Module Praktikum Jaringan Komputer

tim penyusun
Andry Maulana, M.Kom
Ahmad Fauzi, M.Kom

KATA SAMBUTAN

Alhamdulillah segala puji bagi allah tuhan seru sekalian alam. Dengan rahmat dan hidayahnya yang selalu terus mengalir dalam kehidupan. Sholawat dan salam atas nabi besar muhammad saw yang telah memberi petunjuk dari kesesatan menuju jalan yang terang benderang. Kami penulis bersyukur karena dapat menyelesaikan buku pembelajaran (modul) dengan judul praktikum jaringan komputer. Semoga dengan buku ini dapat menjadi bahan referensi pembelajaran bagi mahasiswa/i universitas nusa mandiri. Segala bentuk kesalahan dapat disampaikan dalam bentuk kritik dan saran.

Jakara , 08 oktober 2018

Tim penyusun

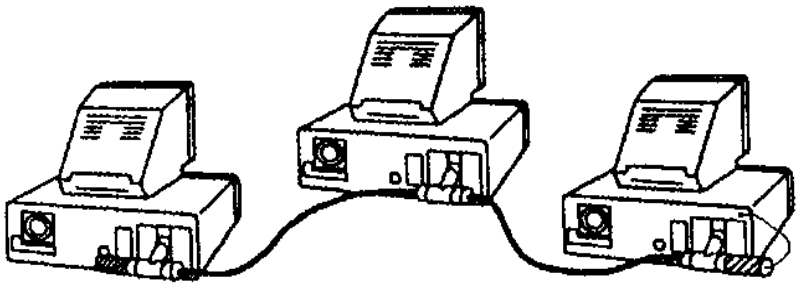
DAFTAR ISI

PENGANTAR
PRAKTIKUM JARINGAN KOMPUTER

A. Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang dihubungkan satu dengan yang lainnya melalui media transmisi atau media komunikasi sehingga dapat saling berbagi data-informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan lain sebagainya.

Awalnya networking atau jaringan komputer adalah sambungan komputer ke komputer dalam bentuk topologi bus



Sambungan jaringan komputer di PC ditemukan oleh Dr. Robert M. Metcalfe pada tahun 1976, diberi nama Ethernet

Suatu Jaringan tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu

1. Komponen Hardware

   Personal Computer (PC), Network Interface Card (NIC), Kabel, Topologi jaringan.

2. Komponen Software

   Sistem Operasi Jaringan, Network Adapter Driver, Protokol Jaringan.

Agar suatu komputer dapat berkomunikasi dengan komputer lain, kedua komputer tersebut membutuhkan kesepakatan tentang tata cara berkomunikasi. Tata cara atau aturan komunikasi ini yang disebut dengan protokol.

Protokol mendefinisikan apa yang dikomunikasikan bagaimana dan kapan terjadinya komunikasi

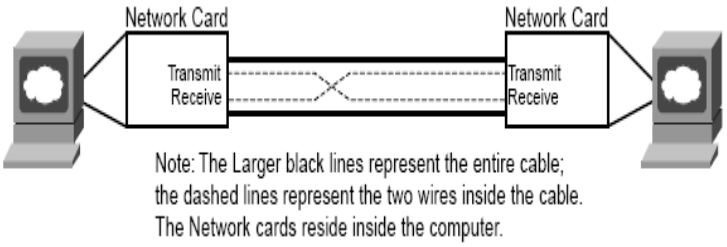
Ditentukan berdasarkan jarak jangkauan, dan kebutuhan peralatan yang digunakan seperti Repeater, Bridge, Router, atau Gateway.

1. Jaringan komputer Local (LAN)
2. Jaringan komputer Metropolitan (MAN)
3. Jaringan komputer skala luas (WAN)

Terdapat dua tipe utama dalam jaringan yaitu :

1. Peer to peer (workgroup)

   Pada jaringan tipe ini semua komputer berkedudukan sama, dapat bertindak sebagai sebuah PC client (*information requestor*) maupun PC server (information provider).



2. Client Server (Domain)

   Pada jaringan tipe ini terdapat sebuah PC server yang berfungsi untuk mengatur, dan membagikan informasi kesetiap PC client yang terhubung dengannya

   Server (pelayan) menyediakan sarana untuk client (pemakai jasa) untuk mengambil data, sharing perangkat keras dan mengkonfigurasi security pada suatu jaringan.

B. Topologi

Topologi adalah susunan geometri beberapa komputer terminal (node) dan sistem kabelnya pada suatu jaringan komputer. Penentuan topologi jaringan akan berpengaruh pada:

1. Tipe peralatan (equipment) jaringan yang dibutuhkan,
2. Kemampuan peralatan (equipment),
3. Pertumbuhan Jaringan,
4. Penanganan manajemen jaringan

Bentuk topologi dapat dilihat secara fisik yaitu dengan melihat bentuk pengkabelan yang digunakan maupun secara logika yaitu dengan melihat bagaimana aliran data melalui topologi jaringan tersebut

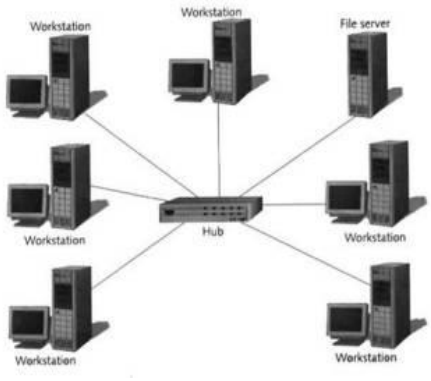
1. Bus (Linear Bus)

   Pada topologi Bus, setiap komputer dihubungkan dengan sebuah kabel tunggal yang disebut trunk, backbone, atau segment. media koneksi yang digunakan adalah kabel CoAX (RG58) atau 10Base-2

   Untuk mengefisiensikan penggunaan jaringan, digunakan metode CSMA/CD (Carrier Sense Multiple Access / Collision Detected) yang dapat mengurangi terjadinya masa tenggang (saluran kosong) dengan mendeteksi tabrakan informasi.

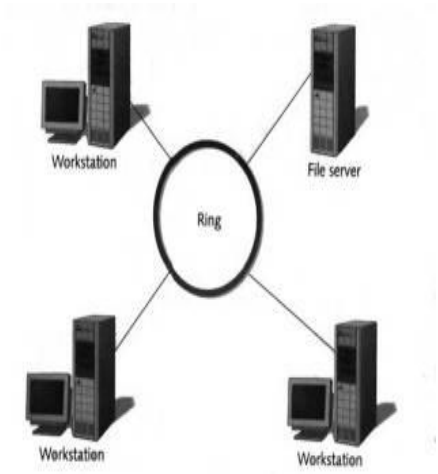
2. **Topologi Star**

   Pada topologi Star, setiap komputer dikonsentrasikan pada sebuah komponen yang disebut HUB/Multipoint Repeater/Concentrator sehingga membentuk seperti Bintang. Media koneksi yang digunakan adalah kabel UTP atau 10/100/1000Base-T



3. Topologi Ring

   Pada topologi Ring, setiap komputer dihubungkan dengan sebuah kabel tunggal sehingga membentuk lingkaran tanpa memiliki ujung kabel. Topologi ini mirip seperti topologi BUS dan setiap komputer akan mempengaruhi sinyal data. media koneksi yang digunakan adalah kabel UTP cat 3 atau TokenRing



C. IP Address

IP address merupakan alamat dari sebuah komputer yang dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian panjangan terdiri dari 8 buah bit. IP address merupakan sebuah indetitas dari host pada jaringan computer. IP address yang digunakan untuk keperluan LAN/intrenet disebut sebagai IP address local. Sedangkan IP address yang digunakan untuk keperluan internet disebut IP address public. Ruang lingkup dari pengalamatan IPv4 mencangkup semua kemungkinan. Kombinasi angka untuk 32 bit alamat IPv4. Secara harfiah 232 nilai yang berbeda ada dengan nomor 32 bit. Kombinasi angka-angka dapat dimulai dari “0 - 255” dalam empat octad: 0.0.0.0, 0.0.0.1, 0.0.0.2 sampai ke 255.255.255.255. Contoh penulisan dari IP address sebagai berikut:

10000000.00001010.00001010.00000001

Apabila setiap bagian kita konversikan ke bilangan decimal maka IP address diatas menjadi: 192.10.10.1

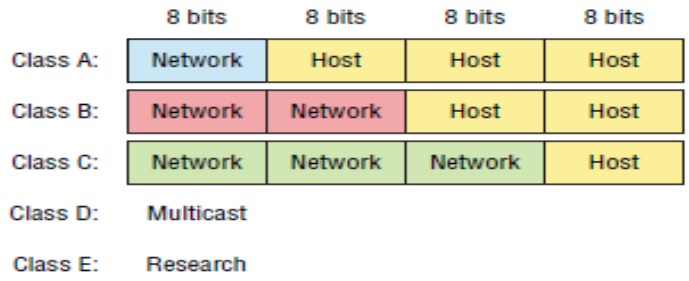
Pada bentuk penulisan IP address diatas dikenal dengan istilah notasi “doted decimal”. Dalam praktiknya, IP address dalam bentuk decimal inilah yang akan kita gunakan dalam konfigurasi jaringan computer. Saat ini alokasi ataupun penyedian dari IP address versi 4 (IPv4) semakin berkurang dikarenakan semakin banyaknya pengguna IP versi 4 itu. IPv4 sudah digunakan lebih dari 20 Tahun lamanya. Untuk mengatasinya kini sudah dikembangkan penggunakan IPv6 atau IPng (IP next generation). Salah satuPraktikum Jaringan Komputer [Networking] Page 9 keuntungan dari IPv6 adalah jumlahnya yang sangat besar. Sehingga dapat mengantisipasi lonjakan permintaan dari IPv4 tersebut. IPv4 menggunakan 32 bit sedangkan IPv6 menggunakan 128 bit, sehingga kurang lebih dapat menanpung 4 Milyar computer yang terhubung ke internet. Namun, semakin tingginya penggunakan dari perangkat genggam,

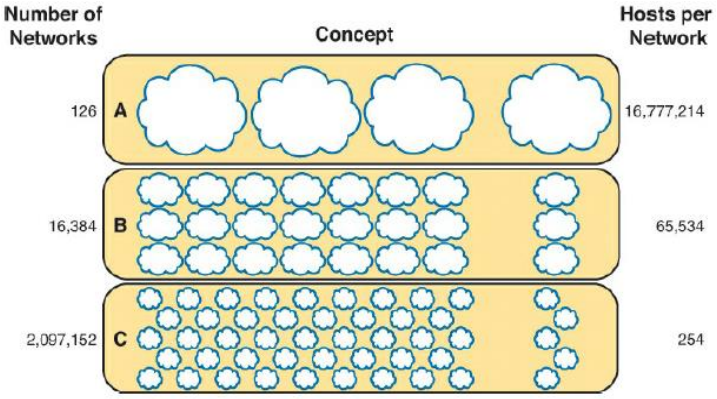
seperti PDA, smartphone, blackberry maka sitadaknya paling sedikit terdapat 1600 address tiap RT, Secara umum IP address dibagi menjadi 5 buah kelas. Kelas A, B, C, D, dan E. Namun, pada praktiknya hanya menggunakan kelas A, B dan C saja untuk keperluan umum. Sedangkan IP address kelas D dan E dipergunakan untuk keperluan khusus ataupun penelitian. IP address (kelas A, B, dan C) dapat dipisahkan menjadi 2 bagian, yakni bagian network (bit-bit networks/networks bit) dan bagian host (bit-bit host/host bits). Network bit berperan sebagai pembeda antar-network atau identifikasi (ID) network. Sedangkan host bit berperan sebagai identifikasi host. Semua host yang terhubung pada network yang sama, pasti akan memiliki network bit yang sama juga.

KELAS	IP Address
A	1.0.0.0 – 126.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255

KELAS	IP Address
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Pada jaringan TCP/IP, perbedaan network tidak ditentukan pada topologi yang digunakan, media yang digunakan, akses, system operasi dan aplikasi yang digunakan. Berikut ini penjelasan dari masing-masing kelas IP address.





1. Kelas A

   IP address kelas A dapat ditulisankan sebagai berikut:

   nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

   “n” menerangkan sebagai network, sedangkan “h” menerangkan sebagai host. Sebagai contoh:

   IP: 10.11.12.1

   Subnet: 255.0.0.0

   Ket:

   10 > Sebagai Network.

   11, 12, dan 1 > merupakan host yang dapat digunakan pada kelas A.

2. Kelas B

   IP address kelas B dapat ditulisankan sebagai berikut:

   nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

   Sebagai contoh:

   IP: 172.168.10.1

   Subnet: 255.255.0.0

   Ket:

   172.168 > Sebagai Network

   10.1> merupakan host yang dapat digunakan pada kelas B

3. Kelas C

   IP address kelas C dapat ditulisankan sebagai berikut:

   nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

   Sebagai contoh:

   IP: 192.168.10.1

   Subnet: 255.255.255.0

   Ket:

   192.168.10 > Sebagai Network

   1 > merupakan host yang dapat digunakan pada kelas C.

   Selain IP address, terdapat pula netmask yang merupakan jenis IP address khusus. Setiap kelas-kelas IP memiliki nilai netmask yang berbeda. IP kelas A dengan netmask 255.0.0.0 sedangkan kelas B 255.255.0.0 dan kelas C 255.255.255.0.

KELAS	Netmask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Penggunakan netmask dapat menentukan besarnya jumlah client yang dapat mengakses ke dalam sebuah jaringan computer. Contoh penggunaan netmask pada kelas B adalah 172.168.10.1 dengan netmask 255.255.0.0. IP address ini jika kita konversikan ke bilangan biner maka hasil yang didapat adalah:

255.255.0.0

11111111.11111111.00000000.00000000

Ket:

1 > Network (N)

0> Host (H)

Maka untuk melakukan perhitungan jumlah client yang dapat terkoneksi kedalam sebuah jaringan computer kita dapat menggunakan rumus:

Network= 2n

Host= 2h-2

Maka dapat kita hitung jumlah host yang dapat terkoneksi adalah:

H= (216)-2 = 65524

Dapatkan anda membayangkan, sebuah kabel jaringan atau sebuah topologi jaringan yang dapat menampung sampai 65524 client??. Untuk mengatasi masalah tersebut, kita dapat memecahnya menjadi sebuah network yang lebih kecil. Network yang lebih kecil ini disebut dengan subnetwork.

Contoh IP Subneting:

1. IP Address: 192.168.0.0/24
   a. Netmask : 255.255.255.0
   b. Prefix : /24
   c. IP Network : 192.168.0.0
   d. First Host IP : 192.168.0.1
   e. Last Host IP : 192.168.0.254
   f. Broadcast : 192.168.0.255

Jadi dengan menggunakan “/24” jumlah host yang dapat terkoneksi sebanyak 254 client.

2. IP Address: 192.168.0.0/25
   a. Netmask : 255.255.255.128
   b. Prefix : /25
   c. IP Network : 192.168.0.0
   d. First Host IP : 192.168.0.1
   e. Last Host IP : 192.168.0.126
   f. Broadcast : 192.168.0.127

Jadi dengan menggunakan “/24” jumlah host yang dapat terkoneksi sebanyak 127 client.

D. Subneting

Subnetting adalah metode atau 14amper membuat net Id dengan cara mengorbankan bit host. Karena Ipv4 pengalamatan sangat terbatas dengan makin banyaknya user jaringan maka dibuat metode 14amper14r1414.

Kegunaan Subnetting

1. Untuk menentukan batas network ID dalam suatu subnet
2. Memperbanyak jumlah network (LAN)
3. Mengurangi jumlah host dalam satu network

Tujuan lain dari subnetteing yang tidak kalah penting adalah untuk mengurangi tingkat konggesti (gangguan/tabrakan) lalulintas data dalam suatu network

1. Efisiensi pengguanan IP Address
2. Pendelegasian kekuasan untuk pengaturan
3. Mempermudah manajemen jaringan
4. Mengatasi masalah perbedaan hardware dan topologi fisik jaringan

Menghitung Subbnetting

Rumus untuk menghitung jumlah subnet adalah : 2n – 2, “N” adalah jumlah bit yang diselubungi/dikorbankan

Rumus untuk menghitung jumlah host per subnet : 2N–2, “N” adalah jumlah bit yang masih tersisa untuk host ID

Contoh subnet kelas A:

IP = 10.0.0.0/25

Subnet = 25 bit

= 11111111.11111111.11111111.10000000

= 255.255.255.128

Jumlah net id baru = 2n – 2

= 217 – 2

= 131070

*n = 17 = 111111111.11111111.11111111.10000000

Jumlah host per subnet = 2N – 2

= 27 – 2

= 126

*N = 7 = 1111111.11111111.11111111.10000000

Variable Length Subnet Mask (VLSM)

Jika pada pengalokasian IP Address classfull, suatu network ID hanya memiliki satu subnetmask, maka VLSM menggunakan metode yang berbeda, yakni dengan memberikan lebih dari satu subnet.

Contoh:

Satu blok IP address (169.254.0.0/20) dibagi menjadi 16

1. Subnet 1 = 4094 host – Net Address = 169.254.0.0/20
2. Subnet 1 = 4094 host – Net Address = 169.254.16.0/20
3. Subnet 1 = 4094 host – Net Address = 169.254.32.0/20

4. Subnet 1 = 4094 host – Net Address = 169.254.64.0/20
5. Subnet 1 = 4094 host – Net Address = 169.254.240.0/20
6. Subnet Mask = 255.255.240.0

Berikutnya Subnet 2 akan dipecah menjadi 16 subnet lagi yang lebih kecil

1. Subnet 2.1 =254 host – Net Address = 169.254.16.0/24
2. Subnet 2.2 =254 host – Net Address = 169.254.17.0/24
3. Subnet 2.3 =254 host – Net Address = 169.254.18.0/24
4. .....
5. Subnet 2.16 =254 host – Net Address = 169.254.31.0/24
6. Subnet Mask = 255.255.255.0

Bila subnet 2.1 akan dipecah lagi menjadi beberapa subnet, misalnya 4 subnet, maka:

1. Subnet 2.1.1 = 62 host –Net Address = 169.254.16.0/26
2. Subnet 2.1.2 = 62 host –Net Address = 169.254.16.64/26
3. Subnet 2.1.3 = 62 host –Net Address = 169.254.16.128/26
4. Subnet 2.1.4 = 62 host –Net Address = 169.254.16.192/26
5. Subnet Mask = 255.255.255.192

Kesimpulan dari contoh:

Terlihat 16ampe pada Subnet 2 (Net Address 169.254.16.0) dapat memecah jaringannya menjadi beberapa subnet lagi dengan mengganti Subnetmask-nya menjadi:

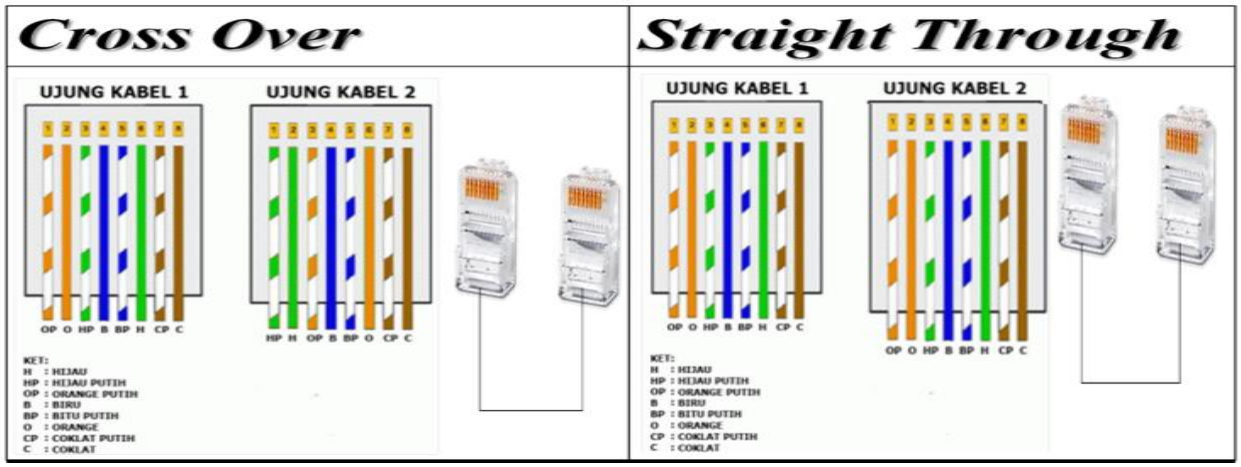
255.255.240.0, 255.255.255.0 dan 255.255.255.192

Jika anda perhatikan, CIDR dan metode VLSM mirip satu sama lain, yaiut blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil.

Perbedaanny adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya local dan tidak dikenal di internet).

E. Pengkabelan

1. Straight trough >> untuk menghubungkan antar device yang berbeda
2. Cross Over >> untuk menghubungkan device yang sama



PRAKTIKUM

- Pembuatan Kabel Straight
- Pembuatan Kabel Cross Over

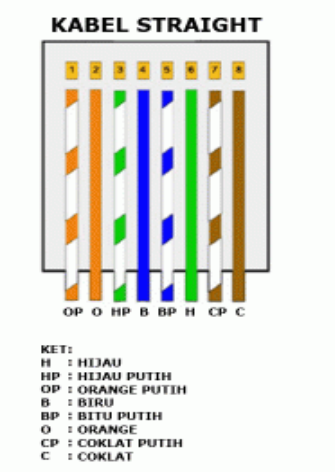
➢ **PROSEDUR PRAKTIKUM**

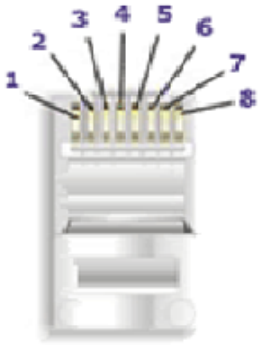
1. Siapkan Tools yang harus di gunakan pada saat pembuatan kabel

- RJ-45
- CRIMPING TOOLS
- KABEL UTP
- LAN TESTER

Merakit Kabel Straight :

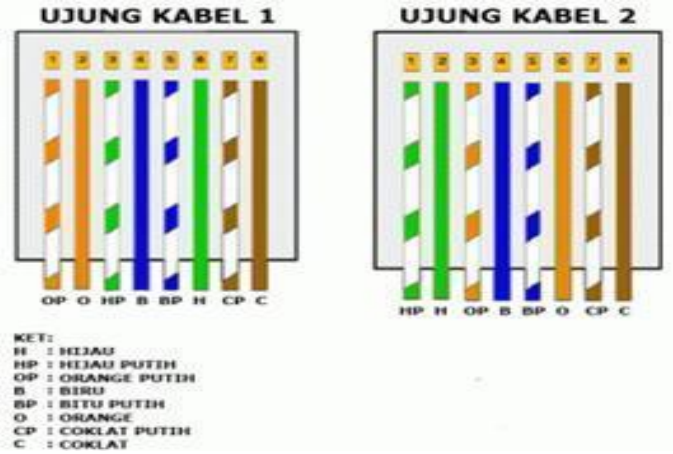
1. Pertama-tama buka bagian ujung kabel UTP sepanjang +/- 2 cm.
2. Luruskan, pisahkan sesuai warna, rapikan ujung kabelnya, hingga rata satu sama lain.
3. Urutan warna untuk UTP Straight, Orange Putih, Orange, Hijau Putih, Biru, Biru Putih, Hijau, Coklat Putih, dan Coklat.
4. Masukkan sampai masuk kabel-kabel kecil ke RJ-45 sesuai dengan urutan warna.
5. Sesudah itu masukkan konektor ke mulut tang crimping, tekan tang sampai terdengar bunyi "klik".





Merakit Kabel Cross Over

1. Pada dasarnya pembuatannya sama saja dengan UTP Straight hanya susunan kabel kecilnya saja yang berbeda.
2. Untuk kabel di ujung pertama susunan kabelnya sama dengan yang tadi, untuk yang ke dua urutan warnanya adalah Hijau Putih, Hijau, Orange Putih, Biru, Biru Putih, Orange, Coklat Putih, Coklat.



Setelah selesai membuat kabelnya sekarang waktunya kita tes menggunakan LAN Tester.

Masukkan ujung kabel/konektor rj-45 ke masing-masing port LAN Tester yang tersedia.

Anda harus memastikan semua lampu 19amper19r19 menyala dari angka 1 sampai 8.

Jika semua lampu menyala berarti anda berhasil membuat kabel UTP Straight dan Cross.

Sekian semoga bermanfaat.

BAB 1
INTRODUCTION OF MIKROTIK ROUTER

1.1. About Mikrotik

Mikrotik merupakan salah satu produsen network terbesar didunia yang menghasilkan produk-produk pada bidang networking bertempatkan di Riga Latvia menjadikan teknologi internet yang lebih murah , cepat, handal dan terjangkau luas. Untuk itu produsen mikrotik hadir ditengah-tengah kebutuhan akan sebuah perangkat network yang semakin tinggi dan tidak ada sebuah perusahan yang tidak menggunakan perangkat jaringan didalamnya oleh karena itu hadirnya mikrotik dapat memberikan angin segar untuk para infrasturktur Network dalam membangun sebuah infrastruktur jaringan baik secara local maupun global.

Didirikan oleh John Trully & Arnis Reikstins pada tahun 1996 dan motto “Routing The Word” makan dapat menjawab sebuah tantangan yang ada didunia ini dan menjadikan Mikrotik sebagai perangkat terpercaya oleh sebagian besar perusahan, baik perusahaan jasa Internet service profider maupun perusahaan non Internet.

1.1.1. Jenis – Jenis Mikrotik

Pada umumnya mikrotik terbagi atas 2 jenis yaitu:

1. MikroTik RouterOS

   Merupakan 20amper operasi yang diperuntukkan sebagai network router. MikroTik routerOS sendiri adalah 20amper operasi dan perangkat lunak yang dapat digunakan untuk menjadikan 20amper20r biasa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless. Fitur-fitur tersebut diantaranya: Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur lainnya. MikroTik routerOS merupakan

21amper operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard 21amper21r PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan sumber daya PC yang memadai dan mendukung:

a. arsitektur yang kompatibel dengan i386
b. SMP – multi-core dan multi-CPU yang kompatibel
c. Minimum 32MB RAM (maksimum didukung 2GB, kecuali pada perangkat Cloud Core dan instalasi CHR, di mana tidak ada maksimum)
d. IDE, SATA, USB dan media penyimpanan flash dengan ruang minimum 64MB
e. Kartu jaringan yang didukung oleh kernel linux v3.3.5 (PCI, PCI-X)
f. Kompatibilitas terhadap perangkat keras pada PC

2. MikroTik RouterBOARD

RouterBOARD merupakan sebuah perangkat keras produksi Mikrotik yang sudah terdapat MikroTik RouterOS didalamnya sehingga sudah dapat digunakan beserta Lisens yang sudah terdaftar, pada RouterBOARD tersedia dari harga yang minim hingga RouterBOARD dengan harga yang tinggi.

Gambar 1.1 Router BOARD

1.1.2. Fitur Mikrotik

Karena keahliannya sebagai router maka Router Mikrotik memiliki Fitur yang umumnya dimiliki oleh sebuah router diantaranya:

1. Firewall
    a. Statefull filtering
    b. Source and destination NAT
    c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)
    d. Internal connection, routing and packet marks
    e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more
    f. Address lists
    g. Custom Layer7 matcher
    h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

2. Routing

a. Statefull filtering

b. Source and destination NAT

c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)

d. Internal connection, routing and packet marks

e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more

f. Address lists

g. Custom Layer7 matcher

h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

3. MPLS

a. Statefull filtering

b. Source and destination NAT

c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)

d. Internal connection, routing and packet marks

e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more

f. Address lists

g. Custom Layer7 matcher

h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

4. VPN

a. Statefull filtering

b. Source and destination NAT

c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)

d. Internal connection, routing and packet marks

e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more

f. Address lists

g. Custom Layer7 matcher

h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

5. Wireless

a. Statefull filtering

b. Source and destination NAT

c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)

d. Internal connection, routing and packet marks

e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more

f. Address lists

g. Custom Layer7 matcher

h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

6. DHCP

a. Statefull filtering

b. Source and destination NAT

c. NAT helpers (h323, pptp, quake3, sip, ftp, irc, tftp)

d. Internal connection, routing and packet marks

e. Filtering by IP address and address range, port and port range, IP protocol, DSCP and many more

f. Address lists

g. Custom Layer7 matcher

h. Ipv6 support

i. PCC – per connection classifier, used in load balancing configurations

j. RAW filtering to bypass connection tracking.

7. Hotspot

a. Plug-n-Play access to the Network

b. Authentication of Local Network Client

c. Users Accounting

d. RADIUS Support for Authentication and Accounting

8. QoS
    a. Hierarchical Token Bucket (HTB) QoS system with CIR, MIR, burst and priority support
    b. Simple and fast solution for basic QoS implementation – Simple queues
    c. Dynamic client rate equalization (PCQ)
9. Proxy
    a. HTTP caching proxy server
    b. Transparent HTTP proxy
    c. SOCKS protocol support
    d. DNS static entries
    e. Support for caching on a separate drive
    f. Parent proxy support
    g. Access control list
    h. Caching list
10. Tools
    a. Ping, traceroute
    b. Bandwidth test, ping flood
    c. Packet sniffer, torch
    d. Telnet, ssh
    e. E-mail and SMS send tools
    f. Automated script execution tools
    g. CALEA
    h. File Fetch tool

i. Advanced traffic generator

11. Other features

a. Samba support

b. OpenFlow support

c. Bridging – spanning tree protocol (STP, RSTP), bridge firewall and MAC natting.

d. Dynamic DNS update tool

e. NTP client/server and synchronization with GPS system

f. VRRP v2 and v3 support

g. SNMP

h. M3P – MikroTik Packet packer protocol for wireless links and ethernet

i. MNDP – MikroTik neighbor discovery protocol, supports CDP (Cisco discovery protocol)

j. RADIUS authentication and accounting

k. TFTP server

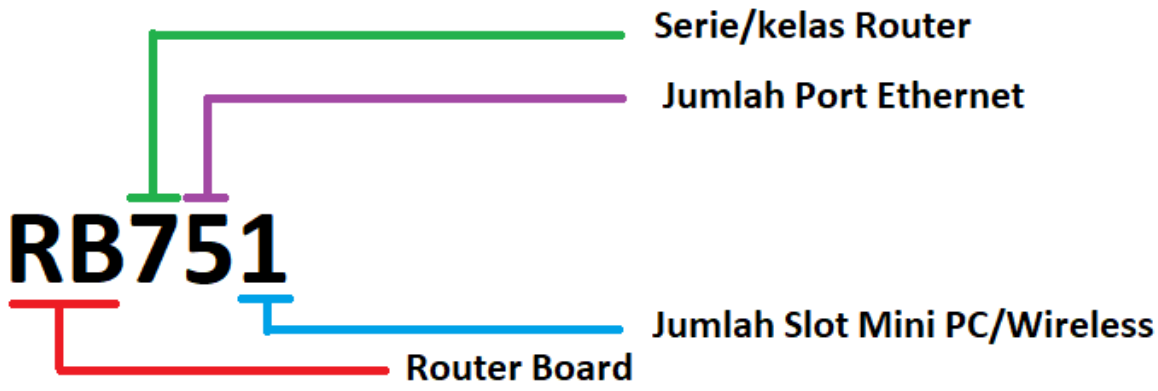
l. Synchronous interface support (Farsync cards only) (Removed in v5.x)

m. Asynchronous – serial PPP dial-in/dial-out, dial on demand

n. ISDN – dial-in/dial-out, 128K bundle support, Cisco HDLC, x75i, x75ui, x75bui line protocols, dial on demand

1.1.3. Tipe Router Board

Pada sebuah RouterBOARD terdapat beberapa series yang didalamnya memiliki arti terentu, bilama kita jabarkan sebuah series routerBOARD maka kita dapatkan spesifikasi perangkat secara umum yang disampaikan melalui Seriesnya.



Gambar 1.2 Series MikrotikBoard

Selain itu juga terdapat kode tambahan pada belakang seris Router diantaranya ada kode sebagai berikut:

U – USB

P – power injection with controller

I – single port power injector without controller

A – more memory and (or) higher license level

H – more powerful CPU

G – Gigabit (may include “U”,”A”,”H”, if not used with “L”)

L – light edition

S – SFP port (legacy usage – SwitchOS devices)

e – PCIe interface extension card

x<N> - where N is number of CPU cores (x2, x16, x36 etc)

R – MiniPCI or MINIPCIe slot

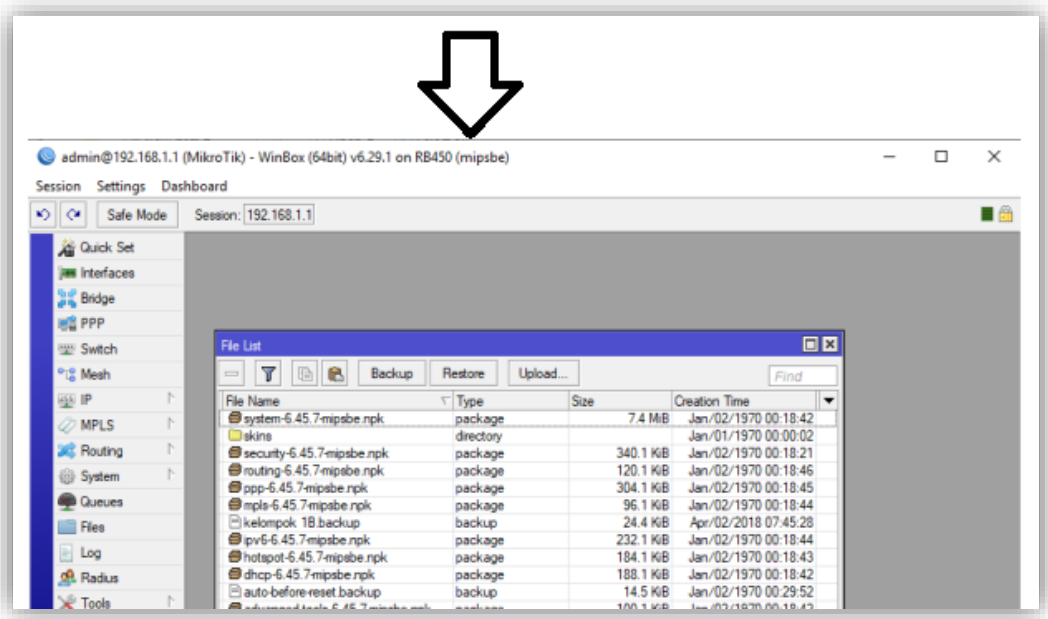
1.1.4. Arsitektur Routerboard

Arsiter RouterBoard dapat dibedakan dari jenis processor yang digunaka pada sebuah series tertentu, arsitek ini dapat menentukan tipe software yang digunakan untuk melakukan Upgrade atau Downgrade pada sebuah perangkat Router, adapun jenis arsitek yang terdapat pada Router Board.

routeros-mipsle (*mipsle*)	combined package for mipsle (RB100, RB500) (includes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing*)
routeros-mipsbe (*mipsbe*)	combined package for mipsbe (RB400) (includes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing*)
routeros-powerpc (*ppc*)	combined package for powerpc (RB300, RB600, RB1000) (includes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing*)
routeros-x86 (*x86*)	combined package for x86 (Intel/AMD PC, RB230) (includes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing*)
mpls-test (*mipsle, mipsbe, ppc, x86*)	Multi Protocol Labels Switching support improvements
routing-test (*mipsle, mipsbe, ppc, x86*)	routing protocols (RIP, OSPF, BGP) improvements

Gambar 1.3 Arsitektur RouterBoard

Dengan melihat jenis arsitektur maka kita dapat menentukan Packeges apa saja yang support dengan perangkat yang digunakan, untuk mengetahui sebuah arsitektur perangkat RouterBoard maka dapat kita lihat ketika sudah berada pada aplikasi winbox.



Gambar 1.4 Mengetahui Jenis Arsitektur RouterBoard

Dapat terlihat jelas arsitertur pada perangkat RouterBoard tersebut pada kasus diatas Arsitektur yang digunakan adalah MIPSBE.

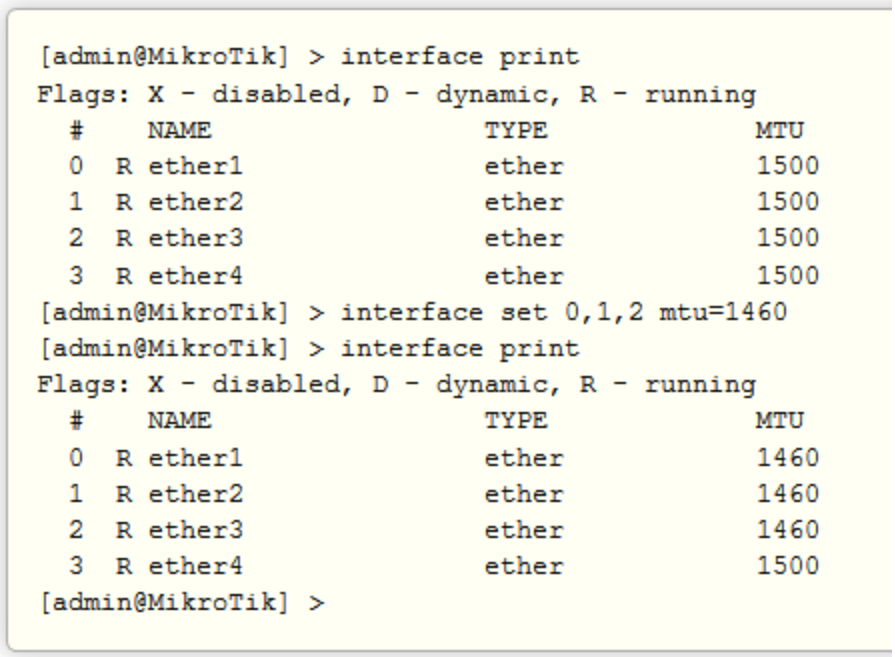
1.2. Accesing the Router

1. Interface Akses Router

Dalam mengakses sebuah Router maka dapat dilakukan dengan berbagai macam cara dan berbagai macam metode, salah satu intruksi yang digunakan dalam mengakses sebuah router terbagi atas 2 cara:

a. Console

Konsol digunakan untuk mengakses konfigurasi MikroTik Router dan fitur manajemen menggunakan terminal teks, baik menggunakan port serial, telnet, SSH atau 30ampe konsol dalam Winbox, atau langsung menggunakan monitor dan keyboard. Konsol juga digunakan untuk menulis skrip. Manual ini menjelaskan prinsip-prinsip operasi konsol umum. Silakan baca Panduan Skrip pada beberapa perintah konsol tingkat lanjut dan cara menulis skrip



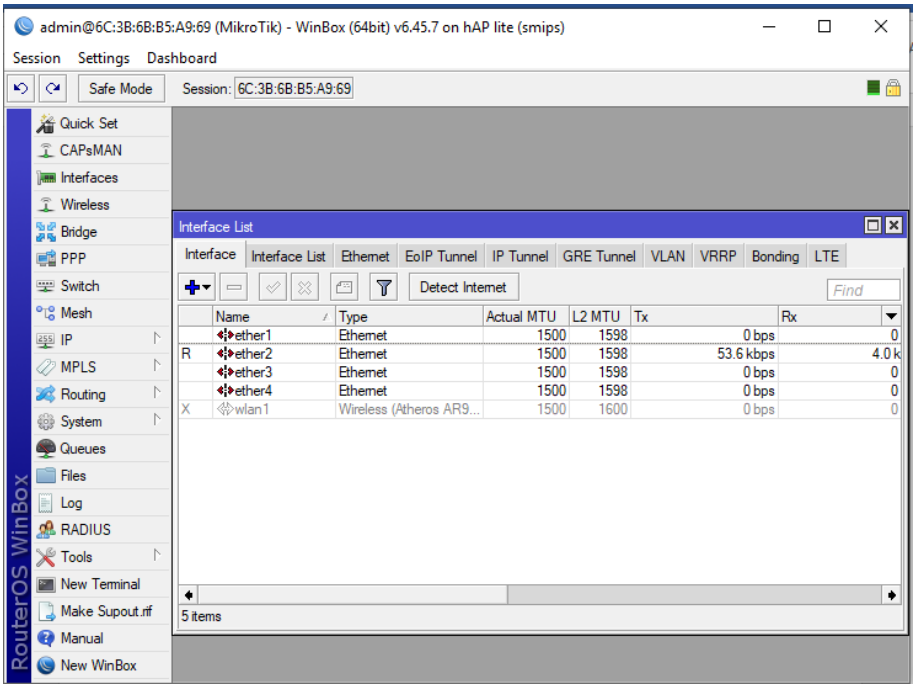
```
[admin@MikroTik] > interface print
Flags: X - disabled, D - dynamic, R - running
  #    NAME                TYPE              MTU
  0  R ether1              ether             1500
  1  R ether2              ether             1500
  2  R ether3              ether             1500
  3  R ether4              ether             1500
[admin@MikroTik] > interface set 0,1,2 mtu=1460
[admin@MikroTik] > interface print
Flags: X - disabled, D - dynamic, R - running
  #    NAME                TYPE              MTU
  0  R ether1              ether             1460
  1  R ether2              ether             1460
  2  R ether3              ether             1460
  3  R ether4              ether             1500
[admin@MikroTik] >
```

Gambar 1.5 Tampilan Console

Jelas pada gambar tersebut adalah sebagai contoh bagaimana kita dapat melihat sebuah Interface atau ethernet yang terdapat pada sebuah Router dengan mengetik perintah ***interface print*** dari informasi yang didapatkan bahwa semua ethernet dalam kodisi sedang berjalan dan tidak ada ether yang mengalami putus koneksi terlihat dengan tanda **"R"** pada sebelah kiri keterangan ether1 sampai 4 , sedangkan pada tanda **"#"** merupakan urutan pengguna ether yang dimulai pada angka **"0".**

b. GUI

Gui merupakan sebuah interface yang dimiliki oleh RouterMikrotik yang memudahkan para pengguna dengan tampila interface yang dapat berintraksi sehingga kalaupun seorang tidak hafal sebuah script console maka dapat menggunaka media GUI ini, untuk media GUI hanya dapat ditemukan pada aplikasi Winbox dan Juga WebFig.



Gambar 1.6 Tampilan GUI

Tampilan GUI dapat sangat membantu administrator dalam management network yang lebih handal karena tidak diperlukan menghafal bahasan consule RouterBoard, dan pada tampilan diatas adalah bagaimana administrator dalam mengecek sebuah interface yang sedang berjalan pada sebuah network yang diansumsikan bahwa ether yang sedang aktif adalah ether 2 ditantai oleh karakter **"R"** dan sama dengan apa yang ditampilkan oleh console.

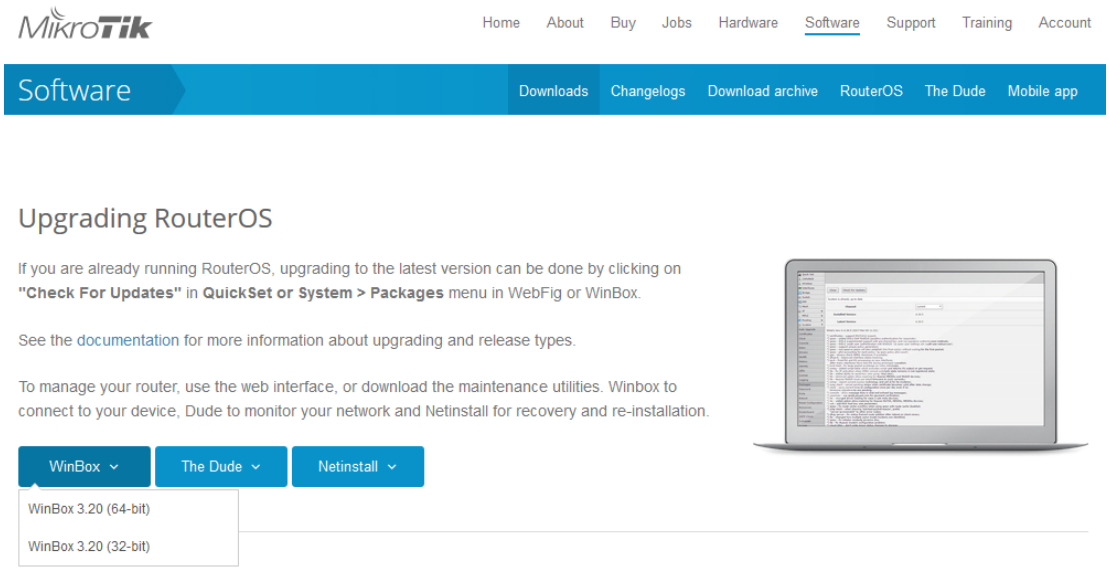
Dengan adanya tampilan Secara Console maupun GUI dapat kita akses sebuah Router Mikrotik, sehingga beberapa cara dalam mengakses atau masuk kedalam system Router Mikrotik, Diantaranya adalah:

2. Software Akses Router Mikrotik

   Diperlukan sebuah software untuk dapat memasuki system pada Router Mikrotik, pada kesempatan kali ini dapat dibahas 3 software yang digunakan untuk dapat memasuki system Router Mikrotik diantaranya adalah:

a. Winbox

Winbox merupakan sebuah software yang dimiki oleh Mikrotik guna sebagai aplikasi berbasis OS Windows dengan series 32 dan 64 bit , adapun cara mendapatkan aplikasi winbox adalah dengan mendownload dihalaman resmi mikrotik.com atau mendapatkan dari rekan anda yang sudah mempunyai aplikasi tersebut, software ini bersifat portable sehingga tidak perlu diinstall.



Gambar 1.7 Download Winbox

Gambar 1.8 Aplikasi Winbox

1) Lab Akses Router Mikrotik dengan Winbox

Untuk Mencoba akses Router Mikrotik dengan aplikasi Winbox maka diperlukan perlengkapan sebagai berikut:

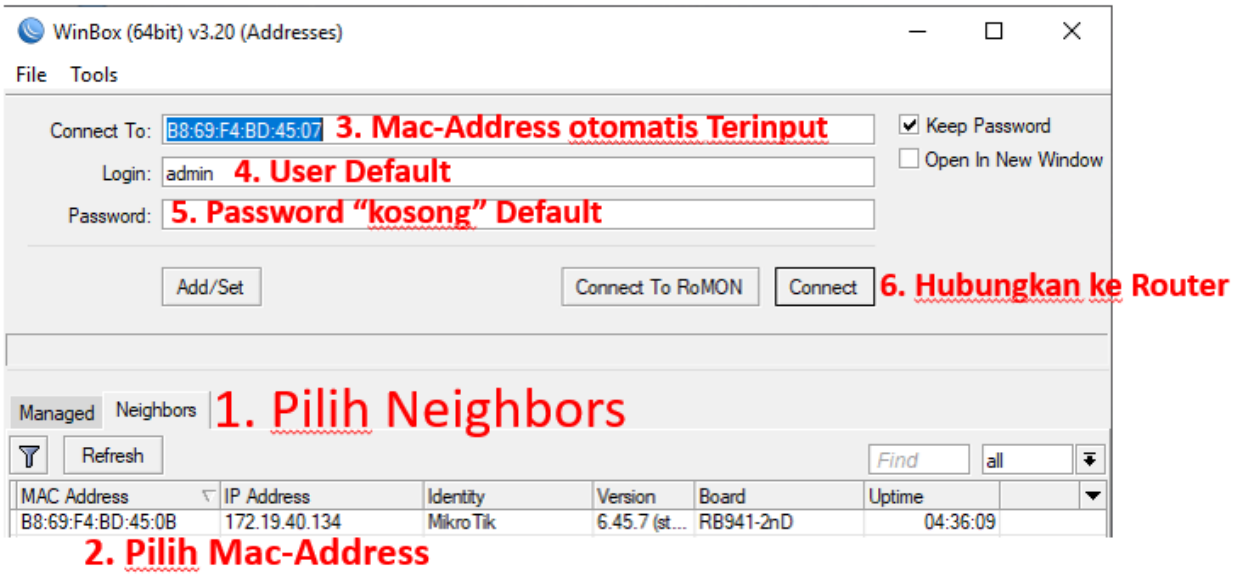
a) Satu buah Router Mikrotik
b) Satu buah Client (PC/Laptop)
c) Kabel LAN (Stright)
d) Aplikasi Winbox yang sudah ada di Client

2) Tugas 1 login/akses dengan menggunakan Mac-Address:

a) Dengan menggunakan kabel LAN maka hubungkan Router Mikrotik selain Ether 1 boleh ether 2,3 atau 4 . karena ether 1 nanti akan digunakan untuk Port akses Internet , dan Ethernet PC

Gambar 1.9 Lab Akses Winbox Via Mac-Address

b) Open Winbox



Gambar 1.10 Login Winbox

c) Pilih Neighbors untuk mendeteksi Router yang terhubung oelh client maka akan muncul secara otomatis Jenis Router yang terkoneksi dengan client, semakin banyak sebuah router terkoneksi makan akan semakin banyak perangkat yang dideteksi oleh Neighbord

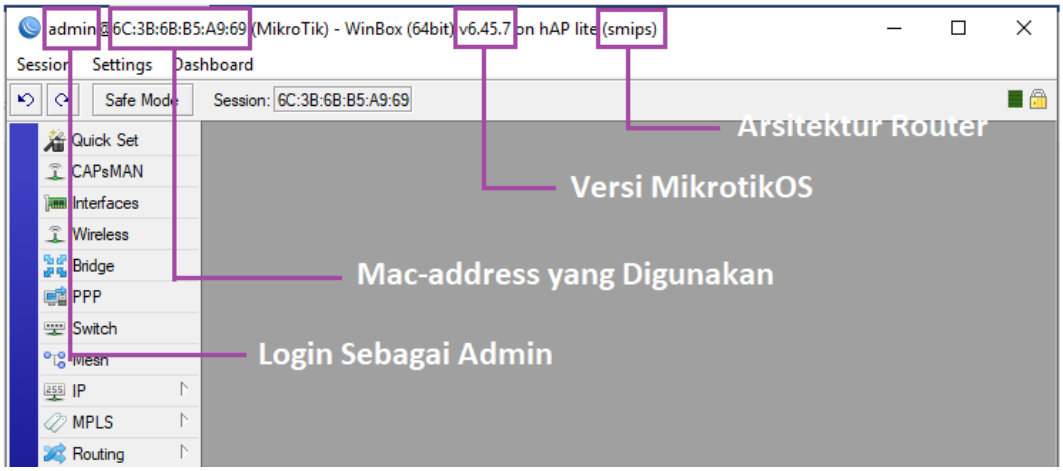
d) Setelah Mucul pada Menu Neighbors akan muncul identitas Mac-Address yang terkoneksi pada clinet, perlu diperhatikan bahwa semua ether memiliki Mac-address secara berurutan tergantung dari ether mana yang terhubung oelh clinet makan Mac-address tersebut yang akan terbaca, maka pilih atau klik Mac-address yang terlist.

e) Setekah dipilih/diklik pada list neighbors Mac-address maka Connet to secara otomatis akan berisikan Mac-Address yang telah terpilih, ingat!!!!! Disini kita login dengan menggunakan Mac-address buka dengan Ip address jadi tidak perlu setting Ip antar perangkat.

f) Untuk login default menggunakan nama : admin yang muncul secara otomatis, bilamana tidak muncul, maka dapat diketik secara manual, perlu diperhatikan bahwa untuk user sensitive Case jadi penulisan huruf besar dan kecil sangat berpengaruh

g) Untuk Password Default di “kosongkan” biarkan saja kosong dan tidak perlu diisi kareakter apapun.

h) Bilamana sudah memenuhi untuk user dan password maka klik tombol Connect seperti yang Digambar.



Gambar 1.11 Tampilan User Interface Winbox

Dari keterangan diatas dapat diamsusikan bahwa client login dengan menggunakan Mac Address.

b. WebFig

Webfig merupakan sebuah service interface yang dapat dilakukan pada Router Mikrotik dengan menggunakan Web Browser atau aplikasi berbasis Web yang perlu diperhatikan untuk dapak membukan interface webfig maka sangat perlu disetting IP Address antara client dan Router, dikarenakan dalam mengakses aplikasi web dengan menggunakan Ip address Gatway client atau Ip router

Untuk Mencoba akses Router Mikrotik dengan aplikasi Winbox maka diperlukan perlengkapan sebagai berikut:

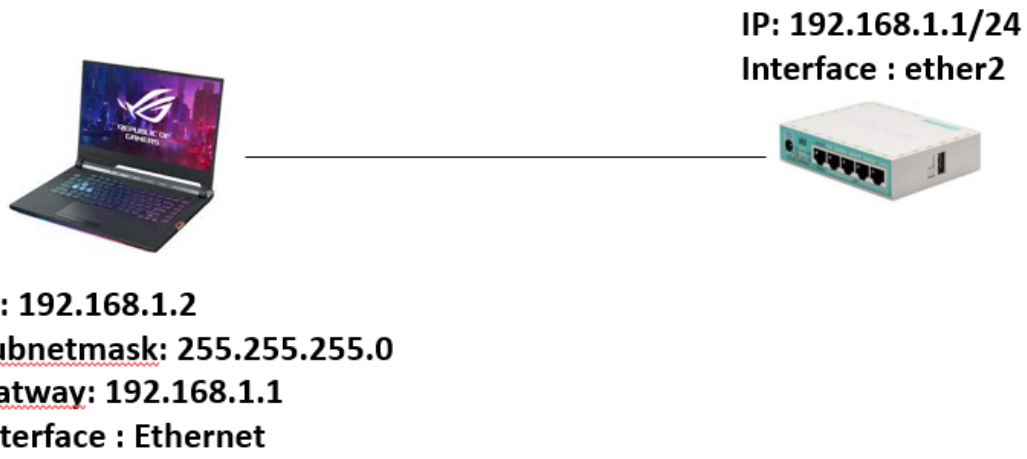
1) Lab Akses Router Mikrotik dengan Webfig

Untuk Mencoba akses Router Mikrotik dengan aplikasi webfig maka diperlukan perlengkapan sebagai berikut:

a) Satu buah Router Mikrotik
b) Satu buah Client (PC/Laptop)
c) Kabel LAN (Stright)
d) Browser Mozilaa, Crome atau Browser apa saja

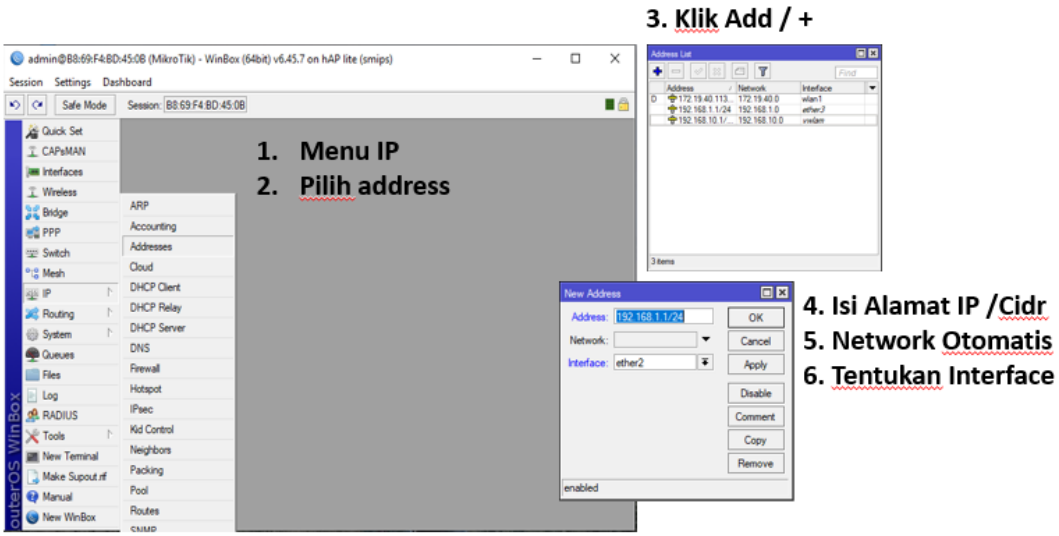
2) Tugas 1 login/akses dengan menggunakan Aplikasi Webfig

a) Dengan menggunakan kabel LAN maka hubungkan Router Mikrotik selain Ether 1 boleh ether 2,3 atau 4 . karena ether 1 nanti akan digunakan untuk Port akses Internet , dan Ethernet PC



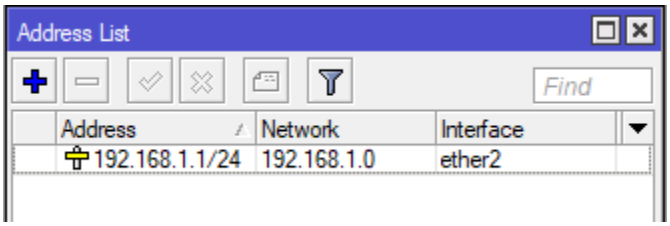
Gambar 1.12 Topologi LAN Akses Webfig

b) Buka Winbox dan Setting IP Address



Gambar 1.12 Setting IP Address

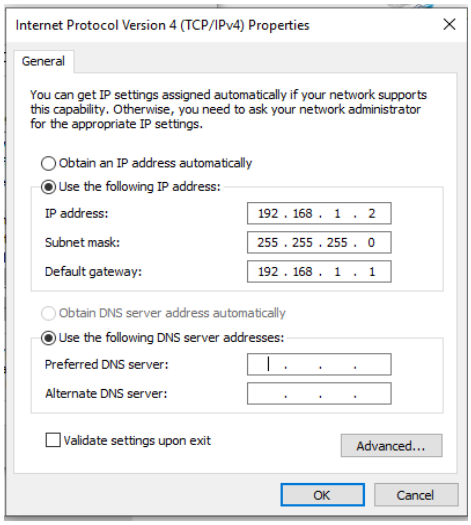
Setelah memuka winbox maka dapat diberikan IP Address pada Ether 2 dengan cara memilih menu IP pada menu GUI => pilih address, maka akan mucul Address list ketika muncul Box Ip List maka klik tanda **"+"** atau add => masukan address 192.168.1.1/24 berikut dengan nilai CIDRnya , untuk network Kosongkan, interface=Ether2, untuk memilih ether , Apply => Ok, Maka Ip address akan masuk pada Address List.



Gambar 1.13 Address List

Dapat terlihat bahwa IP Address yang sudah disetting berada pada ether 2 dan itu sudah sesuai dengan skema sebelumnya.

c) Setting IP Client

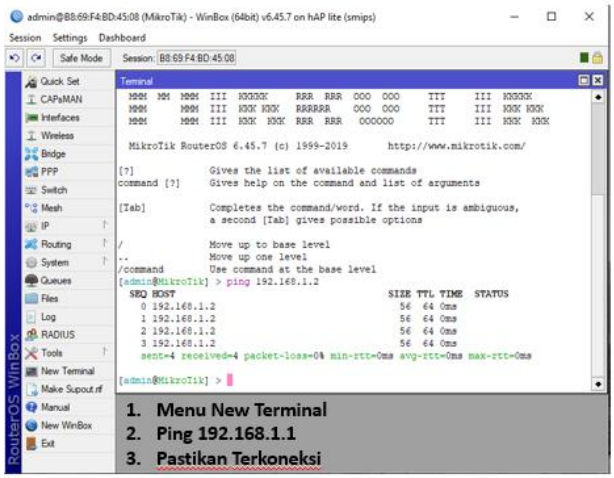


Gambar 1.14 Setting IP Client

Setelah Router sudah dikonfigurasi untuk Ip addressnya maka jangan lupa untuk memasukan Ip address pada client secara manual dengan menggunakan network yang sama yaitu bisa 192.168.1.2 pada computer client.

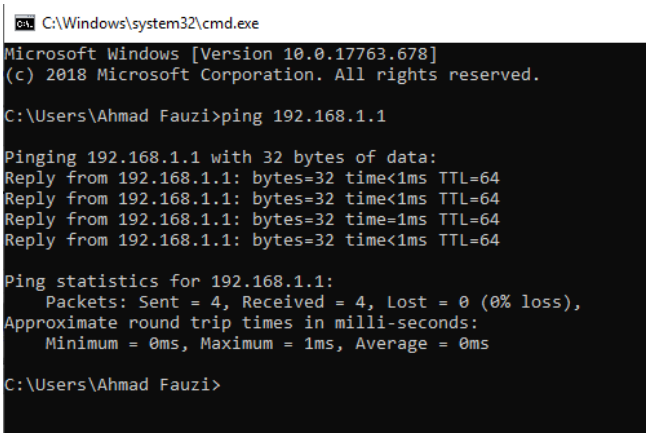
d) Tes Koneksi

Pastikan Tes koneksi adalah awal keberhasilan dari Lab kali ini, dapat dilakukan cek koneksi dari router ke client.



Gambar 1.15 Tes Koneksi Router ke Client

Untuk melakukan tes koneksi pada Router ke client maka bukan kembali Winbox lalu pilih New terminal pada menu winbox maka akan muncul tampilan console winbox, setelah itu gunakan perintah ***ping 192.168.1.2*** untuk mengetest Koneksi antar Router dan client, dan lakukan sebaliknya.

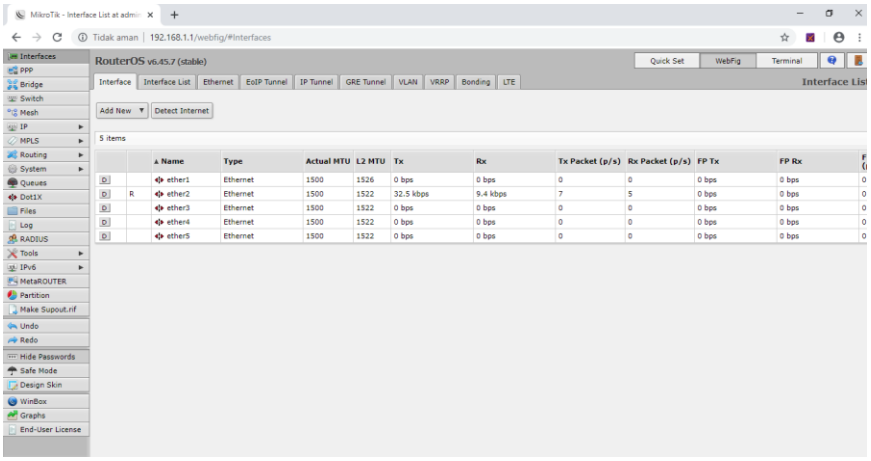


Gambar 1.16 Test Koneksi Client Ke router

Maka diperlukan test untuk Client ke router dengan membuka command Prompt lalu ketikan perintah ***ping 192.168.1.1*** sehingga terjadi Replay dan tidak Request Time Out

e) Buka Browser Untuk menjalankan Web Fig

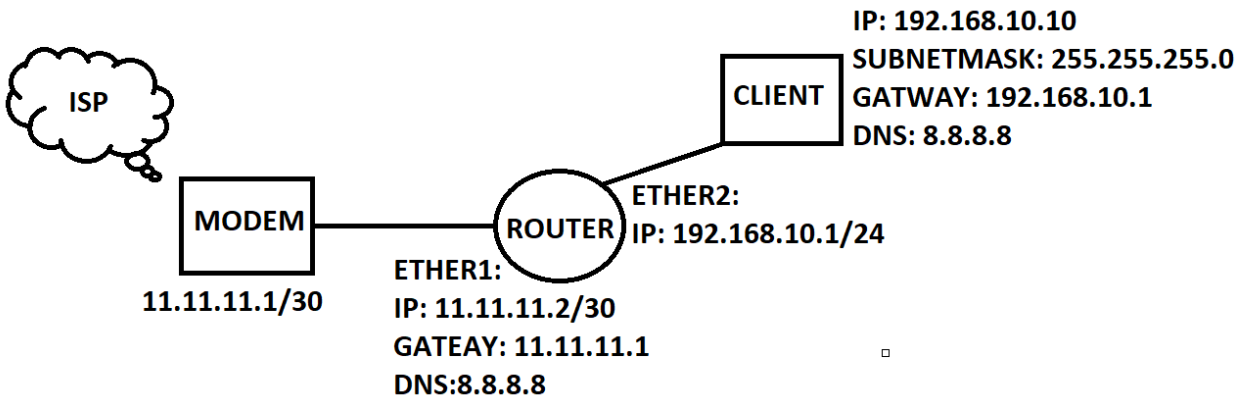
Setelah dipastikan packet data antara client dan Router sudah tidak ada masalah maka buka Browser apapun lalu tembak IP Router pada URL Website.



Gambar 1.17 Tampilan Web Fig

1.3. Setup Internet

1. Lab Akses Internet



Gambar 1.18 Skema Setup Internet

Berikut adalah skema untuk setup Internet dari modem sampai ke client, pada skema tersebut terdapat sebuah ISP (Internet Service Provider) dengan IP Static 11.11.11.1/30 kemudian dihubungkan dengan Ether1 Router Mikrotik dengan konfigurasi IP 11.11.11.2/30, Gatway adalah alamat IP yang digunakan agar Router Mikrotik dapat akses internet dari Modem dengan cara menggunakan IP yang ada "didepan" Ether 1 yaitu IP Modem 11.11.11.1 sebagai alamat gatway untuk Router Mikrotik, maka perlu konfirgurasi gatway pada Router mikrotik dengan IP: 11.11.11.1, serta jangan lupa untuk konfigurasi DNS pada Router Mikrotik agar Mikrotik dapat melakukan koneksi Internet dengan menggunakan domain seperti ping ke detik.com dan lain-lain.

Untuk jaringan local terdapat pada Ether2 Router Mikrotik dengan Konfigurasi IP: 192.168.10.1/24 karena menggunakan CIDR /24 maka Ip Client dapat terkoneksi dengan Ether2 diantaranya range 192.168.10.2 – 192.168.10.254 yang dapat digunakan untuk IP Client, pada Ether2 Router Mikrotik tidak diperlukan gatway karena gatway yang diseeting

sebelumnya sudah mencakup 1 Router Mikrotik itu sendiri jadi cukup memasukan IP pada Ether2 Router Mikrotik.

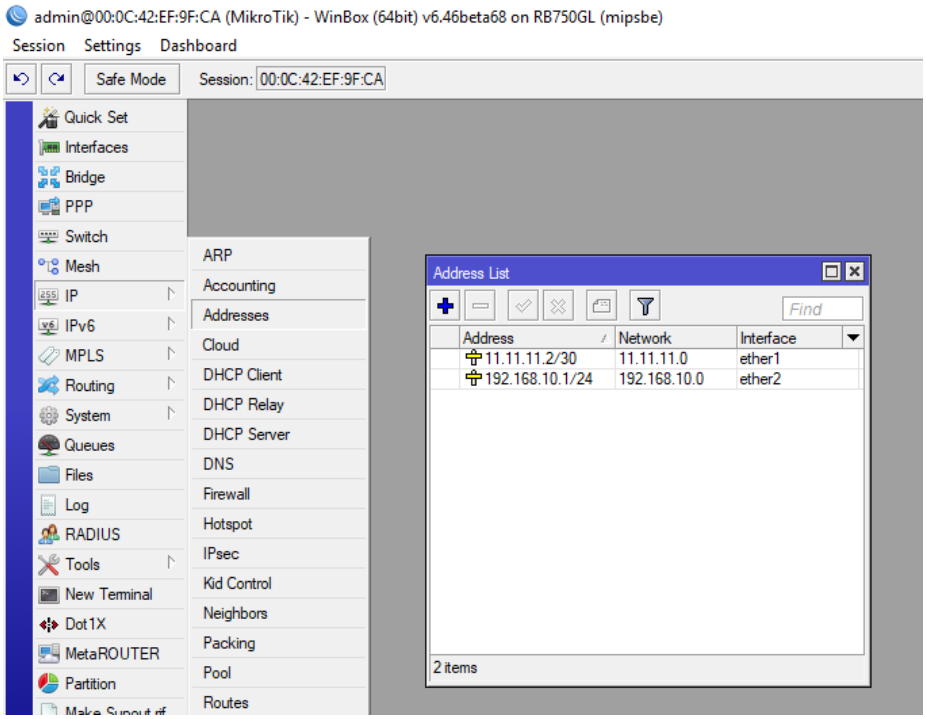
Sedangkan untuk Client karena terhubung dengan Ether2 Router Mikrotik maka Network yang digunakan haruslah 192.168.10.0 maka client dapat menggunakan IP: 192.168.10.10, subnetmask 255.255.255.0 gatway menggunakan IP yang ada "didepan" Client yaitu 192.168.10.1 dan DNS 8.8.8.8.

Untuk lebih jelasnya silakan perhatikan langah-langkah berikut:

Tabel 1.1 Langkah-langkah Konfigurasi Setup Internet

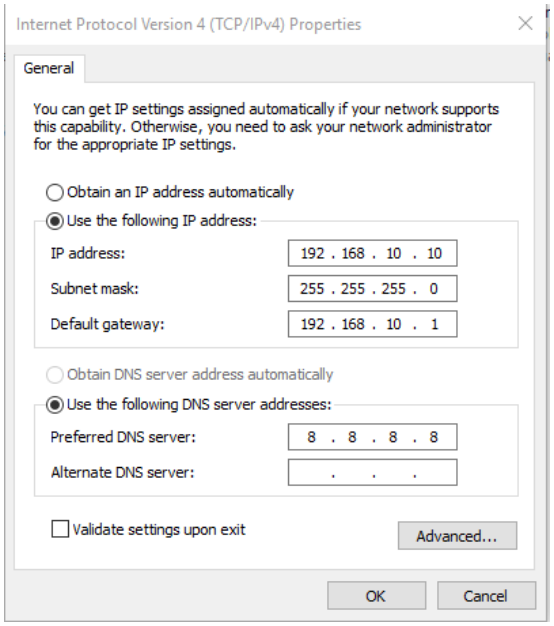
No	Penyelesaian
1	Membuat IP pada setiap Ether sertakan CIDR pada Router
2	Setting IP Client + DNS yang terkoneksi terhadap Ether tertentu
3	Cek Koneksi pastikan dari client dapat ping ke Router
4	Cek koneksi router ke ISP/modem
	akses internet
5	Setting gatway dan DNS pada Router Mikrotik gatway: ip route add gatway=10.10.10.25 (via terminal) DNS: ip -> DNS (via GUI)
6	Cek koneksi internet router mikrotik ping 8.8.8.8 ping google.com
7	Agar client dapat akses internet setting Firewall NAT ip -> firewall ->NAT -> + -> General, Chain:srcnat , outinterface:ether1 -> Action, Action:masqurade
8	test koneksi client ke internet

1. Membuat IP pada setiap Ether sertakan CIDR pada Router



Gambar 1.19 Konfigurasi IP Router

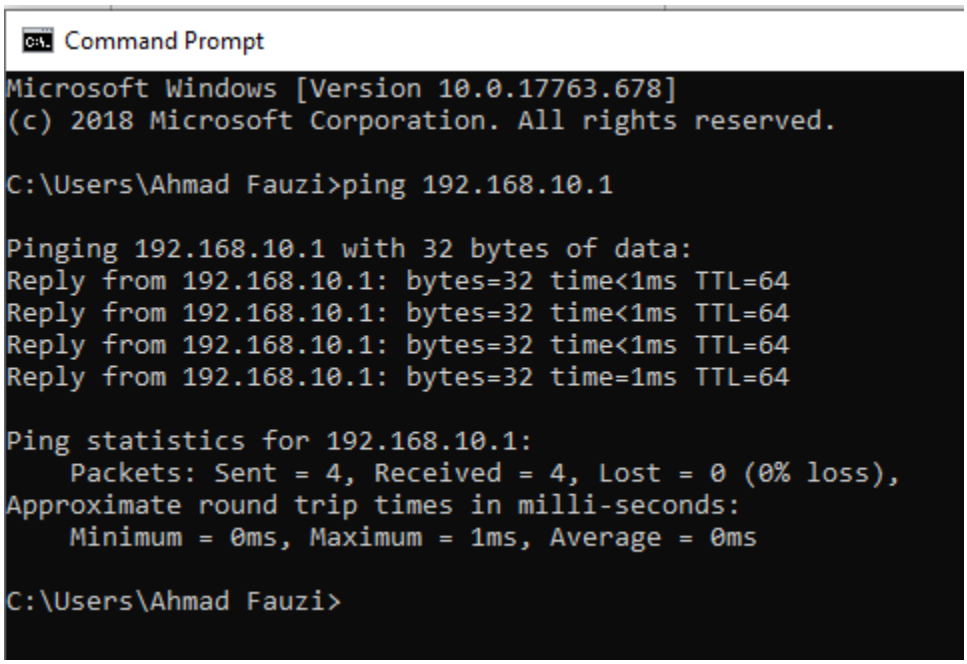
2. Setting IP Client + DNS yang terkoneksi terhadap Ether tertentu



Gambar 1.20 Konfigurasi IP Client

3. Cek Koneksi pastikan dari client dapat ping ke Router

   Buka CMD Client lalu ketik ping 192.168.10.1 yang merupakan IP dari Ether2 atau IP Router Mikrotik

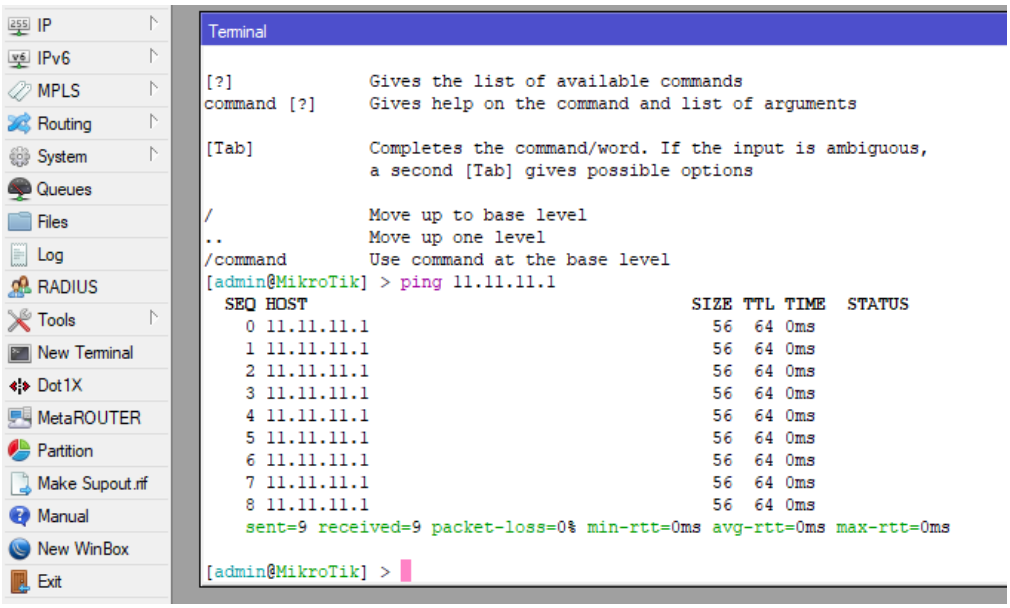


Gambar 1.21 Test Koneksi CMD client ke Router

Pastikan berhasil dan mendapar Replay dari router. Untuk kesempatan ini fokusnya adalah Ping dari client ke router abaikan jika tidak bisa ping dari client to client karena yang paling pokok adalah client dapat mengakses router.

4. Cek koneksi router ke ISP/modem

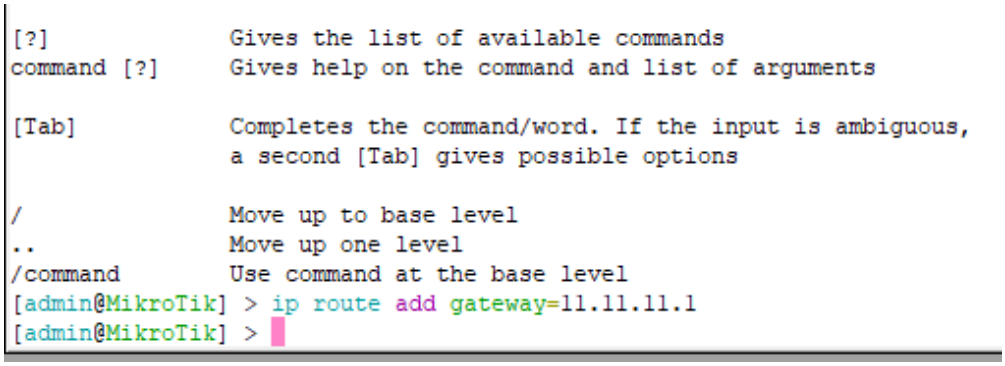
   Buka New Terminal pada Winbox dan ketikan ping 11.11.11.1 yaitu Ip dari Modem ISP.



Gambar 1.22 Test Koneksi Terminal Router ke Modem ISP

5. Setting gatway dan DNS pada Router Mikrotik

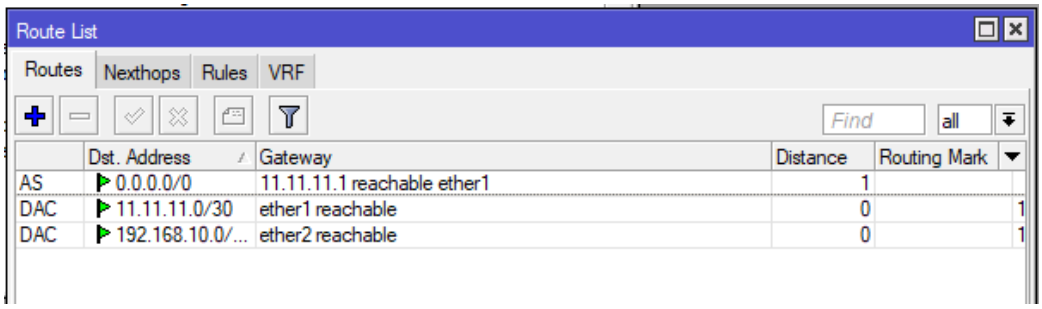
   Setting Gatway kita dapat menggunakan Commad pada Terminal dengan perintah "ip route add gatway=11.11.11.1"



Gambar 1.23 Setting Gatway dengan Terminal Router

Dan Pastikan sudah terdapat pada Route List.

Pada menu IP => Routes

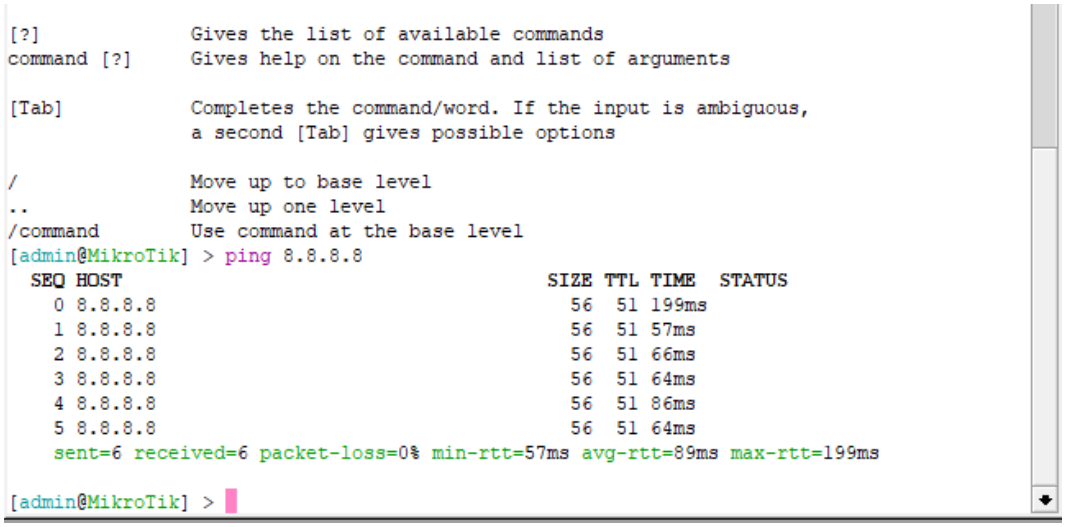


Gambar 1.24 Route List gatway yang sudah tersetting

Sudah masuk dengan Dst. Address 0.0.0.0/0 berpapun IP yang dituju maka dapat menggunakan IP gatway 11.11.11.1.

6. Cek koneksi internet router mikrotik

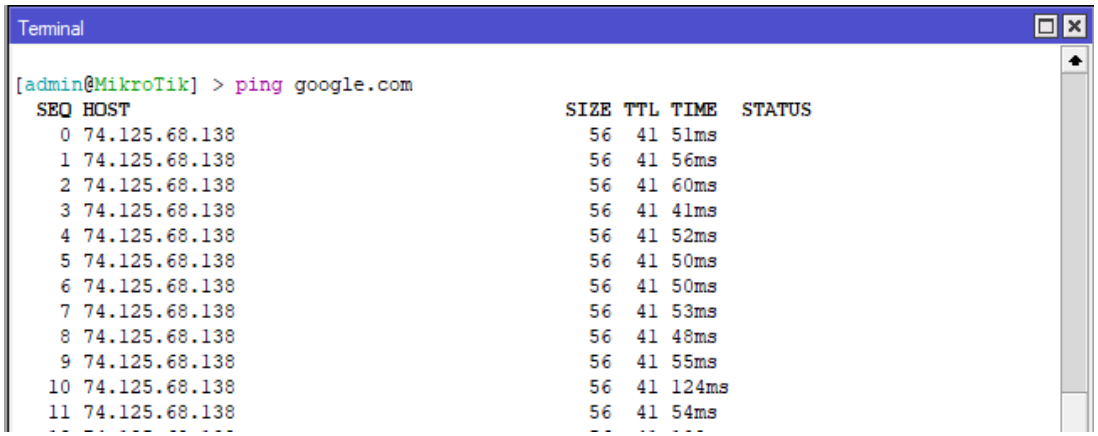
Dengan menggunaka Terminal maka lakukan ping 8.8.8.8, maka hasilnya:



Gambar 1.25 Cek Koneksi Terminal Router ke IP Google

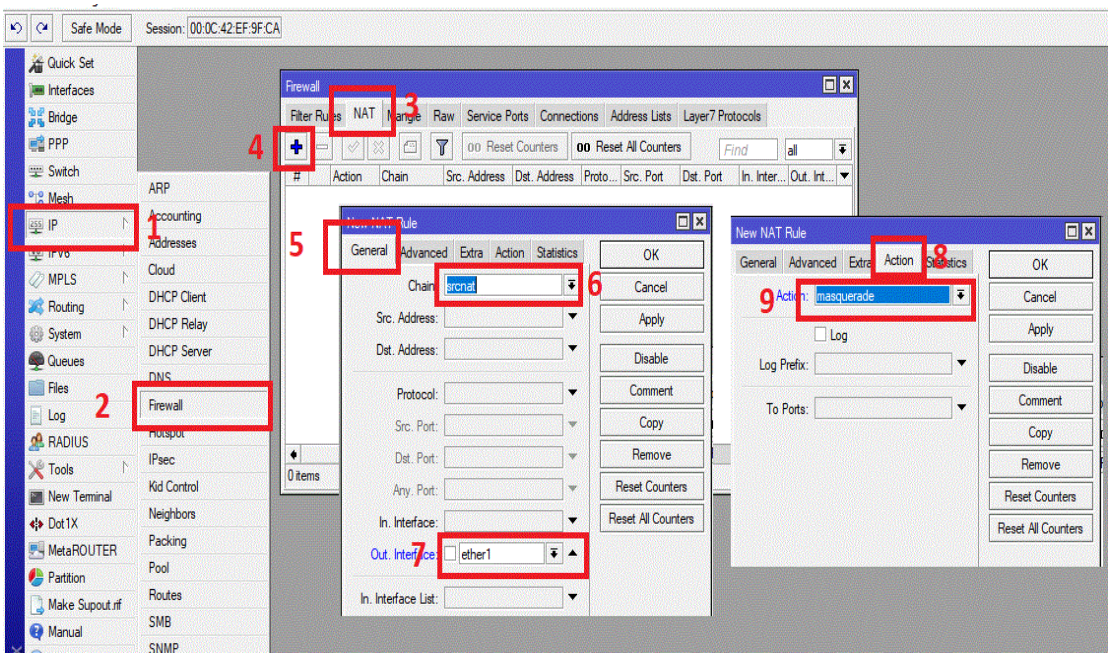
Pastikan Router Mikrotik dapat melakukan ke IP Google 8.8.8.8

Setelah dapat melakukan test koneksi dengan menggunakan IP google, maka sekarang dapat dilakukan dengan menggunakan domain google.com. buka terminal kembali dan ping google.com



Gambar 1.26 Cek Koneksi Terminal Router ke DNS Google

7. Agar client dapat akses internet setting Firewall NAT

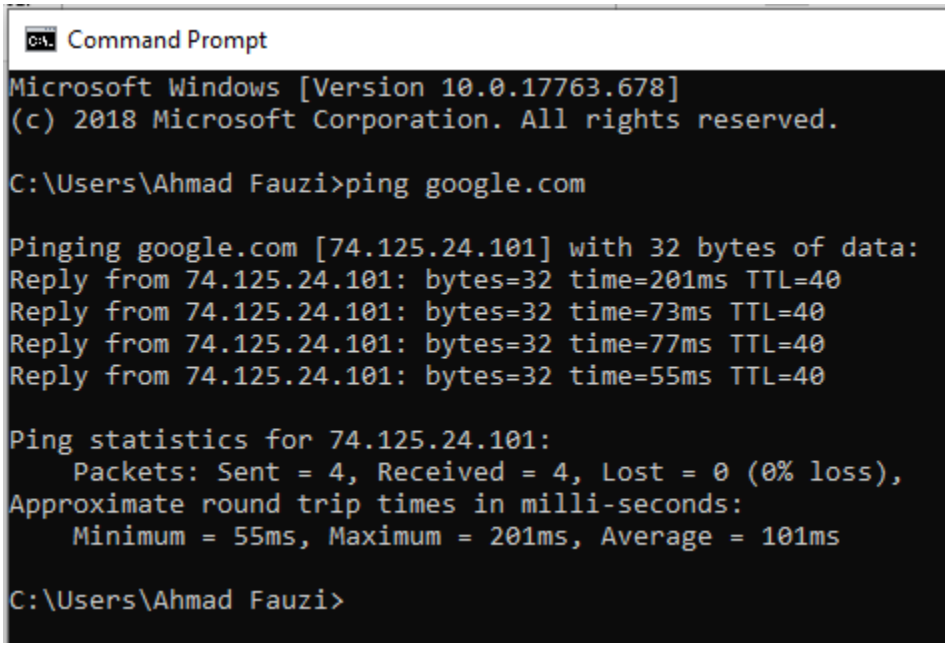


Gambar 1.27 Konfigurasi NAT

1. Pilih IP
2. Firewall
3. Menu NAT
4. Ketik “+”
5. Menu General
6. Chain: srcnat
7. Out. Interface: Ether 1 (Ether yang dapat akses kemodem Internet)
8. Menu Action
9. Action: masquerade

8. Test koneksi client ke internet

   Setelah Sudah diatru untuk firewall NAT maka pastikan Client sudah dapat mengakses internet dengan membuka CMD lalu ping kedomain google.com



Gambar 1.28 Test Koneksi Client Ke Internet

Pastikan sudah dapat Reply dari google dan sudah dapat digunakan akses Internet untuk clientnya,

1.4. Basic TCP/IP Subnetting

Penggunaan IP Address merupakan hal sangat penting untuk membentuk sebuah komunikasi antar perangkat yang terhubung ke jaringan. Setiap jaringan yang dibangun tentunya memiliki model yang berbeda-beda karena disesuaikan dengan kebutuhan yang ada. Dengan perbedaan topologi suatu jaringan maka terdapat juga perbedaan dalam penggunaan jenis alamat (Address Type).

Secara umum dalam dunia networking dikenal ada 4 macam 'Address type', yaitu Unicast, Broadcast, Multicast, Anycast. Masing-masing jenis tersebut memilki perbedaan dalam fungsi transmisi data. Dan berikut ini ulasan singkat mengenai perbedaan dari 'Address type' diatas.

1. Unicast

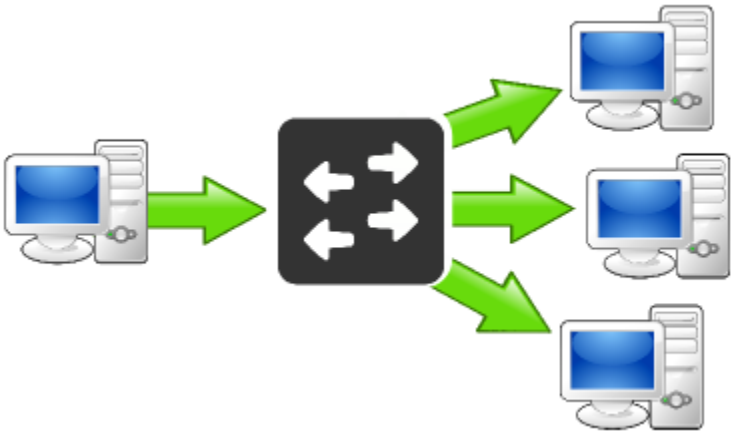
   Unicast merupakan suatu metode pengiriman (transmisi) data dalam jaringan dengan mekanisme 1 : 1 atau PTP (Point-to-Point). Dengan kata lain pengiriman data dilakukan antara satu alamat pengirim dan satu alamat penerima. Ketika data berhasil diterima maupun gagal diterima, maka si-pengirim akan memberikan informasi ke pengirim. Untuk topologi jaringan dengan komunikasi 'Connection-Oriented' (TCP), jika data gagal diterima maka akan dilakukan pengiriman ulang sampai data dapat dikirim secara lengkap.

Gambar 1.29 Unicast

Contoh dari transmisi data menggunakan tipe alamat Unicast sering dilakukan dalam komunikasi perngakt sehari-hari. Misal, file sharing antar 50amper50r, browsing, akses file server, dan lain-lain.

2. Broadcast

Broadcast merupakan metode pengiriman (transmisi) data ke banyak perangkat sekaligus atau PTMP (Point to MultiPoint). Dalam pengiriman ke banyak titik (Point) dengan metode ini tidak perlu memperhatikan apakah data tersebut sampai ke penerima atau tidak. Dan juga tidak melihat apakah perangkat penerima pada setiap titik tersebut sedang aktif siap menerima paket data atau tidak. Metode ini komunikasi biasanya dilakukan pada setiap perangkat yang tergabung di dalam jaringan yang sama atau dengan kata lain tergabung dalam satu alamat broadcast yang sama. Kalau kita mempelajari subnetting maka alamat broadcast merupakan alamat terakhir dari sebuah subnet. Misal, jika ada network dengan subnet 192.168.1.0/24 maka alamat broadcastnya adalah 192.168.1.255. Dan hal itu biasa disebut sebagai Subnet Broadcast. Ada juga Limited Broadcast yang mana transmisi data menggunakan alamat 255.255.255.255



Gambar 1.30 Broadcast

Contoh penggunanan jenis transmisi broadcast ini banyak dilakukan untuk siaran TV dan Radio. Dan sering kita temukan juga biasanya digunakan dalam proses DHCP.

3. Multicast

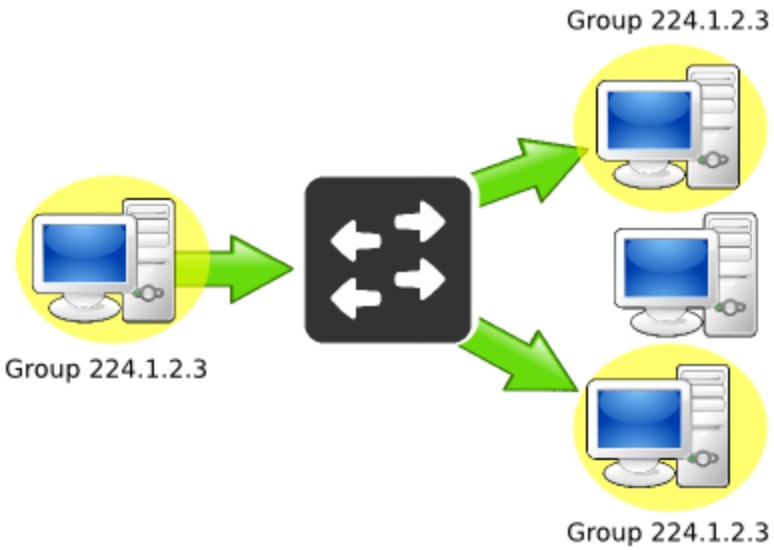
Multicast metode yang digunakan juga 51amper sama dengan broadcast. Namun perbedaannya untuk multicast ini akan melakukan transmisi data ke banyak titik (point) yang tergabung ke group alamat yang sama. Jadi jika ada perangkat yang tidak tergabung ke dalam group maka tidak akan mendapatkan transmisi data. Dan alamat yang digunakan disini adalah biasa disebut dengan alamat multicast. Ada beberapa alamat multicast yang digunakan tergantung jenis service-nya. Contohnya seperti berikut:

a. 224.0.0.18 : VRRP

b. 224.0.0.5-224.0.0.6 : OSPF LSA/DR

c. 224.2.0.0-224.2.127.253 : Multimedia Conference Call

Masih banyak lagi service yang menggunakan alamat multicast. Selengkapnya bisa kita lihat pada link disini.

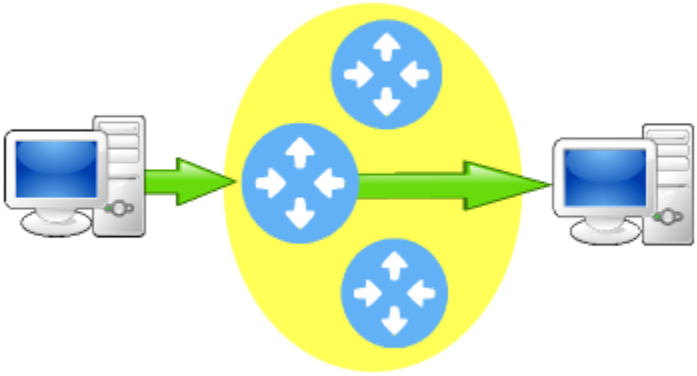


Gambar 1.31 Multicast

Contoh penggunaan dari multicast lebih sering dikenal dalam melakukan Real-Time Streaming Video (RTSP).

4. Anycast

   Anycast merupakan sebuah metode transmisi (pengiriman) data Point-to-Point-Nearest. Bisa dibilang untuk mekanisme dari anycast ini gabungan antara unicast dengan multicast. Di dalam transmisi Anycast antara si-pengirim dan si-penerima mempunyai alamat yang jelas, namun untuk menuju ke penerima akan menggunakan titik (point) sebuah group yang memiliki jalur terdekat.



Gambar 1.32 Anycast

Alamat ini juga digunakan hanya sebagai alamat tujuan (destination address) dan diberikan hanya kepada router, bukan kepada host-host biasa. Contoh penggunaan alamat anycast ini banyak ditemukan pada Ipv6.

5. Subnetting Perhitungan Sederhana

   Sebelumnya sudah dijelaskan cara menentukan Subnetwork, Ip awal, Ip akhir hingga Ip broadcast pada penjelasan sebelumnya, pada kali ini kita akan menentukan Ip yang dapet terkoneksi denga ip sebuah client.

   Contohnya adalah:

   a. Berikut adalah IP pada client A =10.10.10.45/28, maka berapakah IP yang dapat terkoneksi dengan client A?

      Untuk menjawab pertanyaan diatas bilamana kita menggunakan Cara yang sebelumnya tentunya akan memakan banyak waktu oleh karena itu pertanyaan tersebut dapat dijawab dengan langkah berikut:

      Gunakan Tabel untuk mengetahui jumlah ip ada setiap CIDR

Tabel 1.2 Subnet Mask

Prefix	Subnet Mask 255.255.255.(256-jml IP)	Jumlah IP	Jumlah Host (Jml IP – 2)
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	-
/32	255.255.255.255	1	-

Perhatikan untuk /28 maka jumlah ip yang dapat digunaka adalah 16 maka dengan itu dapat dibuatkan pola sebagai berikut:

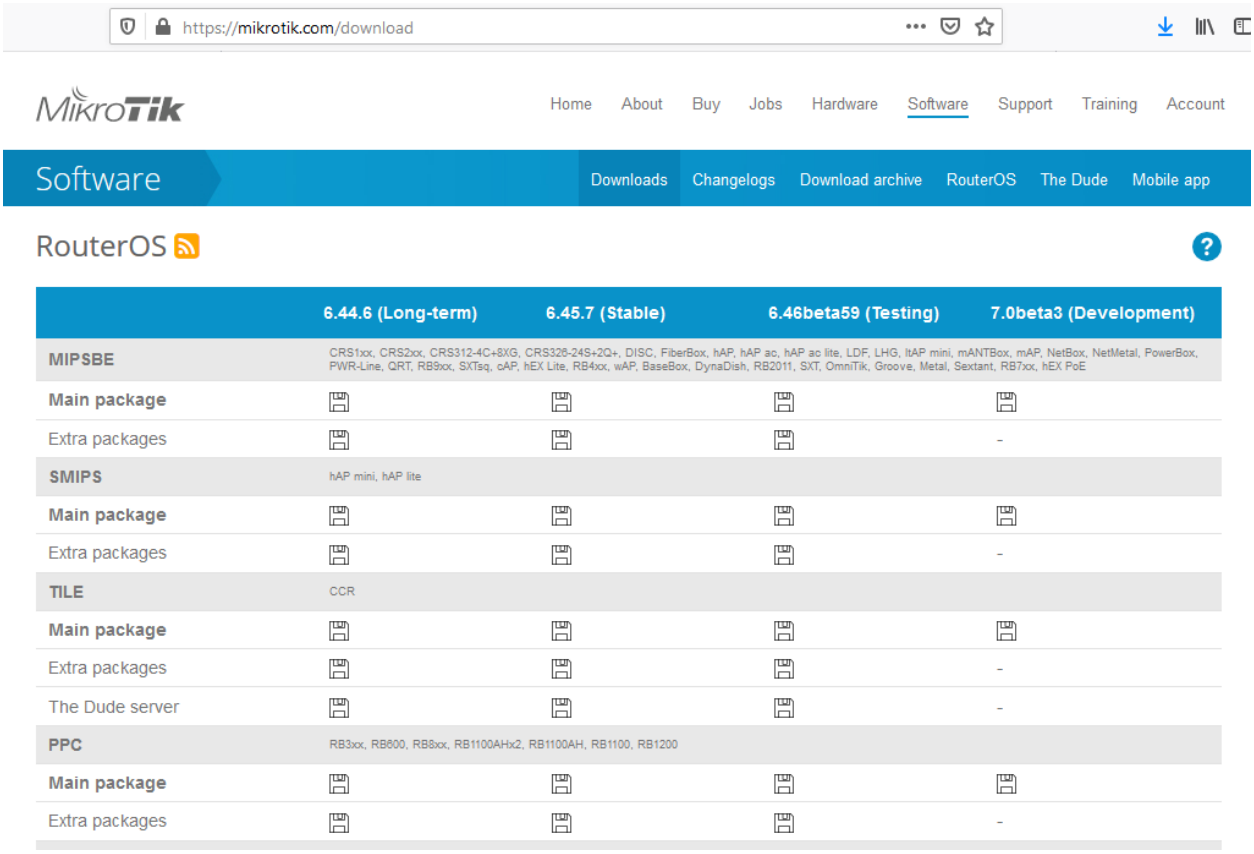
Subnet			Broadcast
<	awal +1	akhir -1	>
0			15
16			31
32	**33**	**46**	**47**
48			63
64			

Subnet didapatkan dari kelipata dari 16 dan dimulai dari angka 0 lalu 16 lalu 32 hasil pertambahan bukan kelipan 16, untuk broadcast didapatkan pada baris 1 maka 16-1 = 15, maka dimulai dari 15. Lalu baris kedua didapatkan dari 32-1=31 dan seterusnya, hingga dapat dicar untuk Ip Awal ditambah 1 sedangkan ip akhir dikurangi 1 dan dapat disimpulkan bahwa ip yang dapat terkoneksi oleh

10.10.10.45/28 adalah **Ip 10.10.10.32 s/d 10.10.10.47**

BAB II
Upgrade Router OS

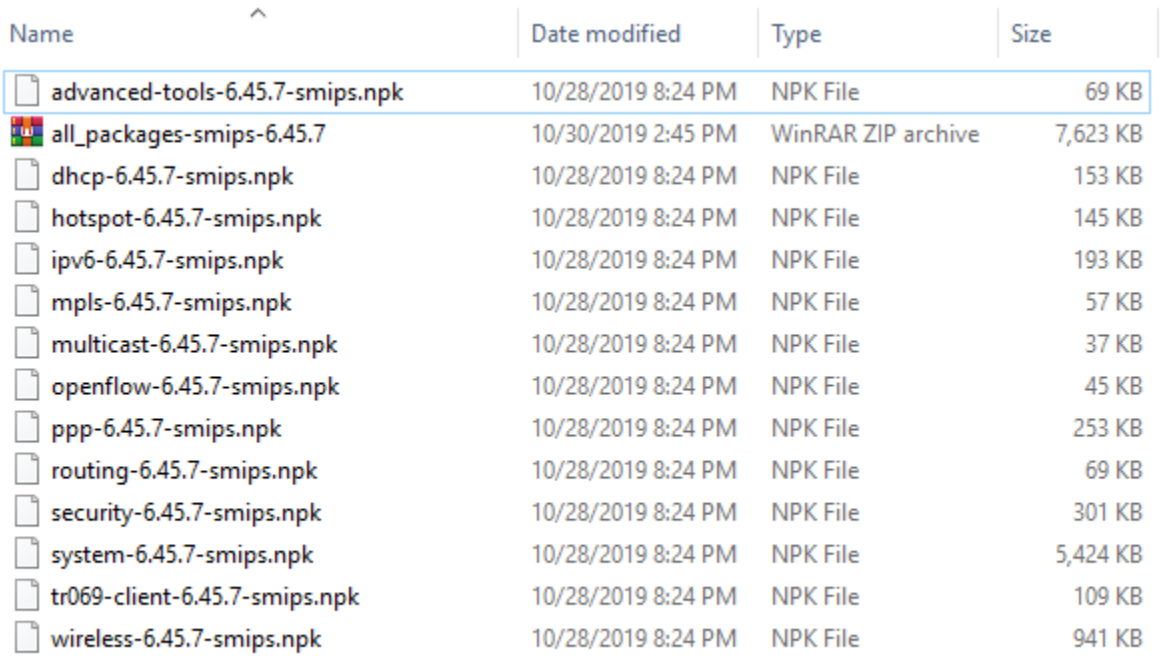
Upgrade Router dilakukan agar dapat meningkatkan versi sebuah OS mIkrotik yang kemungkinan akan selalu menutupi dan memperbaiki bug-bug yang ada pada versi sebelumnya atau dapat untuk meningkatkan keamanan yang lebih baik dibandingan dengan versi sebelumnya, untuk itu cara melakukan upgrade diperlukan bahan MikrotikOS dengan cara mendownload dihalaman resmi Mikrotik.com



Gambar 2.1 Download OS Router Mikrotik

Pada situs mikrotik.com akan selalu mengalami update untuk itu sebagai administrator network maka kita harus memperhatikan atau dapat mengikuti perkembangan update versi dari

sebuah Router Mikrotik agar dapat diterapkan atau diinstal pada perangkat Router yang kita miliki, dan perlu diperhatikan bahwa dalam melakukan upgrade kita harus mengetahui jenis Processor yang digunakan pada sebuah router yang sudah dijelaskan pada materi sebelumnya, terdapat keterangan main package merupakan sebuah Update yang berikan secara keseluruhan atau satu bundle sedangkan untuk extra Packages merupakan satu kesatuan aplikasi yang terpisah dan dapat diinstall menyesuaikan kebutuhan dari sebuah network.

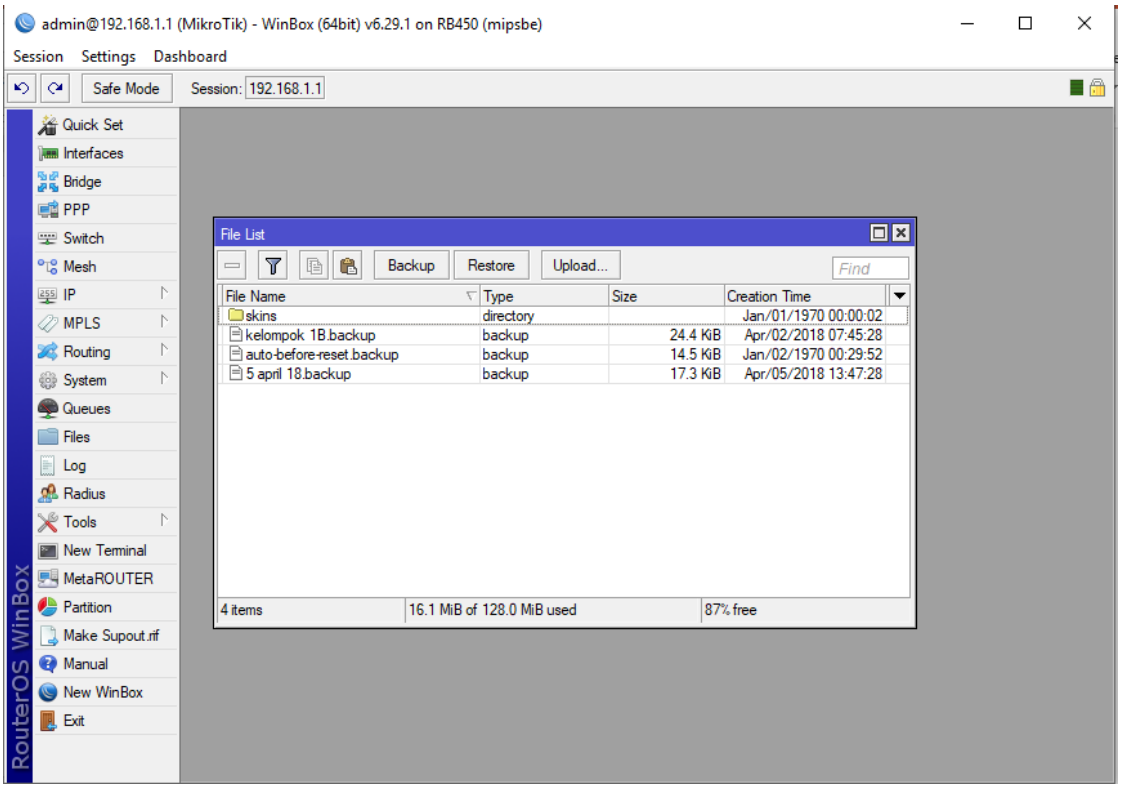


Name	Date modified	Type	Size
advanced-tools-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	69 KB
all_packages-smips-6.45.7	10/30/2019 2:45 PM	WinRAR ZIP archive	7,623 KB
dhcp-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	153 KB
hotspot-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	145 KB
ipv6-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	193 KB
mpls-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	57 KB
multicast-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	37 KB
openflow-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	45 KB
ppp-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	253 KB
routing-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	69 KB
security-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	301 KB
system-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	5,424 KB
tr069-client-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	109 KB
wireless-6.45.7-smips.npk	10/28/2019 8:24 PM	NPK File	941 KB

Gambar 2.2 OS Versi Extra Packages

Berikut cara melakukan Upgrade:

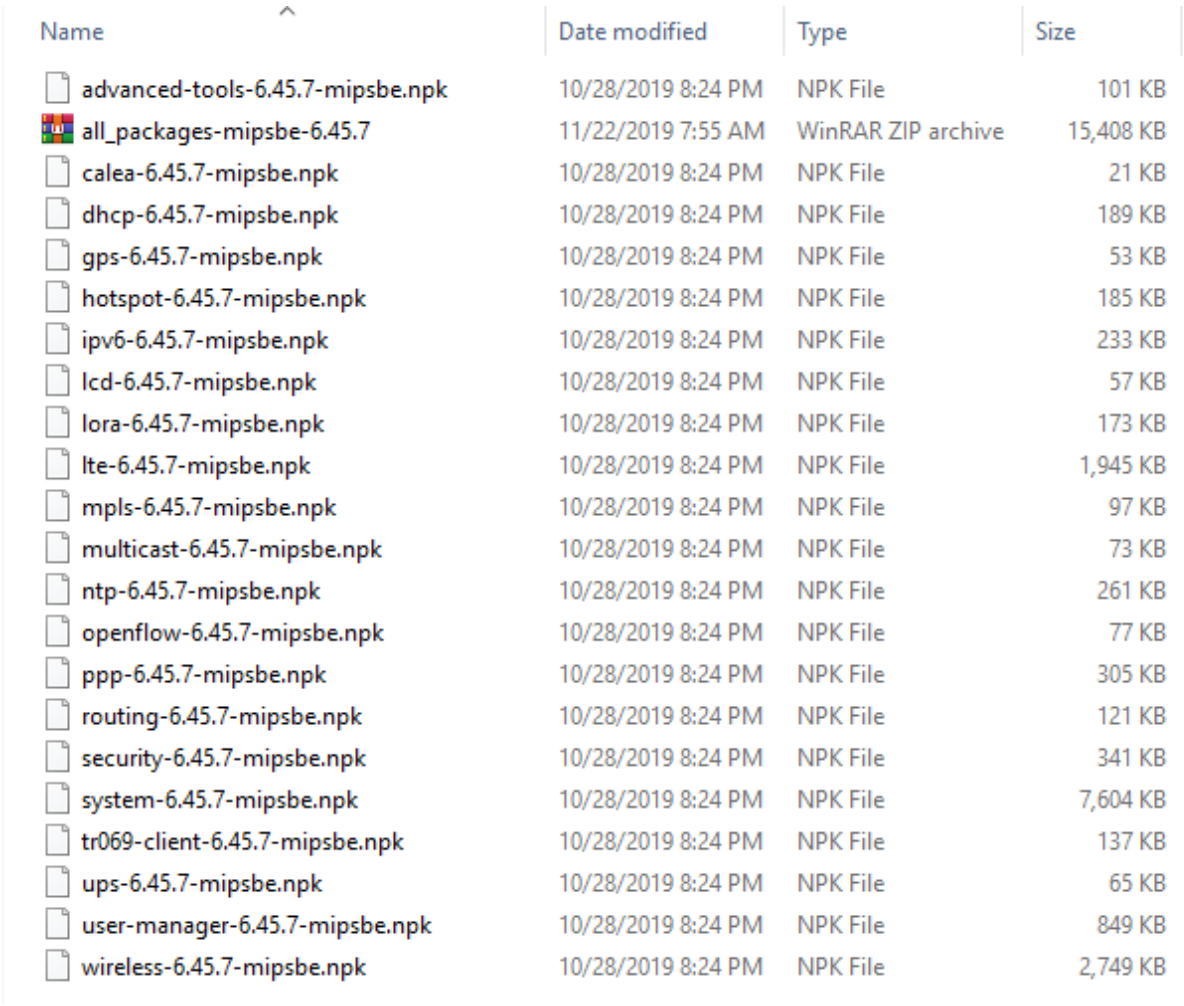
1. Router Mikrotik versi 6.29



Gambar 2.3 Tampilan Menu List

Pada gambar diatas bahwa Router Mikrotik masih menggunakan versi yang lama yaitu v 6.29

Untuk melakukan upgared siapkan dahulu software yang sama dengan arsitektur Router tersebut disini menggunakan arsitektur mipsbe



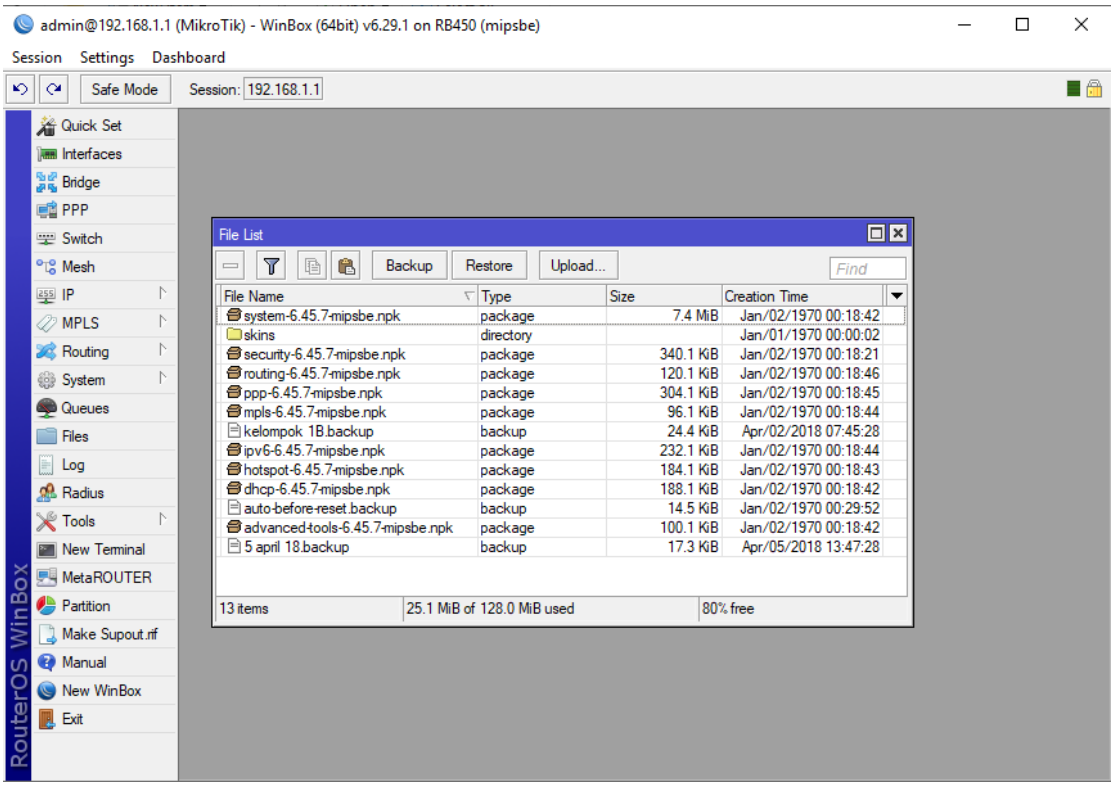
Name	Date modified	Type	Size
advanced-tools-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	101 KB
all_packages-mipsbe-6.45.7	11/22/2019 7:55 AM	WinRAR ZIP archive	15,408 KB
calea-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	21 KB
dhcp-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	189 KB
gps-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	53 KB
hotspot-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	185 KB
ipv6-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	233 KB
lcd-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	57 KB
lora-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	173 KB
lte-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	1,945 KB
mpls-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	97 KB
multicast-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	73 KB
ntp-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	261 KB
openflow-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	77 KB
ppp-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	305 KB
routing-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	121 KB
security-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	341 KB
system-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	7,604 KB
tr069-client-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	137 KB
ups-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	65 KB
user-manager-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	849 KB
wireless-6.45.7-mipsbe.npk	10/28/2019 8:24 PM	NPK File	2,749 KB

Gambar 2.4 Tampilan Extra Packages versi Mipsbe

Sudah didownload dan di extrack sehingga terlihat service-service yang dapat kita tentukan sendiri dan ini buka versi bundle atau satu paket.

2. Import dengan cara Klik and drag dari folder computer kedalam file Router

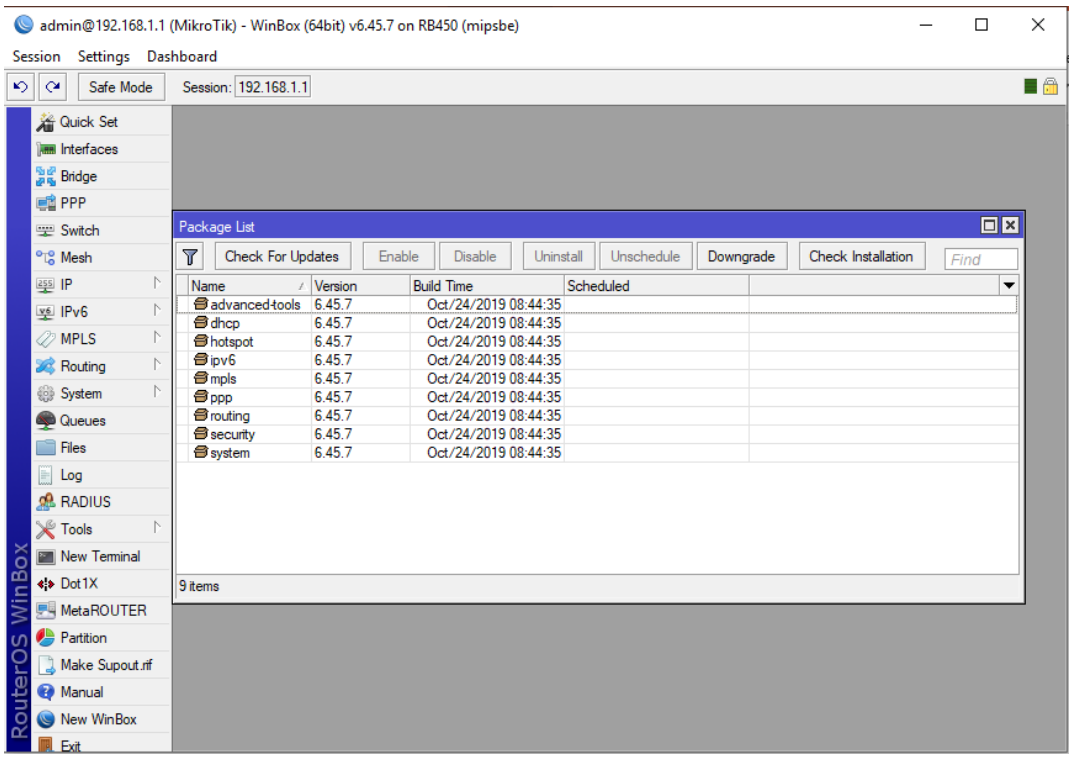
   Setelah kita memilih service apa saja yang akan digunakan maka Klik and Drag dari folder computer menuju File Router Mikrotik



Gambar 2.5 Drag File kedalam File List

Maka Semua Service yang kita perlukan sudah ditransfer kedalam file Router Mikrotik pastikan pada tahaap ini aliran listrik ke Router Mikrotik jangan sampai terputus, bilamana dalam proses reboot aliran listrik terputus akan menyebabkan kerusakan secara software pada perangkat Router Mikrotik, sekali lagi pastikan power yang terhubung benar-benar dalam kondisi yang baik.

3. Reboot



Gambar 2.6 Hasil Update pada File List

Setelah dilakukan reboot maka file yang sebelumnya ada pada menu File akan menghilang dan dapat dilihat pada System => packages sudah terupdate menjadi versi 6.45 yang sebelumnya adalah versi 6.29

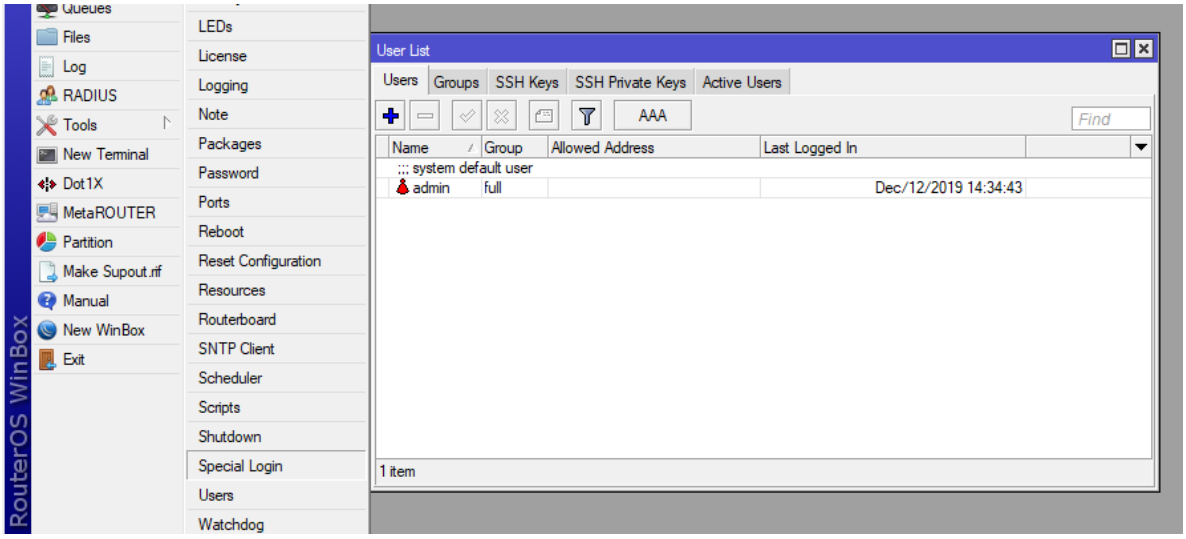
Login & Service

Login adalah sebuah akses yang digunakan untuk masuk kedalam system sebuah Router Mikrotik dengan format username dan password, pada Router Mikrotik yang masih default maka menggunakan username:admin dan password:"kosong", permasalahannya adalah ketika masih menggunakan user yang default maka dapat dimasuki oleh pihak luar dengan sangat sangat mudah, oleh sebeb itu perlu dibuatkan Hak akses untuk login pada Router Mikrotik dibagi menjadi 3 kategori:

FULL : adalah akses yang dikelolah dapat merubah, melihat isi konfigurasi pada Router Mikrotik dan dapat membuat Login baru

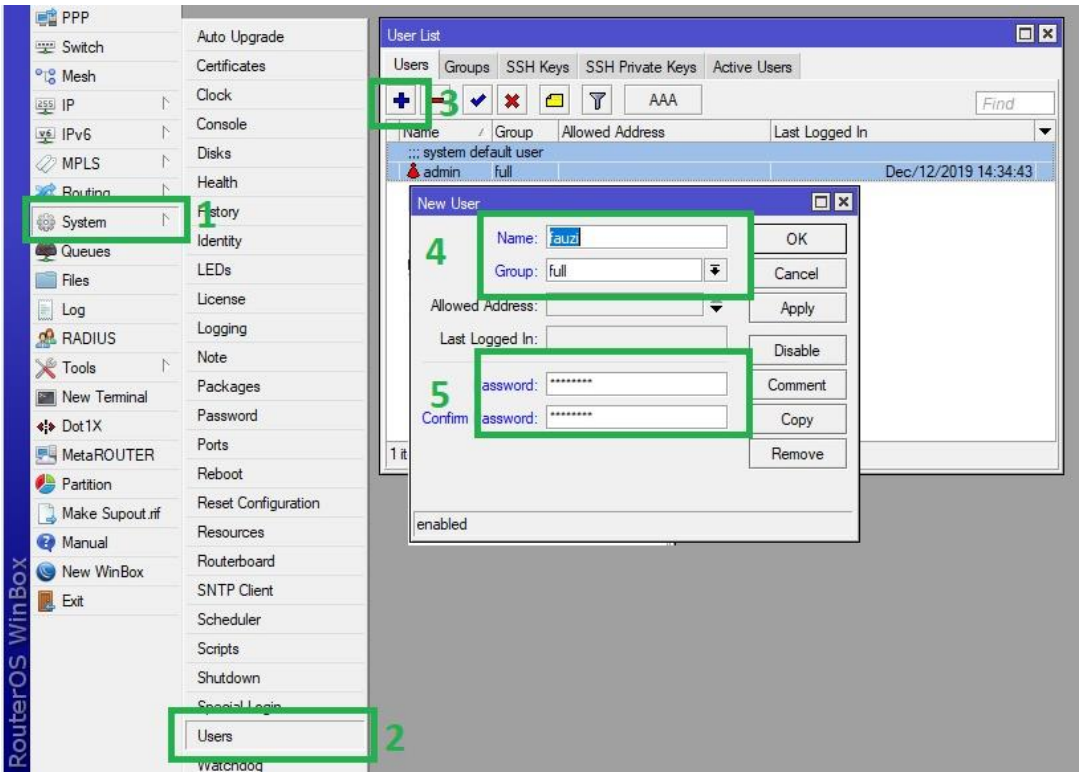
READ : adalah akses yang dikelolah semata-mata hanya dapat melihat isi konfigurasi dari Router Mikrotik ia tidak dapat merubah sedikitpun konfigurasi

WRITE : adalah akses yang dikelolah hanya dapat merubah dan melihat sebuah konfiguarasi Router Mikrotik akan tetapi tidak dapat membuat akun login baru untuk orang lain.



Gambar 2.7 Tampilan User List

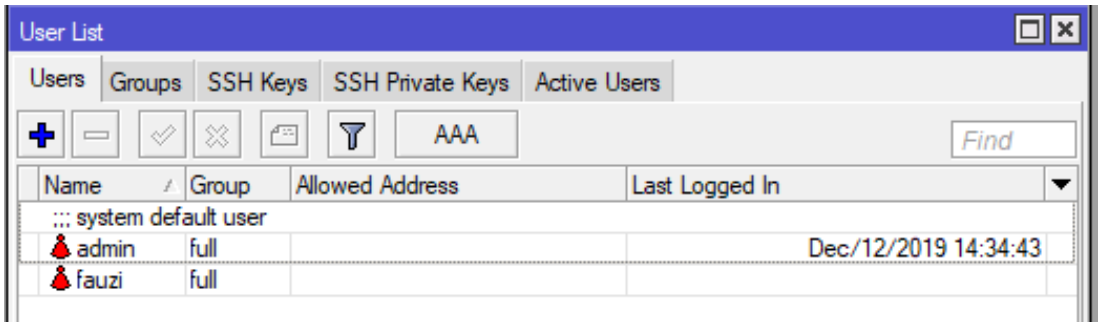
Untuk dapat membuat akun user baru maka dapat menngunakan menu System => User maka akan tampil userlist yang masih default, untuk itu tambakan 1 user baru dengan nama Fauzi dan password=password.



Gambar 2.8 Tampilan Membuat User List

System => User => pilih + => Name: Fauzi , Grup: Full, password=password, confirm password: password => Apply => OK

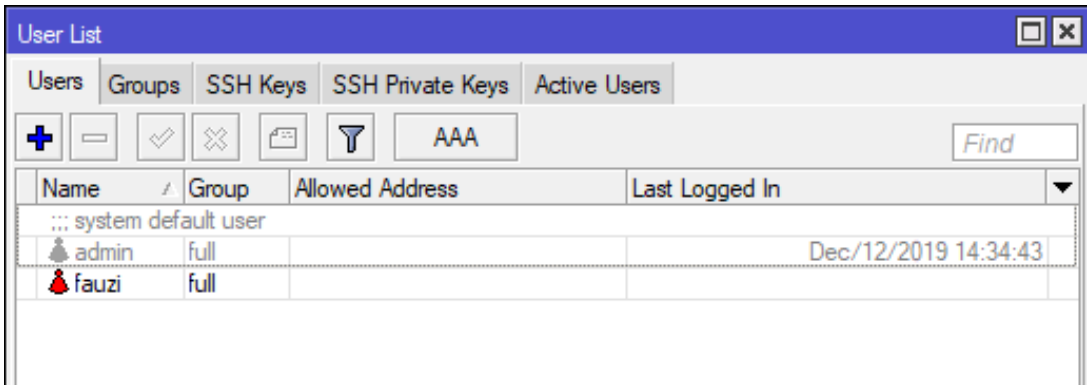
Maka sudah masuk kedalam User List



Gambar 2.9 Tampilan User List akun Baru

Agar orang lain tidak dapat login dengan user default maka untuk user admin dapat disable atau dihapus, pada kesempatan ini akan disable dengan cara :

Pilih user admin => pilih tanda X



Gambar 2.10 Tampilan User List yang disable

Maka user login admin default sudah tidak dapat lagi digunakan dengan cara disable atau dihapus.

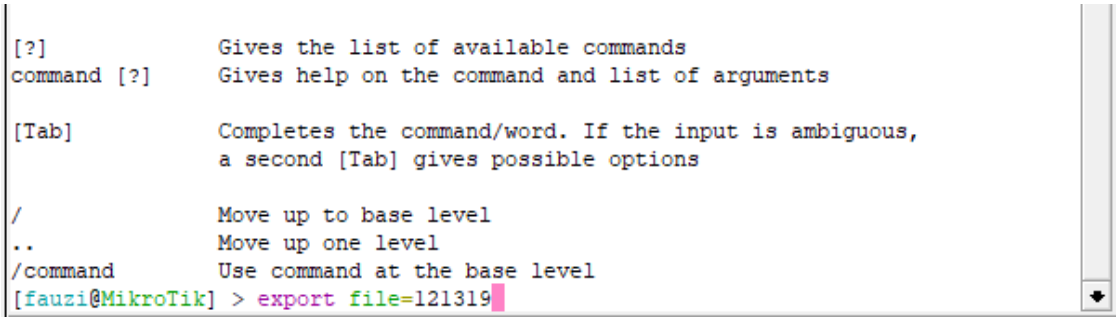
Backup Configuration

Dalam membackup sebuah settingan atau konfigurasi mikrotik terdapat 2 buat metode dan masing-masing metode memunya perbedaan disaat melakukan backup konfigurasi berikut ada metode yang digunakan untuk membackup sebuah konfigurasi:

Tabel 2.1 Perbedaan Scrip Backup dan Binnary Backup

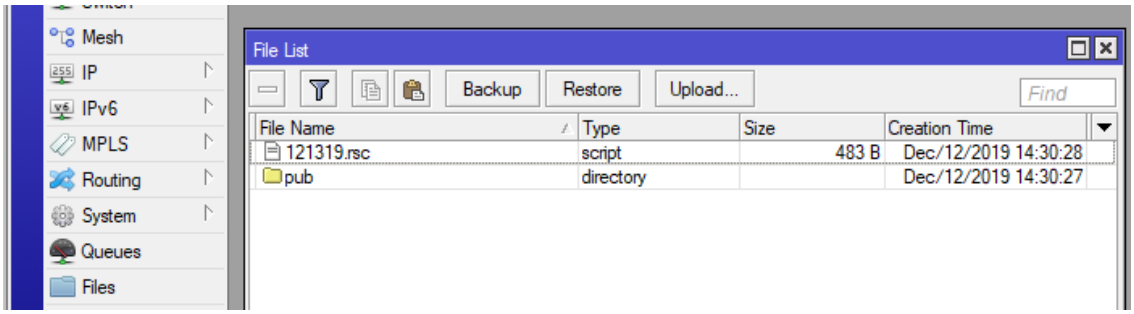
Perbedaan	Script Backup	Binnary Backup
Command	Export / Import	Backup / Restore
Bisa dengan menu klik	No	Yes
Backup all config	No (user&Pass)	Yes
Need reboot to restore	No	Yes
Backup sebagian config	Yes	No
Bisa dibaca test editor	Yes	No

Metode yang digunakan adalah Script Backup untuk melakukam backup dengan metode script maka dalam membuka Terminal => ketik “export file=”nama file”.



Gambar 2.11 Script Export File

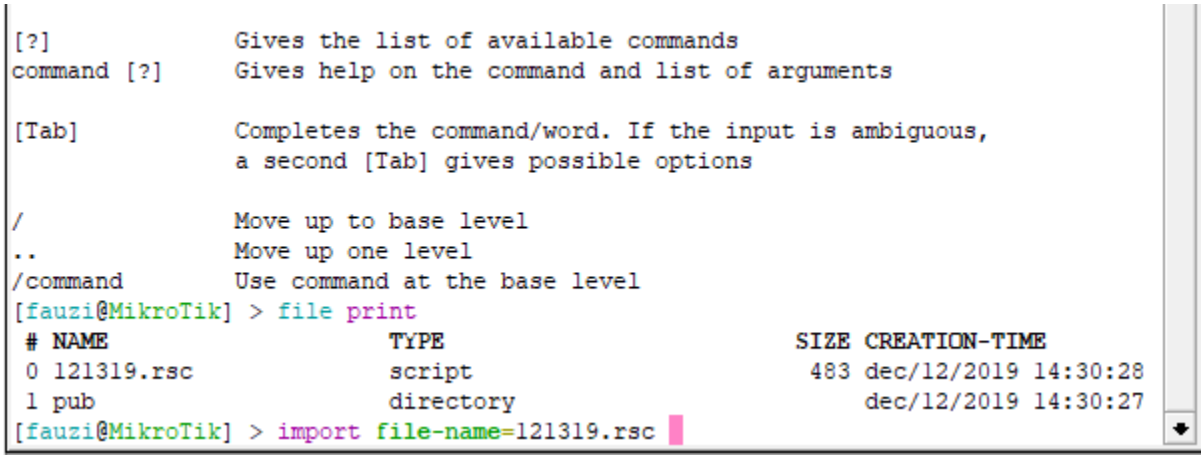
Bahwa metode script backup hanya dapat dilakukan dengan menggunakan command line dengan perintah “EXPORT” , tidak terdapat pada menu GUI, user dan password tidak akan berbackup artinya hanya isi dari semua kofigurasi kecuali hak akses atau user, tanda maelakukan reboot sudah masuk semua konfigurasi, dapat melakukan backup sebagian konfigurasi sepeti hanya backup IP saja dan lain-lain dan dapat dibuka pada menu editor dan dapat dipindahkan antar Router Mikrotik dengan versi yang berneda-beda.



Gambar 2.12 hasil Backup pada Menu File List

Hasil backup script backup pada menu File terdapat file yang sudah terbackup dengan extantion .rcs dengan nama file 121319.rcs, klik kanan pada file tersebut dan download maka akan tersimpan dikomputer user.

Untuk melakukan restore pada script backup “export” perlu diperhatikan bahwa router dalam keadaan bersih atau sudah direset semua kofigurasi yang terdapat pada router tersebut.



Gambar 2.13 Script Import

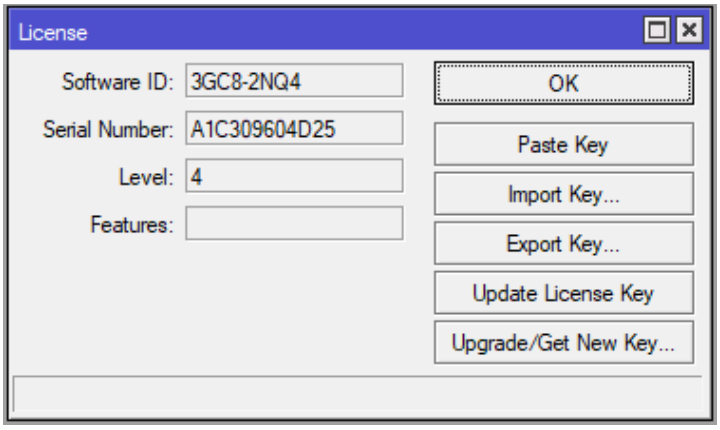
Bila data backup tidak terdapat pada file, maka dapat dilakukan klik and drag dari file pada computer client kedalam file.

Untuk melihat data difile maka gunakan command line “file print” maka akan terlihat file yang terdapat padda menu file pastikan file backup sudah tersedia.

Untuk lakukan restor maka menggunakan perintah “import file-name=121319.rsc”, maka semua konfigurasi akan tersetting kembali pada router mikrotik.yang baru.

Router OS Lisence

Lisence adalah sebuah serial Key yang didapatnya dengan berbagai macam ada yang berbayar dengan sebuah lisence tertentu dan ada yang sudah include dengan perangkat router, untuk lisence dapat dilihat pada menu System => Lisence



Gambar 2.14 Tampilan Lisence

Pada ganbar diatas terdapat sebuah informasi bahwasannya perangkat tersebut terdaftar sebagai Lisence pada level 4 , adapun level-level yang terdapat pada RouterOS diantaranya level 0 sampai dengan Level 6.

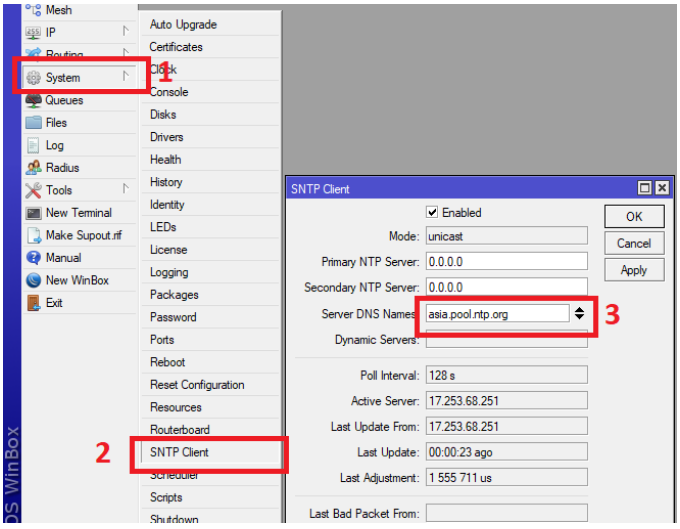
Tabel 2.2 Perbedaan Lisence

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

Pada level 0 maka semua service secara real time akan tersimpan dalam waktu 24 jam dan selebihnya konfigurasi akan hilang dengan sendirinya, pada level 1 bisa dikatakan pada lisence ini hanya sebagai ujicoba atau trial dengan jumlah client hanya sebanyak 1 buah sebagai ujicoba, sedangkan yang membedakan level 3,4,5 dan 6 adalah harga lisence dan jumlah client yang dapat diakses oleh Router dengan versi 6 maka tidak ada Batasan dalam menfigurasi client.

1.5. NTP & Netinstall

NTP (Netwok Time Protokol) adalah sebuag sevice untuk memberi informasi waktu yang diberikan oleh sebuah Router secara real time, Kebanyakan RB tidak memiliki power untuk menyimpan waktu dan hanya versi-versi tertentu yang dapat menyimpan waktu seperti versi RB230, sangatlah penting dalam penyesuaian NTP agar sesuai dengan waktu real time tujuannya adalah ketika akan mendokumetasikan sebuah file LOG makan data akan sesuai dengan watu yang sedang berjalan, makan NTP pada Router dapat menyesuaikan dengan sebuah waktu server sepeti asia.pool.ntp.org, atau id.pool.ntp.org dapat dikonfiguras secara client NTP karena menerima data waktu dari server waktu.

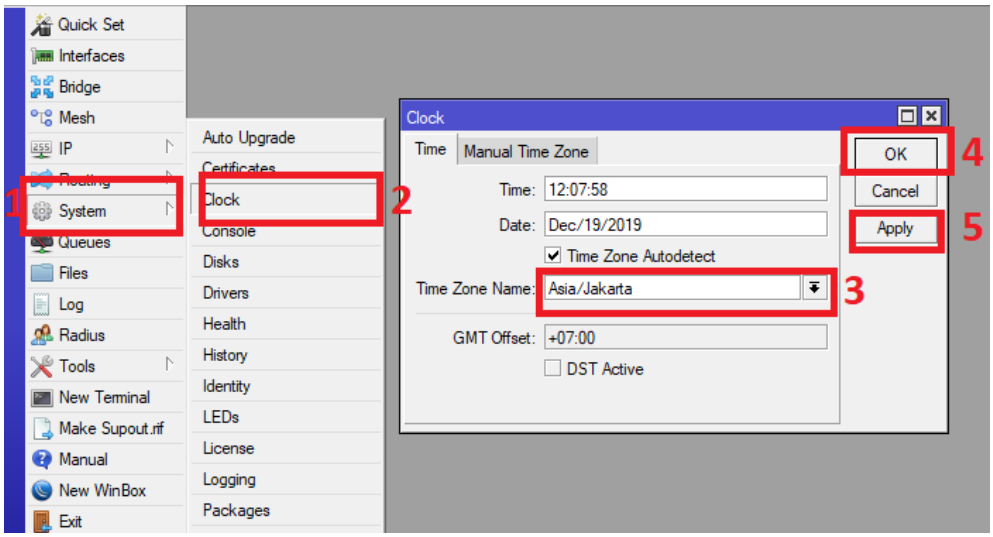


Gambar 2.15 Setting SNTP

1. Pilih System
2. SNTP Client pastikan Router sudah Terkoneksi dengan internet
3. Server DNS Name masukan URL Server waktu asia.pool.ntp.org
4. Apply
5. OK

Maka akan terisi otomatis untuk IP server yang digunakan pada router tersebut.

Langkah selanjutnya menyesuaikan jam router dari wilayah tempat kita berada/tinggal.

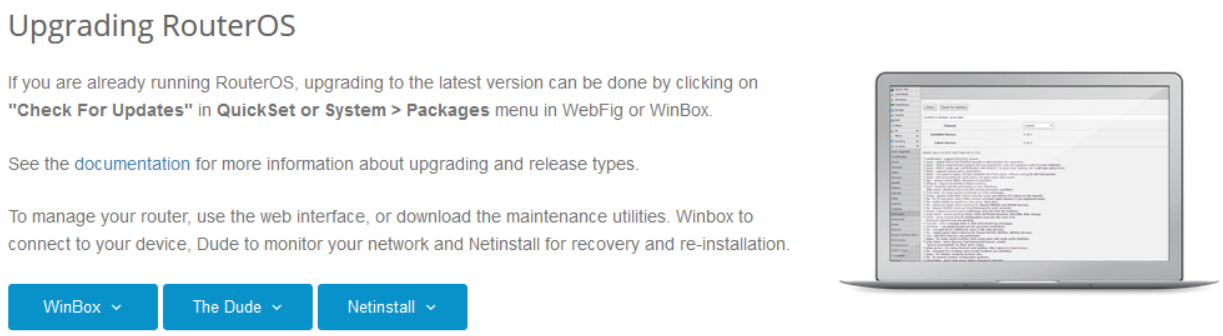


Gambar 2.16 Setting Clock Router

1. System
2. Clock
3. Setiing Zona berdasarkan tempat tinggal anda
4. Apply
5. OK

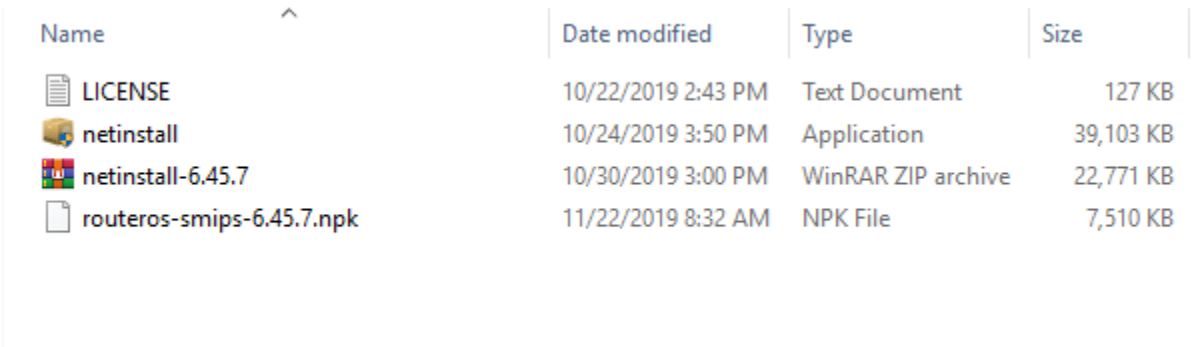
Netinstall adalah sebuah aplikasi yang digunakan untuk Install ulang sebuah RouterBoard yang mengalami kerusakan secara system sehingga sebuah router tidak dapat diakses dengan menggunakan Winbox, secara kegagalan system dapat terjadi diantaranya: mati daya saat melakukan upgrade via Winbox, RouterBoard yang sudah using atau sudah lama tidak digunakan, peningkatan versi yang tidak sesuai dengan versi sebelumnya akan menyebabkan router tidak dapat terbaca oleh winbox dan tidak terdeteksi oleh winbox oleh karena itu yang dapat dilakukan adalah install ulang dengan menggunakan Netinstall.

Aplikasi Netinstall harus didownload langsung dari situs remi Mikrotik.com



Gambar 2.17 Download Netinstall

Dapat didownload pada menu NetInstall lalu extrack pada folder masing-masing.



Gambar 2.18 Extrack Netinstall

Sudah terekstrak dan siapkan Router OS dengan mendownload pada mikrotik.com dan sesuaikan dengan jenis Processor Router

RouterOS

	6.44.6 (Long-term)	6.46.1 (Stable)
MIPSBE	CRS1xx, CRS2xx, CRS312-4C+8XG, CRS326-24S+2Q+, DISC, FiberE PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox,	
Main package		
Extra packages		
SMIPS	hAP mini, hAP lite	
Main package		
Extra packages		

Gambar 2.19 OS Main packeg

BAB III

Wireless

3.1. Wireless Network Overview

Jaringan wireless adalah jaringan yang memungkinkan pengiriman informasi atau data antar host dilakukan secara nirkabel atau tanpa menggunakan kabel. Jaringan wireless ini menggunakan gelombang elektromagnetik untuk membawa informasi antara saru host dengan host lainnya. Tentunya gelombang elektromagnetik ini akan merambat melalui media udara. Dilain pihak beberapa spektrum atau bagian dari gelombang elektromagnetik tersebut tidak dapat digunakan secara bebas. Pemerintah dari suatu negara pasti menerapkan aturan-aturan tertentu tentang penggunaan gelombang elektromagnetik ini.

Sebelum jauh membahas implementasi atau penerapan wireless LAN ada baiknya kita lihat kategori teknologi wireless secara umum. Teknologi wireless dikelompokan ke dalam 4 kategori besar yaitu;

1. **Wireless Personal Area Network (WPAN)**
   Merupakan jaringan wireless dengan area kerja terkecil. Umumnya digunakan untuk menghubungkan berbagai macam peripheral seperti mouse, keyboard, speaker. Teknologi umum yang sering digunakan adalah Bluetooth dan infrared.
2. **Wireless Local Area Network (WLAN)**
   Merupakan perluasan dari jaringan Lan kabel. WLAN menggunakan Radio Frequency (RF) dan memungkinkan beberapa host terhungung satu sama lain ataupun terhubung ke jaringan kabel dengan bantuansebuah perangkat yang disebut sebagai Access point. WLAN ini sering juga gisebut sebagai Wireless Fidelity (WiFi)
3. **Wireless Metropolitan Area Network (WMAN)**
   Merupakan jaringan wireless yang daerah cakupannya lebh luas dari WLAN. Adapun contoh teknologi yang digunakan oleh WMAN adalah Wi-Max
4. **Wireless Wide Area Network (WWAN)**
   Merupakan jaringan yang mentediakan akses dengan area yang sangat luas. Jaringan telefon seluler mengginakan teknologi seperti Global System fot Mobile Communication (GSM) atau pun Code Division Multiple Access (CDMA)

Dari beberapa teknologi yang digunakan untuk wireless maka sejumlah standarisasi dibuat dan disusun untuk memastikan perangkat wireless dapat berkomunikasi dengan baik. Standarisasi tersebut berisikan beberapa infotmasi penting yang harus di sertakan pada saat perangkat wireless tersebut dibuat. Organisasi utama yang bertanggung jawab dengan standarisasi perangkat wireless ini adalah Institute of Electical and Electronics Engineers (IEEE).

IEEE membentuk beberapa kelompok kerja yang bertujuan menghasilkan standarisasi, termasuk standarisasi WLAN ini dikenal dengan kelompok kerja 802.11. itu pula yang mendasari standarisasi WLAN yang dihasilkan IEE dikenal sebagai standar IEEE 802.11.

Beberapa literatur terkadang hanya menuliskan dengan istilah 802.11. standar IEEE 802.11 inilah yang mengatur teknologi WLAN, seperti radio frequency (RF) yang akan digunakan, kecepatan pengiriman dara (data rate), bagaimana informasi tersebut dikirimkan informasi tersebut dikirimkan melalui media udara dan lain-lain. Sejauh ini ada 5 (lima) perubahan besar yang dilakukan oleh IEEE terhadap perkembangan teknolofi WLAN. Perubahan standar tersebut diberi label 802.11a, 802.11b, 802.11g, 802.11n, dan 802.11ac. sstandar-standar ini juga dikenal sebagai Wireless Fidelity (WiFi).

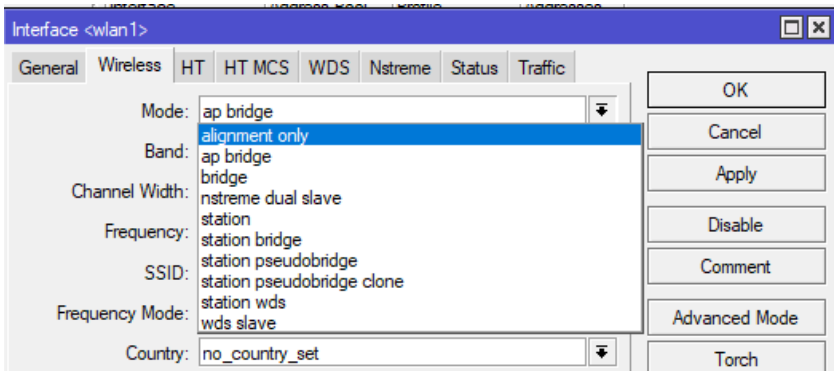
Standard	Tahun Rilis	Frequency Band	Bandwidth	Modulation	Max. Data Rate
802.11	1997	2,4 Ghz	20 MHz	DSSS, FHSS	2 Mbps
802.11b	1999	2,4 Ghz	20 MHz	DSSS	11 Mbps
802.11a	1999		20 MHz	OFDM	54 Mbps
802.11g	2003	2,4 Ghz	20 MHz	DSSS, FHSS	54 Mbps
802.11n	2009	2,4 GHz 5 GHz	20 MHz 40 MHz	OFDM	600 Mbps
802.11ac	2013	5 GHz	20, 40, 80,160 MHz	OFDM	6,93 Gbps
802.11ad	2012	60 GHz	2,16 GHz	SC, OFDM	6,76 Gbps

3.2. Parameter Dasar MikroTik

Untuk membangun sebuah Wireless LAN tentunya akna menggunakan beberapa perangkat wireless dan bila perankat wirelesssmua sudaj tersedia, maka pekerjaan selanjutnya adalah melakukan konfigurasi.

3.2.1. Mode

Parameter yang pertama adalah **mode**. Parameter ini menentukan fungsi apa yang akan dijalankan olehsebuah perangkat wireless.



Mode yang ada di wireless MikroTik :

1. Mode Alignment Only

Mode Alignment only, biasa digunakan untuk membantu pada saat pointing dengan indikator beeper /buzzer pada RouterBoard, sebagai contoh kita bisa menambahkan script dimana ketika mendapatkan sinyal bagus maka beeper akan berbunyi.

2. Mode AP-Bridge

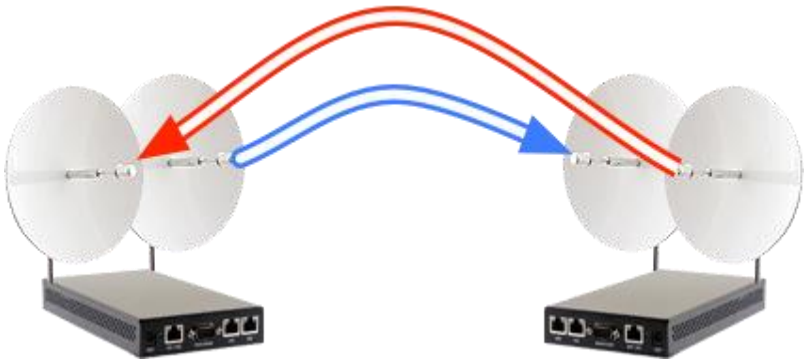
Mode AP-bridge digunakan sebagai Access point atau pemancar yang bisa melayani banyak client atau disebut juga dengan PTMP (Point To Multi Point), mode ini bisa kita gunakan untuk network yang sifatnya Routing ataupun Bridging. Untuk menggunakan mode AP-Bridge ini perangkat Routerboard minimal harus memiliki lisensi level 4.

3. Mode Bridge

Mode bridge digunakan sebagai Access point atau pemancar akan tetapi hanya bisa melayani satu client atau disebut juga dengan PTP (Point To Point), mode ini juga bisa kita gunakan untuk network yang sifatnya Routing ataupun Bridging. Untuk menggunakan mode ini perangkat Routerboard minimal memiliki lisensi level 3, sebagai contoh untuk type produk Embedded 5.xGHz jenis SXT-5HnD yang hanya memiliki license level 3, kita bisa membuat koneksi point to point dengan menggunakan 2 buah perangkat tersebut.

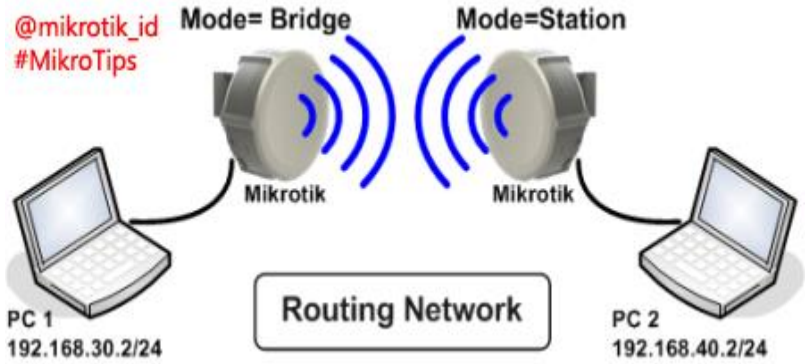
4. Mode Nstreme dual slave

Pada dasarnya mekanisme kerja pada interface wireless adalah half duplex, akan tetapi dengan menggunakan mode ini kita dapat mengaktifkan mekanisme kerja full duplex, mode ini merupakan proprietary didalam wireless mikrotik, tentunya kita juga membutuhkan 2 wireless card dan 2 antenna pada masing-masing wireless router mikrotik



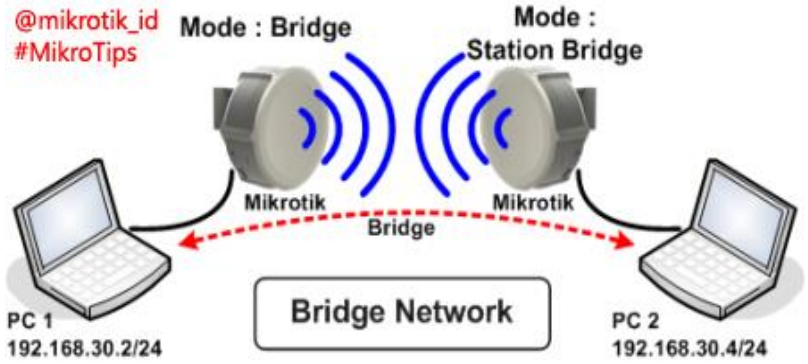
5. Mode Station

Wireless dengan Mode station ini digunakan sebagai wireless client/ penerima pada topologi PTP (Point To Point) atau PTMP (Point To Multi Point), wireless Mode station hanya bisa digunakan untuk membentuk network yang sifatnya routing, sehingga mode ini merupakan salah satu mode yang efektif dan efisian jika pada sisi wireless client/station tidak dibutuhkan bridging



6. Mode Station-Bridge

Mode Station-Bridge merupakan mode pada interface wireless yang berfungsi sebagai penerima / client dan support untuk bridge network, perlu di ketahui bahwa untuk mode ini hanya bisa digunakan apabila perangkat AP nya Mikrotik juga.



7. Mode Station-Psudobridge

Mode Station-Pseudobridge merupakan pengembangan dari Mode Station standar, sama-sama menjadikan wireless sebagai penerima/client, perbedaannya adalah pada Mode Station-Pseudobridge support untuk membuat network yang sifatnya Bridge Network, Di dalam penggunaan mode ini terdapat konsekuensi dimana untuk bridging pada L2 tidak bisa dilakukan secara penuh, dalam artian mac-address sebuah perangkat yang berada di bawah perangkat wireless (PC end user) tidak terbaca pada sisi Access Point.

8. Mode Station-Pesudobridge-Clone

Mode Station-Pseudobridge-Clone hampir sama dengan Mode Station-Pseudobridge yang membedakan adalah didalam mode ini bisa melakukan cloning mac-address, umumnya pada sebuah link wireless, yang terbaca pada sisi Access point adalah mac-address dari interface wireless client, tetapi jika menggunakan Mode Station-Pesudobridge-Clone yang terbaca adalah mac-address dari perangkat yang terhubung ke station (end user), Secara default yang terbaca adalah mac-address pada frame header yang pertama di teruskan, atau bisa ditentukan pada ﷺstation-bridge-clone-macﷺ

9. Mode Station-WDS

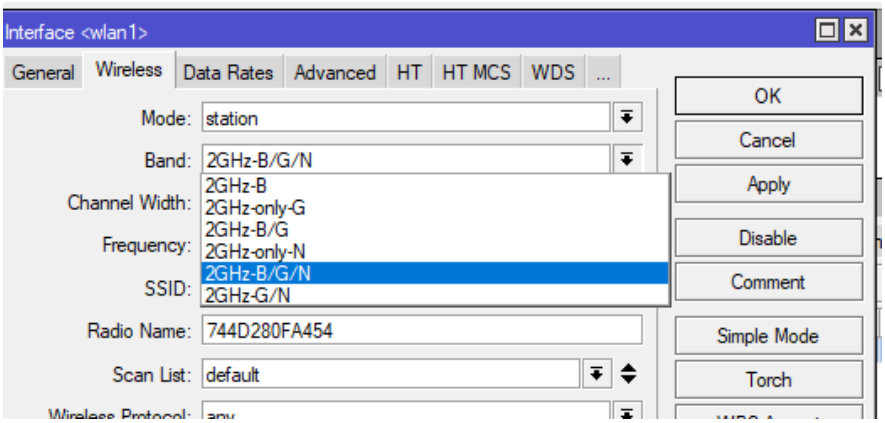
Mode Station-WDS berfungsi sebagai penerima/client dari sebuah Access Point yang mengaktifkan protocol WDS, Kekurangan protokol WDS adalah penurunan throughput wireless hingga 50%, perlu diketahui bahwa antara vendor yang satu dengan vendor yang lain fungsi WDS belum tentu compatible, begitu juga dengan WDS pada mikrotik.

10. Mode WDS-Slave

Mode WDS-Slave ini berfungsi sebagai pemancar (Access Point) sekaligus sebagai penerima (Station) atau disebut juga dengan repeater, Mode ini merupakan salah satu solusi apabila ingin membangun sebuah repeater tetapi perangkat yang dimiliki hanya menggunakan 1 card wireless card.

3.2.2. Band

Parameter ini menujukkan standarisasi apa yang dapat digunakan oleh sebuah perangkat. Pemilihan parameter ini juga mengntukan jenis perangkat lainnya yang dapat terhubung. Untuk router mikrotik serti terbaru, pilihan parameter band ini akan terlihat seperti berikut :



3.2.3. Channel (Frequency)

Pada saat access point ingin memancarkan RF untuk membawa traffic data maka perangkat tersebut harus menggunakan spektrim drekuensi tertentu, juka melihat dari spesifikasi atau standar IEEE 802.11 WLAN akan menggunakan spektrum frekuensi 2,4 GHz.

Rentang frekuensi ini masih dibafi-bagi menjadi beberapa channel. Adapun channel yang dapat digunakan untuk implrementasi jaringan wireless dapat dilihat dari table berikut ini..

Channel	Frekuensi (GHz)
Channel 1	2,412
Channel 2	2,417
Channel 3	2,422
Channel 4	2,427

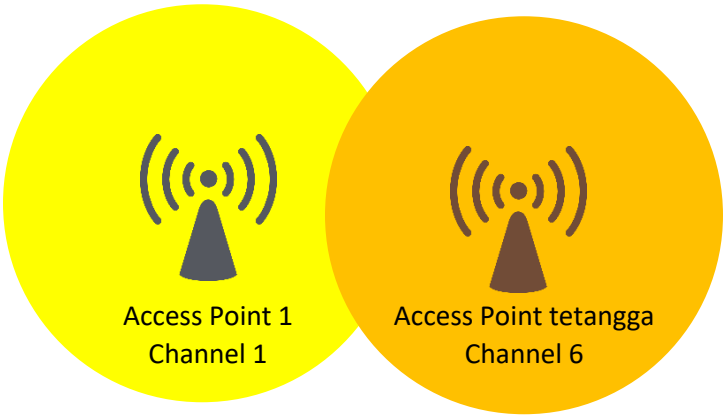
Channel 5	2,432
Channel 6	2,437
Channel 7	2,442
Channel 8	2,447
Channel 9	2,452
Channel 10	2,457
Channel 11	2,462
Channel 12	2,467
Channel 13	2,472
Channel 14	2,482

Dari table diatas terlihat bahwa frekuensi pertama yang dapat digunakan pada saat melakukan konfigurasi sebuah access point adalah 2,412 GHz. Frekuensi 2,412 GHz inilah yang disebut sebagai channel 1. Begitu pula frekuensi 2,417 GHz yang disebut sebagai channel 2 dan seterusnya.

Pemilihan channel pada saat akan melakukan konfigurasi harus mengikuti aturan spektrum frekuensi di suatu negara. Misalnya saja jika membangun WLAN di negara Amerika Serikat, maka channel yang diijinkan untuk digunakan hanyalah channel 1 sampai dengan channel 11. Sedangkan untuk Indonesia, diijinkan untuk menggunakan channel 1 sampai dengan channel 13.

Saat akan menentukan beberapa frekuensi yang akan digunakan pada access point. Anda harus melakukan **site survey** terlebih dahulu (site survey adalah kegiatan untuk melihat adakah radio frekuensi lain di sekitar tempat anda akan membangun WLAN.) apakah ada access point lain di sekitar tempat tersebut. Dan bila ternyata ada access point lain maka anda harus mencari tahu berapakah frekuensi atau channel yang digunakan oleh perangkat tersebut.

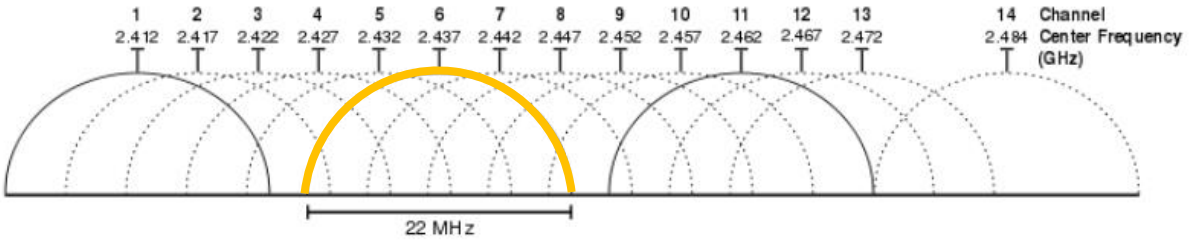
Contoh kasus :



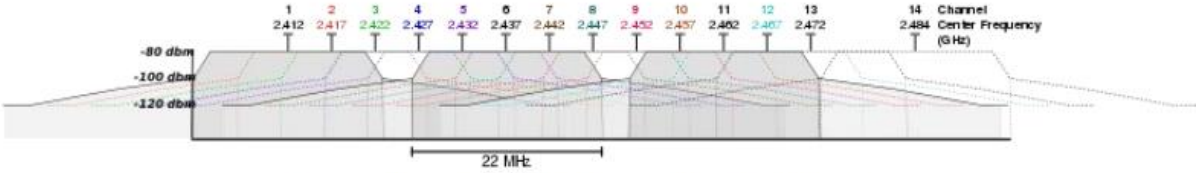
Misalnya pada contoh berikut pada saat melakukan site survey dan disekitar anda terdapat access point lain uang menggunakan frekuensi 2,437 GHz (Channel 6), maka access point yang akan anda bangun disarankan untuk tidak menggunakan frekuensi uamg sama dengan frekuensi 2,437 Ghz. Ini dimaksudkan untuk mencegah terjadinua interferensi pada radio frekuensi (RF). Interferensi frekuensi nantinya akan membuat performa jaringan wireless anda menurun drastis. Koneksi station ke access point akan banyak mengalami kegagalan karena frekuensi yang anda gunakan juga dipakai oleh access point “tentangga”.

Jika tetnagga tadi sudah menggunakan channel 6 pada access pointnya, maka disarankan untuk menggunakan channel 1 ataupun channel 11.

Sebuah frekuensi yang digunakan access point memiliki lebar frekuensi dan secara default lebar frekuensi tersebut adalah 22 MHz. ini yang menyebabkan access point yang menggunakan channel 6, masih akan dapat mempengaruhi access point yang berada pada channel 5 ataupun channel 7.



Graphical representation of Wi-Fi channels in the 2.4-GHz band



Spectral mask for 802.11b/g in the 2.4-GHz band

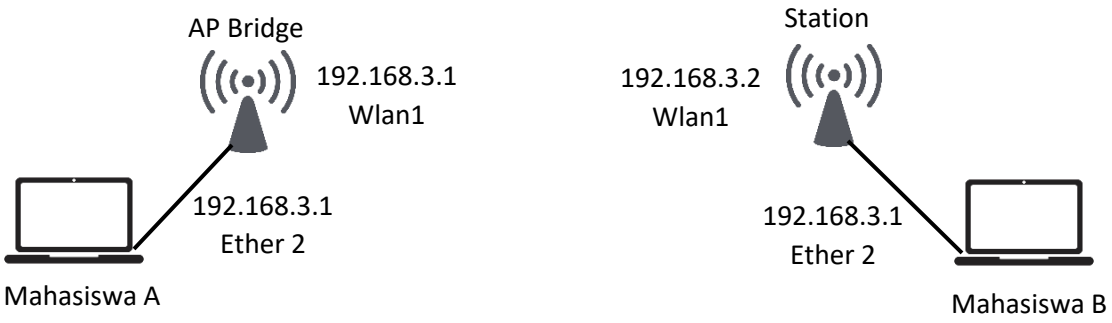
Sehingga untuk penggunaan secara praktis dilapangan berlaku aturan +5 atau -5 pada saat akan menggunakan sebuah frekuensi atau channel. Aturan ini dapat dijadikan pedoman untuk menghindari overlap (interferensi) frekuensi antara satu access point dengan access point lainnya.

Contoh kasus yang tadi jika access point menggunakan channel 6 maka dengan prinsip +5 dan -5, maka anda sebaiknya menggunakan channel 1 (karna 6 – 5 = 1) atau channel 11 (karna 6 + 5 = 11) pada access point anda.

3.3. Koneksi Wireless + LAB

Koneksi terjadi antara access point (AP) dengan satu atau lebih station. Koneksi terjadi apa bila ada kesamaan SSID dan kesamaan Band. Station secara otomatis akan mengikuti channel frekuensi pada AP. Station hanya dapat melakukan scan AP dengan list channel frekuensi yang di set pada station.

Buatlah koneksi antara access point dan client berpasangan antar mahasiswa.

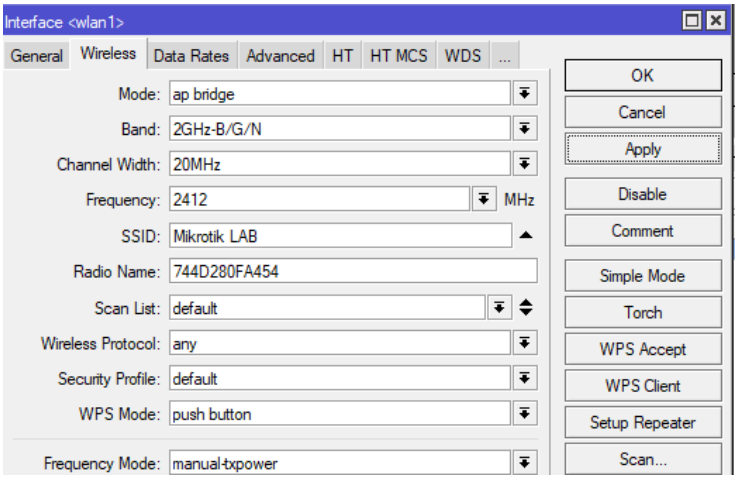


Skenario :

Menghubungkan antara laptop mahasiswa A dengan laptop mahasiswa B melalui jaringan wireless yang terdapat pada MikroTik. IP yang digunakan setiap access point adalah static.

Pembahasan :

Konfigurasi Mikrotik sebagai AP Bridge :

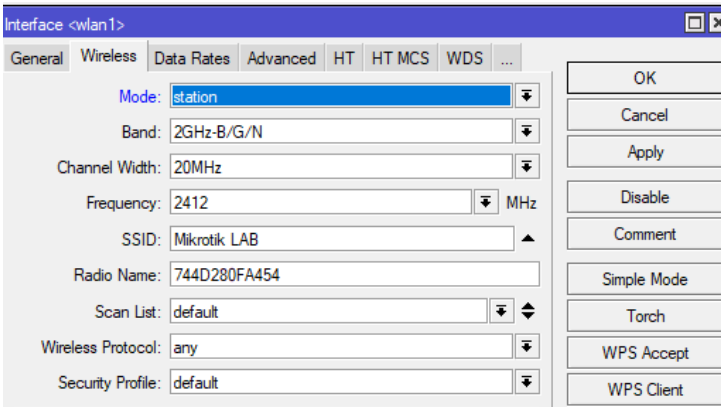


Ingat !!

Mode AP Bridge adalah mode wireless yang difungsikan sebagai Access Point

- Konfigurasi Interface wireless
  - Mode = AP Bridge
  - Band = 2 GHz-B/G/N
  - Frekuensi = 2412
  - SSID = Mikrotik LAB
  - Security Profile = Default
- Tambahkan IP address wlan1 = **192.168.3.1**

Konfigurasi Mikrotik Sebagai Station :



Ingat!!

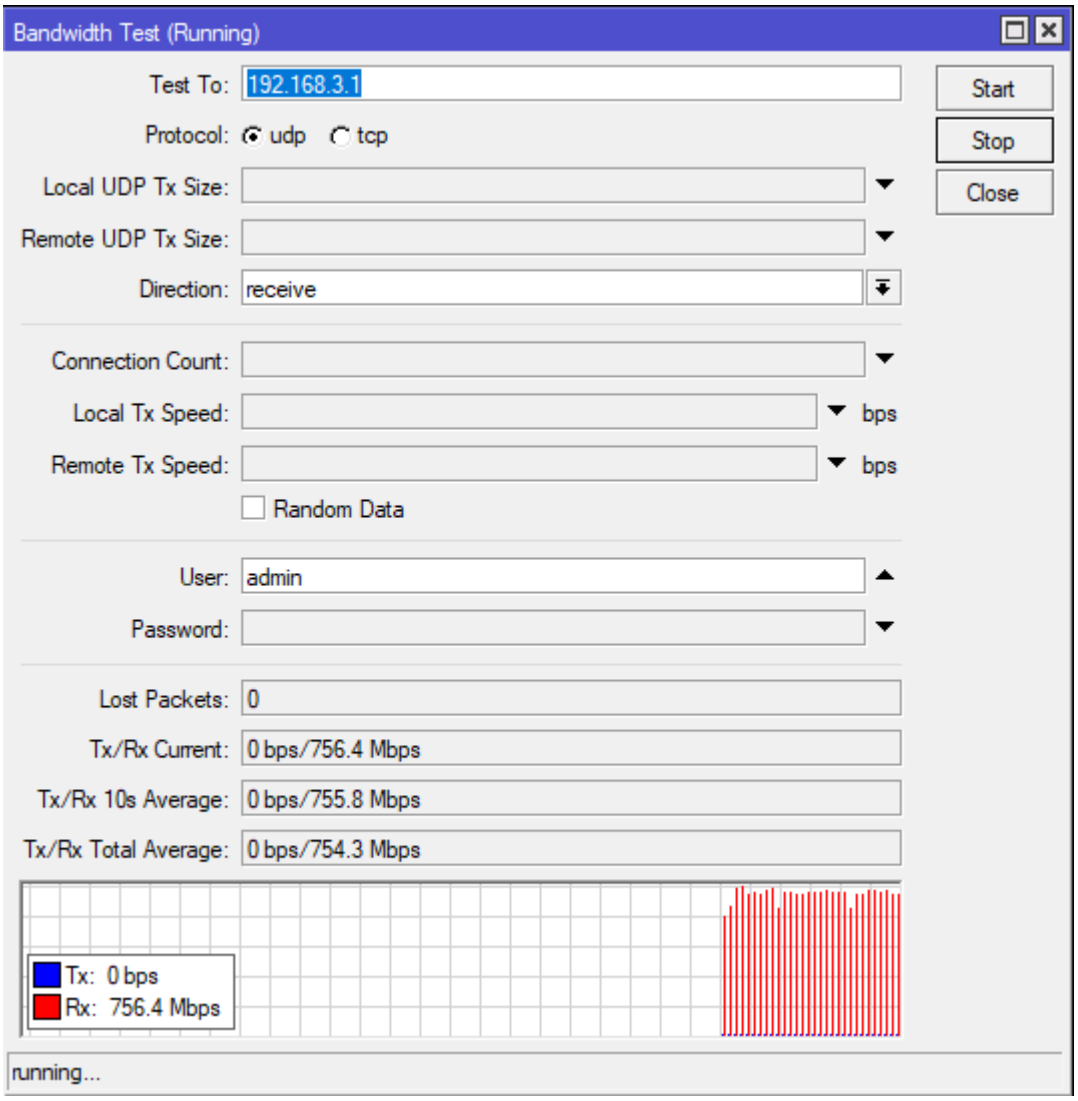
Mode Station digunakan untuk menangkap wireless yang diberikan oleh Access Point

- Konfigurasi interface sama dengan AP Bridge
- Tambahkan IP address wlan1 = **192.168.3.2**

Pengujian

```
[admin@MikroTik] > ping 192.168.3.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.3.1                                56  64 0ms
    1 192.168.3.1                                56  64 0ms
    2 192.168.3.1                                56  64 0ms
    3 192.168.3.1                                56  64 0ms
    4 192.168.3.1                                56  64 0ms
    sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

- Lakukan ping antar mahasiswa menggunakan terminal di MikroTik, pastikan reply bukan time out
- Cobalah menggunakan tool freq. usage dan snooper untuk mencari signal frekuensi yang maksimal (ccq tertinggi).
- Lakukan test ping dan bandwidth menggunakan Tools -> Bandwidth



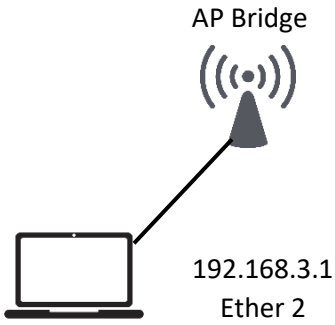
3.4. Virtual Access Point + LAB

Virtual access point akan menjadi cabang dari wlan (interface real), dan dapat di set dengan SSID yang berbeda, namun menggunakan frekuensi dan band yang sama dengan wlan induk.

Virtual Access Point bersifat sama seperti AP yaitu :

1. Dapat dikoneksikan dengan station/client
2. Dapat difungsikan sebagai DHCP Server
3. Dapat difungsikan sebagai Hotspot Server

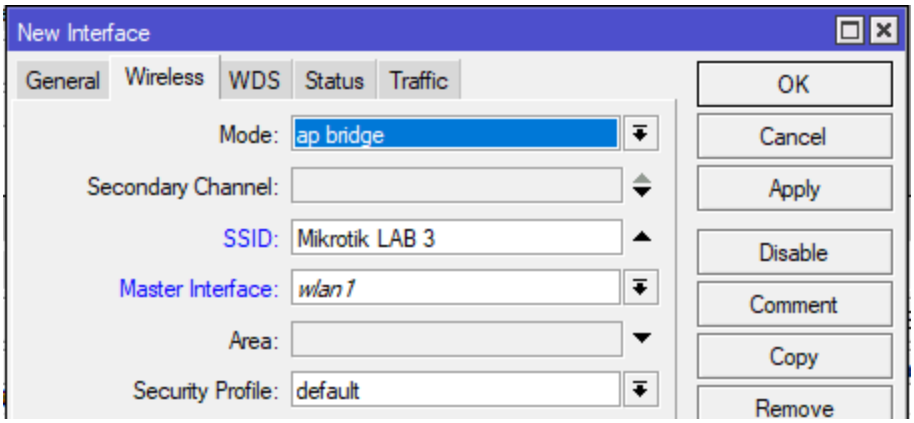
Skenario :

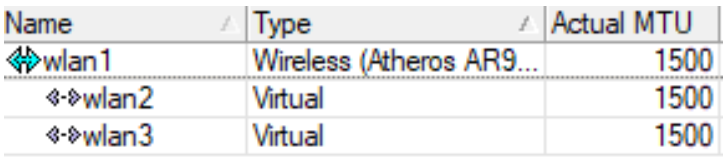


Int Name	Type	IP Address	SSID
Wlan1	Wireless	192.168.3.xxx	Mikrotik LAB
Wlan2	Virtual AP	192.168.4.xxx	Mikrotik LAB 2
Wlan3	Virtual AP	192.168.5.xxx	Mikrotik LAB 3

Pembahasan :

1. Wireless -> Add Virtual -> tab wireless -> Advanced Mode -> ubah SSID seperti pada table address diatas. Lakukan langkah yang sama pada vitual AP selanjutnya.





2. Jika sudah terbentuk seperti diatas ini, maka selanjutnya menambah ip address dimasing-masing interfacenya.

Pengujian

- Gunakan tool scanning dan snooper dari router mahasiswa lain untuk mengamatinya.

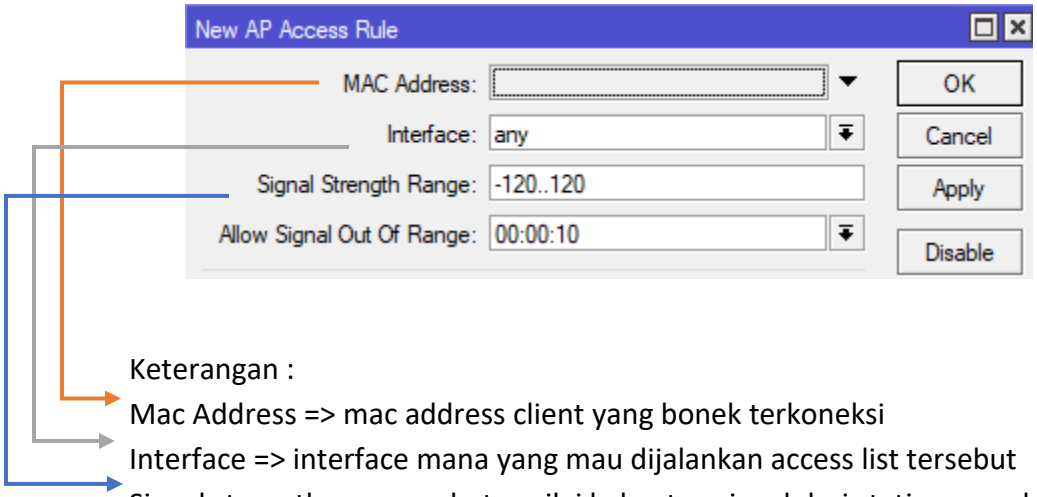
1. Access List dan Connection List

Untuk keamanan koneksi wireless terdapat salah satu fitur mikrotik yang dapat melakukan filtering mac address

- **Pada mode access point,** pembatasan hak akses dapat dilakukan dimana access point hanya dapat dikonek oleh station yang sudah di daftarkan di access list
- **Pada mode station**, agar tidak tertipu dengan SSID access point yang sama, dapat di lock dengan MAC Address filtering (Connect list)

3.1.1. Access List

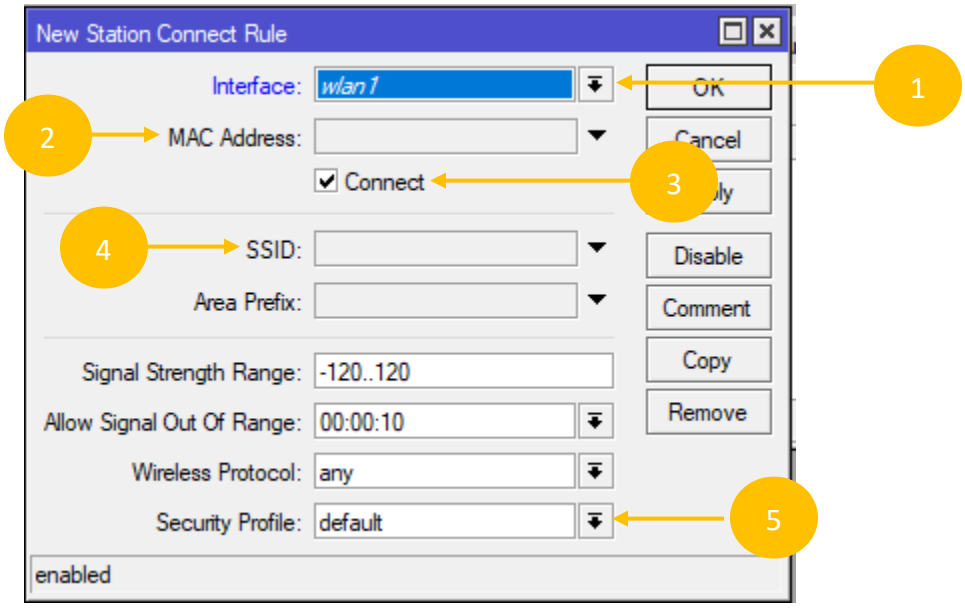
Access list mengatur client/station mana saja yang boleh atau tidak boleh terkonesi dengan interface wireless pada suatu AP.



Keterangan :
Mac Address => mac address client yang bonek terkoneksi
Interface => interface mana yang mau dijalankan access list tersebut
Signal strength range => batas nilai kekuatan signal dari station yang boleh terkoneksi

3.1.2. Connection List

Connect list membatasi access point mana saja yang boleh/tidak boleh dikoneksikan oleh interface wireless suatu station



Keterangan :

1. Interface yang di fungsikan sebagai client
2. Mac Address AP yang akan di koneksikan
3. Kondisi enable/disable, jika di enable maka boleh terkoneksi dengan MAC Address diatas.
4. SSID yang ingin dikoneksikan, bila kosong berari any access point
5. Security profile, jika menggunakan fitur ini harus di apply di rule connection list

3.5.3. Registration List

Untuk mempermudah memasukkan informasi AP atau station kedalam access point maupun connection list

BAB IV
BRIDGE

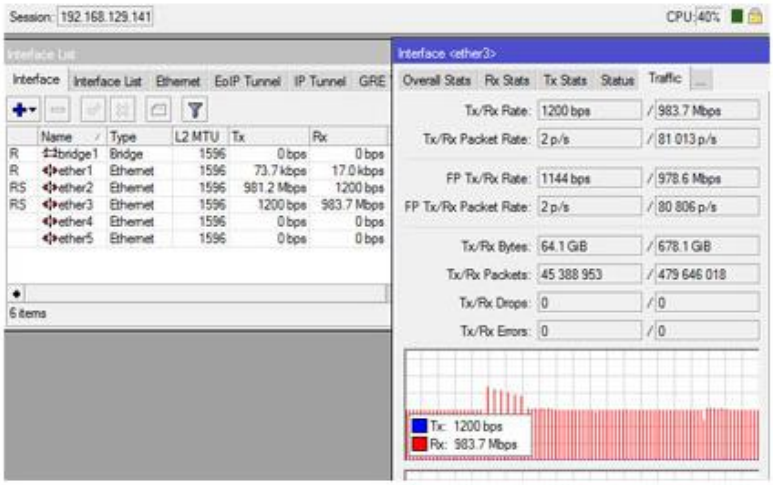
4.1 Perbedaan Bridge dan Switch

1. Bridge

   Hampir mirip dengan switch, kita bisa menggabungkan beberapa interface yang berbeda menjadi satu segmant dengan menggunakan teknik bridging. Membuat beberapa interface seolah-olah menjadi satu artinya adalah tidak ada perbedaan segmen jaringan didalamnya. Misal, kedua interface ethernet dibridge maka kedua interface tersebut akan menangani jaringan yang sama. Kita juga bisa melakukan bridging antara interface ethernet dengan wireless yang mana hal tersebut tidak bisa dilakukan dengan metode switching. Artikel mengenai cara setting brigde pada Mikrotik dapat kita lihat disini. Teknik bridge bisa dilakukan di semua produk Mikrotik baik routerboard maupun PC.

   Dengan menggunakan mode bridge kita dapat menanggulangi network loop dengan mudah, yakni menggunakan protocol STP (Spanning Tree Protocol) dan RSTP (Rapid Spanning Tree Protocol).

   Namun dengan menggunakan teknik bridge ini kita bisa memoritoring trafik antar port. Ada 4 jenis ethernet yang dapat dijadikan bridge port yakni Ethernet, Vlan, Wireless, VPN (mengaktifkan BCP), dan Tunnel (EoIP). Karena teknik bridge ini bekerja dilevel software, maka paket data yang masuk akan terbaca di prosessor sehingga menyebabkan CPU-Loadnya akan naik. Kita akan melakukan pengetesan untuk mengetahui CPU Load-nya. Berikut hasilnya



Gambar 4.1 Trafik CPU proses Bridge

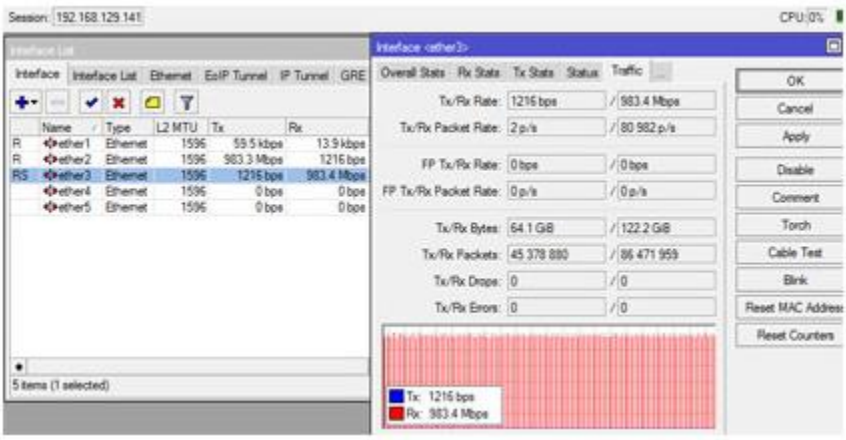
Dari hasil diatas terlihat bahwa dengan melewatkan trafik yang cukup tinggi maka CPU Load-nya naik menjadi 40%. Hal ini terjadi karena mode bridge untuk prosesnya dilakukan di CPU.

2. Switch

Pada umumnya RouterBoard memiliki beberapa interface ethernet. Walaupun interface-interface tersebut merupakan interface router yang setiap interfacenya harus terhubung ke jaringan yang berbeda-beda. Namun, interface tersebut dapat difungsikan sebagai port switch.

Untuk menghubungkan beberapa port ethernet, dibutuhkan hardware khusus yakni switch chip yang ditanam di routerboard. Sebuah routerboard bisa difungsikan sebagai switch bila didalam router tersebut sudah terpasang switch-chip. Switch-chip mampu melakukan forwarding frame ethernet secara full duplex dan independen tanpa membebani prosesor di Router.

Terdapat berbagai macam jenis Switch chip yang ada pada routerboard. Walaupun sama-sama memiliki fungsi switch, namun masing-masing memiliki fitur yang berbeda-beda. Fungsi switch hanya bisa melakukan penggabungan ethernet interface selama ethernet tersebut masih dalam satu switch chip yang sama. Artikel mengenai switch-chip pada routerboard sudah pernah kita bahas disini. Dengan fungsi port switching ini memungkinkan melakukan tranfer data dengan kecepatan penuh diantara sekelompok port. Namun kelemahannya, kita tidak bisa memonitoring trafik antar port yang masih dalam satu switch. Kita telah melakukan pengetesan untuk mengetahui penggunaan CPU Load bila menggunakan teknik switch ini. Lalu bagaimana hasilnya? Berikut hasil pengetesan yang sudah dilakukan



Gambar 4.2 Trafik CPU proses Switch

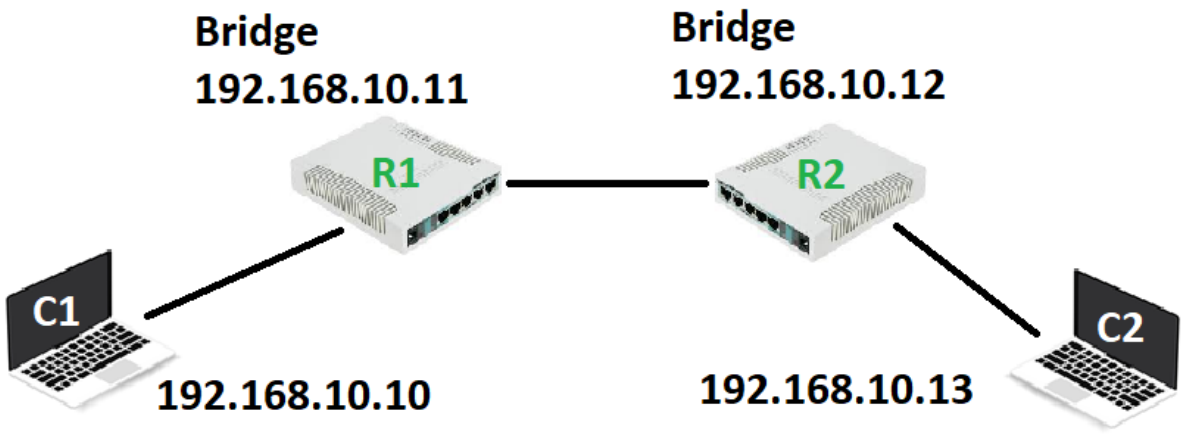
Terlihat bahwa CPU Load-nya 0%. Kenapa bisa begitu? karena proses switching terjadi dilevel hardware yakni pada switch-chip yang tertanam di routerboard sehingga tidak membebani prossesor.

Sangat mudah untuk membangun jaringan bridge/switch tetapi masalah juga sering terjadi. Beberapa masalah kadang terjadi pada jaringan yang bersifat bridge/switch, misal :

a. Permasalahan pada host di dalam segmen akan berimbas ke host lain di bridge yang sama (mis: ip conflict, netcut, DHCP tandingan dll)

b. Sulit untuk membuat fail over system

4.2 Lab – Bridging



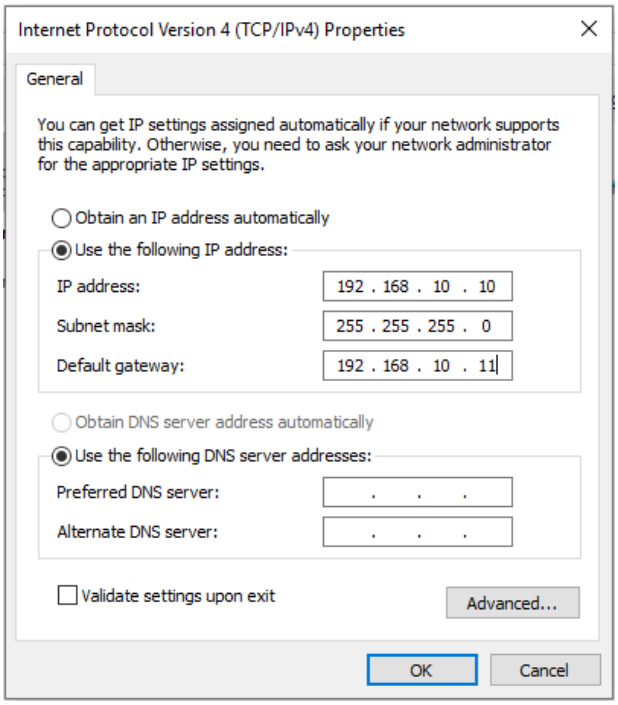
Gambar 4.3 Lab Bridge

Terdapat sebuah Skema dimana C1 memili sebuah IP 192.168.10.10 yang terhubung dengan Ether2 Router Mikrotik R1 dan pada Ether1 Router Mikrotik R1 terhubung dengan Ether1 Router Mikrotik R2 lalu C2 memili sebuah IP 192.168.10.13 yang terhubung dengan Ether2 Router Mikrotik R2.

Buatlah sebuah Bridging agar pada skema tersebut dapat berjalan dengan netwok yang sama antara LAN R1 dan LAN R2?

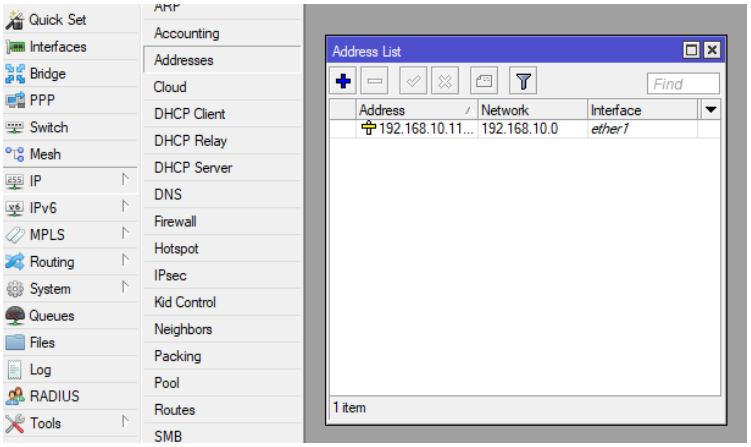
Untuk melakukan LAB Bridging maka harus melakukan konfigurasi percobaan pada LAN R1, Berikut Percobaan pada LAN RI koneksikan C1 pada Port Ether2 R1 lalu lakukan langkah-langkah sebagai berikut:

1. Setting IP Client C1



Gambar 4.4 Setting IP C1

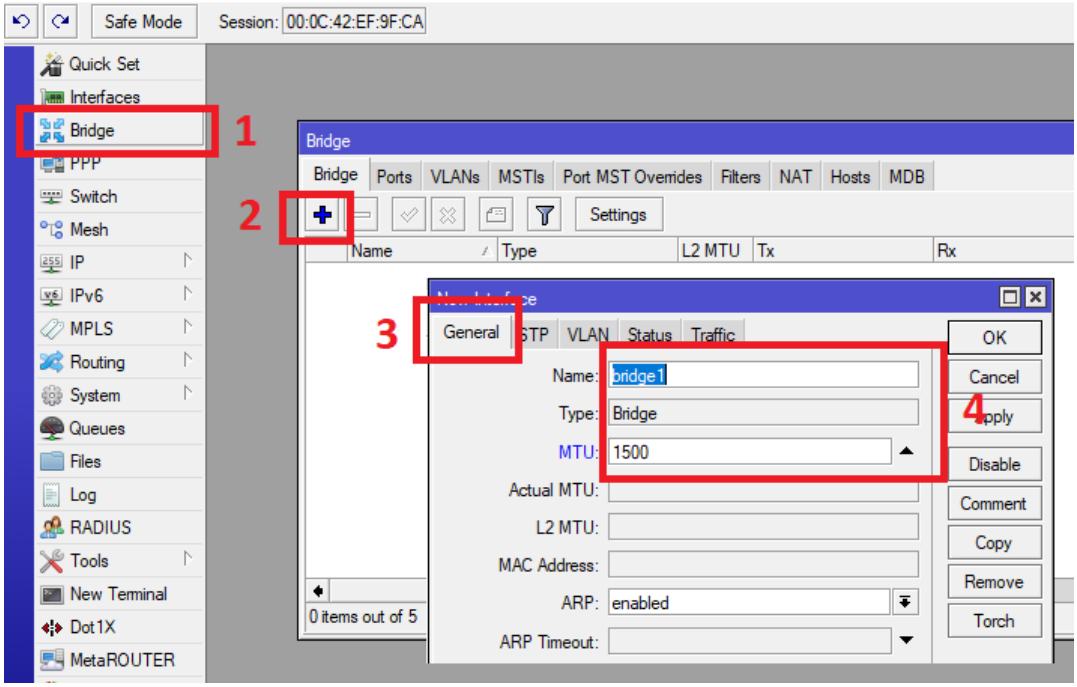
2. Setting Router Mikrotik R1



Gambar 4.5 Setting IP pada Ether1 R1

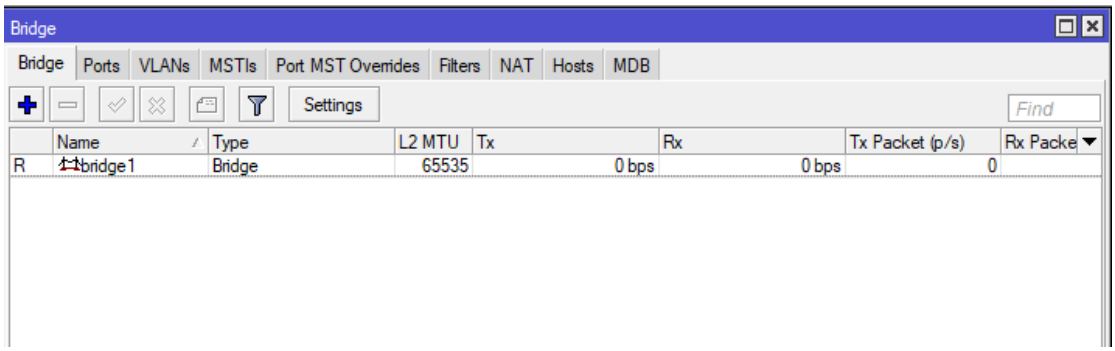
Masukan IP 192.168.10.11/24 pada ether1 R1 sehingga router ether 1 memiliki IP dengan network 192.168.10.0/24.

3. Setting Bridge Router R1



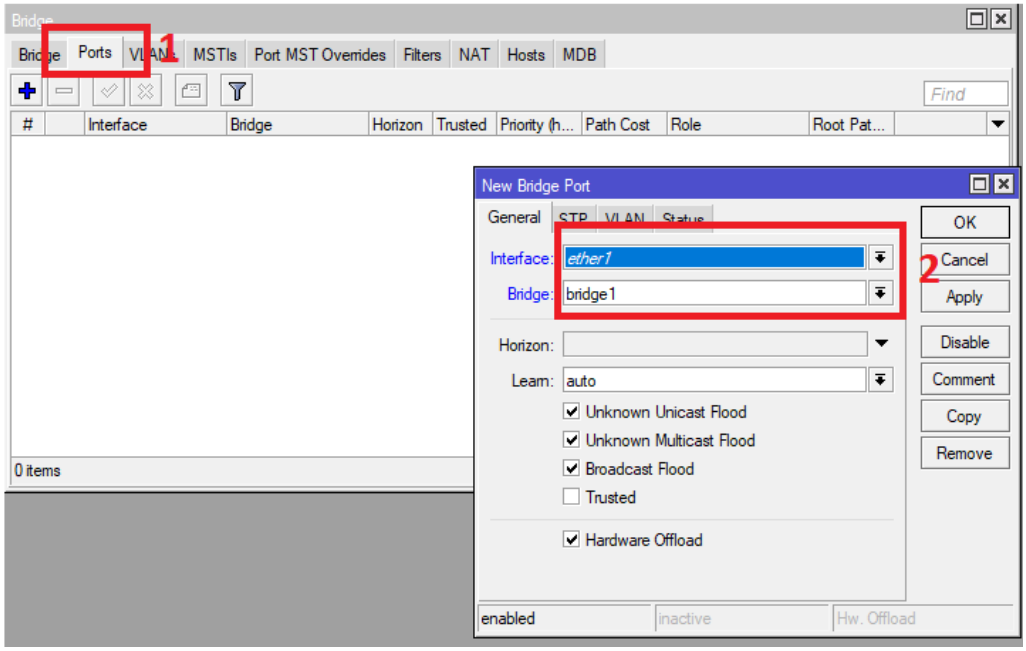
Gambar 4.6 Setting Bridge R1

Pilih menu Bridge => klik + => menu General => isi name = bridge1 “Bebas untuk penamaan”, Type=Brdige, MTU 1500 => Apply => OK



Gambar 4.7 Bridge1 sudah terkonfigurasi

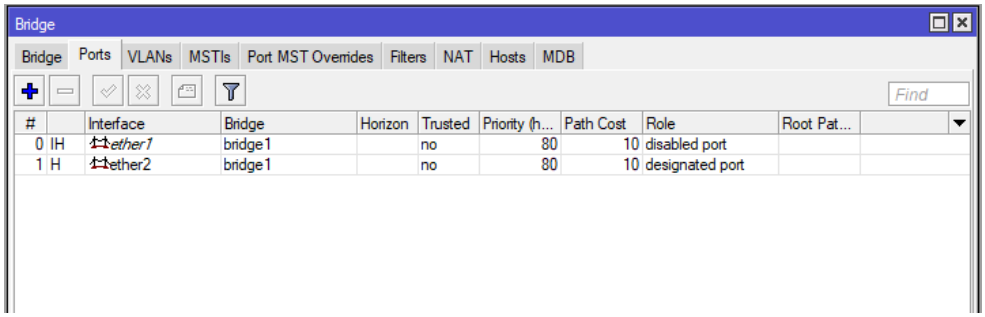
4. Daftarkan Port yang ingin terbridge



Gambar 4.8 Daftarkan Bridge Untuk Masing-masing Ether

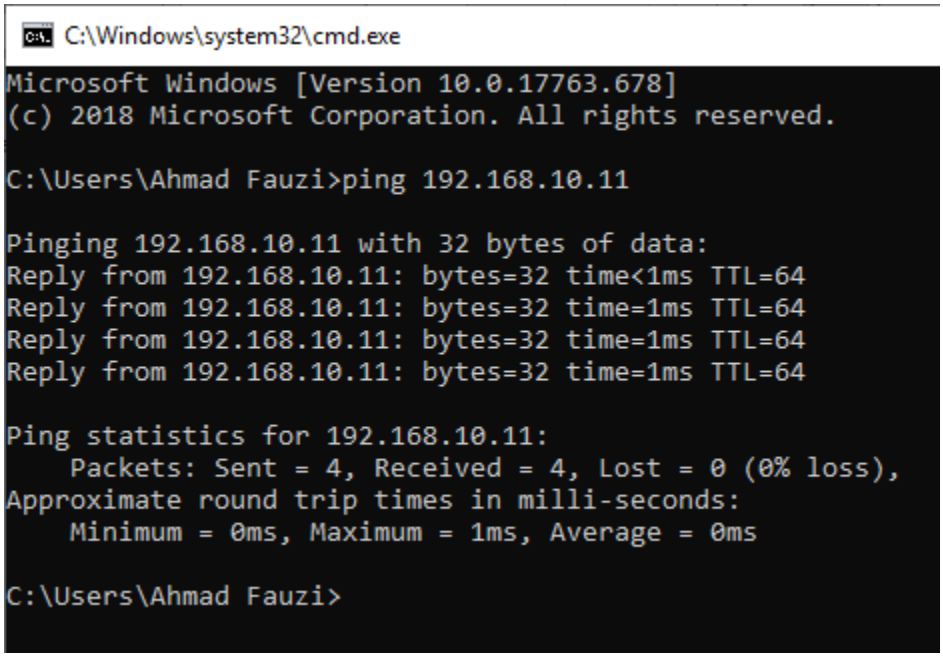
Pilih menu Port => Interface: ether1 “pilih ether yang ingin dibridge” => Bridge: bridge1 => Apply => OK (untuk konfigurasi Ether 1 sebagai brige1)

Pilih menu Port => Interface: ether2 “pilih ether yang ingin dibridge” => Bridge: bridge1 => Apply => OK (untuk konfigurasi Ether 2 sebagai bdrige1)



Gambar 4.9 List Ether yang sudah terdaftar pada bridge1

5. Ping C1 ke IP 192.168.10.11

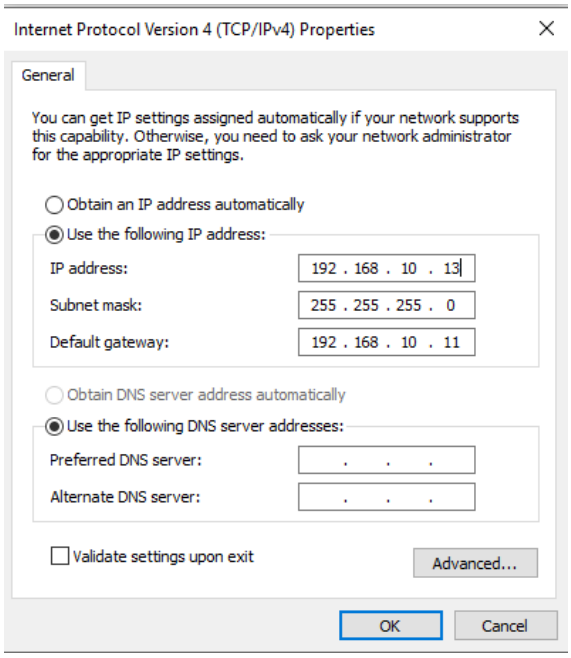


Gambar 4.10 Ping C1 Ke Ether2 R1

Pada percobaan tersebut didapatkan hasil bahwa C1 dapat melakukan PING ke IP 192.168.10.11 yang pada hakikatnya terdapat pada ether1 R1 sehingga bilamana tidak menggunakan Bidge maka C1 tidak akan dapat terkoneksi dengan Ether1 dengan network yang sama

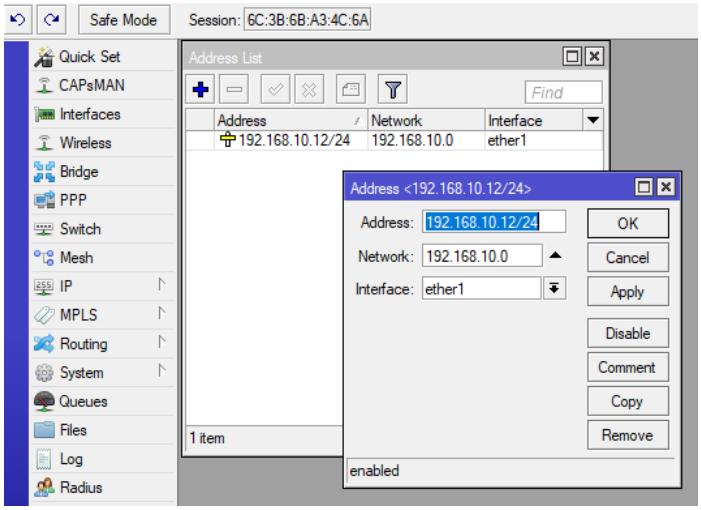
Percobaan pada LAN 1 sudah berhasil dilakuka lalu kofigurasi pada LAN 2 R2 sebagai berikut:

1. Setting IP Client 2



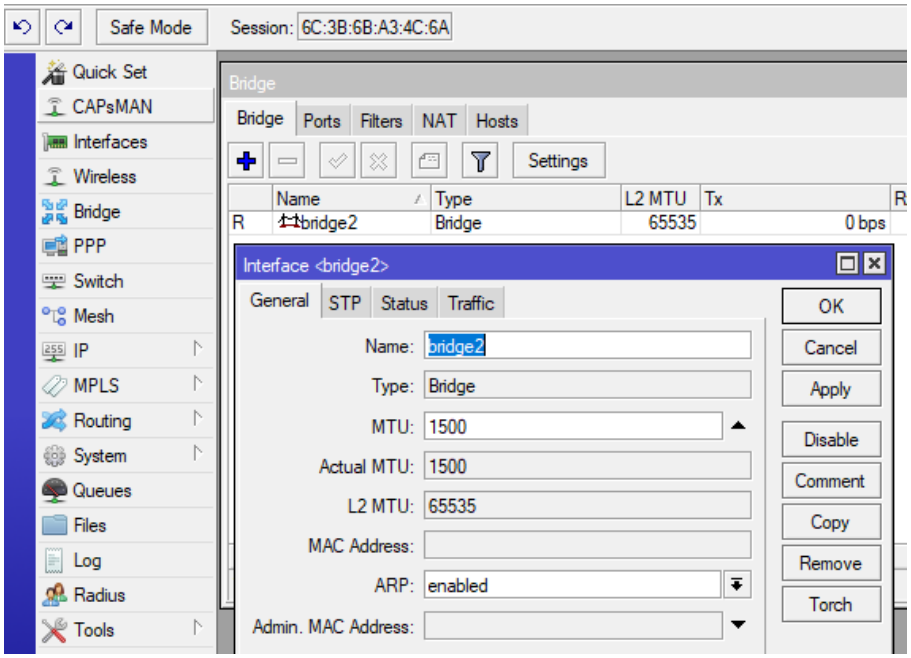
Gambar 4.11 Setting IP C2

2. Setting Router Mikrotik R1



Gambar 4.12 Setting IP pada Ether1 R2

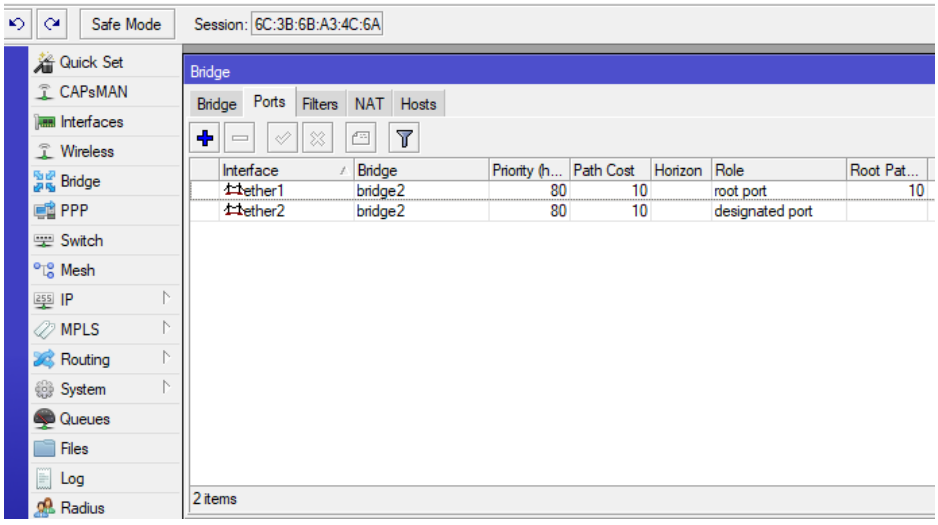
3. Setting Bridge Router R1



Gambar 4.13 Setting Bridge R1

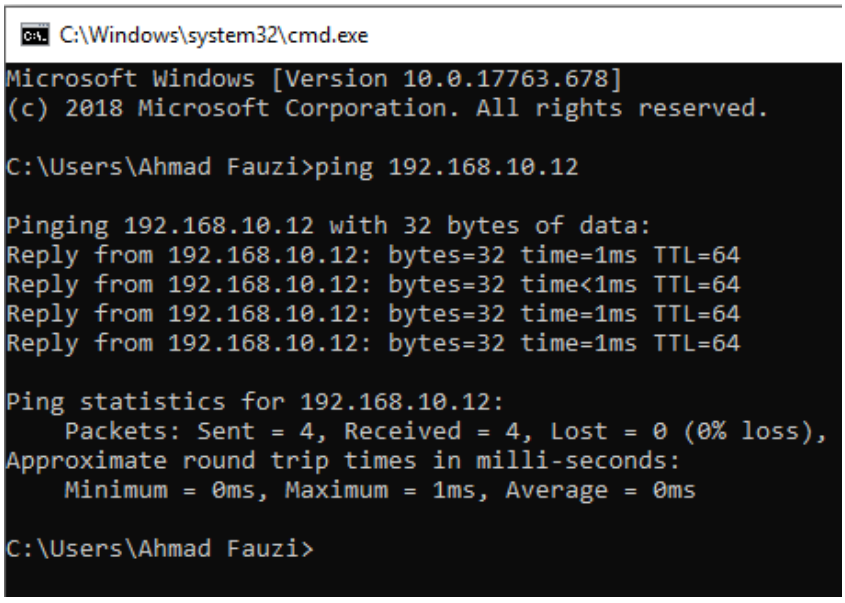
Pada konfigurasi bridge R2 untuk nama bridge kita gunakan nama yang beda yaitu bridge2

4. Daftarkan Port yang ingin terbridge



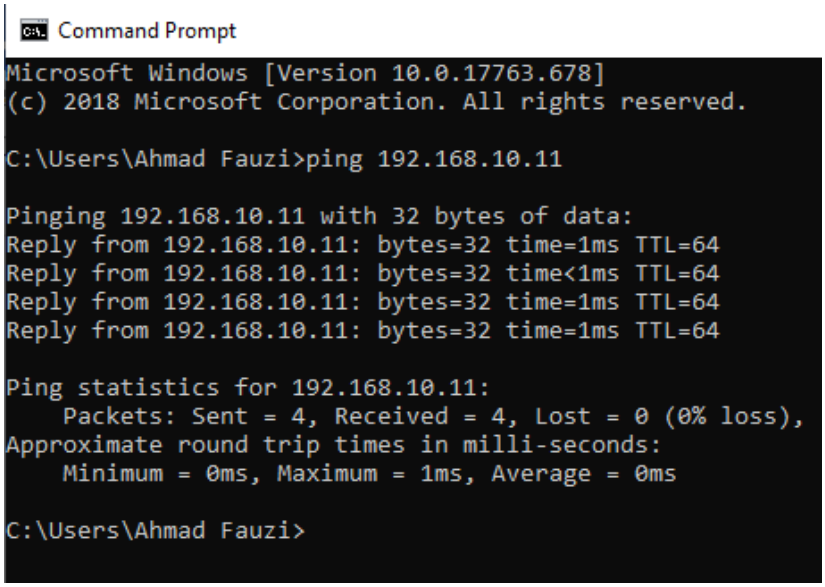
Gambar 4.14 List Ether yang sudah terdaftar pada bridge2

5. Ping C2 ke IP 192.168.10.12



Gambar 4.15 Ping C2 Ke Ether2 R2

6. Ping C2 ke IP R1 192.168.10.11



Gambar 4.16 Ping C2 Ke Ether2 R1

Pada keterangan tersebut sudah dapat disimpulkan bahwa network LAN 1 dan LAN 2 sudah terkoneksi dengan network yang sama yaitu 192.168.10.0/24 yang dengan metode bridge dapat mengkoneksikan antar ether dengan menggunakan 1 IP atau 1 network.

BAB V
ROUTING

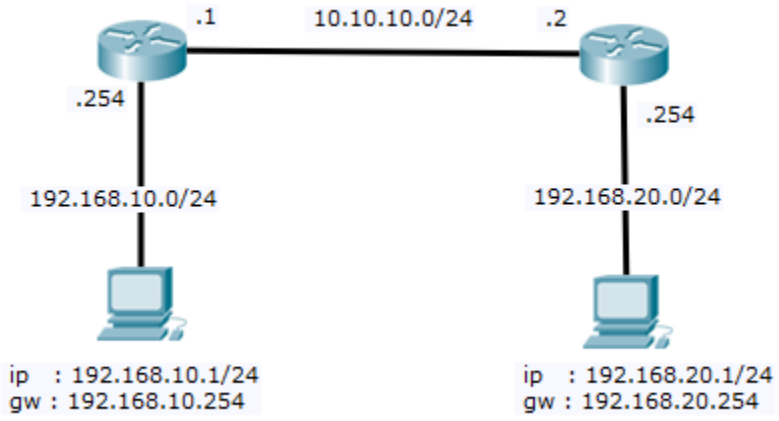
Routing adalah suatu cara agar menentukan alamat jaringan yang berbeda segment ip address dapat saling terhubung. Routing juga dapat diartikan sebagai sebuah proses untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya sehingga menjadi rute tertentu. Routing memiliki dua jenis yaitu routing statis dan dinamis.

5.1. Routing Statis (Static Routing)

Routing statis digunakan untuk model jaringan skala yang kecil yang dapat terdiri dari kurang lebih satu sampai dengan lima router. Proses routing ini dengan memasukan alamat alamat tujuan router yang ingin di capai. Untuk lebih memahami metode routing ini maka dapat digunakan rumus :

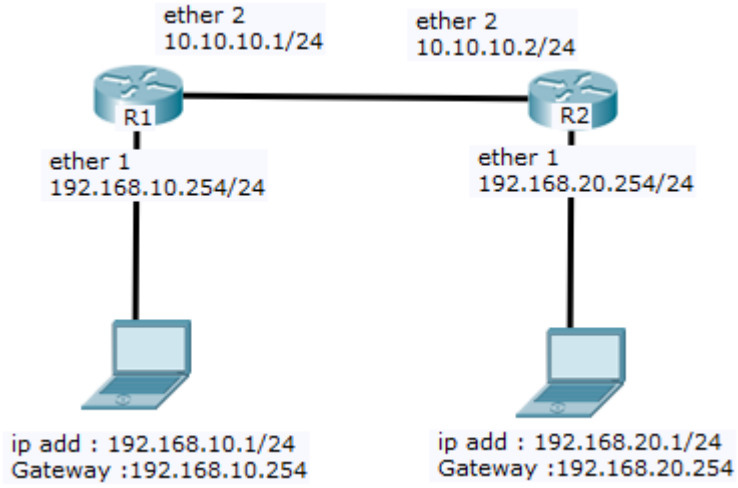
DARI MANA – MAU KEMANA – LEWAT MANA

Sebagai contoh perhatikan topologi dibawah ini :



Gambar 5.1 Rute Routing

Apabila pc dengan ip 192.168.10.1 **(dari mana)** ingin ke tujuan 192.168.20.1 **(mau kemana)** maka jalur yang dipilih sebagai routing adalah 10.10.10.2 **(lewat mana).**untuk menerapkan topologi diatas pada router mikrotik maka kedua router tersebut harus dikonfigurasi. Perhatikan topologi yang harus dibuat seperti dibawah ini bahwa untuk alamat ip address dengan alamat gateway harus merupakan ip address yang satu segment alias peer to peer.

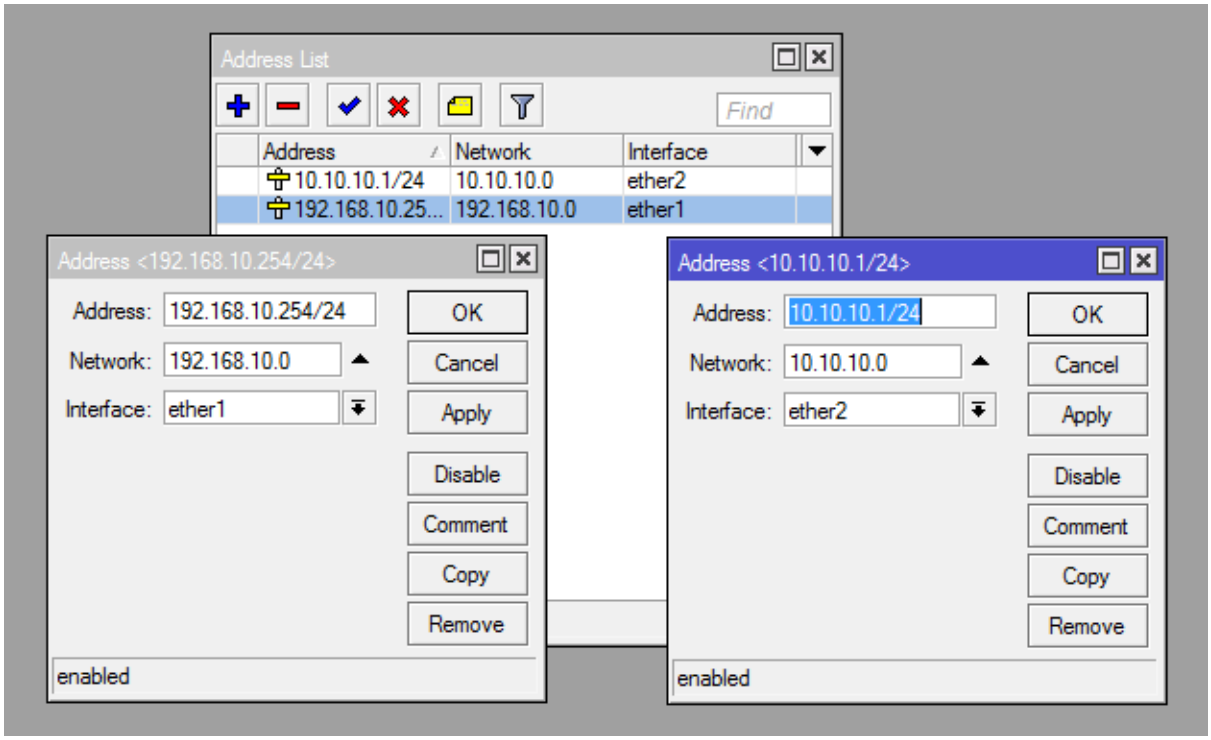


Gambar 5.2 Topologi Routing

Login ke dalam winbox dan berikan ip address pada masing masing router. Untuk memberikan ip address pada R1 dengan perintah berikut.

```
[admin@R1] ip address add address=192.168.10.254/24 interface=ether1
[admin@R1] ip address add address=10.10.10.1/24 interface=ether2
```

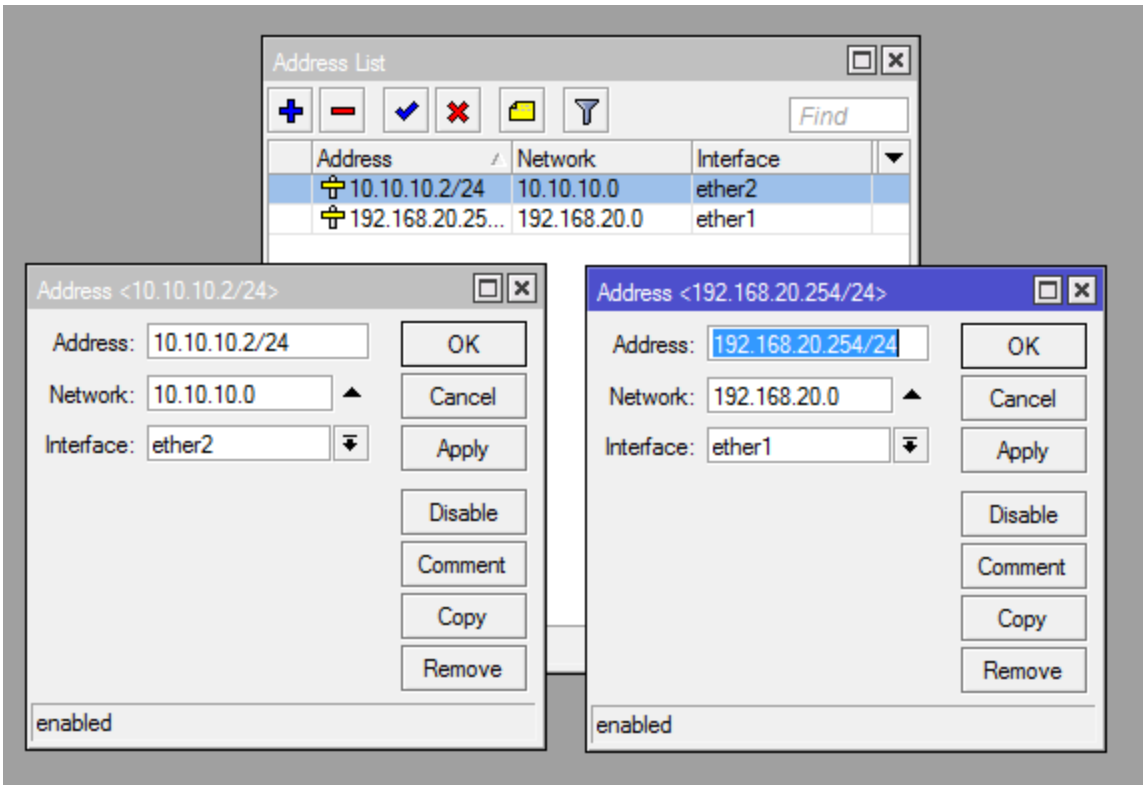
Dedangkan pada winbox terdapat pada menu **IP – ADDRESS -ADD (+)**



Gambar 5.3 IP Routing R1

Lakukan hal yang sama terhadap router R2. Perhatikan kembali untuk ip address yang diberikan beserta port ether yang mengarah ke router sebelah ataupun kearah PC client.

```
[admin@R2] ip address add address=192.168.20.254/24 interface=ether1
[admin@R2] ip address add address=10.10.10.2/24 interface=ether2
```

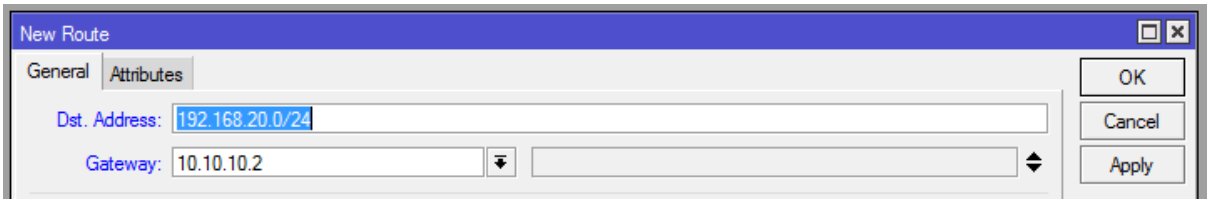


Gambar 5.4 IP Routing R2

Setelah memasukan ip address langah selanjutnya adalah melakukan routing. Routing statis pada mikrotik dapat di masukan dengan perintah berikut :

```
[admin@R1] ip route add dst-address=192.168.20.0/24 gateway=10.10.10.2
```

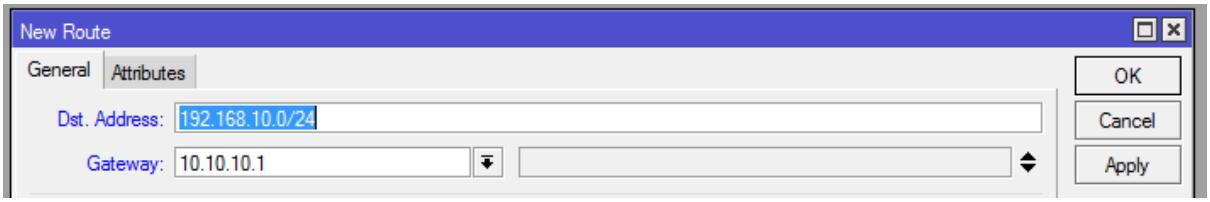
Konfigurasi dilakukan dengan menggunakan winbox pada menu IP – route -add (+). Masukan alamat tujuan pada kolom dst-address dan gateway yang dapat dilalui dengan 10.10.10.2



Gambar 5.5 Konfigurasi routing R1

Pada router R2 juga harus dilakukan konfigurasi dengan memasukan dst-address dan gateway yang ada pada router R1

```
[admin@R2] ip route add dst-address=192.168.20.0/24 gateway=10.10.10.2
```

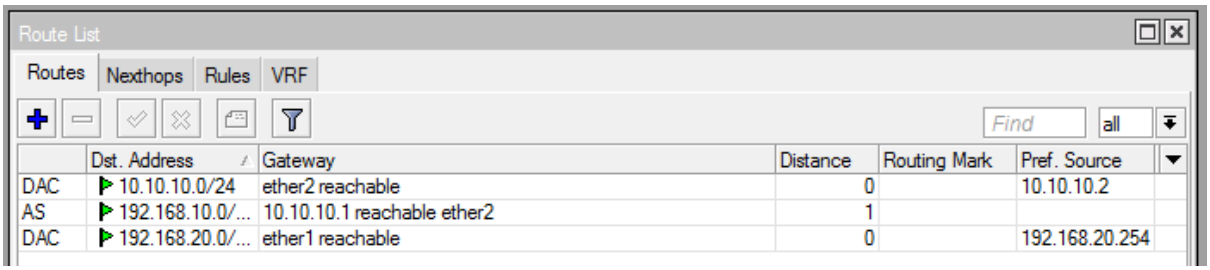


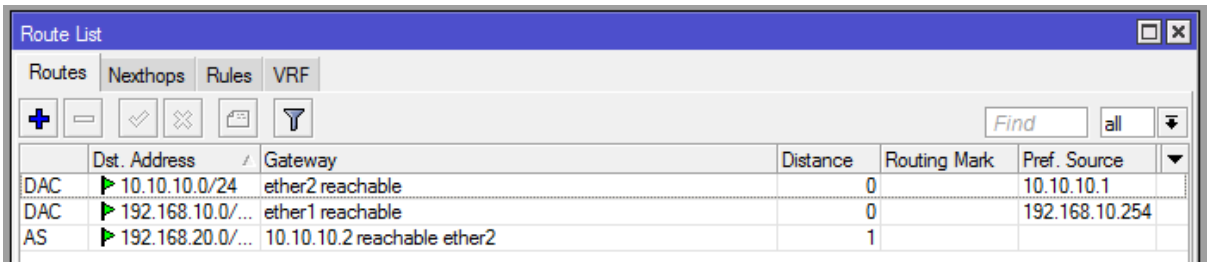
Gambar 5.6 Konfigurasi routing R2

Setelah konfigurasi routing statis selesai pada kedua router maka dapat dilihat pada routing tabel yang telah terbentuk. Routing statis dapat ditandai dengan label AS (Active Static). Perintah tyang digunakan pada terminal router adalah

```
[admin@R1] ip route print
```

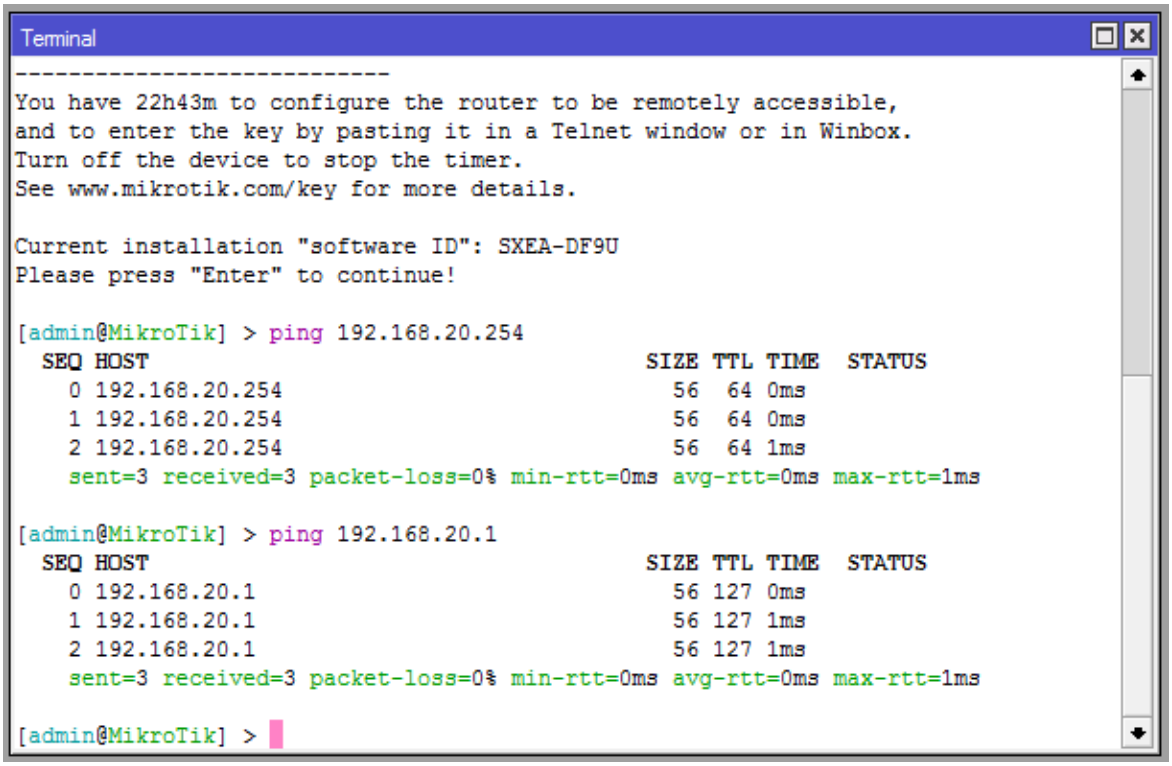
Untuk tampilan pada winbox akan terbentuk tabel routing pada kedua router seperti berikut ini :





Gambar 5.7 Routing Table

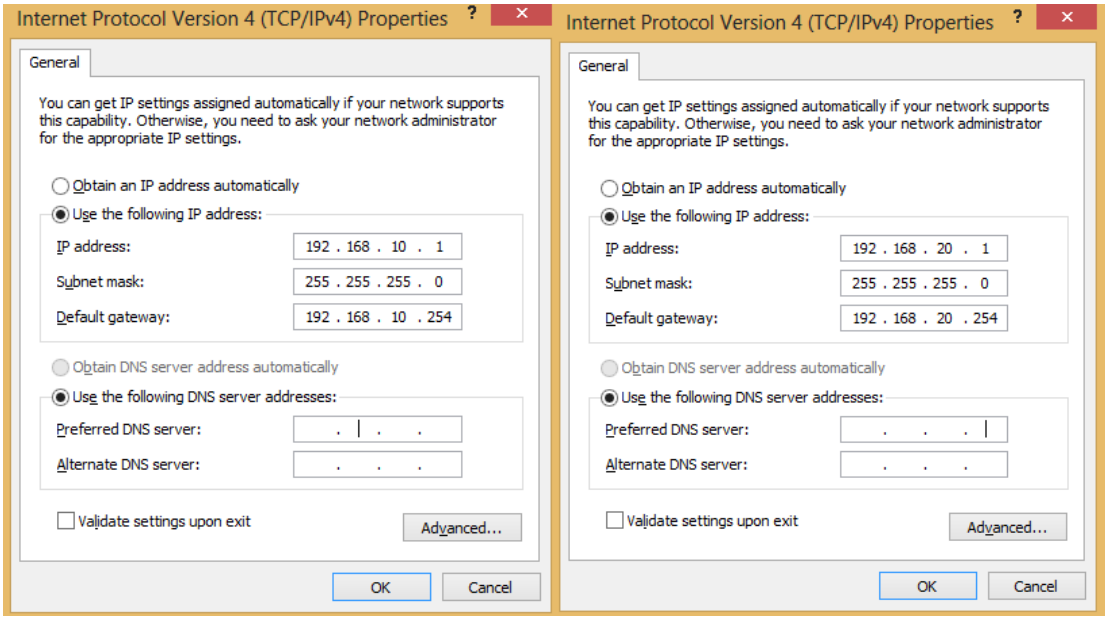
Untuk memastikan jaringan routing kita sudah dapt bekerja dan berkomunikasi antar segment jaringan yang berbeda maka langkah pengujian adalah dengan mencoba ping pada masing masing router tersebut kearah router tetangga maupun ke komputer host bagitu sebaliknya



Gambar 5.8 Uji koneksi

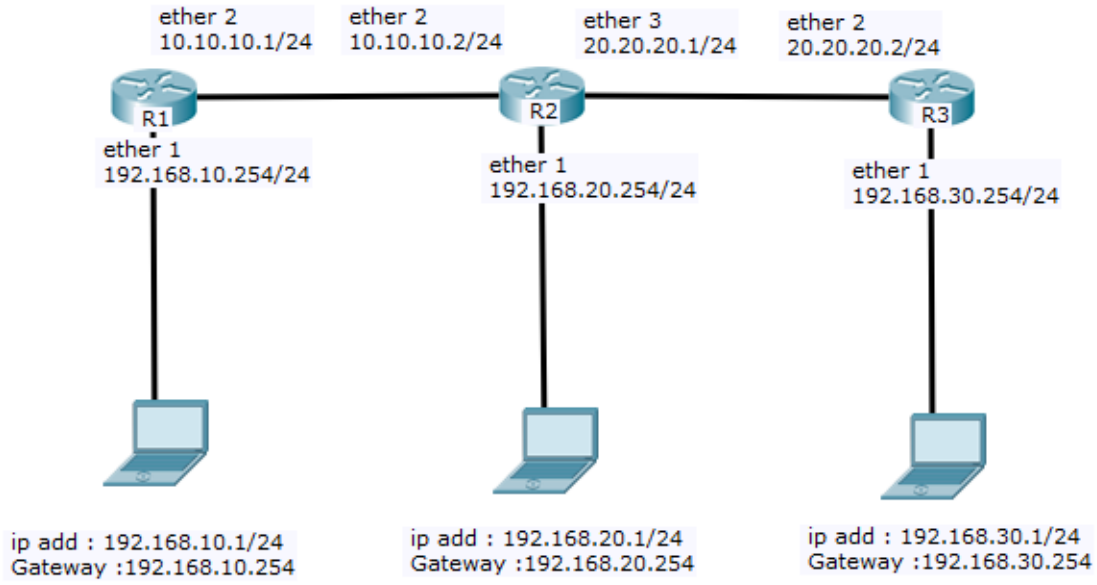
Apabila terjadi kesalahan pada proses ping seperti RTO (riquest time out) maka dapat dilakukan pengecekan pada masing masing pc client yang terhubung apakah sudah memasukan ip

address dan gateway yang sudah benar. Kemudian untuk sementara matikan fungsi firewall yang ada pada pc tersebut.

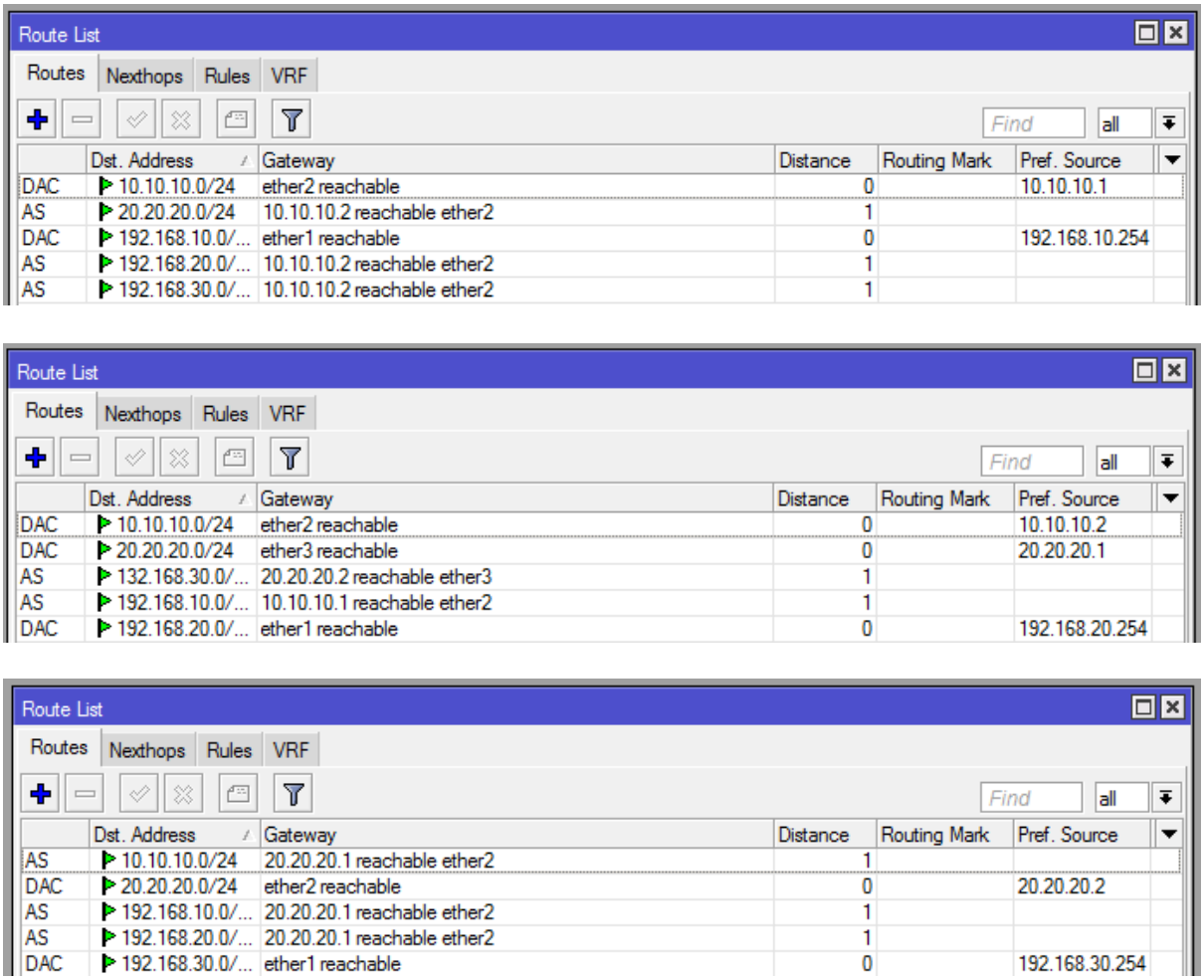


Gambar 5.9 Konfigurasi Ip PC

Buatlah topologi berikut ini dengan menggunakan tiga router. Perhatikan dengan baik port ether dan ip address yang harus digunakan.



Gambar 5.10 Konfigurasi Routing 3 Router



Route List

Routes | Nexthops | Rules | VRF

Find | all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.10.10.0/24	ether2 reachable	0		10.10.10.1
AS	20.20.20.0/24	10.10.10.2 reachable ether2	1		
DAC	192.168.10.0/...	ether1 reachable	0		192.168.10.254
AS	192.168.20.0/...	10.10.10.2 reachable ether2	1		
AS	192.168.30.0/...	10.10.10.2 reachable ether2	1		

Route List

Routes | Nexthops | Rules | VRF

Find | all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.10.10.0/24	ether2 reachable	0		10.10.10.2
DAC	20.20.20.0/24	ether3 reachable	0		20.20.20.1
AS	132.168.30.0/...	20.20.20.2 reachable ether3	1		
AS	192.168.10.0/...	10.10.10.1 reachable ether2	1		
DAC	192.168.20.0/...	ether1 reachable	0		192.168.20.254

Route List

Routes | Nexthops | Rules | VRF

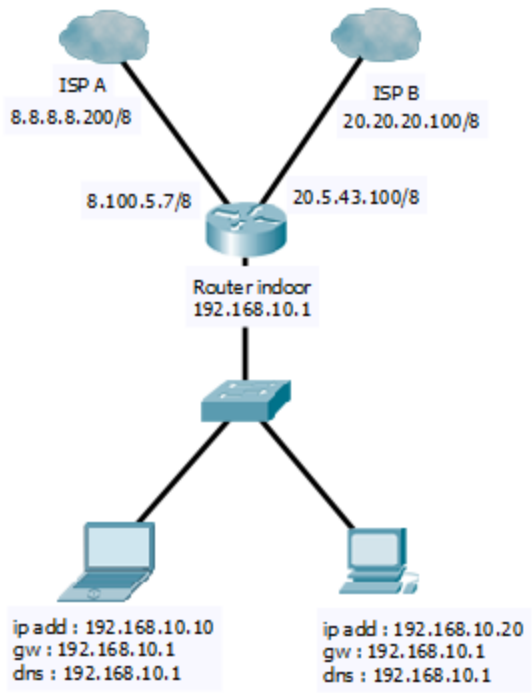
Find | all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	10.10.10.0/24	20.20.20.1 reachable ether2	1		
DAC	20.20.20.0/24	ether2 reachable	0		20.20.20.2
AS	192.168.10.0/...	20.20.20.1 reachable ether2	1		
AS	192.168.20.0/...	20.20.20.1 reachable ether2	1		
DAC	192.168.30.0/...	ether1 reachable	0		192.168.30.254

Gambar 5.11 Tabel Routing 3 Router

5.2 Load Balancing

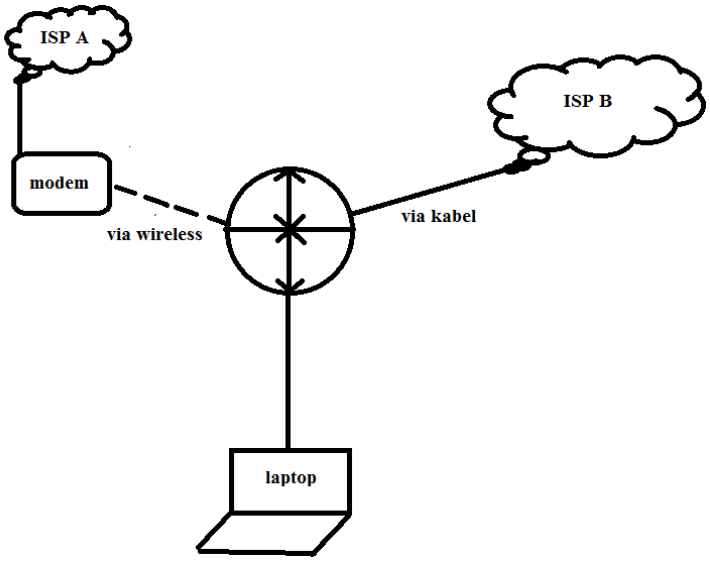
Load balancing adalah suatu metode menggabungkan beberapa link secara bersama sama untuk melewatkan paket data dalam jaringan. Fungsi ini bertujuan untuk memberikan jalur alternative (cadangan) apabila suatu waktu salah satu link terputus maka paket dapat dikirim menggunakan jalur lainnya. Sebagai contoh perhatikan gambar dibawah ini.



Gambar 5.12. Load balancing

Apabila kita ingin mendalami teknik load balancing sebenernya memiliki banyak macamnya seperti interface bonding, NTH, Routing Policy atau ECMP. Namun disini akan dibahas penggunaan load balancing dasar menggunakan ECMP. ECMP sendiri adalah metode load balancing dengan menggunakan aloritma Round Roubin dimana paket yang dikirim dengan menggunakan dua link atau lebih akan diacak dan dipilih salah satu linknya.

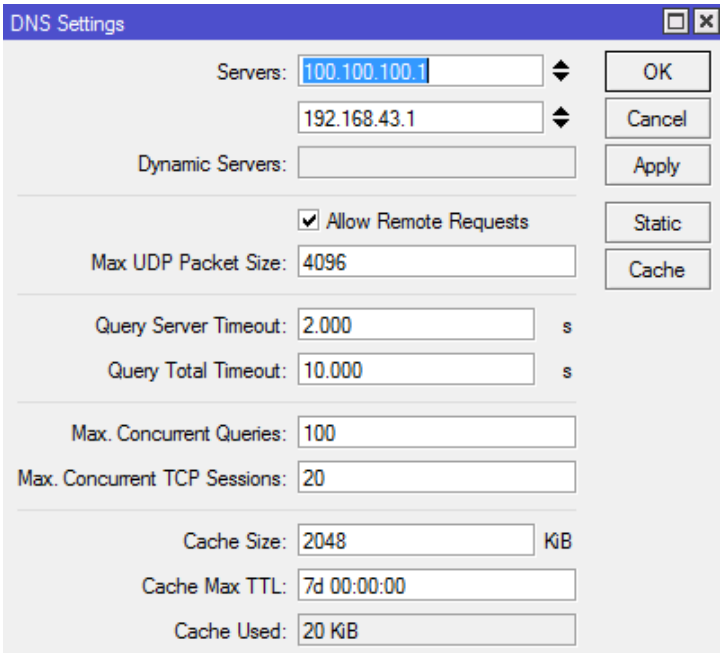
Sekarang perhatikan topologi dibawah ini. Kita akan membuat dua jalur koneksi dengan menggunakan kabel dan wireless. Ip dengan menggunakan kabel diberi secara statik sedangkan ip yang didapat dari wireless juga diberi **statik jangan dibuat manual**. Dengan jalur ini diharapkan apabila salah satu link terputus maka kondisi internet tetap berjalan.



Gambar 5.13. Load balancing ECMP

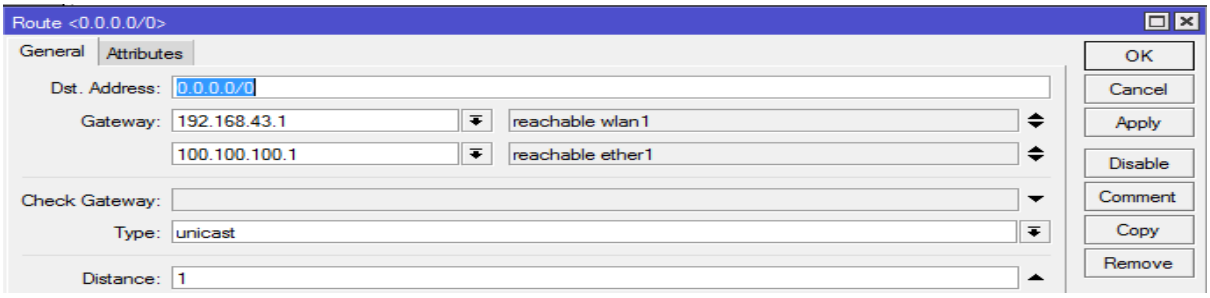
Bila melihat topologi diatas maka kita asusumsikan router yang terkoneksi menggunakan kabel mendapat ip 100.100.100.2/24 sedangkan ip yang menggunakan modem wireless adalah 192.168.43.250/24. Satu lagi kita beri ip address ke arah laptop client adalah 192.168.10.1/24. Masukan semua alamat ini pada router mikrotik baik menggunakan winbox ataupun terminal.

Langkah selanjutnya adalah tambahkan dua DNS pada menu IP-DNS. Pada kolom server masukan ip 100.100.100.1 dan 192.168.43.1. ip ini adalah ip masing masing provider.



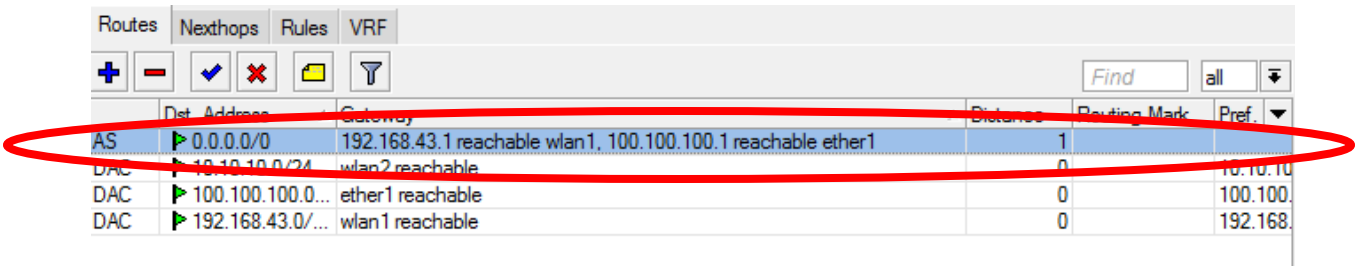
Gambar 5.12 DNS Load balancing

Pada menu IP – Routes buatkan default router yang mengarah ke 0.0.0.0/0 dengan dua buah gateway yang mengarah ke 100.100.100.1 dan 192.168.43.1



Gambar 5.13 Route load balancing

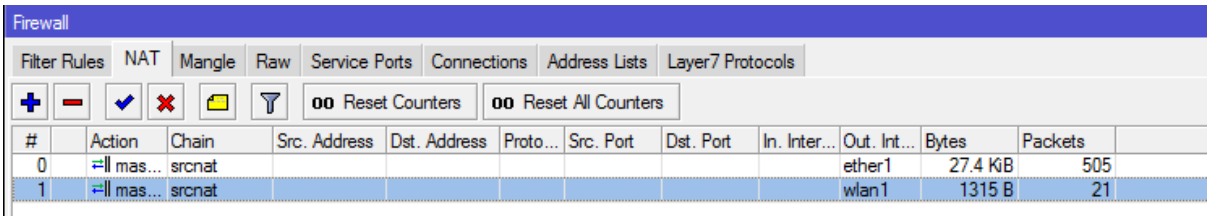
Jika dilihat dari konfigurasi telah dilakukan maka akan terbentuk tabel routing statis dengan kode AS. Pada kondisi ini kedua ether dalam kondisi hidup dengan ditandai dengan reachable wan dan reachable ether 1.



Gambar 5.14 Tabel Routing ECMP

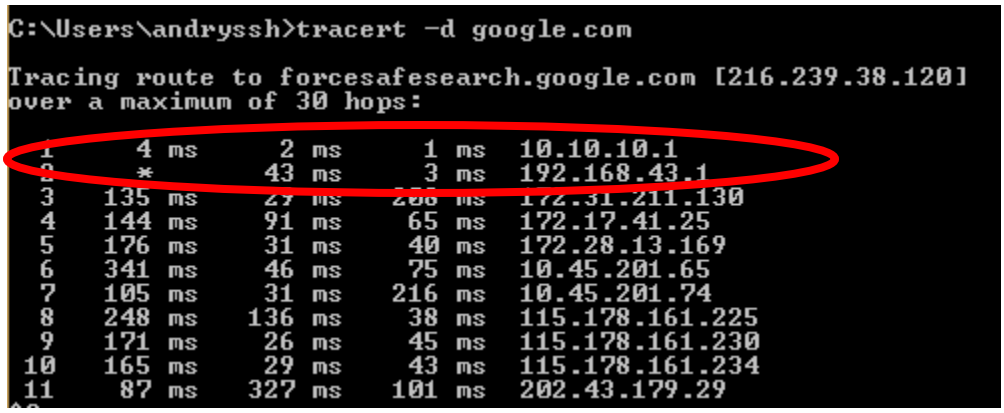
Ketika client mengakses internet maka kondisi ini dipilih secara acak berdasarkan algoritma round robin dari kombinasi SRC/DST address. Step terakhir adalah mengkonfigurasi IP Nat pada menu **IP – Firewall**. Kemudian masuk ke bagian **NAT – ADD**. Masukan dua kondisi berikut ini.

```
[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=ether1
action=masquerade
[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=wlan1
action=masquerade
```



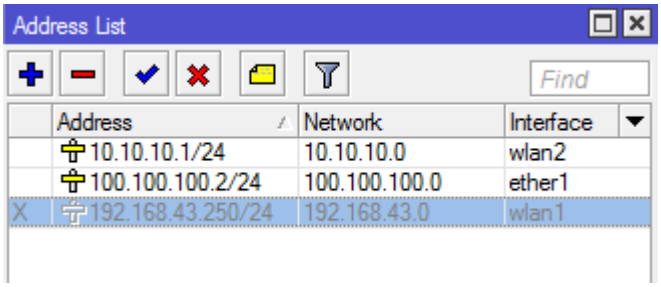
Gambar 5.15 Konfigurasi NAT

Sekarang kita uji koneksi dengan menggunakan cmd. Kita coba tracert ke google.com maka didapatan hasil sebagai berikut. Ternyata link yang dilewati ke internet via 192.168.43.1 yakni wlan1.



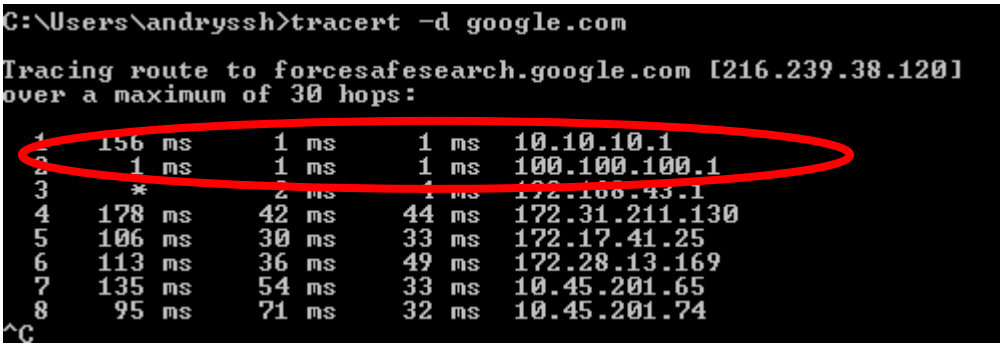
Gambar 5.16 Tes Koneksi Load balancing pertama

Kemudian kita coba dengan mendesable link wlan1 dan pastikan bahwa internet akan pindah ke jalur ether1 sebagai link internetnya.



Gambar 5.17 Disable Link

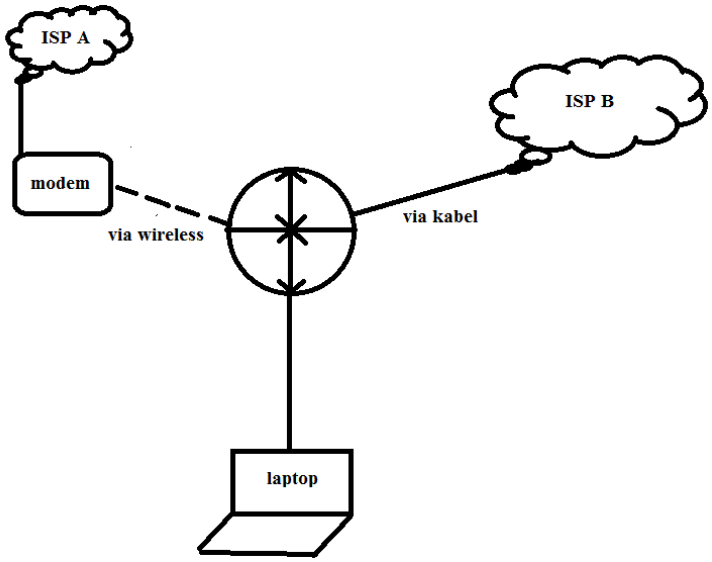
Sekarang link internet sudah berubah via 100.100.100.1 via ether1 sebagi jalur internetnya. Inilah cara load balancing dengan ECMP bekerja.



Gambar 5.18 Tes Koneksi Load balancing Kedua

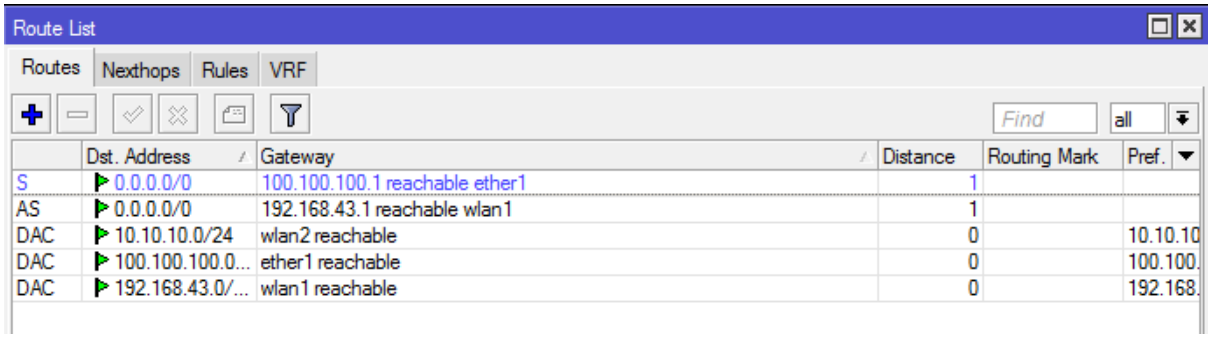
5.3 Fail Over

Fail Over adalah sistem proteksi untuk menjaga apabila link utama terganggu, secara otomatis akan memfungsikan jalur cadangan (link kedua, ketiga, dst). Perbedaan fail over dengan load balancing adalah apabila menggunakan load balancing maka kedua interface baik ether1 dan wlan1 keduanya reachable (aktif) hanya saja pemilihan jalur dilakukan secara acak. Sedangkan pada fail over link yang dibuat menjadi terpisah dan hanya salah satu yang aktif. Apabila satu link putus maka oromatis link yang tidak aktif menjadi aktif.



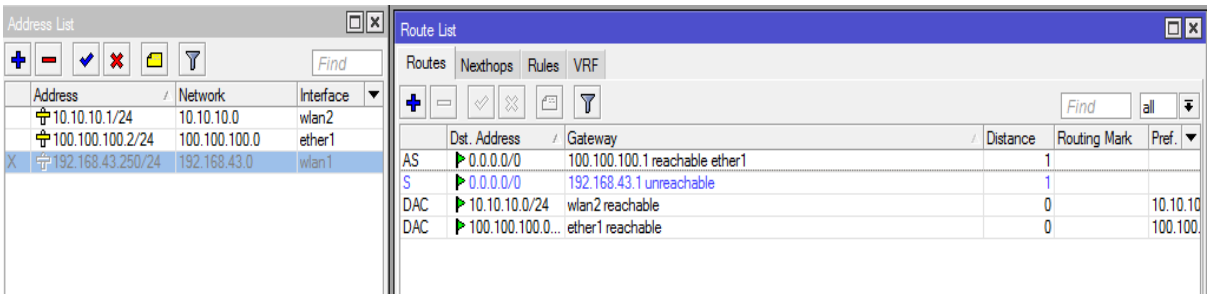
Gambar 5.19 Fail Over

Masih menggunakan topologi diatas. Konfigurasi yang dilakukan untuk ip address, nat dan dns masih sama hanya saja diubah pada konfigurasi routenya saja. Link yang berwarna biru menjadi tidak aktif dan menjadi link cadangan.



Gambar 5.20 konfigurasi Fail Over

Sekarang kita disable pada wlan1 sehingga link yang tidak aktif yakni ether1 berubah menjadi aktif.



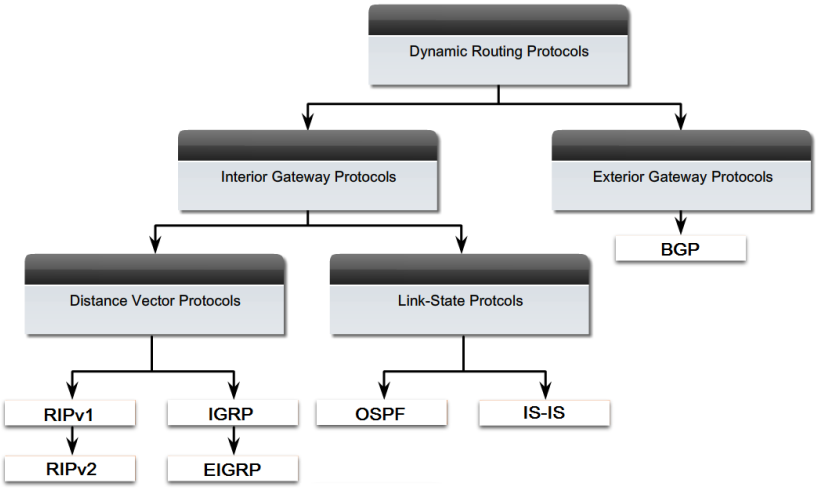
Gambar 5.21 Merubah link fail over

5.4 Routing Dinamis (Dynamic Routing)

Routing dinamis digunakan untuk model jaringan skala yang besar yang memerlukan penanganan khusus karena banyaknya router yang saling terhubung. Routing dinamis ini terbagi menjadi beberapa bagian. Dilihat dari AS (Autonomus System) Number routing dinamsi terbagi menjadi dua yaitu IGP dan EGP. IGP (Interior Routing Protocols) adalah router dinamis yang berkerja pada AS Number yang sama sedangkan EGP (Exterior Routing Protocols) adalah router yang bekerja untuk menghubungkan router yang memiliki AS Number yang berbeda. Routing ini dinamakan dengan BGP.

Sedangkan dilihat dari metode pengiriman paket dalam jaringan router dinamis terbagi menjadi dua bagian yaitu berdasarkan Distance Vector dan Link State. Router yang bekerja dengan

Distance Vector adalah router yang lebih berdasarkan arah dan jarak. Routing ini terdiri dari RIP, RIPv3, IGRP dan EIGRP. Adapun routing berdasarkan Link State adalah routing yang bekerja dengan membangun database routing yang berhubung dengan melihat nilai cost yang terdapat pada tiap router. Router yang bekerja dengan link state adalah OSPF dan IS-IS

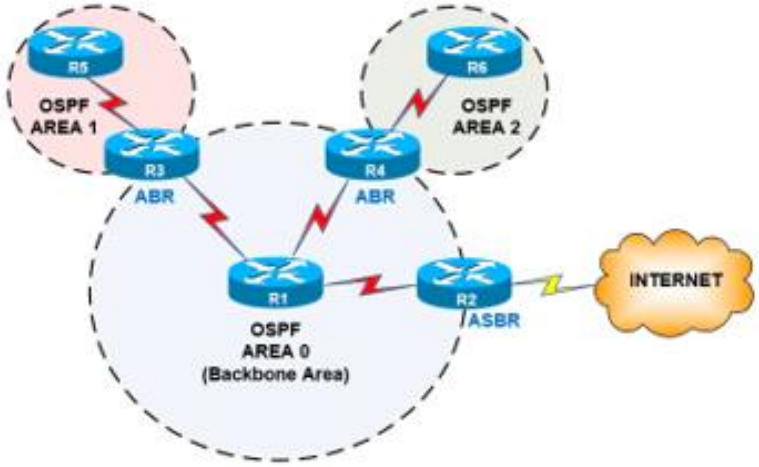


Gambar 5.22 Hirarki Routing Dinamis

5.5 Open Shortest Path First (OSPF)

Ospf adalah protokol routing dinamis tang termasuk kedalam IGP(Interior Gateway Protocol). Prookol routing ini berkerja dengan Link-State dengan menggunakan algoritma Dijkstra(alogritma pencarian jarak terpendek). Ospf mampu menjaga, mengatur dan mendistribusikan informasi routing walaupun topologi network tersebut berubah-ubah secara dinamis. Sedangkan ospf ini bekerja pada layer ke 3 nomor 89.

5.6 OSPF Areas



Gambar 5.22 OSPF Areas

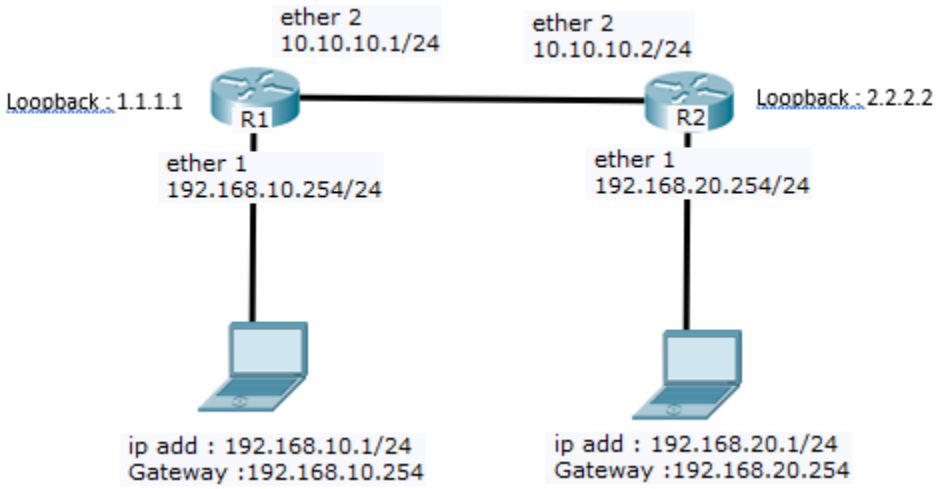
AS (Autonomus System) number adalah suatu kelompok yang terdiri dari satu atau lebih IP Prefix yang terkoneksi yang dijalankan oleh satu atau lebih operator jaringan dibawah satu kebijakan routing yang didefinisikan dengan jelas. AS diperlukan bila suatu jaringan terhubung ke lebih dari satu AS yang memiliki kebijakan routing yang berbeda

Dalam suatu AS terdiri dari beberapa area. **Gambar diatas menunjukan area area ospf yang berkumpul dalam satu AS number**. Identitas area ditulis dalam bit 32-but (0.0.0.0 – 255.255.255.255).

1. IR adalah router yang tergabung dalam sebuah area, jumlah maksimal IR dalam satu area adalah 80 router.
2. ABR adalah router yang menjembatani area satu dengan area yang lain.
3. ASBR adalah sebuah router yang terletak di perbatasan sebuah AS (Router terluar dari sebuah AS) dan bertugas untuk menjembatani antara router yang ada di dalam AS dengan Network lain (Berbeda AS). ASBR juga bisa berarti sebuah router anggota OSPF yang menjembatani routing OSPF dengan Routing protocol yang lain (RIP,BGP dll).

4. Area 0 atau Backbone Area merupakan area dimana ABR berkumpul untuk saling menukarkan informasi routing dari area- area yang lain.
5. Setiap non Backbone Area harus terhubung langsung dengan Area Bakbone.

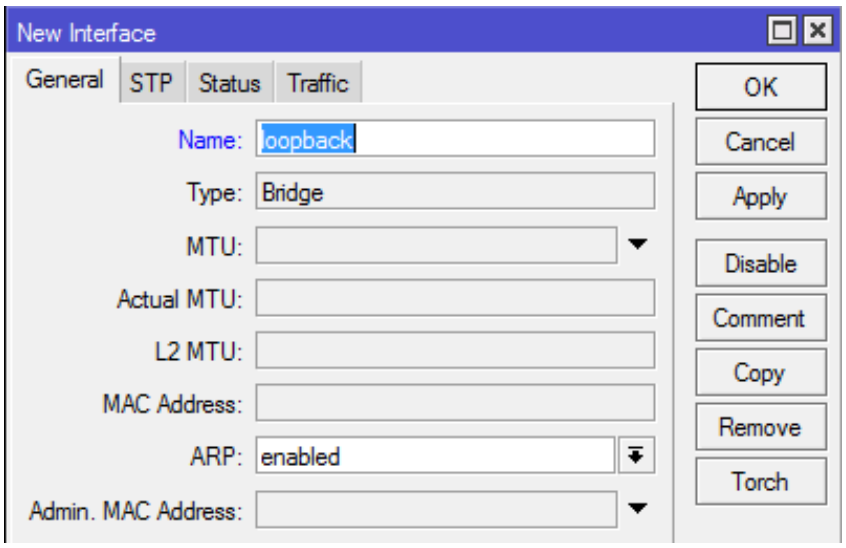
Untuk praktik dasar routing ospf kita gunaka n topologi yang pernah digunakan untuk routing statis. Konfigurasi ini kita buat untuk konfigurasi routing dalam backbone area.



Gambar 5.23 Topologi Routing Ospf

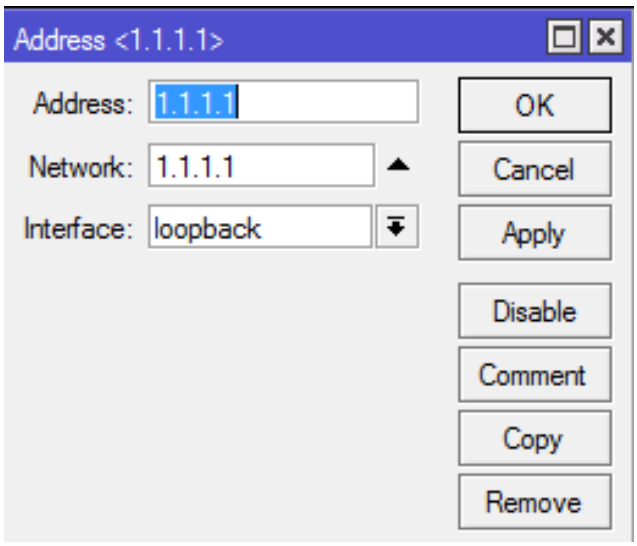
Langkah awal adalah seting ip address pada masing masing router. Saya angggap semua sudah dapat melakukan hal tersebut

Kedua buat interface bride tanpa port pada menu bride dan klik icon plus (+). Masukan pada kotak Name. penamaan tidak harus dengan kata loopback



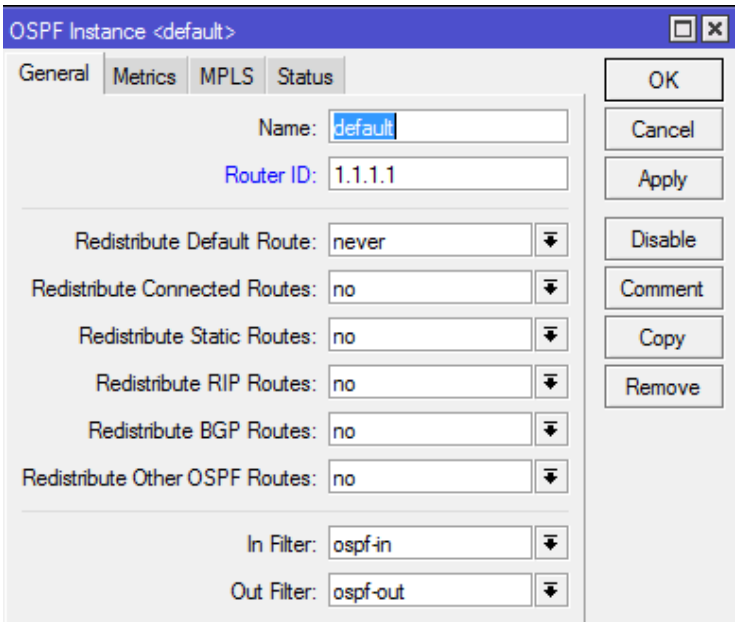
Gambar 5.24 Add interface loopback

Berikan ip address pada interface bride 1.1.1.1



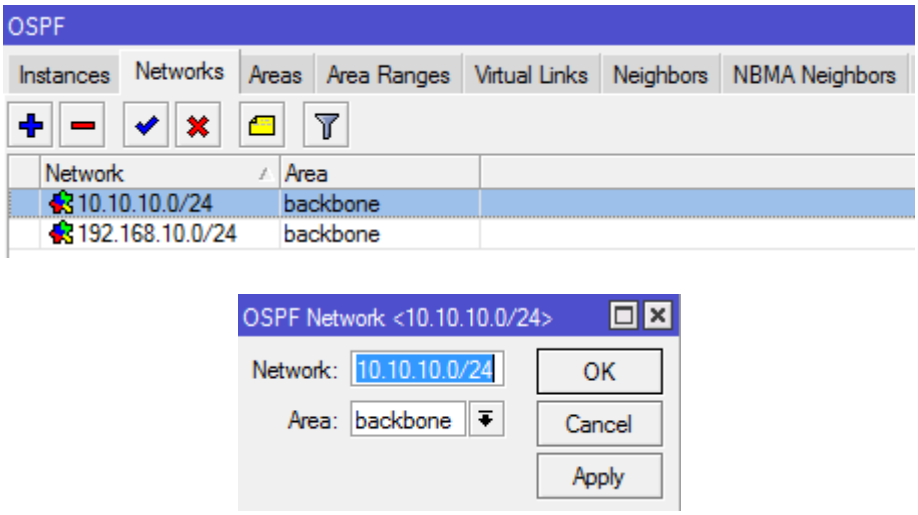
Gambar 5.24 Berikan ip pada interface loopback

Selanjutnya menuju menu **routing – pilih ospf.** Pada menu OSPF pilih tab **instances** edit pada default instance dan masukan **Router ID** dengan ip interface loopback.



Gambar 5.25 Set instance

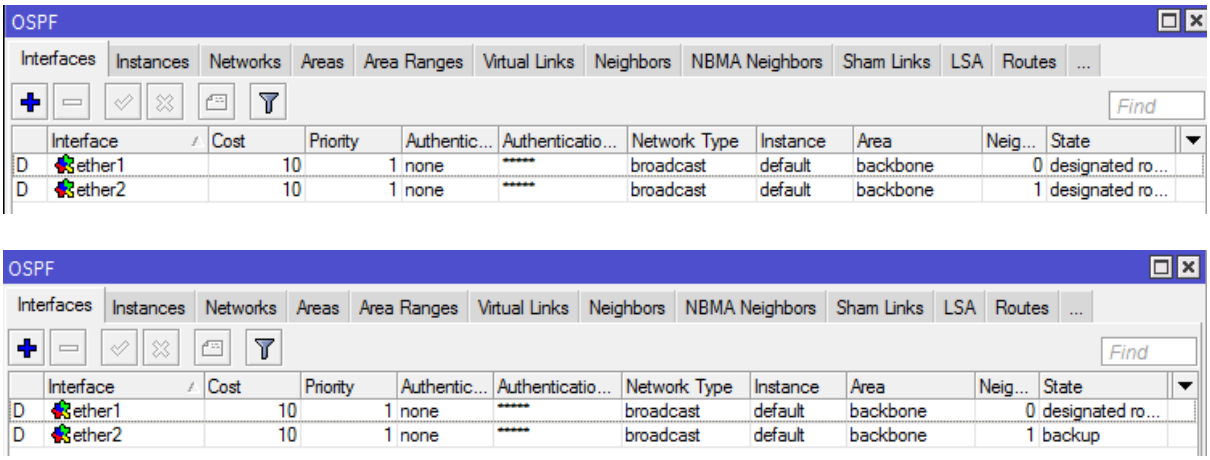
Kemudian setelah itu masuk ke tb network dan tambahkan kedua network yang ada pada router yaitu 10.10.10.0/24 dan 192.168.10.0/24 dan pilih pada kotak area dengan backbone.



Gambar 5.26 Add network

Sampai dengan tahap ini pengaturan router R1 sudah selesai. Lakukan hal yang sama dengan Router R2 seperti diatas dan sesuaikan dengan network dan interface loopbacknya. Apabila kedua

router tersebut sudah dikonfigurasikan maka akan terjadi adjency yang menunjukan router tersebut telah membentuk tabel routing dan mendistribusikan tabel routingnya ke router yang berada disebelahnya. Kita bisa melihat hal tersebut pada tab interface pada menu OSPF.



Gambar 5.27 Interface pada OSPF

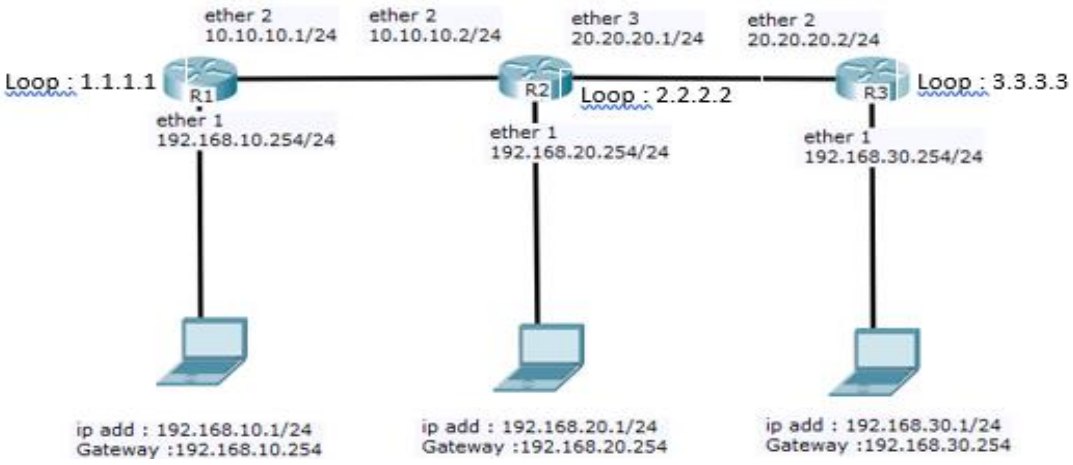
Pastikan kedua router tersebut sudah dapat saling berkomunikasi satu sama lain dengan menggunakan ping antar alamat network.

```
[admin@R1] > ping 192.168.20.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.20.1                               56 127 0ms
    1 192.168.20.1                               56 127 1ms
    2 192.168.20.1                               56 127 1ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms

[admin@R2] > ping 192.168.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.10.1                               56 127 0ms
    1 192.168.10.1                               56 127 1ms
    2 192.168.10.1                               56 127 1ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
```

Gambar 5.28 Uji Koneksi OSPF

Lanjutkan konfigurasi router dibawah ini sebagai latihan. Tambahkan beberapa router dan konfigurasi kembali dengan menggunakan OSPF



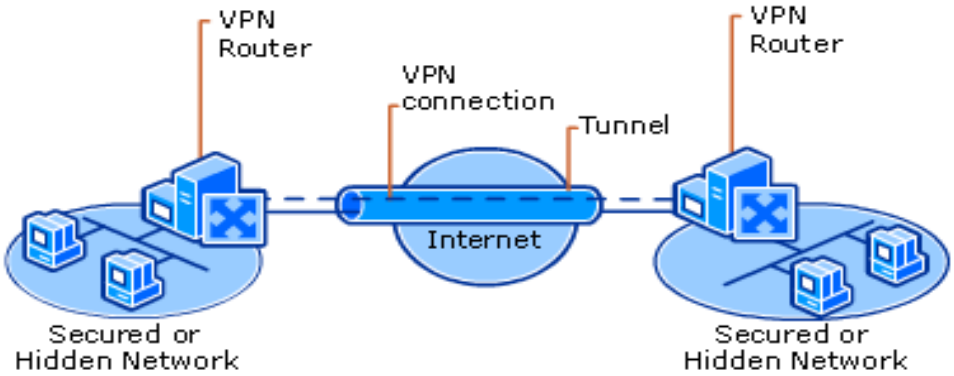
Gambar 5.29 Latihan OSPF

BAB VI
TUNNELING

6.1. Tunnel Overview

6.1.1. Tunnel

Tunnel adalah sebuah metode penyelubungan (encapsulation) paket data di jaringan. Sebelum dikirim, paket data mengalami sedikit pengubahan atau modifikasi, yaitu penambahan header dari tunnel Ketika data sudah melewati tunnel dan sampai di tujuan (ujung) tunnel, maka header dari paket data akan dikembalikan seperti semula (header tunnel dilepas).



Gambar 6.1 Tunnel VPN

VPN merupakan sebuah metode untuk membangun jaringan yang menghubungkan antar node jaringan secara aman / terenkripsi dengan memanfaatkan jaringan publik (Internet / WAN). Contoh implementasi adalah ketika Anda mengelola network yang terdiri dari beberapa kantor di lokasi yang berbeda. Akan membutuhkan biaya besar jika kita kemudian membangun link wireless atau fiber optik padahal bisa jadi antar kantor berada di kota atau bahkan pulau yang berbeda. Dengan VPN, kita bisa membangun sebuah link antar kantor dengan memanfaatkan jaringan internet yang sudah ada. Link yang terbentuk diamankan dengan enkripsi sehingga meminimalisir kemungkinan data akan diakses oleh orang yang tidak bertanggung jawab. Mikrotik support beberapa metode VPN seperti PPTP, L2TP, SSTP, dan OpenVPN. Dengan adanya beberapa opsi ini, kita perlu memilih tipe VPN yang cocok untuk jaringan kita. Secara umum semua type tersebut memiliki fungsi yg sama. Yang membedakan adalah autentikasi dan enkripsi yg digunakan.

VPN secara pengamanannya terbagi 2, yaitu :

1. Security VPN, yaitu metode sambungan VPN yang menerapkan beberapa hal terkait pengamanan komunikasi data - seperti enkripsi dan sebagainya. Contoh Security VPN : Point-to-Point Tunneling Protocol (atau PPTP), IP Security (atau IPSec), Layer 2 Tunneling Protocol (atau L2TP), Secure Socket Layer (atau SSL) dan sebagainya.
2. IP VPN, yaitu metode sambungan VPN yang dilakukan oleh ISP melalui media IP secara keseluruhan didalam jaringan internalnya. Contoh IP VPN adalah mekanisme Multi Protocol Label Switching (atau MPLS) dan Virtual Private LAN Service (atau VPLS) dan seterusnya.

6.1.2. Macam-macam Tunnel

1. PPTP (Point to Point Tunnel Protocol)

   PPTP merupakan salah satu type VPN yang paling sederhana dalam konfigurasi. Selain itu juga fleksibel. Mayoritas operating system sudah support sebagai PPTP Client, baik operating system pada PC ataupun gadget seperti android. Komunikasi PPTP menggunakan protokol TCP port 1723, dan menggunakan IP Protocol 47/GRE untuk enkapsulasi paket datanya. Pada setting PPTP, kita bisa menentukan network security protocol yang digunakan untuk proses autentikasi PPTP pada Mikrotik, seperti pap,chap,mschap dan mschap2. Kemudian setelah tunnel terbentuk, data yang ditransmisikan akan dienkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE). Proses enskripsi biasanya akan membuat ukuran header paket yang ditransmisikan akan bertambah. Jika kita monitoring, traffick yang melewati tunnel PPTP akan mengalami overhead.

2. L2TP (Layer 2 Tunnel Protocol)

   L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan

L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. Traffick yang melewati tunnel L2TP akan mengalami overhead.

3. SSTP (Secure Socket Tunneling Protocol)

   Untuk membangun vpn dengan metode SSTP diperlukan sertifikat SSL di masing-masing perangkat, kecuali keduanya menggunakan RouterOS. Komunikasi SSTP menggunakan TCP port 443 (SSL), sama hal nya seperti website yang secure (https). Anda harus memastikan clock sudah sesuai dengan waktu real jika menggunakan certificate. Manyamakan waktu router dengan real time bisa dengan fitur NTP Client. Sayangnya belum semua OS Support VPN dengan metode SSTP. Traffick yang melewati tunnel SSTP akan mengalami overhead.

4. OpenVPN

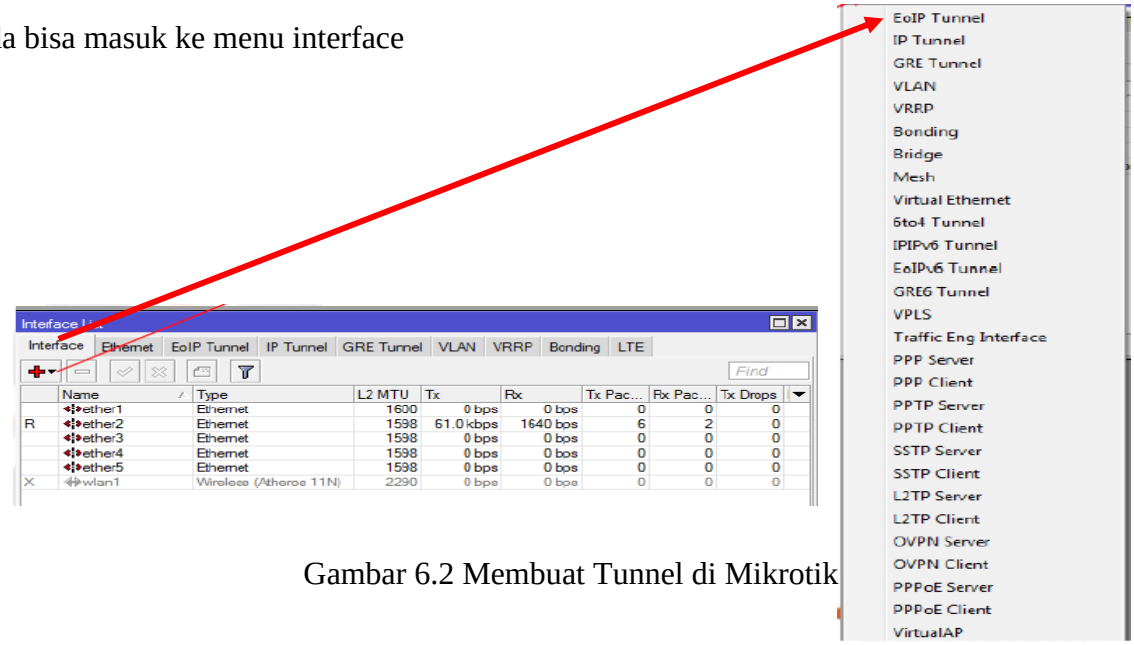
   VPN ini Biasa digunakan ketika dibutuhkan keamanan data yg tinggi. Secara default, OpenVPN menggunakan UDP port 1194 dan dibutuhkan certificate pada masing-masing perangkat untuk bisa terkoneksi. Untuk client compatibility, OpenVPN bisa dibangun hampir pada semua Operating System dengan bantuan aplikasi pihak ketiga. OpenVPN menggunakan algoritma sha1 dan md5 untuk proses autentikasi, dan menggunakan beberapa chiper yaitu blowfish128, aes128, aes192 dan aes256. Trafik yang melewati tunnel OpenVPN akan mengalami overhead.

Perlu diingat, bahwa semakin kita membutuhkan sebuah jaringan yg aman, maka akan semakin kompleks konfigurasi yang perlu diterapkan, begitu juga dengan penggunaan resource hardware, semakin tinggi enkripsi yang digunakan, penggunaan resource, khususnya CPU juga akan naik. Kesimpulan yang bisa kita ambil, jika Anda menginginkan VPN dg kompatibilitas perangkat client yg baik , maka PPTP bisa menjadi pilihan. Selain itu, PPTP juga bisa menjadi pilihan jika Anda tidak ingin terlalu repot untuk melakukan konfigurasi. Tetapi jika Anda menginginkan sebuah VPN dengan keamanan lebih bagus, gunakan L2TP/IPsec atau OpenVPN. Biasanya untuk OS windows, secara default menggunakan L2TP/IPSec, sehingga tinggal diseusuaikan pada sisi server. Jika memang perangkat Anda support dan Anda membutuhkan keamanan yg tinggi pada

jalur VPN anda, L2TP/IPSec bisa menjadi pilihan. Satu hal yang menjadi catatan, penggunaan VPN tidak bisa meningkatkan bandwidth (lebih tepatnya mengurangi bandwidth anda karena ada penambahan headernya), tergantung dari besar bandwidth langganan anda.

Untuk membuat tunneling di mikrotik

Anda bisa masuk ke menu interface



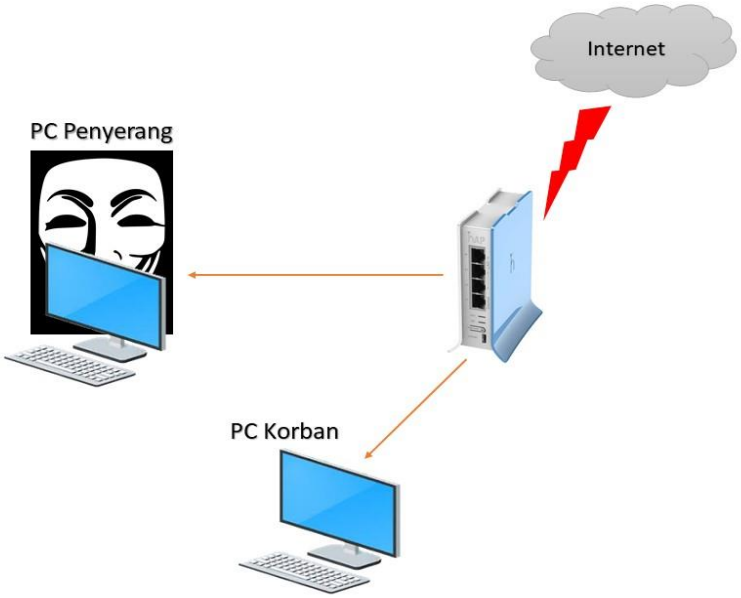
Gambar 6.2 Membuat Tunnel di Mikrotik

7.2. Point To Point Over Ethernet (PPPoE)

7.2.1. PPPoE

Service yang terfasilitasi di Mikrotik salah satunya adalah Point To Point Over Ethernet (PPPoE) yang biasa digunakan sebagai penangkal NetCut. Aplikasi NetCut adalah aplikasi yang sering digunakan untuk melakukan penyerangan terhadap jaringan yang menyerang layer 2 dengan melakukan broadcast ARP pada jaringan yang di serang, lalu penyerang akan mendapatkan inforamsi MAC Address dan IP Address yang terpasang pada client yang ada di jaringan tersebut.

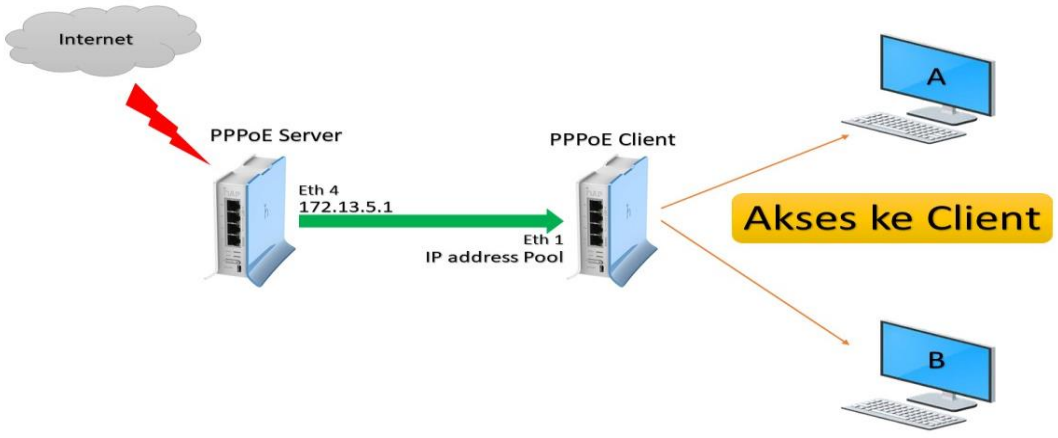
Setelah informasi tersebut didapatkan, penyerang akan sangat mudah untuk melakukan pemutusan traffik jaringan dari client-client yang ada di jaringan tersebut, dengan cara mengirimkan informasi ARP palsu kepada router (gateway) serta kepada client, sehingga posisi penyerang berada di antara router gateway dengan client.



Gambar 6.3 Ilustrasi Topologi Serangan NetCut

Gambar di atas merupakan ilustrasi topologi dari serangan NetCut, cara pencegahan dengan memanfaatkan fitur PPPoE yang ada pada router Mikrotik dapat kita praktekan dalam Lab PPPoE berikut ini.

7.2.2. Lab Membangun Jaringan PPPoE

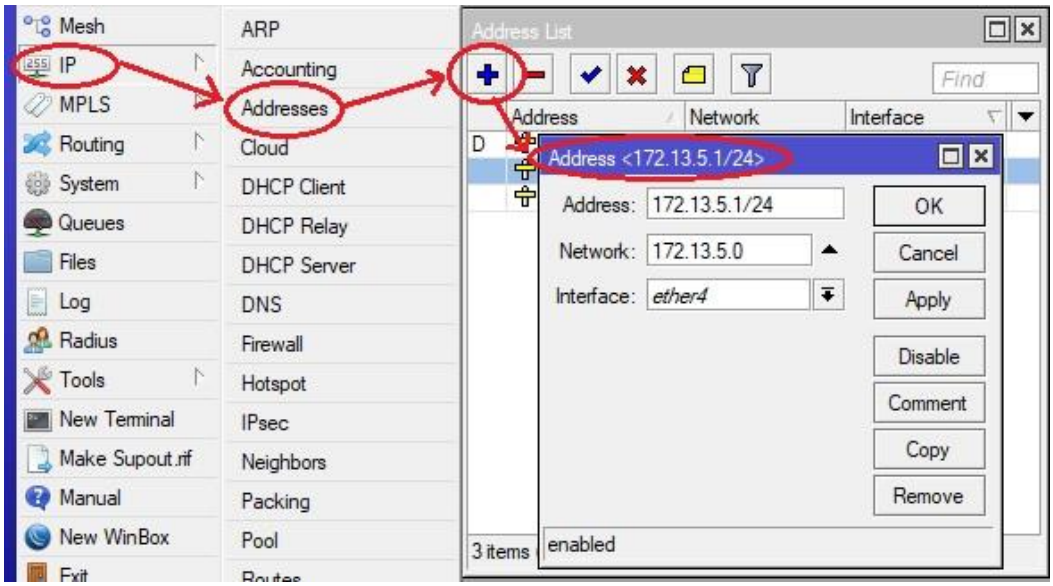


Gambar 6.4 Topologi Lab Jaringan PPPoE

Dalam lab ini kita akan mencoba untuk membangun jaringan PPPoE sesuai dengan skema topologi di atas. Lab ini berhasil jika PPPoE Client bisa mendapat akses internet dari PPPoE Server. sebelumnya pastikan router mikrotik yang digunakan sebagai PPPoE Server sudah mendapatkan

akses ke internet tetapi router mikortik yang digunakan sebagai PPPoE Client dan PC Client belum mendapatkan akses internet.

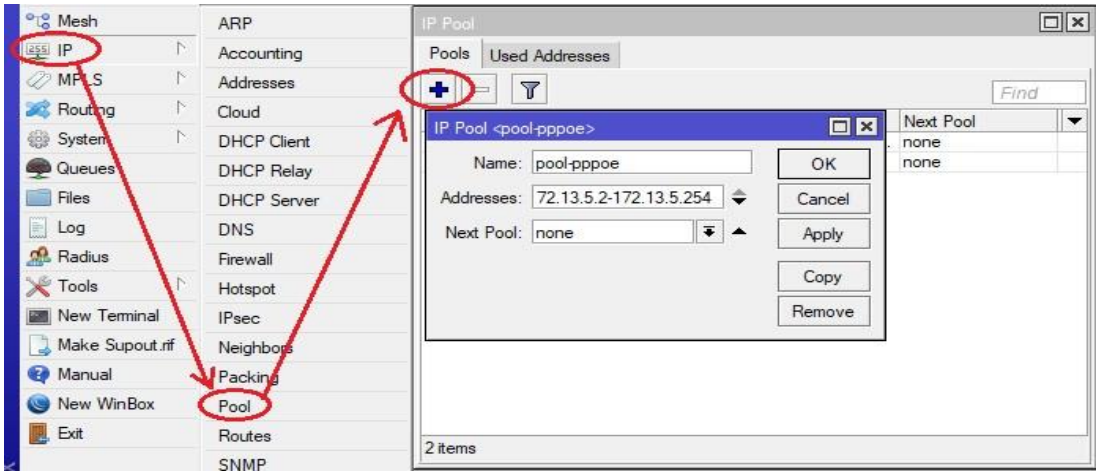
1. Setting IP Address PPPoE Server, dapat dilihat pada gambar di bawah ini :



Gambar 6.5 Setting IP Address PPPoE Server

Langkah pertama adalah kita akan memberikan IP Address pada ethernet yang terhubung ke PPPoE Client, disini kita menggunakan ether4. Masuk ke menu IP, lalu pilih address, klik tanda tambah dan isikan address, network, dan interface sesuai pada gambar di atas, klik apply dan ok.

2. Setting IP Pool PPPoE Server, dapat dilihat pada gambar di bawah ini :



Gambar 6.6 Setting IP Pool PPPoE Server

Masih di menu IP, pilih Pool, lalu klik tanda tambah dan isikan :

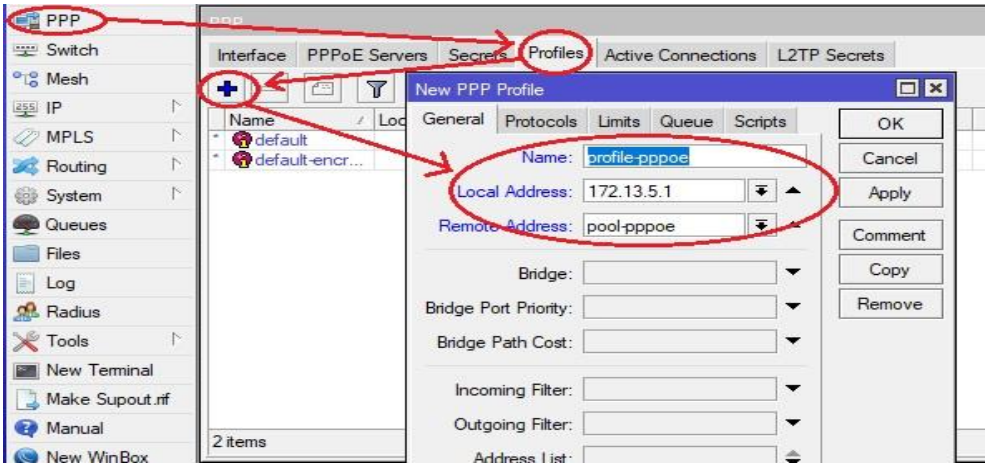
Name : pool-pppoe (disesuaikan)

Address : 172.13.5.2-172.13.5.254

Next Pool : none

apply dan ok.

3. Setting PPP Profile PPoE Server, dapat dilihat pada gambar di bawah ini :



Gambar 6.7 Setting PPP Profile PPPoE Server

Pilih menu PPP, lalu profile, klik tanda tambah dan isikan :

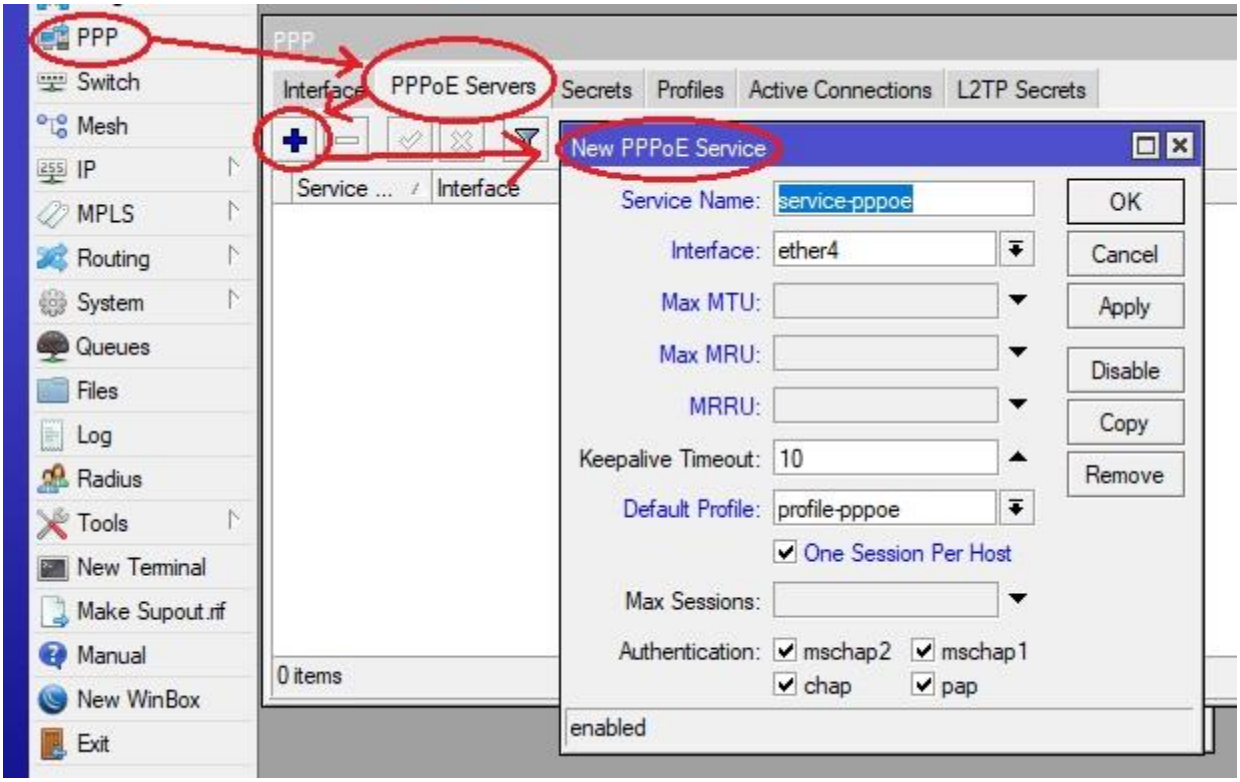
Name : profile-pppoe (disesuaikan)

Loc. Address : 172.13.5.1 (adalah ip ether 4 PPPoE Server)

Rem. Address : pool-pppoe (sesuai ip pool yang sudah dibuat sebelumnya)

Apply dan Ok.

4. Setting PPP Service PPoE Server, dapat dilihat pada gambar di bawah ini :



Gambar 6.8 Setting PPP Service PPPoE Server

Masih di menu PPP, pada bagian PPPoE Servers klik tambah dan isi :

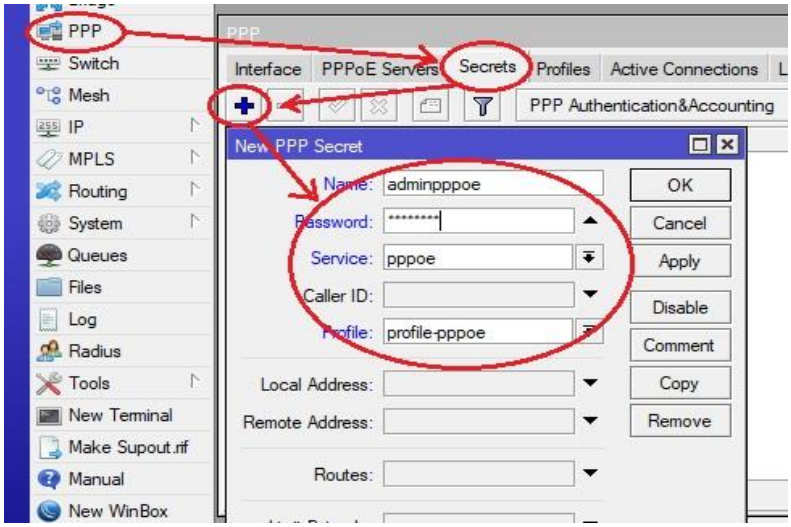
Service Name : service-pppoe (disesuaikan)

Interface : ether4

Keepalive Time : 10

Ceklis pada one session per host untuk meastikan hanya 1 host saja yang dapat terkoneksi per session, apply dan ok.

5. Setting PPP Secret PPPoE Servers, dapat dilihat pada gambar di bawah ini :



Gambar 6.9 Setting PPP Secret PPPoE Server

Masih di menu PPP, pilih Secrets lalu klik tambah dan isi :

Name : adminpppoe (disesuaikan)

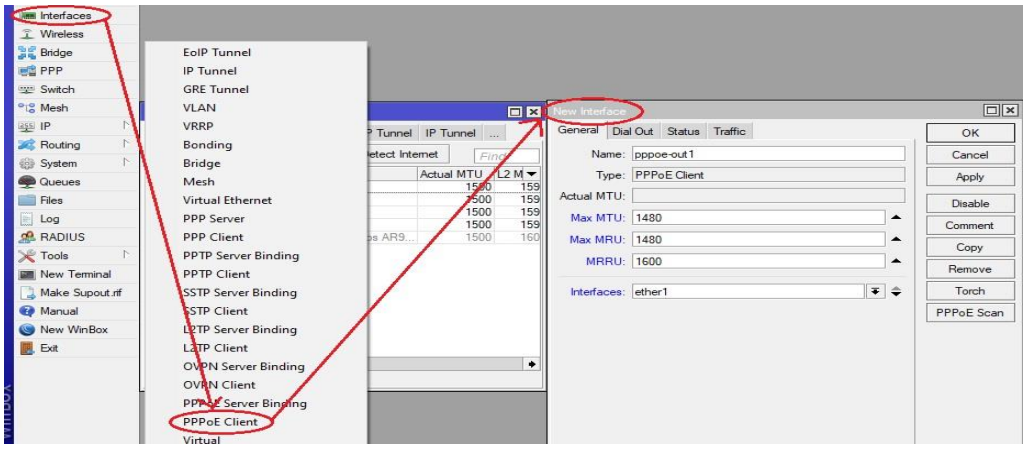
Password : 12345678 (disesuaikan)

Profile : profile-pppoe (sesuai profile yang sudah dibuat sebelumnya)

Apply dan Ok.

Sampai disini kita sudah selesai melakukan konfigurasi pada router yang digunakan sebagai PPPoE Server, selanjutnya kita akan melakukan konfigurasi pada router satunya yang digunakan sebagai PPPoE Client, sebagai berikut:

6. Setting Interface PPPoE Client, dapat dilihat pada gambar di bawah ini :



Gambar 6.10 Setting Interface PPPoE Client

Setelah login winbox di router satunya, silahkan pilih menu interface, lalu pilih PPPoE Client, pada bagian generel isi :

Name : pppoe-out1

Max MTU : 1480

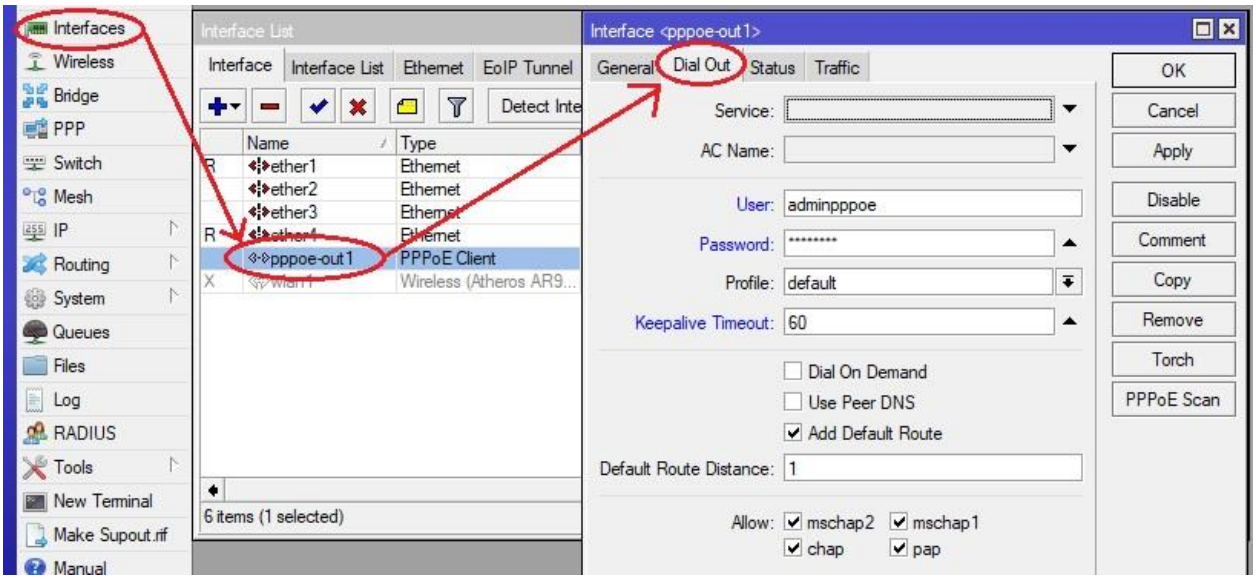
Max MRU : 1480

MRRU : 1600

Interface : ether1 (sesuai interface yang terkoneksi ke router PPPoE Sever)

Apply dan OK.

7. Setting Dial Out PPPoE Clients, dapat dilihat pada gambar di bawah ini :



Gambar 6.11 Dial Out PPPoE Client

Masi di menu Interfaces, double klik pada pppoe-out1 yang sudah dibuat sebelumnya, dan di bagian Dial Out isikan :

User : adminpppoe (sesuaikan dengan user yang dibuat di PPPoE Server)

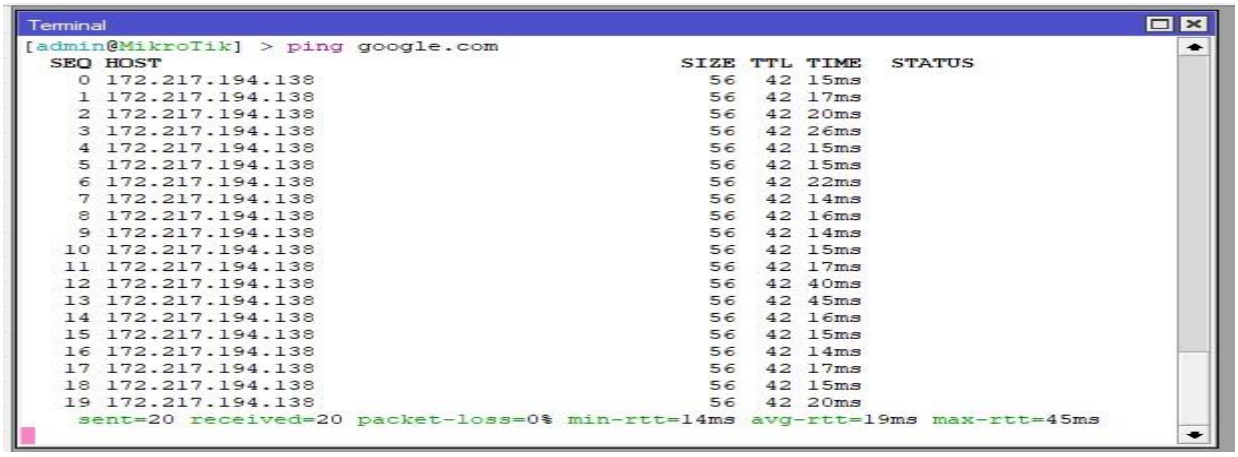
Pasword : 12345678 (sesuaikan dengan password yang dibuat di PPPoE Server)

Profile : default

Apply dan Ok.

Setelah proses ini pastikan ada huruf R pada interface pppoe-out1, R disini berarti Running, menandakan PPPoE Client sudah berhasil terkoneksi dengan PPPoE Server.

8. Tes Koneksi Dengan PING, dapat dilihat pada gambar di bawah ini :



Gambar 6.12 Tes Koneksi PPPoE

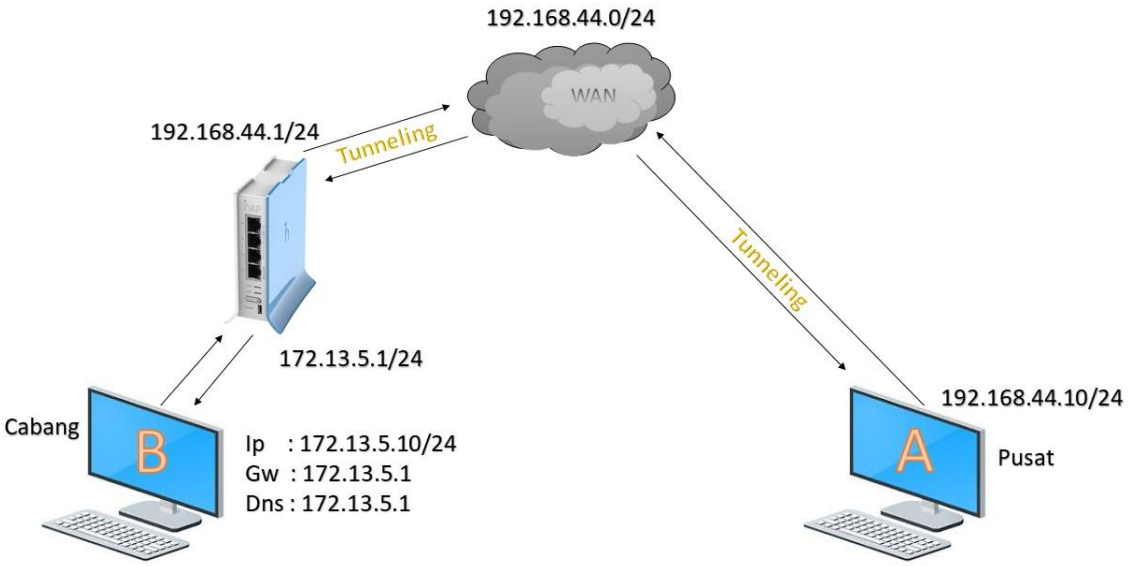
7.3. Point To Point Tunnel Protocol (PPTP)

7.3.1. PPTP

Service yang terfasilitasi di Mikrotik salah satunya adalah Point Tunnel Protocol (PPTP) yang biasa digunakan untuk membangun sebuah jaringan VPN. Dalam membangun jaringan PPTP dibutuhkan Server dan Client. Mikrotik RouterOS bisa difungsikan baik sebagai server maupun client atau bahkan diaktifkan keduanya bersama dalam satu mesin yang sama. Fasilitas ini sudah termasuk dalam package PPP sehingga anda hanya perlu cek di menu system package apakah paket tersebut sudah ada di router atau belum. Fungsi PPTP Client juga sudah ada di hampir semua OS, sehingga kita bisa menggunakan Laptop/PC sebagai PPTP Client.

Biasanya PPTP ini digunakan untuk jaringan yang sudah melewati multihop router (Routed Network). Jika anda ingin menggunakan PPTP pastikan di Router anda tidak ada rule yang melakukan blocking terhadap protocol TCP 1723 dan IP Protocol 47/GRE karena service PPTP menggunakan protocol tersebut.

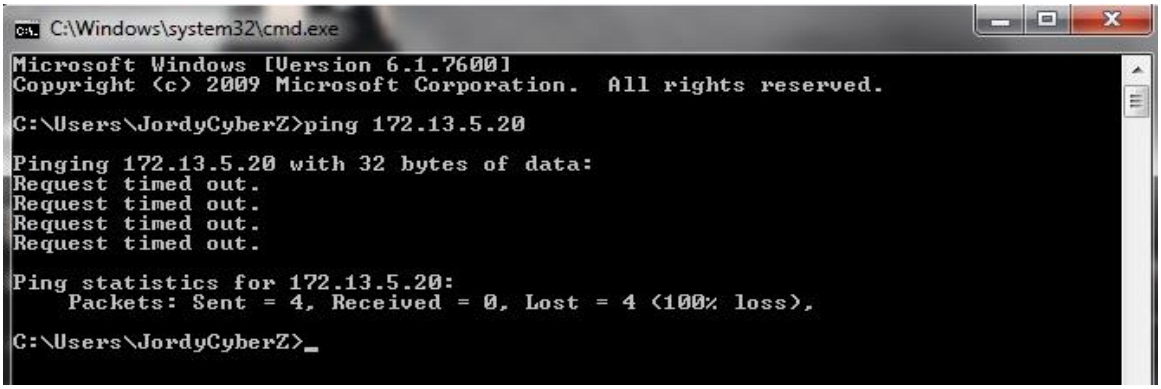
7.3.2. Lab Membangun Jaringan PPTP



Gambar 6.13 Topologi Lab Jaringan PPTP

Dalam lab ini kita akan mencoba untuk membangun jaringan PPTP sesuai dengan skema topologi di atas. Lab ini berhasil jika PC di kantor pusat dapat terkoneksi dengan PC di kantor cabang melalui jaringan VPN PPTP. Berikut ini langkah-langkah yang dapat dilakukan untuk melakukan konfigurasi dalam membangun jaringan PPTP, sebelumnya pastikan router mikrotik, pc kantor cabang, dan kantor pusat sudah dapat terkoneksi ke internet.

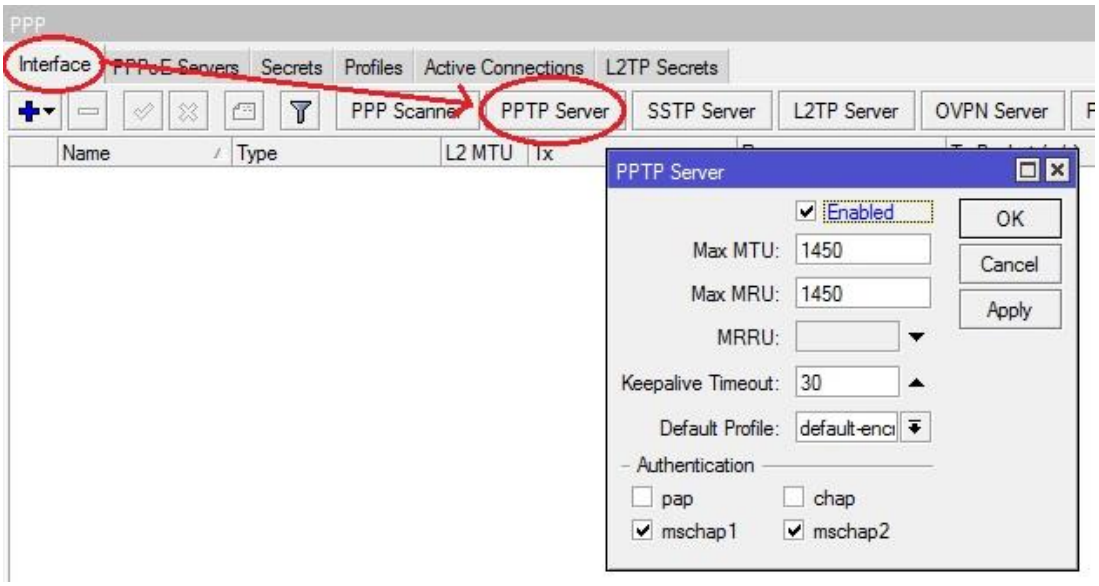
1. Uji PING sebelum konfigurasi, dapat dilihat pada gambar di bawah ini :



Gambar 6.14 Uji Ping Sebelum Konfigurasi PPTP

Dapat dilihat uji ping dari kantor pusat ke kantor cabang masih tidak bisa, ditandai dengan status ping Request Timed Out (RTO).

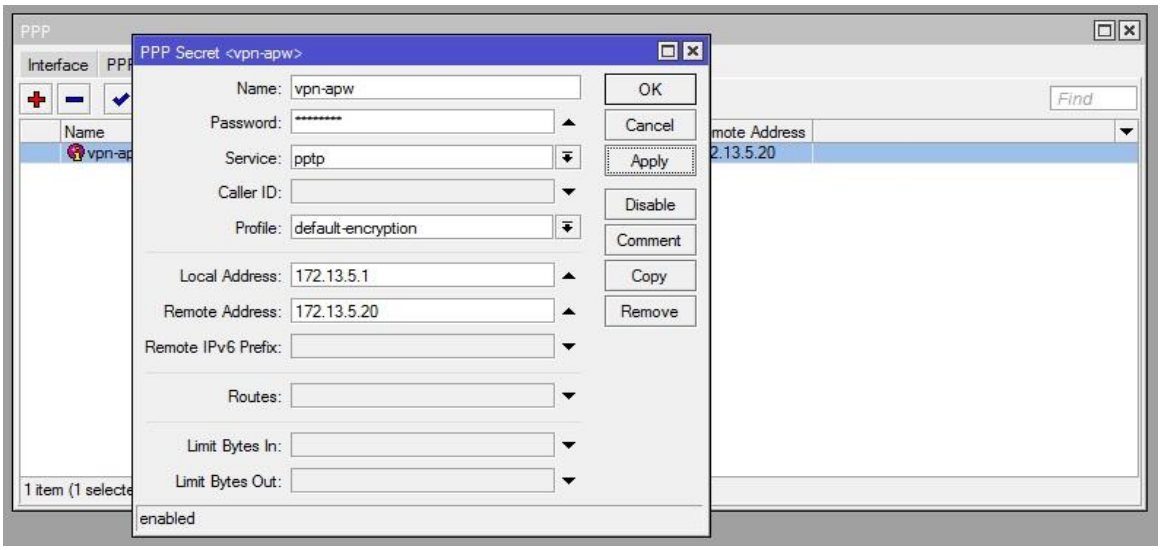
2. Aktifasi PPTP Server. Dapat dilihat pada gambar di bawah ini :



Gambar 6.15 Aktifasi PPTP Server

Setelah login ke dalam winbox, langkah selanjutnya masuk ke dalam menu PPP, pada bagian interface pilih PPTP Server dan terakhir ceklis Enabled, apply dan ok.

3. Membuat user PPTP. Dapat dilihat pada gambar di bawah ini :

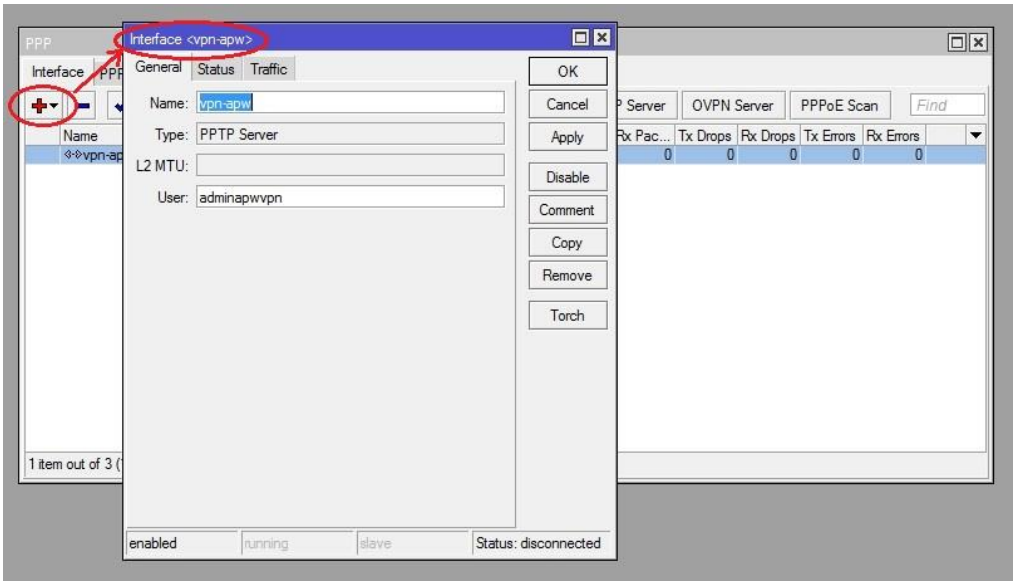


Gambar 6.16 Membuat User PPTP

Masih di menu PPP, pilih ppp secret untuk membuat username dan password untuk proses autentikasi Client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil

akan berpengaruh. Untuk name diisi sesuai nama user yang akan kita gunakan begitu juga dengan password menyesuaikan saja, untuk service pilih pptp, profile default-encryption, local address diisi sesuai ip lokal yang ada di kantor cabang dan remote address diisi ip kantor pusat.

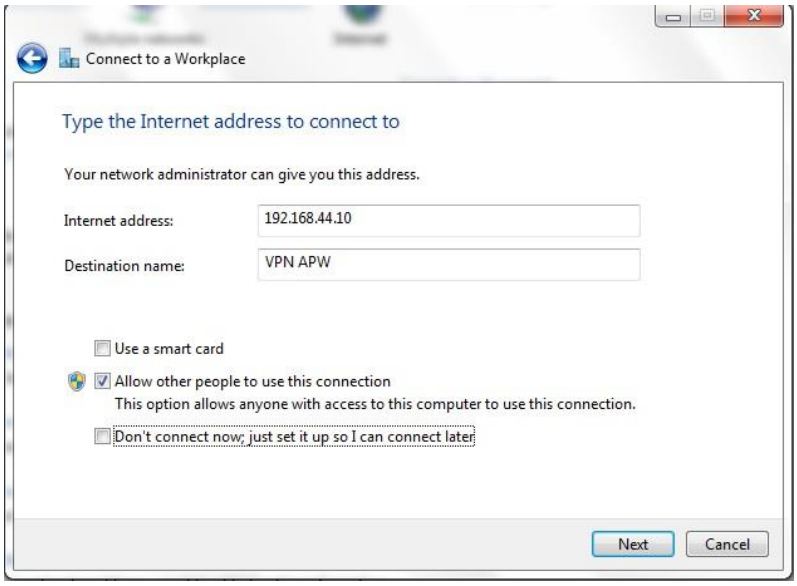
4. Menambahkan user VPN. Dapat dilihat pada gambar di bawah ini :



Gambar 6.17 Membuat User VPN

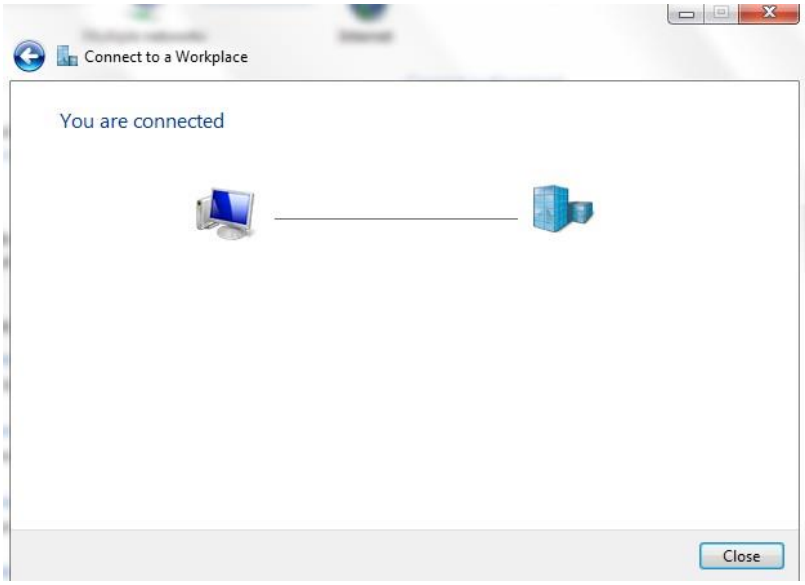
Masih di menu PPP, pada bagian interface kita tambahkan user yang sudah kita buat di konfigurasi sebelumnya dengan klik tanda tambah dan isi name sesua username pada saat kita membuat user, dan pada bagian user kita isi sesuai dengan authentifikasi user yang kita buat diperuntukkan kepada siapa. Lalu pilih apply dan ok.

5. Konfigurasi PPTP Client pada windows, dapat dilihat pada gambar di bawah ini :



Gambar 6.18 Konfigurasi PPTP Client

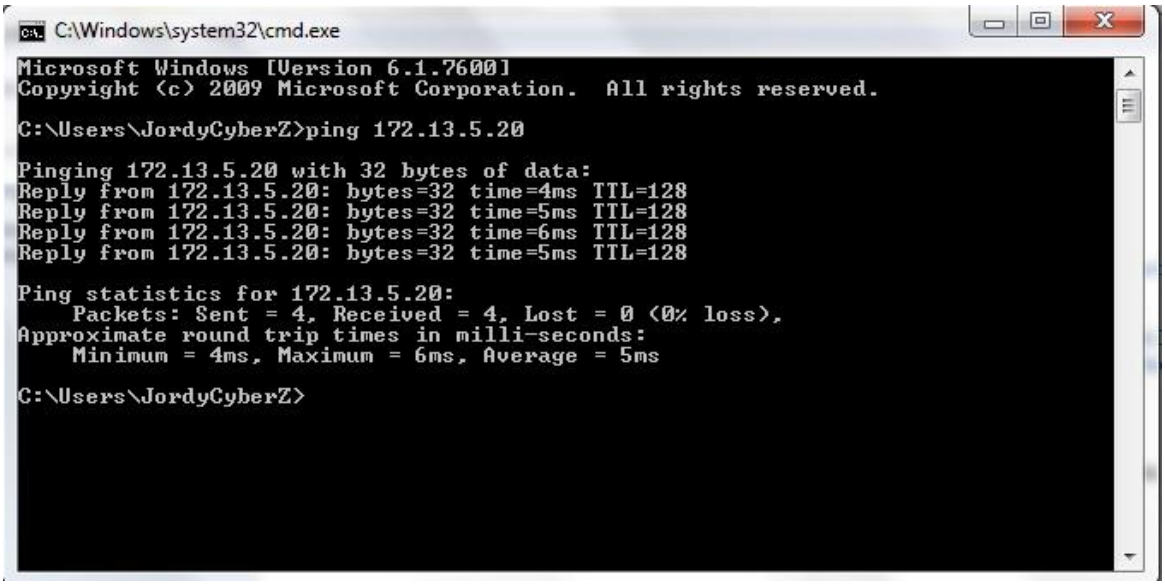
Di Network & Sharing Centre cari VPN dan lakukan konfigurasi seeprti gambar di atas, untuk internet address diisi dengan IP Publik Kantor Cabang, dan Destination Name diisi nama VPN yang mau kita tuju (disesuaikan saja), lalu klik next.



Gambar 6.19 Status Koneksi PPTP Client

Jika sudah ada tulisan “you are connected” berarti anda sudah terkoneksi antara kantor pusat ke kantor cabang, lalu klik close.

6. Jalankan uji PING untuk memastikan koneksi tersebut, dapat dilihat pada gambar di bawah ini :



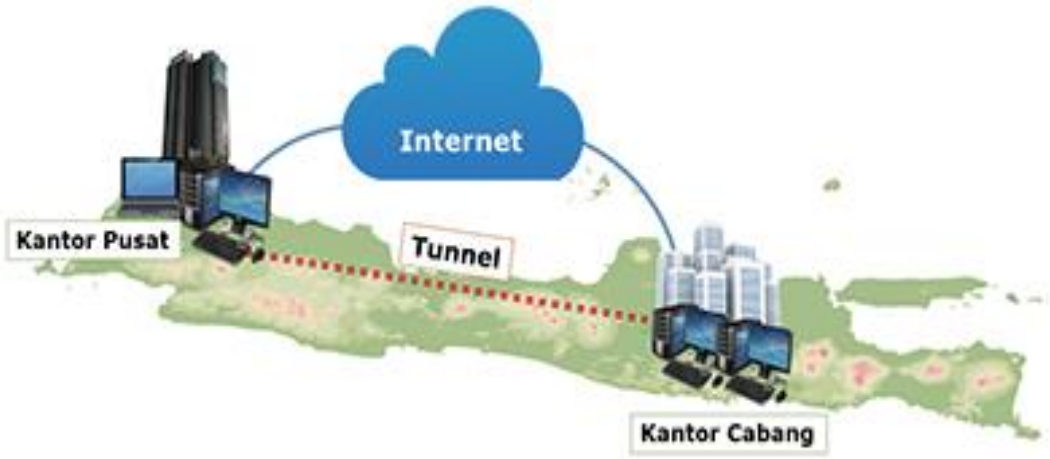
Gambar 6.14 Uji Ping Setelah Konfigurasi PPTP

Jika status PING reply, maka koneksi vpn menggunakan pptp dari kantor pusat ke kantor cabang berhasil.

6.3.3 EoIP Tunelling

Untuk membangun tunnel, kedua kantor baik kantor cabang maupun kantor pusat harus terkoneksi ke internet dan memiliki **IP public static**. Tunneling merupakan salah satu cara untuk

membangun sebuah jalur antar mikrotik router di atas sebuah koneksi TCP/IP. Jika digambarkan dalam bentuk topologi, akan terlihat seperti berikut :



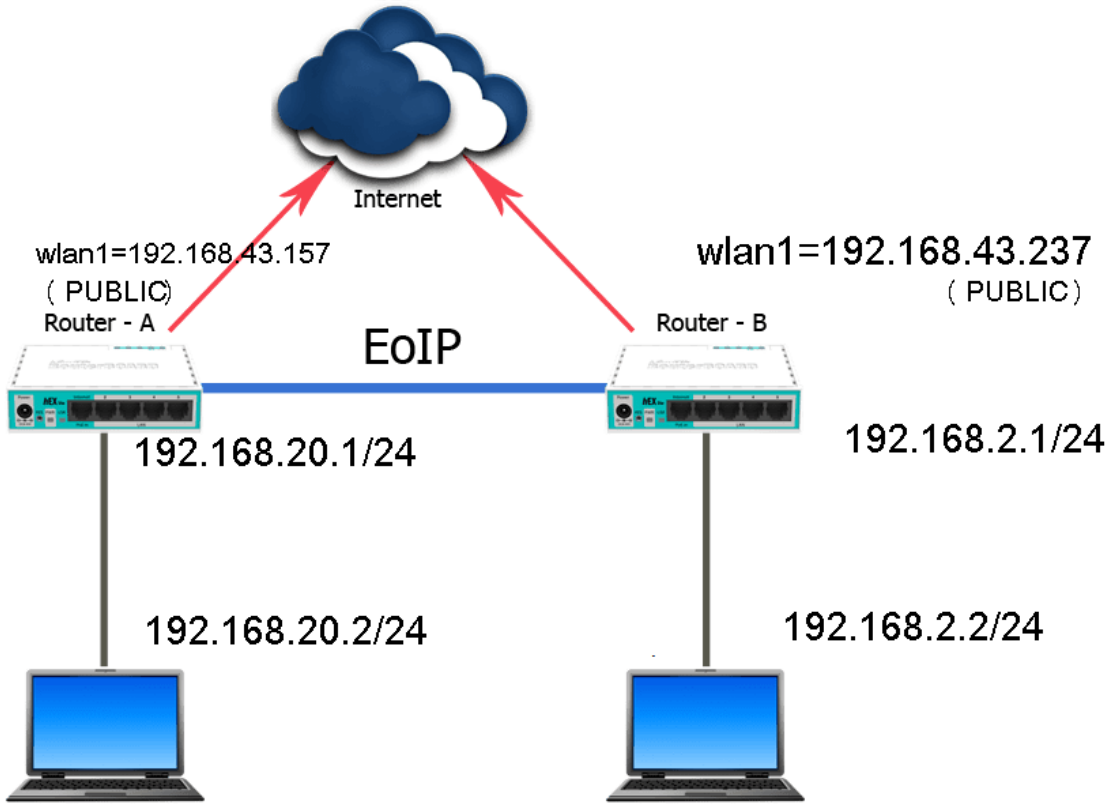
Gambar 6.20 Tunnel

Seperti gambar diatas terdapat 2 (dua) Gedung yang memiliki koneksi internet pada keduanya. Namun dengan adanya Tunel mereka seolah-olah mempunyai jembatan Pribadi sebagai media penghubung, sehingga diantara kedua jaringan tersebut bisa saling berkomunikasi.

Keuntungan EOIP adalah :
1. Komunikasi jaringan jarak Jauh layaknya seperti dalam satu jaringan.
2. Biarpun jaringan kita mau melewati beberapa router mau 2,3 maupun 10 nggak ada masalah. maka hal ini dengan kita gunakan yg namanya **EOIP** tunnel sehingga dengan menggunakan EOIP tunnel ini maka jaringan yang kita tuju akan menjadi satu subnet dengan alokasi ip yang kita inginkan.
3. Lebih efisien

Kerugian EOIP adalah :
Dikarenakan melewati beberapa router yang berbeda .maka secara otomatis bisa membaca jaringan tetangganya atau router yang dilewati (biasanya dalam 1 hub) yang masuk, maka jaringan tersebut akan bisa dibaca. Jadi sangat2 rentan karena network kita bisa terbaca. Namun hal ini bisa dihindari yaitu dengan cara port scan yg di gunakan winbox itu kita tutup di router yang bersangkutan dengan begitu walaupun kita scan berkali-kali tidak akan terlihat.

STUDI KASUS



Gambar 6.21 Studi Kasus EoIp

Konfigurasi STEP 1

1. Lakukanlah konfigurasi router A dan B dengan menjadikannya station serta mengkonfigurasi sampai Router A dan B masing-masing mempunyai koneksi internet.
2. IP Wlan1 didapatkan dari masing-masing ISP yang Anda gunakan dengan melakukan set up DHCP Client pada wlan1

Table 6.1 IP address dan Interface

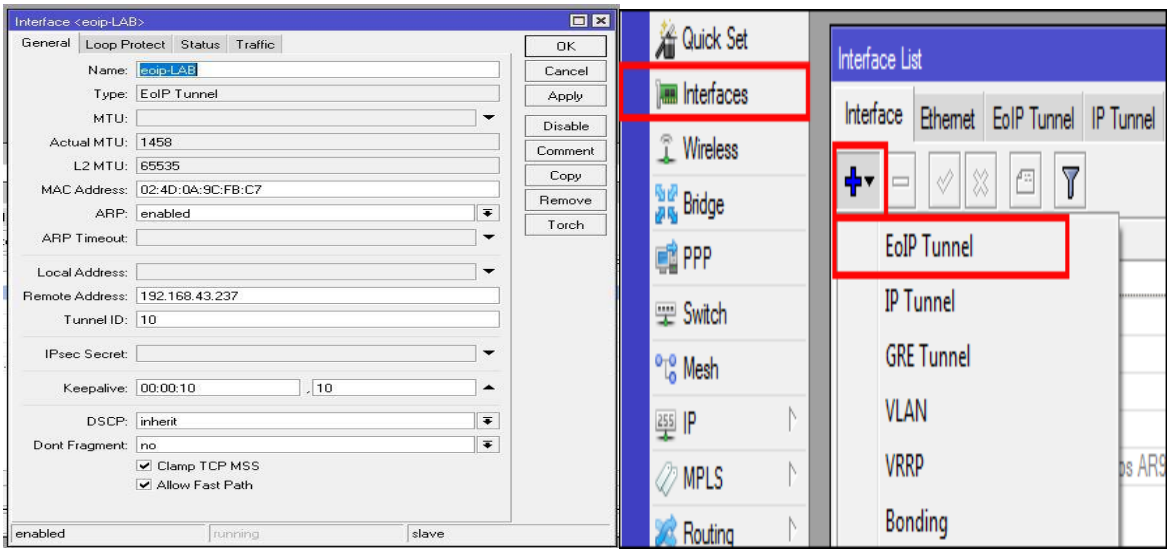
No	Interface	IP Address	Hardware
1	Wlan 1	IP didapatkan dari masing-masing ISP	ROUTER A
2	Wlan 1	IP didapatkan dari masing-masing ISP	ROUTER B
3	Ether 2	192.168.20.1/24	ROUTER A
4	Ether 2	192.168.2.1/24	ROUTER B
5	EoIP-LAB	10.10.10.1	ROUTER A
6	EoIP-LAB	10.10.10.2	ROUTER B
7	Ethernet Laptop	192.168.20.2/24	LAPTOP A
8	Ethernet Laptop	192.168.2.2/24	LAPTOP B

Konfigurasi STEP 2

ROUTER A

Berikan Penamaan pada Interface EoIP

```
[admin@MikroTik] > interface eoip add name=EoIP-LAB remote-address=192.168.2.1 tunnel
id=0
[admin@MikroTik] >
```

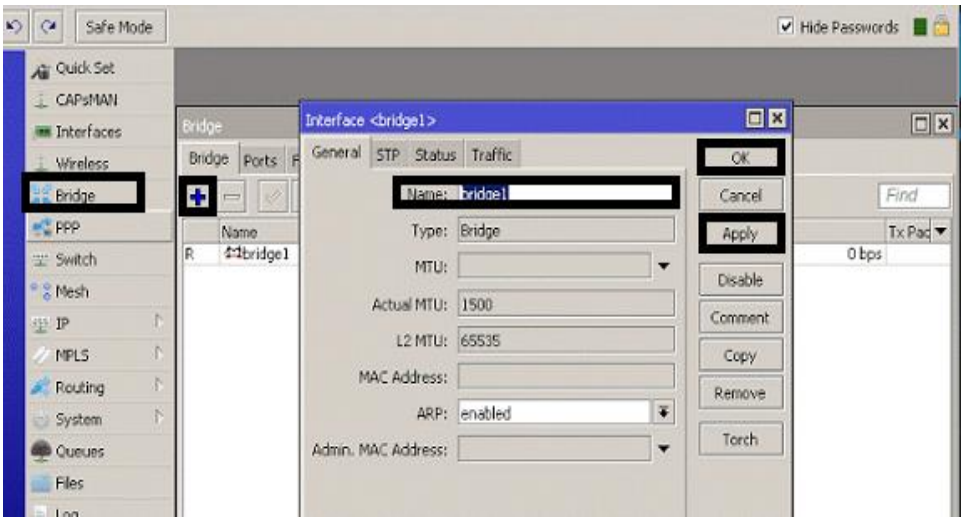


Gambar 6.22 Add Eoip

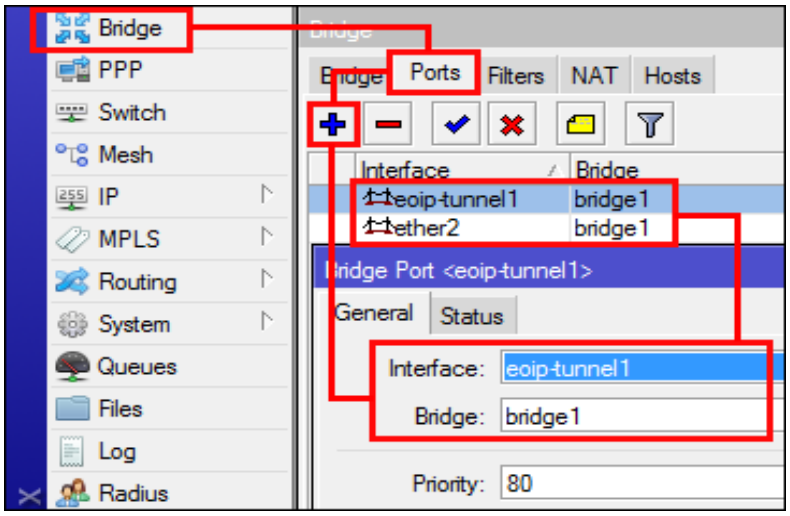
Konfigurasi STEP 3

Jika EoIP sudah berjalan dan muncul flag "R", selanjutnya kita buat bridge yang nanti akan menjembatani transmisi data dari jaringan LAN yang akan melewati EoIP. Masuk ke menu Bridge, kemudian klik tombol + (add). Isi nama bridge sesuai keinginan.

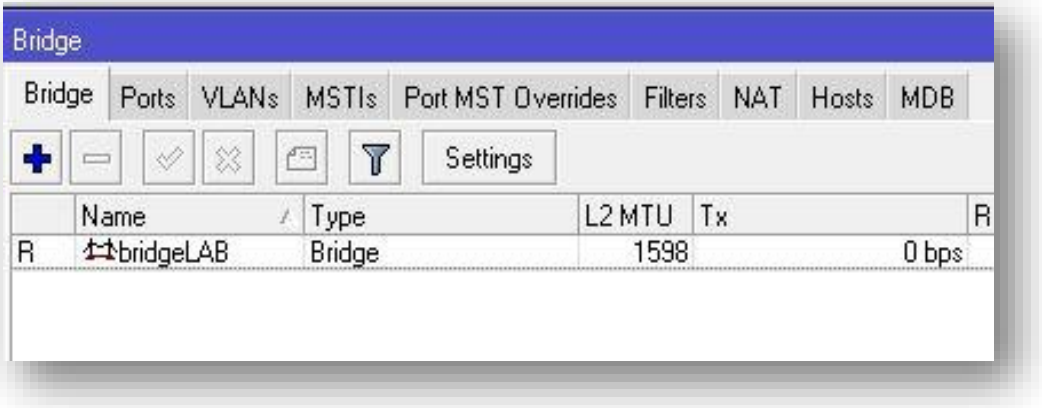
Buatlah Bridge untuk menghubungkan antara kedua Port berikan Penamaan pada bridge Jadikanlah Port Ethernet Lokal yang menuju ke Komputer Anda dan EoIP Tunnel menjadi bridge.



Gambar 6.23 Bridge setting 1

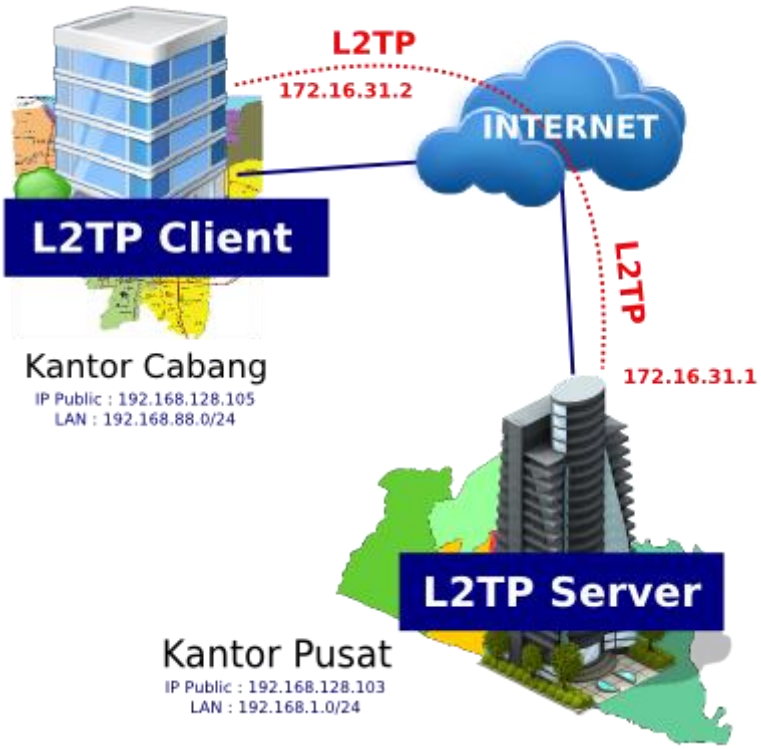


Gambar 6.24 Bridge setting 2



Gambar 6.25 Bridge setting 3

6.3.4 L2TP Tunelling



Gambar 6.26 L2TP Topologi
Sumber : mikrotik.co.id

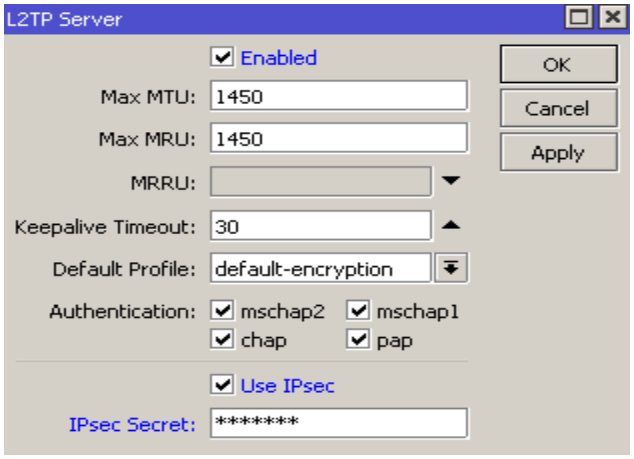
VPN mempermudah Anda apabila harus bekerja walau sedang berada di luar kantor. Anda dapat mengaksesnya dari jarak jauh seperti file,email dan database di kantor Anda dengan menggunakan jaringan VPN yang relatif lebih murah dan aman dibandingkan dengan mengkoneksikan diri langsung ke server kantor Anda atau mengirim file melalui Internet. Ada beberapa metode yang bisa digunakan VPN dalam mikrotik yaitu PPTP, SSTP, L2TP, dan OVPN namun kali ini kita akan menjelaskan metode L2TP (*Layer 2 Tunneling Protocol*) yang merupakan pengembangan dari PPTP dan secara umum lebih baik dan lebih aman.

Salah satu service VPN yang terdapat di Mikrotik adalah **L2TP** (*Layer 2 Tunneling Protocol*). L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi

daripada PPTP yg menggunakan MPPE. Trafik yang melewati tunnel L2TP akan mengalami overhead.

L2TP Server

Pertama, kita akan melakukan konfigurasi untuk *L2TP Server*. Untuk mengaktifkan router sebagai *L2TP server* caranya pun cukup mudah. Pada menu **PPP** -> Pilih **L2TP Server**. Maka akan tampak seperti tampilan berikut.



Gambar 6.27 L2TP Server

Kemudian centang opsi '**Enabled**'. Nah, secara otomatis L2TP Server telah aktif. Selanjutnya kita akan melakukan setting pada Tab **Secret**. Pilih Tab **Secret** -> Klik **Add [+]**.

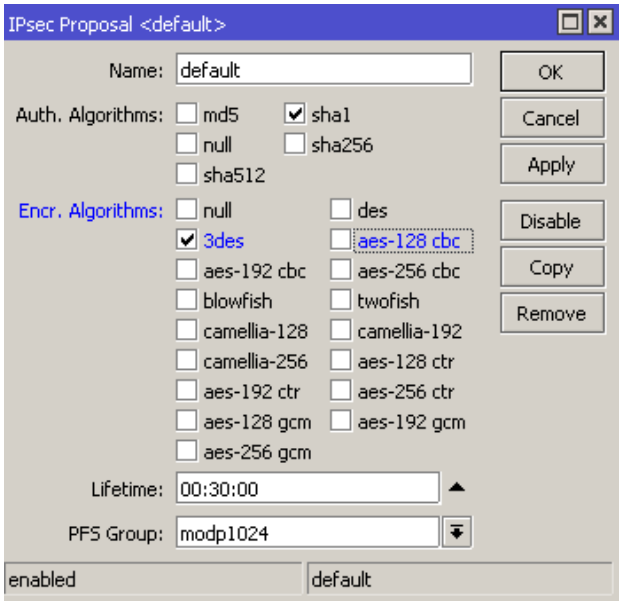
Gambar 6.28 PPP secret

Disini kita akan mengisi beberapa parameter standar yang utama untuk melakukan koneksi. Seperti '***Name & Password***' diisikan untuk dial koneksi L2TP dari client. Kemudian '***Service***' bisa diisikan dengan '***l2tp***' dan bisa juga dengan '***any***' untuk semua jenis service PPP. Dan parameter selanjutnya yang juga penting adalah setting Ip Address pada "***Local Address***" dan "***Remote Address***". IP

Address inilah yang nantinya kan ditambahkan secara otomatis ketika koneksi L2TP terbentuk dan sebagai gateway untuk komunikasi data. Kita juga bisa menambahkan pada parameter "***Route***" dengan mengisikan network dari 'Kantor Cabang", sehingga akan ditambahkan rule routing baru secara otomatis.

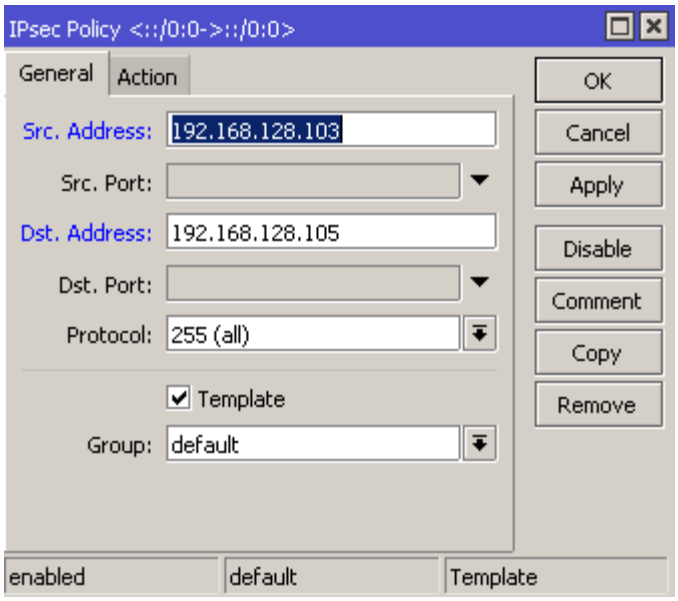
IPSec untuk L2TP Server

Untuk menambah tingkat keamanan kita akan memadukan L2TP dengan IPSec. Pilih pada menu IP -> IPSec. Kemudian kita akan melakukan setting terlebih dahulu pada tab 'IPsec Proposal'. Pada parameter yang tersedia kita isikan seperti tampilan gambar berikut.

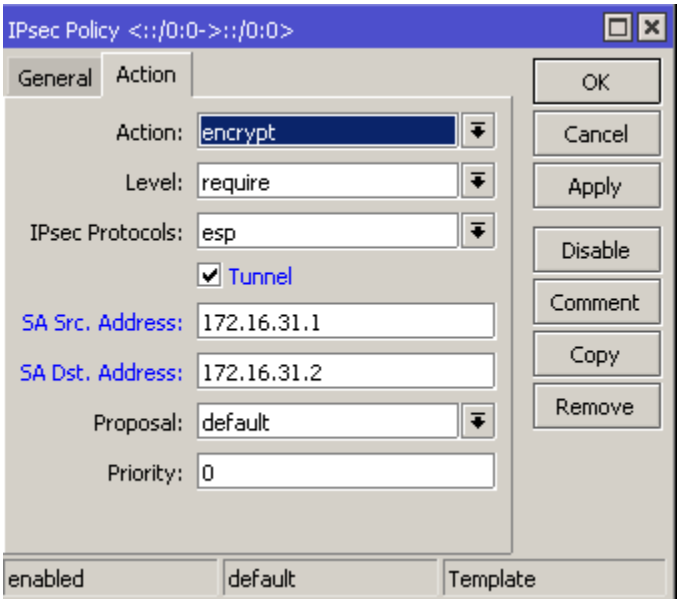


Gambar 6.29 IP sec Proposal

Selanjutnya kita melakukan setting pada Tab 'IPSec Policy'. Tambahkan juga parameter seperti pada tampilan berikut.

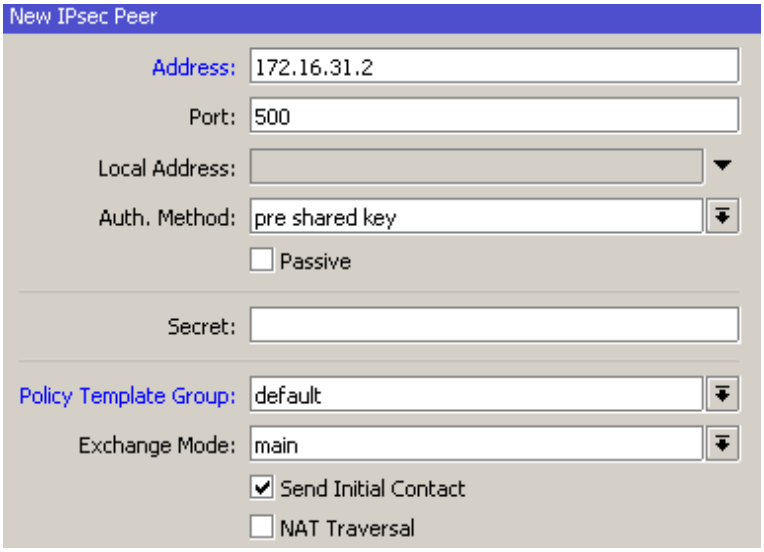


Gambar 6.30 IPsec Policy

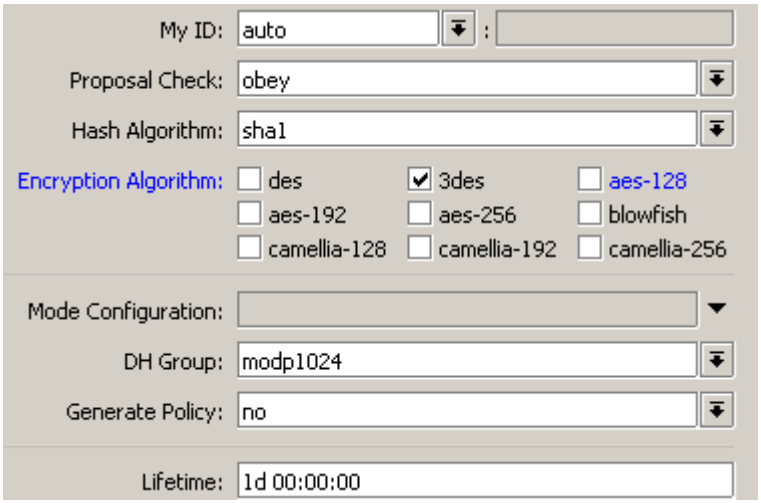


Gambar 6.31 IPsec policy 2

Setelah konfigurasi pada Tab 'IPSec Proposal' dan 'IPSec Policy' telah dilakukan, kita akan melanjutkan konfigurasinya pada Tab 'IPSec Peer'. Isikan sesuai dengan parameter seperti pada tampilan gambar berikut.



Gambar 6.32 IPSec Peer

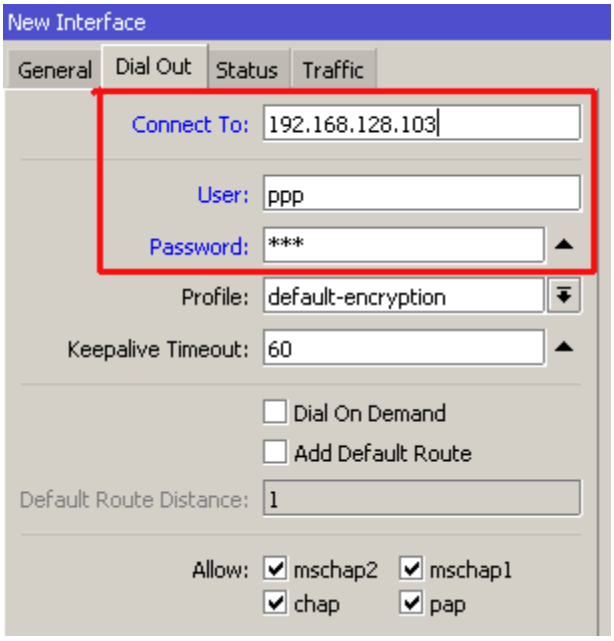


Gambar 6.33 IPSec peer 2

Nah, konfigurasi IPSec untuk L2TP Server sudah selesai.

L2TP Client

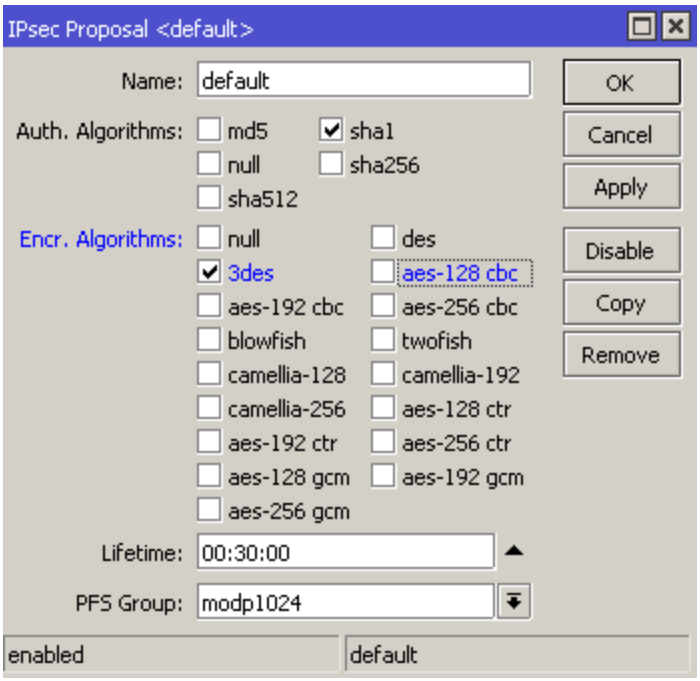
Setelah kita melakukan setting pada sisi L2TP Server, kita akan membuat L2TP Client. Untuk L2TP client kita tinggal melakukan dial ke L2TP server. Pilih menu **PPP** -> Klik **Add [+]** -> **L2TP Client**. Kemudian akan muncul tampilan seperti berikut.



Gambar 6.34 New Interface

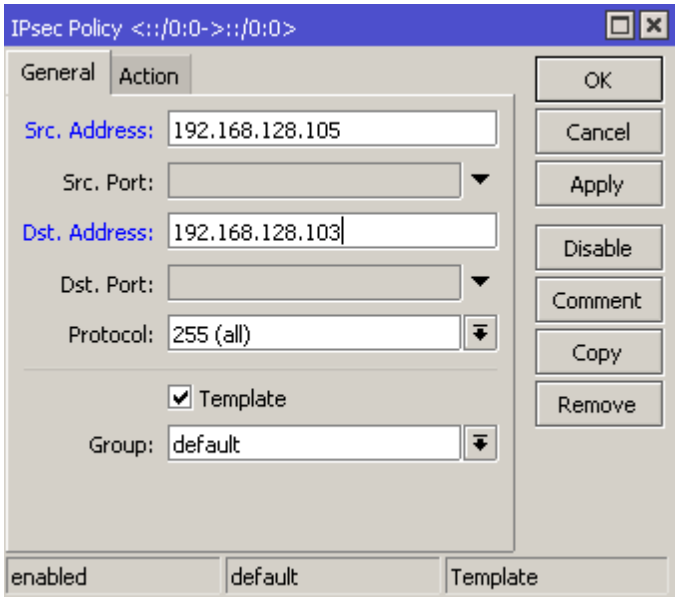
Isikan parameter yang ada. Diantaranya '**Connect To**' kita isikan dengan IP Public dari router di kantor pusat yang menjadi L2TP server. Kemudian parameter '**User & Password**' kita isikan seperti konfigurasi '**Secret**' di L2TP Server sebelumnya.

Sebelumnya kita sudah melakukan konfigurasi IPSec untuk L2TP Server. Dan sekarang kita juga akan melakukan konfigurasi untuk sisi L2TP Client. Pada dasarnya parameter yang digunakan antara IPSec baik sisi L2TP Server maupun Client sama, namun kita akan sedikit melakukan perubahan yaitu pada parameter IP Address. Pada Tab 'IPSec Proposal' tidak ada perbedaan dengan konfigurasi IPsec untuk L2TP Server.

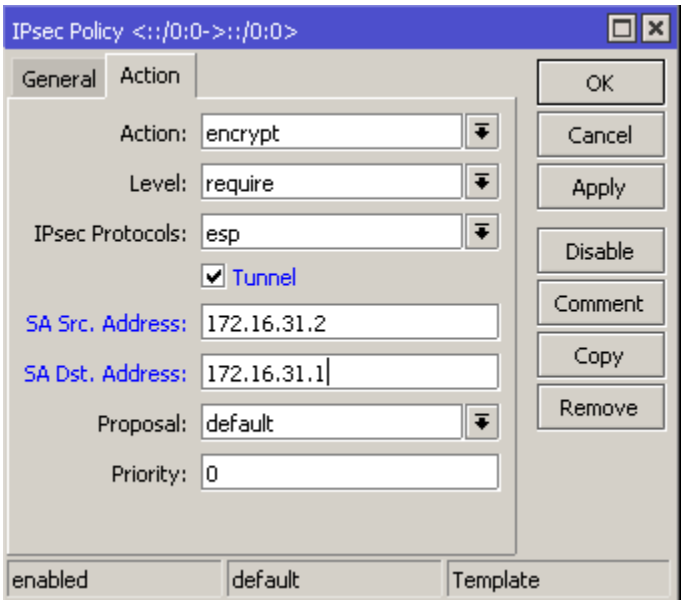


Gambar 6.35 IpSec Proposal

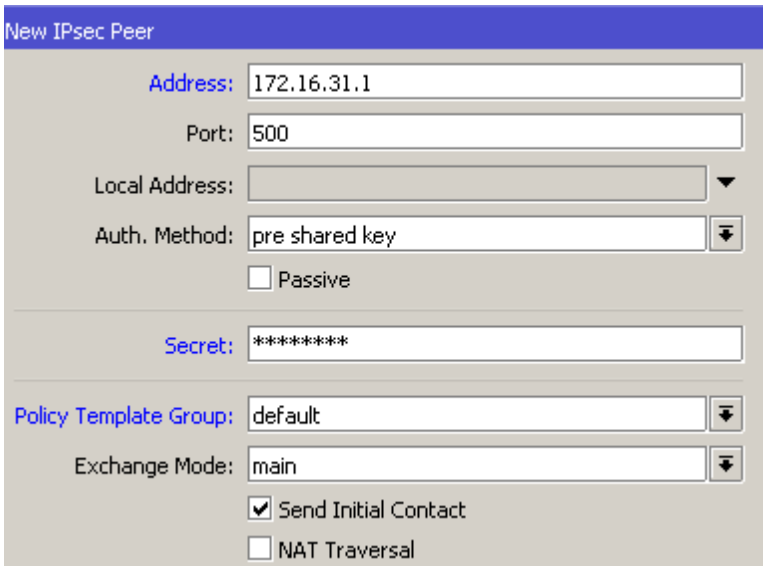
Kemudian untuk selanjutnya pada Tab 'IPSec Policy' kita akan mengganti IP Address dan untuk parameter yang lain kita samakan dengan IPsec di sisi L2TP Server.



Gambar 6.36 IPsec Policy

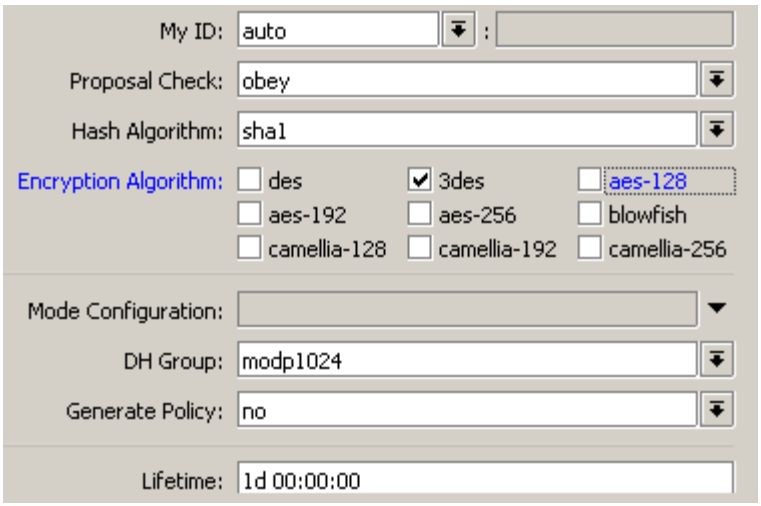


Gambar 6.37 IP policy 2



Gambar 6.38 New IP sec

Setelah kita setting 'IPSec Policy' maka kita akan melakukan setting juga untuk 'IPsec Peer'. Kita juga tinggal mengganti IP Address dan set parameter yang lain seperti halnya pada IPsec di sisi L2TP Server.

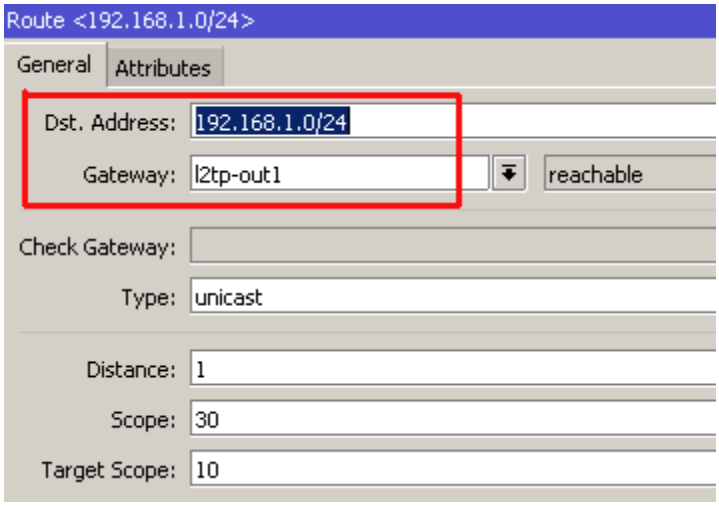


Gambar 6.39 Koneksi L2TP

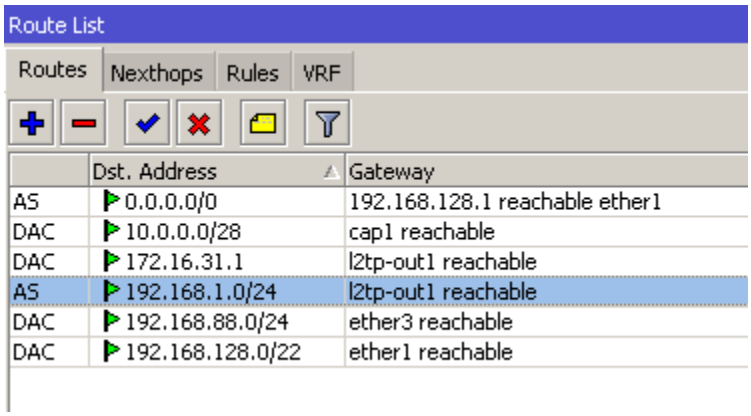
memerikasa apakah koneksi L2TP telah tersambung atau belum. Apabila konfigurasi benar dan tersambung maka akan tercantum pada info '*Status : Connected*' serta akan muncul sebuah interface baru dari L2TP

Interkoneksi Jaringan antara Kantor Pusat dengan Kantor Cabang

Jika koneksi L2TP telah terbentuk, saatnya kita akan melakukan setting untuk interkoneksi jaringan lokal melalui L2tp. Pada contoh kali ini, kita mempunyai jaringan local untuk '**Kantor Pusat**' dengan segment 192.168.1.0/24 dan pada '**Kantor Cabang**' dengan segment 192.168.88.0/24. Secara otomatis apabila koneksi L2TP terbentuk akan ditambahkan pada menu */IP Address* yaitu kombinasi dari "**Local Address**' dan "**Remote Address**" sesuai dengan konfigurasi Secret di L2TP Server sebelumnya. Agar jaringan local dari kedua sisi bisa saling komunikasi kita harus menambhakan rule routing baru. Penambahan rule tersebut harus dilakukan di kedua sisi baik di kantor pusat maupun di kantor cabang. Khusus untuk kantor pusat secara otomatis akan ditambahkan rule routing, karena kita sebelumnya telah menambahkan pada parameter '*Route*' di L2TP Server pada konfigurasi Secret. Nah, untuk disisi client kita tambahkan secara manual seperti pada tampilan berikut.



Gambar 6.39 Route L2tp



Gambar 6.40 Route List

Langkah terakhir untuk pengecekan apakah konfigurasi berjalan dengan baik, kita bisa melakukan traceroute atau ping dari PC/Laptop dari jaringan local di Kantor pusat ke kantor cabang dan juga bisa sebaliknya. Sebagai catatan, agar IPSec bisa berjalan dengan baik pastikan setting waktu kedua router sesuai dengan kondisi real-time. Perbedaan informasi waktu pada router dapat mengakibatkan kegagalan interkoneksi IPSec.

BAB VII
QOS

7.1. Quality of Services (QoS)

QoS tidak selalu berarti pembatasan *bandwidth.* QoS adalah cara yang digunakan untuk mengatur penggunaan bandwidth atau lebih familian dengan penyebutan bandwidth manajemen. Selain itu QoS juga biasa digunakan dalam pengaturan prioritas trafik berdasarakan parameter-parameter tertentu. Contohnya adalah jika di dalam sebuah perusahaan, staff administrasi hanya bertugas dalam kegiatan administratif. Maka, untuk staff administratif cukup di berikan bandwidth sedikit saja. Sedangnkan bagi seorang manager yang membutuhkan akses internet yang cepat, maka untuknya akan di berikan bandwidth yang lebih besar.

Menurut (Wijaya & Handoko, M.Kom, 2014) mengatakan bahwa, "Bandwidth adalah kapasitas atau daya tampung kabel ethernet agar dapat dilewati trafik paket data dalam jumlah tertentu". Sedangkan menurut (Sahari & Putra, 2015) memberikan batasan bahwa, "Bandwidth adalah besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui sebuah network". Dapat disumpulkan bahwa bandwidth adalah suatu besaran data yang dapat dilewati melalui jaringan dengan jumlah tertentu. Semakin besar bandwidth yang diberikan maka proses download dan upload akan berjalan lancar.

Dalam praktiknya, ada 2 cara dalam pengontrolan traffic ini, yaitu :

1. **Rate Limiting**, yaitu menolak semua paket yang masuk jika melebihi batas maksimal yang telah di tentukan.
2. **Rate Equalizing**, yaitu paket-paket yang masuk akan di tahan sementara jika melebihi batas maksimal, kemudian paket-paket tersebut akan di kirimkan kembali.

Selain itu, pada RouterOS juga dikenal 2 jenis limitasi, yaitu :

1. **CIR (Committed Information Rate)** :

   Dalam keadaan terburuk, client akan mendapatkan bandwidth sesuai dengan “limit-at” (dengan asumsi bandwidth yang tersedia cukup untuk CIR semua client).

2. **MIR (Maximal Information Rate)** :

   Jika masih ada bandwidth yang tersisa setelah semua client mencapai “limit-at”, maka client bisa mendapatkan bandwidth tambahan hingga “max-limit”.

Dalam MiktoTik RouterOS terdapat beberapa jenis QoS yang dapat digunakan. Masing-masing jenis QoS mempunyai mekanisme sendiri sendiri, berikut adalah macam-macam jenis QoS dalam MikroTik RouterOS :

1. Simple Queue

Pembatasan trafik tidak dapat dilakukan pada suatu interface. Satu-satunya cara untuk mengontrol adalah dengan buffering (menahan sementara). Selain itu jika paket yang berada dalam buffer telah melampaui limit buffer, akan dilakukan drop pada paket tersebut. Pada paket TCP, cara ini cukup efektif karena paket yang didrop akan dikirimkan ulang. Sehingga tidak ada kehilangan paket data. Cara termudah melakukan queue di RouterOS adalah menggunakan simple queue. Dengan menggunakan simpel queue, sebuah traffic dapat dilimit tx-rate-nya (untuk upload), rx-rate-nya (untuk download) dan tx+rx-rate-nya (akumulasi).

2. Brust

Burst adalah salah satu cara menjalankan QoS yang memungkinkan penggunaan data-rate yang melebihi max-limit untuk periode waktu tertentu. Jika data rate lebih kecil dari burst-threshold, burst dapat dilakukan hingga data-rate mencapai burst-limit. Setiap detik, router mengkalkulasi data rate rata-rata pada suatu kelas queue untuk periode waktu terakhir sesuai dengan burst-time. Perlu diingat bahwa burst time tidak sama dengan waktu yang diijinkan oleh router untuk

melakukan burst. Dalam Burst dikenal beberapa istilah penting yaitu burst-limit & burst-threshold.

3. **Per Connection Queue**

   Untuk kondisi client yang sangat banyak dan sangat merepotkan jika harus membuat banyak rule maka bisa menggunakan metode PCQ. PCQ dibuat sebagai penyempurnaan dari metode SFQ. Kelebihan PCQ adalah bisa membatasi bandwith untuk masing-maing client secara merata. Namun PCQ mempunyai kekurangan yaitu PCQ membutuhkan memori yang cukup besar.

4. **Queue Tree & Mangle**

   QueueTree adalah tool pada MikroTik RouterOS yang memiliki kemampuan untuk melimitasi bandwith yang lebih lengkap dibandingkan dengan simple-queue. Dengan QueueTree dimungkinkan untuk melakukan limitasi yang lebih fleksibel. Agar sebuah QueueTree dapat berjalan maka harus menggunakan Mangle yang dionfigurasikan terlebih dahulu.

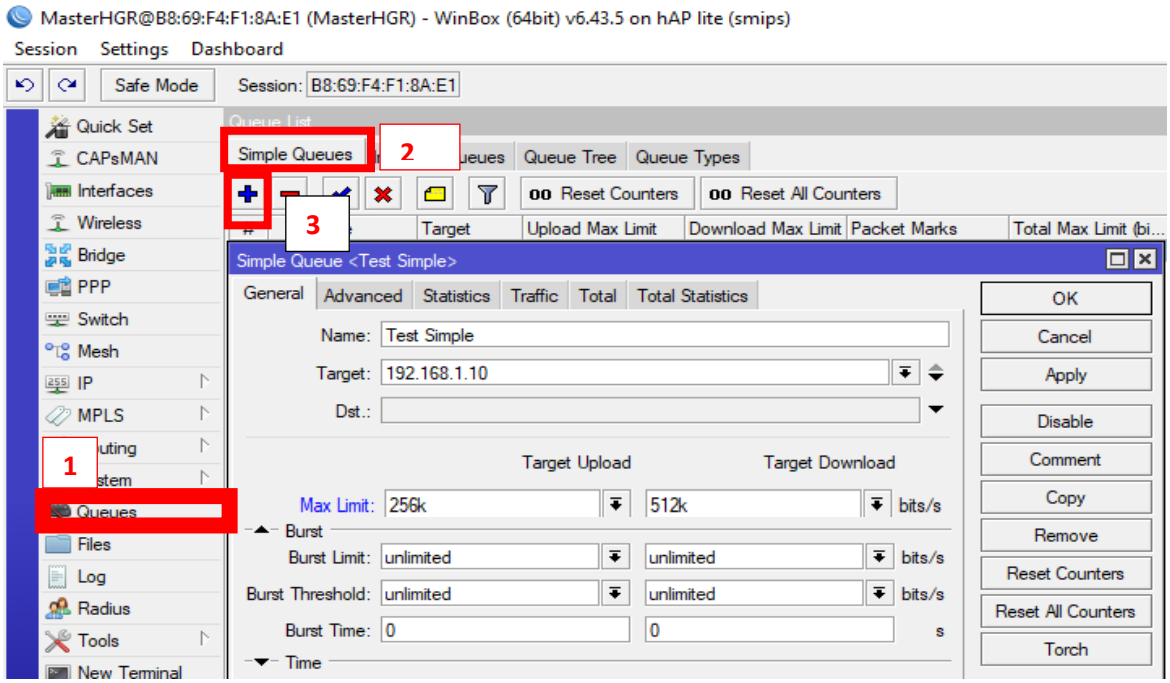
Namun pada modul ini, kami hanya akan membahas tentang Simple Queue dan Per Connectios Queue saja.

7.2. Simple Queue - Lab

Cara paling mudah untuk melakukan queue pada RouterOS adalah dengan menggunakan Simple Queue. Kita bisa melakukan pengaturan bandwidth secara sederhana berdasarkan IP Address client dengan menentukan kecepatan upload dan download maksimum yang bisa dicapai oleh client.

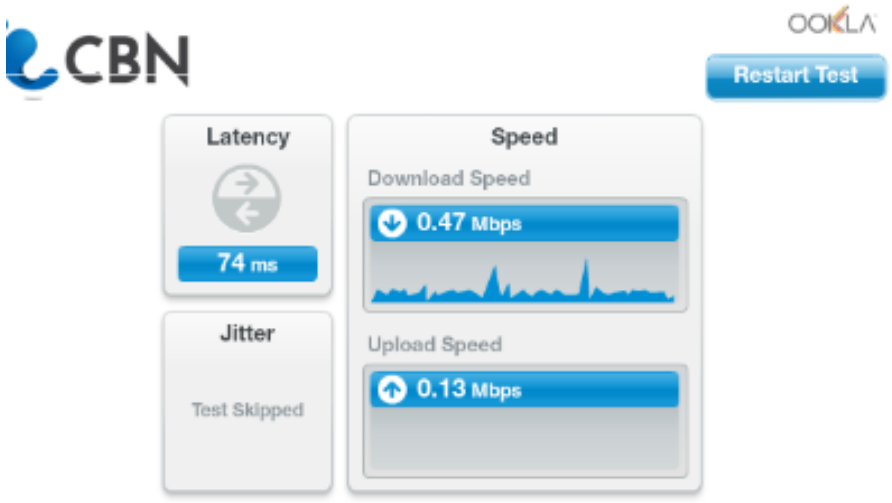
Sebagai contoh, kita akan melimitasi penggunaan bandwidth dengan sekenario target downloadnya adalah 512kbps dan upload 256kbps. Langkah-langkahnya sebagai berikut :

1. Buka winbox dana tur scenario queue seperti pada contoh kasus di atas. Queue → Simple Queue → + → General. Kemudian isikan target yang kita tuju dan besaran bandwidth yang kita inginkan. Jika sudah klik apply → OK



Gambar 7.1 Simple Queue

Dengan pengaturan tersebut maka Client dengan IP 192.168.1.10 akan mendapatkan kecepatan maksimum downloadnya adalah 512kbps dan upload 256kbps dalam keadaan apapun selama bandwidth memang tersedia. Setelah itu kita coba lakukan test pada user yang sudah kita buat tadi. Maka hasilnya akan seperti berikut ini.



Gambar 7.2 Hasil Test Client

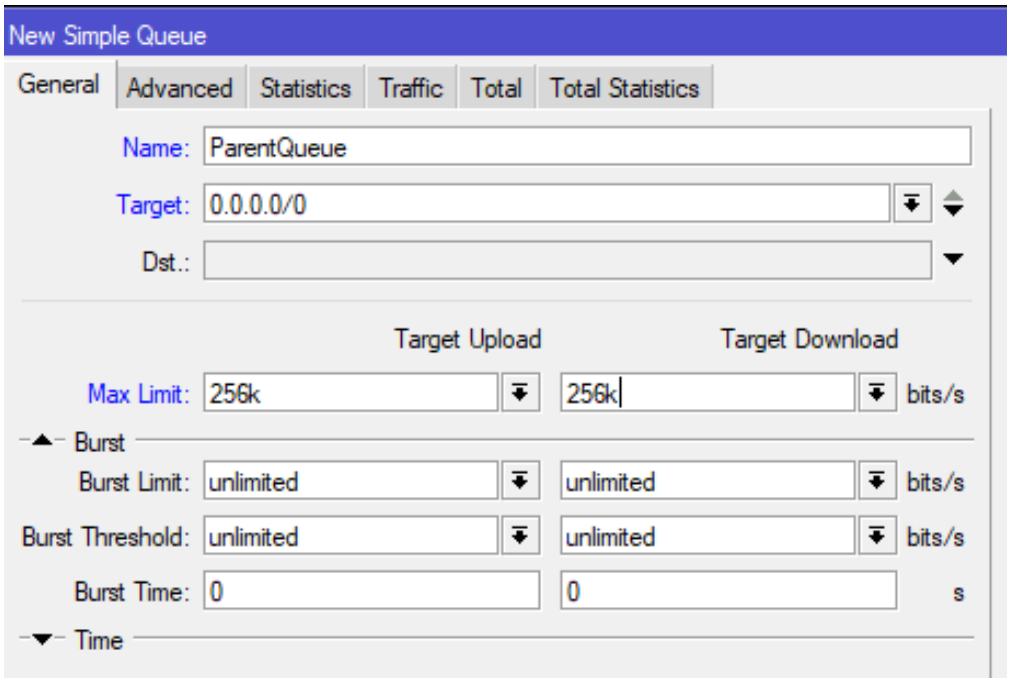
Selain digunakan untuk melakukan manajemen bandwidth fix seperti pada contoh sebelumnya, kita juga bisa memanfaatkan Simple Queue untuk melakukan pengaturan bandwidth share dengan menerapkan Limitasi Bertingkat.

Sebagai contoh kita akan melakukan pengaturan bandwidth sebesar 512kbps untuk digunakan 3 client. Sekenarionya sebagai berikut :

1. Dalam keadaan semua client melakukan akses, maka masing-masing client akan mendapat bandwidth minimal 128kbps.
2. Jika hanya ada 1 Client yang melakukan akses, maka client tersebut bisa mendapatkan bandwidth hingga 512kbps.
3. Jika terdapat beberapa Client (tidak semua client) melakukan akses, maka bandwidth yang tersedia akan dibagi rata ke sejumlah client yg aktif.

Router kita tidak tahu berapa total bandwidth real yang kita miliki, maka kita harus definisikan pada langkah pertama. Pendefinisian ini bisa dilakukan dengan melakukan setting Queue Parent.

Besar bandwidth yang kita miliki bisa diisikan pada parameter **Target Upload Max-Limit** dan **Target Download Max-Limit.**

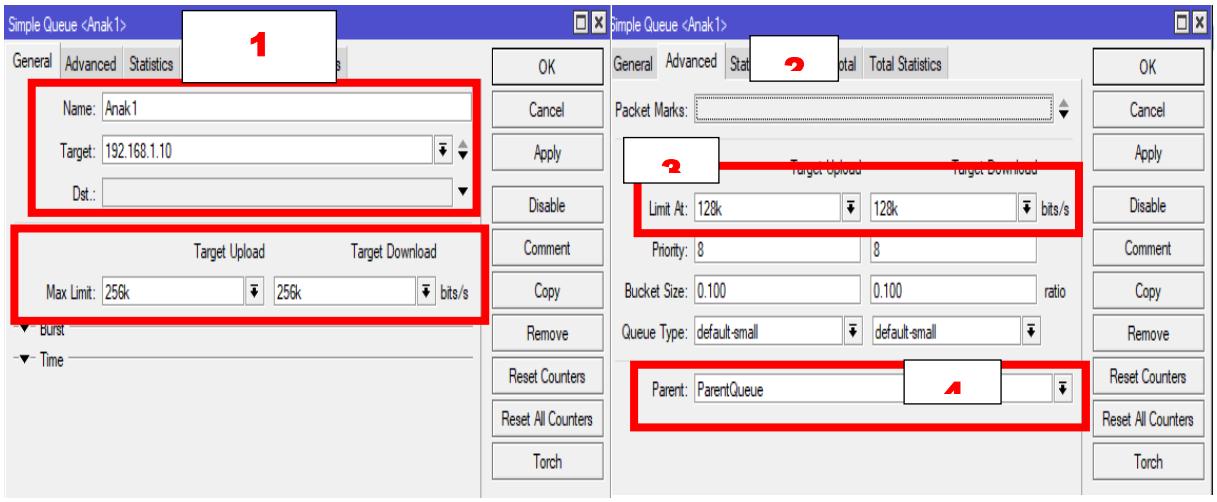


Gambar 7.3 Pengaturan Queue bertingkat

Langkah selanjutnya kita akan menentukan limitasi per client dengan melakukan setting child-queue. Pada child-queue kita tentukan target-address dengan mengisikan IP address masing-masing client. **Terapkan Limit-at (CIR) : 128kbps dan Max-Limit (MIR) : 512kbps**. Arahkan ke Parent Total Bandwidth yang kita buat sebelumnya, seperti pada contoh berikut ini :

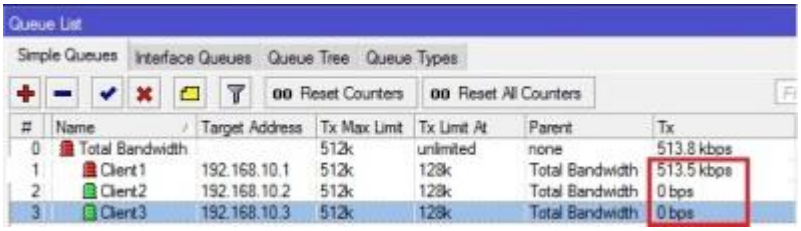
Konfigurasi awal sama seperti konfigurasi pada pembahasan sebelumnya. Setelah Queue Parent terbentuk, kemudian kita klik add lagi untuk menambahkan Queue anak. Masukan target download dan upload sebesar 256kbps. Kemudian klik tab Advanced, dan masukan target yang sama. Jangan lupa untuk memasukkannya ke dalam queue pqrent yang sudah kita buat dengan cara mengklik

combo box parent. Ulangi untuk memberikan limitasi pada client yang lain, sesuaikan Target-Address.



Gambar 7.4 Pengaturan client

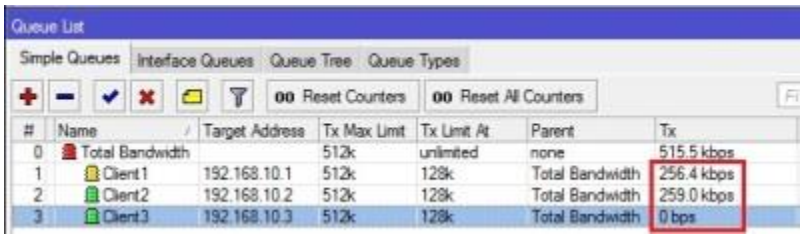
Selanjutnya lakukan pengetesan dengan melakukan download di sisi client. Pada gambar berikut menunjukkan perbedaan kondisi penggunaan bandwidth client setelah dilakukan limitasi bertingkat



Gambar 7.5 Pengetesan pada client 1

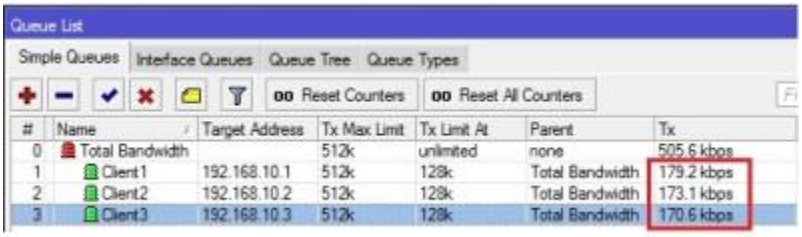
Gambar 7.5 menunjukkan ketika hanya 1 client saja yg menggunakan bandwidth, maka Client tersebut bisa mendapat hingga Max-Limit. Pertama Router akan memenuhi Limit-at Client yaitu 128kbps. Bandwitdh yang tersedia masih sisa 512kbps-128kbps=384kbps. Karena client yang lain

tidak aktif maka 384kbps yang tersisa akan diberikan lagi ke Client1 sehingga mendapat 128kbps+384kbps =512kbps atau sama dengan max-limit.



Gambar 7.6 Test Client 2

Gambar 7.6 menggambarkan ketika hanya 2 client yang menggunakan bandwidth. Pertama router akan memberikan limit-at semua client terlebih dahulu. Akumulasi Limit-at untuk 2 client = 128kbps x 2 =256kbps . Bandwidth total masih tersisa 256kbps. Sisa diberikan kemana.? Akan dibagi rata ke kedua Client. Sehingga tiap client mendapat Limit-at + (sisa bandwidth / 2) = 128kbps+128kbps =256kbps



Gambar 7.7 Test Clinet 3

Gambar 7.7 menunjukkan apabila semua client menggunakan bandwidth. Pertama Router akan memenuhi Limit-at tiap client lebih dulu, sehingga bandwidth yang digunakan 128kbps x 3 = 384kbps. Bandwidth total masih tersisa 128kbps. Sisa bandwidth akan dibagikan ke ketiga client secara merata sehingga tiap client mendapat 128kbps + (128kbps/3) = 170kbps.

7.3. Per Connection Queue (PCQ) – LAB

Simple queue bisa dikatakan sebuah solusi paling mudah dalam melakukan bandwidth management, sebagai admin jaringan kita hanya perlu isikan target address dengan ip komputer client kemudian kita tentukan bandwith yang dialokasikan untuk user tersebut. Permasalahan muncul jika ternyata user yang kita handle merupakan user dengan jumlah yang cukup banyak. Belum lagi jika user tersebut sifatnya dynamic. Mereka bisa konek ataupun disconnect sesuai kemauan mereka. Akan sangat repot jika kita harus membuat simple queue satu per satu. Salah satu fitur mikrotik yang dapat digunakan untuk mengatasi permasalah ini adalah dengan PCQ,

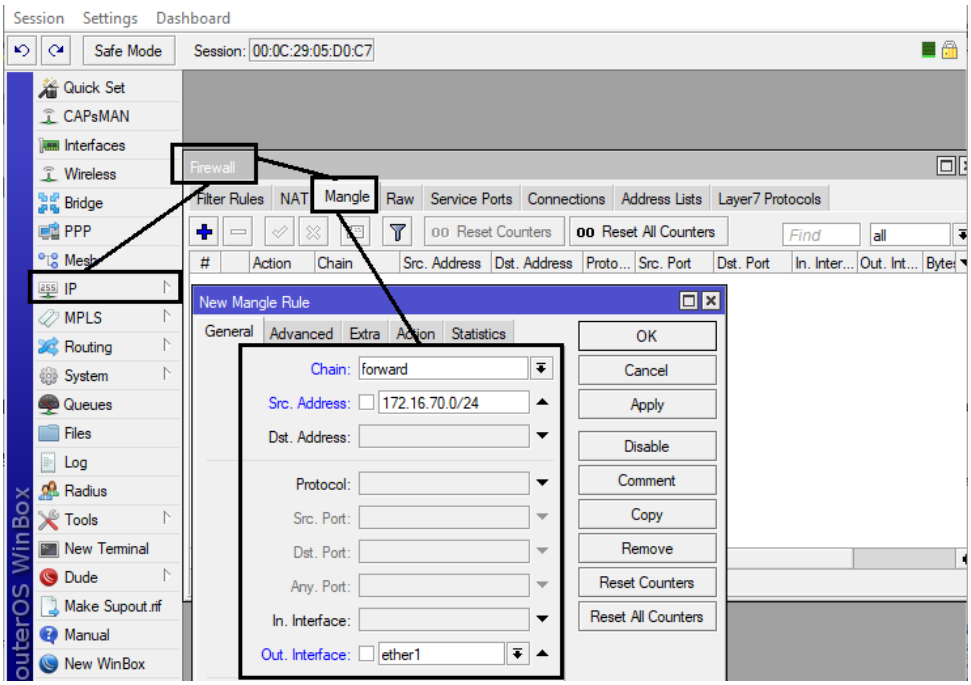
PCQ merupakan salah satu cara melakukan manajemen bandwidth yang cukup mudah dimana PCQ bekerja dengan sebuah algoritma yang akan membagi bandwidth secara merata ke sejumlah client yang aktif. PCQ ideal diterapkan apabila dalam pengaturan bandwidth kita kesulitan dalam penentuan bandwidth per client.

Misalnya, sebelumnya kita bisa melakukan bandwidth management dengan system HTB dimana jumlah client sedikit, maka masih mudah bagi admin jaringan dalam menentukan parameter limit-at. Tetapi bagaimana jika bandiwdth 1 Mbps namun ingin dibagi rata ke 200-an client. Jika menggunakan model HTB, akan sulit untuk menentukan limit-at . Dengan kondisi seperti ini, akan lebih mudah jika kita serahkan perhitungan management bandwidth ke router, agar Router yang akan membagi bandwidth secara otomatis ke client.

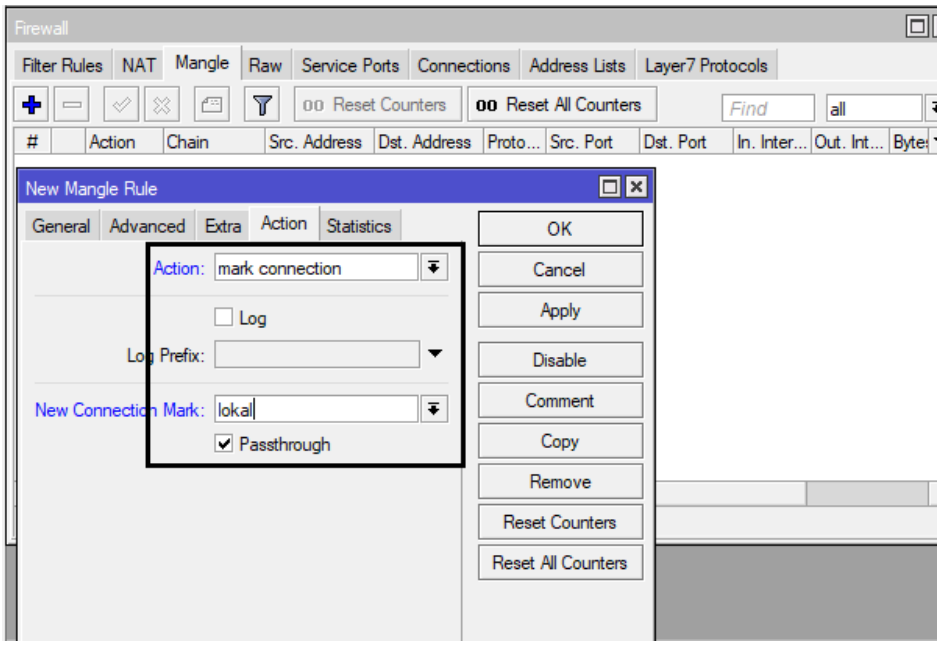
Sebagai Contohnya jika kita memiliki bandwidth sebesar 2Mbps jika terdapat 2 client pada satu jaringan maka masing-masing client akan mendapatkan kecepatan sebesar 1Mbps. Dan ketika 10 client menggunakannya secara bersamaan, maka pada kondisi tersebut setiap client akan mendapatkan bandwidth sekitar 200Kbps dengan rata.

Langkah – Langkahnya sebagai berikut :

1. Pilih IP – Firewall – Mangle klik “+” buat pengaturan pada General untuk Chain kita gunakan Forward lalu Src.Address adalah IP lokal 172.16.70.0/24 kemudian untuk Out. Interface kita pilih ether1. Kita pindah ke menu action pada action kita pilih mark connection dan beri judul pada New Mark Connection lalu ceklis pada passthrough.

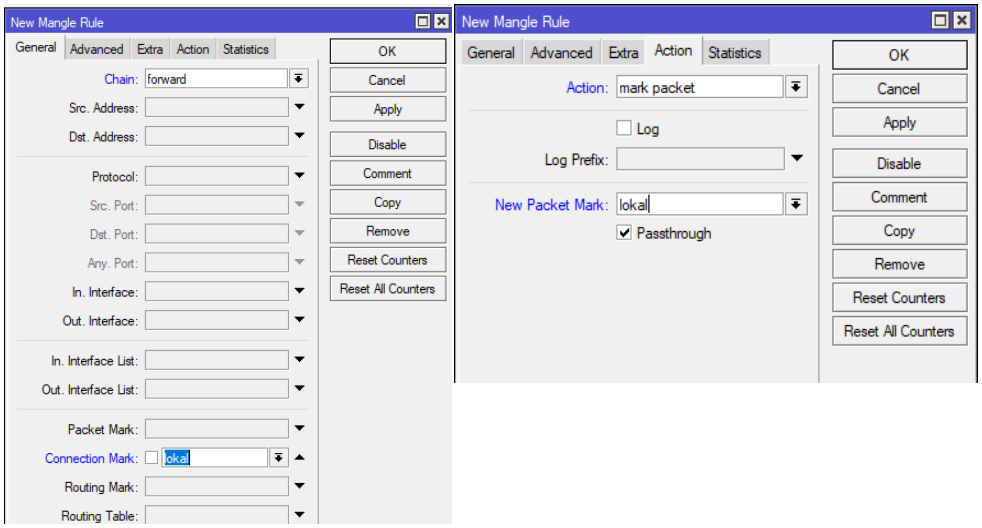


Gambar 7.8 Penyetingan PCQ



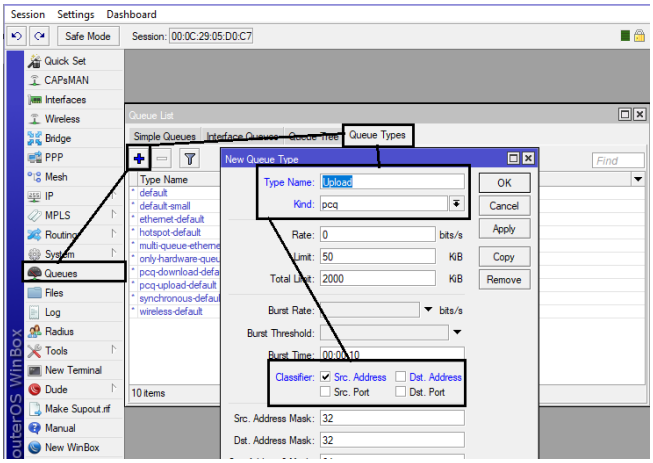
Gambar 7.8 Penyetingan Mangle

2. Selanjutnya hampir sama seperti langkah pertama hanya saja disini kita hanya memilih Chain menjadi forward dan Connection Mark nya kepada mark connection yang sudah dibuat sebelumnya. Lalu ke menu action kita pilih mark pakcet dan kita buat nama new packet mark nya.



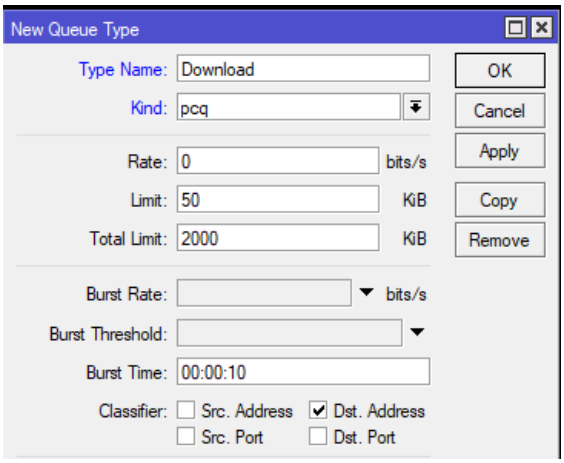
Gambar 7.9 Penyettingan Mangle rule

3. Masuk ke menu Queues pilih Queue Types dan klik “+” kita buat Type Name berikan nama Upload dan Kind kita pilih PCQ lalu pada classifier ceklis pada Src. Address dan pilih OK.



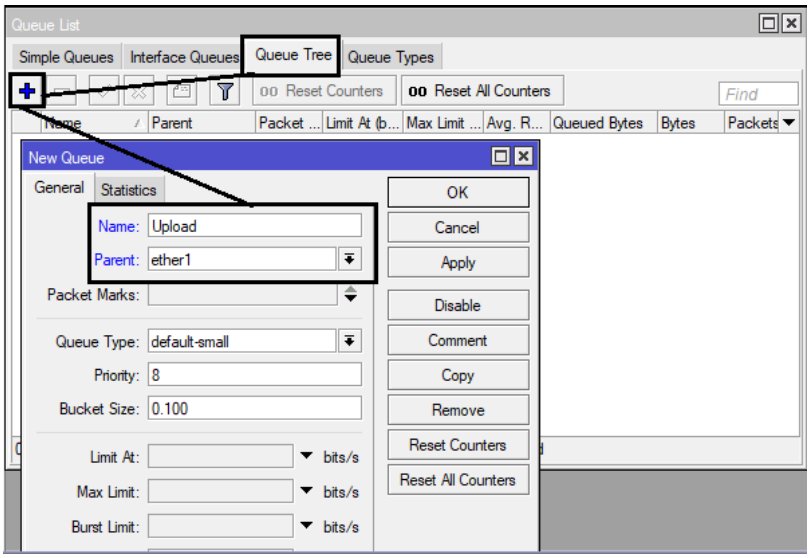
Gambar 7.10 Penyettingan PCQ

Dan untuk selanjutnya hampir sama dengan sebelumnya hanya saja disini kita buat untuk download dan pada Classifier kita pilih Dst. Address.



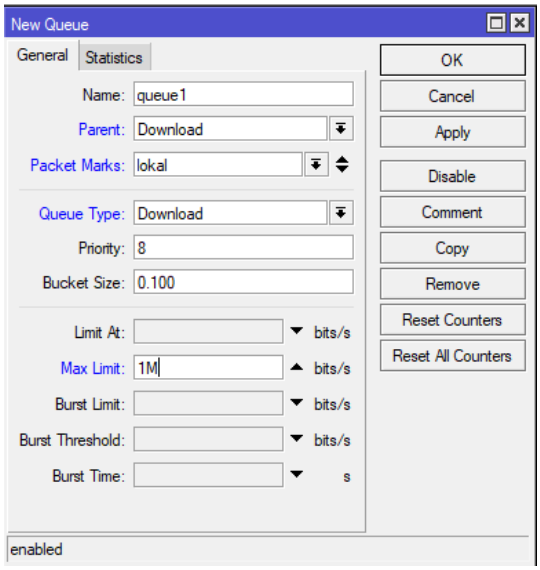
Gambar 7.11 Setting download PCQ

4. Pada langkah ini kita pilih pada Queue Tree lalu pada Name kita berikan nama Upload dan pada Parent kita pilih ether1. Selanjutnya kita ulangi kembali hanya saja pada Name kita berikan Download dan Parent kita pilih ether2.



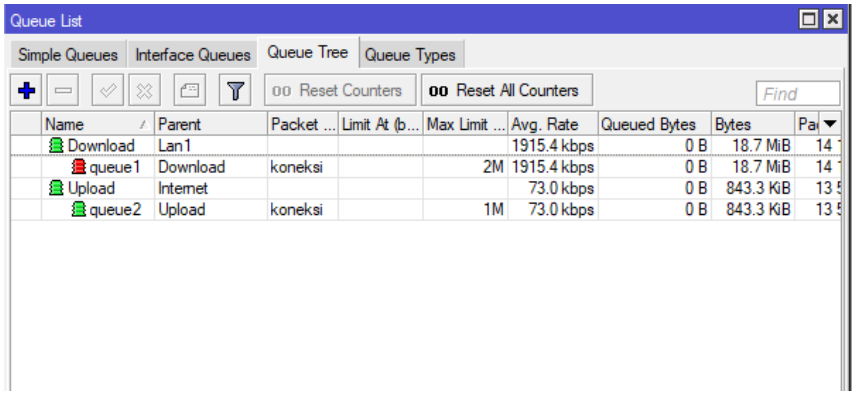
Gambar 7.12 Queue Tree

5. Pada langkah ini kita membuat batasan bandwidth dengan menentukan dengan mengisi Parent menjadi Download lalu untuk Packet Marks kita pilih sesuai yang sudah kita buat tadi dan untuk Queue Type nya menjadi Download selanjutnya Max. Limit kita sesuaikan dengan bandwidth yang kita miliki.



Gambar 7.13 Limitasi Bandwidth

Dengan hasil akhir nya sebagai berikut:



Gambar 7.14 Hasil Akhir

7.4 QUEUE LANJUTAN

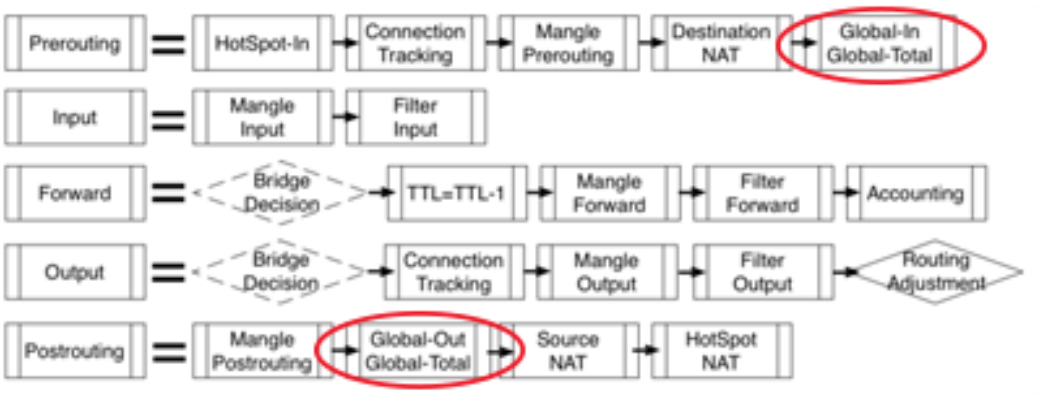
Management Bandwidth merupakan implementasi dari proses mengantrikan data, sehingga fungsi management bandwidth di Mikrotik disebut dengan istilah Queue. Ada dua metode Queue pada Mikrotik yaitu Simple Queue dan Queue Tree. Kedua metode tersebut memanfaatkan Memory/RAM di router sebagai buffer penampungan antrian paket data. Jika antrian paket data sudah memenuhi penampungan maka paket data yang tidak tertampung akan di Drop. Jika protocolnya TCP, paket yang di drop akan dikirim ulang oleh server.

Baik Simple Queue maupun Queue Tree memiliki keunggulannya masing-masing. Simple Queue, seperti namanya, cukup mudah dalam melakukan konfigurasi. Jika kebutuhannya untuk melakukan limitasi berdasarkan target IP Address atau interface, maka Simple Queue merupakan pilihan yang tepat. Sehingga kita tidak disibukkan dengan pengaturan mangle.

Sedangkan Queue Tree, seperti yang sudah dijabarkan sebelumnya harus menggunakan Mangle, harus sangat cermat dalam pembuatannya. Namun jika kebutuhan Queue lebih detail berdasarkan service, protocol, port, dsb maka Queue Tree adalah jawabannya. Simple Queue juga memiliki parameter mark-packet, namun dari sisi management akan lebih mudah jika mark-packet diterapkan pada Queue Tree.

Untuk mengetahui lebih detail, kita akan melihat alur proses yang terjadi di dalam Router. Di bawah ini merupakan gambaran aliran proses paket data (packet flow) RouterOS versi5. Proses

pembacaan Queue dilakukan pada Global-in (prerouting) dan Global-Out (postrouting).

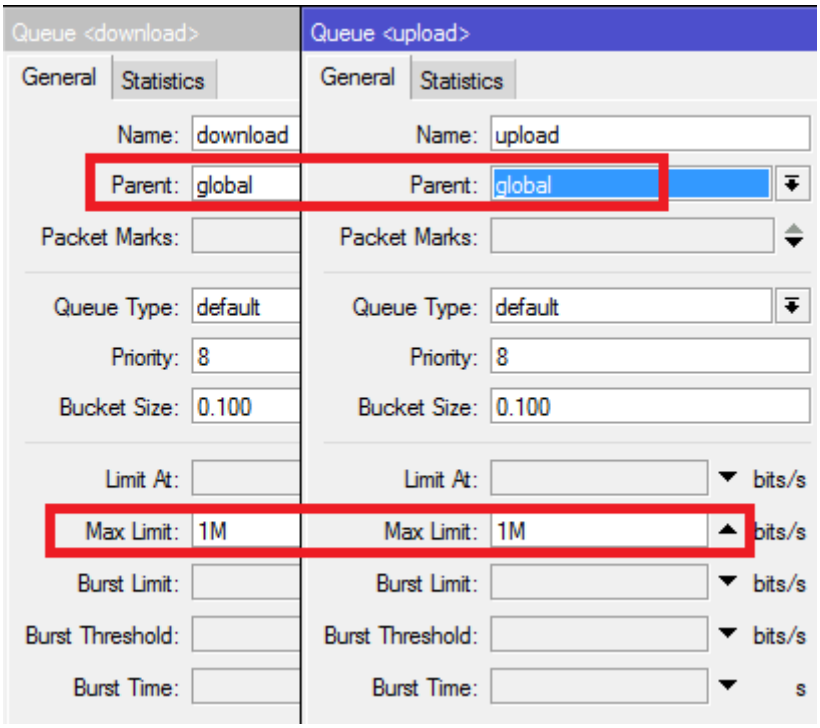


Gambar 7.15 Pembacaan Queue

7.5 Mangle pada queue tree

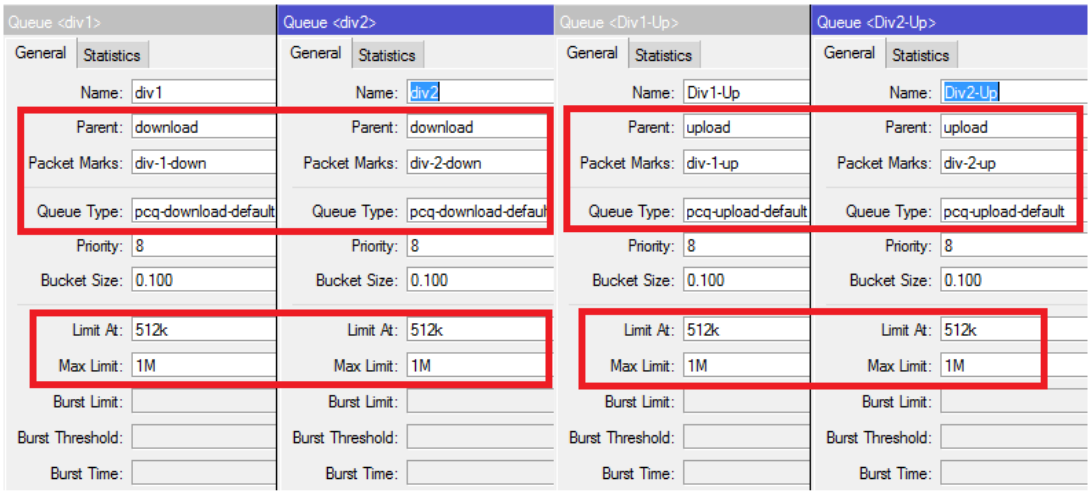
Mangle pada Firewall mikrotik dapat digunakan untuk manandai packet data. Tanda (marking) tersebut bisa digunakan pada fitur lain seperti Filter, Routing, NAT, ataupun Queue. Pada implementasi di lapangan mangle bisa digunakan untuk melakukan loadbalance, Router yang melakukan loadbalance biasanya merupakan router Utama yang juga digunakan untuk melakukan management bandwidth.

Queue Tree dapat dibuat dengan metode hirarki parent dan child. Maka parent menggunakan max-limit sesuai akumulasi 2 layanan internet yang dimiliki. Sebagai contoh pada kasus ini setiap ISP memberikan bandwidth 512k.



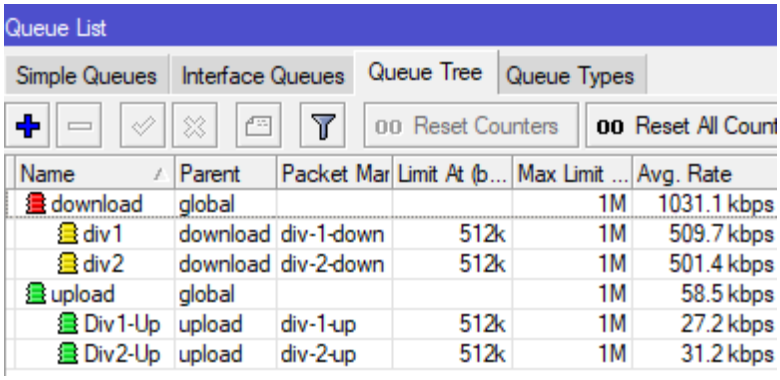
Gambar 7.15 Parent queue tree

Kemudian child bisa menggunakan kombinasi dengan PCQ di Queue Type-nya untuk memberikan pembagian secara merata jika di setiap LAN ada banyak user di dalamnya.



Gambar 7.16 child queue tree

Sehingga kedua LAN bisa berbagi bandwidth dengan metode HTB tanpa mepertimbangkan trafik tersebut melewati gateway ISP yang mana.



Gambar 7.17 queue tree

Jika LAN 1 tidak menggunakan bandwidth maka bisa digunakan oleh LAN 2, begitu pula sebaliknya. Jika kedua Online secara bersamaan akan dibagi sama besar.

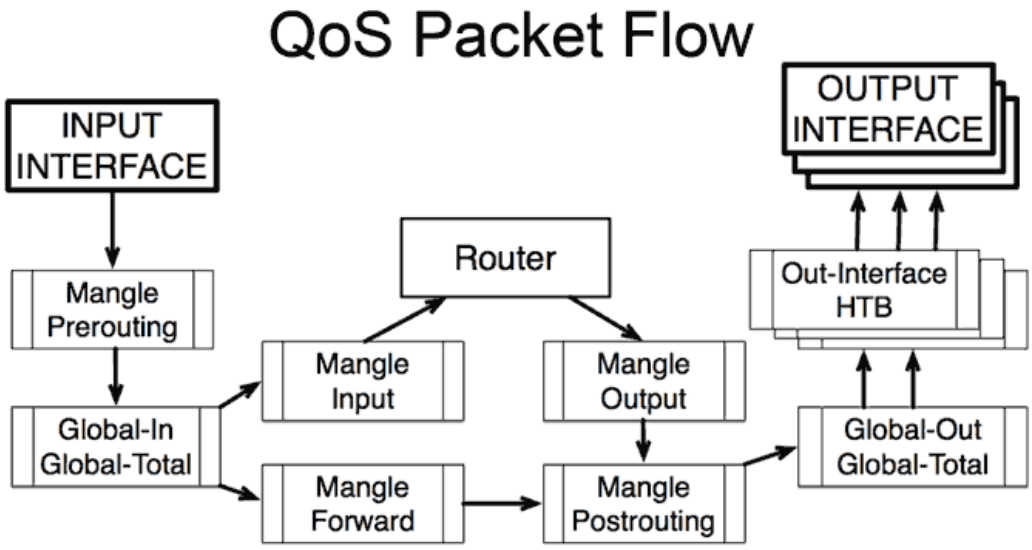
Mangle structure

1. Mangle diatur dan diorganisasikan chains
2. Ada 5 built in chain mangle dalam mikrotik :

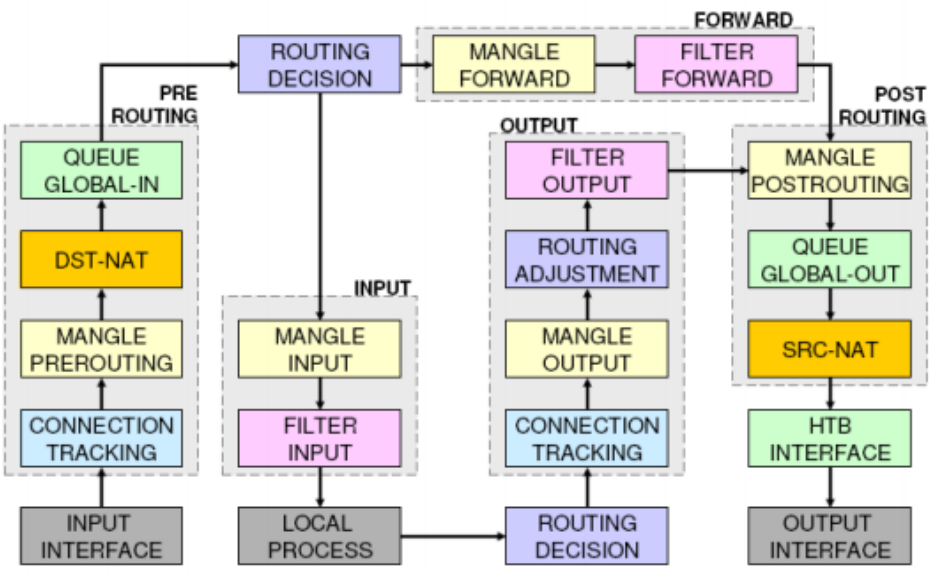
- Prerouting-making a mark before global-in queue
- Postrouting-making a mark before global out queue
- Input – making a mark before input filter
- Output- making a mark before output filter
- Forward – making a mark before forward filter

3. Jika dibutuhkan user dapat membuat chain baru dengan nama tertentu

7.6 QOS Packet Flow



Gambar 7.18 QOS Packet Flow



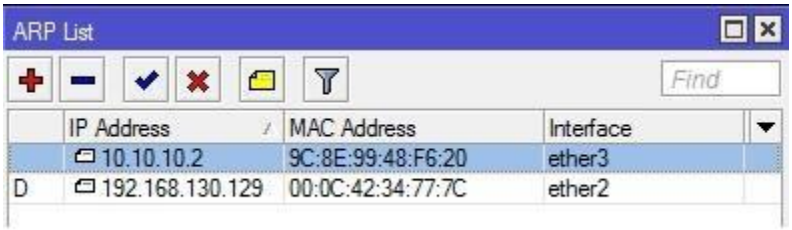
Gambar 7.19 Packet Flow

BAB VIII
NETWORK MANAGEMENT

8.1. ARP

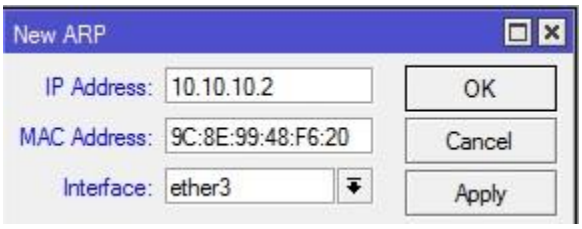
Pernahkah anda menerapkan konsep pengelompokan kebijakan Client pada jaringan lokal berdasarkan IP Address.? Misalnya, anda buat limitasi bandwidth yang berbeda antara Group IP Manajemen dengan Group IP Karyawan pada sebuah kantor. Anda berikan bandwidth yang besar untuk Group Manajemen, sedangkan untuk Karyawan anda berikan kecil. Penerapan konsep tersebut akan efektif ketika pemakaian IP Address sesuai. Akan tetapi bagaimana jika Karyawan mengganti IP PC mereka menjadi IP yang seharusnya digunakan oleh Manajemen.? Maka Karyawan akan mendapatkan bandwidth yang besar sesuai limitasi untuk group Manajemen. Kita bisa menerapkan sebuah konsep, ketika client mengubah IP Address pada PC, Router tidak akan memberikan response terhadap request client tersebut sehingga client malah tidak bisa melakukan akses ke jaringan lain (internet). Kita bisa memanfaatkan ARP untuk menerapkan konsep tersebut.

Sebuah router memiliki tabel ARP yang berisi entri ARP. Entri ARP terdiri dari alamat IP dan alamat hardware (MAC Address) yang sesuai . Pada Router Mikrotik tabel ARP bisa dilihat pada menu /ip arp



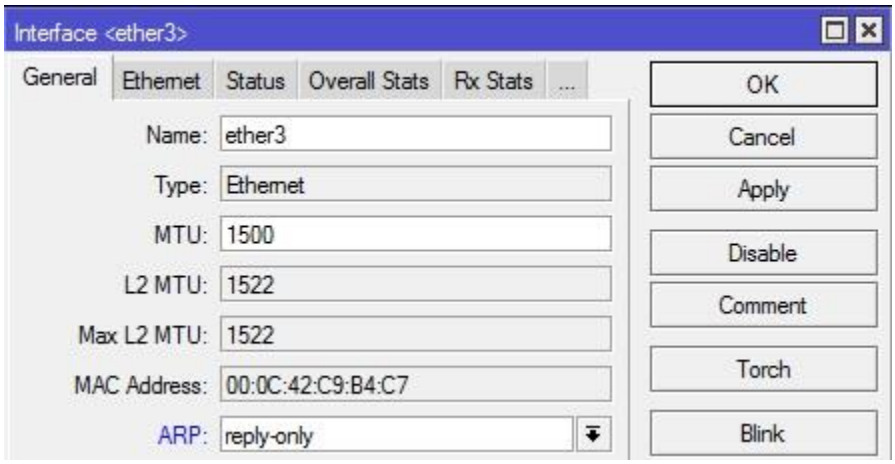
Gambar 8.1 Tabe; ARP

By default, entri ARP ini akan ditambahkan secara otomatis oleh interface Router ketika ada perangkat yang terkoneksi pada interface tersebut (dynamic ARP). Akan tetapi, untuk meningkatkan keamanan jaringan, kita bisa menambahkan entri ARP ini secara manual (Static ARP).



Gambar 8.2 Manual Input ARP

Selanjutnya ubah setting pada interface lokal menjadi arp=reply only.



Gambar 8.3 Mengaktifkan ARP pada sebuah Ether

Pada kondisi ini, interface Router hanya akan meresponse request client dengan kombinasi IP Address dan MAC Address yang sesuai dengan tabel ARP, tanpa menambahkan entri ARP secara otomatis.

Karyawan tidak lagi bisa menggunakan IP Address Manajer. Saat karyawan mengubah IP Adress kombinasi yang terbentuk tidak sesuai dengan ARP Tabel.Konsep ini bisa juga digunakan untuk mencegah IP Address lain yang tidak dikehendaki menggunakan akses jaringan kita.

Interface ARP Mode:

1. Enable

   Mode ini default enable pada semua interface di MikroTik. Semua ARP akan ditemukan dan secara dinamik ditambahkan dalam ARP tabel

2. Proxy ARP

   Router dengan mode ARP proxy akan bertindak sebagai transparan proxy ARP antara dia atau lebih jaringan yang terhubung langsung.

3. Reply Only

   ARP reply-only memungkinkan router hanya kan mereply ARP statis ditemukan di table ARP, akses ke router dan ke jaringan di belakang router hanya dapat diakses oleh kombinasi Ip dan mac address yang ditemukan di tabel ARP

4. Disable

   permintaan ARP dari klien tidak dijawab oleh router. Oleh karena itu, statis arp entri harus ditambahkan disamping disisi router juga disisi client. misal pada Windows menggunakan perintah arp:

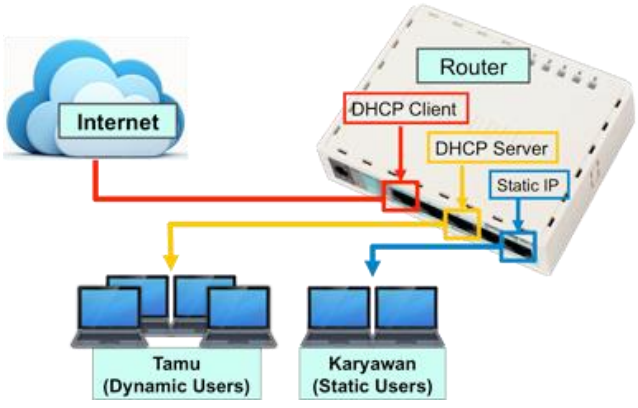
   C: \> arp-s 192.168.2.1 00-aa-00-62-c6-09

8.2. DHCP Server

Dynamic Host Configuration Protocol (DHCP) merupakan service yang memungkinkan perangkat dapat mendistribusikan/assign IP Address secara otomatis pada host dalam sebuah jaringan. Cara kerjanya, DHCP Server akan memberikan response terhadap request yang dikirimkan oleh DHCP Client.

Selain IP Address, DHCP juga mampu mendistribusikan informasi netmask, Default gateway, Konfigurasi DNS dan NTP Server serta masih banyak lagi custom option (tergantung apakah DHCP client bisa support).

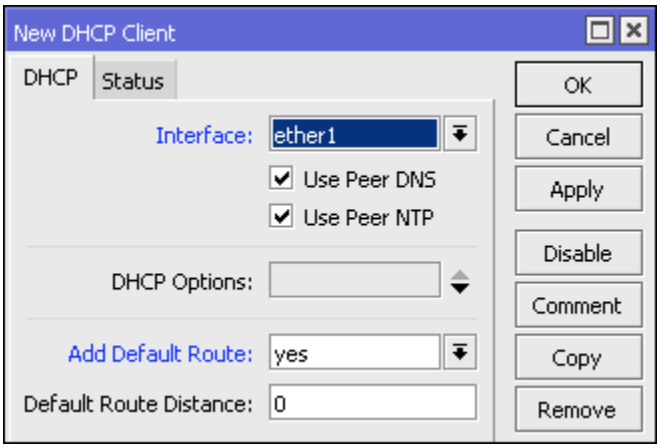
Mikrotik dapat digunakan sebagai DHCP Server maupun DHCP Client atau keduanya secara bersamaan. Sebagai contoh, misalnya kita berlangganan internet dari ISP A. ISP A tidak memberikan informasi IP statik yang harus dipasang pada perangkat kita, melainkan akan memberikan IP secara otomatis melalui proses DHCP.



Gambar 8.4 Skema DHCP

1. Mikrotik sebagai DHCP Client

Dalam kasus ini, untuk dapat memperoleh alokasi IP Address dari ISP, yang nantinya dapat digunakan untuk terkoneksi ke internet, kita bisa menggunakan fitur DHCP Client. Langkah-langkah pembuatan DHCP Client dapat dilakukan pada menu IP -> DHCP Client -> Add.



Gambar 8.5 DHCP Client

Untuk pengaktifkan DHCP Client, definisikan parameter interface dengan interface yang terhubung ke DHCP Server, atau dalam kasus ini adalah interface yang terhubung ke ISP. Karena kita ingin semua traffic ke internet menggunakan jalur koneksi dari ISP, maka Use-Peer-DNS=yes dan Add-Default-Route=yes.

Terdapat beberapa parameter yang bisa disesuaikan dengan kebutuhan jaringan;

a. Interface : Pilihlah interface yang sesuai yang terkoneksi ke DHCP Server
b. Use-Peer-DNS : Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
c. Use-Peer-NTP : Bila kita hendak menggunakan informasi pengaturan waktu di router (NTP) sesuai dengan informasi dari DHCP

d. Add-Default-Route : Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP

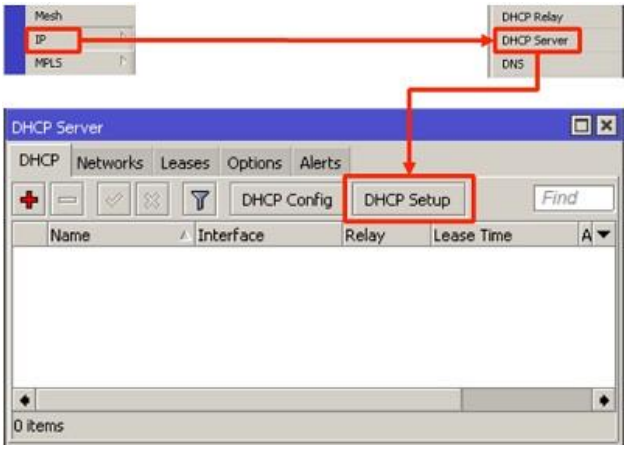
e. Default-Route-Distance : Menentukan nilai Distance pada rule routing yang dibuat secara otomatis. Akan aktif jika add-default-route=yes

Sampai langkah ini, seharunya Router sudah bisa akses ke internet. Selanjutnya lakukan setting DHCP Server untuk distribusi IP Address ke arah jaringan lokal /LAN.

2. Mikrotik sebagai DHCP Server

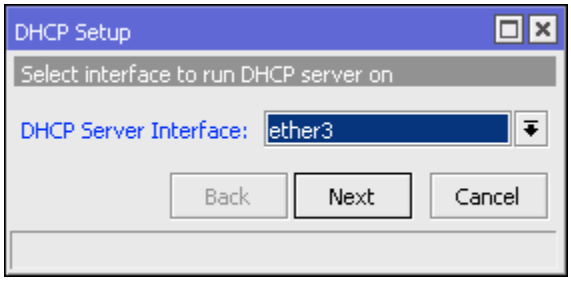
DHCP Server akan sangat tepat diterapkan jika pada jaringan memiliki user yang sifatnya dinamis. Dengan jumlah dan personil yang tidak tetap dan selalu berubah. Jika pada kasus ini sifat user seperti itu dapat kita temui pada tamu yang berkunjung.

Konfigurasi DHCP Server dapat dilakukan pada menu IP -> DHCP Server -> Klik DHCP Setup



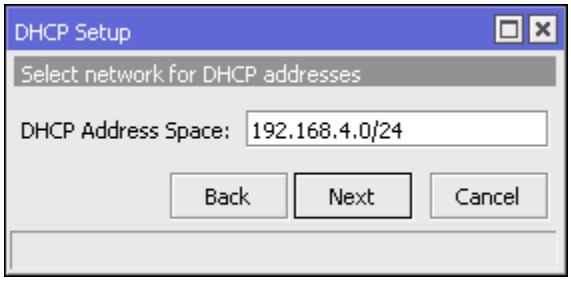
Gambar 8.6 DHCP Server

Dengan menekan tombol DHCP Setup, wizard DHCP akan menuntun kita untuk melakukan setting dengan menampilkan kotak-kotak dialog pada setiap langkah nya.



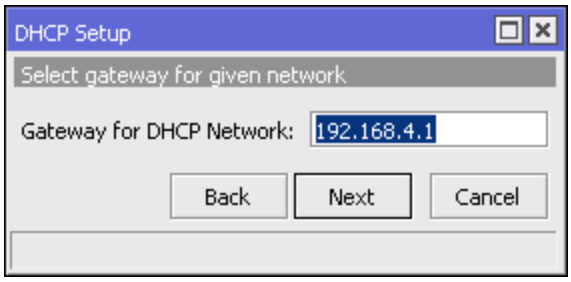
Gambar 8.7 DHCP Server Target DHCP

Langkah pertam, kita diminta untuk menentukan di interface mana DHCP Server akan aktif. Pada kasus ini DHCP Server diaktifkan pada ether3. Selanjutnya Klik Next



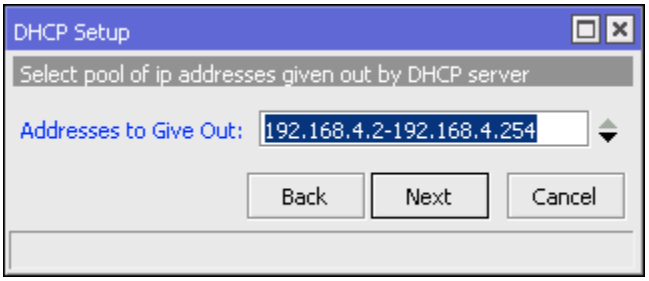
Gambar 8.8 DHCP Server Space

Sebelumnya pada ether3 sudah dipasang IP Address 192.168.4.0/24. Maka pada langkah kedua, penentuan DHCP Address Space akan otomatis mengambil segment IP yang sama. Jika interface sebelumnya belum terdapat IP, bisa ditentukan manual pada langkah ini.



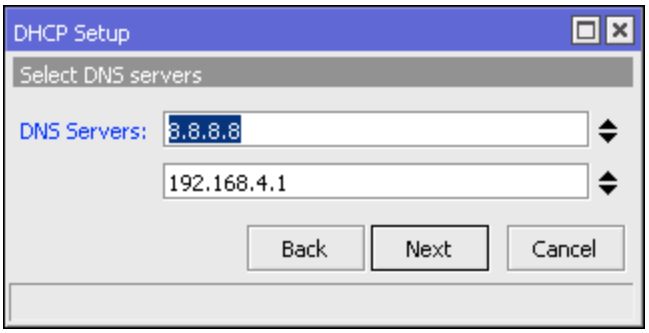
Gambar 8.9 DHCP Server Gatway

Selanjutnya, kita diminta menentukan IP Address yang akan digunakan sebagai default-gateway oleh DHCP Client nantinya. Secara otomatis wizard akan menggunakan IP Address yang terpasang pada interface ether3.



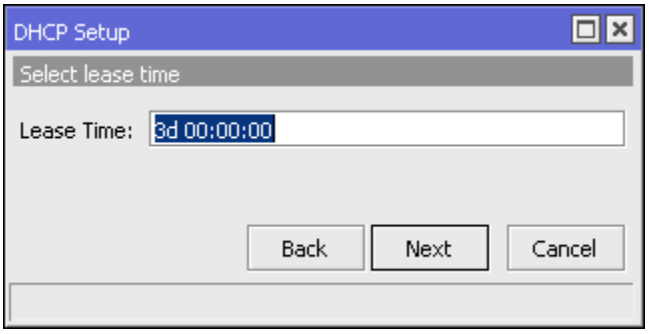
Gambar 8.10 DHCP Server Range Out

Tentukan IP Address yang akan di-distribusikan ke Client. Secara otomatis wizard akan mengisikan host ip pada segment yang telah digunakan. Pada contoh ini, IP 192.168.4.1 tidak masuk dalam Addresses To Give Out, sebab IP tersebut sudah digunakan sebagai gateway dan tidak akan di-distribusikan ke Client.



Gambar 8.11 DHCP Server DNS

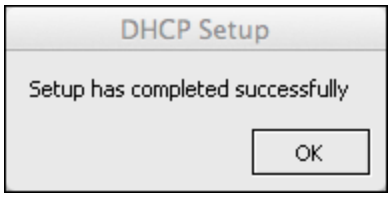
Kita harus menentukan juga, nantinya DHCP Client akan melakukan rquest DNS ke server mana. Secara otomatis wizard akan mengambil informasi setting DNS yang telah dilakukan pada menu /ip dns . Tetapi bisa juga jika kita ingin menentukan request DNS Client ke server tertentu.



Gambar 8.12 DHCP Server Lease Time

Langkah terakhir kita diminta untuk menentukan Lease-Time, yaitu berapa lama waktu sebuah IP Address akan dipinjamkan ke Client. Untuk menghindari penuh / kehabisan IP, setting Lease-Time jangan terlalu lama, misalkan 1 hari saja.

Sampai langkah ini, jika di klik Next akan tertampil pesan yang menyatakan bahwa setting DHCP telah selesai.



Gambar 8.12 DHCP Server Complate

3. ARP Pada DHCP Server

Jika sebelumnya contoh implementasi manual ARP pada jaringan ip static, akan cukup merepotkan jika client berjumlah banyak dan bersifat dinamis. Kita bisa implementasi keamanan menggunakan ARP pada jaringan DHCP dengan mengaktifkan opsi "Add ARP For Leases". Opsi ini bisa di set melalui menu IP --> DHCP Server --> tab DHCP, double klik service DHCP, kemudian centang opsi "Add ARP For Leases"

Gambar 8.13 ARP untuk DHCP Server

Selanjutnya, setting interface yang menjalankan DHCP Server dengan arp=reply-only sama seperti pada langkah static ARP sebelumnya. Setting ini akan melakukan blok terhadap client yang melakukan setting ip address manual, hanya client yang mendapatkan ip address dari proses DHCP yang boleh terkoneksi.