INTRA TRAINING CENTER

MIKROTIK MTCNA

LAB GUIDE

GNS3®

Kata Pengantar

Puji syukur Alhamdulillah, penulis panjatkan kehadirat Allah S.W.T atas ridha dan rahmat- Nya yang dilimpahkan sehingga pada akhirnya penulis dapat menyusun dan menyelesaikan buku ini yang berjudul “MTCNA LAB GUIDE”.

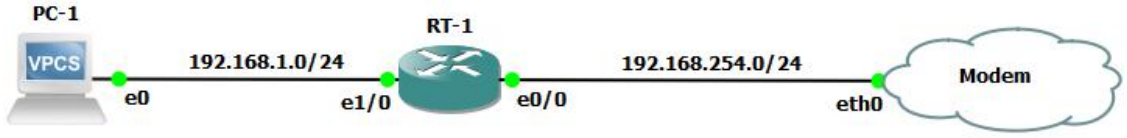
Melalui buku ini, saya ingin mengucapkan Terima kasih kepada mentor saya : Denny Darmawan. Atas dukungan dan motivasinya sehingga saya bisa menyelesaikan karya buku ini.

Dan juga saya ber-Terima Kasih banyak kepada Orang Tua dan Keluarga saya yang sudah mendidik saya semenjak lahir hingga besar sekarang, Guru-Guru saya semasa sekolah yang telah berjasa dan juga kepada para sahabat saya. Jika ada Saran, Kritik, Komentar & Review tentang buku ini silahkan kontak saya melalui andri.widiyanto17@gmail.com

Daftar Isi

Basic Configure RouterOS

Konfigurasi Interface




```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #    NAME                                TYPE       MTU L2MTU  MAX-L2MTU
 0  R  ether1                             ether      1500
 1  R  ether2                             ether      1500
 2  R  ether3                             ether      1500
 3  R  ether4                             ether      1500
 4  R  ether5                             ether      1500
```

Mengganti Interface

```
[admin@MikroTik] > interface set 0 name=Modem
[admin@MikroTik] > interface set 1 name=Client
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #    NAME                                TYPE       MTU L2MTU  MAX-L2MTU
 0  R  Modem                              ether      1500
 1  R  Client                             ether      1500
 2  R  ether3                             ether      1500
 3  R  ether4                             ether      1500
 4  R  ether5                             ether      1500
```

Menambahkan IP Address

```
[admin@MikroTik] > ip address add address=192.168.254.1/24 interface=Modem
[admin@MikroTik] > ip address add address=192.168.1.1/24 interface=Client
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK       INTERFACE
 0   192.168.254.1/24   192.168.254.0 Modem
 1   192.168.1.1/24     192.168.1.0   Client
```

Untuk menghapus IP Address bias menggunakan syntax **remove**.

```
[admin@MikroTik] > ip address remove 0
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS          NETWORK       INTERFACE
 0   192.168.1.1/24   192.168.1.0   Client
```

Menambahkan Gateway

Kita lanjutkan Konfigurasi Router nya agar terhubung dengan koneksi internet, sekarang kita akan melakukan konfigurasi Gateway. Gateway berfungsi sebagai ”gerbang” antara router dengan koneksi internet, yang mana nantinya Gateway ini kita isi dengan IP Address ISP (biasanya, ISP menggunakan IP Host pertama, contoh 192.168.100.1) dan dst-address (destination address / alamat tujuan) nya menggunakan IP 0.0.0.0/0 karena kita akan menghubungkan router dengan koneksi internet. Kita langsung saja ke langkah konfigurasinya.

```
[admin@MikroTik] > ip route add dst-address=0.0.0.0/0 gateway=192.168.254.1
```

Setelah itu, kita cek gateway yang tadi kita buat dengan menggunakan perintah : **ip route print** Bisa kita lihat di sebelah kiri terdapat symbol **A S** yang berarti *Active Static*

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 A S  0.0.0.0/0                         192.168.254.1          1
 1 ADC  192.168.137.0/24  192.168.137.2   ether1                 0
 2 ADC  192.168.254.0/24  192.168.254.2   ether1                 0
```

Menambahkan DNS Server

Setelah menambahkan default gateway, sekarang kita akan menambahkan DNS Server. Sekarang, kita langsung saja ke langkah konfigurasi nya :

Disini saya akan menggunakan DNS dari ISP (sama seperti gateway tadi, yaitu 192.168.254.1).

```
[admin@MikroTik] > ip dns set servers=192.168.254.1 allow-remote-requests=yes
```

> *(Allow Remote Requests disini berfungsi menjadikan Router sebagai DNS Server bagi client. Jadinya, Client tidak perlu menggunakan dns dari ISP lagi. Client Cukup menggunakan IP dari interface Router yang terhubung dengan Client (ether2). Karena nantinya Client akan diarahkan menuju DNS Server Router MikroTik)*

Kita sudah selesai mengatur IP Address, Gateway, DNS Server nya. Berarti sekarang, router sudah bisa terkoneksi dengan Jaringan Internet. Untuk melakukan pengujian,

Coba kita lakukan ping google.com pada router. Jika reply, artinya router telah terhubung dengan jaringan internet.

```
[admin@MikroTik] > ping google.com
HOST                    SIZE TTL TIME  STATUS
74.125.24.102             56  45 30ms
74.125.24.102             56  45 24ms
74.125.24.102             56  45 34ms
74.125.24.102             56  45 26ms
74.125.24.102             56  45 27ms
74.125.24.102             56  45 24ms
74.125.24.102             56  45 23ms
  sent=7 received=7 packet-loss=0% min-rtt=23ms avg-rtt=26ms max-rtt=34ms
```

Setelah router terhubung ke internet, sekarang kita akan melakukan konfigurasi di PC agar PC client juga mendapatkan koneksi internet dari router dengan menggunakan fitur NAT.

Konfigurasi NAT

Sekarang, kita akan melakukan konfigurasi agar PC Client dapat terhubung ke Internet melalui Router MikroTik. Kita akan menggunakan fitur NAT. NAT sendiri berfungsi untuk mengubah IP Address private menjadi IP Address public. Dan Masquerade sendiri berfungsi untuk "menyamarkan" IP Address client dan menggantinya dengan IP Address router. Jadi, pada saat PC client melakukan browsing di internet, web server tidak akan mengetahui IP dari client,

```
[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade out-interface=ether1
```

Sekarang, kita akan mengganti IP Client menjadi Static, dan menggunakan IP yang 1 network dengan IP ether2 (192.168.1.1/24).

Setelah itu, kita ganti IP Address client menjadi static dengan menggunakan IP Address yang satu network dengan IP Address ether2 (192.168.1.1/24) berarti kita isi dengan IP 192.168.1.2/24

```
PC1> ip 192.168.1.2 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1
```

Setelah mengganti IP Address client nya, seharusnya Client telah berhasil terkoneksi dengan jaringan Internet. Coba kita test dengan melakukan *browsing* atau coba *ping* google.com melalui CMD pada PC client. Jika reply, berarti berhasil.

```
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=56 time=60.456 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=56 time=94.580 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=56 time=194.734 ms
```

Merubah System Identity MikroTik

Setelah kalian menghubungkan routerboard ke internet, sekarang kita akan merubah Identitas / nama dari routerboard kita. Kita bisa lihat identitas routerboard di Terminal saat kita mengetikkan perintah text (CLI), yaitu **[admin@*MikroTik*] >** yang saya beri garis bawah, itulah identitas dari router, defaultnya bernama "MikroTik". Sedangkan *"admin"* adalah user yang kita gunakan pada router mikrotik tersebut, kita akan bahas selanjutnya. Kita bisa merubah identitas system dengan cara :

```
[admin@MikroTik] > system identity set name=RT-Pusat
[admin@RT-Pusat] >
```

Manajemen User di MikroTik

Setelah tadi kita merubah identitas router MikroTik, kita juga bisa menambah / menghapus user yang dapat mengakses Router. Pada konfigurasi default, MikroTik hanya mempunyai satu user, yaitu **admin** dan tidak memiliki password. User pada MikroTik sendiri mempunyai *Group* atau Hak akses yang dapat di lakukan oleh User tersebut. Diantaranya :

- ***Full* =** User dengan hak akses full bisa melakukan semua konfigurasi di router MikroTik. Dan bisa menambah/menghapus User.
- ***Write* =** User dengan hak akses write hanya bisa melakukan konfigurasi (menulis), dan tidak bisa menambah / menghapus user yang ada
- ***Read* =** User dengan hak akses Read hanya bisa melihat konfigurasi di Router MikroTik saja. Tidak bisa melakukan konfigurasi apapun.
-

Untuk menambahkan user baru, dengan cara berikut :

```
[admin@RT-Pusat] > user add name=andri group=write password=admin address=192.168.1.2
[admin@RT-Pusat] > user print
Flags: X - disabled
 #   NAME              GROUP             ADDRESS
 0   ;;; system default user
     admin             full
 1   andri             write             192.168.1.2/32
```

Untuk menghapus user bias menggunakan cara berikut :

```
[admin@RT-Pusat] > user remove 1
[admin@RT-Pusat] > user print
Flags: X - disabled
 #   NAME              GROUP             ADDRESS
 0   ;;; system default user
     admin             full
```

NTP Client

Setelah mengatur user, sekarang kita masuk ke pembahasan *NTP*. Pengaturan Waktu pada Router MikroTik itu sangat penting jika kalian mengkonfigurasi router MikroTik untuk bekerja di waktu tertentu (misalkan memblokir situs di jam jam tertentu). Pengaturan NTP client ini tidak usah dilakukan jika kalian menginstall / menggunakan RouterOS di PC. Karena PC mempunyai baterai cmos untuk menyimpan waktu. Sekarang, kita mulai ke langkah konfigurasi nya.

Sebelum itu, Router MikroTik kita harus terkoneksi dengan internet dan mengetahui IP dari NTP Server nya. Untuk waktu Indonesia sendiri, ada beberapa server yang bisa digunakan, yaitu :

0.id.pool.ntp.org = 203.160.128.59

1.id.pool.ntp.org = 119.2.43.91

Kita bisa menggunakan 1 (primary) atau 2 (Primary & Secondary) Untuk perintah text (CLI) nya sebagai berikut :

```
[admin@RT-Pusat] > system ntp client set enabled=yes primary-ntp=203.160.128.59
```

Setelah mengatur NTP Client, sekarang kita mengatur Zona Waktu. Zona waktu tergantung dimana kalian tinggal, WIB (Asia/Jakarta), WIT (Asia/Jayapura), WITA (Asia/Makassar). Atau kita juga bisa menggunakan fitur *auto detect* pada Router MikroTik untuk mendeteksi otomatis zona waktu tempat kalian tinggal, jika kalian tidak tau Zona waktu tempat kalian tinggal. Bisa dilakukan dengan perintah

```
[admin@RT-Pusat] > system clock set time-zone-name=Asia/Jakarta
```

Untuk melakukan pengecekan, kita bisa gunakan perintah :

```
[admin@RT-Pusat] > system clock print
        time: 19:25:19
        date: jul/09/2017
  time-zone-name: Asia/Jakarta
     gmt-offset: +07:00
```

Pengaturan waktu sudah selesai. Sekarang, *selama Router masih terkoneksi dengan NTP Server*, maka waktu tidak akan lagi kembali ke waktu default meskipun router di *reboot*.

Backup & Restore

Setelah tadi kita melakukan berbagai konfigurasi, sekarang kita akan melakukan *backup* konfigurasi yang sudah kita konfigurasikan tadi, lalu *restore* jika sewaktu-waktu kita membutuhkan nya. Jadi, sudah tau kan maksud dari *Backup & Restore?* Backup itu berfungsi untuk menyimpan hasil konfigurasi, dan Restore itu *kebalikan nya*, yaitu untuk mengembalikan konfigurasi yang sudah di *backup*.

Kita bisa melakukan Backup konfigurasi pada Router MikroTik. Perintahnya adalah :

```
[admin@RT-Pusat] > system backup save name=temp_andri
Saving system configuration
Configuration backup saved
```

Jika melakukan restore melalui perintah text bisa dilakukan dengan perintah :

```
[admin@RT-Pusat] > system backup load name=temp_andri.backup
Restore and reboot? [y/N]:
y
Restoring system configuration
System configuration restored, rebooting now
```

Soft Reset Configure

Setelah membackup dan melakukan restore pada konfigurasi, jika kalian ingin melakukan reset pada router pada konfigurasi bawaan pabrik,

```
[admin@RT-Pusat] > system reset-configuration
Dangerous! Reset anyway? [y/N]:
y
system configuration will be reset
```

Hard Reset Configure

Maksud dari Hard Reset ini, kita melakukan reset konfigurasi pada Router melalui *hardware* nya itu sendiri, tidak melalui software atau perintah. Kita langsung ke langkahnya.

1. Pertama, kalian lihat pada Routerboard lalu kalian cari tombol reset. Biasanya ada di samping power chord atau disamping slot Ethernet. (tombolnya kecil, biasanya tersembunyi. Jadi harus pakai pulpen atau lidi untuk menekan nya)

2. Pastikan routerboard dalam keadaan mati, dan tidak ada kabel yang tersambung..
3. Tekan tombol resetnya, sambil colokan routerboard dengan kabel adapter.
4. Sambil menekan tombolnya, coba lihat lampu LED / ACT nya akan berkedip, tunggu lampu LED (ACT) nya sampai berhenti berkedip dan mati. Terus tekan tombol resetnya, sampai Lampu LED Ethernet menyala kemudian mati
5. Setelah lampu ethernetnya mati, cabut power adapter MikroTik nya.
6. Lalu, nyalakan kembali routernya. Maka, konfigurasi routerboard akan kembali default bahkan IP router sendiri berubah menjadi 0.0.0.0

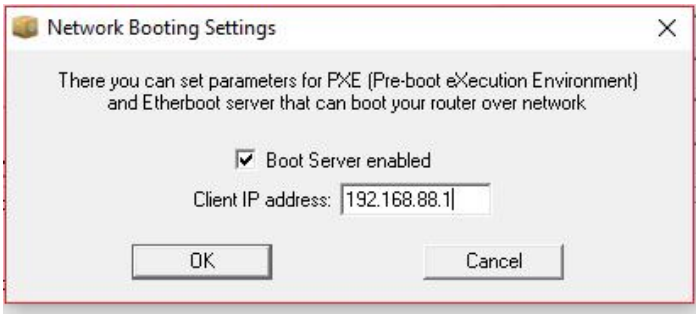
Netinstall

Sekarang kita akan menginstall ulang Routerboard dengan Netinstall. Netinstall ini berguna kalau misalkan lupa password , atau router gagal booting. Sebelum itu, kita siap kan dulu alat alatnya :

1. Routerboard yang akan di install ulang,
2. Software Netinstall (bisa di download di www.MikroTik.com/download),
3. Combined routerOS Package (download sesuai dengan tipe router nya. Disini saya contoh disini saya menggunakan router tipe *SMIPS*),
4. Kabel UTP Straight-throught,
5. PC atau Laptop.

Sekarang, jika alatnya sudah dipersiapkan, langsung saja menuju langkah konfigurasinya. :

1. Setting IP PC/Laptop menjadi IP Static misalkan 192.168.88.2,setelah itu sambungkan router dengan pc mengunakan kabel UTP di port 1
2. Buka Software Netinstall nya, klik **Netbooting** lalu ceklis **Boot Server enabled** setelah itu di bagian **Client IP Address**, isikan IP Routerboard setelah itu, klik OK

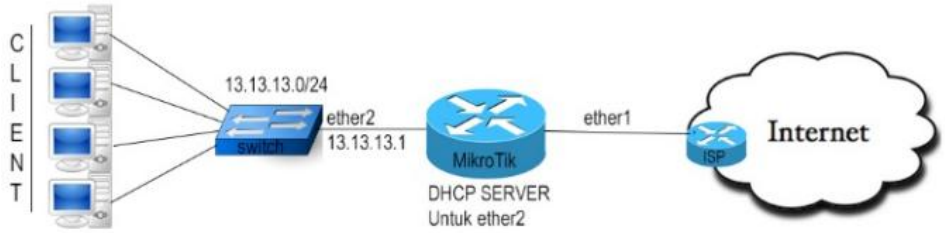


3. Klik tombol **Browse** , lalu cari dimana kalian menyimpan file routerOS all package tadi (.npk)
4. Matikan routerboard (cabut power adapternya), lalu reset routerboard (Hard Reset) dengan cara tekan tombol reset pada routerboard, tahan tombol reset. Sambal ditekan, kita nyalakan lagi routerboard (colokan power adapternya)
5. Nanti akan terdeteksi MAC Address dari router tersebut. Lalu lepaskan tombol resetnya
6. Klik MAC Addressnya, lalu pilih paket yang akan di install (select All saja), setelah itu,klik Install
7. Setelah install selesai, klik tombol Reboot. Instalasi selesai.

DHCP

DHCP atau Dynamic Host Control Protocol berfungsi untuk memberikan *IP Address, DNS , Gateway* otomatis dari Server kepada Client. Pada Bab ini kita akan membahas langkah konfigurasi *DHCP Server, DHCP Client, dan beberapa pengelolaan DHCP Server* pada router MikroTik.

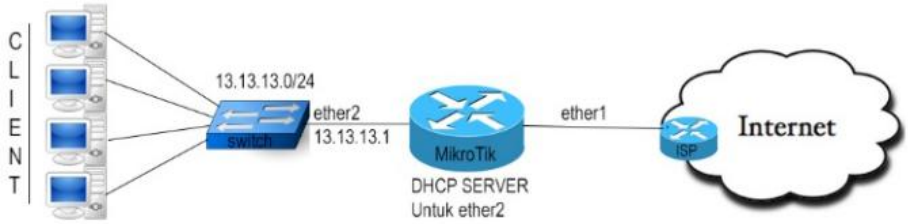
Pada MikroTik sendiri, kita dapat membuat router menjadi DHCP Server untuk para Client, dan bisa juga Router MikroTik menjadi DHCP Client dan meminta *IP , DNS , Gateway* dari ISP atau dari router lain yang terhubung melalui jaringan *Ethernet* atau pun *Wireless*.



DHCP Server biasanya digunakan oleh penyedia *hotspot.* Sedangkan DHCP Client di router MikroTik bisa kalian pakai jika kalian *malas* mengkonfigurasi router dengan jaringan internet (ISP) atau jika kalian tidak tahu IP Address dari router ISP tersebut.

DHCP Server

Sekarang kita akan mengkonfigurasi DHCP Server pada MikroTik. Agar lebih jelas, bisa kita lihat gambar topologi dibawah ini



Bisa kita lihat gambar diatas, Router MikroTik bertindak sebagai DHCP Server bagi PC Client yang terhubung dengan Router melalui interface *ether2*

Sekarang kita langsung saja ke langkah konfigurasi nya :

```
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 192.168.1.0/24
Select gateway for given network

gateway for dhcp network: 192.168.1.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.2-192.168.1.254
Select DNS servers

dns servers: 8.8.8.8
Select lease time

lease time: 3d
```

Setelah itu, kita cek menggunakan perintah berikut :

```
[admin@MikroTik] > ip dhcp-server print detail
Flags: X - disabled, I - invalid
 0   name="dhcp1" interface=ether2 lease-time=3d address-pool=dhcp_pool1 bootp-
     support=static authoritative=after-2sec-delay
```

Untuk pengujian DHCP Server diatas, sekarang kita coba ganti IP Address Client menjadi Dynamic.

```
PC1> ip dhcp
DORA IP 192.168.1.254/24 GW 192.168.1.1
```

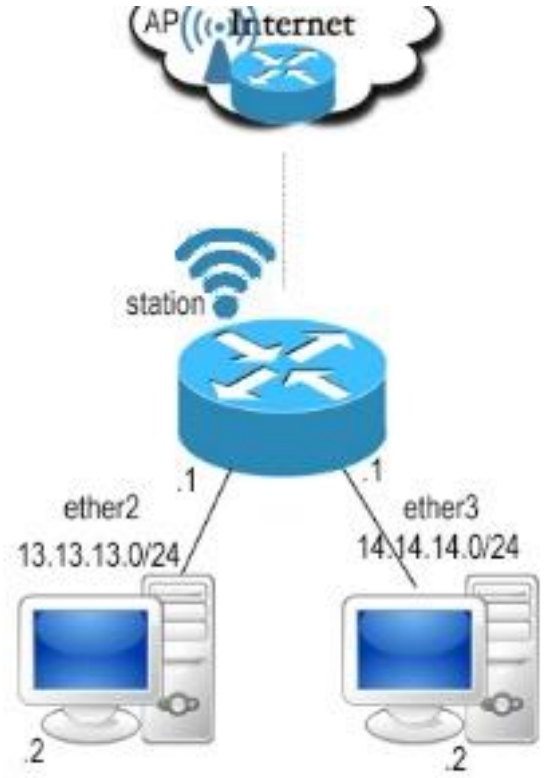
Bisa kita lihat gambar diatas, Client sudah mendapatkan IP DHCP dari Server (router)

Untuk melakukan pengecekan PC Client mana saja yang mendapatkan IP DHCP dari Client, bisa menggunakan perintah **ip dhcp-server lease print**

```
[admin@MikroTik] > ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
 #    ADDRESS                 MAC-ADDRESS       HOST-NAME  SERVER  RATE-LIMIT  STATUS
 0 D 192.168.1.254           00:50:79:66:68:00 PC11       dhcp1                  bound
```

IP Pool

IP Pool adalah suatu kumpulan IP Address yang akan diberikan pada Client. Jadi, selain mengkonfigurasi IP DHCP secara manual, kita bisa juga menggunakan fitur IP Pool. Nantinya fitur IP Pool ini bisa digunakan pada konfigurasi DHCP Server ataupun konfigurasi PPP Secret pada pembahasan PPPoE dan PPTP. Sebelum mengkonfigurasi kan IP Pool, kita lihat dulu gambar topologi dibawah ini



Terlihat pada gambar diatas, terdapat 1 router dengan 2 jaringan local. Kita lihat pada router 1, terdapat 2 network yang terhubung, 1 melalui interface *ether2* dengan ip network 13.13.13.0/24 dan yang 1 nya lagi melalui *ether3* dengan IP network 14.14.14.0/24. Disini kita akan mengkonfigurasi kan IP Pool untuk kedua network tersebut. Disini saya akan memberi nama ***pool1*** untuk *ether2* dan ***pool2*** untuk *ether3*. Untuk langkah konfigurasi melalui perintah text (CLI) adalah sebagai berikut :

Sebagai contoh, disini saya akan memberikan 4 IP Address untuk PC Client. Berarti, perintahnya adalah sebagai berikut

```
[admin@MikroTik] > ip pool add name=pool1 range=13.13.13.2-13.13.13.5
[admin@MikroTik] > ip pool add name=pool1 range=14.14.14.2-14.14.14.5
```

Setelah IP Pool kita buat, sekarang kita akan coba mengimplementasi kan IP Pool kepada konfigurasi DHCP Server. Tetapi, sebelum kita lakukan konfigurasi DHCP Server, kita harus mengatur DHCP Server Network nya terlebih dahulu, karena router 2 memiliki dua network yang terhubung (*ether2 dan ether3*). Untuk langkah konfigurasi nya adalah sebagai berikut :

Untuk network ether2

```
[admin@MikroTik] > ip dhcp-server network add address=13.13.13.0/24 dns-server=13.13.13.1
gateway=13.13.13.1
```

Untuk network ether3

```
[admin@MikroTik] > ip dhcp-server network add address=14.14.14.0/24 dns-server=14.14.14.1
gateway=14.14.14.1
```

Setelah kita melakukan konfigurasi dhcp-server network diatas, barulah sekarang kita melakukan konfigurasi DHCP Server pada router2. Untuk konfigurasi DHCP Server nya adalah sebagai berikut :

Untuk network 1 (*ether2*)

```
[admin@MikroTik] > ip dhcp-server add name=net1 address-pool=pool1 interface=ether2 lease-
time=00:30:00 disabled=no
```

Untuk network 2 (*ether3*)

```
[admin@MikroTik] > ip dhcp-server add name=net2 address-pool=pool2 interface=ether3 lease-
time=00:30:00 disabled=no
```

Sekarang, kita ubah IP Address dari PC Client menjadi Dynamic (automatis)

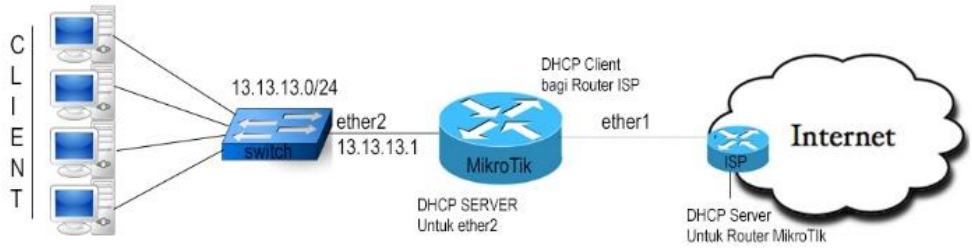
```
PC1> ip dhcp
DORA IP 13.13.13.5/24 GW 13.13.13.1
```

Konfigurasi DHCP Server kita sudah selesai. Untuk memonitoring siapa saja yang telah menggunakan IP Pool, bisa menggunakan perintah text (CLI) sebagai berikut :

```
[admin@MikroTik] > ip pool print
POOL            ADDRESS     OWNER           INFO
pool1           13.13.13.5  DHCP            00:50:79:66:68:00
```

DHCP Client

Sekarang kita masuk ke pembahasan DHCP Client. Jadi nantinya kita akan meminta *IP,DNS,Gateway* secara otomatis dari DHCP Server (ISP). Jika kalian menerapkan DHCP Client, maka nantinya kalian tidak dapat melakukan konfigurasi IP Address *ether1* secara manual. Dan nantinya *ether1* menggunakan IP Address, DNS, Gateway dari DHCP Server.



Untuk langkah konfigurasi nya adalah sebagai berikut :

Disini kita akan meminta DHCP dari ISP (DHCP Server), berarti interface nya kita pilih yang menyambung dengan koneksi internet, yaitu *wlan1*. Perintah Text (CLI) nya adalah sebagai berikut :

```
[admin@MikroTik] > ip dhcp-client add interface=ether1 disabled=no
```

setelah itu kita cek menggunakan **ip dhcp-client print .** Jika berhasil, maka status nya adalah **bound**.

```
[admin@MikroTik] > ip dhcp-client print
Flags: X - disabled, I - invalid
 #   INTERFACE                USE-PEER-DNS ADD-DEFAULT-ROUTE  STATUS      ADDRESS
 0   ether1                    yes          yes                bound       11.11.11.254/24
```

Setelah itu, kita cek apakah sudah mendapatkan IP, DNS, Gateway dari ISP. Perintah text nya adalah sebagai berikut :

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK       INTERFACE
 0 D 11.11.11.254/24    11.11.11.0    ether1
```

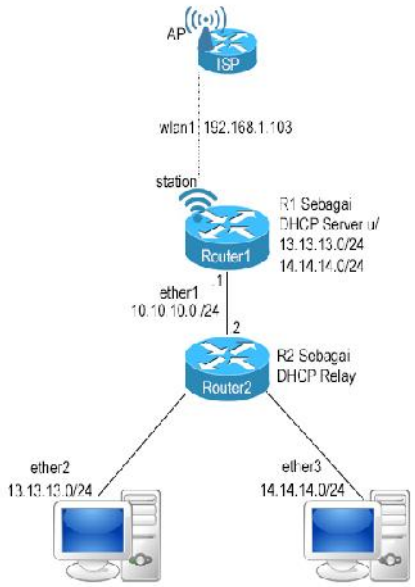
```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY          DISTANCE
 0 ADS  0.0.0.0/0                        11.11.11.1           1
 1 ADC  11.11.11.0/24     11.11.11.254   ether1               0
```

```
[admin@MikroTik] > ip dns print
                    servers:
          dynamic-servers: 8.8.8.8
 allow-remote-requests: no
    max-udp-packet-size: 4096
                cache-size: 2048KiB
            cache-max-ttl: 1w
               cache-used: 8KiB
```

Seperti kita lihat diatas, maka *ether1* akan mendapatkan IP, DNS, Gateway Dinamik (D) dari ISP. Gateway ADS yang berarti *Active Dynamic Static*

DHCP Relay

DHCP Relay berfungsi sebagai Proxy untuk menerima request permintaan IP Address dari PC Client (DHCP Request) dan nanti akan meneruskan DHCP Request tersebut kepada DHCP Server. Jadi nantinya DHCP Server hanya terpusat pada 1 router saja, tanpa harus kita konfigurasi kan DHCP Server kepada router 1 per 1. Agar lebih jelas, kita bisa lihat topologi dibawah ini :



Seperti kita lihat diatas, terdapat 2 router MikroTik tersambung melalui interface ether1. Router 1 nantinya akan berperan sebagai DHCP Server, lalu Router 2 akan menjadi DHCP Relay. Router 1 nantinya akan menjadi DHCP Server untuk semua jaringan local yang terhubung dengan router 2, *in this case* yaitu 13.13.13.0/24 dan 14.14.14.0/24. Kita langsung saja ke langkah konfigurasi DHCP Server dan DHCP Relay

Pertama, kita akan konfigurasi kan dulu IP Pool pada Router 1 untuk masing masing network yang akan di berikan DHCP Server. (13.13.13.0/24 , 14.14.14.0/24)

Untuk *ether2* (13.13.13.0/24) disini saya hanya akan memberikan 4 range IP Address, yaitu 13.13.13.2-13.13.13.5 dengan nama *ether2.* Maka perintah nya adalah sebagai

```
[admin@MikroTik] > ip pool add name=ether2 range=13.13.13.2-13.13.13.5
```

Untuk *ether3* (14.14.14.0/24) saya akan melakukan konfigurasi yang sama. 4 range IP Address, dengan nama *ether3*. Maka perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > ip pool add name=ether3 range=14.14.14.2-14.14.14.5
```

Setelah kita lakukan konfigurasi IP Pool, sekarang kita lakukan konfigurasi Network DHCP Server. Kita akan lakukan konfigurasi seperti berikut

Untuk *ether2*

```
[admin@MikroTik] > ip dhcp-server network add address=13.13.13.0/24 gateway=13.13.13.1
dns-server=13.13.13.1,10.10.10.1 ntp-server=10.10.10.1
```

untuk *ether3*

```
[admin@MikroTik] > ip dhcp-server network add address=14.14.14.0/24 gateway=14.14.14.1
dns-server=14.14.14.1,10.10.10.1 ntp-server=10.10.10.1
```

Setelah kita konfigurasi IP Pool dan Network DHCP Server pada router 1, sekarang kita akan lakukan konfigurasi DHCP Server nya. Untuk konfigurasi DHCP Server sendiri caranya sama seperti sebelumnya. Hanya saja, sekarang kita akan menambahkan perintah text *Relay* yang berisikan IP Address interface ether2 dan ether3 dari router2 yaitu 13.13.13.1 untuk ether2 dan 14.14.14.1 untuk ether3. Perintah nya adalah sebagai berikut :

```
[admin@MikroTik] > ip dhcp-server add name=ether2 interface=ether2 address-pool=ether2
relay=13.13.13.1 lease-time=00:03:00 disabled=no
[admin@MikroTik] > ip dhcp-server add name=ether3 interface=ether2 address-pool=ether3
relay=14.14.14.1 lease-time=00:30:00 disabled=no
```

Setelah itu kita cek menggunakan perintah berikut :

```
[admin@MikroTik] > ip dhcp-server print
Flags: X - disabled, I - invalid
 #   NAME       INTERFACE       RELAY        ADDRESS-POOL     LEASE-TIME ADD-ARP
 0   ether2       ether2        13.13.13.1    ether2           3m
 1   ether3       ether2        14.14.14.1    ether3           30m
```

Konfigurasi pada router 1 sudah selesai, sekarang kita akan melakukan konfigurasi *DHCP Relay* pada router2. Untuk melakukan konfigurasi nya sendiri bisa melalui perintah text (CLI), perintahnya adalah sebagai berikut

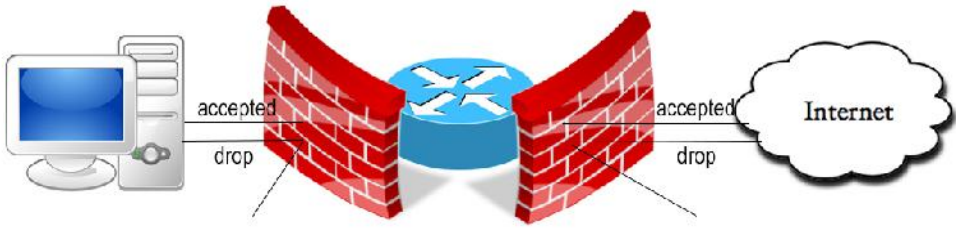
```
[admin@MikroTik] > ip dhcp-relay add name=relay1 interface=ether2 dhcp-server=10.10.10.1
local-address=13.13.13.1 disabled=no
[admin@MikroTik] > ip dhcp-relay add name=relay1 interface=ether3 dhcp-server=10.10.10.1
local-address=14.14.14.1 disabled=no
```

Firewall

Firewall adalah system pengaman (keamanan) yang memeriksa paket data yang keluar dan yang masuk. Dengan Firewall, kita bisa melindungi jaringan kita (local) dari serangan jaringan luar. Misalkan, melindungi jaringan LAN kita dari internet.

Firewall bisa digunakan untuk memblokir sebuah situs yang akan diakses oleh suatu client. Misalkan situs Pornografi, atau situs-situs perjudian. Firewall ini sangat berguna jika kalian mempunyai warnet. Agar client tidak sembarangan membuka situs-situs terlarang, apalagi yang membuka masih anak kecil.

Untuk mengetahui contoh cara kerja Firewall, kita bisa lihat Topologi sederhana dibawah ini



Kita langsung saja ke pembahasan pertama, yaitu Firewall NAT

Firewall NAT Menggunakan Masquerade

Maksud dari judul diatas adalah membatasi IP Address (client) yang hanya boleh terkoneksi dengan jaringan Internet melalui Router MikroTik. Cara ini hampir sama seperti yang dibahas sebelumnya (konfigurasi NAT) hanya saja, disini Source Address nya kita isi dengan IP client yang boleh menggunakan koneksi internet.

Untuk langkah konfigurasi menggunakan perintah berikut :

Sekarang, kita akan coba buat rule hanya IP yang mempunyai network 13.13.13.0/24 yang bisa terkoneksi dengan jaringan Internet. Perintah Text (CLI) nya

```
[admin@MikroTik] > ip firewall nat add chain=srcnat src-address=13.13.13.0/24 out-
interface=ether1 action=masquerade
```

Setelah dibuat, kita cek dengan perintah **ip firewall nat print**

```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade src-address=13.13.13.0/24 out-interface=ether1
```

Setelah rule diatas dibuat, jadi hanya PC Client dengan IP Network 13.13.13.0/24 saja yang hanya bisa terkoneksi dengan Jaringan Internet melalui Router MikroTik

Sekarang kita coba membuat rule, jadi hanya IP Client 13.13.13.1-13.13.13.10 saja yang bisa terkoneksi dengan Internet. Tetapi sebelum itu, **kita harus menghapus Rule firewall yang sebelumnya.** Karena MikroTik membaca Rule dari atas kebawah, jadi kalau rule yang sebelumnya (13.13.13.0/24) masih ada, maka PC Client yang mempunyai IP dengan network tersebut (13.13.13.1-13.13.13.254) masih bisa menggunakan internet, jadinya firewall yang kita buat akan sia-sia. Untuk menghapus rule firewall nya, bisa gunakan perintah text sebagai berikut

```
[admin@MikroTik] > ip firewall nat remove 0
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
```

Bisa kita lihat diatas, Firewall Rules nya sudah kosong (tidak ada). Sekarang, kita lanjut buat firewall rules nya.

```
[admin@MikroTik] > ip firewall nat add chain=srcnat src-address=13.13.13.1-13.13.13.10 out-
interface=ether1 action=masquerade
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade src-address=13.13.13.1-13.13.13.10 out-interface=ether1
```

Bisa kita lihat diatas, firewall rule sudah kita buat. Sekarang, untuk melakukan pengujian pada *rule* yang kita buat tadi, Kita ganti IP Address PC Client selain IP 13.13.13.1-13.13.13.10. Sebagai contoh disini saya akan menggunakan IP Address

```
PC1> ip 13.13.13.11 255.255.255.0 13.13.13.1
Checking for duplicate address...
PC1 : 13.13.13.11 255.255.255.0 gateway 13.13.13.1

PC1> save
Saving startup configuration to startup.vpc
.  done
```

Setelah itu, kita coba ping google.com dengan PC tersebut. Maka hasilnya akan RTO karena tidak terhubung dengan jaringan internet

```
C:\Users\Windows 8>ping google.com

Pinging google.com [172.217.24.110] with 32 bytes of data:
Request timed out.
Request timed out.
```

Jika RTO, berarti rule yang kita buat sudah selesai. Jadi, hanya client yang mempunyai IP 13.13.13.1-13.13.13.10 saja yang bisa terhubung dengan koneksi internet

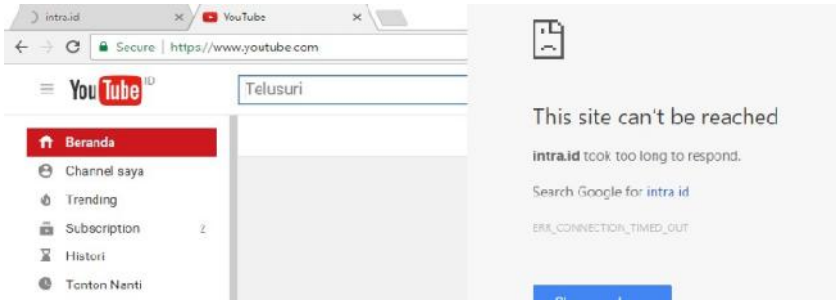
Firewall NAT Masquerade Port Tertentu

Masih di materi masquerade, sekarang kita akan melakukan masquerade pada port tertentu. Konfigurasinya hampir sama, hanya saja nanti kita akan mengisi bagian protocol dan dst-port. Misalnya, jika kalian ingin membatasi client hanya bisa melakukan browsing, berarti kalian isi HTTP (port 80) dan HTTPS (port 443) di dst-port dan pilih protocol nya tcp. Sekarang, langsung saja kita coba praktekan. Disini, saya akan membatasi client hanya bisa browsing website yang menerapkan HTTPS. Berarti client tersebut tidak bisa browsing website dengan HTTP. Sebelumnya, kita hapus dulu rules yang sebelumnya, atau bisa juga diedit (melalui Winbox).

```
[admin@MikroTik] > ip firewall nat add chain=srcnat src-address=13.13.13.1-13.13.13.10 out-interface=ether1 protocol=tcp dst-port=443 action=masquerade
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade protocol=tcp src-address=13.13.13.1-13.13.13.10 out-interface=ether1 dst-port=443
```

Setelah itu, untuk melakukan pengujian kita coba melakukan browsing menuju web yang menggunakan protocol https, misalnya **youtube**. Dan test browsing menuju web yang menggunakan protocol http, misalnya **intra.id**

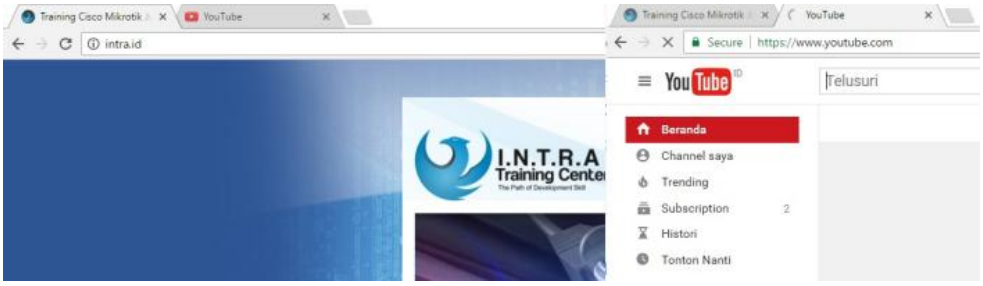
Bisa kita lihat gambar yang dibawah ini. Youtube berhasil terbuka, sedangkan intra.id tidak terbuka sama sekali.



Agar client juga bisa browsing web yang menggunakan protocol http, dibagian dst-port kita tambahkan port http, yaitu 80. rule seperti dibawah ini.

```
[admin@MikroTik] > ip firewall nat set 0 dst-port=80,443
```

Bisa kita lihat dibawah, sekarang web http (intra.id) nya bisa terbuka



Jika konfigurasi nya sudah dilakukan, maka sekarang PC Client hanya bisa browsing dan download melalui web dengan protocol port HTTP dan HTTPS. Tidak bisa menggunakan Yahoo Mesenger dan sebagainya karena port nya berbeda. Untuk menambahkan portnya, langkahnya sama seperti langkah konfigurasi diatas.

Firewall Filter Input & Forward

Firewall Filter ini berfungsi menyaring (*filter*) paket data yang masuk dan keluar dari jaringan dalam (local) atau dari jaringan luar (internet). Jadi, nantinya router akan menyaring data apa saja yang boleh masuk atau keluar. Firewall filter sendiri mempunyai 3 mode *(chain)* yaitu :

- ***Forward* =** Filter ini berfungsi untuk menangani paket data yang melewati router
- ***Input* =** Filter ini berfungsi untuk menangani paket data yang masuk ke router
- ***Output* =** Filter ini berfungsi untuk menangani paket data yang keluar dari router

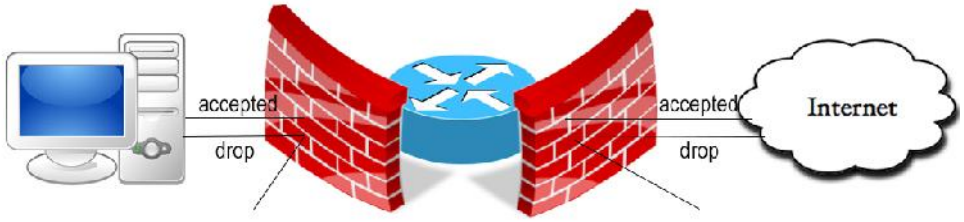
Disini saya hanya akan membahas filter *Input* dan *Forward*.

Firewall Chain Input

firewall input ini berfungsi untuk menangani paket data yang masuk ke dalam router, seperti melakukan konfigurasi pada router (seperti menambah IP address, dsb) maupun *ping* dari jaringan luar (internet) dan jaringan local. Di MikroTik sendiri, port untuk konfigurasi seperti *WinBox (8291), Telnet (23)* itu terbuka. Maksudnya, bisa di akses oleh siapa saja yang terkoneksi dengan router MikroTik tersebut. *Nah, bahaya kan kalau misalkan ada yang mengkonfigurasi router kita sembarangan?* Disinilah

contoh fungsi firewall input. Jadi nantinya kita bisa membatasi siapa saja yang bisa mengkonfigurasi routerboard.

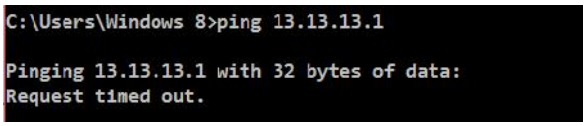
Agar lebih paham, Kita bisa lihat cara kerja dari Firewall Input pada gambar dibawah ini



Sekarang kita akan melakukan percobaan *drop* semua paket data yang masuk ke router. Langsung ke langkah konfigurasi nya. perintahnya adalah sebagai berikut :

```
[admin@MikroTik] > ip firewall filter add chain=input action=drop
```

Sekarang untuk melakukan percobaan, lakukan *ping* dari pc client menuju router.



Bisa kita lihat gambar diatas, hasilnya akan RTO karena semua data yang masuk kedalam router akan di drop.

Cara diatas hanya untuk percobaan saja dan bertujuan untuk mengerti cara kerja dari firewall input.

Sekarang, kita akan coba membatasi siapa saja yang dapat mengakses *port* konfigurasi pada router MikroTik dari jaringan local (ether2). Disini saya akan coba membuat rule, jadi hanya PC Admin (dengan IP 13.13.13.2) yang bisa melakukan konfigurasi pada router MikroTik. Selain dari PC admin (contoh 13.13.13.3) tidak akan bisa melakukan konfigurasi pada router. Port konfigurasi pada MikroTik : Winbox (8291) , Telnet (23) , SSH (22) , WebFig (80), ftp (20 & 21)

```
[admin@MikroTik] > ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether2
action=accept

 [admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept src-address=13.13.13.2 in-interface=ether2
```

Sekarang, kita akan membuat action *drop* nya. Perintah text nya adalah

```
[admin@MikroTik] > ip firewall filter add chain=input in-interface=ether2 protocol=tcp dst-
port=8291,23,22,80,20,21 action=drop
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept src-address=13.13.13.2 in-interface=ether2

 1   chain=input action=drop protocol=tcp in-interface=ether2 dst-port=8291,23,22,80,20,21
```

Setelah itu, coba kalian buka melalui IP *selain* dari 13.13.13.2, maka akan di *drop*.

Dengan rule diatas, kita telah mengamankan konfigurasi router dari PC Client yang lain. Sekarang, bagaimana cara mengamankan port yang terbuka dari jaringan luar (internet)? Caranya sama, tetapi pada bagian *in-interface ,* kita isi dengan *interface* yang menuju ke Internet, yaitu *ether1*.

Karena MikroTik membaca Rule dari atas baru ke bawah, maka kita buat dulu *rule* dengan IP Address yang diperbolehkan mengakses router. Disini saya akan membuat IP Address 13.13.13.2 bisa mengakses port konfigurasi pada router. Maka perintah text (CLI) nya adalah sebagai berikut :

```
[admin@MikroTik] > ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether1
action=accept
```

Setelah itu, kita buat lagi rule yang kedua, yaitu rule *drop* perintahnya adalah :

```
[admin@MikroTik] > ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-
port=8291,23,22,80,20,21 action=drop
```

Untuk mengecek *rule* yang tadi telah kita buat, perintah text nya adalah :

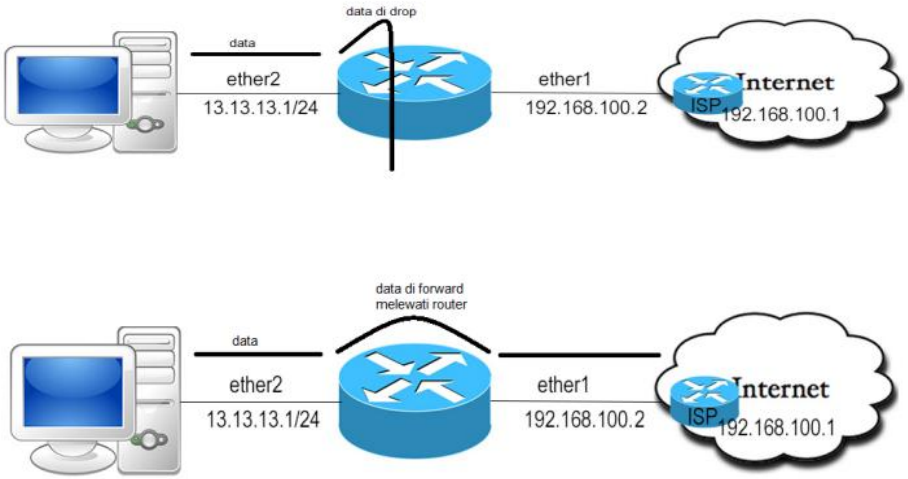
```
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept src-address=13.13.13.2 in-interface=ether1

 1   chain=input action=drop protocol=tcp in-interface=ether1 dst-port=8291,23,22,80,20,21
```

Sekarang, berarti hanya PC dengan IP 13.13.13.2/24 saja yang bisa mengakses router melalui jaringan luar (internet)

Firewall Forward

Firewall Forward ini berfungsi untuk menangani paket data yang melewati (melintasi) router, baik dari jaringan local atau jaringan luar. Firewall Forward juga mengatur boleh / tidak nya suatu paket menuju jaringan internet atau jaringan local, jadi firewall forward ini bisa kita pakai untuk memblokir website yang akan di akses client. Menggunakan firewall forward hampir sama dengan menggunakan *srcnat* yang kita sudah bahas sebelumnya. Hanya saja, jika menggunakan *srcnat,* srcnat akan melakukan perubahan IP Address pada pengirim data. Tetapi, jika pada *firewall forward*, firewall forward hanya akan mengirim data dari si pengirim tanpa melakukan perubahan IP Address.

Untuk mengerti cara kerja firewall forward, kita akan melakukan percobaan blok akses internet pada client (*Drop*).



Langsung ke langkah konfigurasi nya, yaitu :

```
[admin@MikroTik] > ip firewall filter add chain=forward action=drop
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=drop
```

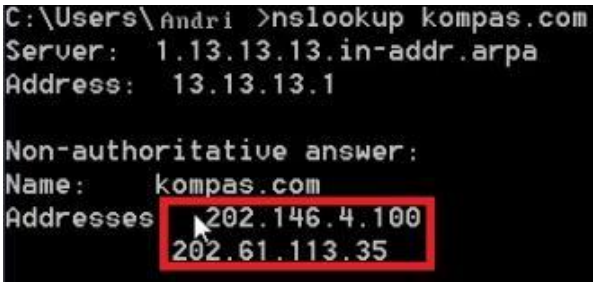
Setelah itu, kita test dengan cara ping dari pc client menuju internet, maka hasilnya akan RTO karena akses forward nya sudah kita *drop*. Rule diatas hanya untuk

percobaan saja, agar mengerti cara kerja dari firewall forward. Sebelum ke langkah selanjutnya, kita hapus dulu rule firewall forward drop ini.

Setelah itu, kita akan coba untuk blokir situs yang akan diakses client menggunakan firewall forward (berdasarkan IP)

Firewall Forward Blokir Website berdasarkan IP Address

Setelah kita melakukan percobaan Firewall Forward, sekarang kita coba memblokir situs dengan firewall forward. Disini kita akan memblokir website tersebut berdasarkan *IP Address* nya. Jadi, sebelum memblokir website tersebut, kita harus mengetahui IP Address dari website tersebut. Caranya, kita bisa menggunakan perintah **nslookup di** CMD atau CLI. Sebelum menggunakan nslookup, pastikan dulu pc sudah terhubung akses internet. Disini saya akan mencoba memblokir situs web kompas.com, berarti perintahnya adalah sebagai berikut : **nslookup kompas.com**

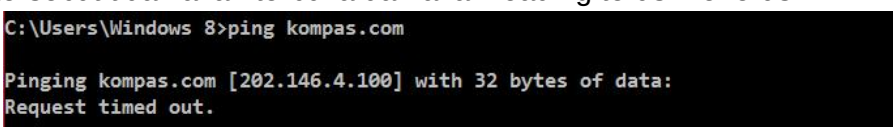


Bisa kita lihat diatas, kompas.com mempunyai 2 IP yang berbeda. Berarti kita harus membuat 2 rule dengan 2 IP tujuan (*dst-address)* yang berbeda untuk memblokir situs kompas.com tersebut. Langsung saja ke langkah konfigurasi nya :

Jika melalui perintah text (CLI), maka perintahnya :

```
[admin@MikroTik] > ip firewall filter add chain=forward dst-address=202.146.4.100 action=drop
[admin@MikroTik] > ip firewall filter add chain=forward dst-address=202.61.113.35 action=drop
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=drop dst-address=202.146.4.100

 1   chain=forward action=drop dst-address=202.61.113.35
```

Rule sudah dibuat, sekarang kita coba buka kompas.com atau lakukan *ping*, maka website tersebut tidak akan terbuka dan akan loading terus menerus.



Kita sudah berhasil memblokir website kompas. Tetapi dengan cara ini, mungkin sedikit *repot* karena harus mengetahui IP address dari website tersebut. Ada cara yang mungkin lebih *efisien,* yaitu memblokir situs berdasarkan content website.

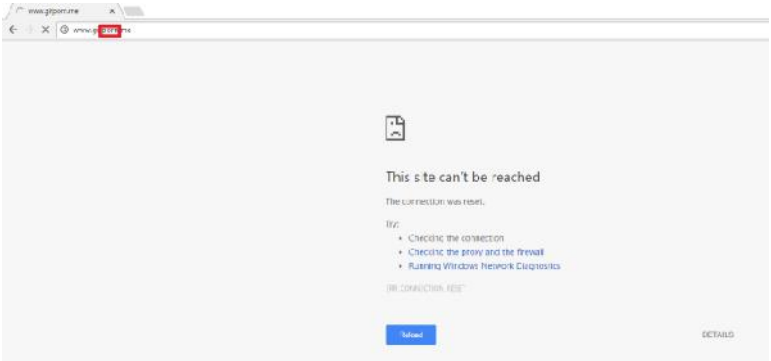
Firewall Forward Blokir Website Berdasarkan Konten

Sekarang kita akan mencoba memblokir situs berdasarkan konten nya. Menggunakan fitur konten ini juga bisa untuk memblokir *download* suatu ekstensi file (contoh .3gp) agar user tidak sembarangan download yang bukan-bukan. Sekarang langsung ke langkah konfigurasi :

Disini, saya akan coba membuat 2 rule untuk memblokir content **porn** dan juga ekstensi **.3gp** Untuk perintah CLI berikut syntaksnya :

```
[admin@MikroTik] > ip firewall filter add chain=forward content=porn action=drop
[admin@MikroTik] > ip firewall filter add chain=forward content=.3gp action=drop
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=drop content=porn

 1   chain=forward action=drop content=.3gp
```

Rule diatas sudah dibuat. Berarti, siapa saja yang terkoneksi (termasuk admin) dengan router, maka tidak akan bisa mengakses website yang mengandung content “porn” dan “.3gp”.



Disini juga kita bisa menambahkan *src-address* nya. Jadi, hanya IP tertentu saja yang tidak boleh mengakses website yang mempunyai content tersebut. Disini saya akan coba menambahkan *src-address* , jadi hanya IP Admin saja yang bisa mengakses web yang berisi konten tersebut. Langkah konfigurasinya adalah sebagai berikut :

Disini saya contohkan IP Address yang dimiliki admin adalah 13.13.13.2/24 . Jadi sisanya adalah IP Address client (13.13.13.3-13.13.13.254) yang akan kita masukkan ke *src-address* :

```
[admin@MikroTik] > ip firewall filter add chain=forward src-address=13.13.13.2 action=accept
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop content=porn

 1    chain=forward action=drop content=.3gp
```

Setelah itu, kita pindahkan rule yang tadi kita buat menjadi urutan paling atas dengan menggunakan perintah **ip firewall move 2 0**

```
[admin@MikroTik] > ip firewall filter move 2 0
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address=13.13.13.2

 1    chain=forward action=drop content=porn

 2    chain=forward action=drop content=.3gp
```

Sekarang, coba kita test mengakses website yang mempuyai content tersebut menggunakan PC dengan IP (13.13.13.2) maka akan berhasil. Sekarang, coba kita buka website dengan konten tersebut menggunakan PC selain dari IP 13.13.13.2 , maka akan gagal.

Address List

Address List adalah suatu fitur di MikroTik yang berfungsi untuk menandakan IP Address tertentu menjadi sebuah Nama. Misalkan disini saya akan membuat 2 Address List dengan IP Address 13.13.13.2 dan akan saya namai "*IP admin"* dan untuk IP Address 13.13.13.0/24 saya namai "*IP Client".* Langkah konfigurasinya

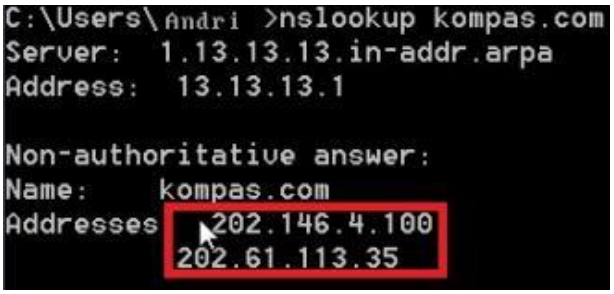
```
[admin@MikroTik] > ip firewall address-list add address=13.13.13.2 list="IP Admin"
[admin@MikroTik] > ip firewall address-list add address=13.13.13.0/24 list="IP Client"
[admin@MikroTik] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                ADDRESS
 0   IP Admin                            13.13.13.2
 1   IP Client                           13.13.13.0/24
```

Kita sudah buat Address List nya, sekarang kita akan coba menggunakan Address List nya. Misalkan disini kita akan buat pc admin mendapatkan semua akses internet, sedangkan PC client hanya bisa browsing dan tidak bisa mendownload file ber ekstensi **.iso** . Maka perintah textnya adalah sebagai berikut :

```
[admin@MikroTik] > ip firewall filter add chain=forward src-address-list="IP Admin" action=accept
[admin@MikroTik] > ip firewall filter add chain=forward src-address-list="IP Client" action=drop
 [admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address-list=IP Admin

 1    chain=forward action=drop src-address-list=IP Client
```

Kita bisa lihat diatas, di bagian *src-address* kita tidak perlu lagi masukkan IP Address dari pc admin, melainkan kita hanya perlu masukkan nama Address List nya saja. Address List juga bisa digunakan untuk memblokir website. Caranya sama seperti tadi, kita buat dulu Address List dari website yang ingin kita blok. Cara lengkapnya bisa lihat dibawah ini :

Misalkan, kita akan blokir website kompas.com menggunakan Address List. Pertama kita cek dulu IP Address kompas.com menggunakan nslookup.



Bisa kita lihat diatas, kalau kompas.com mempunyai 2 IP address. Jadi, kita harus membuat 2 Address List kompas dengan nama yang sama. untuk perintah text,

```
[admin@MikroTik] > ip firewall address-list add address=202.146.4.100 list="IP Kompas"
[admin@MikroTik] > ip firewall address-list add address=202.61.113.35 list="IP Kompas"
[admin@MikroTik] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                ADDRESS
 0   IP Admin                            13.13.13.2
 1   IP Client                           13.13.13.0/24
 2   IP Kompas                           202.146.4.100
 3   IP Kompas                           202.61.113.35
```

Setelah kita buat address list nya, sekarang kita buat *rule* perintah *drop* nya. Perintah text nya adalah

```
[admin@MikroTik] > ip firewall filter add chain=forward dst-address="IP Kompas" action=drop
```

Jika ada firewall rule yang sebelumnya, kita pindahkan dulu rule yang kita buat ke urutan atas

sekarang, coba kalian buka kompas.com, maka website tersebut tidak akan terbuka dan hanya loading terus menerus karena sudah kita *drop*.

Untuk mengganti IP Address dari Address List tadi yang kita buat, bisa dilakukan dengan perintah text : **ip firewall address-list set [no index address list] address=[ip pengganti]** untuk contoh, disini saya akan mengganti IP Admin dengan nomor index (urutan) 0 dengan IP 13.13.13.3. berarti perintah text nya adalah

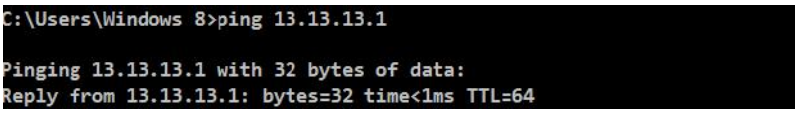
```
[admin@MikroTik] > ip firewall address-list set 0 address=13.13.13.3
[admin@MikroTik] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                ADDRESS
 0   IP Admin                             13.13.13.3
 1   IP Client                            13.13.13.0/24
```

IP address telah diganti. Jadi, misalkan sewaktu-waktu pc admin mengganti IP addressnya, kita hanya tinggal merubahnya di Address List, tidak perlu mengkonfigurasi ulang rule firewall nya.

Address List juga bisa digunakan untuk menambahkan IP Address dari computer yang mencoba melakukan *ping* kepada router. Perintah text nya adalah :

```
[admin@MikroTik] > ip firewall filter add chain=input in-interface=ether2 protocol=icmp
action=add-src-to-address-list address-list="tukang ngeping"
```

Sekarang, coba kalian ping menggunakan user client, setelah itu kita cek Address List nya (**ip address-list print**) maka, IP Address yang ngeping ke router kalian akan di tambahkan dengan nama *tukang ngeping*.



Firewall Mangle

Firewall Mangle fungsinya untuk memberi tanda (mark) pada paket data dan koneksi tertentu. Tujuan nya sendiri adalah agar paket data lebih mudah dikenali. Dengan menggunakan Firewall Mangle (Marking) pada Router MikroTik ini, akan memudahkan dalam mengelola sebuah paket data. Misalnya, menerapkan *marking* pada firewall *filter, NAT, Routing*. Fitur Mangle ini hanya bisa digunakan pada router MikroTik itu sendiri dan tidak dapat digunakam oleh router lain. Karena *marking* tersebut akan dilepas pada saat paket data akan keluar / meninggalkan router.

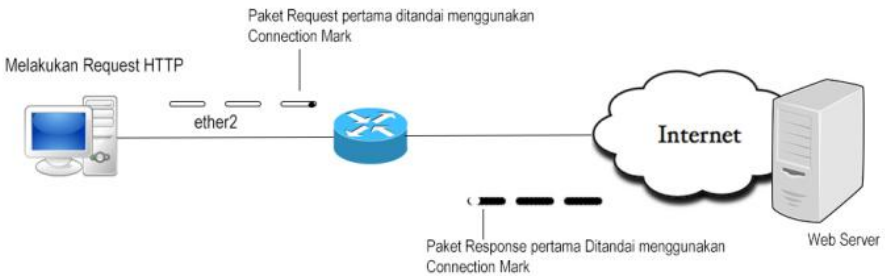
Di dalam Firewall Mangle ini, ada 3 jenis Marking yang bisa kita gunakan, yaitu

1. **Connection Mark (Penandaan pada Koneksi)**
2. **Packet Mark (Penandaan pada paket data)**
3. **Routing Mark (Penandaan pada Routing)**

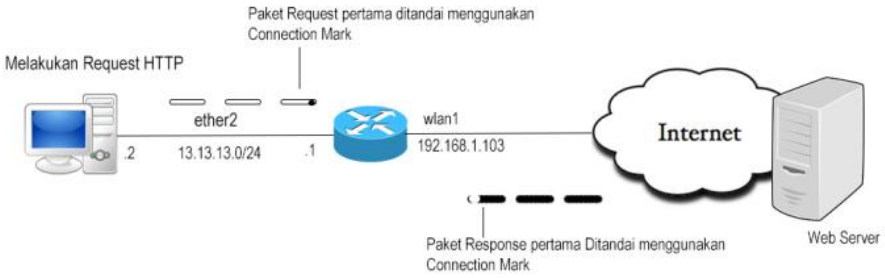
Kita langsung saja pada pembahasan *marking* yang pertama, yaitu *Connection Mark*

Connection Mark

Connection Mark ini berfungsi untuk menandai sebuah Koneksi. *Connection Mark* bisa digunakan untuk memberikan tanda atau marking pada paket pertama yang dikeluarkan oleh Client ataupun Paket Response yang pertama dikeluarkan oleh Web Server



Bisa kita lihat gambar diatas, Client melakukan Request HTTP terhadap suatu Web Server. Terlihat pada gambar diatas, Request dari Client tersebut memiliki 3 paket, pada *connection mark* ini yang ditandai adalah paket yang pertama keluar dari Client, untuk paket ke dua dan ke tiga tidak ditandai. Begitu juga pada paket Response dari Web Server, paket yang pertama keluar dari Web Server tersebut yang akan ditandai.



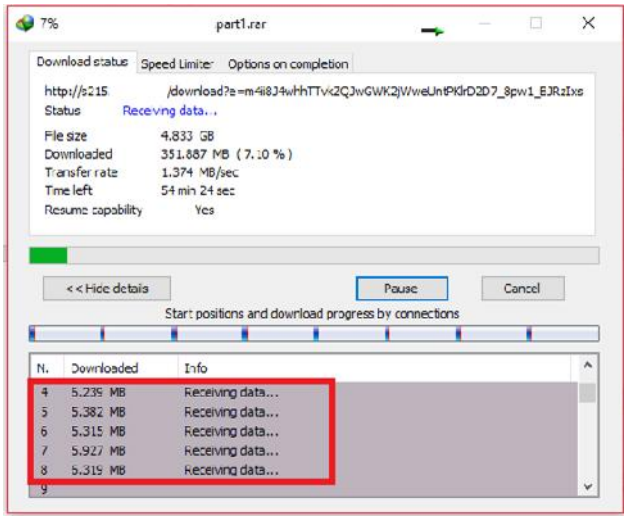
Kita akan melakukan *Connection Marking* pada interface ether2 yang melakukan aktifitas browsing HTTP. Perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.2
protocol=tcp dst-port=80 in-interface=ether2 action=mark-connection new-connection
mark=browsing
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=prerouting action=mark-connection new-connection-mark=browsing
     passthrough=yes protocol=tcp src-address=13.13.13.2 in-interface=ether2 dst-port=80
```

Kita juga bisa melakukan *marking* sesuai dengan content yang diakses user. Misalnya, melakukan *connection marking* pada content file berekstensi *.rar*. Untuk melakukan konfigurasi nya hampir sama seperti sebelumnya. Hanya saja, disini kita akan menambahkan perintah *content*. Langsung saja ke langkah konfigurasi nya :

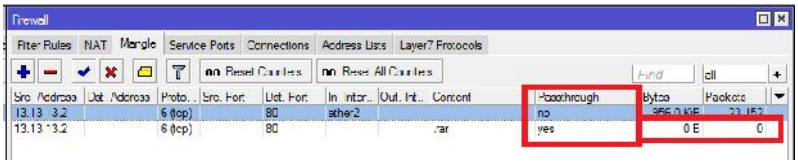
```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.2
protocol=tcp port=80 content=.rar action=mark-connection new-connection-
mark=download_rar
[admin@MikroTik] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=prerouting action=mark-connection new-connection-mark=browsing
     passthrough=yes protocol=tcp src-address=13.13.13.2 in-interface=ether2 dst-port=80

 1   chain=prerouting action=mark-connection new-connection-mark=download_rar
     passthrough=yes protocol=tcp src-address=13.13.13.2 port=80 content=.rar
```

Kita juga perlu memperhatikan perintah *passtrough*, jika *passtrough* pada rule pertama (0) adalah *no* , maka marking pada paket data tidak akan dilanjutkan pada rule selanjutnya. Jika *passtrough=yes* marking akan dilanjutkan pada rule selanjutnya. Agar lebih jelas, kita akan coba melakukan download file berekstensi rar.

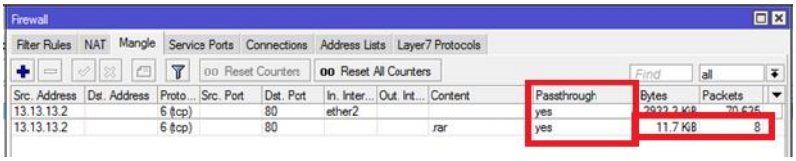


IDM membuat 8 Koneksi pada saat mendownload file diatas

Jika passtrough pada rule pertama adalah *no*



Jika passtrough pada rule pertama adalah *yes*



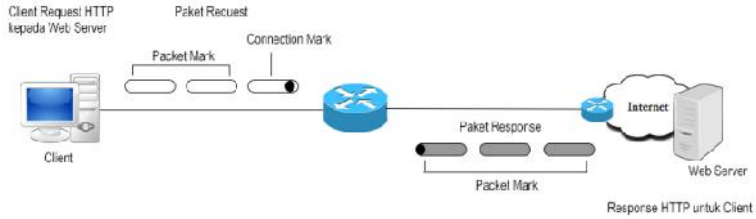
Bisa kita lihat perbandingan diatas, rule ke 2 akan “menangkap” 8 paket (melakukan connection mark) pada saat client mendownload file rar jika parameter passtrough adalah *yes*. Berbeda jika pada rule pertama perintah *passtrough* nya adalah *no.*

Jika kita lihat pada gambar diatas, kita melakukan test download menggunakan Internet Download Manager. Jika kita mendownload menggunakan IDM ini, nantinya download manager tersebut akan membuat beberapa koneksi seperti seperti gambar dibawah ini.

Jika salah satu koneksi tersebut telah selesai mendownload, maka IDM akan membuat koneksi baru, dan pada *Counter Packet* connection mark juga akan bertambah sesuai dengan koneksi yang dibuat oleh download manager

Packet Mark

Setelah kita membahas tentang *Connection Mark*, sekarang kita akan ke pembahasan selanjutnya, yaitu *Packet Mark*. Packet Mark sendiri berfungsi untuk melakukan *marking* pada paket data. Jika tadi *Connection Mark* hanya melakukan *Marking* pada paket yang pertama keluar dari Router, maka *Packet Mark* berfungsi untuk menandai paket paket selanjutnya. Agar lebih jelas, bisa lihat gambar dibawah ini :



Bisa kita lihat gambar diatas, Client melakukan Request HTTP kepada Web Server. Pada Request Client tersebut, Client mengirimkan 3 paket data (*Traffic Upload*). Paket pertama, ditandai atau di *marking* menggunakan Connection Mark, lalu paket selanjutnya ditandai / di *marking* menggunakan Packet Mark. Lalu Web Server meresponse dengan mengirim 3 paket data (*Traffic Download*) pada client. Pada gambar diatas, kita akan melakukan 3 konfigurasi *Firewall Mangle*, yaitu *Connection Mark*, *Packet Mark* untuk *Traffic Upload* dan *Packet Mark* untuk *Traffic Download.*

Sekarang, kita akan mencoba melakukan konfigurasi *Marking* pada topologi dibawah ini

Bisa lihat gambar diatas, Router mempunyai 1 Client melalui Interface *ether2* lalu Router terhubung dengan internet melalui interface *wlan1*. Disini kita akan melakukan *Marking* pada *Traffic Upload* dan *Download* yang dilakukan oleh Client.

Untuk langkah pertama, kita akan lakukan konfigurasi *Connection Mark* untuk komputer Client dengan IP Network 13.13.13.0/24 yang terhubung melalui interface *ether2.* Konfigurasinya adalah sebagai berikut :

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.0/24 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client passthrough=yes
```

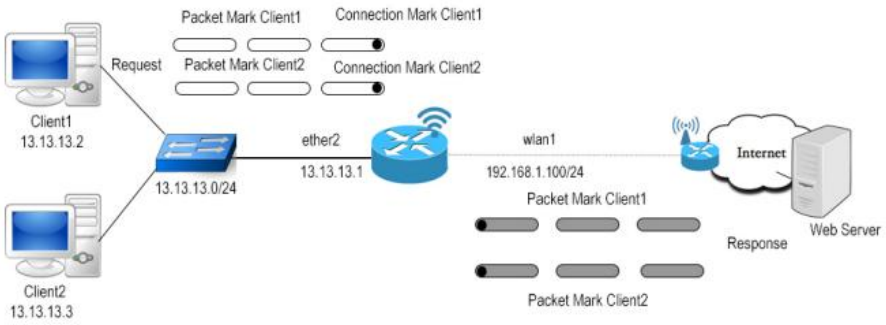
Setelah melakukan konfigurasi *Connection Mark*, sekarang kita lakukan konfigurasi *Packet Mark* untuk *Traffic Upload.* Yang perlu diperhatikan pada konfigurasi ini adalah perintah text *mark-connection* kita isi dengan menggunakan connection mark yang tadi kita buat, yaitu *koneksi_client.* Lalu pada bagian *in-interface* kita isi dengan *ether2* karena PC Client terhubung melalui interface *ether2*, jadi traffic upload akan masuk melalui interface tersebut. Dan perintah *passthrough* kita isi dengan *no* agar packet mark tidak dilanjutkan kepada *rule* selanjutnya

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client action=mark-packet new-packet-mark=upload_client passthrough=no
```

Setelah selesai konfigurasi *Packet Mark* untuk *Traffic Upload,* Sekarang kita lakukan konfigurasi *Packet Mark* untuk *Traffic Download*. Untuk konfigurasi nya hampir sama dengan membuat rule Packet Mark untuk *Traffic Upload*, hanya saja disini kita akan menggunakan in-interface *wlan1* karena nantinya paket data download akan masuk melalui interface *wlan1*.

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=wlan1 connection-mark=koneksi_client action=mark-packet new-packet-mark=download_client passthrough=no
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=browsing
      passthrough=yes protocol=tcp src-address=13.13.13.2 in-interface=ether2 dst-port=80

 1    chain=prerouting action=mark-connection new-connection-mark=download_rar
      passthrough=yes protocol=tcp src-address=13.13.13.2 port=80 content=.rar

 2    chain=prerouting action=mark-connection new-connection-mark=koneksi_client
      passthrough=yes src-address=13.13.13.0/24 in-interface=ether2

 3    chain=prerouting action=mark-packet new-packet-mark=upload_client passthrough=no in-interface=ether2 connection-mark=koneksi_client

 4    chain=prerouting action=mark-packet new-packet-mark=download_client passthrough=no
      in-interface=wlan1 connection-mark=koneksi_client
```

Konfigurasi *Marking* diatas sudah selesai. Sekarang, bagaimana cara untuk melakukan *marking* pada PC Client 1 per 1? Agar lebih jelas, kita lihat gambar topologi dibawah ini



Untuk melakukan *marking* pada topologi diatas, kita hanya perlu melakukan konfigurasi marking 1 per 1 untuk client tersebut. Langsung saja kita mulai konfigurasi marking untuk client dengan IP 13.13.13.2

Jika melalui perintah text, maka perintahnya adalah sebagai berikut.

Konfigurasi *Connection Mark* Client 1

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.2 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client1 passthrough=yes
```

Konfigurasi Packet Mark traffic upload Client 1

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client1 action=mark-packet new-packet-mark=upload_client1 passthrough=no
```

Konfigurasi Packet Mark Traffic Download Client 1

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=wlan1 connection-mark=koneksi_client1 action=mark-packet new-packet-mark=download_client1 passthrough=no
```

Setelah itu, Kita cek menggunakan perintah **ip firewall mangle print detail**

```
[admin@Mikrotik2] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=koneksi_client1 passthrough=yes src-address=13.13.13.2 in-interface=ether2 log=no log-prefix=""

 1    chain=prerouting action=mark-packet new-packet-mark=upload_client1 passthrough=no in-interface=ether2 connection-mark=koneksi_client1 log=no log-prefix=""

 2    chain=prerouting action=mark-packet new-packet-mark=download_client1 passthrough=no in-interface=wlan1 connection-mark=koneksi_client1 log=no log-prefix=""
```

Sekarang kita akan mengkonfigurasi marking untuk client 2 (13.13.13.3)

Konfigurasi *Connection Mark* Client 2

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.3 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client2 passthrough=yes
```

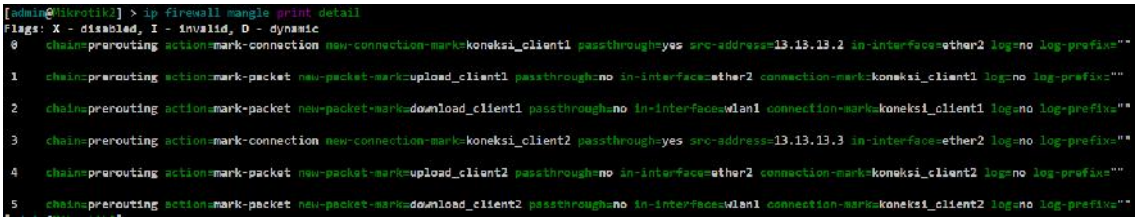
Konfigurasi Packet Mark Traffic Upload Client 2

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client2 action=mark-packet new-packet-mark=upload_client2 passthrough=no
```

Konfigurasi Packet Mark Traffic Download Client 2

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=wlan1 connection-mark=koneksi_client2 action=mark-packet new-packet-mark=download_client2 passthrough=no
```

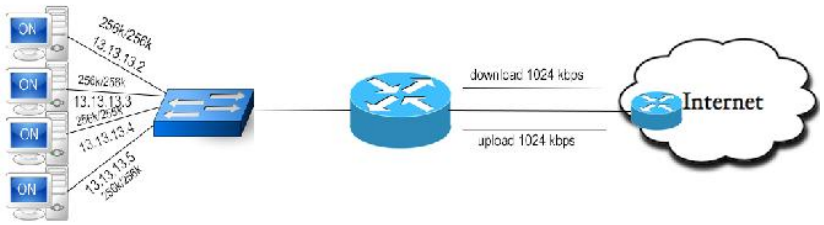
Setelah itu, kita cek semua rule firewall mangle yang telah kita buat dengan menggunakan perintah **ip firewall mangle print detail**



Quality of Service

Bandwidth Manajemen

Quality of Service ini adalah Kualitas dari Jaringan kita, Misalnya melakukan manajemen Bandwidth yang merata pada setiap PC Client, Kecepatan yang akan didapat oleh Setiap Client, dan sebagainya yang berhubungan dengan Kualitas Jaringan. Sebagai contoh dari Quality of Service Bandwidth Manajemen kita bisa lihat gambar topologi dibawah ini



Pada Mikrotik sendiri, penerapan Bandwith manajemen bisa menggunakan fitur *Queue*. Queue sendiri terbagi 2, yaitu *Simple Queue & Queue Tree*. Yang pertama saya bahas disini adalah *Simple Queue*. Pada saat menerapkan *Queue* pada jaringan, akan ada 2 jenis Rate, yaitu *MIR dan CIR*.

- MIR (Maximum Information Rate) adalah Bandwidth Maksimal yang akan di dapatkan oleh Client ketika jaringan sedang tidak sibuk (tidak digunakan User Lain)
- CIR (Committed Information Rate) adalah Bandwidth yang akan di dapatkan saat kondisi jaringan (traffic) penuh / sibuk. Tetapi, tidak akan mendapatkan Bandwidth dibawah CIR.

Simple Queue

Melakukan manajemen bandwidth dengan Simple Queue adalah cara paling sederhana. Pada simple queue kita bisa melimit Bandwidth berdasarkan IP Address Client. Baik itu bandwidth *Download* ataupun *Upload*. Untuk pembahasan pertama, saya akan mencoba melakukan limit bandwidth seperti pada gambar topologi dibawah ini

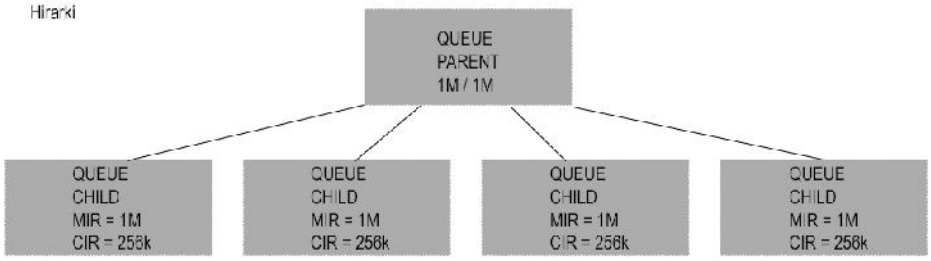
Bisa kita lihat gambar diatas, ISP memberikan Bandwidth terhadap Router MikroTik untuk Download dan Upload sebesar 2M/2M. Bisa kita lihat juga pada gambar diatas Router MikroTik mempunyai 1 buah PC Client yang terhubung melalui interface *ether2* dengan IP Address 13.13.13.5. Disini kita akan melakukan konfigurasi limit bandwidth terhadap PC Client tersebut, melimit bandwidth Download dan Upload nya menjadi maksimal 1Mbps. *Loh, ngapain di limit jadi 1 mbps? Yang 1 mbps nya lagi mubazir dong nggak kepake?* Sisa dari bandwidth yang diberikan ISP akan kita buat menjadi bandwidth *cadangan.* Bisa terpakai pada *Burst* atau yang lain nya.

Sekarang, kita langsung saja menuju langkah konfigurasinya melalui perintah text :

```
[admin@MikroTik] > queue simple add name=client target=13.13.13.5 max-limit=1M/1M
[admin@MikroTik] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0   name="client" target-addresses=13.13.13.5/32 interface=all parent=none packet-marks="" direction=both
     priority=8 queue=default-small/default-small limit-at=0/0 max-limit=1M/1M burst-limit=0/0
     burst-threshold=0/0 burst-time=0s/0s total-queue=default-small
```

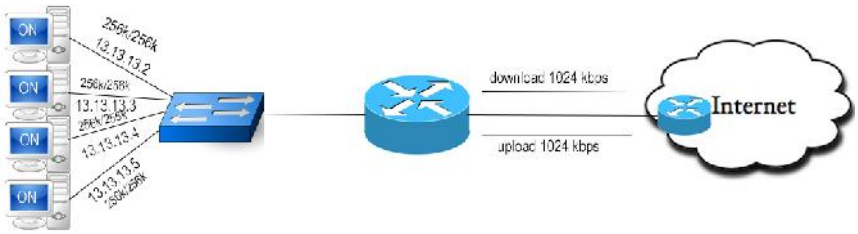
Konfigurasi diatas sudah selesai. Maka, sekarang user dengan IP 13.13.13.5 hanya akan dapat bandwidth download/upload sebesar 1Mbps. Kita bisa menggunakan Speedtest atau tool ***Torch*** MikroTik untuk melakukan pengujian.

Sekarang, kita akan mencoba melakukan pembagian Bandwidth pada 4 user client. Disini kita akan memanfaatkan fitur *parent* dan *child*. Jadi, nantinya setiap *child* akan menginduk dan meminta jatah bandwidth terhadap bandwidth *parent.*



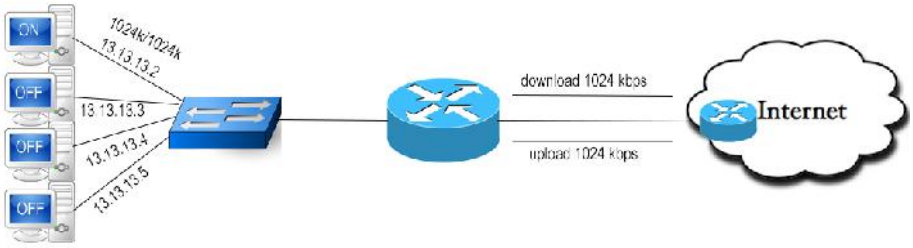
Ketika jaringan penuh, semua pc client akan mendapatkan bandwidth *CIR*. Agar lebih jelas, lihat gambar dibawah ini :

Ketika jaringan penuh :



Ketika jaringan sedang sepi, yang memakai jaringan hanya 1 PC Client, maka PC Client tersebut akan mendapatkan bandwidth MIR.

Ketika jaringan hanya 1 yang memakai



Teknik ini biasa disebut juga dengan teknik Bandwidth type *Hirarki*.

Sekarang kita langsung saja ke langkah konfigurasi nya.

Sebelum itu, lebih baik kita hapus dulu rule yang sebelumnya dengan menggunakan perintah berikut :

```
[admin@MikroTik] > queue simple remove 0
[admin@MikroTik] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
```

Pertama, kita akan membuat queue simple yang akan digunakan sebagai induk atau *parent* terlebih dahulu. Kita akan membuat limit bandwidth maksimal (MIR) 1Mbps, baik download maupun upload untuk semua PC Client. Perintah text (CLI) nya adalah sebagai berikut :

```
[admin@MikroTik] > queue simple add name=induk target-addresses=13.13.13.0/24 max-limit=1M/1M
```

Sekarang, kita lakukan konfigurasi CIR dan MIR untuk 4 user client. Perintah text nya hampir sama seperti sebelumnya, hanya saja disini kita menambahkan perintah *parent* yang nantinya ajan diisi dengan nama queue parent yang kita buat sebelumnya. Perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > queue simple add name=Client1 target-addresses=13.13.13.2 max-limit=1M/1M limit-at=256k/256k parent=induk
```

bagian *max-limit* adalah MIR, *limit-at* adalah CIR. Sekarang, kita buat perintah konfigurasi untuk client yang lain nya.

```
[admin@MikroTik] > queue simple add name=Client2 target-addresses=13.13.13.3 max-limit=1M/1M limit-at=256k/256k parent=induk
[admin@MikroTik] > queue simple add name=Client3 target-addresses=13.13.13.4 max-limit=1M/1M limit-at=256k/256k parent=induk
[admin@MikroTik] > queue simple add name=Client4 target-addresses=13.13.13.5 max-limit=1M/1M limit-at=256k/256k parent=induk
[admin@MikroTik] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0   name="induk" target-addresses=13.13.13.0/24 interface=all parent=none packet-marks="" direction=both priority=8 queue=default-small/default-small limit-at=0/0 max-limit=1M/1M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-queue=default-small

 1   name="Client1" target-addresses=13.13.13.2/32 interface=all parent=induk packet-marks="" direction=both priority=8 queue=default-small/default-small limit-at=256k/256k max-limit=1M/1M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-queue=default-small

 2   name="Client2" target-addresses=13.13.13.3/32 interface=all parent=induk packet-marks="" direction=both priority=8 queue=default-small/default-small limit-at=256k/256k max-limit=1M/1M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-queue=default-small

 3   name="Client3" target-addresses=13.13.13.4/32 interface=all parent=induk packet-marks="" direction=both priority=8 queue=default-small/default-small limit-at=256k/256k max-limit=1M/1M burst limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-queue=default-small
```

```
4   name="Client4" target-addresses=13.13.13.5/32 interface=all parent=induk packet-
    marks="" direction=both priority=8 queue=default-small/default-small limit-at=256k/256k
    max- limit=1M/1M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-
    queue=default-small
```

Jika sudah dikonfgurasi, maka, jika hanya 1 user yang menggunakan jaringan, nantinya user1 akan mendapatkan bandwidth full 1Mbps. Ketika jaringan sibuk, 4 client tersebut menggunakan jaringan maka semuanya akan mendapatkan kecepatan minimum (CIR).

Simple Queue dengan Burst

Masih berkaitan dengan *Simple Queue*, tetapi kita sekarang akan memakai Fitur Mikrotik yang bernama Burst. Burst atau Bahasa indonesianya *lonjakan,* berfungsi memungkinkan Client mendapat *Rate* yang lebih besar dari *rate* MIR (maksimal) selama waktu tertentu. Jadinya, client akan mendapatkan bandwidth yang melebihi maksimum di awal awal. Di dalam menggunakan Burst, ada beberapa istilah, yaitu :

- ***Burst Limit*** adalah nilai Bandwidth / Kecepatan maksimal yang akan diterima oleh Client saat Burst di jalankan. Nilai Burst limit ini harus lebih besar dari Max Limit Bandwidth (tanpa Burst) yang telah ditentukan
- ***Burst Time*** adalah waktu untuk menghitung data rate, bukan lama nya waktu burst dijalankan
- ***Burst Threshold*** adalah nilai rata rata yang menentukan kapan Burst harus dijalankan dan kapan harus Dihentikan.

Harus diperhatikan, jadi jika aliran data rata-rata di bawah *burst threshold*, maka, burst akan aktif dan bandwidth akan mengikuti *Burst Limit.* Setelah itu, router akan menghitung setiap detik *Burst Time* terakhir dijalankan, jika aliran data rata rata melebihi atau sama seperti *Burst Threshold*, maka Burst akan berhenti, dan bandwidth kembali mengikuti *Max limit*. Dibawah ini adalah rumus untuk menghitung lama nya setiap User mendapatkan Burst

- Lama burst = (Burst Threshold / Burst Limit) * Burst Time

Kita langsung masuk ke langkah konfigurasi nya :

Disini kita akan mencoba konfigurasi Sebagai Berikut

- Max Limit = 1Mbits (Upload&Download)
- Burst-threshold = 512 kbps
- Burst Limit = 2Mbps

- Burst Time = 12s

Sekarang, kita akan coba hitung lamanya Burst akan dijalankan

- (512/2048) * 12 = 3 detik

Sudah dapat, sekarang kita langsung menuju langkah konfigurasi nya.

Sebagai contoh, disini saya akan menambahkan Burst limit sebesar 2M/2M terhadap PC Client router MikroTik yang memiliki IP Address 13.13.13.2. maka perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > queue simple add name=user target-addresses=13.13.13.2 max-limit=1M/1M
limit-at=256k/256k burst-threshold=512k/512k burst-limit=2M/2M burst-time=12s/12s
[admin@MikroTik] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0    name="user" target-addresses=13.13.13.2/32 interface=all parent=none packet-marks=""
      direction=both priority=8 queue=default-small/default-small limit-at=256k/256k max-
      limit=1M/1M burst-limit=2M/2M burst-threshold=512k/512k burst-time=12s/12s total-
      queue=default-small
```

Setelah itu coba kita test menggunakan Bandwidth Mikrotik test

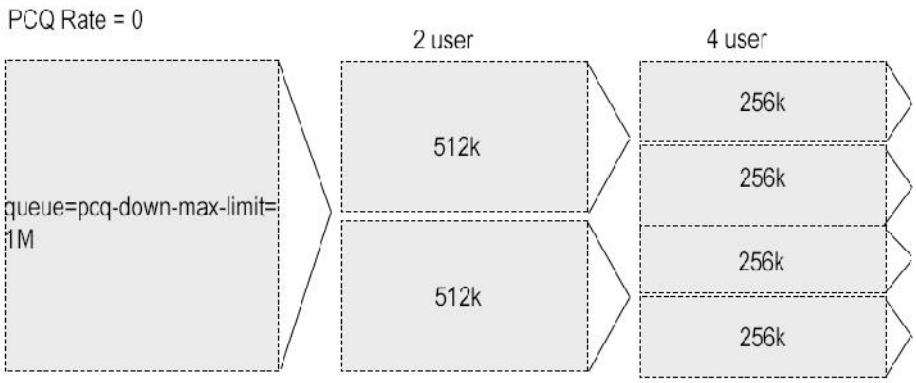
Jika aliran data rata-rata dibawah *Burst Threshold*, Maka, selama 3 detik, client tersebut akan mendapatkan Bandwidth maximal dari Burst, setelah itu akan kembali normal sesuai dengan Queue yang kita buat

Simple Queue dengan PCQ

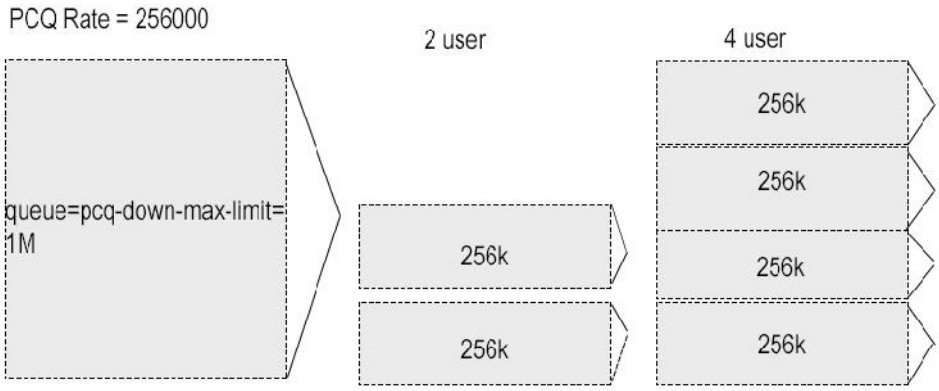
Sekarang, kita lanjut ke pembahasan selanjutnya yaitu Simple Queue dengan PCQ. *Apa itu PCQ?* PCQ adalah Per Connection Queue yang berfungsi membagi bandwidth secara merata kepada client yang aktif dengan membuat beberapa *Sub Stream*. PCQ Sendiri biasanya digunakan pada jaringan yang mempuyai Client sangat banyak, agar kita tidak perlu melakukan konfigurasi bandwidth 1 per 1 pada Client tersebut, meskipun Client nya bertambah atau pun berkurang

Untuk Cara kerja dari PCQ *simple nya begini*. Misalnya saya mempunyai 10 PC dengan Bandwidth 10Mbps. masing masing PC akan mendapat jatah Bandwidth minimal 1Mbps, jadi kalau hanya 1 PC yang menggunakan Koneksi, PC tersebut mendapatkan bandwidth 10mbps. Kalau 2 PC yang menggunakan koneksi, PCQ membuat 1 Sub Stream lagi maka max bandwidth nya dibagi dua jadi masing masing PC mendapatkan 5mbps, dan seterusnya. di dalam PCQ sendiri ada yang istilah *pcq-rate*, yang befungsi untuk memberikan seberapa besar Bandwidth maksimal yang

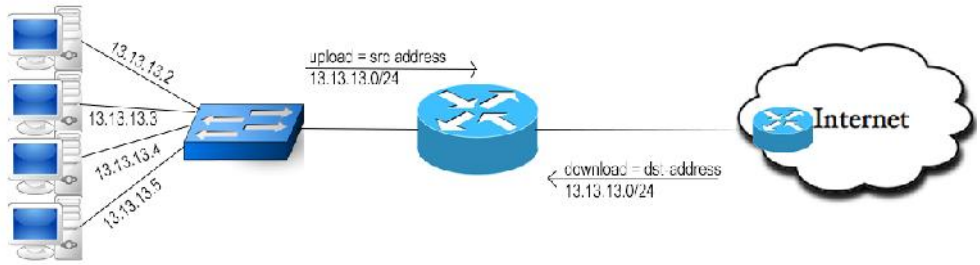
akan di berikan kepada suatu PC Client jika keadaan jaringan sedang tidak sibuk. Sebagai contoh, Misalnya kita mengisi *pcq-rate=0,* maka, jika hanya 1 PC yang menggunakan jaringan, PC tersebut akan mendapatkan Bandwidth maksimal sesuai dengan konfigurasi Queue yang kita buat (seperti contoh cara kerja PCQ diatas).



misalnya *pcq-rate* nya saya isi dengan 256k , maka akan seperti dibawah ini :



Meskipun hanya 2 user saja yang memakai Jaringan, kedua User tersebut hanya akan mendapatkan bandwidth sebesar 256k. Berbeda jika kita menggunakan *pcq-rate=0* yang akan membagi-bagi MIR sesuai dengan User yang memakai jaringan tersebut. Sekarang, kita lanjutkan ke langkah Konfigurasinya.



Pertama-tama, kita akan membuat dulu *PCQ* nya. *PCQ Upload =src-address* ,*PCQ Download =dst-address*. Disini kita akan membuat *pcq* dengan rate=0

Jika melalui perintah text (CLI) maka, perintahnya adalah sebagai berikut :

```
[admin@MikroTik] > queue type add name="PCQ-Download" kind=pcq pcq-rate=0 pcq-
classifier=dst-address
[admin@MikroTik] > queue type add name="PCQ-Upload" kind=pcq pcq-rate=0 pcq-
classifier=dst-address
[admin@MikroTik] > queue type print
Flags: * - default
 0 * name="default" kind=pfifo pfifo-limit=50

 1 * name="ethernet-default" kind=pfifo pfifo-limit=50

 2 * name="wireless-default" kind=sfq sfq-perturb=5 sfq-allot=1514

 3 * name="synchronous-default" kind=red red-limit=60 red-min-threshold=10 red-max-
      threshold=50 red-burst=20 red-avg-packet=1000

 4 * name="hotspot-default" kind=sfq sfq-perturb=5 sfq-allot=1514

 5   name="PCQ-Download" kind=pcq pcq-rate=0 pcq-limit=50 pcq-classifier=dst-address pcq
     total-limit=2000 pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s pcq-src-address-
     mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128 pcq-dst-address6-mask=128

 6   name="PCQ-Upload" kind=pcq pcq-rate=0 pcq-limit=50 pcq-classifier=dst-address pcq-total-
     limit=2000 pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s pcq-src-address-
     mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128 pcq-dst-address6-mask=128

 7 * name="only-hardware-queue" kind=none

 8 * name="multi-queue-ethernet-default" kind=mq-pfifo mq-pfifo-limit=50

 9 * name="default-small" kind=pfifo pfifo-limit=10
```

Bisa kita lihat gambar diatas, *PCQ* nya sudah berhasil dibuat. Sekarang, kita akan membuat rule *simple queue*. Jika melalui perintah text adalah :

```
[admin@MikroTik] > queue simple add name=pcqtest target-addresses=13.13.13.0/24 max-
limit=1M/1M queue=PCQ-Upload/PCQ-Download
[admin@MikroTik] > queue simple print
Flags: X - disabled, I - invalid, D - dynamic
 0    name="pcqtest" target-addresses=13.13.13.0/24 interface=all parent=none packet-marks=""
      direction=both priority=8 queue=PCQ-Upload/PCQ-Download limit-at=0/0 max-
      limit=1M/1M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s total-queue=default-
      small
```

Rule Simple Queue dengan PCQ diatas sudah berhasil dibuat, Sekarang untuk melakukan pengujian, coba kita test menggunakan 1 PC (Client). Maka, PC tersebut akan mendapat kan bandwidth yang full (1Mbps). Jika kita menggunakan 2 PC, maka bandwidth tersebut akan di bagi dua (512kbps)

Queue Tree

Sekarang, kita masuk ke materi *Queue Tree*. Bedanya Queue Tree dan Queue Simple yang kita bahas sebelumnya, Queue Tree bersifat satu arah atau *one way,* jadi hanya bisa digunakan pada 1 jenis traffic. Jadi, jika kita melakukan konfigurasi bandwidth download menggunakan Queue Tree, maka konfigurasi tersebut tidak bisa digunakan oleh traffic upload. Jika kalian ingin menggunakan Queue Tree untuk melakukan konfigurasi limit Bandwidth Upload dan Download, maka kalian harus membuat 2 konfigurasi Queue Tree nya.

Dalam menggunakan Queue Tree, nantinya kita juga akan melibatkan Firewall Mangle. Karena Queue Tree nantinya menggunakan *Packet Mark.* Hal ini yang membuat konfigurasi Queue Tree terlihat lebih *rumit* daripada Simple Queue. Pemilihan Interface *parent* juga membuat Queue Tree menjadi lebih rumit.

Sekarang, kita akan melakukan Konfigurasi Dasar Queue Tree pada gambar topologi dibawah ini :

Bisa kita lihat gambar diatas, MikroTik mendapatkan Bandwidth maksimal dari ISP baik itu Download maupun Upload sebesar 2Mbps. Kita juga bisa lihat pada gambar diatas, Router MikroTik memiliki 1 PC Client yang memiliki IP Address 13.13.13.2 dan terhubung melalui Interface *ether2*. Kita akan melakukan limit Bandwidth terhadap PC tersebut, maks download 1M dan maks upload 1M menggunakan Queue Tree. Sekarang, kita langsung saja menuju langkah konfigurasi nya

Pertama, kita akan lakukan konfigurasi Firewall Mangle nya terlebih dahulu. Prinsip *top-to-bottom* masih berlaku dalam Firewall Mangle, jadi, Kita akan melakukan konfigurasi *Connection Mark* nya terlebih dahulu setelah itu Mark Packet nya. Perintah text nya adalah sebagai berikut :

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.2 in-
interface=ether2 action=mark-connection new-connection-mark=koneksi_client passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting connection-mark=koneksi_client
action=mark-packet new-packet-mark=paket_client passthrough=no
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=koneksi_client
      passthrough=yes src-address=13.13.13.2 in-interface=ether2

 1   chain=prerouting action=mark-packet new-packet-mark=paket_client passthrough=no
     connection-mark=koneksi_client
```

Konfigurasi Firewall Mangle telah selesai, sekarang kita lakukan konfigurasi Queue Tree nya. Yang pertama, kita akan lakukan konfigurasi untuk bandwidth *Upload sete* Setelah itu, kita lakukan konfigurasi untuk bandwidth *download*. Perintah text nya adalah sebagai berikut :

```
[admin@MikroTik] > queue tree add name=upload parent=wlan1 packet-mark=paket_client
max-limit=1M
[admin@MikroTik] > queue tree add name=download parent=ether2 packet-mark=paket_client
max-limit=1M
[admin@MikroTik] > queue tree print
Flags: X - disabled, I - invalid
 0    name="upload" parent=wlan1 packet-mark=paket_client limit-at=0 queue=default
      priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

 1    name="download" parent=ether2 packet-mark=paket_client limit-at=0 queue=default
      priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s
```

Keterangan

- ***parent=wlan1,*** pada perintah text ini, kita isi dengan interface router yang digunakan untuk terhubung dengan internet / ISP
- ***packet-mark,*** pada bagian ini, kita isi dengan nama konfigurasi *packet mark* yang kita buat sebelumnya

Sekarang, untuk melakukan pengujian kita gunakan Speedtest atau dapat menggunakan tool ***Torch*** bawaan MikroTik.

Konfigurasi Queue Tree diatas telah selesai. Sekarang, kita akan lakukan konfigurasi Queue Tree tipe *Hirarki* pada topologi dibawah ini

Bisa kita lihat gambar topologi diatas, terdapat 2 PC Client pada Router MikroTik yang terhubung melalui interface *ether2*. Yang pertama kita konfigurasikan adalah Marking atau Firewall Mangle nya terlebih dahulu. Untuk langkahnya sendiri sama seperti sebelumnya, hanya saja disini kita tambahkan lagi untuk Client 2. Agar lebih jelasnya bisa lihat konfigurasi dibawah ini :

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=13.13.13.3 in-
interface=ether2 action=mark-connection new-connection-mark=koneksi_client
passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting connection-mark=koneksi_client2
action=mark-packet new-packet-mark=paket_client2 passthrough=no
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=prerouting action=mark-connection new-connection-mark=koneksi_client
     passthrough=yes src-address=13.13.13.2 in-interface=ether2

 1   chain=prerouting action=mark-packet new-packet-mark=paket_client passthrough=no
     connection-mark=koneksi_client

 2   chain=prerouting action=mark-connection new-connection-mark=koneksi_client
     passthrough=yes src-address=13.13.13.3 in-interface=ether2

 3   chain=prerouting action=mark-packet new-packet-mark=paket_client2 passthrough=no
     connection-mark=koneksi_client2
```

Konfigurasi Firewall Mangle sudah selesai, sekarang Kita akan melakukan konfigurasi Queue Tree tipe Hirarki, berarti yang pertama kita lakukan adalah membuat Rule Queue Parent nya terlebih dahulu, baik itu untuk bandwidth *download* dan *upload*. Sebaiknya, kita hapus dulu rule queue tree yang sebelumnya kita buat menggunakan perintah text

```
[admin@MikroTik] > queue tree remove 0,1
[admin@MikroTik] > queue tree print
Flags: X - disabled, I - invalid
```

Kita langsung saja menuju langkah konfigurasi nya melalui perintah text adalah sebagai berikut :

Untuk Download, ingat pada *parent* kita pilih interface *ether2,* penghubung antara PC Client dan Router MikroTik. Untuk Upload, *parent* kita isi dengan interface penghubung antara Router MikroTik dengan jaringan internet atau ISP, yaitu *wlan1*

```
[admin@MikroTik] > queue tree add name=induk_download parent=ether2 max-limit=1M
[admin@MikroTik] > queue tree add name=induk_upload parent=wlan1 max-limit=1M
[admin@MikroTik] > queue tree print
Flags: X - disabled, I - invalid
 0   name="induk_download" parent=ether2 packet-mark="" limit-at=0 queue=default priority=8
     max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

1    name="induk_upload" parent=wlan1 packet-mark="" limit-at=0 queue=default priority=8
     max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s
```

Setelah kita lakukan konfigurasi *parent* nya, sekarang kita lakukan konfigurasi queue *child* nya untuk masing masing client. Pertama, kita buat queue child download nya. Perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > queue tree add name=download_client1 parent=induk_download packet-
mark=paket_client limit-at=512k max-limit=1M
[admin@MikroTik] > queue tree add name=download_client2 parent=induk_download packet-
mark=paket_client2 limit-at=512k max-limit=1M
```

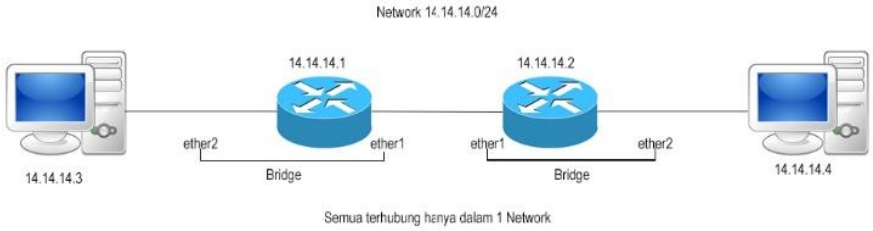
Sekarang, kita lakukan konfigurasi untuk queue child upload nya. Perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > queue tree add name=upload_client1 parent=induk_upload packet-
mark=paket_client limit-at=512k max-limit=1M
[admin@MikroTik] > queue tree add name=upload_client2 parent=induk_upload packet-
mark=paket_client2 limit-at=512k max-limit=1M
[admin@MikroTik] > queue tree print
Flags: X - disabled, I - invalid
 0   name="induk_download" parent=ether2 packet-mark="" limit-at=0 priority=8 max
     limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

 1   name="induk_upload" parent=ether1 packet-mark="" limit-at=0 priority=8 max-limit=1M
     burst-limit=0 burst-threshold=0 burst-time=0s

 2   name="download_client1" parent=induk_download packet-mark=paket_client limit-at=512k
     queue=default priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

 3   name="download_client2" parent=induk_download packet-mark=paket_client2 limit-at=512k
     queue=default priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

 4   name="upload_client1" parent=induk_upload packet-mark=paket_client limit-at=512k
     queue=default priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s

 5   name="upload_client2" parent=induk_upload packet-mark=paket_client2 limit-at=512k
     queue=default priority=8 max-limit=1M burst-limit=0 burst-threshold=0 burst-time=0s
```

Konfigurasi Queue Tree tipe Hirarki diatas sudah selesai. Sekarang, untuk melakukan pengujian bisa gunakan Speedtest atau tool ***Torch*** MikroTik. Jadi, jika hanya 1 PC yang menggunakan koneksi internet, maka PC tersebut mendapatkan Bandwidth Full, yaitu 1Mbps. Tetapi, jika kedua PC tersebut menggunakan koneksi internet, maka akan dibagi 2 bandwidth nya, menjadi 512kbps.

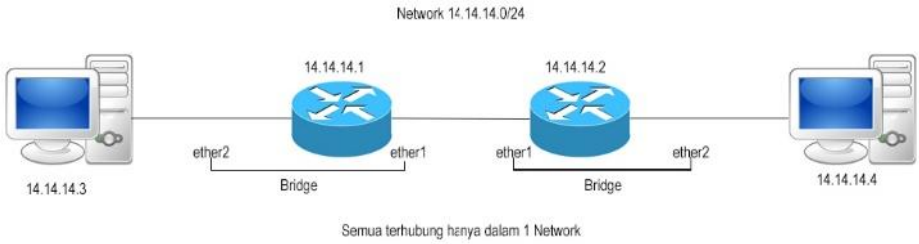
BRIDGING

Bridging adalah suatu teknik untuk menggabungkan beberapa interface router menjadi satu segmen Jaringan. Jika menerapkan teknik *bridging* ini, nantinya cara kerja router bisa diibaratkan seperti *switch*. agar lebih jelas, bisa lihat gambar topologi teknik *bridging* dibawah ini :



Bisa kita lihat gambar diatas, jika kita menerapkan teknik *Bridging*, maka semuanya terhubung hanya dengan 1 Network. Jika kita tidak menerapkan teknik *bridging* ini, seharusnya topologi diatas akan mempunyai 3 network yang berbeda. Hal itu disebabkan karena router melakukan teknik *bridging* pada interface *ether1 dan ether2*. Jadi, interface *ether1 dan ether2* akan memiliki Network yang sama. dan Router akan bekerja seperti *switch*.

Kita akan lakukan konfigurasi dasar *bridging* sesuai dengan topologi dibawah ini :



Setelah semuanya terhubung, kita akan membuat interface *bridge* pada Router MikroTik 1. Untuk langkah konfigurasi nya adalah sebagai berikut :

```
[admin@MikroTik1] > interface bridge add name=jembatan1
[admin@MikroTik1] > interface bridge print
Flags: X - disabled, R - running
 0  R name="jembatan1" mtu=1500 l2mtu=65535 arp=enabled mac-address=00:00:00:00:00:00
      protocol-mode=none priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-
      message-age=20s forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

Setelah interface bridge nya selesai dibuat, sekarang kita masukkan interface *ether1* dan *ether2* kedalam interface bridge ***jembatan1***. Perintah nya adalah

```
[admin@MikroTik1] > interface bridge port add interface=ether1 bridge=jembatan1
[admin@MikroTik1] > interface bridge port add interface=ether2 bridge=jembatan1
[admin@MikroTik1] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #   INTERFACE                 BRIDGE                 PRIORITY  PATH-COST   HORIZON
 0   ether1                    jembatan1                 0x80         10     none
 1   ether2                    jembatan1                 0x80         10     none
```

Setelah kita membuat konfigurasi interface *bridge* pada router MikroTik 1, sekarang kita lakukan konfigurasi yang sama pada router MikroTik 2

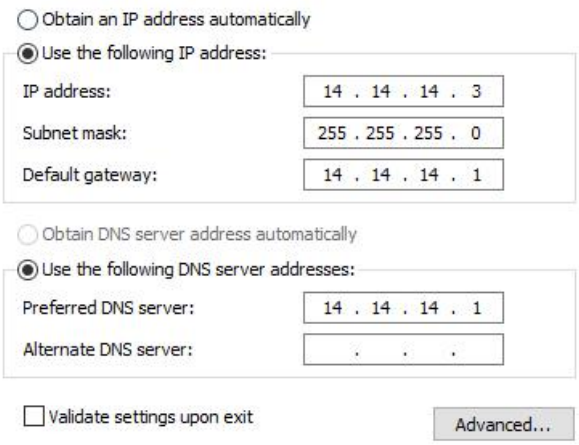
```
[admin@MikroTik2] > interface bridge port add interface=ether1 bridge=jembatan1
[admin@MikroTik2] > interface bridge port add interface=ether2 bridge=jembatan1
[admin@MikroTik2] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #   INTERFACE                 BRIDGE                 PRIORITY  PATH-COST   HORIZON
 0   ether1                    jembatan1                 0x80         10     none
 1   ether2                    jembatan1                 0x80         10     none
```

Setelah semua konfigurasi *bridge* sudah dibuat, sekarang kita tambahkan IP Address untuk port *Ethernet* nya. Sebenarnya, kita bisa saja tidak menambahkan IP Address pada interface *Ethernet*, karena sekarang router kita bekerja *layaknya* switch, dan kita tidak perlu melakukan konfigurasi IP Address pada switch. Tetapi, agar sesuai dengan topologi yang kita buat tadi, sebaiknya kita tambahkan juga IP Address pada port *Ethernet* dan juga PC Client.

Sekarang, kita tambahkan IP Address untuk port Ethernet router 1&2, setelah itu pada PC client router 1 & 2.

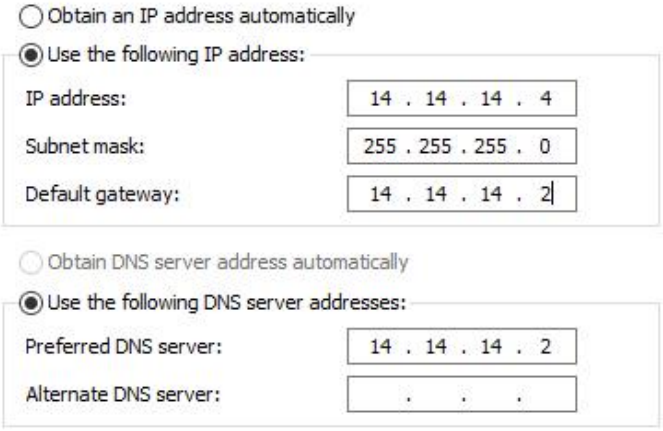
Router 1

```
[admin@MikroTik1] > ip address add address=14.14.14.1/24 interface=ether2
[admin@MikroTik1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   14.14.14.1/24      14.14.14.0      ether2
```

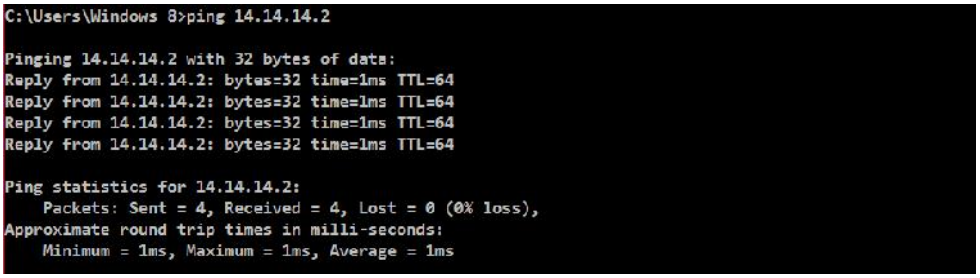


Router 2

```
[admin@MikroTik2] > ip address add address=14.14.14.2/24 interface=ether2
[admin@MikroTik2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   14.14.14.2/24      14.14.14.0      ether2
```



Setelah kita tambahkan IP Address, sekarang untuk melakukan pengujian, kita lakukan *ping* dari PC Client 1 menuju Router 2 dan sebaliknya.

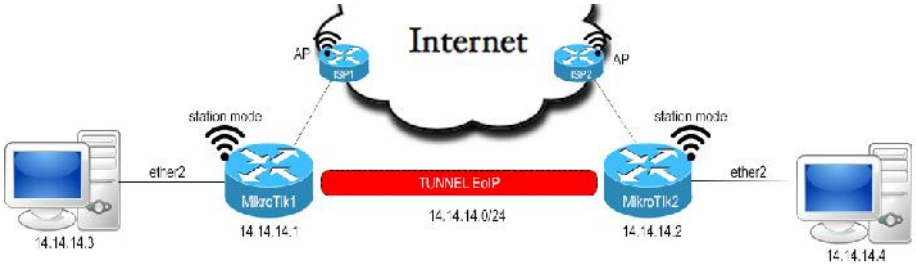


```
[admin@Mikrotik2] > ping 14.14.14.3
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 14.14.14.3                                 56 128 0ms
    1 14.14.14.3                                 56 128 0ms
    2 14.14.14.3                                 56 128 0ms
    3 14.14.14.3                                 56 128 0ms
    4 14.14.14.3                                 56 128 0ms
    5 14.14.14.3                                 56 128 0ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Bisa kita lihat gambar diatas, baik PC Client maupun Router melakukan *Reply* atau merespon *ping* yang dilakukan, yang berarti konfigurasi diatas telah berhasil

Ethernet Over IP (EoIP)

EoIP atau Ethernet over IP adalah salah satu fitur MikroTik yang memungkinkan menggunakan teknik *bridging* pada router yang terpisah jauh / berbeda jaringan internet. Sebagai contoh, disini kita akan melakukan teknik *bridge* pada router yang berbeda ISP nya. Agar lebih Jelas, bisa dilihat gambar topologi dibawah ini :



Bisa kita lihat gambar topologi diatas, kedua router tersebut menggunakan 2 ISP yang berbeda. Jadi, *EoIP* ini nantinya akan membuat *Tunnel* / Terowongan yang melewati jaringan internet untuk menghubungkan kedua router yang mempunyai jaringan internet berbeda. Sebelum kita melakukan konfigurasi *EoIP*, pastikan router 1 dan 2 telah diberi *IP Address, DNS, Gateway, NAT*, dan sudah terhubung jaringan internet dengan baik.

Setelah kedua Router tersebut terkoneksi dengan jaringan internet, sekarang kita akan membuat interface *EoIP* nya pada **Router 1**. Untuk langkah konfigurasi nya seperti dibawah ini

```
[admin@MikroTik1] > interface eoip add name="router1-ke-router2" remote-
address=192.168.100.7 tunnel-id=1
[admin@MikroTik1] > interface eoip
[admin@MikroTik1] > interface eoip print
Flags: X - disabled, R - running
 0  R name="router1-ke-router2" mtu=1500 l2mtu=65535 mac-address=FE:D1:B2:A8:97:98
arp=enabled
     local-address=0.0.0.0 remote-address=192.168.100.7 tunnel-id=1
```

Keterangan :

- ***Remote-Address =*** IP address dari Router lawan yang menyambung dengan internet (IP Address *ether1* atau *wlan1*)
- ***Tunnel-ID =*** Nomor (ID) tunnel yang kita akan buat. Router 1 dan Router 2 harus memiliki *Tunnel ID* yang sama nantinya.

Jika sudah membuat interface *EoIP* nya, sekarang kita akan membuat interface *bridge* untuk router1. Untuk langkah konfigurasi nya adalah sebagai berikut

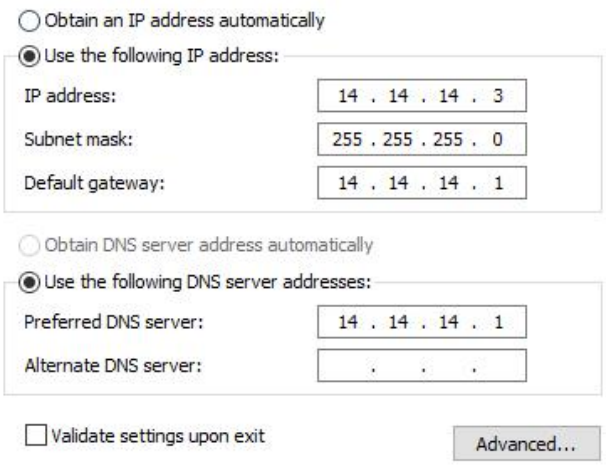
Jika melalui perintah text (CLI)

```
[admin@MikroTik1] > interface bridge add name=jembatan1
[admin@MikroTik1] > interface bridge print
Flags: X - disabled, R - running
 0  R name="jembatan1" mtu=1500 l2mtu=65535 arp=enabled mac-address=00:00:00:00:00:00
      protocol-mode=none priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-
      message-age=20s forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

Setelah membuat interface *bridge*, sekarang kita akan masukkan interface *EoIP* yang telah kita buat dan interface *ether2* kedalam interface *bridge*. Perintah text nya adalah sebagai berikut :

```
[admin@MikroTik1] > interface bridge port add interface=router1-ke-router2 bridge=jembatan1
[admin@MikroTik1] > interface bridge port add interface=ether2 bridge=jembatan1
 [admin@MikroTik1] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #   INTERFACE                BRIDGE                PRIORITY  PATH-COST   HORIZON
 0   ether2                     jembatan1               0x80         10     none
 1   router1-ke-router2         jembatan1               0x80         10     none
```

Setelah konfigurasi diatas, kita lakukan konfigurasi IP Address pada PC Client. IP Address harus 1 network



Setelah kita melakukan konfigurasi Interface *EoIP* dan *Bridge* pada router1 , sekarang kita akan melakukan konfigurasi yang sama pada Router2. Langkahnya sama seperti sebelumnya. Hanya saja, di bagian *Remote-Address* kita masukkan IP address dari Router1. Untuk lebih jelasnya, lihat konfigurasi dibawah ini.

```
[admin@MikroTik2] > interface eoip add name="router2-ke-router1" remote-
address=192.168.100.2 tunnel-id=1
[admin@MikroTik2] > interface eoip print
Flags: X - disabled, R - running
 0  R name="router2-ke-router1" mtu=1500 l2mtu=65535 mac-address=FE:97:00:5E:0F:73
      arp=enabled local-address=0.0.0.0 remote-address=192.168.100.2 tunnel-id=1
```

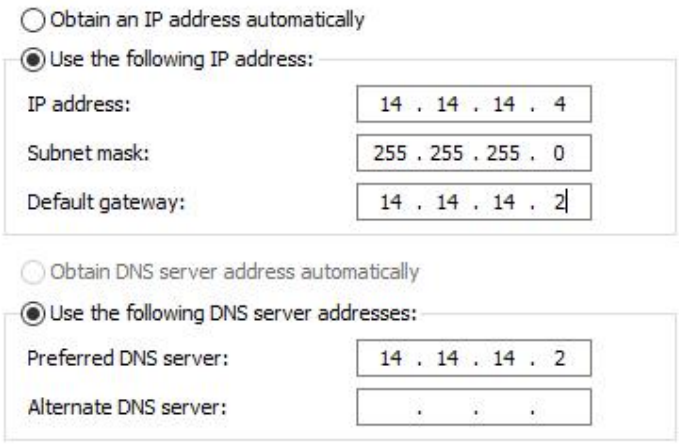
Sekarang kita akan membuat interface *bridge* untuk router2. Langkah konfigurasi nya sama seperti router1.

```
[admin@MikroTik2] > interface bridge add name=jembatan1
[admin@MikroTik2] > interface bridge print
Flags: X - disabled, R - running
 0  R name="jembatan1" mtu=1500 l2mtu=65535 arp=enabled mac-address=00:00:00:00:00:00
      protocol-mode=none priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-
      message-age=20s forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

Setelah membuat interface *bridge*, sekarang kita akan memasukkan interface *EoIP* dan *ether2* kedalam interface *bridge*. Perintah nya adalah sebagai berikut :

```
[admin@MikroTik2] > interface bridge port add interface=router2-ke-router1 bridge=jembatan1
[admin@MikroTik2] > interface bridge port add interface=ether2 bridge=jembatan1
[admin@MikroTik2] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #   INTERFACE            BRIDGE          PRIORITY  PATH-COST  HORIZON
 0   router2-ke-router1   jembatan1          0x80         10     none
 1   ether2               jembatan1          0x80         10     none
```

Setelah itu, lakukan konfigurasi IP Address pada PC Client router 2.



Untuk melakukan test, kita coba lakukan *ping* antar PC Client atau PC Client menuju Router. Maka hasilnya akan *reply*.

Tunneling

Tunneling adalah teknik menghubungkan Jaringan local dengan jaringan public (internet) agar bisa saling terhubung / berkomunikasi melalui sebuah “terowongan” atau *tunnel*.

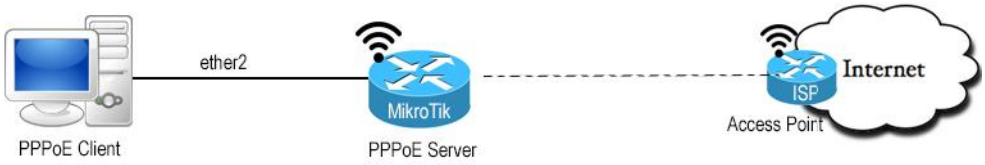
PPPoE SERVER

PPPoE atau Point to Point Protocol over Ethernet adalah pengembangan dari PPP (Point to Point Protocol). *PPP* sendiri adalah *Protocol Point to Point* yang digunakan untuk menghubungkan langsung antara perangkat satu dengan perangkat lain nya. PPP diterapkan pada serial Modem, agar modem tersebut terhubung langsung atau *face-to-face* dengan ISP. Sebagai contoh dari Point to Point, kita bisa lihat gambar topologi sederhana pada gambar dibawah ini.

Bisa kita lihat gambar diatas, PC Client dan Router terhubung melalui sebuah switch. Tetapi, dengan teknik *Point to Point* ini, nantinya PC Client seolah olah terhubung langsung dengan Router, atau istilahnya *face-to-face* dengan router.

Jika kita menerapkan *Point to Point* antar Client dan Router, maka nantinya setiap Client yang terhubung dengan Router harus memiliki *Autentikasi* terlebih dahulu. Jadi, jika Client ingin saling berkomunikasi antar Client lain nya, harus melalui Router terlebih dahulu karena Client langsung berhubungan dengan Router.

Bedanya *PPP* dan *PPPoE* sendiri ada di bagian penggunaan atau penerapan nya. Pada *PPP* digunakan pada jaringan yang menggunakan serial modem, Jika *PPPoE* digunakan pada jaringan Ethernet.



Kita akan melakukan konfigurasi PPPoE seperti gambar diatas, dimana router MikroTik akan menjadi *PPPoE* server, terhubung dengan koneksi internet melalui *Access Point (wlan1)*, dan terkoneksi dengan PC Client melalui interface *ether2*. Untuk langkah konfigurasi nya, bisa lihat seperti dibawah ini

Pertama, kita akan membuat dulu *IP Pool* untuk *remote-address* atau IP yang akan diberikan kepada Client nantinya. Untuk membuat *IP Pool*, perintah text (CLI) nya adalah sebagai berikut :

Sebagai contoh, disini saya akan membuat *IP Pool* dengan nama *ppoe* dan hanya mempunyai 5 range address, dimulai dari *13.13.13.5-13.13.13.10*

```
[admin@MikroTik] > ip pool add name=ppoe range=13.13.13.5-13.13.13.10
[admin@MikroTik] > ip pool print
 # NAME                                    RANGES
 0 ppoe                                    13.13.13.5-13.13.13.10
```

Setelah kita membuat *IP Pool*, sekarang kita akan menambahkan *profile PPP*. Langkah konfigurasi nya adalah sebagai berikut :

```
[admin@MikroTik] > ppp profile add name=ppoe local-address=13.13.13.1 remote-address=ppoe
[admin@MikroTik] > ppp profile print
Flags: * - default
 0 * name="default" remote-ipv6-prefix-pool=none use-ipv6=yes use-mpls=default use-
     compression=default use-vj-compression=default use-encryption=default only-one=default
     change-tcp-mss=yes

 1   name="ppoe" local-address=13.13.13.1 remote-address=ppoe remote-ipv6-prefix-pool=none
     use-ipv6=yes use-mpls=default use-compression=default use-vj-compression=default use-
     encryption=default only-one=default change-tcp-mss=default
```

Keterangan :

Local-address = IP Address dari interface *ether2* (interface *PPPoE server*)

Remote-Address = IP address yang akan diberikan kepada client. Kita masukkan dengan *IP Pool* yang sudah kita buat sebelumnya.

Setelah mengatur *PPP Profile,* sekarang kita akan membuat *PPP Secret. PPP Secret* ini adalah username dan password yang nantinya akan digunakn oleh *PPPoE Client*. Untuk membuat *PPP secret*, perintah text nya adalah sebagai berikut

```
[admin@MikroTik] > ppp secret add name=andri password=andri123 service=pppoe profile=ppoe
[admin@MikroTik] > ppp secret print
Flags: X - disabled
 #   NAME            SERVICE CALLER-ID       PASSWORD        PROFILE         REMOTE-ADDRESS
 0   andri           pppoe                   andri123        ppoe
```

Pada bagian *service* kita isi dengan *pppoe,* karena *ppp secret* tersebut nantinya hanya akan digunakan untuk *service pppoe.* Agar *ppp secret* tersebut bisa digunakan untuk semua *service*, bisa kita isi dengan perintah *any.*

Setelah membuat *PPP Secret*, sekarang kita akan menambahkan *PPPoE Server*nya.

```
[admin@MikroTik] > interface pppoe-server server add service-name=ppoe interface=ether2
one-session-per-host=yes default-profile=ppoe disabled=no
[admin@MikroTik] > interface pppoe-server server print
Flags: X - disabled
 0    service-name="ppoe" interface=ether2 max-mtu=1480 max-mru=1480 mrru=disabled
      authentication=pap,chap,mschap1,mschap2 keepalive-timeout=10 one-session-per
      host=yes max-sessions=0 default-profile=ppoe
```

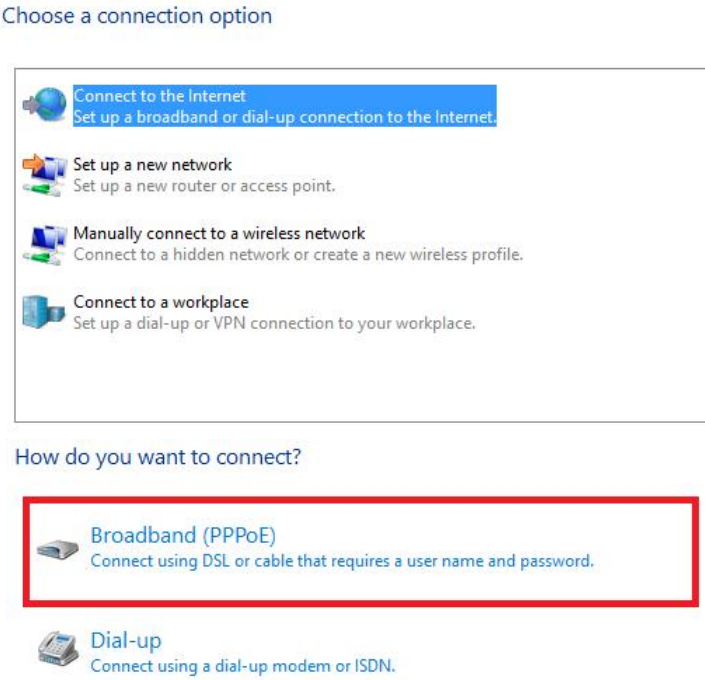
pada bagian *interface* kita isi dengan *ether2,* karena *PPPoE Client* terhubung melalui interface *ether2*

Konfigurasi pada *PPPoE Server* telah selesai. Sekarag, kita akan lakukan konfigurasi atau pengujian pada *PPPoE Client* yang mempunyai OS Windows

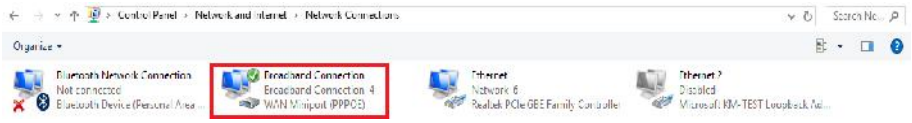
Langkah Pengujian *PPPoE* pada Client yang mempunyai OS Windows adalah sebagai berikut

1. Buka ***Network Sharing and Center*** lalu klik ***Set up a new Connection or Network***

2. Setelah itu, kita pilih ***Connect to the Internet*****,** lalu pilih ***Broadband (PPPoE)***



3. Setelah itu, akan ada form *Username dan Password*. Isi Username dan Password dengan akun *PPP Secret* yang telah kita buat sebelumnya. Jika sudah, klik Connect
4. Setelah selesai, akan ada ***Broadband Connection*** pada *Network sharing and Center.* Itu berarti, konfigurasi *PPPoE Server* kita telah berhasil

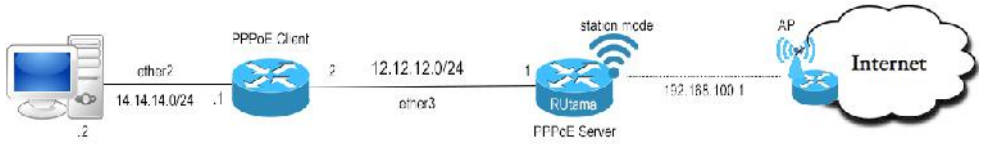


Untuk melakukan monitoring pada Client yang terhubung dengan *PPPoE server*, bisa menggunakan perintah berikut :

```
[admin@MikroTik] > ppp active print
Flags: R - radius
 #   NAME      SERVICE CALLER-ID          ADDRESS      UPTIME   ENCODING
 0   andri     pppoe   08:62:66:B5:F8:55  13.13.13.5   2m54s
```

PPPoE Client

Setelah tadi kita menjelaskan tentang cara membuat router MikroTik menjadi *PPPoE server* bagi PC Client, sekarang kita akan membahas bagaimana cara membuat router MikroTik berperan menjadi *PPPoE client*. Agar lebih jelas, coba kita lihat gambar topologi dibawah ini



Bisa kita lihat gambar diatas, yang berperan menjadi *PPPoE server* adalah *Router Utama.* Sesuai dengan gambar topologi diatas, kita akan menggunakan media Kabel sebagai penghubung antara *PPPoE server* dan *PPPoE client*. Hal yang pertama kita lakukan adalah melakukan konfigurasi pada *Router Utama* atau *PPPoE Server.*

Untuk melakukan konfigurasi *Router Utama* sebagai *PPPoE Server*, pertama, kita akan membuat *PPP Secret* terlebih dahulu yang nantinya akan digunakan oleh router 1 atau *PPPoE Client*. Sebagai contoh, disini kita akan membuat *PPP Secret* dengan Username *router1, remote-address* gunakan IP address dari *ether3* Router 1, yaitu 12.12.12.2 dan *local-address* menggunakan IP *ether3* dari Router utama, yaitu 12.12.12.1. Maka perintah text (CLI) nya adalah sebagai berikut :

```
[admin@RUtama] > ppp secret add name=client password=router1 service=pppoe local-
address=12.12.12.1 remote-address=12.12.12.2
[admin@MikroTik] > ppp secret print
Flags: X - disabled
 #  NAME      SERVICE CALLER-ID     PASSWORD      PROFILE      REMOTE-ADDRESS
 0  client    pppoe                 router1       default      12.12.12.2
```

Setelah kita melakukan konfigurasi *PPP Secret* untuk *Router1*, sekarang kita lakukan konfigurasi *PPPoE server* pada *Router Utama*. Untuk melakukan konfigurasi *PPPoE Server*, langkah konfigurasinya sama seperti pada pembahasan sebelumnya. Disini saya akan melakukan konfigurasi *PPPoE Server* dengan nama *server* dan interface nya adalah *ether3,* karena Router Utama dan Router 1 terhubung melalui Interface *ether3*. Maka perintah text (CLI) nya adalah sebagai berikut

```
[admin@RUtama] > interface pppoe-server server add service-name=server interface=ether3
one-session-per-host=yes disabled=no
[admin@RUtama] > interface pppoe-server server print
Flags: X - disabled
 0    service-name="server" interface=ether3 max-mtu=1480 max-mru=1480 mrru=disabled
      authentication=pap,chap,mschap1,mschap2 keepalive-timeout=10 one-session-per host=yes
      max-sessions=0 default-profile=default
```

Setelah kita melakukan konfigurasi PPPoE Server pada Router Utama, sekarang kita akan lakukan konfigurasi *PPPoE Client* pada Router 1. Untuk melakukan konfigurasi *PPPoE Client* pada Router 2 bisa dilakukan dengan cara dibawah ini :

Untuk melakukan konfigurasi *PPPoE Client* pada Router 1, nantinya kita akan menggunakan *PPP Secret client* yang kita telah buat pada *Router Utama* sebelumnya. Untuk langkah konfigurasi menggunakan perintah text (CLI) perintahnya adalah sebagai berikut :

```
[admin@MikroTik1] > interface pppoe-client add service-name=server user=client
password=router1 interface=ether3 add-default-route=yes use-peer-dns=yes disabled=no
[admin@MikroTik1] > interface pppoe-client print
Flags: X - disabled, R - running
 0  R name="pppoe-out1" max-mtu=1480 max-mru=1480 mrru=disabled interface=ether3
      user="client" password="router1" profile=default service-name="server" ac-name="" add-
      default-route=yes dial-on-demand=no use-peer-dns=yes allow=pap,chap,mschap1,mschap2
```

Keterangan :

- *service-name* pada Router 1 harus sama dengan *service-name* pada Router Utama, yaitu *server*
- perintah *add-default-route* berfungsi untuk menambahkan gateway default bagi router1

Bisa kita lihat gambar diatas, dibagian sebelah kiri pada daftar *PPPoE Client*, akan ada symbol **R** yang berarti *Running* (berjalan) yang artinya *PPPoE Client dan PPPoE Server* telah terhubung

Setelah kita melakukan konfigurasi diatas, berarti koneksi *PPPoE client* dan *PPPoE server* MikroTik telah berhasil dilakukan.

Setelah itu, kita lakukan pengecekan *IP Address* pada Router 1, dengan menggunakan perintah :

```
[admin@MikroTik1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK       INTERFACE
 0   14.14.14.1/24      14.14.14.0    ether2
 1   12.12.12.2/24      12.12.12.0    ether3
 2 D 12.12.12.2/32      12.12.12.1    pppoe-out1
```

Bisa kita lihat gambar diatas, Router 1 mendapatkan IP Address dari *PPPoE Server* atau Router Utama dan memiliki symbol **D** yang berarti *Dynamic*

Sekarang, kita cek apakah Router 1 telah mendapatkan *gateway* default dari Router Utama menggunakan perintah :

```
[admin@MikroTik1] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS        PREF-SRC      GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                       12.12.12.1             1
 1 ADC  12.12.12.0/24     12.12.12.2    ether3                 0
 2 ADC  12.12.12.1/32     12.12.12.2    pppoe-out1             0
 3 ADC  14.14.14.0.0/24   14.14.14.1    ether1                 0
```

Bisa kita lihat gambar diatas, router1 juga telah mendapatkan *default gateway* dari Router Utama.

Jika kita lihat lagi gambar topologi diatas, pada Router 1 terhubung dengan PC Client melalui interface *ether2*. Agar PC client tersebut bisa terhubung dengan jaringan internet melalui Router Utama, kita bisa menggunakan *Firewall NAT Masquerade*, menggunakan teknik *Static Routing,* atau menambahkan *DHCP Server* interface *ether2.* Jika menggunakan masquerade, kita hanya tinggal membuat rule *firewall nat*

```
[admin@MikroTik1] > ip firewall nat add chain=srcnat out-interface=pppoe action=masquerade
[admin@MikroTik1] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade out-interface=pppoe-out1
```

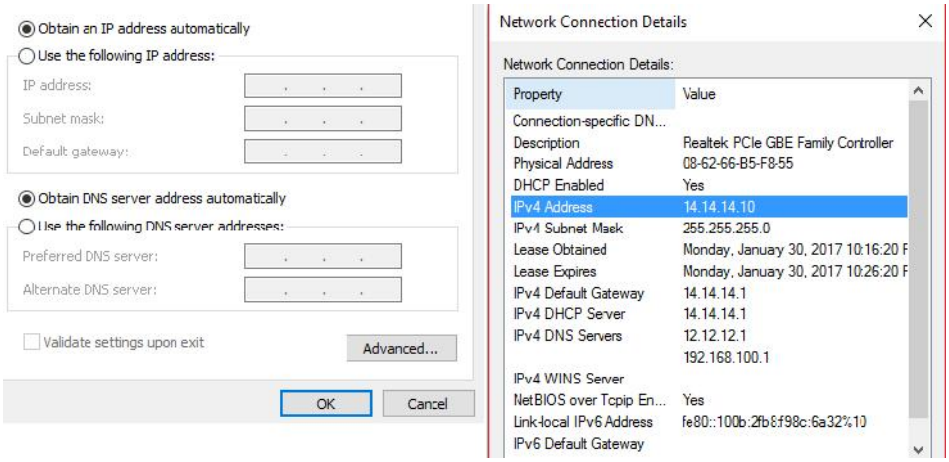
Selain menggunakan teknik *masquerade* kita juga bisa menggunakan teknik *routing static* pada Router Utama. Jika menggunakan teknik *routing static*, kita akan

```
[admin@RUtama] > ip route add dst-address=14.14.14.0/24 gateway=12.12.12.2
[admin@RUtama] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS          PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                           192.168.100.1          0
 1 ADC  12.12.12.0/24       12.12.12.2      ether3                 0
 2 ADC  12.12.12.2/32       12.12.12.1      <pppoe-client>         0
 3 A  S  14.14.14.0/24                      12.12.12.2             1
 4 ADC  192.168.100.0/24    192.168.100.14  wlan1                  0
```

Jika kedua cara itu tidak *ampuh* dan PC Client masih tidak bisa terkoneksi dengan jaringan internet, kita bisa menambahkan *DHCP Server* pada Router 1. Untuk langkah konfigurasinya sendiri sama seperti yang dibahas di bab *DHCP*. Disini kita akan menggunakan interface *ether2*. Perintah text (CLI) untuk *DHCP server* adalah sebagai berikut :

```
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 14.14.14.0/24
Select gateway for given network

gateway for dhcp network: 14.14.14.1
If this is remote network, enter address of DHCP relay

There is no such IP network on selected interface
dhcp relay: 14.14.14.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 14.14.14.2-14.14.14.10
Select DNS servers

dns servers: 12.12.12.1,192.168.100.1
Select lease time

lease time: 10m
```

Setelah itu, kita lakukan konfigurasi *IP Address* dari PC Client menjadi Dynamic. Lalu kita lihat ***detail*** dari koneksi ethernet, maka PC Client akan mendapatkan IP Address automatis dari router 1

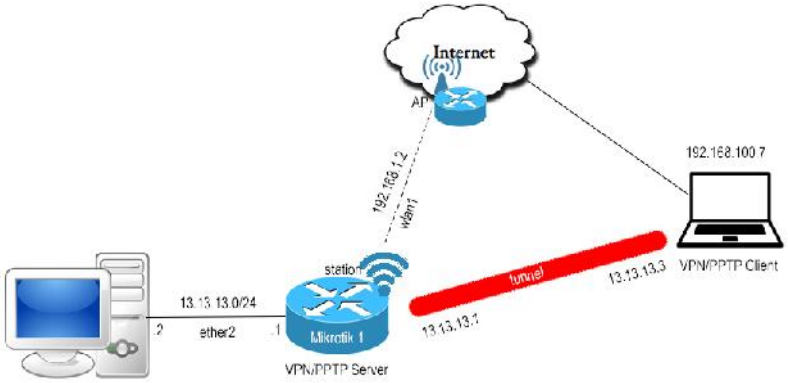


Konfigurasi diatas sudah selesai, maka seharusnya PC Client sudah dapat terkoneksi dengan jaringan Internet.

PPTP Server

Dalam menggunakan protocol *PPTP* ini nantinya akan membentuk suatu *VPN* (Virtual Private Network). *VPN* sendiri adalah teknik menggabungkan beberapa jaringan local melalui jaringan internet (public) menggunakan teknik *tunneling*.

Disini kita akan mencoba konfigurasi PPTP dengan topologi sepeti dibawah ini



Bisa kita lihat topologi diatas, router MikroTik bertindak sebagai *VPN Server*, lalu ada satu Laptop yang bertindak sebagai *VPN Client*.

Pada topologi diatas, router MikroTik terhubung dengan 1 PC Client melalui jaringan local (*ether2 dengan IP network 13.13.13.0/24*) PC tersebut memiliki IP Address 13.13.13.2, dan ada sebuah Laptop (*remote host)* yang terhubung melalui jaringan Internet dan memiliki IP Address *192.168.100.7.*

Nantinya, Laptop atau PC *remote host* ini ketika terhubung dengan *VPN/PPTP server*, akan memiliki IP address yang satu network dengan PC Client yang terhubung melalui jaringan local (13.13.13.0/24). Jadi, PC Remote host ini akan mempunyai 2 IP, yaitu *IP Public* dan *IP Private*.

IP Public digunakan untuk terhubung dengan jaringan Internet, sedangkan *IP private,* nantinya akan digunakan untuk berkomunikasi dengan PC Client jaringan local (13.13.13.0/24). Jadi, Laptop atau PC *remote host* akan tergabung dalam jaringan local 13.13.13.0/24 secara *Virtual*. Jadi itulah VPN.

Untuk konfigurasi awal, kita akan membuat *PPP Secret* untuk Laptop atau *PC remote host* terlebih dahulu. Untuk langkah konfigurasinya sendiri sama seperti pada pembahasan sebelumnya, tetapi di bagian *service* kita isi dengan ***pptp,*** karena akun atau *PPP Secret* ini akan digunakan untuk *PPTP* bukan *PPPoE.* Perintah text nya adalah sebagai berikut :

```
[admin@RUtama] > ppp secret add name=andri password=asdqwe local-address=13.13.13.1
remote-address=13.13.13.3 service=pptp
```

Setelah itu, kita akan melakukan konfigurasi *PPTP server* pada router MikroTik. Jika melalui Perintah text (CLI) perintahnya adalah

```
[admin@RUtama] > interface pptp-server server set enabled=yes
[admin@RUtama] > interface pptp-server server print
                  enabled: yes
                  max-mtu: 1460
                  max-mru: 1460
                      mrru: disabled
          authentication: mschap1,mschap2
     keepalive-timeout: 30
          default-profile: default-encryption
```

Agar Laptop atau *PC remote host* dapat melakukan *ping* kepada PC client local, maka kita harus melakukan konfigurasi *ARP* terlebih dahulu pada interface *ether2*. Perintah text (CLI) nya adalah sebagai berikut

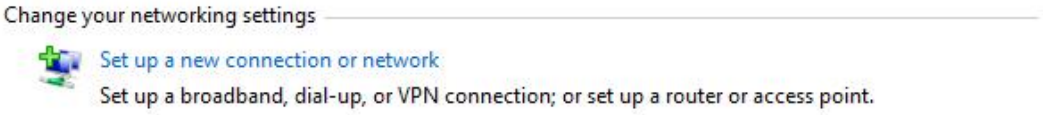
```
[admin@RUtama] > interface ethernet set ether2 arp=proxy-arp
[admin@RUtama] > interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                MTU MAC-ADDRESS       ARP
 0 R  ether1                              1500 00:04:96:BC:9F:00 enabled
 1 R  ether2                              1500 00:04:96:BC:9F:01 proxy-arp
 2 R  ether3                              1500 00:04:96:BC:9F:02 enabled
 3 R  ether4                              1500 00:04:96:BC:9F:03 enabled
 4 R  ether5                              1500 00:04:96:BC:9F:04 enabled
```

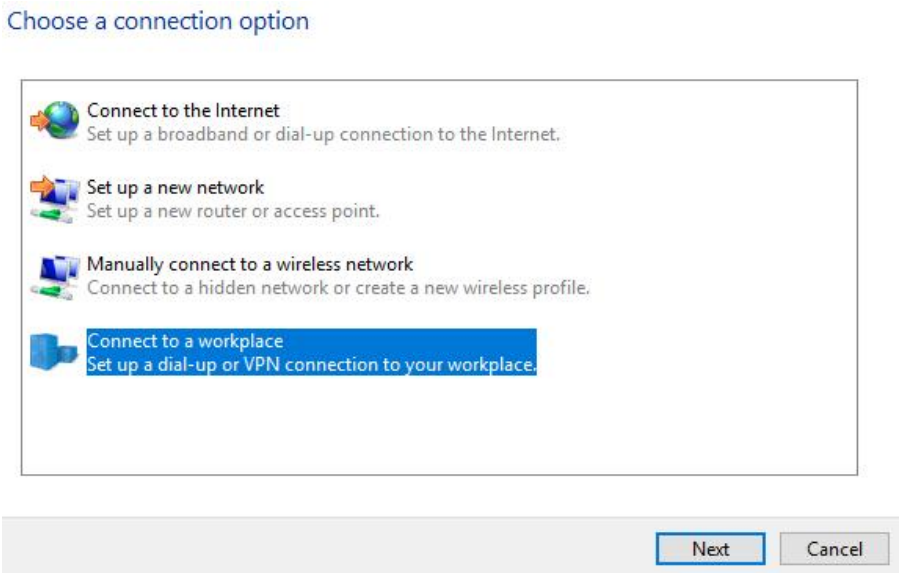
Konfigurasi pada Router atau *PPTP Server* sudah selesai. Sekarang, kita akan melakukan pengujian pada *PPTP Client* yang menggunakan OS Windows

Langkah konfigurasi *PPTP Client* (OS Windows)

1. Pertama, kita buka ***Network Sharing and Center*** di Control Panel

2. Setelah itu klik ***Setup a new connection or network,*** lalu pilih ***Connect to a Workplace***





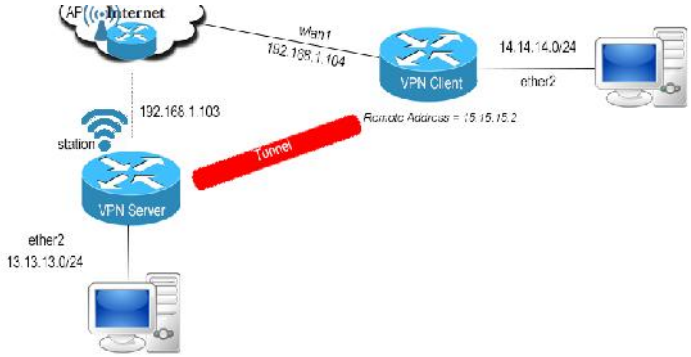
3. Pilih ***No, create a new connection*** lalu pilih ***use my internet connection (VPN)***

4. Lalu isi internet address dengan IP Address Router MikroTik terhubung dengan internet *(wlan1)* setelah itu klik next, maka akan form login username dan password (disini saya menggunakan os windows 10, jadi mungkin akan seditik berbeda)
5. Isi Username dan Password dengan *PPP Secret* yang telah kita konfigurasi sebelumnya, lalu klik *Connect*.
6. PC Remote Host seharusnya telah terhubung dengan *PPTP Server* lalu akan ada *VPN Connection* pada *Network sharing and Center.*

Konfigurasi PPTP Server diatas sudah selesai. Jadi, setiap *PC Remote Host* ingin terkoneksi dengan jaringan Internet, harus melalui Router MikroTik (*VPN / PPTP Server*) terlebih dahulu. Meskipun PC Remote Host tadi mempunyai jaringan internet sendiri. Hal itu dikarenakan *PC Remote Host* tadi sudah masuk ke dalam Jaringan Lokal secara *Virtual*.

PPTP Client

Setelah kita melakukan konfigurasi *PPTP* dengan topologi sebelumnya, yaitu melakukan konfigurasi Router MikroTik sebagai *PPTP Server.* Sekarang, bagaimana cara melakukan konfigurasi jika Router MikroTik menjadi *PPTP Client*? Untuk lebih jelasnya, kita bisa lihat gambar topologi dibawah ini



Bisa kita lihat gambar diatas, terdapat 2 router MikroTik dengan masing masing PC Client. Router MikroTik 1 bertindak sebagai *PPTP Server*, lalu Router MikroTik 2 sebagai *PPTP Client*.

Bisa kita lihat pada topologi diatas, Router 1 akan menggunakan IP Local (*local-address*) 15.15.15.1 dan nantinya Router 2 akan memiliki IP (*remote-address*) 15.15.15.2. IP Address Local tersebut fungsi nya agar router bisa saling terhubung pada saat membuat *tunnel*.

Untuk langkah konfigurasi yang pertama, kita akan melakukan konfigurasi *PPP Secret* pada Router 1 (*PPTP* Server) yang nantinya akan digunakan oleh Router 2 (*PPTP Client*).

Untuk langkah konfigurasi *PPP Secret* nya sendiri, sama seperti sebelumnya. Hanya saja, disini kita akan menambahkan perintah text atau parameter *routes* agar PC client pada jaringan local bisa saling terhubung satu sama lain. Untuk *gateway* nya, kita akan menggunakan IP network dari Interface *ether2* pada Router 2 lalu menggunakan *remote-address* dari Router 2. Perintah text (CLI) nya adalah sebagai berikut :

```
[admin@RUtama] > ppp secret add name=router2 password=mikrotik2 local-address=15.15.15.1
remote-address=15.15.15.2 routes="14.14.14.0/24 15.15.15.2" service=pptp
[admin@RUtama] > ppp secret print detail
Flags: X - disabled
 0    name="router2" service=pptp caller-id="" password="mikrotik2" profile=default local-
      address=15.15.15.1 remote-address=15.15.15.2 routes="14.14.14.0/24 15.15.15.2" limit-bytes-
      in=0 limit-bytes-out=0
```

Setelah kita melakukan konfigurasi *PPP Secret*, sekarang kita lanjutkan dengan mengaktifkan *PPTP Server* pada router1. Perintah text nya adalah sebagai berikut

```
[admin@RUtama] > interface pptp-server server set enabled=yes
[admin@RUtama] > interface pptp-server server print
               enabled: yes
               max-mtu: 1460
               max-mru: 1460
                  mrru: disabled
     authentication: mschap1,mschap2
 keepalive-timeout: 30
      default-profile: default-encryption
```

Konfigurasi pada Router 1 atau *PPTP Server* sudah selesai, sekarang kita lanjutkan dengan melakukan konfigurasi pada *PPTP Client* atau Router 2.

Pada Router 2, disini kita akan mengaktifkan interface *PPTP Client* menggunakan *PPP Secret* yang telah kita konfigurasikan sebelumnya. Untuk mengaktifkan *PPTP Client* pada Router 2 melalui perintah text (CLI), perintah nya adalah sebagai berikut

```
[admin@MikroTik1] > interface pptp-client add user=router2 password=mikrotik2 connect-
to=192.168.1.103 disabled=no
[admin@MikroTik1] > interface pptp-client print
Flags: X - disabled, R - running
 0  R name="pptp-out1" max-mtu=1460 max-mru=1460 mrru=disabled connect-to=192.168.1.103
      user="router2" password="mikrotik2" profile=default-encryption add-default-route=no dial-
      on-demand=no allow=pap,chap,mschap1,mschap2
```

Kita bisa lihat gambar diatas, dibagian sebelah kiri ada symbol **R** yang berarti *Running* atau *PPTP Client* telah berhasil terkoneksi

Konfigurasi pada Router 2 atau *PPTP Client* sudah selesai.

Sekarang, untuk melakukan pengecekan terhadap *PPTP Client* yang terhubung dengan *PPTP Server* melalui Router 1, bisa menggunakan perintah text sebagai berikut :

```
[admin@RUtama] > ppp active print
Flags: R - radius
 #   NAME          SERVICE CALLER-ID        ADDRESS         UPTIME   ENCODING
 0   router2       pptp    192.168.1.104    15.15.15.2      3m56s
```

Bisa kita lihat gambar diatas, terdapat 1 Client yang terhubung dengan *PPTP Server*, yaitu Router 2. Artinya, konfigurasi *PPTP Server dan PPTP Client* telah berhasil.

Untuk melakukan pengecekan *Interface* yang aktif pada Router 1, bisa menggunakan perintah berikut :

```
[admin@RUtama] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU  MAX-L2MTU MAC-ADDRESS
 0     ether1                              ether            1500  1598       2028 6C:3B:6B:4F:CA:81
 1  R  ether2                              ether            1500  1598       2028 6C:3B:6B:4F:CA:82
 2     ether3                              ether            1500  1598       2028 6C:3B:6B:4F:CA:83
 3     ether4                              ether            1500  1598       2028 6C:3B:6B:4F:CA:84
 4  R  wlan1                               wlan             1500  1600       2290 6C:3B:6B:4F:CA:85
 5 DR  <pptp-router2>                      pptp-in          1450
```

Bisa kita lihat diatas, terdapat interface <*pptp-router2*> yang aktif pada interface router1. Bisa kita lihat juga pada sebelah kiri dari interface <*pptp-router2*> terdapat symbol **DR** yang berarti ***Dynamic & Running***.

Untuk melakukan pengecekan IP Address dari *PPTP Client* yang terkoneksi pada Router 1, bisa menggunakan perintah berikut :

```
[admin@RUtama] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   13.13.13.1/24      13.13.13.0      ether2
 1   192.168.1.3/24     192.168.1.0     wlan1
 2 D 192.168.1.103/24   192.168.1.0     wlan1
 3 D 15.15.15.1/32      15.15.15.2      <pptp-router2>
```

Setelah itu, kita lakukan pengecekan *ip route* pada Router 1. Perintah nya adalah :

```
[admin@RUtama] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADS  0.0.0.0/0                          192.168.1.1               0
 1   S  0.0.0.0/0                          192.168.1.1               1
 2 ADC  13.13.13.0/24      13.13.13.1      ether2                    0
 3 ADS  14.14.14.0/24                      15.15.15.2                1
 4 ADC  15.15.15.2/32      15.15.15.1      <pptp-router2>            0
 5 ADC  192.168.1.0/24     192.168.1.3     wlan1                     0
```

Konfigurasi *PPTP Server* dan *PPTP Client* sudah selesai.

Sekarang, untuk melakukan pengujian, kita coba lakukan *ping* antar router 1 dan router 2.

Dari Router 1 ke Router 2

```
[admin@RUtama] > ping 14.14.14.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 14.14.14.1                                 56  64 2ms
    1 14.14.14.1                                 56  64 2ms
    2 14.14.14.1                                 56  64 2ms
    3 14.14.14.1                                 56  64 1ms
    4 14.14.14.1                                 56  64 1ms
    5 14.14.14.1                                 56  64 1ms
    sent=6 received=6 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

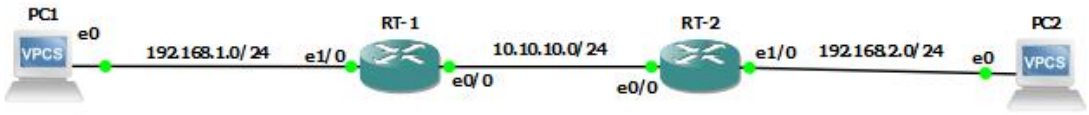
Dari Router 2 ke Router 1

```
[admin@Mikrotik1] > ping 14.14.14.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 14.14.14.1                                 56  64 0ms
    1 14.14.14.1                                 56  64 0ms
    2 14.14.14.1                                 56  64 0ms
    3 14.14.14.1                                 56  64 0ms
    4 14.14.14.1                                 56  64 0ms
    5 14.14.14.1                                 56  64 0ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Routing Protocol

Routing adalah teknik menghubungkan beberapa jaringan yang memiliki Network yang berbeda. Routing sendiri sebagian besar di bagi menjadi 2 teknik, yaitu Static dan Dynamic.

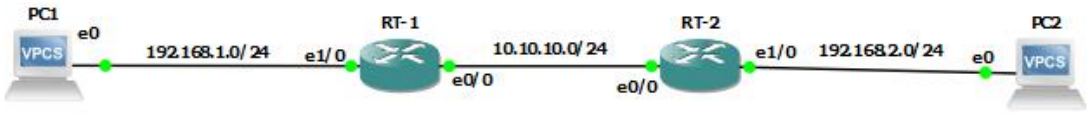
Disini kita akan membahas tentang Routing Static. Teknik Routing Static ini sebenarnya sudah kita lakukan pada pembahasan menghubungkan Routerboard dengan internet. Jika menggunakan teknik routing static, kita harus mengetahui IP tujuan (dst-address) dan Jalur (gateway) yang akan dilalui. Sebagai contoh, kita bisa lihat gambar topologi dibawah ini



Bisa kita lihat gambar diatas, Router MikroTik 1 (10.10.10.1) dan PC Client dari MikroTik 2 (192.168.2.10/24) mempunyai IP Address dan Network yang berbeda. Dan begitu pula sebaliknya. Router MikroTik 2 (10.10.10.2) dan PC Client MikroTik 1 (192.168.1.10/24) mempunyai IP Address dan Network yang berbeda. Jadi, bagaimana jika Router MikroTik 1 ingin menuju/berkomunikasi dengan PC Client MikroTik 2 ? Kita akan membahasnya di Bab ini.

Static Routing

Sekarang, kita akan mencoba teknik routing static dengan topologi masih menggunakan di atas. Tujuan nya, agar mengerti bagaimana cara kerja dan konfigurasi dari routing static itu sendiri.



Sekarang, kita langsung ke langkah konfigurasi Routing Static dengan topologi diatas. Pertama, kita tambahkan dulu IP Address Router RT-1 (ether1 & ether2) dan PC IP

Address PC client nya(Karena contohnya sudah ada di bab sebelumnya maka tidak saya tampilkan).

Setelah menambahkan IP Address kedua router dan pc tersebut, sekarang kita akan buat IP Route nya agar kedua router dan pc tersebut saling tersambung. Untuk melakukan pengecekan pada konfigurasi IP Route dari kedua router tersebut, kita bisa menggunakan perintah text berikut :

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS         PREF-SRC       GATEWAY         DISTANCE
 0 ADC  10.10.10.0/24      10.10.10.1     ether1               0
 1 ADC  192.168.1.0/24     192.168.1.1    ether2               0
```

Pertama, kita akan konfigurasi IP Route di Router MikroTik 1. Jika Router1 ingin menuju Network 192.168.2.0/24 (dst-address), maka router1 harus melalui Jalur (gateway) 10.10.10.2. Berarti, konfigurasi IP Route Router MikroTik 1 adalah sebagai

```
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24 gateway=10.10.10.2
```

Setelah itu, kita cek menggunakan perintah berikut :

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADC  10.10.10.0/24     10.10.10.1      ether1               0
 1 ADC  192.168.1.0/24    192.168.1.1     ether2               0
 2 A S  192.168.2.0/24                    10.10.10.2           1
```

Bisa kita lihat gambar diatas, maka akan ada symbol **A S** yang berarti Active Static. Sekarang, kita konfigurasi kan Router MikroTik 2. Jika Router2 ingin menuju Network 192.168.1.0/24 , maka harus melewati 10.10.10.1 sebagai Jalur (gateway) nya. Untuk langkah konfigurasinya adalah sebagai berikut .

```
[admin@MikroTik] > ip route add dst-address=192.168.1.0/24 gateway=10.10.10.1
```

Setelah itu, kita cek menggunakan perintah **ip route print**

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS      PREF-SRC      GATEWAY         DISTANCE
 0 ADC  10.10.10.0/24    10.10.10.2    ether1              0
 1 A S  192.168.1.0/24                 10.10.10.1          1
 2 ADC  192.168.2.0/24   192.168.2.1   ether2              0
```

Konfigurasi nya sudah selesai, maka sekarang jaringan diatas sudah saling terhubung. Untuk mengetest nya, coba lakukan ping dari PC 1 ke PC 2 dan sebaliknya. Jika berhasil, maka akan reply.

```
PC1> ping 192.168.2.10
84 bytes from 192.168.2.10 icmp_seq=1 ttl=62 time=87.535 ms
84 bytes from 192.168.2.10 icmp_seq=2 ttl=62 time=22.807 ms
84 bytes from 192.168.2.10 icmp_seq=3 ttl=62 time=25.312 ms
```

```
PC2> ping 192.168.1.10
84 bytes from 192.168.1.10 icmp_seq=1 ttl=62 time=16.456 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=62 time=10.448 ms
84 bytes from 192.168.1.10 icmp_seq=3 ttl=62 time=14.265 ms
```

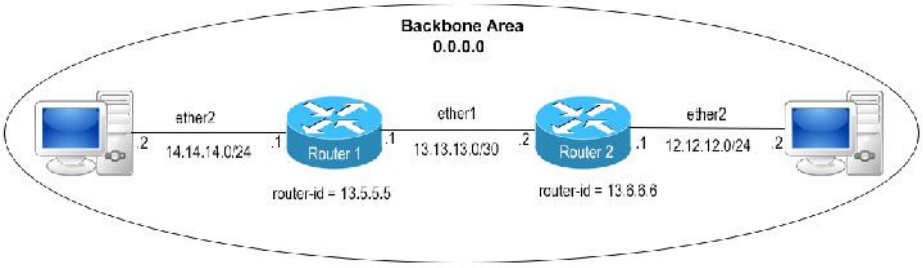
OSPF

OSPF atau *Open Shortest Path First* adalah Protocol Routing jenis *Link State* yang digunakan untuk menghubungkan berbagai Router yang terdapat dalam satu *Autonomous System*. Autonomous System sendiri seperti yang telah dijelaskan pada sub menu sebelumnya adalah kumpulan beberapa router yang berada dibawah kendali admin dan strategi routing yang sama. Oleh karena itu OSPF masuk kedalam kategori IGP (Interior Gateway Protocol).

Dalam mengimplementasikan OSPF sendiri, terdapat dua cara, yaitu *Single Area OSPF* dan *Multi Area OSPF*. Penggunaan Multi Area OSPF sendiri biasanya digunakan jika jumlah Router lebih dari 50.

Konfigurasi Dasar OSPF Single Area

Kita akan lakukan konfigurasi OSPF single area pada topologi dibawah ini



Bisa kita lihat pada gambar diatas, Router 1 dan Router 2 terhubung melalui interface *ether1* dan masing masing Router mempunyai Client dengan Network 14.14.14.0/24 (R1) dan 12.12.12.0/24 (R2). Karena kita akan melakukan konfigurasi OSPF Single Area, maka kita tidak perlu melakukan konfigurasi *regular area*, cukup menggunakan Backbone saja. Untuk Backbone Area sendiri telah tersedia secara default oleh MikroTik, jadi kita tidak perlu membuatnya terlebih dahulu. Untuk melihat area yang ada pada router mikrotik, bisa menggunakan perintah text seperti dibawah ini

```
[admin@MikroTik] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #   NAME                                AREA-ID       TYPE    DEFAULT-COST
 0  * backbone                            0.0.0.0      default
```

Sekarang, menuju langkah yang pertama, yaitu mengaktifkan OSPF pada interface Router

Untuk mengaktifkan Routing Protocol OSPF pada topologi diatas, kita hanya perlu mengaktifkan Routing Protocol OSPF pada interface *ether1* terhadap kedua Router, tidak perlu diaktifkan pada *ether2* karena PC Client tidak membutuhkan OSPF Packet. Untuk mengaktifkan OSPF, perintah text nya adalah sebagai berikut :

```
[admin@RT-1] > routing ospf interface add interface=ether1
```

```
[admin@RT-2] > routing ospf interface add interface=ether1
```

Setelah kita mengaktifkan OSPF pada interface *ether1,* sekarang kita lakukan konfigurasi *Router-ID* pada kedua Router.

Untuk melakukan konfigurasi Router ID melalui perintah text, perintahnya adalah sebagai berikut

```
[admin@RT-1] > routing ospf instance set default router-id=13.5.5.5
[admin@RT-1] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.5.5.5 distribute-default=never redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-
      ospf=no metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-
      bgp=auto metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

```
[admin@RT-2] > routing ospf instance set default router-id=13.6.6.6
[admin@RT-2] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.6.6.6 distribute-default=never redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
      metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

Konfigurasi router-id diatas telah selesai. Sekarang, untuk langkah konfigurasi terakhir kita lakukan konfigurasi *Advertise Network*.

Untuk melakukan konfigurasi Advertise Network, perintah nya adalah sebagai berikut

```
[admin@RT-1] > routing ospf network add network=13.13.13.0/24 area=backbone
[admin@RT-1] > routing ospf network add network=14.14.14.0/24 area=backbone
[admin@RT-1] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK          AREA
 0   13.13.13.0/24    backbone
 1   14.14.14.0/24    backbone
```

```
[admin@RT-2] > routing ospf network add network=13.13.13.0/24 area=backbone
[admin@RT-2] > routing ospf network add network=12.12.12.0/24 area=backbone
[admin@RT-2] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK          AREA
 0   13.13.13.0/24    backbone
 1   12.12.12.0/24    backbone
```

Konfigurasi Advertise Network telah selesai. Maka, seharusnya jaringan-jaringan telah mencapai kondisi *convergence* dan dapat terhubung satu sama lainnya. Untuk melakukan pengujian, kita bisa lakukan *ping* antar PC Client Router 1 dan 2

```
PC1> ping 12.12.12.2
84 bytes from 12.12.12.2 icmp_seq=1 ttl=62 time=32.002 ms
84 bytes from 12.12.12.2 icmp_seq=2 ttl=62 time=11.000 ms
84 bytes from 12.12.12.2 icmp_seq=3 ttl=62 time=19.002 ms
```

```
PC2> ping 14.14.14.2
84 bytes from 14.14.14.2 icmp_seq=1 ttl=62 time=35.002 ms
84 bytes from 14.14.14.2 icmp_seq=2 ttl=62 time=8.001 ms
84 bytes from 14.14.14.2 icmp_seq=3 ttl=62 time=24.001 ms
```

Bisa kita lihat diatas, hasilnya *reply* yang berarti kedua jaringan telah mencapai kondisi *convergence* dan saling terhubung satu sama lain

Konfigurasi OSPF Single Area pada Topologi diatas telah selesai. Sekarang, coba kita lihat table routing pada Router 1, maka akan terlihat seperti dibawah ini

```
[admin@RT-1] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADo  12.12.12.0/24                    13.13.13.2          110
 1 ADC  13.13.13.0/24     13.13.13.1     ether1                0
 2 ADC  14.14.14.0/24     14.14.14.1     ether2                0
```

Bisa kita lihat diatas, pada no index 0 terdapat entry routing dengan symbol **ADo,** yang berarti *Active, Dynamic, OSPF.* Sekarang kita lihat table routing pada router 2

```
[admin@RT-2] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADC  12.12.12.0/24     12.12.12.1     ether2                0
 1 ADC  13.13.13.0/24     13.13.13.2     ether1                0
 2 ADo  14.14.14.0/24                    13.13.13.1          110
```

Bisa kita lihat juga pada gambar diatas, Router 2 mendapatkan entry routing dynamic dari OSPF untuk menuju network 14.14.14.0/24.

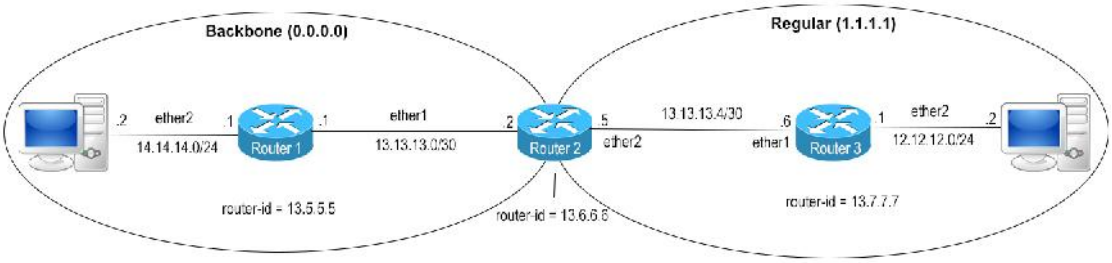
Kita juga bisa melihat Network yang diketahui oleh Router melalui OSPF. Untuk melihatnya, kita bisa menggunakan perintah text berikut :

```
[admin@RT-1] > routing ospf route print
 # DST-ADDRESS      STATE       COST      GATEWAY       INTERFACE
 0 12.12.12.0/24    intra-area  20        13.13.13.2    ether1
 1 13.13.13.0/24    intra-area  10        0.0.0.0       ether1
 2 14.14.14.0/24    intra-area  10        0.0.0.0       ether2
```

Bisa kita lihat pada OSPF route diatas, terdapat network-network yang dikenal router melalui OSPF. Terdapat juga nilai *cost* dari masing masing entry tersebut, dimana nilai cost untuk menuju network 12.12.12.0/24 adalah 20 karena melewati 2 interface. Bisa kita lihat lagi, terdapat parameter STATE yang berisi *intra-area.* Maksud dari intra-area tersebut menunjukkan bahwa ketiga Network tersebut berada di area yang sama, yaitu Backbone Area.

Konfigurasi Dasar OSPF Multi Area

Setelah sebelumnya kita melakukan konfigurasi Dasar OSPF Single Area, sekarang kita akan lakukan konfigurasi dasar OSPF Multi Area.



Oke, kita langsung saja menuju langkah konfigurasi nya. Pertama, kita akan *mengaktifkan routing protocol OSPF* pada interface Router. Untuk langkahnya sendiri hampir sama seperti Single Area, perbedaan nya disini terletak pada Router 2 dimana kita akan mengaktifkan interface *ether1* dan *ether2* karena pada Router 2 kedua interface tersebut terhubung dengan Router OSPF lain nya.

```
[admin@RT-1] > routing ospf interface add interface=ether1
```

```
[admin@RT-2] > routing ospf interface add interface=ether1
[admin@RT-2] > routing ospf interface add interface=ether2
```

```
[admin@RT-3] > routing ospf interface add interface=ether1
```

Setelah mengaktifkan interface OSPF, sekarang kita akan menambahkan **Router ID** pada setiap Router. Untuk langkah konfigurasi nya sama seperti pada *Single Area*.

```
[admin@RT-1] > routing ospf instance set default router-id=13.5.5.5
[admin@RT-1] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.5.5.5 distribute-default=never redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
      metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

```
[admin@RT-2] > routing ospf instance set default router-id=13.6.6.6
[admin@RT-2] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.6.6.6 distribute-default=never redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
      metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

```
[admin@RT-3] > routing ospf instance set default router-id=13.7.7.7
[admin@RT-3] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.7.7.7 distribute-default=never redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
      metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

Konfigurasi Router ID diatas telah selesai. Sekarang, kita akan melakukan konfigurasi *Regular Area* pada Router 2 dan Router 3. Pada Router 1 tidak perlu dilakukan konfigurasi Regular Area karena Router 1 berada pada Area *Backbone*.

Kita akan lakukan konfigurasi Regular Area pada Router 2 dan 3 dengan *area-id=1.1.1.1*. Perintah text nya adalah sebagai berikut

```
[admin@RT-2] > routing ospf area add name=reguler area-id=1.1.1.1
[admin@RT-2] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                    AREA-ID       TYPE    DEFAULT-COST
 0  * backbone                                  0.0.0.0       default
 1    reguler                                   1.1.1.1       default
```

```
[admin@RT-3] > routing ospf area add name=reguler area-id=1.1.1.1
[admin@RT-3] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                    AREA-ID       TYPE    DEFAULT-COST
 0  * backbone                                  0.0.0.0       default
 1    reguler                                   1.1.1.1       default
```

Konfigurasi *Regular Area* diatas telah selesai. Sekarang barulah kita lakukan konfigurasi *Advertise Network*

Konfigurasi Advertise Network pada Multi Area hampir sama pada Single Area. Dalam melakukan konfigurasi Advertise Network kita harus memperhatikan parameter *area* pada setiap Network nya. Kita langsung saja menuju langkah konfigurasi

Pada Router 1, kedua Network berada pada Area Backbone. Jadi, pada parameter area kedua Network kita isi dengan perintah text *area=backbone*

```
[admin@RT-1] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@RT-1] > routing ospf network add network=14.14.14.0/24 area=backbone
[admin@RT-1] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK          AREA
 0   13.13.13.0/30    backbone
 1   14.14.14.0/24    backbone
```

Pada Router 2 sedikit berbeda. Network *ether1* (13.13.13.0/24) pada Router 2 masuk kedalam Area *Backbone.* Sedangkan Network *ether2* (13.13.13.4/30) pada Router 2 masuk kedalam Area *Regular*. Maka perintah text nya adalah sebagai berikut

```
[admin@RT-2] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@RT-2] > routing ospf network add network=13.13.13.4/30 area=reguler
[admin@RT-2] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK          AREA
 0   13.13.13.0/30    backbone
 1   13.13.13.4/30    reguler
```

Pada Router 3, kedua Network masuk kedalam Area *Regular*. Perintah text nya adalah sebagai berikut

```
[admin@RT-3] > routing ospf network add network=13.13.13.4/30 area=reguler
[admin@RT-3] > routing ospf network add network=12.12.12.0/24 area=reguler
[admin@RT-3] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK          AREA
 0   13.13.13.4/30    reguler
 1   12.12.12.0/24    reguler
```

Konfigurasi Advertise Network telah selesai. Sekarang, seharusnya jaringan kita telah mencapai kondisi *convergence.*

Konfigurasi OSPF Multi Area diatas telah selesai. Sekarang, kita lakukan pengecekan pada Routing Table dan juga OSPF Route.

```
[admin@RT-1] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADo  12.12.12.0/24                    13.13.13.2          110
 1 ADC  13.13.13.0/30     13.13.13.1     ether1              0
 2 ADo  13.13.13.4/30                    13.13.13.2          110
 3 ADC  14.14.14.0/24     14.14.14.1     ether2              0
```

```
[admin@RT-2] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADo  12.12.12.0/24                    13.13.13.6          110
 1 ADC  13.13.13.0/30     13.13.13.2     ether1              0
 2 ADC  13.13.13.4/30     13.13.13.5     ether2              0
 3 ADo  14.14.14.0/24                    13.13.13.1          110
```

```
[admin@RT-3] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADC  12.12.12.0/24     12.12.12.1     ether2              0
 1 ADo  13.13.13.0/30                    13.13.13.5          110
 2 ADC  13.13.13.4/30     13.13.13.6     ether1              0
 3 ADo  14.14.14.0/24                    13.13.13.5          110
```

Bisa kita lihat pada gambar Routing Table diatas, ketiga router mendapatkan entry routing dynamic dari OSPF .

```
[admin@RT-1] > routing ospf route print
 # DST-ADDRESS       STATE        COST          GATEWAY        INTERFACE
 0 12.12.12.0/24     inter-area   30            13.13.13.2     ether1
 1 13.13.13.0/30     intra-area   10            0.0.0.0        ether1
 2 13.13.13.4/30     inter-area   20            13.13.13.2     ether1
 3 14.14.14.0/24     intra-area   10            0.0.0.0        ether2
```

```
[admin@RT-2] > routing ospf route print
 # DST-ADDRESS       STATE       COST          GATEWAY       INTERFACE
 0 12.12.12.0/24     intra-area  20            13.13.13.6    ether2
 1 13.13.13.0/30     intra-area  10            0.0.0.0       ether1
 2 13.13.13.4/30     intra-area  10            0.0.0.0       ether2
 3 14.14.14.0/24     intra-area  20            13.13.13.1    ether1
```

```
[admin@RT-3] > routing ospf route print
 # DST-ADDRESS       STATE       COST          GATEWAY       INTERFACE
 0 12.12.12.0/24     intra-area  10            0.0.0.0       ether2
 1 13.13.13.0/30     inter-area  20            13.13.13.5    ether1
 2 13.13.13.4/30     intra-area  10            0.0.0.0       ether1
 3 14.14.14.0/24     inter-area  30            13.13.13.5    ether1
```

Biografi Penulis

Nama lengkap Mohammad Andri Widiyanto, Lebih akrab dengan panggilan Andri. Lulusan dari SMK SORE Tulungagung jurusan TKJ dan saat ini sedang melanjutkan program studi S1 di kampus Areta Informatics Tangerang. Kemudian penulis juga aktif sebagai pengajar IT Networking di INTRA Training Bekasi sekaligus menjabat sebagai COO.

Facebook : www.facebook.com/andri.widiyanto17

Email : andri.widiyanto17@gmail.com

Linkedin : https://www.linkedin.com/in/andri-widiyanto/