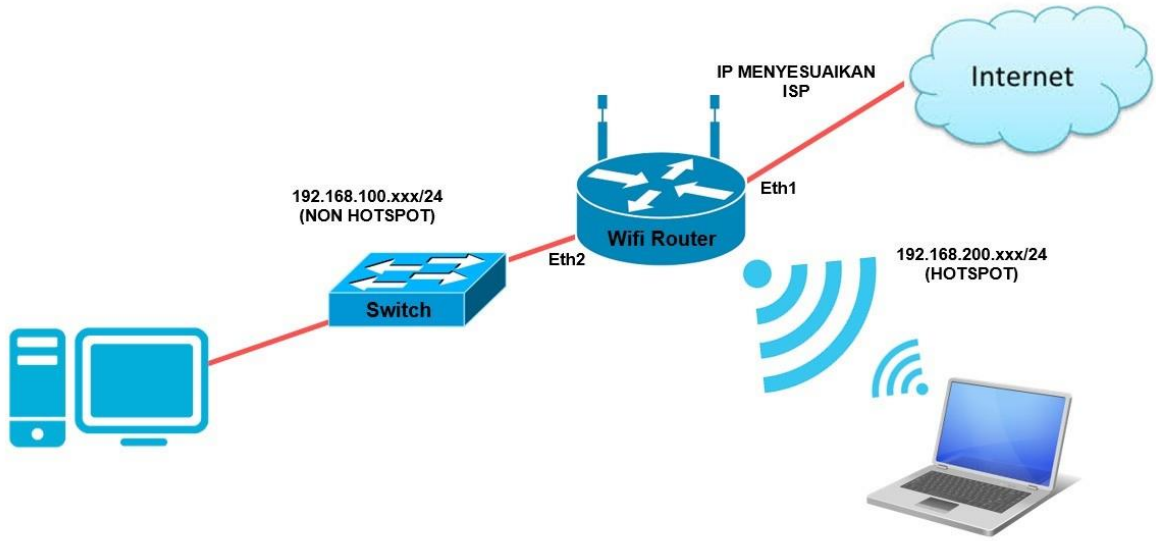
Pembahasan UPK TKJ 2017/2018 Paket 2 K13

Ariyolo.id Topologi dari tugas yang akan kita kerjakan adalah seperti ini, gambar ini langsung saya ambil dari soal.



Ether 1 – Internet Gateway

Tahap paling awal yang harus teman-teman lakukan adalah memastikan bahwa router telah terhubung ke internet. Mengapa? Karena jika router belum terhubung ke internet maka untuk tahap selanjutnya niscaya tidak bisa diuji keberhasilannya karena butuh internet. Untuk pembuatan

> Jika ada bagian yang menggunakan CLI maka pengguna Winbox harap menyesuaikan.

Untuk membuat terkoneksi ke internet kita bisa menggunakan perintah-perintah seperti di bawah ini. Untuk yang menggunakan tanda # berarti itu adalah penjelasan dari perintah yg di bawahnya.

Berikan IP pada antarmuka gateway, tetapi agar tidak bolak-balik sekalian saja berikan IP pada antarmuka ether2 dan wlan1.

Memberikan **IP Address**

```
1 /ip address
2 add address=192.168.1.253/24 interface=ether1 network=192.168.1.0
3 add address=192.168.100.1/24 interface=ether2 network=192.168.100.0
4 add address=192.168.200.1/24 interface=wlan1 network=192.168.200.0
```

Selanjutnya kita berikan *rule routing* yang dimana jika IP Address yang dimaksud tidak diketahui maka akan diteruskan ke jaringan publik (ether1)

Routing ke Internet

```
1 /ip route
2 add distance=1 gateway=192.168.1.1
```

Agar jaringan di antarmuka lain bisa ke internet kita juga harus menambahkan fitur NAT yang mengarah ke ether1

Fitur **NAT**

```
1 /ip firewall nat
2 add action=masquerade chain=srcnat out-interface=ether1
```

Karena jika berselancar kita mengakses menggunakan nama Domain dan bukan IP maka kita harus atur juga DNS dengan perintah di bawah ini. Sedikit catatan saya menggunakan DNS Google, kemungkinan teman-teman nanti menggunakan DNS yang diberikan oleh guru masing-masing.

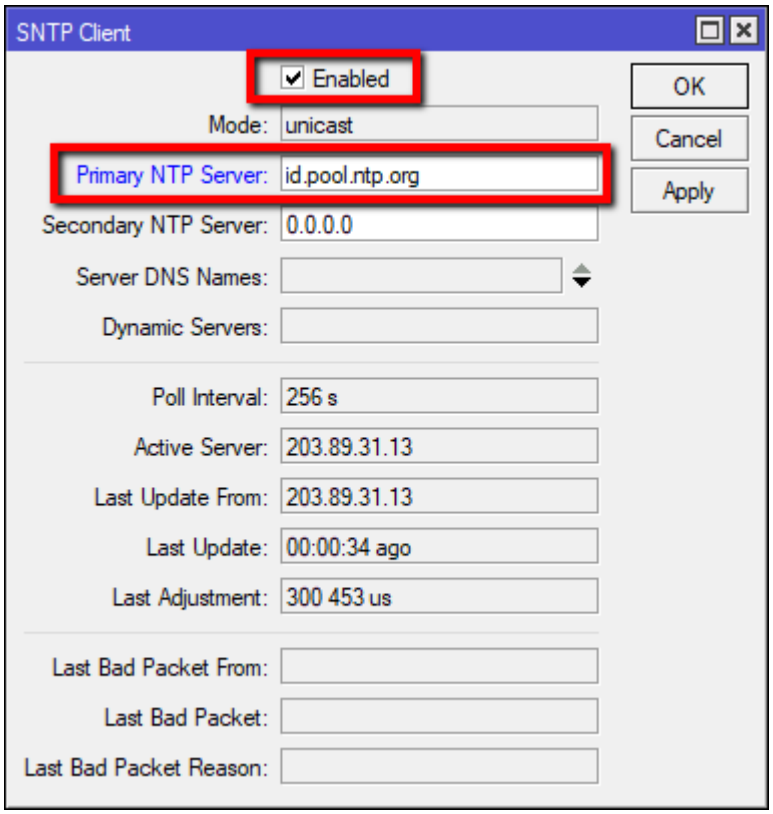
DNS

```
1 /ip dns
2 set allow-remote-requests=yes servers=8.8.8.8
```

Seharusnya saat ini teman-teman sudah berhasil terhubung ke internet, silahkan untuk mengecek di dari PC yang terhubung ke ether 2 bisa berselancar atau tidak. Namun sebelumnya isi dulu IP PC nya dengan yang satu network dengan ether2.

Network Time Protocol

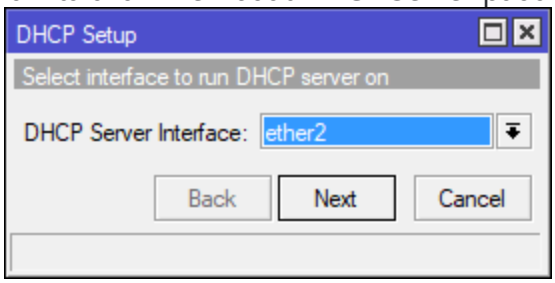
Secara bawaan waktu pada Router MikroTik adalah tahun 1970. Untuk menyetarakan dengan kondisi saat ini bisa saja namun sebenarnya ada fungsi Network Time Protol atau NTP. NTP adalah layanan yang berfungsi untuk menyamakan waktu antar perangkat. NTP dilakukan setelah router terkoneksi ke internet agar bisa mengecek ke server waktu internasional.
Untuk mengkonfigurasinya teman-teman bisa ke **System > SNTP Client**, lalu buat seperti di bawah ini dan terakhir klik OK.



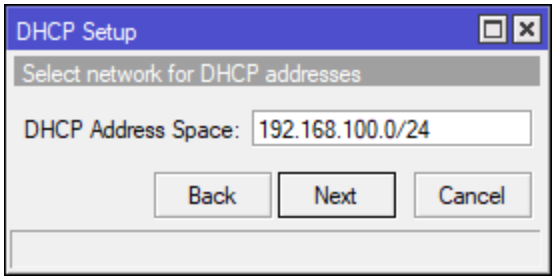
Saat ini router kita telah terhubung dengan sistem waktu internasional, selanjutnya tinggal kita sesuaikan dengan daerah kita. Caranya bisa ke **System > Clock** lalu klik **Time Zone Autodetect** dan pada kolom **Time Zone Name** cari Asia/Jakarta dan klik OK. Saat ini router kita telah memiliki waktu yang *real*.

Ether 2 – Modul DHCP

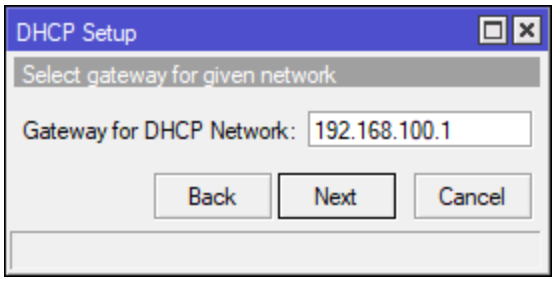
Sesuai dengan soal bahwa di Ether2 disuruh membuat DHCP Server. Karena DHCP Server cukup sulit ketika menggunakan CLI maka saya akan menggunakan Winbox saja. Silahkan teman-teman menuju **IP > DHCP Server** pada **tab DHCP** pilih **DHCP Setup**. Di tampilan ini silahkan pilih ether2 karena kita akan membuat DHCP Server pada ether2



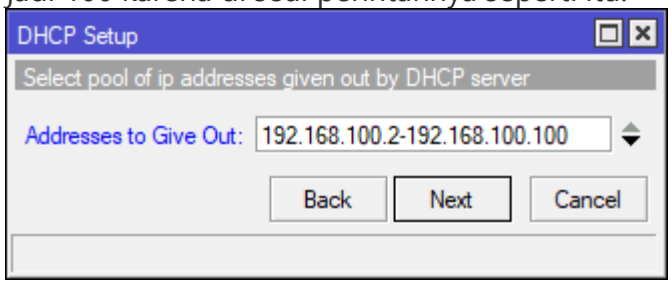
Pada pemilihan network dibiarkan saja karena secara otomatis akan menyesuaikan dengan prefix yang kita isi di ether2



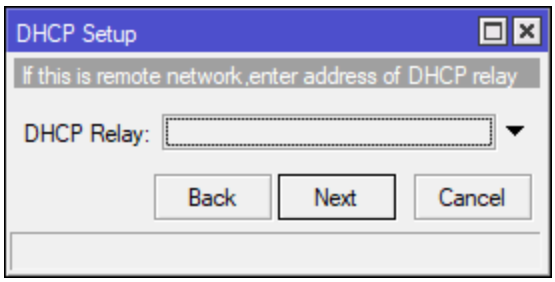
Untuk gateway dibiarkan juga karena secara otomatis akan menyesuiakan dengan IP Address yang terpasang di ether2



Untuk alamat yang diberikan secara bawaan router akan menentukan mengikuti subnetting, tetapi kita akan ubah jadi 100 karena di soal perintahnya seperti itu.



DHCP Relay biarkan kosong karena kita tidak menggunakan fitur ini

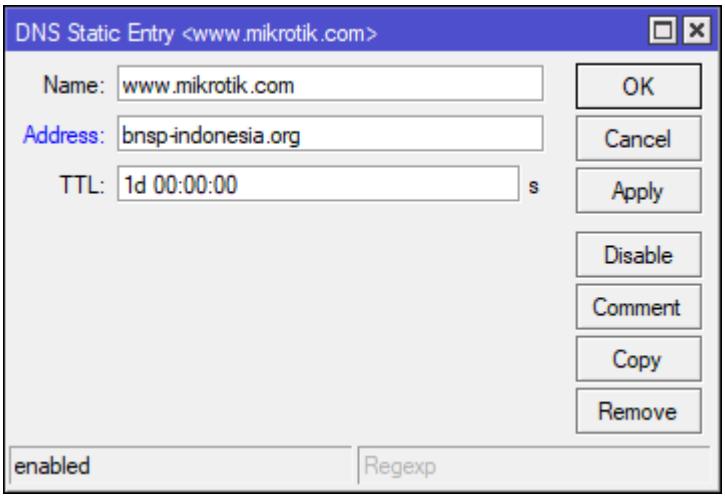


Sekarang silahkan teman-teman periksa pada komputer yang disambungkan ke ether2, seharusnya saat ini telah mendapatkan IP secara DHCP.

Ether 2 – Static DNS

Fitur static DNS ini digunakan ketika kita ingin mendifinisikan domain pada router kita sendiri. Sehingga ketika pengguna mengakses suatu domain maka akan diarahkan ke tujuan tertentu. Untuk menggunakan fitur ini silahkan pergi ke **IP > DNS > Static > + (add)** lalu tambahkan domain yang akan didefinisikan pada Name serta tujuannya pada Address.

Ralat alamat yang benar adalah bsnp-indonesia.org



Sebenarnya kolom Address hanyalah bisa membaca IP, namun pada fitur mikrotik yang baru dimana bisa melakukan *resolve* pada domain maka ketika kita memasukkan domain bsnp-indonesia.org akan otomatis berubah menjadi IP Address dari bsnp-indonesia.org.

Setelah tahap ini selesai silahkan coba membuka www.mikrotik.com pada peramban teman-teman, kalau belum berhasil silahkan diperiksa kembali tahapannya,

Ether 2 – Blokir PING

Firewall pertama yang akan dibuat adalah pembatasan IP 192.168.100.2 – 192.168.100.50 tidak bisa melakukan ping ke Router. Karena saat ini kita memiliki 3 IP Address pada router maka semua IP Address ini harus dimasukkan ke dalam *rule*.

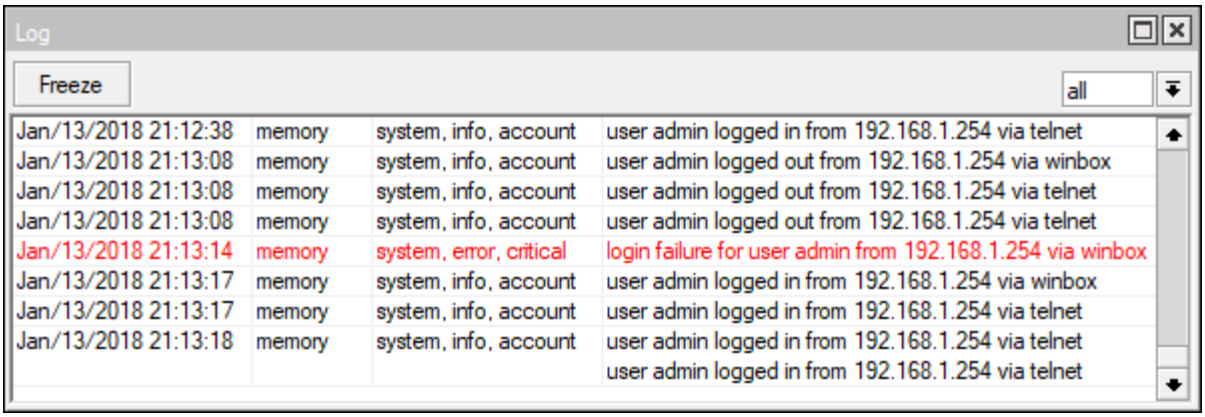
Blokir ping ke Router

```
1 /ip firewall filter
2 add action=drop chain=input dst-address=192.168.1.253 protocol=icmp src-address=192.168.100.1-192.168.100.50
3 add action=drop chain=input dst-address=192.168.100.1 protocol=icmp src-address=192.168.100.1-192.168.100.50
4 add action=drop chain=input dst-address=192.168.200.1 protocol=icmp src-address=192.168.100.1-192.168.100.50
```

Arti dari perintah di atas adalah jika ada paket ping (icmp) yang masuk ke router melalui IP tersebut maka akan di drop. Sebenarnya ada cara lain dengan menggunakan address list namun saya pilih ini karena secara lebih simpel baik melalui CLI dan GUI. Sekarang silahkan uji dari komputer kalian apakah ping ke router masih bisa atau tidak.

Ether 2 – Logging

Sebenarnya saya cukup bingung dengan perintah yang satu ini. Di soal tertulis ***"Buat rule agar setiap akses ke router tercatat di logging"***. Ini maksudnya apakah log ketika pengguna masuk ke router atau log bagi semua aktivitas yang masuk ke router?



Jika maksdunya adalah log ketika pengguna masuk ke router maka ini sudah ada secara bawaan, silahkan cek log router teman-teman pastinya ada laporan ketika pengguna masuk dengan laporan berhasil atau tidak. Sedangkan jika log semua aktivitas maka pada menu log akan sangat banyak baris yang tercipta. Dimana nantinya khawatir baris yang berfungsi sebagai bahan analisa malah "tenggelam".

Tetapi di luar itu saya coba menangkap mungkin maksud ke 2 yang benar, yaitu semua aktivitas yang masuk ke router yang dicatat. Jadi kita akan membuat *rule* nya, tetapi satu hal yang harus teman-teman ketahui inti dari *rule* ini adalah aktifitas yang sesuai akan masuk ke dalam LOG.

LOG

```
1 /ip firewall filter
2 add chain=input log=yes log-prefix=login
```

Perhatikan di situ ada log=yes dan itulah yang menjadi fokus teman-teman, ketika nanti soalnya diganti atau diperbaharui semoga kalian bisa. Oh yaa arti log-prefix di perintah tersebut adalah untuk memberi tanda di LOG bahwa yang menggunakan kata **login** sebagai prefix merupakan log yang dibuat oleh aturan firewall yang kita masukkan.

Kepada Bapak/Ibu guru, untuk bagian ini alangkah baiknya diganti saja menjadi aktivitas lain yang dimasukkan ke dalam log. Contohnya adalah aktivitas ping ke router.

Ether 2 – Rule HTTP dan HTTPS

Ini juga membuat saya bingung, karena secara bawaan ketika saya mengaktifkan fitur NAT maka secara otomatis pengguna dari **CLIENT Network** bisa mengakses ke internet. Namun saya ada pandangan lain, dimana mungkin maksudnya adalah CLIENT Network ke Internet hanya diizinkan mengakses HTTP & HTTPS saja dan akses lain seperti PING akan diblokir.

Menginzinkan hanya **web** yang bisa **diakses**

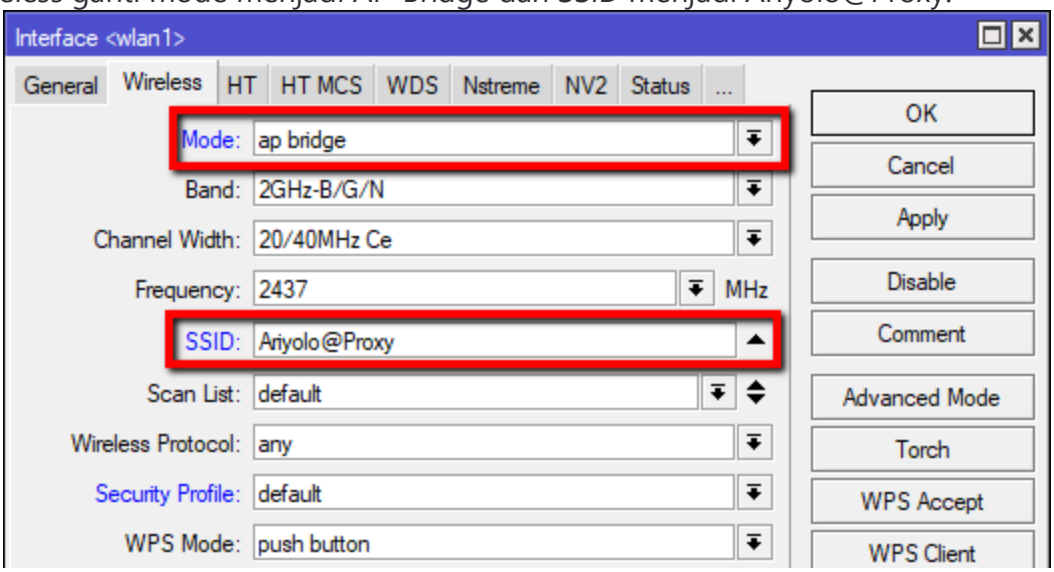
```
1 /ip firewall filter
2 add action=drop chain=forward dst-port=80,443 in-interface=ether2 out-interface=ether1 protocol=tcp
```

Sekarang silahkan kalian coba akses www.google.com (80 & 443) dari peramban, seharusnya bisa berjalan dengan baik. Lalu setelah itu coba akses ke ftp://ftp.itb.ac.id/ (port 21) dan seharusnya yang menggunakan port 21 tidak bisa diakses.

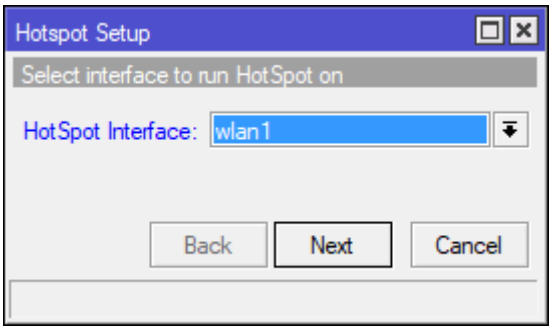
WLAN 1 – Hotspot

Sebenarnya pada soal di bagian wireless tidak ada kata-kata hotspot, namun jika dilihat dari topologi ada tulisan hotspot yang di wlan1 dan non hotspot di ether2. Jadi saya beranggapan bahwa di soal ini ada maksud bahwa wlan1 digunakan sebagai hotspot login namun tidak didefinisikan lebih lanjut lagi.

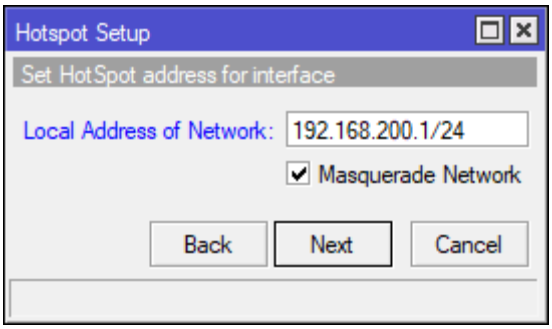
Sebelum membuat hotspot, kita akan ubah dulu mode wlan1 menjadi pemancar atau AP-Bridge. Teman-teman bisa menuju ke menu **Interfaces > tab interface > wlan1** lalu pada tab wireless ganti mode menjadi AP-Bridge dan SSID menjadi Ariyolo@Proxy.



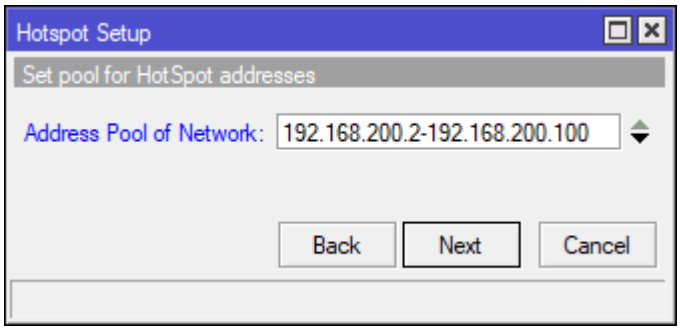
Jika wlan1 sudah menjadi pemancar maka selanjutnya tinggal tahapan hotspot. Silahkan menuju ke IP > Hotspot > tab Server > Hotspot Setup. Lalu pilih antarmuka yang akan dijadikan hotspot, dalam hal ini adalah wlan1.



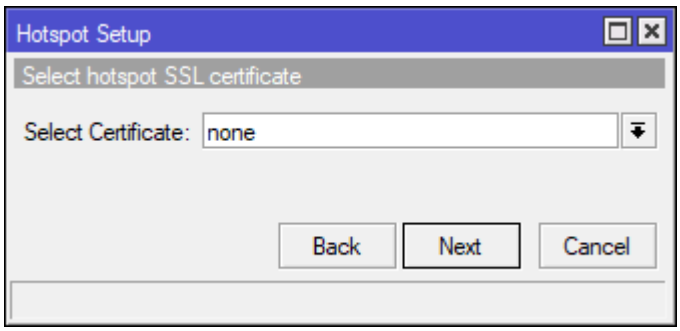
Di tampilan selanjutnya Untuk alamat IP akan menyesuaikan dengan IP yang telah kita isi di awal-awal pembahasan. Selanjutnya yang dilakukan adalah *unchecklist* pada ***Masquerade Network*** karena kita telah membuat NAT Masquerade di awal pembahasan pada **Ether1 – Internet Gateway**.



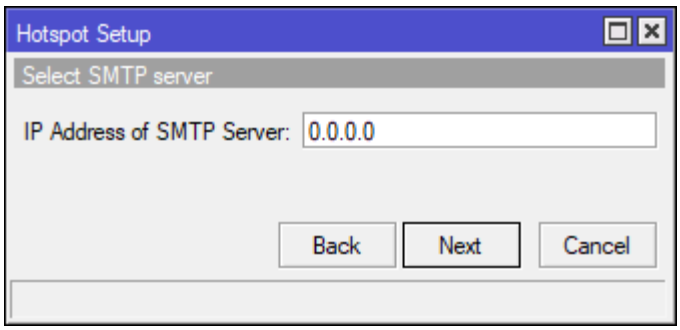
Untuk address pool ubah dari 192.168.200.2 – 192.168.200.254 menjadi hanya sampai 100 saja agar sesuai dengan soal.



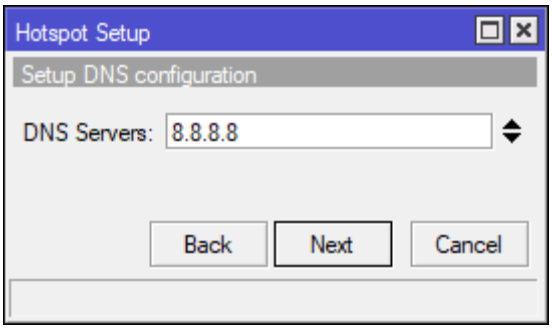
Selanjutnya karena kita tidak memiliki sertifikat SSL maka pada tampilan ini pilih Next saja.



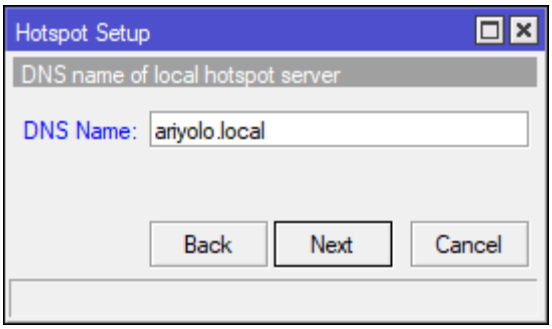
IP Address of SMTP Server biarkan saja dan langsung pilih Next karena kita tidak menggunakannya.



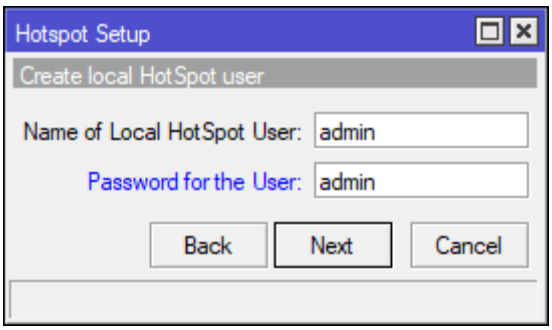
Untuk DNS secara otomatis akan menyesuikan dengan yang ada di pengaturan DNS dari router. Pada bagian ini juga sama, yaitu diamkan saja.



Pada tahapan selanjutnya teman-teman diminta untuk memasukkan domain yang akan digunakan untuk mengakses portal hotspot. Contoh pada kali ini saya isi dengan **ariyolo.local**



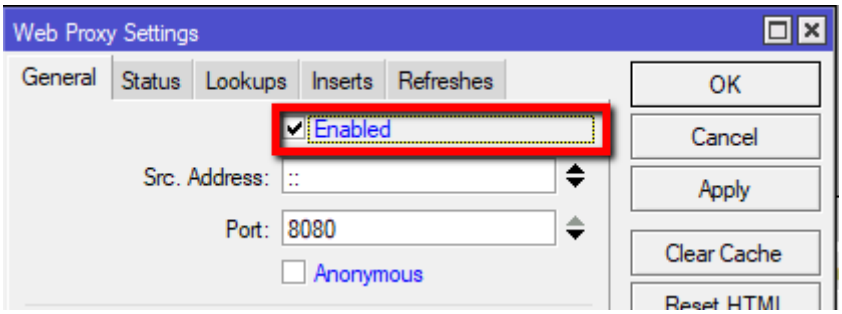
Tahapan terakhir adalah menentukan nama pengguna dan kata sandi yang bisa digunakan untuk masuk ke dalam hotspot. Karena tidak ada ketentuan seperti soal-soal UPK paket atau tahun yang lain jadi biar cepat saya isi seperti di bawah ini saja.



Jika telah selesai silahkan untuk masuk ke hotspot portal dan pastikan teman-teman bisa mengakses Internet.

Wlan 1 – Proxy

Untuk mengaktifkan Proxy cukup mudah yaitu dengan pergi ke **IP > Proxy** lalu pada **tab General** lakukan *checklist* pada pilihan Enable maka Proxy akan berjalan pada *port* 8080. Pada **kolom cache administrator** jangan lupa mengisi ariyolo@sekolah.sch.id, karena itu ada di soal.



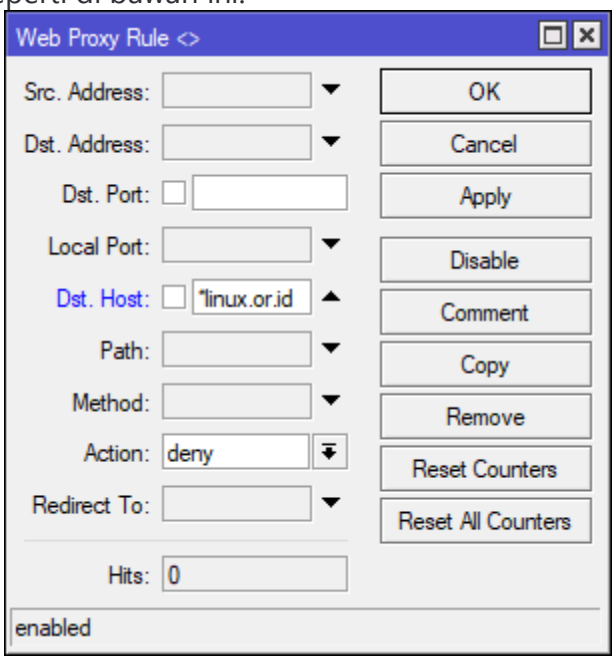
Sampai saat ini proxy telah aktif, namun agar pengguna bisa terkena efek dari Proxy ini pengguna harus melakukan pengaturan pada perampan mereka. Cara lain agar pengguna bisa otomatis terkeda dampak dari Proxy adalah dengan menggunakan bantuan *rule* pada firewall untuk membuat **Transparent Proxy**. Caranya adalah dengan menggunakan perintah seperti di bawah ini (winbox menyesuaikan). Karena hanya wlan1 saja yang terkena dampaknya maka pada ***in-interface*** diisi wlan1.

Mengatur **Proxy** agar **Transparent**

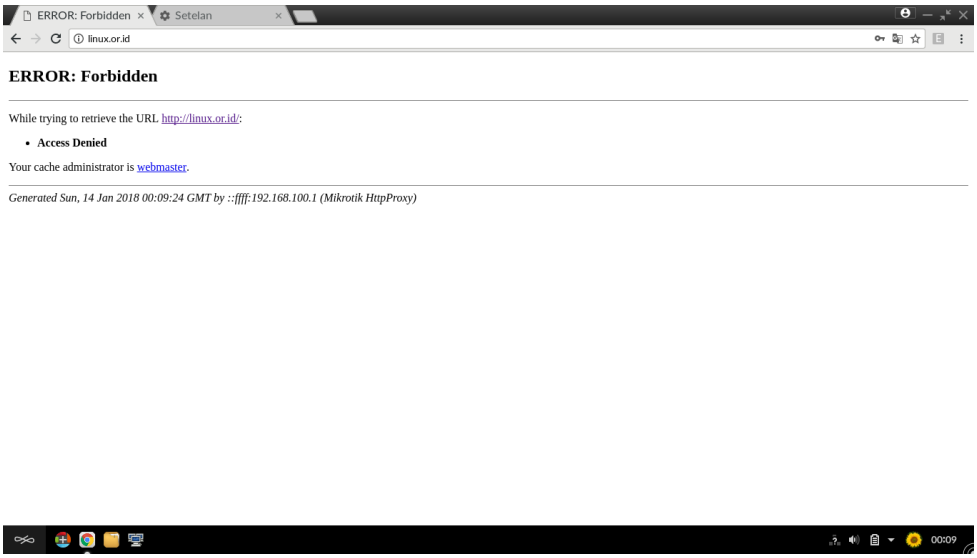
```
1 /ip firewall nat
2 add action=redirect chain=dstnat dst-port=80 in-interface=wlan1 protocol=tcp to-ports=8080
```

Wlan 1 – Pemblokiran Situs

Pemblokiran situs sebenarnya bisa menggunakan Firewall dan DNS Static, namun kalau dilihat-lihat tampaknya pembuat soal menginginkan kita menggunakan Proxy. Maka dari itu teman-teman silahkan pergi ke IP > Proxy > tab general > tombol access lalu tambahkan *rule* baru seperti di bawah ini.

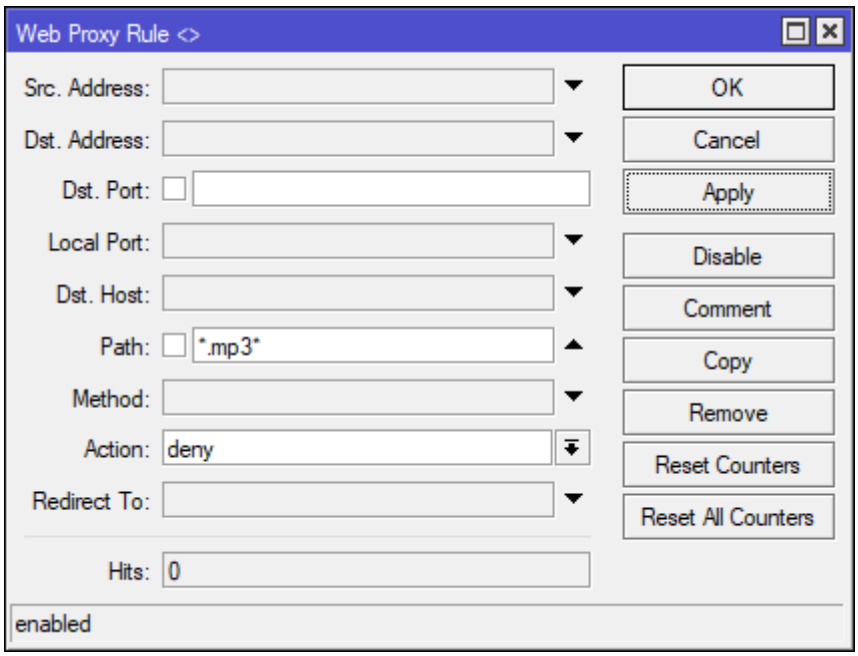


Mungkin ada dari teman-teman yang bertanya mengapa saya tidak mengisi kolom *redirects to*, alasannya adalah karena tidak ada perintah *redirect* pada soalnya . Jika telah selesai silahkan untuk membuka situs www.linux.or.id maka seharusnya tidak bisa dibuka dan muncul tampilan seperti di bawah ini.



Wlan 1 – Pemblokiran File

Untuk teknik pemblokiran yang digunakan kali ini adalah menggunakan Proxy maka itu teman-teman bisa menuju ke IP > Proxy > tab general > tombol access lalu tambahkan rule baru seperti di bawah ini.



Arti dari aturan di atas adalah bahwa setiap URL yang akan diproses oleh router jika mengandung esktensi mp3 maka akan diblokir atau ditolak. Sekarang teman-teman silahkan untuk mengunduh berkas mp3 untuk mengujinya, apakah berhasil atau tidak?

Wlan 1 – Pemblokiran Konten

Untuk pemblokiran konten kita tidak menggunakan Proxy lagi tetapi menggunakan Firewall. Intinya adalah ketika ada packet yang memiliki konten ***mikrotik*** maka oleh router akan langsung di tolak. Untuk pengunaannya bisa menggunakan perintah berikut ini.

Blokir Konten

```
/ip firewall filter
add action=drop chain=forward content=mikrotik
```

Silahkan diuji membuka dan melakukan ping pada mikrotik.com, harusnya sih tidak bisa .

Wlan 1 – Pembatasan Waktu

Sesuai dengan soal untuk pembatasan waktu kita akan menggunakan firewall. Perintahnya sudah saya buat di bawah ini. Ada alasan mengapa harus menggunakan 2 aturan, yaitu karena pada MikroTik fungsi waktu hanya berlaku dalam waktu 1 hari mulai 00:00:00 – 23:59:59. Maka dari itu saya membuat 2 aturan yang dimana aturan tersebut adalah pemblokiran dari wlan1 ke ether1 pada pukul **19:00:00 – 23:59:59** dan **00:00:00 – 07:00:00**.

Pembatasan Waktu

```
/ip firewall filter
add action=drop chain=forward in-interface=wlan1 out-interface=ether1 time=19h-23h59m59s,sun,mon,tue,wed,thu,fri,sat
add action=drop chain=forward in-interface=wlan1 out-interface=ether1 time=0s-7h,sun,mon,tue,wed,thu,fri,sat
```

Itu dia tadi pembahasan untuk UPK TKJ tahun pelajaran 2017/2018 yang menggunakan Paket 2. Memang agak sedikit membingungkan jika kita telaah kata-katanya, tetapi yaa sisanya tentu ada di tangan guru yang berhak mengubah soal-soal ini.