 Protocols** untuk pencocokan **file** dengan ekstensi **mkv**.

Pilih tombol  pada *toolbar* dari kotak dialog **Firewall tab Layer7 Protocols** untuk menambahkan *rule* baru maka akan tampil kotak dialog **New Firewall L7 Protocol**.

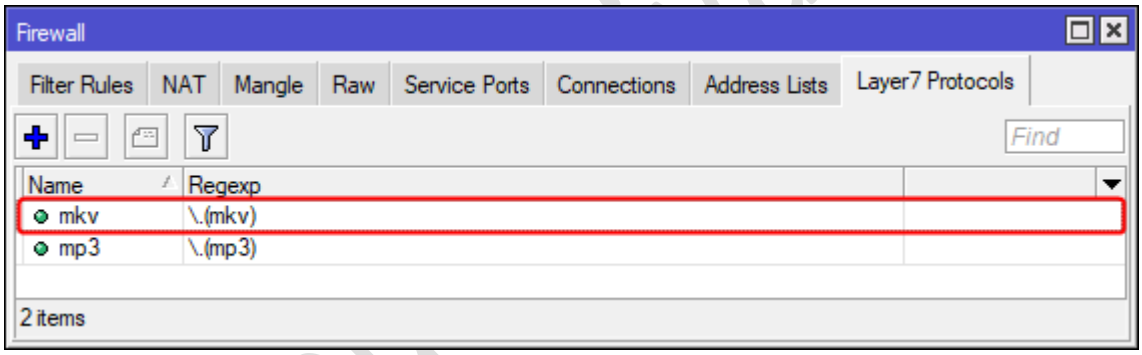
Terdapat beberapa parameter yang harus diatur yaitu:

- **Name**, digunakan untuk menentukan nama pengenal *L7 Protocol* yang dibuat, sebagai contoh **mkv**.
- **Regexp**, digunakan untuk menentukan pola pencocokan regular expression terkait *file* dengan ekstensi *mkv*, yaitu **\.(mkv)**

Hasil dari pengaturan parameter tersebut, seperti terlihat pada gambar berikut:

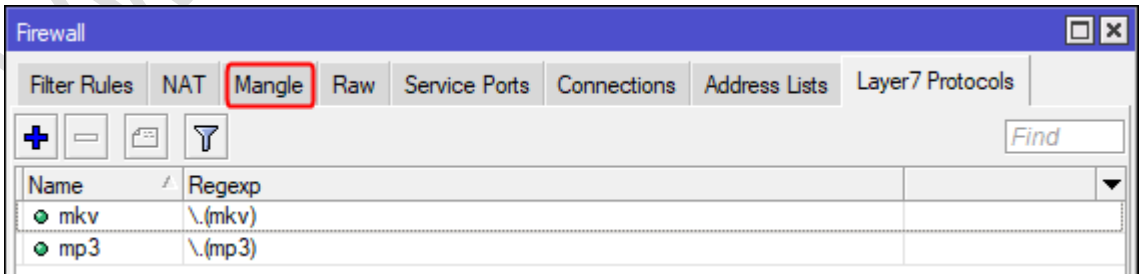


Klik tombol **OK** untuk menyimpan. Hasil dari penambahan *rule* tersebut akan terlihat seperti gambar berikut:

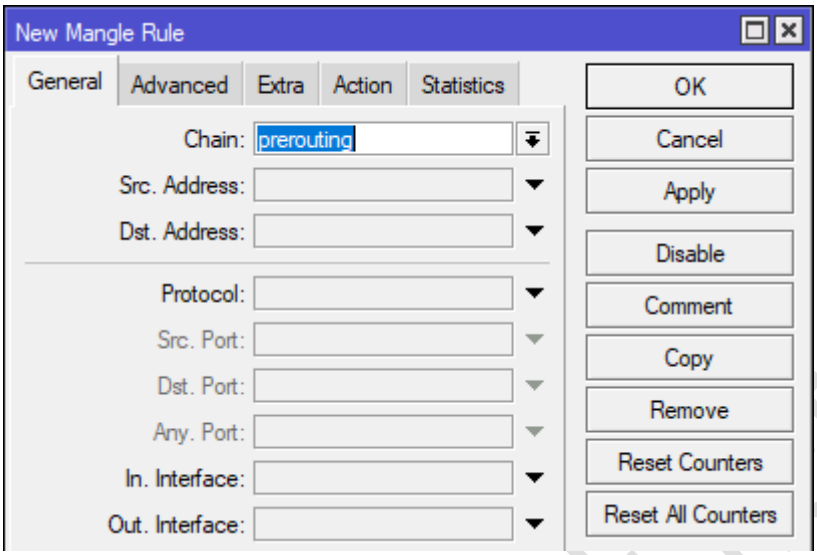


c) Membuat **IP Firewall Mangle** untuk menandai koneksi (**mark connection**) dan paket (**mark-packet**) terkait *file* berekstensi **.mp3**.

Pilih tab **Mangle** pada kotak dialog **Firewall** yang tampil, seperti terlihat pada gambar berikut:

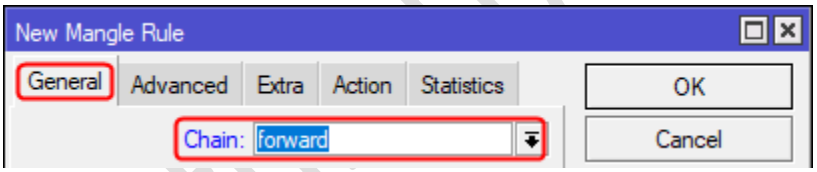


Untuk menambahkan *rule* baru, pilih tombol  pada *toolbar* dari kotak dialog **Firewall tab Mangle** maka akan tampil kotak dialog **New Mangle Rule,** seperti terlihat pada gambar berikut:

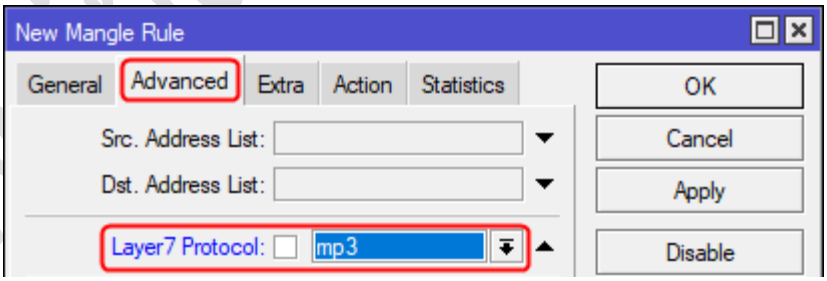


Terdapat beberapa parameter yang harus diatur yaitu:

- Pada tab **General**, pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati *Mikrotik*), seperti terlihat pada gambar berikut:

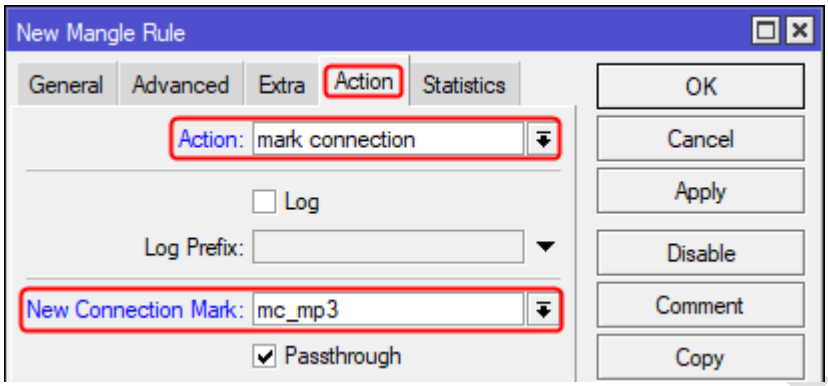


- Pindah ke tab **Advanced**, pastikan pilihan parameter **Layer7 Protocol** adalah **mp3**, seperti terlihat pada gambar berikut:

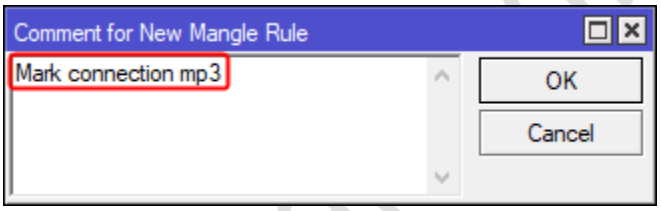


- Pindah ke tab **Action** dan lakukan pengaturan pada 2 (dua) parameter berikut:
  - ✓ **Action**, digunakan untuk mengatur tindakan yang akan diambil jika paket cocok dengan aturan. Pilih **mark connection** untuk menandai koneksi terkait *file* berekstensi **.mp3**.
  - ✓ **New Connection Mark**, digunakan untuk mengatur nama pengenal dari **mark connection** yang dibuat, sebagai contoh **mc_mp3**.

Hasil dari pengaturan pada tab *Action*, seperti terlihat pada gambar berikut.



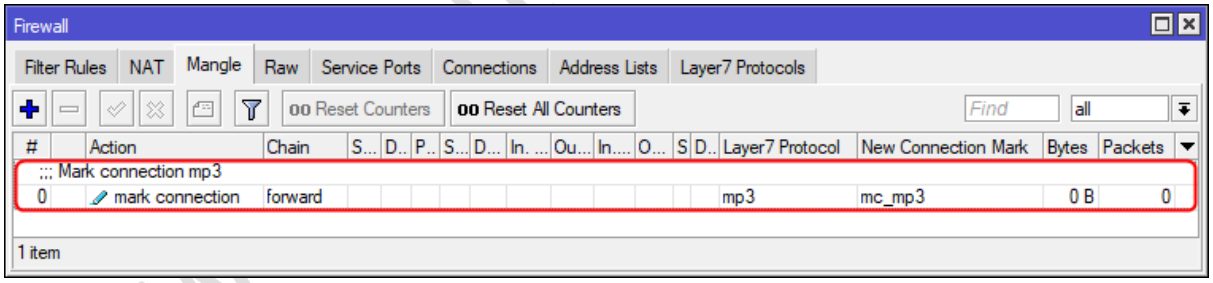
Selanjutnya lakukan penambahan deskripsi terkait *mangle rule* yang dibuat dengan menekan tombol **Comment.** Pada kotak dialog **Comment for New Mangle Rule** yang tampil, masukkan "**Mark connection mp3**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *mangle rule* baru.

Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:

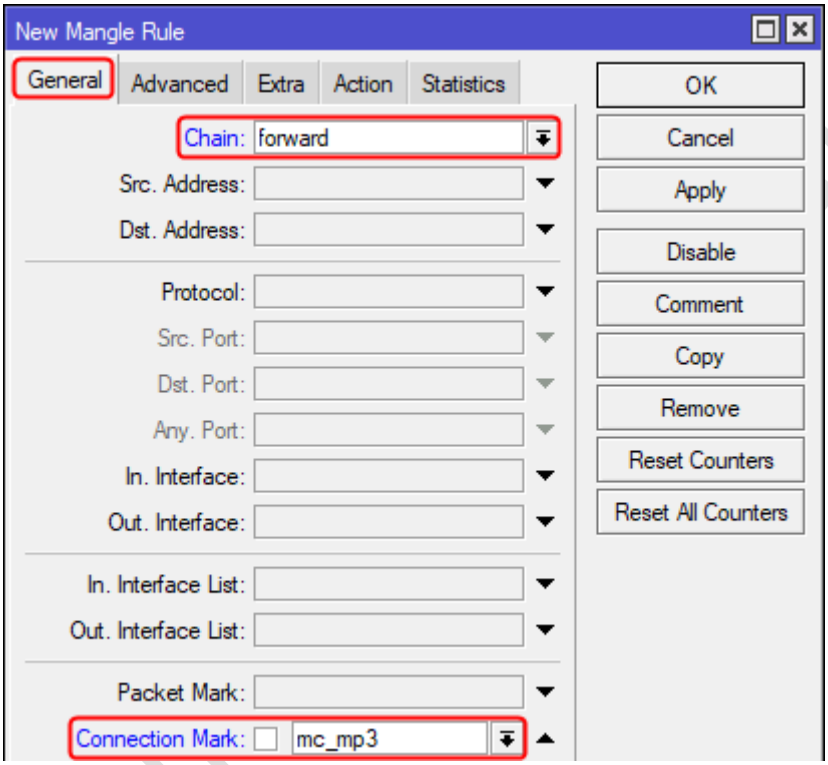


Untuk menampilkan kolom **Layer7 Protocol** dan **New Connection Mark** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **Layer7 Protocol dan New Connection Mark.**

Dengan cara yang sama, lakukan penambahan *rule* baru terkait **mark paket** dengan memilih tombol ✚ pada *toolbar* dari kotak dialog **Firewall tab Mangle.**

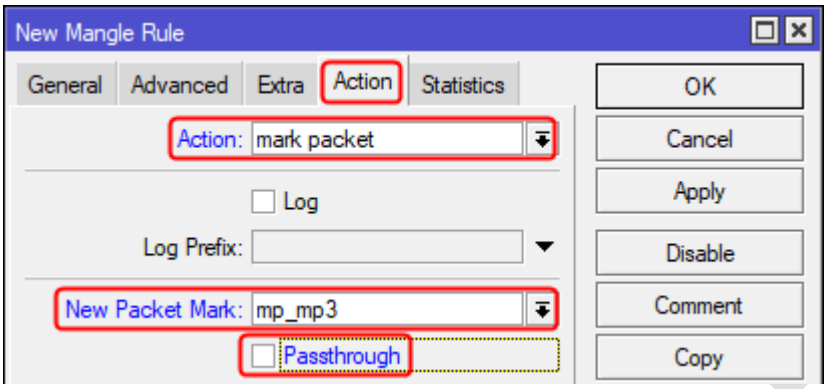
Terdapat beberapa parameter yang harus diatur pada kotak dialog **New Mangle Rule** yang tampil, yaitu:

- Pada tab **General**, pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati *Mikrotik*) dan **Connection Mark** adalah **mc_mp3**, seperti terlihat pada gambar berikut:

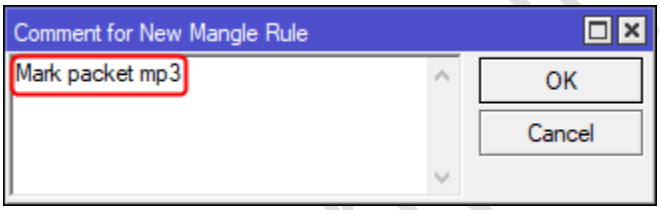


- Pindah ke tab **Action** dan lakukan pengaturan pada 3 (tiga) parameter berikut:
  - ✓ **Action**, digunakan untuk mengatur tindakan yang akan diambil jika paket cocok dengan aturan. Pilih **mark packet** untuk menandai paket terkait *file* berekstensi **.mp3**.
  - ✓ **New Packet Mark**, digunakan untuk mengatur nama pengenal dari **packet mark** yang dibuat, sebagai contoh **mp_mp3**.
  - ✓ Hilang tanda centang atau *checkmark* pada *checkbox* dari parameter **Passthrough** agar paket meninggalkan *Mangle* setelah *rule* ini dan tidak terpengaruh oleh *rule mangle* berikutnya.

Hasil dari pengaturan pada tab *Action*, seperti terlihat pada gambar berikut.



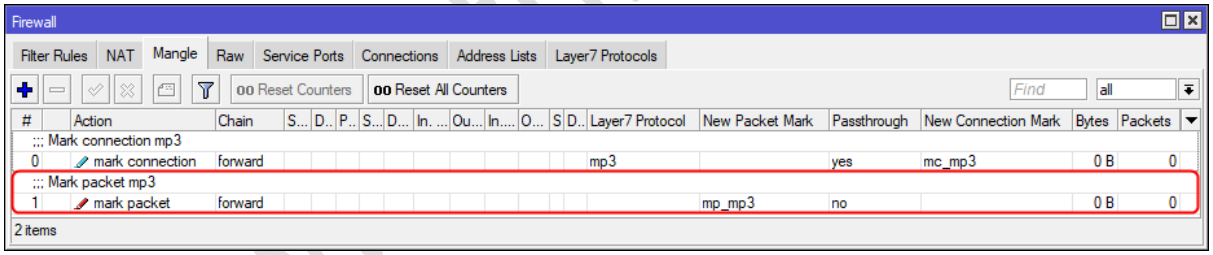
Selanjutnya lakukan penambahan deskripsi terkait *mangle rule* yang dibuat dengan menekan tombol **Comment.** Pada kotak dialog **Comment for New Mangle Rule** yang tampil, masukkan "**Mark packet mp3**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *mangle rule* baru.

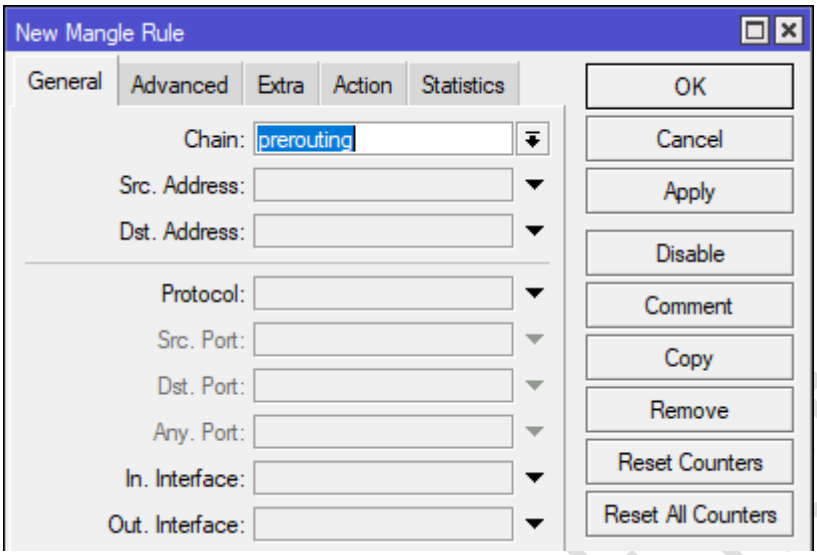
Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



Untuk menampilkan kolom **Passthrough** dan **New Packet Mark** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **Passthrough dan New Packet Mark.**

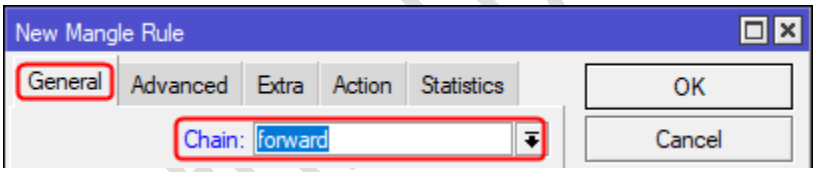
d) Membuat **IP Firewall Mangle** untuk menandai koneksi (**mark connection**) dan paket (**mark-packet**) terkait *file* berekstensi **.mkv**.

Pilih tombol ✚ pada *toolbar* dari kotak dialog **Firewall tab Mangle** untuk menambahkan *rule* baru, maka akan tampil kotak dialog **New Mangle Rule,** seperti terlihat pada gambar berikut:

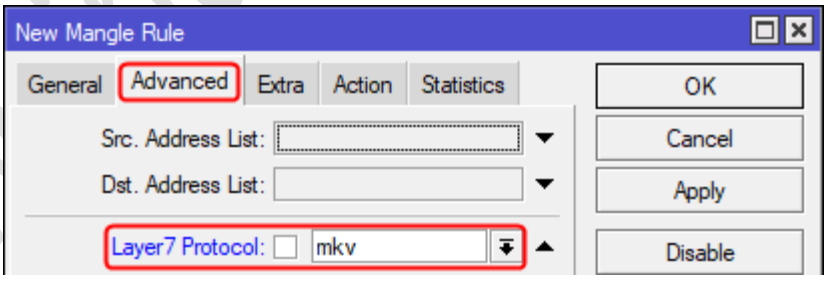


Terdapat beberapa parameter yang harus diatur yaitu:

- Pada tab **General**, pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati *Mikrotik*), seperti terlihat pada gambar berikut:

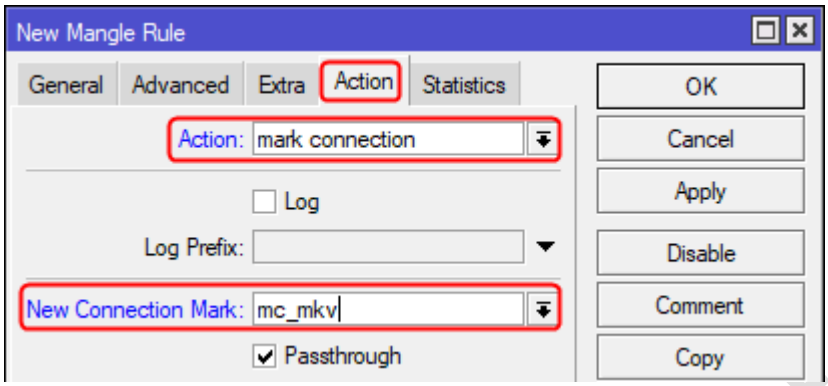


- Pindah ke tab **Advanced**, pastikan pilihan parameter **Layer7 Protocol** adalah **mkv**, seperti terlihat pada gambar berikut:

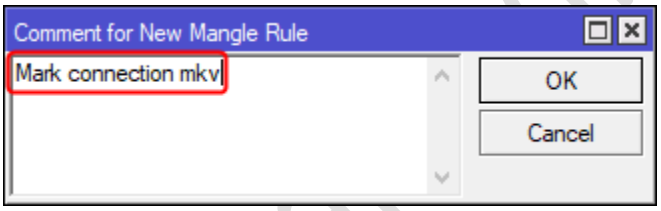


- Pindah ke tab **Action** dan lakukan pengaturan pada 2 (dua) parameter berikut:
  - ✓ **Action**, digunakan untuk mengatur tindakan yang akan diambil jika paket cocok dengan aturan. Pilih **mark connection** untuk menandai koneksi terkait *file* berekstensi **.mkv**.
  - ✓ **New Connection Mark**, digunakan untuk mengatur nama pengenal dari **mark connection** yang dibuat, sebagai contoh **mc_mkv**.

Hasil dari pengaturan pada tab *Action*, seperti terlihat pada gambar berikut.



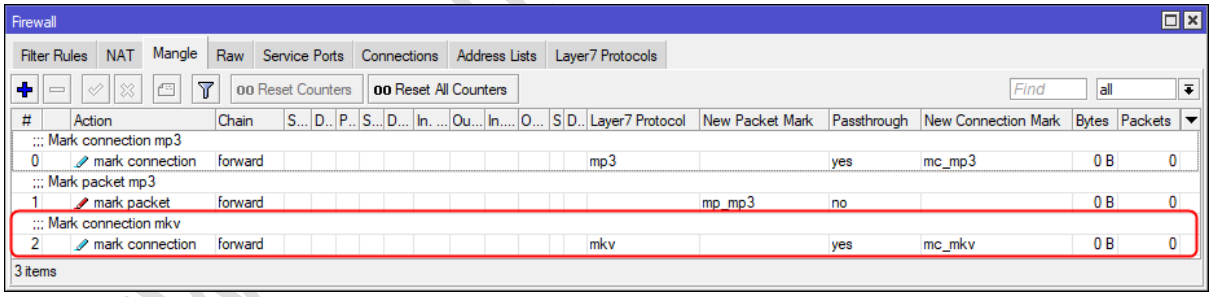
Selanjutnya lakukan penambahan deskripsi terkait *mangle rule* yang dibuat dengan menekan tombol **Comment.** Pada kotak dialog **Comment for New Mangle Rule** yang tampil, masukkan "**Mark connection mkv**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *mangle rule* baru.

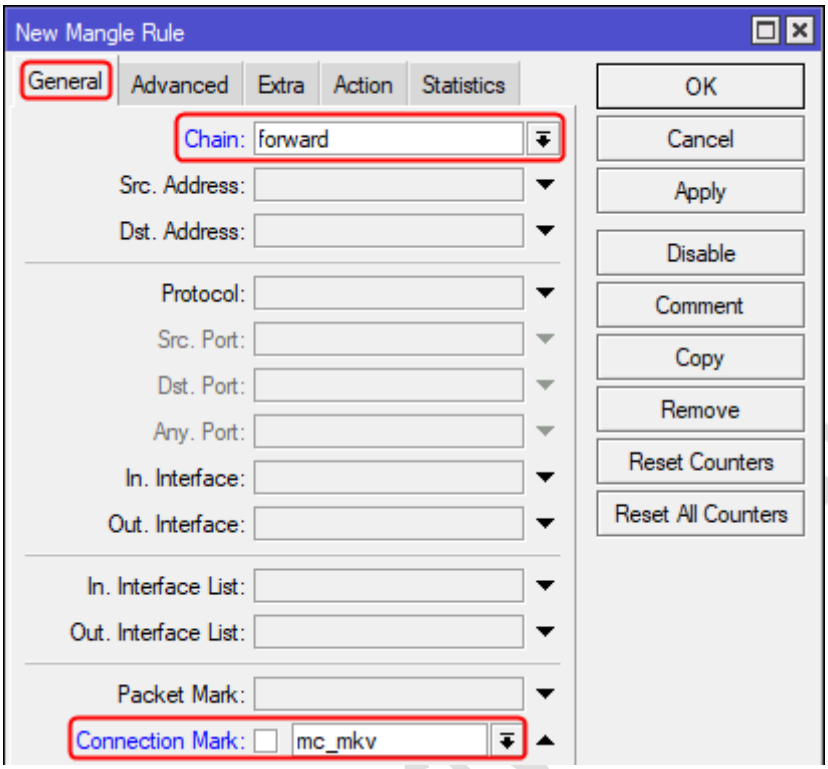
Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



Dengan cara yang sama, lakukan penambahan *rule* baru terkait **mark paket** dengan memilih tombol  pada *toolbar* dari kotak dialog **Firewall tab Mangle.**

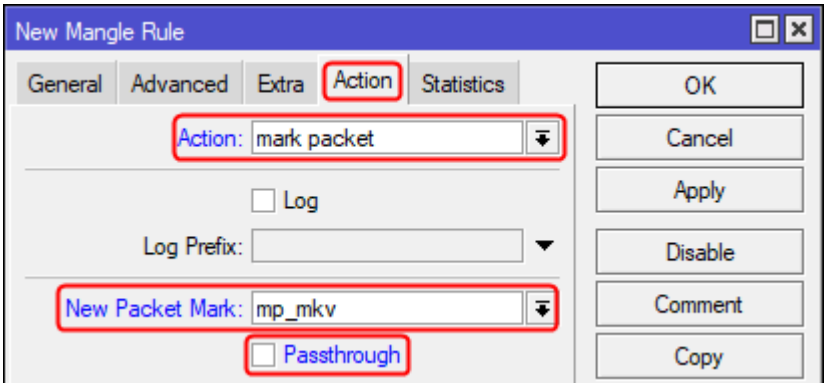
Terdapat beberapa parameter yang harus diatur pada kotak dialog **New Mangle Rule** yang tampil, yaitu:

- Pada tab **General**, pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati *Mikrotik*) dan **Connection Mark** adalah **mc_mkv**, seperti terlihat pada gambar berikut:

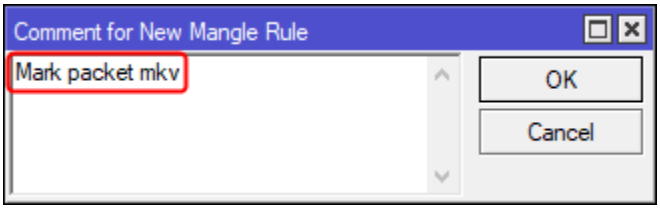


- Pindah ke tab **Action** dan lakukan pengaturan pada 3 (tiga) parameter berikut:
  - ✓ **Action**, digunakan untuk mengatur tindakan yang akan diambil jika paket cocok dengan aturan. Pilih **mark packet** untuk menandai paket terkait *file* berekstensi **.mkv**.
  - ✓ **New Packet Mark**, digunakan untuk mengatur nama pengenal dari **packet mark** yang dibuat, sebagai contoh **mp_mkv**.
- ✓ Hilang tanda centang atau *checkmark* pada *checkbox* dari parameter **Passthrough** agar paket meninggalkan *Mangle* setelah *rule* ini dan tidak terpengaruh oleh *rule mangle* berikutnya.

Hasil dari pengaturan pada tab *Action*, seperti terlihat pada gambar berikut.



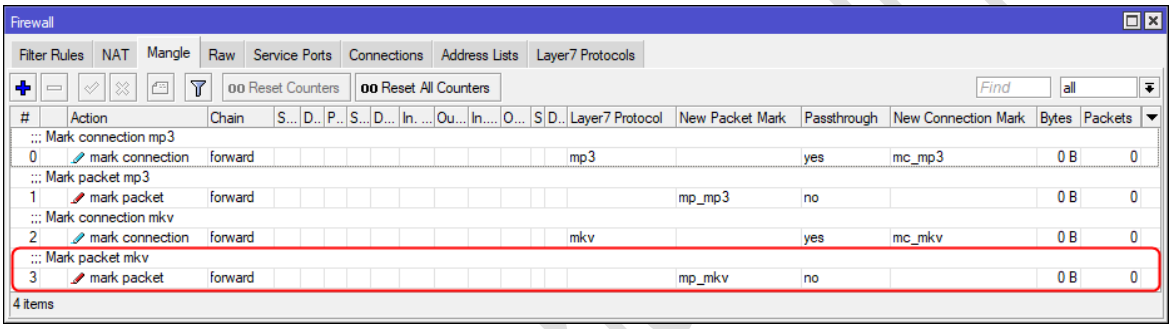
Selanjutnya lakukan penambahan deskripsi terkait *mangle rule* yang dibuat dengan menekan tombol **Comment.** Pada kotak dialog **Comment for New Mangle Rule** yang tampil, masukkan "**Mark packet mkv**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

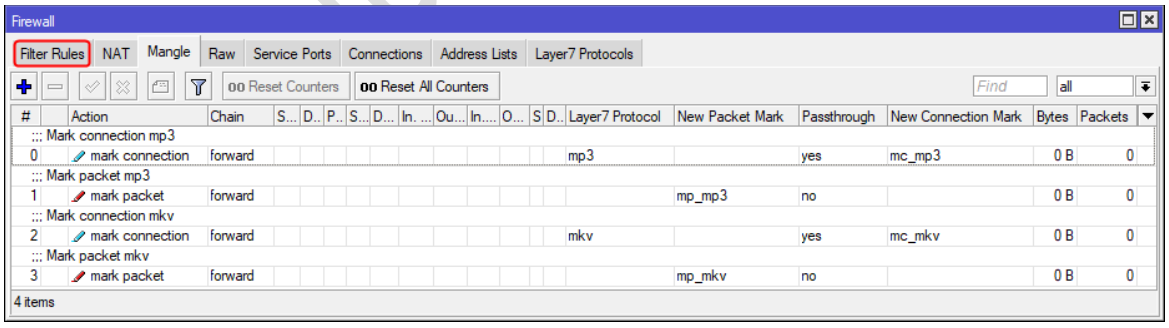
Klik tombol **OK** untuk menyimpan pengaturan *mangle rule* baru.

Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



e) Membuat *IP Firewall Filter Rules* untuk memblokir **file** dengan ekstensi **mp3** berdasarkan **mark packet mp_mp3** yang telah dibuat sebelumnya.

Pilih tab **Filter Rules** pada kotak dialog **Firewall** yang tampil, seperti terlihat pada gambar berikut:

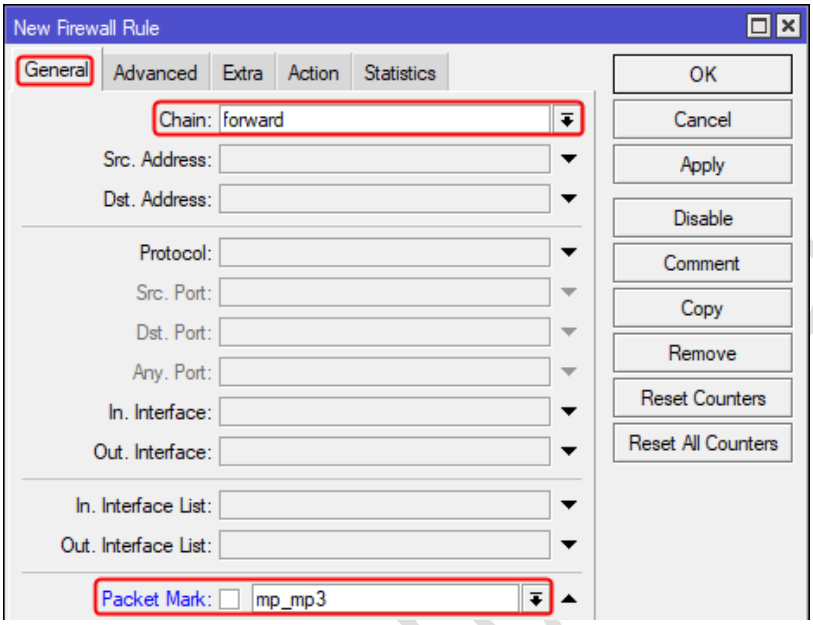


Pilih tombol  pada *toolbar* dari kotak dialog **Firewall** untuk menambahkan *rule* baru maka akan tampil kotak dialog **New Firewall Rule**.

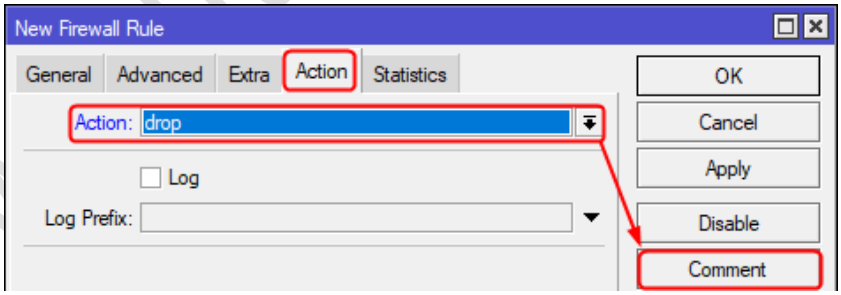
Terdapat beberapa parameter yang harus diatur yaitu:

- Pada tab **General**, terdapat 2 (dua) parameter yang diatur yaitu pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati

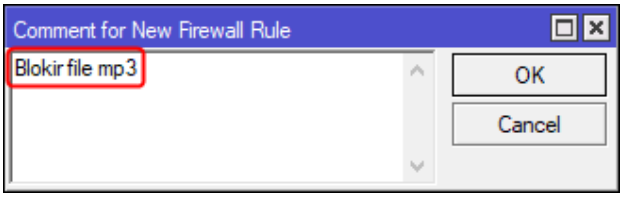
Mikrotik) dan **Packet Mark** adalah **mp_mp3** (untuk mencocokkan paket terkait *file* berekstensi **.mp3** yang telah ditandai menggunakan *mangle*), seperti terlihat pada gambar berikut:



- Lanjut pindah ke tab **Action**, pastikan pilihan parameter **Action** adalah **drop** untuk menolak paket yang cocok dengan *rule* yang ditentukan dan lakukan penambahan deskripsi terkait *firewall rule* yang dibuat dengan menekan tombol **Comment**, seperti terlihat pada gambar berikut:



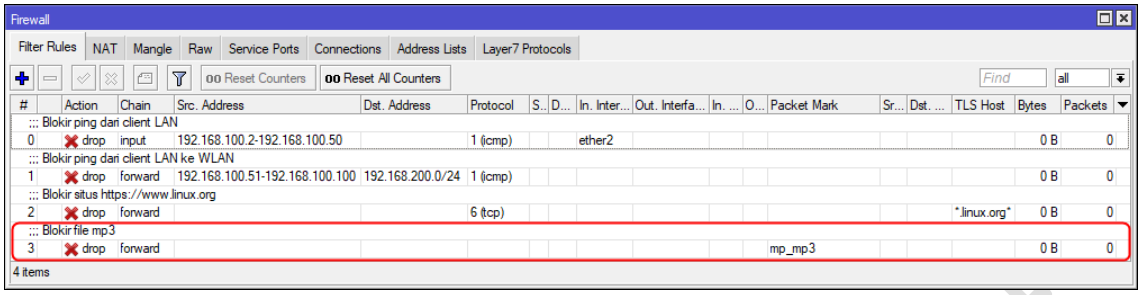
Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Blokir file mp3**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

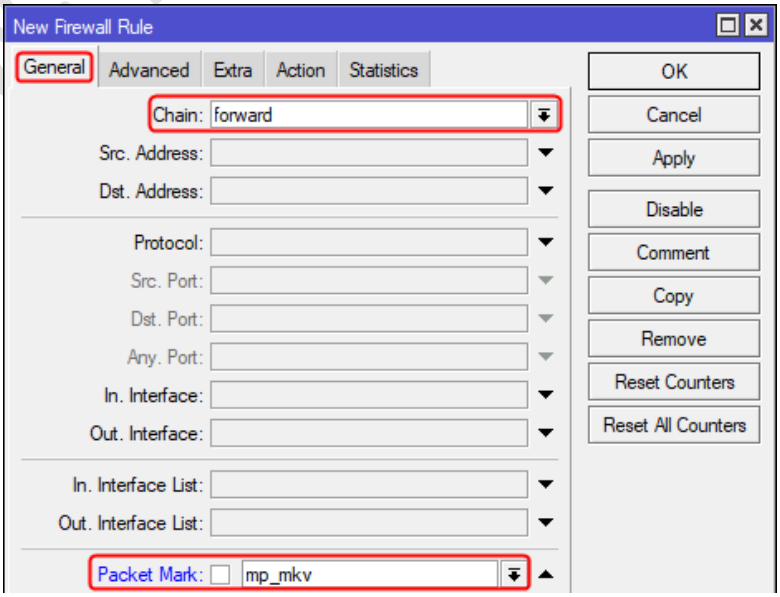
Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



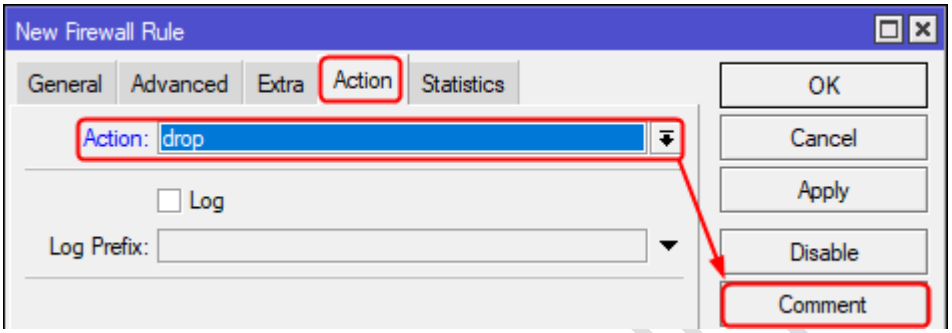
Untuk menampilkan kolom **Packet Mark** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **Packet Mark.**

f) Membuat *IP Firewall Filter Rules* untuk memblokir **file** dengan ekstensi **mkv** berdasarkan **mark packet mp_mkv** yang telah dibuat sebelumnya. Pilih tombol ✚ pada *toolbar* dari kotak dialog **Firewall** untuk menambahkan *rule* baru maka akan tampil kotak dialog **New Firewall Rule**. Terdapat beberapa parameter yang harus diatur yaitu:

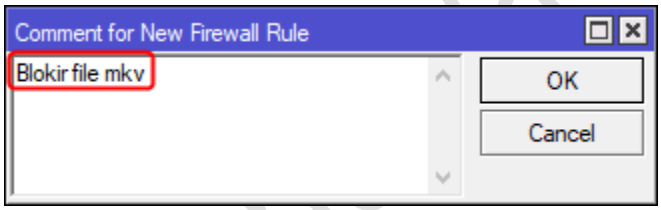
- Pada tab **General**, terdapat 2 (dua) parameter yang diatur yaitu pastikan pilihan parameter **Chain** adalah **forward** (agar memproses paket yang melewati *Mikrotik*) dan **Packet Mark** adalah **mp_mkv** (untuk mencocokkan paket terkait *file* berekstensi **.mkv** yang telah ditandai menggunakan *mangle*), seperti terlihat pada gambar berikut:



- Lanjut pindah ke tab **Action**, pastikan pilihan parameter **Action** adalah **drop** untuk menolak paket yang cocok dengan *rule* yang ditentukan dan lakukan penambahan deskripsi terkait *firewall rule* yang dibuat dengan menekan tombol **Comment**, seperti terlihat pada gambar berikut:



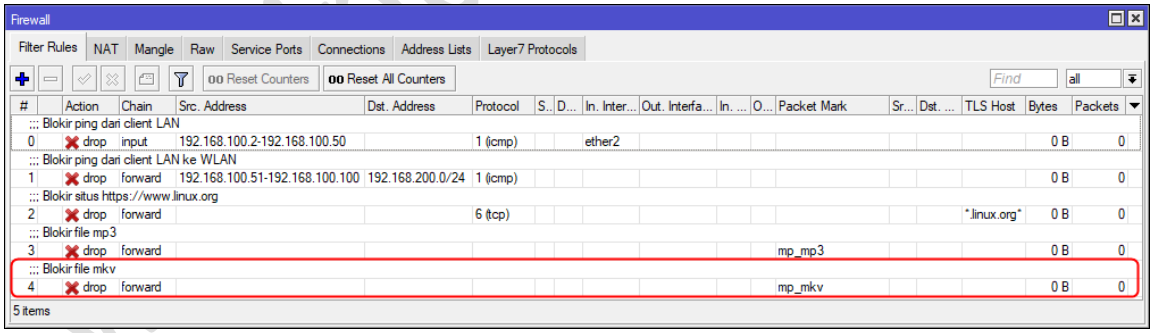
Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Blokir file mkv**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

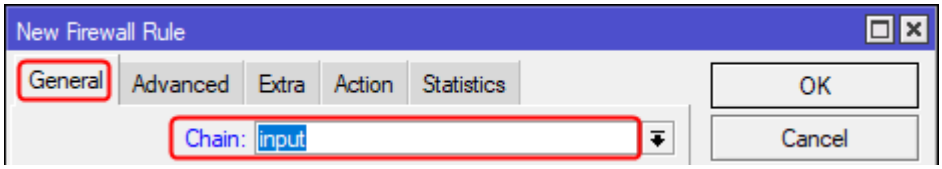
Hasil dari penambahan *rule* akan terlihat seperti pada gambar berikut:



15. Membuat **rule** agar setiap akses ke *router* tercatat di **log dan tersimpan di disk** menggunakan **IP Firewall Filter** dan **System Logging**.

a) Menambahkan **Filter Rules** untuk mencatat (*log*) setiap akses ke *router* dengan memilih tombol  pada *toolbar* dari kotak dialog **Firewall** tab **Filter Rules** maka akan tampil kotak dialog **New Firewall Rule.** Pada tab **General** dari kotak dialog **New Firewall Rule** lakukan pengaturan parameter **Chain** yang digunakan untuk

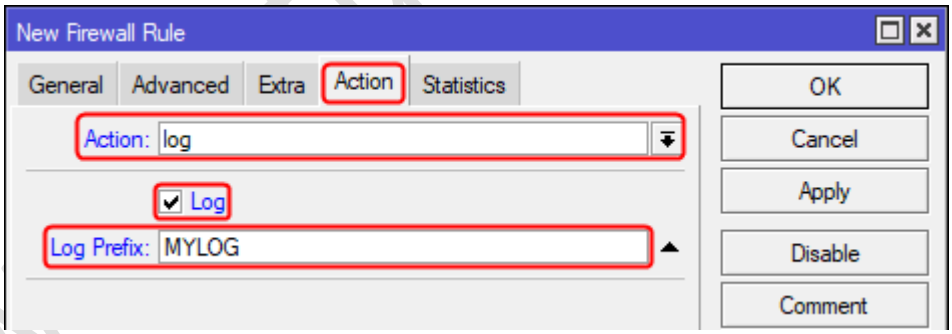
menentukan jenis *chain* yang dibuat *rule*nya yaitu **input** sehingga dapat mem*filter* paket yang masuk ke *router*, seperti terlihat pada gambar berikut:



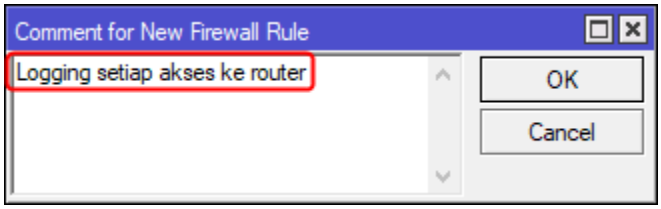
Selanjutnya pindah ke tab **Action.** Terdapat beberapa parameter yang diatur pada kotak dialog **New Firewall Rule** tab **Action** ini yaitu:

- **Action**, digunakan untuk mengatur tindakan yang akan diambil jika paket cocok dengan aturan. Pilih **log** agar mencatat setiap akses yang diterima pada *interface* dari *router* ke *system log*.
- **Log**, tandai atau centang pilihan ini untuk mengaktifkan *log* dengan cara memilih inputan *checkbox* yang terdapat diawal dari keterangan parameter ini.
- **Log Prefix:** digunakan untuk menambahkan teks di awal dari setiap pesan log, sebagai contoh dengan nilai "**MYLOG**".

Hasil dari pengaturan pada tab *Action*, seperti terlihat pada gambar berikut:



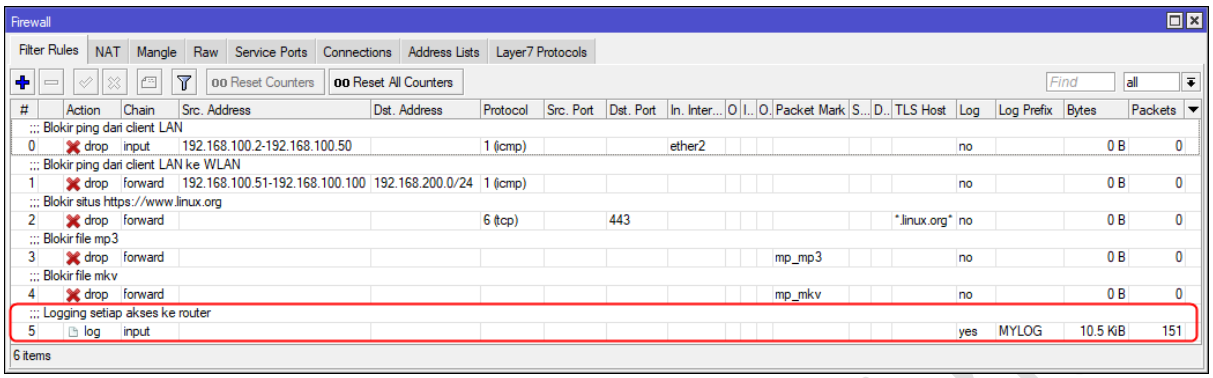
Selanjutnya klik tombol **Comment** untuk menambahkan deskripsi terkait *firewall rule* yang dibuat. Pada kotak dialog **Comment for New Firewall Rule** yang tampil, masukkan "**Logging setiap akses ke router**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

Klik tombol **OK** untuk menyimpan pengaturan *firewall rule* baru.

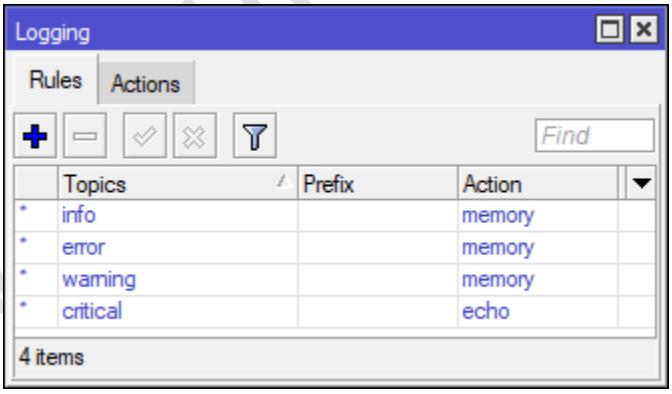
Hasil dari penambahan **Filter Rules** tersebut, seperti terlihat pada gambar berikut:



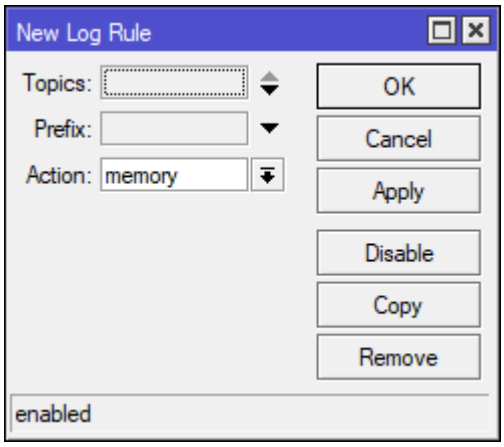
Untuk menampilkan kolom **Log** dan **Log Prefix** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **Log dan Log Prefix.**

b) Membuat **rule** pada **System Logging** agar **log** dengan **prefix MYLOG** pada langkah **15a** sebelumnya tersimpan secara permanen ke **disk**.

Pada panel sebelah kiri *Winbox*, pilih **System > Logging** maka akan tampil kotak dialog *Logging*, seperti terlihat pada gambar berikut:



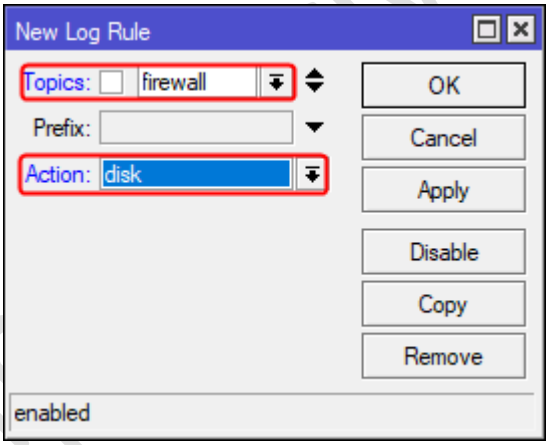
Pilih tombol  pada *toolbar* dari kotak dialog **Logging** tab **Filter Rules** untuk menambahkan **rule** maka akan tampil kotak dialog **New Firewall Rule**, seperti terlihat pada gambar berikut:



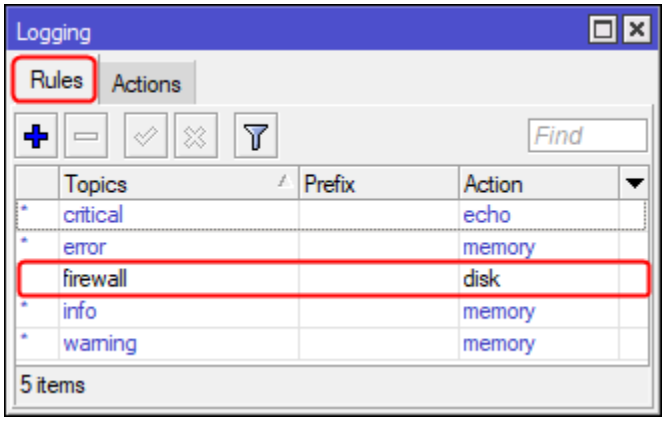
Terdapat beberapa parameter yang diatur pada kotak dialog ini yaitu:

- **Topics:** digunakan untuk menentukan topik sebagai sumber dari pesan log. Pilih **firewall**.
- **Action:** digunakan untuk menentukan lokasi penyimpanan log. Pilih **disk**.

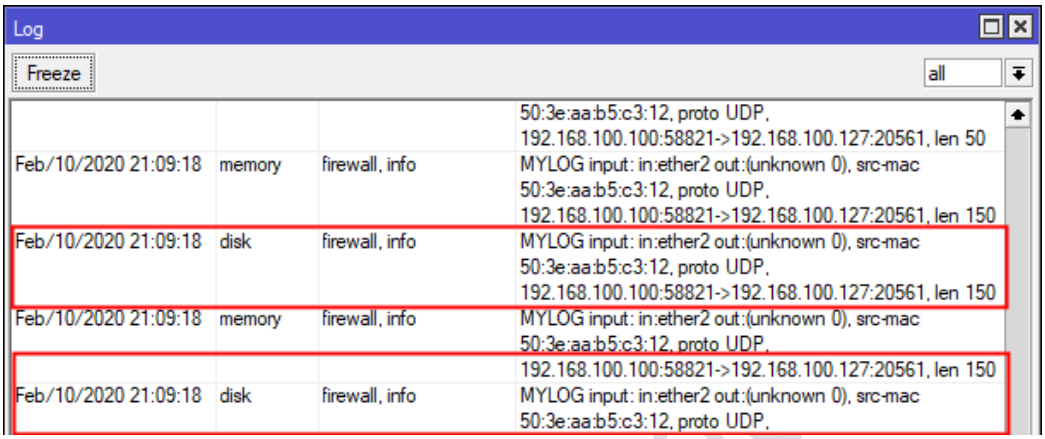
Hasil dari pengaturan **New Log Rule**, seperti terlihat pada gambar berikut:



Klik **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *rule system logging*, seperti terlihat pada gambar berikut:

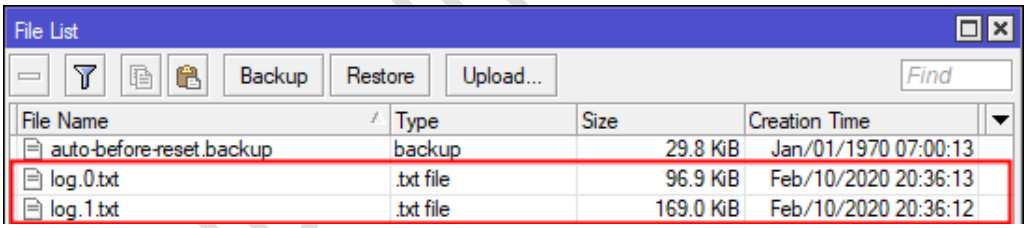


16. Memverifikasi hasil pengaturan **system logging** terkait pencatatan setiap akses ke *router* yang akan disimpan ke **disk** dengan mengakses menu **Log** pada panel sebelah kiri dari *Winbox*. Selanjutnya akan tampil kotak dialog **Log**, seperti terlihat pada gambar berikut:



Terlihat *log* dengan **prefix MYLOG** berhasil disimpan ke **disk**. Tutup kotak dialog *Log*.

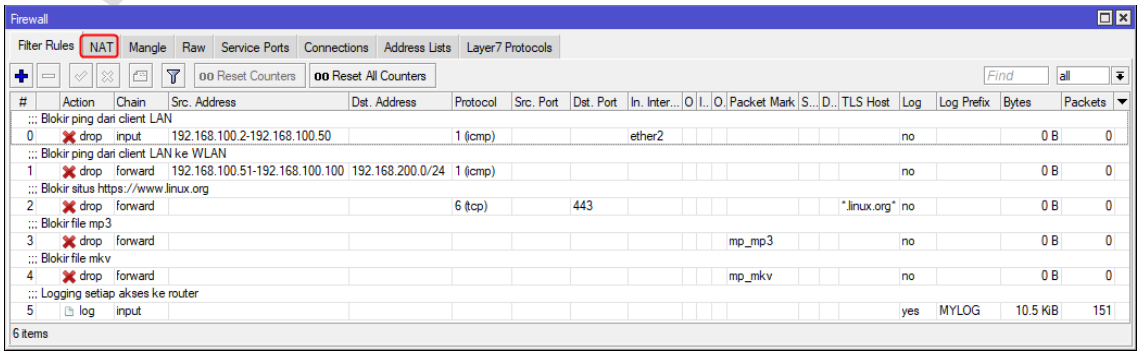
17. Memverifikasi **file log** sebagai hasil dari penyimpanan *log* ke **disk** dengan mengakses menu **Files** melalui panel sebelah kiri dari *Winbox*. Selanjutnya akan tampil kotak dialog **Files**, seperti terlihat pada gambar berikut:



Terlihat **file** dengan nama **log.0.txt** dan **log.1.txt**. Tutup kotak dialog **Files**.

18. Mengatur **Source Network Address Translation (SNAT)** untuk **Internet Connection Sharing (ICS)** baik bagi **client LAN** maupun **WLAN** menggunakan **IP Firewall NAT**.

Pengaturan ICS dapat dilakukan dengan memilih tab **NAT** pada kotak dialog **Firewall**, seperti terlihat pada gambar berikut:

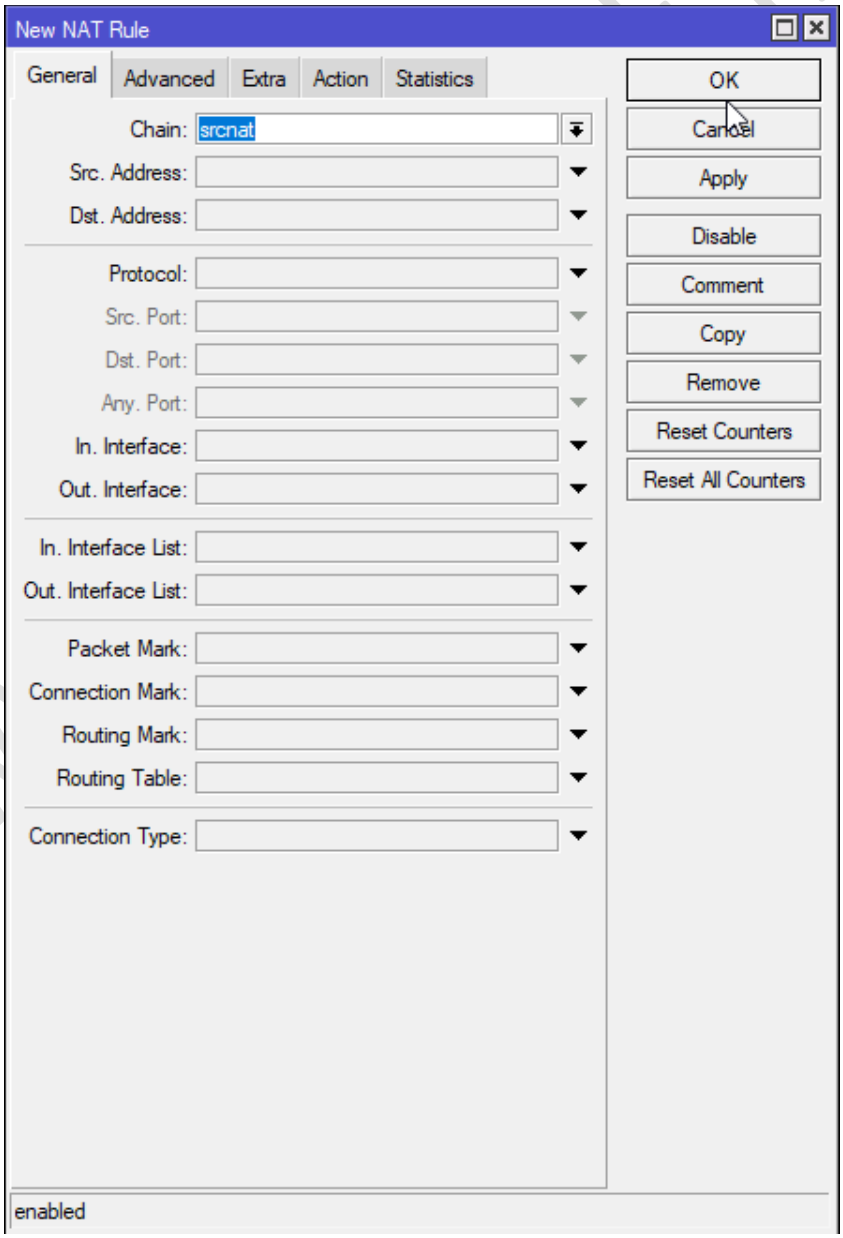


Perhatian:

Apabila kotak dialog **Firewall** belum terakses atau tampil maka silakan mengakses kembali melalui panel sebelah kiri dari *Winbox* dan memilih **IP > Firewall** serta pilih tab **NAT** setelah tampil kotak dialog **Firewall**.

Pilih tombol  pada *toolbar* dari kotak dialog **Firewall** tab **NAT** untuk menambahkan *NAT rule* sehingga mengijinkan akses Internet bagi seluruh client baik berkabel maupun nirkabel.

Selanjutnya akan tampil kotak dialog **NAT Rule**, seperti terlihat pada gambar berikut:

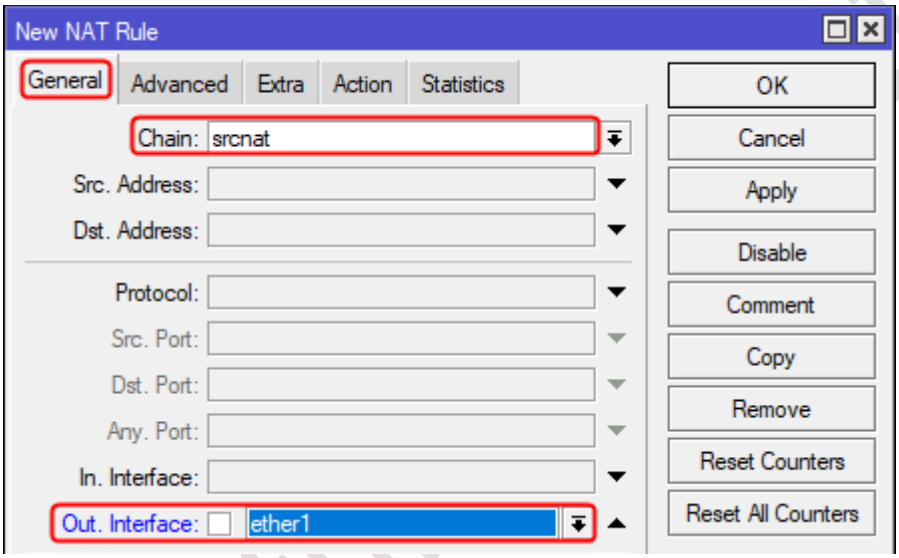


Pada tab **General** terdapat beberapa parameter yang diatur yaitu:

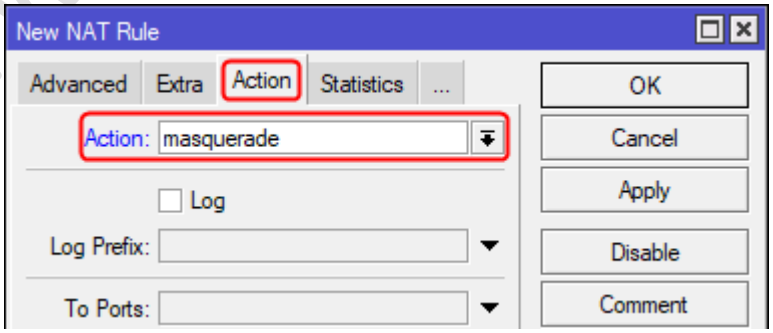
a) **Chain**, digunakan untuk menentukan jenis *chain* yang dibuat *rule*nya yaitu **srcnat** untuk mentranslasi alamat IP sumber.

b) **Out Interface**, digunakan untuk menentukan interface yang mengarah ke *Internet* yaitu **ether1**.

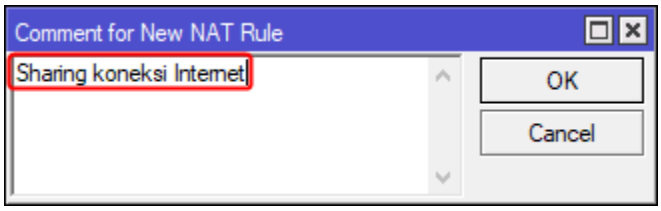
Hasil dari pengaturan pada tab *General* akan terlihat seperti pada gambar berikut:



Selanjutnya pindah ke tab **Action** dan lakukan pengaturan parameter **Action** dengan pilihan **masquerade** untuk melakukan translasi alamat IP sumber menjadi alamat IP yang digunakan oleh *interface ether1* sebagai interface yang terhubung ke Internet, seperti terlihat pada gambar berikut:



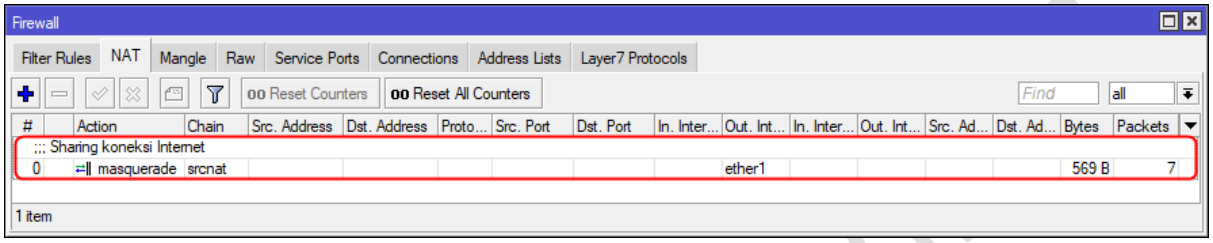
Selanjutnya klik tombol **Comment** untuk menambahkan deskripsi terkait *firewall rule* yang dibuat. Pada kotak dialog **Comment for New NAT Rule** yang tampil, masukkan "**Sharing koneksi Internet**", seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan pengaturan **Comment**.

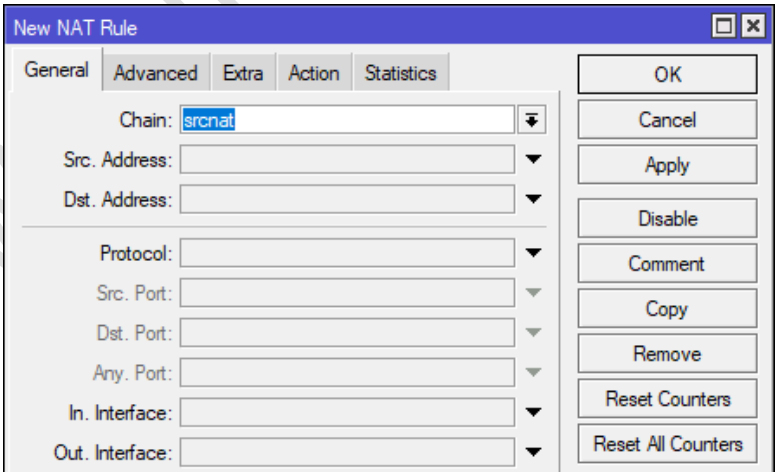
Klik tombol **OK** untuk menyimpan.

Hasil dari pengaturan NAT tersebut akan terlihat seperti pada gambar berikut:



19. Mengatur **Destination Network Address Translation (DNAT)** untuk melakukan **transparent proxy** bagi *client* baik **LAN** maupun **WLAN** sehingga menggunakan *web proxy* yang telah dibuat menggunakan **IP Firewall NAT**.

    a) Membuat **NAT rule** untuk mengatur *transparent proxy* bagi **client LAN** dengan memilih tombol  pada *toolbar* dari kotak dialog **Firewall tab NAT**. Selanjutnya akan tampil kotak dialog **NAT Rule**, seperti terlihat pada gambar berikut:

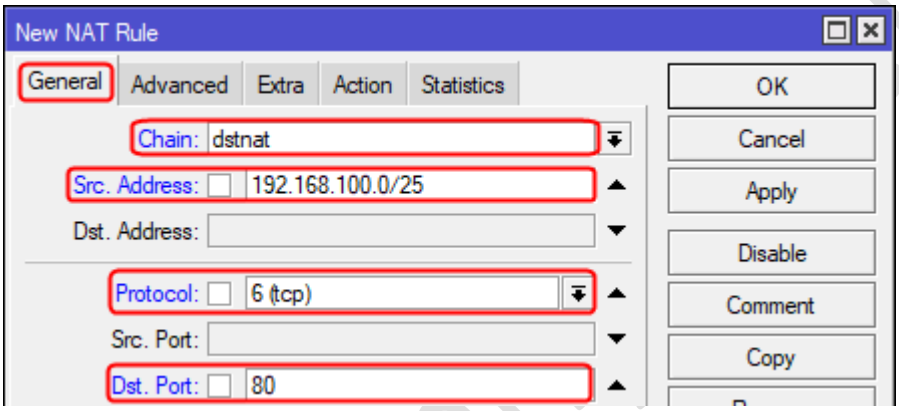


Pada kotak dialog **New NAT Rule** tab **General** yang tampil, terdapat beberapa parameter yang diatur yaitu:

- **Chain**, digunakan untuk menentukan jenis *chain* yang dibuat *rule*nya yaitu **dstnat** untuk mentranslasi alamat IP tujuan.

- **Src. Address** digunakan untuk menentukan alamat IP sumber yaitu **192.168.100.0/25** untuk **LAN.**
- **Protocol**, digunakan untuk menentukan protocol *transport* yang digunakan yaitu **6 (tcp)**.
- **Dst Port**, digunakan untuk menentukan nomor port tujuan yaitu **80**.

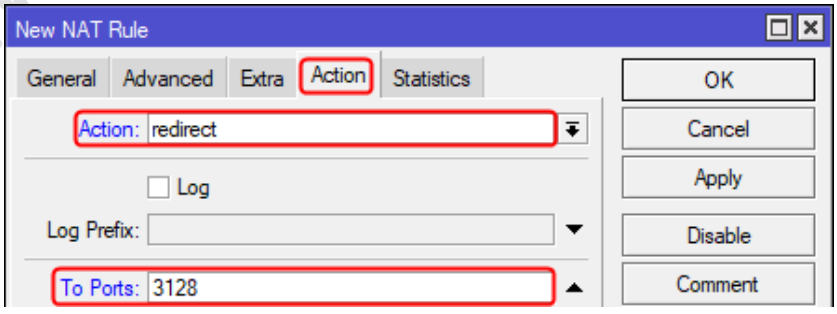
Hasil dari pengaturan pada tab *General* akan terlihat seperti pada gambar berikut:



Selanjutnya pindah ke tab **Action**. Pada tab **Action** terdapat beberapa parameter yang diatur yaitu:

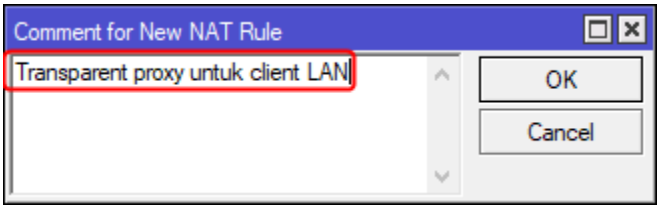
- **Action**, digunakan untuk menentukan aksi yang akan dilakukan jika paket cocok dengan aturan yaitu **redirect**.
- **To Ports**, digunakan untuk menentukan nomor port sebagai pengganti dari nomor port tujuan asal yaitu **3128**.

Hasil dari pengaturan pada tab **Action** akan terlihat seperti pada gambar berikut:

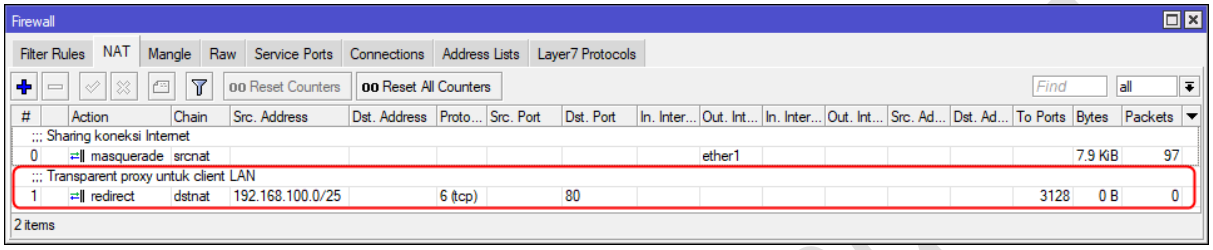


Selanjutnya klik tombol **Comment** untuk menambahkan deskripsi terkait *firewall rule* yang dibuat. Pada kotak dialog **Comment for New NAT Rule** yang tampil,

masukkan "**Transparent proxy untuk client LAN**", seperti terlihat pada gambar berikut:



Hasil dari pengaturan **DSTNAT** tersebut akan terlihat seperti pada gambar berikut:



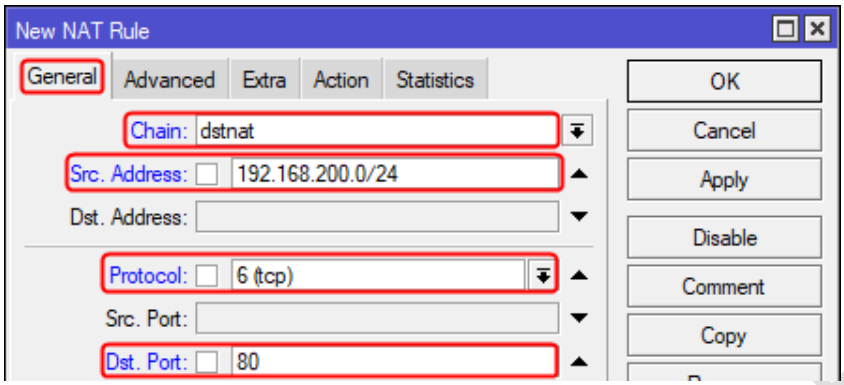
Untuk menampilkan kolom **To Ports** dapat dilakukan dengan cara klik kanan pada tanda ▼ dan pilih **Show Columns** serta pilih nama kolom yang ingin ditampilkan yaitu **To Ports.**

b) Membuat **NAT rule** untuk mengatur *transparent proxy* bagi **client WLAN** dengan memilih tombol ✚ pada *toolbar* dari kotak dialog **Firewall tab NAT**.

Pada kotak dialog **New NAT Rule** tab **General** yang tampil, terdapat beberapa parameter yang diatur yaitu:

- **Chain**, digunakan untuk menentukan jenis *chain* yang dibuat *rule*nya yaitu **dstnat** untuk mentranslasi alamat IP tujuan.
- **Src. Address** digunakan untuk menentukan alamat IP sumber yaitu **192.168.200.0/24** untuk **LAN.**
- **Protocol**, digunakan untuk menentukan protocol *transport* yang digunakan yaitu **6 (tcp)**.
- **Dst Port**, digunakan untuk menentukan nomor port tujuan yaitu **80**.

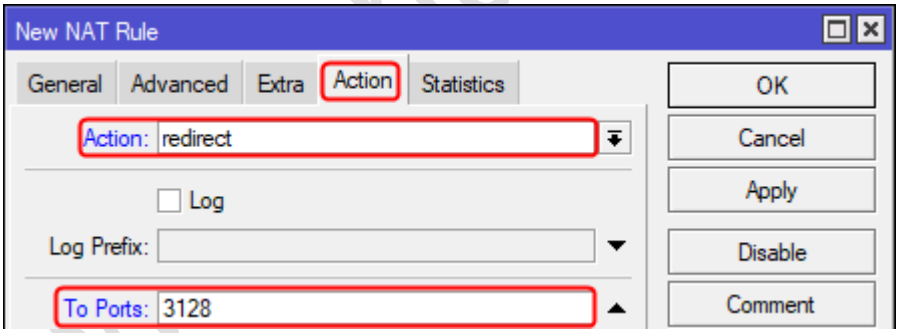
Hasil dari pengaturan pada tab *General* akan terlihat seperti pada gambar berikut:



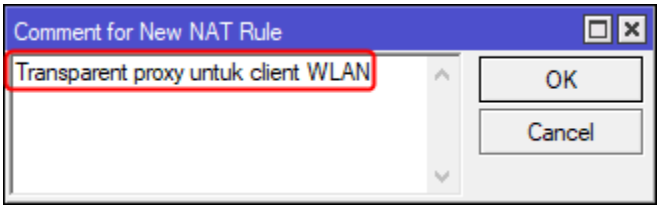
Selanjutnya pindah ke tab **Action**. Pada tab **Action** terdapat beberapa parameter yang diatur yaitu:

- **Action**, digunakan untuk menentukan aksi yang akan dilakukan jika paket cocok dengan aturan yaitu **redirect**.
- **To Ports**, digunakan untuk menentukan nomor port sebagai pengganti dari nomor port tujuan asal yaitu **3128**.

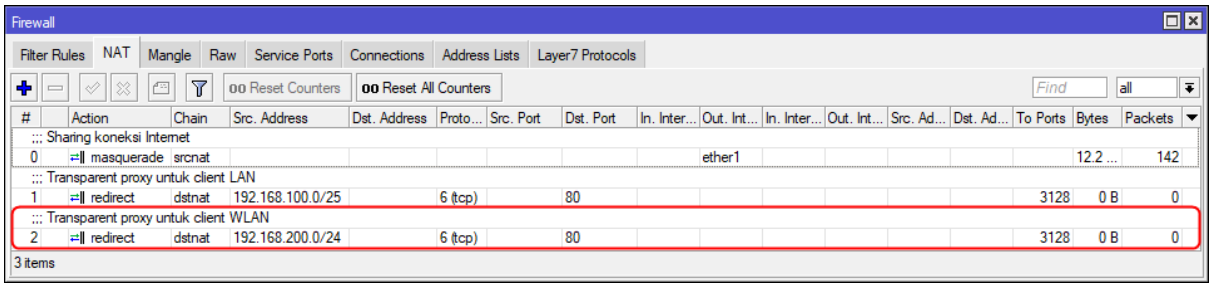
Hasil dari pengaturan pada tab **Action** akan terlihat seperti pada gambar berikut:



Selanjutnya klik tombol **Comment** untuk menambahkan deskripsi terkait *firewall rule* yang dibuat. Pada kotak dialog **Comment for New NAT Rule** yang tampil, masukkan "**Transparent proxy untuk client WLAN**", seperti terlihat pada gambar berikut:



Hasil dari pengaturan **DSTNAT** tersebut akan terlihat seperti pada gambar berikut:



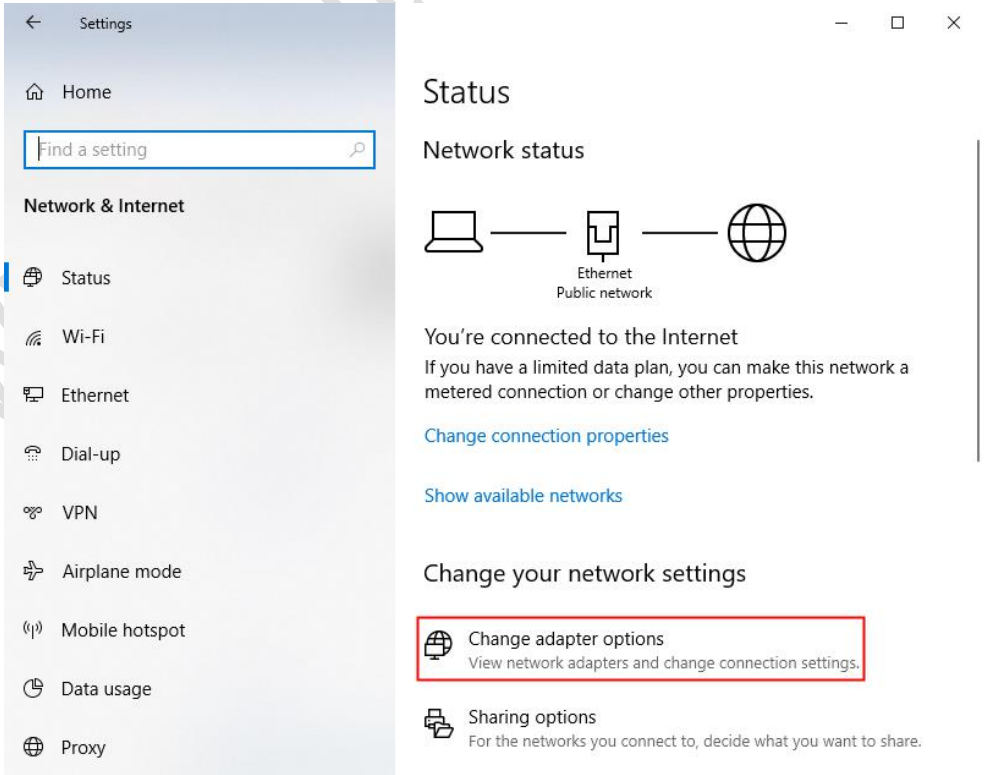
Tutup kotak dialog **Firewall**.

D. KONFIGURASI KOMPUTER CLIENT LAN WINDOWS 10 SEBAGAI DHCP CLIENT

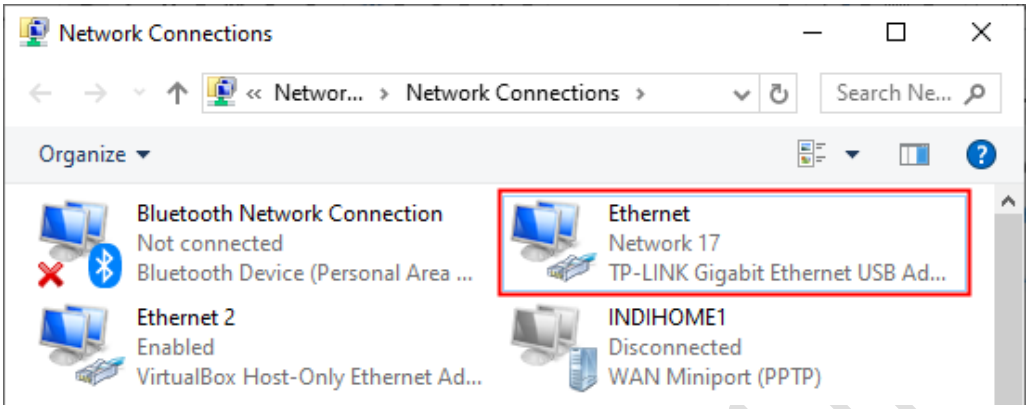
Adapun langkah-langkah konfigurasi yang dilakukan pada computer *client* LAN dengan sistem operasi **Windows 10** adalah sebagai berikut:

1. Mengatur pengalamatan IP dan parameter TCP/IP lainnya melalui **taskbar bagian pojok kanan bawah** dengan cara **klik kanan** pada icon **Connections are available** dan pilih **Open Network & Internet settings**, seperti terlihat pada gambar berikut:

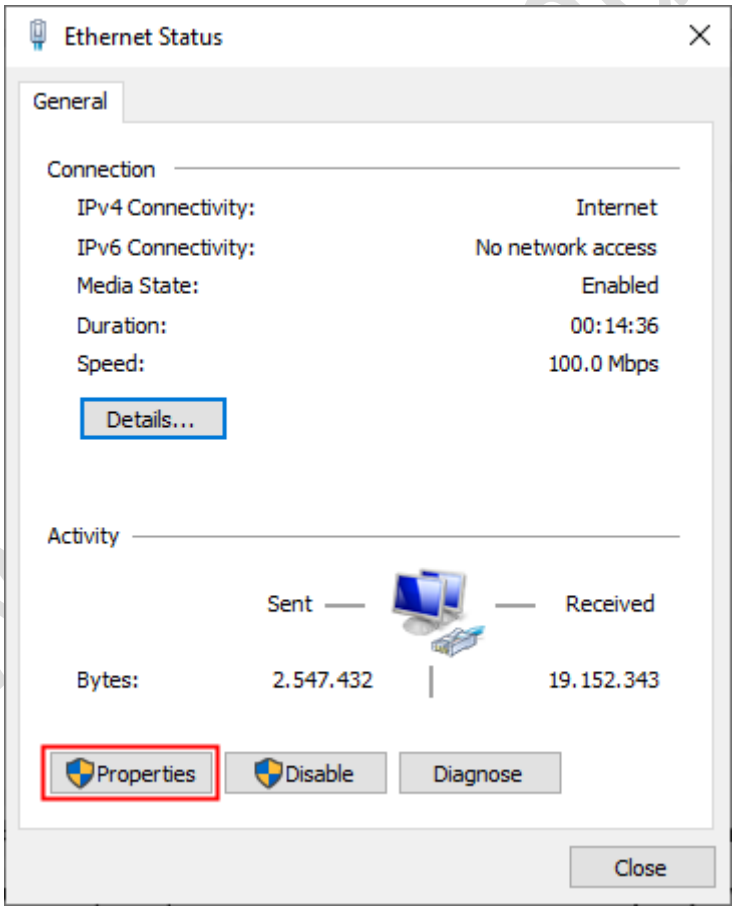
2. Tampil kotak dialog **Settings**. Klik pada **Change adapter options**, seperti terlihat pada gambar berikut:



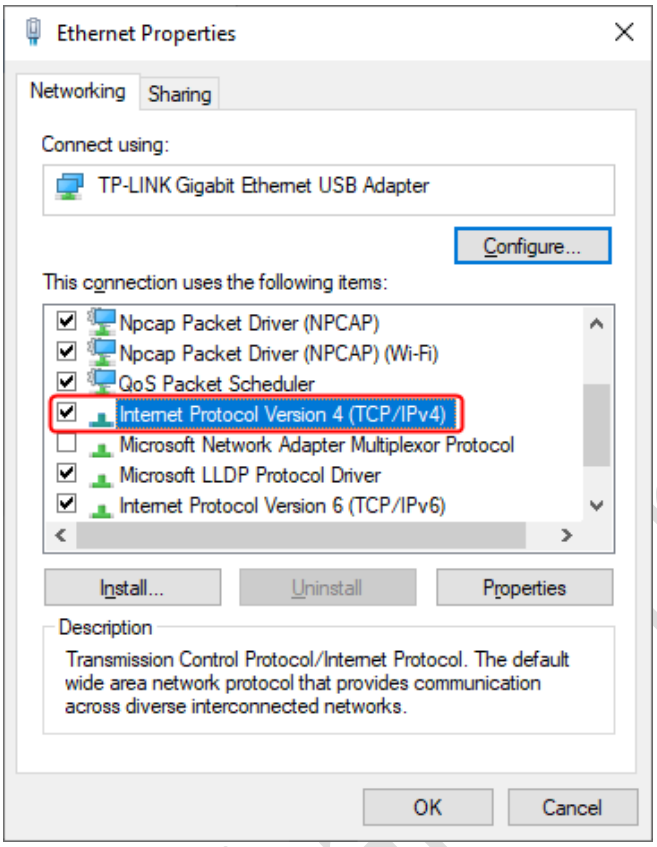
3. Tampil kotak dialog **Network Connections**. Klik pada *adapter* **Ethernet**, seperti terlihat pada gambar berikut:



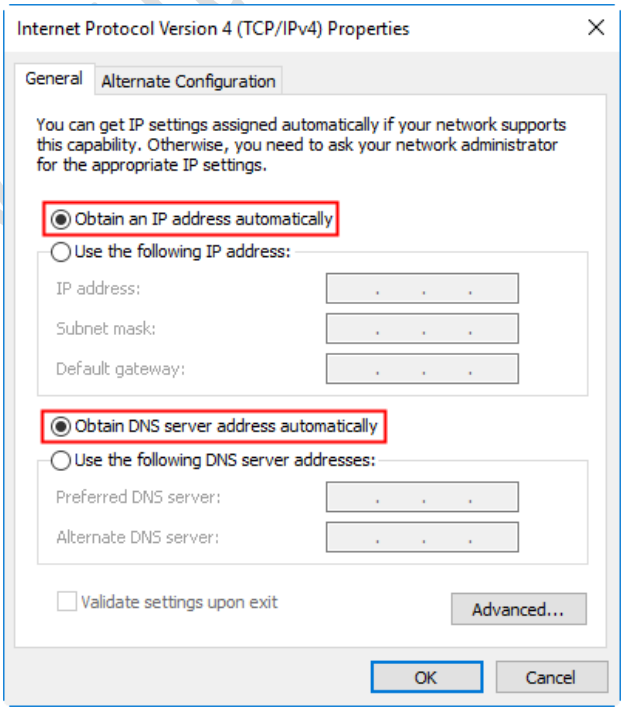
4. Tampil kotak dialog **Ethernet Status**. Klik tombol **Properties**, seperti terlihat pada gambar berikut:



5. Tampil kotak dialog **Ethernet Properties**. Pada bagian "**This connection uses the following items:**", klik dua kali pada pilihan **Internet Protocol Version 4 (TCP/IPv4)**, seperti terlihat pada gambar berikut:

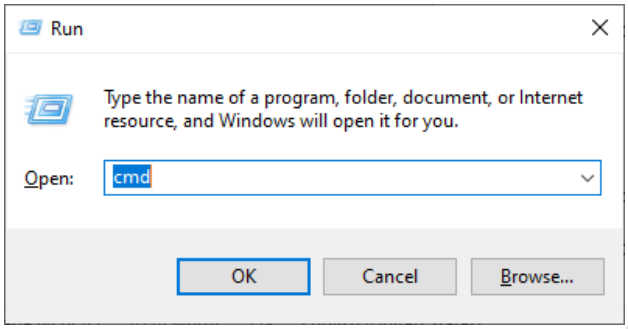


6. Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties**. Pilih *Obtain an IP address automatically* dan *Obtain DNS server address automatically*, seperti terlihat pada gambar berikut:

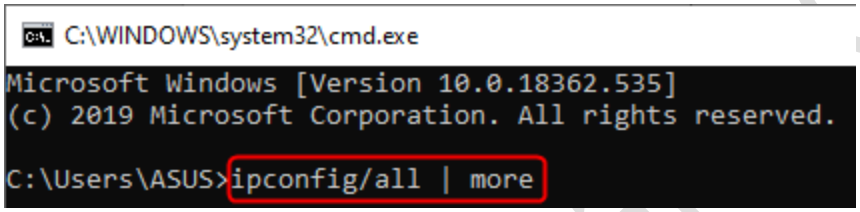


Klik tombol **OK > OK > Close**. Tutup kotak dialog **Network connections**.

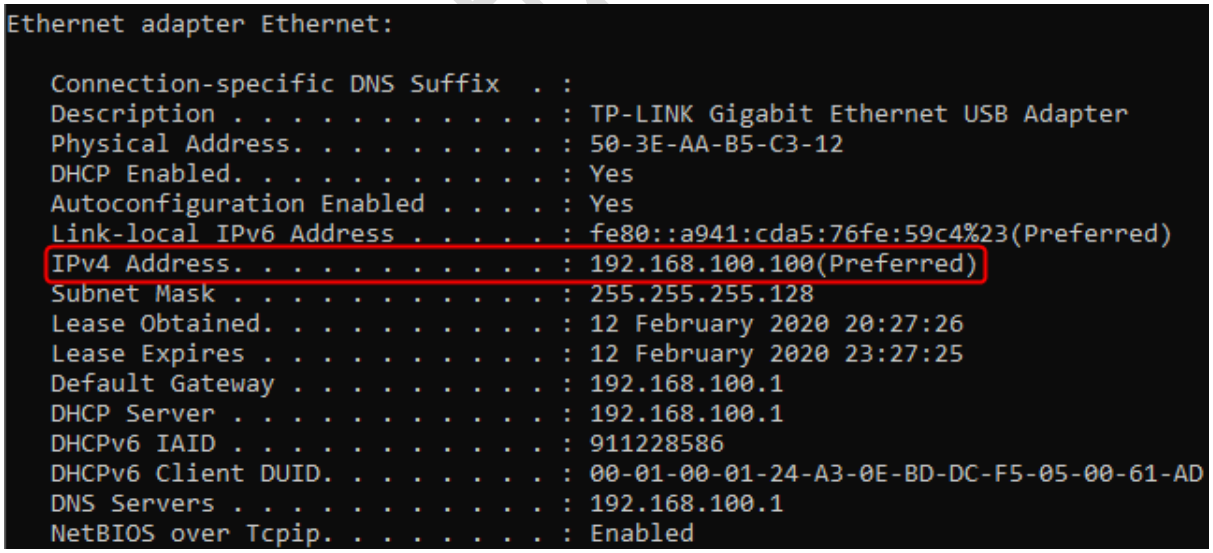
7. Buka **Command Prompt Windows** dengan menekan tombol **Windows+R**. Pada inputan parameter **Open:** dari kotak dialog **Run** yang tampil, ketik"**cmd**" dan tekan tombol **Enter**, seperti terlihat pada gambar berikut:



8. Pada **Command Prompt** masukkan perintah "**ipconfig/all | more**" untuk memverifikasi pengalamatan IP yang telah diatur, seperti terlihat pada gambar berikut:

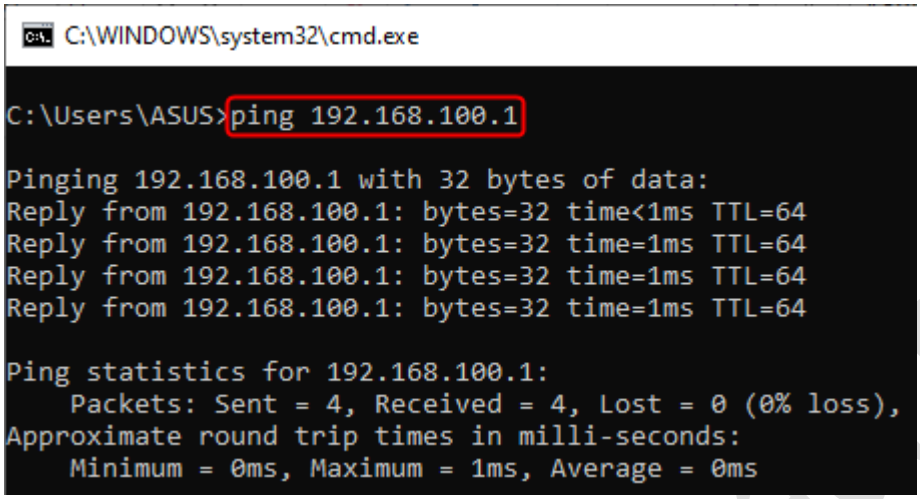


Pastikan adapter **Ethernet** telah mendapatkan pengalamatan IP dari **DHCP Server**, seperti terlihat pada gambar berikut:



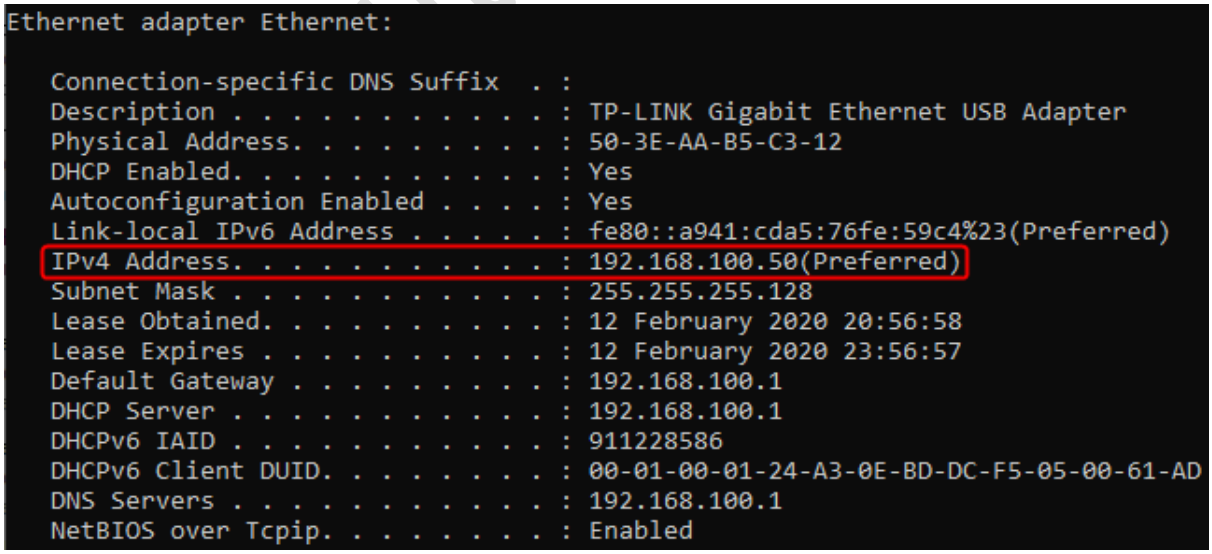
Terlihat alamat IP yang diperoleh dari **DHCP Server** untuk **Ethernet adapter Local Area Connection** adalah **192.168.100.100**. Tekan tombol **spasi** untuk menampilkan layar berikutnya. Tekan tombol **q** untuk keluar.

9. Verifikasi koneksi dari *client LAN* ke *interface ether2 dari Router Mikrotik* menggunakan perintah "**ping 192.168.100.1"** pada **Command Prompt Windows**, seperti terlihat pada gambar berikut:

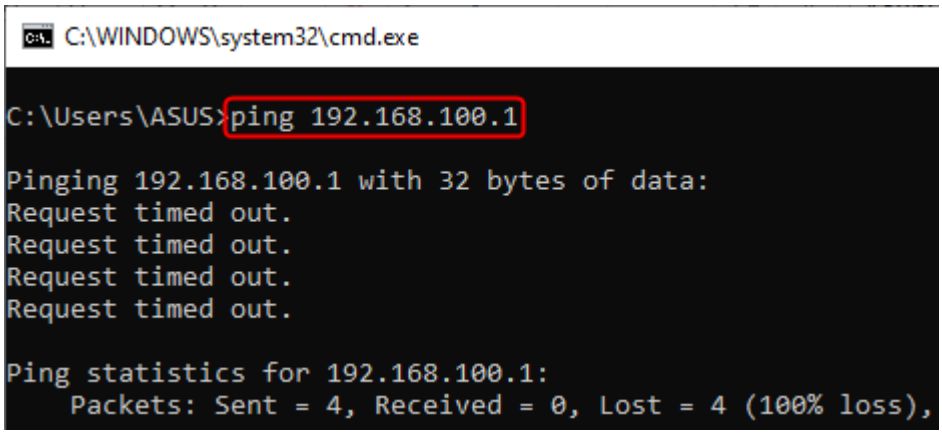


Terlihat verifikasi koneksi ke *router Mikrotik* **sukses** dilakukan karena alamat IP **192.168.100.100** yang digunakan oleh **client LAN berada diluar rentang alamat IP 192.168.100.2-192.168.100.50 yang diblokir akses ping-nya** di *router Mikrotik.*

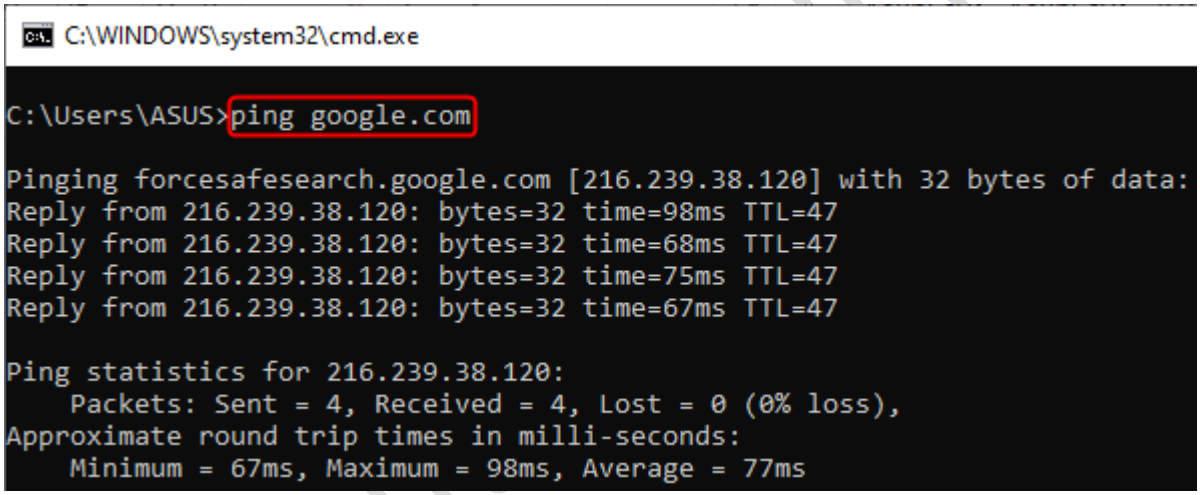
Sebaliknya apabila alamat IP yang digunakan oleh **client LAN termasuk ke dalam rentang alamat IP yang ditolak atau diblokir akses ping-nya di router Mikrotik yaitu 192.168.100.2-192.168.100.50**, seperti terlihat pada gambar berikut:



Maka verifikasi koneksi ke *router Mikrotik* menggunakan **ping** akan **gagal dilakukan**, seperti terlihat pada gambar berikut:



10. Verifikasi koneksi ke Internet menggunakan perintah **ping** ke salah satu situs di Internet, sebagai contoh **google.com**, seperti terlihat pada gambar berikut:



Terlihat verifikasi koneksi ke **google.com** berhasil dilakukan.

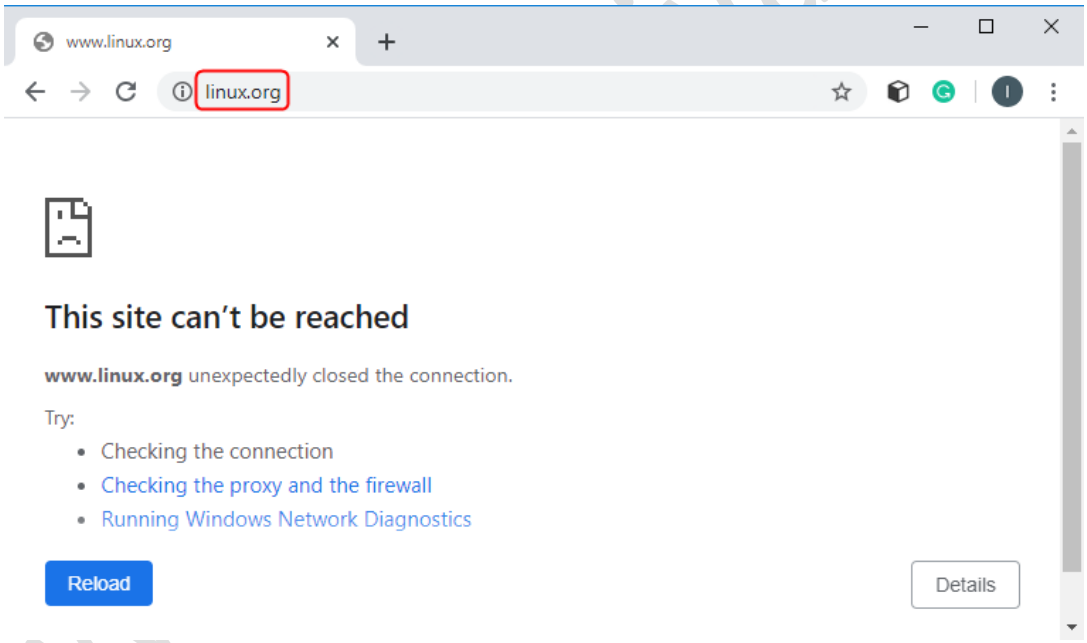
E. UJICOBA KONEKSI INTERNET DARI CLIENT LAN WINDOWS 10

Adapun langkah-langkah verifikasi ujicoba koneksi Internet dari client LAN dengan sistem operasi *Windows 10* adalah sebagai berikut:

1. Buka salah satu *browser* yang terinstalasi di computer, sebagai contoh *browser* **Chrome**.
2. Pada *address bar* dari browser **Chrome**, masukkan alamat situs yang ingin diakses sebagai contoh **https://www.iputuhariyadi.net**. Hasil ujicoba pengaksesan situs tersebut, terlihat seperti pada gambar berikut:

Terlihat **Client LAN** dapat mengakses situs tersebut.

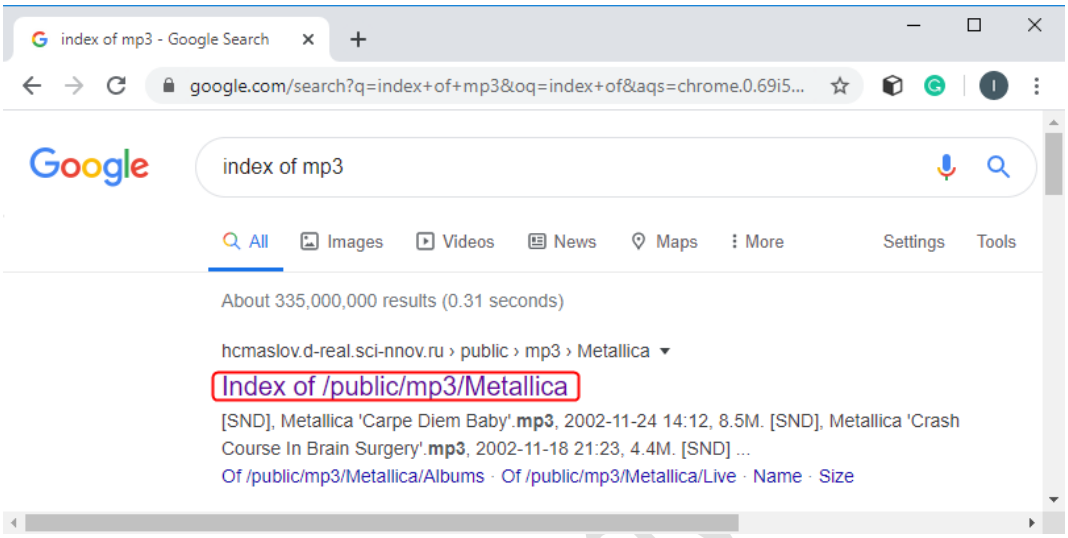
3. Mengakses situs yang telah diatur untuk **diblokir** yaitu https://www.linux.org. Hasil ujicoba pengaksesan situs tersebut, seperti terlihat pada gambar berikut:



Terlihat **Client LAN** tidak dapat mengakses situs tersebut dimana ditandai dengan pesan "**This site can't be reached**". Hal ini menunjukkan bahwa pemblokiran terhadap situs tersebut berhasil dilakukan.

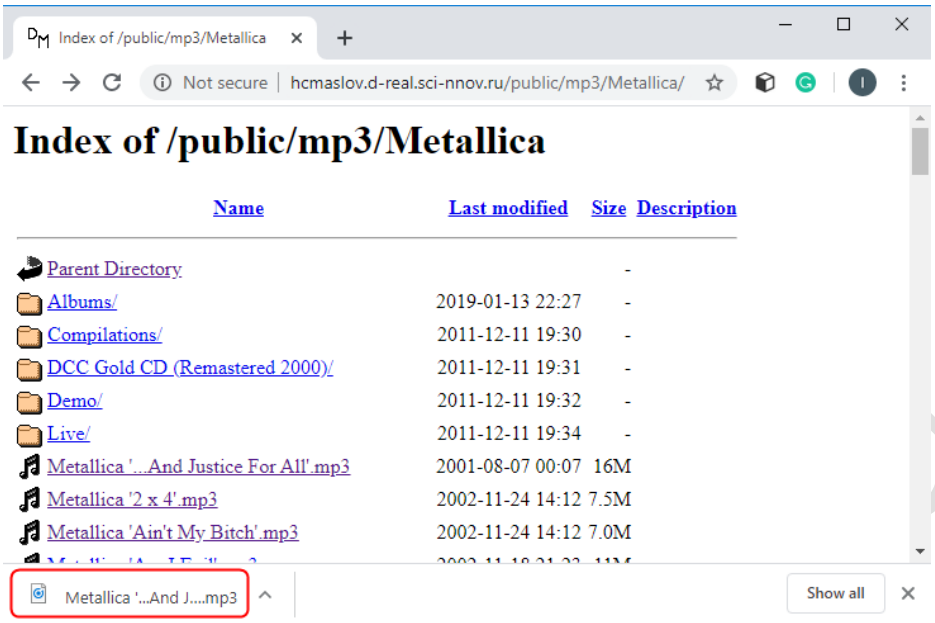
4. Mengakses *file* dengan ekstensi **.mp3** dari salah satu situs di *Internet* yang telah diatur untuk **diblokir** ketika **rule transparent proxy untuk client LAN dan WLAN** pada fitur **IP Firewall NAT** dari *router Mikrotik* masih **diaktifkan**.

Pada *address bar* dari *browser* **Chrome**, masukkan kata kunci "**index of mp3**" dan tekan **Enter** maka akan terlihat hasil dari pencarian dengan kata kunci tersebut. Akses salah satu situs sebagai hasil dari pencarian tersebut, sebagai contoh http://hcmaslov.d-real.sci-nnov.ru/public/mp3/Metallica/, seperti terlihat pada gambar berikut:



Maka akan tampil konten pada situs tersebut yang memuat *file-file* dengan ekstensi **.mp3.** Lakukan percobaan mengunduh salah satu *file* **mp3** tersebut, sebagai contoh "**Metallica%20'...And%20Justice%20For%20All'.mp3**", seperti terlihat pada gambar berikut:

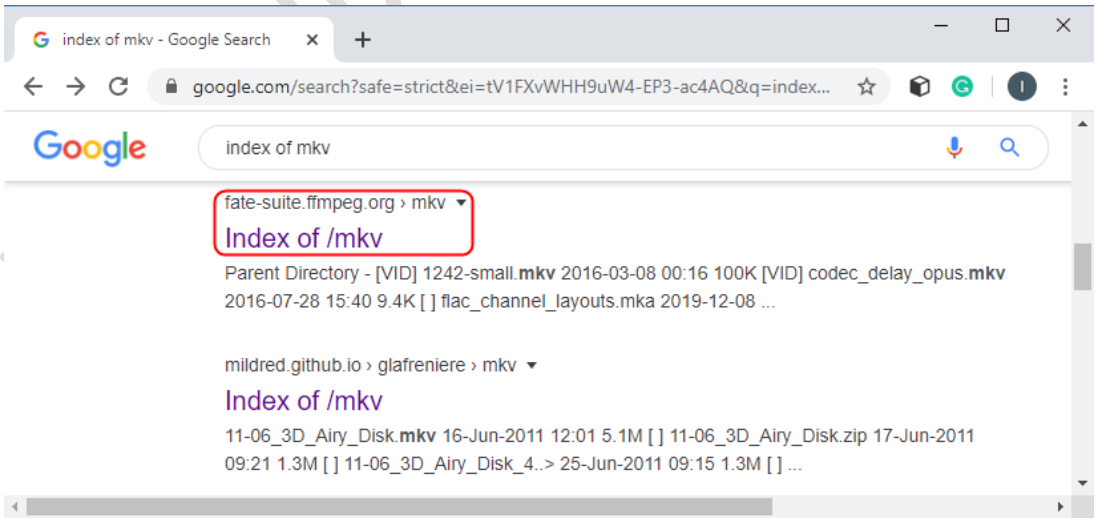
File **.mp3** tersebut masih tetap berhasil diunduh atau tidak terblokir, seperti terlihat pada gambar berikut:



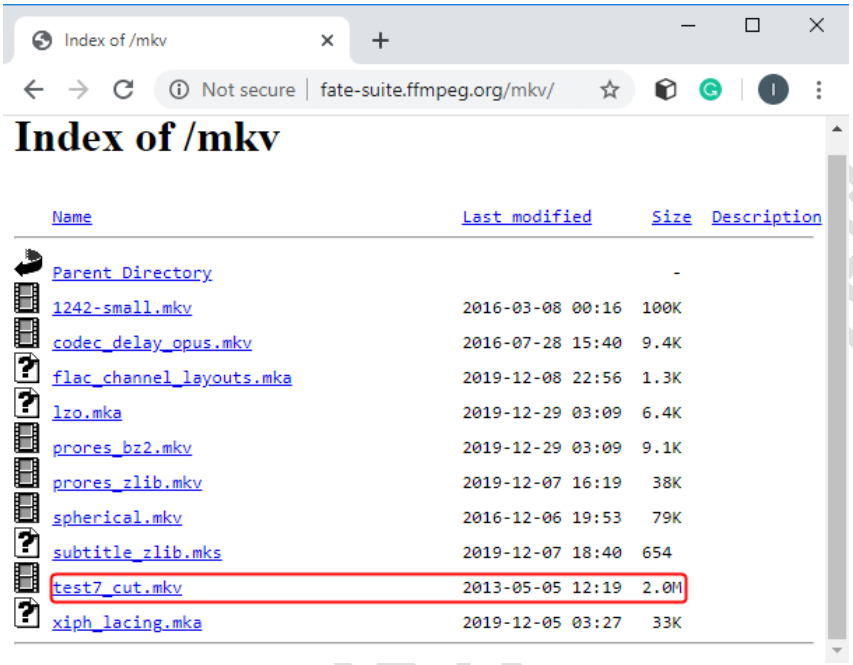
Hal ini sebagai dampak dari pemanfaatan *web proxy* secara *transparent*.

5. Mengakses file dengan ekstensi **.mkv** dari salah satu situs di *Internet* yang telah diatur untuk **diblokir** ketika **transparent proxy untuk client LAN dan WLAN** pada *router Mikrotik* masih **diaktifkan**.

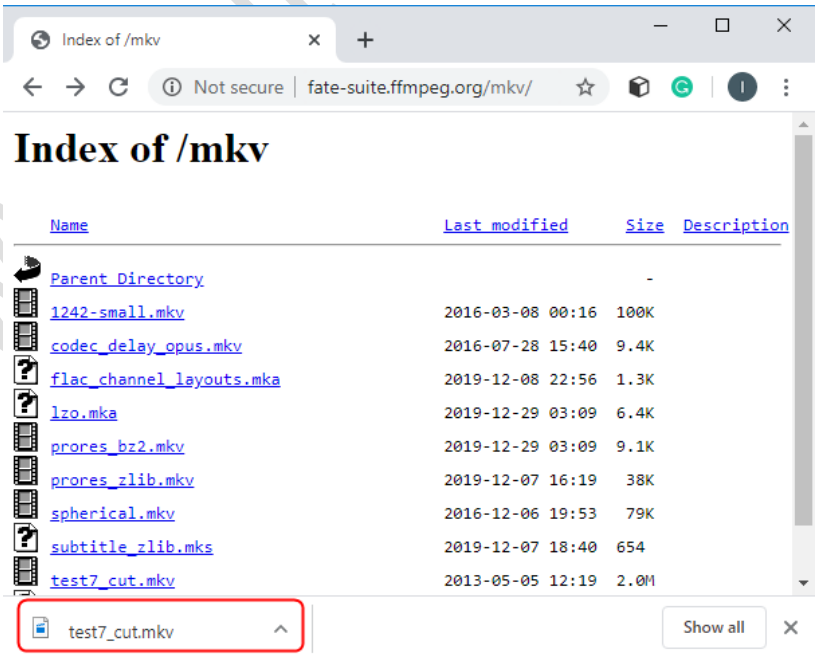
   Pada *address bar* dari *browser* **Chrome**, masukkan kata kunci "**index of mkv**" dan tekan **Enter** maka akan terlihat hasil dari pencarian dengan kata kunci tersebut. Akses salah satu situs sebagai hasil dari pencarian tersebut, sebagai contoh http://fate-suite.ffmpeg.org/mkv/, seperti terlihat pada gambar berikut:



Maka akan tampil konten pada situs tersebut yang memuat *file-file* dengan ekstensi **.mkv**. Lakukan percobaan mengunduh salah satu *file* **mkv** tersebut, sebagai contoh "**test7_cut.mkv**", seperti terlihat pada gambar berikut:



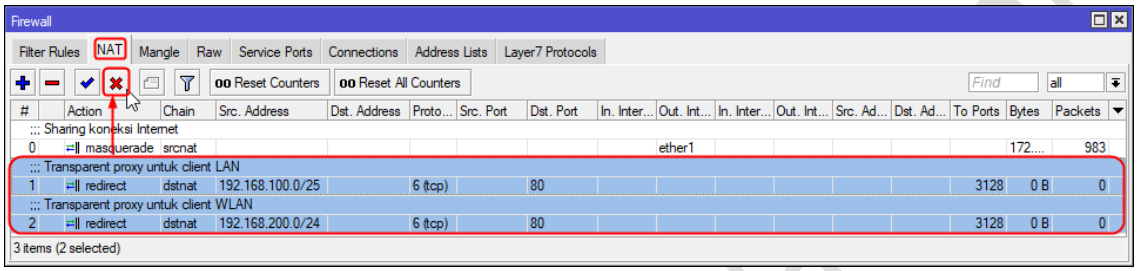
File **.mkv** tersebut masih tetap berhasil diunduh atau tidak terblokir, seperti terlihat pada gambar berikut:



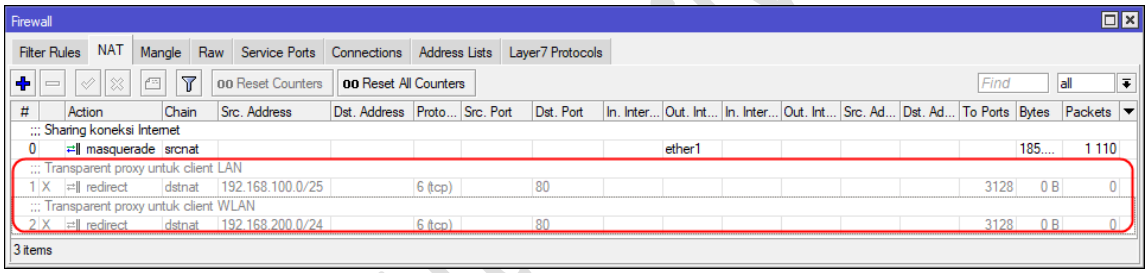
Hal ini sebagai dampak dari pemanfaatan *web proxy* secara *transparent*.

6. Mengakses *file* dengan ekstensi **.mp3** dari salah satu situs di *Internet* yang telah diatur untuk **diblokir** ketika **rule transparent proxy untuk client LAN dan WLAN** pada fitur **IP Firewall NAT** dari *router Mikrotik* **dinonaktifkan**.

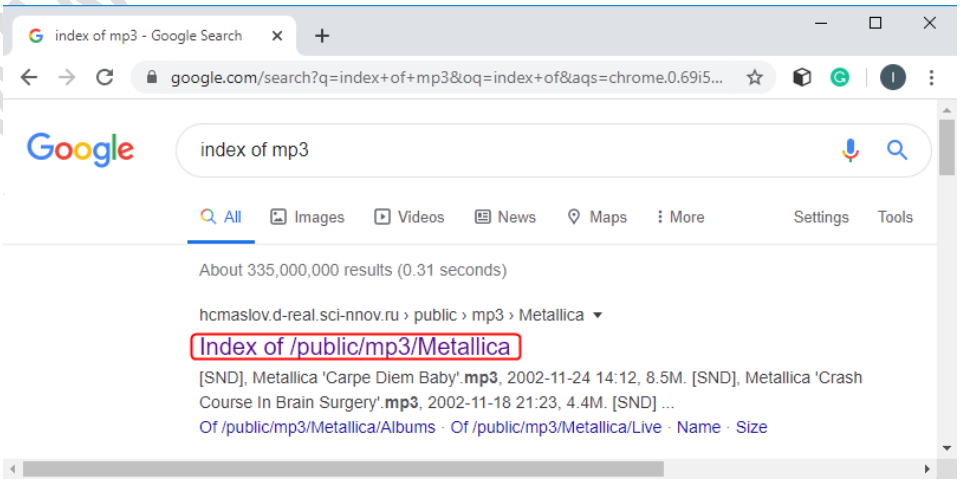
   Pada panel sebelah kiri dari *Winbox*, pilih menu **IP > Firewall** maka akan tampil kotak dialog **Firewall**. Pilih tab **NAT** pada kotak dialog **Firewall** yang tampil dan lakukan seleksi 2 (dua) *NAT rule* terkait *transparent proxy* dan klik tombol  untuk menonaktifkan (**Disable**) kedua *rule* tersebut, seperti terlihat pada gambar berikut:



   Hasil dari penonaktifkan rule tersebut, seperti terlihat pada gambar berikut:

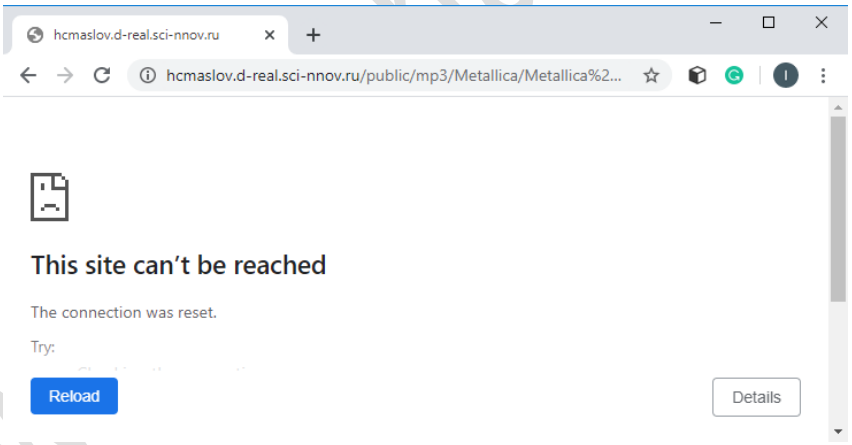


   Selanjutnya pada *address bar* dari *browser* **Chrome**, masukkan kata kunci "**index of mp3**" dan tekan **Enter** maka akan terlihat hasil dari pencarian dengan kata kunci tersebut. Akses salah satu situs sebagai hasil dari pencarian tersebut, sebagai contoh http://hcmaslov.d-real.sci-nnov.ru/public/mp3/Metallica/, seperti terlihat pada gambar berikut:



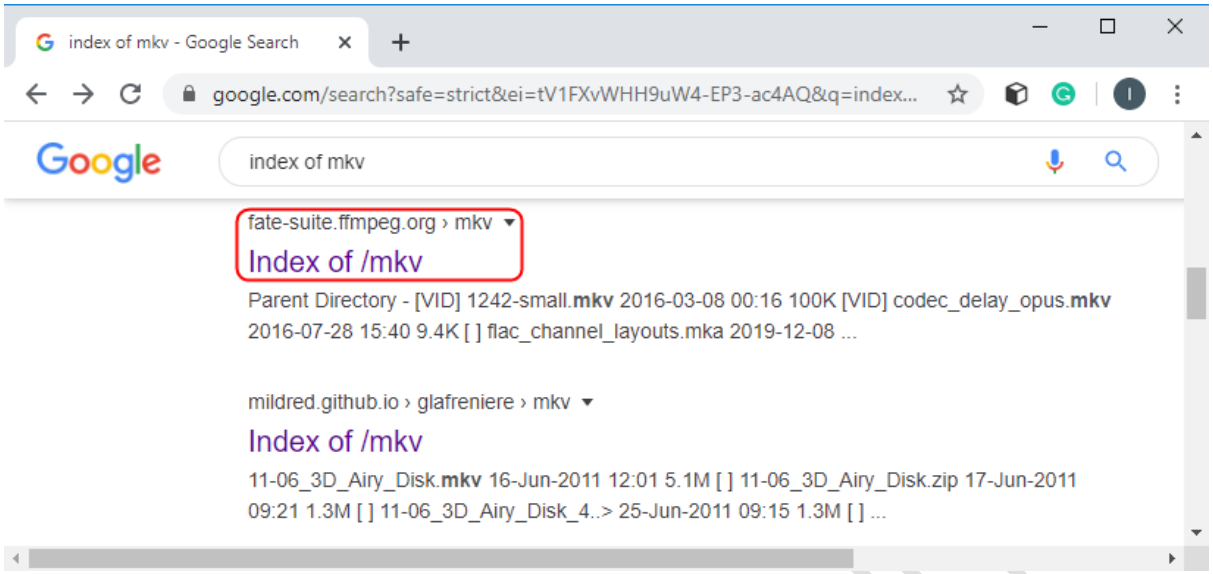
Maka akan tampil konten pada situs tersebut yang memuat *file-file* dengan ekstensi **.mp3.** Lakukan percobaan mengunduh salah satu *file* **mp3** tersebut, sebagai contoh "**Metallica%20'...And%20Justice%20For%20All'.mp3**", seperti terlihat pada gambar berikut:

Tunggu beberapa saat hingga terlihat pesan "**This site can't be reached**" yang menunjukkan bahwa **file .mp3** tidak dapat diunduh, seperti terlihat pada gambar berikut:

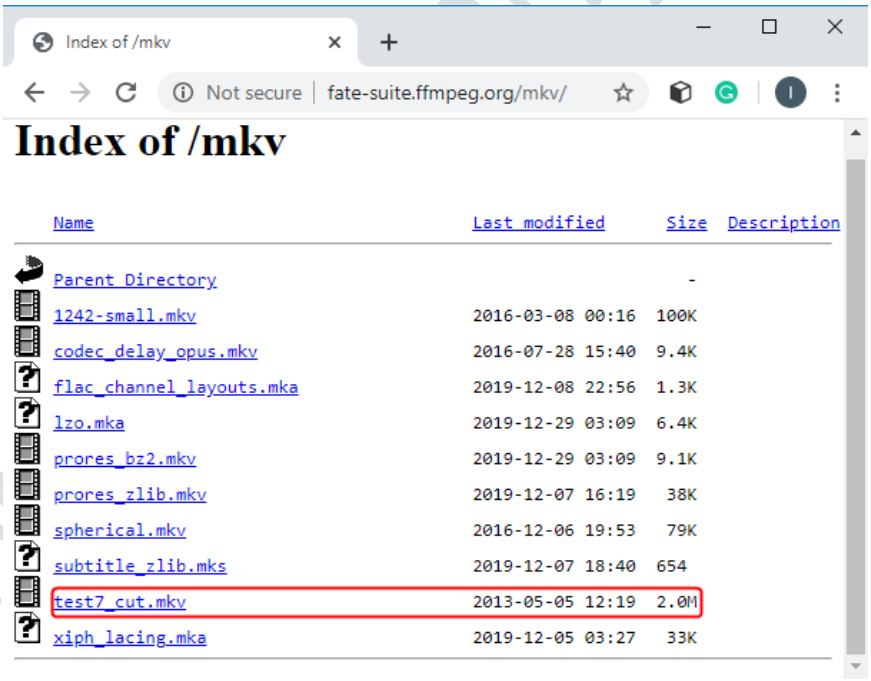


7. Mengakses file dengan ekstensi **.mkv** dari salah satu situs di *Internet* yang telah diatur untuk **diblokir** ketika **transparent proxy untuk client LAN dan WLAN** pada *router Mikrotik* **dinonaktifkan**.

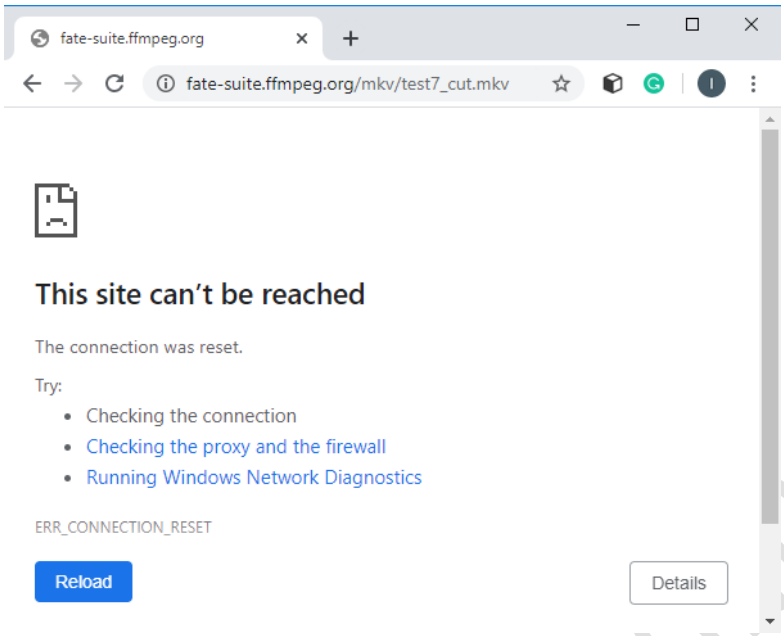
   Pada *address bar* dari *browser* **Chrome**, masukkan kata kunci "**index of mkv**" dan tekan **Enter** maka akan terlihat hasil dari pencarian dengan kata kunci tersebut. Akses salah satu situs sebagai hasil dari pencarian tersebut, sebagai contoh http://fate-suite.ffmpeg.org/mkv/, seperti terlihat pada gambar berikut:



Maka akan tampil konten pada situs tersebut yang memuat *file-file* dengan ekstensi **.mkv**. Lakukan percobaan mengunduh salah satu *file* **mkv** tersebut, sebagai contoh "**test7_cut.mkv**", seperti terlihat pada gambar berikut:



Tunggu beberapa saat hingga terlihat pesan "**This site can't be reached**" yang menunjukkan bahwa **file .mkv** tidak dapat diunduh, seperti terlihat pada gambar berikut:

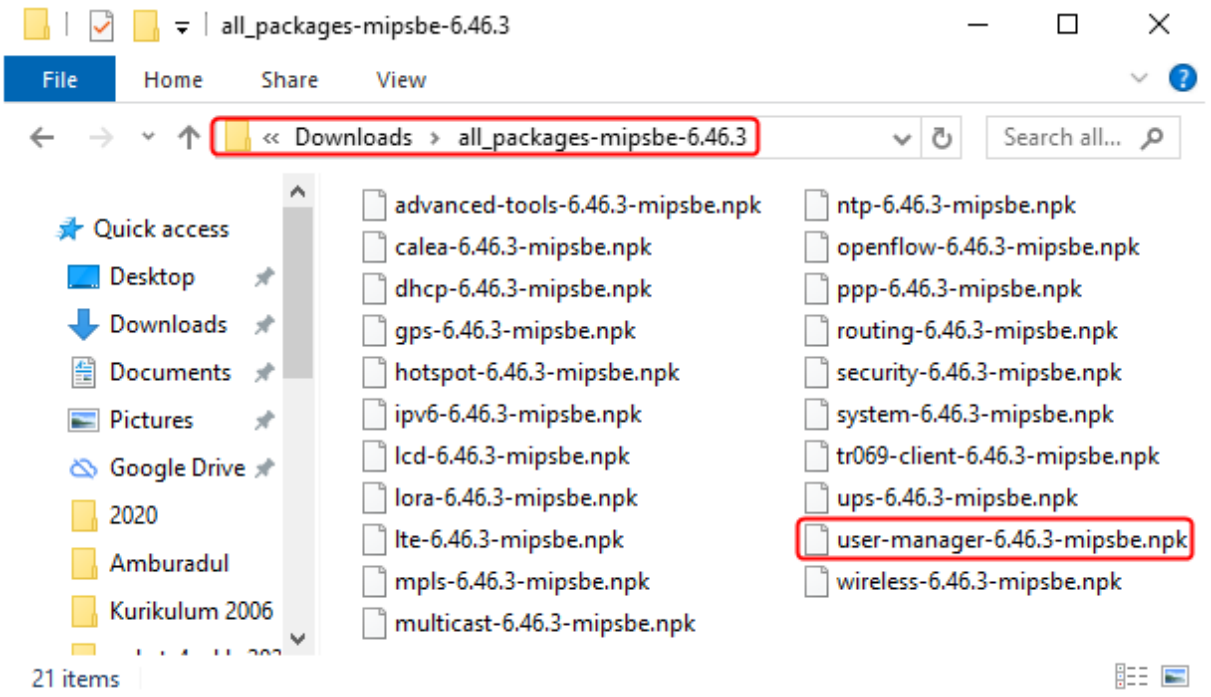


F. KONFIGURASI RADIUS DAN HOTSPOT PADA ROUTER MIKROTIK

Adapun langkah-langkah instalasi dan konfigurasi **RADIUS** serta **hotspot** pada *router Mikrotik* adalah sebagai berikut:

1. Menginstalasi dan konfigurasi **server RADIUS** menggunakan **User Manager** untuk **Hotspot**.
   a) Mengunduh *file* **Extra Packages**.
      Sebelum dapat menginstalasi paket *User Manager*, pastikan telah memiliki file **Extra Packages** yang didalamnya memuat paket **user-manager** sesuai dengan arsitektur prosesor atau tipe dari **Mikrotik Routerboard** dan versi **RouterOS** yang digunakan, sebagai contoh prosesor bertipe **MIPSBE** dengan versi **RouterOS 6.46.3**.
      Apabila belum memiliki, silakan mengunduh **file Extra Packages 6.46.3 (Stable)** dari situs *Mikrotik* pada alamat https://mikrotik.com/download, seperti terlihat pada gambar berikut:

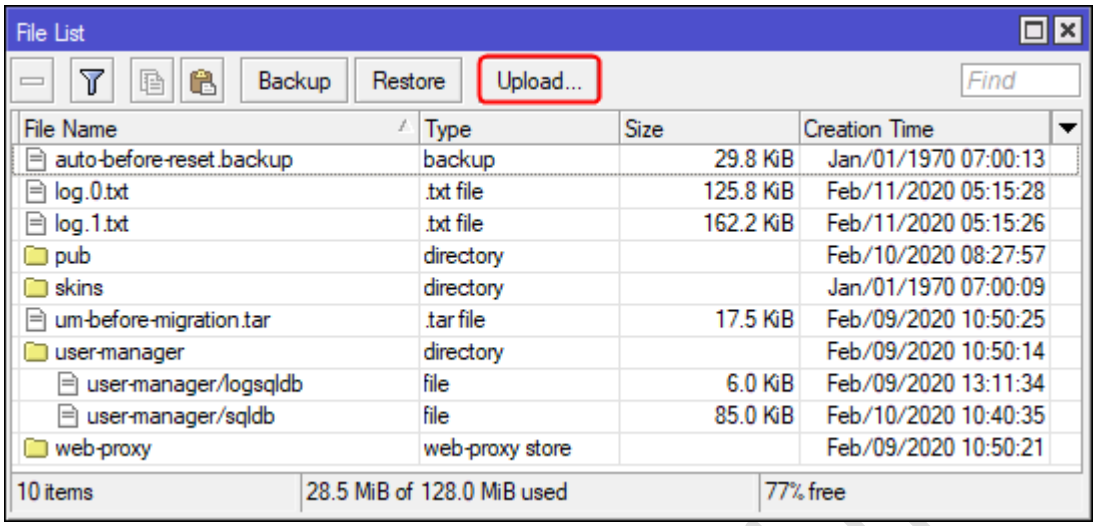
Diasumsikan *file Extra Packages* untuk tipe *MIPSBE RouterOS 6.46.3* telah berhasil diunduh dan tersimpan di *folder* **Downloads** dengan nama file **all_packages-mipsbe-6.46.3.zip**. Ekstrak *file Extra Packages* yang masih terkompresi tersebut, sehingga hasilnya terlihat seperti gambar berikut:



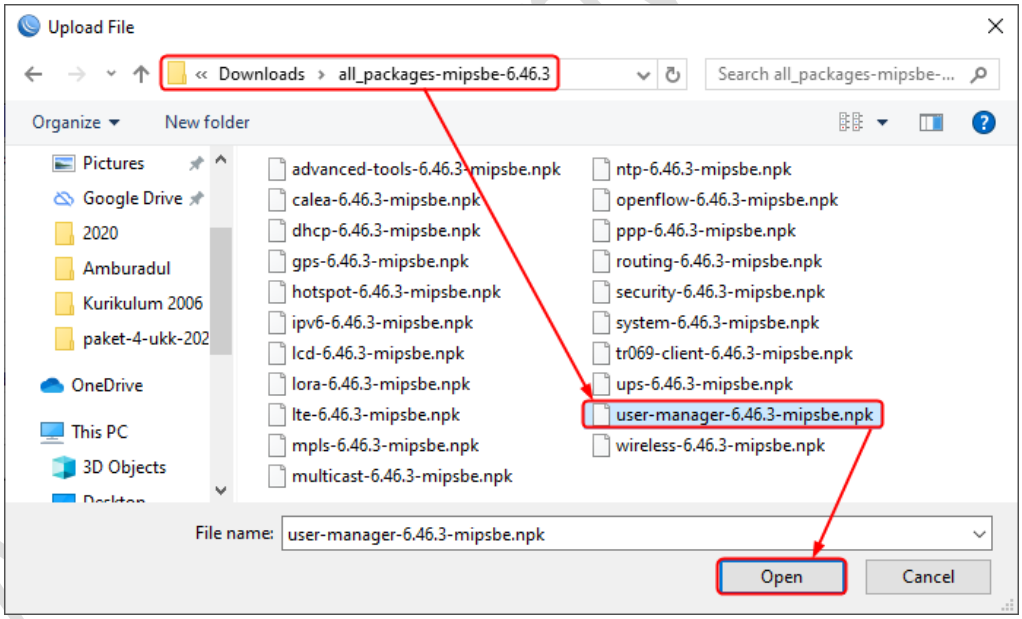
Terlihat didalam folder hasil ekstrak *file Extra Packages* terdapat file paket **user-manager-6.46.3-mipsbe.npk**.

b) Menginstalasi paket **User Manager**.

Mengunggah *file* **user-manager-6.46.3-mipsbe.npk** ke **Mikrotik Routerboard** dengan mengakses menu **Files** pada panel sebelah dari *Winbox* dan menekan tombol **Upload** pada kotak dialog **Files** yang tampil, seperti terlihat pada gambar berikut:

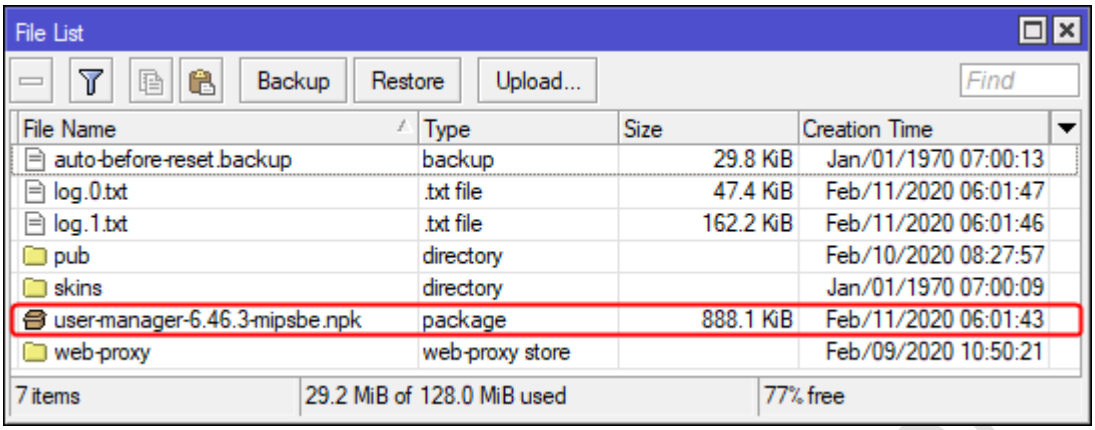


Tampil kotak dialog **Upload File**. Arahkan ke lokasi penyimpanan *file* **.npk** dari **user-manager** yaitu di *folder* **Downloads > all_packages-mipsbe-6.46.3** dan pilih pada *file* **user-manager-6.43.6-mipsbe.npk** serta tekan tombol **Open**, seperti terlihat pada gambar berikut:



Tunggu hingga proses unggah selesai dilakukan.

Hasil pengunggahan *file* **.npk** dari **user-manager** tersebut akan terlihat seperti pada gambar berikut:

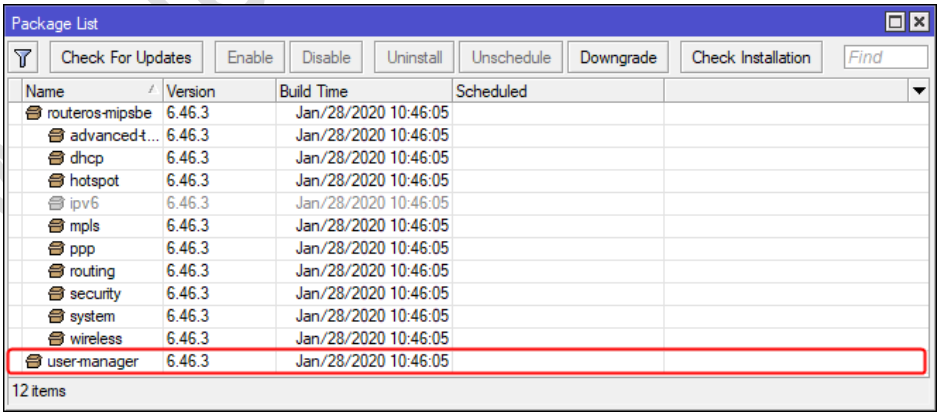


Tutup kotak dialog dari **Files**.

Selanjutnya dilakukan **reboot router Mikrotik** agar paket **user-manager-6.46.3-mipsbe.npk** yang telah diunggah dapat terinstall dengan memilih menu **System > Reboot** pada panel sebelah kiri dari *Winbox*. Tampil kotak dialog **Reboot** dengan pesan "**Do you want to reboot the router?**" yang mengkonfirmasi proses *reboot*. Tekan tombol **Yes** untuk melakukan reboot router.

Koneksi *Winbox* ke *router Mikrotik* akan terputus. Tunggu beberapa saat hingga proses *reboot* selesai dilakukan. **Silakan mengkoneksikan kembali Winbox ke router Mikrotik sehingga konfigurasi dapat dilanjutkan.**

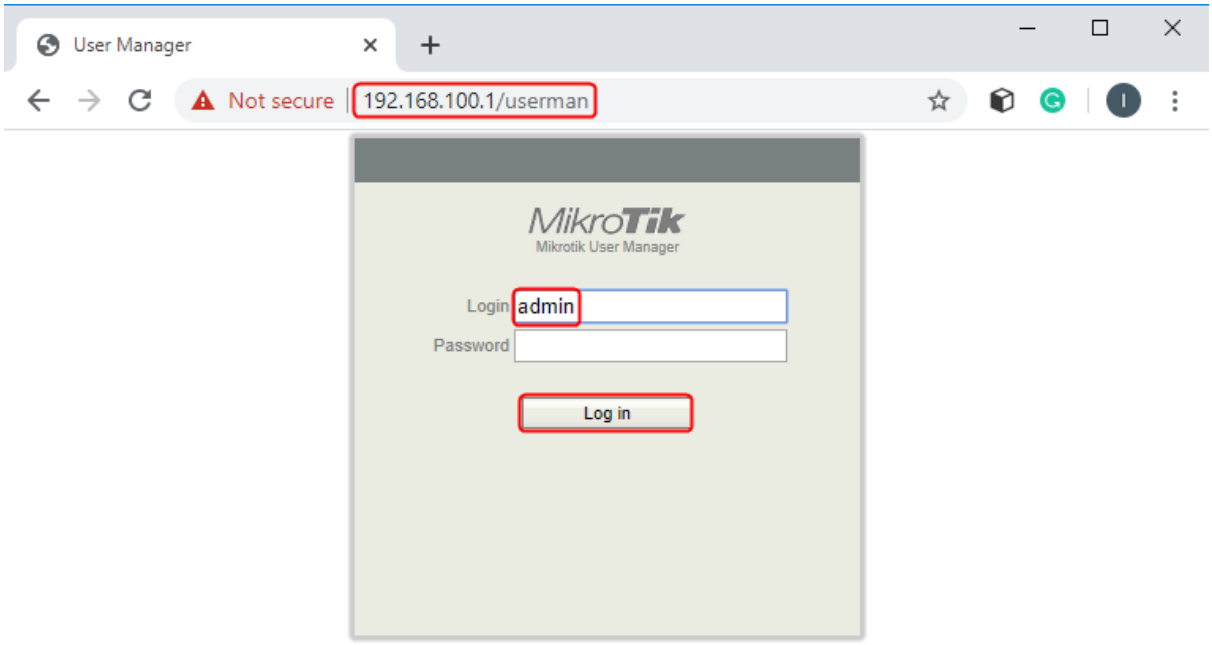
c) Memverifikasi hasil instalasi paket **user-manager** dengan mengakses menu **System > Packages** pada panel sebelah kiri dari *Winbox***.** Tampil kotak dialog **Package List**, seperti terlihat pada gambar berikut:



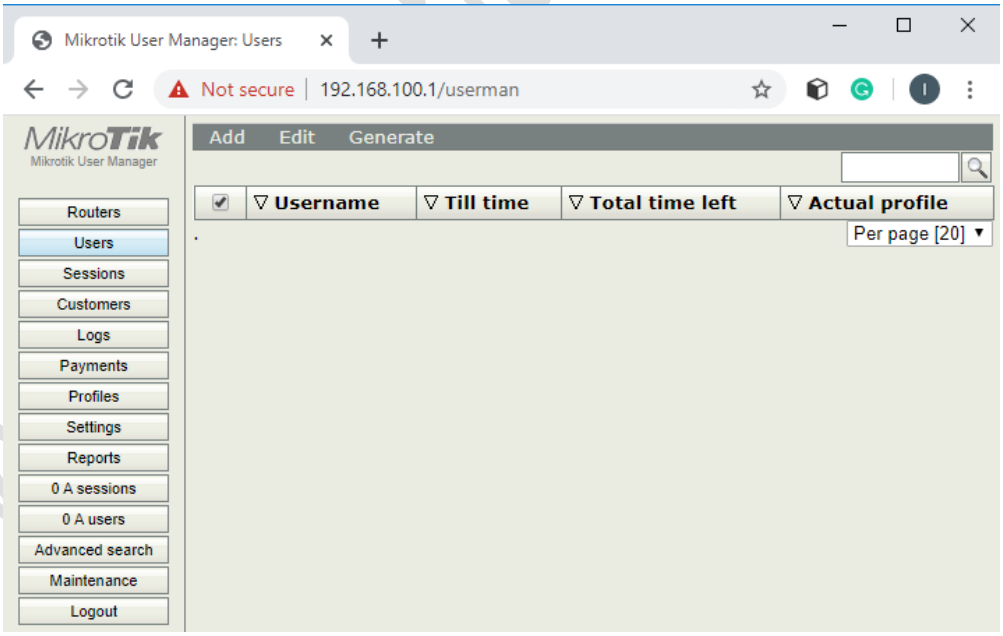
Terlihat paket **user-manager** telah berhasil terinstalasi.

Mengkonfigurasi **User Manager** dengan mengakses antarmuka berbasis *web* melalui *browser* pada alamat http://192.168.100.1/userman. Pada halaman *login* dari *user*

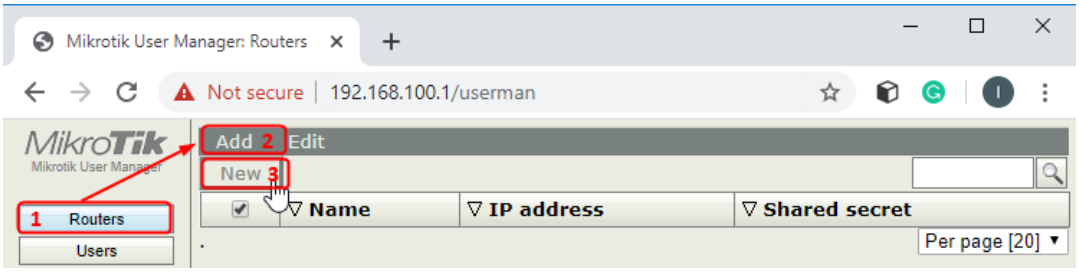
manager yang tampil, masukkan "**admin**" pada inputan **Login** dengan **password** kosong (tanpa sandi) dan tekan tombol **Log in**, seperti terlihat pada gambar berikut:



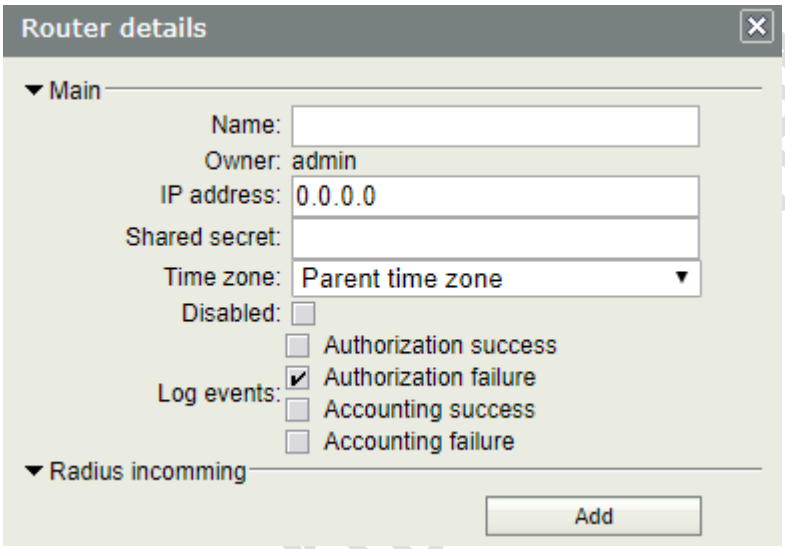
Apabila proses otentikasi berhasil dilakukan maka akan tampil halaman **Users**, seperti terlihat pada gambar berikut:



d) Menambahkan **router** yang bertindak sebagai **RADIUS Client** sehingga dapat mengakses **User Manager** dengan memilih menu **Routers > Add > New**, seperti terlihat pada gambar berikut:



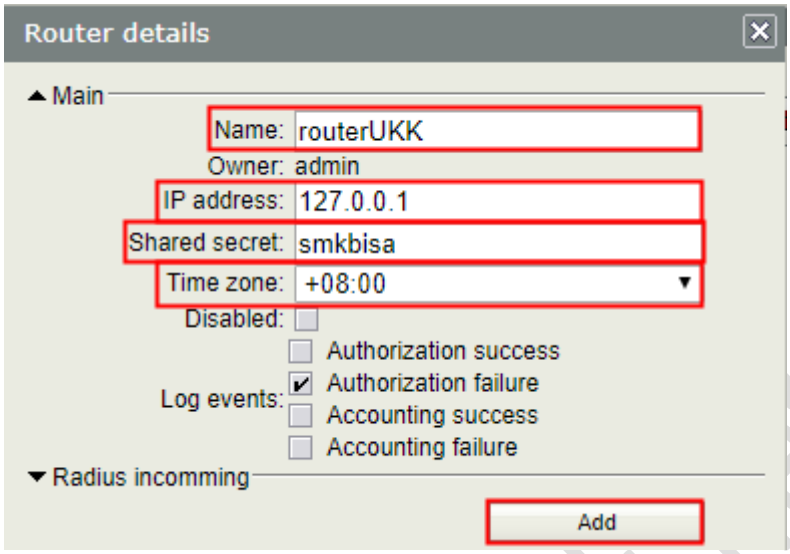
Tampil kotak dialog **Router details**, seperti terlihat pada gambar berikut:



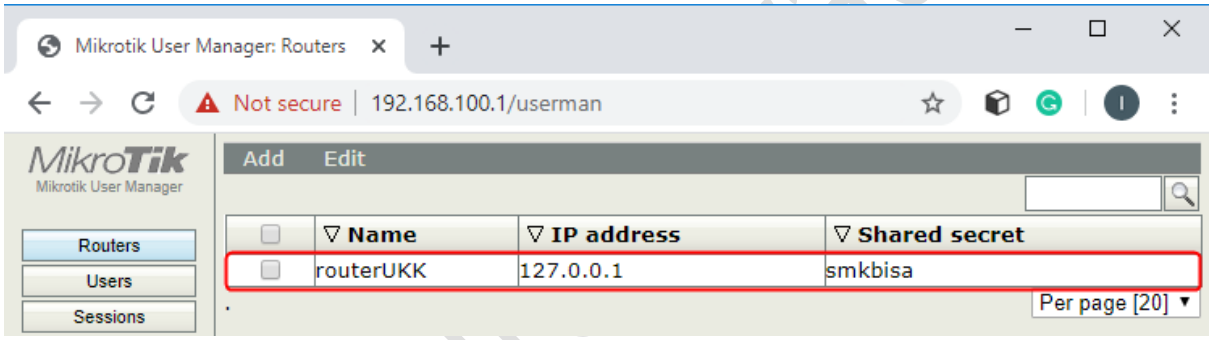
Terdapat beberapa parameter yang diatur yaitu:

- **Name**, digunakan untuk mengidentifikasi *router*, sebagai contoh **routerUKK**.
- **IP Address**, digunakan untuk mengatur alamat IP dari *router* yang bertindak sebagai *RADIUS Client*, yaitu **127.0.0.1**.
- **Shared secret**, digunakan untuk mengatur kunci sebagai metode dalam mengamankan komunikasi antara *RADIUS server* dan *RADIUS Client*, sebagai contoh **smkbisa**.
- **Time zone**, berfungsi untuk mengatur zona waktu menggunakan **Greenwich Mean Time (GMT)** sehingga penampilan data seperti informasi *session* dan *credit* pada **User Manager** sama dengan zona waktu pada **RouterOS**, sebagai contoh pilih **+08:00** untuk **WITA**. Sedangkan untuk **WIB** dapat menggunakan **+07:00** dan untuk **WIT** menggunakan **+09:00**.

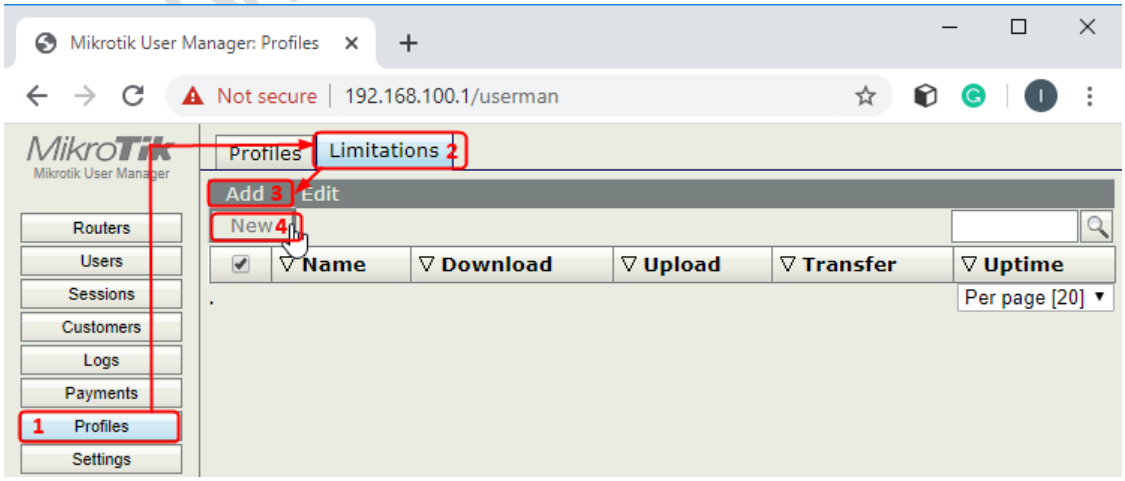
Hasil pengaturan parameter tersebut akan terlihat seperti pada gambar berikut:



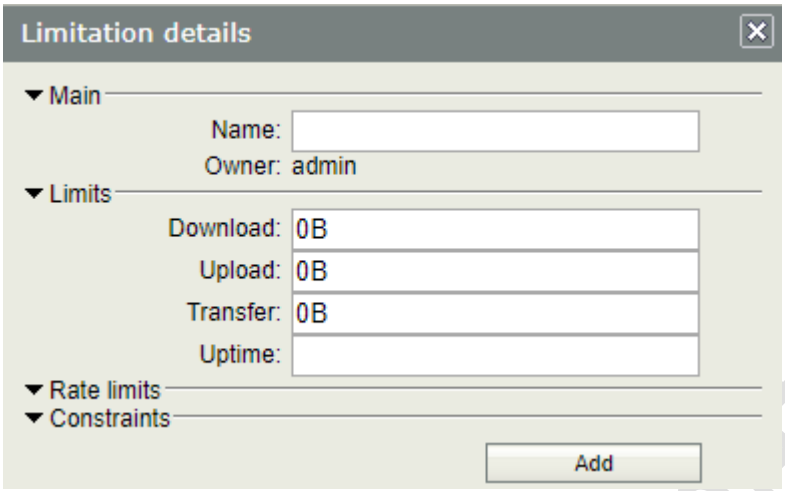
Klik tombol **Add** untuk menyimpan pengaturan. Hasil penambahan *router* sebagai *RADIUS Client*, terlihat seperti pada gambar berikut:



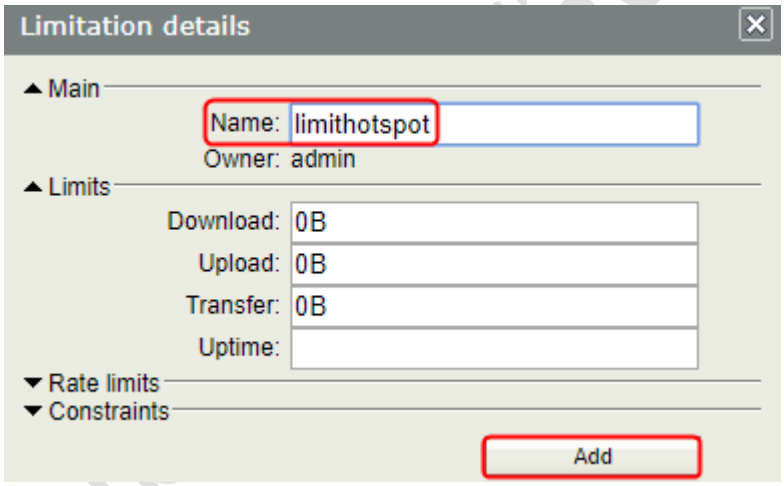
e) Mengijinkan akses Internet hanya pada pukul **07:00-16:00** bagi **user hotspot** dengan menggunakan **Profiles** dan **Limitations**. Pembuatan *limitation* dapat dilakukan dengan memilih menu **Profiles > Limitations > Add > New**, seperti terlihat pada gambar berikut:



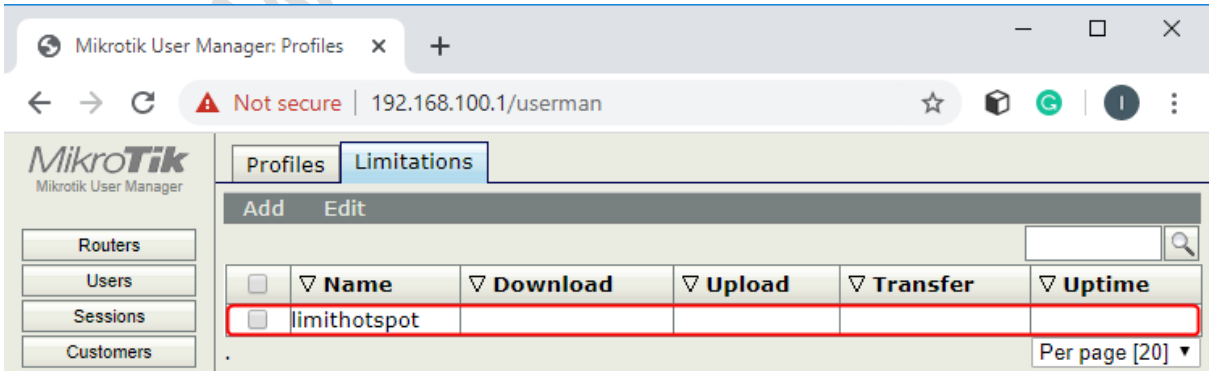
Tampil kotak dialog **Limitation details**, seperti terlihat pada gambar berikut:



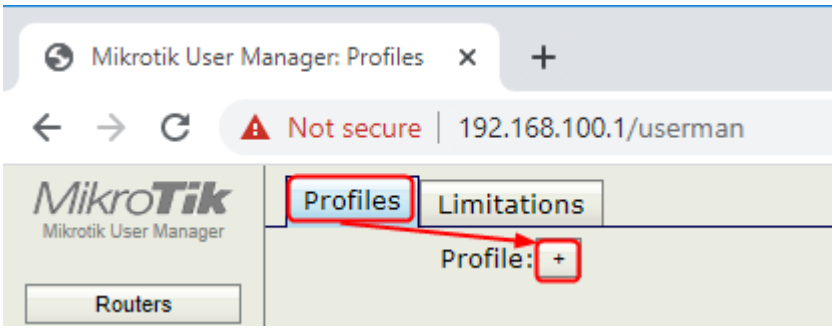
Pada parameter **Name:**, masukkan nama pengenal sebagai identifikasi dari limitasi, sebagai contoh **limithotspot** dan klik tombol **Add** untuk menyimpan pengaturan, seperti terlihat pada gambar berikut:



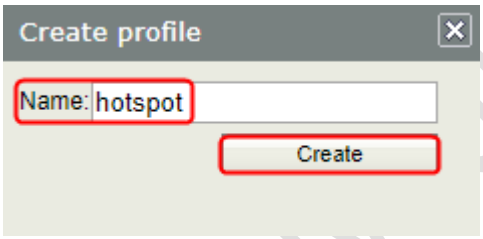
Hasil penambahan **Limitations** tersebut, seperti terlihat pada gambar berikut:



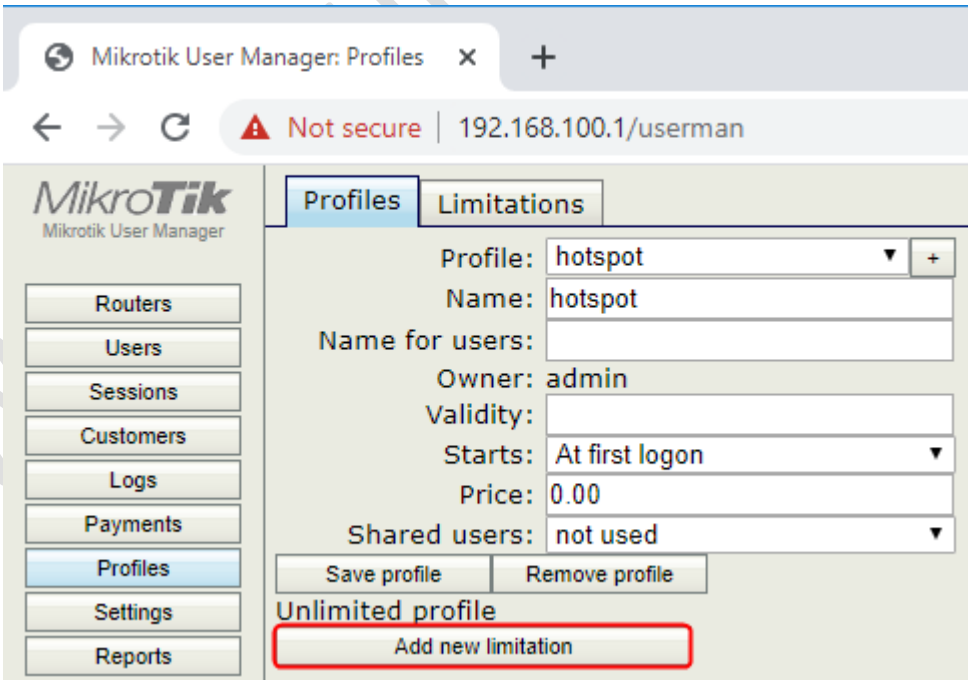
Selanjutnya pindah ke tab **Profiles** dan klik tombol + untuk menambahkan *profile* baru, seperti terlihat pada gambar berikut:



Pada kotak dialog **Create profile** yang tampil, masukkan "**hotspot**" sebagai nama pengenal *profile* baru yang dibuat pada inputan **Name:** dan klik tombol **Create**, seperti terlihat pada gambar berikut:



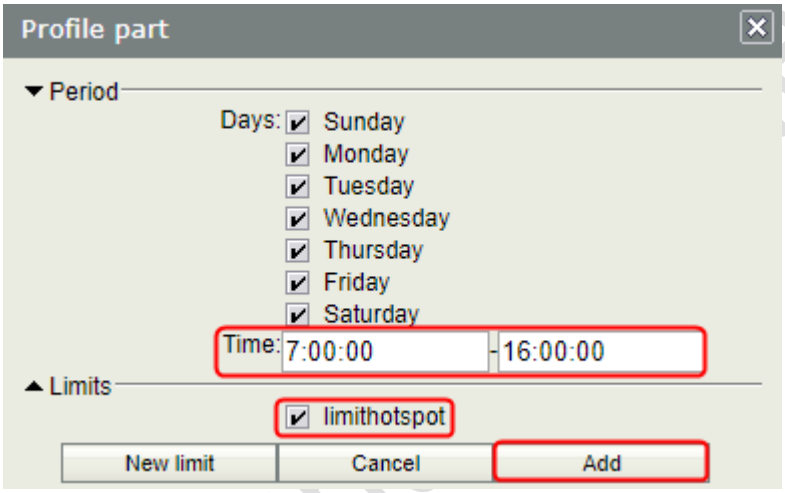
Tampil hasil dari pembuatan *profile* dengan nama **hotspot**. Selanjutnya lakukan penambahan limitasi terkait waktu akses Internet dengan menekan tombol **Add new limitation**, seperti terlihat pada gambar berikut:



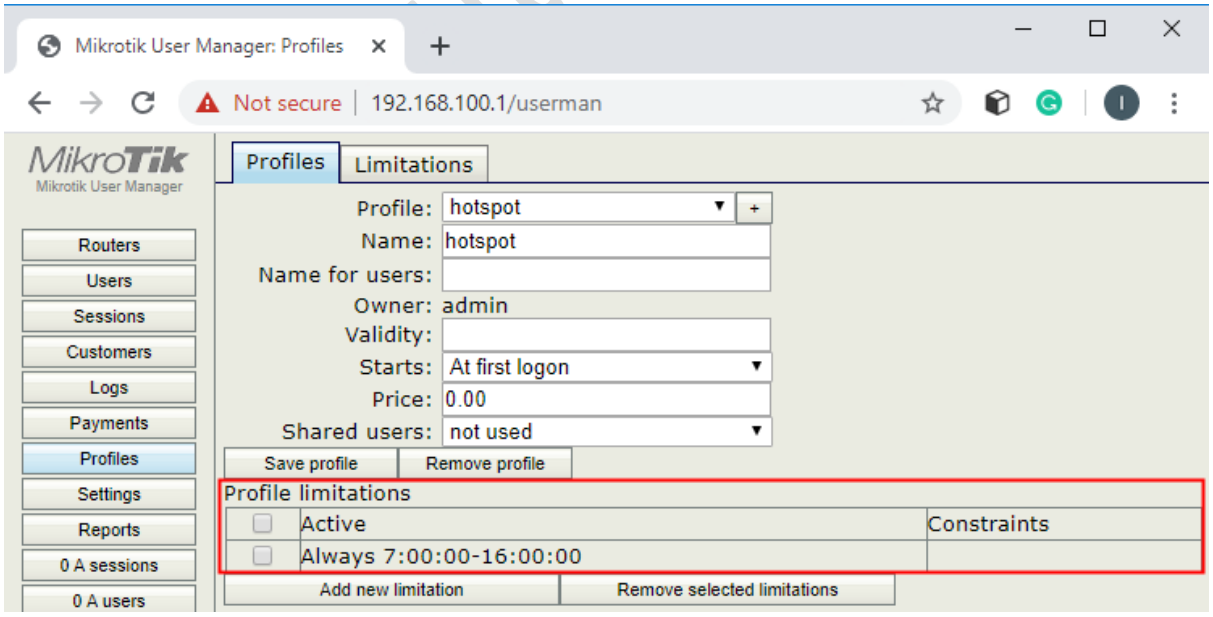
Pada kotak dialog **Profile part** yang tampil, lakukan pengaturan beberapa parameter berikut:

- **Time,** digunakan untuk mengatur limitasi akses berdasarkan waktu. Masukkan **7:00:00** pada inputan sebelah kiri yang merupakan jam mulai (**from-time**) dan masukkan **16:00:00** pada inputan sebelah kanan yang merupakan jam berakhir (**till-time**).
- Tandai atau centang inputan *checkbox* pada awal dari parameter **limithotspot** yang merupakan **limitation** yang telah dibuat pada langkah sebelumnya.

Hasil dari pengaturan tersebut, seperti terlihat pada gambar berikut:

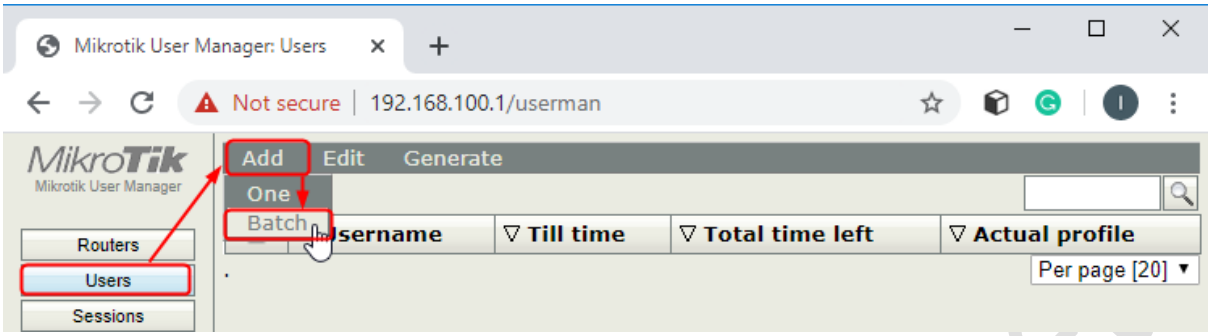


Klik tombol **Add** untuk menyimpan pengaturan maka hasilnya akan terlihat seperti pada gambar berikut:



Klik tombol **Save profile** untuk menyimpan perubahan pake **profile**.

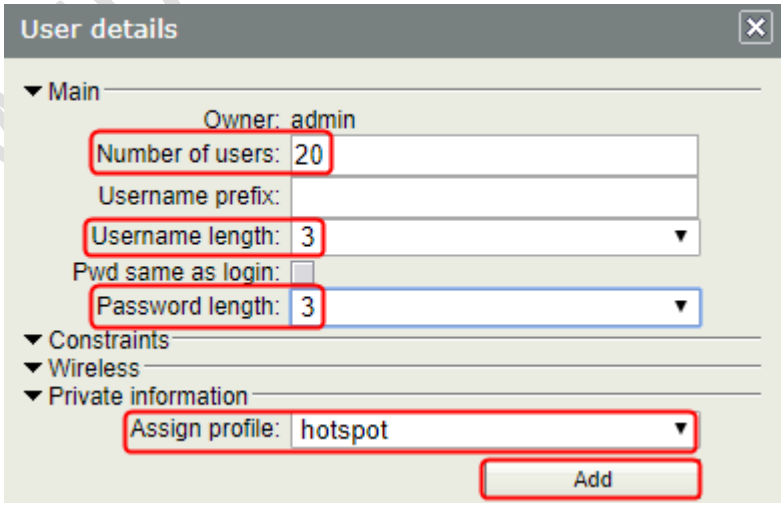
f) Membuat 20 (duapuluh) akun hotspot secara *random* dengan mengakses menu **Users > Add > Batch**, seperti terlihat pada gambar berikut:



Pada kotak dialog **User details** yang tampil, lakukan pengaturan beberapa parameter berikut:

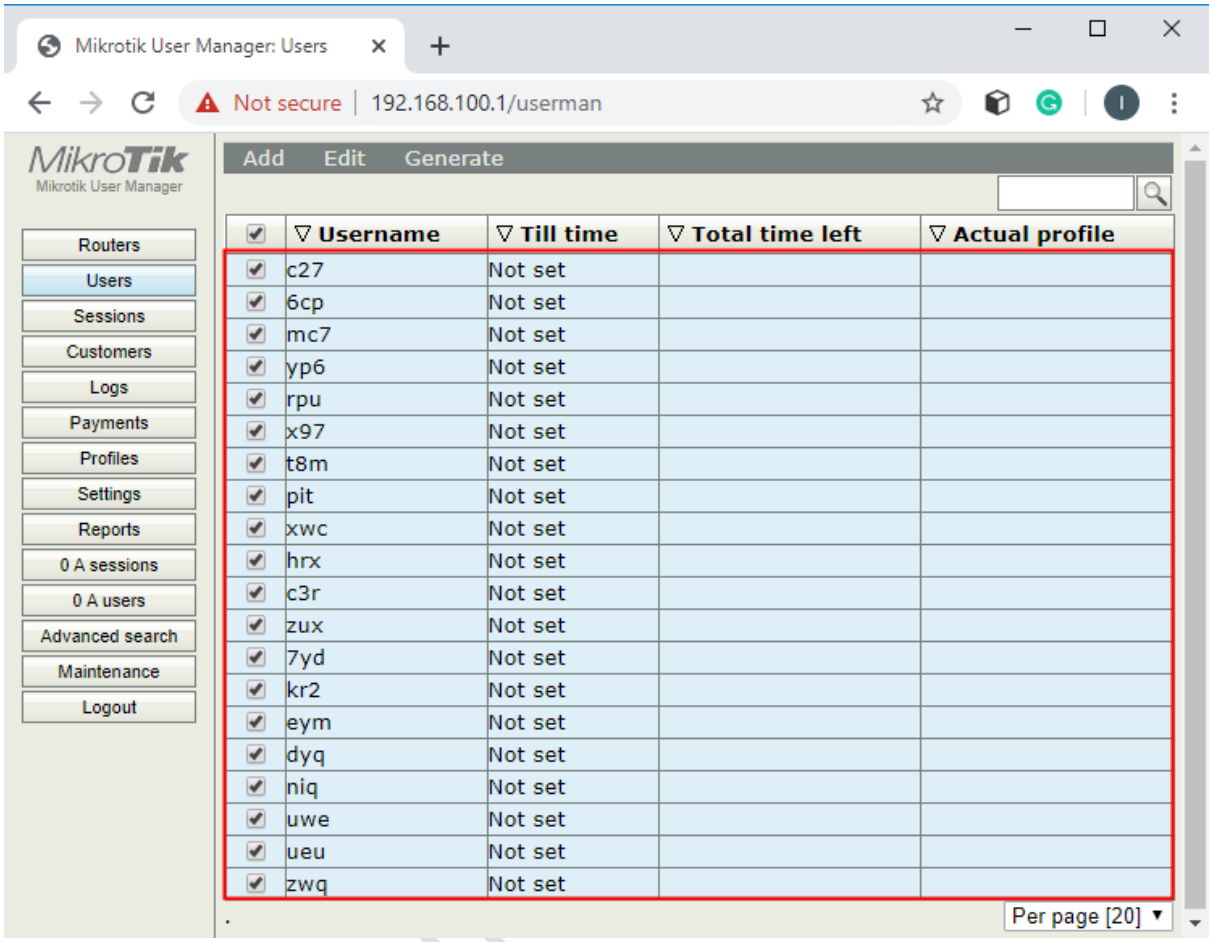
- **Number of users**, digunakan untuk menentukan jumlah *user hotspot* yang akan dibuat yaitu **20**.
- **Username length**, digunakan untuk menentukan panjang dari nama *login* dari *user hotspot* yang dibuat, sebagai contoh **3**.
- **Password length**, digunakan untuk menentukan panjang dari sandi *login* dari *user hotspot* yang dibuat, sebagai contoh **3**.
- **Assign profile**, digunakan untuk memilih *profile* yang akan diterapkan ke *user hotspot* yang dibuat yaitu **hotspot**.

Hasil dari pengaturan parameter tersebut, seperti terlihat pada gambar berikut:

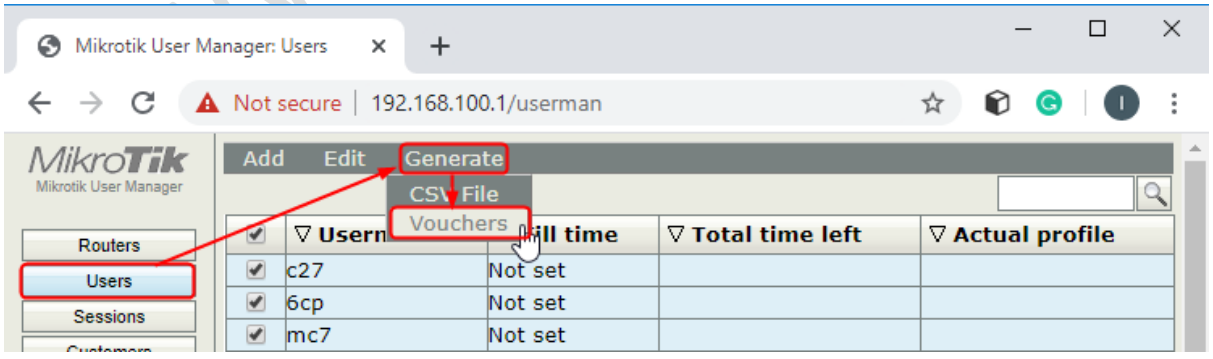


Klik tombol **Add** untuk memproses pembuatan **user**. Tampil pesan **Operation successful** yang menginformasikan bahwa pembuatan user berhasil dilakukan. Tutup kotak dialog **User details**.

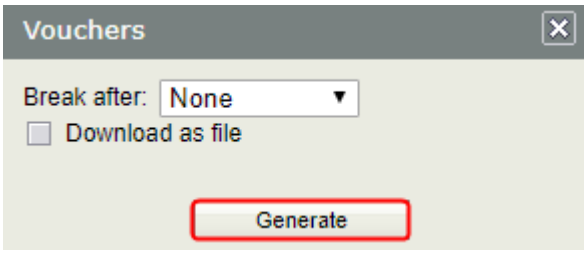
Terlihat hasil dari pembuatan 20 (duapuluh) user hotspot secara random, seperti pada gambar berikut:



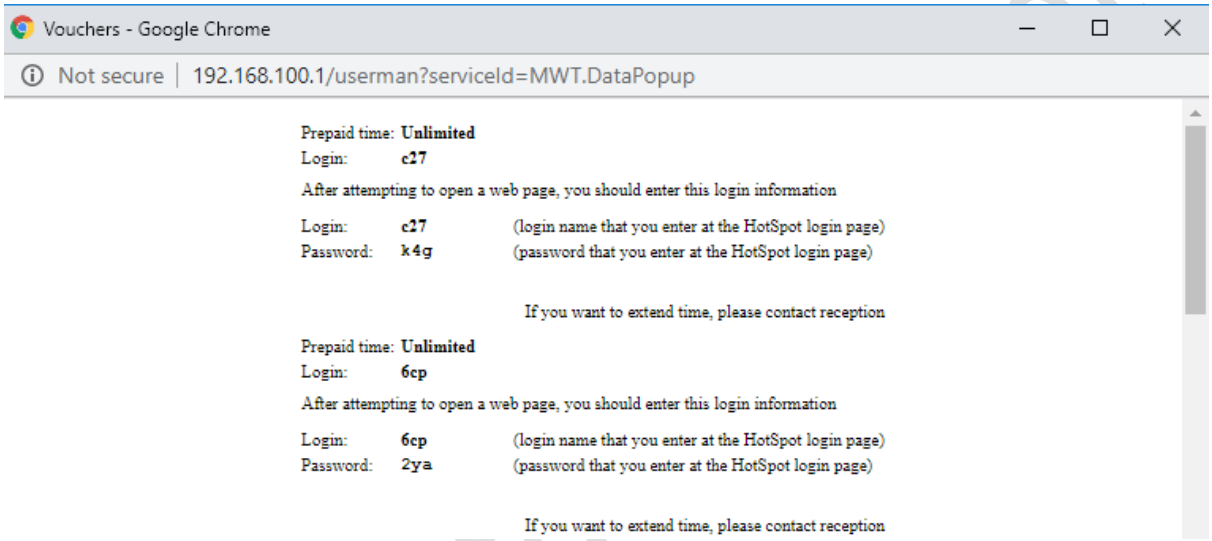
g) Meng-*generate* **Voucher User Hotspot** dengan mengakses menu **Generate > Vouchers** pada bagian **Users** sehingga dapat didistribusikan ke pengguna yang membutuhkan akses *hotspot*, seperti terlihat pada gambar berikut:



Tekan tombol **Generate** pada kotak dialog **Vouchers** yang tampil, seperti terlihat pada gambar berikut:



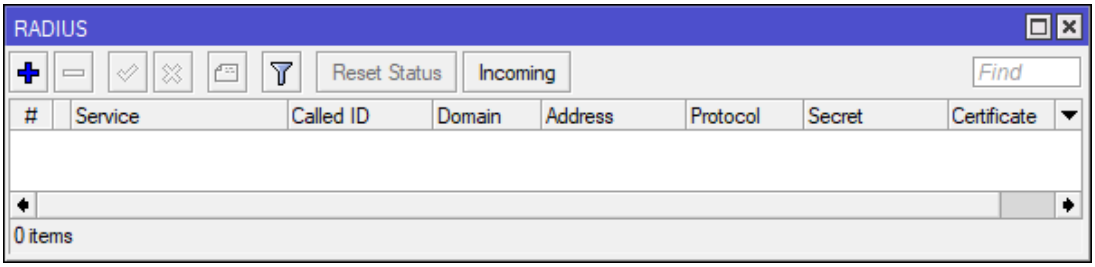
Tampil kotak dialog yang menampilkan informasi **Login** dan **Password** dari 20 (duapuluh) akun hotspot yang di *generate*, seperti terlihat pada gambar berikut:



Terlihat salah satu akun *login* yang dapat digunakan adalah **c27** dengan *password* **k4g**. Akun login tersebut akan digunakan ketika ujicoba mengakses Internet melalui *Hotspot*. Tutup kotak dialog tersebut.

Selanjutnya tutup pula kotak dialog **Vouchers** dan klik menu **Logout** untuk keluar dari penggunaan antarmuka berbasis web dari **User Manager**.

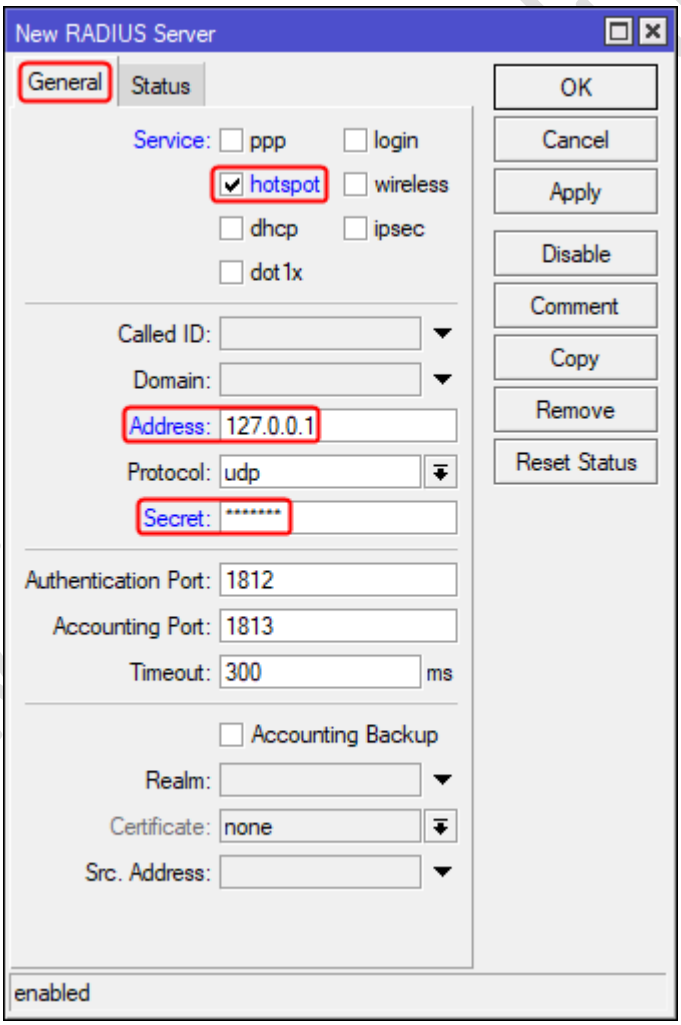
2. Mengatur *router Mikrotik* agar dapat terkoneksi ke *User Manager* yang bertindak sebagai **RADIUS Server** dengan mengakses menu **Radius** pada panel sebelah kiri dari *Winbox*. Tampil kotak dialog **RADIUS**, seperti terlihat pada gambar berikut:



Klik tombol  untuk menambahkan *RADIUS Server* maka akan tampil kotak dialog **New RADIUS Server**. Terdapat beberapa parameter yang perlu diatur pada tab **General** yaitu:

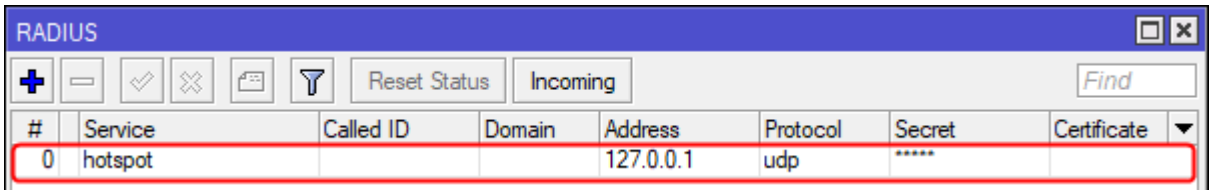
- **Service**, pilih **hotspot** sebagai layanan yang memanfaatkan **User Manager**.
- **Address**, masukkan alamat IP dari **RADIUS Server** yaitu **127.0.0.1**.
- **Secret**, masukkan **smkbisa** sebagai kunci untuk pengamanan komunikasi ke *RADIUS Server*. Hal ini sesuai dengan **router secret** yang telah diatur pada **User Manager** pada langkah 20d.

Hasil dari pengaturan parameter tersebut akan terlihat seperti gambar berikut:



Klik tombok **OK** untuk menyimpan pengaturan.

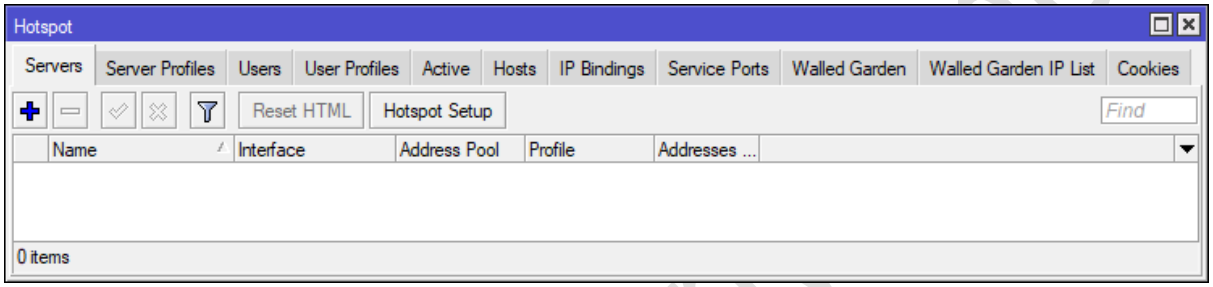
Hasil dari penambahan **RADIUS Server**, terlihat seperti pada gambar berikut:

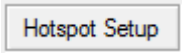


Tutup kotak dialog **RADIUS**.

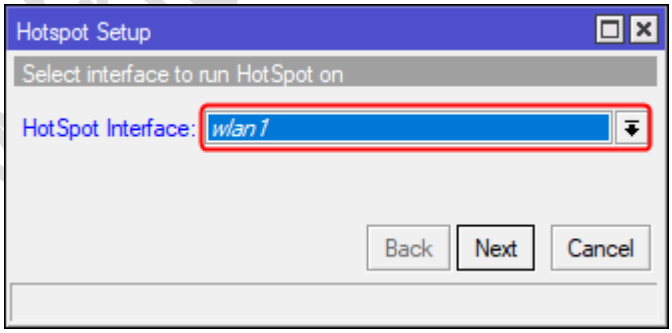
3. Mengaktifkan fitur *Hotspot* pada *interface wlan1*.

Pada panel sebelah kiri pilih menu **IP > Hotspot**, maka akan tampil kotak dialog **Hotspot**, seperti terlihat pada gambar berikut:



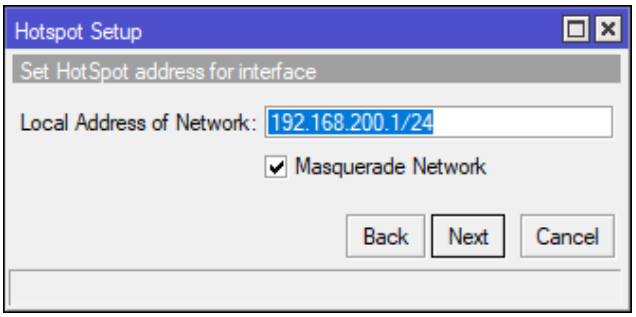
Pada toolbar dari kotak dialog **Hotspot** Tab **Servers**, klik tombol 

maka akan tampil kotak dialog wizard **Hotspot Setup**. Pada parameter **Hotspot Interface** dari kotak dialog **Hotspot Setup**, pilih *interface* **wlan1** sebagai *interface* untuk menjalankan *Hotspot*, seperti terlihat pada gambar berikut:

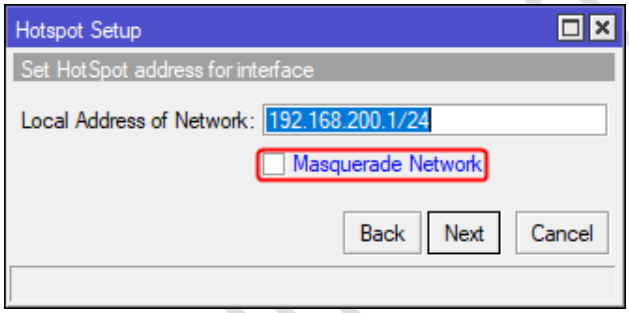


Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan alamat IP untuk *interface hotspot*, seperti terlihat pada gambar berikut:

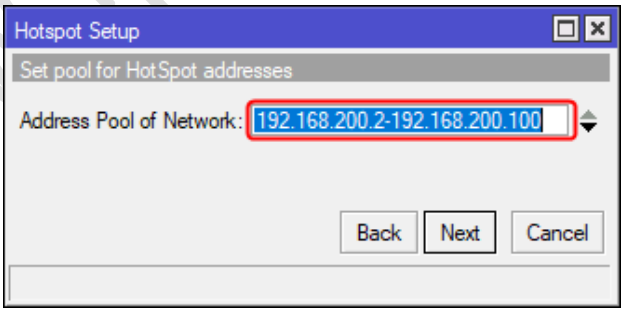


Pada parameter **Local Address of Network** secara langsung telah terisi dengan alamat IP yang telah diterapkan pada interface **wlan1** yaitu **192.168.200.1/24**. Hilangkan tanda cek (√) pada *checkbox* parameter **Masquerade Network**, seperti terlihat pada gambar berikut:



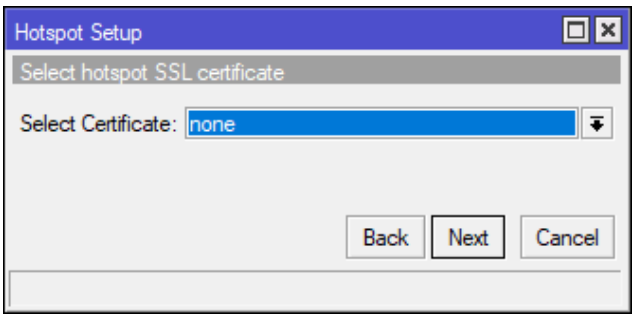
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan jangkauan alamat IP yang disewakan (*Address Pool*), seperti terlihat pada gambar berikut:



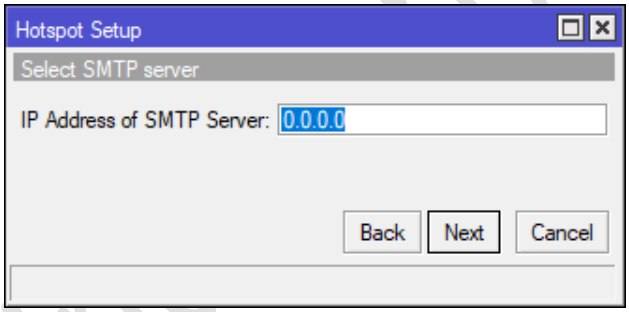
Pada parameter **Address Pool of Network** secara langsung telah terisi dengan rentang alamat **192.168.200.2-192.168.200.100** sebagai hasil dari konfigurasi **DHCP Server** di langkah sebelumnya. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan pemilihan sertifikat **SSL** untuk layanan hotspot, seperti terlihat pada gambar berikut:



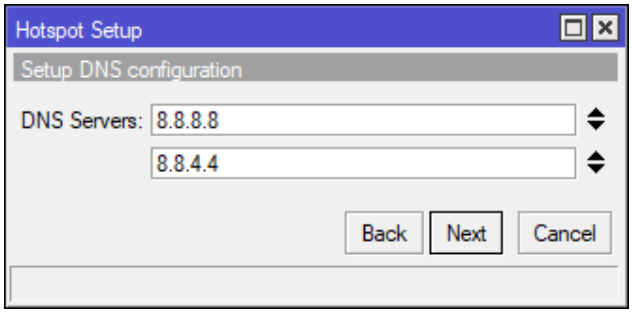
Pada parameter **Select Certificate**, secara *default* telah terpilih **none**. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan alamat IP dari *server SMTP*, seperti terlihat pada gambar berikut:



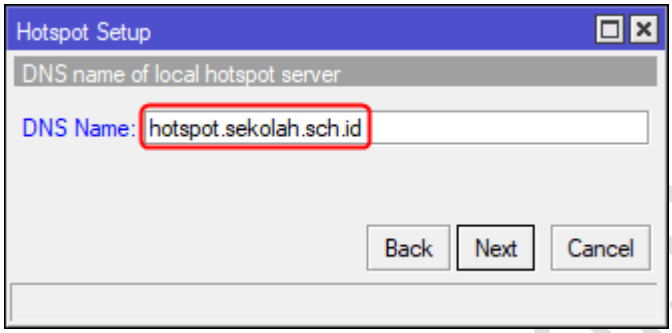
Pada parameter **IP Address of SMTP Server**, secara *default* telah terisi dengan alamat **0.0.0.0**. Sesuaikan nilai alamat IP ini apabila memiliki *server SMTP*. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan alamat IP dari **server DNS**, seperti terlihat pada gambar berikut:



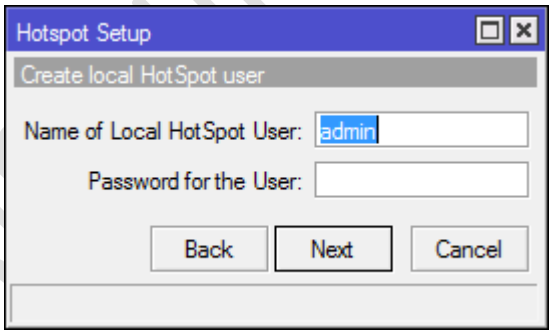
Pada parameter **DNS Server** telah terisi dengan dua alamat yaitu **8.8.8.8** dan **8.8.4.4**. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk menentukan nama **DNS** dari *server hotspot* lokal yang dibuat, seperti terlihat pada gambar berikut:

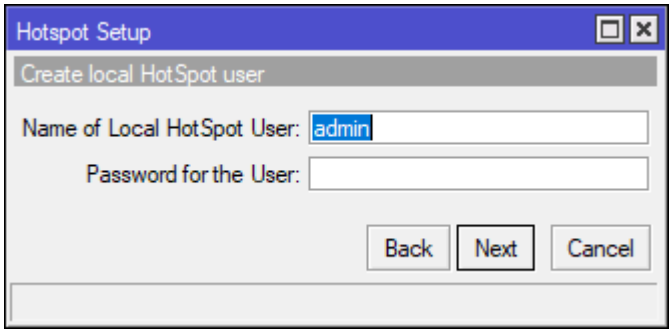


Pada parameter **DNS Name** masukkan **hotspot.sekolah.sch.id**. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog untuk membuat *user hotspot local*, seperti terlihat pada gambar berikut:

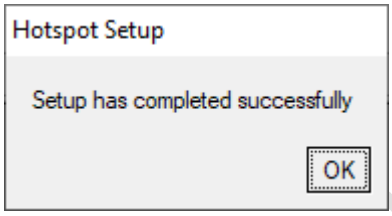


Pada parameter **Name of Local HotSpot User** secara *default* telah terisi dengan nilai "**admin**", seperti terlihat pada gambar berikut:



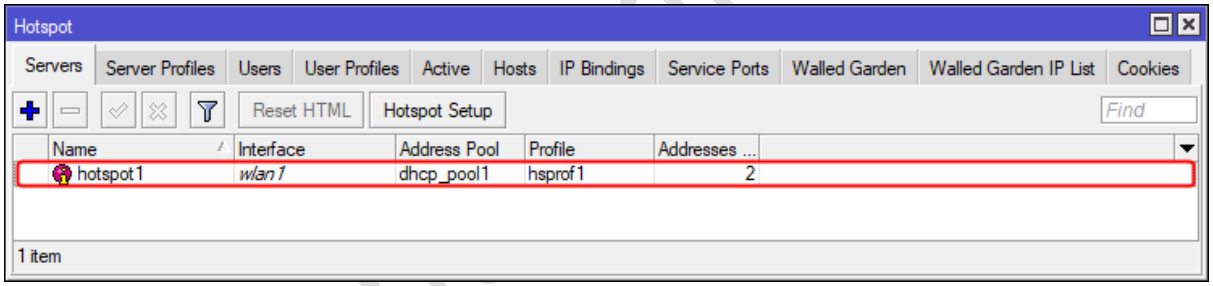
Apabila diinginkan dapat juga dilakukan pengaturan sandi dari *user hotspot* "**admin**" tersebut dengan pada parameter **Password for the User**. Sebagai contoh dibiarkan tetap tanpa *password*. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog yang menginformasikan bahwa *Hotspot Setup* telah berhasil diselesaikan, seperti terlihat pada gambar berikut:



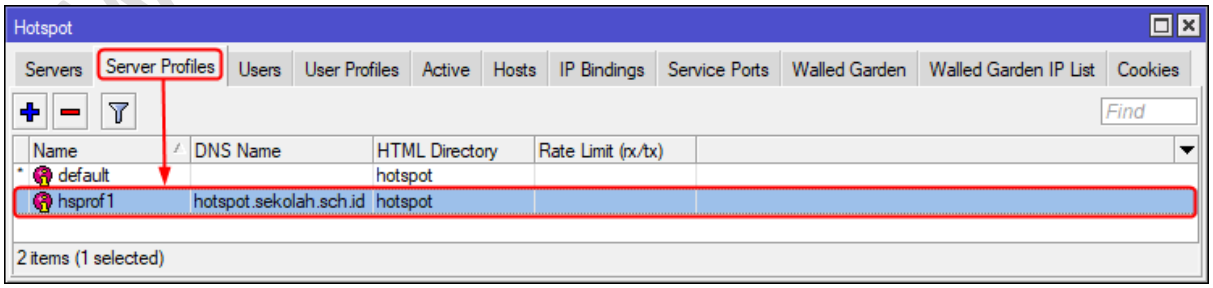
Klik tombol **OK**.

Hasil dari pembuatan hotspot dapat dilihat melalui tab **Servers** pada kotak dialog **Hotspot**, seperti ditunjukkan pada gambar berikut:

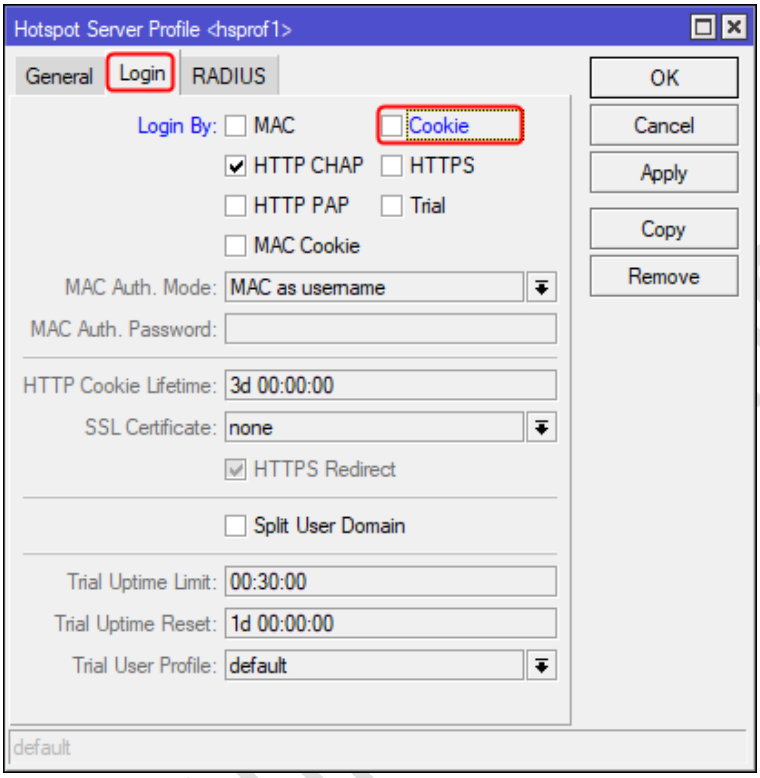


4. Menonaktifkan fitur **Cookies** dari **Hotspot** dan mengatur **Server Profiles** agar menggunakan **RADIUS** untuk mengotentikasi **user hotspot**.

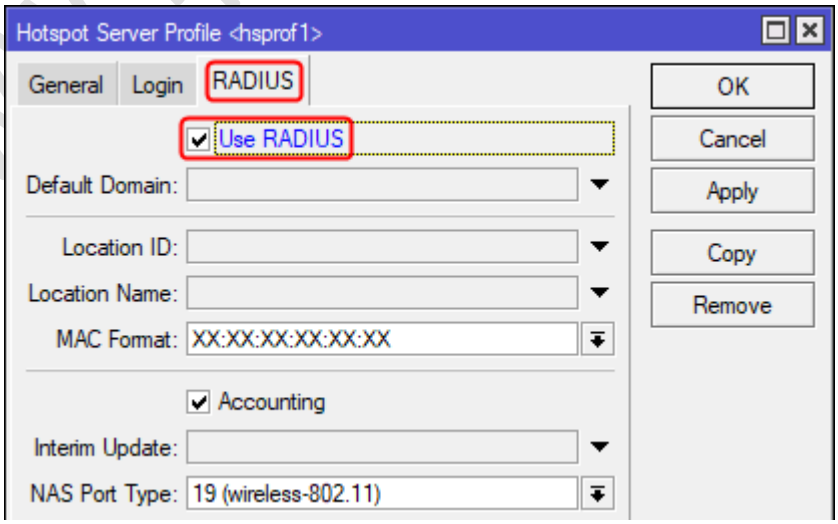
   Pilih tab **Server Profiles** pada kotak dialog **Hotspot** yang tampil dan klik dua kali pada *server profiles* dengan nama **"hsprof1"**, seperti terlihat pada gambar berikut:



Pada tab **Login** dari kotak dialog **Hotspot Server Profile <hsprof1>** yang tampil, hilangkan tanda centang atau *checkmark* pada *checkbox* dari parameter **Cookies**, seperti terlihat pada gambar berikut:



Klik pada tab **RADIUS** dari kotak dialog **Hotspot Server Profile <hsprof1>** dan tandai atau centang pada *checkbox* dari parameter **Use RADIUS** sehingga otentikasi *hotspot* menggunakan **User Manager** yang bertindak sebagai **RADIUS Server**, seperti terlihat pada gambar berikut:

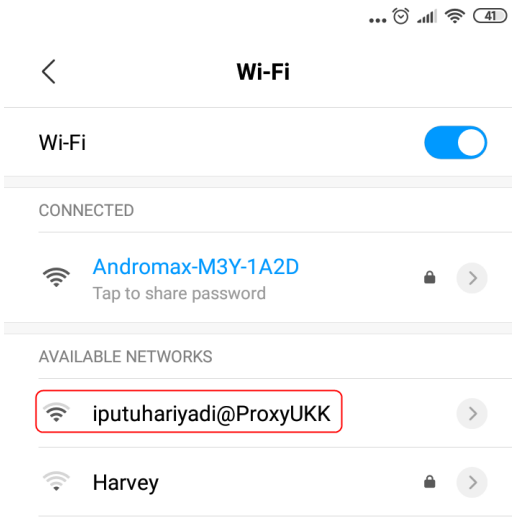


Klik tombok **OK** untuk menyimpan pengaturan.

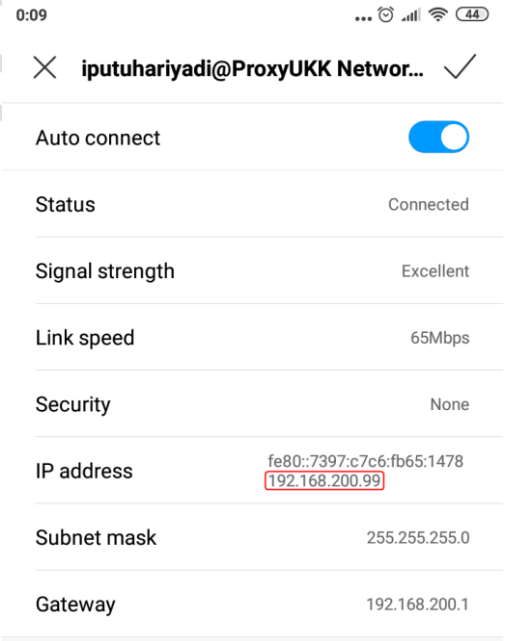
G. UJICOBA AKSES INTERNET MENGGUNAKAN SMARTPHONE ANDROID

Adapun langkah-langkah mengujicoba akses *Internet* menggunakan **smartphone android** adalah sebagai berikut:

1. Koneksikan *smartphone* ke **Wi-Fi** dengan **SSID iputuhariyadi@ProxyUKK**, seperti terlihat pada gambar berikut:

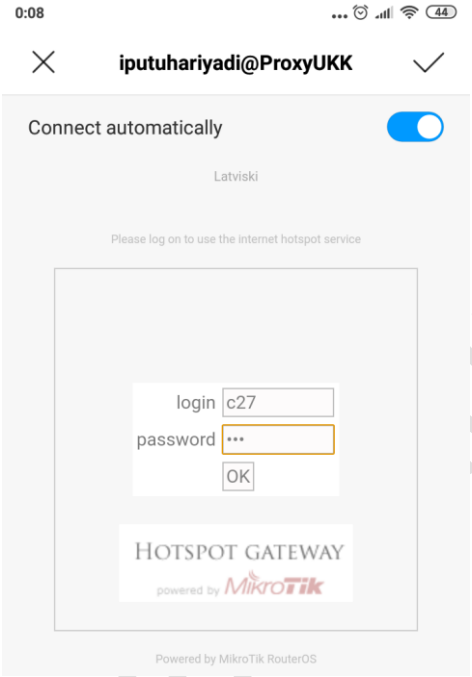


Apabila koneksi ke **SSID** tersebut berhasil dilakukan maka akan ditandai dengan pesan **Connected**. Pengalamatan IP dan parameter TCP/IP lainnya yang diperoleh *smartphone* yang telah berhasil terkoneksi tersebut, seperti terlihat pada gambar berikut:

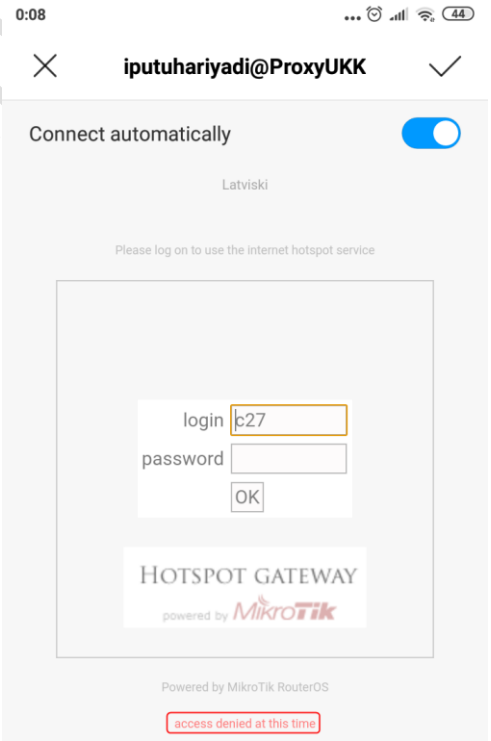


Terlihat pengalamatan IP yang diperoleh adalah **192.168.200.99**.

2. Secara otomatis akan diarahkan ke halaman **login hotspot** dari *Mikrotik*. Login ke *hotspot* menggunakan salah satu akun yang telah dibuat pada **User Manager**, sebagai contoh menggunakan *username* **c27** dengan *password* **k4g**, seperti terlihat pada gambar berikut:

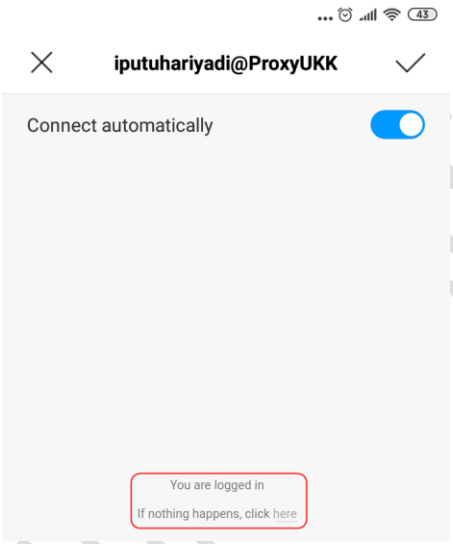


Tekan tombol **OK.** Hasil dari proses otentikasi login terlihat seperti pada gambar berikut:

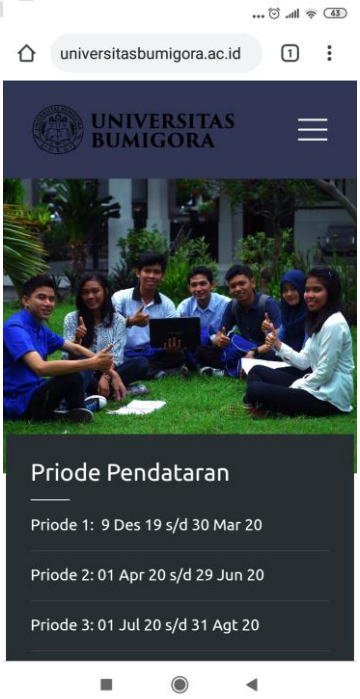


Terlihat pesan "**access denied at this time**" yang menginformasikan bahwa koneksi *Internet* tidak dapat dilakukan saat ini. Hal ini karena layanan *hotspot* dilimitasi agar hanya dapat dilakukan pada jam **07:00-16.00**. Sedangkan waktu ujicoba pengaksesan ini terlihat pada pojok kanan bawah dari taskbar menunjukkan jam **0:08** dini hari.

Sebaliknya apabila koneksi dilakukan pada jam **07:00-16:00** maka akan tampil pesan "**You are logged in**" yang menandakan bahwa otentikasi *login hotspot* berhasil dilakukan, seperti terlihat pada gambar berikut:



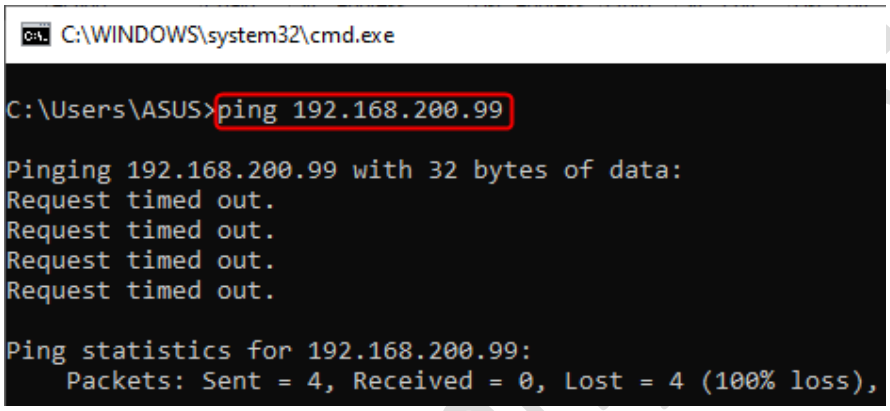
3. Buka browser dan lakukan verifikasi akses ke salah satu situs di Internet, sebagai contoh https://universitasbumigora.ac.id, seperti terlihat pada gambar berikut:



Terlihat akses ke situs **Universitas Bumigora** tersebut berhasil dilakukan.

H. VERIFIKASI PEMBLOKIRAN PING DARI CLIENT LAN KE CLIENT WLAN

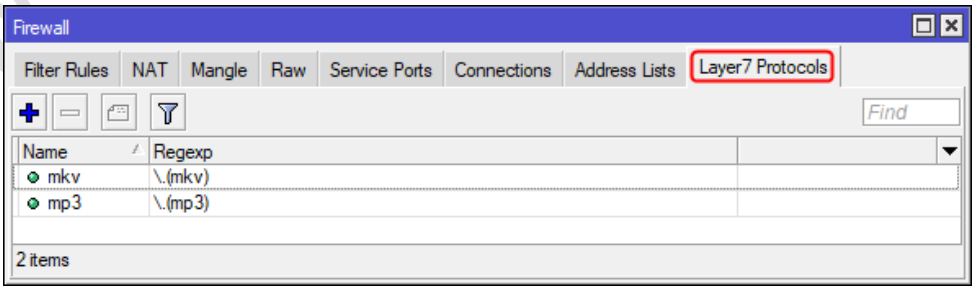
Melalui **command prompt** dari **client LAN** dengan sistem operasi **Windows 10**, eksekusi perintah **ping** ke alamat IP dari **smartphone android** yaitu 192.168.200.99 **(Sesuaikan alamat IP ini dengan yang diperoleh smartphone yang digunakan)**, seperti terlihat pada gambar berikut:



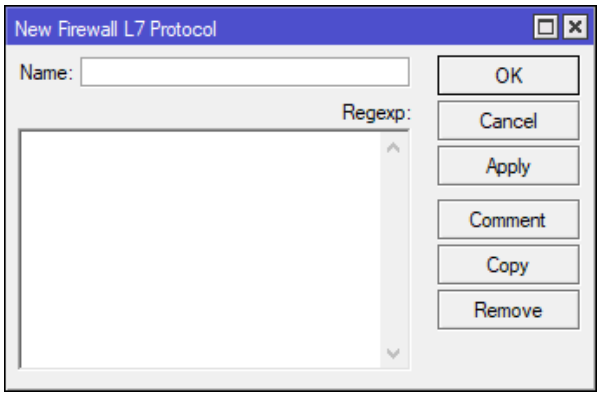
Terlihat **ping** dari **client LAN** ke alamat IP dari **client WLAN** telah berhasil diblokir.

I. PEMBLOKIRAN SITUS HTTPS://WWW.LINUX.ORG MENGGUNAKAN IP FIREWALL FILTER RULES DAN LAYER7 PROTOCOLS

Apabila pemblokiran situs https://www.linux.org dengan menggunakan **TLS-HOST** gagal dilakukan (**bandel** ☺) maka dapat menggunakan lainnya yaitu dengan **IP Firewall Filter Rules** dan **Layer7 Protocols**. Pada panel sebelah kiri **Winbox**, Pilih **IP > Firewall**, maka akan tampil kotak dialog **Firewall**. Pilih tab **Layer 7 Protocols** pada kotak dialog tersebut seperti terlihat pada gambar berikut:



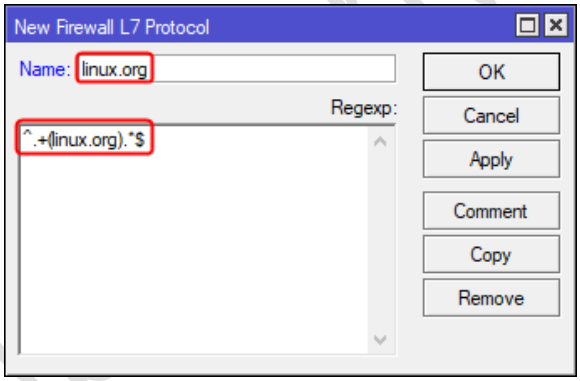
Untuk menambahkan rule baru, pilih tombol  pada toolbar dari kotak dialog **Firewall** maka akan tampil kotak dialog **New Firewall L7 Protocol** seperti terlihat pada gambar berikut:



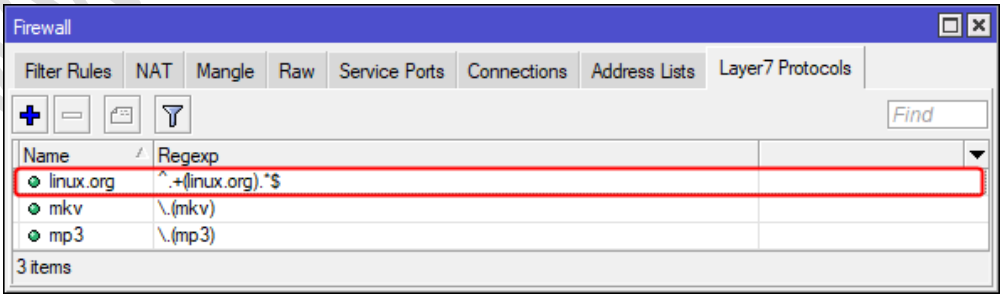
Terdapat beberapa parameter yang harus diatur yaitu:

a. **Name**, digunakan untuk menentukan nama pengenal *L7 Protocol* yang dibuat, sebagai contoh **linux.org**.
b. **Regexp**, digunakan untuk menentukan pola pencocokan regular expression, sebagai contoh **^.+(linux.org).*$**

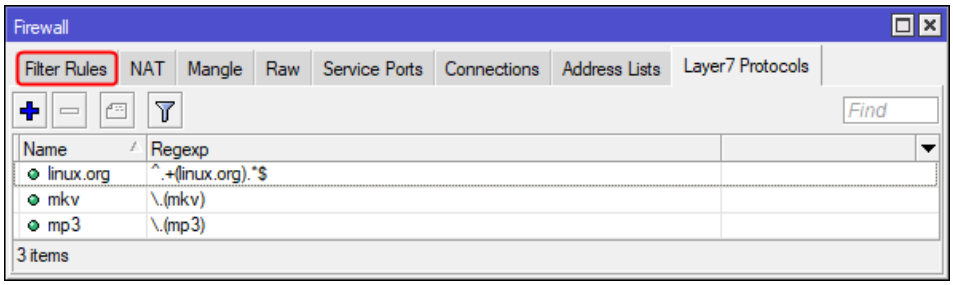
Hasil dari pengaturan parameter tersebut akan terlihat seperti pada gambar berikut:



Klik tombol **OK** untuk menyimpan. Hasil dari penambahan *L7 Protocol* tersebut akan terlihat seperti gambar berikut:

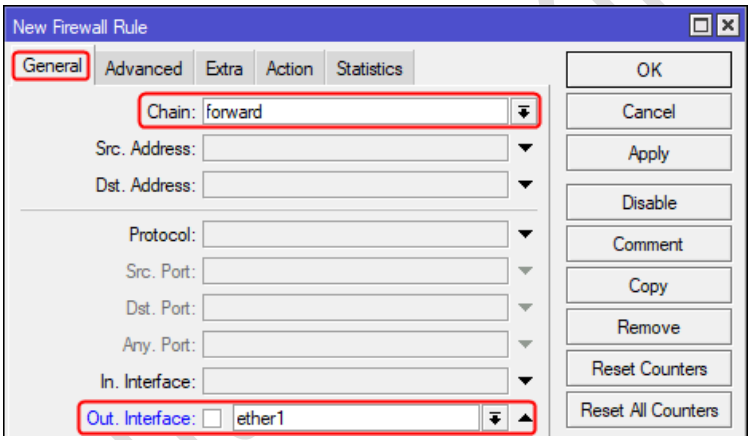


Selanjutnya membuat *IP Firewall Filter Rules* untuk memblokir situs berdasarkan pola *Layer7 Protocols* yang telah dibuat sebelumnya dengan memilih tab **Filter Rules** pada kotak dialog **Firewall**, seperti terlihat pada gambar berikut:

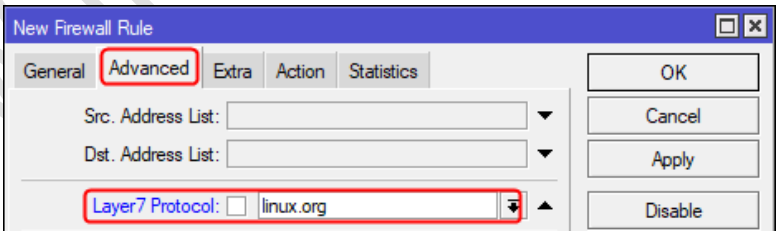


Untuk menambahkan rule baru, pilih tombol  pada toolbar dari kotak dialog **Firewall tab Filter** Rules. Pada kotak dialog **New Firewall Rule** yang tampil, terdapat beberapa parameter yang harus diatur yaitu:

- Pada tab **General**, pastikan pilihan parameter **Chain** adalah **forward** dan **Out. Interface** adalah **ether1**, seperti terlihat pada gambar berikut:



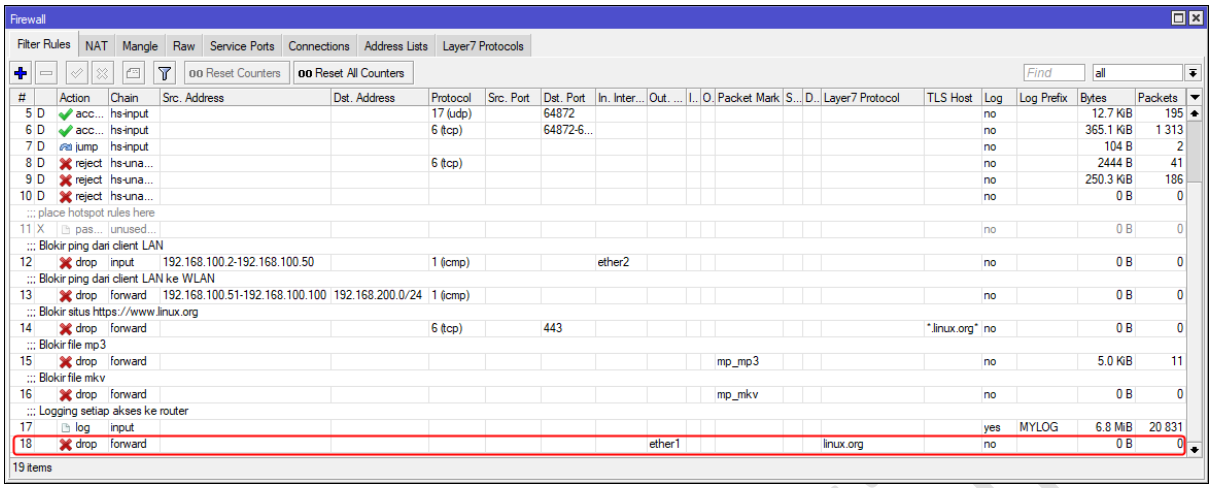
- Selanjutnya pindah ke tab **Advanced**, pastikan pilihan parameter **Layer7 Protocol** adalah **linux.org**, seperti terlihat pada gambar berikut:



- Lanjut Pindah ke tab **Action**, pastikan pilihan parameter **Action** adalah **drop** untuk menolak paket yang cocok dengan rule yang ditentukan, seperti terlihat pada gambar berikut:

Klik tombol **OK** untuk menyimpan pengaturan.

Hasil dari penambahan *rule* tersebut akan terlihat seperti pada gambar berikut:



Selamat Anda telah berhasil menyelesaikan soal Uji Kompetensi Keahlian (UKK) SMK TKJ Paket 4 Kurikulum 2013 Tahun 2020. Semoga pembahasan soal ujian ini bermanfaat bagi rekan-rekan SMK TKJ. Terimakasih ☺.