



DIREKTORAT SEKOLAH MENENGAH KEJURUAN
DIREKTORAT JENDERAL PENDIDIKAN VOKASI
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN RISET DAN TEKNOLOGI
TAHUN 2022

SMKN 6 KOTA BENGKULU
TJKT

Teknik Komputer Jaringan dan Telekomunikasi

MATERI AJAR

Manajemen Jaringan



**SMK
FASE F
(Kelas XI)**

SMKN 6 KOTA BENGKULU

DIBUAT OLEH
Budi Riyanto

 smkn6kotabengkulu@gmail.com

 www.smkn6bkl.sch.id

MATERI AJAR

MANAJEMEN JARINGAN

- Sharing Data
- Konfigurasi IP Address dan DHCP pada Mikrotik
 - Virtual Local Area Network ~ VLAN
 - Routing
 - NAT
 - Proxy Server

SHARING DATA

A. Pengertian

File sharing atau berbagi berkas adalah aktivitas membagi atau menyediakan akses data ke media digital di internet kepada orang lain. Data yang dibagi bisa sangat beragam, mulai dari program komputer, dokumen, buku elektronik, ataupun multimedia (gambar, video, dan audio). Untuk bisa saling berbagi, penyedia berkas harus meng-*upload* berkas ke komputer server terlebih dulu. Kemudian barulah orang lain bisa mengunduhnya dari komputer server tersebut.

B. Manfaat Sharing Data

Manfaat dengan adanya sharing data diantaranya :

- Memudahkan pengelolaan folder/drive terhadap jaringan
- Dengan berbagi folder, kita tidak mesti mencopy suatu file/folder dari Satu computer kedalam sarana penyimpanan untuk setelah itu kita buka terhadap komputer lainnya
- Pengirim dan penerima tidak mesti berjumpa untuk berbagi file ataupun folder
- Kemudahan dalam berbagi berkas kepada orang lain yang tak terbatas jumlahnya.

C. Kelebihan dan Kekurangan Sharing Data :

Kelebihan :

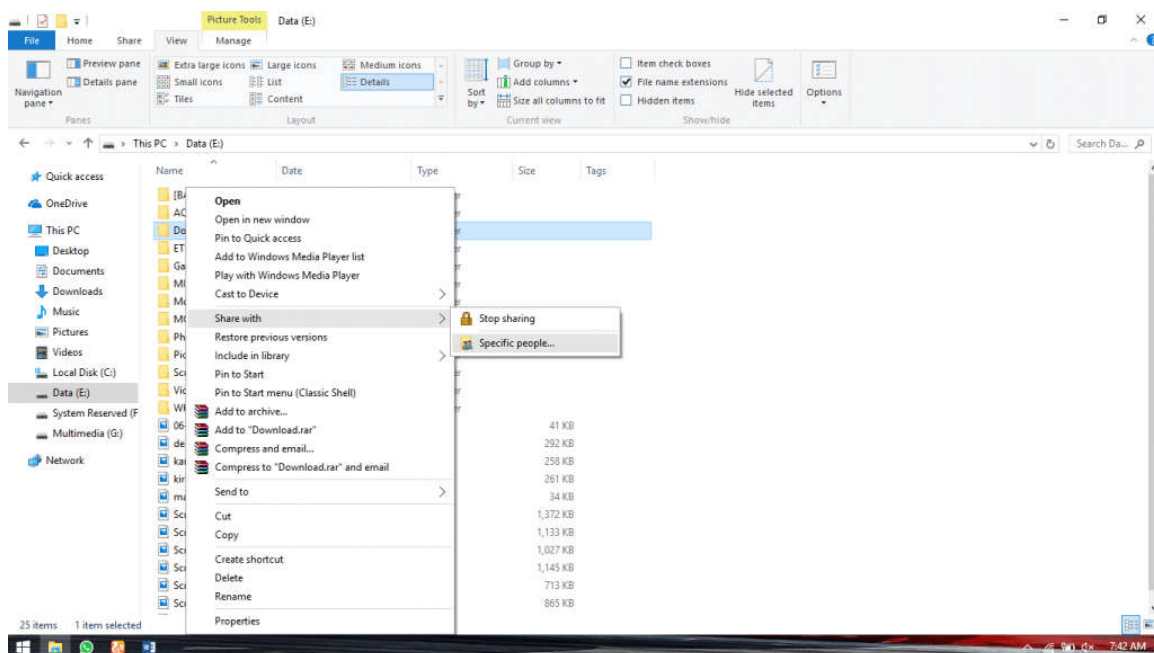
1. Memudahkan didalam pengelolaan/management folder/drive terhadap jaringan.
2. Dengan layanan ini kita tidak mesti mencopy suatu file/folder berasal dari satu pc kedalam media penyimpanan (flashdisk, disket, cd, dll) untuk selanjutnya kita membuka terhadap pc lainnya.
3. Sentralisasi drive (floppy & cd-room) untuk selanjutnya di sharingkan.

Kekurangan :

1. Kehilangan folder dan file-file, yang terkandung terhadap folder berbagi
2. Dapat dimanfaatkan oleh virus serta kroni-kroninya yang mampu sebabkan sarang/bercokol terhadap folder/drive yang disharring dan kebanyakan ber-asal berasal dari pc didalam jaringan yang tingkat securitynya rendah

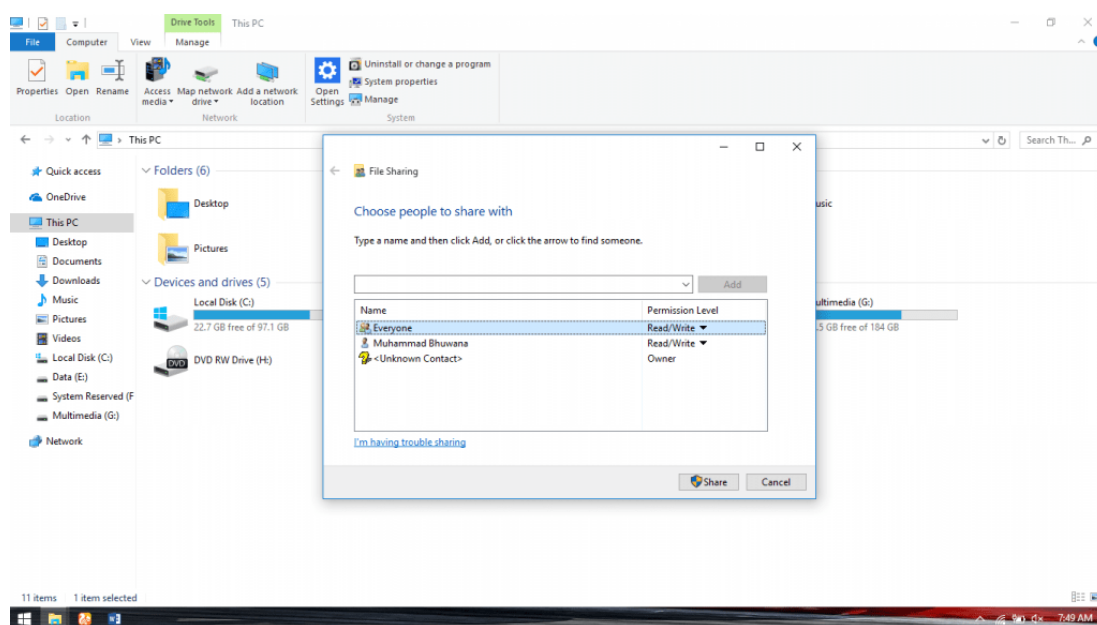
D. Cara Sharing Data di Windows

1. Buka Windows Explorer, pilih dulu folder mana yang ingin kamu share. Kemudian klik kanan pilih share with > Specific people.



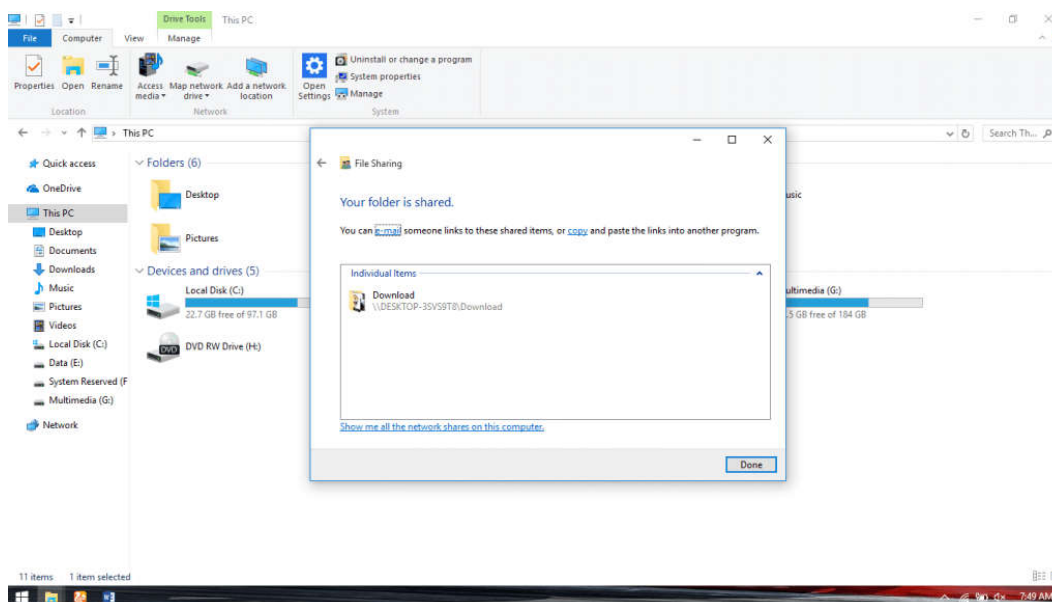
Gambar 1 : Sharing Data

2. Akan muncul jendela file sharing. Di bagian ini kamu tambahkan user Everyone, kemudian klik Add. Setelah user Everyone masuk dalam daftar, klik share.



Gambar 2 : Menambahkan Akses

3. Setelah itu akan dapat konfirmasi "Your Folder is Shared", kemudian klik done.



Gambar 3 : Sharing Selesai

4. Dan proses Sharing folder pun selesai.

ROUTER

A. Pengertian Router

Router adalah perangkat network switching yang digunakan untuk menentukan rute paket ke jaringan atau perangkat lain yang sesuai.

B. Fungsi Router

Setelah membaca apa itu router, tentunya Anda penasaran apa saja fungsi router bukan? Berikut adalah beberapa diantaranya:

- Menghubungkan beberapa jaringan ke beberapa perangkat.
- Transmisi informasi dari satu jaringan ke jaringan yang lainnya.
- Menghubungkan atau mengkoneksikan dua jaringan dengan media yang berbeda.
- Menghubungkan jaringan lokal ke koneksi DSL untuk keamanan ekstra.
- Menyimpan routing table untuk menentukan rute terbaik LAN ke WAN.
- Membaca sumber dan tujuan alamat IP secara logis agar bisa sampai tujuan.

C. Jenis Router

Ada banyak jenis router yang ada di luar sana. Berikut ini adalah penjelasan singkat tentang beberapa tipe router yang bisa Anda pilih!

1. Wireless

Wireless router adalah perangkat yang mempunyai kemampuan wireless secara default. Sebagian besar router ini juga menawarkan port untuk koneksi kabel.

Umumnya, wireless router menggunakan kabel Ethernet untuk terhubung ke modem dan mendistribusikan data dengan mengubah paket dari kode biner menjadi sinyal radio.

Kemudian wireless router akan menyiarkan dan membagikan radio sinyal menggunakan antena yang ada pada perangkat router tersebut.

Router wireless tidak menggunakan LAN melainkan WLAN (wireless local area network) yang menghubungkan beberapa perangkat menggunakan komunikasi nirkabel.

2. Wired

Seperti router nirkabel, wired router atau router kabel juga menggunakan kabel Ethernet untuk terhubung ke jaringan yang ada pada modem.

Namun, router kabel kemudian menggunakan kabel terpisah untuk menghubungkan ke satu atau lebih perangkat ke jaringan tersebut.

Wired router juga bisa digunakan untuk membuat LAN, menghubungkan perangkat dalam jaringan itu ke Internet, dan masih banyak lagi.

3. Virtual Router

Router virtual atau vRouter adalah aplikasi perangkat lunak yang mempunyai fungsi yang sama seperti router perangkat keras standar.

vRouter ini memungkinkan komputer/server untuk memiliki kemampuan router lengkap dalam fungsionalitas dan perutean paket melalui aplikasi perangkat lunak.

Virtual Router Redundancy Protocol (VRRP) dapat mengimplementasikan router virtual untuk meningkatkan performa jaringan dan sebagai cadangan jika salah satu mesin gagal.

4. Core Router

Berbeda dengan router yang digunakan dalam LAN rumah atau bisnis kecil, core router digunakan oleh perusahaan dan bisnis yang mengirimkan paket data volume tinggi.

Core router menghubungkan semua perangkat jaringan dan menyediakan beberapa antarmuka

komunikasi data cepat. Kata “inti” mengacu pada keseluruhan struktur fisik jaringan.

Router core beroperasi pada “inti” jaringan dan tidak berkomunikasi dengan jaringan eksternal.

5. Edge Router

Sementara core router secara eksklusif mengelola lalu lintas data dalam jaringan skala besar, edge router berkomunikasi dengan router inti dan jaringan eksternal.

Router edge hidup di “tepi” jaringan dan menggunakan BGP (Border Gateway Protocol) untuk mengirim dan menerima data dari LAN dan WAN luar jaringan.

D. Berbagai macam Merek Router

1. Mikrotik

Mikrotik adalah sistem operasi yang berbasis perangkat lunak (*software*) yang dipergunakan untuk menjadikan komputer sebagai router sebuah jaringan. Mikrotik juga menggunakan sistem operasi berbasis Linux dan menjadi dasar *network router*. Sistem operasi (OS) ini sangat cocok untuk membangun administrasi jaringan komputer yang berskala kecil hingga besar.

Ada banyak fitur yang ditawarkan oleh router mikrotik. Di bawah ini beberapa fiturnya:

- Routing – Static routing
- NAT dan Firewall
- Hotspot
- Data Rate Management
- IPsec
- DHCP
- Web proxy
- NTP
- UPnP
- SNMP
- Caching DNS client
- Universal Client
- MNDP

Terdapat dua jenis mikrotik yang ada saat ini yaitu RouterBoard dan Mikrotik RouterOS.

Penjelasan mengenai keduanya adalah sebagai berikut:

- **Mikrotik RouterOS:** jenis mikrotik yang termasuk ke dalam OS UNIX. Mikrotik yang satu ini mampu menjadikan sebuah komputer biasa memiliki berbagai fitur seperti firewall, router, hotspot, bridge, proxy, dan lain sebagainya. Dikarenakan mudah digunakan bahkan oleh orang awam sekali pun, maka tidak heran jika mereka memiliki sistem operasi ini di dalam membangun sebuah router
- **RouterBoard:** merupakan jenis mikrotik yang berupa perangkat keras atau hardware yang disediakan sendiri oleh perusahaan mikrotik. RouterBoard akan diinstall OS Mikrotik RouterOS. Meskipun termasuk perangkat keras, namun mikrotik yang satu ini memiliki ukuran yang sangat kecil serta praktis. RouterBoard terdiri dari Prosesor, ROM, RAM, serta memory flash. Untuk harga pasarannya berkisar antara 600 sampai dengan 700 ribu



Gambar 4 : RouterBoard Mikrotik

2. Cisco

Cisco adalah peralatan utama yang banyak digunakan pada Jaringan Area Luas atau Wide Area Network (WAN). Dengan cisco router, informasi dapat diteruskan ke alamat-alamat yang berjauhan dan berada di jaringan computer yang berlainan. Yang bertujuan untuk dapat meneruskan paket data dari suatu LAN ke LAN lainnya, Cisco router menggunakan tabel dan protocol routing yang berfungsi untuk mengatur lalu lintas data.

Paket data yang tiba di router diperiksa dan diteruskan ke alamat yang dituju. Agar paket data yang diterima dapat sampai ke tujuannya dengan cepat, router harus memproses data tersebut dengan sangat tepat. Untuk itu, Cisco Router menggunakan Central Processing Unit (CPU) seperti yang digunakan di dalam komputer untuk memproses lalu lintas data tersebut dengan cepat. Seperti komputer.

Sertifikat Cisco

1. CCNA (Cisco Certified Network Associate)

merupakan sertifikasi tingkat pertama. Sertifikasi ini mengajarkan setiap IT people dari hal yang benar-benar *BASIC* hingga memiliki konsep dasar *network* sempurna. Dengan memiliki sertifikasi ini *IT People* akan mampu *handle network* dengan kapasitas sekitar 250-500 *user*. (*Note* : TIDAK ADA syarat apapun untuk mengikuti *training* CCNA RS).

2. CCNP (Cisco Certified Network Professional)

merupakan sertifikasi tingkat kedua yang berisi pendalaman materi serta kasus-kasus yang lebih kompleks. Melalui sertifikasi ini, *IT people* akan mampu *handle network* dengan kapasitas di atas 500-2000 *user* dan bersifat multi-area. (*Note* : Syarat mengikuti *training* CCNP adalah sudah menguasai materi CCNA).

CCIE (Cisco Certified Internetwork Expert)

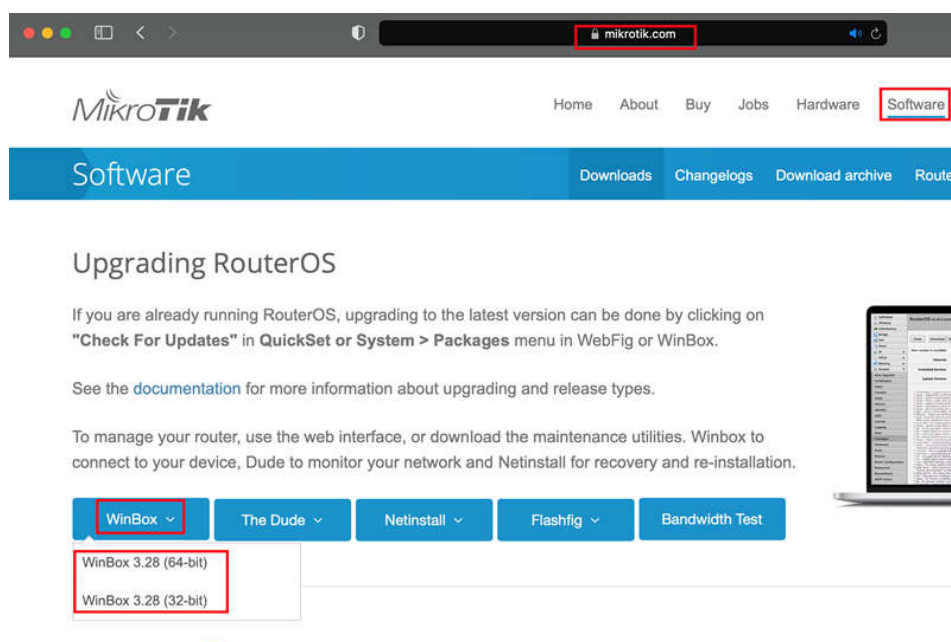
merupakan sertifikasi tingkat tertinggi yang berisi pendalaman serta materi khusus hingga level *SERVICE PROVIDER connectivity*. Dengan memiliki sertifikasi CCIE, setiap *IT people* akan mampu *handle network* dengan kapasitas lebih dari 2000 *user*. (*Note* : Syarat mengikuti *training* CCIE adalah sudah menguasai materi CCNA dan CCNP).

KONFIGURASI ROUTERBOARD MIKROTIK

A. Cara Koneksi mikrotik dengan winbox

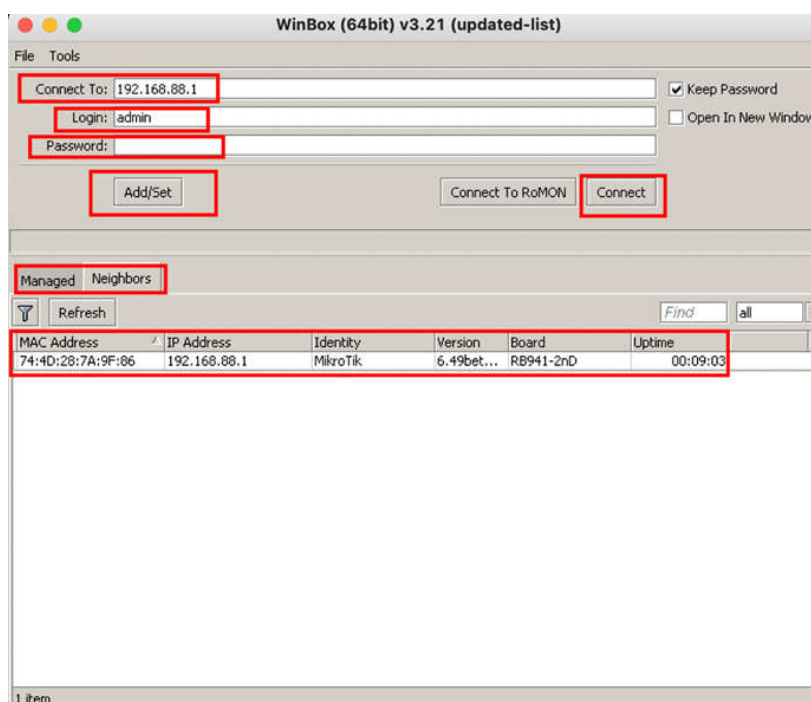
Winbox adalah aplikasi kecil yang dapat digunakan untuk melakukan administrasi terhadap Mikrotik RouterOS dengan cepat dan dengan tampilan **GUI**. Winbox dapat digunakan pada Linux, MacOs dan Windows.

Sebelum kita konfigurasi winbox, pastikan anda menggunakan winbox versi yang terbaru karena beberapa tipe hardware mikrotik, jika ingin dikonfigurasi, perlu menggunakan winbox yang versi terbaru. Untuk download winbox versi terbaru, anda perlu mengunjungi website official www.mikrotik.com lalu pilih versi yang terbaru yang sesuai bit operating sistem anda.



Gambar 5 : Download Winbox

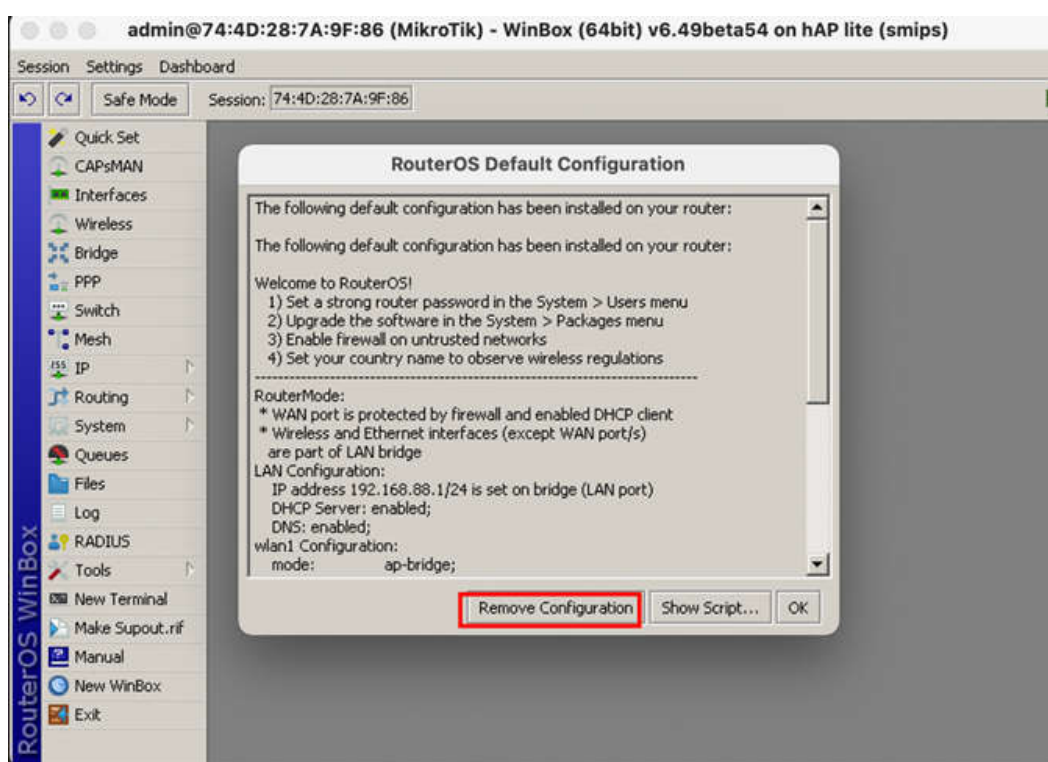
Berikut tampilan winbox pertama kali ketika dibuka :



Gambar 6 : Tampilan Awal Winbox

Ada beberapa fitur dasar ketika kita ingin konek ke router kita :

1. Connect To = Masukkan IP Router atau MAC Address Router yang kita inginkan
2. Login = Masukkan username dan password login ke router anda (default = admin)
3. Password = Masukkan Password untuk router yang ingin anda koneksikan (default tidak diisi)
4. Add/Set = Untuk menyimpan informasi berupa IP/MAC Router, Login, Password, ke menu Managed, jadi ketika konek ke router kedepan nya, tidak perlu ketik lagi.
5. Connect = Untuk connect ke router kita.
6. Managed = Hasil list IP/MAC Router, Login, Password yang tersimpan
7. Neighbors = Akan muncul list router yang terhubung langsung dengan router kita.



Gambar 7 : Remove Configuration

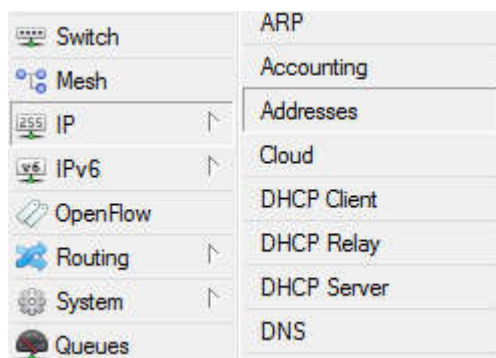
Pertama kali login, akan muncul menu yang dinamakan RouterOS Default Configuration. Jadi ketika menggunakan winbox pertama kali, routerboard sudah memiliki konfigurasi bawaan pabrik atau lebih dikenal dengan RouterOS Default Configuration, tiap routerboard beda beda tergantung perangkat nya tipe apa. Karena kita mulai dari dasar, jadi kita bisa hapus saja.

B. Setting IP Address pada Mikrotik

Ada dua cara yang dapat dilakukan untuk mengkonfigurasi IP Address pada Mikrotik yang diakses melalui winbox, yaitu dapat dengan mode GUI ataupun mode CLI. Dengan mode GUI akan sedikit lebih mudah untuk mengkonfigurasinya. Karena akan sangat terbantu dengan tampilan graphic yang tinggal klik dan klik. Sedangkan mengkonfigurasi dengan mode CLI atau text terlebih dahulu harus tau perintah apa yang dibutuhkan.

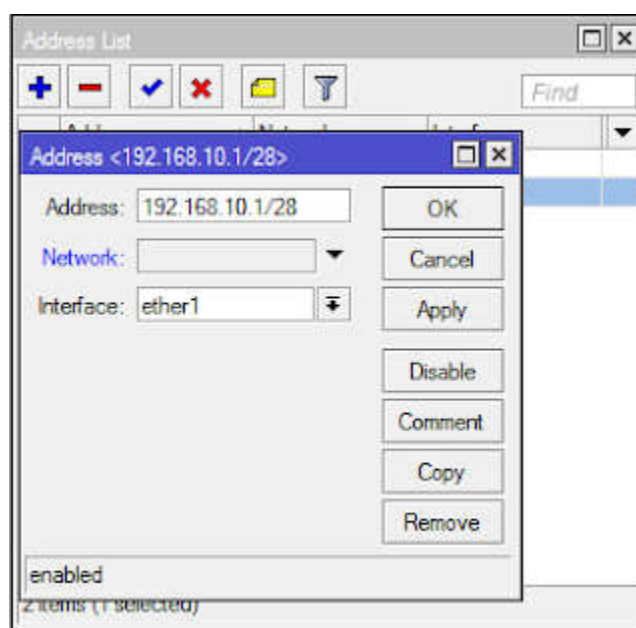
Berikut langkah-langkah yang harus dilakukan ketika mengkonfigurasi dengan mode GUI.

1. Klik menu IP > Addresses



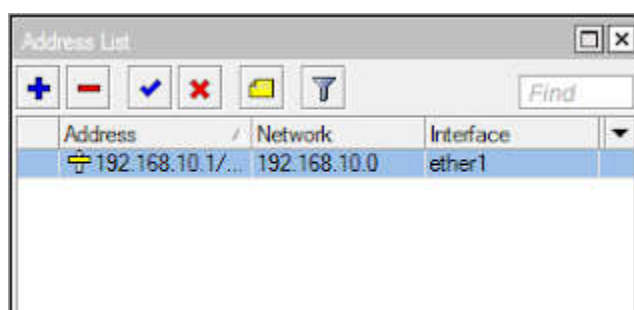
Gambar 8 : Menu IP Address pada Mikrotik

2. Isi kolom Address sesuai IP yang diinginkan dan arahkan pada interface yang ingin dikonfigurasi



Gambar 9 : Tab Menu IP Address

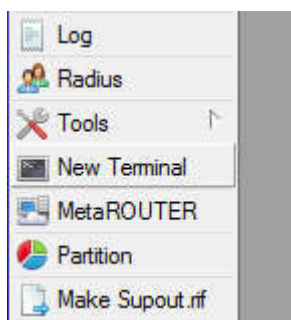
3. Setelah mengisi IP Address dan memilih interface klik Apply > OK



Gambar 10 : Memasukan IP Address

Jika ingin mengkonfigurasi dengan mode CLI atau text, berikut perintah yang harus dilakukan

1. Buka New Terminal pada winbox



Gambar 11 : Menu New terminal

2. Untuk mengkonfigurasinya masukan perintah seperti berikut

```
[admin@Iwud] > ip address add address="IP Address" interface="ethernet yang dituju"
```

Contoh :

```
[admin@Iwud] > ip address add address=192.168.20.1/28 interface=ether2
```

3. Cek IP Address tersebut sudah terkonfigurasi atau belum dengan perintah berikut

```
[admin@Iwud] > ip address print
```

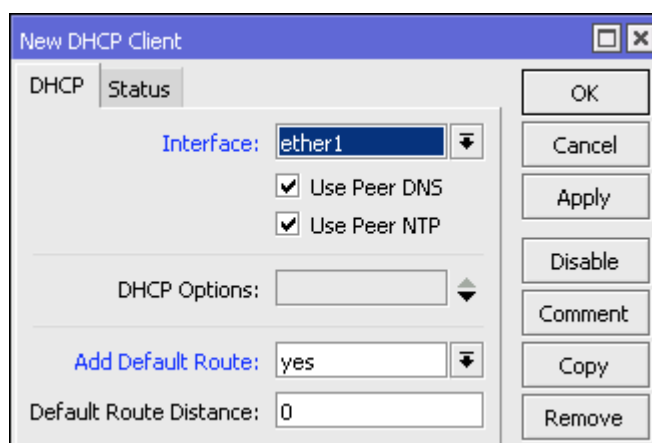
```
[admin@Iwud] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK      INTERFACE
0   192.168.20.1/28    192.168.20.0 ether2
```

Gambar 12 : Menu CLI

C. Setting DHCP Client dan DHCP Server Pada ROuterBoard Mikrotik

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 13 : Konfigurasi 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;

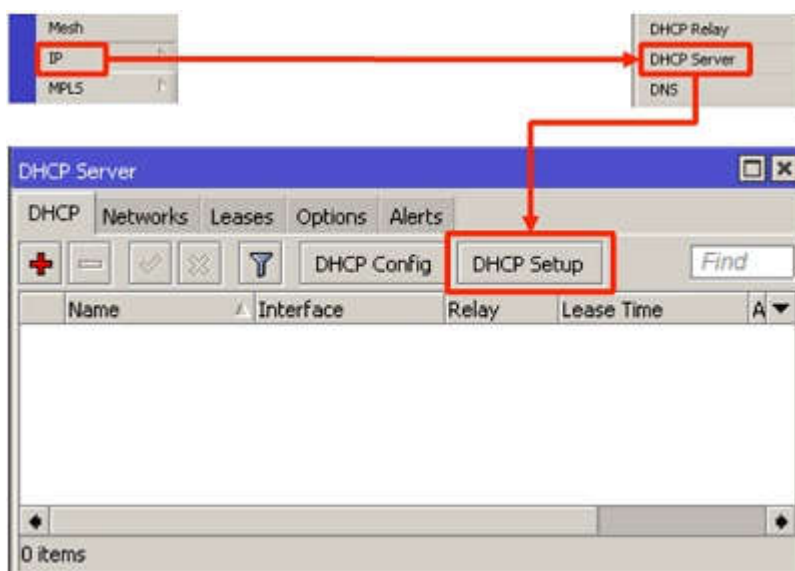
- *Interface* : Pilihlah interface yang sesuai yang terkoneksi ke DHCP Server
- *Use-Peer-DNS* : Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
- *Use-Peer-NTP* : Bila kita hendak menggunakan informasi pengaturan waktu di router (NTP) sesuai dengan informasi dari DHCP
- *Add-Default-Route* : Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP
- *Default-Route-Distance* : Menentukan nilai Distance pada rule routing yang dibuat secara otomatis. Akan aktif jika `add-default-route=yes`

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

Mikrotik sebagai DHCP Server

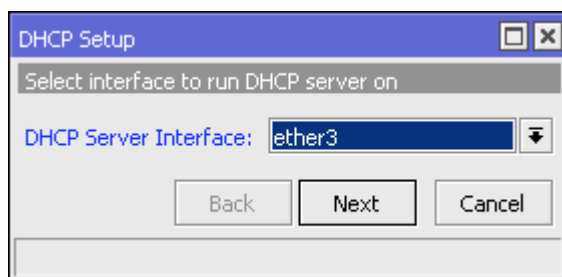
DHCP Server akan sangat tepat diterapkan jika pada jaringan memiliki user yang sifatnya dinamis. Dengan jumlah dan personel yang tidak tetap dan selalu berubah. Jika pada kasus ini sifat user seperti itu dapat kita temui pada tamu yang berkunjung.

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



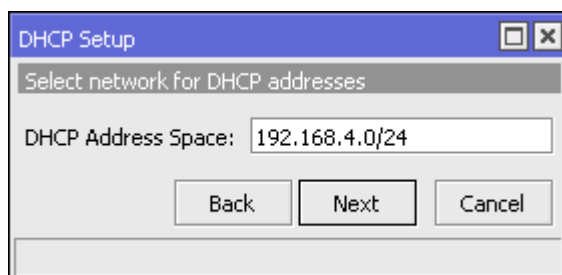
Gambar 14 : Konfigurasi DHCP Server

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



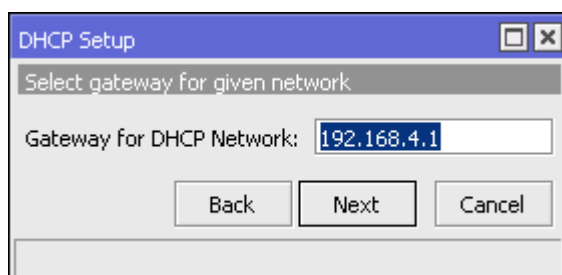
Gambar 15 : memilih Interfaces

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



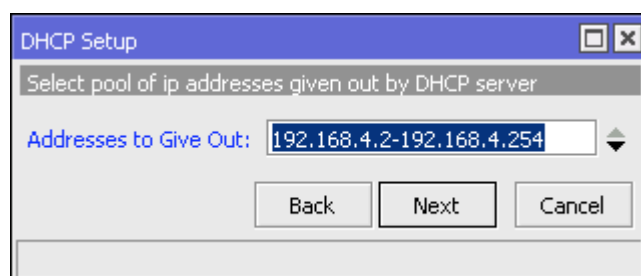
Gambar 16 : Network DHCP Server

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.



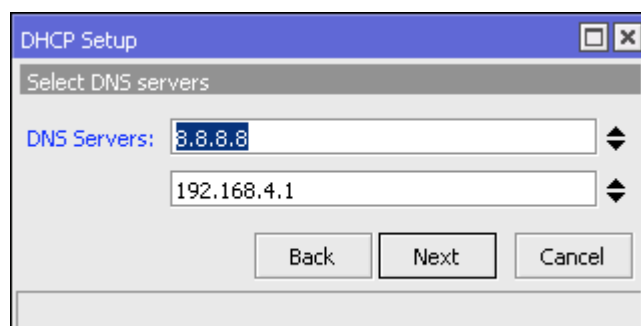
Gambar 17 : Gateway DHCP Server

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.



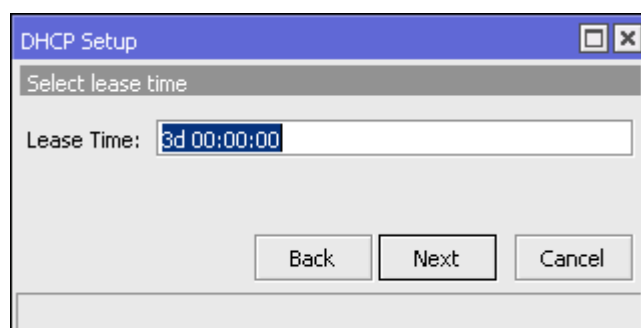
Gambar 18 : Batas IP DHCP Server

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 19 : Memasukan DNS

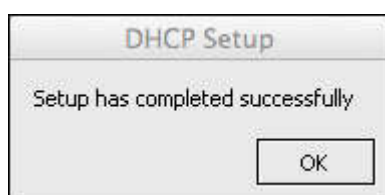
Kita harus menentukan juga, nantinya DHCP Client akan melakukan request DNS ke server mana. Secara otomatis wizard akan mengambil informasi setting DNS yang telah dilakukan pada menu /ip dns . Tetapi bisa juga jika kita ingin menentukan request DNS Client ke server tertentu.



Gambar 20 : DHCP 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 21 : Konfigurasi DHCP Selesai

Untuk melakukan percobaan, hubungkan PC ke ether3 kemudian ubah pengaturan IP PC pada posisi "obtain an IP address automatically" .



Gambar 22 : Tab Konfigurasi IP Address Windows

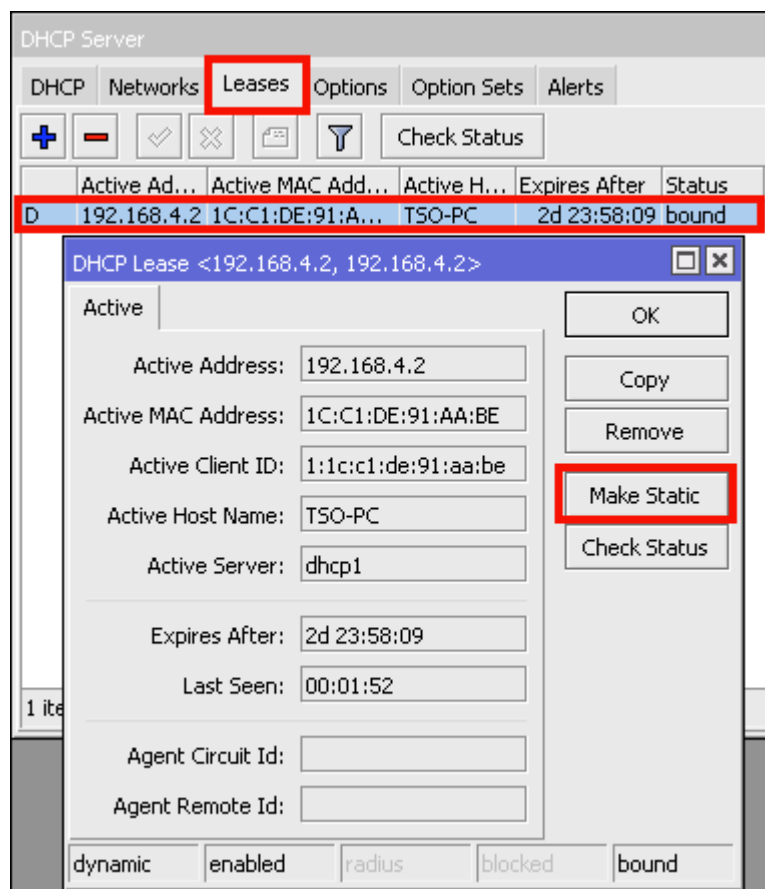
Seharusnya Laptop akan mendapatkan assign IP otomatis dari Router. Perhatikan expired time, seharusnya sama dengan parameter Lease-Time yang sudah ditentukan pada DHCP Server.

DHCP Leases

Daftar perangkat yang sudah diberikan IP secara otomatis akan ada pada `/ip dhcp-server leases`. Secara default, ip address yang akan diberikan ke client diurutkan dari belakang (192.168.4.254). Akan tetapi, kita juga bisa melakukan pengaturan agar sebuah IP hanya akan dipinjamkan ke Client tertentu. Misalnya, jika Client-A melakukan request DHCP, maka Server akan selalu memberikan IP 192.168.4.254.

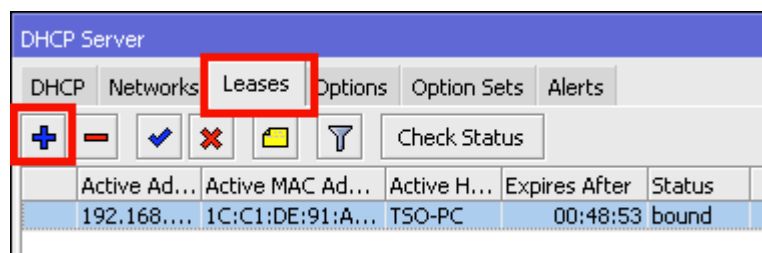
Konsep tersebut dapat diterapkan dengan menggunakan Static Leases. Ide dasarnya adalah melakukan reservasi sebuah IP Address untuk sebuah MAC Address tertentu. Ada 2 cara konfigurasi yang bisa dilakukan.

Pertama, dengan melihat dari daftar perangkat yang ada pada tab Leases. Jika dilakukan dengan cara ini client harus sudah mendapat IP Address dahulu.

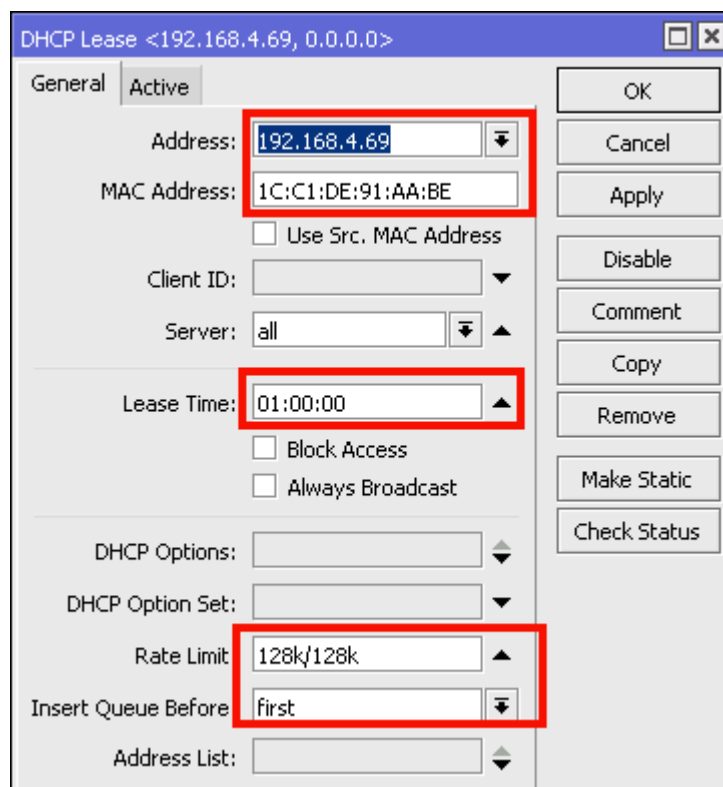


Gambar 23 : TAB DHCP Lease

Cara kedua dengan menambahkan secara manual pada tab Leases.



Gambar 23 : Menu DHCP Leases



Gambar 24 : Konfigurasi DHCP Leases

Selain dapat digunakan untuk reservasi IP Address, Static Leases juga bisa digunakan untuk menentukan :

- Lease-Time yang berbeda untuk tiap MAC Address (Client)
- Limitasi bandwidth (rate-limit) , jika ditentukan maka rule simpe queue akan secara otomatis muncul ketika client mendapat assign IP dari server.
- Melakukan blocking MAC Address tertentu agar tidak bisa mendapat pinjaman IP, dengan opsi "Block-Access=yes".

Jadi, selain dapat mendistribusikan IP secara otomatis, dengan DHCP Server juga dapat melakukan manajemen terhadap DHCP Client dengan menggunakan Static Leases.

Virtual Local Area Network (VLAN)

A. Pengertian

VLAN (Virtual LAN) adalah model jaringan yang secara logis membagi jaringan menjadi beberapa VLAN yang berbeda. VLAN tidak terbatas pada kondisi jaringan fisik seperti LAN. VLAN dapat dikonfigurasi dalam praktek tanpa harus memeriksa kondisi perangkat. Akibatnya, VLAN memiliki fleksibilitas dalam manajemen jaringan dan memungkinkan administrator jaringan untuk memartisi jaringan mereka sesuai dengan kemampuan jaringan dan persyaratan keamanan.

Virtual Local Area Network (VLAN) adalah metode membuat jaringan yang diatur secara logis satu per satu. VLAN sendiri berada di jaringan area lokal (LAN), sehingga satu atau lebih VLAN dapat ada di jaringan (LAN). Jadi kita dapat menyimpulkan bahwa kita dapat membentuk satu atau lebih jaringan (jaringan dalam suatu jaringan) dalam suatu jaringan. Konfigurasi VLAN itu sendiri dilakukan melalui perangkat lunak (software) sehingga komputer berada di jaringan VLAN yang sama ketika sedang bergerak.

B. Cara Kerja VLAN

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan, menggunakan port dan alamat MAC. Semua informasi yang mengandung penandaan / pengalamatan VLAN disimpan dalam database (tabel). Jika label didasarkan pada port yang digunakan, database harus menentukan port yang digunakan oleh VLAN.

Untuk mengatur sakelar / jembatan inilah maka biasanya digunakan, yang bisa diatur atau bisa diatur. Sakelar / jembatan ini menyimpan semua informasi dan konfigurasi VLAN dan memastikan bahwa semua sakelar / jembatan memiliki informasi yang sama. Switch menentukan ke mana data dialihkan, dan seterusnya. Anda juga dapat menggunakan perangkat lunak penghubung untuk merekam / menandai VLAN dan stasiun kerjanya. Koneksi antara VLAN membutuhkan router.

C. Fungsi VLAN

Fungsi Virtual Local Area Network (VLAN) pada jaringan komputer adalah untuk memberikan metode pada jaringan yang dapat membagi jaringan fisik menjadi beberapa domain siaran. Domain broadcast ini biasanya batas subnet IP. Setiap subnet memiliki VLAN. VLAN memungkinkan beberapa LAN virtual berdampingan dalam LAN fisik (sakelar). Sama seperti ada dua mesin yang terhubung dalam satu saklar, keduanya tidak dapat mengirim frame Ethernet ke mesin lain bahkan dalam kabel yang sama.

D. Jenis-Jenis VLAN

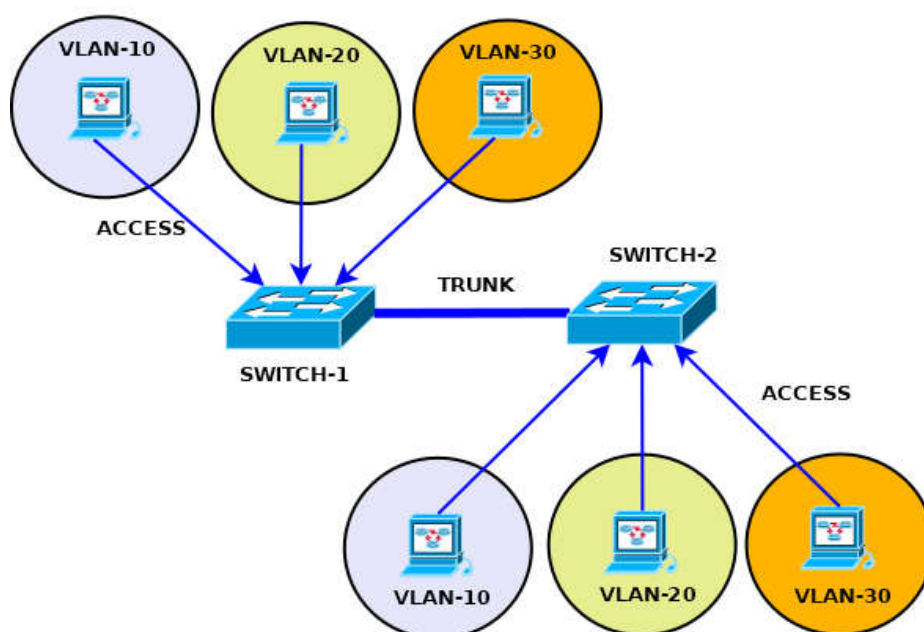
1. VLAN default adalah VLAN sejak sakelar dinyalakan pertama kali. Selama konfigurasi, semua port switch disertakan dalam VLAN standar dan dapat dihubungkan ke setiap port. Di Cisco, VLAN default adalah VLAN.
2. Data VLAN adalah VLAN yang hanya mengatur lalu lintas data di VLAN.
3. VLAN asli adalah VLAN yang dikembalikan ke port jika tidak ada di bagasi dan tidak memiliki tag.

4. VLAN Suara adalah VLAN yang mendukung VoIP dan dirancang khusus untuk komunikasi data suara dalam VLAN.
5. Management VLAN adalah VLAN yang dikonfigurasi untuk sakelar manajemen.

D. Keuntungan Menggunakan VLAN

1. Keamanan, semua data sensitif dipisahkan dari jaringan yang ada, sehingga pelanggaran akses ke informasi rahasia dan penting berkurang.
2. Penghematan biaya dapat menghemat biaya dengan menghilangkan biaya mahal dari peningkatan jaringan dan penggunaan bandwidth dan uplink yang efisien.
3. Kinerja yang lebih tinggi dapat mengurangi lalu lintas jaringan dan meningkatkan kinerja dengan membagi jaringan Layer 2 menjadi kelompok kerja logis.
4. Broadcast Storm Mitigation, dapat mengurangi jumlah perangkat yang berpartisipasi dalam siaran.
5. Peningkatan efisiensi staf TI memfasilitasi manajemen jaringan karena pengguna dengan kebutuhan jaringan yang sama menggunakan VLAN yang sama.
6. Manajemen proyek atau aplikasi yang lebih mudah membuatnya lebih mudah untuk mengelola suatu proyek atau pekerjaan karena memiliki fungsi yang terpisah.

VLAN-VIRTUAL LOCAL AREA NETWORK



Gambar 25 : VLAN

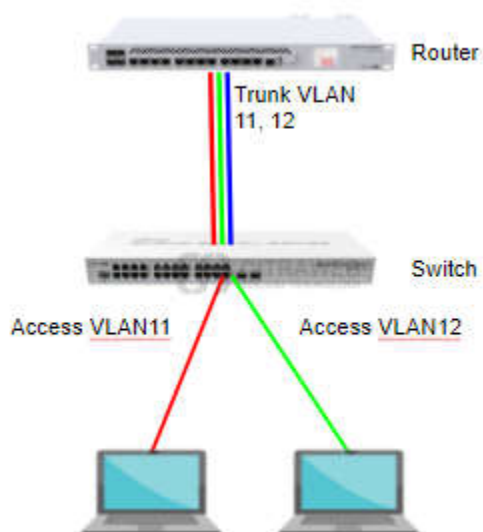
D. Konfigurasi VLAN pada Mikrotik

Contoh yang pertama kita akan mencoba untuk menggunakan perangkat CRS 3XX Series. Cara ini juga bisa digunakan untuk perangkat router (routerboard / ccr) yang ingin difungsikan sebagai switch.

- **Mode Untagged**

Untuk mode untagged akan sederhana karena kita akan memberikan IP pada interface bridge nya langsung. Kita tidak akan membuat interface vlan management pada router maupun switch.

Contoh topologi yang kita gunakan adalah seperti gambar berikut:



Gambar 26 : Topologi VLAN

Konfigurasi pada router, IP Address untuk management terpasang pada interface yang mengarah ke switch.

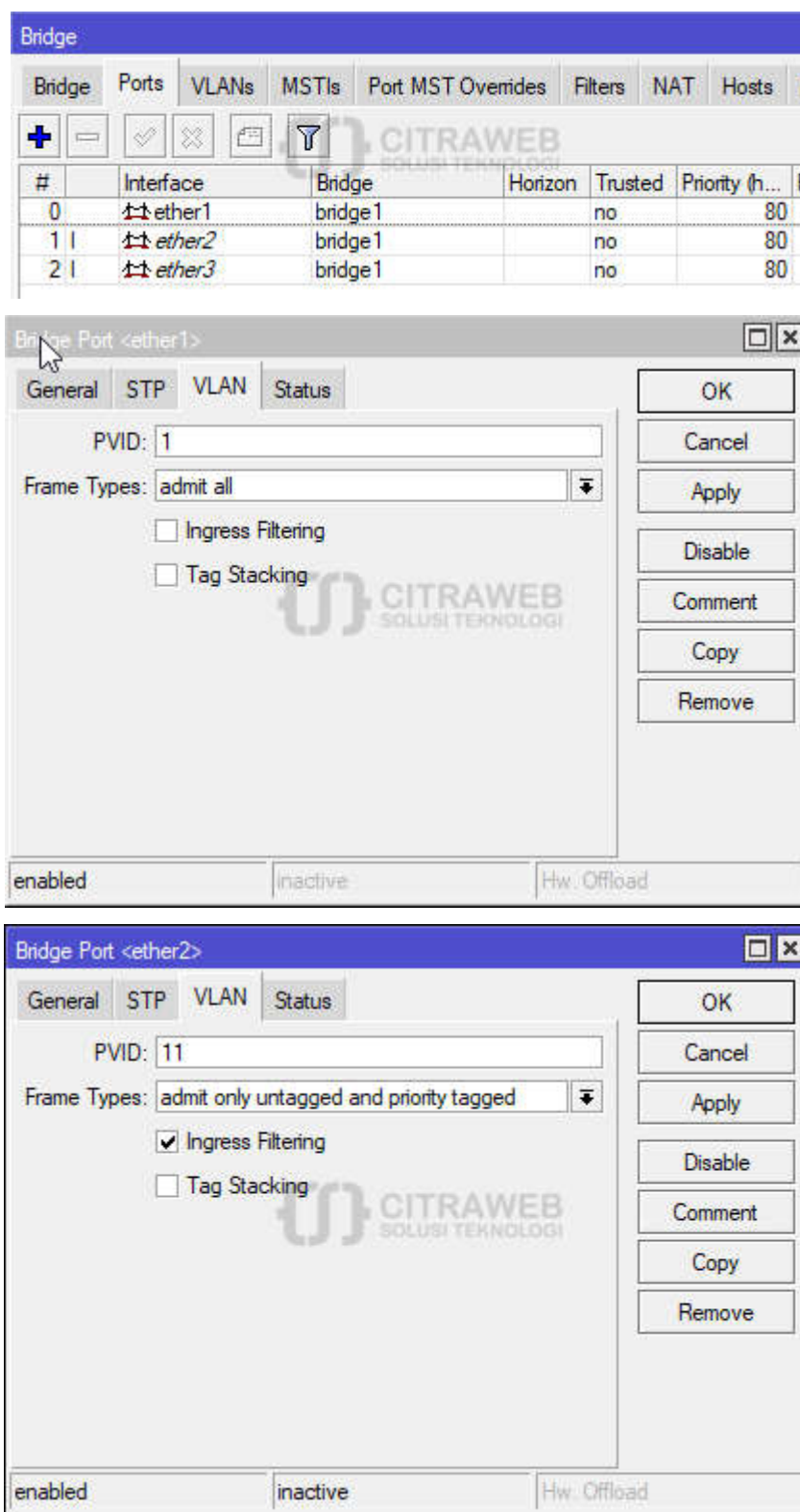
Gambar 27 : Input IP Address

Dan konfigurasi pada switch adalah sebagai berikut:

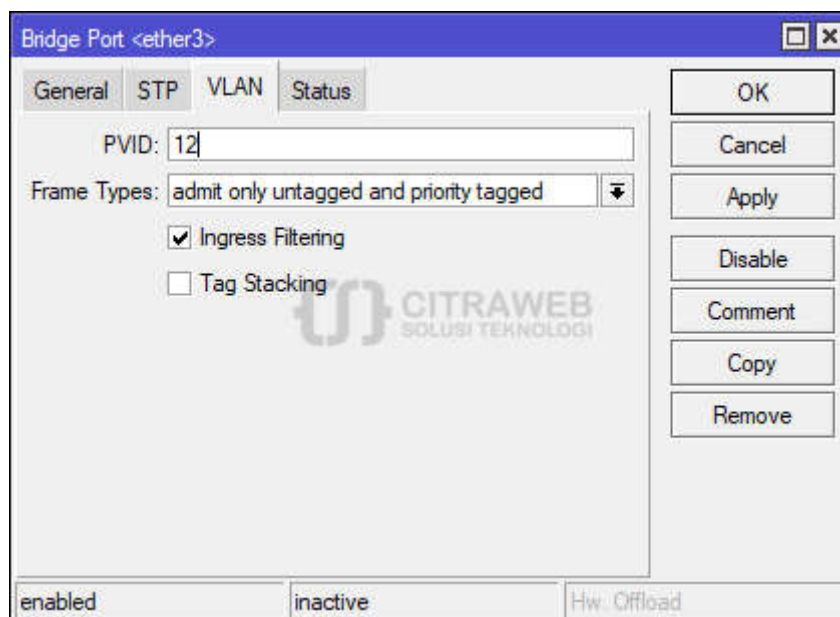
Pada kasus ini ether1 adalah trunk, ether2, dan ether3 adalah port access yang akan digunakan untuk client.

Gambar 28 : Penambahan Bridge

Pertama, buat bridge untuk ether1 (trunk), ether2 (access), dan ether3 (access). Jangan lupa tentukan pvid untuk port access, detail cek pada gambar berikut:

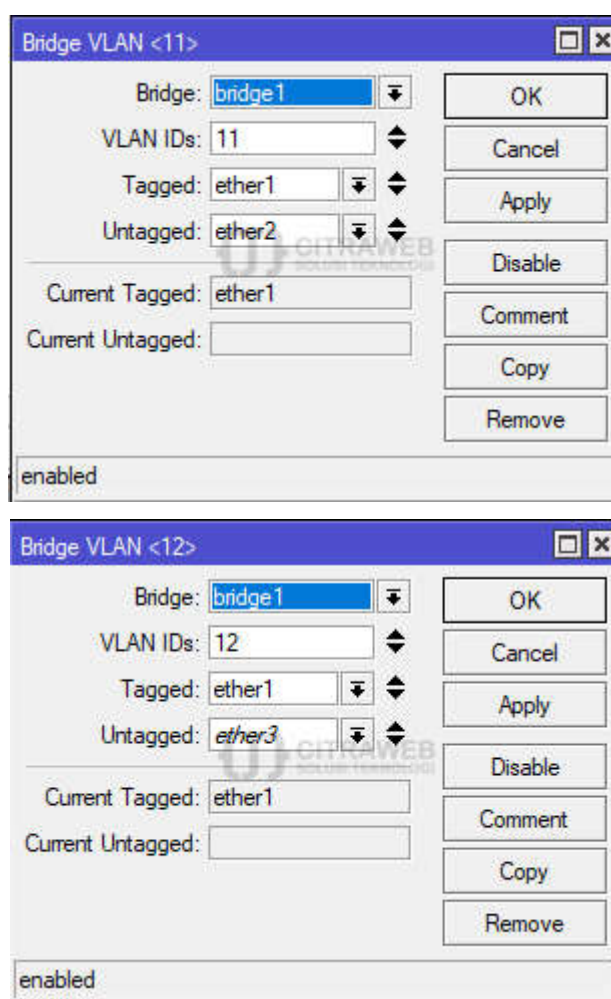


Gambar 29 : Pengaturan VLAN ID 1



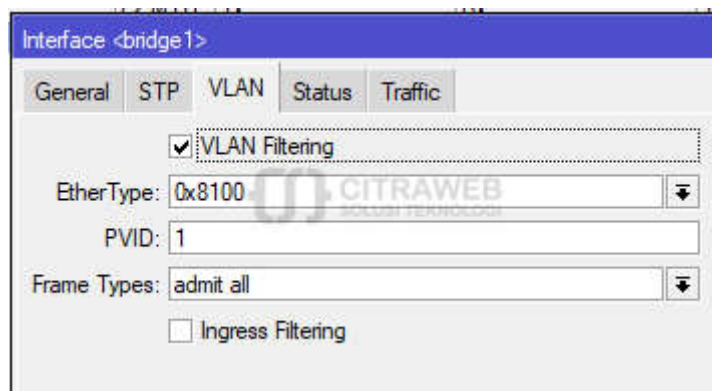
Gambar 30 : Pengaturan VLAN ID 2

Kemudian konfigurasi pada tab VLANs



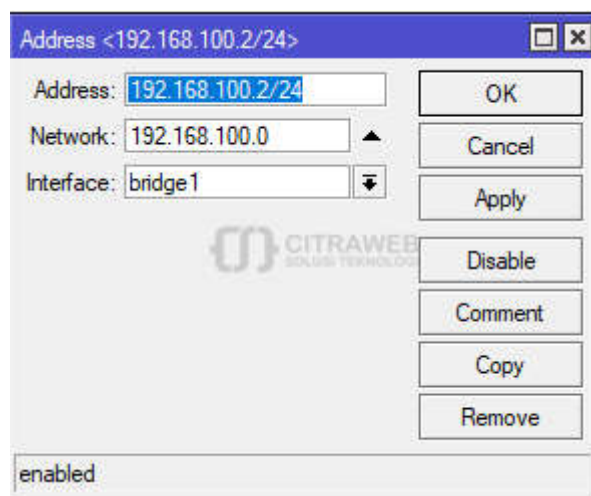
Gambar 31 : Konfgurasi VLAN TAB

Jangan lupa aktifkan vlan filtering pada bridge yang kita buat tadi.



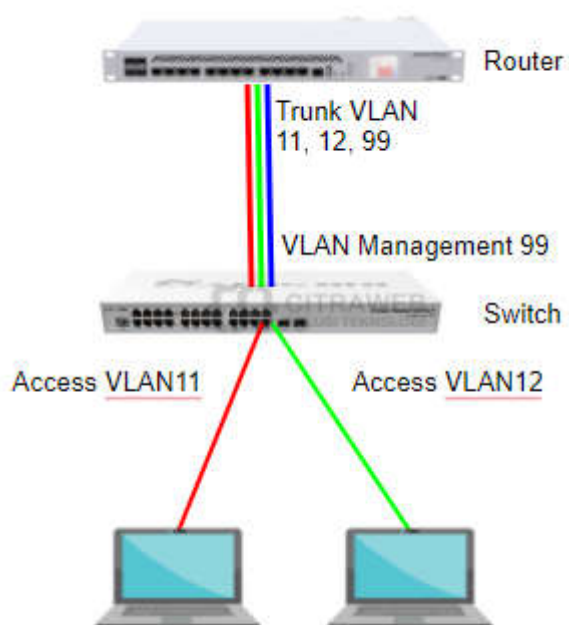
Gambar 32 : VLAN Filtering

Selanjutnya konfigurasi IP address untuk vlan management pada interface bridge yang sudah dibuat tadi.



Gambar 33 : Konfigurasi IP Address untuk VLAN Bridge

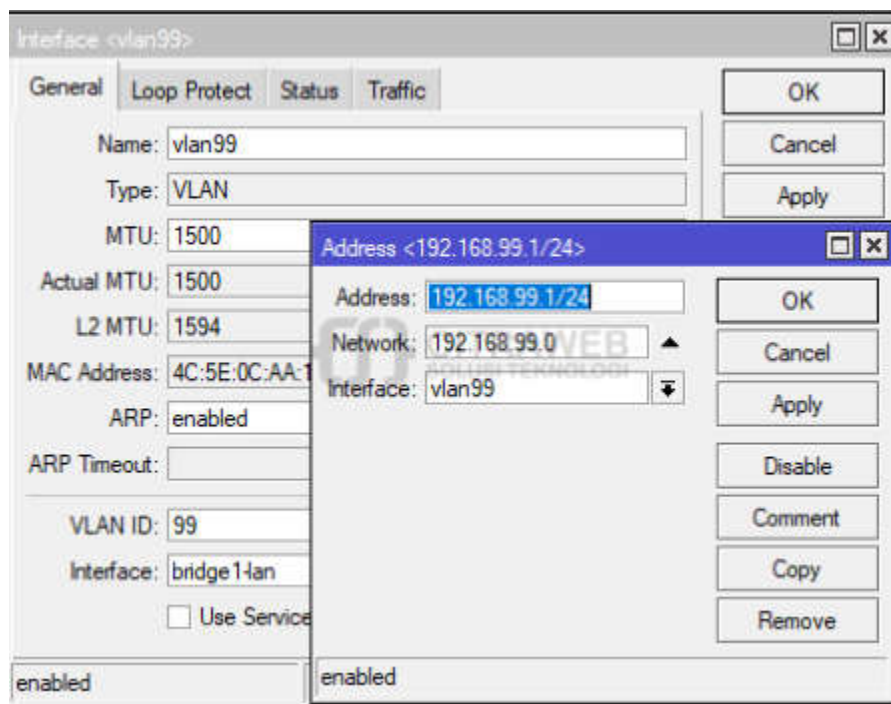
- **Mode Tagged**



Gambar 34 : Topologi VLAN

Dengan menggunakan mode tagged ini kita akan membuat interface vlan untuk vlan management. Sebagai contoh disini akan menggunakan vlan 99 untuk vlan management nya.

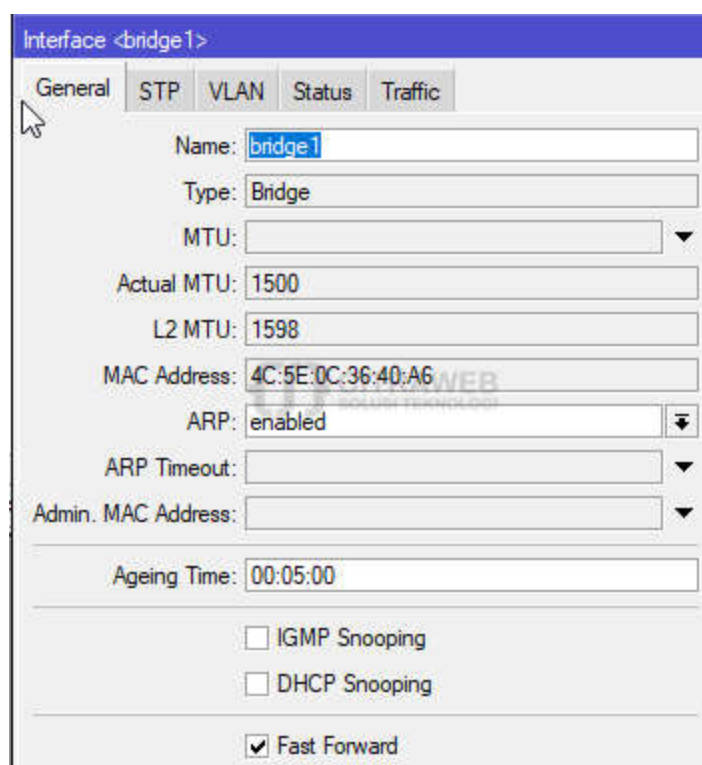
Konfigurasi pada router



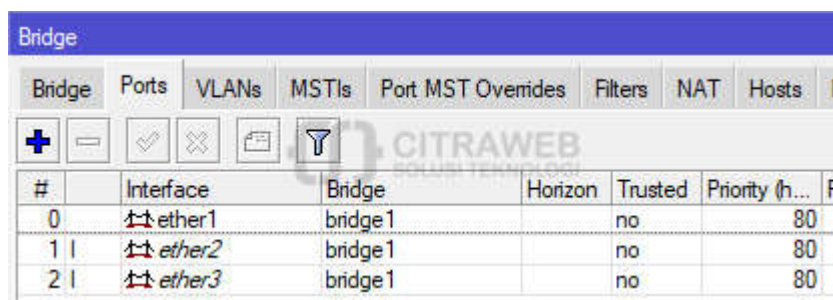
Gambar 35 : Input IP Address

Pada router terdapat interface vlan management yaitu vlan 99 dan IP address terpasang pada interface vlan tersebut.

Konfigurasi pada switch Untuk topologi nya masih sama, di ether1 sebagai trunk, ether2 dan ether3 sebagai port access.



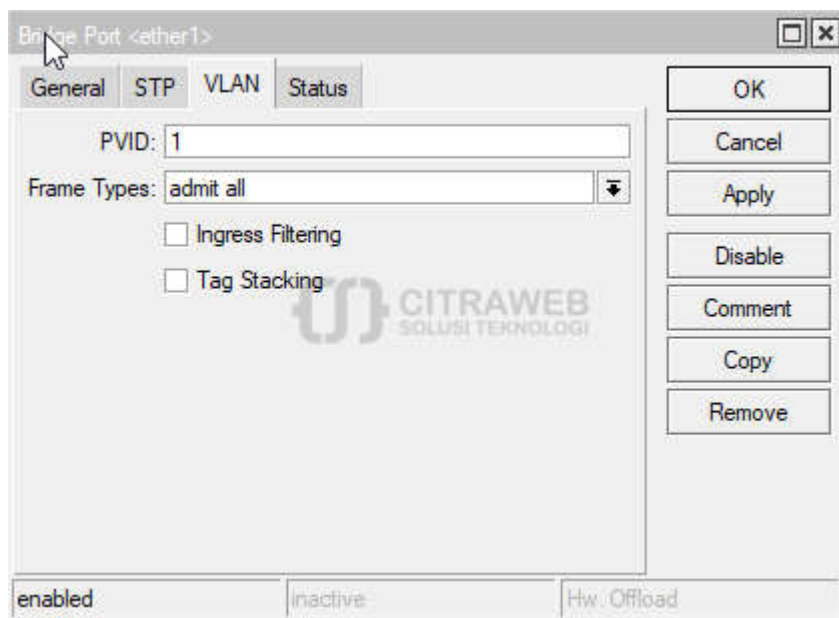
Gambar 36 : Penambahan bridge



#	Interface	Bridge	Horizon	Trusted	Priority (h...)
0	ether1	bridge 1		no	80
1	ether2	bridge 1		no	80
2	ether3	bridge 1		no	80

Gambar 37 : Pengaturan port Bridge

Buat bridge untuk ether1 (trunk), ether2 (access), dan ether3 (access). Jangan lupa tentukan pvid untuk port access, detail cek pada gambar berikut:



Bridge Port <ether1>

General STP VLAN Status

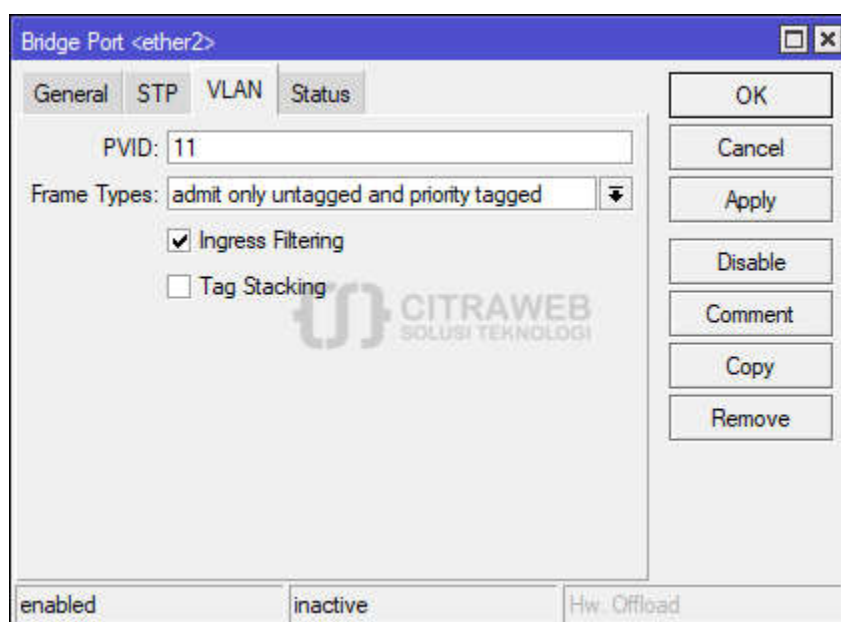
PVID: 1

Frame Types: admit all

Ingress Filtering

Tag Stacking

enabled inactive Hw. Offload



Bridge Port <ether2>

General STP VLAN Status

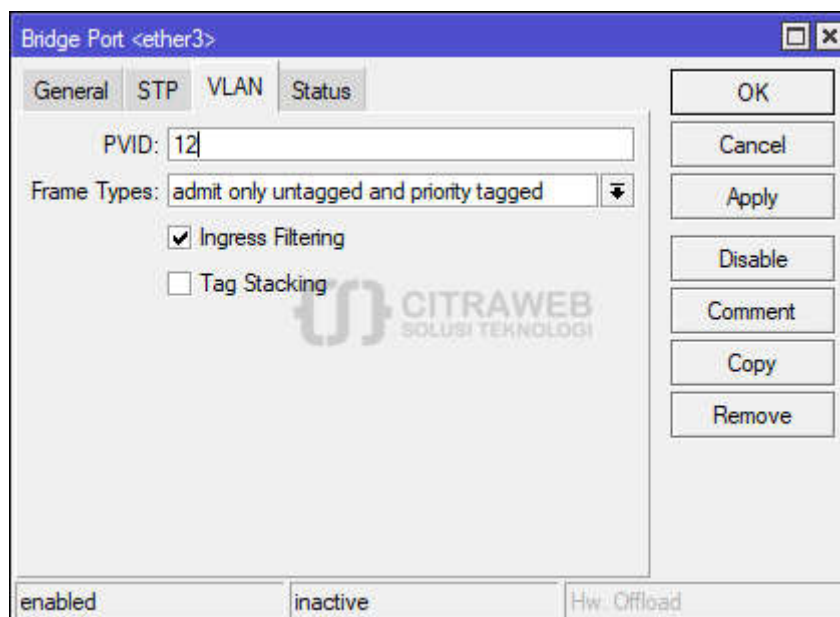
PVID: 11

Frame Types: admit only untagged and priority tagged

Ingress Filtering

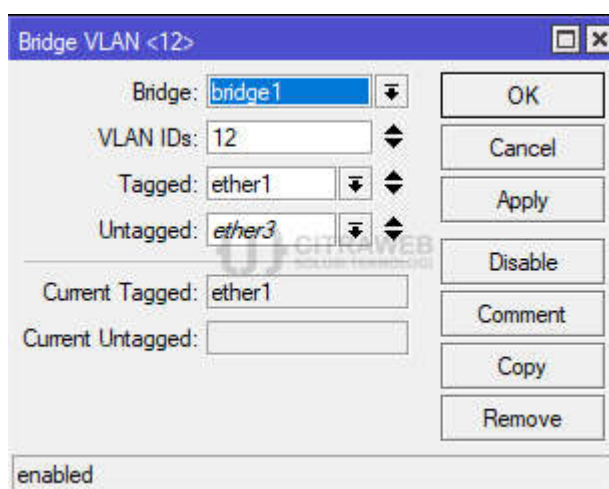
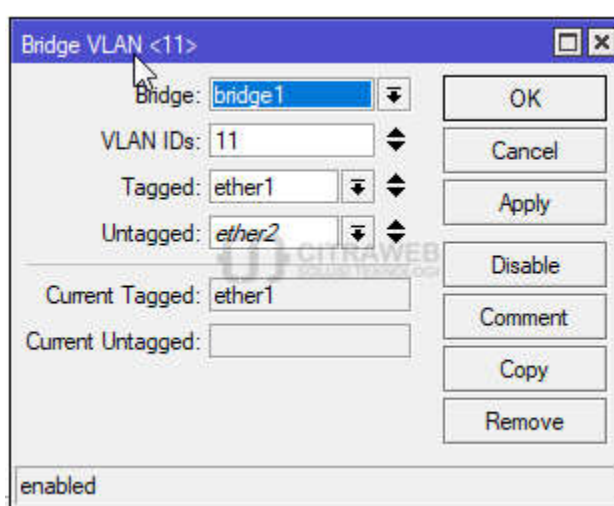
Tag Stacking

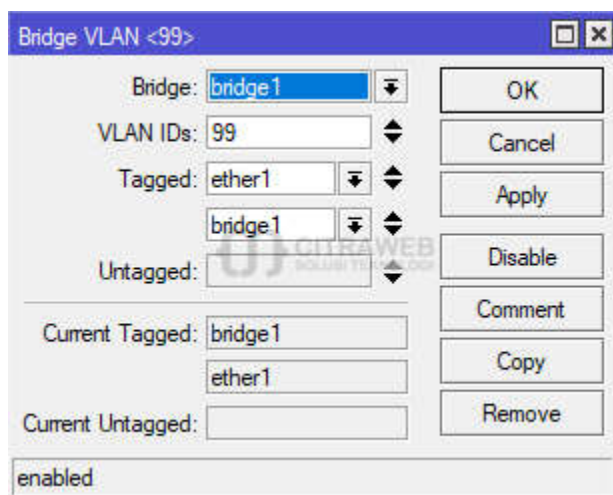
enabled inactive Hw. Offload



Gambar 38 : Pengaturan VLAN ID 1

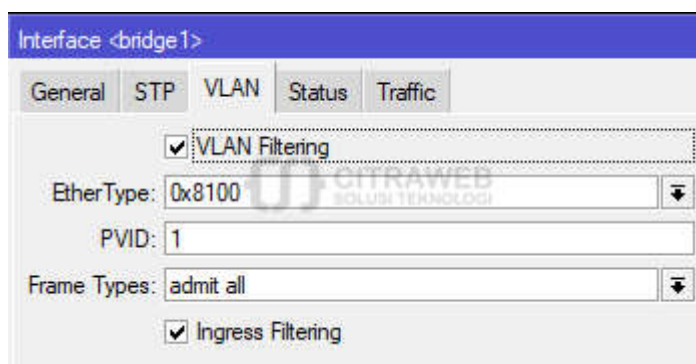
Selanjutnya buat pada tab VLANs untuk vlan 11, vlan 12, dan vlan 99. Untuk VLAN management yaitu vlan 99, tambahkan juga port bridge sebagai tagged.





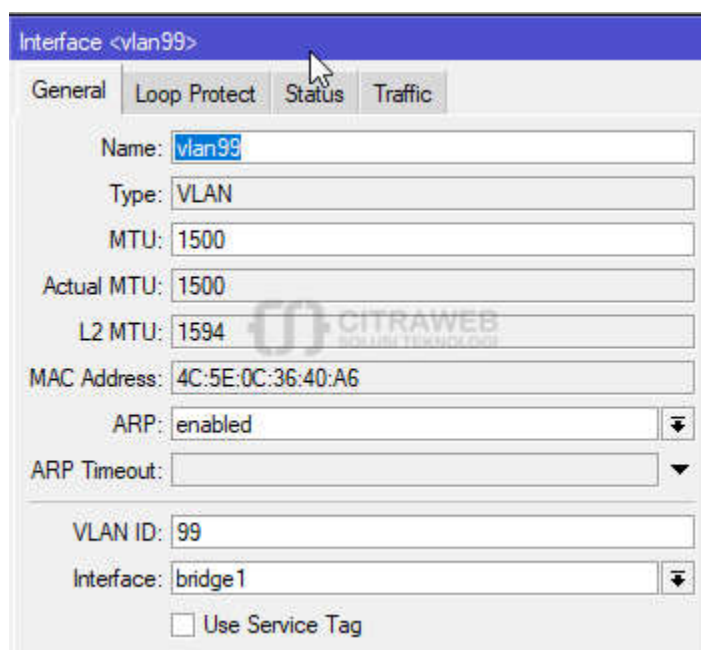
Gambar 39 : Pengaturan VLAN ID 2

Setelah itu bisa kita aktifkan untuk vlan filtering nya.



Gambar 40 : Mengaktifkan VLAN filtering

Kemudian kita bisa membuat interface vlan dengan vlan id 99. Setelah itu bisa diberi IP pada interface vlan99 tersebut sesuai dengan alokasi untuk IP vlan management yang sudah teman teman tentukan sebelumnya. Sampai disini vlan management untuk CRS 3XX Series sudah bisa digunakan.



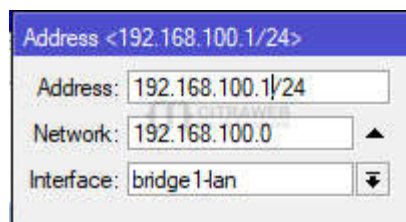
Gambar 41 : Penamaan VLAN

Konfigurasi VLAN Management pada CRS 1XX / 2XX Series

Untuk konfigurasi VLAN pada CRS 1XX / 2XX Series ini sedikit berbeda. Kita tidak menggunakan menu bridge, namun menggunakan menu switch.

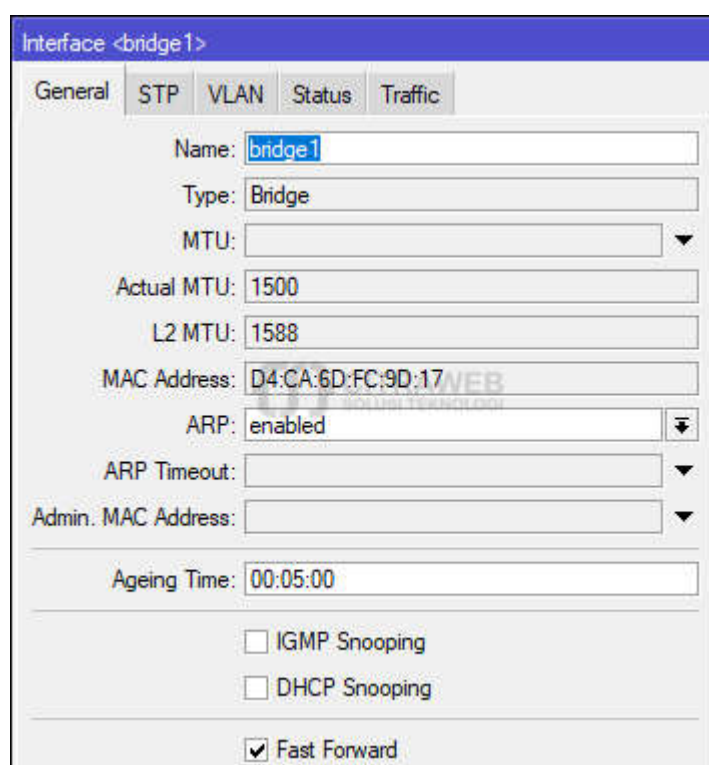
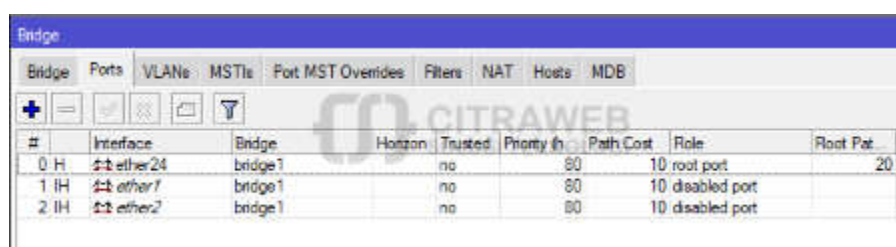
- **Mode Untagged**

Konfigurasi pada router, IP Address untuk management terpasang pada interface yang mengarah ke switch.



Gambar 42 : Input IP Address

Untuk konfigurasi pada switch bisa dilihat pada gambar berikut:

#	Interface	Bridge	Horizon	Trusted	Priority (h)	Path Cost	Role	Root Pat
0	H ether24	bridge1		no	80	10	root port	20
1	IH ether1	bridge1		no	80	10	disabled port	
2	IH ether2	bridge1		no	80	10	disabled port	

Gambar 43 : Penambahan bridge

Kita buat terlebih dahulu untuk bridge nya, masukkan port ethernet yang menjadi trunk dan access di satu bridge yang sama. Pada contoh ini ether24 adalah trunk, sedangkan ether1 dan ether2 adalah access.

Selanjutnya kita masuk ke menu Switch → VLAN

Tambahkan konfigurasi Ingress VLAN

Ingress VLAN Translation <ether1>	Ingress VLAN Translation <ether2>
Ports: ether1	Ports: ether2
Protocol:	Protocol:
Service VLAN Lookup For: any	Service VLAN Lookup For: any
Service VID:	Service VID:
Service PCP:	Service PCP:
Service DEI:	Service DEI:
Customer VLAN Lookup For: any	Customer VLAN Lookup For: any
Customer VID: 0	Customer VID: 0
Customer PCP:	Customer PCP:
Customer DEI:	Customer DEI:
New Service VID:	New Service VID:
New Customer VID: 11	New Customer VID: 12
<input type="checkbox"/> PCP Propagation	<input type="checkbox"/> PCP Propagation
<input checked="" type="checkbox"/> SA Learning	<input checked="" type="checkbox"/> SA Learning
enabled	enabled

Gambar 44 : Menu ingress VLAN

Tambahkan konfigurasi Egress VLAN

Switch Egress Tag VLAN <11>

VLAN ID: 11

Tagged Ports: ether24

OK

Cancel

Apply

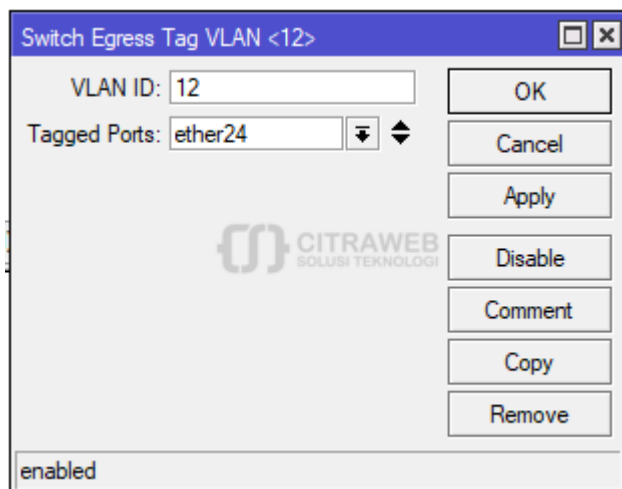
Disable

Comment

Copy

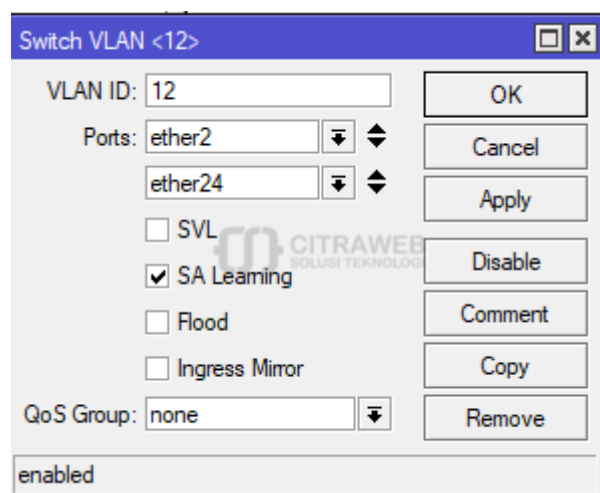
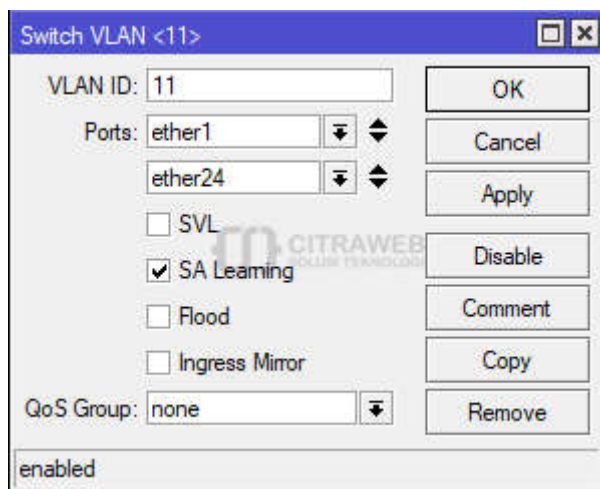
Remove

enabled



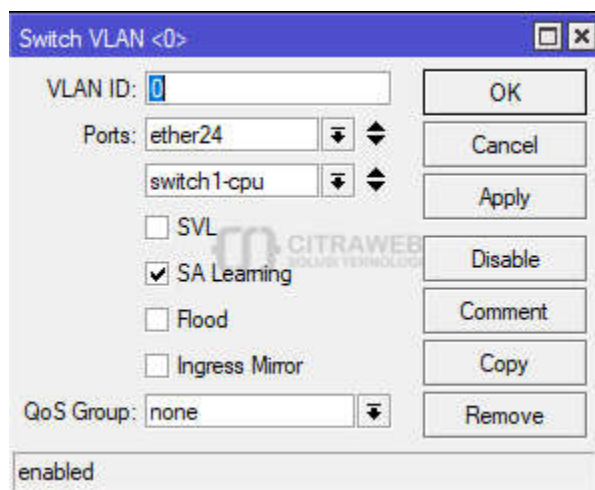
Gambar 45 : Penambahan ingress VLAN

Konfigurasi Switch VLAN



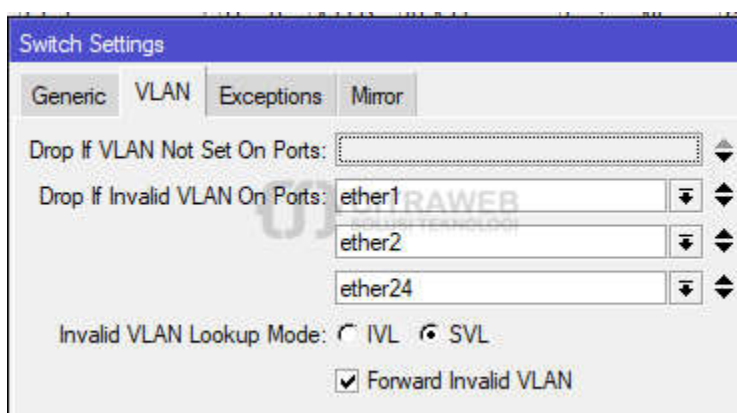
Gambar 46 : Konfigurasi switch VLAN

Kita tambahkan juga vlan id 0 untuk port ether24 (trunk) dan switch1-cpu.



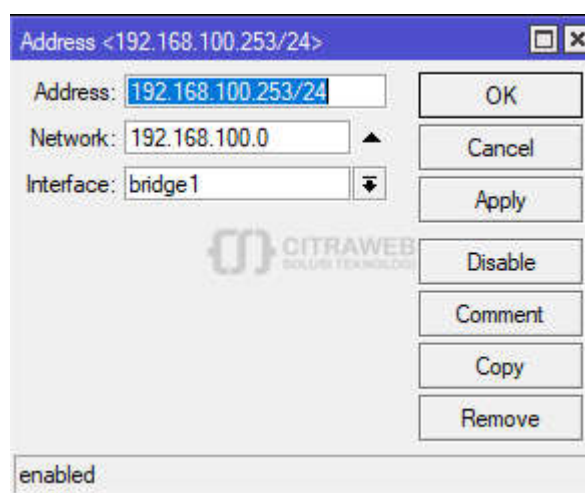
Gambar 47 : Penambahan VLAN ID

Konfigurasi pada menu switch → settings dan set untuk Drop If Invalid VLAN On Ports ether24 (trunk), ether1 (access), dan ether2 (access).



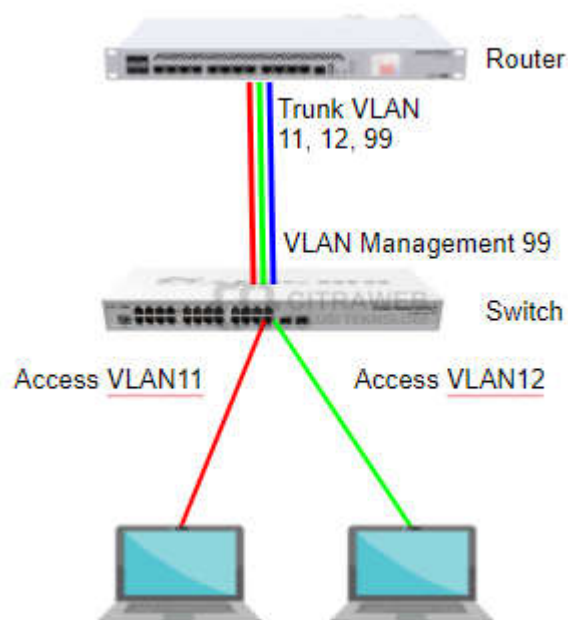
Gambar 48 : Setting dan set drof if

Kemudian sudah bisa kita tambahkan IP address untuk interface bridge1 nya.



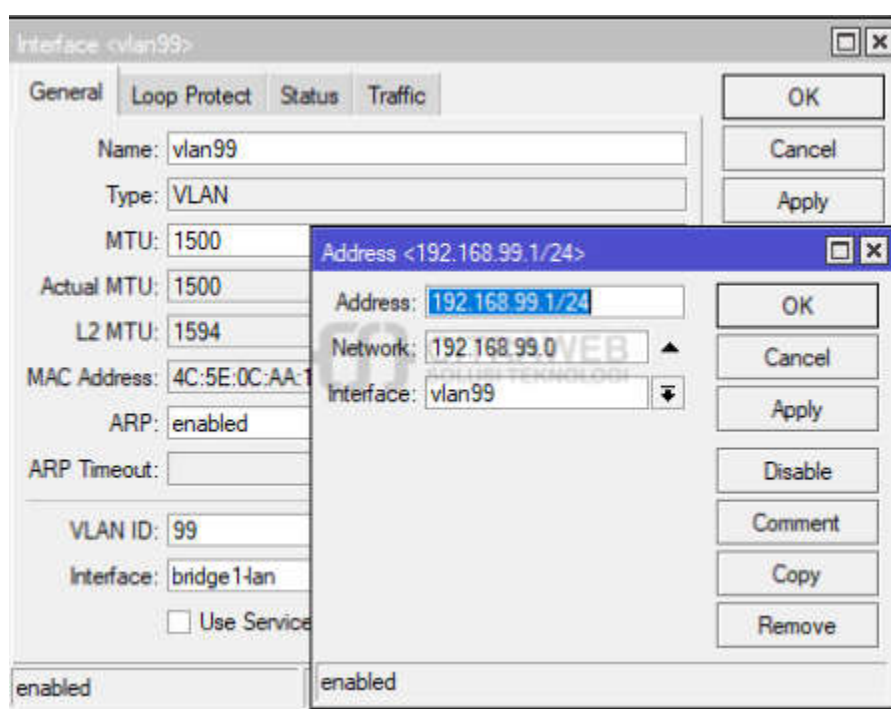
Gambar 49 : Input IP Address

- Mode Tagged



Gambar 50 : Topologi VLAN

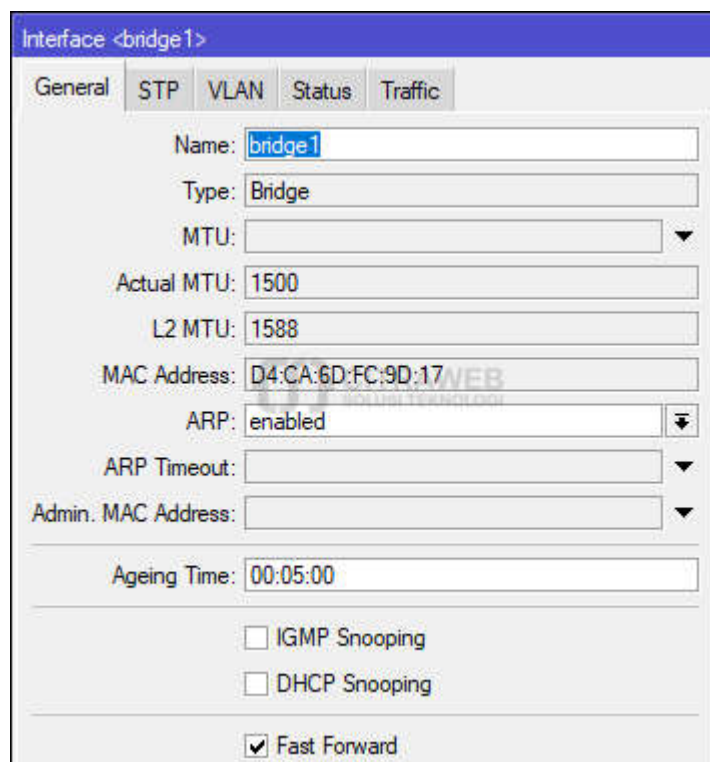
Konfigurasi pada router



Gambar 51 : Input IP address

Seperti kasus pertama, pada router membuat interface vlan management dan berikan ip address pada vlan tersebut.

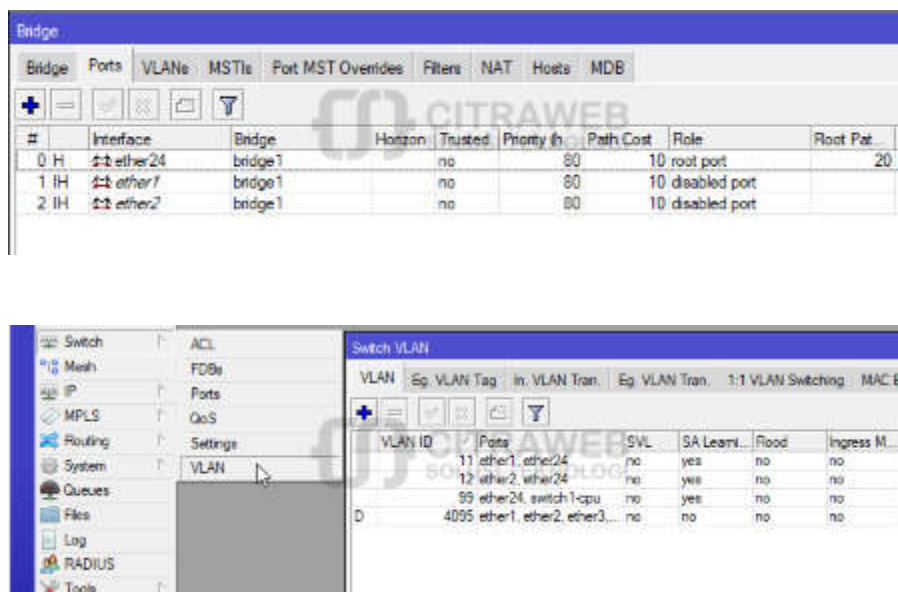
Konfigurasi pada switch



Gambar 52 : Penambahan Bridge

Kita buat terlebih dahulu untuk bridge nya, masukkan port ethernet yang menjadi trunk dan access di satu bridge yang sama.

Kemudian kita masuk ke menu Switch → VLAN



Gambar 53 : TAB menu Switch VLAN

Tambahkan konfigurasi Ingress VLAN

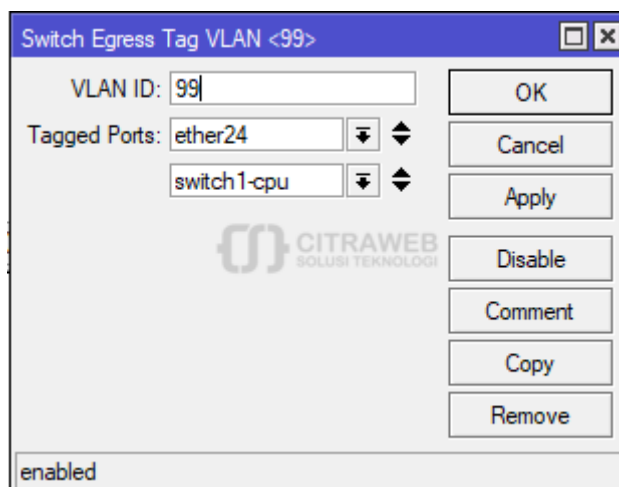
Ingress VLAN Translation <ether1>	Ingress VLAN Translation <ether2>
Ports: ether1	Ports: ether2
Protocol:	Protocol:
Service VLAN Lookup For: any	Service VLAN Lookup For: any
Service VID:	Service VID:
Service PCP:	Service PCP:
Service DEI:	Service DEI:
Customer VLAN Lookup For: any	Customer VLAN Lookup For: any
Customer VID: 0	Customer VID: 0
Customer PCP:	Customer PCP:
Customer DEI:	Customer DEI:
New Service VID:	New Service VID:
New Customer VID: 11	New Customer VID: 12
<input type="checkbox"/> PCP Propagation	<input type="checkbox"/> PCP Propagation
<input checked="" type="checkbox"/> SA Learning	<input checked="" type="checkbox"/> SA Learning
enabled	enabled

Gambar 54 : Konfigurasi ingress VLAN

Kemudian tambahkan konfigurasi Egress VLAN. Pada vlan id 99 tambahkan juga switch1-cpu untuk Tagged Ports nya.

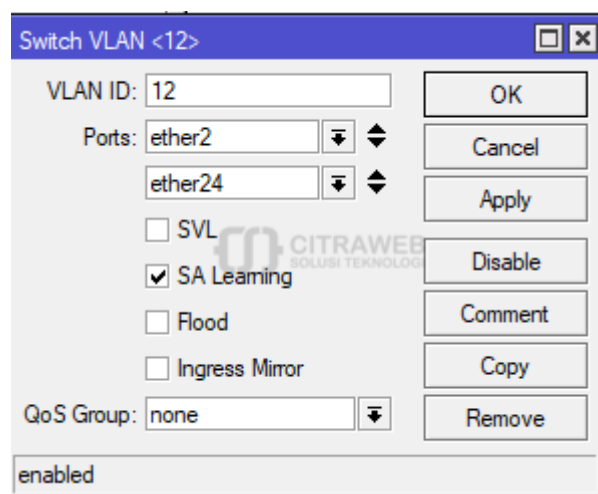
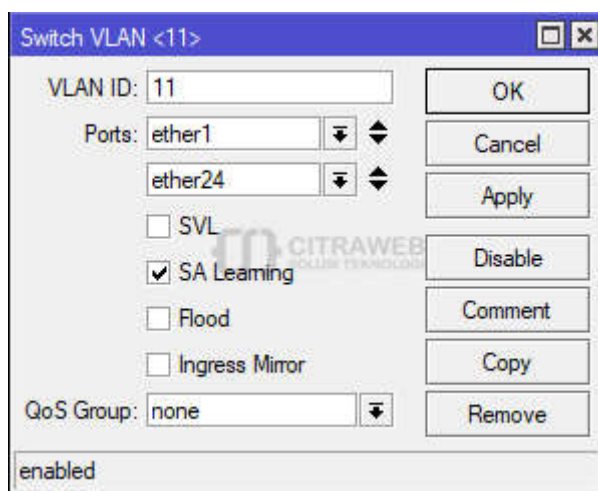
Switch Egress Tag VLAN <11>
VLAN ID: 11
Tagged Ports: ether24
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Disable"/> <input type="button" value="Comment"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/>
enabled

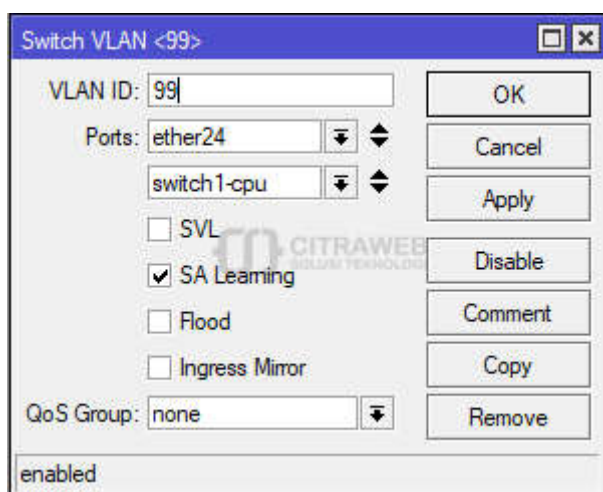
Switch Egress Tag VLAN <12>
VLAN ID: 12
Tagged Ports: ether24
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Disable"/> <input type="button" value="Comment"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/>
enabled



Gambar 55 : Penambahan VLAN 1

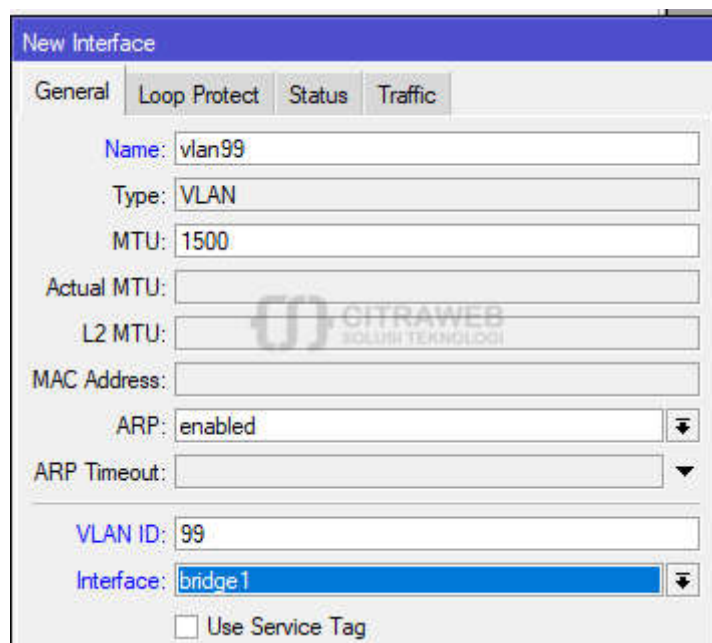
Selanjutnya tambahkan konfigurasi Switch VLAN, pada vlan management yaitu vlan 99 tambahkan switch1-cpu untuk port nya.





Gambar 56 : Penambahan VLAN 2

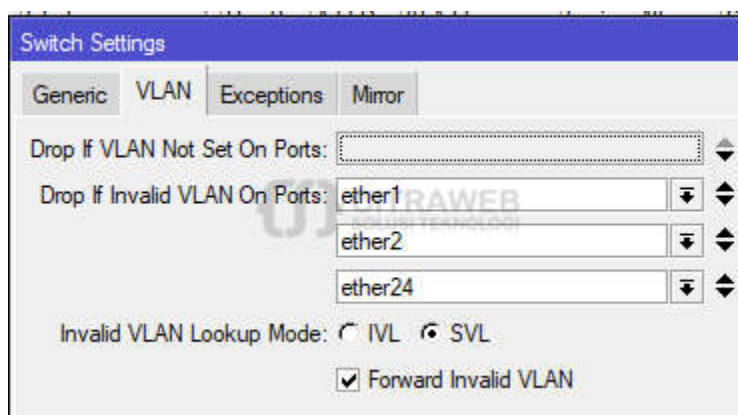
Setelah itu kita bisa buat interface vlan baru dengan vlan id 99 dan interface bridge yang kita buat di awal tadi.



Gambar 56 : Pembuatan Interfaces VLAN

Terakhir, kita konfigurasi pada menu switch → settings dan set untuk Drop If Invalid VLAN On Ports ether24 (trunk), ether1 (access), dan ether2 (access).

Kita sudah bisa menambahkan IP address pada interface vlan99 yang kita buat tadi dan vlan management sudah bisa digunakan.

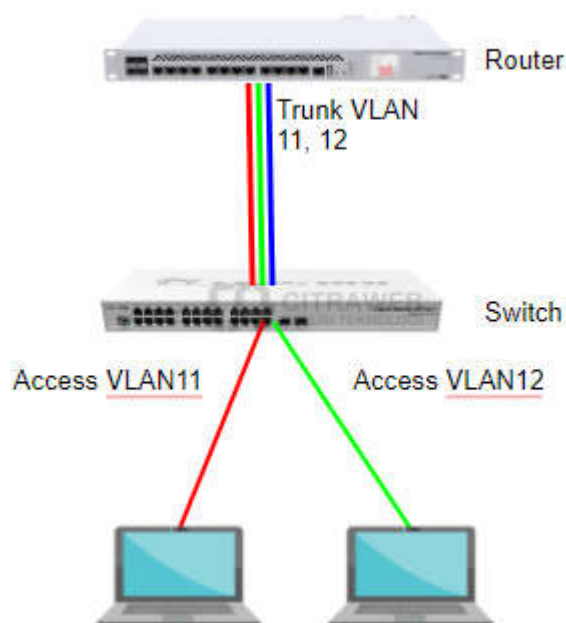


Gambar 57 : Menu TAB switch

Konfigurasi VLAN Management pada CSS (Switch OS)

Karena seri CSS menggunakan Switch OS, maka bisa kita konfigurasi melalui web browser. Memang untuk tampilannya lebih simpel dari pada CRS yang menggunakan Router OS.

Untuk topologi yang kita gunakan masih sama.



Gambar 58 : Topologi VLAN





Gambar 59 : Tampilan menu switch OS

Pertama, kita konfigurasi terlebih dahulu untuk port yang menjadi trunk dan access. Untuk contoh kali ini kita menggunakan port 1 untuk trunk, port 2 untuk access vlan 11, dan port 3 untuk access vlan 13.



Gambar 60 : Input IP Address

Kemudian untuk membuat vlan management bisa kita atur di menu System. Tentukan "IP Address" dan "Allow From VLAN" kemudian klik apply. Tunggu sesaat dan seharusnya switch sudah bisa di akses.

ROUTING STATIC DAN ROUTING DINAMIS

A. Cara Kerja Routing

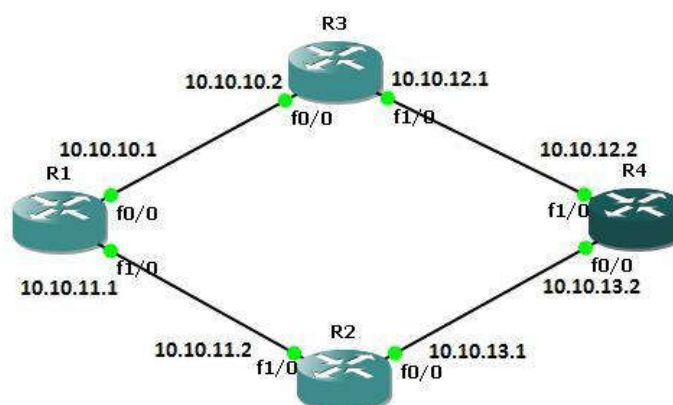
routing secara khusus bekerja dengan merujuk pada tabel *routing* internal dalam membuat keputusan tentang bagaimana merutekan paket di sepanjang jalur jaringan yang diminati.

Tabel *routing* bertugas mencatat jalur-jalur yang harus diambil paket untuk mencapai setiap tujuan. Dalam proses *routing* ini perangkat keras *router* bekerja sebagai gawai aktif yang bekerja dengan cara menerima paket internet, membaca *header*, memeriksa alamat tujuan, menentukan jalur mana yang harus dilalui, dan ke mana tujuan *routing* berdasarkan informasi dalam tabel *routing*.

Proses *routing* dilakukan dengan tiga jenis *routing* dan dua jenis algoritma *routing*. Hal ini dilakukan berdasarkan administrator jaringan secara manual dalam menyiapkan tabel perutean statis. Hal ini pada dasarnya bertugas untuk mengatur rute yang diambil oleh paket data internet di seluruh jaringan.

B. Macam-macam Routing

1. Static routing



Gambar 61 : Bentuk konfigurasi routing statis

Static routing merupakan jenis teknik *routing* jaringan yang bersifat statis dan berkonfigurasi manual. *Routing static* umumnya dikelola oleh administrator jaringan dan digunakan dalam skenario di mana parameter jaringan dan lingkungan jaringan tetap konstan/stabil.

Routing statis bisa optimal dalam situasi tertentu, meski begitu ada konsekuensi dari jenis jaringan *routing* ini seperti degradasi jaringan, latensi, dan kemacetan jaringan. Secara umum, *routing static* tidak fleksibel karena tidak memiliki penyesuaian ketika rute utama tidak tersedia. Kelebihan *routing* statis adalah tidak adanya penggunaan *bandwidth* antar *router* dan juga memiliki keamanan yang lebih baik karena terpusat pada administrator. Namun, *routing* statis memiliki kekurangan di bagian administrator manual dan juga kemampuan lebih di bidang topologi jaringan *routing*.

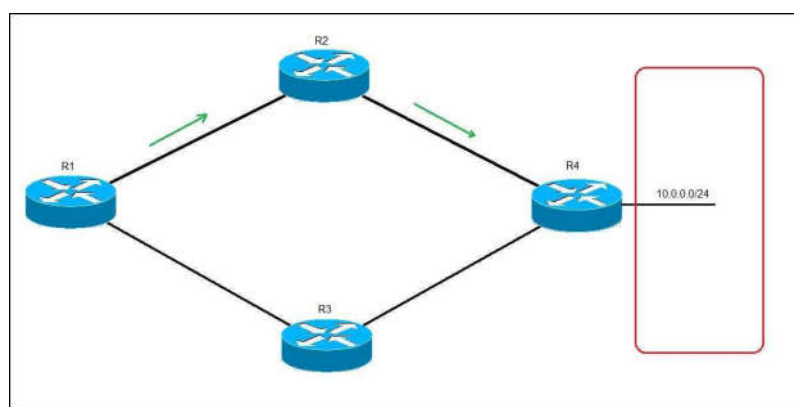
2. Default routing

Default routing merupakan metode *routing* yang mengandalkan konfigurasi untuk mengirim semua paket ke satu *router*. Pengiriman ini tidak bergantung pada jaringan tertentu dan di mana jaringan itu berada. Pengiriman yang fleksibel ini kemudian diteruskan ke *router* dalam suatu konfigurasi *routing default*.

Umumnya, *default routing* dipakai dalam sebuah *router* rintisan yang hanya memiliki satu rute untuk menjangkau semua jaringan lain. Sistem *default routing* ini juga akrab disebut dengan *gateway of last resort*, untuk dapat menuju ke semua paket data ke jaringan tertentu.

Router meneruskan paket menggunakan *default routing* ketika tidak ada rute khusus yang cocok dengan alamat IP tujuan paket di tabel *routing*. *Default routing* tidak spesifik dan digunakan untuk menghubungkan situs ISP (*Internet Service Provider*) atau situs utama.

3. Dynamic routing



Gambar 62 : Contoh konfigurasi dynamic routes

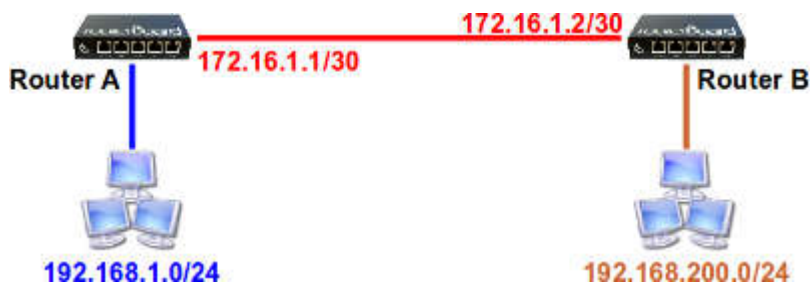
Dynamic routing atau perutean dinamis merupakan penyesuaian otomatis dari rute jaringan dalam tabel *routing*. *Dynamic routing* dapat menggunakan protokol tertentu dalam menemukan tujuan jaringan dan rute tertentu untuk mencapai tujuan tersebut.

Protokol *dynamic routing* memiliki beberapa fitur seperti *router* harus menjalankan protokol yang sama untuk bertukar rute dan *router* perlu mengiklankan ke *router* lainnya jika terjadi perubahan topologi *routing*. Tabel *routing* dinamis dapat terbaru secara otomatis dan dapat menggunakan berbagai protokol *routing* untuk menentukan jalur terpendek dan tercepat. *Dynamic routing* lebih efektif secara proses, terlebih pada jaringan yang berukuran sedang atau besar.

Secara khusus, *dynamic routing* merupakan jenis *routing* yang paling mudah dikonfigurasi dan lebih efektif dalam memiliki rute terbaik untuk sebuah tujuan jaringan serta dapat menemukan jaringan terluar. Namun, *dynamic routing* memiliki kelemahan karena lebih boros *bandwidth* dan kurang aman dibandingkan *routing* statis.

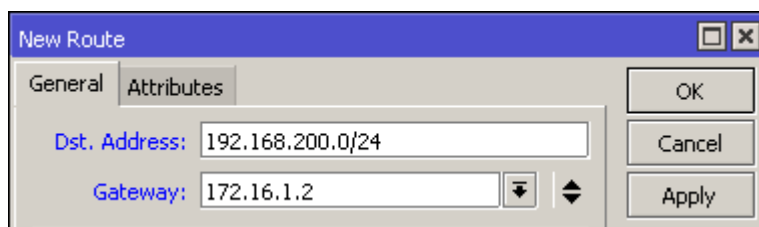
C. Konfigurasi Routing Static di Mikrotik RouterBoard

Topologi 1

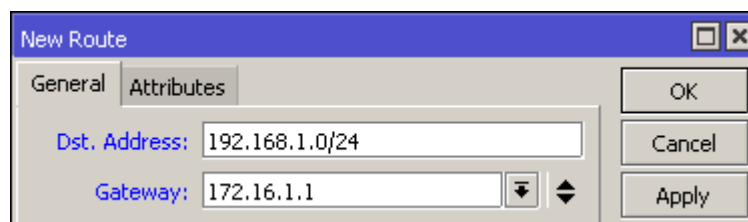


Gambar 63 : topologi 1

Topologi yang paling sederhana. Router A dan Router B direct connect / terhubung langsung via ethernet. Maka pengaturan routing yang perlu ditambahkan sebagai berikut



Gambar 64 : Penambahan routing di Router A

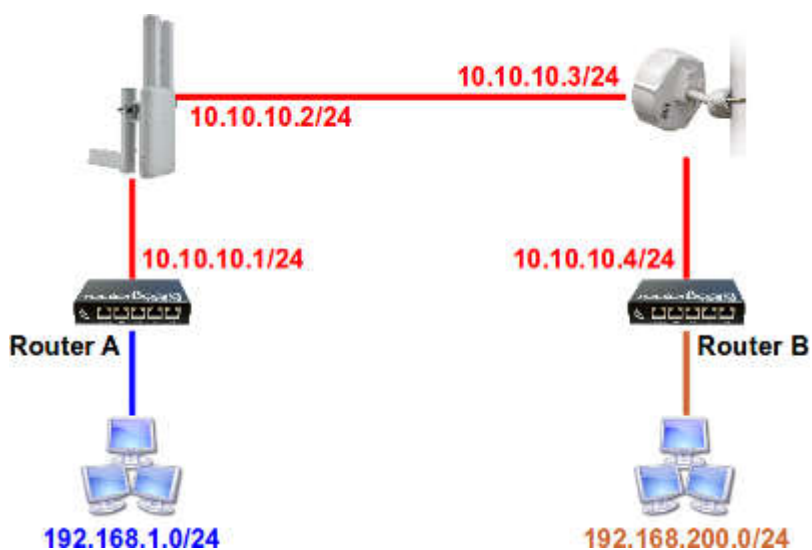


Gambar 65 : Penambahan routing di Router B

Cukup mudah bukan??

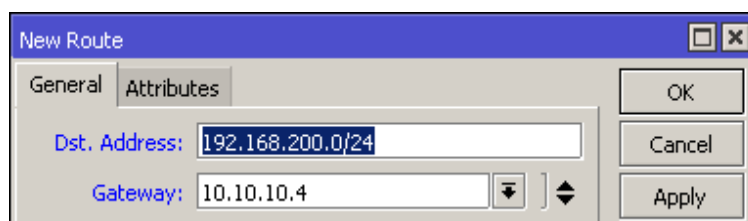
Sekarang bagaimana kalau router A dan router B tidak bisa direct connect, mungkin harus melewati perangkat lain, misalnya link wireless, atau mungkin tunnel / VPN?. Contoh berikutnya yaitu topologi 2.

Topologi 2

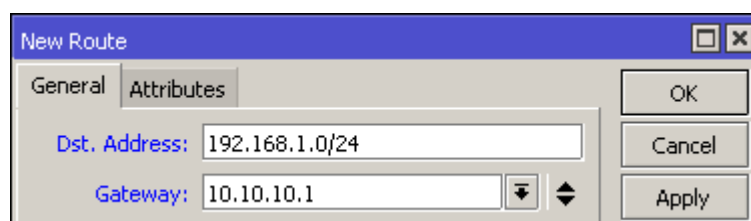


Gambar 66 : Topologi routing 2

Disini Router A dan Router B supaya bisa berkomunikasi harus melewati perangkat lain yang melakukan **BRIDGING**. Pada umumnya, perangkat-perangkat router / wireless bisa melakukan fungsi bridging. Ciri paling mudah mengenali perangkat yang dilewati (dalam contoh ini perangkat wireless) apakah melakukan bridging atau tidak adalah IP Router A, IP wireless router/perangkat lain dan IP Router B memiliki IP segment yang sama (10.10.10.x/24) Karena Router A dan Router B memiliki IP segment yang sama, maka metode routingnya sama dengan contoh topologi 1. Tinggal disesuaikan IPnya



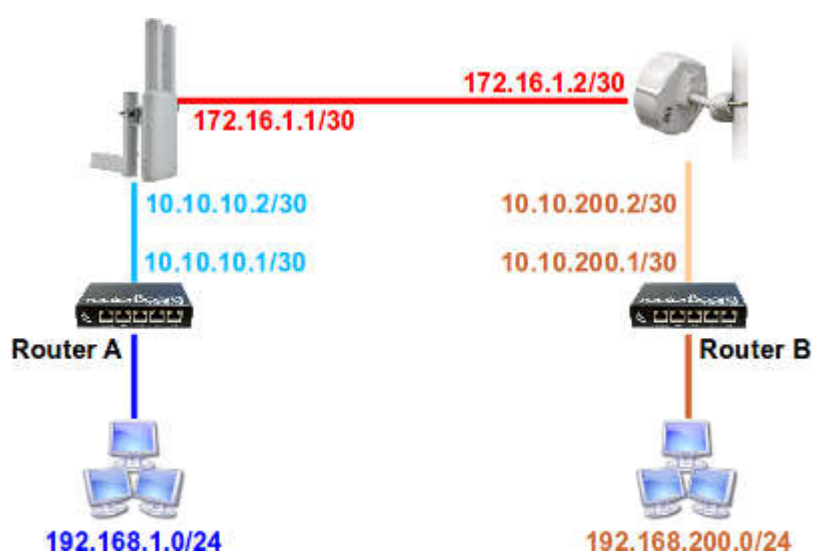
Gambar 67 : Penambahan routing di Router A



Gambar 68 : Penambahan routing di Router B

Dari kedua contoh topologi diatas, mungkin masih terlalu sederhana. Mari kita ulas untuk topologi yang sedikit lebih kompleks.

Topologi 3.



Gambar 69 : Topologi routing 3

Topologi 3 ini mirip dengan contoh topologi sebelumnya (topologi 2), tetapi untuk topologi 3 ini,

perangkat yang menghubungkan antara Router A dan Router B juga menggunakan metode **ROUTING**. Apakah anda melihat perbedaannya??

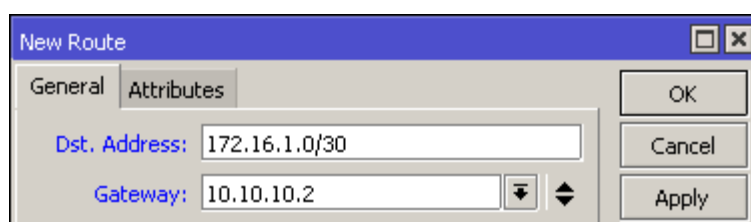
Benar sekali, antara router A, wireless Router, dan router B menggunakan IP segment yang berbeda.

Apakah sudah mulai ada bayangan di router mana kita harus membuat membuat tabel routingnya?

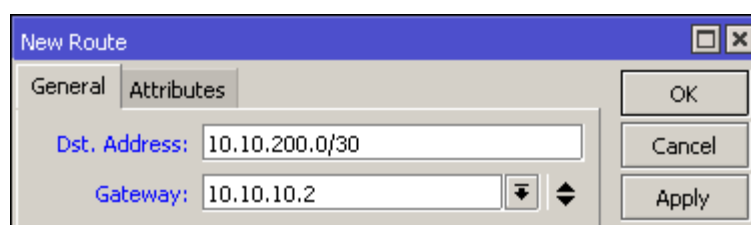
Jawabannya adalah di keempat router tersebut.

Capture dari tabel routing keempat router tersebut sebagai berikut :

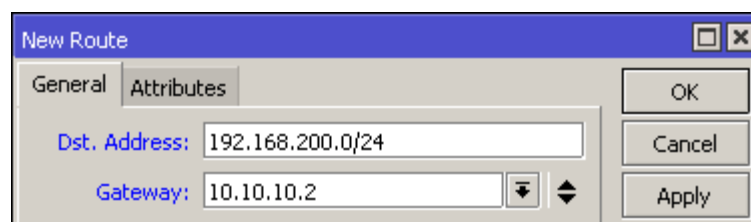
Di sisi Router Indoor A :



Gambar 70 : Penambahan routing di Router indoor A pertama

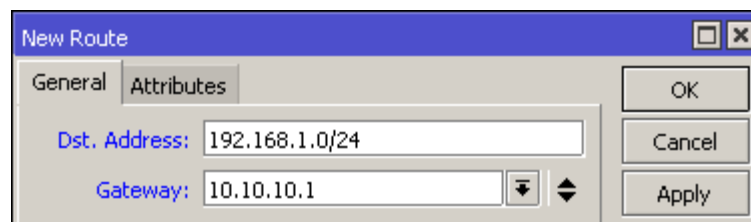


Gambar 71 : Penambahan routing di Router indoor A kedua

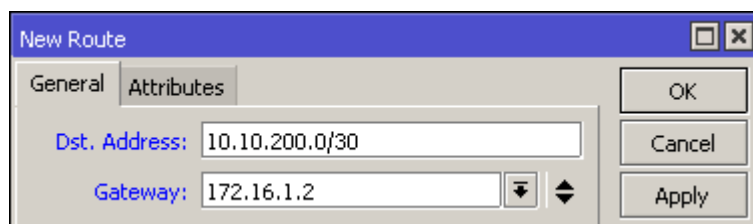


Gambar 72 : Penambahan routing di Router indoor A ketiga

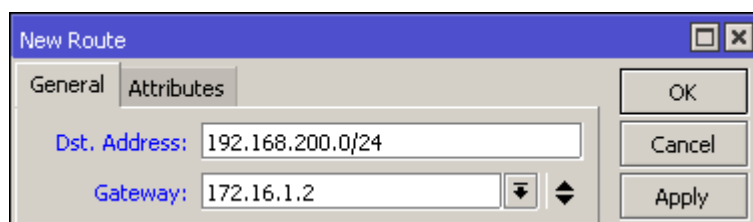
Di sisi Wireless Router A :



Gambar 73 : Penambahan routing di Wireless Router A pertama

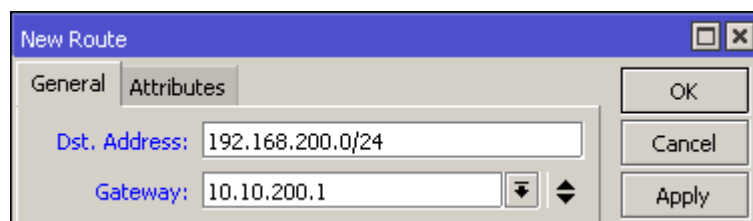


Gambar 74 : Penambahan routing di Wireless Router A kedua

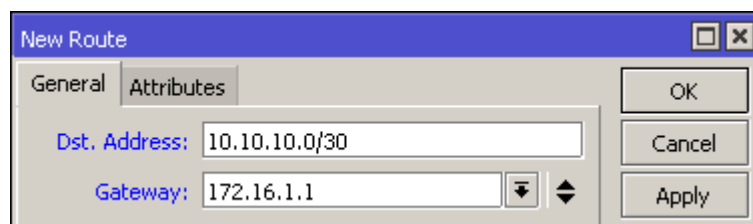


Gambar 75 : Penambahan routing di wireless Router A ketiga

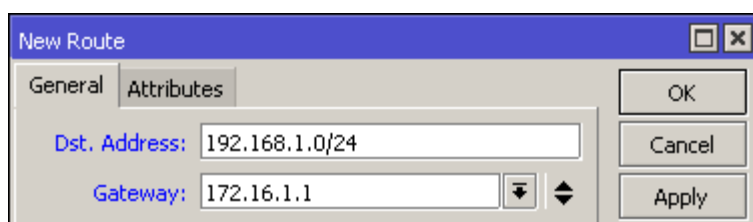
Di sisi Wireless Router B :



Gambar 76 : Penambahan routing di wireless Router B pertama

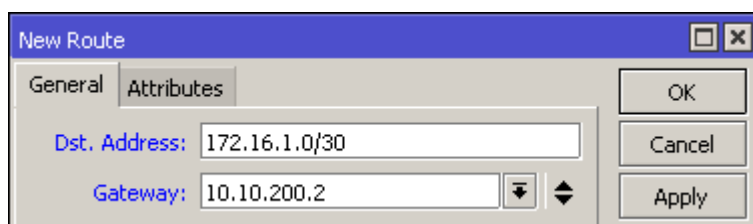


Gambar 77 : Penambahan routing di wireless Router B kedua

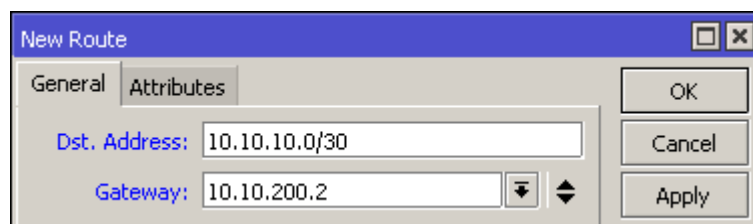


Gambar 78 : Penambahan routing di wireless Router B ketiga

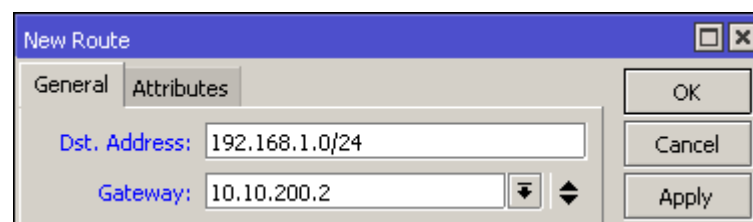
Di sisi Router Indoor B :



Gambar 79 : Penambahan routing di Router indoor B pertama



Gambar 80 : Penambahan routing di Router indoor B kedua



Gambar 81 : Penambahan routing di Router indoor B ketiga

D. Konfigurasi Routing Dinamic di Mikrotik RouterBoard

Open Shortest Path First (OSPF) adalah sebuah protokol routing otomatis (Dynamic Routing) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar network mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah Autonomus System (AS) yaitu sebuah gabungan dari beberapa jaringan yang sifatnya routing dan memiliki kesamaan metode serta policy pengaturan network, yang semuanya dapat dikendalikan oleh network administrator. Dan memang kebanyakan fitur ini digunakan untuk management dalam skala jaringan yang sangat besar. Oleh karena itu untuk mempermudah penambahan informasi routing dan meminimalisir kesalahan distribusi informasi routing, maka OSPF bisa menjadi sebuah solusi.

OSPF termasuk di dalam kategori IGP (Interior Gateway Protocol) yang memiliki kemampuan Link-State dan Algoritma Dijkstra yang jauh lebih efisien dibandingkan protokol IGP yang lain. Dalam operasinya OSPF menggunakan protokol sendiri yaitu protokol 89.

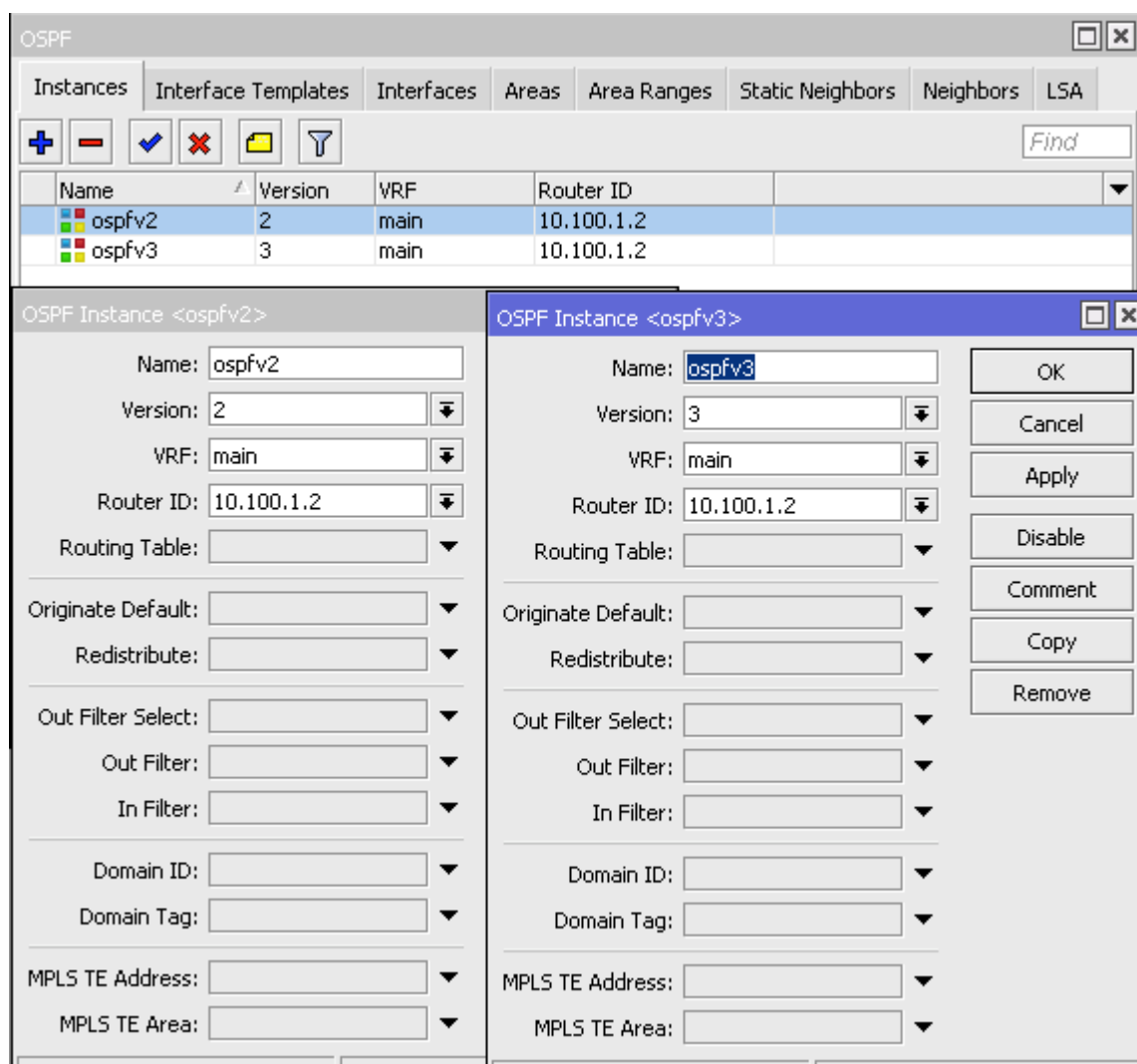
Pada kesempatan kali ini, kami akan mencoba membahas mengenai OSPF pada RouterOS versi 7, dimana untuk konfigurasi OSPF pada versi ini terdapat sedikit penyesuaian. OSPF pada versi 7 akan dibagi menjadi 2 bagian yaitu OSPFv2 dan OSPFv3. OSPFv2 akan lebih fokus ke IPv4 dan OSPFv3 digunakan untuk IPv6.

Konfigurasi

Pada Mikrotik Router OS versi7, OSPFv3 dan OSPFv2, konfigurasinya di lakukan di satu menu yaitu /routing ospf. Saat ini, pada versi 7.1.1 stable tidak disediakan instance dan area default, sehingga ketika ingin melakukan konfigurasi OSPF pada Router OSv7, maka kita bisa membuat instance dan area terlebih dahulu.

Konfigurasi Instance

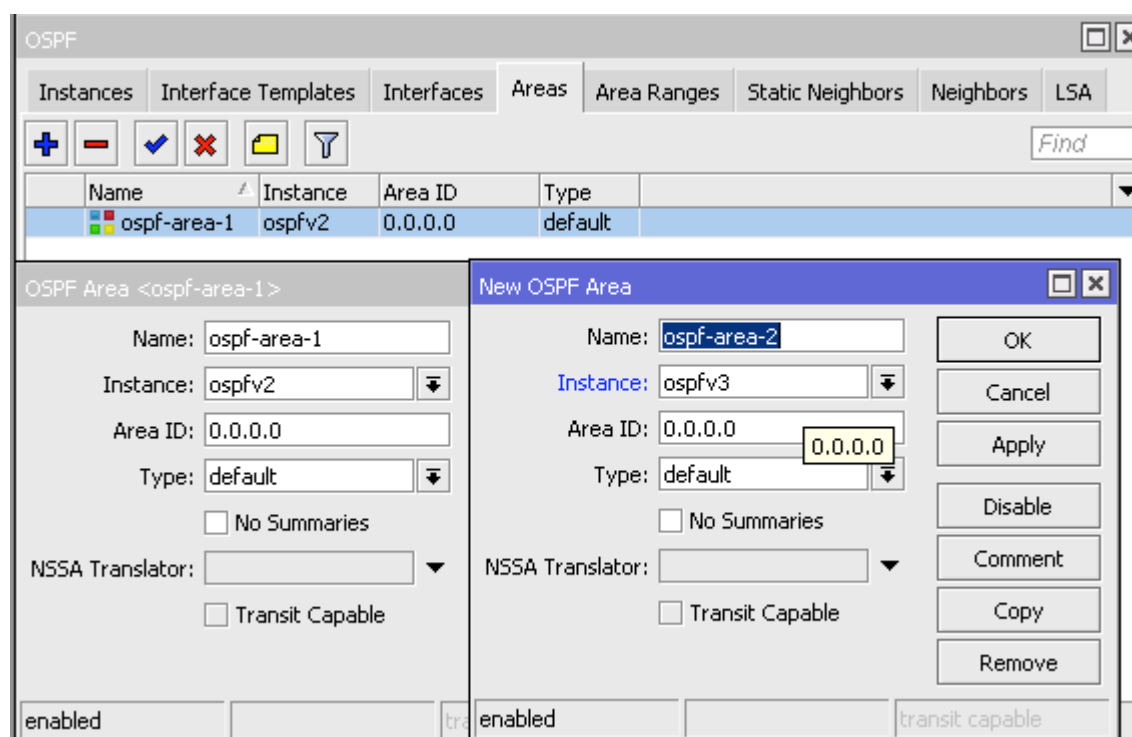
Tambahkan instance untuk mendefinisikan Router ID dan versi OSPF yang digunakan.



Gambar 82 : Menambahkan Instance OSPF

Konfigurasi Area

Lalu tambahkan Area yang akan kita gunakan untuk jaringan Backbone OSPF.

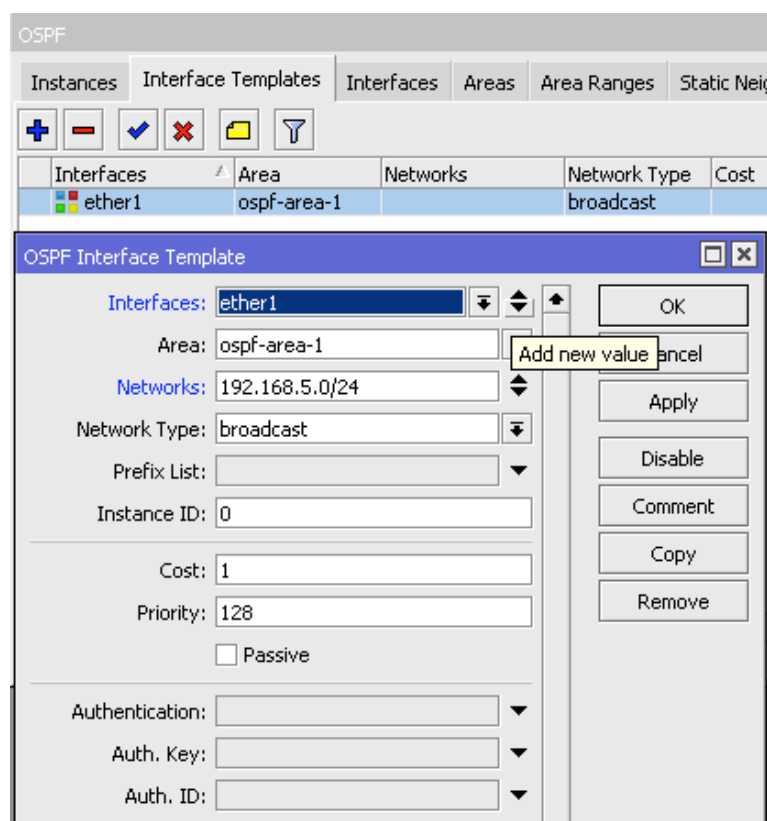


Gambar 83 : OSPF Area

Selanjutnya untuk mengaktifkan ospf, kita perlu menambahkan interface template. Menu ini agak berbeda dibandingkan versi sebelumnya (v6) yang menggunakan menu Network.

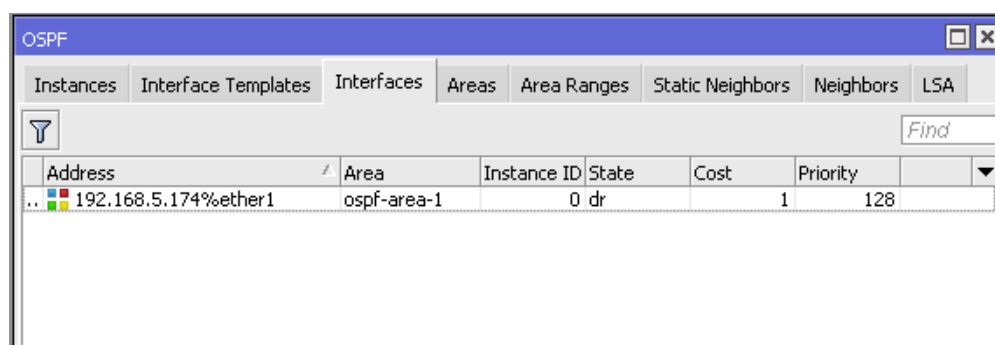
Tambahkan interface template baru, dan tentukan ke interface atau network mana kita akan mengaktifkan OSPF. Kita bisa menggunakan parameter Network ATAU Interface.

Konfigurasi Interface Template

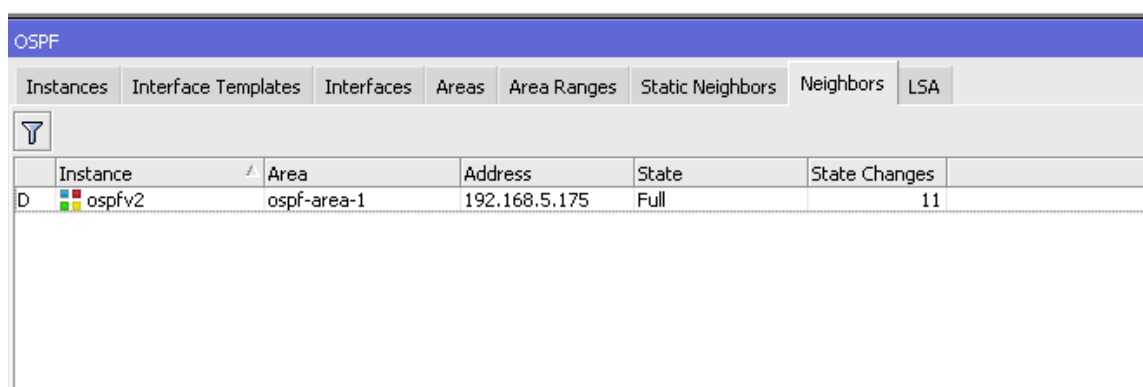


Gambar 84 : OSPF interfaces template

Untuk monitoring apakah ospf sudah berjalan atau tidak, kita bisa menggunakan menu **Interfaces**. Bisa juga menggunakan menu **Neighbors** untuk mengetahui kondisi pertukaran data dan state yang berjalan di OSPF.



Gambar 85 : Menu neighbors



Instance	Area	Address	State	State Changes
D ospfv2	ospf-area-1	192.168.5.175	Full	11

Gambar 86 : OSPF interfaces

Dengan konfigurasi diatas, OSPF pada versi 7 sudah berjalan dan bisa saling komunikasi. Router juga akan melakukan pertukaran informasi routing jika terdapat perubahan di jaringan.

Secara default, ketika mengaktifkan routing dynamic maka kita akan menerima seluruh informasi routing yang tersedia. Untuk mengatasi hal ini maka kita bisa mengaktifkan Routing Filter. Routing Filter pada versi 7 Mikrotik juga sedikit berbeda formatnya dengan versi 6.

Network Address Translation (NAT)

A. Pengetian

Network Address Translation (NAT) merupakan sebuah sistem untuk menggabungkan lebih dari satu komputer untuk dihubungkan ke dalam jaringan internet hanya dengan menggunakan sebuah alamat IP. Sehingga setiap komputer di dalam NAT ketika berselancar di internet akan terlihat memiliki alamat IP yang sama jika dilacak. Dengan kata lain, sebuah alamat IP pada jaringan lokal akan terlebih dahulu ditranslasikan oleh NAT untuk dapat mengakses IP publik di jaringan komputer. Sebelum proses translasi ini, maka pengguna tidak dapat terhubung ke internet.

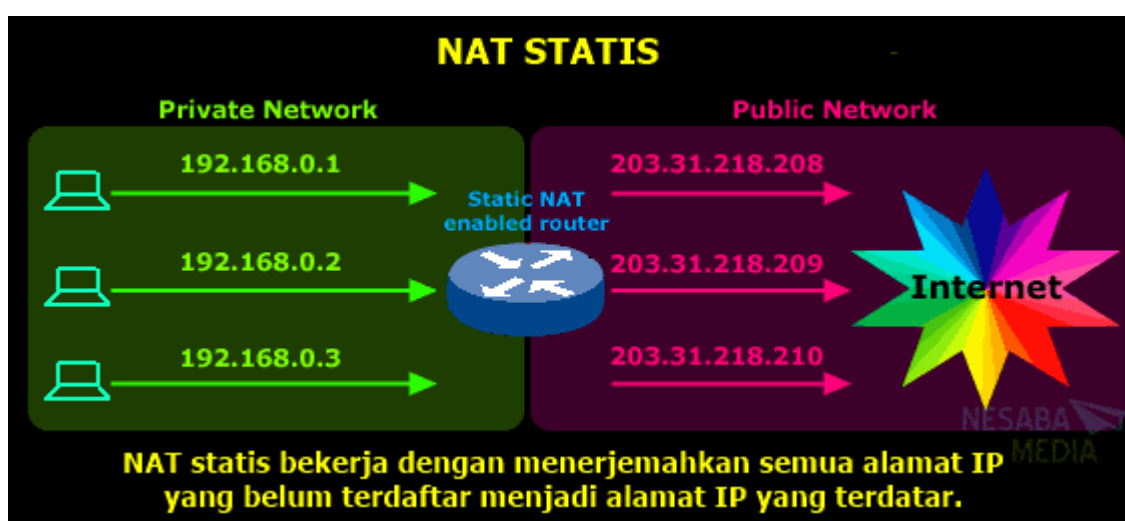
Banyak yang berpendapat bahwa NAT sebetulnya mirip dengan proxy server, namun bedanya adalah jika proxy server menyediakan mekanisme caching, tak begitu halnya dengan NAT. Sehingga dengan penggunaan NAT, tidak ada batasan mengenai jumlah halaman web yang dapat diakses.

Cukup banyak pengguna NAT yang memanfaatkan sistem ini, bisa jadi dikarenakan ketersediaan alamat IP yang terbatas, membutuhkan keamanan lebih, atau ada pula yang menggunakan NAT karena dinilai lebih fleksibel dalam hal administrasi jaringan, sebab jaringan NAT didesain menyederhanakan alamat IP dan untuk melindunginya.

B. Jenis-Jenis NAT

Secara singkat, ada empat jenis NAT yang perlu diketahui, yaitu NAT tipe statis, dinamis, overloading, dan overlapping. Perbedaan antara keempatnya akan dibahas dalam poin berikut :

1. NAT Statis



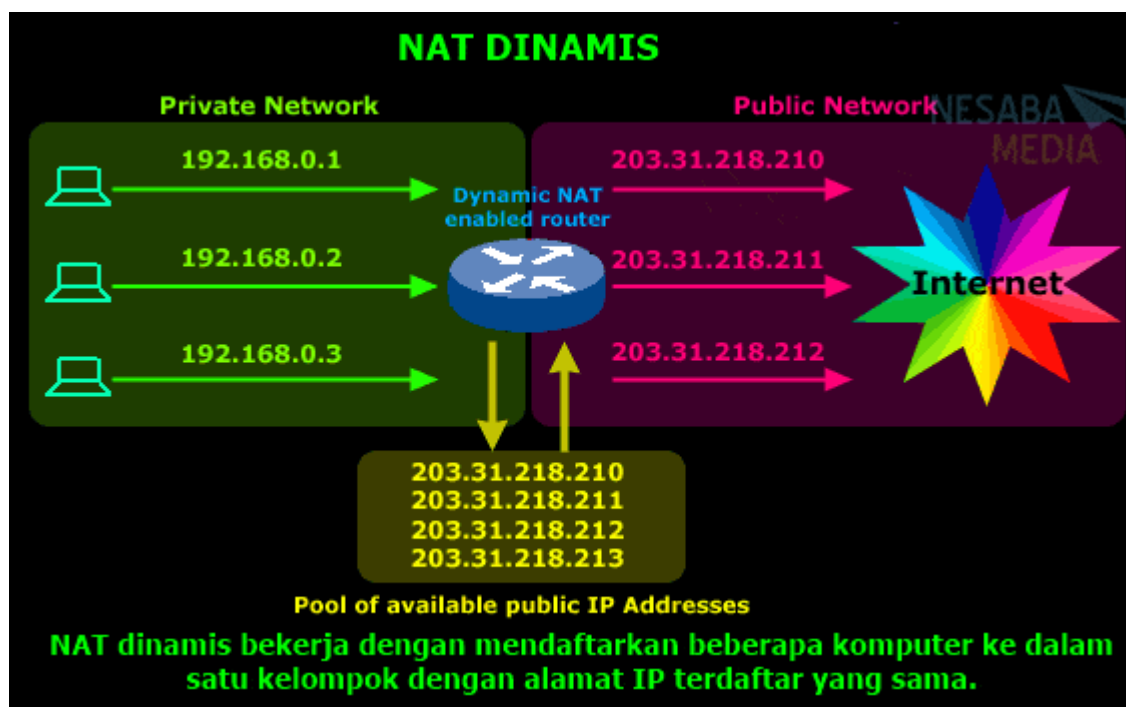
Gambar 87 : NAT Static

Bekerja dengan menerjemahkan semua alamat IP yang belum terdaftar menjadi alamat IP yang terdaftar. NAT Statis banyak digunakan untuk komputer yang ingin dapat diakses dari luar.

NAT statis ini sebetulnya bisa dibilang pemborosan terhadap alamat IP yang didaftarkan, sebab setiap satu komputer dipetakan untuk satu alamat IP terdaftar, sehingga jika ada banyak komputer yang didaftarkan, tentu semakin terbatas pula alamat IP yang masih tersedia.

Kekurangan lain dari NAT Statis adalah kurang aman dibandingkan NAT dinamik, sebab setiap komputer memiliki alamat IP tersendiri, dan akhirnya risiko penyusup masuk langsung ke dalam jaringan private lebih besar.

2. NAT Dinamis



Gambar 88 : NAT Dinamic

Berbeda dengan NAT Statis, NAT Dinamis bekerja dengan mendaftarkan beberapa komputer ke dalam satu kelompok dengan alamat IP terdaftar yang sama. Sehingga nantinya ada beberapa komputer yang memiliki kesamaan alamat IP terdaftar. Keuntungan menggunakan NAT dinamis ini tentu lebih amannya penelusuran di internet.

Ketika ada penyusup yang ingin menembus komputer Anda yang menggunakan NAT dinamik, maka penyusup tersebut pasti mengalami kesulitan, sebab alamat IP yang diasosiasikan ke suatu komputer selalu berubah secara dinamis. Walaupun begitu, NAT dinamis juga memiliki kekurangan, yaitu jika semua alamat IP sudah terpenuhi dan terpakai semua, maka jika ada penambahan komputer lain, komputer tersebut tidak lagi dapat terhubung ke internet melalui NAT.

3. Overloading NAT

Memungkinkan lebih dari satu klien terhubung menuju satu IP publik, namun pada port yang berbeda. Sehingga saat NAT menerima permintaan dari klien untuk dihubungkan kepada server, NAT kemudian akan menentukan nomor IP dan port untuk klien tersebut. Keuntungannya adalah walaupun sebuah nomor IP telah digunakan, namun masih bisa dipakai untuk klien lain sebab berada dalam port yang berbeda.

4. Overlapping NAT

Bentuk NAT yang melakukan penerjemahan dua arah, terutama jika terdapat nomor yang sama antara alamat IP publik dan lokal. Agar tidak terjadi konflik, maka NAT mengubah nomor IP publik menjadi nomor yang tidak terdapat dalam jaringan lokal.

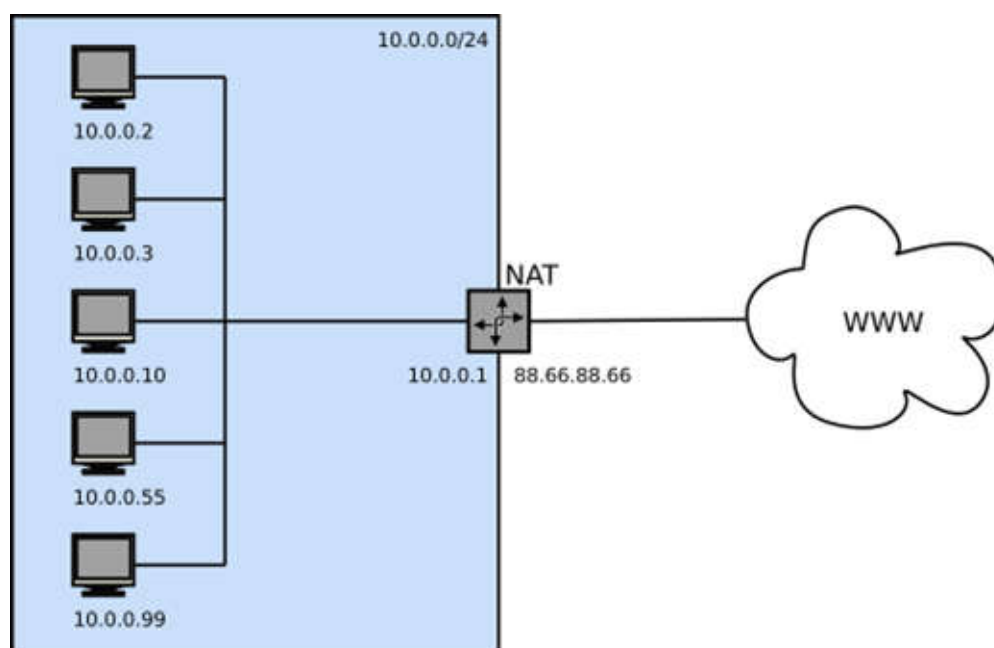
C. Fungsi NAT

Setelah mengenal pengertian dan variasi NAT yang ada, lalu sebenarnya apakah fungsi NAT ini? Paling tidak, ada beberapa fungsi NAT, yaitu :

1. Melakukan penghematan terhadap IP legal yang disediakan oleh *Internet Service Provider* (ISP).
2. Meminimalisir adanya duplikasi alamat IP dalam jaringan.
3. Ketika terjadi perubahan jaringan, menghindari proses pengalamatan kembali.
4. Menambah fleksibilitas untuk terhubung dengan jaringan internet.
5. Melakukan peningkatan terhadap keamanan sebuah jaringan.
6. Dibandingkan dengan aplikasi alternatif seperti proxy, penggunaan NAT memberikan fleksibilitas dan performa yang lebih baik.

Walaupun begitu, dibalik semua fungsi dan kelebihanannya, sebetulnya ada juga beberapa kekurangan yang mesti dirasakan pengguna NAT, seperti misalnya mengalami *delay switching* ketika proses translasi, kehilangan kemampuan melacak *IP end to end*, dan juga ada beberapa aplikasi yang menolak bekerja saat menggunakan NAT.

D. Cara Kerja NAT



Gambar 89 : Cara kerja NAT

cara kerja NAT

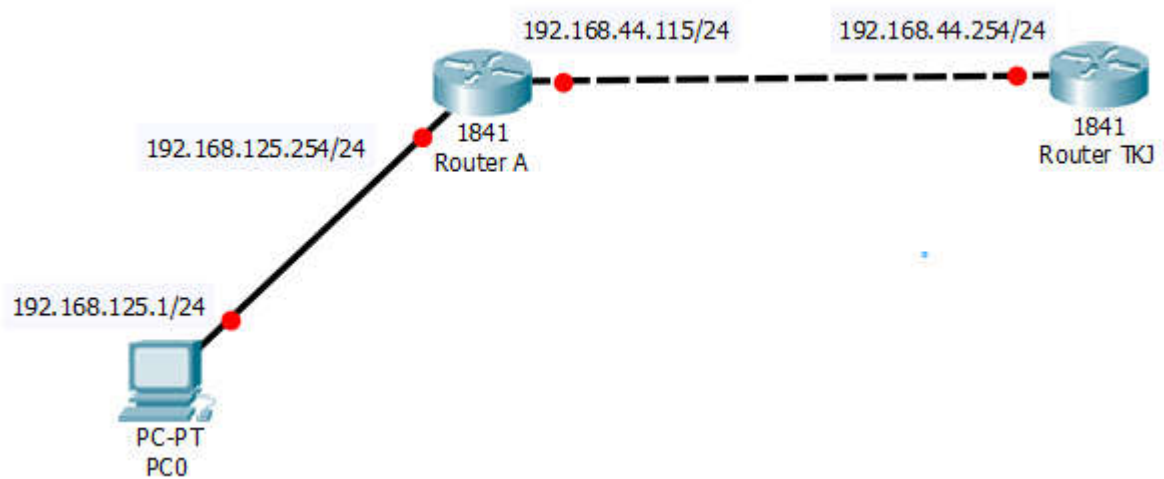
Saat menggunakan NAT, seorang klien dapat terhubung dengan internet melalui proses-proses berikut :

1. Pertama-tama, NAT menerima permintaan dari klien berupa paket data yang ditujukan untuk sebuah server remote di internet.

2. NAT kemudian mencatat alamat IP klien, lalu menyimpannya ke dalam tabel translasi alamat. Selanjutnya, alamat IP komputer klien tersebut diubah oleh NAT menjadi nomor IP NAT, lalu NAT lah yang akan melakukan permintaan kepada server.
3. Server kemudian merespon permintaan tersebut. Dari sudut pandang server, yang terlihat adalah alamat IP NAT, bukan alamat IP klien yang meminta data bersangkutan.
4. NAT menerima respon dari server, lalu melanjutkannya dengan mengirimkan ke alamat IP klien yang bersangkutan.
5. Keempat tahapan tersebut terjadi berulang-ulang, sehingga walaupun klien komputer tidak memiliki alamat IP publik, namun tetap dapat mengakses internet.

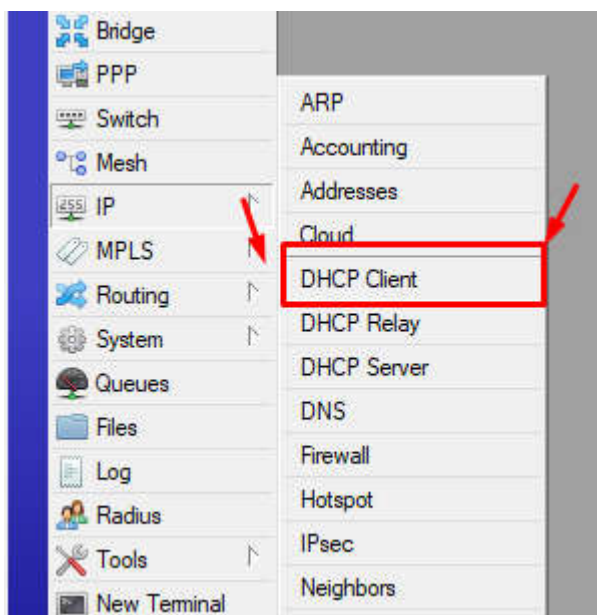
E. Konfigurasi NAT di mikrotik

Konfigurasi NAT menggunakan MikroTik



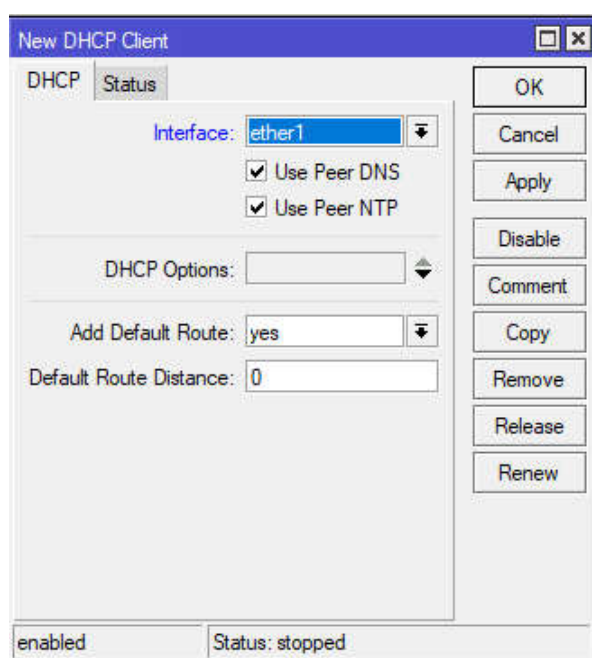
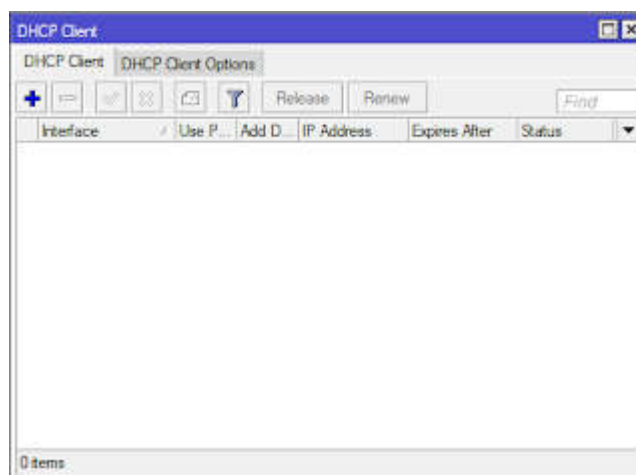
Gambar 90 : NAT

- 1) Langkah - langkah
 - a) Sambungkan Kabel LAN yang tersambung internet ke Mikrotik pada ether1 dan PC client ke ether2 atau ether lainnya yang sesuai..
 - b) Pada PC client buka Winbox lalu masuk ke setting MikroTik.
 - c) Lalu setting DHCP client pada mikrotik dengan cara IP - DHCP Client



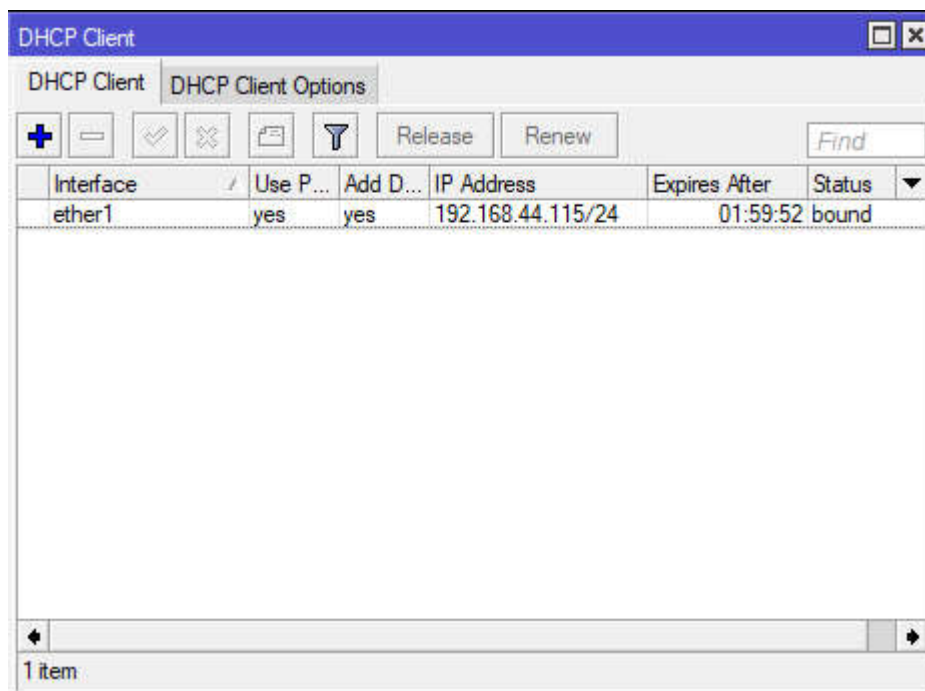
Gambar 91 : DHCP Client

1. klik tanda (+) dan pilih interface ether1 yang tersambung dengan kabel yang tersambung dengan internet, klik OK



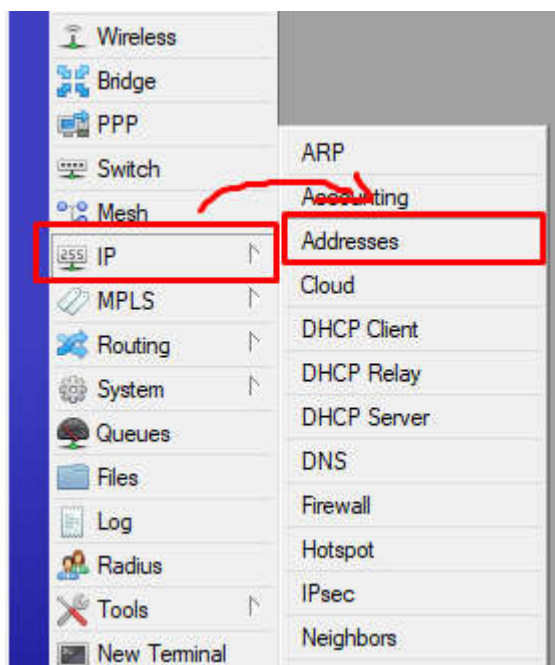
Gambar 92 : Konfigurasi DHCP Client

2. Lihat pada list DHCP client apakah sudah tertera tulisan bound di ether1, berarti ether1 sudah mendapat IP address dari sambungan LAN



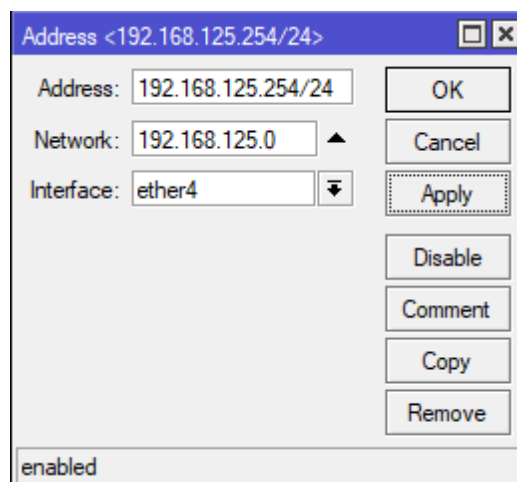
Gambar 93 : Konfigurasi DHCP Client berhasil

3. Sekarang buat IP address pada ether2 atau ether lainnya yang tersambung ke PC client.
4. Dengan cara masuk IP>addresses



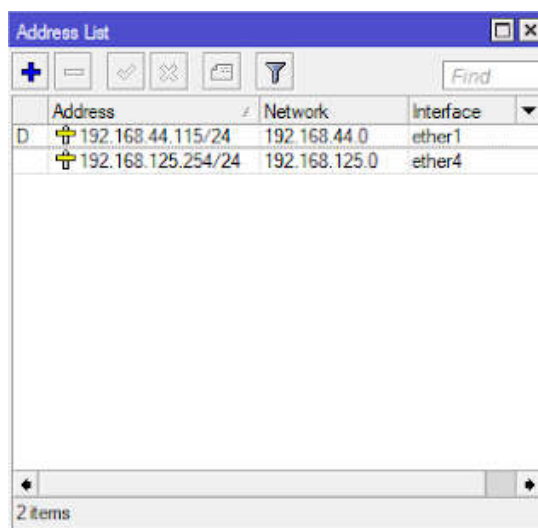
Gambar 94 : Menu IP Address

5. Lalu tekan tanda (+) masukan IP privat misal 192.168.125.254/24 dan interface ether4 atau yang bersangkutan lalu Apply dan OK



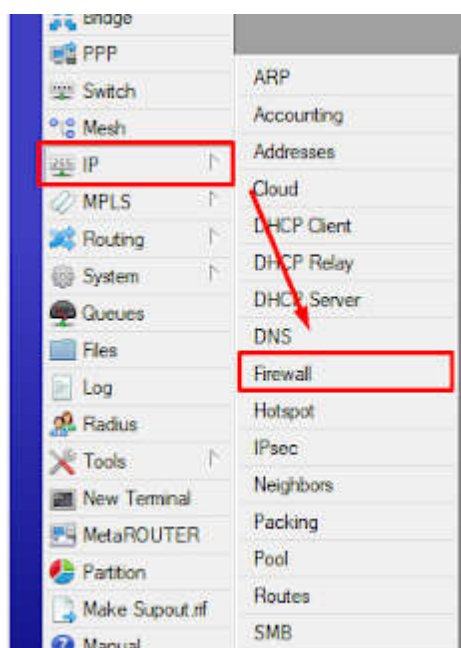
Gambar 95 : Input IP Address

6. IP sudah ditambahkan



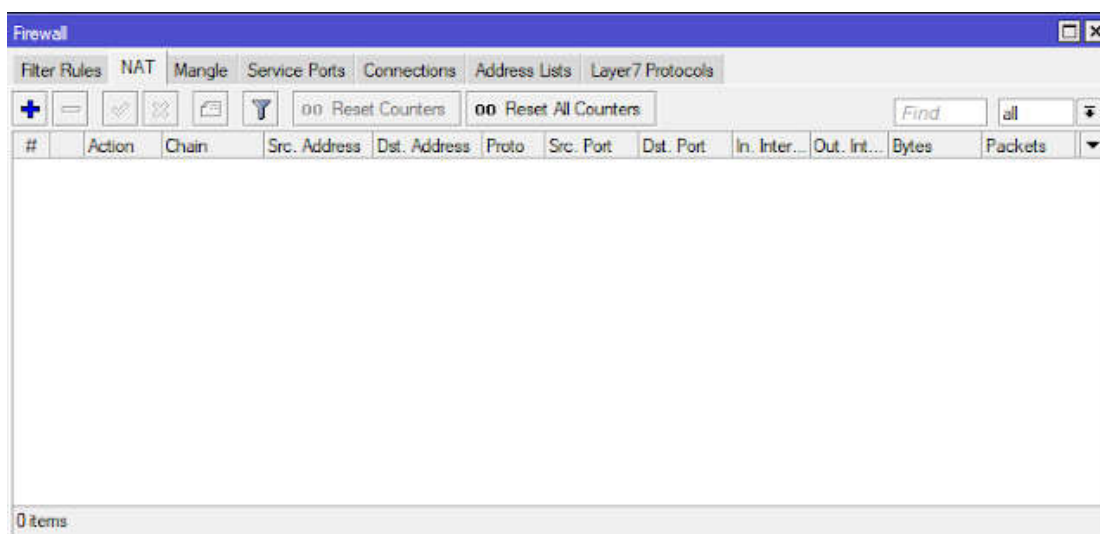
Gambar 96 : Menambahkan IP Address berhasil

7. Sekarang setting NAT, dengan cara buka IP - Firewall



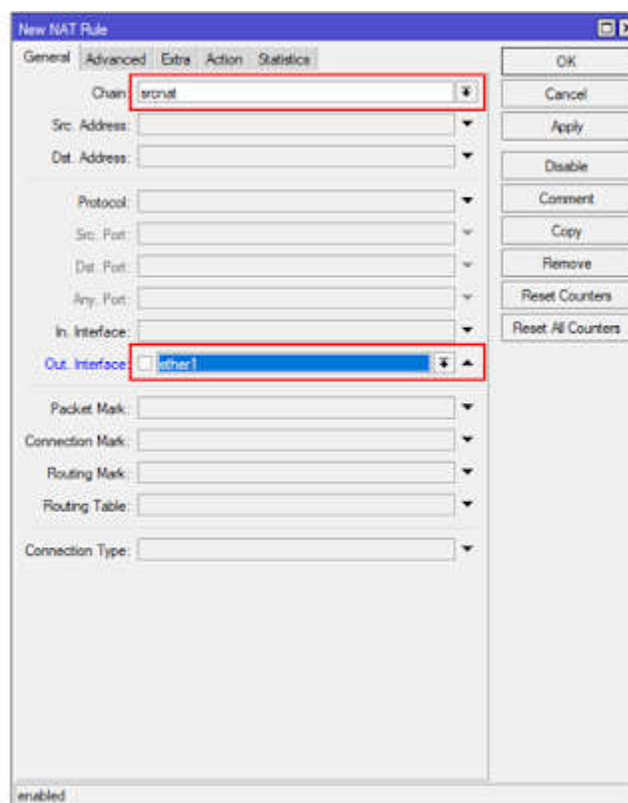
Gambar 97 : Menu firewall

8. Pada tab NAT pilih tanda (+) untuk menambah konfigurasi NAT



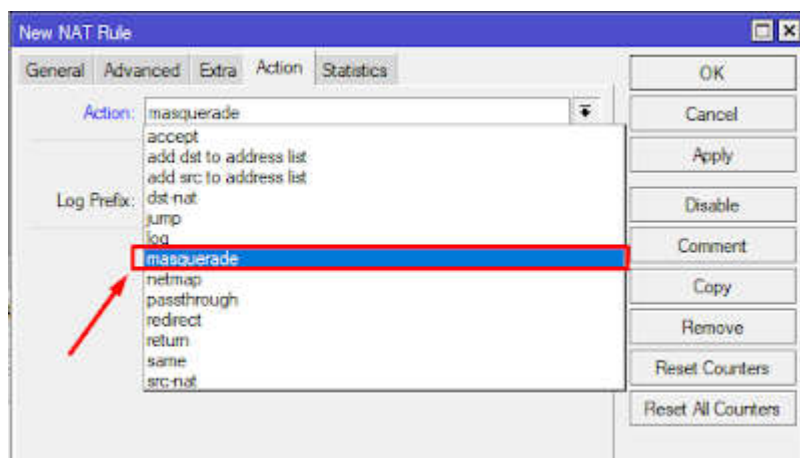
Gambar 98 : TAB NAT

9. pilih chain srcnat dan out interface pilih ether1



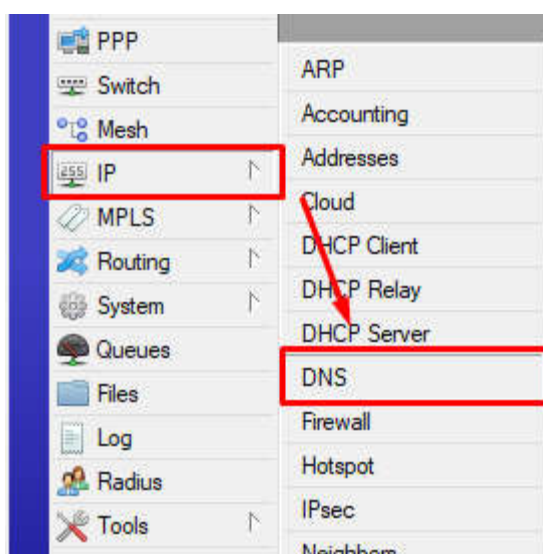
Gambar 99 : Konfigurasi srcnat

10. Pada Tab Action pilih masquerade lalu OK



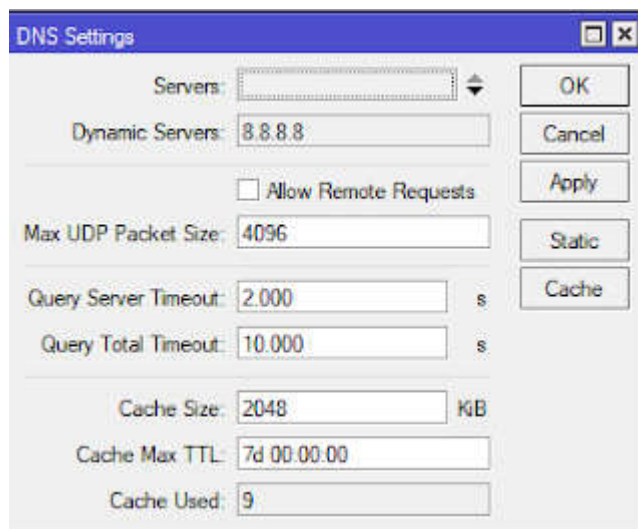
Gambar 100 : Konfigurasi masquerade

11. setting DNS dengan pilih IP-DNS



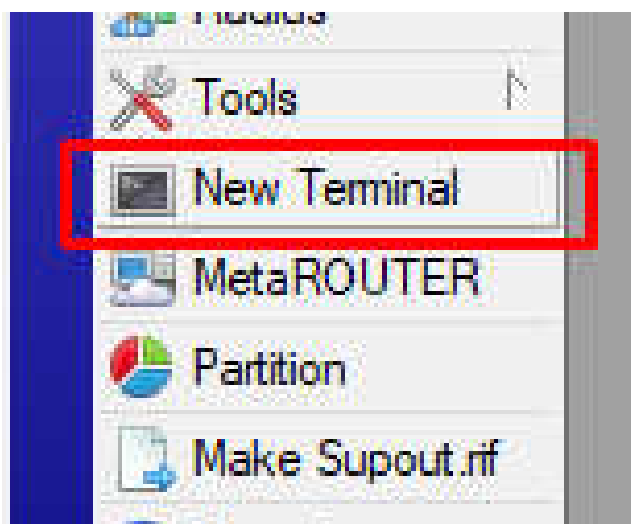
Gambar 101 : Menu DNS

12. Masukkan DNS google yaitu 8.8.8.8 lalu Apply dan OK.



Gambar 102 : Input DNS

13. Cek terlebih dahulu dengan masuk ke New Terminal



Gambar 103 : menu terminal

14. Lalu cek dengan menuliskan "ping 8.8.8.8" dan "ping google.com", jika sudah berhasil lanjut dengan cek di cmd

```
C:\Users\User>ping 192.168.125.254

Pinging 192.168.125.254 with 32 bytes of data:
Reply from 192.168.125.254: bytes=32 time<1ms TTL=64
Reply from 192.168.125.254: bytes=32 time<1ms TTL=64
Reply from 192.168.125.254: bytes=32 time<1ms TTL=64
Reply from 192.168.125.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.125.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\User>ping 192.168.44.115

Pinging 192.168.44.115 with 32 bytes of data:
Reply from 192.168.44.115: bytes=32 time<1ms TTL=64
Reply from 192.168.44.115: bytes=32 time<1ms TTL=64
Reply from 192.168.44.115: bytes=32 time<1ms TTL=64
Reply from 192.168.44.115: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.44.115:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\User>ping 192.168.44.254

Pinging 192.168.44.254 with 32 bytes of data:
Reply from 192.168.44.254: bytes=32 time<1ms TTL=63
Reply from 192.168.44.254: bytes=32 time<1ms TTL=63
Reply from 192.168.44.254: bytes=32 time<1ms TTL=63
Reply from 192.168.44.254: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.44.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```

C:\Users\User>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=33ms TTL=116
Reply from 8.8.8.8: bytes=32 time=32ms TTL=116
Reply from 8.8.8.8: bytes=32 time=33ms TTL=116
Reply from 8.8.8.8: bytes=32 time=31ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 33ms, Average = 32ms

```

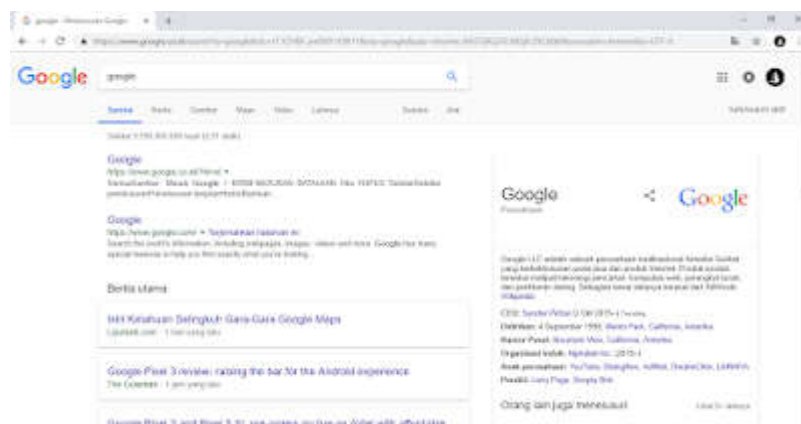
Gambar 104 : test koneksi

15. Konfigurasi NAT sudah selesai,
16. Icon sambungan internet akan berubah menjadi seperti berikut



Gambar 105 : ikon sambungan internet pada windows

17. Sekarang PC client sudah dapat menggunakan internet



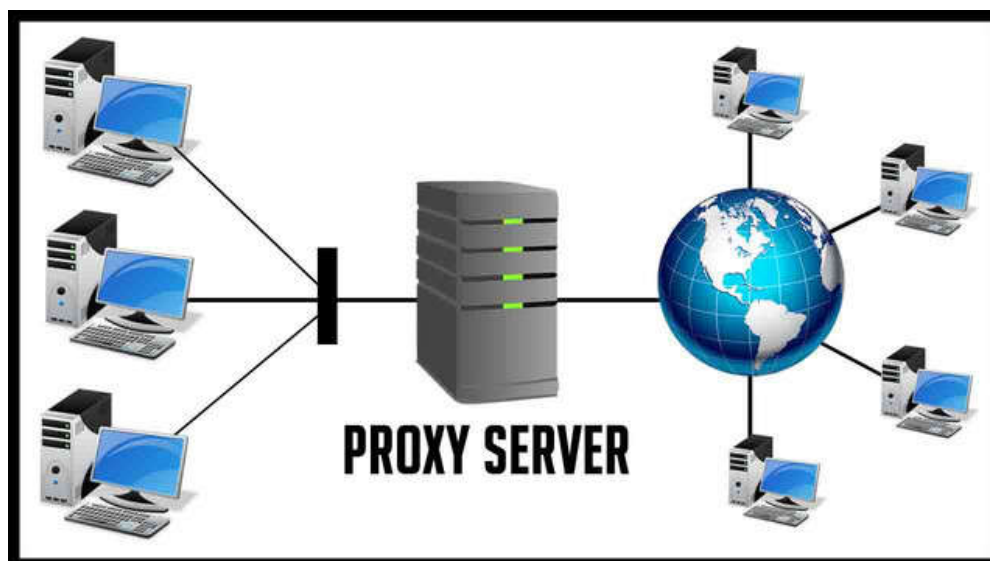
Gambar 106 : koneksi client berhasil

PROXY SERVER

A. Pengertian

Pengertian Proxy Server atau peladen pewali adalah suatu server komputer yang menyediakan layanan untuk meneruskan permintaan user ke server lainnya yang berada di internet. Dengan adanya proxy server maka sebuah komputer bisa dihubungkan dengan komputer lainnya melalui internet.

Pada umumnya proxy server digunakan untuk mengamankan jaringan komputer pribadi yang terhubung dengan jaringan publik. Jadi, dari proxy server tersebut maka biasanya server diletakkan di antara aplikasi server dengan aplikasi client, dimana aplikasi client berupa web browser, client FTP dan lainnya sedangkan aplikasi server berupa server FTP dan web server.



Gambar 107 : Proxy server

Proxy server adalah server yang diletakkan di antara sebuah aplikasi client dan aplikasi server yang dihubungi. Aplikasi client tersebut bisa berupa browser web, client FTP, dan sebagainya. Sedangkan aplikasi server dapat berupa server web, server FTP, dan sebagainya.

Proxy Server yang berada di antara aplikasi client dan aplikasi server tersebut dapat digunakan sebagai pengendali maupun monitoring lalu-lintas paket data yang melewatinya.

B. Cara Kerja Proxy Server

Setelah memahami pengertian proxy server, tentunya kita juga perlu mengetahui bagaimana prinsip cara kerja proxy server dan mengapa suatu proxy dibutuhkan.

Dari pengertian proxy server di atas kita tahu bahwa proxy server berperan sebagai penghubung komputer dengan internet, maka cara kerja program ini yakni user menggunakan layanan pada server proxy kemudian melakukan permintaan data atau file yang terdapat di internet (*public server*). Selanjutnya proxy akan meneruskan permintaan tersebut ke internet dengan seolah-olah server tersebutlah yang memintanya.

Jika pengguna sudah mendapatkan permintaannya proxy akan memberi respon kepada user dimana seolah dia yang menjadi public servernya. Pada intinya di sini server proxy dapat menyembunyikan identitas alamat IP seseorang atau perusahaan.

C. Fungsi Proxy Server

Dari penjelasan tentang pengertian proxy dan cara kerjanya tersebut, maka berikut ini 3 fungsi utama server proxy yang harus diketahui:

1. Fungsi Connection Sharing

Disini server proxy berfungsi secara teknis untuk menjadi sebuah gateway dimana berperan untuk membatasi penggunaan jaringan lokal dan jaringan luar.

Sehingga jika jaringan komputer perusahaan menanamkan program server proxy maka dapat mengakses sambungan gateway dari jaringan lokal ke jaringan internet secara bersamaan.

2. Fungsi Filtering

Dalam fungsi ini, server proxy bertindak seperti Firewall sebagai media penyaringan atau *filtering* sebuah jaringan internet dimana setiap paket-paket data yang ditransmisikan akan discan dan difilter untuk mengurangi kegagalan.

Tujuan lainnya juga untuk melindungi jaringan lokal perusahaan dari serangan luar seperti retasan. Selain itu server proxy juga dapat membantu meminimalisir serangan virus dan malware yang merugikan.

3. Fungsi Caching

Adanya server proxy dapat menyimpan objek dan data yang pernah di *search* atau diminta user saat browsing menggunakan aplikasi internet. Misalnya ketika Anda melakukan pencarian pada situs tertentu maka data-data tersebut akan disimpan dalam bentuk cache.

Semua data yang diminta dan diakses akan disimpan pada proxy server. Sehingga dari fungsi ini bisa dimanfaatkan untuk mendeteksi dokumen-dokumen apa saja yang sering diakses di komputer perusahaan.

D. Manfaat Proxy Server

Selain dari ketiga fungsi utama diatas, penggunaan server proxy juga memiliki manfaat berikut ini untuk user:

1. Menghemat Bandwidth

Proxy server bisa dimanfaatkan untuk menghemat penggunaan bandwidth dari koneksi internet user karena adanya proses caching yang menyimpan *cookies* dari situs-situs yang pernah dikunjungi.

2. Meningkatkan Kinerja Internet

Proxy server dapat membantu meningkatkan kinerja jaringan internet user karena adanya penghematan bandwidth.

3. Memblokir Situs Tertentu

Proxy server dapat secara otomatis memblokir situs-situs yang mengandung sara atau situs yang tidak diinginkan dengan adanya fitur filtering. Sehingga dengan manfaat ini bisa menghindari karyawan membuka situs-situs terlarang melalui jaringan internet lokal perusahaan.

4. Keamanan Jaringan Komputer

Seperti yang telah disebutkan di awal artikel, proxy server dapat meningkatkan keamanan komputer dari serangan virus dan gangguan malware.

Meskipun proxy bermanfaat besar bagi keamanan jaringan komputer namun masih terdapat kekurangan penggunaan proxy. Salah satunya adalah sering terjadi kesalahpahaman terhadap suatu situs yang dianggap harus diblokir oleh server sehingga perlu dilakukan pembukaan blokir secara manual.

5. Akses Internet Lebih Cepat

Masih berhubungan dengan poin #2, proxy server dapat meningkatkan kinerja internet. Dengan begitu maka akses internet akan menjadi lebih cepat.

E. Jenis Proxy Server

Ada empat jenis proxy server berdasarkan karakteristiknya, yaitu:

1. Anonymous Proxy (Proksi Anonim)

Ini adalah jenis proxy yang memberikan informasi mengenai komputer pengguna. Saat pengguna melakukan request pada sebuah website, maka website itu tidak akan mengetahui alamat IP pribadi si pengguna, hanya mengetahui IP proxy nya saja.

2. High Anonymity Proxy

Ini adalah jenis proxy yang tidak mengidentifikasi dirinya sebagai proxy server dan tidak menyediakan alamat IP original.

Proxy ini menggunakan header REMOTE_ADDR dengan sebuah alamat IP menuju proxy server, sehingga dari pengguna akan terlihat bahwa proxy server-nya berperan sebagai klien.

3. Transparent Proxy (Proksi Transparan)

Ini adalah jenis proxy yang melanjutkan permintaan pengguna ke sumber yang diinginkan tanpa mengungkap informasi komputer si pengguna. Pada umumnya proxy jenis ini banyak dipakai pada komputer di perkantoran.

4. Reverse Proxy

Ini adalah jenis proxy yang digunakan untuk mencegah klien terhubung dengan data/ informasi sensitif. Dan ketika caching pada proxy jenis ini diaktifkan maka trafik jaringan akan menurun.

F. Kegunaan Web Proxy

Web proxy merupakan komputer server yang dapat bertindak sebagai komputer lainnya. Web proxy ini berfungsi untuk melakukan permintaan terhadap konten dari jaringan internet dan intranet.

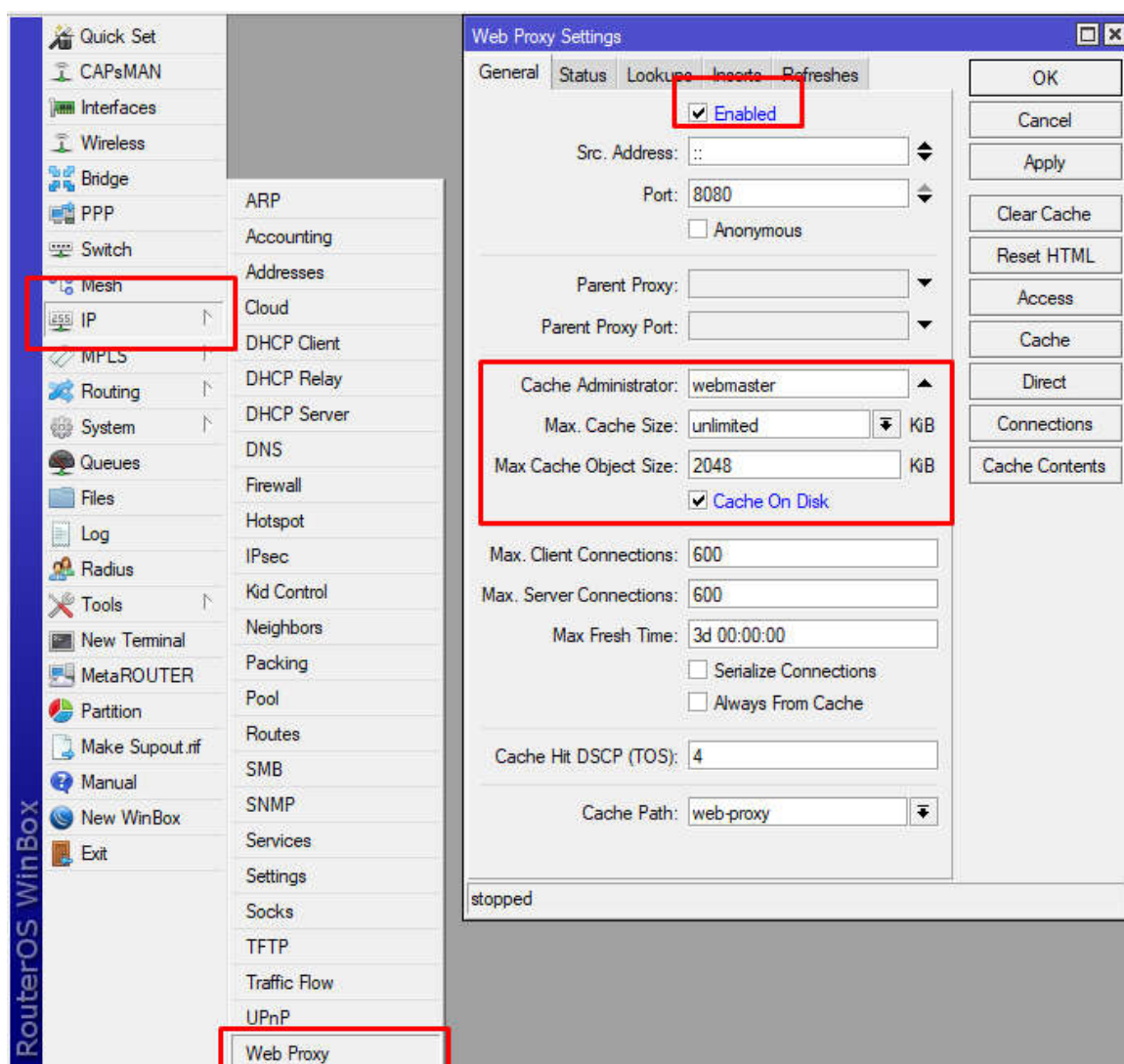
Web proxy dapat melakukan hal-hal berikut ini:

- Menyembunyikan alamat IP komputer
- Mengakses situs yang diblokir oleh ISP
- Memblokir akses ke situs sensitif atau berbahaya
- Menyaring cookies yang tidak diinginkan
- Meningkatkan keamanan dan privacy pengguna internet

G. Konfigurasi Proxy Server di Mikrotik RouterBoard

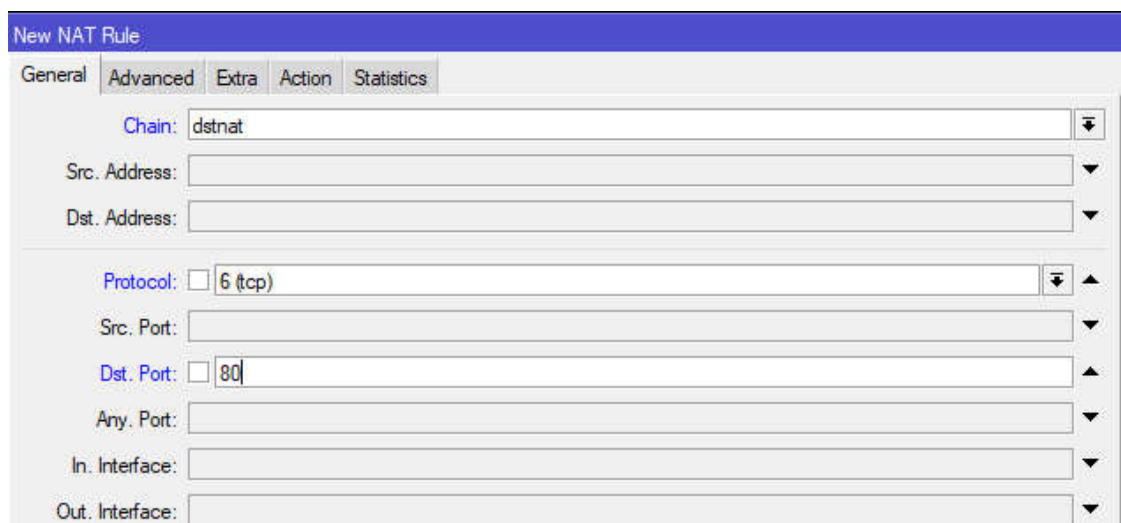
Salah satu fitur pada Mikrotik adalah Web proxy yang bisa digunakan sebagai proxy server yang nantinya akan menjadi perantara antara browser user dengan Web Server di Internet. Langkah-langkah yang perlu dilakukan adalah sebagai berikut :

- Pada Winbox masuk ke menu **IP** → **Web Proxy**
- Untuk mengaktifkan Web Proxy, pada tab **General** centang pilihan **“Enabled”**
- Isikan **Port** yang akan digunakan oleh Proxy, misal port 8080
- **Cache Administrator** bisa Anda ganti dengan email sesuai preferensi Anda selaku Admin.
- **Max. Cache Size** menentukan berapa besar alokasi memori untuk menyimpan cache proxy. Isi sesuai kebutuhan atau bisa saja pilih unlimited.
- Centang opsi **Cache On Disk** agar penyimpanan dilakukan pada hard disk MikroTik dan bukan pada RAM, karena biasanya hard disk Mikrotik memiliki kapasitas lebih besar daripada RAM.
- Klik **Apply** → **OK**



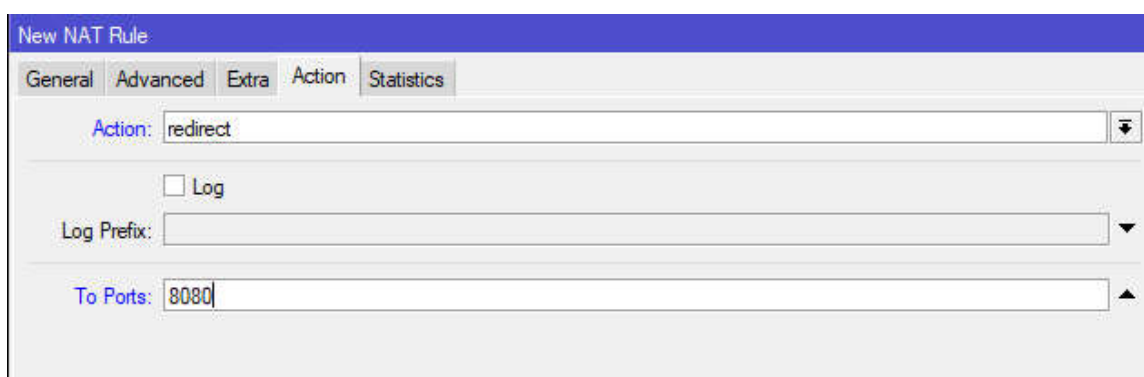
Gambar 108 : Menu web proxy

- Selanjutnya Anda harus membuat NAT untuk mengalihkan (*redirect*) Traffic data HTTP (destination port 80) ke port yang digunakan proxy yaitu 8080. Caranya adalah dengan mengkonfigurasi Firewall NAT dengan mengisi kolom **Chain=dstnat**; **Protocol** : tcp; **Dst. Port** : 80 pada tab **‘General’**



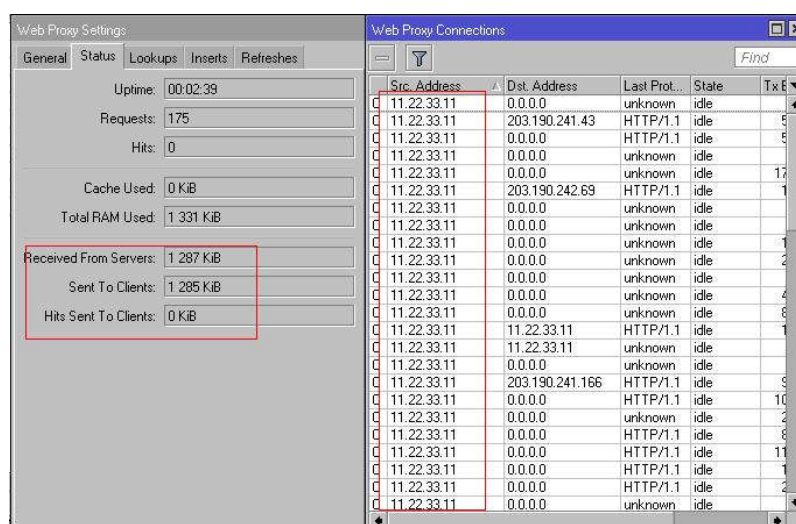
Gambar 109 : Menu NAT rule (General)

- Pada tab **Action** isi kolom **Action** : redirect dan pada kolom **To Ports** : 8080



Gambar 110 : Menu NAT rule (Action)

- Sekarang Web Proxy Mikrotik sudah Transparent, selanjutnya, buka menu **IP** → **Web Proxy** di Winbox. Masuk tab **Status** dan klik **Connections**. Kalau keduanya sudah isinya, tandanya transparent Proxy Mikrotik sudah jalan.



Gambar 111 : Status koneksi web proxy

- Selain itu pengecekan juga dapat melalui *browser*, kemudian masukkan alamat apapun (yang tidak valid) supaya terjadi pesan *error*. Jika Transparent Proxy MikroTik sudah berjalan, maka akan muncul pesan *error* dari MikroTik nya seperti gambar berikut dan pengaturan pada MikroTik sudah selesai.



Gambar 112 : Konfigurasi berhasil