Expert

SemangArt Belajar Bersama

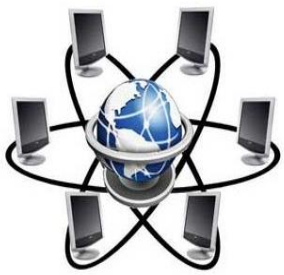
MTCNA

MikroTik Certified Network Associate

63 LAB MikroTik

Akses Mikrotik dengan Telnet, SSH, Webfig, Winbox, Backup, Restore, Export, Import, Reset, Install Ulang Mikrotik, DHCP Server, DHCP MAC Static, DHCP Server Security, DHCP Client, Router Gateway, Static Routing, Wireless AP Bridge, Bridge, Station, Station Bridge, Nstreme, Static Routing Wireless, Router Gateway Wireless, Security Profile, Virtual AP, Filtering dengan Wireless Access List, dll.

Devitriana Elizami



KATA PENGANTAR

Assalamu'alaikum warrohmatullahi wabarokatu

Dengan menyebut nama Allah Subhanawata'ala yang Maha Pengasih lagi Maha penyayang. Puji syukur saya panjatkan kehadirat-Nya yang telah memberikan kesehatan jasmani dan rohani, sehingga saya dapat menyelesaikan buku ini. Sholawat serta salam saya haturkan kepada Nabi Besar Muhammad Shallallahu 'alaihiwasallam, beserta keluarganya, sahabatnya dan para pengikutnya. Saya mengucapkan terimakasih kepada semua pihak yang telah membantu terselesaikannya buku "SemangArt Belajar Otodidak MTNA", terutama untuk Orang Tua, Guru Pembimbing Kejuruan Teknik Komputer dan Jaringan serta teman-teman seperjuangan.

Saya berharap buku ini dapat bermanfaat untuk semua orang terutama adik kelas yang akan mempelajarinya. Saya sadar bahwa dalam menyusun buku ini masih banyak yang harus diperbaiki, maka dari itu saran dan kritik yang sifatnya membangun sangat saya harapkan agar dapat lebih baik lagi kedepannya.

Bekasi, Februari 2017

Devitriana Elizami

DAFTAR ISI

BAB I

Basic Mikrotik

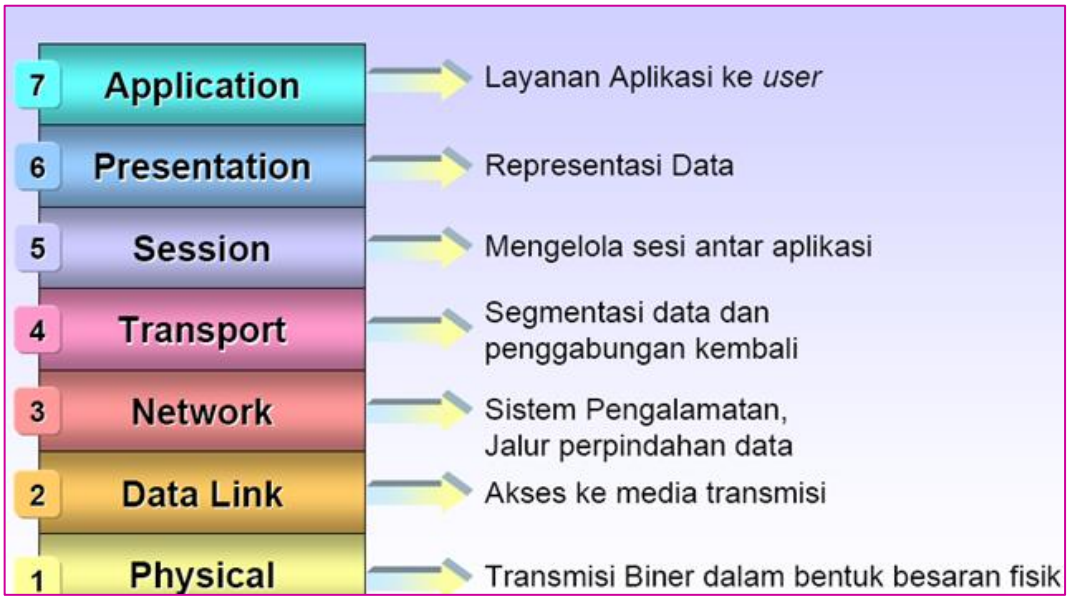
LAB 1 – 7 Layer OSI

Kenapa 7 layer OSI diciptakan?

Karena alat komunikasi yang diciptakan oleh IBM tidak dapat saling berkomunikasi dengan vendor lain atau jaringan yang berbeda. Sehingga oleh International Organization for Standardization (ISO) di Eropa pada tahun 1977 diciptakanlah standard OSI yang dapat saling berkomunikasi dengan vendor yang berbeda.

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protokol jaringan dan metode transmisi.

Ke 7 model layer OSI itu adalah :



Gambar 1.1 7 Layer OSI

7. Application Layer

Application Layer adalah lapisan yang menyediakan interface antara aplikasi yang digunakan untuk berkomunikasi dan jaringan yang mendasarinya, dimana pesan-pesan kesalahan akan dikirim. Protokol Application Layer digunakan untuk pertukaran data antara program yanng berjalan pada source dan host tujuan. Lapisan ke-7 ini menjelaskan spesifikasi untuk lingkup dimana aplikasi jaringan berkomunikasi dengan layanan jaringan.

Beberapa fungsi dari Application Layer adalah :

1. Sebagai alat pengumpul informasi dan data yang dikirimkan melalui jaringan
2. Sebagai user interface dalam menampilkan data dan informasi

Berikut adalah protokol yang berada dalam lapisan ini :

1. Web Server : HTTP (Hyper Text Transfer Protocol) dan HTTPS
2. Mail : SMTP (Simple Mail Transfer Protocol),
   POP3 (Post Office Protocol Version 3), dan
   IMAP (Internet Message Access Protocol)
3. FTP (File Transfer Protocol)
4. DHCP (Dynamic Host Configuration Protocol)
5. Telnet (Telecommunication Network)
6. DNS (Domain Name System)
7. SNMP (Simple Network Management Protocol)

6. Presentation

Berada pada layer ke 6 pada saat sebuah data akan diterima oleh user. Layer Presentation ini memiliki fungsi utama sebagai penerjemah. Yaitu menterjemahkan aplikasi menjadi bentuk data yang akan ditransmisikan ke layer-layer berikutnya atau sebaliknya (mentransmisikan/menterjemahkan data-data kedalam bentuk aplikasi).

Presentation Layer juga merupakan lapisan dimana data mulai disajikan dalam bentuk-bentuk tertentu (format), seperti .JPEG, .JPG, .DOC, dll.

Berikut adalah beberapa fungsi Presentation Layer :

1. Melakukan encrypsi (pengamanan) data atau pesan
2. Melakukan proses Kompresi dan Dekompresi
   - **Kompresi** adalah pemadatan atau pengecilan kapasitas data
   - **Dekompresi** adalah membuka dan memperjelas data yang akan diterima dan diteruskan ke Application Layer

5. Session

Adalah sebuah layer yang bertugas untuk mengendalikan dialog-dialog yang terjadi antar node dan untuk melakukan menagement dari sebuah koneksi serta mendefinisikan bagaimana sebuah koneksi dapat dibangun.

Session Layer mempunyai beberapa fungsi yaitu :

1. Melakukan komunikasi pada sebuah jaringan
2. Pembentukan hubungan
3. Pemindahan dan pertukaran data

Protokol pada Session Layer adalah :

1. NetBIOS (NetBIOS Extended User Interface)
2. PAP (Printer Access Protocol)\
3. NETBEUI
4. NFS (Network File System)
5. SQL (Structured Query Language)
6. RPC (Remote Procedure Call)
7. ASP (Apple Talk Session Protocol)

Contoh dari Session Layer adalah Gateway.

Network Component adalah Gateway.

3. Transport

Lapisan ini bertanggung jawab untuk menyediakan layanan yang dapat diandalkan kepada protocol yang terletak diatasnya.

Beberapa layanannya adalah :

1. Flow Control (Mengatur Alur), yaitu untuk menjamin bahwa perangkat yang mentransmisi data tidak mengirimkan lebih banyak data daripada yang dapat ditangani oleh perangkat yang menerimanya.
2. Packet Sequencing (Megurutkan Paket) untuk mengubah data yang hendak dikirimkan menjadi segmen-segmen data (proses segmentasi) dan tentunya memiliki fitur untuk menyusunnya kembali.
3. Fitur Acnowledgment untuk menjamin bahwa data dikirimkan dengan benar dan akan dikirimkan lagi jika data tidak sampai ke tujuan.

Fungsi dari Transport Layer adalah :

1. Menerima data dari Session Layer untujk diproses
2. Memecah data menjadi bagian-bagian yang lebih kecil untuk memudahkan proses transmisi data dan mempermudah data agar bisa melewati layer/lapisan selanjutnya dengan lebih baik, optimal dan efisien.
3. Meneruskan data ke Network Layer

4. Network

Layer ini digunakan untuk menghubungkan jaringan-jaringan yang berbeda agar dapat saling berinteraksi. Misalnya dalam perpindahan paket dari satu jaringan ke jaringan lain dapat menimbulkan masalah yang banyak. Cara pengalamatan yang digunakan oleh sebuah jaringan dapat berbeda dengan cara yang dipakai oleh jaringan lainnya. Suatu jarigan mungkin tidak adapat menerima paket sama sekali karena ukuran kapasitas paket data yang terlalu besar, protokolnya pun bisa berbeda pula. Oleh karena itu network ditugaskan untuk menyelesaikan persoalan tersebut.

Berikut adalah beberapa fungsi dari Network Layer :

1. Menentukan tujuan data pada sebuah jaringan
2. Mendefinisikan alamat IP
3. Membuat paket data terurut (header)
4. Melakukan prosess routing

Protokol pada Network Layer adalah IP, ARP, RARP, ICMP, RIP, OSPF, IGMP, IPX, NWLink, NetBEUI, OSI, DDP, DECnet, dll.

Network Component : Router, Brouter, Frame Relay Device, ATM Switch, advanced Cable Tester, dll.

5. Data Link

Dalam proses transmisi data yang terjadi, Data Lnk Layer merupakan layer ke 6 bagi transmitter (pengirim data) dan merupakan layer ke 2 bagi receiver (menerima data).

Data Link Layer memiliki tugas utama yaitu untuk menyediakan sebuah prosedur pengiriman data antar jaringan. Jadi, dengan adanya data link layer ini, setiap paket data akan ditransmisikan ataupun akan diterima oleh user, akan diproses, sehingga memungkinkan untuk dilanjutkan ke layer berikutnya, yaitu Network Layer ataupun Physical Layer.

Salah satu ciri yang terpenting pada Data Link Layer adalah bahwa lapisan ini secara fisik memiliki alamat tersendiri atau address yang sudah dikodekan secara langsung ke dalam sebuah network card atau kartu jaringan tersebut ketika pertama kali dibuat. Inilah yang dikenal dengan istilah **MAC Address**. Jadi, apabila kita mendengar nama MAC Address didalam jaringan komputer, maka hal ini sudah pasti mengacu pada lapisan atau Data Link layer.

Data Link Layer memiliki beberapa fungsi yaitu :

1. Melakukan proses Grouping secara logic (tidak terlihat)
   Grouping adalah proses penyusutan beberapa paket data menjadi satu kesatuan yang utuh. Perlu kita ketahui, ketika paket data mulai berjalan melewati lapisan OSI, maka paket data tersebut akan terpecah-pecah menjadi beberapa bagian kecil. Tugas dari data link layer inilah yang dapat melakukan proses grouping.
2. Menyediakan akses ke dalam media menggunakan MAC Address
3. Mendeteksi kesalahan pengiriman dan penerimaan paket data dan melakukan proses pengkoreksian
4. Menggabungkan paket data ke dalam byte dan menggabungkan byte ke dalam frame

1. Physical Layer

Merupakan lapisan ke 7 pada layer OSI ketika sebuah paket data mulai ditransmisikan oleh transmitter. Dimana dalam hal ini adalah sebuah server komputer dan merupkan lapisan yang pertama kali harus dilewati oleh paket data atau informasi ketika akan melakukan proses penerimaan oleh receiver.

Physical Layer merupakan layer yang memiliki koneksi dan juga definisi terdekat dengan perangkat keras jaringan, yang kemudian membantu sebuah transmisi jaringan dapat berjalan dengan lancar sesuai dengan apa yang diinginkan.

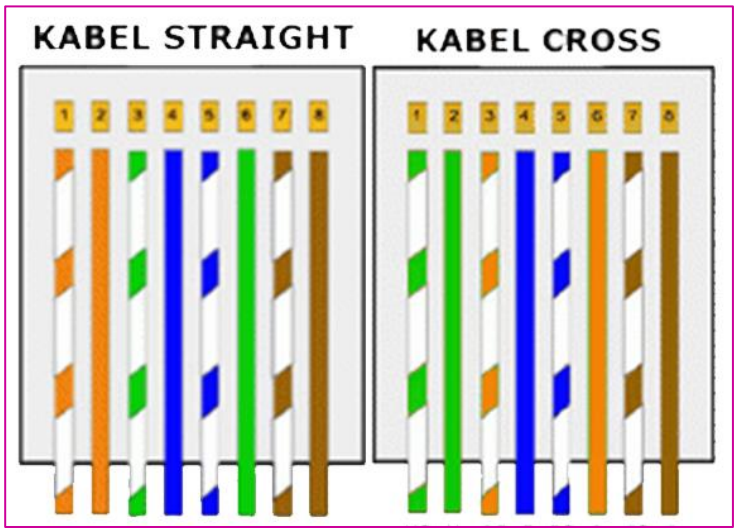
Berikut adalah proses penting yang dilakukan oleh Physical Layer adalah :

1. Physical Layer akan terhubung langsung dengan perangkat keras jaringan, seperti kabel, hub, switch, LAN Card, dll.
2. Melakukan proses sinkronisasi etrhadap bit data.
3. Physical Layer mampu berkomuniaksi secara langsung dengan berbagai jenis media transmisi
4. Physical Layer dapat menentukan kebutuhan listrik, prosedur dan juga fungsional dari sebuah jaringan komputer.
5. Dapat melakukan proses penonaktifan hubungan fisik antar sistem
6. Dapat melakukan proses pemindahan bit antar device atau alat

Karena merupakan layer yang berhubungan dengan bentuk fisik dari beberapa perangkat keras jaringan komputer, maka berikut adalah media fisik yang memanfaatkan lapisan Physical Layer :

1. Kabel : UTP, Coaxial, Fiber Optik, dll
2. NIC (Network Interface Card)
3. Hub
4. Switch

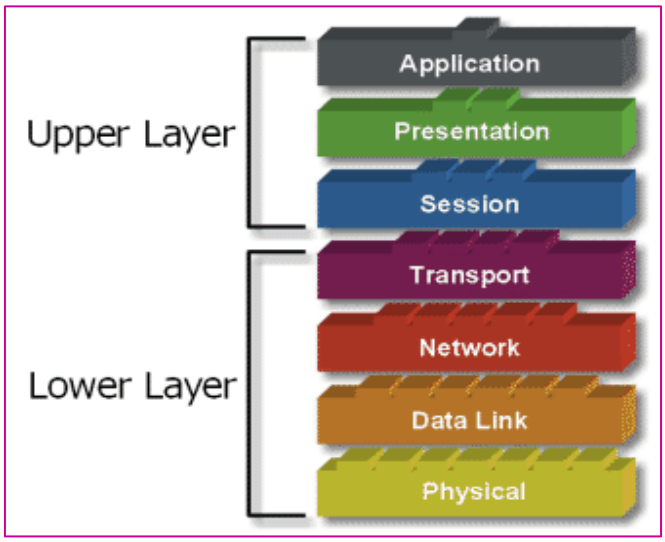
a. Berikut adalah urutan straight dan cross pada kabel UTP (Unshielded Twisted Pair) :



Gambar 1.2 Urutan Kabel Straight dan Cross

	1	2	3	4	5	6	7	8
Straight	Putih Orange	Orange	Putih Hijau	Biru	Putih Biru	Hijau	Putih Coklat	Coklat
Cross	Putih Hijau	Hijau	Putih Orange	Biru	Putih Biru	Orange	Putih Coklat	Coklat

b. Upper dan Lower Layer



Gambar 1.3 Upper dan Lower Layer pada model OSI

- **Upper Layer (Lapisan Atas)**

Layer ini fokus pada penanganan tampilan akhir kepada pengguna dan bagaimana file direpresentasikan pada komputer. Upper layer juga berhubungan dengan persoalan aplikasi dan pada umumnya diimplementasikan pada software aplikasi yang berisi sebuah komponen komunikasi.

- **Lower Layer (Lapisan Bawah)**

Adalah inti dari proses komunikasi didalam jaringan. Lower layer juga mengendalikan persoalan transportasi data yang diimplementasikan ke dalam hardware dan software pada media jaringan.

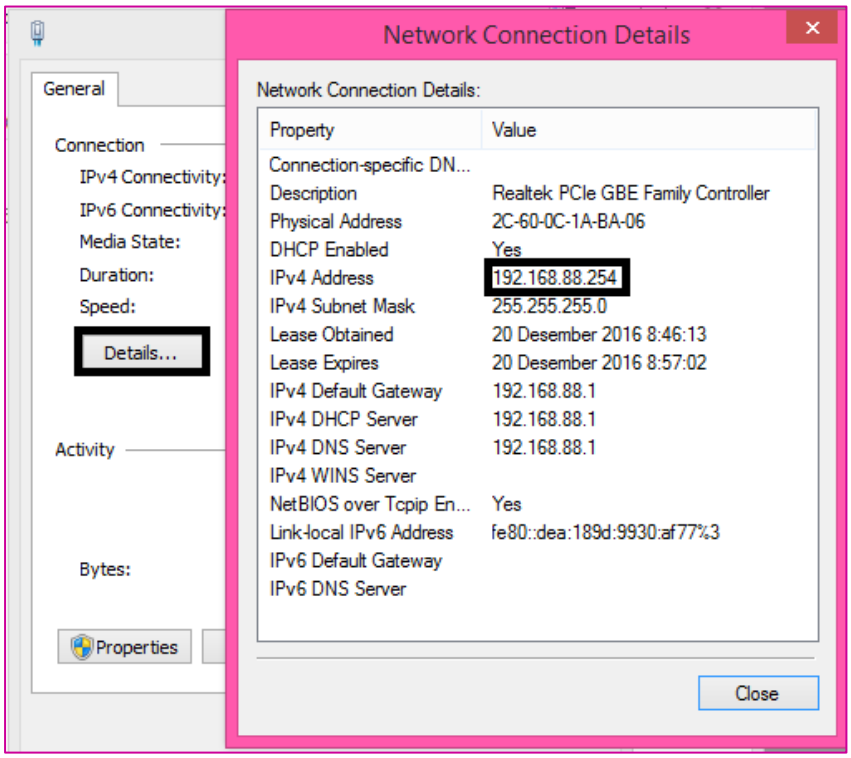
Kedua layer tersebut tidak dapat dipisahkan. Maka setiap layer harus bisa berkomunikasi dengan layer diatasnya maupun dibawahnya melalui serangkaian protokol dan standar.

LAB 2 – Default Configuration Mikrotik

Saat kita membeli sebuah **"Router Board"** yang baru, maka kita akan mendapat default configuration. Adapun default configuration tersebut diantaranya adalah :

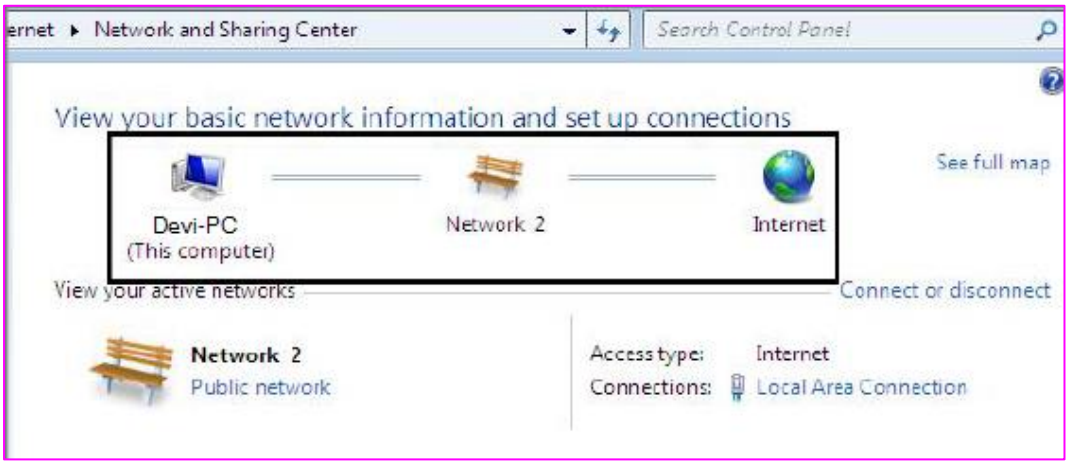
Default Configuration	Keterangan
IP : 192.168.88.1/24	Interface *ether2* memiliki ip address tersebut, kemudian interface *ether3* dan seterusnya di *slave* ke *ether2*
DHCP Server	DHCP Server aktif Pada interface *ether2* dan seluruh interface yang di *slave* ke *ether2*
DHCP Client	Setiap router yang baru, akan mengaktifkan fungsi dhcp client pada interface *ether1*
Router Gateway	Saat kita menghubungkan *ether1* ke internet dan *ether2* ke client, maka client otomatis akan dapat mengakses internet

Kita juga akan mendapatkan default configuration (konfigurasi yang sudah otomatis ada) seperti diatas saat kita baru saja *mereset* routerboard. Pada lab ini, coba tancapkan kabel UTP yang terhubung dari komputer ke *ether2* yang ada pada routerboard (Mikrotik). Selanjutnya lakukan analisa terhadap IP Address komputer client.



Gambar 2.1 IP Address Client

Perhatikan bahwa komputer client akan mendapatkan IP Address dari mikrotik secama dynamic (otomatis) dengan rentang IP 192.168.88.xx/24. Perhatikan parameter Ipv4 DHCP Server yang menunjukkan IP Address mikrotik, yaitu 192.168.88.1/24.



Gambar 2.2 Internet Access Di Client

Secara default, router mikrotik juga sudah berfungsi sebagai router gateway. Perhatikan gambar diatas yang menunjukkan bahwa client mendapat internet access dari router mikrotik yang baru.

LAB 3 – Mengakses Mikrotik dengan Telnet

Ada beberapa cara yang dapat kita gunakan untuk mengakses mikrotik. Perhatikan tabel berikut. Tabel ini menunjukkan beberapa cara yang dapat kita gunakan untuk mengakses mikrotik.

Akses Via	CLI	GUI	Need IP Address
Serial Console	Yes	-	-
Telnet	Yes	-	Yes
SSH	Yes	-	Yes
Winbox	Yes	Yes	-
FTP	Yes	-	Yes
Webfig	-	Yes	Yes
MAC Telnet	Yes	-	-

Dari beberapa cara diatas, yang paling sering digunakan untuk mengakses mikrotik adalah menggunakan Telnet, SSH, dan Winbox. Jika memperhatikan tabel diatas kita bisa mengetahui bahwa sebelum mengakses mikrotik menggunakan telnet, mikrotik harus mempunyai IP Address terlebih dahulu.

Telnet (Telecommunications Network Protocol) merupakan remote login yang terjadi pada sebuah jaringan internet disebabkan karena adanya service dari protocol telnet yang memungkinkan penggunanya dapat login dan bekerja pada sistem jarak jauh. Dengan adanya telnet, pengguna dapat mengakses komputer lain secara remote melalui jaringan internet.

Berdasarkan penggunaannya, telnet memakai 2 program yaitu :

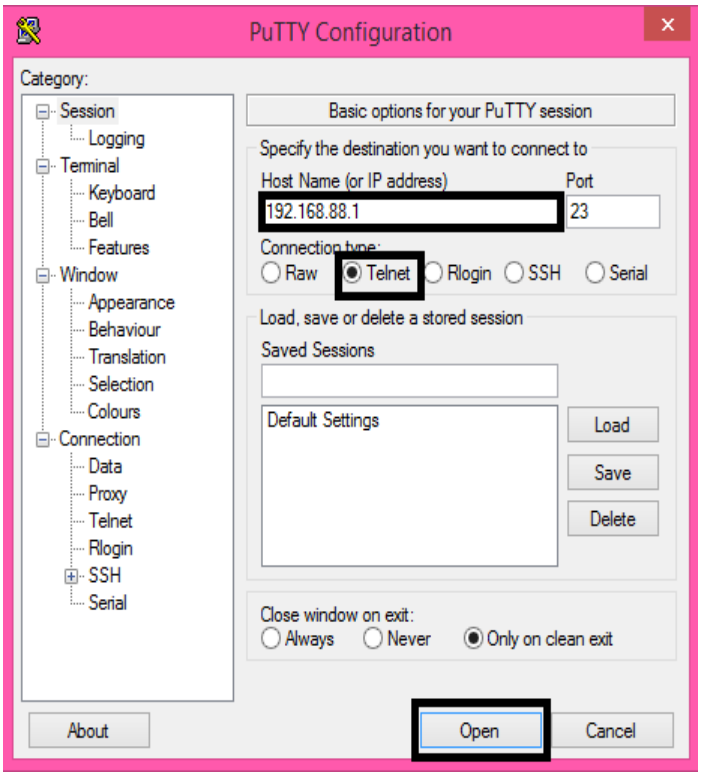
1. Client : Program pada client digunakan untuk meminta layanan pada server.
2. Server : Program yang terdapat pada server akan memberikan layanan yang diminta oleh client.

Telnet mempunyai beberapa kelebihan dan kekurangan diantaranya :

1. **Kelebihan** : User interface yang cukup ramah. Maksudnya pengguna dapat memberikan perintah dari jarak jauh (remote) jadi seolah-olah penggunanya mengeksekusi perintah pada command line komputer.
2. **Kekurangan** : Dimana ada kelebihan selalu ada kekurangan. Adapun kekurangan dari telnet yaitu pengguna NTLM authentication tanpa adanya encrypsi, sehingga dapat memudahkan pencurian password yang dilakukan oleh sniffers.

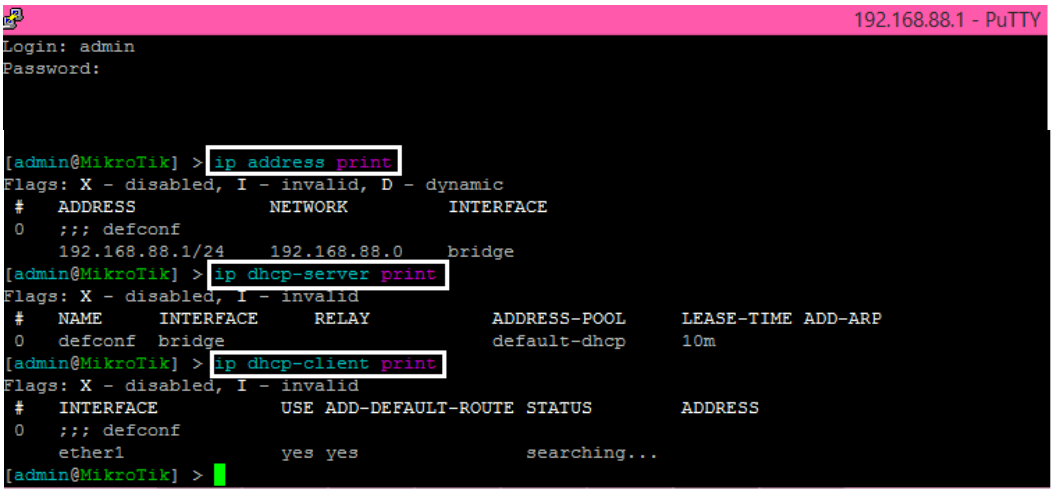
Secara default mikrotik memiliki IP 192.168.88.1 sehingga kita bisa manfaatkan IP ini. Untuk melakukan telnet ke mikrotik, kita membutuhkan sebuah software

telnet client. Salah satu software yang paling banyak digunakan adalah "**Putty**". Silahkan download di http://www.putty.org/



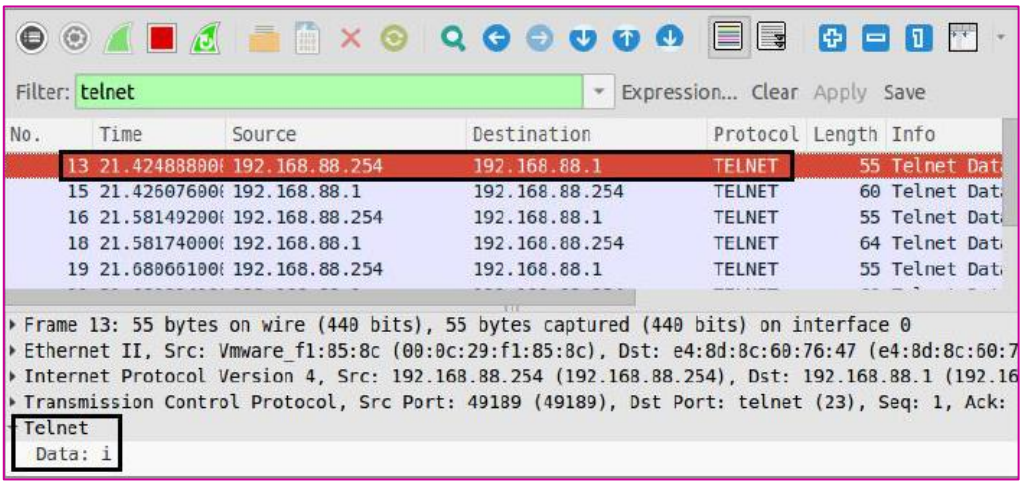
Gambar 3.1 Mengakses Mikrotik Dengan Telnet

Secara default pula, user yang digunakan untuk login adalah *admin* dengan password (kosong). Perhatikan gambar berikut yang menunjukkan hasil setelah kita mengakses mikrotik menggunakan telnet.



Gambar 3.2 Akses Mikrotik Dengan Telnet

Saat ini penggunaan telnet sudah sangat jarang, atau bahkan sudah tidak pernah digunakan. Hal ini dikarenakan penggunaan telnet sangatlah tidak aman. Jika kita meremote mikrotik menggunakan telnet, maka setiap perintah yang kita ketik di terminal, dapat dilihat oleh orang yang tidak bertanggung jawab dengan sangat mudah. Perhatikan gambar berikut yang menunjukkan hasil tangkapan paket telnet.

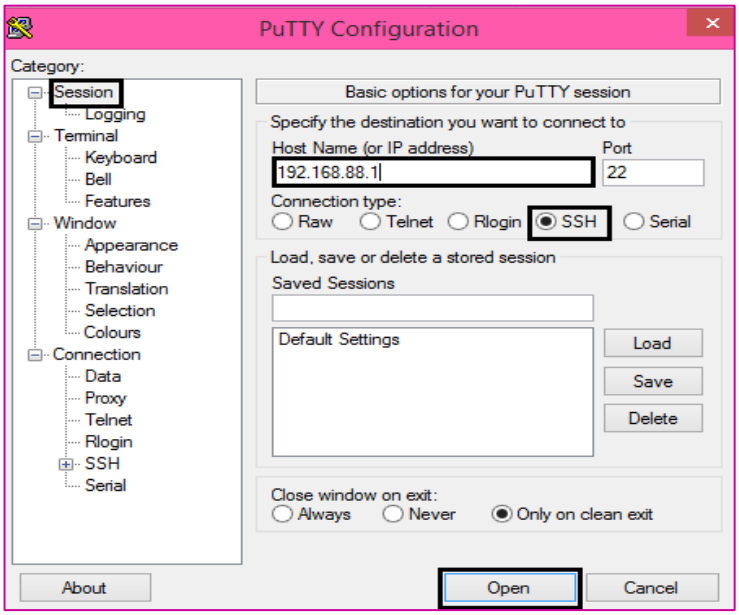


Gambar 3.3 Penggunaan Telnet Tidak Aman

Pada gambar diatas terlihat bahwa ada parameter *Data*. Parameter ini menunjukkan perintah yang kita ketikkan diterminal mikrotik. Tentunya jika terjadi hal seperti ini akan sangat membahayakan.

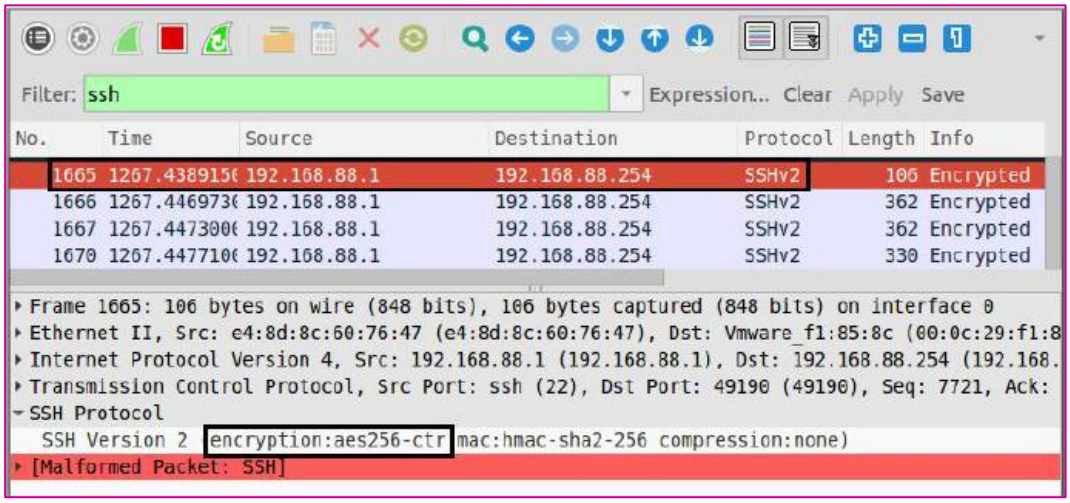
LAB 4 – Mengakses Mikrotik dengan SSH

SSH (Secure Shell) adalah sebuah protocol jaringan yang terencrypsi untuk menjalankan Shell Session (terminal) dengan aman dan tidak bisa terbaca oleh orang lain karena terkoneksi melalui SSH Tunneling. Jadi website, account, dll yang kita input tidak akan tercatat pada log dirouter ataupun server. Jika kita ingin mengakses mikrotik dengan metode teks dengan cara yang "**AMAN**", maka solusinya adalah SSH. Kita ketikkan IP default mikrotik dan pilih SSH :



Gambar 4.1 Akses Mikrotik Dengan SSH

Jika kita menggunakan SSH, maka orang yng tidak bertanggung jawab akan sulit untuk melihat apa saja yang kita lakukan terhadap mikrotik. Hal ini dikarenakan perintah-perintah yang kita ketikkan dimikrotik akan dienkripsi oleh SSH.



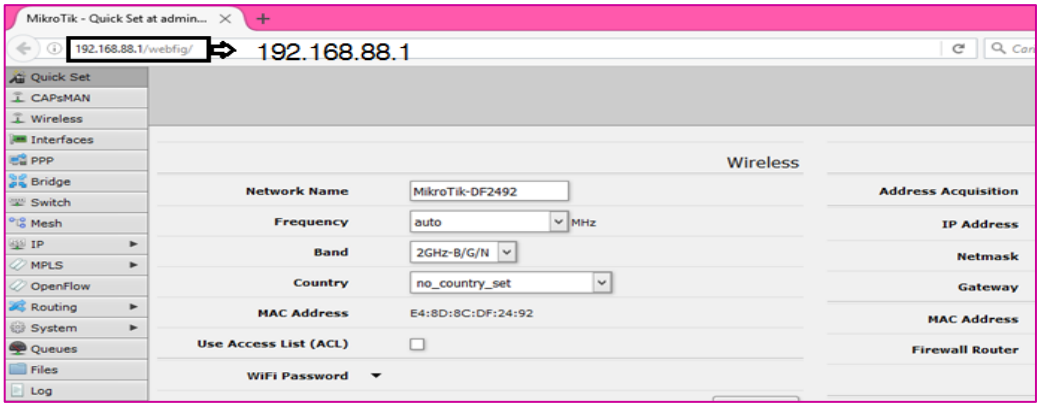
Gambar 4.2 Paket SSH Akan Di Enkripsi

LAB 5 – Mengakses Mikrotik dengan Webfig

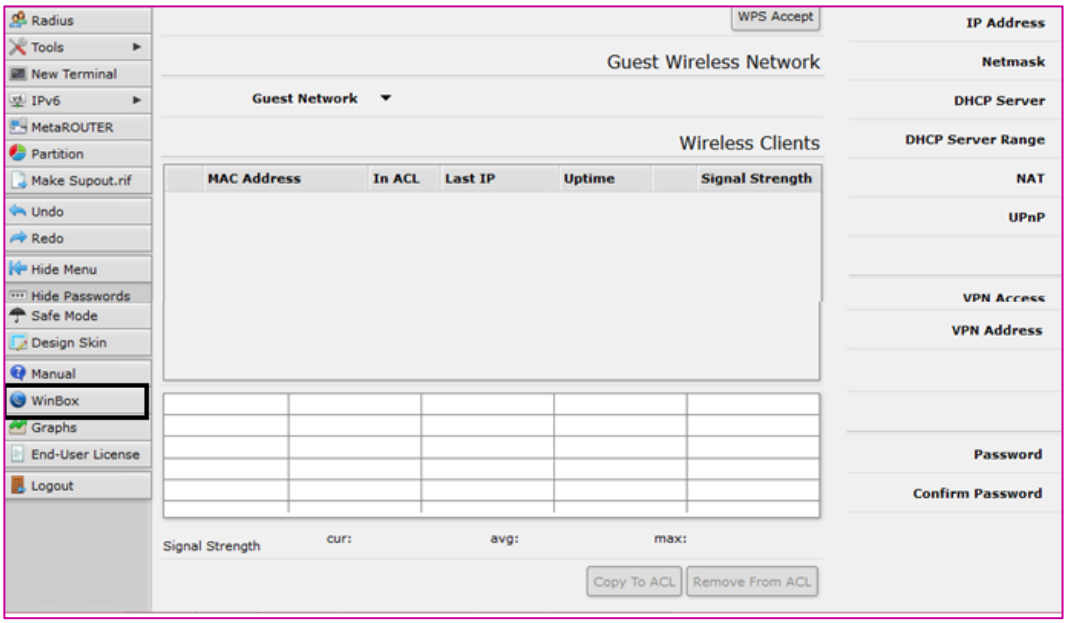
Telnet dan SSH **hanya** mengizinkan kita untuk mengkonfigurasi mikrotik dengan CLI. Tentu hal ini akan menyulitkan bagi orang-orang yang baru belajar mikrotik. Maka dari itu kita bisa menggunakan webfig untuk mengkonfigurasi mikrotik. **Webfig ini sudah mendukung fitur GUI.**

Namun, jika kita menggunakan webfig, ada beberapa hal yang tidak bisa kita lakukan. Sehingga biasanya orang mengakses mikrotik via webfig untuk mendownload winbox. Selanjutnya untuk konfigurasi mikrotik, kebanyakan orang akan menggunakan winbox.

Untuk masuk ke webfig, buka browser lalu ketik **192.168.88.1/webfig/**



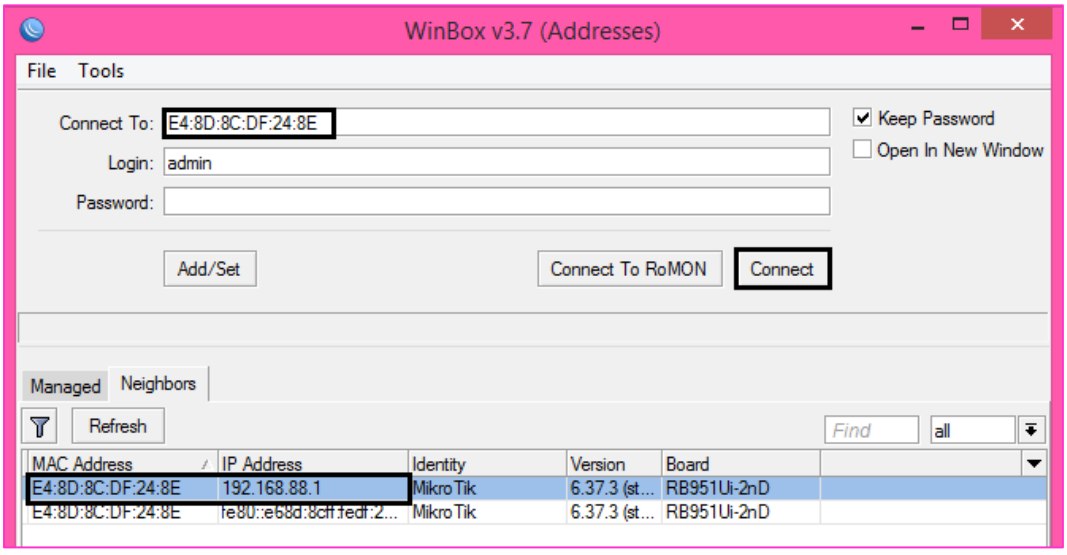
Gambar 5.1 Mengakses Winbox Dan Webfig



Gambar 5.1 Mengakses Winbox Dan Webfig

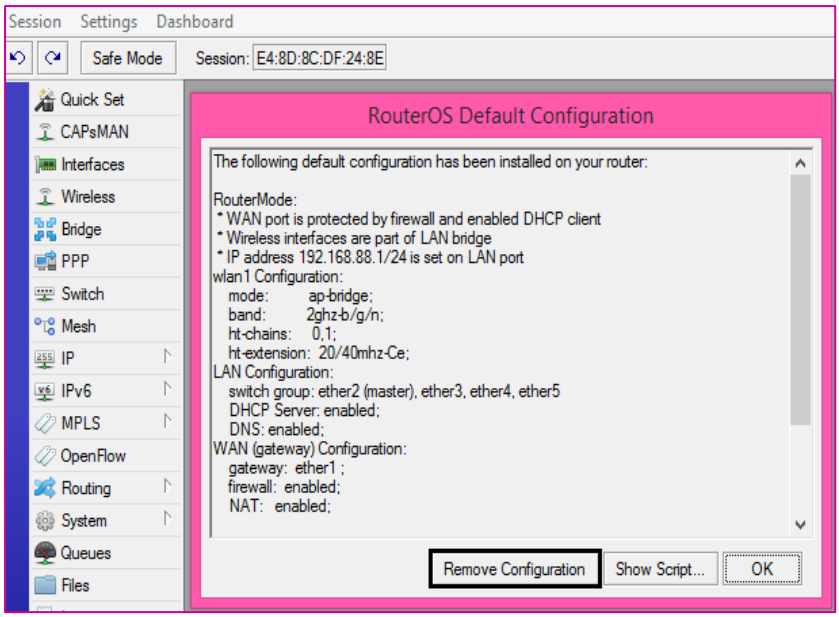
LAB 6 – Mengakses Mikrotik dengan Winbox

Cara yang paling sering digunakan untuk mengakses mikrotik adalah dengan winbox. Selain mempunyai mode GUI dan CLI sekaligus, kita juga akan bisa menggunakan fitur-fitur yang dimiliki mikrotik dengan maksimal jika mengkonfigurasi menggunakan winbox.



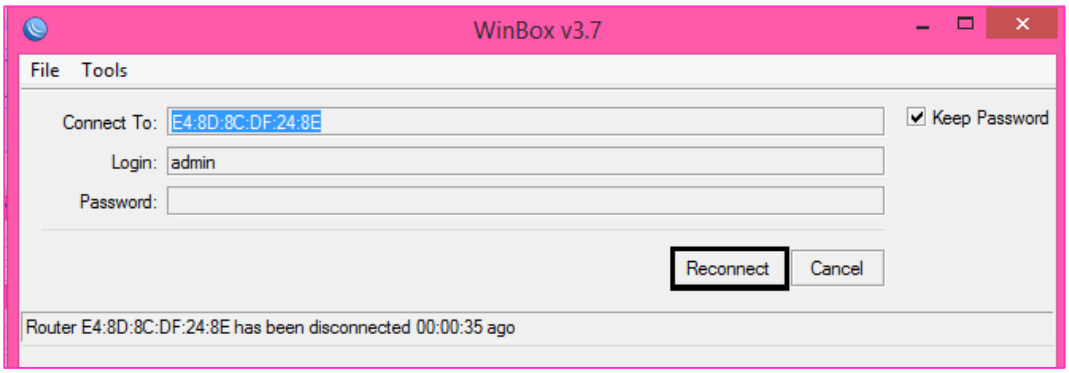
Gambar 6.1 Akses Mikrotik Menggunakan Winbox

Saat pertama kali kita meremote mikrotik, akan muncul sebuah peringatan apakah kita ingin menghapus default configuration atau tidak. Tetapi disarankan untuk menghapus default configuration tersebut. Karena beberapa default configuration tersebut akan mempersulit kita dalam melakukan konfigurasi.



Gambar 6.2 Halaman Utama Winbox

Sesaat setelah meremove default configuration mikrotik, kita akan otomatis disconnect dari winbox, selanjutnya kita hanya perlu reconnect.



Gambar 6.3 Reconnect Winbox Mikrotik

LAB 7 – License Mikrotik

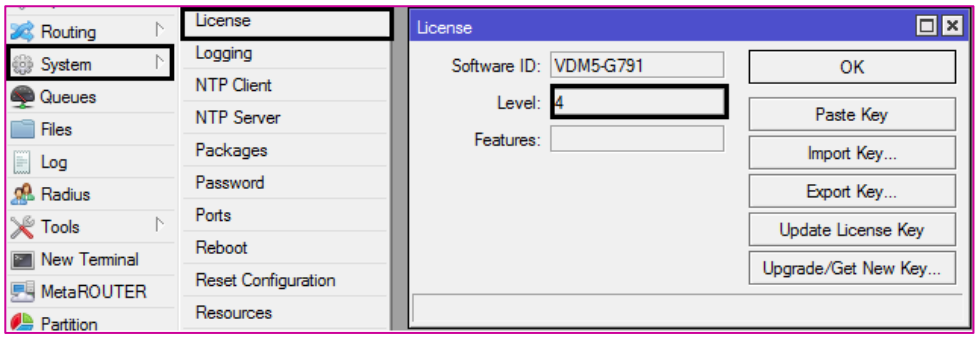
Mikrotik mempunyai beberapa level license. Setiap level mempunyai beberapa perbedaan dalam hal fitur dan fungsi. Berikut adalah perbedaan antara masing-masing level license yang ada pada mikrotik.

Fitur	Level 0	1	3	4	5	6
Wireless Client dan Bridge	24 Jam	-	Yes	Yes	Yes	Yes
Wireless AP	24 Jam	-	-	Yes	Yes	Yes
EoIP Tunnels	24 Jam	1	Unlimited	Unlimited	Unlimited	Unlimited
PPPoE Tunnels	24 Jam	1	200	200	500	Unlimited
PPTP Tunnels	24 Jam	1	200	200	Unlimited	Unlimited
L2TP Tunnels	24 Jam	1	200	200	Unlimited	Unlimited

VLAN	24 Jam	1	Unlimited	Unlimited	Unlimited	Unlimited
Hostpot Active Users	24 Jam	1	1	200	500	Unlimited

Tabel diatas menunjukkan beberapa perbedaan yang mencolok antara beberapa license yang ada pada mikrotik. Selain perbedaan diatas, masih banyak perbedaan lain yang tidak saya masukkan (level 2 tidak ada, karena sudah dari sananya).

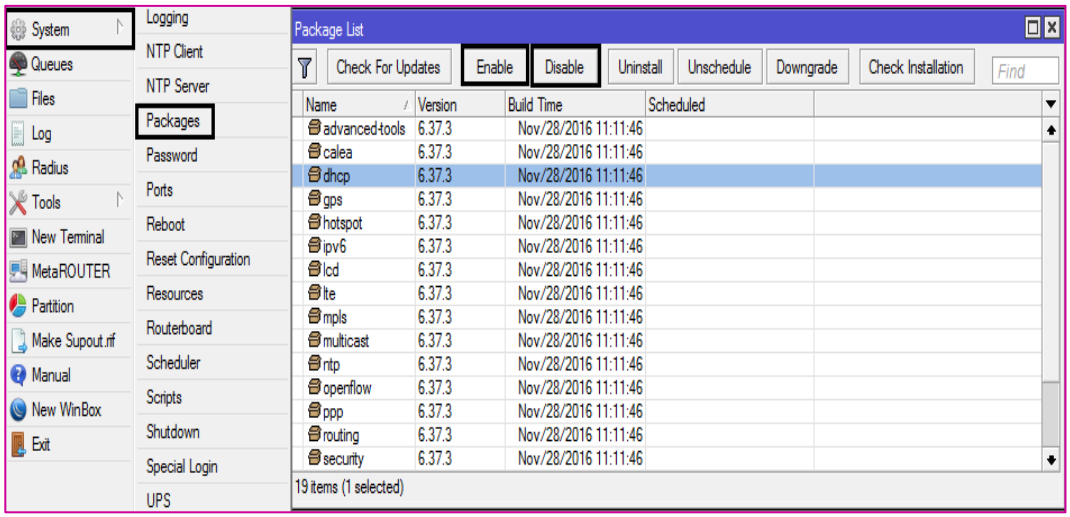
Berikut adalah langkah-langkah melihat level license pada mikrotik.



Gambar 7.1 Melihat License Pada Mikrotik

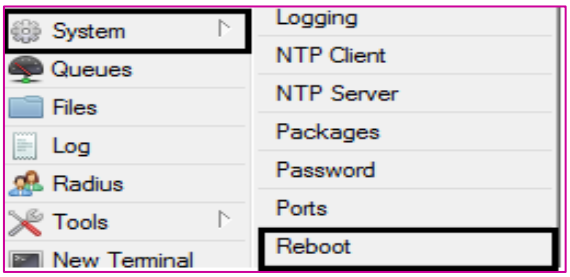
LAB 8 – Enable / Disable Package

Kita dapat mendisable beberapa fitur yang tidak kita butuhkan dalam mikrotik. Contohnya kita tidak butuh fitur dhcp, kita dapat mendisable fitur tersebut dengaan cara :



Gmbar 8.1 Enable Atau Disable Package Mikrotik

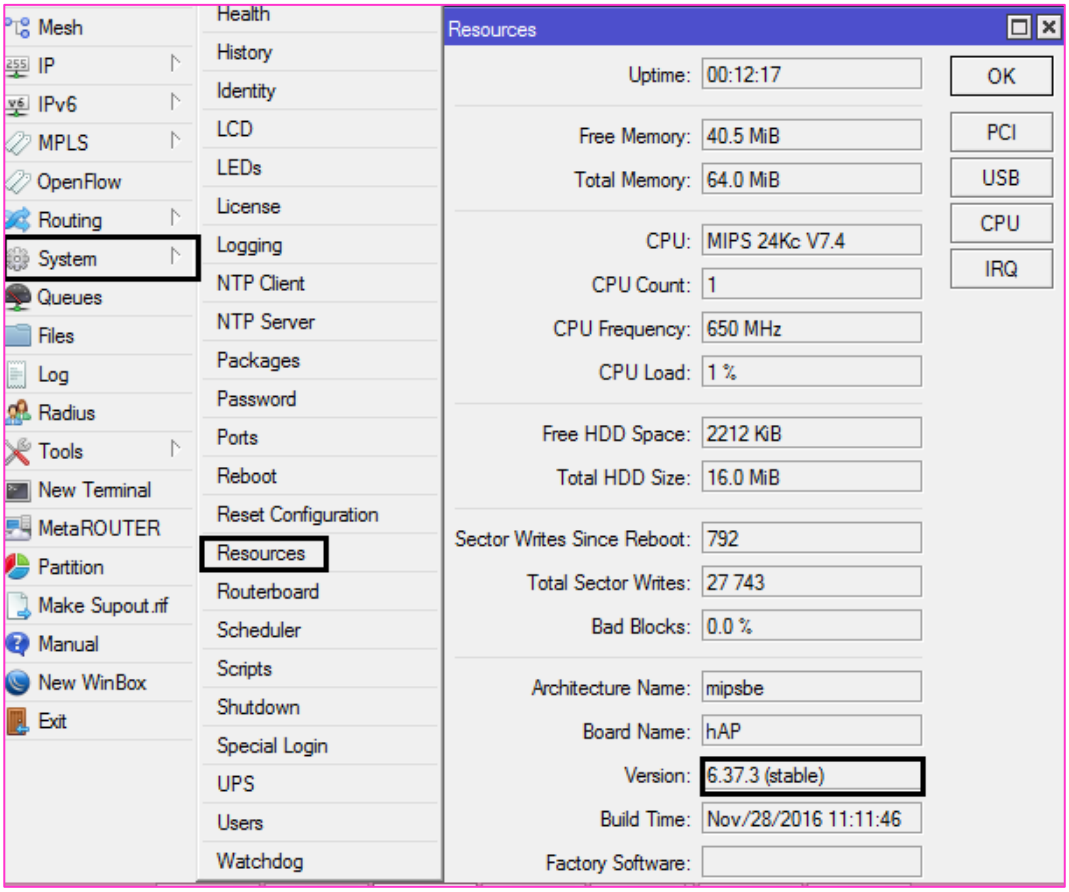
Setelah mendisable mikrotik dengan langkah seperti diatas, kita harus mereboot dengan router untuk melakukan perubahan.



Gambar 8.2 Reboot Mikrotik

LAB 9 – Version Mikrotik

Selain memiliki level license, mikrotik juga memilikiversion. Sampai saat ini versi mikrotik sudah mencapai level 6.37. Berikut adalah langkah-langkah untuk melihat versi pada mikrotik.



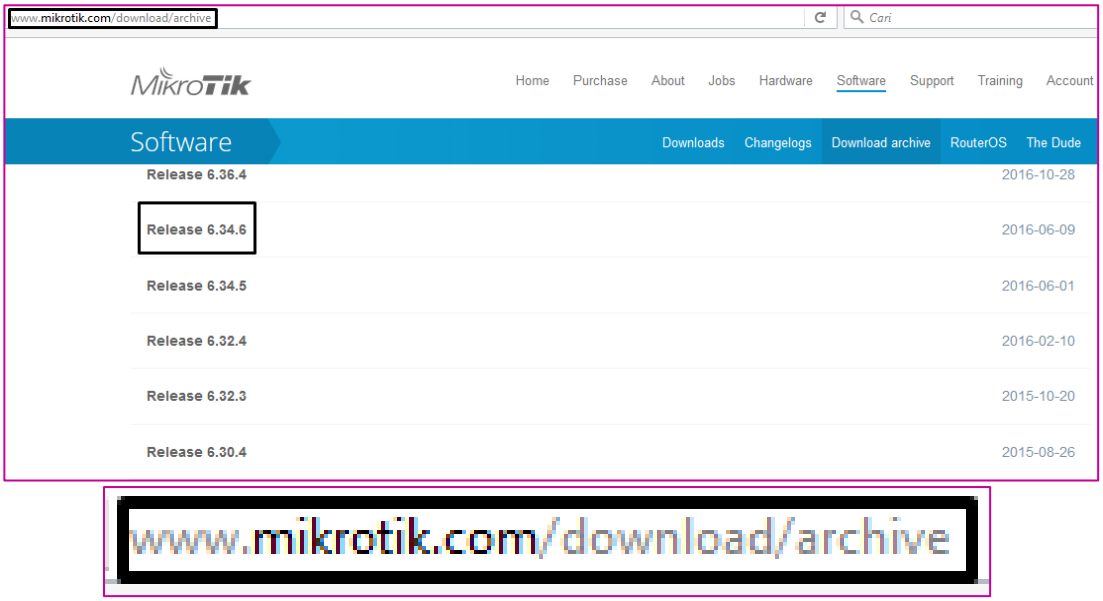
Gambar 9.1 Version Pada Mikrotik

LAB 10 – Upgrade Version Mikrotik

Seiring berjalannya waktu, mikrotik terus membuat perbaharuan version. Setiap versi baru pasti memiliki kelebihan dari versi yang lama. Sangat disarankan untuk melakukan upgrade ke versi terbaru untuk *bugfix* dan mendapat fitur-fitur terbaru.

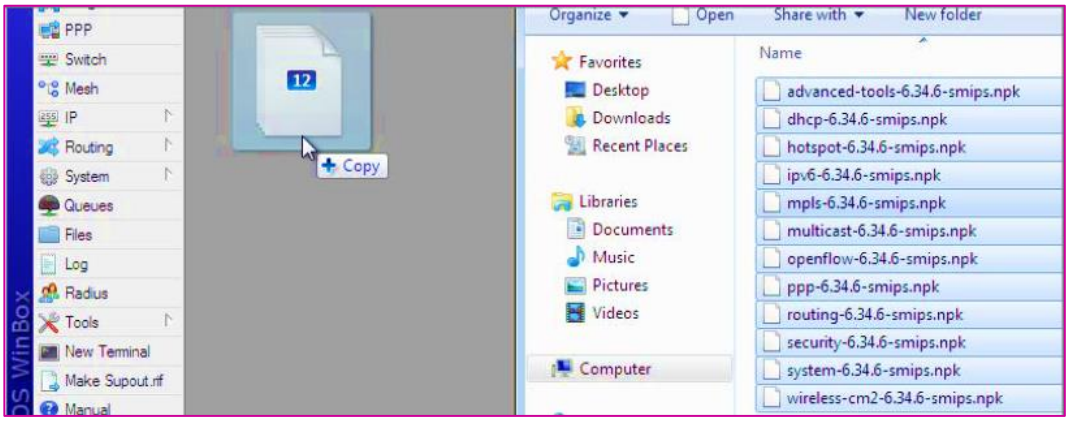
Untuk melakukan upgrade, hal pertama yang harus kita lakukan adalah mendownload paket mikrotik terbaru di http://mikrotik.com/download/archive. Pastikan download paket yang sesuai dengan routerboard yang kita miliki.

- Paket Mipsbe : digunakan untuk CRS, Netbox, PowerBox, QRT, RB9xx, hAP, mAP, RB4xx, cAP, hEX, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, dan RB7xx
- Paket Smips : digunakan untuk hAP lite
- Paket Tile : digunakan untuk CCR
- Paket PPC : digunakan untuk RB3xx, RB600. RB8xx, dan RB1xx
- Paket ARM : digunakan untuk RB3011
- Paket X86 : digunakan untuk RB230, dan X86
- Paket Mipsle : digunakan untuk RB1xx, RB5xx, dan Crossroads

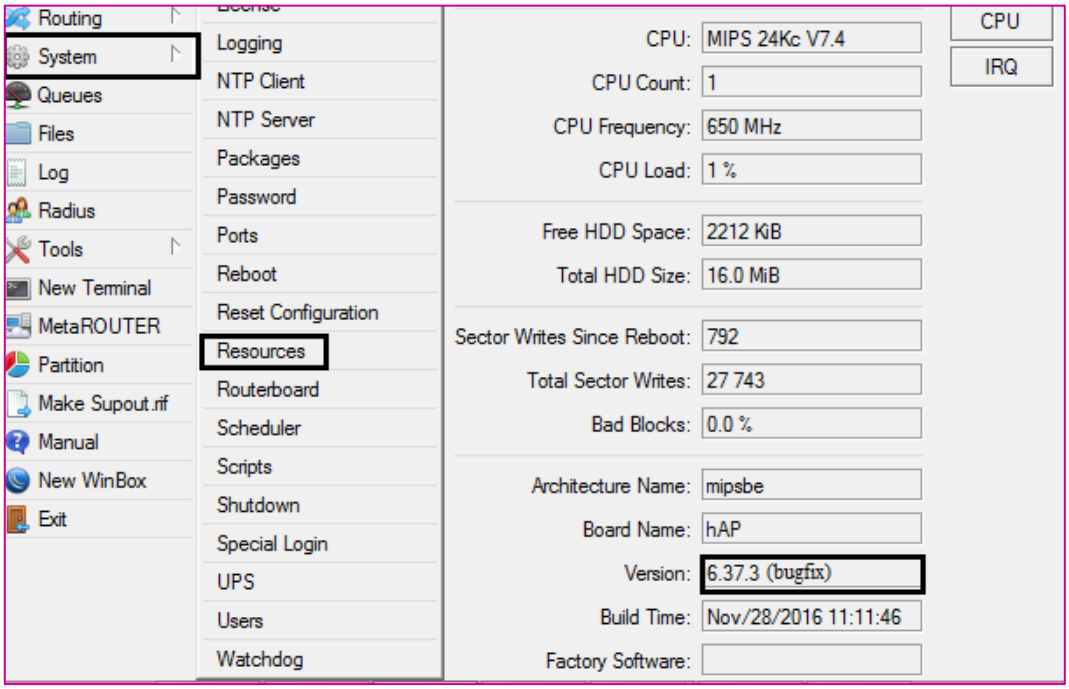


Gambar 10.1 Download Paket Mikrotik

Setelah download paket mikrotik diatas, langkah selanjutnya adalah extract paket tersebut kemudian upload ke mikrotik dengan cara drag and drop. Seperti terlihat pada gambar berikut :

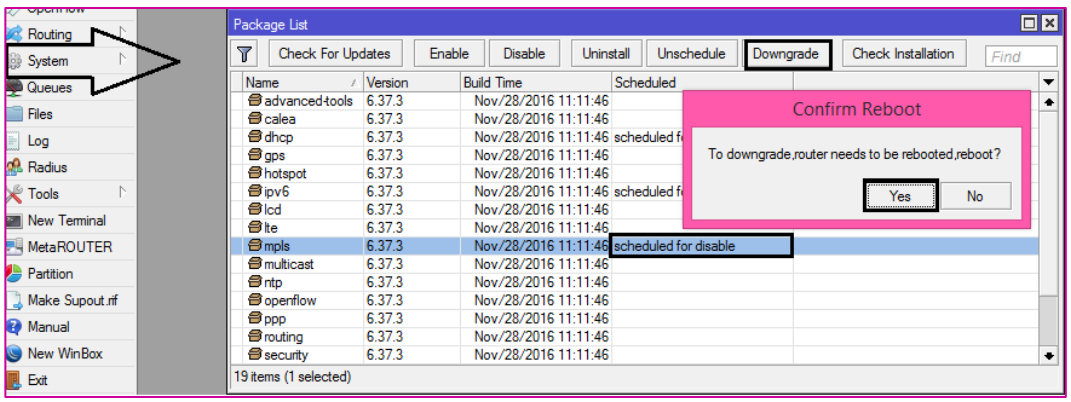


Gambar 10.2 Upload Paket Mikrotik Ke Winbox



Gambar 10.3 Hasil Upgrade Mikrotik

LAB 11 – Downgrade Mikrotik

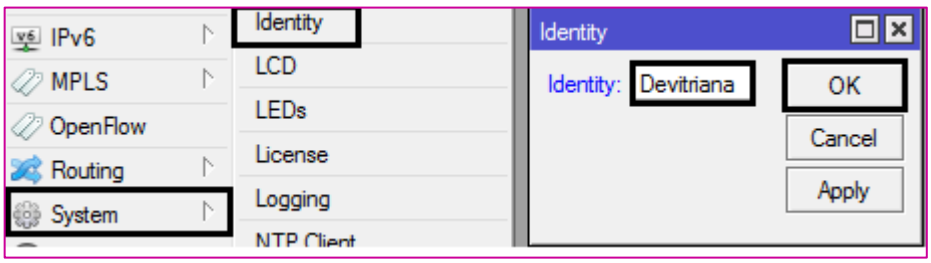


Gambar 11.1 Downgrade Mikrotik

Downgrade biasanya kita perlu lakukan jika ternyata routerboard kita tidak support dengan mikrotik versi terbaru. Terlihat pada gambar diatas, untuk melakukan downgrade, kita harus download versi mikrotik yang lama, upload ke winbox kemudian pilih opsi “Downgrade” pada menu package.

LAB 12 – Konfigurasi Identity Mikrotik

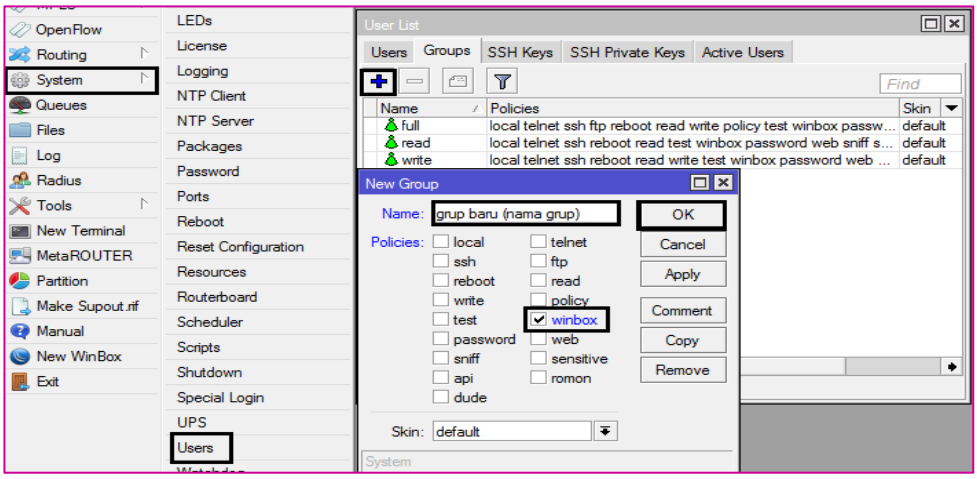
Sebuah identitas dari perangkat itu sangat dibutuhkan guna mengenali perangkat apa yang sedang kita akses dan konfigurasi supaya tidak salah melakukan konfigurasi jika ada banyak alat yang terpasang. Identity merupakan pengenal mikrotik dalam jaringan, atau biasa kita menyebutnya sebagai **hostname**.



Gambar 12.1 Konfigurasi Identity

Setelah diganti, nama identity kalian akan muncul diatas jendela winbox. Dan jika kalian keluar dari winbox, maka nanti ada nama kalian di jendela sebelum memasuki winbox.

LAB 13 – Management Group Mikrotik

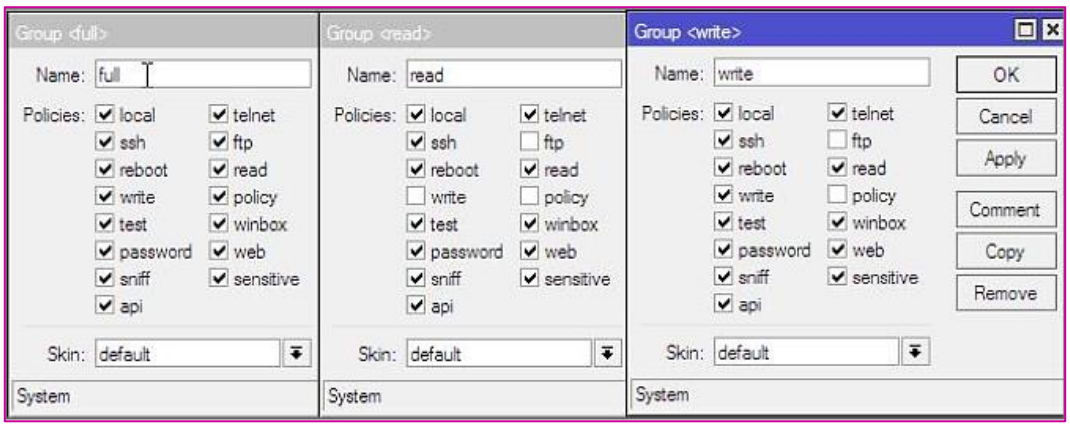


Gambar 13.1 Menambahkan group mikrotik

Secara default mikrotik memiliki tiga group, yaitu full, read, dan write. Kita bisa melakukan manipulasi terhadap ke tiga group ini. Selain itu kita juga bisa menambahkan group ke mikrotik sesuai dengan keinginan kita.

Pada gambar diatas menunjukkan cara untuk menambahkan sebuah group di mikrotik. Group yang ditambahkan pada gambar diatas hanya memiliki hak akses winbox. Sedangkan nantinya user yang termasuk grup ini hanya bisa melakukan winbox tanpa bisa melakukan hal lain. (yang dicentang ialah yang dapat diakses, begitu sebaliknya).

Adapun group default yang dimiliki mikrotik adalah sebagai berikut :



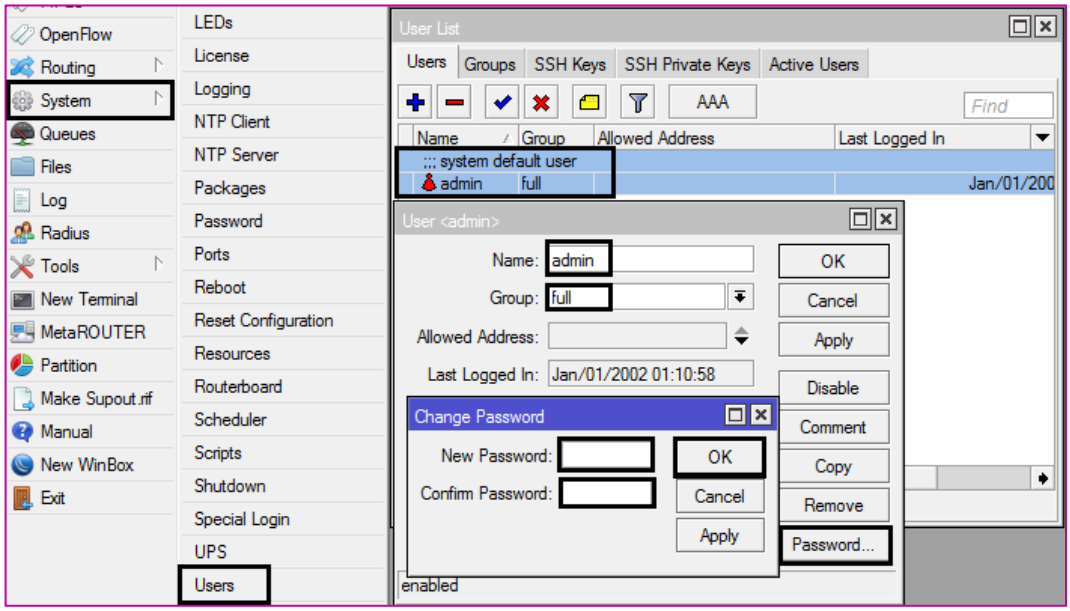
Gambar 13.2 Group Default Mikrotik

Meskipun ketiga group tersebut merupakan group default (dari sananya) yang dimiliki mikrotik, namun kita bisa memanipulasi ketiga group tersebut sesuai kebutuhan.

Setelah melakukan management group, kita dapat menerapkan group tersebut ke dalam user-user yang ada dimikrotik.

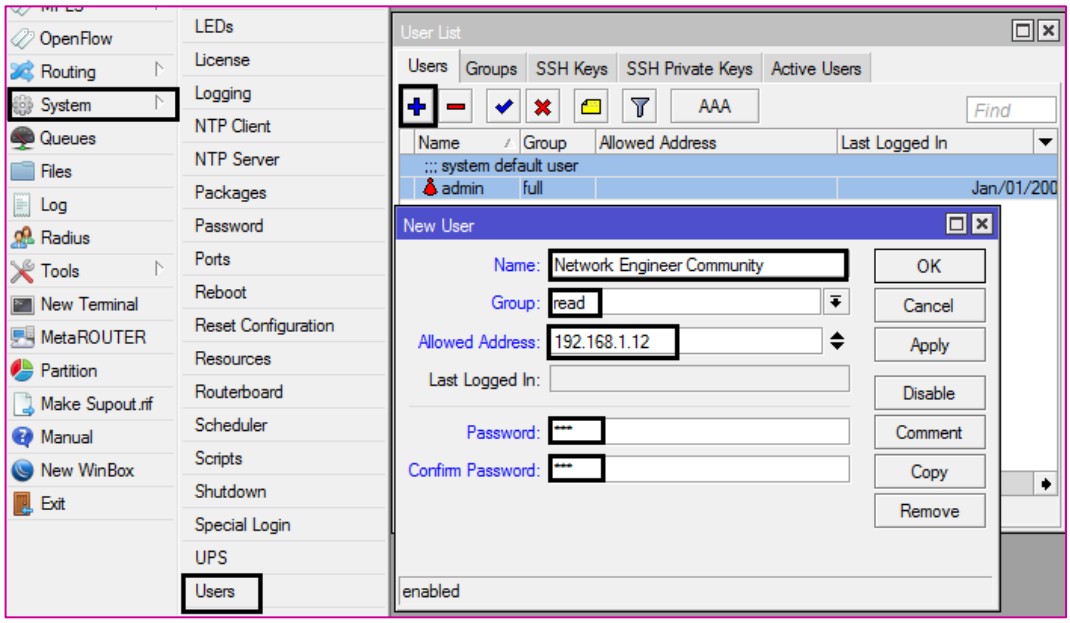
LAB 14 – Mengakses Mikrotik dengan SSH

Secara default user mikrotik adalah *admin* dengan password (kosong). Tentunya kita sebagai Network Engineer tidak akan membiarkan hal ini. Kita harus merubah default user tersebut dengan mengklik 2x.



Gambar 14.1 Management user mikrotik

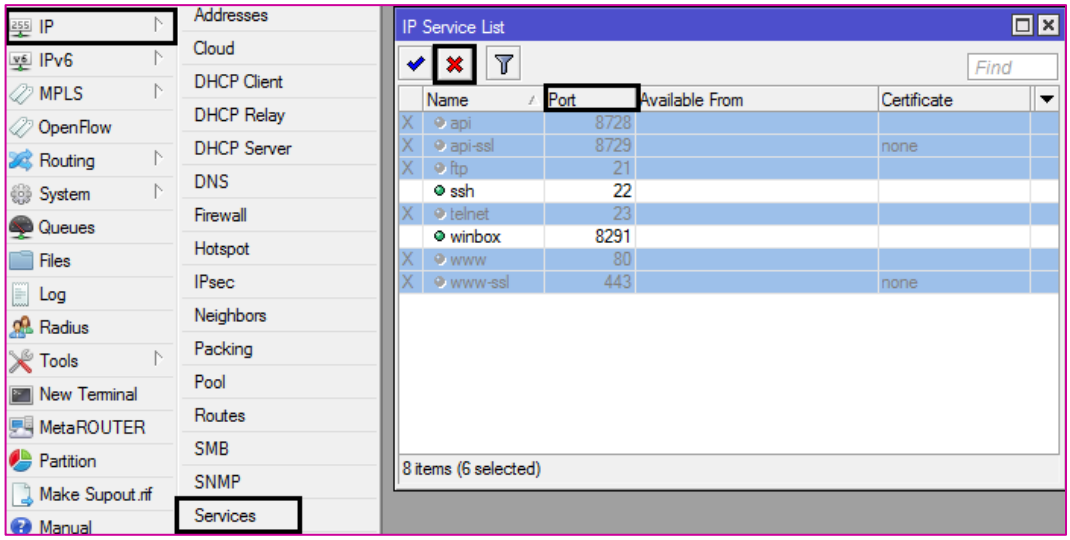
Kita juga menambahkan user pada mikrotik. Hal ini biasanya dilakukan jika kita mempunyai banyak anak buah. Untuk menginginkan agar anak buah kita tersebut bisa login ke mikrotik, namun tidak mempunyai hak akses full. Sehingga solusinya kita perlu menambahkan user dengan hak akses read.



Gambar 14.2 Menambah user dengan hak akses read

LAB 15 – Managemen Service Mikrotik

Secara default, kita bisa meremote mikrotik menggunakan beberapa cara seperti yang sudah kita bahas sebelumnya. Namun untuk alasan keamanan, kita diharuskan untuk mendisable beberapa cara.

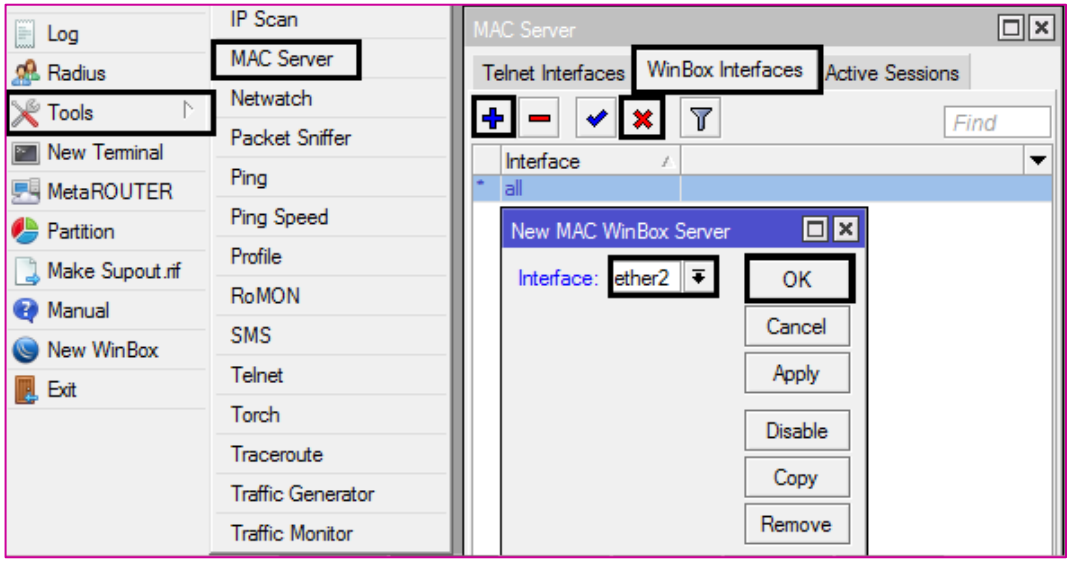


Gambar 15.1 Management service mikrotik

LAB 16 – Managemen MAC Server Mikrotik

Secara default, jika kita menghubungkan client mikrotik, baik melalui ether1, ether2, ataupun ether yang lain. Client bisa mendeteksi mac address mikrotik menggunakan winbox dan bisa meremote dengan mudah.

Ada beberapa saat dimana kita harus mengaktifkan fungsi ini, sehingga jika ada orang-orang yang tidak bertanggung jawab terhubung dengan mikrotik, dia tidak akan bisa meremote mikrotik dengan mudah. Namun demikian, kita tetap harus men-enable fungsi ini pada salah satu interface mikrotik untuk keperluan recovery.

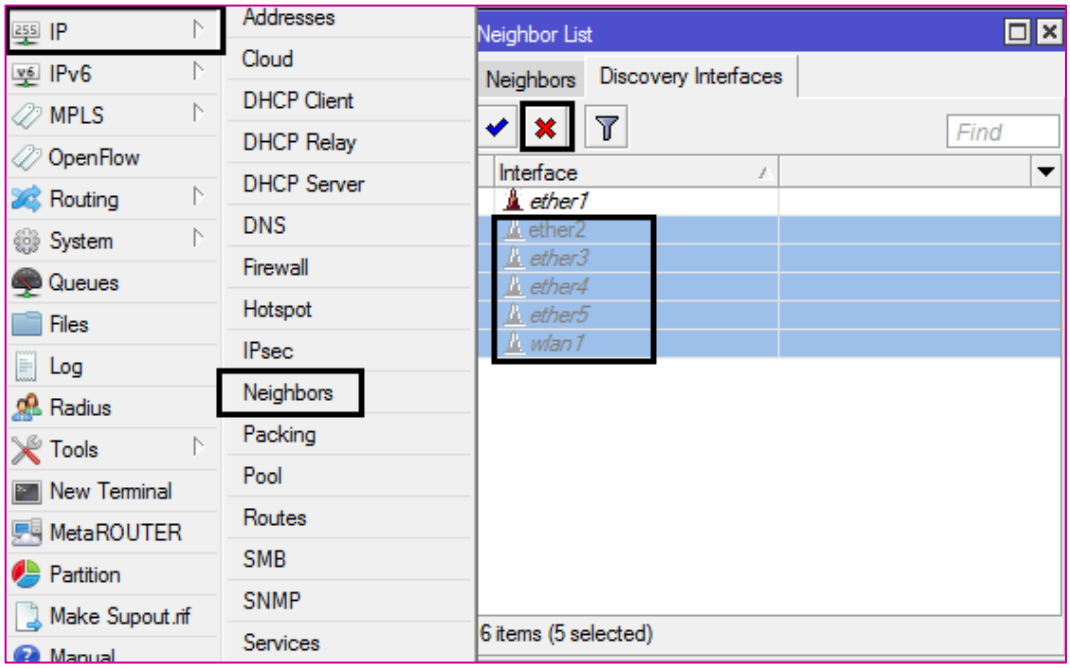


Gambar 16.1 Management MAC Server Mikrotik

Pada langkah diatas pertama kita disable "*all",* hal ini dikarenakan *all* berarti mengaktifkan mac server pada seluruh interface. Selanjutnya baru kita tambahkan satu interface untuk mengaktifkan mac server.

LAB 17 – Managemen MNDP

Mikrotik Neighbor Discovery Protocol (MNDP) adalah protokol yang memyngkinkan kita bisa mnegtahui mikrotik lain yang terhubung langsung dengan mikrotik kita. Ada kalanya kita harus mengaktifkan fitur ini, namun ada kalanya juga kita harus menonaktifkan fitur ini. Kesimpulannya adalah penggunaan fitur ini sesuai dengan kebutuhan kita.

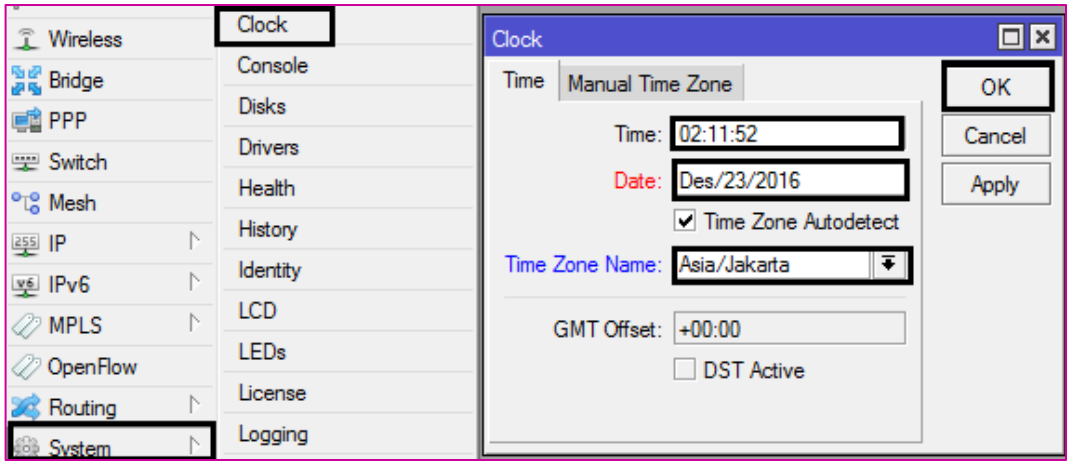


Gambar 17.1 Management MNDP mikrotik

Pada gambar diatas, terlihat bahwa kita mendisable MNDP pada interface ether2, ether3, ether4, dan *wlan1*. Sehingga jika suatu saatada router lain yang terhubung dengan router kita ini ke ether2, maka router lain tersebut tidak akan bisa mendeteksi keberadaan router kita.

LAB 18 – Management Waktu

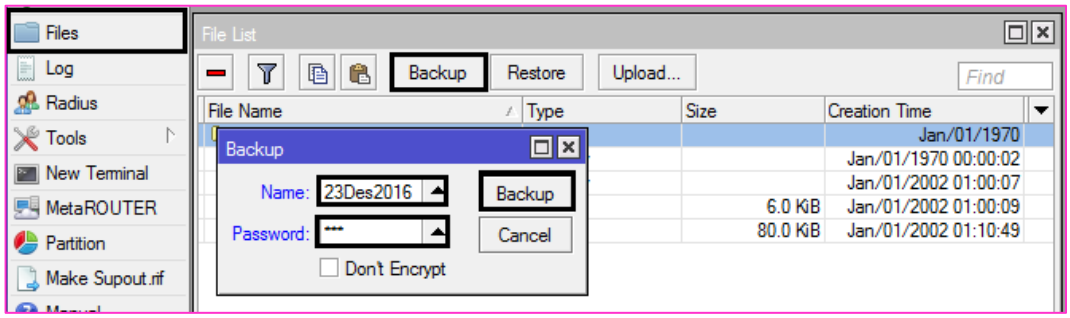
Agar mikrotik memiliki waktu yang sesuai dengan wilayah tempat kita tinggal, kita diharuskan untuk mengkonfigurasi clock seperti berikut.



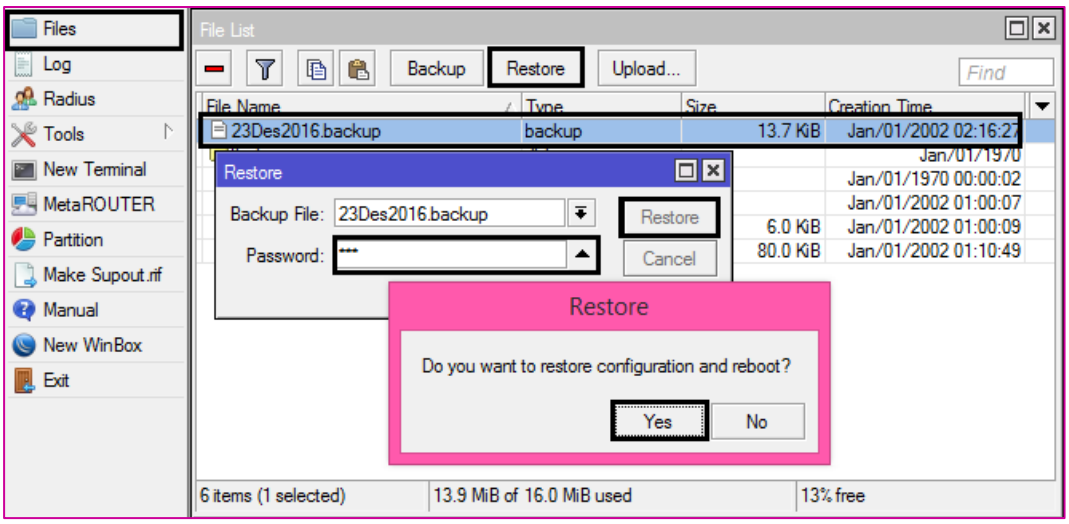
Gambar 17.1 Konfigurasi clock mikrotik

LAB 19 – Backup Dan Restore

Mikrotik yang kita miliki tidak akan selamanya berjalan normal. Ada kalanya mikrotik tiba-tiba *hank* dan seluruh konfigurasi tiba-tiba hilang. Untuk berjaga-jaga jika sewaktu-waktu hal seperti itu terjadi, maka kita harus melakukan backup konfigurasi. Selanjutnya jika suatu saat terjadi masalah, maka kita tidak perlu mengkonfigurasi dari awal lagi, kita hanya perlu merestore konfigurasi yang telah kita backup sebelumnya.



Gambar 19.1 Backup Konfigurasi Mikrotik



Gambar 19.2 Restore konfigurasi mikrotik

Terlihat bahwa router akan otomatis reboot saat kita melakukan restore konfigurasi di mikrotik.

LAB 20 – Export Dan Import

Selain menggunakan fitur backup dan restore, kita juga bisa menggunakan fitur export dan import. Dari segi fungsi, kedua cara ini sama. Namun terdapat beberapa perbedaan pada fitur ini. Berikut adalah tabel perbedaan dari fitur tersebut :

Karakteristik	**Backup & Restore**	**Import & Export**
Bisa dengan GUI	Yes	No
Backup semua konfig	Yes	No (user & password)
Reboot setelah Restore	Yes	No
Enkripsi	Yes	No

Berikut adalah perintah yang digunakan untuk melakukan **export** :

```
[admin@Devitriana] > export file=”23Des2016”
```

perintah **export** diatas digunakan untuk export seluruh konfigurasi mikrotik (kecuali username dan password). Jika ingin **export** konfigurasi IP Address saja, maka kita dapat menggunakan perintah dibawah ini :

```
[admin@Devitriana] > ip address export file=”konfigurasi ip 23Des2016”
```

Sedangkan untuk import dapat menggunakan perintah berikut :

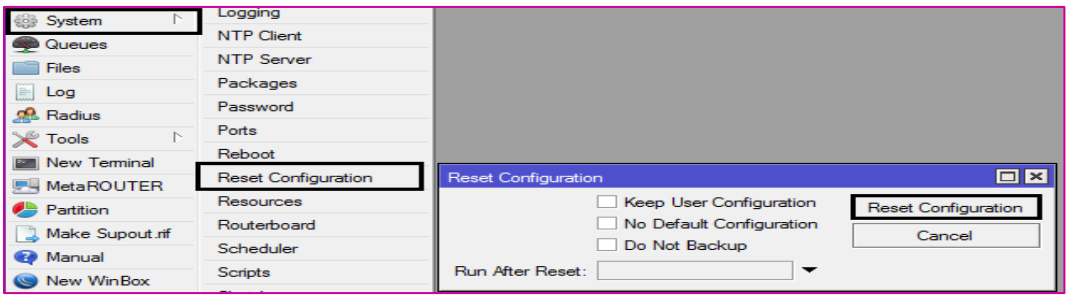
```
[admin@Devitriana] > import file-name=”konfigurasi ip 23Des2016”
```

LAB 21 – Mengakses Mikrotik dengan SSH

Jika diminta untuk konfigurasi ulang mikrotik dari awal. Saat ada perintah seperti itu, maka kita harus mereset seluruh konfigurasi mikrotik. Sebaiknya sebelum mereset, selalu lakukan backup agar data tidak lenyap begitu saja.

Ada 2 cara untuk mereset mikrotik :

1. Soft reset (menggunakan winbox atau ssh)



Gambar 21.1 Soft reset mikrotik

2. Hard reset (cara ini biasanya digunakan saat kita lupa username dan password untuk login mikrotik atau saat mikrotik error dan kita tidak bisa login ke mikrotik).

Gambar 21.2 Hard reset mikrotik

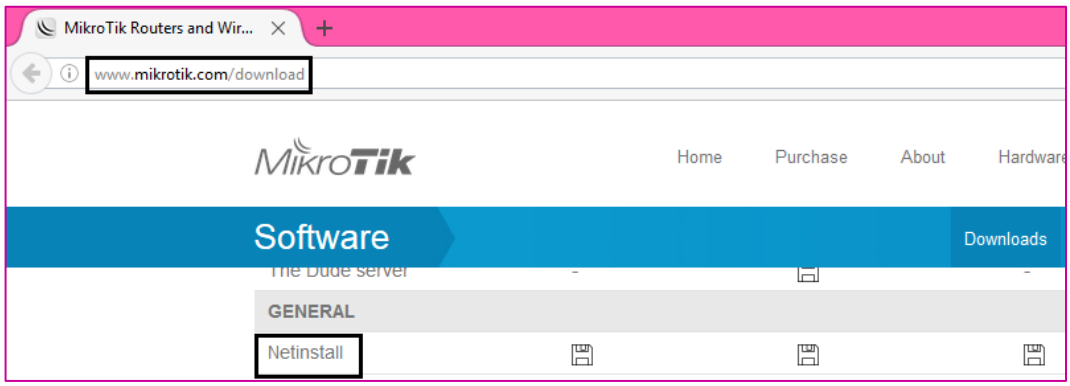
Adapun langkah-langkah yang harus dilakukan :

- Cabut kabel power
- Tekan tombol reset (menggunakan pulpen/sejenisnya)
- Tancapkan kabel power (tombol reset tetap ditekan)
- Lepas tombol reset jika lampu indikator ACT sudah berkedip-kedip

LAB 22 – Mengakses Mikrotik dengan SSH

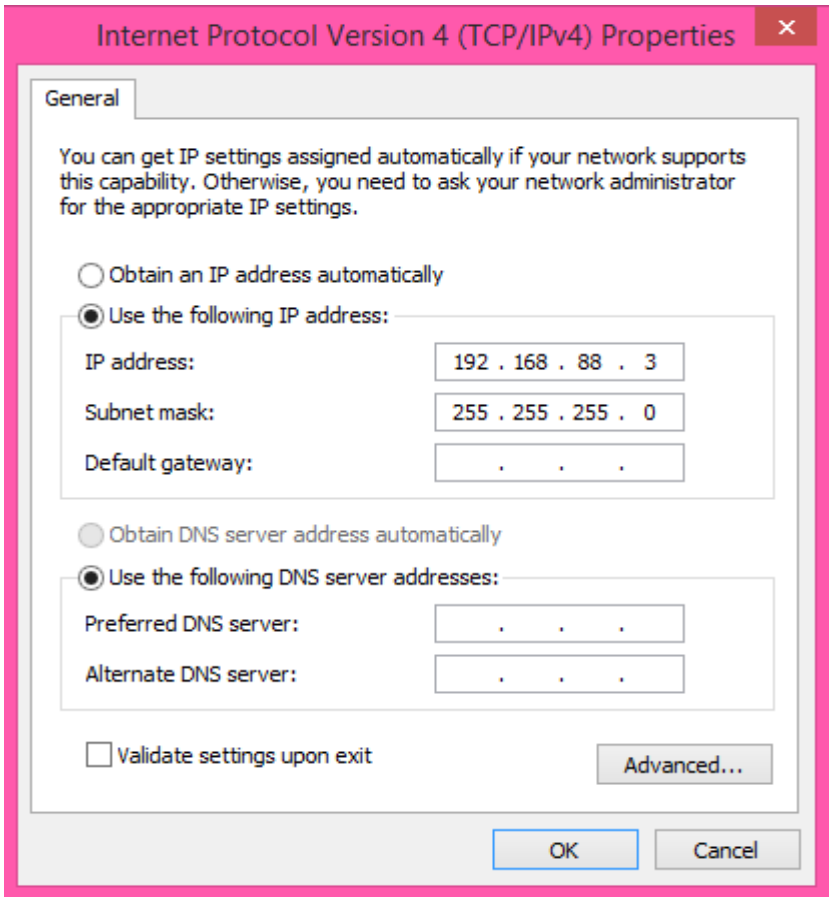
Saat mikrotik yang kita miliki error, kita bisa melakukan install ulang terhadap mikrotik layaknya instal ulang sebuah komputer. Untuk install mikrotik, kita membutuhkan **netinstall,** silahkan download di :

http://www.mikrotik.com/download



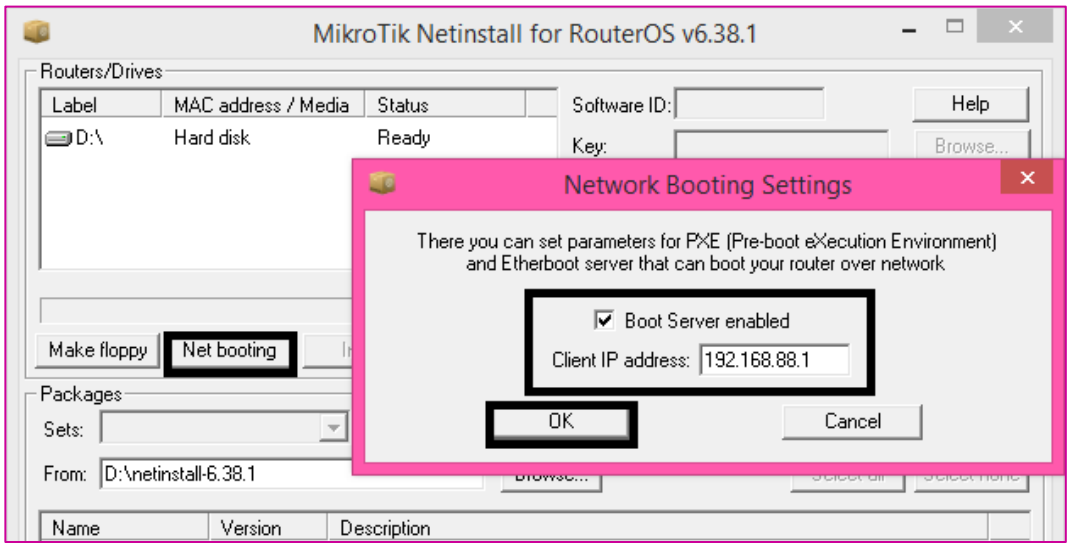
Gambar 22.1 Download Netinstall

Selanjutnya pastikan kita mengkonfigurasi IP Address pada client secara manual (sesuka hati)



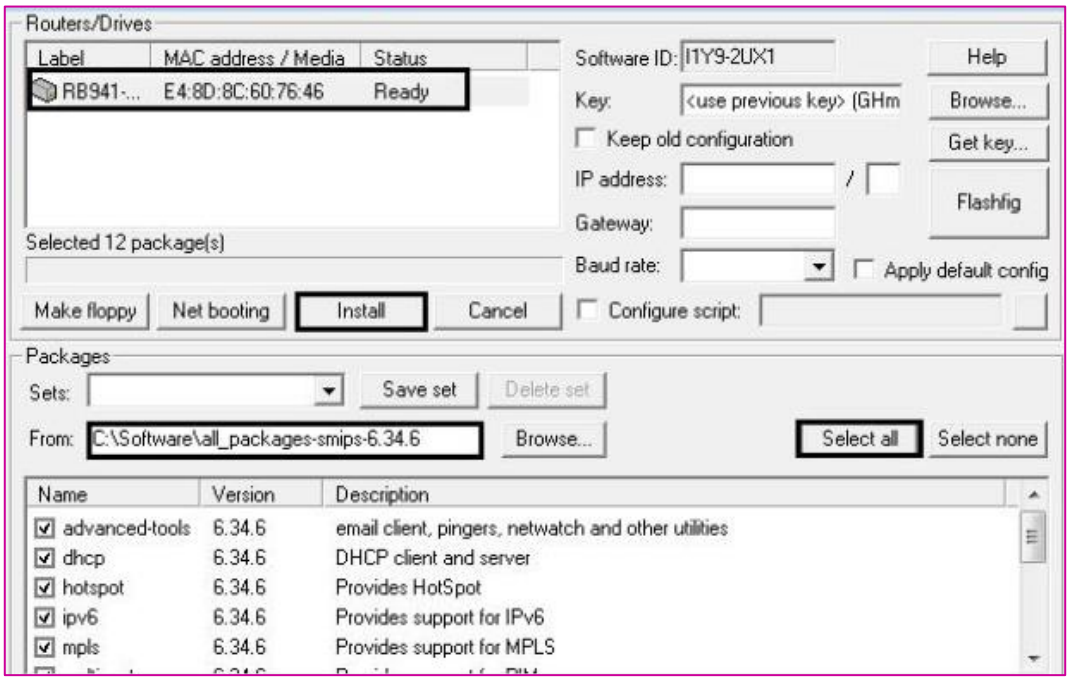
Gambar 22.2 Konfigurasi IP Address Pada Client

Selanjutnya hubungkan komputer client ke ether1 mikrotik dan buka aplikasi netinstall yang baru saja didownload. Konfigurasikan net booting seperti berikut :



Gambar 22.3 Konfigurasi Net Booting

Saat konfigurasi net booting seperti diatas, kita bisa memasukkan IP sesuka hati tetapi harus satu jaringan dengan IP Address yang kita konfigurasikan pada client sebelumnya. Setelah mengkonfigurasi net booting, tekan tombol reset pada mikrotik layaknya saat kita mereset mikrotik, hingga mikrotik terdeteksi di net install.



Gambar 22.4 Install Mikrotik Menggunakan Net Install

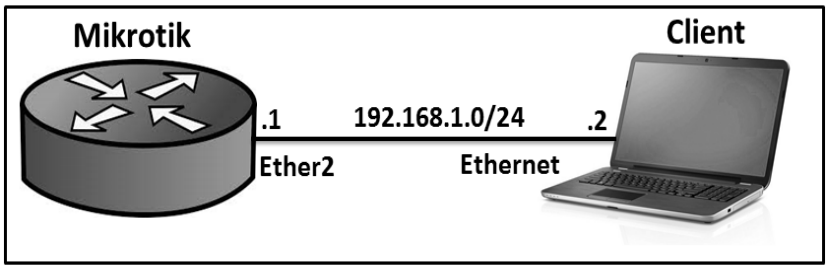
Pada bagian *from* arahkan ke folder dimana kita menyimpan paket-paket mikrotik yang telah kita download pada lab upgrade mikrotik sebelumnya. Terakhir pilih install dan tunggu proses instalisasi selesai.

BAB II

Management Network

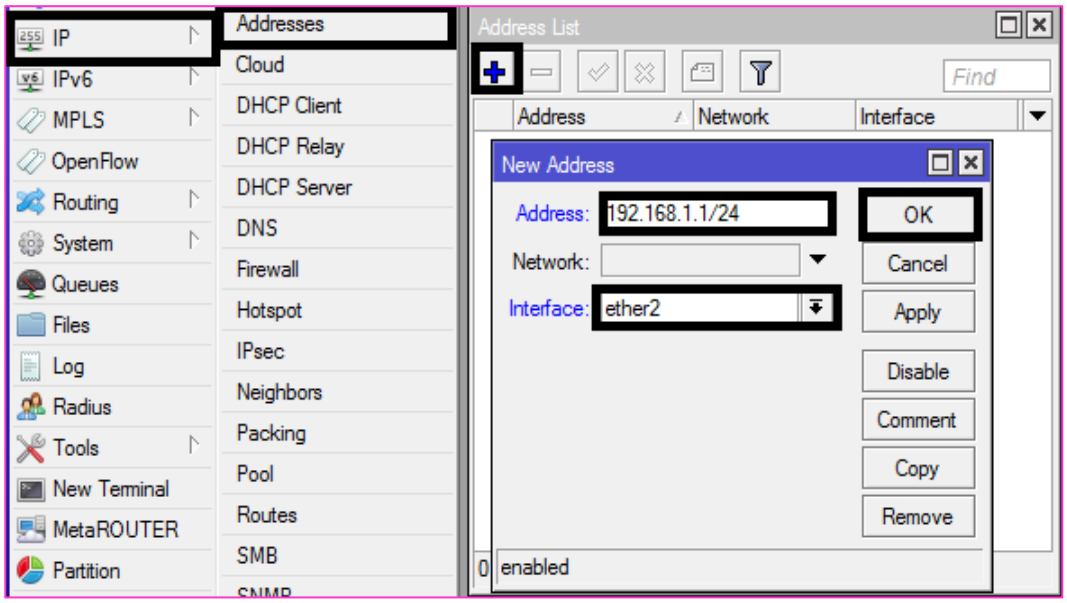
LAB 23 – Konfigurasi IP Address

Pada lab ini kita akan belajar konfigurasi ip address pada mikrotik. Berikut ini adalah topologi yang akan kita gunakan :



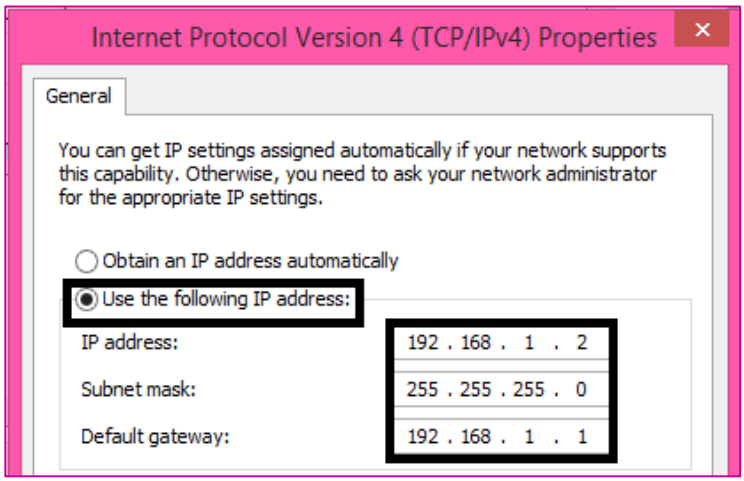
Gambar 22.1 Topologi konfigurasi IP Address

Berikut langkah-langkah yang bisa kita gunakan untuk konfigurasi IP Address di mikrotik :



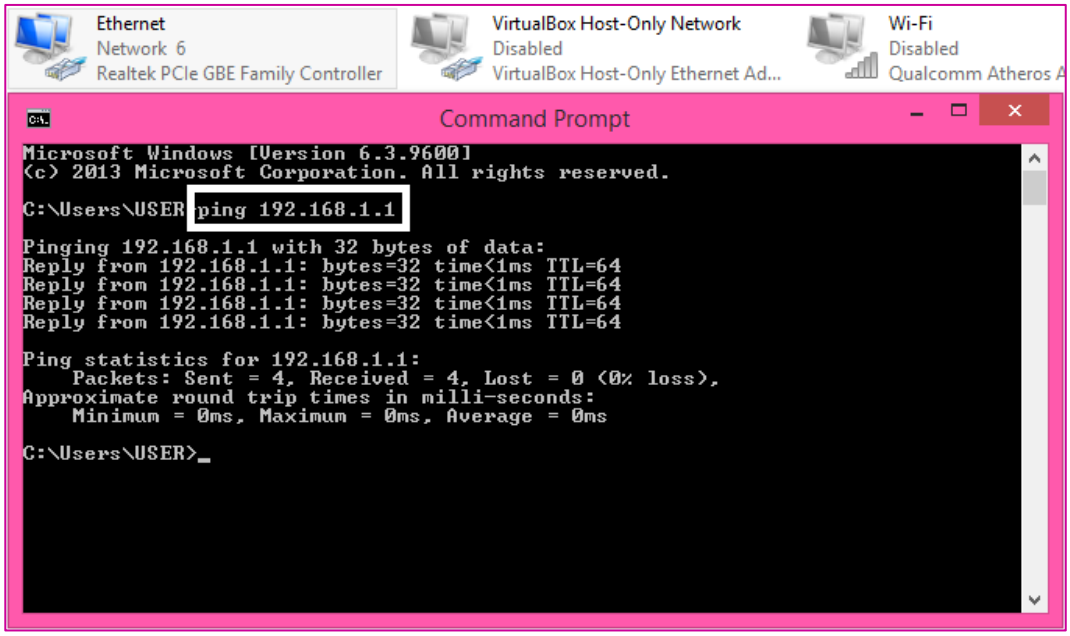
Gambar 22.2 Konfigurasi IP Address mikrotik

Selanjutnya lakukan konfigurasi IP Address pada client :



Gambar 23.3 Konfigurasi IP Pada Client

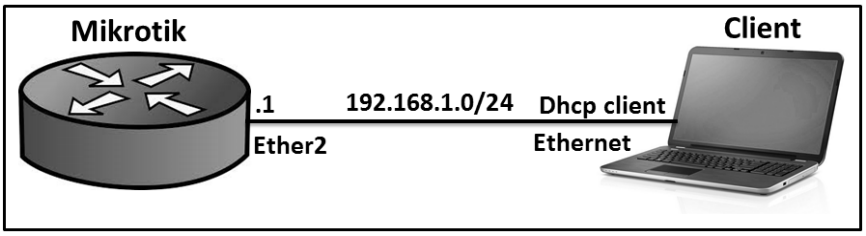
Untuk pengujian, lakukan ping dari client ke mikrotik



Gambar 23.4 Ping Dari Client Ke Mikrotik

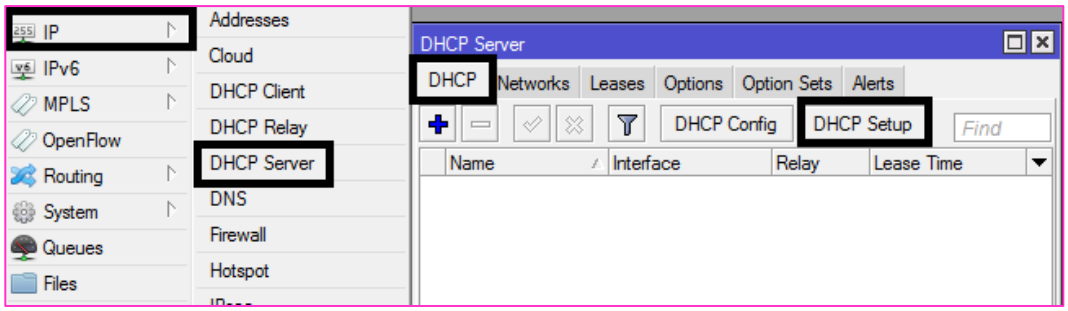
LAB 24 – DHCP Server

Untuk mempermudah client agar tidak perlu mengkonfigurasi IP Address secara manual, maka kita bisa menggunakan fitur **dhcp server** pada mikrotik. Berikut adalah topologi yang akan kita gunakan :



Gambar 24.1 Topologi DHCP Server

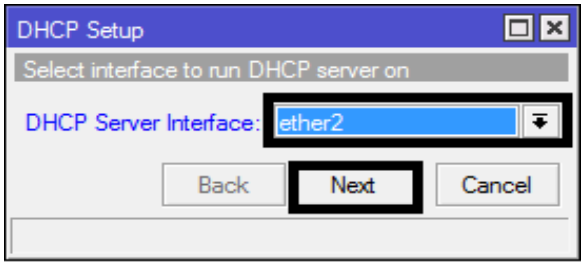
Diasumsikan kita telah melakukan konfigurasi IP Address pada mikrotik. Selanjutnya kita lakukan konfigurasi DHCP Server.



Gambar 24.2 Setup DHCP Server Mikrotik

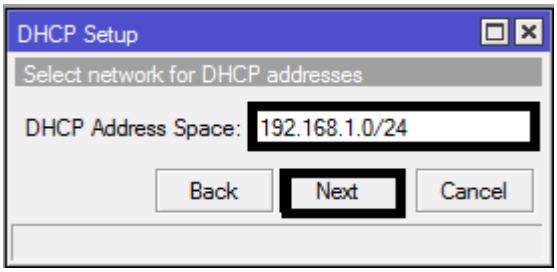
Berikut adalah langkah-langkahnya :

1. Kita diminta untuk menentukan di interface mana DHCP Server akan diaktifkan. Disini saya mengaktifkan pada ether 2.



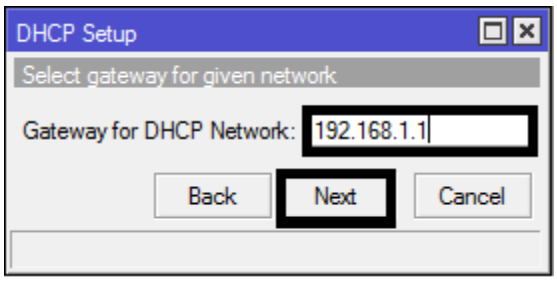
Gambar 24.3

2. Sebelumnya pada ether 2 sudah terpasang IP Addres 192.168.1.0/24. Maka pada langkah kedua, penentuan DHCP Space akan otomatis mengambil segment IP yang sama. Jika sebelumnya belum terdapat IP maka kita dapat menentukannya secara manual.



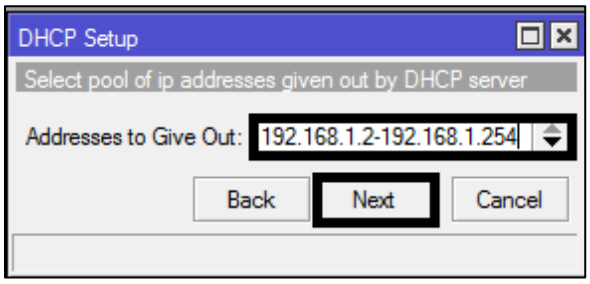
Gambar 24.4

3. Selanjutnya kita diminta untuk menentukan IP Address yang akan digunakan sebagai default-gateway oleh DHCP Client nantinya. Secara otomatis wizard akan menggunakan IP Address yang terpasang pada interface ether 2.



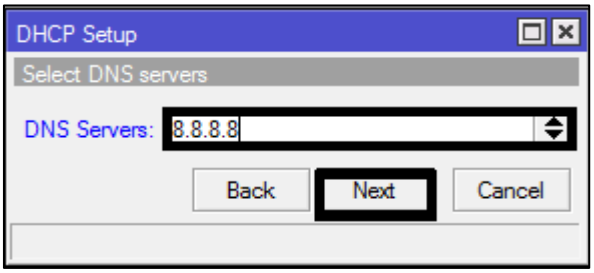
Gambar 24.5

4. Kemudian kita tentukan IP Address yang akan di distribusikan ke client. Secara otomatis wizard akan mengisikan host IP pada segment yang telah digunakan. IP 192.168.1.1 tidak akan masuk dalam Address TO Give Out, sebab IP tersebut telah digunakan sebagai gateway dan tidak akan di distribusikan ke client.



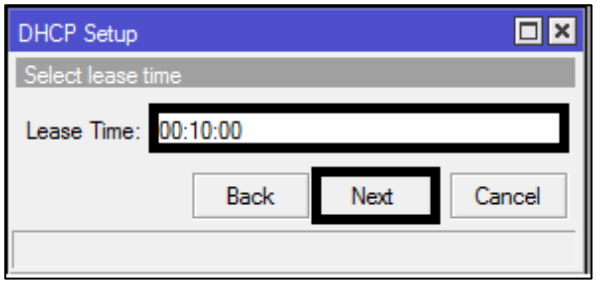
Gambar 24.6

5. Kita juga haris menentukan, 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 kita igin menentukan request DNS Client ke server tertentu.

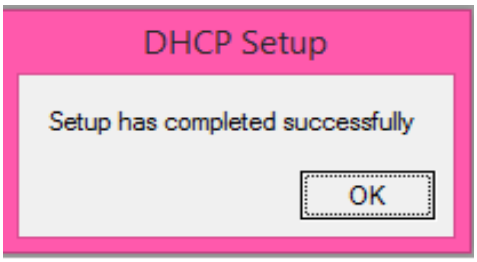


Gambar 24.7

6. Langkah terakhir kita diminta untuk menentukan Lease-Time, yaitu berapa lma sebuah IP Address akan dipinjamkan ke Client. Untuk menghindari penuh atau kehabisan IP, setting Lease-Time jangan terlalu lama, misalkan beberapa menit saja.

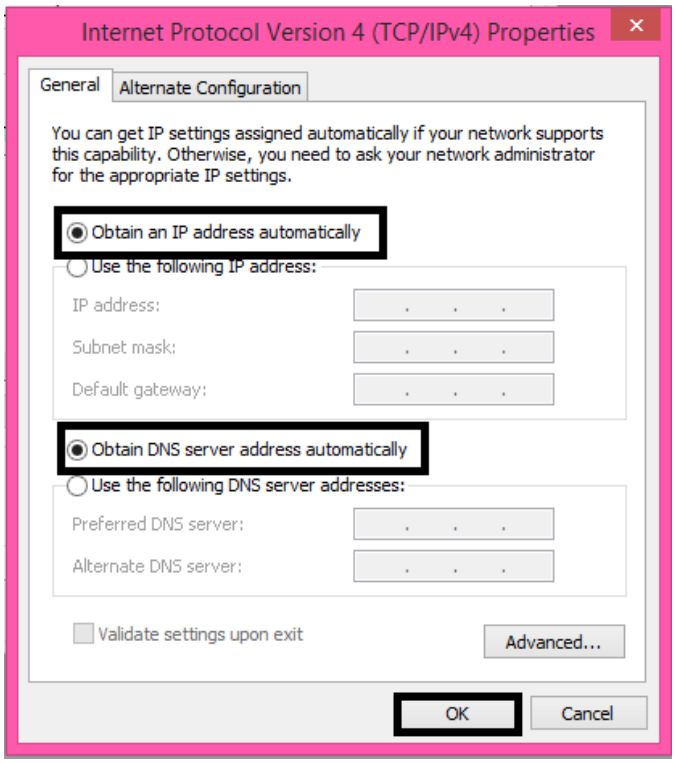


Gambar 24.8



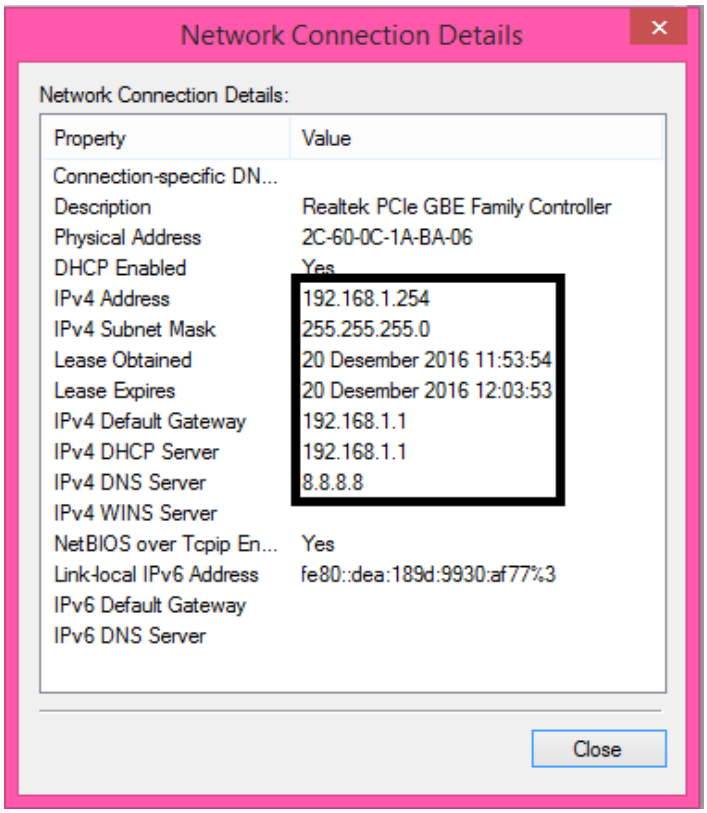
Gambar 24.9 Proses Setup DHCP Server Selesai

Untuk melakukan pengujian, lakukan konfigurasi dhcp client di komputer client :



Gambar 24.10 Konfigurasi DHCP Client

Hasil akhir dari lab ini adalah komputer client mendapatkan IP Address dari mikrotik secara otomatis.

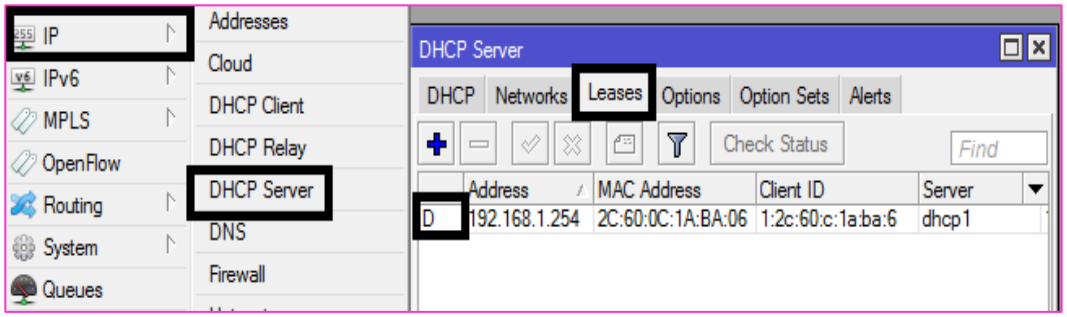


Gambar 24.11 Client Mendapatkan IP DHCP

LAB 25 – DHCP MAC Static

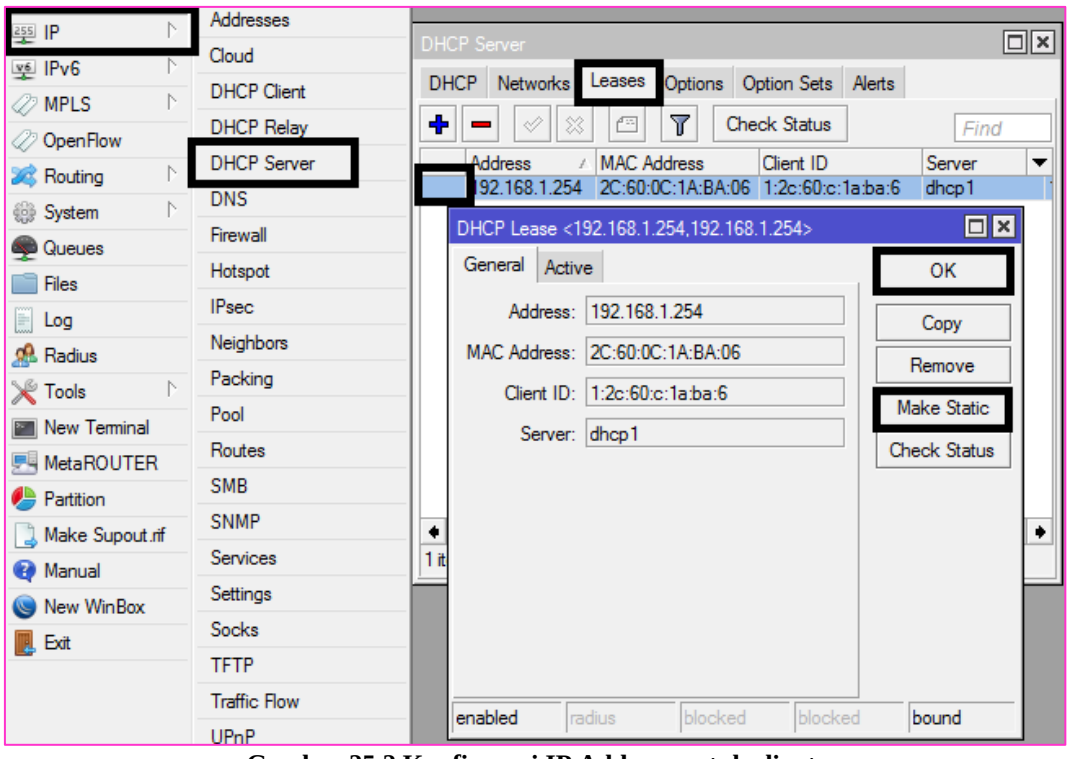
Pada lab sebelumnya kita sudah belajar membuat DHCP Server di mikrotik. Selanjutnya pada lab ini kita akan belajar bagaimana agar sebuah client selalu mendapatkan IP Address yang sama saat request IP secara DHCP (otomatis). Kita memakai topologi yang sama seperti lab 24.

Tujuan kita pada lab ini adalah mengkonfigurasi agar komputer client selalu mendapat IP Address 192.168.1.2 saat request dhcp ke dhcp server. Berikut konfigurasi yang harus kita lakukan :



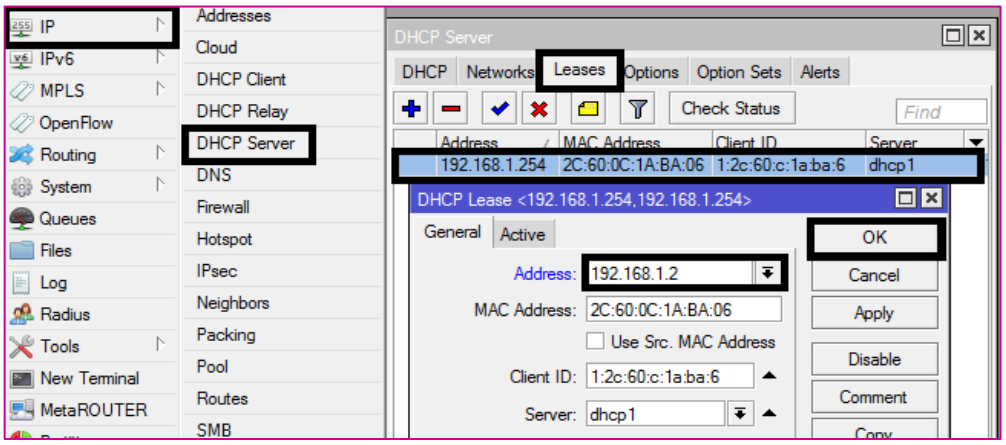
Gambar 25.1 Konfigurasi DHCP MAC Static

Selanjutnya pilih kembali pada bagian leases untuk mengkonfigurasi IP Address yang diinginkan.



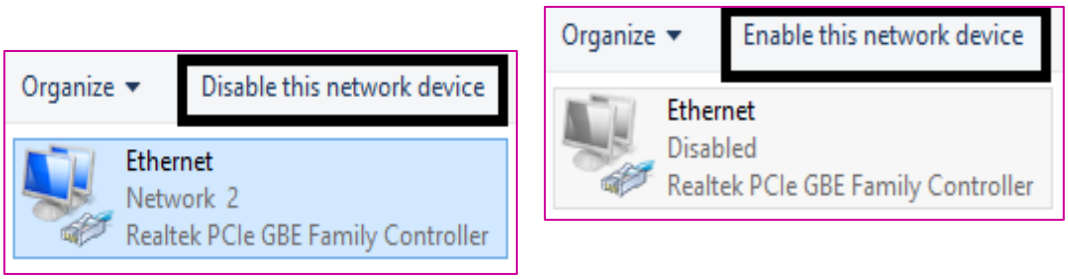
Gambar 25.2 Konfigurasi IP Address untuk client

Ketika kita mengklik "Make Static" secara otomatis tanda **D** pada kolom disamping address akan hilang. Itu menandakan DHCP MAC static sudah berhasil dikonfigurasi.



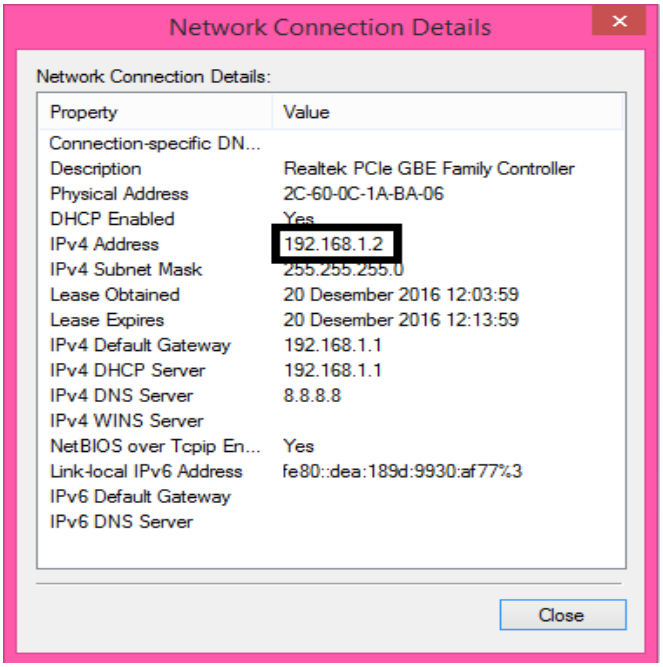
Gambar 25.3 DHCP MAC Static Berhasil Dibuat

Untuk pengujian, lakukan disable dan enable interface pada komputer client



Gambar 25.4 Disable dan Enable Interface Pada Komputer Client

DHCP MAC Static juga bisa dikatakan berfungsi sebagai pemberi IP secara otomatis tetapi kita bisa atur secara static. Berikut adalah hasil konfigurasi dhcp mac static. Perhatikan bahwa client mendapatkan IP 192.168.1.2 sesuai yang kita inginkan.

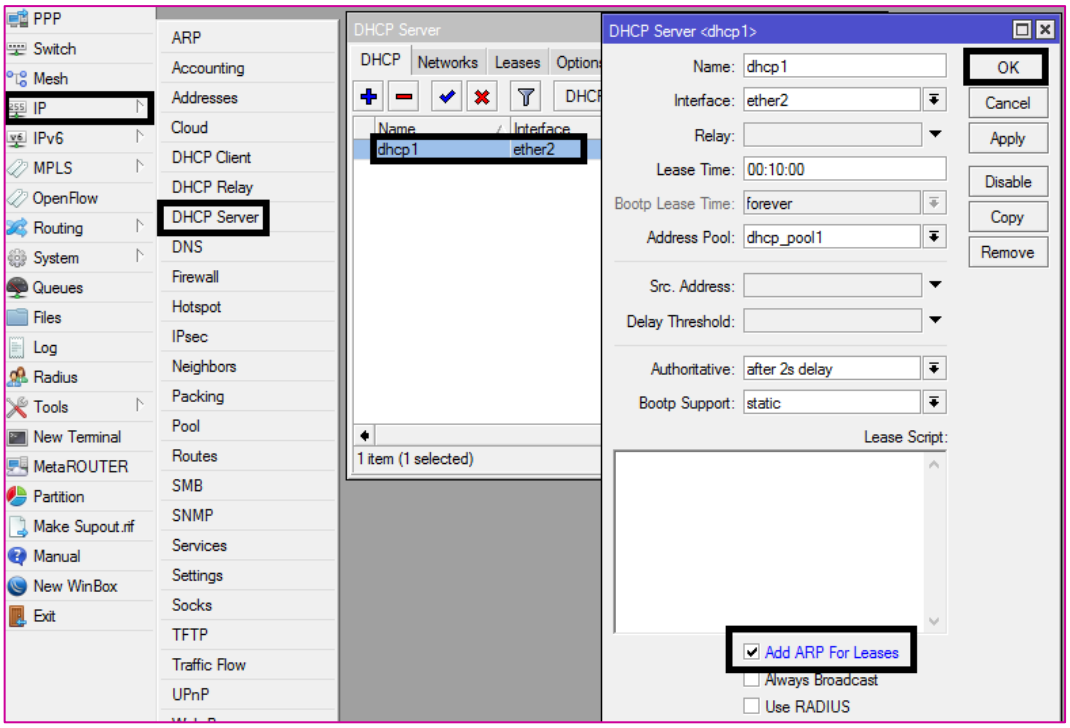


Gambar 25.5 Hasil DHCP MAC Static

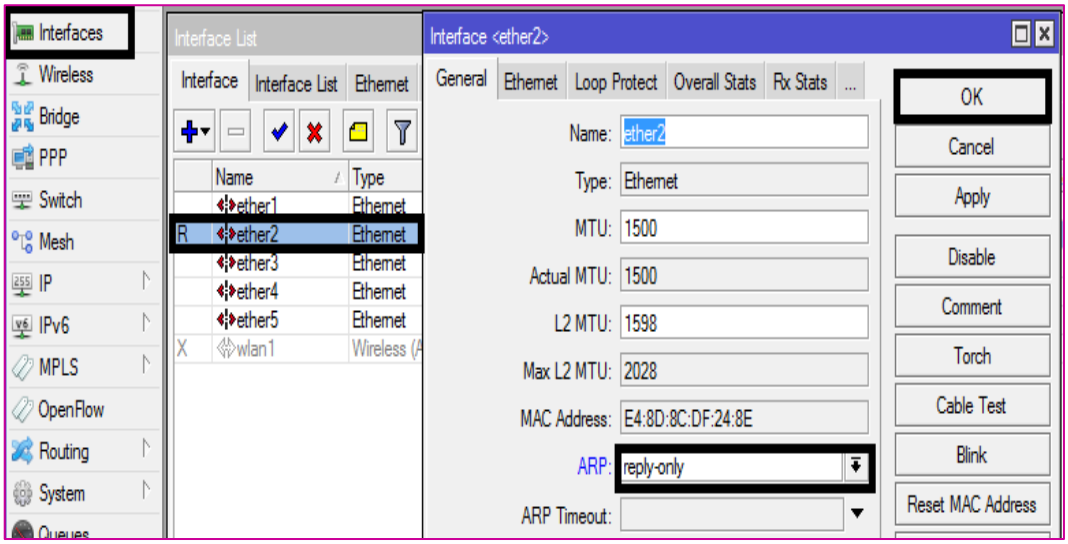
LAB 26 – DHCP Server Security

Tujuan lab ini adalah mengkonfigurasi agar jika client mengkonfigurasi IP Secara manual, maka client tersebut tidak akan bisa terhubung ke router atau bisa dikatakan tujuan lab ini adalah mencegah client mengkonfigurasi IP secara manual.

Pada lab ini kita juga menggunakan topologi yang sama seperti lab 24. Selanjutnya berikut konfigurasi yang perlu kita lakukan :

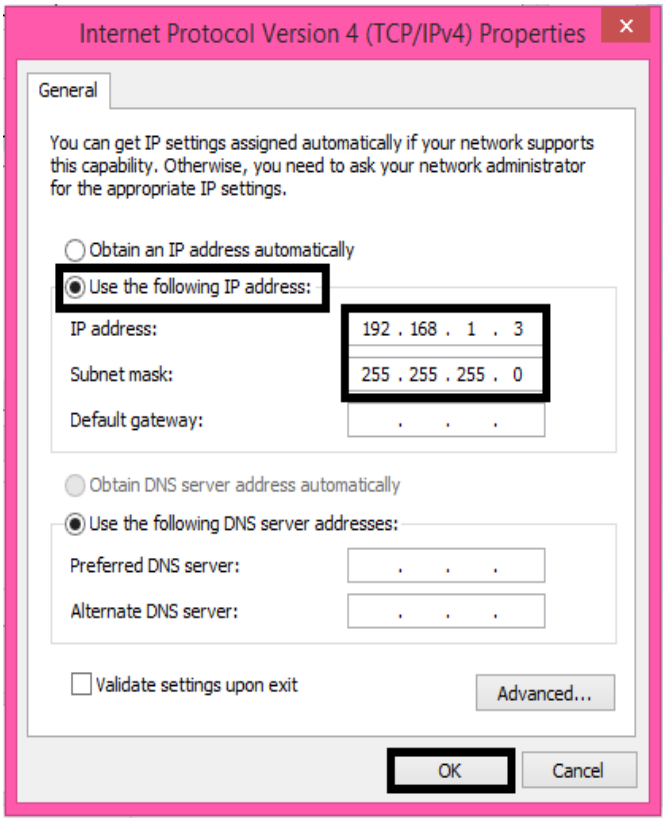


Gambar 26.1 Konfigurasi DHCP Security



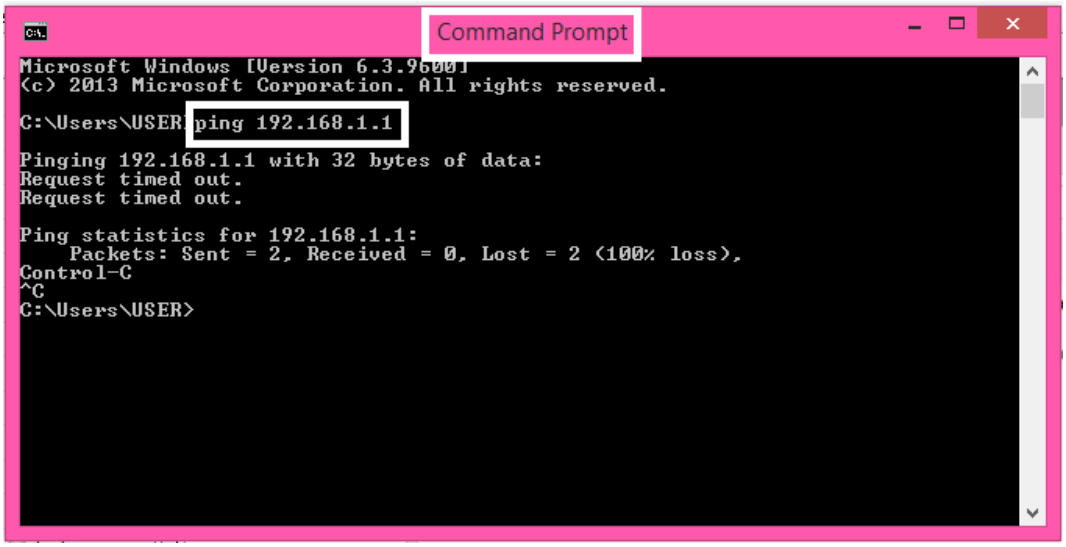
Gamabr 26.2 Konfigurasi DHCP Security

Untuk pengujian, coba konfigurasikan IP Address secara manual dikomputer



Gambar 26.3 Konfigurasi IP secara manual

Sekarang coba lakukan ping dari client ke mikrotik (cmd)

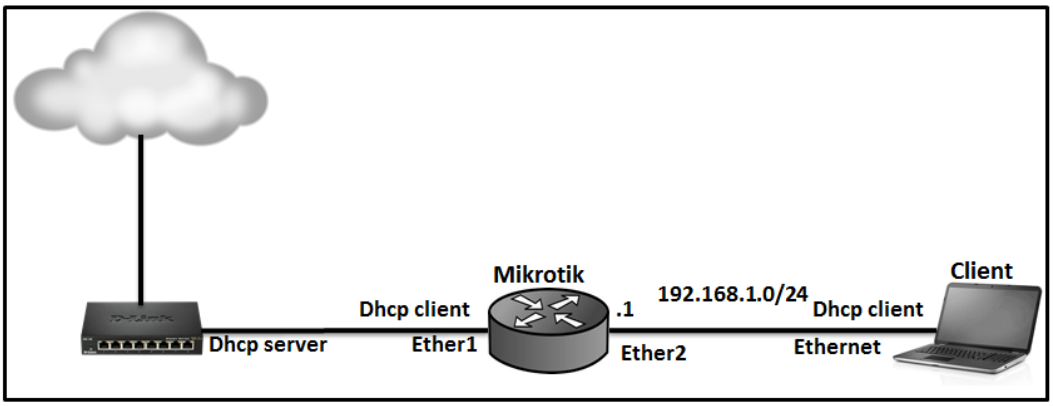


Gambar 26.4 Ping dari client ke mikrotik

Kita tadi mengkonfigurasi ip secara manual, maka hasilnya akan **"request time out"** atau tidak dapat tersambung ke router. Jika ingin tersambung lakukan konfigurasi ip secara otomatis (dhcp).

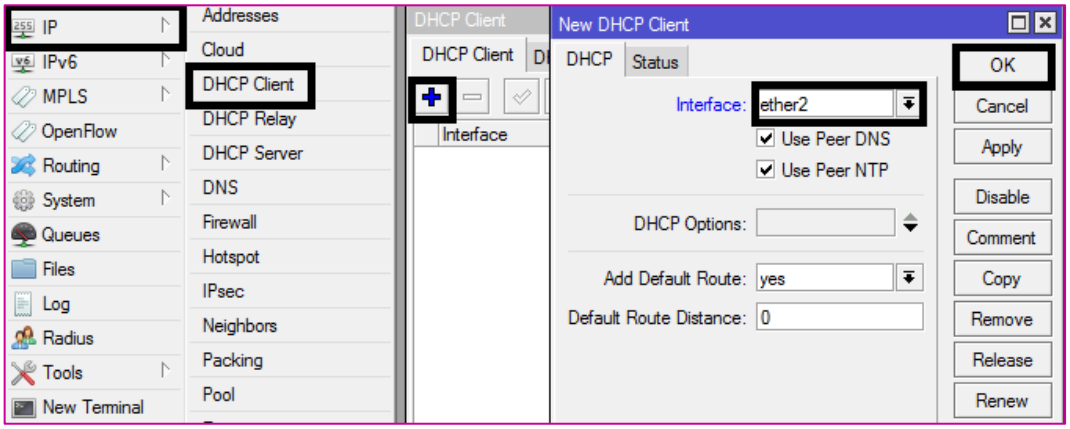
LAB 27 – DHCP Client

Jika kita mengkonfigurasi DHCP client di mikrotik, artinya kita menginginkan agar mikrotik mendapat IP Address secara otomatis dari DHCP server. Biasanya DHCP client ini diaktifkan pada interface mikrotik yang terhubung dengan modem internet.



Gambar 27.1 Topologi DHCP Client

Seperti yang terlihat pada topologi diatas, bahawa kita akan mengkonfigurasi dhcp client pada ether1 mikrotik. Berikut adalah langkah-langkahnya :

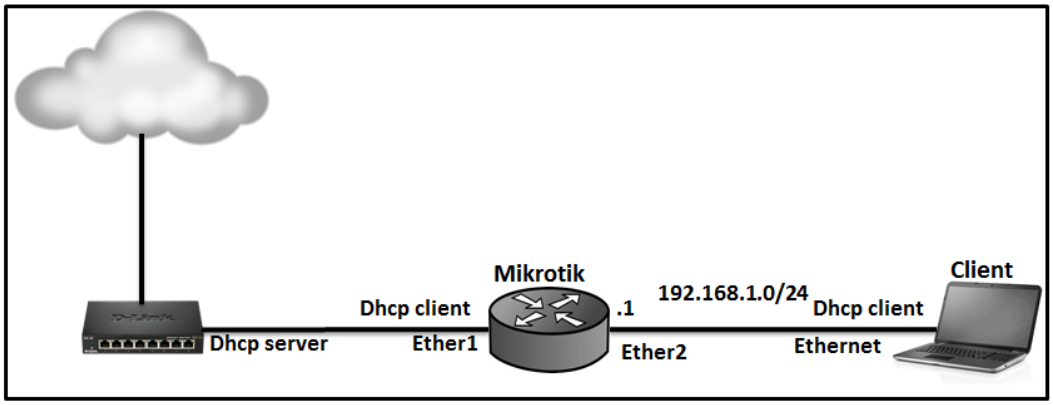


Gambar 27.2 Konfigurasi IP DHCP Client

Untuk pengujian, coba lihat pada menu IP Address, apakah mikrotik sudah mendapatkan IP Address atau belum. Jika sudah nanti kalian akan menemukan tanda **D** di depan IP Address, label ini menunjukkan bahwa IP Address tersebut didapat secara **Dynamic** atau otomatis

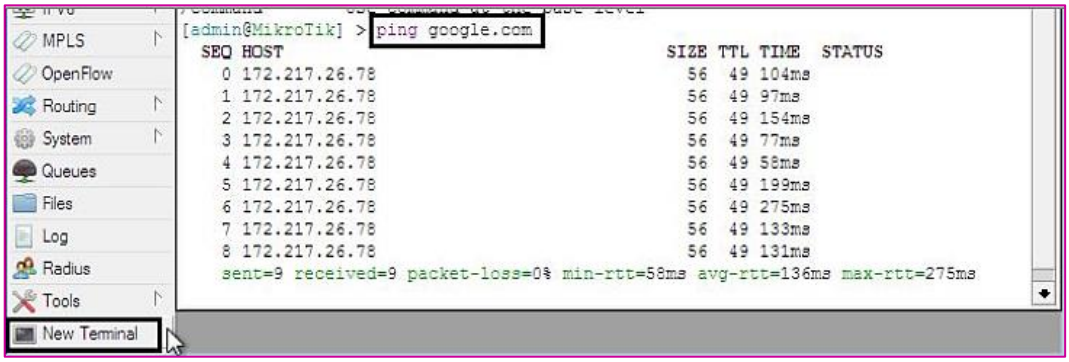
LAB 28 – Router Gateway

Pada lab ini kita akan mengkonfigurasi router gateway pada mikrotik agar komputer client yang terhubung ke mikrotik bisa melakukan akses internet. Berikut adalah topologi yang kita gunakan :



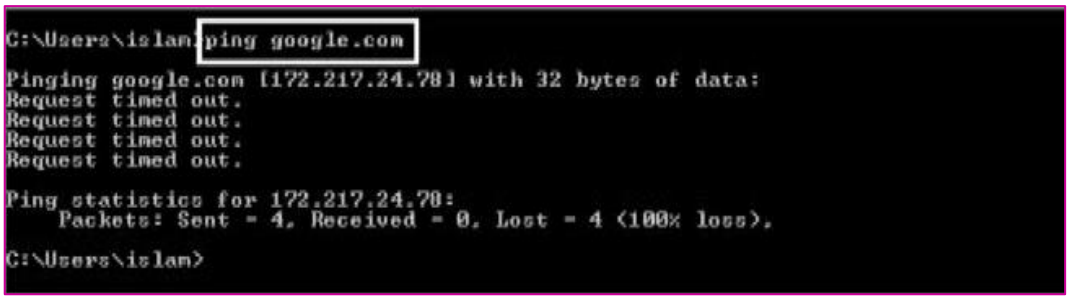
Gambar 28.1 Topologi Router Gateway

Seharusnya setelah kita mengkonfigurasi dhcp client pada lab sebelumnya, maka mikrotik sudah bisa ping ke google seperti terlihat pada gambar berikut :



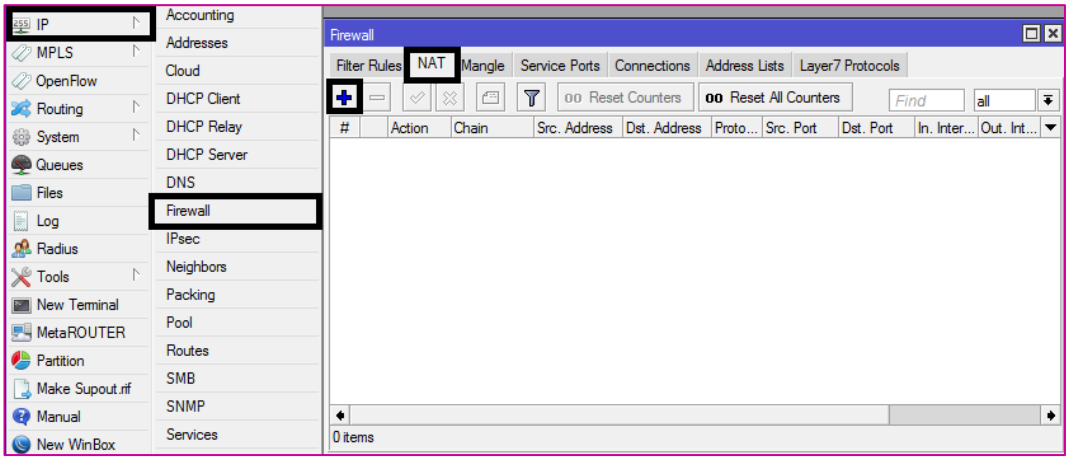
Gambar 28.2 Ping dari Mikrotik ke Internet

Selanjutnya kita coba ping google dari client :

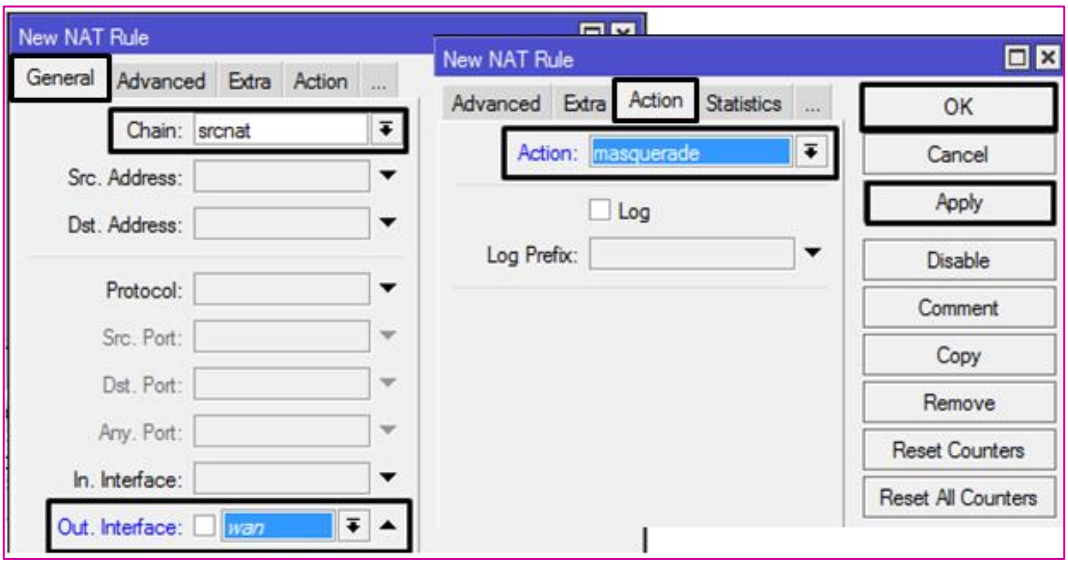


Gambar 28.3 Client Tidak Bisa Ping Ke Google

Perhatikan bahwa sebelum mengkonfigurasi router gateway, client tidak akan bisa ping ke internet. Untuk mengkonfigurasi router gateway, kita harus menambahkan sebuah firewall NAT (Network Address Translation) pada mikrotik supaya dapat merubah field IP Address, baik ip address pengirim maupun ip address tujuan



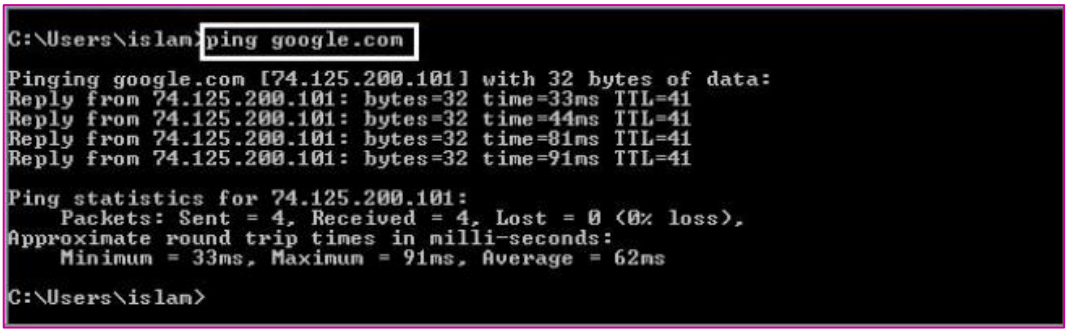
Gambar 28.4 Konfigurasi NAT di Mikrotik



Gambar 28.5 Konfigurasi NAT di Mikrotik

Parameter ***out interface*** pada gambar diatas menunjukkan interface yang terhubung dengan internet (modem). Sedangkan maksud dari ***action masquerade*** akan saya jelaskan pada lab selanjutnya.

Untuk pengujian, coba lakukan ping google dari client



Gambar 28.6 Client Bisa Ping Ke Internet

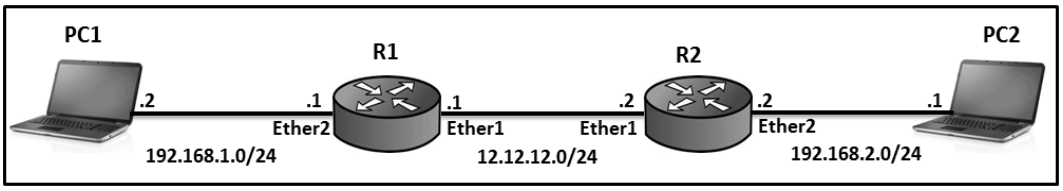
LAB 29 – Static Routing

Routing merupakan sebuah cara yang digunakan untuk menghubungkan dua atau lebih network yang berbeda. Ada dua teknik routing yaitu :

1. Static Routing
2. Dynamic Routing

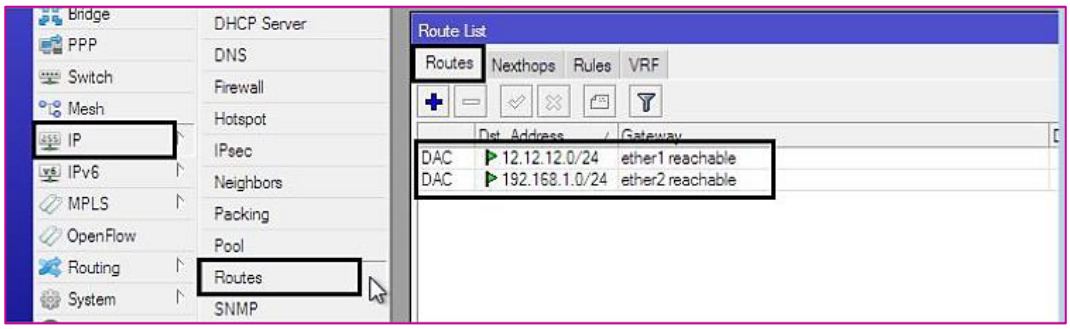
Pada lab ini kita fokus mempelajari static routing

Static Routing adalah metode routing dimana Network Engineer (user) harus mengkonfigurasi routing secara manual (namanya juga static). Berikut adalah topologi yang akan kita gunakan :

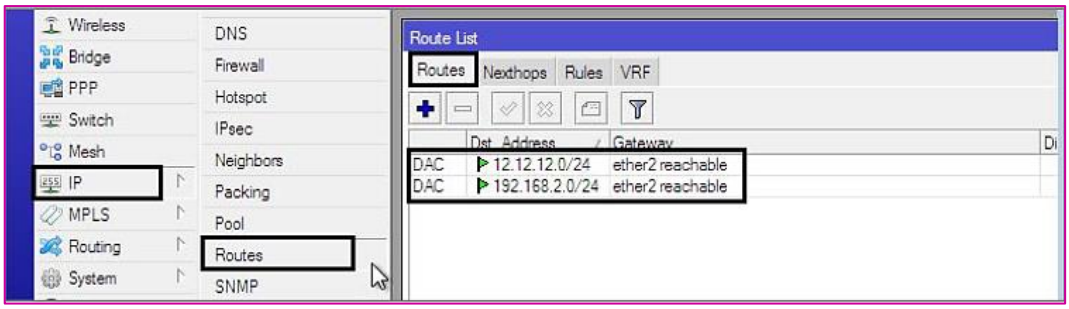


Gambar 29.1 Topologi Static Routing

Diasumsikan kita telah mengkonfigurasi ip address sesuai topologi diatas. Selanjutnya kita coba lihat tabel routing R1 dan R2.



Gambar 29.2 Tabel Routing di R1



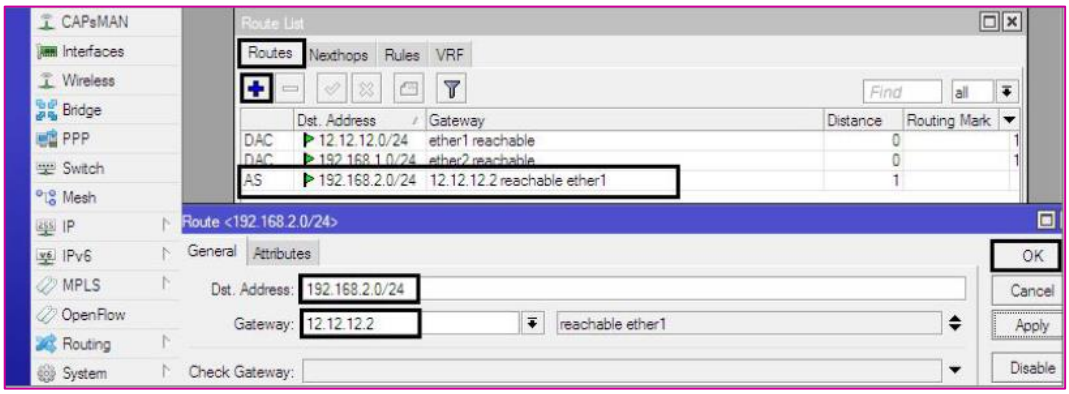
Gambar 29.3 Tabel Routing di R2

Perhatikan bahwa R1 dan R2 hanya memiliki informasi tentang redictly connected network (jaringan yang terhubung langsung) pada tabel routingnya masing-masing. Pada kasus seperi ini, PC1 tidak akan dapat berkomunikasi dengan PC2.

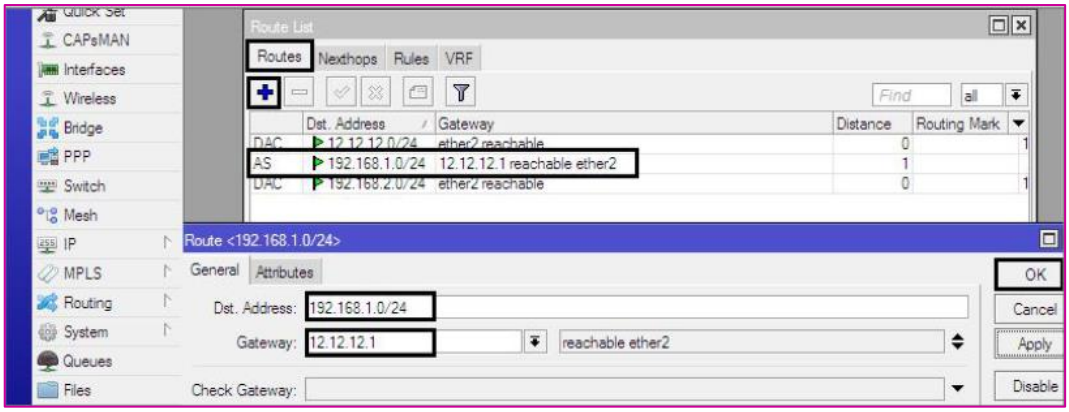
Gambar 29.4 Ping dari PC1 ke PC2

Terlihat bahwa ada kata **Destination not unreachable**

Agar PC1 dan PC2 bisa saling berkomunikasi kita harus mengenalkan network 192.168.1.0/24 ke R2 dan network 192.168.2.0/24 ke R1 (timbal balik). Menggunakan static routing seperti berikut :



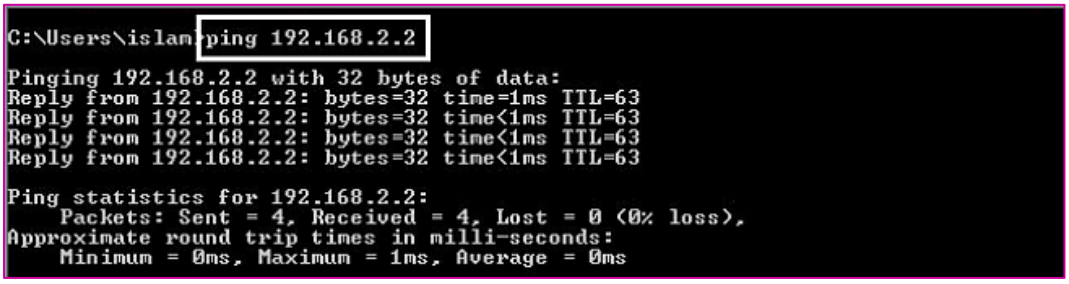
Gambar 29.5 Konfigurasi Static Routing di R1



Gambar 29.6 Konfigurasi Static Routing di R2

Setelah konfigurasi static routing, baik di R1 maupun R2 akan mengenali remote networknya (network yang tidak terhubung langsung) dengan label **AS** (*Active Static*).

Untuk pengujian kita coba lakukan ping dari PC1 ke PC2



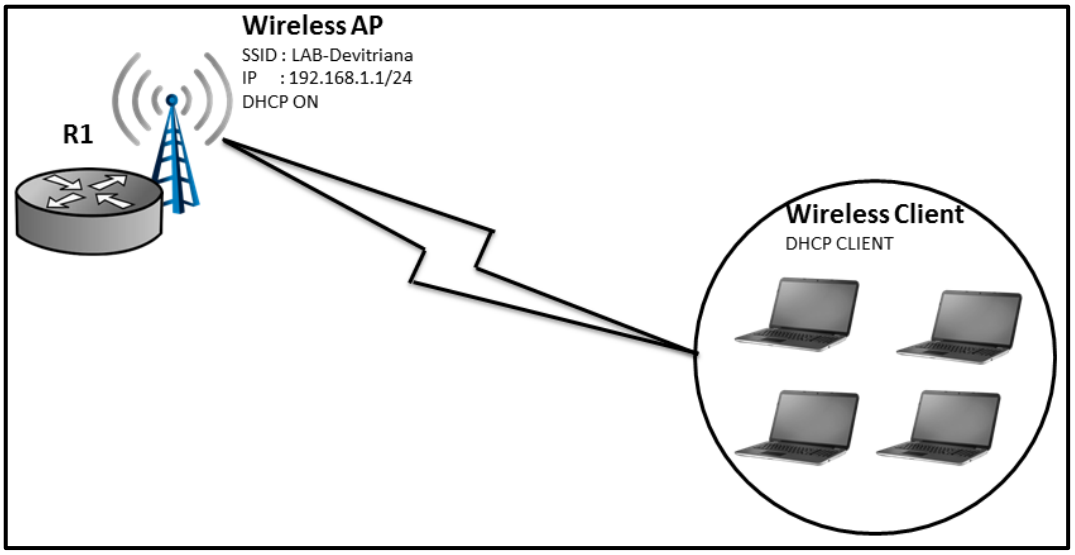
Gambar 29.7 Ping dari PC1 ke PC2

BAB III

Mikrotik Wireless

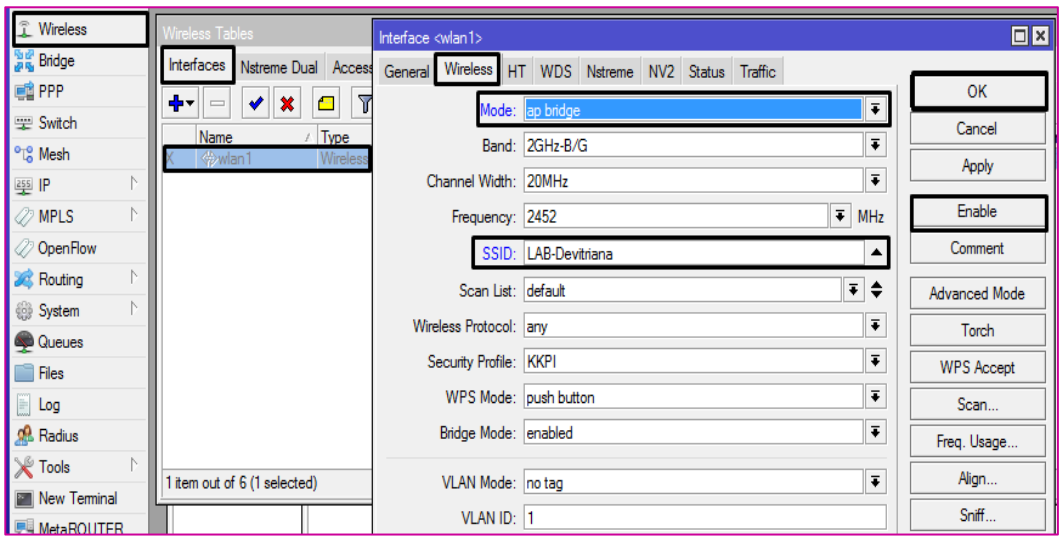
LAB 30 – Wireless AP Bridge

Pada lab ini kita akan melakukan konfigurasi mikrotik untuk menjadi wireless Access Point. Berikut topologi yang akan kita gunakan :



Gambar 30.1 Topologi Wireless AP Bridge

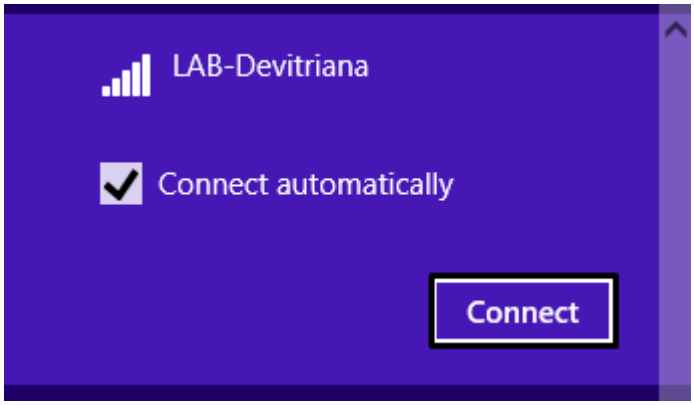
Selain mengkonfigurasi wireless AP, kita juga akan melakukan konfigurasi IP Address dan DHCP Server pada mikrotik. Berikut adalah langkah-langkah yang harus kita lakukan : (klik 2x pada wlan1)



Gambar 30.2 Konfigurasi Wireless AP

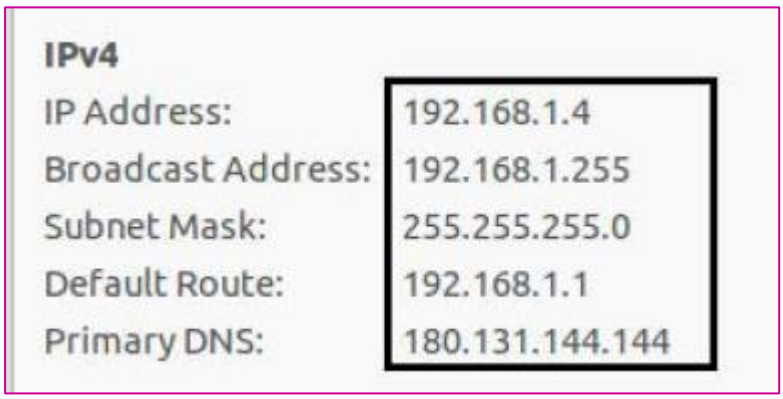
Perhatikan gambar diatas, bahwa *mode* yang digunakan adalah *AP Bridge*. Mode ini digunakan jika kita ingin agar wireless mikrotik menjadi **pemancar** dan sejumlah client lebih dari 1.

Selanjutnya untuk mengkonfigurasi IP Address silahkan mengacu pada Lab 22, sedangkan untuk mengkonfigurasikan DHCP Server silahkan mengacu pada Lab 23. Untuk pengujian, konfigurasi ip client agar connect ke wireless AP yang baru saja kita setting.



Gambar 30.2 Konfigurasi Wireless Client

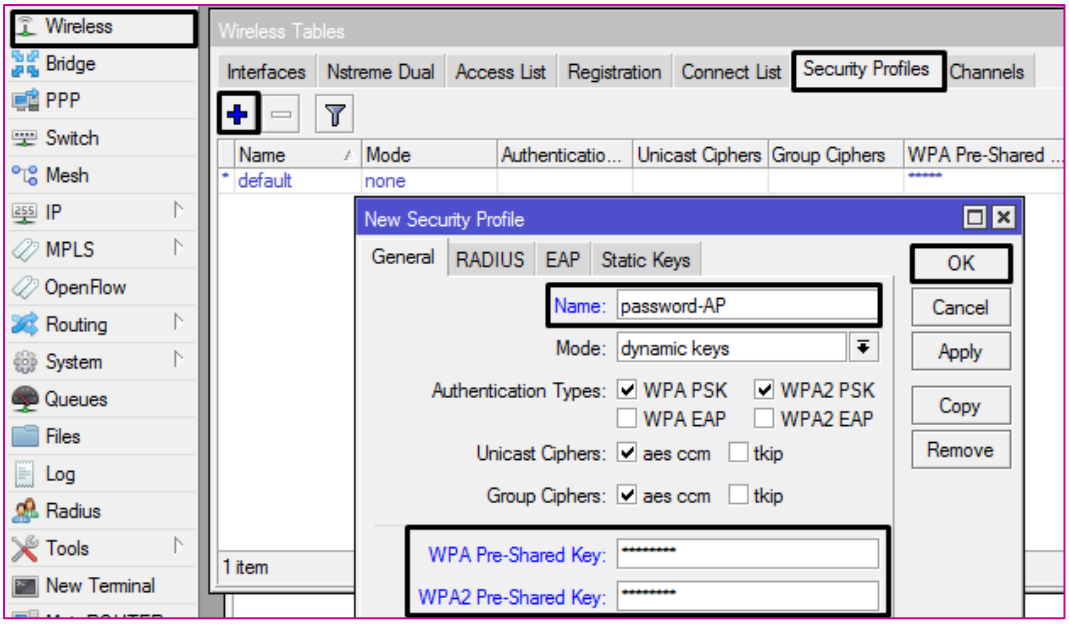
Pastikan client mendapat IP dhcp dari mikrotik melalui wireless :



Gambar 30.3 Status Koneksi Client

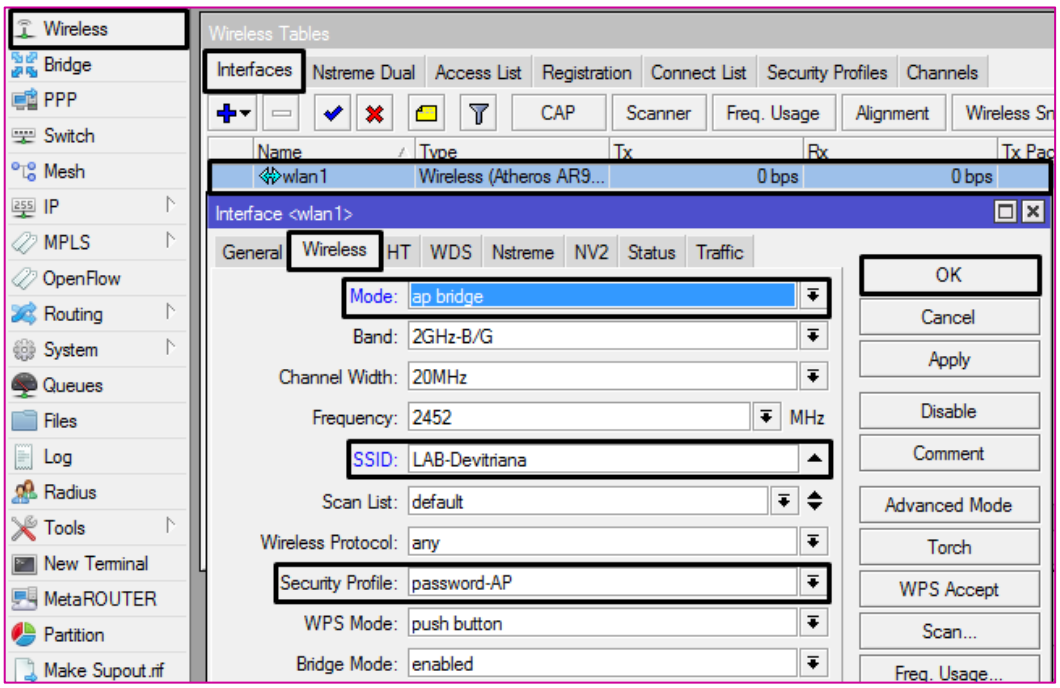
LAB 31 – Security Profile

Lab ini merupakan kelanjutan dari lab sebelumnya. Tujuan lab ini adalah agar wireless AP yang kita konfigurasikan sebelumnya dilengkapi fitur authentifikasi, sehingga akan lebih aman. Hal pertama yang kita harus lakukan adalah membuat security profile.



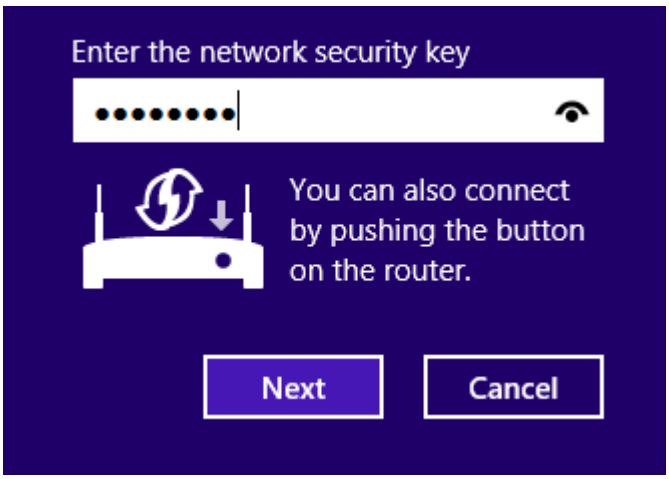
Gambar 31.1 Membuat Security Profile

Langkah selanjutnya adalah mengkonfigurasi wireless AP, agar dapat menggunakan security profile yang baru saja kita buat.



Gambar 31.2 Menambahkan Security Profile

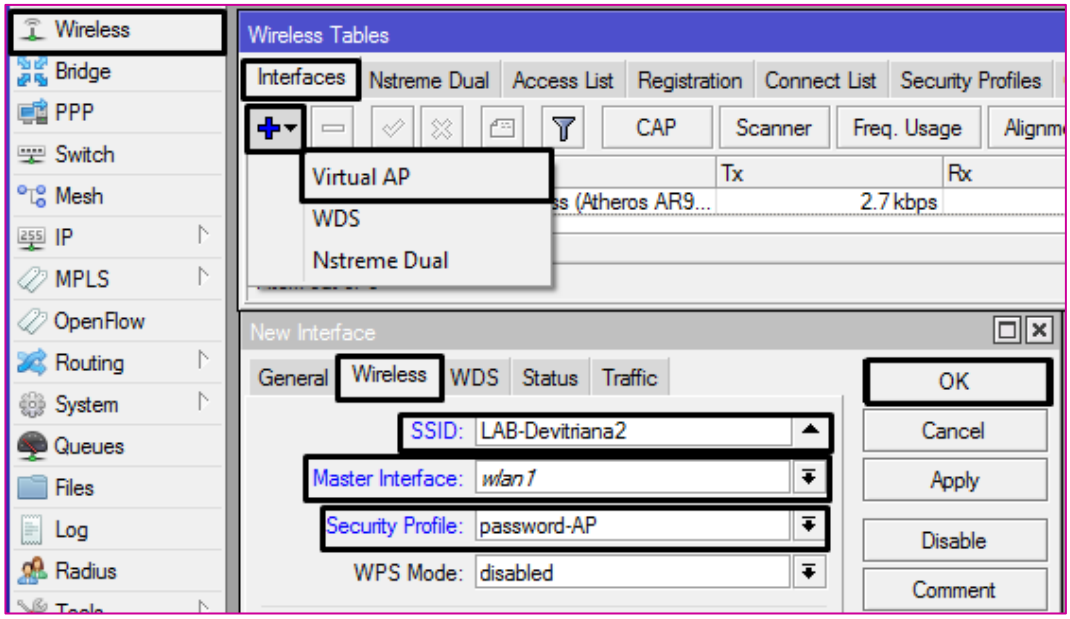
Setelah konfigurasi security profile seperti diatas, maka saat client ingin connect ke LAB-Devitriana akan diminta untuk memasukkan password authentifikasi seperti berikut :



Gambar 31.3 Authentikasi Wireless Client

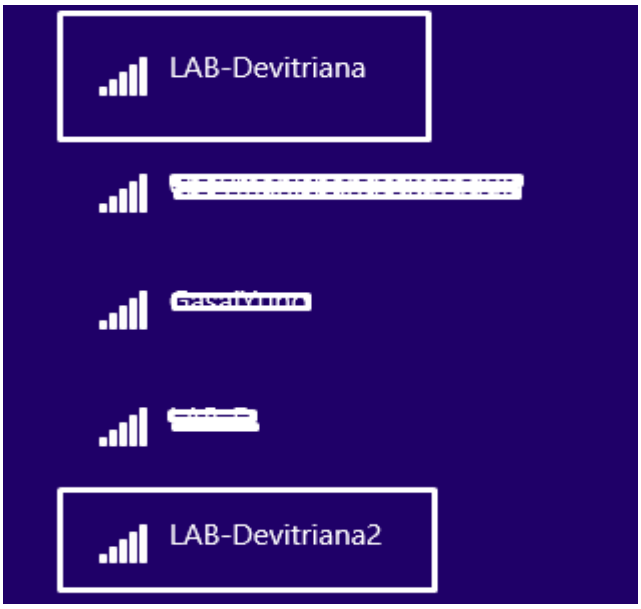
LAB 32 – Virtual Access Point

Kita bisa memiliki dua wireless AP dengan SSID yang berbeda hanya dengan menggunakan sebuah perangkat mikrotik. Fitur yang dapat kita manfaatkan untuk hal ini adalah Virtual Access Point. Berikut langkah-langkah yang dapat kita digunakan untuk menambahkan virtual AP.



Gambar 32.1 Konfigurasi Virtual AP

Untuk konfigurasi virtual AP, kita bisa mneggunakan SSID dan security profile sesuka hati. Sedangkan untuk master interface kita harus mengarahkan ke interface wireless *real* (nyata) yang dimiliki oleh mikrotik.



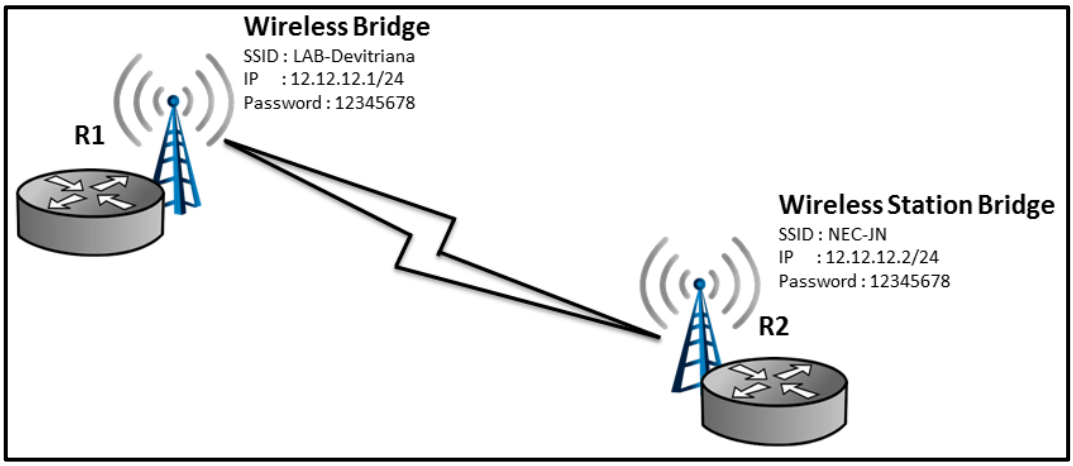
Gambar 32.2 Wireless Virtual AP

Perhatikan bahwa saat ini kita bisa mendeteksi ada 2 SSID yaitu LAB-Devitriana dan LAB-Devitriana2. Kedua wireless tersebut dibuat pada 1 perangkat mikrotik.

LAB 33 – Wireless Bridge

Pada lab sebelumnya kita telah belajar satu mode yang dapat digunakan pada wireless mikrotik. Yaitu **AP Bridge**, dimana mode ini digunakan saat kita menginginkan agar wireless mikrotik menjadi **pemancar dan jumlah client lebih dari satu**.

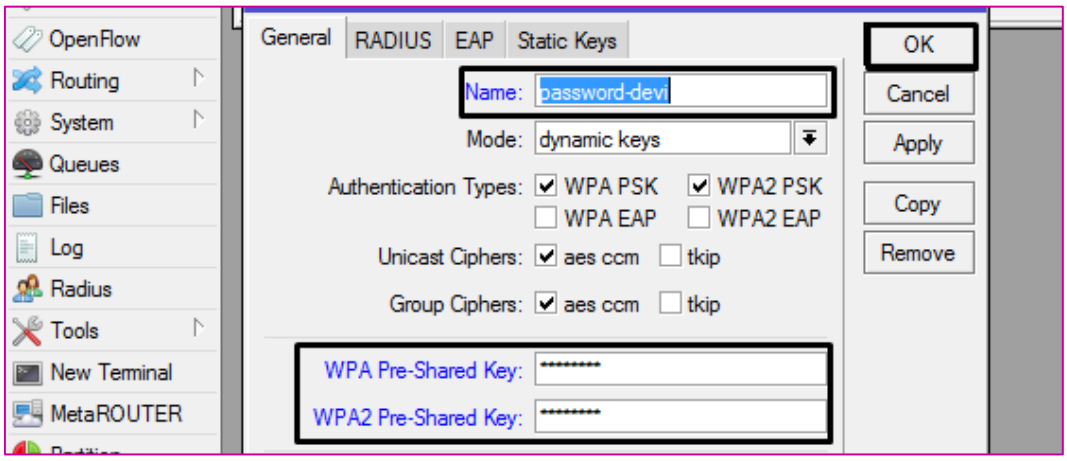
Selanjutnya pada lab ini kita akan belajar mode **Bridge**, dimana mode ini kita gunakan saat kita menginginkan agar wireless mikrotik menjadi **pemancar dan jumlah client hanya 1.** Bisa disebut juga bahwa mode ini kita gunakan untuk membangun jaringan **Point To Point**. Berikut adalah topologi yang akan kita gunakan.



Gambar 33.1 Topologi Point to Point

Pada lab ini kita hanya fokus pada konfigurasi di R1. Konfigurasi R2 akan kita bahas di lab selanjutnya.

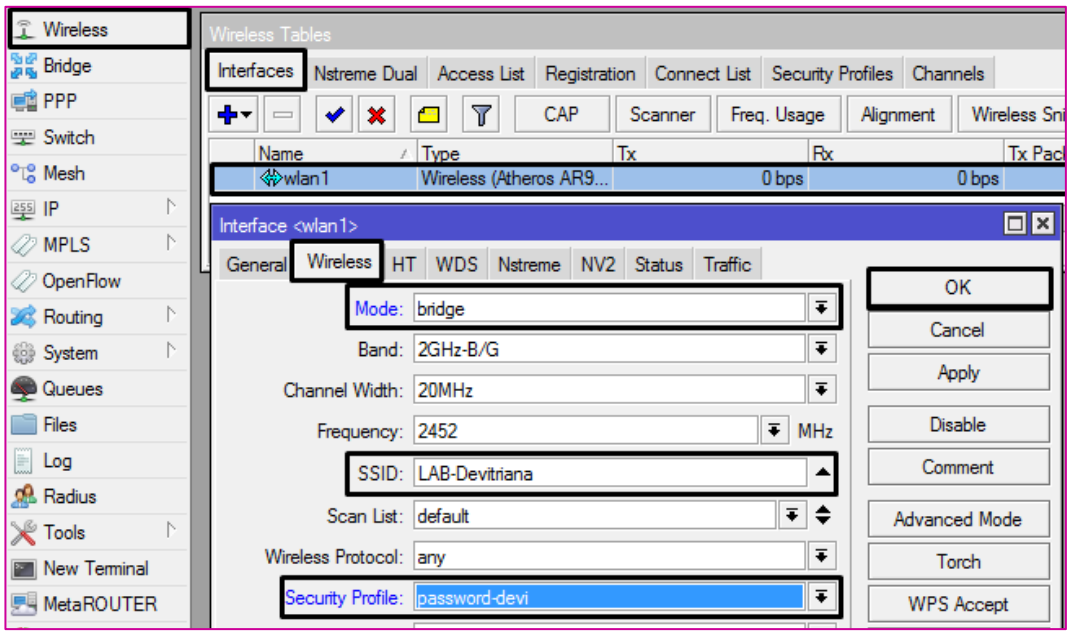
Sebelum melakukan konfigurasi bridge, silahkan buat securuty profile terlebih dahulu (untuk cara pembuatan security profile silahkan mengacu pada Lab 31.



Gambar 33.2 Membuat Security Profile untuk Bridge

Selanjutnya konfigurasikan IP Address pada interface wireless sesuai topologi gambar 33.1 diatas.

Adapun konfigurasi yang perlu dilakukan pada R1 adalah sebagai berikut :



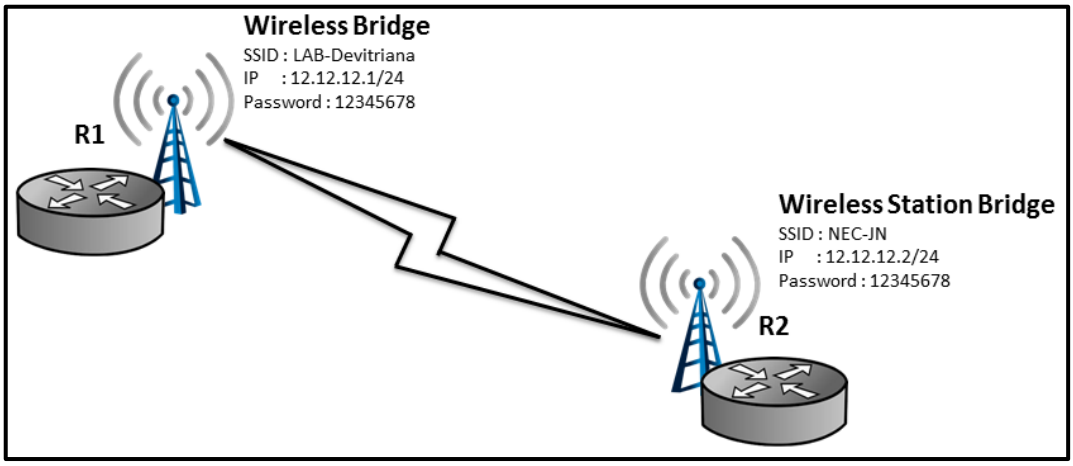
Gambar 33.2 Membuat Security Profile untuk Bridge

LAB 34 – Wireless Station Bridge

Sebelumnya kita telah belajar dua mode wireless pada mikrotik yang berfungsi untuk memancarkan, yaitu **AP Bridge dan Bridge**. Selanjutnya pada lab ini kita akan memperlajari mode wireless pada mikrotik yang berfungsi sebagai penerima.

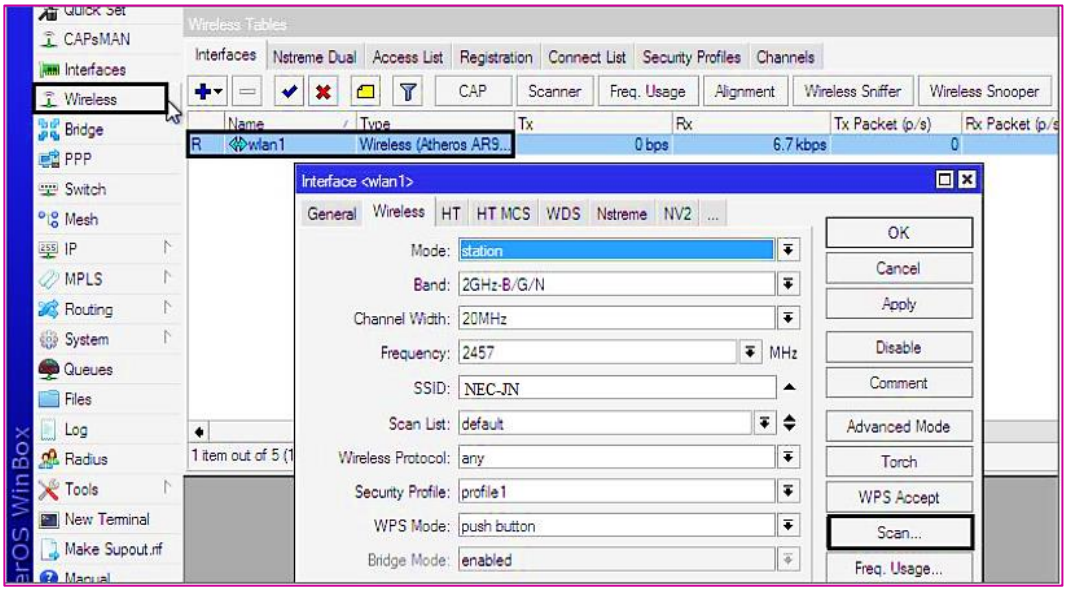
Ada beberapa mode wireless pada mikrotik yang dapat berfungsi sebagai **penerima**, seperti **Station, Station Bridge, Station Pseudobridge, Station Pseudobridge Clone,dll**. Namun pada lab ini kita hanya **fokus pada mode Station Bridge.**

Mode station bridge kita gunakan saat yang jadi pemancar **juga berasal dari mikrotik.** Perhatikan topologi berikut :



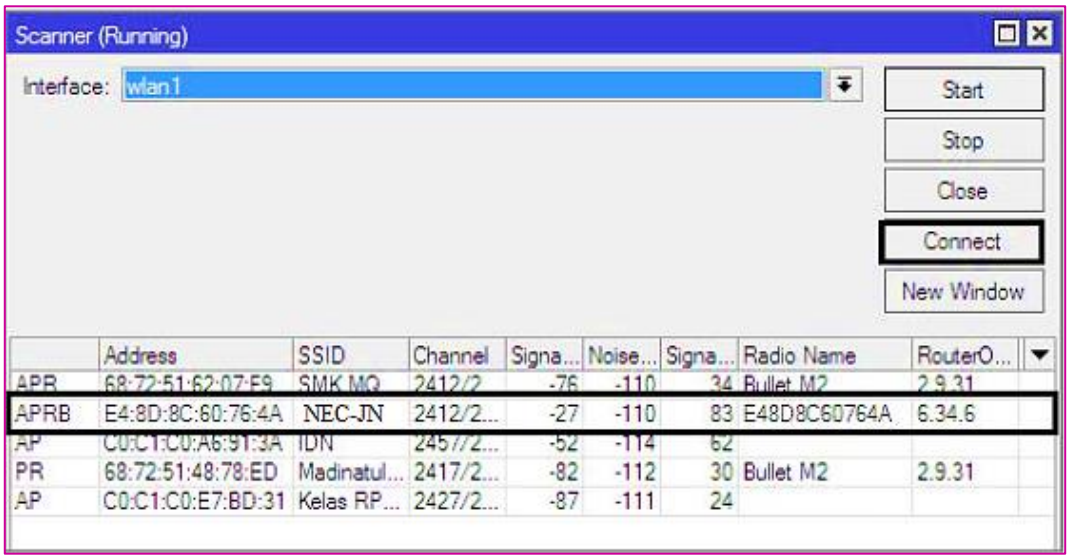
Gambar 34.1 Topologi Wireless Station Bridge

Pada gambar diatas, kita bisa tahu bahwa yang jadi pemancar (R1) adalah router mikrotik. Sehingga pada R2 kita bisa menggunakan mode station bridge.adapun langkah-langkah yang harus kita lakukan adalah :



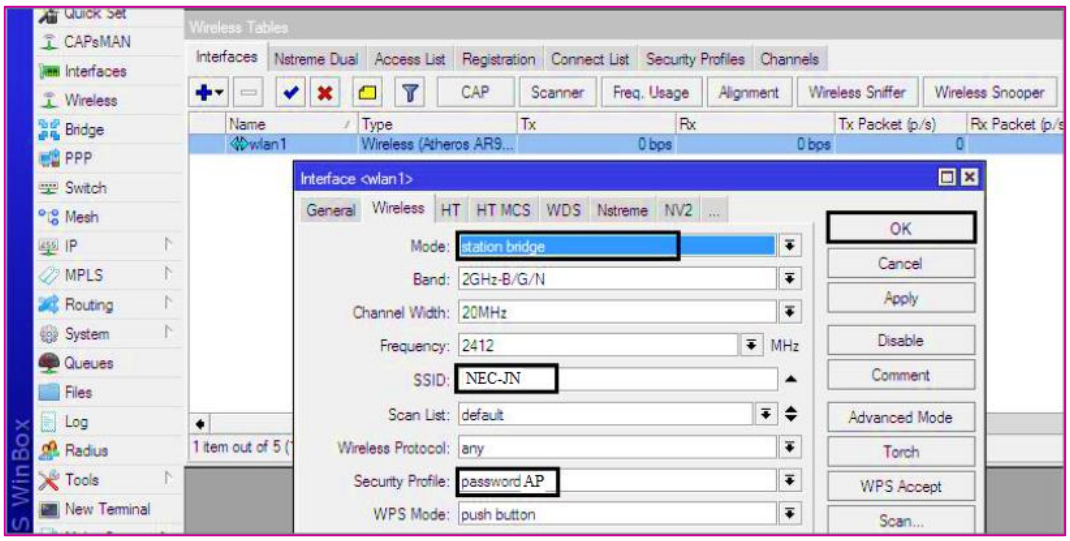
Gambar 34.2 Konfigurasi Wireless Station Bridge

Pada langkah diatas, kita tidak perlu memperdulikan parameter mode terlebih dahulu, kita hanya perlu memilih menu *Scan* untuk mencari pemancar apa saja yang berada disekitar kita.



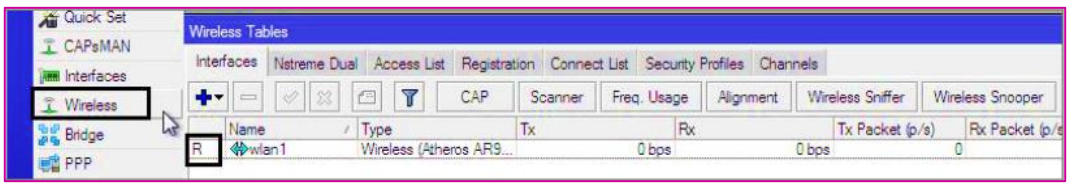
Gambar 34.3 Konfigurasi Wireless Station Bridge

Sesaat setelah kita klik connect seperti diatas, maka Mode dan SSID akan terisi secara otomatis, kita hanya perlu melakukan penyesuaian pada security profile. Sebagai catatan bahwa sebelum melakukan langkah ini, kita sudah harus membuat security profile terlebih dahulu.



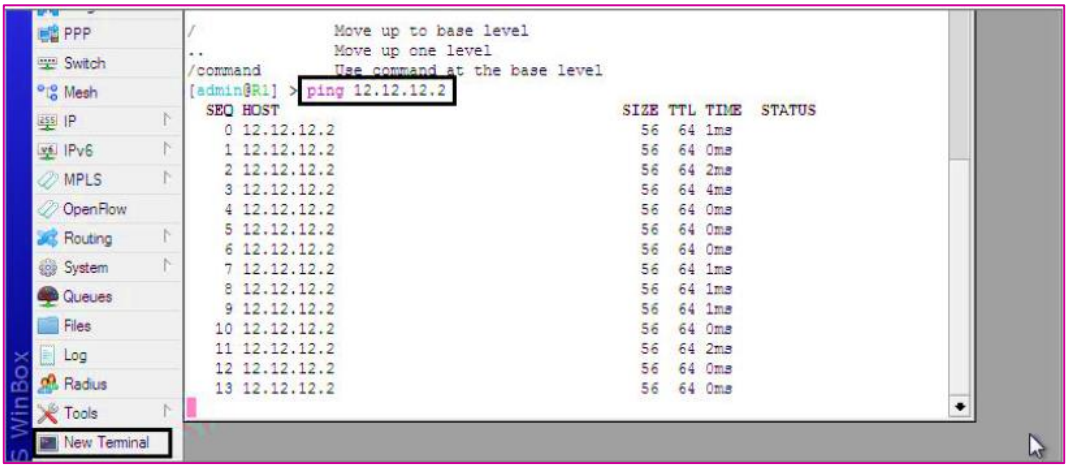
Gambar 34.4 Konfigurasi Wireless Station Bridge

Jika antara pemancar dan penerima sudah connect, maka baik pemancar ataupun penerima akan muncul label *R* dimenu interface yang artinya Running.



Gambar 34.5 Status Running

Setelah dipastikan antara pemancar dan penerima connect, selanjutnya konfigurasikan IP Address sesuai topologi gambar 33.1 diatas. Berikut penguijan ping dari R1 ke R2.

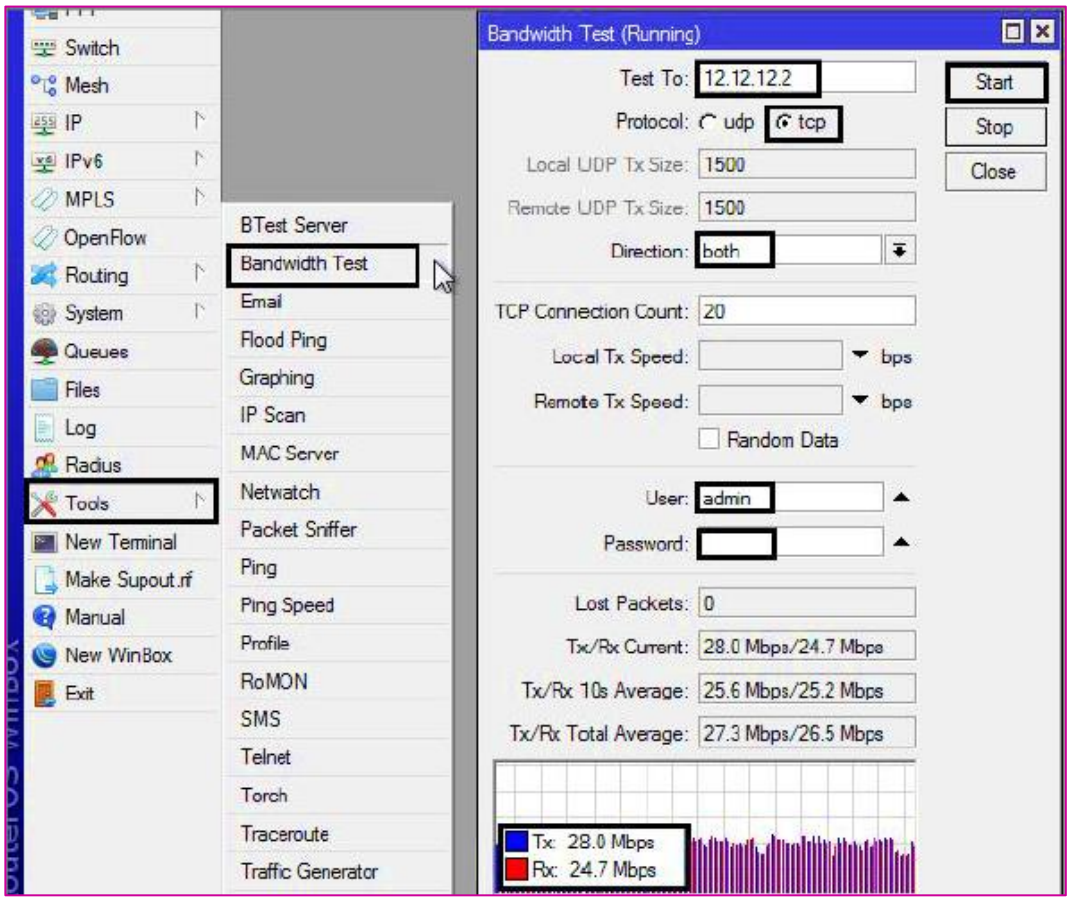


Gambar 34.6 Pengujian Ping dari PC1 ke PC2

LAB 35 – Wireless Nstreme

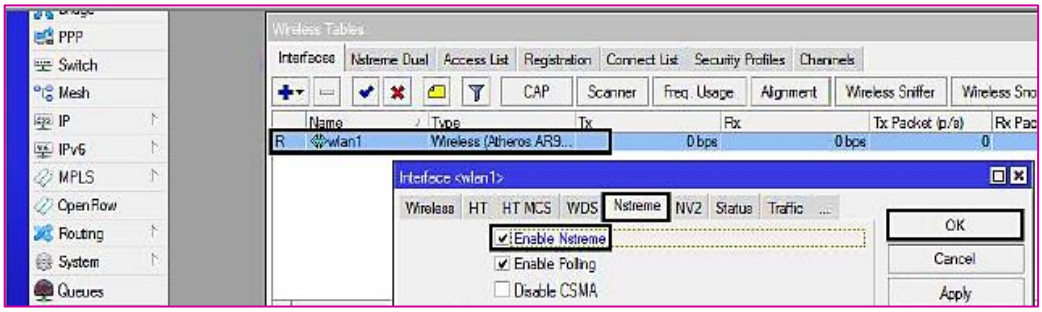
Wireless Nstreme merupakan fitur pada mikrotik yang digunakan untuk keperluan optimalisasi link wireless. Fitur ini hanya bisa digunakan **jika pemeancar dan penerima merupakan mikrotik.**

Lab ini akan mengacu pada Lab 33 dan 34 yang telah dibahas sebelumnya. Pada kedua lab tersebut kita telah mengkonfigurasi link point to point. Menggunakan 2 perangkat mikrotik. Jika kita tidak mengaktifkan fitur Nstreme, maka bandwidth pada link tersebut tidak akan maksimal. Perhatikan bandwidth test dari R1 ke R2 berikut :

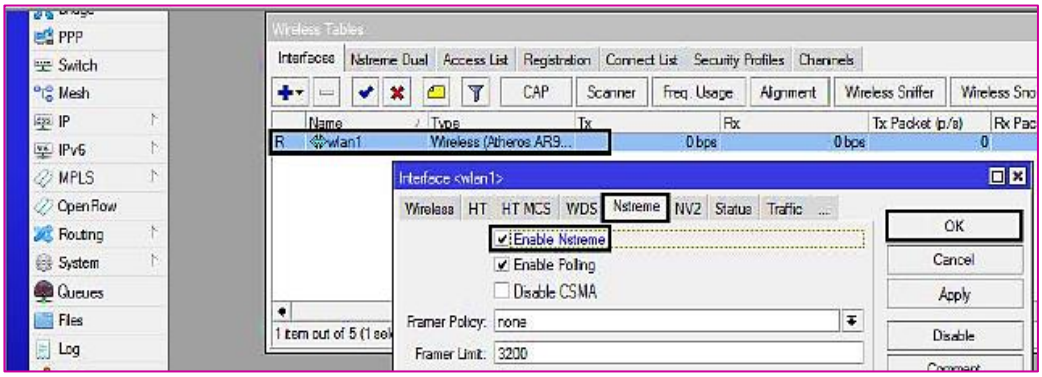


Gambar 35.1 Bandwidth Link tanpa Nstreme

Selanjutnya kita coba aktifkan fitur nstreme pada R1 dan R2 untuk memaksimalkan bandwidth pada link ini.

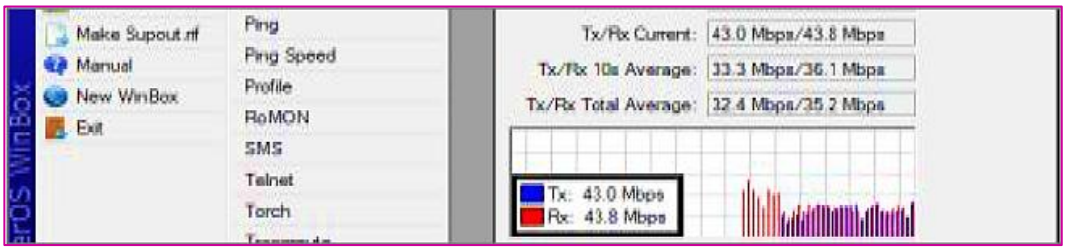


Gambar 35.2 Konfigurasi Nstreme di R1



Gambar 35.3 Konfigurasi Nstreme di R2

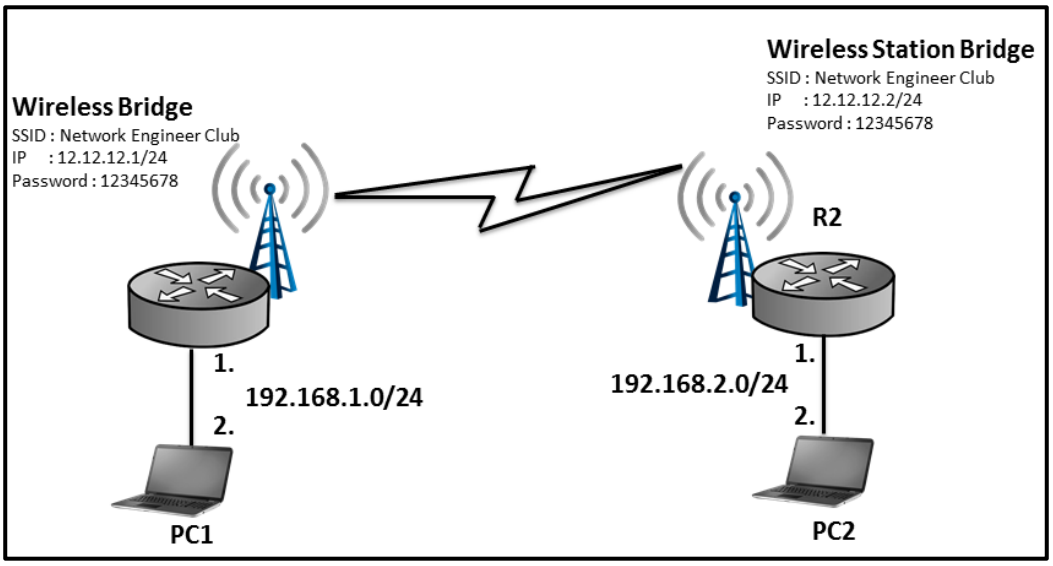
Setelah mengaktifkan nstreme pada kedua router, coba lakukan bandwidth test kembali, jika sukses hasilnya akan seperti dibawah ini :



Gambar 35.4 Bandwidth Link menggunakan Nstreme

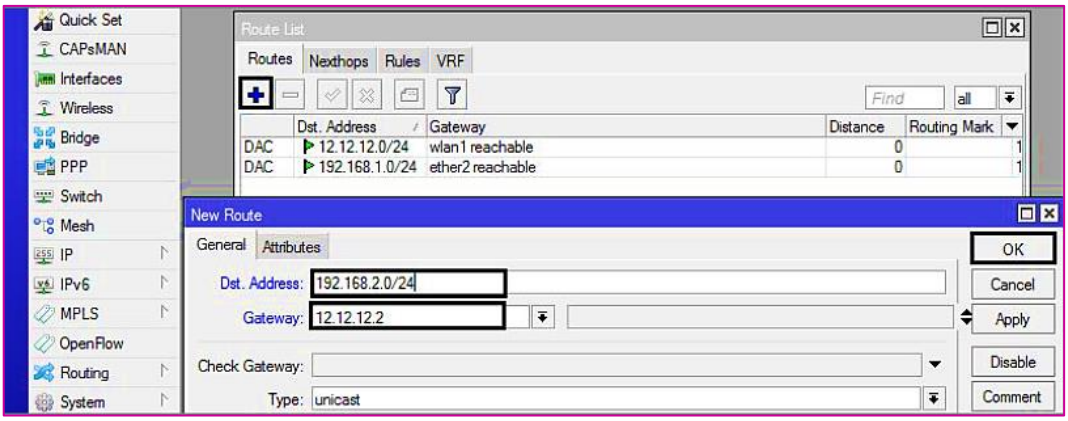
LAB 36 – Static Routing Wireless

Sebelumnya kita telah belajar routing static pada LAB 28. Selanjtnya pada lab ini kita akan mengkombinasikan routig static dengan materi wireless yang telah kita bahas pada LAB 34 dan 35.



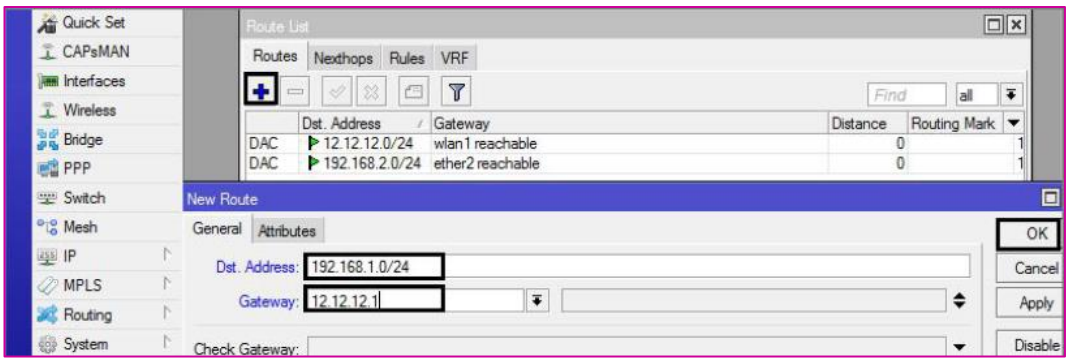
Gambar 36.1 Topologi Wireless Point to Point

Berikut konfigurasi pada R1 yang harus kita lakukan



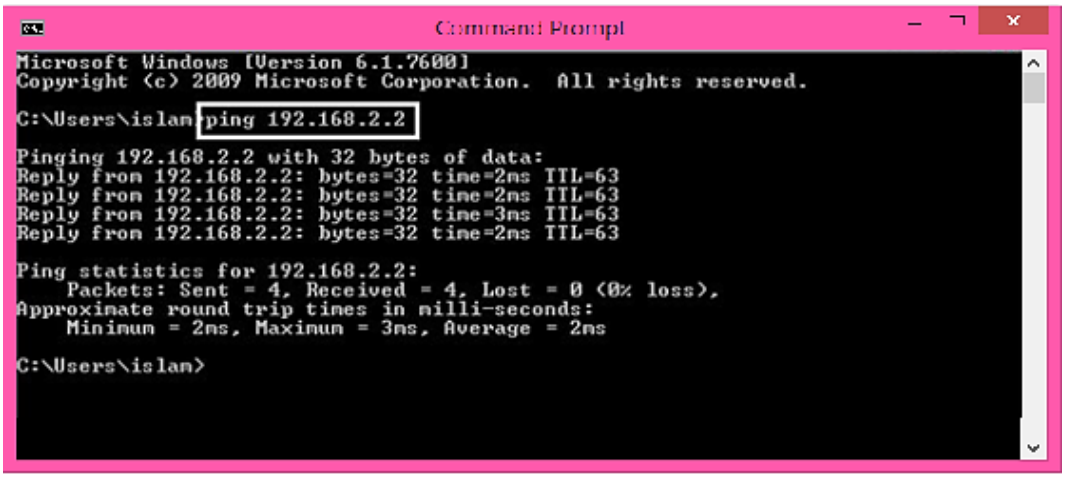
Gambar 36.2 Konfigurasi Static Routing di R1

Adapun konfigurasi R2 yang harus kita lakukan



Gambar 36.3 Konfigurasi Static Route di R2

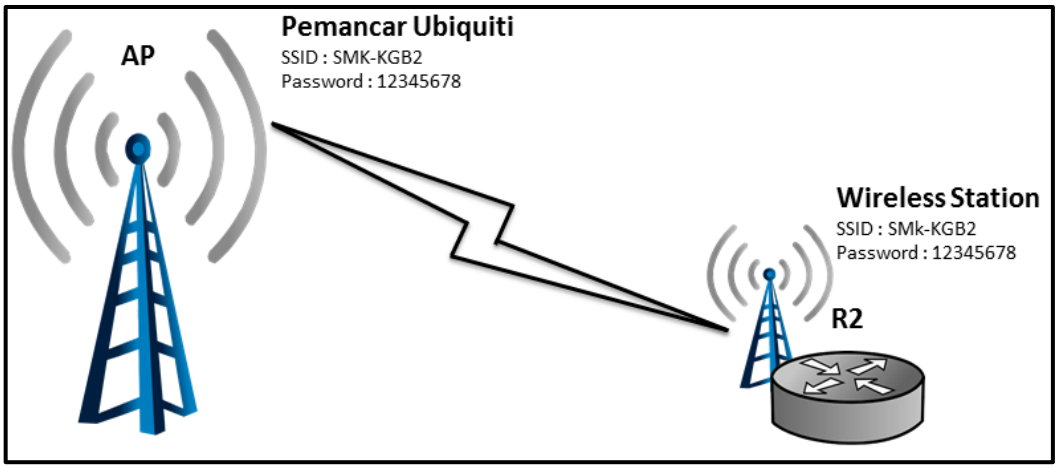
Untuk pengujian, lakukan ping dari PC1 ke PC2



Gambar 36.4 Pengujian Ping dari PC1 ke PC2

LAB 37 – Wireless Station

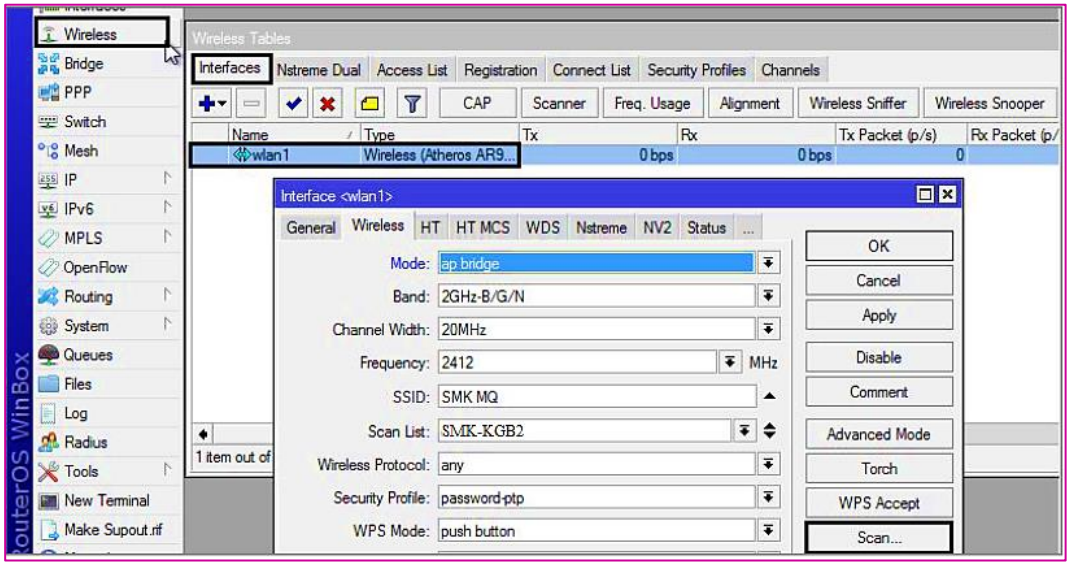
Sebelumnya pada Lab 34 kita telah membahas tentang mode Station Bridge yang digunakan saat mikrotik menjadi penerima dari pemancar yang juga mikrotik. Selanjutnya pada lab ini kita akan membahas tentang mode **Station**. Mode ini digunkan saat mikrotik menjadi penerima dari pemancar yang bukan mikrotik, misalnya Ubiquiti, atatu pemancar dari vendor lain.



Gambar 37.1 Topologi Wireless Station

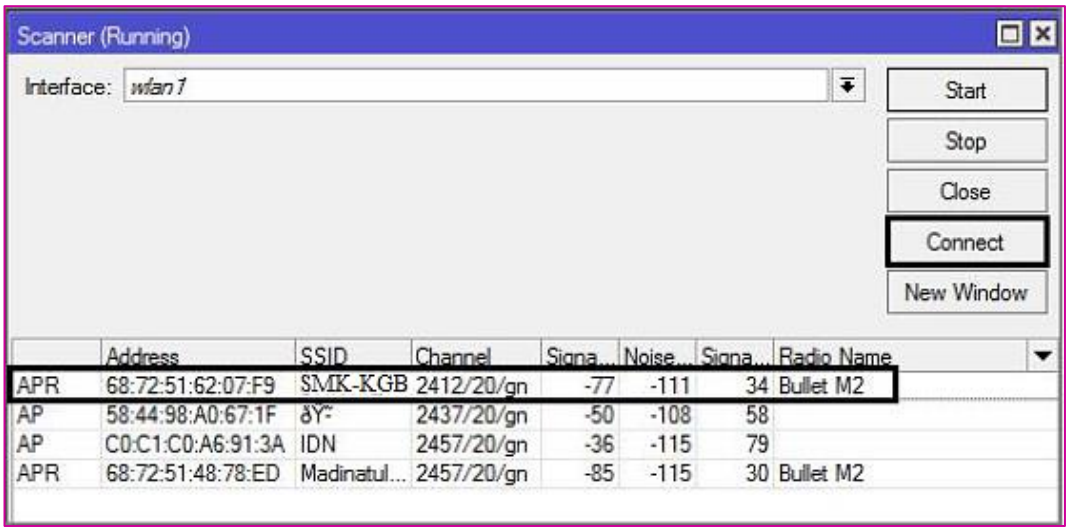
Pada contoh topologi diatas, kita harus mengkonfigurasi R2. Menggunakan mode station. **Kita tidak akan bisa menggunakan mode station bridge**, hal ini dikarenakan pemancar yang kita miliki adalah berasal dari vendor selain mikrotik.

Berikut konfigurasi yang perlu kita lakukan pada R2

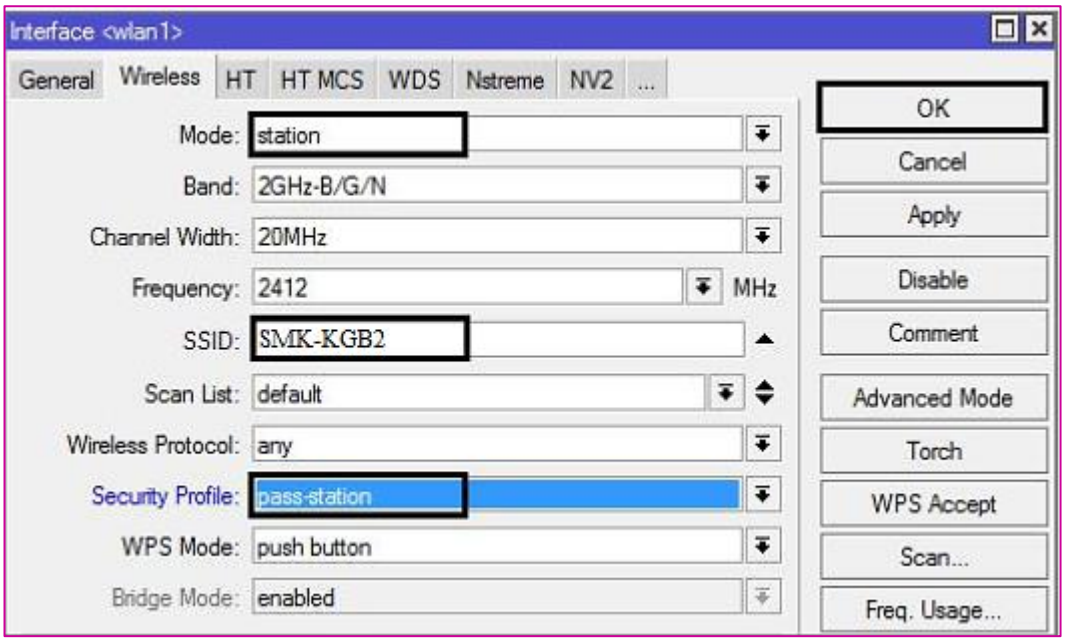


Gambar 37.2 Scanning Wireless

Pada tahap diatas kita hanya perlu melakukan *Scan*. Kita tidak perlu memperdulikan mode atau parameter yang lain.

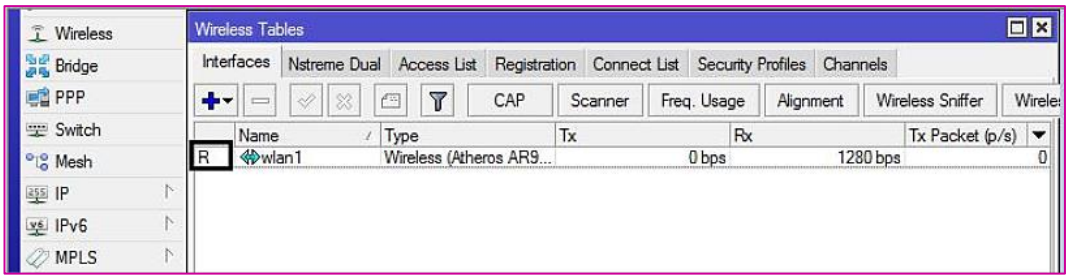


Gambar 37.3 Connect ke Pemancar Bullet



Gambar 37.4 Konfigurasi Wireless Station

Perhatikan gambar bahwa mode dan SSID akan berubah secara otomatis setelah kita connect ke pemancar. Kita hanya perlu menyesuaikan pada bagian security profile saja. Jika R2 sudah connect ke pemancar, maka akan ada label *R* seperti berikut :

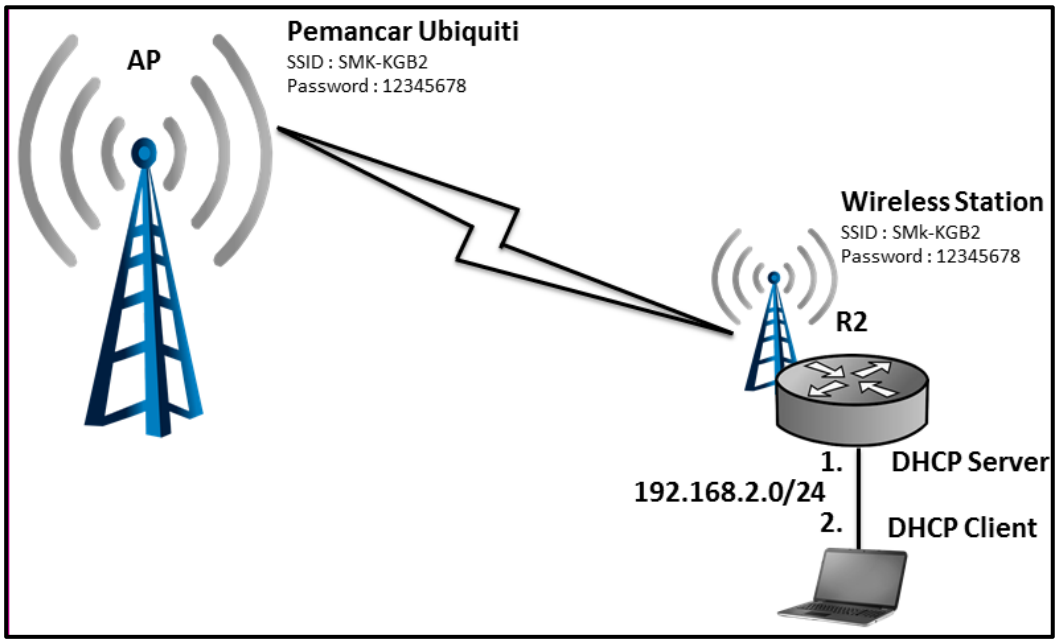


Gambar 37.5 Hasil Konfigurasi Wireless Station

Selain dengan cara diatas, kita juga bisa melihat pada bagian registration list pada menu wireless untuk verifikasi.

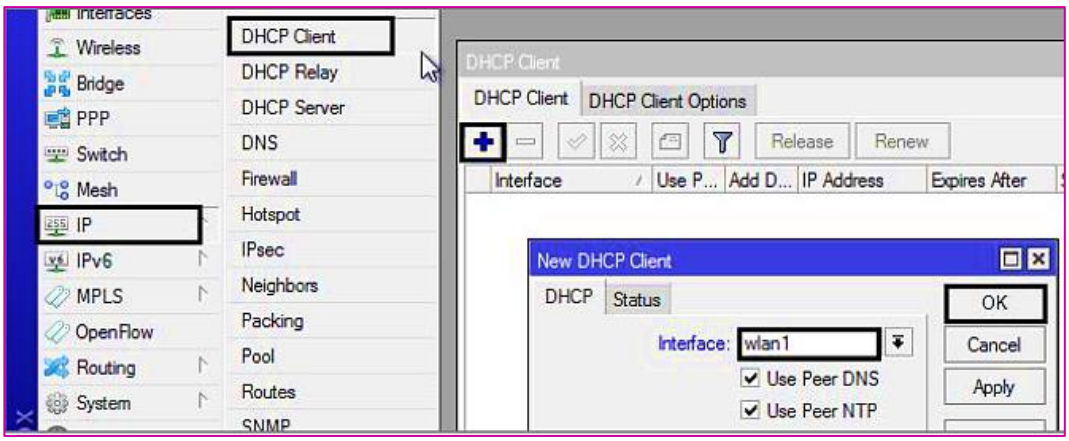
LAB 38 – Router Gateway Wireless

Sebelumnya kita telah membahas materi tentang router gateway pada Lab 27 yaitu memperoleh sumber internet dari wireless. Sedangkan pada Lab ini mendapat sumber internetnya dari modem (kabel ethernet). Berikut adalah topologi yang akan kita gunakan :



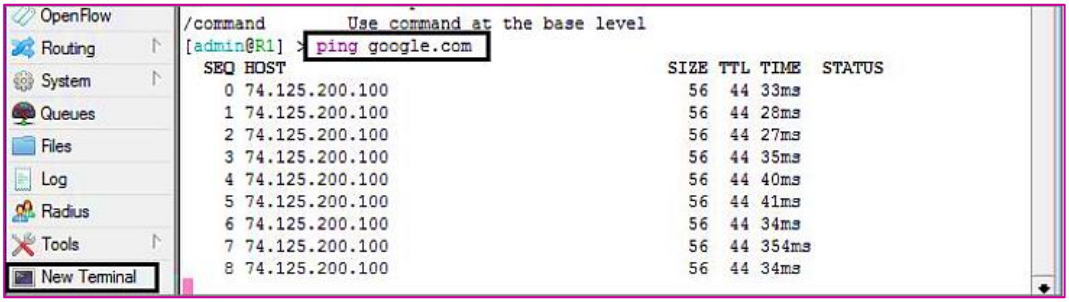
Gambar 38.1 Topologi Router Gateway Wireless

Diasumsikan kita telah connect ke pemancar internet menggunakan mode station (lihat Lab 37). Selanjutnya kita harus mengkonfigurasi DHCP client pada mikrotik.



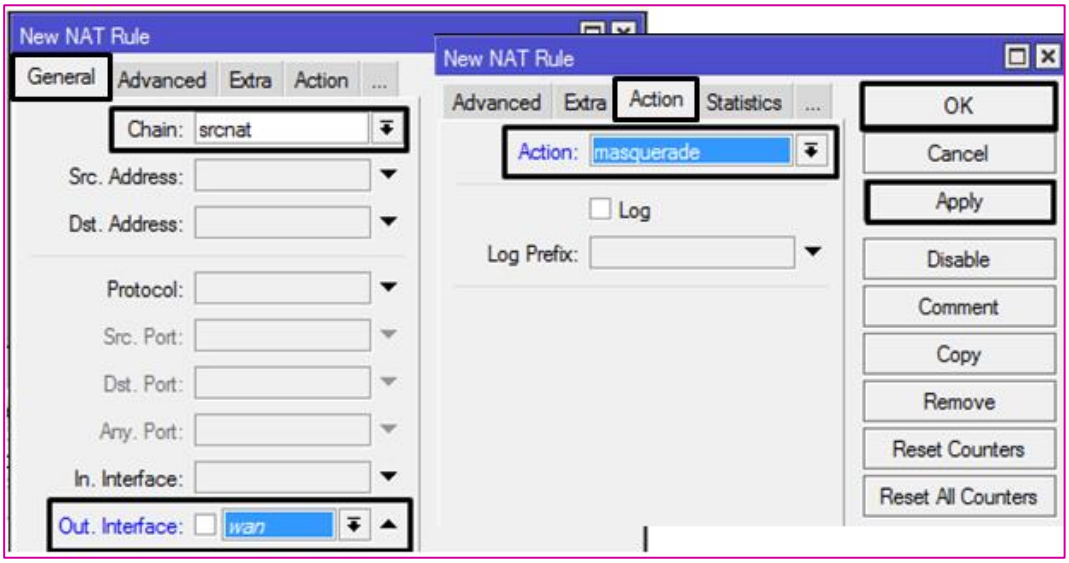
Gambar 38.2 Konfigurasi DHCP Client

Setelah mengkonfigurasi DHCP client, seharusnya mikrotik sudah bisa ping ke ke internet.



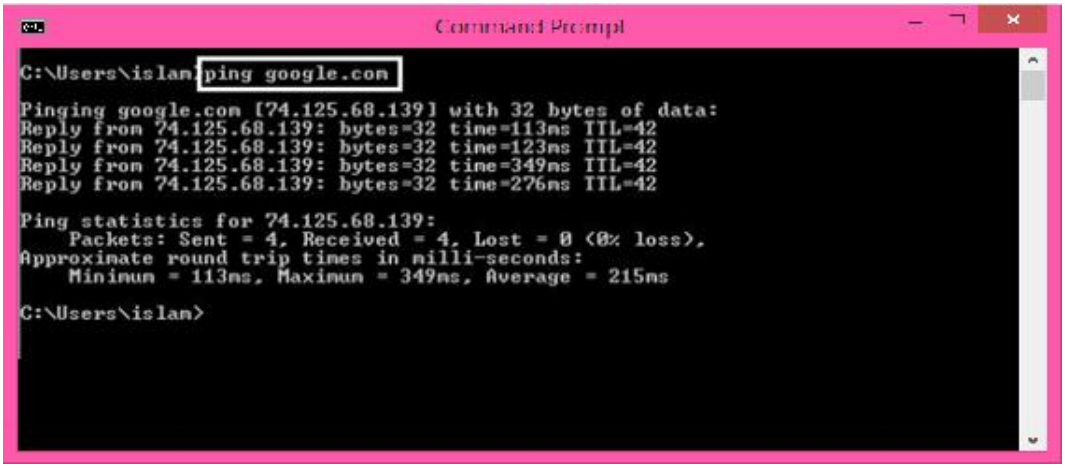
Gambar 38.3 Ping ke Internet

Langkahnya selanjutnya yang harus kita lakukan adalah mengaktifkan dhcp server pada interface yang terhubung ke client. Untuk mengkonfigurasi dhcp server, silahkan baca kembali LAB 24. Langkah terkahir adalah menambahkan firewall NAT agar client bisa internet.



Gambar 38.4 Konfigurasi Firewall NAT

Untuk pengujian, lakukan ping ke internet dari client

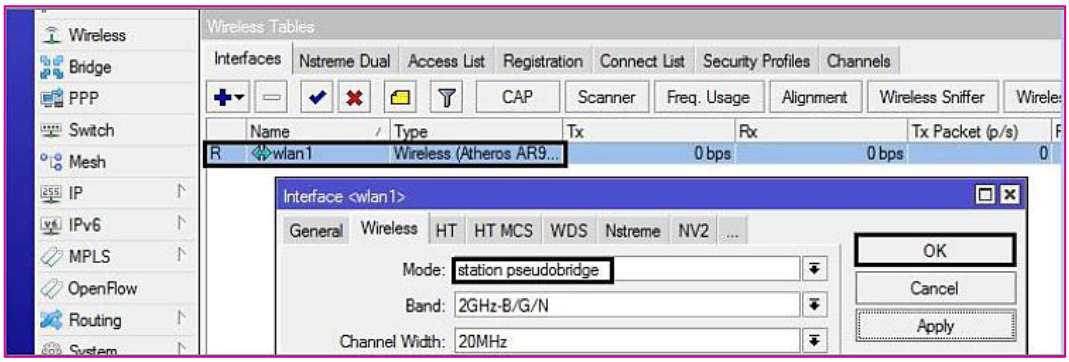


Gambar 38.5 Ping dari Client ke Internet

LAB 39 – Wireless Station Pseudobridge

Pada lab sebelumnya kita telah belajar tentang mode station pada mikrotik. Selanjutnya pada lab ini kita akan belajar tentang **mode station pseudobridge**. **Perbedaannya adalah**, jika mode station tidak akan bisa dibridge, sedangkan mode station pseudobridge bisa dibridge. Bridge disini berarti sebagai pemancar.

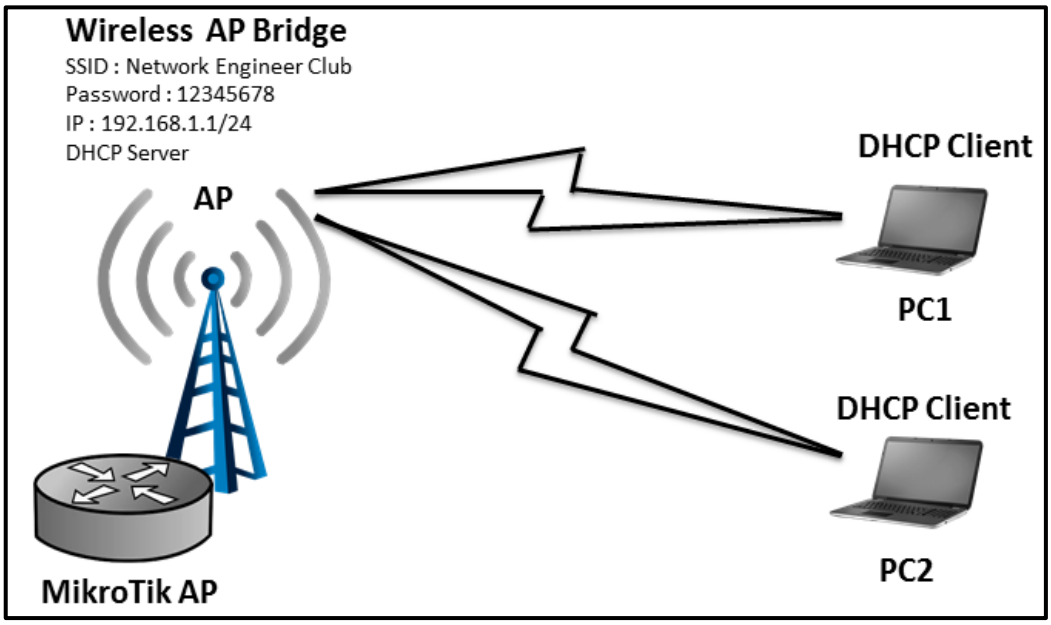
Materi tentang bridge akan kita pelajari pada lab selanjutnya. Pada lab ini kita hanya perlu tahu bahwa mode station tidak bisa di bridge, sedangkan mode station pseudobridge bisa di bridge. Konsep station dan station pseudobridge adalah sama, sehingga di lab ini kita hanya perlu merubah mode pada wireless menjadi station pseudobridge.



Gambar 39.1 Konfigurasi Station Pseudobridge

LAB 40 – Default Forward

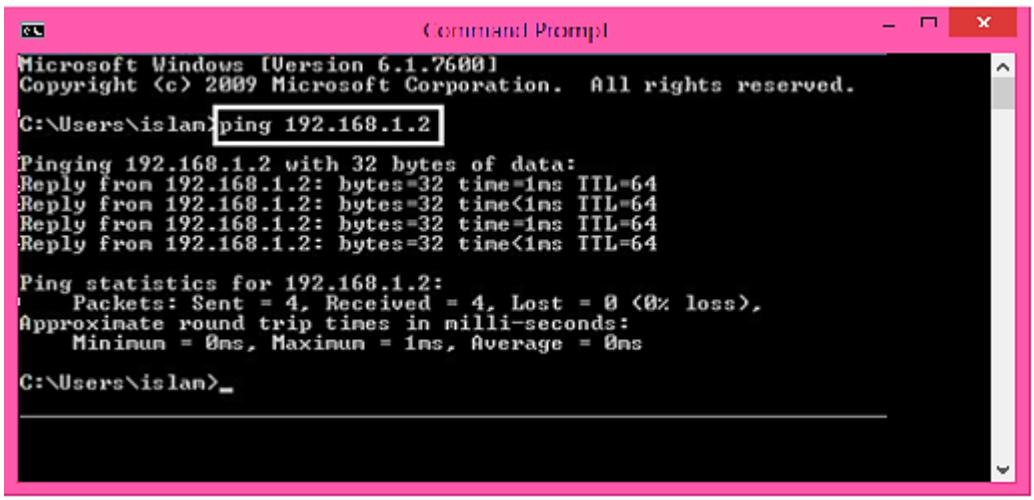
Pada lab ini kita akan belajar salah satu fitur keamanan jaringan pada wireless. Berikut adalah topologi kasus yang akan kita gunakan :



Gambar 40.1 Topologi Jaringan Wireless

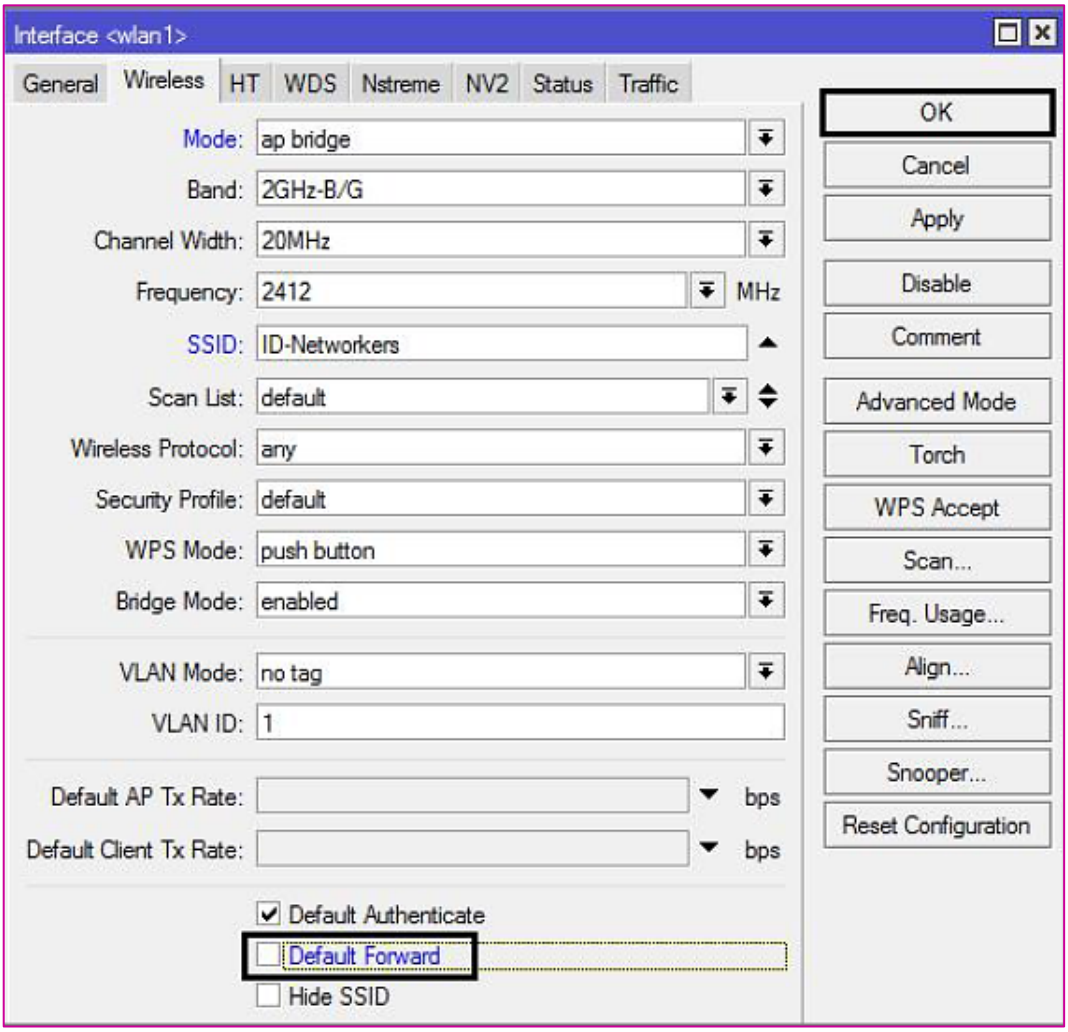
Pada contoh topologi diatas, maka secara default PC1 akan bisa berkomunikasi dengan PC2, akibatnya bisa saja PC1 melakukan netcut ke PC2. Suatu saat mungkin saja kita diminta untuk melakukan konfigurasi agar PC1 dan PC2 tidak bisa saling berkomunikasi, namun kedua PC tersebuttetap bisa berkomunikasi dengan Mikrotik AP.

Untuk menyelesaikan kasus diatas, kita dapat menonaktifkan kasus default forward pada mikrotik. Diasumsikan kita telah mengkonfigurasi mikrotik sebagai wireless ap bridge. Sebelum menonaktifkan fitur default forward, pastikan bahwa PC1 (192.168.1.2) dan PC2 (192.168.1.3) masih dapat berkomunikasi.



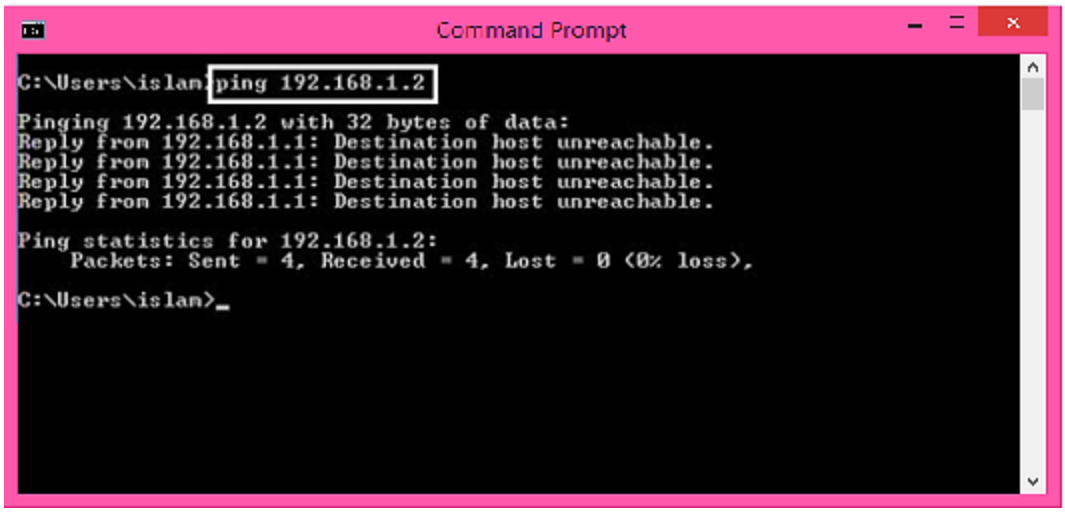
Gambar 40.2 Ping dari PC2 ke PC1 (Sukses)

Selanjutnya untuk menonaktifkan fitur default forward adalah sebagai berikut :



Gambar 40.3 Menonaktifkan Default Forward

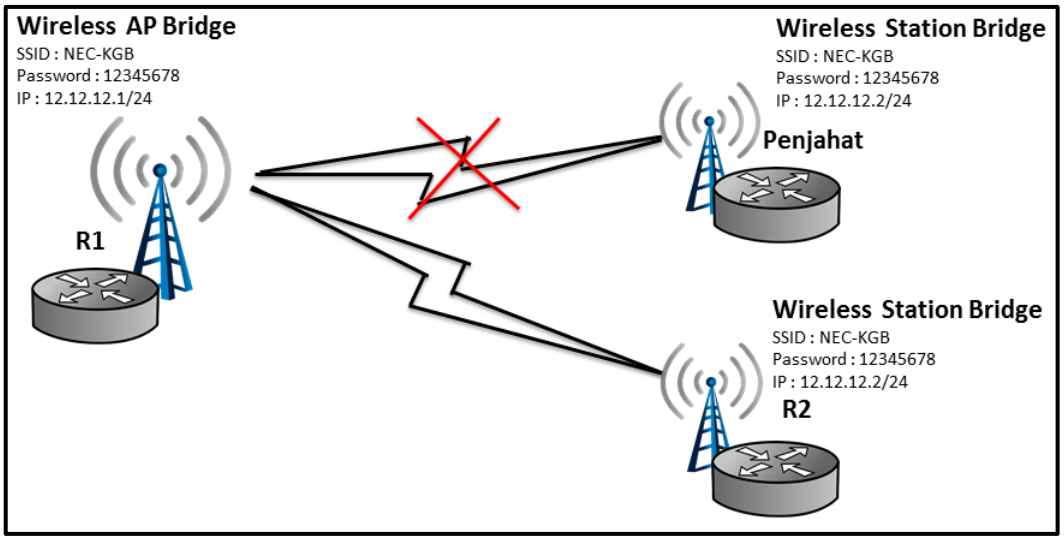
Setelah menonaktifkan fitur default forward seperti diatas, maka PC1 tidak akan bisa berkomunikasi dengan PC2 lagi.



Gambar 40.4 Ping dari PC2 ke PC1 (Gagal)

LAB 41 – Filtering dengan Wireless Access List

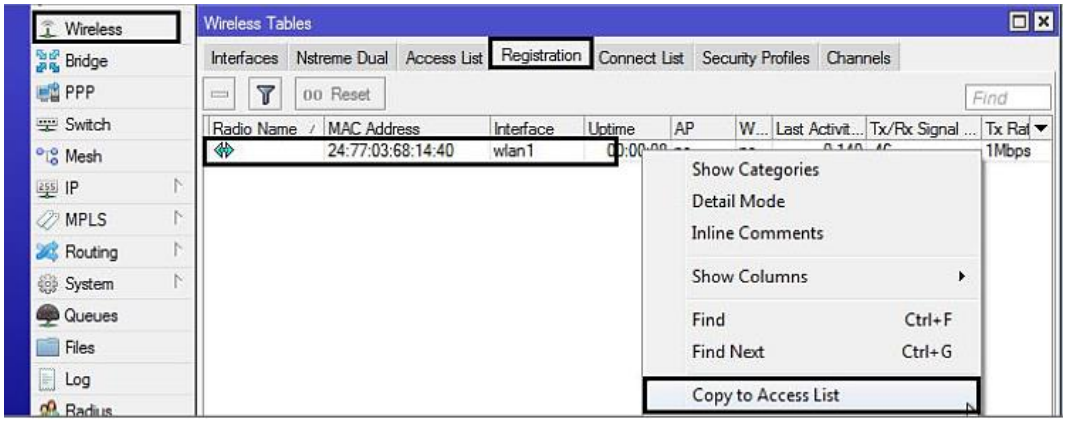
Masih berkaitan dengan keamanan jaringan wireless, pada lab ini kita akan melakukan filtering pada jaringan wireless. Berikut adalah topologi contoh kasus yang akan kita gunakan :



Gambar 41.1 Topologi Wireless Filtering Access List

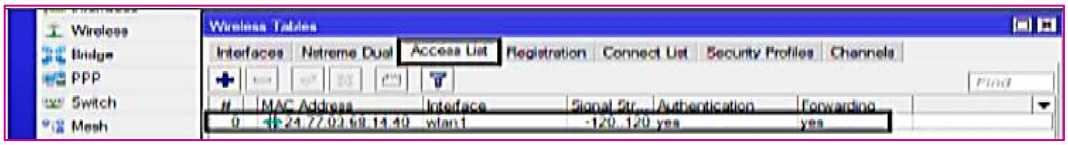
Pada lab ini tujuan kita adalah melakukan konfigurasi agar hanya *client* (mikrotik atau laptop) yang dapat connect dengan wireless AP kita. Untuk menyelesaikan kasus tersebut, kita akan mendaftarkan MAC Address dari client yang diizinkan kemudian menonaktifkan fitur *default authentification* pada wireless mikrotik agar hanya client yang terdaftar saja yang dapat connect.

Diasumsikan kita telah mengkonfigurasi wireless AP Bridge, selanjutnya untuk mendaftarkan client yang diizinkan untuk connect adalah sebagai berikut :



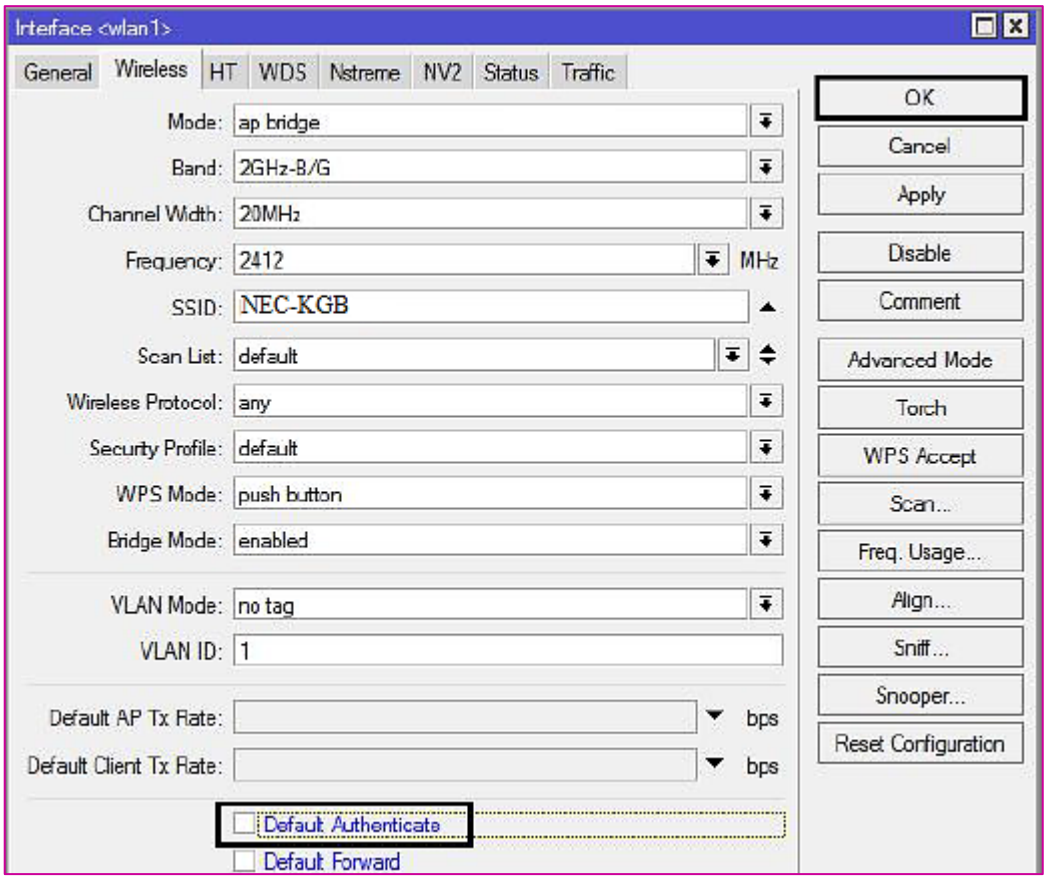
Gambar 41.2 Mendaftarkan Client yang diizinkan

Menu registation diatas menunjukkan daftar client yang connect dengan wireless AP yang kita miliki. Selanjutnya untuk mendaftarkan beberapa client yang diinginkan, kita tinggal klik kanan kemudian pilih opsi *Copy to Access List*. Setelah melakukan langkah tersebut, maka kita bisa melihat daftar client-client yang diizinkan pada menu access list seperti berikut ini :



Gambar 41.3 Daftar Client yang diizinkan

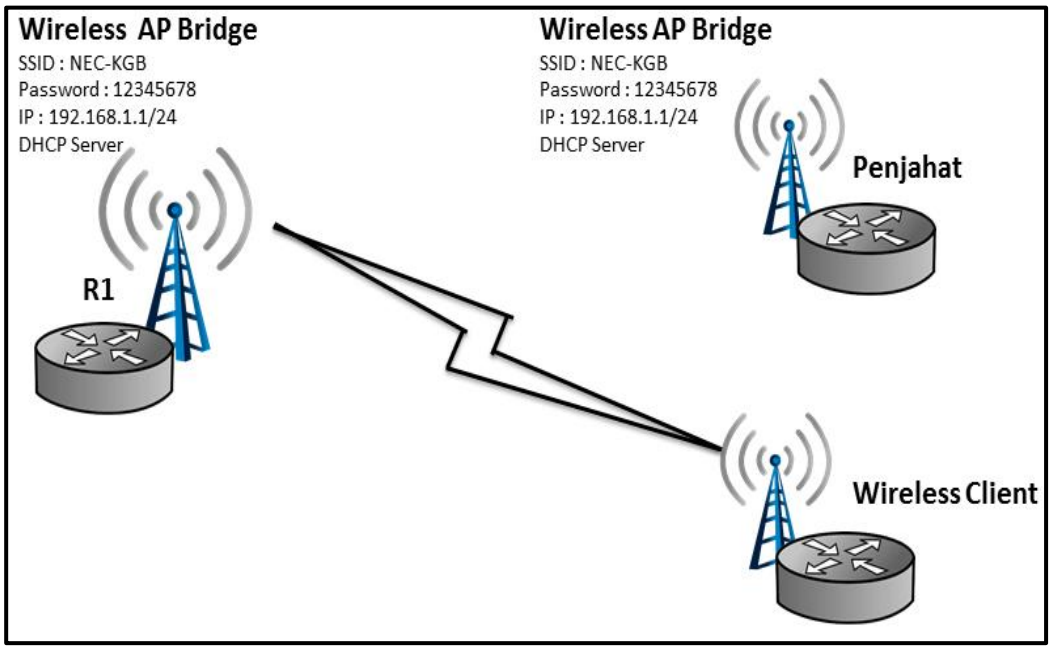
Setelah mendaftarkan client yang diinginkan, langkah selanjutnya adalah menonaktifkan fitur default authentication agar hanya client yang diizinkan saja yang bisa connect.



Gambar 41.4 Mengaktifkan Fitur Default Authentication

LAB 42 – Wireless Filtering dengan Connect List

Lab ini hampir sama dengan LAB 41, hanya saja jika LAB 41 kita mengkonfigurasi pada sisi AP (pemancar), maka pada lab ini kita akan mengkonfigurasi pada sisi client (penerima). Berikut adalah topologi contoh kasus yang akan kita gunakan :

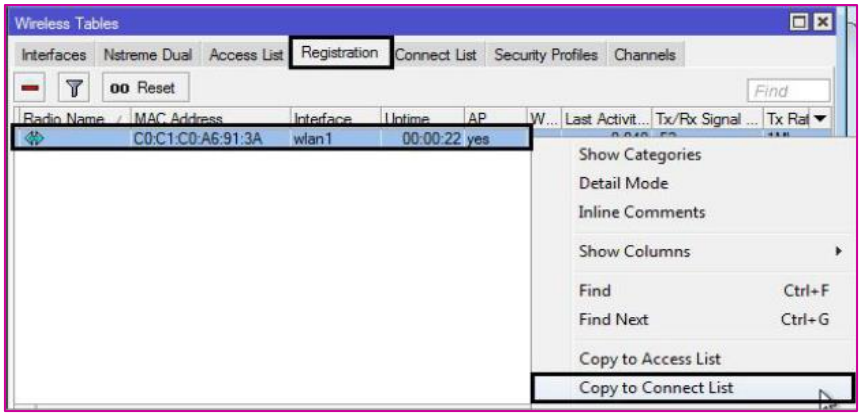


Gambar 42.1 Topologi Jaringan Wireless

Perhatikan topologi diatas, terlihat bahwa ada 2 AP yang memiliki SSID dan Password yang sama. AP pertama adalah AP yang valid sedangkan wireless AP yang kedua adalah penjahat. Jika contoh kasusnya seperti ini maka wireless client akan connect ke wireless AP yang memiliki sinyal tertinggi dan bisa saja yang memiliki sinyal tertinggi adalah AP penjahat. Jika kasus ini terjadi maka client akan connect ke wireless AP penjahat. Yang bisa mengakibatkan pencurian data client oleh wireless AP penjahat.

Untuk megatasi hal ini, kita akan mendaftarkan AP yang valid ke wireless client untuk selanjutnya menonaktifkan fitur default authentication agar wireless client hanya bisa connect ke AP yang terdaftar saja.

Diasumsikan kita telah mengkonfigurasi mikrotik sebagai wireless station (client) dan sudah connect ke AP yang valid. Selanjutnya untuk mendaftarkan AP yang valid adalah sebagai berikut :

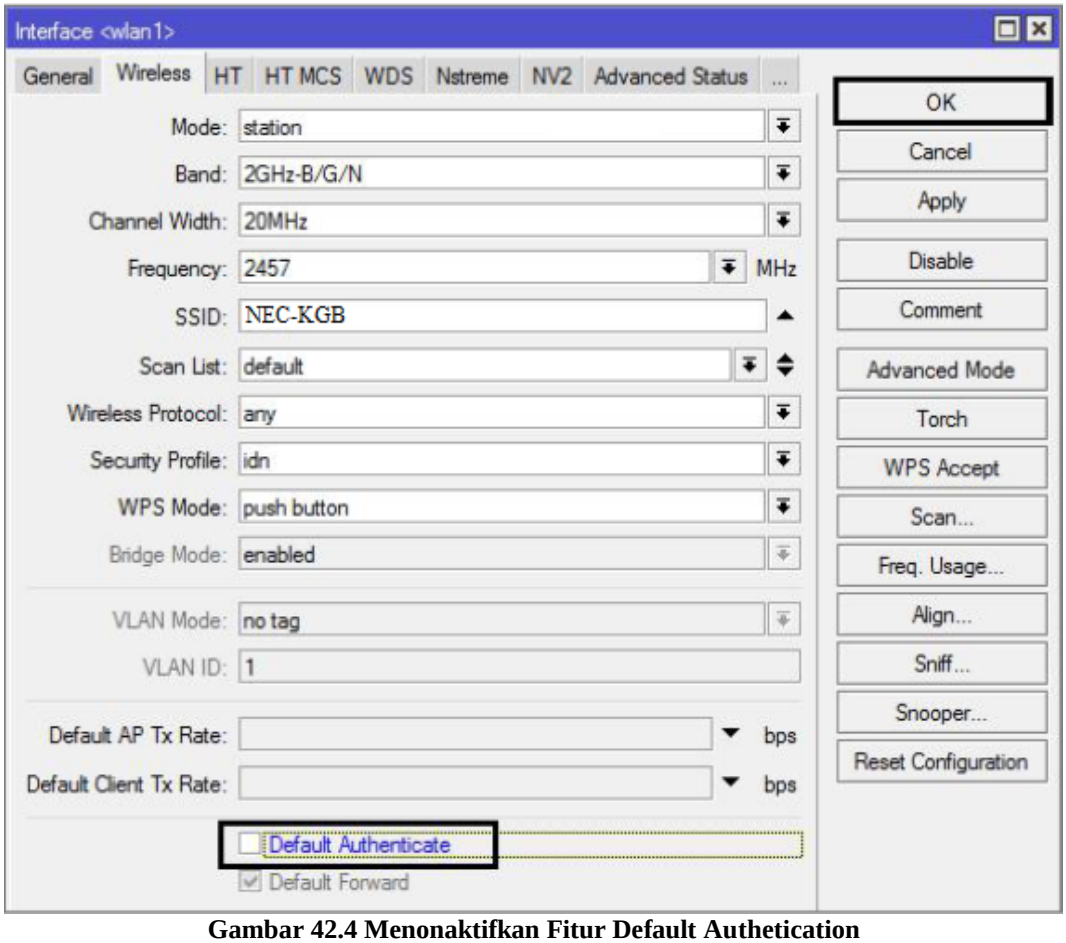


Gambar 42.2 Mendaftarkan AP yang valid

Setelah melakukan langkah diatas, kita bisa melihat daftar AP yang valid pada menu connect list seperti berikut :

Gambar 42.3 Daftar AP yang valid

Langkah terakhir yang harus kita lakukan adalah menonaktifkan fitur default authentication agar wireless client hanya bisa connect ke AP yang terdaftar saja.



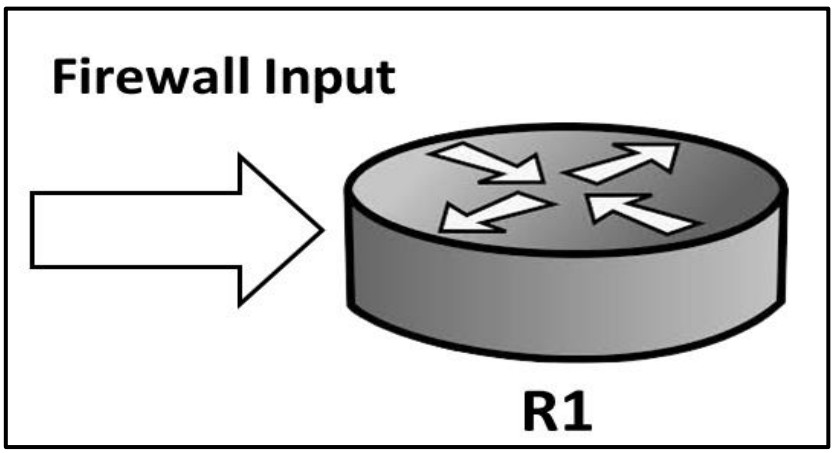
Gambar 42.4 Menonaktifkan Fitur Default Authetication

BAB VI

Firewall Mikrotik

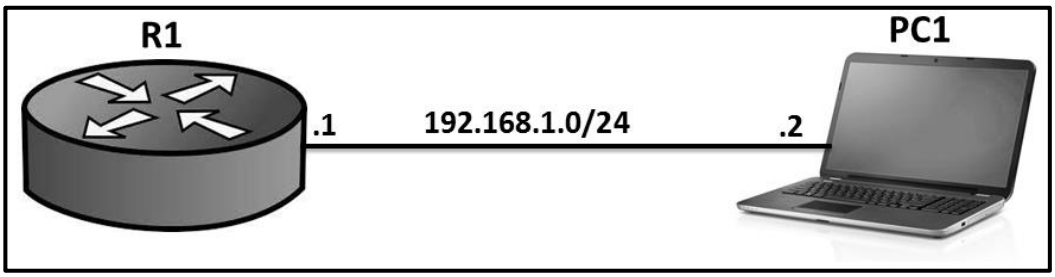
LAB 43 – Firewall Filtering Input

Firewall filter input berfungsi untuk membuat kebijakan-kebijakan terhadap paket masuk ke router. Perhatikan gambar berikut :



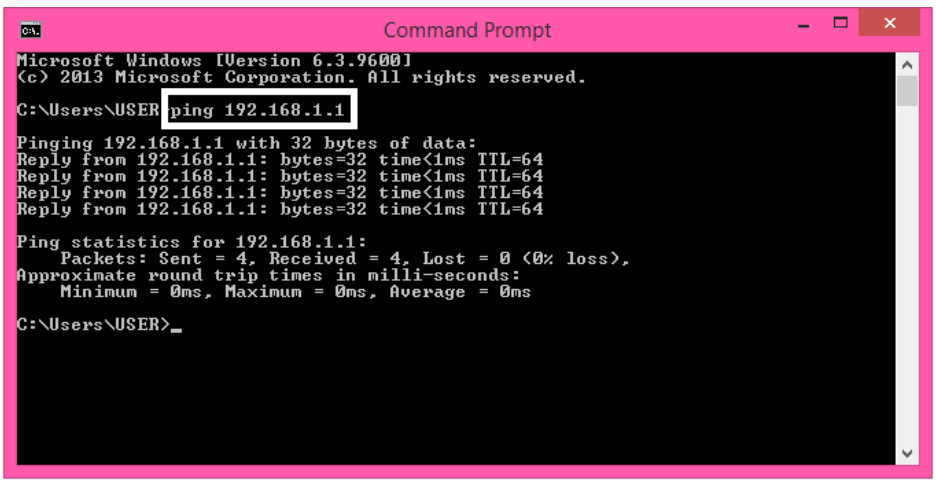
Gambar 43.1 Firewall Input

Salah satu contoh paket yang masuk ke router adalah paket ping dari client ke router. Pada lab ini kita akan coba memblokir paket ping yang berasal dari clirnt ke router.



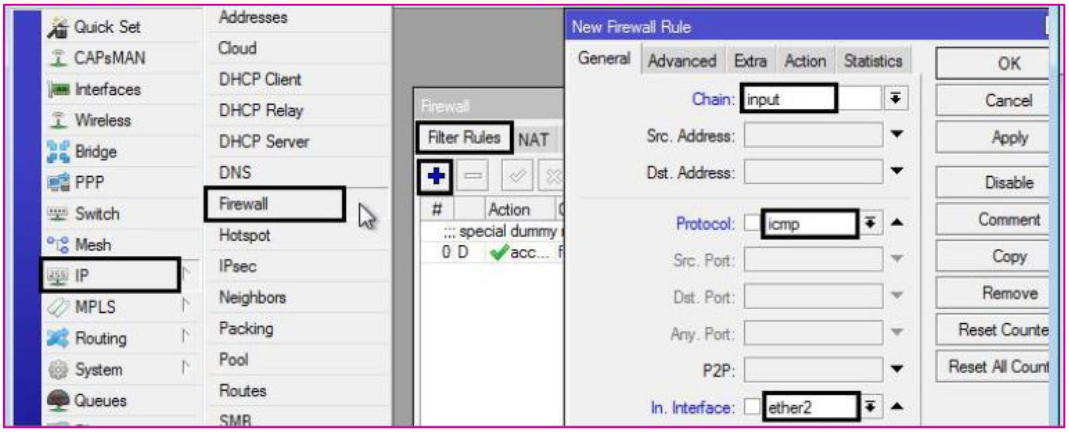
Gambar 43.2 Topologi Firewall Input

Diasumsikan bahwa R1 dan PC1 sudah dikonfigurasi IP Address sesuai topologi diatas dan sudah bisa saling berkomunikasi.

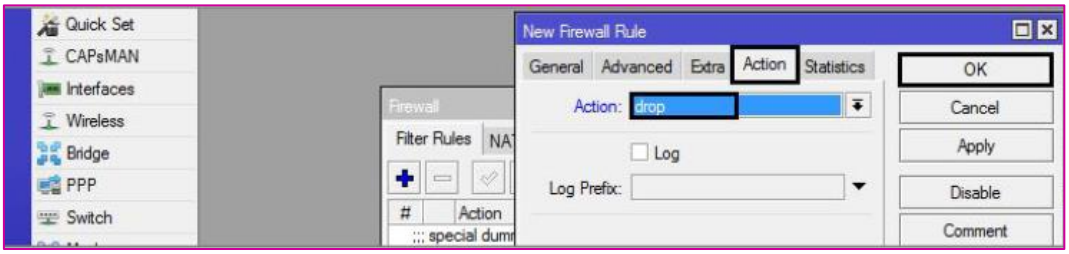


Gambar 43.3 PC1 bisa ping ke R1

Selanjutnya agar PC1 tidak bisa ping ke R1, kita harus membuat rule pada firewall filter seperti berikut :

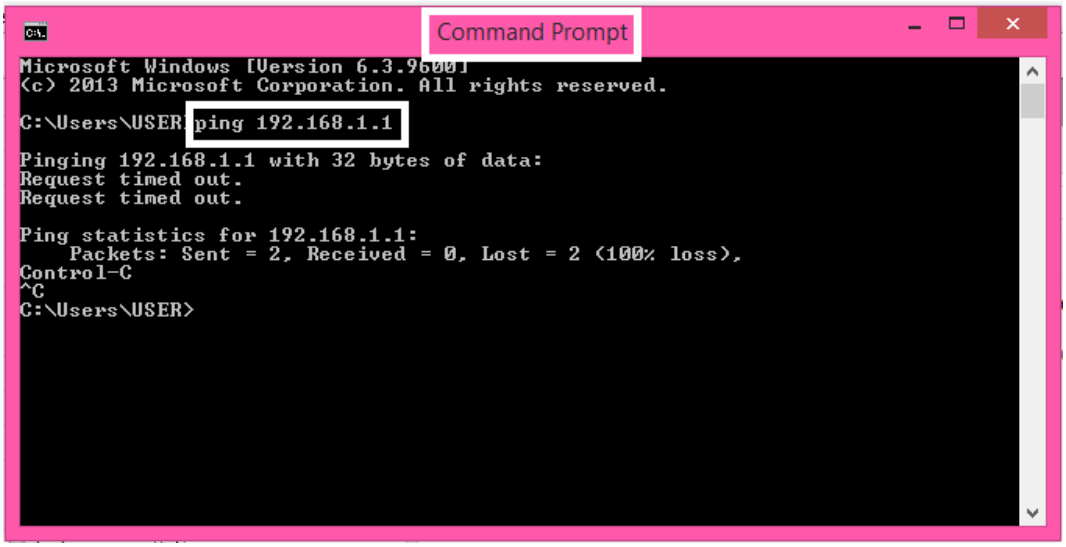


Gambar 43.4 Konfigurasi Firewall Filter Input



Gambar 43.5 Konfigurasi Firewall Filter Input

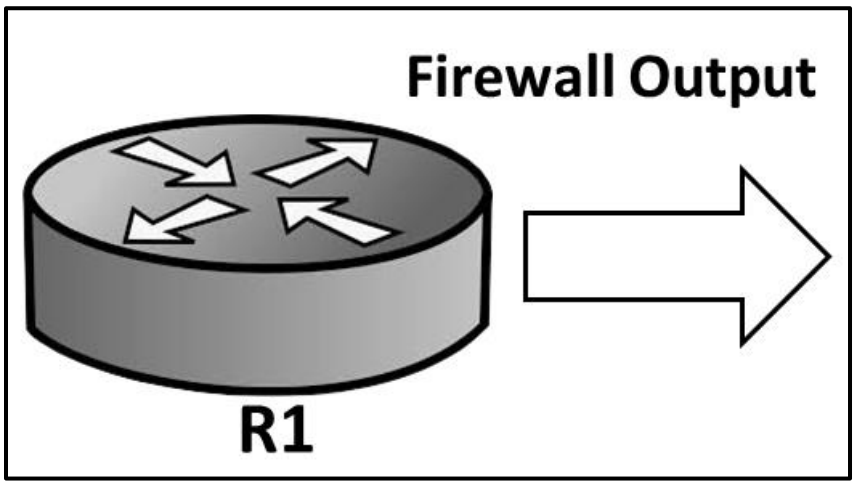
Setelah mengkonfigurasi firewall filter input seperti diatas, maka PC1 tidak akan bisa ping ke R1.



Gambar 43.6 PC1 tidak bisa ping ke R1

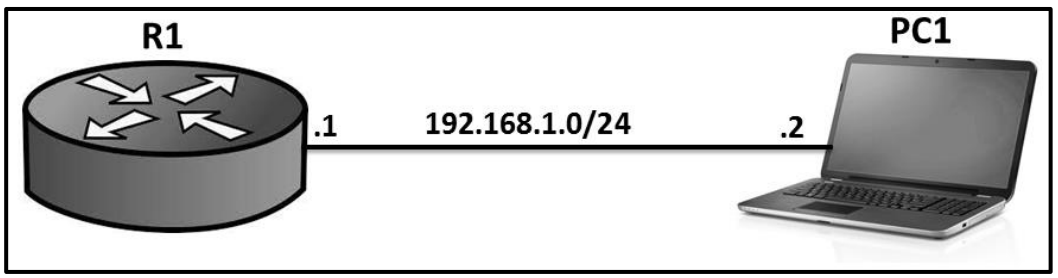
LAB 44 – Firewall Filtering Output

Sebelumnya kita telah membahas tentang firewall filter input yang akan menangani paket masuk ke router. Selanjutnya pada lab ini kita akan membahas materi tentang firewall filter output merupakan firewall yang akan menangani paket yang keluar dari router. Untuk lebih jelasnya perhatikan ilustrasi berikut :



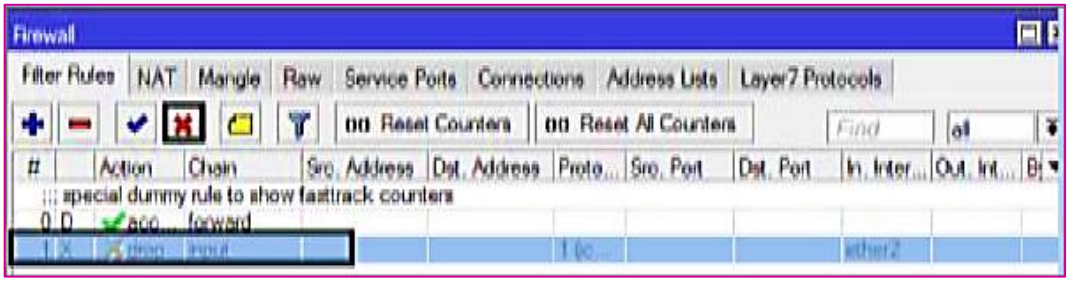
Gambar 44.1 Firewall Output

Salah satu contoh paket output adalah paket ping yang berasal dari router ke client. Pada lab ini kita akan coba untuk memblokir paket ping yang berasal dari router ke client.



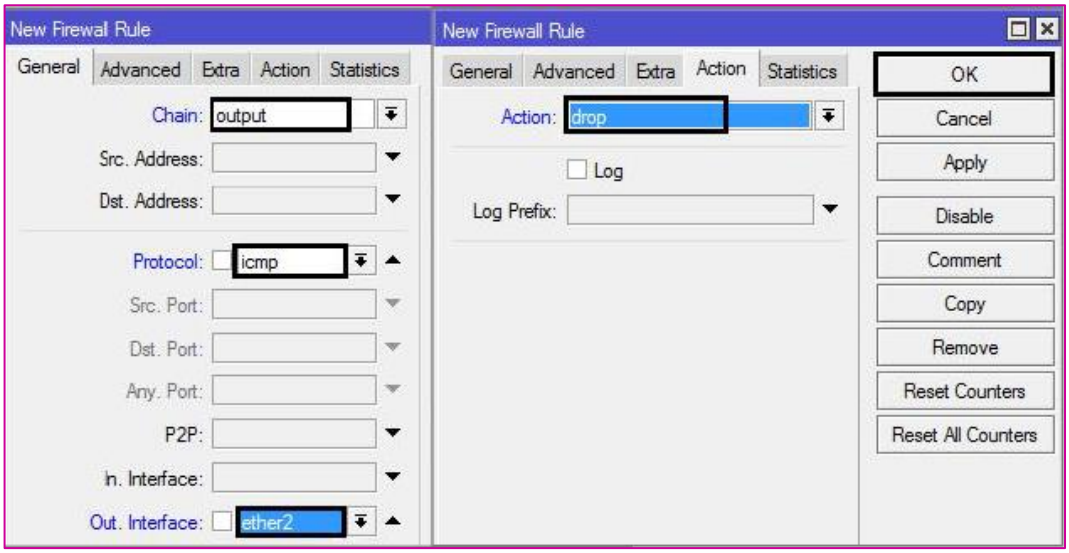
Gambar 44.2 Topologi Firewall Filter Output

Sebelum membuat rule firewall filter output, disable dulu rule firewall input yang kita telah buat sebelumnya. Hal ini dikarenakan rule firewall input tersebut juuga memblokir paket ping dari router ke client. Kenapa demikian? Bukankah rule tersebut adalah firewall input dan paket yang berasal dari router adalah output?? Kita akan membahas materi ini pada tab *connection state*.



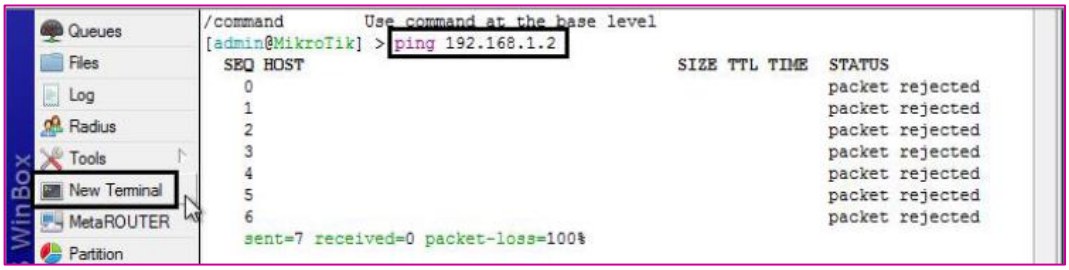
Gambar 44.3 Disable Firewall Output

Selanjutnya kita buat firewall output untuk blokir ping dari router ke client.



Gambar 44.4 Konfigurasi Firewall Filter Output

Setelah mengkonfigurasi firewall filter output seperti diatas, maka seharusnya R1 sudah tidak bisa ping ke PC1

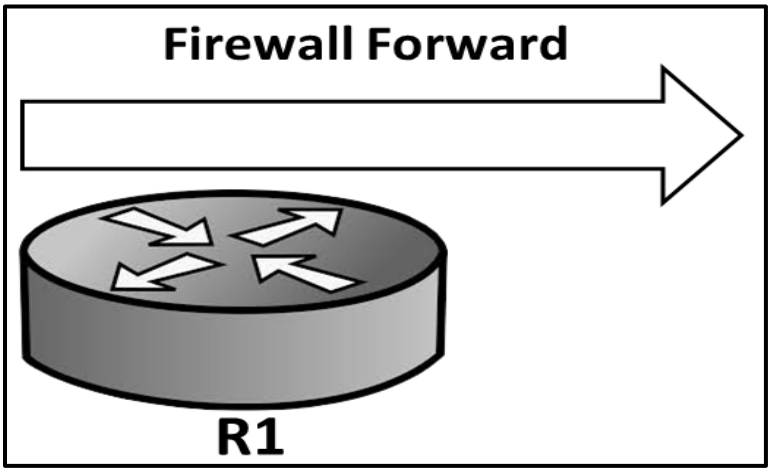


Gambar 44.5 R1 tidak bisa ping ke PC1

LAB 45 – Firewall Filtering Forward

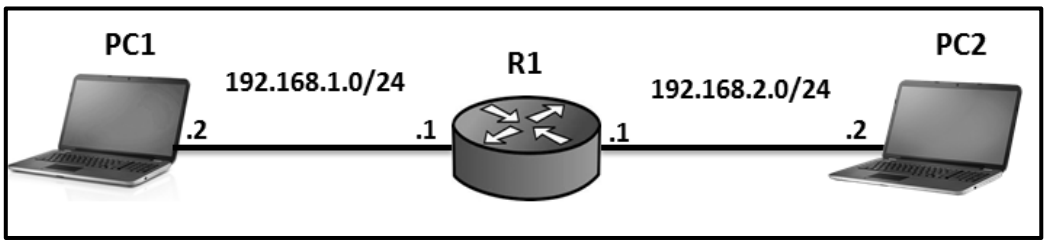
Jika firewall input menangani paket yang masuk ke router, firewall output menangani paket yang melewati router, maka firewall filter forward adalah firewall yang menangani (memfilter) paket yang melewati router.

\



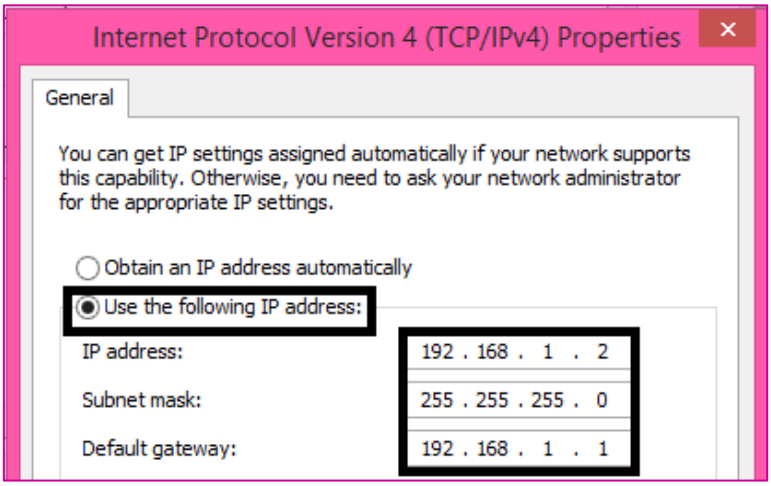
Gambar 45.1 Firewall Forward

Berikut adalah contoh topologi yang kita gunakan yaitu paket yang melewati router adalah paket ping dari PC1 ke PC2.

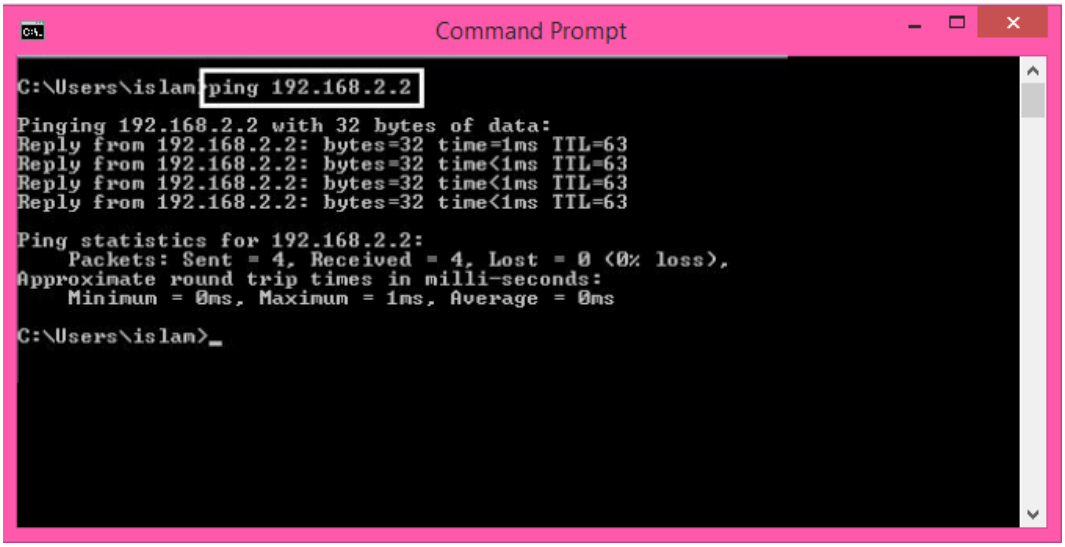


Gambar 45.2 Topologi Jaringan Firewall Forward

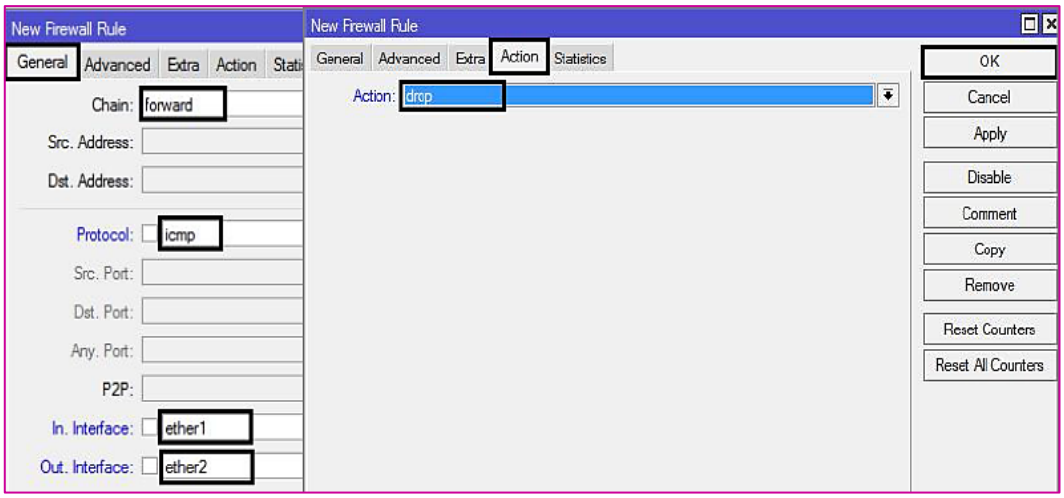
Pada lab ini kita akan mencoba blokir paket ping yang berasal dari PC1 ke PC2. Namun sebelumnya pastikan PC1 bisa ping ke PC2. ***(Note : PC1 dan PC2 harus sudah dikonfigurasi gateway)***



Gambar 45.3 Konfigurasi IP Address dan Gateway

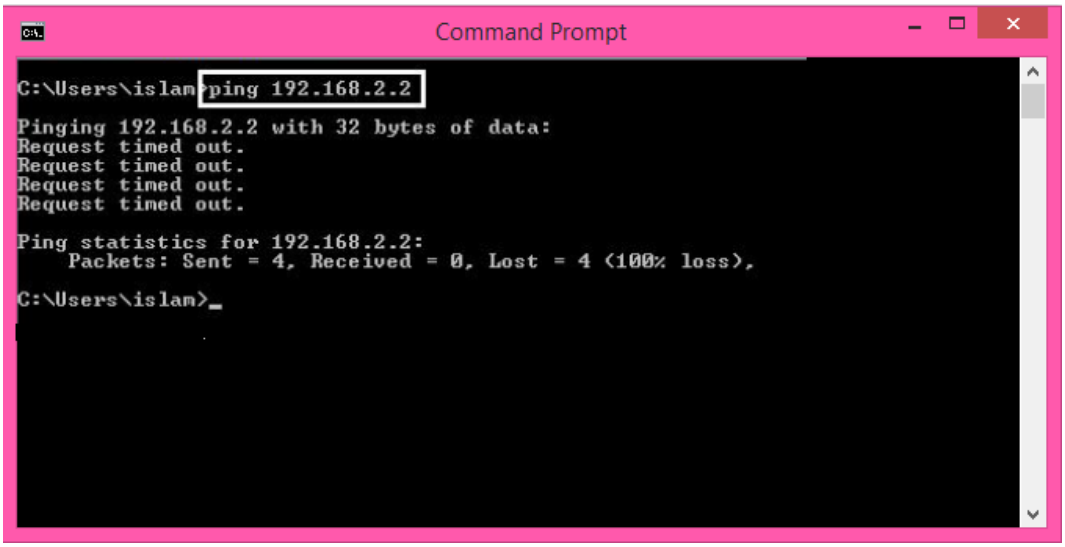


Gambar 45.4 Ping dari PC1 ke PC2 (Sukses)



Gambar 45.5 Konfigurasi Firewall Filter Forward

Setelah membuat rule firewall filter forward seperti diatas, maka PC1 tidak akan bisa lagi berkomunikasi dengan PC2.

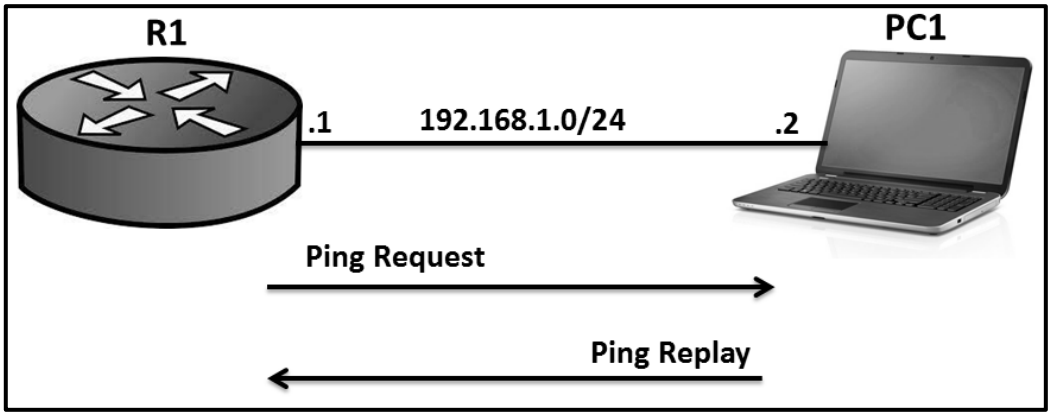


Gambar 45.6 PC1 tidak bisa ping ke PC2

LAB 46 – Connection State

Pada lab sebelumnya telah saya jelaskan bahwa saat kita membuat rule firewall input untuk blokir ping dari client ke mikrotik, maka mikrotik juga tidak akan bisa ping ke client. Padahal kita tahu bahwa seharusnya firewall input hanya mengurus paket yang masuk ke router saja, sedangkan paket drai router ke client merupakan paket yang seharusnya ditangani oleh firewall output.

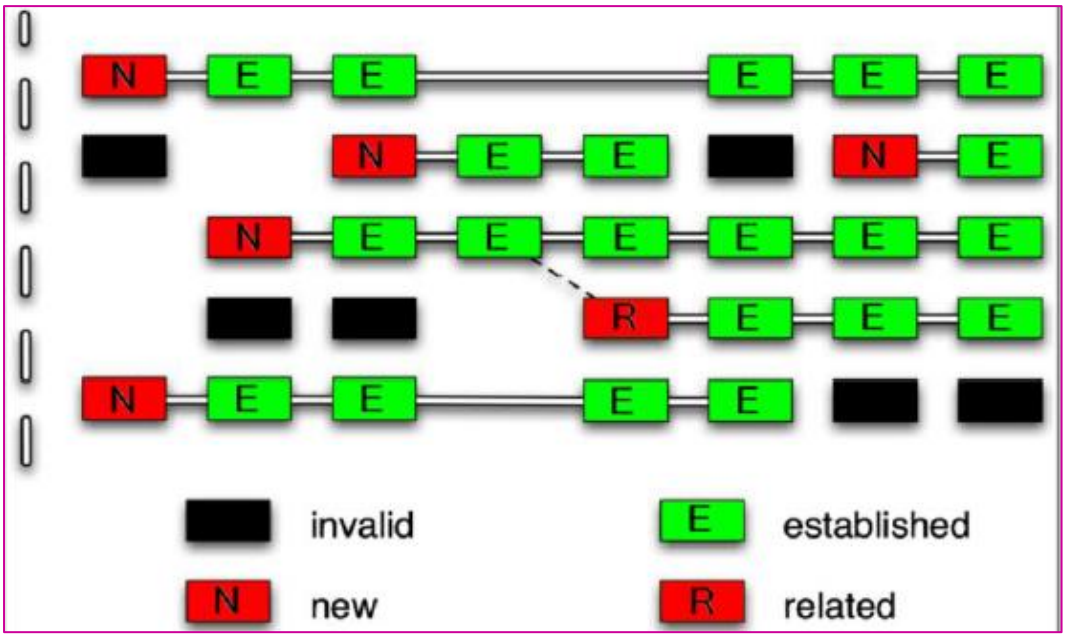
Perhatikan ilustrasi berikut!



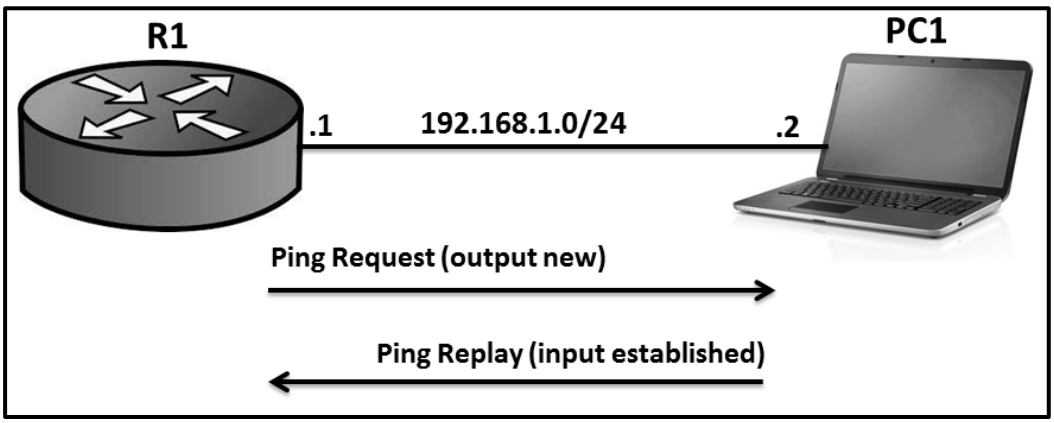
Gambar 46.1 Ilustrasi Connection State

Perhatikan saat R1 ping ke PC1, maka PC1 akan mengirimkan paket replay ke R1. Paket replay ini tentu akan ditangani oleh firewall input. Jika teryata difirewall input sudah ada rule untuk paket ping, maka tentu saja R1 tidak akan bisa ping ke PC1.

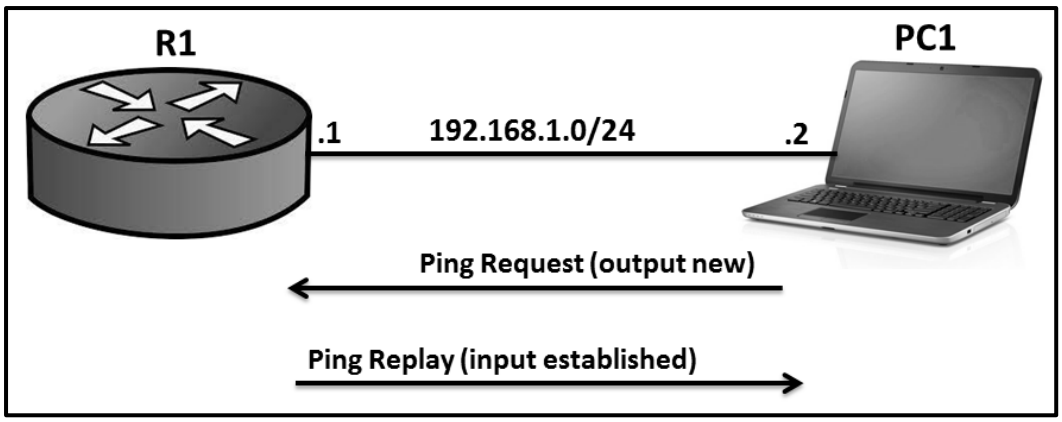
Pertanyaannya adalah bagaimana jika kita menginginkan agar PC1 tidak bisa ping ke R1 namun R1 masih tetap bisa ping ke PC1?? Untuk meyeselsaikan contoh kasus seperti itu, maka kita harus memahami connection state dari sebuah paket.



Gambar 46.2 Connection State

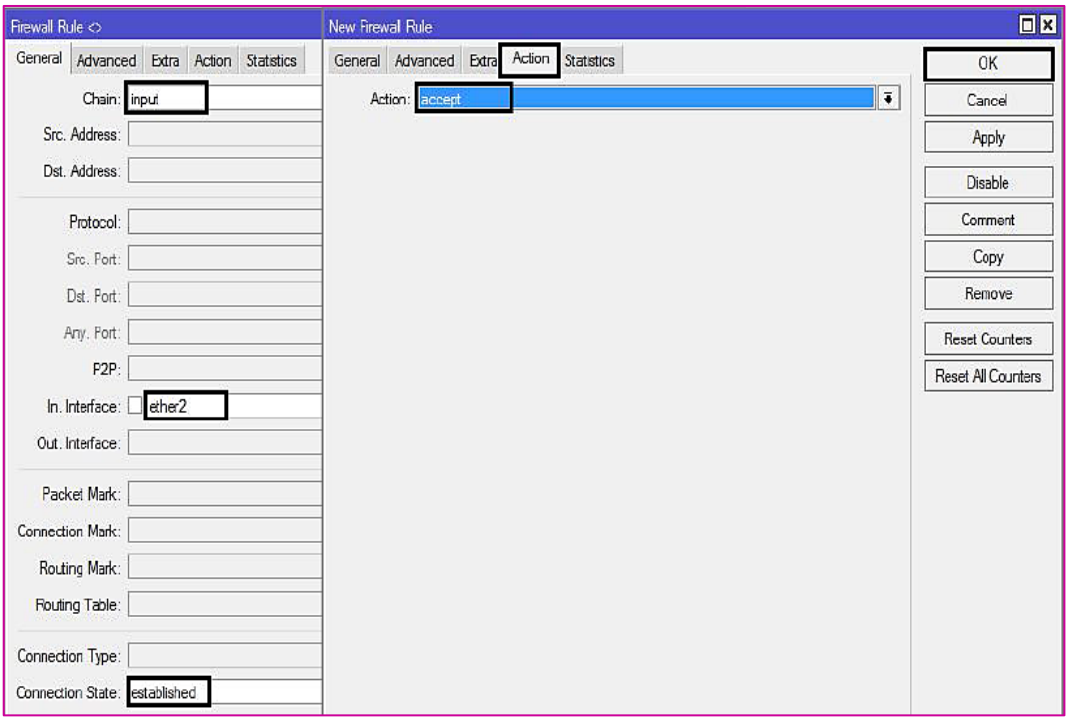


Gambar 46.3 Paket Ping dari Router ke Client

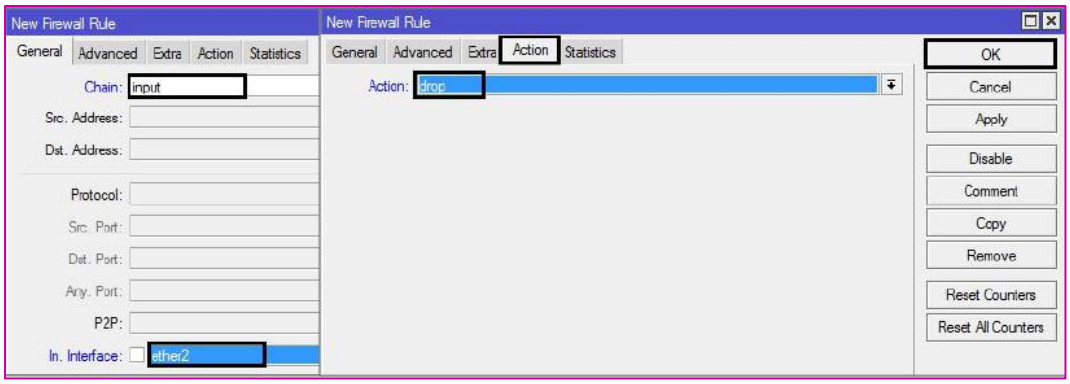


Gambar 46.4 Paket Ping dari Client ke Router

Jika kita menginginkan agar PC1 tidak bisa ping ke R1, namun R1 masih tetap bisa ping ke PC1. Maka kita harus menolak paket input **New** dan memperbolehkan paket input **established,** sesuai dengan ilustrasi diatas.

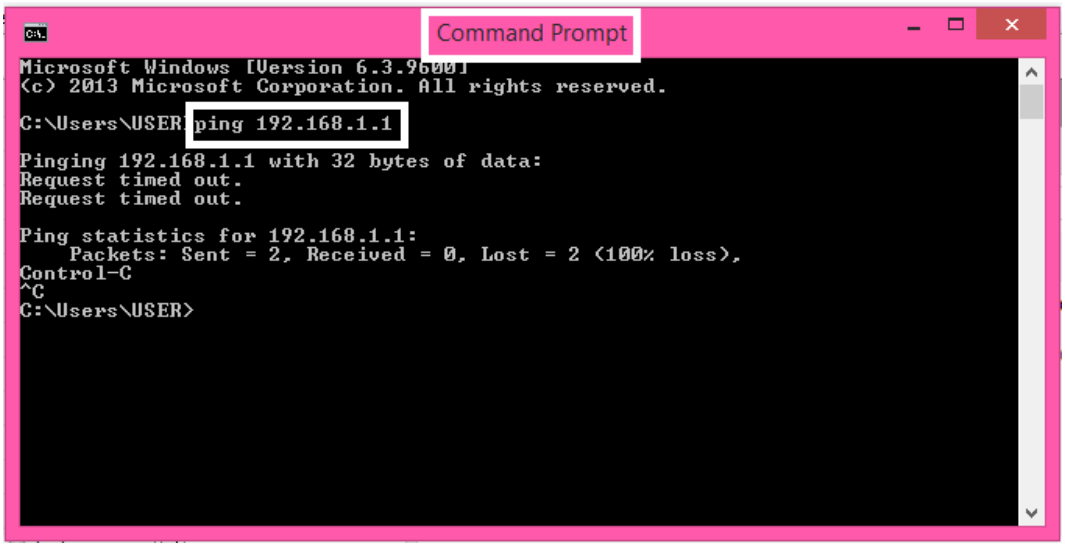


Gambar 46.5 Konfigurasi Firewall Input

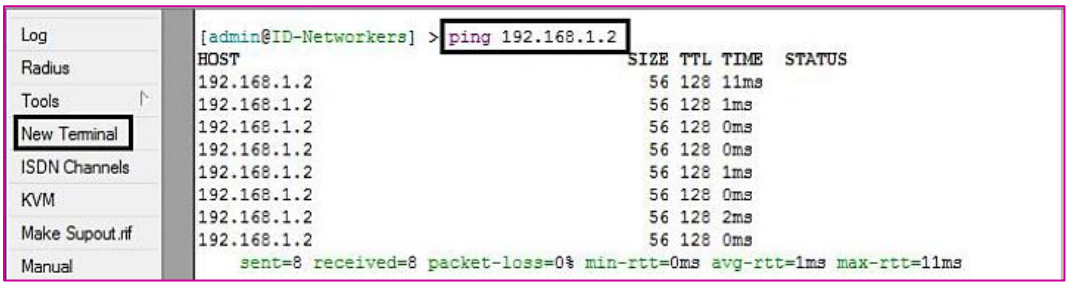


Gamba 46.6 Konfigurasi Firewall Input

Untuk pengujian coba lukukan ping dari PC1 ke R1



Gambar 46.7 PC1 tidak bisa ping ke R1



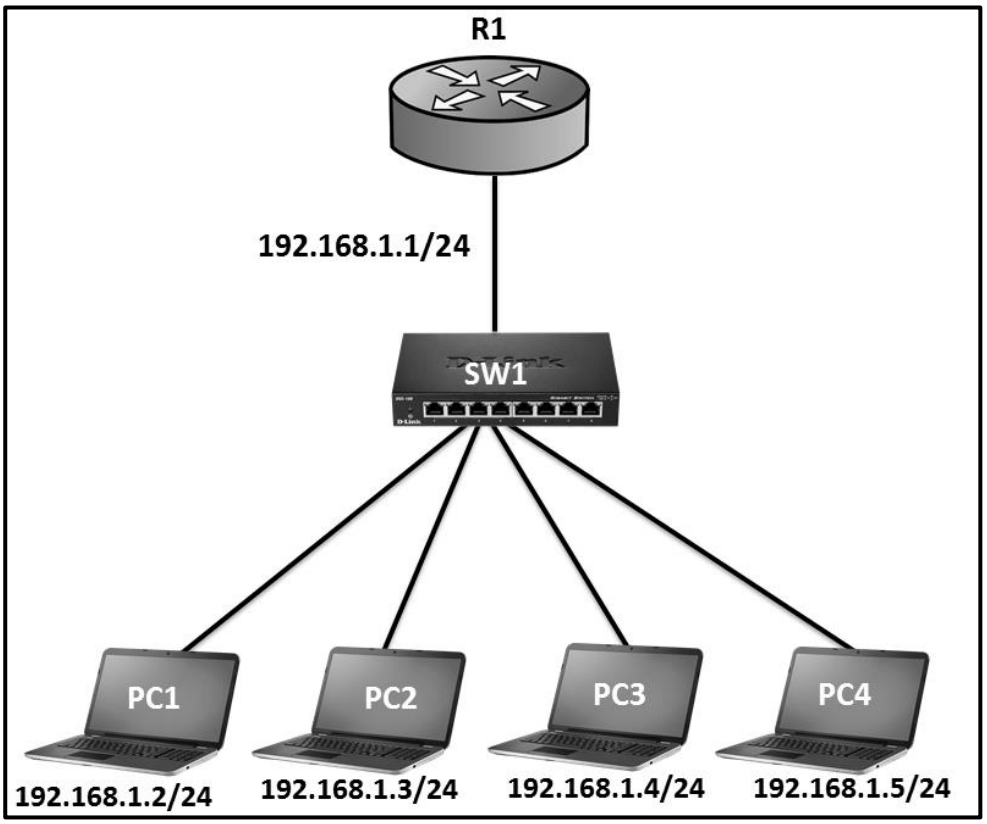
Gambar 46.8 R1 berhasil ping ke PC1

Pastikan bahwa PC1 tidak bisa ping ke R1 namun R1 bisa ping ke PC1.

LAB 47 – Firewall Strategy (drop view accept any)

Ada dua strategi yang dapat kita gunakan, strategi pertama yaitu *drop beberapa, keudian acceptsemua* atau biasa disebut *accept view drop any*. Pada lab ini kita hanya fokus belajar tentang strategi pertama.

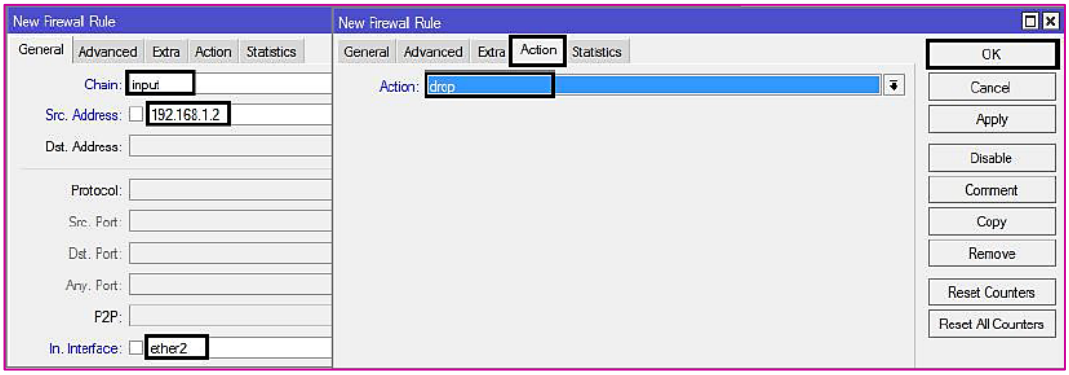
Perhatikan contoh kasus berikut :



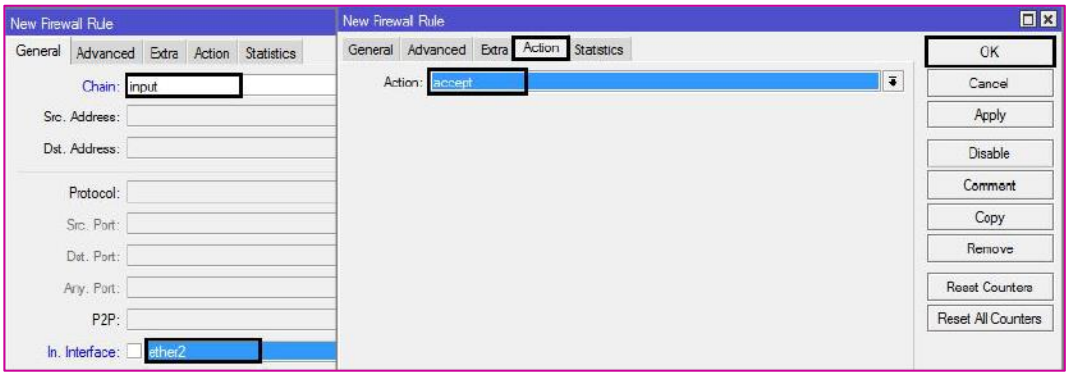
Gambar 47.1 Topologi Jaringan Sederhana

Misal kita menginginkan PC1 tidak bisa ping ke router namun PC2, PC3 dan PC4 bisa ping ke router. Untuk mengerjakan contoh kasus tersebut, strategi yang paling tepat dilakukan adalah *drop view accept any*.

Berikut konfigurasi pada R1

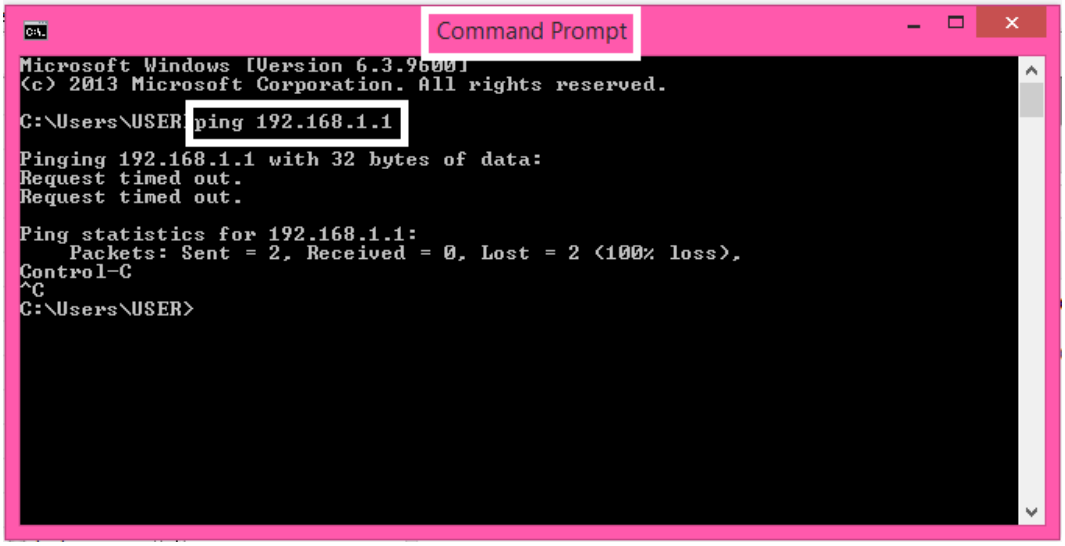


Gambar 47.2 Konfigurasi Drop View

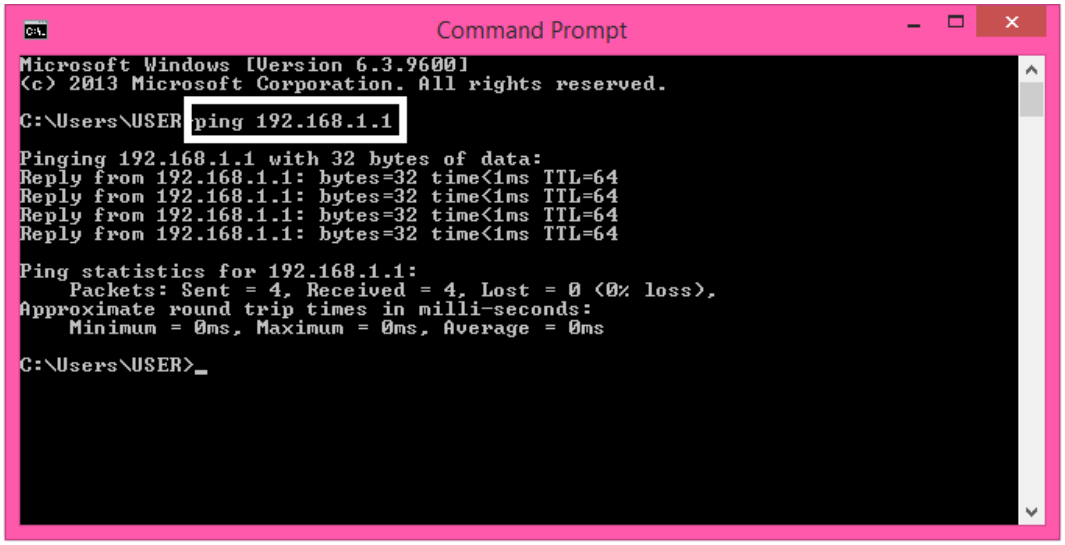


Gambar 47.3 Konfigurasi Accept Any

Untuk pengujian kita coba lakukan ping dari PC1 dan PC2



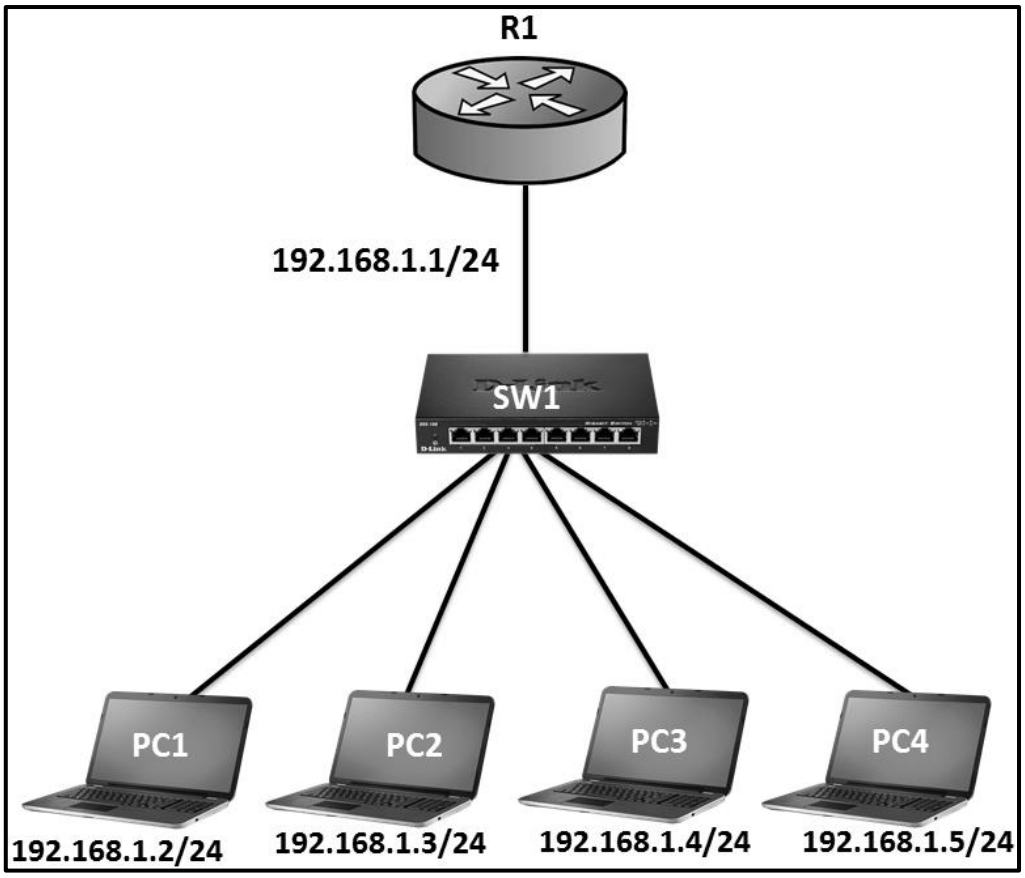
Gambar 47.4 PC1 tidak bisa ping ke R1



Gambar 47.5 PC2 bisa ping ke R1

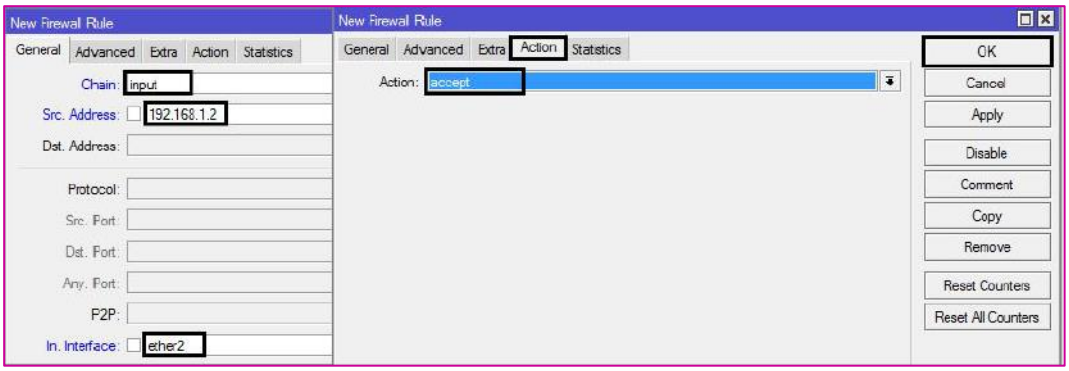
LAB 48 – Firewall Strategy (accept view drop any)

Pada lab sebelumnya kita telah membahas firewall strategy yang pertama. Selanjutnya pada lab ini kita akan belajar firewall strategy yang kedua. Berikut contoh kasus yang akan kita gunakan :

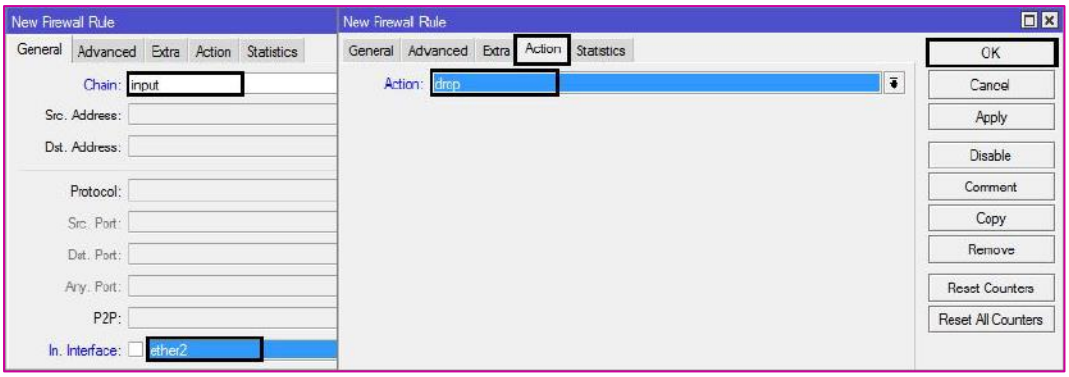


Gambar 48.1 Topologi Jaringan Sederhana

Tujuan kita pada lab ini adalah hanya mengizinkan paket ping yang berasal dari PC1 saja. Paket ping dari PC2, PC3 dan PC4 tidak diizinkan untuk mauk ke router. Untuk mengerjakan contoh kasus tersebut tentu strategy yang paling tepat untuk ita gunakan adalah *accept view drop any*. Beikut konfigurasi pada R1 :

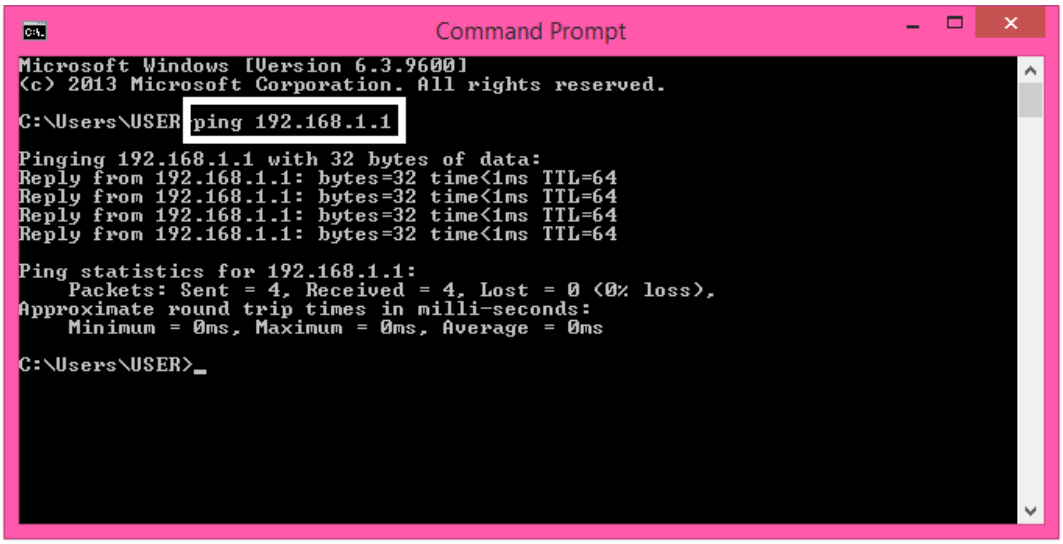


Gambar 48.2 Konfigurasi accept view

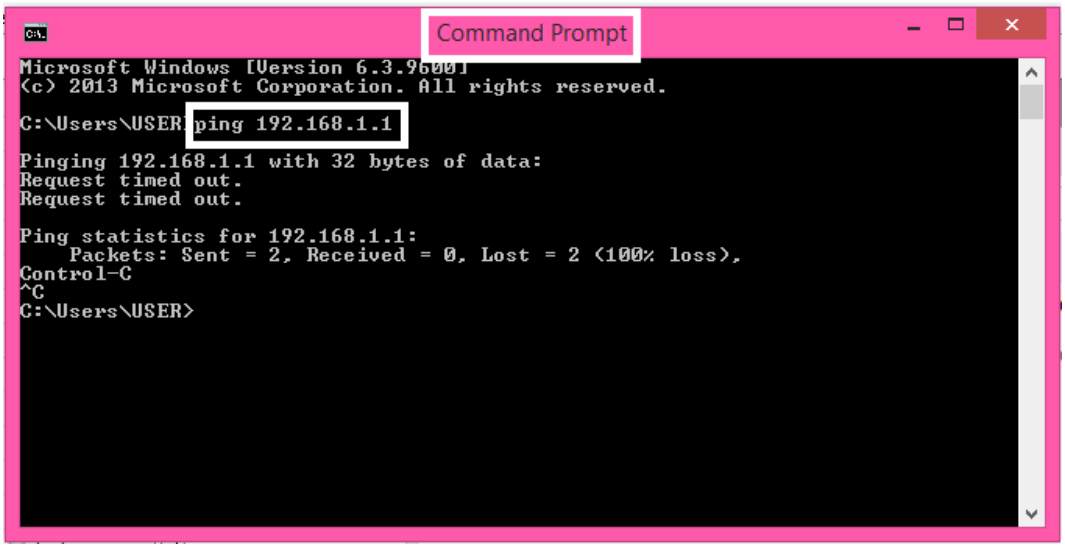


Gambar 48.3 Konfigurasi Drop Any

Untuk mengujinya lakukan ping dari PC1 ke PC2



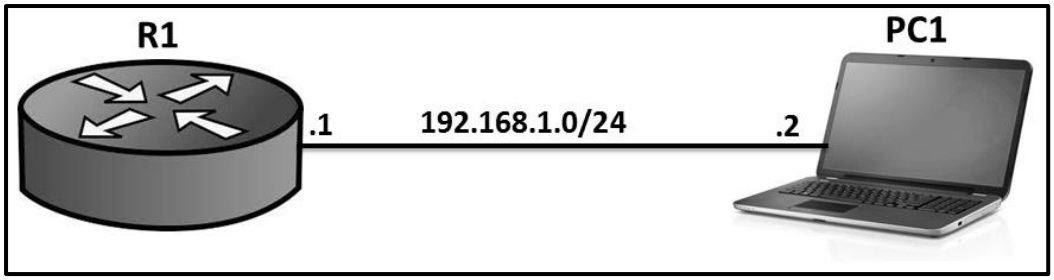
Gambar 48.4 PC1 berhasil ping ke R1



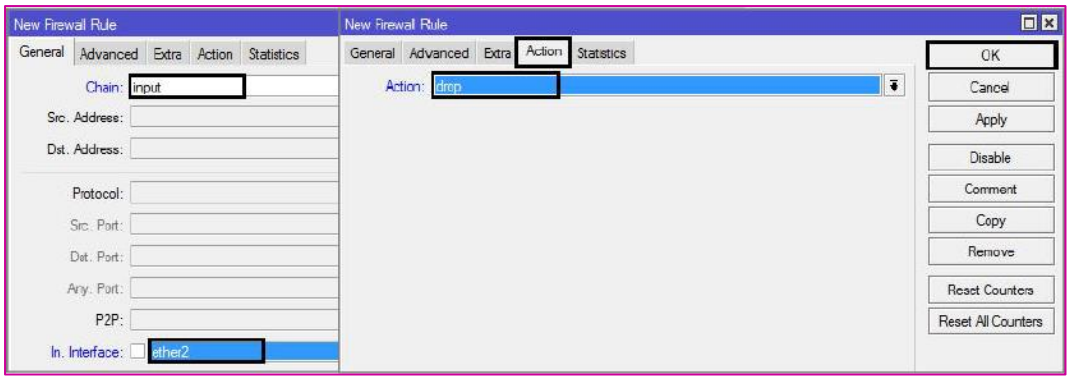
Gambar 48.5 PC2 gagal ping ke R1

LAB 49 – Action Drop

Action Drop digunakan untuk menolak paket tanpa memberikan pemberitahuan. Ibarat ada cowok nembak cewek, si cewek nolak tanpa memberitahukan ke si cowok. Jadi si cowok tidak tahu kalau si cewek menolak karena tidak ada pemberitahuan. Di PHP'in jadi galau, kesiannn... ☺

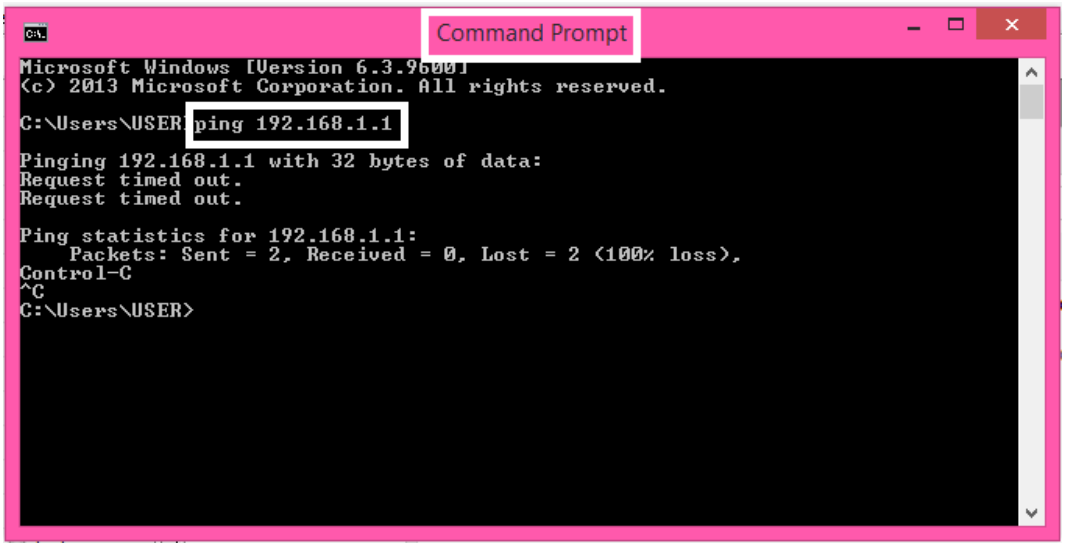


Gambar 49.1 Topologi Jaringan Sederhana



Gambar 49.2 Konfigurasi Firewall Action Drop

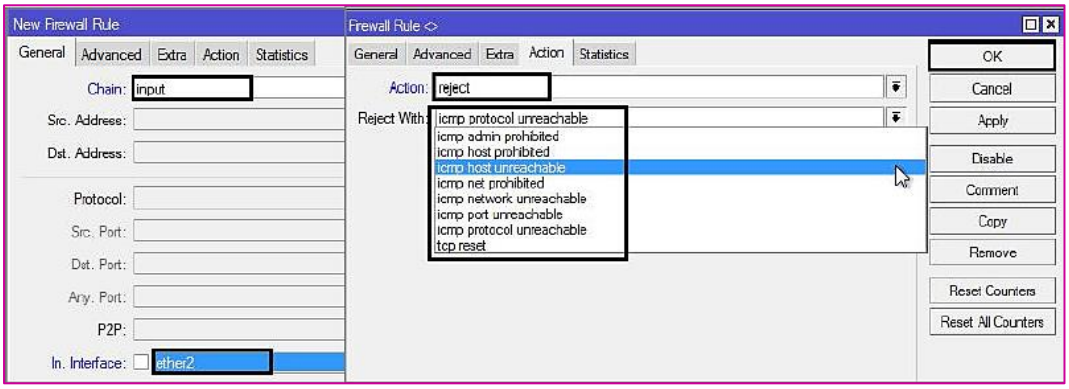
Berikut hasil pengujian ping dari PC1 ke R1



Gambar 49.3 Hasil Action Drop

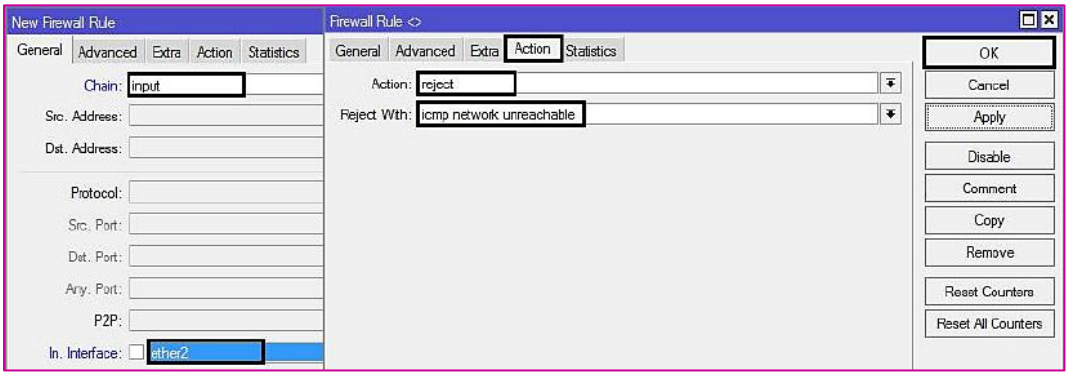
LAB 50 – Action Reject

Jika action **drop** si cewek menolak tanpa memberitahu. Pada **action reject,** si cewek menolak tapi memberitahu ke si cowok. Jadi di sini si cewe tidak PHP. Langsung saja kita lihat hasil dari action reject ini dan bedakan dengan hasil drop. Kita akan menggunakan topologi pada LAB 49 atau sebelumnya.



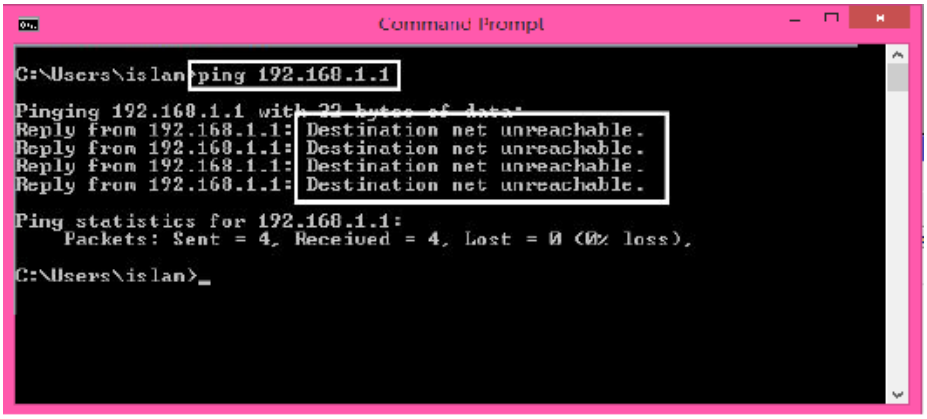
Gambar 50.2 Konfigurasi Action Reject

Perhatikan saat kita mengkonfigurasi **action reject,** akan banyak jawaban yang bisa kita gunakan. Nantinya jika kita pilih *icmp host prohibited*, maka pada client akan muncul pesan *destination host prohibited*, jika kita memilih *icmp host prohibited*, maka pada client akan muncul pesan *destination net prohibited*, dst.

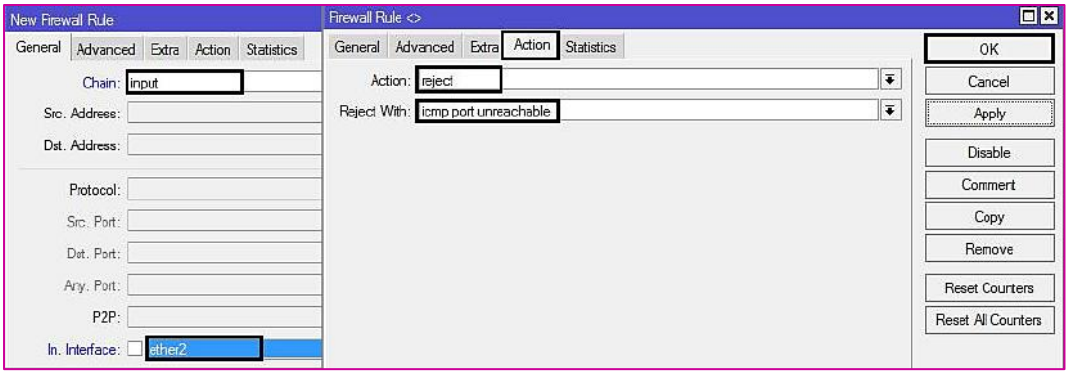


Gambar 50.3 Konfigurasi Action Reject ICMP Net Unreachable

Untuk pengujian, kita lakukan test ping pada PC1

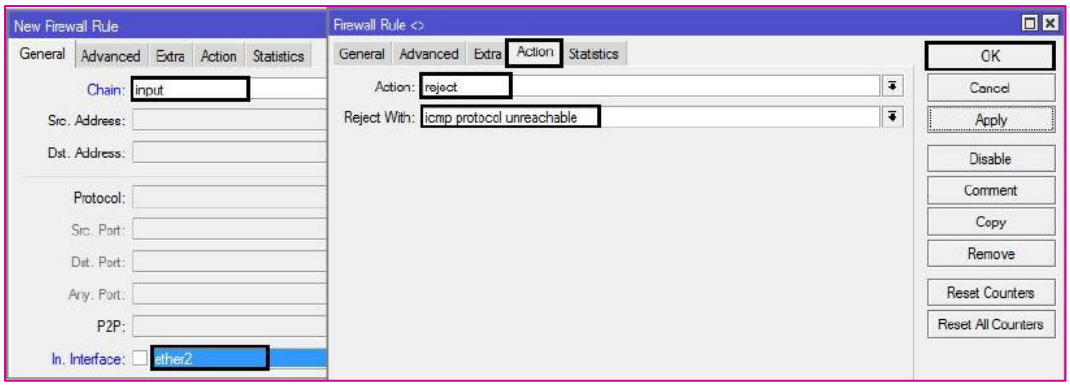


Gambar 50.4 Muncul peringatan net unreachable

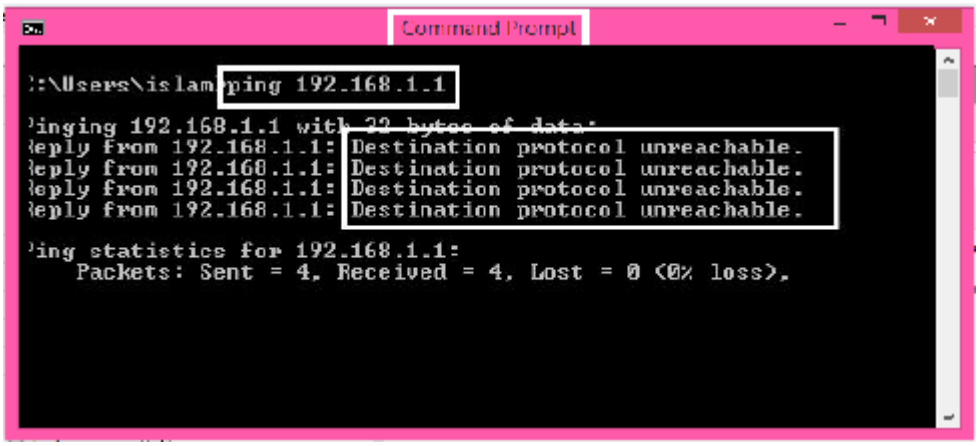


Gambar 50.5 Konfigurasi Reject ICMP Port Unreachable

Gambar 50.6 Muncul Peringatan Port Unreachable



Gambar 50.7 Konfigurasi Reject ICMP Protocol Unreachable

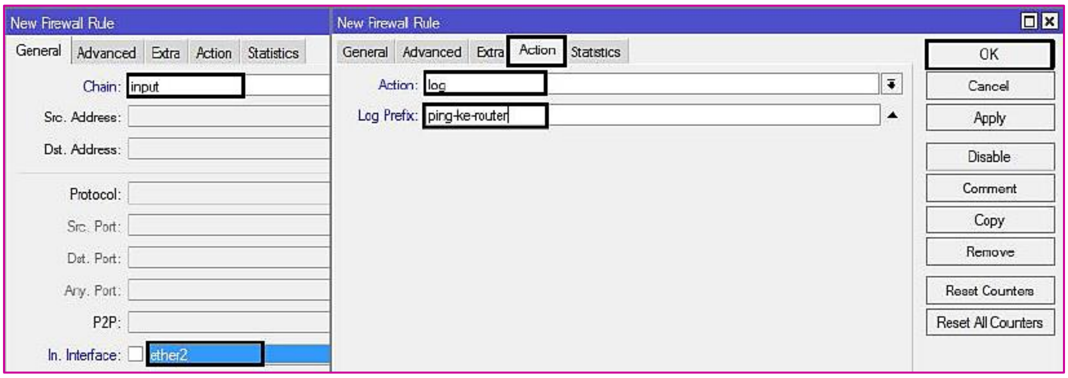


Gambar 50.8 Muncul peringatan protocol unreachable

LAB 51 – Firewall Logging

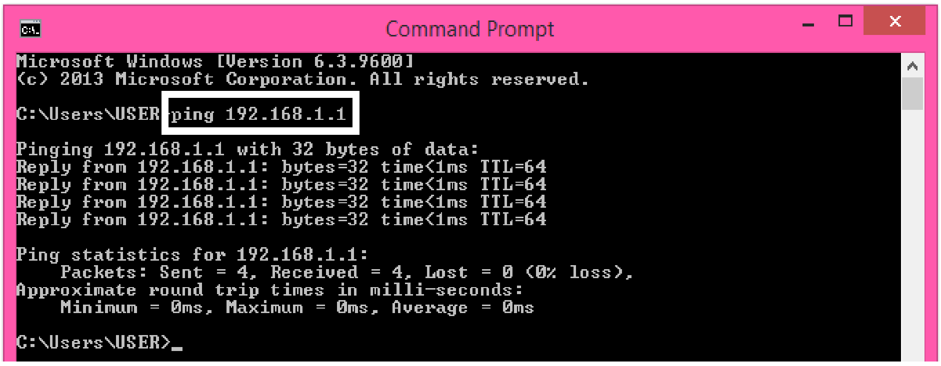
Firewall logging merupakan firewall yang dapat kita gunakan untuk mencatat suatu aktifitas. Misal kita ingin mencatat siapa saja yang melakukan ping ke router kita, mak kita bisa menerapkan firewall logging. Kita memakai topologi yang sama pada lab sebelumnya.

Tujuan kita adalah jika ada client yang mencoba ping ke R1, maka R1 akan mencatat IP Address client yang melakukan ping tersebut

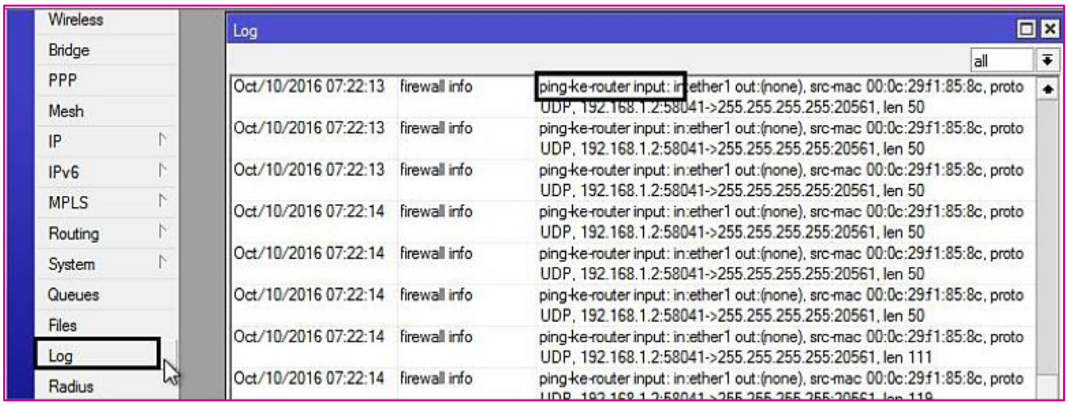


Gambar 51.1 Konfigurasi Firewall Logging

Untuk pengujian lakukan ping dari PC1 ke R1



Gambar 51.2 Ping dari PC1 ke R1

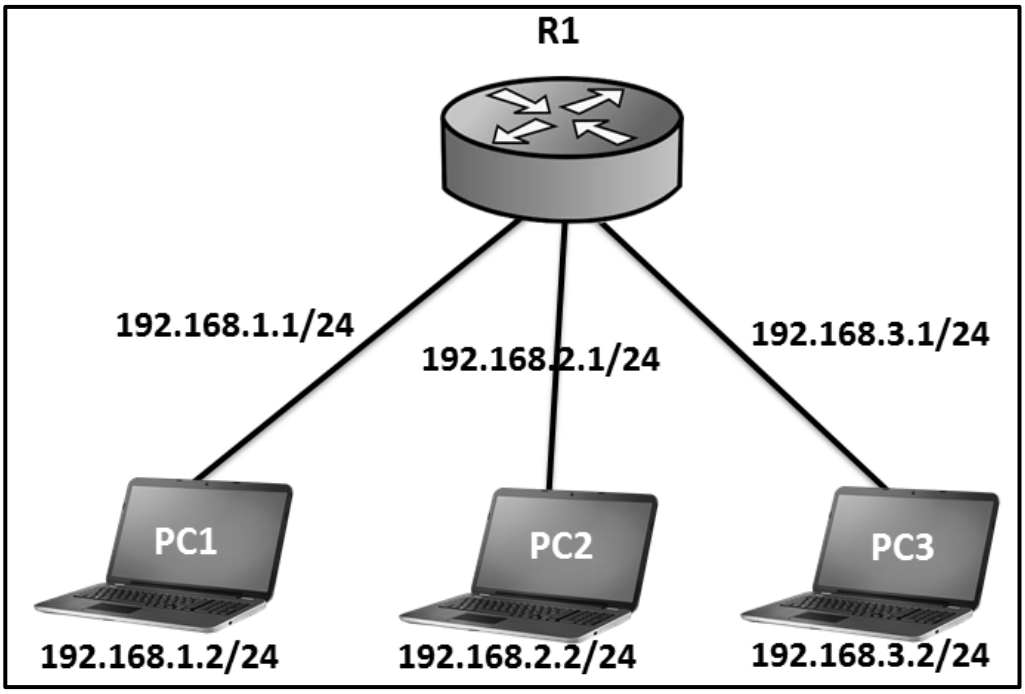


Gambar 51.3 Melihat Log pada R1

Perhatikan pada tabel log bahwa ada sebuah log yang menunjukkan PC1 melakukan ping ke R1

LAB 52 – Firewall Address List

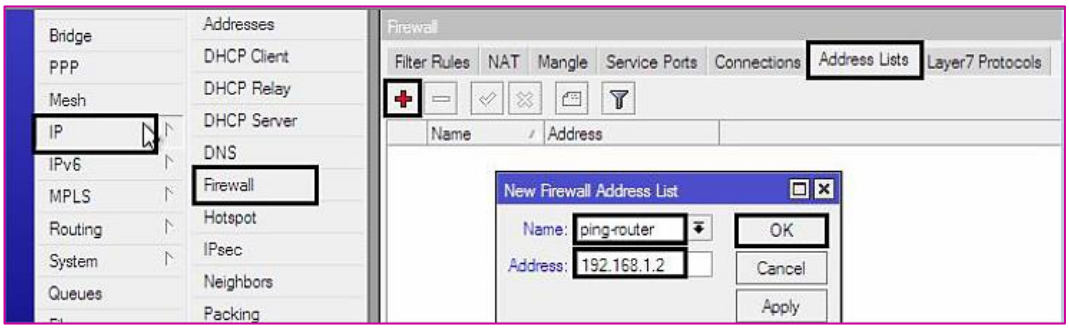
Firewall address list merupakan fitur yang digunakan untuk mengelompokkan beberapa IP Address. Kemudian kita dapat menggunakan kelompok IP Address tersebut ke firewall filter. Berikut contoh kasus yang akan kita selesaikan :



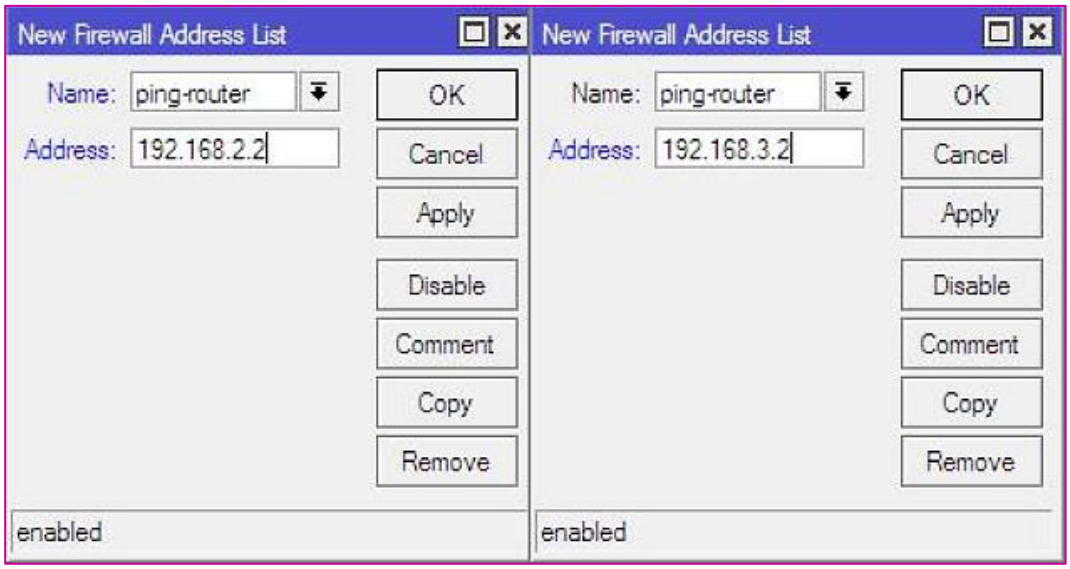
Gambar 52.1 Topologi Jaringan Sederhana

Misal kita ingin agar PC1, PC2 dan PC3 tidak bisa ping ke router. Jika hanya menggunakan firewall filter seperti yang sudah kita bahas pada lab-lab sebelumnya, maka kita akan membutuhkan 3 rule firewall. Namun jika menggunakan address list, kita hanya perlumembuat sebuah rule saja pada firewall filter.

Pertama kita buat terlebih dahulu address list pada R1

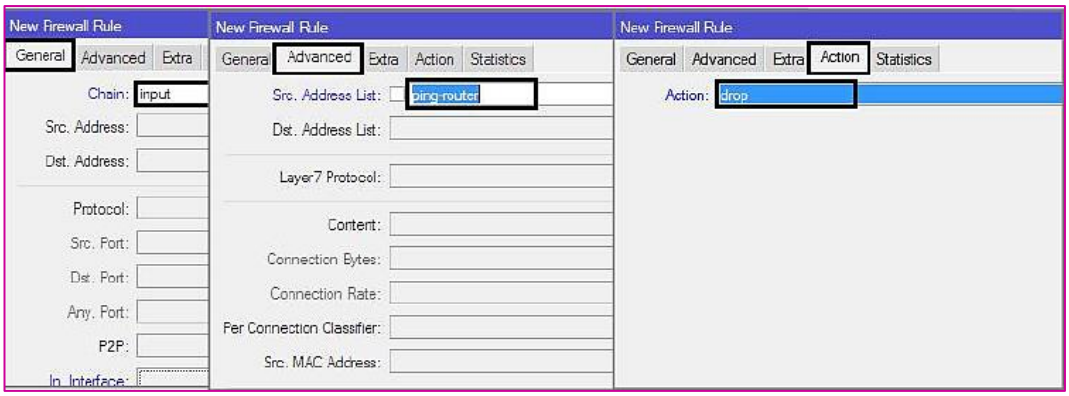


Gambar 52.2 Konfigurasi Address List



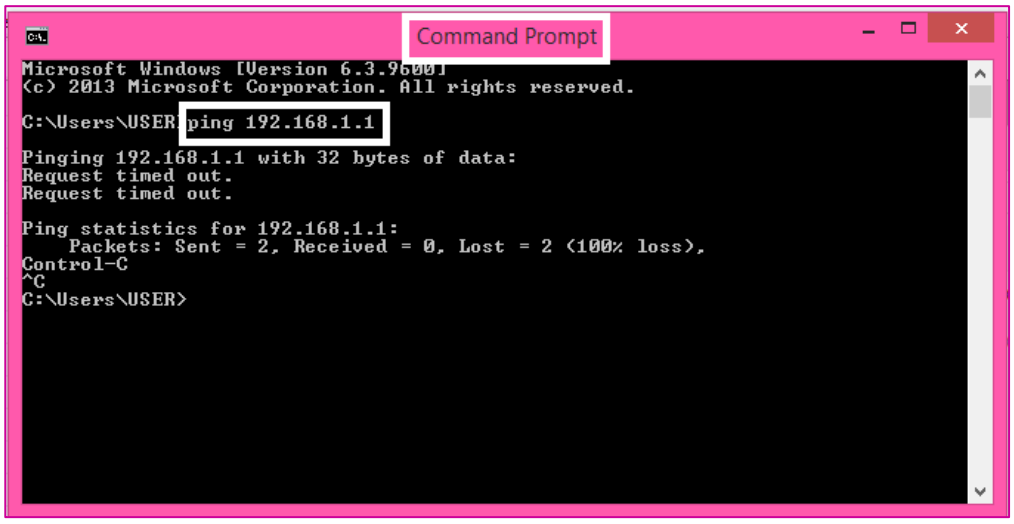
Gambar 52.3 Konfigurasi Address List

Setelah membuat address list seperti diatas, baru kita konfigurasi firewall filter

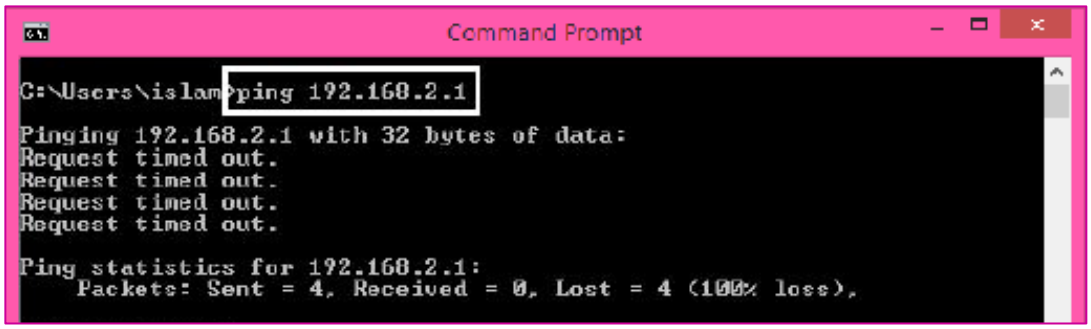


Gambar 52.4 Konfigurasi Firewall Filter

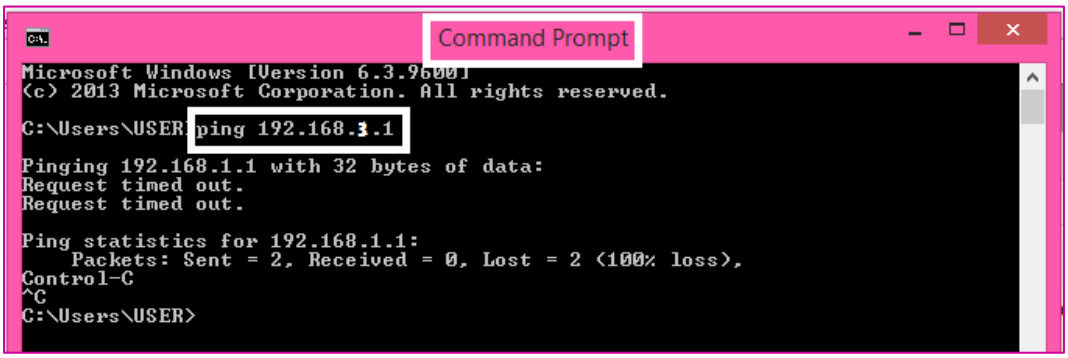
Untuk pengujian, coba lakukan ping dari PC1, PC2 dan PC3



Gambar 52.5 Pengujian Ping dari PC1



Gambar 52.6 Pengujian ping dari PC2

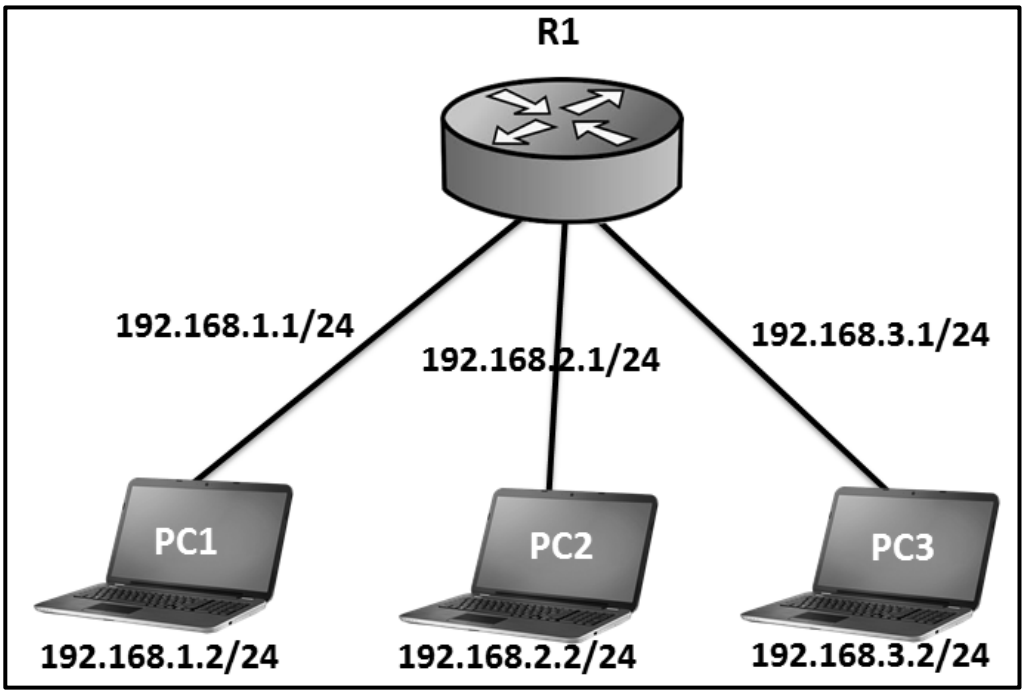


Gambar 52.7 Pengujian ping dari PC3

LAB 53 – Add Source To Address List

Pada lab ini kita akan belajar menggabungkan antara firewall filter dengan address list. Skenarionya adalah jika ada client yang melakukan ping ke router, maka client tersebut akan dimasukkan ke address list. Kemudian kita akan memblokir address list tersebut menggunakan firewall filter.

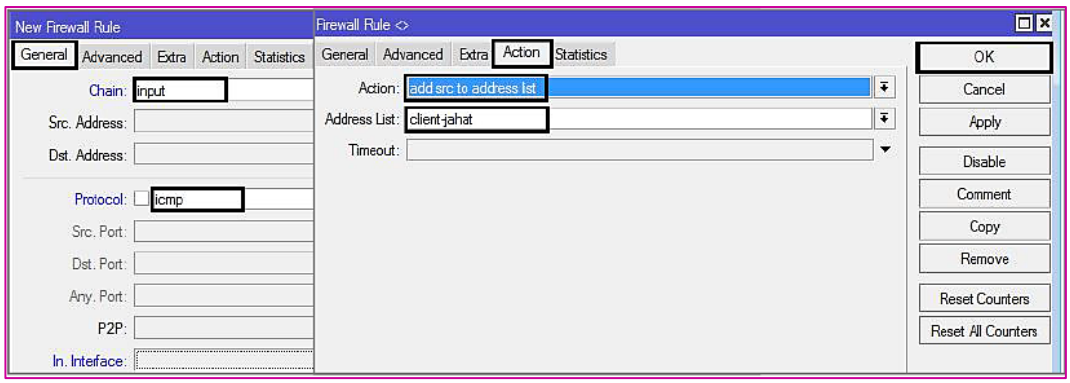
Berikut adalah contoh kasusnya :



Gambar 53.1 Topologi Jaringan Sederhana

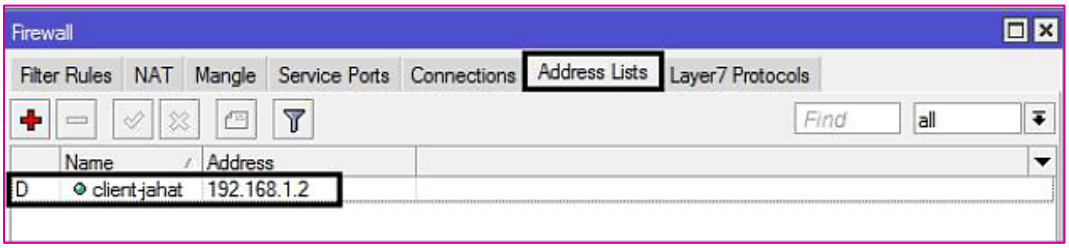
Tujuan kita di lab ini adalah jika sewaktu-waktu ada client yang melakukan ping ke router, maka IP Address tersebut akan dimasukkan address list ***client-jahat.*** Selanjutnya kita akan membuat firewall filter untuk memblokir address list ***client-jahat.***

Pertama kita buat terlebih dahulu firewall filter agar jika ada client yang ping, maka IP Address nya dimasukkan address list.



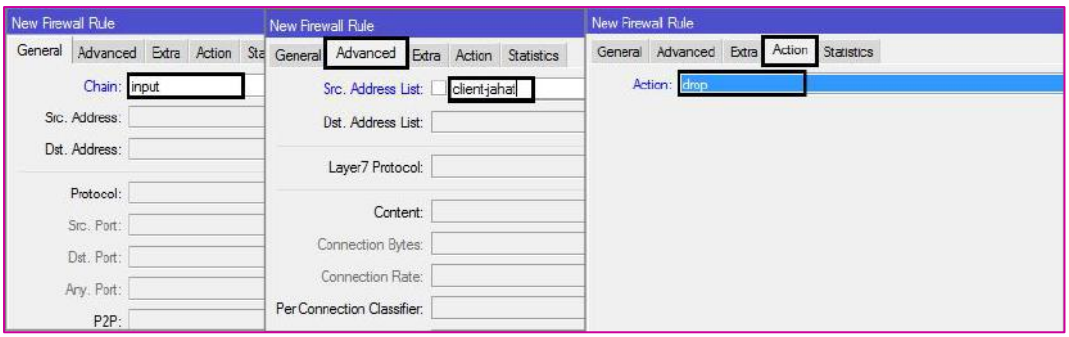
Gambar 53.2 Konfigurasi Filter untuk menambahkan address list

Setelah membuat address list seperti diatas, jika ada client yang ping, maka IP Address client tersebut akan secara otomatis ditambahkan ke address list seperti berikut :



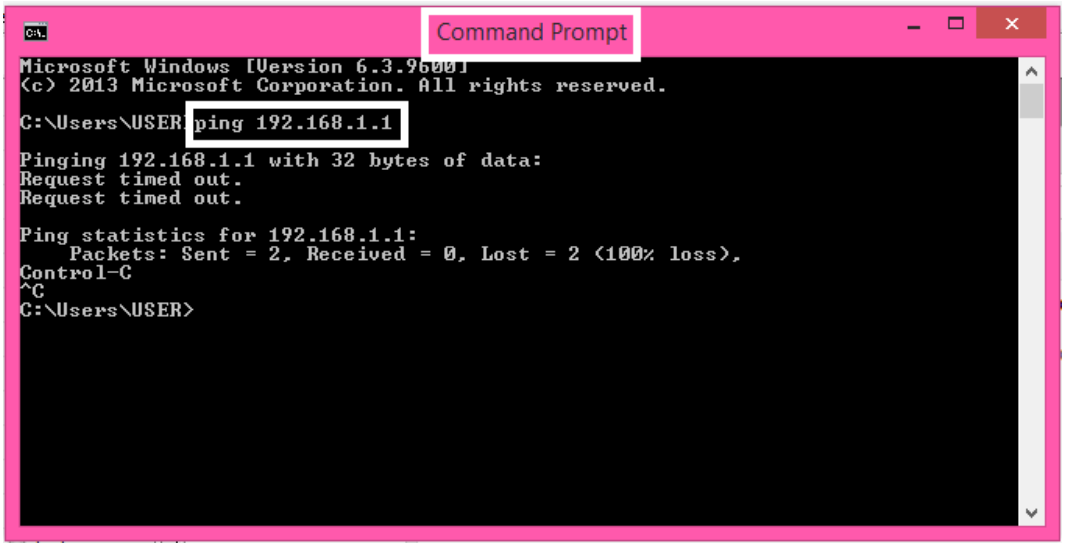
Gambar 53.3 Address List Dynamic

Selanjutnya kita buat firewall filter untuk memblokir paket yang berasal dari client yang ada di address list ***client-jahat*** tersebut.



Gambar 53.4 Konfigurasi Firewall Filter untuk blokir client-jahat

Untuk pengujian coba lakukan ping dari client ke router.

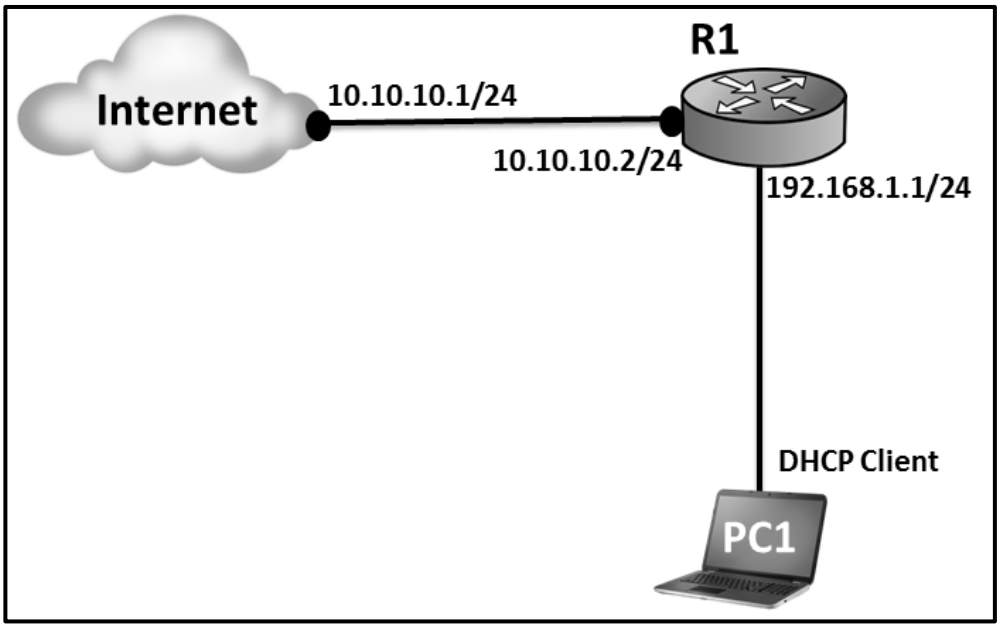


Gambar 53.5 Client gagal melakukan ping ke router

LAB 54 – Firewall NAT Action src-nat

Firewall NAT dengan action **scr-nat** digunakan untuk merubah alamat IP sumber **(source address)** dengan metode satu ke satu.

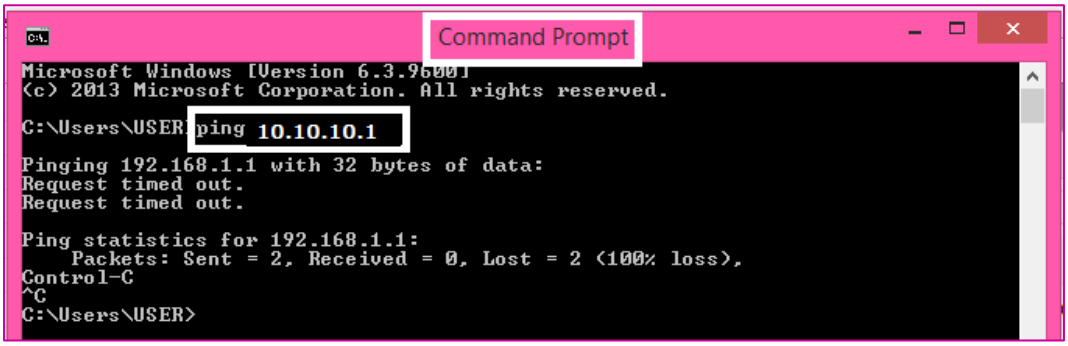
Berikut adalah contoh kasus yang akan kita selesaikan :



Gambar 54.1 Topologi NAT Action src-nat

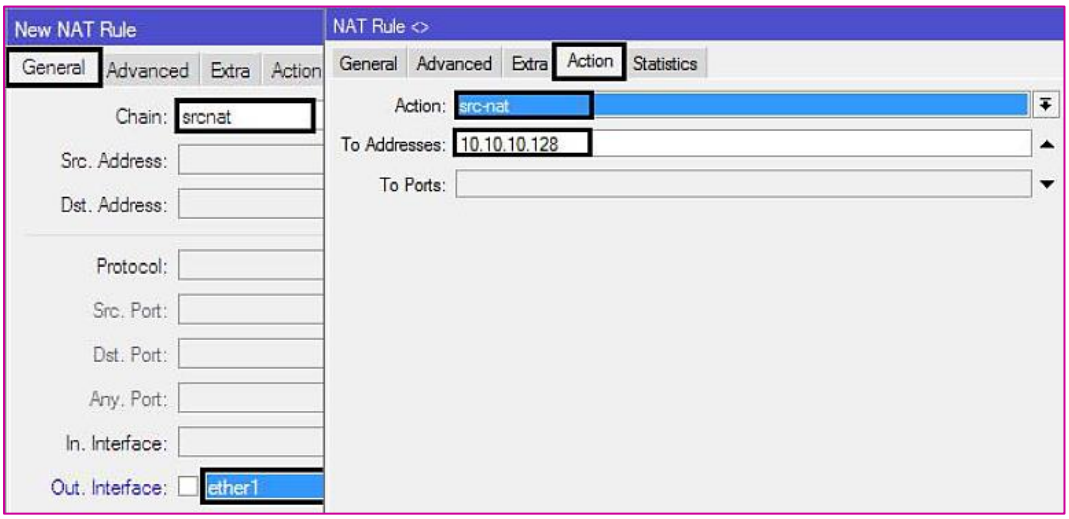
Pada contoh kasus seperti diatas, kita harus mengkonfigurasi NAT dengan action src-nat agar client bisa terhubung ke jaringan internet. Jika kita tidak mengkonfigurasi scr-nat, maka client tidak akan bisa terhubung. Hal ini dikarenakan IP Private tidak akan bisa berkomunikasi dengan IP Public. Satu-satunya cara agar IP Private bisa berkomunikasi dengan IP Public adalah merubah IP Address sumber (source address) menjadi IP Public.

Diasumsikan kita telah mengkonfigurasi seperti topologi diatas. Selanjutnya kita hanya fokus pada konfigurasi firewall NAT dengan action src-nat. Perhatikan gambar berikut yang menunjukkan bahwa client tidak bisa ping ke internet sebelum di konfigurasi src-nat.



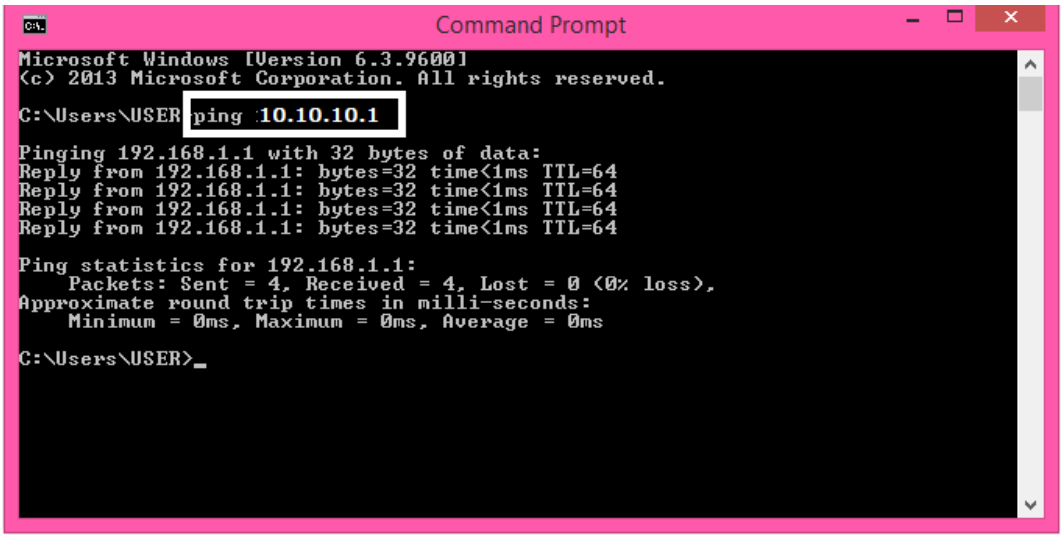
Gambar 54.2 PC1 gagal ping ke internet

Selanjutnya kita coba konfigurasi firewall NAT ation src-nat



Gambar 54.3 Konfigurasi Firewall NAT Action src-nat

Berikut percobaan ping dari PC1 ke internet setelah dikonfigurasikan firewall NAT action src-nat.

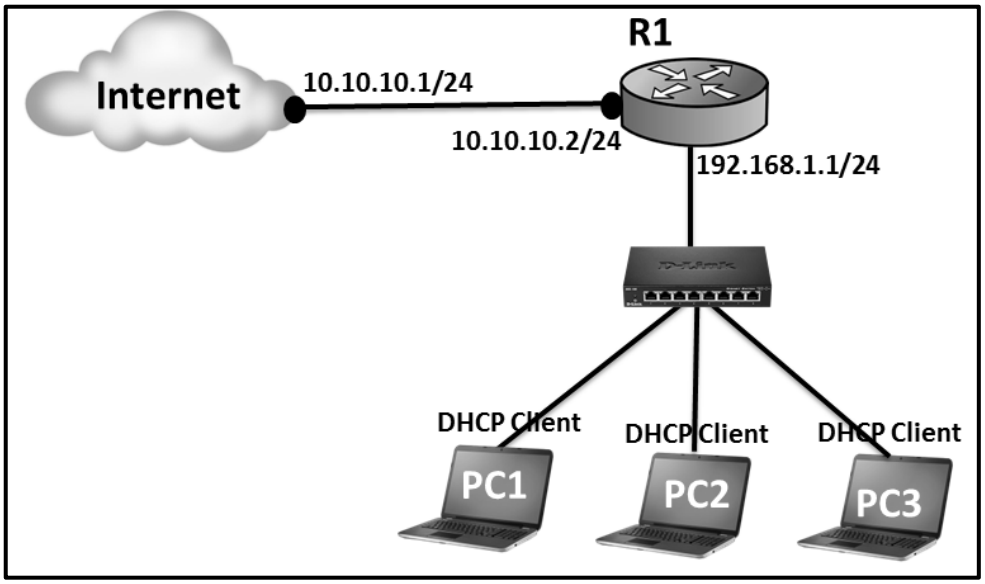


Gambar 54.4 PC1 berhasil ping ke internet

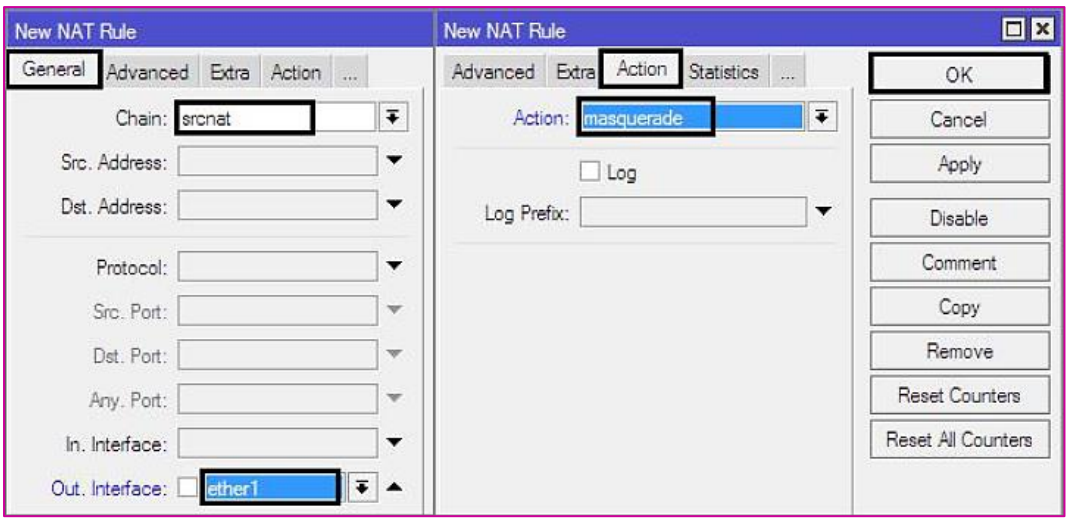
LAB 55 – Firewall NAT Action Masquerade

Firewall NAT dengan action masquerade hampir sama dengan action src-nat. Yaitu merubah IP Address sumber (source address). Hanya saja **action masquerade kita gunakan saat jumlah client yang kita miliki lebih dari satu.**

Berikut adalah topologi yang akan kita gunakan :



Gambar 55.1 Topologi Jaringan Sederhana

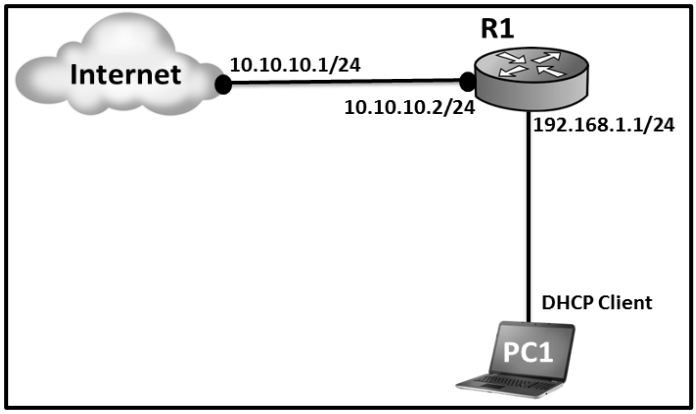


Gambar 55.2 Konfigurasi Firewall NAT Action Masquerade

Firewall masquerade seperti diatas digunakan untuk merubah IP Private menjadi IP Public, **dengan catatan IP Private yang dirubah lebih dari satu.**

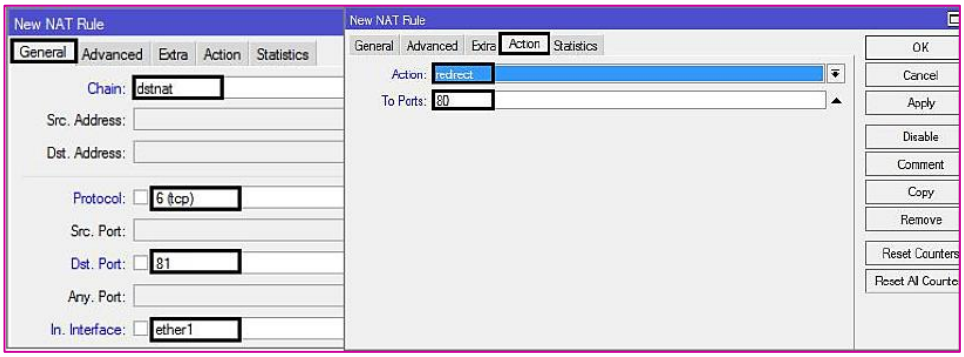
LAB 56 – Firewall NAT Action Redirect

Firewall NAT dengan action redirect digunakan untuk merubah alamat IP tujuan menjadi router sendiri. Contoh kasusnya seperti berikut :



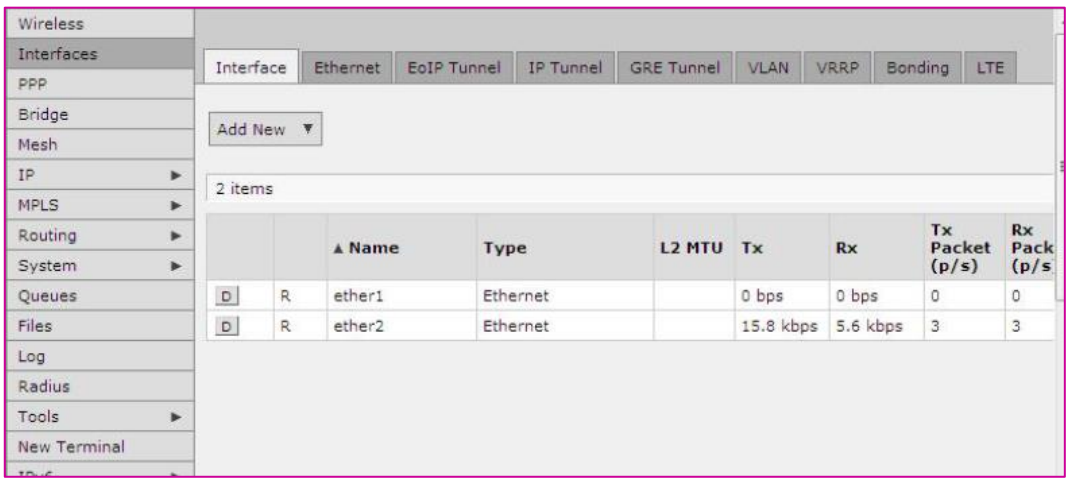
Gambar 56.1 Topologi Jaringan Sederhana

Kita menginginkan agar saat ada orang lain mengakses IP Public kita (10.10.10.2) dengan port 81, akan diarahkan ke router itu sendiri dengan port 80. Maka kita bisa menggunakan firewall NAT dengan action redirect.



Gambar 56.2 Konfigurasi Firewall NAT Action Redirect

Setelah mengkonfigurasi firewall NAT, maka pada saat orang lain mengakses IP Public kita (10.10.10.2) dengan port 81 akan diarahkan ke port 80.

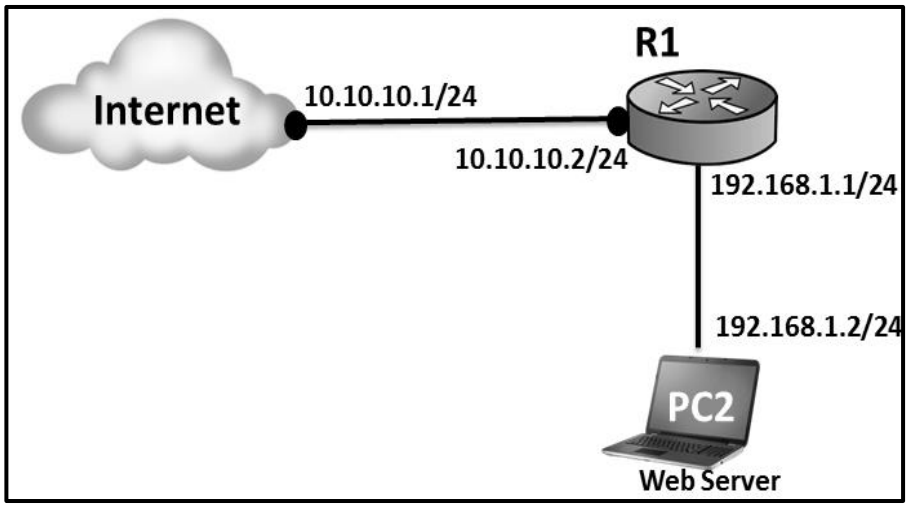


Gambar 56.3 Access Port 81 di redirect ke port 80

LAB 57 – Firewall NAT Action dst-nat

Firewall NAT dengan action dst-nat digunakan untuk merubah IP Address tujuan (destination address).

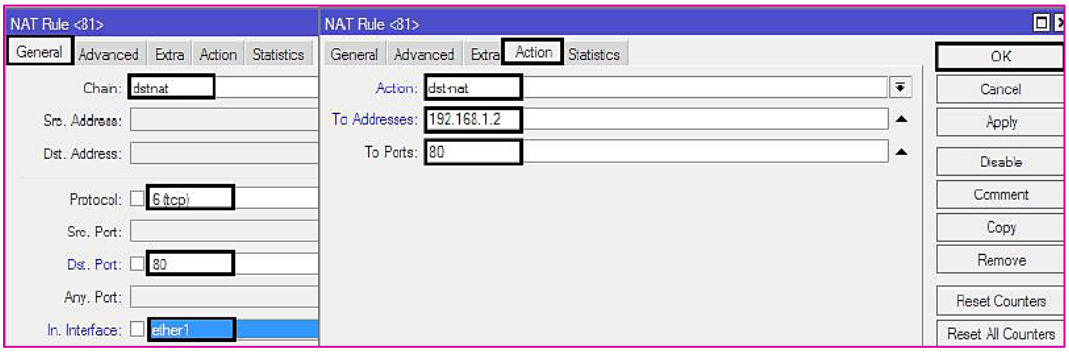
Berikut adalah contoh kasusnya :



Gambar 57.1 Topologi Firewall NAT Action dst-nat

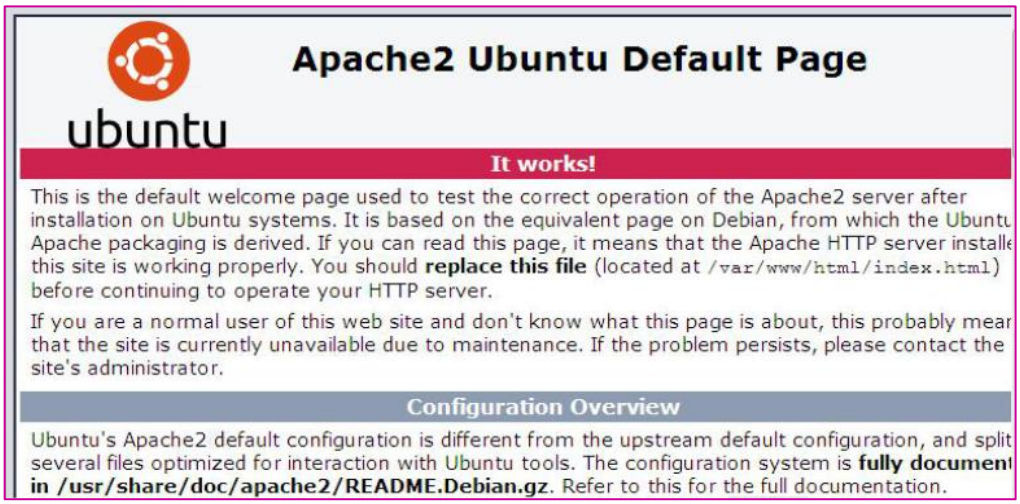
Tujuan kita pada lab ini adalah agar pada saat ada orang lain mengakses IP Public kita dengan port 80, maka akan diarahkan ke web server yang dimiliki IP Private.

Berikut adalah konfigurasi firewall NAT pada R1 untuk mengerjakan contoh kasus diatas.



Gambar 57.2 Konfigurasi Firewall NAT action dst-nat

Setelah mengkonfigurasi firewall dst-nat seperti diatas, saat orang lain mengakses IP Public kita, maka akan diarahkan ke web server lokal kita.



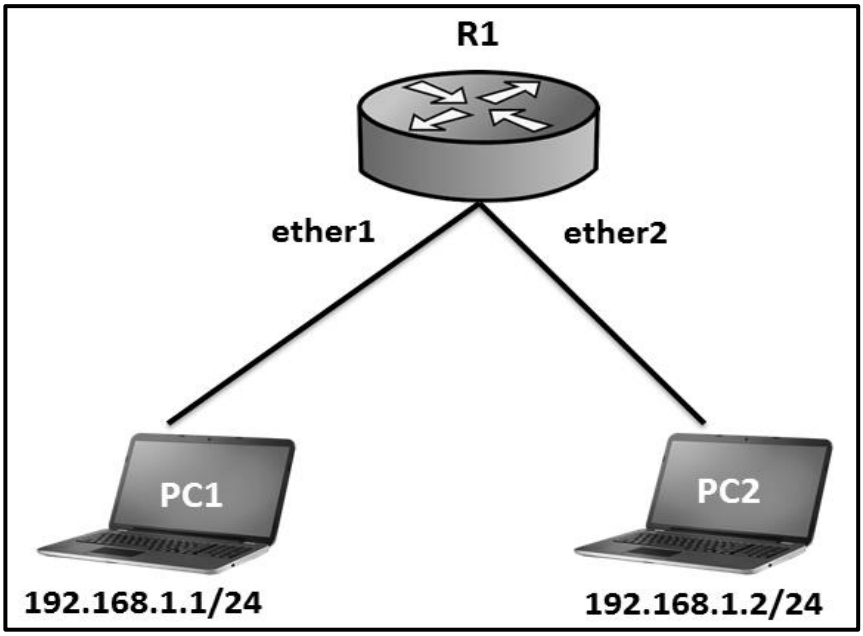
Gambar 57.3 Akses ip publik akan di redirect (dialihkan) ke web server lokal

BAB V

Bridge Mikrotik

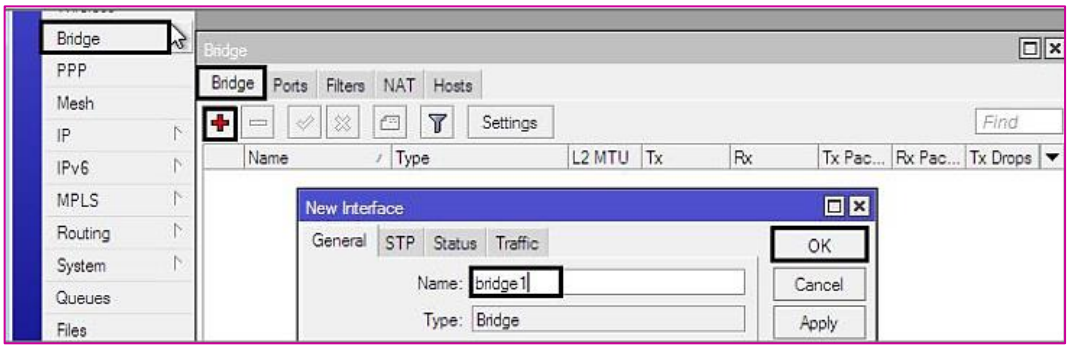
LAB 58 – Bridge Skenario 1

Pada lab ini kita akan belajar tentan bridge di mikrotik dengan berbagai skenario. Berikut skenario pertama yang akan kita gunakan :

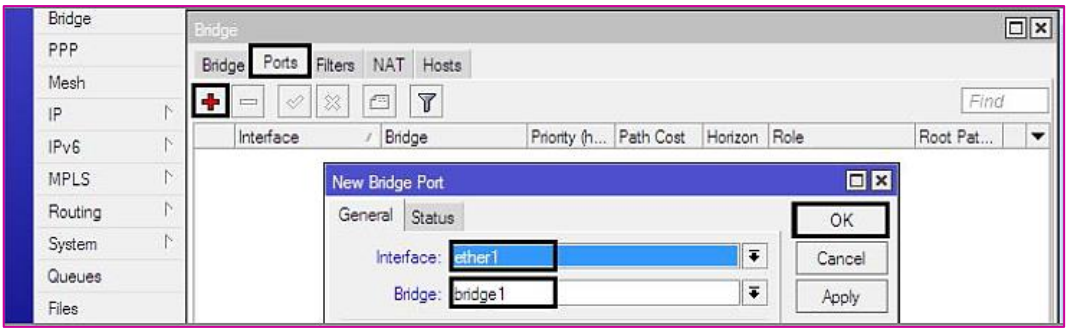


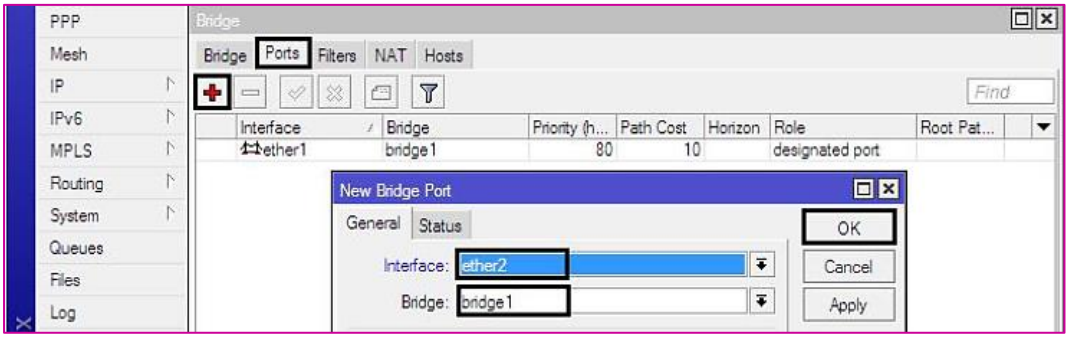
Gambar 58.1 Topologi Jaringan Bridge

Dengan mengkonfigurasi bridge, maka PC1 dan PC2 akan bisa saling berkomunikasi tanpa melalui proses routing, meskipun PC1 dan PC2 tersebut terhubung pada interface router yang berbeda. Berikut konfigurasi bridge pada R1



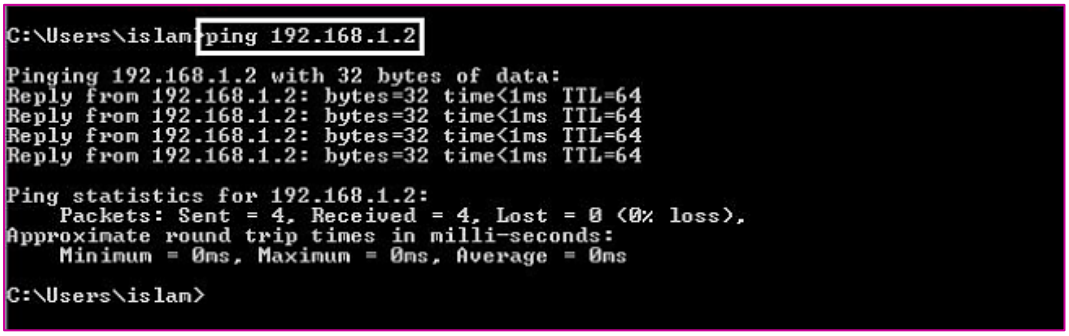
Gambar 58.2 Menambahkan interface bridge





Gambar 58.3 Menambahkan interface ke interface bridge

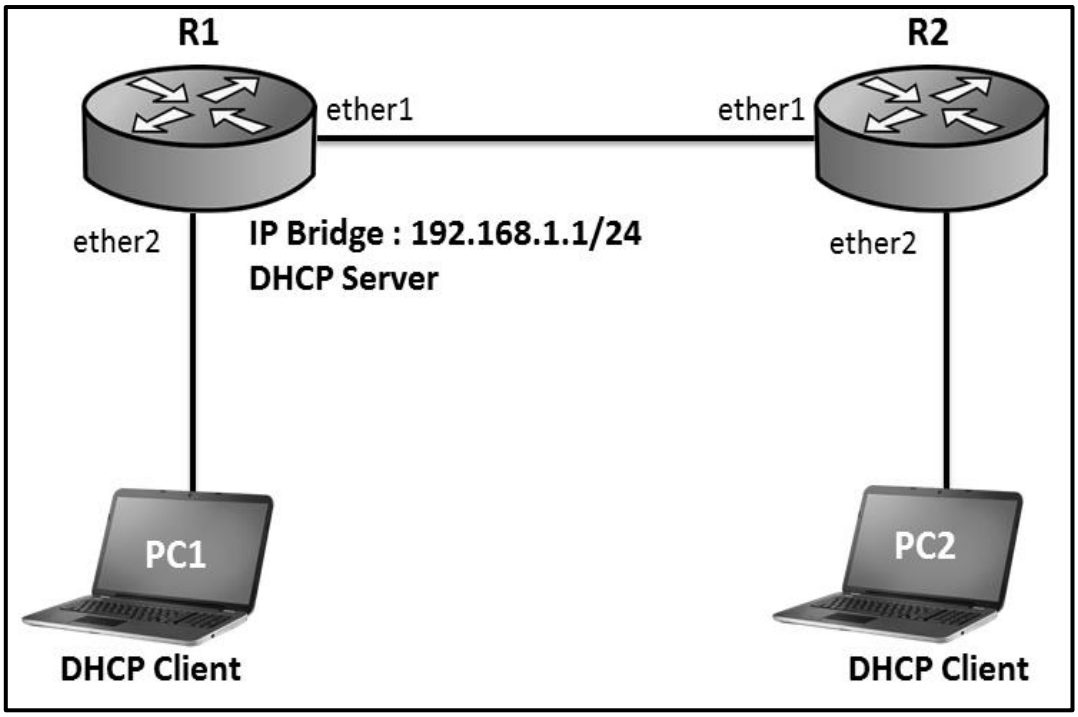
Setelah mengkonfigurasi bridge seperti diatas. Maka PC1 akan langsung bisa berkomunikasi dengan PC2



Gambar 58.5 Pengujian Ping dari PC1 ke PC2

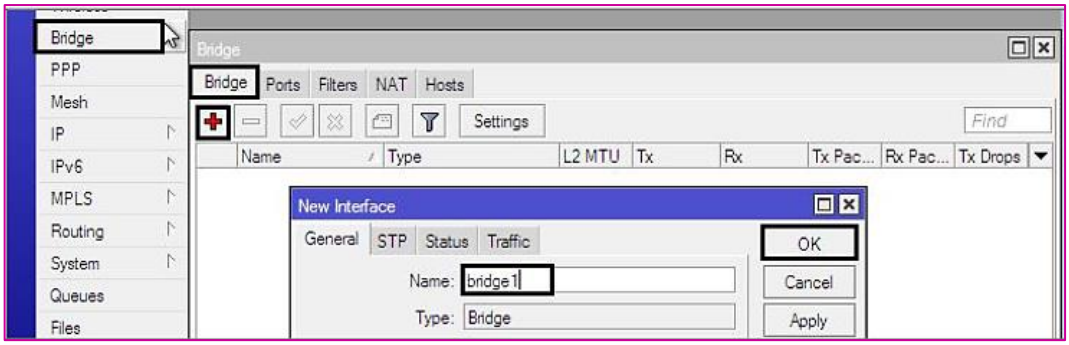
LAB 59 – Bridge Skenario 2

Sebenernya untuk konfigurasi bridge hanya itu saja. Tidak akan ada konfigurasi bridge yang istimewa. Hanya saja bridge bisa digunakan pada berbagai skenario. Berikut skenario yang akan kita gunakan :

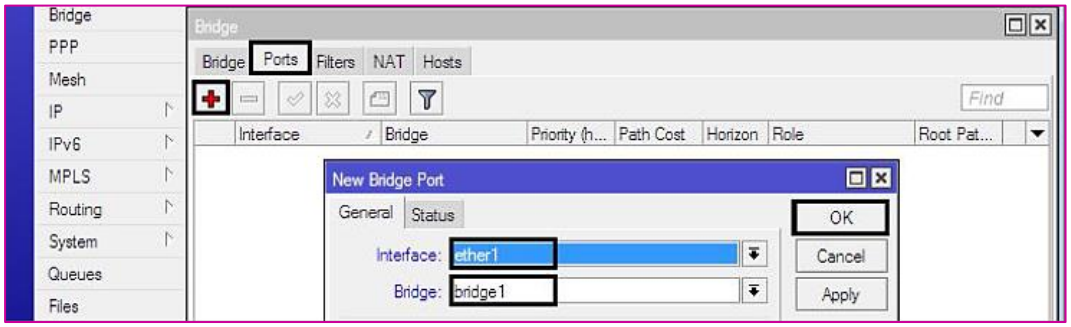


Gambar 59.1 Topologi Bridge Skenario 2

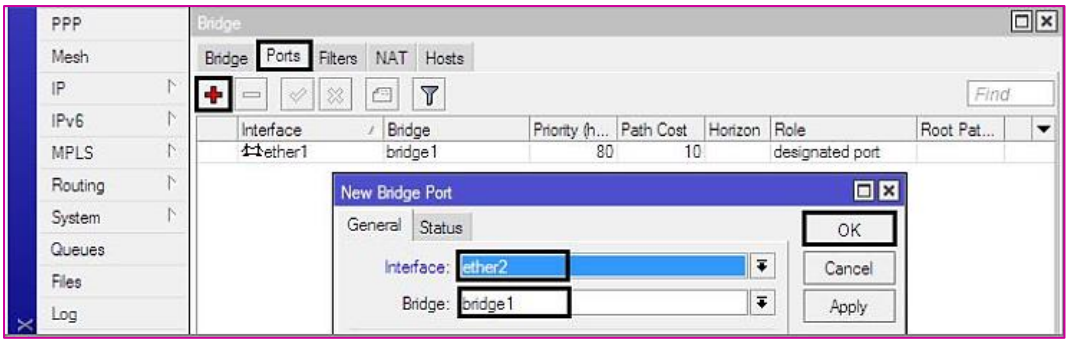
Pada skenario diatas, kita akan mengkonfigurasi bridge pada R1 dab R2 untuk melakukan bridge pada interface **ether1** dan **ether2.** Selanjutnya kita akan menambahkan IP Address 192.168.1.1/24 pada interface bridge di R1 dan mengaktifkan DHCP Server. Dengan konfigurasi sepert diatas, maka PC1 dan PC2 akan mendapatkan DHCP Client dari R1. Berikut konfigurasi pada R1 :



Gambar 59.2 Menambahkan interface bridge pada R1

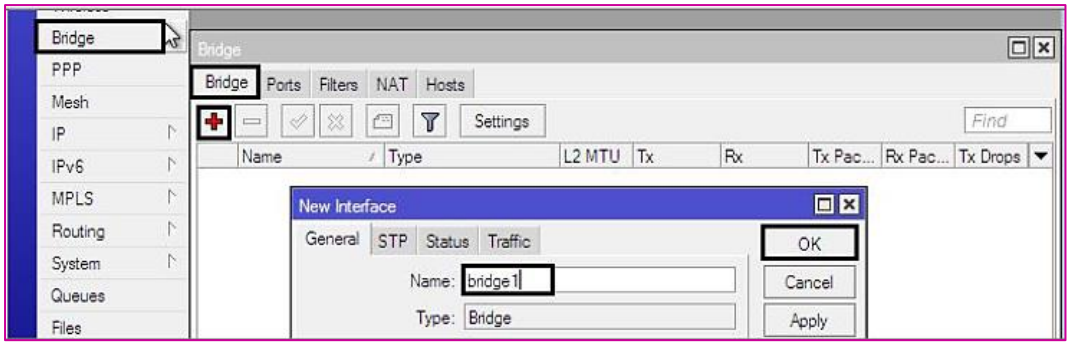


Gambar 59.3 Menambahkan interface bridge pada R1

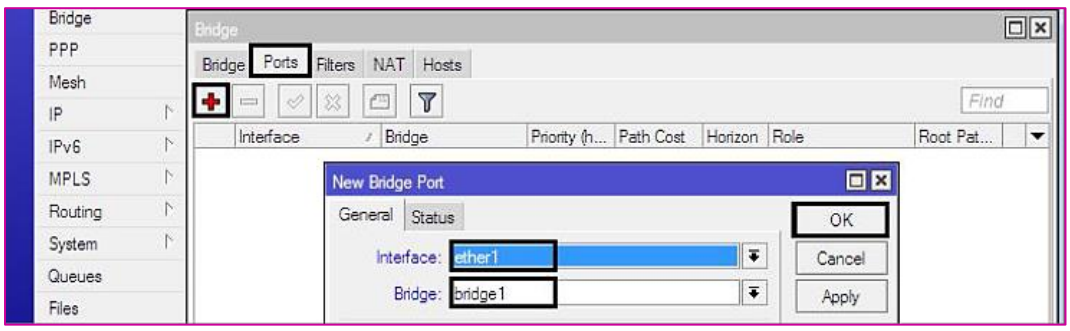


Gambar 59.4 Menambahkan interface bridge pada R1

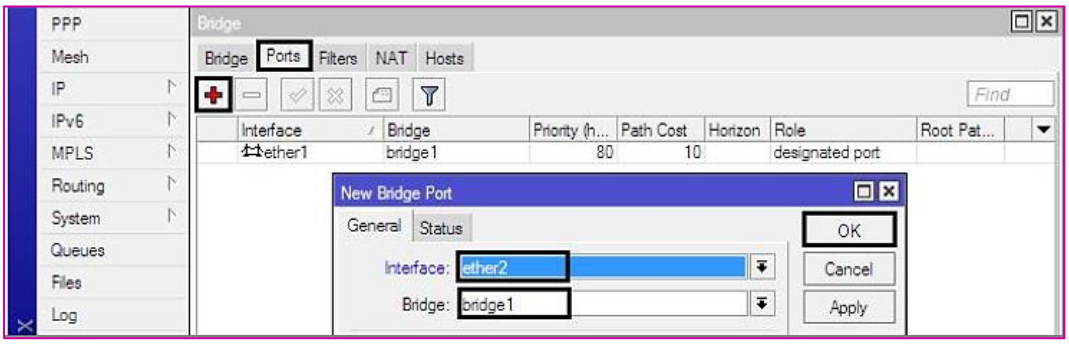
Berikut konfigurasi pada R2



Gambar 59.5 Menambahkan interface bridge pada R2

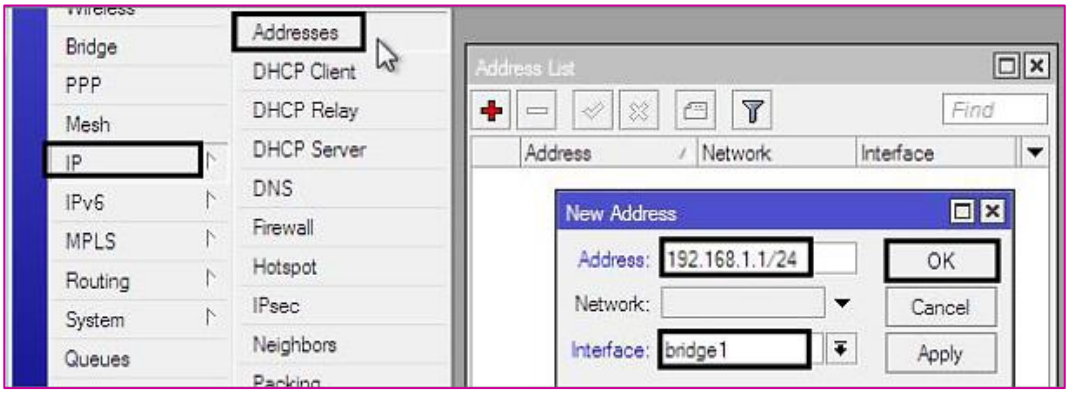


Gambar 59.6 Menambahkan interface bridge pada R2



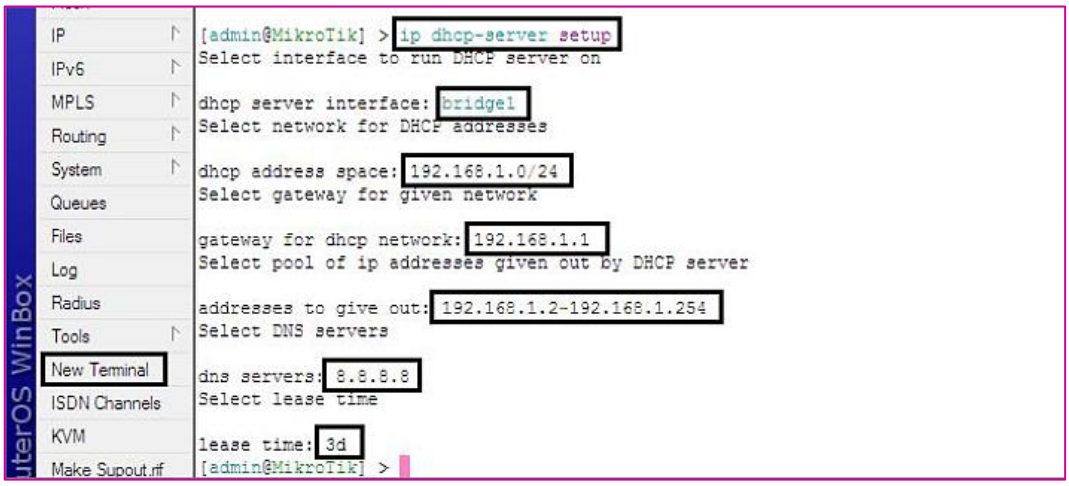
Gambar 59.7 Menambahkan interface bridge pada R2

Selanjutnya lakukan konfigurasi IP Address pada interface bridge di R1



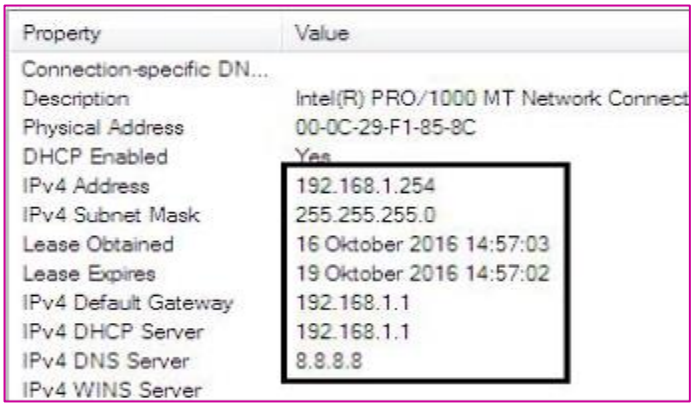
Gambar 59.8 Konfigurasi IP Address di interfaxe bridge R1

Terakhir kita aktifkan DHCP Server pada interface bridge R1 tersebut

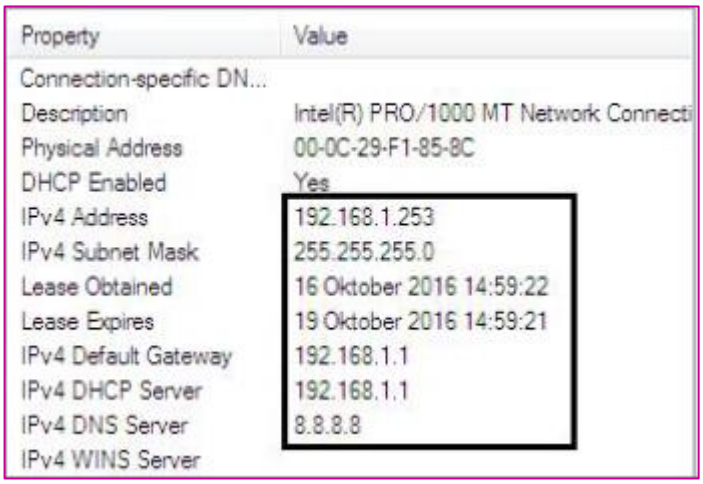


Gambar 59.9 Konfigurasi DHCP Server di R1

Untuk pengujian kita coba lakukan DHCP Client pada PC1 dan PC2

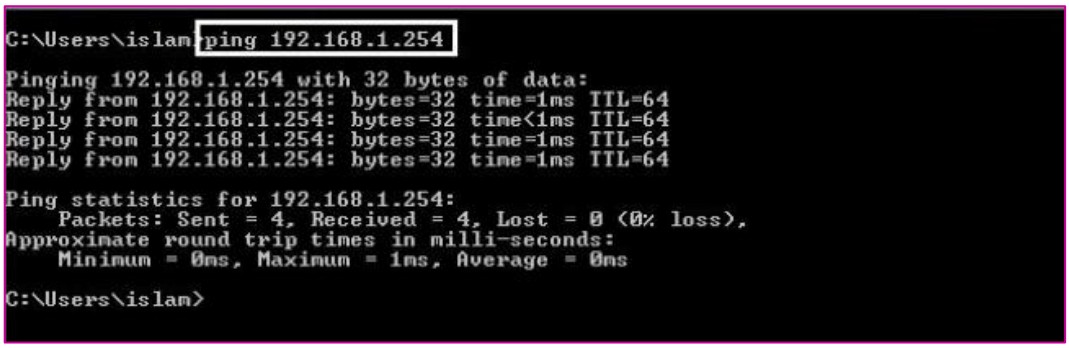


Gambar 59.10 DHCP Client pada PC1



Gambar 59.11 DHCP Client pada PC1

Perhatikan bahwa kedua PC mendapat IP **secara dynamic** dari R1. Selanjutnya coba lakukan ping dari PC1 ke PC2 atau sebaliknya.



Gambar 59.12 Pengujian ping dari PC2 ke PC1

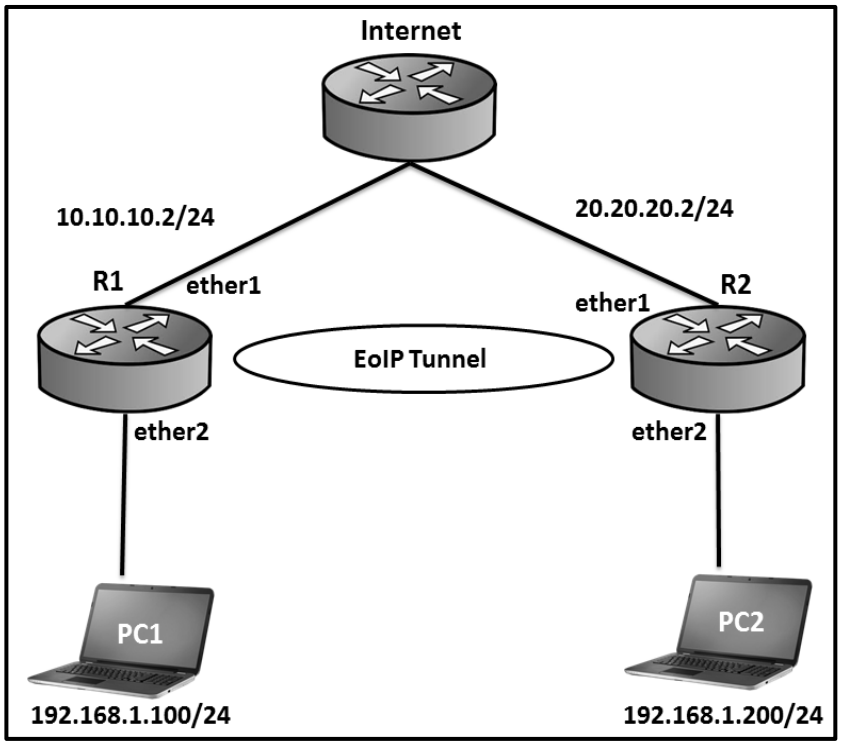
Perhatikan bahwa PC2 sudah berhasil melakukan ping ke PC1. Sampai disini kita sudah selesai dan berhasil melakukan konfigurasi pada bridge skenario 2.

BAB VI

Mikrotik Tunnel

LAB 60 – EoIP Tunnel

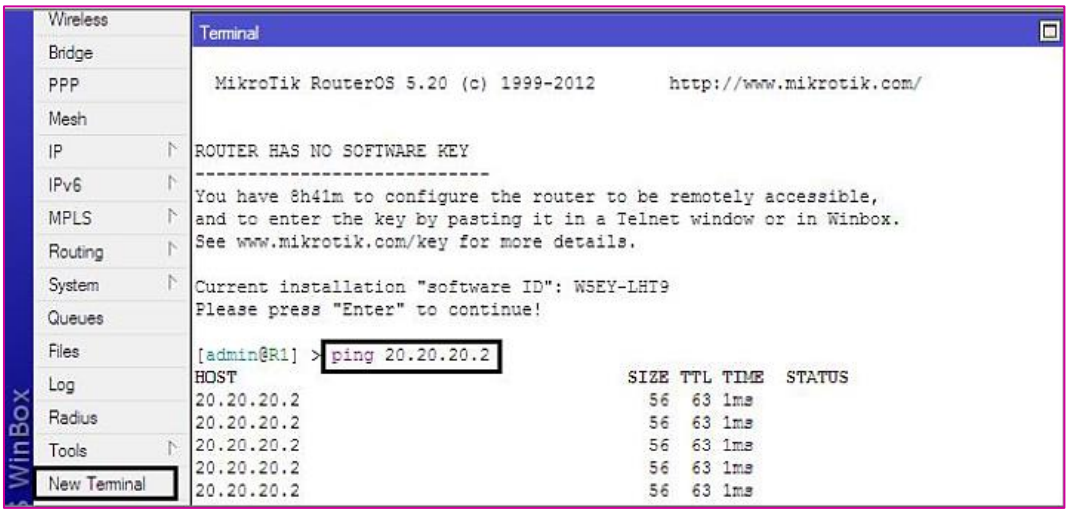
Berikut adalah topologi yang akan kita gunakan pada lab ini :



Gambar 60.1 Topologi EoIP Tunnel

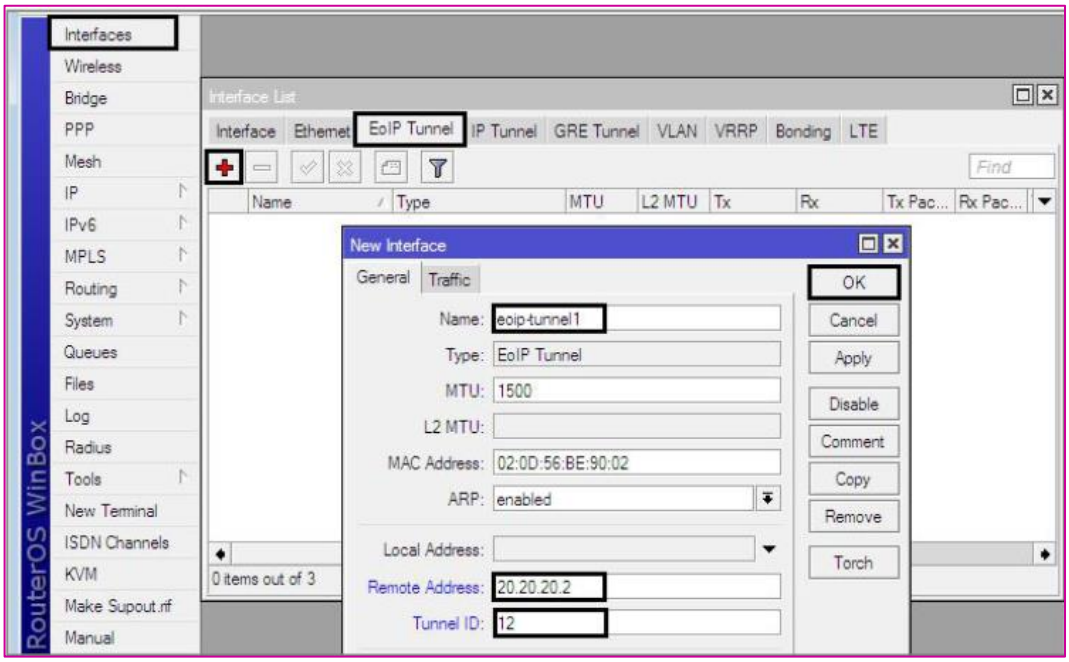
Pada lab diatas, tujuan kita adalah menghubungkan PC1 dan PC2 yang masing-masing mempunyai IP Private. Jika tidak menggunakan EoIP Tunnel, maka PC1 tidak akan bisa saling berkomunikasi, karena kedua PC tersebut menggunakan IP Address Private.

Syarat utama untuk konfigurasi EoIP Tunnel adalah kedua router harus memiliki IP Address Public dan bisa saling berkomunikasi.



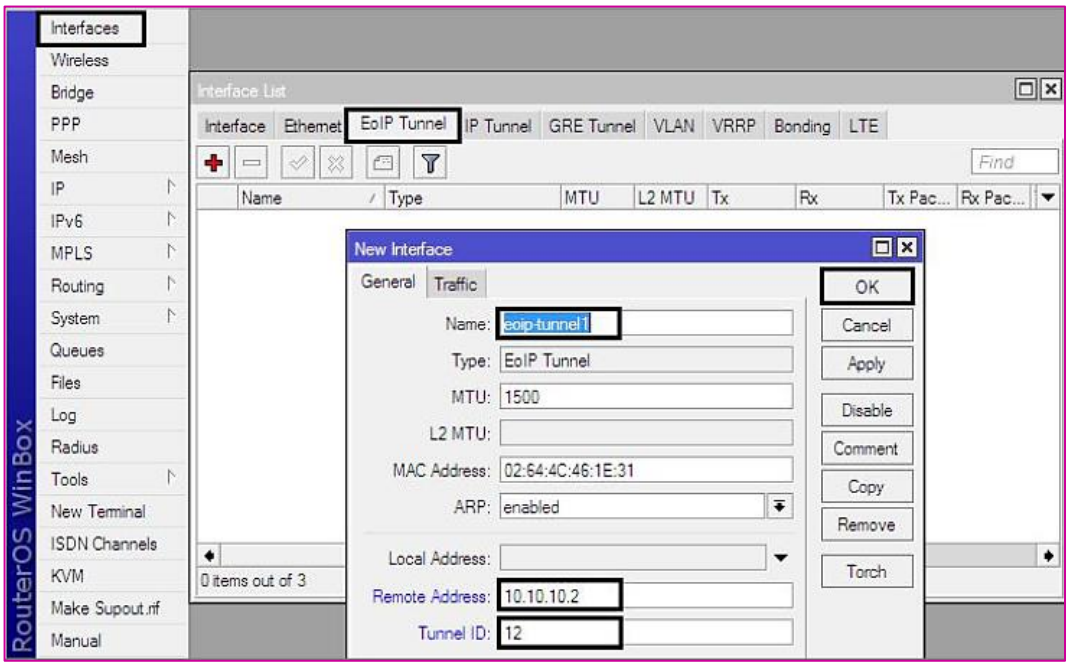
Gambar 60.2 Ping dari R1 ke R2

Setelah dipastikan R1 dan R2 sudah bisa saling berkomunikasi, langkah selanjutnya adalah mengkonfigurasi EoIP Tunnel. Berikut konfigurasi EoIP Tunnel pada R1



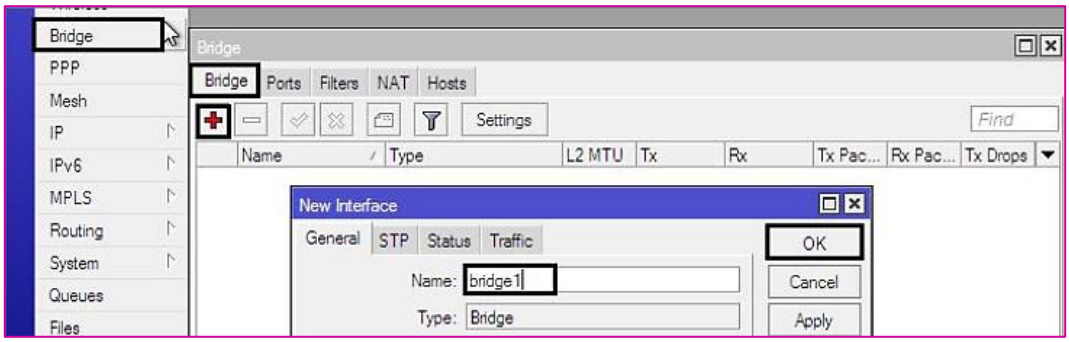
Gambar 60.3 Konfigurasi EoIP di R1

Selanjutnya untuk konfigurasi EoIP pada R2 adalah sebagai berikut :

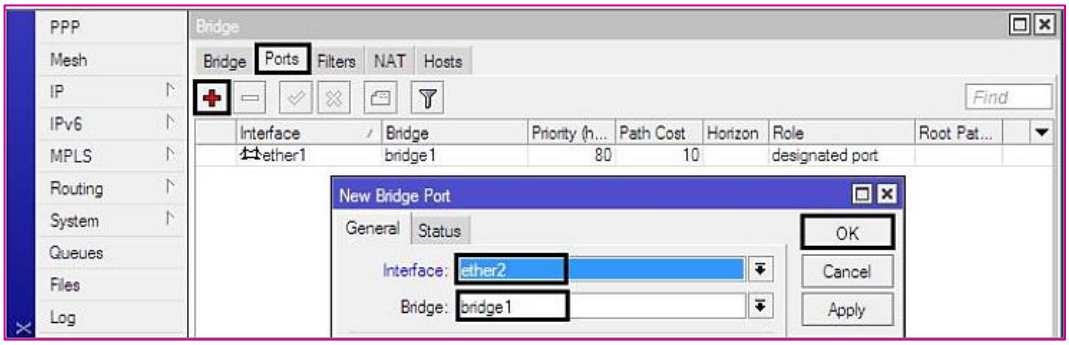


Gambar 60.4 Konfigurasi EoIP di R2

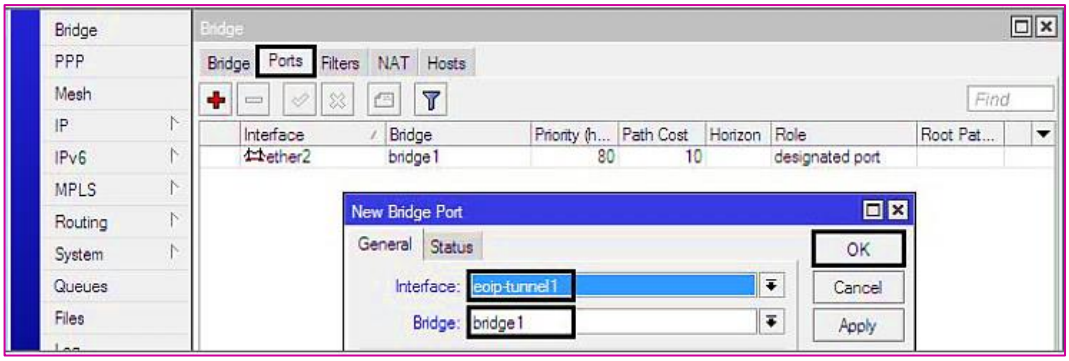
Langkah selanjutnya adalah melakukan bridge interface yang terhubung ke client dengan interface EoIP pada R1 dan R2



G ambar 60.7 Menambahkan interface EoIP ke bridge di R1

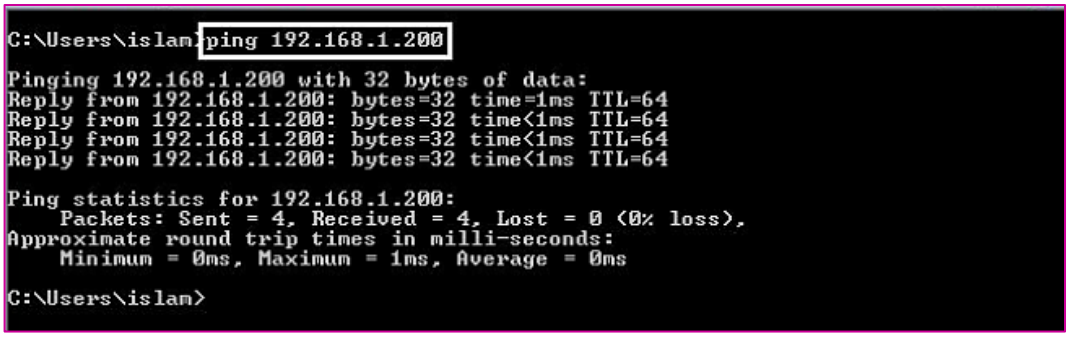


Gambar 60.6 Menambahkan interface EoIP ke bridge di R1



Gambar 60.7 Menambahkan interface EoIP ke bridge di R1

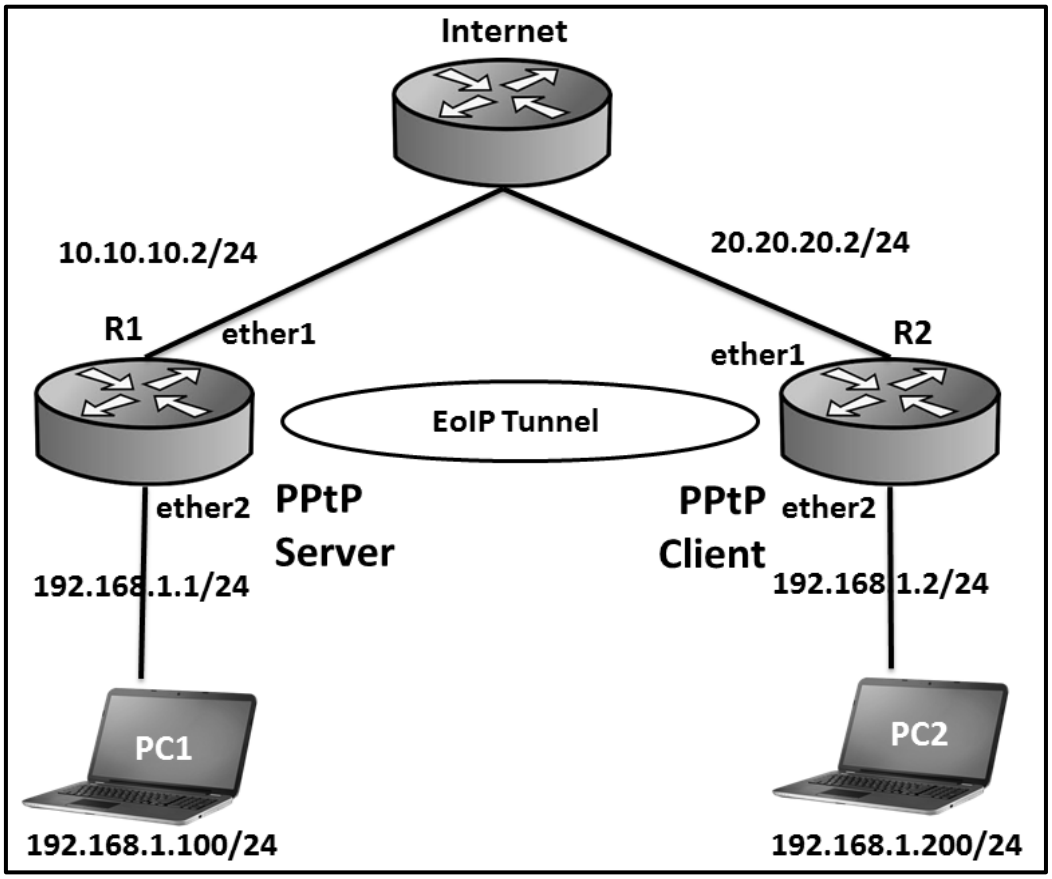
Lakukan langkah yang sama seperti diatas pada R2, selanjutnya untuk pengujian lakukan ping dari PC1 ke PC2



Gambar 60.8 Pengujian ping dari PC1 ke PC2

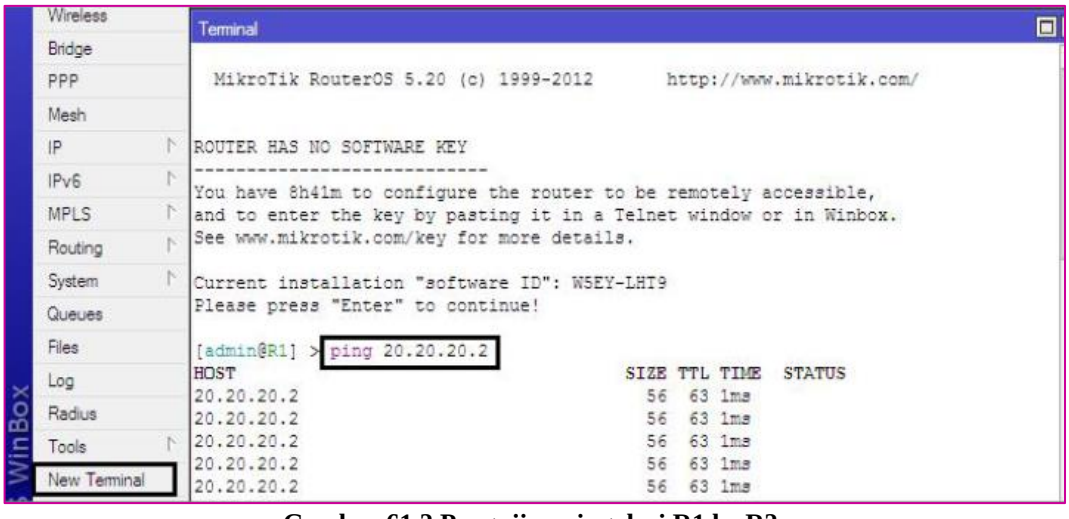
LAB 61 – PPtP Tunnel

Selanjutnya pada lab ini kita akan belajar tentang PPtP, berikut adalah topologi yang akan kita gunakan pada lab ini :



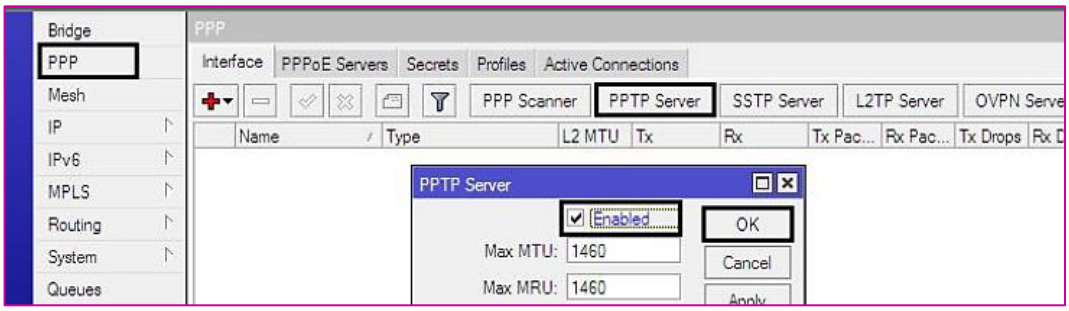
Gambar 61.1 Topologi PPtP Tunnel

Tujuan kita adalah sama dengan lab sebelumnya, yaitu menghubungkan PC1 dan PC2 yang berada dijaringan **private** melalui jaringan **public** (internet). Hanya saja pada lab ini kita akan menggunakan PPtP. Pertama pastikan R1 dan R2 sudah bisa salinng berkomunikasi menggunakan IP Public.

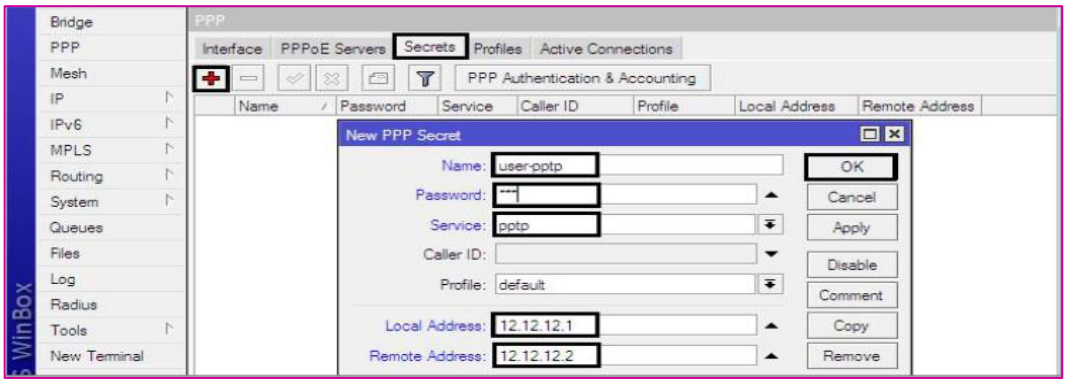


Gambar 61.2 Pengujian ping dari R1 ke R2

Setelah dipastikan R1 dan R2 bisa ping, selanjutnya PPtP Server pada R1 sebagai berikut :

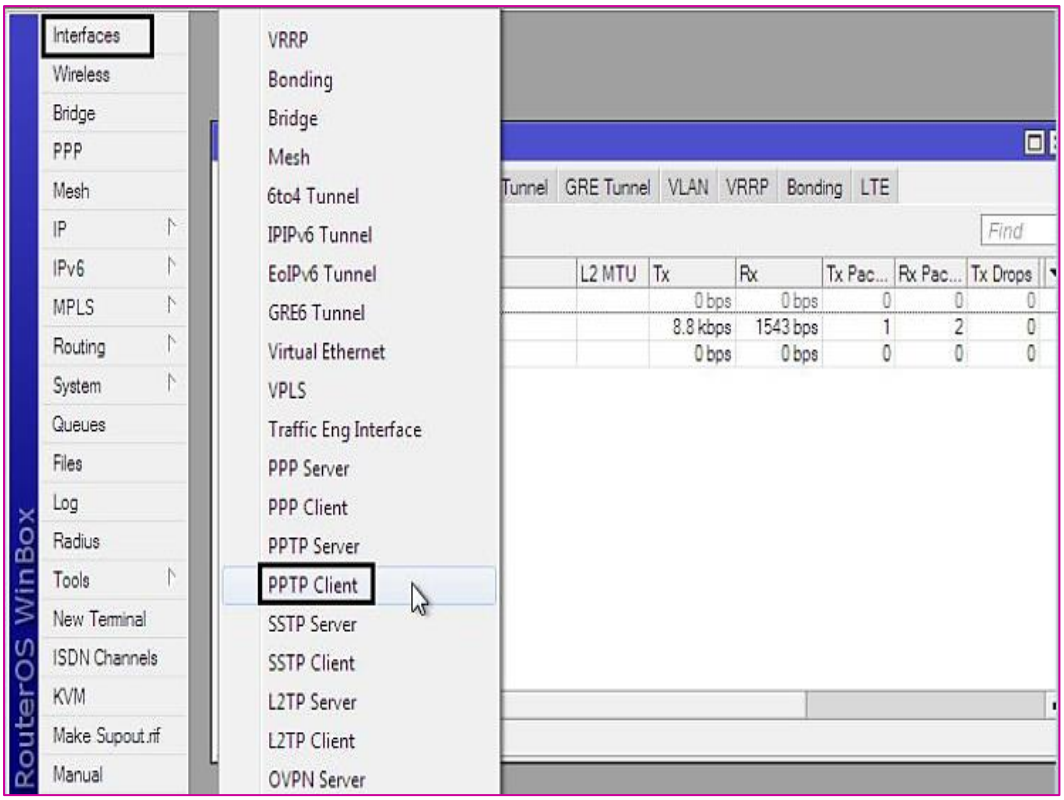


Gambar 61.3 Konfigurasi PPtP Server di R1

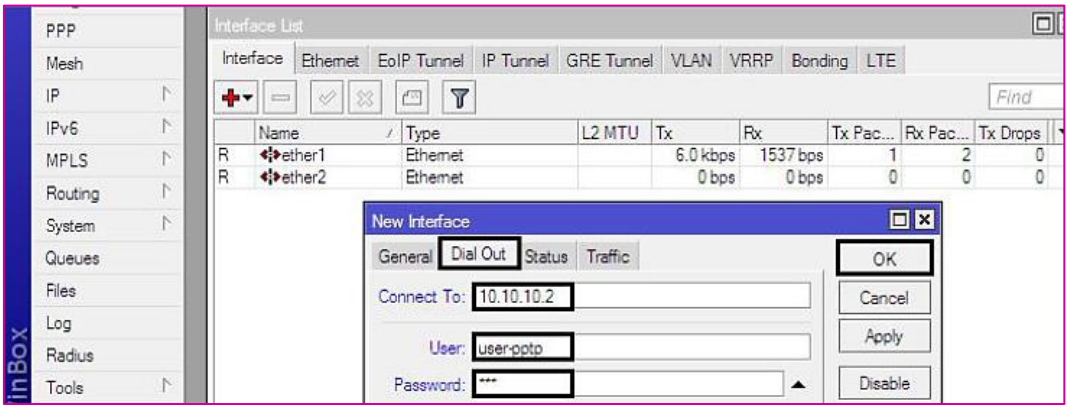


Gambar 61.4 Konfigurasi user pada PPtP Server

Sampai disini kita sudah selesai mengkonfigurasi PPtP server di R1. Selanjutnya lakukan konfigurasi PPtP client di R2 seperti berikut :



Gambar 61.5 Konfigurasi PPtP Client di R1

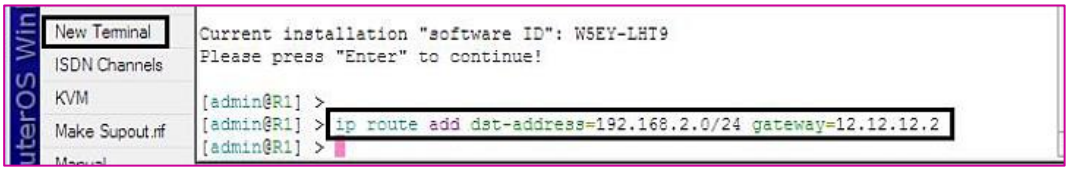


Gambar 61.6 Konfigurasi PPtP client di R2

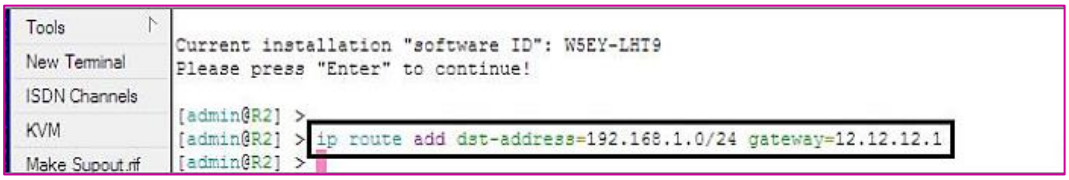
Setelah mengkonfigurasi PPtP server dan client seperti diatas, maka R1 dan R2 akan memiliki IP Address Dynamic seperti berikut :

Gambar 61.7 Konfigurasi user pada PPtP Server

Langkah terakhir yang perlu kita lakukan adalah mengkonfigurasi static routing pada R1 dan R2 untuk menghubungkan PC1 dan PC2

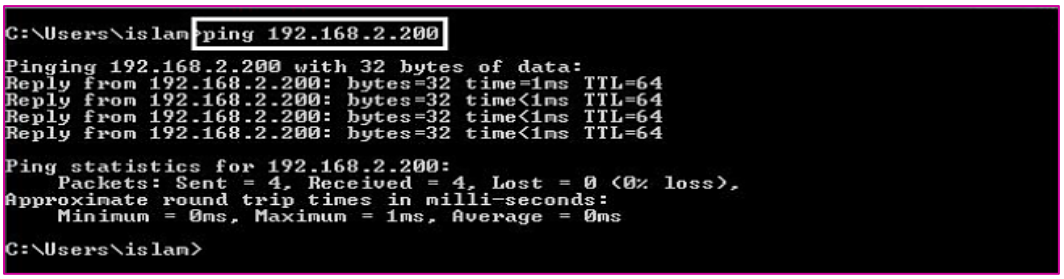


Gambar 61.8 Konfigurasi static routing di R1



Gambar 61.9 Konfigurasi static routing pada R2

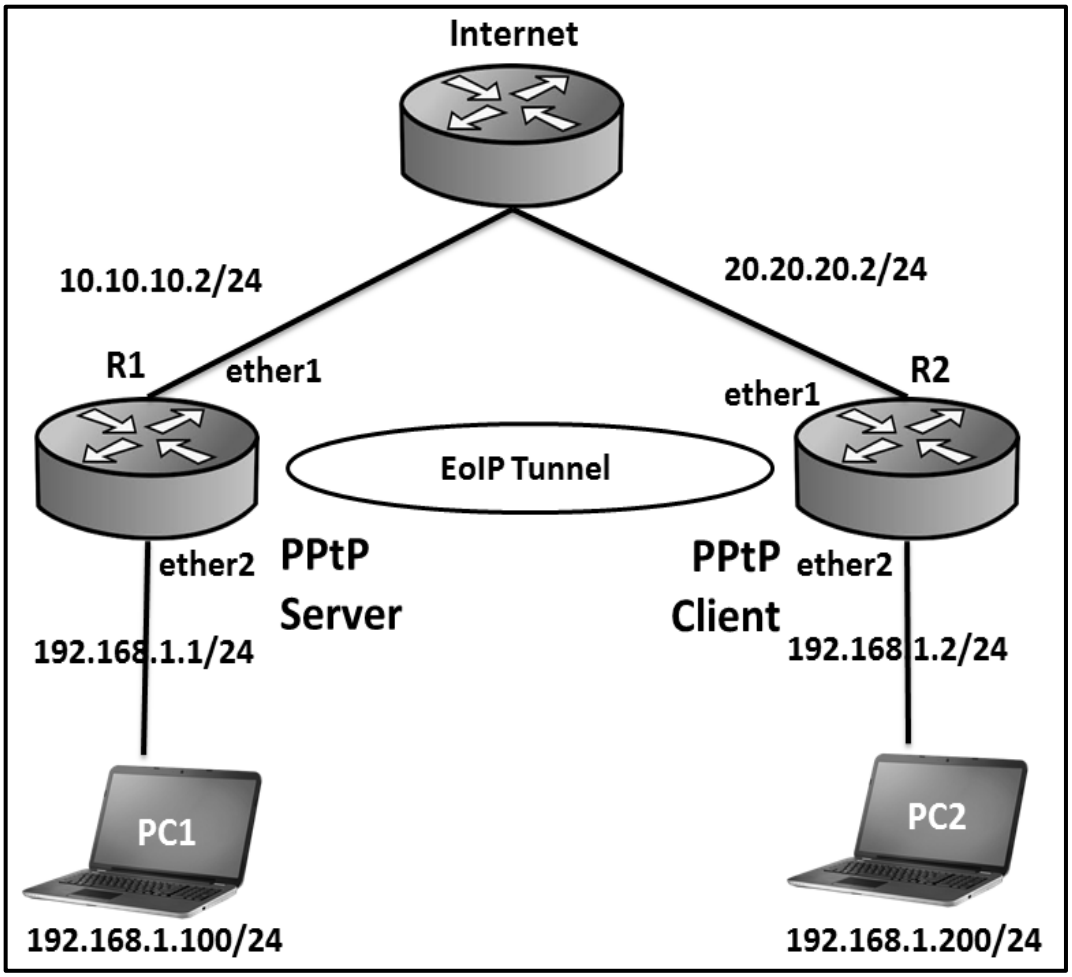
Setelah mengkonfigurasi static route seperti diatas, maka PC1 dan PC2 sudah bisa saling beerkomunikasi.



Gambar 61.10 Ping dari PC1 ke PC2

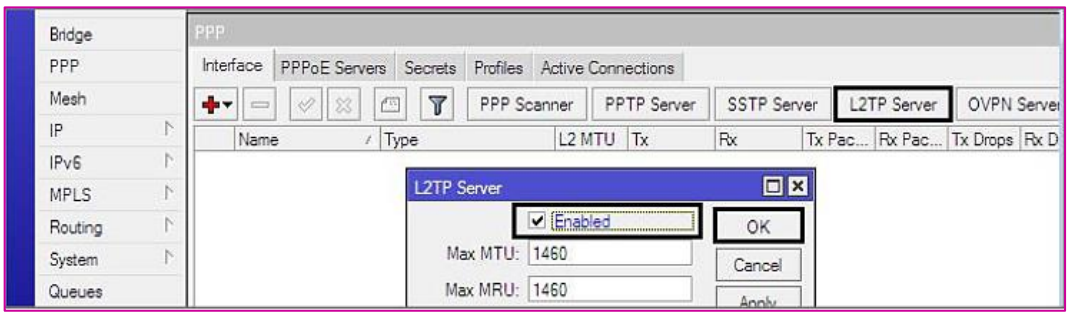
LAB 62 – L2TP Tunnel

Berikut adalah topologi yang akan kita gunakan :

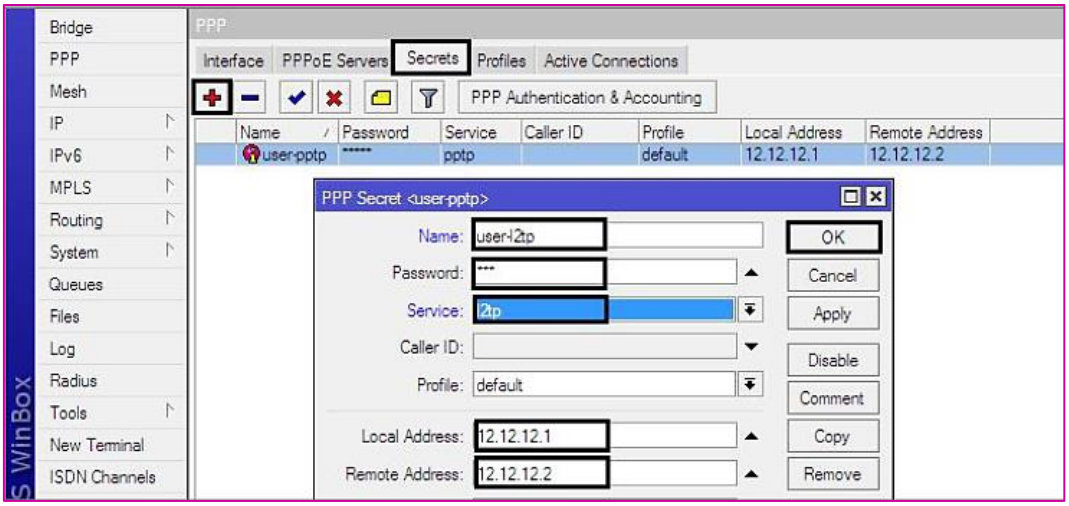


Gambar 62.1 Topologi L2TP Tunnel

Konsepnya sama persis dengan PPtP, perbedaannya hanya terletak pada protocol dan beberapa konfigurasi saja. Berikut konfigurasi L2TP Server pada R1.

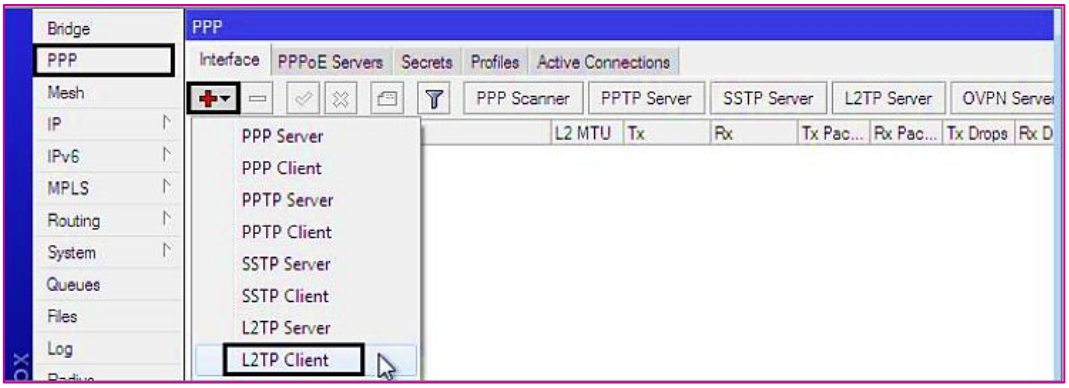


Gambar 62.2 Konfigurasi L2TP Server di R1

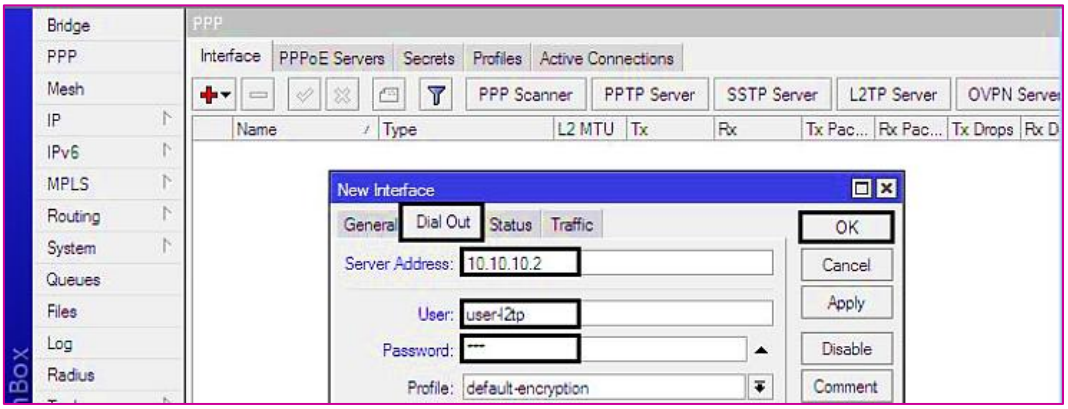


Gambar 62.3 Konfigurasi L2TP Server di R1

Selanjutnya konfigurasikan L2TP Client di R2

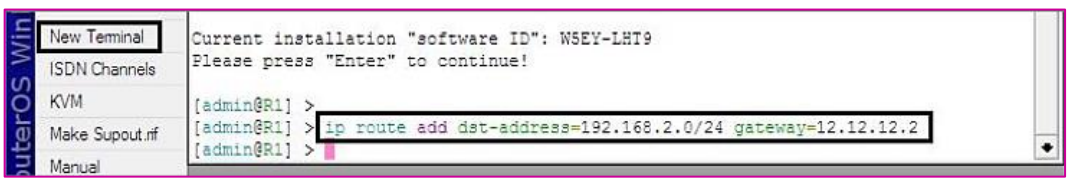


Gambar 62.4 Konfigurasi L2TP Client di R2

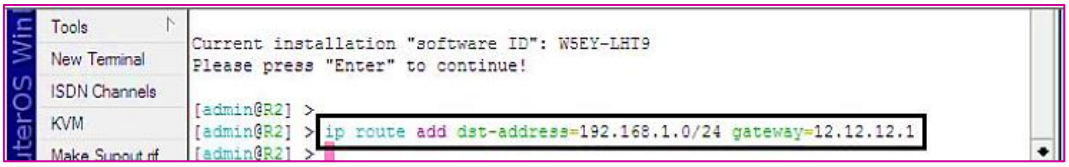


Gambar 62.5 Konfigurasi L2TP Client di R2

Terakhir kita konfigurasikan static routing di R1 dan R2, serta PC1 dan PC2 bisa saling berkomunikasi

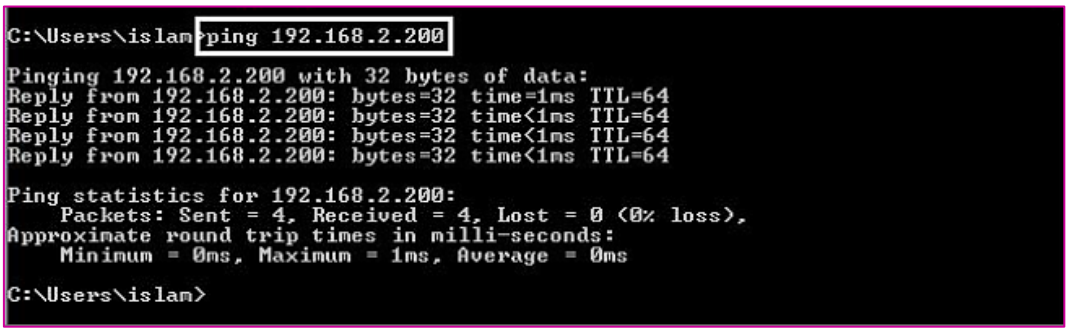


Gambar 62.6 Konfigurasi routing Static di R1



Gambar 62.7 Konfigurasi Static Routing di R2

Untuk pengujian coba kita lakukan ping dari PC1 ke PC2

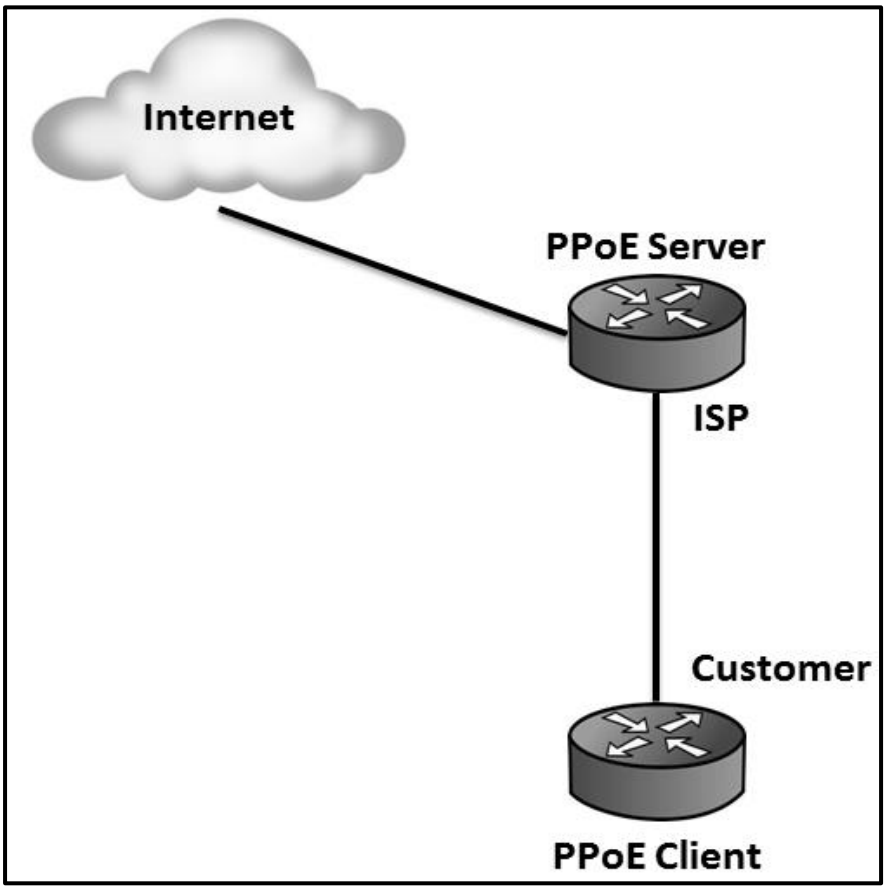


Gambar 62.8 Pengujian ping dari PC1 ke PC2

LAB 63 – PPPoE Tunnel Skenario 1

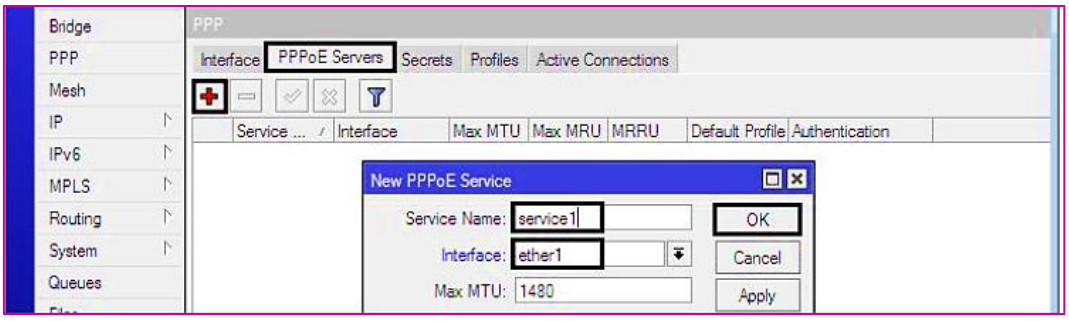
PPPoE Tunnel biasanya dikonfigurasikan pada sisi ISP (provider), untuk keperluan authentikasi customer.

Berikut adalah topologi yang akan kita gunakan :

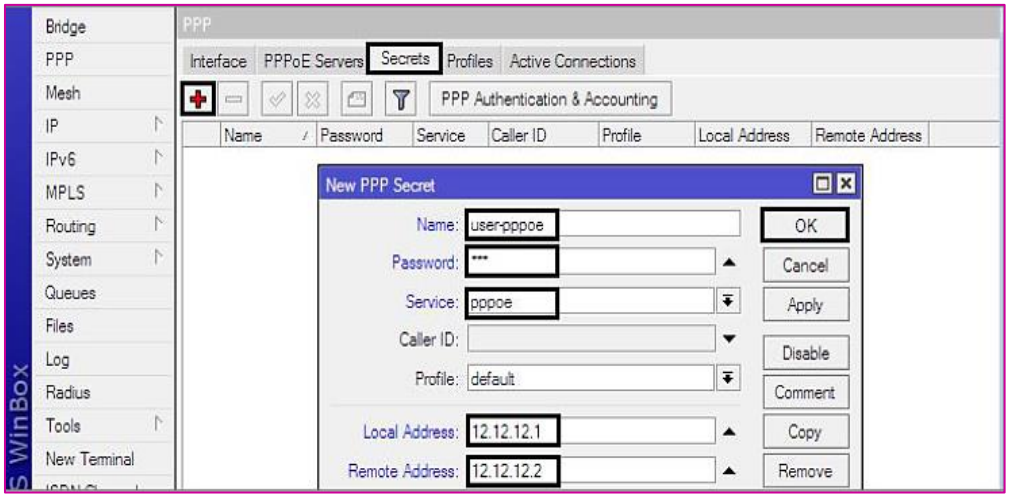


Gambar 63.1 Topologi PPtP Tunnel

Berikut konfigurasi PPPoE Server di R1

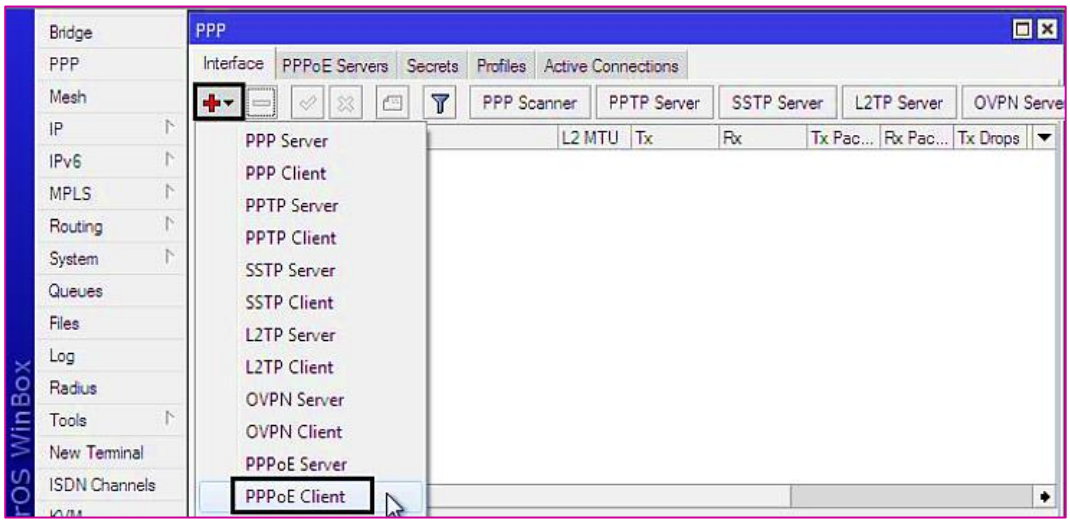


Gambar 63.2 Konfigurasi PpoE Server di R1

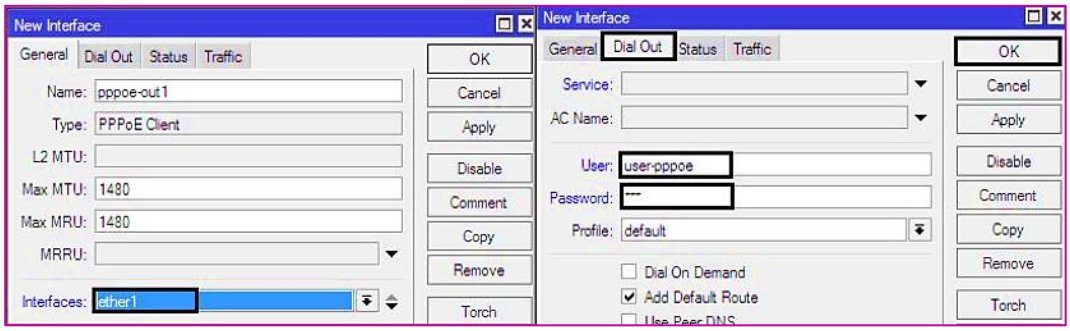


Gambar 63.3 Konfigurasi PpoE Server di R1

Selanjutnya kita konfigurasikan PPPoE Client di R2



Gambar 63.4 Konfigurasi PpoE Client di R2

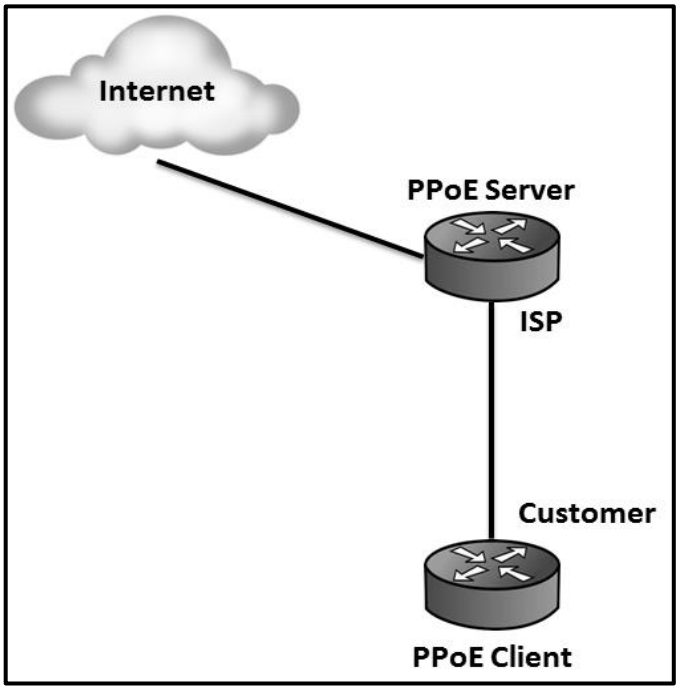


Gambar 63.5 Konfigurasi PpoE Client di R2

LAB 64 – PPPoE Tunnel Skenario 2

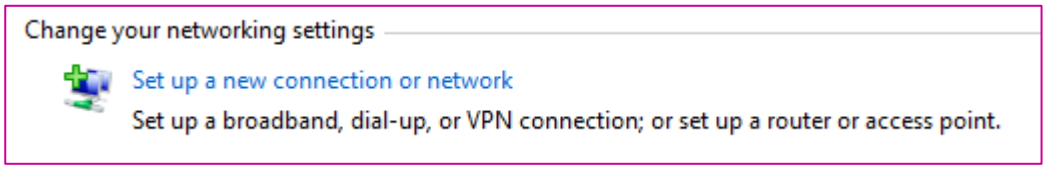
Pada lab 63, kita telah membuat skenario bahwa customer berupa router mikrotik.

Selanjutnya pada lab ini kita akan membuat skenario bahwa client berupa komputer windows.

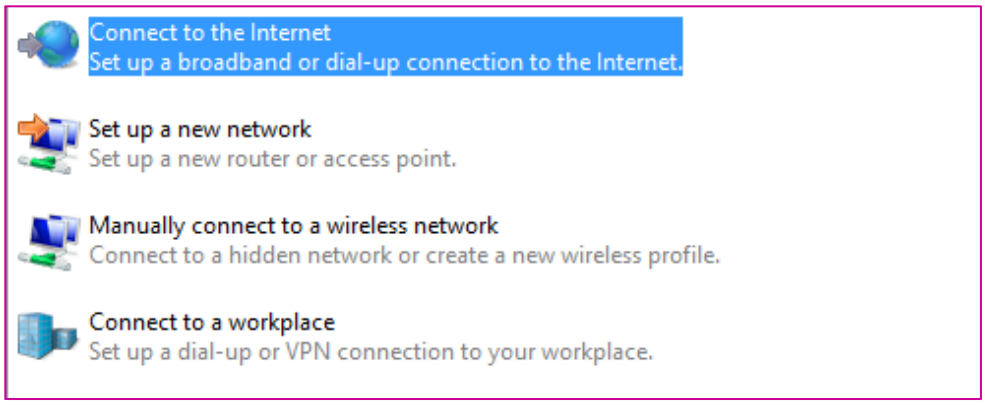


Gambar 63.1 Topologi PPPoE Tunnel

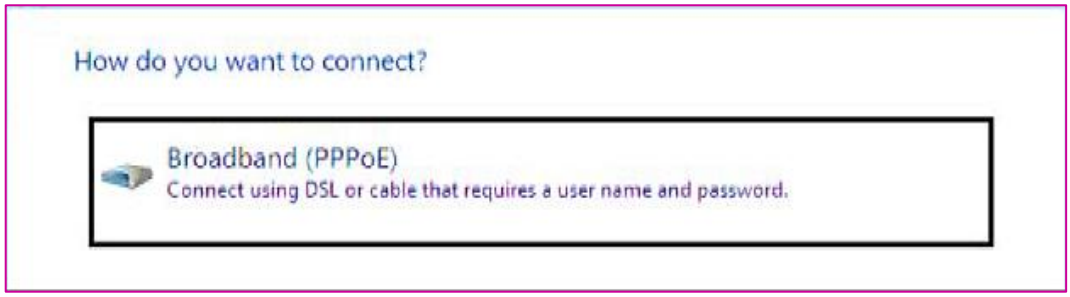
Untuk konfigurasi disisi PPPoE Server adalah sama percis dengan konfigurasi pada lab sebelumnya. Pada lab ini kita hanya akan fokus pada konfigurasi PPPoE client di wondows 7.



Gambar 63.2 Konfigurasi PPPoE Client di Windows 7



Gambar 63.3 Konfigurasi PPPoE Client di Windows



Gambar 63.4 Konfigurasi PpoE Client di Windows

Gambar 53.5 Konfigurasi PPPoE Client di Windows

PROFILE PENULIS

Assalamu'alaikum wr.wb

Saya adalah seorang gadis yang lahir delapan belas tahun lalu di Bekasi, tepatnya pada 23 Desember 1998. Nama lengkap saya Devitriana Elizami. Saya lahir dikeluarga yang serba berkecukupan, tetapi alhamdulillah dengan selalu syukur, hidup kami insyaallah selalu bahagia. Saya anak ke dua dari tiga bersaudara, dan saya anak perempuan satu-satunya.

Saya mempunyai hobi menggambar, dan saya bercita-cita menjadi seorang pelukis profesional. Sejak umur 14 tahun saya sudah mulai bekerja sebagai tukang gambar sambil bersekolah hingga duduk dibangku SMK. Penghasilan saya tidak bisa ditetapkan setiap bulannya, karena tergantung seberapa banyak saya mendapatkan pesanan dan seberapa sanggup saya mengerjakan pesanan tersebut.

Alhamdulillah saya selalu mendapatkan peringkat 5 besar di pendidikan formal dan sering mendapatkan beasiswa. Sedangkan dipendidikan non-formal saya pernah mendapat 2 piala beserta sertifikat yaitu juara 3 Lomba Menggambar Pahlawan dalam rangka Hari Pahlawan dan Bulan Bahasa, dan juara 2 Lomba Mading dalam rangka Memperingati Hari Kartini. Selain itu banyak lomba dan sertifikat yang saya menangkan di event online berbagai grup seni. Semua karya saya, saya share lewat account Facebook dengan nama DevitrianArt, dan Instagram saya DevitrianArt.

Saat ini saya duduk dibangku SMK kelas 12 berjurusan Teknik Komputer dan Jaringan di SMK Karya Guna Bhakti 2 Kota Bekasi. Saya baru saja menyelesaikan training networking MTCNA, MTCRE, dan CCNA untuk mendapatkan sertifikat internasional dengan mengikuti examinationnya. Saat ini saya sedang menyelesaikan 3 buku yaitu CCNA, MTCNA, dan MTCRE. Dan website aktif saya yaitu https://www.curhatanseorangit.wordpress.com .

Pasti banyak yang bertanya-tanya, kenapa saya mengambil 2 arah yang berbeda (Seni dan Komputer), saya senang dan merasa tertantang jika menguasai 2 hal yang bersamaan. Kalau bisa saya ingin jadi Multitalent ☺

Lambat laun cita-cita sebagai pelukis profesional itu mulai bercabang. Perkembangan zaman yang semakin hari semakin canggih, dan persaingan di dunia kerja pun makin ketat. Membuat saya berfikir harus memanfaatkan dan mengembangkan potensi diri. Masalah "**cita-cita**" sebenarnya hanya patokan, yang pasti maksimalkanlah apa yang akan dihadapi, dengan doa dan ikhtiar insyaallah hasilnya akan lebih baik.

Demikian profile saya, jika ada kesalahan kata mohon dimaafkan. Terimasih.
Wassalamu'alaikum wr.wb